Math-for-industry
Education & Research Hub

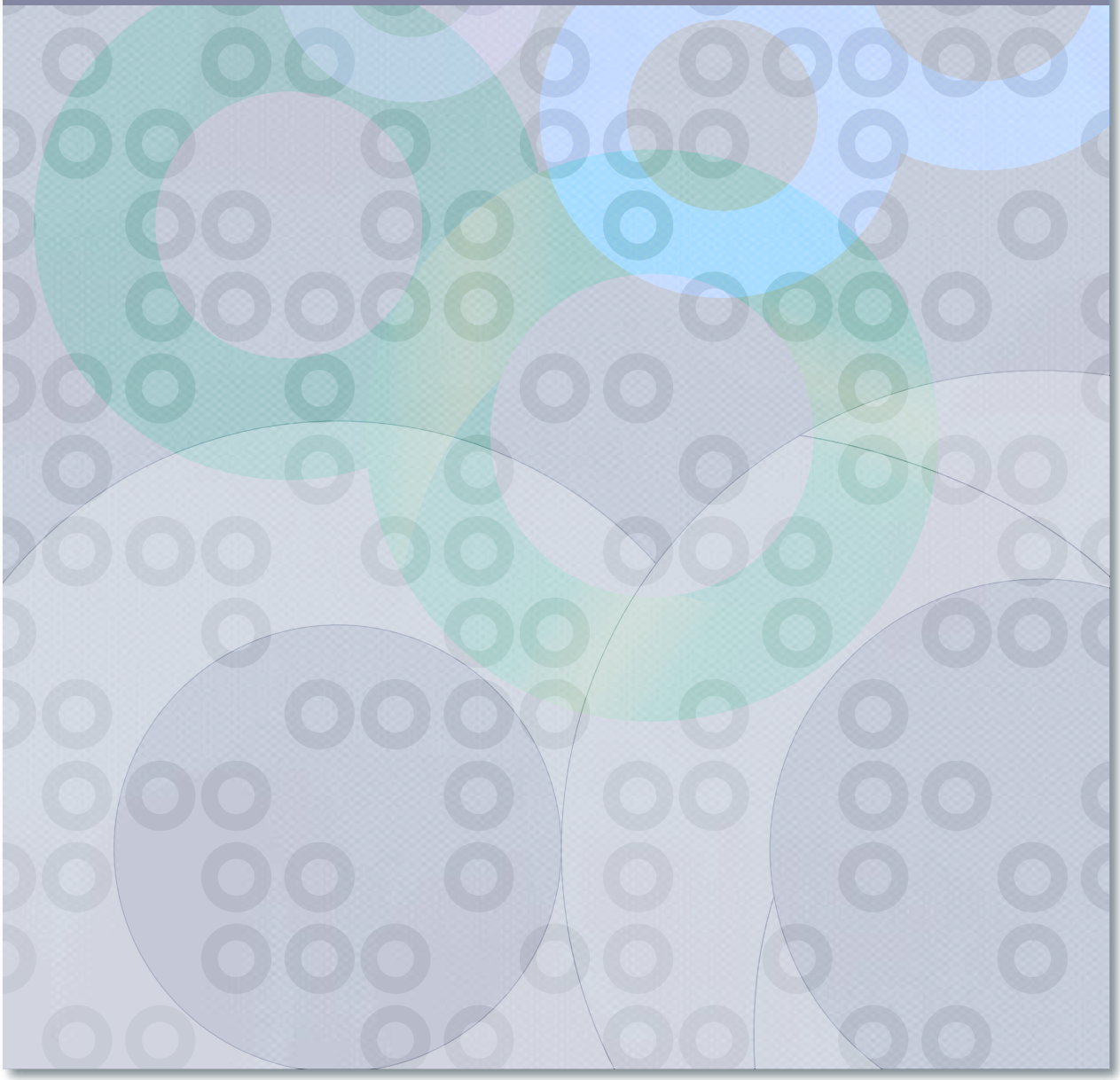
ISSN2188-1200

2023 年度採択分　九州大学マス・フォア・インダストリ研究所 共同利用研究集会

現代暗号に対する安全性解析・攻撃の数理

編集：國廣昇, 池松泰彦, 伊豆哲也, 穴田啓晃, 縫田光司

九州大学マス・フォア・インダストリ研究所



MI Lecture Note Vol.94 : Kyushu University

2023年度採択分 九州大学マス・フォア・インダストリ研究所 共同利用研究集会

現代暗号に対する安全性解析・攻撃の数理

編集：國廣　昇，池松泰彦，伊豆哲也，穴田啓晃，縫田光司

About MI Lecture Note Series

The Math-for-Industry (MI) Lecture Note Series is the successor to the COE Lecture Notes, which were published for the 21st COE Program "Development of Dynamic Mathematics with High Functionality," sponsored by Japan's Ministry of Education, Culture, Sports, Science and Technology (MEXT) from 2003 to 2007. The MI Lecture Note Series has published the notes of lectures organized under the following two programs: "Training Program for Ph.D. and New Master's Degree in Mathematics as Required by Industry," adopted as a Support Program for Improving Graduate School Education by MEXT from 2007 to 2009; and "Education-and-Research Hub for Mathematics-for-Industry," adopted as a Global COE Program by MEXT from 2008 to 2012.

In accordance with the establishment of the Institute of Mathematics for Industry (IMI) in April 2011 and the authorization of IMI's Joint Research Center for Advanced and Fundamental Mathematics-for-Industry as a MEXT Joint Usage / Research Center in April 2013, hereafter the MI Lecture Notes Series will publish lecture notes and proceedings by worldwide researchers of MI to contribute to the development of MI.

October 2022
Kenji Kajiwara
Director, Institute of Mathematics for Industry

Mathematics of Security Analysis for Modern Cryptography

MI Lecture Note Vol.94, Institute of Mathematics for Industry, Kyushu University
ISSN 2188-1200
Date of issue: January 11, 2024
Editors: Noboru Kunihiro, Yasuhiko Ikematsu, Tetsuya Izu, Hiroaki Anada, Koji Nuida
Publisher:
Institute of Mathematics for Industry, Kyushu University
Graduate School of Mathematics, Kyushu University
Motooka 744, Nishi-ku, Fukuoka, 819-0395, JAPAN
Tel +81-(0)92-802-4402, Fax +81-(0)92-802-4405
URL https://www.imi.kyushu-u.ac.jp/

はじめに

情報通信の発達により，暗号技術への期待がより一層高まっている．暗号を長期的に安全に使用するためには，アドホックな安全性解析ではなく，数理的な基盤にしっかり立脚した精密な安全性評価が必要である．暗号の安全性評価において，様々な，なおかつ、本質的に重要な場面で数理的な側面が登場する．本研究集会は，「現代暗号に対する安全性解析・攻撃の数理」というテーマに関して，最新成果を紹介するとともに，研究討議を行うことを目的として開催された．以下では，本研究集会で扱ったテーマについて述べる．

近年になり量子計算機の脅威が現実になりつつある．このような状況下で，現在使われている暗号の量子計算機に対する厳密な安全性評価が必須である．さらに，量子計算機を用いても破られない暗号（耐量子計算機暗号）の研究も進んでいる．格子問題や多次多変数問題，符号問題，同種写像問題などの数学的に定義された問題の困難さが用いられており，安全性評価が必須である．

現実社会での脅威，例えばサイドチャネル攻撃に対しても安全性を担保できなくてはならない．秘密鍵が持つ代数的な性質と統計量を組み合わせることにより秘密鍵を復元する攻撃もあり，数理的な側面が大きい．サイドチャネル攻撃に対する安全性評価に加えて，ハードウェアにまで踏み込んだ安全性評価も重要な研究テーマである．

現在の暗号技術は，公開鍵暗号技術と共通鍵暗号技術の両方の組み合わせにより実現している．送信者と受信者間で鍵共有ができれば，共通鍵暗号を利用できるため，共通鍵暗号の安全性評価は，常に重要である．共通鍵暗号の安全性評価では，混合整数線形計画法などの数理的な道具が活用されている．

本研究集会の主たる目的は，暗号の安全性解析を中心に据え，安全性解析に対する様々な数学的アプローチを共有することである．その目的を達成させるため，日本及び海外から産業界と学界の研究者を集め，暗号の安全性解析の最近の結果についての招待講演を行った．本会議録は，研究集会の成果物として，すべての講演の短い要約及びスライドを含んだものである．

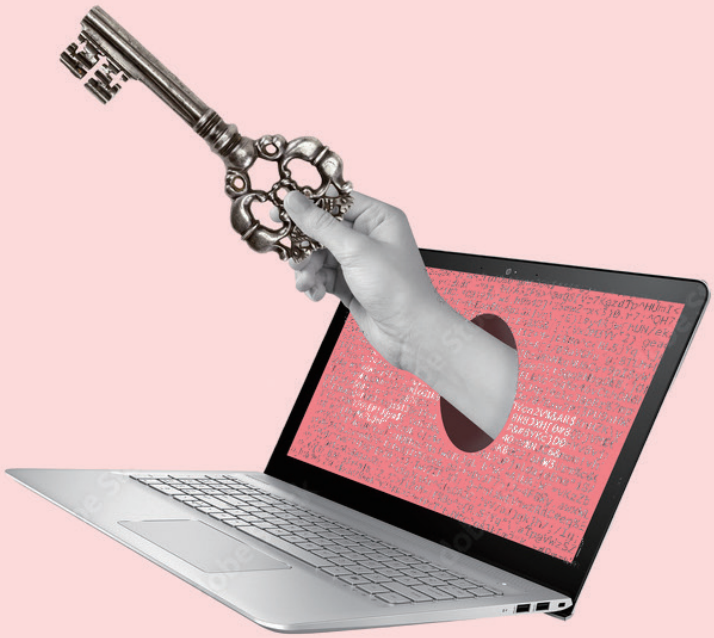
研究代表者　國廣昇
筑波大学システム情報系

謝辞

本ワークショップは，2023 年度九州大学 IMI 研究所共同利用研究 一般研究-研究集会(I)の助成を受けて行われました．暗号の安全性解析の研究者が一同に集まる場は非常に貴重であり，このような機会を頂けたことに感謝いたします．

2023年度九州大学マス・フォア・インダストリ研究所 共同利用・共同研究　一般研究–研究集会（I）

現代暗号に対する安全性解析・攻撃の数理



2023

9.20水 ▶ 22金

ハイブリッド開催　JR博多シティ9階会議室1

参加無料
事前申込制

講演者

林　優一（奈良先端科学技術大学院大学）
上野　嶺（東北大学）
Abdul Rahman Taleb (CryptoExperts and Sorbonne University)
井上　明子（NEC）
藤堂　洋介（NTT）
大西　健斗（三菱電機）
山口　純平（富士通）
草川　恵太（Technology Innovation Institute）
伊東　燦（NTT）

研究代表者

國廣　昇（筑波大学）

組織委員

池松　泰彦（九州大学・IMI）
伊豆　哲也（富士通）
穴田　啓晃（青森大学）
縫田　光司（九州大学・IMI）

共催機関

九州大学マス・フォア・インダストリ研究所
JST CREST「ポスト量子社会が求める高機能暗号の数理 基盤創出と展開」
富士通株式会社

九州大学 KYUSHU UNIVERSITY
Institute of Mathematics for Industry Kyushu University
Joint Research Center for Advanced and Fundamental Mathematics-for-Industry
文部科学大臣認定「産業数学の先進的・基礎的共同研究拠点」
九州大学マス・フォア・インダストリ研究所

https://joint.imi.kyushu-u.ac.jp/post-9072/

現代暗号に対する安全性解析・攻撃の数理

開催日程：9/20(水) - 9/22(金)
開催場所：JR 博多シティ 9 階会議室 1

9/20（水）

13:00-13:10 Opening

Session 1: ハードウェアの安全性

13:10-14:10 林優一（奈良先端科学技術大学院大学）
現代暗号を含むハードウェアからの電磁的情報漏えいの数理
【アブストラクト】
本講演では、現代暗号を含むハードウェアからの電磁的情報漏えいメカニズムに着目し、漏えい源となる暗号モジュールから電磁波を通じてモジュール内部の秘密鍵が機器外部に漏えいする過程を数理モデルにより説明する。また、電磁気学の相反性から、機器外部から到来した電磁波によって暗号モジュールから秘密鍵が漏えいする過程も同様のモデルで説明できることを概説する。

14:25-15:25 上野嶺 (東北大学)
メモリ暗号化のための暗号技術とハードウェアアーキテクチャ
【アブストラクト】
CPU の外部に配置されるメインメモリは盗聴や改ざんなどの脅威に晒されうるため，それに対抗するためにメモリ暗号化が用いられる．特に近年では，不揮発メモリ (NVM) の高性能化や大容量化に伴い，データセンタや IoT 機器，さらに現代の CPU において省消費電力化や高性能化を目的として不揮発メモリ (NVM) の採用例が増えている．一方で，NVM はそのデータの永続性から盗聴や改ざんのリスクが DRAM に比べて高まる．そこで，大容量の NVM をリアルタイムで暗号化・認証するメモリ暗号化技術が強く求められる．本講演では，セキュア NVM のための暗号化技術およびそのハードウェアアーキテクチャについて，講演者らによる最新の成果を交えながら概説する．

15:40-16:40　Abdul Rahman Taleb (CryptoExperts and Sorbonne University)
Towards Achieving Provable Side-Channel Security in Practice
Abstract:
Physical side-channel attacks are powerful attacks that exploit a device's physical emanations to break the security of cryptographic implementations. Many countermeasures have been proposed against these attacks, especially the widely-used and efficient masking countermeasure. Nevertheless, proving the security of masked implementations is challenging. Current techniques rely on empirical approaches to validate the security of such implementations. On the other hand, the theoretical community introduced leakage models to provide formal proofs of the security of masked implementations. Meanwhile, these leakage models rely on physical assumptions that are difficult to satisfy in practice, and the literature lacks a clear framework to implement proven secure constructions on a physical device while preserving the proven security.

9/21(木)

Session 2: 共通鍵暗号の安全性

10:00-11:00 井上明子（NEC）
共通鍵暗号の認証暗号利用モードの安全性と攻撃について
【アブストラクト】
認証暗号は平文の秘匿と暗号文の改ざん検知が同時に実現できる共通鍵暗号方式である．その安全性は, 2000 年に秘匿と改ざん検知の 2 つとして正式に定義されたが, その後, これらの安全性を満たす認証暗号が実装上の過失により破れる場合があることや, 認証暗号を用いるプロトコルが, 秘匿と改ざん検知以上の安全性を認証暗号に要求している場合があることが攻撃により示されている．本発表では, ブロック暗号等の固定長入出力暗号部品を用いた認証暗号構成を中心の話題として, 基本的な認証暗号の安全性及びそれに対する攻撃, そして上記のように基本の安全性を超えた攻撃や, それらを考慮した認証暗号の拡張された安全性について紹介する．

11:15-12:15 藤堂洋介（NTT）
キャッシュランダム化関数の安全性モデルと SCARF の設計・安全性評価
【アブストラクト】

キャッシュ攻撃とはキャッシュとメモリの遅延差を利用したサイドチャネル攻撃である。キャッシュ攻撃を防ぐ方法としてキャッシュランダム化が注目されている。Usenix Security2023 で、キャッシュランダム化関数の安全性モデル、調整可能暗号を用いた設計理論、具体的な関数 SCARF を設計・発表した。本講演では、この安全性モデルの解説、実際の SCARF の設計プロセス、SCARF に対する具体的な暗号解読の取り組みを紹介する。

Session 3: 量子計算機に対する安全性

13:45-14:45 大西健斗（三菱電機）
効率的な近似量子フーリエ変換を利用した Shor アルゴリズム
【アブストラクト】
本発表では，素因数分解問題を解く Shor アルゴリズムの効率化手法について議論する．現在利用されている主な公開鍵暗号として，RSA 暗号や楕円曲線暗号があり，素因数分解問題や離散対数問題に安全性の基盤を置いている．Shor アルゴリズムは，これらの問題を多項式時間で解く量子アルゴリズムである．現在の公開鍵暗号が危殆化する時期を見積もるため，Shor アルゴリズムの計算コスト評価は極めて重要である．本発表では，近似量子フーリエ変換に基づく Shor アルゴリズムについて議論する．特に，本発表では，将来実現しうる大規模な耐故障性量子計算機を考慮し，耐故障性を持つ Shor アルゴリズムについて計算コストの削減方法を議論する．

15:00-16:00 山口純平（富士通）
素因数分解問題に対する新しい量子アルゴリズム SQIF の実装と解析
【アブストラクト】
2022 年 12 月に Shor よりも少ない量子ビットで素因数分解可能とする
新しい量子アルゴリズム SQIF(Sublinear-resource Quantum Integer Factorization)が提案された．SQIF は平方差法をベースとしており，特に平方差法の関係式計算を組み合わせ最適化問題に帰着し， その近似解を量子アルゴリズム QAOA を用いて計算することで関係式を得る．本講演では，2023 年 5 月の CSEC で発表した「格子と最適化手法を用いた素因数分解法の実験報告」の詳細を紹介する．まず SQIF の詳細を紹介し，関係式が数個しか計算できないという問題点を指摘する．次に，十分な数の関係式が計算可能な拡張 SQIF を提案し，その実験結果を紹介する．実験を大規模にするため QAOA の代わりに古典的なアニーリング計算を使用し， 11 から 55 ビットの合成数の素因数分解に成功した．最後に，2048 ビット合成数の分解に必要な量子ビット数および計算量の見積もりを与える．

16:10-16:40 田口 廉 (東京大学)
バイナリ ECDLP を解く Shor のアルゴリズムにおける楕円曲線加算の量子リソース削減
【アブストラクト】
離散対数問題を多項式時間で解く Shor のアルゴリズムの実装に係る量子リソース評価の研究が数多く行われており，バイナリ楕円曲線では量子逆元計算が主要な計算であることが知られている．その中でも我々は Toffoli ゲート数と深さの面でより有効な量子 FLT 逆元計算に着目する. 我々は, 既存の量子 FLT 逆元計算アルゴリズムを純粋に改良する量子 FLT 逆元計算アルゴリズムを提案し，量子ビット数をさらに削減できることを示す.

9/22(金)

Session 4: サイドチャネル攻撃に対する安全性

10:00-11:00 草川恵太（TII）
格子ベースの鍵カプセル化方式に対するサイドチャネル攻撃を利用した鍵回復攻撃
【アブストラクト】
量子計算機の開発の進展を受け、耐量子計算機暗号（PQC）の標準化や実装が盛んになっている。大きな影響を持つ NIST の PQC 標準化では、サイズ・速度・安全性といった観点から鍵カプセル化方式（KEM）として格子暗号の Kyber が選ばれた。一方、標準化される暗号は様々な機器で実装されることから、サイドチャネル攻撃耐性も重要視される。本発表では Kyber を中心とした格子暗号に対するサイドチャネル攻撃を利用した鍵回復攻撃を、紹介する。特に、サイドチャネル攻撃を用いて平文判定オラクルや復号オラクルを構築した後の、攻撃の効率化について紹介する。

11:20-12:20 伊東燦（NTT）
深層学習に基づくサイドチャネル攻撃とその対策
【アブストラクト】
暗号モジュールから副次的に発生する消費電力・漏洩電磁波（サイドチャネル情報）を用いることで、暗号モジュール内の秘密鍵を推定する攻撃をサイドチャネル攻撃という。本講演では、近年高い注目を集めているニューラルネットワークを用いたサイドチャネル攻撃（DL-SCA)について解説を行う。DL-SCA では、あらかじめ攻撃対象モジュールのサイドチャネル情報について学習することで、従来よりも強力な攻撃が可能なことが知られている。また、サイドチャネル攻撃に対する代表的な対策手法であるマスキング対策と、その理論的な安全性についても紹介し、マスキング対策が DL-SCA に対しても有効であることを説明する。

12:20-12:30 Closing

13:00-15:00 Free Discussion

目　次

現代暗号を含むハードウェアからの電磁的情報漏えいの数理
林　優一（奈良先端科学技術大学院大学）・・・・・・・・・・・・・・・・・・・・・・・・・1

メモリ暗号化のための暗号技術とハードウェアアーキテクチャ
上野　嶺（東北大学）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・29

Towards Achieving Provable Side-Channel Security in Practice
Abdul Rahman Taleb（CryptoExperts and Sorbonne University）・・・・・・・・・・・・47

共通鍵暗号の認証暗号利用モードの安全性と攻撃について
井上明子（NEC）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・77

キャッシュランダム化関数の安全性モデルと SCARF の設計・安全性評価
藤堂洋介（NTT）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・107

効率的な近似量子フーリエ変換を利用した Shor アルゴリズム
大西健斗（三菱電機）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・139

素因数分解問題に対する新しい量子アルゴリズム SQIF の実装と解析
山口純平（富士通）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・167

バイナリ ECDLP を解く Shor のアルゴリズムにおける楕円曲線加算の量子リソース削減
田口　廉（東京大学）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・185

格子ベースの鍵カプセル化方式に対するサイドチャネル攻撃を利用した鍵回復攻撃
草川恵太（TII）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・205

深層学習に基づくサイドチャネル攻撃とその対策
伊東　燦（NTT）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・239

Mathematics of Electromagnetic Information Leakage Including Modern Cryptography

Hayashi Yuichi

Nara Institute of Science and Technology
yu-ichi@is.naist.jp

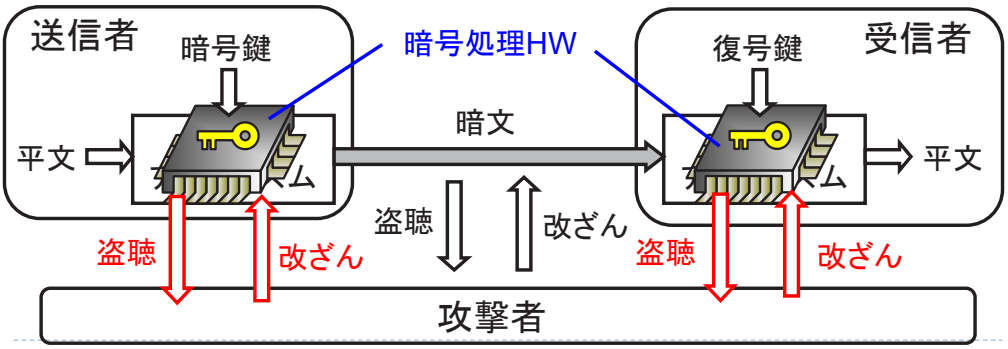
This talk focuses on the mechanism of electromagnetic information leakage from hardware, including modern cryptography, and explains the process of leakage of a secret key inside a module to the outside of a device through electromagnetic waves using a mathematical model. The same model can also explain the process of secret key leakage due to intentional electromagnetic interference based on the electromagnetic reciprocity theorem.

現代暗号を含むハードウェアからの電磁的情報漏えいの数理

林　優一（NAIST）

暗号処理ハードウェアへの物理攻撃

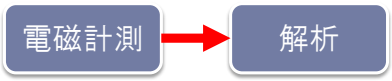
- 物理攻撃
  - 暗号処理HWへの物理的アクセスに基づく攻撃
  - 暗号アルゴリズム設計段階で考慮されない攻撃：安全と言われているアルゴリズムでも解読される可能性がある
  - ハードウェア実装の安全性が不可欠



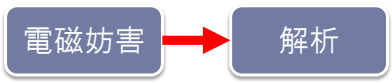
2

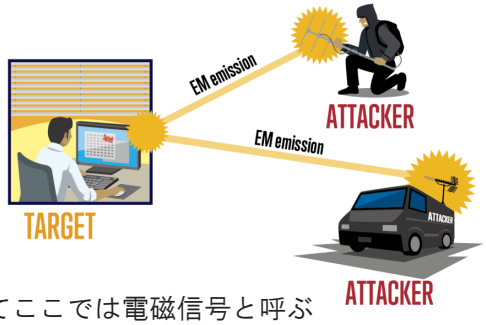
この講演で着目するポイント

①漏えい電磁信号※1による脅威
→サイドチャネル攻撃、TEMPEST



②意図的な電磁妨害※2による脅威
→故障利用攻撃





※1 電流・電圧・電磁界などを総称してここでは電磁信号と呼ぶ
※2 レーザー照射含む（最終的には基板上の電磁気的な変化を引き起こすため）

3

マクスウェルの方程式

$$
\begin{aligned}
\nabla \cdot \boldsymbol{B}(t,\boldsymbol{x}) &= 0 \\
\nabla \times \boldsymbol{E}(t,\boldsymbol{x}) + \frac{\partial \boldsymbol{B}(t,\boldsymbol{x})}{\partial t} &= 0 \\
\nabla \cdot \boldsymbol{D}(t,\boldsymbol{x}) &= \rho(t,\boldsymbol{x}) \\
\nabla \times \boldsymbol{H}(t,\boldsymbol{x}) - \frac{\partial \boldsymbol{D}(t,\boldsymbol{x})}{\partial t} &= \boldsymbol{j}(t,\boldsymbol{x})
\end{aligned}
$$

4

The EM Side-Channel(s)

The EM Side–Channel(s)

Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi

IBM T.J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598
{agrawal,barch,jrrao,rohatgi}@us.ibm.com

Abstract. We present results of a systematic investigation of leakage of compromising information via electromagnetic (EM) emanations from CMOS devices. These emanations are shown to consist of a multiplicity of signals, each leaking somewhat different information about the underlying computation. We show that not only can EM emanations be used to attack cryptographic devices where the power-side-channel is unavailable, they can even be used to break power analysis countermeasures.

1 Introduction

Side–channel cryptanalysis has been used successfully to attack many cryptographic implementations [7,8]. Most published literature on side–channels deals with attacks based on timing or power. With the recent declassification of portions of the TEMPEST documents [5], and other recent results [9,6], an awareness of the potential of the EM side–channel is developing. However, some basic questions remain unanswered. For instance, what are the causes and types of EM emanations? How does information leaked via EM emanations compare with leakages from other side–channels? What new devices and implementations are vulnerable to EM side–channel attacks? Can the EM side–channel overcome countermeasures designed to provide protection against other side–channel attacks? With questions such as these in mind, we conducted a systematic investigation of EM side–channel leakage from CMOS devices. In this paper, we address each of these basic questions.

In Section 2, we discuss the causes and types of various EM signals and describe the equipment required to capture and extract these signals. In addition to the direct emanations, EM signals consist of several compromising signals which are unintentional and are found in unexpected places. For instance, researchers have thus far missed the faint, but far more compromising amplitude modulated EM signals present even in the power line.

Section 3 presents experimental results illustrating various types of emanations and Section 4 provides a qualitative comparison of information leakages from EM and power. These results are very instructive. One crucial observation is that even a *single* EM sensor can easily pick up multiple compromising signals of different types, strengths and information content. Moreover, significant amount of compromising information is to be found in very low energy signals.

B.S. Kaliski Jr. et al. (Eds.): CHES 2002, LNCS 2523, pp. 29–45, 2003.

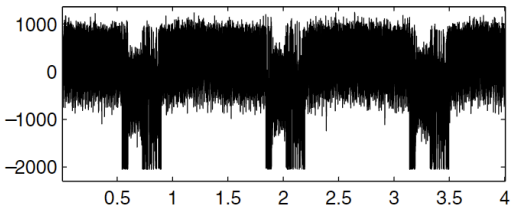


Fig. 5. EM Signal from SSL Accelerator S

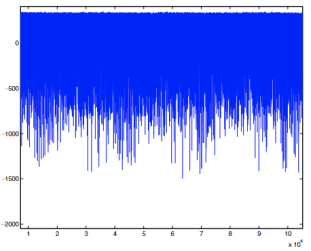


Fig. 6. EM Signal on Power Line for 3 rounds of DES on smartcard B

5

Get your hands off my laptop: physical side-channel key-extraction attacks on PCs

J Cryptogr Eng (2015) 5:95–112
DOI 10.1007/s13389-015-0100-7

CrossMark

CHES 2014

Get your hands off my laptop: physical side-channel key-extraction attacks on PCs

Extended version

Daniel Genkin[1,2] · Itamar Pipman[2] · Eran Tromer[2]

Received: 5 December 2014 / Accepted: 8 April 2015 / Published online: 6 May 2015

Abstract We demonstrate physical side-channel attacks on a popular software implementation of RSA and ElGamal, running on laptop computers. Our attacks use novel side channels, based on the observation that the "ground" electric potential, in many computers, fluctuates in a computation-dependent way. An attacker can measure this signal by touching exposed metal on the computer's chassis with a plain wire, or even with a bare hand. The signal can also be measured on the ground shield at the remote end of Ethernet, USB and display cables. Through suitable cryptanalysis and signal processing, we have extracted 4096-bit RSA keys and 3072-bit ElGamal keys from laptops, via each of these channels, as well as via power analysis and electromagnetic probing. Despite the GHz-scale clock rate of the laptops and numerous noise sources, the full attacks require a few seconds of measurements using Medium Frequency (MF) signals (around 2 MHz), or one hour using Low Frequency (LF) signals (up to 40 kHz).

Keywords Side channel attack · Power analysis · RSA · ElGamal

✉ Eran Tromer
ern-jon2rran@tromer.org; tromer@tau.ac.il
Daniel Genkin
danielg3@cs.technion.ac.il
Itamar Pipman
itamarp@tau.ac.il

1 Technion, Haifa, Israel
2 Tel Aviv University, Tel Aviv, Israel

1 Introduction

1.1 Background

Side-channel attacks that exploit unintentional and abstraction-defying information leakage from physical computing devices have proven effective in breaking the security of numerous cryptographic implementations [4,23,26]. However, most research attention has been focused on small devices: smartcards, RFID tags, FPGAs, microcontrollers, and simple embedded devices. The "PC" class of devices (commodity laptop/desktop/server computers) has been studied from the perspective of side channels measured by resident software (see [20] and subsequent works) and from peripherals (e.g., [25]).

PCs, however, have received little academic attention with regard to physical emanations from cryptographic computations, presumably due to three main barriers. First, PCs have highly complicated system architecture and CPU micro architecture, with many noise sources and asynchronous events. Fine low-level events are thus difficult to model and measure. Second, most physical side-channel cryptanalysis approaches require the leakage signal to be acquired at rates well beyond the device's clock rate; for multi-GHz CPUs, the requisite equipment is expensive, and the signals are difficult to probe. Finally, attack scenarios differ: the aforementioned small devices are often deployed into potentially malicious hands, where they could be subjected to lengthy or invasive attacks; but for PCs, the typical scenario (short of theft) is where a physical attacker gains physical proximity for a restricted amount of time, and must operate surreptitiously.

Recently, a key extraction attack on PCs was demonstrated using the acoustic side channel, addressing all three barriers: using a chosen-ciphertext attack, the sound emanations of interest are made very robust, brought down

Springer

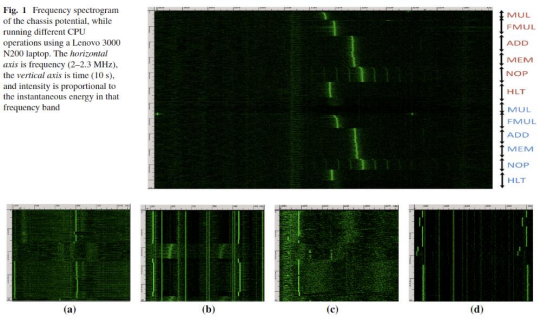
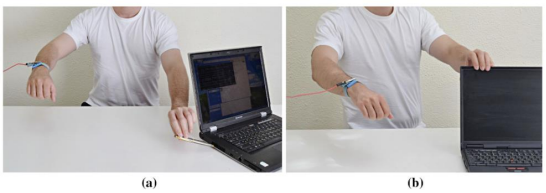


Fig. 1 Frequency spectrogram of the chassis potential, while running different CPU operations using a Lenovo 3000 N200 laptop. The *horizontal axis* is frequency (2–2.3 MHz), the *vertical axis* is time (10 s), and intensity is proportional to the instantaneous energy in that frequency band

Fig. 2 Chassis measurements of various target computers performing MUL, HLT and MEM in this order. Note that the three operations can be distinguished on all machines. **a** Dell Latitude E6400, **b** Gateway W340UA, **c** Lenovo ThinkPad T61, **d** HP HDX 18



6

Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers

Session 2A: Side Channel 1 CCS'18, October 15-19, 2018, Toronto, ON, Canada

Screaming Channels:
When Electromagnetic Side Channels Meet Radio Transceivers

Giovanni Camurati, EURECOM, camurati@eurecom.fr
Sebastian Poeplau, EURECOM, poeplau@eurecom.fr
Marius Muench, EURECOM, muench@eurecom.fr
Tom Hayes, EURECOM, hayes@eurecom.fr
Aurélien Francillon, EURECOM, aurelien.francillon@eurecom.fr

ABSTRACT

This paper presents a new side channel that affects mixed-signal chips used in widespread wireless communication protocols, such as Bluetooth and WiFi. This increasingly common type of chip includes the radio transceiver along with digital logic on the same integrated circuit. In such systems, the radio transmitter may unintentionally broadcast sensitive information from hardware cryptographic components or software executing on the CPU. The well-known electromagnetic (EM) leakage from digital logic is inadvertently mixed with the radio carrier, which is amplified and then transmitted by the antenna. We call the resulting leak "screaming channels". Attacks exploiting such a side channel may succeed over a much longer distance than attacks exploiting usual EM side channels.

The root of the problem is that mixed-signal chips include both digital circuits and analog circuits on the same silicon die in close physical proximity. While processing data, the digital circuits on these chips generate noise, which can be picked up by noise-sensitive analog radio components, ultimately leading to leakage of sensitive information. We investigate the physical reasons behind the channel, we measure it on several popular devices from different vendors (including Nordic Semiconductor nRF52832, and Qualcomm Atheros AR9271), and we demonstrate a complete key recovery attack against the nRF52832 chip. In particular, we retrieve the full key from the AES-128 implementation in ctr_aes_e of 1 m with a correlation attack.

Screaming channel attacks change the threat models of devices with mixed-signal chips, as those devices are now vulnerable from a distance. More specifically, we argue that protections against side channels (such as masking or hiding) need to be used on this class of devices. Finally, chips implementing other widespread protocols (e.g., 4G/LTE, BTE) need to be inspected to determine whether they are vulnerable to screaming channel attacks.

ACM ISBN 978-1-4503-5693-0/18/10…$15.00
https://doi.org/10.1145/3243734.3243982

KEYWORDS

Electromagnetic side channels; Mixed-signal chips

ACM Reference Format:

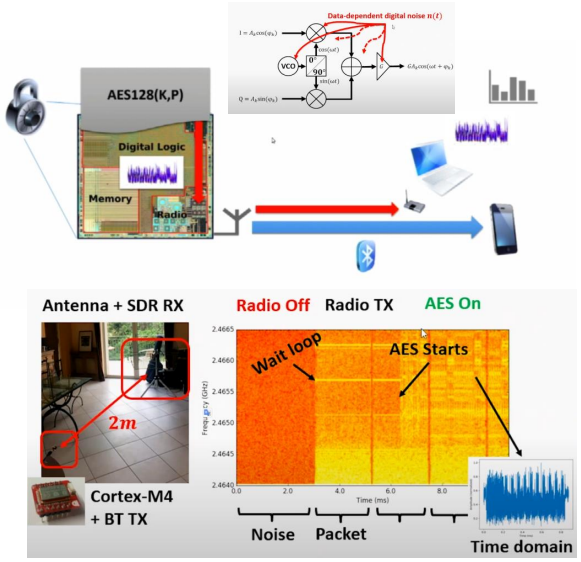
Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, and Aurélien Francillon. 2018. Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers. In *2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18), October 15–19, 2018, Toronto, ON, Canada.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3243734.3243982

1 INTRODUCTION

The drive for ever smaller and cheaper components in microelectronics has popularized so-called *mixed-signal circuits* (i.e., circuits in which analog and digital circuitry reside on the same piece of silicon, called a *die*). A typical example is a WiFi chip featuring a (digital) microcontroller as well as the (analog) radio. The special challenge of such designs is to separate the "noisy" digital circuits from the sensitive analog side of the system. In this paper we show that improper separation of digital and analog components leads to novel side-channel attacks that can break cryptography implemented in mixed-signal chips over at least 10 meters.

Modern cryptographic algorithms have been designed with a wide range of attacks in mind and are thus hardened against the more traditional ways of breaking the secrecy that cryptography is meant to provide. More recently, a lot of research attention has therefore been focused on side-channel attacks. In a side-channel scenario, attackers do not break the algorithm directly, but instead gain knowledge of the algorithm's internal state by means of observing its physical implementation; whenever such knowledge is not meant to be public, it can be used to undermine the algorithm's integrity. For example, Kocher et al. showed in 1999 that observing the power consumption of a smart card running an unprotected implementation of DES allows an attacker to guess the key, effectively breaking the cryptosystem [35]. Those results and related work spawned a long line of work on side-channel attacks against the implementations of all common cryptographic algorithms.

Measuring a system's power consumption usually requires direct physical access and potentially invasive application of probes on the power supply. A more discreet avenue of attack that has since been proved feasible are Electromagnetic (EM) attacks. Such attacks use inadvertent electromagnetic emissions that are common in digital circuitry—the key observation is that the emanations correlate with certain computations [5]. EM attacks often use specialized magnetic-field antennas in close proximity of the target chip, typically within



https://www.youtube.com/watch?v=0IafNH2WHxk

7

Eavesdropping a (Ultra-)High-Definition Video Display from an 80 Meter Distance Under Realistic Circumstance

Eavesdropping a (Ultra-)High-Definition Video Display from an 80 Meter Distance Under Realistic Circumstances

1st Pieterjan De Meulemeester, *Department CISS, ESAT, Royal Military Academy, KU Leuven*, Brussels 1000, Belgium, Leuven, 3000, Belgium, pieterjandemeulemeester@gmail.com
2nd Bart Scheers, *Department CISS, Royal Military Academy*, Brussels 1000, Belgium, bart.scheers@rma.ac.be
3rd Guy A.E. Vandenbosch, *Department ESAT, Katholieke Universiteit Leuven*, Leuven 3000, Belgium, guy.vandenbosch@kuleuven.be

***Abstract*—In this paper a method is presented which successfully reconstructs the video image of a video display unit (VDU) by exploiting its leakage emissions at a distance of 80 meters. The video image reconstruction is realized without any prior knowledge of the leaking VDU and by using commercial off-the-shelf material. The tested VDUs comprise of an UHD (ultra-high-definition) video display and a full HD (high-definition) video display, both employing an HDMI (high-definition multimedia interface) cable as a video data signaling interface linked to a notebook. The tested setups are located in an urban environment with sporadic radio emissions and occupied frequency bands. Subsequently, the methods and results are thoroughly discussed which give new insights into this video eavesdropping risk for improving video data security.**

***Index Terms*—TEMPEST, Compromising emanations, video display units, side-channel attack, HDMI, large distance.**

I. Introduction

Electronic-based systems inevitable leak energy in various forms such as in mechanical, thermal and electromagnetic energy. Consequently, the information security of electronic-based systems which process and store data e.g. personal computers (PC), notebooks, smartphones and smart devices could be compromised due to this leaking. In the specific case of electromagnetic leakage emissions originating from video display units (VDUs), it is confirmed that these emissions are correlated in some way to the processed/transmitted video data inside the device [1]–[3]. Video information is not encrypted rendering it vulnerable for data theft by exploiting the leakage emanations of the VDU. Consequently, these leakage emanations form a video eavesdropping risk and could result in electromagnetic compatibility (EMC) and electromagnetic interference (EMI) problems. This specific threat is referred in literature as TEMPEST or EMSEC (emission security) attacks which are a subset of side-channel attacks [4]–[6]. This threat has been investigated and examined in the last 70 years mostly by defence organizations. It is not until the 1980s, when researchers such as W. Van Eck revealed this eavesdropping risk to the scientific community. W. Van Eck demonstrated the possibility of eavesdropping cathode ray tubes (CRT) using a standard TV broadcast antenna, an AM (amplitude modulation) receiver and a signal generator [1]. Others researchers picked up the threat in the 1990s and 2000s of which the most notable work comes from M.G. Kuhn [2], [7]. Kuhn showed that flat-panel displays also suffer from the same eavesdropping risk. Furthermore, Kuhn revealed that not only analog-based systems are affected but also digital-based systems. Not much later, others confirmed Kuhn's findings and addressed and further investigated the video leakage phenomena. [8]–[13]. It is generally accepted that the video eavesdropping risk is mainly limited to the range on which it can operate. The effective eavesdropping distance observed in previous mentioned research works is around 10 meters. With the exception of the research work [14] in which a distance of 46 meters is confirmed. However, the resolution of the paper's reconstructed video images is not high, only fonts of 36 points or higher are readable. Also, the tested VDUs are relatively outdated. Nonetheless, an eavesdropping range of 10 meter does pose a considerable threat for information security however it implies that the eavesdropping system needs to be in the same building or in the relative near-vicinity of the target VDU. This certainly puts some constraints on the effectiveness of this type of side-channel attack.

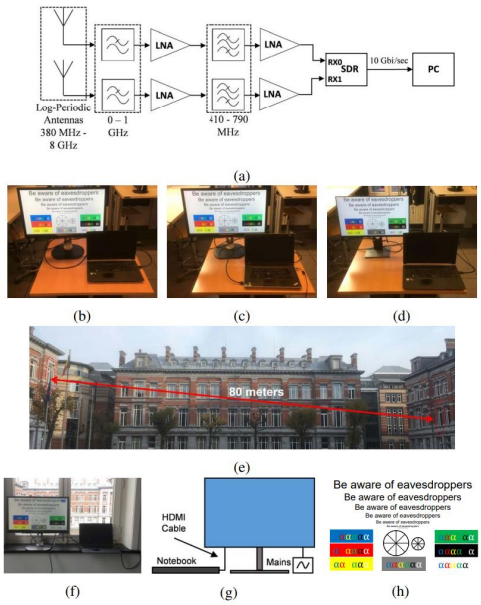
This paper possesses the effective eavesdropping range by deploying a new designed signal-acquisition chain and applying improved leakage detection and image reconstruction methods compared to our previous works [10], [13]. Furthermore, it specifically investigates the eavesdropping risk at a distance of 80 meters of an UHD and a full HD resolution video display which employs an HDMI cable linked to a notebook for video data transmission.

II. Methods & Tested Video Setups

A. Background of Video Leakage Phenomena

The signaling of video data inside VDUs is generally digital-based with the exception of VGA (video gate array) cables which employ analog signaling. Digital signals employ square waves which contain many high frequencies. These high frequencies can leak as radio waves in the very high

978-1-7281-7430-3/20/$31.00 ©2020 IEEE



8

A Threat for Tablet PCs in Public Space: Remote Visualization of Screen Images Using EM Emanation

A Threat for Tablet PCs in Public Space: Remote Visualization of Screen Images Using EM Emanation

Yuichi Hayashi
Tohoku University
Aramaki aza Aoba 6-3-09,
Aoba-ku Sendai, Japan
+81-22-795-6094
yu-ichi@gcc.ne.jp

Naofumi Homma
Tohoku University
Aramaki aza Aoba 6-6-05,
Aoba-ku Sendai, Japan
+81-22-795-7169
homma@aoki.ecei.tohoku.ac.jp

Mamoru Miura
Tohoku University
Aramaki aza Aoba 6-6-05,
Aoba-ku Sendai, Japan
+81-22-795-7169
miura@aoki.ecei.tohoku.ac.jp

Takafumi Aoki
Tohoku University
Aramaki aza Aoba 6-6-05,
Aoba-ku Sendai, Japan
+81-22-795-7169
aoki@ecei.tohoku.ac.jp

Hideaki Sone
Tohoku University
Aramaki aza Aoba 6-3,
Aoba-ku Sendai, Japan
+81-22-795-6091
sone@isc.tohoku.ac.jp

ABSTRACT

The use of tablet PCs is spreading rapidly, and accordingly users browsing and inputting personal information in public spaces can often be seen by third parties. Unlike conventional mobile phones and notebook PCs equipped with distinct input devices (e.g., keyboards), tablet PCs have touchscreen keyboards for data input. Such integration of display and input device increases the potential for harm when the display is captured by malicious attackers. This paper presents the description of reconstructing tablet PC displays via measurement of electromagnetic (EM) emanation. In conventional studies, such EM display capture has been achieved by using non-portable setups. Those studies also assumed that a large amount of time was available in advance of capture to obtain the electrical parameters of the target display. In contrast, this paper demonstrates that such EM display capture is feasible in real time by a setup that fits in an attaché case. The screen image reconstruction is achieved by performing a prior course profiling and a complimental signal processing instead of the conventional fine parameter tuning. Such complemental processing can eliminate the differences of leakage parameters among individuals and therefore correct the distortions of images. The attack distance, 2 m, makes this method a practical threat to general tablet PCs in public places. This paper discusses possible attack scenarios based on the setup described above. In addition, we describe a mechanism of EM emanation from tablet PCs and a countermeasure against such EM display capture.

Categories and Subject Descriptors

K.6.5 [Management of Computing and Information Systems]: Security and Protection –Physical security

General Terms

Security

CCS'14, November 3–7, 2014, Scottsdale, Arizona, USA.

http://dx.doi.org/10.1145/2660267.2660292.

Keywords

Touch-screen devices; Tablet PCs; Remote screen-image visualization; EM information leakage

1. INTRODUCTION

The number of touchscreen devices such as tablet PCs has rapidly increased in recent years. Accordingly, many users of such devices enjoy browsing and inputting personal information in public spaces, where third parties are present, in addition to doing so in private spaces. Unlike conventional PCs, the users of tablet PCs usually input data with keyboards displayed on the screen, using so-called software keyboards, as shown in Fig. 1.

Such integration of display with input device causes a serious risk of harm when the integrated display is captured by malicious attackers. Both the entered keys and their purpose (i.e., place on the screen), displayed on the same screen, can be stolen simultaneously by a single display capture. In particular, software key-boards often enhance the entered key by luminance changing or visually popping-up to support user confirmation, which makes it easier to steal key information. Even if an entered key is changed to an asterisk in the password section, as shown in Fig. 1, an attacker can obtain the key information from the enhancement effects. Such threats are potentially present in many applications that use login

Figure 1: Typical screen shot of tablet PC with software keyboard.

9

Transient IEMI Threats for Cryptographic Devices

Transient IEMI Threats for Cryptographic Devices

Yu-ichi Hayashi, *Member, IEEE*, Naofumi Homma, *Member, IEEE*, Takaaki Mizuki, *Member, IEEE*, Takafumi Aoki, *Member, IEEE*, and Hideaki Sone, *Member, IEEE*

***Abstract*—This paper presents a new type of intentional electromagnetic interference (IEMI) which causes information leakage in electric devices without disrupting their functions or damaging their components. Such IEMI could pose a severe threat to a large number of electric devices with cryptographic modules since it can be used for performing fault injection attacks, which in turn allows for obtaining faulty outputs (i.e., ciphertexts) from cryptographic modules and exploiting them to reveal information about secret keys. Such faulty outputs are usually generated by inducing faults into target modules through modification or invasion of the modules themselves. In contrast, IEMI-based fault injection can be performed on the target modules from a distance by using an off-the-shelf injection probe, without leaving any hard evidence of the attack. We demonstrate the impact of the aforementioned IEMI through experiments using the Advanced Encryption Standard, which is one of the ISO/IEC 18033 block ciphers, implemented as a module on a standard evaluation board. The experimental results indicate that generating exploitable faults is feasible and, therefore, such IEMI presents a tangible threat to various existing electric devices and systems that use cryptographic modules for secure communication and transactions.**

***Index Terms*—Cryptographic devices, electromagnetic (EM) information leakage, fault injection analysis, intentional electromagnetic interference (IEMI), transient faults.**

I. Introduction

THE problem of electromagnetic interference (EMI) is a major concern for researchers and designers of electric circuits. EMI is commonly recognized as a disturbance that interferes with an electric circuit as a consequence of either conducted or radiated emission from other devices. Such EMI has been studied as noise in the field of electromagnetic Compatibility (EMC), and many studies on noise suppression and reduction have been conducted in order to devise a way to protect electronic devices [1]. Some EMC-related committees, such as Federal Communications Commission and Comite International Special Des Perturbations Radioelectriques, have summarized the aforementioned knowledge and experience, and have standardized the acceptable values (i.e., guidelines) for EM radiation during device operation. Most current electronic devices are designed to satisfy these EMC standards, and devices conforming to the standards are expected to be immune against EMI.

EMI can also be used intentionally for malicious purposes, as in the case of radio jamming. However, the aforementioned standards cover mainly unintentional EMI rather than intentional EMI (IEMI), which is defined as "Intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems, thus disrupting, confusing, or damaging these systems for terrorist or criminal purposes" [2], [3]. IEMI is an overt threat which usually causes permanent damage when applied to electronic devices, and therefore requires stricter standards to be considered. In the context of the IEMI problem, a number of studies have been conducted on the following topics: classification of IEMIs; the ability to generate IEMI waveforms; the coupling process as applied to cables and systems; and the effects of IEMI on equipment, systems, communication, protection, measurements, and standards [3].

In this paper, we present a new type of IEMI that causes transient faults in electronic devices without damaging their operation and hardware. A preliminary, partial version of this paper was presented in [4]. The IEMI technique inverts one or several bytes in the intermediate result, which can be recovered after a reset or at the end of the operation. Here, the functionality of the module is expected to remain unchanged during such fault injection. This type of IEMI can pose a severe threat to various electric devices with cryptographic modules since transiently injected faults can be utilized for implementing an emerging type of attack known as "fault injection attack."

A fault injection attack is a physical attack against cryptographic hardware and embedded systems. In this type of attack, the attackers first inject transient faults into intermediate data of cryptographic operations and obtain a faulty ciphertext, after which they repeat the attack as necessary and derive the secret key from several faulty ciphertexts. Conventional fault injection techniques require direct physical access to the target cryptographic modules and/or modification of the modules themselves in order to inject transient faults. In contrast, fault injection based on IEMI can be performed on the target modules from a distance without leaving any hard evidence of the attack. IEMI-based fault injection attacks have the potential to become a new threat to a wide variety of cryptographic devices, such as security servers located in data centers, even if the devices implement conventional countermeasures against direct access and invasion.

This paper demonstrates an IEMI-based fault injection attack through experiments using the most popular block cipher, namely the Advanced Encryption Standard (AES) [5],

Manuscript received December 28, 2011; revised April 13, 2012; accepted May 29, 2012. Date of publication July 17, 2012; date of current version February 13, 2013.

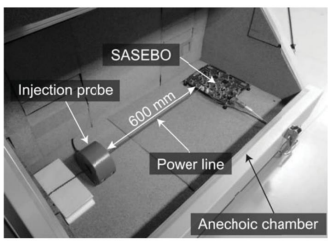
Y. Hayashi is with the Department of Electrical and Communication Engineering, Graduate School of Engineering, Tohoku University, Aramaki, Aoba-ku, Sendai 980-8579, Japan (e-mail: yu-ichi@mail.ieice.tohoku.ac.jp).

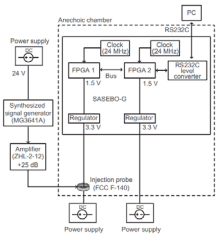
N. Homma and T. Aoki are with the Department of Computer and Mathematical Sciences, Graduate School of Information Sciences, Tohoku University, Aramaki, Aoba-ku, Sendai 980-8579, Japan (e-mail: homma@aoki.ecei.tohoku.ac.jp; aoki@ecei.tohoku.ac.jp).

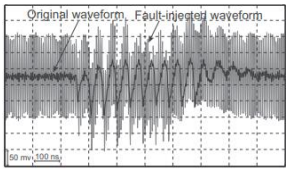
T. Mizuki and H. Sone are with Cybersicence Center, Tohoku University, Aramaki, Aoba-ku, Sendai 980-8579, Japan (e-mail: tm-paper+iemi2011@g-mail.tohoku-university.jp; sone@isc.tohoku.ac.jp).

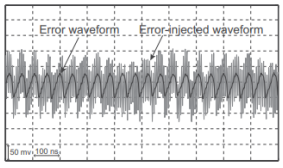
Digital Object Identifier 10.1109/TEMC.2012.2206393

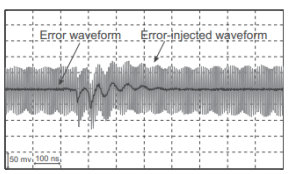
0018-9375/$31.00 © 2012 IEEE

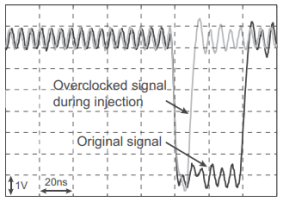












10

Inaudible Attack on Smart Speakers With Intentional Electromagnetic Interference

IEEE TRANSACTIONS ON
MICROWAVE THEORY AND TECHNIQUES

Inaudible Attack on Smart Speakers With Intentional Electromagnetic Interference

Zhifei Xu, *Member, IEEE*, Runbing Hua, Jack Juang, Shengxuan Xia, Jun Fan, *Fellow, IEEE*, and Chulsoon Hwang, *Senior Member, IEEE*

***Abstract*—This paper demonstrates an inaudible attack on smart speakers using electromagnetic interference (EMI). The EMI induces voltages on the order of a few millivolts on conductors, which are then converted to baseband signals by exploiting the inherent nonlinearity of microphones. The EMI signal is specially pre-processed to minimize the useless harmonics generation at the microphone output signals, which significantly improves the recognition rate as well as nullify the previous countermeasures based on the harmonics detection. The sensitive carrier frequency found by our proposed method can improve the attack distance as well. A measurement-based methodology is applied to locate the sensitive regions for noise coupling without knowing the layout of the printed circuit board (PCB), and the transfer function is also obtained to insure the main coupling location. Our experiments show that in open space, intentional EMI under 2.5 W can inject commands at distances up to 2.5 m on smart speakers.**

***Index Terms*—Hardware security, intentional electromagnetic interference (IEMI), inaudible attack, smart speaker.**

I. Introduction

A SMART speaker nowadays is not a just music player. With more and more devices connected, smart speakers such as Google Home and Amazon Echo can serve as a 'home assistant' that can provide control of common household tasks, such as environmental control (thermostat), lighting, door locks, security monitoring, and more.

The security of these smart speakers can have substantial effects, such as compromised home security and information leakage. Since smart speakers are having Wi-Fi or Bluetooth connections, various attacks can be performed through the apps and networks [1]-[3]. Researchers have implemented two application-level attacks, voice squatting and voice masquerading, which impersonate the smart speakers to steal and eavesdrop the conversations [4], [5]. A security researcher from MWR Info Security has demonstrated an attack on Amazon Echo speakers by placing the malware which enables the adversary to have access to control the smart speaker [6], [7]. However, these attacks cannot be executed remotely.

On the other hand, as the system trusts the microphone readings, a physical layer attack can readily bypass conventional security algorithm providing an unchecked entry point to the system. The application layer with software running on the smart speaker systems makes critical decisions of the input data acquired by the microphone circuit. Recently, several publications have demonstrated inaudible voice commands injection on the physical layer of the smart speakers by exploiting the nonlinearity of the microphone [8]-[17].

The dolphin attack or ultrasound attack [9]-[15] has demonstrated that a voice-enabled device can respond to inaudible ultrasound voice commands. More recently, laser pointers have been demonstrated as another tool for attacking microphone-based devices [8]. Some defense methods regarding the ultrasound attack have been investigated recently [9], [15] such as the voice signal processing method proposed in [15]. However, these attack types are limited by obstacles such as windows. The ultrasound is mechanical waves which need strong power to propagate through the window [27], the laser pointer attack requires the device insight because the microphone of the smart speaker needs to be pointed while attacking.

In contrast to other types of attacks such as ultrasound and light command, EMI based attack can penetrate windows with relatively low loss and does not need to have the target in sight. The high-power intentional EMI can stop electrical network such as electric cars, trains, transformers [20]-[27], and radio communicating devices such as cellphone, computer and other electronics will be impacted as well [20], [23], the required high-power can be deduced by [22] for a long-distance attack. The IEMI can also be applied to inject information into the analog devices which operate in the order of a few millivolts [16]-[19]. This attack with circuit easily affected is known as "back-door" interfering [17]. Since the acquisition process requires much lower energy, microphone circuit with cables or copper PCB interconnects is vulnerable to interference [21] and allows the information injection [17]. The intentional EMI has been employed to attack the headset cable of smartphones [16], the audio signal has been injected through the electromagnetic coupling on the cable of the headset because the cable can act as an antenna which can receive the electromagnetic interference. The intentional EMI has also been employed to attack the analog sensor of the microphone of cardiac electronic devices [17]. However, in their application, the attack setup needs to be placed very close to the cardia electronic device.

This paper is the first paper demonstrating the IEMI attack on the smart speakers and attempted to increase the IEMI attack distance for the smart speakers and cellphones. Different from previous cellphone attack work, we targeted at the microphones of the devices not the headset cable. The attack principles including the EM coupling and microphone nonlinearity are presented in Section II. Then the attack signal is optimized by exploring the nonlinearity performance of the

Manuscript received xxxxx. This work was supported by the National Science Foundation under Grant No. IIP-1916535.

Zhifei Xu, Runbing Hua, Jack Juang, Shengxuan Xia, Jun Fan and Chulsoon Hwang are with the Electromagnetic Compatibility Laboratory, Missouri University of Science and Technology, Rolla, MO 65401, USA (e-mail: zxfdc, rhm2, jjryb, sx7c3, jfan, hwangc@mst.edu).

Digital Object Identifier: 10.1109/TMTT.2021.3056565

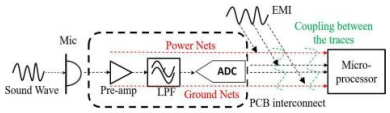


Fig. 1. Microphone circuit diagram and the anticipated coupling path

Fig. 2. Demodulation due to the inherent nonlinearity of microphones

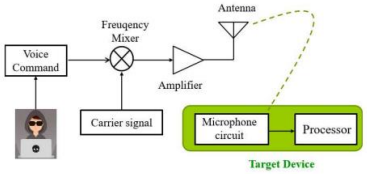


Fig. 3. Intentional EMI attack schematic

11

Echo TEMPEST: EM Information Leakage Induced by IEMI for Electronic Devices

IEEE TRANSACTIONS ON ELECTROMAGNETIC COMPATIBILITY, VOL. 65, NO. 3, JUNE 2023 655

Echo TEMPEST: EM Information Leakage Induced by IEMI for Electronic Devices

Shugo Kaji, *Student Member, IEEE*, Daisuke Fujimoto, *Senior Member, IEEE*, Masahiro Kinugawa, *Member, IEEE*, and Yuichi Hayashi, *Senior Member, IEEE*

***Abstract*—Electromagnetic (EM) information leakage encourages attacks, wherein the attackers passively capture and analyze EM waves that are unintentionally generated by devices. Generally, devices with weak EM emission intensities are not targeted. However, even these devices would be subject to attacks if it becomes possible to actively sense the electrical changes that occur within them when information is processed. This article demonstrates the feasibility of the information leakage threat induced by the active sensing of input impedance changes in the input/output (I/O) circuit of an integrated circuit (IC). Specifically, the changes in the input impedance when information was transmitted from the IC, were measured by irradiating the EM waves from outside the target device. This article labels the threat as Echo TEMPEST. The experiment validated Echo TEMPEST with an evaluation board that simulated the I/O circuit of the IC, UART modules, and USB keyboards. It was also demonstrated that attackers could control the distance (obtained information from the target device), depending on the intensity of the irradiated EM waves. Furthermore, we discussed countermeasure methods focusing on the conditions for executing Echo TEMPEST.**

***Index Terms*—Eavesdrop, electromagnetic emanations, electromagnetic information leakage, hardware security, information security, intentional electromagnetic interference, TEMPEST.**

I. Introduction

PREVIOUSLY, measures for ensuring the security of devices with access to confidential information had isolated them from the Internet and other public networks, thereby eliminating the path for executing attacks [1].

However, when information is processed inside an electronic device, it generates electrical signals, such as current and voltage, which vary with time. These time-varying signals unintentionally generate electromagnetic (EM) waves that radiate from the device. If an attacker captures such radiated EM waves, the device's confidential information is leaked [2], [3]. In particular, input/output (I/O) information of human-oriented devices (e.g., displays, keyboards, printers, and audio) is not encrypted, and an attacker can obtain it by capturing and analyzing the radiated EM waves.

Until now, attacks, known under the code name TEMPEST [4], against information devices by capturing the radiated EM waves have been discussed only in the fields of military and diplomacy. Discussions related to commercial products [5], [6], [7], [8], [9], [10], [11], [12], [13] began after the possibility of such an attack was demonstrated by the Dutch researcher Wim van Eck in the early 1980s [14].

Fig. 1 illustrates the information processing and electrical signal propagation of I/O devices. Electrical signals are the main target of information leakage caused by the capture of radiated EM waves (EM information leakage). Radiated EM waves are generated in the process indicated in Fig. 1(a)–(d) or their mixed signals based on the mechanism shown in Fig. 2 [15], [16].

The above-cited threat of EM information leakage is a passive attack in which the attacker captures EM waves radiated from the device against the designer's intention. It is difficult for

Manuscript received 3 November 2022; accepted 12 February 2023. Date of publication 3 April 2023; date of current version 13 June 2023. This work was supported by the JSPS KAKENHI under Grant JP19H01104, Grant JP21K19772, Grant JP22K12031, and Grant JP22H04999. (*Corresponding author: Shugo Kaji.*)

Shugo Kaji, Daisuke Fujimoto, and Yuichi Hayashi are with the Nara Institute of Science and Technology, Ikoma 630-0192, Japan (e-mail: kaji.shugo.kp0@is.naist.jp; fujimoto@is.naist.jp; yu-ichi@is.naist.jp).

Masahiro Kinugawa is with the University of Fukuchiyama, Fukuchiyama 620-0886, Japan (e-mail: kinugawa@fukuchiyama.ac.jp).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TEMC.2023.3252636.

Digital Object Identifier 10.1109/TEMC.2023.3252636

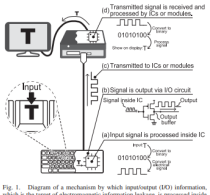
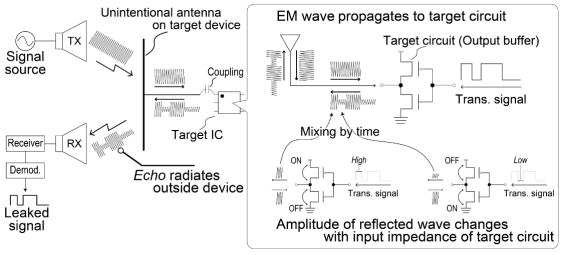
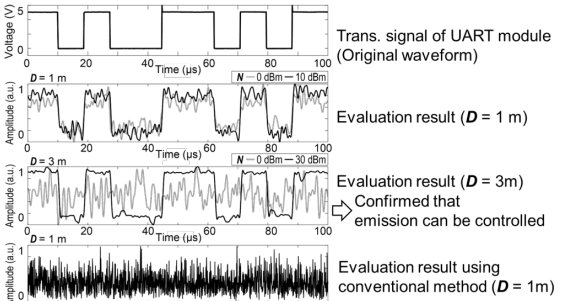


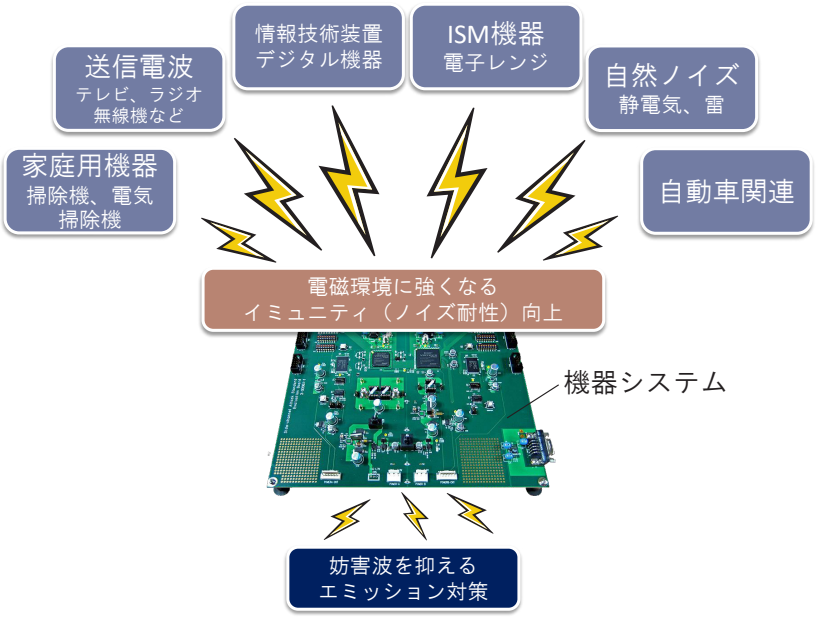
Fig. 1. Diagram of a mechanism by which input/output (I/O) information, which is the target of electromagnetic information leakage, is processed inside the device and propagated as an electrical signal. (a) User's input signals or signals inside the device are processed inside the integrated circuit (IC). (b) Signal is output to the transmission line as an electrical signal through the IC's I/O circuit. (c) Signals output from the I/O circuit are transmitted to the ICs or modules for the next processing. (d) Transmitted electrical signals are received and processed by the ICs or modules.





12

電子機器における電磁放射と電磁妨害



13

電子機器に求められる電磁両立性

電磁両立性
EMC
(Electromagnetic Compatibility)

両立する

EMI
(Electromagnetic Interference)
自他のシステムに
電磁的障害を与えない

EMS
(Electromagnetic Susceptibility)
自他のシステムから
電磁的影響を受けない

14

電子機器に求められるノイズ規制

IEC（国際電気標準会議）ITU（国際電気通信連合）
ISO（国際標準化機構）CISPR（国際無線障害特別委員会）
CCIR（国際無線通信諮問委員会）CCITT（国際電信電話諮問会議）

各国代表の審議に基づく勧告を受けて、
各国が国内法を整備したり自主規制を行う

勧告

欧州
EN（欧州規格）

EUの統一規格
EMC指令などをクリアした製品にCEマーク（安全マーク）の添付が許される

日本
VCCI（情報処理装置等電波障害自主規制協議会）

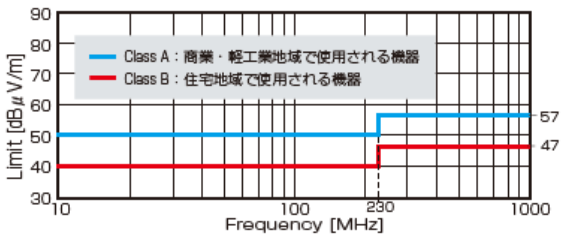
CISPR勧告に沿って1985年策定された業界の自主規制

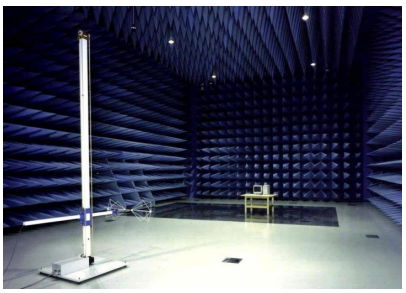
米国
FCC（連邦通信委員会）
ANSI（米国規格協会）
MIL（米軍仕様書）

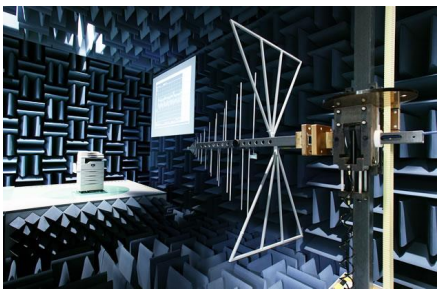
米軍の規格。世界的に規格が決まっていない分野で参考にされる

15

製品出荷のためのEMC試験

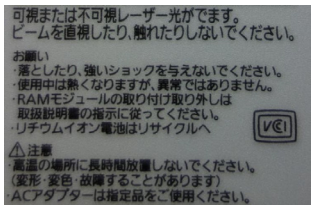






16

規格を満たした電子機器



17

電磁放射を発生させる３要因モデル

EMI ＝ Source × Path × Antenna

Source

- 情報システムを動作させるために必要な所望の信号
  - 情報システム内部の保護すべき電気信号
  - 情報システムが通信に用いる伝送信号

Path

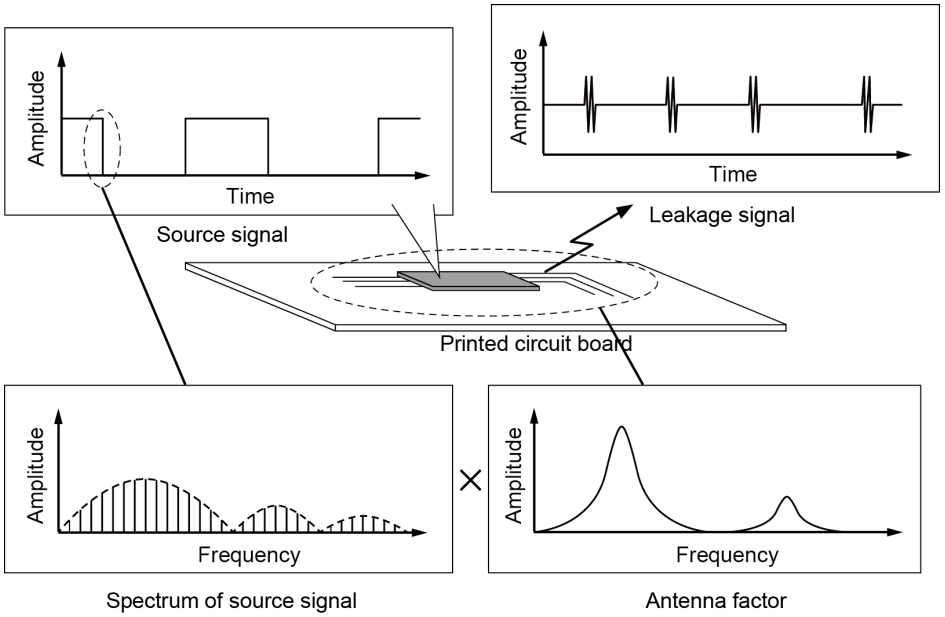
- ディファレンシャルモードからコモンモードへの変換
  - 情報システム内部の電気信号を漏洩成分に変換

Antenna

- 情報システムの物理構造により構成されるアンテナ

18

電子機器から電磁放射メカニズム

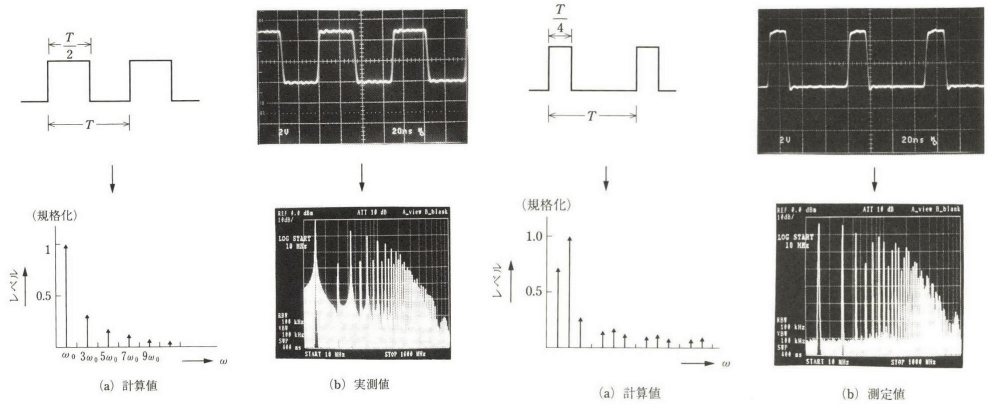


19

Source

20

信号源のスペクトル



周期や信号の立ち上がりによって放射されるスペクトルが異なる

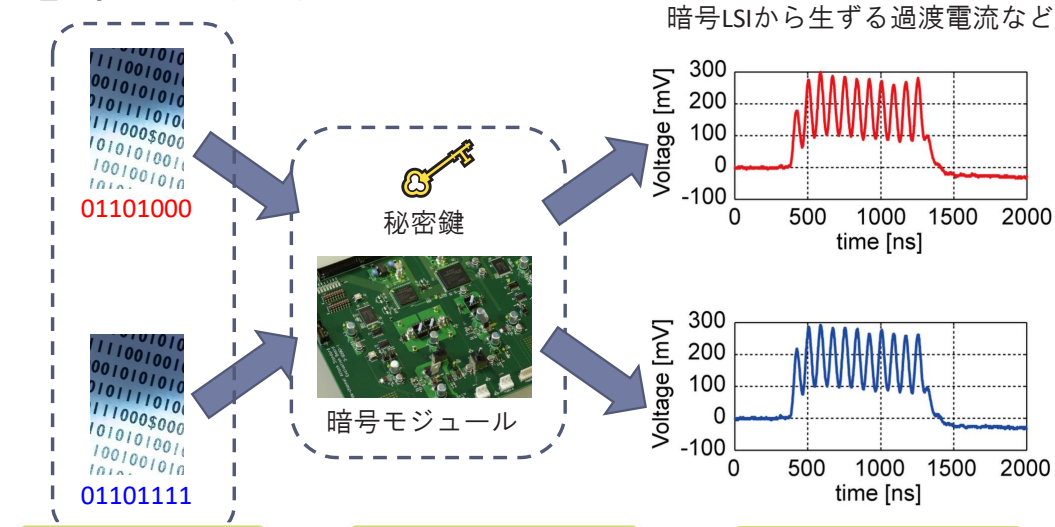
EMCと基礎技術,工学図書

21

暗号回路の動作に伴い発生する信号

処理対象となるビット列

暗号LSIから生ずる過渡電流など

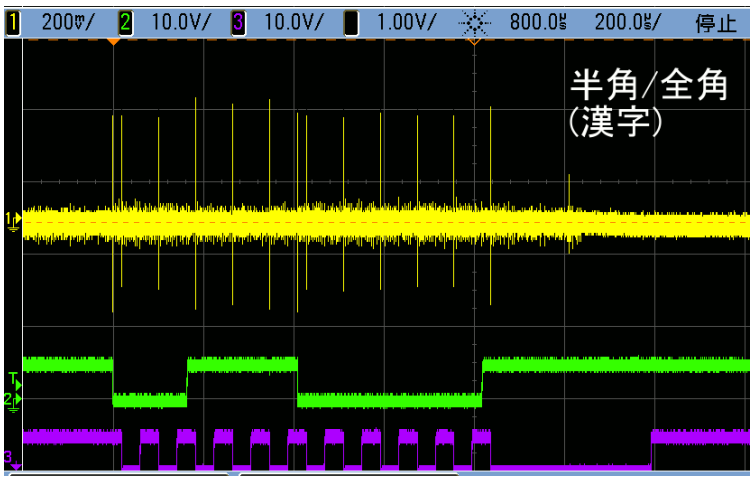


データ毎に変化　データによらず不変　データ毎に変化

22

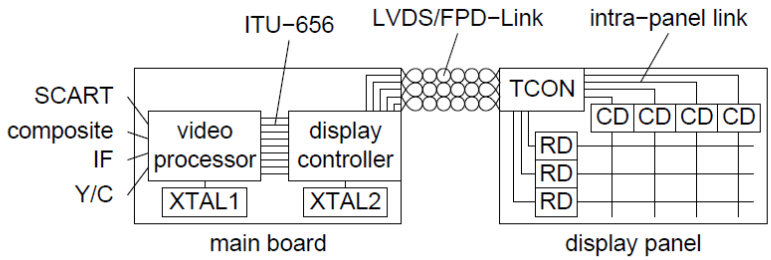
PCとキーボード間で伝送される信号

入力キーによって信号パターンが変化するため、打鍵情報の特定が可能

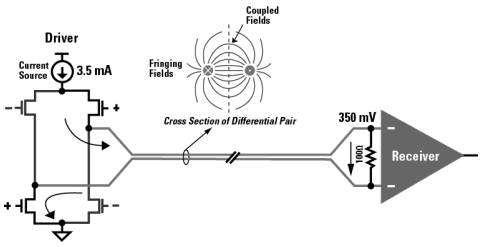


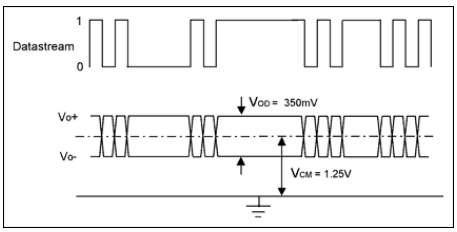
23

PCとディスプレイ間で伝送される信号



Modern LCD TV = two chips on main board



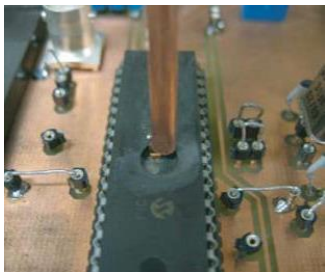


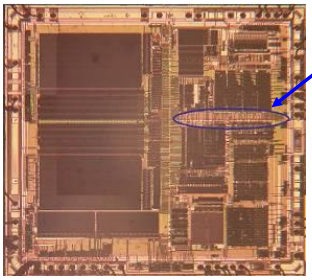
www.maximintegrated.com

24

マイクロプロービングによる局所電磁波攻撃

- 暗号モジュールの表面に磁界プローブを接近させることにより，特定の箇所からの漏洩情報を正確に観測
  - 従来対策の想定（攻撃者が観測する電磁波のモデル）を越えた攻撃が可能





近年，局所的な漏洩電磁波を用いた高度な攻撃（局所電磁波攻撃）の報告が多くなされている

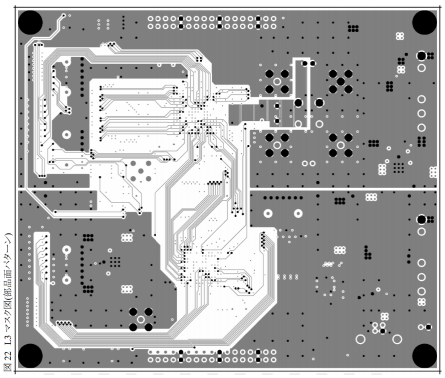
25

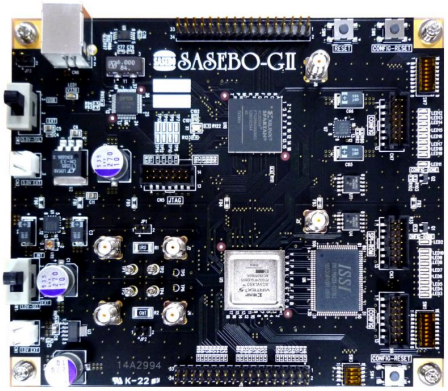
E. Peeters, VLSI J 2007

Coupling path

26

電子機器の設計



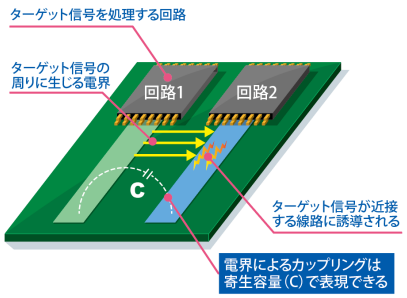


「電流は配線に沿って流れる」と考えて機器を設計

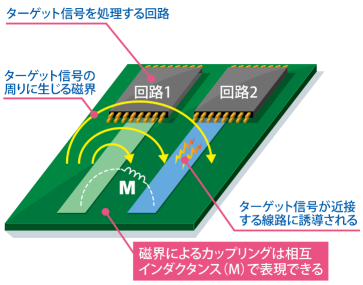
でも実際は・・・・

27

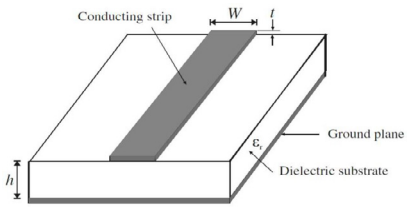
容量・誘導結合

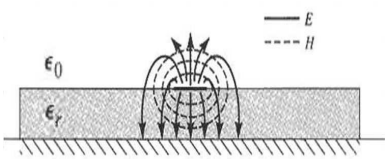


（a）電界を通じたターゲット信号の漏えい



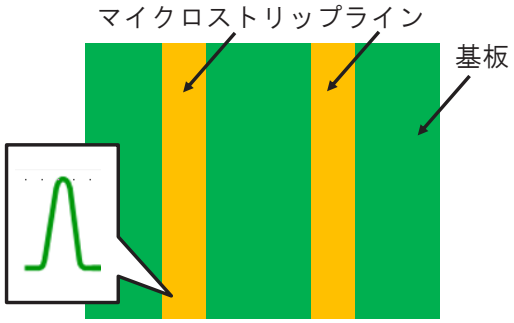
（b）磁界を通じたターゲット信号の漏えい

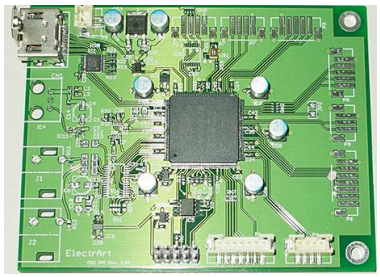




28

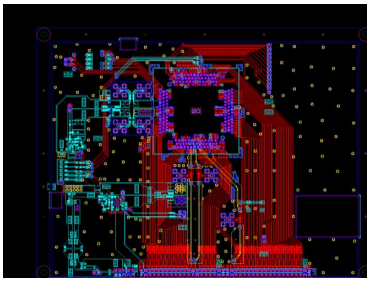
線路間カップリングの様子





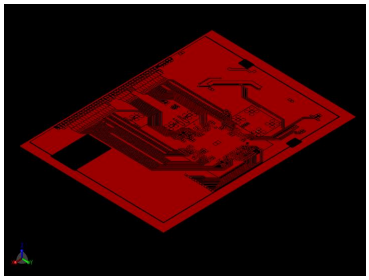
29

複雑な基板からの電磁放射



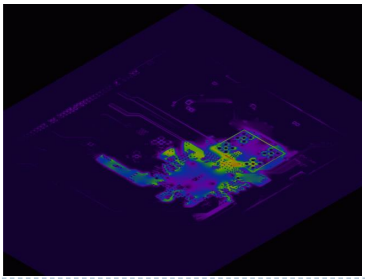
Design pattern

Design patternに基づきシミュレーションモデルを作成



Simulation model for electrical device

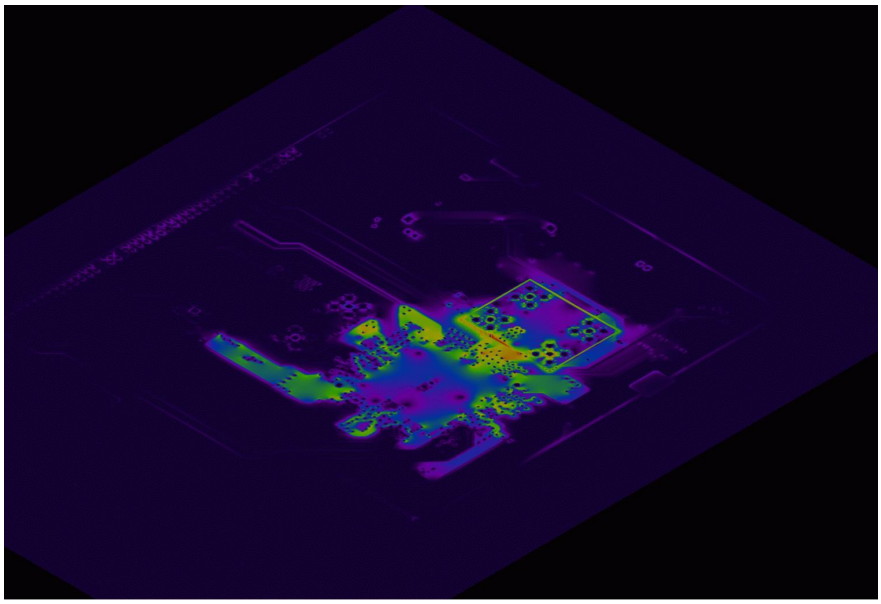
実機からの電磁放射をシミュレーション



EM emission map using simulation

30

複雑な基板におけるカップリングの様子

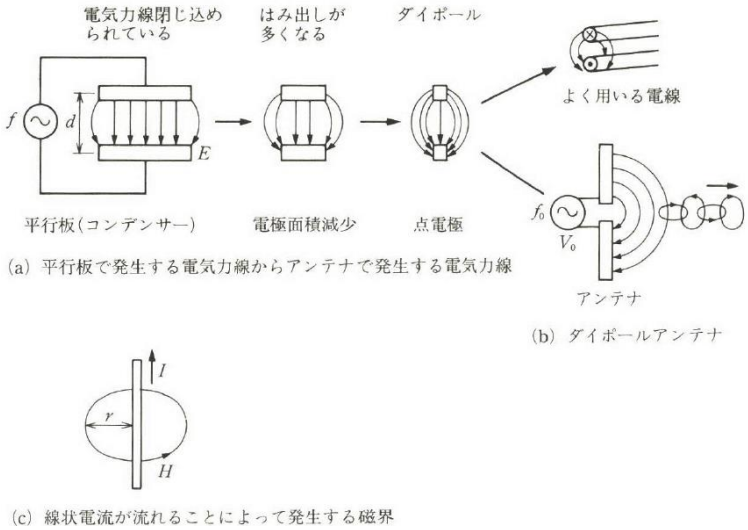


31

Antenna

32

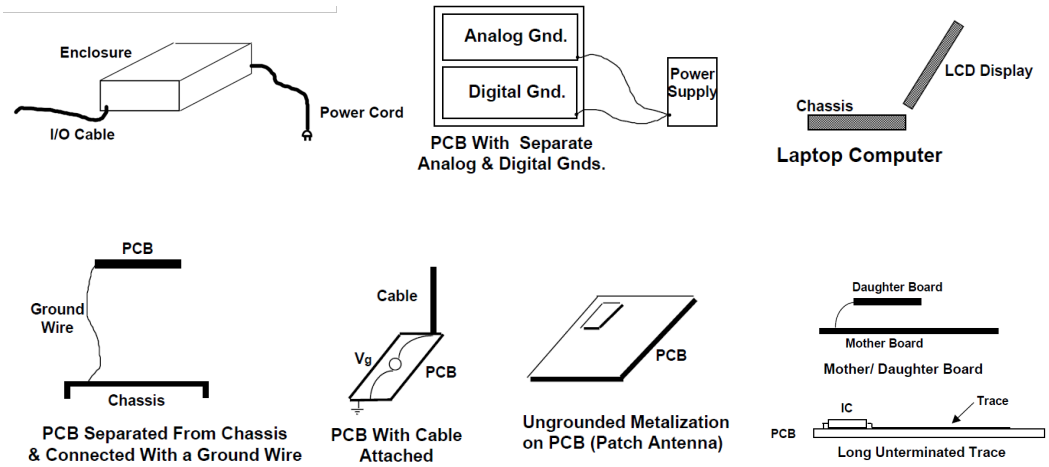
電界と磁界の発生



EMCと基礎技術,工学図書

33

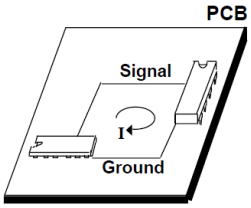
モノポール・ダイポールアンテナ



UNDERSTANDING AND FINDING THE INVISIBLE ANTENNAS IN YOUR DESIGN, Henry W. Ott, 1998

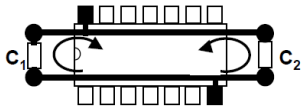
34

ループアンテナ



Clocks on PCBs

Large ICs (≥ 1")

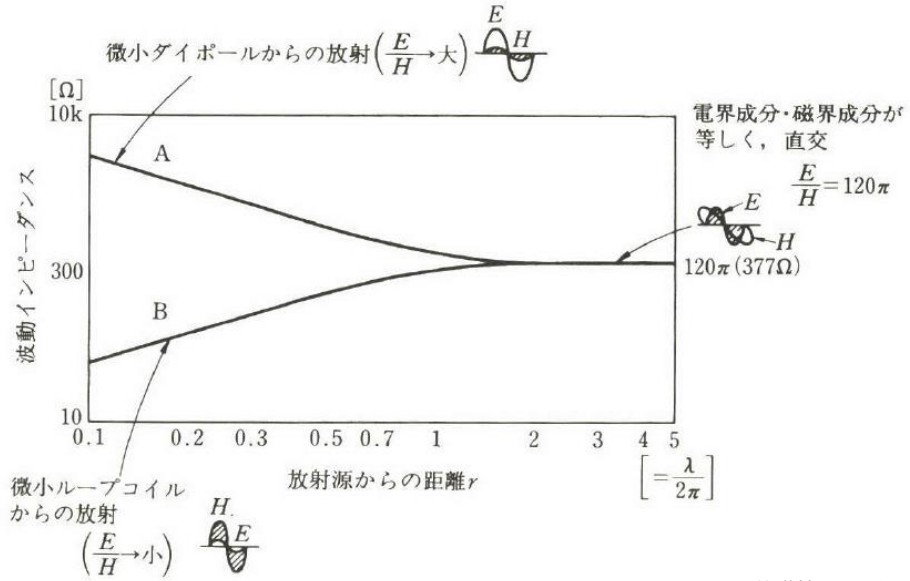


Decoupling Capacitors

UNDERSTANDING AND FINDING THE INVISIBLE
ANTENNAS IN YOUR DESIGN, Henry W. Ott, 1998

35

波動インピーダンス特性



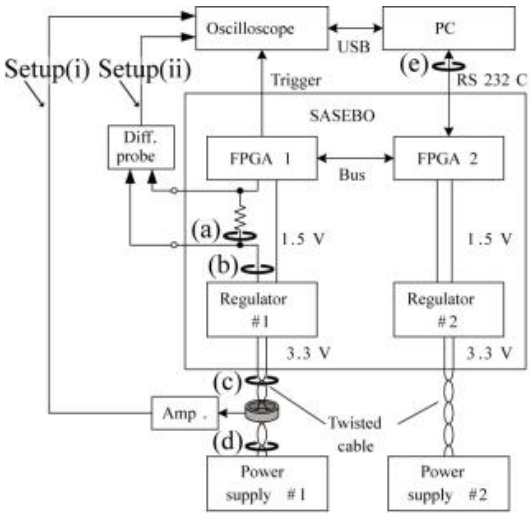
EMCと基礎技術,工学図書

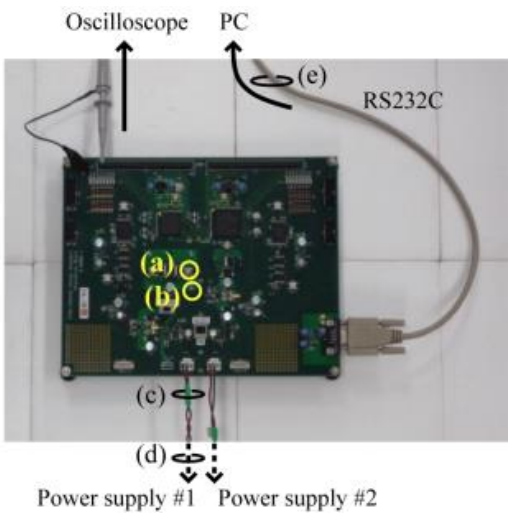
36

（例）暗号モジュールからの漏えい

37

暗号モジュールからの漏えい電磁波評価系

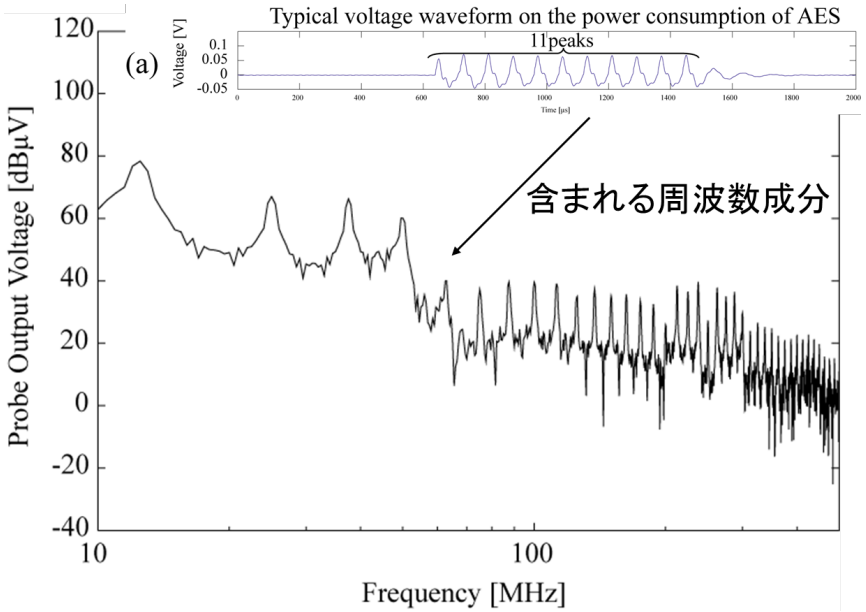




38

Source

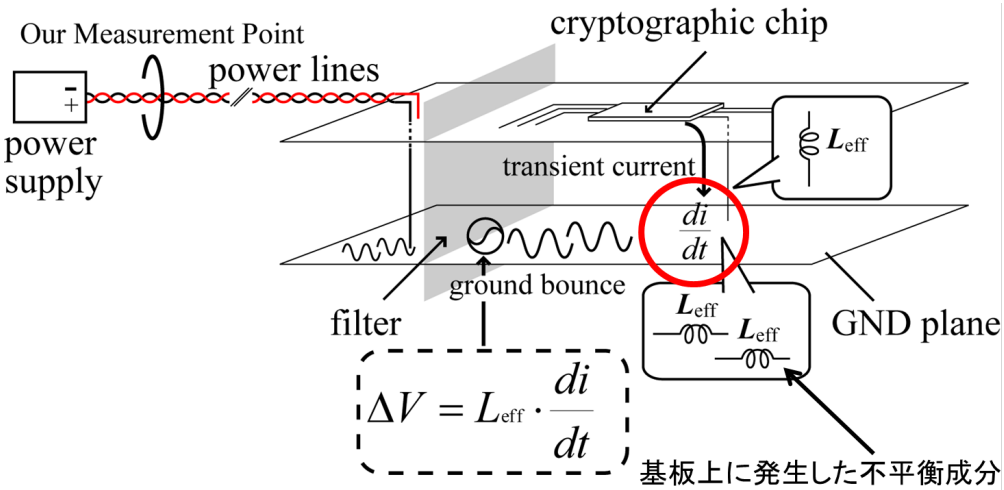
暗号モジュールから発生する過渡電流の周波数特性



40

Coupling path

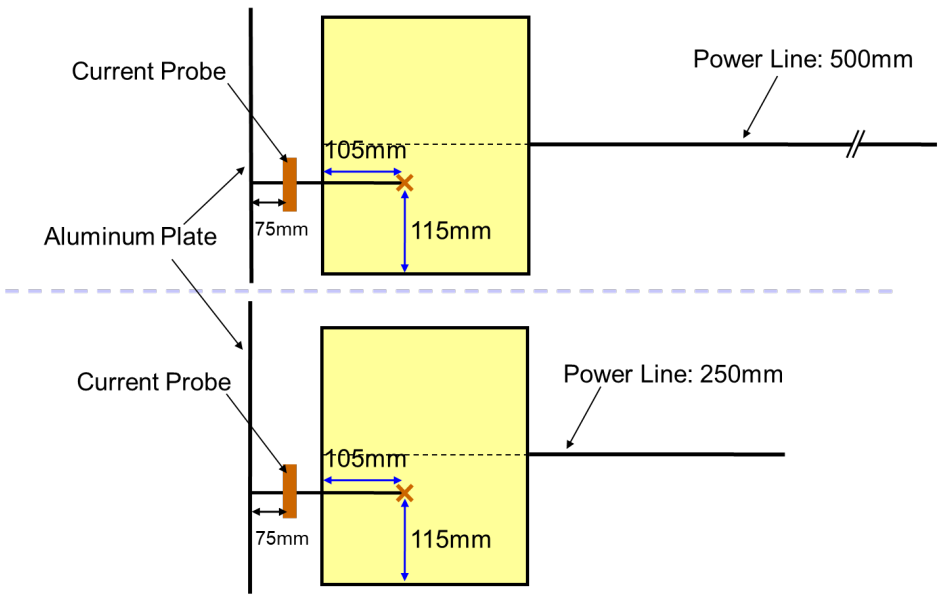
寄生インダクタンスによる不平衡成分の発生



42

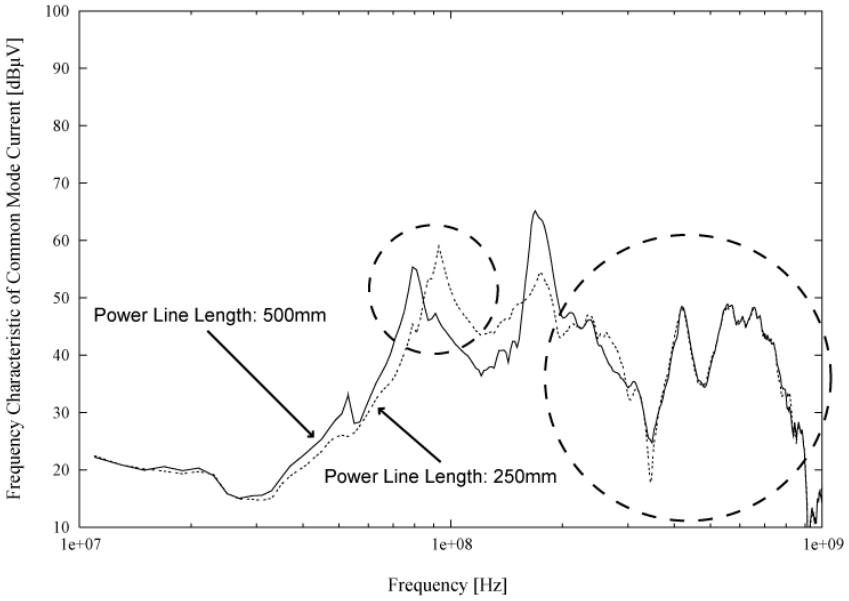
Antenna

接続線路により構成されるアンテナ生



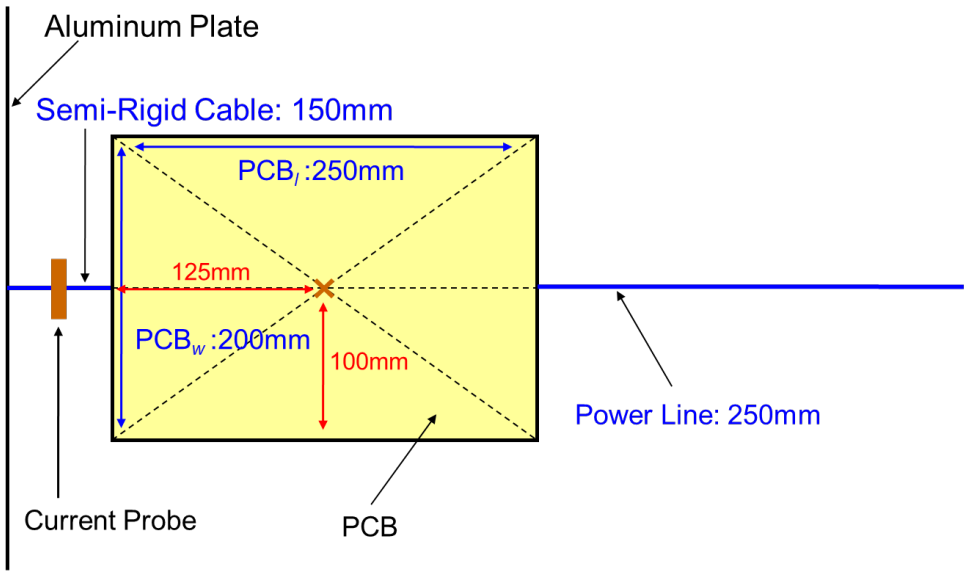
44

接続する線路によって異なるアンテナ特性



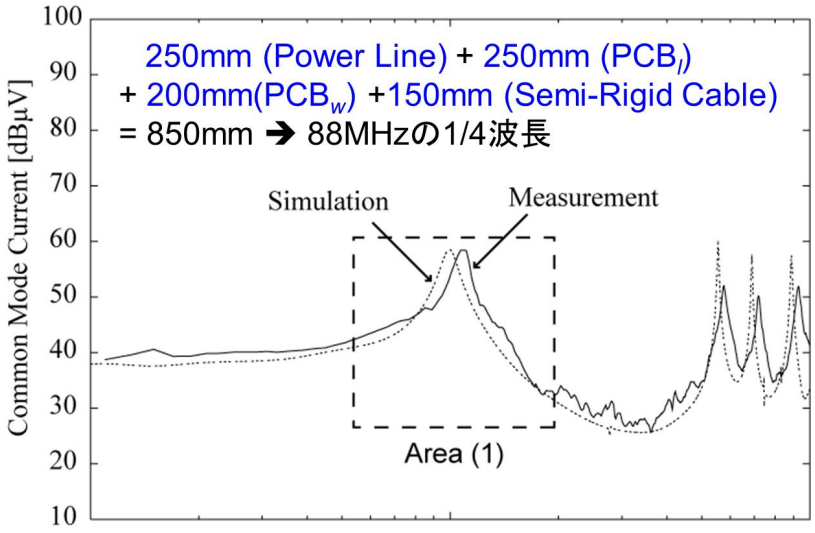
45

アンテナ特性を決定する要因



46

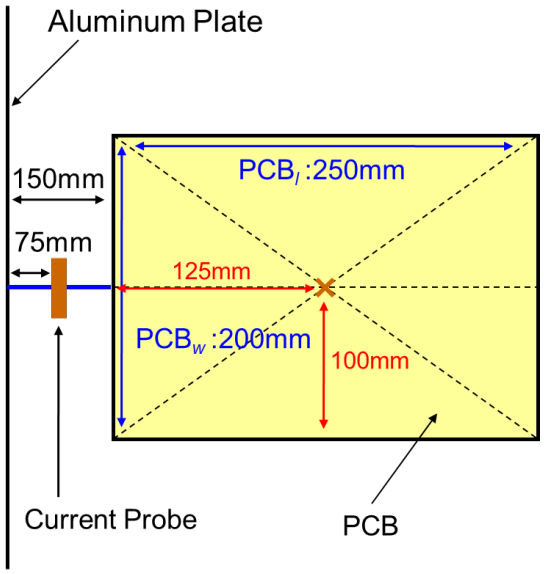
EMI放射モデルを用いた情報漏洩のメカニズム：接続されたケーブルと基板サイズに応じた共振



銅線(250mm) を接続し，給電部（セミリジット）75mmの位置でCM電流を測定

47

基板サイズによって変化するアンテナ特性



48

EMI放射モデルを用いた情報漏洩のメカニズム：基板により発生する平行平板共振

平行平板共振周波数の理論値 (*m*, *n*の次数は3まで)

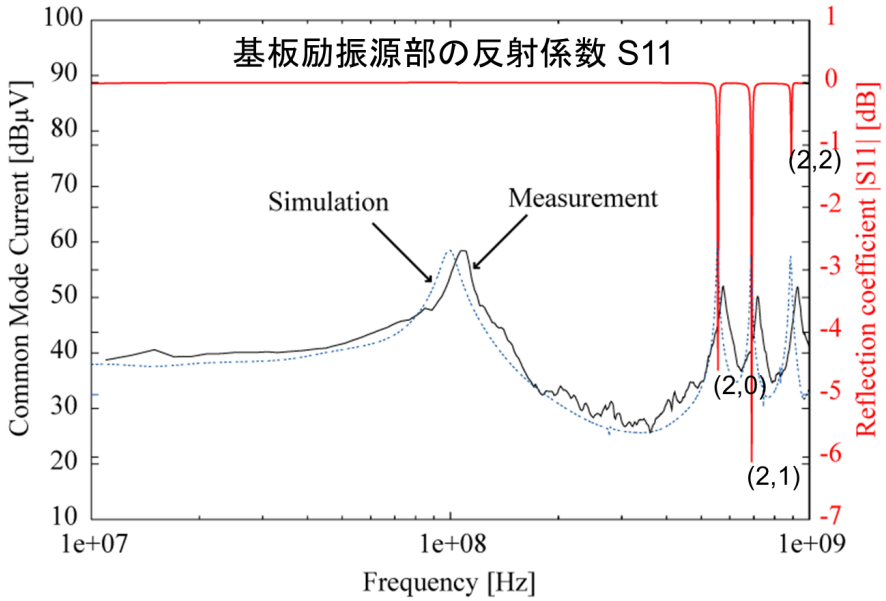
Cavity Resonances (The Poles of Equation)

$$f_r = \frac{150}{\sqrt{\varepsilon_r}}\sqrt{\left(\frac{m}{PCB_w}\right)^2 + \left(\frac{n}{PCB_l}\right)^2} \quad [\mathrm{MHz}]$$

		m			
		0	1	2	3
n	0		283	566	849
	1	353	452	667	919
	2	707	761	905	1104
	3	1061	1098	1202	1358

49

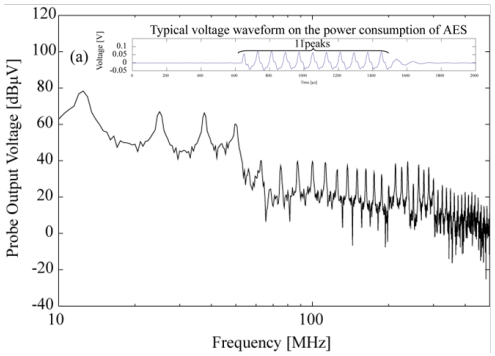
基板における平行平板共振の周波数特性

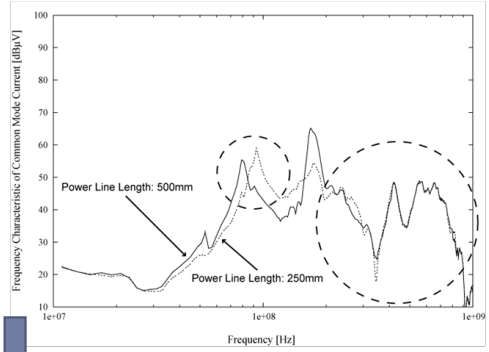


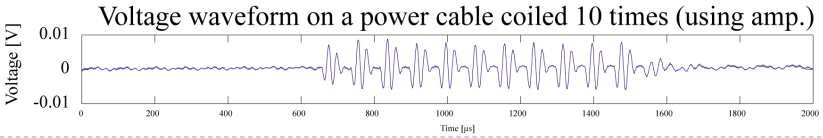
50

機器外部に発生する漏えい電磁波

Source × **Path, Antenna**

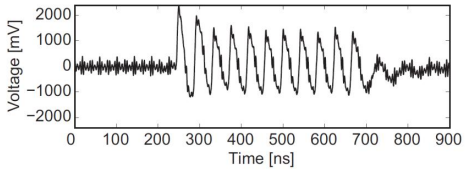




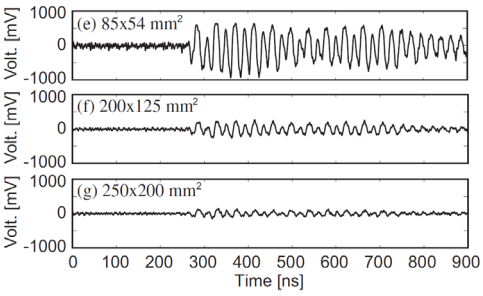


51

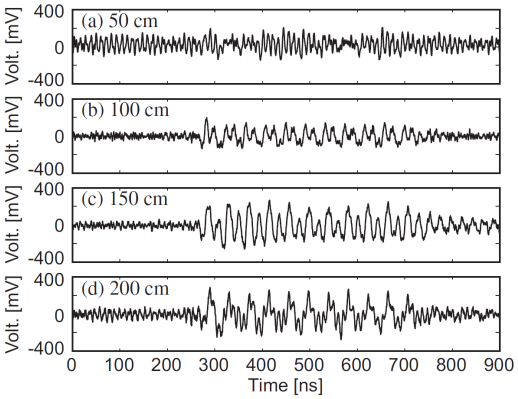
機器の物理構造の違いが生む漏えい波形の変化



機器を構成する基板や接続線路の長さが変化すると漏えい信号のスペクトルに変化が生ずる



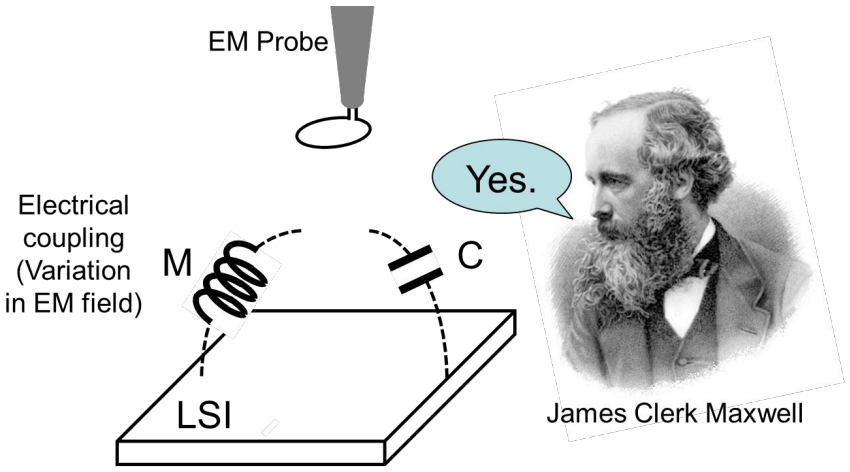
基板のサイズが変化した場合



接続線路の長さが変化した場合

52

物理法則上回避不可能な攻撃検知



Physical law unavoidable in EM measurement

Sense EM attacks by observing EM field variation

53

まとめ

- 暗号モジュールを含む電子デバイスから電磁波を通じた情報漏えいに着目
- 電磁波の漏えい過程を「ソース」「パス」「アンテナ」の3要素に分解し、それらの組み合わせで電磁波による情報の漏えいが生じることを説明した
- 電磁波の計測時にはかならず「侵襲」が発生するので、計測の気配（寄生結合）をセンシングすることにより、物理法則上回避不可能な対策手法を構築できる可能性を示した

54

メモリ暗号化のための暗号技術とハードウェアアーキテクチャ

上野 嶺
東北大学
rei.ueno.a8@tohoku.ac.jp

Memory encryption is essential to realize the privacy and trust of date stored in main memory, which is placed outside the CPU. Especially in recent years, with the advanced performance and greater capacity of Non-Volatile Memory (NVM), adoption of NVM has grown in data centers, IoT devices, and modern CPUs for power efficiency and performance improvement. However, NVM poses a higher risk of eavesdropping and tampering/data manipulation due to its data non-volatility, than DRAM. Therefore, a memory encryption mechanism, which is capable of encryption and authentication for large-capacity NVM with real-time processing, is strongly demanded. In this presentation, we will provide an overview of cryptographic primitives for secure NVM, incorporating the latest findings from the presenters.

References

[1] Institute of Mathematics for Industry, Kyushu University Web Page: `http://www.imi.kyushu-u.ac.jp/`
[2] Dimetre Triadis, Philip Broadbridge, Kenji Kajiwara and Ken-ichi Maruno, Integrable Discrete Model for One-dimensional Soil Water Infiltration, Stud. Appl. Math. 140(4)(2018) 483–507. doi:10.1111/sapm.12208

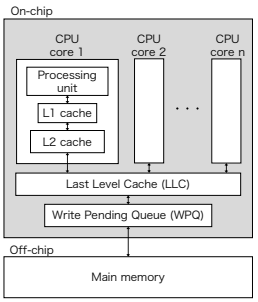
メモリ暗号化のための暗号技術とハードウェアアーキテクチャ

上野嶺

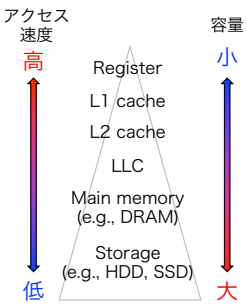
東北大学　電気通信研究所

現代コンピュータとメモリ

- 現代のコンピュータは高速な動作が可能だがメインメモリへのアクセスが相対的に遅く処理速度低下の原因になる
- メインメモリへのアクセス回数を減らすためにキャッシュをCPUコアの近くに配置
  - 一度使用したデータはキャッシュに保管し以降はキャッシュからロード
  - 記憶素子のアクセス速度と容量はトレードオフの関係にある
- メインメモリはCPU外部に配置されるためCPU上のデータよりも容易に盗聴・改ざんが可能
  - メモリ暗号化の主な動機



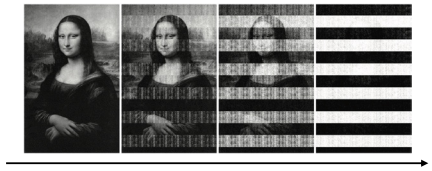
現代コンピュータの典型的なシステムモデル



メモリの階層構造

Cold boot attack [HSH+09]

- メインメモリ (DRAM) はコンデンサに蓄えた電荷で情報を記憶する
  - 電源を切っても情報はすぐに消失せず残留する
  - 冷却することで残留時間が伸びる
- DRAMを（冷却して）取り外してダンプすることでデータを盗聴可能
  - ストレージ暗号化をバイパス可能
  - AESやRSA，格子暗号などの秘密鍵回復の成功例も報告



時間

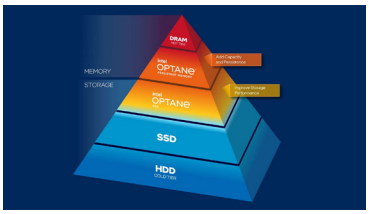
電源遮断後のDRAMデータの変化

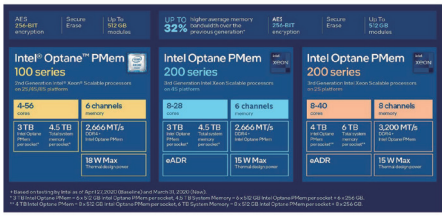
実際にDRAMを冷却して取り外す様子

[HSH+09] J. A. Halderman et al., “Lest we remember: cold-boot attacks on encryption keys,” *Communication of the ACM*, vol. 52, pp. 91–98, 2009. （図は同文献より引用）

不揮発メモリ・永続メモリの台頭

- 不揮発メモリ (NVM) の高性能化・大容量化に伴い活用例が増加
  - データの保持に電力が不要なので省エネルギー化に大きく貢献
- メインメモリ，あるいはメインメモリとストレージの中間層として活用した高性能CPUも開発された (NVDIMMやIntel Optane PMなど)





Intel Optane Persistent Memory の概要

- ただしDRAMよりも盗聴や改ざんが遥かに容易に
  - Intel Optane Persistent Memory は AES–XTS による暗号化をサポート

図の引用：https://www.intel.co.jp/content/www/jp/ja/products/docs/memory-storage/optane-persistent-memory/optane-persistent-memory-200-series-brief.html

5

本講演の内容

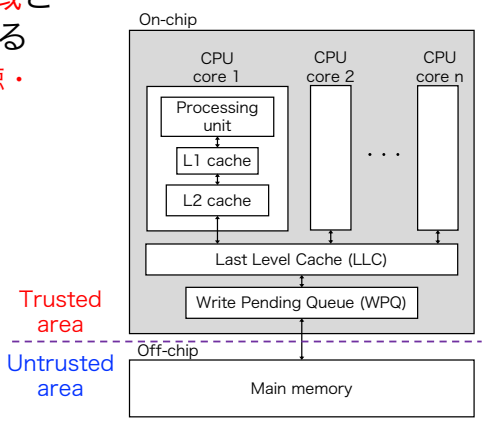
- （不揮発）メモリ暗号化のための脅威・安全性モデルとメモリ暗号化のための主要暗号プリミティブを紹介
  - 講演者らのグループが開発したメモリ暗号化スキームELMを解説 [1]
  - ELMを実際のCPUで安全かつ実用的に運用するためのハードウェアアーキテクチャを解説 [2, 3] (本公開版では割愛)
- Disclaimer: TEEメモリ暗号化とは（関連はあるが）異なるトピック
  - TEEでは仮想攻撃者は悪意ある特権ユーザやOS（CPU内部の存在）などだが, 本講演では外部からメモリデータの盗聴・改ざんを試みる攻撃者を仮定
  - Remote attestationやEnclaveなどは今回は扱わない
- NECセキュアプラットフォーム研究所との共同研究成果を含みます

[1] Akiko Inoue, Kazuhiko Minematsu, Maya Oda, Rei Ueno, and Naofumi Homma, “ELM: A Low-Latency and Scalable Memory Encryption Scheme,” IEEE Transactions on Information Forensics and Security, Vol. 17, pp. 2628–2643, 2022.
[2] 羽田大倫, 上野嶺, 本間尚文, 井上明子, 峯松一彦, “分離カウンタを用いたセキュアNVMの効率的な復旧保証,” 情報処理学会研究報告, Vol. 2022-ARC-250, No. 15, pp. 1–9, 2023.
[3] 羽田大倫, 上野嶺, 本間尚文, 井上明子, 峯松一彦, “更新並列化可能認証木に基づく高速なセキュア不揮発性メモリの実現,” 情報処理学会研究報告, Vol. 2022-ARC-250, No. 15, pp. 1–9, 2022.

6

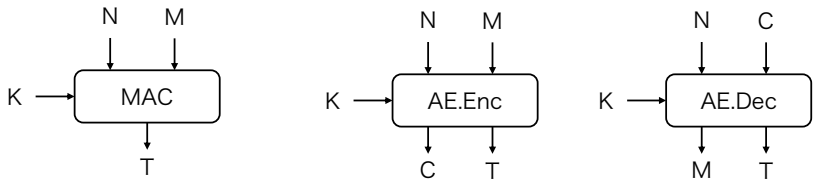
メモリ暗号化のシステムモデル

- コンピュータは信頼できるOn-chip領域と信頼できないOff-chip領域に分割される
  - 攻撃者はOn-chip領域のデータは全く盗聴・改ざんできない
  - 攻撃者はOff-chip領域のデータを任意に盗聴・改ざんできる
- メモリ暗号化の目的はOff-chipに格納されるデータの機密性と完全性の保証
  - On-chipデータは全面的に信頼する
    - メモリ暗号化も安全に行われる
  - On-chip領域は安全な計算環境と数千ビットのレジスタを提供する
    - このレジスタに秘密鍵やナンスを格納



メモリ暗号化のための暗号技術

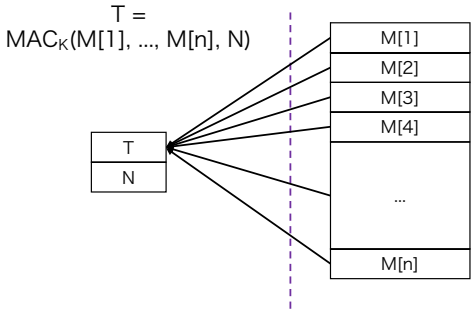
- メモリ暗号化では通常，共通鍵暗号を使用
  - メモリデータはCPU上に読み込まれるときに復号・検証して，メモリに書き込むときに暗号化すればよい（On-chipの秘密鍵のみで処理が完結する）
- メモリデータの秘匿性と完全性を実現する主要暗号技術
  - ナンスベースメッセージ認証符号 (MAC) および認証暗号 (AE)



K: 秘密鍵，N: ナンス，M: メッセージ/平文，C: 暗号文，T: タグ
（本講演ではAEのAssociated Dataは考慮しない）

共通鍵暗号の利用の検討1

- メモリ全域に対してMACを一回計算
  - メモリアクセスの度にメモリ全域へのフルアクセスが必要
    - リアルタイム処理が不可能

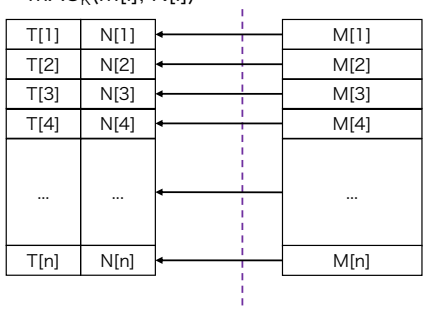


安全性	OK
計算量（遅延）	O(n)
On-chip メモリ量	O(1)
Off-chipメモリ オーバーヘッド	なし

共通鍵暗号の利用の検討2

- 各データブロックに対してMACを計算
  - On-chip に Off-chip と同等の量のデータを格納しなければならない
    - これが可能ならそもそもOn-chipに平文を格納すればよい

$T[i] = MAC_K(M[i], N[i])$



安全性	OK
計算量（遅延）	O(1)
On-chip メモリ量	O(n)
Off-chipメモリ オーバーヘッド	なし

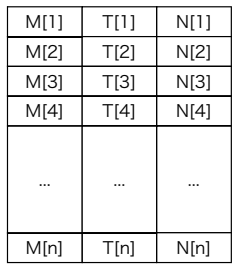
Trusted on-chip area　　Untrusted off-chip memory

共通鍵暗号の利用の検討3

- 計算したタグとナンスをOff-chipに格納する
  - リプレイ攻撃を防げない
    - 検証はOn-chip上のナンス (Root-of-Trust) に紐付けることが絶対に必要

$T[i] = MAC_K(M[i], N[i])$

（秘密鍵のみ）

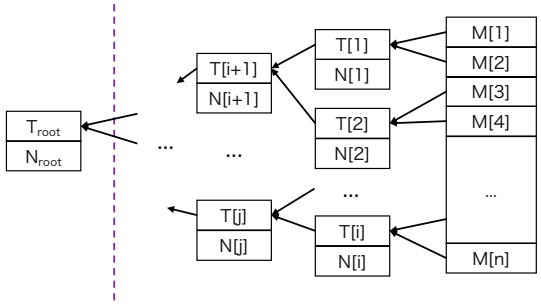


安全性	脆弱性あり
計算量（遅延）	O(1)
On-chip メモリ量	O(1) （秘密鍵のみ）
Off-chipメモリ オーバーヘッド	O(n)

Trusted on-chip area　　Untrusted off-chip memory

メモリ認証木

- リアルタイムでの暗復号および認証を実現
  - あるアドレスにアクセスするときは関連するタグのみを検証
- 現実的なOn-chipメモリ量でリプレイ攻撃対策を実現

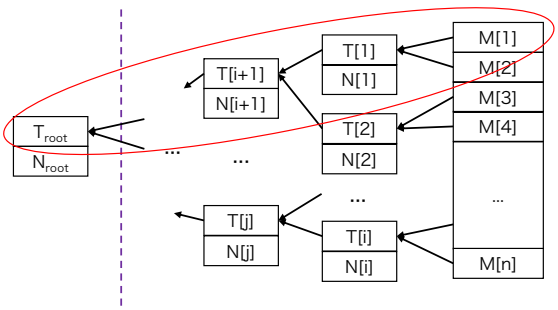


安全性	OK
計算量（遅延）	O(bd) = O(b $\log_b n$)
On-chip メモリ量	O(1)
Off-chipメモリ オーバーヘッド	O(b^{d-1})

d: 木の深さ，b: 木の分岐数 (Arity)

メモリ認証木

- リアルタイムでの暗復号および認証を実現
  - あるアドレスにアクセスするときは関連するタグのみを検証
- 現実的なOn-chipメモリ量でリプレイ攻撃対策を実現



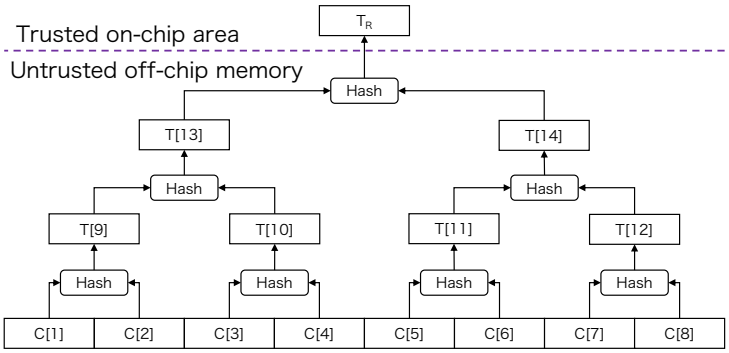
安全性	OK
計算量（遅延）	O(bd) = O(b $\log_b n$)
On-chip メモリ量	O(1)
Off-chipメモリ オーバーヘッド	O(b^{d-1})

d: 木の深さ，b: 木の分岐数 (Arity)

13

Merkle tree

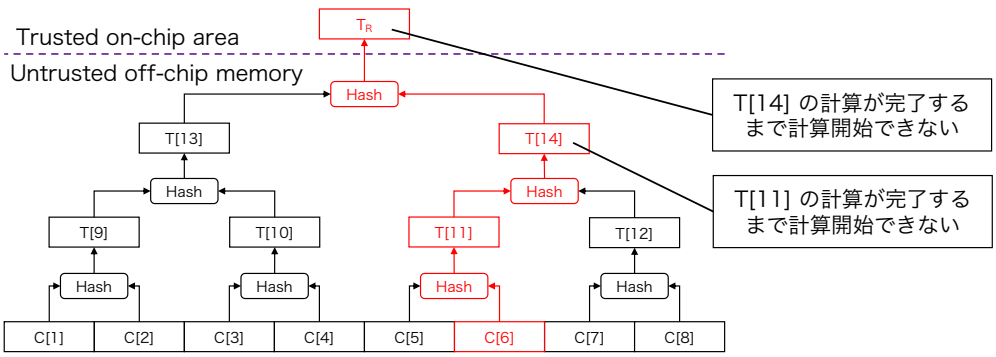
- 最も代表的な認証木構造
  - メモリ暗号化以外でもたびたび使われる（ハッシュベース署名など）
  - 暗号化にはカウンターモードAESを利用するのが一般的
    - カウンターに対して認証木を作ることで効率化（BMT: Bonsai MT）



14

Merkle treeの（メモリ暗号化における）欠点

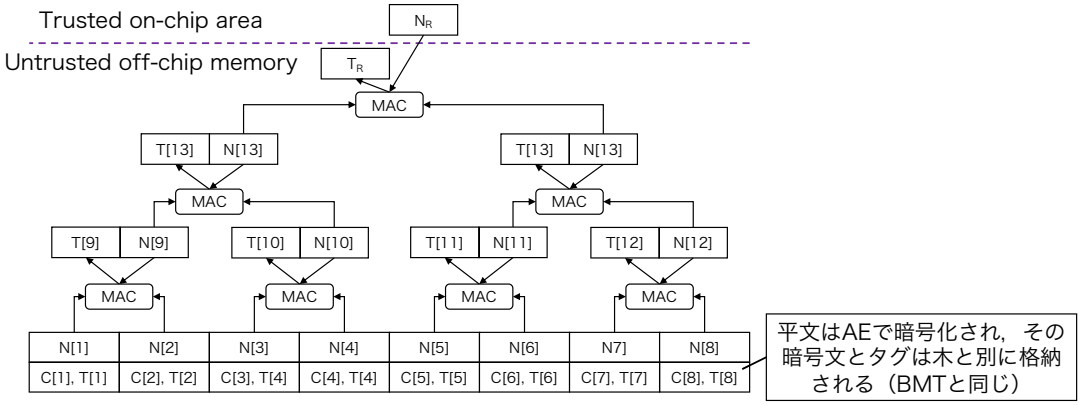
- 更新（書き込み）が並列化できないため更新に大きな遅延がかかる
  - 中間/ルートノードの計算にはその子ノードの計算完了を待つ必要がある
  - 大容量を守るために木が深くなるほどに致命的



15

Parallelizable Authentication Tree (PAT)

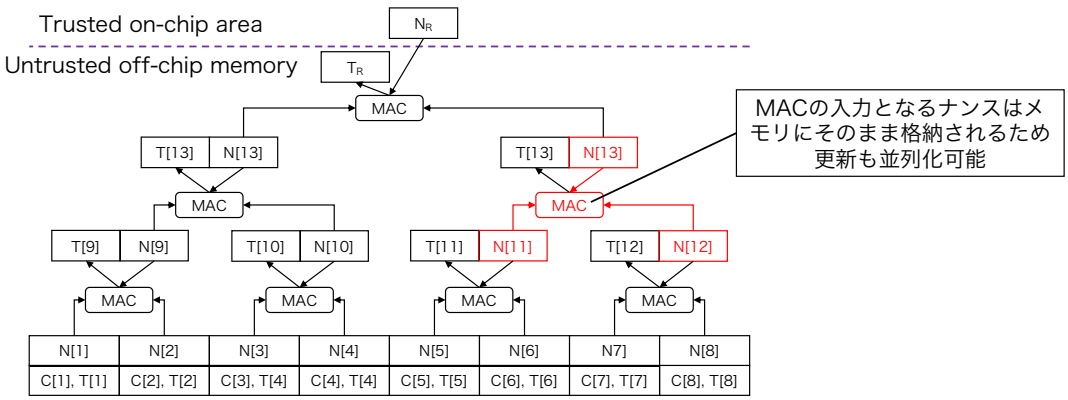
- 子ノードのタグではなく**ナンス**をMACを用いて認証する木
  - 親ノードのナンスがMACのナンスで，子ノードのナンスは検証対象データ
  - ナンスはNVMにそのまま格納できるため，更新も並列化可能



16

Parallelizable Authentication Tree (PAT)

- 子ノードのタグではなく**ナンス**をMACを用いて認証する木
  - 親ノードのナンスがMACのナンスで，子ノードのナンスは検証対象データ
  - ナンスはNVMにそのまま格納できるため，更新も並列化可能



17

本研究グループのアプローチ

- メモリ暗号化に最適化された新たなPATインスタンス ELM を提案
  - Encryption for Large Memory
  - 低遅延AEおよびMACである Flat–OCB および PXOR–MAC を提案（BCベース）
  - 遅延・On-chipメモリ量の観点からIntel SIT より大容量メモリに対しスケーラブル

- 現実世界で安全かつ効率的にELMを運用するためのハードウェアアーキテクチャを提案（本資料では割愛）

図の引用：https://commons.wikimedia.org/wiki/File:Ulmus_glabra_Lutescens_02.jpg

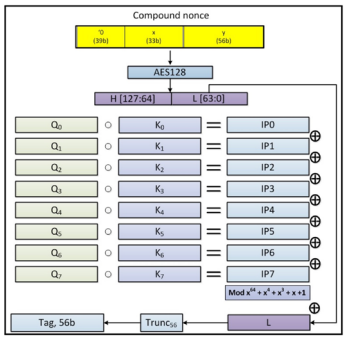
18

ELMの紹介

19

既存PAT: Intel SGX Integrity Tree (SIT)

- 代表的なTEEメモリ暗号化スキームだが不揮発メモリ暗号化の文脈でも最もメジャーなPATインスタンスの一つ [Gue16]
  - MAC: Inner-product MAC（汎用ハッシュを用いたWegman–Carter MAC）
  - AE: カウンターモードAESとInner-product MACの汎用結合
- メモリアドレスをImplicitナンスとして利用
  - ナンスデータ量を削減
  - Splicing（データ位置を入れ替える攻撃）対策
  - Explicitナンスはアップカウンターで実現



SITのMAC

[Gue16] S. Gueron, “A Memory Encryption Engine Suitable for General Purpose Processors ,” IACR ePrint Archive 2016/204.（図は同文献より引用）

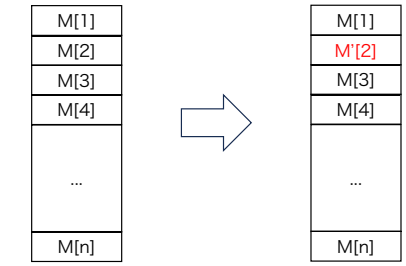
20

補足

- SITは128 MBの保護領域に特化している
  - より大きな領域の保護がOn-chipメモリオーバーヘッドの観点から非常に困難
    - Inner-product MACの鍵長が入力ビット長に対して線形なため
    - 汎用ハッシュをGHASH風にする（AES–GCMを利用する）ことも考えられるが，追加で遅延・回路面積が必要になる
- その他の既存PATについて
  - コンピュータアーキテクチャ分野の論文ではAESカウンターモードとHMACを想定して評価しているが，具体的な暗号や実装は考慮されないことが多い
  - 暗号化とHMACにかかる遅延は過去の論文に習って決め打ちしている
    - 160，80，40，あるいは20クロックサイクルと仮定されることが多いためおそらくSHA1 HMACを想定している（講演者の予想）

Key technique: Incremental cryptography

- 高効率なメモリ暗号化のために MAC の Incrementality を活用
  - メッセージブロックの一部がアップデートされた場合に，旧タグ，旧メッセージブロック，新旧ナンス，新メッセージブロックのみから新たなタグを計算
  - メモリ書き込みでは通常1ブロックごとに処理を行い，すべてのメッセージブロックが同時に更新されることはほとんどない



アップデート前　　アップデート後

ブロック暗号 (BC) ベースMACのBCコール回数

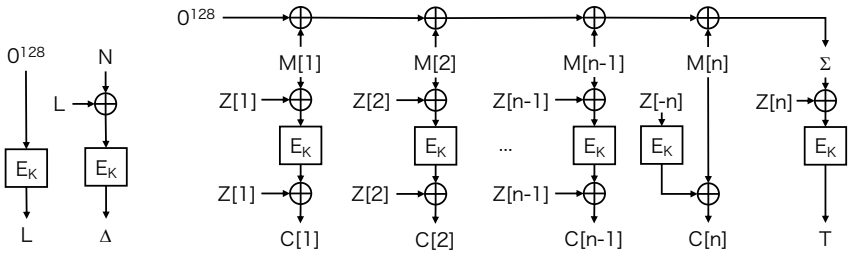
Tag generation and verification	O(n)
Non-incremental update	O(n)
Incremental update	O(1)

ELM: Encryption for Large Memory

- 可能な限り低遅延なAEとMACを用いたPAT
  - Flat–OCB: メモリ暗号化に特化してOCBを改良したAESベースAE
  - PXOR–MAC: IncrementalityとRate-1を備えたAESベースMAC
- 大きなNVMを効率的に保護
  - 鍵長は保護領域 n に対してO(1)
  - AESへの安全性帰着
- 想定：深さdの木を使用するときはd個のMAC/AEハードウェアで並列処理が可能
  - dは利用可能なハードウェアリソースあるいはメモリ帯域幅に従って決定
  - その上で木の分岐数b（MACの入力長に対応）と葉ノードのAEのブロック長 l をmax(MACの遅延，AEの遅延) が最小となるように決定

AEの利用の検討：OCB

- ISO/IEC にもインスタンスがリストされている代表的な Rate-1 AE
  - 暗号化/復号に必要なBCコール回数が入力ブロック数と（ほぼ）同じ
    - 例えばEncryption-then-MACなどの汎用結合は暗号化した後に暗号文に対してMACを計算するのでRate-1ではない
  - 並列化可能 (Parallelizable)：暗号化/復号処理は並列化可能
    - パイプラインやマルチコアによる低遅延実装が可能



（Z[i] はLとΔから決定的に計算）

OCB暗号化フロー（平文ビット長が128の倍数のとき）

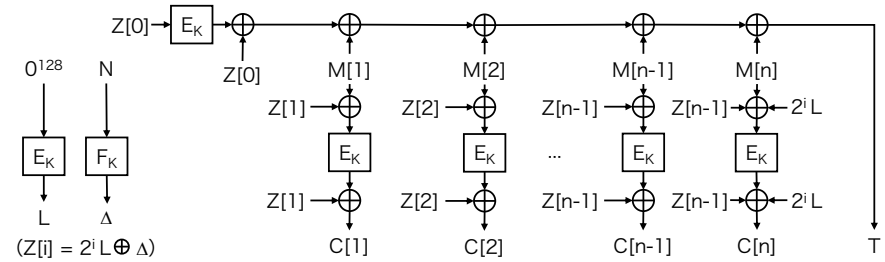
Flat-OCBの設計思想

- Rate-1（入力ブロック数とほぼ同等のBCコール数で暗号化とタグ生成を実現）
  - 暗号化モードとMACを組み合わせた汎用結合では達成不可
    - 例えばGCMやCCMは暗号文に対してGHASHやCMACを適用するためRate-1ではない（GF(2^{128}) 乗算はBCコール一回相当とみなす）
    - 既存のメジャーなPATは汎用結合を用いていた
  - 既存のOCBはこれを満たしている
- 並列化可能 (Parallelizable) かつ低遅延 (Low depth)
  - Depth: 暗号化とタグ生成までに必要な**並列化できない**BCコールの数
    - OCB暗号化はナンス処理（Initialization）と暗号化処理でdepth 2
    - OCB復号はナンス処理と暗号化処理とタグ生成でdepth 3
  - 暗復号の両方でdepth 2を達成したい
    - メモリ暗号化の文脈に特化することで何か最適化できないか

25

Flat-OCBの仕様

- AEではメッセージ長を特定する処理にコストを割くことが多い
  - メモリ暗号化では基本的に固定（あるいは128の倍数）と仮定してよい
    - メッセージ長特定の処理を簡易化して復号depthを2に
- ナンス処理では完全なBCは不要なのでナンス処理 F_K を低遅延化
  - 4ラウンドAESか，depth 1の GF(2^{64}) 乗算だけで安全に実現可能



Flat-OCB暗号化フロー（平文ビット長が128の倍数のときのみ利用可能）

26

AEの比較

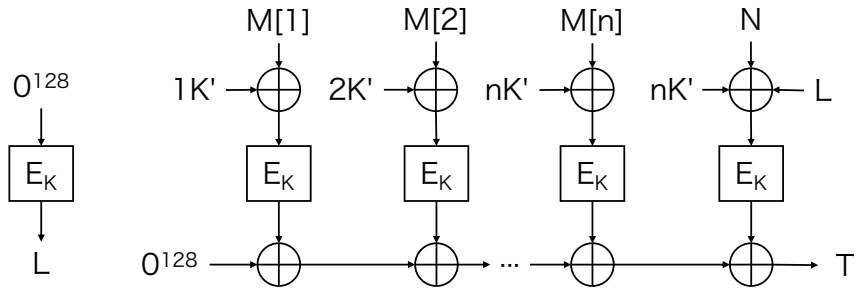
Scheme	Enc latency	Dec latency	Circuit size to achieve the best latency	Total size of key and preprocessed data (bits)
ΘCB [KR11]	1 TBC call	2 TBC calls	$m+1$ TBCs	n
Flat-ΘCB (This work)	1 TBC call	1 TBC calls	$m+1$ TBCs	n
OCB [KR11]	2 BC calls	3 BC calls	$m+1$ BCs	n
SIT-AE [Gue16b]	1 BC call + 1 multi.	max{1 BC call, 1 multi. }	$m+1$ BCs and $2m$ multipliers	$2n+mn$
Flat-OCB-f (This work)	1BC call + 1 AES4 call	1BC call + 1 AES4 call	$m+1$ BCs and one AES4	$2n+512$
Flat-OCB-m (This work)	1BC call + 1 multi.	1BC call + 1 multi.	$m+1$ BCs and 4 multipliers	$4n$

m: 入力ブロック数，n: (T)BC ビット長

27

PXOR-MACの設計仕様と思想

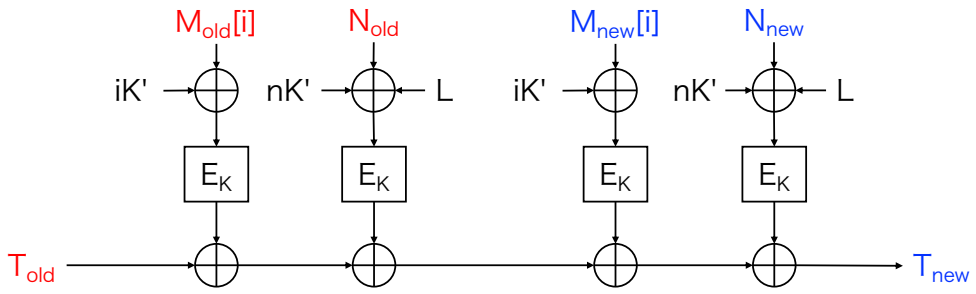
- BCベース，256ビット鍵 (K, K')，ナンスベース
- 低遅延：Rate-1かつdepth 1（並列化可能）
- Incrementality: タグ更新が O(1) で可能
- PMACあるいはXOR-MACをベースに実現



28

Incremental update

- 旧タグ T_{old}, 旧メッセージ $M_{old}[i]$, 旧ナンス N_{old} が利用可能なとき，新メッセージ $M_{new}[i]$, 新ナンス N_{new} に対する新タグ T_{new} をAESコール4回のみで計算可能

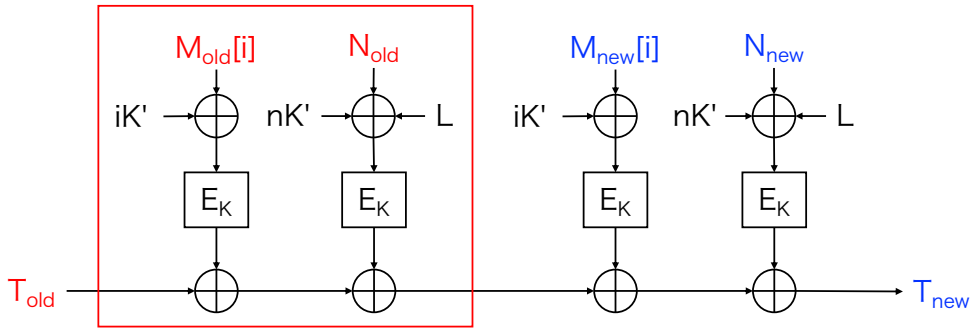


29

Incremental update

- 旧タグ T_{old}, 旧メッセージ $M_{old}[i]$, 旧ナンス N_{old} が利用可能なとき, 新メッセージ $M_{new}[i]$, 新ナンス N_{new} に対する新タグ T_{new} をAESコール4回のみで計算可能

T_{old}が含む$M_{old}[i]$とN_{old}の寄与分をキャンセル

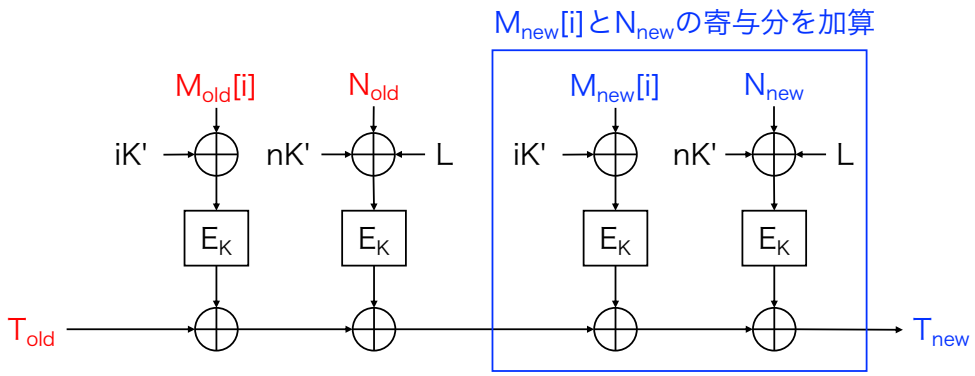


30

Incremental update

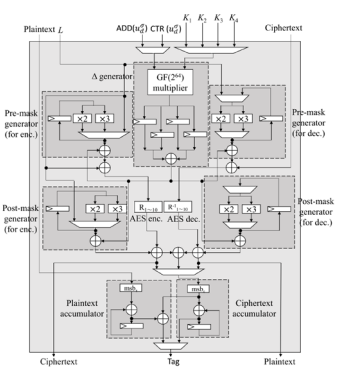
- 旧タグ T_{old}, 旧メッセージ $M_{old}[i]$, 旧ナンス N_{old} が利用可能なとき, 新メッセージ $M_{new}[i]$, 新ナンス N_{new} に対する新タグ T_{new} をAESコール4回のみで計算可能

$M_{new}[i]$とN_{new}の寄与分を加算

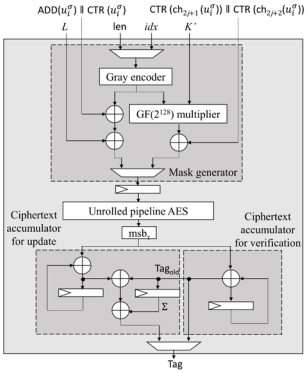


ハードウェア実装

- 10クロックサイクルの遅延で1ブロック/1サイクルのスループット
  - 動作周波数はモダンなCPUよりも高い（Nangate 15nmでの評価）



Flat-OCB



PXOR-MAC

Intel SITとELMのアルゴリズムレベル比較

- 様々な木パラメータに対して遅延と保護領域サイズを評価
  - Updateは検証も含む
  - max(AEの遅延, MACの遅延)をクロックサイクルで評価
- ELMは大容量を低遅延で保護可能
  - SIT はオンチップ容量のオーバーヘッドも無視できない

分岐数 b	リーフサイズ ℓ	Update			Verify		Covered region [Byte]		
		SIT	Incr. SIT	ELM	SIT / Incr. SIT	ELM	木の深さ $d=3$	$d=5$	$d=7$
8	512	**20**	**20**	21	**14**	18	32K	2M	134M
	1,024	32	32	**25**	**18**	22	65K	4M	268M
	2,048	64	64	**33**	32	**30**	131K	8M	536M
	4,096	128	128	**49**	64	**46**	262K	16M	1G
	8,192	256	256	**81**	128	**78**	524K	33M	2G
16	512	32	**20**	22	**16**	20	262K	67M	17G
	1,024	32	32	**25**	**18**	22	524K	134M	34G
	2,048	64	64	**33**	32	**30**	1M	268M	68G
	4,096	128	128	**49**	64	**46**	2M	536M	137G
	8,192	256	256	**81**	128	**78**	4M	1G	274G
32	512	64	33	**30**	32	**28**	2M	2G	2T
	1,024	64	33	**30**	32	**28**	4M	4G	4T
	2,048	64	64	**33**	32	**30**	8M	8G	8T
	4,096	128	128	**49**	64	**46**	16M	17G	17T
	8,192	256	256	**81**	128	**78**	33M	34G	35T
64	512	128	65	**46**	64	**44**	16M	68G	281T
	1,024	128	65	**46**	64	**44**	33M	137G	562T
	2,048	128	65	**46**	64	**44**	67M	274G	1P
	4,096	128	128	**49**	64	**46**	134M	549G	2P
	8,192	256	256	**81**	128	**78**	268M	1T	4P
128	512	256	129	**78**	128	**76**	134M	2T	36P
	1,024	256	129	**78**	128	**76**	268M	4T	72P
	2,048	256	129	**78**	128	**76**	536M	8T	144P
	4,096	256	129	**78**	128	**76**	1G	17T	288P
	8,192	256	256	**81**	128	**78**	2G	35T	576P

まとめ

- （不揮発）メモリ暗号化は現代のコンピュータの高性能化とセキュリティを両立するための重要な基盤技術
- リアルタイム保護そのものの難しさと，その運用や実装においても様々な困難がある
- 今回の講演ではメモリ認証木の最適化を紹介
  - 大容量NVMの保護における遅延とスケーラビリティを大きく改善

Towards Achieving Provable Side-Channel Security in Practice

Abdul Rahman Taleb

CryptoExperts and Sorbonne University
abdul.taleb@cryptoexperts.com

Physical side-channel attacks are powerful attacks that exploit a device's physical emanations to break the security of cryptographic implementations. Many countermeasures have been proposed against these attacks, especially the widely-used and efficient masking countermeasure. Nevertheless, proving the security of masked implementations is challenging. Current techniques rely on empirical approaches to validate the security of such implementations. On the other hand, the theoretical community introduced leakage models to provide formal proofs of the security of masked implementations. Meanwhile, these leakage models rely on physical assumptions that are difficult to satisfy in practice, and the literature lacks a clear framework to implement proven secure constructions on a physical device while preserving the proven security.

Towards Achieving Provable Side-Channel Security in Practice

https://eprint.iacr.org/2023/1198

Abdel Rahman Taleb

CryptoExperts, France
Sorbonne Université, CNRS, LIP6, F-75005 Paris, France

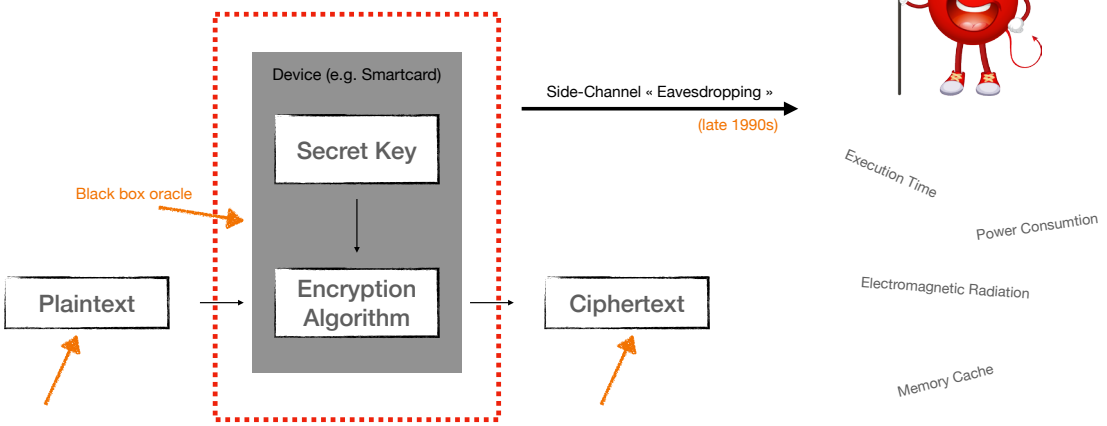
Mathematics of Security Analysis for Modern Cryptography

20/09/2023

CRYPTOEXPERTS
WE INNOVATE TO SECURE YOUR BUSINESS

SORBONNE UNIVERSITÉ

Side-Channel Attacks



2

Countermeasure

Masking *Chari et al. [CRYPTO'99], Goubin and Patarin [CHES'99]*

each observation comes with noise
Number of observations grows $\Longrightarrow$ harder to retrieve the secret

Secret Variable $x \in \mathbb{F}_2$ (field)

Encode

shares

Secret Vector $\overrightarrow{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$

s.t.

$x_1 \xleftarrow{\$} \mathbb{F}_2$

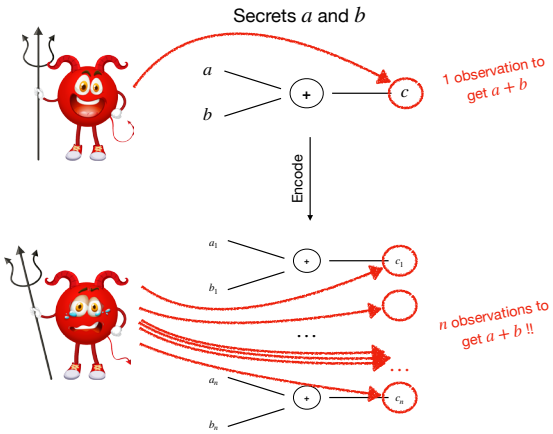
$\ldots$

$x_{n-1} \xleftarrow{\$} \mathbb{F}_2$

$n-1$ random values

secret recombination

$x_n \leftarrow x - x_1 \ldots - x_{n-1}$



3

Countermeasure

Gadgets

Intuitively, a gadget is considered « secure » if an attacker needs at least n observations to retrieve the secrets

Operations over variables $\mathbb{F}_2$

Atomic gates

a, b $+$ $a+b$

a, b $\times$ $a \times b$

random

r $r \xleftarrow{\$} \mathbb{F}_2$

Operations over masked variables in $\mathbb{F}_2^n$

n-share Gadgets formed of atomic gates

$(a_1, \ldots, a_n), (b_1, \ldots, b_n)$ G_+ $(c_1, \ldots, c_n)$ s.t. $c_1 + \ldots + c_n = a + b$

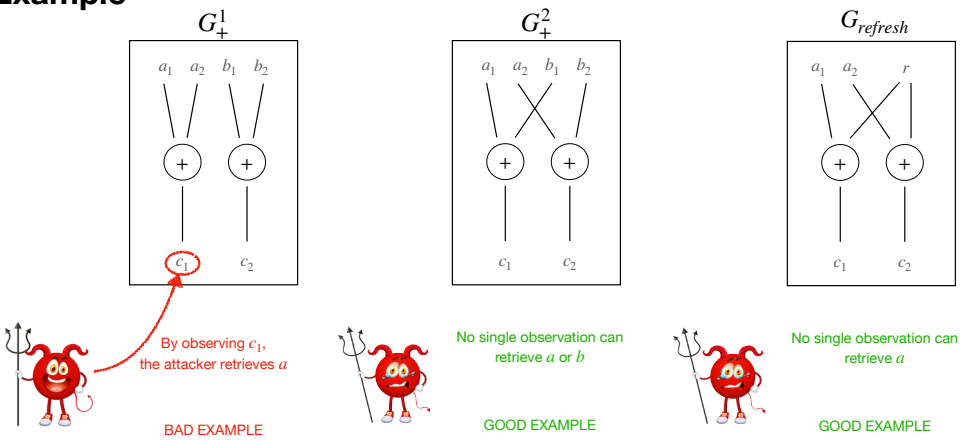
$(a_1, \ldots, a_n), (b_1, \ldots, b_n)$ $G_\times$ $(c_1, \ldots, c_n)$ s.t. $c_1 + \ldots + c_n = a \times b$

$(a_1, \ldots, a_n)$ $G_{refresh}$ new fresh shares $(c_1, \ldots, c_n)$ s.t. $c_1 + \ldots + c_n = a$

4

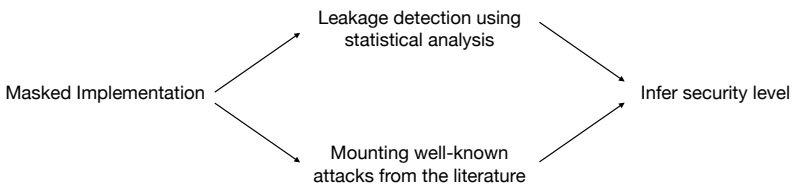
Gadgets
Example

Intuitively, a gadget is considered « secure » if an attacker needs at least n observations to retrieve the secrets



5

Security of Masked Implementations
Empirical Approach



How to have formal security guarantees ?

6

Security of Masked Implementations
Leakage Models

Theoretical view of masked implementations

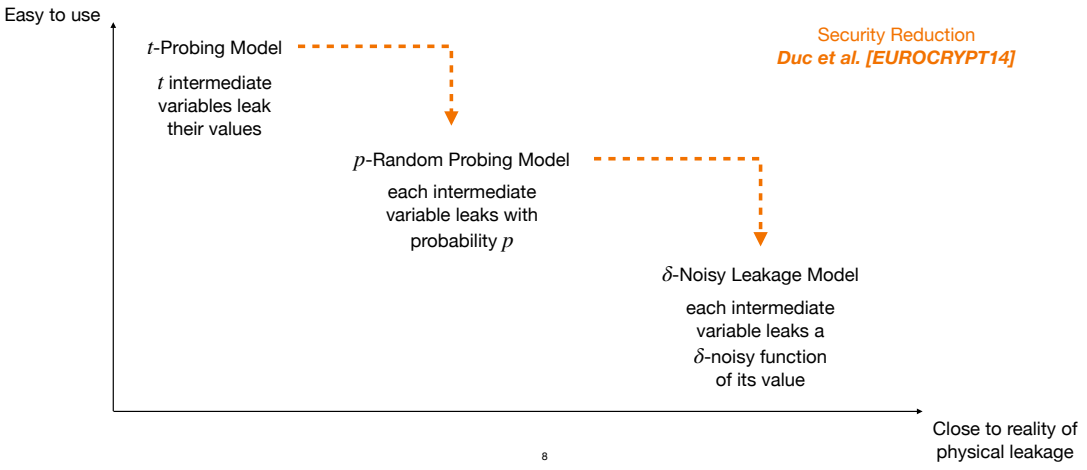
↓

Formally define side-channel attackers' capabilities

↓

Quantified security levels based on leakage models

Leakage Models

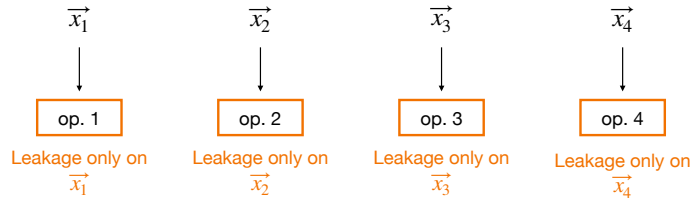


Leakage Models

Physical Assumptions

Each operation leaks during execution

Sequential execution of operations



Data Independence Assumption: each operation leakage only depends on its inputs

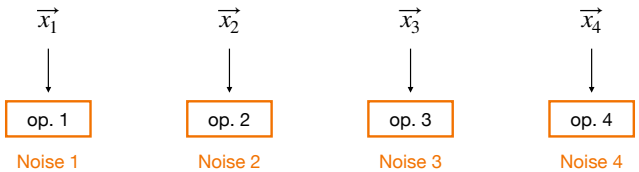
9

Leakage Models

Physical Assumptions

Physical noise occurs during side-channel acquisitions

Sequential execution of operations



Noise Independence Assumption: each noise is independent of the others

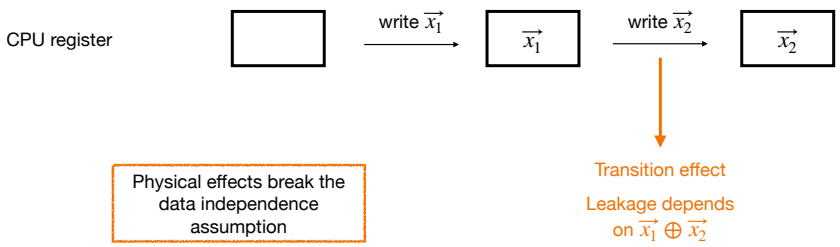
10

Leakage Models
Practical Issues

- No proper methodology to implement proven secure constructions on physical devices, while preserving security from the leakage models
- Physical Assumptions usually not satisfied in practice

11

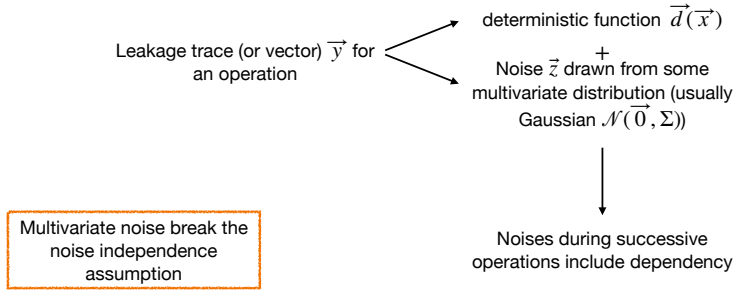
Leakage Models
Practical Issues



12

Leakage Models

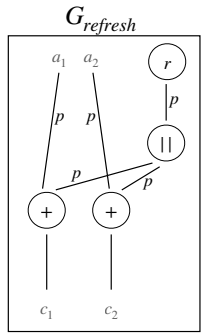
Practical Issues



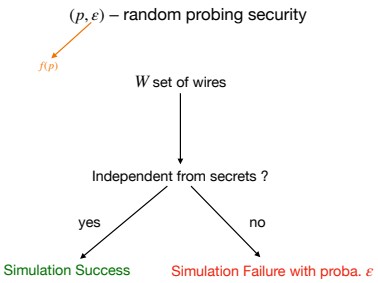
Contributions

- Propose a methodology to turn a masking scheme proven secure in the random probing (or noisy leakage) model into a physical implementation satisfying provable security in practice
- Address issues with physical assumptions
  - Propose a novel test to (in)validate data independence on a physical implementation
  - Integrate the loss of noise independence in the analysis, quantifying the implied loss of security
- Highlight design goals to achieve provable side-channel security in practice
- Discuss main limitations and issues, to finally bridge the gap between theory and practice once and for all

Technical Background
Random Probing Model



Choice: no leak on output shares, inputs of the next circuit



Examples

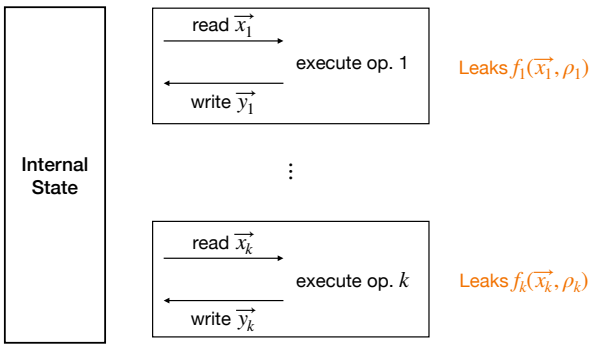
Success $\{a_1\}$ $Pr(\{a_1\}) = p(1-p)^4$

Success $\{a_2, r\}$ $Pr(\{a_2, r\}) = p^2(1-p)^3$

Failure $\{a_1, a_2\}$ $Pr(\{a_1, a_2\}) = p^2(1-p)^3$

15

Technical Background
Noisy Leakage Model



f_i is a noisy function with 2 inputs

sensitive input $\overrightarrow{x_i}$

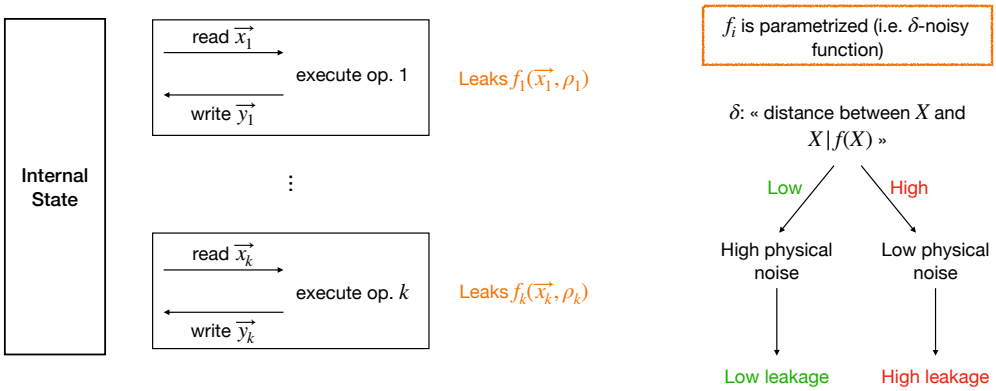
random string ρ_i to model noise

f_i is parametrized (i.e. δ-noisy function)

16

Technical Background

Noisy Leakage Model



Technical Background

Security Reduction

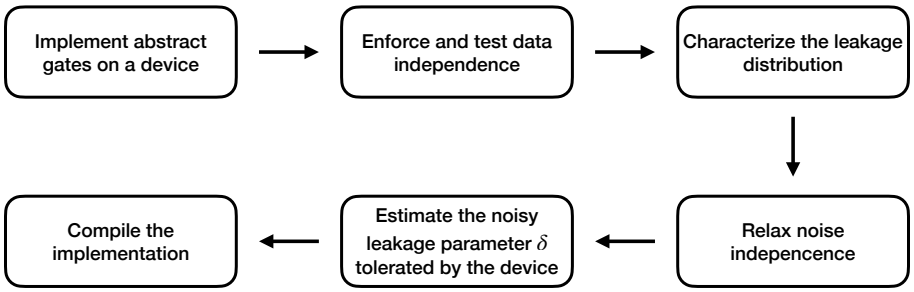
(p, ε)-random probing security $\Longrightarrow$ δ-noisy leakage security
($\delta = f(p)$, details later)

Why ?

δ-noisy leakage adversary **reduces to** a random probing adversary with leakage probability $f^{-1}(\delta)$

Circuit secure against p-random probing adversary, is also secure against δ-noisy leakage adversary for $p = f^{-1}(\delta)$

Methodology
Overview



19

Methodology
Overview

20

Implementing Abstract Gates

- Operation in the noisy leakage model:
  - read input from memory
  - execute operation
  - write output into memory

```
operation_xor:
  ldr r0, [r0]
  ldr r1, [r1]
  eor r0, r1 r0 // For other operations, change ALU instruction.
  str r0, [r2]
```

21

Implementing Abstract Gates

Assembly implementation

```
operation_xor:
  ldr r0, [r0]
  ldr r1, [r1]
  eor r0, r1 r0 // For other operations, change ALU instruction.
  str r0, [r2]
```

C signature interface

```
void operation_xor(const uint32* aPtr,
                   const uint32* bPtr,
                   uint32* cPtr);
```

Abstract circuit implementation

```
operation1(a1Ptr, b1Ptr, c1Ptr);
operation2(a2Ptr, b2Ptr, c2Ptr);
operation3(a3Ptr, b3Ptr, c3Ptr);
...
```

22

Methodology
Overview

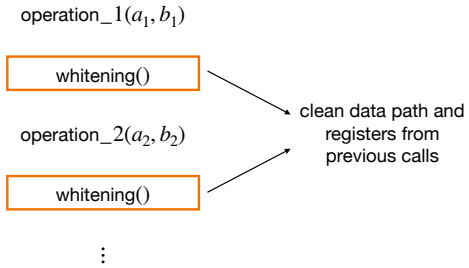
23

Data Independence
Enforcing

- Leakage of an operation must only depend on its inputs
- Physical defaults (e.g. transitions) break this assumption
- How to enforce it on a physical device ?
  - *data whitening*

24

Data Independence
Data Whitening

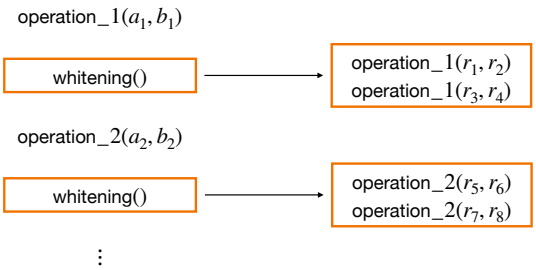


Example: call same operation with random inputs

Effectiveness depends on CPU micro-architecture

25

Data Independence
Data Whitening



How to test if it works ?

26

Data Independence
Testing

operation_1(a_1, b_1)
whitening()

operation_2(a_2, b_2)
whitening()

→ during operation_2, residual leakage of operation_1 might be present →

Relax data independence to tolerate residual linear leakage but not **joint leakage** on previous operation's inputs

Additively split leakage to separate operation signals

27

Data Independence
Testing

Leakage trace starting at operation_1 and ending after operation_2

operation_1(a_1, b_1)
whitening()

operation_2(a_2, b_2)
whitening()

→

Full leakage trace

$$\overrightarrow{y}(a_1, b_1, a_2, b_2) = \overrightarrow{d_1}(a_1, b_1) + \overrightarrow{d_2}(a_2, b_2) + \overrightarrow{N}$$

Noise independent of inputs

We need to ensure that the leakage trace satisfies the above form

We assume it is the case, and then validate / invalidate our assumption

28

Data Independence
Proposed Statistical Test

Fix a set of values (a_1, b_1, a_2, b_2)

Execute the following blocks several times

operation_1(a_1, b_1) whitening() operation_2(a_2, b_2) whitening()	operation_1(a_1, b_1) whitening() operation_2(0,0) whitening()	operation_1(0,0) whitening() operation_2(a_2, b_2) whitening()
Set of traces $T_{(1,1)}$	Set of traces $T_{(1,0)}$	Set of traces $T_{(0,1)}$
for each trace $\vec{y}$ in the set, we compute $\vec{y'} = \vec{y} - \overline{T_{(1,0)}} - \overline{T_{(0,1)}}$ to obtain a new set $T'_{(1,1)}$	under our assumption Average trace $\overline{T_{(1,0)}} = \vec{d_1}(a_1, b_1) + \vec{d_2}(0,0) + \vec{0}$ (Noise = $\vec{0}$ since it is gaussian of mean vector $\vec{0}$)	under our assumption Average trace $\overline{T_{(0,1)}} = \vec{d_1}(0,0) + \vec{d_2}(a_2, b_2) + \vec{0}$ (Noise = $\vec{0}$ since it is gaussian of mean vector $\vec{0}$)

under our assumption $\vec{y'} = d_1(a_1, b_1) + d_2(a_2, b_2) + \mathcal{N}(\vec{0}, \Sigma) - \vec{d_1}(a_1, b_1) - \vec{d_2}(0,0) - \vec{d_1}(0,0) - \vec{d_2}(a_2, b_2) = \mathcal{N}(\vec{0}, \Sigma) - \vec{d_2}(0,0) - \vec{d_1}(0,0)$

29

Data Independence
Proposed Statistical Test

Fix a set of values (a_1, b_1, a_2, b_2)

Under our assumption, the new set of traces $T'_{(1,1)}$ contains traces of the form $-\vec{d_1}(0,0) - \vec{d_2}(0,0) + \mathcal{N}(\vec{0}, \Sigma)$

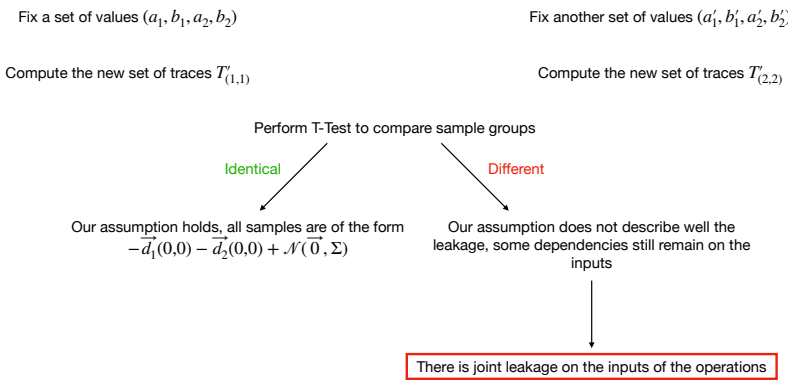
↓

traces that do not depend on any input (Multivariate Gaussian noise + constant vectors)

Does our assumption hold ?

30

Data Independence
Proposed Statistical Test



Data Independence
Proposed Statistical Test

- After several executions of the test with different inputs, the assumption can be (in)validated
- We argue that the absence of dependency for adjacent operations guarantees the absence of dependency for non-adjacent ones
- We perform our test with a chipwhisperer, on an STM32F3 MCU based on an ARM Cortex-M4, with 8-bit operations

```
xor_func:
  ldr r0, [r0]
  ldr r1, [r1]
  eor r0, r1 r0
  str r0, [r2]
```

```
and_func:
  ldr r0, [r0]
  ldr r1, [r1]
  and r0, r1 r0
  str r0, [r2]
```

```
left_shift_func:
  ldr r0, [r0]
  mov r0, r0, LSL 1
  str r0, [r1]
```

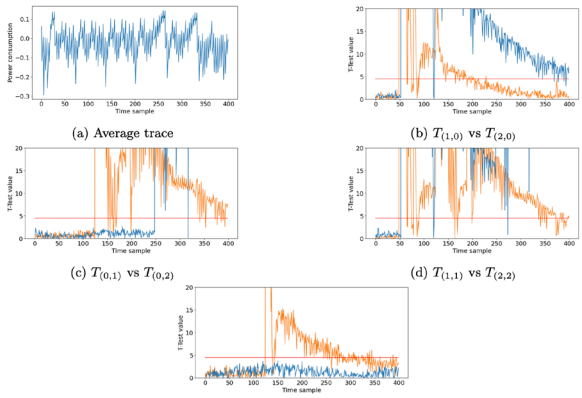
```
right_shift_func:
  ldr r0, [r0]
  mov r0, r0, LSR 1
  str r0, [r1]
```

```
void whitening(void) {
  xor_func(a1Ptr, b1Ptr, c1Ptr);
  xor_func(a2Ptr, b2Ptr, c2Ptr);
  xor_func(a3Ptr, b3Ptr, c3Ptr);
}
```

Fig. 3: Elementary Operations (xor, and, left shift, right shift) and whitening as implemented on the STM32F3 MCU.

Data Independence

Proposed Statistical Test



(a) Average trace

(b) $T_{(1,0)}$ vs $T_{(2,0)}$

(c) $T_{(0,1)}$ vs $T_{(0,2)}$

(d) $T_{(1,1)}$ vs $T_{(2,2)}$

(e) Proposed T-Test

Fig. 4: Data Isolation Test. Blue (with whitening). Orange (without whitening).

33

Methodology

Overview

34

Leakage Distribution
Characterization

- A well-studied problem in the literature
- The leakage of an operation with input $\vec{x}$ takes the form $\vec{y} = \vec{d}(\vec{x}) + \mathcal{N}(\vec{0}, \Sigma)$
- Procedure:
  - Acquire a set of traces for the considered operation
  - Estimate the deterministic functions $\vec{d}(\cdot)$ ($d_i(\cdot)$ for each time sample i)
  - Acquire a new set of traces and remove the deterministic part (i.e. $\vec{y} - \vec{d}(\vec{x})$)
  - Compute the covariance matrix Σ from the resulting traces

35

Leakage Distribution
Characterization

For each time sample i, $d_i(\vec{x}) = \sum_{j=1}^{m} \alpha_i \cdot h_i(\vec{x})$

α_i are coefficients to be estimated

h_i are functions that depend on the bits of the input $\vec{x}$

We can use linear regression to estimate the coefficients

36

Methodology
Overview

37

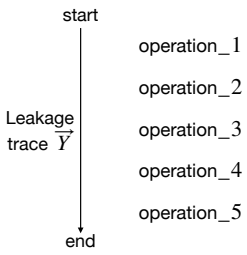
Noise Independence
Relaxation

- Leakage models require noise independence assumption
- Difficult to ensure in practice
  - Multivariate noise induces dependencies between operations
- Relax noise independence instead of enforcing it
  - Split the noise occurring at each time sample among the different operations
  - Need to take into account the noisiness level (lower noise $\Longrightarrow$ higher information leakage)
  - An attacker with access to the split noise, can easily recover the original noise $\Longrightarrow$ easy security reduction

38

Noise Independence

Trivial Relaxation



$$\overrightarrow{Y} = \overrightarrow{S_1} + \overrightarrow{S_2} + \overrightarrow{S_3} + \overrightarrow{S_4} + \overrightarrow{S_5} + \overrightarrow{N}$$

each S_i is only the leakage of operation_i (data independence assumption)

Split $\overrightarrow{N}$ among the operations instead of having time-separated noises for each operation

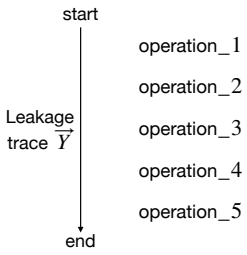
$$\overrightarrow{N} = \overrightarrow{N_1} + \overrightarrow{N_2} + \overrightarrow{N_3} + \overrightarrow{N_4} + \overrightarrow{N_5} \text{ such that } \overrightarrow{N_i} = \frac{1}{5}\overrightarrow{N}$$

Drawback: more operations $\Longrightarrow$ less noise on each operation $\Longrightarrow$ more leakage $\Longrightarrow$ lower security level in the leakage models

39

Noise Independence

Attempt at an Optimized Relaxation



$$\overrightarrow{Y} = \overrightarrow{S_1} + \overrightarrow{S_2} + \overrightarrow{S_3} + \overrightarrow{S_4} + \overrightarrow{S_5} + \overrightarrow{N}$$

Each $\overrightarrow{S_i}$ has most leakage during operation_i, then residual weaker leakage during next operations

Need more noise in $\overrightarrow{N_i}$ during the execution of operation_i

Can be expressed as an optimization problem: how to rewrite $\overrightarrow{N} = \overrightarrow{N_1} + \ldots + \overrightarrow{N_5}$, such as to minimize the information leakage (e.g. Signal-to-Noise ratio) of the different operations ?

40

Methodology
Overview

41

Noisy Leakage Parameter

(p, ε)-random probing security $\implies$ δ-noisy leakage security

- Mainly two metrics for δ
  - Statistical distance
  - Average relative error

Definition 6 (Pointwise Mutual Information). *Let X, Y be random variables over $\mathcal{X}, \mathcal{Y}$ respectively. For any $x \in \mathcal{X}, y \in \mathcal{Y}$, the exponential form of the pointwise mutual information (PMI) is defined as:*

$$\mathrm{PMI}_{X,Y}(x, y) = \frac{P[X = x, Y = y]}{P[X = x] \cdot P[Y = y]} - 1 \ .$$

42

Noisy Leakage Parameter

(p, ε)-random probing security $\implies$ δ-noisy leakage security

- Mainly two metrics for δ
  - Statistical distance
  - Average relative error

Definition 7. *Let X, Y be random variables over $\mathcal{X}, \mathcal{Y}$ respectively. We can define the L1 statistical distance (SD) as follows:*

$$\mathrm{SD}(X|Y) = \frac{1}{2}\,\mathbb{E}_{Y=y}\mathbb{E}_{X=x}\left[\left|\mathrm{PMI}_{X,Y}(x,y)\right|\right] .$$

The average relative error (ARE) can also be expressed as:

$$\mathrm{ARE}(X|Y) = \mathbb{E}_{Y=y}\left[\max_{x}\left|\mathrm{PMI}_{X,Y}(x,y)\right|\right] .$$

Noisy Leakage Parameter

(p, ε)-random probing security $\implies$ δ-noisy leakage security

- When ARE noisy functions $\implies p \approx \delta$
- When SD noisy functions $\implies p \approx |\mathcal{X}| \cdot \delta$

Definition 7. *Let X, Y be random variables over $\mathcal{X}, \mathcal{Y}$ respectively. We can define the L1 statistical distance (SD) as follows:*

$$\mathrm{SD}(X|Y) = \frac{1}{2}\,\mathbb{E}_{Y=y}\mathbb{E}_{X=x}\left[\left|\mathrm{PMI}_{X,Y}(x,y)\right|\right] .$$

The average relative error (ARE) can also be expressed as:

$$\mathrm{ARE}(X|Y) = \mathbb{E}_{Y=y}\left[\max_{x}\left|\mathrm{PMI}_{X,Y}(x,y)\right|\right] .$$

Noisy Leakage Parameter

(p, ε)-random probing security $\implies$ δ-noisy leakage security

- When ARE noisy functions $\implies p \approx \delta$
- When SD noisy functions $\implies p \approx |\mathcal{X}| \cdot \delta$
- Random probing model: worst-case model
- ARE: worst-case metric
- SD: average-case metric

45

Noisy Leakage Parameter

$$
\begin{aligned}
ARE &= \mathbb{E}_Y \max_{X=\boldsymbol{x}} |PMI| \\
&= \mathbb{E}_Y \max_{X=\boldsymbol{x}} \left| \frac{P[X=\boldsymbol{x}, Y=\boldsymbol{y}]}{P[X=\boldsymbol{x}] \cdot P[Y=\boldsymbol{y}]} - 1 \right| \\
&= \mathbb{E}_Y \max_{X=\boldsymbol{x}} \left| \frac{P[Y=\boldsymbol{y}|X=\boldsymbol{x}]}{\sum_{X=\boldsymbol{x}'} P[Y=\boldsymbol{y}|X=\boldsymbol{x}']} \cdot \frac{1}{P[X=\boldsymbol{x}]} - 1 \right|
\end{aligned}
$$

$$
\begin{aligned}
SD &= \frac{1}{2} \mathbb{E}_Y \mathbb{E}_X |PMI| \\
&= \mathbb{E}_Y \frac{1}{2} \sum_{X=\boldsymbol{x}} \left| \frac{P[Y=\boldsymbol{y}|X=\boldsymbol{x}]}{\sum_{X=\boldsymbol{x}'} P[Y=\boldsymbol{y}|X=\boldsymbol{x}']} \cdot \frac{1}{P[X=\boldsymbol{x}]} - 1 \right|
\end{aligned}
$$

Critical operations:
- expected value
- conditional probability
- max

46

Noisy Leakage Parameter

- After the leakage characterization, the conditional probability can be computed

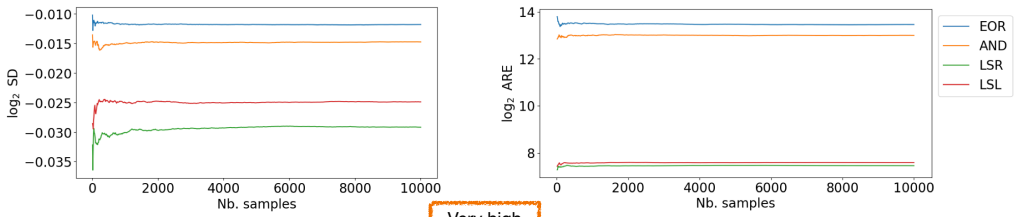
$$P[Y = \boldsymbol{y}|X = \boldsymbol{x}] = \frac{1}{\sqrt{(2\pi)^n \left|\Sigma\right|}} \exp\Big(-\frac{1}{2}(\boldsymbol{y} - d(\boldsymbol{x}))^T \Sigma^{-1}(\boldsymbol{y} - d(\boldsymbol{x}))\Big)$$

- We also estimate the expected values using Monte-Carlo convergence method

Noisy Leakage Parameter

(p, ε)-random probing security $\implies$ δ-noisy leakage security

- When ARE noisy functions $\implies p \approx \delta$
- When SD noisy functions $\implies p \approx |\mathcal{X}| \cdot \delta$ here $|\mathcal{X}| = 2^{16}$



(a) SD

Very high levels!

(b) ARE

Each ARE and SD value is computed using the inferred deterministic function, and the noise covariance matrix

Methodology
Overview

49

Wrapping up

- Implement random probing secure gadgets tolerating a leakage probability p, based on δ computed on the physical device
- Best gadgets from the state of the art tolerate $p \approx 2^{-7} \Longrightarrow$ MCU chip not adapted for provable side-channel security!

σ	**ARE**	**SD**
5	2^{-7}	2^{-10}
10	2^{-8}	2^{-11}
20	2^{-9}	2^{-12}
40	2^{-10}	2^{-13}
1280	2^{-15}	2^{-18}

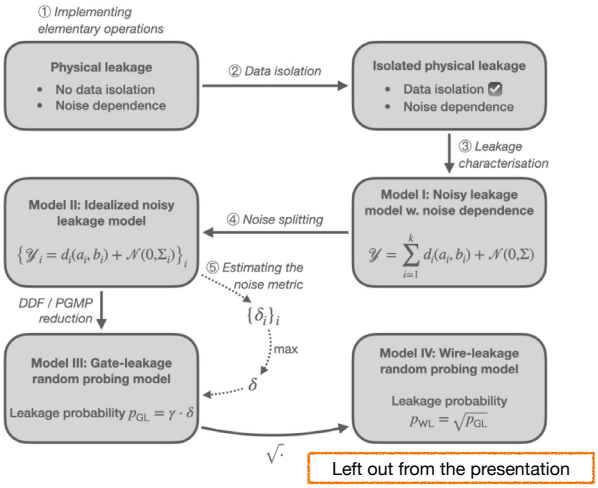
ARE and SD values after adding artificial noise to side-channel traces on the chip

σ : standard deviation of added noise

$\sigma_{\text{signal}} \approx 2^{-8}$

50

Conclusion



Left out from the presentation

Conclusion

- Methodology exhibits all steps to use provably secure gadgets on physical devices
- Novel test for data independence
- The first attempt in the literature to directly tackle the noise independence assumption and relax it
- Noise levels are critical for security levels → tested component showcases the results but is not suited for the use-case
  - How to achieve high physical noise when designing hardware?
- Can we make leakage models and security proofs tighter?
- Can we solve the remaining limitations of the approach ?

Future Works

- Many future works!
- Many questions are raised to completely bridge the gap between theory and practice
  - Extend the approach to hardware implementations
  - Integrate potential data/noise dependence in the security proofs instead of enforcing/ relaxing them.
  - Find components which satisfy the required noise and security levels
  - Apply the noise relaxation technique on real-life devices
  - parallel implementations ?
  - …

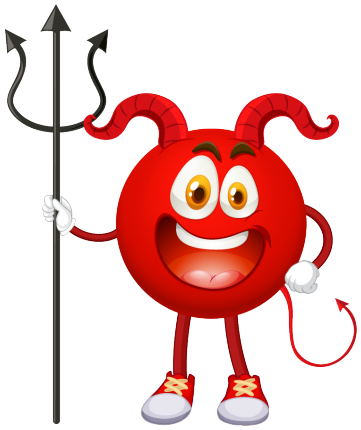
53

Our main goal is to popularize the research topic and make room for many future advances

https://eprint.iacr.org/2023/1198

54

ありがとうございました！
Any questions ?



55

共通鍵暗号の認証暗号利用モードの安全性と攻撃について

井上 明子
NEC
a_inoue@nec.com

認証暗号は平文の秘匿と暗号文の改ざん検知が同時に実現できる共通鍵暗号方式である. その安全性は, 2000 年に秘匿と改ざん検知の 2 つとして正式に定義されたが, その後, これらの安全性を満たす認証暗号が実装上の過失により破れる場合があることや, 認証暗号を用いるプロトコルが, 秘匿と改ざん検知以上の安全性を認証暗号に要求している場合があることが攻撃により示されている. 本発表では, ブロック暗号等の固定長入出力暗号部品を用いた認証暗号構成を中心の話題として, 基本的な認証暗号の安全性及びそれに対する攻撃, そして上記のように基本の安全性を超えた攻撃や, それらを考慮した認証暗号の拡張された安全性について紹介する.

\Orchestrating a brighter world NEC

現代暗号に対する安全性解析・攻撃の数理 2023/09/20~2023/09/22

共通鍵暗号の認証暗号利用モードの安全性と攻撃について

NEC セキュアシステムプラットフォーム研究所 井上明子

今回の発表内容

- ◆ 認証暗号のGIFT-COFBを例にとって以下を話します
- ◆ 認証暗号とは
  - ■ 基本の安全性: 秘匿, 改ざん検知
- ◆ 拡張された安全性: ナンス誤用
  - ■ Nonce-misuse resistance
  - ■ Nonce-misuse resilience
- ◆ その他の拡張された安全性の紹介
  - ■ 耐未検証平文漏洩安全性, 耐漏洩安全性, Key committing security

- ■ COFBの構成, 設計思想
- ■ 攻撃: 主張された安全性の誤りの証明 @ACNS2022

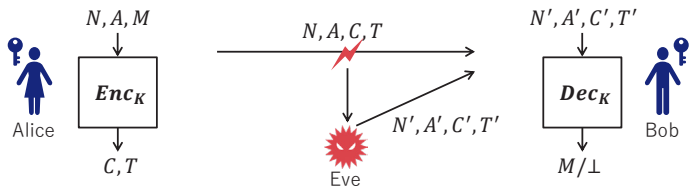
- ■ COFBのNonce misuse resistanceの攻撃
- ■ COFBのNonce misuse resilienceの証明 @IET Info. Sec.

\Orchestrating a brighter world NEC

認証暗号 (Authenticated Encryption with Associated Data)

◆ 入力データの暗号化と改ざん検知が同時に実現できる共通鍵暗号方式 [Rog02]

- M: 平文, C: 暗号文, K: 秘密鍵, N: Nonce (初期ベクトル), T: 認証タグ, A: Associated Data (AD)
- 暗号化関数 : $Enc_K(N, A, M) = (C, T)$
- 復号関数 : $Dec_K(N', A', C', T') = \begin{cases} M & \text{(改ざんが検知されない場合)} \\ \perp & \text{(改ざんが検知された場合)} \end{cases}$
- NISTによる軽量認証暗号標準化コンペ (NIST Lightweight Cryptography: NIST LwC) が開催された
  - 57件の応募のうち, 2021年3月にファイナリスト10件が選出. 2023年2月にAsconが標準化されることが発表された

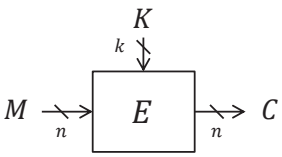


認証暗号の実現方法

◆ 対象: **固定長入出力の暗号プリミティブ**を組み合わせる方法 (**暗号利用モード**)

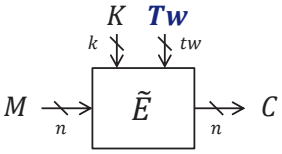
◆ ブロック暗号

- $E: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$
- 固定長入出力の鍵付き置換: E_Kは$\{0,1\}^n$上の置換となる
- 安全性: ランダム置換と判別困難



◆ Tweakable ブロック暗号 (TBC)

- $\tilde{E}: \{0,1\}^k \times \{\mathbf{0,1}\}^{\boldsymbol{tw}} \times \{0,1\}^n \to \{0,1\}^n$
- ブロック暗号の入力に**Tweak** (公開調整値) を含めた鍵付き置換: $\tilde{E}_K^{\boldsymbol{Tw}}$は$\{0,1\}^n$上の置換となる
- Tweakが異なるTBCはそれぞれ独立なブロック暗号と見なせる
- ブロック暗号を用いたモードとしても実現可能

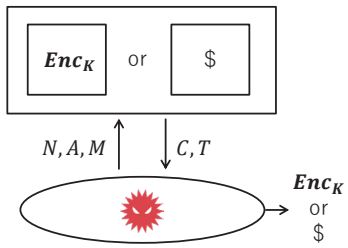


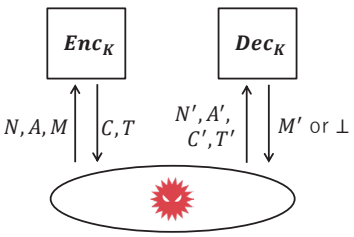
◆ **認証暗号の安全性を暗号プリミティブの安全性に帰着させて安全性証明を行う**

認証暗号の安全性

◆ 暗号化の安全性 (PRIV)
- Encクエリを行う攻撃者が, $\boldsymbol{Enc_K}$と
  ランダムオラクル $ を判別できる確率で評価
- 同じナンスは繰り返さない (Nonce-respecting)

◆ 改ざん検知の安全性 (AUTH)
- $\boldsymbol{Enc_K}$と$\boldsymbol{Dec_K}$にアクセスする攻撃者が
  $\boldsymbol{Dec_K}$から ⊥ 以外を受け取る確率で評価
- Encクエリでは Nonce-respecting



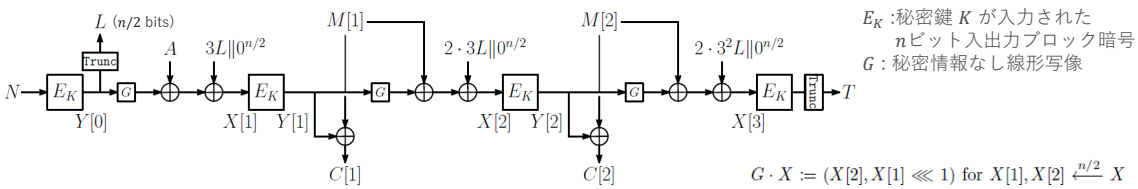


◆ 認証暗号全体の安全性をPRIV + AUTHで評価する場合もある

GIFT-COFB [BCI+21]

◆ NIST LwC ファイナリストの10件のうちの1つ
- ブロック暗号GIFT-128 [BPP+17] とCOFBモードの組み合わせ

◆ COFB (COmbined-FeedBack mode)
- CHES2017にてChakrabortiらによって提案 [CIMN17]
- 若干スペックが異なるバージョン JoC版 [CIMN20], NIST LwC版 [BCI+21] があるが,
  今回はNIST LwC版に着目して解析する



GIFT-COFB

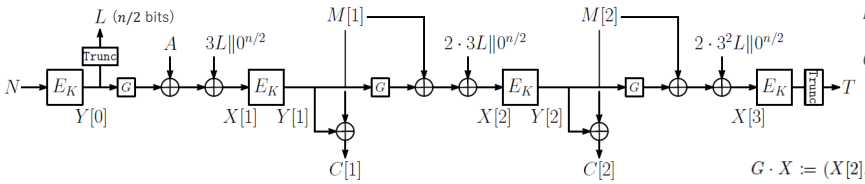
◆ 構造

■ 図: ナンス N を用いてnビットAD A と$2n$ビット平文 $M = M[1] \,||\, M[2]$ を処理

- Nを暗号化した値のうち$n/2$ビットの値 L を取得. L はその後のAD処理と平文処理で利用
- 暗号化結果 $Y[0]$ は線形写像 G によって変換され, ADブロックとXOR
- L を用いた $n/2$ ビットのマスク値をXORした値を暗号化. AD処理終了
- 暗号化処理もAD処理と同様. 暗号文導出はステート $Y[\cdot]$ とのXOR. 最後のステートがタグとなる
- $Dec_K(N, A, C, T)$ は暗号化と逆向きの処理. 最後のステートと入力タグの一致/不一致で改ざんを検知

■ ポイント

- $n/2$ビットマスクを更新しながら, マスク値をブロック暗号入力前にXORした形でシリアルにAD/平文を処理
- 線形写像 G によってステートが更新 (G の条件: I が単位行列のとき, 行列 G 及び $G \oplus I$ のランクがほぼFull)



E_K :秘密鍵 K が入力された
nビット入出力ブロック暗号
G : 秘密情報なし線形写像

$G \cdot X := (X[2], X[1] \lll 1)$ for $X[1], X[2] \xleftarrow{n/2} X$

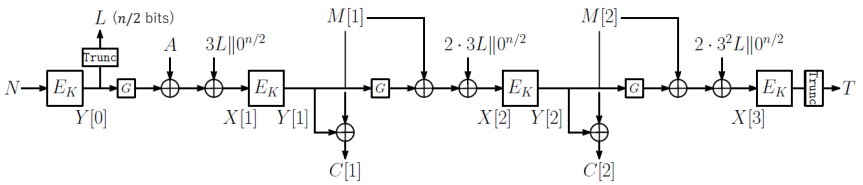
COFBの特徴

◆ **レート1** : 1回のブロック暗号呼び出しで1ブロック平文処理が可能

■ 現行NIST標準GCM, CCMはレート1/2: 1ブロック平文処理に2回のブロック暗号呼び出し必要

■ **Gの導入によりブロック暗号ベース & Feedback型の構成でもレート1を達成**

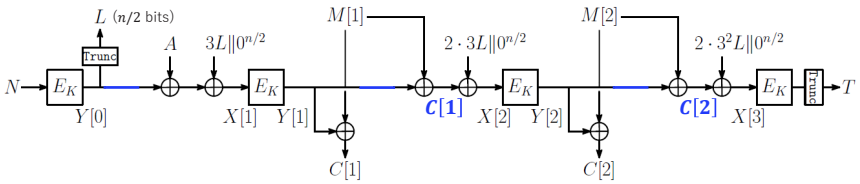
- 例: Gが単位行列のとき, 安全な認証暗号にならないことを示す



COFBの特徴

◆ **レート1** : 1回のブロック暗号呼び出しで1ブロック平文処理が可能

- 現行NIST標準GCM, CCMはレート1/2: 1ブロック平文処理に2回のブロック暗号呼び出し必要
- **Gの導入によりブロック暗号ベース & Feedback型の構成でもレート1を達成**
  - 例: Gが単位行列のとき, 安全な認証暗号にならないことを示す
  - 暗号化方式 CFB (Ciphertext FeedBack) モード 的な方式: CFBはCPA安全なのでPRIVは大丈夫そう → AUTHは?

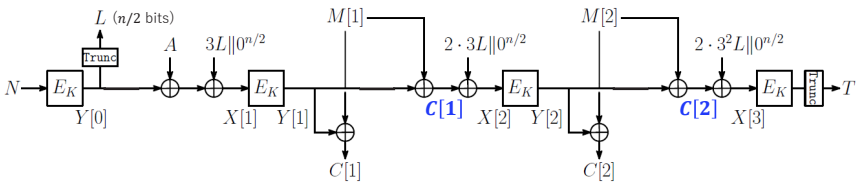


COFBの特徴

◆ **レート1** : 1回のブロック暗号呼び出しで1ブロック平文処理が可能

- 現行NIST標準GCM, CCMはレート1/2: 1ブロック平文処理に2回のブロック暗号呼び出し必要
- **Gの導入によりブロック暗号ベース & Feedback型の構成でもレート1を達成**
  - 例: Gが単位行列のとき, 安全な認証暗号にならないことを示す
  - 暗号化方式 CFB (Ciphertext FeedBack) モード 的な方式: CFBはCPA安全なのでPRIVは大丈夫そう → AUTHは?

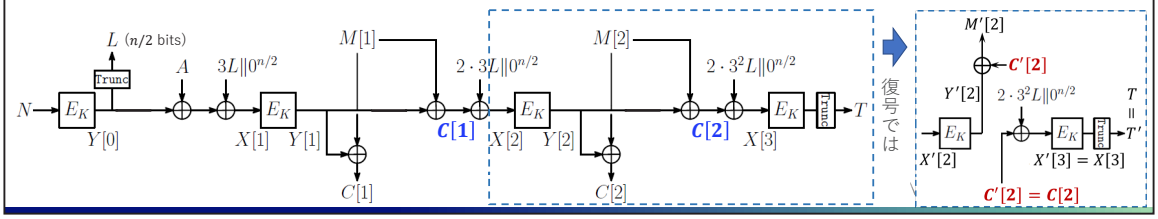
  - AUTHにおいて, 攻撃者はEncクエリで取得した暗号文/タグを利用してDecクエリできる
  - 図の様に(N, A, M)をクエリして(C, T)を受け取り, (N, A, C', T) s.t. $C'[1] \neq C[1]$, $C'[2] = C[2]$ をクエリすれば攻撃成功



COFBの特徴

◆ **レート1** : 1回のブロック暗号呼び出しで1ブロック平文処理が可能

- 現行NIST標準GCM, CCMはレート1/2: 1ブロック平文処理に2回のブロック暗号呼び出し必要
- **Gの導入によりブロック暗号ベース & Feedback型の構成でもレート1を達成**
  - 例: Gが単位行列のとき, 安全な認証暗号にならないことを示す
  - 暗号化方式 CFB (Ciphertext FeedBack) モード 的な方式: CFBはCPA安全なのでPRIVは大丈夫そう → AUTHは?
  - AUTHにおいて, 攻撃者はEncクエリで取得した暗号文/タグを利用してDecクエリできる
  - 図の様に(N, A, M)をクエリして(C, T)を受け取り, (N, A, C', T) s.t. $C'[1] \neq C[1]$, $C'[2] = C[2]$ をクエリすれば攻撃成功

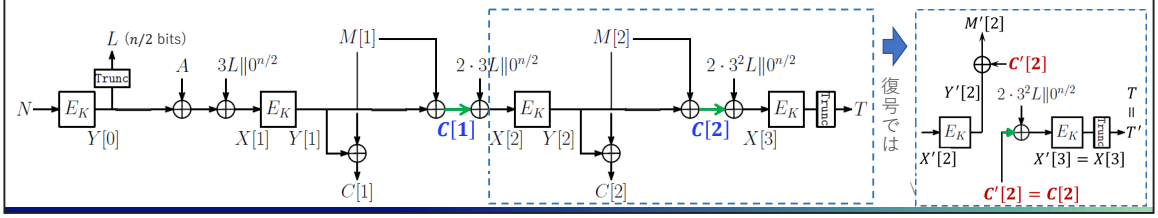


COFBの特徴

◆ **レート1** : 1回のブロック暗号呼び出しで1ブロック平文処理が可能

- 現行NIST標準GCM, CCMはレート1/2: 1ブロック平文処理に2回のブロック暗号呼び出し必要
- **Gの導入によりブロック暗号ベース & Feedback型の構成でもレート1を達成**
  - 例: Gが単位行列のとき, 安全な認証暗号にならないことを示す
  - 暗号化方式 CFB (Ciphertext FeedBack) モード 的な方式: CFBはCPA安全なのでPRIVは大丈夫そう → AUTHは?
  - AUTHにおいて, 攻撃者はEncクエリで取得した暗号文/タグを利用してDecクエリできる
  - 図の様に(N, A, M)をクエリして(C, T)を受け取り, (N, A, C', T) s.t. $C'[1] \neq C[1]$, $C'[2] = C[2]$ をクエリすれば攻撃成功

- $Y[\cdot]$が未知のとき, 暗復の両方で **緑部分** を攻撃者が任意の値に操作できないことが必要

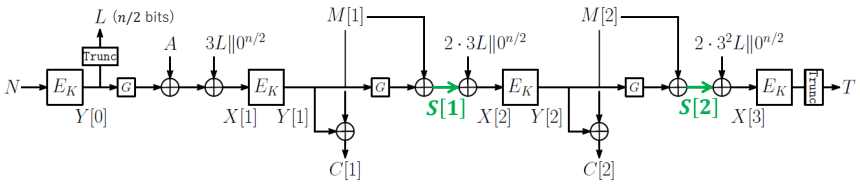


COFBの特徴

◆ **レート1**：1回のブロック暗号呼び出しで1ブロック平文処理が可能

- 現行NIST標準GCM, CCMはレート1/2: 1ブロック平文処理に2回のブロック暗号呼び出し必要
- **Gの導入によりブロック暗号ベース & Feedback型の構成でもレート1を達成**
  - 例: Gが単位行列のとき, 安全な認証暗号にならないことを示す
  - 暗号化方式 CFB (Ciphertext FeedBack) モード 的な方式: CFBはCPA安全なのでPRIVは大丈夫そう → AUTHは?
  - AUTHにおいて, 攻撃者はEncクエリで取得した暗号文/タグを利用してDecクエリできる
  - 図の様に(N, A, M)をクエリして(C, T)を受け取り, (N, A, C', T) s.t. $C'[1] \neq C[1]$, $C'[2] = C[2]$ をクエリすれば攻撃成功
- $Y[\cdot]$が未知のとき, 暗復の両方で　$S[\cdot]$　を攻撃者が任意の値に操作できないことが必要
  - 暗号化時: $S[\cdot] = G(Y[\cdot]) \oplus M[\cdot]$
  - 復号時　: $S[\cdot] = G(Y[\cdot]) \oplus Y[\cdot] \oplus C[\cdot] = (G \oplus I)(Y[\cdot]) \oplus C[\cdot]$

⇒ **G の条件が導出される**

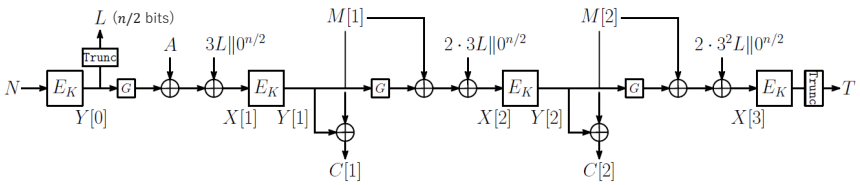


COFBの特徴

◆ **省ステートサイズ：鍵長 ビット $+ 1.5n$**

- ステートサイズ: 暗号方式を実装する際に必要なメモリサイズ
- $1.5n$ の内訳: ブロック暗号ステート n ビット + マスク $n/2$ ビット
- 一般にマスク値はブロック暗号の入出力サイズと同じ
- マスクの長さが$n/2$ビットであることが驚きの構成. これにより省ステートサイズを達成

◆ **安全性: PRIVは$n/2$ビット, AUTHは$n/2 - \log(n)$ビット安全性**



COFBへのPRIV攻撃

Akiko Inoue, Tetsu Iwata, Kazuhiko Minematsu:
Analyzing the Provable Security Bounds of GIFT-COFB and Photon-Beetle.
ACNS 2022: 67-84

COFBへの従来攻撃

- [Kha20a]：$L = 0^{n/2}$の時にに全てのマスクが $0^{n/2}$ になることを利用したAUTHへの攻撃
- [Kha20b]：異なる N における Lのコリジョンを利用したAUTHへの攻撃
- [Kha21]：L の値を推測してDecクエリを繰り返すAUTHへの攻撃
  - JoC版COFBの安全性バウンドと矛盾する攻撃. 安全性証明の誤りを示した
- [IM21]：ステート衝突を利用したAUTHへの攻撃

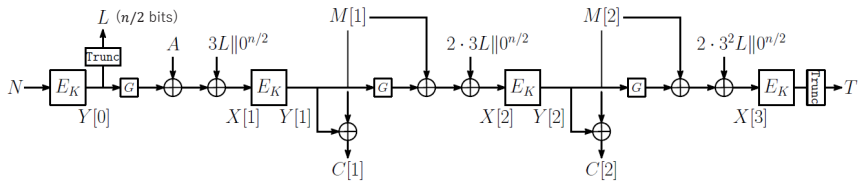
◆ これらの攻撃はいずれもNIST LwC版のCOFBで主張される安全性バウンドとは矛盾せず, 主張バウンドが (ほぼ) タイトであることを示す攻撃

◆ **本発表ではPRIVへの攻撃提案により, NIST LwC版COFBの主張バウンドに誤りがあることを証明する**

- **注: 安全性レベルを無効化するような攻撃ではない**

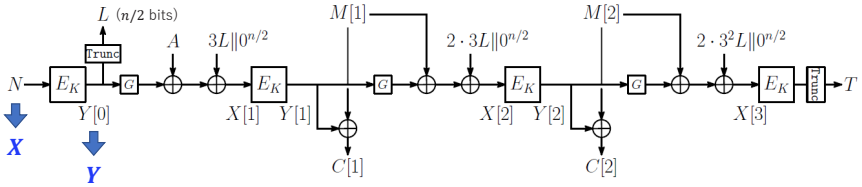
PRIVへの攻撃: アイディア

- 攻撃者は裸のブロック暗号の入出力が1つ得られれば即攻撃可能
  - 攻撃者が (X, Y) s.t. $E_K(X) = Y$ を入手したとする



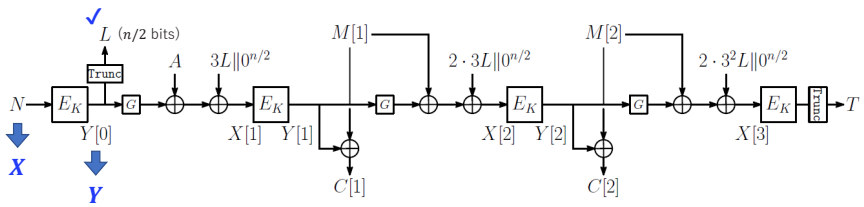
PRIVへの攻撃: アイディア

- 攻撃者は裸のブロック暗号の入出力が1つ得られれば即攻撃可能
  - 攻撃者が (X, Y) s.t. $E_K(X) = Y$ を入手したとする
  - 攻撃者はEncクエリで X をナンス N として使用可能 ⇒ $Y[0] = Y$ となる



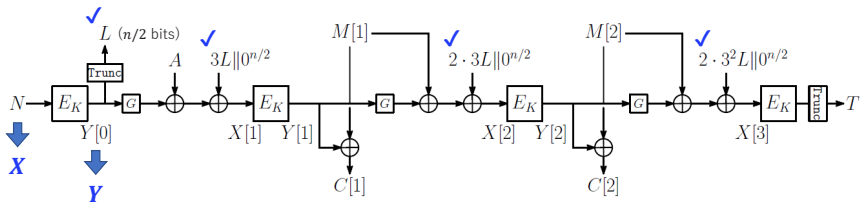
PRIVへの攻撃: アイディア

- 攻撃者は裸のブロック暗号の入出力が1つ得られれば即攻撃可能
  - 攻撃者が (X, Y) s.t. $E_K(X) = Y$ を入手したとする
  - 攻撃者はEncクエリで X をナンス N として使用可能 ⇒ $Y[0] = Y$ となる
  - **$L = \mathrm{msb}_{n/2}(Y)$ が既知**



PRIVへの攻撃: アイディア

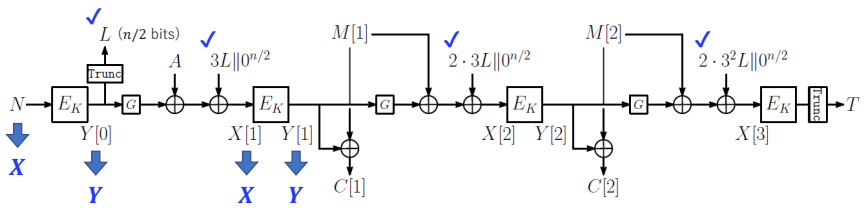
- 攻撃者は裸のブロック暗号の入出力が1つ得られれば即攻撃可能
  - 攻撃者が (X, Y) s.t. $E_K(X) = Y$ を入手したとする
  - 攻撃者はEncクエリで X をナンス N として使用可能 ⇒ $Y[0] = Y$ となる
  - **$L = \mathrm{msb}_{n/2}(Y)$ が既知 ⇒ 全てのマスク値が攻撃者にとって既知となる**



PRIVへの攻撃: アイディア

◆ 攻撃者は裸のブロック暗号の入出力が1つ得られれば即攻撃可能

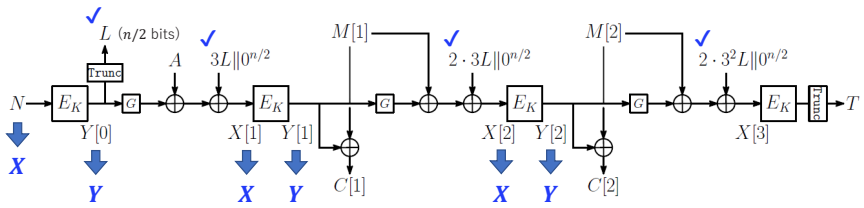
- 攻撃者が (X, Y) s.t. $E_K(X) = Y$ を入手したとする
- 攻撃者はEncクエリで X をナンス N として使用可能 ⇒ $Y[0] = Y$ となる
- **$L = \mathrm{msb}_{n/2}(Y)$ が既知 ⇒ 全てのマスク値が攻撃者にとって既知となる**
- 攻撃者は A を操作 $(A = X \oplus G(Y) \oplus 3L \,||\, 0^{n/2})$ し $X[1] = X$ 及び $Y[1] = Y$ となるようにできる



PRIVへの攻撃: アイディア

◆ 攻撃者は裸のブロック暗号の入出力が1つ得られれば即攻撃可能

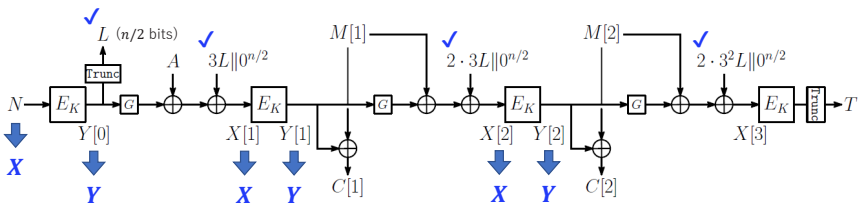
- 攻撃者が (X, Y) s.t. $E_K(X) = Y$ を入手したとする
- 攻撃者はEncクエリで X をナンス N として使用可能 ⇒ $Y[0] = Y$ となる
- **$L = \mathrm{msb}_{n/2}(Y)$ が既知 ⇒ 全てのマスク値が攻撃者にとって既知となる**
- 攻撃者は A を操作 $(A = X \oplus G(Y) \oplus 3L \,||\, 0^{n/2})$ し $X[1] = X$ 及び $Y[1] = Y$ となるようにできる



PRIVへの攻撃: アイディア

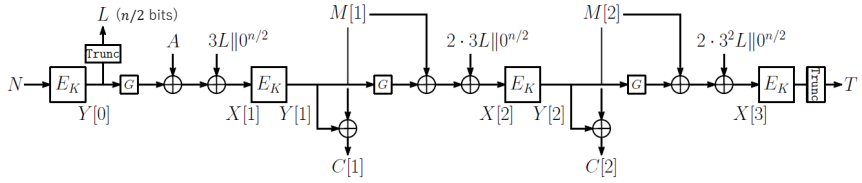
◆ 攻撃者は裸のブロック暗号の入出力が1つ得られれば即攻撃可能

- 攻撃者が (X, Y) s.t. $E_K(X) = Y$ を入手したとする
- 攻撃者はEncクエリで X をナンス N として使用可能 ⇒ $Y[0] = Y$ となる
- **$L = \mathrm{msb}_{n/2}(Y)$ が既知 ⇒ 全てのマスク値が攻撃者にとって既知となる**
- 攻撃者は A を操作 $(A = X \oplus G(Y) \oplus 3L \,||\, 0^{n/2})$ し $X[1] = X$ 及び $Y[1] = Y$ となるようにできる
- Real world: $C[1] = M[1] \oplus Y$, $C[2] = M[2] \oplus Y$ が確率1で得られる
- Ideal world: $C[1]$と$C[2]$ はランダム ⇒ 上記が起こる確率は $1/2^{2n}$



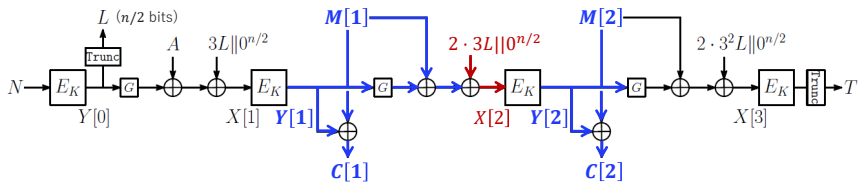
PRIVへの攻撃: 手順

- 任意の (N, A, M) s.t. $|A| = n$, $|M| = 2n$ をEncクエリして (C, T) をゲット



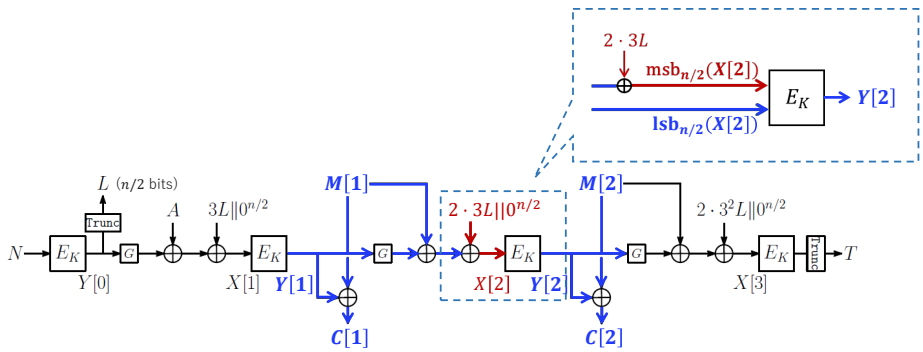
PRIVへの攻撃: 手順

- 任意の (N, A, M) s.t. $|A| = n$, $|M| = 2n$ をEncクエリして (C, T) をゲット
- 攻撃者は**青の値**を計算可能だが, **赤部分**は計算できない



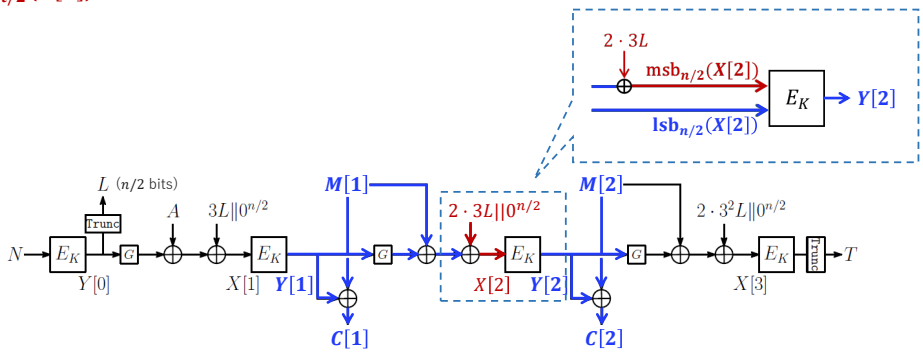
PRIVへの攻撃: 手順

- 任意の (N, A, M) s.t. $|A| = n$, $|M| = 2n$ をEncクエリして (C, T) をゲット
- 攻撃者は**青の値**を計算可能だが, **赤部分**は計算できない
- [ ] 部分に着目すると, $(X[2], Y[2])$ の中で攻撃者が未知の値は $\mathbf{msb}_{n/2}(X[2])$ だけ



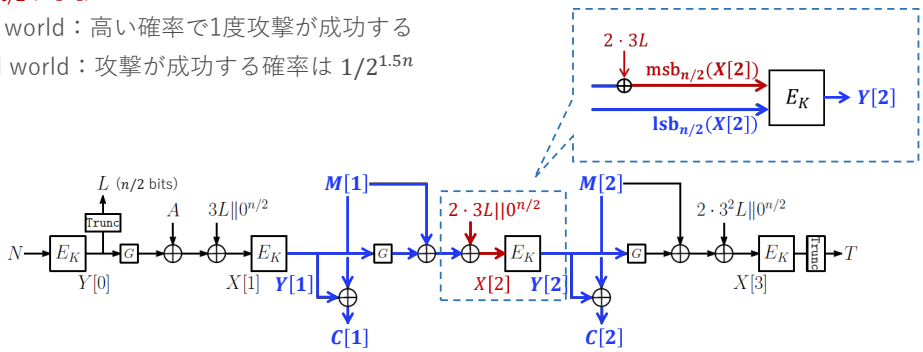
PRIVへの攻撃: 手順

- 任意の (N, A, M) s.t. $|A| = n$, $|M| = 2n$ をEncクエリして (C, T) をゲット
- 攻撃者は**青の値**を計算可能だが, **赤部分**は計算できない
- ⬚ 部分に着目すると, $(X[2], Y[2])$ の中で攻撃者が未知の値は $\mathbf{msb}_{n/2}(\boldsymbol{X[2]})$ だけ
- $\mathbf{msb}_{n/2}(\boldsymbol{X[2]})$ の取り得る値 $2^{n/2}$ 個を試して前スライドの攻撃が通るか確認する



PRIVへの攻撃: 手順

- 任意の (N, A, M) s.t. $|A| = n$, $|M| = 2n$ をEncクエリして (C, T) をゲット
- 攻撃者は**青の値**を計算可能だが, **赤部分**は計算できない
- ⬚ 部分に着目すると, $(X[2], Y[2])$ の中で攻撃者が未知の値は $\mathbf{msb}_{n/2}(\boldsymbol{X[2]})$ だけ
- $\mathbf{msb}_{n/2}(\boldsymbol{X[2]})$ の取り得る値 $2^{n/2}$ 個を試して前スライドの攻撃が通るか確認する
- Real world：高い確率で1度攻撃が成功する
- Ideal world：攻撃が成功する確率は $1/2^{1.5n}$



提案攻撃とClaimed Boundとの矛盾

- 提案攻撃の成功確率： $q_e/2^{n/2}$ （q_e：攻撃者によるEncクエリの回数）
  - COFBのPRIV安全性はn/2ビットだった: 一見矛盾なさそうだが…?

提案攻撃とClaimed Boundとの矛盾

- 提案攻撃の成功確率： $q_e/2^{n/2}$ （q_e：攻撃者によるEncクエリの回数）
  - COFBのPRIV安全性はn/2ビットだった: 一見矛盾なさそうだが…?
- Claimed Bound

$$\mathbf{Adv}^{\mathbf{ae}}_{\mathsf{GIFT\text{-}COFB}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathbf{prp}}_{\mathsf{GIFT}}(q', t') + \frac{\binom{q'}{2}}{2^n} + \frac{1}{2^{n/2}} + \frac{q_d(n+4)}{2^{n/2+1}} + \frac{3\sigma_e^2 + q_d + 2(q_e + \sigma_e + \sigma_d) \cdot \sigma_d}{2^n},$$

σ_e: Encクエリの総アクセスブロック数
q_d: Decクエリ数
σ_d: Decクエリの総アクセスブロック数
$q' = q_e + q_d + \sigma_e + \sigma_d$

提案攻撃とClaimed Boundとの矛盾

◆ 提案攻撃の成功確率： $q_e/2^{n/2}$　(q_e：攻撃者によるEncクエリの回数)

■ COFBのPRIV安全性はn/2ビットだった: 一見矛盾なさそうだが…?

◆ Claimed Bound

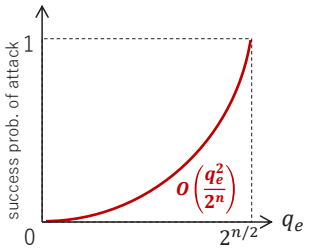
$$\mathbf{Adv}^{\mathrm{ae}}_{\text{GIFT-COFB}}(\mathcal{A}) \le \mathbf{Adv}^{\mathrm{prp}}_{\text{GIFT}}(q',t') + \frac{\binom{q'}{2}}{2^n} + \frac{1}{2^{n/2}} + \frac{q_d(n+4)}{2^{n/2+1}} + \frac{3\sigma_e^2 + q_d + 2(q_e+\sigma_e+\sigma_d)\cdot\sigma_d}{2^n},$$

σ_e: Encクエリの総アクセスブロック数
q_d: Decクエリ数
σ_d: Decクエリの総アクセスブロック数
$q' = q_e + q_d + \sigma_e + \sigma_d$

■ $\sigma_d = q_d = 0$, $\sigma_e \approx q_e$として簡略化:

$$\mathbf{Adv}^{\mathrm{ae}}_{\text{GIFT-COFB}}(\mathcal{A}) \le \mathbf{Adv}^{\mathrm{prp}}_{\text{GIFT}}(q',t') + \boldsymbol{O}\left(\frac{\boldsymbol{q_e^2}}{\boldsymbol{2^n}}\right)$$

■ COFBに対する（上記制約を満たす）任意の攻撃の成功確率は**赤**で抑えられる



提案攻撃とClaimed Boundとの矛盾

◆ 提案攻撃の成功確率： $q_e/2^{n/2}$　(q_e：攻撃者によるEncクエリの回数)

■ COFBのPRIV安全性はn/2ビットだった: 一見矛盾なさそうだが…?

◆ Claimed Bound

$$\mathbf{Adv}^{\mathrm{ae}}_{\text{GIFT-COFB}}(\mathcal{A}) \le \mathbf{Adv}^{\mathrm{prp}}_{\text{GIFT}}(q',t') + \frac{\binom{q'}{2}}{2^n} + \frac{1}{2^{n/2}} + \frac{q_d(n+4)}{2^{n/2+1}} + \frac{3\sigma_e^2 + q_d + 2(q_e+\sigma_e+\sigma_d)\cdot\sigma_d}{2^n},$$

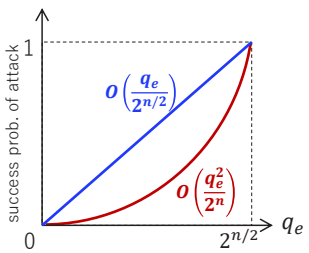
σ_e: Encクエリの総アクセスブロック数
q_d: Decクエリ数
σ_d: Decクエリの総アクセスブロック数
$q' = q_e + q_d + \sigma_e + \sigma_d$

■ $\sigma_d = q_d = 0$, $\sigma_e \approx q_e$として簡略化:

$$\mathbf{Adv}^{\mathrm{ae}}_{\text{GIFT-COFB}}(\mathcal{A}) \le \mathbf{Adv}^{\mathrm{prp}}_{\text{GIFT}}(q',t') + \boldsymbol{O}\left(\frac{\boldsymbol{q_e^2}}{\boldsymbol{2^n}}\right)$$

■ COFBに対する（上記制約を満たす）任意の攻撃の成功確率は**赤**で抑えられる

■ **しかし $0 < q_e < 2^{n/2}$のとき, $q_e/2^{n/2} > q_e^2/2^n$ ⇒ 矛盾**



攻撃による影響

- 主張されている安全性バウンドが正しくない ⇒ 安全性証明を修正する必要
  - $O(q_e^2/2^n)$ ≈ nビットの乱数がq_e個あるとき, 少なくともこのうち1ペアで衝突が起こる確率
    - 誕生日のパラドックスに因んでバースデーバウンドと呼ばれる. モードの安全性バウンドでは頻出
  - 従来の安全性証明ではステートnビットの衝突は考慮できていたが, 今回の攻撃のような q_e に対して線形に成功確率が上がっていくケースを考慮できていなかったのが原因
  - 攻撃提案後, 誤りが修正された安全性バウンドがアップされた

$$\mathbf{Adv}^{\mathrm{AE}}_{\mathsf{COFB}}((q,q_f),(\sigma,\sigma_f),t) \le \mathbf{Adv}^{\mathrm{prp}}_{\mathsf{GIFT}}(q',t') + \frac{\binom{q'}{2}}{2^n} + \frac{\sigma+1}{2^{n/2}} + \frac{q_f(n+4)}{2^{n/2+1}} + \frac{3\sigma^2+q_f+2(q+\sigma+\sigma_f)\cdot\sigma_f}{2^n}$$

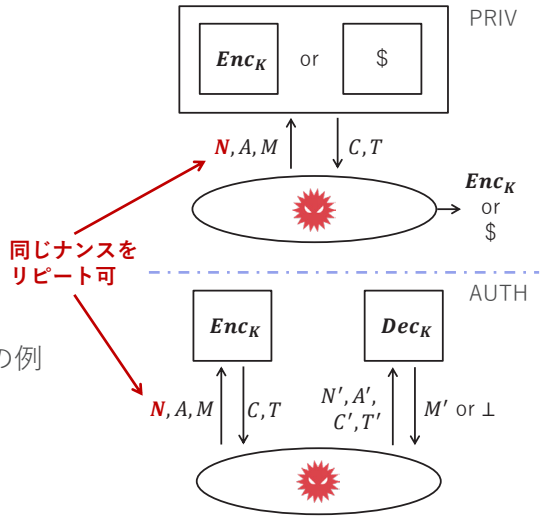
σ: Encクエリの総アクセスブロック数

- COFB全3バージョンのうち, 今回の攻撃はNIST LwC版のみに適用可能
  - 他バージョンはナンスが64ビットのため, 今回のような攻撃は不可能
  - 他バージョンでは $O(q_e/2^{n/2})$ の項が含まれている

従来の安全性を超えた安全性要件: ナンス誤用

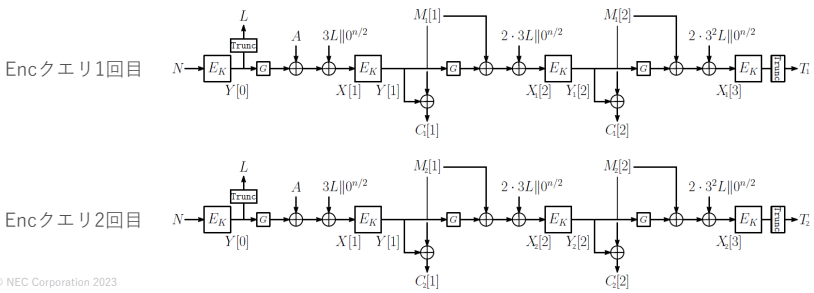
ナンス誤用設定

- PRIV, AUTHはEncクエリで
  Nonce respectingである必要があった
- 実装のミス等で同じナンスを誤って
  用いることがあり得る
  → ナンス誤用しても安全な方式への需要
- Nonce misuse **resistance** [RS06]
  - 従来のPRIV, AUTHの定義から
    Nonce respectingを取り去る
- Nonce misuse resistant でない認証暗号の例
  - GCM: ナンス誤用のクエリ2回で, 攻撃者は
    タグ生成に用いる鍵を求められる
  - COFB: PRIV, AUTH共にO(1)で攻撃可能



COFBのNonce misuse resistance

- $O(1)$でPRIV攻撃可能
  - 同じナンスとAD, 異なる平文で2回Encクエリ
    - 任意の (N, A, M_1) s.t. $|A| = n$, $|M_1| = 2n$ をEncクエリ → (C_1, T_1) をゲット
    - 任意の (N, A, M_2) s.t. $|M_2| = 2n$, $M_2[1] \neq M_1[1]$ をEncクエリ → (C_2, T_2) をゲット



COFBのNonce misuse resistance

◆ $O(1)$でPRIV攻撃可能

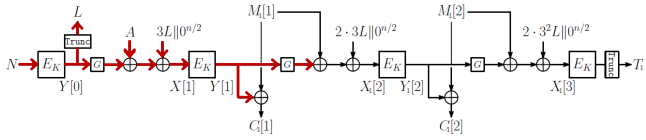
■ 同じナンスとAD, 異なる平文で2回Encクエリ

- 任意の (N, A, M_1) s.t. $|A| = n$, $|M_1| = 2n$ をEncクエリ → (C_1, T_1) をゲット
- 任意の (N, A, M_2) s.t. $|M_2| = 2n$, $M_2[1] \neq M_1[1]$ をEncクエリ → (C_2, T_2) をゲット

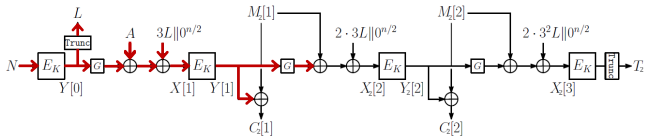
■ **赤部分**, 特に $\boldsymbol{Y[1]}$ までは2回のEncクエリで同じ値であることを利用して判別

- $M_1[1] \oplus C_1[1]$, $M_2[1] \oplus C_2[1]$ を計算し, $Y[1]$の値が衝突するかチェック
- Realでは確率1で衝突するが, Idealでは高い確率で衝突しない

Encクエリ1回目



Encクエリ2回目



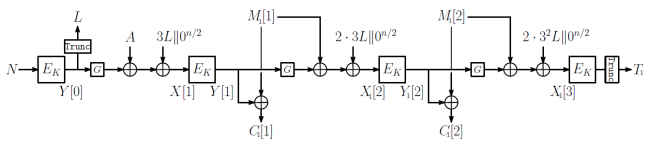
COFBのNonce misuse resistance

◆ $O(1)$でAUTH攻撃可能

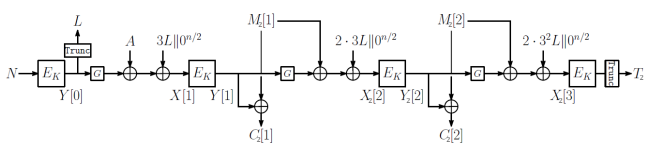
■ 同じナンスとAD, 異なる平文で2回Encクエリ

- 任意の (N, A, M_1) s.t. $|A| = n$, $|M_1| = 2n$ をEncクエリ → (C_1, T_1) をゲット
- 任意の (N, A, M_2) s.t. $|M_2| = 2n$, $M_2[1] \neq M_1[1]$ をEncクエリ → (C_2, T_2) をゲット

Encクエリ1回目



Encクエリ2回目



COFBのNonce misuse resistance

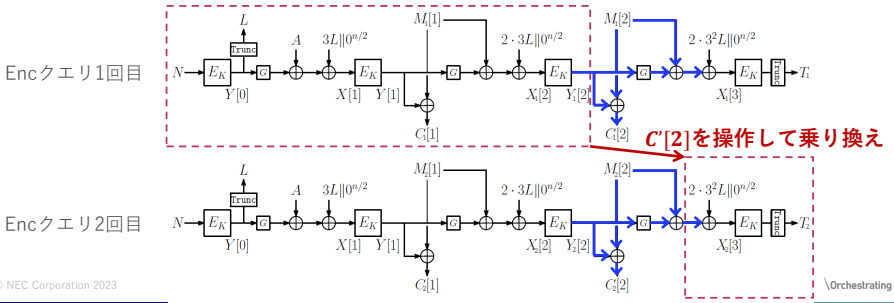
◆ $O(1)$でAUTH攻撃可能

■ 同じナンスとAD, 異なる平文で2回Encクエリ

- 任意の (N, A, M_1) s.t. $|A| = n$, $|M_1| = 2n$ をEncクエリ → (C_1, T_1) をゲット
- 任意の (N, A, M_2) s.t. $|M_2| = 2n$, $M_2[1] \neq M_1[1]$ をEncクエリ → (C_2, T_2) をゲット

■ 攻撃者は **青部分** を計算可能. 2つのEncクエリを「**乗り換える**」ような以下のDecクエリが可能

- (N', A', C', T') s.t. $N' = N$, $A' = A$, $C' = C_1[1] \,||\, C'[2]$, $C'[2] = G(Y_1[2]) \oplus Y_1[2] \oplus G(Y_2[2]) \oplus Y_2[2] \oplus C_2[2]$, $T' = T_2$
- これは非自明な復号関数入力の偽造で, 十分高い確率で受理される



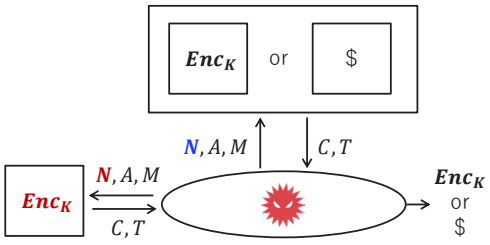
“Resistance” から “Resilience” への緩和

◆ 現状, Nonce misuse resistanceを持つ認証暗号はレート1/2以下 → 非効率☹

◆ Nonce misuse **resistance** より弱い耐ナンス誤用安全性の提案:
Nonce misuse **resilience** (**NMRL**) [ADL17]

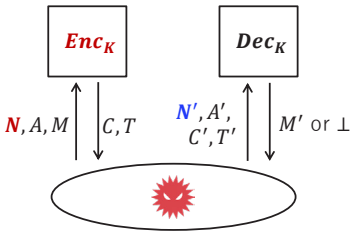
■ NMRL-PRIV

- 攻撃者はナンス誤用OKな$\boldsymbol{Enc_K}$にクエリ可能
- **ナンス誤用しないEncクエリ**によって,
$\boldsymbol{Enc_K}$と$を判別できる確率で評価
- $\boldsymbol{Enc_K}$と$\boldsymbol{Enc_K}$ / $ で同一のナンスはクエリ禁止



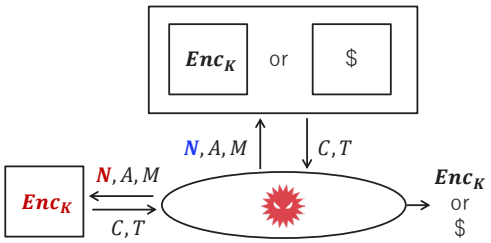
■ NMRL-AUTH

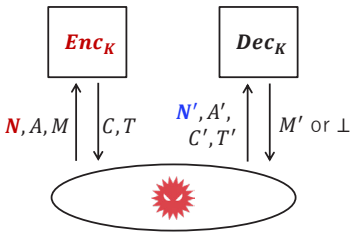
- 攻撃者はナンス誤用OKな$\boldsymbol{Enc_K}$にクエリ可能
- その下で$\boldsymbol{Dec_K}$から⊥以外を受け取る確率で評価
- Decクエリでは**誤用していないナンス**のみ使用可能



Nonce misuse resilience

- NMRLを持つ認証暗号 = ナンスを誤用しても, 誤用していないナンスを使うクエリに関しては安全性を担保可能
  - GCMのNMRL-AUTHの例: ナンス誤用のクエリ2回でタグ生成に用いる鍵が漏洩
    - → 誤用していないナンスのクエリにも攻撃可能
    - → GCM は Nonce misuse resilience でない
- **COFB: NMRL-PRIV, AUTH共に $O(2^{n/4})$の安全性が証明できる**
  - 安全性は低いが一定のレベルが証明できることを示した





41

COFBのNonce misuse resilience証明

Akiko Inoue, Chun Guo, Kazuhiko Minematsu:
Nonce-misuse resilience of Romulus-N and GIFT-COFB.
IET Inf. Secur. 17(3): 468-484 (2023)

\Orchestrating a brighter world NEC

準備: TBCの安全性 [LRW02]

◆ 理想状態「Tweakable Uniform Random Permutation」 との判別確率で定義

■ **(n, tw)-Tweakable permutation:**
$\tilde{P}: \{0,1\}^{tw} \times \{0,1\}^n \to \{0,1\}^n$ が Tweakable permutation とは,
任意のTweak $Tw \in \{0,1\}^{tw}$ に対して $\tilde{P}(Tw,\cdot)$ が $\{0,1\}^n$ 上の置換となる関数

■ **TPerm(n, tw):**
入出力nビット, Tweak twビットのTweakable permutation全体の集合

■ **(n, tw)-Tweakable Uniform Random Permutation (TURP):**
TPerm(n, tw) から一様ランダムに選ばれた (n, tw)-Tweakable permutation

■ **TBCのTweakable Pseudo Random Permutation安全性 (TPRP安全性):**
攻撃者がEncクエリとして**任意の平文とTweak**をクエリできるときのTURPとの判別困難確率

準備: モードによるTBCの構成方法

◆ ブロック暗号の入力 / 入出力にマスク値を足すことで安全なTBCが構成できる

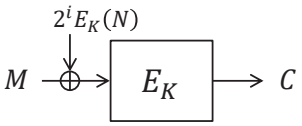
◆ 安全性はブロック暗号の入出力の衝突確率によって評価できる

■ XE [Rog04] の例: $\tilde{E}_K^{N,i}(M) = E_K\left(M \oplus 2^i E_K(N)\right)$ $(i \in \{1,2,\dots\})$

■ 同一のN, 異なるiでのブロック暗号入力衝突を見つける
- 攻撃者は C の衝突により入力衝突を検出できる

■ $M \oplus 2^i E_K(N) = M' \oplus 2^{i'} E_K(N)$ より $E_K(N)$ の値を求めることで,
他のTweakに対する出力結果をクエリなしで予測可能
となり, TURPとの判別が可能になる

■ 安全性はブロック暗号の入出力長の半分 (**バースデーバウンド**)



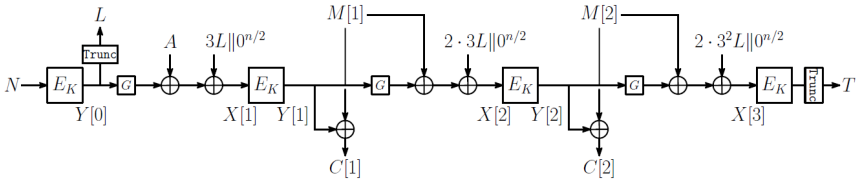
◆ マスクの長さがnビット未満の場合

■ 攻撃者はマスクが足されていない部分を確率1で衝突させるようにクエリができる

■ **安全性はマスク値の長さの半分**となる

COFBのNonce misuse resilience

◆ 証明概要: Hybrid argument を用いる

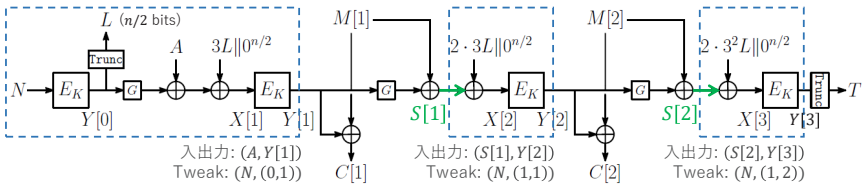


COFBのNonce misuse resilience

◆ 証明概要: Hybrid argument を用いる

■ [ ] 部分をTBCと見なす

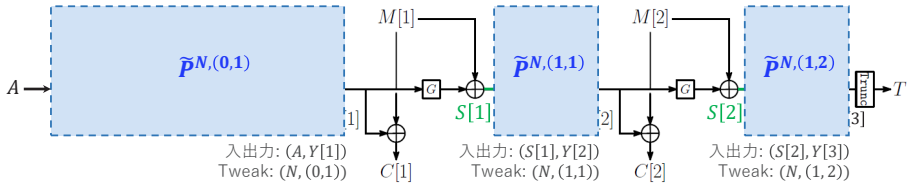
• マスク値がn/2ビットなのでn/4ビット安全性のTBCとなる



COFBのNonce misuse resilience

◆ 証明概要: Hybrid argument を用いる

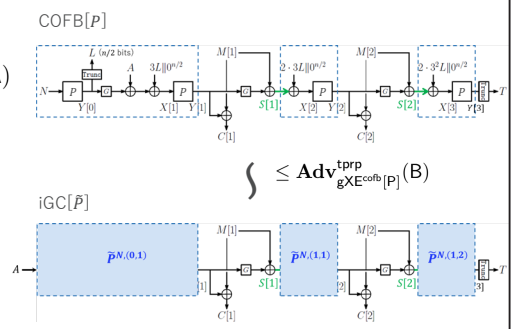
- ■ [ ] 部分をTBCと見なす
  - マスク値がn/2ビットなのでn/4ビット安全性のTBCとなる
- ■ [ ] 部分をTURPで置き換えて得られる認証暗号のNonce misuse resilienceを証明
  - PRIVはperfect security, AUTHはnビット安全性が 証明できる
  - TURPにより, Tweakを変える度に一様ランダムに置換が選ばれる ＝ Tweakが異なるクエリの情報は攻撃には寄与しない ことが担保されているため, 証明は比較的煩雑になりにくい
- ■ 全体としてn/4ビット安全性が証明できる



COFBのNonce misuse resilience

◆ つまり以下が成立

- ■ $\mathbf{Adv}^{\text{nmrl-priv}}_{\text{GIFT-COFB[P]}}(A) \le \mathbf{Adv}^{\text{tprp}}_{\mathbf{gXE}^{\mathbf{cofb}}\text{[P]}}(B) + \mathbf{Adv}^{\text{nmrl-priv}}_{\mathbf{iGC}[\widetilde{P}]}(A)$
  - 左辺: COFBのNMRL-PRIV安全性
  - 右辺第一項: TBC **gXE$^{\text{cofb}}$** ([ ] 部分) のTPRP安全性
  - 右辺第二項: **gXE$^{\text{cofb}}$** をTURPに置き換えて得られる認証暗号 **iGC** のNMRL-PRIV安全性
  - NMRL-AUTHでも同様
- ■ COFBとiGCの判別確率をgXE$^{\text{cofb}}$の安全性で上界している



◆ Hybrid argumentを用いる上での注意点

- ■ NMRL-PRIVゲームの攻撃者Aが, TPRPゲームの攻撃者Bでシミュレートできる必要がある
- ■ **TPRPゲームでは攻撃者のTweakリピートに関する制約はない**
- ■ **Aのゲームがナンス誤用を含んでいてもBでシミュレートができるため, Hybrid argument が使える**

COFBのNonce misuse resilience: まとめと課題

- **NMRL-PRIV, AUTH共に $O(2^{n/4})$の安全性を持つことを証明した**
  - $n/2$ビットマスクを持つTBCを使ってHybrid argumentを用いた
- 課題: 示したバウンドがタイトかどうかはオープン
  - 計算量$O(2^{n/4})$の攻撃は示せていない
  - 上記のような攻撃ができてタイトであることが証明できるかもしれないし,
    更によいNonce misuse resilienceバウンドが証明できるかもしれない
  - 後者なら今回のようなHybrid argumentを使えないはずなので,
    恐らく証明は煩雑なものになるのでは

従来の安全性を超えた安全性要件: その他

RUP (Release of Unverified Plaintext) [ABL+14]

◆ 攻撃者が未検証平文にアクセスできる設定での安全性

■ 通常の認証暗号では, 復号関数で改ざんが検知された場合の出力は単一のエラー

• 改ざんが検知された時の復号平文は攻撃者は取得できない設定

■ メモリ制約のある実行環境では未検証平文全体の格納は困難 ⇒ RUP設定下での安全性の需要

◆ RUP設定下のAUTH: INT-RUP (Integrity under RUP)

■ 認証暗号の関数を定義しなおす

• 暗号化関数: $Enc_K(N, A, M) = (C, T)$

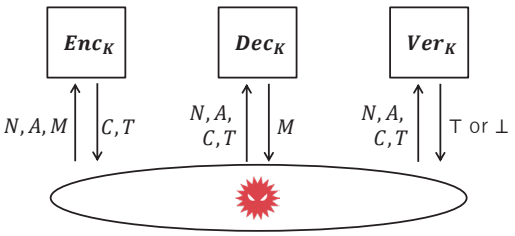
• 復号関数: $Dec_K(N, A, C, T) = M$ （検証なしに復号結果を出力）

• 検証関数: $Ver_K(N, A, C, T) = \begin{cases} \top & \text{(改ざんが検知されない場合)} \\ \bot & \text{(改ざんが検知された場合)} \end{cases}$

■ Enc, Dec, Verクエリできる攻撃者が Ver_K から ⊤ を受け取る確率で評価

■ Encクエリではnonce respecting

■ Dec, Verクエリではナンス制限なし



COFBの場合

◆ Nonce misuse resistanceでの攻撃がほぼそのままINT-RUPへの攻撃となる

■ INT-RUPでのDecクエリにナンス制限はないため, Nonce misuse resistanceでの攻撃におけるナンス誤用Encクエリを, INT-RUPゲームのDecクエリで再現できればOK

• Encクエリ1回, Decクエリ1回, もしくは Decクエリ2回 でナンス誤用クエリを再現する

• 右のDecクエリと同じVerクエリにより, 高い確率でTが取得可能

COFBのNonce misuse resistance

◆ $O(1)$でAUTH攻撃可能

■ 同じナンスとAD, 異なる平文で2回Encクエリ

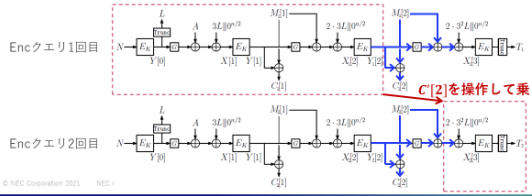
• 任意の (N, A, M_1) s.t. $|A| = n, |M_1| = 2n$ をEncクエリ → (C_1, T_1) をゲット

• 任意の (N, A, M_2) s.t. $|M_2| = 2n, M_2[1] \neq M_1[1]$ をEncクエリ → (C_2, T_2) をゲット

■ 攻撃者は **青部分** を計算可能. 2つのEncクエリを「**乗り換える**」ような以下のDecクエリが可能

• (N', A', C', T') s.t. $N' = N, A' = A, C' = C_1[1] \,||\, C'[2], C'[2] = G(Y_1[2]) \oplus Y_1[2] \oplus G(Y_2[2]) \oplus Y_2[2] \oplus C_2[2], T' = T_2$

• これは非自明な復号関数入力の偽造で, 十分高い確率で受理される



従来の安全性を超えた安全性要件: その他

- Leakage resilient security
  - サイドチャネル情報等, 攻撃者がブラックボックス以上の情報を取得することができる場合でも安全性を担保できる
    - 通常の認証暗号に対してマスキング等を施すことでも達成できるが, 非効率になり得る
    - モードでも何らかの仮定を置いて, 漏洩情報ありver. PRIV/AUTHを持った, より効率的な認証暗号を構成できないか？
  - 安全性定義は複数存在する
    - 漏洩ありオラクルアクセスにおけるLeft-or-Right判別ゲーム
    - 漏洩ありオラクルアクセスが可能な攻撃者の漏洩なしオラクルReal-or-Ideal判別ゲーム
- Key committing security
  - 攻撃者が秘密鍵を含めて入力を選択できるとき, $Enc_K(N, A, M) = Enc_{K'}(N', A', M') = (C, T)$ なる相異なるEnc入力2つを見つけることが困難 という安全性
    - 暗号化関数の出力 (暗号文, タグ) の衝突困難性
  - Message FrankingといったEnd-to-Endプロトコルで必要であることから近年注目されつつある
    - E2Eプロトコルにおいて Key committing securityがない認証暗号を用いた場合, 悪意のあるメッセージを受け取ったときの通報機能が機能しなくなる恐れがある

本発表のまとめ

- 認証暗号の基本的な安全性と拡張された安全性について紹介した
  - 秘匿 (PRIV), 改ざん検知 (AUTH)
  - Nonce misuse resistance/resilience
  - INT-RUP, Leakage resilience, Key committing security
- COFB
  - NIST LwC版に対して主張された安全性バウンドを破る攻撃を紹介
  - Nonce misuse resilience について$O(2^{n/4})$の安全性が示せることを証明

参考文献

- [Rog02]: Rogaway, P.: Authenticated-encryption with associated-data. CCS 2002
- [BN00]: Bellare, M., Namprempre, C.: Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. ASIACRYPT 2000
- [BCI+21]: Banik, S., Chakraborti, A., Iwata, T., Minematsu, K., Nandi, M., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: GIFT-COFB v1.1. Submission to the NIST Lightweight Cryptography project (2021)
- [BPP+17]: Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: GIFT: A small present - towards reaching the limit of lightweight encryption. CHES 2017
- [CIMN17]: Chakraborti, A., Iwata, T., Minematsu, K., Nandi, M.: Blockcipher-based authenticated encryption: How small can we go? CHES 2017.
- [CIMN20]: Chakraborty, A., Iwata, T., Minematsu, K., Nandi, M.: Blockcipher-based authenticated encryption: How small can we go? Journal of Cryptology 33(3), 703–741 (Jul 2020).
- [Kha20a]: Khairallah, M.: Weak keys in the rekeying paradigm: Application to COMET and mixFeed. IACR Trans. Symm. Cryptol. 2019(4), 272–289 (2019).
- [Kha20b]: Khairallah, M.: Observations on the tightness of the security bounds of GIFT-COFB and HyENA. Cryptology ePrint Archive, Report 2020/1463 (2020).
- [Kha21]: Khairallah, M.: Security of COFB against Chosen Ciphertext Attacks. IACR Trans. Symm. Cryptol. 2022(1), 138–157 (2022).

参考文献

- [IM21]: Inoue, A., Minematsu, K.: GIFT-COFB is tightly birthday secure with encryption queries. Cryptology ePrint Archive, Report 2021/737 (2021).
- [RS06]: Rogaway, P., Shrimpton, T.: A provable-security treatment of the key-wrap problem. EUROCRYPT 2006.
- [ADL17]: Ashur, T., Dunkelman, O., Luykx, A.: Boosting authenticated encryption robustness with minimal modifications. CRYPTO 2017
- [LRW02]: Liskov, M., Rivest, R.L., Wagner, D.A.: Tweakable Block Ciphers. CRYPTO 2002
- [Rog04]: Rogaway, P.: Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. ASIACRYPT 2004
- [ABL+14]: E. Andreeva, A. Bogdanov, A. Luykx, B. Mennink, N. Mouha, and K. Yasuda. How to Securely Release Unverified Plaintext in Authenticated Encryption. ASIACRYPT 2014

キャッシュランダム化関数の安全性モデルとSCARFの設計・安全性評価

藤堂 洋介
NTT 社会情報研究所
yosuke.todo@ntt.com

キャッシュ攻撃とはキャッシュとメモリの遅延差を利用したサイドチャネル攻撃である [1, 2]。キャッシュ攻撃を防ぐ方法としてキャッシュランダム化が注目されている [3, 4, 5, 6, 7, 8, 9, 10]。Usenix Security2023 で、キャッシュランダム化関数の安全性モデル、調整可能暗号を用いた設計理論、具体的な関数 SCARF を設計・発表した [11]。本講演では、この安全性モデルの解説、実際の SCARF の設計プロセス、SCARF に対する具体的な暗号解読の取り組みを紹介する。

References

[1] Daniel J Bernstein. Cache-timing attacks on AES. 2005.
[2] Dag Arne Osvik, Adi Shamir, and Eran Tromer. Cache attacks and Countermeasures: The Case of AES. IACR Cryptol. ePrint Arch., page 271, 2005.
[3] Moinuddin K. Qureshi. CEASER: Mitigating Conflict-Based Cache Attacks via Encrypted-Address and Remapping. In 51st Annual IEEE/ACM International Symposium on Microarchitecture, MICRO 2018, Fukuoka, Japan, October 20-24, 2018, pages 775–787. IEEE Computer Society, 2018.
[4] Moinuddin K. Qureshi. New attacks and defense for encrypted-address cache. In Srilatha Bobbie Manne, Hillery C. Hunter, and Erik R. Altman, editors, Proceedings of the 46th International Symposium on Computer Architecture, ISCA 2019, Phoenix, AZ, USA, June 22-26, 2019, pages 360–371. ACM, 2019
[5] Gururaj Saileshwar and Moinuddin K. Qureshi. MIRAGE: Mitigating Conflict-Based Cache Attacks with a Practical Fully-Associative Design. In Michael Bailey and Rachel Greenstadt, editors, 30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021, pages 1379–1396. USENIX Association, 2021.
[6] Wei Song, Boya Li, Zihan Xue, Zhenzhen Li, Wenhao Wang, and Peng Liu. Randomized Last-Level Caches Are Still Vulnerable to Cache Side-Channel Attacks! But We Can Fix It. In 42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021, pages 955–969. IEEE, 2021.
[7] Qinhan Tan, Zhihua Zeng, Kai Bu, and Kui Ren. PhantomCache: Obfuscating Cache Conflicts with Localized Randomization. In 28th Annual Network and Distributed System Security Symposium, NDSS 2021, virtually, February 21-25, 2021. The Internet Society, 2021.
[8] Jan Philipp Thoma, Christian Niesler, Dominic A. Funke, Gregor Leander, Pierre Mayr, Nils Pohl, Lucas Davi, and Tim Güneysu. ClepsydraCache - Preventing Cache Attacks with Time-Based Evictions. CoRR, abs/2104.11469, 2021.
[9] Zhenghong Wang and Ruby B. Lee. New cache designs for thwarting software cache-based side channel attacks. In Dean M. Tullsen and Brad Calder, editors, 34th International Symposium on Computer Architecture (ISCA 2007), June 9-13, 2007, San Diego, California, USA, pages 494–505. ACM, 2007.
[10] Mario Werner, Thomas Unterluggauer, Lukas Giner, Michael Schwarz, Daniel Gruss, and Stefan Mangard. ScatterCache: Thwarting Cache Attacks via Cache Set Randomization. In Nadia Heninger and Patrick Traynor, editors, 28th USENIX Security Symposium, USENIX Security 2019, Santa Clara, CA, USA, August 14-16, 2019, pages 675–692. USENIX Association, 2019.
[11] Federico Canale, Tim Güneysu, Gregor Leander, Jan Philipp Thoma, Yosuke Todo, and Rei Ueno, SCARF – A Low-Latency Block Cipher for Secure Cache-Randomization.. USENIX Security 2023.

NTT

キャッシュランダム化関数の安全性モデルとSCARFの設計・安全性評価

NTT社会情報研究所

藤堂　洋介

アジェンダ

NTT

- 今日の概要
- キャッシュ攻撃
  - キャッシュ攻撃とその脅威
  - キャッシュランダム化とその効果
- キャッシュランダム化関数の安全性モデル
  - どのような関数が求められるのか
  - 攻撃者モデル
    - 衝突モデル
    - Enc-then-Decモデル
- SCARFの設計と安全性評価
  - 設計技術の概要紹介
  - 暗号解析結果の紹介

[機密性1/Confidentiality1]

一応、自己紹介

NTT

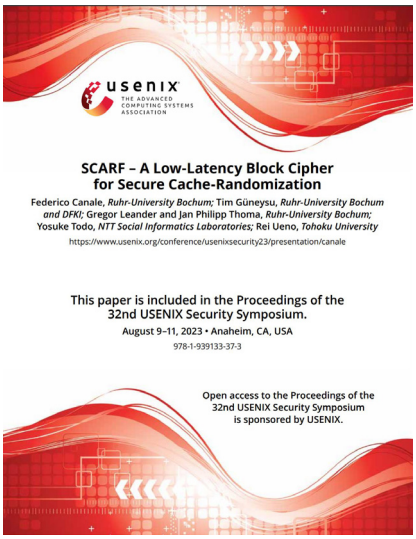
- 藤堂 洋介 (Yosuke Todo)
  - NTT社会情報研究所
  - 略歴
    - 2012.3 神戸大学 修士
    - 2012.4 NTT入社
    - 2017.3 神戸大学 博士(工学)
    - 2019.7 RUB(独)客員研究員(2020.10まで)
  - 最近の研究テーマ
    - 共通鍵暗号プリミティブの安全性評価理論
    - **目的特化型の共通鍵暗号の設計**

[機密性1/Confidentiality1]

今日の概要

NTT

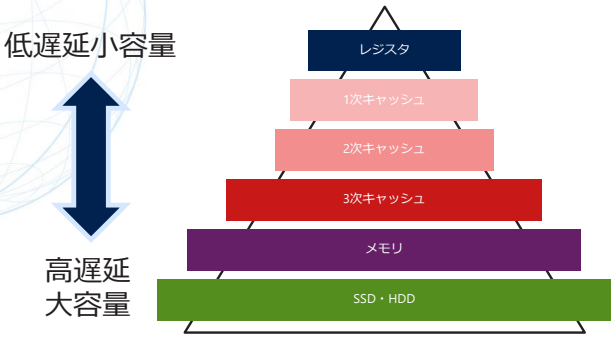
- Usenix Security 2023で発表した
  SCARF – A Low-Latency Block Cipher for Secure Cache-Randomization
  の解説をします。
- 本研究は、
  RUBのFederico, Tim, Gregor, Jan
  東北大の上野先生
  との共同研究です。



[機密性1/Confidentiality1]

キャッシュメモリ

NTT



毎回メモリにアクセスしていては遅延が大きくCPUの性能が上がらない。
メモリと演算機の間にキャッシュを導入することで、性能の底上げを図る。
今ではキャッシュメモリも階層化（１次、２次、３次キャッシュ）されている。

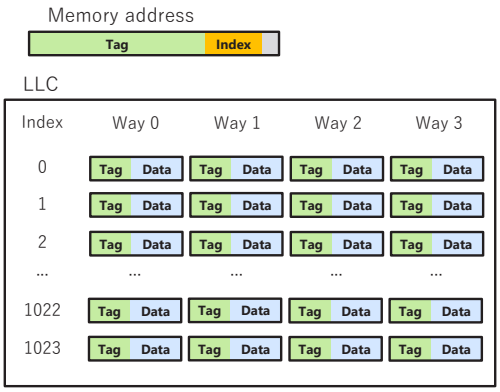
5

[機密性1/Confidentiality1]

Set-associative キャッシュ

NTT

- 現代のキャッシュシステムのほとんどは Set-associative※
  - キャッシュインデックスは複数の Way を持つ
  - 同じインデックスを持つデータは同じ行（キャッシュセット）に格納
  - 同じインデックスのデータがWayの数以上にロードされるとデータがキャッシュから追い出される



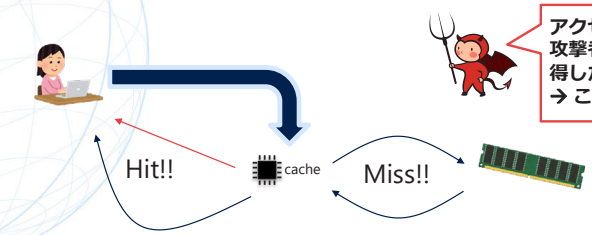
※ Wayの数が1つだとDirect map
Index（キャッシュセット）の数が1つだとFull-associativeと呼ばれる
Set-associativeはこの中間の構成を指す.

6

[機密性1/Confidentiality1]

キャッシュ攻撃

NTT



アクセス遅延差を計測
攻撃者は攻撃対象がキャッシュ内のデータを取得したか否かを判定できる。
→ この特徴を利用して脆弱性を引き起こす。

キャッシュ攻撃と関連した脆弱性

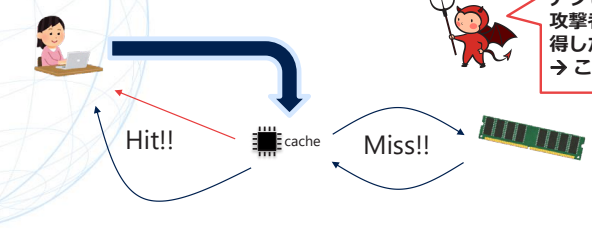
- 暗号実装に対する鍵回復攻撃
  - 例えばAESのソフト実装に対するキャッシュ攻撃
  - どのS-boxの値を使ったのかが漏洩し、そこから鍵回復攻撃につなげられるリスク
- 投機的実行処理との組み合わせ(Spectre, Meltdown, Downfallなど)
  - 最近のCPUは先読み(投機的実行)処理を行い、無駄になるかもしれない計算をCPUが勝手に実行
  - 無駄になれば、当然、そのデータは外部に出さない・・・しかしキャッシュには残ってしまう・・・
  - 投機的実行処理と組み合わせ、本来漏れてはいけない情報を奪い取る。

7

[機密性1/Confidentiality1]

キャッシュ攻撃の種類

NTT



アクセス遅延差を計測
攻撃者は攻撃対象がキャッシュ内のデータを取得したか否かを判定できる。
→ この特徴を利用して脆弱性を引き起こす。

キャッシュ攻撃とはメモリアクセスとキャッシュアクセスの遅延差を利用した攻撃

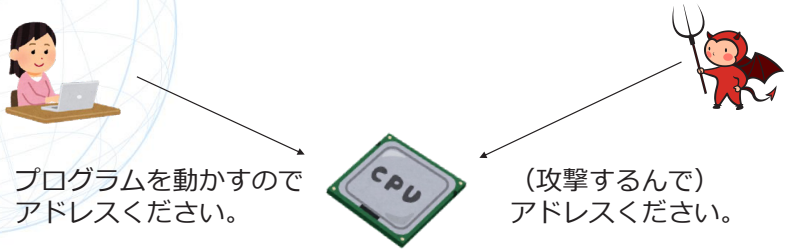
- Flush型キャッシュ攻撃
  - Flush+Reload型キャッシュ攻撃など
  - 現実環境としては、かなりキツい前提条件が成り立つ必要があるが、それが成り立つなら効率的。
- 競合型キャッシュ攻撃
  - Prime+Probe型キャッシュ攻撃など
  - Flush型のような前提条件を必要とせず、どこでも実行可能。
    Flush型が動くなら、そっちの方が精度が良い。

8

[機密性1/Confidentiality1]

Flush型キャッシュ攻撃

NTT



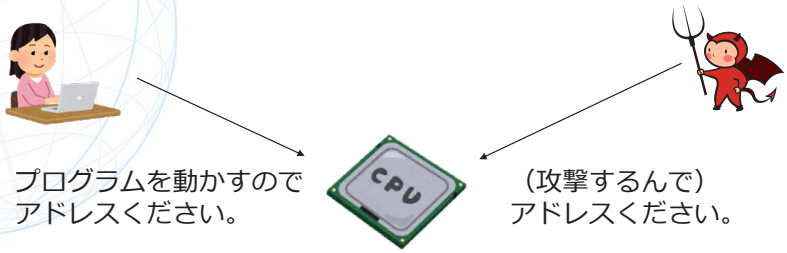
- 攻撃者とVictimが**同一のアドレス空間**を触れる状況を前提
- 普通は、なかなか成立しない
  - 無理やりVictimのアドレスを触れば落ちる
- 一部、VMなどの環境では現実で起こりえる
- Flush型が動くならキャッシュ攻撃は結構簡単で精度も良い

9

[機密性1/Confidentiality1]

競合型キャッシュ攻撃

NTT



- 攻撃者とVictimが**別のアドレス空間**を割り当てられる。
  - 自然な設定
- アドレス空間は異なっていてもキャッシュ空間は共有。
- キャッシュ空間の取り合い(競合)に基づくキャッシュ攻撃。
- 攻撃の仮定が少なく基本、どのような環境でも動く。
  - ただし精度はFlush型ほどよくない。

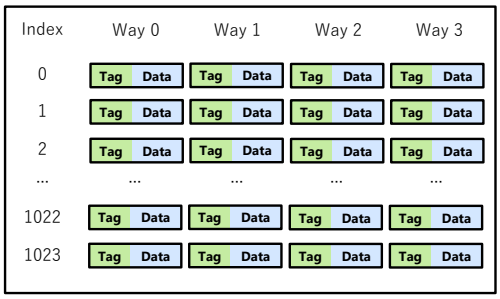
10

[機密性1/Confidentiality1]

競合型キャッシュ攻撃

NTT

- Victimと攻撃者がキャッシュを共有していると仮定
  - 攻撃者は Victim があるキャッシュセットにアクセスしたかどうかを推定
    1. 攻撃者は対象キャッシュセットを自分のデータで埋める
    2. 一定時間待つ（Victimがアクセスしたらキャッシュセットが変化）
    3. 攻撃者は対象キャッシュセットに再アクセスし読み込み時間を計測



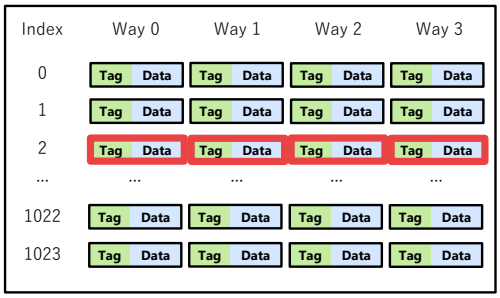
11

[機密性1/Confidentiality1]

競合型キャッシュ攻撃

NTT

- Victimと攻撃者がキャッシュを共有していると仮定
  - 攻撃者は Victim があるキャッシュセットにアクセスしたかどうかを推定
    1. 攻撃者は対象キャッシュセットを自分のデータで埋める
    2. 一定時間待つ（Victimがアクセスしたらキャッシュセットが変化）
    3. 攻撃者は対象キャッシュセットに再アクセスし読み込み時間を計測



12

[機密性1/Confidentiality1]

競合型キャッシュ攻撃

NTT

- Victimと攻撃者がキャッシュを共有していると仮定
  - 攻撃者は Victim があるキャッシュセットにアクセスしたかどうかを推定
    1. 攻撃者は対象キャッシュセットを自分のデータで埋める
    2. 一定時間待つ（Victimがアクセスしたらキャッシュセットが変化）
    3. 攻撃者は対象キャッシュセットに再アクセスし読み込み時間を計測

Index	Way 0	Way 1	Way 2	Way 3
0	Tag Data	Tag Data	Tag Data	Tag Data
1	Tag Data	Tag Data	Tag Data	Tag Data
2	Tag Data	Tag Data	Tag Data	Tag Data
…	…	…	…	…
1022	Tag Data	Tag Data	Tag Data	Tag Data
1023	Tag Data	Tag Data	Tag Data	Tag Data

13

[機密性1/Confidentiality1]

競合型キャッシュ攻撃

NTT

- Victimと攻撃者がキャッシュを共有していると仮定
  - 攻撃者は Victim があるキャッシュセットにアクセスしたかどうかを推定
    1. 攻撃者は対象キャッシュセットを自分のデータで埋める
    2. 一定時間待つ（Victimがアクセスしたらキャッシュセットが変化）
    3. 攻撃者は対象キャッシュセットに再アクセスし読み込み時間を計測

Index	Way 0	Way 1	Way 2	Way 3
0	Tag Data	Tag Data	Tag Data	Tag Data
1	Tag Data	Tag Data	Tag Data	Tag Data
2	Tag Data	Tag Data	Tag Data	Tag Data
…	…	…	…	…
1022	Tag Data	Tag Data	Tag Data	Tag Data
1023	Tag Data	Tag Data	Tag Data	Tag Data

14

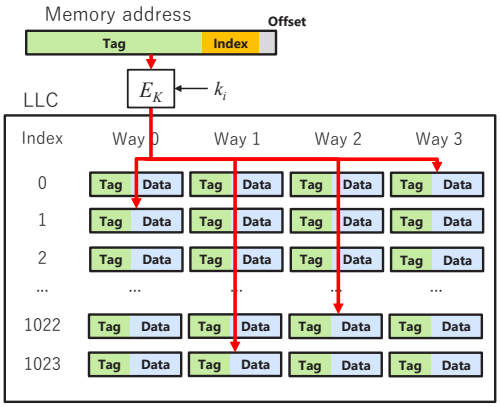
[機密性1/Confidentiality1]

キャッシュランダム化という解決策

NTT

- 競合型キャッシュ攻撃を実行するためには、
  どのキャッシュセットを触っているのか認識する必要がある。
  - Victimが触るか識別したいアドレスが
    どのIndexを用いるのか認識する必要
  - 認識したうえで、同一のIndexを持つ
    キャッシュセットを埋める必要

- ランダム化関数 F_K を用いて
  インデックスをランダム化する。
  - データは**ランダム化された**候補インデックスのどこかに配置される
  - CPUアーキテクチャの変更が少ない
- **ただ、ランダムってなに？**

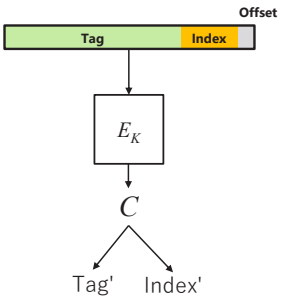


[機密性1/Confidentiality1]

既存研究～低遅延ブロック暗号の転用

NTT

- 例えば低遅延ブロック暗号PRINCEを使う
  - 平文に メモリアドレス を入力
  - 暗号文の10ビットをIndex'として利用
  - 暗号文の48ビットをTag'として保存
  - メモリアドレスではOffsetだった部分は
    保存しておかないと復号できなくなるので、
    暗号文の残り6ビット分は、何らかの手段で保存
  - 問題点
    - 6ビット追加保存は決してnegligibleではない
    - そもそも安全性的にブロック暗号の利用はオーバーキルではないか？

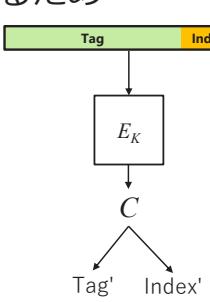


[機密性1/Confidentiality1]

なぜ、ブロック暗号はオーバーキルなのか？

NTT

- ランダム化の目的は、VictimのIndex'と一致する物理アドレスを自分のアドレス空間から選択できないようにするため
- ブロック暗号の設計ゴールはSPRP。
  - Index'を見える仮定で識別不可能性。
  - 見えるどころか選択も可能。
  - 本音では、Ideal cipherですら、あってほしい。



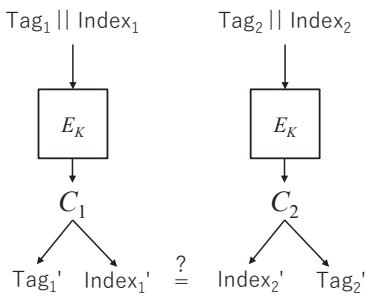
- キャッシュランダム化関数は、
  平文は見える（選択できる）が暗号文は見えない！！
  - SPRP？Ideal cipher？そんなもんは要らん！！

[機密性1/Confidentiality1]

最初の発想 ~専用58ビットブロック暗号を作る

NTT

- ６ビットの運用ロスは回避可能
  - 仕様的には問題はない
- どのように安全性を定義するか
  - **攻撃者は暗号文を観測できない**
  - **Reduced-roundにする？**
  - **でも、どれだけ？**
- このモデルでは部分暗号文衝突の確率を用いて安全性を定義は可能
  - ただ理論的に定義出来ても、
    それでいい感じに作れるかは別問題
  - （研究の超初期は、切詰差分攻撃とこのモデルを真剣に議論していた）
  - 遅延削減・ラウンド数削減に向けた最適化の議論はこのモデルでは難しそう

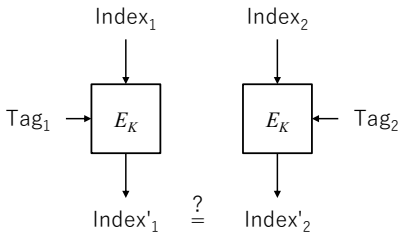


[機密性1/Confidentiality1]

Tweakableブロック暗号はどうだろうか？

NTT

- そもそもTagをランダム化するモチベーションはない。
  - Index部分が平文で、Tag部分はTweakだとみなせばいいのでは？
- 48-bit tweak 10-bit block Tweakableブロック暗号
  - かなり変態的パラメータだが設計目標は定まる。
- 安全性モデルは定義可能か？
  - 部分衝突→衝突に変わる。
  - 切詰差分などという議論はいらない。
  - しかも、よくあるSPRPっぽい定義が可能



19

[機密性1/Confidentiality1]

安全性定義

NTT

Security Requirement 1 *Let O_{real} be the oracle in the real world that takes addresses (x_1, T_1) and (x_2, T_2), and returns 1 if $E_{T_1}(x_1) = E_{T_2}(x_2)$ and 0 otherwise, where E is SCARF. Let O_{ideal} be the oracle in the ideal world that takes addresses (x_1, T_1) and (x_2, T_2), and returns 1 if $\Pi_{T_1}(x_1) = \Pi_{T_2}(x_2)$ and 0 otherwise, where Π is a tweakable random permutation with the same input/tweak/output lengths to SCARF. An adversary is allowed to make at most 2^{40} queries. Then, the adversary running in time at most 2^{80} cannot distinguish the real from the ideal world.*

※Even/Odd Permutationを用いた識別攻撃は除外

20

[機密性1/Confidentiality1]

気持ち

NTT

- 攻撃者は常にペア((x1,T1), (x2,T2))でクエリする。
- 攻撃者は暗号文を見れない
- 暗号文は見れないが、ペアの暗号文が一致したかどうかの0/1の情報はオラクルから学ぶことができる。

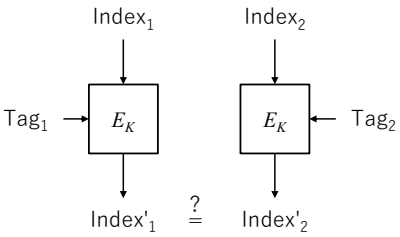
- 実は、ちょっとインチキがある・・・
  - 本当はペアではなく、セットでも実行は可能。
  - セットの場合、セット内に一切衝突がないか、少なくとも衝突が一つあるかが分かる。
  - ただ、これを定式化するのは難しいので無視することにした。

21

[機密性1/Confidentiality1]

これを作りたいんだけど・・・

NTT



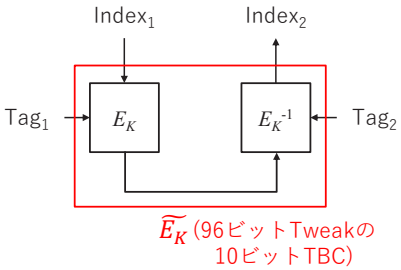
じっと眺める・・・

22

[機密性1/Confidentiality1]

これを作りたいんだけど・・・

NTT



$\widetilde{E_K}$ (96ビットTweakの10ビットTBC)

これって、こういうことでは？

23

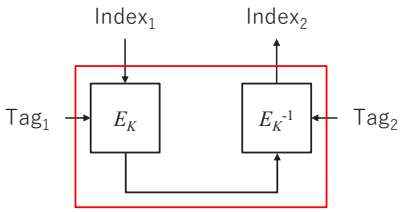
[機密性1/Confidentiality1]

Enc-then-Decモデル

NTT

- Index 1をTweak T1で暗号化し、Tweak T2で復号したものがIndex 2
- 攻撃者に96-bit tweak 10-bit TBCを直接触らせることにしよう。
  - 衝突モデルのオラクルから構成可能

- 共通鍵暗号学者の直観が叫んでいる…
  段数半分でいいんでね？



$\widetilde{E_K}$ (96ビットTweakの10ビットTBC)

24

安全性定義 2

NTT

Security Requirement 2 *Let $\tilde{O}_{real}$ be the oracle in the real world that takes a plaintext P and a pair of tweaks T_1, T_2 as input and returns C such that $C = E_{T_2}^{-1} \circ E_{T_1}(P)$, where E is SCARF. Let $\tilde{O}_{ideal}$ be the oracle in the ideal world that takes a plaintext P and a pair of tweaks T_1, T_2 as input and returns C such that $C = \Pi_{T_2}^{-1} \circ \Pi_{T_1}(P)$, where Π is a tweakable random permutation with the same input/tweak/output lengths to SCARF. An adversary is allowed to make at most 2^{40} queries. Then, the adversary running in time at most 2^{80} cannot distinguish the real from the ideal.*

※Even/Odd Permutationを用いた識別攻撃は除外

気持ち

NTT

- 攻撃者は(x,T1,T2)をでクエリする。
- Tweak T1で暗号化し、Tweak T2で復号した結果を返す。
- 真の暗号文は$\widetilde{E_K}$の半分の段数の中間暗号文ということにする。
  - ここが見えないのは、ブロック暗号にとって当たり前の話。
- $\widetilde{E_K}$そのものは安全なTBCにはならない。
  - 例えば、T1=T2でクエリすればIdentity mapである。
  - $E_{T_2}^{-1} \circ E_{T_1}$ or $\Pi_{T_2}^{-1} \circ \Pi_{T_1}$ の二つのWorldの識別不可能性で定義する。
    - Realは、二つの連結による段数水増し効果を期待。
    - Idealは、そもそもがtweakable random permutation。
  - IdealもT1=T2なら、Identity mapであり、この二つが識別不可能なら、確かに設計された暗号は、あるべきように、理想的と言える。

NTT

SCARFの作り方

[機密性1/Confidentiality1]

SCARFの設計目標は決まった

NTT

- パラメータについて
  - 48-bit tweak
  - 10-bit block
- 安全性について
  - 安全性レベルは80-bit level
  - E_T単体では80-bit安全に到達しない
  - $\widetilde{E_{T_1,T_2}} = E_{T_2}^{-1} \circ E_{T_1}$ となり、初めて80-bit安全に到達。
- 性能について
  - 超低遅延、CPUの動作を可能な限り邪魔せずオーバーヘッドを抑えるため
    - PRINCEなどのよくある低遅延ブロック暗号の倍速を目指す。
  - 逆像が計算可能/復号可能、書き戻し（Write-back）できることが必要なため

28

[機密性1/Confidentiality1]

SCARFの設計目標は決まった・・・が

NTT

- 実はそんなに作るのは簡単ではない。

- 何が難しい？
  - ブロック長があまりにも短すぎる。
    - 鍵を巻き込むコストが高い。
  - 段数水増し効果を得るには細工が必要。
    - 暗号化して復号する。
    - 副鍵が一致すると段数２段分、消えてしまう・・・

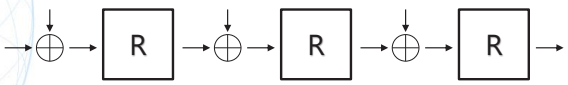
29

[機密性1/Confidentiality1]

まずは基本構造をどうするか

NTT

- SPN構造



  - ブロック長が10-bitしかないと、よく知られる鍵排他的論理和で秘密情報を足すと80-bitを入れるには最低でも8段必要。
  - 中間一致攻撃とかを考慮すると、これで低遅延(段数削減)はかなり厳しい。
  - 鍵排他的論理和以外の方法で秘密情報を入れるのも手だが（例、加算器とか）、可逆にする必要性があるため制約が多く、低遅延な入れ方が出来ない。
  - SPN構造は低遅延暗号の鉄板構造であるが、ここまでブロック長が短いと向かない。

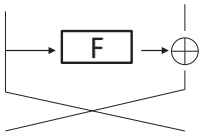
30

[機密性1/Confidentiality1]

まずは基本構造をどうするか

NTT

- Feistel構造



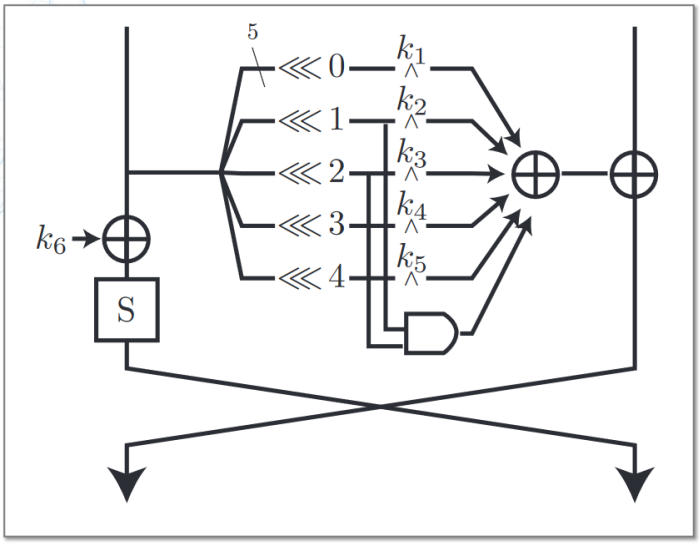
  - 5-bitな鍵依存F関数を作ればよい
  - SPN構造と異なり、F関数自体は可逆である必要がないので、低遅延で多くの鍵ビットを巻き込むことも理論的に可能
    - 問題は、それで安全なのか・・・という話
  - 一般にFeistel構造は１段あたりの非線形性がSPN構造より乏しく、高遅延になりがちである。
  - 私の知る限り、Feistel構造を採用した低遅延暗号は存在しない。

31

[機密性1/Confidentiality1]

SCARFの構造

NTT



32

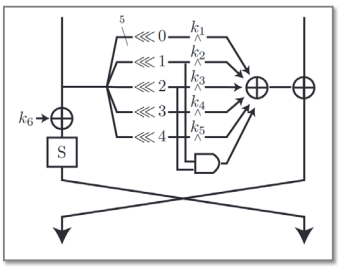
SCARFの構造

NTT

- Feistel構造とSPN構造を混ぜたような構造。
- MISTY構造の変種ともいえる。

- MISTY構造のようにSboxを配置する
  - ２段のSboxの並列実行が可能で、暗号化に関しては、SPN構造と同効率

- MISTY構造では単なるXOR部分に
  超低遅延で大量の鍵を巻き込むG関数を配置



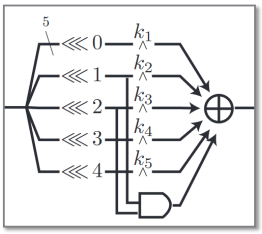
まずG関数を設計

NTT

- Bit rotation + AND gate
  - Bit rotationはcost 0
  - AND gateは最も低遅延なgateの一つ
- 数学的な構造
  - 追加のAND gateを無視すると鍵固定のもとで線形関数

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \end{pmatrix} = \begin{pmatrix} k_{1,1} & k_{2,1} & k_{3,1} & k_{4,1} & k_{5,1} \\ k_{1,2} & k_{2,2} & k_{3,2} & k_{4,2} & k_{5,2} \\ k_{1,3} & k_{2,3} & k_{3,3} & k_{4,3} & k_{5,3} \\ k_{1,4} & k_{2,4} & k_{3,4} & k_{4,4} & k_{5,4} \\ k_{1,5} & k_{2,5} & k_{3,5} & k_{4,5} & k_{5,5} \end{pmatrix} \times \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix}$$

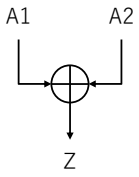
  - 異なる鍵で、同一の写像が生成されることはない。
- 追加のAND gate
  - 上記の、異なる鍵で同一の写像が生成されない性質は引き継がれる。
  - XOR-tree構造での最適化、XOR gate一個分足してもコスト増が少ないため。



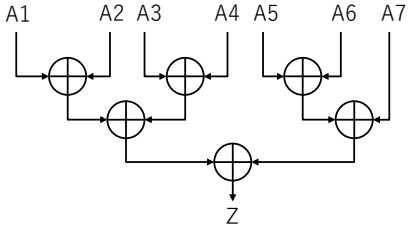
XORツリーのハードウェア実装

NTT

- Q1: 8入力XORと9入力XORでは遅延に大きな差がある
  - A1: YES! 2入力XORゲートの深さ(直列接続されるゲートの数)が変わるため
- Q2: 8入力XORと7入力XORでは遅延はあまり変わらない
  - A2: NO! 論理合成の自由度が大きく変わるため有意な差がある
    - ゲートの深さだけでは評価できない要因が大きな影響を与える



A1 to ZとA2 to Zの遅延には差がある
(信号の立ち上がりと立ち下がりでも違う)



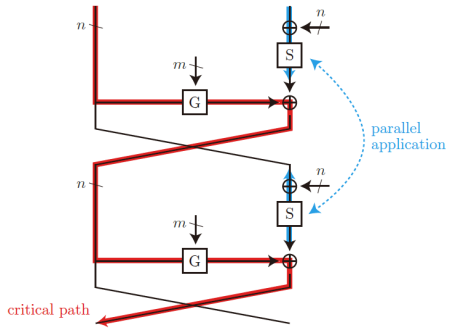
A1–A7は信号到着時間が異なる
(到着が遅い入力ポートには短い遅延を割り当てる
必要があるが，8入力XORだと自由度が少ない)

35

より詳細な設計の詰め方

NTT

- S-boxの設計
  - G関数は1段での鍵の巻き込み量を増やす目的で低遅延に最適化されている。
  - ただし、G関数のみでは安全にならない。
    - 次数が低すぎる。
    - 数学的構造が残りすぎている。
  - 非線形なS-boxを足したいが、それで高遅延になっては意味がない。
  - G関数のパス(赤色)は避けようのないcritical pathとなっているため、このcritical pathが維持される範囲で強いS-boxを用意し配置する。



36

S-boxの設計

NTT

$$S(x) = \Big((\tau_0(x) \vee \tau_1(x)) \wedge (\overline{\tau_3(x)} \vee \overline{\tau_4(x)})\Big) \oplus \Big((\tau_0(x) \vee \tau_2(x)) \wedge (\overline{\tau_2(x)} \vee \tau_3(x))\Big).$$

- 差分確率 $p = \frac{4}{32} = 2^{-3}$
- 線形相関 $c = \pm\frac{12}{32} = 2^{-1.41504}$
- 代数次数 4

Enc-then-Dec構造による脆弱性の最小化

NTT

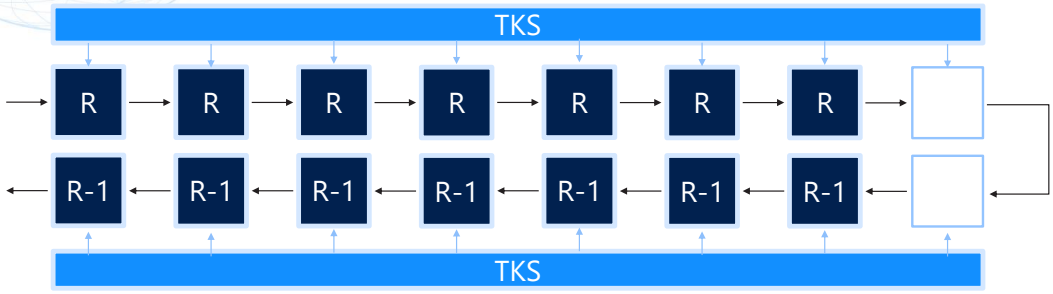
- No Last-Round Cancellation
  - $R_{k'}^{-1} \circ R_k$ という状況は避けようがない。
  - この関数がidentity mapになるのは k=k'のときに限られる。
  - Tweak長は30 bitsよりも長いためlast-round cancellationを起こすtweak pairsの存在は否定できない。
- No Last-Two-Round Cancellation
  - $R_{k_1'}^{-1} \circ R_{k_2'}^{-1} \circ R_{k_2} \circ R_{k_1}$
  - この関数がidentity mapになるのは $(k_1', k_2') = (k_1, k_2)$のときに限られる。
  - Tweak長は60 bitsよりも短いため、そのようなペアはないようにTweak key scheduleを設計したい。

[機密性1/Confidentiality1]

安全性モデルを意識したTweakey schedule

NTT

- 多くのTBCはLinear tweak(ey) scheduleを採用
  - Tweak(ときどき秘密鍵)を線形に混ぜながら副鍵を生成していく
- SCARF的には、これはよろしくない。
  - 線形だと、Last round cancellationが簡単に出来てしまう。



2^{18}個のΔTにおいてLast roundは消滅し、鍵の推測なしで、それが得られる。

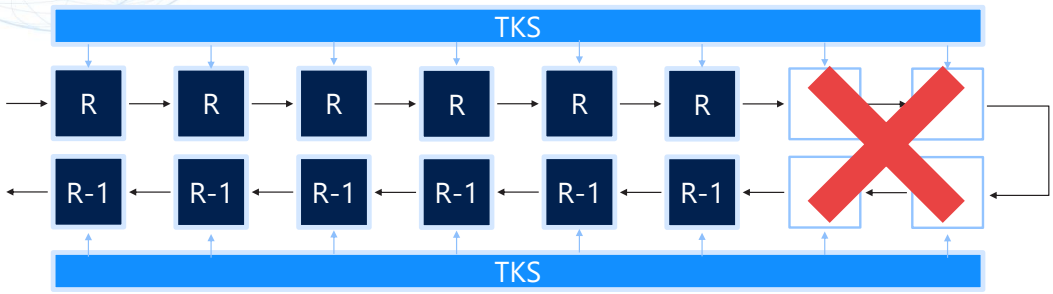
39

[機密性1/Confidentiality1]

安全性モデルを意識したTweakey schedule

NTT

- **Nonlinear** tweak(ey) scheduleにする
  - Tweakey schedule自体をブロック暗号のように設計する。
  - Last Two RoundsがTweakと置換になるようにする。
  - これにより、No Last Two-Round Cancellationの性質が全体でも成立する。



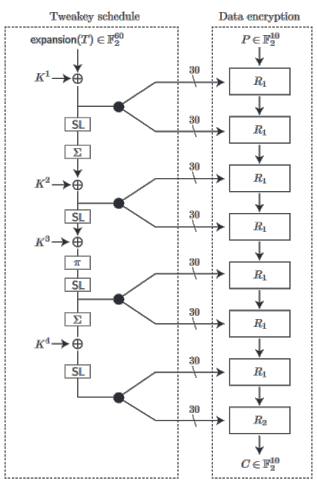
40

[機密性1/Confidentiality1]

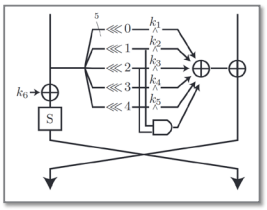
SCARFの全体像

NTT

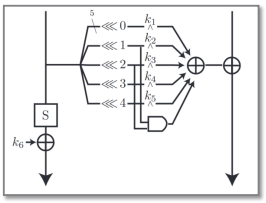
- 入力
  - 10ビット平文
  - 240ビット鍵
  - 48ビットTweak
- 7+1ラウンド
  - アンロールドハードウェアでの実装を想定
  - 最終段は鍵加算位置を変更
- TKS
  - データランダム部より遅延しない範囲で設計



ラウンド関数 (R_1)



最終ラウンド関数 (R_2)



41

[機密性1/Confidentiality1]

ハードウェア性能評価

NTT

- Nangate Open Cell Library を用いてSCARFと既存の代表的な低遅延暗号を合成・評価
  - 全てアンロールド実装
  - 合成条件や設計スタイルは可能な限り統一した
  - 平文，鍵，Tweak，暗号文を格納するためのレジスタの遅延・面積を含む
- SCARFは既存暗号に比べてほぼ半分の遅延と面積を達成
  - SCARFは現代のキャッシュシステムに適合するよう設計されているため，キャッシュランダム化の実装に関するオーバーヘッドは無し
    - 既存のブロック暗号を使用した場合のオーバーヘッドは不明（必ず必要にはなる）

Table 1. Synthesis results using Nangate OCLs

Technology	45 nm		15 nm	
	Latency [ns]	Area [GE]	Latency [ps]	Area [GE]
PRINCE	4.74	12,554	628.49	17,484
MANTIS6	4.73	13,129	630.07	17,641
QARMA5	4.40	13,915	563.62	18,455
SCARF	**2.26**	**7,335**	**305.76**	**8,118**

42

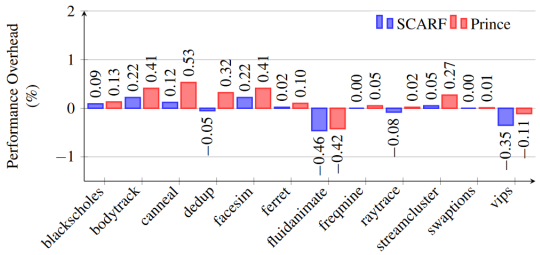
[機密性1/Confidentiality1]

システムレベルシミュレーション

NTT

- SCARFとPrinceを用いてキャッシュランダム化を実装した場合のCPUの性能をgem5シミュレータ※を使って評価
  - キャッシュランダム化にかかると想定した遅延
    - SCARF: 1サイクル
    - Prince: 2サイクル
  - CPUの詳細は論文を参照
- SCARFは全てのプログラムをPrinceより高速に実行

ベンチマークプログラムの実行時間
（キャッシュランダム化無しの場合からの増分・減分で評価）



※ gem5：CPUの動作をサイクルレベルでシミュレーションするソフトウェア．コンピュータアーキテクチャ分野の研究で標準的に使われている．

NTT

SCARFの安全性

[機密性1/Confidentiality1]

SCARFは本当に安全なのか？

NTT

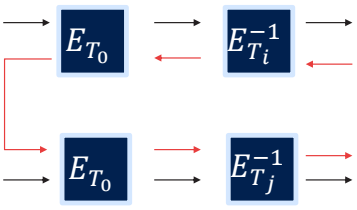
- 従来のTBCとは、かなり構造が違うので、第三者解析が望まれる。

[機密性1/Confidentiality1]

Birthday queryからFull queryを学ぶ

NTT

- 攻撃者はN+1個のTweak $(T_0, T_1, \ldots, T_N)$を選ぶ。
- $\tilde{E}_{T_0,T_j}$に対してfull code bookをqueryする。
  - Query complexityは$N \times 2^{10}$
- 任意の(i, j)に対して、$\tilde{E}_{T_i,T_j} = \tilde{E}_{T_0,T_j} \circ \tilde{E}^{-1}_{T_0,T_i}$が成立する。
  - $\tilde{E}_{T_i,T_j}$に対しては$N^2 \times 2^{10}$の情報を学べる。



46

統計的解読法

NTT

- 差分解読法 $\Pr_x(E(x) \oplus E(x \oplus \alpha) = \beta) > 2^{-n}.$
- 線形解読法 $\Pr_x(\langle \alpha, x \rangle \oplus \langle \beta, E(x) \rangle) = \frac{1}{2} + \frac{c}{2}$
- Boomerang

$$\Pr_x(E^{-1}(E(x) \oplus \beta, k) \oplus E^{-1}(E(x \oplus \alpha) \oplus \beta) = \alpha) > 2^{-n}$$

- Differential-Linear

$$\Pr_x(\beta, E(x) \oplus E(x \oplus \alpha) = 0) = \frac{1}{2} + \frac{c}{2}$$

47

統計的解読法

NTT

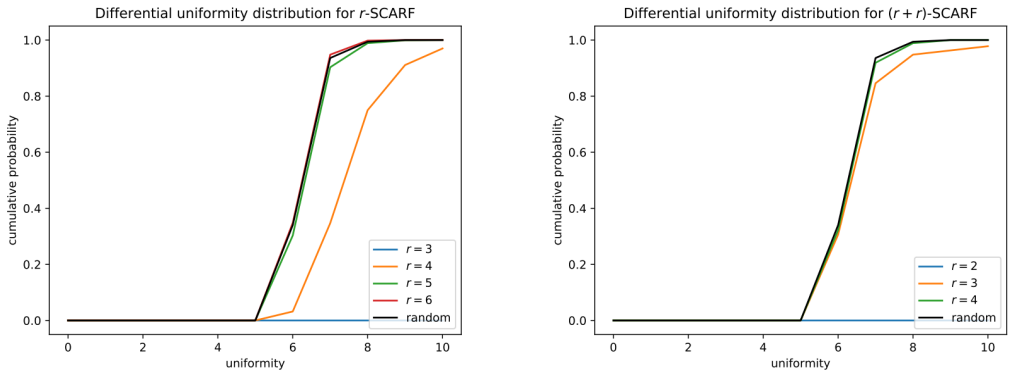
- 普段の私たち
  - 普通のブロック暗号の場合、ブロック長は128ビットや64ビット
  - 差分確率や線形確率などを正確に計算することは計算量的に不可能。
  - ラウンド関数の差分確率などを計算し、独立や鍵平均を仮定し、差分特性確率や、Differential effectを評価する。
- SCARFの場合
  - ブロック長は10-bitしかない。
  - それなら、10-bit lookup tableを鍵やTweakをランダムに生成し、実験的に評価することが可能。

48

[機密性1/Confidentiality1]

差分解読法

NTT



(a) r-round SCARF (b) $(r+r)$-round SCARF

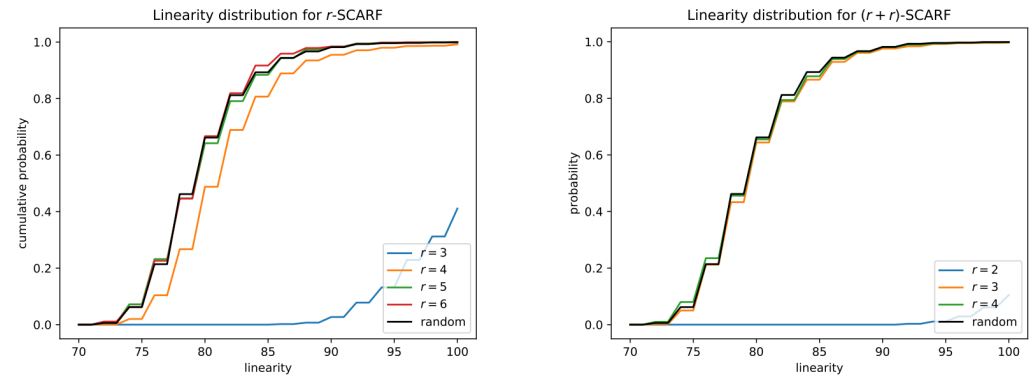
Fig. 8. Cumulative probability distribution for the differential uniformity of SCARF.

49

[機密性1/Confidentiality1]

線形解読法

NTT



(a) r-round SCARF (b) $(r+r)$-round SCARF

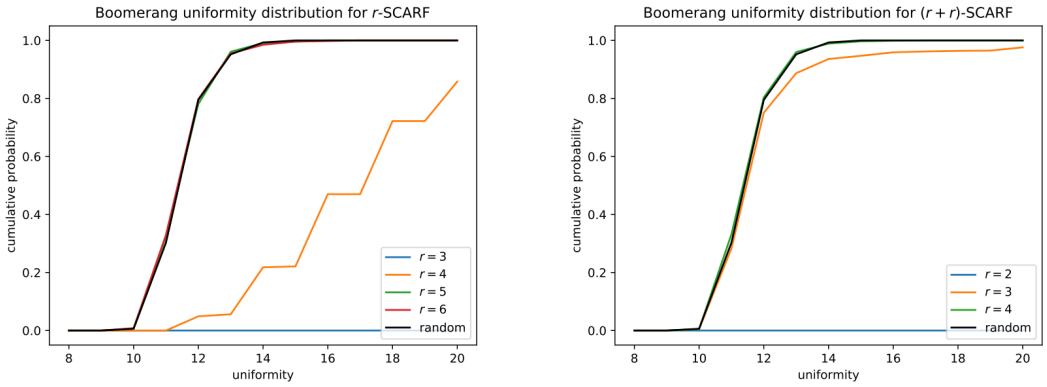
Fig. 9. Cumulative probability distribution for the linearity of SCARF.

50

[機密性1/Confidentiality1]

Boomerang

NTT



(a) r-round SCARF (b) $(r+r)$-round SCARF

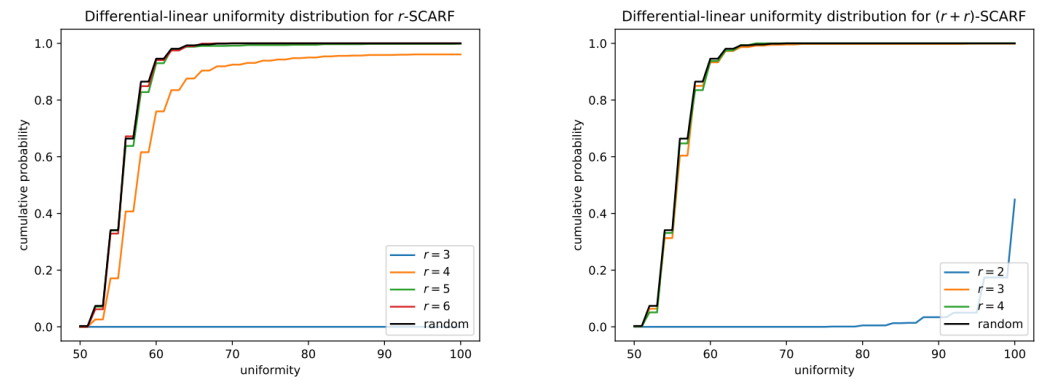
Fig. 10. Cumulative probability distribution for the boomerang uniformity of SCARF.

51

[機密性1/Confidentiality1]

Differential-Linear

NTT



(a) r-round SCARF (b) $(r+r)$-round SCARF

Fig. 11. Cumulative probability distribution for the differential linear uniformity of SCARF.

52

Multiple-tweak attack

NTT

- ブロック長が10-bitしかないため、ブロック長が確率の限界となるような解読法を走らせてランダムと識別するのは難しそう。

- Tweak長や鍵長がブロック長よりもはるかに大きいことを利用した攻撃が怖い。
  - Tweakey scheduleが非線形で、Tweakがactiveな場合、Tweakey scheduleの差分特性確率や線形特性確率は十分に小さくなるように設計されている。
  - これはRelated-tweak attackは難しいことを意味する。
  - 単に、多くのTweakを利用する、Multiple-tweak attackが脅威と言える。

Multiple-tweak differential attack

NTT

- 攻撃シナリオ
- 攻撃者は入力差分α、出力差分βを満足するx, T1, T2の確率の偏りを評価する。
  - ランダムでも発生する確率は1/1023ある。
  - 偏りを評価する、つまり

$$\Pr_{x,T_1,T_2}(\tilde{E}_{T_1,T_2}(x)\oplus\tilde{E}_{T_1,T_2}(x\oplus\alpha)=\beta)=\frac{1}{1023}+\varepsilon.$$

  - およそ、ε^{-2}のクエリを行えば、識別が可能なはず。

[機密性1/Confidentiality1]

Multiple-tweak differential attack

NTT

- x, T1, T2をランダムに取る場合
  - Birthday queryで学ぶtrickが使えない。
  - SCARFは2^{40}queryまでしか認めていないため$\varepsilon = 2^{-20}$程度で頭打ちとなる。
- xをFull code book聞いて、T1とT2を単一セットから選ぶ
  - Birthday queryで学ぶtrickが使える。
  - $N^2 \times 2^9$ pairsを学ぶ。
  - 例えばN=2^{23}のとき、2^{55} pairsを収集でき、この偏りを実験的に評価する。

55

[機密性1/Confidentiality1]

実験結果

NTT

Round	α	β	Bias ε
2+2	(0x00, 0x01)	(0x00, 0x01)	$2^{-9.6792}$
3+3	(0x00, 0x01)	(0x00, 0x01)	$2^{-14.6761}$
4+4	(0x00, 0x01)	(0x00, 0x01)	$2^{-24.8467}$
5+5	(0x00, 0x01)	(0x00, 0x01)	$2^{-29.8025}$
4+4	(0x00, 0x01)	(0x00, 0x02)	$2^{-29.7363}$
4+4	(0x00, 0x01)	(0x00, 0x03)	$-2^{-29.8138}$
4+4	(0x00, 0x01)	(0x00, 0x04)	$2^{-26.5813}$
4+4	(0x00, 0x01)	(0x00, 0x05)	$-2^{-30.6340}$
4+4	(0x00, 0x02)	(0x00, 0x01)	$2^{-30.1689}$
4+4	(0x00, 0x02)	(0x00, 0x02)	$2^{-24.8833}$
4+4	(0x00, 0x02)	(0x00, 0x02)	$2^{-24.8833}$
4+4	(0x00, 0x02)	(0x00, 0x03)	$-2^{-27.9966}$
4+4	(0x00, 0x02)	(0x00, 0x04)	$2^{-30.0152}$
4+4	(0x00, 0x1F)	(0x00, 0x1C)	$2^{-28.1046}$
4+4	(0x00, 0x1F)	(0x00, 0x1D)	$2^{-28.1773}$
4+4	(0x00, 0x1F)	(0x00, 0x1E)	$2^{-27.9916}$
4+4	(0x00, 0x1F)	(0x00, 0x1F)	$2^{-24.4674}$

Table 2. Examples of observed differential bias given experimentally: we used $N_T = 2^{23}$ to get these results, i.e., $2^{23+23+9} = 2^{55}$ pairs.

56

[機密性1/Confidentiality1]

考察

NTT

- 一般的にα=βで、左側Branchがゼロのときに強い偏りが出る。
  - 言い換えると、強い偏りを持つのは、$2^5 - 1 = 31$個程度である。
- 4+4段までは優位な偏りが多く観察される。
- 5+5段の場合、α=βかつ左側Branchがゼロなら、ある程度の偏りを持つ。
- 6+6段の場合、優位な偏りは観測されなかった。

57

[機密性1/Confidentiality1]

考察、収集可能なデータ数について

NTT

- SR1を用いた場合
  - 衝突が発生し一致を学べる確率をランダムに仮定
  - 2^{40}のquery complexityだと$2^{21+21+9} = 2^{51}$程度まで学べる。
  - 今回の実験は、$2^{23+23+9} = 2^{55}$とSR1の設定よりも多くのデータを利用している。
  - SR1の設定でMultiple-tweak differentialが動く可能性は低い。
- SR2を用いた場合
  - 2^{40}のquery complexityだと$2^{29+29+9} = 2^{67}$程度まで学べる。
  - 5+5までは識別可能になるだろう。
  - 6+6は？
    - 2+2 → 3+3、や4+4→5+5ではBiadが2^{-5}ほど劣化
    - 3+3 → 4+4は2^-10ほど劣化
    - 仮に、6+6は2^-10ほど劣化するなら、攻撃出来ないだろう。
    - 仮に、6+6は2^-5ほど劣化なら、ギリギリ識別可能かもしれない。
    - 識別できたとしても、8+8を攻撃するには、2+2段分の鍵回復が必要だが非自明。

58

[機密性1/Confidentiality1]

Multiple-tweak linear attack?

NTT

- 差分で出来るなら線形でも出来るのでは？
- ただ、拡張は簡単ではない。
  - 線形の場合、Tweakが変わると確率のPositive/Negativeが変わる。
  - Positiveか、Negativeかは、鍵に依存して決定されるため、攻撃者には予測が出来ない。
  - その場合、分散値の差で識別する必要がある。
  - PRESENTの線形解読法のモデルを利用すると、KPモデルで
    - Real $\mathcal{N}(0, \frac{1}{N} + 2^{-10} + \epsilon^2)$
    - Random $\mathcal{N}(0, \frac{1}{N} + 2^{-10})$
  - おそらく、Nを大きくしても、この二つは識別できない・・・

[機密性1/Confidentiality1]

さいごに

NTT

- SCARF (Secure CAche Randomization Function)
  - （隠れた意味）
    scarfは動詞で「ガツガツ食べる」という意味がある。
    SCARFは副鍵を無理やり暴飲暴食しているという様も表す。
- なんでUsenix Securityだったの？
  - CRYPTO, Eurocrypt, Asiacryptだと、落ちそうだったから（笑）
  - キャッシュ攻撃の攻撃者モデルを、暗号学的に落とし込むところは、色々と雑な議論をしている。
    - 現実のセキュリティと、暗号という理想論を、何のしこりもなく奇麗に橋渡しをするのは、やはり難しい。
    - IACRだと、SCARFの安全性が現実のセキュリティに帰着していないから意味がない・・・とか面倒くさいこと言うやつ、絶対いる。
    - セキュリティ会議の、大丈夫そうならOK、という"雑さ"が嬉しい。

効率的な近似量子フーリエ変換を利用したShorアルゴリズム

大西 健斗
三菱電機株式会社情報技術総合研究所
Onishi.Kento@ap.MitsubishiElectric.co.jp

本発表では，素因数分解問題を解くShorアルゴリズムの効率化手法について議論する．現在利用されている主な公開鍵暗号として，RSA暗号や楕円曲線暗号があり，素因数分解問題や離散対数問題に安全性の基盤を置いている．Shorアルゴリズムは，これらの問題を多項式時間で解く量子アルゴリズムである．現在の公開鍵暗号が危殆化する時期を見積もるため，Shorアルゴリズムの計算コスト評価は極めて重要である．本発表では，近似量子フーリエ変換に基づくShorアルゴリズムについて議論する．特に，本発表では，将来実現しうる大規模な耐故障性量子計算機を考慮し，耐故障性を持つShorアルゴリズムについて計算コストの削減方法を議論する．

効率的な近似量子フーリエ変換を利用したShorアルゴリズム

三菱電機株式会社
情報技術総合研究所
大西　健斗

三菱電機株式会社

自己紹介

おおにし　けんと
大西　健斗

所属: 三菱電機株式会社　情報技術総合研究所

出身: 東京大学大学院　情報理工学系研究科
数理情報学専攻　暗号数理情報学研究室

博士論文(2021)	公開鍵暗号に対するサイドチャネル攻撃および量子攻撃の安全性評価
2016～2021	公開鍵暗号に対するサイドチャネル情報が誤り付きで得られた場合の秘密鍵復元手法の研究
2018～	Shorアルゴリズムの効率化を踏まえた，公開鍵暗号の安全性評価
2021～	敵対的patch攻撃(画像認識AIシステムへの攻撃手法の一つ)に対するAIシステムの安全性評価

目次

1. 研究背景
2. 既存研究: [RC18]の制御付き剰余乗算の構成
3. 研究成果: 近似QFTを利用したShorアルゴリズムの改良
4. まとめ

目次

1. 研究背景
2. 既存研究: [RC18]の制御付き剰余乗算の構成
3. 研究成果: 近似QFTを利用したShorアルゴリズムの改良
4. まとめ

研究背景

現在利用されている以下の公開鍵暗号は，
量子計算機を利用したShorアルゴリズム[Sho94]により危殆化
- ・RSA暗号[RSA78] (安全性の基盤: 素因数問題)
- ・楕円曲線暗号[Mil86,Kob87] (安全性の基盤: 離散対数問題)

例えば，合成数Nの素因数分解にかかる時間計算量は，
- ・古典計算機: $\log N$の準指数時間 [LLMP90]
- ・量子計算機: $\log N$の多項式時間

しかし，現在の量子計算機の規模はあまり大きくないため，
現状，上記暗号を破るShorアルゴリズムは実現していない

暗号の危殆化時期を見積もるため，
精密なShorアルゴリズムの計算量評価が極めて重要

[LLMP90] Lenstra et al.: The Number Field Sieve. STOC 1990, 1990.
[Sho94] Shor: Algorithms for Quantum Computation: Discrete Logarithms and Factoring. FOCS 1994, 1994.

量子計算機の現状

IBM，Googleなどが，
将来の量子計算機の実現に向けた開発競争を行っている

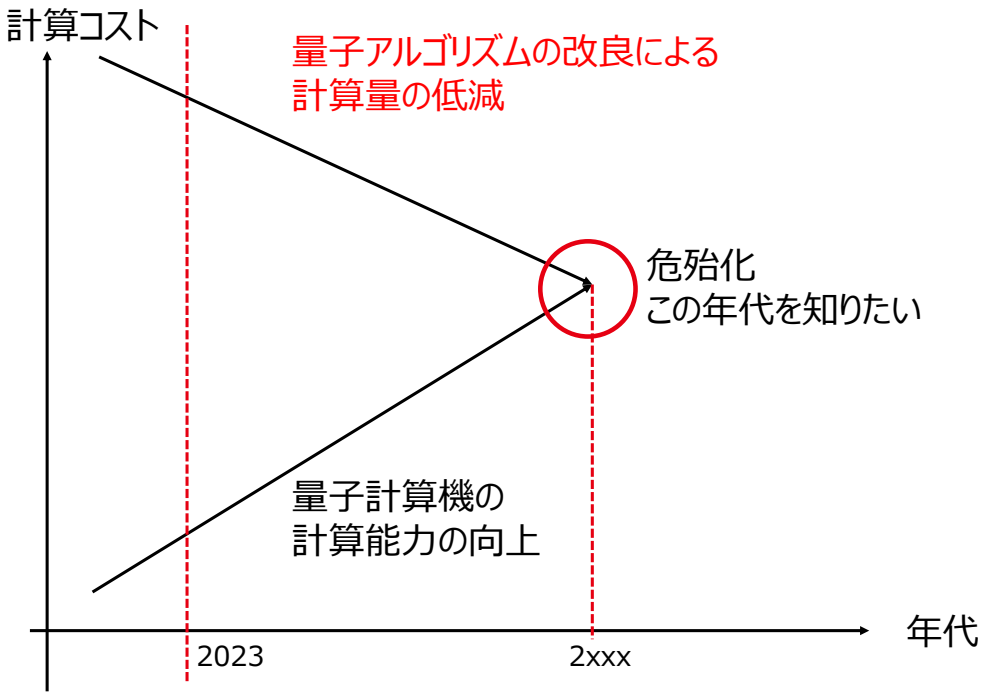
例えば，IBMは2022年に，433量子ビットの「Osprey」をリリース
https://jp.newsroom.ibm.com/2022-11-10-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Twoより

IBMは，今後，量子計算機のさらなる規模拡大を計画
- ・2023年中: 1,121量子ビット (デバイス名:「Condor」)
- ・2024年中: 1,386量子ビット (デバイス名:「Flamingo」)
- ・2025年中: 4,158量子ビット (デバイス名:「Kookaburra」)
- ・2026年以降: 10万量子ビット

https://jp.newsroom.ibm.com/2022-05-13-IBM-Unveils-New-Roadmap-to-Practical-Quantum-Computing-Era-Plans-to-Deliver-4,000-Qubit-Systemより

今後，量子計算機のHWの開発競争が，さらに激化する

将来の危殆化のイメージ



量子計算機の構成モデル

・Jonesら[JVF+12]のモデルでは，量子計算機は5層で構成
・論理量子ビット(誤りがほぼない量子ビット)を，
多数の物理量子ビット(誤りがとても多い量子ビット)で構成

＊Layer 1: Physical
物理量子ビットをHWにより実現する層
＊Layer 2: Virtual
物理量子ビットの演算を行う層

物理層
(量子ビットの実現)

＊Layer 3: QEC
誤り訂正により，論理量子ビットを実現する層
＊Layer 4: Logical
任意の量子計算を実現する層

誤り訂正

＊Layer 5: Application
所望の量子アルゴリズムを実現する層

実計算
(今回の対象)

[JVF+12] Jones et al.: Layered Architecture for Quantum Computing. PRX, 2, 031007, 2012.

現状の量子計算機

・IBMやGoogleが開発している量子計算機は，
NISQ(Noisy Intermediate-Scale Quantum Computer)
と呼ばれる
・物理量子ビットのみ実現

＊Layer 1: Physical
物理量子ビットをHWにより実現する層

＊Layer 2: Virtual
物理量子ビットの演算を行う層

物理層
(量子ビットの実現)

量子ビットの誤りが極めて多いため，誤り訂正が必要
このまま量子ビット数だけ増大しても，Shorアルゴリズムは実現しない

量子計算機モデルでの誤り訂正

＊Layer 3: QEC
誤り訂正により，論理量子ビットを実現する層
→表面符号[FSG09]により実現
しかし，一部の量子演算(量子ゲート)しか利用できない
これらの量子ゲートのみでは，Shorアルゴリズムは実現不可

＊Layer 4: Logical
任意の量子計算を実現する層
→Distillation[FSG09]により実現
全ての量子ゲートが，近似的に利用可能となる
新たに利用可能となる量子ゲートの計算コストは極めて大きい

Shorアルゴリズムの計算コスト評価のためには，
計算コストの高い量子ゲートでの計算量評価が重要

[FSG09] Fowler et al.: High Threshold Universal Quantum Computation on the Surface Code. PRA, 80, 052312, 2009.

計算量評価指標

よく利用される主な計算量指標

・量子ビット数
・量子ゲート数
・回路深さ (量子ゲートを並列に同時実行した際の計算ステップ数)

しかし，どれか一つを減らすと，他の計算量が大きくなる
→回路の評価指標として，KQなる指標[Ste03]がある

$$\mathrm{KQ} = (\text{量子ビット数}) \times (\text{回路深さ})$$

上記の量子回路が正確な出力を行う確率は、$(\text{各ゲートの精度})^{\mathrm{KQ}}$
→KQを小さくすると、量子計算の早期実現につながる [JVF+12]

本発表では，回路深さ及びKQの最小化を行う

[Ste03] Steane: Overhead and Noise Threshold of Fault-Tolerant Quantum Error Correction. PRA, 68, 042322, 2003.

量子計算のイメージ (1/2)

・量子計算は，複数の数値の重ね合わせ状態(量子状態)で演算
具体例 1量子ビットで表現される，$|0\rangle, |1\rangle$の重ね合わせ

$$a_0|0\rangle + a_1|1\rangle, \text{where } a_0, a_1 \in \mathbb{C} \text{ and } |a_0|^2 + |a_1|^2 = 1$$

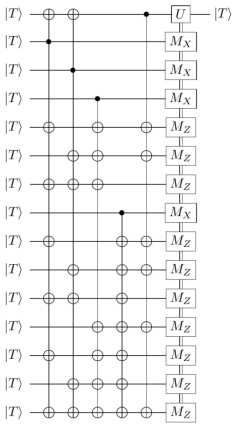
$|a_0|^2, |a_1|^2$は，それぞれ，$|0\rangle, |1\rangle$を出力する確率であり，
以上の量子状態を$\begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$と表記する

・n量子ビットでは，$|0\rangle, |1\rangle, \ldots |2^n - 1\rangle$を表現可能
それぞれの量子状態の係数を$a_0, a_1, \ldots, a_{2^n-1}$としたとき，
量子状態は，2^n次元ベクトル$[a_0, a_1, \ldots, a_{2^n-1}]^{\mathrm{T}}$(Tは転置)で表記

・量子アルゴリズムは，量子ゲートにより，
＊量子状態の各数値
＊各量子状態の係数(出力確率)
を操作し，所望の出力を得る

量子計算のイメージ (2/2)

量子アルゴリズムは，1量子及び2量子ビットゲートに分解，実行される
主な量子ゲートは以下の通り



1量子ビットゲート

・量子ビット反転: $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}$

・位相操作: $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, S = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{bmatrix}, T = \begin{bmatrix} 1 & 0 \\ 0 & \exp(\mathrm{i}\pi/4) \end{bmatrix}$

・量子状態の重ね合わせ: $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

2量子ビットゲート

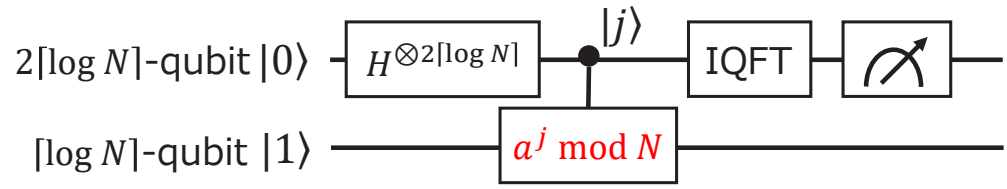
制御NOT(CNOT)ゲート $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ $\begin{matrix} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |11\rangle \\ |11\rangle \to |10\rangle \end{matrix}$

以上の量子ゲートセットで，任意の量子回路を記述可能
Tゲートの計算コストが極めて大きい(Layer4で実現されるため)
Tゲートに関する計算コストを小さくすることが重要

Shorアルゴリズム

現在利用されている公開鍵暗号の安全性の基盤となっている，
素因数分解問題や離散対数問題を効率的に解くアルゴリズム

具体例 合成数Nの素因数分解回路 [Sho94]



上記の量子回路を含め，現在までに提案された実装法は
・量子状態の重ね合わせ
・剰余べき乗算 (Shorアルゴリズム内の主要部分)
・逆量子フーリエ変換 (IQFT)
で構成される

精密な計算量評価には，効率的な剰余べき乗算の構成が必要不可欠

量子算術回路の歴史

Shorアルゴリズムの提案から約30年間，以下の研究トレンドで遷移
現在は、計算コストの大きいTゲートを削減する量子回路について，
研究が進められている

1994年 Shorアルゴリズムが提案される

Shorの回路の実装法を模索
量子算術回路の基礎が完成

2005年

qubitの接続性を考えた量子回路の構成法がトレンドに
(LNN,2D etc.)

2010年

新規の量子算術回路の研究は下火だが、
可逆回路の応用先としての研究が行われた
(ただし、小規模回路が主な研究テーマ)

2017年

Tゲートを減らす量子算術回路の研究がトレンドに

剰余べき乗算の計算コスト(誤り訂正を考慮せず)

・1量子及び2量子ビットゲートに量子回路を分解
・すべてのゲートのコストを等価と扱う
→主要な既存研究の計算コストは以下 ($n = \lceil \log N \rceil$，以降も同様)

計算方法	論理量子ビット数	ゲート数	回路深さ(depth)
Ripple-Carry [CDKM04]	$3n$	$O(n^3)$	$O(n^3)$
Carry-Lookahead [DKRS06]	$5n$	$O(n^2 \log n)$	$O(n^2 \log n)$
Fourier-Basis [RC18]	$2n$	$O(n^3)$	$O(n^2)$

計算方法の違いは以下の通り (下の手法ほど，ゲートの並列度が高い)
・Ripple-Carry: 1ビットごとに繰り上がり(carry)を計算する
・Carry-Lookahead: Carryを先に計算する
・Fourier-Basis: Fourier基底上で計算を行う

誤り訂正を考慮しなければ，[RC18]の計算コストが最小

剰余べき乗算の計算コスト(誤り訂正を考慮)

・スライドp.12の量子ゲートに量子回路を分解
・Tゲートのコストに着目する
　以降，Tゲート数をT-count，Tゲートの回路深さをT-depthと呼ぶ
→主要な既存研究の計算コストは以下の通り

計算方法	論理 量子ビット数	T-count	T-depth
Ripple-Carry [CDKM04]	$3n$	$O(n^3)$	$O(n^3)$
Carry-Lookahead [DKRS06]	$5n$	$O(n^2 \log n)$	$O(n^2 \log n)$
Fourier-Basis [RC18]	$2n$	$O(n^3 \log n)$	$O(n^2 \log n)$

[RC18]では，T-count，T-depthがともに$\log n$倍
∵位相ゲート$\mathrm{P}(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & \exp(\mathrm{i}\theta) \end{bmatrix}$の近似に，$\Theta(\log n)$個の$T$ゲートが必要 [RS16]

[RS16] Ross and Selinger: Optimal Ancilla-Free Clifford+T Approximation of Z-Rotations. Quantum Information & Computation, 16(11-12), 901–953, 2016.

計算時間を見積もった関連研究

※前提条件が違うので，直接の比較は不可

Ripple-Carry [GE21]
- 2048-bit RSAを破るため，8時間の攻撃時間を要する
- 上記攻撃に，2000万個の物理量子ビットを利用
- 様々な近似計算テクニックを利用しており，
　量子ビット数及びT-countを増大させる代わりに，T-depthが減少

Carry-Lookahead [Oon20]
- [JVF+12]に基づき，解読可能時期と解読時間を算出
- 1024-bit RSAは，2046年に，16.2時間で攻撃可能
- 2048-bit RSAは，2048年に，2.97日で攻撃可能

Fourier-Basis [RC18]
- 計算時間の見積もりは行われていない

[GE21] Gidney and Ekerå: How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits. Quantum, 5, 433, 2021.
[Oon20] Oonishi: Security Evaluation of Public-Key Cryptography against Side-Channel Attacks and Quantum Attacks, Doctoral Thesis, 2020.
[RC18] Rines and Chuang: High Performance Quantum Modular Multipliers. eprint arXiv 1801.01081, 2018.

研究対象

計算方法	論理量子ビット数	T-count	T-depth
Ripple-Carry [CDKM04]	$3n$	$O(n^3)$	$O(n^3)$
Carry-Lookahead [DKRS06]	$5n$	$O(n^2 \log n)$	$O(n^2 \log n)$
Fourier-Basis [RC18]	$2n$	$O(n^3 \log n)$	$O(n^2 \log n)$

・最終的には，Shorアルゴリズムの精密な計算量評価のため，
どの手法が効率的なのかを明確にしたい

・Ripple-Carryに基づく方法及びCarry-Lookaheadに基づく方法は，
多数の既存研究が存在する

・Fourier-Basisに基づく方法では，あまり研究が進められていない

Fourier-Basisに基づく方法は，どの程度効率化が可能か？

目次

1. 研究背景

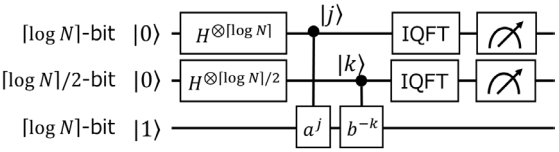
2. 既存研究: [RC18]の制御付き剰余乗算の構成

3. 研究成果: 近似QFTを利用したShorアルゴリズムの改良

4. まとめ

剰余べき乗算の分解

剰余べき乗算
$|j\rangle|x\rangle \to |j\rangle|xa^j \bmod N\rangle$



Shorアルゴリズムの亜種[EH17]により，
$1.5n$個に分解

制御つき乗算
$|c\rangle|x\rangle \to \begin{cases} |0\rangle|x\rangle \text{ if } c = 0, \\ |1\rangle|ax \bmod N\rangle \text{ otherwise} \end{cases}$

2個に分解

(制御なし)乗算
$|x\rangle|y\rangle \to |x\rangle|(y + ax) \bmod N\rangle$

$|c\rangle|x\rangle|0\rangle \to \begin{cases} |0\rangle|0\rangle|x\rangle \\ |1\rangle|x\rangle|0\rangle \end{cases} \to \begin{cases} |0\rangle|0\rangle|x\rangle \\ |1\rangle|x\rangle|ax\rangle \end{cases}$
$\to \begin{cases} |0\rangle|0\rangle|x\rangle \\ |1\rangle|ax\rangle|x\rangle \end{cases} \to \begin{cases} |0\rangle|0\rangle|x\rangle \\ |1\rangle|ax\rangle|0\rangle \end{cases} \to \begin{cases} |0\rangle|x\rangle|0\rangle \\ |1\rangle|ax\rangle|0\rangle \end{cases}$

量子フーリエ変換上での，
乗算回路の計算コストを削減

[EH17] Ekerå and Håstad: Quantum Algorithms for Computing Short Discrete Logarithms and Factoring RSA Integers. PQCrypto 2017, 2017.

既存研究[RC18]の乗算回路

・Montgomery乗算を利用して乗算を計算
$|x\rangle|0\rangle \to |x\rangle|axR^{-1} \bmod N\rangle$
計算を簡単にするため，Rとしては2のべき乗(2^m)が利用される
なお，本文献では，$m = \log n$を利用

・各位相ゲートの近似精度をεとした下で，計算コストを評価
→計算コストの多くが量子フーリエ変換(QFT)に由来する

近似精度がεの場合の，乗算回路のコスト見積もり

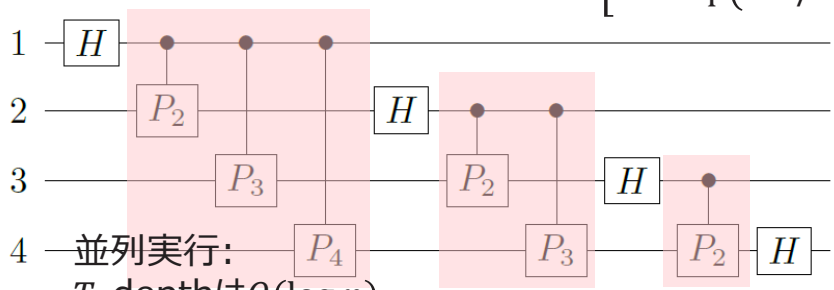
演算	T-count	T-depth
Multiplication	$4.5n^2\log(1/\varepsilon)$	$3n\log(1/\varepsilon)$
Reduction	$3n^2\log(1/\varepsilon)$	$6n\log(1/\varepsilon)$
Uncomputation	$1.5n^2\log(1/\varepsilon)$	$3n\log(1/\varepsilon)$
合計	$9n^2\log(1/\varepsilon)$	$12n\log(1/\varepsilon)$

量子フーリエ変換 (QFT)

・nビットのQFTは，
　＊$n(n-1)/2$個の制御付き位相ゲート
　＊$O(n\log n)$の回路深さ
　を必要とする
・下式により，量子状態$|y\rangle$を変換

$$|x\rangle \to \sum_{y=0}^{2^n-1} \exp\left(2\pi \mathrm{i}\frac{xy}{2^n}\right)|y\rangle$$

具体例 4量子ビットの量子フーリエ変換　$P_j = \begin{bmatrix} 1 & 0 \\ 0 & \exp(2\pi \mathrm{i}/2^j) \end{bmatrix}$



並列実行:
T-depthは$O(\log n)$

QFT上での加算 [Dra00]

量子状態$|x\rangle$に対する古典値aの加算(加算結果$|x+a\rangle$)は以下の通り

$$|x\rangle \to \sum_{y=0}^{2^n-1} \exp\left(2\pi \mathrm{i}\frac{xy}{2^n}\right)|y\rangle \quad \text{QFT}$$

$$\to \sum_{y=0}^{2^n-1} \exp\left(2\pi \mathrm{i}\frac{xy}{2^n}\right)\exp\left(2\pi \mathrm{i}\frac{ay}{2^n}\right)|y\rangle \quad \text{位相ゲートの適用}$$

$$\exp\left(2\pi \mathrm{i}\frac{ay}{2^n}\right) = \prod_{k=0}^{n-1}\exp\left(2\pi \mathrm{i}\frac{a2^k}{2^n}y_k\right)$$
where $y = \sum_{k=0}^{n-1} 2^k y_k$ and $y_k \in \{0,1\}$

$$= \sum_{y=0}^{2^n-1} \exp\left(2\pi \mathrm{i}\frac{(x+a)y}{2^n}\right)|y\rangle$$

$$\to |x+a\rangle \quad \text{inverseQFT}$$

[Dra00] Draper: Addition on a Quantum Computer. eprint arXiv quant-ph/0008033, 2000.

MITSUBISHI ELECTRIC Changes for the Better | QFT上での制御つき加算

・量子状態$|c\rangle \in \{|0\rangle, |1\rangle\}$に応じて，
量子状態$|x\rangle$に古典値aを加算する演算(加算結果$|x + ca\rangle$)
・n個の制御つき位相ゲートにより構成

$$|c\rangle|x\rangle \to |c\rangle \sum_{y=0}^{2^n-1} \exp\left(2\pi \mathrm{i} \frac{xy}{2^n}\right)|y\rangle \quad \text{QFT}$$

$$\to |c\rangle \sum_{y=0}^{2^n-1} \exp\left(2\pi \mathrm{i} \frac{xy}{2^n}\right) \exp\left(2\pi \mathrm{i} \frac{cay}{2^n}\right)|y\rangle \quad \text{制御つき位相ゲートの適用}$$

$$\exp\left(2\pi \mathrm{i} \frac{cay}{2^n}\right) = \prod_{k=0}^{n-1} \exp\left(2\pi \mathrm{i} \frac{a2^k}{2^n} c y_k\right)$$
where $y = \sum_{k=0}^{n-1} 2^k y_k$ and $y_k \in \{0,1\}$

$$= |c\rangle \sum_{y=0}^{2^n-1} \exp\left(2\pi \mathrm{i} \frac{(x + ca)y}{2^n}\right)|y\rangle$$

$$\to |c\rangle|x + ca\rangle \quad \text{inverseQFT}$$

以上の制御付き加算を繰り返すことで，Montgomery乗算を実現

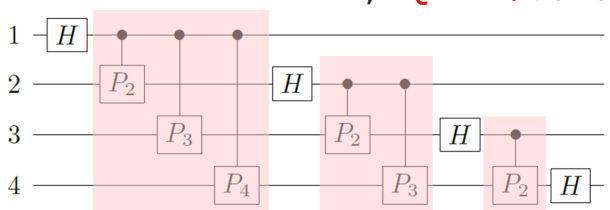
MITSUBISHI ELECTRIC Changes for the Better | Multiplication [RC18]

QFT領域上で，剰余演算を行わない乗算の結果を出力

$|x\rangle|0\rangle \to |x\rangle|0\rangle_\phi$ ※以降，QFT領域のレジスタはϕを記載

$$\to |x\rangle|ax\rangle_\phi = |x_{n-1}x_{n-2}\dots x_1 x_0\rangle \left|\sum_{k=0}^{n-1} x_k (2^k a \bmod N)\right\rangle_\phi$$

制御つき位相ゲートは，制御ビットと標的ビットを入れ替えても変化なし
→制御ビットをスケジューリングすることで，QFTと乗算を同時に実行



計算量は，
・T-count: $1.5n^2\log(1/\varepsilon) + 3n^2\log(1/\varepsilon) = 4.5n^2\log(1/\varepsilon)$
・T-depth: $3n\log(1/\varepsilon)$

Reduction [RC18]

Montgomery Reductionを実行 (3ステップで構成)

$|ax\rangle_\phi \rightarrow |axN^{-1}\bmod 2^{m+1}\rangle|ax2^{-m}\bmod N\rangle_\phi$を計算

・Estimation (第2レジスタの計算)

$(N-1)/2$の制御つき減算をm回実施

・Extract (QFT2回分、計算量の主要項)

IQFT及びQFTで、第2レジスタの最上位ビットを取得

・Correction (第2レジスタの調整)

＊第2レジスタの最上位ビットを、第1レジスタの最上位ビットへ

＊第1レジスタの最上位ビットが1のとき、第2レジスタにNを足す

計算結果: $|x\rangle|ax\rangle_\phi \rightarrow |x\rangle|axN^{-1} \bmod 2^{m+1}\rangle|ax2^{-m} \bmod N\rangle_\phi$

計算量は以下の通り

＊T-count: $2 \times 1.5n^2\log(1/\varepsilon) = 3n^2\log(1/\varepsilon)$

＊T-depth: $2 \times 3n\log(1/\varepsilon) = 6n\log(1/\varepsilon)$

Uncomputation [RC18]

補助ビット(前ページ第3レジスタ)の値を削除

Multiplicationと同様，制御なしかけ算1回分で実装可能

$|x\rangle|axN^{-1}\bmod 2^{m+1}\rangle|ax2^{-m}\bmod N\rangle_\phi$

$\rightarrow |x\rangle|axN^{-1}\bmod 2^{m+1}\rangle_\phi|ax2^{-m}\bmod N\rangle_\phi$

第2レジスタに
m次元のQFT
(計算量は微小)

$\rightarrow |x\rangle|0\rangle_\phi|ax2^{-m} \bmod N\rangle$

・第1レジスタのaN^{-1}倍を第2レジスタから減算
・第3レジスタにn次元のIQFT
計算量は、
・T-count: $nm \times 3\log(1/\varepsilon) + 1.5n^2\log(1/\varepsilon)$
$\sim 1.5n^2\log(1/\varepsilon)$
・T-depth: $3n\log(1/\varepsilon)$

$\rightarrow |x\rangle|0\rangle|ax2^{-m} \bmod N\rangle$

第2レジスタのすべての量子ビットにHゲートを適用
(計算量は微小)

※第2レジスタの値は，$aN^{-1} \bmod 2^{m+1}$倍の逆操作により消去

目次

1. 研究背景

2. 既存研究: [RC18]の制御付き剰余乗算の構成

3. 研究成果: 近似QFTを利用したShorアルゴリズムの改良

4. まとめ

本節の内容は，以下の研究成果に基づく

大西健斗，國廣昇: 効率的な近似量子フーリエ変換を利用したShorアルゴリズム，QIT47，2022.

本研究の成果

既存研究 [RC18]

↓ 素朴な近似QFTへの取り換え
T-countが1/3に減少

素朴な近似QFTを利用した構成

↓ 改良版近似QFTの提案
T-depthが1/2に減少

改良版近似QFTを利用した構成

↓ KQを最小にするスケジューリング方法の提案
KQが1/2に減少 (T-depthは増加)

KQを最小化した構成

既存研究[RC18]の乗算回路 **(再掲)**

・Montgomery乗算を利用して剰余積を計算

$$|x\rangle|0\rangle \rightarrow |x\rangle|axR^{-1} \bmod N\rangle$$

計算を簡単にするため，Rとしては2のべき乗(2^m)が利用される
なお，本文献では，$m = \log n$を利用

・各位相ゲートの近似精度をεとした下で，計算コストを評価
→計算コストの多くが量子フーリエ変換(QFT)に由来する

近似精度がεの場合の，乗算回路のコスト見積もり

演算	T-count	T-depth
Multiplication	$4.5n^2\log(1/\varepsilon)$	$3n\log(1/\varepsilon)$
Reduction	$3n^2\log(1/\varepsilon)$	$6n\log(1/\varepsilon)$
Uncomputation	$1.5n^2\log(1/\varepsilon)$	$3n\log(1/\varepsilon)$
合計	$9n^2\log(1/\varepsilon)$	$12n\log(1/\varepsilon)$

本研究の成果

$o(n)$の補助ビットを追加し、回路深さが$o(n\log n)$の近似QFTを構築
→Shorアルゴリズム全体のコスト削減に成功

1.QFTを近似QFTに置き換え (T-countが減少)
2.近似QFTの効率化 (T-depthが減少)

近似精度がεの場合の，乗算回路のコスト見積もり

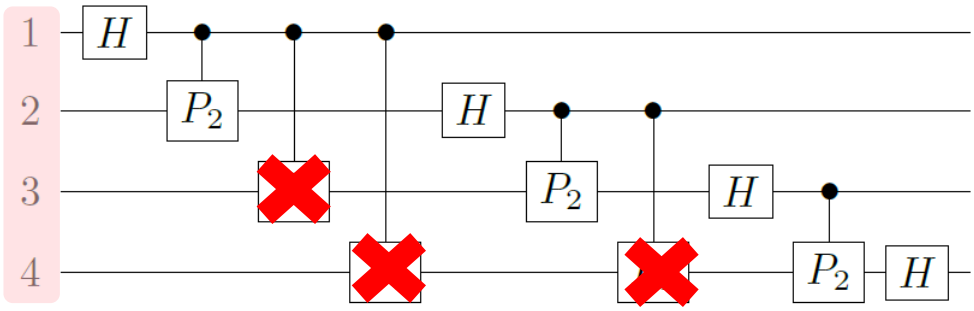
演算	T-count	T-depth
Multiplication	$3n^2\log(1/\varepsilon)$	$3n\log(1/\varepsilon)$
Reduction	$3n\log n\log(1/\varepsilon)$	$16n\log\log(1/\varepsilon)$
Uncomputation	$3n\log n\log(1/\varepsilon)$	$3n\log(1/\varepsilon)$
合計	$3n^2\log(1/\varepsilon)$	$6n\log(1/\varepsilon)$

T-countが1/3倍に、T-depthが1/2に減少

素朴な近似QFT

近似精度がεのとき、

位相がε以下の制御$P_{\log\left(\frac{1}{\varepsilon}\right)} = \begin{bmatrix} 1 & 0 \\ 0 & \exp(2\pi i\varepsilon) \end{bmatrix}$ゲートを省略



以降のスライドで，
量子ビット番号と呼ぶ

既存研究[RC18]では，別種の位相エラーがあっても計算可能
→近似QFTによる計算コスト削減も可能

素朴な近似QFTへの置き換え

・番号aの量子ビットは、$a < b$なる番号bの量子ビットに，
制御R_{b-a+1}ゲートを適用

→各量子ビットのゲート数が平均$n/2$個から平均$\log(1/\varepsilon)$個へ減少
近似QFTのT-countは、主要項でなくなるため，
Montgomery乗算のT-countが1/3に減少

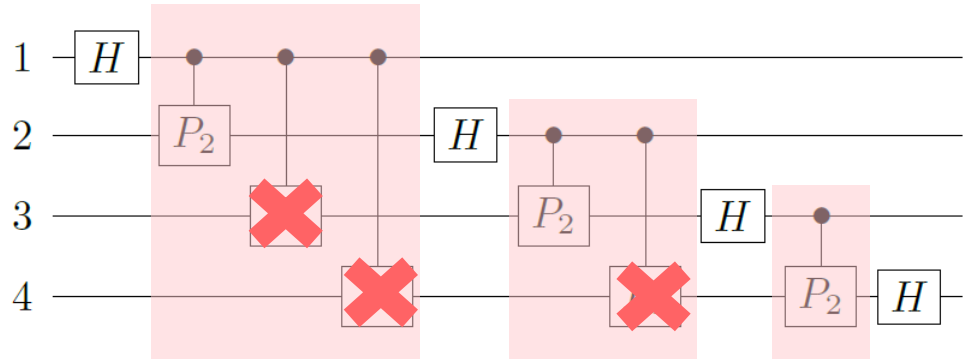
近似精度がεの場合の，制御付き乗算回路のT-count

演算	[RC18]	素朴なQFT
Multiplication	$4.5n^2\log(1/\varepsilon)$	$3n^2\log(1/\varepsilon)$
Reduction	$3n^2\log(1/\varepsilon)$	$o\left(n^2\log(1/\varepsilon)\right)$
Uncomputation	$1.5n^2\log(1/\varepsilon)$	$o\left(n^2\log(1/\varepsilon)\right)$
合計	$9n^2\log(1/\varepsilon)$	$3n^2\log(1/\varepsilon)$

1/3

効率的な近似QFT (1/3) [NSM20]

近似QFTの並列部分を加算回路に置き換え，
さらなるT-countの削減に成功



[NSM20] Nam et al.: Approximate Quantum Fourier Transform with $O(n\log(n))$ T gates. Npj Quantum Information, 6(1), 1-6, 2020.

効率的な近似QFT (2/3) [NSM20]

・番号aの量子ビットは、$a < b$なる番号bの量子ビットに，
制御R_{b-a+1}ゲートを適用
つまり，量子ビットaとbの値がともに1のときのみ位相が変化
→(番号aの量子ビット) ∧ (番号bの量子ビット)を$k_{m-1-(b-a)}$に格納
$k_{m-1-(b-a)}$が1ならば，制御R_{b-a+1}を適用

・$k_{m-1-(b-a)}$に加え，さらに補助量子状態を準備し，
これらの補助量子状態上で，以下の演算を行う

$$\left(\frac{1}{\sqrt{2^m}}\sum_{j=0}^{2^m-1}\exp\left(-2\pi\mathrm{i}\frac{j}{2^m}\right)|j\rangle\right)|k_{m-2}\dots k_1k_0\rangle$$

$$\rightarrow\left(\frac{1}{\sqrt{2^m}}\left(\prod_{l=0}^{m-2}\exp\left(k_l\times 2\pi\mathrm{i}\times 2^{l-m}\right)\right)\sum_{j=0}^{2^m-1}\exp\left(-2\pi\mathrm{i}\frac{j}{2^m}\right)|j\rangle\right)|k_{m-2}\dots k_1k_0\rangle$$

効率的な近似QFT (3/3) [NSM20]

$$\left(\frac{1}{\sqrt{2^m}}\sum_{j=0}^{2^m-1}\exp\left(-2\pi\mathrm{i}\frac{j}{2^m}\right)|j\rangle\right)|k_{m-2}\dots k_1k_0\rangle$$

$$\rightarrow\left(\frac{1}{\sqrt{2^m}}\sum_{j=0}^{2^m-1}\exp\left(-2\pi\mathrm{i}\frac{j}{2^m}\right)|(j+k_{m-2}\dots k_1k_0)\bmod 2^m\rangle\right)|k_{m-2}\dots k_1k_0\rangle$$

加算

$$=\left(\frac{1}{\sqrt{2^m}}\sum_{j=0}^{2^m-1}\exp\left(-2\pi\mathrm{i}\frac{j}{2^m}\right)\exp\left(2\pi\mathrm{i}\sum_{l=0}^{m-2}\frac{2^lk_l}{2^m}\right)|j\rangle\right)|k_{m-2}\dots k_1k_0\rangle$$

$$=\left(\frac{1}{\sqrt{2^m}}\left(\prod_{l=0}^{m-2}\exp\left(k_l\times 2\pi\mathrm{i}\times 2^{l-m}\right)\right)\sum_{j=0}^{2^m-1}\exp\left(-2\pi\mathrm{i}\frac{j}{2^m}\right)|j\rangle\right)|k_{m-2}\dots k_1k_0\rangle$$

位相ゲートの積

$|k_{m-2}\dots k_1k_0\rangle$は，前半の量子状態に関わらず，$|0\rangle$に初期化可能

以上より、位相ゲートの積が正しく計算できる

近似QFTの改良

・[NSM20]では，T-countを減らすため，[Gid18]の加算回路を利用
→近似精度がεのとき，最小位相の位相ゲートが$R_{\log(1/\varepsilon)}$より，

- ＊T-count: $8n\log(1/\varepsilon)$
- ＊T-depth: $2n\log(1/\varepsilon)$
- ＊補助量子ビット: $2\log(1/\varepsilon)\ll n$

・この加算回路を[DKRS06]に取り換えると，回路深さが減少
※加算回路自体の回路深さが小さくなるため

- ＊T-count: $32n\log(1/\varepsilon)$
- ＊T-depth: $8n\log\log(1/\varepsilon)\ll 2n\log(1/\varepsilon)$
- ＊補助量子ビット: $4.5\log(1/\varepsilon)\ll n$

近似QFTの時間計算量は、他の回路部分と比べ無視できる

実際に，計算量はどうなるか？

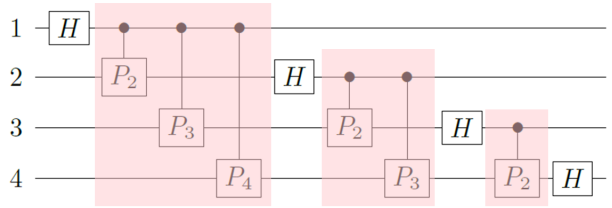
Multiplication [RC18] **(再掲)**

QFT領域上で，剰余演算を行わない乗算の結果を出力

$|x\rangle|0\rangle \rightarrow |x\rangle|0\rangle_\phi$　※以降，QFT領域のレジスタはϕを記載

$$\rightarrow |x\rangle|ax\rangle_\phi = \left|x_{n-1}x_{n-2}\dots x_1x_0\right\rangle \left|\sum_{k=0}^{n-1} x_k\left(2^k a \bmod N\right)\right\rangle_\phi$$

制御つき位相ゲートは，制御ビットと標的ビットを入れ替えても変化なし
→制御ビットをスケジューリングすることで，QFTと乗算を同時に実行



計算量は，　QFT　Mult.

・T-count: $1.5n^2\log(1/\varepsilon) + 3n^2\log(1/\varepsilon) = 4.5n^2\log(1/\varepsilon)$

・T-depth: $3n\log(1/\varepsilon)$

Multiplication **(本研究)**

既存研究

制御ビットをスケジューリングすることで，QFTと乗算を並列実装

本研究

近似QFTとMultiplicationを分離，近似QFTのコストを無視

計算量は、　近似QFT　Mult.

・T-count: ~~$32n\log(1/\varepsilon) + 8$~~ $3n^2\log(1/\varepsilon) \approx 3n^2\log(1/\varepsilon)$

・T-depth: $3n\log(1/\varepsilon)$

Reduction [RC18] **(再掲)**

Montgomery Reductionを実行 (3ステップで構成)
$|ax\rangle_\phi \rightarrow |axN^{-1}\bmod 2^{m+1}\rangle|ax2^{-m}\bmod N\rangle_\phi$を計算

・Estimation (第2レジスタの計算)
$(N-1)/2$の制御つき減算をm回実施

・Extract (QFT2回分、計算量の主要項)
IQFT及びQFTで、第2レジスタの最上位ビットを取得

・Correction (第2レジスタの調整)
＊第2レジスタの最上位ビットを、第1レジスタの最上位ビットへ
＊第1レジスタの最上位ビットが1のとき、第2レジスタにNを足す

計算結果: $|x\rangle|ax\rangle_\phi \rightarrow |x\rangle|axN^{-1}\bmod 2^{m+1}\rangle|ax2^{-m}\bmod N\rangle_\phi$

計算量は以下の通り
＊T-count: $2\times 1.5n^2\log(1/\varepsilon) = 3n^2\log(1/\varepsilon)$
＊T-depth: $2\times 3n\log(1/\varepsilon) = 6n\log(1/\varepsilon)$

Reduction **(本研究)**

Montgomery Reductionを実行 (3ステップで構成)
$|ax\rangle_\phi \rightarrow |axN^{-1}\bmod 2^{m+1}\rangle|ax2^{-m}\bmod N\rangle_\phi$を計算

・Estimation (第2レジスタの計算)
$(N-1)/2$の制御つき減算をm回実施

時間計算量が大幅減少

・Extract (QFT2回分、計算量の主要項)
IQFT及びQFTで、第2レジスタの最上位ビットを取得

・Correction (第2レジスタの調整)
＊第2レジスタの最上位ビットを、第1レジスタの最上位ビットへ
＊第1レジスタの最上位ビットが1のとき、第2レジスタにNを足す

	Estimation	Extact	Correction	合計
T-count	$3n\log n\log(1/\varepsilon)$	$64n\log(1/\varepsilon)$	$3n\log(1/\varepsilon)$	$3n\log n\log(1/\varepsilon)$
T-depth	$3\log n\log(1/\varepsilon)$	$16n\log\log(1/\varepsilon)$	$3\log(1/\varepsilon)$	$16n\log\log(1/\varepsilon)$

Uncomputation [RC18] **(再掲)**

補助ビット(前ページ第3レジスタ)の値を削除

Multiplicationと同様，制御なしかけ算1回分で実装可能

$|x\rangle|axN^{-1}\bmod 2^{m+1}\rangle|ax2^{-m}\bmod N\rangle_\phi$

$\rightarrow |x\rangle|axN^{-1}\bmod 2^{m+1}\rangle_\phi|ax2^{-m}\bmod N\rangle_\phi$

第2レジスタに
m次元のQFT
(計算量は微小)

$\rightarrow |x\rangle|0\rangle_\phi|ax2^{-m}\bmod N\rangle$

・第1レジスタのaN^{-1}倍を第2レジスタから減算
・第3レジスタにn次元のIQFT
計算量は、
・T-count: $nm\times 3\log(1/\varepsilon)+1.5n^2\log(1/\varepsilon)$
$\sim 1.5n^2\log(1/\varepsilon)$
・T-depth: $3n\log(1/\varepsilon)$

$\rightarrow |x\rangle|0\rangle|ax2^{-m}\bmod N\rangle$

第2レジスタのすべての量子ビットにHゲートを適用
(計算量は微小)

※第2レジスタの値は，$aN^{-1}\bmod 2^{m+1}$倍の逆操作により消去

Uncomputation **(本研究)**

補助ビットの値を削除

Multiplicationと同様、制御なしかけ算1回分で、実装可能

$|x\rangle|axN^{-1}\bmod 2^{m+1}\rangle|ax2^{-m}\bmod N\rangle_\phi$

$\rightarrow |x\rangle|axN^{-1}\bmod 2^{m+1}\rangle_\phi|ax2^{-m}\bmod N\rangle_\phi$

第2レジスタに
m次元のQFT
(計算量は微小)

$\rightarrow |x\rangle|0\rangle_\phi|ax2^{-m}\bmod N\rangle$

・第1レジスタのaN^{-1}倍を第2レジスタから減算
・第3レジスタにn次元のIQFT
計算量は、
・T-count: $nm\times 3\log(1/\varepsilon)$ ~~$+32n\log(1/\varepsilon)$~~
$\sim 3n\log n\log(1/\varepsilon)$
・T-depth: $3n\log(1/\varepsilon)$

$\rightarrow |x\rangle|0\rangle|ax2^{-m}\bmod N\rangle$

第2レジスタのすべての量子ビットにHゲートを適用
(計算量は微小)

※第2レジスタの値は，$aN^{-1}\bmod 2^{m+1}$倍の逆操作により消去

本研究の成果 (再掲)

$o(n)$の補助ビットを追加し、回路深さが$o(n\log n)$の近似QFTを構築
→Shorアルゴリズム全体のコスト削減に成功

1.QFTを近似QFTに置き換え (T-countが減少)
2.近似QFTの効率化 (T-depthが減少)

近似精度がεの場合の，乗算回路のコスト見積もり

演算	T-count	T-depth
Multiplication	$3n^2\log(1/\varepsilon)$	$3n\log(1/\varepsilon)$
Reduction	$3n\log n\log(1/\varepsilon)$	$16n\log\log(1/\varepsilon)$
Uncomputation	$3n\log n\log(1/\varepsilon)$	$3n\log(1/\varepsilon)$
合計	$3n^2\log(1/\varepsilon)$	$6n\log(1/\varepsilon)$

T-countが1/3倍に、T-depthが1/2に減少

Shorアルゴリズムのコスト

Shorアルゴリズムでは，$O(n^{-3})$の近似精度が必要
(∵乗算回路を$3n$回繰り返し，位相ゲート数が$O(n^3)$となるから)
→近似精度εを$\varepsilon \sim n^{-3}$とする

Shorアルゴリズムの計算コスト

演算	T-count	T-depth
Multiplication	$27n^3\log n$	$27n^2\log n$
Reduction	$27(n\log n)^2$	$48n^2\log\log n$
Uncomputation	$27(n\log n)^2$	$27n^2\log n$
合計	$27n^3\log n$	$54n^2\log n$

KQの最小化 (1/3)

・今までの議論: 計算時間の最小化
・ここからの議論: ゲートの要求精度の最小化

上記の量子回路が正確な出力を行う確率は、$(\text{各ゲートの精度})^{\mathrm{KQ}}$
→KQを小さくすると、量子計算の早期実現につながる [JVF+12]

KQの小さいスケジューリング方法とは？

KQの最小化 (2/3)

Oonishiらの手法[OTU+21]に従い、最適化

・計算コストの大きいTゲートに着目し、以下のKQ_Tを最小化

$$\mathrm{KQ}_T = (\text{量子ビット数}) \times (T - \mathrm{depth})$$

・上式の最小化のため，最大並行実行Tゲート数n_Tを最適化
・Tゲートのdistillationに必要な量子ビット数を$c_g + 1$とする
※+1はSゲートに必要な補助量子ビット

このとき，T-depthの主要項に着目すると，
・量子ビット数: $2n + (c_g + 1)n_T$
・T-depth: $\frac{27n^3 \log n}{n_T} + 27n^2 \log n$

演算	T-count	T-depth
Multiplication	$27n^3 \log n$	$27n^2 \log n$
Reduction	$27(n \log n)^2$	$48n^2 \log\log n$
Uncomputation	$27(n \log n)^2$	$27n^2 \log n$
合計	$27n^3 \log n$	$54n^2 \log n$

[OTU+21] Oonishi et al.: Efficient Construction of a Control Modular Adder on a Carry-Lookahead Adder Using Relative-Phase Toffoli Gates, IEEE ToQE, 3, 1–18, 2021.

KQの最小化 (3/3)

$$\mathrm{KQ}_T = \left(2n + (c_g + 1)n_T\right)\left(\frac{27n^3 \log n}{n_T} + 27n^2 \log n\right)$$

$$27n^2 \log n\left((c_g + 1)n_T + \frac{2n^2}{n_T} + n(c_g + 3)\right)$$

最小化の対象	n_T	KQ_T
計算時間	n	$54n^3 \log n(c_g + 3)$
KQ_T	$n\sqrt{2/(c_g + 1)}$	$27n^3 \log n(c_g + 3)$

1/2

目次

1. 研究背景

2. 既存研究: [RC18]の制御付き剰余乗算の構成

3. 研究成果: 近似QFTを利用したShorアルゴリズムの改良

4. まとめ

まとめ

[RC18]のShorアルゴリズムを改良
1. 素朴な近似QFTの利用により、T-countが1/3に減少
2. 改良版近似QFTの利用により、T-depthが1/2に減少
3. スケジューリング方法の工夫により、KQ_Tが1/2に減少

以上により、Shorアルゴリズム回路全体の計算時間の削減を行った

Shorアルゴリズムの計算コスト

演算	T-count	T-depth
[RC18]	$81n^3 \log n$	$108n^2 \log n$
本研究	$27n^3 \log n$	$54n^2 \log n$

最小化の対象	n_T	KQ_T
計算時間	n	$54n^3 \log n(c_g + 3)$
KQ_T	$n\sqrt{2/(c_g+1)}$	$27n^3 \log n(c_g + 3)$

1/2

参考文献 (1/2)

[CDKM04] Cuccaro, S.A., Draper, T.G., Kutin, S.A., and Moulton, D.P.: A New Quantum Ripple-Carry Addition Circuit. eprint arXiv quant-ph/0410184, 2004.

[Dra00] Draper, T.G.: Addition on a Quantum Computer. eprint arXiv quant-ph/0008033, 2000.

[DKRS06] Draper, T.G., Kutin, S.A., Rains, E.M., and Svore, K.M.: A Logarithmic-Depth Quantum Carry-Lookahead Adder. Quantum Information & Computation, **6**(4), 351–369, 2006.

[EH17] Ekerå, M. and Håstad, J.: Quantum Algorithms for Computing Short Discrete Logarithms and Factoring RSA Integers. PQCrypto 2017, pp. 347–363, 2017.

[FSG09] Fowler, A.G., Stephens, A.M., and Groszkowski, P.: High Threshold Universal Quantum Computation on the Surface Code. Physical Review A, **80**(5), 052312, 2009.

[Gid18] Gidney, C.: Halving the Cost of Quantum Addition. Quantum, **2**, 74, 2018.

[GE21] Gidney, C. and Ekerå, M.: How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits. Quantum, **5**, 433, 2021.

[JVF+12] Jones, N.C., Van Meter, R., Fowler, A.G., McMahon, P.L., Kim, J., Ladd, T.D., and Yamamoto, Y.: Layered Architecture for Quantum Computing. Physical Review X, **2**(3), 031007, 2012.

[Kob87] Koblitz, N.: Elliptic Curve Cryptosystems. Mathematics of computation, **48**(177), 203–209, 1987.

[LLMP90] Lenstra, A.K., Lenstra Jr, H.W, Manasse, M.S., and Pollard, J.M.: The Number Field Sieve. STOC 1990, pp. 564–572, 1990.

参考文献 (2/2)

[Mil86] Miller, V.S.: Use of Elliptic Curves in Cryptography, CRYPTO 1985, pp. 417–426, 1986.

[NSM20] Nam, Y., Su, Y., and Maslov, D.: Approximate Quantum Fourier Transform with $O(n\log(n))$ T gates. Npj Quantum Information, **6**(1), 1-6, 2020.

[Oon20] Oonishi, K.: Security Evaluation of Public-Key Cryptography against Side-Channel Attacks and Quantum Attacks, Doctoral Thesis, 2020.

[OTU+21] Oonishi, K., Tanaka, T., Uno, S., Satoh, T., Van Meter, R., and Kunihiro, N.: Efficient Construction of a Control Modular Adder on a Carry-Lookahead Adder Using Relative-Phase Toffoli Gates, IEEE Transactions on Quantum Engineering, **3**, 1–18, 2021.

[RC18] Rines, R. and Chuang, I.: High Performance Quantum Modular Multipliers. eprint arXiv:1801.01081, 2018.

[RSA78] Rivest, R.L., Shamir, A., and Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, **21**(2), 120–126, 1978.

[RS16] Ross, N.J. and Selinger, P.: Optimal Ancilla-Free Clifford+T Approximation of Z-Rotations. Quantum Information & Computation, **16**(11-12), 901–953, 2016.

[Sho94] Shor, P.W.: Algorithms for Quantum Computation: Discrete Logarithms and Factoring. FOCS1994, pp. 124–134, 1994.

[Ste03] Steane, A.M.: Overhead and Noise Threshold of Fault-Tolerant Quantum Error Correction. Physical Review A, **68**(4), 042322, 2003.

MITSUBISHI ELECTRIC

Changes for the Better

素因数分解問題に対する 新しい量子アルゴリズム SQIF の実装と解析

山口 純平
富士通株式会社
j-yamaguchi@fujitsu.com

2022 年 12 月に Shor アルゴリズムよりも少ない量子ビットで素因数分解可能とする新しい量子アルゴリズム SQIF(Sublinear-resource Quantum Integer Factorization) が提案された [1]．SQIF は平方差法をベースとしており，特に平方差法の関係式計算を組み合わせ最適化問題に帰着し，その近似解を量子アルゴリズム QAOA を用いて計算することで関係式を得る．本講演では，2023 年 5 月の CSEC 研究会で発表した「格子と最適化手法を用いた素因数分解法の実験報告」[2] の詳細を紹介する．まず SQIF の詳細を紹介し，関係式が数個しか計算できないという問題点を指摘する．次に，十分な数の関係式が計算可能な拡張 SQIF を提案し，その実験結果を紹介する．実験を大規模にするため QAOA の代わりに古典的なアニーリング計算を使用し，11 から 55 ビットの合成数の素因数分解に成功した．最後に，2048 ビット合成数の分解に必要な量子ビット数および計算量の見積もりを与える．

References

[1] Bao Yan, et al. “Factoring integers with sublinear resources on a superconducting quantum processor.” arXiv preprint arXiv:2212.12372, 2022.
[2] 山口純平，伊豆哲也，國廣昇，“格子と最適化手法を用いた素因数分解法の実験報告”，研究報告インターネットと運用技術（IOT），2023-IOT-6-22，pp. 1–8，2023.

現代暗号に対する安全性解析・攻撃の数理

素因数分解問題に対する新しい量子アルゴリズムSQIFの実装と解析

2023年9月21日(木)
富士通株式会社 富士通研究所
データ＆セキュリティ研究所
山口 純平

背景: RSA暗号 (1/2)

- 現在広く使用されている公開鍵暗号
  - RSA暗号（素因数分解問題）
  - 楕円曲線暗号（離散対数問題）
  - …
- 古典計算機に対する計算量評価
  - 米国：NIST, 日本：CRYPTREC などが実施
  - CRYPTRECの予測によるとRSA2048の分解は早くても2040年以降[1)]

1) CRYPTREC報告書, 暗号技術検討会 2022年度報告書 CRYPTREC RP-1000-2022

背景: RSA暗号 (2/2)

FUJITSU

- 量子計算機に対する計算量評価(=Shorアルゴリズムの評価)
  - 我々の見積もり (誤りなし量子計算機を仮定) [YYT+23]
    - 2048ビット合成数の分解には、深さ約 2.22×10^{12}, ゲート数 1.79×10^{12}, 量子ビット数 10241 が必要
    - 解読に要する時間=約104日
      - 2019年にGoogle社が公開した量子計算機Sycamoreをベースに試算
      - Sycamore: 53量子ビットの処理性能でゲート数約1500, 深さ約40, サンプル数10^6の計算に約200秒
        → $200/40/10^6 \times 1.79\times10^{12} = 8.95\times10^6$ = 約104日

  → **現在の量子計算技術ではここまで長時間に渡った量子計算は困難なため、当面は解読不可能**

  - [GE21]の見積もり (誤りあり量子計算機を仮定)
    - 2048ビット合成数の分解には、約2000万量子ビットで7.44時間

  → **ここまで大規模な量子計算機の実現はまだまだ先のため、当面は解読不可能**

[YYT+23] Yamaguchi, J., Yamazaki, M., Tabuchi, A., Honda, T., Izu, T., & Kunihiro, N. (2023). Estimation of Shor's Circuit for 2048-bit Integers based on Quantum Simulator. *Cryptology ePrint Archive*.
[GE21] Gidney, C., Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum, 5, 433.

新たな量子素因数分解アルゴリズムの発見@2022年12月

FUJITSU

- 主張1: SQIFはShorアルゴリズムよりも少ないsublinear個の量子ビットで素因数分解可能
  (※**S**ublinear-resources **Q**uantum **I**nteger **F**actorization)
- 主張2: 特に、2048bit合成数 N は $\frac{2\log N}{\log\log N} \approx 372$ 量子ビットで素因数分解可能

→ Osprey(433量子ビット)で実行可能なレベルのため、SQIFの早急な評価が求められる

Yan, Bao, et al. "Factoring integers with sublinear resources on a superconducting quantum processor." arXiv preprint arXiv:2212.12372 (2022).

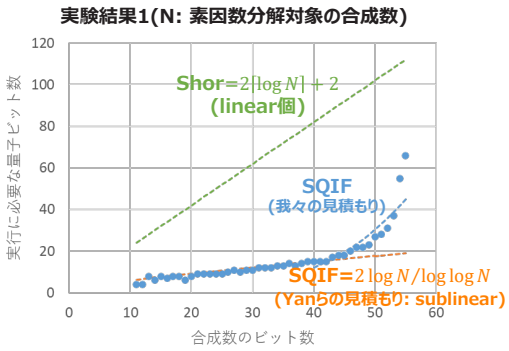
我々の反論(2023年5月)

山口純平，伊豆哲也，國廣昇，”格子と最適化手法を用いた素因数分解法の実験報告”，研究報告インターネットと運用技術（IOT），2023-IOT-6-22，pp. 1-8，2023.

FUJITSU

大規模な実験により以下の2点を明らかにした

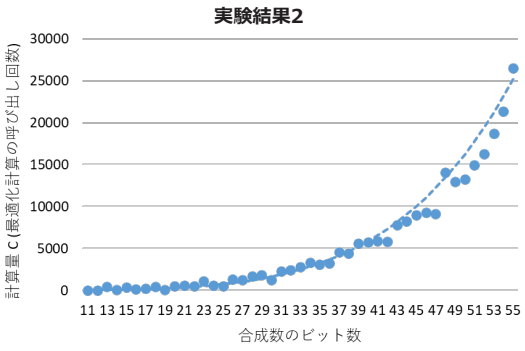
1. Yanらの主張より多くの量子ビットが必要



▼ 2048ビット合成数なら…

6.70×10^8 量子ビット必要 (>> 4098(Shor))

2. SQIFはその計算量も膨大となる



▼ 2048ビット合成数なら…

約2.31×10^{12}回の最適化計算が必要
(1回当たり1秒としても約7万年)

本講演の流れ

FUJITSU

1. SQIFの概要の紹介
2. 我々の結果の紹介

FUJITSU

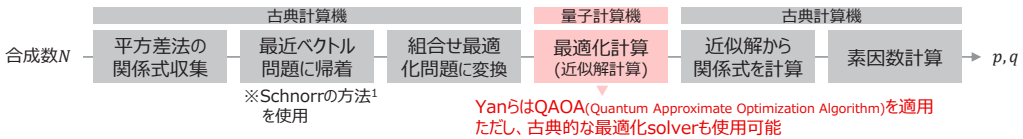
1. SQIFの概要

Yan et al., “Factoring integers with sublinear resources on a superconducting quantum processor”
https://arxiv.org/pdf/2212.12372.pdf

SQIFの概要

FUJITSU

○ SQIFの処理手順



○ SQIFのポイント

- ○ 素因数分解問題を組合せ最適化問題に帰着し、その近似解さえ計算できれば良い
  → SQIFの本質は組合せ最適化問題の近似解を高速に計算する点
- ○ Yanらは量子最適化アルゴリズムQAOAを用いることで高速に近似解を計算できると主張
  - ○ ただし、大きな合成数に対してQAOAがうまくワークするかは実験しないとわからない
  - ○ 一方で、SQIFは近似解で十分なので(=量子計算機のノイズに強い)、NISQデバイスしか使用できない現代では大きなメリット
- ○ ShorアルゴリズムとSQIFのメリット: 量子ビットが少ない、量子回路が浅い、ノイズに強い

1) Schnorr, “Factoring integers by CVP algorithms.”

平方差法の関係式収集 (1/4)
平方差法とは

FUJITSU

○ 平方差法の手順

1. 合成数 N に対して、$X^2 = Y^2 \bmod N$ を満たす X, Y を見つける(平方差と呼ぶ)
   → $(X+Y)(X-Y) = 0 \bmod N$ を満たすため、$X \pm Y$ が高い確率でNの素因数p, qの倍数になっている
2. $\gcd(X \pm Y, N)$ を計算する。素因数が得られない場合は1に戻る。

○ 手順1での平方差の計算方法

i. 右に示す**「関係式」**をたくさん収集する:
ii. 関係式を組み合わせて平方差を計算する

関係式: $p_1^{e_{1,j}} \cdots p_k^{e_{k,j}} = p_0^{e'_{0,j}} p_1^{e'_{1,j}} \cdots p_k^{e'_{k,j}} \bmod N$

$p_0^{e'_{0,j}}$: -1, $p_1^{e'_{1,j}}$: 2, $p_k^{e'_{k,j}}$: k番目の素数
$(p_0, \ldots, p_k)$ の組を因子基底 と呼ぶ)

○ 具体例: N=1961=37*53, k=14 ($p_{14} = 43$)

i. 以下のように**関係式**が収集できているとする
① $2^3 * 3^5 = -17^1 \bmod N$
② $2^4 * 5^3 = 3^1 * 13^1 \bmod N$
③ $3^1 * 5^4 = -2 * 43^1 \bmod N$
④ $2^5 * 5^2 = -3^3 * 43^1 \bmod N$

両辺の積

ii. ③④の積を取ると指数部分が全て偶数に
$2^5 * 3 * 5^6 = 2 * 3^3 * 43^2 \bmod N$
$\Rightarrow 2^4 * 5^6 = 3^2 * 43^2 \bmod N$
$X = 2^2 * 5^3, Y = 3 * 43$ (指数部分を1/2したもの)
に対して、$X^2 = Y^2 \bmod N$ (平方差)

手順2により
$\gcd(X+Y, N) = 37$
$\gcd(X-Y, N) = 53$
が計算される

平方差法の関係式収集 (2/4)
組合せはどうやって見つけるか？ 関係式を何個収集すればよいか？

FUJITSU

○ A. 以下の行列 $\mathbf{R}$ の行ベクトルに対して、一次従属になる組合せを見つければよい
→ 掃き出し法で計算可能

関係式
$2^3 * 3^5 = -17^1 \bmod N$
$2^4 * 5^3 = 3^1 * 13^1 \bmod N$
$3^1 * 5^4 = -2 * 43^1 \bmod N$
$2^5 * 5^2 = -3^3 * 43^1 \bmod N$

i 個目の関係式において、
素数 p_j の指数が奇数のとき(i, j)成分=1,
偶数のとき0を取る行列

行列 $\mathbf{R}$

	-1	2	3	5	…										43
	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0
	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0
	1	1	1	1	0	1	0	0	0	0	0	0	0	0	1
	1	1	1	1	0	1	0	0	0	0	0	0	0	0	1

1次従属
(実際は掃き出し法で計算)

○ A. 因子基底の数kに対して、k+1個以上計算すればよい

平方差法の関係式収集 (3/4)
関係式を計算する方法(1/2)

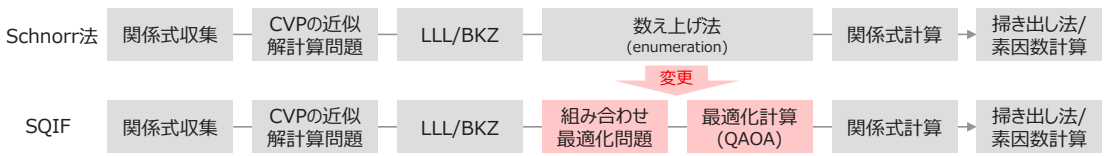
FUJITSU

- 古くからある方法(1920年~)
  - Dixon法、二次篩法、…
- Schnorrの方法 (SQIFの基)
  - 平方差法の関係式収集問題を最短ベクトル問題(SVP)/最近ベクトル問題(CVP)の近似解計算問題に帰着
  - それをLLL/BKZ + enumerationで求解(SVP/CVPに対する一般的な求解法)
  - 実際に 47ビット合成数の素因数分解に成功
    - N=100000980001501

平方差法の関係式収集 (4/4)
関係式を計算する方法(2/2)

FUJITSU

- SQIF
  - Schnorr法のうち、CVPの近似解の計算方法を「組み合わせ最適化問題に変換」して「最適化計算」で求解に変更

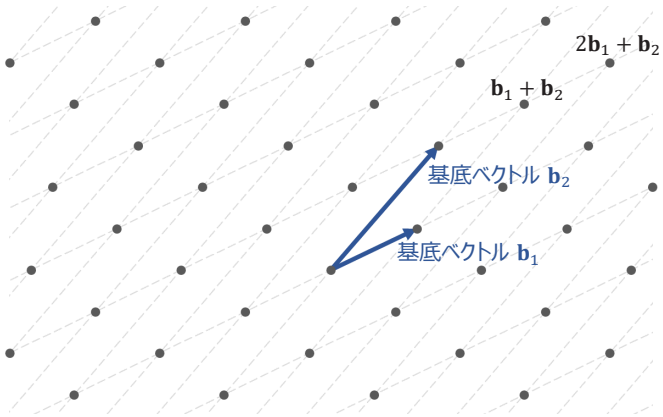


CVPの近似解計算問題に帰着 (1/6)

格子 (Lattice)

FUJITSU

○ 基底ベクトルの整数係数の線型和で表されるベクトルの集合 (下図の ● の集合)



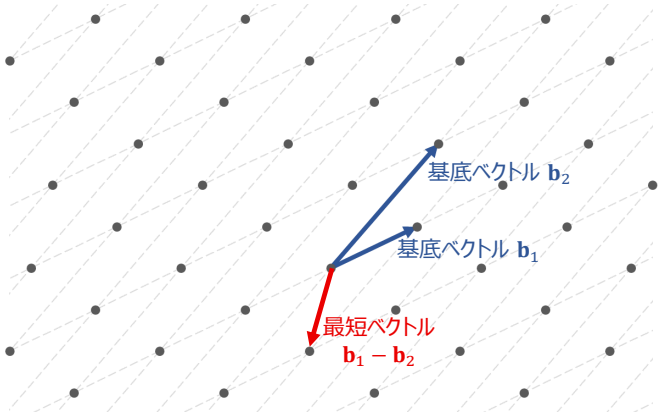
CVPの近似解計算問題に帰着 (2/6)

最短ベクトル問題 (SVP: Shortest Vector Problem)

FUJITSU

○ Given: 基底ベクトル $\mathbf{b}_1, \ldots, \mathbf{b}_n$

○ Find: 長さが最小の(非零な)格子ベクトル (格子次元 n が大きいときは解くのが難しい)

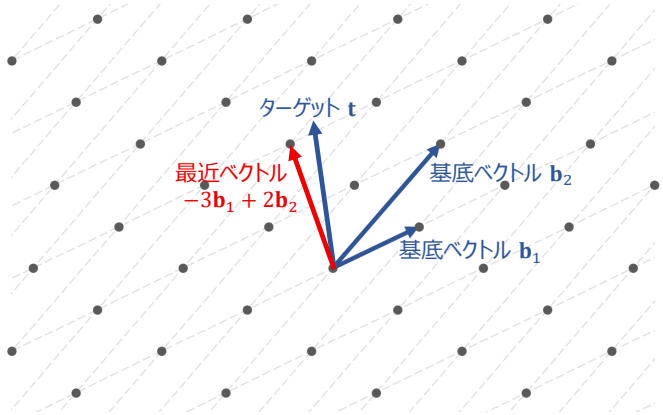


CVPの近似解計算問題に帰着 (3/6)

最近ベクトル問題 (CVP: Closest Vector Problem)

FUJITSU

- Given: 基底ベクトル $\mathbf{b}_1, \ldots, \mathbf{b}_n$ と ターゲット $\mathbf{t}$
- Find: ターゲットに最も近い格子ベクトル (格子次元 n が大きいときは解くのが難しい)



CVPの近似解計算問題に帰着 (4/6)

関係式収集をCVPの近似解計算問題に帰着する方法

FUJITSU

- 目標: 関係式 $p_1^{e_{1,j}} \cdots p_k^{e_{k,j}} = p_0^{e'_{0,j}} p_1^{e'_{1,j}} \cdots p_k^{e'_{k,j}} \bmod N$ を収集する (k: 因子基底の数)

- 帰着方法
  - 格子次元を $n \leq k$ で設定し、基底ベクトルとターゲットを以下とするCVPの近似解計算問題に帰着する

	基底ベクトル	ターゲット
Schnorr法	$\mathbf{B}_{n,c} = \begin{pmatrix} \sqrt{\log p_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \sqrt{\log p_n} \\ N^c \log p_1 & \cdots & N^c \log p_n \end{pmatrix}$	$\mathbf{t} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ N^c \log N \end{pmatrix}$
SQIF	$\mathbf{B}_{n,c} = \begin{pmatrix} f(1) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & f(n) \\ 10^c \log p_1 & \cdots & 10^c \log p_n \end{pmatrix}$	$\mathbf{t} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 10^c \log N \end{pmatrix}$

※$f(1), \ldots, f(n)$ は, 1,1,2,2,3,3,… の置換

- ポイント
  - CVPの近似解は**高確率で**関係式を**1つ**与える(次ページで説明) → 素因数分解にはたくさんの近似解が必要
  - 格子次元 n がCVPの近似解計算の計算量を決定する
    - ただし n は大きい方が高確率で関係式を与えるので計算量とのトレードオフとなる

CVPの近似解計算問題に帰着 (5/6)

近似解が関係式を与える理由 と その具体例

FUJITSU

近似解を与える理由

近似解 $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{Z}^n$ (計算できたと仮定)

$$\begin{pmatrix} f(1) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & f(n) \\ 10^c \log p_1 & \cdots & 10^c \log p_n \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \approx \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 10^c \log N \end{pmatrix}$$

最終成分の比較により

$x_1 \log p_1 + \cdots + x_n \log p_n \approx \log N \iff p_1^{x_1} \cdots p_n^{x_n} \approx N$

nが大きいほど良い近似が得られる
(一方、近似解計算コストは増加)

$u \coloneqq \prod_{x_i>0} p_i^{x_i}, v \coloneqq \prod_{x_i<0} p_i^{-x_i}$ に対して

$\frac{u}{v} \approx N \iff u - vN \approx 0$

以下の式が高い確率で**関係式**を与える

$u = u - vN \bmod N$

定義より $p_1, \ldots, p_n$ で素因数分解される $(n \le k)$

0に近いので**高い確率**で $p_0, \ldots, p_k$ で素因数分解される
(近似解が良いほど確率が高くなる)

具体例

$N = 1961$
$k = 14\ (p_{14} = 43)$

$\mathbf{B}_{3,1.5} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \\ 22 & 35 & 51 \end{pmatrix}$, $\mathbf{t} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 240 \end{pmatrix}$ の近似解 $\begin{pmatrix} 3 \\ 5 \\ 0 \end{pmatrix}$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \\ 22 & 35 & 51 \end{pmatrix} \begin{pmatrix} 3 \\ 5 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 5 \\ 0 \\ 241 \end{pmatrix} \approx \begin{pmatrix} 0 \\ 0 \\ 0 \\ 240 \end{pmatrix}$$

最終成分の比較により

$2^3 3^5 5^0 = 1944 \approx N = 1961$

$u \coloneqq 2^3 3^5, v \coloneqq 1$ に対して

$u - vN = 1944 - 1961 = -17$

この近似解は以下の**関係式**を与えている

$2^3 * 3^5 = -17^1 \ mod\ 1961$

CVPの近似解計算問題に帰着 (6/6)

Schnorr法で用いられるSVP/CVP解法

FUJITSU

- LLL アルゴリズム (Lenstra, Lenstra, Lovasz, 1982年)
  - SVP の近似解を求める(格子次元に関する)多項式時間アルゴリズム
  - 最短ベクトルの $\sqrt{2}^{n-1}$ 倍以内の近似が得られる
- BKZ アルゴリズム (Schnorr, 1987年)
  - SVP の近似解を求めるアルゴリズム
  - パラメータによって近似度と計算量のトレードオフを実現できる

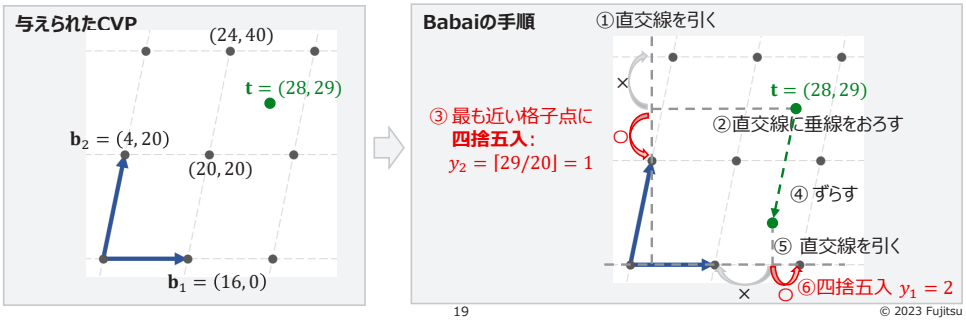
格子ベクトルを短く・互いに直交に近くなるように変換する効果があり、数え上げ法や組合せ最適化問題の計算量を下げる効果があるため、それらの前処理としてよく使用される

- Babai アルゴリズム (Babai, 1986年)
  - CVP の近似解を求めるアルゴリズム
  - LLL アルゴリズムを併用した場合, 最近ベクトルの $2\left(\frac{3}{\sqrt{2}}\right)^n$ 倍以内の近似が得られる
- 数え上げ法 (enumeration)
  - SVP/CVPの解を全数探索(指数時間計算量)で数え上げる方法
  - 近似解をたくさん計算可能

組合せ最適化問題に変換(1/2)
Babaiアルゴリズム

FUJITSU

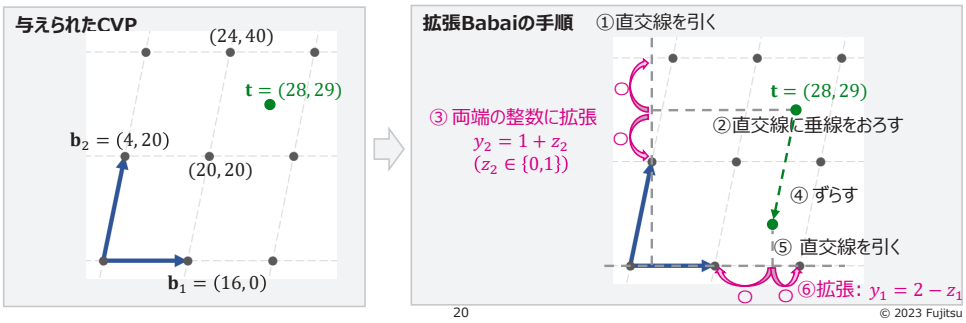
- 入出力
  - Input:　格子の基底 $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$, ターゲットベクトル $\mathbf{t}$
  - Output: CVPの近似解 $\boldsymbol{y}$　(ただし $\|\mathbf{By} - \mathbf{t}\| \leq 2^{n/2}\ \|\mathbf{Bz} - \mathbf{t}\|$, $\mathbf{z}$: 任意の整数ベクトル)
- ポイント
  - 係数を**最も近い整数値に四捨五入する**ことでCVPの近似解を計算する(厳密な解と比較して指数倍のズレを許容)
- 例: 2次元の場合のイメージ
  - 下図通り, $\boldsymbol{y} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$ が計算され, ターゲットに近い格子点 $\begin{pmatrix} 16 & 4 \\ 0 & 20 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 36 \\ 20 \end{pmatrix}$ を得る (厳密解$\begin{pmatrix} 24 \\ 40 \end{pmatrix}$ではない)



組合せ最適化問題に変換(2/2)
拡張Babaiアルゴリズム

FUJITSU

- アイデア
  - Babaiにおいて、**四捨五入(1択)を両端の整数(2択)に拡張**
    → 2択が格子次元個 = 2^n 個の選択肢の中からより良い解を計算する最適化問題に変換される
  - 特に、自明な解はBabaiの解を与えるため自然な拡張になっている
- 前ページの例
  - $H(z_1, z_2) = \left\| \begin{pmatrix} 16 & 4 \\ 0 & 20 \end{pmatrix} \begin{pmatrix} 2 - z_1 \\ 1 + z_2 \end{pmatrix} - \mathbf{t} \right\|^2 = \left\| \begin{pmatrix} 16 & 4 \\ 0 & 20 \end{pmatrix} \begin{pmatrix} -z_1 \\ z_2 \end{pmatrix} + \mathbf{b}_{op} - \mathbf{t} \right\|^2$ ($\mathbf{b}_{op}$: Babaiの解)
  - $(z_1, z_2) = (0, 0)$ はBabaiと同じ解を与えるが、$(1, 1)$ はBabaiより良い近似解(厳密解)を与える



最適化計算

FUJITSU

- 最適化計算の目標
  - 拡張Babaiで計算された 2^n個の選択肢の中からより良い近似解を計算する
- 最適化solverについて
  - Yanらは量子アルゴリズムQAOAを適用している(n 次元格子に対して n 量子ビット使用)
  - 一方で、古典計算を用いた最適化手法であるアニーリング計算等でも代用可能である

→ 量子計算がSQIFの本質というわけではない

Yanらの主張 と SQIFの実験結果

FUJITSU

- 主張
  1. 合成数Nに対して、SQIFを用いることで $O(\log N / \log\log N)$ 量子ビットで関係式を計算可能
     - ただし、$n = \lceil \log N / \log\log N \rceil$ に対して $k = 2n^2$ である (つまり $p_0, p_1, \ldots, p_{2n^2}$を因子基底とする関係式を計算可能)
  2. 特にNが2048ビット合成数のときは、372($\approx 2 * \log N / \log\log N$)量子ビットで素因数分解(に挑戦)可能
- 実験による主張1の裏付け
  - 以下の合成数に対して、n 量子ビットを使用したSQIF(量子計算機+QAOA)で数個の関係式を計算することに成功
    - $N_1 = 1961$ (11bit), $N_2 = 48567227$ (26bit), $N_3 = 261980999226229$ (48bit)
  - N_2の場合の数値例:

$$B_{5,4} = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 6931 & 10986 & 16094 & 19459 & 23979 \end{pmatrix} \quad t_5 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 176985 \end{pmatrix}$$

LLL-0.99

$$D_{5,4} = \begin{pmatrix} 6 & -8 & 2 & -4 & -4 \\ -4 & -3 & 11 & -5 & -3 \\ 6 & 6 & 3 & 0 & -3 \\ 4 & -2 & 0 & 12 & 4 \\ -2 & 2 & -6 & -2 & 1 \\ -3 & 5 & -3 & 4 & -17 \end{pmatrix}$$

拡張Babai

$$\begin{aligned} H = & -54z_1z_2 + 14z_1z_3 + 72z_1z_4 \\ & - 70z_{1,5} - 116z_{2,3} + 78z_{2,4} \\ & + 136z_{2,5} - 126z_{3,4} + 10z_{3,5} \\ & - 18z_{4,5} + z_1 + 42z_2 + 77z_3 \\ & + 5z_4 + 38z_5 + 229 \end{aligned}$$

実際に5番目の近似解 z=00111 をQAOAで計算し、
関係式 $5 * 11^9 = 2 * 41 * 43 * 47 * 73 \bmod N_2$ を得ている

Yan et al., “Factoring integers with sublinear resources on a superconducting quantum processor.”

FUJITSU

2.我々の結果の紹介

山口純平，伊豆哲也，國廣昇，”格子と最適化手法を用いた素因数分解法の実験報告”，
研究報告インターネットと運用技術（IOT），2023-IOT-6-22，pp. 1-8，2023.

SQIFの問題点 と 我々の研究成果

FUJITSU

- 問題点
  - SQIFで求められる関係式は数個程度で、SQIFのみで素因数分解に成功する数の関係式を求めることはできていない
    - 特に論文中に列挙されている $N_2 = 48567227$ (26bit) に関する55個の関係式のうち、SQIF+QAOAで求めたものは1個であり残りの54個はおそらく古典計算機で計算している
  - 実験の数が少ない
  - 計算量について触れられていない

- 成果
  - ① 素因数分解に十分な数の関係式を計算できるようにSQIFを拡張
  - ② 拡張SQIFを用いて11-55ビット合成数の素因数分解に成功
    - ただし大規模実験を可能にするため、最適化solverに富士通の第三世代Digital Annealerを使用
  - ③ この実験結果をもとに、2048ビット合成数に対する拡張SQIFに必要な量子ビット数、計算量の見積もりを与えた
    → SQIFだけで関係式を十分集めるにはYanらの見積もりである372より多くの量子ビットが必要ということがわかった

組合せ最適化solverで、
量子アニーリング計算を
古典的にシミュレートした計算機
(量子計算は不使用)

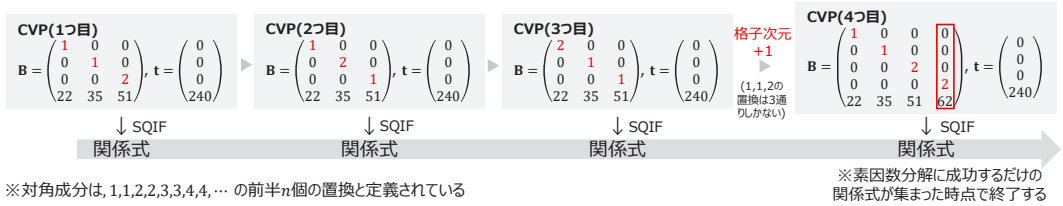
①SQIFの拡張 (1/3)

FUJITSU

○ 問題点: 関係式が数個程度しか計算できない

○ 解決策: 以下を組み合わせる
1. 置換を取り換えることで別のCVPを生成し、それを解くことで他の関係式を収集
2. 置換がなくなったときは、格子の次元を+1して1に戻る

○ イメージ:



※対角成分は, 1,1,2,2,3,3,4,4, … の前半n個の置換と定義されている

※素因数分解に成功するだけの関係式が集まった時点で終了する

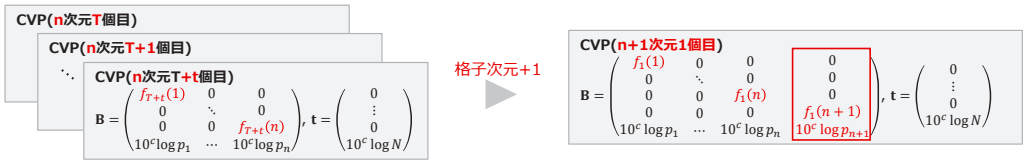
○ 解決策のポイント
- ○ できるだけ小さな次元のCVPから関係式を収集するので、QAOAに必要な量子ビット数を抑えることができる
- ○ 異なるCVPの生成方法は他にも様々あるが(例: f を変える)、今回の目的はSQIFの解析であるためSQIFに近い設定とした

①SQIFの拡張 (2/3)

FUJITSU

○ 工夫点: 新しい関係式が t回連続 得られなかった場合も、格子次元を +1 する

○ イメージ:



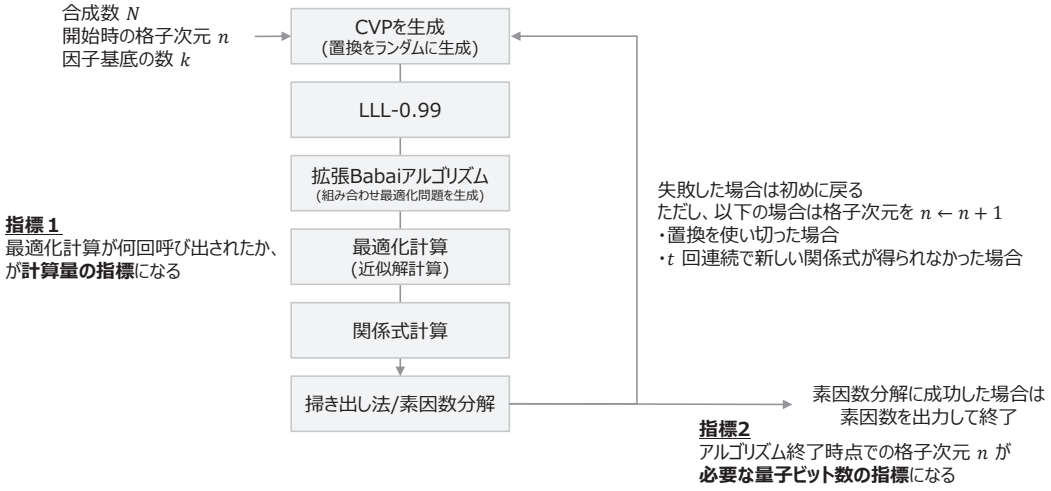
$$p_1^{e_{1,j}} \cdots p_n^{e_{n,j}} = p_0^{e'_{0,j}} p_1^{e'_{1,j}} \cdots p_k^{e'_{k,j}} \bmod N$$

$$p_1^{e_{1,j}} \cdots p_{n+1}^{e_{n+1,j}} = p_0^{e'_{0,j}} p_1^{e'_{1,j}} \cdots p_k^{e'_{k,j}} \bmod N$$

①SQIFの拡張 (3/3)

FUJITSU

○ 拡張SQIFアルゴリズム と 指標(2つ)



指標１
最適化計算が何回呼び出されたか、
が**計算量の指標**になる

指標2
アルゴリズム終了時点での格子次元 n が
必要な量子ビット数の指標になる

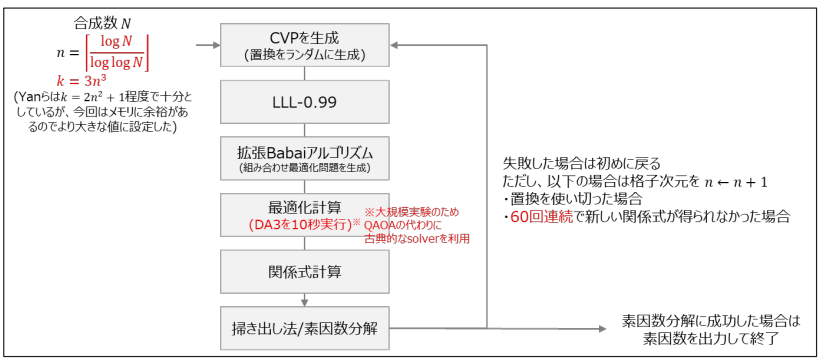
②DA3を用いた実験 (1/2)

FUJITSU

○ 実験方法
- ○ 11-55bit合成数をランダムに1つずつ生成し、**拡張SQIF(最適化solver=DA3)**を用いてNの素因数p, qを計算
- ○ 計算量の指標、量子ビット数の指標を評価する

※実験を大規模にするため、
今回はQAOAではなく古典的なアニーリング計算機を使用
(DA3 = Fujitsuの第三世代 Digital Annealer)

○ 実験のパラメータ設定について



②DA3を用いた実験 (2/2)

FUJITSU

○ 実験結果: 生成した11-55bitすべての合成数の素因数分解に成功

N	ビット数	得られた関係式の数	最適化呼出回数C	格子次元 n_e
1763	11	1	3	4
3599	12	1	3	4
7811	13	34	477	8
9047	14	14	63	6
28459	15	40	384	8
49163	16	33	180	7
108539	17	37	246	8
206711	18	37	426	8
342029	19	11	51	6
695683	20	47	558	8
1973551	21	75	639	9
2381663	22	66	555	9
8350847	23	89	1089	9
10586183	24	68	627	9
20903063	25	51	519	9
42021971	26	120	1374	10
90476623	27	127	1236	11
153713251	28	155	1698	10
490565857	29	188	1839	11
583036847	30	123	1242	11
2047104727	31	201	2286	12
2529975709	32	232	2457	12
5726447347	33	247	2775	12
12604829417	34	330	3321	13
32465228347	35	325	3111	13
40949546243	36	340	3243	14
114391859609	37	360	4551	13
222974630273	38	370	4407	14
516842741119	39	443	5595	15
769319877019	40	399	5721	15
2186142147529	41	546	5922	15
2267839867523	42	562	5844	15
7089643535393	43	647	7845	17
12963867991967	44	673	8223	18
31528690042043	45	664	9000	18
44213622448507	46	667	9270	20
112723142241341	47	693	9153	22
262855838692547	48	1041	14085	22
510125949419747	49	1003	12978	23
910320918319427	50	999	13254	27
1819353647681699	51	1034	14946	28
2805286934279257	52	1094	16293	31
8864496934928671	53	1135	18684	37
15873314879556307	54	1166	21357	55
34834030903967657	55	1547	**26526**	66
			≒約3日	

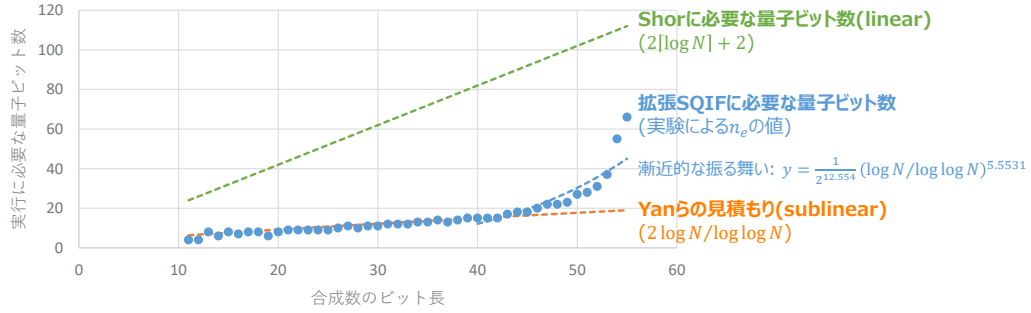
③2048ビット合成数に対する 量子ビット数の見積もり

FUJITSU

○ 見積もり結果 (ただし、DA3とQAOAが同程度の近似解求解性能があると仮定)

- ○ 漸近的な振る舞いが $y = a(\log N/\log\log N)^b$ の形で見積もれると仮定する(Yanらの見積もりは a=2, b=1)
- ○ 両辺対数を取って 40-55bit合成数の結果からa, bを最小二乗法で見積もると $a = 2^{-12.554}, b = 5.5531$ となる
  → sublinearではない
- ○ Nが2048ビット合成数のとき、量子ビット数は $\approx 6.70 \times 10^8$ >> 4098(Shor) となる

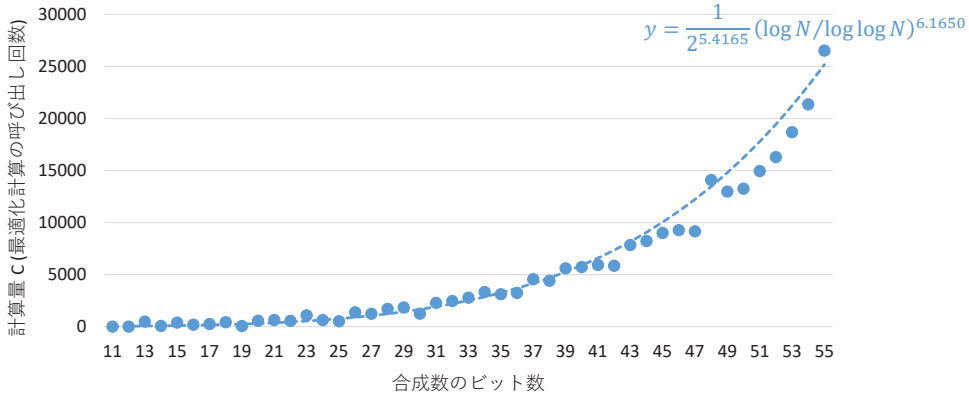
○ Yanらの見積もり・Shorとの比較



③2048ビット合成数に対する
計算量(最適化の呼び出し回数)の見積もり

FUJITSU

○ 見積もり結果
- ○ 量子ビット数と同様に $y = a(\log N/\log\log N)^b$ の形で見積もると、$a = 2^{-5.4165}, b = 6.1650$ となる
- ○ Nが2048ビット合成数のとき、計算量は $\approx 2.31 \times 10^{12}$ (今回の設定の場合、約732496年)となる



見積もりに対する考察

FUJITSU

○ 必要な量子ビット数がYanらの見積もりより多くなる原因
- ○ 合成数Nが大きくなったとき、帰着するCVPの次元も大きくなり、良い近似解が得られにくくなるため
- ○ 具体的には以下の2つの理由が考えられる
  1. CVPの次元が大きくなるにつれ、最適化solver(今回はDA3)で得られる近似解の質が下がる(組合せ爆発)
  2. CVPの次元が大きくなるにつれ、拡張Babaiが含む近似解の質が下がる

  (最適化solverの計算時間を長くする/格子基底簡約を強力にすることで一時的に解決可能だが、合成数が大きくなると同じ状況になると考えられる)

※Yanらは拡張Babai＋QAOAがCVPの次元によらず同程度の近似解を計算できると仮定
→ 次元の増加の影響を考慮していないため、量子ビット数の見積もりが甘くなっている

○ 拡張SQIFの設定について
- ○ 下記は量子ビット数や計算量に大きな影響を与えると考えられる
  今回はこれらを決め打ちしたが、より正確な見積もりを与えるにはこれらを変えたときの実験が必要で、今後の課題である
  - ○ 繰り返し回数 t (より大きく設定することで、必要な量子ビット数が下がり、計算量が大きくなると考えられる)
  - ○ 最適化solver (特にQAOAを使用した実験が重要)

まとめ

FUJITSU

○ Yanらの主張
1. SQIF※はShorアルゴリズムよりも少ないsublinear個の量子ビットで素因数分解可能
2. 特に、2048bit合成数は $\frac{2\log N}{\log\log N} \approx 372$ 量子ビットで素因数分解可能

○ 我々の成果
① 素因数分解に十分な数の関係式を計算できるようにSQIFを拡張
② ①を用いて11-55ビット合成数の素因数分解に成功
  ○ ただし大規模実験を可能にするため、最適化solverに富士通の第三世代Digital Annealer(DA3)を使用
③ この実験結果をもとに、2048ビット合成数に対する拡張SQIFに必要な量子ビット数、計算量の見積もりを与えた
  → SQIFのみで十分な関係式を集めるには
  Yanらの見積もりである372量子ビットより多く必要 (具体的には、6.70×10^8 量子ビット)
  計算量(最適化計算の呼び出し回数)は 2.31×10^{12} と非常に大きく、量子ビット数と合わせて考慮すべき

○ 今後の課題
  ○ 見積もりは実験パラメータに大きく依存するため、より正確な見積もりを与えるにはより多くの実験が必要
    ○ 特に、繰り返し回数 t を変えたときの実験や、**QAOAを適用したときの実験が重要**

33

Thank you

FUJITSU

バイナリ ECDLP を解く Shor のアルゴリズムにおける楕円曲線加算の量子リソース削減

田口 廉
東京大学大学院情報理工学系研究科
rtaguchi-495@g.ecc.u-tokyo.ac.jp

Shor のアルゴリズムは，素因数分解問題・離散対数問題を多項式時間で解く量子アルゴリズムであり，その実装に係る量子リソース評価の研究が数多く行われている．本講演で扱うバイナリ楕円曲線上の離散対数問題を解く Shor のアルゴリズムにおいては，量子逆元計算が主要な計算であることが知られている．その中でも我々はより Toffoli ゲート数と深さの少ない量子 FLT 逆元計算に着目する．量子 FLT 逆元計算アルゴリズムには 2 つの既存手法があり，それぞれ量子ビット数が少ない，深さが少ないという特徴がある．我々は，これら 2 手法をそれぞれ純粋に改良する 2 つの量子 FLT 逆元計算アルゴリズムと，量子ビット数をさらに削減する量子 FLT 逆元計算アルゴリズムを紹介する．

バイナリECDLP を解くShor のアルゴリズムにおける楕円曲線加算の量子リソース削減

○田口 廉（東京大学）　高安敦（東京大学）

2023/09/21

量子コンピュータによる暗号への攻撃

現在用いられている暗号

・RSA暗号　（素因数分解の困難性に基づく）

・楕円曲線暗号　（ECDLP の困難性に基づく）

Shorのアルゴリズムによる
多項式時間解法

これまでの実装結果

素因数分解　・・・21 = 3 × 7

ECDLP　・・・実装なし

効率的な実装法の
考案が必要

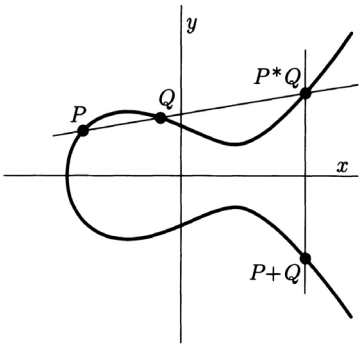
本研究：楕円曲線暗号とECDLP

ECDLP

✓楕円曲線上の有理点全体は
加法について可換群をなす

有理点P
自然数k
→（簡単）
k倍点$[k]P$

有理点P
k倍点$[k]P$
→（困難）
自然数k



出典：[1]

楕円曲線上の離散対数問題（ECDLP）

[1] J. H. Silverman, J. Tate, “Rational Points on Elliptic Curves”

楕円曲線暗号

楕円曲線を用いた暗号方式の総称

楕円曲線暗号の例

- ◆楕円ディジタル署名アルゴリズム（ECDSA）
- ◆楕円Diffie-Hellman鍵共有（ECDH）
- ◆楕円ElGamal暗号

→ ECDLPの
計算量的困難性が
大きく関わる

さまざまな楕円曲線で定義可能

バイナリ楕円曲線

ディジタル署名においてNISTの推奨する楕円曲線

- 素体上の楕円曲線
- $\mathbb{F}_2$の拡大体上の楕円曲線（バイナリ楕円曲線）
- Koblitz曲線

ディジタル署名におけるバイナリ楕円曲線（次数 n ）の式

$$y^2 + xy = x^3 + ax^2 + b \ (a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^*)$$

バイナリ楕円曲線におけるNISTの推奨　…　$n = 163, 233, 283, 571$

5

バイナリ楕円曲線における加算公式

楕円曲線上の有理点 $P(x_1, y_1), Q(x_2, y_2) \in \mathbb{F}_{2^n}^2$ が与えられたとき，

$P + Q = (x_3, y_3) \in \mathbb{F}_{2^n}^2$は以下で与えられる

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$$
$$y_3 = (x_2 + x_3)\lambda + x_3 + y_2$$
$$\left(\lambda = \frac{y_1 + y_2}{x_1 + x_2} \in \mathbb{F}_{2^n}\right)$$

Shorのアルゴリズム

楕円曲線加算 ＞ 量子フーリエ変換

コスト

$\mathbb{F}_{2^n}$上の逆元計算が必要

効率的に量子実装したい

6

既存の効率化

量子アルゴリズムで比較される要素

量子ビット・Toffoliゲート（TOF）・CNOTゲート（CNOT）・深さ

上の量子リソースのトレードオフ関係

バイナリ楕円曲線での先行研究

量子GCD逆元計算（量子ビット・CNOTが少ない）：Banegasら（BBHL21-GCD）

量子FLT逆元計算（TOF・深さが少ない）：Putrantoら（PWLK22-FLT）＊深さ・CNOTを節約
Banegasら（BBHL21-FLT）＊量子ビットを節約

7

結果①（CT-RSA2023）

✓基本アルゴリズム・拡張アルゴリズムを提案

✓NISTの推奨するバイナリ楕円曲線（$n = 163, 233, 283, 571$）について比較

① 基本アルゴリズム：PWLK22-FLTの量子ビット数・CNOT・深さを全てのnについて削減
ex.) $n = 571$ → 量子ビット：-26%　CNOT：-6%

② 拡張アルゴリズム：BBHL21-FLTのCNOT・深さを全てのnについて削減
ex.) $n = 571$ → CNOT：-20%　深さ：-18%

8

結果②（SCIS2023）

- ✓初期化アルゴリズムを提案
- ✓従来手法を一部変更した，量子楕円曲線加算アルゴリズムを提案
- ✓NISTの推奨するバイナリ楕円曲線（$n = 163, 233, 283, 571$）について比較

① 初期化アルゴリズム：
＋提案楕円曲線加算アルゴリズム

TOFゲート数を少ない水準に抑えつつ，
全手法の中で最も少ない量子ビット数を達成
ex.) $n = 571$ → BBHL21-GCD：4,015 ビット
提案手法：3,998 ビット

目次

1. FLT逆元計算
2. Putrantoらの量子FLTアルゴリズムと基本アルゴリズム
3. Banegasらの量子FLTアルゴリズムと拡張アルゴリズム
4. 初期化アルゴリズム
5. 比較
   5.1. 基本アルゴリズム・拡張アルゴリズム
   5.2. 初期化アルゴリズム
6. まとめ・展望

目次

1. FLT逆元計算
2. Putrantoらの量子FLTアルゴリズムと基本アルゴリズム
3. Banegasらの量子FLTアルゴリズムと拡張アルゴリズム
4. 初期化アルゴリズム
5. 比較
   - 5.1. 基本アルゴリズム・拡張アルゴリズム
   - 5.2. 初期化アルゴリズム
6. まとめ・展望

FLT逆元計算①（$n = 163$）

- $f \in \mathbb{F}_{2^{163}}^{*}$ が与えられたときに，f^{-1}を求める

Fermatの小定理の一般化

$$f^{2^{163}-1} = 1$$

$$f^{-1} = f^{2^{163}-2} = \left(f^{2^{162}-1}\right)^{2}$$

◆ $162 = 2^7 + 2^5 + 2^1$ に注意して以下の手順で計算

Step.1：$f^{2^{2^1}-1}, f^{2^{2^2}-1}, \ldots, f^{2^{2^7}-1}$を順次計算

Step.2：$f^{2^{2^7+2^5}-1}, f^{2^{2^7+2^5+2^1}-1}$を順次計算

FLT逆元計算②（$n = 163$）

入力：$f = f^{2^{2^0}-1}$　　出力：$f^{2^{162}-1}$

Step.1：$\left(f^{2^{2^{i-1}}-1}\right)^{2^{2^{i-1}}} \times f^{2^{2^{i-1}}-1} = f^{2^{2^i}-2^{2^{i-1}}} \times f^{2^{2^{i-1}}-1} = f^{2^{2^i}-1}$

$(i = 1,2,\ldots,7)$

Step.2：$\left(f^{2^{2^7}-1}\right)^{2^{2^5}} \times f^{2^{2^5}-1} = f^{2^{2^7+2^5}-2^{2^5}} \times f^{2^{2^5}-1} = f^{2^{2^7+2^5}-1}$

$\left(f^{2^{2^7+2^5}-1}\right)^{2^{2^1}} \times f^{2^{2^1}-1} = f^{2^{2^7+2^5+2^1}-2^{2^1}} \times f^{2^{2^1}-1} = f^{2^{2^7+2^5+2^1}-1}$

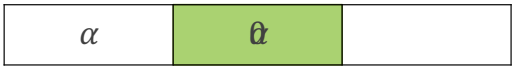
$= 162$

目次

1. FLT逆元計算
2. Putrantoらの量子FLTアルゴリズムと基本アルゴリズム
3. Banegasらの量子FLTアルゴリズムと拡張アルゴリズム
4. 初期化アルゴリズム
5. 比較
   - 5.1. 基本アルゴリズム・拡張アルゴリズム
   - 5.2. 初期化アルゴリズム
6. まとめ・展望

$\mathbb{F}_{2^{163}}$上の量子基本計算のリソース

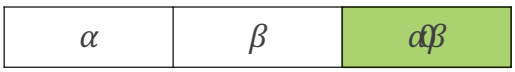
- 加算（Banegasら）



$n = 163$ 量子ビット（1レジスタ）

- 二乗算（Banegasら）

- 乗算（Kimら）



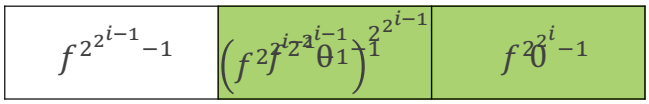
各量子計算と必要なリソース

	TOF	新規レジスタ	CNOT
加算	×	○	○
二乗算	×	×	○
乗算	○	○	○

TOFやレジスタ（量子ビット）を要する加算・乗算に焦点を置く

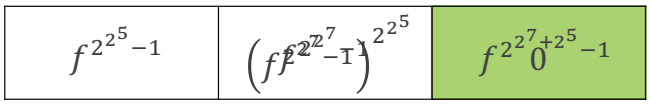
量子FLT逆元計算アルゴリズム（PWLK22-FLT）

Step.1： $\left(f^{2^{2^{i-1}}-1}\right)^{2^{2^{i-1}}} \times f^{2^{2^{i-1}}-1} = f^{2^{2^i}-1} \quad (i = 1,2,\dots,7)$



新しいレジスタを２つ
乗算を１回

Step.2： $\left(f^{2^{2^7}-1}\right)^{2^{2^5}} \times f^{2^{2^5}-1} = f^{2^{2^7}+2^5-2^5} \times f^{2^{2^5}-1} = f^{2^{2^7}+2^5-1}$



新しいレジスタを１つ
乗算を１回

既存手法と加法連鎖列

計算過程 Step.1：$f^{2^{2^0}-1}, f^{2^{2^1}-1}, f^{2^{2^2}-1}, \ldots, f^{2^{2^7}-1}$

Step.2：$f^{2^{2^7+2^5}-1}, f^{2^{2^7+2^5+2^1}-1}$

→ $\{1 = 2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^7 + 2^5, 2^7 + 2^5 + 2^2 = 162\}$

… 162 の加法連鎖列

加法連鎖列

$\{p_0 = 1, p_1, \ldots, p_\ell = N\}$ がNの加法連鎖 ⇔ 任意の $1 \le s \le \ell$ について，ある $0 \le i, j < \ell$ があって $p_s = p_i + p_j$

基本アルゴリズムのアイデア：162の別の加法連鎖列を入力とし，量子リソースを減らす

17

提案基本アルゴリズム

PWLK22-FLTの加法連鎖列$\{p_0 = 1,2,4,8,16,32,64,128,160, p_9 = 162\}$

Step.1の計算：$\{2,4,8,16,32,64,128\}$ … 二倍計算で得られる

Step.2の計算：$\{160,162\}$ … 二倍でない加算で得られる

乗算を9回，新しいレジスタを**16**個

提案基本アルゴリズム

加法連鎖列 $\{p_0 = 1,2,3,6,9,18,27,54,108, p_9 = 162\}$ を用いる

$\{2,6,18,54,108\}$：二倍計算で得られる … Step.1の計算

$\{3,9,27,162\}$ ：二倍でない加算で得られる … Step.2の計算

乗算を9回，新しいレジスタを**14**個

18

加法連鎖列と量子リソース（一般の場合）

◆$f^{2^{n-1}-1}$の計算に$n-1$の加法連鎖列$\{p_s\}_{s=0}^{\ell}$を用いる（n：次数）

□ $p_1, \ldots, p_\ell$のうち，二倍計算で得られる項が d 項，そうでない項が m 項

fから始めて$f^{2^{p_1}-1}, \ldots, f^{2^{p_\ell}-1} = f^{2^{n-1}-1}$を順々に計算する際のコスト

乗算 ℓ 回，新規レジスタ $(2d+m) = (\ell + d)$ 個

良い加法連鎖列：長さが短く，二倍計算で得られる項が少ない

19

目次

1. FLT逆元計算
2. Putrantoらの量子FLTアルゴリズムと基本アルゴリズム
3. Banegasらの量子FLTアルゴリズムと拡張アルゴリズム
4. 初期化アルゴリズム
5. 比較
   - 5.1. 基本アルゴリズム・拡張アルゴリズム
   - 5.2. 初期化アルゴリズム
6. まとめ・展望

20

量子FLT逆元計算アルゴリズム（BBHL21-FLT）

PWLK22-FLT

Step.1： $\left(f^{2^{2^{i-1}}-1}\right)^{2^{2^{i-1}}} \times f^{2^{2^{i-1}}-1} = f^{2^{2^i}-1} \quad (i = 1,2,\dots,7)$

$f^{2^{2^{i-1}}-1}$	$\left(f^{2^{2^{i-1}}-1}\right)^{2^{2^{i-1}}}$	$f^{2^{2^i}-1}$

新しいレジスタを２つ
乗算を１回

BBHL21-FLT

Step.1： $\left(f^{2^{2^{i-1}}-1}\right)^{2^{2^{i-1}}} \times f^{2^{2^{i-1}}-1} = f^{2^{2^i}-1} \quad (i = 1,2,\dots,7)$

$f^{2^{2^{i-1}}-1}$	$\left(f^{2^{2^{i-1}}-1}\right)^{2^{2^{i-1}}}$	$f^{2^{2^i}-1}$

新しいレジスタを１つ
乗算を１回

提案拡張アルゴリズム

- BBHL21-FLT： PWLK22-FLTのStep.1における
  コピー先のレジスタを使い回す

入力：任意の加法連鎖

提案拡張アルゴリズム

BBHL21-FLT ：1 個のレジスタを使い回す

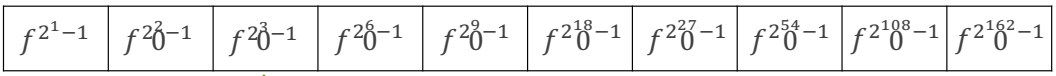
提案拡張アルゴリズム：L 個のレジスタを使い回す → L を動かすと量子ビットとCNOT・深さのトレードオフ

目次

1. FLT逆元計算
2. Putrantoらの量子FLTアルゴリズムと基本アルゴリズム
3. Banegasらの量子FLTアルゴリズムと拡張アルゴリズム
4. 初期化アルゴリズム
5. 比較
   - 5.1. 基本アルゴリズム・拡張アルゴリズム
   - 5.2. 初期化アルゴリズム
6. まとめ・展望

提案初期化アルゴリズム①

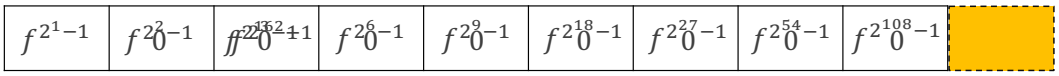
拡張アルゴリズム（補助レジスタ数：9）



f^{2^9-1}の計算以降は使われない

f^{2^9-1}を計算した後は
f^{2^3-1}を消してしまって良い

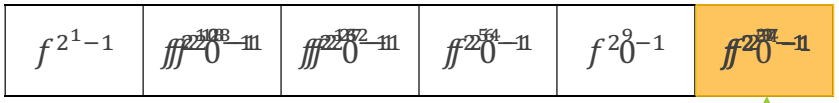
f^{2^3-1}の初期化（補助レジスタ数：8）



拡張アルゴリズムから1レジスタ（n 量子ビット）節約

提案初期化アルゴリズム②

$f^{2^6-1} \to f^{2^3-1} \to f^{2^2-1} \to f^{2^{27}-1} \to f^{2^{18}-1}$の順に初期化（補助レジスタ数：5）



①逆元計算以外で再利用できないか？

既存の量子楕円曲線加算アルゴリズムを変更することで
補助レジスタとして利用可能に

②さらに減らすことはできるのか？

後述

25

目次

1. FLT逆元計算
2. Putrantoらの量子FLTアルゴリズムと基本アルゴリズム
3. Banegasらの量子FLTアルゴリズムと拡張アルゴリズム
4. 初期化アルゴリズム
5. 比較
   - 5.1. 基本アルゴリズム・拡張アルゴリズム
   - 5.2. 初期化アルゴリズム
6. まとめ・展望

26

目次

1. FLT逆元計算
2. Putrantoらの量子FLTアルゴリズムと基本アルゴリズム
3. Banegasらの量子FLTアルゴリズムと拡張アルゴリズム
4. 初期化アルゴリズム
5. 比較
   5.1. 基本アルゴリズム・拡張アルゴリズム
   5.2. 初期化アルゴリズム
6. まとめ・展望

比較の条件

✓加法連鎖列：　長さ（TOF）を最小にする列の中で
二倍算回数（量子ビット数）が最小になるもの

- $n = 163, 233, 283, 571$
- 項目：TOF・量子ビット・CNOT・深さ（上界）
- 条件：Shorのアルゴリズム１回

基本・拡張アルゴリズムで用いる加法連鎖列

$n = 163$

	$\{\tilde{p}_s^{163}\}_{s=0}^{9}$	提案
ℓ	9	9
d	7	5

$n = 233$

	$\{\tilde{p}_s^{233}\}_{s=0}^{10}$	提案
ℓ	10	10
d	7	4

$n = 283$

	$\{\tilde{p}_s^{283}\}_{s=0}^{10}$	提案
ℓ	11	11
d	8	3

従来と同じ長さだが，二倍算回数が少ない加法連鎖列を発見

$n = 571$

	$\{\tilde{p}_s^{571}\}_{s=0}^{13}$	提案
ℓ	13	12
d	9	4

従来より短く，二倍算回数も少ない加法連鎖列を発見

Shorのアルゴリズムでの比較（$n = 163$）

$n = 163$（長さが先行研究と同じで，二倍算が少ない加法連鎖列）

	TOF	量子ビット	CNOT	深さ
基本アルゴリズム	13,175,432	2,772	1,072,118,184	204,448,960
PWLK22-FLT	13,175,432	3,098	1,072,545,896	204,451,584
拡張アルゴリズム	13,175,432	1,957	1,086,823,080	210,949,920
BBHL21-FLT	13,175,432	1,957	1,101,105,512	231,735,936
BBHL21-GCD	288,641,640	1,157	322,348,232	342,017,408

基本
- TOFは変わらず，量子ビット・CNOT・深さが減少

拡張
- TOF・量子ビットは変わらず，CNOT・深さが減少

Shorのアルゴリズムでの比較 ($n = 571$)

$n = 571$ （長さが先行研究より短い加法連鎖列）

	TOF	量子ビット	CNOT	深さ
基本アルゴリズム	**228,787,416**	10,850	55,651,292,840	8,000,884,320
PWLK22-FLT	246,235,704	14,276	59,611,633,224	8,283,571,296
拡張アルゴリズム	**228,787,416**	**8,566**	55,778,093,800	8,053,979,648
BBHL21-FLT	246,235,704	9,137	61,566,056,552	10,217,128,064
BBHL21-GCD	10,156,396,536	4,015	13,091,280,488	12,963,368,704

基本
- 量子ビット・CNOT・深さだけでなくTOFも減少

拡張
- CNOT・深さだけでなくTOF・量子ビットも減少

31

目次

1. FLT逆元計算
2. Putrantoらの量子FLTアルゴリズムと基本アルゴリズム
3. Banegasらの量子FLTアルゴリズムと拡張アルゴリズム
4. 初期化アルゴリズム
5. 比較
   - 5.1. 基本アルゴリズム・拡張アルゴリズム
   - 5.2. 初期化アルゴリズム
6. まとめ・展望

32

比較（量子ビット数）

比較条件
- $n = 163, 233, 283, 571$について，BBHL21-GCD及び拡張アルゴリズムと比較
- 加法連鎖列は，各 n について最短となるものを用いる

■提案手法の使用する補助レジスタ数

➢ 全ての n について，発見できたものでは5レジスタが最小

1回の逆元計算における量子ビット数比較

	$n = 163$	$n = 233$	$n = 283$	$n = 571$
BBHL21-GCD	830	1,180	1,431	2,872
拡張アルゴリズム	1,630	2,563	3,396	7,423
提案手法	978	1,398	1,698	3,426

提案FLT逆元計算による量子ビット節約

Shorのアルゴリズムにおける量子ビット数比較

	$n = 163$	$n = 233$	$n = 283$	$n = 571$
BBHL21-GCD	1,157	1,647	1,998	4,015
拡張アルゴリズム	1,957	3,030	3,963	8,566
提案手法	1,142	1,632	1,982	3,998

楕円曲線加算の変更による量子ビット節約

33

Shorのアルゴリズムでの比較（$n = 571$）

Shorのアルゴリズムにおける量子ビット数・TOFゲート数・CNOTゲート数・深さの比較（$n = 571$）

	量子ビット	TOF	CNOT	深さ
BBHL21-GCD	4,015	10,156,396,536	13,091,280,488	12,963,368,704
拡張アルゴリズム	8,566	228,787,416	55,778,093,800	8,053,979,648
提案手法	3,998	368,373,720	93,673,235,656	16,669,416,192

◆全ての n について量子ビット数最小を達成

◆BBHL21-GCDと比較して，TOFゲート数を大幅に削減しているもののCNOTゲート数・深さは増加

◆拡張アルゴリズムと比較して，量子ビット数は半分以下となったがその他の量子リソースは全て増加

□ KimらのGCDが，BBHL21-GCDからCNOTゲート数を増やして3,473 量子ビットを達成

34

目次

1. FLT逆元計算
2. Putrantoらの量子FLTアルゴリズムと基本アルゴリズム
3. Banegasらの量子FLTアルゴリズムと拡張アルゴリズム
4. 初期化アルゴリズム
5. 比較
   - 5.1. 基本アルゴリズム・拡張アルゴリズム
   - 5.2. 初期化アルゴリズム
6. まとめ・展望

まとめ

既存の量子FLT逆元計算を加法連鎖の観点から再評価

✓提案基本アルゴリズム … PWLK22-FLTのTOFを変えず
量子ビット・CNOT・深さを削減

✓提案拡張アルゴリズム … BBHL21-FLTのTOF・量子ビットを変えず
CNOT・深さを削減

✓提案初期化アルゴリズム … GCD・FLT全ての従来手法の中で
＋提案楕円曲線加算アルゴリズム 最小の量子ビット数を達成

展望

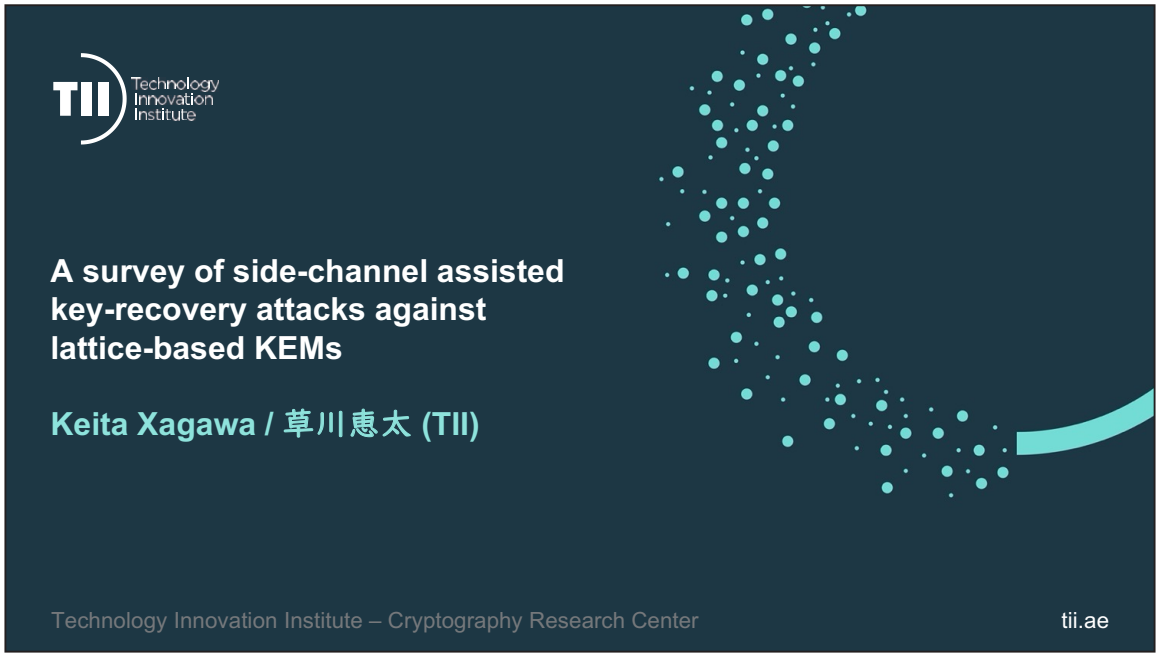
- CNOTゲートや深さがより少ない加法連鎖列の探索
- 初期化アルゴリズムで使用する補助レジスタ数の下限導出
- Koblitz曲線にフォーカスした量子楕円曲線加算アルゴリズムの考案

格子ベースの鍵カプセル化方式に対するサイドチャネル攻撃を利用した鍵回復攻撃

草川 恵太

Technology Innovation Institute
keita.xagawa@tii.ae

量子計算機の開発の進展を受け、耐量子計算機暗号（PQC）の標準化や実装が盛んになっている。大きな影響を持つ NIST の PQC 標準化では、サイズ・速度・安全性といった観点から鍵カプセル化方式（KEM）として格子暗号の Kyber が選ばれた。一方、標準化される暗号は様々な機器で実装されることから、サイドチャネル攻撃耐性も重要視される。本発表では Kyber を中心とした格子暗号に対するサイドチャネル攻撃を利用した鍵回復攻撃を、紹介する。特に、サイドチャネル攻撃を用いて平文判定オラクルや復号オラクルを構築した後の、攻撃の効率化について紹介する。



自己紹介

草川　恵太（Keita Xagawa）

経歴

- 2010 東京工業大学　博士（理学）
- 2010 NTT入社
- 2023 Technology Innovation Institute

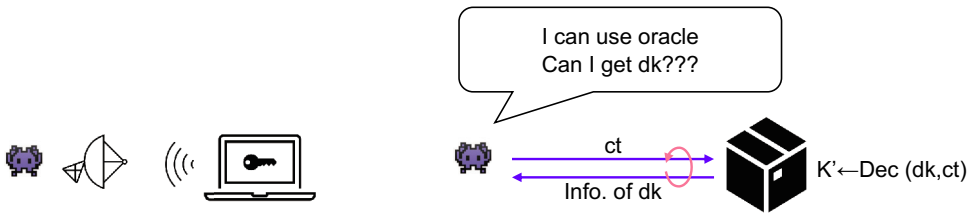
研究内容

- 耐量子計算機暗号 (PQC)・プロトコルの設計・解析など
- 量子ランダムオラクルを使った安全性証明など

SCA-assisted Key-Recovery Attack

1. Implement oracle leaking secret

2. Mount key-recovery attack using the oracle



Agenda

- Introduction
- KEM and FO
- Side-channel analysis
- PKE and K-PKE
- Key-recovery attack using plaintext-checking oracle
- Key-recovery attack using decryption oracle

NIST's PQC: Draft of Standards

1. FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*
   ML-KEM a.k.a. (CRYSTALS-)Kyber
2. FIPS 204, *Module-Lattice-Based Digital Signature Standard*
   ML-DSS a.k.a. (CRYSTALS-)Dilithium
3. FIPS 205, *Stateless Hash-Based Digital Signature Standard*
   SH-DSS a.k.a. SPHINCS+
4. FIPS ???, ???
   ??-DSS a.k.a. Falcon

ML-KEM a.k.a. Kyber

- Based on Module Lattice
- Obtained by applying FO_{KEM} to K-PKE
- Efficient

	|ek|	|dk|	|ct|	gen	encaps	decaps
ML-KEM-512	800	1632	768	18k	29k	22k
ML-KEM-768	1184	2400	1088	32k	44k	34k
ML-KEM-1024	1568	3168	1568	42k	59k	46k
RSA-KEM-2048 (e=3)	256	384	256	**109032k	14k	2540k
Curve25519	32	32	32	121k	160k	160k

Taken from SUPERCOP "amd64; Ice Lake (706e5); 2019 Intel Core i3-1035G1; 4 x 1000MHz;". Sizes are in bytes. Speeds are in cycles
*: sk = (p, q, pinv). **: Median

KEM and ML-KEM

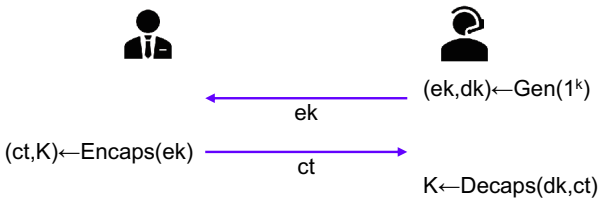
KEM – Key Encapsulation Mechanism

Syntax:

$Gen(1^k) \rightarrow (ek,dk)$

$Encaps(ek) \rightarrow (ct,K)$

$Decaps(dk,ct) \rightarrow K/\perp$



IND-CCA Security:

$(ek, Encaps(ek)) \sim_c (ek, Encaps(ek)_1, U(K))$
where A can access to Decaps oracle

FO_{KEM} [FO99,HHK17,JZCWM18,…]

KEM = FO_{KEM}[PKE,G,H]:

Encaps(ek;x):

- ct=Enc(ek,x;G(x))
- K=H(x)

Decaps(dk,ct):

1. x'←Dec(dk,ct)
2. if Enc(ek,x';G(x'))=ct
3. then return K=H(x')
4. else return K=H'(s,ct) or ⊥

Adapted version [FO99]:

FO_{KEM} is IND-CCA in ROM
if PKE is OW-CPA (and some)

New techniques for PQC

[HHK17,JZCWM18,SXY18,HKSU20,JZM19,XY19,LW21] HU, HFO

[Zhandry19,…] Explicit Rejection

Kyber in Round 3 vs. ML-KEM

Kyber in Round 3:

Use dedicated FO_{KEM}

IND-CCA in QROM is not proven! [GMP23]

Dedicated proofs [CLJL23,MX23,BH23]

ML-KEM:

Use FO_{KEM}

IND-CCA in QROM is proven [HHK17, etc]

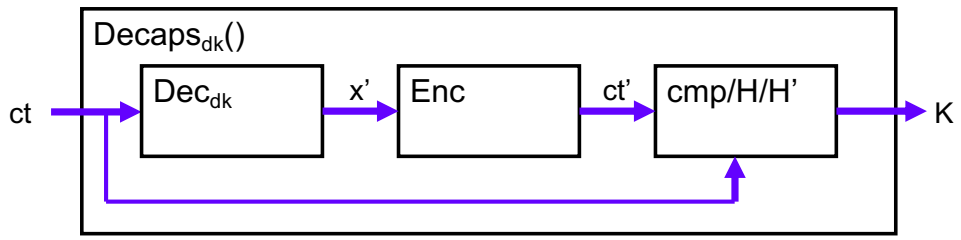
[GMP23] Grubbs, Maram, and Paterson (EUROCRYPT2023)
[CLJL23] Chen, Lu, Jia, and Li (Inscrypt2022)
[MX23] Maram and X (PKC2023)
[BH23] Barbosa and Hülsing (EPRINT2023/755)

SCA and Oracles (KMO/PCO/FDO)

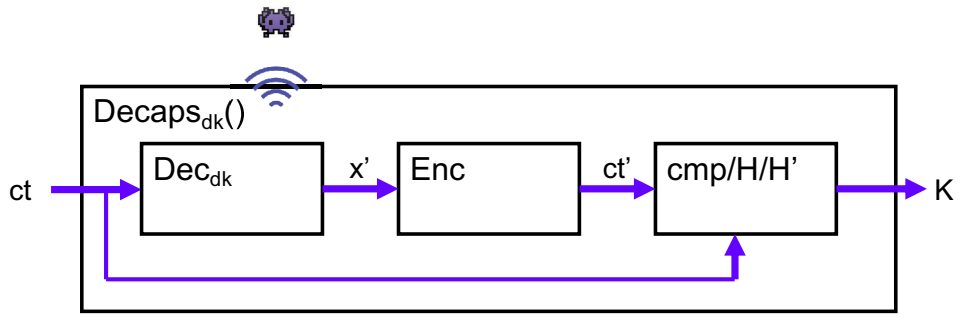
Decaps and Side-Channel Analysis

Decaps(dk,ct):

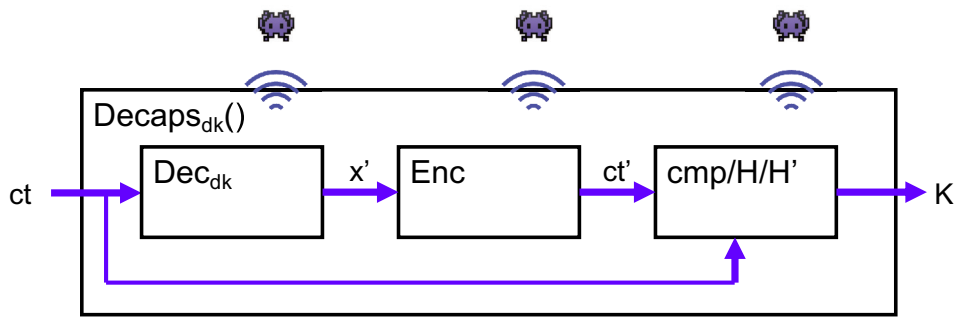
1. x'←Dec(dk,ct)
2. if Enc(ek,x';G(x'))=ct return K=H(x') else return K=H'(s,ct) or ⊥



Direct Attack (Obtain dk from traces)



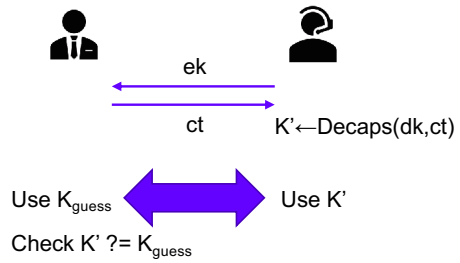
Non-Direct Attack (Implement Oracle)



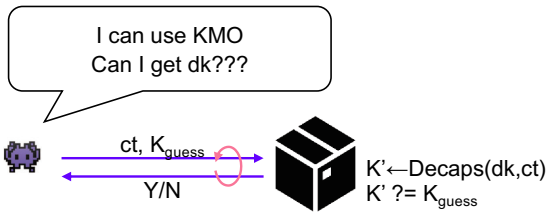
Key-Mismatch Oracle (KMO)

Key-Mismatch Oracle:

e.g., key exchange w/ fixed secret



KRA-KMO against KEM



Plaintext-Checking Oracle (PCO)

Plaintext-Checking Oracle:

KEM w/ FO and KE w/ fixed secret

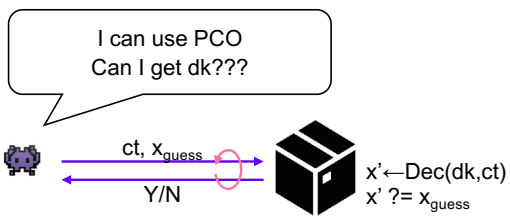
→ KMO checks K'?=K_{guess}

→ We can check H(x')?=H(x_{guess})

→ We can implement PCO of PKE

Ref: OW-PCA [OP01]

KRA-PCO against PKE



Faulty Decapsulation Oracle (FDO)

Faulty Decapsulation Oracle:

KEM w/ FO_{KEM}

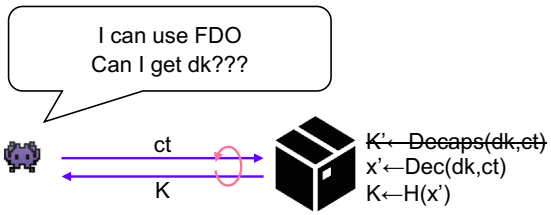
Decapsulation ignores the validity test

FDO always returns H(x')

e.g.: [XIU+21] FIA to skip "if" of FO_{KEM}

Cf. PCO ≪ FDO ≪ DO

KRA-FDO against KEM/PKE



Technology Innovation Institute

PKE and K-PKE

tii.ae

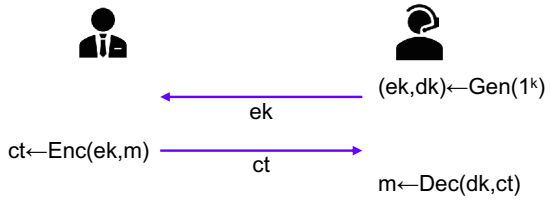
PKE – Public-Key Encryption

Syntax:

Gen(1^k)→(ek,dk)

Enc(ek,m)→ct

Dec(dk,ct)→m/⊥



IND-CPA Security:

(ek, Enc(ek,m_0)) ~$_c$ (ek, Enc(ek,m_1))

Kyber.CPAPKE-512 (K-PKE-512 in FIPS 203 Draft)

Parameters:

$\mathcal{R}_q=\mathbb{Z}_q[x]/(x^{256}+1)$ w/ q = 3329

Ψ_3= CBD(1/2,6) over $[-3,+3]^{256}$

Gen(pp):

A←$\mathcal{R}_q^{2\times 2}$, s, d←$\Psi_3^2$, B=As+d

ek = (A,B), dk = s

Enc(ek,μ; t,e,f): μ in $\{0,1\}^{256}$

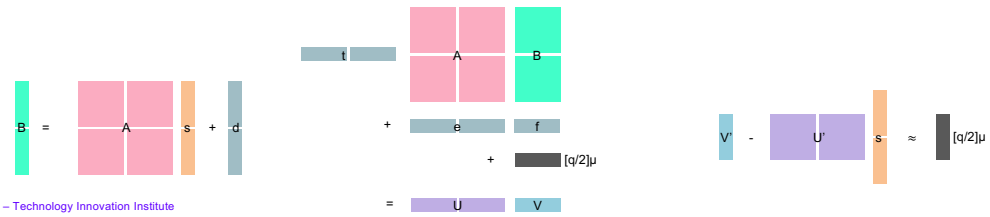
U = tA + e, V = tB + f + decmp$_1$(μ)

ct=(c_1,c_2) = (cmp$_{10}$(U),cmp$_4$(V))

Dec(dk,ct):

(U',V') = (decmp$_{10}$(c_1), decmp$_4$(c_2))

μ' = cmp$_1$(V'-U's)



$\mathcal{R}_q=\mathbb{Z}_q[x]/(x^{256}+1)$?

$\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$

$\mathbb{Z}_q[x] = \{a_0+a_1x+a_2x^2+\ldots : a_i \text{ in } \mathbb{Z}_q\}$

Quotient ring modulo the ideal $(x^{256}+1)$

ex. $x^{257}+1 = x \cdot x^{256}+1 = -x+1$

ex. $-x^{258}+2 = -x^2x^{256}+2 = x^2+2$

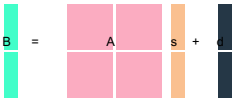
Let

$a = a_0+a_1x+a_2x^2+\ldots+a_{255}x^{255}$

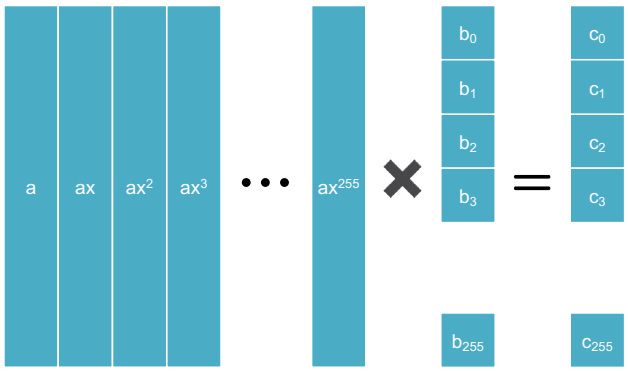
$b = b_0+b_1x+b_2x^2+\ldots+b_{255}x^{255}$

$c = c_0+c_1x+c_2x^2+\ldots+c_{255}x^{255}$

How to compute c = a * b



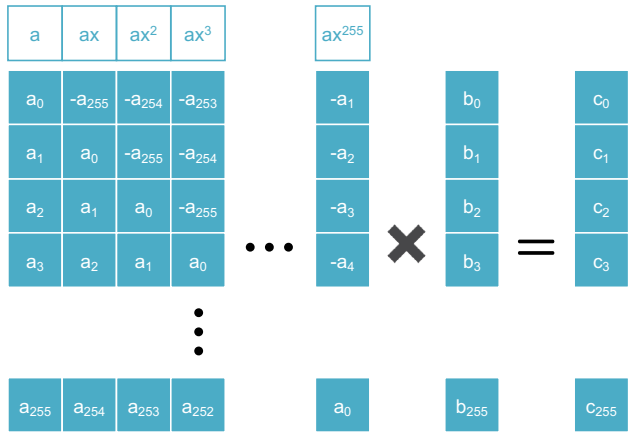
a*b = c in $\mathcal{R}_q=\mathbb{Z}_q[x]/(x^{256}+1)$



$a = a_0+a_1x+a_2x^2+\ldots+a_{255}x^{255}$
$b = b_0+b_1x+b_2x^2+\ldots+b_{255}x^{255}$
$c = c_0+c_1x+c_2x^2+\ldots+c_{255}x^{255}$

$c = a * b = \sum_{i=0..255} ax^i\, b_i$
$x^{256} = -1 \in \mathcal{R}_q$

a*b = c in $\mathcal{R}_q=\mathbb{Z}_q[x]/(x^{256}+1)$



$a = a_0+a_1x+a_2x^2+\ldots+a_{255}x^{255}$
$b = b_0+b_1x+b_2x^2+\ldots+b_{255}x^{255}$
$c = c_0+c_1x+c_2x^2+\ldots+c_{255}x^{255}$

$c = a * b = \sum_{i=0..255} a x^i b_i$
$x^{256} = -1 \in \mathcal{R}_q$

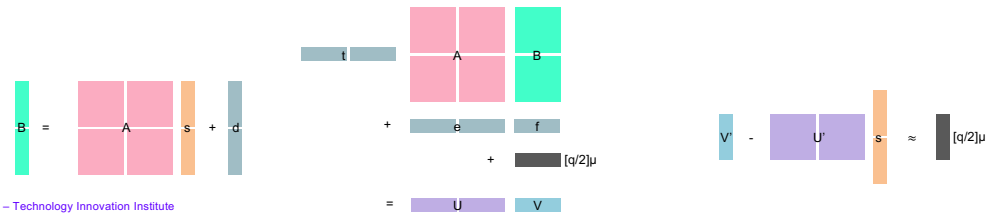
Kyber.CPAPKE-512 (K-PKE-512 in FIPS 203 Draft)

Parameters:
$\mathcal{R}_q=\mathbb{Z}_q[x]/(x^{256}+1)$ w/ q = 3329
Ψ_3= CBD(1/2,6) over $[-3,+3]^{256}$

Gen(pp):
$A \leftarrow \mathcal{R}_q^{2\times 2}$, s, $d \leftarrow \Psi_3^2$, B=As+d
ek = (A,B), dk = s

Enc(ek,μ; t,e,f): μ in $\{0,1\}^{256}$
U = tA + e, V = tB + f + $decmp_1(\mu)$
ct=(c_1,c_2) = (cmp_{10}(U),cmp_4(V))

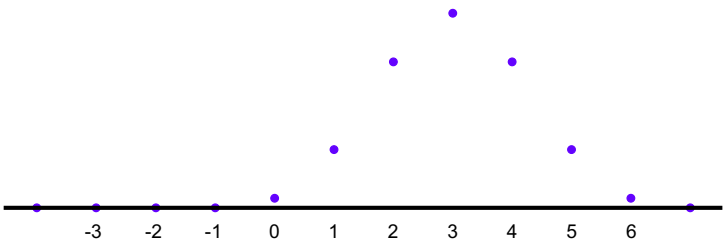
Dec(dk,ct):
(U',V') = ($decmp_{10}(c_1)$, $decmp_4(c_2)$)
μ' = cmp_1(V'-U's)



CBD: centered binary distribution

Ψ_3= CBD(1/2,6) over $[-3,+3]^{256}$ Blue: BD(1/2,6)

BD(1/2,n): # heads of n coin flips



CBD: centered binary distribution

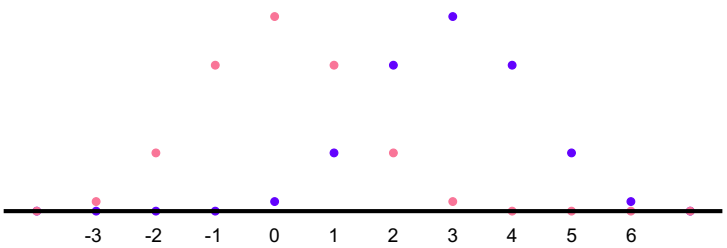
Ψ_3= CBD(1/2,6) over $[-3,+3]^{256}$

BD(1/2,n): # heads of n coin flips

CBD(1/2,n): BD(1/2,n) – n/2

Blue: BD(1/2,6)
Pink: CBD(1/2,6)

	-3	-2	-1	0	1	2	3
pr.	1/64	6/64	15/64	20/64	15/64	6/64	1/64



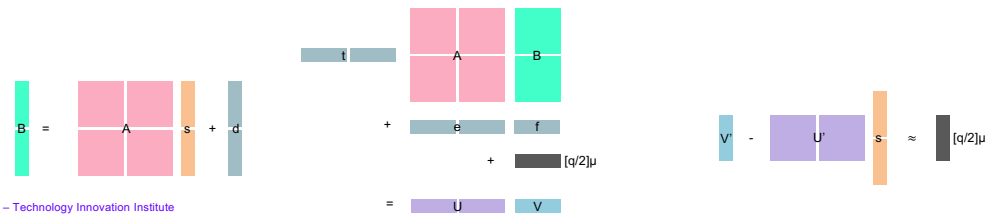
Kyber.CPAPKE-512 (K-PKE-512 in FIPS 203 Draft)

Parameters:
$\mathcal{R}_q=\mathbb{Z}_q[x]/(x^{256}+1)$ w/ q = 3329
Ψ_3= CBD(1/2,6) over $[-3,+3]^{256}$

Gen(pp):
$A \leftarrow \mathcal{R}_q^{2\times 2}$, s, $d \leftarrow \Psi_3^2$, B=As+d
ek = (A,B), dk = s

Enc(ek,μ; t,e,f): μ in $\{0,1\}^{256}$
U = tA + e, V = tB + f + $\text{decmp}_1(\mu)$
ct=(c_1,c_2) = (cmp_{10}(U),cmp_4(V))

Dec(dk,ct):
(U',V') = ($\text{decmp}_{10}(c_1)$, $\text{decmp}_4(c_2)$)
μ' = cmp_1(V'-U's)



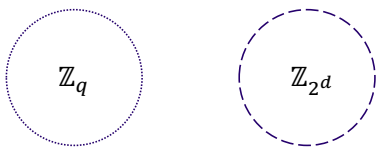
comp, decomp, correctness

$\text{near} : \mathbb{Q} \to \mathbb{Z} : x \mapsto \lfloor x + 1/2 \rfloor$

$\text{cmp}_d : \mathbb{Z}_q \to \mathbb{Z}_{2^d} : x \mapsto \text{near}\left((2^d/q)x\right)$

$\text{decmp}_d : \mathbb{Z}_{2^d} \to \mathbb{Z}_q : x \mapsto \text{near}\left((q/2^d)x\right)$

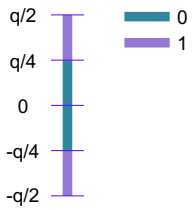
$\left[\text{decmp}_d(\text{cmp}_d(x)) - x\right] \bmod q \le q/2^{d+1}$



q=3329

θ_i = $\text{decmp}_1(0)$ or $\text{decmp}_1(1)$
= 0 or 1665

cmp_1(a) for a in [-1664,1664]
= 0 if -832 <= a <= 832
= 1 o.w.



correctness

Let θ = $decmp_1(\mu)$. q = 3329

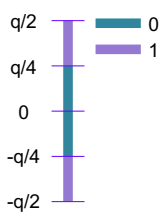
Gen:
B = As+d

Enc:
U = tA + e, V = tB + f + θ
$(c_1,c_2) = (cmp_{10}(U),cmp_4(V))$

Dec:
$(U',V') = (decmp_{10}(c_1), decmp_4(c_2))$
$\mu' = cmp_1(V'-U's)$

$U' = U+e_u$, $V' = v+e_v$ w/ short e_u,e_v

q=3329
$\theta_i = decmp_1(0)$ or $decmp_1(1)$ = 0 or 1665
$cmp_1(a)$ for a in [-1664,1664]
= 0 if -832 <= a <= 832
= 1 o.w.



V'-U's
$= tB+f+\theta+e_v-(tA+e+e_u)s$
$= t(As+d)+f+\theta+e_v-(tA+e+e_u)s$
$= \theta + (td + f + e_v - es + e_us)$
ß~ θ + err.

If err is small, then PKE is corerct.

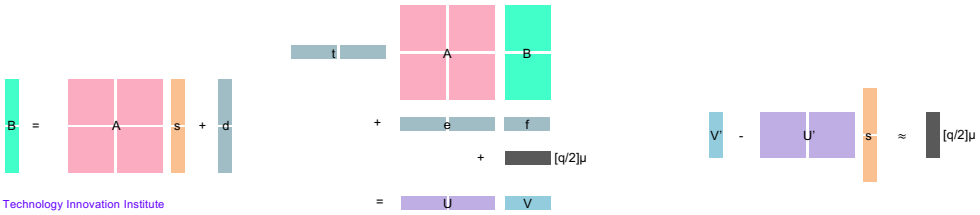
CPA security

Parameters:
$\mathcal{R}_q=\mathbb{Z}_q[x]/(x^{256}+1)$ w/ q = 3329
Ψ_3= CBD(1/2,6) over $[-3,+3]^{256}$

Gen(pp):
$A \leftarrow \mathcal{R}_q^{2\times 2}$, s, $d \leftarrow \Psi_3^2$, B=As+d
ek = (A,B), dk = s

Enc(ek,μ; t,e,f): μ in $\{0,1\}^{256}$
U = tA + e, V = tB + f + $decmp_1(\mu)$
$ct=(c_1,c_2) = (cmp_{10}(U),cmp_4(V))$

CPA security:
1. (A,B) ~$_c$ (A, random): ML-LWE
2. (U,V) ~$_c$ (random, random): ML-LWE



Technology Innovation Institute

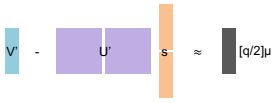
Example: Kyber-512

tii.ae

KRA-PCO against Kyber-512 *Round-3*

Kyber-512's PKE:

- $\mathcal{R}_q = \mathbb{Z}_q[x]/(x^{256}+1)$
- $\Psi_3 =$ CBD over $[-3,+3]^{256}$
- Dec(dk,ct): s←Ψ_3^2
  1. **(U',V')=(decmp$_{10}$(c$_1$), decmp$_4$(c$_2$))**
  2. **μ' = cmp$_1$(V'-U's) mod 2**



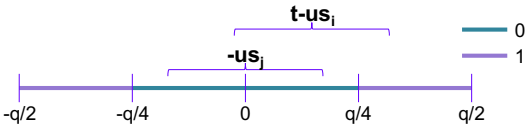
Idea [HV20] for Kyber-512 Round-2**:**

Consider c$_1$=cmp$_{10}$(u,0), c$_2$=cmp$_4$(t)

μ$_i$' = cmp$_1$(t - u s$_i$)

μ$_j$' = cmp$_1$(-u s$_j$)

Determine s$_i$ by checking μ$_i$'



[HV20] Huguenin-Dumittan and Vaudenay (ACNS2020)
[XIU+21] X, Ito, Ueno, Takahashi, Homma (ASIACRYPT2021)

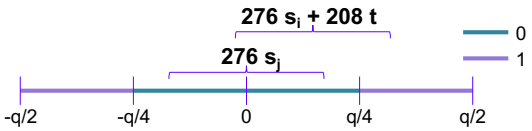
Behavior of μ_i' w/ u=-276

For Kyber-512 Round-3 [XIU+21]:

Consider U=(-276,0), V = 208t x^i

$\mu_i' = cmp_1(276\ s_i + 208\ t)$
$\mu_j' = cmp_1(276\ s_j)$

Determine s_i by checking if
μ' =0…010…0 or 0…000…0



(a) Kyber512

sk_i \ t	−3	−2	−1	0	1	2	3
−3	1	1	1	0	0	0	0
−2	1	1	0	0	0	0	0
−1	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0
+1	0	0	0	0	0	0	1
+2	0	0	0	0	0	1	1
+3	0	0	0	0	1	1	1

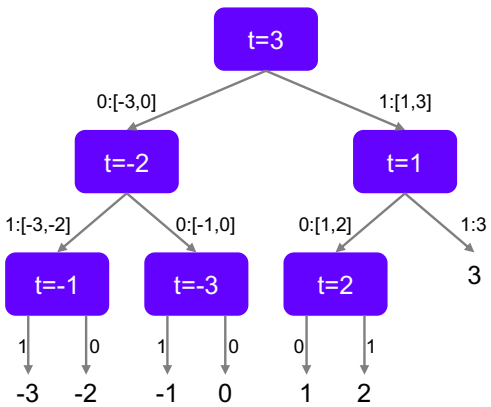
[HV20] Huguenin-Dumittan and Vaudenay (ACNS2020)
[XIU+21] X, Ito, Ueno, Takahashi, Homma (ASIACRYPT2021)

KRA-PCO – #Q1

3 queries determine sk_i in [-3,+3]

sk_i \ t	−3	−2	−1	0	1	2	3
−3	1	1	1	0	0	0	0
−2	1	1	0	0	0	0	0
−1	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0
+1	0	0	0	0	0	0	1
+2	0	0	0	0	0	1	1
+3	0	0	0	0	1	1	1

U = (-276,0), V = 208t x^i, $c_1 = cmp_{10}(U)$, $c_2 = cmp_4(V)$



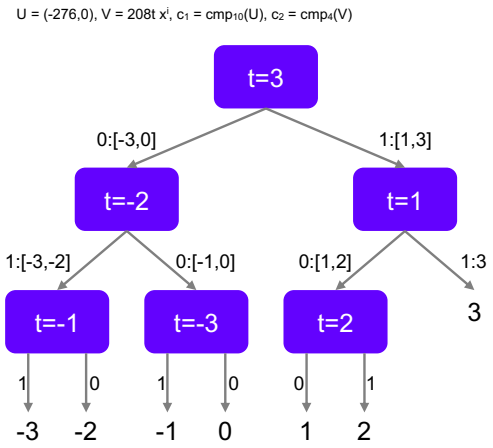
KRA-PCO – #Query (contd.)

3 queries determine sk_i in [-3,+3]
in the worst case (#Q1=3)

sk = s←Ψ_3^2 has 256*2 coefficients

→ #Query = 512 * #Q1 = 1536
in the worst case

1. Decide s_1 by U = (u,0) w/ 256*#Q1 queries
    1. For i in [0,255]: decide s_{1j} by V=208tx^i
2. Decide s_2 by U = (0,u) w/ 256*#Q1 queries
    1. For i in [0,255]: decide s_{2j} by V=208tx^i



Plaintext-Checking Oracle (PCO) from SCA

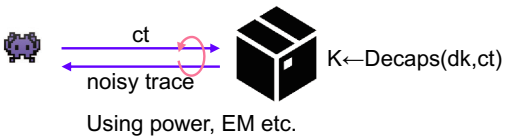
Implement PCO by SCA:

What we need:
Checking if μ_i' ?= 1 and others' = 0

How to implement PCO

1. All 0 or Random
2. All 0 or e_i for i in [0,255]
3. All 0 or e_0

SCA



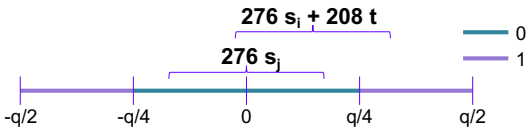
In general, all 0 or e_0 is better

Learning s_i via μ_0'

Idea [TUX+23] inspired by [OUKT21]:
U=(-276,0) for i=0
U=(276 x^{256-i},0) for i≠0
V = 208t

μ_0'= cmp_1(276 s_i + 208 t)

μ_j' = cmp_1(276 s_j)



(a) Kyber512

sk_i \ t	−3	−2	−1	0	1	2	3
−3	1	1	1	0	0	0	0
−2	1	1	0	0	0	0	0
−1	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0
+1	0	0	0	0	0	0	1
+2	0	0	0	0	0	1	1
+3	0	0	0	0	1	1	1

[HV20] Huguenin-Dumittan and Vaudenay (ACNS2020)
[TUX+23] Tanaka, Ueno, X, Ito, Takahashi, Homma (TCHES2023(3))
[OUKT21] Osumi, Uemura, Kudo, Takagi (SCIS 2021)

Technology Innovation Institute

Optimizing #Queries

tii.ae

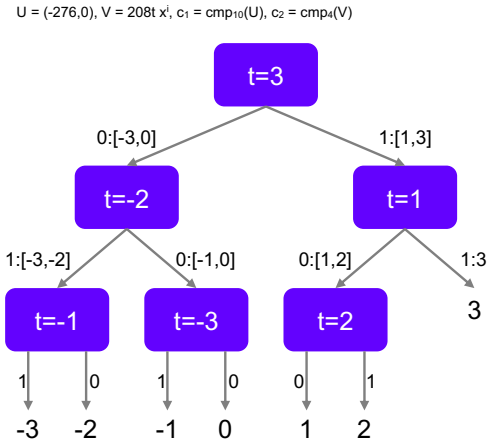
Optimizing #Queries

#Q1 = 3
in the worst case

Q: can we reduce #queries
in the average case?

The distribution of sk_i is CBD(1/2,6)

sk_i	-3	-2	-1	0	1	2	3
pr.	1/64	6/64	15/64	20/64	15/64	6/64	1/64

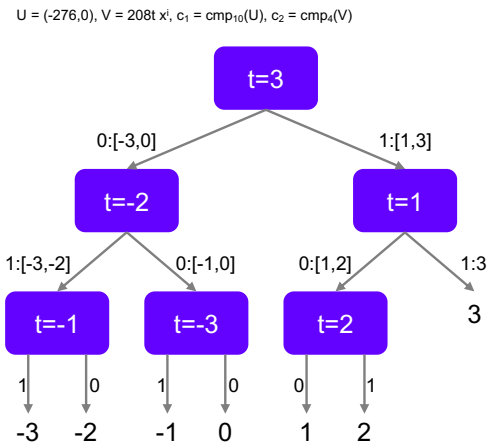


E.g.: E(#Q1)

sk_i	-3	-2	-1	0	1	2	3
pr.	1/64	6/64	15/64	20/64	15/64	6/64	1/64
d	3	3	3	3	3	3	2

E(#Q1)
= 3*63/64 + 2*1/64 = 2.9843..

E(#Query)=512*E(#Q1)=1528



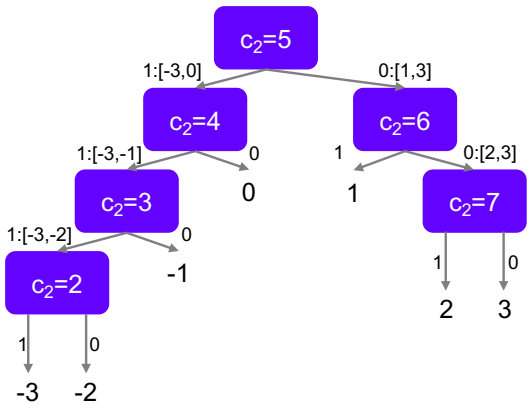
[QCZ+21] BDT by Huffman Coding

sk_i	-3	-2	-1	0	1	2	3
pr.	1/64	6/64	15/64	20/64	15/64	6/64	1/64
d	4	4	3	2	2	3	3

E(#Q1)
= 4*7/64 + 3*22/64 + 2*35/64 = 2.5625

E(#Query)=512*E(#Q1)=1312

U = (208,0), $c_1 = cmp_{10}(U)$, c_2 in {2,…7}



[QCZ+21] Qin, Cheng, Zhang, Pan, Hu, and Ding (ASIACRYPT2021)
https://github.com/AHaQY/Key-Mismatch-Attack-on-NIST-KEMs

Open Problem: more optimization

sk_i	-3	-2	-1	0	1	2	3
pr.	1/64	6/64	15/64	20/64	15/64	6/64	1/64
d	4	4	2	2	2	4	4

E(#Q1) = 4*14/64 + 2*50/64 = 2.4375

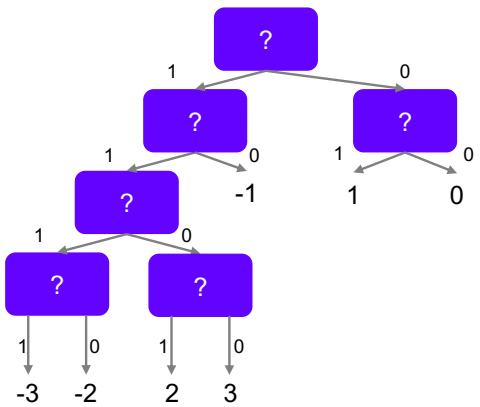
E(#Query)=512*E(#Q1)=1248

Can we design such tests?

Huffman Bound ~ 1216 [QCZ+21]

Shannon Bound ~ 1195 [GM23]

($H(sk_i)$ ~ 2.3334)



[QCZ+21] Qin, Cheng, Zhang, Pan, Hu, and Ding (ASIACRYPT2021)
[GM23] Guo and Mårtensson (PQCrypto2023)

Technology Innovation Institute

Tests P-bits in Parallel

tii.ae

Reducing #Query

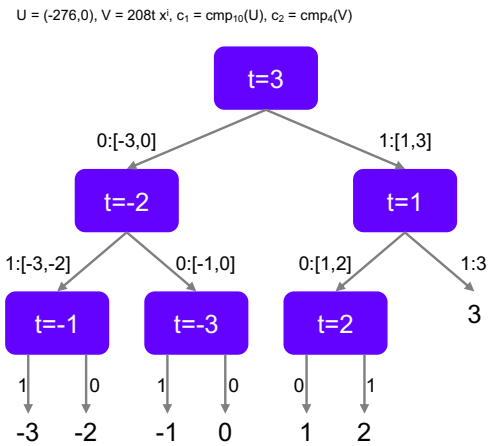
#Q1 = 3 *in the worst case*

sk = s←Ψ_3^2 has 256*2 coefficients

→ #Query = 512 * #Q1 = 1536
in the worst case

Q: Can we reduce #Query?

→ Test in parallel



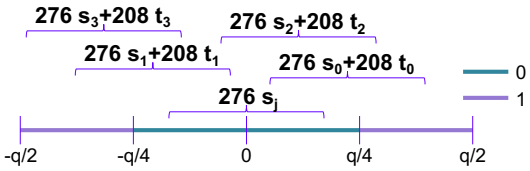
P-parallel test

Idea [TUX+23,RRD+23,etc]:

U=(-276,0), V = $208(t_0+t_1x+t_2x^2+t_3x^3)$

$\mu_i' = cmp_1(276\ s_i + 208\ t)$ (i=0,1,2,3)
$\mu_j' = cmp_1(276\ s_j)$

→ Determine $s_{0,\dots,}s_3$ by checking
μ' ?= 0000 0…0/…/1111 0…0



[TUX+23]:

Implement MV-PCO

Consider P-parallel test

→ #Q = 2*#Q1*ceil(256/P)~1536/P
in the worst case

Trade-off between 2^P and #traces

[XIU+21] X, Ito, Ueno, Takahashi, Homma (ASIACRYPT2021) for ntrulpr
[TUX+23] Tanaka, Ueno, X, Ito, Takahashi, Homma (TCHES2023(3))
[RRD+23] Rajendran, Ravi, D'Anvers, Bhasin, Chattopadhyay (TCHES2023(2))

[RRD+23] Observation on Parallel BDT in [QCZ+21]

sk_i	-3	-2	-1	0	1	2	3
pr.	1/64	6/64	15/64	20/64	15/64	6/64	1/64
d	4	4	3	2	2	3	3

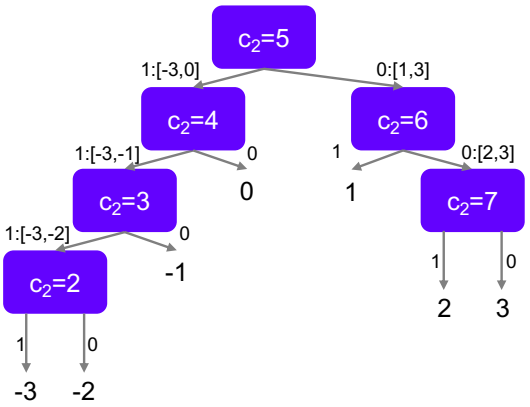
E(#Q1)
= 4*7/64 + 3*22/64 + 2*35/64 = 2.5625

If $(sk_0,sk_1)=(-3,0)$, $\#Q2=\max(d_{-3},d_0)=4$

E(#Q2)
= $4*1/2^{12} + \dots + 3*1/2^{12}$ = 2.9077…

E(#Q4)
= $4*1/2^{24} + \dots + 3*1/2^{24}$ = **3.2813… > 3**

U = (208,0), $c_1 = cmp_{10}(U)$, c_2 in {2,…7}



[QCZ+21] Qin, Cheng, Zhang, Pan, Hu, and Ding (ASIACRYPT2021)
https://github.com/AHaQY/Key-Mismatch-Attack-on-NIST-KEMs
[RRD+23] Rajendran, Ravi, D'Anvers, Bhasin, Chattopadhyay (TCHES2023(2))

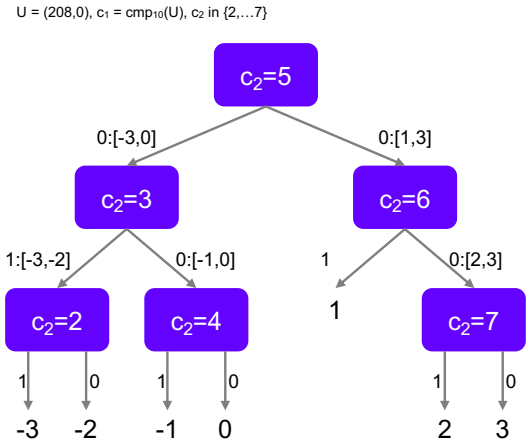
[RRD+23]'s BDT (and more)

#QP = 3 *in the worst case*

sk = s←Ψ_3^2 has 256*2 coefficients

→ #Query=2*#Q1*ceil(256/P)~1536/P *in the worst case*

Use LWE with Hint [DDGR20] to complement partial KRA



[RRD+23] Rajendran, Ravi, D'Anvers, Bhasin, Chattopadhyay (TCHES2023(2))
[DDGR20] Dachman-Soled, Ducas, Gong, Rossi (CRYPTO 2020)

[GM23] 2-positional mismatch attack

If we can check μ_0' and μ_{128}':

Let a = 208
Consider U=(ab + ac x^{128},0), V=at for b, c in {-1,0,+1}

μ_0'=cmp_1(t - abs_0 + acs_{128})

μ_{128}'=cmp_1(t - acs_0 - abs_{128})

μ_j' = cmp_1(abs_j + acs_{128+j})

(or swap b and c for 128 < j)

[GM23] designs good tests

For example:

μ_0' \ s_0	-3	-2	-1	0	1	2	3
-3	1	1	1	1	1	1	1
-2	1	1	1	1	1	1	0
-1	1	1	1	1	1	0	0
s_{128} 0	1	1	1	1	0	0	0
1	1	1	1	0	0	0	0
2	1	1	0	0	0	0	0
3	1	0	0	0	0	0	0

Note: μ_{128}' might be 1

[GM23] Guo and Mårtensson (PQCrypto2023)

[GM23] 2-positional mismatch attack

If we can check μ_0' and μ_{128}':

[GM23] designs good tests (Fig.11+13)

#Q2		s_0						
		-3	-2	-1	0	1	2	3
s_{128}	-3	10	8	8	7	8	10	10
	-2	10	7	6	5	6	7	9
	-1	9	6	4	4	4	5	8
	0	9	5	4	3	4	5	8
	1	9	5	4	4	4	6	8
	2	8	7	6	5	6	7	9
	3	9	9	9	8	9	10	10

$E(\#Q2)=10*1/2^{12}+\ldots+3*400/2^{12}\sim4.70825$

$E(\#Q) \sim 1205.3$

cf:
Huffman Bound 1dim. ~ 1216 [QCZ+21]
Shannon Bound ~ 1195 [GM23]

Note: We need to check
μ' ?= `10…0?0…0` or `00…0?0…0`

If we can check 2^2 cases in one query, then $E(\#Q) < 1536 / 2 = 768$
[RRD+23,TUX+23]

[GM23] Guo and Mårtensson (PQCrypto2023)
[RRD+23] Rajendran, Ravi, D'Anvers, Bhasin, Chattopadhyay (TCHES2023(2))
[TUX+23] Tanaka, Ueno, X, Ito, Takahashi, Homma (TCHES2023(3))

[SLZ23] pairwise-parallel attack

Run [GM23] in P-parallel
Check μ_0',…, μ_{P-1}' and μ_{128}',…, $\mu_{128+P-1}$'

Note: If P = 2, we need to check
μ' ?=
`000…0??0…0, 010…0??0…0`
`100…0??0…0, 110…0??0…0`

> 6 queries to determine 2P positions

$E(\#Q) < 2*6*\text{ceil}(256/2P)$

Note:

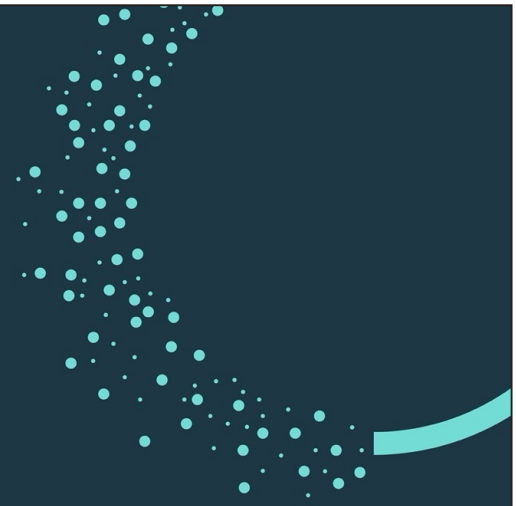
If we can check 2^P cases in one query, then $E(\#Q) < 2*3*\text{ceil}(256/P)$

[RRD+23,TUX+23]

[SLZ23] Shao, Liu, Zhou (EPRINT2023)
[RRD+23] Rajendran, Ravi, D'Anvers, Bhasin, Chattopadhyay (TCHES2023(2))
[TUX+23] Tanaka, Ueno, X, Ito, Takahashi, Homma (TCHES2023(3))

Technology Innovation Institute

Imperfect Oracles



tii.ae

Effect of Imperfect PC Oracle

SCA oracle might be imperfect

α_O : accuracy of the oracle
α_1 : accuracy of each coeff. [QCZ+23]
$\alpha_1 = \alpha_O^{2.5625}$
$E(\#err) = 512\ (1 - \alpha_1)$

brute force cost=(#err from 512)*$7^{\#err}$
#err=13: cost ~ $2^{120.7}$
#err=1 : cost ~ $2^{11.8}$

(Will be reduced by LWE with hints)

α_O	α_1	E(#err)
0.999999	0.999997…	0.0013…
0.99999	0.99997…	0.013…
0.9999	0.9997…	0.131…
0.999	0.9974…	1.310…
0.99	0.9745…	13.017…
0.95	0.8768…	63.061…
0.90	0.7633…	121.144…
0.80	0.5645…	222.973…

[SCZ+23] Shen, Cheng, Zhang, Guo, Jiang (TCHES2023(1))

Boosting Accuracy

α_O : accuracy of the oracle

Majority Vote with t traces:

$$\alpha_{MV} = 1 - \sum_{s=0}^{\lfloor t/2 \rfloor} \binom{t}{s} \alpha_O^s (1-\alpha_O)^{t-s}$$

Likelihood comparison
by NLL (negative log likelihood)

$\mathrm{NLL}_b(q, \hat{\theta}) = -\frac{1}{t}\sum_{s=1}^{t} \log q(b|x_s; \hat{\theta})$,
where x_s is s-th trace,
$q(b|x_s; \hat{\theta})$ is a PDF trained by NN

Experimental result [UXT+22]

	α_O	MV	NLL
SW	0.999	0.99999 by 5	100% by 2
HW	0.998	0.99999 by 5	100% by 2
Masked SW	0.960	0.99999 by 11	100% by 5

#Traces = t * #Query

[UXT+22] Ueno, X, Tanaka, Ito, Takahashi, Homma (TCHES2022(1))

[SCZ+23] Strategy

Strategy:

1. Obtain ŝ by PCO with α_O
   #Q_{RR}=1312
2. Detect err. blocks by “fast checking”
   #Q_{FC}=2*512/4
3. Correct wrong coefficients
   #Q_{final}=3*#err*4+…

α_O=0.99, α_1=0.974, E(#err)=13

Fast Checking:

Check 4 coeff. by 2 queries

From ŝ, we can compute ct_0 & ct_1 with
$u_0^{b'}, u_1^{b'}, u_2^{b'}, u_3^{b'}, v^{b'}$ s.t.
1. $\mu_0^{b'} = \mathrm{cmp}_1(v^{b'} - (u_0^{b'}s_0 + \ldots + u_3^{b'}s_3))$
2. $\mu_i' = 0$
3. $s_0s_1s_2s_3$ is correct $\Leftrightarrow \mu_0^{0'}\,\mu_0^{1'} = 01$

[SCZ+23] Shen, Cheng, Zhang, Guo, Jiang (TCHES2023(1))

[SCZ+23] Simulation (Table.6 and 8)

cf.#Q_{avg}=1312 in [QCZ+21] and #Q_{worst}=1536 in [UXT+22]

	MV		[SCZ+23]	
α_O	#traces	#err	#traces	#err
0.995 (t=3)	3936.5	0.10	1645.1	0.51
0.950 (t=7)	9185.0	0.25	3874.5	0.15
0.900 (t=11)	14433.3	0.39	7773.9	0.25
	NLL		[SCZ+23]	
α_O	#traces	#err	#traces	#err
0.998 (t=2)	3072	~0.00	1663.3	0.04
0.960 (t=5)	7680	~0.00	3424.9	0.05

[SCZ+23] Shen, Cheng, Zhang, Guo, Jiang (TCHES2023(1))

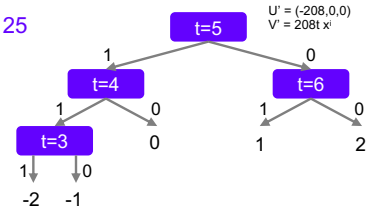
Kyber-768

Kyber-768:
Ψ_2=CBD(1/2,4) over $[-2,+2]^{256}$, s←Ψ_2^3

CBD(1/2,4)

sk_i	-2	-1	0	1	2
pr.	1/16	4/16	6/16	4/16	1/16
dep.	3	3	2	2	2

E(#Q1)=2.3125



PCO-based KRA:
E(#Q) = 768 * E(#Q1) = 1776

P-parallel PCO-based KRA:
#Q <= 3*3*ceil*(256/P)
P=2: #Q <=1152
P=4: #Q <= 576

…

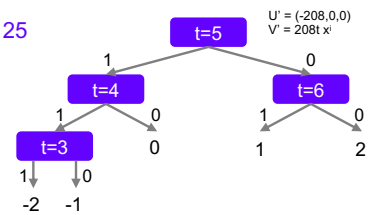
DO = 256-Parallel PCO

Kyber-768:
Ψ_2=CBD(1/2,4) over $[-2,+2]^{256}$, s←Ψ_2^3

CBD(1/2,4)

sk_i	-2	-1	0	1	2
pr.	1/16	4/16	6/16	4/16	1/16
dep.	3	3	2	2	2

E(#Q1)=2.3125



PCO-based KRA:
E(#Q) = 768 * E(#Q1) = 1776

P-parallel PCO-based KRA:
#Q ≦ 3*3*ceil*(256/P)
P=2: #Q ≦ 1152
P=4: #Q ≦ 576

DO-based KRA:
P=256: #Q ≦ 9

DO = 256-Parallel PCO

Kyber-768:
Ψ_2=CBD(1/2,4) over $[-2,+2]^{256}$
$s \leftarrow \Psi_2^3$

Natural DO-based KRA:
#Q = 9 (in the worst case)

1. Decide s_1 by U = (u,0,0) w/ 3 queries
2. Decide s_2 by U = (0,u,0) w/ 3 queries
3. Decide s_3 by U = (0,0,u) w/ 3 queries

[GNNJ23] SCA-LDPC (DO-Based KRA)

cf. 256-parallel PCO-based KRA:
#Q = 9 (in the worst case)

U=(-u,0,0), V = $a(t_0+t_1x+t_2x^2+t_3x^3)$

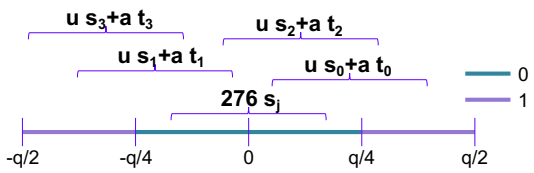
$\mu_i' = cmp_1(u\ s_i + a\ t)$

$\mu_j' = cmp_1(u\ s_j)$

Observation 1:

No need to $-q/4 < u\ s_j < q/4$

u is flexible



[GNNJ23] Guo, Nabokov, Nilsson, Johansson (EPRINT2023/294)

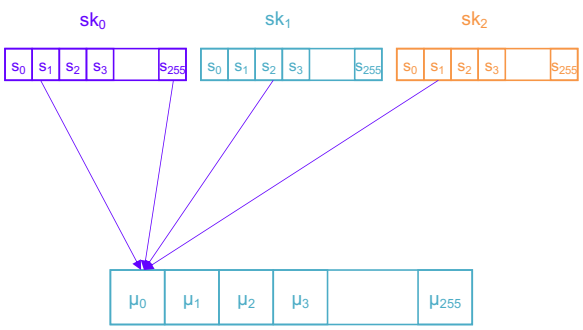
[GNNJ23] SCA-LDPC (DO-Based KRA)

cf. 256-parallel PCO-based KRA:
#Q = 9 (in the worst case)

Use LDPC to check error

DO-based KRA against Kyber-768:
E(#Q) = 7 (Shannon Bound)

Experiment:
12 traces for 1st masking Kyber-768
ρ=0.995: 10 traces



[GNNJ23] Guo, Nabokov, Nilsson, Johansson (EPRINT2023/294)

Summary

Summary

- Side-channel analysis
  - Direct attack
  - Indirect attack
- Key-recovery attack using (MV) plaintext-checking oracle
  - Perfect PCO
  - Perfect MV-PCO
  - Imperfect PCO
- Key-recovery attack using decryption oracle
  - Perfect DO
  - Coding

深層学習に基づくサイドチャネル攻撃とその対策

伊東 燦
NTT 社会情報研究所
akira.itoh@ntt.com

暗号モジュールから副次的に発生する消費電力・漏洩電磁波（サイドチャネル情報）を用いることで、暗号モジュール内の秘密鍵を推定する攻撃をサイドチャネル攻撃という。本講演では、近年高い注目を集めているニューラルネットワークを用いたサイドチャネル攻撃（DL-SCA）について解説を行う。DL-SCA では、攻撃対象モジュールのサイドチャネル情報についてあらかじめ学習することで、従来よりも強力な攻撃が可能なことが知られている。また、サイドチャネル攻撃に対する代表的な対策手法であるマスキング対策と、その理論的な安全性についても紹介し、マスキング対策が DL-SCA に対しても有効であることを説明する。

NTT

深層学習に基づくサイドチャネル攻撃とその対策

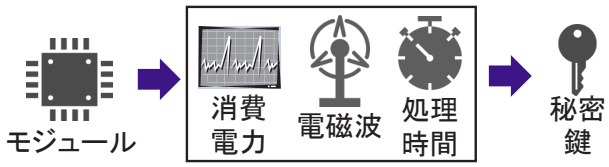
伊東燦　（NTT社会情報研究所）

サイドチャネル攻撃とは

NTT

■ チップから漏洩する電磁波、消費電力から秘密情報を盗み取る攻撃

- 漏洩する情報を**サイドチャネル情報**と呼ぶ
- 通常は、暗号モジュール（暗号化処理を行うチップ）から秘密鍵を窃取



サイドチャネル攻撃

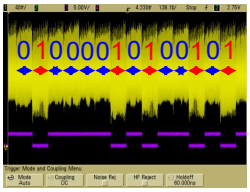
サイドチャネル攻撃の種類

NTT

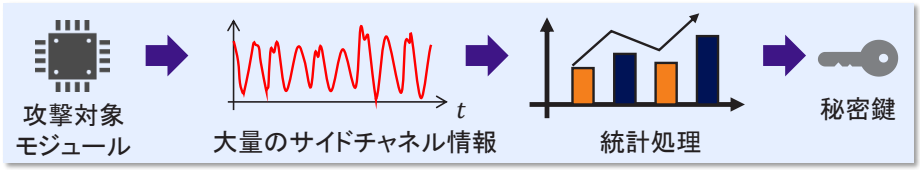
■ 単純電力/電磁波解析（Simple Power/EM Analysis: SPA/SEMA）

RSA暗号が実装されたボード

計測



■ 統計処理を用いた攻撃（相関電力/電磁波解析など）



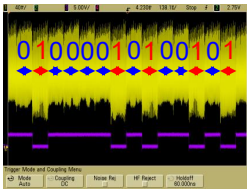
サイドチャネル攻撃の種類

NTT

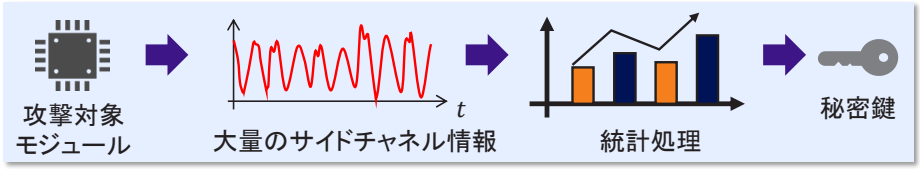
■ 単純電力/電磁波解析（Simple Power/EM Analysis: SPA/SEMA）

RSA暗号が実装されたボード

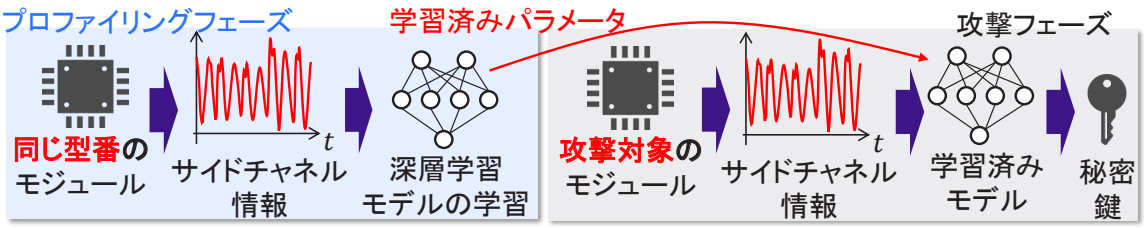
計測



■ 統計処理を用いた攻撃（相関電力/電磁波解析など）



プロファイリング型サイドチャネル攻撃



■ 深層学習に基づくSCA（DL-SCA）

- 従来の攻撃と比べてより強力な攻撃が可能
  - › 数倍から数十倍強力
- 専門知識があまりなくても実行可能
  - › 波形の前処理などがほとんど必要ない

DL-SCAの現状

■ **学習と攻撃のデバイスが違っても攻撃に問題はないのか？**

- 機械学習のドメイン適応を用いることで解消可能なことが示されている
- ただし，うまく行かない場合もある

■ **攻撃可能な暗号は？**

- 共通鍵はAES，公開鍵はRSA，ECC，格子ベース暗号などが報告
- ただし現状の主な対象はAES（ほぼほぼAES）
  - › AES以外への攻撃については，今後増えていくと思われる

■ **性能指標は適切か？**

- よく使われる目的関数である負の対数尤度と，攻撃成功確率の関係は現在進行系の研究課題

■ **DL-SCAに対しても意味のある対策はあるのか？**

- 従来のマスキング対策は，意味がある対策になることが実験的・理論的にわかってきてる

DL-SCAの現状

■ **学習と攻撃のデバイスが違っても攻撃に問題はないのか？**

- 機械学習のドメイン適応を用いることで解消可能なことが示されている
- ただし，うまく行かない場合もある

■ **攻撃可能な暗号は？**

- 共通鍵はAES，公開鍵はRSA，ECC，格子ベース暗号などが報告
- ただし現状の主な対象はAES（ほぼほぼAES）
  - › AES以外への攻撃については，今後増えていくと思われる

今回はAESへの攻撃を対象として以下の２つに着目

■ **性能指標は適切か？**

- よく使われる目的関数である負の対数尤度と，攻撃成功確率の関係は現在進行系の研究課題

■ **DL-SCAに対しても意味のある対策はあるのか？**

- 従来のマスキング対策は，意味がある対策になることが実験的・理論的にわかってきてる

本講演の内容

AESへの攻撃を題材として以下の二つについて解説

■ DL-SCAの損失関数と、攻撃成功確率の間の関係[1]

- DNNで一般的な負の対数尤度（Negative Log Likelihood: NLL）と攻撃成功確率（Success Rate: SR）の間の関係に着目
- SRがNLLから推定できることを説明

■ マスキング対策の安全性[2]

- サイドチャネル攻撃で一般的なマスキング対策が、DL-SCAにも有効であることを説明

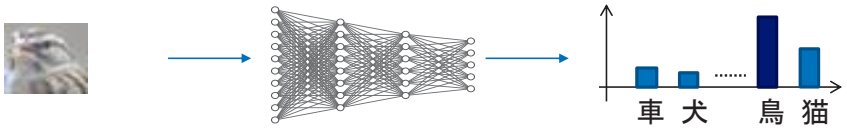
[1] Akira Ito, Rei Ueno, and Naofumi Homma, N. Perceived Information Revisited: New Metrics to Evaluate Success Rate of Side-Channel Attacks. TCHES 2022,
[2] Akira Ito, Rei Ueno, and Naofumi Homma, On the Success Rate of Side-Channel Attacks on Masked Implementations: Information-Theoretical Bounds and Their Practical Usage, ACM CCS 2022

AESへのDL-SCA

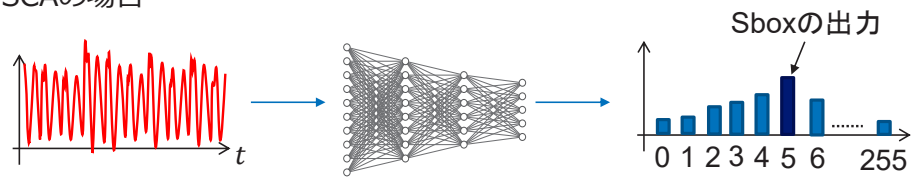
深層学習による推論

■ 波形から中間値の推定に深層学習（DL)を使用

- 画像分類の場合

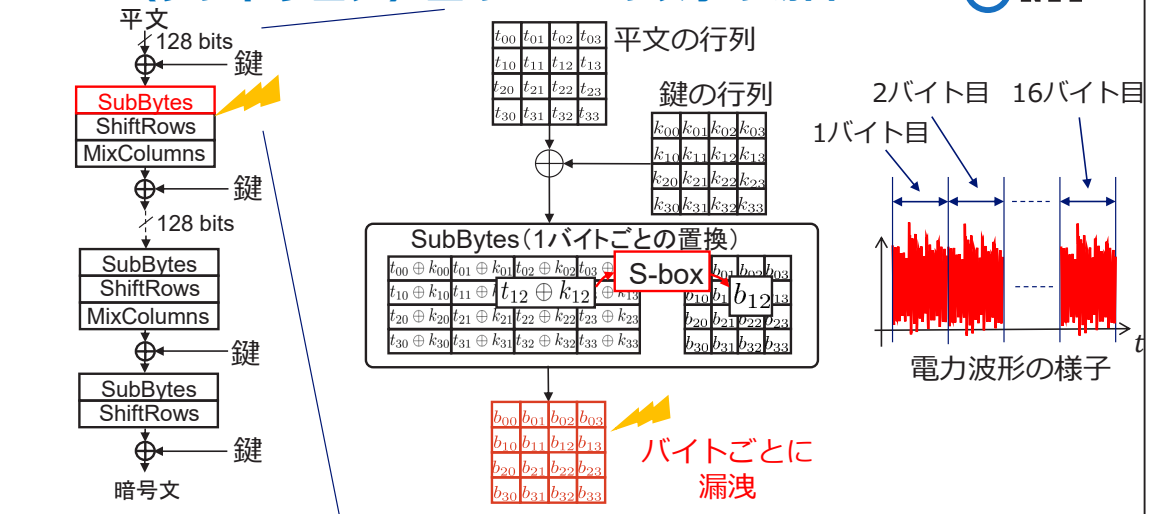


- SCAの場合

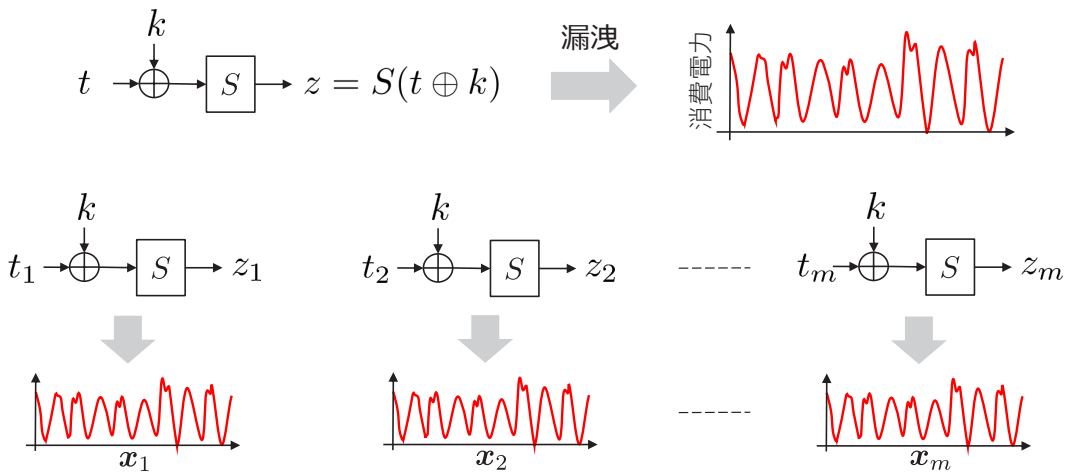


- DL-SCAでは
  - › プロファイリングフェーズでもっともらしい確率分布を学習
  - › 攻撃フェーズで、学習により得た確率分布で中間値を推定

CPU（ソフトウェア）上のAESへの攻撃の場合



一バイトごとのサイドチャネル攻撃

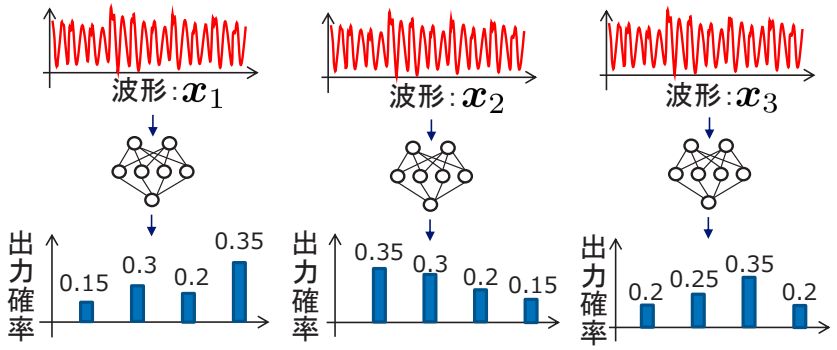


平文を変えたときの中間値の値のパターンから鍵の値を絞り込む

NNを使った攻撃のイメージ

NTT

■ 推定する部分鍵が２ビットの場合（鍵候補は4つ）



$k=0$

$k=1$

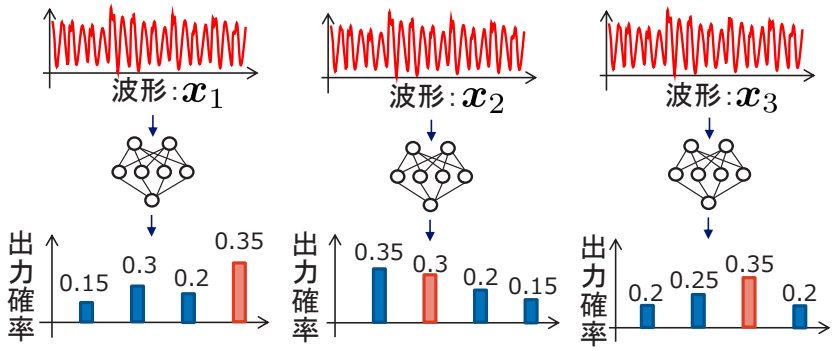
$k=2$

$k=3$

NNを使った攻撃のイメージ

NTT

■ 推定する部分鍵が２ビットの場合（鍵候補は4つ）



$k=0$ $S(0 \oplus t_1) = 3$ 0.35 $S(0 \oplus t_2) = 1$ 0.3 $S(0 \oplus t_3) = 2$ 0.35 0.0365

$k=1$ 乗算

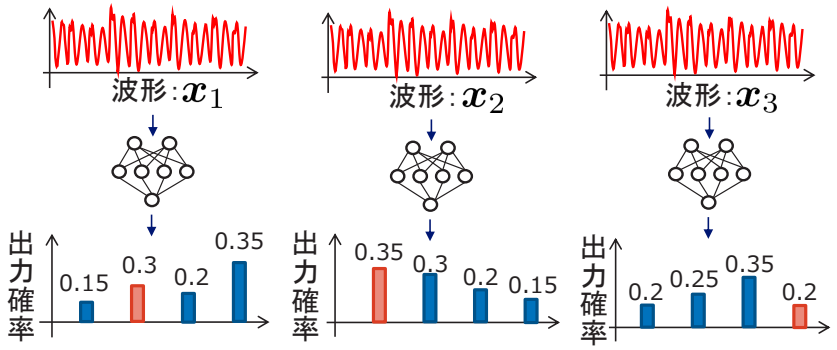
$k=2$

$k=3$

NNを使った攻撃のイメージ

NTT

■ 推定する部分鍵が２ビットの場合（鍵候補は4つ）



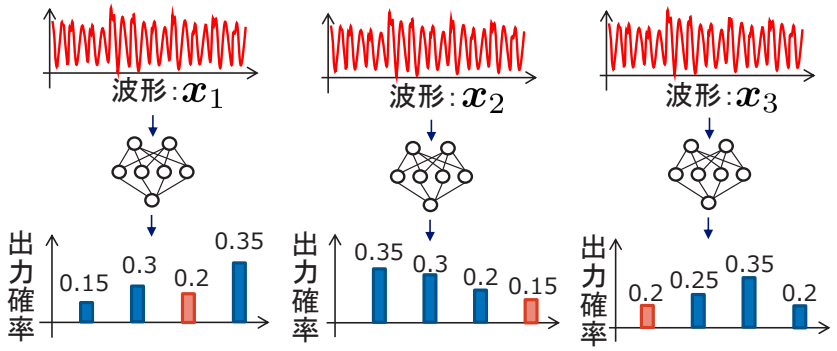
$k=0$	$S(0\oplus t_1)=3$	0.35	$S(0\oplus t_2)=1$	0.3	$S(0\oplus t_3)=2$	0.35
$k=1$	$S(1\oplus t_1)=1$	0.3	$S(1\oplus t_2)=0$	0.35	$S(1\oplus t_3)=3$	0.2
$k=2$						
$k=3$						

0.0365
0.0021
乗算

NNを使った攻撃のイメージ

NTT

■ 推定する部分鍵が２ビットの場合（鍵候補は4つ）



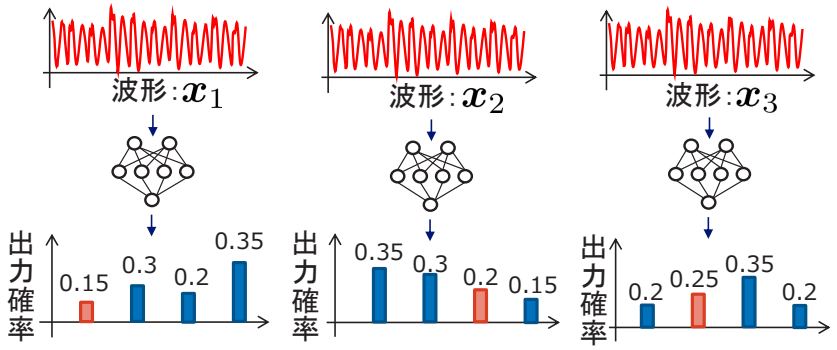
$k=0$	$S(0\oplus t_1)=3$	0.35	$S(0\oplus t_2)=1$	0.3	$S(0\oplus t_3)=2$	0.35
$k=1$	$S(1\oplus t_1)=1$	0.3	$S(1\oplus t_2)=0$	0.35	$S(1\oplus t_3)=3$	0.2
$k=2$	$S(2\oplus t_1)=2$	0.2	$S(2\oplus t_2)=3$	0.15	$S(2\oplus t_3)=0$	0.2
$k=3$						

0.0365
0.0021
0.006
乗算

NNを使った攻撃のイメージ

NTT

■ 推定する部分鍵が２ビットの場合（鍵候補は4つ）



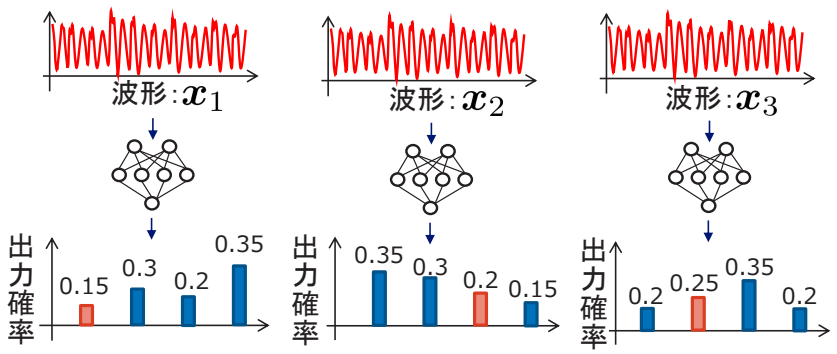
$k=0$	$S(0\oplus t_1)=3$	0.35	$S(0\oplus t_2)=1$	0.3	$S(0\oplus t_3)=2$	0.35	0.0365
$k=1$	$S(1\oplus t_1)=1$	0.3	$S(1\oplus t_2)=0$	0.35	$S(1\oplus t_3)=3$	0.2	0.0021
$k=2$	$S(2\oplus t_1)=2$	0.2	$S(2\oplus t_2)=3$	0.15	$S(2\oplus t_3)=0$	0.2	0.006
$k=3$	$S(3\oplus t_1)=0$	0.15	$S(3\oplus t_2)=2$	0.2	$S(3\oplus t_3)=1$	0.25	0.0075

乗算

NNを使った攻撃のイメージ

NTT

■ 推定する部分鍵が２ビットの場合（鍵候補は4つ）



$k=0$	$S(0\oplus t_1)=3$	0.35	$S(0\oplus t_2)=1$	0.3	$S(0\oplus t_3)=2$	0.35	0.0365
$k=1$	$S(1\oplus t_1)=1$	0.3	$S(1\oplus t_2)=0$	0.35	$S(1\oplus t_3)=3$	0.2	0.0021
$k=2$	$S(2\oplus t_1)=2$	0.2	$S(2\oplus t_2)=3$	0.15	$S(2\oplus t_3)=0$	0.2	0.006
$k=3$	$S(3\oplus t_1)=0$	0.15	$S(3\oplus t_2)=2$	0.2	$S(3\oplus t_3)=1$	0.25	0.0075

一番大きい k=0を正解と予想

負の対数尤度（Negative log likelihood:NLL）

NTT

- 確率の積の対数を取ってマイナスしたもの
  - θ：モデルパラメータ
  - $q_\theta(z \mid x)$：条件付き確率（モデル）
  - 対数を取ることでアンダーフローを防げる
- 確率が大きいほど、NLLは小さい

$$L(q_\theta) = -\frac{1}{m} \log \left(\prod_{i=1}^{m} q_\theta(z_i \mid x_i) \right)$$

対数を内側に入れる

$$L(q_\theta) = -\frac{1}{m} \sum_{i=1}^{m} \log q_\theta(z_i \mid x_i)$$

プロファイリングフェーズ

入力：学習データ$\left((x_1, z_1), (x_2, z_2), \ldots, (x_m, z_m)\right)$
（ただし，$z_i = S(t_i \oplus k)$）
出力：NLLを最小とするパラメータ$\hat{\theta}$

$$\hat{\theta} \in \arg\min_{\theta} -\frac{1}{m} \sum_{i=1}^{m} \log q_\theta(z_i \mid x_i)$$

アタックフェーズ

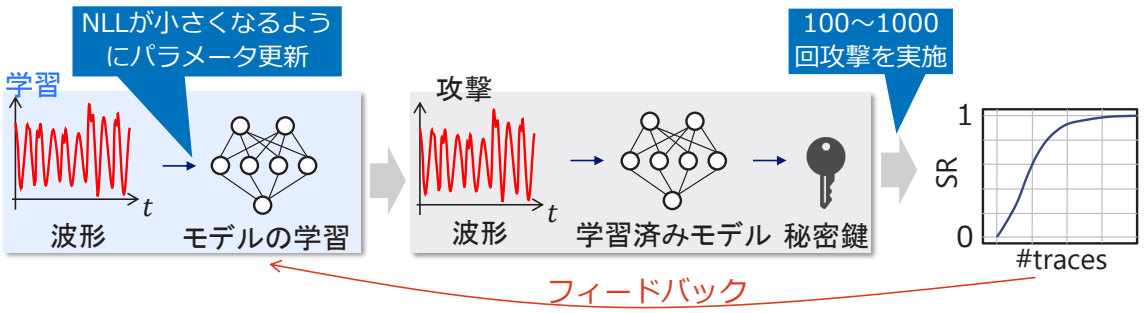
入力：データ$\left((x_1, t_1), (x_2, t_2), \ldots, (x_{m'}, t_{m'})\right)$
学習済みパラメータ$\hat{\theta}$
出力：NLLを最小とする部分鍵$\hat{k}$

$$\hat{k} \in \arg\min_{k} -\frac{1}{m'} \sum_{i=1}^{m'} \log q_{\hat{\theta}}(S(t_i \oplus k) \mid x_i)$$

NTT

DL-SCAの安全性評価

デバイスへのDL-SCAの評価方法

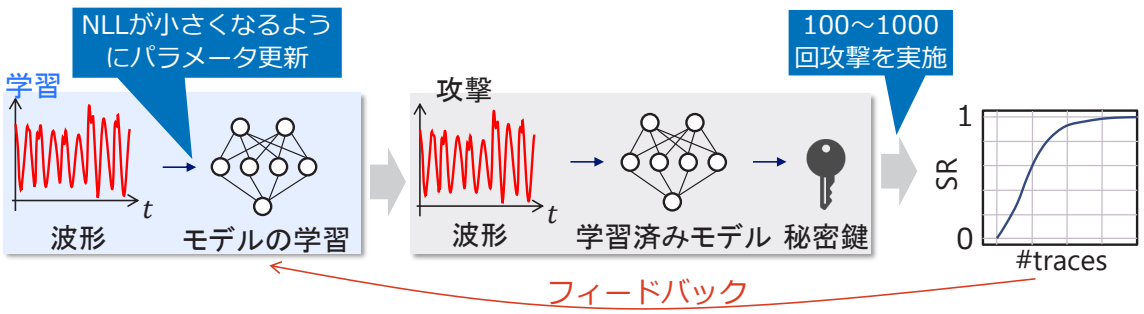


- Success Rate(SR)：m波形使ったときに，正解鍵Kを当てられる確率

$$\mathrm{SR}_m(q_\theta) = \Pr\left(K \in \arg\min_k L_k(\hat{\theta})\right)$$

■ 学習と攻撃、SRの計算を繰り返し最適なハイパーパラメータパラメータを決定

デバイスへのDL-SCAの評価方法

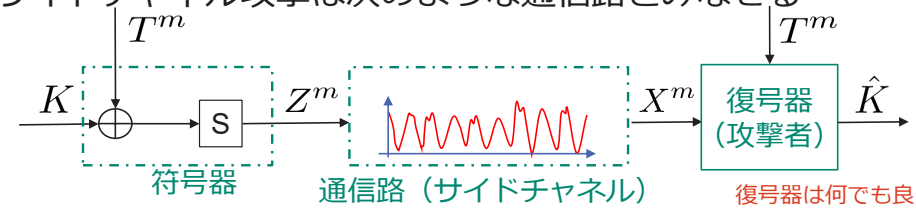


- 目的関数であるNLLとSRの関係性がよくわかってない
  - NLLが小さい方が，SRが大きくなるという根拠がない
  - 普通に考えると，SRを直接小さくしたほうが良いのでは？
- SRの計算コストが高い
  - NLLから推定できるとよい

NLLとSRの間の関係を明らかにすることが重要

通信路モデル

■ サイドチャネル攻撃は次のような通信路とみなせる



復号器は何でも良いことに注意

mの指数はm個の組のこと（例：$T^m = (T_1, T_2, \ldots, T_m)$）

- 攻撃者はサイドチャネル情報X^mを受信して，鍵Kを推定
  - › サイドチャネルを用いて，中間値Zを送信していると解釈
- de Chérisey らは，通信理論の結果から，次式を証明

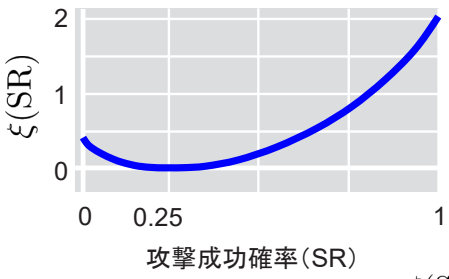
$$\xi(\mathrm{SR}_m) \leq mI(Z;X)$$

  - › mは波形数，$I(Z;X)$は相互情報量，SR_mは任意の攻撃を使った場合の最大の攻撃成功確率

$\xi(\mathrm{SR}_m) \leq mI(Z;X)$の意味

■ 与えられたSRに対して，何ビット受信する必要があるかを表現

鍵が2ビットのときの $\xi(\mathrm{SR})$ のグラフ



- SR=1のとき
  - すべての鍵のビット（２ビット）が必要
- SR=0.25のとき
  - 当てずっぽうなので，0ビットでよい

$$\xi(\mathrm{SR}_m) \leq mI(Z;X)$$

必要な情報量（鍵のビット数）を表現　　一波形あたりで伝送可能な中間値のビット数

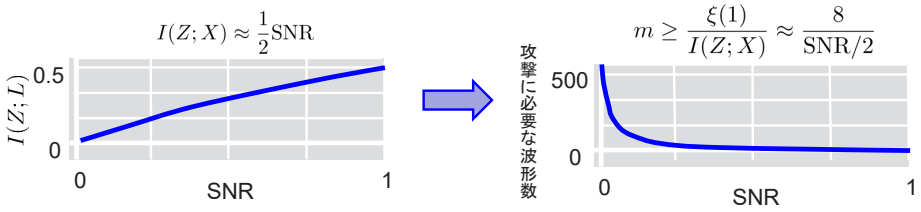
式の使い方

■ 相互情報量が与えられると，攻撃に必要な波形数がわかる

- 例：１波形あたり$I(Z;X) = 0.1$ビットが伝送可能なとき，あるバイトの部分鍵への攻撃が成功（SR=1）するために必要な波形数m

$$m \geq \frac{\xi(1)}{I(Z;X)} = \frac{8}{0.1} = 80$$

■ ガウスノイズのときは，相互情報量はSNRがわかると計算可能



- ガウスノイズじゃないときは，他の何らかの推定手法を用いる

クロスエントロピーによるSRの概算

■ NLLはクロスエントロピー（Cross Entropy: CE)に（概）収束

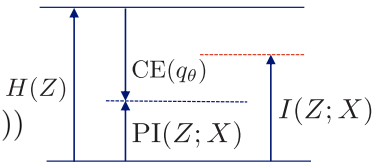
$$L(q_\theta) = -\frac{1}{m}\sum_{i=1}^{m} \log q_\theta(Z_i \mid X_i) \xrightarrow{a.s.} \mathrm{CE}(q_\theta) = -\mathbb{E}\log q_\theta(Z \mid X) \quad (m \to \infty)$$

■ 相互情報量$I(Z;X)$に関して，$I(Z;X) \geq H(Z) - \mathrm{CE}(\theta)$が成立

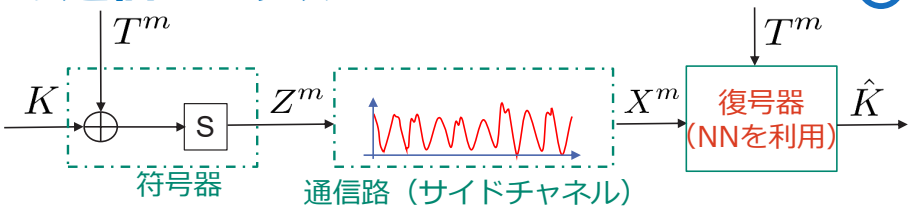
- NLL（CE)が小さくできるためには，波形に中間値の情報が乗ってる必要がある
- 見方を変えると，$H(Z) - \mathrm{CE}(q_\theta)$はモデルが取り出せる情報量を意味していそう
- そこで，$H(Z) - \mathrm{CE}(q_\theta)$を知覚情報$\mathrm{PI}_{q_\theta}(Z;X)$と呼ぶ

■ TCHES 2021でMasureらは，
次が成り立ってるのではないかと予想

$$\xi(\mathrm{SR}_m(q_\theta)) \leq m\mathrm{PI}_{q_\theta}(Z;X)$$
$$= m(H(Z) - \mathrm{CE}(q_\theta)) \approx m(H(Z) - L(q_\theta))$$



NNの通信路モデル



■ このモデルにおいて，Masureらが述べていることは次のこと

- NNが１波形あたりから取り出せる中間値の情報量はおそらく

$$\mathrm{PI}_{q_\theta}(Z;X) = H(Z) - \mathrm{CE}(q_\theta) \approx H(Z) - L(\theta)$$

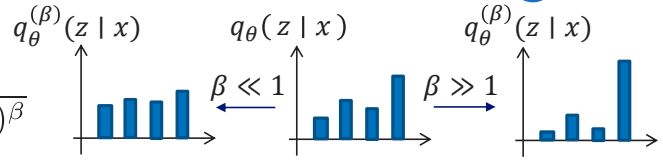
- したがって，攻撃成功確率SRは次式で抑えられるのではないか

$$\xi(\mathrm{SR}_m(q_\theta)) \le m\mathrm{PI}_{q_\theta}(Z;X)$$

- 実験的には成り立ってそうなことを確認

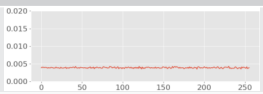
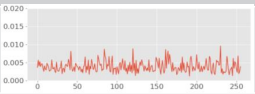
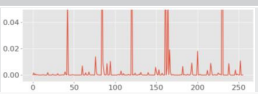
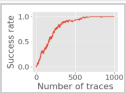
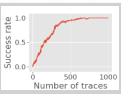
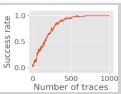
逆温度による変換と予想の反例

$$q_\theta^{(\beta)}(z \mid x) = \frac{q_\theta(z \mid x)^\beta}{\sum_{z'} q_\theta(z' \mid x)^\beta}$$



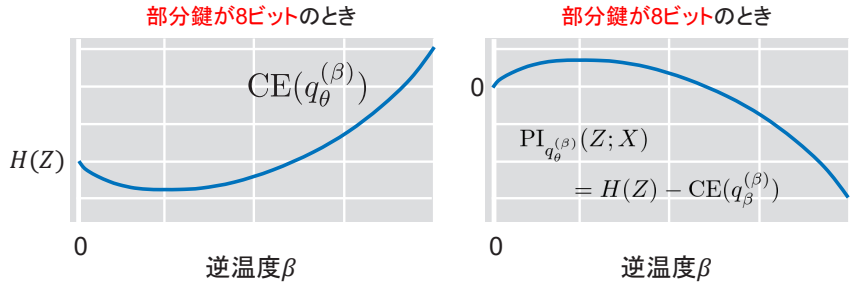
実は，SRはβに対して変化しないのに対して，CE（NLL)は変化する

ソフトウェア実装のAESへの攻撃結果

β	0.1	1	10
NLL	0.7933	0.7789	1.565
$q_\theta^{(\beta)}$			
Attack result			

βに対するCEの挙動

■ 特殊な状況を除いて，CE（NLL)はβに対して凸関数

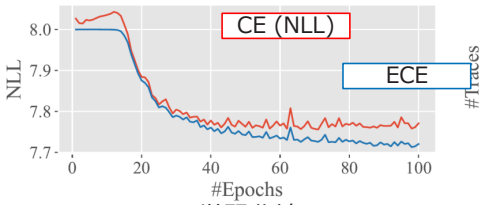


- PIが小さい分布$q_\theta(z \mid x)$でも，βの変換でPIが大きくなる可能性がある
  - › TCHES 2022で，我々はβに対して最小となるCEをEffective CE（ECE）と定義

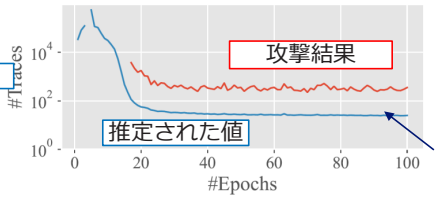
$$\mathrm{ECE}(q_\theta) = \inf_{\beta>0} \mathrm{CE}(q_\theta^{(\beta)})$$

実験結果

ASCADデータセット（ソフトウェアAES)の場合の結果



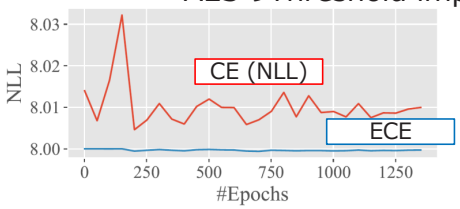
学習曲線



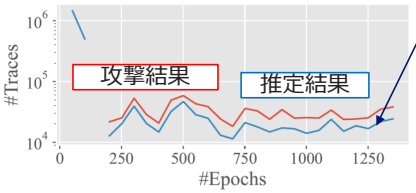
SR=0.9に必要な波形数

攻撃結果をNLLから推定できそう

AESのThreshold implementationの場合の結果



学習曲線



SR=0.9に必要な波形数

DL-SCAへの対策

DL-SCAへの対策

■ DL-SCAは従来の攻撃より強力

- 未対策のマイコン実装のAESでは，３波形程度で鍵が推定可能

■ DL-SCAへの対策は意味があるのか？

- 実験的にはマスキング対策は効果がありそうな事がわかっている
  - › マスキングは証明可能安全な対策
- ただし，理論的には安全ではない！
  - › 従来の証明（Eurocrypt 2015）では，大雑把にいえば，サイドチャネル情報のSNRが中間値のビット数nに対して，指数的に小さくないと意味がない
    - » ノイズの量が、ビット数に対して指数的に大きくないとマスキング対策は意味がない
  - › マイコン実装では，明らかに上回っているので，マスキング対策が意味がないことになる

どうにか現実と理論のギャップを埋めたい！

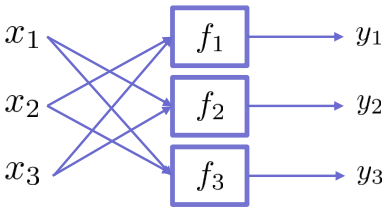
マスキングの例：Threshold Implementation (TI)

NTT

■ TIは代表的な一次マスキングスキーム

- 3シェアの場合：$y = f(x) = f_1(x_2, x_3) \oplus f_2(x_1, x_3) \oplus f_3(x_1, x_2)$

$x = x_1 \oplus x_2 \oplus x_3$



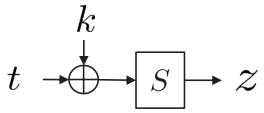
$y = y_1 \oplus y_2 \oplus y_3$

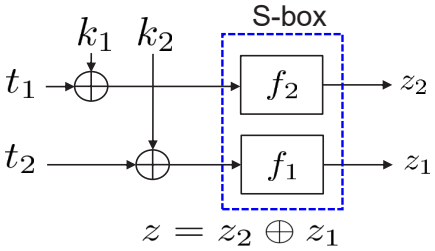
- Correctness：シェアから関数を復元可能
- Non-completeness：関数復元にはすべてのシェアが必要
- Uniformity：マスク値の確率に偏りがない（一様分布）

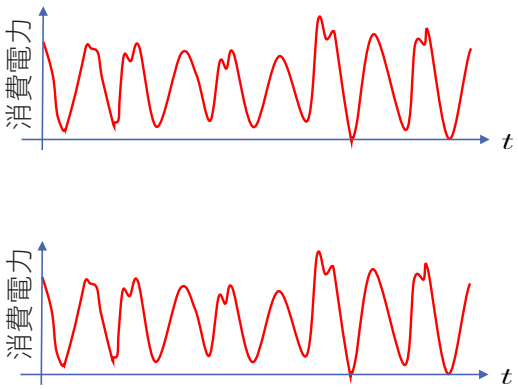
マスキング実装への攻撃：TIの場合

NTT

■ TIへの攻撃では，個別に漏れるシェアの情報の連結が必須

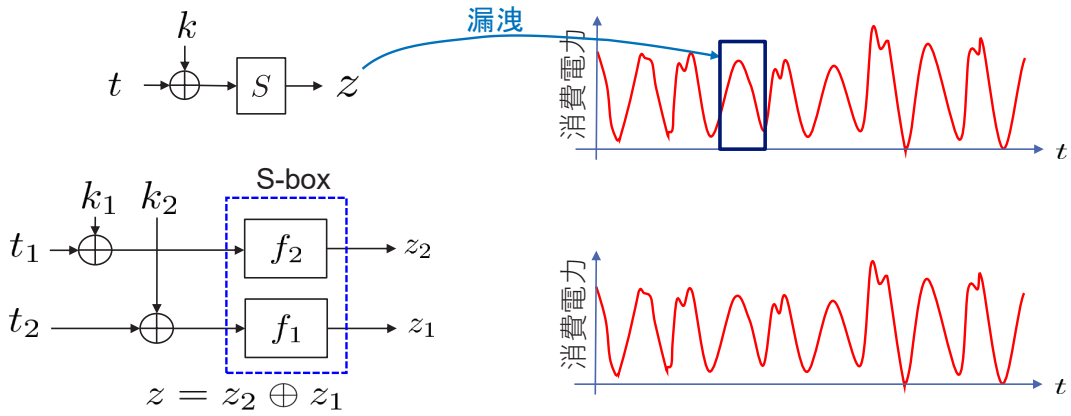






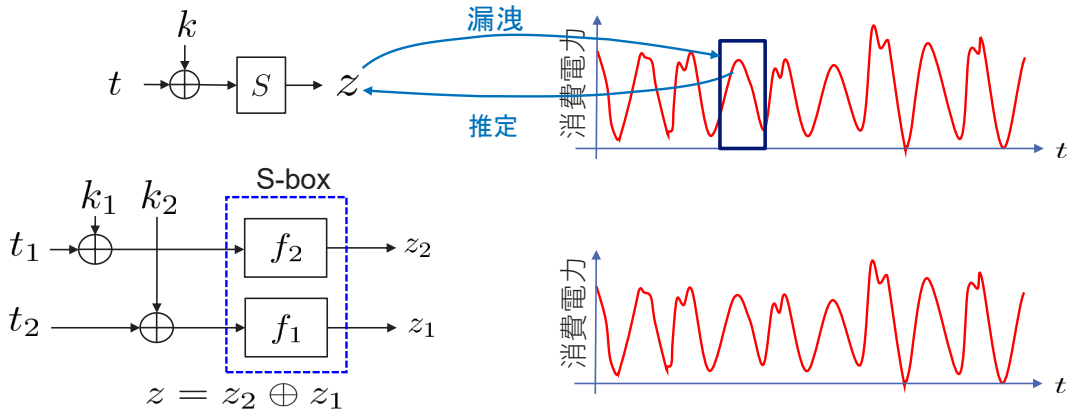
マスキング実装への攻撃：TIの場合

■ TIへの攻撃では，個別に漏れるシェアの情報の連結が必須



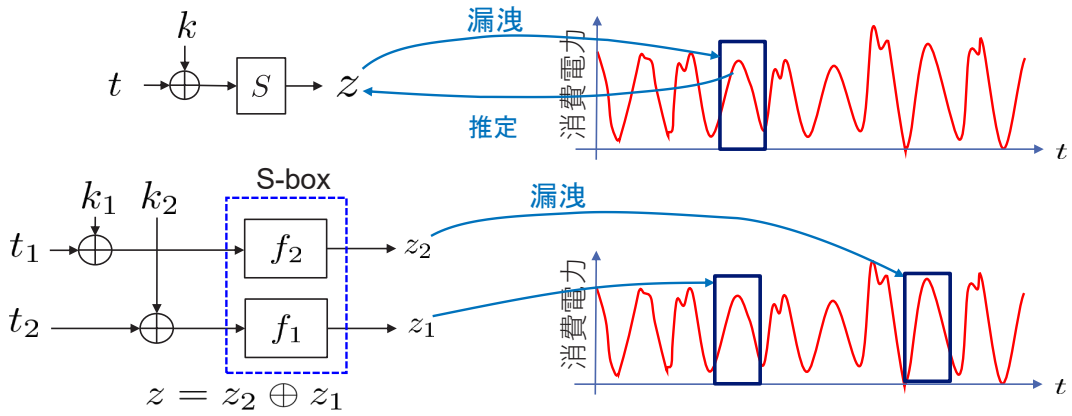
マスキング実装への攻撃：TIの場合

■ TIへの攻撃では，個別に漏れるシェアの情報の連結が必須



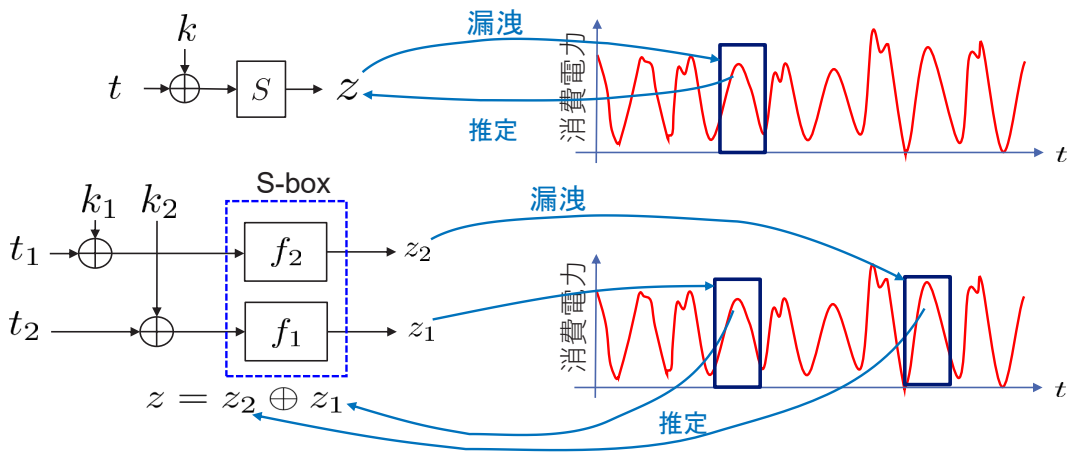
マスキング実装への攻撃：TIの場合

■ TIへの攻撃では，個別に漏れるシェアの情報の連結が必須



マスキング実装への攻撃：TIの場合

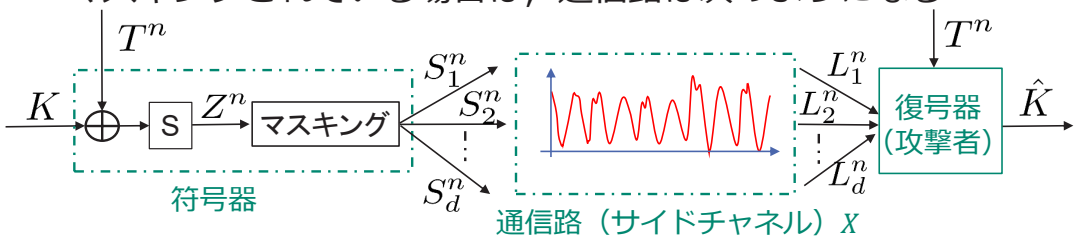
■ TIへの攻撃では，個別に漏れるシェアの情報の連結が必須



シェアに分割することで攻撃難易度が上昇しそう

マスキングされている場合の通信路

■ マスキングされている場合は，通信路は次のようになる



- dはシェアの数
- 同時に漏洩している場合を考えるとややこしいので，各シェアに関する情報が個別に漏れていると仮定
- シェアを増やして、$I(Z;X)$が減れば、送れる情報量が減って安全ということ

このとき，シェアの数を増やしたらどのくらい安全になるか？

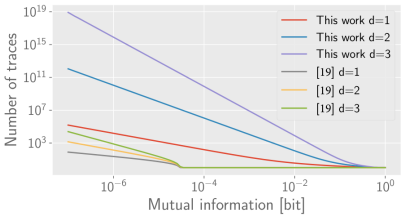
得られた結果

■ CCS 2022で$I(Z;X)$が次で抑えられることを示した

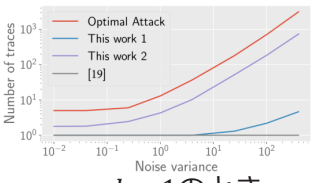
$$I(Z;X) \leq \log\left((2^n-1)(2\ln(2))^d \prod_{i=1}^{d} I(S_i;L_i)+1\right)$$

各シェアの相互情報量の積

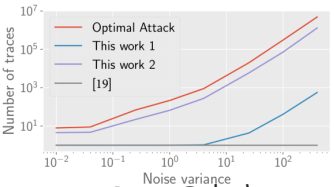
- 各シェアについて$I(S_i;L_i) < 1/(2\ln 2) \approx 0.72$なら，シェアを増やすほど安全



SR=0.99を達成するために必要な波形数



$d = 1$のとき



$d = 2$のとき

まとめ

- DL-SCAについて紹介
- DL-SCAの現状の問題を紹介
- 最近の研究成果について紹介
  - 損失関数と攻撃成功確率の間の関係
  - マスキング対策による安全性の向上

MI レクチャーノートシリーズ刊行にあたり

本レクチャーノートシリーズは、文部科学省 21 世紀 COE プログラム「機能数理学の構築と展開」（H15-19 年度）において作成した COE Lecture Notes の続刊であり、文部科学省大学院教育改革支援プログラム「産業界が求める数学博士と新修士養成」（H19-21 年度）および、同グローバル COE プログラム「マス・フォア・インダストリ教育研究拠点」（H20-24 年度）において行われた講義の講義録として出版されてきた。平成 23 年 4 月のマス・フォア・インダストリ研究所（IMI）設立と平成 25 年 4 月の IMI の文部科学省共同利用・共同研究拠点として「産業数学の先進的･基礎的共同研究拠点」の認定を受け、今後、レクチャーノートは、マス・フォア・インダストリに関わる国内外の研究者による講義の講義録、会議録等として出版し、マス・フォア・インダストリの本格的な展開に資するものとする。

2022 年 10 月
マス・フォア・インダストリ研究所
所長　梶原 健司

2023年度採択分　九州大学マス･フォア･インダストリ研究所 共同利用研究集会

現代暗号に対する安全性解析・攻撃の数理

発　行　2024年 1 月 11 日
編　集　國廣　昇，池松泰彦，伊豆哲也，穴田啓晃，縫田光司
発　行　九州大学マス・フォア・インダストリ研究所
九州大学大学院数理学府
〒819-0395 福岡市西区元岡744
九州大学数理・IMI 事務室
TEL 092-802-4402　FAX 092-802-4405
URL https://www.imi.kyushu-u.ac.jp/

印　刷　城島印刷株式会社
〒810-0012 福岡市中央区白金 2 丁目 9 番 6 号
TEL 092-531-7102　FAX 092-524-4411

シリーズ既刊

Issue	Author／Editor	Title	Published
COE Lecture Note	Mitsuhiro T. NAKAO Kazuhiro YOKOYAMA	Computer Assisted Proofs - Numeric and Symbolic Approaches - 199pages	August 22, 2006
COE Lecture Note	M.J.Shai HARAN	Arithmetical Investigations - Representation theory, Orthogonal polynomials and Quantum interpolations- 174pages	August 22, 2006
COE Lecture Note Vol.3	Michal BENES Masato KIMURA Tatsuyuki NAKAKI	Proceedings of Czech-Japanese Seminar in Applied Mathematics 2005 155pages	October 13, 2006
COE Lecture Note Vol.4	宮田　健治	辺要素有限要素法による磁界解析 - 機能数理学特別講義 21pages	May 15, 2007
COE Lecture Note Vol.5	Francois APERY	Univariate Elimination Subresultants - Bezout formula, Laurent series and vanishing conditions - 89pages	September 25, 2007
COE Lecture Note Vol.6	Michal BENES Masato KIMURA Tatsuyuki NAKAKI	Proceedings of Czech-Japanese Seminar in Applied Mathematics 2006 209pages	October 12, 2007
COE Lecture Note Vol.7	若山　正人 中尾　充宏	九州大学産業技術数理研究センター キックオフミーティング 138pages	October 15, 2007
COE Lecture Note Vol.8	Alberto PARMEGGIANI	Introduction to the Spectral Theory of Non-Commutative Harmonic Oscillators 233pages	January 31, 2008
COE Lecture Note Vol.9	Michael I.TRIBELSKY	Introduction to Mathematical modeling 23pages	February 15, 2008
COE Lecture Note Vol.10	Jacques FARAUT	Infinite Dimensional Spherical Analysis 74pages	March 14, 2008
COE Lecture Note Vol.11	Gerrit van DIJK	Gelfand Pairs And Beyond 60pages	August 25, 2008
COE Lecture Note Vol.12	Faculty of Mathematics, Kyushu University	Consortium “MATH for INDUSTRY” First Forum 87pages	September 16, 2008
COE Lecture Note Vol.13	九州大学大学院 数理学研究院	プロシーディング「損保数理に現れる確率モデル」 ― 日新火災・九州大学 共同研究2008年11月 研究会 ― 82pages	February 6, 2009

シリーズ既刊

Issue	Author／Editor	Title	Published
COE Lecture Note Vol.14	Michal Beneš, Tohru Tsujikawa Shigetoshi Yazaki	Proceedings of Czech-Japanese Seminar in Applied Mathematics 2008 77pages	February 12, 2009
COE Lecture Note Vol.15	Faculty of Mathematics, Kyushu University	International Workshop on Verified Computations and Related Topics 129pages	February 23, 2009
COE Lecture Note Vol.16	Alexander Samokhin	Volume Integral Equation Method in Problems of Mathematical Physics 50pages	February 24, 2009
COE Lecture Note Vol.17	矢嶋　　徹 及川　正行 梶原　健司 辻　　英一 福本　康秀	非線形波動の数理と物理 66pages	February 27, 2009
COE Lecture Note Vol.18	Tim Hoffmann	Discrete Differential Geometry of Curves and Surfaces 75pages	April 21, 2009
COE Lecture Note Vol.19	Ichiro Suzuki	The Pattern Formation Problem for Autonomous Mobile Robots —Special Lecture in Functional Mathematics— 23pages	April 30, 2009
COE Lecture Note Vol.20	Yasuhide Fukumoto Yasunori Maekawa	Math-for-Industry Tutorial: Spectral theories of non-Hermitian operators and their application 184pages	June 19, 2009
COE Lecture Note Vol.21	Faculty of Mathematics, Kyushu University	Forum “Math-for-Industry” Casimir Force, Casimir Operators and the Riemann Hypothesis 95pages	November 9, 2009
COE Lecture Note Vol.22	Masakazu Suzuki Hoon Hong Hirokazu Anai Chee Yap Yousuke Sato Hiroshi Yoshida	The Joint Conference of ASCM 2009 and MACIS 2009: Asian Symposium on Computer Mathematics Mathematical Aspects of Computer and Information Sciences 436pages	December 14, 2009
COE Lecture Note Vol.23	荒川　恒男 金子　昌信	多重ゼータ値入門 111pages	February 15, 2010
COE Lecture Note Vol.24	Fulton B.Gonzalez	Notes on Integral Geometry and Harmonic Analysis 125pages	March 12, 2010
COE Lecture Note Vol.25	Wayne Rossman	Discrete Constant Mean Curvature Surfaces via Conserved Quantities 130pages	May 31, 2010
COE Lecture Note Vol.26	Mihai Ciucu	Perfect Matchings and Applications 66pages	July 2, 2010

シリーズ既刊

Issue	Author／Editor	Title	Published
COE Lecture Note Vol.27	九州大学大学院 数理学研究院	Forum “Math-for-Industry” and Study Group Workshop Information security, visualization, and inverse problems, on the basis of optimization techniques　100pages	October 21, 2010
COE Lecture Note Vol.28	ANDREAS LANGER	MODULAR FORMS, ELLIPTIC AND MODULAR CURVES LECTURES AT KYUSHU UNIVERSITY 2010　62pages	November 26, 2010
COE Lecture Note Vol.29	木田　雅成 原田　昌晃 横山　俊一	Magma で広がる数学の世界　157pages	December 27, 2010
COE Lecture Note Vol.30	原　　隆 松井　　卓 廣島　文生	Mathematical Quantum Field Theory and Renormalization Theory 201pages	January 31, 2011
COE Lecture Note Vol.31	若山　正人 福本　康秀 高木　　剛 山本　昌宏	Study Group Workshop 2010 Lecture & Report　128pages	February 8, 2011
COE Lecture Note Vol.32	Institute of Mathematics for Industry, Kyushu University	Forum “Math-for-Industry” 2011 “TSUNAMI-Mathematical Modelling” Using Mathematics for Natural Disaster Prediction, Recovery and Provision for the Future　90pages	September 30, 2011
COE Lecture Note Vol.33	若山　正人 福本　康秀 高木　　剛 山本　昌宏	Study Group Workshop 2011 Lecture & Report　140pages	October 27, 2011
COE Lecture Note Vol.34	Adrian Muntean Vladimír Chalupecký	Homogenization Method and Multiscale Modeling　72pages	October 28, 2011
COE Lecture Note Vol.35	横山　俊一 夫　　紀恵 林　　卓也	計算機代数システムの進展　210pages	November 30, 2011
COE Lecture Note Vol.36	Michal Beneš Masato Kimura Shigetoshi Yazaki	Proceedings of Czech-Japanese Seminar in Applied Mathematics 2010 107pages	January 27, 2012
COE Lecture Note Vol.37	若山　正人 高木　　剛 Kirill Morozov 平岡　裕章 木村　正人 白井　朋之 西井　龍映 栄　伸一郎 穴井　宏和 福本　康秀	平成23年度 数学・数理科学と諸科学・産業との連携研究ワークショップ　拡がっていく数学　～期待される “見えない力” ～ 154pages	February 20, 2012

シリーズ既刊

Issue	Author／Editor	Title	Published
COE Lecture Note Vol.38	Fumio Hiroshima Itaru Sasaki Herbert Spohn Akito Suzuki	Enhanced Binding in Quantum Field Theory 204pages	March 12, 2012
COE Lecture Note Vol.39	Institute of Mathematics for Industry, Kyushu University	Multiscale Mathematics: Hierarchy of collective phenomena and interrelations between hierarchical structures 180pages	March 13, 2012
COE Lecture Note Vol.40	井ノ口順一 太田　泰広 筧　　三郎 梶原　健司 松浦　　望	離散可積分系・離散微分幾何チュートリアル2012 152pages	March 15, 2012
COE Lecture Note Vol.41	Institute of Mathematics for Industry, Kyushu University	Forum “Math-for-Industry” 2012 “Information Recovery and Discovery” 91pages	October 22, 2012
COE Lecture Note Vol.42	佐伯　　修 若山　正人 山本　昌宏	Study Group Workshop 2012 Abstract, Lecture & Report 178pages	November 19, 2012
COE Lecture Note Vol.43	Institute of Mathematics for Industry, Kyushu University	Combinatorics and Numerical Analysis Joint Workshop 103pages	December 27, 2012
COE Lecture Note Vol.44	萩原　　学	モダン符号理論からポストモダン符号理論への展望 107pages	January 30, 2013
COE Lecture Note Vol.45	金山　　寛	Joint Research Workshop of Institute of Mathematics for Industry (IMI), Kyushu University “Propagation of Ultra-large-scale Computation by the Domain-decomposition-method for Industrial Problems (PUCDIP 2012)” 121pages	February 19, 2013
COE Lecture Note Vol.46	西井　龍映 栄　伸一郎 岡田　勘三 落合　啓之 小磯　深幸 斎藤　新悟 白井　朋之	科学・技術の研究課題への数学アプローチ ―数学モデリングの基礎と展開― 325pages	February 28, 2013
COE Lecture Note Vol.47	SOO TECK LEE	BRANCHING RULES AND BRANCHING ALGEBRAS FOR THE COMPLEX CLASSICAL GROUPS 40pages	March 8, 2013
COE Lecture Note Vol.48	溝口　佳寛 脇　　隼人 平坂　　貢 谷口　哲至 島袋　　修	博多ワークショップ「組み合わせとその応用」 124pages	March 28, 2013

シリーズ既刊

Issue	Author／Editor	Title	Published
COE Lecture Note Vol.49	照井　章 小原　功任 濱田　龍義 横山　俊一 穴井　宏和 横田　博史	マス・フォア・インダストリ研究所　共同利用研究集会 II 数式処理研究と産学連携の新たな発展　137pages	August 9, 2013
MI Lecture Note Vol.50	Ken Anjyo Hiroyuki Ochiai Yoshinori Dobashi Yoshihiro Mizoguchi Shizuo Kaji	Symposium MEIS2013: Mathematical Progress in Expressive Image Synthesis　154pages	October 21, 2013
MI Lecture Note Vol.51	Institute of Mathematics for Industry, Kyushu University	Forum “Math-for-Industry” 2013 “The Impact of Applications on Mathematics”　97pages	October 30, 2013
MI Lecture Note Vol.52	佐伯　修 岡田　勘三 髙木　剛 若山　正人 山本　昌宏	Study Group Workshop 2013 Abstract, Lecture & Report 142pages	November 15, 2013
MI Lecture Note Vol.53	四方　義啓 櫻井　幸一 安田　貴徳 Xavier Dahan	平成25年度　九州大学マス・フォア・インダストリ研究所 共同利用研究集会　安全・安心社会基盤構築のための代数構造 ～サイバー社会の信頼性確保のための数理学～　158pages	December 26, 2013
MI Lecture Note Vol.54	Takashi Takiguchi Hiroshi Fujiwara	Inverse problems for practice, the present and the future　93pages	January 30, 2014
MI Lecture Note Vol.55	栄　伸一郎 溝口　佳寛 脇　隼人 渋田　敬史	Study Group Workshop 2013 数学協働プログラム Lecture & Report 98pages	February 10, 2014
MI Lecture Note Vol.56	Yoshihiro Mizoguchi Hayato Waki Takafumi Shibuta Tetsuji Taniguchi Osamu Shimabukuro Makoto Tagami Hirotake Kurihara Shuya Chiba	Hakata Workshop 2014 ~ Discrete Mathematics and its Applications ~　141pages	March 28, 2014
MI Lecture Note Vol.57	Institute of Mathematics for Industry, Kyushu University	Forum “Math-for-Industry” 2014: “Applications + Practical Conceptualization + Mathematics = fruitful Innovation”　93pages	October 23, 2014
MI Lecture Note Vol.58	安生健一 落合啓之	Symposium MEIS2014: Mathematical Progress in Expressive Image Synthesis　135pages	November 12, 2014

シリーズ既刊

Issue	Author／Editor	Title	Published
MI Lecture Note Vol.59	西井　龍映 岡田　勘三 梶原　健司 髙木　　剛 若山　正人 脇　　隼人 山本　昌宏	Study Group Workshop 2014 数学協働プログラム Abstract, Lecture & Report　196pages	November 14, 2014
MI Lecture Note Vol.60	西浦　　博	平成26年度九州大学 IMI 共同利用研究・研究集会（I） 感染症数理モデルの実用化と産業及び政策での活用のための新たな展開　120pages	November 28, 2014
MI Lecture Note Vol.61	溝口　佳寛 Jacques Garrigue 萩原　　学 Reynald Affeldt	研究集会 高信頼な理論と実装のための定理証明および定理証明器 Theorem proving and provers for reliable theory and implementations (TPP2014)　138pages	February 26, 2015
MI Lecture Note Vol.62	白井　朋之	Workshop on “β-transformation and related topics”　59pages	March 10, 2015
MI Lecture Note Vol.63	白井　朋之	Workshop on “Probabilistic models with determinantal structure” 107pages	August 20, 2015
MI Lecture Note Vol.64	落合　啓之 土橋　宜典	Symposium MEIS2015: Mathematical Progress in Expressive Image Synthesis　124pages	September 18, 2015
MI Lecture Note Vol.65	Institute of Mathematics for Industry, Kyushu University	Forum “Math-for-Industry” 2015 “The Role and Importance of Mathematics in Innovation”　74pages	October 23, 2015
MI Lecture Note Vol.66	岡田　勘三 藤澤　克己 白井　朋之 若山　正人 脇　　隼人 Philip Broadbridge 山本　昌宏	Study Group Workshop 2015 Abstract, Lecture & Report 156pages	November 5, 2015
MI Lecture Note Vol.67	Institute of Mathematics for Industry, Kyushu University	IMI-La Trobe Joint Conference “Mathematics for Materials Science and Processing” 66pages	February 5, 2016
MI Lecture Note Vol.68	古庄　英和 小谷　久寿 新甫　洋史	結び目と Grothendieck-Teichmüller 群 116pages	February 22, 2016
MI Lecture Note Vol.69	土橋　宜典 鍛治　静雄	Symposium MEIS2016: Mathematical Progress in Expressive Image Synthesis　82pages	October 24, 2016
MI Lecture Note Vol.70	Institute of Mathematics for Industry, Kyushu University	Forum “Math-for-Industry” 2016 “Agriculture as a metaphor for creativity in all human endeavors” 98pages	November 2, 2016
MI Lecture Note Vol.71	小磯　深幸 二宮　嘉行 山本　昌宏	Study Group Workshop 2016 Abstract, Lecture & Report　143pages	November 21, 2016

シリーズ既刊

Issue	Author／Editor	Title	Published
MI Lecture Note Vol.72	新井　朝雄 小嶋　　泉 廣島　文生	Mathematical quantum field theory and related topics　133pages	January 27, 2017
MI Lecture Note Vol.73	穴田　啓晃 Kirill Morozov 須賀　祐治 奥村　伸也 櫻井　幸一	Secret Sharing for Dependability, Usability and Security of Network Storage and Its Mathematical Modeling　211pages	March 15, 2017
MI Lecture Note Vol.74	QUISPEL, G. Reinout W. BADER, Philipp MCLAREN, David I. TAGAMI, Daisuke	IMI-La Trobe Joint Conference Geometric Numerical Integration and its Applications　71pages	March 31, 2017
MI Lecture Note Vol.75	手塚　　集 田上　大助 山本　昌宏	Study Group Workshop 2017 Abstract, Lecture & Report　118pages	October 20, 2017
MI Lecture Note Vol.76	宇田川誠一	Tzitzéica 方程式の有限間隙解に付随した極小曲面の構成理論 ―Tzitzéica 方程式の楕円関数解を出発点として―　68pages	August 4, 2017
MI Lecture Note Vol.77	松谷　茂樹 佐伯　　修 中川　淳一 田上　大助 上坂　正晃 Pierluigi Cesana 濵田　裕康	平成29年度　九州大学マス・フォア・インダストリ研究所 共同利用研究集会（I） 結晶の界面，転位，構造の数理　148pages	December 20, 2017
MI Lecture Note Vol.78	瀧澤　重志 小林　和博 佐藤憲一郎 斎藤　　努 清水　正明 間瀬　正啓 藤澤　克樹 神山　直之	平成29年度　九州大学マス・フォア・インダストリ研究所 プロジェクト研究　研究集会（I） 防災・避難計画の数理モデルの高度化と社会実装へ向けて 136pages	February 26, 2018
MI Lecture Note Vol.79	神山　直之 畔上　秀幸	平成29年度　AIMaP チュートリアル 最適化理論の基礎と応用　96pages	February 28, 2018
MI Lecture Note Vol.80	Kirill Morozov Hiroaki Anada Yuji Suga	IMI Workshop of the Joint Research Projects Cryptographic Technologies for Securing Network Storage and Their Mathematical Modeling　116pages	March 30, 2018
MI Lecture Note Vol.81	Tsuyoshi Takagi Masato Wakayama Keisuke Tanaka Noboru Kunihiro Kazufumi Kimoto Yasuhiko Ikematsu	IMI Workshop of the Joint Research Projects International Symposium on Mathematics, Quantum Theory, and Cryptography　246pages	September 25, 2019
MI Lecture Note Vol.82	池森　俊文	令和2年度　AIMaP チュートリアル 新型コロナウイルス感染症にかかわる諸問題の数理 145pages	March 22, 2021

シリーズ既刊

Issue	Author／Editor	Title	Published
MI Lecture Note Vol.83	早川健太郎 軸丸　芳揮 横須賀洋平 可香谷　隆 林　　和希 堺　　雄亮	シェル理論・膜理論への微分幾何学からのアプローチと その建築曲面設計への応用　49pages	July 28, 2021
MI Lecture Note Vol.84	Taketoshi Kawabe Yoshihiro Mizoguchi Junichi Kako Masakazu Mukai Yuji Yasui	SICE-JSAE-AIMaP Tutorial Advanced Automotive Control and Mathematics　110pages	December 27, 2021
MI Lecture Note Vol.85	Hiroaki Anada Yasuhiko Ikematsu Koji Nuida Satsuya Ohata Yuntao Wang	IMI Workshop of the Joint Usage Research Projects Exploring Mathematical and Practical Principles of Secure Computation and Secret Sharing　114pages	February 9, 2022
MI Lecture Note Vol.86	濱田　直希 穴井　宏和 梅田　裕平 千葉　一永 佐藤　寛之 能島　裕介 加葉田雄太朗 一木　俊助 早野　健太 佐伯　　修	2020年度採択分　九州大学マス・フォア・インダストリ研究所 共同利用研究集会 進化計算の数理　135pages	February 22, 2022
MI Lecture Note Vol.87	Osamu Saeki, Ho Tu Bao, Shizuo Kaji, Kenji Kajiwara, Nguyen Ha Nam, Ta Hai Tung, Melanie Roberts, Masato Wakayama, Le Minh Ha, Philip Broadbridge	Proceedings of Forum “Math-for-Industry” 2021 -Mathematics for Digital Economy-　122pages	March 28, 2022
MI Lecture Note Vol.88	Daniel PACKWOOD Pierluigi CESANA, Shigenori FUJIKAWA, Yasuhide FUKUMOTO, Petros SOFRONIS, Alex STAYKOV	Perspectives on Artificial Intelligence and Machine Learning in Materials Science, February 4-6, 2022　74pages	November 8, 2022

シリーズ既刊

Issue	Author／Editor	Title	Published
MI Lecture Note Vol.89	松谷　茂樹 落合　啓之 井上　和俊 小磯　深幸 佐伯　　修 白井　朋之 垂水　竜一 内藤　久資 中川　淳一 濵田　裕康 松江　　要 加葉田雄太朗	2022年度採択分 九州大学マス・フォア・インダストリ研究所 共同利用研究集会 材料科学における幾何と代数 III　356pages	December 7, 2022
MI Lecture Note Vol.90	中山　尚子 谷川　拓司 品野　勇治 近藤　正章 石原　　亨 鍛冶　静雄 藤澤　克樹	2022年度採択分 九州大学マス・フォア・インダストリ研究所 共同利用研究集会 データ格付けサービス実現のための数理基盤の構築　58pages	December 12, 2022
MI Lecture Note Vol.91	Katsuki Fujisawa Shizuo Kaji Toru Ishihara Masaaki Kondo Yuji Shinano Takuji Tanigawa Naoko Nakayama	IMI Workshop of the Joint Usage Research Projects Construction of Mathematical Basis for Realizing Data Rating Service 610pages	December 27, 2022
MI Lecture Note Vol.92	丹田　　聡 三宮　　俊 廣島　文生	2022年度採択分 九州大学マス・フォア・インダストリ研究所 共同利用研究集会 時間・量子測定・準古典近似の理論と実験 ～古典論と量子論の境界～　150pages	Janualy 6, 2023
MI Lecture Note Vol.93	Philip Broadbridge Luke Bennetts Melanie Roberts Kenji Kajiwara	Proceedings of Forum “Math-for-Industry” 2022 -Mathematics of Public Health and Sustainability-　170pages	June 19, 2023

九州大学マス・フォア・インダストリ研究所
九州大学大学院 数理学府
〒819-0395 福岡市西区元岡744　TEL 092-802-4402　FAX 092-802-4405
URL https://www.imi.kyushu-u.ac.jp/