Misuseシナリオにおける格子暗号への秘密鍵・乱数復元攻撃

東京大学大学院情報理工学系研究科
岡田 怜士

2021.11.17
新世代暗号の設計・評価
@九州大学

紹介する研究

1. 格子暗号NewHopeに対する鍵不一致攻撃の改良
   - Satoshi Okada, Yuntao Wang, and Tsuyoshi Takagi, “Improving key mismatch attack on NewHope with fewer queries”, *The 25th Australasian Conference on Information Security and Privacy (ACISP 2020)*, Springer LNCS, Vol. 12248, pp. 505-524, 2020.

2. 格子暗号CRYSTALS-KYBERとSABERに対する乱数再利用攻撃
   - Satoshi Okada and Yuntao Wang, “Recovery attack on Bob's reused randomness in CRYSTALS-KYBER and SABER”, *The 15th International Conference on Provable and Practical Security (ProvSec 2021)*, Springer LNCS, Vol. 13059, pp. 155-173, 2021.

Misuse scenarioとは

- “a **misuse situation** where the same key pair is reused for multiple key establishment by the private key owner”
  - Bauer, Aurélie, et al. “Assessment of the key-reuse resilience of NewHope.” *Cryptographers’ track at the RSA conference (CT-RSA 2021)*. Springer, Cham, 2019.

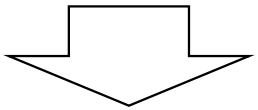
- 鍵や乱数の再利用
  - プロトコルの仕様としては、毎回鍵や乱数はリフレッシュされる
  - 実利用や派生したプロトコルではそのように明記されていない場合も
    ex.) TLS 1.3のpre-shared key mode, SIGMA protocol

1. 格子暗号NewHopeに対する鍵不一致攻撃の改良

研究内容

格子暗号NewHopeに対する鍵不一致攻撃の改良

- 既存研究[Qin et al.@ESORICS 2019]
  - 攻撃成功確率：96.9%
  - 攻撃に要するクエリ数が大きい



- 提案手法
  - 攻撃成功確率：**100.0%**
  - クエリ数：約**42%削減**

目次

1. 研究背景・準備
2. NewHopeに対する鍵不一致攻撃
3. 提案手法
4. 実験・結果
5. まとめ

目次

研究背景

- 米国国立標準技術研究所（NIST）による、耐量子暗号の標準化
  - NewHope, CRYSTALS-KYBER, SABER, …
  - 現在third roundまで進んでいる

- 鍵交換プロトコル (NewHope)
  - Second -> Third roundで落選..

出典:https://news.mynavi.jp/photo/article/20171117-a245/images/001l.jpg

出典:https://www.nist.gov/

数学的準備

- Z_q: 法をqとした整数の剰余環
- $Z_q[x]$: 全ての係数が Z_qである多項式環
- R_q: $x^n + 1$を法とした$Z_q[x]$の剰余環, $Z_q[x]/(x^n + 1)$
- $c[i](c \in R_q)$: 多項式cのx^iの係数
- $\lfloor x \rfloor$はxを超えない最大の整数

目次

1. 研究背景・準備
2. NewHopeに対する鍵不一致攻撃
3. 提案手法
4. 実験・結果
5. まとめ

NewHope[Alkim et al.@USENIX2016]

- Ring-LWEベースの格子暗号

$$(a, b = as + e) \in R_q \times R_q$$

- NewHopeとRing-LWE
  - 公開鍵：$P_A = as_A + e_A$
  - 暗号化：$c = P_A s_B + e' + encode(m)$
- 秘密鍵の復元
  - 係数$s[i] \in [-8, 8]$（二項分布）
  - 総当たり攻撃 → 17^{1024}という膨大な計算量

	n	q	Security level	Security category
NewHope 512	512	12289	AES-128	I
NewHope 1024	1024	12289	AES-256	V

NewHope への鍵不一致攻撃 [Alkim et al.@USENIX2016]

不正なクエリの受付

サーバ

クライアント

攻撃者

再利用

1.
公開鍵P_A, 秘密鍵s_A

2.
公開鍵P_A

3.
共有鍵key_B
公開鍵P_B, 秘密鍵s_B
$cap = \mathrm{Enc}(P_A, P_B, key_B)$

4.
公開鍵P_B, キーのカプセルcap
共有鍵key_Bに関する情報

これらクエリを選択する

5.
$key_A = \mathrm{Dec}(s_A, P_B, cap)$

6.
共有鍵の一致不一致

7.
共有鍵で暗号化通信

一致不一致からs_Aを推測

NewHopeのプロトコル

pre-shared key $\mathbf{a}$		
Alice		Bob
$\mathbf{s}_A, \mathbf{e}_A \xleftarrow{\$} \psi_8^n$		
$\mathbf{P}_A \leftarrow \mathbf{a}\mathbf{s}_A + \mathbf{e}_A$	$\xrightarrow{\mathbf{P}_A}$	$\mathbf{s}_B, \mathbf{e}_B, \mathbf{e}'_B \xleftarrow{\$} \psi_8^n$ $\mathbf{P}_B \leftarrow \mathbf{a}\mathbf{s}_B + \mathbf{e}_B$ $\nu_B \xleftarrow{\$} \{0,1\}^{256}$ $\nu'_B \leftarrow \text{SHA3-256}(\nu_B)$ $\mathbf{k} \leftarrow \texttt{Encode}(\nu'_B)$ $\mathbf{c} \leftarrow \mathbf{P}_A\mathbf{s}_B + \mathbf{e}'_B + \mathbf{k}$
$\mathbf{c}' \leftarrow \texttt{Decompress}(\overline{\mathbf{c}})$ $\mathbf{k}' = \mathbf{c}' - \mathbf{P}_B\mathbf{s}_A$ $\nu'_A \leftarrow \texttt{Decode}(\mathbf{k}')$ $S_{k_A} \leftarrow \text{SHA3-256}(\nu'_A)$	$\xleftarrow{(\mathbf{P}_B, \overline{\mathbf{c}})}$	$\overline{\mathbf{c}} \leftarrow \texttt{Compress}(\mathbf{c})$ $S_{k_B} \leftarrow \text{SHA3-256}(\nu'_B)$

Algorithm 3: $\texttt{Encode}(\nu'_B)$

Input: $\nu'_B \in \{0,1\}^{256}$
Output: $\mathbf{k} \in \mathcal{R}_q$

```
k ← 0
for i ← 0 to 255 do
    for j ← 0 to 3 do
        k[i + 256j] ← 4s · ν'_B[i]
Return k
```

Algorithm 4: $\texttt{Decode}(\mathbf{k}')$

Input: $\mathbf{k}' \in \mathcal{R}_q$
Output: $\nu'_A \in \{0,1\}^{256}$

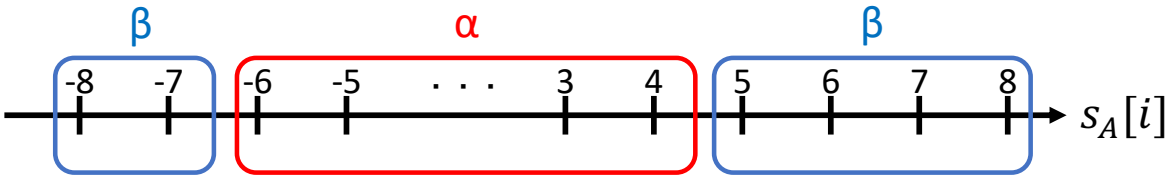
```
ν'_A ← 0
for i ← 0 to 255 do
    m ← Σ_{j=0}^{3} |k'[i + 256j] − 4s|
    if m < q then
        ν'_A[i] ← 1
    else
        ν'_A[i] ← 0
Return ν'_A
```

既存の攻撃手法1[Bauer et al.@CT-RSA2019]

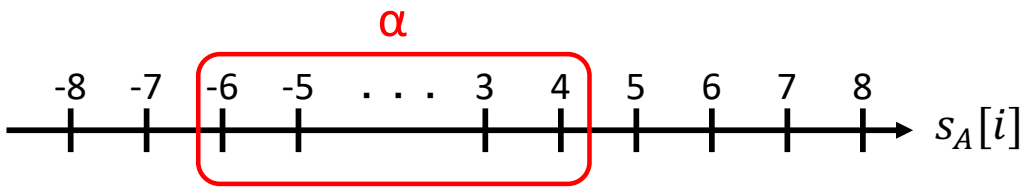
- 初めてNewHopeに対する鍵不一致攻撃を提案
  - $s_A[i]$の値で場合分け

- αへの攻撃を提案
  - ただし復元成功率は**75%**と高くなかった

- βへの攻撃
  - ブルートフォース攻撃を実施
  - {-8, -7, 5, 6, 7, 8}は1つの秘密鍵に平均10個→6^{10} $(\sim 6\times 10^7)$の計算量



既存研究の攻撃手法1[Bauer et al.@CT-RSA2019]



例： $s_A = 4x^3 + 3x^2 - 7x + 1$の$s_A[2]$

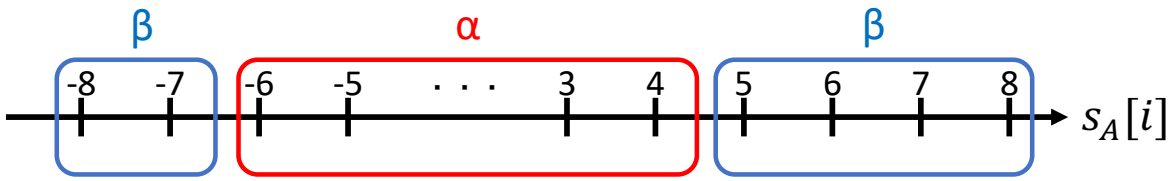
1. $P_B = x^{-2}$, $c = \sum_{j=0}^{3} l_j x^j$, $key_B = 1$と設定

2. $c - P_B s_A = (l_3 - 7)x^3 - (l_2 + 1)x^2 + (l_1 - 4)x + l_0 - 3$
3. $m = |l_0 - 3| + |l_1 - 4| + |l_2 + 1| + |l_3 - 7|$
4. $m < 8 \rightarrow key_A = 1,\ m \geq 8 \rightarrow key_A = 0$

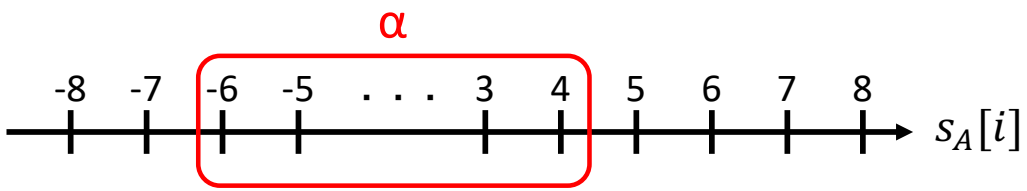
5. $l_0 = -4 \sim 3 \rightarrow s_A[2]$を特定

既存研究の攻撃手法2[Qin et al.@ESORICS2019]

- Bauerらによる攻撃を改良
- αへの攻撃を改良
  - 復元成功率は**99.2%**
- βに対して新たな効率的なアルゴリズムを提案



既存研究の攻撃手法2[Qin et al.@ESORICS2019]



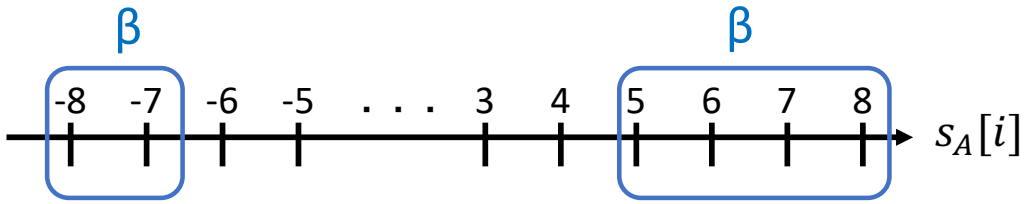
$s_A[i] = 3$を求める

1. Bauerらの攻撃を実施
2. 推測値τを50個収集
3. 内訳から$s_A[i]$ を決定

決して求められない秘密鍵
約6%

例）35個がτ = 3, 15個がτ = 2 → $s_A[i] = 3$

既存研究の攻撃手法2[Qin et al.@ESORICS2019]



$s_A[i] = -7$を求める

※ $s_A[i+256], s_A[i+512], s_A[i+768]$：既知

1. Bauerらの攻撃を実施

   → $s_A[i]$ の正負のみ

2. 新しい攻撃手法で$|s_A[i]| = 7$ を導出

   →正負から$s_A[i]$ を決定

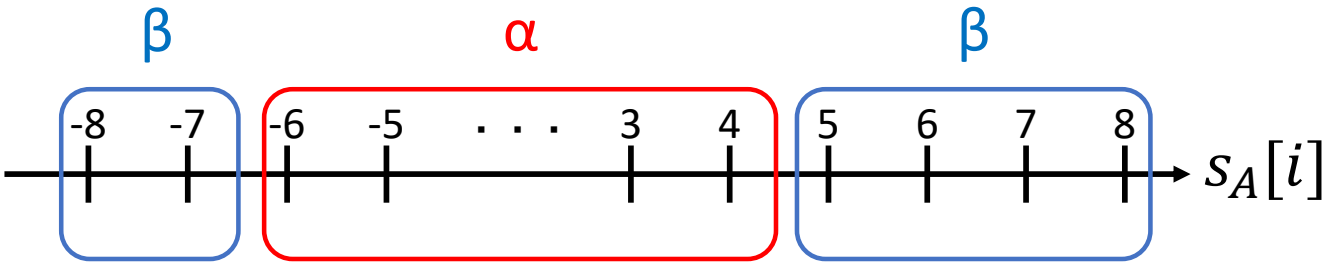
攻撃成功確率：**約11%**
必要クエリ数：**約1000**

目次

1. 研究背景・準備
2. NewHopeに対する鍵不一致攻撃
3. 提案手法
4. 実験・結果
5. まとめ

既存研究で着目した点

- 領域βに対する攻撃
  - 攻撃成立条件
  - 攻撃成立可能性: 高くても約11%
- 決して復号できない秘密鍵s_A ：約6%
- 1つの秘密鍵を復号する際に要するクエリ数が約880,000

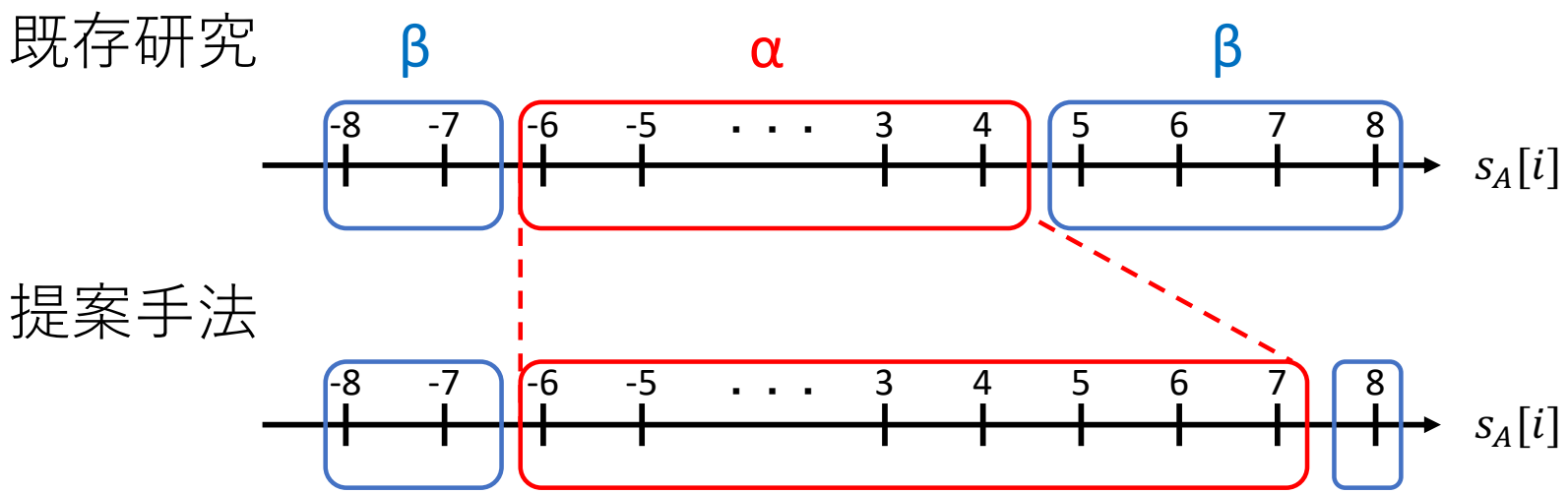


既存研究で着目した点

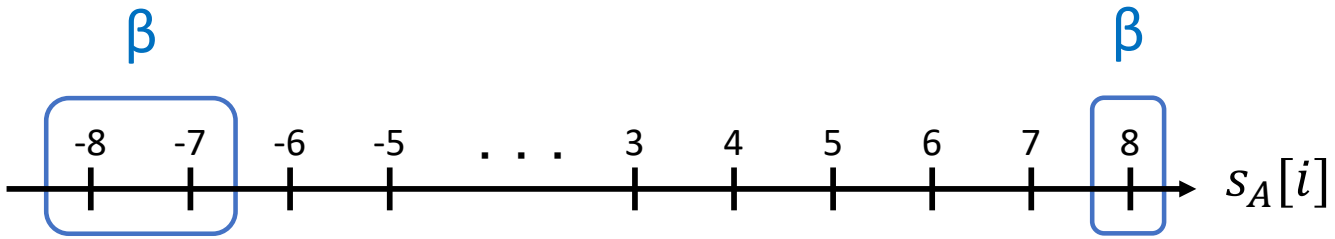
- 領域βに対する攻撃
  - 攻撃成立条件
  - 攻撃成立可能性: 高くても約11%
- 決して復号できない秘密鍵s_A ：約6%
- 1つの秘密鍵を復号する際に要するクエリ数が約880,000

改良1

- 既存研究の領域αに対する攻撃を[-6,7]まで拡張
  - 詳細は後述



改良1



- 領域βに対する攻撃
  - {-8, -7, 8}：秘密鍵１つあたり平均0.28個(二項分布より)
  - 総当たり攻撃を行う

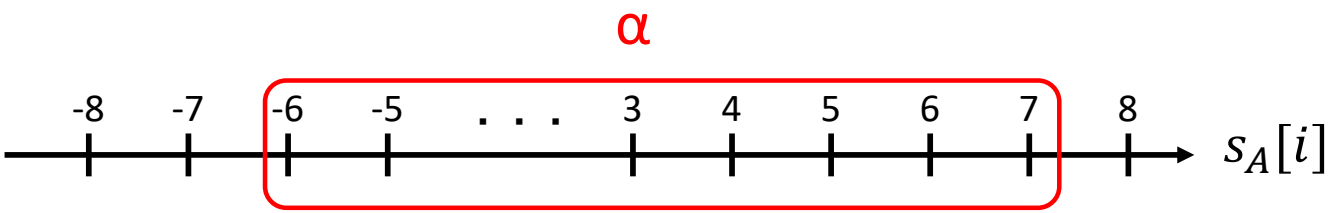
    →攻撃成立に必要な条件無し
  - 必要クエリ数：平均（最悪）$3^{0.28} < 1000$

➡ 攻撃成功率の上昇、クエリ数の削減

既存研究で着目した点

- 領域βに対する攻撃
  - 攻撃成立条件
  - 攻撃成立可能性: 高くても約11%
- 決して復号できない秘密鍵s_A ：約6%
- 1つの秘密鍵を復号する際に要するクエリ数が約880,000

改良2



- クエリの生成方法の改良

既存研究

- $P_B = \frac{1}{2}\left\lfloor \frac{q}{8} \right\rfloor x^{-i}$
- $key_B = [1, 0, 0, \ldots, 0]$

提案手法

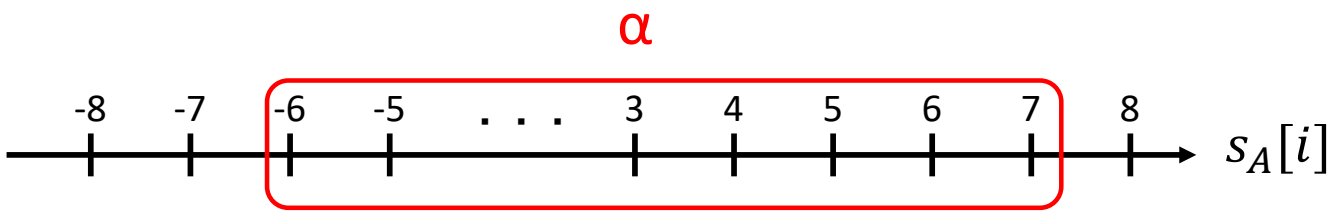
- $P_B = \frac{1}{2}\left\lfloor \frac{q}{8} \right\rfloor x^{\boldsymbol{i}}$
- key_B: 秘密鍵毎に探索、設定

ほぼ全ての秘密鍵が復号可能

既存研究で着目した点

- 領域βに対する攻撃
  - 攻撃成立条件
  - 攻撃成立可能性: 高くても約11%
- 決して復号できない秘密鍵s_A ：約6%
- 1つの秘密鍵を復号する際に要するクエリ数が約880,000

改良3



- 推測値τから$s_A[i]$を決定する手法を改良

既存研究

例： $s_A[i] = 3$

- 推測値τを50個集める
- 内訳が2が15個、3が35個
  →$s_A[i] = 3$と決定

提案手法

- $s_A[i] = k$
  → 推測値は必ず$\tau = k - 1\ or\ k$
- 2種類のτ or 1種類のτをp回得たらクエリを停止

クエリ数の削減

改良3の補足

- 実は[-8, 8] の全ての係数が前のページの方法で復元可能

- $\tau = 8$が得られた時
  - 沢山クエリを投げると、高い確率で$s_A[i]$が {-8, -7, 8} の内どれかを判別できる

- {-8, -7, 8}の登場回数は非常に少ない（平均0.28個）のでブルートフォースの方が精度も高く低コスト

$s_A[i]$	-8	7		8	
τ	8	8	-7	7	8

目次

実験詳細

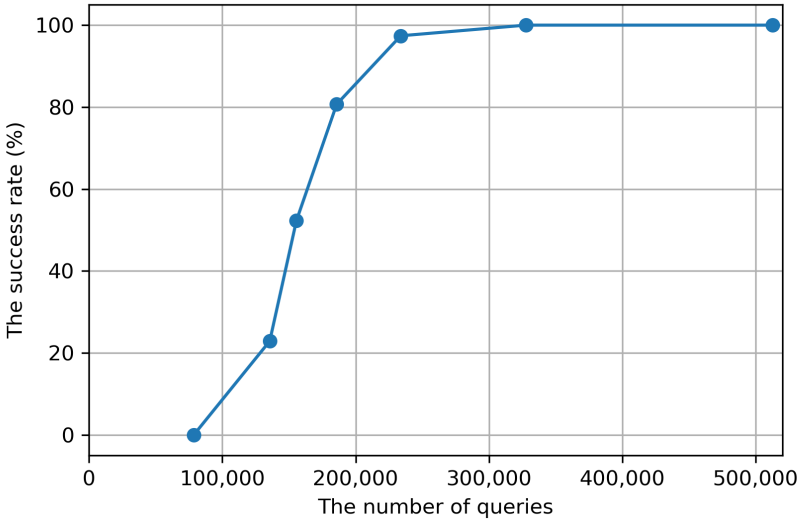
- Python3のnumpy.poly1dを用いてパラメータ(n,q)=(1024, 12289)のNewHope1024-CPA-KEMを実装

- ランダムに生成された秘密鍵1000個を復元

- パラメータpの値を変えて、必要なクエリの数と成功率の関係を調査

実験結果

- 必要なクエリの数と成功率間にトレードオフ
  （左から右へ p= 5, 10, 12, 15, 20, 30, 50）
- p = 20の場合、成功率はQinらのものとほぼ同じで、クエリの数は約73%減少



	Yue Qin, et al.	Our attack
The success rate	96.9%	**97.4%**
The number of queries	879,725	**233,803**

約73%減

目次

1. 研究背景・準備
2. NewHopeに対する鍵不一致攻撃
3. 提案手法
4. 実験・結果
5. まとめ

まとめ

- NewHopeに対する鍵不一致攻撃の改良
  →クエリ数は大幅に減少、攻撃成功率上昇

- 攻撃成立条件

  1. 不正なクエリの受付 → 藤崎・岡本変換を施したIND-CCA安全なNewHope
  2. 秘密鍵の再利用 → 定期的な秘密鍵のリフレッシュ

参考研究

- Huguenin-Dumittan, Loïs, and Serge Vaudenay. "Classical misuse attacks on NIST round 2 PQC." *International Conference on Applied Cryptography and Network Security (ACNS 2020)*. Springer, Cham, 2020.

- NIST標準化のsecond roundまで残っている暗号に対する鍵不一致攻撃
  - LACやCRYSTALS-KYBER, SABERに対する攻撃手法を提案

2. 格子暗号CRYSTALS-KYBERとSABERに対する乱数再利用攻撃

研究概要

- 格子暗号CRYSTALS-KYBERとSABER *に対する鍵再利用攻撃の提案

- 既存研究[Wang et al.@ProvSec2020]
  - 格子暗号NewHope, LACに対する鍵再利用攻撃

- 提案手法
  - Wangらの手法を拡張・応用
  - CRYSTALS-KYBERとSABERへの鍵再利用攻撃の提案
  - 攻撃成功率：100%, 必要クエリ数: 最大で6クエリ

* NIST耐量子暗号標準化における有力候補

目次

1. 研究背景・準備
2. 提案手法
3. 実験・結果
4. まとめ

目次

1. 研究背景・準備
2. 提案手法
3. 実験・結果
4. まとめ

CRYSTALS-KYBER[Bos et al. @EuroS&P 2018]

- Module-LWEベースの格子暗号

$$(\boldsymbol{a}, b = \boldsymbol{a}^T \boldsymbol{s} + e) \in R_q^{k \times 1} \times R_q$$

- CRYSTALS-KYBERとModule-LWE
  - 公開鍵：$\boldsymbol{P_A} = \boldsymbol{A}^T \boldsymbol{s_A} + \boldsymbol{e}$
  - 暗号化：$c = \boldsymbol{P_A}^T \boldsymbol{s_B} + e' + \lceil \frac{q}{2} \rfloor m$
- 秘密鍵の復元
  - $\boldsymbol{s_B}[i] \in [-2, 2]$
  - 総当たり攻撃: 最悪5^{nk}の計算量

	n	k	q	Security level
Kyber-512	256	3	3329	Ⅰ (AES-128)
Kyber-768	256	4	3329	Ⅲ (AES-192)
Kyber-1024	256	5	3329	Ⅴ (AES-256)

SABER[D'Anvers et al. @AFRICACRYPT2018]

- Module-LWRベースの格子暗号

$$\left(\boldsymbol{a}, b = \left\lfloor \frac{q}{p} \boldsymbol{a}^T \boldsymbol{s} \right\rfloor\right) \in R_q^{k \times 1} \times R_p$$

- SABERとModule-LWR ※$\epsilon_x = \log x$
  - 公開鍵：$\boldsymbol{P_A} = (\boldsymbol{A}^T \boldsymbol{s_A} + \boldsymbol{h}) \gg (\epsilon_q - \epsilon_p)$
  - 暗号化：$c = \left(\boldsymbol{P_A^T}\, \boldsymbol{s_B} + h_1 - \frac{p}{2} m\right) \gg (\epsilon_p - \epsilon_T)$
- 秘密鍵の復元
  - $\boldsymbol{s_B}[i] \in [-\frac{\mu}{2}, \frac{\mu}{2}]$
  - 総当たり攻撃: 最悪$(\mu + 1)^{nk}$の計算量

	n	k	q	p	T	μ	Security level
Light-Saber	256	2	8192	2^{10}	2^3	10	Ⅰ (AES-128)
Saber	256	3	8192	2^{10}	2^4	8	Ⅲ (AES-192)
Fire-Saber	256	4	819	2^{10}	2^6	6	Ⅴ (AES-256)

乱数再利用攻撃

Alice Eve

Bob

不正なクエリの受付

1.
公開鍵P_A, 秘密鍵s_A

自由に選択する

2.
公開鍵P_A

3.
共有鍵key_B
公開鍵P_B, 秘密乱数s_B
$c = \mathrm{Enc}(P_A, s_B, key_B)$

再利用

4.
公開鍵P_B, 暗号文 c

これらからs_Bを復元

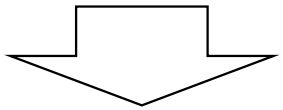
5.
$key_A = \mathrm{Dec}(s_A, P_B, c)$

7.
共有鍵で暗号化通信

meta-PKEモデル[Wang et al.@ProvSec2020]

- 格子暗号におけるPKEの暗号化のステップを抽象化
- CRYSTALS-KYBERにおける暗号化

$$v_B = P_A^T s_B + e'_B + m$$



$$V = B \times t + f + Y$$

meta-PKEにおける定理[Wang et al.@ProvSec2020]

補題 3 [Wang et al.@ProvSec2020]

$t, f, Y \in R_q, t[i], f[i] \in \{-D, \ldots, D\}, D \ll q, Y_i \in \left\{0, \frac{q}{2}\right\}, B \in Z_q,$

$V = t \times B + f + Y \ (mod\ q)$ とする時、$2D + 1 \leq B < \frac{q}{4D} - 1$であれば、 Vから t, f, Yの全ての係数が復元できる。

- VがCompressされていない時のみ成立

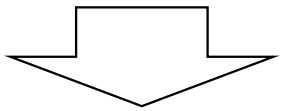
目次

1. 研究背景・準備
2. 提案手法
3. 実験・結果
4. まとめ

提案手法の考え方

- Wangらの定理を改良・拡張
  - VがCompressされていても、秘密鍵が復元可能
  - CRYSTALS-KYBER, SABERに適応

- Wangらの定理
  - Vを写像と見た時に (t, f, Y)に対してVが単射になるための条件



Compress$(V(t, Y))$が単射になる条件を探す

提案する定理（CRYSTALS-KYBER）

定理 4

$t, f, Y \in R_q, t[i], f[i] \in \{-D, \dots, D\}, D \ll q, Y_i \in \left\{0, \frac{q}{2}\right\}, B \in Z_q$ とし、$V = t \times B + f + Y \ (mod\ q)$ とする。また、Compress関数

Compress: $Z_q \to Z_p$ を $\lceil \frac{p}{q} x \rfloor$ とする時 $\left\lfloor \frac{p(B-2D)}{q} \right\rfloor = 1, \frac{p\left(\frac{q}{2}-2DB-2D\right)}{q} \geq 1,$ $4D + 2 \leq p$ の3条件が満たされた場合、Compress(V) から t, Y を完全に復元することができる。

証明のイメージ

- $V = t \times B + f + Y\ (mod\ q)$ において攻撃者が設定するのはB
  - B を整数 (Z_q) の場合を考える

- この設定下でCompress(V)がtに関して単射になる条件を考えている

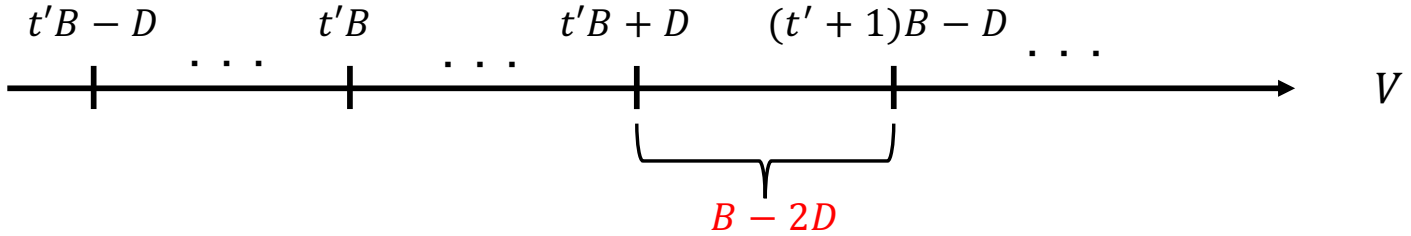
- 単射とは
  - $V_1 = t_1 \times B + f_1 + Y_1, V_2 = t_2 \times B + f_2 + Y_2$
  - $t_1, t_2 \in \{-D, \dots, D\}$ について、
    $t_1 \neq t_2 \Longrightarrow$ Comress($V_1(t_1)$) ≠ Comress($V_2(t_2)$)

証明のイメージ

- $V = t \times B + f + Y$の係数が取り得る値の範囲

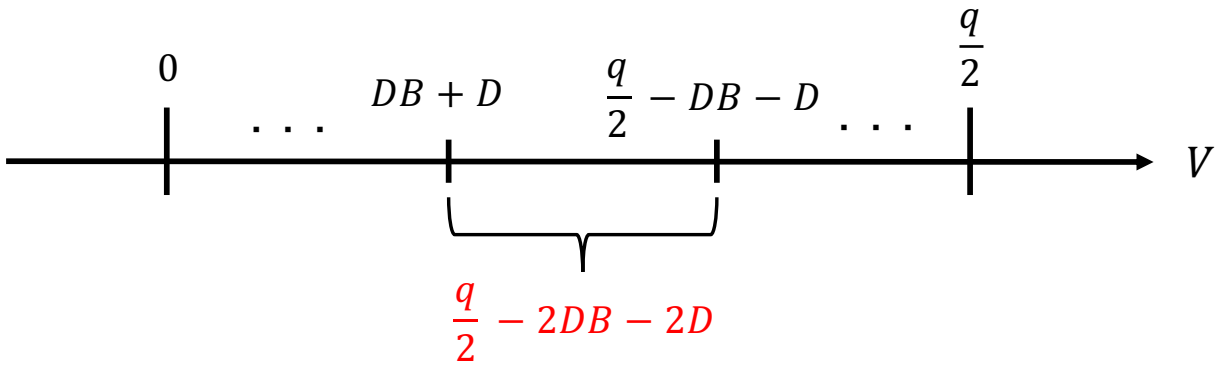
$$V[i] \in (\{-DB - D, -DB - (D-1), \quad \dots, DB + (D-1), DB + D\} \cup \{-DB - D + \frac{q}{2}, -DB - (D-1) + \frac{q}{2}, \dots, DB + D + \frac{q}{2}\})$$

- $V_1 = t_1 \times B + f_1 + Y_1, V_2 = t_2 \times B + f_2 + Y_2$において、$Y_1$と$Y_2$が同じ値の時$V_1$と$V_2$の差の最小値
  - この差分をcompress関数に通した時に1になれば、 Comress(V) は1刻みになる



証明のイメージ

- Y_1とY_2が異なる値の時V_1とV_2の差の最小値は



- この差分をcompress関数に通した時に1以上になれば、Compress(V) の値が重複しない

証明のイメージ

- 以上の2条件が満たされる時、Compress(V)のimageのサイズは$4D+2$になる

- これはCompress: $Z_q \to Z_p$を踏まえると、$4D+2 \leq p$が必要

提案する定理（SABER）

定理 5

$t, f, Y \in R_q, t[i], f[i] \in \{-D, \dots, D\}, p = 2^{\epsilon_p}, T = 2^{\epsilon_T},\ D \ll p, Y_i \in \left\{0, \frac{p}{2}\right\}, B \in Z_q$とし、$V = t \times B + f + Y\ (mod\ q)$ とする。この時、$B \gg \left(\epsilon_p - \epsilon_T\right) = 1, \left(\frac{p}{2} - 2DB\right) \gg \left(\epsilon_p - \epsilon_T\right) \geq 1,\ 4D + 2 \leq p$ の3条件が満たされた場合、$V \gg \left(\epsilon_p - \epsilon_T\right)$ から t, Yを完全に復元することができる。

攻撃手法（CRYSTALS-KYBER）

- Kyber-768, Kyber-1024
  - 定理4を満たす
  - 1クエリで1つの多項式が復元可能
  - 必要クエリ数は秘密鍵ベクトルのサイズkに等しい

$c[j]$ $\mathbf{s}_{Bi}[j]$ / $m[j]$	-2	-1	0	1	2
0	14	15	0	1	2
1	6	7	8	9	10

Kyber-1024, B = 213

$c[j]$ $\mathbf{s}_{Bi}[j]$ / $m[j]$	-2	-1	0	1	2
0	30	31	0	1	2
1	14	15	16	17	18

Kyber-1024, B = 105

攻撃手法（CRYSTALS-KYBER）

- Kyber-512
  - 定理4を満たさないため、1クエリで秘密鍵の一部しか復元できない
  - 1つの多項式を復元するために最大2クエリ必要
  - 最大$2k$クエリ必要

B	421					631				
$c[j]$ $\mathbf{s}_{Bi}[j]$ / $m[j]$	-2	-1	0	1	2	-2	-1	0	1	2
0	6	7	0	1	2	5	6	0	2	3
1	2	3	4	5	6	1	2	4	6	7

Kyber-512, B = 421, 631

攻撃手法（SABER）

- Fire-Saber
  - 定理5を満たす
  - 必要クエリ数は秘密鍵ベクトルのサイズ$k(=4)$に等しい

$c[j]$ \ $\mathbf{s}_{Bi}[j]$ / $m[j]$	-3	-2	-1	0	1	2	3
0	61	62	63	0	1	2	3
1	29	30	31	32	33	34	35

FireSaber, B = 16

攻撃手法（SABER）

- Saber
  - 定理5を満たさない
  - 1つの多項式を復元するために最大2クエリ必要
  - 最大$2k(=6)$クエリ必要

B	64									96								
$c[j]$ $\mathbf{s}_{Bi}[j]$ / $m[j]$	-4	-3	-2	-1	0	1	2	3	4	-4	-3	-2	-1	0	1	2	3	4
0	12	13	14	15	0	1	2	3	4	10	11	13	14	0	1	3	4	6
1	4	5	6	7	8	9	10	11	12	2	3	5	6	8	9	11	12	14

Saber, B = 64, 96

攻撃手法（SABER）

- Light-Saber
  - 定理5を満たさない
  - 最大$3k\ (=6)$クエリ必要

$c[j]$ \ $\mathbf{s}_{Bi}[j]$ / $m[j]$	-5	-4	-3	-2	-1	0	1	2	3	4	5
0	3	4	5	6	7	0	1	2	3	4	5
1	7	0	1	2	3	4	5	6	7	0	1

LightSaber, B = 128

B	16										
$c[j]$ \ $\mathbf{s}_{Bi}[j]$ / $m[j]$	-5	-4	-3	-2	-1	0	1	2	3	4	5
0	7	7	7	7	7	0	0	0	0	0	0
1	3	3	3	3	3	4	4	4	4	4	4

192										
-5	-4	-3	-2	-1	0	1	2	3	4	5
0	2	3	5	6	0	1	3	4	6	7
4	6	7	1	2	4	5	7	0	2	3

目次

1. 研究背景・準備
2. 提案手法
3. 実験・結果
4. まとめ

実験とその結果

- CRYSTALS-KYBERとSABERの各スキームに対して攻撃を実施
- Python3のnumpy.poly1dをベースにR_qの演算を実装
- 攻撃成功率は100%
- 要したクエリは以下の通り

Cryptoscheme	CRYSTALS-KYBER			SABER		
Parameter set	KYBER-512	KYBER-768	KYBER-1024	LightSaber	Saber	FireSaber
Number of queries	≤4	3	4	≤ 6	≤6	4

目次

1. 研究背景・準備
2. 提案手法
3. 実験・結果
4. まとめ

まとめ

- CRYSTALS-KYBER, SABERに対する鍵再利用攻撃を提案
  - 復元成功率100%を達成
  - 要したクエリ数は小さい

- 本攻撃の対策
  - 定期的な秘密鍵のリフレッシュ

  →鍵を生成するサーバに負荷

参考文献

[1] Qin Y., Cheng C., Ding J. (2019) A Complete and Optimized Key Mismatch Attack on NIST Candidate NewHope. In: Sako K., Schneider S., Ryan P. (eds) Computer Security – ESORICS 2019. ESORICS 2019. Lecture Notes in Computer Science, vol 11736. Springer, Cham

[2] Bauer A., Gilbert H., Renault G., Rossi M. (2019) Assessment of the Key-Reuse Resilience of NewHope. In: Matsui M. (eds) Topics in Cryptology – CT-RSA 2019. CT-RSA 2019. Lecture Notes in Computer Science, vol 11405. Springer, Cham

[3] Alkim E., Ducas L., Pöppelmann T., Schwabe P. (2016) Post-quantum key exchange—a new hope. In: 25th USENIX Security Symposium (USENIX Security 16) (pp. 327-343).

[4] J. W. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe,G. Seiler, and D. Stehlé. CRYSTALS - kyber: A cca-secure module-lattice-basedKEM. In2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018.

参考文献

[5] J. D'Anvers, A. Karmakar, S. S. Roy, and F. Vercauteren. Saber: Module-lwrbased key exchange, cpa-secure encryption and cca-secure KEM. InProgress inCryptology - AFRICACRYPT 2018 - 10th International Conference on Cryptology in Africa.

[6] Wang K., Zhang Z., Jiang H. (2020) Security of Two NIST Candidates in the Presence of Randomness Reuse. In: Nguyen K., Wu W., Lam K.Y., Wang H. (eds) Provable and Practical Security. ProvSec 2020.