耐量子計算機暗号と量子情報の数理

暗号数理入門

三菱電機　情報技術総合研究所 / JST ACT-X

相川　勇輔

この講演の目的

■暗号の基礎知識が全くない方が以降の講演を聴けるように

- 社会の中での暗号の役割
- 暗号特有の考え方
- 基本的な用語

を準備すること

■インフォーマルな説明も多々あると思いますが、ご容赦ください！

- 量子情報の基礎知識は竹内さんのご講演で、
- 詳細な暗号理論の基礎知識は廣政さんのご講演で解説されます

アジェンダ

1. 情報セキュリティと暗号技術
2. 暗号技術とその安全性
3. 共通鍵暗号と公開鍵暗号
4. 公開鍵暗号の構成とその安全性
5. 次世代の公開鍵暗号：耐量子計算機暗号

準備　1/2

- あるデータの**サイズ**と言った場合、その情報をビット列で表現したときのビット数を指す
  - 例えば10進表現で与えられた整数Nのサイズを言えば、日常的に言う桁数のことではなくて、2進表示したときの桁数$\lfloor \log_2 N \rfloor + 1$のこと
- アルゴリズムの**計算量**は、手順を完了するまでに要する基本演算の回数のことをいう

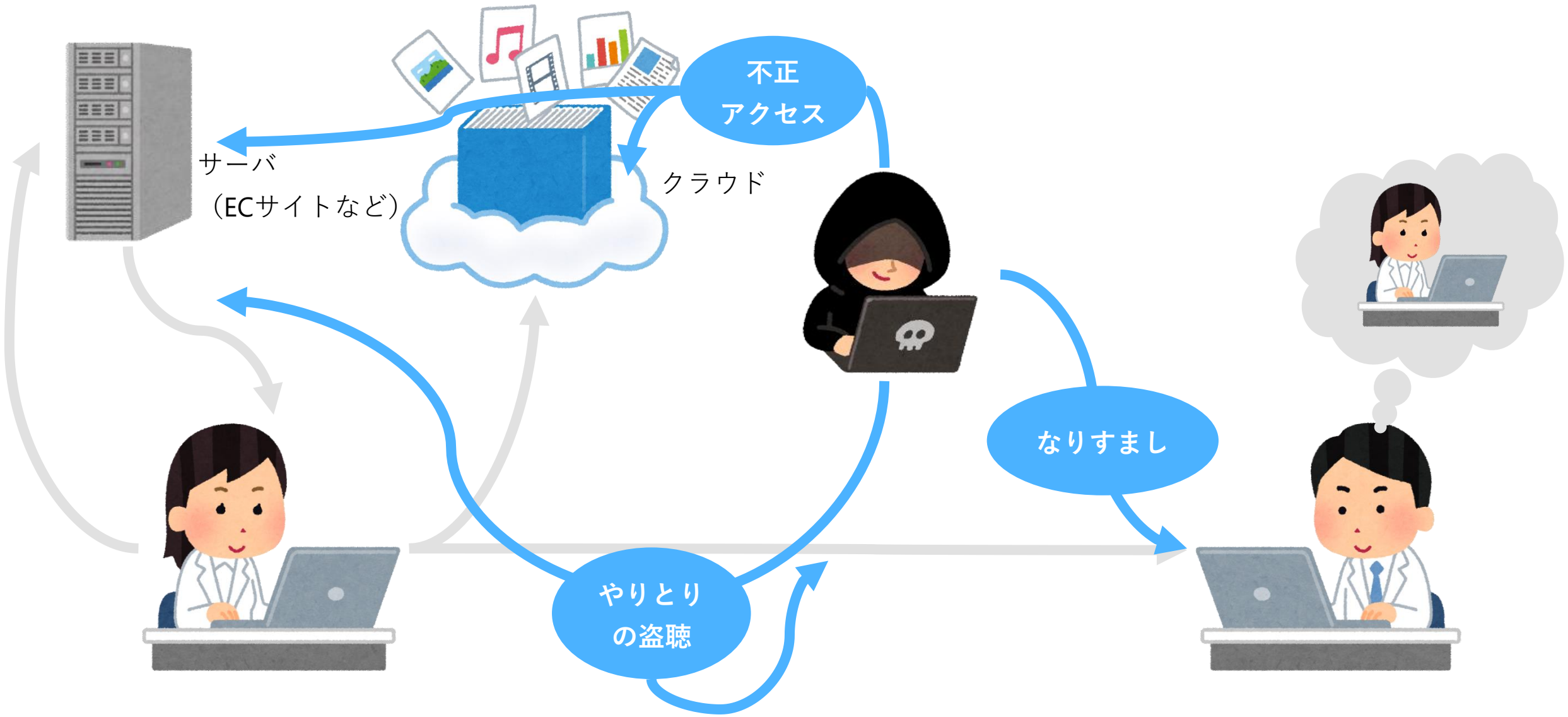
- アルゴリズムの計算量が、入力の何らかのパラメータについて多項式（resp. 指数）オーダーのとき**多項式（resp.指数）時間アルゴリズム**という

準備　2/2

- 暗号が**効率的**とは主にアルゴリズムの処理速度が速いとか、使用するデータのサイズが小さくて済むということ
  - あくまで相対的な表現、例えば
    - 方式Aは方式Bとアルゴリズムの処理速度は変わらないのに鍵のサイズが小さいから効率的、とか
    - 方式Cは方式Dより鍵サイズは大きいけど処理速度は速い、などなど
    - 暗号アルゴリズムの処理速度は（環境にもよるが）ミリ秒とかマイクロ秒のオーダーで競う
    - データ（鍵や署名など）サイズが1kBだと「大きいなあ・・・」という印象（電機メーカーに居るからかも）

1 情報セキュリティと暗号技術

ネットワークで繋がった社会に潜む脅威

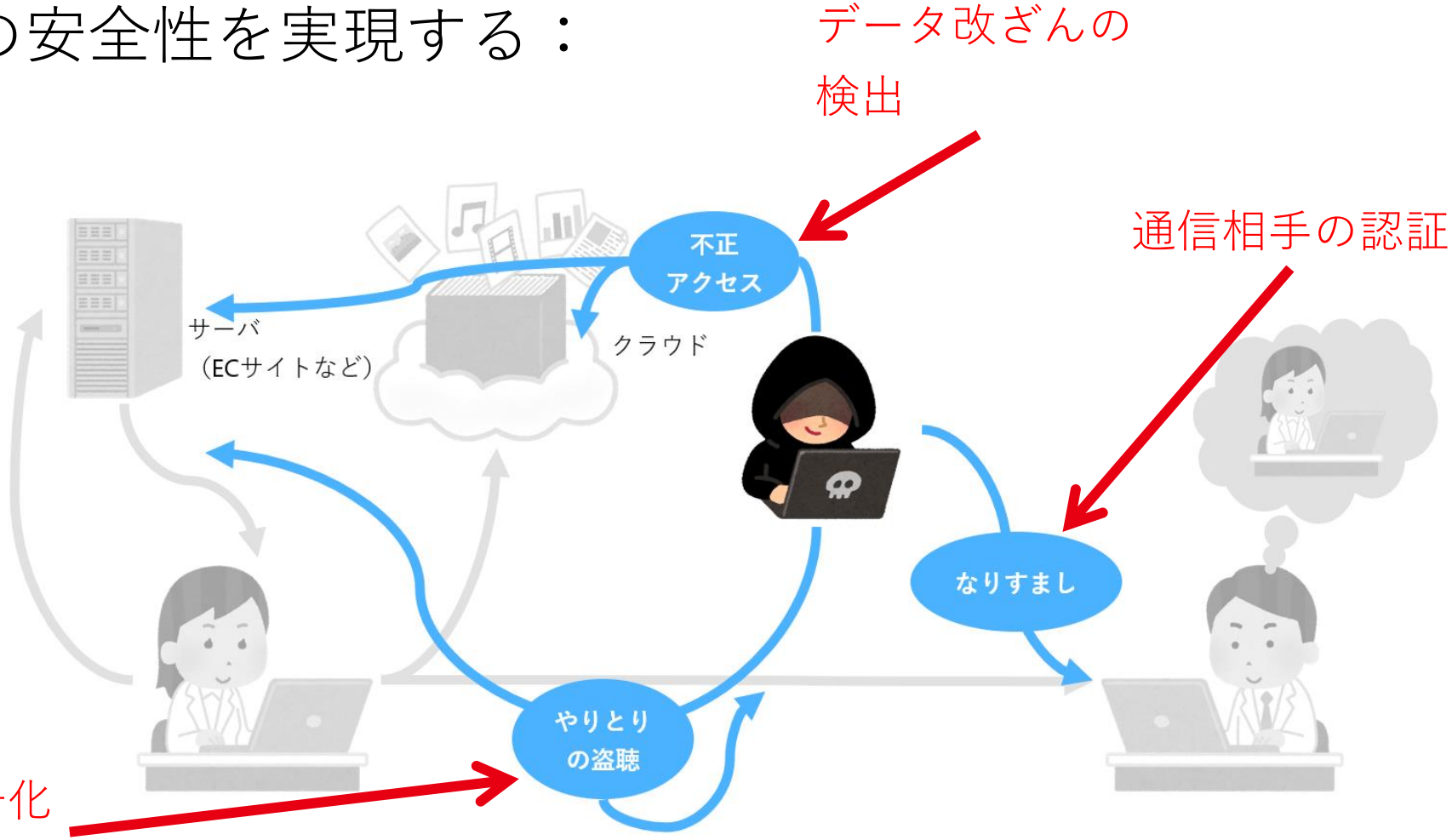


情報セキュリティ

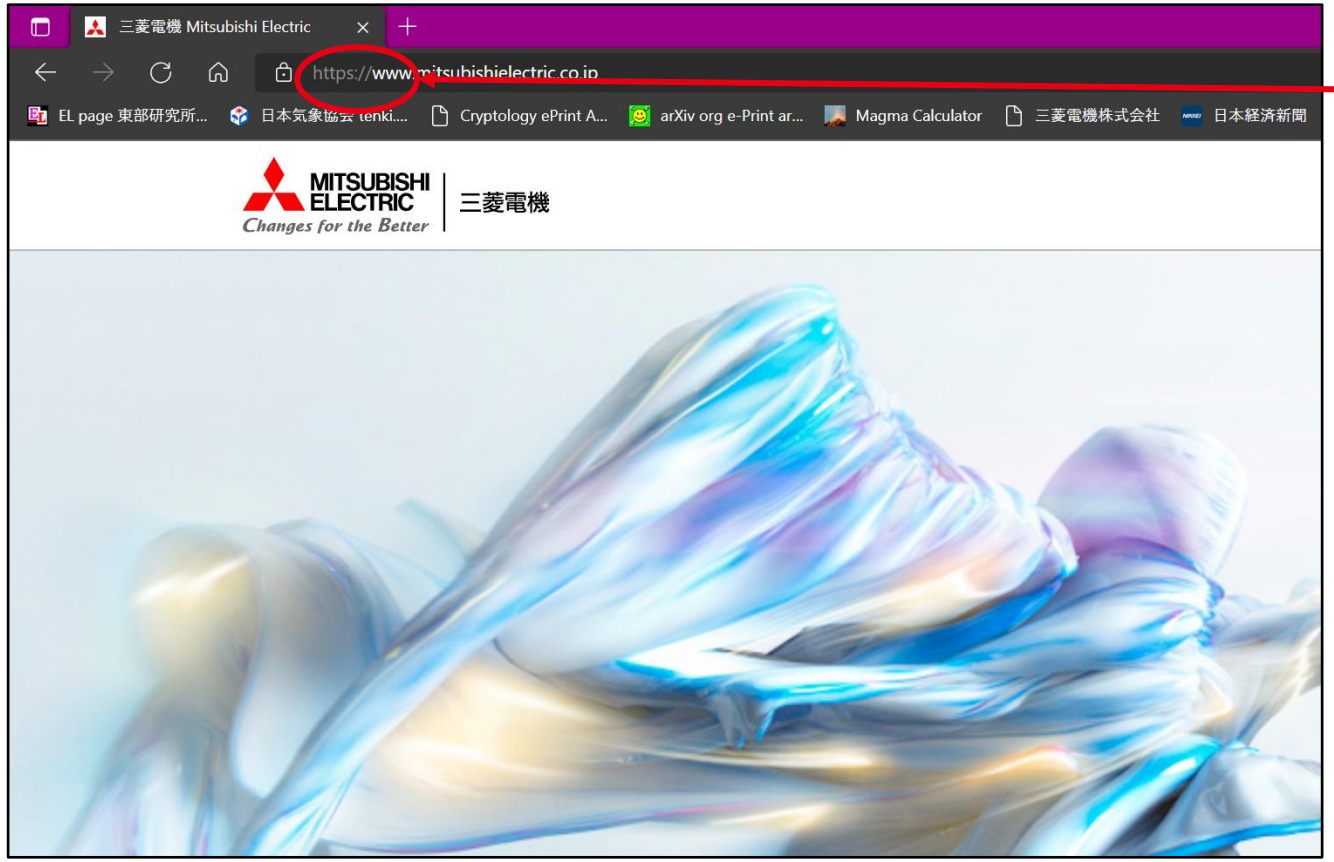
- **情報セキュリティ**とは、不正なアクセスやシステムの破壊などの脅威から組織や個人の情報資産を守ること
  - 今回は主に、第三者の悪意により引き起こされる脅威を念頭に置く
- 情報セキュリティは以下の性質から構成される：
  - **機密性（Confidentiality）**；許可された者だけが情報へアクセス可
  - **完全性（Integrity）**；情報が破壊や改ざんされていないこと
  - **可用性（Availability）**；情報へアクセスが正常にできる状態を保つ
- 暗号技術、セキュリティプロトコル、認証、ファイアウォール、Webセキュリティ等**様々な要素技術の総体**として実現される

暗号技術

- 情報セキュリティの中核をなす要素技術の一つ
- 暗号は例えば以下の安全性を実現する：
  - **情報の秘匿**
  - **認証**



暗号の適用例：セキュリティプロトコル

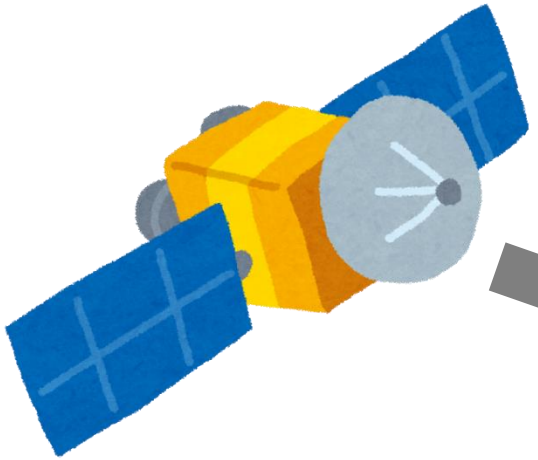


https://.....

hypertext transfer protocol secure

このsはTLSプロトコルによってWebサーバの認証や、その間の通信内容の暗号化や改竄検出がされてますよ、という証！

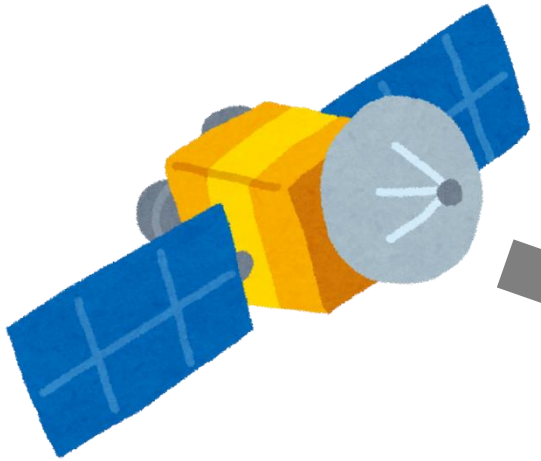
暗号の適用例：衛星測位



搬送波
疑似雑音符号
航法メッセージ

信号を補足・追尾し、
位置、速度、時刻を推定

暗号の適用例：衛星測位



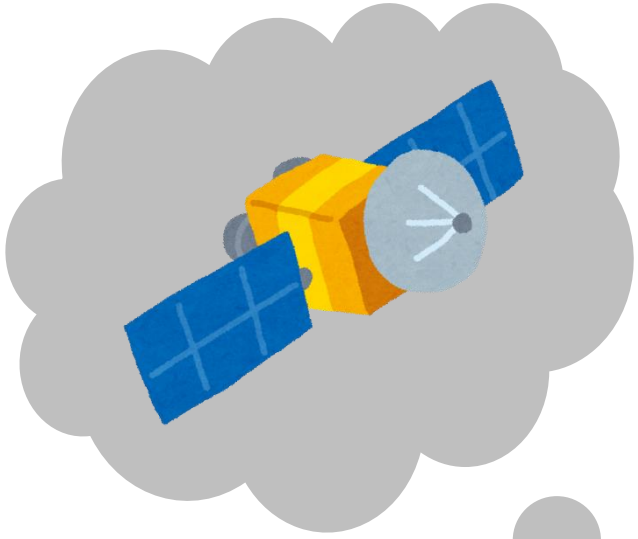
高精度測位補正信号

ドローン

自動運転車

暗号の適用例：衛星測位

位置情報を誤ると
重大な事故につな
がりかねない！

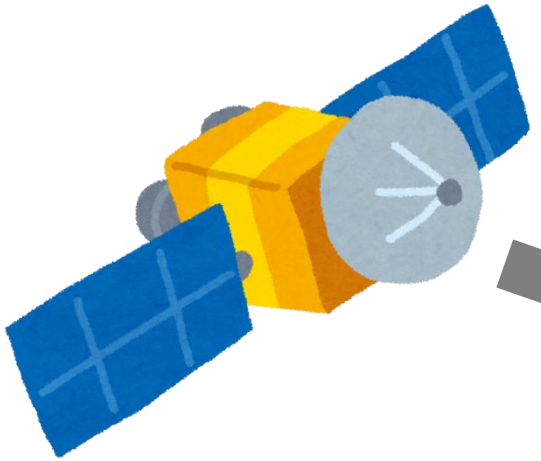


偽の信号

GNSSシュミレータ
を利用したなりすまし攻撃

自動運転車

暗号の適用例：衛星測位



高精度測位補正信号

認証データ

正しい認証データが付いてるから衛星からの信号だな！

ここに**暗号技術**が使われる！（例：[FHRA]）

[FHRA] I.Fernandez-Hernandez, R.Hirokawa, V.Rijmen, Y.Aikawa, PPP/PPP-RTK Message Authentication, ION GNSS+ 2021.

このように・・・

■ あらゆるものがネットワークで繋がることが前提となった社会では、情報セキュリティは社会インフラを形成する必須技術

暗号技術はその根幹をなす要素技術の一つ

■ では、情報の秘匿や認証が可能な暗号技術は

- どのように構成できるのか？
- 安全性はどのように保証されるのか？
- これまでにどのような課題があったのか？
- さらに、現在どのような課題に直面しているのか？
- また、それらの解決のために数学には何ができるのか？

2 暗号技術とその安全性

情報の秘匿：暗号化

インターネット

暗号文
j¥ @]w*PK?Wo

2 暗号化アルゴリズム

暗号文
j¥ @]w*PK?Wo

暗号化鍵

暗号文
j¥ @]w*PK?Wo

3 復号アルゴリズム

復号鍵

1 鍵生成アルゴリズム

Vernam暗号

- Vernam暗号はG. Vernamが開発した方式（1919年に特許を取得）
- nビットのメッセージ$m = (m_1, m_2, \ldots, m_n) \in \{0,1\}^n$は以下のように暗号化される

■ **鍵生成（Key generation）** 一様ランダムなビット列$k = (k_i) \in \{0,1\}^n$を出力

■ **暗号化（Encryption）** メッセージmと鍵kの排他的論理和$\oplus$を計算し暗号文$c \in \{0,1\}^n$を得る

$$c = m \oplus k = (m_1, m_2, \cdots, m_n) \oplus (k_1, k_2, \cdots, k_n)$$
$$= (m_1 \oplus k_1, m_2 \oplus k_2 \cdots, m_n \oplus k_n) = (c_1, c_2, \cdots, c_n)$$

■ **復号（Decryption）** 暗号文cと鍵kの排他的論理和を計算する

$$c \oplus k = (c_1 \oplus k_1, c_2 \oplus k_2, \cdots, c_n \oplus k_n) = (m_1 \oplus k_1 \oplus k_1, m_2 \oplus k_2 \oplus k_2 \cdots, m_n \oplus k_n \oplus k_n)$$
$$= (m_1, m_2, \ldots, m_n)$$

完全秘匿性

Vernam暗号の安全性を考える

- 暗号の構成から一様ランダムに選ばれた鍵の情報を得ることとメッセージの情報を得ることは等価
- したがって、鍵の情報を全く知らない攻撃者は、メッセージのいかなる情報も持ちえない

- このように攻撃者が「暗号文を持っている状態」と「暗号文を持っていない状態」とでメッセージに関して得られる情報に差がないという安全性を**完全秘匿性**という
- この安全性を持つ暗号は、無限大の計算能力を持つ攻撃者に対しても条件なしに安全である

Vernam暗号の欠点

- 処理速度は効率的だが、鍵の使いまわしができない
  - 複数のメッセージを一つの鍵で暗号化すると安全でなくなる

- メッセージを送るたびに鍵を生成する必要があり、しかもその鍵の一つ一つのサイズがメッセージと等しく実用コストが極めて高い
- 長所を差し出し、短所を補うことで実用的な暗号の設計へ

計算量的安全性

- 完全秘匿性を持たずとも「暗号文から平文の情報を得るために１億年以上かかる計算が必要」であれば、現実的には問題ないといえる

- 有限の計算で暗号を解読できるが、実行しようとすると膨大な計算が必要である、という安全性を**計算量的安全性**という
  - 現代暗号ではこの安全性に依拠し安全性と実用性の両立をはかることが多い

- 限定された計算能力を持つ攻撃者に対して保証される安全性で、その保証のために数学的仮定が用いられる

計算量的安全性を具体的に（この計算は鶴丸さん（三菱電機）の講義スライドから拝借しました！）

MITSUBISHI ELECTRIC
Changes for the Better

128ビットの鍵を考えてみる

- 鍵の総数は2^{128}個なので、総当たりで探せばいずれ正解が見つかる！

総当たりにどれくらい時間がかかるか推定してみよう

- 世界中のPCを1000億台と仮定する
- 世界中のPCのCPUのクロック周波数は3GHzと仮定する
- 1クロックで１つの鍵が当たりかどうか試せると仮定する

つまり１秒間で3×10^9個の鍵を試せる

1000億台を総動員すると1年で

$$3 \times 10^9 \times 60 \times 60 \times 24 \times 365 \times 10^{11} < 2^{93}$$

の鍵を試すことができる

全ての鍵を試すのに　$2^{128-93}=2^{35}$年>300億年>宇宙の年齢　かかる

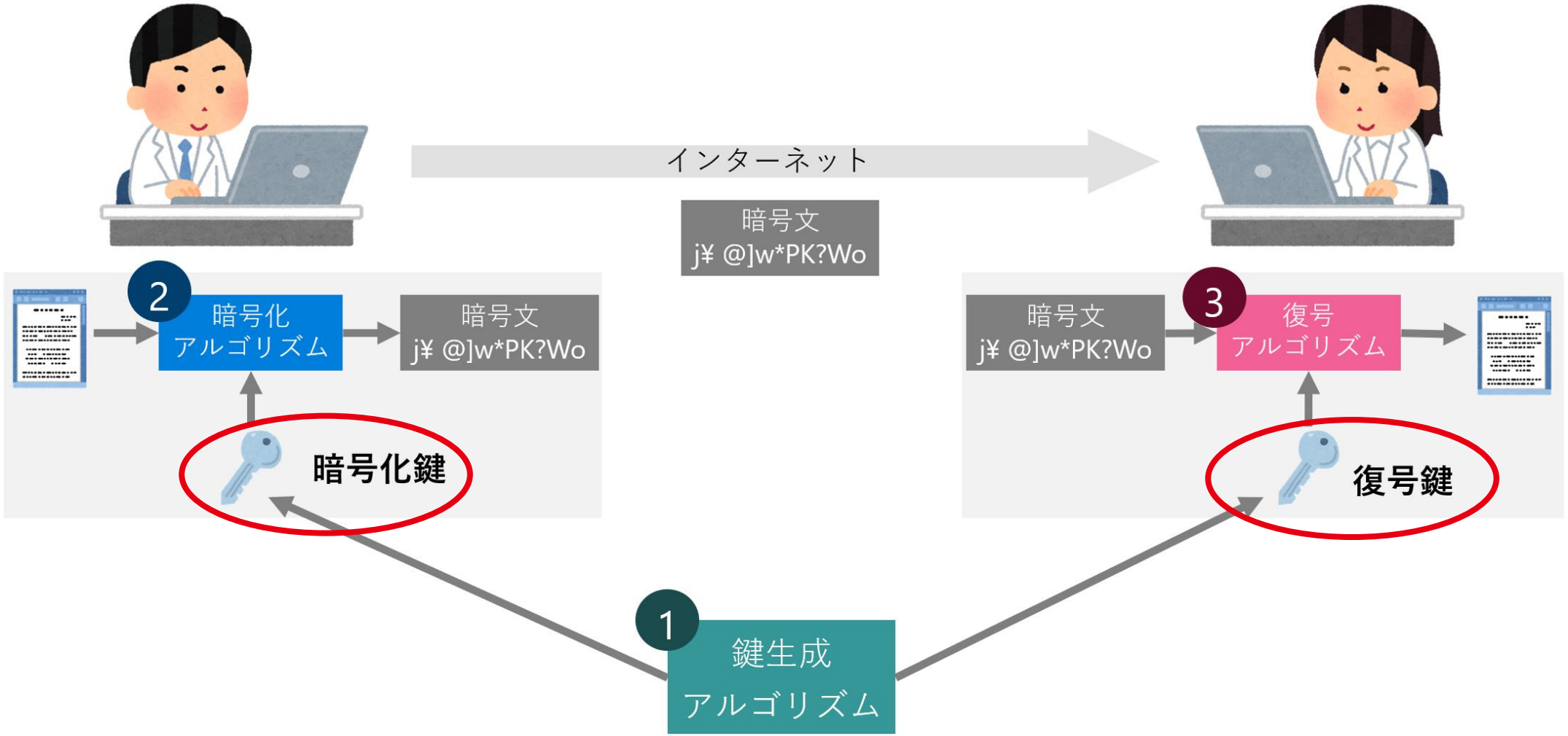
セキュリティレベル

- セキュリティレベルとは**暗号の安全性の強度**を表す概念
  - セキュリティレベルが128ビットセキュリティとは、暗号の解読に必要な計算量が2^{128}個のデータから総当たりで当たりを見つけるのと同程度ということ
  - ある暗号方式に対し鍵の総数が2^{128}個になるようにパラメータ設定したとしても、例えば2^{100}個の全数探索と同じ計算量で鍵を暴くアルゴリズムが発見された場合128ビットセキュリティを達成できなくなる
    - パラメータサイズを上げるなどして所望のセキュリティレベルを達成することになるが、効率性が犠牲になる
    - 多項式時間で鍵を暴くアルゴリズムが見つかった場合は、完全に解読されたと見なす
  - セキュリティレベルを指定するパラメータを**セキュリティパラメータ**という

3 共通鍵暗号と公開鍵暗号

暗号化方式

■暗号では送信者と受信者それぞれが鍵を使う



共通鍵暗号

- **暗号化鍵と復号鍵が等しい暗号を共通鍵暗号**とよぶ

Vernam暗号も一例

- 現在は**計算量的安全性を持つ暗号**を利用することが多い

例

  - AES(Advanced Encryption Standard) [FIPS197]
    DaemenとRijmenが開発、2001年にNISTが標準化
  - MISTY [MISTY]
    1995年に松井充らが開発、近年解読技術の研究が進展[T]

- **鍵サイズが小さく**、一般にアルゴリズムは主にビット列の排他的論理和と置換から構成されるため**処理速度が速い**（マイクロ秒のオーダー）

- しかし**鍵の共有が必要**なためインターネットのような不特定多数がネットワーク利用する状況への適用が困難

[FIPS197] NIST, Federal Information Processing Standards Publication 197: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
[MISTY] 暗号技術仕様書　MISTY1: https://www.cryptrec.go.jp/cryptrec_03_spec_cypherlist_files/PDF/05_02jspec.pdf, [T] Y.Todo, Integral Cryptanalysis on Full MISTY1, CRYPTO 2015.

公開鍵暗号

- MerkleおよびDiffieとHellman[DH]は公開通信路を用いた安全な鍵共有方式を提案し、鍵の共有問題を解決した(1976)
  - **公開する鍵**と**秘密の鍵**の２つの鍵を利用し、公開通信路を用いて２者間で共通の鍵を共有する方法を実現：Diffie-Hellman鍵共有（後述）
  - **公開鍵暗号の原理に基づく暗号化とデジタル署名**のアイデアを提出[DH]

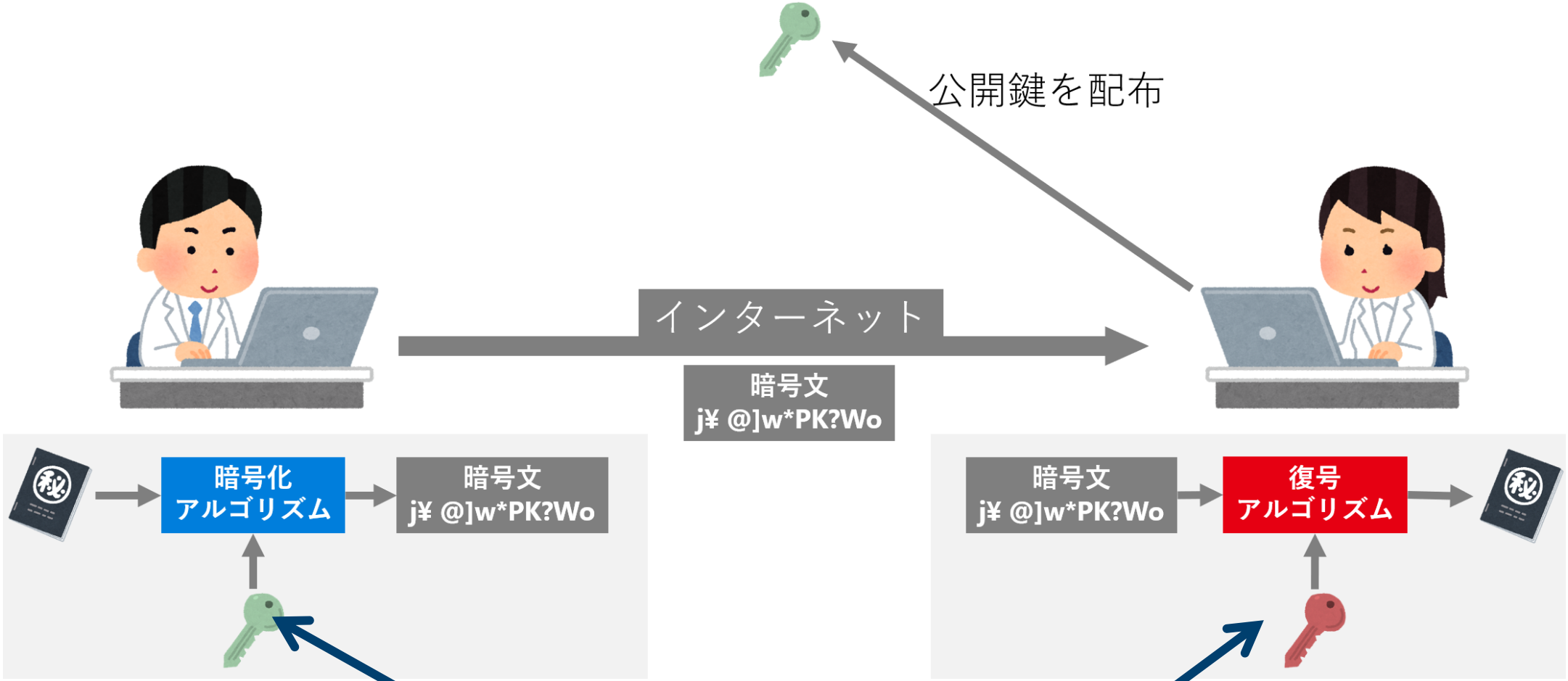
  （具体的に構成はしていない）
  - 整数論を利用することで公開鍵暗号は実現、実用化に至っている
- 公開鍵暗号は一般に数論演算を多用するため処理速度が遅い

  （共通鍵暗号の1000倍くらい遅い）

⇒ 実用的には、公開鍵暗号と共通鍵暗号を組み合わせて使う

[M] R. C. Merkle, Secure communications over insecure channels, Commun.ACM, 1978.
[DH]W. Diffie, M.Hellman, New directions in cryptography, IEEE Transactions on Information Theory, 1976.

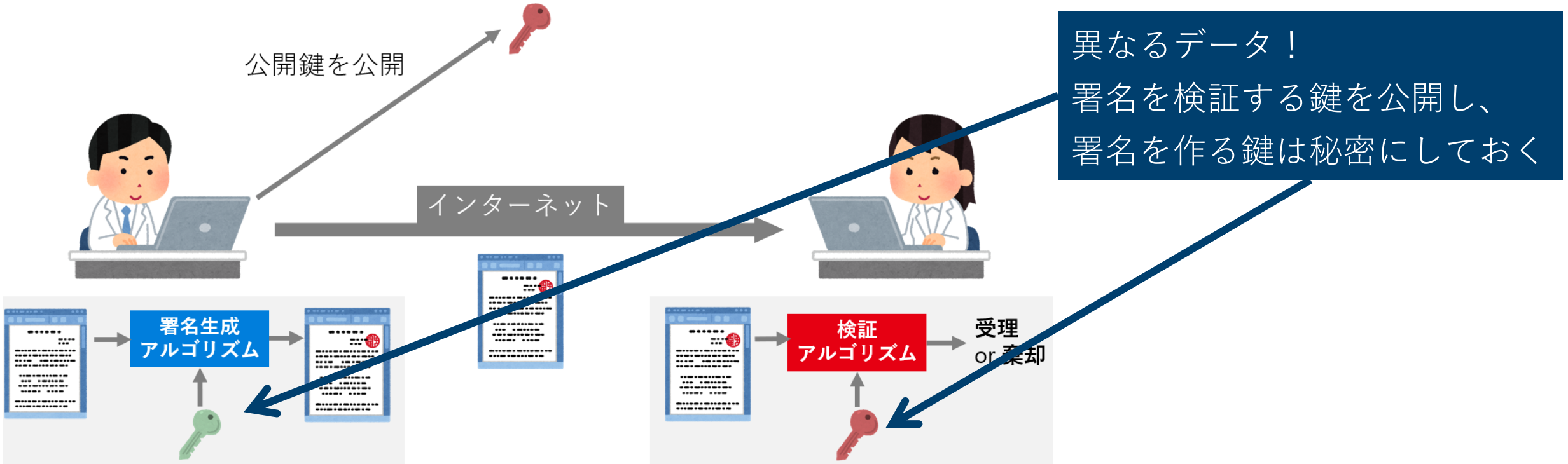
公開鍵暗号：暗号化



公開鍵暗号：デジタル署名

デジタル署名は電子情報への署名を可能にする

- 正しいデジタル署名を作成できるのは署名者本人のみ
- 正しい署名者が作成したデジタル署名の正当性は誰でも検証できる



公開鍵と秘密鍵

- 秘密鍵の漏洩は暗号文の解読や署名の偽造などをただちに意味する
- **本講演では公開鍵から秘密鍵が計算できないとき安全であると考える**
  - この条件は暗号方式に求める安全性を達成するための必要条件

例
- 巨大な合成数（10進600桁程度）の素因数分解問題
- 群の離散対数問題

厳密には、この問題に帰着される問題の困難性の仮定（例：DDH仮定）のもとで暗号の安全性を達成する

4 公開鍵暗号の構成とその安全性

RSA暗号

- 1977年にRivest, ShamirおよびAdlemanは初等整数論から公開鍵暗号を具体的に構成した[RSA]
  - 実用的には``教科書的な"RSA暗号を変換したRSA-OAEP[BR],[PKCS#1]の利用が推奨されている

- サイズがほぼ等しい素数の組(p, q)(現在は1024ビット以上)を秘密鍵に、その積$n = pq$を公開鍵の一部に用いる

⇒ nの高速な素因数分解はRSA暗号の解読に直結

（素因数分解することなくRSA暗号を解読できるかどうかはわかっていない）

[RSA] R.L.Rivest, A.Shamir, L.M.Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun.ACM, 1978. [BR]M.Bellare, P.Rogaway, Optimal asymmetric encryption, EUROCRYPT 1994. [PKCS#1] RFC 8017 - PKCS #1: RSA Cryptography Specifications Version 2.2 (ietf.org) (https://datatracker.ietf.org/doc/html/rfc8017)

数学へ与えられる課題

- 巨大な素数（秘密鍵）を高速に見つけられるか？
  - Miller-Rabin法のような実用的アルゴリズムがある（cf. [FIPS186-4]）
- 素因数分解アルゴリズムの研究および実装を進めて安全性を見積もる
  - 暗号では、できるだけ最高の実装環境で既存の最も高速なアルゴリズムを動かしても現実的な時間では解けないようにパラメータを設定する
  - 問題を解く計算時間の下限を理論的な証明は困難なため、アルゴリズムの開発と解読実験は実用上重要
  - 解読コンテストRSA Facoring Challenge（終了済）

[FIPS186-4] NIST, Federal Information Processing Standards Publication 186-4: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

一般の合成数に対する素因数分解アルゴリズム

- 小さい素数から順に割っていく
  - 入力の合成数Nに対し$O(\sqrt{N})$の計算量を持つ指数時間アルゴリズム
- 数体ふるい法[LLMP],[LL]
  - 現状最速の素因数分解アルゴリズム:計算量$O(\exp((\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}))$
  - RSAで用いるような合成数に対する素因数分解実験の記録（現在の最高記録は829ビット）のほとんどは数体ふるい法によって得られている(cf. [KAF+], [BGG+])
- 楕円曲線法(ECM)[L]
  - 小さい素因数をたくさん持つ合成数に対して有効とされる

[LLMP]A. K. Lenstra, H.W. Lenstra, M.S. Manasse, J.M. Pollard, The number field sieve, STOC 1990. [LL] A. K. Lenstra, H. W. Lenstra, Jr., editors. “The development of the number field sieve”, LNM1554, Springer, 1993. [KAF+] Kleinjung, T. *et al.* (2010). Factorization of a 768-Bit RSA Modulus. CRYPTO 2010. [BGG+] cado-nfs - [Cado-nfs-discuss] Factorization of RSA-250 - arc (inria.fr) (https://sympa.inria.fr/sympa/arc/cado-nfs/2020-02/msg00001.html) [L] H. W. Lenstra, Jr., “Factoring integers with elliptic curves”. Ann. of Math. 1987.

特殊な素因数を持つ合成数に対する素因数分解アルゴリズムの例

- 特殊な素数を素因数として持つ合成数に特化した高速な素因数分解アルゴリズムが見つかると、そのような素数の秘密鍵としての利用は推奨できなくなる（弱い鍵の研究）
  - 楕円曲線法と楕円曲線生成法であるCM法を組み合わせることで、特殊な素数を持つ合成数を高速に分解するアルゴリズムが構成されている[ANS]
  - 判別式$-D$を用いて``$4p = 1 + Dv^2$"あるいは``$4p = t^2 + Dv^2$かつ$p + 1 - t$がスムース"な素数を多項式時間で素因数分解できる

[ANS] Y. Aikawa, K. Nuida, M. Shirase, Elliptic Curve Method using Complex Multiplication Method, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2019.

Diffie-Hellman(DH)鍵共有

公開パラメータ

群G s.t. $\#G = p$（素数位数）

$g \in G$　ベースポイント

秘密鍵

1．$a \in \{0, \ldots, p-1\}$をランダムに選ぶ

2．$h_a := g^a$を計算する

1．$b \in \{0, \ldots, p-1\}$をランダムに選ぶ

2．$h_b := g^b$を計算する

公開鍵

h_a　h_b

3．$(h_b)^a = g^{ab}$を計算する

3．$(h_a)^b = g^{ab}$を計算する

必ずしも安全でない通信路

同じ値を秘密裏に共有できた！

離散対数問題(DLP)

- DH鍵共有を行った２者間から共有鍵を盗み取りたい攻撃者は、通信路を流れる情報から共有鍵を計算することを試みる

- 直接的には、公開鍵から秘密鍵を計算できてしまえばよい！

群Gの離散対数問題(Discrete Logarithm Problem, DLP)

組$(G, g \in G, g^a)$が与えられたとき、$a \in \mathbb{Z}$を求めよ

ElGamal暗号[E]: DLPに基づく暗号化方式の例

- Gを（素数位数の）群とし$g \in G$を固定する。また、$p = \#G$とおく。

■ **鍵生成（Key generation）**　$s \in \{0, \dots, p-1\}$をランダムに選び、$h = g^s$を計算
（pk, sk）$=(h, s)$とする

■ **暗号化（Encryption）**

1．メッセージを$m \in G$とする

2．$r \in \{0, \dots, p-1\}$をランダムに選び
$C_1 = g^r, C_2 = h^r m$を計算

3．暗号文を$C = (C_1, C_2) \in G \times G$とする

■ **復号（Decryption）**

1．秘密鍵sを使って$C_1^{-s} C_2 \in G$を計算

計算用紙　$C_1^{-s} C_2 = (g^r)^{-s} h^r m$

$= (g^r)^{-s} (g^r)^s m$

$= m$

[E]T.ElGamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, CRYPTO1984.

楕円曲線 -群を出力する数学的装置-

■ 1985年、Koblitz[K]とMiller[M]は独立に群として楕円曲線の利用を提案

定義（<u>有限体上</u>の楕円曲線）：
pを（５以上の）素数とする。$\mathbb{F}_p$を有限体とする。
$\mathbb{F}_p$上の**楕円曲線E**とは、$\mathbb{F}_p$上の種数１の非特異射影代数曲線のこと。
楕円曲線は以下のモデルを持つ：

$$Y^2 = X^3 + aX + b \left(a, b \in \mathbb{F}_p, 4a^3 + 27b^2 \neq 0\right).$$

■ $E(\mathbb{F}_p)$でEの$\mathbb{F}_p$上の解に無限遠点∞を付け加えた集合を表す

■ $E(\mathbb{F}_p)$にはアーベル群の構造が定まる（暗号では楕円曲線群とよぶこともある）

■ 係数a, bを定めと楕円曲線群が出力されるが、位数は以下のバウンドに収まる

$$p + 1 - 2\sqrt{p} \leq \#\, E\left(\mathbb{F}_p\right) \leq p + 1 + 2\sqrt{p}$$

[K] N. Koblitz. “Elliptic curve cryptosystems”. Mathematics of Computation, 1987. [M] V. Miller. “Use of elliptic curves in cryptography”. CRYPTO 1985.

数学への課題：特殊な曲線に対するECDLP解読アルゴリズム

- 合成数位数の曲線
  - 中国式剰余定理で素因数位数の群のDLPへ帰着
- MOV攻撃[MOV], [FR]
  - 楕円曲線上のペアリングを利用して楕円曲線のDLPを有限体の情報群上のDLPへ帰着
  - 特にEが超特異曲線のときに有効
- SSSA攻撃[S], [S], [SA]
  - アノマラス曲線（$\#E(\mathbb{F}_p) = p$なる曲線）上のDLPを有限体の加法群上のDLPへ帰着

[MOV]A. J. Menezes, T. Okamoto, S. A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Transactions on information Theory, 1993. [FR] G. Frey, H-G, Ruck, A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves, Mathematics of computation, 1994. [S] I. A. Semaev, Summation polynomials and the discrete logarithm problem on elliptic curves, IACR ePrint Archive 2004/31.[S] N. P. Smart, The discrete logarithm problem on elliptic curves of trace one, Journal of cryptology, 1999. [SA] T.Sato, K.Araki, Fermat equations and the polynomial time discrete log algorithm for anomalous curves, 1998.

実用的な曲線の例：NIST　Curve P-256

p=115792089210356248762697446949407573530086143415290314195533631308867097853951

$E: Y^2 = X^3 - 3X$

$+ 41058363725152142129326129780047268409114441015993725554835256314039467401291$

$\#E(\mathbb{F}_p)$=115792089210356248762697446949407573529996955224135760342422259061068512044369

5 次世代の公開鍵暗号：耐量子計算機暗号

量子コンピュータとShorのアルゴリズム

- 現在私たちが利用している公開鍵暗号の安全性は主に素因数分解と群の離散対数問題の計算量的な困難性に基づく

- 1994年にShorはこれらの問題を多項式時間で解く量子アルゴリズムを提案した（**Shorのアルゴリズム**）[S]
  - 大規模な量子コンピュータの実現は公開鍵暗号の危殆化を意味する
  - 量子コンピュータの計算原理は竹内さんにご講演いただきます
  - 実際に量子アルゴリズムによる暗号解読の手法および動向を深い知見をお持ちの國廣さん（筑波大） [招待]にご講演いただきます

[S] Shor, P. W., Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput, 1997.

耐量子計算機暗号(Post-Quantum Cryptography, PQC)

- 量子コンピュータによる解読にも耐えうる新たな公開鍵暗号の実用化に向けた研究が進められている

  ⇒ 総称して**耐量子計算機暗号(PQC)**という（cf. [高木], [縫田]）

- 2016年よりNISTはPQCの公募による標準化を進めており2022年7月に暗号化方式１つ、デジタル署名方式３つが標準化された[Selected]
  - これらに加えさらに候補を絞り込み[Round4]、標準化方式を固める（2024年ごろまで方式選定が続き、2030年までに米国政府はPQCへ移行する予定）
  - デジタル署名方式に関しては2022年夏に再公募を行うとのこと[Report]

[高木] 高木剛,暗号と量子コンピュータ: 耐量子計算機暗号入門, オーム社, 2019. [縫田] 縫田光司, 耐量子計算機暗号, 森北出版 2020.
[Selected] Selected Algorithms: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022
[Round4] Round4 submissions: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions
[Report] NISTIR 8413 Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf

耐量子計算機暗号へのアプローチ 1/3

格子暗号

- 最短ベクトル問題（Shortest Vector Problem, SVP）に基づく暗号方式
- 暗号化Kyber、デジタル署名DILITHIUM, FALCONがPQCとして標準化されており、将来的に実用化されていく見込み
- 方式の設計については廣政さん（三菱電機）に、解読については深い知見をお持ちの安田さん（立教大）[招待]に講演いただきます

耐量子計算機暗号へのアプローチ 2/3

符号暗号

- 誤り訂正符号に基づく暗号で、NIST標準化では暗号化BIKE, ClassicalMcEliece, HQCがRound 4候補として残っている
- 2019年に開始の解読チャレンジ[Code]で多く成果[KDDI]を挙げておられる成定さん（KDDI総合研究所）[招待]にご自身の成果をご講演いただきます

計算量理論によるアプローチ

- 近年、コルモゴロフ複雑度の計算問題のアルゴリズム[HN]および暗号学的[LP]研究が進められている
- 計算量理論にて成果を挙げておられる七島さん（東工大）[招待]よりご自身の成果[HN]含めご講演いただきます

[Code] Challenges for code-based problems (decodingchallenge.org)(https://decodingchallenge.org/index.php) [KDDI]世界初、1161次元の符号暗号を解読！～10の48乗通りの候補が存在する前人未到の問題を、約375時間で成功！～(https://www.kddi-research.jp/newsrelease/2021/011401.html [HN] S. Hirahara, M. Nanashima, On Worst-Case Learning in Relativized Heuristica, FOCS2021[LP]Y. Liu, R. Pass, On One-way Functions and Kolmogorov Complexity, FOCS2022.

耐量子計算機暗号へのアプローチ 3/3

■多変数多項式暗号

- 二次多変数多項式方程式の求解問題（MQ問題）やEIP問題に基づくと考えられる暗号で、NIST標準化においてはRound 3にて全ての方式が脱落
- デジタル署名の構成を得意とし、その構成については古江さん（東大）に、近年進展の著しい解読については池松さん（九大）にご講演いただきます

■同種写像暗号

- 楕円曲線とその同種写像を用いた方式で、NIST標準化では暗号化SIKEがRound 4候補に選ばれている（楕円曲線暗号とは異なることに注意）
- 鍵共有や暗号化を守谷さん（東大）に、デジタル署名の構成を小貫さん（東大）にご講演いただき、それらの数学的基礎付けを相川が発表いたします
- 7/30にCastryckとDecruにより効率的な鍵復元攻撃が発表された

耐量子計算機暗号の量子暗号プロトコルへの応用

- Mahadevによる計算量的安全な量子計算の古典検証[M] を契機に、耐量子計算機暗号と量子情報のインタラクションが加速
  - [M]の内容については水谷さん（三菱電機）にご講演いただきます
  - この分野で[CCY]など多くの成果を挙げておられる山川さん（NTT）にご自身の研究含め、最近の進展についてご講演いただきます

[M]U. Mahadev, Classical Verification of Quantum Computations, FOCS2018.
[CCY] N-H. Chia, K-M. Chung, T. Yamakawa, Classical Verification of Quantum Computations with Efficient Verifier, TCC2020.

研究集会の見取り図

量子情報技術
(竹内さんのご講演)

計算量的仮定に基づく量子暗号プロトコル
（水谷さん、**山川さん**のご講演）

大規模な量子コンピュータの実現で
Shorのアルゴリズムにより解読
（**國廣さん**のご講演）

既存の公開鍵暗号

- RSA暗号
- 楕円曲線暗号
- ペアリング暗号　など

耐量子計算機暗号の候補

数学によるアプローチ

- 格子暗号（廣政さん、**安田さん**のご講演）
- 符号暗号（**成定さん**のご講演）
- 多変数多項式暗号（池松さん、古江さんのご講演）
- 同種写像暗号（小貫さん、守谷さん、相川のご講演）

計算量理論からのアプローチ（**七島さん**のご講演）

2030年？

2016年～：NISTによる**PQC標準化**

※太字のお名前は招待講演者