NICTサイバーセキュリティシンポジウム2021
2021年2月17日

耐量子計算機暗号に関する
セキュリティ基盤研究室の取り組み

国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所
セキュリティ基盤研究室
篠原　直行

国立研究開発法人
情報通信研究機構
National Institute of Information and
Communications Technology

暗号技術の重要性
（コロナ禍におけるセキュリティと暗号）

量子コンピュータによる解読の脅威

- テレワークの活用が進んでいる
- VPN（Virtual Private Network）の重要性
  - VPN：インターネット上等で、暗号技術等を利用して、保護された仮想的な専用線環境を構築する仕組み。
  - インターネットにおいては、悪意の第三者が通信内容を傍受している可能性がある。
  - 機密情報かどうかに関わらず、オフィスと電子データのやりとりを行う場合は、VPN等、通信経路を暗号化した状態でやりとりできる経路を用いるのが安全

※参照：テレワークセキュリティガイドライン（第4版）：総務省
（https://www.soumu.go.jp/main_content/000545372.pdf）

概要

Q: 量子コンピュータが実用化されると何が問題に？

A: 現在利用されている公開鍵暗号は安全性が低下する.

Q: 耐量子計算機暗号（PQC: *Post-quantum* cryptography）とは？

A: 十分な規模の量子コンピュータが実用化されても
安全性を保つことができる暗号.

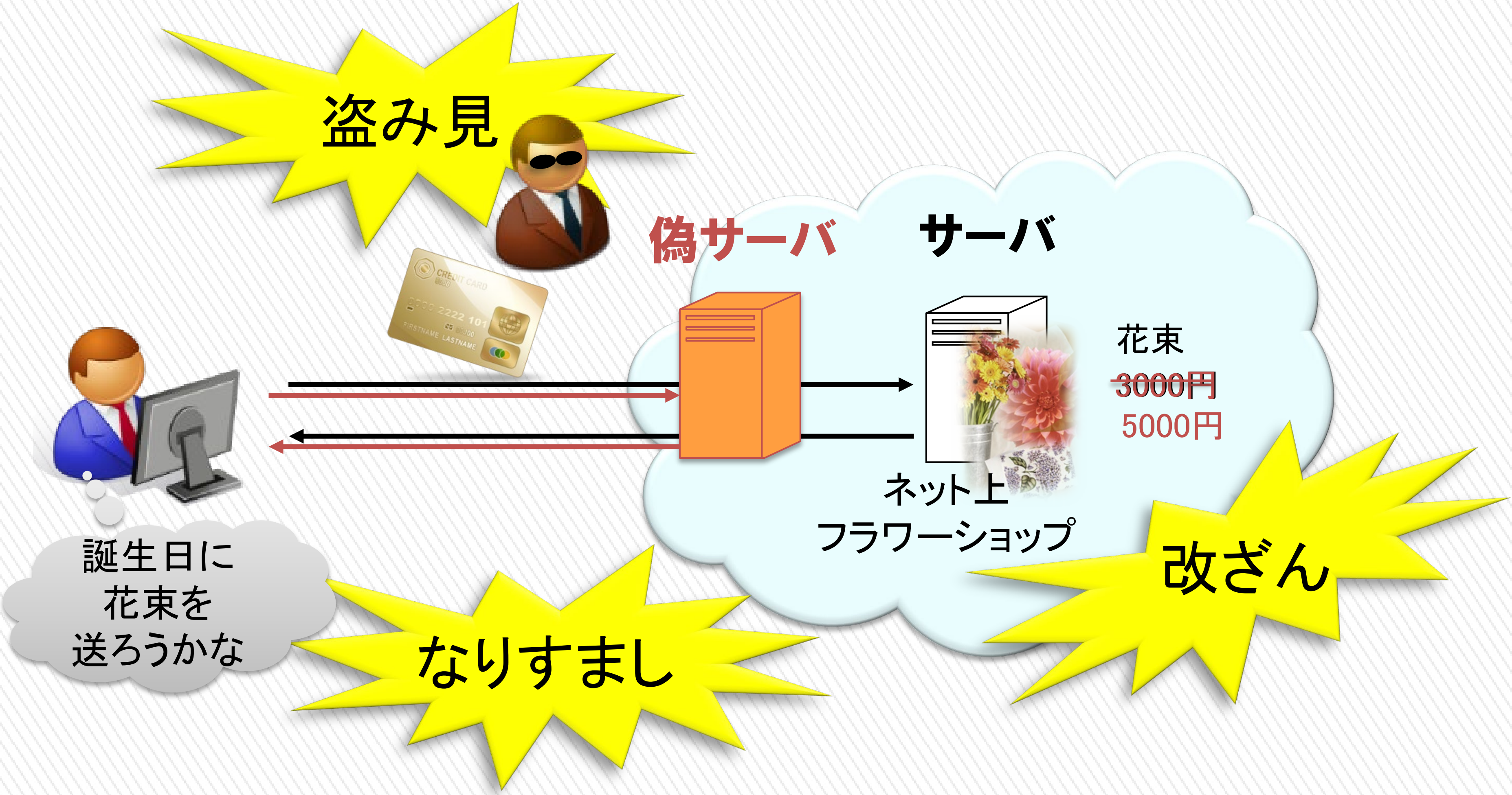
Q: PQC について NICT が取り組んでいることは？

A: PQC の使用に向けた準備及び PQC の研究開発

NICTサイバーセキュリティシンポジウム2019後の進捗

1　暗号技術と量子コンピュータ

ネットワーク社会における脅威の例



ネット社会の安全を支える暗号技術

暗号技術の役割

秘匿

- データを暗号化し、第三者に秘密にする

改ざん検出

- データ書き換えの有無をチェックする

相手認証

- 通信相手が正しいかどうかチェックする

暗号技術の分類

- 共通鍵暗号(AES 等)
  - 暗号化と復号に使う鍵が同じ
  - 暗号処理が公開鍵暗号に比べて効率的
  - 暗号化通信前に秘密に鍵を共有する必要あり

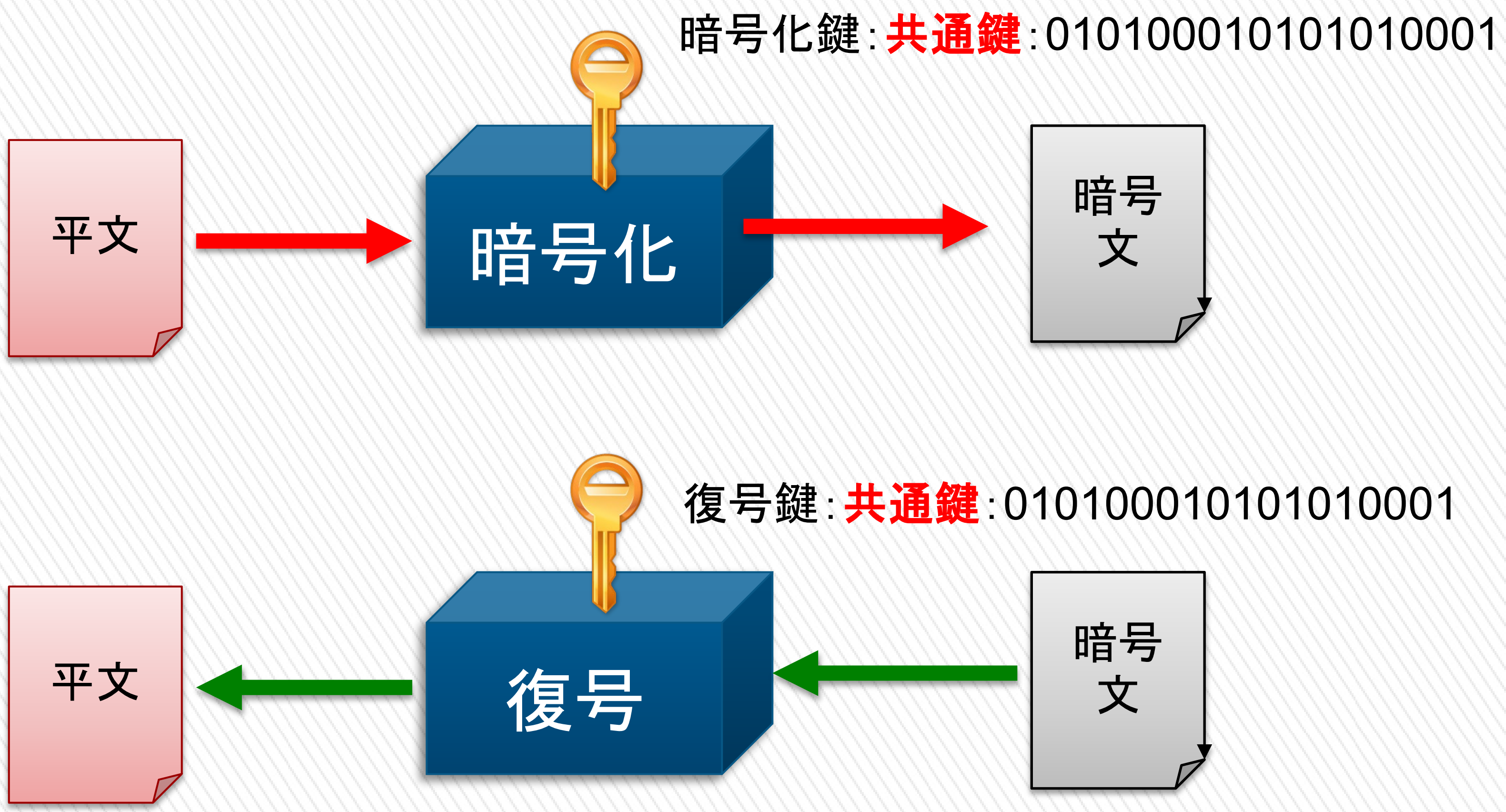
- 公開鍵暗号(RSA暗号など)
  - 公開鍵と秘密鍵の鍵ペアを使って暗号化・復号
  - 事前に鍵を共有する必要がない

暗号化は誰でもできる

復号は秘密鍵を
もっている人だけ

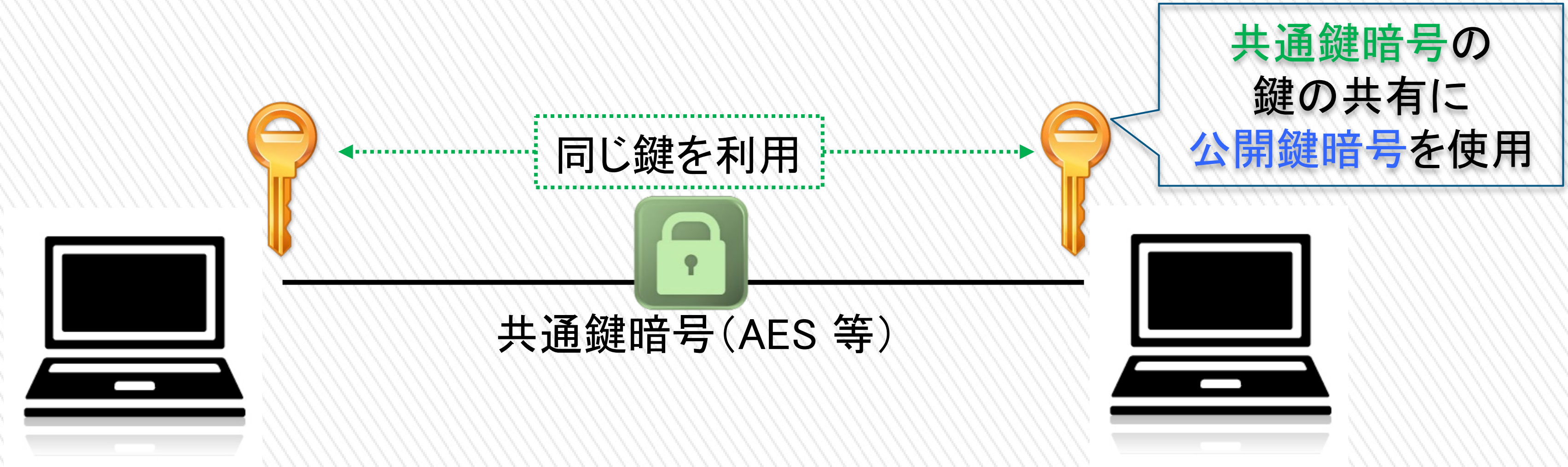
共通鍵暗号のしくみ

- “同じ鍵(**共通鍵**)”を使って暗号化・復号を行う



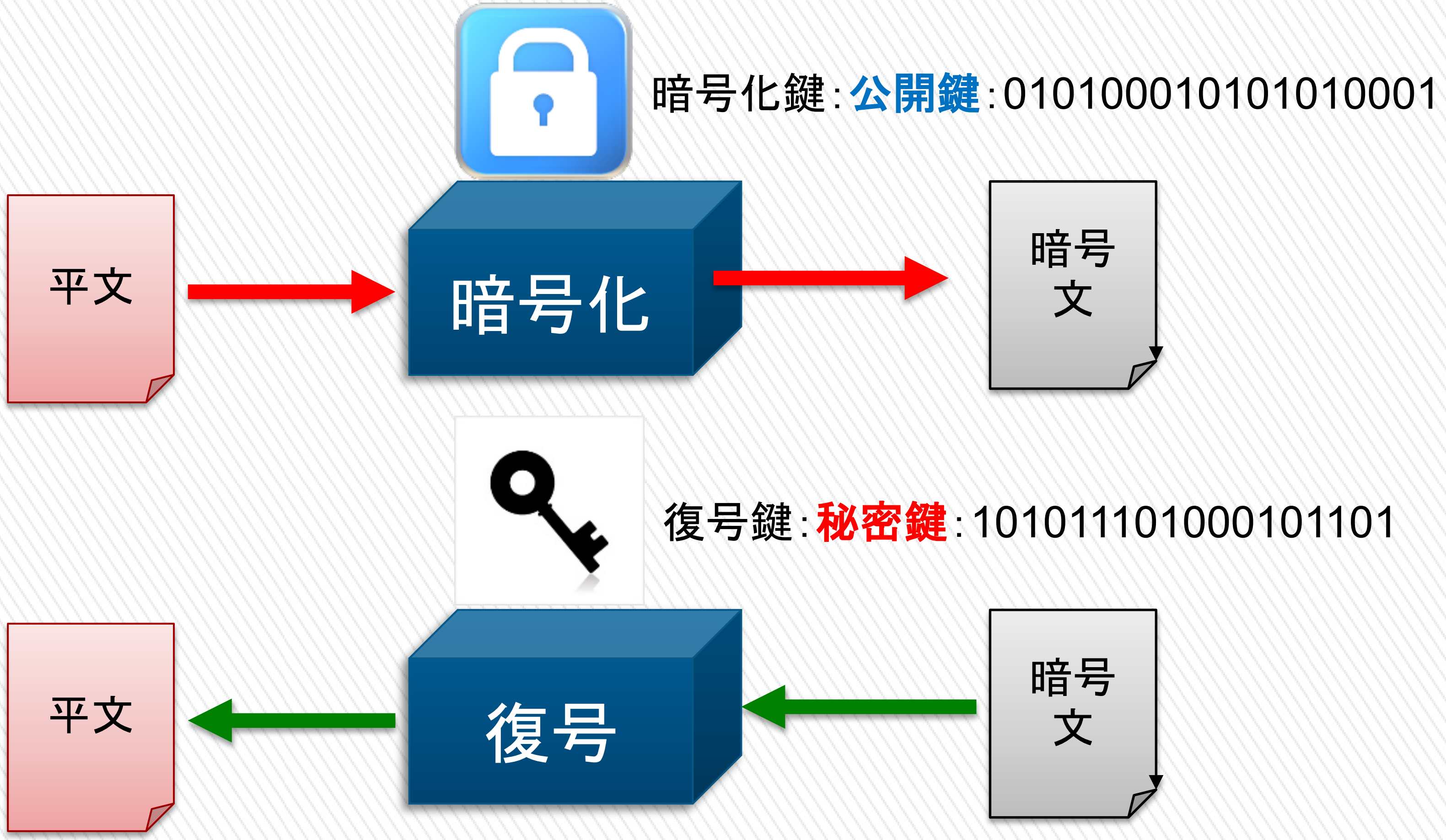
共通鍵暗号の使用例と鍵共有問題

- インターネットショッピングなどの場合
  https://www.********
  - SSL/TLS プロトコル(暗号技術)を利用してHTTP通信を行う。
  - データの暗号化通信に共通鍵暗号を使用



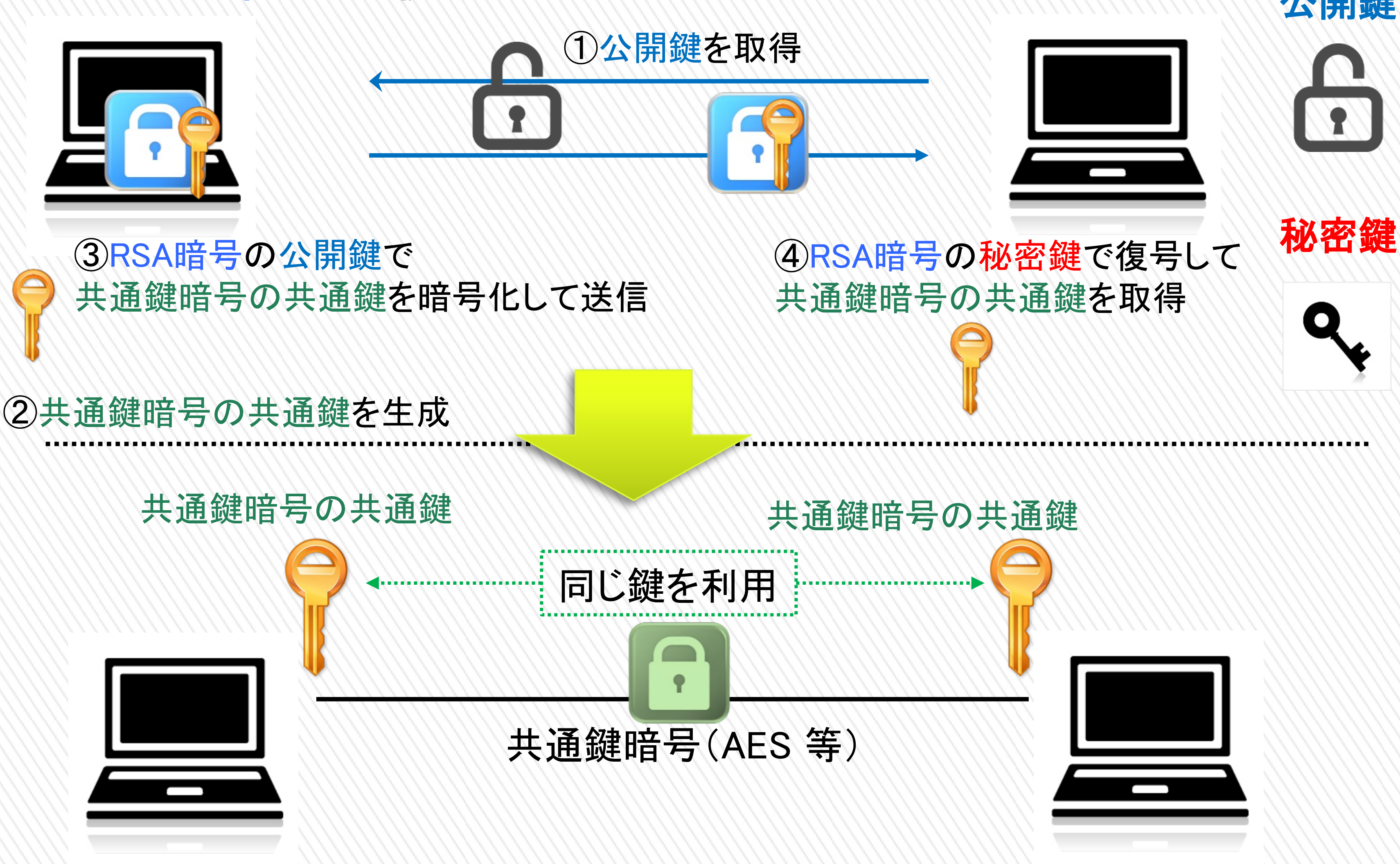
公開鍵暗号のしくみ

- “公開鍵”を使って暗号化し、
- “秘密鍵”を使って復号を行う。



公開鍵暗号による共通鍵暗号の鍵共有

- RSA 暗号を使用した鍵共有の例



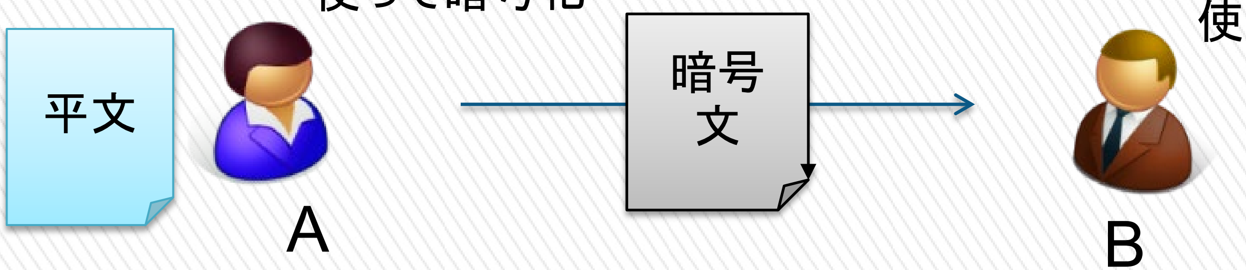
公開鍵暗号：暗号化と署名

暗号化　(目的：秘匿)

Bの公開鍵を
使って暗号化

Bだけが
復号できる

Bの秘密鍵を
使って復号



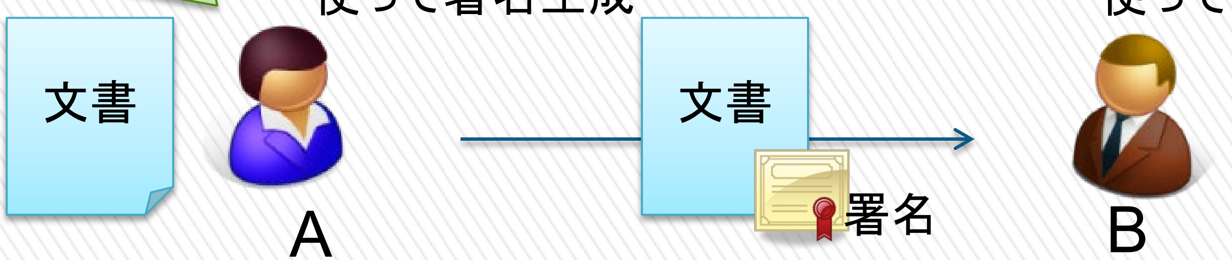
署名　（目的：改ざん防止・相手認証）

誰でもAの署名
を検証できる

Aしか自分の署名
を生成できない

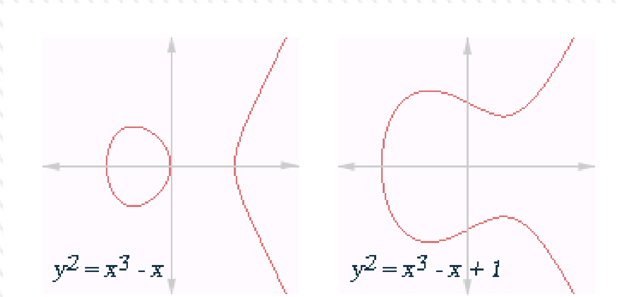
Aの秘密鍵を
使って署名生成

Aの公開鍵を
使って署名検証



公開鍵暗号と量子コンピュータの関係（1）

- 公開鍵暗号の安全性は数学と深い結びつきがある
  - 素因数分解問題に基づく方式
    - 公開鍵暗号 RSA
  - 離散対数問題に基づく方式
    - 鍵共有方式 DH, 電子署名方式 DSA
  - 楕円曲線上の離散対数問題に基づく方式
    - 鍵共有方式 ECDH, 電子署名方式 ECDSA



RSA：Rivest, Shamir, Adleman
DH　：Diffie-Hellman
DSA：Digital Signature Algorithm
EC　：Elliptic Curve

公開鍵暗号と量子コンピュータの関係(2)

- 整数を素数の積の形で表す

$$360 = 2^3 \times 3^2 \times 5$$

RSAにおける公開鍵と秘密鍵の関係

巨大な合成数　素数　素数

$$\underset{\text{公開鍵}}{n} = \underbrace{p \times q}_{\text{秘密鍵}}$$

- 巨大な合成数の素因数分解は難しい

⇒ RSAは(公開鍵を公開しても秘密鍵が漏れないため)安全

公開鍵暗号と量子コンピュータの関係(3)

量子コンピュータと Shorのアルゴリズム(1994)で 効率よく解くことができる

- 現在使用されている公開鍵暗号
  - RSA 暗号: 整数の素因数分解
  - 楕円曲線暗号: 楕円曲線上の離散対数問題

- PQC として期待される公開鍵暗号
  - 格子に基づく暗号: 格子問題(LWE 問題等)
  - 符号に基づく暗号: LPN 問題
  - 多変数多項式に基づく暗号: MP 問題, IP 問題
  - 同種写像に基づく暗号: 同種写像問題

NICT第4期中長期計画(2016-2020)における目標

【中長期計画】1-4. サイバーセキュリティ分野　(3) 暗号技術

機能性暗号技術	暗号技術の安全性評価	プライバシー保護技術
IoTの展開に伴って生じる新たな社会ニーズに対応するため、新しい機能を備えた機能性暗号や軽量暗号・認証技術の研究開発に取り組む	暗号技術の安全性評価を実施し、新たな暗号技術の普及・標準化に貢献するとともに、安心・安全なICTシステムの維持・構築に貢献	パーソナルデータの利活用に貢献するためのプライバシー保護技術の研究開発を行い、適切なプライバシー対策を技術面から支援

- 暗号技術の安全性評価における日本随一の研究拠点
  - ✓ 中立公平で信頼性の高い安全性評価情報の継続的発信
- セキュリティ＆プライバシー保護技術の研究連携拠点に
  - ✓ S&Pの新たな研究開発テーマでの国内外研究連携拠点を目指す
- 社会で活用される研究開発成果の創出と社会展開
  - ✓ パーソナルデータ利活用や改正個人情報保護法施行に資する技術開発

２．PQC の使用に向けたNICTの取り組み（CRYPTREC）

CRYPTREC

- CRYPTREC (Cryptography Research and Evaluation Committees)
  - 電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト

暗号技術検討会
事務局：総務省、経済産業省

暗号技術評価委員会
事務局：NICT, IPA

暗号技術の安全性・実装評価を中心とした技術的な検討課題を担当

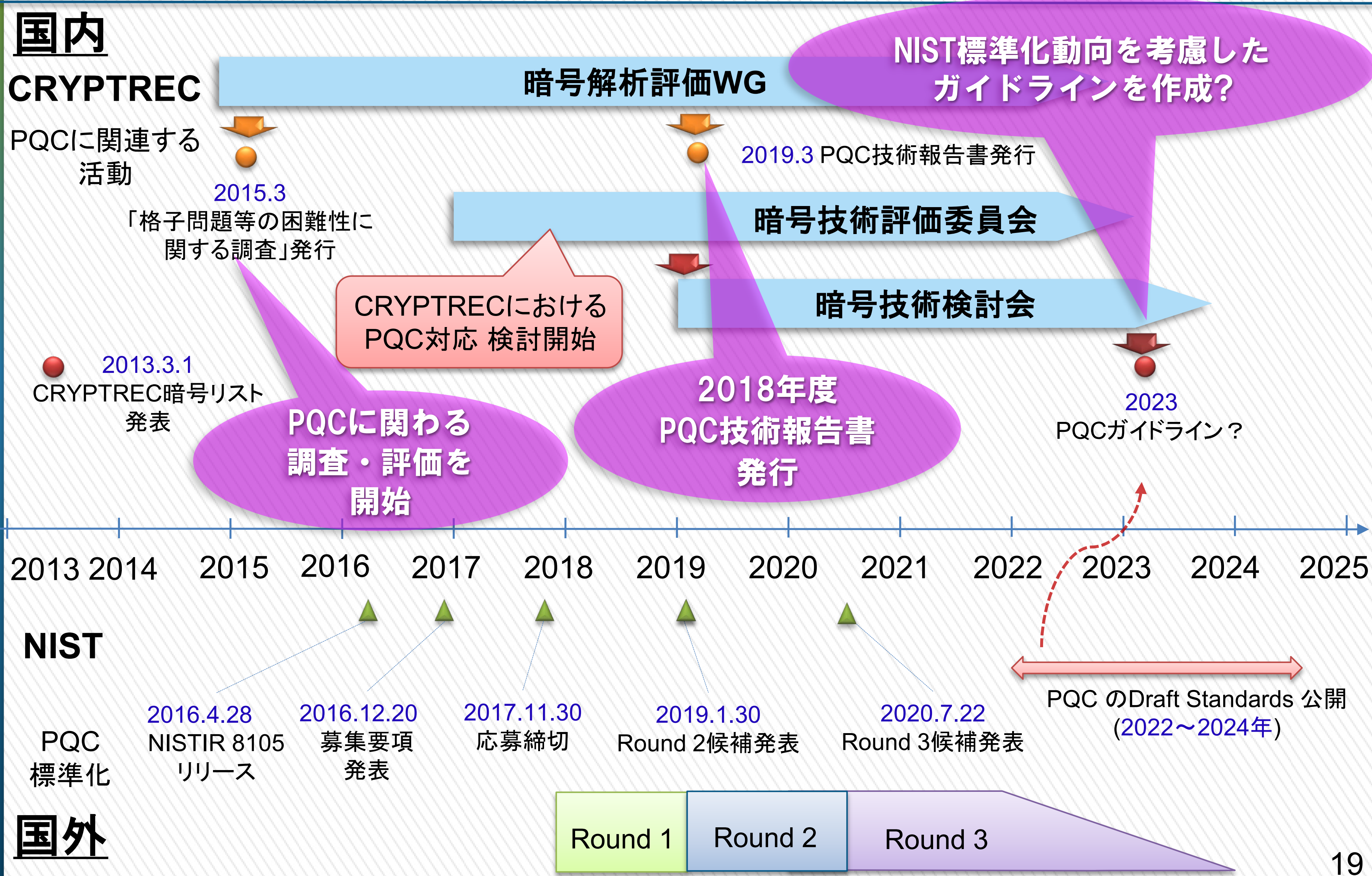
暗号技術活用委員会
事務局：IPA, NICT

セキュリティ対策の推進、暗号技術の利用促進及び産業化を中心とした暗号利用に関する検討課題を担当

暗号技術調査WG
（暗号解析評価WG）

PQC の技術動向調査、暗号への量子コンピュータの影響の調査

PQC の標準化をめぐる国内外の動き



PQC研究動向調査報告書の公開

CRYPTREC
Cryptography Research and Evaluation Committees

ENGLISH

- CRYPTREC概要
- 注意喚起
- CRYPTREC暗号
- CRYPTREC報告書
- ガイドライン
- 技術報告書
- 会議資料
- イベント
- 関連機関等のご案内

トピックス

耐量子計算機暗号の研究動向調査報告書の公開

平成31年4月5日
国立研究開発法人情報通信研究機構
独立行政法人情報処理推進機構

国立研究開発法人情報通信研究機構（略称NICT）と独立行政法人情報処理推進機構（略称IPA）が共同で運営する「暗号技術評価委員会」の2017～2018年度の活動成果として、「耐量子計算機暗号の研究動向調査報告書」を公開いたします。

- 「耐量子計算機暗号の研究動向調査報告書」(PDFファイル: 1,981KB)

本報告書に対するお問い合わせは、下記までお願いいたします。 問い合わせ等の受付はe-mailのみといたします。
CRYPTREC事務局
E-mail : info@cryptrec.go.jp

https://www.cryptrec.go.jp/topics/cryptrec_20190405_tr_2001_2018.html

現在の量子コンピュータによる暗号技術の安全性への影響(1)

- CRYPTREC概要
- 注意喚起
  - 【最新】注意喚起情報
  - 注意喚起一覧
- CRYPTREC暗号
- CRYPTREC報告書
- ガイドライン
- 技術報告書
- 会議資料
- イベント
- 関連機関等のご案内

注意喚起情報

CRYPTREC ER-0001-2019

現在の量子コンピュータによる暗号技術の安全性への影響

2020年(令和2年)2月17日
CRYPTREC 暗号技術評価委員会

> 今般、ゲート型の量子コンピュータが量子超越を実現したという報告があり、暗号技術の危殆化が一部で懸念されております。しかし、現在の量子コンピュータの開発状況をふまえると、暗号解読には規模の拡大だけでなく量子誤り訂正などの実現が必要であるため、CRYPTRECとしては、CRYPTREC暗号リスト記載の暗号技術が近い将来に危殆化する可能性は低いと考えています。
> 今後も、本暗号リスト記載の暗号技術の監視活動を引き続き実施していきます。

今般、ゲート型の量子コンピュータが量子超越を実現したと主張する論文がNature誌に発表されました[1]。この論文では、ランダム量子回路からのサンプリング問題を、古典計算機を用いた場合には1万年かかるところ、量子コンピュータを用いると200秒で完了すると主張しています。この主張は、ランダム量子回路からのサンプリング問題を、量子コンピュータが古典計算機よりも高速に解くことを示しています。これにより、現在広く使用されている公開鍵暗号であるRSA暗号及び楕円曲線暗号などの安全性が大

https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2019.html

現在の量子コンピュータによる暗号技術の安全性への影響(2)

- ゲート型の量子コンピュータが量子超越を実現したという報告があり、暗号技術の危殆化が一部で懸念されている。
- 使用されている量子コンピュータは53量子ビットであり、ターゲットとする問題の性質上、量子誤り訂正は組み込まれていない。
- その一方で、量子コンピュータを用いて2048ビットRSA合成数の素因数分解を行う場合には、量子誤りが一切ないという理想的な環境下でも、4098量子ビットが必要であり、量子誤りがあるという現実的な環境下では、2000万量子ビットが必要であるという見積もりあり。
- 実現されている量子コンピュータと素因数分解を行うのに必要とされる量子コンピュータの性能に関しては、依然として大きな乖離があります。これは離散対数問題を利用する暗号についても同様です。近い将来に、2048ビットの素因数分解や256ビットの楕円曲線上の離散対数問題が解かれる可能性は低い

現在の量子コンピュータによる暗号技術の安全性への影響(3)

- R1年度：共通鍵暗号

年度	報告書名	著者名	報告
2019	量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価	細山田 光倫	CRYPTREC EX-2901-2019
2019	XTSモードの実装性能調査	株式会社レピダム	CRYPTREC EX-2902-2019

【調査報告書に対する暗号解析評価WGの見解】
CRYPTRECの電子政府推奨暗号リストにある共通鍵暗号、暗号利用モード、ハッシュ関数に対する直近で現実的な脅威が生じる可能性は極めて低く、現状ではCRYPTRECでの具体的な対応は不要である。

https://www.cryptrec.go.jp/ex_reports.html

- R2年度：RSA暗号、楕円曲線暗号等（素因数分解、離散対数問題）
  - （仮）Shorの量子アルゴリズムによる現代暗号への脅威に関する調査
  - 来年度に公開予定

３．量子コンピュータを用いて離散対数問題を解く計算の検証

離散対数問題(DSA等で利用)

【(有限体上の)離散対数問題 (DLP)】

与えられた素数 p, 自然数 $g, t(\leq p-1)$ に対して、

$$t = g^X \pmod p$$

を満たす自然数 Xが存在するなら、それを計算せよ。

- 離散対数問題の例

$$5 = 3^X \pmod 7.$$

$3 = 3^1 \pmod 7$, $2 = 3^2 \pmod 7$, $6 = 3^3 \pmod 7$,

$4 = 3^4 \pmod 7$, $5 = 3^5 \pmod 7$, $1 = 3^6 \pmod 7$,

$$X = 5.$$

- Shorのアルゴリズムと現在の量子コンピュータで解ける離散対数問題の大きさを知りたい！

→ 現在解けるのは

$$\boxed{1 = 2^{x} \pmod{3}}.$$

- 報道発表（2020/12/09）

量子コンピュータ実機を用いた離散対数問題の求解実験に成功

～次世代における暗号の安全性確保に向けて～

2020年12月9日

国立研究開発法人情報通信研究機構

ツイート いいね！ 133

ポイント

- IBM社の超電導量子コンピュータを用いた離散対数問題の求解実験に成功
- 離散対数問題の多様性のある特性を生かした量子コンピュータ向けプログラミング
- 現在の暗号への脅威の将来予測、耐量子計算機暗号への移行の第一歩に向けて

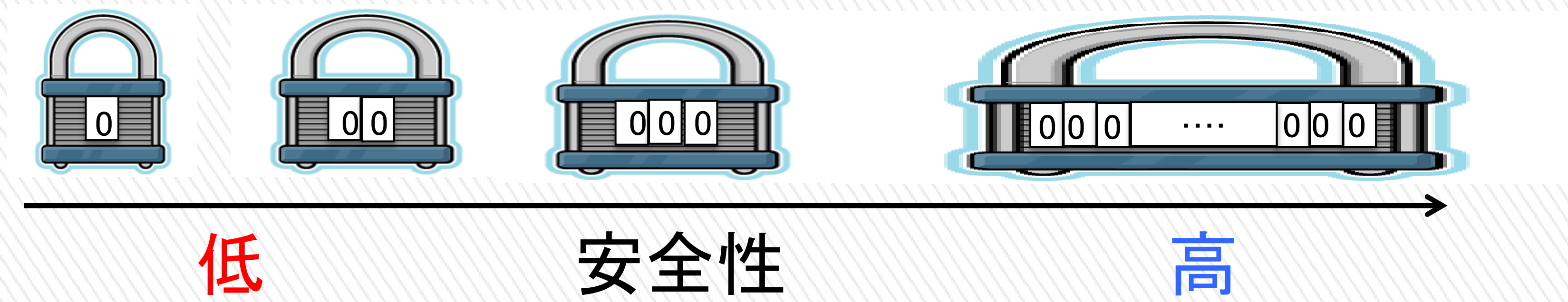
国立研究開発法人情報通信研究機構（NICT）、学校法人慶應義塾（慶應大学）、株式会社三菱UFJフィナンシャル・グループ（MUFG）、株式会社みずほフィナンシャルグループ（MHFG）は、IBM Q Hub at Keio Universityのある慶應義塾大学量子コンピューティングセンター（KQCC）において、量子コンピュータ時代における暗号の安全性確保のための第一歩として、クラウドからアクセス可能な量子コンピュータであるIBM Quantumを使用した小規模離散対数問題の求解実験に成功しました。

https://www.nict.go.jp/press/2020/12/09-1.html

４．　耐量子計算機暗号の安全性評価

公開鍵暗号の安全性評価

- 公開鍵暗号の鍵長と安全性



- ＲＳＡ暗号の場合

15 = 3・5,　687947247083 = 765881・898243

- 現時点での技術力で解ける鍵長の最大値を**解読実験の世界記録**から見積もる

公開鍵暗号と量子コンピュータの関係(3)

量子コンピュータと
Shorのアルゴリズム(1994)で
効率よく解くことができる

- 現在使用されている公開鍵暗号
  - RSA 暗号: 整数の素因数分解
  - 楕円曲線暗号: 楕円曲線上の離散対数問題

今日のお話

- PQC として期待される公開鍵暗号
  - 格子に基づく暗号: 格子問題(LWE 問題等)
  - 符号に基づく暗号: LPN 問題
  - 多変数多項式に基づく暗号: MP 問題, IP 問題
  - 同種写像に基づく暗号: 同種写像問題

多変数多項式に基づく暗号

- 連立代数方程式を解く計算の困難性を
  暗号の安全性の根拠とする暗号

$$f_1(x_1, x_2) = {x_1}^2 + 2x_1x_2 + 11{x_2}^2 + 2x_1 + 5x_2 + 29 \equiv 25 \pmod{31}$$
$$f_2(x_1, x_2) = 5{x_1}^2 + x_1x_2 + 2{x_2}^2 + 10x_1 + 2x_2 + 4 \equiv 27 \pmod{31}$$
$$f_3(x_1, x_2) = 6{x_1}^2 + 5x_1x_2 + 5{x_2}^2 + 3x_1 + 6x_2 + 16 \equiv 2 \pmod{31}$$
$$f_4(x_1, x_2) = 11{x_1}^2 + 13x_1x_2 + 17{x_2}^2 + 19x_1 + 23x_2 + 29 \equiv 17 \pmod{31}$$

- 変数が増えるほど問題が難しくなり安全性が高まる

- 変数が少ないほど暗号処理のコストが減る

多変数多項式に基づく暗号の安全性評価

- Fukuoka MQ Challenge

https://www.mqchallenge.org/

  - MQ問題を解くコンテスト
  - 6種の問題が設定されている

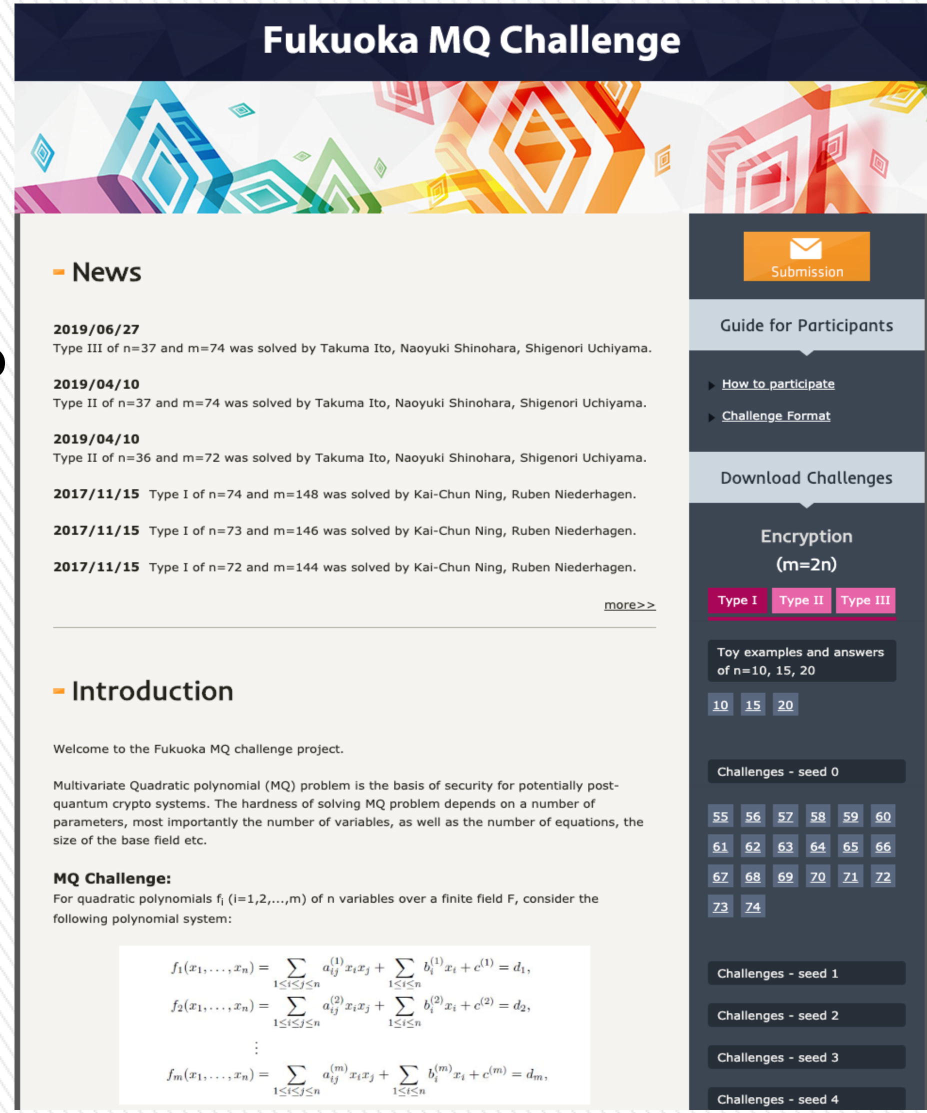
    【暗号用の問題】

    Type I～III: $m = 2n$

    【署名用の問題】

    Type IV～VI: $n \approx 1.5m$

  - どのようなアルゴリズムを用いて, 何変数まで解けたかが報告されている
  - 高木教授: 主催者の一人



報道発表及び国際会議での発表

- 2019/6/27 に報道発表

耐量子計算機暗号の安全性評価で世界記録を達成

～量子コンピュータを使用しても解読が困難な"多変数公開鍵暗号"の実用化に向けて～

2019年6月27日

国立研究開発法人情報通信研究機構
公立大学法人首都大学東京

Type II,III で
37変数

- 耐量子計算機暗号の一つとされる多変数公開鍵暗号の安全性評価のコンテストで世界記録達成
- 従来の解読方法より計算が5倍速く、メモリ使用量を8分の1に削減することに成功
- 量子コンピュータ時代でも安全かつ高速な暗号技術の実用化に期待

https://www.nict.go.jp/press/2019/06/27-1.html

- IWSEC2019

グレブナー基底計算
アルゴリズム

Awards

Best Paper Award

An Efficient F4-style Based Algorithm to Solve MQ Problems
Takuma Ito, Naoyuki Shinohara, and Shigenori Uchiyama

https://www.iwsec.org/2019/

2020/08/03:Type III 記録更新（38変数）
T. Chou, R. Niederhagen, B.-Y. Yang
計算手法：XL with block Wiedemann

概要(まとめ)

Q: 量子コンピュータが実用化されると何が問題に？

A: 現在利用されている公開鍵暗号は安全性が低下する.

Q: 耐量子計算機暗号（PQC: *Post-quantum* cryptography）とは？

A: 十分な規模の量子コンピュータが実用化されても
安全性を保つことができる暗号.

Q: PQC について NICT が取り組んでいることは？

A: PQC の使用に向けた準備及び PQC の研究開発