資料8－1

耐量子計算機暗号(PQC)と NICTの研究開発

国立研究開発法人情報通信研究機構

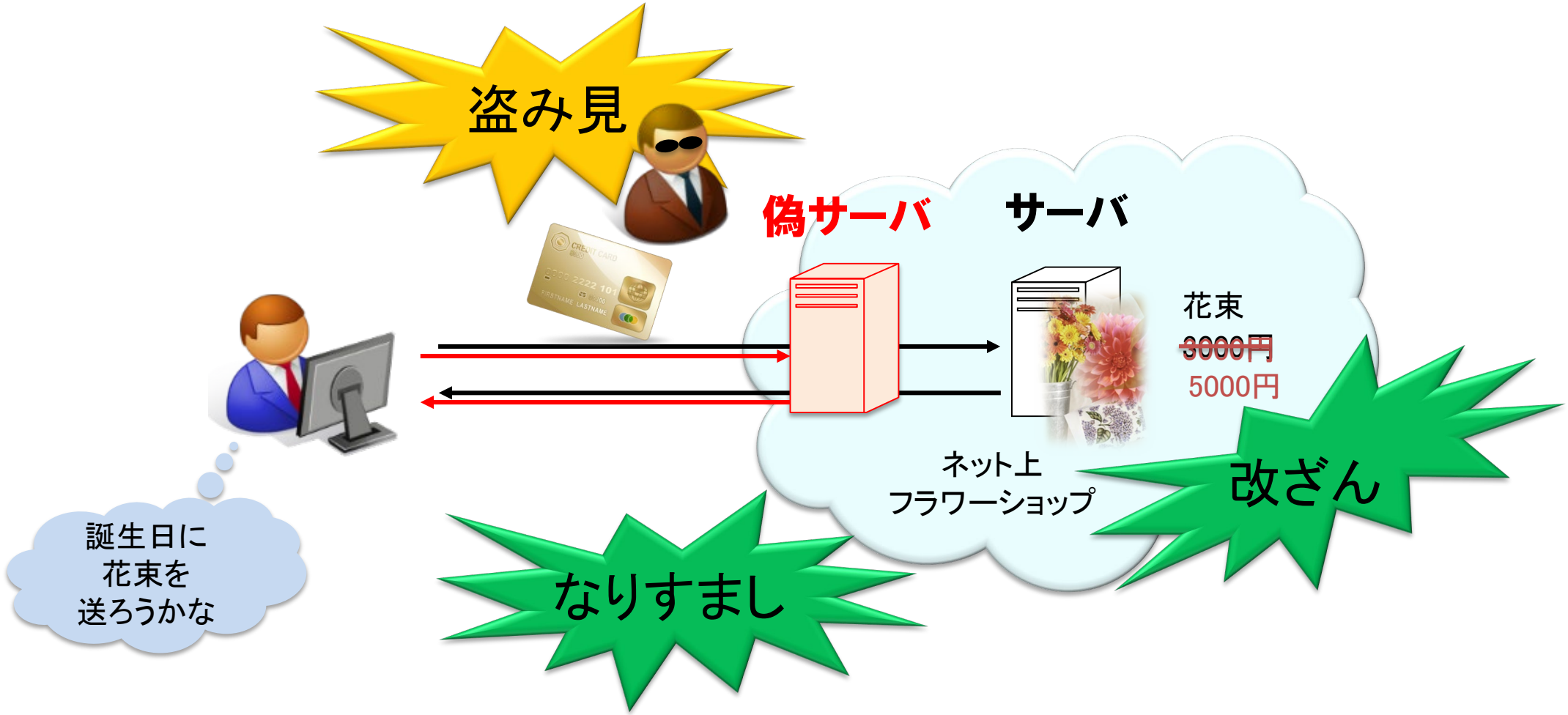
サイバーセキュリティ研究所　セキュリティ基盤研究室

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

１．耐量子計算機暗号

ネットワーク社会における脅威の例



総務省ICTサイバーセキュリティ政策分科会(2024年5月27日)

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

総務省ICTサイバーセキュリティ政策分科会(2024年5月27日)

主要な暗号の例

CRYPTREC LS-0001-2022

電子政府における調達のために参照すべき暗号のリスト
（CRYPTREC暗号リスト）

令和５年３月30日
デジタル庁・総務省・経済産業省

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。なお、利用する鍵長について、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[5]の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。

技術分類		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		EdDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号(注2)	該当なし
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
		SHA-256

公開鍵暗号（署名）：
改ざん検出、相手認証

公開鍵暗号（守秘・鍵共有）：
共通鍵暗号を使うために使う

共通鍵暗号：秘匿

総務省ICTサイバーセキュリティ政策分科会(2024年5月27日)

https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022.pdf

公開鍵暗号に対する量子コンピュータの脅威

CRYPTREC LS-0001-2022

電子政府における調達のために参照すべき暗号のリスト
（CRYPTREC暗号リスト）

令和５年３月30日
デジタル庁・総務省・経済産業省

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という）
び実装性能が確認された暗号技術[2]につい
か今後の普及が見込まれると判断され、当該技術
なお、利用する鍵長について、「暗号強度要件（アルゴリズ
設定基準」[5]の規定に合致しない鍵長を
暗号技術を利用しているとは見なされないこと

技術分類		
公開鍵暗号	署名	DSA
		ECDSA
		EdDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号(注2)	該当なし
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
		SHA-256

量子コンピュータの性能が向上すると
解読されるおそれがある.
（現時点での量子コンピュータの
性能ではまだ無理. ）

量子コンピュータと
Shor’s algorithm（1994）で
効率よく解くことができる

素因数分解や離散対数問題が
解けると解読されてしまう

鍵長を2倍にする必要がある

総務省ICTサイバーセキュリティ政策分科会(2024年5月27日)

https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022.pdf

耐量子計算機暗号について

- **耐量子計算機暗号（PQC）**
  - ✓ 従来の公開鍵暗号が使われている環境で従来と同様に使用でき、量子コンピュータ及び旧来のコンピュータを利用しても その安全性を保つことができる使える公開鍵暗号
  - ✓ 大規模量子コンピュータによる従来型公開鍵暗号の危殆化のおそれがあるため、PQCへの移行を進めていく必要があり、その研究開発をする必要がある

- **耐量子計算機暗号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
  - ✓ **ハッシュ関数に基づく署名**: 原像計算困難性等

耐量子計算機暗号の研究開発と実装に向けて

★：後のスライドで説明

実装

PQC への移行

PQC標準化(ガイドラインなど)★

活用方法の整理
（PQCと既存の公開鍵暗号の併用など）

研究開発

- **暗号方式の性能向上**
  （高機能化、高速実装、使用データ削減など）
- **暗号方式の開発**★
  （格子暗号、符号暗号、多変数多項式暗号、同種写像暗号、ハッシュ関数署名など）

耐量子計算機暗号の研究

- **実装によって生じる脆弱性の解析と対策**
  （サイドチャネル攻撃対策など）
- **安全性の根拠となる問題の解析・設定** ★
  （暗号解読コンテストへの挑戦など）

安全性評価の研究
（既存の公開鍵暗号を含む）

研究

世界におけるPQCの準備状況

- 米国等では標準化の動きがある
  - ✓ **米国NIST**は、標準化のコンペティションを行い、標準となるPQCを選定中
    - 2016年から募集を開始し、2024年に標準化完了予定
    - **2022年に4候補が選定**されたが、**追加の募集**も行われている
  - ✓ 米国大統領が、PQCに関する覚書に署名（2022年5月4日）
    - 2035 年までに量子コンピュータによる脅威を可能な限り軽減することを目標

NIST のPQC 標準化

２．耐量子計算機暗号に関する NICT の研究開発

NICT　サイバーセキュリティ研究所　セキュリティ基盤研究室

国立研究開発法人 情報通信研究機構

暗号技術が専門

- 電磁波研究所
- ネットワーク研究所
- **サイバーセキュリティ研究所**
  - **セキュリティ基盤研究室**
  - サイバーセキュリティ研究室
- ユニバーサルコミュニケーション研究所
- 未来ICT研究所
- Beyond 5G研究開発推進ユニット
- 量子ICT協創センター

セキュリティ基盤研究室 研究計画 (2021-2025)

量子コンピュータ時代に向けた暗号技術の安全性評価

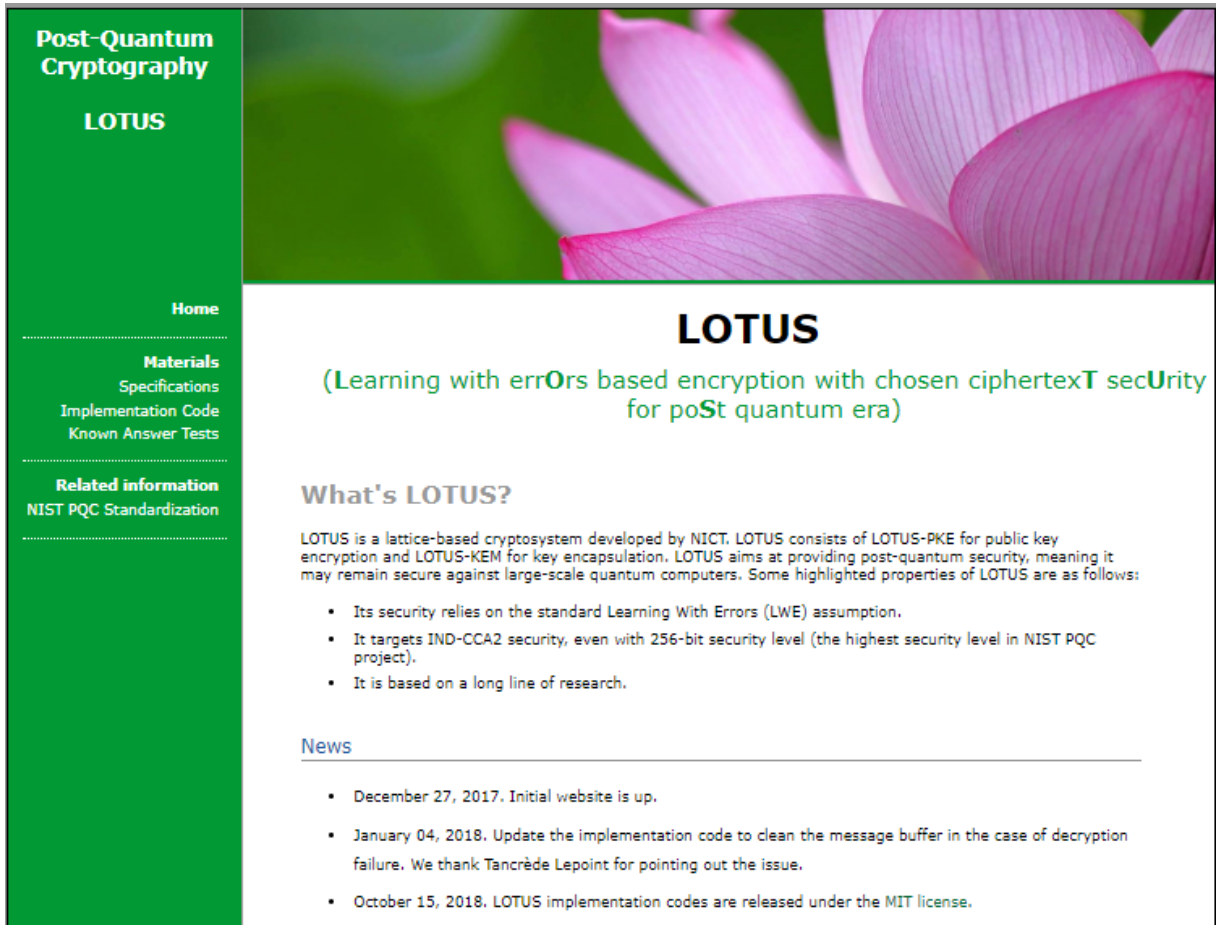
- **耐量子計算機暗号の研究開発**
- **CRYPTREC：電子政府システム等において使用される暗号技術の安全性評価**
- 国民生活を支えるシステムの安全な運用に貢献

安全なデータ利活用技術

- データのセキュリティ・プライバシーの確保
- 秘密計算等のプライバシー保護解析技術
- 組織横断連携を含むデータ利活用技術
- 安全なテレワーク等に資する研究開発

NICTにおけるPQC関連の暗号方式の研究開発

- 新たな暗号LOTUS
  - ✓NICTが開発した耐量子計算機暗号
  - ✓格子暗号に分類される
  - ✓ベースとなる暗号方式に対して、復号の際に暗号文が破損していないことをチェックする機構を追加することで、ブラウザ、データベースをはじめ、多くのシステムに組み込むことが可能



NICTにおけるPQC関連の安全性評価の研究開発

- PQCの解読コンテストでの世界記録達成
  - ✓ 格子暗号の解読コンテスト
    - TU Darmstadt LWE Challenge
    - ノイズを含む線型方程式を解く方法の開発
    - ノイズの大きさと変数の個数で難易度が決まる
  - ✓ 多変数公開鍵暗号の解読コンテスト
    - Fukuoka MQ Challenge
    - 連立代数方程式を解く方法の開発
    - 変数の個数で難易度が決まる

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

ツイート　いいね！ 386

ポイント

- 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

安全な暗号パラメータの評価や
耐量子計算機暗号ガイドラインの策定に貢献

現在利用されている暗号技術の安全性評価

- 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

$$1 = 2^X \pmod 3.$$

（実用$y=g^x \pmod p$, p: 600桁程度）

現時点では量子コンピュータの脅威が生じていないことの根拠

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。

3. 耐量子計算機暗号に関する CRYPTREC の取り組み

CRYPTREC（Cryptography Research and Evaluation Committees）

クリプトレック

CRYPTRECとは日本の電子政府推奨暗号リストや暗号に関わるガイドラインを作成、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である。

デジタル庁 Digital Agency
総務省 MIC Ministry of Internal Affairs and Communications
経済産業省 Ministry of Economy, Trade and Industry

暗号技術検討会
事務局：デジタル庁、総務省、経済産業省

国立研究開発法人 情報通信研究機構 NICT National Institute of Information and Communications Technology
IPA Better Life with IT 情報処理推進機構

暗号技術評価委員会
事務局：NICT, IPA

暗号技術の安全性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

日本（CRYPTREC）におけるPQCの準備状況

- 2021年度から2024年度において、CRYPTRECの暗号技術評価委員会の下にPQCを専門に検討する**「暗号技術調査ワーキンググループ（耐量子計算機暗号）（通称　PQC WG）」**を設置。
  PQC WGの事務局はNICTとIPA。
- PQC WGにおいてPQCの動向を調査し、2022年度に「**耐量子計算機暗号の研究動向調査報告書**」を発行し、それをもとに **「CRYPTREC暗号技術ガイドライン（耐量子計算機暗号）」**を策定し発行。
- さらに調査を続け、2024年度末に**新たな調査報告書**を発行し、それを基にした**新たなガイドライン**を策定し発行する予定。

耐量子計算機暗号の研究動向調査報告書／CRYPTREC暗号技術ガイドライン（耐量子計算機暗号）

- 「耐量子計算機暗号の研究動向調査報告書」
  - PQCのいろいろな方式、その安全性などを調査するとともに、国内の有識者により選定された有望と考えられるPQCをリストアップし、その詳細について報告
- 「CRYPTREC暗号技術ガイドライン（耐量子計算機暗号）」
  - 一般の利用者にPQCを利用していただくためのガイドライン

耐量子計算機暗号ガイドラインの目次（2022年度版）

1. 導入
2. 耐量子計算機暗号の活用方法
3. 格子に基づく暗号技術
4. 符号に基づく暗号技術
5. 多変数多項式に基づく暗号技術
6. 同種写像暗号に基づく暗号技術
7. ハッシュ関数に基づく暗号技術

- 1章
  - ✓PQCの動向について
  - ✓（量子コンピュータによる現代暗号への脅威など）
- 2章
  - ✓実社会でのPQCの活用事例を説明。
  （特に守秘・鍵交換・署名の活用事例）
- 3章～7章
  - ✓安全性の根拠となる問題の説明
  - ✓各暗号技術の説明
  （アルゴリズムの擬似コード、暗号文・署名分、鍵長のサイズなど）