耐量子計算機暗号の最新動向

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

概要

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

A: 十分な規模の量子計算機が実用化されても
安全性を保つことができる暗号.

Q: 量子計算機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: PQC について NICT が取り組んでいることは？

A: PQC の最新動向調査及びPQC の開発・安全性評価.

1．暗号技術と量子計算機

ネットワーク社会の安全を守る暗号技術

ネットワークの発展とともに、暗号技術は
通信・交通・ビジネスの根幹を支える身近な技術へ







暗号技術の身近な利用例

- インターネットショッピングなどで見かける
  https://www.*********
  - Hyper Text Transfer Protocol Secure:
    SSL/TLS プロトコル（暗号技術）を利用して
    HTTP通信を行う。

公開鍵暗号の歴史

RSA暗号（素因数分解問題）

広く普及　楕円曲線暗号（離散対数問題）

ペアリング暗号（クラウド時代向けの暗号）

標準化、製品化

耐量子計算機暗号（PQC）: 格子理論，多変数多項式,符号理論,同種写像

完全準同型暗号，多重線形性暗号

研究段階

公開鍵暗号と数学と量子計算機

量子計算機と
Shor's algorithm 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

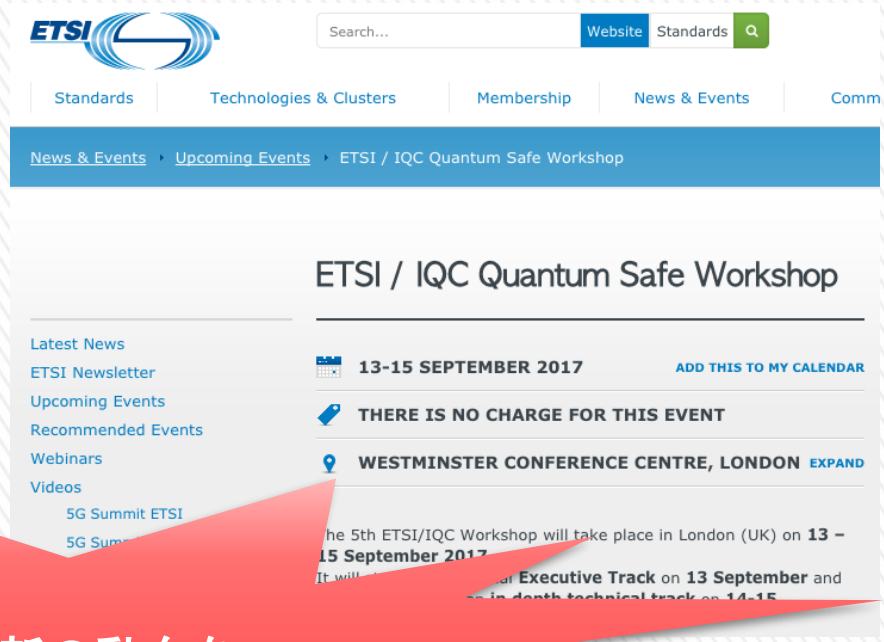
- PQC として期待される公開鍵暗号
  - 格子に基づく暗号: 格子問題(LWE 問題等)
  - 符号に基づく暗号: LPN 問題
  - 多変数多項式に基づく暗号: MP 問題, IP 問題
  - 同種写像に基づく暗号: 同種写像問題

PQC の実用化に向けた世界的な動き

- 背景
  - もし十分な規模の量子計算機が実用化されると RSA 暗号や楕円曲線暗号は安全性を保てない.
  - 今後20年以内に十分な規模の量子計算機が構築されると予想されている.
  - 現在利用されている暗号は，普及するまで20年近くかかっている.
  - 今から PQC の実用化に取り組む必要がある.

参照（NIST）：https://csrc.nist.gov/projects/post-quantum-cryptography

- 世界各国の動き
  - 米国(NIST): PQCを公募し(締め切り:2017.11.30)、現在は評価の段階
  - 欧州(ETSI):PQCの調査を実施
  - 日本(CRYPTREC): PQCの調査を実施



PQCに関する最新の動向を
把握する必要性が高まっている.

2．PQC の最新動向調査（CRYPTREC での活動）

暗号技術における NICTの取り組み

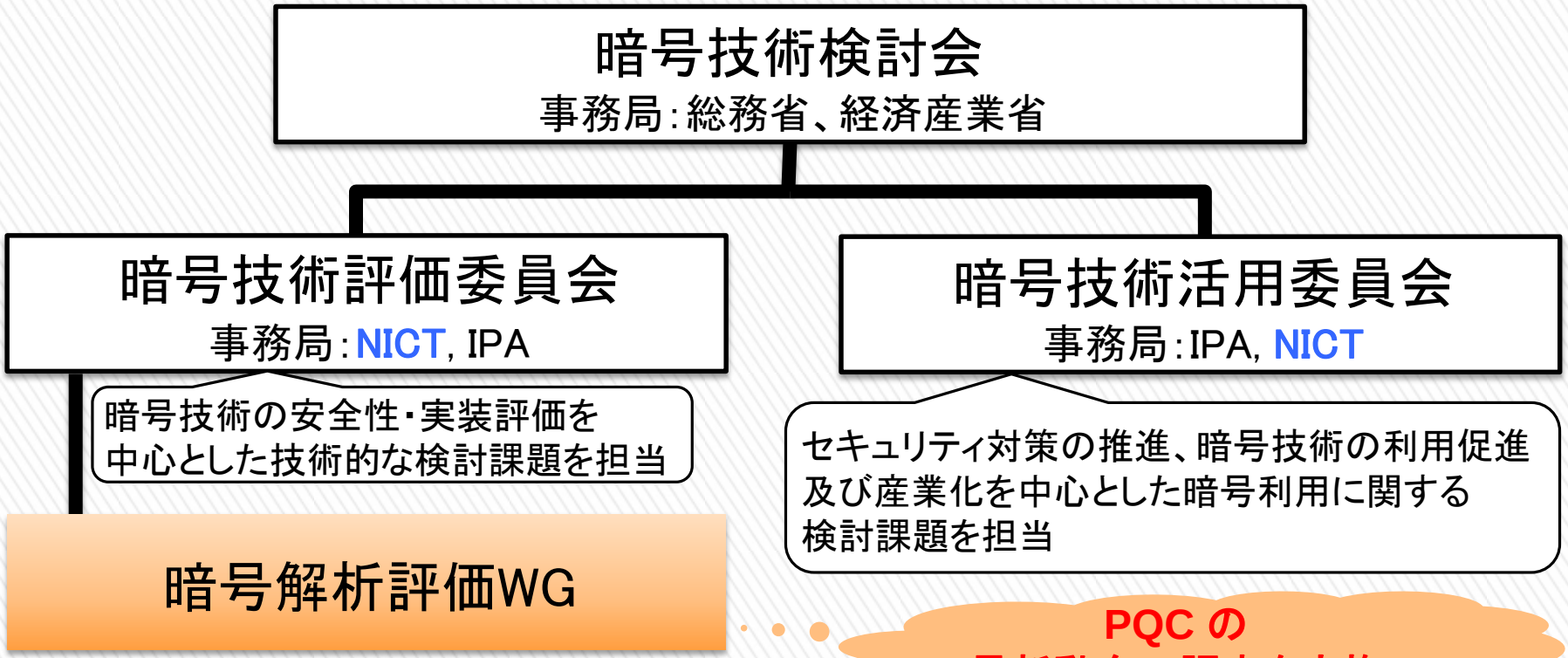
【中長期計画】1-4. サイバーセキュリティ分野　(3) 暗号技術

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

CRYPTREC とは

- 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



PQCの最新動向調査計画

- 活動内容(2017 年度及び 2018 年度)

  PQCの代表的な四方式について

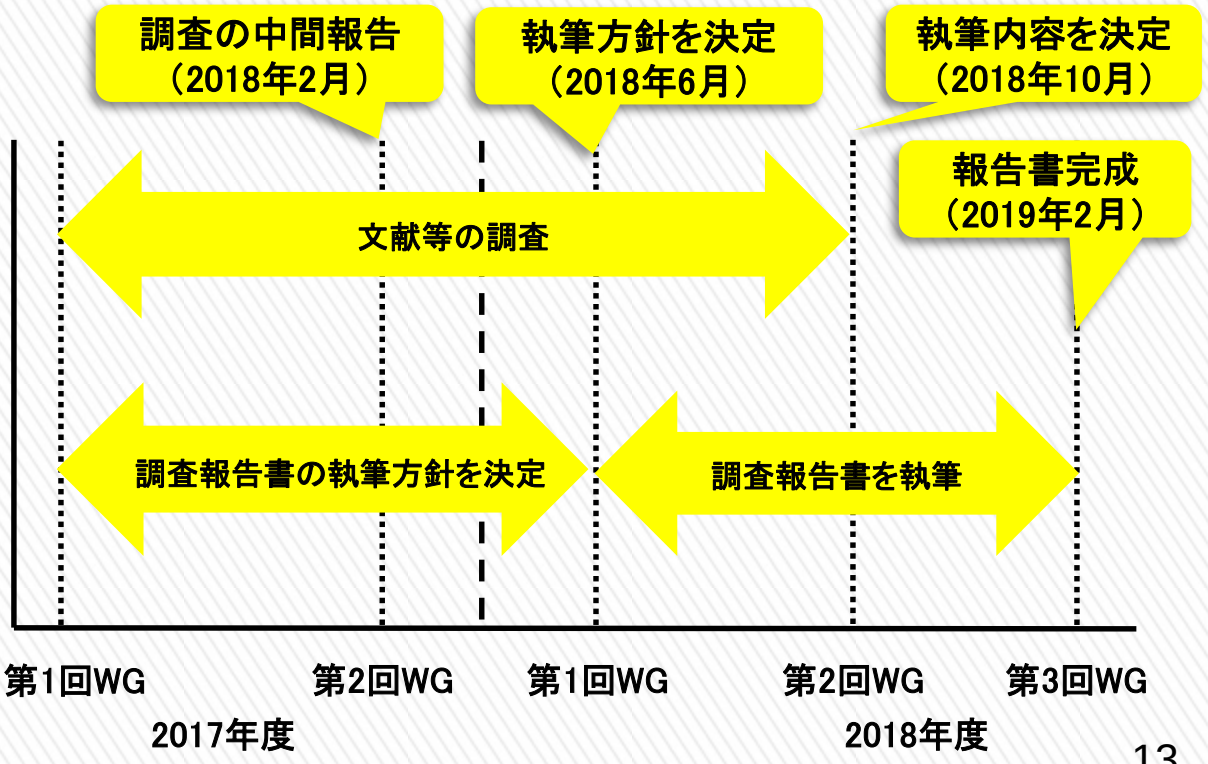
  三つの機能を中心に調査し, 結果をまとめる。

四つの暗号方式

- 格子に基づく暗号
- 符号に基づく暗号
- 多変数多項式に基づく暗号
- 同種写像に基づく暗号

三つの機能

- 暗号
- 署名
- 鍵交換



3. 格子に基づく暗号の安全性評価

安全性評価へのNICTの取り組み

現在利用されている暗号技術

- 電子政府推奨暗号
- 国際標準暗号
- その他デファクト暗号

RSA, ECC, AES, SHA*, …

安全性評価

安心・安全なICTシステムの維持・構築に貢献

今後の利用が想定される暗号技術

- **格子に基づく暗号**
- 多変数多項式に基づく暗号
- 準同型暗号

…

安全性評価

新たな暗号技術の信頼性向上・普及・標準化に貢献

安全性を評価する技術及び理論

数体篩法、関数体篩法、格子理論、代数方程式理論（グレブナー基底）など

公開鍵暗号と数学と量子計算機

量子計算機と
Shor's algorithm で
効率よく解くことができる

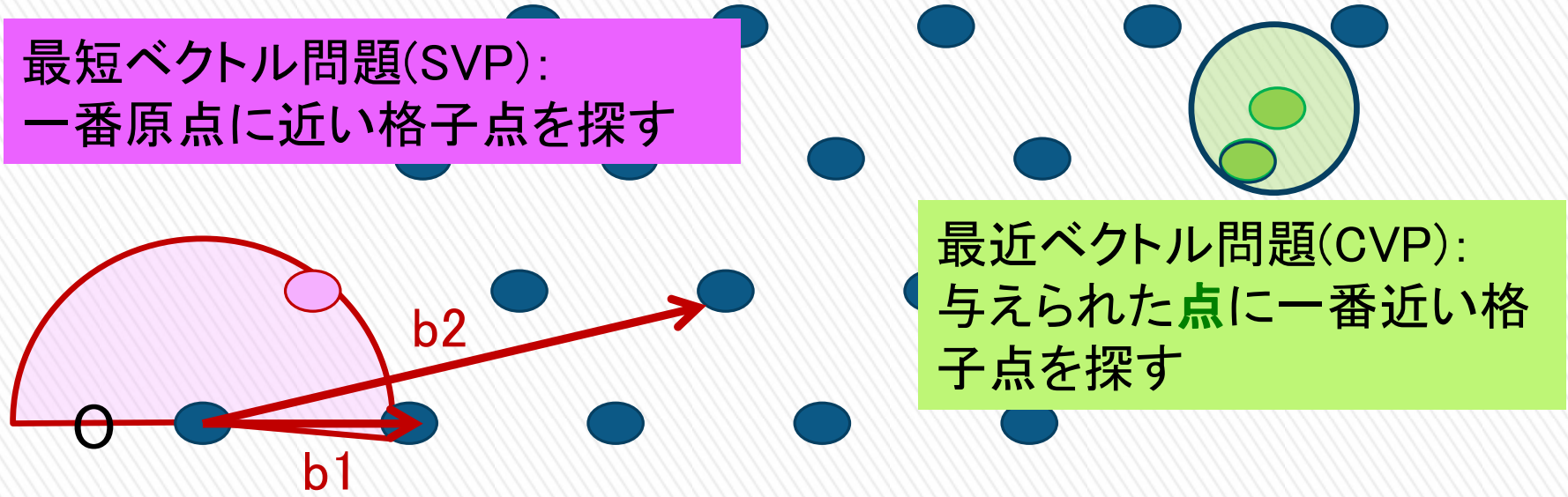
- 現在使用されている公開鍵暗号
  - RSA 暗号: 整数の素因数分解
  - 楕円曲線暗号: 楕円曲線上の離散対数問題

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

格子に基づく暗号

- 格子問題を解く計算の困難性を
  暗号の安全性の根拠とする暗号



- CVPの仲間の、LWE(Learning with errors)問題と
  その亜種がよく使われる

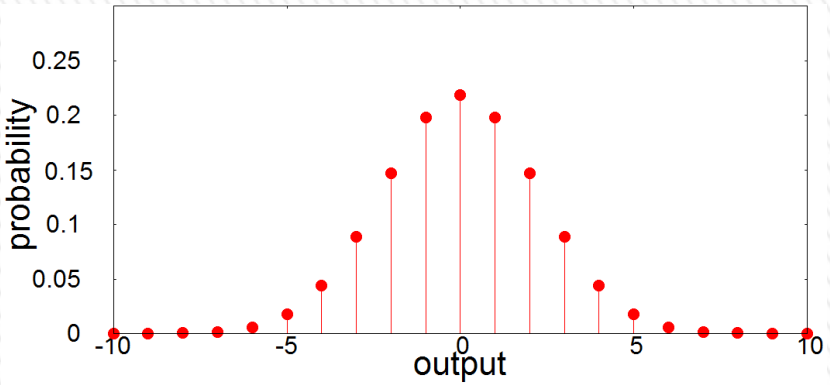
LWE（Learning With Errors）問題とは

- 秘密情報：$\boldsymbol{s} \in \mathbf{Z}_q^{n\times 1}$ と $\boldsymbol{e} \in \psi_{\alpha q}^{m\times 1}$
- 公開情報：$\mathbf{A} \in \mathbf{Z}_q^{n\times m}$ と $\boldsymbol{b} \in Z_q^{m\times 1}$

b = s A + e (mod q)

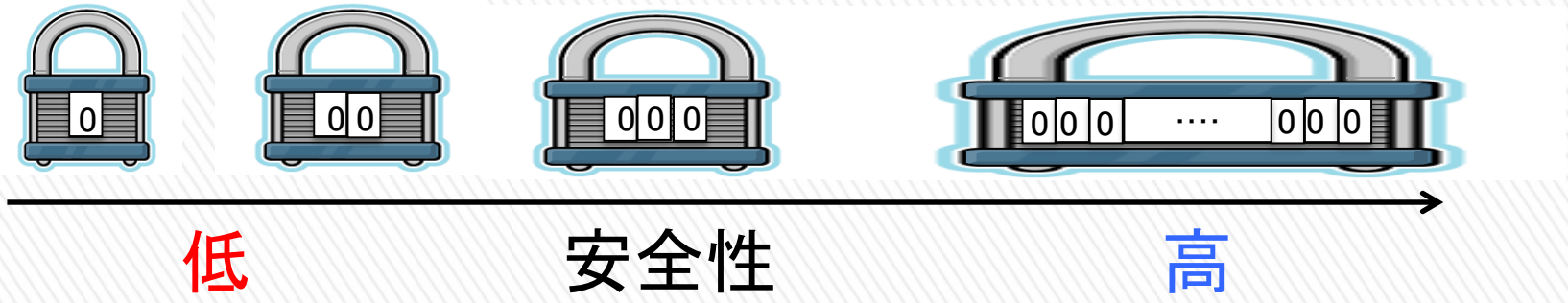
e=(e1,･･･,em) はノイズ

- $\boldsymbol{s}$ または $\boldsymbol{e}$ を計算せよ
- 素因数分解や離散対数問題とは異なる問題



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

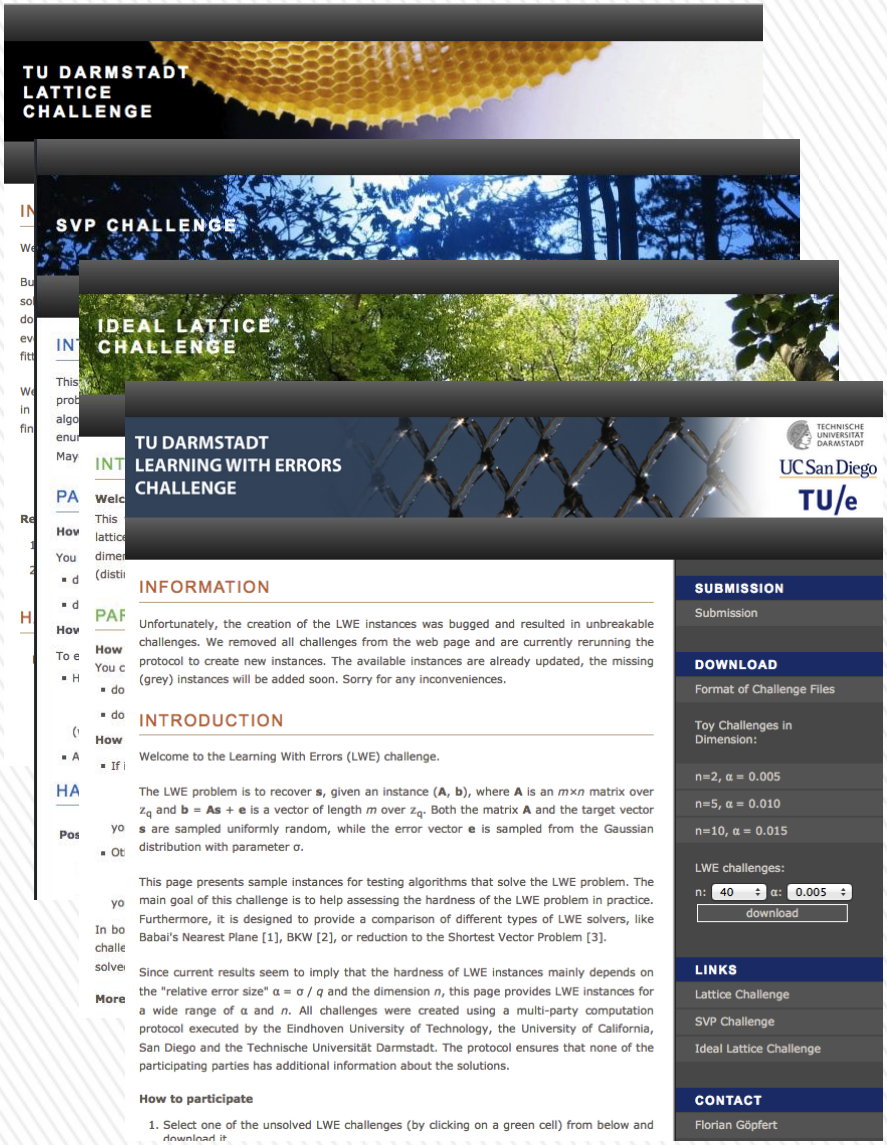
- 現時点での技術力で解ける鍵長の最大値を
  解読実験の世界記録から見積もる

格子に基づく暗号の安全性評価

- TU Darmstadt Lattice Challenge

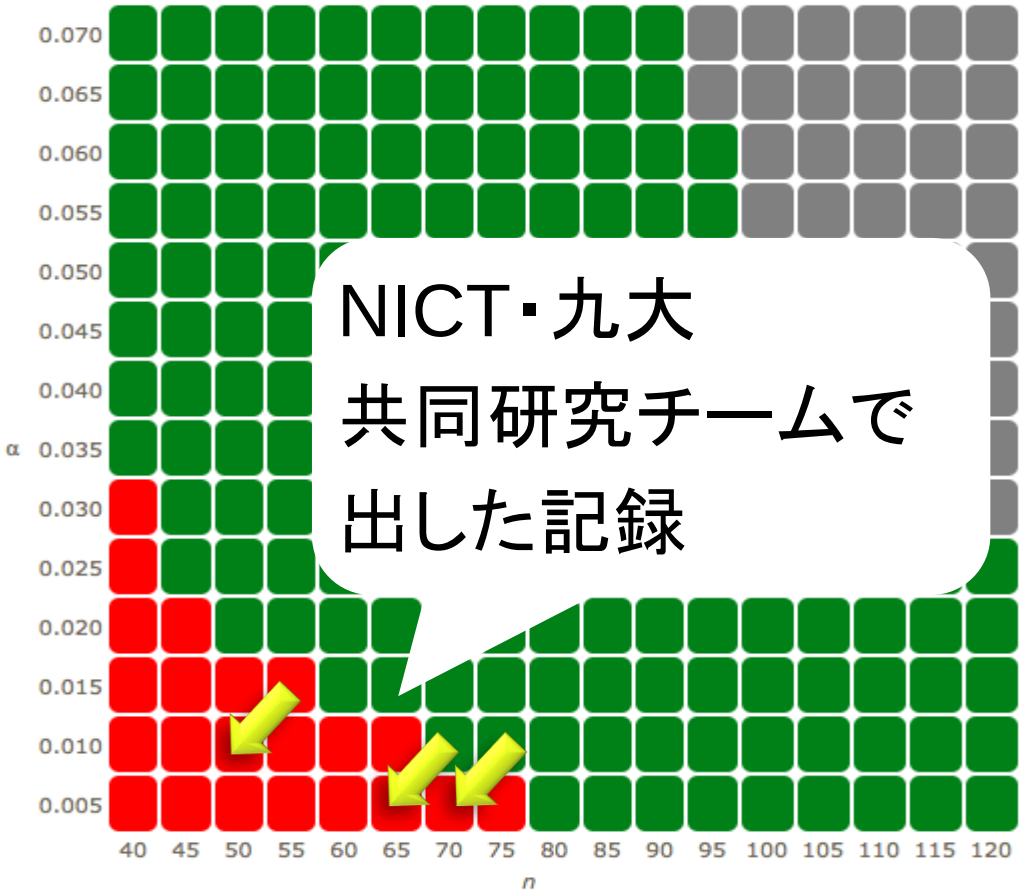
  http://www.latticechallenge.org/

  - 独ダルムシュタット工科大学が2008年より主催しているさまざまな格子問題のコンテスト
    - Lattice Challenge
    - SVP Challenge
    - Ideal Lattice Challenge
    - **LWE Challenge**



格子に基づく暗号の安全性評価（世界記録の更新）

TU Darmstadt LWE Challenge



ノイズの大きさ

問題生成中

未解読問題

解かれた問題

次元

4. PQC の新方式の開発

PQC の開発

- LOTUS(ロータス)
  - **L**earning with err**O**rs based encryption with chosen ciphertex**T** sec**U**rity for po**S**t quantum era
  - LWE 問題を利用した公開鍵暗号

NIST の公募に提案

Timeline

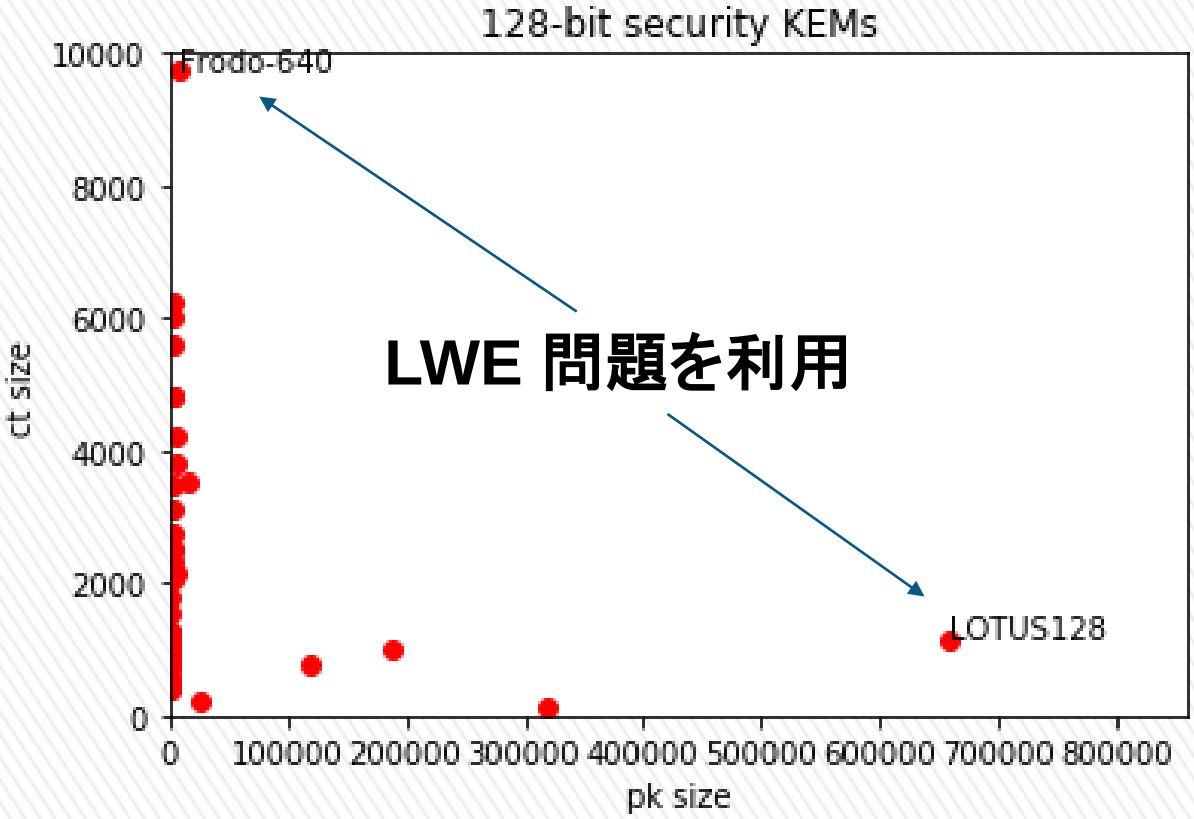
**This is a tentative timeline, provided for information, and subject to change.*

Date	
Feb 24-26, 2016	NIST Presentation at PQCrypto 2016: *Announcement and outline of NIST's Call for Submissions (Fall 2016)*, *Dustin Moody*
April 28, 2016	NIST releases NISTIR 8105, Report on Post-Quantum Cryptography
Dec 20, 2016	Formal Call for Proposals
Nov 30, 2017	Deadline for submissions
Dec 4, 2017	NIST Presentation at AsiaCrypt 2017: *The Ship Has Sailed: The NIST Post-Quantum Crypto "Competition"*, *Dustin Moody*
Dec 21, 2017	Round 1 algorithms announced (69 submissions accepted as "complete and proper")
Apr 11, 2018	NIST Presentation at PQCrypto 2018: *Let's Get Ready to Rumble - The NIST PQC "Competition"*, *Dustin Moody*
April 11-13, 2018	First PQC Standardization Conference - Submitter's Presentations
January 30, 2019	Second Round Candidates announced
August 22-24, 2019 *(tentative)*	Second PQC Standardization Conference
2020/2021	Round 3 begins or select algorithms
2022/2024	Draft Standards Available

参照（NIST）：https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline

LOTUS と FrodoKEM の比較

	公開鍵のサイズ	暗号文のサイズ	双方の和のサイズ
LOTUS	658.9 KB	1.1 KB	660 KB
FrodoKEM	9.6 KB	9.7KB	19.3 KB



詳しくは
NISTIR 8240
参照

概要(まとめ)

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

A: 十分な規模の量子計算機が実用化されても
安全性を保つことができる暗号.

Q: 量子計算機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: PQC について NICT が取り組んでいることは？

A: PQC の最新動向調査及びPQC の開発・安全性評価.