資料１

「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」開催要綱（案）

１．名称

本検討会は「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」（以下「タスクフォース」という。）と称する。

２．開催の趣旨・目的

近年、耐量子計算機暗号の研究開発・標準化が各国で進められているところ、大規模な量子コンピュータの出現に向けて、我が国においても耐量子計算機暗号について議論を行う必要性が高まっていることから、量子コンピュータの動向及び耐量子計算機暗号を含む新たな暗号技術の動向等を踏まえた、次期 CRYPTREC 暗号リストに求められる要件や課題等を整理することを目的として開催する。

３．検討事項

（１）大規模な量子コンピュータの動向を踏まえた次期 CRYPTREC 暗号リストに求められる要件等の検討

（２）その他新たな暗号技術の動向等（軽量暗号や秘密計算に利用される準同型暗号等）を踏まえた検討等

４．構成等

（１）タスクフォースの構成員は、別紙のとおりとする。

（２）タスクフォースの座長は、構成員の互選により定める。

（３）座長は、タスクフォース構成員の中から座長代理を指名できる。

（４）座長は、タスクフォースの議事を掌握する。

（５）座長が、緊急の理由によりやむを得ず不在となった場合、座長代理が座長に代わり議事を掌握する。

（６）座長が必要と認めた者については、オブザーバとしてタスクフォースに出席することができる。

（７）座長が必要と認めるときは、暗号技術の提案者、関連する利害関係者その他の参考人から意見を聴取することができる。

（８）その他、タスクフォースの運営に関し必要な事項は、座長が定めるところによる。

５．議事の公開

タスクフォースは非公開とする。タスクフォースで使用した資料及びタスクフォースの議事概要については、次の場合を除き、公開する。

（１）公開することにより当事者又は第三者の権利、利益や公共の利益を害するおそれがあると座長が認める場合
（２）その他、非公開とすることが必要と座長が認める場合

６．庶務

タスクフォースの庶務は、総務省、経済産業省、国立研究開発法人情報通信研究機構及び独立行政法人情報処理推進機構において処理する。

（別紙）

構成員・オブザーバ名簿

（五十音順、敬称略）

（構成員）

宇根　正志　日本銀行　金融研究所　情報技術研究センター
　　情報技術研究グループ長
國廣　昇　　筑波大学　システム情報系　教授
高木　剛　　東京大学大学院　情報理工学系研究科　教授
松井　充　　三菱電機株式会社　開発本部　役員技監
松本　勉　　横浜国立大学大学院　環境情報研究院　教授
松本　泰　　セコム株式会社　IS 研究所
　　コミュニケーションプラットフォームディビジョン　マネージャー
満塩　尚史　内閣官房 情報通信技術(IT)総合戦略室 政府 CIO 補佐官

（オブザーバ）

内閣サイバーセキュリティセンター
警察庁
個人情報保護委員会事務局
総務省
法務省
外務省
財務省
文部科学省
厚生労働省
経済産業省
防衛省
警察大学校
国立研究開発法人産業技術総合研究所

CRYPTREC
Cryptography Research and Evaluation Committees

資料2

量子コンピュータ時代に向けた
暗号の在り方検討タスクフォースの設置について

令和元年６月２４日
CRYPTREC事務局

背景：暗号技術の課題

- 遠くない将来に現在のRSA暗号や楕円曲線暗号は容易に解読されるようになるおそれ
  （コンピュータの性能向上や、大規模な量子コンピュータが実用化された場合）
- 大規模システムの改修・更改には十年以上を要する

コンピュータ性能の向上に伴い、
より鍵長の長いRSA暗号、楕円曲線暗号も危殆化のおそれ

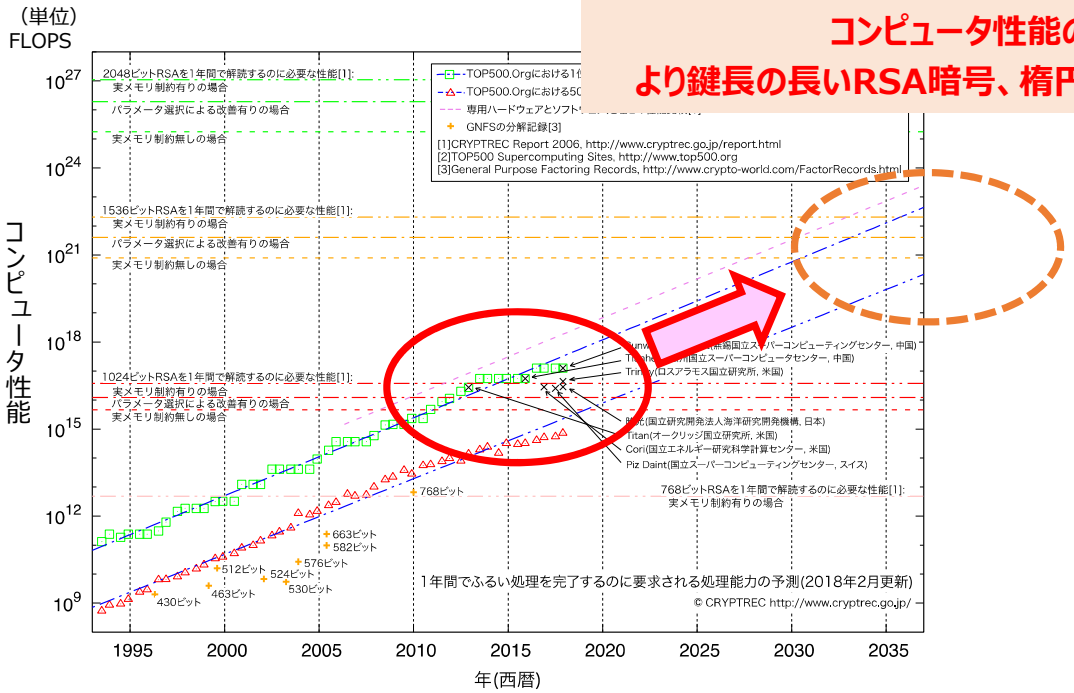


図１：RSA暗号（※）の安全性評価

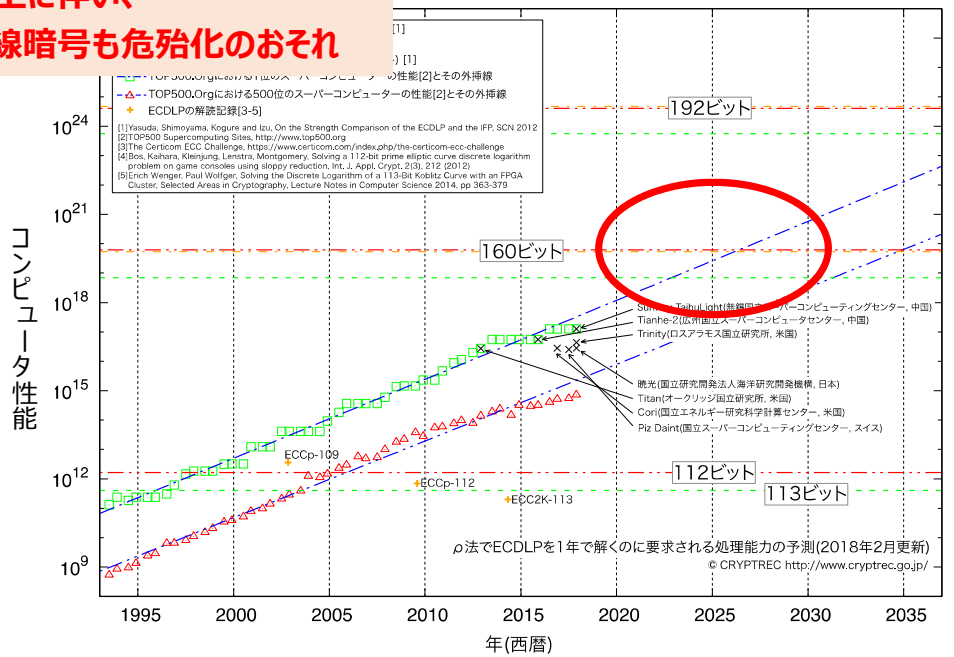


図２：楕円曲線暗号の安全性評価

（※）桁数が大きい合成数の素因数分解が困難であることを安全性の根拠とした公開鍵暗号。過去、1024ビットの鍵長のものが使われていたが、その危殆化（解読されるおそれがあること）により、現在は2048ビット以上の鍵長のものが推奨されている。

（注）グラフの縦軸は、コンピュータが１秒間に処理可能な演算の回数（FLOPS：Floating-Point Operations Per Second）。

設置に至る経緯

- 現在のCRYPTREC暗号リストの策定（2013年3月1日）から6年が経過することや、量子コンピュータの動向や新たな暗号技術の動向を踏まえて、次期CRYPTREC暗号リストの改定方針の素案を、2018年度の暗号技術評価委員会及び暗号技術活用委員会において議論。
- 両委員会の委員からは、**改定方針よりも先に、次期CRYPTREC暗号リストに求められる要件を明確にすべき**という意見。
- これらの議論を受けて、2018年度第1回暗号技術検討会（以下「検討会」という。）での審議の結果、検討会の下に「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」（以下「タスクフォース」という。）を設置し、次期CRYPTREC暗号リストに求められる要件や課題等を整理することとした。

（参考）
2018年度 暗号技術検討会　資料5別添「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」の設置について（案）

２．検討事項

① 大規模な量子コンピュータの動向を踏まえた次期CRYPTREC暗号リストに求められる要件等の検討
② その他新たな暗号技術の動向等（軽量暗号や秘密計算に利用される準同型暗号等）を踏まえた検討等

CRYPTREC活動体制（2019年度）

暗号技術検討会

（１）CRYPTREC暗号のセキュリティ及び信頼性確保のための調査・検討
（２）CRYPTREC暗号リストの改定に関する調査・検討
（３）関係機関と連携した暗号技術の普及による情報セキュリティ対策の推進検討・提言

量子コンピュータ時代に向けた暗号の在り方検討タスクフォース

暗号技術評価委員会

（１）暗号技術の安全性及び実装に係る監視及び評価
（２）新世代暗号に係る調査
（３）暗号技術の安全な利用方法に関する調査

暗号技術調査WG（暗号解析評価）

暗号技術活用委員会

（１）暗号の普及促進・セキュリティ産業の競争力強化に係る検討
（２）暗号技術の利用状況に係る調査及び必要な対策の検討
（３）暗号政策の中長期的視点からの取組の検討

TLS暗号設定ガイドラインWG

今後の進め方（案）

- タスクフォースは、四半期に１回程度の開催を想定し、原則、会合毎に検討事項を絞った議論を行う。
- 議論の結果は、暗号技術検討会（年度末を予定）で報告の上、次期CRYPTREC暗号リストの策定に活用。

第1回～第3回までの進め方イメージ

① 耐量子計算機暗号関係
- 量子コンピュータの動向把握
- 耐量子計算機暗号の動向把握
- 次期CRYPTREC暗号リストへの追加にあたっての論点整理

② その他、新しい暗号技術関係
- 軽量暗号や秘密計算に利用される準同型暗号等、新たな暗号技術の研究開発・標準化動向
- 次期CRYPTREC暗号リストへの追加にあたっての論点整理

第1回（今回）
第2回（9月頃）
第3回（12月頃）

資料3

量子コンピュータの動向について
（素因数分解を例にして）

國廣　昇（筑波大学）

「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」第1回会合

2019年6月24日

素因数分解はそもそも難しいのか？

現状把握

(1) 理論的に知られていること

- 多項式時間アルゴリズムは知られていない
- 知られている最善のアルゴリズムは，準指数関数時間

$$\exp\left(\left(\sqrt[3]{64/9}+o(1)\right)(\ln n)^{1/3}(\ln\ln n)^{2/3}\right)$$

(2) 実験で確認されていること

- 2009年12月 : 768ビット (232桁)の素因数分解
- 数体ふるい法を使用
- ふるいフェーズ : 1500年 AMD Opteron processor (2.2 GHz with 2 GB RAM)

未来を予測

(3) 計算機能力の向上

- ムーアの法則:
  集積回路上のトランジスタ数は「18か月ごとに2倍になる」
- スーパーコンピュータの性能向上

暗号の将来の脆弱性をできるだけ正確に予測するには. . .
(1) 理論的にどこまでわかっているか？
(2) 現在の技術で，実際にどこまで破られるか？
(3) 計算機能力向上の将来動向
を調査することにより行う.

この発表で話したいこと

量子計算機を用いた場合は？
（古典計算機では，根拠を積み重ねて評価している）

「安全」，「危険」の極論ではなく，

- できるだけ正確に危険性を理解したい．
- もしくは，理解に向けて少しでも前進したい．

量子計算機の場合でも．．．
(1) 理論的にどこまでわかっているか？
(2) 現在の技術で，実際にどこまで破られるか？
(3) 計算機能力向上の将来動向
を知りたい．

量子アルゴリズム

1985年: Deutschが，量子Turing Machineを提案
1994年: Simonのアルゴリズム（周期関数の位数発見）
1994年: Shorの素因数分解アルゴリズム，
　　離散対数問題の解法アルゴリズムの提案
　　（可換隠れ部分群問題への拡張）
1996年： Groverのアルゴリズム（探索問題）

参考：これ以外のアルゴリズム
Quantum Algorithm Zoo
https://math.nist.gov/quantum/zoo/

量子計算機と暗号を取り巻く環境の変化

1.ポスト量子暗号の募集

2015年8月：NSAが，ポスト量子暗号への移行を表明
2016年2月：NISTが，ポスト量子暗号の標準化計画を公表
量子計算機の実現に備えて，素因数分解，離散対数問題の困難さに依存しない暗号の募集

69件が応募
2019年1月30日，Round 2 algorithmsを公表
2022～2024年までに標準化

2. Noisy Intermediate-scale Quantum (NISQ)の開発

小さいながらも，実際の量子計算機が出来てきた
Noisy Intermediate-scale Quantum (NISQ) system

- Google 72量子ビット
- IBM 50量子ビット
- Intel 49量子ビット

ただし，ノイズは大きい

このまま，大規模化が進むのか？

(3) 将来の量子計算機の動向を予測する

Quantum Computing: Progress and Prospects (2018)*

- 大規模でノイズの小さい（誤り訂正機能付き）量子計算機がいつ出来るかの予測をするには早すぎる
  (it is still too early to be able to predict the time horizon for a scalable quantum computer.)
- NISQの開発を当分を目指す．まずは，できるものを作る.
- 商業的に成功すれば，もっと大きい物を目指す

*National Academies of Sciences, Engineering, and Medicine発行
https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects

(1) 量子計算機による素因数分解に関する事実

1. 素因数分解，離散対数問題を多項式時間で解くことができる
2. 実際の回路構成や精密なリソース（量子ビット数，ゲートの個数）はよく理解されている．
   - 素因数分解 (K05, TK08, HRS16)
   - 楕円離散対数問題 (RNSL17)

nビットの素因数分解を行うのに．．．

- 標準的な回路構成では，
  $3n+2$ 量子ビット，$O(n^3)$個の基本ゲート
- 量子ビットを削減した回路では，
  $2n+2$量子ビット，$O(n^4)$個の基本ゲート

（理想的な環境下：誤りは全く無い，各量子ビットは完全結合）

Shorの素因数分解アルゴリズムの概略

戦略：合成数N，自然数aに対して，$a^r = 1 (\mathrm{mod}\ N)$となる最小の自然数 r（位数）を求める，

Step1: 初期状態 |0＞|1＞を構成

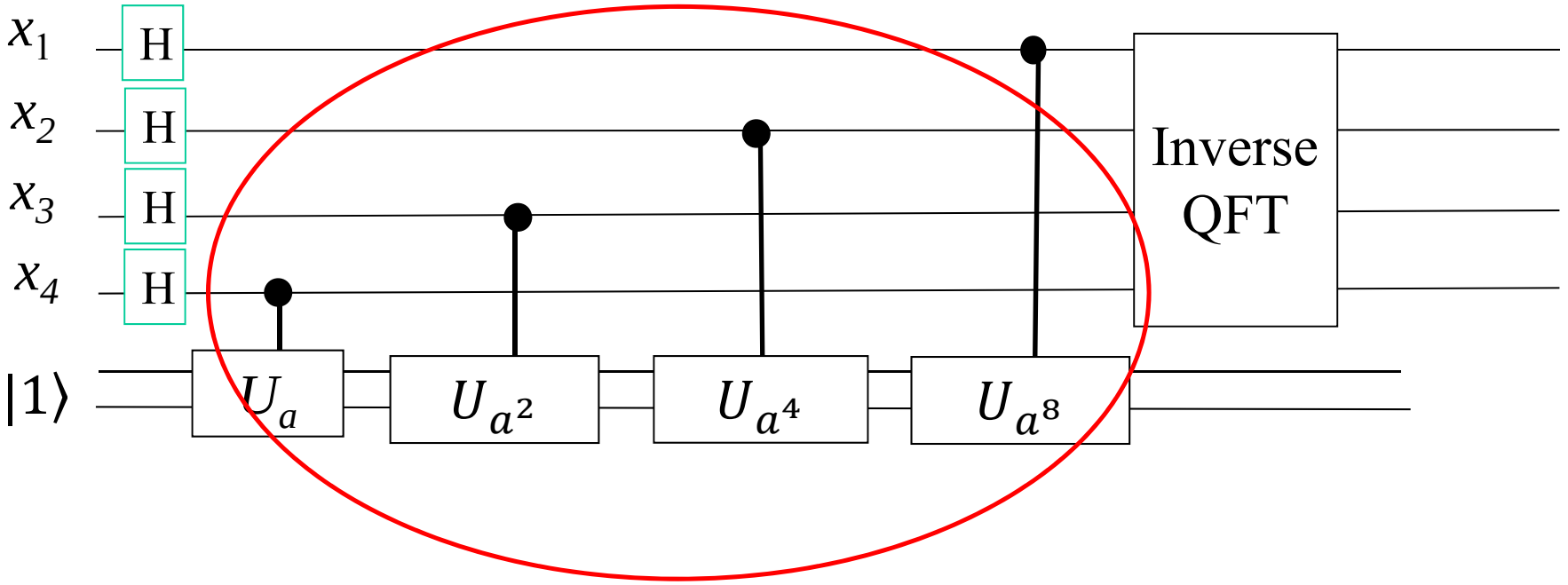
Step2: Hadamard変換を適用 $\rightarrow \frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} |j\rangle |1\rangle$

Step3: べき乗剰余演算を適用 $\rightarrow \frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} |j\rangle |a^j \bmod N\rangle$

Step:4 逆QFTを適用 $\rightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left|\frac{\tilde{s}}{r}\right\rangle |u_s\rangle$

Step5: 第1レジスタを観測：$\rightarrow \frac{\tilde{s}}{r}$

Step6: 連分数展開を行い r を求める.

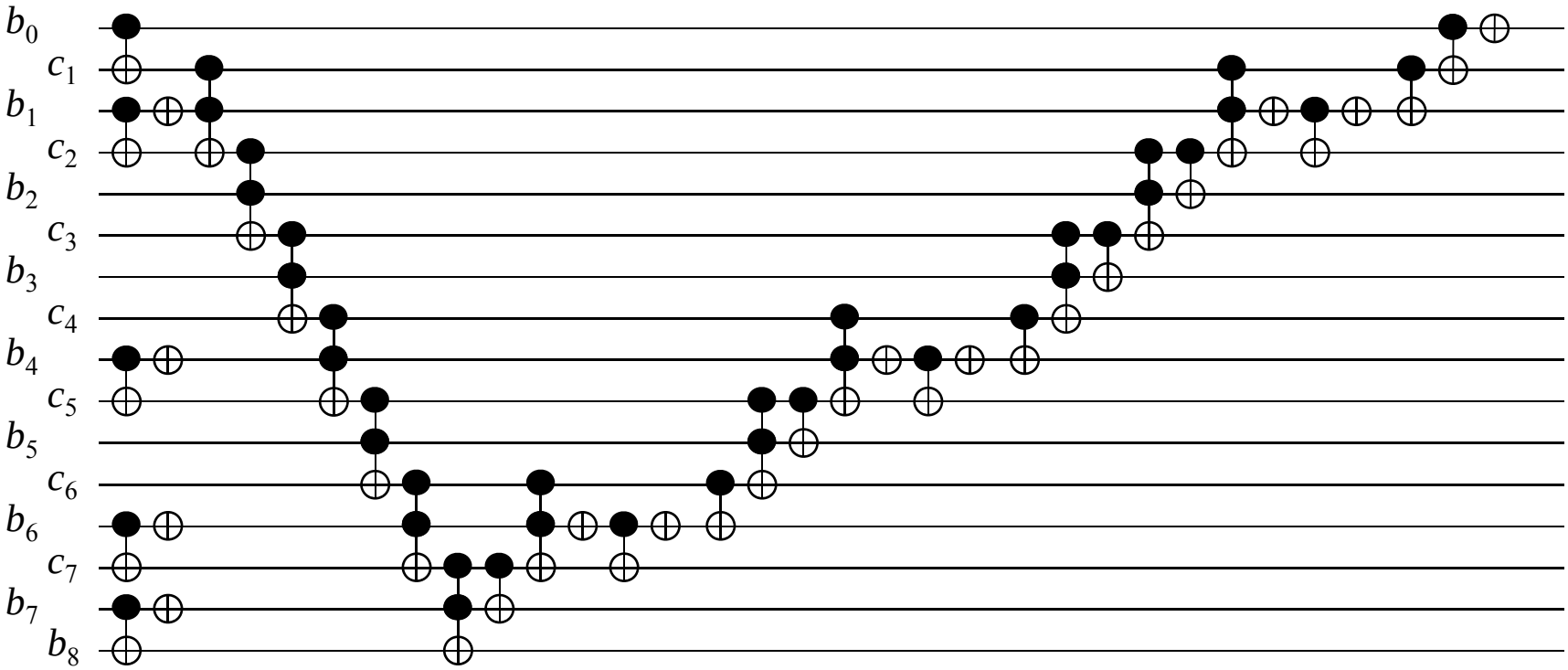


$U_b: |x\rangle \rightarrow |bx \bmod N\rangle$

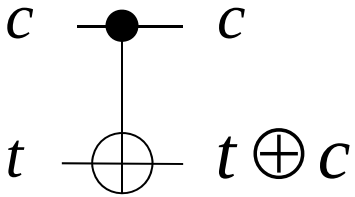
aとkを固定すると，$U_{a^{2^k}}$ は，量子回路で記述可能

回路の(一部分の)例:

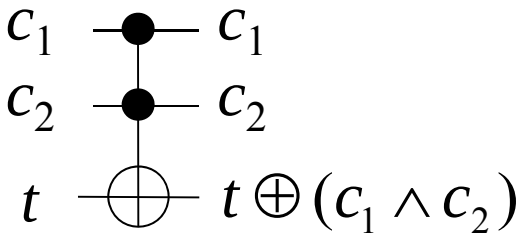
$(11010011)_2$=211の加算



C-NOT gate



Toffoli gate



素因数分解をするのに必要な量子ビット数，ゲート数*

	768ビット合成数		2048ビット合成数	
	# of qubits	# of gates	# of qubits	# of gates
標準的な構成	2306	1.22×10^{11}	6146	3.04×10^{12}
量子ビット削減回路	1539	--	4099	1.35×10^{15}
上記の近似版	1539	8.68×10^{11}	4099	1.22×10^{13}

* N. Kunihiro, “Exact Analysis of Computational Time for Factoring in Quantum Computers,” IEICE Trans. Vol. 88-A, No.1 2005.

- 1500～4000量子ビットが必要
- 10^{11}～10^{13}程度の量子ゲートが必要

ただし，量子誤りが全くないという前提

(2) Shorのアルゴリズムに基づく素因数分解実験

[1] Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance, Nature, 2001.

[2] Shor’s Quantum Factoring Algorithm on a Photonic Chip, Science, 2009.

[3] Computing prime factors with a Josephson phase qubit quantum processor, Nature Physics, 2012.

[4] Realization of a scalable Shor algorithm, Science, 2016.

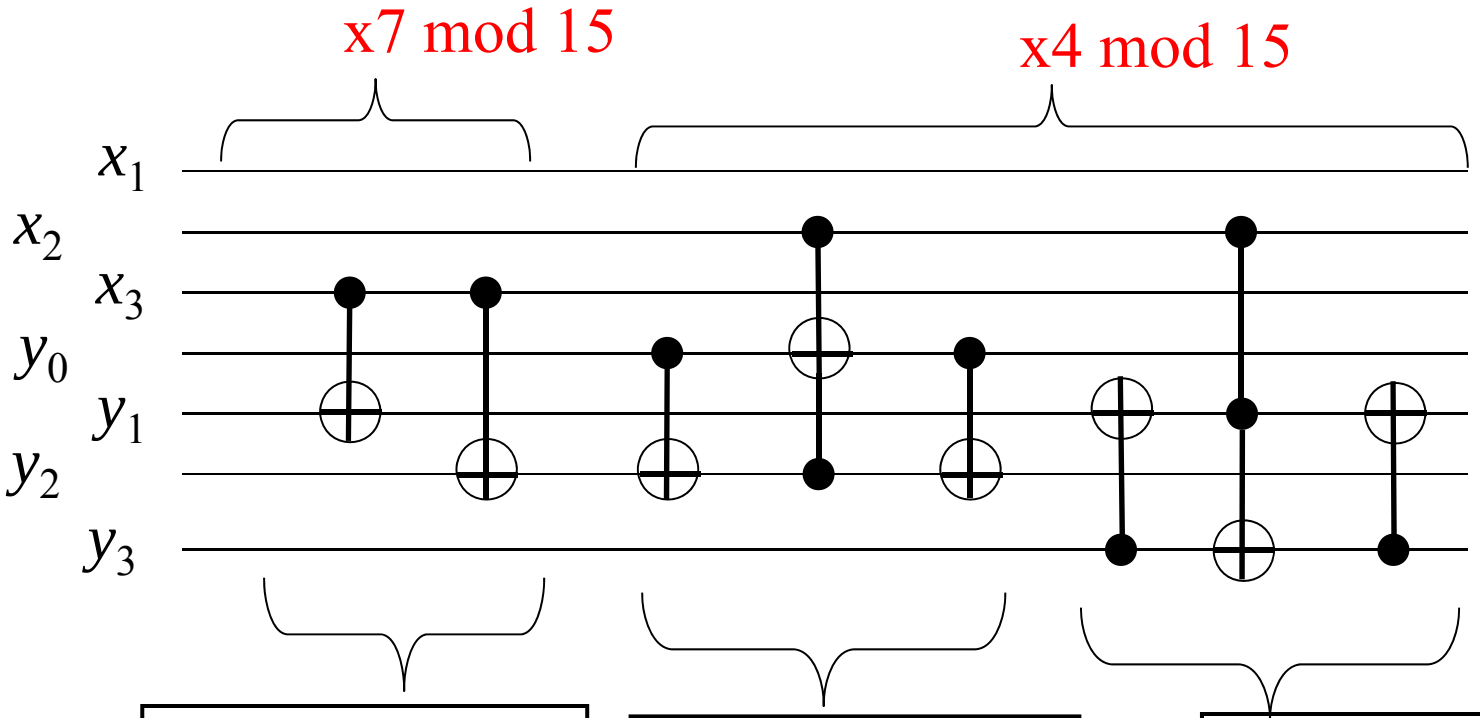
[5] Experimental realisation of Shor’s quantum factoring algorithm using qubit recycling, Nature Photonics, 2012.

Device	研究機関	Year	合成数	Journal
NMR	IBM	2001	15	Nature
Photonic chip	U. of Bristol	2009	15	Science
Superconductivity	UCSB	2012	15	Nature Physics
Ion Trap	U. Innsbruck	2016	15	Science
Photon	U. of Bristol	2012	21	Nature Photonics

- 標準的な回路構成では，10〜14 qubit必要.
- いずれも，かなり少ないqubit数で実験を行っている.
- 汎用的ではない回路構成になっている.

[1]で用いられた回路（IBM, NMR）

$$\frac{1}{\sqrt{2^3}}\sum_{x=0}^{7}|x\rangle|1\rangle \rightarrow \frac{1}{\sqrt{2^3}}\sum_{x=0}^{7}|x\rangle|7^x \bmod 15\rangle$$



この回路は，N=15 であることを利用

1 → x_3==1のとき，1に6を足す
→ x_2==1のとき，$4y \bmod 15$を実行

$y=(y_3 y_2 y_1 y_0)_2$とすると，

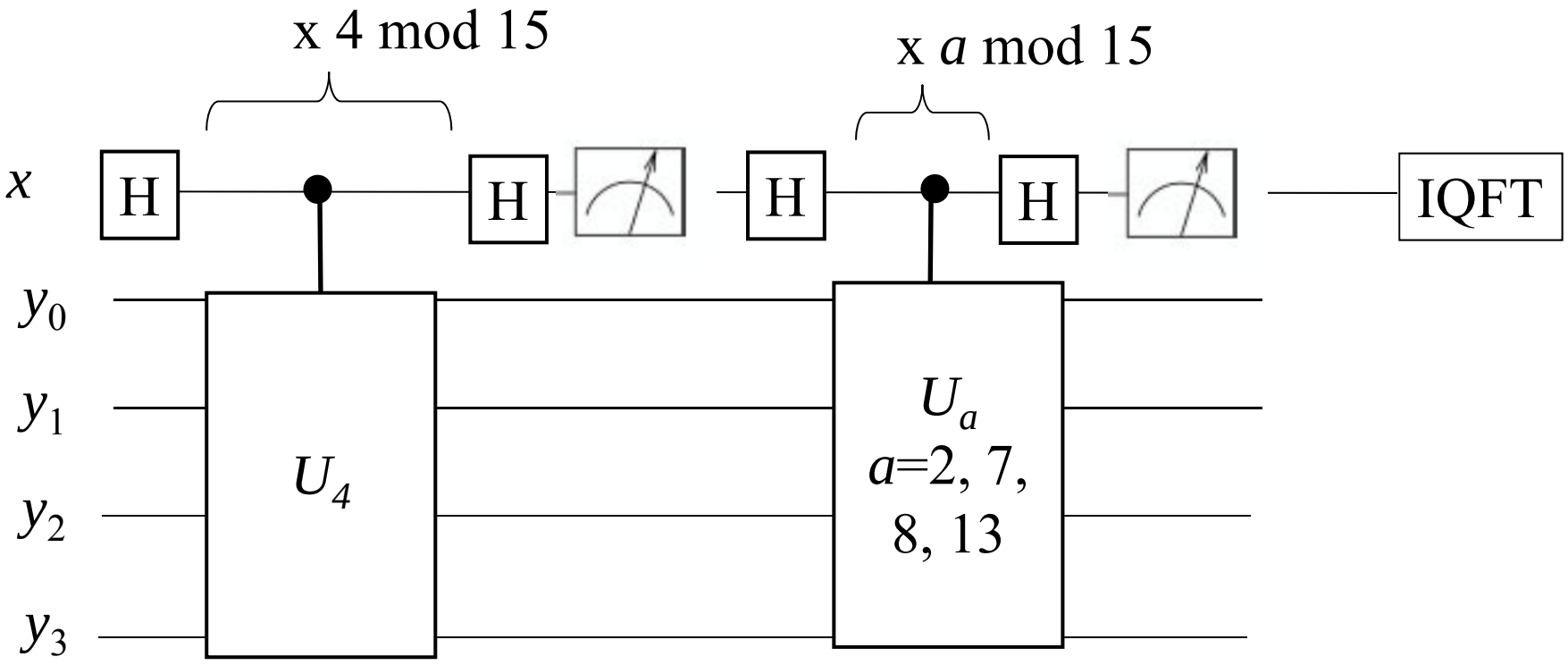
$4y=(y_3 y_2 y_1 y_0 00)_2=16\times(y_3 y_2)_2+(y_1 y_0 00)_2$

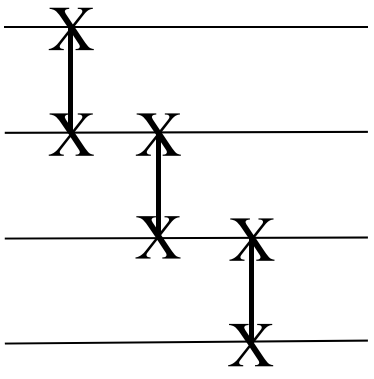
$4y \bmod 15=(y_3 y_2)_2+(y_1 y_0 00)_2=(y_1 y_0 y_3 y_2)_2$

2個のSWAPで実行可能

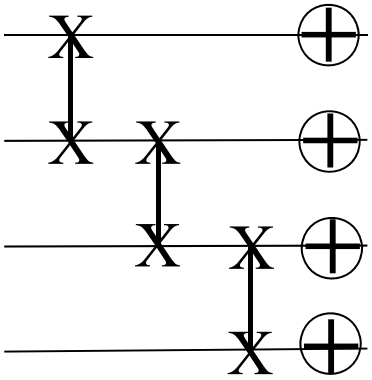
[4]で用いられた回路 (Innsbruck, Ion Trap)

a=2, 7, 8, 13を使用

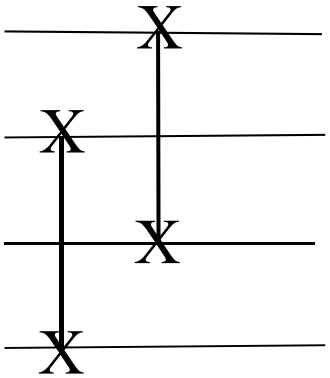




U_2

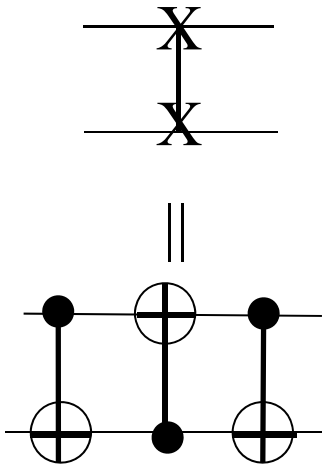


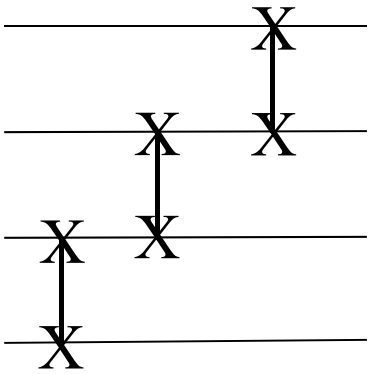
U_{13}



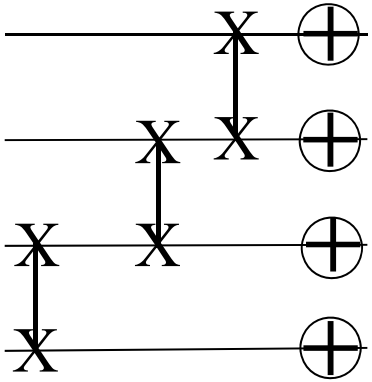
U_4

SWAP

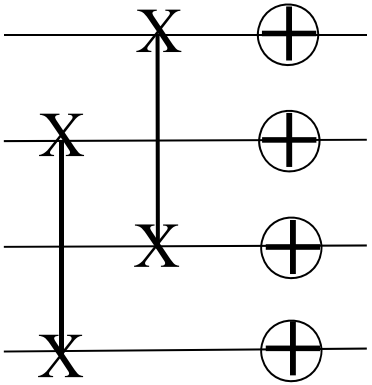




U_8

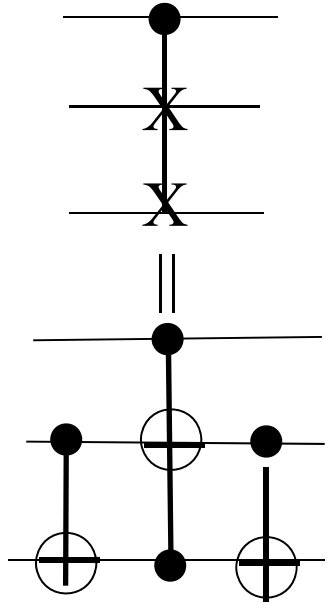


U_7

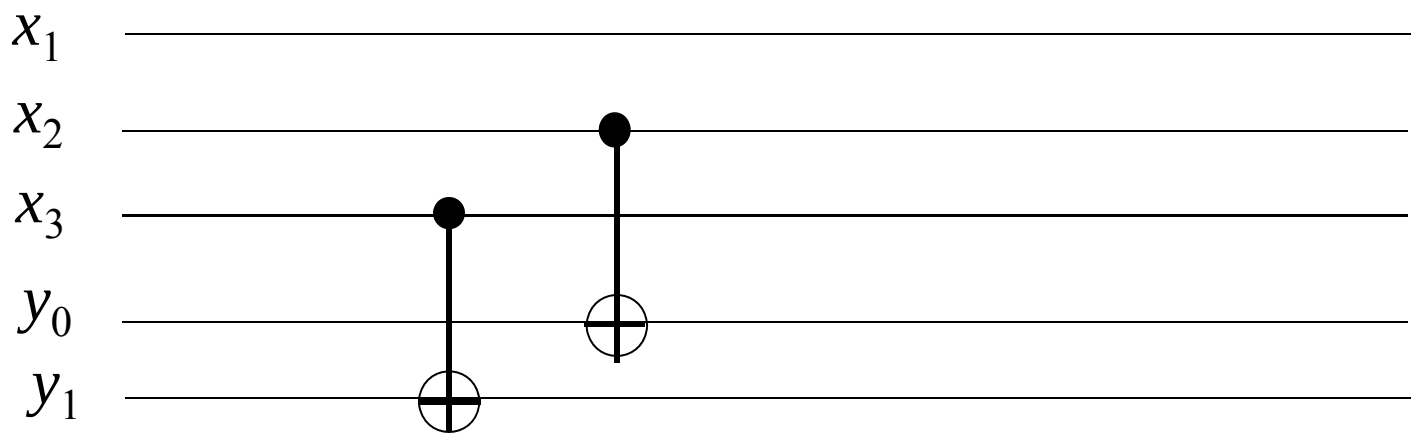


U_{11}

C-SWAP



[2]で用いられた回路 (U. of Bristol, Photonic chip)



a=7を使用

$7^0=1$, $7^1=7$, $7^2=4$, $7^3=13$, $7^4=1$であることを使用

Trick: 以下のencodeを使用

$1\rightarrow (00)_2$, $7\rightarrow (01)_2$, $4\rightarrow (10)_2$, $13\rightarrow (11)_2$.

U_7: $(00)_2\rightarrow (01)_2$, U_4: $(0x)_2\rightarrow (1x)_2$

この回路は，位数が4であるという事実を使いすぎている．
そもそも，Shorのアルゴリズムの目的は位数を求めること．

21の素因数分解実験 [5]

a=4を使用．回路構成において，4の21を法とした位数が3 ($4^3 \bmod 21=1$)であることを使用．

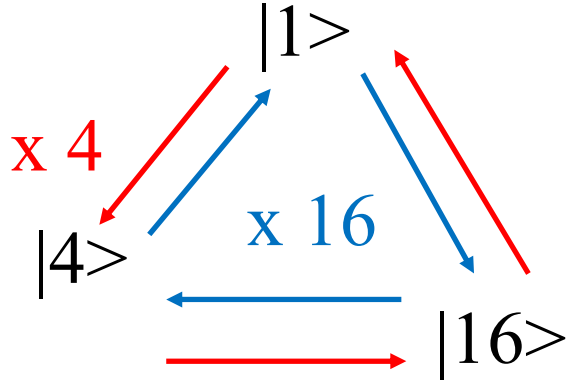
$4^i \bmod 63$ for i=0, 1, 2,… において，1, 4, 16しか現れない

$4^1 \bmod 63 = 4$

$4^2 \bmod 63 = 16$

$4^4 \bmod 63 = 4$

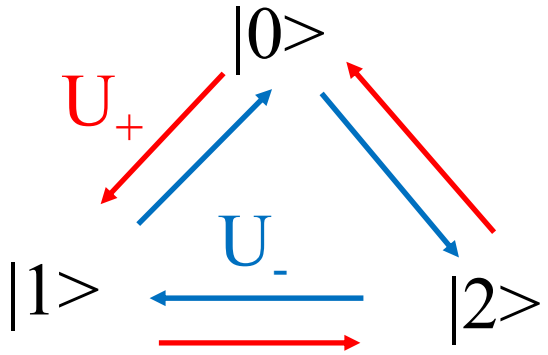
$4^8 \bmod 63 = 16$



符号化：$1 \rightarrow 0, 4 \rightarrow 1, 16 \rightarrow 2$

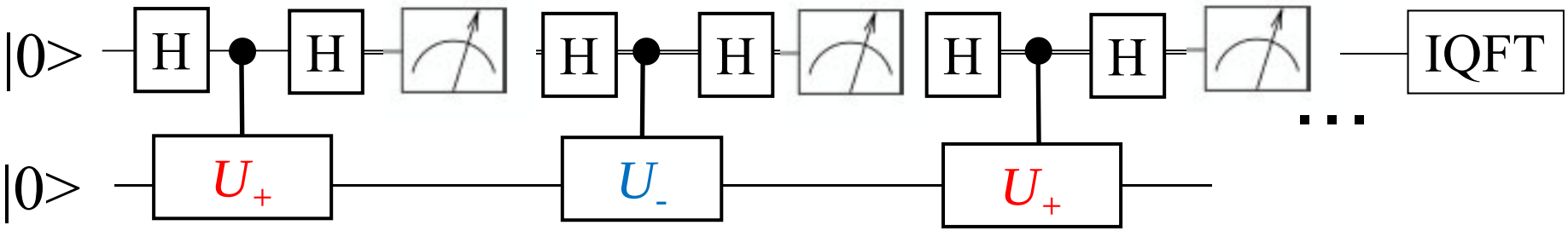
U_+: $|x\rangle \rightarrow |x+1 \bmod 3\rangle$

U_-: $|x\rangle \rightarrow |x-1 \bmod 3\rangle$



qubitではなく，qutrit (=3量子状態を持つ) を利用

実際の回路



回路設計において，位数が3であるという事実を使っている．
しかし，Shorのアルゴリズムの目的は，位数を求めることだった．

[2][5]の回路の一般化

Shorのアルゴリズムのもともとの形

$$\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|1\rangle \rightarrow \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|a^x \bmod N\rangle$$

“simplified” or “compiled”版のShorのアルゴリズム

$$\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|0\rangle \rightarrow \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle|x \bmod r\rangle$$

r は，そもそも計算したかったもの．
Shorのアルゴリズム（の簡略版）としては不適当

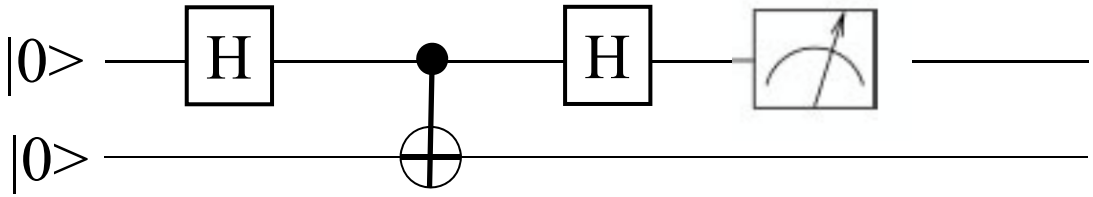
Oversimplifying Quantum Factoring*

*a*を位数2の元とする $(a^2 \bmod N = 1)$

$$\frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle|1\rangle \rightarrow \frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle|a^x \bmod N\rangle$$

“oversimplified”版Shorのアルゴリズム

$$\frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle|0\rangle \rightarrow \frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle|x \bmod 2\rangle$$



- 論文中では，20,000-bit！の素因数分解を示している
- ビットサイズだけを追求しても意味はないことを主張

* A Smolin, John & Smith, Graeme & Vargo, Alexander. (2013). Oversimplifying quantum factoring. Nature. 499. 163-165.

*N, a*の具体的な計算法

SageMathによる実装

```
k=4096
p=random_prime(2^k-1, false, 2^(k-1))
q=random_prime(2^k-1, false, 2^(k-1))
N=p*q
a= crt(1, -1, p, q)
```

計算時間:
2048-bit RSAの場合:一瞬
4096-bit RSAの場合:1秒程度
8192-bit RSAの場合:10秒程度

量子計算機を用いた素因数分解実験の現状把握

- 素因数分解された合成数で最大のものは15
- ただし，「15」であることを利用している．

Quantum Factoringのレベルの提言

Level 1 QF: 位数の情報を回路に組み込む
Level 2 QF: 特殊な合成数だけに有効
Level 3 QF: 全ての合成数に有効

現状では，Level 1とLevel 2の実装のみであり，
Level 3での実装は2019年現在，存在しない．

Quantum Computing: Progress and Prospectsの主張の抜粋（関連部分のみ）

Key Finding 1:
Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm based public key cryptosystems will be built within the next decade.

Key Finding 10:
Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, the hazard of such a machine is high enough - and the time frame for transitioning to a new security protocol is sufficiently long and uncertain - that prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster.

Key Finding 3:
Research and development into practical commercial applications of noisy intermediate scale quantum (NISQ) computers is an issue of immediate urgency for the field. The results of this work will have a profound impact on the rate of development of large-scale quantum computers and on the size and robustness of a commercial market for quantum computers.

Key Finding 4:
Given the information available to the committee, it is still too early to be able to predict the time horizon for a scalable quantum computer. Instead, progress can be tracked in the near term by monitoring the scaling rate of physical qubits at constant average gate error rate, as evaluated using randomized benchmarking, and in the long term by monitoring the effective number of logical (error corrected) qubits that a system represents.

まとめ

量子計算機と暗号技術の関係について整理

(1) 理論的には，多項式時間で解読可能
- 回路構成，必要なリソースもよく知られている

(2) 実際の素因数分解実験を紹介
- いくつかの物は，素因数分解実験としては不適当
- いくつかの物は，ターゲットとする合成数に強く依存
- 汎用的な回路による実験が望ましい

(3) 量子計算機の将来の動向を調査
- 将来を予測することは難しい

- 量子計算機の到来時期を正確に予測できるのは，当分先の話（＝準備をしなくて良いということではない）
- 色々な方面から研究を進める必要がある.

資料4

量子コンピュータ時代に向けた
暗号の在り方検討タスクフォース
令和元年6月24日

耐量子計算機暗号の動向について

高木　剛

東京大学大学院情報理工学系研究科
http://crypto.mist.i.u-tokyo.ac.jp/

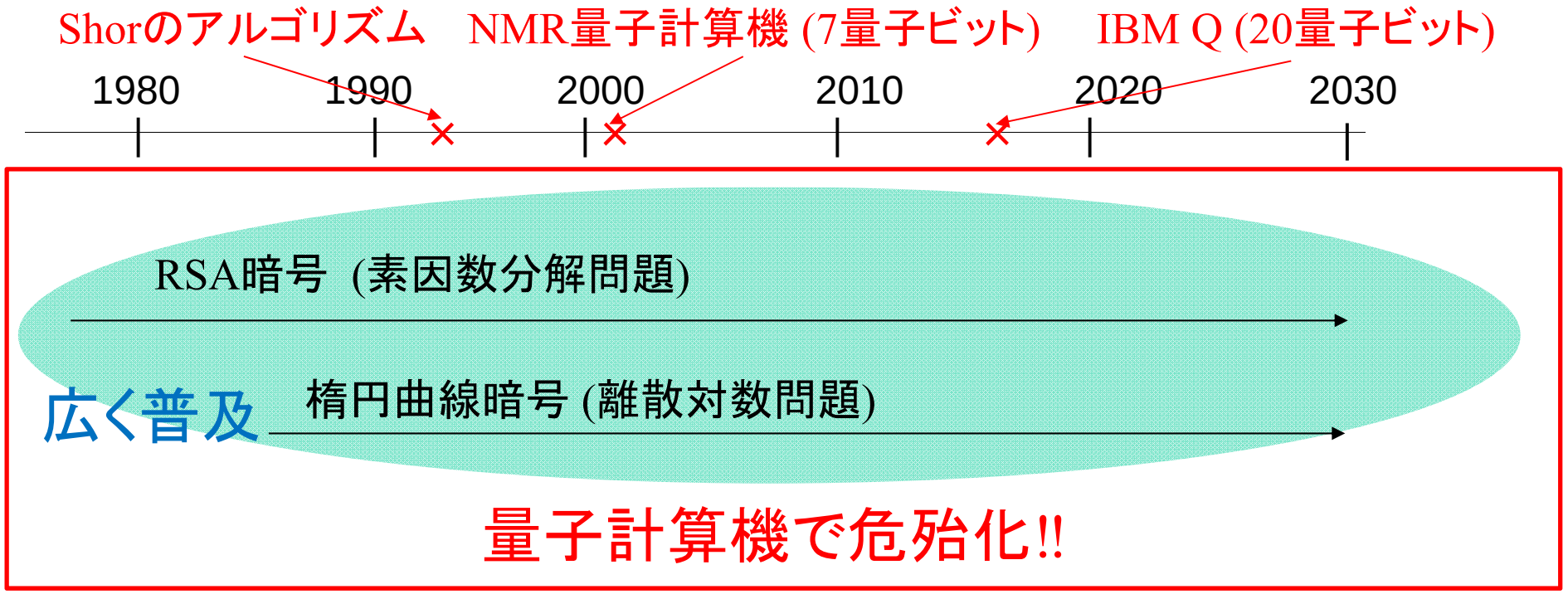
東京大学
THE UNIVERSITY OF TOKYO

講演概要

- 耐量子計算機暗号(PQC)
- NIST PQC標準化
- CRYPTREC における PQC への取り組み
- 暗号の安全性評価方法
- 格子暗号

CRYPTREC暗号技術評価委員会
「耐量子計算機暗号の研究動向調査報告書」
2019年4月5日公開済 https://www.cryptrec.go.jp/

公開鍵暗号の歴史

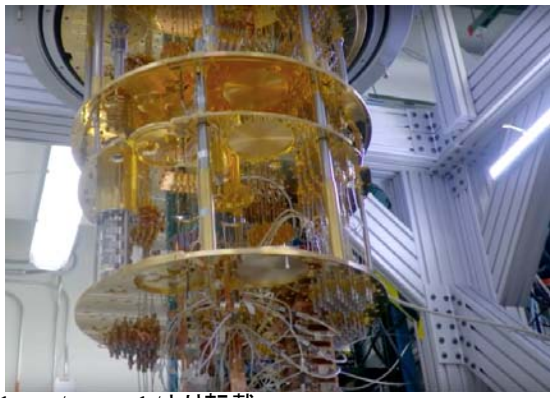


耐量子計算機暗号(PQC)

(格子, 符号, 多変数多項式, ハッシュ関数など)

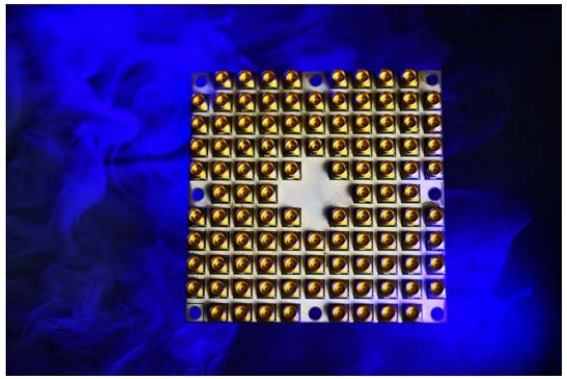
実用化に向けた
研究段階

量子クラウド IBM Q



https://www.research.ibm.com/ibm-q/network/より転載

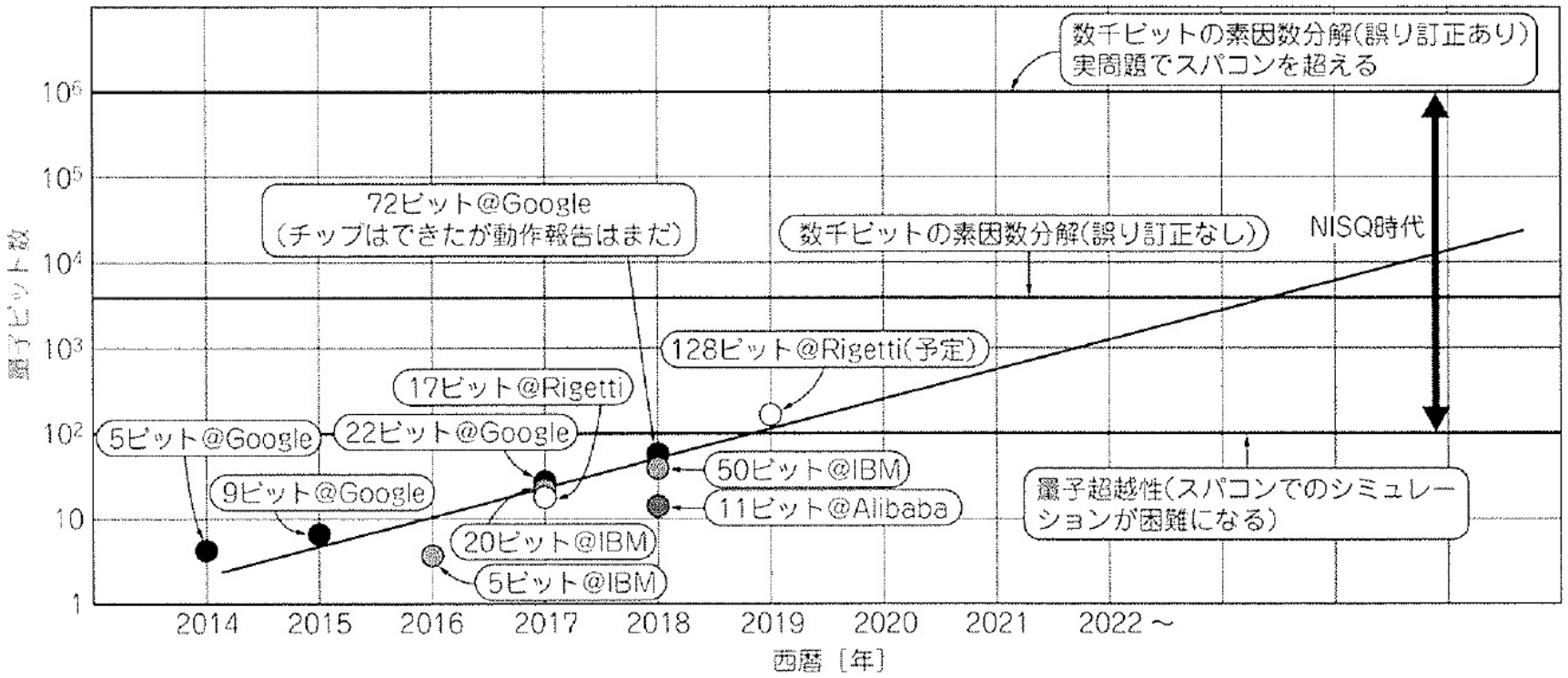
IBM Q、2017年11月、20量子ビットの量子計算機
近い将来に50量子ビットに拡張予定



https://jp.techcrunch.com/2018/03/06/2018-03-05-googles-new-bristlecone-processor-brings-it-one-step-closer-to-quantum-supremacy/より転載
http://www.itmedia.co.jp/news/articles/1801/10/news099.htmlより転載

Google Bristlecone 72量子ビット、Intel Tangle Lake: 49量子ビット

量子コンピュータの規模予測



Interface 2019年 3月号、CQ出版社から転載

東京大学
THE UNIVERSITY OF TOKYO

- 参加者240名(北米80名、欧州60名、アジア60名、日本40名)
- NISTが耐量子計算機暗号の標準化計画を発表した

NIST PQC 標準化計画

http://csrc.nist.gov/groups/ST/post-quantum-crypto/

公開鍵暗号プリミティブを公募(2017年11月30日〆切)

- 鍵交換方式 (SP 800-56 B)
- 暗号化 (SP 800-56 A)
- ディジタル署名 (FIPS PUB 186-4)

公募〆切後、3～5年かけて安全性と効率性を評価する。

利用される数学問題

- 格子暗号 (Lattice-based cryptography)
- 符号暗号 (Code-based cryptography)
- 多変数多項式暗号 (Multivariate polynomial cryptography)
- ハッシュ関数署名 (Hash-based signature)
- 同種写像暗号 (Isogeny-based cryptography)

2017年12月応募状況 (69件)

- **格子暗号 (24件)**

Compact LWE, CRYSTALS-DILITHIUM, CRYSTALS-KYBER, Ding Key Exchange, DRS, EMBLEM and R.EMBLEM, FALCON, Frodo, HILA5, KINDI, LAC, LIMA, Lizard, LOTUS, NewHope, NTRU-HRSS-KEM, NTRU Prime, NTRUEncrypt, Odd Manhattan, pqNTRUSign, qTESLA, Round2, SABER, Titanium

- **符号暗号 (16件)**

BIG QUAKE, BIKE, Classic McEliece, DAGS, Edon-K, HQC, LEDAkem, LEDApkc, McNie, NTS-KEM, pqsigRM, QC-MDPC KEM, RaCoSS, Ramstake, RLCE-KEM, RQC

- **多変数多項式暗号 (10件)**

CFPKM, DME, DualModeMS, GeMSS, Gui, HiMQ-3, LUOV, MQDSS, Rainbow, SRTPI

- **ハッシュ関数署名 (2件)**

Gravity-SPHINCS, SPHINCS+

- **同種写像暗号 (1件)**

SIKE

- **その他 (16件)**

Giophantus, Guess Again, HK17, LAKE, Lepton, LOCKER, Mersenne-756839, OKCN/AKCN/CNKE, Ouroboros-R, Picnic, Post-quantum RSAEncryption, Post-quantum RSASignature, RankSign, RVB, Three Bears, WalnutDSA

2019年1月から第2ラウンド (26件)

格子暗号	
	鍵交換・暗号化 (9方式): CRYSTALS-KYBER, Frodo-KEM, LAC, NewHope, NTRU, NTRU Prime, Round5, SABER, Three Bears ディジタル署名 (3方式): CRYSTALS-DILITHIUM, FALCON, qTESLA
符号暗号	
	鍵交換・暗号化 (7方式): BIKE, Classic McEliece, HQC, ROLLO, LEDAenc, NTS-KEM, RQC
多変数多項式暗号	
	ディジタル署名 (4方式): GeMSS, LUOV, MQDSS, Rainbow
ハッシュ関数署名	
	ディジタル署名 (1方式): SPHINCS+
同種写像暗号	
	鍵交換・暗号化 (1方式)：SIKE
その他	
	ディジタル署名 (1方式)： Picnic

NIST PQC 標準化スケジュール

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline

- 2017年12月～2018年12月: 第1ラウンド評価期間
- 2019年1月: 第2ラウンド選出暗号発表
- 2019年～2020年: 第2ラウンド評価期間
- 2020年/2021年: 最終候補選出 or 第3ラウンド開始
- 2022年/2024年: 標準規格ドラフト
- 2030年まで SP 800-56, FIPS PUB 186-4を利用可能

2030年の移行問題

耐量子計算機暗号を利用？
RSA暗号の鍵長を伸ばして利用？

x **2030年: RSA暗号(2048ビット)の使用終了**

耐量子暗号への移行期間

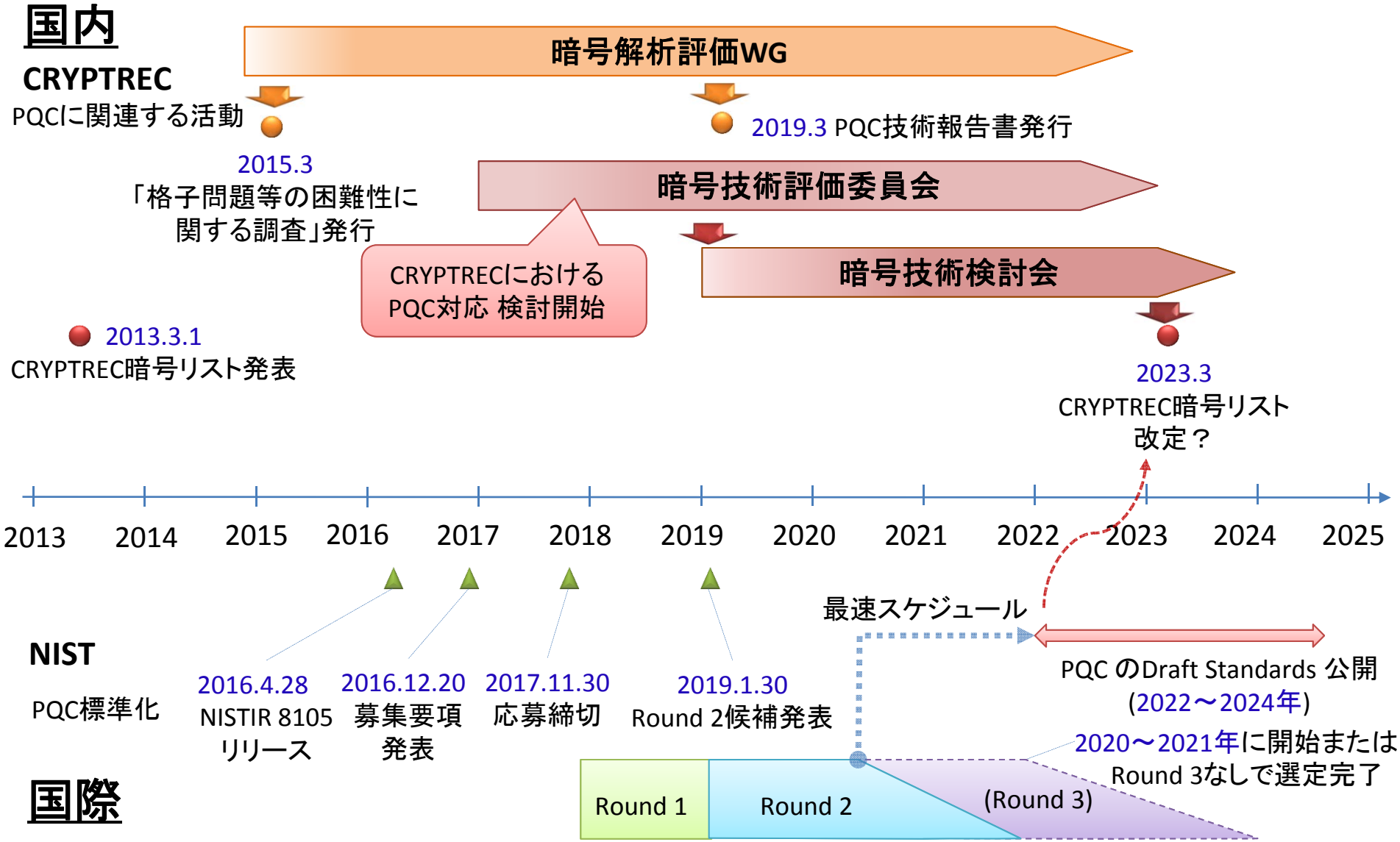
x 2022年-2024年: 耐量子計算機暗号の標準規格ドラフト

x 2020年: 最終候補選定または第3ラウンド開始

x 2019年8月: 第2回NIST PQC標準化会議

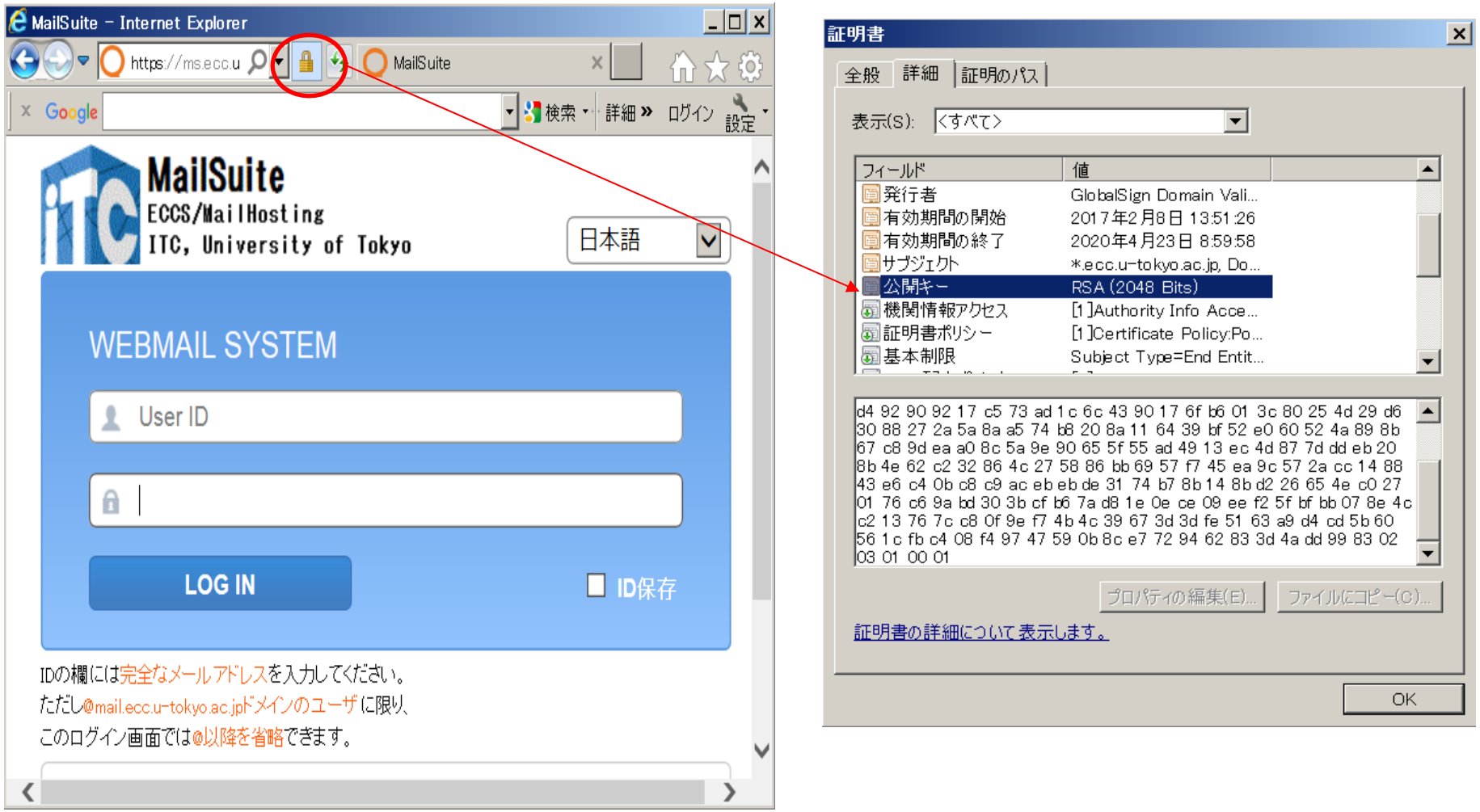
東京大学
THE UNIVERSITY OF TOKYO

PQC標準化をめぐる国内外の動き



東京大学
THE UNIVERSITY OF TOKYO

RSA暗号の公開鍵

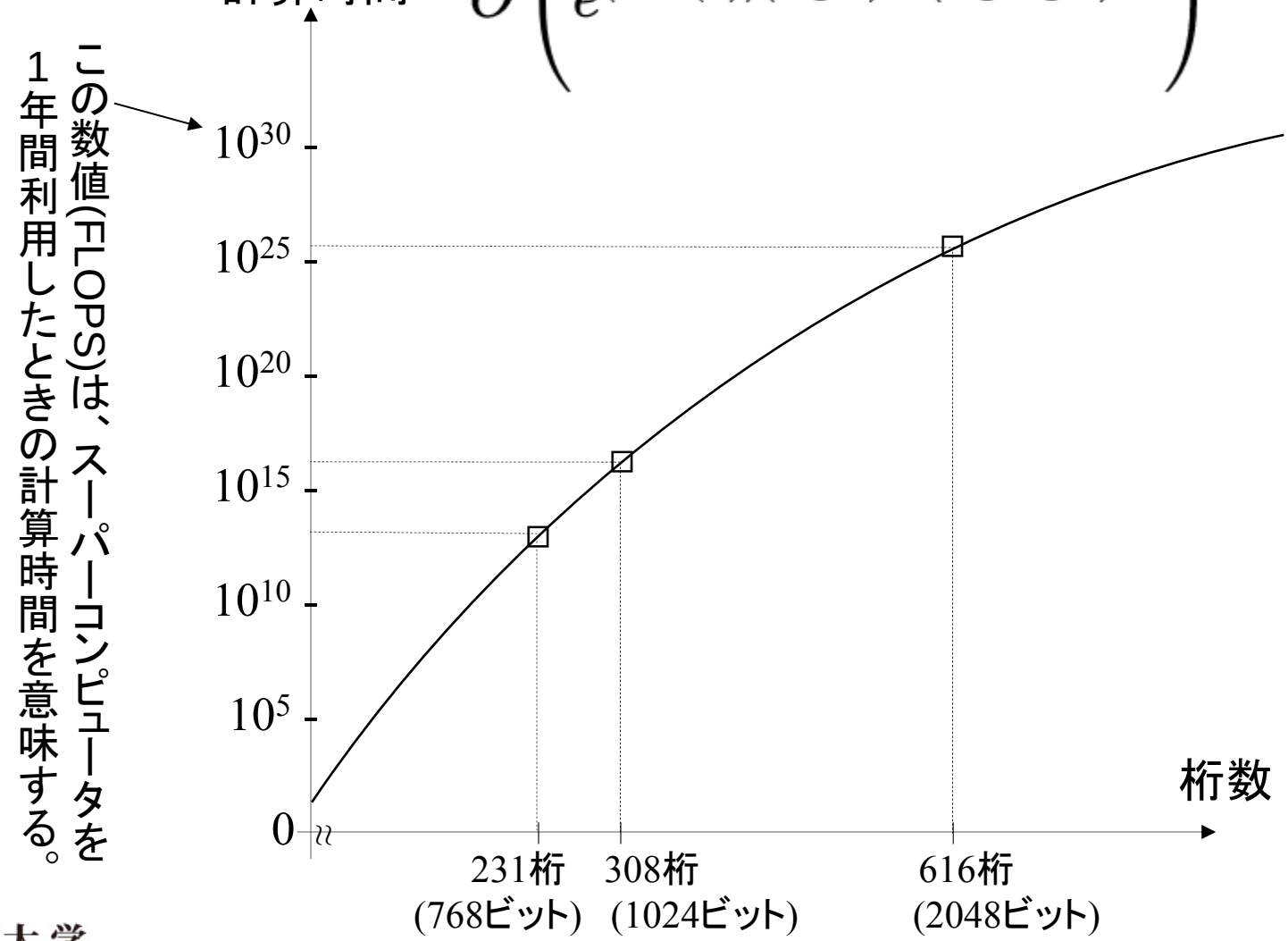

MailSuite – Internet Explorer
https://ms.ecc.u
MailSuite
Google
検索
詳細 »
ログイン
設定
MailSuite
ECCS/MailHosting
ITC, University of Tokyo
日本語
WEBMAIL SYSTEM
User ID
LOG IN
ID保存
IDの欄には完全なメールアドレスを入力してください。
ただし@mail.ecc.u-tokyo.ac.jpドメインのユーザに限り、
このログイン画面では@以降を省略できます。
証明書
全般
詳細
証明のパス
表示(S): <すべて>
フィールド
値
発行者
GlobalSign Domain Vali...
有効期間の開始
2017年2月8日 13:51:26
有効期間の終了
2020年4月23日 8:59:58
サブジェクト
*.ecc.u-tokyo.ac.jp, Do...
公開キー
RSA (2048 Bits)
機関情報アクセス
[1]Authority Info Acce...
証明書ポリシー
[1]Certificate Policy:Po...
基本制限
Subject Type=End Entit...
d4 92 90 92 17 c5 73 ad 1c 6c 43 90 17 6f b6 01 3c 80 25 4d 29 d6
30 88 27 2a 5a 8a a5 74 b8 20 8a 11 64 39 bf 52 e0 60 52 4a 89 8b
67 c8 9d ea a0 8c 5a 9e 90 65 5f 55 ad 49 13 ec 4d 87 7d dd eb 20
8b 4e 62 c2 32 86 4c 27 58 86 bb 69 57 f7 45 ea 9c 57 2a cc 14 88
43 e6 c4 0b c8 c9 ac eb eb de 31 74 b7 8b 14 8b d2 26 65 4e c0 27
01 76 c6 9a bd 30 3b cf b6 7a d8 1e 0e ce 09 ee f2 5f bf bb 07 8e 4c
c2 13 76 7c c8 0f 9e f7 4b 4c 39 67 3d 3d fe 51 63 a9 d4 cd 5b 60
56 1c fb c4 08 f4 97 47 59 0b 8c e7 72 94 62 83 3d 4a dd 99 83 02
03 01 00 01
プロパティの編集(E)...
ファイルにコピー(C)...
証明書の詳細について表示します。
OK

RSAチャレンジ問題の解読記録推移

解読達成日	解読桁長	計算時間(パソコン1台換算)
1991年4月	100桁 (330ビット)	
1993年6月	120桁 (397ビット)	
1996年4月	130桁 (430ビット)	約7年 (1500 MIPS年)
1999年2月	140桁 (463ビット)	
1999年8月	155桁 (512ビット)	約36年 (8000 MIPS年)
2003年12月	174桁 (576ビット)	
2005年5月	200桁 (663ビット)	約55年 (Opteron 2.2 GHz)
2009年12月	231桁 (768ビット)	約1500年 (Opteron 2.2 GHz)
未解読	308桁 (1024ビット)	
未解読	616桁 (2048ビット)	

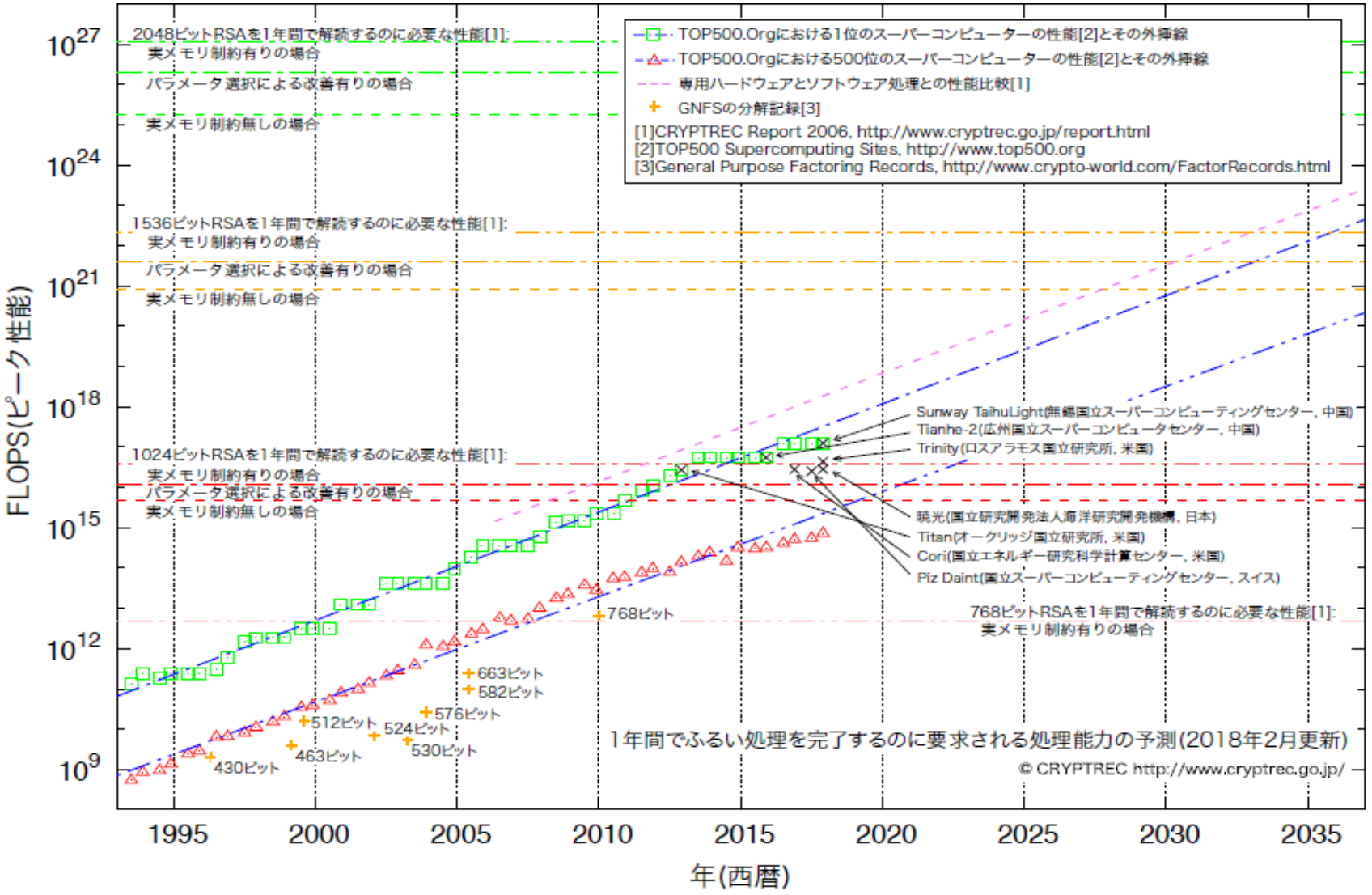
数体篩法

計算時間 $O\left(e^{(c+o(1))(\log n)^{\frac{1}{3}}(\log\log n)^{\frac{2}{3}}}\right)$



東京大学 THE UNIVERSITY OF TOKYO

素因数分解の困難性に関する計算量評価

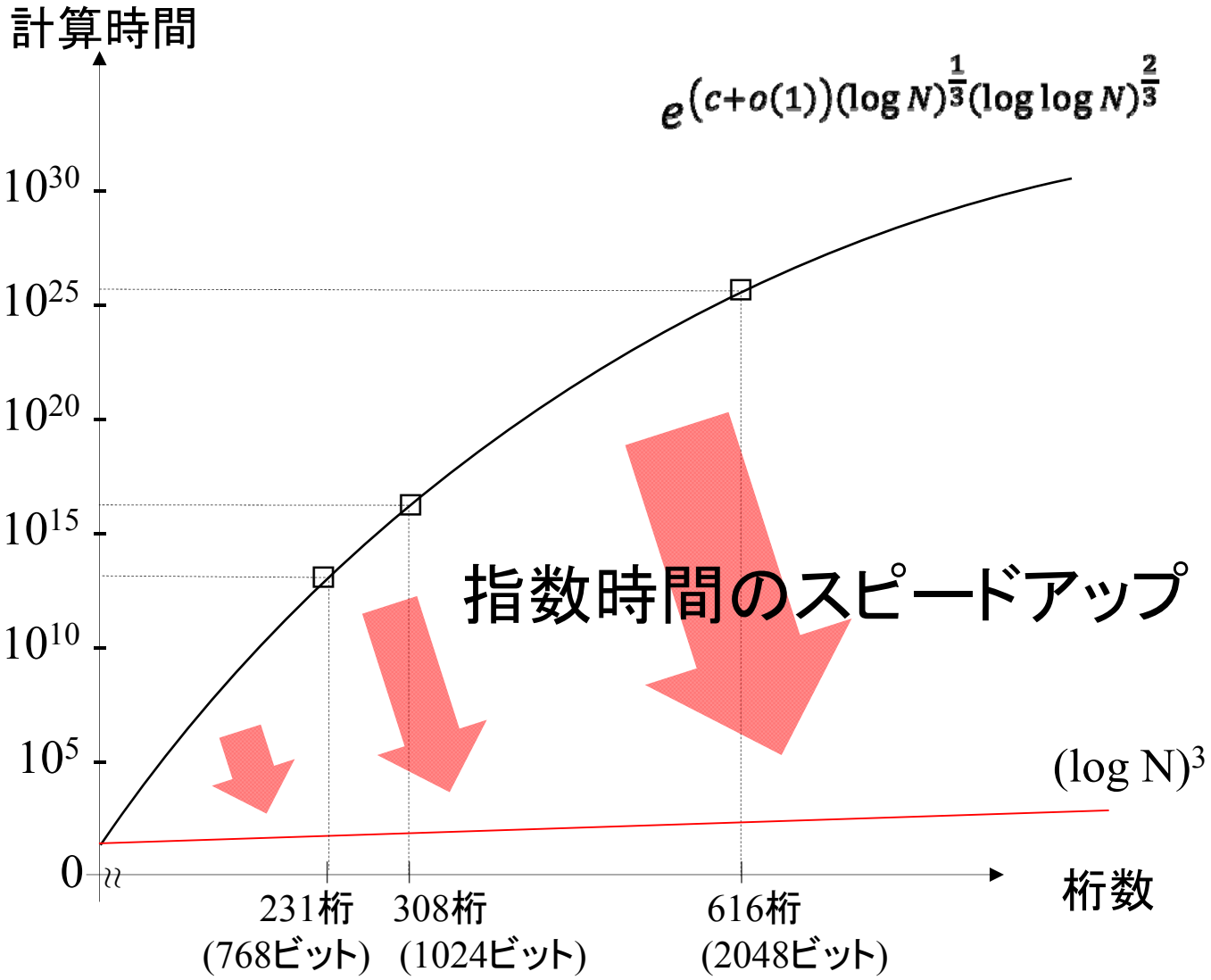


(http://www.cryptrec.jp/)

図 1：素因数分解の困難性に関する計算量評価

1 年間でふるい処理を完了するのに要求される処理能力の予測、2018 年 2 月更

量子コンピュータによる素因数分解



東京大学
THE UNIVERSITY OF TOKYO

格子暗号

ノイズ付き連立一次方程式 (LWE問題)

・連立一次方程式: 容易に解が求まる

$$\begin{cases} 2x - 3y = 0 \\ -x + 2y = 1 \end{cases}$$

・ノイズ付き連立一次方程式: 解を求めるのは困難

$$\begin{cases} 2x - 3y + e_1 = 0 \\ -x + 2y + e_2 = 1 \end{cases}$$

e_1, e_2 : ノイズ

(次元 or ノイズ: 増加させると)

LWE問題は計算が困難となる

NIST PQC 第2ラウンド
格子暗号の技術分類

分類		公開鍵暗号・鍵交換方式	ディジタル署名
NTRU暗号系		NTRU, NTRU Prime	FALCON
LWE問題系	LWE問題	Frodo-KEM	-
	Ring-LWE問題	NewHope	qTESLA
	Module-LWE問題	CRYSTALS-KYBER	CRYSTALS-DILITHIUM
	LWR問題	Round5, SABER	-
	他のLWE問題	LAC, Three Bears	-

ダルムシュタットLWE問題チャレンジ

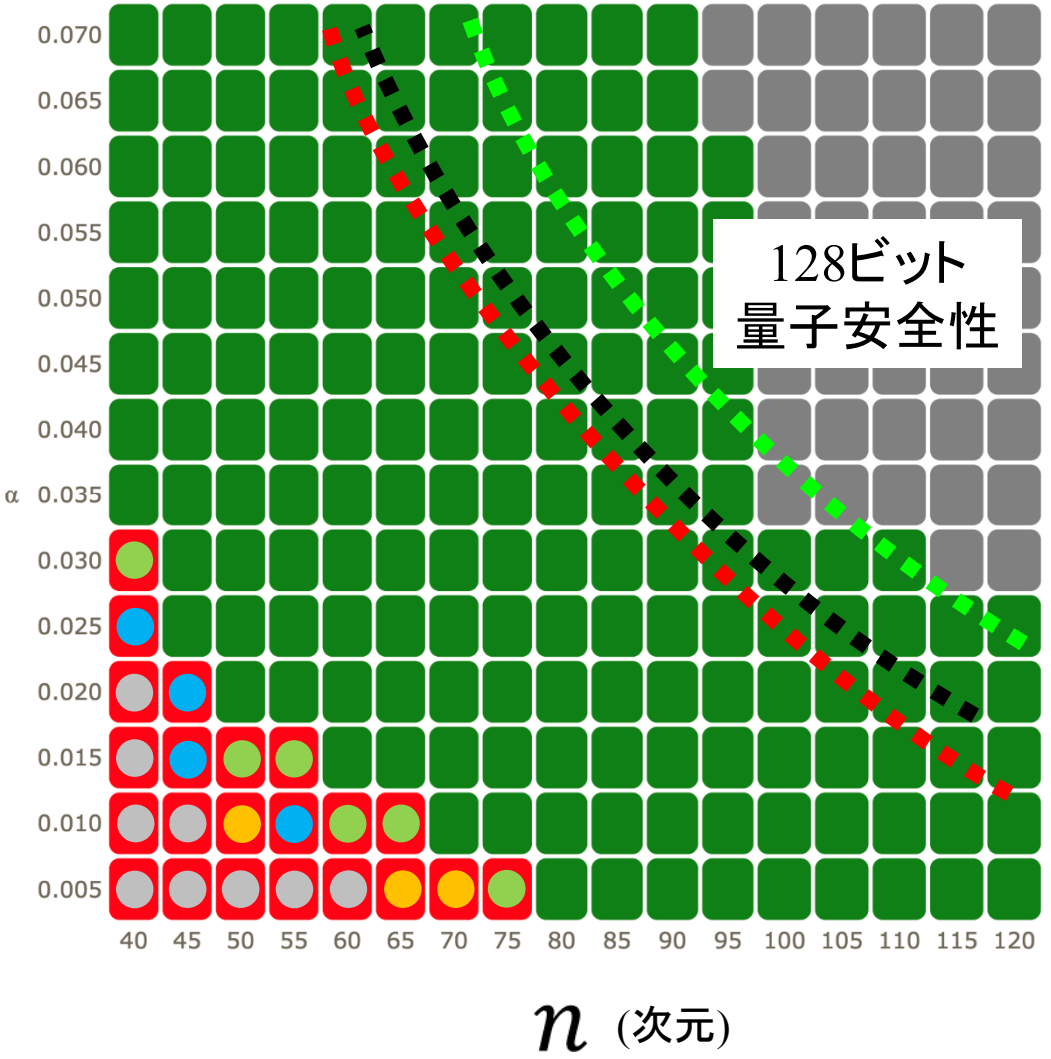
$\alpha = \sigma/q$ (ノイズ)

2018-19: G6K algorithm (部分篩法)
+ 埋め込み法
(Albrecht, Ducas, Herold, Kirshanova, Postlethwaite, Stevens)

2017: RSR algorithm + 埋め込み法
(柏原, 照屋)

2016: Progressive-BKZ algorithm
+ 埋め込み法
(王, 青野, 林, 高木)

2016: BKZ 2.0 algorithm
+ 最近平面法
(Xui, 福島, 清元, 高木)



東京大学
THE UNIVERSITY OF TOKYO

まとめ

- 耐量子計算機暗号の最新動向

  米国標準技術研究所NISTによる標準化計画

  CRYPTRECにおける PQCへの取り組み

- 格子暗号

  ダルムシュタットLWE問題チャレンジ

CRYPTREC暗号技術評価委員会
「耐量子計算機暗号の研究動向調査報告書」
2019年4月5日公開済 https://www.cryptrec.go.jp/

参考資料

（平成 31 年３月 29 日　暗号技術検討会　資料５）

次期 CRYPTREC 暗号リストの改定に向けた議論について

現在の CRYPTREC 暗号リストの策定（2013 年 3 月 1 日）から６年が経過することや、量子コンピュータの動向や新たな暗号技術の動向等を踏まえ、次期 CRYPTREC 暗号リストの改定に向けて、CRYPTREC 事務局で作成した改定方針等の素案について、暗号技術評価委員会及び暗号技術活用委員会でいただいたご意見を紹介する。

次期 CRYPTREC 暗号リストについて（CRYPTREC 事務局において作成した素案）

1 改定方針

- 【改定時期】現在の CRYPTREC 暗号リストは 2013 年 3 月 1 日に改定されており、改定より 10 年後の 2023 年 3 月の改定を目指して検討を開始する。
- 【リスト構成】現在の「電子政府推奨暗号リスト」「推奨候補暗号リスト」「運用監視暗号リスト」から大幅見直しは行わない。
- 【暗号公募について】一般への暗号公募は行わない。
- 【新たに追加する暗号技術の候補について】主として標準化動向をもとに事務局で選出を行い、暗号技術検討会で審議の上決定する。学会に提案されている新たな暗号技術については、仕様、安全性評価、知的財産権、調達可能性等の観点で問題ないと判断できれば候補になりうる。
- 【暗号技術評価委員会の役割】暗号技術評価委員会では、安全性評価および実装評価を行う。評価対象は新たに追加する暗号技術の候補のみとする。現リストに掲載されている暗号技術については安全性監視を継続しており、改めて評価を行うことはしない。
- 【暗号技術活用委員会の役割】暗号技術活用委員会では、利用実績調査を行う。
- 【選考基準について】選考基準は 2021 年度までに両委員会で議論の上、暗号技術検討会で決定する。

2 耐量子計算機暗号への対応

- 次期 CRYPTREC 暗号リストへの反映
  - 2022 年度開始までに NIST PQC 標準化で選定された方式を、新たに追加する暗号技術の候補の参考とする。
  - Hash-based signature については IETF 標準をベースに新たに追加する暗号技術の候補の参考とする。
- PQC への移行計画策定については、その時期を含めて NISC でご検討頂く。
- RSA-2048 からの移行については既に始まっているところもあり、何をすべきか議論を開始する。

3 軽量認証暗号・軽量ハッシュ関数への対応

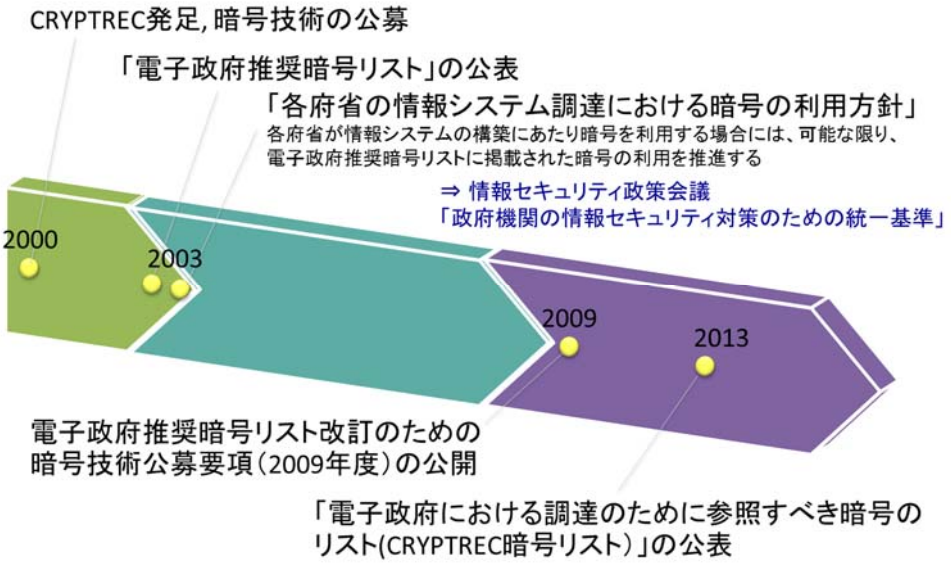
- 次期 CRYPTREC 暗号リストへの反映
  - 2022 年度開始までに NIST 軽量暗号標準化で選定された方式を、新たに追加する暗号技術の候補の参考とする。
    - NIST 軽量暗号標準化
      軽量認証暗号と軽量ハッシュ関数のみ(2019.2.25 応募締切、2-4 年後完了)
      “some algorithms could be selected for standardization after two to four years”

4 その他

次期 CRYPTREC 暗号リストの改定に向けて議論すべき項目は何か、追加・削除を検討すべき技術分類はあるか。

例)

- 64 ビットブロック暗号の利用について
- 64 ビットブロック暗号を安全に利用するための暗号利用モード
- 現リストに掲載されている暗号技術に対する量子計算機の影響
  (鍵長、パラメータ等)
- 秘密分散(ISO/IEC 19592) や準同型暗号(ISO/IEC 18033-6)など



図：これまでの電子政府推奨暗号リストおよび CRYPTREC 暗号リストの改定の流れ

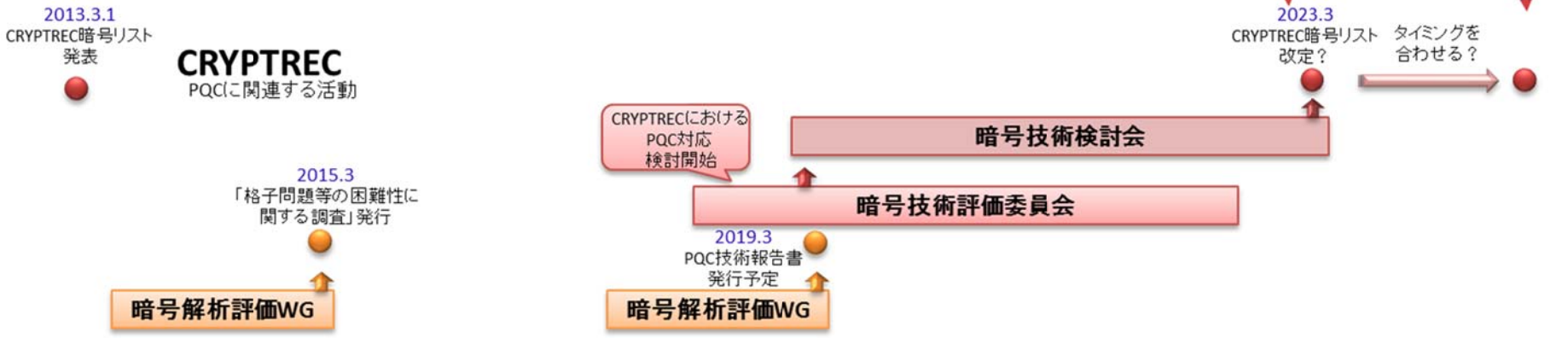
参考：PQC標準化をめぐる国内外の動き

国際

ISO/IEC SC27 WG2 SD8 (Post-Quantum Cryptography)

Asia Asia PQC Forum

EU H2020 ECRYPT
PQCRYPTO
ETSI Quantum-Safe Cryptography



国内

暗号技術評価委員会（2018 年 7 月 19 日、2019 年 3 月 11 日開催）で頂いた主な意見

● 「耐量子計算機暗号について」

- 量子計算機の性能については、不確定要素が多いことから、予想通りには進展しないかもしれないが、進展した場合に備えて暗号技術評価委員会で PQC に関する技術的な検討を行う必要がある。
- PQC への移行計画を考えるのは時期尚早であろう。また、簡単ではない。
- PQC への移行について、複数の方式を対応する「暗号 Agility」の考え方で対応が検討されている。

● 「RSA-2048 からの移行について」

- PQC への移行以前に、RSA-2048 からの移行問題が先にあり、20 年という期間の対応が求められている認証局ではすでに移行が始まっている。それは電子政府関係も無縁ではない。例えば電子パスポートについては、国際的な観点から ICAO の動きに対応して移行が検討されている。ICAO 仕様のルート証明書に ECDSA が含まれている。

● 「量子コンピュータの共通鍵暗号への影響について」

- 共通鍵暗号分野においても、量子計算機による影響について適切に監視する必要がある。

● 「軽量暗号について」

- NIST では軽量暗号の認証暗号やハッシュ関数の標準化公募を始めようとしている。2023 年のリスト改定に向けては、PQC だけではなく軽量暗号のことも考えておいた方が良い。
- 軽量暗号技術は、その性質上、セキュリティマージンを厳しく設定していることが多く、一般的な実装とは思想的に違う位置づけになるのかもしれない。64 ビットブロック暗号も多いということから、CRYPTREC 暗号リストの枠組みとの整合性を整理した上でリストの改定にのぞむべきである。
- NIST の公募と CRYPTREC における軽量暗号の範囲との関係を整理する必要がある。

● 「CRYPTREC 暗号リスト（の改定）について」

- 次期 CRYPTREC 暗号リストの改定方針について議論する前に、そもそも次期リストに求める要件を明確にする必要がある。
- リストの構成は、このままでよいのかという点を改めて議論してもよいと思われる。
- 産業界や政府、NISC などにヒアリングして、これまで CRYPTREC がどのように役に立ってきたのかを確認してはどうか。その際に、従来の暗号技術の評価と監視だけではなく、別の役割を求められているのならそれを含めて検討した方が良い。

暗号技術活用委員会（2019 年 3 月 14 日開催）で頂いた主な意見

- **「改定方針を前提とするのではなく、リストの位置づけから根本的に見直したほうがよい」**

- 改定方針には、暗号そのものを考える暗号アルゴリズムに閉じた世界ではなくて、今後どうやって暗号を使ってもらうのかということが盛り込まれていて欲しい。
- 他の政策テーマやアーキテクチャなどの連携との関連性を整理して暗号リストを位置づけてもらいたい。何のための暗号リストなのかの大方針を明確にすべきである。
- 現在リストが 3 個あるが、その形態が妥当であるかについても考える必要がある。

- **「次の暗号アルゴリズムの移行に向けて政策的な議論をする場が必要である」**

- 前回（RSA1024 から RSA2048 への移行）は移行のためのリソースや体制等があり業界全体が一致して動いたが、今はそれだけのリソースも体制もない。資金手当てを含めた政策的な誘導がないと移行が進まないし、時間もかかると思われる。
- PQC への移行は相当困難である。暗号技術活用委員会としては、暗号を移行できる（暗号アジリティ(Crypto-agility)を持った)システムを作らせるという活動をすべきである。PQC への移行を考える前に、暗号を移行できるシステムを作るということを念頭においた活動を行わないと、現実的には PQC への移行は破綻するのではないかと思われる。
- RSA2048 から（PQC ではなく、より強度が高い公開鍵暗号）の移行が、少なくともルート認証局では始まっており、新しく建てるルート認証局では RSA2048 はなくなりつつあると思われるので、実態調査を実施した方がよい。
- スマホでどの程度の強度の暗号がハードウェアでサポートされているのかなど、RSA2048 よりも強度の高いアルゴリズムがどのように使われるか、今現在使えるのか、といった点について、実態調査を実施した方がよい。
- RSA2048 からの移行は直近に移行完了させなければならない課題ではないので、無理なく暗号を移行できるために必要なプロセスの洗い出しから始めたほうがよい。それを専門に検討するチームで議論してもらうべきである。