耐量子計算機暗号の最新動向

高木 剛

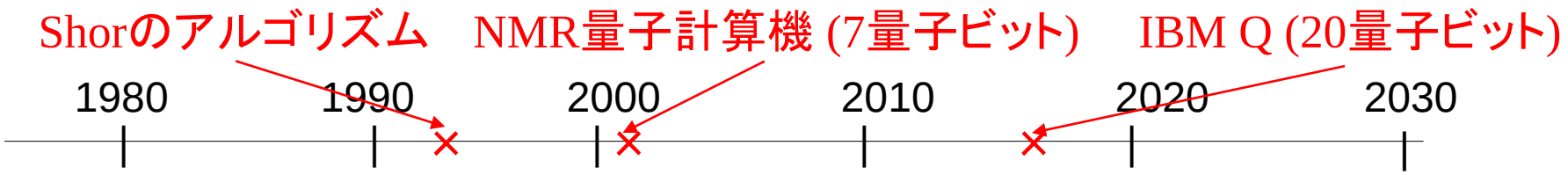
東京大学大学院情報理工学系研究科
数理情報学専攻
http://crypto.mist.i.u-tokyo.ac.jp/

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

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)

量子計算機で危殆化!!

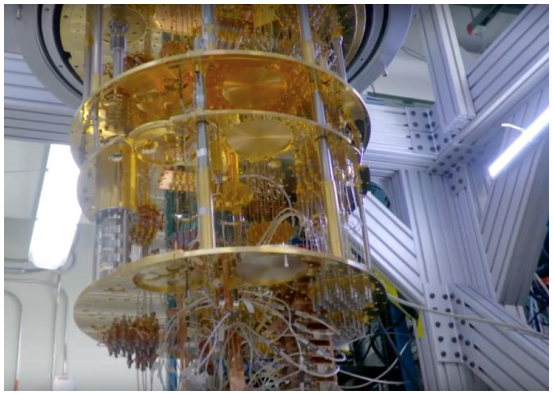
耐量子計算機暗号(PQC)

(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

東京大学
THE UNIVERSITY OF TOKYO

量子クラウド IBM Q

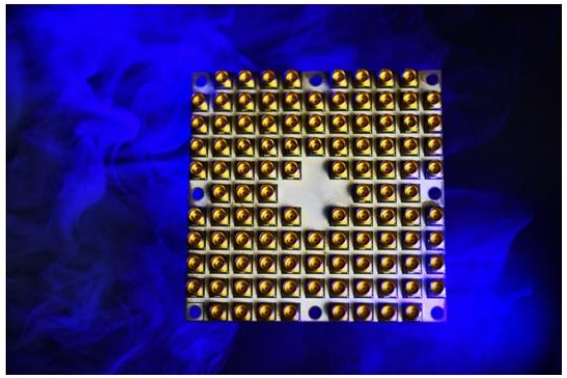


https://www.research.ibm.com/ibm-q/network/より転載

IBM Q、2017年11月、20量子ビット

IBM Quantum Roadmap
1,121 qubits (2023年)
433 qubits (2022年)
127 qubits (2021年)
65 qubits (2020年)

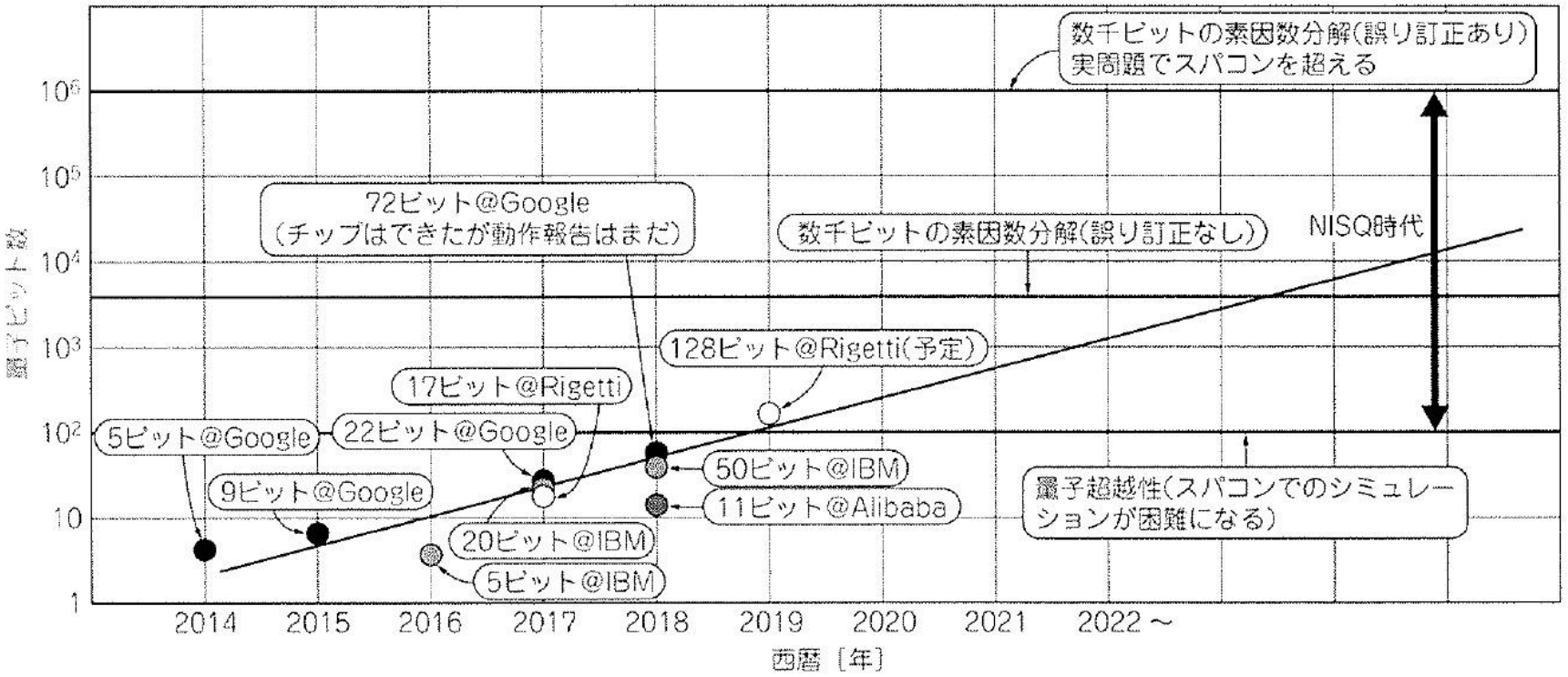
https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/



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

- 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

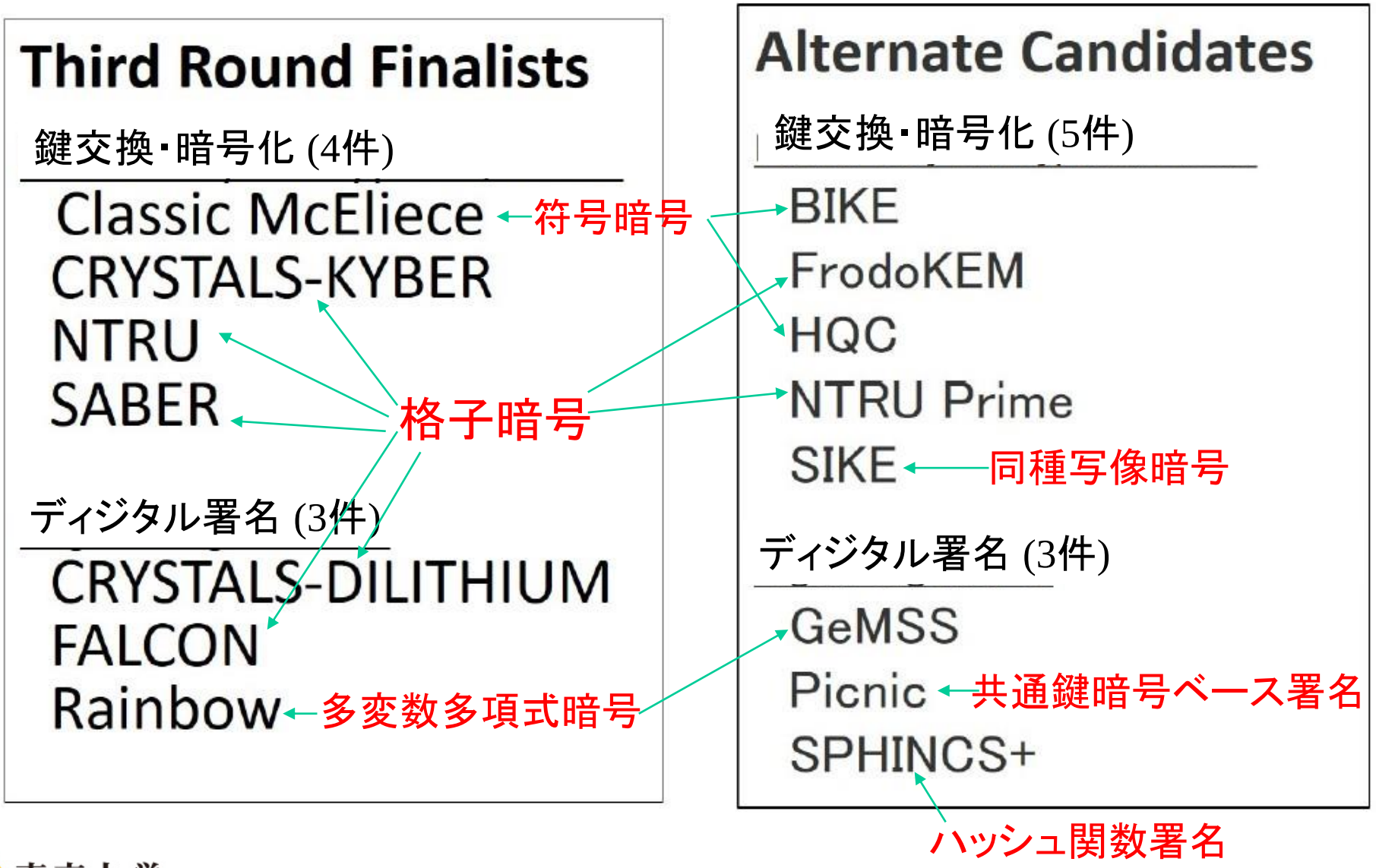
- **その他 (16件)**

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

2020年7月から第3ラウンド(15件)



NIST PQC 標準化スケジュール

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

- 2017年11月: 公募〆切
- 2019年1月: 第2ラウンド選出暗号発表
- 2020年7月: 第3ラウンド選出暗号発表
- 2021年6月: 第3回NIST PQC標準化会議
- 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**

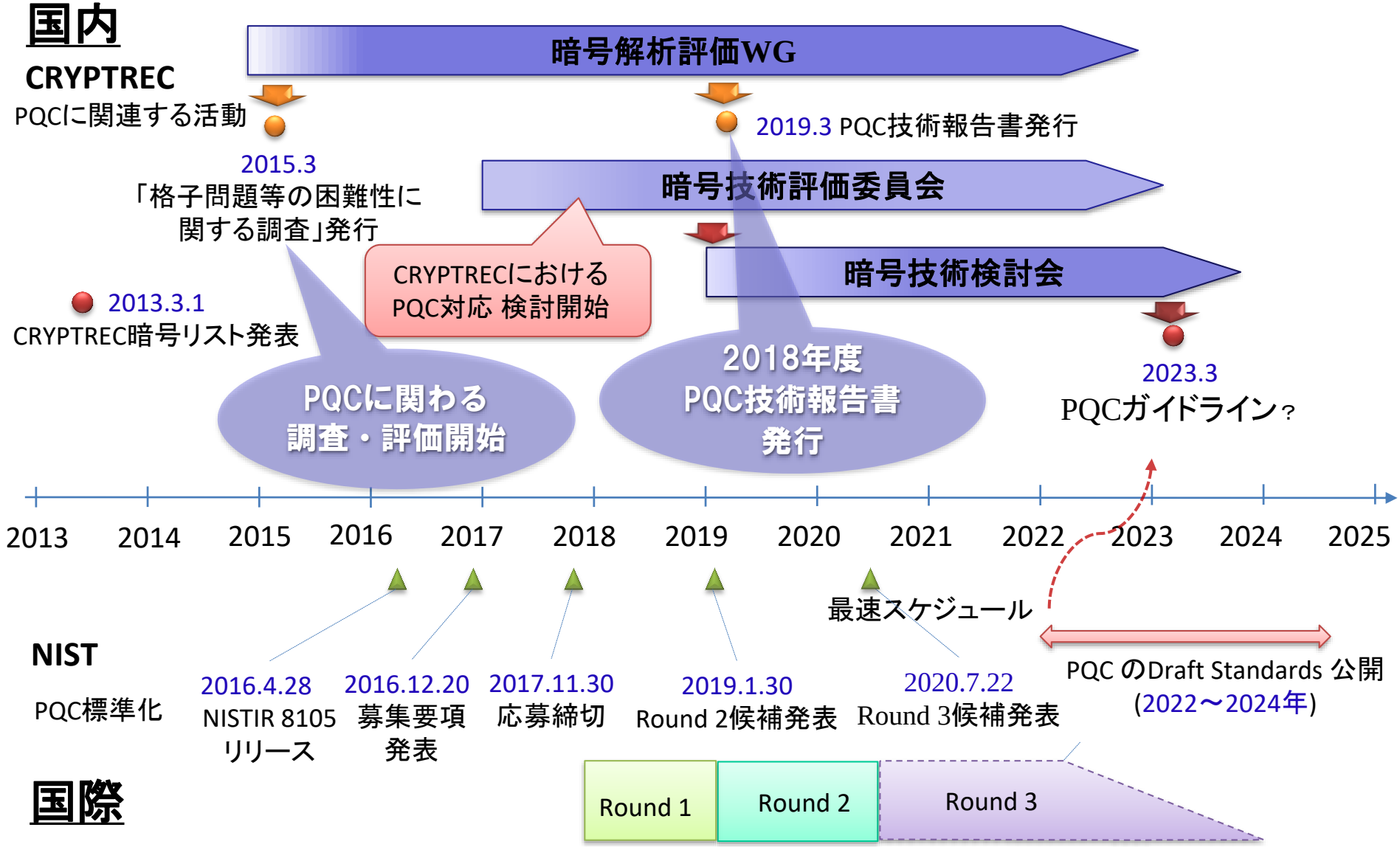
耐量子暗号への移行期間

x 2022年-2024年: 耐量子計算機暗号の標準規格ドラフト

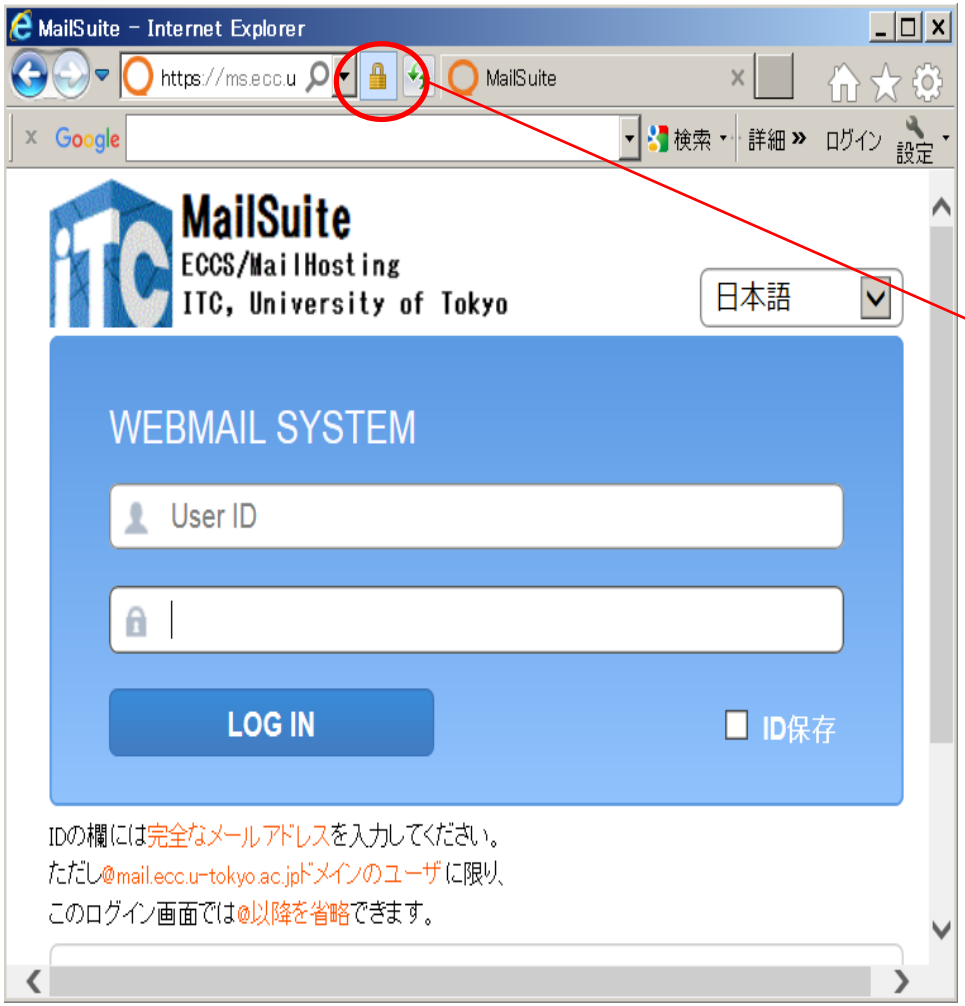
x 2021年6月: 第3回NIST PQC標準化会議

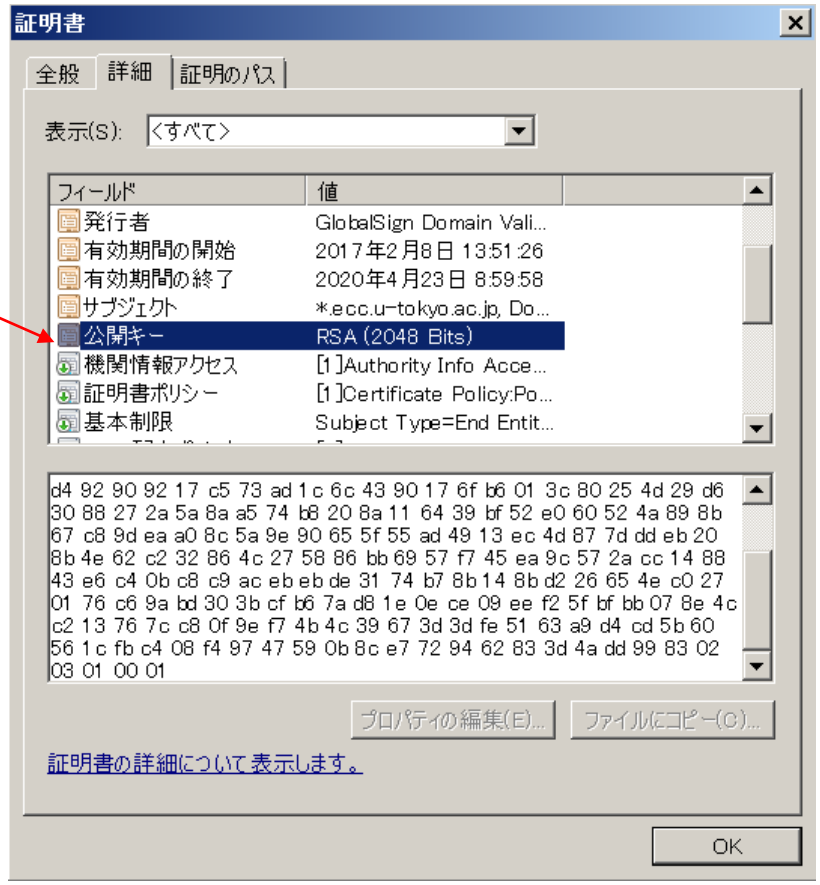
x 2020年7月: 第3ラウンド開始

PQC標準化をめぐる国内外の動き



RSA暗号の公開鍵

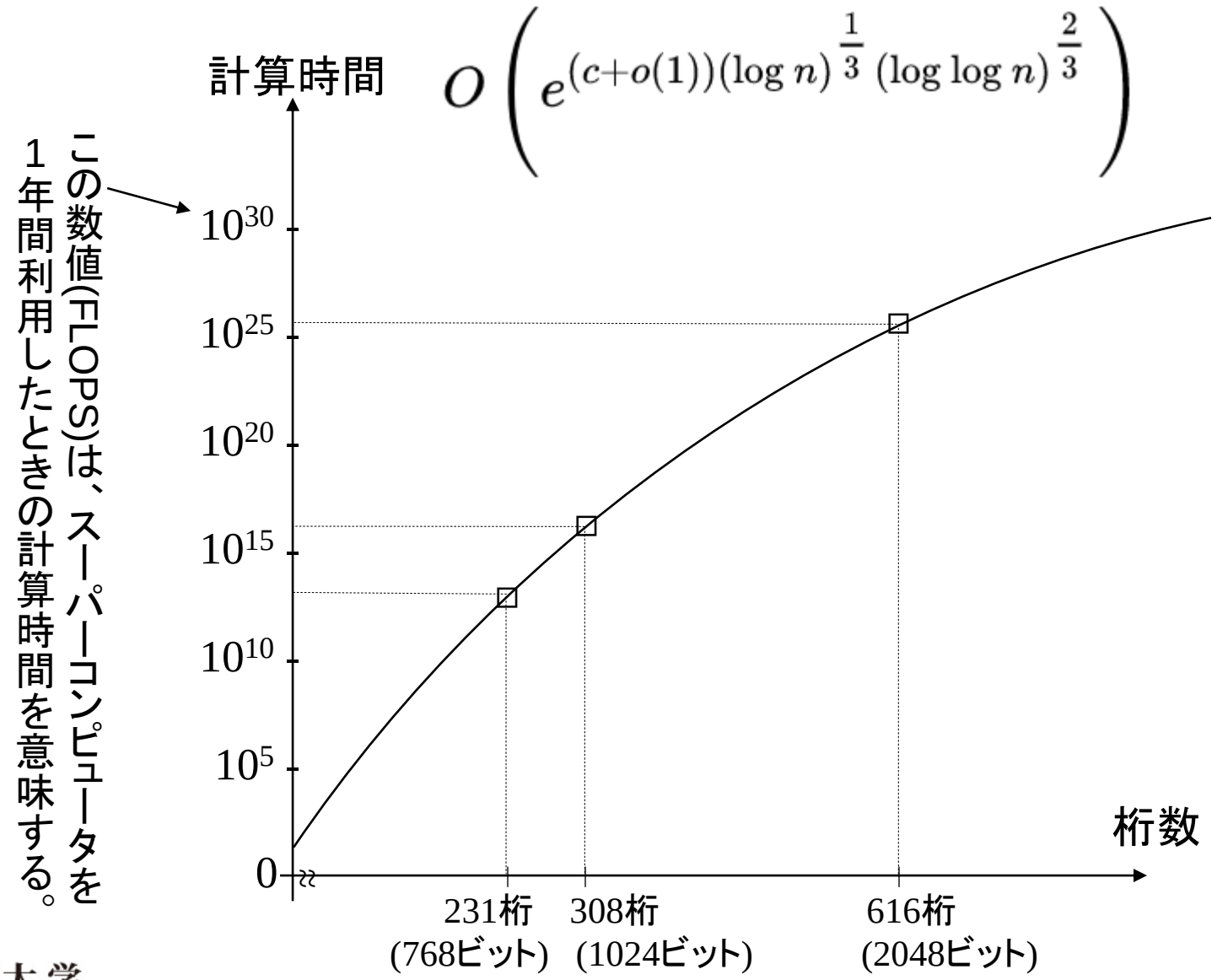

MailSuite - Internet Explorer
https://ms.ecc.u
MailSuite
Google
検索
詳細 »
ログイン
設定
MailSuite
ECCS/MailHosting
ITC, University of Tokyo
日本語
WEBMAIL SYSTEM
User ID
LOG IN
ID保存
IDの欄には完全なメールアドレスを入力してください。
ただし@mail.ecc.u-tokyo.ac.jpドメインのユーザに限り、
このログイン画面では@以降を省略できます。


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
$O\left(e^{(c+o(1))(\log n)^{\frac{1}{3}}(\log\log n)^{\frac{2}{3}}}\right)$
この数値(FLOPS)は、スーパーコンピュータを1年間利用したときの計算時間を意味する。
10^{30}
10^{25}
10^{20}
10^{15}
10^{10}
10^{5}
0
桁数
231桁 (768ビット)
308桁 (1024ビット)
616桁 (2048ビット)

素因数分解の困難性に関する計算量評価

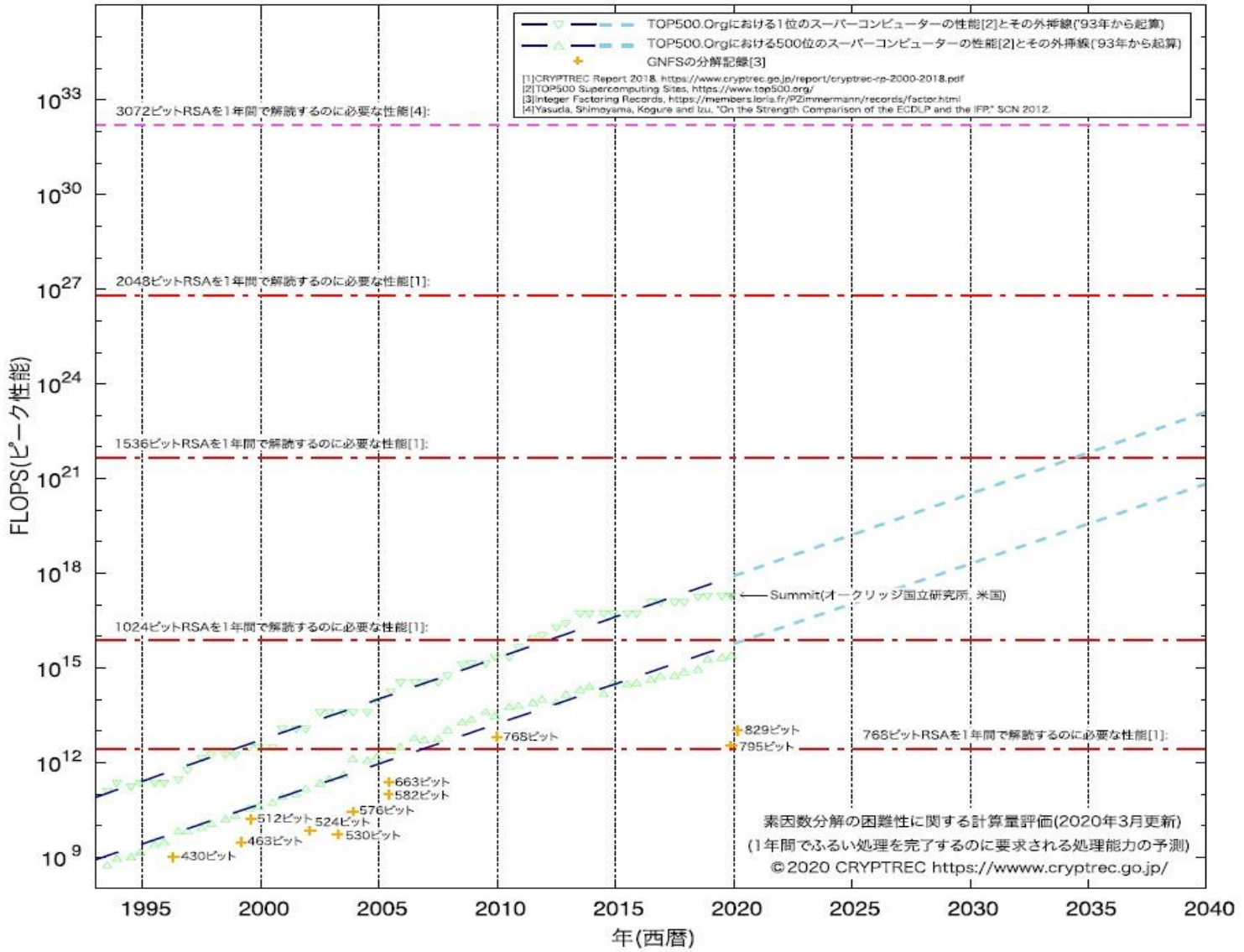
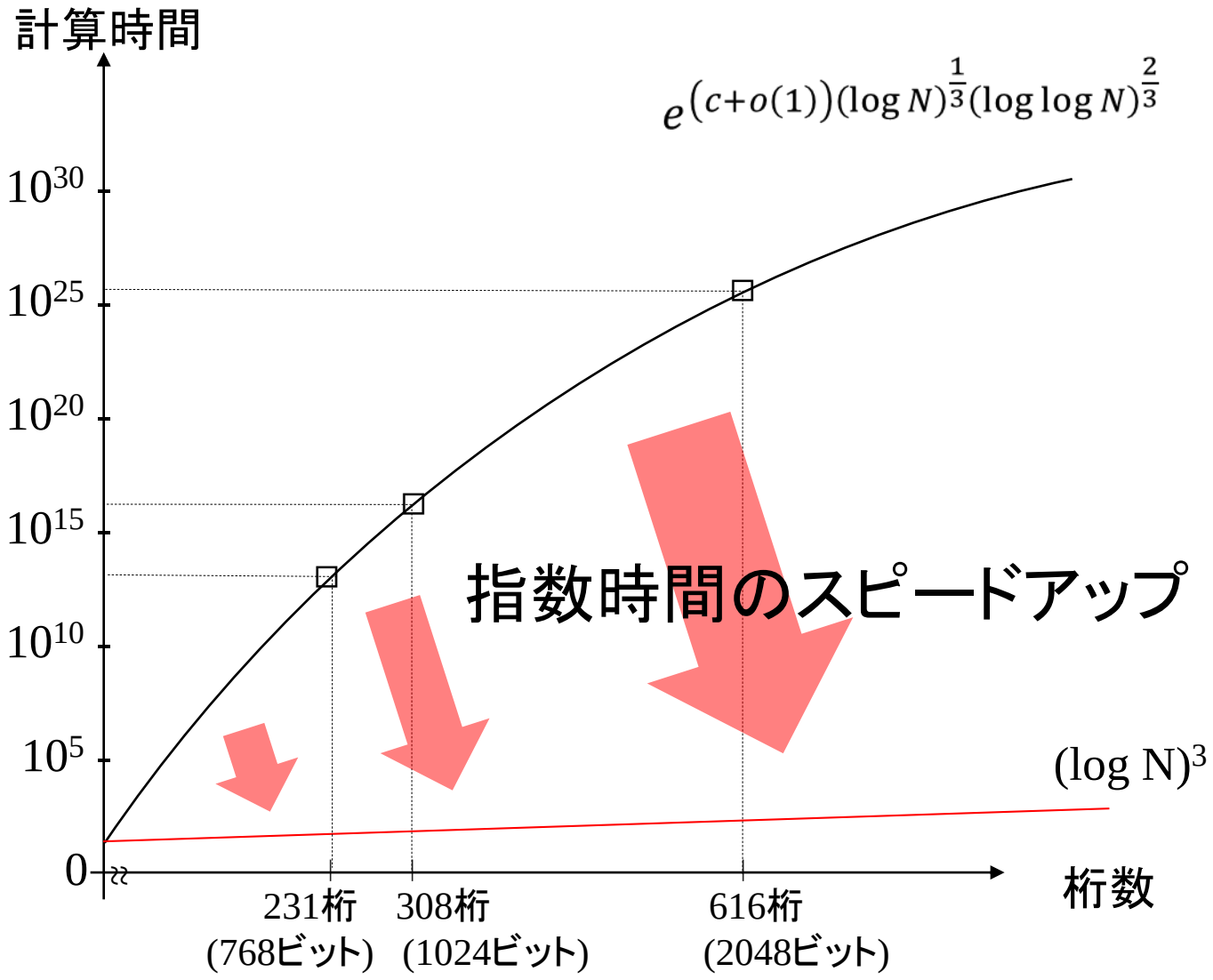


図 3.1：素因数分解の困難性に関する計算量評価　(http://www.cryptrec.jp/)

(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、2020 年 3 月更新)[3]

量子コンピュータによる素因数分解



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&3ラウンド 格子暗号の技術分類

赤色：第3ラウンドFinalists, 青色：第3ラウンドAlternative candidates

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

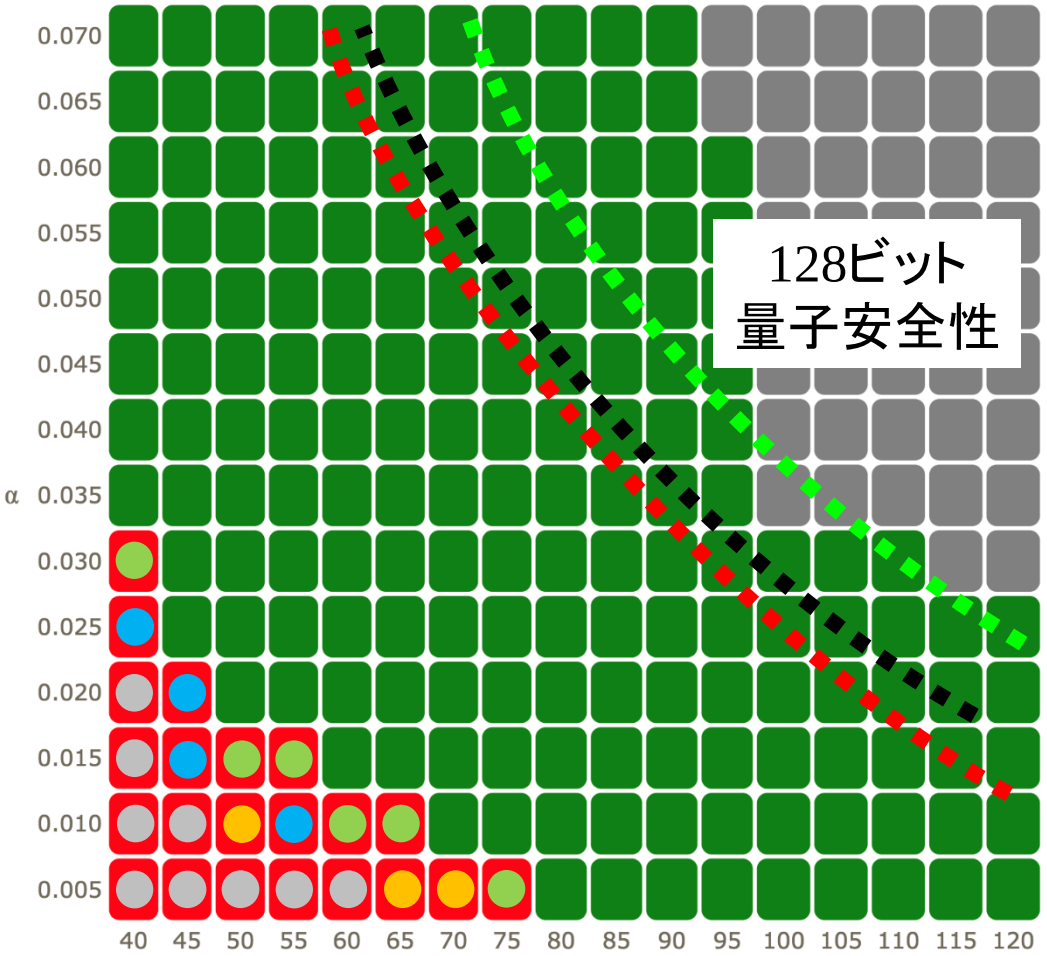
$\alpha = \sigma/q$ (ノイズ)

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)



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

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年8月.