量子コンピューターによる暗号への影響に関する，NICTセキュリティ基盤研究室の取り組み

サイバーセキュリティシンポジウム2023

サイバーセキュリティ研究所
Cybersecurity Research Institute

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　主任研究員　青野　良範
2023/02/17　15:05-15:35

自己紹介

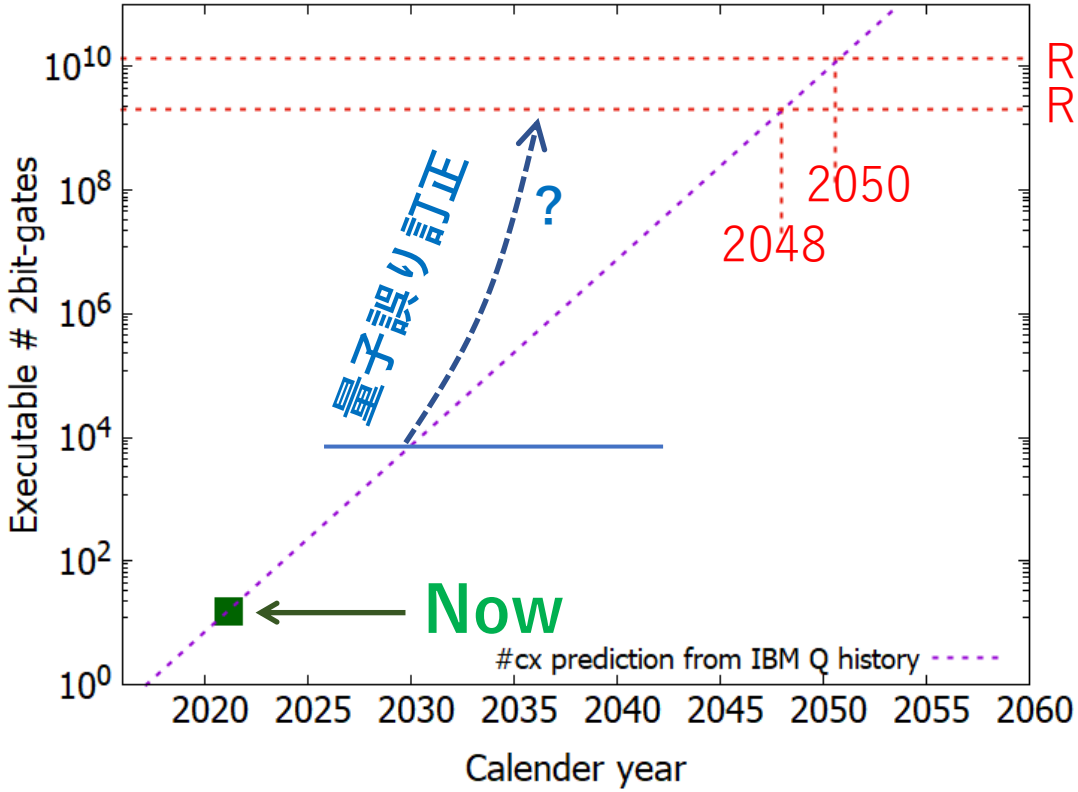
青野　良範（AONO, Yoshinori）
国立研究開発法人情報通信研究機構（NICT）
サイバーセキュリティ研究所　セキュリティ基盤研究室　主任研究員

略歴
東京工業大学　情報理工学研究科　数理・計算科学専攻（理学）

2011年に情報通信研究機構サイバーセキュリティ研究所に入所後、
公開鍵暗号の安全性評価に関わる研究を行う。
2019年より慶應義塾大学量子コンピューティングセンターとともに共同研究を開始、
量子コンピュータの公開鍵暗号に対する影響を調査。

目次

- 研究背景説明（量子コンピュータと暗号に関する研究活動の調査）
- 量子コンピュータを用いた離散対数問題の計算実験と将来予測

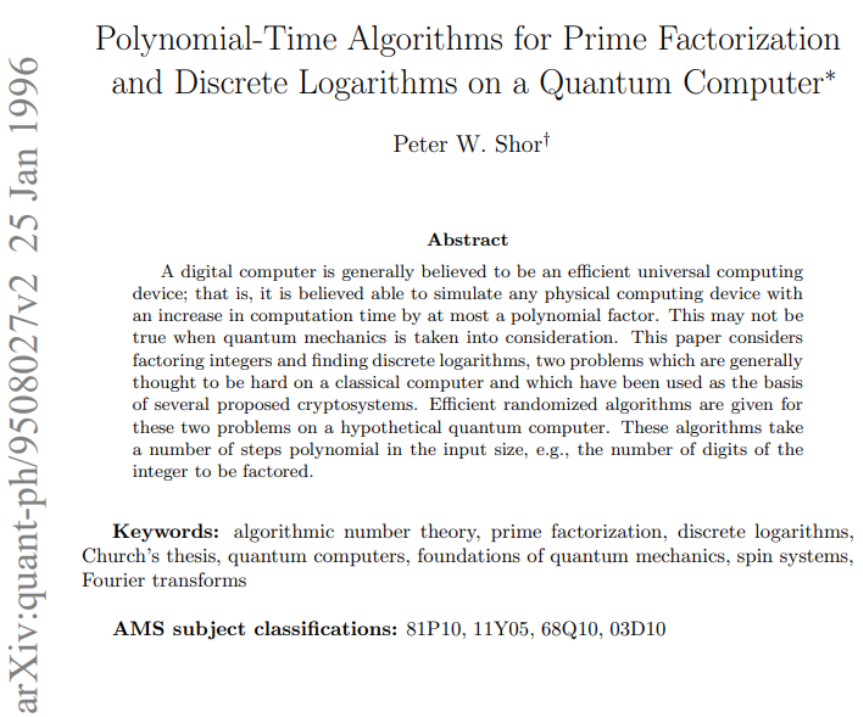


RSA-2048
RSA-1024
} RSA暗号の量子解読計算量 [Gidney-Ekerå, 2019]

※量子デバイスのCNOTゲートエラーが
1年ごとに半分になるトレンドが長期間続くと
仮定したときの予測

量子コンピュータの発展と暗号への影響

✔量子コンピュータが発展すると公開鍵暗号の解読が
おそらく現実的な時間で可能になる [Shor@ANTS, FOCS1994]



Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

AMS subject classifications: 81P10, 11Y05, 68Q10, 03D10

技術分類		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		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
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
	秘匿モード	CBC
		CFB

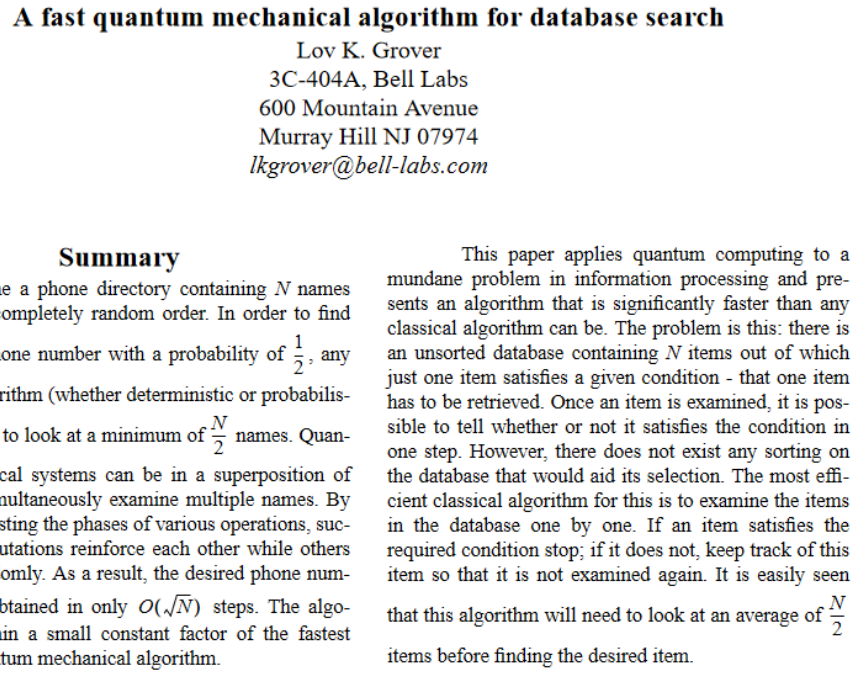
現在使われている公開鍵暗号・署名が危殆化

CRYPTREC暗号リスト　（最終更新2022/04/30）

✔現代暗号に影響する範囲として特にRSA暗号、楕円曲線暗号など
（素因数分解、離散対数問題が量子多項式時間で解ける）

量子コンピュータの発展と暗号への影響

✔量子コンピュータが発展すると暗号解読が<u>大幅に高速化</u>する [Grover@STOC1996]



A fast quantum mechanical algorithm for database search

Lov K. Grover
3C-404A, Bell Labs
600 Mountain Avenue
Murray Hill NJ 07974
lkgrover@bell-labs.com

Summary

Imagine a phone directory containing N names arranged in completely random order. In order to find someone's phone number with a probability of $\frac{1}{2}$, any classical algorithm (whether deterministic or probabilistic) will need to look at a minimum of $\frac{N}{2}$ names. Quantum mechanical systems can be in a superposition of states and simultaneously examine multiple names. By properly adjusting the phases of various operations, successful computations reinforce each other while others interfere randomly. As a result, the desired phone number can be obtained in only $O(\sqrt{N})$ steps. The algorithm is within a small constant factor of the fastest possible quantum mechanical algorithm.

This paper applies quantum computing to a mundane problem in information processing and presents an algorithm that is significantly faster than any classical algorithm can be. The problem is this: there is an unsorted database containing N items out of which just one item satisfies a given condition - that one item has to be retrieved. Once an item is examined, it is possible to tell whether or not it satisfies the condition in one step. However, there does not exist any sorting on the database that would aid its selection. The most efficient classical algorithm for this is to examine the items in the database one by one. If an item satisfies the required condition stop; if it does not, keep track of this item so that it is not examined again. It is easily seen that this algorithm will need to look at an average of $\frac{N}{2}$ items before finding the desired item.

技術分類		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		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
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
	秘匿モード	CBC
		CFB

現在使われている
共通鍵暗号・ハッシュ関数に影響

CRYPTREC暗号リスト　（最終更新2022/04/30）

✔共通鍵暗号・ハッシュ関数の解読計算量が大幅に下がる：　$2^n \rightarrow 2^{0.5n}$

- ETSI GR QSC 006 V1.1.1, Limits to Quantum Computing applied to symmetric key sizes (2017)
- CRYPTREC技術報告書「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」(2019)

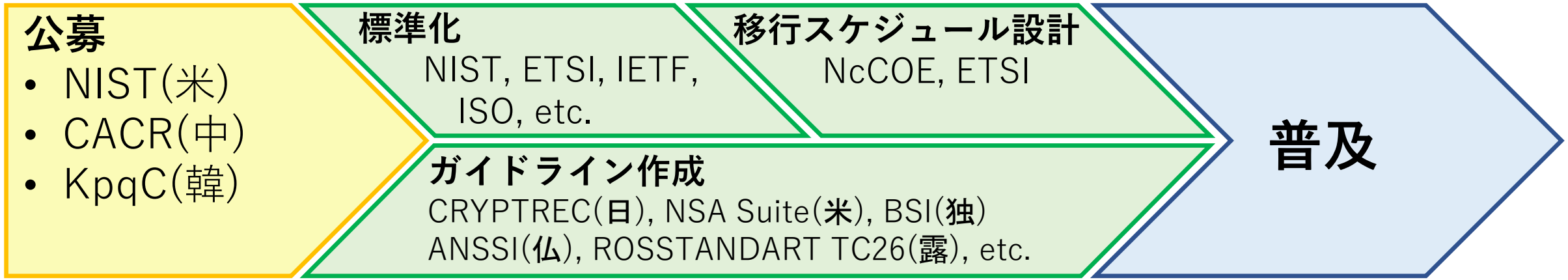
量子コンピュータの発展と暗号への影響

✔有名なShor, Grover以外でも，大型の量子コンピュータが登場することで様々な暗号に影響を与えることが知られている.

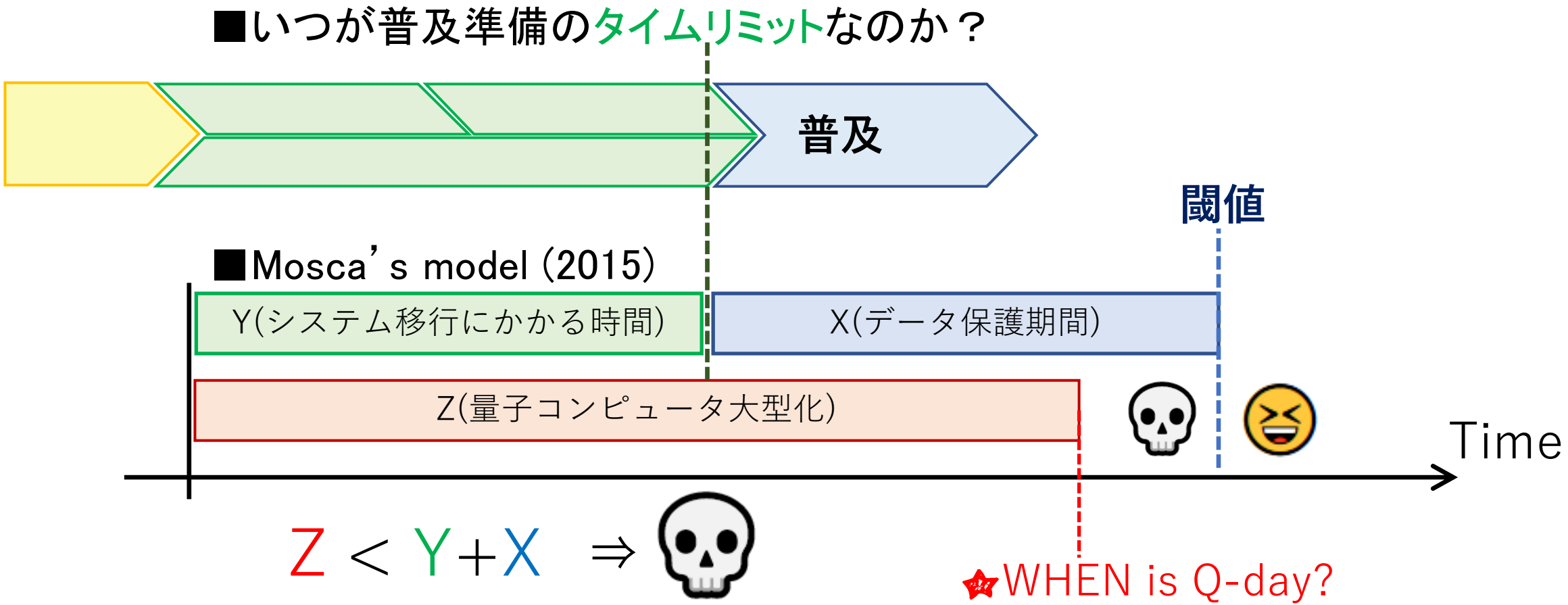
- RSA暗号，楕円曲線暗号のように量子コンピュータで安全性が極端に低下するもの
  →**新しい暗号（耐量子計算機暗号）**への移行

- 共通鍵暗号，ハッシュ関数のように量子コンピュータで安全性が低下するが
  それでも安全と考えられるもの　→パラメータの見直し

★耐量子計算機暗号の普及までのスケジュール



暗号の移行スケジュールを立てるために

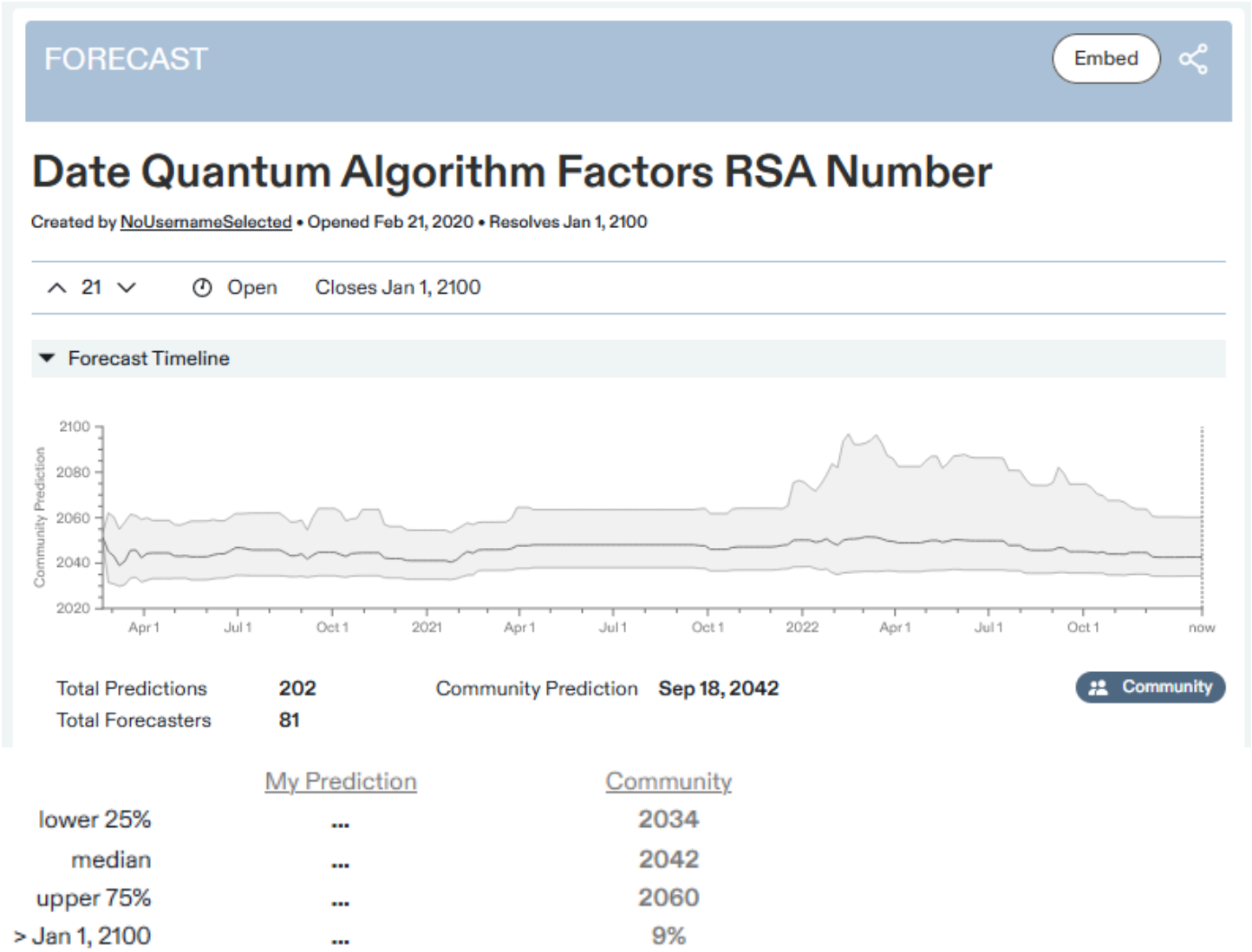


Mosca and Piani “Quantum Threat Timeline Report 2021” より引用・加筆

When is Q-day? 文献調査 1/3

✔Metaculus
- ★オンラインの予測サイト
- △誰でも投票可能

✔2023/1/24現在の状況
- 202個/81人の予測
- 中央値 2042年



When is Q-day? 文献調査 2/3

✔専門家の予測（招待講演＆アンケート）

予測者 (機関)	Q-day 予測	根拠	補足情報
Mariantoni	2029		PQCrypto 招待講演
Mosca	2026～2031		Workshop on CS in a PQ world
Mosca & Piani	2036	量子 C 専門家へのアンケート	半数以上の専門家が，50% 以上の確率で開発成功を予測
NISTEP	2033～2035	科学技術専門家へのアンケート	科学技術的実現と社会的実現
米国科学・工学・医学アカデミー	2028～	量子 C の開発状況と進化スピード	10 年以内の実現は期待できない

When is Q-day? 文献調査 2/3

✔専門家の予測（招待講演＆アンケート）

予測者 (機関)	Q-day 予測	根拠	補足情報	予測発表年	差
Mariantoni	2029		PQCrypto 招待講演	2014	15 年
Mosca	2026～2031		Workshop on CS in a PQ world	2015	11～16 年
Mosca & Piani	2036	量子 C 専門家へのアンケート	半数以上の専門家が，50% 以上の確率で開発成功を予測	2021	15 年
NISTEP	2033～2035	科学技術専門家へのアンケート	科学技術的実現と社会的実現	2019	14～16 年
米国科学・工学・医学アカデミー	2028～	量子 C の開発状況と進化スピード	10 年以内の実現は期待できない	2018	>10 年

When is Q-day? 文献調査 2/3

✔専門家の予測（招待講演＆アンケート）

予測者 (機関)	Q-day 予測	根拠	補足情報	予測発表年	差
Mariantoni	2029		PQCrypto 招待講演	2014	15 年
Mosca	2026～2031		Workshop on CS in a PQ world	2015	11～16 年
Mosca & Piani	2036	量子 C 専門家へのアンケート	半数以上の専門家が，50% 以上の確率で開発成功を予測	2021	15 年
NISTEP	2033～2035	科学技術専門家へのアンケート	科学技術的実現と社会的実現	2019	14～16 年
米国科学・工学・医学アカデミー	2028～	量子 C の開発状況と進化スピード	10 年以内の実現は期待できない	2018	>10 年

△予測年−発表年≒15年の法則

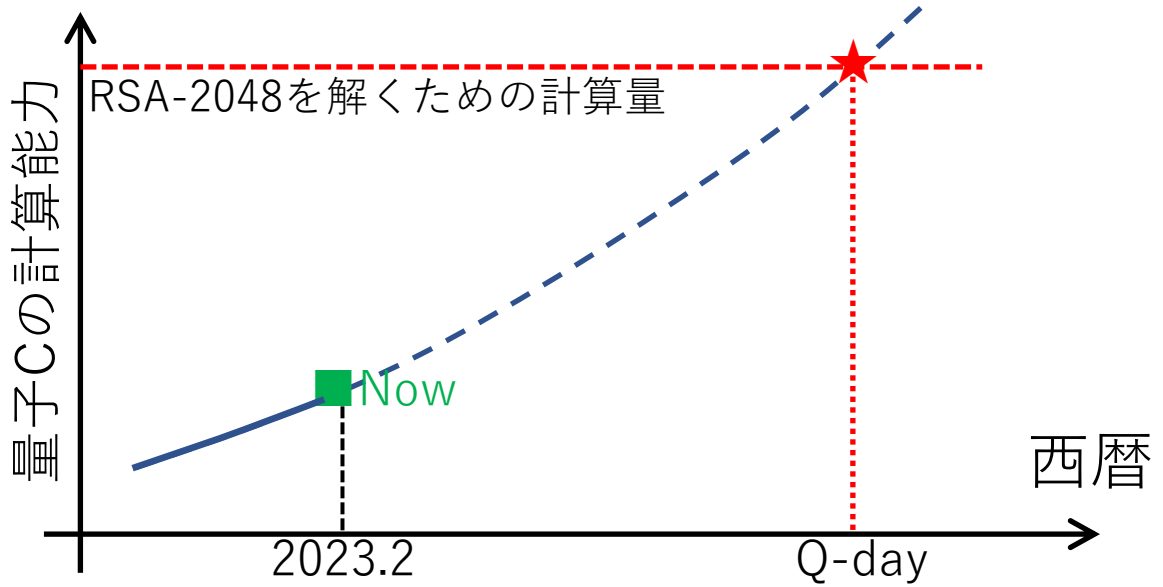
……一部ではQuantum jokeと呼ばれているらしい？

★もう少しデータに基づいた将来予測が必要

When is Q-day? 文献調査 3/3

過去の実績からの外挿

参考文献	RSA-2048 Break	根拠
Sevilla & Riedel (2020)	2039～	既存の量子 C 性能からの外挿
Runge (2022)	2048～2092	量子ビット数の伸びからの外挿
Aono et al. (2022)	2050	2-qubit gate error の減り方からの外挿



過去の実績からの外挿に関する先行研究

■必要な仕事

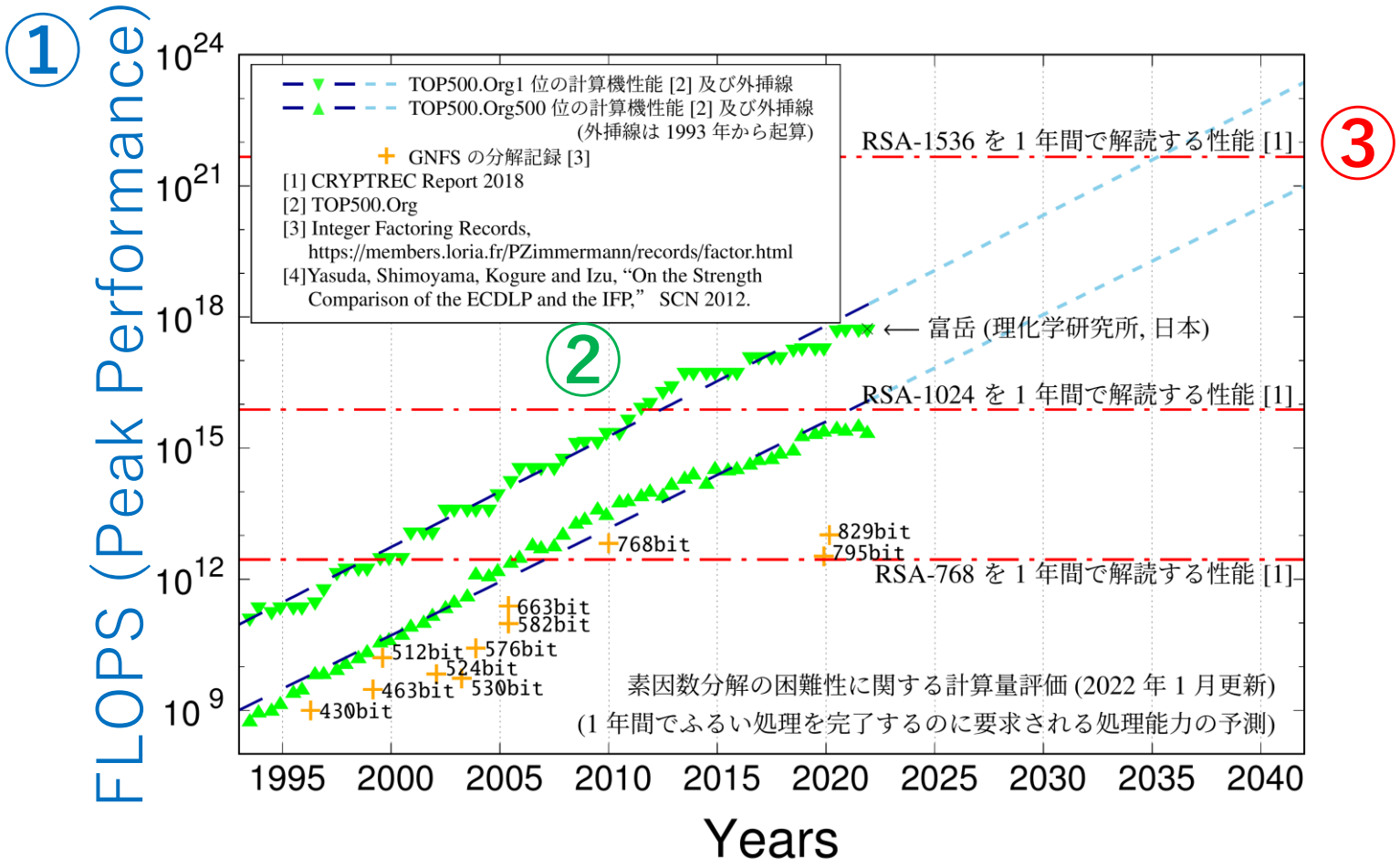
① 単位を決める

② 過去のトレンドを調べて将来を予測

- 指数関数的な成長を仮定（〇〇版ムーア）
- 未知の物理的な限界は無いと仮定
- 新技術による加速、予算・エネルギーの制約による原則も無いと仮定

③ 暗号の解読計算量の見積もり

- RSA-〇〇を1年間で解読する性能



※CRTPTREC Report 2021 図3.2-1をスライド向けに改変

単位選択に関する先行研究

△FLOPSのようなデファクトスタンダードが確立していれば良いのだが、
現状(NISQ)量子コンピュータの性能を測るための評価軸は様々なものが提案中

指標名	提案者（年）	定義	ロードマップ・将来予測	単一指標
量子ビット数	–	実行可能な回路の量子ビット数	✓	✓
ゲートのエラー率	–	NOT, CNOT などの基本的なゲート操作の誤り率	✓	✓
Quantum Volume (量子体積)	Cross et al. (2019)	n 量子ビット深さ d のランダム回路が高精度で実行できたときの $2^{\min(n,d)}$	✓	✓
Q-Score	Martiel et al. (2019)	QAOA により MaxCut を解くことのできる最大サイズ		✓
Generalized logical qubit	Sevilla & Riedel (2020)	誤りなしに実行可能な量子ビットの数	✓	✓
Quantum LINPACK	Dong and Lin (2020)	連立方程式の求解に関する成功確率		✓
QASMBench	Li et al. (2020)	複数の基本的な回路を実行したときの精度		
Algorithmic Qubits	IonQ (2022)	n 量子ビット回路に対して $\min(n, \sqrt{\#\texttt{CNOTgates}})$	✓	✓
SupermarQ	Tomesh et al. (2022)	複数の基本的な回路を実行したときの精度		

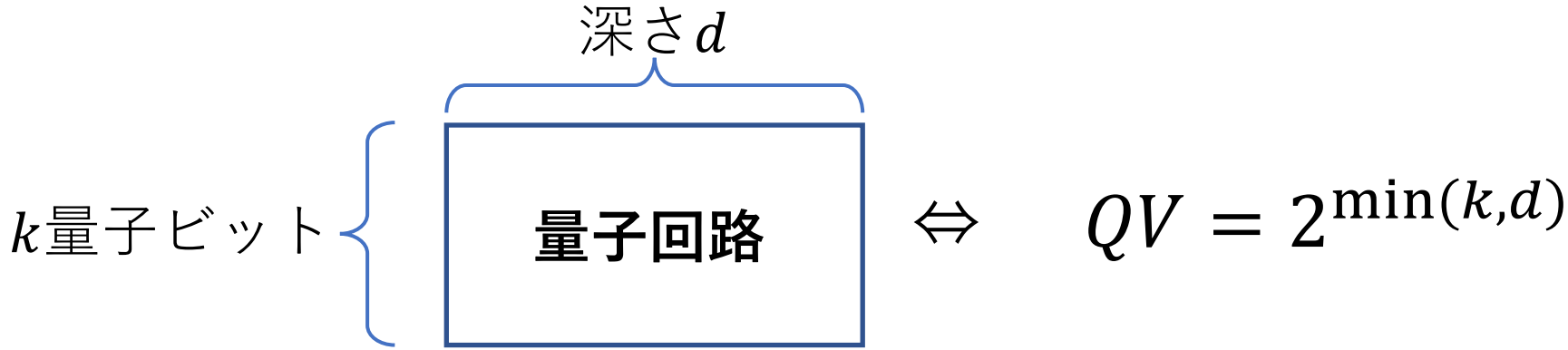
✔全体的な傾向として
- 計算速度は気にしない
- 答えを知った上でそこからの近さを測る（NISQデバイス向け）

将来予測に求められる性質
- 単一指標
- ロードマップ、過去のトレンドからの将来予測が用意されている

単位選択の重要性（Quantum Volume）

✔Quantum Volume（量子体積）
- 2019年IBMの研究者により提案
- 回路計算型量子コンピュータの汎用的なベンチマークを基にしている

IBMがロードマップを公開（少なくとも2倍/年：指数関数的な成長）



$\Leftrightarrow \quad QV = 2^{\min(k,d)}$

△将来予測の（あまり上手くない）例 [Aono et al. QIT43 (2020)]

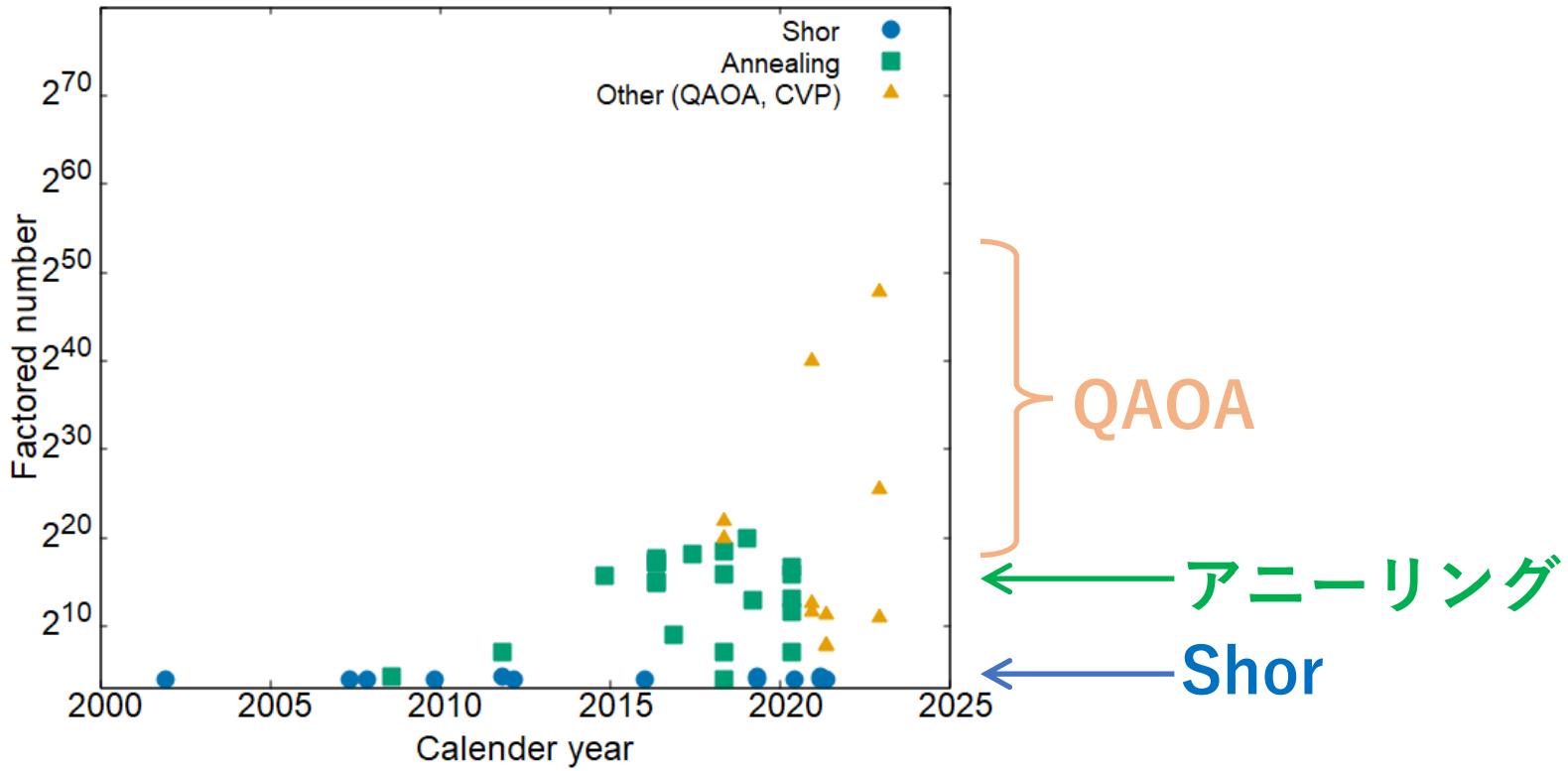
✔2020年10月の時点で$QV = 64 = 2^6$, 大体6量子ビットの（あまり深くない）回路を実行可能

✔**毎年QVが2倍⇒実行可能な回路サイズが毎年+1量子ビット**

△nビットの素因数分解回路で最良のものでも$k = 2n + 2$量子ビット必要
RSA-2048だとそれぞれ4000年後、 EdDSA(448ビット)でも1300年後

単位選択の重要性（分解された数のトレンド）

✪素因数分解の実験報告からの将来予測を試みる
✔この20年間で30件ほどの実験報告（Shorに限っても10件）



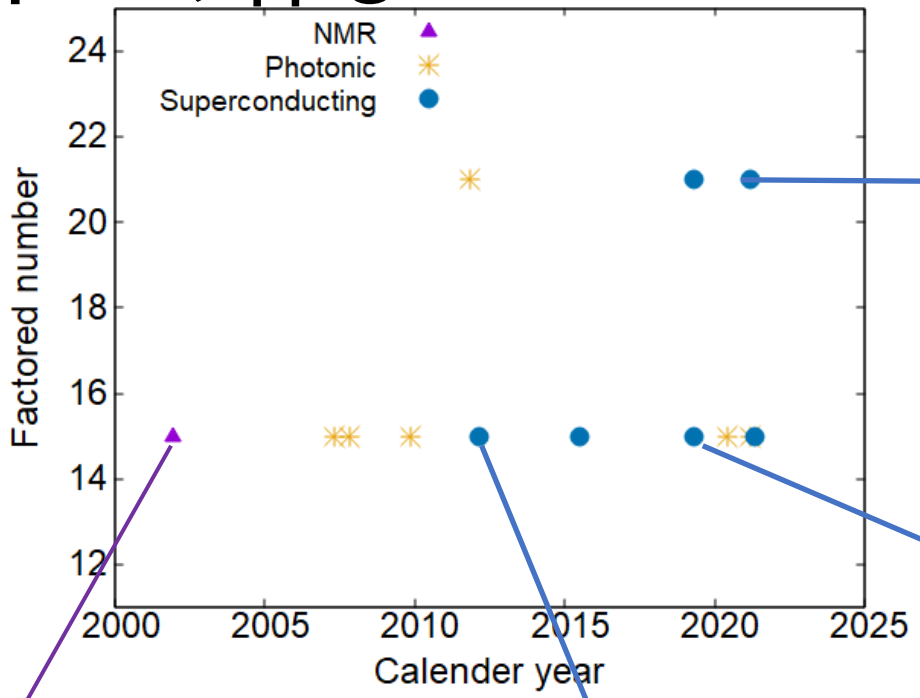
✔ Shor以外の伸びは凄まじいが
アルゴリズムが異なりトレンド予測が困難

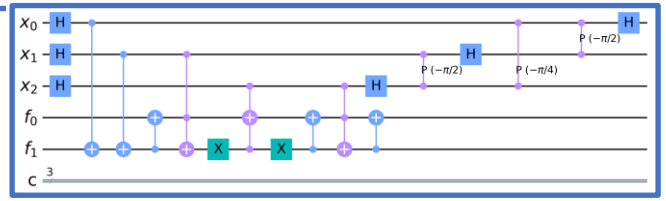
Shorに関する回路サイズの伸び

✔2010年以前はNMR, フォトニックによる実験
✔近年は超電導量子C

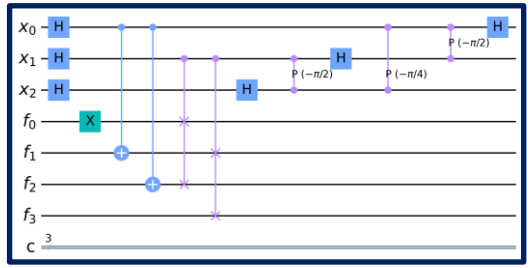
✸特殊化された回路の実行
- 分解対象の数に現れない部分での進歩
- 少しずつ大型化して一般的なものに近づいている
- 解けたかどうかの基準が統一されていない

✸状況をもっと詳しく見るための量子C実機による実験が必要

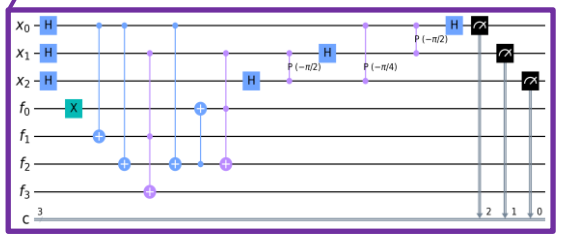




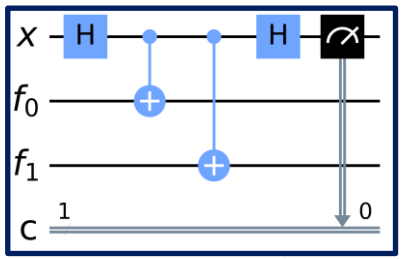
Skosana-Tame (2021)
5 qubits, (数値の圧縮表現)



Amico et al. (2019)
5 qubits
(指数部分の分割実装)



Vandersypen et al. (2001)
7 qubits, NMR



Lucero et al. (2012)
3 qubits, Josephson gate

CRYPTREC外部評価報告書『Shor のアルゴリズム実装動向調査』(2021)より

ここまでのまとめ

✔耐量子計算機暗号への移行スケジュールのためにQ-dayの予測が必要

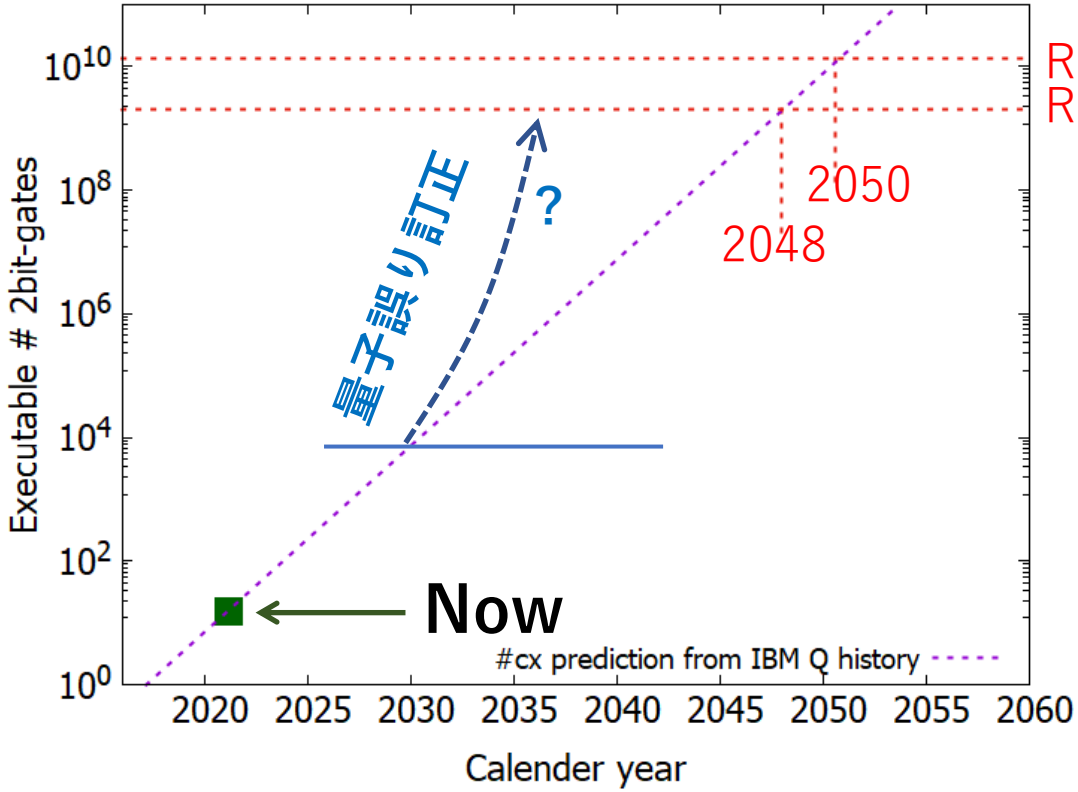
✔Q-dayの予測のために予測のグラフが必要
- 計算性能の指標（縦軸）は単一かつロードマップのあるものが欲しい

✔単一でロードマップのある指標はいくつか存在する
- NISQ向けロードマップを単純に引き延ばすとあまり良くない予想になる可能性

✔先行研究の多くは部分回路を使った予備実験的なもの
- 解けたかどうかの基準が統一されていない

目次

- 研究背景説明（量子コンピュータと暗号に関する先行研究の調査）
- ***量子コンピュータを用いた離散対数問題の計算実験と将来予測***



RSA-2048
RSA-1024
} RSA暗号の量子解読計算量 [Gidney-Ekerå, 2019]

※量子プロセッサのCNOTゲートエラーが
1年ごとに半分になるトレンドが長期間続くと
仮定したときの予測

研究内容の概要

- 量子コンピュータの暗号に対する将来的な影響を調査する目的で，4者での共同研究
  - 情報通信研究機構
  - 慶應義塾
  - 三菱UFJフィナンシャル・グループ
  - みずほフィナンシャルグループ

- 『解けた』の基準作り
  - ✔量子コンピュータから何が出てきたら問題が解けたと主張できるのか？
    - 将来予測をするベースとして『今の量子Cはどこまでの問題が解けるのか』
    - 予測図を描くにしても『性能指数が〇〇を超える量子コンピュータはRSA−△△，DLP−△△を解くことができる』ということが読み取れるようにしたい
- 離散対数問題の実験
  - △回路が最小になるインスタンス：$2^z \equiv 1 \pmod 3, 2^z \equiv 2 \pmod 3$
  - △教科書に載っている15の素因数分解回路はまだ厳しい
- 実験とロードマップからの将来予測

実験の役割分担

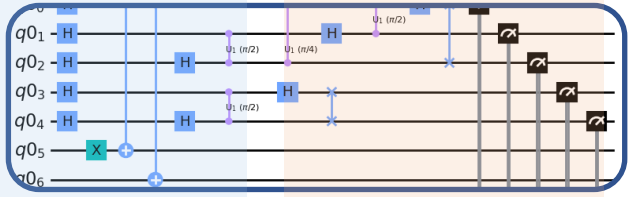
NICT　三菱　みずほ　慶應義塾

実際に解く問題・
インスタンス選択

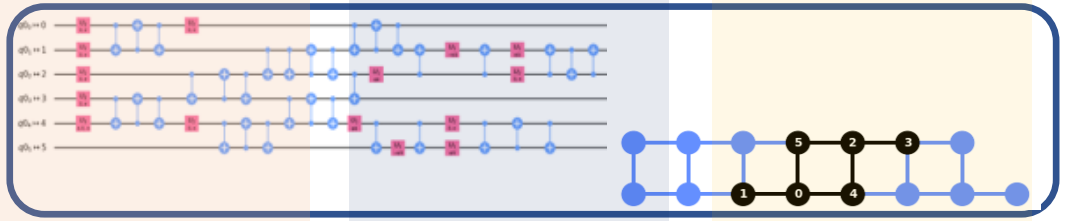
- RSA or DLP
- Size of instances

	DLP instance	n_x	n_y	N_L	N_g
I	$2^z = 1 \bmod 3$	2	2	19	31
II		3	2	24	44
III	$2^z = 2 \bmod 3$	3	2	25	93
IV		3	3	31	123
V	$4^z = 2 \bmod 7$	3	3	39	227
VI	$3^z = 4 \bmod 7$	4	4	89	861

論理レベル回路設計

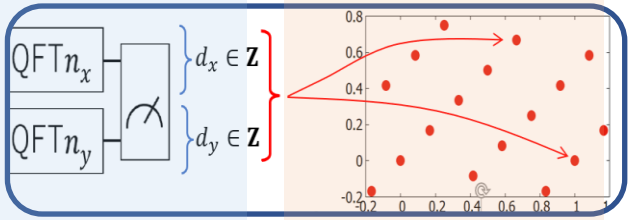


回路のトランスパイル
＆最適化



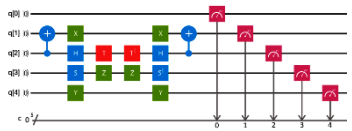
量子コンピュータ実機
での実行

出力結果の後処理

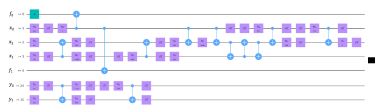


NISQコンピュータの実行

NISQ量子コンピュータの実行順序



量子回路
(論理レベル)



量子回路
(トランスパイル後)

同じ回路を
何千回も実行

1: 0011010101
2: 1101010111
3: 0101100111
⋮
8190: 0101100111
8191: 0011001110
8192: 1101001010

後処理

解の候補が何千個も出てくる

✔同じ回路を何度も実行して測定を行う
- 量子Cはある確率分布からのサンプル(＋ノイズ)をビット列として出力
- ビット列を後処理して離散対数，素因数の候補を出力
- ノイズが大きいとほぼ乱数になる

△今のところ、小さいインスタンスの回路しか実行できない
- 離散対数問題($2^z \equiv 1 \bmod 3$)、素因数分解(15)
- 何千回も実行したらたとえ乱数でも1、2回は当たる

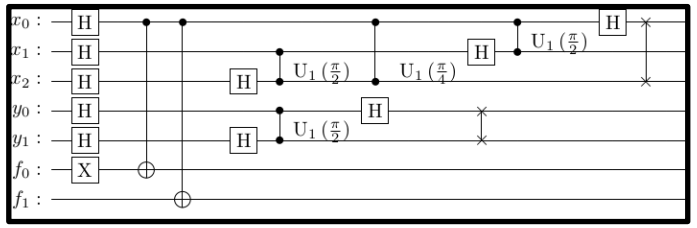
量子コンピュータの写真：https://www.flickr.com/photos/ibm_research_zurich/51331567650/in/album-72157703845574031/

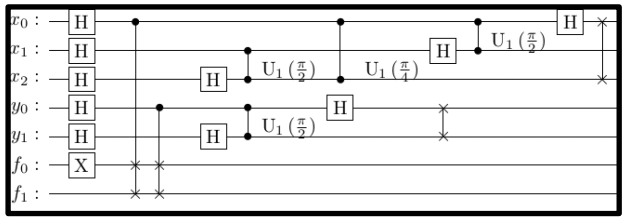
実験結果と解釈

$2^z \equiv 1 \bmod 3$

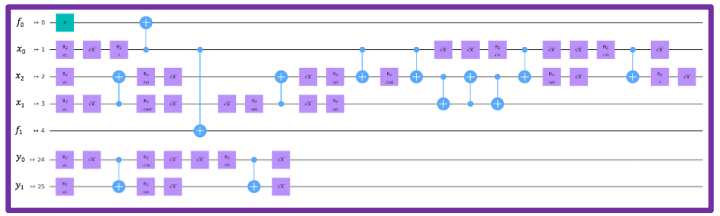
$2^z \equiv 2 \bmod 3$

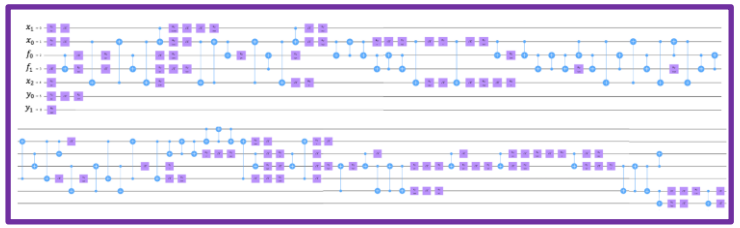
論理レベル回路



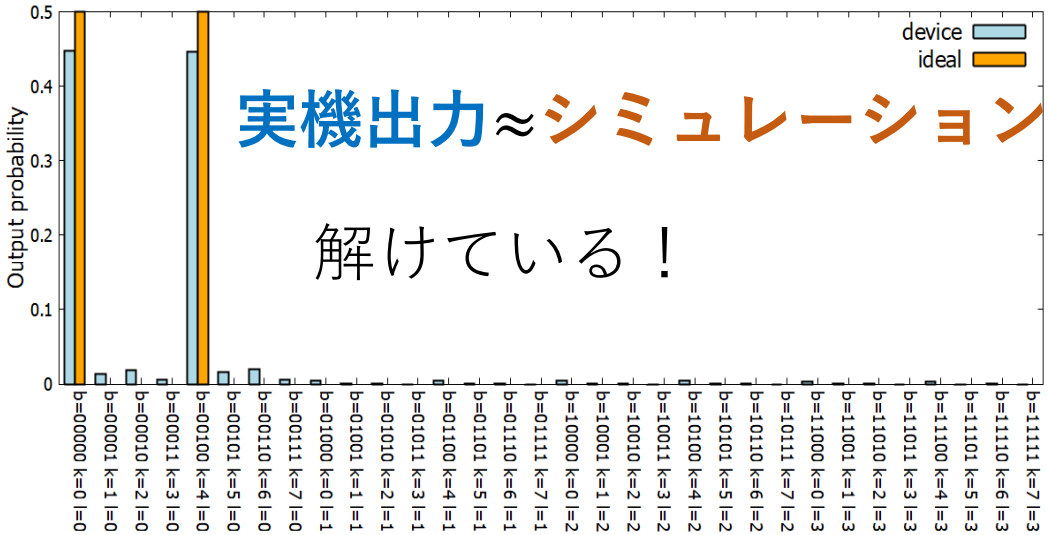


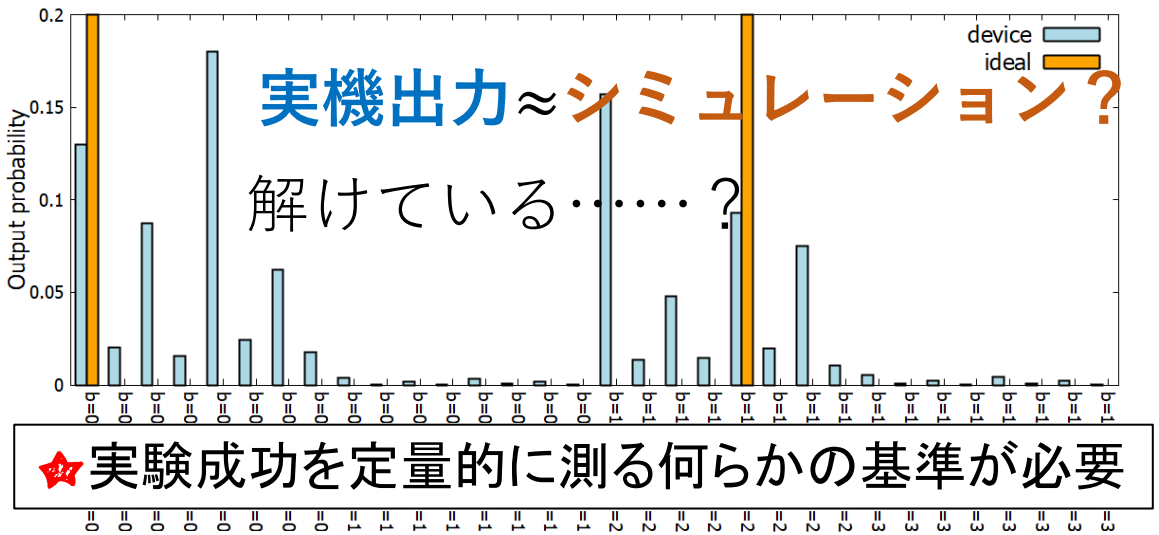
トランスパイル後





実行後の確率分布

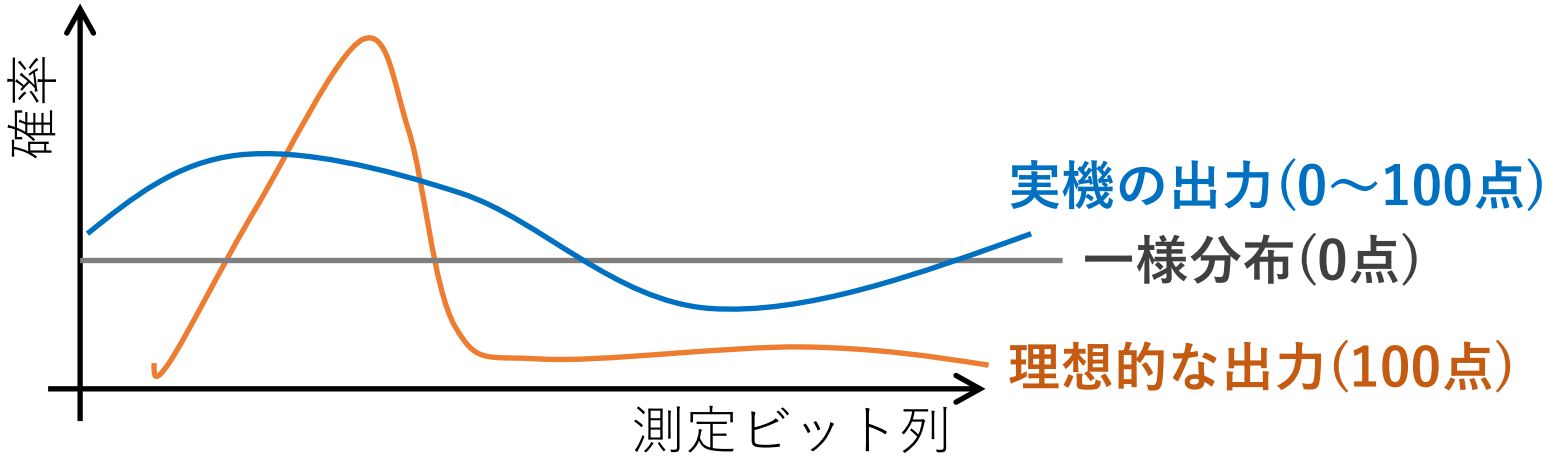




正解率ベースの成功定義

✔量子(NISQ)コンピュータによる実験が成功したかどうかを定量的に測りたい

✔先行研究：確率変数のスコアによる中間値基準の判定



- 確率分布に対して数値を割り当てる
- 数値が中間値よりも上ならば実験成功とする

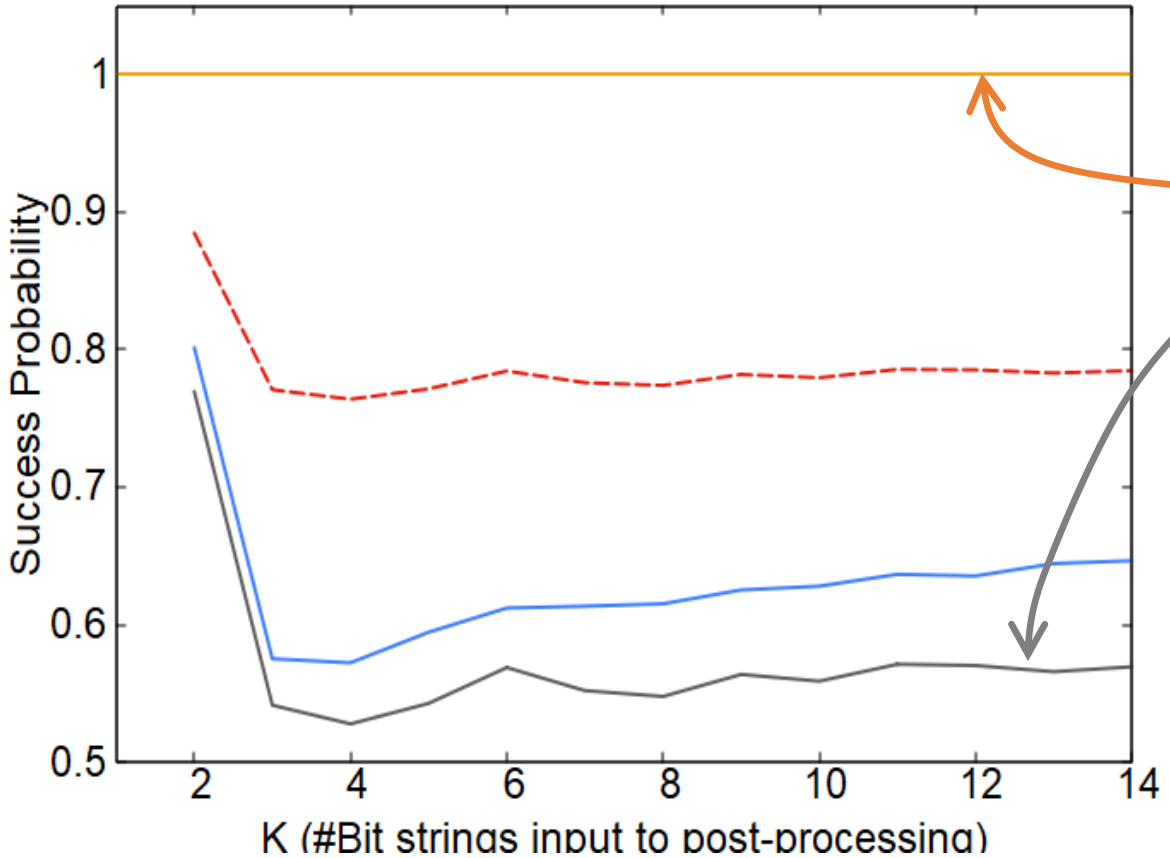
Score(実験) > (Score(理想)+Score(ランダムノイズ))/2 ⇒ 

■我々のスコアは後処理アルゴリズムの正解率とした

- 離散対数問題の解の候補zに対して，$g^z \equiv a \pmod{p}$を満たすかどうか

実際の実験（$2^z \equiv 2 \bmod 3$ は解けているか？）

正解率



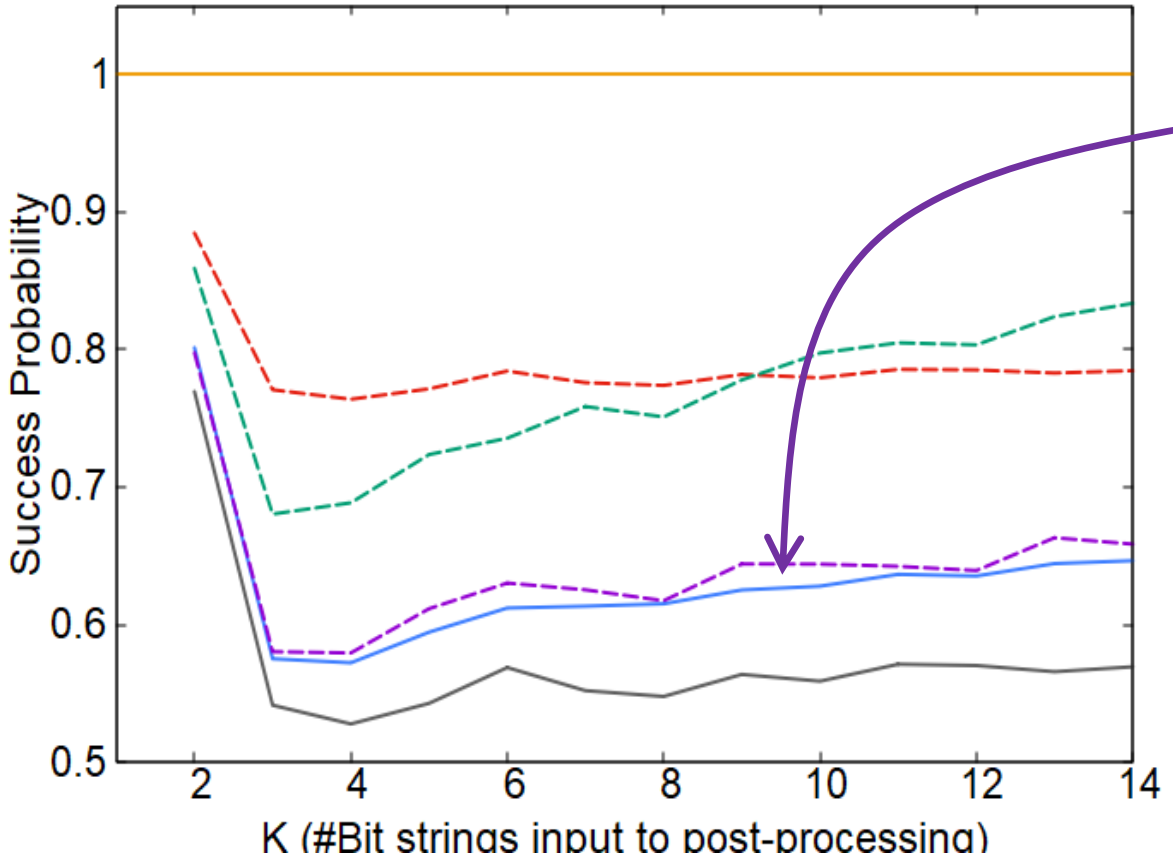
★実機出力の正解率の他に、４種類のシミュレーションを行い正解率を比較
- 量子ノイズの無い回路の出力
- 一様ランダムなビット列
- これらの平均値が成功のしきい値

△結論としてまだ解けていない
- いつ解けるようになるのか？

※Shorによる離散対数問題の特徴として、後処理アルゴリズムに複数個のビット列を入力することが可能で、それにより正解率が少しだけ上がる
※ibm_kawasakiによる実験は2021年7月

実際の実験（$2^z \equiv 2 \bmod 3$ は解けているか？）

正解率



- 実機ノイズのパラメータ化
  - CNOT error=0.07としたシミュレーション
- error↓　正解率↑

- CNOT error=0.04まで下げると成功になると予想される

- 量子Cが進化しエラーレートが半分になるのを待つ

※Shorによる離散対数問題の特徴として、後処理アルゴリズムに複数個のビット列を入力することが可能で、それにより正解率が少しだけ上がる
※ibm_kawasakiによる実験は2021年7月

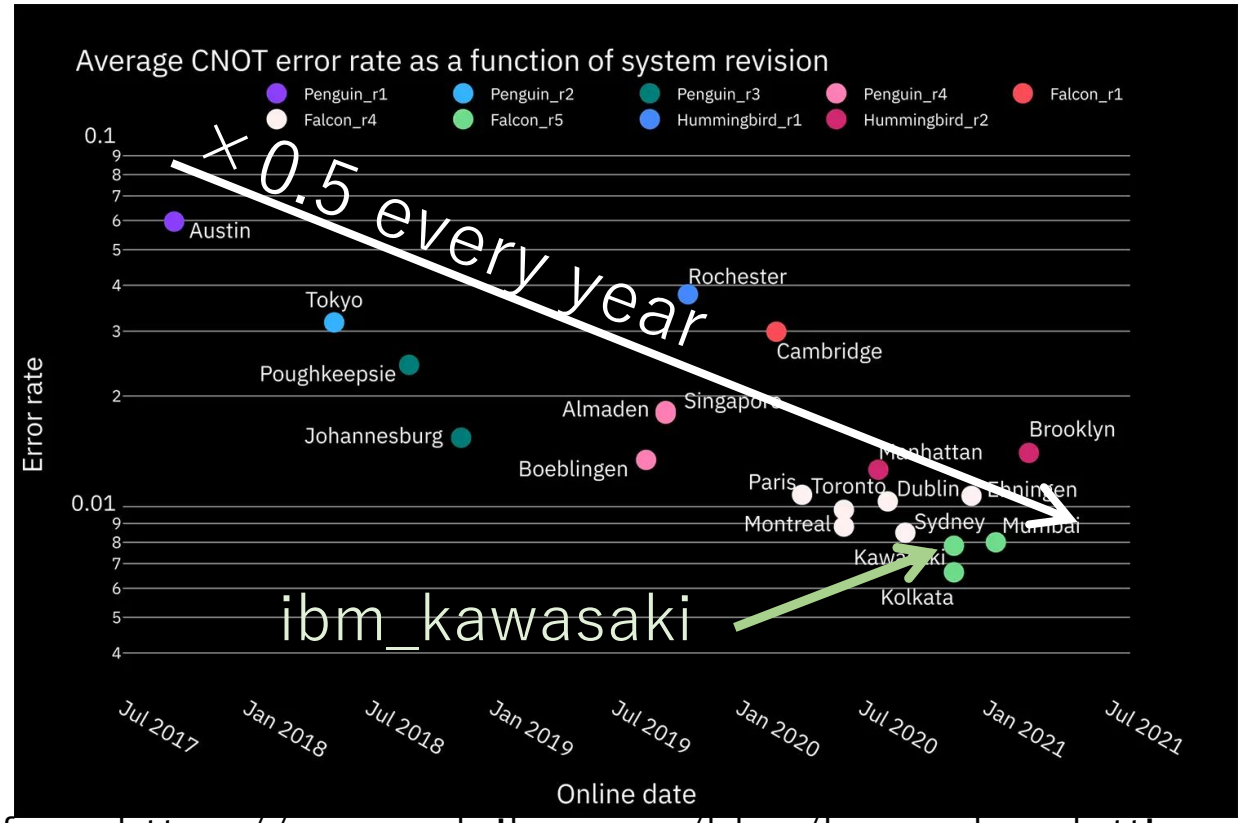
$2^z \equiv 2 \bmod 3$ はいつ解けるのか？

✔ノイズが今の半分なると『解けた』と宣言できる
- いつ半分になるのかを予測

✔ IBMの量子プロセッサはCNOTゲートのエラーレートを公開している
  - 過去５年間の実績として
    毎年エラーレートが半減

✯エラーレートを半分にするには
１年待てば良い

✯前頁の実験は2021年7月に
ibm_kawasakiを用いたもの



Picture from https://research.ibm.com/blog/heavy-hex-lattice

さらに遠い将来予測のために

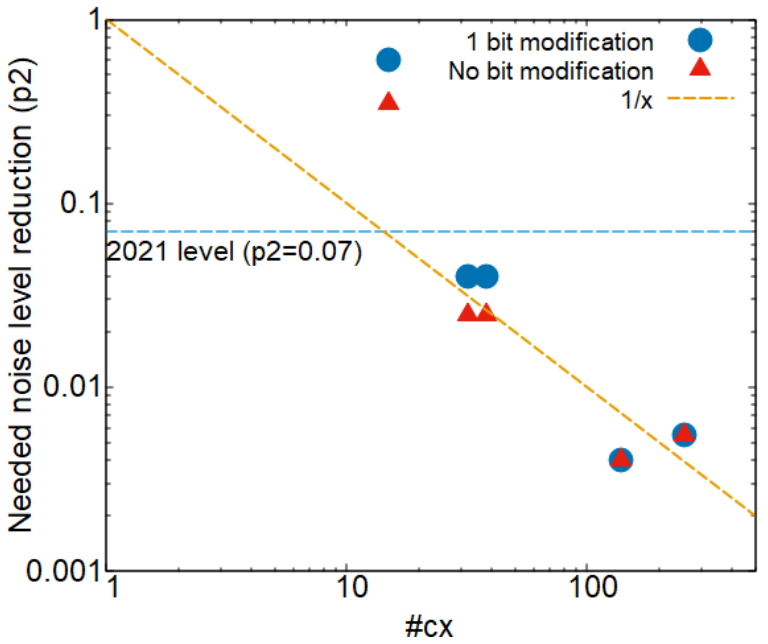
🌟色々な仮定を盛り込む必要がある

🌟シミュレーション上でのCNOTエラー率と
トランスパイル後のCNOTゲート数の関係の傾向

$$\text{CNOT ゲートエラー} < \frac{1}{\text{CNOT ゲート数}} \quad \Rightarrow \quad \text{解ける}$$

✔解釈：回路中1か所でもエラーが起きると，
後処理アルゴリズムが正しい答えを出さなくなる

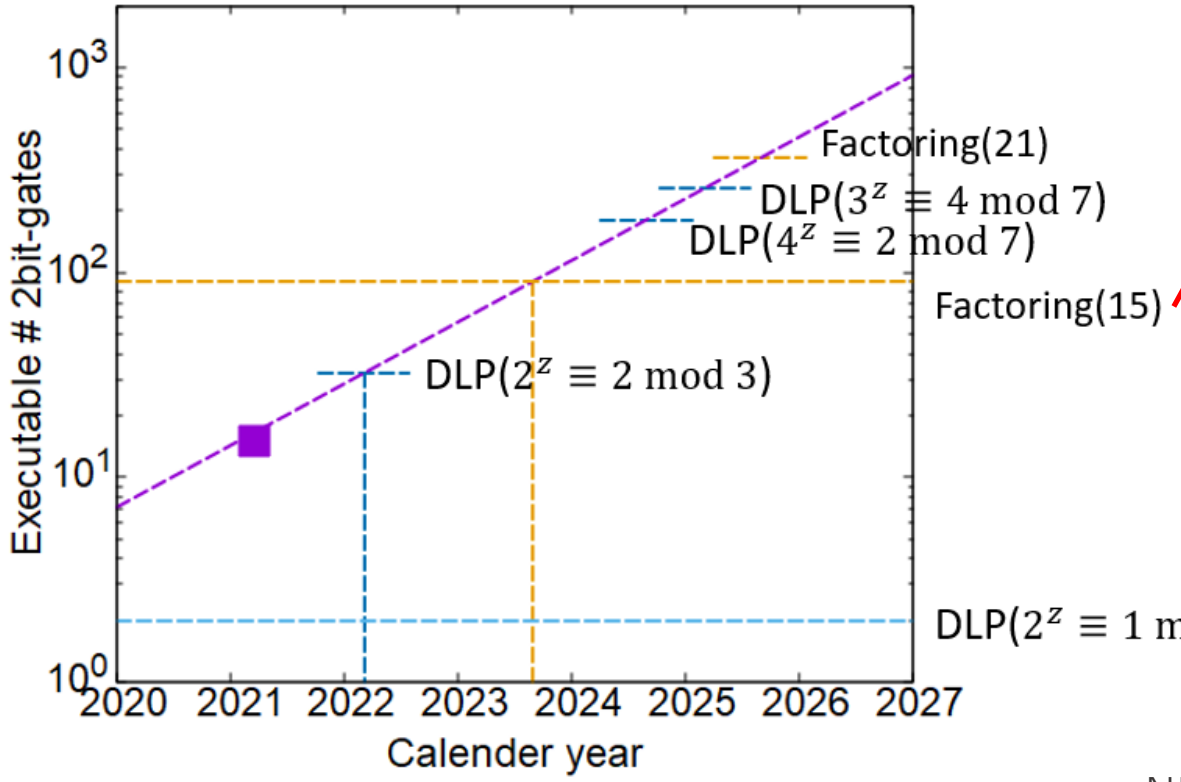
🌟毎年ノイズが半減⇒実行可能な回路規模が毎年倍増
　△搭載量子ビットによる制約は考えない

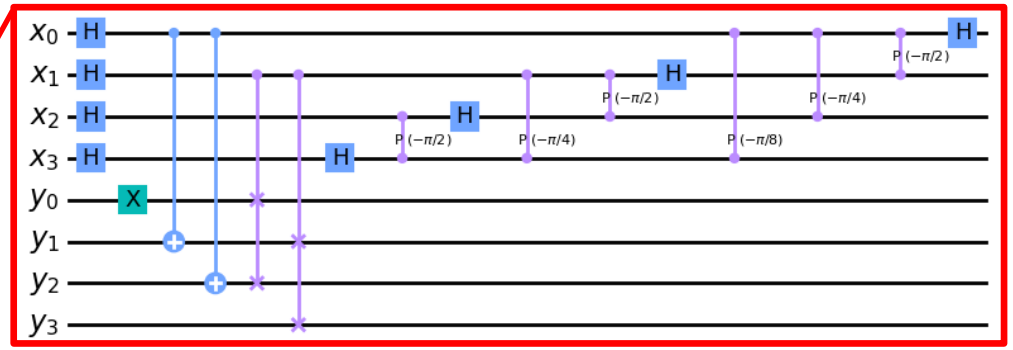


Aono et al., IEEE TQE (2022-3), Fig. 11

近未来予想

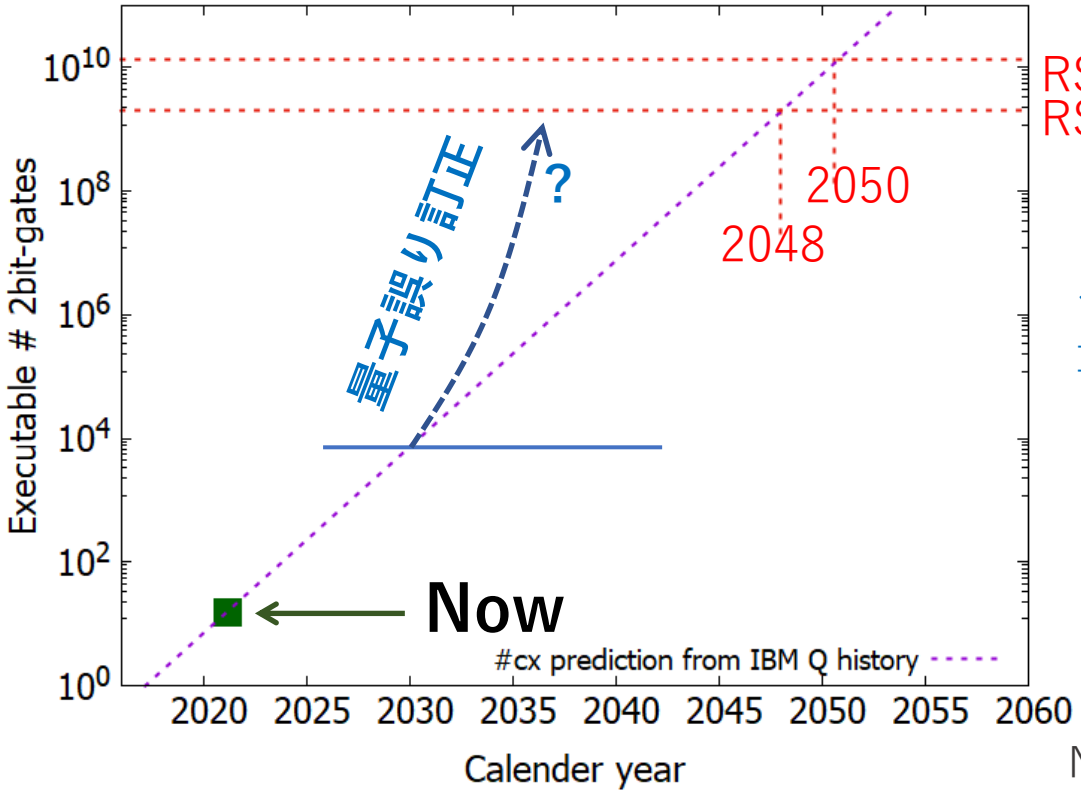
- トランスパイル後の実行可能CNOTゲート数は2021年7月リリースのibm_kawasakiで大体1/0.07=14
  - これが単純に1年で2倍になると仮定
- 教科書的な15の素因数分解回路（数値表現4量子,QFT4量子,#CNOT=86）がそろそろ実行可能になるか？





遠い将来の予想

- ★Gidney-Ekerå(2019)によると、RSA-2048を解くためには大体1.35×10^{10}のCNOTゲート
- ✔トランスパイルによる増大が無いと仮定しても大体2050年前後
- △不確定要素がかなり多い
  - Q-dayを遅らせる要因：物理的な限界
  - 早める要因：量子誤り訂正、量子メモリ、アルゴリズムの改良



RSA-2048
RSA-1024
RSA暗号の量子解読計算量
[Gidney-Ekerå, 2019]

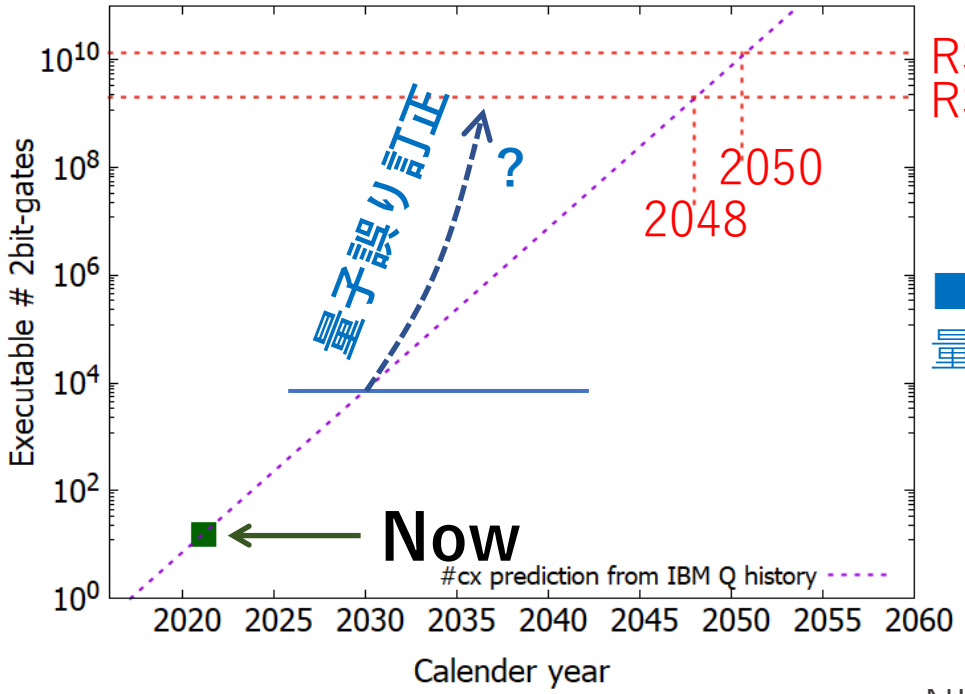
★量子誤り率が10^{-3}～10^{-4}程度まで下がると
量子誤り訂正が効いてくるため、加速する可能性

※量子プロセッサのCNOTゲートエラーが
1年ごとに半分になるトレンドが長期間続くと
仮定したときの予測

まとめ

★量子コンピュータと暗号に関する研究活動の調査
- 量子コンピュータの大規模化により、公開鍵暗号が危殆化、共通鍵暗号・ハッシュ関数にも影響
- 量子コンピュータの性能進化に関する将来予測が重要だが、単位のスタンダードはまだない

★量子コンピュータを用いた離散対数問題の計算実験と将来予測
- 現在の量子CでShorのアルゴリズムを実行するためには、何らかの簡略化を使う必要がある
- ノイズが1年で半分になる等の仮定から将来予測をすると、RSA-2048は2050年ごろに解かれる



RSA-2048
RSA-1024
} RSA暗号の量子解読計算量 [Gidney-Ekerå, 2019]

■量子誤り率が10^{-3}～10^{-4}程度まで下がると量子誤り訂正が効いてくるため、加速する可能性

※量子プロセッサのCNOTゲートエラーが1年ごとに半分になるトレンドが長期間続くと仮定したときの予測

ご清聴ありがとうございました

参考文献一覧

■pp.4-5に関する資料

- Shorによる素因数分解と離散対数問題の量子多項式時間アルゴリズム

Peter W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer
https://arxiv.org/abs/quant-ph/9508027

- Groverによる量子探索アルゴリズム:

Lov K. Grover, A fast quantum mechanical algorithm for database search
https://arxiv.org/abs/quant-ph/9605043

- 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、最終更新2022/04/30）

https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r7.pdf

■p.5の量子コンピュータの大型化による共通鍵暗号への影響に関する議論

- ESTI, Limits to Quantum Computing applied to symmetric key sizes, ETSI GR QSC 006 V1.1.1 (2017-02)

https://www.etsi.org/deliver/etsi_gr/QSC/001_099/006/01.01.01_60/gr_qsc006v010101p.pdf

- CRYPTREC技術報告書「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」(2019)

https://www.cryptrec.go.jp/exreport/cryptrec-ex-2901-2019.pdf

■p.6のShor,Grover以外の量子アルゴリズムが暗号に与える影響に関する文献

- Y. Aono et al. Quantum Lattice Enumeration and Tweaking Discrete Pruning, https://eprint.iacr.org/2018/546
- Andrew M. Childs, David Jao, Vladimir Soukharev, Constructing elliptic curve isogenies in quantum subexponential time, https://arxiv.org/pdf/1012.4019.pdf

参考文献一覧

■p.6の耐量子計算機暗号の公募に関する資料

- NIST Post-Quantum Cryptography PQC, https://csrc.nist.gov/Projects/post-quantum-cryptography
- CACR 全国密码算法设计竞赛通知, https://sfjs.cacrnet.org.cn/site/content/309.html
- KpqC Competition, https://kpqc.or.kr/

■p.6の耐量子計算機暗号の標準化に関する資料

- NIST Post-Quantum Cryptography PQC, https://csrc.nist.gov/Projects/post-quantum-cryptography
- ETSI Quantum-Safe Cryptography (QSC), https://www.etsi.org/technologies/quantum-safe-cryptography
- IETF https://trac.ietf.org/trac/sec/wiki/PQCAgility

■p.6の耐量子計算機暗号への移行に関する資料

- ETSI releases migration strategies and recommendations for Quantum-Safe schemes, https://www.etsi.org/newsroom/press-releases/1805-2020-08-etsi-releases-migration-strategies-and-recommendations-for-quantum-safe-schemes
- NIST Migration to Post-Quantum Cryptography, https://csrc.nist.gov/publications/detail/white-paper/2021/08/04/migration-to-post-quantum-cryptography/final

参考文献一覧

■p.6の耐量子計算機暗号に関するガイドラインに関する資料

- CRYPTREC,耐量子計算機暗号の研究動向調査報告書, https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2018.pdf
- NSA, Announcing the Commercial National Security Algorithm Suite 2.0, https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
- BSI TR-02102-1: "Cryptographic Mechanisms: Recommendations and Key Lengths" Version: 2023-1, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?_blob=publicationFile&v=6
- ANSSI views on the Post-Quantum Cryptography transition, https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/

■p.7のタイムラインに関する資料

- Michele Mosca, Cybersecurity in a Quantum World: will we be ready? https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf, 2015
- Michele Mosca and Marco Piani, 2021 Quantum Threat Timeline Report: Global Risk Institute, https://globalriskinstitute.org/publication/2021-quantum-threat-timeline-report-global-risk-institute-global-risk-institute/

■p.8: Metaculus内の量子コンピュータがRSAを破る日付の予想

- https://www.metaculus.com/questions/3684/when-will-a-quantum-computer-running-shors-algorithm-or-a-similar-one-be-used-to-factor-one-of-the-rsa-numbers-for-the-first-time/

参考文献一覧

■p.9-11の専門家の予測に関する資料

- Matteo Mariantoni, Building a Superconducting Quantum Computer, PQCrypto 2014 invited talk
- Michele Mosca, Cybersecurity in a Quantum World: will we be ready?

https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf, 2015

- Michele Mosca and Marco Piani, 2021 Quantum Threat Timeline Report: Global Risk Institute,

https://globalriskinstitute.org/publication/2021-quantum-threat-timeline-report-global-risk-institute-global-risk-institute/

- 科学技術・学術政策研究所科学技術予測センター, 第11回科学技術予測調査 デルファイ調査
- Emily Grumbling and Mark Horowitz, 米国科学・工学・医学アカデミーによる量子コンピュータの進歩と展望 (西森 秀稔 翻訳)

■p.12の過去の実績からの外挿に関する資料

- Jaime Sevilla and C. Jess Riedel, Forecasting timelines of quantum computing, arXiv:2009.05045, https://arxiv.org/abs/2009.05045
- Tilman Runge, Dismantling the Quantum Threat, Master Thesis, 2022
- Aono et al., The present and future of discrete logarithm problems on noisy quantum computers, IEEE TQE 2022-3

■p.13のグラフ参照先

- CRYPTREC Report 2021, https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2021.pdf

参考文献一覧

■p.14の単位に関する参考文献

- 量子ビットのロードマップに関するまとめは例えばhttps://www.adlittle.com/de/node/24039
- IBMによるCNOTゲートの実績　https://research.ibm.com/blog/heavy-hex-lattice
- 量子体積の提案論文はAndrew W. Cross et al., Validating quantum computers using randomized model circuits, Phys. Rev. A 100-3, (2019). また、実績とロードマップに関しては https://research.ibm.com/blog/quantum-volume-256
- Q-score: Simon Martiel, Thomas Ayral, Cyril Allouche, Benchmarking quantum co-processors in an application-centric, hardware-agnostic and scalable way, IEEE-TQE, 2 (2021)
- Generalized logical circuit: Jaime Sevilla and C. Jess Riedel, Forecasting timelines of quantum computing, arXiv:2009.05045, https://arxiv.org/abs/2009.05045
- Yulong Dong, Lin Lin, Random circuit block-encoded matrix and a proposal of quantum LINPACK benchmark, PQA 103-6
- Ang Li et al.,QASMBench: A Low-Level Quantum Benchmark Suite for NISQ Evaluation and Simulation, ACM Transactions on Quantum Computing
- Algorithmic Qubits: A Better Single-Number Metric, https://ionq.com/posts/february-23-2022-algorithmic-qubits
- SupermarQ: https://www.super.tech/supermarq/

■p.15の素因数分解，離散対数問題の必要量子ビットに関する参考文献

Yasuhiro Takahashi and Noboru Kunihiro, A quantum circuit for shor's factoring algorithm using 2n + 2 qubits, Quantum Information & Computation, 6, 2 (2006)

Häner et al., Factoring using 2n + 2 qubits with Toffoli based modular multiplication, Quantum Information & ComputationVolume 17, 7-8 (2017)

参考文献一覧

■p.16の素因数分解履歴に関する参考文献
- Shorのアルゴリズムのサーベイ: CRYPTREC 外部評価報告書『Shorのアルゴリズム実装動向調査』 https://www.cryptrec.go.jp/exreport/cryptrec-ex-3005-2020.pdf
- アニーリングによる素因数分解記録は主に以下を参考とした:山口, 伊豆, イジング計算を用いた暗号解析について, オペレーションズ・リサーチ, 2022-06

■p.17の具体的な回路に関しては個々の論文を参照した
- Vandersypen et al.,Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance, Nature, 414, 6866 (2001)
- Lucero et al., Computing prime factors with a Josephson phase qubit quantum processor, Nature Physics, 8, 10 (2012)
- Amico et al., Experimental study of Shor's factoring algorithm using the IBM Q Experience, PRA 100-1 (2019)
- Skosana and Tame, Demonstration of Shor's factoring algorithm for N=21 on IBM quantum processors (2021)

■p.19以降の内容は主に以下の論文による
- Aono et al.,超電導量子回路を用いた離散対数問題の求解実験, QIT43(2020)
- Aono et al., The present and future of discrete logarithm problems on noisy quantum computers, IEEE TQE 2022-3

■p.22 量子コンピュータの写真は以下のサイトから取得した
https://www.flickr.com/photos/ibm_research_zurich/51331567650/in/album-72157703845574031/

■p.24の成功条件を中間値とすることに関しては、以下の先行研究をフォローした
- Andrew W. Cross et al., Validating quantum computers using randomized model circuits, Phys. Rev. A 100-3, (2019)
- T. Satoh, Y. Ohkura, and R. Van Meter, Subdivided phase oracle for NISQ search algorithms, IEEE-TQE, 1 (2020)

■p.27のCNOTゲートの実績はhttps://research.ibm.com/blog/heavy-hex-lattice