暗号技術検討会
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４回（2020年度第１回））

令和３年３月３日
１０:００～１２:００
オンライン開催

議事次第

１　開会

２　議題

（１）本年度の検討内容等について

（２）量子コンピュータに関する動向等について

（３）量子コンピュータに対する暗号技術の動向等について

（４）CRYPTREC暗号リストでの推奨候補暗号リストの取扱いについて

（５）その他

３　閉会

配付資料一覧

資料１　これまでの議論と本年度の検討内容について

資料２　量子コンピューティング最前線

資料３　耐量子計算機暗号の動向等について

資料４　量子コンピュータにおける素因数分解の評価について

資料５　量子コンピュータにおける離散対数問題の求解実験について

資料６　CRYPTREC暗号リストでの推奨候補暗号リストの取扱いについて

参考資料　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)

CRYPTREC
Cryptography Research and Evaluation Committees

資料1

これまでの議論と
本年度の検討内容について

令和３年３月３日
CRYPTREC事務局

CRYPTREC
Cryptography Research and Evaluation Committees

2019年度のＴＦ検討状況（量子コンピュータ等関係）

量子コンピュータ等の技術動向

- ✓ 量子コンピュータの**現状の規模（量子ビット数）は50程度**だが、**暗号解読には数千程度以上**が必要。
- ✓ 量子コンピュータの性能は、量子ビット数に加えて、**ノイズ（計算誤り）**や**演算可能回数**も重要な指標。
- ✓ 現状は**ノイズ（誤り）等の問題があり**、規模だけ拡大しても**暗号解読に活用できる水準**ではない。

→ **現状の暗号技術が近い将来に危殆化する可能性は低い**旨、2020年２月に公表・周知した。
https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2019.html

耐量子計算機暗号（PQC）の技術動向

- ✓ 米国NIST（国立標準技術研究所）が標準化作業中で、2022～2024年に標準化ドラフトが策定予定。

CRYPTREC暗号リスト（電子政府推奨暗号リスト）における位置付けについて

- ✓ **CRYPTREC暗号リスト**は、利用環境によらない安全性の評価に加え、**利用実績等も考慮**して作成。
- ✓ **PQC**は、**多数の方式が提案**され安全性を検討している段階で、利用実績等に言及できる段階ではない。
- ✓ 今後、利用が拡大すると想定される、IoT機器等に用いられる「**軽量暗号**」や、暗号状態で情報処理が可能な「**高機能暗号**」は、**利用環境やアプリケーションが限定**され、従来暗号とは取り扱いが異なる。

→ **PQC**、**軽量暗号**、**高機能暗号**は、CRYPTREC暗号リストに組み込まず、**別途ガイドライン**を作成する。
（暗号技術評価委員会にて、CRYPTREC暗号リストの改定作業（2022年度末目途）と並行して実施予定）

タスクフォースの今後の取組

- ✓ **量子コンピュータやPQCの状況をフォロー**するため、2020年度以降も**タスクフォースを継続して開催**。

2019年度のＴＦ検討状況（CRYPTREC暗号リスト関係）

CRYPTREC暗号リストの構成

- ✓ CRYPTREC暗号リストは、次の３リスト構成となっている。
  - **①電子政府推奨暗号リスト**（安全性・実装性能が確認され、利用実績や普及見込みがあると判断されたもの）
  - **②推奨候補暗号リスト**（安全性・実装性能が確認され、今後①のリストに掲載される可能性のあるもの）
  - **③運用監視暗号リスト**（危殆化等により推奨すべき状態ではなく、互換性維持のために継続利用を容認するもの）
- ✓ ①と③のリストは維持するものの、**②のリスト**には掲載から十分な期間を経ても普及したとは言えない暗号技術もあり、その**必要性等について、引き続き検討が必要**。
- ✓ 各暗号技術は十分成熟しているため、技術分類は変更せず、新たな暗号技術の公募も実施しない。

暗号技術のパラメータ

- ✓ CRYPTREC暗号リストでは推奨する暗号技術（暗号アルゴリズム）を示してきたが、パラメータは提示していない。
- ✓ 推奨パラメータの明示は、安全なシステム構築や計画的な暗号技術の移行を促進するために有用。

→ **推奨パラメータを規定する別の文書を新たに作成**する。（CRYPTREC暗号リストから当該文書を参照する構成とする。）
（暗号技術活用委員会にて作成に向けた検討を実施中）

CRYPTREC暗号リストの今後の改定

- ✓ 2003年に作成、2013年に改定を行い、今般、2023年目途に改定作業中であり、10年単位で改定。
- ✓ 常に危殆化等の監視を行い、必要に応じた暗号技術の加除等も行っており、10年単位とする必要もない。

→ 次の改定以後は、改定後５年以内を目途に暗号技術検討会において改定是非を判断することとする。

今後に向けた取組

- ✓ **CRYPTREC暗号リストの構成等について議論するため、**2020年度以降も**タスクフォースを継続して開催。**

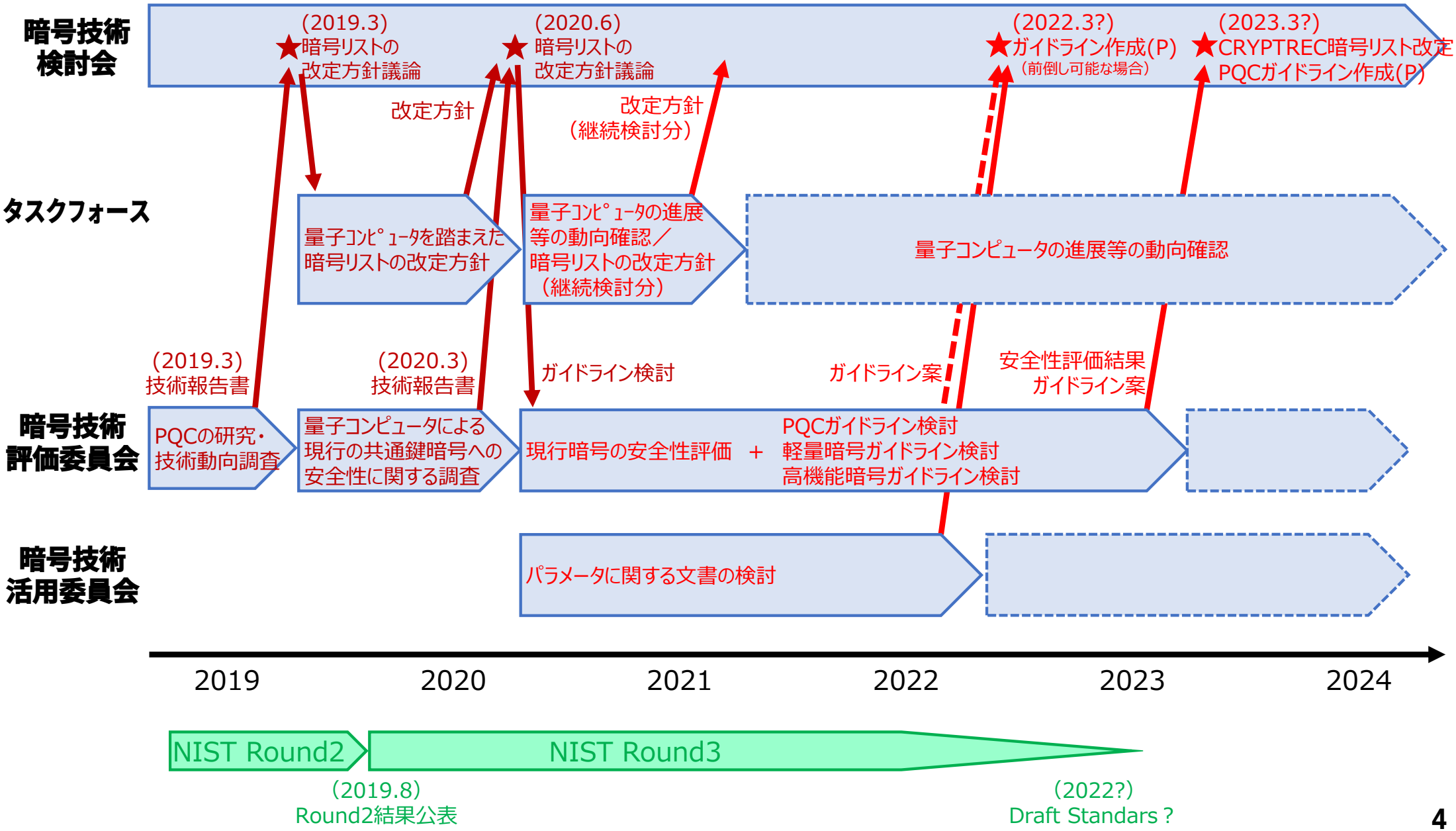
2019年度のタスクフォースの検討結果を受けた対応

暗号技術検討会(2020年度第１回)決定事項

CRYPTREC暗号リストの在り方及び暗号技術の動向等について、次のように取り扱う。

1　耐量子計算機暗号、軽量暗号、高機能暗号について、CRYPTREC暗号リストには含めず、それぞれ別の文書とする。また、当該文書の重要性がわかるよう、取りまとめたものとする。	暗号技術評価委員会にてガイドライン作成検討中
2　2023年目途のCRYPTREC暗号リストの改定について、現行の３リスト構成の在り方については引き続き検討することとする。また、技術分類については現行のものを踏襲し、公募は行わない方針とする。	**本年度のタスクフォースにおいて議論**
3　推奨される暗号のパラメータについて、CRYPTREC暗号リストから参照する形で別の文書としてまとめる方針とする。	暗号技術活用委員会にて該当文書作成検討中
4　１及び３に係る新たな文書も含め、CRYPTREC暗号リストを含むCRYPTRECの文書の位置付けを整理する。	該当文書の作成検討と併せて検討予定
5　量子コンピュータや耐量子計算機暗号の状況をフォローするため、及び引き続き継続検討とした内容の議論を行うため、2020年度以降もタスクフォースを継続設置する。	**本年度のタスクフォースにおいて議論**

全体スケジュール（イメージ）



量子コンピューティング最前線

伊藤公平

慶應義塾大学 理工学部
慶應義塾大学IBM Q Network Hub @ Keio ファウンダー

文科省 光・量子飛躍フラッグシッププログラム（Q-LEAP ）
量子情報処理分野プログラムディレクタ（PD）
JSTさきがけ「量子の状態制御と機能化」領域総括

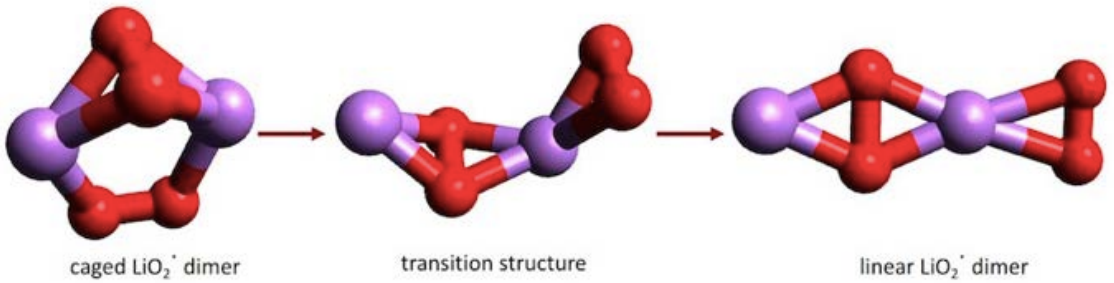
古典コンピュータで不可能な問題

極めて大きな場合の数を含む計算

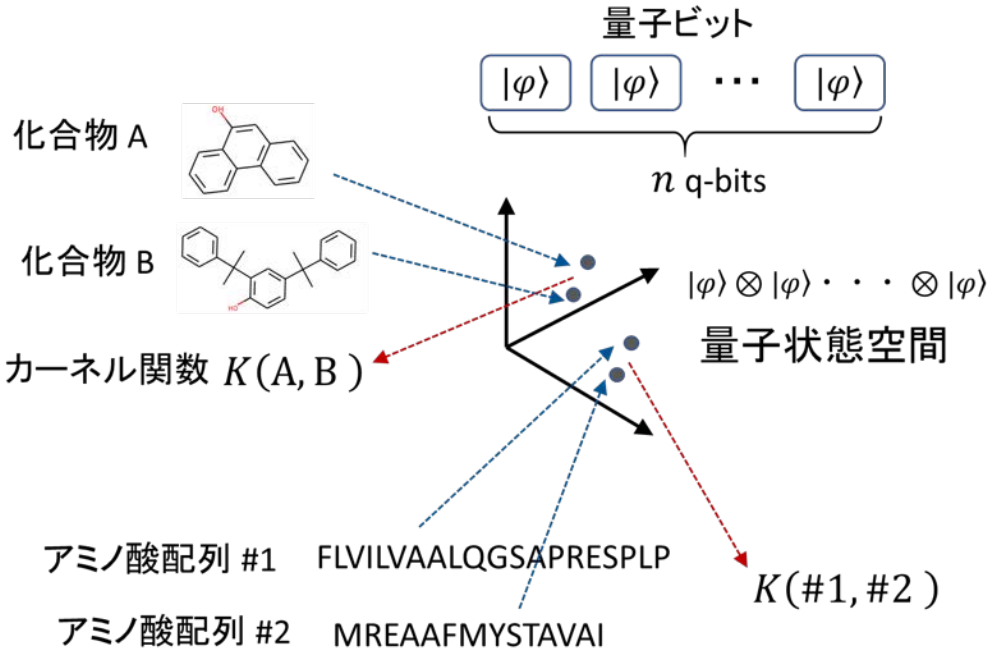
例：六本木ミッドタウンから日比谷ミッドタウンへの最適ルート探し

コンピュータで不可能な問題

量子物質の構造・反応計算や機械学習による分類分け



量子空間での直接的分類分け：非構造データの量子カーネル関数の開発



量子コンピュータの科学的可能性

- 古典情報（いわゆる世間のビッグデータ）を量子状態に変換する（量子コンピュータに読み込ませる）ためには膨大な計算量が必要となる
- 量子力学に基づく情報（素粒子、原子、分子など）を直接量子ビットで担う（量子状態を量子状態で表す）．科学的可能性としてはそのような計算を量子ビットで実行すべき．（金融、最適化といった産業応用は別問題）

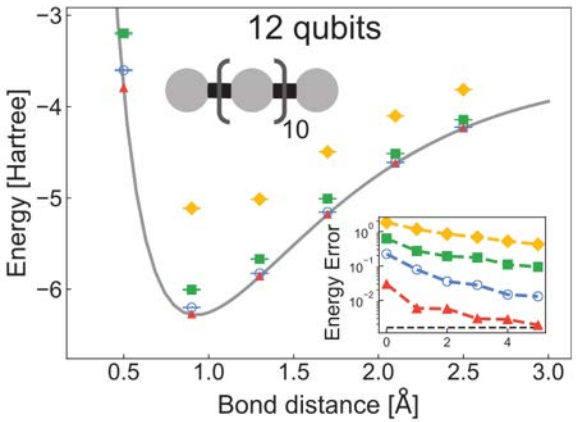
QUANTUM COMPUTING

Rubin *et al.*, *Science* **369**, 1084–1089 (2020) 28 August 2020

Hartree-Fock on a superconducting qubit quantum computer

Google AI Quantum and Collaborators*†

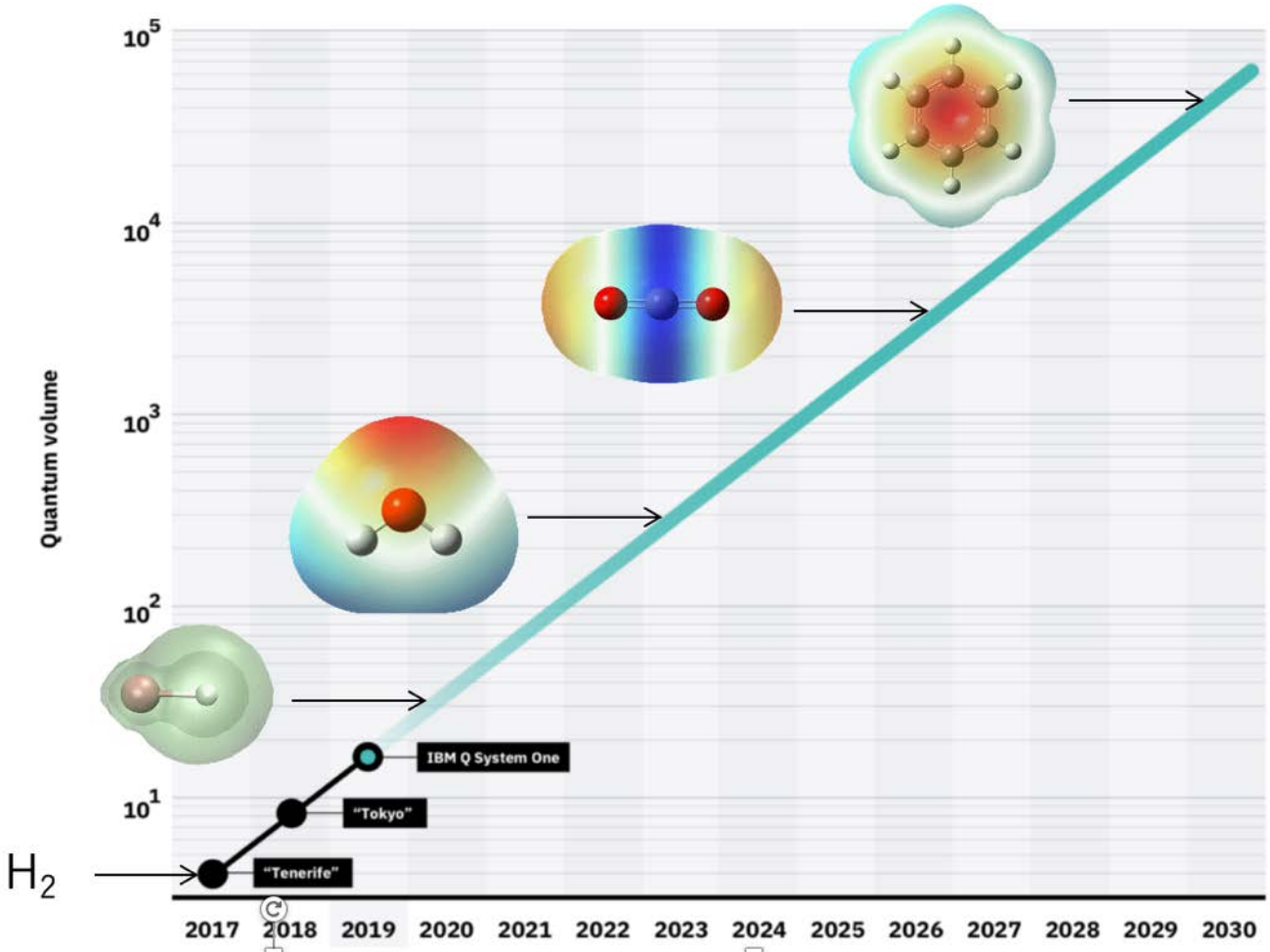
The simulation of fermionic systems is among the most anticipated applications of quantum computing. We performed several quantum simulations of chemistry with up to one dozen qubits, including modeling the isomerization mechanism of diazene. We also demonstrated error-mitigation strategies based on *N*-representability that dramatically improve the effective fidelity of our experiments. Our parameterized



H_{12}分子の結合長

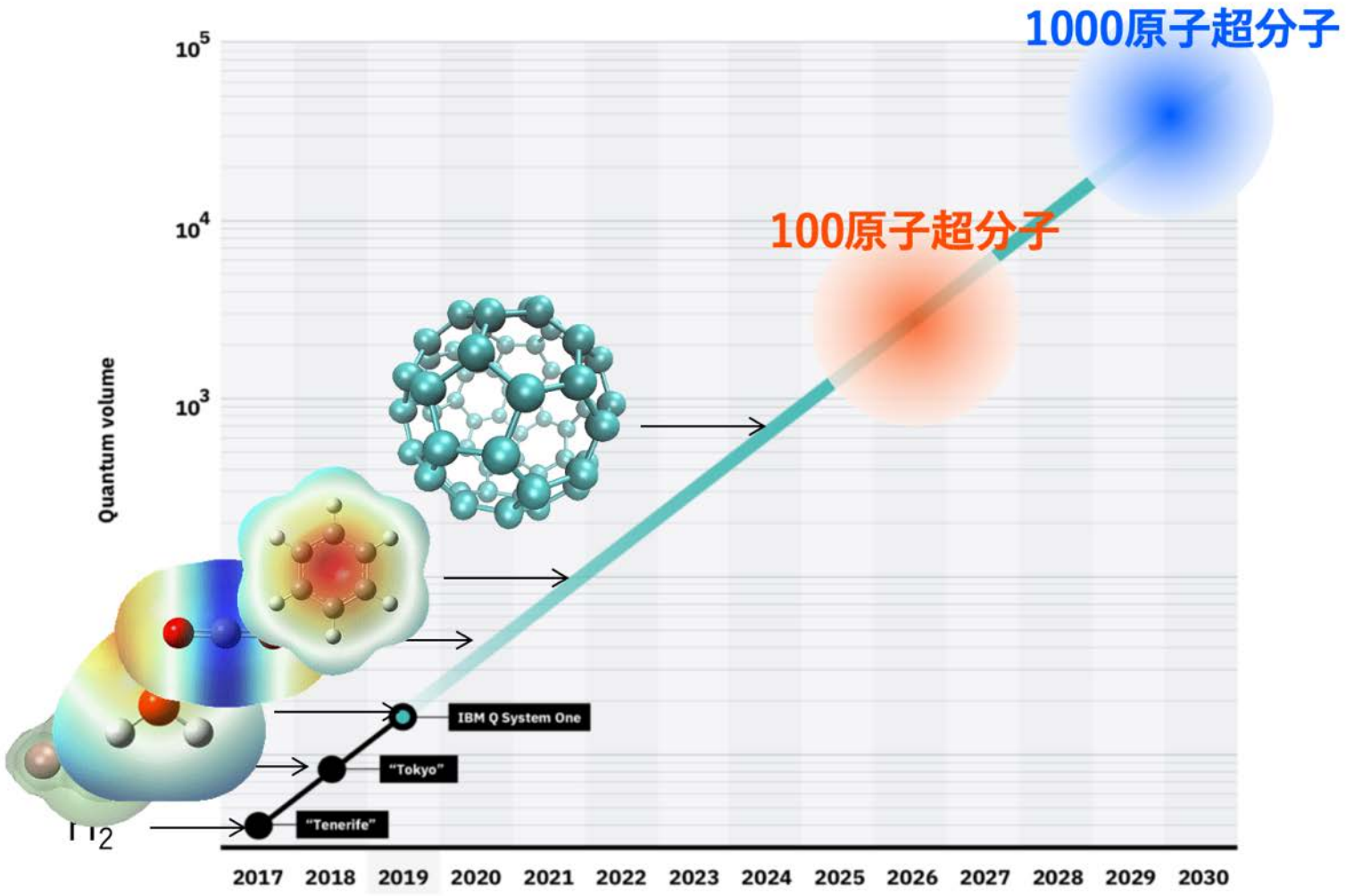
現状の延長では…

Gate Complexity ∝ $O(N^3)$の場合



Exponential Forecast for Growth of Quantum Processing Power
出典：https://www.ibm.com/blogs/research/2019/03/power-quantum-device/

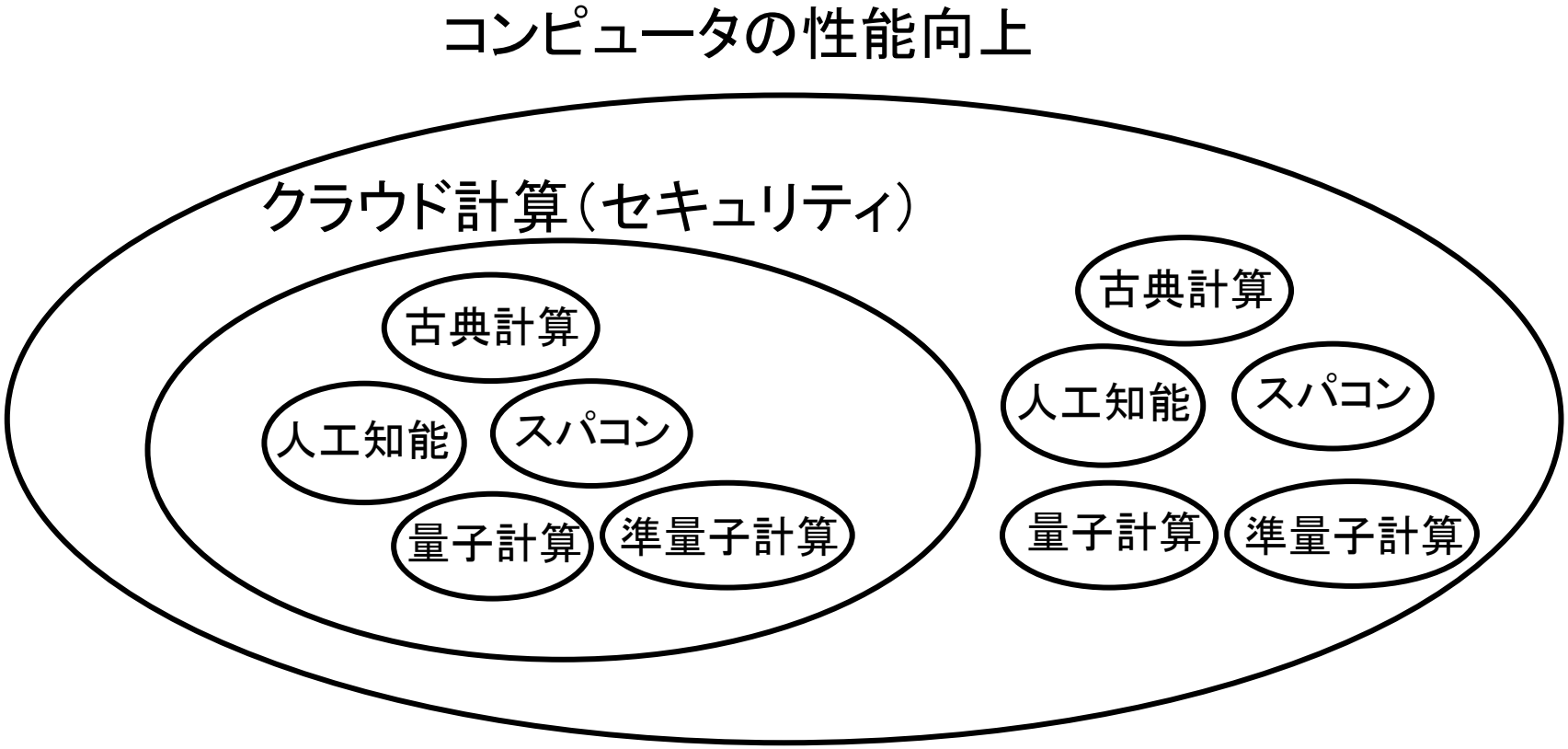
量子ハード・ソフト協調の子育てが必要



Exponential Forecast for Growth of Quantum Processing Power
出典：https://www.ibm.com/blogs/research/2019/03/power-quantum-device/

量子コンピュータの時代？

1. Quantum Leap (Quantum Supremacy)は得られるか？
2. スパコンに勝てる日は来るか？
3. 一社に一台量子コンピュータの時代は来る？



超並列計算(量子並列性)

量子ビット (qubit)

0	0	0	0
0	0	1	1
0	1	0	2
0	1	1	3
1	0	0	4
1	0	1	5
1	1	0	6
1	1	1	7

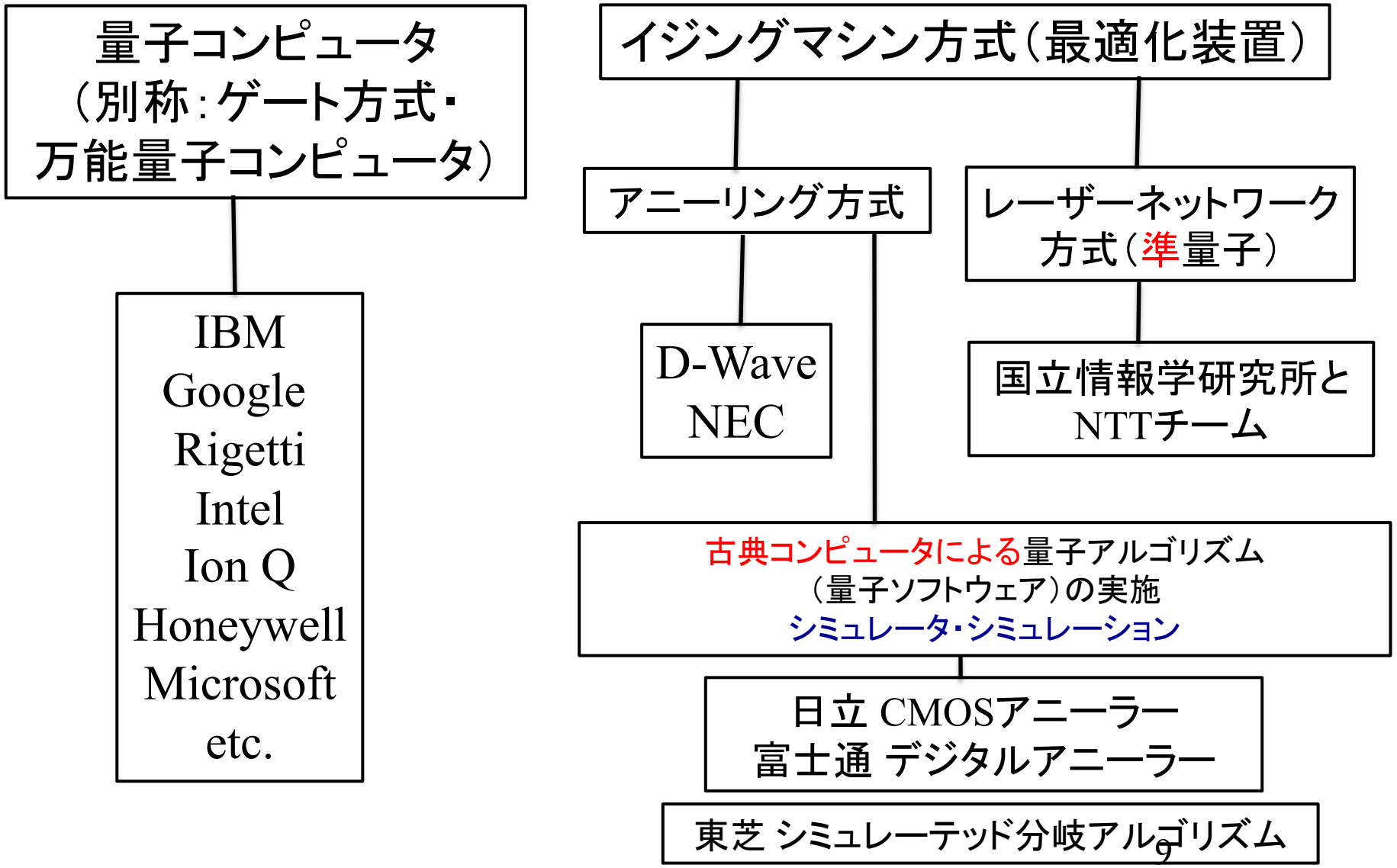
2進数

10進数

2^n通りの数が一気に処理できる

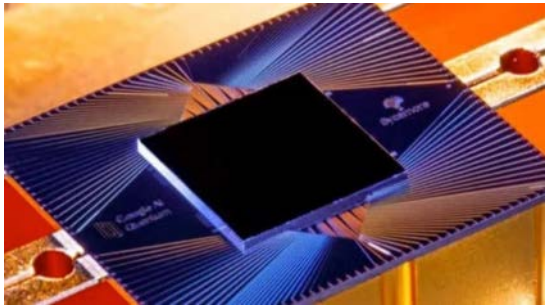
280量子ビット
$\rightarrow 2^{200} \sim 10^{83}$
宇宙の原子数！

量子コンピュータの種類



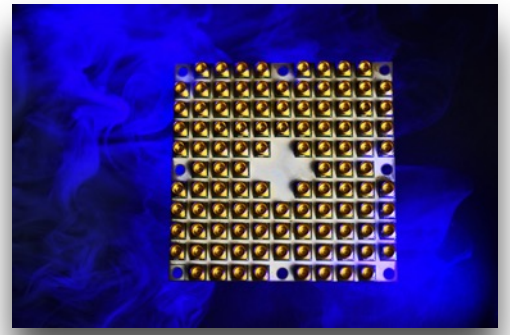
超伝導量子コンピュータ

Google



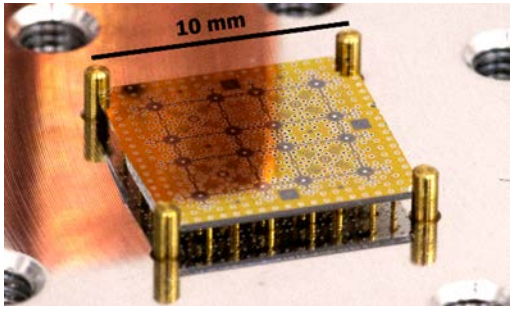
引用： https://gigazine.net/news/20180307-google-new-quantum-processor/

Intel

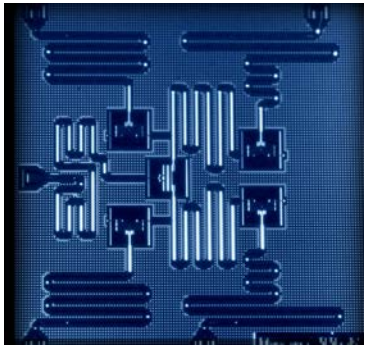


引用： https://www.engadget.com/2018/01/08/intel-s-quantum-computing-efforts-take-a-major-step-forward/

Riken



IBM



引用：https://www.technologyreview.jp/s/62657/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/

Rigetti computing

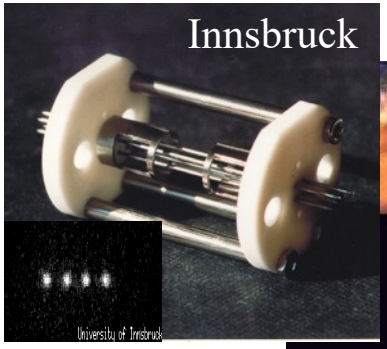
引用： https://www.rigetti.com/

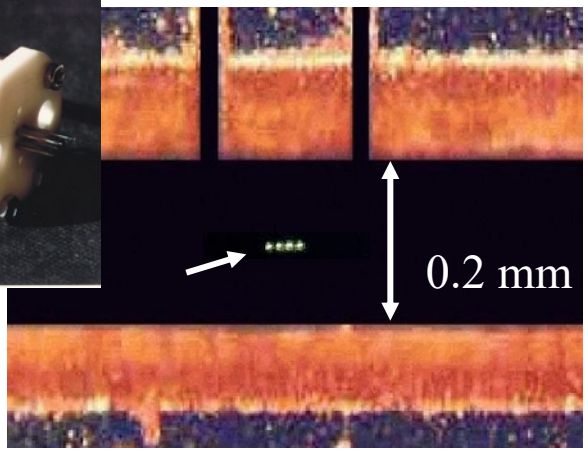
Experimental demonstration of a robust, high-fidelity geometric two ion-qubit phase gate

D. Leibfried*†, B. DeMarco*, V. Meyer*, D. Lucas*‡, M. Barrett*, J. Britton*, W. M. Itano*, B. Jelenković*§, C. Langer*, T. Rosenband* & D. J. Wineland*

* *Time and Frequency Division, National Institute of Standards and Technology, 325 Broadway, Boulder, Colorado 80305, USA*
† *Physics Department, Campus Box 390, University of Colorado, Boulder, Colorado 80309, USA*
‡ *Department of Physics, University of Oxford, Parks Road, Oxford OX1 3PU, UK*
§ *Institute of Physics, PO Box 57, 11001 Belgrade, Serbia-Montenegro*

NATURE | VOL 422 | 27 MARCH 2003

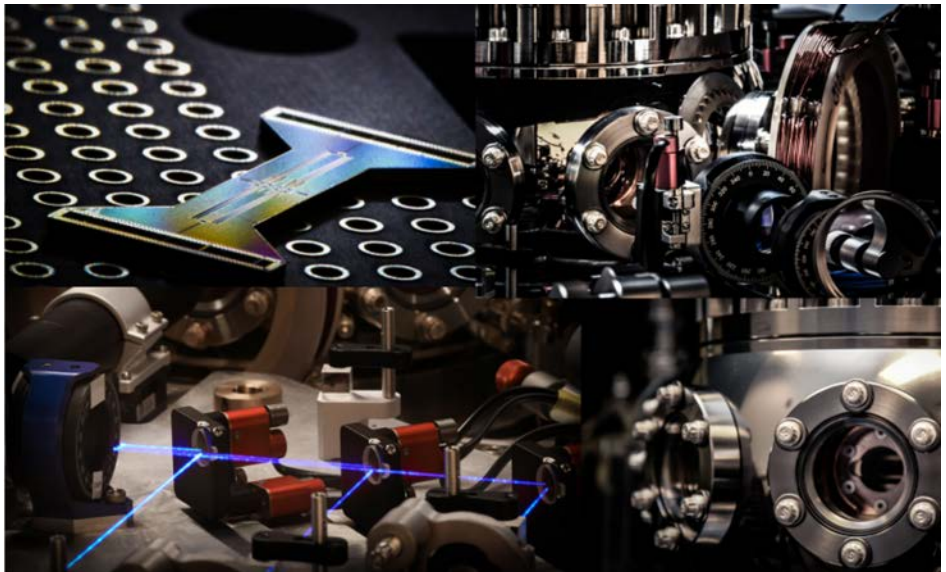




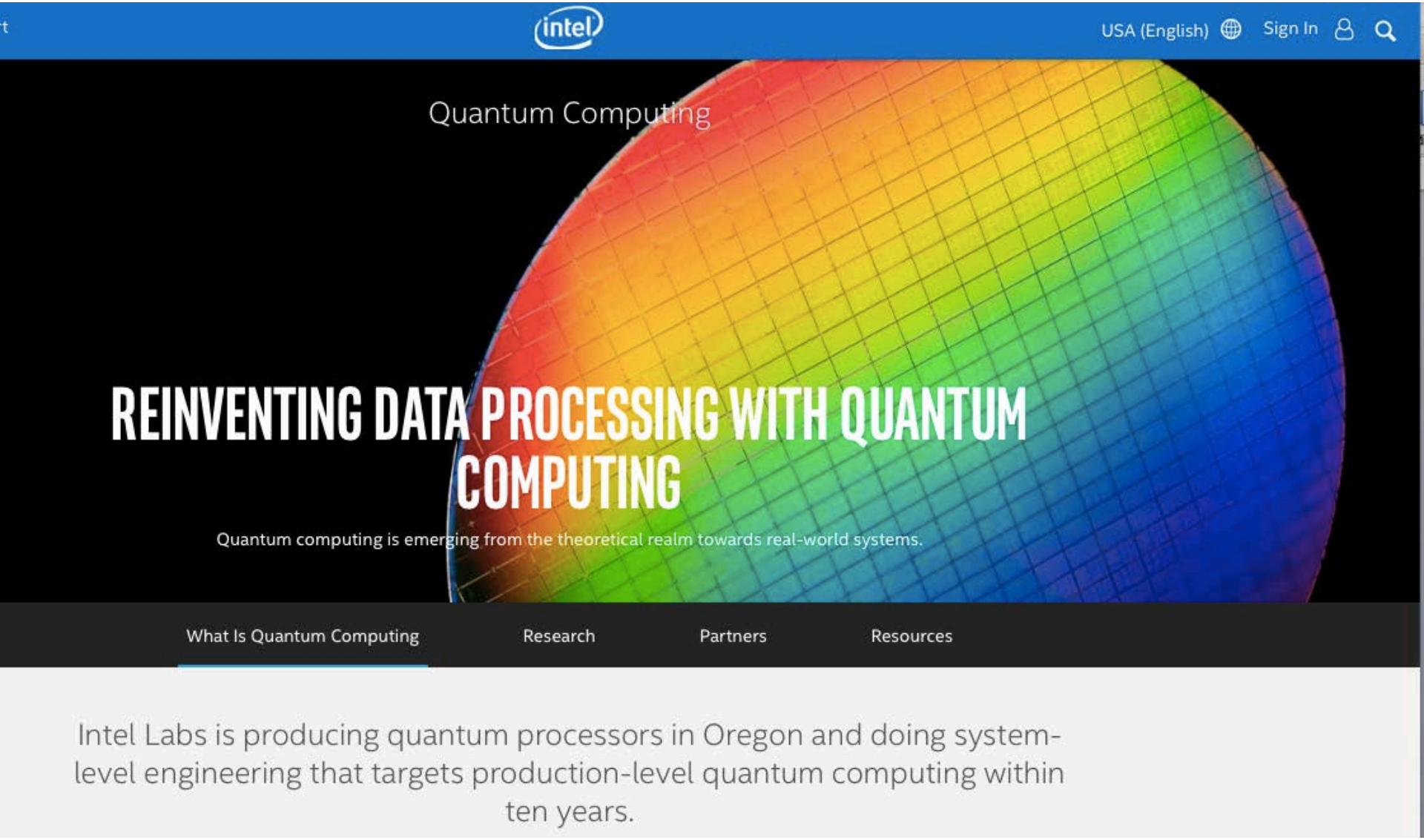
Courtesy D. Wineland, NIST

Honeywell

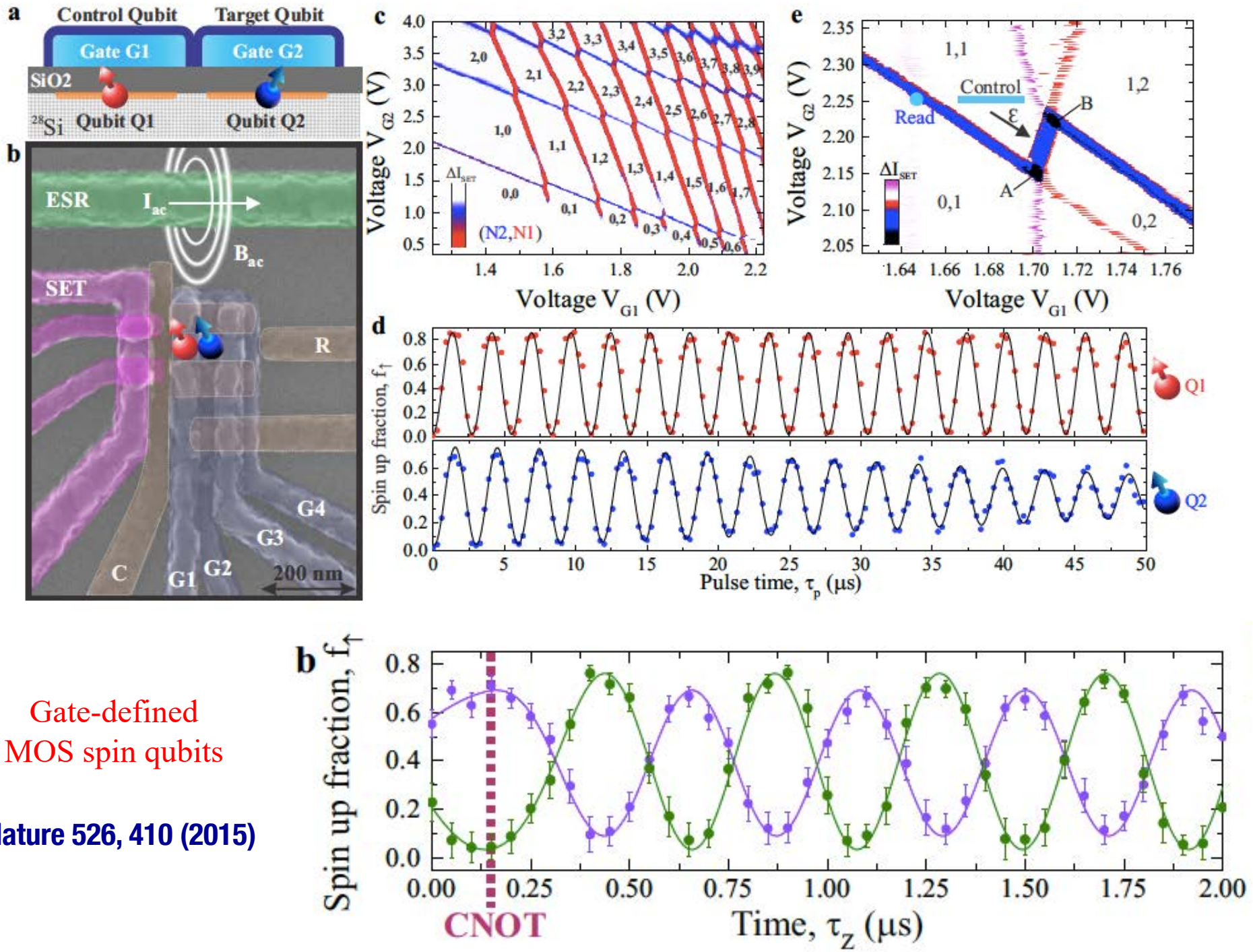
2020



シリコン量子コンピュータ



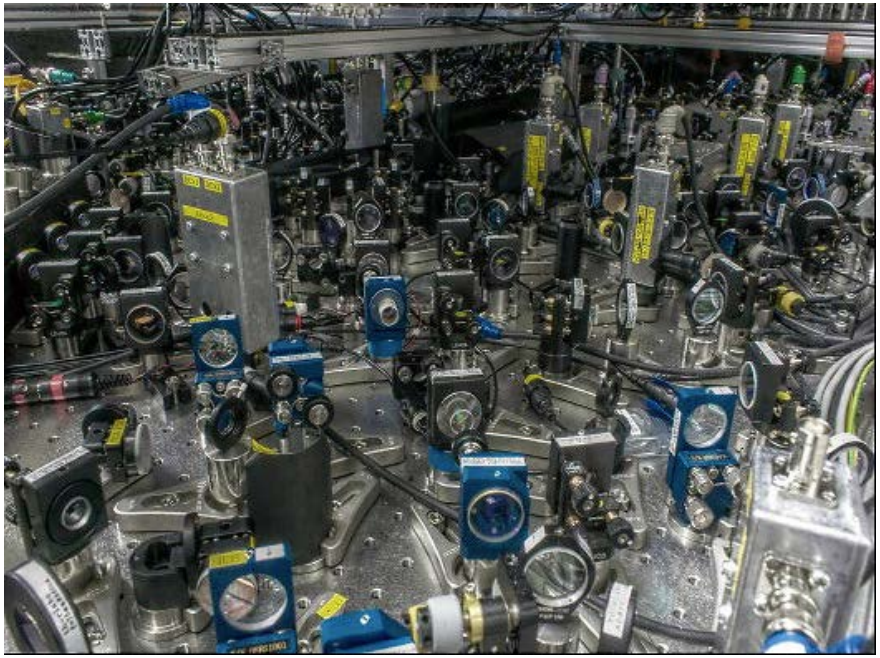
https://www.intel.com/content/www/us/en/research/quantum-computing.html



Gate-defined
MOS spin qubits

Nature 526, 410 (2015)

光量子コンピューティング
東大　古澤明教授

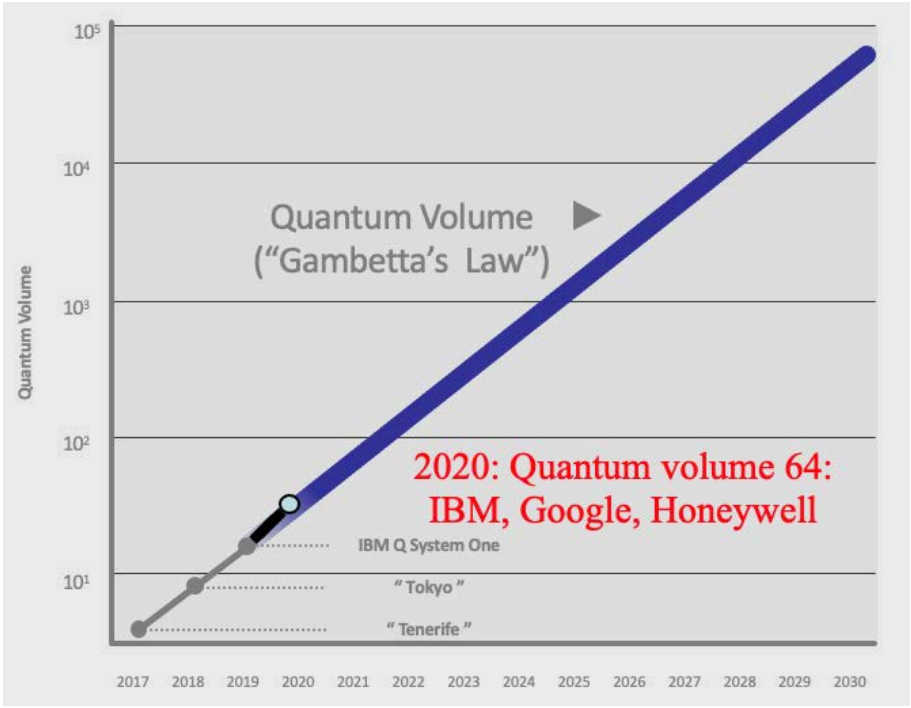


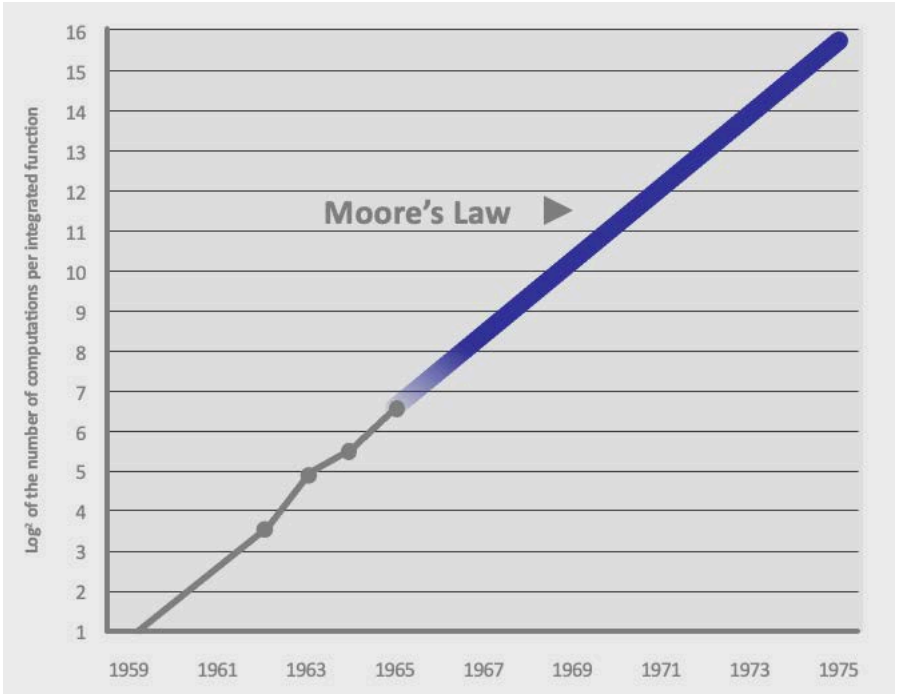
Teleportation of Schrodinger's cat
wave-packets of light
Science, 332, 330 (2011)

Continuous-variable entanglement
on a chip
Nature Photonics, 9, 316 (2015)

量子コンピュータ性能の発展予想

性能指標：Quantum volume
2020年の64は、2の6乗．6つの量子ビットで6段の高精度計算が可
2021年は128 (?)、2の7乗．7つの量子ビットで7段の高精度計算が可





Quantum volumeの決定方法（実際の例）

Example; find the quantum volume of a 27-qubit quantum computer

Success means >2/3 measuring success with >97.725% confidence interval)

Step 1: Try random 2-qubit circuit of depth 2, run it lots of times -> success
Step 2: Try random 3-qubit circuit of depth 3, run it lots of times -> success
Step 3: Try random 4-qubit circuit of depth 4, run it lots of times -> success
Step 4: Try random 5-qubit circuit of depth 5, run it lots of times -> success
Step 5: Try random 6-qubit circuit of depth 6, run it lots of times -> success
Step 6: Try random 7-qubit circuit of depth 7, run it lots of times -> fail

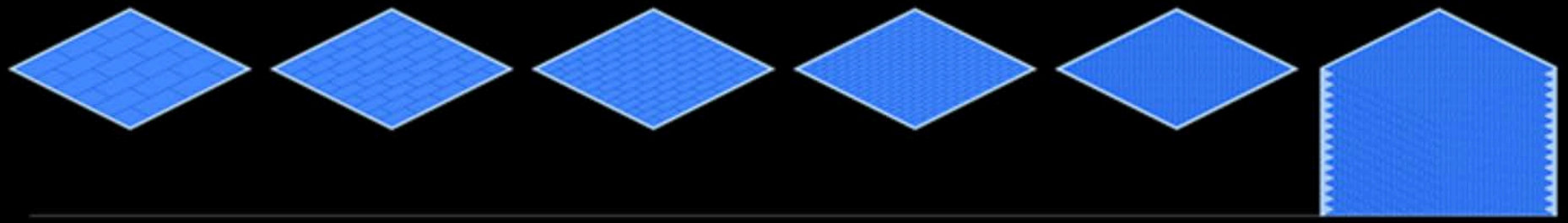
Quantum volume is 2^6=64

Scaling IBM Quantum technology

IBM

IBM Q System One (Released) | (In development) | Next family of IBM Quantum systems

2019	2020	2021	2022	2023	and beyond
27 qubits *Falcon*	65 qubits *Hummingbird*	127 qubits *Eagle*	433 qubits *Osprey*	1,121 qubits *Condor*	Path to 1 million qubits and beyond *Large scale systems*



Key advancement	Key advancement	Key advancement	Key advancement	Key advancement	Key advancement
Optimized lattice	Scalable readout	Novel packaging and controls	Miniaturization of components	Integration	Build new infrastructure, quantum error correction

IBM Q Network Hub @ Keio University

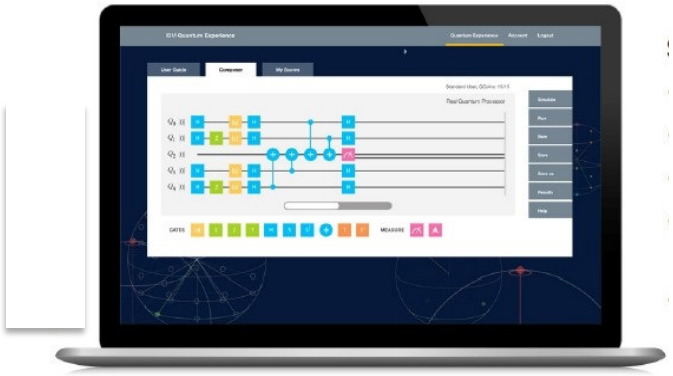
理工学部矢上キャンパス
(Keio Q Hub)

クラウド量子計算

プログラム送信

計算結果

IBMワトソン研究所
(New York)



常に進化し続ける

量子ソフトウェア開発

量子コンピュータ IBM Q 開発

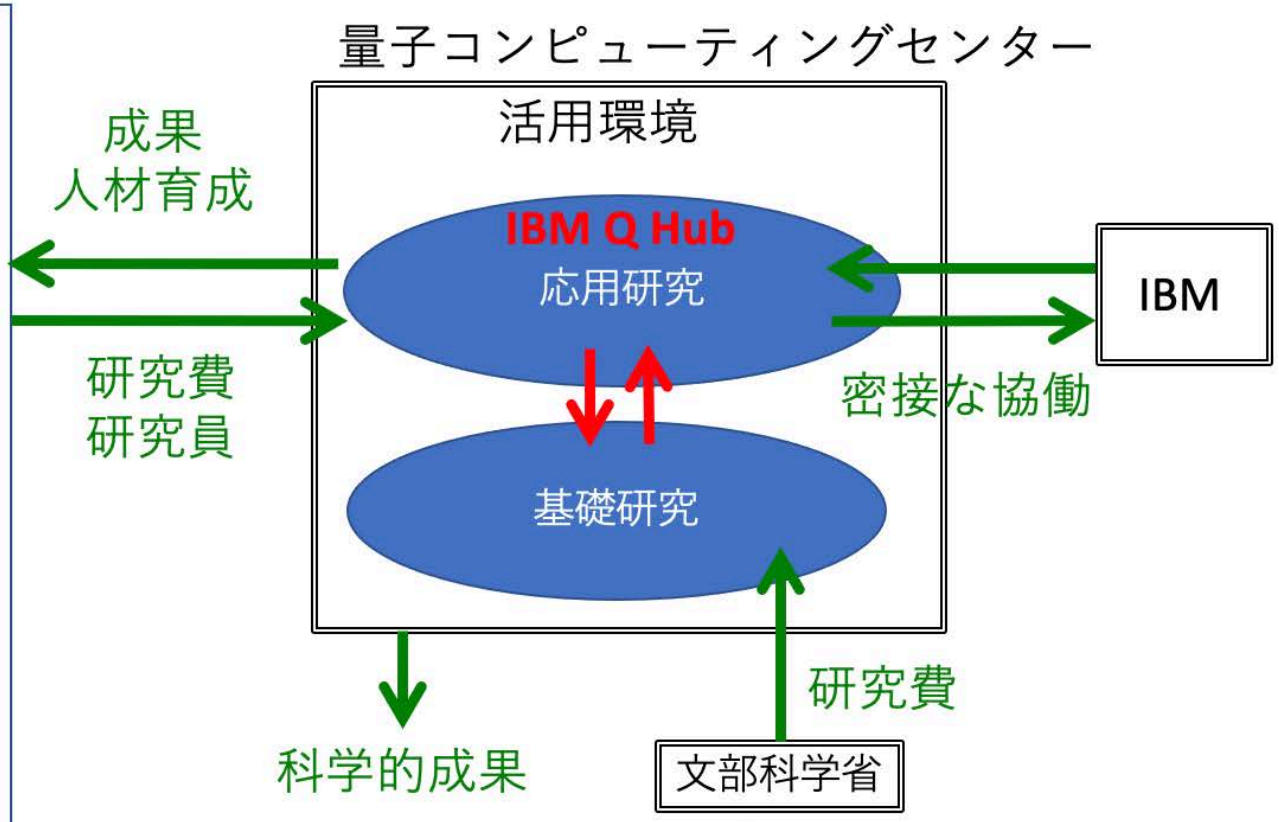
慶應義塾大学における取り組み

Keio Q Hub

（2018年5月活動開始、第1期:2020年12月末終了、第2期2021年1月開始）

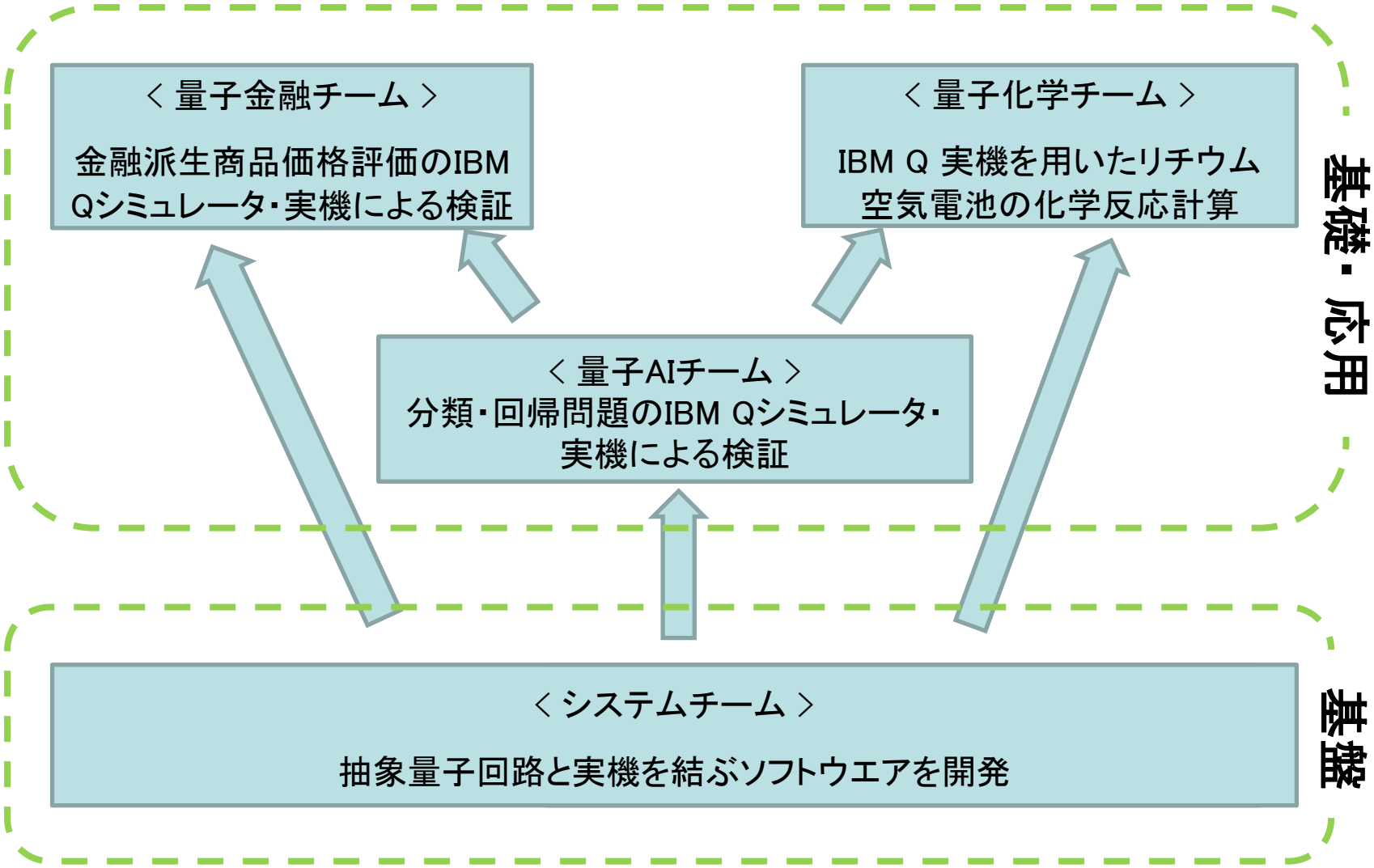
Hub 参加企業

- JSR株式会社
- 三菱ケミカル株式会社
- みずほフィナンシャルグループ
- 三菱UFJフィナンシャル・グループ
- 三井住友信託銀行株式会社
- ソニー株式会社

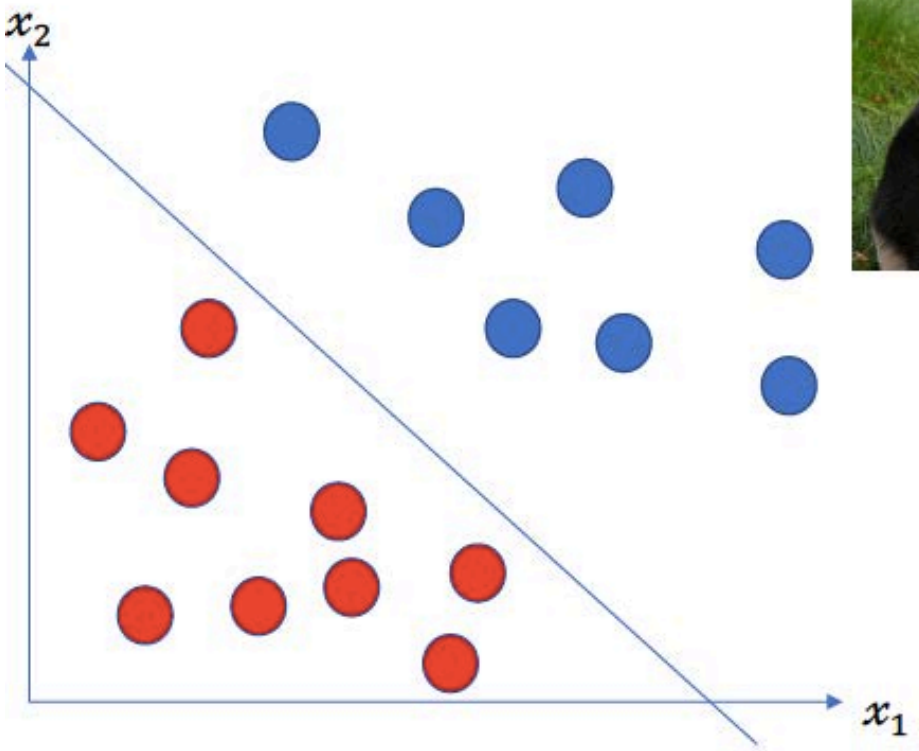


Q-LEAP 「量子ソフトウェア」代表 山本直樹

Keio Q Hub Team の構成



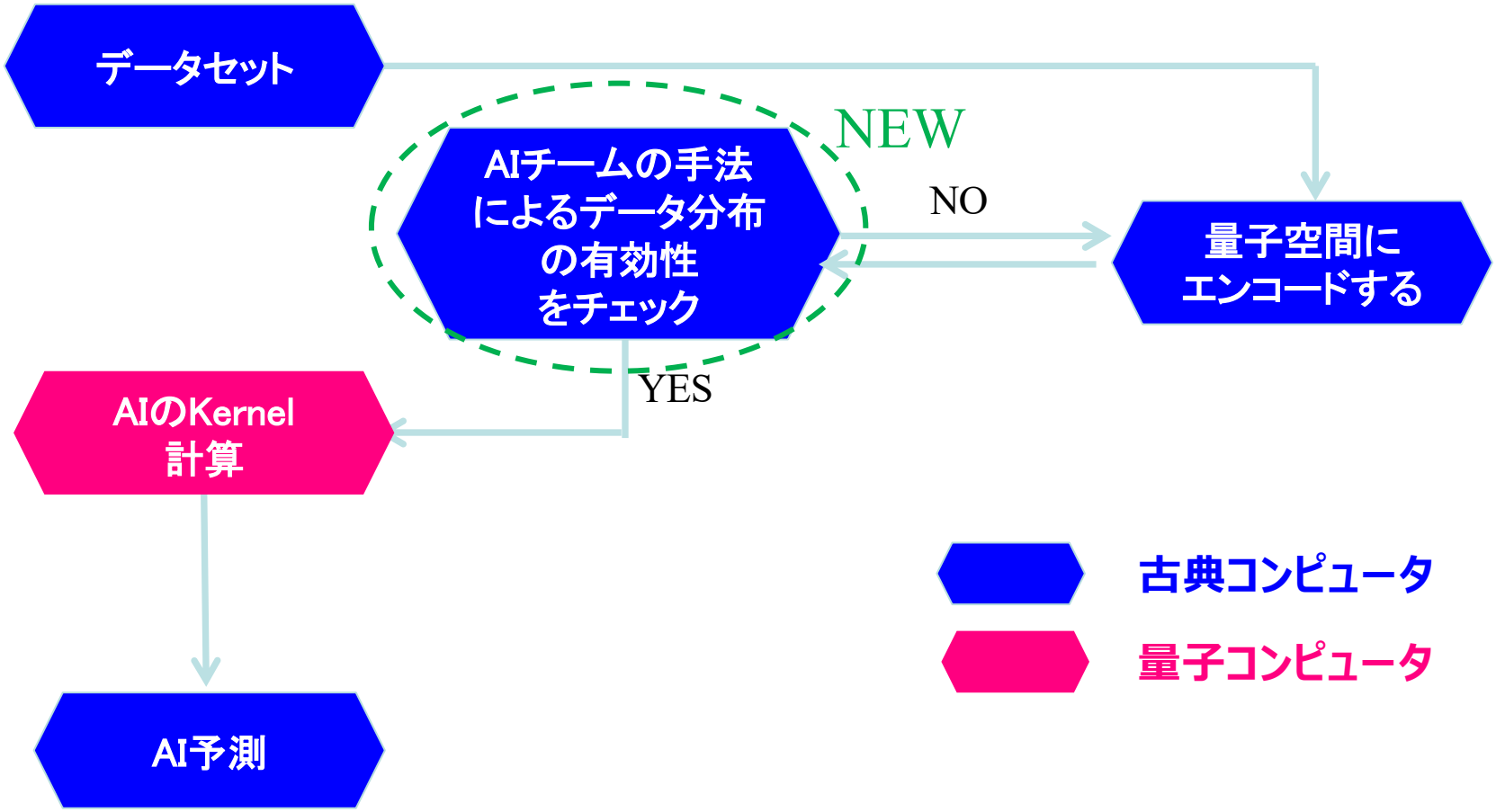
Keio Quantum AI Team：Quantum Support Vector Machine
Classification problem



Keio Q Hub 量子AIチームの研究成果

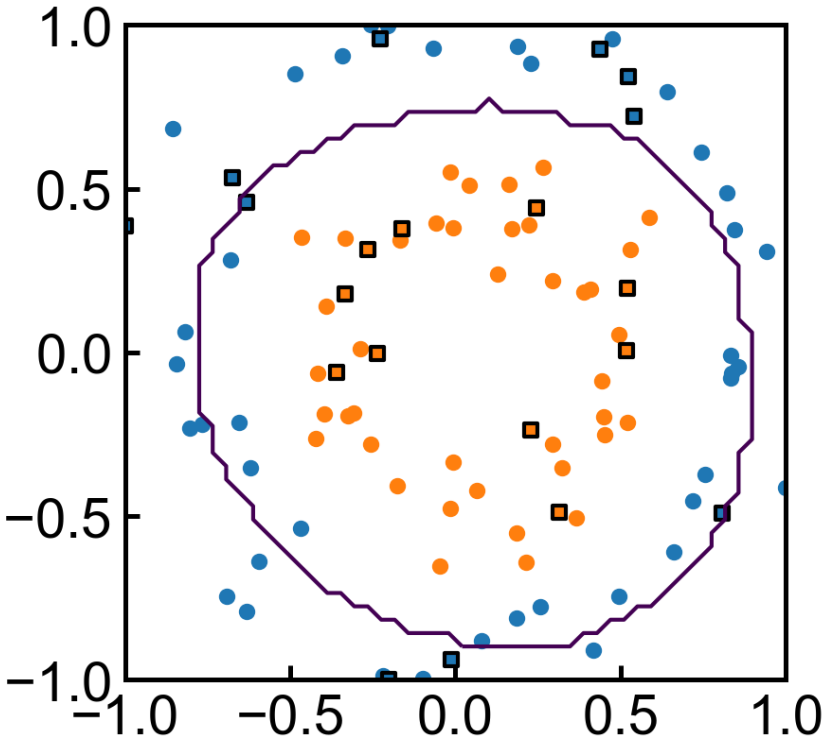
✓ **IBM手法の改良版を提案。**

<Keio Q Hub 量子AIチーム 改良手法>

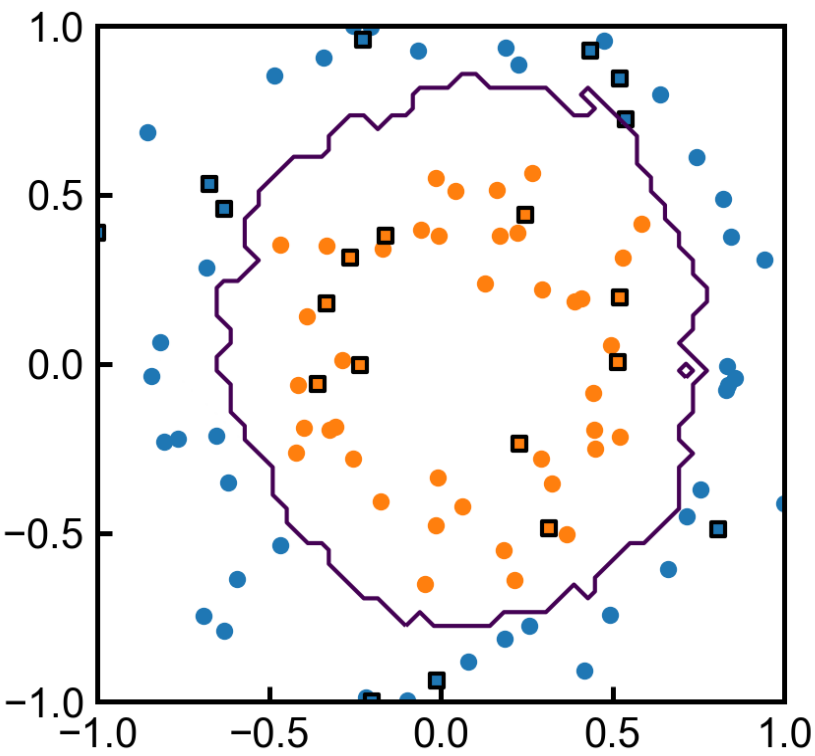


IBM Q実機での分類分け

20 Qubit IBM Q
Accuracy : 0.88

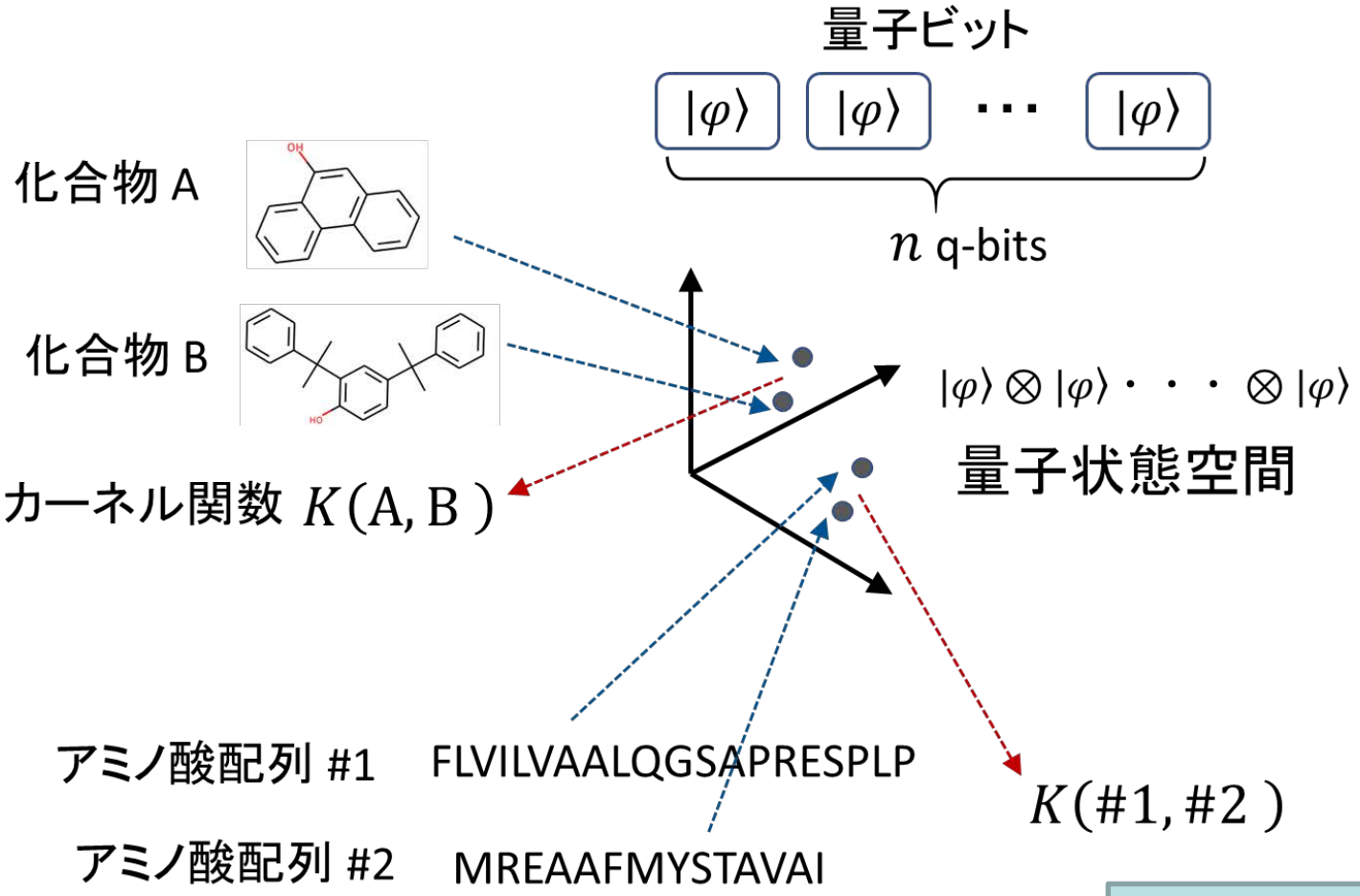


Simulator
Accuracy : 1.00



量子創薬・生命科学イニシアチブ

慶應義塾（理工学部、医学部）+ 早稲田大学



非構造データの量子カーネル関数の開発

文科省 Q-LEAP
（2018 PRISM）

量子化学チーム

変分型量子固有値ソルバー(VQE)による化学反応過程のシミュレーション:リチウム水素電池への応用

DESIGNLINES | POWER MANAGEMENT DESIGNLINE

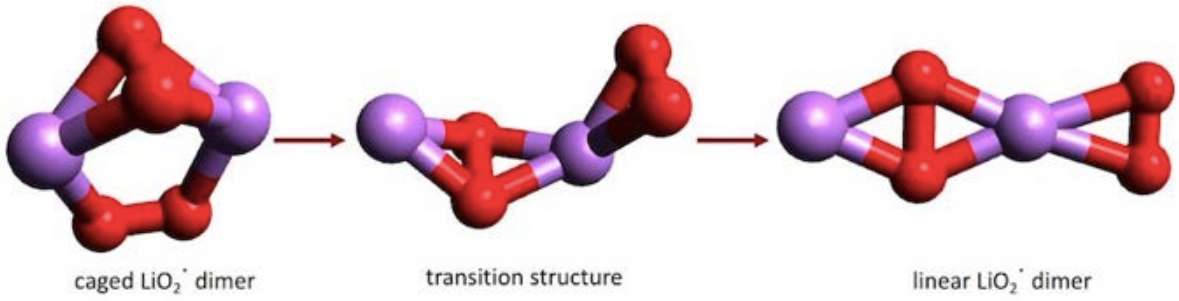
Battery Research Advances Quantum Computing Capabilities

Studying reactions in Li-air batteries was also a research challenge for IBM.

EETimes

July 28, 2019

Li-air battery research collaboration between industry and academia goes back to the mid-1990s, said Dr. Naoki Yamamoto, associate professor and the chair of the Keio University Quantum Computing Center, which is part of the IBM Q Hub. "Because both the charge and discharge process in the lithium-air battery are very complicated and sensitive to the surrounding environment, it is still hard to elucidate the reaction mechanism at the atomic level, which has limited the progress of the technology."



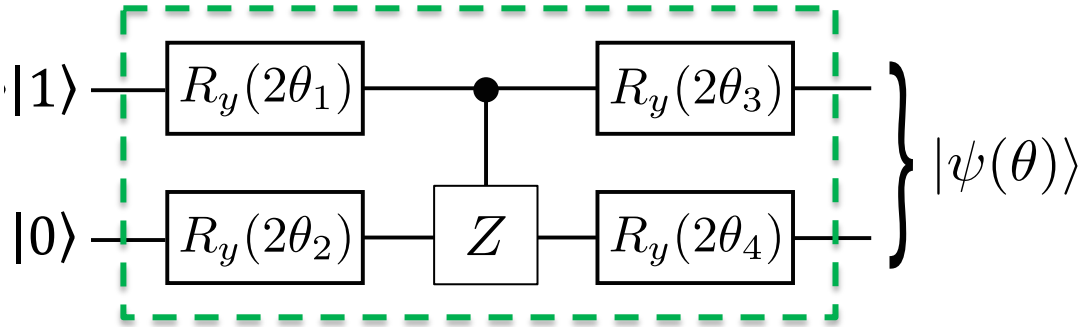
Reactant TS Product

変分型量子固有値ソルバー (Variational Quantum Eigensolver, VQE):

Ansatz state: $|\psi(\theta)\rangle = U(\theta)|\psi_0\rangle$

エネルギー値 $\langle\psi(\theta)|H|\psi(\theta)\rangle$ が小さくなるようにパラメータ θ を更新

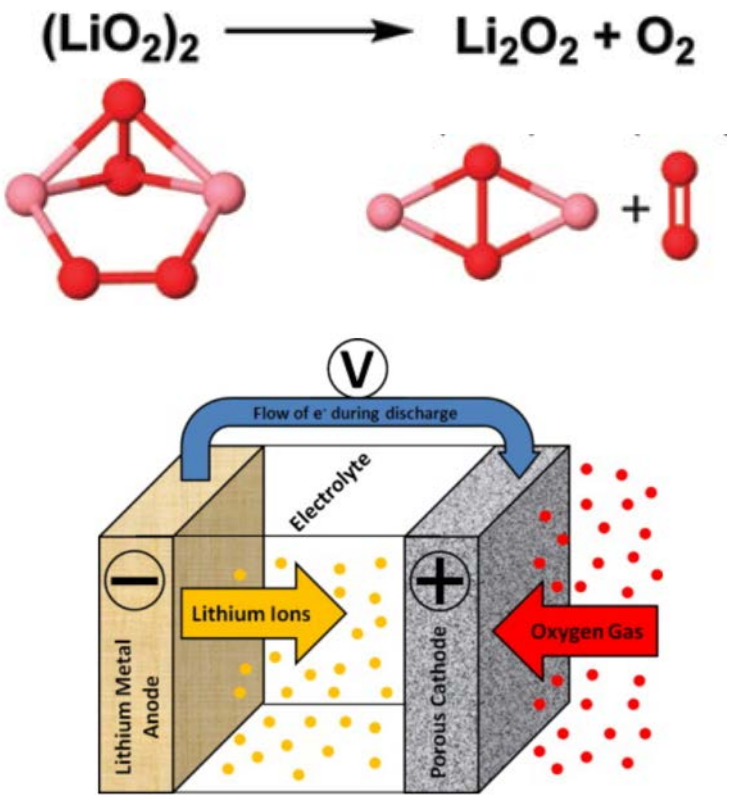
VQE for LiOx: 2量子ビットでモデル化（3種のハミルトニアンすべてで）

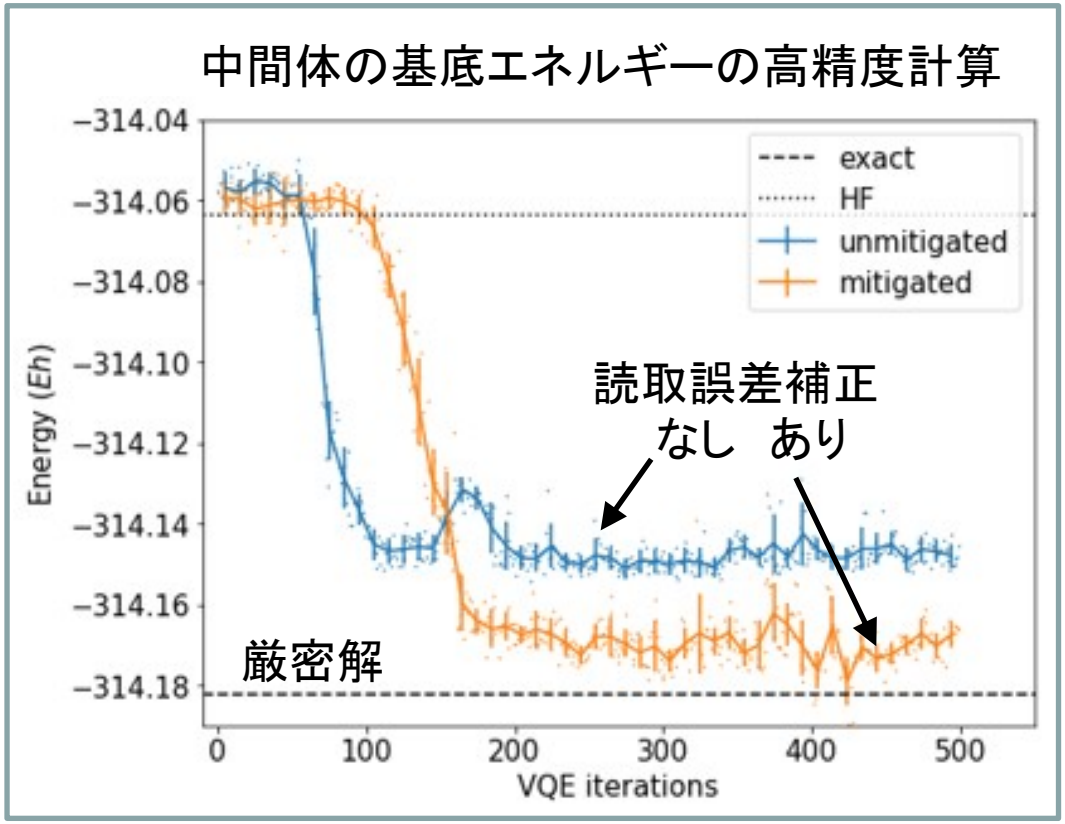


Computational Investigations of the Lithium Superoxide Dimer Rearrangement on Noisy Quantum Devices, Q. Gao, H. Nakamura, T. P. Gujarati, G. O. Jones, J. E. Rice, S. P. Wood, M. Pistoia, J. M. Garcia, and N. Yamamoto, arXiv:1906.10675.

量子化学チーム:リチウム空気電池の反応解析

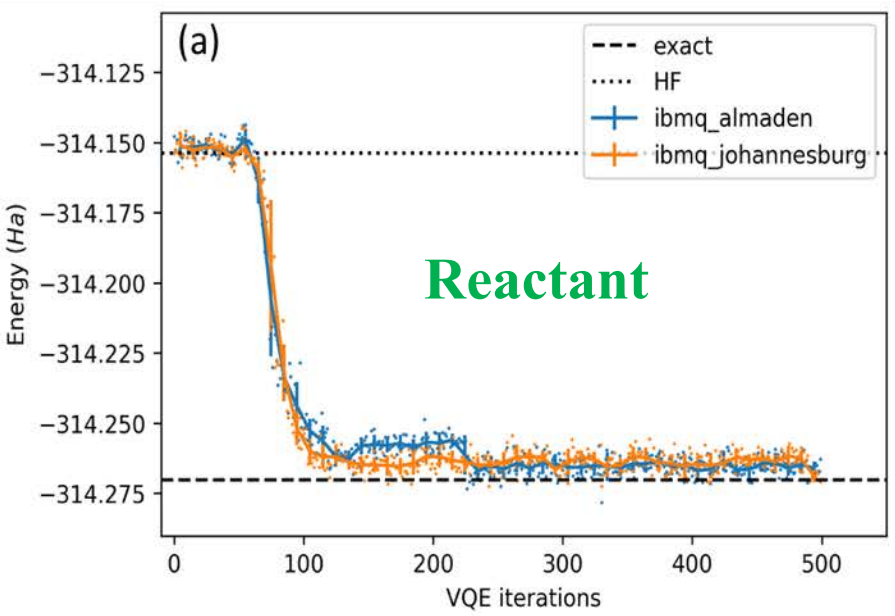
慶應義塾 + 三菱ケミカル + IBM

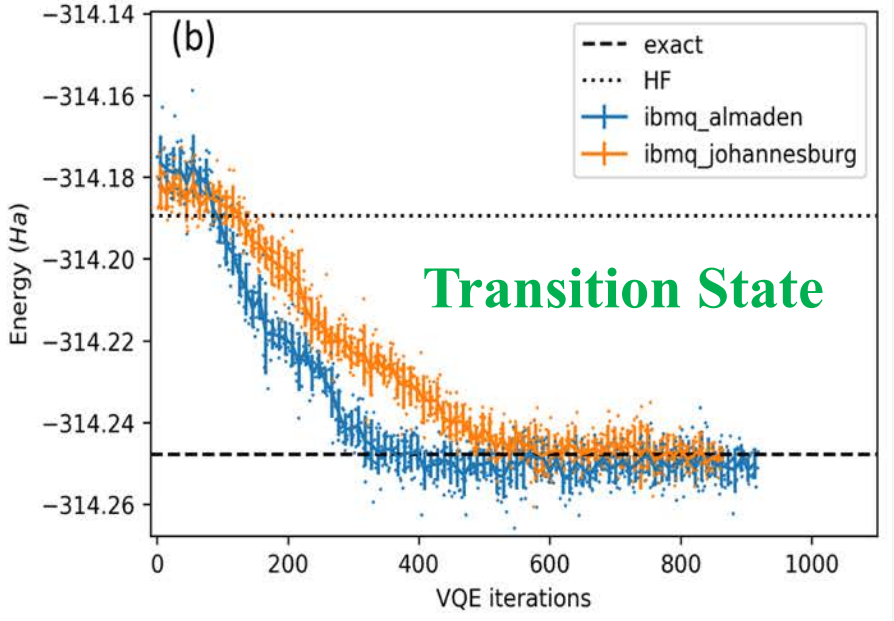


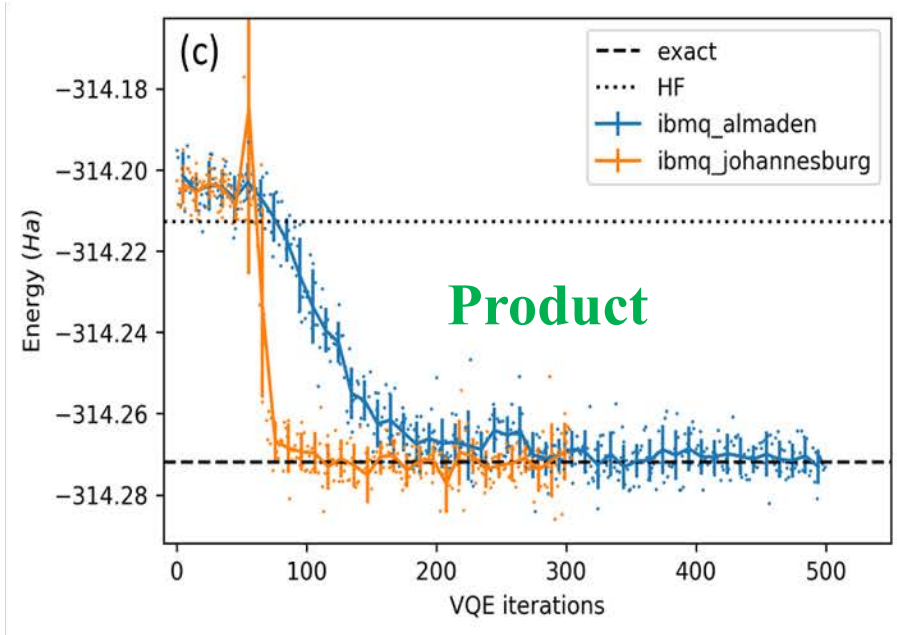


IBM Q 実機を用いてリチウム空気電池の化学反応計算に成功！

IBM Q による実験結果





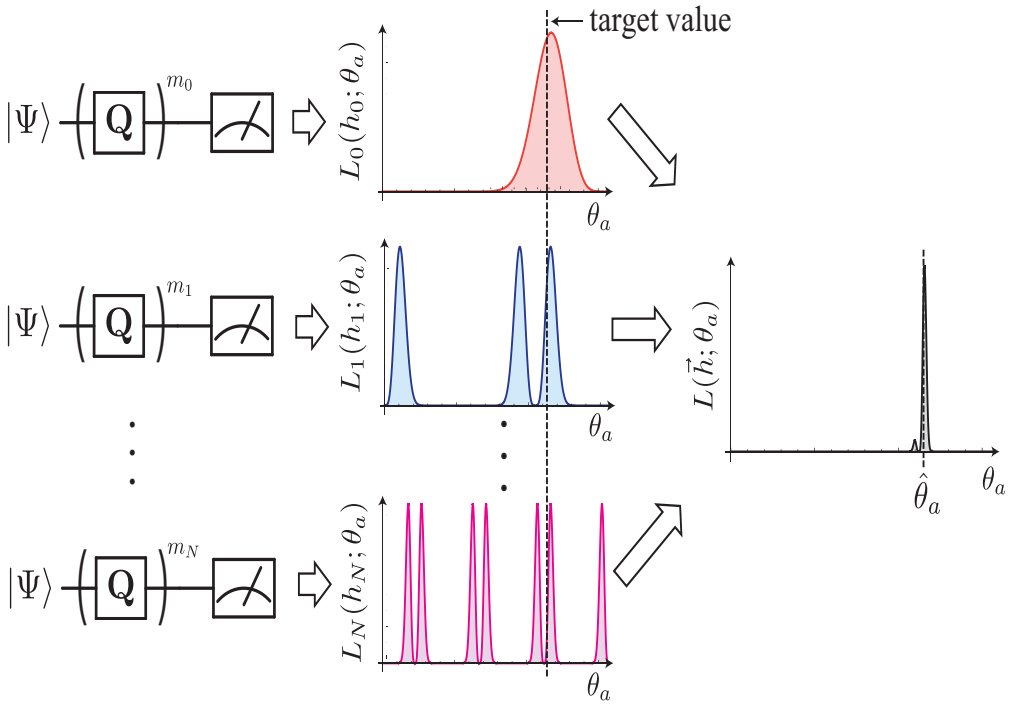


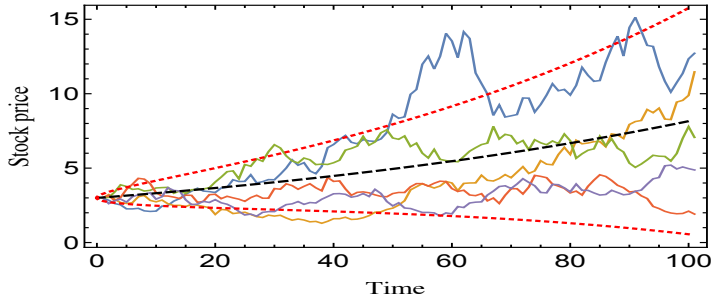
TS, Product の場合は、基底状態と第１励起状態のエネルギー差が大きい
→ ほぼ基底状態が得られた。

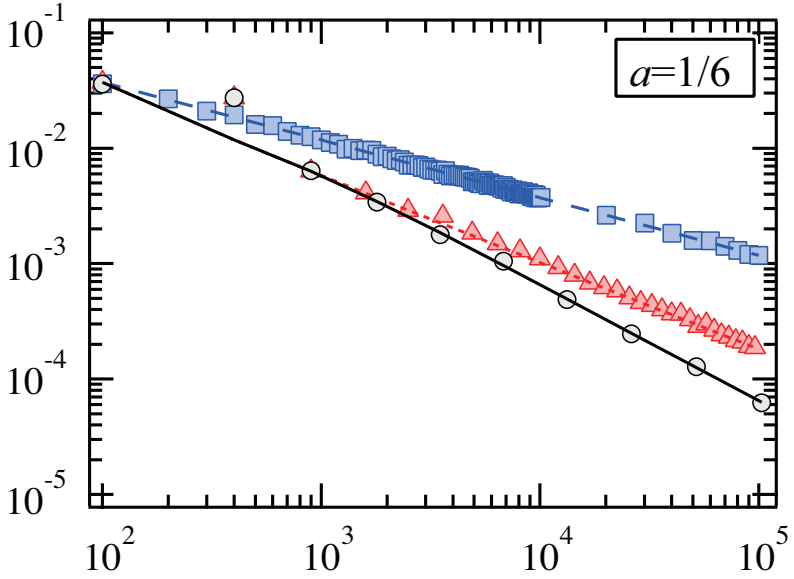
Reactant の場合は、基底状態と第１励起状態がエネルギー縮退に近い
→ 生成された状態の解析が必要

量子金融チーム：高速モンテカルロ計算

慶應義塾 + みずほ + MUFG + IBM







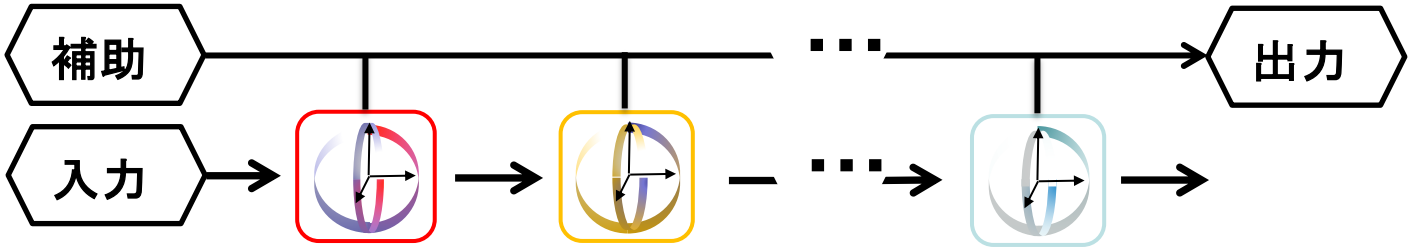
基礎理論構築 & IBM Q シミュレータ・実機による検証

新規振幅推定アルゴリズムと金融問題への展開

振幅推定アルゴリズム --- モンテカルロ計算などで量子2乗加速を保証

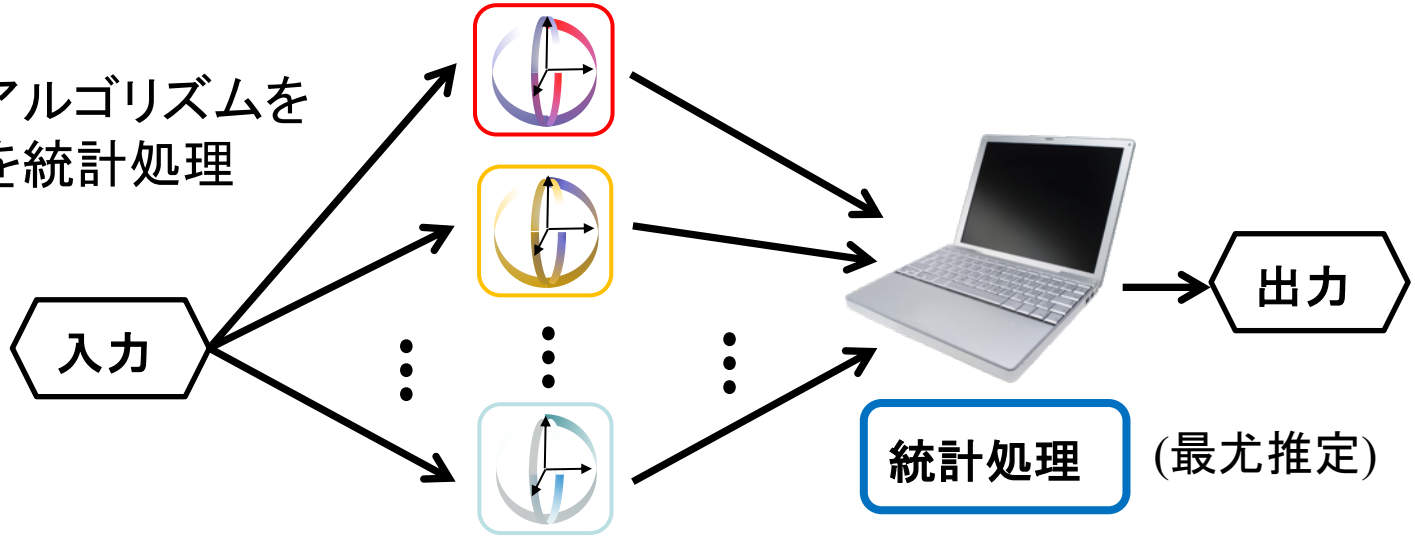
従来法

グローバー
＋位相推定



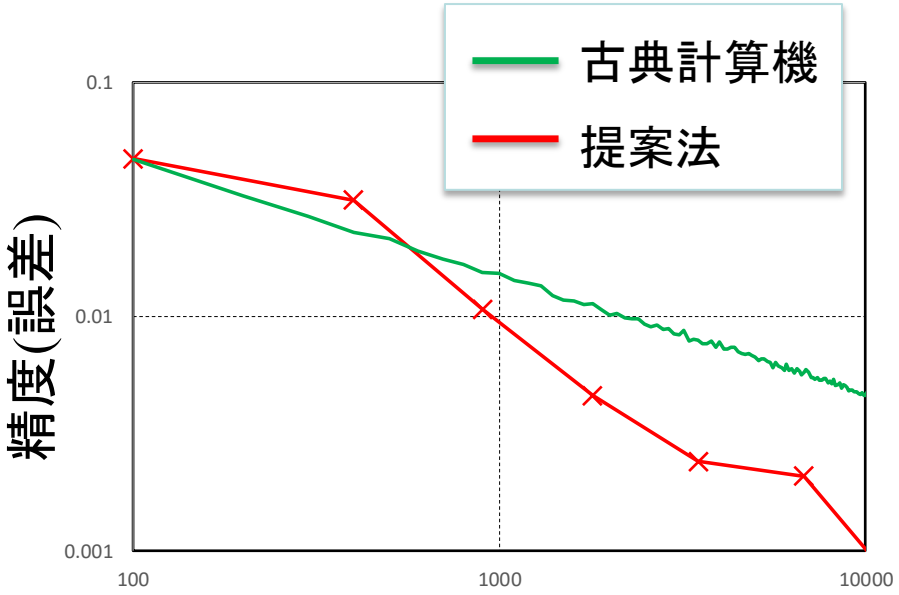
提案法

異なるグローバーアルゴリズムを
並列で実行、結果を統計処理
(位相推定は不要)

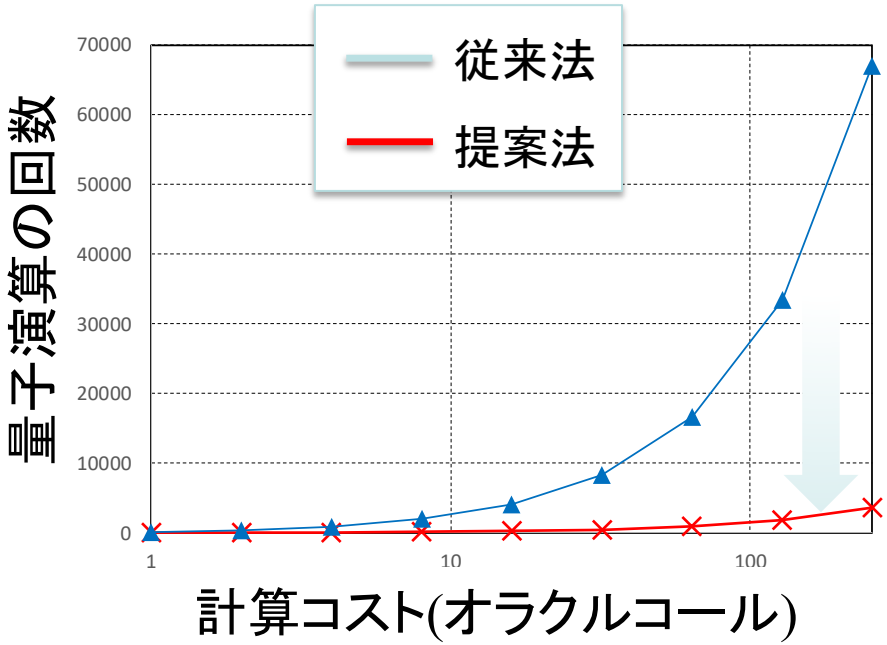


Amplitude estimation without phase estimation, Y. Suzuki, S. Uno, R. Raymond, T. Tanaka, T. Onodera and N. Yamamoto, arXiv:1904.10246

モンテカルロ積分への応用

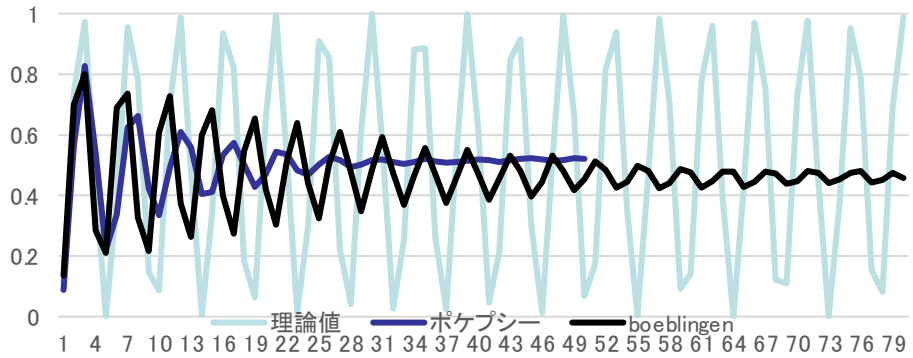


従来法と同等の性能



演算の長さを従来法に対して約95%削減

[実験] 減衰ラビ振動 (+ 不明項) を観測



--- 実機に対する統計解析理論の構築が必要(進行中)

量子金融チーム（暗号）：ショアアルゴリズムの実装

慶應義塾 + 東京大学 + MUFG + みずほ

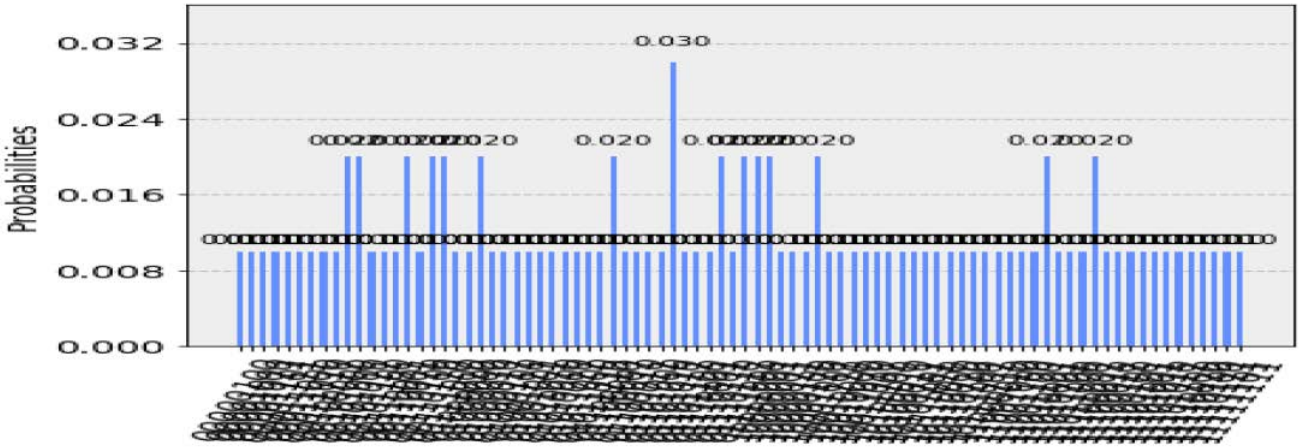
ショアアルゴリズム – 素因数分解を現実的な時間で解いてしまう。
RSA暗号方式に大きな影響。

IBM20Qでの動作結果

- ゲート数：63
- 回路の深さ：17

実機実装

- ゲート数：331
- 回路の深さ：109



IBM Q 実機を用いて ショアアルゴリズムの実装に挑戦！

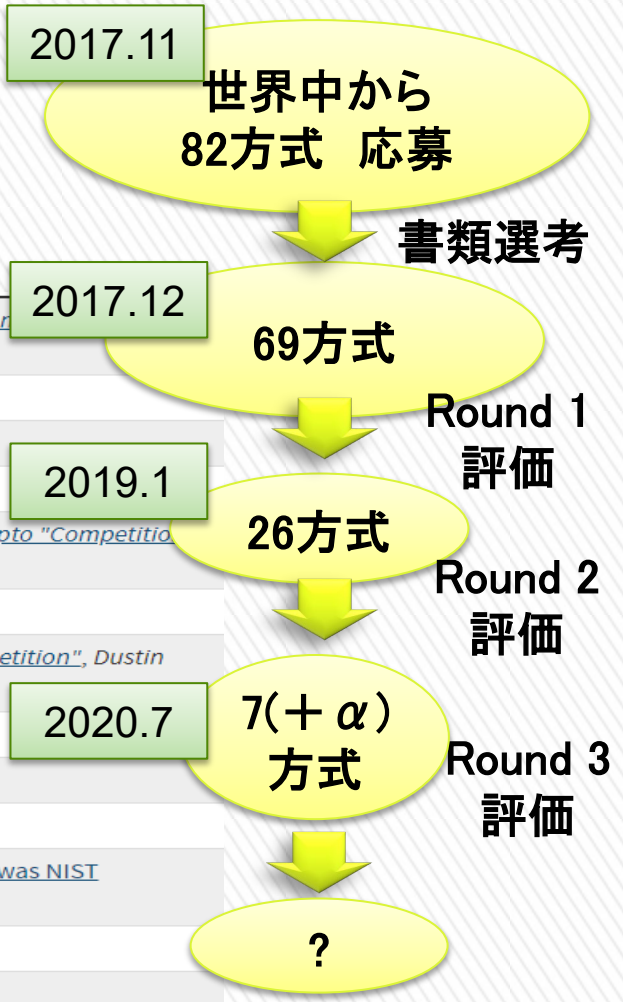
資料3

耐量子計算機暗号の動向等について

米国NIST PQC 標準化

- 2016年募集開始
- 2022–2024年完了予定
  - 標準ドラフト公開

Feb 24-26, 2016	NIST Presentation at PQCrypto 2016: *Announcement and outline of NIST's Call for Subr 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 "Competitio 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 (26 algorithms)
March 15, 2019	Deadline for updated submission packages for the Second Round
May 8-10, 2019	NIST Presentation at PQCrypto 2019: Round 2 of the NIST PQC "Competition" - What was NIST Thinking? (Spring 2019), *Dustin Moody*
August 22-24, 2019	Second PQC Standardization Conference
July 22, 2020	Third Round Candidates announced (7 Finalists and 8 Alternates)
October 1, 2020	Deadline for updated submission packages for the Third Round
2022/2024	Draft Standards Available



https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline

Created January 03, 2017, Updated August 11, 2020

NIST第3ラウンドの7方式（＋α）

- **格子に基づく暗号**
  - 鍵交換・暗号化：**CRYSTALS-KYBER、NTRU、SABER、**（FrodoKEM、NTRU Prime）
  - 署名：**CRYSTALS-DILITHIUM、FALCON**
- **符号に基づく暗号**
  - 鍵交換・暗号化：**Classic McEliece**、（BIKE、HQC）
- 多変数多項式に基づく暗号
  - 署名：**Rainbow、**（GeMSS）
- ハッシュ関数に基づく署名
  - 署名：（**SPHINCS+**）

Finalist に昇格？

- 同種写像に基づく暗号
  - 鍵交換・暗号化:（SIKE）
- その他
  - 署名：（Picnic）

資料4

量子コンピュータにおける素因数分解の評価について

高安敦（NICT）

2021/3/3

量子計算機の脅威

Shorの“量子”アルゴリズム[Sho@FOCS'94]により，素因数分解・離散対数問題が理論的には多項式時間で解けることがわかった.

現代暗号への脅威

2016年2月：NISTが耐量子計算機暗号の標準化計画を発表

2017年11月：提案締め切り

2017年12月：Round 1 Algorithms発表

2019年1月：Round 2 Algorithms 発表

2020年7月：Round 3 Algorithms発表

Shorのアルゴリズムの現実的な脅威

Shorのアルゴリズムは理論的には脅威だが，実装上はこれまで小さなパラメータにしか適用できていない．

- 素因数分解
  $15 = 3 \times 5,\ 21 = 3 \times 7$
- （素体・楕円曲線上）離散対数問題
  $2^x = 1 \mod 3$

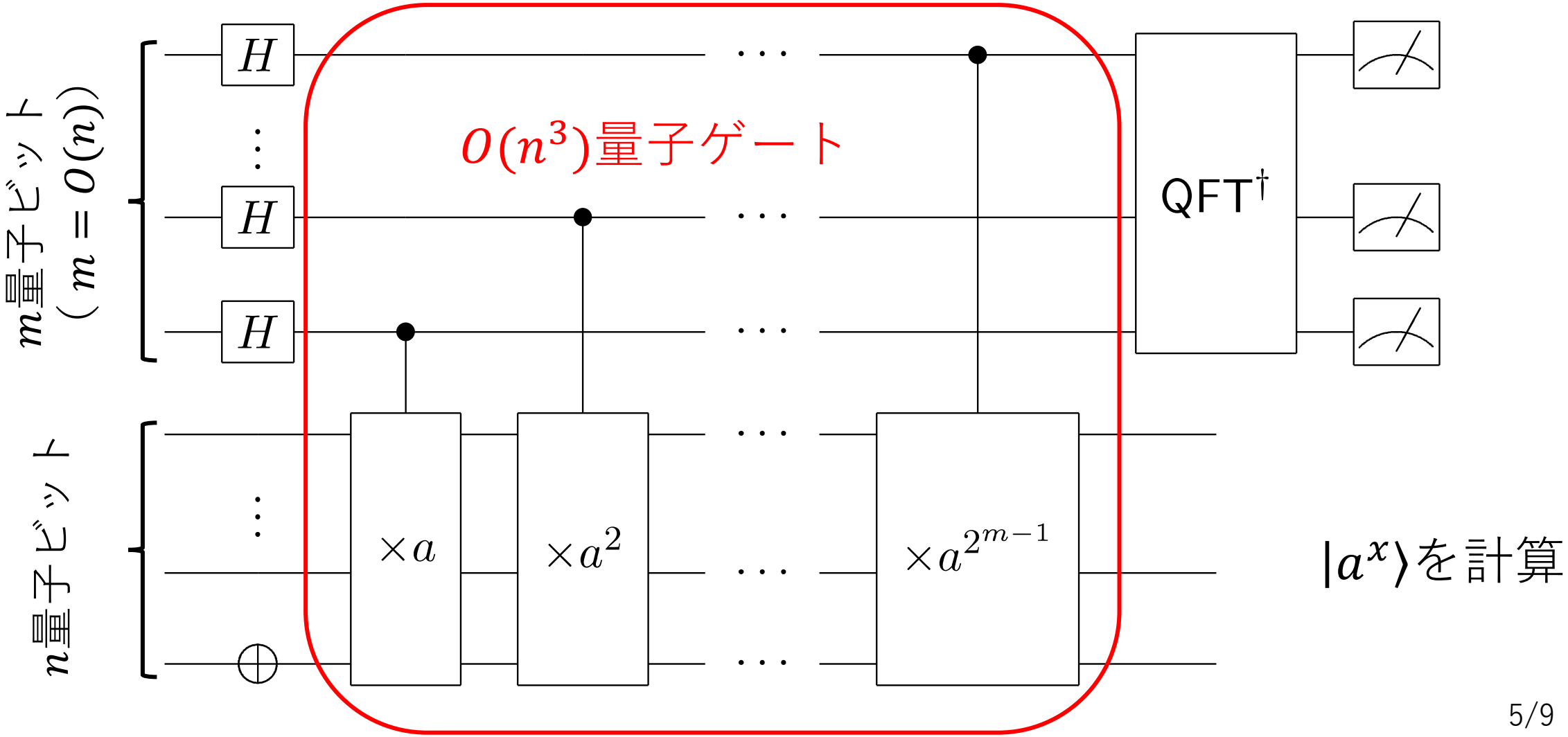
現実的にどれだけの脅威となるのか評価する必要がある

量子素因数分解アルゴリズムの実装動向

- Shorのアルゴリズム
  $15 = 3 \times 5,\ 21 = 3 \times 7$
- 量子アニーリング
  $376289 = 571 \times 659$
  S. Jiang et al. Quantum annealing for prime factorization. Scientific Reports, 2018.
- Groverのアルゴリズム
  $4088459 = 2017 \times 2027$
  A. Dash et al. Exact search algorithm to factorize large biprimes and a triprime on IBM quantum computer. arXiv: 1805.10478, 2018.

古典アルゴリズムより速いという理論的根拠があるのはShorだけ

素因数分解の量子回路


m量子ビット
$(m = O(n))$
n量子ビット
H
H
H
$\times a$
$\times a^2$
$\times a^{2^{m-1}}$
$O(n^3)$量子ゲート
QFT†
$|a^x\rangle$を計算

素因数分解の実装結果

研究グループ	合成数	a	量子ビット数	冪乗計算ゲート数
[VSB+01]	15	$11, 7$	$7, 7$	$2, 9$
[LWL+07]	15	$4, 2$	$7, 5$	$2, 2$
[LBYP07]	15	11	5	2
[PMO09]	15		5	6
[LBC+12]	15	4	3	2
[MLLL+12]	21	4	$1 + \log_2 3$	
[SSV13]	20000ビット		2	1
[MNM+16]	15	$2, 7, 8, 11, 13$	$5, 5, 5, 5, 5$	$11, 15, 11, 2, 15$
[ASK19]	21	2	6	19
[DLQ+20]	15	$7, 8$	3	3

Shorのアルゴリズムによる素因数分解の実装結果まとめ

- これまで適切に素因数分解されたと言えるのは15, 21のみで，15の素因数分解は特別に簡単
- いずれの実験もなるべく簡略化した量子回路を用いており，一般的に同様の簡略化は難しそう.
- 求める位数の情報を使った実装があるが，そのような場合には任意に大きな合成数を素因数分解できるため不適切
- 適切に$21 = 3 \times 7$の素因数分解を行なった論文においても，$35 = 5 \times 7$の素因数分解に失敗している.
- 小さなパラメータにおいて離散対数問題の実験結果も報告されている.

➢ 現在の量子コンピュータで暗号で用いられるような大きなパラメータの問題が解けるとは考えにくい.

素因数分解アルゴリズムの漸近的な比較（[GE19]のTABLE I）

研究グループ	量子ビット数	測定の深さ	Toffoli ゲート数
[VBE96]	$7n+1$	$80n^3+O(n^2)$	$80n^3+O(n^2)$
[Zal98]	$5n+O(1)$	$600n^3+O(n)$	$52n^3+O(n^2)$
[Bea03]	$2n+3$	$144n^3+O(n^2\log n)$	$576n^3\log n$ $+O(n^3\log n)$
[FMMC12]	$3n+O(1)$	$40n^3+O(n^2)$	$40n^3+O(n^2)$
[HRS17]	$2n+2$	$52n^3+O(n^2)$	$64n^3\log n+O(n^3)$
[GE19]	$3n+0.002n\log n$	$500n^2+n^2\log n$	$0.3n^3+0.0005n^3\log n$

ゲートの分解などを行い実装に適したアルゴリズムが年々改良されている.

[GE19]: C. Gidney and M. Ekera. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. arXiv:1905.09749, (2019)

素因数分解アルゴリズムのパラメータごとの比較（[GE19]のTABLE I）

比較しているのは，量子ビット数（100万個）×計算時間（日）

研究グループ	$n = 1024$	$n = 2048$	$n = 3072$
[VBE96]	240	4100	23000
[Zal98]	16	250	540
[Bea03]	32000	380000	1700000
[FMMC12]	53	850	4600
[HRS17]	230	2800	13000
[GE19]	0.5	5.9	21

[GE19]による共通の設定：ゲート誤り率0.1%, 表面符号測定時間1マイクロ秒,
反応時間10マイクロ秒，格子結合（超伝導量子ビット）

参考文献(6ページ)

[ASK19] Mirko Amico et al. Experimental study of shor's factoring algorithm using the ibm q experience. Phys. Rev. A, 100:012305, 2019.

[DLQ+20] Zhao-Chen Duan et al. Proof-of-principle demonstration of compiled Shor 's algorithm using a quantum dot single-photon source. Optics Express, 28:18917–18930, 2020.

[LBC+12] E. Lucero et al. Computing prime factors with a Josephson phase qubit quantum processor. Nature Physics, 8:719–723, 2012.

[LBYP07] Chao-Yang Lu et al. Demonstration of a compiled version of Shor 's quantum factoring algorithm using photonic qubits. Phys. Rev. Lett., 99, 2007.

[LWL+07] B. P. Lanyon et al. Experimental demonstration of a compiled version of Shor's algorithm with quantum entanglement. Phys. Rev. Lett., 99, 2007.

[MLLL+12] E. Martin-Lopez et al. Experimental realisation of Shor 's quantum factoring algorithm using qubit recycling. Nature Photon, 6:773–776, 2012.

[MNM+16] T. Monz et al. Realization of a scalable Shor algorithm. Science, 351:1068–1070, 2016.

[PMO09] A. Politi, J. C. F. Matthews, and J. L. O 'Brien. Shor 's quantum factoring algorithm on a photonic chip. Science, 325:1221, 2009.

[SSV13] John A. Smolin et al. Oversimplifying quantum factoring. Nature, 499:163–165, 2013.

[VSB+01] L. Vandersypen et al. Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance. Nature, 414:883–887, 2001.

参考文献(8ページ)

[Bea03] S. Beauregard. Circuit for shor's algorithm using 2n + 3 qubits. Quantum Inf. Comput., 3:175–185, 2003.

[FMMC12] Austin G. Fowler et al. Surface codes: Towards practical large-scale quantum computation. Phys. Rev. A, 86:032324, 2012.

[GE19] C. Gidney and M. Ekera. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. arXiv preprint arXiv:1905.09749, 2019.

[HRS17] Thomas Haener et al. Factoring using 2n + 2 qubits with toffoli based modular multiplication. Quantum Information and Computation, 18(7-8):673–684, 2017.

[VBE96] Vlatko Vedral et al. Quantum networks for elementary arithmetic operations. Phys. Rev. A, 54:147–153, 1996.

[Zal98] Christof Zalka. Fast versions of Shor's quantum factoring algorithm. arXiv preprint quantum-ph/9806084, 1998.

資料 5

量子コンピュータにおける離散対数問題の求解実験について

発表者：青野 良範（NICT）
mail: aono@nict.go.jp
日時：2021/03/03 CRYPTREC TF

本日の概要

資料5

超電導量子回路を用いた離散対数問題の求解実験

- 2020/12/11 QIT43発表[青野-Liu-田中-宇野-Van Meter-篠原-野島]

- IBM Q(Melbourne, Paris)を用いた計算機実験の報告

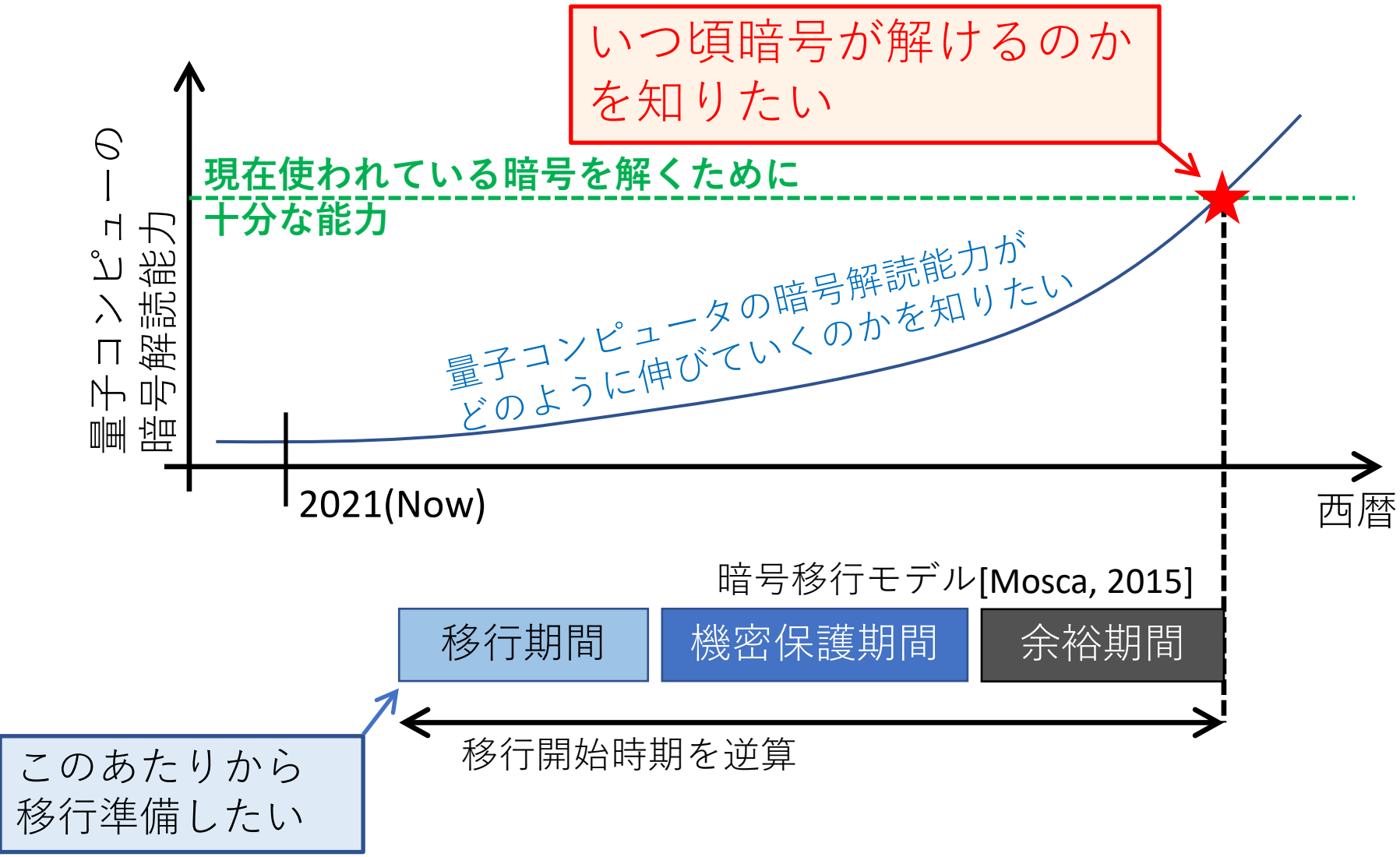
【大目標】量子計算機とショアのアルゴリズムが
現在用いられているDLPベースの署名方式に与える影響の
将来予測と移行時期の見積もり

【報告内容】

- 最新の量子計算機でどの程度の大きさのインスタンスが解けるのかの調査
  - $2^z \equiv 1 \bmod 3$: 解けている？　$2^z \equiv 2 \bmod 3$: 難しい
- 将来予測を行うために解決すべき問題点の洗い出し
  - 量子計算機の性能をどう測るのか
  - 実験の成功（問題が解けたということ）をどう定量的に評価するのか

資料５

量子コンピュータと暗号の危殆化

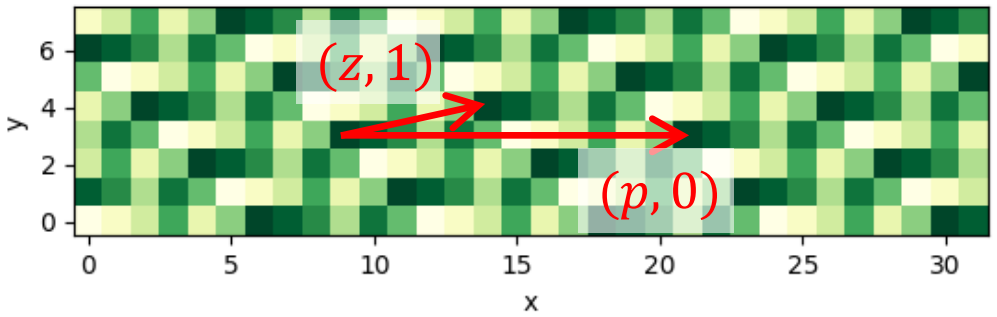


【ターゲット】有限体F_p上の離散対数問題(DLP; Discrete Logarithm Problem)

素数pと自然数$g, a \leq p-1$に対して
$$g^z \equiv a \pmod{p}$$
を満たす自然数zを求めよ

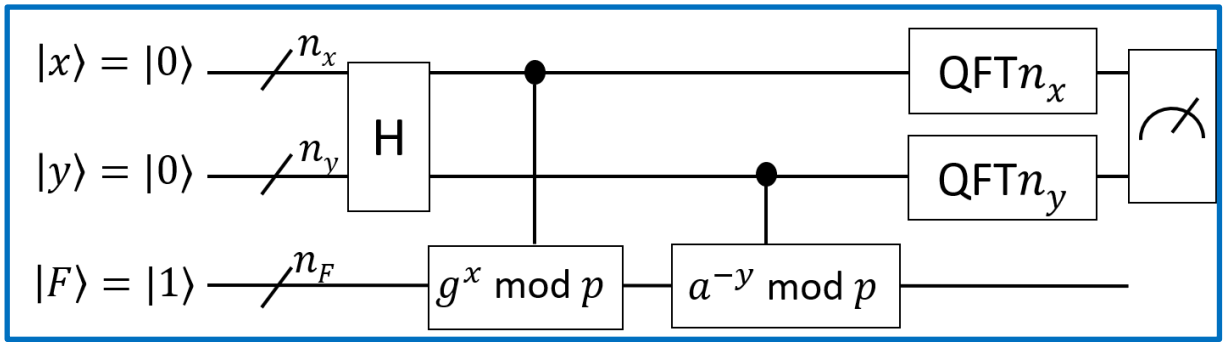
- 素因数分解問題に関しては、多くの実験データが存在
（[Vandersypen et al.2001]～[Monz et al.2016]）
- 離散対数問題に関しては実験データが無い

【方針】インスタンスを表す三つ組み(g, a, p)に対して、関数$F(x, y) = g^x a^{-y} \bmod p$は周期$(z, 1), (p, 0)$を持つため、それらを位相推定を用いて発見すると、問題の解zが導かれる



F(x,y)の値を濃淡によって表現した図

【量子回路設計】標準的なShorのアルゴリズムを用いる

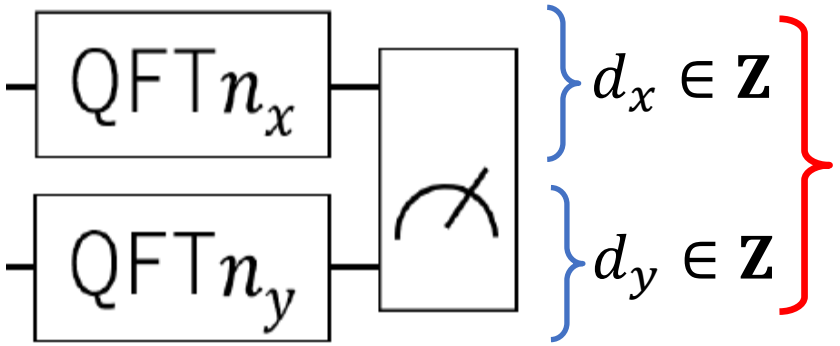


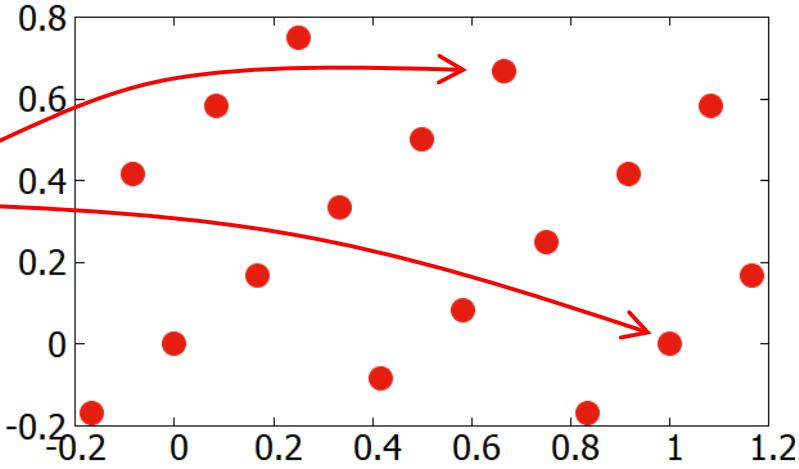
- 最も複雑（コストが高い）のが中央のべき乗回路
  - 素因数分解の先行研究[Monz et al.2016]と同様の簡略化を行う
    - p=3,7におけるmod 計算のシフト演算への置き換え等の論理回路レベルでの簡略化
    - IBM Qのトポロジーに合わせた実行レベル簡略化
  - 現行の量子デバイスでは簡略化無しの動作は困難[大西et al., QIT41]

【測定結果からの解の取り出し】

資料５

- QFTの結果を複数回測定し、後処理アルゴリズムPPを用いてDLPの解zを復元





$F(x,y)$の周期$(z,1),(p,0)$が張る格子の双対格子の点の近似が高確率で得られる

- 量子回路でDLPが解ける：　$\Pr[\mathrm{PP}(o_1,\ldots,o_K)\rightarrow z]$　が大きい

- （論文内での）計算機実験成功の定義：

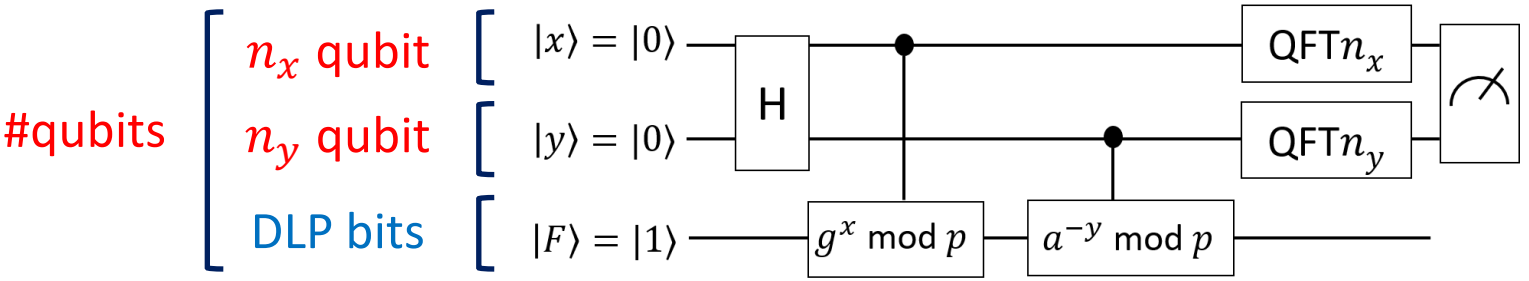
$D_{KL}(Device||Ideal)$ が小さい

実際にはランダムノイズとのダイバージェンスを大小比較

実験のターゲットと回路

資料5

- Qiskitフレームワークを用いて構成
- qubits数を決めるパラメータn_x, n_yを導入



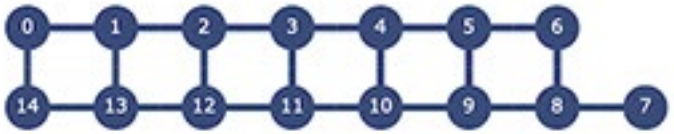
	DLP instance	DLP bits	n_x	n_y	#qubits	N_L	N_g
I	$2^z = 1 \bmod 3$	2	2	2	6	19	31
II			3	2	7	24	44
III	$2^z = 2 \bmod 3$		3	2	7	25	93
IV			3	3	8	31	123
V	$4^z = 2 \bmod 7$	3	3	3	9	39	227
VI	$3^z = 4 \bmod 7$		4	4	11	89	861

- N_L: circuit.size()の出力（論理ゲート数のカウント）の順にインスタンスI,II,…,VIと名付ける
- N_g: ゲートセットを{c1,c2,c3,cx}のみに制限したときのゲート数カウント

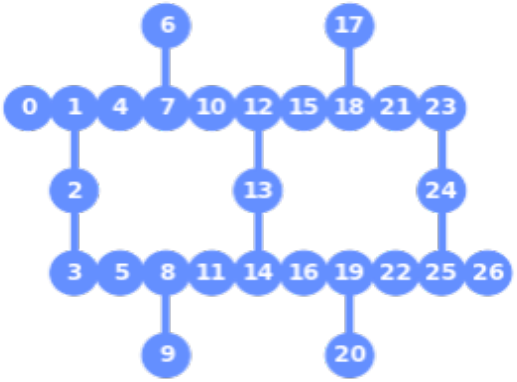
実験デバイス

資料５

- ibmq_16_melbourne
  - 2018年リリース
  - QV=8
  - Connectivity:○
  - Error rate:△



- ibmq_paris
  - 2020年リリース
  - QV=32
  - Connectivity:△
  - Error rate:○

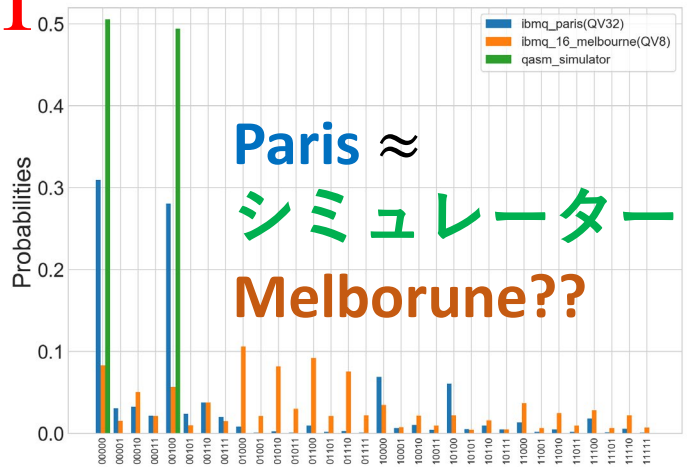


実験結果

資料 5

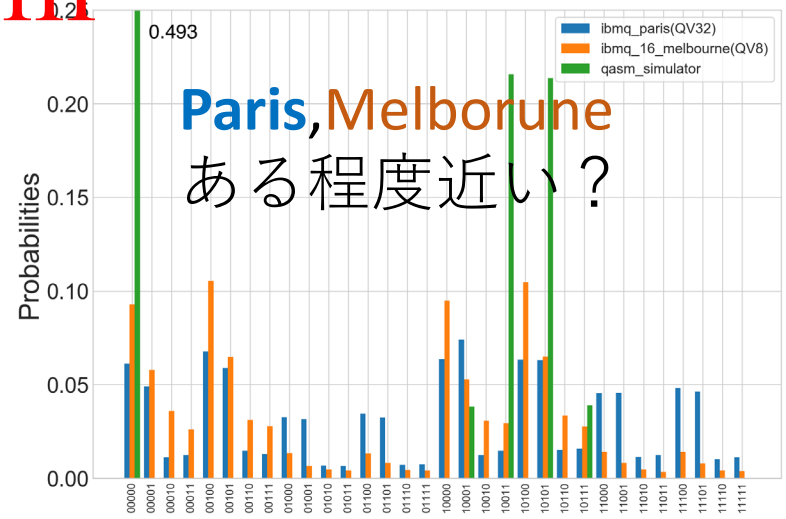
- **Paris**, Melbourne,**シミュレーター**の出力分布比較(n=8192)

II

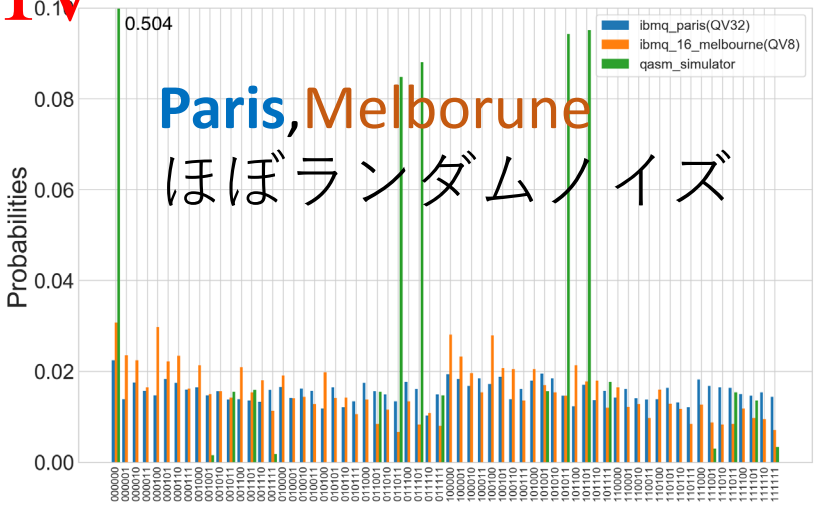


	DLP instance	n_x	n_y	N_L	N_g
I	$2^z = 1 \bmod 3$	2	2	19	31
II		3	2	24	44
III	$2^z = 2 \bmod 3$	3	2	25	93
IV		3	3	31	123
V	$4^z = 2 \bmod 7$	3	3	39	227
VI	$3^z = 4 \bmod 7$	4	4	89	861

III



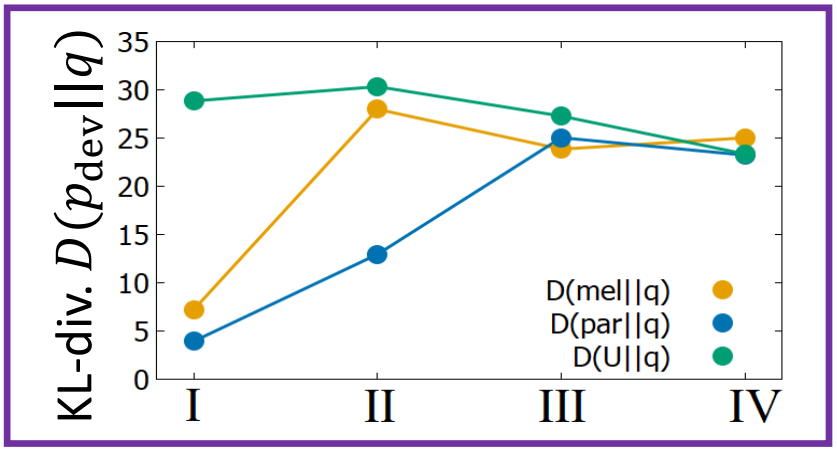
IV



実験結果の解釈(KL-divergence)

- Kullback-Leibler divergenceの比較：

$$D_{KL}(\text{デバイス出力 } p|| \text{ シミュレーター出力 } q) := \sum p(x) \log \frac{p(x)}{q(x)}$$



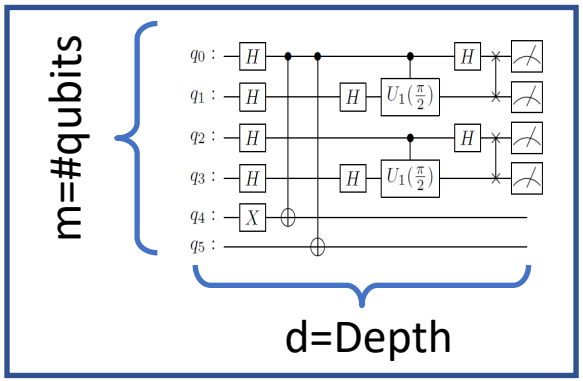
- I: Melbourune,Parisともに良い出力
- II: Parisはそれなりに良い出力
- III: KL-div.の観点からはランダムに近い
- IV以降: ランダムノイズ

■Shorアルゴリズムを用いてDLPを解く際の「成功」に関して合意が得られている定義は無いが，ParisのKL-div.の比較からI,IIに関しては良い出力が得られていると考えられる

解読能力の伸びの予測

資料 5

- Quantum Volume[Cross et al.]はわかりやすいが注意が必要
  - ○ $QV \approx 2^{\min(m,d)}$ [Cross et al.]　　$\approx 2^{\sqrt{md}}$ [Metwalli et al.]
  - ○ 1年間で2倍になる（少し前のIBM Roadmap）
  - × 計算問題ではなく、デバイスの評価
  - × For modest size (m ≲50)



- 暗号評価に必要なqubits数は数千以上
  - 2n+2 qubit 素因数分解回路[高橋-國廣2006] [Häner et al.2017]にn=2048を代入すると4098qubit必要
  - 離散対数を考えても同様の規模

【今後の方針】QVほど汎用的な基準ではなくても良いので、暗号の予測ができるものが欲しい

CRYPTREC
Cryptography Research and Evaluation Committees

資料6

CRYPTREC暗号リストでの推奨候補暗号リストの取扱いについて

令和３年３月３日
CRYPTREC事務局

CRYPTREC
Cryptography Research and Evaluation Committees

論点：リスト構成（推奨候補暗号リスト）について①

CRYPTREC暗号リストは、①電子政府推奨暗号リスト※1　②推奨候補暗号リスト※2　③運用監視暗号リスト※3　の３リスト構成となっており、この構成を維持すべきか。

※1　CRYPTRECにより安全性及び実装性能が確認された暗号技術について、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。
※2　CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト。
※3　実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったとCRYPTRECにより確認された暗号技術のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。

- ✓ 昨年度、「②推奨候補暗号リスト」については、次の点から引き続き継続検討することとされた。
  - 現行リスト改定の際に「②推奨候補暗号リスト」を含めた３リスト構成としたのは、国産暗号技術の普及展開を促進することもその目的の一つ※であるが、３リスト構成とした意図が十分に活用されている状況とは言いがたい。
    ※2011年度第1回暗号技術検討会資料3-2
  - 一方、「②推奨候補暗号リスト」は、（利用実績等が十分でないものの）安全性及び実装性能が確認されていることから、将来的に「①電子政府推奨暗号リスト」に載る可能性がある暗号アルゴリズムの受け皿としての機能もある。
  - 現状の「②推奨候補暗号リスト」には、将来的に普及することが予想され「①電子政府推奨暗号リスト」に載る可能性がある暗号技術と、掲載から十分な期間を経てもあまり普及したとは言えない暗号技術とが混在している。
  - 「②推奨候補暗号リスト」から暗号技術を削除する際の基準や手続きが定まっていない。

論点：リスト構成（推奨候補暗号リスト）について②

- ✓ 「①電子政府推奨暗号リスト」に掲載される暗号技術は、複数の利用実績等があるものが選定されており、市場からの製品調達に当たって選択性が確保されているという観点がある。
- ✓ 「②推奨候補暗号リスト」は、利用実績等が十分確認できていないものの、安全性及び実装性能を確認したものであることから、調達状況によっては有用な場合も考えられる。
- ✓ また、利用実績等の調査については、調査工数が大きく容易にできるものではないことを鑑みれば、予見可能性を高める観点からも、「①電子政府推奨暗号リスト」の予備軍として「②推奨候補暗号リスト」があることは有意義と考えられる。

→ **以上から、「②推奨候補暗号リスト」は維持することとしてよいのではないか。**

- ✓ 一方で、「②推奨候補暗号リスト」は、「「①電子政府推奨暗号リスト」に掲載される可能性のある暗号技術」とされているが、長年掲載され続けている（利用実績等がない）ものもある。
- ✓ 「②推奨候補暗号リスト」に掲載されている以上は、暗号技術の安全性に関する継続的な監視活動や再評価が必要となる。
- ✓ 今後、耐量子計算機暗号（PQC）や、軽量暗号、高機能暗号に関する評価・検討活動が必要となることから、活動リソースの最適化が必要。

→ **以上から、「②推奨候補暗号リスト」からの移行ルールを明確化すべきではないか。**

論点：リスト構成（推奨候補暗号リスト）について③

①電子政府推奨暗号リスト

次の条件のいずれかを満たすと暗号技術検討会が決定した場合
1．５年ごとの利用実績調査により、複数の利用実績を確認した場合
2．その他、普及していることが明らかな場合

安全性維持が困難（危殆化した）と暗号技術検討会が決定した場合
※電子政府推奨暗号リストに掲載された暗号技術は、利用者がいる前提であり、原則として、危殆化以外の理由では遷移させず、また、移行のための時間を確保する必要があるため、いきなりリストから削除することはしない。

標準化等により将来的な利用が見込まれ、安全性や実装性能が十分にあると暗号技術検討会が決定した場合（公募や事務局提案等）

②推奨候補暗号リスト

CRYPTREC暗号リストへの掲載から20年を超えた後に実施する最初の利用実績調査までに、十分な利用実績を確認できなかったもの
※暗号アルゴリズムの設計寿命は20年程度以上であることが期待されているが、実際にはセキュリティ向上のため、DES→TDES→AESの世代交代や公開鍵暗号の鍵長変更が20年程度で行われていることを踏まえると、20年超後に電子政府推奨暗号リストとなり活用される見込みが低い

安全性維持が困難(危殆化した)と判断した場合

③運用監視暗号リスト

2019年度暗号技術検討会で決定
次の条件のいずれかを満たすと暗号技術検討会が決定した場合、削除猶予期間を定めて周知を行った上で、その期間の満了後に自動的に削除する。
1．運用監視暗号リストに掲載している注釈で示した互換性維持のための利用形態が必要なくなり、削除が妥当と判断した場合
2．互換性維持の継続利用として使うにしても安全性維持が極めて困難で、互換性維持の継続利用が容認できないと判断した場合
3．その他、運用監視暗号リストに掲載している必要性の根拠を満たさなくなったと判断した場合

リストから削除

※利用実績調査の具体的な実施内容・評価基準については、暗号技術活用委員会において検討し、暗号技術検討会の承認を経た上で実施する。

（参考）統一基準群における記載状況

＜参考：政府機関等の対策基準策定のためのガイドライン（平成30年度版）（平成30年7月25日 内閣官房 内閣サイバーセキュリティセンター）＞

6.1.5 暗号・電子署名＜遵守事項＞

(1) 暗号化機能・電子署名機能の導入

(b) 情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「**電子政府推奨暗号リスト**」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、以下の事項を含めて定めること。

(ア) 職員等が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「**電子政府推奨暗号リスト**」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。

(イ) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「**電子政府推奨暗号リスト**」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。

(ウ) 暗号化及び電子署名に使用するアルゴリズムが**危殆化した**場合又はそれを利用した安全なプロトコルに**脆弱性が確認された場合**を想定した緊急対応手順を定めること。

(エ) 暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定めること。

（解説）

遵守事項6.1.5(1)(b)(イ)「やむを得ない場合」について

情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合においては、「**電子政府推奨暗号リスト**」に記載されたアルゴリズムを採用することが原則であるが、連携する他の情報システム側で対応していないなどの場合も想定される。このような場合においては、「**電子政府推奨暗号リスト**」に記載されたアルゴリズム以外のものを採用することもやむを得ないと考えられるが、「**推奨候補暗号リスト**」や「**運用監視暗号リスト**」を参照の上、安全性が高いアルゴリズムを採用することが必要である。

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）

平成２５年３月１日
総務省・経済産業省
（最終更新：令和2年12月21日）

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。

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
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード(注13)	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
認証暗号		該当なし
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

[1] 総務省サイバーセキュリティ統括官及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、総務省及び経済産業省における施策の検討に資することを目的として開催。

[2] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

（注1） 「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」（平成20年４月情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
https://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成25年３月１日現在）

（注2） CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注4） 初期化ベクトル長は96ビットを推奨する。

（注13） CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術[3]のリスト。

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM(注5)
共通鍵暗号	64ビットブロック暗号(注6)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128ビットブロック暗号	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
		SC2000
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01(注7)
ハッシュ関数		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128(注12)
		SHAKE256(注12)
暗号利用モード	秘匿モード	XTS(注17)
	認証付き秘匿モード(注14)	該当なし
メッセージ認証コード		PC-MAC-AES
認証暗号		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-4

（注5） KEM (Key Encapsulating Mechanism) - DEM (Data Encapsulating Mechanism) 構成における利用を前提とする。

（注6） CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注7） 平文サイズは64ビットの倍数に限る。

（注12） ハッシュ長は256ビット以上とすること。

（注14） CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

（注17） ブロック暗号には、CRYPTREC暗号リスト掲載128ビットブロック暗号を使う。利用用途はストレージデバイスの暗号化に限り、実装方法はNIST SP800-38Eに従うこと。

[3] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったとCRYPTRECにより確認された暗号技術[4]のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5(注8)(注9)
	鍵共有	該当なし
共通鍵暗号	64ビットブロック暗号(注15)	3-key Triple DES
	128ビットブロック暗号	該当なし
	ストリーム暗号	128-bit RC4(注10)
ハッシュ関数		RIPEMD-160
		SHA-1(注8)
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード(注16)	該当なし
メッセージ認証コード		CBC-MAC(注11)
認証暗号		該当なし
エンティティ認証		該当なし

（注8） 「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」（平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
https://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成25年3月1日現在）

（注9） TLS 1.0, 1.1, 1.2で利用実績があることから当面の利用を認める。

（注10） 互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。TLSでの利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。

（注11） 安全性の観点から、メッセージ長を固定して利用すべきである。

（注15） CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注16） CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

[4] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

変更履歴情報

変更日付	変更箇所	変更前の記述	変更後の記述
平成27年 3月27日	（注10）	128-bit RC4は、SSL（TLS1.0以上）に限定して利用すること。	互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。SSL/TLSでの利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。
平成28年 3月29日	推奨候補暗号リスト （技術分類：ハッシュ関数）	該当なし	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256（注12）
	（注12）	[新規追加]	ハッシュ長は256ビット以上とすること。
平成29年 3月30日	推奨候補暗号リスト （技術分類：ハッシュ関数）	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256（注12）	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE128（注12） SHAKE256（注12）
平成30年 3月29日	（注2） （注6）	より長いブロック長の暗号が利用できるのであれば、128ビットブロック暗号を選択することが望ましい。	CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。
	（注15）	[新規追加]	
	電子政府推奨暗号リスト（技術分類：共通鍵暗号）	3-key Triple DES（注3）	該当なし
	（注3）	3-key Triple DESは、以下の条件を考慮し、当面の利用を認める。 1） NIST SP 800-67として規定されていること。 2） デファクトスタンダードとしての位置を保っていること。	[削除]
	運用監視暗号リスト （技術分類：共通鍵暗号）	該当なし	3-Key Triple DES（注15）
	電子政府推奨暗号リスト	[技術分類の新設]	技術分類：認証暗号 暗号技術：該当なし
	推奨候補暗号リスト		技術分類：認証暗号 暗号技術：ChaCha20-Poly1305
	運用監視暗号リスト		技術分類：認証暗号 暗号技術：該当なし

	（注13） （注14） （注16）	[新規追加]	CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。
	電子政府推奨暗号リスト（見出し）	名称	暗号技術
	推奨候補暗号リスト（見出し）		
	運用監視暗号リスト（見出し）		
令和２年12月21日	推奨候補暗号リスト（技術分類：暗号利用モード　秘匿モード）	該当なし	XTS（注17）
	（注17）	[新規追加]	ブロック暗号には、CRYPTREC暗号リスト掲載128ビットブロック暗号を使う。利用用途はストレージデバイスの暗号化に限り、実装方法はNIST SP800-38Eに従うこと。