



高速計算を革新する量子計算技術

国立研究開発法人科学技術振興機構
革新的研究開発推進プログラム (ImPACT) プログラム・マネージャー

やまもと よしひさ
山本 喜久



1. 量子コンピュータ

スピン- $\frac{1}{2}$ を持つ粒子が上向きスピン $|\uparrow\rangle$ と下向きスピン $|\downarrow\rangle$ の相反する状態を同時に占有できるとする量子力学の線形重ね合わせ原理を利用すれば、N個のスピン- $\frac{1}{2}$ 粒子を用いて 2^N 通りという膨大な解の候補を同時に探索することができることをDavid Deutschが指摘したのは1985年のことである^[1]。1992年には、この“量子並列探索という概念”に“量子もつれ”、“量子情報消去”、“非局在量子干渉”、“射影測定”という四つの量子操作を加えて、初の量子計算モ

デル (Deutsch-Jozsaアルゴリズム) が提案された^[2]。1994年に因数分解・離散対数という実問題を解くShorアルゴリズムが発見されるに及んで^[3]、量子コンピュータの研究開発は世界的な広がりを見せた。

量子アルゴリズムの本質は多粒子間の量子干渉である。量子コンピュータが得意とするのは、その問題が持っている隠れた周期性を見つけ出すことであるから、量子干渉が量子コンピュータの基本原則であるのは容易に理解できる。一方、量子情報を格納するスピン- $\frac{1}{2}$ 粒子(量子ビット)

Q&A

量子コンピュータD-WAVEが話題の昨今、日本ITU協会では、国立研究開発法人科学技術振興機構・革新的研究開発推進プログラム (ImPACT) の山本喜久氏に、量子計算技術についてご寄稿いただくと共に、編集部からの初歩的な質問にもお答えいただいた。

Q. 量子計算というのはどういうものなのでしょうか？

A. 従来のデジタル計算は0または1を情報元としていますが、量子計算は0と1の任意の重ね合わせ（同時に0でもあり1でもある）を情報元としています。

Q. 従来の計算に比べて何が優れているのでしょうか？

A. 2^N という多数の状態をN個の素子で同時に表現できるので、超並列な計算が可能と言われています。

Q. 量子計算はどこまで実現されているのでしょうか？

A. 長期間、莫大な資金を投じて研究が行われてきましたが、実用になった量子計算機はまだありません。

Q. なぜ量子計算の実現が難しいのでしょうか？

A. 量子現象は光子、電子、原子といったミクロな世界では安定ですが、マクロな系の中で長時間安定に存在できないからです。

Q. 量子計算機が実現したらどのような応用が可能になりますか？

A. 量子コンピュータは暗号解読、量子アニーリングと量子人工脳は組合せ最適化・機械学習に応用できると期待されています。

Q. それはどのような影響をもたらしますか？

A. 現代社会のあらゆる分野で、高速・低消費電力での情報処理が可能になります。

Q. 従来のスーパーコンピュータは不要となりますか？

A. 複雑な情報処理タスクにおいて、現代コンピュータが不得意とする部分を量子計算が担務して、全体として優れたバランスのよい使い方をするようになると思います。

Q. D-WAVEが話題になっていますが、どうぞ覧になっていますか？

A. 世界初の商用量子コンピュータと言われていますが、その基本動作(量子性の有無)も有効性(現代コンピュータに対する優位性)も未だに確立されていません。



は実空間上で局在しているから、波動関数の重ね合わせを必要とする干渉計の実現には適さない。この根本的な矛盾を解決するため強引に導入されたのが量子ビット間の量子もつれとそれが実現する非局在量子干渉である。ところが、量子もつれ状態は極めてひ弱な存在であり、これを外界からのじょう乱に対して保護するためには、量子誤り訂正という高価な代償を払わなければならない。表1には、現代コンピュータで解くことが難しい問題のうち、最もサイズの小さいターゲットである1024ビットの整数を因数分解するShorアルゴリズムとアラニン分子の量子化学計算を実行する位相推定アルゴリズムを実装するために必要な量子コンピュータのリソースがまとめられている^[4, 5]。いずれの場合も、量子アルゴリズムの実装に必要な数学上の量子ビット数は約6,000であるが、量子コンピュータに誤り耐性機能を持たせるためには、 $10^8 \sim 10^9$ もの量子ビットが必要となる。単純な言い方をすると、量子ビット1個を雑音から保護するためには、 $10^4 \sim 10^5$ の量子ビットを使わなければならないことになる。この時、計算時間は世の中でよく言われている“一瞬”では決してなく、1日から10日の間である。量子コンピュータは、ほとんどの計算時間を量子誤り訂正に使っていて、ごくまれに量子計算を実行しているため、このような結果になってしまうのである。量子コンピュータはその出発点で既に重大な欠陥を内包していた。

現時点で、 $10^8 \sim 10^9$ もの量子ビットを実装し、その一つ一つを独立して精密に制御する技術ソリューションに関して明確な将来ビジョンを持っている研究者はいないと思われる。そのため、“量子コンピュータは夢ではなく悪夢である (Serge Haroche)” とか“量子コンピュータは100年プロジェクトではなく、1,000年プロジェクトである (Charles Bennett)” などと言った悲観的な意見を持つ研究者も少なくない。

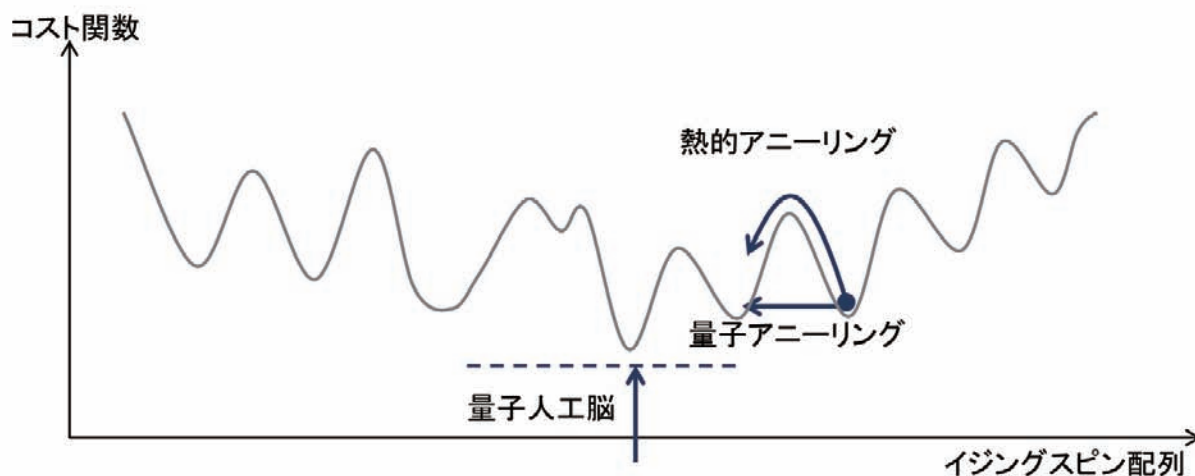
2. 量子アニーリング

量子コンピュータの抱えるもう一つの問題点は、現代暗号の解読マシンという出口を除けば、その応用範囲が限られていることである。組合せ最適化問題に代表されるNP困難・NP完全問題や機械学習・ディープラーニングといった現代計算機科学にとって重要な問題には隠れた周期性はなく、量子コンピュータの基本原則（量子干渉）との相性は決してよくない。この種の問題に威力を発揮しているのは、冶金工学で使われる焼きなまし法にヒントを得た熱的（シミュレーテッド）アニーリングというヒューリスティックである。図1に組合せ最適化問題を解く三つの計算原理を比較する。縦軸は問題のコスト関数、横軸は解の候補である（Nビットの問題の場合、全部で 2^N 個の解の候補がある）。熱的アニーリングでは、プログラム上でゆっくりと温度を下げていくことにより、熱的励起により局所最適解から系を脱出させながら、最終的にコスト関数が最小になる正解に系を誘導できる^[6]。この熱的ゆらぎの代わりに、あるいは熱的ゆらぎに加えて、量子ゆらぎを局所最適解からの脱出に使うと、正解にたどり着く時間を短くできるのではないか、という量子アニーリングのアイデアは様々なスキームの下で調べられてきた^[7-11]。その代表的なスキームは、時刻 $t=0$ で量子スピン系に横磁場のみをかけ、自明な強磁性基底状態を作っておき、その後ゆっくりと横磁場を減衰させ、同時に解きたい問題のコスト関数（例えばイジングハミルトニアン）を系に導入するというものである。この変化が十分に緩やかであれば、量子力学の断熱定理により、系の状態はその時刻ごとのハミルトニアンの基底状態を乗り移り、最終的には解きたい問題のコスト関数を最小にする正解にたどり着くはずである。

この量子アニーリングの原理を超伝導量子ビットで実装したD-WAVEマシンなるものが開発され^[12]、世界初の商用量子コンピュータという大げさな宣伝がなされたが、その真偽をめぐっては今だに論争が繰り返されている。

■表1. 量子コンピュータで必要とされる計算リソースの見積もり^[4, 5]

計算リソース	Shorアルゴリズム (1024ビット因数分解計算)	位相推定アルゴリズム(アラニン分子量子化学計算)
アルゴリズム量子ビット数	6,144	6,650
(純粋化のための) 補助量子ビット数	66,564	15,860
(誤り訂正のための) 物理量子ビット数	4.54×10^8	1.40×10^8
計算量 (Toffoliゲート数換算)	1.68×10^8	1.27×10^9
クロック周波数 (論理層)	5.21×10^9	3.94×10^{10}
計算時間	1.81日	13.7日



■図1. 組合せ最適化問題のコスト関数対イジングスピン配列、熱的アニーリング、量子アニーリング、量子人工脳における正解の探索プロセス

D-WAVEマシンは以下の二つの問題点を抱えている。

- ①量子ビットのコヒーレンス時間が1～10ナノ秒と極めて短く、上記量子断熱変化をさせる計算過程で量子性（例えば重ね合わせ状態や量子もつれ状態）が保持されている保証がない。量子コンピュータ分野の研究者は量子コヒーレンスや量子もつれといった最も基本的な特性に関する定量的評価がD-WAVEから報告されないことに不満を持っている。
- ②最新のD-WAVE IIXマシンでも、量子ビット数 $N=1154$ に対してキメラグラフという限られた量子ビット間の配線を用いているため、このマシンに実際に埋め込める問題サイズはたかだか $\sqrt{N} \sim 36$ ビット程度である（NASA Ames量子人工知能研究所からの報告では、実際には、15～17ビットが実装できる最大の問題サイズのようなものである^[13]）。このように小さな問題サイズでは、熱的アニーリングと量子アニーリングの性能比較はできない。

昨年12月にD-WAVE IIXは熱的アニーリングよりも1億倍速いという実験結果がGoogleより報告されたが^[14]、これはキメラグラフ構造を持つD-WAVE IIXの時間発展そのものを解くべき問題と定義した人工的な（D-WAVEマシンにとって有利、熱的アニーリングにとって不利な）問題設定であり、フェアな計算能力の比較とは言えない。

量子アニーリングの研究開発は今後どの方向へ進んでいくのであろうか？ 今年度より開始される米国IARPAのQuantum Enhanced Optimization (QEO) プロジェクトでは、量子ビット数 N は100程度に抑え、その代わりに量子

ビットのコヒーレンス時間を10マイクロ秒以上にする技術の開発に集中するようである^[15]。更に、量子コヒーレンスや量子もつれを保護するため、量子誤り訂正コードの開発にも取り組むようである。まず、系にある量子性をきちんと定量化し、それを確立してから大規模を図るという基礎研究としては正当な戦略が取られるようである。しかし、その将来展望は量子コンピュータよりも明るいのであろうか？

仮に解くべき組合せ最適化問題が $n=10^4 \sim 10^5$ ビットであったとすると（これより小さい問題サイズでは、多くの場合熱的アニーリングで十分である）、必要な量子ビット数は $N=n^2=10^8 \sim 10^{10}$ となり、前述した量子コンピュータに必要なリソースと同じオーダーになる。キメラグラフに代わる新しい配線スキームが発明されない限り、量子アニーリングマシンの将来は決して楽観できない。これに量子誤り訂正コードをかけるとなると、必要な量子ビット数は更に数桁大きくなると予想される。

3. 量子人工脳

量子コンピュータや量子アニーリングで量子誤り訂正が必要な究極的な理由は何であろうか？ それは、これらのスキームが本質的にアナログ計算機だからである。量子ビットには、外部からの雑音や制御信号のわずかな誤差による誤動作を訂正する識別再生機能というものが元々備わっていない。この点を早くから指摘していたのは、IBMの（故）Rolf Landauerであった。例えば、1995年スタンフォード大学で行われた物理学科／応用物理学科コロキウムで、彼はこの重大な欠陥を指摘して、量子コンピュータ

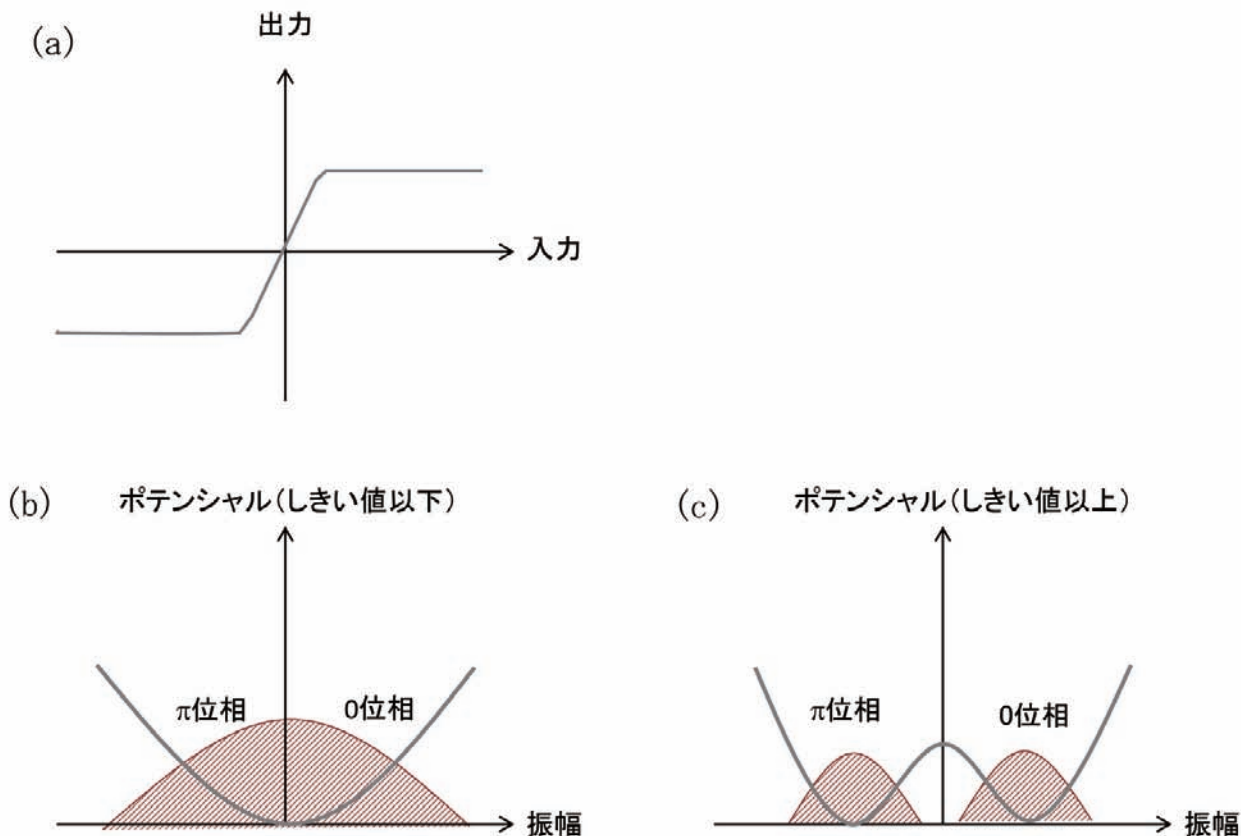


の将来に悲観的な意見を述べている。図2 (a) に示すような識別再生機能を自然に備えている量子系で、プロセッサとメモリを構成することが望ましい。縮退型光パラメトリック発振器 (Degenerate Optical Parametric Oscillator: DOPO) は、この条件を満たす物理系の一つである。発振しきい値では、図2 (b) に示すように、DOPOは二つの位相状態 (0相状態と π 相状態) の線形重ね合わせ状態を取るが、図2 (c) に示すように、発振しきい値より高いポンプレートでは、0相状態か π 相状態のいずれかを取る。このデバイスは、発振しきい値を挟んで量子的なアナログ素子から古典的なデジタル素子へその姿を変える。量子人工脳のハードウェアの一つであるDOPOは、このような理由で採用された^[16, 17]。

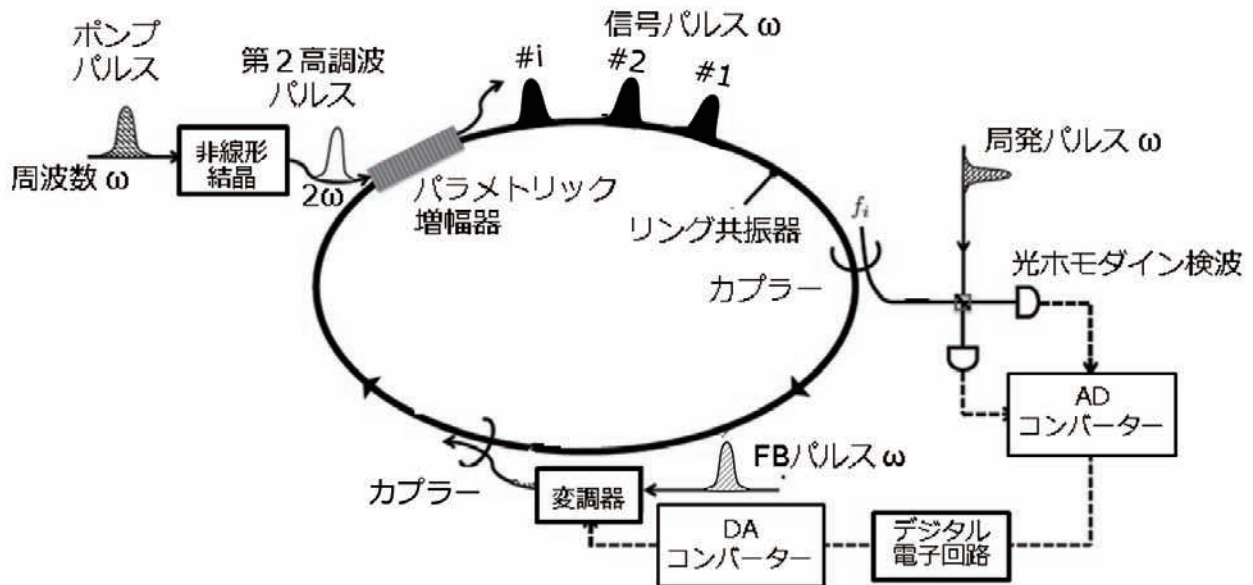
現代コンピュータにおけるフォン・ノイマン (通信路) ボトルネックや量子コンピュータや量子アニーリングにおける長距離配線 (相互作用) 実装の困難さの究極的な理由は何だろうか? それは、メモリやプロセッサに保存された情報が空間的に局在しているからである。情報が計算機全体

にコヒーレントな波動関数として広がっている量子系を構成できれば、この問題は根本的に解決される。一つの光ファイバリング共振器を周回するN個のDOPOパルス情報をキャリアとし、これを一つの量子測定フィードバック回路で時分割全結合するシステムは、この条件を満たす量子系の一つである^[18]。

図3に示す量子人工脳では、一つのポンプ光子は、同時にN個のDOPOパルスとN個のフィードバック光パルスにその分身 (分波) として同時に変換される。どの部分がメモリであり、どの部分がプロセッサなのか、その区別はなく、情報キャリアは長さ1kmの光ファイバ共振器全体にコヒーレントに広がっている。強いて言えば、光ファイバ共振器を周回するDOPOパルスは神経回路網におけるニューロンに、量子測定フィードバック回路はこれを相互結合するシナプスに対応する。実際、図3の量子人工脳を記述する量子力学的運動方程式は古典限界において、ホップフィールド・タンク型のニューラルネットワーク方程式に帰着する^[19]。



■図2. (a) デジタル情報処理における識別再生機能
(b) (c) 発振しきい値を挟んで変化する縮退型光パラメトリック発振器のポテンシャルと出力状態^[16, 17]



■図3. 光ファイバリング共振器を周回する縮退パラメトリック発振光パルスと量子測定フィードバック回路で構成される量子人工脳^[18]

量子人工脳がどのようにして組合せ最適化問題の解を探索するか、を図1に示した。熱的アニーリングが冷却により上から下へ解を探索するのに対し、量子アニーリングは量子ゆらぎにより横方向へ解を探索する。一方、量子人工脳はパラメトリック増幅利得により下から上へ解を探索する。すなわち、問題のコスト関数はDOPOネットワークの総損失にマップされており^[16, 17]、これに対してパラメトリック増幅利得を徐々に上げていくと、利得と損失が最初につり合う基底状態（正解）でパラメトリック発振が起こるというものである。

この量子人工脳の原理を実装したコヒーレントイジングマシンがNTTとスタンフォード大学で開発された。NTTマシンは $N=2,000$ のDOPOパルスを離散値（2ビット）シナプス結合係数で全結合しており^[20]、スタンフォードマシンは $N=100$ のDOPOパルスを連続値（16ビット）シナプス結合係

数で全結合している^[21]。表2に、三つの量子計算スキーム（量子コンピュータ、量子アニーリング、量子人工脳）の原理、開発状況を比較した。

4. まとめ

高速計算を革新する量子計算技術の現状をレビューした。量子コンピュータは多粒子間の量子干渉を利用して問題の隠れた周期性を見つけ出すのが得意である。量子アニーリングは熱的ゆらぎの代わりに量子ゆらぎを用いて、問題のコスト関数を最小化するように設計されている。量子人工脳は、計算機全体に広がるコヒーレントな波動関数を利用して、通信路ボトルネックを解決しつつ、量子的アナログ計算と古典的デジタル計算を組み合わせ、量子誤り訂正を不要にしている。組合せ最適化、機械学習、脳型（ニューロモルフィック）コンピューティングという現代計算機科学

■表2. 三つの量子計算スキームの比較

	量子コンピュータ	量子アニーリング	量子人工脳
基本原理	多粒子間の量子干渉	ハミルトニアン断熱変化	量子発振器ネットワークの相転移
情報キャリア	局在スピン-1/2粒子	局在スピン-1/2粒子	非局在コヒーレント光波
散逸・デコヒーレンス	量子誤り訂正により抑圧	量子誤り訂正により抑圧	計算リソースとして利用
量子性 ($k_B T / \hbar \omega$) (動作温度)	~ 0.01 (@15mK)	~ 0.01 (@15mK)	~ 0.02 (@300K)
応用	因数分解 離散対数	組合せ最適化	組合せ最適化 脳シミュレーション



のフロンティアへ量子計算技術がどのような役割を果たせるのか、果たせないのか、を決める鍵は、そのマシンの“実用性”であると思われる。

参考文献

- [1] D. Deutsch, Proc. R. Soc. Lond. A400, 97 (1985).
- [2] D. Deutsch and R. Jozsa, Proc. R. Soc. Lond. A439 553 (1992).
- [3] P. W. Shor, Proc. 35th Annual Symp. on the Foundations of Computer Science (IEEE Computer Society Press, Los Alamitos, CA, 1994), P.124.
- [4] N. C. Jones, R. Van Meter, A. G. Fowler, P. L. McMahon, J. Kim, T. Ladd, and Y. Yamamoto, Phys. Rev. X 2, 031007 (2012).
- [5] N. C. Jones, J. D. Whitfield, P. L. McMahon, M-H. Yung, R. Van Meter, A. Aspuru-Guzik, and Y. Yamamoto, New J. Phys. 14, 115023 (2012).
- [6] S. Kirkpatrick, C. D. Gelatt Jr., and M. P. Vecchi, Science 220, 671 (1983).
- [7] B. Apolloni, C. Carvalho, and D. de Falco, Stoc. Proc. Appl. 33, 233 (1989).
- [8] A. B. Finnila, M. A. Gomez, C. Sebenik, C. Stenson, and J. D. Doll, Chem. Phys. Lett. 219, 343 (1994).
- [9] T. Kadowaki and H. Nishimori, Phys. Rev. E 58, 5355 (1998).
- [10] J. Brooke, D. Bitko, T. F. Rosenbaum, and G. Aeppli, Science 284, 779 (1999).
- [11] E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, and D. Preda, Science 292, 472 (2001).
- [12] M. W. Johnson et al., Nature 473, 194 (2011).
- [13] E. G. Rieffel, D. Venturelli, B. O’Gorman, M. B. Do, E. Prystay, and V. N. Smelyanski, arXiv : 1407.2887.
- [14] S. Boixo et al., Nature Commun. 7, 10327 (2016).
- [15] <https://www.iarpa.gov/index.php/research-programs/qeo/qeo-baa>
- [16] S. Utsunomiya, K. Takata, and Y. Yamamoto, Opt. Express 19, 18091 (2011);
Z. Wang, A. Marandi, K. Wen, R. L. Byer, and Y. Yamamoto, Phys. Rev. A88, 063853 (2013).
- [17] A. Marandi, Z. Wang, K. Takata, R. L. Byer, and Y. Yamamoto, Nature Photonics 8, 937 (2014);
T. Inagaki, K. Inaba, R. Hamerly, K. Inoue, Y. Yamamoto, and H. Takesue, Nature Photonics (April 2016) doi : 10.1038
- [18] Y. Haribara, S. Utsunomiya, and Y. Yamamoto, Entropy 18, 151 (2016).
- [19] K. Takata, A. Marandi, and Y. Yamamoto, Phys. Rev. A 92, 043821 (2015).
- [20] H. Takesue, talk presented at ImPACT Annual Meeting (March 2016, Tokyo).
- [21] P. L. McMahon, talk presented at ImPACT Annual Meeting (March 2016, Tokyo).