2-8　エレクトロニクス技術を変革する量子情報技術

Quantum Information Technology:Quantum Innovation in Electronics, Information and Communication

井元信之　北川勝浩

Abstract

量子力学を使うことによって古典力学よりも本質的に優れた性能を発揮し得る量子暗号，量子情報処理，量子計測などの量子情報技術の現状と将来展望を述べる．量子コンピュータでは，最も進んでいる超伝導で 20 量子ビット程度が実現しており，50 量子ビットへの競争が始まっている．量子計測では，光格子時計が現在の秒の標準より二桁高い精度を達成し，次の秒の標準の有力候補となっている．

キーワード：量子情報，量子暗号，量子コンピュータ，量子アルゴリズム，量子シミュレーション，量子計測，光格子時計

1. は　じ　め　に

超伝導もレーザも量子力学でなければ説明できないという意味では量子技術である．しかし，量子力学を使うことによって，情報処理や通信や計測において古典力学よりも本質的に優れた性能を発揮し得るものを，ここでは量子情報技術と呼び，量子暗号，量子コンピュータ，量子計測の現状と将来展望について述べる．本特集の趣旨と，量子情報技術がまだほとんど世に出ていない研究途上の分野であることから，本稿で述べる将来展望は，筆者らの見解であって，必ずしも分野のコンセンサスとは限らないことをお断りしておく．

2. 量子暗号の現状と将来展望

量子暗号は「絶対安全な夢の暗号」として期待されるが，実際は「実用の域にあるが絶対安全と言えない」ものから「課題山積みだが絶対安全が期待される」ものまである．量子暗号は 1984 年の BB84 の提案[(1)]に遡るが，他者の参入が始まったのは，理論は 1990 年頃から[(2)]，実験は 1993 年頃からである．日本では 1995 年には論文が書かれ[(3)]，以来分野として定着・発展してきた．2000 年前後には市販装置を手がけるヴェンチャーが欧米で相次いで設立され，日本でも 2010 年の東京 QKD[(4)]の現場試験に企業群が参加し，それを NICT の佐々木らが統括した．2012 年になると中国でも量子暗号ネットワークの実験が行われ，ロスアラモス研究所では量子暗号を利用した電力系統の制御保護実験を行っている．光ファイバでなく空間伝搬を用いる量子暗号の研究も 2000 年頃から本格的に始まった．当初の目的は光ファイバの損失制限の打破であったが，次第に衛星間あるいは地上―衛星間量子暗号へ移ってきている．2016 年に中国が量子暗号実験衛星を打ち上げたのは記憶に新しい．今年の Quantum 2017 では Huawei が衛星間量子暗号構想を発表していた．

こう見ると量子暗号は商用間近に見えるが，目的基礎研究の様相も強い．例えば量子信号は途中で識別再生や増幅により安全でなくなるので，長距離伝送のためには量子中継器が必要となる．これは弱まった信号が雑音に埋もれる前に識別し再生する現行の中継器の量子版で，重ね合わせ状態を壊さないよう「識別せずに再生する」中継器である．また最初の提案である BB84 方式は量子

井元信之　大阪大学大学院基礎工学研究科物質創成専攻
E-mail　imoto@mp.es.osaka-u.ac.jp
北川勝浩　大阪大学大学院基礎工学研究科システム創成専攻
E-mail　kitagawa@ee.es.osaka-u.ac.jp
Nobuyuki IMOTO and Masahiro KITAGAWA, Nonmembers (Graduate School of Engineering Science, Osaka University, Toyonaka-shi, 560-8531 Japan).
電子情報通信学会誌　Vol.100 No.9 pp.968-973 2017 年 9 月

もつれを使わないが E91 は使う方式である．これは「ベル不等式が破れているなら安全，そうでなければ安全は保証されない」方式で，基礎研究段階にある．データのみから安全性が確認できる E91 は，装置が信頼できない場合に特に必要となる．これを進めたのが「装置無依存量子暗号」[5]である．

量子暗号の安全性証明は運用実績を積むことが大事であるが，導入前は理論的な証明しかない．最初は理想的デバイスを仮定する証明に始まり徐々に現実を取り入れた証明に進歩している．日本でも小芦[6]，小柴らの研究が大きく貢献しており，最近若い研究者も多く参入し，日々進歩している．

実用的な量子暗号の研究に限っても要素技術は目的基礎研究のものが多い．単一光子源はまだ「オンデマンドで確率 1 できっかり 1 個」の光子を出すまでに至っていない．単一光子検出器も量子効率が 1 でかつダークカウントが 0 のものはない．近年開発されている SSPD[7]や TES[8]などの超伝導光子検出器はダークカウントが少なく，量子効率も高く，ジッタも少なく，通信波長帯（波長 1.5 μm 近辺）にも高い量子効率を有するなどの特徴がある．こうした検出器の重要性を示す例を挙げると，市販の半導体光子検出器ではジッタが大きいので，その時間揺らぎをカバーするよう時間的窓を広げる必要があるが，そうすると雑音を拾うので，本当は量子領域を実現している実験でも，統計的推定の結果古典領域を越えていないという判定になる．しかしジッタの少ない SSPD を使うと窓を狭めて SN 比を上げられるので，信頼できる統計的推定ができるようになる[9]．

以上，光子ベースの量子暗号の話を主体に述べてきたが，現行のコヒーレント光通信に近い方式として，光子でなくコヒーレント状態を用いる量子暗号もある．中でも注目されるのは DPSK（Differential Phase Shift Keying）方式[10]，それを「隣同士の光パルスでなくランダムに」位相比較するラウンドロビン方式[11]，はたまたその改良を図った方式[12]があり，実証実験も行われたが[13]，実用には更なる改良が必要である．同じくコヒーレント状態を用いるもう少し実用的な方法としてデコイ方式と呼ばれる方式もある[14]．デコイというのは囮（おとり）の意味で，盗聴者の検知のためのテスト光パルスの強さを複数用意することで検出効率を格段に上げるもので，実際に検証もされている．

量子暗号の研究開発はいろいろなベクトルを向いており，実用までの距離も様々である．究極の安全性や長距離伝送を追究する目的基礎研究は多様なまま発展するだろう．一方，商用に近い手軽な量子暗号はいずれ淘汰のフェーズに入って行くであろう．実用のためには「標準化」が必要であるが，今はまだその動きが少ない．まずは要素技術の標準化を進め，徐々に方式の標準化に向かう必要がある．今後の量子暗号の研究開発は，高度な方式の多様な追究と実用を目指した標準化の動きの両方が重要となろう．

3. 量子情報処理の現状と将来展望

まず，量子コンピュータの歴史を簡単に述べる．1982 年にファインマンが，量子物理系を古典コンピュータでシミュレートすると計算量が爆発する困難を指摘し，それを解決できる万能量子シミュレータとして量子コンピュータの概念に触れた[15]．ドイチェが，1985 年に計算の量子力学的モデルを示し，万能量子コンピュータを万能チューリングマシンの量子版である量子チューリングマシンとして表し[16]，1989 年に論理ゲートと論理回路の量子版である量子ゲートと量子回路を導入して表した[17]．彼は 1992 年に，量子コンピュータで古典コンピュータよりも速く解ける問題とアルゴリズムを例示した[18]．1993 年には，バーンスタインとヴァジラニが量子チューリングマシンの計算量[19]，ヤオが量子回路の計算量を研究し[20]，量子計算量理論の端緒が開かれた．1994 年には，ショアが桁数 n の整数の素因数分解を $O(n^3)$ 以下の手間で効率的に解く量子アルゴリズムを考案した[21]が，素因数分解は知られている最良のアルゴリズムである一般数体ふるい法でも n の準指数の手間がかかり，その素因数分解の困難性が RSA 公開鍵暗号の安全性の根拠であったので，大きな衝撃を与えた．これを契機として量子コンピュータが広く知られるようになり，その実現を目指した研究が様々な物理系で行われるようになった．1996 年にはグローヴァーが，ソートされていない N 個のデータから一つのデータを検索するのに，古典的には $O(N)$ 回掛かるのを $O(\sqrt{N})$ 回で済む量子アルゴリズムを考案した[22]．

ここで，量子コンピュータを量子回路モデルで簡単に説明する．量子コンピュータでは，コンピュータのビットに相当する量子ビット（qubit）が情報を担い，それに対して量子ゲートを作用させて計算を行う．量子ビットは物理的にはスピン 1/2 であり，論理レベルの 0 と 1 を表す $|0>$ と $|1>$ の任意の重ね合わせ状態 $|\psi>=\alpha|0>+\beta|1>$ を取ることができる（$\alpha,\beta\in\boldsymbol{C}$）．1 量子ビットの量子ゲートとしては，例えば，古典的な NOT に相当する X ゲート（$X=|1><0|+|0><1|$）や，$Z=|0><0|-|1><1|$ ゲートなどがある．量子回路で頻繁に現れるアダマールゲート $H=(X+Z)/\sqrt{2}$ は，$|0>$ に作用すると $H|0>=(|0>+|1>)/\sqrt{2}$ と重ね合わせを作る．これらの演算子は，物理的にはスピンの π 回転を表す．また，2-qubit の代表的な量子ゲートである制御 NOT ゲートは $CN=|0><0|\otimes I+|1><1|\otimes X$ で表され，1-qubit 目が $|1>$ のときのみ 2-qubit 目を NOT する．

量子ビットに重ね合わせの状態を許すと，量子並列性

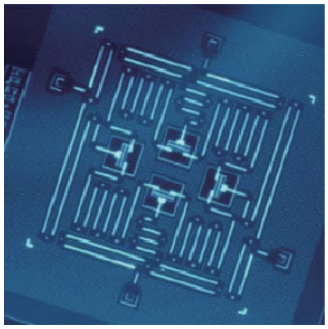
が生じる．n-qubit が初期状態 $|0\rangle\cdots|0\rangle$ にあるとして，全ての qubit に H を作用させると，$|\psi\rangle=((|0\rangle+|1\rangle)/\sqrt{2})\cdots((|0\rangle+|1\rangle)/\sqrt{2})=(|0\cdots0\rangle+|0\cdots1\rangle+\cdots+|1\cdots1\rangle)/2^{n/2}$ となり，n-bit の全ての数の重ね合わせの状態ができる．ユニタリ変換 U が x から $f(x)$ を計算するタスクを $U|x\rangle|0\rangle=|x\rangle|f(x)\rangle$ とすると，$U|\psi\rangle|0\rangle=(|0\rangle|f(0)\rangle+|1\rangle|f(1)\rangle+\cdots+|2^n-1\rangle|f(2^n-1)\rangle)/2^{n/2}$ によって 2^n 個の x について並列的に $f(x)$ の計算が行われ，手間は一つの x と変わらない．しかし，$|x\rangle|f(x)\rangle$ の確率振幅は $1/2^{n/2}$ であり，確率 $1/2^n$ でしか結果を読み出せないので，それだけでは計算は速くならない．ここで $f(x)$ が周期関数の場合には，$|x\rangle$ の方に FFT の量子版である量子フーリエ変換（QFT）[18] を適用すると，干渉効果で周期が抽出できる．これがショアのアルゴリズム [21] の原理である．このように，干渉効果によって，正解の確率振幅は足し合わされ，不正解の確率振幅は打ち消し合うようにするのが，量子アルゴリズムであり [18]，そのためには重ね合わせの位相が保たれていなければならない．

量子ビットの重ね合わせの位相は，環境との相互作用によって容易に破壊されてしまう．このデコヒーレンスが，量子コンピュータを実現する上で最大の障害となることは，当初から予想されており，ショアのアルゴリズム提案後すぐに量子誤り訂正符号のアイデアが出された [23]．古典的な誤り訂正と本質的に異なるところは，量子状態は複製できないこと，観測すると $|0\rangle$ か $|1\rangle$ に収縮してしまい重ね合わせの情報が失われること，量子誤りはビットフリップ X と位相フリップ Z 及びそれらが同時に起こることを解決しなければならないことである．古典的な線形符号を組み合わせて X 基底と Z 基底で誤り訂正を行うが，符号化された量子情報は観測せずに，誤りのシンドロームのみを観測することによって量子誤りが訂正可能であることが示された．例えば，1-qubit を 7-qubit に符号化することによって 1-qubit の量子誤りから守ることができる．更に，1997 年には，量子誤り訂正過程を含む全ての量子演算に誤差を許しても，誤差があるしきい値以下であれば，信頼性の高い量子計算が行われる誤り耐性量子計算の概念によって，大規模量子計算の可能性が示された [24]．ここまでの教科書として文献 (25) を挙げておく．当初のしきい値は 0.001% 程度と悲観的な値であったが，2007 年にラッセンドルフが，Kitaev のトポロジカル量子計算 [26] から，二次元的に配列した qubit で最隣接間の量子演算だけを用いた表面符号に基づき 0.75% のしきい値を持つ方式を考案し [27]，実現の可能性が現実味を帯びてきた．

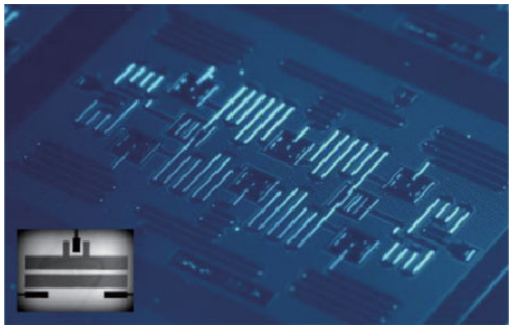
本稿を執筆している 2017 年春の時点で，量子コンピュータをめぐる状況は大きく動いている [28]．現時点で，量子コンピュータのハードウェアとして最も進んでいるのは超伝導量子ビットである．主な研究拠点は，米国では UCSB/Google，IBM，Yale 大，Rigetti，欧州ではオランダの Delft 工科大，日本では東大／理研／NEC などである．最近では IBM が 2017 年 3 月に，産業界初の万能量子計算システム IBM Q の商用化を目指すと発表し，2〜3 年以内に 50-qubit を目標にすることを明らかにした．IBM は，既に 5-qubit の超伝導量子コンピュータをクラウド経由で公開していたが，5 月には 16-qubit に更新した．Google は，後で述べる D-Wave から 512-qubit のマシンを買っていたが，その後 2014 年の秋に UCSB の Martinis グループを自前の量子コンピュータを作るために雇った [28]．Google は今年中に 50-qubit の超伝導量子コンピュータを作って，スーパコンピュータに対する量子優越性 [29] を達成する計画のようである [28]．このように，現在，超伝導量子コンピュータのトップグループは 50-qubit [注1] を目指してしのぎを削っている．C. Rigetti は，Yale 大で 7 年，IBM で 3 年超伝導量子ビットの研究に携わった後，2013 年に独立して起業し，既に 70 億円の投資を集めた．量子コンピュータへの投資という点で，先鞭をつけたのは D-Wave であり，1,000 万円の出資金で 1999 年に起業し，総額 180 億円の投資を集めた．量子コンピュータの開発には，途方もないリソースとエフォートが必要だが，その中には大きなブレークスルーをもたらす天才的なアイデアが必要な部分と，人海戦術で膨大なリソースを投入すれば解決できる部分があり，ばく大な投資が集められれば後者は確実に加速し，前者の天才的人材も集められるかもしれない．しかし，超伝導量子ビットをここまで育て上げたのは，地道な基礎研究であった．

1999 年に世界で初めて超伝導量子ビットを実現したのは，NEC 基礎研究所の中村，Tsai らであり，Cooper Pair Box の電荷の状態を量子ビットとしたものであった [30] が，コヒーレンス時間は 1 ns しかなかった．超伝導では，電荷のほかに，磁束，位相などの状態を量子ビットとして用いることができ，回路や材料の改良とともに，コヒーレンス時間の大幅な改善がなされてきた [31], [32]．現時点で最もコヒーレンス時間が長いのは 2007 年に Yale 大が考案したトランズモン（transmon）型 [33] であり，当時 1 μs を実現した．これは，Cooper Pair Box を大きな静電容量でシャントして非線形振動子にしたもので，下から二つの準位を量子ビットとして用いる．電荷エネルギーよりもジョセフソンエネルギーの方が支配的で，電荷揺らぎの影響を受け難いため，非常に長いコヒーレンス時間を示す．その後もトランズモン型量子ビットは改良され続けて，コヒーレンス時間は 100 μs まで伸びている [34]．現在，主要グループの超伝

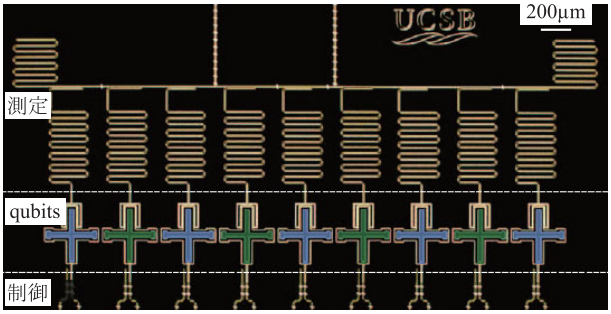
（注 1） 50-qubit の量子系はスーパコンピュータでシミュレートすることが困難であり，量子優越性が期待される．また，7×7＝49-qubit が表面符号による量子誤り訂正のマイルストーンと考えられている．



(a) IBMの4-qubit[34]



(b) IBMの8-qubit[34]



(c) UCSBの9-qubit[36]

図1　トランズモン型超伝導量子ビットの集積回路

導量子ビットはほとんどトランズモン型である（図1）．量子演算の精度も向上し，2014年に表面符号による誤り耐性しきい値[27]以下の誤差が達成された[35]．表面符号を意識した二次元の実験[34]や一次元の9-qubit実験[36]も行われている．誤り耐性を確保するには多数の量子ビットを二次元的に配列し，最近接qubit間の量子演算で表面符号を実装する必要があるが，当面は50-qubit程度までの実装が目標であろう．中国も超伝導量子ビットで急速に実力を付けてきており，最近10-qubitのエンタングルメントを報告している[37]．

量子ビットの規模として超伝導とほぼ並んでいるのが，イオントラップであり，メリーランド大のモンローのグループは，5-qubitで任意の量子回路を組み，小規模なアルゴリズムを実行している[38]．モンローは2015年にIonQを起業している[28]．Microsoft Station Qは，まだ全くの未知数であるが物理的に頑強な量子ビットになると期待されるマヨラナ粒子を用いたトポロジカル量子計算[26]に絞って，Delft工科大などとコンソーシアムを組んで研究を行っている[28]．半導体では原子レベルのドーピングや量子ドットを用いた方式が提案され，日，欧，豪などで実験されているが，詳細は最近の解説[32],[39]を参照されたい．

現在，量子コンピュータが注目されているもう一つの理由は，D-Waveが2,000-qubitの量子コンピュータを既に市販し，しかも，NP困難な組合せ最適化問題を速く解くと喧伝していることである[40]．このD-Waveマシンは，超伝導量子ビットを2,000個集積化してはいるが，量子ゲートは実装されておらず，門脇・西森の量子アニーリング[40]をハードウェア的に実行する専用機である．組合せ最適化問題を，イジングモデルという古典スピン（$\sigma_i=\pm1$）の多体系のエネルギー$H=-\sum_{i<j}J_{ij}\sigma_i\sigma_j$を最小化して基底状態を求める問題にマップすることができ，それを解く方法の一つが量子アニーリングである．問題はスピン間の相互作用を表すJ_{ij}としてプログラムされる．我が国で開発されたコヒーレントイジングマシンは，光パラメトリック発振器のポンピングを発振しきい値に下から近付けてゆくと最も損失の小さいモードで発振するという原理に基づいてHを最小化し，2,000ノードの実験が行われている[41]．これらは，最小化しようとしているHをアナログ量として実現しているため，本質的にアナログ計算機であり，NP困難な問題に答えを出しても計算量理論に反しないが，不可避な誤差によってどこまでスケールするか不明である．

ファインマンが想起した量子シミュレーション[15]は，ディジタル量子コンピュータではソフトウェア的に実現される．現時点では比較的制御性の高い量子系である光格子中の中性原子やイオントラップを用いたアナログ量子シミュレーションの実験が盛んに行われている[42]．これはパラメータが比較的自在に変えられる量子物理実験であり，ハバードモデルによる高温超伝導の機構解明などが期待されている．これが，新しい電子材料の開発につながることを期待したい．

4. 量子計測の現状と将来展望

量子計測のうち本会に最も関係が深い時間標準・周波数標準では，香取が2001年に提案した光格子時計[43]が10^{-18}の精度を実現し，現在の秒の標準であるセシウム原子時計の10^{-16}を既に二桁凌駕している．秒の二次表現に採用され，次の秒の標準の有力候補となっている．光格子時計の精度は，一般相対論に基づく重力による時間の遅れを介して標高差をセンチメートル精度で計測できることを意味しており，測地や資源探索への応用も期待される[44]．光格子時計の原理を簡単に説明する．

ドップラーシフトを避けるために，原子は極低温に冷却されて，強いポテンシャル中に閉じ込められていなければならない．しかし，一つの原子が出す信号は量子不確定性のためにSN比が悪く，多数回繰り返し測定しなければ精度が出ない．光格子時計では，レーザで三次元的な干渉じま（光格子）を作り，電界の腹に原子をトラップすることによって，一度にN個の原子の信号を見ることで，SN比は1個の場合の$\sqrt{N}$倍に向上する．原子をトラップするための光格子の強力な電界によって，原子のエネルギー準位がシフトし，遷移周波数が電界に依存して変わってしまうと標準として使えないが，時計遷移の両方の準位に対するシフトが等しくなる波長（魔法波長）が存在することに香取は気付き，それが光格子時計の誕生へとつながった．

光格子時計の原子数Nによる精度向上は，量子力学的にはスピン1/2をN個集めて同じ状態にしたスピン$N/2$のコヒーレントスピン状態の量子不確定性が$1/\sqrt{N}$となる標準量子限界に相当する．N個のスピンの間にエンタングルメントを作れば，量子不確定性を真の量子限界（ハイゼンベルク限界）$1/N$まで減らせる可能性があり[45]，この原理が量子計測に実用的な恩恵をもたらすことを期待したい．

5. おわりに

大規模な量子コンピュータの実現は非常に挑戦的な目標であるが，科学と工学のフロンティアであることは間違いなく，アポロ計画のようにその過程で多くの科学的，技術的な副産物を生み出すことが期待される．欧米は官民ともにばく大な研究投資を始めており[28]，量子情報に特化した研究センターや研究プログラムで人材育成も行われている．

超伝導量子ビットに限らず量子ビット系の課題は，集積化であろう[34]．量子ビットをたくさん並べて，それらの間を量子的な媒体でつないで演算する方式で集積度を上げるには，マイクロ波技術や材料，半導体で培われた集積技術などを駆使する必要がある．そういう意味で，量子コンピュータの開発には，本会の様々な分野の専門家が貢献できる可能性がある．2016年秋にはERATO中村巨視的量子機械プロジェクトが始まり，超伝導量子コンピュータの研究に我が国でも大きな期待がかかっている．本格的な量子コンピュータ実現への道はまだまだ入口の段階であり，将来的にどの物理系が大規模化を実現するかはまだ分からない[28]．欧米中並の研究投資を人材育成まで含めて長期的視野で行えば，我が国にも十分チャンスはあるはずである．

量子コンピュータは素因数分解しかできないという誤解があるが，素因数分解は古典コンピュータよりも量子コンピュータが強力であることの強い傍証の一つにすぎない．それ以外にも，量子シミュレーションや量子化学計算[46]には大きな期待があるし，機械学習に使える可能性もある[47]．まだ存在もしない量子コンピュータのアルゴリズムを考えたのはほんの一握りの研究者であったが，既に目の前に16-qubitの量子コンピュータがあって誰でもインターネットからアクセスでき，近々50-qubitの量子コンピュータが実現するとすれば，話は違ってくる．これからは誰でも量子アルゴリズムの研究ができる．新しい画期的な量子アルゴリズムが生み出されることを期待したい．

文　献

（1） C.H. Bennett and G. Brassard, “Quantum cryptography : Public key distribution and coin tossing,” Proc. IEEE Inter. Conf. on Computers Systems and Signal Processing, pp. 175-179, Bangalore India, Dec. 1984.

（2） A.K. Ekert, “Quantum cryptography based on Bell’s theorem,” Phys. Rev. Lett., vol. 67, no. 6, pp. 661-663, Aug. 1991.

（3） B. Huttner, N. Imoto, N. Gisin, and T. Mor, “Quantum cryptography with coherent states,” Phys. Rev. A, vol. 51, pp. 1863-1970, March 1995.

（4） M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J.F. Dynes, A.R. Dixon, A.W. Sharpe, Z.L. Yuan, A.J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger. “Field test of quantum key distribution in the Tokyo QKD Network,” Opt. Express, vol. 19, no. 11, pp. 10387-10409, 2011.

（5） U. Vazirani and T. Vidick, “Fully device-independent quantum key distribution,” Phys. Rev. Lett., vol. 113, 140501, Sept. 2014.

（6） M. Koashi, “Simple security proof of quantum key distribution based on complementarity,” New J. Phys., vol. 11, 045018, April 2009.

（7） S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, and Z. Wang, “Multichannel SNSPD system with high detection efficiency at telecommunication wavelength,” Opt. Lett., vol. 35, no. 13, pp. 2133-2135, 2010.

（8） D. Fukuda, G. Fujii, A. Yoshizawa, H. Tsuchida, R.M.T. Damayanthi, H. Takahashi, S. Inoue, and M. Ohkubo, “High speed photon number resolving detector with Titanium transition edge sensor,” J. Low Temp. Phys., vol. 151, no. 1, pp. 100-105, Jan. 2008.

（9） R. Ikuta, T. Kobayashi, K. Matsuki, S. Miki, T. Yamashita, H. Terai, T. Yamamoto, M. Koashi, T. Mukai, and N. Imoto, “High-fidelity conversion of photonic quantum information to telecommunication wavelength with superconducting single-photon detectors,” Phys. Rev. A, vol. 87, 010301(R), July 2013.

（10） K. Inoue and Y. Iwai, “Differential-quadrature-phase-shift quantum key distribution,” Phys. Rev. A, vol. 79, 022319, Feb. 2009.

（11） T. Sasaki, Y. Yamamoto, and M. Koashi, “Practical quantum key distribution protocol without monitoring signal disturbance,” Nature, vol. 509, pp. 475-478, May 2014.

（12） Y. Hatakeyama, A. Mizutani, G. Kato, N. Imoto, and K. Tamaki, “Differential-phase-shift quantum-key-distribution protocol with a small number of random delays,” Phys. Rev. A, vol. 95, 042301, April 2017.

（13） H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, “Experimental quantum key distribution without monitoring signal disturbance,” Nature Photonics, vol. 9, no. 12, pp. 827-831, 2015.

（14） W.-Y. Hwang, “Quantum key distribution with high loss : Toward global secure communication,” Phys. Rev. Lett., vol. 91, no. 5, 057901, Aug. 2003.

（15） R.P. Feynman, “Simulating physics with computers,” Int. J. Theor.

Phys., vol. 21, nos. 6/7, pp. 467-488, 1982.
(16) D. Deutsch, “Quantum theory, the Church-Turing principle and the universal quantum computer,” Proc. R. Soc. Lond. A, vol. 400, no. 1818, pp. 97-117, July 1985.
(17) D. Deutsch, “Quantum computational networks,” Proc. R. Soc. Lond. A, vol. 425, no. 1868, pp. 73-90, Sept. 1989.
(18) R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, “Quantum algorithms revisited,” Phil. Trans. R. Soc. Lond. A, arXiv : quant-ph/9708016, 1997.
(19) E. Bernstein and U. Vazirani, “Quantum complexity theory,” SIAM J. Comput., vol. 26, no. 5, pp. 1411-1473, 1997.
(20) A.C.-C. Yao, “Quantum circuit complexity,” Proc. 34th Ann. IEEE Symp. Found. Comp. Sci., pp. 352-361, 1993.
(21) P.W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM J. Comput., vol. 26, no. 5, pp. 1484-1509, 1997.
(22) L.K. Grover, “Quantum mechanics helps in searching for a needle in a haystack,” Phys. Rev. Lett., vol. 79, no. 2, p. 325, July 1997.
(23) A.R. Calderbank and P.W. Shor, “Good quantum error-correcting codes exist,” Phys. Rev. A, vol. 54, no. 2, pp. 1098-1106, Aug. 1996.
(24) J. Preskill, “Fault-tolerant quantum computation,” arXiv : quant-ph/9712048, 1997.
(25) M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information, Cambridge Univ. Press, 2000.
(26) A.Y. Kitaev, “Fault-tolerant quantum computation by anyons,” arXiv : quant-ph/9707021, 1997.
(27) R. Raussendorf and J. Harrington, “Fault-tolerant quantum computation with high threshold in two dimensions,” Phys. Rev. Lett., vol. 98, no. 19, 190504, May 2007.
(28) G. Popin, “Scientists are close to building a quantum computer that can beat a conventional one,” Dec. 2016, http://www.sciencemag.org/news/2016/12/scientists-are-close-building-quantum-computer-can-beat-conventional-one, D. Castelvecchi, “Quantum computers ready to leap out of the lab in 2017,” Nature, vol. 541, no. 7635, pp. 9-10, Jan. 2017.
(29) J. Preskill, “Reliable quantum computers,” arXiv : quant-ph/1203.5813v3, 2012.
(30) Y. Nakamura, Y.A. Pashkin, and J.S. Tsai, “Coherent control of macroscopic quantum states in a single-cooper-pair box,” Nature, vol. 398, pp. 786-788, April 1999.
(31) W.D. Oliver and P.B. Welander, “Materials in superconducting quantum bits,” MRS Bulletin, vol. 38, no. 10, pp. 816-825, Oct. 2013.
(32) 阿部英介，伊藤公平，“固体量子情報デバイスの現状と将来展望，”応用物理，vol. 86, no. 6, pp. 453-466, 2017.
(33) J. Koch, T.M. Yu, J. Gambetta, A.A. Houck, D.I. Schuster, J. Majer, A. Blais, M.H. Devoret, S.M. Girvin, and R.J. Schoelkopf, “Charge-insensitive qubit design derived from the Cooper pair box,” Phys. Rev. A, vol. 76, no. 4, 042319, Oct. 2007.
(34) J.M. Gambetta, J.M. Chow, and M. Steffen, “Building logical qubits in a superconducting quantum computing system,” npj Quantum Information, vol. 3, no. 2, Jan. 2017.
(35) R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T.C. White, J. Mutus, A.G. Fowler, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, C. Neill, P. O’Malley, P. Roushan, A. Vainsencher, J. Wenner, A.N. Korotkov, A.N. Cleland, and J.M. Martinis, “Superconducting quantum circuits at the surface code threshold for fault tolerance,” Nature, vol. 508, pp. 500-503, April 2014.
(36) J. Kelly, R. Barends, A.G. Fowler, A. Megrant, E. Jeffrey, T.C. White, D. Sank, J.Y. Mutus, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, I.-C. Hoi, C. Neill, P.J.J. O’Malley, C. Quintana, P. Roushan, A. Vainsencher, J. Wenner, A.N. Cleland, and J. M. Martinis, “State preservation by repetitive error detection in a superconducting quantum circuit,” Nature, vol. 519, pp. 66-69, March 2015.
(37) C. Song, K. Xu, W. Liu, C. Yang, S.-B. Zheng, H. Deng, Q. Xie, K. Huang, Q. Guo, L. Zhang, P. Zhang, D. Xu, D. Zheng, X. Zhu, H. Wang, Y.-A. Chen, C.-Y. Lu, S. Han, and J.-W. Pan, “10-qubit entanglement and parallel logic operations with a superconducting circuit,” arXiv : 1703.10302, 2017.
(38) S. Debnath, N.M. Linke, C. Figgatt, K.A. Landsman, K. Wright, and C. Monroe, “Demonstration of a small programmable quantum computer with atomic qubits,” Nature, vol. 536, pp. 63-66, Aug. 2016.
(39) 川上恵里加，“Si 量子ドット中の単一電子スピンを用いた量子コンピューターの実現へ向けて，”日本物理学会誌，vol. 72, no. 5, pp. 334-338, May 2017.
(40) 西森秀稔，大関真之，量子コンピュータが人工知能を加速する，日経 BP, 2016.
(41) T. Inagaki, Y. Haribara, K. Igarashi, T. Sonobe, S. Tamate, T. Honjo, A. Marandi, P.L. McMahon, T. Umeki, K. Enbutsu, O. Tadanaga, H. Takenouchi, K. Aihara, K. Kawarabayashi, K. Inoue, S. Utsunomiya, and H. Takesue, “A coherent Ising machine for 2000-node optimization problems,” Science, vol. 354, no. 6312, pp. 603-606, Nov. 2016.
(42) 福原　武，“光格子中の冷却原子により実現する量子シミュレーター，”光学，vol. 44, no. 12, pp. 476-481, 2015.
(43) 香取秀俊，“光格子時計の発明と展開，”応用物理，vol. 81, no. 8, pp. 656-662, 2012.
(44) T. Takano, M. Takamoto, I. Ushijima, N. Ohmae, T. Akatsuka, A. Yamaguchi, Y. Kuroishi, H. Munekane, B. Miyahara, and H. Katori, “Geopotential measurements with synchronously linked optical lattice clocks,” Nature Photon., vol. 10, pp. 662-666, Aug. 2016.
(45) M. Kitagawa and M. Ueda, “Squeezed spin states,” Phys. Rev. A, vol. 47, no. 6, 5138, June 1993.
(46) A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P.J. Love, A. Aspuru-Guzik, and J.L. O’Brien, “A variational eigenvalue solver on a photonic quantum processor,” Nat. Commun., vol. 5, 4213, 2014.
(47) I. Kerenidis and A. Prakash, “Quantum recommendation systems,” arXiv : 1603.08675v3, 2016.

井元（いもと）　信之（のぶゆき）

昭 50 東大・工・物工卒．昭 52 同大学院修士課程了．同年日本電信電話公社（現 NTT）入社．量子光学の研究に従事．平 11 総研大に，平 16 阪大に移り，量子通信，量子論基礎の研究に従事．現在阪大・基礎工・教授．JST/CREST 量子情報，量子技術の研究代表者を歴任．工博．

北川（きたがわ）　勝浩（まさひろ）

昭 56 阪大・工・電子卒．昭 58 同大学院修士課程了．同年日本電信電話公社（現 NTT）入社．量子光学の研究に従事．平 5 阪大に移り，以来，量子情報，量子計算，磁気共鳴の研究に従事．現在，阪大・基礎工・教授．JST/CREST 電子光子，量子情報，量子技術の研究代表者を歴任．理博．