トレンド

最先端量子技術

Cutting-Edge Quantum Technologies

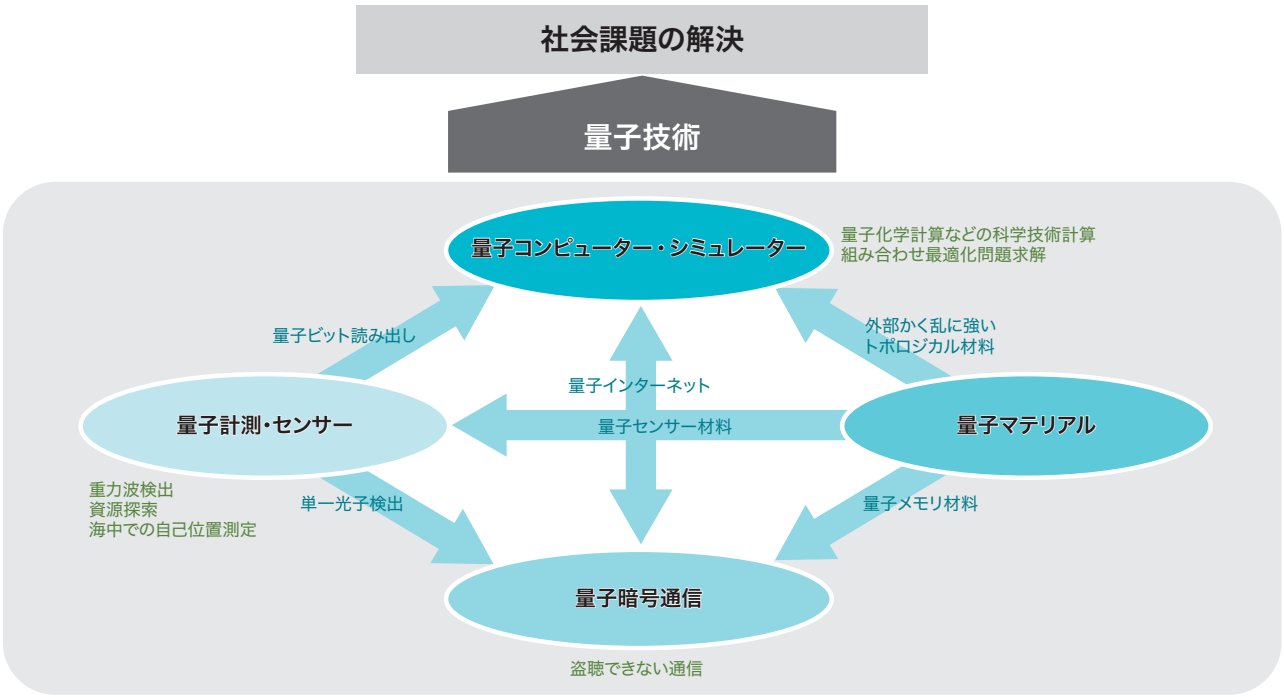
平岡　俊郎 HIRAOKA Toshiro　　市村　厚一 ICHIMURA Kouichi

量子技術は，将来にわたる様々な社会課題を解決できる技術として，その研究開発が世界中で活発化している。産業競争力の源泉としての期待が高まるとともに，安全保障上も重要視され，各国政府による研究開発投資も盛んである。

このような中で東芝グループは，単一光子源などの量子技術を起点として，量子鍵配送（QKD：Quantum Key Distribution）を事業化した。また，量子コンピューターの研究開発から派生した，組み合わせ最適化問題を解くことが可能なシミュレーテッド分岐マシン（Simulated Bifurcation Machine，SBMと略記）を開発し事業化した。基礎研究から社会実装まで多方面の取り組みにより，量子技術による高度に情報化された，豊かで安全な社会の実現に貢献できる。

The research and development of quantum technologies, which have the potential to solve various present and future social issues, has accelerated both in Japan and other countries. From the perspective of the foundations of industrial competitiveness as well as national security concerns, various national governments are promoting strategic investment in the research and development of such quantum technologies.

In this context, the Toshiba Group has developed and commercialized the following technologies: quantum key distribution based on various quantum technologies including single photon generation, and the Simulated Bifurcation Machine (SBM) capable of solving combinatorial optimization problems as an outcome of its efforts in the research and development of quantum computers. Our approaches to quantum technologies from the fundamental research stage through to social implementation are expected to contribute to the realization of a highly information-oriented, affluent, and safe society.



特集の概要図．様々な社会課題の解決が期待される量子技術

Quantum technologies expected to solve social issues in various areas

1. 高まる量子技術への期待

量子力学に特徴的かつ基本的な性質である重ね合わせの状態や，量子もつれ，量子干渉などを精密に制御する技術が，近年，急速に発展している。それに伴い，これらの性質を計測・センシング，暗号通信，情報処理，及び新規材料創出に巧みに活用する，量子計測や，量子センサー，量子暗号通信，量子コンピューター，量子シミュレーター，量子マテリアルなどの研究開発が世界中で盛んに行われている。

日常的な感覚や直感的理解とは相いれない量子力学に特徴的な性質の活用は，新しい動作原理に基づく常識を超えた機能・性能を持つデバイスや測定法を生む可能性がある。例えば，量子センサーの研究開発では，高精度で絶対重力が測れる原子干渉計型重力計の研究開発が進められ，重力波検出などの基礎研究への適用だけでなく，資源探査などでの実用化も期待されている。また，極めて高感度の原子干渉計型慣性センサーは，自己位置推定の高精度化によって，電波の届かない海中での非GPS（Global Positioning System）航行などへの応用が期待されている。量子暗号通信では，光子の重ね合わせ状態の利用と巧妙な古典情報のやり取りによって，第三者による暗号鍵の盗聴を検知可能とすることで，原理的安全性の下で暗号鍵を共有できる。情報を担う量子ビットとして重ね合わせ状態を利用する量子コンピューターでは，処理するデータサイズに対して必要なリソース（計算時間や装置の規模）が指数関数的に増大してしまう，いわゆる“計算量爆発”の回避や軽減が期待されている。量子マテリアルでは，外部環境からのかく乱に耐性を持つ，トポロジカル材料と呼ばれる物質を量子コンピューターに適用する研究開発が進められている。これらの量子技術は，ある技術がほかの技術の要素技術になるなどして，深く関係し合っている。**特集の概要図**に，量子技術での解決が期待される課題と，量子技術相互の関係を示した。

このように，新原理に基づく今までにない新機能や飛躍的な性能の向上で，様々な課題を解決する量子技術への期待が，近年，大いに高まっている。しかし一方で，課題も見え始めている。量子技術の研究開発の多くは，いまだ基礎研究の段階にある。また，量子技術の実用化には，量子物理の深い理解とともに高度かつ多種の量子関連技術や要素技術が必要となり，一企業，一研究機関だけでは困難なことも多い。更に今までにない新機能や高い性能の活用には，実社会における用途の具体化が重要となる。

こうした課題を克服しながら，東芝グループは，事業展開を進める量子暗号通信，及び，派生技術が早期の事業化に結び付いた量子コンピューターの研究開発に取り組んでいる。ここでは，これら最先端の量子技術について述べる。

2. 量子暗号通信への取り組み

現在，ネットワークの安全を支えている公開鍵暗号は，素因数分解問題や離散対数問題の計算困難性に立脚している。したがって，将来，量子コンピューターがそうした問題を効率的に解けるようになれば，解読可能になってしまうと予想されている。また，現在流通している通信データも，傍受したデータを，時間を掛けて，あるいは技術の進歩を待って解読する攻撃への対処が必要である。量子暗号通信は，このような危険にさらされる現在及び将来の通信データを，量子的性質により守る技術である。

2.1 量子鍵配送技術

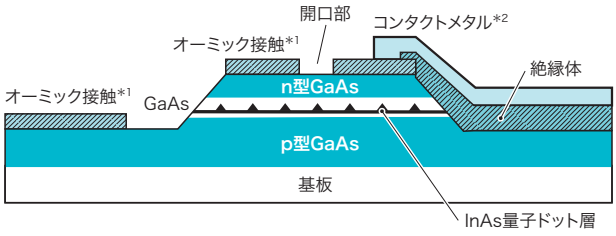
量子暗号通信は，QKDを利用して共有した暗号鍵を，送信者と受信者の共通鍵とする暗号通信である。QKDは，通信路を通る光子の量子状態（偏光や位相など）によって暗号鍵の情報を運ぶ。盗聴（観測）による光子の状態変化が原理的に制御不能であるという量子的性質と，光子による通信後に行う古典情報のやり取りにより，通信路での盗聴が検出できる。盗聴されていないことを確認しながら共有した暗号鍵によって，計算困難性に依存しない安全性が確保できる（この特集のp.13–15参照）。

2.1.1 光子制御技術

単一光子発生や，量子もつれ光子対発生，光子検出などの光子制御技術は，量子暗号通信や，その通信距離を伸長する量子中継，光を量子ビットとする量子コンピューター，量子コンピューターを量子通信でつなぐ量子インターネットなどの，様々な量子技術に対する重要な共通基盤である。

東芝欧州社のケンブリッジ研究所では，発光ダイオード構造の中の半導体量子ドットを利用した電気駆動の単一光子源を世界に先駆けて開発した（**図1**）[(1)]。更に電気駆動の量子もつれ光子対発生源の開発[(2)]や，三つ以上の光子での量子もつれを生成する光子源などの開発を行ってきた[(3)]。これらは単に共通基盤の技術的進展を示すだけでなく，量子技術の産業化において，微細加工や大量生産の点で成熟した半導体技術が適用できることを示唆している。これらの光子制御技術が，東芝グループにおける光を量子ビットとする情報処理や量子暗号通信の研究開発につながった。

量子暗号通信は今後，DX（デジタルトランスフォーメーション）からQX（クオンタムトランスフォーメーション）へと進化する社会の安全・安心な通信を支える技術として期待



GaAs：ガリウムヒ素　　InAs：インジウムヒ素

＊1：電流の向きや電圧の大きさによらず抵抗が一定で整流作用のない接合
＊2：半導体と配線をつなぐ金属

図1．東芝欧州社のケンブリッジ研究所で開発された電気駆動単一光子源の断面構造

単一の量子ドットが発する光子だけを，狭い開口部から取り出している。

Cross-sectional structure of single photon source developed by Cambridge Research Laboratory of Toshiba Research Europe Limited

される。その社会実装に向けて，東芝グループは鍵配送速度の高速化，及び鍵配送距離の増大に取り組んでいる。また，様々な利用形態でユーザーが簡単に使えるように，装置の小型化を推進している。

2.1.2　鍵配送速度の高速化

暗号鍵の配送には，鍵情報を担う微弱な光子の検出と検出後の暗号鍵生成のための信号処理が必要となる。光子検出の妨げとなるバックグラウンドノイズを除去する自己差分型回路技術[4]と信号処理アルゴリズムの開発[5]により，世界最高（注1）の鍵配送速度を実現した[6]（同p.9–12参照）。

2.1.3　鍵配送距離の増大

任意の距離の2点間で量子鍵配送を行うためには，物質の量子メモリーを使う量子中継や，多数の光子が量子もつれで結合したクラスター状態の光子団を使う全光量子中継の開発が望まれる。しかし，それらの実現には克服すべき技術的課題が多い。東芝グループは，物質の量子メモリーやクラスター状態を使わずに配送距離を2倍に伸ばすTwin Field QKDを考案し[7]，600 kmを超える配送距離を達成している[8]（同p.21–24参照）。

2.1.4　小型化

様々な利用場面での適用を狙い，QKDシステムの小型化が進められている。光集積回路化した“QKD送信チップ”，“QKD受信チップ”，“量子乱数生成チップ”をシステムとしてパッケージ化し，リアルタイムでのQKDの実証に成功している[9]（同p.16–20参照）。

2.2　事業化に向けた取り組み

事業化のための社会実装の実証実験や，システムの高速化，小型化などの研究開発を，国家プロジェクトへ参画して，他研究機関や医療，金融などの現場と共同で進めている。内閣府 SIP（戦略的イノベーション創造プログラム）の「光・量子を活用したSociety 5.0実現化技術」（管理法人：国立研究開発法人 量子科学技術研究開発機構）ではゲノム解析データ保管や株式取引への量子暗号通信の適用実証を，総務省「グローバル量子暗号通信網構築のための研究開発」プロジェクトでは高速化・長距離化・広域化に向けた技術開発を，総務省「グローバル量子暗号通信網構築のための衛星量子暗号技術の研究開発」プロジェクトでは人工衛星を利用した衛星量子暗号通信開発を，国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務「チップベース量子暗号通信の多重化に関する研究開発」においては光集積回路化したシステムとその多重化の技術開発を，それぞれ行っている。

海外でも，事業化に向けてプロジェクト参画を進めている（同p.25–28参照）。EU（欧州連合）のHorizon 2020プロジェクト「Open European Quantum Key Distribution Testbed」では，EU各国でのQKDネットワークの実装及び実証に取り組んでいる。また，英国UK Research and InnovationのプロジェクトNext Generation Satellite QKD」では，人工衛星によるQKDの研究開発を行っている。

3．量子コンピューターへの取り組み

量子技術の中でも最も社会的なインパクトが大きいと予想されるのが，量子コンピューターである。量子力学的重ね合わせ状態である量子ビットの利用により，因数分解などでは，従来技術に対して情報処理速度の指数関数的な加速が期待できる。

3.1　ゲート型とイジング型

量子コンピューターは，量子ビットの使い方によってゲート型とイジング型の2種類に分類される。ゲート型は，様々なアルゴリズムを実行できる汎用量子コンピューターとして期待されている。アニーリング型とも呼ばれるイジング型は，組み合わせ最適化問題の専用マシンである。

ゲート型は，量子ビットを初期化した後，順次個別に量子状態操作（量子ゲート操作）をして解の状態に導く。一方，イジング型は，最初に与えられた問題に対応した量子ビット間相互作用と外場（注2）を設定した上で，解の状態として取り得る全状態の重ね合わせを生成する強い外場を全量子ビットに印加する。次いで徐々に強い外場を除く量子ビットの一括操作で最適解の状態に導く。このような操作方法

（注1）　2022年8月現在，東芝グループ調べ。

（注2）　考えている粒子（ここでは量子ビット）に対して，粒子からの反作用を受けずに及ぼされる外部からの力や作用（磁場など）。

は断熱量子計算と呼ばれる。因数分解の指数関数的加速が示され，量子コンピューターの研究開発が活発化する契機となった1994年に発表のショアのアルゴリズムは，ゲート型を対象としている。一方，まだ量子コンピューターの実用化は遠いと思われていた2011年に，商用量子コンピューターとしてD-Wave Systems社から発売されて世界に衝撃を与えたD-Wave Oneはイジング型である。

3.2　量子分岐マシン

東芝グループは，Kerrパラメトリック発振器（KPO）の二つの発振状態の重ね合わせを量子ビットとする，イジング型の量子コンピューターである量子分岐マシンを提案した[10]。D-Wave Systems社で採用されている磁束量子ビットとは異なり，設計・制御の自由度が大きい回路量子電気力学に基づく新規な超伝導量子ビットを用いることで，高性能化が期待できる。

3.3　量子分岐マシンのシミュレーテッド分岐マシンへの展開（古典マシンへの展開）

量子分岐マシンの動作を表す量子力学を古典力学の運動方程式に変換した仮想的マシンの動作が，通常の古典情報処理装置の並列実行で高速にシミュレーションできることが見いだされた。その後，方程式の改変で更に高速のシミュレーションが可能になった際に導き出されたのが，シミュレーテッド分岐（SB）アルゴリズムである。このような，量子原理若しくは量子計算に着想を得た原理に基づく技術は“量子インスパイアード技術”と呼ばれており，その一つであるSBアルゴリズムは，“量子インスパイアードアルゴリズム”と呼ばれている。このアルゴリズムを商用のFPGA（Field-Programmable Gate Array）やGPU（Graphics Processing Unit）上で実行することで，高速で大規模な組み合わせ最適化マシンであるSBMが生まれた[11]（この特集のp.29–32，及びp.35–36参照）。

2019年には金融取引マシンのコンセプト実証機を開発し，SBMによる金融領域への展開が進められている（同p.37–40参照）。またアルゴリズムの改良が進み[12]，2019年にはAWS Marketplaceを利用したGPU版SBMのクラウドサービスが，2020年にはGPU版SBMのパートナー企業への有償提供が始まった。そして2022年には，計算創薬への適用性が確認され（同p.33–34参照），また，仮想発電所の制御への有効性が確認された（同p.41–42参照）。

3.4　量子分岐マシンのゲート型への展開

量子分岐マシンで提案されたKPOによる量子ビットはゲート型にも利用可能である[13]。その研究開発を加速するため，東芝グループは，NEDOが推進する国家プロジェクト「高効率・高速処理を可能とするAIチップ・次世代コンピューティングの技術開発」の「量子計算及びイジング計算システムの統合型研究開発」に参画している。**図2**にイジング型とゲート型の量子分岐マシン及びSBMの関係を示す。

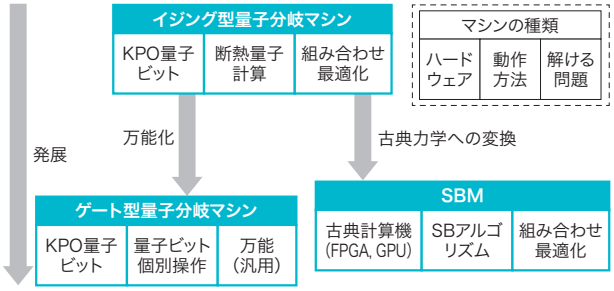


図2．量子分岐マシンの発展
ハードウェアや動作方法を変化させ，発展を続けている。
Evolution of quantum bifurcation machines

4.　今後の展望

量子技術の実用化には，最先端の量子力学に基づく技術の高度化とともに，社会課題の解決に向け，量子技術以外の周辺技術との融合や実証試験など，社会実装への取り組みが求められる。また，ゲート型量子コンピューターのように，実用化には今一段の性能向上が求められる技術については，中長期的な視点から，技術の進展に合わせた，使いこなしに関する知見の蓄積とその体系化も非常に重要となる。

一たび社会実装が始まれば，更なる投資の加速に加えて，応用現場から得られる知見のフィードバックによって，量子技術とその応用展開は加速度的に発展していくと予想される。また，発展する新技術分野の魅力は多くの優れた人材を引き付け，量子技術の発展の更なる加速につながるに違いない。

東芝グループは，QKDやSBMの社会実装を急ぐとともに，ゲート型量子コンピューターなど，その先の量子技術の実現と応用展開にも貢献していく。

文　献

(1) Yuan, Z. et al. Electrically Driven Single-Photon Source. Science. 2002, **295**, 5552, p.102–105.
(2) Salter, C. L. et al. An entangled-light-emitting diode. Nature. 2010, **465**, p.594–597.
(3) Lee, J. P. et al. A quantum dot as a source of time-bin entangled multi-photon states. Quantum Sci. Technol. 2019, **4**, 2, 025011.
(4) Comandar, L. C. et al. Gigahertz-gated InGaAs/InP single-photon detector with detection efficiency exceeding 55% at 1550 nm. J. Appl. Phys. 2015, **117**, 8, 083109.
(5) Takahashi, R. et al. “Practical Implementation of Privacy Amplification in Quantum Key Distribution”. 9th International Conference on Quantum Cryptography. Montreal, Canada, 2019-08, QCrypt. 2019, Poster 77.

⑹ 東芝.“量子暗号通信で世界初の10Mbpsを超える鍵配信速度を達成”. ニュースリリース. <https://www.global.toshiba/jp/news/corporate/2017/09/pr1501.html>, (参照 2022-07-28).
⑺ Lucamarini, M. et al. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature. 2018, **557**, 7705, p.400–403.
⑻ Pittaluga, M. et al. 600-km repeater-like Quantum communications with dual-band stabilization. Nature Photonics. 2021, **15**, 7, p.530–535.
⑼ Paraïso, T. K. et al. A photonic integrated quantum secure communication system. Nature Photonics. 2021, **15**, 11, p.850–856.
⑽ Goto, H. Bifurcation-based adiabatic quantum computation with a nonlinear oscillator network. Scientific Reports. 2016, **6**, 21686.
⑾ Goto, H. et al. Combinatorial optimization by simulating adiabatic bifurcations in nonlinear Hamiltonian systems. Science Advances. 2019, **5**, 4, eaav2372.
⑿ Goto, H. et al. High-performance combinatorial optimization based on classical mechanics. Science Advances. 2021, **7**, 6, eabe7953.
⒀ Goto, H. Universal quantum computation with a nonlinear oscillator network. Phys. Rev. A. 2016, **93**, 5, 050301(R).

平岡　俊郎　HIRAOKA Toshiro
研究開発センター ナノ材料・フロンティア研究所
Nano Materials and Frontier Research Labs.

市村　厚一　ICHIMURA Kouichi, D. Sc.
研究開発センター ナノ材料・フロンティア研究所
フロンティアリサーチラボラトリー
博士（理学）　日本物理学会・応用物理学会・日本光学会会員
Frontier Research Lab.