量子情報処理によるセキュリティと量子情報のデータ保護

量子情報処理を用いると高速計算以外にもセキュリティに対して原理的な安全性，コピー防止など独特の応用が期待されています．その実用に向けてはノイズに弱い量子情報を保護する誤り耐性処理が必須となり，ネットワーク化のためには量子中継をベースとした量子通信の誤り耐性処理が鍵となります．これらに対するNTTセキュアプラットフォーム研究所の取り組みを紹介します．

徳永 裕己（とくなが ゆうき）
鈴木 泰成（すずき やすなり）
遠藤 傑（えんどう すぐる）
西巻 陵（にしまき りょう）
北川 冬航（きたがわ ふゆき）
為近 彩智（ためちか さち）

NTTセキュアプラットフォーム研究所

はじめに

近年，量子情報処理による新たな高速計算の可能性が注目されていますが，量子情報処理を用いた新たなセキュリティおよび量子情報のデータ保護も重要な研究テーマです．まず，量子情報は非常にノイズに弱いことが知られていて，正しく情報処理を行うためには，量子情報をノイズやエラーから守ってあげる必要があります．このような情報処理の「可用性」を守ることも，セキュリティの3要素*の1つであり，セキュリティの重要な役割の1つとなっています．これができない限り，いくら計算が速くても，新たなセキュリティ応用があったとしても，正しく情報処理がこなせないことになります．この量子データをノイズから保護する機能は量子情報処理の最重要課題であり，量子情報処理の屋台骨を支える量子情報処理自体のセキュリティであるといえます．また量子情報処理を用いた新たなセキュリティの可能性としては，ある意味このノイズに対する弱さを逆手にとったものともいえますが，盗聴や偽造を行おうとして量子状態に触れるとどうしてもノイズとしての痕跡が残ってしまうという量子状態の性質があります．これを大いに活かして，盗聴者の検出を行い原理的な安全性を保てるのが量子暗号の仕組みです（量子暗号は通常，秘密鍵の配送に用いるため量子鍵配送とも呼ばれます）．さらにそれを偽造防止という方向に用いることも可能であり，コピーによる偽造は原理的に不可能となる量子マネーや量子著作権保護といった応用の可能性があります．またこのような機能は量子的なネットワークが充実してきてより利用価値が高まるものであり，そのためには量子中継を実現して規模の大きな量子ネットワークの構築をめざす必要があります．量子通信も損失やノイズに弱いため，量子通信のデータをノイズから保護する機能は，量子通信を保護する量子通信自体のセキュリティともいえます．

本稿では，まず量子情報のデータを保護するための2種類の重要な技術である量子誤り訂正と量子誤り抑制の紹介をし，次に新たな応用の可能性としての偽造防止について，そして量子ネットワークをめざすための基盤技術となる量子中継の研究を紹介し，最後に展望を述べます．

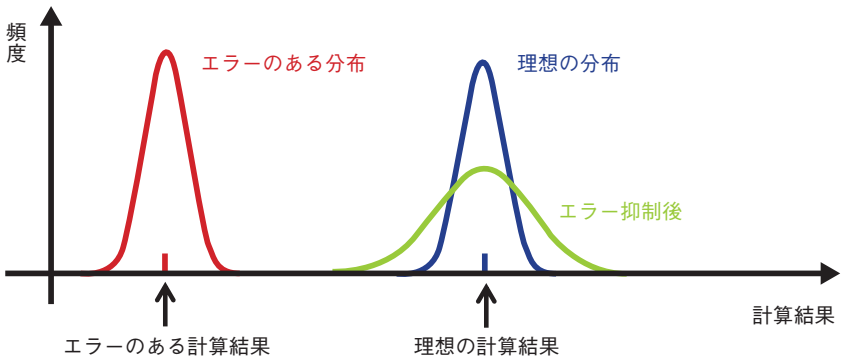
量子情報のデータを守る誤り耐性技術

量子情報処理の多くの応用において，計算中に誤りが生じる確率は十分小さい必要があります．量子誤り訂正は，複数の量子ビットを用いて量子ビットの情報を符号化し，これを逐次的に誤りを検出，訂正することで，実効的な誤り率を大幅に低減することができる技術です．量子誤り訂正を用いながら量子計算を行う誤り耐性量子計算[(1)]は，スケーラブルに誤り率を低減できる手法であり，将来，規模の大きな量子情報処理の実現するうえで必須になると予想されます．しかし一方

＊情報セキュリティの3要素：「機密性（Confidentiality）」「完全性（Integrity）」「可用性（Availability）」．

で，量子誤り訂正は多くの量子ビットやフィードバックなどの複雑な処理を必要とするため，実用的な性能の誤り耐性量子計算機を構築することは容易なことではありません．したがって，実用的な誤り耐性量子計算機を構築するには，多くのトレードオフやボトルネックの問題に立ち向かうことで，ソフトウェアからハードウェアまで一貫して効率的なアーキテクチャを研究開発することが求められます．私たちのグループは，実用的な誤り耐性量子計算機の実現をめざして，特にソフトウェア基盤の研究開発に取り組んでいます．具体的には，分散型処理を意識した誤り耐性量子計算手法[2]，小規模な符号の復号回路を機械学習で最適化する手法[3]，復号アルゴリズムを中心とした低レイテンシな制御を行う周辺装置の設計[4]，集積化された量子ビットを精度良く制御するための校正手法[5]，高速に実験を実施するフレームワークの構築，そしてこれらを包括的に評価し精度を高めるための一連の基盤ソフトウェアの開発を行っています．

また，近年near-term量子計算という研究が非常に注目を集めています．なぜなら，2019年10月に，非常に特定の，実用的ではない問題ですが，既存のコンピュータでは解くのに非常に長時間かかるといわれた問題を53量子ビットの小規模な実際に作製された量子コンピュータを用いて高速に解くことができたとGoogleが発表し，脚光を浴びたからです．現在，このような量子デバイスをどのように実用上役立てれば良いかと世界中の研究者が検討しており，例えば機械学習や化学計算などへの応用が注目を集めています．ただし，このような小規模な量子コンピュータの計算能力を引き出すには計算エラーを抑える必要があります．計算エラーを取り除くために長年研究されてきた分野として量子誤り訂正がありますが，この手法は量子ビットをエラー抑制のためのリソースとして用いるため，量子ビット数が限られる現在，および近い将来に実現し得る規模の小さな量子デバイスとは相性が良くありません．そこでその代わりに，量子誤り抑制（または量子ノイズ補償）という量子ビット数を（大幅に）増やさずにエラーを抑制する手法が提案され，最近多くの論文が発表されています．量子誤り抑制は量子アルゴリズムにエラーを抑えるための操作を加え，さらに読み出される測定結果に対して既存の古典情報処理をすることによって計算エラーを実効的に抑制する手法です（**図1**）．その際，量子誤り抑制に必要なリソースはより多くの測定回数（計算回数）です．多くの測定から得られる情報を基にエラーを抑えるので，オーバーヘッドがかかり，この手法はスケーラブルな手法ではないですが，計算エラーの頻度が量子アルゴリズム中で少数回であれば，効果的にエラーを抑えることができると示されています[6]．また最近，私たちのグループは誤り耐性量子計算に対しても量子誤り抑制手法を組み合わせて用いることで，実行的に誤り耐性量子計算に必



near-term の量子アルゴリズムでは測定結果の平均値を計算結果として得る．量子誤り抑制をしたあとは，確率分布は正しい平均値（計算結果）のまわりに分布するが分散が増加するため，より多くの測定回数が必要となる．

図1　量子誤り抑制の機能についての概念図

要な量子ビット数の削減が可能であることを示し，量子誤り抑制が広い用途を持つ技術であることを示しました[7]．

暗号と量子情報技術の融合による安全なコピー防止技術

一口に量子情報処理と暗号といってもその内容は一意に定まりません．この2つが関連する技術は大きく分けて①量子コンピュータに対しても安全な暗号技術（耐量子暗号技術），②暗号通信を行うために量子情報処理を利用する量子暗号，③量子情報処理を使って初めて実現される新しい暗号技術，の3つに分類できます．本稿では③が主題ですが，まず①と②について簡単に説明します．①は暗号技術そのものには量子情報処理や量子コンピュータの力は必要ありませんが，攻撃者は量子コンピュータを使用して攻撃するという前提で安全性が考えられた暗号のことです．②は暗号技術にも量子情報処理あるいは量子コンピュータが用いられますが，達成される暗号機能そのものは基本的に既存の技術と変わらない暗号のことです．例えば秘匿通信自体は量子の力がなくとも実現できますが，量子の力を使うことでより安全性を高めることができます．それに対して主題の③は量子の力なくしては絶対に達成できない機能を持つ暗号技術です．具体的な例がデータあるいはソフトウェアのコピー防止です．

デジタルデータはいくらでも複製可能であるので，データやソフトウェアのコピーを防ぐことは原理的に不可能です．しかしそれは量子情報技術を考慮しない場合の話です．量子情報理論には「未知の量子状態はコピーできない」という複製不可能定理[8],[9]が存在するので，これを暗号技術に応用することでコピー不可能なデータやソフトウェアを実現できる可能性があります．特にコピーを防止したいデータとして通貨が考えられ，絶対にコピー不可能な量子マネーが提案されています[10]（**図2**）．

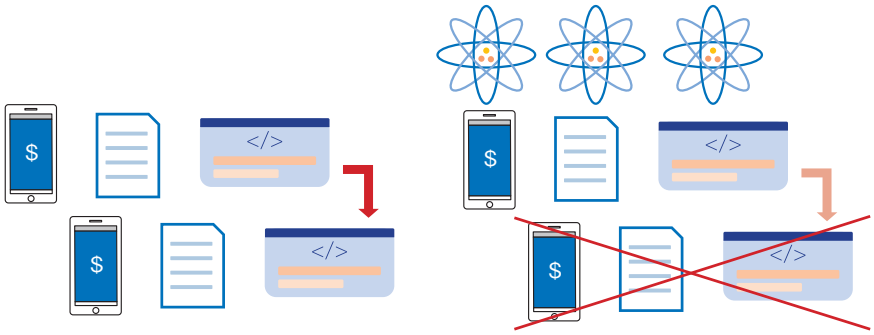


図2　量子技術によるコピー不可能性のイメージ図

現在のソフトウェアはデジタルデータであるため海賊版の作成を防ぐことが原理的に難しく，安全性を保証できるコピー防止策はこれまで存在しませんでした．安全性が証明可能なソフトウェアコピー防止は暗号と量子技術を用いてソフトウェアのコピー作成を完全に不可能にする技術です．当グループではこの実現を目標の1つとしています．コピー防止技術は量子マネー，ソフトウェアコピー防止以外にも応用が多く，例えばクラウドに預けていた（暗号化）データを手元に戻したときにクラウドにはコピーが残らないようにすることが可能であり，忘れられる権利（General Data Protection Regulation 第17条）の実現につながります．またソフトウェアを期間限定で貸し出し，返却後の使用を完璧に防ぐといったことが可能となります[11]．当グループでは以上のような量子情報の力を利用して初めて達成可能な新しい暗号技術を実現するために研究開発を行っています[12]．

量子ネットワークに向けた量子中継技術

現在のコンピュータを用いた計算や通信の技術はすべて古典物理のルールに基づいたものであり，古典物理が許す範囲の計算や通信しか行うことができません．これはセキュリティについても同様です．現在は古典物理が許す

限られた範囲のセキュリティしか提供することができませんが，量子力学を用いることで私たちが提供するセキュリティの可能性を広げることができます．例えば共通鍵配送において盗聴者の検知が可能になり[13]，秘密計算においては1台のサーバで情報理論的に安全かつ簡潔なプロトコルが行えるようになります[14]．

このような量子力学の効果を出すための通信としてのリソースはエンタングルメント（量子もつれ）と呼ばれる量子力学特有の相関であることが分かっています．量子力学に基づいたセキュリティのアプリケーションを地球規模で利用可能にするためには，量子力学特有の相関であるエンタングルメントを作成し，そのエンタングルメントを長距離かつ複数個所に共有できる量子ネットワークを構築する必要があります（**図3**）．

エンタングルメントを長距離間で共有したい場合，量子状態はコピーできないという性質から単純な増幅ができないため，従来の通信で用いている中継手法を使うことはできません．損失によりエンタングルメントの片側を直接伝送できる確率は指数関数的に小さくなるため，何らかの方法での中継が必要となります．ここでは要点だけを以下にかいつまんで述べます．まず損失が多大にならない程度の距離に中継器を置くことで直接伝送の距離を短くし損失を減らします．しかし，ある程度の損失やエラーは避けられないので，中継地点ごとに冗長に複数の通信を重ねて行い，それらに対して量子誤り訂正に相当する処理を行うことで損失やエラーを抑えた伝送を可能にします．これはエンタングルメント通信の誤り耐性処理といえ，複数の不完全なエンタングルメントから完全に近いエンタングルメントを取り出す作業となるので，エンタングルメント蒸留（純粋化）とも呼ばれています．

私たちのグループでは超低損失ナノ光ファイバ共振器[15]を用いた量子中継器の構築をめざしています．超低損失ナノ光ファイバ共振器とは超低損失テーパーファイバと超低損失ファイバブラッググレーティングの2つの要素を組み合わせたものです．これを量子メモリ部分に用いることで以下のように性能を上げる手法を検討しています．通常のファイバより格段に細いテーパーファイバ近傍に量子メモリとなる原子を捕獲することで，テーパーファイバを通る光子と原子の作用を可能にします．このように中継の系全体をファイバ内にすることで，従来いったん光子を自由空間に出して原子と作用していた損失の多い過程をなくし，光損失を減らすことが可能となります．また，ファイバブラッググレーティングによる共振器構造を用いて量子メモリから放射される光がファイバに結合する確率を上げることができます．これらは結果として量子メモリへの書

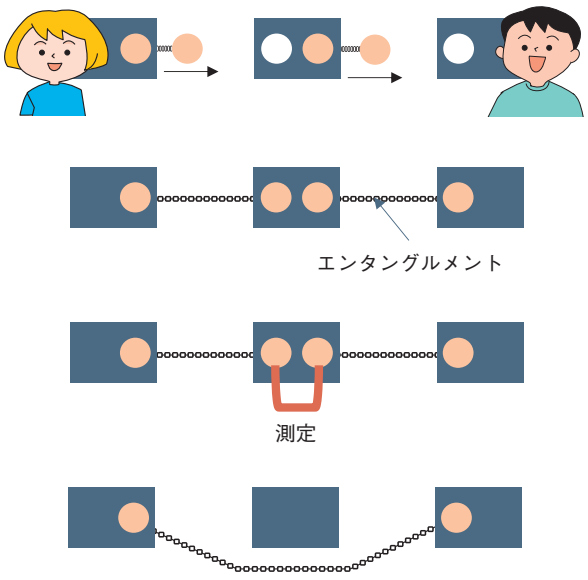


図3　量子中継器を用いたエンタングルメントの共有方法の概略図

き込みや読み出しの操作の成功率を上げることにつながり，全体の中継器としての性能を上げることができます(16)．

また，高性能な量子中継器を用いた量子ネットワークの実現により，さまざまなセキュリティのアプリケーションを提供することができるようになります．特に想定されるターゲットとしては外交や防衛といった安全保障分野や遺伝子情報を扱う医療分野，また金融機関などが挙げられます．

おわりに

量子情報や量子通信自体のデータ保護となる誤り耐性技術，量子中継技術は量子情報処理を正しく安全に実行するために欠かせない重要課題であることを最後にもう一度強調しておきます(17)．量子情報処理の誤り耐性処理のための優れたアーキテクチャは未開拓な部分が多く，今後の研究によるブレークスルーが期待されます．また量子情報処理のセキュリティ応用としては，原理的に安全な秘匿通信やコピー防止以外にも，量子秘密計算や量子を活用した通信計算量の削減など新たなものが期待されます．まだ規模のそれほど大きくないnear-term量子セキュリティというものも今後に期待される研究テーマです．

■参考文献

(1) A. G. Fowler and C. Gidney：“Low overhead quantum computation using lattice surgery,” arXiv:1808.06709 , 2018.
(2) K. Fujii and Y. Tokunaga: “Fault-Tolerant Topological One-Way Quantum Computation with Probabilistic Two-Qubit Gates,” Phys. Rev. Lett., Vol. 105, No. 25, 250503, 2010.
(3) A. Davaasuren, Y. Suzuki, K. Fujii, and M. Koashi: “General framework for constructing fast and near-optimal machine-learning-based decoder of the topological stabilizer codes,” Phys. Rev. Research, Vol. 2, No. 3, 033399, 2020.
(4) Y. Ueno, M. Tanaka, Y. Suzuki, Y. Tabuchi, and M. Kondo: “Quantum Error Correction with a Superconducting Decoder,” QCCC 2020, Dec. 2020.
(5) K. Heya, Y. Suzuki, Y. Nakamura, and K. Fujii: “Variational Quantum Gate Optimization,” arXiv:1810.12745, 2018.
(6) S. Endo, S. C. Benjamin, and Y. Li：“Practical Quantum Error Mitigation for Near-Future Applications,” Phys. Rev. X, Vol. 8, No. 3, 031027, 2018.
(7) Y. Suzuki, S. Endo, K. Fujii, and Y. Tokunaga: “Quantum error mitigation for fault-tolerant quantum computing,” arXiv preprint arXiv:2010.03887, 2020.
(8) W. Wootters and W. Zurek：“A single quantum cannot be cloned,” Nature, Vol. 299, pp. 802-803, 1982.
(9) D. Dieks：“Communication by EPR devices,” Phys. Lett. A, Vol. 92, No. 6, pp. 271-272, 1982.
(10) S. Wiesner：“Conjugate Coding,” SIGACT News, Vol. 15, No. 1, pp. 78-88, 1983.
(11) P. Ananth and R.L. La Placa：“Secure software leasing,” CoRR, abs/2005.05289, 2020.
(12) F. Kitagawa, R. Nishimaki, and T. Yamakawa：“Secure software leasing from standard assumptions,” CoRR, abs/2010.11186, 2020.
(13) https://www.ntt.co.jp/journal/0608/files/jn200608049.pdf.
(14) T. Morimae：“Measurement-only verifiable blind quantum computing with quantum input verification,” Phys. Rev. A, Vol. 94, 042301, Oct. 2016.
(15) S. Ruddell, K. E. Webb, M. Takahata, S. Kato, and T. Aoki：“Ultra-low-loss nanofiber Fabry–Perot cavities optimized for cavity quantum electrodynamics,” Opt. Lett., Vol. 45, No. 17, pp. 4875-4878, 2020.
(16) 為近・鈴木・徳永・青木：“ナノファイバー共振器QED系を用いた量子中継の検討,” 日本物理学会第76回年次大会，2021.
(17) https://journal.ntt.co.jp/wp-content/uploads/2021/03/JN202103043.pdf

（上段左から）徳永　裕己/ 鈴木　泰成/ 遠藤　傑
（下段左から）西巻　陵/ 北川　冬航/ 為近　彩智

量子情報処理をセキュリティに応用するまでにはまだ時間はかかりますが，実りの多い将来が待っていると期待しています．量子情報を守る誤り耐性処理，量子ネットワークに向けた量子中継などの必須の技術を着実に進歩させ，新たな応用を生み出していきます．

◆問い合わせ先
NTTセキュアプラットフォーム研究所
企画担当
E-mail　scpflab＠hco.ntt.co.jp