PRESS RELEASE（2026/01/07）

コピーできない量子情報を“暗号化して複製”：量子技術の根本的制約を矛盾なく乗り越える新手法

～量子複製禁止定理と矛盾しない“暗号化クローン”生成プロトコルの開発に成功～

ポイント

① 量子情報は複製できないため、安全なバックアップや冗長化が困難だった。
② 本研究では、量子状態の“暗号化クローン”を複数生成し、量子的な鍵を用いて任意に選んだいずれか一つのクローンを復号できるプロトコルを構築した。
③ 量子情報の安全な多重保存を可能にし、量子クラウドストレージなどへの応用が期待される。

概要

量子情報は、古典情報とは異なり完全には複製できないという「量子複製禁止定理（※1)」に従います。この制約のため、量子データを安全にバックアップしたり、多重に保存して耐故障性を確保したりすることが困難であり、量子通信・量子計算・量子クラウド技術の発展における大きな障壁の一つとなっていました。その一方で、この制約と矛盾せずに量子情報を複数の複製として冗長化する方法はこれまで知られておらず、その解明が強く求められていました。

本研究では、量子複製禁止定理と整合したまま量子情報の“暗号化クローン”を複数生成し、これらのクローンのうちの任意に選んだ一つから元の情報を復元できる新しいプロトコルを構築しました。特に、通常は“ノイズ”となりうる量子的ゆらぎを意図的に導入し、それと量子的に結びついた補助系を「鍵」として復元に利用する構造により、複製禁止定理に反さずに冗長化を実現した点に特徴があります。

九州大学大学院システム情報科学研究院の山口幸司特任助教は、University of Waterloo の Achim Kempf 教授と共同で、複数のベル対（※2）を用いた新しいプロトコルにより、量子情報の「暗号化された複製」を任意数作成できること、さらに補助量子系を用いてそのうちの任意の一つを完全に復号できることを理論的に示しました。

本成果は、量子情報を安全に多重化して保存するための新しい基盤を与えるものであり、量子クラウドストレージや量子ネットワークの耐故障性向上などへの応用が期待されます。また、将来的には量子データの分散管理や安全な量子クラウド技術の開発など、多様な量子情報インフラへの展開が見込まれます。

本研究成果はアメリカの雑誌「Physical Review Letters」に 2026 年 1 月 6 日（火）付で掲載されました。さらに、本論文は同誌の“PRL Editors' Suggestion”に選出されました。Editors' Suggestion は、PRL 掲載論文のうち約 6 本に 1 本のみが選ばれる特別な称号で、編集部が特に重要かつ興味深いと評価した論文に与えられます。

研究者からひとこと：

科学技術では、ノイズは普通“邪魔者”として扱われます。しかし今回の研究では、そのノイズをあえて加えることで、情報を外から見えなくする暗号化を実現し、複製禁止定理に抵触しない“暗号化クローン”を作ることができました。さらに、そのノイズと量子的につながった「鍵」を使うことで、必要なときに元の量子情報を完全に取り出すことができます。コントロール可能な形でノイズを使うことで“邪魔者”を味方に付けるという、少し意外な発想から生まれた成果だと思っています。

（山口幸司）

【研究の背景と経緯】

量子コンピュータや量子通信などの量子技術では、「量子情報」と呼ばれる種類の情報を扱います。量子情報は古典的な情報とは異なる特有の性質を示しますが、とりわけ興味深いのは、情報をそのままコピーできないという「量子複製禁止定理」に従う点です。この制約のため、量子データを安全にバックアップしたり、多重に保存して耐故障性を確保したりすることが難しく、量子通信・量子計算・量子クラウド技術の発展における大きな障壁の一つとなっていました。したがって、この制約と矛盾しない形で量子情報を安全かつ冗長に管理する方法を確立することは、将来の量子インフラの実現に向けた重要な課題でした。

【研究の内容と成果】

本研究では、量子複製禁止定理に抵触することなく、未知の量子状態の情報を“暗号化された複製（暗号化クローン）”として複数生成する新しいプロトコルを構築しました。

このプロトコルでは、ベル対によって生じる強く結びついた量子的なゆらぎを、情報の暗号化とその復号化に利用する点が重要な役割を果たします。具体的には、複数のベル対を準備し、その片側だけをすべて集めた量子系がもつ量子的なゆらぎ（ノイズ）を複製したい量子情報と組み合わせて処理することで、その量子情報の複数のクローンを“外からは何も読み取れない完全な暗号化状態（単独では最大混合状態）”として生成することができます。

さらに、ベル対のもう一方の側にあたる量子系全体が保持する量子的なゆらぎを「鍵」として利用することで、生成された暗号化クローンのうち任意に選んだ一つを復号し、もとの量子情報を完全に復元することができます。重要なのは、この復号操作において「鍵」が消費されるため、復号できるクローンは常に一つに限定され、量子複製禁止定理との整合性が厳密に保たれている点です。

本成果は、九州大学大学院システム情報科学研究院の山口幸司特任助教と University of Waterloo の Achim Kempf 教授の共同研究により得られたものであり、量子情報の暗号化と冗長化を両立させる新しい手法を明らかにするものです。

【今後の展開】

今回の成果は、量子情報を安全に多重化して保存するための新しい基盤技術となるものであり、量子クラウドストレージや量子ネットワークの耐故障性向上への応用が期待されます。たとえば、量子データの“暗号化クローン”を複数の量子クラウドに分散して保管し、利用者側が鍵となる量子系を保持することで、「どこか一つのクラウドから暗号化クローンを取り出せれば、元の量子情報を復元できる」という、安全かつ冗長な量子データ管理が可能になります。

また、「本来は邪魔であるはずのノイズを、制御可能な形であえて加えて利用する」という今回の発想は、将来的に量子セキュリティ、量子センシング、量子レーダーといった分野における新しい方式の開発にもつながる可能性があります。量子情報のコピー禁止という根本的な制約と整合しつつ、その制約を“うまく利用する”ことで、量子情報インフラを柔軟かつ有効に設計するための、今後の理論的・実験的な展開が期待されます。

【用語解説】

(※1) 量子複製禁止定理（no-cloning theorem）

量子情報（未知の量子状態）を完全に複製する操作は、量子力学の基本原理（とくにユニタリ性）と矛盾するため不可能であることを示す定理。この性質は、量子暗号の安全性の基盤となる一方で、量子通信や量子計算の設計における重要な制約にもなっている。

（※2）ベル対（Bell pair）
量子情報の最小単位である「量子ビット」が二つ組になり、最大限にエンタングルした（量子的に強く結びついた）状態のことをいう。このとき、それぞれの量子ビットは単独で見ると強い量子的なゆらぎをもつが、二つの量子ビットのゆらぎは互いに強く相関している。

【謝辞】
本研究は JSPS 海外特別研究員制度、JSPS 科研費 （JP24KJ0085）の助成を受けたものです。

【論文情報】
掲載誌：Physical Review Letters
タイトル：Encrypted Qubits can be Cloned
著者名：Koji Yamaguchi and Achim Kempf
D O I ：10.1103/y4y1-1ll6

【お問合せ先】
＜研究に関すること＞
九州大学　大学院システム情報科学研究院　特任助教　山口幸司（ヤマグチコウジ）
TEL：092-802-3637
Mail：yamaguchi.koji.848@m.kyushu-u.ac.jp

＜報道に関すること＞
九州大学　広報課
TEL：092-802-2130　FAX：092-802-2139
Mail：koho@jimu.kyushu-u.ac.jp