新量子認証プロトコルの開発と量子通信の安全性と効率に関する基礎研究
(061402010)

New quantum authentication protocol and security and efficiency of quantum communication

研究代表者
小澤 正直　名古屋大学大学院情報科学研究科
Masanao Ozawa
Graduate School of Information Science, Nagoya University

研究分担者
堀田 昌寛† 林 正人††
Masahiro Hotta† Masahito Hayashi††
†東北大学大学院理学研究科 ††東北大学大学院情報科学研究科
†Graduate School of Science, Tohoku University
††Graduate School of Information Science, Tohoku University

研究期間 平成 18 年度～平成 20 年度

概要
本研究開発は、個人情報保管の安全性を高める新しい原理に基づく量子認証プロトコルの開発を目的とし、また、そのために必要となる量子通信の安全性と効率に関する新たな一般理論を展開することを目的とする。現在、クレジット暗証番号などの個人情報漏洩による様々な犯罪が大きな社会問題となっている。この根本原因は古典情報に基づいた認証システムの脆弱性にある。本研究開発では、物理学の根本原理に基いてその安全性が保証される、量子情報に基づく認証システムを開発する。また、新しい不確定性原理に基づいて、広範な量子通信に対して成立する安全性と効率に関する一般的関係を明らかにする。

Abstract
The purpose of the present project is twofold. One is to develop a new quantum authentication protocol, and the other is to make a fundamental study of security and efficiency of general quantum communication channels. A recent surge in crimes involving skimming and leakage of passwords in smart cards reveals the fragility of conventional authentication methods using classical information. Here, we develop an authentication method using only quantum information and show its security. For a basis of this research, we also show a general security bound for general quantum communication channels based on the recently developed universal uncertainty principle.

１．まえがき
本研究グループでは、これまで主に量子測定理論の基礎研究およびその量子情報理論への応用に関する研究を推進してきた。本研究開発では、その蓄積に立脚して、安全性や実現性の議論が乏しい認証問題に着目し、新しい原理に基づく量子認証プロトコルの開発を行うことを目的とし、また、本研究グループで近年、研究が進められた不確定性原理の新しい定式化に基づいて、広範なプロトコルに応用可能な量子通信の安全性に関する新しい一般理論を確立することを目的とする。

近年、クレジットカード暗証番号の認証プロトコルの脆弱性が社会問題になっている。暗証番号が盗まれ、銀行預金が不正にひきおろされるケースが後を絶たない。その対策である暗証番号の暗号化には、将来的に不安があり、新しい原理に基づく認証方式が求められている。インターネットで実用化されている公開鍵暗号は、公開鍵と秘密鍵の間に生まれる計算量ギャップをその安全性の根拠にしているが、1994 年に Shor によって発見された量子アルゴリズムにより、この計算量ギャップが将来は崩壊する可能性がある。

この問題の根本的解決として BB84 などの量子鍵配送プロトコルの研究が欧米諸国や我が国で活発に進められている。このプロトコルでは、正規な通信者は盗聴検知が可能であり、理論的に無条件安全な鍵配送が可能であると期待されている。しかし、そのためには、高価な単一光子検出器等の装置が必要とされ、精度の限界から鍵配送の通信レートが大きく制約されている。量子鍵配送プロトコルを利用して無条件安全な暗号通信を実現するには、ワンタイム・パッドと呼ばれる配送された鍵を使い捨てにする古典秘密鍵通信方式が不可欠であり、暗号通信の通信レートは、鍵配送の通信レートに押さえられてしまう。従って、量子鍵配送プロトコルのような、高度の安全性を実現できるが、そのためには高速化が困難かつ高価であるシステムが、ギガビット級のインターネットによる実際の需要を満たすかは将来的に不透明である。

以上のように、量子鍵配送プロトコルの万能性には疑問があり、将来的には、それぞれの用途に特化した量子暗号プロトコルの研究開発を行う必要があると考えられる。本研究開発では、コピーが可能な古典情報にもとづいた認証システムの原理的脆弱性に着目し、照合に古典情報を必要としない新しい原理に基づく量子認証プロトコルの開発を目的とし、また、従来の量子鍵配送に特化した安全性証明を超えて、広範なプロトコルに応用可能な量子通信の安全性に関する新しい一般理論を確立することを目的とする。

２．研究内容及び成果
２．1．不確定性原理に基づく量子通信の安全性
量子暗号プロトコルは、盗聴者の測定行為が暗号通信路の状態を不可避に乱すという不確定性原理から安全性が

保証されると考えられてきた。しかし、不確定性原理の従来の定量的定式化では、所与の状態における物理量の揺らぎの相反関係が明らかにされただけであり、実際にガンマ線顕微鏡のような測定精度と擾乱の相反関係が常に成立しているのかは、近年まで明らかにされていなかった。この問題は、2003 年に本研究代表者の研究によって明らかにされ、これまで予想されたことのない、新しい測定精度と擾乱の関係（普遍的不確定性原理）が明らかにされた。本研究では、この関係式をもとに、任意の量子通信路が示す擾乱と盗聴の精度の間に普遍的な相反関係が存在することを数学的に証明することに成功した。

アリスとボブの間に量子通信路があり、それをイブが盗聴していると想定する。量子通信路は、アリスとボブが共有し、環境と相互作用する媒体からなり、初期状態をアリスが準備し、終状態でボブの測定が可能とする。一方、イブは終状態における環境のみが直接測定可能とする。この時、ある定数 K が存在して、2 つの観測量の組 A、B に対して、イブによる A の盗聴測定の精度 $\varepsilon(A)$ と通信路における B の擾乱 $\eta(B)$ の間に、

$$\varepsilon(A)\eta(B)+\varepsilon(A)\sigma(B)+\sigma(A)\eta(B)\geqq K$$

の関係が成り立つ。ここで、σ は量子通信路の入力状態における標準偏差を表す。K が大きいほどその通信路の安全性が高いと言える。量子暗号では、アリスは媒体の一部を保持し、環境と相互作用しない部分（デコヒーレンスフリー部分空間）が存在する。デコヒーレンスフリー部分空間だけを変化させるユニタリ変換の集合を S とすると、

$$K=\sup_{V\in S}(1/2)|\langle V[A,B]\rangle|$$

が成り立つ。ただし、sup は、S に属する全ての V についてとるものとする。特に、環境と相互作用しない部分系（デコヒーレンスフリー部分系）が存在する場合は、A、B はそれと相補的な系に属し、初期状態の部分トレースを ρ とすると、

$$K=(1/2)\mathrm{Tr}|\sqrt{\rho}[A,B]\sqrt{\rho}|$$

が成り立つ。これらの関係から、量子鍵配送の安全性が新しい方法で導くことができ、量子暗号一般に対する安全性理論の基礎を与える。

２．２．新量子認証プロトコルの開発

本研究では、従来の古典情報を用いた暗号技術に代わる技術として、量子情報を利用することによって原理的レベルから情報漏えい防止や盗聴検知を行う量子クレジットカードプロトコルを提案した。このプロトコルでは顧客Aは認証機関Bにいかなる古典的照合情報も預けず、替わりにベル状態にある一方の量子ビット系の列のみを預ける。このBの量子系には顧客の情報は全く含まれない。ベル状態の他方の量子ビット列は量子クレジットカードに保管してAが保持する。また下図の（1）のように量子カードには顧客Aの併用する古典的暗証番号によって鍵をかける。認証ではAは図の（2）のように非直交量子状態に符号化された量子暗証番号を量子カード中の量子ビット列とともにBに送る。Bは自分が保管していた量子ビット列とAから来た量子カードにあったビット列とを合わせて、入力された量子暗証番号で量子鍵を開錠する(図中（3）)。そして得られた2 量子ビット列の状態からAが持つべき正規の量子状態と同じかどうかを判定する(図中（4）)。このとき我々の発明した量子鍵部分は量子暗証番号とベル状態量子ビット列との間には量子もつれを生成しないことが特徴である。このため認証後、量子暗証番号部分をBは破棄して、Aの量子カードに収納するベル状態の量子ビット列の片方のみを送り返せばよい(図中（5）)。この量子暗証番号の使い捨てにより、Aはカード以外に暗証番号用の量子ホルダーを携帯する必要がない。顧客Aの古典的暗証番号はBや他に全く知らせる必要がない。また、AはBと通信することなく、いつでも暗証番号を手持ちの量子カード中の量子ビット列にユニタリー変換を施すことによって変更することもできる。つまりAの暗証番号は認証の度に変更して使い捨てにすることも可能である。

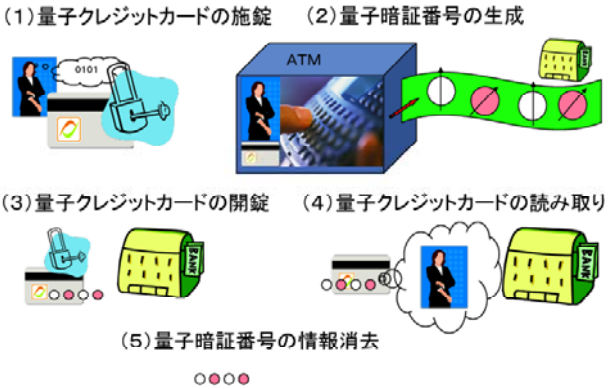

図 1. 新量子認証プロトコルの概要

３．むすび

量子暗号の安全性は、盗聴者の測定行為が通信路の状態を不可避に乱すという不確定性原理から保証されると考えられてきたが、従来の定量的定式化は、普遍性がなくその目的を果たすことができなかった．本研究では、測定精度と擾乱の正しい関係を示す普遍的不確定性原理に基づいて、量子通信路の安全性を保証する関係式を導いた．最近、量子鍵配送の安全性証明に対する情報理論的アプローチの弱点が指摘されたこともあり、本研究のアプローチは、今後、ますます重要性を増すと予想される。

本研究で提案した量子認証プロトコルでは、認証機関に古典情報を預けないことにより情報漏洩を防止しながら量子クレジットカードを暗証番号で施錠することによりカード盗難による成り済ましを防ぐという、これまでのプロトコルにない特長を持つ。この新しい認証方式は、高度 IT 時代の社会システムに不可欠な認証方式として将来の国際標準化が期待できる。

【誌上発表リスト】

[1] M. Hotta and M. Ozawa, “A Protocol of Quantum Authentication with Secure Quantum Passwords”, Quantum Communication, Measurement and Computing (QCMC): Ninth International Conference on QCMC, AIP Conference Proceedings Vol.1110, pp.388-391 (2009).

[2] Masahiro Hotta, “Quantum measurement information as a key to energy extraction from local vacuums”, Physical Review D Vol.78, Art.045006 (pp.1-9) (18 July 2008).

[3] Masahito Hayashi, “Optimal ratio between phase basis and bit basis in quantum key distributions” Physical Review A Vol. 79, Art.020303(R) (pp.1-4) (5 February 2009)

【申請特許リスト】

[1] 小澤正直、堀田昌寛、量子認証方法、量子認証システム及び量子認証装置、日本国、2007 年 9 月 28 日（特願 2007-255159、特開 2009-88916）

【受賞リスト】

[1] 小澤正直、2008 年度日本数学会賞秋季賞、“量子情報の数学的基礎”、2008 年 9 月 25 日