平成 26 年 5 月 8 日

玉川大学 量子情報科学研究所

量子鍵配送の安全性理論の数理的誤りを証明

最近、科学技術に関する過大な成果報告に対し、科学者自身による真摯な検証が求められている。玉川大学量子情報科学研究所（町田市玉川学園 6-1-1 所長：広田 修）の加藤 研太郎 准教授と岩越 丈尚 助教とノースウエスタン大学の Yuen 教授は、その渦中の一つである Bennett-Brassard 型量子鍵配送やその派生モデルの安全性理論の数理的な誤りを証明する事に成功した。特に、現理論の安全性の定量的保証の正当化に用いられる数学理論（カップリング定理）が、その正当化を保証しないことを証明した。これにより、現存する全ての量子鍵配送システムの安全性の保証は白紙に戻り、これまで、原理的な欠陥があるという主張が厳密に実証された。この結果に関する本学の成果は平成 26 年 5 月 12 日（月）、国内の全ての量子鍵配送研究グループが集う電子情報通信学会量子情報技術研究会、ノースウエスタン大学は 5 月 12 日（月）、Proceedings of IEEE 用の論文として電子アーカイブで発表する。

【掲載論文名】

“岩越・広田、トレース距離を量子鍵配送の失敗確率とする解釈における課題”

“ H.P.Yuen, Can Quantum Key Distribution be Secure ? ”

【今回の成果】

現代暗号学において無条件安全な暗号は、ビット毎に鍵ビットを使い捨てる鍵使い捨暗号以外には存在しない。その実現に必要な大量の鍵ビットを配送するためには無条件安全な量子鍵配送技術が必要であると主張され、世界中の研究機関で開発競争が実施されている。その安全性は配送された鍵列を表す量子状態列が理想的なものとならない“失敗確率”によって保証されている。その根拠を提供する数理理論はカップリング定理であるとされていたが、これまで、このような理論体系は量子鍵配送の真の安全性を評価していないという疑念が多数示されていた。

しかし、今回、玉川大学の加藤 研太郎 准教授のカップリング定理解析を基に、その定理は、現理論が望むような失敗確率という解釈を与えないことを具体例を持って証明する事に成功した。また、更に詳細な結果はノースウエスタン大学の Yuen 教授によって Proceedings of IEEE で発表される。本学の結果は、平成 26 年 5 月 12 日（月）、国内の全ての量子鍵配送研究グループが集う電子情報通信学会・量子情報技術研究会（会場：名古屋大）において発表される。

【取材に関するお問い合わせ】
学校法人 玉川学園
キャンパス インフォメーション センター
TEL：042-739-8710 FAX：042-739-8723
E-mail：pr@tamagawa.ac.jp
〒194-8610 町田市玉川学園 6-1-1

【研究内容に関するお問い合わせ】
玉川大学 量子情報科学研究所
教授 広田 修（ひろた おさむ）
研究室：042-739-8674
E-mail: hirota@lab.tamagawa.ac.jp

＜資料＞

【背景】

量子鍵配送は、単一光子などの量子効果の強い微弱な光信号を用いる。その安全性は多くの理論研究者によって証明済であると考えられており、世界的に開発が続けられている。上記のシステムはノルウエー・ドイツのチームにより受信機に対するサイドチャンネル攻撃と呼ばれる攻撃によってハッキングされた。現在、それを避けるために受信装置に依存しない量子鍵配送プロトコル開発に移行している。しかし、あらゆるサイドチャンネル攻撃を防いでも、最後には現在の安全性証明の真偽に行き着く。これまで、その安全性の最終証明の原理的な欠陥を指摘する論文が専門的なジャーナルに多数公開されていたが[1]、それらは理論的概念の難易度が高く、一般の研究者には本質を見分けることが困難であった。今回、その簡易的な説明が可能となった。

【安全性の意味の重要性】

量子鍵配送は、盗聴者が単一光子信号から入手可能な鍵系列に対する情報を推定して、その知見に基づいて秘密増幅を実行する事によって鍵配送の情報理論的安全性を保証する。安全性を定量的に評価するために、配送鍵を表す量子状態列と完全ランダムな理想量子状態列の近さを測るトレース距離という数学的測度が採用される。このトレース距離の上限は量子通信の種々のパラメータから具体的に決まり、その値を情報理論的安全性の定量的評価値とする。この上限値はカップリング定理から、実際の量子通信によって配送された鍵系列が理想の鍵系列にならない確率、いわゆる“失敗確率”であると結論づけられている。Yuen 教授が本学での講演で、そのカップリング定理の誤用の核心部分を指摘し[2]、それを基に加藤 研太郎 准教授が具体的な論理矛盾を証明した[3]。今回、失敗確率の根拠の論理矛盾をさらに単純に説明する証明を与えることに成功した。

トレース距離の上限値が失敗確率でないとなると、何を意味するのかが課題となる。Yuen 教授と Hirota 教授は、その上限値は盗聴者が配送鍵を推定する際の鍵列の均一性を表し、実現可能なその上限値は計算量的安全性に基づく数理暗号よりぜい弱を意味すると主張していた[4]。今回の成果は、両教授の主張である「この種の量子暗号は情報理論的安全であっても計算量的安全な暗号の計算時間より遥かに速く、確実に鍵系列を言い当てることができ、従来暗号より強くできない」をさらに堅固なものにした。

[1] H.P.Yuen, “Fundamental quantitative security in quantum key distribution”,
Physical Review A, 82, 062304, 2010.

[2] H.P.Yuen, “On the nature and claims of quantum key distribution”,
Open Lecture of Tamagawa University Quantum ICT Institute, 5 December, 2013.

[3] 加藤, “QKD のトレース距離基準での最大失敗確率解釈は成立しない”,
量子情報ミニワークショップ（愛知県立大主催）、2 月、2014.

[4] O.Hirota, “Incompleteness and limit of quantum key distribution”,
Quantum ICT Research Institute Bulletin, vol-2, 2012.