平成 26 年 5 月 26 日

玉川大学 量子情報科学研究所

「Nature 発表の新方式（信号擾乱検出なし）量子鍵配送の脆弱性証明に成功」

不確定性原理によって安全性を保証する量子鍵配送技術は、暗号学に基づく定量的な安全性評価において欠陥を持つことが指摘されてから、その不確定性原理による信号擾乱を検出する方式を捨て、情報因果律などを採用する方式が Nature などの論文誌で提案されるようになった。玉川大学量子情報科学研究所(所長：広田修)の加藤 研太郎准教授と岩越 丈尚助教はノースウエスタン大学の Yuen 教授と協力し、それらの新しい方式は従来技術と同様、実用性のある安全性が保証されないことを指摘し、さらに、その方式では伝送速度がゼロになる事を証明する事に成功した。この結果に関する本学の成果は平成 26 年 8 月と 9 月にサンディエゴやアムステルダムで開催される SPIE 国際会議で発表する。

【今回の成果】

量子鍵配送技術の安全性の根拠は、単一光子などの微弱な光信号を盗聴者が測定しようとする際に不確定性原理などにより擾乱が起こり、その擾乱の計量値を基に秘密増幅などの処理を実行することによって送受信者間で共有したビット系列の安全性（一様乱数性）を保証するものであった。しかし、本研究所は、その安全性を保証する評価理論は Nielsen の本[1]に記載されている理論を誤用していることを指摘してきた。その結果、従来の量子鍵配送は従来の暗号技術よりはるかに弱い、すなわち、共有される鍵系列は一様なランダム性を持つことが無く、非常に強い相関を持つことを証明している。一方、最近、光子信号への擾乱量の検出なしのプロトコルなどが提案されるようになった。しかし、今回、玉川大学グループは上記の新しいプロトコルの安全性もまた、これまで本研究所が解明してきた理論に従うことを証明し、それらの安全性はほとんど無いに等しいことを示した。この成果は平成 26 年 8 月と 9 月に開催される SPIE 国際会議で発表する。また、更に詳細な結果はノースウエスタン大学の Yuen 教授の Quantum Information Processing(Springer)に掲載される論文で発表される。

[1] M. Nielsen and I. Chuang, “Quantum Computation and Quantum Information”, Cambridge University Press, 2000.

■論文名

“T. Iwakoshi and O. Hirota, Problem with Interpretation of Trace Distance in Quantum Key Distribution”

“ H. P. Yuen, Some Physics and System Issues in the Security Analysis of Quantum Key Distribution Protocols”

【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】

近年、研究機関の報道に過大な表現が散見され、科学者自身による成果表現の精査が必要となっている。特に、(a)ＳＴＡＰ細胞、(b)量子鍵配送、(c)小澤不等式などには多くの疑念が提出され、論争が開始されているのは周知であり、学会での詳細な議論が求められている。ノースウエスタン大学を中心とする理論グループは、量子鍵配送の基本理論とその実験検証については、大きな欠陥と誤りがあり、その安全性は従来の暗号の性能以下であることを、繰り返し解説してきた。最近、Nature に発表された「擾乱を用いない量子鍵配送」[1]論文は警鐘を無視し、多くの誤りを含んでいる。今回、当該論文の誤りと、その一般社会向けへの成果報告の齟齬を解明した。

[1] T.Sasaki, Y.Yamamoto, M.Koashi, “Practical quantum key distribution protocol without monitoring signal disturbance”, Nature, vol-509, 22 May, 2014.

【擾乱を用いない量子鍵配送の安全性の欠如に関する解説】

上記論文の問題点を簡単に解説する。まず、この論文では、どれだけの効率で鍵系列を伝送できるのかが主題となっており、その鍵系列の安全性の定量的評価を解析する式もなければ、詳細な分析もない。本来、暗号の論文であれば、どれほどの安全性の下でどれだけの効率で鍵系列が伝送されるかを明記することが必須である。提案しているシステムの安全性に関しては、既存の理論論文を引用するにとどまっており、ノースウエスタン大学と玉川大学が解明した既存理論の誤りに関する論文[2,3,4,5]に言及せず、これまでの概念をそのまま継承している。さらに、効率を表す論文[1]中の式（１）は正確な根拠がなく、推量でしかない。特に、盗聴者がプローブから得るであろう情報が全く考慮されず、誤り訂正符号や秘密増幅符号から漏れる情報も考慮されていない。これらをこの論文が想定するシステム条件で考慮すれば、効率はゼロになることが導ける。このように、量子鍵配送と言う暗号学的機能の論文でありながら、全く暗号学的な考察が無いことが科学論文としての問題点である。さらに、安全な鍵の伝送速度に格段の進歩が期待できるという成果報道の内容は、本証明によって、正しくないことが示された。

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

[3] H.P.Yuen, “On the nature and claims of quantum key distribution”, Open Lecture of Tamagawa University Quantum ICT Institute, 5 December, 2013. URL. http://www.tamagawa.jp/research/quantum/openlecture/

[4] O.Hirota, “Incompleteness and limit of quantum key distribution”, Quantum ICT Research Institute Bulletin, vol-2, 2012. URL. http://www.tamagawa.jp/research/quantum/bulletin/2012.html

[5]加藤研太郎, “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.