2010．10．15

玉川大学 学術研究所

「量子鍵配送の安全性神話の崩壊」を例証

玉川大学学術研究所：量子情報科学研究センターは、単一光子量子鍵配送を用いたバーナム暗号の安全性が無条件安全とは程遠いことを、量子鍵配送の欠陥を指摘した Northwestern 大学の Yuen 教授の理論に基づいたシミュレーションによって例証した。これによって、これまで究極のセキュリティ技術と考えられていた現在開発中の量子鍵配送システムには原理的な欠陥があることが明らかになった。

この結果を平成 22 年 11 月 18 日（木）、電子情報通信学会光通信システム研究会において発表する。

【今回の成果】

現代暗号学において無条件安全な暗号は、鍵を使い捨てる暗号であるバーナム暗号以外には存在しない。その実現に必要な鍵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。最近の量子暗号理論に基づき、量子鍵配送の性能をシミュレーションによって分析した結果、それらの量子鍵配送による生成鍵を用いたバーナム暗号は無条件安全ではなく、極めて安全性が低いことが数値的に示された。

本結果を、平成 22 年 11 月 18 日（木）、電子情報通信学会・光通信システム研究会（会場：大阪）において発表する。

■論文名

“ 単一光子量子暗号のネットワークへの不適合性と盗聴可能性に関する考察 ”

＜取材に関する　問い合わせ先＞
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（担当：奥田、井上）
TEL：042-739-8710　：E-mail：pr@tamagawa.ac.jp

＜研究に関する　問い合わせ先＞
玉川大学学術研究所 量子情報科学研究センター　TEL：042-739-8674