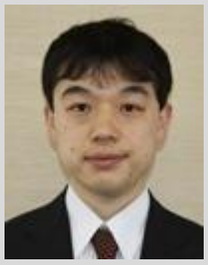
No. G-1

会津大学

現実の環境において安全な量子鍵配送方式



上級准教授　渡邊　曜大

概要

○現在標準的に用いられているほとんどの暗号技術の安全性は、桁数の大きい素因数分解問題や離散対数問題を解くのが難しいといういわゆる計算量的な仮定にもとづいています。このような計算量的な仮定にもとづく暗号は、計算機能力の向上やアルゴリズムの発展に伴い、長い期間にわたってその安全性を確保することが難しくなってきています。一方、量子鍵配送の目的は、無限の計算資源をもつ攻撃者に対しても安全に鍵を共有することです。したがって、その安全性は計算機能力の向上やアルゴリズムの発展とは完全に独立であり、「無条件の安全性」とも呼ばれています。

○量子鍵配送では、量子力学の原理を利用することによって、盗聴行為を検出できるようにプロトコルを設計します。これまでに提案されている方式では、送受信機の誤差が無視できると仮定されていますが、現実の実装では、通常無視できません。我々の研究では、送受信機に任意の誤差があっても、その誤差を適切に反映した秘匿性増強を行うことによって、安全に鍵を配送する方式を提案しました。

実用化の可能性

○量子鍵配送装置の開発

任意の誤差を許した送信機および受信機に対して安全性が保証できる量子鍵配送方式を提案しました。本方式を用いることによって、現実の実装において安全な量子鍵配送の実用化が期待できます。

UBICからのメッセージ

○送信者が光子に載せた鍵情報を受信者に送ります。送信者が送った鍵情報と受信者が受け取った鍵情報が一致しないときは、盗聴されていると仮定します。

○従来の技術では、量子鍵送受信機の誤差があると送信者と受信者の鍵が一致しないので盗聴があると判断してしまい、鍵配送の効率が悪かったのです。

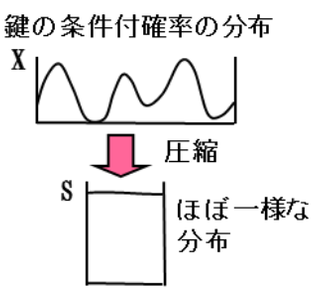
○本技術は、量子鍵送受信機に誤差があっても鍵を安全に配送することができ、鍵配送の効率を向上することができます。

研究概要図

量子鍵配送の実行手順

①情報の送受信
②エラー率推定
　送受信情報間の誤りを推定
③誤り訂正
　送受信情報間の誤りを訂正
④秘匿性増強
　盗聴者にランダムにみえるように情報を圧縮し、鍵を生成する

秘匿性増強の概念図



■問題
盗聴者が何らかの部分情報を持っている共有鍵（左図の X）から安全な秘密鍵（左図の S）を作る

■解決法
➢圧縮関数としてユニバーサルハッシュ関数を用いる
➢圧縮率を2次のレニーエントロピーの値で定める

無限の計算資源をもつ攻撃者に対しても安全な暗号