

情報通信の基礎研究

准教授　松本 隆太郎

研究分野：量子情報理論、ネットワーク符号化、情報理論的セキュリティ

ホームページ: http://www.rmatsumoto.org/research.html

●研究内容・目的

　より高い効率を有する量子暗号プロトコルの構成

1. ネットワーク符号化によるコンピュータネットワークの高速化
2. ネットワーク符号化による通信デバイスの省電力化

●研究テーマ

１．暗号の情報理論的な安全性

インターネットなどで現在よく使われているRSAなどの暗号方式は、大きな整数の素因数分解などのいくつかの計算問題を短い時間で解く方法が知られていないことに安全性の根拠を置いている。このような安全性を計算量的安全性と呼ぶが、もし素因数分解などを高速に解く方法が発見されれば計算量的安全性にもとづく暗号方式は使用できなくなってしまう。一方、秘密にしたい情報と悪意を持つ第三者が持つ情報が統計的に独立であれば、悪意を持つ第三者がいかに強力な計算機を持っているとしても秘密にしたい情報を当てずっぽうに推測するよりも正確に知ることはできない。秘密にしたい情報の統計的独立性を保証することによって得られる安全性を情報理論的安全性と呼び、本研究室では情報理論的安全性を保証できる以下のような暗号方式の研究を行っている。

１－１．量子暗号（量子鍵配送（QKD）プロトコル）

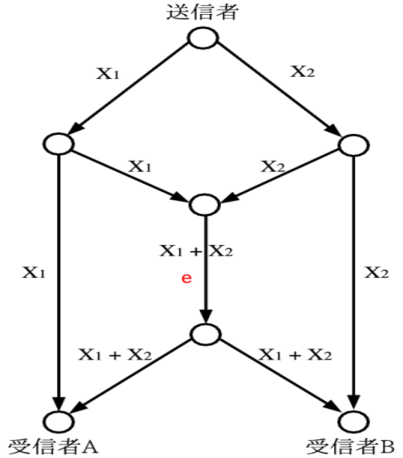
量子暗号の中の代表的な方式である量子鍵配送（QKD）プロトコルは、情報理論的に安全な暗号方式でもある。QKDプロトコルの目的はAliceとBobと呼ばれる正規ユーザーの間でEveと呼ばれる盗聴者に知られないように乱数列を共有することである。共有乱数列はAliceからBobに秘密裏に情報を伝えるために用いることができる。乱数列を共有するために、AliceはBobに単一光子の偏光などの量子力学の性質が強く現れる物理媒体を送る。もしEveがこの物理媒体を測定すると、量子力学の原理により測定された物理媒体の状態が変化してしまう。AliceとBobは送受信状態の変化からEveが得た情報量を推定し、送受信情報を適切に短くすることによってEveが得た情報と統計的に独立な乱数列を生成する。送受信状態の変化の仕方を推定することを通信路推定と呼ぶ。本研究室では、通信路推定に従来は捨てられていたデータを用いるとより正確に通信路推定が可能になるため共有できる乱数の量が増加することを明らかにし（文献[1]）、提案した通信路推定法に合わせて物理媒体の送信方法を変えるとさらに共有できる乱数が増加することを示した（文献[2]）。

１－２．雑音を用いた乱数の共有

前述の量子鍵配送プロトコルの実現には今のところ高価なデバイスを用意する必要がある。情報理論的に安全な鍵共有を比較的安価に実現するために自然界に存在する雑音を利用した鍵共有法がMaurerによって提案されている。Maurerの方法では前述のAlice, Bob, Eveが共通の雑音源（天体や無線LANなどなんでもよい）から信号を受信しているときに、Eveが盗聴することができる公開通信路を用いてAliceとBobが対話をすることによってEveに知られていない乱数を共有する。実際に受信する雑音は電波などの連続量であるが、Maurerの方法は雑音が離散的なディジタル情報である場合に対してしか検討が行われていなかった。そこで本研究室では文献[3]において雑音源が連続量であるときにEveに知られずに共有できる乱数の量を評価し、また連続的な雑音源を量子化したのちに従来のMaurerの方法を用いる場合にくらべて、より多くの乱数を共有できる方式を開発した。

２．ネットワーク符号化

従来のコンピュータネットワークでは情報の中継ノードでは、隣接したノードから受け取る情報を別のノードにそのまま転送することしか許されていなかった。しかし、中継ノードにおいて複数の隣接ノードから受け取った情報を加工してから転送することを許すと、通信速度や消費電力が向上することが近年明らかにされた。

　例えば、右図のように、送信者が受信者Aと受信者Bに同一のデータを送信したいとする。中継ノードが受信情報をそのまま転送しなければいけない場合は、情報X1とX2の両方を受信者AとBに届けることはできない。しかしながら、リンクeに送出する情報をX1とX2の和（正確には排他的論理和）とすることにより、送信者AはX1とX1+X2を受け取り、それらから送信情報であるX1とX2を復元することができる。このように中継ノードに複数の隣接ノードからの情報を加工して転送することを許す方式をネットワーク符号化と呼ぶ。

●教員からのメッセージ

　粘り強く取り組める論理的思考が好きな学生をお待ちしています。

●関連する業績、プロジェクトなど

**論文 :**

**[1] S. Watanabe, R. Matsumoto, and T. Uyematsu, “Tomography increases key rates of quantum-key-distribution protocols,” Physical Review A, vol. 78, no. 4, p. 042316, October 2008.**

**[2] R. Matsumoto and S. Watanabe, “Narrow basis angle doubles secret key in the BB84 protocol,” Journal of Physics A: Mathematical and Theoretical, to be published, April 2010.**

**[3] M. Naito, S. Watanabe, R. Matsumoto, T. Uyematsu, “Secret key agreement by soft-decision of signals in Gaussian Maurer’s model,” IEICE Transactions on Fundamentals, vol.E92-A, no.2, pp.525-534, February 2009.**

**受賞 : 電子情報通信学会論文賞 (2001, 2008, 2011, 2014), 電子情報通信学会喜安善市賞(2008, 2014), 丹羽保次郎記念論文賞(2003)**