國廣　昇
電気通信大学　准教授

量子力学に安全性の根拠をおく量子プロトコル（量子選挙、量子現金などの）の構築を目指して研究を行った。構成すべき量子プロトコルは不確定性原理に安全性の根拠を置くため、計算量的な安全性を持つ暗号プロトコルが崩壊後も安全であるという特徴がある。

プロトコルを提案する上で、その基となる量子的な道具として、量子 fingerprint を採用した。このプロトコルを用いれば、量子状態がわからなくても、二つの量子状態が等しいかどうかを高い確率で判定することが可能となる。このプロトコルの効果的な利用法の模索を行ない、量子現金方式の提案を行った。

量子現金方式は、古くからいろいろな方式が提案されているが、我々が目指した方式は、オフライン検証性を満たし、なおかつ追跡不可能性を満たす量子現金方式である。オフライン検証性とは、商店が、その都度、銀行に現金の正しさを検証する必要がない方式である。小額決済ではこの特徴があることが望ましい。追跡不可能性とは、現金を正しく顧客が使った場合は、銀行と商店が結託をしても、その顧客の個人情報が漏れないことである。これらの方式は、現金として満たすことが望ましい方式である。我々は、この二つを満たす方式を提案し、その安全性解析を行っている。提案方式を安全に運用するためには、若干の運用上の制約を設ける必要があるものの（現金の有効期限を設ける、店、顧客の信用度に応じて、情報の発行量の調整をするなど）、量子通信路、量子操作が可能となった場合には、有効な方式の一つなりうる方式である。

これの結果を。国際会議 1 件、国内のシンポジウムで 2 件口頭発表を行っている。

研究成果

オフライン検証性を満たす追跡不可能な量子現金について
2006 年暗号と情報セキュリティシンポジウム　3C2-3　2006

Untraceable Off-Line Verifiable Quantum Cash
Proc. of TQC2006　P21-22　2006

オフライン検証性を満たす追跡不可能な量子現金

暗号関連ミニワークショップ 2006