京都量子暗号ワークショップ

２０２１年３月１６日　Zoom ハイブリッド

動画（午前）
https://www2.yukawa.kyoto-u.ac.jp/~tomoyuki.morimae/kyotoQcrypt_morning.mp4

９：００－１０：００　森前智行（京大基研）
「局所ハミルトニアンによる量子計算の検証」
量子計算が正しく動作しているかどうかを検証するプロトコルは量子計算の検証プロトコルと呼ばれている。本講演では、２０１８年に我々が提案した局所ハミルトニアンに基づくプロトコルを紹介し、さらに、その最近の発展（ゼロ知識証明、Trusted center モデル、マハデフによる検証者の古典化）についても簡単に解説する。

１０：００－１１：００　竹内勇貴（NTT CS 研）
「ハイパーグラフ状態のブラインド量子計算への応用」
ブラインド量子計算は、弱い計算能力しか有していないクライアントが、計算の入力、出力、量子アルゴリズムを漏洩すること無く、遠隔地のサーバにユニバーサル量子計算を委託することを可能にする。さらに、委託した量子計算をサーバが正しく実行しているかの検証も行うことが出来る。これまで、クライアントに必要な量子操作を簡易化するための様々な研究が行われてきた。本発表では、グラフ状態の一般化であるハイパーグラフ状態を応用することで、クライアントの量子操作をパウリ X, Z 測定まで減らせることを示す。情報理論的に安全なブラインド量子計算を構成するためには古典クライアントでは不十分だという証拠がいくつか見つかっているため、クライアントに必要な測定の種類を減らすのは有望な方向性である。

１３：００－１４：００　水谷明博（三菱電機）
「任意の独立同一分布に従う状態を用いた量子鍵配送」
量子鍵配送の安全性証明は、送受信者の装置に数学的モデルを

仮定したもとで行われる。実装の観点からは、この数学的モデルは現実の装置の物理特性を反映したものであることが望ましく、これまでの量子鍵配送の安全性証明は、この数学的モデルの実現難度を緩和する方向で進められてきた。我々は、送信装置が独立同一分布に従う状態を放出するならば、どんな送信装置を用いても、安全な量子鍵配送が可能であることを示した。本講演では、提案したプロトコルと安全性証明の概要を解説する。

１４：３０－１５：３０　廣政良（三菱電機）

「(量子) 完全準同型暗号と回路秘匿性」

完全準同型暗号は公開鍵暗号の一種で、暗号化したまま任意の（古典）回路を計算できる暗号方式である。量子完全準同型暗号は完全準同型暗号の量子的な類似方式で、暗号化したまま量子回路を計算できる暗号方式である。本発表では、格子問題の困難性に基づく完全準同型暗号、量子完全準同型暗号の具体的な構成と、その二種類の暗号方式を結び付ける回路秘匿性と呼ばれる安全性概念について紹介する。

１６：００－１７：００　相川勇輔（三菱電機）

「同種写像暗号の数理」

量子計算機による解読に耐えうる次世代の公開鍵暗号、すなわち耐量子計算機暗号の研究が現在世界的に進められており、楕円曲線を用いた同種写像暗号はその有力な候補の一つと考えられている。本講演では異分野の方々との情報共有を念頭に同種写像暗号の数学的背景や暗号の数理モデリングを、最近の我々の研究を紹介しながら解説したい。さらに時間が許せば、同種写像暗号への量子攻撃に関する最近の進展についても触れたい。