大阪産業大学　研究シーズシート

研究シーズテーマ	量子暗号の新方式提案および安全性検証に関する基礎研究
分　野	量子情報科学
キーワード	量子暗号
研究者名・職位	吉田雅一・講師
所　属	デザイン工学部情報システム学科

研究シーズ概要	暗号は安全・安心な情報社会を支えるための必須技術です。広く使われている暗号の多くは、解読に膨大な時間が必要になるという仮定のもとで、安全性を保証しています。そのため、計算機やアルゴリズムの進歩にともない、長期的に安全性を保証することが困難になります。 一方で、量子情報科学の応用技術である量子暗号は、計算機やアルゴリズムが進歩したとしても安全性を保証すると期待されています。本研究では、量子暗号の利活用に向けて、新方式の提案、機能の拡張、安全性の検証に関連した基礎研究を行います。特に、従来の量子暗号の利用では１対１の通信を想定していますが、本研究ではより実用的な 1 対多および多対多の通信への適用を視野にいれた量子暗号に着目します。
進捗状況	[着想・構想段階]　基礎研究段階　実証段階
連携研究の範囲・方法	◆量子暗号の実用性の検討 ◆量子情報科学の応用技術の実用性の検討 ◆量子暗号に関する技術講習会の実施 ◆量子情報科学に関する技術講習会の実施
用途・効果・市場	◆用途：情報システムにおける機密性の保証 ◆効果：高い機密性を保証することが可能 ◆市場：高い機密性が求められる情報システム産業
研究者の業績等	◆ Ayumu Nakayama, Masakazu Yoshida, and Jun Cheng, "Quantum Key Distribution using Extended Mean King's Problem," The International Symposium on Information Theory and Its Applications 2018, pp. 339-343, Oct. 28-31, Singapore, (2018). ◆Masakazu Yoshida, Takayuki Miyadera, and Hideki Imai, "On the Security of Quantum Key Distribution Ping-Pong Protocol," Journal of Quantum Information Science, Vol. 3, No. 1, pp. 16-19, (2013).

連絡先	大阪産業大学 社会連携・研究推進センター　産業研究所事務室 TEL：072-875-3001（内線 2814・2819） FAX：072-875-6551 E-mail：sangaku@cnt.osaka-sandai.ac.jp