量子鍵配送安全性の最新理論

Introduction of latest security proofs of quantum key distribution

○ 玉木 潔 (NTT 物性科学基礎研究所)

Kiyoshi Tamaki (NTT Basic Research Lab)

E-mail: tamaki.kiyoshi@jsap.or.jp

量子鍵配送の一番の特徴は『絶対に破ることができない安全性を有する』ことであろう。しかし、このような究極の安全性は、実際に達成することができるのであろうか？例えば、量子鍵配送装置に仕掛けられた盗聴装置によって、装置内の情報がばらまかれているような状況では、安全性は明らかに崩壊している。この例から、量子鍵配送装置に何の条件も課さずに、安全な通信を達成することは不可能であることが分かる。それでは『絶対に破ることができない安全性を有する』という主張は、正確には何を意味しているのだろうか？それは、『安全性理論から課される装置の条件を、量子鍵配送装置が満たして初めて、絶対に破ることができない安全性を有する』である。つまり、安全性理論が課す条件を量子鍵配送装置が満たすことが安全性には必須なのである。残念ながら、どのように装置を作ったら量子鍵配送がその条件を満たすのか？またその条件をどのようにチェックするのか？という疑問に対しては、この主張は答えてくれていない。

安全性理論が装置に課す要求と実際の装置のこの乖離はサイドチャネルと呼ばれているおり、量子鍵配送に限らず現代暗号にも存在するものである。サイドチャネルを埋めれば埋めるほど実際の量子暗号装置は理想装置に近づき、その結果『絶対に破ることができない安全性を有する』という理想郷が達成される。従って、このサイドチャネルを埋める研究は実際の量子鍵配送装置の安全性保証のために必須である。そのためには、以下の2点が必須となる。

1. 安全性理論を改良し、量子鍵配送装置に課す要求を緩める。特に、その要求は実験によってチェック可能でなければならない。
2. 量子鍵配送装置を作成する際に、装置要求が満たされているかをチェックする。また、チェックするのが難しい際には、更なる理論改良を行う。

1の理論改良と2の装置改良は車の両輪のようなものであり、お互いが協力しながらサイドチャネルを埋める必要がある。本講演では、実際の装置の安全性保証へ向けた最新理論を紹介する。特に、測定装置がもつ任意のサイドチャネルに対する対策、装置がもつ雑音の影響を解決するための理論 [2]、そして装置に対する覗き見攻撃を含む情報漏れ対策の理論 [3] を中心に紹介する。

参考文献

- [1] H.-K. Lo, M. Curty and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
- [2] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Phys. Rev. A **90**, 052314 (2014).
A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, New J. Phys. **17**, 093011 (2015).
Y. Nagamatsu, A. Mizutani, R. Ikuta, T. Yamamoto, N. Imoto, and K. Tamaki, Phys. Rev. A **93**, 042325 (2016).
- [3] K. Tamaki, M. Curty, and M. Lucamarini, New Journal of Physics **18**, 065008, (2016).