Vol.2021-QS-3 No.4
2021/7/1

量子鍵配送の現状と理論的課題について

佐々木 寿彦[1,a)]

概要：量子鍵配送（QKD）は遠隔 2 者間に秘密乱数を共有するプロトコルである．これを用いると長期的な秘匿性をもった暗号化通信が可能となる．QKD は他の量子技術に比べて要求技術レベルが相対的に低く，実際に現状技術で実現可能である．さらに最近では QKD に関するデジュール標準が次々と承認されており，実際に社会実装されそうな勢いがある．
QKD の理論が行うことは QKD プロトコルの安全性を，装置やプロトコルの性質を用いて証明することである．安全性の証明は，一般的な傾向として装置に要求できる性質が増えれば簡単になる．しかし実際の装置には様々な不完全性が存在するので，なるべく多くの不完全性に対応できるように装置に要求する性質はなるべく少なくすることが求められる．
近年では，コヒーレント光通信技術で使われる光ホモダイン検波や光ヘテロダイン検波技術を用いた連続量 QKD（CV-QKD）が注目されている．これ自体は 2000 年から提案されていたものだが，様々なところに無限次元の難しさが現れるために安全性証明が難しかった．しかし，近年になって安全性証明に手が届くようになってきて新たな注目を集めている．私の所属する小芦研でも，ホモダイン検波を使いつつ比較的現実的な設定で安全性が証明できることを最近示した．[Nat. Commun. 12, 252 (2021)]
本講演では，最近の QKD を取り巻く状況を外観した後，特に CV-QKD を題材にして QKD の理論構造を解説し，現状の理論的課題についても議論する．

[1] 東京大学大学院工学系研究科物理工学専攻
[a)] sasaki@qi.t.u-tokyo.ac.jp