Quantum key distribution using practical devices

07 絶対に安全な共有鍵を作れるか

～今あるハードウェアで量子暗号の実現を図る～

どんな研究

絶対に盗聴されることなくランダムなビット列を二者間で共有する方法を見つける研究です。量子暗号と呼ばれる方法で、原理的には実現可能なことが保証されています。実際の装置でも実現できるように、緩やかな前提条件でも可能であると示すことを目的としています。

どこが凄い

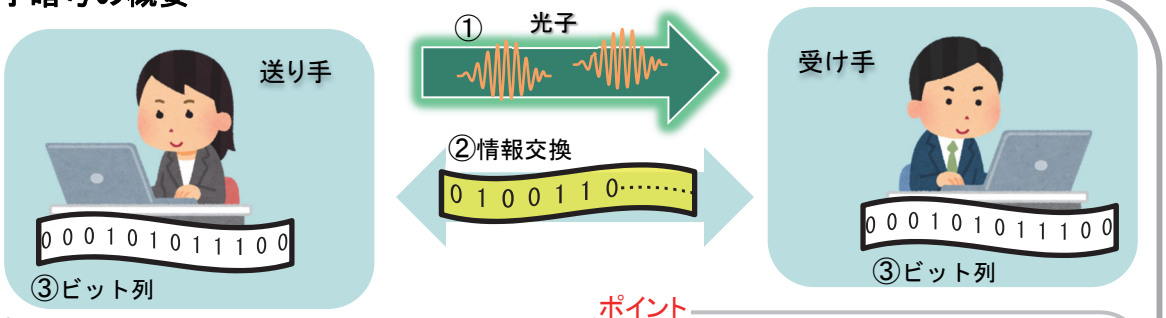
これまでの量子暗号の安全性を保証する理論では、装置が無限大の精度で動作することが仮定されていました。しかし、新しい解析手法を創出したことで、一定の精度で動作することが保証できれば、同一の手順で実施したとしても安全性を担保できることを証明しました。

めざす未来

これまでの原理の実現を目指して開発された量子暗号装置では、製造者を信頼することでしか安全性を担保することができない部分が存在します。しかし、この研究の先には、利用者が直接幾つかの項目をチェックすることによって安全性が担保できる世界が待っています。

安全な秘密通信はランダムな秘密のビット列（秘密鍵）の共有で実現
このようなビット列の共有は通常の公開通信では原理的に不可能

量子暗号の概要

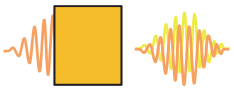


① 送り手が受け手に光子をたくさん送る
② 光子の送受の状況に応じて情報を交換
③ 光子の送受の状況及び交換した情報から送り手と受け手が秘密のビット列を生成

ポイント
- 生成されたビット列は同じでかつ秘密
- 手順①で量子力学の原理の影響を受ける

手順①の詳細な構造

— 手順①を実施するうえで従来要求されていた装置への条件

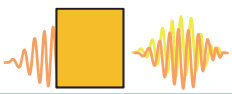


- ちょうど逆位相に変換できなければいけない

光子という粒は量子力学で考えるからこそ現れる

- 光子の数を数えられなければいけない

— 手順①を実施するうえで本研究で緩和された装置への条件



- 逆位相から多少ずれても良い

- 光子の有無がわかればよい

関連文献

[1] K. Tamaki, M. Curty, G. Kato, H. K. Lo, K. Azuma, “Loss-tolerant quantum cryptography with imperfect sources,” *Physical Review* A, 90, 052314, 2014.
[2] G. Kato, K. Tamaki, “Security of six-state quantum key distribution protocol with threshold detector,” *Scientific Reports,* 6, Article number: 30044, 2016.

連絡先
加藤 豪 (Go Kato) メディア情報研究部 情報基礎理論研究グループ
E-mail: kato.go(at)lab.ntt.co.jp