09 新たな秘密がこれまでの秘密を脅かす

～「量子情報を用いた秘密分散」の脆弱性の検証～

どんな研究

秘密情報を安全に保管する方法として「量子情報を用いた秘密分散」が提案されていますが、その安全性を確認するには、量子状態の推定可能性を解明することが不可欠です。この展示では、未知の量子状態が増えれば増えるほど、全状態を推定できるようになるという現象の解析結果を紹介します。

どこが凄い

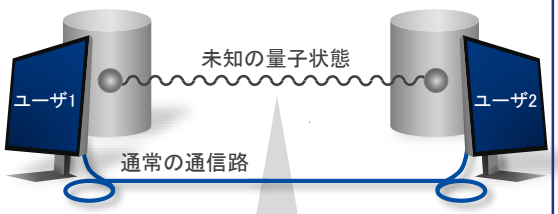
上記の現象が起こる必要十分条件を世界で初めて示し、その現象を引き起こす実装可能な推定方法を発見しました。この結果は、量子状態の推定可能性の解明に大きく貢献し、同時に、「量子情報を用いた秘密分散」の決定的な脆弱性を顕在化させました。

めざす未来

量子状態の推定可能性の解明は、量子情報を用いた未来の様々な情報処理技術の実現に貢献します。これらが実現することで、飛躍的に安全な情報処理が可能となります。また、今の技術では原理的に実現できない機能を持った情報処理が可能となることも期待されています。

量子状態の推定タスク

1. ランダムに選ばれた量子状態を分割してユーザに配る
2. ユーザは通常の通信路を用いて、配られた量子状態を推定する



量子状態が4種類のベル状態（量子情報処理における特有かつ有用な量子状態）からランダムに選ばれる時

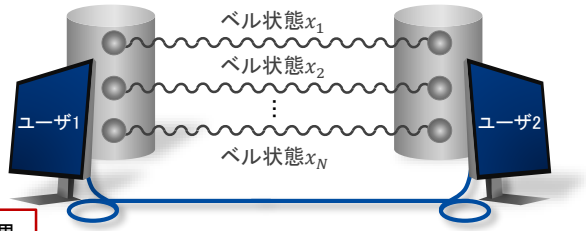
ベル状態1
ベル状態2
ベル状態3
ベル状態4

ベル状態x

推定成功確率< 1

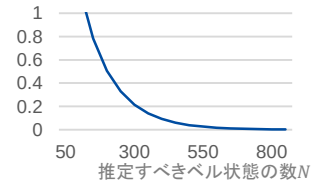
ベル状態の一斉推定タスクの解析

1. ランダムに選ばれた多数のベル状態をユーザに配る
2. ユーザは通常の通信路を用いて、配られたベル状態の種類 $x_1, x_2, \cdots, x_N$を全て推定する



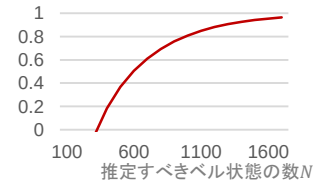
解析結果

ランダムさのエントロピー > 1の時
全推定に成功する確率の上限



▶ どんな推定方法を用いても全推定に成功することは困難

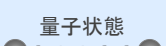
ランダムさのエントロピー < 1の時
全推定に成功する確率の下限



▶ 実装可能な推定方法を用いて高い確率で全推定に成功

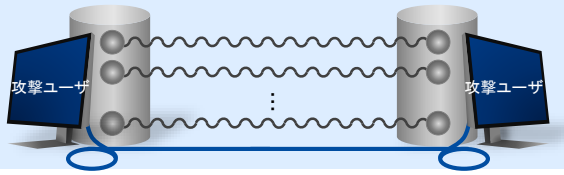
「量子情報を用いた秘密分散」の脆弱性の検証

1. 秘密情報xを量子状態に符号化し、通常の通信路で結ばれたユーザに配る



$x = 1$の時、ベル状態1
$x = 2$の時、ベル状態2
$x = 3$の時、ベル状態3
$x = 4$の時、ベル状態4

2. 攻撃ユーザは、配られた量子状態を推定して秘密情報$x_1, x_2, \cdots, x_N$を読み出そうする



本解析結果→秘密情報の数Nが増えれば増えるほど、全ての秘密情報を読み出されてしまう危険性がある

関連文献

[1] S. Akibue, G. Kato, "Bipartite discrimination of independently prepared quantum states as a counterexample to a parallel repetition conjecture," *Physical Review A*, Vol. 97, No. 10, 042309, 2018.

連 絡 先

秋笛 清石 (Seiseki Akibue) メディア情報研究部　情報基礎理論研究グループ
Email: cs-liaison-ml at hco.ntt.co.jp

Innovative R&D by NTT
オープンハウス 2019