

量子鍵配送の民間航空分野への 適用に関する検討

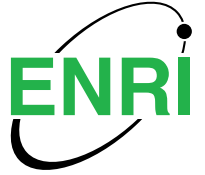
監視通信領域 ※金田直樹、宮崎裕己

2022年6月16日(木) 16:00～

2022年6月17日(金) 16:00～

電子航法研究所研究発表会 ポスターセッション

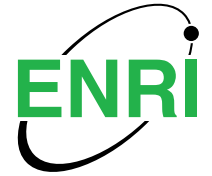
本発表の概要



1

- 研究の背景
- 量子鍵配送とは
- 調査の概要
- 量子鍵配送の民間航空への適用検討
- まとめ

研究の背景



2

- インフラの情報セキュリティが重要となっている
- 航空交通も重要なインフラ
→ 安全な航空交通を実現するため、ICAOは重要な情報通信システムとデータに対するセキュリティ対策を求めている
- 情報セキュリティの重要な要素：機密性、完全性、可用性
 - **機密性**：許可されていない人が情報を閲覧したり利用できない
→ 暗号
 - 鍵配送問題：(無線通信のように)だれでも傍受できる通信により機密性を確保するための方法？
→ **公開鍵暗号**
- 公開鍵暗号の解読にはスパコンでも数万年以上必要
→ 事実上解読不可能
→ コンピュータの計算速度は日々向上しており、現在の公開鍵暗号は将来的に解読されるかも？

量子鍵配送とは



3

- 量子鍵配送(Quantum Key Distribution)
量子力学の基本原則を用い、送信者と受信者の間で乱数(鍵)を安全に共有
 - 送信者と受信者が協力して盗聴を検出可能
→ 鍵が盗聴されていないことを保証できる
 - 量子暗号: QKDで生成した鍵を用いる暗号
 - QKDの安全性は量子力学の基本原則に依拠
量子力学の基本原則は将来にわたり覆りそうもなく、
将来的にも安全と考えられる
- 本調査
 - 量子鍵配送は民間航空でも使える？

■ 国内外の量子情報技術政策

- 欧米と我が国の量子情報に関する研究開発の規模や目標

■ 論文等の文献調査

- 量子鍵配送技術の動向
- 量子鍵配送に必要なとなる素子などの要素技術

→ 技術的な課題

- 鍵生成速度に起因する通信速度の制限
- 伝送距離(途中で増幅できない)

QKDの民間航空への適用検討

6

- 技術的な課題を踏まえ、量子鍵配送の民間航空への適用を検討
- 仮定
 - 航空機の運航は航空会社が行う
 - 量子鍵配送の鍵生成速度: 100kbps
- 監視技術の試算例: 拡張スキッタ方式ADS-Bを24時間動作させるのに必要な鍵を量子鍵配送で生成する時間は100秒未満
→ 運航に支障を及ぼさないと考えられる

まとめ



7

- 調査の結果、量子鍵配送は民間航空分野に利用できる可能性あり
- 具体的な試算例：拡張スキッタ方式ADS-B
- 量子鍵配送は新しいセキュリティ対策として有用と考えている