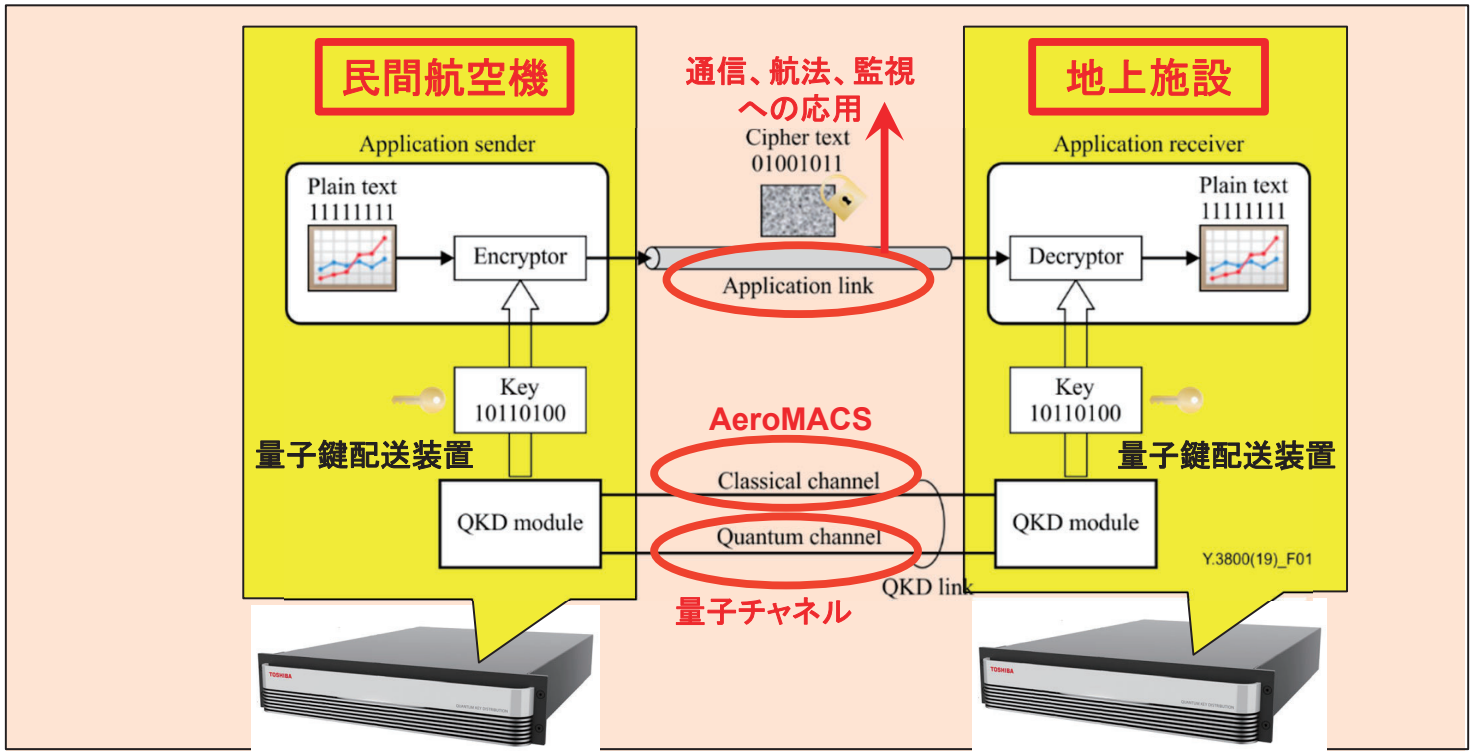
量子鍵配送の民間航空分野への適用に関する検討

監視通信領域　※金田　直樹、宮崎　裕己



民間航空機と地上施設間における将来的な量子鍵配送装置の利用例

◆背景

近年、私たちの生活と経済活動の基盤となる重要なインフラの情報セキュリティが重要となっています。航空交通もまた重要なインフラであり、安全な航空交通を実現するため、国際民間航空機関(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行うよう求めています。情報セキュリティの重要な要素として「許可されていない人が情報を閲覧したり利用できない」という機密性があり、機密性は暗号により確保されています。無線通信のようにだれでも傍受できる通信でも機密性を確保するため、現在は公開鍵暗号が利用されています。公開鍵暗号を解読するにはスパコンでも数万年以上必要と見積もられ、事実上解読不可能と考えられていますが、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懸念があります。

量子鍵配送は量子力学の基本原理を用いて、送信者と受信者の間で鍵と呼ばれる乱数を共有する技術です。このとき送信者と受信者が協力することで鍵が傍受されていないことを保証することができます。量子鍵配送で生成した鍵を用いた暗号が量子暗号です。量子力学の基本原理は将来にわたり覆りそうがなく、量子暗号は将来にわたり解読できないと考えられています。そのような長所を持つ量子鍵配送は民間航空における将来的なセキュリティ対策の一つとして有望と我々は考えました。

◆調査の概要と成果

本調査研究では、まず、量子鍵配送技術の動向、量子鍵配送に必要となる素子などの要素技術に関する文献調査を行いました。また、国内外の量子情報技術政策に関する文献調査を行い、各国の研究開発の規模や目標などについて調査しました。その結果に基づき、量子鍵配送の民間航空分野への適用可能性について検討しました。

量子鍵配送は送信者と受信者間が協力して鍵を生成しますが、実際に応用するには鍵生成速度に起因する通信速度の制限、伝送可能な距離が短いことなどが技術的な課題となっています。そこで、我々は航空会社による航空機の運航を前提として量子鍵配送を適用可能かどうかについて試算しました。

以下は、量子鍵配送の鍵生成速度を現時点で達成可能と考えられる 100 kbpsと仮定した事例です。拡張スキッタ方式の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した場合、航空機の運航に支障を及ぼさない100秒未満と試算されました。この結果、量子鍵配送を民間航空分野に利用できる可能性があることがわかりました。

拡張スキッタ方式のADS-Bはなりすまし等が懸念されており、ICAO等で対策が検討されています。現在の技術で実現可能かつ長期的に安全な量子鍵配送は航空機の位置情報など、航空の安全のために重要なデータにおける新しいセキュリティ対策の一つとして有用と考えています。