JSASS-2012-4303

2S07　量子鍵配送システムの実用化検討

○佐藤洋平，知識柔一，志賀基英，植田泰士，有川善久，花田達也，山川史郎（宇宙航空研究開発機構）

Feasibility study of practical quantum key distribution system

Yohei Satoh, Yoshikazu Chishiki, Motohide Shiga, Yasushi Ueda, Yoshihisa Arikawa, Tatsuya Hanada and Shiro Yamakawa (JAXA)

Key Words: Quantum key distribution, QKD, Feasibility study

Abstract

Quantum keys distribution can realize cryptographic communication with unconditional security. The keys are provided by a quantum communication link which can detect eavesdropping using the principle of quantum mechanics. A satellite based free space optical communication link is the only way to distribute the keys globally, since an optical fiber cannot be used for hundreds kilometer distance because of its internal optical loss, at the moment. This paper shows the result of feasibility study for the satellite-based link system.

1.　背景

現代社会には様々な情報システムが普及しており、その通信の安全性は、暗号通信技術に立脚をしている。この情報化社会の健全な維持・発展のためには、信頼性のある暗号技術の発展が不可欠であり、将来、新しい暗号方式に需要が発生する可能性は高いといえる。

次世代暗号技術の最有力候補の１つに、量子暗号技術がある。従来の暗号技術が解読されまいとする技術であるのに対し、量子暗号技術は盗聴を確実に検知する技術である。この特色により、量子暗号技術は様々な通信傍受の脅威に対し有効と言われている。

これを普及させるためには、衛星を用いた「量子鍵配送システム」が必要であり、ESA(SpaceQUEST)・中国・カナダのチームなどが実証計画を発表している。筆者らも実証実験に向けた検討を開始しており、本発表では、この実現に向けたこれまでの検討状況及び今後の研究計画について報告する。

2.　量子鍵配送システムとは

量子鍵配送システムとは、秘密が保障された安全な暗号鍵（量子鍵）を各通信者へ配送することができるシステムである。このシステムには、量子力学の原理を用いて確実に盗聴を検知できる回線（量子回線）が用いられる（図１）。

ただし、量子回線は盗聴を防ぐ事が出来るわけではない。そこで、まず送信者は無意味なランダムデータを送り、盗聴が検知されずに相手に届いたことを確認したうえで、これを共通鍵として送りたいデータを暗号化して古典回線を用いて送信する。これが、量子暗号通信である。

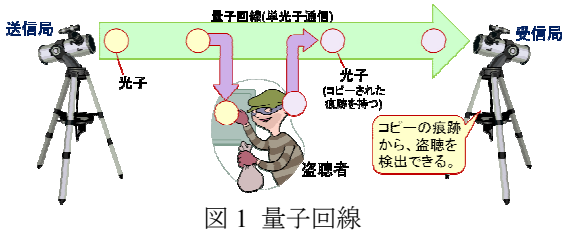

図 1　量子回線

3.　衛星利用の優位性

量子回線の代表的な方式として、光子１つに情報を1～2bit搭載する単光子通信が盛んに研究されている。これは光通信の一種である。しかし、あらゆる光子への相互作用は盗聴によるものと区別できない影響を発生させるため、光増幅など光ファイバー通信網の中継手段は全て量子回線には適用できない。このため、光ファイバーを用いた量子鍵配送の伝送距離は、その減衰の影響により数百 km 程度が限度である。しかしながら、光ファイバー中の伝搬損失の低減は 1980 年代中ごろには理論限界（SiO_2 分子のレイリー散乱による減衰のみの値）に極めて接近してしまっており、これ以上の大幅な低減は考え難い状況である（図 2）。

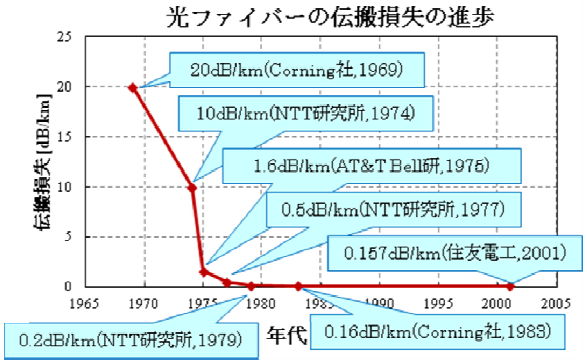

図 2 光ファイバーの伝搬損失の進歩 [1)]

一方で、自由空間伝送はファイバーより長距離で量子鍵配送が可能と言われている [2)3)]。図 3 は、ファイバー中の損失と自由空間損失を比較したものである。ファイバー中の損失は 0.20dB/km で、自由空間伝送は OICETS[4)]と同じ条件（送信側光アンテナ径 : ϕ27cm、受信側の光アンテナ径 : ϕ1.5m、波長 : 855nm）にて計算している。前者は距離の指数関数に比例、後者は距離の二乗に比例するため、特に長距離領域で自由空間伝送が有利となる。このため、ファイバーでは量子鍵配送が実現できない距離でも、自由空間伝送ならばこれを実現できる。これに人工衛星の軌道運動を組合せる事で、量子鍵配送システムの全地球規模での展開が可能となる。

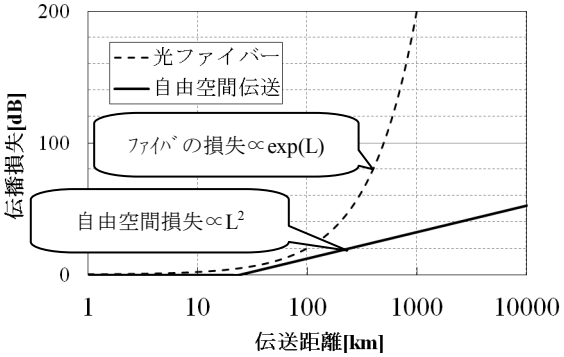

図 3 伝送損失の比較

以上より、人工衛星は全地球規模で量子鍵配送システムを実現する唯一の手段といえる。

4. ミッション検討

4.1 量子鍵配送の問題点と解決策

量子鍵配送の問題点としては、下記が存在する。

① 伝送速度

伝送速度が数 bps～数百 kbps と低速である。量子鍵を用いたワンタイムパッド通信では、通信速度がこれと同一となるため、現状の通信網の通信速度と比較して、大きな制限を受けることとなる。

② 通信可能時間

衛星からの量子鍵配送のためには、衛星可視・晴天・夜間の 3 条件が揃う必要がある。これでは数日に 1 度、夜に 10 分程度のみ暗号通信可能といった通信可能時間となるため、そのままでは実用に耐えない。

③ ユーザー負荷

量子暗号通信を実施するエンドユーザは、全て光アンテナや衛星追尾装置を持たなければならず、これが大きなユーザ負荷として想定される。

①の解決策として、筆者らは乱数拡張方式を用いた高速通信方式を検討している。これにより、現実的な量子鍵の情報量で実用的な安全性と通信速度を実現可能である。ワンタイムパッド通信により実現可能な無条件安全性と現実的な通信速度、どちらをとるかは今後の検討課題である。②については、地上局側に量子鍵データを蓄積し、必要に応じて使用していくことで解決できる。③については、光ファイバーを用いた近距離の量子鍵配送を活用して解決することを考えている。具体的には、地域毎に地上局と量子鍵を受信・保管しておくサーバ（量子鍵サーバ）を設置し、各エンドユーザは何らかのサーバ・クライアント型の通信方式で量子鍵サーバに接続することで、近距離量子暗号通信にて量子鍵を取得する方法である。この地上ファイバー網との連携イメージを図 4 に示す。

図 4 地上ファイバー網との連携

これらの工夫により、量子鍵配送の実用性について大幅に改善する事が出来る見込みを得た。

5. システム検討

下記を前提としたシステムを検討する。

①量子鍵サーバ数は国内だけで約 3000 局

この仮定は、電話局の様な地域の通信網の拠点に、それぞれ 1 台の量子鍵サーバを配置するという想定に基づく。

参考文献 5)によれば、NTT 東西の交換機収容局数は全国で約 5000 局である。ただし、都市部では複数の電話局が近接 (東京 23 区内だけで 144 局存在) しているため、目標とする国内の量子鍵サーバ数は、仮に 3000 局とする。

②量子鍵データベースの更新周期は 3 ヶ月

量子鍵サーバも攻撃対象となる可能性があるため、その内部のデータベースも漏洩リスクを考慮して定期的に更新するものとする。

③各地上局に配布される量子鍵は 3000 セット

量子鍵サーバ数と同じ量子鍵数が必要である。

④量子鍵 1 セットのデータ量は 256bit

AES256 暗号(共通鍵長:256bit)の危殆化時期は 2213 年頃と予想されており [6]、乱数拡張方式の種の長さとしては十分安全ということが出来る。よって、量子鍵のデータ量としては、この値を想定する。

⑤１晩の有効可視時間は 5 分(300s)程度

⑥衛星の可視条件は、国内中で毎晩１回存在

仮定①②より、１晩に量子鍵を配送する量子鍵サーバ数は約 30 である。また、仮定③④から、各量子鍵サーバに１回で伝送しなければならない量子鍵データ容量は、96kByte である。つまり、１晩で合計 3.2MByte の量子鍵データを配送しなければならない。以上と仮定⑤⑥から、必要な配送速度は約 85kbps である。有効な回線成立率(晴天率)を３割と仮定すれば、280kbps が必要な量子鍵配送速度があれば、本ミッションは成立し得るといえる。これは、現状の量子鍵配送研究(伝送路の損失が 20dB の条件時に 100kbps[7])と比較しても、実現性のある目標と言える。

また、昼間の屋外で量子鍵配送に成功した例 [8]も存在しており、宇宙空間からの量子鍵配送をする上で問題となる迷光についても、これら成果の活用で解決可能と考えられる。尚、仮定⑥については、軌道シミュレーションソフトにて、低軌道傾斜角の衛星３基を想定すれば実現性があることを確認している。

6. まとめ

将来の宇宙利用ミッションとして、量子鍵配送システムへの衛星利用は有望である。

乱数拡張やサーバ・クライアント方式などの手法を導入することで、このシステムの実用性を大幅に向上する見込みを得た。また、簡易的なシステム検討を実施し、その実現性に目処を得ることができた。

今後、情報通信研究機構(NICT)の専門家と解決すべき技術課題を整理し、地上実証実験およびフライト実証実験の目的を詳細化する。また、多数研究されている量子鍵配送方式の中から本実証計画に最適な方式を選定し、実証実験の準備およびフライト実証システムの検討を開始する予定である。現在までに、量子鍵配送の研究を実施している NICT と協力関係構築に向け調整を開始している。

加えて、ポテンシャルユーザの発掘と要求調査を行い、その要求分析を実施する。

参考文献

1) 光関係（情報通信）研究開発プロジェクト追加評価報告書（平成 15 年８月)、産業構造審議会・産業技術分科会・評価小委員会・光関係（情報通信）研究開発プロジェクト追跡評価 WG
2) Long-Distance Quantum Communication With Entangled Photons Using Satellites, Markus Aspelmeyer, IEEE JOURNAL OF SELECTED TOPICS IN QUANTUM ELECTRONICS, VOL. 9, NO. 6, NOVEMBER/DECEMBER 2003, 1541
3) Feasibility of free space quantum key distribution with coherent polarization states, D Elser et al 2009 New J. Phys. 11 045014 doi:10.1088/1367-2630/11/4/045014
4) 光衛星間通信実験衛星「きらり」(OICETS) http://www.jaxa.jp/projects/sat/oicets/index_j.html
5) 総務省, DSL コロケーション情報 http://warp.ndl.go.jp/info:ndljp/pid/258151/www.soumu.go.jp/joho_tsusin/whatsnew/dsl/index.html
6) 暗号等価安全性, 富士通研究所ソフトウェアシステム研究所　森川邦也、下山武司、電子情報通信学会誌　平成 23 年 11 月 Vol.94
7) Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate, A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields. Optics Express, Vol. 16, Issue 23, pp. 18790-18979
8) Feasibility of free space quantum key distribution with coherent polarization states, D Elser, New Journal of Physics 11(2009)045014