空間伝送用量子暗号通信システムの地上伝送実験

情報通信研究機構　豊嶋守生、竹中秀樹、高山佳久、國森裕生、武岡正裕、藤原幹生、佐々木雅英

Field quantum key distribution experiments by using a bread board model for free-space quantum cryptography

Morio Toyoshima, Hideki Takenaka, Yoshihisa Takayama, Hiroo Kunimori, Masahiro Takeoka, Mikio Fujiwara, and Masahide Sasaki
National Institute of Information and Communications Technology (NICT),
4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795
E-Mail: morio@nict.go.jp

Abstract: A free-space quantum key distribution system is being developed by the National Institute of Information and Communications Technology (NICT) in Koganei, Japan. Quantum cryptography is a new technique for transmitting information where the security is guaranteed by the laws of physics. In such systems, a single photon is used for the quantum information; however, since the transmission distance in optical fibers is limited by the absorption of photons by the fiber, the maximum demonstrated range has been about 100 km. Free-space quantum cryptography between an optical ground station and a satellite is a possible solution to extend the distance for a quantum network further beyond the limits of optical fibers. At NICT, a laser communication demonstration between the NICT optical ground station and a low earth orbit satellite was successfully conducted in 2006. For such space communication links, free-space quantum cryptography is considered an important application for the future. A bread board model for free-space quantum cryptography using a free-space polarization tracking scheme has been developed by NICT, and the preliminary test results for the quantum key distribution with the polarization tracking between two buildings in NICT are presented.

Key words; Space Utilization, International Space Station, Quantum Cryptography, Quantum Key Distribution, Free Space Laser Communication, Polarization tracking

１．はじめに

近年、大災害や事故の多発、世界的な感染症の流行、テロの頻発や国内の治安の悪化など、社会の安全･安心を脅かす危険や脅威が顕在化し始めている。科学技術は、社会的な価値を創出していく手段であり、知的な価値の創出、産業的な価値の創出と並んで、これらの危険や脅威に対処し社会の安全・安心を確保する要請に応えるもので、近年特に重要となっていきている。情報通信技術では、情報漏えいや不正アクセスなどを防止する情報セキュリティ技術の要請が高まっており、盗聴技術が高度化する中で暗号技術は益々重要になってきている。

光や電子の量子効果を直接制御することで従来にはない革新的な性能を実現する量子情報通信技術が近年注目されている。盗聴を完全に見破る量子暗号[1]や、量子もつれ現象を使った遠距離での量子テレポーテーション[2]、従来の通信容量のシャノン限界を超える符号化技術[3]等、新しい原理が実証され、実用化に向けた研究が加速している。既にファイバベースの商用では、実際の量子暗号装置として、スイス Id Quantique 社製品の Cerberis,Vectis および Clavis、米国 MagiQ Technologies 社製品の MAGIQ QPN SECURITY GATEWAY 7505、フランス SmartQuantum 社製品の SQBox などのベンチャー企業数社から販売されるに至っている[4-6]。

我が国では、第３期科学技術基本計画における情報通信分野の重要な研究開発課題の１つとして、「2030 年までに、情報通信の大容量化と高秘匿性を確保する量子通信技術を実現する」ことを研究開発目標としている。情報セキュリティの重要性については、同基本計画の中で、「世界一安全な国・日本を実現する」ということが述べられており、量子暗号はその実現に貢献するものである。絶対安全性を保証する量子暗号は、インターネット等で既に普及している公開カギ暗号技術が新たな計算アルゴリズムや量子コンピュータの台頭で無効になった場合、代替手段として有望視されており、近い将来、社会的に実用領域で期待されている技術である。

量子暗号通信は、現状、光ファイバでは 100km 程度の距離の伝送が限界であり、それより遠距離になると、受信器の雑音やファイバ中の散乱光の雑音、また偏光を用いる場合には非線形性等の影響により、中継なしにそれ以上遠方へ送ることができない[1]。しかし、自由空間においては空間的な損失はあるが、非線形要因がないため遠方への伝送には理想的な媒体である。これが宇宙において量子暗号が期待される所以である。

情報通信研究機構（NICT）では、欧州宇宙機関（ESA）で検討されている宇宙量子鍵配布実験への参画を目的とした共同研究や、日本独自の宇宙量子暗号通信ミッション立ち上げに向けた検討を開始した。宇宙航空研究開発機構（JAXA）宇宙環境利

用科学委員会研究班ワーキンググループ活動でも、2006 年度より本研究に関する活動を実施している。本稿では、NICT における空間伝送用の量子鍵配布地上モデルの研究開発を行い、地上伝送実験を行ったので報告する。

２．量子暗号システムの地上モデル

２．１　概要

情報通信研究機構（NICT）では、日本独自の宇宙量子暗号通信ミッションを立ち上げていくことを目指して、基礎検討を開始した。具体的には、宇宙量子暗号通信の概念検討作業、試作試験用プロトタイプモデル製作、宇宙環境への適応性評価など、量子暗号通信機器の実現性の見極めと、量子通信技術の衛星搭載化に向けた検討を行っている。これらの研究開発により、宇宙量子暗号通信のグローバル量子ネットワーク実験の国際連携プロジェクトの立ち上げや、日本独自の搭載ミッション提案につなげていきたいと考えている。

NICT における宇宙量子通信の研究開始にあたり、空間伝送を行う地上用量子鍵配布送システムの試作試験用モデル（BBM）を構築する独自研究を開始した。微弱コヒーレント光の送受信技術を用いて、空間伝送による量子暗号の実現性を検討するものである。基本素子調達を開始し、まずは光学ベンチ上で量子暗号システムの BBM を試験し、今回はビル間での量子鍵配布実験を実施した。

２．２　方式と構成

量子暗号システムの地上 BBM モデルは、微弱コヒーレント光で B92 プロトコルを用いる方式を採用した[4]。図 1 に開発した量子暗号システムの送信部（Alice）を、図 2 に受信部（Bob）の構成を示す。暗号用のレーザは 0.8μm帯、通信信号用のレーザは 1.5μm帯を用いており、単一光子検出には通信用レーザの信号を時刻検出に用いている。信号処理回路は Field Programmable Gate Array（FPGA）により構成されており、送信部では GPS クロックの同期、通信信号の生成、パルス発生器への信号生成、ランダム信号列の生成、偏光変調器の変調信号の生成、各信号の記録を行う。受信部では、GPS クロックの同期、通信信号のデータ・クロック再生、単一光子光受信機へのゲートパルス生成、ランダム信号列の生成、偏光変調器の変調信号の生成及び、各信号の記録を行う。

また、重要な機能として、移動体間では空間での伝搬遅延時間の変化や、偏光方向の追尾が問題となる。例えば、衛星では時々刻々と衛星との距離が変化し、相対的に送受信機が回転する。また、追尾系のミラー等の反射光学系が可動する場合には、入射する見かけの像が回転するなどの補正が必要となる。本プロトタイプモデルでは、FPGA により 1.5μm の参照信号を用いて、カウンタにより伝搬遅延時間を算出できるようにして、送信と受信で量子暗号用のビットを同期している。また、相手の送信機の偏光方向が判別できるように波長板を用いた偏光追尾装置を備えている。

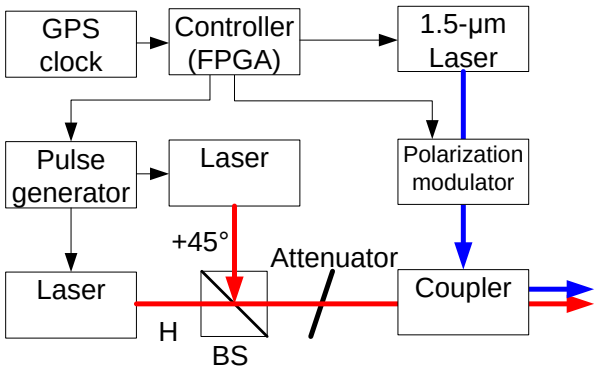

Fig. 1. Configuration of transmitter (Alice).

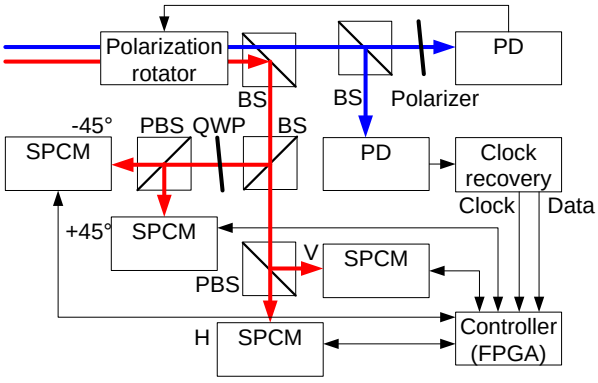

Fig. 2. Configuration of receiver (Bob).

３．実験結果

図 3 に、フィールドでの量子鍵配布実験をビル間で行った様子を示す。空間の伝送距離は 75m 程度の伝搬路である。また、図 4 に送信した偏光基底と受信した偏光基底の相関を示す。送信した偏光基底は、受信部では同じ偏光基底で受信しないと全くランダムな結果となるため、偏光基底を同じものに合わせる必要がある。このとき量子誤り率（QBER）は 0.9%で、平均光子数はμ = 0.11 フォトン/パルスであった。ビット誤りがあるので、BBBSS プロトコル[7]によりパリティチェックを行い、誤り訂正を行った後の相関を図 5 に示す。シフトキーレートでは、98 kbps の伝送が可能であることが分かった。秘匿性増強は今回行っていないが、最終鍵レートに換算すると、43.8 kbps の伝送が可能である。表 1 に実験結果をまとめた。

図 6 に、本実験における性能の位置づけと、長距離化について示した。現状ではバックグランドノイズの改善なしには、100km 以上伝送できない。今後さらに、バックグランドノイズとパルスのクロックレートを上げた場合の性能改善を図 7 に示す。これにより、地上ー低軌道衛星間の距離で量子鍵配布が可能となることが分かる。

今後は、フィールドでの量子鍵配布実験の距離を延ばして、NICT 敷地内と敷地外のターゲットとの間で空間伝搬させて行う予定であり、自由空間における実環境での動作確認実験を行い、大気ゆらぎの

影響などを評価したいと考えている。

また、図 8 に本システムで実装した偏光方向の追尾特性を示す。設定した角度に 0.2deg(rms)で追尾させることができた。今後は、移動体間で必須な空間偏光方向追尾の機能も、性能を向上して実験する予定である。

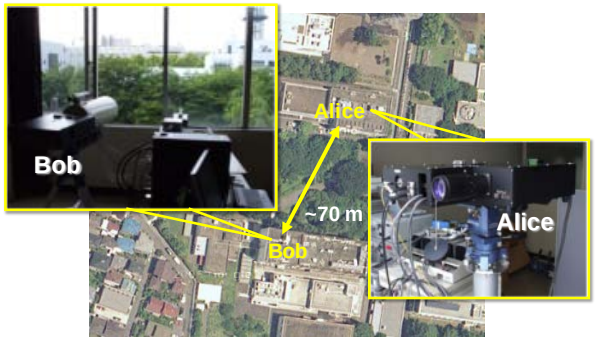

Fig. 3. Photographs of the field QKD experiments in the NICT facility.

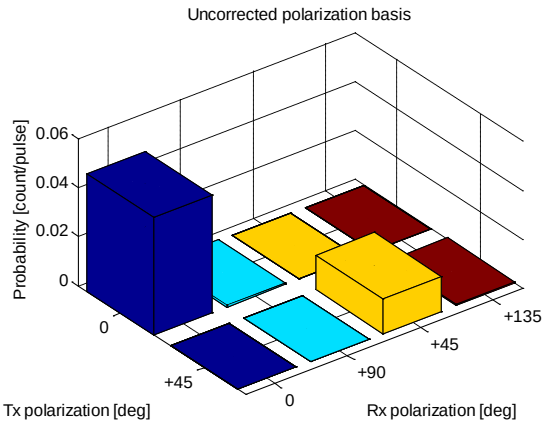

Fig. 4. Correlation of detected photons without the corrected polarization basis between transmitter and receiver.

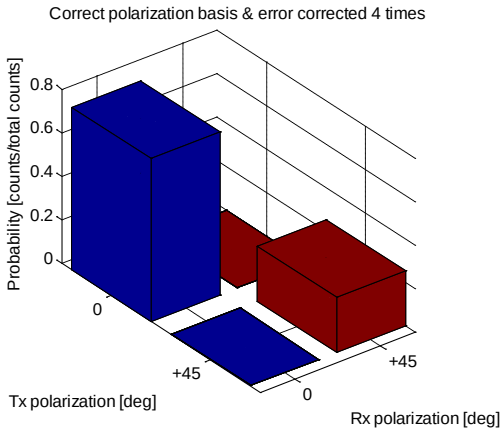

Fig. 5. Correlation of detected photons with error correction between transmitter and receiver.

Table 1. Parameters for the QKD system.

Protocol	B92
Clock rate	20 MHz
Mean photon number	0.11 photons/pulse
Dark count rate	4.90E-4
QBER	0.90%
Sift key rate	98.1 kbps
Final key rate	43.8 kbps (estimated)
Distance	70 m

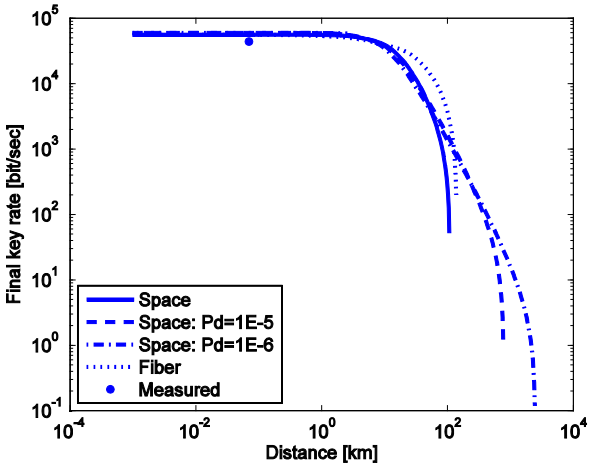

Fig. 6. Final key rates for free-space and fiber-based transmission systems as a function of the dark count rate. Pd stands for the dark count rate. The dot “Measured” shows the experimental result of the BBM model.

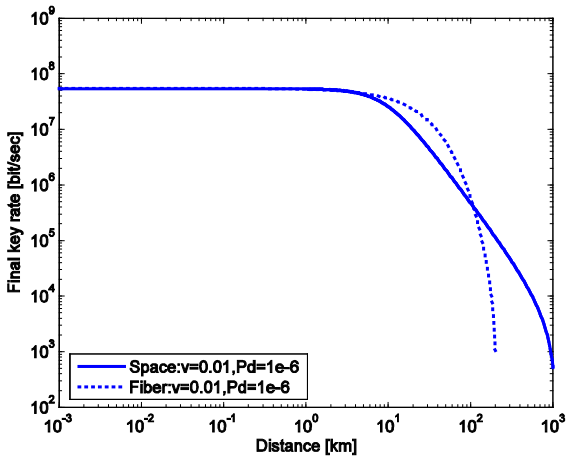

Fig. 7. Final key rates for free-space and fiber-based transmission systems as a function of the distance with a clock rate of 2.5 GHz, dark count rate of 1e–6 and imperfection of 0.01

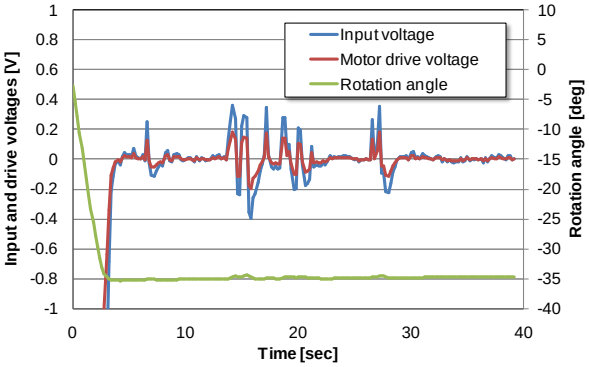

Fig. 8. Rotation angle of the halfwave plate mounted on the mechanical rotator at -35 deg and the input and output drive voltages of the motor control signals.

４．ロードマップ

図 9 に、現在検討中である宇宙量子暗号ミッションを実現させるための宇宙量子通信のロードマップを示す。宇宙機搭載へのはじめのステップとしては、ファイバでは商用としても市販品が出回ってきている量子暗号を宇宙ミッションとすることであろう。宇宙搭載性については、部品選定等を考慮する必要があるが、技術的には実用段階にある。図のロードマップでは、5～10 年後の打ち上げにより宇宙実証を目指した量子鍵配布ミッションを示している。一方、NICT ではシャノン限界を越える量子符号化の実証実験が行われており[3]、その様な超高感度な量子通信機器は、深宇宙通信におけるアプリケーションとして、またオリジナリティある国産開発技術として魅力的で、将来への衛星通信におけるパラダイムシフトにつながる可能性がある。しかしながら、こちらはここ 5 年程度のスパンでは、まだ実現は難しい技術である。

５．まとめ

NICT における宇宙量子暗号通信の研究開発及び量子鍵配布の地上伝送実験について述べた。現段階では、検討を開始したばかりであり、まずは基本的な技術を把握することからであると考えている。BBM モデルにより、原理的には移動体間で量子鍵配布が問題なく可能である見通しを得ている。しかしながら、鍵の伝送速度については安全性が保証されている現方式では速度的に遅く、安全性と実用性を考慮して様々な方式を検討し、今後最適な方式を採用していく必要があろう。量子暗号は誰でも享受できる、安心・安全な情報セキュリティ技術の究極の最終形態であり、情報通信において今後益々欠かせない存在になってくると考えられる。

参考文献

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, ”Quantum Cryptography,” Rev. Mod. Phys., 74, 145–195 (2002).
[2] “The Physics of Quantum Information,” Eds. D. Bouwmeester, A. Ekert, A. Zeilinger, (Springer, New York, 2000)
[3] M. Fujiwara, M. Takeoka, J. Mizuno, and M. Sasaki, “Exceeding classical capacity limit in quantum optical channel,” Phys. Rev. Lett., 90(16), 167906 (2003).
[4] http://www.optoscience.com/pdf/id/id200.pdf
[5] http://www.magiqtech.com/
[6]http://www.smartquantum.com/SQBox-defender.html
[7] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental Quantum Cryptography,” J. Cryptology 5, 3-28 (1992).

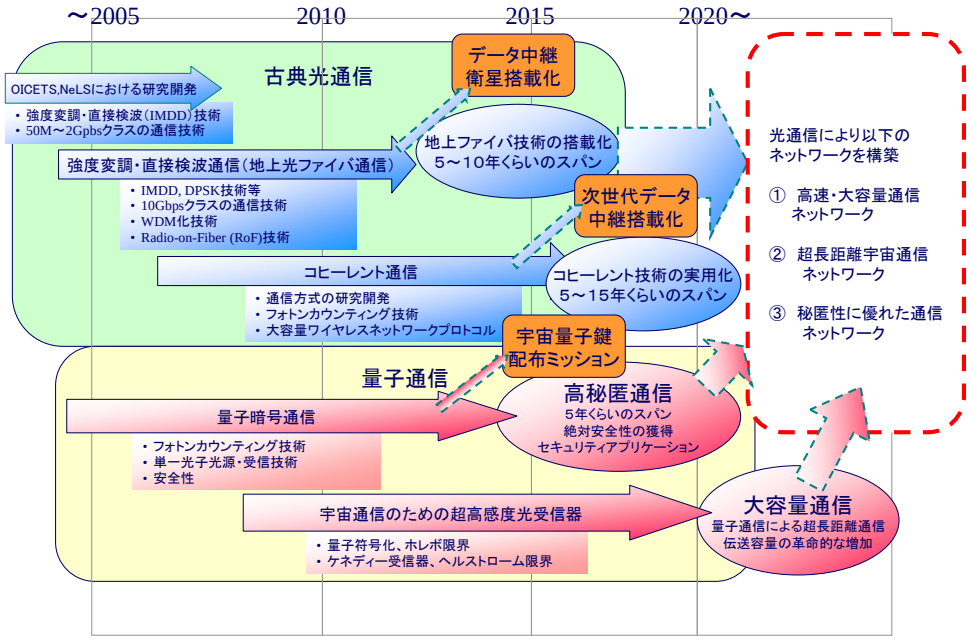

Fig. 9. R&D roadmap for space laser communications