

空間伝送用量子暗号通信システムの試作試験モデルの開発

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

Development of a bread board model for free-space quantum cryptography

Morio Toyoshima, 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: Quantum cryptography is a new technique for the transmission of information whose security is guaranteed by the laws of physics. In such systems, the vehicle to transfer quantum information is a single photon, however, the transmission distance is limited by the absorption of photons in an optical fiber in which the maximum demonstrated range is about 100 km. Free-space quantum cryptography between a ground station and a satellite will be a possible solution to send the quantum information beyond further distances than that with optical fibers since there is no birefringence effect in the atmosphere. At the National Institute of Information and Communications Technology (NICT), the 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, the free-space quantum cryptography is considered to be an important application in the future. A prototype system for free-space quantum cryptography using weak coherent pulse sources and a telecom communication channel is developed. The preliminary results are presented.

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

１．はじめに

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について報告する。

２．宇宙量子鍵配布研究の状況

２．１　米国の状況

量子暗号は 1984 年に Bennett と Brassard により 30cm の空間での量子鍵配信実験が行われて以来[7]、盛んに研究が行われてきた。米国 Los Alamos National Laboratory では、10km の伝送距離を夜だけでなく、昼間にも伝送することに成功している[8]。近年の衛星におけるレーザ通信の成功[9-11]もあり、宇宙における衛星通信に応用する検討も行われている[12]。

２．２　欧州の現状

ドイツ Ludwig-Maximilian University の Weinfurter らのグループによる微弱光を用いたビル間や山頂間で 23km の長距離空間伝送の量子鍵配布実験が行われている[13]。また、安全性を高めるデコイ方式を用いて、スペインのカナリア諸島で島を隔てた 144km の量子鍵配布実験も成功裏に実施されている[14]。

ウイーン大学の Zeilinger 教授のグループらは量子通信を国際宇宙ステーション（ISS）のコロンバスモジュールに搭載し、宇宙空間で実証することを提案している[15-18]。このプロジェクトは、Space-QUEST と呼ばれており、ELIPS2(the European programme for Life and Physical Sciences and applications utilizing the ISS)という ESA の ISS 搭載ミッション選定では、基礎物理分野で評判がよく、2013 年頃に打ち上げを計画している[19,20]。ウイーン大学のグループは、2005 年秋にはテネリフェ島における 144km の量子もつれの伝送に成功しており、宇宙実証の実現性はさらに高まったといえる[21]。現段階では、Space-QUEST は概念検討レベルであり、基本設計に入るため準備が行われているようである。

２．３　中国

中国では中国科学技術大学の潘建偉教授が、2004 年に地上伝搬において 13km の距離で量子もつれによる光子対の伝送に成功しており[22]、それに続いて 2008 年打上げ予定の有人宇宙船「神舟７号」に量子通信の実験装置を搭載し、数百 km の距離での量子通信実験を行うことを計画しているようである。最近では、量子通信専用の単独ミッションの衛星で実証する動きもあるようである[23]。

２．４　日本

NICT では、日本独自の宇宙量子通信プロジェクトを立ち上げていくことを目指して、基礎検討を開始した。これは、３年間の予定で量子通信技術の衛星搭載化に向けた検討を行う。研究内容は、宇宙量子通信の概念検討作業、試作試験用モデル（BBM）製作作業、宇宙環境への適応性評価などについて行う。基本素子調達・評価も含めた検討を行い、BBM 製作は、量子通信機器の実現性を見極めるために行う。上記研究開発により、宇宙量子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貢献できればと考えている。本稿では、この BBM 構築について報告する。

３．地上局を用いたグローバル量子鍵配信実験

３．１　任意の２つの地上局を用いた量子鍵配信

任意の２つの地上局を用いた量子鍵配信・共有実験は、以下の手順で地球規模で実現可能である。

１）　衛星から量子鍵 α を量子もつれにより生成・配信し、地上局 A で量子鍵 α を保存する。

２）　地上局 B の上空で、衛星から量子鍵 β を生成・配信し、地上局 B で量子鍵 β を保存する。

３）　衛星では量子鍵 $\gamma = \alpha$ XOR β を算出し通常の通信回線で両ユーザに配信する。（XOR は排他的論理輪で、γ は盗聴されてもよい）

４）　それぞれの地上局で自分の量子鍵と γ を XOR することで相手の量子鍵を共有できる。

任意の２つの地上局を用いた量子鍵配信・共有実験は、例えば、ヨーロッパで量子鍵を衛星に送信し、地球の反対側の日本で下ろすことによりグローバルな量子鍵配信が可能となる。ファイバでは現状実現できない長距離伝送が可能である宇宙量子暗号通信において、地球規模で量子鍵配布が可能であるということは、将来の応用へ重要な意味を持つと考えられる。

３．２　光地上局

NICT の光地上局は、2006 年 3 月から 9 月にかけて光衛星間通信実験衛星（OICETS）を用いて、世界初の地上―低軌道衛星間の光通信実験に成功している[11]。低軌道衛星は、見かけの移動角速度が速いため望遠鏡の高い追尾能力が要求される。ISS 等の低軌道衛星と、NICT 光地上局との光通信の実現性については十分な実績があるといえる。例えば、量子鍵配布システムのための送信部と受信部と開発し、この光地上局に送信または受信系を設置して、他方を宇宙器として衛星等に搭載し、量子鍵配布実験を行うことが考えられる。

４．量子暗号システムの地上 BBM モデル

４．１　概要

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 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、基本的な機能を確認した。

４．２　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 BB84 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。

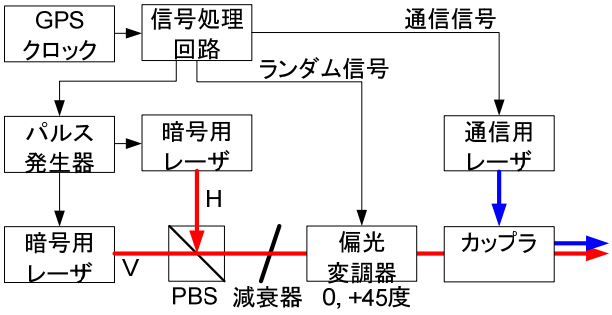

図 1. 量子鍵配布システムの送信部（Alice）の構成

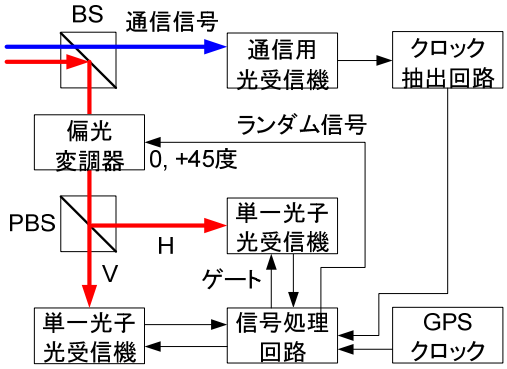

図 2. 量子鍵配布システムの受信部（Bob）の構成

４．３ 実験結果

図 3 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 QBER は 5.5%で、μ = 0.094 あった。このとき、ビット誤りがあるので、BBBSS プロトコル[24]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 4 に示す。シフトキーレートでは、44kbps の伝送が可能であることが分かった。ハッシングによる秘匿性増強などは今回行っていないが、最終鍵レートに換算すると、8.13 kbps の伝送が可能である。

しかしながら、伝送距離は実験室レベルの 4 枚のミラーを通った 3.4m の空間伝送であり、フィールドでの伝搬実験までは至っておらず、今後、NICT 敷地内の鉄塔と光地上局望遠鏡との間で数百 m を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、移動体間で問題になる空間偏光方向追尾の機能も、次のモデルでは搭載していく予定である。

５．ロードマップ

現在、宇宙量子暗号ミッションを宇宙機で実現させるためのロードマップを検討中である。NICT では光波量子・ミリ波 ICT グループで実証実験を行ったシャノンリミットを越える感度を持つ量子通信機器[3]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ある。しかし、ここ 5 年程度のスパンでは実現は難しい技術である。宇宙機搭載へのはじめのステップとしては、実用段階にある量子暗号通信ミッションであろう。図 5 に、光宇宙通信の研究開発ロードマップを示す。現在、5～10 年後の打ち上げを目指して、量子暗号通信ミッションを宇宙実証できるようなロードマップを総務省と共に検討中である。

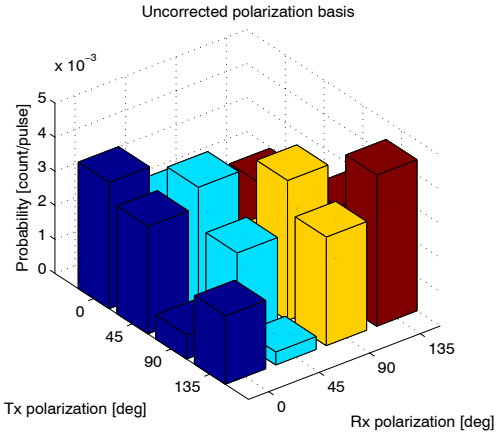

図 3. 送信した偏光基底と受信した偏光基底の相関

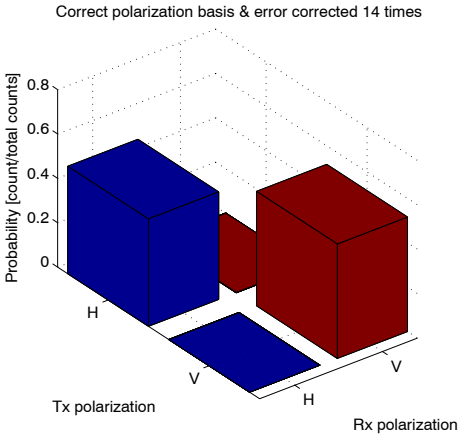

図 4. 誤り訂正を行った後の送信した偏光基底と受信した偏光基底の相関

６．まとめ

NICT における宇宙量子暗号通信の研究開発について現状の活動状況を述べた。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。量子もつれを用いた量子暗号については、ESA のプロジェクトに連携して進めていくシナリオである。一方、日本独自の量子暗号ミッションについては、プロトコルにこだわらず最適なシステムを検討していきたいと考えている。

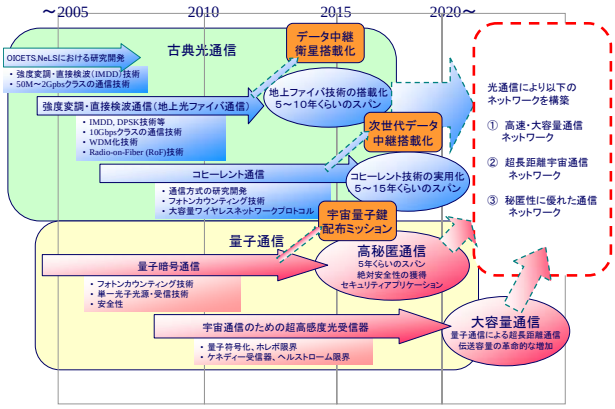

図 5.　光宇宙通信の研究開発ロードマップ

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 and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” in Proceedings of International Conference on Computers, Systems & Signal Processing, Bangalore, India, (1984).

[8] R.J.Hughes, J.E.Nordholt, D.Derkacs, and C.G.Peterson, “Practical free-space quantum key distribution over 10 km in daylight and at night,” New J.Phys. 4, 43.1-43.14 (2002).

[9] K. E. Wilson, J. R. Lesh, K. Araki, and Y. Arimoto, "Overview of the Ground-to-Orbit Lasercom Demonstration," Space Communications, Vol. 15, pp. 89–95, 1998.

[10] T. T. Nielsen, G. Oppenhaeuser, B. Laurent, and G. Planche, "In-orbit test results of the optical intersatellite link, SILEX. A milestone in satellite communication," in Proceedings of the 53rd International Astronautical Congress (IAC-02-M.2.01, Houston, Oct. 2002) pp. 1–11.

[11] M. Toyoshima, K. Takizawa, T. Kuri, W. Klaus , M. Toyoda, H. Kunimori, T. Jono, Y. Takayama, K. Arai, "Development of the optical ground station for the OICETS satellite and experimental results," 57th International Astronautical Congress, IAC-06-B.3.04, pp. 1-11, Valencia, Spain, October 5 (2006).

[12] R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. K. Lamoreaux, G. L. Mokgarn J. E. Nordholt, and C. G. Peterson, “Quantum Cryptography For Secure Satellite Communications,” IEEE (2000).

[13] C.Kurtsiefer, P.Zarda, M.Halder, H.Weinfurter, P.M.Gorman, P.R.Tapster, and J.G.Rarity, “A step towards global key distribution,” Nature 419, 450 (2002)

[14] T. Schmitt-Manderbach, H. Weier, M. Furst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, “Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144km,” Phys.Rev.Lett., 98, 010504 (2007).

[15] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger, “Long-distance quantum communication with entangled photons using satellites,” IEEE Journal of Selected Topics in Quantum Electronics, 9(6), 1541–1551 (2003).

[16] R. Kaltenbaek, M. Aspelmeyer, T. Jennewein, C. Brukner, A. Zeilinger, M. Pfennigbauer and W. R. Leeb, “Proof-of-Concept Experiments for Quantum Physics in Space,” Phys. Rev. A, 67, 022309 (2003).

[17] M. Pfennigbauer, W. R. Leeb, “Quantum Communications in Space (QSpace),” Final Report within ESA/ESTEC/Contract No. 16358/02/NL/SFe (2003).

[18] M. Pfennigbauer, M. Aspelmeyer, W. R. Leeb, G. Baister, T. Dreischer, T. Jennewein, G. Neckamm, J. M. Perdigues, H. Weinfurter, and A. Zeilinger, "Satellite-based quantum communication terminal employing state-of-the-art technology," Journal of Optical Networking, 4, 549–560 (2005).

[19] http://www.spaceflight.esa.int/users/index.cfm?act=default.page&level=16&page=453

[20] http://www.quantum.at/typo/fileadmin/PDF/Space_Brochure.pdf

[21] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, A. Zeilinger, "Free-Space distribution of entanglement and single photons over 144 km," Quantum Physics, quant-ph/0607182 (2006).

[22] C.-Z. Peng, T.Yang, X.-H.Bao, J.-Z, X.-M. Jin, F.-Y. Feng, B.Yang, J. Yang, J.Yin, Q. Zhang, N.Li, B.-L. Tian, and J.-W. Pan, “Experimental free-space distribution of entangled photon pairs over a noisy ground atmosphere of 13 km,” Phys. Rev. Lett. 94, 150501 (2005), quant-ph/0412218 (2004)

[23] 辻野照久、“通信放送衛星システムの利用動向”、科学技術政策研究所、科学技術動向研究センター、科学技術動向 10 月号 http://www.nistep.go.jp/achiev/ftx/jpn/stfc/stt067j/0610_03_featurearticles/0610fa03/200610_fa03.html

[24] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental Quantum Cryptography,” J. Cryptology 5, 3-28 (1992).