宇宙量子暗号通信の動向

豊　嶋　守　生

Trends of Quantum Cryptography in Space

Morio TOYOSHIMA

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. The European Space Agency (ESA) plans to demonstrate a quantum key distribution experiment onboard the ESA's Columbus module onboard the International Space Station (ISS) called Space-Quest. The purpose of this report is to introduce the trends of the quantum key distribution using satellites.

Key words: quantum key distribution, free-space laser communication, satellite communication

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はじめている．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ー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ますます重要になってきている．すでにファイバーベースの商用では，実際の量子暗号装置として，スイス Id Quantique 社，米国 MagiQ Technologies 社，フランス Smart Quantum 社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．2007年10月に行われたスイス ジュネーブ市の選挙において，インターネット投票ですでに量子暗号が採用されている[1]．無条件安全性を保証する量子暗号は，インターネット等ですで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ー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．

しかしながら，量子暗号通信は，光ファイバーでは 100 km 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ー中の散乱光の雑音，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[2]．しかし，自由空間においては空間的な回折による損失はあるが，ファイバー伝送より遠方へ伝送可能であり，これが宇宙において量子暗号が期待されるゆえんである．ヨーロッパでは，国際宇宙ステーション（ISS）からの量子鍵配布ミッションが提案されており，日本からもこのプロジェクトへ参画する予定である．本稿では，宇宙量子暗号通信の動向について報告する．

1.　宇宙における量子鍵配布研究の動向

1. 1　海外の状況

量子暗号は 1984 年に Bennett と Brassard により 30 cm の空間での量子鍵配信実験が行われて以来[3]，盛んに研究が行われてきた．米国 Los Alamos National Laboratory では，10 km の伝送距離を夜だけでなく，昼間にも伝送する

情報通信研究機構（〒184–8795 小金井市貫井北町 4–2–1）　E-mail: morio@nict.go.jp

ことに成功している[4]．近年の衛星におけるレーザー通信の成功[5–7]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[8]．ドイツ Ludwig-Maximilian University の Weinfurter らのグループにより，微弱光を用いたビル間や山頂間で 23 km の長距離空間伝送の量子鍵配布実験が行われている[9]．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 144 km の量子鍵配布実験も成功裏に実施されている[10]．ウィーン大学の Zeilinger 教授のグループらは，量子暗号通信機器を 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[11–13]．このプロジェクトは，章をあらためて動向を紹介する．また，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 13 km 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[14]，それに続いて衛星に量子暗号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[15]．

1.2　日本の状況

情報通信研究機構（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[7]．低軌道衛星は，見かけの移動角速度が速く望遠鏡の高精度な追尾能力が要求されるが，ISS 等の低軌道衛星も OICETS と同様な軌道高度であるので，NICT の光地上局との光通信の実現性は高いといえる．NICT では，ESA で検討されている宇宙量子鍵配布実験のプロジェクト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を立ち上げていくことを目指して，基礎検討を行っている．具体的には，宇宙量子暗号通信の概念検討，試作試験モデルの製作，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くことを考えている．

2.　ESA 量子鍵配布ミッション

2.1　概　　要

欧州宇宙機関（ESA）では，ISS 搭載ミッション選定（ELIPS2: European programme for LIfe and Physical Sciences and applications utilizing the ISS）を実施しており，ISS からの量子鍵配布ミッションは“Space-Quest”とよばれ，基礎物理分野で評判がよく，2015 年ころに打ち上げを計画している．ESA の一般研究プログラム（GSP）のファンディングにより，Quantum communications in Space

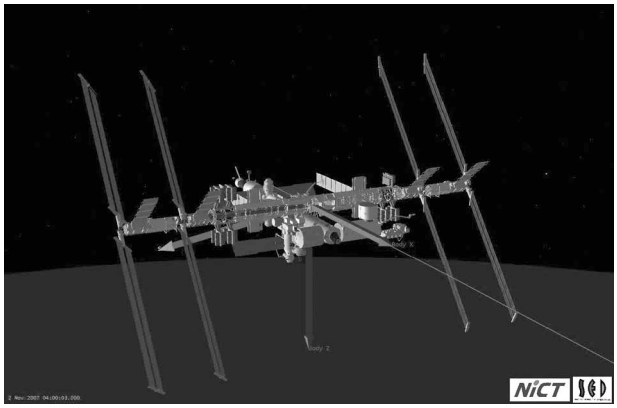

図 1　国際宇宙ステーション．

（“QSpace”）で 2002～2003 年に量子暗号ミッションの概念検討が行われ，その後，Accommodation of a quantum communication transceiver in an optical terminal（“ACCOM”）により 2004 年に実施した衛星搭載性の検討および，Quantum Information and Quantum Physics in Space（“QIPS”）として 2005～2007 年にかけて行われた Space-Quest ミッションのための量子もつれ現象の長距離実証実験（ウィーン大学のグループによる 144 km の量子もつれ伝送実験等）により実現性が示された[13]．2008 年 10 月 18 日には，14 か国 27 機関が協力して国際トピカルチームミーティングがウィーンにて開催され，NICT も正式参加し，開発フェーズ（Phase-A）へ向けて議論がなされた．この後，ESA で量子もつれ光源については開発モデルの開発が始まり，現段階では，Space-Quest は基本設計段階に入りつつある．

2.2　衛星搭載量子暗号ターミナルと光地上局

量子暗号用の衛星搭載光ターミナルは，スイスにある Oerlikon Space が設計を行っている．量子もつれ光子を同時に 2 局へ伝送する必要があるため，2 つの望遠鏡を有している．衛星搭載用の光ターミナルは，質量 80.3 kg，消費電力は 182 W で，ISS 上で実現するには問題ないリソース設計となっている．ISS 以外のプラットフォームでの搭載性も考慮していくとのことであったが，小型衛星で実現するには少しリソースは大きいと思われ，最低限，3 軸姿勢安定制御の衛星が必要である．この光ターミナルを用いた Space-Quest の実験シナリオにおいて，量子もつれを使った量子鍵配布実験は，ISS からの見通し内においてヨーロッパの光地上局を 3 局（スペインの Tenerife ESA 局，Calar Alto 局，イタリアの Matera 局）を使用することが検討されている．その ESA の量子鍵配布実験において，日本から NICT の光地上局が加わることで，地球規模の量子鍵配信実験が可能となるため，NICT の光地上局の参画も予定

している．イタリアの Matera 局と日本の NICT の光地上局の組み合わせが，軌道による可視パターンを考慮すると，量子鍵配布には最適であるとの解析結果が出ている．解析に用いた ISS の解析モデルを図 1 に示す．衛星との通信実験が可能な仰角を 5 度以上と仮定すると，平均リンク時間は 3 分程度と見積もられている．

2. 3　任意の 2 つの地上局を用いたグローバル量子鍵配信

任意の 2 つの地上局を用いれば，量子鍵配信・共有実験が，地球規模で実現可能である．図 2 に示す図を参照しながら，以下にその手順を示す．

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（例えば α＝“1001”）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（例えば β＝“1010”）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ーに配信する．（γ は “1001” xor “1010”＝“0011” で，xor は排他的論理和であり，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．例えば，地上局 A では γ xor α ＝“0011” xor “1001”＝“1010” をとればすなわち β を得られることになり，地上局 B でも γ xor β ＝“0011” xor “1010”＝“1001” をとれば α が判明し，ゆえに両地上局で秘密裏に同じ鍵が共有可能である．

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．したがって，宇宙量子暗号通信では，ファイバーでは現状実現できない地球規模での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もつと考えられる．

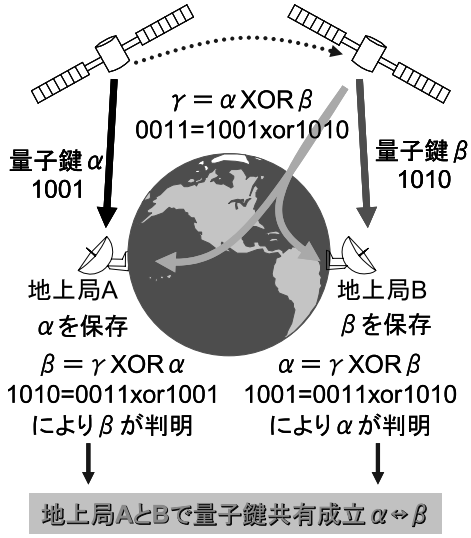

図 2　任意の 2 つの地上局を用いた地球規模での鍵共有．

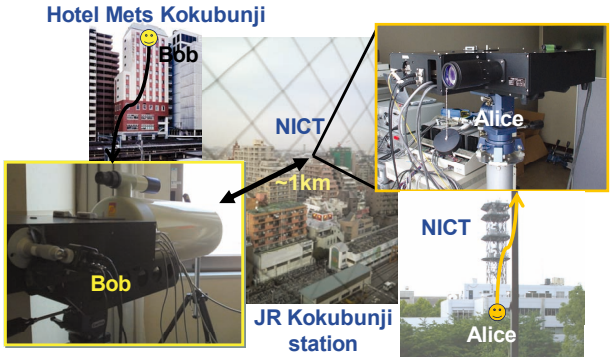

図 3　ホテルメッツと NICT ビル間における約 1 km の量子鍵配布実験の様子．

3.　量子暗号の空間フィールド実験と宇宙への適用性

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，試作試験モデル（BBM）の構築を行った．微弱コヒーレント光の送受信技術を用いて，ビル間での空間伝送による量子鍵配布実験により，その実現性を検討した．図 3 に実験システムの外観を示す．量子暗号システムの BBM モデルは，微弱コヒーレント光を使用し，B92 プロトコルを用いた．B92 で安全性を保つためには，強いリファレンス光が必要とされているが[16]，レーザーが 2 台でシステムが簡素化可能な点と，デコイ方式を用いると伝送距離をさらに伸ばすことが可能であるため[10]，本実験では，大気ゆらぎ存在下におけるフィールド実験で実測した量子ビット誤り率（QBER）とダークカウントを用いて，BB84 プロトコルでデコイを適用して最終鍵レートを見積もることとした．実験で得られたパラメーターを表 1 に示す．BB84 プロトコルでデコイを用いたときの最終鍵レートの計算結果を図 4 に示す．本図は，空間とファイバーシステムに対する最終鍵レートの比較も行っており，ダークカウント Pd を改善したときの効果も示している．デコイの平均フォトン数は 0.5 フォトン/パルスとした．結果より，自由空間伝送のほうが，ファイバー伝送より長距離化できることがわかる．また，ダークカウントの改善により，さらに伝送距離を伸ばすことが可能である．現状システムでは，高度 500 km 程度の低軌道衛星と地上間において，数百 bps 程度の量子鍵配布が可能であり，ダークカウントを改善することにより 1 桁向上させることが可能である．

表1　ビル間での量子鍵配布実験のパラメーター.

Protocol	B92
Clock rate	100 MHz
Mean photon number	0.0962 photons/pulse
Dark count rate（Pd）	4.56E-5
QBER	0.57%
Sift key rate	240.21 kbps
Distance	1.065 km

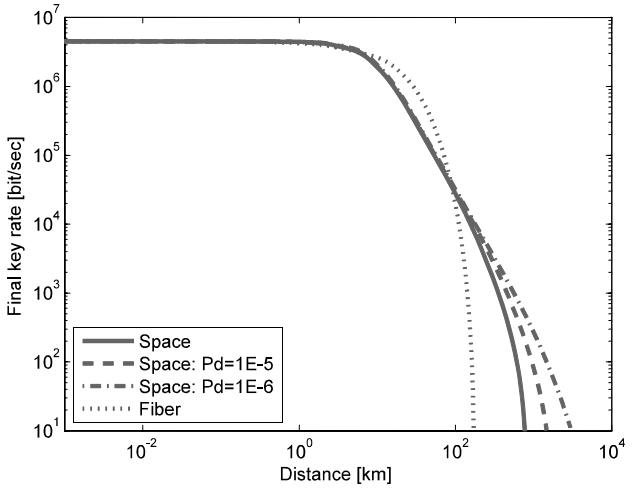

図4　デコイを用いたときの空間およびファイバーシステムにおける最終鍵レートの比較．ダークカウント Pd に対する改善も示している．表1のパラメーターにより算出.

衛星を用いた量子暗号通信の動向について述べた．現段階では，日本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．NICT において試作した BBM モデルにより，原理的には移動体間で量子鍵配布が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さまざまな方式を検討し，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ー技術の究極の最終形態であり，情報通信において今後ますます欠かせない存在になってくると考えられる.

最後に，このようなプロジェクトは国際連携が必須であり，国内外の研究者の方々の先端技術の研究の成果として得られるものであり，今後ともぜひご協力をお願いしたい.

文　　献

1）“Geneva is counting on quantum cryptography as it counts its votes,” Press release of Geneva State Chancellery, October 11 (2007).
http://www.idquantique.com/news/files/com_swissquantum_ang.pdf

2）N. Gisin, G. Ribordy, W. Tittel and H. Zbinden: “Quantum cryptography,” Rev. Mod. Phys., **74** (2002) 145–195.

3）C. H. Bennett and G. Brassard: “Quantum cryptography: Public key distribution and coin tossing,” *Proceedings of International Conference on Computers, Systems & Signal Processing* (Bangalore, India, 1984).

4）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** (2002) 43.1–43.14.

5）K. E. Wilson, J. R. Lesh, K. Araki and Y. Arimoto: “Overview of the ground-to-orbit lasercom demonstration,” Space Commun., **15** (1998) 89–95.

6）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,” *Proceedings of the 53rd International Astronautical Congress*, IAC-02-M.2.01 (Houston, 2002) pp. 1–11.

7）M. Toyoshima, T. Takahashi, K. Suzuki, S. Kimura, K. Takizawa, T. Kuri, W. Klaus, M. Toyoda, H. Kunimori, T. Jono, Y. Takayama and K. Arai: “Ground-to-satellite laser communication experiments,” IEEE Aerospace Electron. Syst. Mag., **23** (2008) 10–18.

8）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,” *Aerospace Conference Proceedings, 2000 IEEE*, Vol. 1 (2000) pp. 191–200.

9）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** (2002) 450.

10）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 144 km,” Phys. Rev. Lett., **98** (2007) 010504.

11）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** (2003) 022309.

12）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,” J. Opt. Networking, **4** (2005) 549–560.

13）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 and A. Zeilinger: “Entanglement based quantum communication over 144 km,” Nat. Phys., **3** (2007) 481–486.

14）C.-Z. Peng, T. Yang, X.-H. Bao, J.-Zhang, 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** (2005) 150501.

15）辻野照久：“通信放送衛星システムの利用動向”，科学技術動向，10 月号（2006）.（http://www.nistep.go.jp/achiev/ftx/jpn/stfc/stt067j/0610_03_featurearticles/0610fa03/200610_fa03.html）

16）K. Tamaki, N. Lütkenhaus, M. Koashi and J. Batuwantudawe: “Unconditional security of the Bennett 1992 quantum key-distribution scheme with a strong reference pulse,” Phys. Rev. A, **80** (2009) 032302.

（2009 年 9 月 7 日受理）