NICT における宇宙量子暗号通信の研究開発状況

情報通信研究機構　豊嶋守生、高山佳久、クラウスヴェルナ、國森裕生、藤原幹生、佐々木雅英

Current status of research and development for space quantum cryptography communications in NICT

Morio Toyoshima, Yoshihisa Takayama, Werner Klaus, Hiroo Kunimori, 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: Free-space quantum cryptography is expected to be a first space application employing quantum technology in the near future because of the suitability for the long distance transmission of photons. European Space Agency (ESA) plans to demonstrate a quantum key distribution experiment onboard the ESA's Columbus module in the International Space Station (ISS) called Space-QUEST. The quantum key distribution employing entangled photons will be demonstrated using three optical ground stations in Europe. Therefore, there is a possibility for Japan to join it as one of the optical ground stations for the global quantum key distribution. NICT has started a feasibility study on the quantum cryptography for space communications. In this paper, the current status of research and development for space quantum cryptography communications in NICT is 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。

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。絶対安全性を保障する量子暗号は、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が可能である。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立ち上げに向けた検討を開始した。本稿では、NICTにおける宇宙量子通信の研究開発の現状について報告する。

2. 欧州の宇宙量子鍵配布プロジェクトの状況

2．1　現状

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[4-7)]。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[8,9)]。ウイーン大学のグループは、1997年に世界で初めて量子テレポーテーションを実験で実証したのを皮切り

に、1999年には量子もつれによる量子暗号、2003年には量子純粋化において世界で最初の実証を行ってきており、量子情報通信分野で著名な業績を上げている。2005年秋には、スペインのカナリア諸島で島を隔てた144kmの空間伝搬により、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[10]。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。

2．2　実験目的

SPACE-QUESTの実験目的を以下に示す。

- 量子もつれを衛星ベースのシステムで宇宙実証する。
- 地上で達成不可能な距離での量子もつれ現象の確認試験。
- 衛星－地上間における長距離量子鍵配布の実証を行う。
- 将来のグローバル量子ネットワークを構築する。

2．3　実験内容

Space-QUESTの実験内容は、以下の3つが考えられている。

(a) 衛星に搭載した単一光子光源から地上局への単一光子量子暗号通信実験

(b) 任意の2つの地上局を用いた量子鍵配信・共有実験

(c) 衛星見通し内にある1600km以上離れた2つの地上局へ量子もつれ状態を伝送する量子鍵配布・共有実験

このうち、(b)の任意の2つの地上局を用いた量子鍵配信・共有実験は、地球規模で図1に示す手順で実現可能である。

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γ＝αXORβ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。長距離伝送が可能である宇宙量子暗号通信において、地球規模で実証をすることは、将来の応用へ重要な意味を持つと考えられる。

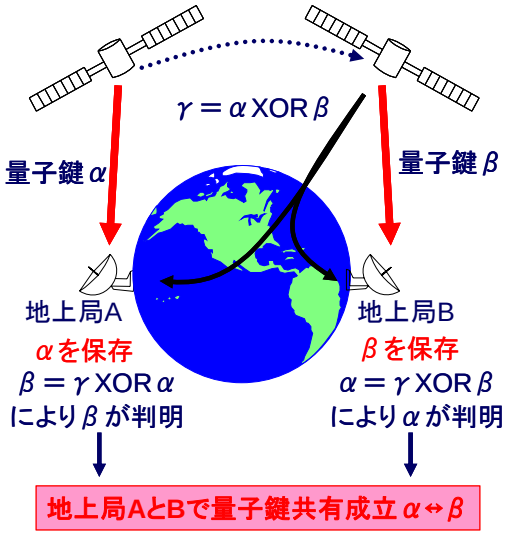

図1．任意の2つの地上局を用いた量子鍵配信・共有実験

2．4　光地上局

ISSにおける実験シナリオにおいて、量子もつれを使った量子テレポーテーション実験は、ISSからの見通し内においてヨーロッパの2つの光地上局を同時に使う必要がある。この量子通信実験のための光地上局には、スペイン2局（本土1局、カナリア諸島テネリフェ島1局）、イタリア1局が現在検討されている。量子もつれを光地上局2局に同時に伝送するための実験時間は、平均で90秒程度と予想されているが、量子鍵配布実験は十分可能であると見積もられている。

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は低軌道であり、NICT光地上局とISS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。ESAの量子鍵配布のプロジェクトにおいて、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。また、ヨーロッパ（ESA）側は、量子通信プロジェクトを推進

する上で、日本の光地上局が使用できることで、1年に100パス程度しかない実験機会をさらに増加させ、有効にプログラムを実施することができると考えられる。

2．5 ウイーン大学との共同研究

NICTでは、NICT所有の光地上局が量子もつれを用いた量子鍵配布に供しえるかどうかの検討を開始した。まず、光地上局が、量子もつれを伝送するための基本特性を備えているかを測定により確認する必要がある。NICTでの望遠鏡サイトでの基本的な測定項目としては、以下を行う予定である。

- 1.5m望遠鏡システムの光学特性測定
  - 望遠鏡光学ロスの測定
  - 偏光特性の測定
  - 背景光の測定
  - 大気透過率の測定等
- 大気ゆらぎの与える影響の評価

上記をNICTとウイーン大学との両機関により実施し、NICT光地上局を含めた宇宙量子鍵配布実験の可能性について検討する予定である。これは、ウイーン大学との共同研究により実施される予定であり、共同研究締結に向けては文書手続きを残すのみとなっている。

3. NICTにおける宇宙量子通信の研究開発

3．1 宇宙量子通信に関する研究の立ち上げ

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年間の予定で以下の研究計画で行う予定である。

3．2 研究計画

量子通信技術の衛星搭載化に向けた研究開発を行う。研究内容は、宇宙量子通信の概念検討作業、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。

- 開始後1年目の目標
  - 量子情報通信機器の概念検討と基本素子調達を行う。
  - 量子情報通信機器に必要な光ターミナルの概念検討と基本素子調達を行う。
  - ウイーン大学と共同研究を締結する。
- 開始後2年目の目標
  - 量子情報通信機器の基本設計とBBM試作を行う。
  - 量子情報通信機器に必要な光ターミナルの基本設計とBBM試作を行う。
- 開始後3年目の目標
  - 量子情報通信機器の基本設計とBBM設計と搭載化評価を行う。
  - 量子情報通信機器に必要な光ターミナルの基本設計とBBM搭載化の評価を行う。

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。

3．3 NICTにおける独自研究の立ち上げ

NICTにおける宇宙量子通信の研究開始にあたり、まず空間伝送を行う地上用量子鍵配布送システムを構築する独自研究を開始した。これは前節におけるBBM試作の元になるものである。単一光子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。今年度、基本素子調達を開始し、量子暗号システムの基本的な機能を確認する予定である。実験は、まずは光学ベンチ上で行い、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。

3．4 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2に、光宇宙通信の研究開発ロードマップを示す。現在、2015年を目指した打ち上げで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。

また、中国では中国科学技術大学の潘建偉教授が、2005年に地上伝搬において13kmの距離で量子もつれによる暗号伝送に成功しており[12)]、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。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。日本における研究開発やロードマップ検討においては、中国の動向を注視しながら遅れを取らないように実施していく必要がある[13]。

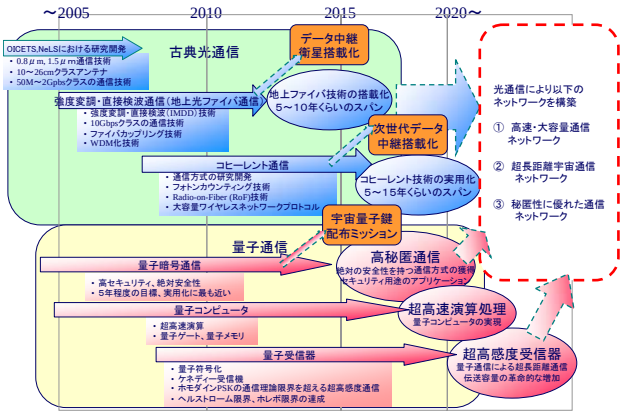

図2. 光宇宙通信の研究開発ロードマップ

4. まとめ

NICT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。

最後に、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が、本研究を立ち上げる上での有益な一助となった。これにより、日本独自の搭載ミッション提案にまで将来つながればと考えている。ここに感謝する次第である。

5. 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) 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).
5) 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).
6) M. Pfennigbauer, W. R. Leeb, “Quantum Communications in Space (QSpace),” Final Report within ESA/ESTEC/Contract No. 16358/02/NL/SFe (2003).
7) 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).
8) http://www.spaceflight.esa.int/users/index.cfm?act=default.page&level=16&page=453
9) 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).
10) http://www.quantum.at/typo/fileadmin/PDF/Space_Brochure.pdf
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) 中国新聞網、2005 年 5 月 6 日。
13) 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