

日本における宇宙量子暗号通信の研究開発について

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

Research and development of space quantum cryptography communications in Japan

Morio Toyoshima, Werner Klaus, Hiroo Kunimori, Mikio Fujiwara, and Masahide Sasaki
National Institute of Information and Communications Technology, 4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795
E-Mail: morio@nict.go.jp

Abstract: A quantum communication demonstration is proposed by Prof. Zeilinger group of University of Vienna as an ESA's scientific mission onboard the Columbus module in the International Space Station (ISS), which is called SPACEQUEST. The quantum cryptography employing entangled photons is demonstrated using three optical ground stations in Europe. There is a possibility for Japan to join it as one of the optical ground stations for the quantum key distribution. In this paper, the overview of the SPACEQUEST project is introduced, and the research and development of space quantum cryptography communications in Japan is discussed.
Key words; Space Utilization, International Space Station, Quantum Cryptography

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。総合科学技術会議の情報通信分野の研究開発推進戦略においても、重点領域における研究開発の目標として以下が述べられている。

「2. 次世代のブレークスルーをもたらす研究開発領域
（1）次世代情報通信技術（10年後以降の実現に向けた基礎的技術）
○量子工学技術を用いた情報通信
比較的短距離（～数十km）での量子暗号鍵配布、量子通信のプロトタイプ等」
（2001年、一部抜粋）

また、情報セキュリティの重要性については、総合科学技術会議（2003年5月）における意見具申（情報通信研究開発の推進）や、e-Japan戦略Ⅱ（2003年7月）においては、国として研究開発を推進する必要性が指摘されているとともに、e-Japan重点計画2003では、政府における情報セキュリティの確保など施策が挙げられている。さらに、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、代替手段として絶対安全な量子暗号技術は有望視されており、近い将来、社会的に実用領域で量子暗号技術が期待されている。

しかしながら、宇宙において量子通信技術を用いることは、具体的に日本においてはほとんど議論されてこなかったのが現状である。本稿では、日本における宇宙量子通信の研究開発について言及する。

2. ESA量子通信実験プロジェクトについて

2. 1　現状

量子通信を宇宙で利用することを具体的に提案しているのは、ウイーン大学のZeilinger教授のグループである[4,5)]。彼らは、1997年に世界で始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。ウイーン大学他、ウイーン工科大、ドイツ、イタリア、フランスによる共同提案として、既に国際宇宙ステーション（ISS）

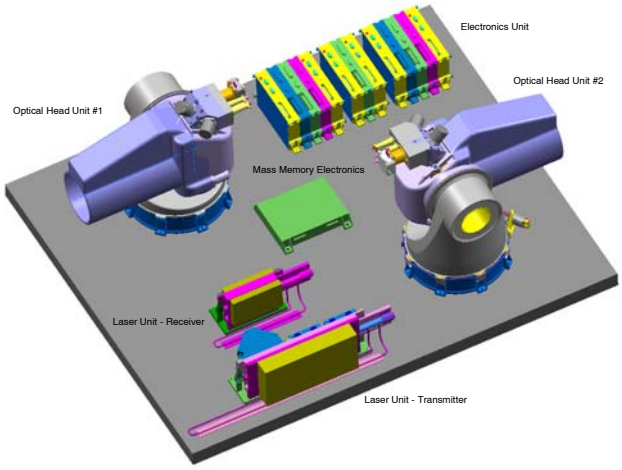

図1. 光ターミナル検討レイアウト例

搭載用の量子通信のための光ターミナルの検討を行っており、これにはファイナルレポートも出されている[6]。図1に検討されている光ターミナルレイアウト例を示す。この光ターミナルは、スイスのContraves Spaceが提供するOPTEL-25というモデルがベースとなっており、ISSのコロンバスモジュールに2台搭載される[7]。最新版のELIPS2というESAのISS搭載ミッション選定では、ISSの量子通信に以下に示すような情報が明記され、基礎物理分野で評判がよく、2011年には打ち上げを計画している[8]。

「Proposal Number: AO-2004-054
Peer Evaluation: Outstanding
Coordinator, Partners, Company, (Country): A. Zeilinger (A), H. Weinfurter (D), W. Leeb (A), C. Barbieri (I), E. Samain (F)
Title Experiment: Quantum communication for space experiments (SPACEQUEST).
Facility: Dedicated external payload on COLUMBUS Laboratory
Experiment Platform Experiment Status: ISS to be Performed」

（ELIPS2リポートから抜粋）

2．2　実験目的

SPACEQUEST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

SPACEQUEST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、図2を用いて以下の手順で地球規模で実現できる。

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＝α 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などにより地球規模でグローバルな実証をすることは、将来の宇宙量子暗号通信における応用へ重要な意味を持つと考えられる。

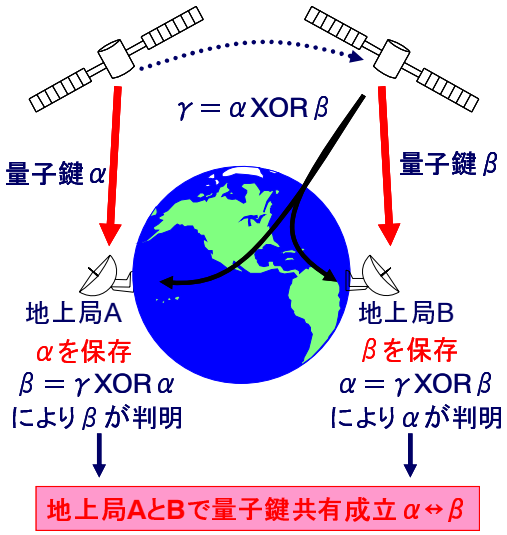

図2．任意の2つの地上局を用いた量子鍵配信・共有実験

2．4　光地上局について

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。図3にこの視野解析例を示す[6]。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。

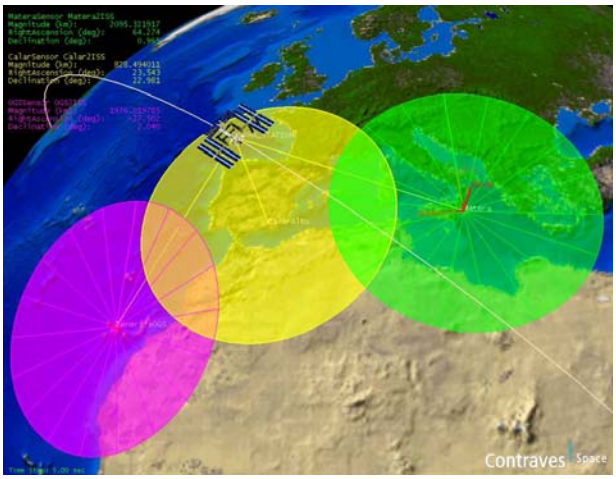

図3. SPACEQUEST の光地上局視野解析例

3. 日本における宇宙量子暗号通信の研究開発

3. 1 開発シナリオ案

ESAのSPACEQUESTと歩調を合わせ、今後日本で研究開発していくシナリオ案としては下記の4通りが考えられる。

(1) 情報通信研究機構(NICT)が搭載用量子通信機器(シャノン限界を超える送受信機、これはNICT量子情報通信グループの成果の活用)と、地上量子通信機器を独自開発し参画
(2) NICTが搭載用量子通信機器(量子鍵送受信機)と地上量子通信機器部分を独自開発し、光地上局側を日本独自に整備
(3) NICTが地上量子通信機器部分のみ独自開発し、光地上局側を日本独自に整備
(4) NICT光地上局望遠鏡を活用し、地上量子通信機器部分をESA、ウイーン大学から借用し実施

シナリオ案(1)であるが、NICTの量子情報通信グループで研究開発し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技術開発として魅力的であるが、ここ5年程度のスパンでは実現は難しそうである。シナリオ案(3)と(4)は衛星搭載化を考慮しない選択であり、将来の実用に向けて日本における搭載化技術開発の必要性からもシナリオ案(2)が必要であると考えられる。

3. 2 搭載用量子通信機器独自開発のシナリオ案

シナリオ案(2)をブレークダウンすると、以下の手法が必要であろう。

- 手法
  1) NICTにおいて、搭載用と地上用量子鍵配布送受信機を開発する。
  2) ESAのISS搭載ターミナルとコンパチブルなインタフェースを構築する。
  3) 日本独自での衛星搭載を考慮し、ISSやその他の衛星を用いて可能な限り機会を狙った宇宙実証を考慮し、2機打ち上げることが出来れば、自国でISSとの衛星間量子通信も視野に入ってくる。
  4) NICTの光地上局と、ISSもしくはその他の衛星等との見通し通信で量子鍵配布実験を行う。

シナリオ案(2)でのメリットとデメリットとしては以下が考えられる。

- メリット
  - 日本の独自衛星への実証計画を考慮することで、他国のプログラムに左右されない日本独自の宇宙実証が可能(リスク管理の面で重要)
  - JAXAやNICTでこれまで行ってきた光宇宙通信技術が継承可能
  - ISSと日本側衛星との間での衛星間量子通信実験も可能
  - ESAの光地上局とも通信を行う選択をすることで伝搬路条件におけるミッション不達成等のリスク低減
  - NICT光地上局の望遠鏡活用
- デメリット
  - 光子の受信時刻同定、偏光の安定化技術が難しい。(しかしウイーン大学では現状実証できている技術レベル)

量子鍵配布のために光地上局に要求される条件としては、望遠鏡の偏光特性の測定・評価、背景光の測定・評価、透過率の測定・評価などが必要である。

3. 3 国際協力について

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。日本においては、将来ビジョンとして量子宇宙通信を始めるための足がかりとなることや、国際協力を推進する観点で有意義なプロジェクトとなる。また、国内でも量子通信の研究を他にやっている大学等と協力するという枠組みも、国内自力で開発する場合には意義がある。

4. まとめ

日本における宇宙量子暗号通信の研究開発について、ESAのプロジェクトに連携して進めていくシナリオ案を示した。光地上局に関しては、日本においてNICTのみならず、JAXA、天文台、大学など様々な機関が低軌道衛星を追尾できる望遠鏡を有している。これらの望遠鏡施設は、量子鍵配布用の受信機のみ設置すれば光地上局として利用できる可能性がある。現段階においては可能性としてどことは限定せずに、これらの利用も含め、様々な機関と協力して研究開発のシナリオを作り進めていければと考えている。これをたたき台に、将来の宇宙量子暗号通信について、さまざまなアイデアや意見を頂けたら幸いである。

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