4-5　量子暗号技術

4-5　Research Activity of Quantum Security

早稲田篤志
WASEDA Atsushi

要旨

量子暗号は理論的に無条件安全性が実現できるとして注目され、各国の研究機関にて研究が行われている。セキュリティ基盤グループではこの量子暗号を始めとした量子セキュリティ技術が広く一般に利用されることを目指してこれまで研究を行ってきた。本稿では、第2期中期計画におけるセキュリティ基盤グループの量子セキュリティ研究の概略を述べるとともに、その中で量子ICTグループを始めとした他のグループとの協力関係や、Updating Quantum Cryptography and Communications（UQCC）などの関係するイベントについても紹介する。

Since only the quantum security can realize the unconditional security, the importance of the quantum security technologies is increasing. Therefore, it is researched by laboratories in each country. The quantum security technology is researched also by Security Fundamental Group aiming at the achievement of the society where the quantum cryptography is widely used in general. In this paper, we report the outline of researches of the quantum security in this group of five years recently, the cooperation with other groups and the relating events such as UQCC.

[キーワード]
量子暗号，量子セキュリティ，Updating Quantum Cryptography and Communications（UQCC）
Quantum cryptography, Quantum security, Updating Quantum Cryptography and Communications (UQCC)

1　まえがき

昨今の技術の発達により、非常に広範なネットワークが張られ、多くのコンピュータがネットワークに接続している。それに伴い、このネットワークを守るためのセキュリティ技術が重要な要素となっている。ネットワークに対する攻撃としてはDoS（Denial of Service）攻撃のような通信システムそのものをダウンさせるような攻撃や、コンピュータウイルスなどを利用したコンピュータの乗っ取りや通信相手になりすましてデータを引き出し、ネットワーク上を流れる通信データの盗聴などによりデータの暴露、改ざんなどを目的とした攻撃などが顕著な例として挙げられ、これに対する対策法としてnicter[1]に代表されるネットワークの監視機構やウイルス対策ソフト、現代暗号技術の導入により対策を施すということが一般的である。

これらの対策のうち現代暗号技術の多くはコンピュータを使用しても解くことが困難であるということを安全性の根拠にしている。しかしながら、昨今のコンピュータ性能の爆発的な発展によりその安全性が危ぶまれている。これに対してはハッシュ関数SHA-1（160［bit］）をSHA-2（256［bit］）への変更や公開鍵暗号RSAの鍵長を1024［bit］から2048［bit］へ延ばす作業などにより安全性の確保がなされている。しかしながらこの暗号技術の入れ替えに伴うシステムの更新はサービスの継続性（BCP）に大きな影響を与えるだけでなく、新旧システムの同時運用や旧データとの互換性維持などに伴う安全性低下の懸念も大きい。さらには、量子コンピュータのような新たなタイプのコンピュータの出現もあり、これまでのようなコンピュータ技術の発達により安全性が左右されない

暗号技術もまた求められている。この要請に対しては現代暗号においても one time pad [2] などの方法が提案されている。しかしながら、これらの方法は非常に効率が悪く実用には至っていなかった。これに対して量子技術を導入することで解決を図ろうという動きがある。特に、量子鍵配送は one time pad における最大の問題点であった安全な鍵の共有という点を解決できるため注目された。結果として SECOQC (Secure Communication based on Quantum Cryptography) [3] や東京 QKD ネットワーク [4] といった量子ネットワークの実証実験を行うまでになっている。以上のように量子技術を用いることで通信やデータ保護の安全性の向上が期待できるため、それを積極的に活用しようとするのが量子セキュリティである。

セキュリティ基盤グループではこのような問題の解決を図るため、量子 ICT グループや宇宙通信ネットワークグループと共同で研究を進めてきている。量子 ICT グループとは量子暗号や他の量子セキュリティプロトコルの安全性評価を行い、宇宙通信ネットワークグループとは量子測定機を用いたときの量子通信の通信路容量の評価などを行ってきた。開始当初には量子 ICT グループは現代暗号の最新動向をフォローアップする体制はできておらず、逆にセキュリティ基盤グループは量子暗号の実験装置や安全性理論について十分な理解が及んでいなかった。そのためお互いの知見をうまくかみ合わせ、知識を融合しながら研究を進め一定の成果を上げることができた。

本稿ではセキュリティ基盤グループにおける量子セキュリティ研究の成果の概要について述べる。まず、**1.1** として第 2 期中期計画における研究成果と行われたイベントを時系列に応じて簡単に述べる。次に **1.2** として当中期計画中に行われた大きなイベントの代表として Updating Quantum Cryptography and Communications [5] を述べ、**1.3** として東京 QKD ネットワークについて述べる。さらに、**1.4** として日本の量子暗号研究の方針を決める量子 ICT 運営会議について概略を述べる。その後にセキュリティ基盤グループ室員が第 2 期中期計画中に行った各研究概要について簡単に述べ、最後にまとめとする。

1.1 第 2 期中期計画中の基盤グループにおける量子セキュリティ研究に関する流れ

セキュリティ基盤グループにおける量子セキュリティに関する研究が本格的にスタートしたのは中期計画 2 年目の 2007 年に著者が専攻研究員として採用されたことにはじまる。この年度は他のグループとの共同研究は本格的には開始しておらず、基本的に基盤グループ単独で研究を行った。この年度の結果として、論文成果としては著者の大学院時代の結果をブラッシュアップすることで量子秘密分散法のバリエーションの 1 つとして量子複数秘密分散法の提案 [6] が情報処理学会論文誌に採択され、国内研究会における発表としてグループ間量子秘密分散法の提案 [7] を暗号と情報セキュリティシンポジウム (SCIS) 2008 にて行った。この年の 10 月には東京で UQC (Updating Quantum Cryptography) 2007 が初めて開催されている。

翌 2008 年度には本格的に量子 ICT グループとの意見交換、および共同研究が開始され、量子通信路の通信路容量の評価を行い、その成果を国内研究会である SCIS2009 にて発表している [8]。また、前年度に提案したグループ間秘密分散法を査読つき国際会議 International Symposium on Information Theory and its Applications (ISITA2008) にて発表を行った [9]。また前年度に引き続き、東京で UQC (Updating Quantum Cryptography) 2008 が開催されている。

2009 年度にも前年度に国内研究会で発表したファイバ帯域の量子通信路の通信路容量についての論文が Journal of the Optical Society of America に採択された [10]。さらにこの結果を宇宙空間に拡張するため、宇宙通信ネットワークグループともコンタクトを取り、その成果について国際会議 2010 International Conference on Availability and Security にて発表を行った [11]。この研究をさらに発展させるため、University of Padua の Dr. Antonio Assalini との意見交換を始めたのもこの年からである。さらに田中グループリーダーが量子秘匿変調方式に対して暗号利用モードを用いた考察を行い、国内研究会 SCIS2010 にて発表を行っている [12]。

中期計画最終年度となる 2010 年度には東京 QKD ネットワークの稼働や UQCC (Updating

Quantum Cryptography and Communications) 2010の開催といった大きなイベントがあった。さらに、研究開発推進ファンド・プリプロジェクトの「超高速移動体通信と高セキュリティグローバル量子鍵配布技術の研究開発」と「高セキュリティを実現するための量子認証・暗号技術基礎開発」の2件のプロジェクトへの採択がされた。研究成果の発表としては、量子認証について複数グループを一度に認証する量子複数認証についてSCIS2011にて発表している[13]。

1.2 Updating Quantum Cryptography[5]

UQC (Updating Quantum Cryptography) およびUQCC (Updating Quantum Cryptography and Communications) (図1) はNICTと独立行政法人情報処理推進機構 (IPA)、独立行政法人産業技術総合研究所 (AIST) が中心となって企画した国際会議であり、これまで3回開催された。

第1回は2007年10月1日から3日までの3日間秋葉原ダイビルのコンベンションホールにて行われ、NIST (National Institute of Standards and Technology) を始めとした海外からも多くの参加者があった。このうちの3日目は専門家のみのclosed sessionが行われた。内容としては各国の量子暗号の最新動向やキーテクノロジーの研究開発動向の報告などが行われた。会期中の討論ではNISTからの参加者らから無条件安全性とサイドチャネル攻撃について積極的な意見が出された。翌4日と5日には第2回量子ICT運営会議がSCATにて開催され、総務省公募研究 (SCOPE)、NICT委託研究の研究概要の報告などが各研究機関より行われ、今後の活動計画についての議論などが行われた。

第2回UQCは2008年12月1・2日の2日間前年度と同じく秋葉原ダイビルのコンベンションホールにて行われた。内容としてはEUで行われたSECOQC (Secure Communication based on Quantum Cryptography) に関する報告や、標準化動向としてETSI (European Telecommunications Standards Institute、欧州電気通信標準化協会) での活動などについて講演が行われた。また、内閣官房、総務省、経済産業省の各省より量子暗号技術を含めたICTに関する日本の国家戦略が紹介された。

第3回UQCCは2010年10月18日から20日までの3日間ANA InterContinental Hotel in Tokyoにて行われた。今回の会議ではその直前の10月14日に東京都内の光ファイバ網をつないだ最新の量子暗号ネットワークである東京QKDネットワークが稼働したこともあり、東京QKDネットワークの紹介や期待等をはじめ、国内外の最新の研究成果や実用化に向けた動向などが紹介された。

1.3 東京QKDネットワーク[4]

東京QKDネットワーク (図2) は2010年10月14日に運用が開始された量子暗号ネットワークのテストヘッドである。運営構築にはNICTの量子ICTグループが中心的役割を果たし、そのほか、日本電気株式会社 (NEC)、三菱電機、日本電信電

図1 UQCC

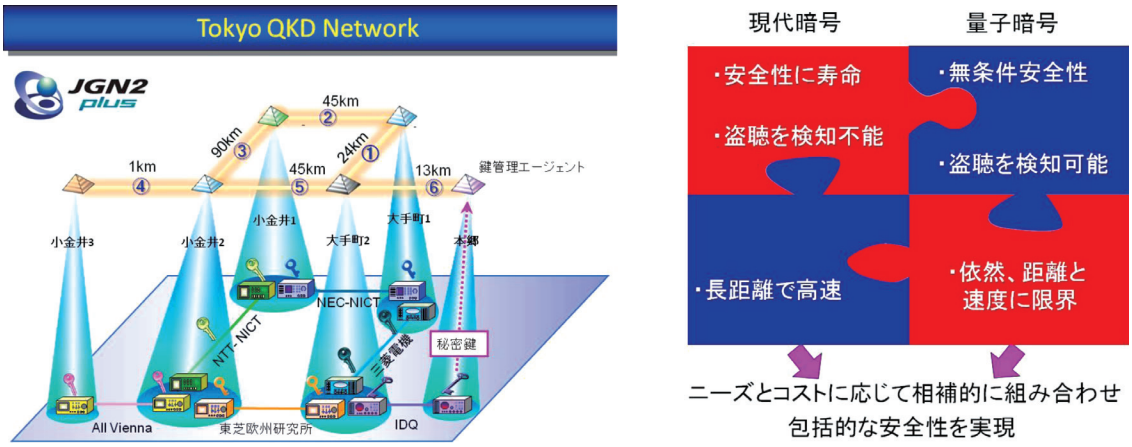

図2 東京 QKD ネットワーク

話株式会社（NTT）が行っている。秘密鍵の生成速度は 45km の光ファイバ回線で毎秒 10 万 bit と実環境では世界最高速を実現している。今後は他のシステムとの相互接続実験や現代暗号との統合運用技術の研究開発などに役立たせる予定である。

1.4 量子 ICT 運営会議

量子 ICT 運営会議は年 1 回のペースで行われ、SCOPE の採択を受けた各研究チームによる最新の研究成果の報告や量子暗号の取り巻く成果の展開方法、他分野との連携、次世代量子暗号、量子中継、量子デバイス、量子情報基礎理論等の重要課題についての議論などの次期研究推進戦略などの議論が行われた。

2 研究概要

ここではセキュリティ基盤グループ室員が第 2 期中期計画中に行ってきた研究成果の概略について述べる。

2.1 量子複数秘密分散法[6]

量子秘密分散法とは秘密の分散符号化を行う秘密分散法について取り扱う秘密を量子状態にしたり、使用する通信路を量子通信路としたりしたものである。本論文では秘密情報を量子状態とし、さらに取り扱う秘密状態の数を複数とした量子複数秘密分散法を初めて定義し、その構成法を提案した。また量子複数秘密分散法の満たすべき諸性質について明らかにした。

定義 参加者の集合を P、秘密の量子状態の集合を $\{S_1,\cdots S_n\}$ とする。各々の秘密 S_i に対し、純粋化に用いた補助系を R_i、アクセス構造を Γ_i とする。さらに、各 Γ_i について $T_i=\{R_1,\cdots,R_n\}\setminus\{R_i\}$ とする。このとき、任意の i について以下の 2 つの条件を満たすものを、量子複数秘密分散法と定義する。

(1) Recoverability

任意の $A\in\Gamma_i$ に対し、$I(R_i:T_iA_i)=I(R_i:S_i)$

(2) Secrecy

任意の $B\notin\Gamma_i$ に対し、$I(R_i:T_iB_i)=0$

ただし、$I(A:B)$ は系 A と系 B の相互情報量である。

この結果は単一の秘密を持つ量子秘密分散法の定義を拡張したものであり、(1) は、秘密 S_i を分散させた量子操作に対し、その逆変換が存在することを示している。(2) については、系 B_i と補助系 T_i を分散させた量子操作に逆変換が存在しないことを示している。

提案方式（図 3）は Monotone Span Program（MSP）を使用した量子秘密分散法を拡張することで得る。集合 P 上における MSP とは、(1) F_q：位数が q の有限体、(2) M：F_q 上の $d\times e$ の行列、(3) g：参加者 P に M の行を割り振る関数（$\{1,\cdots d\}\to P$）、(4) ターゲットベクトル t の (F_q,M,g,t) の 4 つ組によって構成され、ある集合

Aについて$g(\cdot)\in A$となるMの部分行列M_Aにより生成される部分空間にtが含まれるときMSPを受理するという。

MSPを利用して得られた秘密状態をm個、分散情報をt個とし、そのうち任意のd個以上のシェアを集めることですべての秘密の状態を復元できる量子複数秘密分散法を、(m,t,d)量子閾値複数秘密分散法という。この量子閾値秘密分散法について以下のような定理が得られた。

定理　MSPを用いて構成された(m,t,d)量子閾値複数秘密分散法は、Secrecyを満たすとき、かつそのときに限り、以下の2条件を満たす。(1) $d\geq t+m+1$、(2) $e\geq t+m+1$

2.2　グループ間量子秘密分散法[7][9]

前項と同じく量子秘密分散法のバリエーション

である。この方法は量子状態を用いて古典状態の秘密を分散する方法である（図4）。この方法では参加者を2つのグループに分け、分散情報の作成には両グループが協力して行い、秘密情報の復元は各グループメンバのみで行う方式である。また、この方式ではあらかじめ秘密情報を選ぶことができず、秘密の復元がされるまでもとの秘密情報を知ることができない方式であり、ビット共有と秘密分散を同時に行うといった面を持つ方式である。この方式は分散情報の一部が漏えいした際などに秘密情報の変更を行うことなく分散情報の更新を行うなどの応用が期待できる。

2.3　ファイバ帯域の量子通信路の通信路容量の評価[8][10][11]

量子ICTグループとの共同研究における成果と

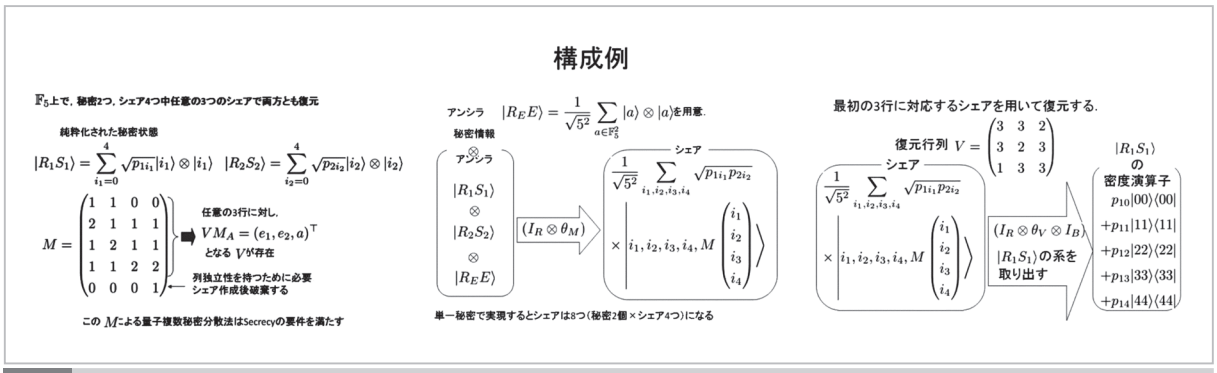

図3　量子複数秘密分散法

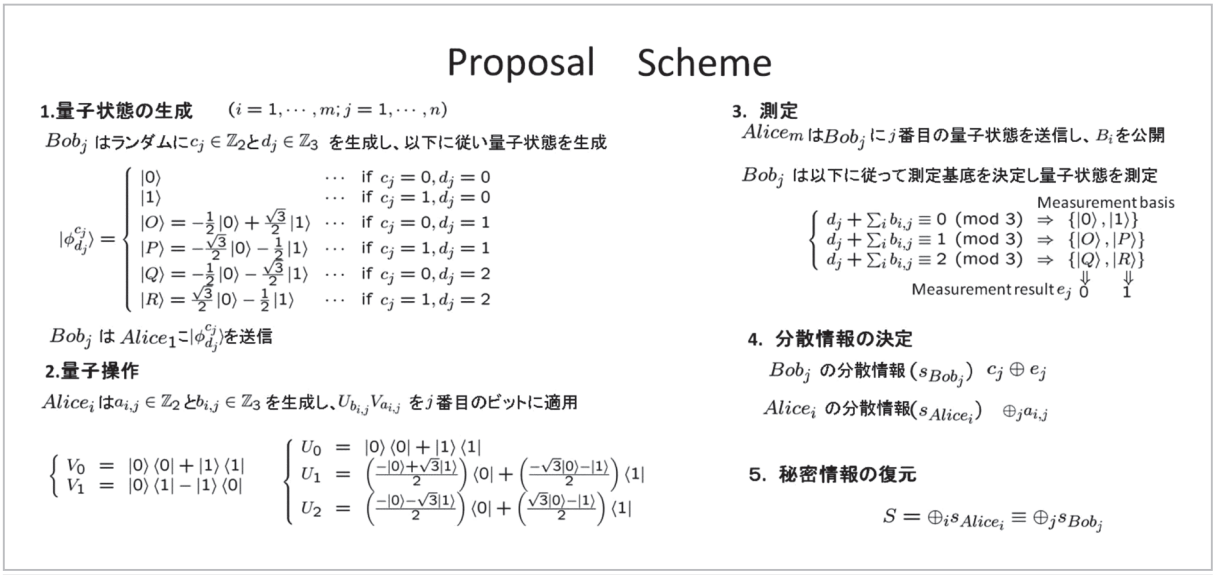

図4　グループ間量子秘密分散法

してファイバによる帯域50Thz（1.2–1.6μm）における phase shift keying（PSK）および quadrature amplitude modulation（QAM）の2変調方式と測定法として homodyne、heterodyne の両ダイン検波、Square Root detection（SRD）および量子測定によって得られる最大の情報量を与える Holevo information を用いた場合のそれぞれについて量子通信路の通信路容量を計算し、Giovannetti らにより与えられた理論的な上限と比較した（図5）。この結果、1mW 以下の入力電力において量子効果を考慮しない現在の光通信よりも優位性を持つことが確認できた。特に、入力電力1μW 以下においては変調方式として BPSK を用い、これにホモダイン検波を行ったときが、また、入力電力1μ以上1mW 以下の場合はより多値で変調を行い、ヘテロダイン検波を行ったときが、それぞれで最も通信路容量が大きくなることが確認できた。

2.4 宇宙通信における量子通信路の通信路容量の評価[11]

前項の内容について宇宙通信に適用して計算を行った。送信、受信アンテナとして直径をそれぞれ305mm、10,000mm としており、比較項目は前項と同じである。すなわち、変調方式として phase shift keying（PSK）および quadrature amplitude modulation（QAM）の2変調方式を、測定法として homodyne、heterodyne の両ダイン検波、Square Root detection（SRD）および量子測定によって得られる最大の情報量を与える Holevo information をそれぞれ用いた場合と Giovannetti らにより与えられた理論的な上限と比較した（図6）。結果として火星までの通信ではこれらのアンテナを用いた場合信号の生成に1W を用いると理論的には10Gbit/sec が実現できることを示した。また遠距離、または入力電力が小さいときは変調方式として BPSK を用い、これにホモダイン検波を行ったときが、逆に近距離、または入力電力が大きいときはより多値で変調を行い、ヘテロダイン検波を行ったときが、それぞれで最も通信路容量が大きくなることが確認できた。

2.5 量子秘匿変調方式の安全性に関する考察[12]

Y-00 に代表される量子秘匿変調方式に対して安全性考察を行った。本方式はストリーム暗号の一種として扱われ、そのように安全性が評価されてきた。これらの評価結果から現代暗号のストリーム暗号と同等の安全性であると帰着されている。本論文では量子秘匿変調方式をストリーム暗号と捉えず、量子通信を仮定した暗号利用モードの一種と捉え、理想的安全な擬似乱数生成器を利用したと仮定し、全数探索以外での攻撃が不能であるとの条件の元で、その構造的安全性の評価を行った。

2.6 量子複数認証方式[13]

量子暗号は無条件安全性を満たす方式として提案されているが欠点としてその通信距離が非常に制限されるという点があげられる。その結果、長

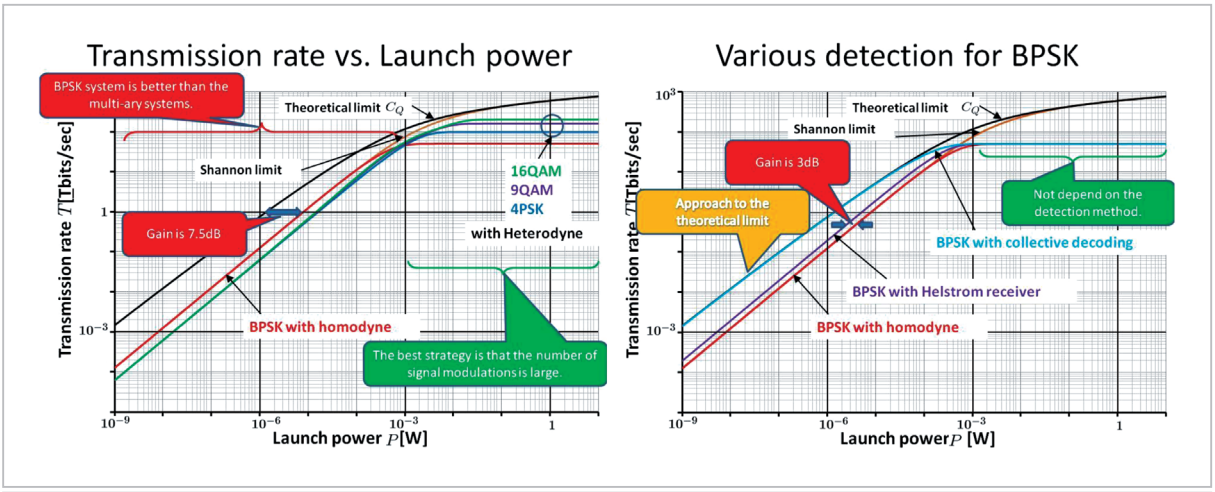

図5 ファイバ帯域における量子通信路の通信路容量

距離の通信を行うためにいくつかのノードを経由して鍵共有を行う。現在、この通信に使用するノードについては信頼できるものとしているが、このような信頼は本来望ましいものではない。そこで、このような複数のノードを経由する通信路において量子状態を用いて各ノードを一度に認証しようというのが量子複数認証方式である（図7）。この研究では既存方式では安全でなかった量子状態や量子変換を改良し、既存方式に強い方式の提案を行った。

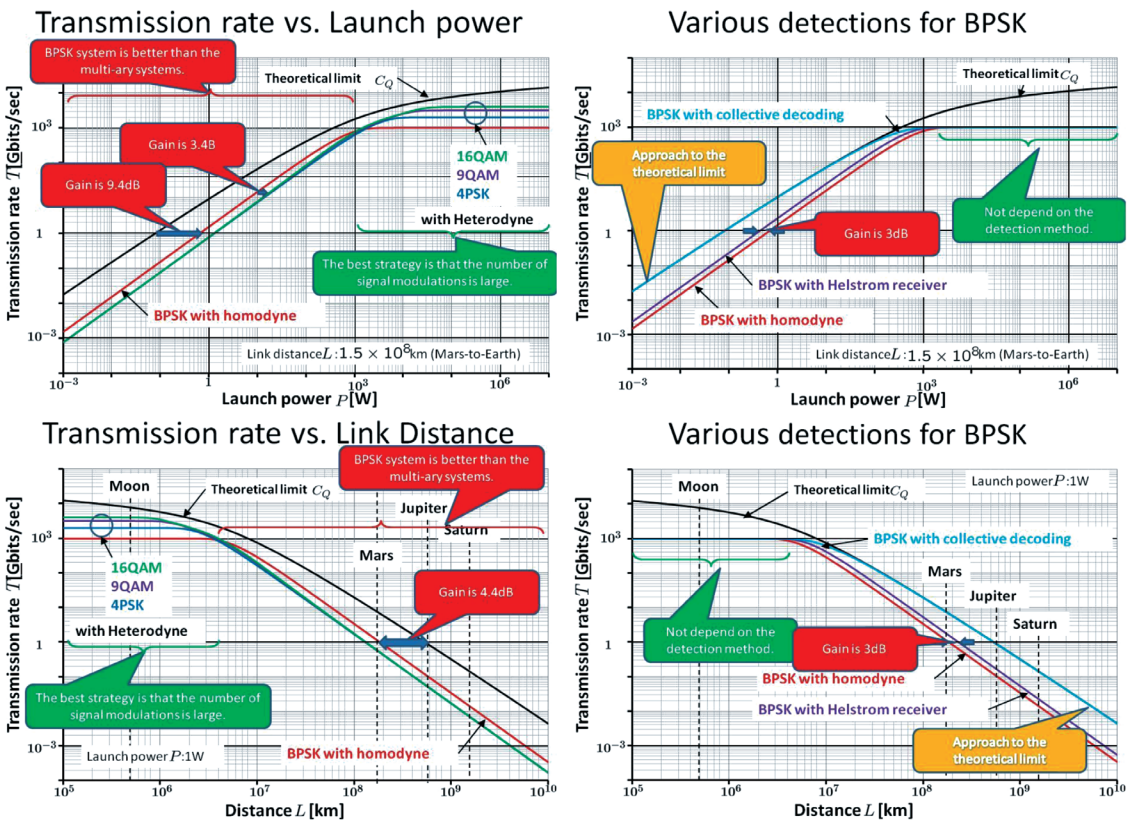

図6　宇宙通信における量子通信路の通信路容量

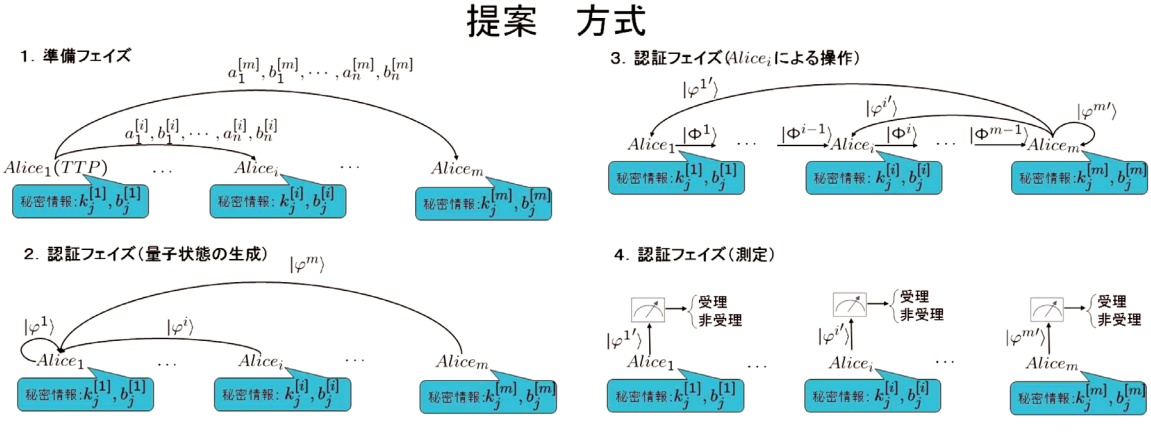

図7　量子複数認証方式

3 まとめ

本論文ではセキュリティ基盤グループが第2期中期計画中に行った量子暗号に関する研究成果の概要やイベントの概要について述べた。これまで述べたように、基盤グループの量子セキュリティに関する研究では、量子ICTグループや宇宙通信ネットワークグループと共同で研究を進めてきている。第3期中期計画では連携プロジェクトなどによって、他の多くの研究室とより親密な関係を構築していき、さらなる相乗効果により研究の成果が発展していくことが期待される。

参考文献

1 http://www.nict.go.jp/publication/NICT-News/0607/research/index.html
2 Douglas R. Stinson,“Cryptography: Theory and Practice, Third Edition,”Chapman and Hall/CRC, 2005.
3 http://www.secoqc.net/
4 http://www2.nict.go.jp/pub/whatsnew/press/h22/101014/101014.html
5 http://www.uqcc2010.org/about/index.html
6 早稲田篤志，双紙正和，宮地充子，“量子複数秘密分散に関する考察,” 情報処理学会論文誌，Vol. 48, No. 7, pp. 2447–2464, 2007.
7 早稲田篤志，高木孝幸，双紙正和，宮地充子，“異なるグループ間における量子秘密分散法の検討,” 暗号と情報セキュリティシンポジウム2008，2008.
8 早稲田篤志，武岡正裕，佐々木雅英，藤原幹生，田中秀磨，“光ファイバー帯域におけるコヒーレント光通信の通信路容量に関する一考察,” 暗号と情報セキュリティシンポジウム2009，2009.
9 Atsushi Waseda, Takayuki Takagi, Masakazu Soshi, and Atsuko Miyaji.“Quantum Secret Sharing between Multiparty and Multiparty against the Attack with Single Photons or EPR-pair,”The 2008 International Symposium on Information Theory and its Applications, Proceedings of ISITA 2008, 2008.
10 Atsushi Waseda, Masahiro Takeoka, Masahide Sasaki, Mikio Fujiwara, and Hidema Tanaka,“Quantum detection of wavelength division multiplexing optical coherent signals,”Journal of the Optical Society of America B-OPTICAL PHYSICS, Vol. 27, No. 2, pp. 259–265, 2010.
11 Atsushi Waseda, Masahide Sasaki, Masahiro Takeoka, Mikio Fujiwara, Morio Toyoshima, and Hidema Tanaka,“Quantum detection of wavelength division multiplexing optical coherent signals in lossy channels,” 2010 International Conference on Availability and Security , Proceedings of ARES 2010, 2010.
12 田中秀磨，佐々木雅英，武岡正裕，藤原幹生，早稲田篤志，“量子秘匿変調方式の安全性に関する一考察,” 暗号と情報セキュリティシンポジウム2010, 2010.
13 早稲田篤志，“複数同時量子認証に関する一考察,” 暗号と情報セキュリティシンポジウム2011, 2011.

（平成23年6月15日 採録）

早稲田篤志（わせだあつし）
ネットワークセキュリティ研究所
セキュリティ基盤研究室専攻研究員
博士（情報科学）
量子セキュリティ