3-2　量子暗号を用いた秘匿通信

3-2 Secure Communication with Quantum Cryptography

長谷川俊夫　西岡　毅　石塚裕一　南部芳弘　富田章久　田島章雄
HASEGAWA Toshio, NISHIOKA Tsuyoshi, ISHIZUKA Hirokazu, NAMBU Yoshihiro, TOMITA Akihisa, and TAJIMA Akio

要旨

量子暗号は物理法則で安全性が保証され、絶対解読不可能な究極の暗号技術として期待されている。三菱電機、日本電気、東京大学の 3 機関は、2001 年から 5 年計画で情報通信研究機構（NICT）委託研究「量子暗号技術の研究開発」を共同で進めており、実用化に向けた開発を行ってきた。研究課題は、単一光子生成技術、単一光子検出技術、乱数発生技術、量子暗号鍵配布システム技術の大きく四つからなる。本稿では、三菱電機、日本電気の取組と成果を幾つかピックアップして紹介する。三菱電機の研究開発では、主に JGN Ⅱ既設光ファイバ網 96 km の長距離フィールド試験について、また、既存のセキュリティと融合した統合量子暗号システムについて紹介する。また、日本電気の研究開発では、商用架空アクセスファイバ 16.3 km で 14 日間以上にわたる長時間連続鍵生成実験と、PLC を用いた一方向量子暗号通信システムの開発について説明する。

Quantum cryptography, which has the advantage of being able to detect eavesdropping on communication channels and security guaranteed by a fundamental physical law, is expected as an absolutely unbreakable cryptography. In 2001, Mitsubishi, NEC and the University of Tokyo started the NICT project "Research and Development on Quantum Cryptography", which includes four research themes: single photon generation, single photon detection, random number generation, and quantum key distribution system. In this paper, we introduce our research activities and some results. In Mitsubishi's part, we report the long-distance field experiment in 96-km installed fiber (JGNⅡ) and the integrated quantum cryptosystem with existing cryptosystem. In NEC's part, we show fortnight continuous key generation field trial over the 16.3-km commercial access fibers and novel backscattering-free unidirectional QKD system based on planar lightwave circuit platforms.

[キーワード]
量子暗号，量子鍵配布，秘匿通信，光子検出，フィールド試験
Quantum cryptography, Quantum key distribution, Secure communication, Single photon detection, Field trial

1　まえがき

量子暗号[1]は、究極の安全性を提供する暗号技術である。一般に現在利用されている暗号技術の多くは、計算量理論に基づき安全性が評価されていて、解読するには膨大な計算量が必要ということを安全性の根拠にしている。このため、現代暗号は将来量子計算機のような超高速計算が実用化すると解読できてしまうという問題があるし、また、盗聴検知できないという課題もある。これに対し量子暗号は物理の基本原理をうまく利用しているため、物理法則で安全性が保証され、この問題点を克服することができる。

本稿では、三菱電機、日本電気、東京大学の 3 機関で進めている量子暗号技術の実用化を目指した NICT 委託研究「量子暗号技術の研究開発」の取組を紹介する。本委託研究では通信波長帯での長距離化／高速化開発など量子暗号の実用化を目

指しており、研究項目は下記のとおり、課題ア〜ウの構成要素技術及びそれらを融合した課題エの大きく四つの柱に関して取り組んでいる。課題エには更に10個のサブ項目に分け、分担して研究を進めている(図1参照)。

課題ア．単一光子生成技術

課題イ．単一光子検出技術

課題ウ．乱数発生技術

課題エ．量子暗号鍵配布システム技術

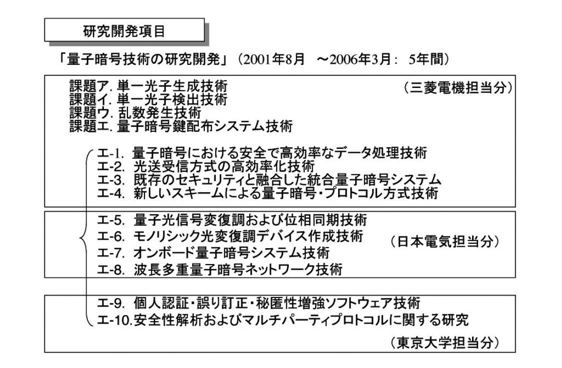

図1 NICT委託研究の開発項目

2 量子暗号の研究開発

2.1 三菱電機の取組

三菱電機は、1999年ごろより研究開発に取り組み始め、2000年の北海道大学と共同での830 nm短波長量子暗号通信システム実験[2]にはじまり、その後2001年からはNICT委託研究「量子暗号技術の研究開発」を日本電気、東京大学とともに進めている。三菱電機は「単一光子生成技術」「単一光子検出技術」「乱数発生技術」とそれらを融合した「量子暗号鍵配布システム技術」の大きく四つを担当し、取り組んでいる。これまでの主な成果は、2002年に通信波長帯1550 nm高性能単一光子検出器(暗計数率 約10^{-6}、検出効率約20 %)を開発[3]、これを用いた87 km長距離量子暗号通信システム実験[3]、2004年には既設ファイバ96 kmを用いて大阪－京都 遠方2地点での量子暗号通信システム実験[4]でその実用性を示したことなどがあげられる。高速化開発では、距離約10 kmで速度数十Kbps程度まで実現し、現在は100 kmで100 kbpsを達成するため開発を続けている。そのほかにも例えば新しい光学スキーム・プロトコル研究では、そのスキームとして「還流型(circular type)量子鍵配布方式」を提案し、従来方式よりも通信速度を高速かつ多人数通信可能な方式の実証実験[5]も行っている。また、展示会に量子暗号装置を出展するなど本技術の普及活動も行っている。例えば2003年にスイスジュネーブ開催の国際展示会ITU TELECOM WORLD 2003、2005年に東京開催のRSA Conference 2005 Japanなどで量子暗号装置を出展デモし、応用アプリケーションとして量子暗号秘匿電話／TV電話の例も示した。本節では、96 kmフィールド試験と、既存のセキュリティと融合した統合量子暗号システムをピックアップして紹介する。

96 kmフィールド試験

フィールド試験環境では、実験室内と比較して、温度変化／振動擾乱、コネクタ接続部の損失／反射などの影響を大きく受ける。これまでフィールド試験例は、スイスのジュネーブ大学が湖底に敷設された67 km光ファイバの実験[6]以外はほとんど行われていなかったのが現状であった。そこで三菱電機では、100 km程度の長距離フィールド試験に適した量子暗号装置を開発し、これを用い、2004年11月に大阪－京都間に敷設されている96 km光ファイバで遠方2地点フィールド試験を実施した。フィールド試験環境を考慮し、前述の点を克服する次の三つの設計方針で開発を行った。(1)柔軟に調整可能な装置パラメータ、(2)遠距離2地点で温度変化／揺らぎ擾乱を吸収し安定動作、(3)小型・軽量で持ち運べる、である。(1)は使用環境に応じ柔軟に対応できるように(通信距離の変更時や、既設光ファイバ途中での予期せぬ反射点の回避の必要がある際)、例えば検出器の印加電圧／パルス幅/遅延時間／デッドタイム設定、駆動周波数も可変(1〜10 MHz)とした。(2)は光トランシーバによる高精度光同期の実現とこれを利用した通信路長変化に応じるタイミング追従である。(3)は主に光子検出器などの小型化である。

図2のようにNICT光ファイバ設備Japan Gigabit Network II(JGN II)を利用し、大阪堂島〜京都けいはんな間96 kmフィールド試験を行った(一部、奈良大安寺での折り返し含む。)。光ファイバ設備は、途中低ノイズ光増幅器を取り外し

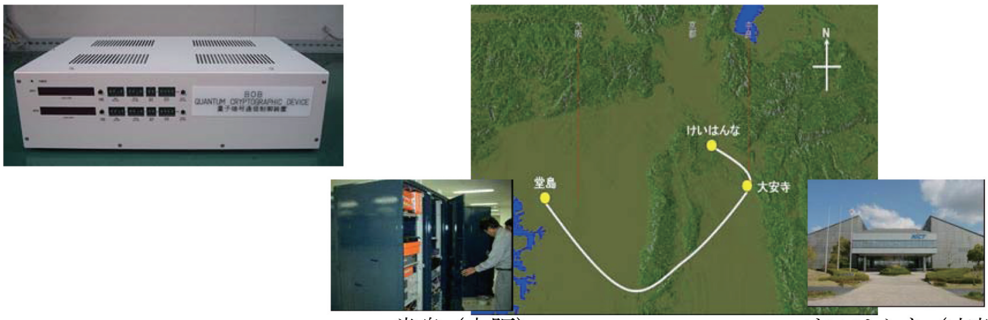

図2　量子暗号装置とフィールド試験を行った地点

Single mode fiber（SMF）で通信路 96 km を構成した。実験では、光学系は改良 Plug &Play 方式[2]－[4]を、プロトコルは BB84[1]を、レーザー繰り返し周波数は 1 MHz、平均光子数はこれまでの実験で通常採用されている 0.1 で行った。検出器は約 200 K に冷却し動作させた。その結果、通信距離 96 km で鍵共有速度 8.2 bps（QBER 9.9％）を達成し、これを用いた秘匿暗号通信が可能なことを確認した。従来は実験室での実験がほとんどであったが、近年、長距離の遠方 2 地点フィールド実験では、Geneva 大学の 67 km 実験[6]、三菱電機の 96 km 実験[4]、中国の 125 km 実験[7]が報告されている。なお、長距離実験では一方向型が適しているが、反射光の影響が大きい往復型方式での実験においては、96 km はフィールド最長距離となる。

既存のセキュリティと融合した統合量子暗号システム

量子暗号では、通信 2 者間で鍵を十分生成共有した後、暗号化したい平文と同じ長さの鍵を用い、One-Time Pad を用いれば、安全性が情報理論的に保証された絶対安全な暗号通信が可能となる。しかし、必要鍵サイズは暗号化する平文サイズと同じため、暗号通信全体では、One-Time Pad の場合、鍵共有速度程度（現状、高々百 K bps 程度）となってしまう。このため、量子暗号をより実用的システムとする応用上の戦略が必要となる。暗号通信速度向上には、(1) 量子暗号の鍵共有速度向上、(2) 現代暗号と融合させ安全性と高速性を両立させる実用的システムの構築、の二つがある。三菱電機は、前者に加え、後者の“既存のセキュリティと融合した統合量子暗号システム”の研究開発を行い、量子暗号の持つ絶対の安全性と現代暗号が持つ高速性を両立させる実用的セキュリティシステムの構築を目指している。既存のセキュリティに量子暗号がすぐに置き換わるのではなく、しばらくは現代暗号と共存すると考えるからだ。このシステムにより量子暗号の実用性を広げ、既存セキュリティインフラへの融合を助長するねらいがある。三菱電機が開発した統合量子暗号システム[3]では、安全性と暗号通信速度をユーザが状況に応じて選択する。すなわち、One-Time Pad に加え共通鍵暗号（DES、MISTY、Camellia、AES 等）も選べ、複数の動作モード（鍵固定、鍵の動的更新、鍵レート固定）も選択可能である。図 3 に PC 画面例を示した。

例えば絶対の安全性を要求する場合、量子暗号と One-Time Pad の組合せで、また、鍵のみ絶対安全に送付し、暗号通信には実用的な安全性で十分という通信速度を優先する場合、量子暗号と共通鍵暗号の組み合わせたシステムとなる。この場合は更にモード選択でセキュリティレベルを詳細設定できる。鍵固定モードは共有した鍵を一定期間固定して動作し、動的更新モードは、量子暗号で共通鍵暗号の鍵長（例えば 128 bit）だけ生成するたびにその鍵を動的に更新する。また、鍵レート固定モードは、更に厳密に、一つの鍵で暗号化するブロック数を設定できる。この場合、レート（ブロック数）を小さくするほど安全性は高くなるが、一般に全体の処理速度は遅くなる。

これらは、量子暗号をいかに既存のセキュリティシステムと融合した実用的なシステムとして使

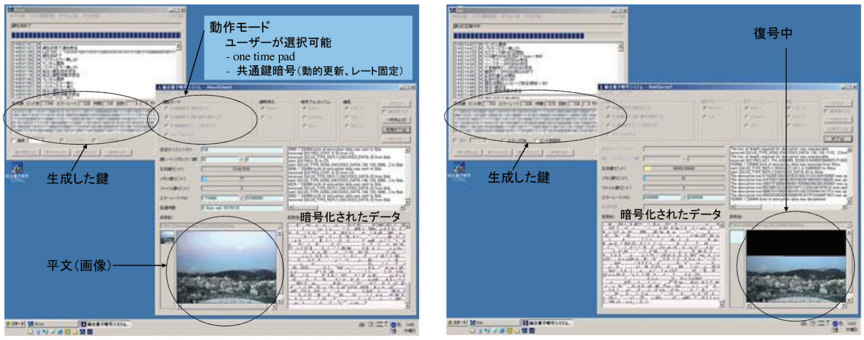

図3 PC画面（左：送信者側での暗号化、右：受信者側での復号）

用していくかという一つの提案となる。また、このシステムで、従来のセキュリティシステムの安全性を量子暗号により向上させるという考え方もできる。

2.2 日本電気の取組

日本電気は1998年に量子情報技術の研究を開始した。当初は絡み合った光子対についての実験的研究や量子暗号プロトコルの理論的研究を主にしていたが、1999年にNEC北米研と量子暗号に関する世界初のワークショップを開催するなど、この分野のプロモーションも積極的に行ってきた。このワークショップでは量子暗号の標準的な安全性証明であるShor-Preskillの方法が初めて公表された。2001年からはNICTより「量子暗号技術の研究開発」を三菱電機、東京大学とともに委託され、量子暗号システムに関する研究を進めている。本研究では特に単一光子の量子暗号伝送技術に注力し、単一光子レベルの信号を安定に変復調する技術をデバイスと装置のそれぞれのレベルで開発した。日本電気が独立行政法人科学技術振興機構とともに開発した高感度の差動型単一光子検出器[8]を利用し、これとモノリシック化した干渉計を組み合わせることにより、量子暗号伝送距離の限界に挑む150 kmファイバ伝送に成功し、100 km超での暗号鍵生成[9]を行った。同時に、メトロネットワークでの実用性を重視して、高速かつ安定に動作する装置[10]開発にも注力した。特に環境変動に対する安定化技術、高信頼化技術、伝送路の遅延時間の変動を補償する高精度自動同期制御システムを開発し、40 kmファイバ伝送後100 kbsの鍵生成に成功した。さらに、このシステムで商用架空ファイバを用いた14日間にわたる自動連続鍵生成にも成功した。さらに、1：多鍵配付や障害時バックアップ切替えによりシステム高信頼化をも達成した。また、NICT研究発表会をはじめとする展示会で本装置の出展デモを行うことにより、量子暗号技術のプロモーション活動を行っている。本稿では、実使用環境下での使用を目指した高速量子暗号通信システムの、14日間にわたるフィールド環境下での運用実証と、高速化・長距離化に向けた平面光回路による単一方向型量子暗号システムの100 km超の秘密鍵伝送を紹介する。

高速量子暗号通信システムの開発

量子暗号技術を活用し暗号化通信システムとして実際に用いるためには、実使用環境下（室内環境下の装置、フィールドの光ファイバ伝送路）において、①長時間安定に単一光子を伝送・受信することと、②光子伝送からシームレスに最終鍵まで生成し続けることが必須である。そこで、(1)

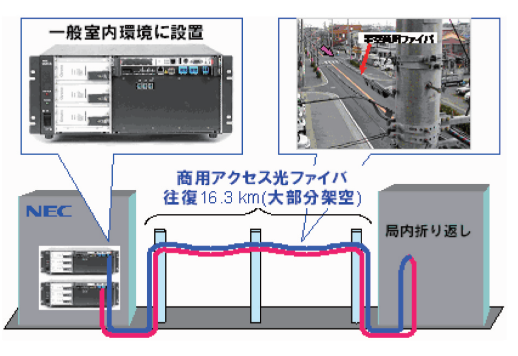

図4 実験イメージ

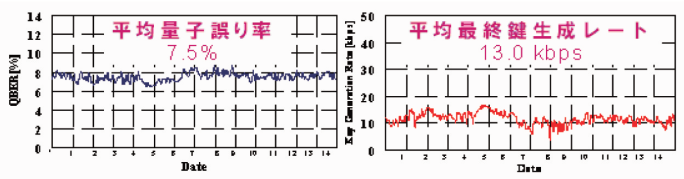

図5 量子誤り率、最終鍵生成レートの推移

実用安定化技術、(2) 連続鍵生成システム技術を開発した[11]。

(1) 実用安定化技術

環境温度に依存しない装置特性と長時間安定動作を実現するための、交互シフト位相変調による温度無依存光干渉技術[12]、広い温度範囲で動作する小型高信頼光子受信モジュール[13]を実現した。

(2) 連続鍵生成システム技術

実使用環境下では、外気温の変化をはじめとする気候変動によって伝送路の遅延が大きく変動する。そのような環境下でも光子伝送からシームレスに最終鍵を生成し続けるために、高精度 bit 同期[14][15]、フレーム同期、異常検出と再同期技術[16]からなる連続鍵生成システム技術を確立した。

(1)、(2) を組み込んだ装置を 19 inch ラックに収容できる (サイズ 480×180×375 mm^3) 形態で実現した。本装置を一般の室内環境下に設置し、アクセスファイバ 16.3 km (区間の大部分は架空) によって接続し、24 時間連続で 14 日間以上にわたる長時間連続最終鍵生成実験を行った。図 4 に実験イメージを示す。実験の結果、無調整で 14 日間以上連続最終鍵を行うことができた。図 5 に示すように 14 日間の平均の量子誤り率は 7.5%、平均の最終鍵生成レートは 13.0 kbps であった。これらより量子暗号システムへの実用性が実証された。

PLC を用いた一方向量子暗号通信システムの開発

Plug &Play システムは、光往復型システムであるがゆえに光ファイバ伝送路中の後方散乱迷光の影響を受けやすく、長距離や高速の鍵伝送には向かない。我々はこの問題をクリア可能な一方向量子暗号システムを、平面光回路技術をベースに開発した[10]。システムは、二つの非対称マッハーツェンダー干渉系平面光回路 (PLC) からなる微弱光干渉系をベースに構成され、二つの PLC をそれぞれ 0.01 ℃の精度で独立に温度制御することにより、光ファイバ中の偏波特性に無依存で 1 時間以上にわたって安定な光干渉を維持する。送信者は二つの位相変調器を用いて鍵情報をエンコードし、受信者は一つの位相変調器と二つの光子検出器を用いて鍵情報をデコードする。事後通信を併用することにより安全な最終鍵を抽出できる。

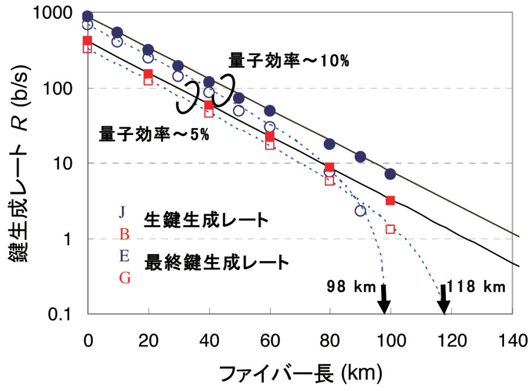

図6 量子暗号鍵伝送評価結果

図 6 は実験室内での伝送評価結果である。光子検出器の検出量子効率が 10 %及び 5 %の場合の鍵生成レートの伝送ファイバ長依存性をセミログプロットされている。シンボル●及び■は共有選別鍵の生成レートを、○及び□は最終鍵の生成レートを示している。選別鍵生成レートはファイバロスによりファイバ長に対して指数関数的に減少する。破線は、別途測定したビットエラー率から算出した最終鍵生成レートのトレンドカーブである。伝送可能距離は量子効率 10 %のとき 98 km であったが、量子効率 5 %とすることで鍵生成レートを犠牲にして検出器の SN を向上でき、118 km に増加させることができた。実験結果よ

り100 kmを超える長距離量子暗号システムへの適用可能性が実証された。

3 むすび

本稿では、2001年から三菱電機、日本電気、東京大学の3機関で進めているNICT委託研究「量子暗号の研究開発」に関して幾つかその取組と成果を紹介した。三菱電機の研究開発では、主にJGN II既設光ファイバ網96 kmの長距離フィールド試験と既存のセキュリティと融合した統合量子暗号システムについて説明した。また、日本電気の研究開発では、商用架空アクセスファイバ16.3 kmで14日間以上にわたる長時間連続最終鍵生成実験と、PLCを用いた一方向量子暗号通信システムの開発について説明した。

本稿では、触れられなかったが、単一光子生成技術では、北海道大学と共同でのパラメトリック・ダウンコンバージョンを用いた通信波長帯の伝令付単一光子源の構築[17]、単一光子検出技術では、APD (avalanche photo diode) デバイスの設計開発を行い、表面リーク電流の抑制方法や検出効率の改善ポイントなど把握し、量子暗号に適したAPDの設計開発を行った。乱数発生技術では、乱数評価システム、擬似乱数生成装置、物理乱数生成装置、システムへの組み込みを実施した。また、誤り訂正や秘匿性増強処理といったデータ処理技術では、三菱電機と東京大学が共同で、LDPC符号を利用した高効率な新しい誤り訂正処理方式の研究と評価を行い[18]、量子暗号装置に実装しその実用性を確認している。安全性に関しては、東京大学が2社の量子暗号装置の評価を行っており、また2006年5月には、三菱電機と日本電気の異種の量子暗号装置の相互接続実験に成功し、ネットワーク化へ前進した。これにより各研究課題及び3機関の成果が統合されることになる。

謝辞

本研究の一部は、総務省「量子情報通信技術の研究開発」の一環として、情報通信研究機構の委託研究「量子暗号技術の研究開発」として実施されました。委託研究を共同で進めています東京大学 今井秀樹教授（現中央大学、産業技術総合研究所）をはじめ関係者の皆様に、また、共同研究しております北海道大学 竹内繁樹助教授に、さらに、実験用にアクセスファイバを借用させていただいた株式会社パワードコム（現KDDI株式会社）に感謝します。

参考文献

1 C.H.Bennett and G.Brassard, "Quantum cryptography: Public key distribution and coin tossing", in Proc. Int. Conf. Computers, Systems and Signal Processing, Bangalore, India 175, 1984.

2 T.Hasegawa, T.Nishioka, H.Ishizuka, J.Abe, K.Shimizu, and M.Matsui, "An experimental realization of quantum cryptosystem", IEICE Trans. Fundamentals, E85-A No.1, 149, 2002.

3 T.Hasegawa, T.Nishioka, H.Ishizuka, J.Abe, M.Matsui, and S.Takeuchi, "Experimental realization of quantum cryptosystem over 87 km", CLEO/QELS2003, QTuB1, Baltimore 2003. T.Hasegawa et al., "Experimental realizatoin of long-distance quantum cryptosystem", SCIS2003, 14D-1, 2003.

4 T.Hasegawa, T.Nishioka, H.Ishizuka, J.Abe, K.Shimizu, and M.Matsui, "Field experiments of quantum cryptosystem in 96km installed fibers", CLEO/Europe-EQEC2005, EH3-4, Munich 2005. T.Hasegawa et al., "Experiments of quantum cryptosystem in 96-km installed fibers", SCIS2005, 2F1-3, 2005.

5 T.Nishioka, H.Ishizuka, T.Hasegawa, and J.Abe, "'Circular type' quantum key distribution", IEEE Phot. Technol. Lett., Vol.14, No.4, 2002.

6 D.Stucki, N.Gisin, O.Guinnard, G.Ribordy, and H.Zbinden, "Quantum key distribution over 67km with a plug and play system", New J.Phys., 4, 41, 2002.

7 X.Mo, B.Zhu, Z.Han, Y.Gui, and G.Guo, "Faraday-Michelson system for quantum cryptography", Opt. Lett. 30, 2632, 2005.
8 A.Tomita and K.Nakamura, "Balanced, gated-mode photon detector for quantum-bit discrimination at 1550nm", Opt. Lett. 27, 1827-1829, 2002.
9 Y.Nambu et al., "One-way Quantum Key Distribution System based on Planar Lightwave Circuits", to be appeared in Jpn. J. Appl. Phys.
10 A.Tajima, A.Tanaka, W.Maeda, S.Takahashi, T.Takeuchi, A.Tomita, and Y.Nambu, "A High-Speed Quantum Cryptosystem", OCS2005-13, 2005.
11 A.Tajima, A.Tanaka, W.Maeda, S.Takahashi, Y.Nambu, and A.Tomita, "Continuous Key Generation Technologies for Practical Quantum Cryptosystems", Proceeding of CPT2006, J-2, pp.191, 2006.
12 A.Tanaka, A.Tomita, A.Tajima, T.Takeuchi, S.Takahashi, and Y.Nambu, "Temperature independent QKD system using alternative-shifted phase modulation method", Proceeding of ECOC2004, Tu4.5.3, 2004.
13 S.Takahashi, A.Tanaka, W.Maeda, A.Tajima, T.Takeuchi, and A.Tomita, "A minimized Photon Receiver for a high-speed quantum cryptosystem", OPE2005-26 LQE2005-25, 2005.
14 W.Maeda, A.Tajima, A.Tanaka, S.Takahashi, and T.Takeuchi, "High-speed QKD system synchronized by automatic phase-alignment mechanism", Proceeding of OFC2005, OWI4, 2005.
15 W.Maeda, A.Tanaka, S.Takahashi, and A.Tajima, "Automatic Installation in QKD System Using Photon-Counting Optical Power Meter", Proceeding of OFC2006, JThB21, 2006.
16 A.Tanaka, W.Maeda, A.Tajima, and S.Takahashi, "Fortnight Quantum Key Generation Field Trial using QBER monitoring", LEOS2005 WM2, 2005.
17 A.Soujaeff, S.Takeuchi, K.Sasaki, T.Hasegawa, and M.Matsui, "Heralded single photon source for quantum cryptography at 1550nm", CLEO/Europe-EQEC2005, EG-10, Munich, 2005. A.Soujaeff, S.Takeuchi, K.Sasaki, T.Hasegawa, and M.Matsui, "Heralded single photon source at 1550nm from pulsed parametric downconversion", to be appeared in J. Mod. Opt. 2006.
18 Y.Watanabe, W.Matsumoto, and H.Imai, "Information reconciliation in quantum key distribution using low-density parity-check codes," in Proceedings of ISITA2004, 1265, 2004.
19 Y.Watanabe, W.Matsumoto, and H.Imai, "Error correction in quantum key distribution using low-density parity-check codes", SCIS2003, 15D-1, 2003. H.Ishizuka, W.Matsumoto, H.Fukushima, T.Shimada, H.Arai, T.Hasegawa, and T.Nishioka, "Evaluation of LDPC code for quantum cryptography", SCIS2004, 2A1-5, 2004.
20 T.Turumaru, "Implementable Quantum Bit-String Commitment Protocol", Phys. Rev. A 71, 012313, 2005.
21 T.Nishioka, T.Hasegawa, H.Ishizuka, K.Imafuku, and H.Imai, "How much security does Y-00 protocol provide us?", Phys. Lett. A 327, 29, 2004.

はせがわとしお
長谷川俊夫
三菱電機株式会社情報技術総合研究所
主席研究員
情報セキュリティ、量子情報

いしづかひろかず
石塚裕一
三菱電機株式会社情報技術総合研究所
主席研究員
情報セキュリティ、量子情報

とみたあきひさ
富田章久
日本電気株式会社基礎・環境研究所
主幹研究員　博士（工学）
量子情報技術

にしおか　つよし
西岡　毅
三菱電機株式会社情報技術総合研究所
主席研究員　博士（理学）
情報セキュリティ、量子情報

なんぶよしひろ
南部芳弘
日本電気株式会社基礎・環境研究所
主任研究員　博士（工学）
量子情報技術

たじまあきお
田島章雄
日本電気株式会社システムプラットフォーム研究所主任研究員
光通信システム