特集論文

高信頼量子暗号装置と量子鍵配送を用いたワンタイムパッド携帯電話ソフトウェア

長谷川俊夫* 酒井康行***
山中忠和*
柴田陽一**

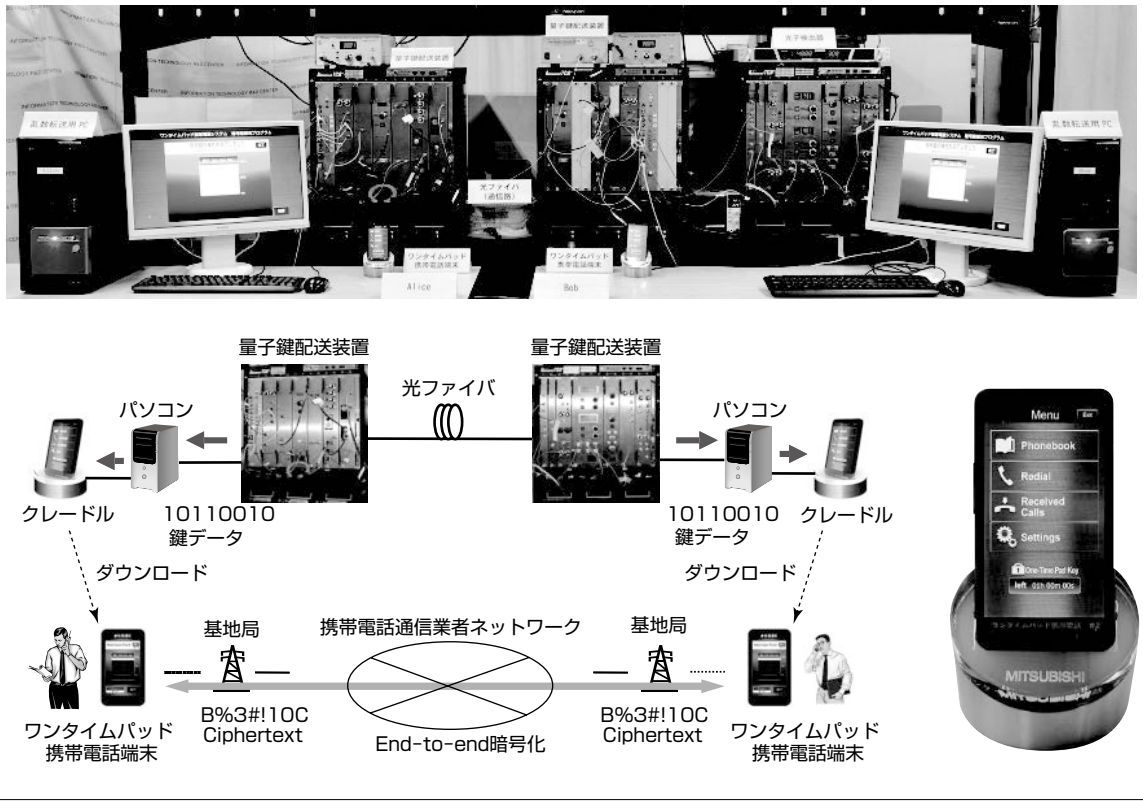
Highly Reliable Quantum Key Distribution System and its Application to One-time Pad Smartphone

Toshio Hasegawa, Tadakazu Yamanaka, Yoichi Shibata, Yasuyuki Sakai

要 旨

量子暗号は，物理の基本原理を利用したもので，物理法則で保証された究極の安全性(暗号の解かれ難さ)を実現する。量子暗号装置の実験や開発はこれまで積極的に行われており，また，理論面でも活発に研究が進められている。量子暗号を実用化するためには，敷設光ファイバ設備(フィールド)でも高い信頼性を実現することが課題である。このため，三菱電機では，量子暗号の実用化を目指して，安定性を高めた量子暗号装置の開発を行い，さらに，フィールド試験を実施した。敷設光ファイバでは，一般に，実験室と比較して伝送路の擾乱(じょうらん)などの影響が大きく，量子暗号装置の安定動作が困難であった。当社では，光伝送路で受ける揺らぎを自動補正することができる偏波補償モジュールを始め，平面光回路を用いて0.01℃の高い精度で温度制御を行うことによって安定動作する干渉計の構築，さらに，−40℃に電子冷却した低ノイズ小型光子検出器等の開発に取り組み，敷設光ファイバでも高い安定性を実現する量子暗号装置を開発した。

また，量子暗号のアプリケーションとして携帯電話(スマートフォン)への適用も行った。量子暗号によって暗号鍵を携帯電話端末間で共有(量子鍵配送)し，この鍵を用いて携帯電話端末間の通話を暗号化するワンタイムパッド携帯電話ソフトウェアを開発した。現状の量子暗号技術では，量子鍵配送自体は通信距離100km程度までしか実現できないが，今回のモバイルアプリケーション開発によって，この距離制限にとらわれず量子暗号技術を展開することが可能となった。これまで，量子暗号は，適用できるアプリケーションが必ずしも明らかではなかったが，１つの身近なアプリケーションを示すことができた。



高信頼量子暗号装置と量子鍵配送を用いたワンタイムパッド携帯電話アプリケーション

上図は，量子鍵配送を用いたワンタイムパッド携帯電話のシステム全体写真である。また，左下図は量子暗号装置からワンタイムパッド携帯電話への鍵のダウンロードの流れと端末間のEnd-to-endの暗号化通信の仕組みである。右下図はワンタイムパッド携帯電話である。

 *情報技術総合研究所 **同研究所(博士(情報学)) ***同研究所(博士(工学))

1. まえがき

量子暗号は，究極の安全性を実現する暗号技術である。現代暗号は，将来，量子計算機のような超高速な計算機が実用化されると解読できてしまうという課題があるが，量子暗号は物理の基本原理を利用したもので，物理法則で安全性が完全に保証されている。量子力学と情報処理を融合した量子情報技術の中でも，量子暗号技術は最も多く実験や量子暗号装置の開発が行われており[(1)(2)(3)]，理論面でも活発に研究が進められている。実用化のためには，敷設光ファイバ設備(フィールド)でも高い信頼性を実現することが必要である。その実現のため，当社は種々の安定化技術を開発し，これを適用した高信頼量子暗号装置の開発を行い，フィールド試験を実施した。

本稿では，量子暗号の実用化に向けた当社の取組みとして，安定性を高めた装置開発とそのフィールド適用について述べる。また量子暗号の1つのアプリケーションとして当社が開発した携帯電話への応用についても述べる。

2. 高信頼量子暗号装置とフィールド適用

2.1 高信頼量子暗号装置の開発

敷設光ファイバ設備では，一般に，伝送路上の温度変化や種々の擾乱によって，伝送される光子の到着タイミングずれや偏光状態の変化が生じる。そのままだと量子暗号装置で量子誤り率(Quantum Bit Error Rate：QBER)が増大し，鍵生成速度が低下又は生成できなくなるなど，安定した鍵生成動作が保証されないことになる。このため，今回，光伝送路での(偏波などの)揺らぎなどを自動補正できる偏波補償モジュールを始め，送受信側で平面光回路(Planar Light Circuit：PLC)を用いて0.01℃の高い精度で温度制御を行うことで安定した干渉計を構築する等，幾つかの技術によって敷設光ファイバでも高い安定性を実現する装置開発を行った[(4)(5)(6)]。その内容について，具体的に述べる。

2.1.1 設計方針

数十km程度の都市圏ネットワークで，実用的な量子暗号装置の実現を目指して設計開発を行った。次の各項目について，設計方針を述べる。

(1) 伝送路損失10dB程度の通信路環境
(2) 高安定性
(3) 高速性(駆動速度100MHz程度)
(4) 波長多重機能
(5) 小型化

(1)に関しては，都市圏ネットワークでの運用を考慮し，通信距離50km程度（光ファイバの損失を0.2dB/km程度として伝送路損失10dB程度)で実用に耐え得ることを目標とする。(2)に関しては，伝送中の偏波揺らぎや温度変化による伝送路の伸縮等の影響があっても安定動作することを目標とする。今回，一方向型の光学系を採用しているが，送受信側で構成する干渉計の安定化を図るため，PLCを用いて高い精度で温度制御することで実現する。(3)の高速性に関しては，100MHz程度で光源，位相変調器，光子検出器の駆動を行う。なお，位相変調では，ダイパルス型の電気信号での制御方式を新たに開発し，DC(Direct Current)フロアの変動なく安定かつ高精度の位相変調を実現する。(4)の波長多重に関しては，量子暗号では一般にタイミング同期のため通常の強度の強い光(古典光)の伝送も同時に行うが，ここで必要となる強度が大幅に異なる光(古典光と微弱光である量子光)の波長分離も実現する。波長分離で100dB程度のチャネルアイソレーションを実現するDEMUX(DEMUltipleXer)装置を開発した。(5)の小型化に関しては，光子検出器は超伝導検出器のように極低温冷却が必要で大型・高価なものではなく，市販APD(Avalanche Photo Diode)を用いた電子冷却可能な温度で動作する小型装置を構築する。また，量子暗号で最終的に安全な鍵を生成するために必要な処理である鍵蒸留処理に関しては，専用ハードウェアを必要とせず，通常のパソコン上のソフトウェア実装で対応できることを目指した。

2.1.2 実験系

量子暗号装置の構成を**図1**に示す。プロトコルは，微弱コヒーレント光を用いたデコイ方式(真空含み4種類の光

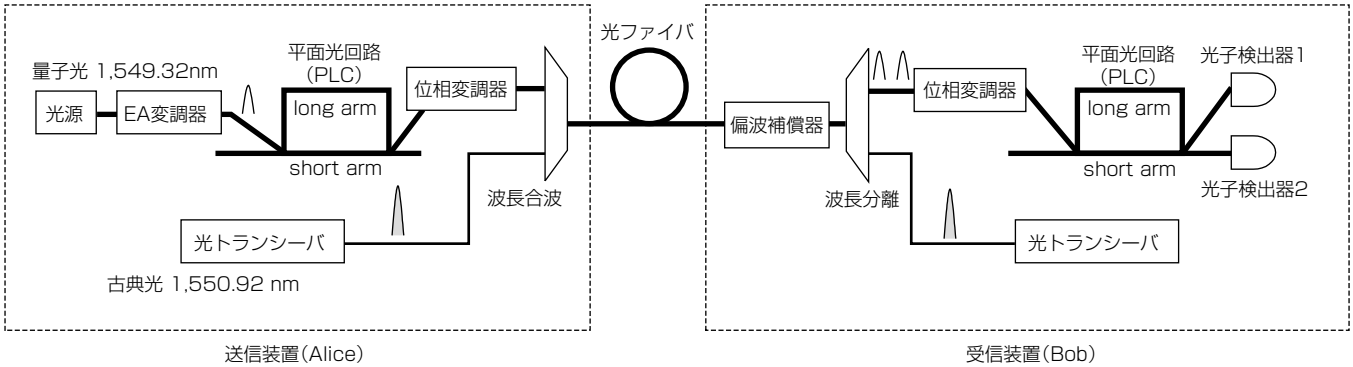


図1．高信頼量子暗号装置の構成図

強度）で実装した。デコイ方式は，基本はBB84方式（BennettとBrassardが1984年に提案した量子暗号の代表的な方式）であるが，送信者Aliceが信号中に“おとり（decoy）光パルス”をある確率でランダムに混ぜて送るものである。今回用いる信号光とdecoy信号の光強度として，パルスあたりの平均光子数μ＝0.63，0.3，0.1，真空を用いた。光源はDWDM（Dense Wavelength Division Multiplexing）DFB（Distributed FeedBack）Laserを用い，100MHzで電気吸収型（EA）変調器を駆動しパルス光としている。量子光波長を1,549.32nm，古典光波長を1,550.92nmとした。光学系は一方向型を採用した。この系では一般に干渉計を安定に保つのが課題であるが，送信側，受信側でPLCを用いることで高精度な温度制御を行い，系全体の安定性を実現した。干渉計は500MHzのものを使用した。

また，タイミング同期のため古典光を量子光に加え波長多重を行う機能と，100dB以上の高いチャネルアイソレーション性能を持つ波長分離モジュールを開発した。さらに，量子光の伝送中の偏波揺らぎなどを補償するために，強度の強い古典光を用いて微弱な量子光の偏波補償を行うモジュールを開発し搭載した。高速性の実現のため，先に述べたとおり，位相変調では，高速かつ安定して変調を行えるよう，ダイパルスによる高速位相変調を行っている。

2.1.3　光子検出器

小型化を重視し，市販のAPDを用いて駆動速度100MHzで動作する光子検出器を開発した。－40℃まで電子冷却し，検出方式は自己差分方式他を用いて実現した。1クロック（今回はT=10ns）ずれた出力波形との差分をとりノイズキャンセルすることで，微弱な光検出信号も効率良く抽出することができる。性能は検出効率数%（3～12%），暗計数率10^{-5}以下（6×10^{-6}）を実現した。

2.1.4　鍵蒸留処理

鍵蒸留処理は，誤り訂正にLDPC（Low Density Parity Check Code）符号を採用し，高い効率を実現した。また，漏洩（ろうえい）情報を無効化する秘匿性増強処理にはToeplitz行列を用い，その実装で高速演算アルゴリズムを用いることで計算量をO（n^2）からO（nlogn）に落とすことができた。これによって，有限長の効果を考慮した場合，ブロック長として1Mビット程度必要となるが，その場合でもFPGA（Field Programmable Gate Array）などの専用ハードウェアが不要であり，通常のパソコン上でのソフトウェア実装だけで高速に実現できた。

2.2　敷設光ファイバ設備JGN2plusへの適用

損失や擾乱が大きい実際の都市圏光ファイバ設備で，開発した量子暗号装置を試験評価することが必要である。今回，（独）情報通信研究機構（NICT）のJGN2plusテストベットの大手町－白山の往復路（距離24km，伝送損失13dB）で，フィールド実験を行った（**図2**）。当初設計では10dB程度の通信路損失に耐え得る量子暗号装置として開発したが，実際のフィールド試験を行った環境は通常の光ファイバよりかなり損失の大きな回線であり，より厳しい条件での試験となった。しかし，この環境下でも，篩（ふるい）鍵生成速度10Kbps，QBER4.5%，最終鍵生成速度2Kbpsの性能を得ることができた。敷設光ファイバ設備では，外気温の変化による顕著な伸縮もあるが，このような環境下でも開発した量子暗号装置が動作することが確認できた。なお，鍵生成速度は通信距離（伝送路損失）とトレードオフにあり，例えば，通信距離10km程度の場合，数十Kbpsとなる。また，この鍵を用いて，日本電気㈱，日本電信電話㈱，NICT等の他機関との鍵リレー及びネットワーク接続実験を行い，正常に動作することを確認することができた[4][5][7]。数日間の連続動作は確認済みであり，今後，更に長期間の連続安定動作を目指す。

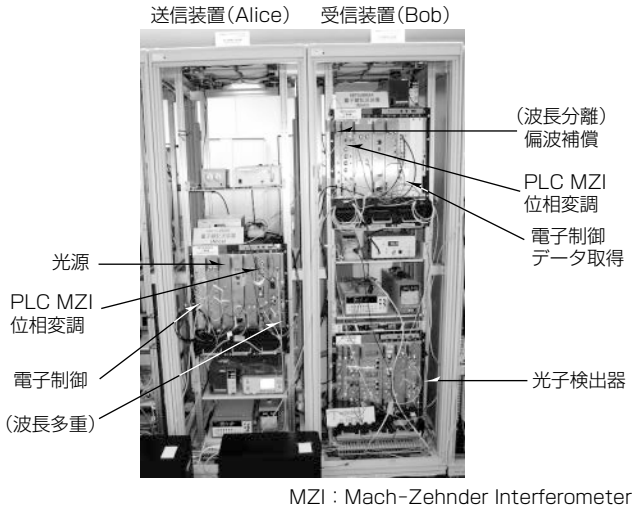


図2．敷設光ファイバ設備での実験

3. 量子暗号のアプリケーション

高信頼量子暗号装置開発に加え，量子暗号のアプリケーションの1つとして携帯電話への適用を図った。

現在の携帯電話では，端末と基地局との間の無線通信区間で，現代暗号を用いて通話を暗号化することによって，盗聴を防止している。しかし，基地局で一旦復号されるため，その先の携帯電話通信事業者が運営する基地局間有線通信区間や事業者間を接続するネットワークで，盗聴される危険性が皆無とは言えない。盗聴を確実に防止するためには，端末で暗号化し相手の端末で復号する方法によって，相対する端末間の全区間で暗号化を行うことが有効である。このような暗号化通信を行うためには，暗号鍵を端末同士で安全に共有する技術が不可欠である。

これらの問題を解決するために，量子鍵配送と携帯電話とを連携させることで，通話の盗聴が原理的に不可能な携帯電話ソフトウェアの開発に成功した[5][6][8][9]。

図3に，今回開発した量子鍵配送を用いたワンタイムパッド携帯電話の仕組みを示す。

①最初に，携帯端末同士で暗号鍵を安全に共有するために，光伝送路(光ファイバ)を使い，量子鍵配送を用いて量子暗号装置間で暗号鍵を絶対安全に共有する。

②次に，この鍵を各々の携帯端末にクレードル経由でダウンロードし，携帯端末間で暗号鍵を共有する。

③最終的に，通話の際に，携帯端末上でこの暗号鍵を用いて音声通話をワンタイムパッドで暗号化する。これによって，端末間の全ての区間でEnd-to-endの秘匿通話が実現できる。

このアプリケーションの詳細は次のとおりである。

音声通話は，データ通信(VoIP(Voice over Internet Protocol))を利用し1KB/sでエンコードしている。音声通話の暗号化は，ワンタイムパッド暗号を用い，音声データと同じ長さの暗号鍵を用いて暗号化する。このため，一般には長いデータサイズの鍵が必要となる。

例えば，10分間の通話では，1.2MBの暗号鍵を事前に共有する必要がある。ワンタイムパッド携帯電話端末は，ダウンロード時にワンタイムパッド用の暗号鍵を補充するが，例えば，2GBのSDカードがあれば，1回の鍵のダウンロードで10日間連続通話可能となる。これは運用上，十分実用的と考えられる。

ワンタイムパッド方式はデータと同じ長さの乱数を鍵として使用し，一度使った鍵は二度と使わないというものである。通話の暗号化に用いる暗号鍵を使い捨てにすることによって，万一端末を紛失したり盗まれたりした場合でも，過去の通話記録からの復号は不可能である。このように，このワンタイムパッド携帯電話ソフトウェアでは，端末の紛失・盗難対策が厳重にほどこされている。

今回，ワンタイムパッド携帯電話ソフトウェアは，Microsoft Windows Mobile(注1)を搭載した端末上のソフトウェアとして開発したため，特定のハードウェアに依存しない。このため，このOSを搭載した様々な携帯端末で利用可能である。

また，現状では，量子暗号装置は通信距離が100km程度までであり，通信距離に制約がある。さらに，量子鍵配送では大規模な量子暗号装置が必要であるため，一般にこの装置を利用できる場所は限られる。しかし，このアプリケーションを用いることによって，これまで存在していた量子暗号装置の通信距離の制限や場所の制約等の課題を克服し量子暗号の究極のセキュリティがどこにいても利用できることになる。

(注1) Windows Mobileは，Microsoft Corp. の登録商標である。

4. むすび

当社の量子暗号の実用化に向けた取組みとして，安定性を高めた量子暗号装置開発とそのフィールド適用について述べた。また，量子暗号のアプリケーションとして，当社が開発した携帯電話向け応用ソフトウェアについて述べた。

装置開発では，実用化のために，フィールドでも高い信頼性を実現することが必要である。その実現のために，種々の安定化技術を開発し，これらを適用した高信頼量子暗号装置開発を行い，フィールド実験を実施した。また，量子暗号を実際に活用するためには，有用なアプリケーションが必要であるが，携帯電話への応用について初めて取り組んだ。当社では，量子暗号などの研究開発だけでなく，“MISTY”などの現代暗号を始め情報セキュリティ分野で様々な開発を行ってきた。これらの経験やノウハウ等が，量子暗号を身近な携帯電話(スマートフォン)に応用すると

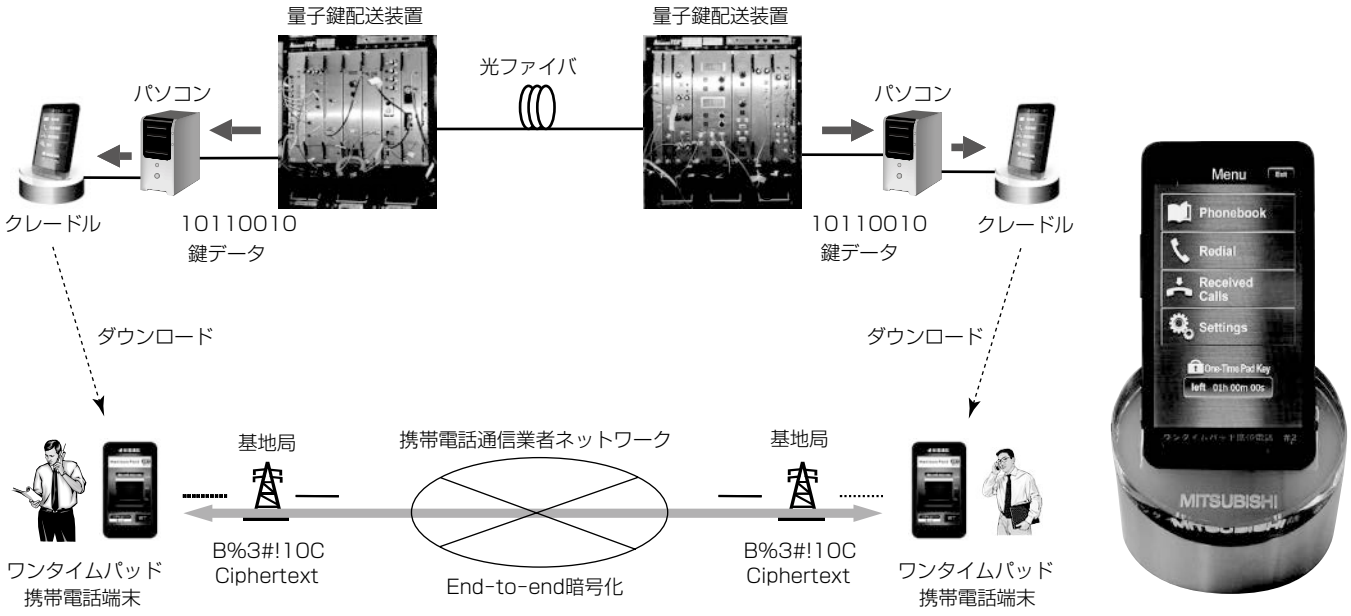


図3．量子鍵配送を用いたワンタイムパッド携帯電話の仕組み

いう今回の開発につながった。

量子暗号の実用化には，まだ解決しなければならない課題が幾つかある。ハードウェア面では量子暗号ネットワーク試験運用プロジェクトのフィールド試験で安定した通信を実現することができたが，量子暗号装置の光子検出器の性能改善や，伝送路のゆらぎを補償する偏波補償やフィードバック制御等によって，速度や通信距離・安定性の更なる向上に今後も取り組む予定である。また，ワンタイムパット携帯電話ソフトウェアについては，最新スマートフォンOSへの対応を進めるほか，“いつでもどこでも安全に通話できる”という理想の通信環境を実現するために，研究開発及び改良を進めていく予定である。

なお，この開発の一部はNICT委託研究の成果である。

参考文献

(1) Hasegawa，T.，et al.：Field experiments of quantum cryptosystem in 96km installed fibers，CLEO/Europe-EQEC2005，EH3-4，Munich（2005）
(2) 長谷川俊夫，ほか：宇宙量子暗号通信の概念検討，第52回宇宙科学技術連合講演会 2F03（2008）
(3) 長谷川俊夫，ほか：宇宙量子暗号通信ミッションの予備設計，第53回宇宙科学技術連合講演会 3D14（2009）
(4) 長谷川俊夫，ほか：高信頼量子暗号装置の開発，SCIS2011，4F2-6 量子セキュリティ（2011）
(5) Sasaki，M.，et al.：Field test of quantum key distribution in the Tokyo QKD Network，Optics Express，**19**，No. 11，10387～10409（2011）
(6) 長谷川俊夫，ほか：高信頼量子暗号装置の開発とアプリケーション，第58回応用物理学関連連合講演会シンポジウム，24a-BT　量子情報：高まる技術と深まる科学，4（2011）
(7) 三菱電機プレスリリース 2010.10.14：量子暗号ネットワークの試験運用開始（2010）
http://www.mitsubishielectric.co.jp/news/2010/1014-a.pdf
(8) 柴田陽一，ほか：ワンタイムパッド携帯電話システムの開発，第74回情報処理全国大会 1F-4（2012）
(9) 三菱電機プレスリリース 2010.09.02：量子鍵配送を用いたワンタイムパッド携帯電話ソフトウェアを開発（2010）
http://www.mitsubishielectric.co.jp/news/2010/0902.pdf