

プレスリリース  
平成 22 年 9 月 2 日  
三菱電機株式会社  
独立行政法人情報通信研究機構

## 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 ～世界初、通話の盗聴が不可能であることを物理学的に保証した携帯電話ソフトウェア～

三菱電機株式会社（以下「三菱電機」という。執行役社長：山西 健一郎）と独立行政法人情報通信研究機構（以下「NICT」という。理事長：宮原 秀夫）は、量子鍵配送を用いることにより、携帯電話端末（以下「端末」）間の通話の盗聴が不可能なことを物理学的に保証した、ワンタイムパッド携帯電話ソフトウェアを開発しました。光回線を使い量子鍵配送で 2 者間に暗号鍵を配り、通話者はそれぞれの量子鍵配送装置から携帯電話に暗号鍵をダウンロードして暗号通信を行います。通話の暗号化に用いる暗号鍵は使い捨てにすることにより、万一端末を紛失したり盗難されたりした場合でも、過去の通話記録を解読されません。

なお、本開発の一部は NICT 委託研究「量子暗号の実用化のための研究開発」（平成 18～22 年度）の成果です。

### 【背景】

現在の携帯電話は、端末と基地局との間の無線通信区間を暗号化して盗聴を防止していますが、基地局で一旦復号された後、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において盗聴される可能性があります。

確実に盗聴を防止するには、端末で暗号化し相手方端末で復号する方法により、相対する端末間の全区間で暗号化を行うことが有効ですが、こうした暗号化通信を行うためには、端末同士で暗号鍵を安全に共有する技術が不可欠です。

今回、量子鍵配送を用いて暗号鍵を端末間で共有し、この暗号鍵を用いて端末間の全ての区間で通話を暗号化する携帯電話ソフトウェアを開発しました。量子鍵配送と携帯電話とを連携させることにより、通話の解読が原理的に不可能な携帯電話ソフトウェアの開発は世界で初めてです。

### 【今回の成果】

#### 1. 量子鍵配送を用いて暗号鍵を共有、ワンタイムパッド暗号により音声暗号化、解読不可能な通話を実現

通話を暗号化するための暗号鍵の共有を、量子鍵配送を用いて実現しました。量子鍵配送は盗聴を即座に検知することが可能であり、物理学の基本法則により乱数を安全に共有できることが保証されています。暗号化には量子鍵配送で共有した乱数を暗号鍵として使用します。また、暗号鍵には暗号化する前のデータと同じ長さの鍵を使用し、さらに一度使った暗号鍵を二度と使わないワンタイムパッド暗号方式を用いており、通話音声を暗号化する機能を、端末上で動作するソフトウェアとして開発しました。

#### 2. 暗号鍵を使用後すぐに消去することにより端末の紛失・盗難に対するリスクを回避

暗号鍵は、使用後ただちに端末から消去するようにしました。したがって、端末間の区間で通話を記録されていた場合でも、暗号鍵は残っていないため、過去の会話を解読される心配がありません。

### 【今後の展望】

今後 3～5 年後を目処に、本ワンタイムパッド携帯電話ソフトウェアの実用化を目指します。

成果の詳細内容は、2010 年 10 月 18 日(月)～20(水)に ANA インターコンチネンタルホテル東京にて開催される NICT 他主催の量子暗号・量子通信国際会議 UQCC2010 においてデモ展示する予定です。

<本件に関する 問い合わせ先>

三菱電機株式会社 広報部

独立行政法人 情報通信研究機構 総合企画部 広報室

TEL : 03-3218-2333

TEL : 042-327-6923

## 【開発内容の補足】

### (1) 量子鍵配送により暗号鍵を共有

「量子鍵配送」は、解読が不可能な鍵共有機能を実現します。「現代暗号」と呼ばれる現在の暗号技術は、盗聴された暗号化されたデータの解読に膨大な計算時間が必要であることを安全性の根拠にしています。このため将来超高速な計算機が出現した場合には、安全性が脅かされることが指摘されています。これに対し量子鍵配送は、光子を利用してデータを運ぶもので、盗聴されたことを必ず検出できるという特長があることから、絶対に解読されない究極の暗号として実用化が期待されています。

### (2) ワンタイムパッド暗号により通話内容を全区間で暗号化

「ワンタイムパッド暗号」は、暗号化対象のデータ(通話内容)と同じ長さの乱数を暗号鍵として暗号化し、さらに一度使用した乱数は二度と使わないようにする暗号方式です。ワンタイムパッド暗号は、解読が不可能であることが情報理論の創始者である C. D. Shannon により数学的に証明されています。今回開発した携帯電話ソフトウェアは、乱数を量子鍵配送により共有し、共有した乱数を暗号鍵として端末同士の通話内容をワンタイムパッド暗号方式で暗号化します。一方の端末で通話内容を暗号化し、他方の端末で復号するため、経路上での盗聴を確実に防止できます。暗号化された通話内容は、携帯電話通信事業者が提供するデータ通信サービスを利用して端末間で交換します。

### (3) ソフトウェアによるワンタイムパッド携帯電話の実現

ワンタイムパッド携帯電話は、Microsoft® Windows Mobile®を搭載した端末(スマートフォン)用のソフトウェアとして実現しています。Microsoft® Windows Mobile®を搭載したさまざまな市販端末で利用することができます。

### (4) 量子鍵配送装置からの乱数の供給と端末の紛失・盗難対策

今回開発したワンタイムパッド携帯電話ソフトウェアでは、音声データと同じ長さの暗号鍵で暗号化するため、長い暗号鍵を必要とします。例えば二者間の通話内容を10分間暗号化するために1,200,000バイトの暗号鍵を事前共有しておくことが必要となります。ワンタイムパッド携帯電話端末は、暗号鍵転送用PCを介して量子鍵配送装置と接続した際に、量子鍵配送を用いて共有した乱数をワンタイムパッド用の暗号鍵として補充します。また、ワンタイムパッドに使用する暗号鍵は、一回限りの使い捨てとし、暗号化または復号処理が終了した時点で端末から消去します。従って、端末の紛失や盗難が発生した時、端末から抜き出した暗号鍵を用いて、傍受しておいた暗号化通話内容を復号するという盗聴を不可能としています。

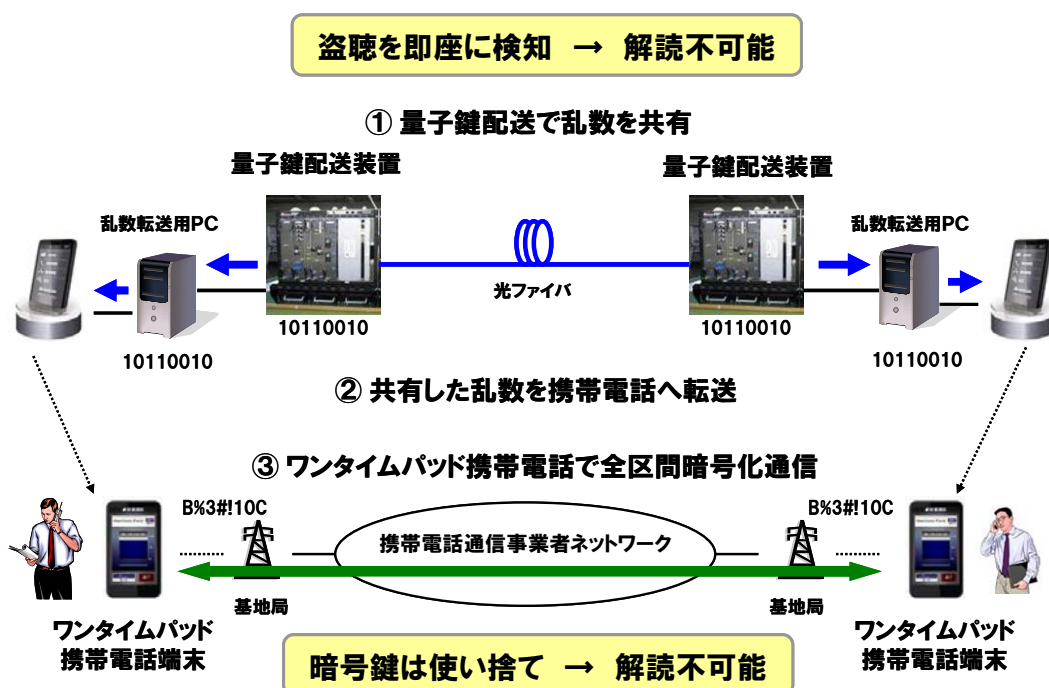


図1 量子鍵配送を用いたワンタイムパッド携帯電話による秘密通信

## 【商標関連】

Microsoft、Windows Mobile は米国 Microsoft Corporation の米国およびその他の国における商標または登録商標です。