HITACHI
Inspire the Next

News Release

2018 年 3 月 13 日
株式会社日立製作所

ランダムなノイズを利用して高い安全性を実現する暗号通信装置を試作

理論上解読が不可能なレベルで長距離の暗号通信が可能に

試作したセキュア通信装置。本体（右）及びノイズ発生器（左）からなる。

株式会社日立製作所(執行役社長兼 CEO:東原 敏昭／以下、日立)は、LAN ケーブルでインターネットに接続された環境において、事実上暗号解読が不可能なほどの高い安全性を実現する暗号通信技術を開発し、本技術を搭載した通信装置を試作しました。本装置では、送信機内にノイズ発生器を設置し、ランダムに発生するノイズを暗号通信に必要なデータに加えて送信することにより、ノイズの除去方法を知っている正規受信者以外の暗号解読を困難にします。さらに、量子暗号通信で必要となる光ファイバーなどの特定の伝送路が不要となり、LAN ケーブルで接続された世界のあらゆる地点への通信が可能です。日立は、今後、本技術を高いセキュリティが要求されるエネルギー、金融、鉄道管理、防衛などの分野へ適用し、安心・安全な社会の実現をめざします。

IoT[*1] の進展に伴い情報セキュリティ対策の重要性が増す中、現在、秘匿性の高いデータをやり取りする際には暗号通信が行われています。しかし、一般的に利用されている共通鍵暗号方式[*2] では、データの暗号化を共通鍵と呼ばれる一つの鍵で行っているために、共通鍵に起因する規則性が見破られ、不正に暗号が解読されてしまうリスクがあります。また、量子光を利用したいわゆる量子暗号方式では、安全性は極めて高いものの、光ファイバーなどの特定の伝送路で PtoP[*3] で直結されている必要があり、さらに伝送路中の光の散乱などにより信号の減衰が生じることから、伝送可能距離が 100 km 程度に制限されてしまう問題がありました。

そこで日立は、ランダムなノイズが予測できないことに着目し、ノイズによりデータを保護する仕組みを構築して、理論上、宇宙年齢(138 億年)をかけても暗号解読ができないほどの安全性を有すると同時に、LAN ケーブルでインターネットに接続されたあらゆる地点への通信が可能な暗号通信技術を開発し、本技術を搭載した通信装置を試作しました。試作した装置の特長は以下の通りです。

1.　共通鍵とランダムに発生するノイズを加えた乱数を用いることで安全性を向上

本通信技術では、まず、予め送受信者間で共通鍵を共有します。そして、送信者は、データ(メッセージ)の送受信に先立ち、任意の乱数を、共通鍵をパラメータにして変換(誤り訂正符号化*4)し、さらにランダムなノイズを加えることで意図的にエラー(ビット誤り)を含んだ状態にして受信者に送信します。続いて、送受信者は双方で送受信した乱数から秘密鍵を生成し、その秘密鍵を使ってメッセージを暗号通信します。このとき、受信者側にあるエラーを含んだ乱数(誤り訂正符号化されている)は共通鍵を使ってノイズが除去された状態で復号(符号化の逆処理。誤り訂正符号では復号時にエラーが訂正される)されておりエラーは訂正済みです。第三者が暗号化されたデータ(乱数及びメッセージ)を傍受してメッセージを解読するためには、秘密鍵を推定する必要がありますが、傍受した乱数を元に推定しようとしても、共通鍵を持たない第三者は誤り訂正符号を復号できないために、エラーを訂正できず秘密鍵の推定ができません。また、暗号化されたメッセージを元に秘密鍵を推定しようとしても、秘密鍵には共通鍵に起因する規則性がないために推定することができず、結局、共通鍵の全数探索が必要となり、事実上暗号解読が不可能なほどに安全性が向上します*5。

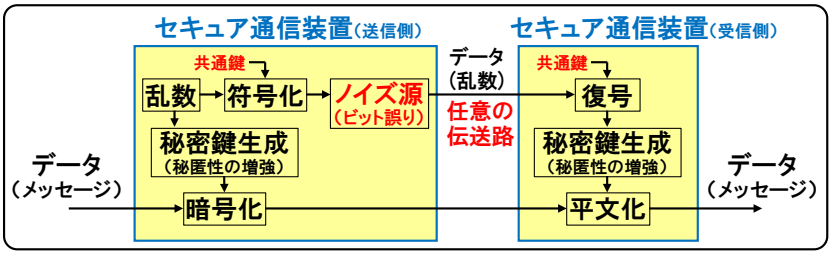

図. 試作したセキュア通信装置におけるデータの通信手順

2.　ノイズ発生器を送信機内に設置し、デジタル信号化により特別な伝送路を不要に

本技術では、データ(メッセージ)の送受信に先立って送信される乱数に加えるノイズが大きいほど効率的に安全性を確保できますが、その一方で正規受信者が除去可能な範囲にノイズを設定する必要があります。そこで、本試作機では光の位相揺らぎを利用した理想的なノイズ発生器を送信機内に設置し、ノイズの大きさを制御可能にしました。また、これにより伝送路に特別に要求される性質がなくなり、ノイズを加えた乱数を通常のデジタル信号として送受信できるようになったため、光ファイバーなどの特定の伝送路が不要になりました*6。本試作機は LAN ケーブルを接続するだけで、伝送距離の制限なく暗号通信が可能です。

オープンネットワークを介して本試作機の通信実験を行い、乱数及び暗号化されたメッセージが一般の伝送路を介して送受信可能なことを確認しました。今回の試作機では共通鍵の長さは 1900 ビットであり*7 全数探索数は 10^{572} となり、宇宙年齢の 138 億年(4.4×10^{17} 秒)を使っても解読が困難なレベルの安全性を実現しました*8。

日立は、今後、本技術を高いセキュリティが要求されるエネルギー、金融、鉄道管理、防衛などの分野へ適用し、安心・安全な社会の実現をめざします。なお、本成果は、2018 年 3 月 17 日から早

稲田大学で開催される「第 65 回応用物理学会春季学術講演会」において発表する予定です。

本研究は、2016 年 3 月終了の文部科学省先端融合領域イノベーション創出拠点形成プログラム「ナノ量子情報エレクトロニクス連携研究拠点」(東京大学)において遂行された研究をその後発展させたものです。

*1 IoT: Internet of Things
*2 共通鍵暗号方式:暗号化と復号化に同一の(共通の)鍵を用いる暗号方式。
*3 PtoP: Point to point
*4 誤り訂正符号:誤り訂正符号はデータを冗長にしてエラーがあった場合にそれを検出及び訂正する技術。本発表の技術では共通鍵を符号化における一つのパラメータとして利用する。よって、復号時にも共通鍵は必須である。
*5 本技術では乱数のエラー訂正、よって符号化が必須である。*4 で記載のように共通鍵はその際の一つのパラメータとして利用する。データ(メッセージ)の暗号化には直接利用しない。本技術において共通鍵に起因する規則性がないのはこの仕組みにも拠る。詳細は arXiv に掲載予定。タイトル:Secret Key Generation from Channel Noise with the Help of a Common Key。
*6 量子暗号では伝送路上において量子光の性質を利用する。
*7 暗号における安全性の高さは、暗号の仕組みと共通鍵の長さに依存する。1900 ビットは解読耐性を示すための有効鍵長であり、試作機における実際の鍵長は 2496 ビットである。
*8 例えば、1 GHz のレートで共通鍵候補の探索が可能なコンピュータを 100 億台使って 138 億年の間共通鍵候補を探索したとすれば、調べられる候補数は 4.4×10^{36} であり、10^{572} と比べると桁違いに小さい。

■照会先

株式会社日立製作所 研究開発グループ 研究管理部 [担当:小平、安井]
〒185-8601 東京都国分寺市東恋ヶ窪一丁目 280 番地
電話:042-323-1111(代表)

以上