特集

ゆらぎと雑音

「Absolutely Secure Communications by Johnson-like Noise and Kirchoff's Laws」の日本語概要

JL 0004/10/4904–0217

1. はじめに

本文章は Laszlo B. Kish 先生の解説論文「Absolutely Secure Communications by Johnson-like Noise and Kirchhoff's Laws」について概要を記したものである．この論文では，ジョンソンノイズ (熱雑音) を利用したセキュアな通信システムについて説明している．ここではセキュア通信についての概要およびセキュア通信の 1 つである量子通信について述べられている 2 章および提案手法である KLJN システムについて述べられている 3 章についての説明を行う．

2. 物理法則を利用した鍵交換

現在のソフトウェアベースのセキュア通信 (たとえばわれわれがインターネットを介して銀行に接続する際に用いるソフトウェア) においては，安全なデータ交換を行うことができる前に，2 つの通信者 (Alice と Bob) は，暗号化鍵を生成し，盗聴者 (Eve) が監視しているであろう通信チャネルを通して，それを共有する必要がある (**図 1**)．このような状況下において Alice と Bob のみが鍵を共有することは現在のソフトウェアによる手法では数学的には不可能であり，通信チャネルから得られるデータは Eve にも同様に得られる．そのため，この鍵生成・共有のプロセスは，Eve がデータを解読することができるが，その解読に時間がかかりすぎるという意味であるところの「計算論的に安全」でしかない．それゆえ，仮に Eve が真に強力な解読アルゴリズムを持っているか，あるいは標準的なアルゴリズムであるが十分に高速なコンピュータを持っていれば，彼女は秘密鍵を手に入れ，通信データを解読することができる．新たなアルゴリズムや計算方法が常に研究されているため，現在のソフトウェアベースのセキュア通信は時限爆弾である可能性がある．

量子鍵配送 [8)~10)] は無条件にセキュアであるといわれる解決策を提供している．情報ビットは単一のフォトンにより運ばれている (**図 2**)．ここでは，「複製不能定理」が通信の安全における理論的基礎である．これが意味しているのは，単一のフォトンはノイズ (エラー) なしでは複製しえないということである．もし Eve がフォトンを捉え測定したとすると，このフォトンは破壊され，Eve はこのフォトンを再生成しチャネルに再投入しなければならない．さもなければこのビットは Alice と Bob からは無効であるとみなされてしまう．しかしながら，この複製不能定理により，Eve がフォトンの捕捉・計測・再投入を行う一方ノイズが入ってしまうので，チャネルのエラーレートは盗聴を行わない場合よりも大きくなる．それゆえ，エラー統計を評価することにより，多くの送信ビットとそのエラーを解析した後に Alice と Bob にはある確率で盗聴が行われていることがわかる．しかしながら，量子通信は Eve がチャネルを切りその間に 2 つの量子通信機を入れるというような中間者攻撃 (man-in-the-middle-attack) に対してはセキュアではない．この場合，Eve は Bob と偽って Alice と通信し，一方では Eve は Alice と偽って Bob と通信をする．これは 1 つの例であるが，つぎの章にて説明するセキュアワイヤ通信機は量子暗号よりも優れている．

多くの量子通信機が繰り返し作られており，規模としては，200 km のモデル通信線 (東芝・NEC) であり，またビット交換率は 0.25 ビット/秒未満である [10)]．これらの多くは光ファイバー上で動作しており，最も高度かつセキュアなものは無線により通信可能である．しかしながら，異なる暗号破りのアイデアを実際に実験することは，通信機そのものを作るよりも高価になる．そのため，今日の量子通信を破るさまざまな試みはほとんど理論的なものであり，提案された暗号破りの手法に関する理論のみの論文は数多くある．これは，たとえば現存するプロトタイプに対して必要な実験は約 10%程度しか行われておらず (量子チャネルに割り込む理論的な方法は多く存在するため)，残りの 90%については，テストを行うことならびにそのテストに基づいた改良であるが，量子デバイスを大規模に商用化する前になされなければならない．

3. 古典熱力学に基づいたセキュア通信機

近年，無条件にセキュアである古典物理的な通信方法であるキルヒホッフ則ジョンソン (状) ノイズ (Kirchhoff-Law-Johnson-(like)-Noise; KLJN) 通信機が提案されており [1)~3),11)]，これは量子通信機と統計的・物理的に競争相手となるものである．「受動的な攻撃」(受動的な電圧・電流

の測定) に対するセキュリティは熱力学第二法則，すなわち第二種永久機関を作ることが不可能であること，に基づく．「能動的な攻撃」(チャネルに電流を注入したり取り出したりする行為) に対するセキュリティは古典的な物理情報の頑健性，すなわち電流や電圧のデータは常に観測することができるということ，に基づく．KLJN システムは 2 組の同一の抵抗のペアから構成される．Logic Low (L) と Logic High (H) の抵抗 R_0 と R_1 は各クロック周期の開始時にはランダムに選ばれ，それぞれのジョンソンノイズ (熱雑音) 電圧あるいは電子的に強調したノイズ (ジョンソン状ノイズ) にて通常の温度で駆動される．実際の実装はファイバーや振幅制御装置などのより多くの要素を含む．暗号鍵は両端の抵抗値が異なる時に生成・交換される．

ジョンソン (状) ノイズの役割は，R_0 や R_1 の実際の場所に関する情報を Eve に提供せずに回路中の総抵抗値を決定することである．回路の抵抗値がわかり (この情報は公になっている)，それが R_0 と R_1 の和である時に，Alice と Bob はそれぞれ自身の抵抗の値から他方の抵抗値を計算することができる．

KLJN 暗号機は中間者攻撃に対しても**図 4** に示すように防御することができる [11]，また同様にして能動的な盗聴についても即座に (単一のビットを送信するのに要する時間よりも短い時間で) 検出することができる [1),11)]．ビットエラーの統計量は不必要である．単一のビットの通信もセキュアである．

上記の量子通信および物理通信が無条件にセキュアであるという主張は理想化したシステム (数学的なモデルのレベル) 上でのことである．実際の実装は理想的ではないし，さまざまな寄生効果や要素が存在する．それゆえ，実装においては，量子通信や KLJN システムは完全にセキュアではない．しかしながら，数学モデルを知ることによりそのセキュリティや他の性能を物理的・経済的な限界に応じて設計することができる．セキュリティに関する究極的なテストは実験的でなければならない：セキュア通信機を販売する前にはすべての既知の解読手法によりテストされなければならない．

文献 12) において指摘されているのは，チャネルの両端において継続的に電圧・電流を監視し，比較することにより Alice と Bob は，Eve が推定しているであろう情報を常に知ることができるということである．これにより，Alice と Bob は Eve が鍵ビットを推定している時にそれが正しいか誤っているかを正確に知ることができる．この特徴は KLJN システムが持つユニークな特徴である．

文献 13) においては，Point-to-Point のシステムではなく鎖状の KLJN ネットワークにおいて高速に鍵を生成・共有することができる手法が開発されている．

KLJN 暗号機についてはそれを破る試みが存在する：文献 14) およびその回答 [15),16)] およびその回答 [17,18)] およびその回答 [12)]．しかしながら，これらのすべてが (正しい提案ではないものも含まれるが)，理想システムからの情報の取り出しを行えない．文献 14) および文献 16) では理想化されていないために生じる少量の情報漏れを利用しているが，これは理想化された状況に近づけるように設計することにより (リソースに依存して) 減少させることができる．残っている情報漏れについては量子通信機においても同様の目的で利用されている privacy amplifier と呼ばれるソフトウェアにより除去することができる．これらの他に前述の Alice と Bob が Eve の推定が正しいか誤っているかを常に知ることができるという特徴もまた防御に利用することができる [12)]．

最後に文献 18) において提唱されているクラッキング方法は，ケーブルの直径に対応したインピーダンスが既知の宇宙の大きさの 28000 倍であるというような物理的でない想定に基づいている．さらに，文献 18) においては，KLJN よりも優れているというサーキュレータに基づいた KLJN システムの偽物が導入されている．しかしながら，文献 12) においてはサーキュレータに基づくシステムは中間者攻撃に対して脆弱であることが示されており，その意味においてこのシステムは元の KLJN システムの競争相手たりえない．

KLJN の考えの初期において 1 つのシステムが製作され 2000 km までのモデル線にてテストされた [19)]．これは提案されているすべての攻撃方法に対して検証され，すべての場合において侵略的な盗聴が単一ビットの通信中に検出された．これは 99.98%の再現度があり，受動的な盗聴において 0.19%の生のビットの情報漏れがあった．200 km における鍵交換の速度は 1 ビット/秒であり，これは文献 10) において示されている東芝–NTT のシステムにおける同じ距離での速度の 4 倍高速である．この価格は数百ドルであり，統合された形において製造コストは PC におけるイーサネットカードと同様である．

(兵庫県立大学　礒川悌次郎)

(2010 年 3 月 2 日受付)