電子技術キーワード解説

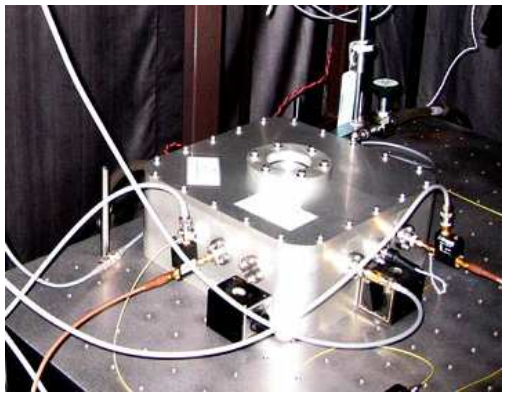
知っておきたい最新の動き

[量子暗号（Quantum cryptography）]

2007 年 4 月、盗聴困難な量子暗号通信を商用光回線で成功したとのニュースがありました。(SI・EMC トピックスレター07 年 4 月号（６）項）コンピュータ技術の進歩次第で、解読されてしまう恐れがある現在の数学的な暗号に代わる技術と考えられている量子暗号通信とは､いったいどのようなものでしょうか。

量子暗号方式では、送信した情報を観測（盗聴）すると情報が瞬時に変化するという物理現象を応用して、盗聴されたことを確実に検知できる、また、盗聴されても情報が変化してしまうので、復元化できないという完全な盗聴防止システムを実現することができます。数学的な方式ではなく、物理学的原理に安全性を依存している為、理論上、永久に解読が絶対不可能な、まさに難攻不落の完全な暗号化方式となります。

現在の暗号化システムは、数学的な暗号化アルゴリズムを用いて、送信時には、見た目は全く異なるデータに変換し、受信側で復元化アルゴリズムにより元のデータへの復元化を行います。このとき、暗号化・復元化を行うために鍵が必要となります。この鍵には、大別すると共通鍵暗号方式、公開鍵暗号方式があります。現在、最も安全性が高いとして普及しているのが公開鍵暗号方式の RSA 暗号方式です。(詳細は省略します。）この RSA 暗号方式は、暗号技術の解読アルゴリズムが開発されているのにも関わらず、その解読には天文学的な計算を行わなければならないとされていました。ところが、今後、量子コンピュータが開発された場合、現在のスーパー・コンピュータが数億年から数十億年かかるとされている暗号解読を僅か数秒から数分で実現してしまうとされています。



そこで、登場したのが、量子コンピュータとは別の量子現象を応用した量子暗号方式です。量子暗号方式では、量子力学におけるハイゼンベルグの不確定性原理をその暗号強度のよりどころとしています。同原理によると、基本的に、素粒子の運動量と位置は同時に測定することができません。その理由は、素粒子の世界では測定に用いる波が被観測系に影響を与えてしまうため、観測すると同時に被観測系の状態が変化してしまうということです。たとえば、光ファイバーにおいて光子単位でデータ通信を行った場合、光子はハイゼンベルグの不確定性原理に従うため、どこかで観測されると、光子の状態が変わってしまいます。したがって、通信が盗聴(観測)されると、必ずそれが明らかになり、それに応じて通信を遮断するなどの処置が可能となります。また、盗聴された時点でそれが判明するため、もちろん改ざんも不可能です。また、光子を複製することも不確定性原理によって不可能とされています。

現在、提案されている量子暗号方式には、単一光子による量子鍵配送と量子ゆらぎ拡散による光通信量子暗号があります。

量子鍵配送（量子鍵拡張）は、従来の暗号に使用される鍵のみを単一光子の通信により行い、実際のデータの暗号化には既存の暗号を採用する方式です。(この理由は、量子暗号通信の通信速度が非常に遅いためです。）無条件安全に配送された鍵を使って、One time pad（平文と同じ数の鍵を用いる方式）と呼ばれる暗号化を行い通信すれば、絶対に解けない暗号通信（完全秘匿）になります。ただし、この鍵を使っ

て従来の暗号に使えば、安全性は従来の暗号と同程度になります。ヨーロッパ、日本では、NTT、NEC、NICT、三菱電機などが研究を進めている方式です。

光通信量子暗号は、最初に数百ビットの鍵を共有します。その鍵を疑似乱数生成器によって伸長して、その疑似乱数と通常の光通信用光変調器を組み合わせることによって情報（平文）を間接的に暗号化する技術です。(従来の暗号方式では、盗聴者が暗号文を入手して、それを解析する事によって解読作業が始まりますが、これとは異なります。)本方式では鍵を知らないで光信号を受信すると量子雑音によって乱され、意味不明になります。これが、量子雑音による暗号化になります。鍵を知って観測すれば量子雑音の効果は無視できるのですが、鍵を知らずに観測すれば、量子雑音による暗号化によって盗聴者の信号には情報が何も見えません。このような原理を使って解読不可能で、かつ Gbps 級の高速な光暗号通信を実現可能とされています。本方式は、玉川大学などが取り組んでいます。

（http://www.tamagawa.ac.jp/sisetu/GAKUJUTU/pderc/rqcs/what.html などを参考）

技術・経営の戦略研究・トータルサポータ
ティー・エム研究所
工学博士
中小企業診断士
社会保険労務士（登録予定）
代表　芳賀　知
E-Mail：GHH12525@nifty.com　URL：http://homepage3.nifty.com/s-haga