# 量子暗号通信

ＪＪ1ＳＸＡ/池

先に「量子コンピューターって？」（22.Nov,2019 up）という記事を書きましたが、今度は「量子暗号通信…Quantum Key Distribution(QKD)」です。

量子暗号通信は、医療データや金融取引等、秘匿性の高い情報を安全にやり取りするために用いられる暗号通信技術の一つだ、解読不可能な暗号化を行うためには、暗号文とその鍵を安全に伝送することが必要となります、量子鍵配信（QKD）では、この暗号鍵を光子に乗せて伝送します、光子が何かに触れると、必ず状態が変化するという量子力学的な性質を利用して、第三者による鍵の盗聴を確実に検知することが可能とのことです。

送信者が送った光子が伝送路（光ファイバーなど）を通るとき、次の4つの可能性が考えられます。

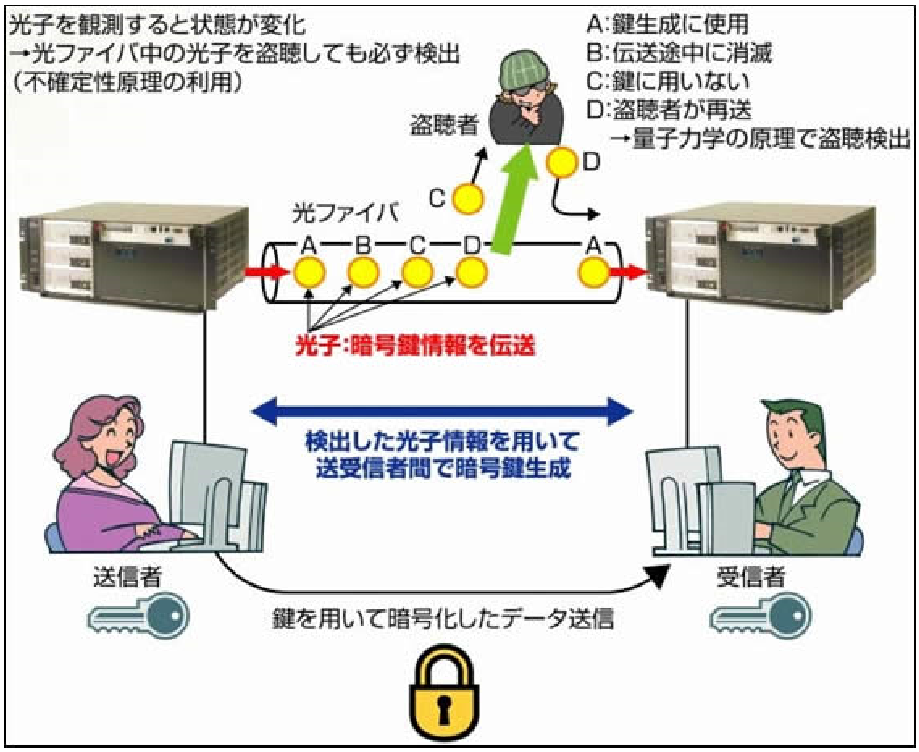
A.盗聴を受けずに受信者に検出される、

B.伝送中に消滅する、

C.盗聴者が盗む、

D.盗聴者が操作した後で受信者に検出される。

このうち、Aは安全な鍵生成に用いることができます、B・Cは受信者に届かないため暗号鍵には使われないので、たとえ盗聴者が持っていても意味がありません、Dでは盗聴が検知され、盗聴された可能性のある情報量の上限が見積もられます、受信者は送信者に光子の伝送が終わった後で、何番目のビットで光子が検出したかを連絡し、鍵生成に利用できるビットを決めます、さらに誤り訂正と秘密増幅といった操作を行って最終的に利用する鍵（最終鍵）を得ます。



東芝は1991年にケンブリッジ研究所を設立し、基礎研究を開始し、2000年に単一光子検出器の開発に成功し、その後、長期間の安定運転や鍵配信距離・速度で世界記録を更新し続けている、量子暗号技術開発のトップランナーです。
東芝が保有する光子検出や安定化制御、長距離化技術を駆使し、量子暗号通信技術の更なる研究開発を進めており、現在世界各地において実証実験を行い、優位性を実証しています。

報道によると、「東芝は、量子暗号通信を2020年度に実用化の方針、世界市場先導へ」となっています。
送受信した情報を読むのに必要な「暗号鍵」をやりとりする専用機器やソフトウェアなどを定額制で顧客に提供する方針で、31日付の読売新聞朝刊が報じた。
手始めに、金融機関が内部で取引や顧客に関する情報といった秘匿性の高いデータをやりとりする際の利用を想定しているとのこと。

量子暗号通信については、世界で競争になっている。
米国は、新興企業が量子暗号通信を提供するサービスを始めると発表、金融機関向けを想定。
中国は、衛星と地上の間での量子暗号通信に成功、世界最大規模の暗号を用いたネットワークを構築。
欧州は、英国やドイツの通信大手が実証実験のための通信網を整備。
韓国は、通信大手がスイス企業に出資して技術取り込み、5Gなどの通信網への活用を発表。

こんな激烈な競争の中で、日本の東芝が一歩先んじているようだ、このまま競争を勝ち抜いてもらいたいものだ…