2010．10．15

資料

【背景】

暗号学的に無条件安全が保証されるバーナム暗号は鍵使い捨て暗号とも呼ばれ、文章を暗号化する鍵を文章と同じだけ用意して、それを使い捨てながら通信する技術である。そのため、バーナム暗号を実現するためには大量の鍵を安全に配送する技術が別途必要になる。この鍵配送を実現する単一光子量子鍵配送技術（通称、量子暗号）が世界的な規模で研究開発されている。それらの安全性は多くの理論研究者によって証明済であると考えられており、これまで、国内では NEC,三菱電機、NTT などが試作機を開発し、現実のシステムへの適用実験が可能なレベルにまで達している。また、海外のスイスではレマン湖の湖底に専用光回線を敷設し運用実験を行っている他、シンガポール、北京などでは市内で試験的な通信実験がすでに成功している。しかし、上記のシステムはノルウエー・ドイツのチームにより解読された事が Nature Photonics に報告されている[1]。さらに、原理的な安全性の欠陥を指摘する論文も公開されている[2]。

【安全性証明と評価法の進歩】

量子鍵配送の安全性は、盗聴者が通信回線から入手可能な鍵系列に対する情報量を極めて小さくできることによって保証されてきた。その基本原理は以下のように説明される。量子鍵配送の理論研究から、量子通信中に盗聴者に漏れる情報量は、通信システムのパラメータから計算で推量することが可能である。この推量された値に基づいて、正規の送受信者は秘密増幅と呼ばれる手法によって、自らの蓄積した鍵系列の一部を無効にして、盗聴者に漏れた情報量を極めて小さくすることができる。このような通信プロトコルによって生成された鍵系列（最終鍵）はバーナム暗号の実現に応用できる。

ここで、鍵系列のビット当たりの漏洩情報量が指数関数的に小さいとき、この暗号システムは無条件安全であると信じられてきた。また、漏洩情報量以外の評価規範によっても検討され、同じ結論が得られている。以上より、一見、その理論は盤石に見える。

しかし、2009 年にこれまでの安全性評価規範は盗聴者が鍵推定に使える条件付き確率の限界の評価しかできず、暗号の安全性を評価するためには全く役に立っていない事が Northwestern 大学の Yuen 教授によって指摘された[2]。今回、この厳密な理論に基づくシミュレーションによって、現状の量子鍵配送による生成鍵は通常の共通鍵暗号用の鍵として利用するにも危険性があることが例証された。

[1] L.Lyderson et al, Hacking commercial quantum cryptography system by tailored bright illumination, Nature photonics, online Aug. 29, 2010.

[2] H.P.Yuen, Key generation: Foundation and a new quantum approach, IEEE. Journal of Selected Topics in Quantum Electronics, vol-15, 1630-1645, 2009.

注釈　＜無条件安全＞いかなるコンピューターや盗聴技術によっても解読される恐れが無い場合、無条件安全あるいは情報理論的安全という。