Bennett 1992 の盗聴量解析

Analysis for amount of eavesdropping on Bennett 1992

○ 中村 敏幸、中田 賢佑、小川 和久、岡本 淳、富田 章久 (北海道大)

○T. Nakamura, K. Nakata, K. Ogawa, A. Okamoto, A. Tomita. (Hokkaido Univ.)

E-mail: nakamura,nakata@optnet.ist.hokudai.ac.jp, tomita@ist.hokudai.ac.jp

1 背景

二者間で鍵と呼ばれる共通の乱数列を秘密裏に共有することで、安全な通信が可能である。量子鍵配送 (QKD) は、量子力学に基づいた安全性を持った鍵を共有するための方法である。QKD では、盗聴者による盗聴量をビットエラーにより見積もることが可能で、見積もった盗聴量の分だけ鍵を捨てるプライバシー増幅と呼ばれる操作を行うことで安全性を保障する。近年、送信状態と、受信系のセットアップで盗聴量の上限が決まるプロトコルが提案された [1]。このプロトコルの利点として、機器の不完全性によるビットエラーは、二者が推定する盗聴量に影響しない、ビットエラーが大きくても鍵配送ができることが挙げられる。そこで、より簡単な系で盗聴量の上限が決まらないかについて興味がある。

本稿では、Bennett 1992(B92) プロトコル [2] に着目し、盗聴量について解析を行ったところ、intercept/resend 攻撃において、平均光子数に対する盗聴量が決まることを示した。

2 提案手法

強い参照光付き B92 プロトコルは、無条件安全性が証明されている [3]。B92 プロトコルで用いる弱コヒーレント光は、量子光学では非直交状態として記述される。B92 プロトコルは、この状態の識別に失敗することがあるという量子力学的性質により安全性が示されている。B92 においてエラーレートに対する盗聴量見積りがこれまでなされてきた [4] が、エラーレートによらない盗聴量見積りはなされていない。そこで、intercept/resend 攻撃に対する最大盗聴量を平均光子数に対して見積もった。

具体的には、イブが USD 測定・最小誤り測定を行い、ボブにパルスを送信する攻撃を仮定する。イブの USD 測定成功・失敗確率は少なくともアリスの送信するパルスの平均光子数 μ に対して $P_{Succ} = 1 - \exp(-2\mu), P_{Fail} = \exp(-2\mu)$ であり、イブが再送する信号光 μ_S と参照光 μ_R の強度差によるエラー e_d を除いた情報量を $I_{SR} = 1 - H(e_d)$ とする。また、最小誤り測定での誤り率は $P_{ME} = (1/2)(1 - \exp(-4\mu))$ となる。このとき、ボブが 1 光子測定に成功した確率を $P_B = P_{Succ} \cdot (\mu_S + \mu_R)e^{-(\mu_S+\mu_R)} + P_{Fail} \cdot \mu_R e^{-\mu_R}$ とすると、アリス-イブ間、ボブ-イブ間の相互情報量は

$$I_{AE} = \max\left(\frac{P_{Succ} \cdot I_{SR}}{P_B}, 1 - H(P_{ME})\right), I_{BE} = P_B$$

と記述できる。このときのビットエラーは

$$e_{bit} = \frac{P_{Succ} \cdot (\mu_S + \mu_R)e^{-(\mu_S+\mu_R)} \cdot e_d + P_{Fail} \cdot \mu_R e^{-\mu_R} \cdot (1/2)}{P_B}$$

と記述でき、平均光子数に対してイブが持っている情報量とイブの引き起こすビットエラーを計算した。図から平均光子数が小さくなればなるほど、イブが引き起こしてしまうビットエラーが増加し、最大盗聴量が減少していくことがわかる。

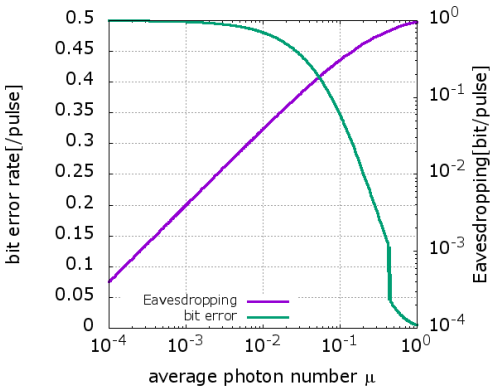

図 1: 平均光子数に対するビットエラーと盗聴量

参考文献

[1] T. Sasaki, Y. Yamamoto and M. Koashi. Nature **509**, 475-478(2014)

[2] Charles H. Bennett. Phys. Rev. Lett. **68**, 3121(1992)

[3] K. Tamaki, N. Lutkenhaus, M. Koashi and J. Batuwantudawe. Phys. Rev. A **80**, 032302(2009)

[4] A. K. Ekert, B. Huttner, G. M. Palma, A. Peres. Phys. Rev. A **50**, 1047(1994)