量子暗号に対する操作的意味を持つ安全性評価指標に関する研究

情報科学科　浅野 駿吾　　指導教員：臼田 毅

1　はじめに

量子暗号の一つである量子鍵配送 (Quantum Key Distribution:QKD) に対する安全性評価問題は近年大きな議論となっている．かつて QKD の評価指標には主として相互情報量が考えられていた．しかし相互情報量が十分に小さい場合でも鍵推定成功確率が安全でない場合がある可能性が指摘された．そのため相互情報量の暗号学的操作的意味が不明確であるとされ，近年，操作的意味のある量に注目が集まっている．それらは以前は注目されていなかったため，様々なケースでの特性が十分に明らかになっていない．本研究ではその一つである鍵推定成功確率の特性について考察する．

ここでは QKD の代表的なプロトコルとして BB84 を取り上げ，相互情報量だけが与えられた場合の鍵推定成功確率の上限・下限 [1] からその特性を考えていく．以降，送信者を Alice，受信者を Bob，盗聴者を Eve とする．

2　相互情報量と鍵推定成功確率

2.1　上限と下限

鍵推定成功確率とは，Eve が盗聴の結果得られた情報をもとにある系列を生成鍵であると推測し，それが生成鍵と一致する最大確率のことを示す．生成鍵 G に対する Eve の相互情報量 $I(G;E)$ だけが与えられた場合の鍵推定成功確率の上限，下限 [1] は，

$$P_{\mathrm{worst}} = I(G;E)/n \tag{1}$$

$$P_{\mathrm{best}} = 2^{-(n-I(G;E))} \tag{2}$$

ただし，n は生成鍵の長さである．今回は BB84 の簡易的なモデルとして Eve の Alice に対する相互情報量 $I(A;E)$ を考える．そのため，Eve が盗聴する系列として生鍵 (誤り訂正や秘匿性増強をおこなっていない系列) を想定し，$I(A;E)$ に対して同じように適用させて考える．また今回，BB84 に対する基本攻撃として以下の二つを取り上げる．

2.2　intercept resend attack

Eve が Alice の送信信号を測定し，測定結果を基に新たな信号を作成し，Bob へと再送する攻撃である．単一光子を送信媒体として用いる BB84 に有効である．このときの盗聴ビット数を $m(<n)$ とすると，相互情報量 $I(A;E)$ と鍵推定成功確率 P_{suc} は次の式で求められる．

$$I(A;E) \sim m\left(\frac{3}{4}\log 3 - 1\right) \tag{3}$$

$$P_{\mathrm{suc}} = \left(\frac{3}{4}\right)^{m}\left(\frac{1}{2}\right)^{n-m} \tag{4}$$

さらに通常の場合 Eve は Alice と同じ基底で測定するが，今回は一般の基底を用いて測定した場合も想定する．基底は θ によって変動するものを考え，$\theta = \pi/8$ の時に Eve の得る相互情報量が最大となる．この基底を Breidbart 基底 [2] と呼ぶ．

2.3　beam splitting attack

Eve が beam splitter(透過率 η) を用いて，Alice-Bob 間の通信路から確率的に光子を盗聴する攻撃である．この攻撃は単一光子に対しては有効ではないが，単一光子が実現困難なため，実験で代わりに用いられる弱コヒーレントに対しては有効である．ここでは，平均光子数 0.1 の弱コヒーレント光を用いた場合を想定する．このとき，

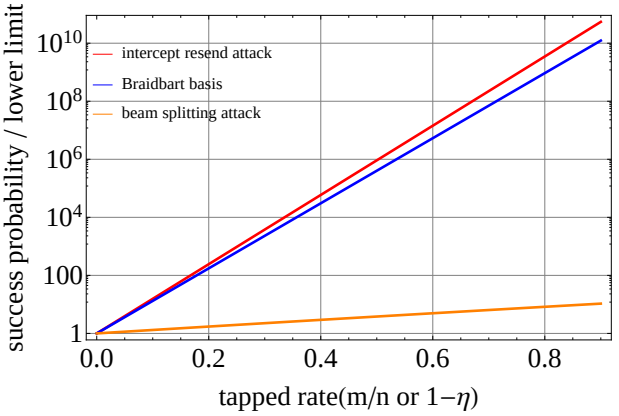

図 1　鍵推定成功確率と下限の比

$$m = n(1 - Po'(0)) \tag{5}$$

として式 (3),(4) に当てはめることで相互情報量と鍵推定成功確率を求めることができる．ここで，$Po'(\cdot)$ は Eve の受け取る平均光子数 0.1 の弱コヒーレントに対応したポアソン分布である．

3　鍵推定成功確率の特性

今回想定した基本攻撃に対する鍵推定成功確率はどれも下限に近い値を示したため，下限との比を表したグラフを図 1 に示す ($n = 100$)．横軸は盗聴割合を表す．intercept resend attack に比べ，beam splitting attack の方が下限に近いような特性を示していることがわかる．また，Eve の得る相互情報量を最大化しているはずの Breidbart 基底を用いた場合では，通常の intercept resend attack に比べて下限に近い特性を示しており，相互情報量を最大化することがより良い盗聴戦略に直接つながるわけではないと言える．

4　まとめ

操作的な意味のある量の代表的なものとして，鍵推定成功確率の特性について調べた．今回は BB84 が安全であると考えられるような基本攻撃について想定しその特性を調べたが，やはり基本攻撃下では鍵推定成功確率は下限に近いような特性，すなわちプロトコルが安全であるような状況であることがわかった．今後の課題として，より効果的な盗聴戦略における鍵推定成功確率の考察や，相互情報量評価以外の観点からのアプローチが挙げられる．

参考文献

[1] H.P. Yuen, IEEE J. Selected Topics in Quantum Electronics, **15**, pp.1630-1645, (2009).

[2] C.H. Bennett, F. Bennett, G. Brrassard, L. Salvail and J. Smolin, J.Cryptol. 5. 3 (1992).