平成 12 年度卒業研究		
入学年度　平成 9 年度	学籍番号　09117948	氏名　　秦 友幸
論文題目　量子暗号を応用したデータ通信プロトコルのシミュレーション		中野研究室

1　はじめに

量子暗号は, 量子力学の原理に基づく安全性を有する暗号化鍵配送方式である．量子暗号に鍵配送以外の機能をもたせる試みとして, 近年, 盗聴検出可能なデータ通信プロトコル (工藤 他, 1998) が提案された．そこで本研究では, このプロトコルの特性をシミュレーションに基づき考察する.

2　盗聴検出可能なデータ通信プロトコル

本プロトコルは, 代表的量子暗号である BB84 プロトコルを応用し, 盗聴者の存在がなければ 100 %正しくデータの受信ができ, かつ盗聴検出が可能となるとしたものである．以下にこのプロトコルの概要を示す.

送信者は量子通信路において, 送信データに検査ビットを混入し, 予備通信により共有した基底を用いて情報を送信する．その後送受信者が, 検査ビットを古典通信路で検証することにより, 盗聴検出を行う.

この方式で共有したデータは, 盗聴者が存在する場合, 送受信者間で不一致ビットが存在する可能性がある．不一致ビットを解消するため, 修正 BBBSS プロトコルを適用させる．まず, ビット位置をランダムに入れ換え, 系列を含まれる不一致ビットが 1 つになるように適当なブロックに分ける．そこで, ブロックに共通のランダムビットを付加し, ブロック毎にパリティを調べる．この際, 盗聴者に対する情報保護のために, 付加したランダムビットを捨てる．送受信者間でパリティの異なったブロックに誤りが存在するとし, そのブロックに対し二分探索を行うことにより, データを失うことなく, 不一致ビットを解消できる.

3　シミュレーションによる考察

本節では, 前節で述べたデータ通信プロトコルの特性を, シミュレーションに基づき考察する.

3.1　シミュレーションの目的

本プロトコルを提案した工藤は, その基本特性は明らかにしたが, パラメータの最適設計等のためのデータが不足していた．そこで本研究では, シミュレーションにより, その特性を定量的に明らかにする.

本プロトコルにおいて, 送受信者は検査ビット中の誤り率から, 送受信者間全体の誤り率を推測する．また，送受信者間の誤り率と関連のある量として，盗聴者の得る情報量，修正 BBBSS プロトコル適用の際の最適ブロックサイズ，使用ランダムビット数などが考えられる．そこで本研究では，シミュレーションを行うことにより，送受信者間の誤り率の正確な見積り条件を定量的に明らかにし，それにより考えられる効果についても考察する.

3.2　シミュレーション条件

通信に用いる送信データは 5000 ビットとし, 盗聴割合は 50 %とした．また, 修正 BBBSS プロトコルを 6 回適用した．また, ここで取る値は, 1000 回試行を繰り返したものを使用している.

最後に, 盗聴者は, 送受信者と同様の基底を用いる盗聴方式 1, 最適 PVM を用いる盗聴方式 2, 最適 POM を用いる盗聴方式 3 のいずれかで盗聴を行うとした.

3.3　真値と見積り値の平均二乗誤差 (誤り率)

図 1は, 送受信者間の誤り率の真値と見積り値の平均二乗誤差を表している．これより, 検査ビットを 1500 ビット程度まで増加させると, どの盗聴方式を用いていても誤差は 1 %程度となることが分かる．これを少量の誤差と考えれば, データ 5000 ビットに対し検査ビットを 1500 ビット程度混入することにより, ほぼ正確な見積りが可能であると考えることができる.

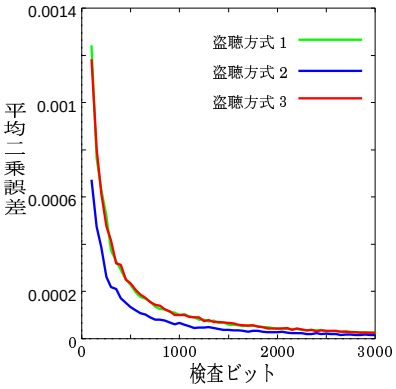

図 1: 真値と見積り値の平均二乗誤差 (誤り率)

3.4　盗聴者の用いる盗聴方式の仮定

盗聴者の得る情報量に関しては, 盗聴者の用いている盗聴方式の仮定が成功した場合のみ正確な見積りが可能となる．本節では, その仮定が誤った場合について考察を行う.

図 2は, 送受信者が盗聴方式 2 と仮定した場合, 盗聴者の得る情報量の真値を見積り値が下回った割合 (%) を示している．送受信者が他の盗聴方式と仮定した場合, 真値を見積り値が大きく下回る部分が存在した．しかし, 図 2 より, 盗聴方式 2 と仮定して見積りを行うことにより, 盗聴者の得る真の情報量を誤って低く見積もることが少なくなる．たとえ, 低く見積もったとしても, 仮定が的中した場合であり, 検査ビット数を増加させることにより, 大きく下回って見積もることは少なくなる.

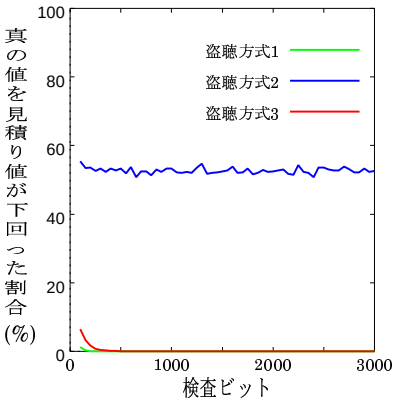

図 2: 真の値を下回った割合 (盗聴方式 2 と仮定)

4　まとめ

本研究では, 盗聴検出可能なデータ通信プロトコルの特性を, シミュレーションに基づき考察した.

参考文献

[1] 秦, 工藤, 臼田, 内匠, “量子暗号原理に基づく古典データ伝送システムに関する一考察” 平成 12 年度電気関係学会東海支部連合大会, 講演論文集, p.220, 2000.