L-003

量子暗号鍵配布プロトコルにおけるワンタイムパッドの研究
Study on One-Time Pads in Quantum Cryptographic Key Distribution Protocols

三重野 凌‡ Ryo Mieno　馬場 優作‡ Yusaku Baba　松本 大輝‡ Hiroki Matsumoto　森下 航‡ Koh Morishita　荒木 智行‡ Tomoyuki Araki

1. はじめに

現在、RSA 暗号などをはじめ、さまざまな暗号技術が存在している。しかし、近年では計算精度が高く、その計算速度も凄まじい量子コンピュータが登場した。その影響により、RSA 暗号などのそれまで多く使われてきた暗号技術が 24 時間以内に容易に解読されてしまうことがある[1]。一方 BB84 プロトコルは量子暗号の技術であり、理論的にも実験的にも多くの研究の蓄積があり、技術的にも最も成熟している[2]。

本研究の目的は、暗号の秘密性を高めることである。今回は、盗聴者がいるかどうかを判別できないかを検討する。そのため、BB84 プロトコル(以下：BB84 とする)を使った量子暗号鍵配布プロトコルにおけるワンタイムパッドの作成について研究を行った。このワンタイムパッドにより、RSA 暗号などの暗号技術では対応が難しい盗聴者に対抗することができると考えた。

2. ワンタイムパッドの作成方法

はじめにワンタイムパッドの作成について、図 1 のように Alice から Bob へ情報を送る例として、示す。

①BB84 を用いたワンタイムパッドの作成手順[3]として、まず、送信者の Alice は“+基底”もしくは“×基底”を選ぶ。さらに、水平、垂直、斜め方向のいずれかを選択し、データを受信者の Bob に送信する。

②次に、受信者 Bob は Alice と同様に“+基底”もしくは“×基底”を選ぶ。さらに、水平、垂直、斜め方向のいずれかの偏向を選択し、データを受信する。このとき、偏光が一致していればデータは正しく受信される。しかし、偏光が一致していなければ 0 か 1 が 50%ずつランダムに受信される。

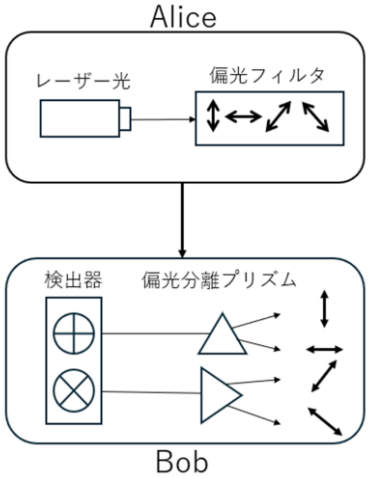

図 1. Alice から Bob へ BB84 による通信

③Alice は Bob に偏光の並びを教え、一致している観測値を用いてワンタイムパッドを作る。

3. 結果

盗聴者がいない場合といる場合とで、それぞれワンタイムパッドを作成した。

表 1 は盗聴者がいない場合のワンタイムパッドを、表 2 は盗聴者(Eve)がいる場合のワンタイムパッドを、それぞれ示す。受信者が観測するものがワンタイムパッドである。

表 1.盗聴者がいない場合のワンタイムパッド

Alice		Bob		
送信	偏光	検出器	検出器	観測
0	+	+	0	0
1	×	×	1	1
1	×	+	-	
0	+	+	0	0
1	+	+	1	(1)
0	×	×	0	(0)
1	+	×	-	
1	+	+	1	1
0	×	×	0	0
1	×	+	-	
1	×	+	-	
0	×	×	0	0
1	+	×	-	
1	+	+	1	(1)
0	×	×	0	0
1	+	+	1	1

盗聴者がいない場合のワンタイムパッドは、受信側の観測で示され、「01010001」であった。

表 2.盗聴者がいる場合の BB84

Alice		Eve		Bob	
送信	偏光	検出器	観測	検出器	観測
0	+	+	0	+	0
1	×	×	1	×	1
1	×	×	0	+	
0	+	+	0	+	(0)
1	×	+	1	+	1
0	×	×	0	×	0
1	+	×	1	×	
1	+	+	1	+	1
0	×	×	0	×	(0)
1	+	+	1	×	
1	×	×	1	+	
0	×	×	0	×	0
1	+	+	1	×	
1	+	+	1	+	1
0	×	+	-	×	
1	+	+	1	+	0

盗聴者がいるときのワンタイムパッドは、受信側の観測で示され、「01101011」となった。

‡広島工業大学　Hiroshima Institute of Technology

このことから、盗聴者がいない場合といる場合とで、ワンタイムパッドが異なることが分かった。このワンタイムパッドは“ビット誤り率”と表現することができる。

ワンタイムパッドの変化を読み取ることで、盗聴者がいることを検出することができた。

4. 考察

本研究により、盗聴者がいるかどうかを判別できるようになり、暗号の秘密性を高めることができた。その結果から盗聴者を即座に検出することができるのが BB84 の特徴であり、実際に検出することができた。

今回のワンタイムパッドの作成では(表１,表２)16bit の bit 列を用いた。この bit 列が 64bit や 256bit など、大きくなることで、より強固なワンタイムパッドの作成が行えると考えた。さらにその時の計算速度や盗聴者の検出の違いも観測したいと考えた。

また、BB84 を使用し、ワンタイムパッドの作成を行うには正しい乱数を使用しなければならない。これは、乱数が悪いことで、盗聴者にメッセージや暗号鍵の予測、検知を簡単にさせてはならないからである。

そして、BB84 は表１、表２、図１より、1bit ずつ暗号化と復号化を行うプロトコルである。したがって、この BB84 は“ストリーム暗号”と呼ばれる暗号技術であると言える。

5. まとめ

今回の研究により、暗号の秘密性を高めることができた。また、BB84 にはストリーム暗号の原理が根底にあることが分かった。

量子暗号鍵配布プロトコルの強度は、ワンタイムパッドを作成するときの「疑似乱数発生の精度[4][5]」に依存する、と考えられる。

また、量子暗号鍵配布プロトコルは、従来の“量子力学の原理を用いた「盗聴者の存在を検出可能」という暗号システム”にはなかった機能がある。

5.1 今後の課題

今回の研究ではコンピュータを使用し、実装やシミュレーションを行うことができなかった。そのため、今後はコンピュータや生成 AI も用いてワンタイムパッドの作成、実装を行いたいと考えている。

近年登場した生成 AI の発展が成長著しい状態にある。生成 AI が今後も成長を続けることで、生成 AI が良い乱数を作成すると期待ができる。

しかし、生成 AI を使用する際には、慎重にかつ頼りすぎることなく活用をするような運用方法を計画したいと考えている。

考察でも書いたように、今回は 16bit のメッセージでのワンタイムパッドの作成となった。これが 64bit、256bit などと bit 列を増やした場合、より強固なワンタイムパッドとなるのか、詳しく研究をしていきたい。

具体的には、計算量が増加されることで、16bit のときに比べて、計算速度や盗聴者の検出に時間がかかってしまうと予想している。

また、BB84 のほかに存在している技術も使い、ワンタイムパッド作成の様子を見たいと考えている。

謝辞

本研究をまとめるにあたり江田英雄先生にご指導をいただきました。謝辞を表します。

参考文献

[1] 情報通信白書令和 6 年版, https://www.soumu.go.jp/johotsusintokei/whitepaper/r06.html （閲覧日 2025 年 6 月 10 日）
[2] 佐々木 雅英, 近代科学者 Digital,“量子鍵配送 基礎と活用法”, 一般社団法人 量子 ICT フォーラム 量子鍵配送技術推進委員会 編初版発行 (2023).
[3] 井上 恭,“工学系のための量子光学”, 森北出版 (2008).
[4] 杉本 幹太, 方 穆湧, 荒木 智行,“ベント関数の量子鍵交換プロトコルへの適用について”, 第 46 回多値論理フォーラム研究ノート, Vol.46, No.4 (2023).
[5] 方 穆湧, 杉本 幹太, 荒木 智行,“ベント関数を使った量子鍵交換プロトコルの評価について”, 第 46 回多値論理フォーラム研究ノート, Vol.46, No.5 (2023).