2018 年度卒業論文

量子鍵配送E91による通信プロトコルの提案とノイズ・盗聴者下における性能評価

A Protocol Suite for E91 Quantum Key Distribution and Distinguishing an Eavesdropper from Noise

慶應義塾大学　環境情報学部
尾澤 慎之介

卒業論文要旨 2018 年度 (平成 31 年度）

量子鍵配送 E91 による通信プロトコルの提案とノイズ・盗聴者下における性能評価

従来の古典通信における秘密鍵共有は、Diffie-Hellman 鍵共有に代表されるように、計算量により安全性が担保されている。量子計算機に代表される高速計算可能な計算機を用いるとこれは解読可能であり、これに代わる新たな秘密鍵共有法として、量子鍵配送が考えられる。量子鍵配送は量子力学に帰因することにより、事実上完全に盗聴者の影響を通信路上から無くすことが可能である。

代表的な鍵共有法として、単一量子を用いる BB84 や量子もつれを用いる E91 が存在するが、E91 は End-to-End 通信が可能となるため、量子ネットワークなどのような広範囲に渡る通信網で効果的であると考える。本研究では、シミュレータを用いて E91 量子鍵配送を用いた通信路上のノイズと盗聴者の影響を変更し、通信可能となるそれぞれの値の閾値を導出した。

シミュレータによる量子通信実験より、E91 では Z エラーが 27%までは通信が可能であるが、28%以上の場合はベル不等式値が常に 2 を下回るためノイズ・盗聴者の識別が不可能となり、通信不可能であることがわかった。

キーワード
1. 量子通信, 2. 量子情報処理, 3. 量子鍵配送,

慶應義塾大学　環境情報学部

尾澤慎之介

Abstract of Bachelor's Thesis

Academic Year 2018

A Protocol Suite for E91 Quantum Key Distribution and Distinguishing an Eavesdropper from Noise

Secret key sharing in the conventional classical communication system is guaranteed by its computational complexity, such as in the the Diffie-Hellman key exchange method.

However, a quantum computer, which has computation powers that cannot be replicated by the classical counterpart, is known to be a potential threat to the classical systems. Some of the encryption methods, such as those based on prime-number factorization, has in fact been demonstrated to be breakable.

Quantum Key Distribution(QKD), is a key distribution technology comprising the laws of quantum physics, where the fundamental quantum phenomena allow the network to detect eavesdroppers, enhancing the communication security.

One of the most well-known QKD technology is the BB84 protocol, which directly uses single qubits as information carriers, and work over adjacent nodes. Another is the E91 protocol. Unlike BB84, E91 operates over entangled qubits, and therefore, works over end-to-end connections.

In this research, we derive threshold rate of the influence of eavesdropper and noise on E91. This is derived from quantum communication simulator, and in this simulator we change the rate of influence of eavesdropper and noise.

Using the quantum communication experiment by the simulator, it was revealed that it is possible o communicate up to 27% of the Z error in E 91. However in the case of 28% or more, the bell inequality value is always below 2, so it is impossible to distinguish noise and eavesdropper.

Keywords:
1. Quantum Communication, 2. Quantum Computation, 3. Quantum Key Distribution,

Keio University, Faculty of Environment and Information Studuies

Shinnosuke Ozawa

目 次

図 目 次

表 目 次

第1章　序論

本章では本研究の背景と貢献分野、本書の構成について述べる。

1.1　背景

人類は古代から紐のような様々な物を用いて計算を行ってきた。1620 年にエドマンド・ガンターが人類最初の計算機である計算尺を考案することにより、人類は機械により計算を行うようになる。計算機にさらなる発展が起こったのは第二次世界大戦中のことである。1941 年にコンラート・ツーゼが開 ‘発した「Zuse Z3」は人類初のプログラム可能な計算機であり、実際に航空機の開発において用いられた。現代では計算機は生活のあらゆる箇所で用いられており、計算機は人類にとって最も重要な発明品の一つであると言える。

計算機はコンピュータとして生活のあらゆる箇所で用いられており、その出力結果を共有すべく、「ネットワーク」によりコンピュータどうしは接続されている。現在のインターネットのようにパケット用いた通信を行うコンピュータネットワークの起源は、1969 年にアメリカ国防総省の高等研究計画局 (DARPA) による「ARPANET」である。人類の計算に対する探究心より誕生した計算機は、この「ARPANET」が発展し、世界中のあらゆる箇所でつながることによりインターネットを構築している。

インターネットの誕生によりコンピュータは世界中のあらゆる箇所で繋がることが可能となったが、コンピュータどうしの接続点において外部からの攻撃の可能性が誕生する。この攻撃からコンピュータ間の通信を守るべく、人々は通信内容を暗号化する暗号通信を行ってきた。現代の暗号通信において暗号鍵の鍵共有において多く用いられている Diffie-Hellman 鍵共有法 [14] は計算量に依存しており、量子計算機などの高速な計算を可能とする計算機を用いると解読が可能である。これに対しどんな計算機を用いても解読が理論上不可能となる暗号として考えられた暗号の一つが量子暗号である。量子暗号は量子力学を背景とすることにより理論上解読が不可能な暗号である。量子暗号の一つである量子鍵配送は、Diffie-Hellman の代替となりうる鍵共有法である。本研究では、様々な量子鍵配送法のうち E91 のシミュレータを実装し、E91 が通信可能となる、ノイズ下における盗聴率の閾値を導出することができた。

1.2　本研究の貢献分野

量子鍵配送は量子力学に基づき鍵共有を行うため、理論上どんな方法を用いても暗号通信が盗聴されることはない。本研究では、量子鍵配送においてどれくらいノイズ耐性が上がると E91 量子鍵配送法が実現可能になるかを示した。

現在多く使われている鍵共有（Diffie-Hellman）は計算量に依存するため、量子計算機などによる高速計算が実現しても解読不可能な量子鍵配送の実現が必須である。現在商用化まで実現している BB84 は単一光子を用いるため、Neighbor-to-Neighbor 通信しかできない。量子もつれ

を用いる E91 では End-to-End 通信が可能となるため、BB84 より得られる利点が大きい。しかし、E91 で盗聴の影響を判定するベル不等式は、盗聴だけでなくノイズの影響でも変化するため、ノイズと盗聴の影響を識別することはできない。

よって本研究ではシミュレータを用いて、通信可能となるノイズと盗聴の閾値を導出し、E91 はどれくらいノイズ耐性が上がると実現可能となるかを示した。また BB84 および E91 シミュレータ上でノイズと盗聴の影響を変化させ、両方の鍵共有のノイズ・盗聴の影響を比較した。

また実験結果をもとに E91 による通信プロトコルを提案した。本プロトコルは End-to-End 通信が可能となるため、量子ネットワークで用いることが可能となると考える。

1.3 本書の構成

次章からの本書の構成は以下の通りである。

第 2 章では、本書で読む上で最低限必要となる量子情報理論の概論について述べる。

第 3 章では、現代のネットワーク通信で用いられる古典暗号における鍵共有法 Diffie-Hellman 鍵共有について述べ、その問題点について述べる。

第 4 章では、Diffie-Hellman 鍵共有の問題点を克服可能な量子鍵配送について述べ、本論文の研究対象である、BB84 および E91 の詳細について述べる。

第 5 章では、Bell Test, BB84・E91 におけるノイズと盗聴の影響を測定した実験内容について述べる。

第 6 章では、第 5 章の実験結果を元に、E91 プロトコルを提案する。

第 7 章で第 2 章から第 6 章までの前提を受け、本論文の結論を述べる。

第2章　量子情報処理概論

本章で本書で読む上で最低限必要となる量子情報理論の概論について述べる。量子計算の誕生と歴史について簡単に述べた後、量子情報処理の概要について述べる。

2.1　量子情報処理の誕生と歴史

量子情報処理の始まりは1980年にリチャード・ファインマンが発表した「計算機による物理系のシミュレーション」である [1]。この論文でファインマンは、任意の物理系のシミュレーションは量子力学に基づく計算機を用いることにより効率的に解くことが可能と述べた。

量子計算だけでなく量子暗号もほぼ同時期に誕生する。1984年、チャールズ・ベネットとジャイルズ・ブラザードにより、量子力学により暗号鍵の共有を行う、量子鍵配送BB84 [2] を考案する。1991年にはアルトュル・エカートが、量子もつれという関係をもった2つの量子ペアを用いた量子鍵配送E91 [3] を考案する。本論文の研究対象はこの量子鍵配送BB84とE91である。

量子計算におけるアルゴリズムも誕生する。1992年、デイヴィッド・ドイチュとリチャード・ジョサが量子コンピュータを用いることにより古典コンピュータより高速に計算可能となる、ドイチュ・ジョサのアルゴリズム [4] を考察する。1994年には実用的なアルゴリズムとして、ピーター・ショアがショアのアルゴリズム [5] を考案する。このアルゴリズムを用いると因数分解を高速に解くことが可能となるため、量子計算によりRSA暗号などの計算量に依存する暗号は解読可能とした。

近年では理論だけでなく、量子情報処理の実験も盛んになる。2001年にはIBMが核磁気共鳴（磁場中の原子核が特定の周波数の電磁波と共鳴すること）を用いて、ショアのアルゴリズムを実際に実装する [6]。量子力学を用いた計算機の実現の研究が盛んとなるが、2016年にibmはクラウド上で実際の量子計算機の処理を可能とするibm-qシステムを公開する。世界中から量子計算機の実機にアクセスし、簡単な量子計算処理を行うことができる。このように現代において量子計算は我々が実際に触れるものとなり、既に身近なものとなっている。

2.2 量子情報の基本

2.2.1 量子ビット, Qubit

従来の古典情報処理において、情報は**ビット**より表される。ビットはバイナリであり、二つの状態を **0 ビット**または **1 ビット**により示すことができる。一方量子情報処理において、情報は**量子ビット, qubit** により表される。量子ビットは**重ね合わせ状態**をとることが可能であり、1qubit の状態は $|0\rangle$ または $|1\rangle$ の和で表すことができる。特に本書では従来のビットのことを、**古典ビット**と呼ぶことにする。

古典ビットは電圧により成立しており、計算機上の回路で閾値より高い電圧だとビットは 1 であり、閾値より低い電圧だとビットは 0 である。これに対し量子ビットは**量子**により成立している。量子は物質の最初単位であり、電子や陽子、中性子、光子（光の最小単位）がこの例として挙げることが可能である。物質を微視的な観点から考察すると、古典力学では考えられないような現象が発生する。これの一つが重ね合わせ状態であり、**ディラックの表記法**を用いることにより簡単に示すことができる。

ディラックの表記法

ポール・ディラックが考案したディラック表記法 [7] を用いることにより、量子力学で考える系の状態である**量子状態**を簡単に示すことができる。量子力学は演算子形式 [8] [9] [10] や経路積分形式 [11] などの形式がある。演算子形式に従うと量子状態は複素ヒルベルト空間 H（複素数全体の集合上の完備な内積付きベクトル空間）上のベクトルや演算子して考えることが可能である。

ディラックの表記法では、列ベクトルを $|\psi\rangle$ と表し、記号 $|\rangle$ を**ケット**と呼ぶ。$a_1, a_2, \ldots, a_n$ を複素数とすると、

$$|\psi\rangle \equiv \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \tag{2.1}$$

である。

特に古典ビットの 0 と 1 に対応させ、本書では

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.2}$$

とする。

以下で、

$$|\psi\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \equiv \begin{pmatrix} a_1, \ldots, a_n \end{pmatrix}^T \tag{2.3}$$

とする。

記号 $\langle|$ はブラと呼び、$|\psi\rangle = \left(a_1,\ldots,a_n\right)^T$ に対し、$\langle\psi|$ は複素共役転置な行ベクトルであり、

$$\langle\psi| = \left(\overline{a_1},\ldots,\overline{a_n}\right) \tag{2.4}$$

となる。ここで 複素数 $c = x+yi$ ($x,y \subset$ 実数 R) に対し$\bar{c} = x-yi$ とした。

$b_1,b_2,\ldots,b_n$ も複素数とすると、$|\psi\rangle = \left(a_1,\ldots,a_n\right)^T$ と、$|\phi\rangle = \left(b_1,\ldots,b_n\right)^T$ に対して $\langle\psi|\phi\rangle$ は、n 次元行ベクトルと n 次元列ベクトルの行列積となり、

$$\langle\psi|\phi\rangle = \left(\overline{a_1},\ldots,\overline{a_n}\right)\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \sum_{i=1}^{n}\overline{a_i}b_i \in \text{複素数}\, C \tag{2.5}$$

より、$\langle\psi|\phi\rangle$ は内積を示す。

量子重ね合わせ

古典ビットの 0 と 1 に対応させ、$|0\rangle \equiv \begin{pmatrix}1\\0\end{pmatrix}, |1\rangle \equiv \begin{pmatrix}0\\1\end{pmatrix}$ としたが、量子ビットはこの 2 状態以外にもこれらの和として表すことができ、a,b を実数 R として、

$$|\psi\rangle = a|0\rangle + b|1\rangle \tag{2.6}$$

をとる場合、測定後にこの量子状態 $|\psi\rangle$ が $|0\rangle$ となる確率は $|a|^2$、$|1\rangle$ となる確率は $|b|^2$ となる。すなわち任意の量子状態 $|\psi\rangle$ は、

$$|\psi\rangle = a|0\rangle + b|1\rangle \qquad (a \text{ と } b \text{ は } |a|^2+|b|^2 = 1 \text{ となる複素数}) \tag{2.7}$$

をとることができ、$|\psi\rangle$ は $|0\rangle$ と $|1\rangle$ の**重ね合わせ状態**であると言うことが可能である。これは任意の量子状態は適当なベクトルの和として表すことが可能ということである。

Bloch 球

重ね合わせ状態 $|\psi\rangle = a|0\rangle + b|1\rangle$ は、オイラーの公式 $e^{i\theta} = \cos\theta + i\sin\theta$ を用いて、

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle \tag{2.8}$$

この重ね合わせ状態を示す式上の (θ,ϕ) に対応する点を図示したものが Bloch 球である。例えば、$(\theta,\phi) = (0,0)$ のとき、$\begin{pmatrix}1\\0\end{pmatrix}$ となり、$(\theta,\phi) = (\pi,0)$ のとき、$|\psi\rangle = |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$ とる。

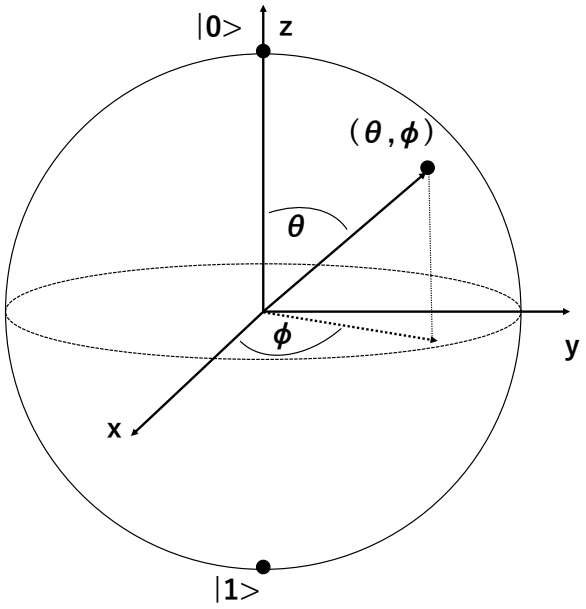


図 2.1: Bloch 球

2.2.2 密度行列

重ね合わせ状態により、任意の量子状態を表現することが可能となったが、実際には重ね合わせ状態では表現できない量子状態が存在する。例えば 1/2 ずつ別々の結果を出す操作（例えばコイン投げなど）を行い、一方の結果が出た場合に $|0\rangle$ をとり、もう一方の結果がでた場合に $|1\rangle$ をとる量子状態は、先ほどの重ね合わせ状態で示すことはできない。この状態は操作の結果により決まるため、

$$\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle \tag{2.9}$$

とは異なる。

単純に重ね合わせ状態で示すことのできる状態を**純粋状態**といい、この例のような、確率的に得られる操作の結果で示される状態を**混合状態**という。この混合状態を簡単に表す方法が**密度行列**である。

上述した例を一般化し、

$$\text{「確率 } p_i \text{で量子状態を} |\psi_i\rangle \text{とする} \qquad (i = 1, \ldots, n)\text{」} \tag{2.10}$$

場合を考える。この場合は重ね合わせ状態では表せないため、密度行列で、

$$\rho \equiv \sum_{i=1}^{n} p_i |\psi_i\rangle \langle\psi_i| \tag{2.11}$$

と表す。

次にこの密度行列で示された量子状態に関する測定を考える。状態に対する測定行列 M が与えられた場合、測定行列に対応した測定値を得る確率は、

$$P(m) = Tr(M^{\dagger} M \rho) \tag{2.12}$$

となる。ただしここで、$|\psi\rangle^{\dagger}$ は $|\psi\rangle = \left(a_1,\ldots,a_n\right)^T$ の転置共役である、$\left(\overline{a_1},\ldots,\overline{a_n}\right)$ とし、$Tr()$ を () 内の行列の対角和とした。またこの場合の測定後の量子状態は、

$$\rho' = \frac{M\rho M^{\dagger}}{Tr(M^{\dagger}M\rho)} \tag{2.13}$$

となる。

例えば、量子状態 $|\psi\rangle$ を 1/2 の確率で $|0\rangle$,1/2 の確率で $|1\rangle$ とするとき、$|0\rangle$ と $|1\rangle$ に対応する測定行列はそれぞれ $M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, M_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ だから、

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \begin{pmatrix} 1/2 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1/2 \end{pmatrix} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix} \tag{2.14}$$

であり、

$$P_0 = Tr(M_0^{\dagger}M_0\rho) = Tr\begin{pmatrix} 1/2 & 0 \\ 0 & 0 \end{pmatrix} = \frac{1}{2} \tag{2.15}$$

の確率で、

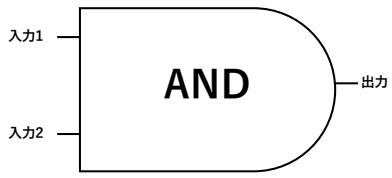
$$\rho_0' = \frac{M_0\rho M_0^{\dagger}}{Tr(M_0^{\dagger}M_0\rho)} = \frac{1}{2}\begin{pmatrix} 1/2 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \tag{2.16}$$

となる。

2.2.3 量子ゲート

古典ゲート

古典計算では、回路上の素子に対応しビット値が変化する。例えば AND 素子は 2 ビットの入力、1 ビットの出力を持ち、下図のようにビット値は変化する。



入力 1	入力 2	出力
0	0	0
0	1	0
1	0	0
1	1	1

図 2.2: AND 素子

量子ゲート

量子計算で用いられる量子回路でも量子ビットに対して量子ゲートが適用可能である。量子ビットゆえ重ね合わせ状態をとることが可能であり、測定するまで量子状態は確定しない。

1. パウリゲート

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.17}$$

1-a. パウリ X ゲート (bit flip ゲート)
量子ビットに対し、ビット反転を行う。

$$\sigma_x(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle \tag{2.18}$$

となる。

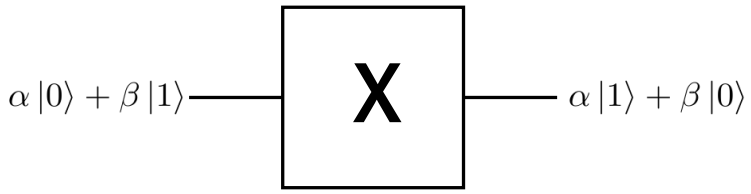


図 2.3: パウリ X ゲート

1-b. パウリ Y ゲート (bit and phase flip ゲート)
量子ビットに対し、ビット反転および位相反転を行う。

$$\sigma_y(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle - \beta|0\rangle \tag{2.19}$$

となる。

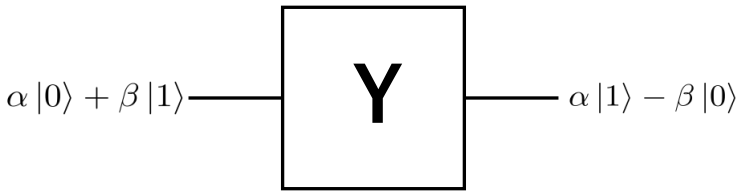


図 2.4: パウリ Y ゲート

1-c. パウリ Z ゲート (phase flip ゲート)
量子ビットに対し、位相反転を行う。

$$\sigma_z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle \tag{2.20}$$

となる。

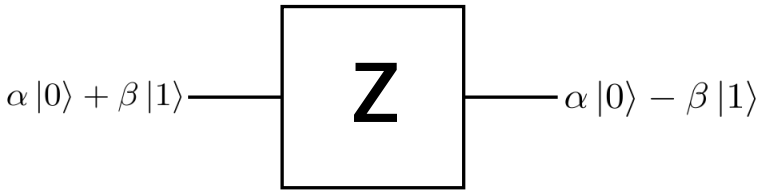


図 2.5: パウリ Z ゲート

2. アダマードゲート

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.21}$$

$|0\rangle$ に適用すると、$|0\rangle$ と $|1\rangle$ の等しい割合である重ね合わせ状態になる。$|1\rangle$ に適用すると、位相が負となる $|0\rangle$ と $|1\rangle$ の等しい割合である重ね合わせ状態になる。

$$H|0\rangle = \frac{|1\rangle + |0\rangle}{\sqrt{2}}, \qquad H|1\rangle = \frac{|1\rangle - |0\rangle}{\sqrt{2}} \tag{2.22}$$

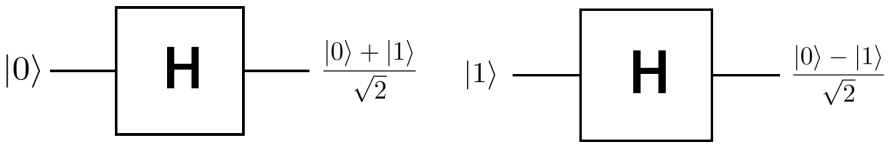


図 2.6: アダマードゲート

3. 回転ゲート

R_x ゲート

Bloch 球上の x 軸周りに状態を回転する。

$$R_x(\theta) = \begin{pmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{pmatrix} \tag{2.23}$$

R_y ゲート

Bloch 球上の y 軸周りに状態を回転する。

$$R_y(\theta) = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix} \tag{2.24}$$

R_z ゲート

Bloch 球上の z 軸周りに状態を回転する。

$$R_z(\theta) = \begin{pmatrix} exp(-i\theta/2) & 0 \\ 0 & exp(i\theta/2) \end{pmatrix} \tag{2.25}$$

2.2.4 量子もつれ

ある 2 つの量子状態がともに $|0\rangle$ または $|1\rangle$ であった場合、この量子状態は $|00\rangle$ または $|11\rangle$ と表現することができる。これらの 2 つの量子状態が等しい割合の重ね合わせ状態を考えると、

$$|\Psi_+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \tag{2.26}$$

となる。ここで、$|\psi\rangle|\psi\rangle = |\psi\rangle \otimes |\psi\rangle = |\psi\psi\rangle$ とした。

$|\Psi_+\rangle$ の片方の量子状態を測定すると、1/2 の確率で 0 が得られるが、重ね合わせ状態より、もう片方の測定結果も 0 となる。逆に片方の量子状態の測定結果が 1 だった場合、もう片方の測定結果も 1 となる。このように片方の測定結果がもう片方の測定結果に影響を及ぼす重ね合わせ状態のことを、**量子もつれ (Entanglement)** という。

上述の $|\Psi_+\rangle$ だけでなく、以下の量子状態も 2 量子の量子もつれとなる。

$$|\Phi_+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \qquad |\Phi_-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} \tag{2.27}$$

$$|\Psi_+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \qquad |\Psi_-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} \tag{2.28}$$

第3章　古典暗号

現代では様々な箇所でコンピュータが用いられ、これらは当然のようにネットワークを構築し繋がっている。ネットワーク上では通信路上の盗聴の問題が発生する。このような現代において、盗聴に対処すべく、暗号を用いた暗号通信を行うことは必須と言える。

次章で量子暗号について触れるため、まず本書では古典暗号における鍵共有法である Diffie-Hellman 鍵共有法について述べる。

3.1　暗号に必要な要素技術

ある二者が通信を行いたいとする。この二者間には盗聴の可能性があり、盗聴に対抗すべく通信内容を暗号化した暗号通信を行うことにする。送信者は送りたい内容（**平文**）を暗号化し**暗号文**を作成する。平文から暗号文を作成するものを**鍵**という。この鍵は暗号化と同時に暗号文を平文に戻す（**復号**）するためにも用いられる。すなわち、通信二者間で鍵を共有し、送信者が鍵により平文を暗号化した暗号文を、受信者は鍵を用いて復号し平文とする。これが基本的な暗号通信のプロセスである。この暗号プロセスに必要とされる主な技術として以下のものを挙げることができる。

- Authentication 認証
- Bulk Data Encryption 暗号文の作成
- Key Decision Generation 鍵配送

認証は、正規の通信相手と通信を行う上で必要となる。古典暗号の多くでは、**公開鍵暗号**である **RSA 暗号** [12] により行われる。RSA 暗号は平文の暗号化は他人に知られてもよい公開鍵を用いて、暗号の復号に公開がきのペアであり他人と決して知られてはならない秘密鍵を用いる。秘密鍵と公開鍵のペアは桁数の大きい因数分解に依存し作成されている。桁数の大きい因数分解は古典計算を用いると莫大な計算を必要とし、これにより RSA 暗号の安全性は担保されている。量子計算機などにより桁数の大きい因数分解の高速計算が可能となると、RSA 暗号は解読可能となる。

暗号文の作成に用いられる技術は **DES** や **3DES**、**AES** [13] である。DES と 3DES は平文を任意の区切りでわけ、鍵により暗号化する。AES は平文を任意の可変長な区切りでわけ、DES や 3DES を同じく鍵により暗号化する。

鍵共有とは、暗号化・復号を行う鍵の共有のことである。この鍵の共有法は古典暗号の中でも特に困難であり、古典暗号技術における問題点の 1 つであると言える。物理的に鍵を輸送する方法が最も安全だが、現実性が非常に低い。古典暗号の多くでは **Diffie-Hellman 鍵共有法** [14] が用いられる。この古典暗号の Diffie-Hellman 鍵共有法に対し、量子力学に基づき鍵共有を行う方法が**量子鍵配送法**である。

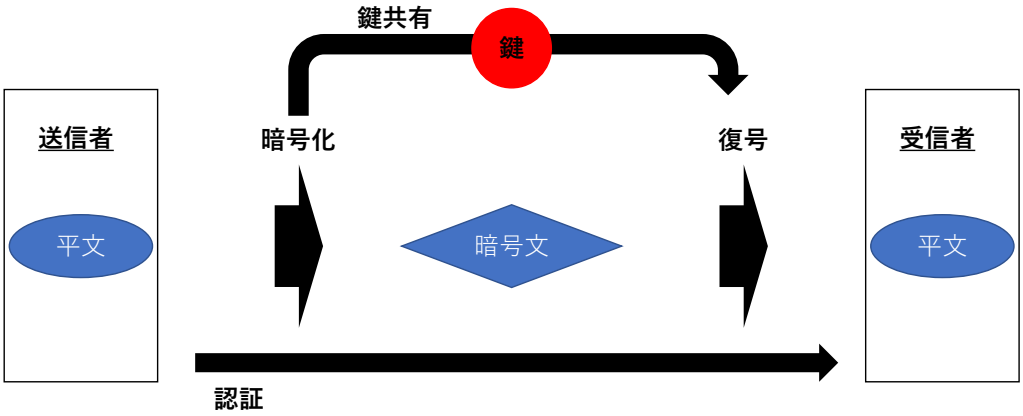


図 3.1: 暗号通信

3.2 Diffie-Hellman 鍵共有法

Diffie-Hellman 鍵共有法の主な過程

送信者 Alice が鍵を受信者 Bob に送る。ここで通信路上に盗聴者 Eve が存在するとする。

1. 二つの素数 p と x を準備する。この p はとても大きな素数である。p と x は公開して良い数であり、Alice と Bob だけでなく、Eve も知ることができる。
2. Alice と Bob はそれぞれ 1〜p-2 の任意の値 a,b を準備する。この数 a と b は公開してはならない秘密の値であり、Eve は知ることができない。
3. Alice は自分が知っている値である (p,x,a) をもとに、$A = x^a \pmod{p}$ を導出し、この値 A を Bob に送信する。
4. Bob も同じく自分が知っている値である (p,x,b) をもとに、$B = x^b \pmod{p}$ を導出し、この値 B を Alice に送信する。
5. Alice は Bob から送られた値 B から
$$B^a \pmod{p} = (x^b \bmod p)^a \bmod p \tag{3.1}$$
を導出する。
6. Bob も同じく Alice から送られた値 A から
$$A^b \pmod{p} = (x^a \bmod p)^b \bmod p \tag{3.2}$$
を導出する。
7. Alice と Bob の導出した値は
$$(x^b \bmod p)^a \bmod p = \tag{3.3}$$
$$x^{ab} \pmod{p} \tag{3.4}$$
$$= (x^a \bmod p)^b \bmod p \tag{3.5}$$

より、等しい値であり、これが共有した鍵となる。

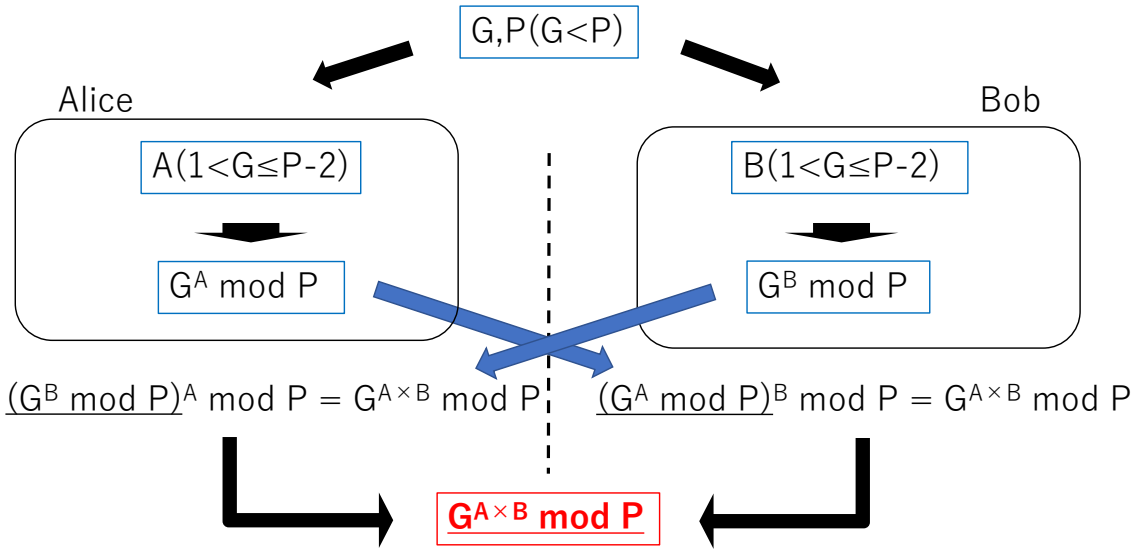


図 3.2: Diffie-Hellman 鍵共有

Diffie-Hellman 鍵共有法の安全性の担保

Diffie-Hellman 鍵共有法は**離散対数問題**により安全性が担保されている。離散対数問題は、素数に関する式

$$y = a^x \mod p \tag{3.6}$$

に対し、(p,a,x) の値から y を求めることは簡単だが、(p,a,y) の値から x を求めることが困難ということである。Diffie-Hellman 鍵共有法において盗聴者 Eve は、(x,p,A,B) の値を知ることができる。Diffie-Hellman 鍵共有法における鍵である

$$B^a \pmod p = (x^b \mod p)^a \mod p = x^{ab} \pmod p = (x^a \mod p)^b \mod p = A^b \pmod p \tag{3.7}$$

において Eve は (x,p,A,B) しか値を知らず、a または b の値を知らないため、鍵の作成は不可能である。

しかし量子計算機などの高速計算が可能な計算機により離散対数問題が解決可能となる場合、Diffie-Hellman 鍵共有法は解読可能となる。量子暗号である**量子鍵配送**は計算量でなく量子力学に依存するため、理論上完全に安全な鍵共有を可能とする。

第4章　量子暗号

古典暗号では鍵共有が計算量に依存するため、高速計算が可能となると解読が可能であった。**量子鍵配送 (Quantum Key Distribution)** は計算量ではなく量子力学に依存するためどんな方法を用いても理論上盗聴は解読は不可能である。量子暗号では、通信路上での測定があった場合に量子状態が変化する。すなわち量子暗号では、第 3 者の通信路上における測定による量子状態の変化を盗聴とみなす。盗聴があった場合に量子状態が変化することより、量子暗号は理論上盗聴が不可能であり、解読も不可能となる。

本章では本論文の研究対象である、量子鍵配送法 **BB84** および **E91** の詳細について述べる。

	古典暗号	量子暗号
秘匿性の原理	計算量（盗聴可能）	量子力学（理論上は盗聴不可能）
通信速度	数 100Mbps 〜 数 10Gbps（高速）	数 10Kbps 〜 1mpbs（低速）

表 4.1: 量子暗号と古典暗号の比較 [15] より

4.1　量子鍵配送

量子力学では、同じ系の 2 つの物理量はを測定したとき、それぞれの測定時の不確定性が共に 0 になることはない (**不確定性原理** [16])。最も代表的な例がある量子の位置と運動量であり、この 2 つのどちらかを測定した場合はもう片方の系が物理量は乱れ、測定誤差が大きくなる。ある量子の物理量のうち位置を測定したときの不確定性を Δx、運動量を測定した時の不確定性を Δp とすると、

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2} \qquad (\hbar : \text{プランク定数}) \tag{4.1}$$

となり、どちらかの不確定性を小さくすると、もう片方の不確定性が大きくなる。

様々な 2 つの物理量の組も同様の性質をもち、そのうちの 1 組が光の偏光である。本研究では光の偏光を用いた量子暗号を研究対象とする。

4.1.1　偏光

太陽光などの通常の可視光は様々な方向に振動している。この様々な方向に振動している光を 1 つの決まった方向に振動させた光が偏光である。偏光は上下方向（垂直）や左右方向（水平）のみに振動する。方解石などが光を偏光させる性質を持ち、これらを使用した偏光板を用いることで偏光を作成できる。

量子力学に従うと、偏光が特定の方向（例えば垂直水平方向のどちらか）に偏光しているかどうかは測定し判定することが可能だが、偏光がどの方向（垂直水平方向か斜め方向のどちら

か）に偏光しているかどうかは判定不可能である（図 4.1, 図 4.2）。

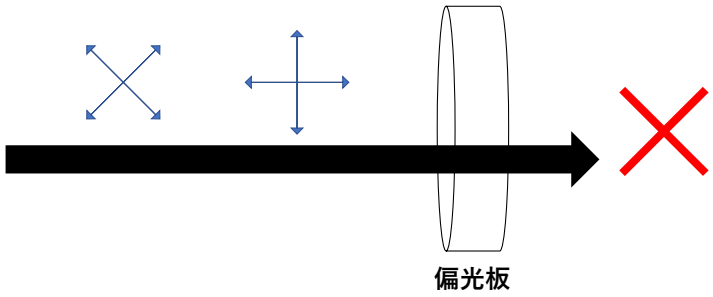


図 4.1: どの方向に偏光しているか

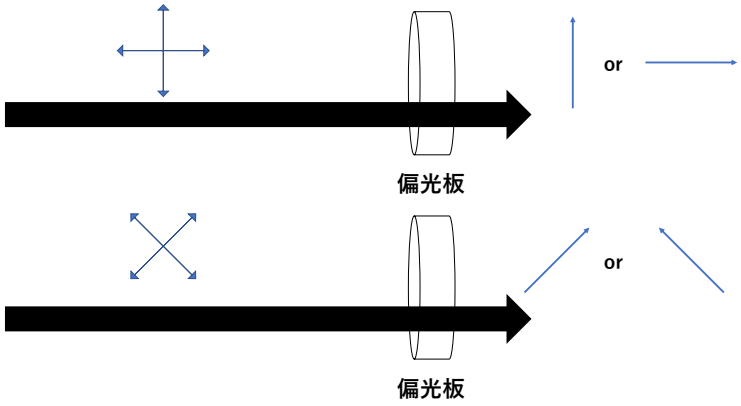


図 4.2: 特定の方向に偏光しているか

偏光をもう一度偏光板に通すことにより、偏光方向を測定可能である。例えば水平方向に偏光させる偏光板を用いて測定をする場合、この偏光板に水平偏光を通すと、偏光板をそのまま通過する。一方この偏光板に垂直偏光を通すと、偏光板を屈折して通過する。この通過した 2 方向の先で測定することにより、入射した光がどの偏光なのかを測定することができる。（図 4.3）

しかし、水平方向に偏光させる偏光板に例えば斜め 45 度に偏光した光を入射すると、入射光は偏光板をそのまま通過するか屈折し通過するかは確率に依存する。水平方向に偏光させる偏光板に斜め 45 度に変更した光を入射させて測定した場合、入射光が垂直水平方向の偏光なのか斜め方向の偏光なのかわからない。すなわち、水平方向に偏光させる偏光板では、入射光が垂直水平方向のどちらかに偏光しているかは測定可能だが、垂直水平方向か斜め方向の偏光かは測定不可能である。このように偏光がどの方向（垂直水平方向か斜め方向のどちらか）に偏光しているかどうかは判定不可能である（図 4.4）。

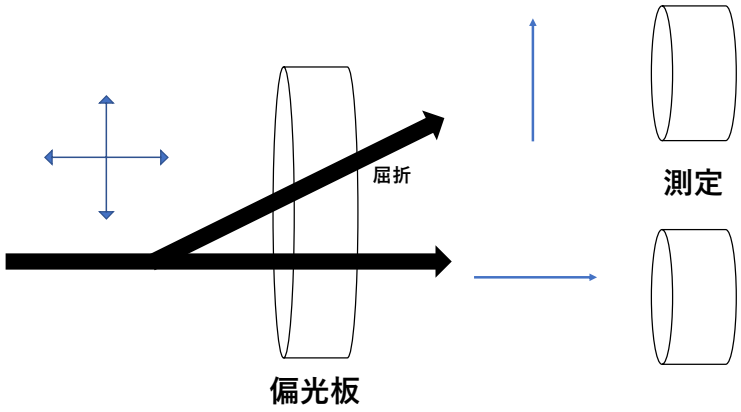


図 4.3: 入射した光がどの偏光なのかを測定する

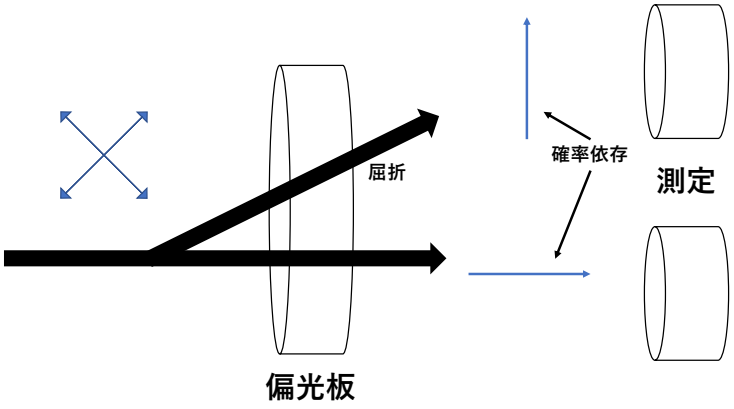


図 4.4: 水平方向に偏光させる偏光板へ斜め 45 度の偏光を入射

4.1.2 偏光を用いた量子暗号

この現象より量子暗号は実現可能である。例えば偏光方向が垂直なら 1 ビット、偏光方向が水平なら 0 ビット、のように、あらかじめ偏光の方向に対して送るデータのビット値を決めておく。この偏光と送るデータの対応を知っている人物は正しい偏光方向で測定すれば正しいビット値を得ることが可能である。

もし誤った偏光方向で測定した場合は、確率に依存してビット値は得られるため、受信者は正しい値を取得できない場合がある。これだけでなく、誤った測定をしたあとの光は測定により状態が変化してしまい、正しい受信方法を知っていても誤った情報を得ることになる。送信者・受信者がこの偏光と送るデータの対応をあらかじめ共有しておけば、仮に通信路上で第三者からの盗聴があっても、状態が変化することにより盗聴の影響を検知することが可能である。

4 つの偏光方向によりビット値を示し鍵共有を行うものが BB84 量子鍵配送である。送信者・受信者が量子もつれをした 2 つの量子を共有し、ベル不等式（量子もつれした 2 つの量子がどれくらい強く関係を持っているかを示す式）を用いて鍵共有を行うものが E91 量子鍵配送法である。本研究では BB84 鍵共有法と E91 鍵共有法を研究対象とし、以下で BB84 と E91 の詳細について述べる。

	E91	BB84
現段階	実験段階	商用化済み
実現可能な通信方法	End-to-End 通信	Neighbor-to-Neighbor 通信

表 4.2: E91 と BB84 の比較

4.2 BB84

光の 4 つの偏光法方向をビット値で示し、重ね合わせの原理を用いて鍵共有を行う方法が BB84 である。1984 年にチャールズ・ベネットとジャイルズ・ブラザードにより考案される [2]。

4.2.1 BB84 における鍵共有

BB84 は「垂直と水平」・「右斜めと左斜め」のような 2 組、4 種類の偏光を用いてビット値を示す。例えば水平を 0 度、垂直を 90 度、右斜めを 45 度、左斜めを 135 度として、偏光の角度とビット値を対応させる。水平偏光と右斜め偏光を 0、垂直偏光と左斜め偏光を 1 のように偏光とビット値は対応させることができる。

偏光	0	1
垂直と水平	→ (0 度)	↑ (90 度)
右斜めと左斜め	↗ (45 度)	↖ (135 度)

表 4.3: BB84 における偏光とビット値の対応

送信者は送りたいビット値に対応して偏光した光を受信者に送信する。ビット値に対する偏光（0 に対する水平偏光と右斜め偏光、1 に対する垂直偏光と左斜め偏光）は任意に選ぶ。受信した光は無作為に偏光しており、受信者はどのように偏光しているかわからないので、任意の偏光角度で測定する。

送信者が垂直偏光または水平偏光で光を送信した場合、受信者が垂直・水平偏光に測定すれば正しい偏光状態を測定することができる。一方この時に受信者が右斜め・左斜め偏光に測定すれば、確率的に偏光状態が測定される（十分に多く測定した場合は垂直・水平偏光がそれぞれ 1/2 の確率に収束する）（図 4.5）。

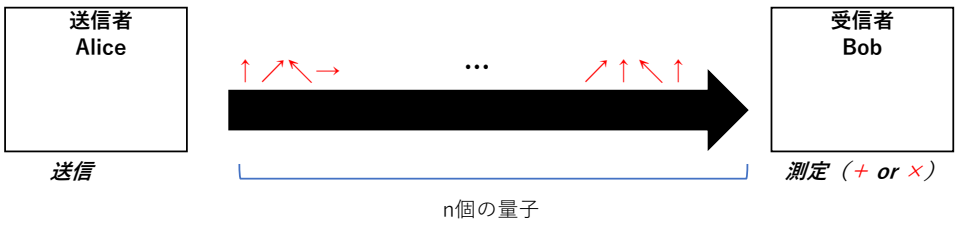


図 4.5: BB84 における送信者・受信者の量子の扱い

これは量子力学に従うと、偏光が特定の方向（例えば垂直水平方向のどちらか）に偏光しているかどうかは測定し判定することが可能だが、偏光がどの方向（垂直水平方向か斜め方向のどちらか）に偏光しているかどうかは判定不可能であることに帰因する。すなわち、送信者と受信者はそれぞれ任意の偏光方向で送信・受信するが、量子力学で判定可能なペア（「垂直・水平」または「右斜め・左斜め」）の偏光角度で送受信をした場合に正しいビット値を得られることになる。

受信者は受信したすべての偏光を測定し終わったら、すべての偏光についてどのような測定方法を用いたかを任意の方法で送信者に送り、どの偏光のときに正しく偏光方向を判定可能な測定をしたかを確認する。正しく偏光方向を測定可能な測定（送受信者はともに「垂直・水平方向」を使った、または「右斜め・左斜め」を使った）ときは、正しいビット値が共有される（図 4.6）。このときの受信した正しいビット値の集まりが、共有した鍵となる。

Aliceが送るビット値	0	1	1	0	0	1	0	1	1	1	0	1	0	…
Aliceが送信する偏光方向	+	+	×	×	+	×	+	×	+	+	×	×	×	…
Aliceが送る偏光	→	↑	↖	↗	→	↖	→	↖	↑	↑	↗	↖	↗	…
Bobが測定する偏光方向	+	×	×	+	×	×	+	+	+	+	×	×	+	…
Bobが測定する偏光	→	↖	↖	→	↗	↖	→	↑	↑	↑	↗	↖	→	…
共有した鍵のもととなるビット値	0		1			1	0		1	1	0	1		…

図 4.6: BB84 における鍵共有

4.2.2 BB84 における盗聴の影響

量子力学に基づき偏光した光により鍵共有が可能となったが、この方法では盗聴することが理論上不可能である。通信路上で考えられる盗聴の方法は以下の通りの方法が考えられる。

1. 送信・受信者がどのような偏光方向で測定したかを盗聴する。
2. 通信路上で偏光を測定し、測定した結果に対応する偏光をもう一度送り直す。
3. 通信路上で偏光を測定しないで保存し、送信・受信者の測定方法を盗聴し、同じ測定をする。

以下でそれぞれの盗聴が理論上不可能となる原理を示す。

1. 送信・受信者がどのような偏光方向で測定したかを盗聴する

この場合は偏光方向を知っただけでは測定する偏光がないため盗聴は不可能である。もし送受信者が測定して得た結果を共有していた場合は、この値を盗聴すれば鍵の盗聴が可能だが、送受信に用いた偏光方向を共有するだけで正しいビット値の共有は可能である（図 4.7）。

2. 通信路上で偏光を測定し、測定した結果に対応する偏光をもう一度送り直す

この場合は、盗聴者は受信者と同じく送信者が使った偏光方向を知らないので、任意の偏光方向で測定する（図 4.8）。以下の場合は送信・受信者は盗聴者の影響に気づくことはない。

- 盗聴者が送信者と同じ偏光方向で測定し、同じ偏光方向で受信者に送信する
- 盗聴者が送信者と異なる偏光方向で測定したが、たまたま送信者と同じ偏光で測定し、この偏光方向で受信者に送信する

1 つ目の場合の確率は、偏光方向が送信者と同じか異なるかで 1/2 の確率である。 2 つ目の場合の確率は、偏光方向が異なる場合の 1/2 の確率の上で、たまたま正しい偏光方向で測定するか、異なる偏光方向で測定するかの 1/2 の確率で、$1/2 \times 1/2 = 1/4$ である。すなわち、 この総和である $1/2 + 1/4 = 3/4$ の確率で盗聴者の影響に気づかれない場合がある。

しかし、送信するビット毎にこの確率だけ盗聴者の影響に気づかれないので、n ビットの情報が送信された場合、$(3/4)^n$ となる。この値は n が十分に大きい場合は小さな値となるため、理論上盗聴の影響はないと言える。

3. 通信路上で偏光を測定しないで保存し、送信・受信者の測定方法を盗聴し、同じ測定をする

量子状態に何らかの作業を加えたとき、状態が変化することは不可避である。すなわちこの場合は、偏光を測定しないで保存することが不可能なため、盗聴は不可能である（図 4.9）。

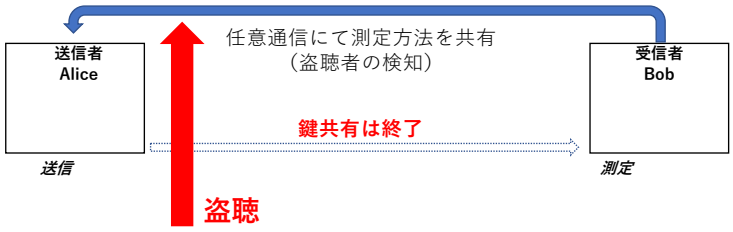


図 4.7: 送信後の偏光方向を盗聴

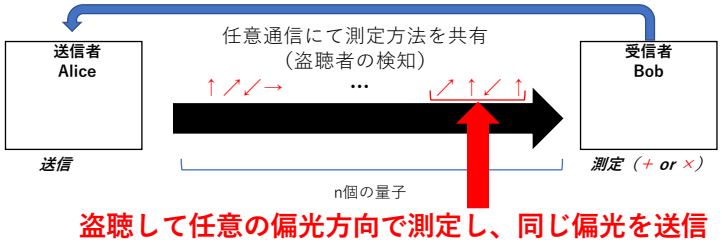


図 4.8: 通信路上で偏光を測定

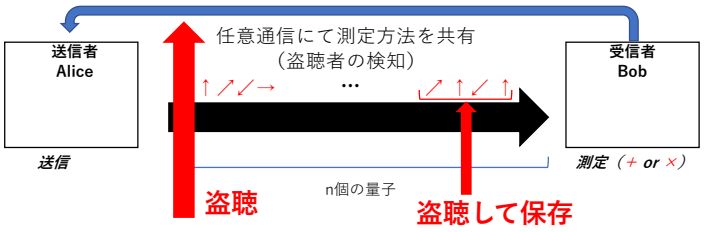


図 4.9: 通信路上で偏光を保存し、盗聴した偏光方向で測定

4.3 E91

送信者・受信者が量子もつれをした 2 つの量子を共有し、ベル不等式（量子もつれした 2 つの量子がどれくらい強く関係を持っているかを示す式）を用いて鍵共有を行うものが E91 である。1991 年にアルトゥル・エカートにより考案される [3]。

まず量子もつれとそれにまつわる EPR パラドックスについて述べる。

4.3.1 量子もつれ

量子もつれとは、ある特定の 2 つの量子状態である。いま 2 つの量子ペアの状態が、

$$|\Phi_+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{4.2}$$

だった場合、1/2 の確率で、両方の量子状態が 0 または両方の量子状態が 1 と測定される。片方の量子状態が確定すると、もう片方の量子状態も即確定する。もしこの両方の量子状態が十分に（銀河系の端と端など）離れていても、片方の量子状態が確定すると、この距離上で光速を超えて測定結果が伝わると考えることができる。

量子もつれは量子のスピン方向にも言える。例えば着目する量子がはじめスピンしていなかったが、何らかの処理により 2 つに別れ、それぞれスピンし始めたとする。もしスピン方向は測定して片方が左周りなら、もう片方は右回りとなる。逆に測定して片方が右回りなら、もう片方は左周りとなる。

この考え方によると局所性 (ある地点での現象は、直ちに遠くへ影響を及ぼすことは無いという性質) を破る。局所性を破ると、すべてのものは光速を超えて伝わることはないというアインシュタインの特殊相対性理論 [17] に反するため、アインシュタイン・ポドルスキー・ローゼンはこのような量子もつれの性質をもつ量子力学に対し反対 [参考文献した。この量子力学の局所性に対する矛盾を **EPR パラドックス**と呼び、ベル不等式によって量子もつれの存在が確認され、矛盾でないことが立証された。

4.3.2 EPR パラドックス

量子力学に反対するアインシュタイン・ポドルスキー・ローゼンは、測定時に 2 つの状態が確定するのではなく、2 つに別れた時点で何らかの隠れた変数によりなにかしらのつながりが発生しているのではないかという理論（隠れた変数理論）を唱えた。量子力学が正しいのか、隠れた変数理論が正しいのかの論争は、1964 年にジョン・ベルが考えた**ベル不等式** [18] によって解決され、量子もつれの存在が確認された。

以下でベル不等式による EPR パラドックスの解決法を述べる。

量子のスピンとその相関

ベル不等式では量子もつれをしている量子ペアの関係の強さの度合い（相関）から不等式の値を求める。

ここでは、先ほどの例と同じく分裂によりスピンを始めた 2 つの量子相関に着目する。スピン方向に関して量子もつれが発生していると言えるのは述べた通りである。着目する量子のスピン方向を、ブロッホ球（図 2.1）の YZ 平面上で x 軸上周りに任意の角度ずらした軸を中心に定めるとする（図 4.10）。

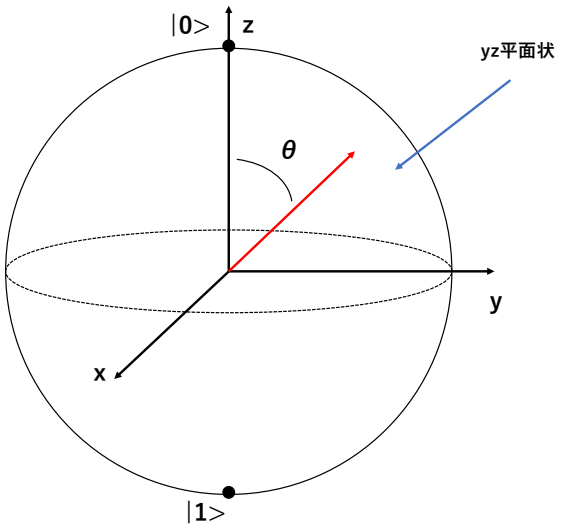


図 4.10: 量子スピンの方向を測定する軸

例えば、ブロッホ球上の x 軸上を 45 度回転した軸をスピン方向の中心とすると、スピン方向がこの軸を中心に時計周りなら 1、反時計周りなら-1 とする。このように x 軸上を何度か回転した軸を中心に、どの方向にスピンしているかを測定する。分裂後のそれぞれが関係（隠れた変数）をもつかどうかをベル不等式を用いて判定する。

古典力学に基づく CHSH 不等式

これをベル不等式を用いて隠れた変数を持たないことを示すことができる。本研究ではベル不等式の 1 つである **CHSH 不等式** [19] を用いた。以下で CHSH 不等式について述べる。

まず測定する軸を 4 種類決める。例えば、0 度、45 度、90 度、135 度と決め、これらの軸で測定した結果である± 1 の値を掛け合わせる。これを十分な回数実行し、それぞれの± 1 の総和から平均値を求める。この平均値を x とすると、

$$-1 \leq x \leq 1 \tag{4.3}$$

となる。

量子もつれをしている 2 つの量子スピンを測定した場合、片方が 1、もう片方が-1 になるときは、2 つの測定結果を掛けた値の平均値は-1 となる。この値は相関となるので、着目する 2 つの量子は分裂した時点で関係があるとされ、隠れた変数理論が正しいことになる。

2 つの測定値を掛けた値の平均値を a,b,c,d とすると、どれも実数であり、その絶対値は 1 以下となる。これらの値から、CHSH 不等式が導出できる。

$$S = |ab + bc - ad + bd| \leq 2 \tag{4.4}$$

量子力学に基づく **CHSH** 不等式

先ほどの例は測定する角度が異なるにも関わらず測定結果を± 1 とした。量子力学に従うと、測定した角度に関係して測定結果は確率に依存するので、ベル不等式の値を超える。

2 つの測定結果に関して、片方の測定結果が例えば 1 で、もう片方の測定結果も 1 になる場合は $\sin^2(\theta/2)$ となる。片方の測定結果が 1 で、もう片方の測定結果が-1 の場合は、$1-\sin^2(\theta/2)$ となる。

これらの確率値より、2 つの測定結果の相関値は

$$\sin^2(\theta/2) + (1 - \sin^2(\theta/2)) = -\cos(\theta) \tag{4.5}$$

となる。

例えば 2 つの測定角度が θ_a と θ_b だった場合、2 つの測定角度は $\theta = \theta_a - \theta_b$ となり、このときの相関値は

$$-\cos(\theta_a - \theta_b) = -\cos(\theta) \tag{4.6}$$

となる。

よって、量子力学に基づくと CHSH 不等式は、

$$S = |-\cos(\theta_a - \theta_b) + (-\cos(\theta_b - \theta_c)) - (-\cos(\theta_a - \theta_d)) + (-\cos(\theta_b - \theta_d))| \leq 2\sqrt{2} \tag{4.7}$$

となる。

1982 年にアラン・アスペが 2 つの光子の偏光に対するベル不等式値を実験により導出 [20] し、ベル不等式の値が $2\sqrt{2}$ を超え、量子力学が正しいことが示された。

4.3.3 E91 における鍵共有

E91 では、送信者・受信者が量子もつれをした 2 つの量子を共有し、ベル不等式を用いて盗聴の影響を測定し、鍵共有を行う。例えば次のような量子もつれをした 2 つの量子状態で偏光状態をビット値と対応させ、鍵を共有することができる。

$$|\Psi\rangle = \frac{|\updownarrow\updownarrow\rangle + |\leftrightarrow\leftrightarrow\rangle}{\sqrt{2}} \tag{4.8}$$

この量子状態に対し、垂直偏光を 1、水平偏光を 0 に対応させるとする（図 4.4）。片方の測定結果が垂直偏光の場合、量子もつれよりもう片方の測定結果も垂直偏光となり、1 が共有されたことになる。一方で片方の測定結果が水平偏光の場合、もう片方も水平偏光となり、0 が共有されたことになる（図 4.11）。

偏光	↔	↕
得られるビット	0	1

表 4.4: E91 における偏光とビット値の対応

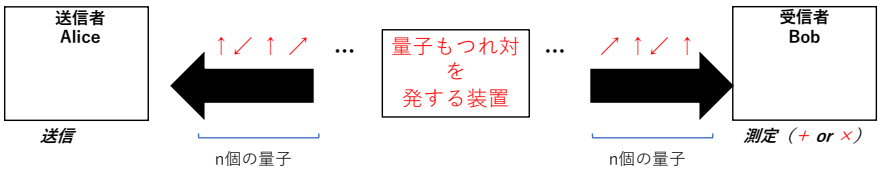


図 4.11: BB84 における送信者・受信者の量子の扱い

送信者、受信者の中央に位置する量子もつれ対の発信機から受信した量子状態を、送信者・受信者は 3 種類の任意の角度で測定する。3 種類のうち 2 種類の角度は同じだが、1 つだけ別々の角度とする。このうちの同じ角度で測定した結果が共有鍵のもとのビット値となる。例えば送信者は ABC、受信者は CDA の角度で測定するとする。受信した量子状態の集まりに対して、それぞれ次の角度で測定した。

・送信者　CABCBCABC …
・受信者　DADCDCACD …

今回は 2 回目、4 回目、6 回目、7 回目で送信者・受信者ともに同じ角度で測定したため、この時の量子状態の測定結果が共有鍵のビット列のともとなる。一方異なる角度で測定した場合のビット列は盗聴者の影響の確認に用いる。BB84 と同じく、通信が終了した後、それぞれどの角度で測定を行ったのかを古典通信などの任意の通信で異なる角度で測定した場合のビット列でベル不等式値を導出し、盗聴者の影響を判定する（図 4.12）。

異なる角度で測定した結果でベル不等式値を導出する

Aliceが送るビット値	0	1	1	0	0	1	0	1	1	…
Aliceが測定する角度	C	A	B	C	B	C	A	B	C	…
Bobが測定する角度	D	A	D	C	D	C	A	C	D	…
共有した鍵のもととなるビット値		1		0		1	0			…

図 4.12: E91 における鍵共有

4.3.4　E91 における盗聴の影響

異なる角度で測定した場合はベル不等式を用いた盗聴の有無の確認に用いる。通信路上で考えられる盗聴の方法は以下の通りの方法が考えられる。

1. 送受信者が受け取る予定の量子を適当な角度で測定を行い、同じ偏光の量子を送り直す。
2. 送受信者が受け取るはずの両方の量子を途中で測定し、測定結果と同じ偏光の量子を送り直す。
3. 送受信者が受け取るはずの両方の量子を途中で測定し、新たに量子もつれ対を送り直す。

以下でそれぞれの盗聴が理論上不可能となる原理を示す。

1. 送受信者が受け取る予定の量子を適当な角度で測定を行い、同じ偏光の量子を送り直す

送受信者が通信後にどの角度で測定を行なったか確認した値のうち異なる角度で測定した値を元にベル不等式値を求める。この場合は、新しい量子を送信するため、送受信者の量子は量子もつれになっていないことになる。このような量子ペアがある程度の割合を超えるとベル不等式は破れなくなる。ベル不等式が破れなくなると、盗聴の検知が可能となる（図 5.3）。

2. 送受信者が受け取るはずの両方の量子を途中で測定し、測定結果と同じ偏光の量子ペアを送り直す

この時、イブは量子もつれの状態を知り、その結果に基づいた量子状態をアリス・ボブに送信する。これはアリスとボブは量子もつれをした光子対を受信したかのように考察することが可能であるが、先ほどの場合と同じく量子もつれしていない光子対を受信するため、このような量子ペアがある程度の割合を超えるとベル不等式は破れなくなる（図 4.14）。

3. 送受信者が受け取るはずの両方の量子を途中で測定し、新たに量子もつれ対を送り直す

この場合は量子もつれを測定結果と同じ状態で送信することはできない。量子もつれは測定することで状態が確定するからである。この場合は盗聴者は通信路上の量子の測定をしても、新たな量子もつれ対を送信するため、送受信者がどのような量子もつれ対を受信するかはわからない。すなわち、送受信者が鍵とするビット自体の盗聴は出来ていない（図 5.5）。

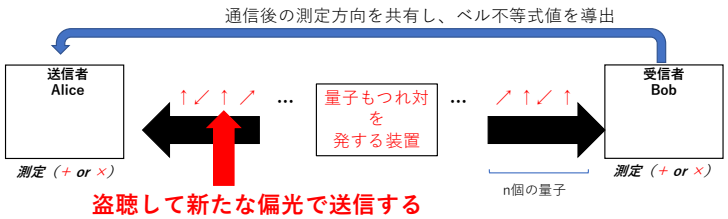


図 4.13: 通信路嬢で片方の量子を測定し、同じ偏光で送る

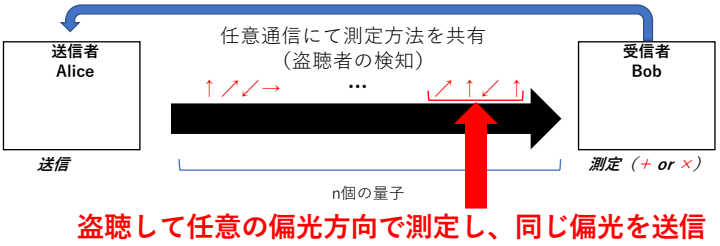


図 4.14: 通信路上で偏光を測定し、同じ偏光で送る

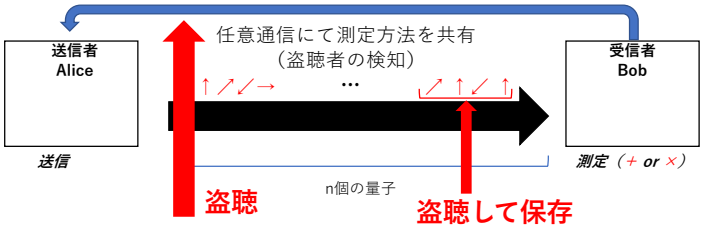


図 4.15: 通信路上で偏光を測定し、新たな偏光で送る

第5章　実験

本章では、本研究の実験内容について述べる。まずシミュレータの概要とシミュレータ内容の概要を述べ、次に実験内容を考察する。

5.1　シミュレータの概要

シミュレート環境は以下の通りである。

OS	OSX High Sierra
プロセッサ	2.7 GHz Intel Core i5
メモリ	16GB
使用言語	python3.7.0

表 5.1: シミュレートを行ったハードウェア情報

本環境で、Bell Test,BB84,E91 についてのシミュレータを実装した。実行したシミュレート実験の内容は次の通りである。

5.2　Bell Test

E91 では送信者・受信者が量子状態の測定を異なる角度で行った場合、ベル不等式で量子もつれをしている量子ペアの関係の強さを導出する。4 つの測定角度を変化させベル不等式値がどのように変化するかを導出した。

シミュレート内容の概要

このシミュレータは、E91 における量子状態を共有する物理層と、物理層における通信後の測定方向の確認をする古典通信をシミュレートする（図 5.1）。本実験では量子相関かどうかを示すのみなので、ノイズの影響は考えない。主な手順は以下の通りである。

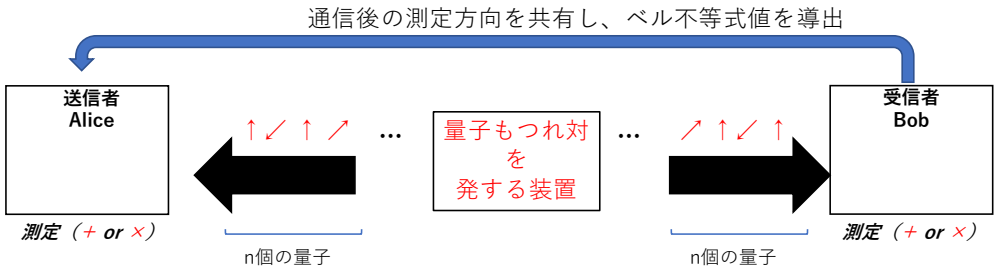


図 5.1: Bell Test

1. 任意のビット数の量子もつれ状態 $|\Phi_+\rangle$ を送信者と受信者で共有する
2. 送信者の測定角度は固定し、受信者の測定角度を± 5 度ずつ変更する
3. 送信者と受信者の測定角度から、量子もつれ状態を回転させる密度行列を導出する送信者の測定角度が 90 度、受信者の測定角度が 45 度の場合、回転行列は

$$R_{sender} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad R_{receiver} = \begin{pmatrix} 0.92387953 & 0.38268343 \\ 0.38268343 & -0.92387953 \end{pmatrix} \tag{5.1}$$

だった場合、このときの量子もつれ状態を回転させる密度行列は

$$\rho_{rotate} = \begin{pmatrix} 0.65328148 & 0.27059805 & 0.65328148 & 0.27059805 \\ 0.27059805 & -0.65328148 & 0.27059805 & -0.65328148 \\ 0.65328148 & 0.27059805 & -0.65328148 & -0.27059805 \\ 0.27059805 & -0.65328148 & -0.27059805 & 0.65328148 \end{pmatrix} \tag{5.2}$$

となる。

4. 求めた密度行列で回転後の密度行列を導出する量子もつれ状態は

$$\rho_{|\Phi_+\rangle} = |\Phi_+\rangle\langle\Phi_+| == \begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 1/2 \end{pmatrix} \tag{5.3}$$

だから、これと先ほど求めた回転行列より、

$$\rho_{|\Phi'_+\rangle} = \rho_{rotate} \cdot \rho_{|\Phi_+\rangle} \cdot \rho^{\dagger}_{rotate} \tag{5.4}$$

$$= \begin{pmatrix} 0.4267767 & -0.1767767 & 0.1767767 & 0.4267767 \\ -0.1767767 & 0.0732233 & -0.0732233 & -0.1767767 \\ 0.1767767 & -0.0732233 & 0.0732233 & 0.1767767 \\ 0.4267767 & -0.1767767 & 0.1767767 & 0.4267767 \end{pmatrix} \tag{5.5}$$

が回転後の密度行列となる。

5. 回転後の密度行列から、測定結果が 0・1 になる確率を導出する

$$M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad M_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \tag{5.6}$$

だから、測定結果が 0 となる確率は、

$$P_0 = Tr(M_0^\dagger M_0 \rho_{|\Phi'_+\rangle}) \tag{5.7}$$

であり、測定結果が 1 となる確率は

$$P_1 = Tr(M_1^\dagger M_1 \rho_{|\Phi'_+\rangle}) \tag{5.8}$$

となる。

6. それぞれの確率の数だけ測定結果を決定する
7. 決定した測定結果を元に相関値を求め、この値をもとにベル不等式を導出する

シミュレータによる実験

1000 組の量子もつれをした量子ペアを共有し、ベル不等式値を導出した。ベル不等式値は送信者の測定する角度は固定し、受信者の測定する角度を± 5 度ずつ変化させるため、1000 組の量子もつれをした量子ペアによるベル不等式の導出を 72 回行った。本実験で E91 に用いたシミュレータが量子相関に伴うかどうか示す。

シミュレータによる実験の結果

シミュレータによる実験の結果は以下の通りである。

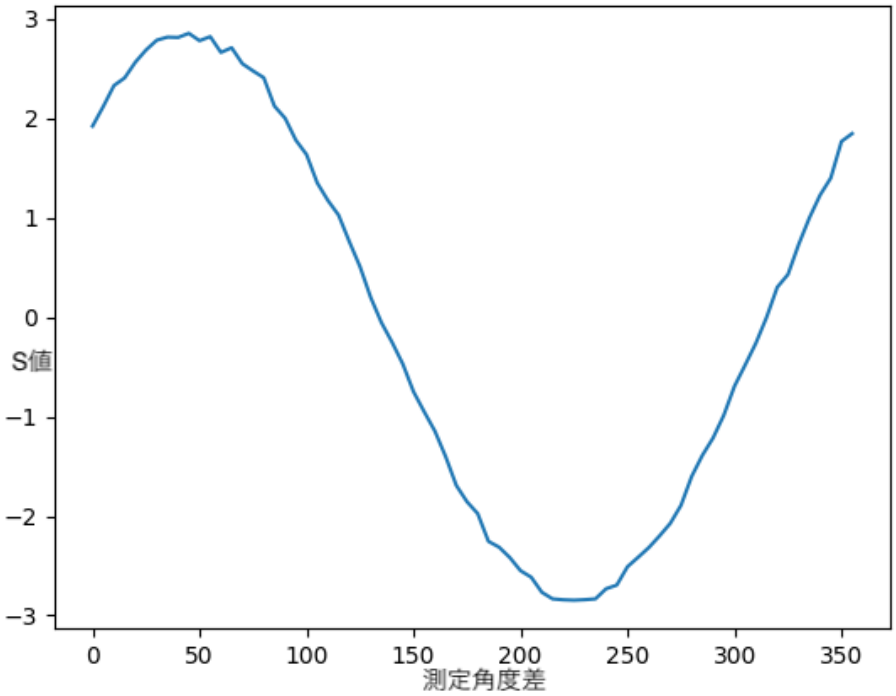


図 5.2: Bell Test のシミュレータによる実験の結果

シミュレータによる実験の結果は量子力学に基づく CHSH 不等式の値である

$$S = |-\cos(\theta_a - \theta_b) + (-\cos(\theta_b - \theta_c)) - (-\cos(\theta_a - \theta_d)) + (-\cos(\theta_b - \theta_d))| \leq 2\sqrt{2} \qquad (5.9)$$

と等しくなった。実験では飛び値が存在する場合があるが、送信するビット数が十分に大きくなればより三角関数のグラフに収束する。

5.3 E91

5.3.1 E91 における盗聴の影響

シミュレート内容の概要

CHSH 不等式と同じように、送信者と受信者は 1 つだけ異なる 3 種類の測定角度にて、ベル不等式を求める。(図 5.3)。このとき通信路上で片方の量子を測定し、同じ偏光で量子を送信し直した場合、ある程度の割合までなら盗聴の影響には気がつかない。

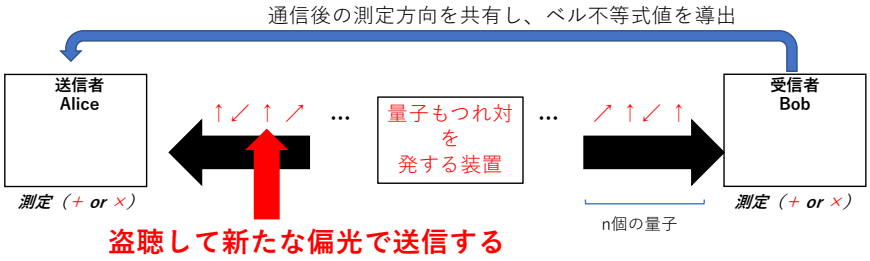


図 5.3: 通信路上で片方の量子を測定し、同じ偏光で送る

シミュレータによる実験

1000 組の量子もつれをした量子ペアを共有し、盗聴者は任意のビットを受信者の前に測定する。盗聴するビット数が増えるとどのような影響がでるか測定した。

シミュレータによる実験の結果

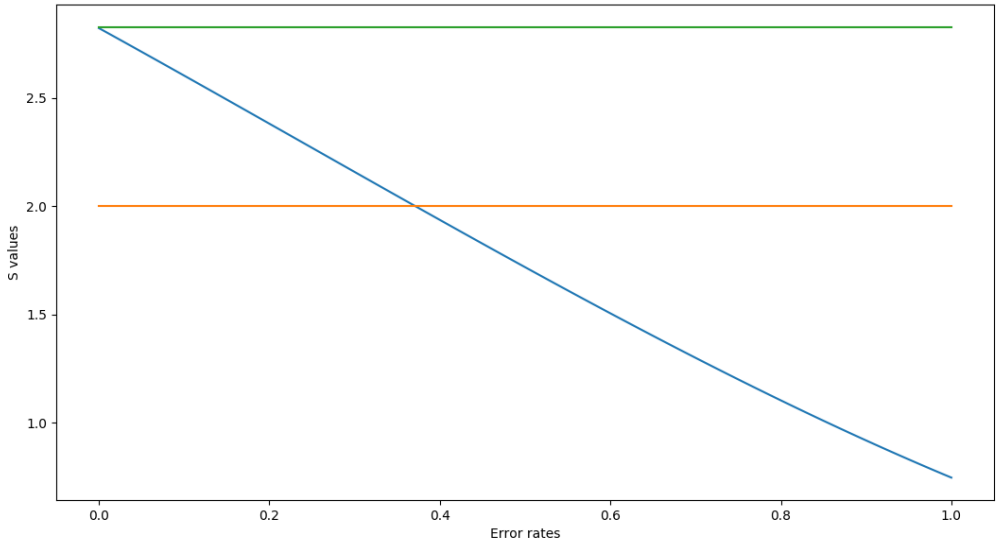


図 5.4: 通信路上で片方の量子を盗聴し、同じ偏光で送る

5.3.2 E91 におけるノイズの影響

実際の E91 上ではノイズの影響を受ける。物理層上でノイズを発生させ量子状態を変化させ、その影響を測る（図 5.5）。用いたノイズは以下の通りである。

- X error：ビット反転を発生させる
- Y error：ビット反転と位相反転を発生させる
- Z error：位相反転を発生させる

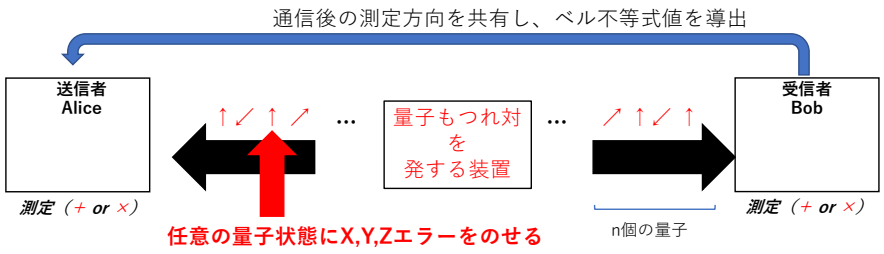


図 5.5: E91 にてエラーを発生させる

シミュレータによる実験

1000 組の量子もつれをした量子ペアを共有し、それぞれのエラー率か 5%ずつ上がった場合の影響を測定した。

シミュレータによる実験の結果

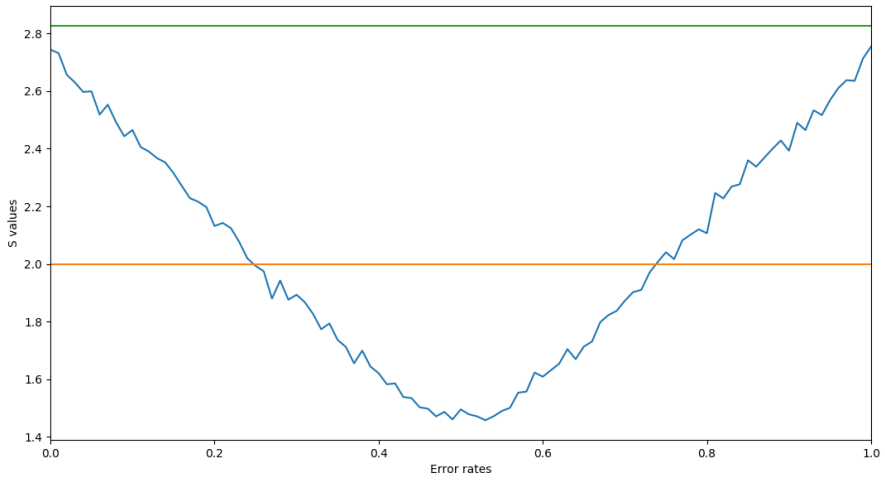


図 5.6: E91 にて X エラーを発生させる

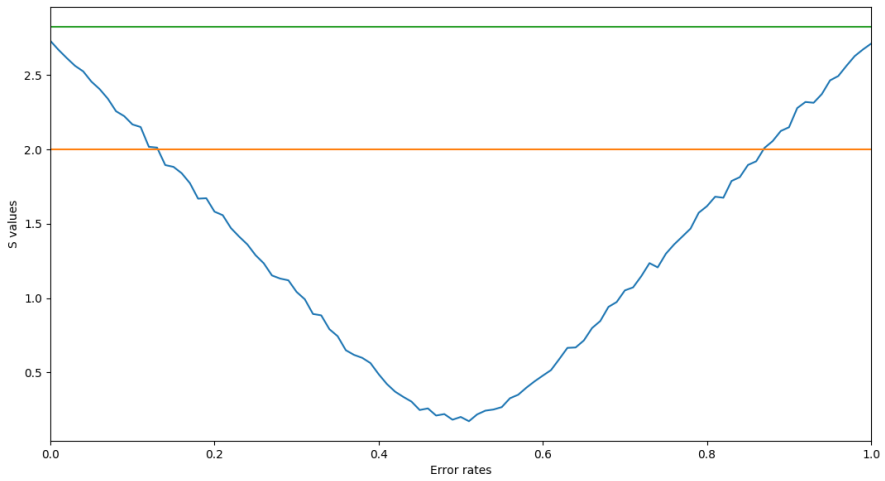


図 5.7: E91 にて Y エラーを発生させる

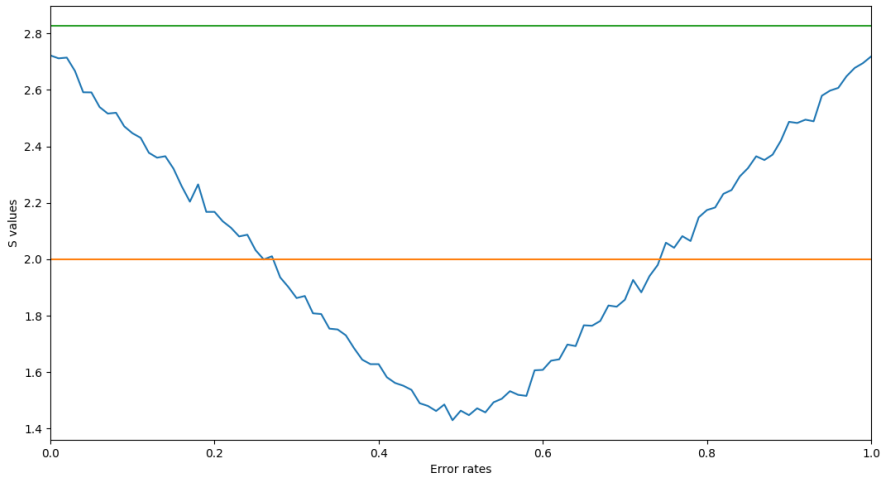


図 5.8: E91 にて Z エラーを発生させる

5.3.3 E91 におけるノイズおよび盗聴の影響

通信路上でノイズ・盗聴により量子状態を変化させ、その影響を測る（図 5.9）。

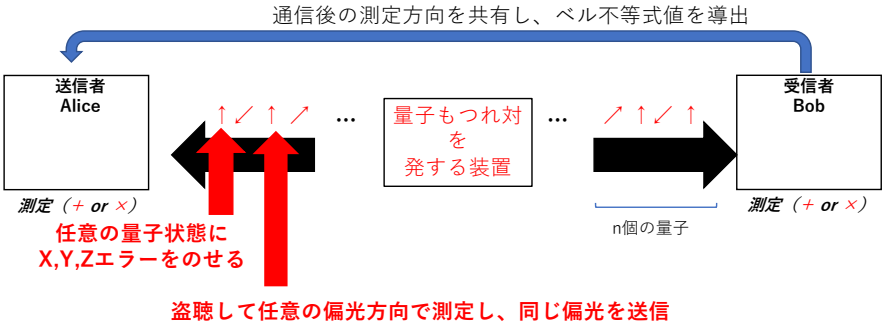


図 5.9: 通信路上で片方の量子を測定し、同じ偏光で送る

シミュレータによる実験

1000 組の量子もつれをした量子ペアを共有し、Z エラーを 25%、27%、28%に固定し発生させ、盗聴率が上がった場合の影響を測定した。

シミュレータによる実験の結果

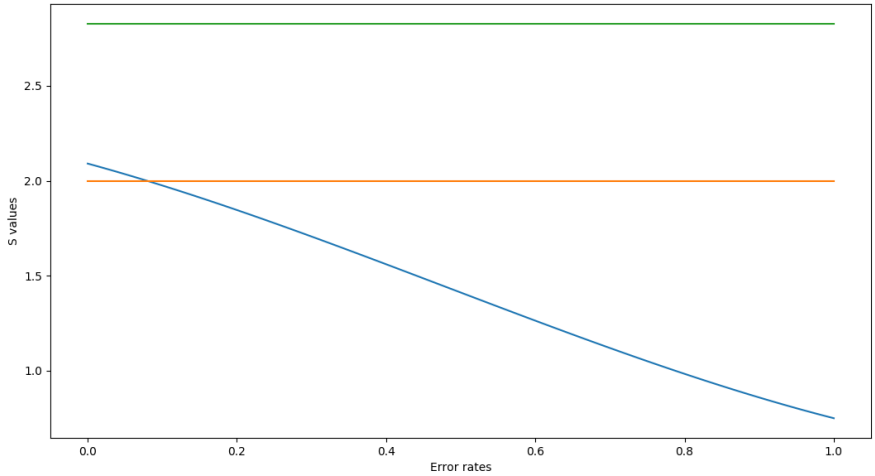


図 5.10: E91 にて Z エラーを 25%に固定し、通信路上で盗聴者を発生させる

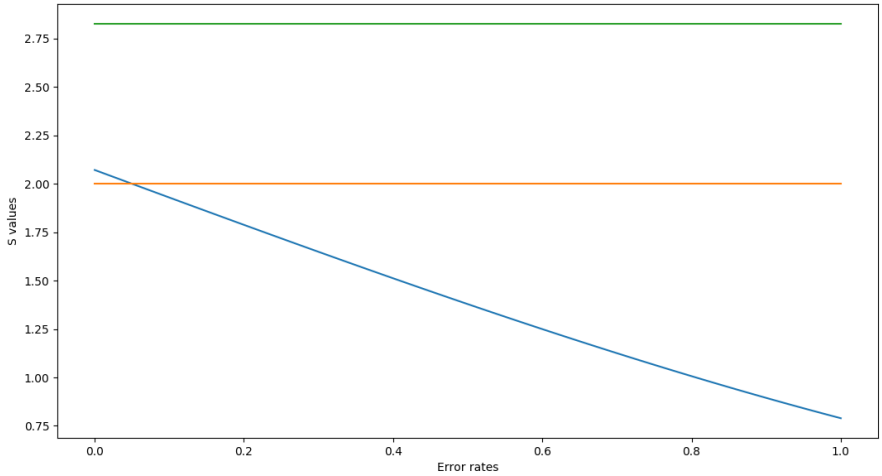


図 5.11: E91 にて Z エラーを 27%に固定し、通信路上で盗聴者を発生させる

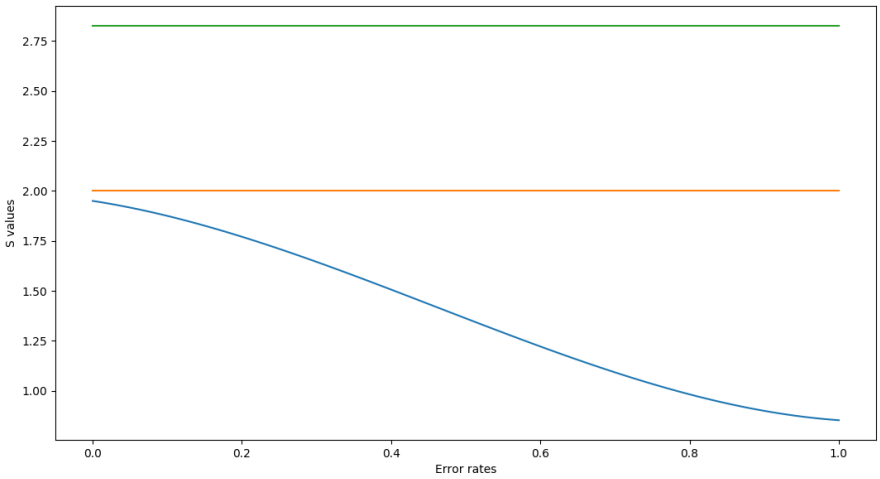


図 5.12: E91 にて Z エラーを 28%に固定し、通信路上で盗聴者を発生させる

第6章　評価

本章では、本研究の実験内容を評価し、E91 プロトコルを設計する。

6.1　実験の評価

6.1.1　Bell Test

まず本実験は量子相関に基づき実験をしていることが Bell Test のシミュレート実験よりわかった。現在は量子実験をするためにも機材が高価ゆえ、事実上量子実験自体が困難である。よって本実験により、本実験のシミュレータは量子実験のシミュレートができることが示された。また量子実験上のエラーレートを変更することにより、実験機器がどれくらいエラー耐性が上がれば量子鍵配送の実現コストが下がるのかが考察可能である。

6.1.2　E91

実験により、E91 が通信可能となる、ノイズ下における盗聴率の閾値を導出することができた。Z エラーが 27%までは通信が可能であるが、28%以上の場合はベル不等式値が常に 2 を下回るためノイズ・盗聴者の識別が不可能となり、通信不可能となることがわかった。

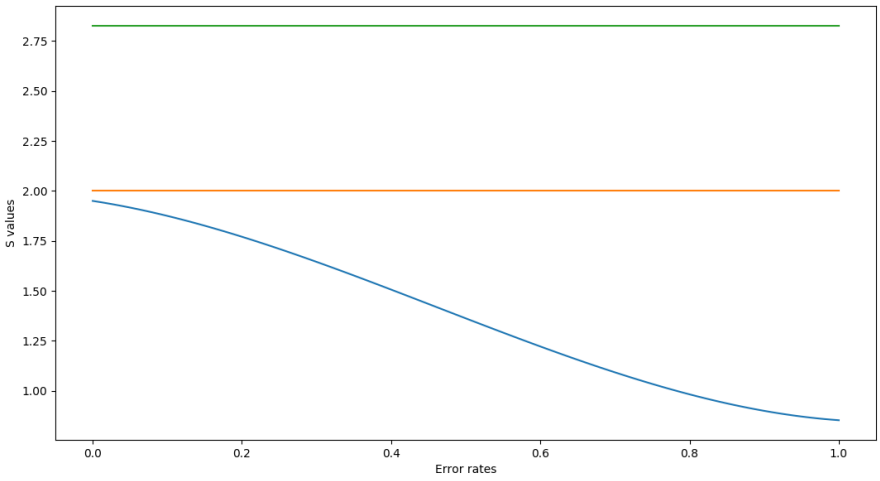


図 6.1: E91 にて Z エラーを 28%に固定した場合は常に 2 を下回るため、通信不可能

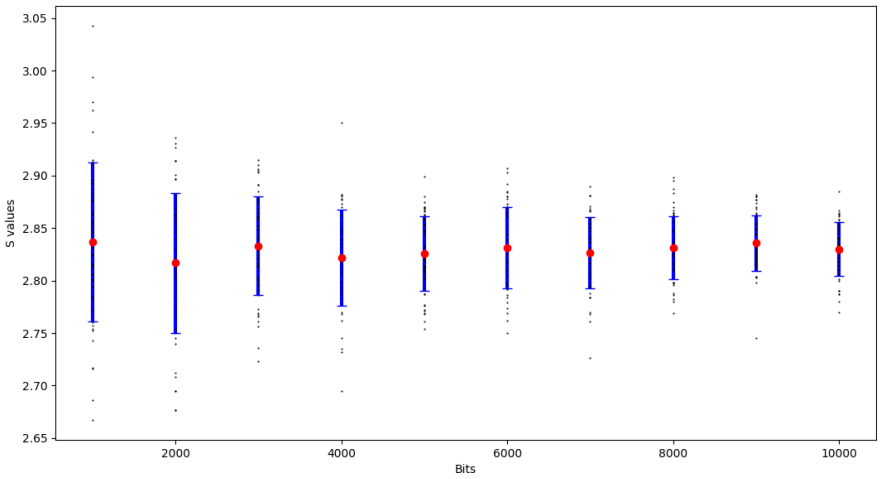


図 6.2: 共有したビット毎の S value

6.2 E91 による通信プロトコルの設計

E91 は現状でベル不等式通信プロトコルが定義されていない。本研究ではノイズ・盗聴によるベル不等式値の変化を 1 つのものとし、通信プロトコルを考案した（図 6.3）。

物理層は偏光のように量子もつれをしている量子ペアであればどんなものを扱っても良い。これが本プロトコルの鍵共有層である。通信を終えた後のそれぞれの測定方法の正誤の確認は、受信者が古典通信を用いて行う。この中の正しい測定方法で得たビット列が鍵となる。（鍵生成層）誤った測定方法で得たビット列は盗聴者の確認に用いる。受信者は手元でベル不等式値を導出する。もし盗聴者の影響が無ければベル不等式は破られるはずである。ベル不等式が破られていなかった場合は、もう通信路を変更し、もう一度通信する（盗聴検知層）。こうして盗聴の影響を受けずに生成された鍵を用いて、暗号通信を行う。既存の暗号通信の鍵共有である Diffie-Hellman に置き換わるので、TLS/SSL と IKE における鍵共有層で E91 を用いられることが可能である。

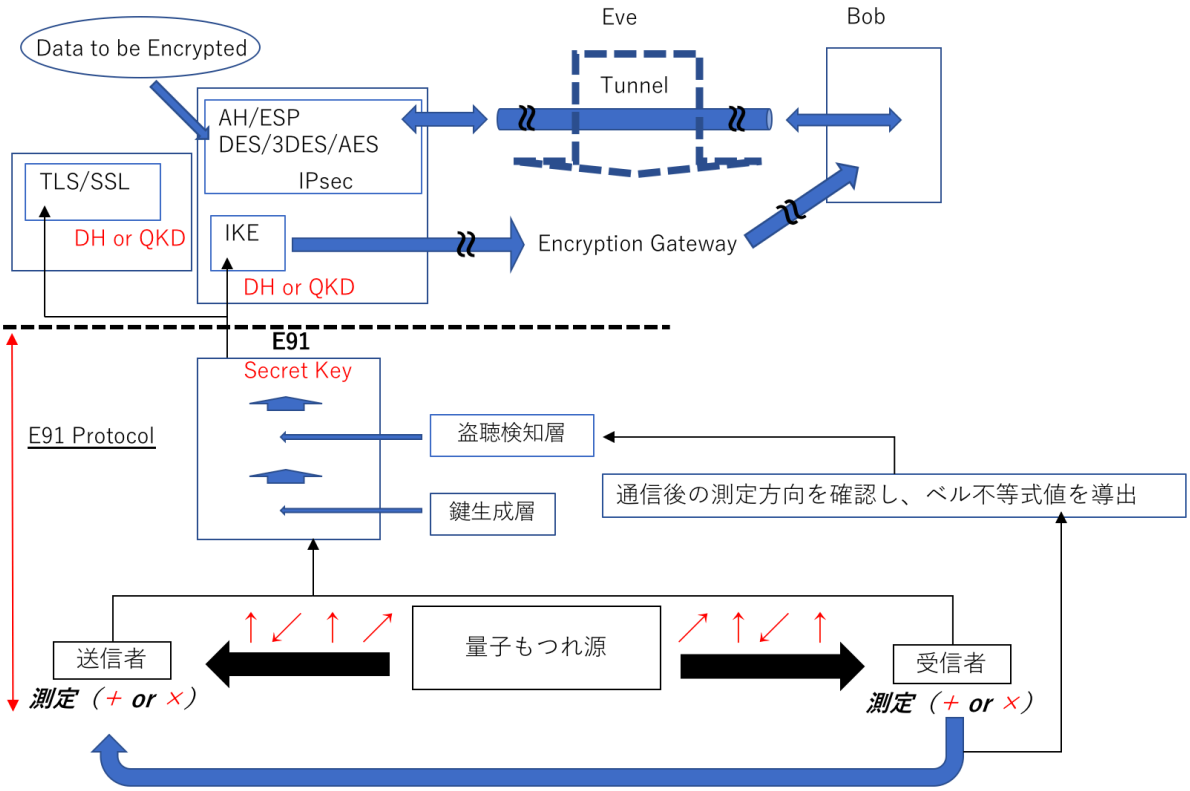


図 6.3: E91 による通信プロトコル

第7章　結論

本研究にて、通信機器のエラー耐性が向上すれば、E91 を用いた暗号通信は実現可能であると考える。E91 では Z エラーが 27%までは通信が可能であるが、28%以上の場合はベル不等式値が常に 2 を下回るためノイズ・盗聴者の識別が不可能となり、通信不可能である。現在は BB84 は商用化段階まで進んでいるが、BB84 は量子もつれを用いらないため Neighbor-to-Neighbor 通信しかできない。量子ネットワークにて広範囲に渡る通信網を築き上げるには、End-to-End 通信が可能な E91 が効果的であると考える。

本研究の対象は鍵共有のみだが、通信内容自体も量子力学により実装可能となると、量子ネットワークの実現が可能となる。このような背景では E91 による鍵共有を行う量子ネットワークの必然性が増すと考える。

今後の展望

本研究では暗号通信のうちの鍵共有層に関する実験を行っている。実際の暗号通信では共有した鍵を用いて通信内容の暗号化・復号を行うため、本量子鍵配送シミュレータで共有した鍵をもとに、実際に既存の暗号通信の実装が可能である。

謝辞

まず最初に、本研究を進める上で慶應義塾大学環境情報学部のロドニー・バンミーター准教授に様々な助言を頂き、指導して頂きました。また CQIS2018 における学会発表や、RIPE Quantum Hackathon2018 へ参加の機会を頂きました。自分にとって今まで体験したことがないものであり、これからの人生に置いてとても有益な体験をさせて頂きました。厚く感謝を申し上げます。

同時に慶應義塾大学政策・メディア研究科の佐藤貴彦特任助教には様々な助言を頂き、また指導して頂きました。自分がまだ研究に関する知識がない内から、基本的なことから教えて頂きました。厚く感謝を申し上げます。

慶應義塾大学政策・メディア研究科の松尾賢明先輩は様々な助言をして頂き、また実験環境の実装について一緒に考えてくれました。自分の研究があるにも関わらず私のために多大な時間を割いてくださりました。また時には夜遅くまで研究室に残り、議論に付き合ってくださいました。厚く感謝を申し上げます。

また、慶應義塾大学村井研究室バンミータ研究会の皆様にも感謝の意を表します。慶應義塾大学総合政策学部の西尾真君には、様々な質問により自分の研究の質を上げてくれました。また自分の研究における誤りを訂正してくれました。研究会の後輩皆様はそれぞれの活動を通し研究会自体を盛り上げ、それぞれの研究活動を通し、自分に様々なことを学ばせてくれ、自分の研究の支えになりました。厚く感謝を申し上げます。

最後に、村井・楠本・中村・高汐・バンミーター・植原・三次・中澤・武田合同研究プロジェクトに所属する研究メンバー全員に自分の研究をできる環境を与えてくださったことに感謝致します。

Bibliography

[1] Richard Feynman and Peter W. Shor. Simulating physics with computers. *International Journal of Theroritical Physics*, 21, 1982.

[2] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of International Conference on Computers, Systems, and Signal Processing*, 560:175 – 179, 1984.

[3] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[4] D Deutsch and R Jozsa. Rapid solutions of problems by quantum computation. *Proc. Roy. Soc. Lond. A*, 439:553 – 558, 1992.

[5] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26:1484 – 1509, 1997.

[6] Lieven M. K. Vandersypen, Matthias Steffen, Gregory Breyta, Costantino S. Yannoni, Mark H. Sherwood, and Isaac L. Chuang. Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414, 2001.

[7] P.A.M. Dirac. A new notation for quantum mechanics. *Mathematical Proceedings of the Cambridge Philosophical Society*, 35:416 – 418, 1939.

[8] W. Heisenberg. Über quantentheoretische umdeutung kinematischer und mechanischer beziehungen. *Zeitschrift für Physik*, 33:879 – 893, 1925.

[9] M. Born and P. Jordan. Zur quantenmechanik. *Zeitschrift für Physik*, 34:858 – 888, 1925.

[10] M. Born, W. Heisenberg, and P. Jordan. Zur quantenmechanik ii. *Zeitschrift für Physik*, 35:557 – 615, 1925.

[11] R. P. Feynman. Space-time approach to non-relativistic quantum mechanics. *Rev. Mod. Phys.*, 20:367 – 387, 1948.

[12] A. Shamir R. L. Rivest and L. M. Adleman. A method for obtaining digital signature and public-key cryptosystems. *Communications of ACM*, 21:120 – 126, 1978.

[13] Joan Daemen and Vincent Rijmen. Aes submission document on rijndael. 1998.

[14] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theor.*, 22:644 – 654, 1976.

[15] 鶴丸豊丸. 量子暗号の基礎とその実用化に向けて. http://ibisml.org/ibis2010/session/ibis2010tsurumaru.pdf, 2010.

[16] W Heisenberg. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Zeitschrift für Physik*, 43:172 — 198, 1927.

[17] Albert Einstein. Zur elektrodynamik bewegter körper. *Annalen der Physik*, 322:892 — 921, 1920.

[18] John S. Bell. On the einstein-podolsky-rosen paradox. *Physics*, 1:195 — 200, 1964.

[19] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880 —, 1969.

[20] A. Aspect, Philippe Grangier, and Gerard Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: A new violation of bell's inequalities. *Physical Review Letters*, 49:91 — 94, 1982.