Student Research of Cryptography, Quantum Mechanics and QKD for Information Security

Joseph Hodges
March 17th, 2017
California State University – Los Angeles

ABSTRACT

Encryption is a principle of means to guarantee the security of information [1]. This process scrambles a message so that its interpretation is difficult for anyone but the intended recipient. Due to the high volume of vulnerability in the technological modern era, more advanced cryptographic algorithmic techniques are imperative to protect our secrecy [2]. This paper will briefly touch on encryption and decryption examples and jump to quantum physic preliminaries for Quantum-Key Distribution (QKD) and its application to cryptography.

1. INTRODUCTION

Cryptography is the practice of secure communication from point *A* to *B* in the presence of third parties. We call these third parties adversaries or eavesdroppers, commonly referred to as Eve. The etymology of cryptography stems from the Greek where crypto means "hidden" or "secret" and graph, "writing" or "message" [3]. It is the discipline of encoding messages intended as immune from attack [4].

Claude Shannon[1], the father of information theory provides *Shannon Entropy* enabling a basic measure in information theory. His theory of *perfect secrecy* serves as configuration of "good" encryption. We evolve to QKD which is likely one of the most promising concepts in quantum information theory.

.

2. CLASSICAL CRYPTOGRAPHY

Classical cryptographic algorithms are categorized into three major fields: One-Time Pad, Public-key and Private-key schemes. This section will briefly discuss the OTP and basic public-key and private-key decryption and encryption examples. Attacks on classical encryption will not be discussed.

2.1 ONE-TIME PAD

Commonly referred to as the *Vernam Cipher*[2], a One-Time Pad is essentially an encryption scheme that uses its key once and never again – or it is destroyed. This renders the OTP impractical. However, it is "information-theoretically secure" [5], meaning that it provides no known information about the original message to the cryptanalyst. Moreover, it is perfectly secure but much too slow for most of sensitive transmissions. The OTP is mathematically expressed as

[1] Claude Elwood Shannon (April 30, 1916 – February 24, 2001) was an American mathematician, electrical engineer, and cryptographer known as "the father of information theory".

[2] Gilbert Sandford Vernam (April 3, 1890 – February 7, 1960) was a Worchester Polytechnic Institute 1914 graduate at AT&T Bell Labs. In 1917 he invented an additive polyalphabetic stream cipher and later co-invented an automated one-time pad cipher.

$$\mathcal{H}(\mathcal{M}) = \mathcal{H}(\mathcal{M}|\mathcal{C}) \tag{1.1}$$

where $\mathcal{H}(\mathcal{M})$ is the entropy of the *plaintext* in the message space $\mathcal{M}$ and $\mathcal{H}(\mathcal{M}|\mathcal{C})$, the conditional entropy of the *plaintext*, is given by the *ciphertext* in space $\mathcal{C}$. The OTP is furthermore defined by the set of all n-bit strings as expressed as

$$\mathcal{M} = \mathcal{C} = \mathcal{K} = \{1,0\}^n \tag{1.2}$$

then encrypt by

$$E(k, m) = k \oplus m \tag{1.3}$$

then decrypt by

$$D(k, c) = k \oplus c \tag{1.4}$$

However, the lemma is that the OTP has perfect secrecy because there exist no *ciphertext only* attacks. In other words, any cipher that has perfect secrecy must contain long keys [6]. Therefore, the key length is expressed as

$$||k|| \geq ||m|| \tag{1.5}$$

meaning that the length of the key is or is at most the length of the message. The *Stream Cipher* essentially makes the OTP *more* practical by replacing the random key by the pseudorandom key.

2.1.1 Stream Cipher

Instead of using a totally random key, we use Pseudorandom Generator (PRG) that is generally expressed as

$$PRG : G{:}\{0,1\}^s \rightarrow \{0,1\}^n, n \gg s \tag{1.6}$$

The PRG is a function, say, *G* that takes a seed $\{0,1\}^s$ mapped into $\{0,1\}^n$ where the property *n* is sufficiently larger than *s* [2]. The goal is that the generator is to serve as efficiently computable by a deterministic algorithm [2]. Importantly, the only random seed that is given is into the function *G*.

Now, our key is used with the generator to expand the seed into a pseudorandom sequence, $G{:}\{0,1\}^s$, and taking the exclusive-or with the message, exactly as expressed in the OTP, equations (1.3) and (1.4). We note that the Stream Cipher can never be perfectly semantically secure because the key is always longer than the message [2].

2.1.2 Unconditional Security

We return to the OTP which shows a perfect implementation of Unconditional Security represented in this paper as

$$\Pr_{k \rightarrow \mathcal{K}}[c = E(m_o, k)] = \Pr_{k \rightarrow \mathcal{K}}[c = E(m_1, k)] \tag{1.7}$$

Equation (1.7) tells us that provided any *ciphertext* c, the probability that, from some *plaintext* m_0, it is very likely that it is from the encryption of a some other *plaintext* or equivalently, the message m_1[7].

2.2 PUBLIC-KEY CRYPTOGRAPHY

Public-key cryptography uses asymmetric encryption for its cryptosystem where encryption and decryption perform using a different key – one public key and one secret key.

2.2.1 Asymmetric Cipher

The asymmetric cipher encryption scheme is defined over a triple of efficient algorithms. The generation algorithm that outputs a randomized public and secret key pair

$$G(k) \rightarrow (pk, sk) \tag{1.8}$$

The randomized encryption algorithm will take a public key and message to output a corresponding *ciphertext*

$$E(pk, m) \rightarrow c \tag{1.9}$$

The decryption algorithm that takes a secret key and *ciphertext* to output the message (or it will output a problem if an error occurred)

$$D(sk, c) \rightarrow m \tag{2.0}$$
$$D(sk, c) \rightarrow \perp \tag{2.1}$$

Therefore, we show the following consistency property is satisfied

$$\forall (pk, sk) \rightarrow G(k) \colon \forall m \in \mathcal{M} : D\big(sk, E(pk, sk)\big) \rightarrow m \tag{2.2}$$

that for all composed public and secret keys, we acquire a generation algorithm, that is provided with all messages, such that the decryption algorithm will use the secret key and encryption algorithm to output the message [4]. This is where the concept of *Semantic Security*[3] for a public-key system to be secure is essential [5].

This is illustrated as follows

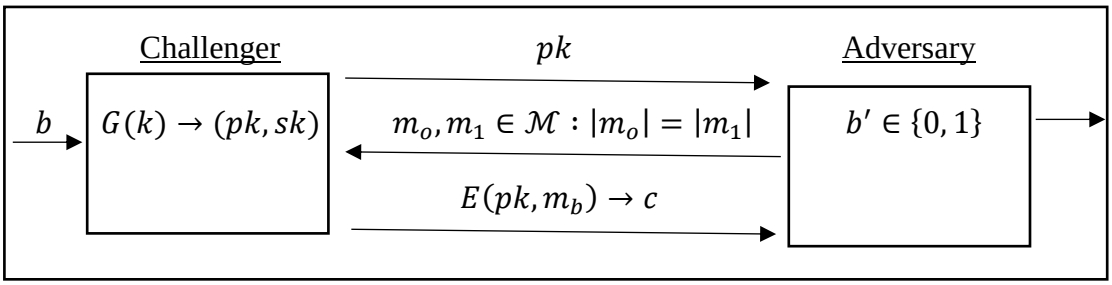

Fig. 2.4 Semantic Security Illustration

[3] Cryptosystems are semantically secure provided any PPTA (Probabilistic Polynomial Time Algorithm) possessing the *ciphtertext* of a particular message (or any distribution of messages) and its length will not reveal any partial information on the message, of course, with probabilistic non-negligibility.

For $b = 0, 1$ we define experiments 0 and 1 as $EXP(0)$ and $EXP(1)$. Therefore, we now show that $E(G(k)), E(pk,\ m_b), D(sk, c)$ is semantically secure [8] if for all efficient A:

$$Adv_{ss}[A, E] = |\ \Pr[EXP(0) = 1] - \Pr[EXP(1) = 1]\ | < negligible \quad (2.3)$$

The expectancy here is always negligible [8]. This means that the adversary cannot distinguish the secret key between the shared key. Although, this renders the asymmetric cipher completely vulnerable to the Man in the Middle Attack (MIMA) [8]. Which leads us to message integrity.

2.2.2 Message Integrity

The Message Authentication Code (MAC) is not an encryption or decryption algorithm. Instead, it serves as an integrity check. It is defined over a triple

$$\forall k \in \mathcal{K}, \forall m \in \mathcal{M}, \forall t \in T \quad (2.4)$$

which satisfies the consistency property such that for all keys in space $\mathcal{K}$, all messages in space $\mathcal{M}$ with all tags in space T. It is composed over two efficient algorithms, the verification and signing algorithm. The signing algorithm will output a tag based on the key and message. The verification algorithm – when composed with the signing algorithm – should produce 0 indicating that the sender is indeed who they say they are.

Unlike the symmetric cipher, the shared key, *k* is unknown to the adversary. Using Figure (2.5) Alice first generates a tag, *t* using the signing algorithm, which outputs a unique tag. Then Bob uses the verification algorithm with the tag, *t* generated from Alice

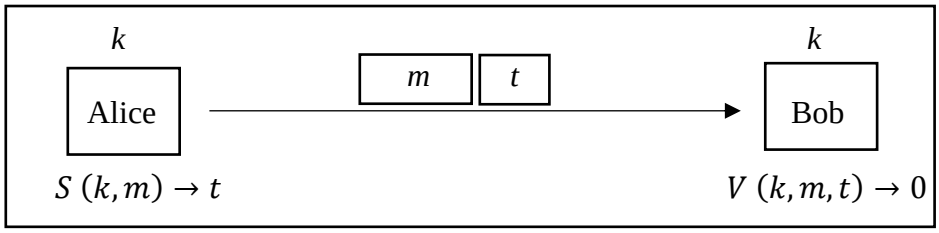

Fig. 2.5 MAC Illustration

Therefore, it is easy to see that

$$\forall k \in \mathcal{K}, \forall m \in \mathcal{M} : V\left(k, m, S(k, m)\right) \rightarrow 0 \quad (2.5)$$

the said composed algorithms satisfy the consistency requirements such that for all keys in space $\mathcal{K}$ and for all messages in space $\mathcal{M}$, when we verify the tag using a particular key and message – provided with some generic signing algorithm – Bob should receive a "yes" in response [9].

2.3 PRIVATE-KEY CRYPTOGRAPHY

Private-key cryptography uses symmetric encryption for its cryptosystem where the encryption and decryption algorithms perform on the same key. In this section, we are focused primarily with a basic symmetric encryption and decryption scheme.

2.3.1 Symmetric Cipher

Suppose Alice and Bob successfully communicate over a secure channel and agreed upon *protocol*[4] [6]. We now define a symmetric cipher over a triple

$$\forall k \in \mathcal{K}, \forall m \in \mathcal{M}, \forall c \in \mathcal{C} \tag{2.6}$$

which follows the consistency property such that for all keys in space $\mathcal{K}$, for all messages in space $\mathcal{M}$ and for all ciphertexts in space $\mathcal{C}$. The cipher is composed over two efficient algorithms, the encryption and decryption algorithm. The encryption algorithm is the product of the keys and the messages that output a *ciphertext*

$$E: \mathcal{K} \times \mathcal{M} \rightarrow c \tag{2.7}$$

The decryption algorithm is the product of the key and the *ciphertext* which outputs the original message

$$D: \mathcal{K} \times \mathcal{C} \rightarrow m \tag{2.8}$$

We start with Figure (2.1). Allow Alice a random byte for her message, *m*, whilst sharing an identical key, *k* with Bob. With Figure (2.2), Alice will then perform an exclusive-or computation to obtain the *ciphertext*.

Fig. 2.1 Concept Setup

Fig. 2.2 Encryption and decryption

Fig. 2.3 Transmission Protocol

With Figure (2.3), the *ciphertext* is sent to the receiving party using a generic protocol. Bob decrypts the message using the *ciphertext* and the *key* to obtain the

[4] Security protocols applies cryptographic methods and describes how algorithms should be used. They specific interactions between particular communicating entities.

original message, m. Since shared keys are identical and there are no eavesdroppers, this scheme is a candidate for secure communication. We find a deterministic result of

$$D\left(k, E\left(k, m\right)\right) \rightarrow m \tag{2.9}$$

meaning that for any decrypted key, *k* with *ciphertext c*, the message *m* will always be the same.

3. QUANTUM PHYSICS

We now move to Quantum physics or quantum mechanics, the fundamental study of subatomic particles such as atoms and, or photons. We are particularly concerned with photons, e.g., light as the transmission through a quantum channel. This is applied to QKD, briefly, as discussed in subsection (*4.1.1*).

3.1 *Heisenberg Uncertainty Principle*

The product of the change in momentum, *p* and position, *x* is or is at most half of *Planks constant*[5]

$$\sigma_x \sigma_p \geq \frac{\hbar}{2} \quad \text{or} \quad \Delta_x \Delta_p \geq \frac{\hbar}{2} \tag{3.0}$$

meaning that the more precise we measure one changing state, say Δ_p the less precise the other state becomes. This is due to the nature of quantum measurement. The constant

$$\hbar \approx 1.054 \times 10^{-34} Js$$

referred to as "h-bar", and many of its variants, is absolute and central to quantum physics [10].

3.2 *The Photon – The Particle of Light*

The photon represents the light we see around our world. It is said to be massless. Physicists use photons to describe properties of the language of *special relativity*[6]. It is the quantum of all forms of electromagnetic radiation [12]. This paper, however, is only concerned with transmission of photons through the quantum channel, as discussed in subsection (*4.2.1*). Essentially, in this technique we map bits to photons.

.

3.3 *Dirac and Bra-Ket Notation*

Coined by *Paul Dirac*[7], most quantum systems include bra-ket notation. It consists of a left part, the bra $\langle\psi|$ and a right part, the ket $|\psi\rangle$. Here we are using the Greek letter ψ to denote its superposition state. This is the standard notation for states in quantum mechanics.

---

[5] Max Karl Planck (April 23, 1858 – October 4, 1947) was a German theoretical physicist whose work on quantum theory won him the Nobel Prize in Physics in 1918.

[6] Special relativity is a theory proposed by Albert Einstein that describes the propagation of matter and light at high speeds.

[7] Paul Adrien Maurice Dirac (August 8, 1902—October 20, 1984) was an English theoretical physicist who made fundamental contributions to early development of both quantum mechanics and quantum electrodynamics.

3.4 *Quantum bit*

Since the beginning of information theory the *bit* has been the most fundamental unit of measurement. We know these states as either 0 or 1. In accordance with this classical concept there exists the quantum concept where two states $|0\rangle$ and $|1\rangle$ are simultaneously possible. In other words, they both exist in a state of superposition.

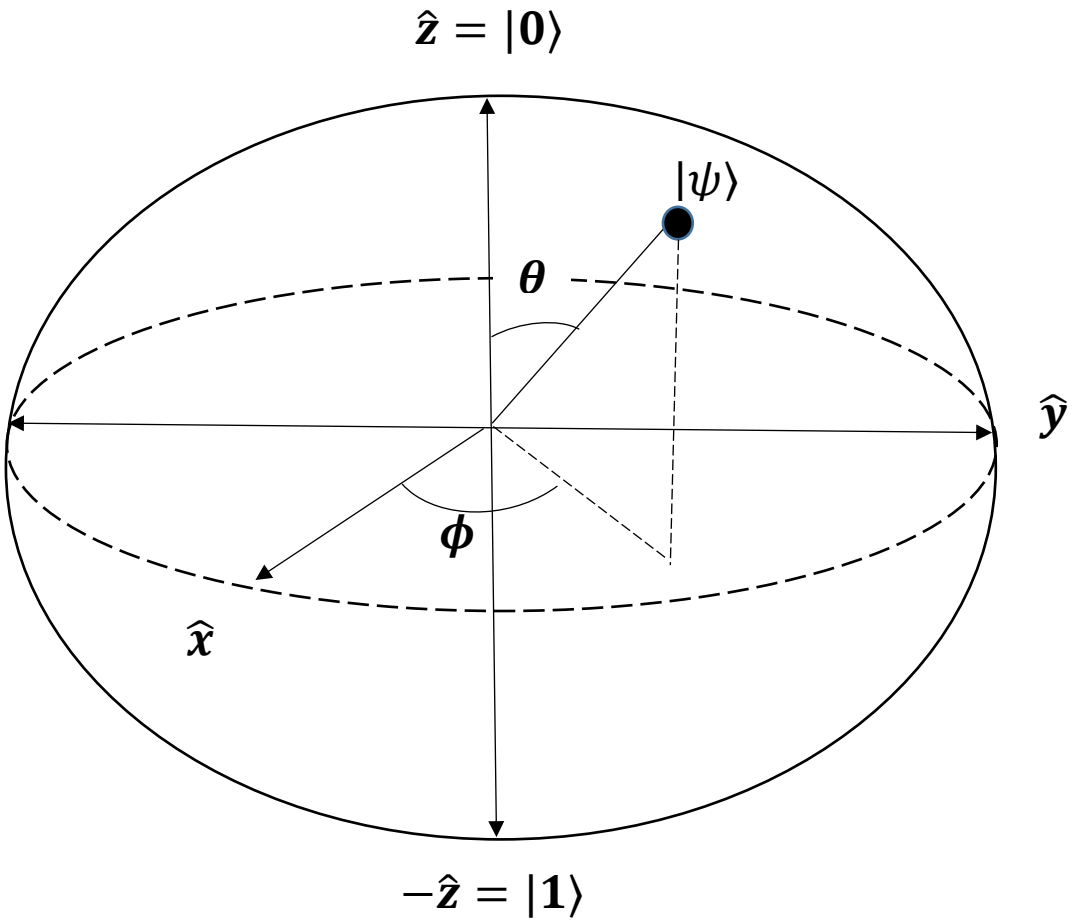

Fig 3.1 Bloch sphere qubit representation

We derive an expression from the *Bloch sphere* and describe the quantum bit or "qubit" from Figure (3.1)

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{3.1}$$

where $\alpha, \beta \in \mathbb{C}$. The scalars α and β exist in the complex vector space $\mathbb{C}$. They are also called the *amplitudes* for the states $|0\rangle$ and $|1\rangle$, respectively. The states $|0\rangle$ and $|1\rangle$ are computational basis states which are orthonormal to each other and represented as

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{3.2}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{3.3}$$

To rewrite the state of the qubit we take

$$\alpha = e^{i\phi_\alpha}\cos\frac{\theta}{2},\ \beta = e^{i\phi_\beta}\sin\frac{\theta}{2} \tag{3.4}$$

where θ, ϕ are real numbers that define the point on the *Bloch sphere.* Then let

$$\phi = \phi_{\beta-\alpha} \tag{3.5}$$

Now, we obtain a trigonometric representation of state of the qubit by extracting the overall phase angle $e^{i\phi_\alpha}$ yielding

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \tag{3.6}$$

The aforementioned process depends on the normalization of the phase angles since the qubit state is a unit vector. This is fulfilled by

$$|\alpha|^2 + |\beta|^2 = 1 \tag{3.7}$$

3.5 *Relative Phase*

The relative phase is given by

$$|+\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{3.8}$$

$$|-\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{3.9}$$

In the state $|+\rangle$ the amplitude of $|1\rangle$ is $\frac{1}{\sqrt{2}}$. In the state $|-\rangle$ the amplitude has the same magnitude but a different sign. We define that two amplitudes α_1, α_2 for some states differ by a relative phase provided there is a real number, ϕ such that $\alpha_1 = e^{i\phi}\alpha_2$.

3.6 *Pauli Matrices*

The Pauli matrices, *X*, *Y*, and *Z* expressed as 2×2 matrices

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{4.0}$$

were created by *Wolfgang Pauli*[8]. With some manipulation [12] of some qubit state, we find the *bit flip*

$$X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}|\psi\rangle = \alpha|1\rangle + \beta|0\rangle \tag{4.1}$$

phase shift

$$Z|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}|\psi\rangle = \alpha|0\rangle - \beta|1\rangle \tag{4.2}$$

or *both*

$$Y|\psi\rangle = ZX|\psi\rangle = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}|\psi\rangle = -\alpha|1\rangle + \beta|0\rangle \tag{4.3}$$

Widely used for *Quantum Error Correction* [12], the *bit-flip*, *phase-shift* or performing both techniques to uncover errors during the *quantum channel*, will help

[8] Wolfgang Ernst Pauli (April 25, 1900 – December 15, 1958) was an Austrian-born Swiss and American theoretical physicist and one of the pioneers of quantum physics. He received the Nobel Prize in Physics for "decisive contribution".

correct transmission of data between Alice and Bob. This pertains to QKD in subsection (*4.1.1)*.

3.7 *Quantum Entanglement and Bell States*

Quantum Entanglement is the physical phenomenon that occurs when two pairs or groups of particles are generated or interact in ways such that the quantum state for each particle cannot be described independently [11]. Instead, a quantum state must be used to describe for the system as a whole [12]. The general definition of quantum entanglement is expressed as

$$\begin{aligned} \alpha_1\beta_1 &= \alpha_2\beta_2 = 0 \\ \alpha_1\beta_2 &= -\alpha_2\beta_1 = 1 \end{aligned} \tag{4.4}$$

which serves as a contradiction. Albeit, we are hastened to the *Bell States* coined by *John Bell*[9]. This helps us conceptualize quantum information science simply with the following

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \tag{4.5}$$

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{4.6}$$

We will manipulate these definitions in the entanglement based attack strategy on the BB84 protocol in section (*4.3*).

3.8 *Vertical and Horizontal Basis*

The BB84 entanglement attack strategy, discussed in section (*4.3*), attempts to maintain variable usage of quantum entanglement in terms of the horizontal, $|H\rangle$ and vertical, $|V\rangle$ basis. This allows for the possibility for multiple polarization entanglement based attacks. Meaning that any polarization state existing in either the vertical or horizontal can be used. For example, $|\uparrow\rangle$, $|\downarrow\rangle$, $|\leftarrow\rangle$, $|\rightarrow\rangle$, $|\nwarrow\rangle$, $|\nearrow\rangle$, $|\searrow\rangle$, $|\swarrow\rangle$, are possible but, of course, within the respective basis.

4. QUANTUM-KEY DISTRIBUTION

Sometimes misconstrued with Quantum Cryptography [13], QKD uses quantum mechanics to attempt nearly perfect secrecy among two or multiple parties. A unique property is for the two parties to detect the presence of any third party trying to access the shared key. In this section we will briefly discuss the BB84 protocol.

4.1 BB84 PROTOCOL

The BB84 protocol will not render all classical conventional cryptographic algorithms obsolete [12]. Most parts of crypto-communication will remain classical. The BB84 protocol will serve as the secure replacement for the insecure classical public channel as needed (subsection (*2.2.2*) contains a justification but vulnerable aspect). The BB84 was

[9] John Stewart Bell (June 28, 1928 – October 1, 1990) was a Northern Irish physicist, and originator of Bell's theorem, an important theorem in quantum physics regarding hidden variable theories.

created and developed by *Charles Bennett*[10] and *Giles Brassard*[11] in 1984. We know from Classical Cryptography that Eve constantly trying to gain secret information from the communication between Alice and Bob. With this section, we shall begin briefly with three fundamental phases of the protocol: the *Quantum Channel*, *Sifting* and briefly, *Authentication Cost of Sifting*. All pivotal phases in the public channel of QKD.

4.1.1 Quantum Channel

The first stage of the BB84 protocol is the transmission of data through a quantum channel. Qubits are represented, in this case, as single photons. By mapping rectilinear polarization states and diagonal polarization states to the computational basis states of the qubit, say, $|0\rangle, |1\rangle$, to $\boxplus, \boxtimes$, respectively, we can then transmit photon data at the quantum level [13]. We begin with the theoretical function of the loss of data of the quantum channel given by

$$g_q = \mu \cdot \alpha_f \cdot \alpha_e \cdot \eta_{\text{det}} \cdot k_{\text{dead}} \tag{4.7}$$

Equation (4.7) represents the effort to save communication traffic [13]. The gain of the quantum channel g_q is the mean of the photon number μ. The next factor, α_f represents a fiber loss (the distance from point *A* to *B*). Briefly, the last component a_e represents any additional loss of the system. The receiver's detector, η_{det} and its detection efficiency, k_{dead} tells the reduction of the photon detection rate due to the dead time (dead time follows each detection event). [13]

4.2 PUBLIC CHANNEL

This setup is crucial for Alice and Bob to negotiate on the bits and then agree to perform on any further steps. To attempt to gain *more* information from a receiving party, say Bob, errors must be corrected, again since the quantum channel is not a noiseless channel there will exist error. Recall, the goal is to reduce Eve's knowledge about the data gained during the protocol demonstrating nearly perfect secrecy [13].

4.2.1 Sifting

The first phase on the public channel is *sifting*. Once Alice has sent randomly mapped bits into randomly chosen quantum basis via photons the two parties can agree upon an identical key.

Table 4.1 Base mapping

Base	Representation bit
Rectilinear	0
Diagonal	1

Table 4.2 Value mapping

Rectilinear	Diagonal	value bit
Horizontal (0°)	+45°	0
Vertical (90°)	−45°	1

[10] Charles Henry Bennett (b. 1943) is a physicist, information theorist and IBM Fellow at IBM Research. He discovered, with Gilles Brassard the concept of quantum cryptography and is one of the founding fathers of modern quantum information theory.

[11] Gilles Brassard (b. 1955) is a faculty member of the University of Montreal, where he has been a Full Professor since 1988 and Canada Research Chair since 2001.

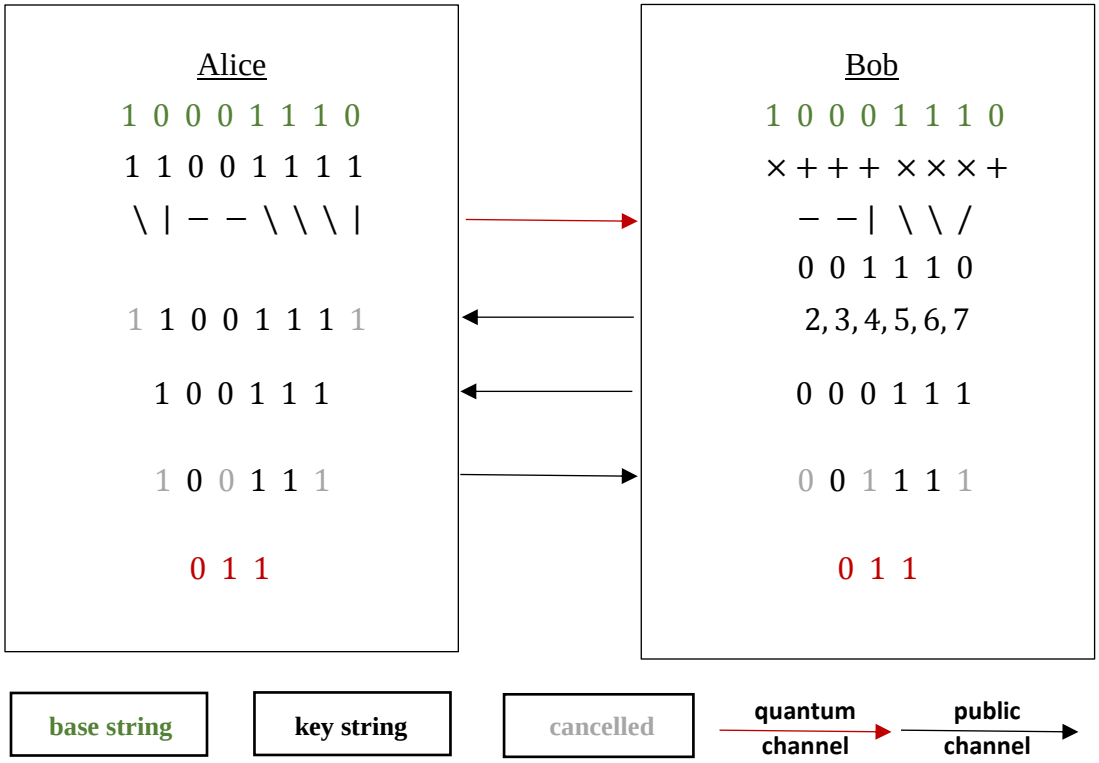

Fig. 4.1 BB84 QKD Sifting Phase

Alice and Bob both begin with a base string spanning one byte in length. Through mapping, each pair of bits in Alice's key string and base string map to a particular polarization state. Bob does this for his base string bits but only mapped to the polarization bases. We use this setup for Alice's transmission of polarization state data through the quantum channel.

Note that since the quantum channel is not a noiseless channel, there will exist error. Therefore, we omit these polarization states on Bob's end (exactly how to correct quantum errors for transmission is undiscussed).

After the bits are confirmed and sent to Alice, Alice publicly announces the bits that have arrived to Bob. Bits that are cancelled remain unused for the final sifted key. Now, based on how the polarization states that match between Alice's mapping scheme and Bob's randomly received quantum polarization states, g_q, both parties should agree upon a shared key. In this case 0 1 1.

Alice and Bob now both share an identical key: the *sifted* key. Now, we must satisfy the length of the key with the following

$$n = m \cdot g_q \cdot \frac{1}{2} = 3 \tag{4.8}$$

where $m = 8$ and $g_q = 0.75$ which is an unrealistic value (as expected) [13].

4.2.2 Authentication Cost of Sifting

We recall the MIMA (*2.2.2*) but now the modification of messages and the combination of an entanglement based attack strategy on the public channel by Eve will ensure that the key yielded by the sifting phase is indeed from the sender,

in this case Alice [13]. The authenticated key length needed for the tag is expressed as

$$w_1 = 4 \cdot (g_{\text{auth}} + \log_2 \log_2(2n(1 + \log_2 m))) \cdot \log_2 (2\text{n}(1 + \log_2 m) \quad (4.9)$$

After Alice has verified the message is indeed from Bob she sends her message with her choice of basis. Her message is of length $2n$. This is expressed as

$$w_2 = 4 \cdot (g_{\text{auth}} + \log_2 \log_2(2n)) \cdot \log_2 2n \quad (5.0)$$

where, g_{auth}, is the length of the resulting tag. Equations (4.9) and (5.0) represent the sum of all costs for the resulting tag, e.g., $t_s = w_1 + w_2$ to authenticate a sifted message [13].

4.3 ENTANGLEMENT BASED ATTACK STRATEGY

The particular attack we are focused with is when Eve uses entanglement to interact with the signal sent by Alice. Eve probes each signal and entangles the probe with it and then passes only the signal on to Bob [13]. Eve is later able to perform a measurement on *any* other quantum operation on her probe to gain information about the original signal [13].One simple strategy is for Eve to use an entangled pair of one of the Bell states

$$|\psi^p m\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \quad (5.1)$$

$$|\phi^p m\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \quad (5.2)$$

Now, we include *m* to represent a message and *p* will represent some entangled pair, quite similar to equations (4.5) and (4.6) implemented with (3.8) and (3.9). To proceed, let $|H\rangle$, $|V\rangle$ to represent states in the horizontal, vertical basis. Then using $\alpha|H\rangle + \beta|V\rangle$,

$$(\alpha|H\rangle + \beta|V\rangle)\frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle) = \frac{1}{2}(|\phi^+\rangle(\alpha|H\rangle + \beta|V\rangle) + |\phi^-\rangle(\alpha|H\rangle - \beta|V\rangle) + |\psi^+\rangle(\alpha|V\rangle + \beta|H\rangle) + |\psi^-\rangle(\alpha|V\rangle - \beta|H\rangle)) \quad (5.3)$$

will show us that Eve indeed has full information about the bit Alice sent. But for Bob, (the signal which Eve forwarded to Alice of which is now in a Bell state) has lost all its data about Alice's basis choice and is in a "fully mixed state", meaning that the *density matrix*[12] describes the quantum system in guaranteed several states [13]. Since the two parties in question will detect many errors they will likely abort the protocol.

We note that the concept is plausible provided Alice and Bob do not use entangled states for communication [13], e.g., a variation of the BB84 protocol.

■

[12] A density matrix is a matrix that describes a quantum system in a *mixed state*, a statistical ensemble of several quantum states.

5. REFERENCES

[1] A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security, Gupreet Singh Supriya C, International Journal of Computer Applications, ., pp 33-1, Volume 3, April 2013.

[2] A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security, Gupreet Singh Supriya C, International Journal of Computer Applications, ., pp 33-3, Volume 3, April 2013.

[3] "Cryptography", https://en.wikipedia.org/wiki/Cryptography

[4] Behrouz A. Forouzan, "Data Communications and networking", McGraw-Hill, 4th Edition.

[5] Thomas Baigeneres, Pascal Junod, Yi Lu, Jean Monnerat and Serge Vaudenay, A Classical Introduction to Cryptography Exercise Book, Springer+Business Medica, Inc., 2006 pp. 6

[6] Sanislaw Jarecki, ICS 268: Cryptography and Communication Security, Crypto Overview, Perfect Secrecy, One-Time Pad, September 28, 2004.

[7] "Unconditional Security" http://crypto.stackexchange.com/questions/20916/how-can-a-cryptosystem-be-unconditionally-secure

[8] Gustavus J. Simmons, Sandia Laboratories, Albuquerque, New Mexico, Symmetric and Asymmetric Encryption

[9] Luca Trevisan, Stanford University, Lecture notes from CS276 2009, Cryptography.

[10] "Planck constant" https://en.wikipedia.org/wiki/Planck_constant

[11] "Quantum entanglement" https://en.wikipedia.org/wiki/Quantum_entanglement

[12] Mladen Pavici, Quantum Computation and Quantum Communication Theory and Experiments, 2007.

[13] Kollmitzer Christian, Pivk Mario Lecture Notes in Physics 797. Applied Quantum Cryptography