A Survey and Simulation of Two Quantum Key Distribution Protocols

Ahmed Mustafa Khokhar
Department of Computer Science
National University of Computer and Emerging Sciences
Karachi, Pakistan
k214502@nu.edu.pk

Laiba Nadeem
Department of Computer Science
National University of Computer and Emerging Sciences
Karachi, Pakistan
k213398@nu.edu.pk

Maha Fatima
Department of Computer Science
National University of Computer and Emerging Sciences
Karachi, Pakistan
k213180@nu.edu.pk

***Abstract*—Private-key ciphers such as the One Time Pad are the only cryptographic systems with mathematically proven security, even against an adversary using a quantum computer. However, the One Time Pad is rarely used in practice due to the difficulty of secretly generating and distributing the long, random keys it requires. Quantum key distribution algorithms exploit the physical properties of quantum bits to provide a method for two parties to establish a shared key with guaranteed security. This paper will examine two of the most common protocols for quantum key distribution and provide a basic simulation and analysis of each.**

I. Introduction

The infeasibility of large-scale key distribution for private-key cryptography has led to the widespread adoption of public-key ciphers such as RSA, which are not quantum-safe. The most secure public-key ciphers today can be broken in polynomial time by an opponent with sufficient quantum computing ability. Quantum key distribution (hence QKD) protocols attempt to improve the usability of private-key schemes such as the One Time Pad or AES by providing a secure method for generating shared keys over public channels. After the two communicating parties perform classical techniques such as error correction and privacy amplification, the key material can be used in any private-key cipher.

QKD protocols exploit three physical laws governing quantum bits such as polarized photons or spin-1/2 particles to achieve guaranteed security:

1) It is impossible to duplicate an unknown quantum state without measuring it
2) Measuring a quantum bit necessarily disturbs its state
3) It is impossible to measure a quantum state in non-compatible bases simultaneously

These properties make it impossible for an eavesdropper to gain information about a quantum key without changing it. We assume two parties, Alice and Bob, wish to establish a shared key while minimizing their mutual information with an eavesdropper, Eve. Even if Eve is allowed to intercept and modify Alice's and Bob's communication over the quantum channel, she will be unable to conceal her measurements and will be detected through classical error analysis. We assume that Eve is also capable of intercepting the classical communication between Alice and Bob, but that she is unable to alter their messages in any way. Therefore, as long as Alice and Bob use an authenticated classical channel and perform error correction and privacy amplification on their keys, Eve will be unable to gain any useful information. This report will focus on two major protocols for quantum key distribution, namely the BB84 protocol proposed by Bennett and Brassard[1] and the B92 protocol proposed by Bennett [2]. Section II will contain background material on classical cryptography and quantum bits as well as the motivation of this project. Section III will describe the two chosen protocols and compare their strengths and weaknesses. Section IV contains a description of the three simulations.

II. Background

A. Classical Cryptography

Most electronic communications today are encrypted using a public-key cipher such as RSA[3]. Public-key algorithms are convenient for everyday use because, unlike private-key systems, they do not require a unique shared key for each pair of users who wish to communicate. Instead, each user possesses a private key, which is used for authentication and digital signing, and a public key, which provides confidentiality. As a result, for a system with n users, any pair of whom wish to communicate, a public-key system only requires $n(n-1)$ total keys, $2n$ of which are unique. For comparison, a similar system using private-key cryptography would require $n(n-1)/2$ unique keys. For example, a system with 100 users would require 200 unique keys using RSA and 4950 unique keys using a private-key cipher.

However, the limitations of public-key cryptography lie in its reliance on problems which are difficult but not computationally infeasible. The most commonly used public-key cipher, RSA, relies on the difficulty of factoring composite integers[3]. Another type of public-key system, the elliptic curve cipher, relies on the difficulty of computing discrete logarithms[4]. These systems are only considered secure because no polynomial-time algorithm has been found to solve either of these problems. It has been shown that a network of computers can solve RSA classically in sub-exponential time[5], and the lower bound on time to solve these problems has not been proven. Additionally, n attacker with a sufficiently complex quantum computer can break RSA and elliptic curve ciphers in polynomial time [6]. Although a quantum computer capable of performing Shor's algorithm on 2048-bit RSA keys is not yet practical, advances such as topological quantum computing may render public-key cryptography obsolete in the near future.

Unlike public-key schemes such as RSA, private-key ciphers require the generation of a new key for every pair of communicators. While this requires a much larger amount of key material, the resulting ciphertext is more secure as it does not rely on the infeasibility of solving difficult problems. Instead, the One Time Pad cipher guarantees that the ciphertext is unbreakable through either brute force or cryptanalysis. The One Time Pad is one of the simplest examples of a private-key cipher. It requires a truly random key at least as long as the message to be encrypted. To encrypt, the sender adds the key (modulo 2) bitwise with the message, and as long as the sender and recipient have the same key the recipient can perform the same operation to decrypt. This cipher is perfectly resilient to brute force attacks, since any number of valid plaintext messages can map to the same ciphertext. Unless the attacker learns the key, it is impossible to determine which plaintext is the original message. Other private-key ciphers such as Triple DES and AES use key expansion to reduce the amount of key material required while maintaining nearly perfect security.

In practice, private-key systems are seldom used due to limitations of classical key distribution:

- Keys must be truly random, as defects in pseudo-random number generators can result in low key entropy[8].
- Keys must be exchanged in secret, classically requiring a face-to-face meeting.
- Keys must be guarded until use and destroyed afterwards.

In order for Alice and Bob to regularly exchange encrypted messages, they would have to meet in secret and generate terabytes of key material each meeting. Alternatively, they could rely on a trusted third party to generate the key material and distribute it to both of them. However, this would mean that the key is not known only to Alice and Bob, introducing a new potential attack vector and making the key unusable for digital signing. QKD protocols address these limitations of private-key cryptography by providing a method for Alice and Bob to generate truly random, shared key material over long distances, even in the presence of eavesdroppers.

B. *Quantum Mechanics*

Part of the security of QKD arises from the fact that neither party intends to use any specific key at the outset. Instead, the key is generated truly randomly from quantum mechanical phenomena such as thermal noise[7]. In most QKD protocols, we assume Alice begins by generating a long string of truly random classical bits. Her goal is to encode this classical information in the states of quantum bits which are subject to the physical laws discussed in Section I.

Quantum bits (hence ’qubits’) are binary systems like classical bits, with a “0” state, $|0\rangle$, and a “1” state, $|1\rangle$. Unlike classical bits, however, a qubit can exist in a linear combination of these states called a superposition:

$$\alpha|0\rangle + \beta|1\rangle$$

According to the Measurement Postulate[9], measuring a state

$$|\Psi\rangle = \sum_i \alpha_i|\emptyset_i\rangle$$

with respect to the basis B = $\{|\emptyset_i\rangle\}$ outputs the label i with probability $|\alpha_i|^2$ and leaves the system in state $|\emptyset_i\rangle$. Because measurement necessarily collapses a superposition state to one of its basis states, it is impossible for Eve to measure Alice’s qubits without disturbing them and revealing her actions.

In quantum mechanics, measurements correspond to operators called ’observables’. The eigenvectors of an observable represent the possible measurable values of a quantum state and thus form an eigenbasis for the state space in which the observable exists[10]. If two observables share at least one common eigenbasis, they are said to ’commute’ and can be measured simultaneously. If they do not commute, the Heisenberg Uncertainty Principle requires that measuring one observable imparts a minimum degree of disturbance on the other[12]. Thus, it is impossible to measure a quantum state with respect to incompatible bases simultaneously.

The No-Cloning Theorem states that it is impossible to clone an unknown quantum state[13]. To prove this, assume that there exists some unitary operator U which, when applied to a quantum state $|\Psi\rangle$, produces a copy of the original state along with the original state. That is,

$$U\,|\Psi\rangle \rightarrow |\Psi\rangle\,|\Psi\rangle$$

The contradiction occurs when U is applied to a superposition such as

$$\alpha|0\rangle + \beta|1\rangle$$

Using the linearity of unitary operators, the application of U on such a superposition can be written as

$$U\,(\alpha|0\rangle) + U\,(\beta\,|1\rangle) \rightarrow \alpha|00\rangle + \beta|11\rangle$$

However, this is not the result we expect from our definition of cloning. A cloning operator should produce the result

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$

which is the original superposition state along with an exact copy of itself. Therefore, it is not possible to clone an unknown state[12].

Any two-level quantum mechanical system can be used to implement a qubit. The most common physical examples of qubits are:

- The energy states of electrons in an atom. – $|0\rangle$, $|1\rangle$ could be defined as ground and excited states, respectively.
- The magnetic spin states of spin-1/2 particles such as electrons.
- The polarization states of photons.

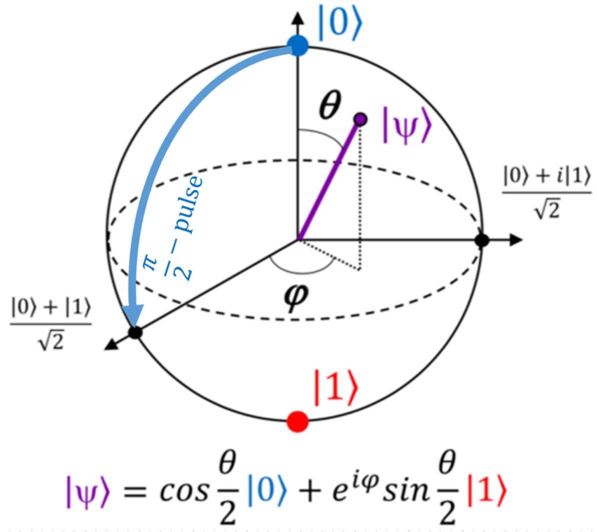
This paper will assume qubits are implemented as polarized photons, with the state $|0\rangle$ representing vertical polarization and the state $|1\rangle$ representing horizontal polarization. The possible polarization states of a photon can be visualized geometrically as three-dimensional complex vectors bounded by a unit sphere called the Bloch Sphere. For example, the pure state $|0\rangle$, representing vertical polarization, corresponds to the unit vector in the $\hat{z}$ direction. Pure superposition states, where $\theta \neq \{0, \pi\}$ and $\|\,|\psi\rangle\,\| = 1$, correspond to polarization axes that lie somewhere between horizontal and vertical polarization. If a photon is measured with respect to the $\{|0\rangle, |1\rangle\}$ basis, the probability it will collapse to either basis state depends on θ as well as φ, the relative phase between the basis states:

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\theta}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

Measuring a photon's polarization with respect to any basis is equivalent to performing a rotation operation and measuring the resulting state in the computational basis, {|0⟩, |1⟩}. For example, to measure the pure state |0⟩ in the Hadamard basis $\{1/\sqrt{}2(|0\rangle \pm |1\rangle)\}$, one can increment θ by π/2 to get the state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

which will collapse to either the |0⟩ or the |1⟩ state with equal probability when measured in the computational basis. The QKD protocols examined in this paper leverage the fact that the results of a measurement depend on the basis in which the measurement in performed to guarantee that any eavesdropping will be detected with high probability.



$|0\rangle$
θ
$|\psi\rangle$
$\frac{|0\rangle + i|1\rangle}{\sqrt{2}}$
$\frac{\pi}{2} - pulse$
φ
$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
$|1\rangle$
$|\psi\rangle = cos\frac{\theta}{2}|0\rangle + e^{i\varphi}sin\frac{\theta}{2}|1\rangle$

Fig.1. Bloch sphere representation [14]

III. SURVEY

A. The BB84 Protocol

The BB84 protocol, inspired by Stephen Wiesner's concept of conjugate coding [13], is the first quantum key distribution (QKD) scheme and remains the most widely used. Its security is based on the principle that two non-commuting observables cannot be measured simultaneously. This ensures that any attempt to measure or clone a quantum state introduces detectable errors. Below is a detailed explanation of the BB84 protocol [1]:

1) Key Generation: Alice uses a truly random number generator to create a sequence of $(4+\delta)n$ classical bits, known as the raw key. These bits are used to encode quantum states, with a subset later forming the final shared key between Alice and Bob.

2) Photon Encoding: Alice encodes each bit of her raw key into the polarization state of a photon using two non-orthogonal bases:

   - **X Basis**: |0⟩,|1⟩, representing vertical (|↑⟩) and horizontal (|→⟩) polarization.

   - **Z Basis**: |+⟩,|−⟩, where

   $$\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$$

   corresponding to diagonal (|−⟩)and anti-diagonal (|) polarization.

   Encoding rules:

   - For "0", Alice randomly sends the |0⟩ state in either the X or Z basis with 50% probability.

   - For "1", she sends the |1⟩ state in either the X or Z basis with 50% probability.

3) Photon Transmission: Alice transmits the polarized photons one by one through a quantum channel to Bob.

4) Bob's Measurements: Bob measures each photon using a birefringent crystal, randomly choosing between the X or Z basis for each photon.

   - If Alice's encoding basis matches Bob's measurement basis, he correctly retrieves the original bit (assuming no noise or interference).

   - If their bases differ, the measurement results are uncorrelated, yielding random outcomes.

5) Key Sifting: After all photons are measured, Bob publicly announces his chosen basis for each measurement over an authenticated classical channel without revealing the measurement results.

   - Alice then reveals the bases she used for encoding.

   - Both discard bits where their bases do not match, leaving them with a "sifted key."

   In the absence of noise or eavesdropping, the sifted keys of Alice and Bob should be identical.

6) Eavesdropping Detection: Alice and Bob verify the security of their communication by disclosing and comparing a subset of their sifted keys. This process detects the presence of an eavesdropper, Eve:

   - If Eve intercepts and measures photons using her own random basis, she introduces detectable bit-flip errors due to the following reasons:

- When Eve’s measurement basis matches Alice’s, she obtains the correct result.

- If Eve’s basis differs, her measurement is random, leading to errors when she re-encodes and forwards the photon to Bob.

Eve’s interference introduces a bit-flip error with a 25% probability for each intercepted photon. By revealing NNN bits of their sifted keys, Alice and Bob can detect eavesdropping with a probability of

$$1-\frac{3^N}{4}$$

7) Error Handling: Errors can occur naturally due to imperfections in the quantum channel or eavesdropping. Alice and Bob calculate the Quantum Bit Error Rate (QBER) and compare it to their measured error rate:

   - If the measured rate exceeds the expected QBER, the protocol is aborted, and a new channel is used.

   - To minimize errors, Eve must limit her measurements to a small subset of photons, reducing her information gain.

B. *The B92 Protocol*

The B92 protocol, introduced by Charles Bennett [2] in 1992, simplifies quantum key distribution (QKD) by using only two non-orthogonal states instead of four, as in the BB84 protocol. This approach relies on polarization filters for photon transmission and measurement, which work probabilistically based on the alignment between the photon’s polarization and the filter's axis. Below is the detailed description of the B92 protocol [2]:

1) Key Generation: Alice uses a truly random number generator to produce a sequence of random classical bits, forming her raw key.

2) Photon Encoding: Alice encodes each bit into the polarization state of a photon using the following scheme:

   - For "0," she sends the state |↑⟩(X-basis).

   - For "1," she sends the state |−⟩ (Z-basis).

3) Photon Transmission: Alice sends the encoded photons to Bob over a quantum channel.

4) Bob’s Measurement: Bob randomly selects one of two polarization filters for each photon:

   - Filter 1: Detects the state |, blocking |−⟩, testing for "0."

   - Filter 2: Detects the state |→⟩, blocking |↑⟩, testing for "1."

   Only 25% of the photons yield conclusive results where Bob’s filter aligns with Alice’s encoding.

5) Classical Communication: After completing measurements, Bob announces which photons yielded results (without disclosing the results) and Alice, knowing the photons she sent, infers Bob’s measurements and derives a shared key.

6) Eavesdropping Detection: Alice and Bob compare a subset of their sifted keys to detect eavesdropping.. They also monitor qubit loss rates to detect potential channel manipulation.

IV. Results

A. *BB84 protocol*

Table 1

A’s bits	0	0	0	0	0	1	0	1	0	1	1	1	0	0	0
A’s bases	1	1	0	1	0	0	0	0	0	0	1	1	1	1	1
Qubits sent	|+⟩	|+⟩	|0⟩	|+⟩	|0⟩	|1⟩	|0⟩	|1⟩	|0⟩	|1⟩	|-⟩	|-⟩	|+⟩	|+⟩	|+⟩
B’s bases	0	1	0	1	1	1	0	1	1	1	1	1	0	0	1
B’s results	1	0	0	0	1	1	0	0	0	1	1	1	1	0	0
A’s key	-	0	0	0	-	-	0	-	-	-	1	1	-	-	0
B’s key	-	0	0	0	-	-	0	-	-	-	1	1	-	-	0
A’s disclosed key		0	-	0			-				1	-			0
B’s Disclosed key		0	-	0			-				1	-			0
A’s Secret key		-	0	-			0				-	1			-
B’s Secret key		-	0	-			0				-	1			-

Fig.2. BB84 without eavesdropping

Table 2

A’s bits	0	1	1	0	1	0	0	0	0	1	0	1	1	0	0
A’s bases	1	1	0	0	1	1	0	0	0	0	0	1	0	0	0
Qubits sent	|+⟩	|-⟩	|1⟩	|0⟩	|-⟩	|+⟩	|0⟩	|0⟩	|0⟩	|1⟩	|0⟩	|-⟩	|1⟩	|0⟩	|0⟩
E’s bases	1	0	0	1	0	1	0	1	1	0	1	1	1	1	1
E’s results	0	1	1	0	0	0	0	0	1	1	1	0	1	1	1
New Qubit	|+⟩	|1⟩	|1⟩	|+⟩	|0⟩	|+⟩	|0⟩	|+⟩	|-⟩	|1⟩	|-⟩	|+⟩	|-⟩	|-⟩	|-⟩
B’s bases	1	0	0	0	0	0	1	0	0	1	0	0	0	1	0
B’s result	0	1	1	0	0	1	0	1	1	0	0	0	0	1	1
B’s key	0	-	1	0	-	-	-	1	1	-	0	-	0	-	1
A’s key	0	-	1	0	-	-	-	0	0	-	0	-	1	-	0
A’s disclosed key	0		-	0				-	0		-		1		-
B’s Disclosed key	0		-	0				-	1		-		0		-

Fig.3. BB84 with eavesdropping

In the BB84 protocol, when there is no eavesdropping, Alice and Bob successfully generate matching secret keys after discarding the mismatched results from their respective basis choices. In this case, Alice's and Bob's final secret keys are aligned, and the key exchange process is secure. However, in the presence of eavesdropping (as illustrated in Table 2), where an eavesdropper (Eve) interferes by measuring the qubits and sending new qubits to Bob, the results show discrepancies between Alice's and Bob's keys. Despite Eve's attempt to intercept and resend the qubits, the errors introduced by Eve's measurements cause mismatches in the keys, which Bob and Alice can detect during the key verification process. This discrepancy demonstrates the vulnerability of the protocol to eavesdropping, as errors in the key exchange increase, ultimately leading to an insecure key generation if the error rate surpasses a tolerable threshold. Thus, the results emphasize the need for key verification in quantum cryptography to ensure security and the detection of potential eavesdropping attempts.

B. B92 protocol

Table 3

A's bits	1	0	0	0	1	0	1	0	0	0	0	1	1	1	1	1
Qubits sent	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$
B's filter	1	1	0	0	0	1	0	1	0	0	0	1	1	0	1	0
B's results	1	-	0	0	-	-	-	-	-	-	0	-	-	-	1	-
A's Sifted key	1	-	0	0	-	-	-	-	-	-	0	-	-	-	1	-
B's Sifted Key	1	-	0	0	-	-	-	-	-	-	0	-	-	-	1	-
A's disclosed key	1		-	0							-				1	
B's Disclosed key	1		-	0							-				1	
A's key	-		0	-							0				-	
B's key	-		0								0				-	

Fig.4. B92 without eavesdropping

Table 4

A's bits	0	0	1	1	1	1	1	1	0	1	0	1	1	1	1	1
Qubits sent	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$
E's filter	1	0	0	1	0	0	1	1	1	0	0	0	0	0	1	1
E's Results	-	0	-	1	-	-	-	-	-	-	0	-	-	-	-	-
New Qubits		$\|0\rangle$		$\|+\rangle$							$\|0\rangle$					
B's filter		1		1							0					
B's Results		-		1							0					
A's sifted key	-	0	1	1	1	1	1	1	0	1	0	1	1	1	1	1
B's Sifted Key				1							0					

Fig.5. B92 with eavesdropping

While B92 requires fewer states than BB84, making it easier to implement, the fact that most of the photons are discarded leaves it vulnerable to a subtle eavesdropping strategy. While we have demonstrated that distinguishing between non-orthogonal states is impossible, Eve can simply discard failed attempts to determine Alice's raw key with 100% accuracy [12]. The only way for Alice and Bob to detect this type of attack is to establish an expected qubit loss rate for the channel and compare it with the actual loss rate. However, if Eve controls the quantum channel while Alice and Bob perform their setup, she may be able to manipulate the expected loss rate and avoid detection. As a result of this vulnerability, B92 is rarely implemented in real-world QKD systems.

V. CONCLUSION

Quantum Key Distribution (QKD) represents a groundbreaking application of quantum mechanics, offering a theoretically unbreakable method for secure key exchange. While classical public-key schemes dominate real-world cryptographic key distribution, the fundamental advantage of QKD lies in its reliance on the immutable laws of quantum physics. Any attempt to compromise QKD would require an attacker to violate these established principles, ensuring unparalleled security.

Among the protocols discussed, BB84 emerges as the most practical and secure option for widespread implementation. Its key advantages include reliance on minimal quantum assumptions, robust eavesdropping detection through the use of non-orthogonal bases, and efficient error detection via sifted keys. These features ensure a high degree of security while maintaining an intuitive and relatively straightforward implementation. However, BB84's limitations include inefficiency due to basis mismatches, vulnerability to channel noise, and susceptibility to intercept-resend attacks, which highlight the importance of continuous improvements in quantum channel reliability and hardware.

On the other hand, the B92 protocol offers a simpler approach by using only two quantum states instead of four and relying on polarization filters rather than birefringent crystals. While these factors reduce implementation complexity, B92 suffers from significant photon loss, with 75% of transmitted photons discarded, leading to reduced efficiency. Furthermore, it is vulnerable to eavesdroppers exploiting discarded photons and channel manipulation, making it less secure and less feasible for practical use. Consequently, B92 is rarely adopted in real-world QKD systems.

Despite the promise of QKD to eventually replace classical methods, current challenges—such as hardware limitations, photon loss, and the difficulty of generating specific quantum states outside controlled environments—must be addressed. In the short term, practical QKD implementations may continue to depend on trusted third parties for qubit generation and distribution. Nevertheless, as advancements in quantum technology improve the range, transmission rates, and reliability of quantum systems, protocols like BB84 may become the gold standard for secure key distribution, revolutionizing cryptographic security.

VI. References

[1] C. H. Bennett and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” Intl. Conf. on Computers, Systems, & Signal Processing, 12 Dec. 1984.

[2] C. H. Bennett, “Quantum Cryptography Using Any Two Nonorthogonal States,” Phys. Rev. Lett., Volume 68, Number 21, 25 May 1992.

[3] R. Rivest, A. Shamir, and L. Adleman, “On Digital Signatures and Public Key Cryptosystems,” Commun. Ass. Comp. Mach., Volume 21 (1978) pp. 120-126.

[4] M Rosing, “Implementing Elliptic Curve Cryptography,” Manning Publications, Greenwich (1999) ISBN 1-884777-69-4.

[5] E. W. Weisstein, “RSA-640 Factored,”MathWorld HeadlineNews,8thNovember(2005), http://mathworld.wolfram.com/news/2005-11-08/rsa640/.

[6] P. Shor, “Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” Siam Journal on Computing, Volume 26, Issue 5 (1997) pp. 1484-1509.

[7] B. Jun and P. Kocher, “The Intel Random Number Generator,” Cryptography Research, Inc. white paper prepared for Intel Corp., 22 Apr. 1999.

[8] N. Heninger, Z. Durumeric, E. Wustrow, J. A. Halderman, “Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices,” Proc. 21st USENIX Security Symposium, Aug. 2012.

[9] P. Kaye, R. LaFlamme, M. Mosca, An Introduction to Quantum Computing, Oxford UP, 2010. Print. ISBN 978-0-19-857049-3.

[10] H. Wimmel, Quantum Physics & Observed Reality: A Critical Interpretation of Quantum Mechanics, World Scientific, 1992. Print. ISBN 981-02-1010-8.

[11] W. K. Wootters and W. H. Zurek, “A Single Quantum Cannot Be Cloned,” Nature, Volume 299, pp. 802-803. 28 Oct. 1982

[12] C. Williams, Explorations in Quantum Computing, Springer, 2011. Print. ISBN 978-1-84628-886-9

[13] S. Wiesner, “Conjugate Coding,” SIGACT News, Volume 15, Number 1, Jan. 1982.

[14] https://www.researchgate.net/publication/335028508_A_Review_on_Quantum_Computing_Qubits_Cryogenic_Electronics_and_Cryogenic_MOSFET_Physics/figures?lo=1