



UNIVERSITY OF  
**BATH**

---


**Suthee Kitcharoenkarnkul**

**Development of Quantum Key Distribution**

**Coursework 1: Cryptographic Research**

**CM50210 Cryptography 2014/15**

# Cover Sheet

 <p style="margin: 0;">UNIVERSITY OF <b>BATH</b></p> <p style="margin: 5px 0 0 0;"><b>Department of Computer Science</b></p> <p style="margin: 5px 0 0 0;"><b>INDIVIDUAL COURSEWORK</b></p> <p style="margin: 5px 0 0 0;">Submission Cover Sheet</p> <p style="margin: 10px 0 0 0;"><b>Please fill in both columns in BLOCK CAPITALS and post into the appropriate Coursework Submission Box outside the Department Office.</b></p>	<p style="margin: 0;"><input type="checkbox"/> Retain for sample</p> <p style="margin: 5px 0 0 0;">Mark:</p> <p style="margin: 5px 0 0 0;"><i>for office use</i></p> <p style="margin: 5px 0 0 0;"><b>Date received:</b></p> <p style="margin: 10px 0 0 0;"><b>Confirmation of Hand-in</b></p> <p style="margin: 10px 0 0 0;"><b>This section will be retained by the Department Office as proof of hand-in</b></p>
<p style="margin: 0;"><b>How to present your work</b></p> <ol style="list-style-type: none"> <li>1. Bind all pages of your assignment (including this submission sheet) so that all pages can be read by the marker without having to loosen or undo the binding. Ensure that the binding you use is secure. Missing pages cannot be marked.</li> <li>2. If you are required to submit part of the work on a disk, place the disk in a sealed envelope and bind the envelope into the submission.</li> </ol> <p style="margin: 5px 0 0 0;"><b>Keep a copy of your assignment and disk.</b> The original is held by the Department for scrutiny by External Examiners.</p>	<p style="margin: 0;"><b>Declaration</b></p> <p style="margin: 5px 0 0 0;"><i>I certify that I have read and understood the entry in the Department of Computer Science Student Handbook on Cheating and Plagiarism and that all material in this assignment is my own work, except where I have indicated with appropriate references. I agree that, in line with Regulation 15.3(e), if requested I will submit an electronic copy of this work for submission to a Plagiarism Detection Service for quality assurance purposes.</i></p>
<p style="margin: 0;">FAMILY NAME</p> <p style="margin: 5px 0 0 40px;"><b>KITCHAROENKARNKUL</b></p>	<p style="margin: 0;">FAMILY NAME</p> <p style="margin: 5px 0 0 40px;"><b>KITCHAROENKARNKUL</b></p>
<p style="margin: 0;">GIVEN NAME (S)</p> <p style="margin: 5px 0 0 40px;"><b>SUTHEE</b></p>	<p style="margin: 0;">GIVEN NAME (S)</p> <p style="margin: 5px 0 0 40px;"><b>SUTHEE</b></p>
<p style="margin: 0;">UNIT CODE</p> <p style="margin: 5px 0 0 40px;"><b>CM50210</b></p>	<p style="margin: 0;">UNIT CODE</p> <p style="margin: 5px 0 0 40px;"><b>CM50210</b></p>
<p style="margin: 0;">UNIT TITLE</p> <p style="margin: 5px 0 0 40px;"><b>CRYPTOGRAPHY</b></p>	<p style="margin: 0;">UNIT TITLE</p> <p style="margin: 5px 0 0 40px;"><b>CRYPTOGRAPHY</b></p>
<p style="margin: 0;">DEADLINE DEAD &amp; TIME</p> <p style="margin: 5px 0 0 40px;"><b>FRIDAY, 17TH APRIL 2015 / 17:00</b></p>	<p style="margin: 0;">DEADLINE DEAD &amp; TIME</p> <p style="margin: 5px 0 0 40px;"><b>FRIDAY, 17TH APRIL 2015 / 17:00</b></p>
<p style="margin: 0;">COURSEWORK PART (if applicable)</p>	<p style="margin: 0;">COURSEWORK PART (if applicable)</p>
<p style="margin: 0;">SIGNATURE</p> <p style="margin: 10px 0 0 40px; font-family: cursive; font-size: 1.2em; color: blue;">Suthe K.</p>	<p style="margin: 0;">SIGNATURE</p> <p style="margin: 10px 0 0 40px; font-family: cursive; font-size: 1.2em; color: blue;">Suthe K.</p>

# Development of Quantum Key Distribution

## Abstract

Quantum cryptography is a cryptographic technology first proposed by Stephen Wiesner in the early 1970s. The technology applies phenomena of quantum physics to secure network communications of two parties. This technology then was developed for distributing symmetric keys using a BB84 algorithm, called quantum key distribution (QKD). Two parties can produce a shared random secret key used to encrypt and decrypt data between them. The primary advantage of QKD is that it can detect eavesdropping using the laws of quantum mechanics. Therefore, QKD guarantees secure key distribution. Nevertheless, practical QKD implementations are vulnerable to imperfect assumptions and have been proved that they could be eavesdropped or attacked by hackers. However, there is a new research using the three-stage quantum cryptography protocol to make the QKD implementations more secure.

## 1. Introduction

Cryptography is a computing approach to secure communication between two parties (usually referred to as Alice and Bob). Its objective is to keep secrets secret from the third party (usually referred to as Eve). That is, messages transmitted over an insecure channel between senders and receivers are prevented from eavesdropping by anyone else. Encryption and decryption are the fundamental concept of cryptography for providing confidentiality. The unencrypted message that can be read by anyone is called plaintext. When Alice sends plaintext to Bob, the plaintext will be encrypted using secret information, a secret key, and then transformed into the ciphertext. The ciphertext will be transferred to Bob over an insecure channel. After receiving the ciphertext, Bob uses the same secret key to decrypt the ciphertext and obtains the original plaintext. The third party Eve may eavesdrop the communication by intercepting the ciphertext. Nevertheless, she cannot derive any information about the plaintext from the observed ciphertext. The approach using the same secret key to both encrypt and decrypt messages is known as symmetric-key cryptography (Delfs and Knebl, 2007).

The strength of symmetric-key cryptography depends on two factors, key distribution and key algorithms (Blumenthal, 2013). To guarantee secure key distribution, quantum mechanics are applied in the process of the key exchange. This concept has been developed and known as quantum key distribution (QKD) (Bennett and Brassard, 1984). Likewise, key algorithms have been strengthened in order to be resistant to quantum computing based attacks, an efficient factoring approach based on quantum mechanics for breaking the encryption. Cryptography systems using the reinforced key algorithm are called post-quantum cryptosystems (Nitaj, n.d.).

This paper mainly provides information about development of QKD, especially the BB84 algorithm which is widely used in the present, QKD eavesdropping proof, using QKD in the real world, hacking quantum cryptography systems, and a new research that enhances the security of QKD.

## 2. Quantum Key Distribution

Quantum cryptography is a cryptographic technology first proposed by Stephen Wiesner in the early 1970s. The technology applies phenomena of quantum physics to secure network communications of two parties. This technology then was developed for distributing symmetric keys, called quantum key distribution (QKD). Two parties can produce a shared random secret key used to encrypt and decrypt data between them. QKD was firstly proposed by Charles Bennett and Gilles Brassard in 1984, called BB84 algorithm. It has been implemented in a number of both research quantum networks and commercial products (Scholz, 2007). Due to the properties of quantum mechanics, the third party cannot determine the secret key without being detected by the sender and the receiver. Therefore, QKD guarantees secure key distribution (Bennett and Brassard, 1984).

In addition to BB84 algorithm, there are other QKD algorithms such as B92 algorithm, entanglement-based QKD algorithm, and Quantum Bit Commitment (QBC) algorithm (Lace et al., 2008). However, this paper will focus on the BB84 algorithm.

## 3. Implementation of BB84 Algorithm

The basic concept of QKD is transmitting an encoded secret key by polarizing single photons along bases. The basis is pairs of orthogonal states. The BB84 algorithm uses two types of bases, rectilinear and diagonal. The rectilinear basis causes linear polarization that can be horizontal ( $0^\circ$ ) or vertical ( $90^\circ$ ) and the diagonal basis causes circular polarization that can be right-handed ( $45^\circ$ ) or left-handed ( $135^\circ$ ). A single polarized photon can encode one bit of data, for instance, vertical or left-handed polarization for “0” and horizontal or right-handed polarization for “1” as shown in figure 1.

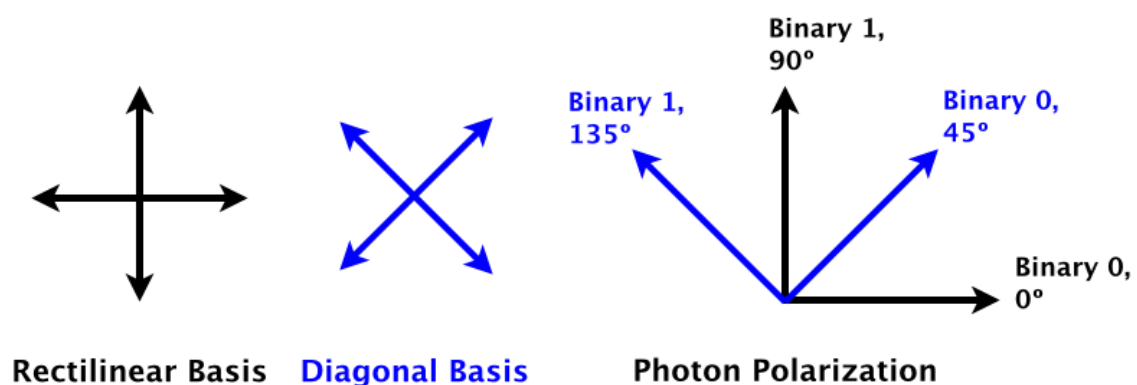


Figure 1 BB84 bit encoding, figure adapted from Haitjema (2007)

In the first step, Alice creates a quantum key by selecting random bits (0 or 1) and a random basis (rectilinear or diagonal) for each bit. She then defines a photon polarization state based on the bit value and the basis as an example presented in figure 2. After that, she transmits the quantum key in the form of a stream of polarized photons to Bob.

Basis		0	1
Rectilinear	+	↑	→
Diagonal	×	↗	↖

Figure 2 Alice's bit encoding

Due to the properties of quantum mechanics, there is no measurement that can distinguish between the four different polarization states. Bob needs to select randomly one of the two bases to measure the photon's polarization for every photon he has received because he does not know the basis the photon has been encoded in. For a particular photon, if he selects the same basis as Alice, he can measure the correct polarization state and obtain the bit value that Alice intended to send. In contrast, if he selects the wrong basis, the measurement will return the polarization state at random. Therefore, he will obtain the correct bit value with a probability of 50%.

After Bob has received and measured all the photons, he notifies Alice over the public communication channel what basis of each photon he selected to measure. Then, Alice sends information about the basis each photon was polarized back to Bob. They both discard the bits corresponding to the photons that Bob used a different basis. The remaining bits, which are half on average, will be a shared secret key used for encryption and decryption (Bennett and Brassard, 1984).

Figure 3 illustrates an example of the bits Alice selected, her bases she encoded the bits in, the bases Bob selected for measurement, and the resulting shared secret key.

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random bases	+	+	×	+	×	×	×	+
Alice's polarizations	↑	→	↖	↑	↖	↗	↗	→
Bob's random bases	+	×	×	×	+	×	+	+
Bob's measurements	↑	↗	↖	↗	→	↗	→	→
Values kept afterwards	✓		✓			✓		✓
Shared secret key	0		1			0		1

Figure 3 An example of establishing a shared secret key using QKD, figure adapted from Scholz (2007)

## 4. Eavesdropping Proofs

QKD relies on two elements of quantum mechanics, the Heisenberg Uncertainty principle and the principle of photon polarization. The Heisenberg Uncertainty principle states that it is impossible to measure the photon polarization without disturbing the system. The principle of photon polarization states that an eavesdropper cannot copy unknown quantum states due to the no-cloning theorem. As a result, Alice and Bob will immediately know if Eve attempts to determine the quantum key (Sharbaf, 2009).

The simplest way to eavesdrop the quantum key is an intercept-resend attack. Eve will measure the photons' polarization states sent by Alice, and then send replacement states to Bob. Like Bob, Eve also has no knowledge of the basis the photon has been encoded in. Hence, she needs to guess which basis to measure in. If she selects correctly, she can measure the correct polarization state as sent by Alice. Then, she resends the same polarization state to Bob. In this case, Eve can eavesdrop the quantum key without being detected. However, if she selects incorrectly, the polarization state she measures will be random. When she resends the same state (opposite basis to Alice) to Bob, if he selects the same basis as Alice, he will get a random result instead of the correct result he would obtain without the presence of Eve. In the case of getting a wrong result, Alice and Bob can discover this error when they negotiate the shared secret key with their bases (Aggarwal, Sharma and Gupta, 2011). Figure 4 shows an example of the eavesdropping.

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random bases	+	×	+	×	×	+	×	+
Alice's polarizations	→	↖	↑	↗	↖	→	↗	↑
Eve's random bases	+	+	×	×	+	×	×	+
Polarization Eve measures and sends	→	→	↗	↗	↑	↗	↗	↑
Bob's random bases	+	×	×	×	+	×	+	+
Polarization Bob measures	→	↗	↗	↗	↑	↗	→	↑
Shared secret key	0	0		0				1
Error generated	✓	✗		✓				✓

*Figure 4 An example of an intercept-resent attack, figure adapted from Aggarwal, Sharma and Gupta (2011)*

To mitigate the errors from eavesdropping, information reconciliation and privacy amplification can be performed to remove the erroneous bits and reduce Eve's knowledge of the quantum key to an arbitrary small value (Bennett et al., 1992).

## 5. Using Quantum Key Distribution in the Real World

As QKD guarantee secure communication and can detect eavesdropping, it has been widely used and applied in many environments. For example:

- There are at least five quantum networks around the world using QKD to provide secure communication such as DARPA QKD network, SECOQC QKD network in Vienna, Hierarchical network in Wuho, China, SwissQuantum, and Tokyo QKD Network.
- The Bank Austria performed the world's first bank transfer encoded via quantum cryptography (SECOQC, 2004).
- In 2007, quantum cryptography was used to secure balloting information in the Swiss election (Messmer, 2007).
- The latest news from the Telegraph states that China has been building a quantum encryption network between Beijing and Shanghai (Moore, 2014).
- For commercial products, there are many companies who provide quantum cryptography solutions. For instance, ID Quantique offers Centauris CN8000 encryptor that uses QKD technique to secure communication between two parties with 100Gbps throughput (Messmer, 2013).

## 6. Hacking Quantum Cryptography Systems

The BB84 algorithm has been proven secure against any attack allowed by quantum mechanics under four conditions. Firstly, Eve cannot physically access encoding and decoding devices. Secondly, the random bit generators used by two parties must be trusted and truly random (e.g. a quantum random bit generator). Thirdly, an unconditionally secure authentication scheme must be used for the public communication channel. Finally, a light source must emit nothing but single photons.

Nonetheless, practical QKD implementations are vulnerable to imperfect assumptions because it is currently impractical to produce single photons. Most practical QKD systems use a laser producing multiple photons as a light source, leading to an eavesdropping attack called the photon number splitting (PSN) attack. In this attack, Eve can split off a single photon from multiple photons of each bit transmission in order to measure the polarization state and allow the rest to forward to Bob. Consequently, Eve can eavesdrop the quantum key without disturbing the system and being detected by Alice and Bob. However, there are many researches that provide potential solutions to prevent the PNS attack such as decoy-state QKD, SARG04 algorithm, differential phase shift QKD, etc (Daniels and Marcellino, 2009).

In the real world, Lydersen et al. (2010) successfully hacked commercial QKD systems using a variant type of an intercept-resend attack, called a fake-state attack. Their research

demonstrated that two BB84-based commercial products from ID Quantique and MagiQ Technologies could be fully cracked using specially tailored bright illumination. As a result, they could eavesdrop the secret key without being detected. Moreover, this attack works equally well on decoy-state BB84 QKDs, SARG04 algorithm, and differential phase shift QKD.

## 7. Three-stage Quantum Cryptography

To protect the quantum system from siphoning attacks (i.e. attacks that exploit the multiple photons emitted by practical light sources, such as PNS attacks), the three-stage quantum cryptography protocol was proposed by Mandal et al. in 2013. In this protocol, multiple photons are allowed for communication, but the protocol still provides secure key distribution. Figure 5 presents the process of the three-stage protocol.

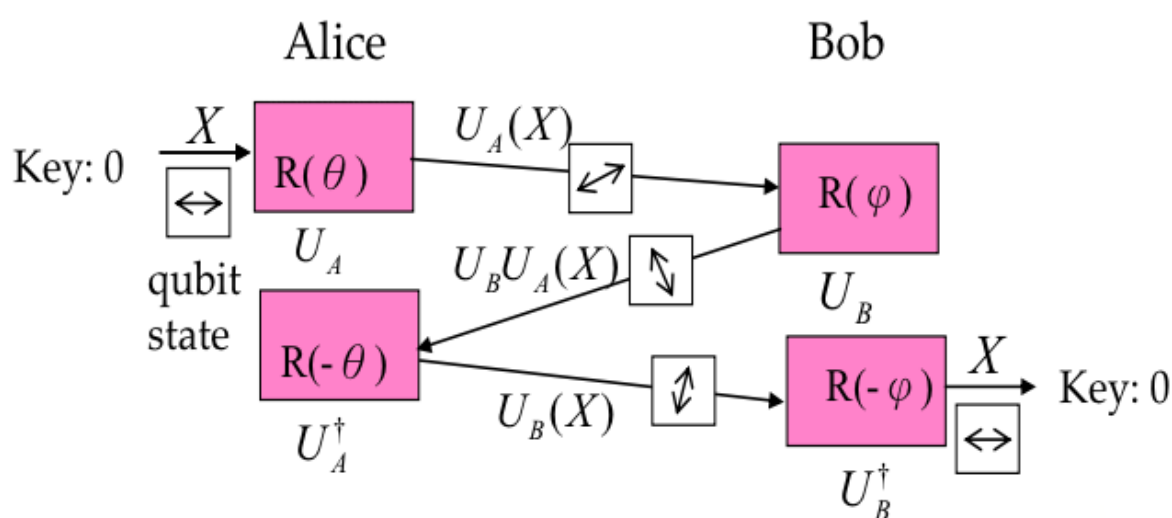


Figure 5 Schematic diagram of the three-stage protocol (Mandal et al., 2013)

Given that  $X$  is the polarization state Alice intends to send to Bob, and secret transformations  $U_A/U_B$  applied by Alice/Bob are commutative, i.e.,  $U_A U_B = U_B U_A$ . Firstly, Alice applies a unitary transformation  $U_A$  on the polarization state  $X$  and sends this message,  $U_A(X)$ , to Bob. Bob then applies  $U_B$  on the  $U_A(X)$ , thereby giving  $U_B U_A(X)$  and returns it to Alice. After that, Alice applies  $U_A^\dagger$  (transpose of the complex conjugate of  $U_A$ ) on the  $U_B U_A(X)$  to get  $U_A^\dagger U_B U_A(X) = U_B(X)$ , and sends it back again to Bob. Finally, Bob applies  $U_B^\dagger$  on  $U_B(X)$  to get the polarization state  $X$ . Although Eve can intercept the message transmitted between Alice and Bob, it is impossible to measure the polarization state without collapsing the transformation  $U_A/U_B$ . Since the unitary transformations,  $U_A/U_B$ , are based on rotations of the photons' polarization states, the principles of quantum mechanics guarantee that Eve cannot tamper with the  $U_A/U_B$  without disturbing it. Therefore, Alice and Bob can detect the eavesdropping (Mandal et al., 2013).



## 8. Conclusion

QKD is the next generation of key distribution systems. It provides secure communication for exchanging the shared secret key between two parties. Due to the principles of quantum mechanics, two parties are capable of detecting eavesdropping performed by the third party. The BB84 algorithm is the first QKD protocol and has been widely applied in a number of both researches and commercial QKD cryptography systems. However, practical QKD implementations are vulnerable to imperfect assumptions and have been proved that they could be attacked by the third party. Several methods including decoy-state BB84 QKDs, SARG04 algorithm, and differential phase shift QKD are invented to mitigate the attacks, but they cannot protect the QKD system from the fake-state attack using tailored bright illumination. Therefore, the new research using three-state quantum cryptography protocol was developed to strengthen the QKD implementations.

## 9. References

- Aggarwal, R., Sharma, H. and Gupta, D. (2011). Analysis of Various Attacks over BB84 Quantum Key Distribution Protocol. *International Journal of Computer Applications*, [online] 20(8), pp.28-29. Available at: <http://www.ijcaonline.com/volume20/number8/pxc3873313.pdf> [Accessed 4 Apr. 2015].
- Bennett, C. and Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. In: *International Conference on Computers, Systems & Signal Processing*. [online] Bangalore, India. Available at: <https://www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf> [Accessed 1 Apr. 2015].
- Bennett, C., Bessette, F., Brassard, G., Salvail, L. and Smolin, J. (1992). Experimental quantum cryptography. *Journal of Cryptology*, [online] 5(1), pp.3-28. Available at: <http://dx.doi.org/10.1007/BF00191318> [Accessed 2 Apr. 2015].
- Blumenthal, M. (2013). *Encryption: Strengths and Weaknesses of Public-key Cryptography*. Undergraduate. Villanova University.
- Daniels, K. and Marcellino, C. (2009). *Security of Quantum Cryptography using Photons for Quantum Key Distribution*.
- Delfs, H. and Knebl, H. (2007). *Introduction to cryptography*. Berlin: Springer, pp.1-12.
- Haitjema, M. (2007). *A Survey of the Prominent Quantum Key Distribution Protocols*. [online] Washington University in St.Louis. Available at: <http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/> [Accessed 4 Apr. 2015].
- Lace, L., Scegulnaja-dubrovska, O., Usov, R. and Zalcmene, A. (2008). Quantum Cryptographic Key Distribution Protocols. *The European Social Fund (ESF)*.
- Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J. and Makarov, V. (2010). Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, [online] 4(10), pp.686-689. Available at: <http://arxiv.org/abs/1008.4593> [Accessed 3 Apr. 2015].
- Mandal, S., Macdonald, G., El Rifai, M., Puneekar, N., Zamani, F., Yuhua Chen, Kak, S., Verma, P., Huck, R. and Sluss, J. (2013). Multi-photon implementation of three-stage quantum cryptography protocol. *The International Conference on Information Networking 2013 (ICOIN)*, [online] pp.6-11. Available at: [http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=6496343](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6496343) [Accessed 3 Apr. 2015].
- Messmer, E. (2007). *Quantum cryptography to secure ballots in Swiss election*. [online] Network World. Available at: <http://www.networkworld.com/article/2286834/lan-wan/quantum-cryptography-to-secure-ballots-in-swiss-election.html> [Accessed 31

Mar. 2015].

Messmer, E. (2013). *Quantum crypto, standard private key blended for first time*. [online] Network World. Available at:

<http://www.networkworld.com/article/2172821/security/quantum-crypto--standard-private-key-blended-for-first-time.html> [Accessed 31 Mar. 2015].

Moore, M. (2014). *China builds computer network impenetrable to hackers*. [online] The Telegraph. Available at:

<http://www.telegraph.co.uk/news/worldnews/asia/china/11216766/China-builds-computer-network-impenetrable-to-hackers.html> [Accessed 31 Mar. 2015].

Nitaj, A. (n.d.). *Quantum and Post Quantum Cryptography*. [online] Available at:

<http://www.math.unicaen.fr/~nitaj/postquant.pdf> [Accessed 31 Mar. 2015].

Scholz, M. (2007). *Quantum Key Distribution via BB84: An Advanced Lab Experiment*. 1st ed.

[ebook] pp.1-7. Available at: <http://www.physik.hu-berlin.de/nano/lehre/f-praktikum/qkr/crypto.pdf> [Accessed 1 Apr. 2015].

SECOQC, (2004). *World Premiere: Bank Transfer via Quantum Cryptography Based on Entangled Photons*. [online] Available at:

[http://www.secoqc.net/downloads/pressrelease/Banktransfer\\_english.pdf](http://www.secoqc.net/downloads/pressrelease/Banktransfer_english.pdf) [Accessed 1 Apr. 2015].

Sharbaf, M. (2009). *Quantum Cryptography: A New Generation of Information Technology Security System. 2009 Sixth International Conference on Information Technology: New Generations*.