Secure Communication Through Identity Based Cryptography Using Quantum Mechanics

Dr. V. Padmavathi [a]

[a] Associate Professor, Department of Computer Science and Engineering, Anurag University, Hyderabad, India.

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

Abstract: Quantum Mechanics laws are employed to cryptography for secure communication which is commonly known as quantum cryptography**.** Quantum cryptography creates an indestructible cryptographic solution by fortifying prime secrecy, which is used in quantum key distribution. It is a eminent technology that allows two entities to securely interact using quantum mechanics. Bits are used in classical cryptography to encode information, but photons and their polarisation, which is commonly known as qubits, are used in quantum cryptography to encode information. The communications are safe because they are based on unbreakable quantum mechanics laws. The identity based cryptosystem, which allows any pair of users to communicate and validate each other's signatures without transferring private or public keys, maintaining key directories, or relying on the services of a third party. This paper aims at explaining identity based cryptography using laws of quantum mechanics.

Keywords: identity based cryptography, quantum cryptography, QKD, qubits, quantum mechanics

1. Introduction (Times New Roman 10 Bold)

In 1969, physicist Stephen Wiesner proposed that the notion of uncertainty may be employed for cryptography [1]. As a result of this, quantum cryptography was born and cryptographers see this as a promising concept. One of the concepts of Wiesner was extended to offer a verifiably secure approach for quantum key distribution, i.e. QKD, based on quantum physics principles [2]. In 1984, Bennet and Brassard, in partnership with Stephen Wiesner, proposed the first QKD, which is now known as the BB84 protocol [4].

Quantum cryptography is a well-known technology that uses quantum mechanics to allow two parties for a secure communication. QKD begins with the transmission of photons that are generated in four arbitrary quantum states pertaining to two basis namely, rectilinear and diagonal which are conjugate to each other [1]. The rectilinear basis is represented in two states with polarizations of 0° horizontally and 90° vertically. The diagonal basis is represented in 45° and 135°[1][4].

The communications are safe because they are based on unbreakable laws of quantum mechanics. Quantum cryptography is built on the fundamentals of quantum mechanics, namely the law of Heisenberg Uncertainty and the law of photon polarisation. The law of Heisenberg Uncertainty states that an observer cannot determine two physical properties that are connected to each other at the same time [4]. Two instances are given in relation to this definition. 1) A common example is the position A and momentum B of a particle P cannot be computed at the same time. A photon cannot be measured in both a rectilinear and a diagonal basis at the same time [1] [2]. If this is done, it will randomise the other. According to the no-cloning theorem [1] [3], the law of photon polarisation states that qubits cannot be replicated. The photons were discovered to be employed for conveying information rather than storing it, which was a huge breakthrough in quantum cryptography [6].

2. Quantum cryptography

Qubit is the fundamental unit of quantum cryptography. It has two states, denoted with ket notations $|0\rangle$ and $|1\rangle$ [1] [5]. A bit can be in either the 0 or 1 state, whereas a qubit can be in either the 0 or 1 state. It can also happen in a state of superposition, which is a linear mixture of the states $|0\rangle$ and $|1\rangle$ since the laws of quantum mechanics are based on the concepts of linear algebra. A state can be denoted using the symbol $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$denotes the state of superposition, where and are complex numbers. A qubit may exist in a superposition state $|0\rangle$ and $|1\rangle$ but this state is impossible to measure. When a qubit is measured, it will almost certainly be in one of two states: $|0\rangle$ and $|1\rangle$ [12]. According to quantum mechanics laws, the chance of acquiring the state $|0\rangle$ or

|1⟩qubit is the modulus squared of. To put it another way, the probability of getting $|\psi\rangle$ in $|0\rangle$ state is α^2, while the probability of getting $|\psi\rangle$ in $|1\rangle$ state is β^2. Squaring the coefficients yields the probability of achieving a measurement result i.e.$|\alpha^2| + |\beta^2| = 1$ [5].

To represent a bit known as a qubit, the photon is polarised in one of the basis. A binary 0 is represented by a photon polarisation of 0° in the rectilinear basis or 45° in the diagonal basis. A binary 1 is represented by a 90° rectilinear polarisation or a 135° diagonal polarisation, as depicted in figure 1 and 2.

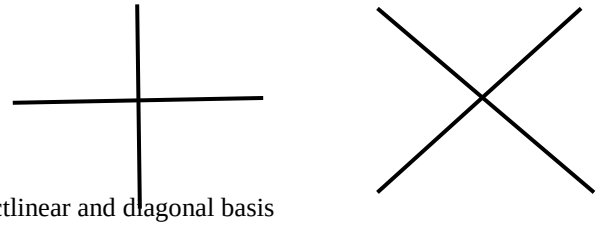

Figure 1: Rectlinear and diagonal basis

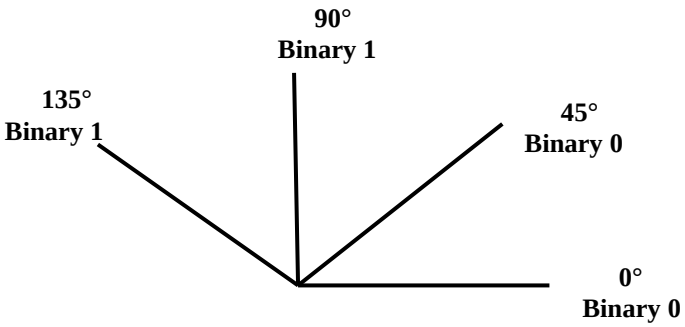

Figure 2: Photon polarization

3. Identity based cryptography

The public key of the user is embedded in a public key certificate in a public key infrastructure environment. This will combine the identity of the certificate owner and public key. This ubiquitous methodology necessitates complete faith in certificate issuers. It has a number of known and inconvenient side effects, including the requirement for faith among users and certificate revocation. The primary issue, though, is the underlying premise that all certifications are public, widespread, and hence easily accessible to anyone. But this statement isn't always true, particularly in wireless networks where the connection is irregular.

Shamir [7] pioneered a new sort of cryptographic technique known as the identity based cryptosystem, which allows any pair of users to securely communicate and validate each other's signatures without transferring private or public keys, maintaining key directories, or relying on the services of a third party. The identity based encryption, alters the nature of getting public keys in which the identities and public keys are mapped one-to-one. As a result, identity-based encryption radically lowers the requirement for public key certificates and certifying authority, as well as their dependence on them. When competent key management and security are required, the identity-based public key cryptosystem can be a viable substitute to certificate based public key infrastructure.

3.1 Procedure

The sender, Alice wishes to establish secure communication with the receiver, Bob. She doesn't want to receive his public key from a key server, and she doesn't want to verify the signature on his public-key certificate with a trusted third party. Bob's public key isn't even something she wants to keep on her own computer. She only wishes to send him a secure message. Bob's public key is made up of his name and IP address. Alice needs a signed digital certificate that has Bob's public key with his identity in conventional public-key cryptography. Bob's public key is his identification in identity-based cryptography. This is a extraordinary thought for a mail system, and it's about as good as it gets: Alice can send Bob secure mail if she knows his address. Trent issues private keys to users according to their identity in the system. If private key of Alice is compromised, she will need to change some part of her identity in order to obtain a new one [13].

4. Quantum Key Distribution Protocol

4.1 BB84 QKD Protocol

In 1984, Bennet and Brassard proposed the quantum key distribution protocol, known as the BB84 protocol, which was based on the Heisenberg Uncertainty principle. The BB84 protocol consists of two basis for specifying photons in rectilinear (R) and diagonal (D) using four polarised photon states. The communicative parties in QKD use both a classical and a quantum communication channel. On the quantum channel, they send polarised single photons, or qubits, whereas on the classical channel, they send conventional communications. The processes for creating a secret key that is shared between two users are as follows and explained in table 1 [9].

1) The sender chooses random basis and generates random bits in a sequence. The sender uses polarised photons to represent bits and transmits the photons to the receiver via the quantum channel.
2) Each of them is measured by the receiver using one of the two bases.
3) If the receiver chooses the same basis as the sender, he or she will share the same binary data with the sender; otherwise no data is being shared.
4) The receiver transmits this via the classical channel, and the sender informs the recipient of the qubits he/she chose on the same basis as the sender.
5) Both parties will eliminate the bits with differing basis, and the remaining bits will form the sifted key [4].

Table 1: BB84 QKD Protocol

Quantum Transmission															
Alice's Random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Alice's random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	/	|	\	–	|	|	–	–	\	/	|	\	/	/	|
Random Bases as received by Bob	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
Public Discussion															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Shared information			1		1			0				1		0	1
Bob reveals some bits at random					1									0	
Alice confirms it					OK									OK	
Sifted Key			1					0				1			1

4.2 B92 QKD Protocol

B92 is a two-state version of the BB84 protocol. Binary 0 is represented by a photon polarisation of 0° in the rectilinear basis, whereas binary 1 is represented by a photon polarisation of 45° in the diagonal basis [8] and shown in figure 3.

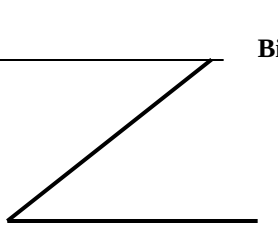

Figure 3: B92 QKD Protocol

4.3 Six-State Protocol (SSP)

The SSP protocol follows the identical stages as the BB84 protocol, with the exception that it permits three orthogonal bases to encode the bits needed for communication between entities. As a result, the bits are represented by six states [10].

4.4 SARG04 protocol

The first step of the SARG04 protocol is the same as that of the BB84 protocol. The second phase is different, as Alice declares a pair of nonorthogonal states. Rather of stating her basis directly, she uses one of them to encrypt her bit. Alice and Bob check which bits have a basis for. If Bob uses the correct basis, he will be able to measure the exact state; otherwise, he will not be able to obtain the bit [11].

5. Proposed method

The identity based quantum cryptography is used for secure communication. Unlike bits which are used in classical method of identity based cryptography, qubits are used in proposed method to generate keys using quantum key distribution method. The keys are generated using identity of the users. The following steps explain the proposed method.

1) Alice considers Bob's identity for generating a key which is generally in bits.
2) She prepares qubits by using random basis from the bits.
3) The qubits transmitted to Bob.
4) Bob receives the key and transforms to bits using random basis.
5) If the key mismatches, then it is disgarded and a new key is generated out of another identity.

6. Conclusion

The identity based cryptography eliminates the infrastructure for public key distribution and the system of Certificate Authority. However, the classical method of identity based cryptography where it uses bits for processing, may fall easily as a prey to quantum computer. So, there is a need for adapting indestructible method through quantum cryptography. As this method relies on laws of quantum mechanics, it renders safe and secure communication between parties. Here the identity of a user is being is used to generate a key using quantum cryptographical methods. Any attempt to identify the key will destroy the qubits due to laws of quantum mechanics and consequently the attack is detected. Thus identity based cryptography using quantum mechanics offers secure communication.

References (APA)

1. Wiesner, S.,"Conjugate Coding", Sigact News, Vol. 15, no. 1, 1983, pp. 78-88; original manuscript written circa 1969.
2. Wiedemann, D., "Quantum cryptography", Sigact News, Vol. 18, no. 2, 1987, pp. 48-51.

3. W. K. Wootters and W. H. Zurek, “A Single Quantum Cannot be Cloned”, Nature 299, 802-803, 1982.
4. Bennett, C.H. and G. Brassard, “Quantum Cryptography: Public key distribution and coin tossing”, Theoretical Computer Science, Elseiver, vol. 560, 2014, pp.7-11.
5. David McMahon, Quantum Computing Explained, IEEE Computer Society, Wiley-Interscience, Copyright @ 2008 John Wiley & Sons, Inc., Publication, ISBN 978-0-470-09699-4.
6. Bennett, C. H., F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography", Journal of Cryptology, vol. 5, no. 1, 1992, pp. 3-28.
7. Shamir, “Identity-based cryptosystems and signature schemes,” in Proc. Crypto 1984, 1984.
8. Bennett, C., "Quantum cryptography using any two nonorthoganol states", Phys. Rev. Lett. 68, 1992, pp. 3121-3124.
9. V. Padamvathi, B. Vishnu Vardhan and A. V. N. Krishna, Quantum cryptography and quantum key
10. distribution protocols: A survey, IEEE the 6th International Conference on Advanced Computing
11. (IACC), pp.556-562, 2016.
12. Bechmann-Pasquinucci, H., and Gisin, N., "Incoherent and coherent eavesdropping in the six-state protocol of
13. quantum cryptography." Phys. Rev. A 59, 4238-4248, 1999.127901(1)- 127901(4).
14. Scarani, A., Acin, A., Ribordy, G., Gisin, N., "Quantum cryptography protocols robust against photon number
15. splitting attacks", Physical Review Letters, vol. 92, 2004.
16. M. A. Nielsen and I. Chuang, Quantum Computation and Quantum Information, 10th Anniversary
17. Edition, Cambridge University Press, 2002.
18. Schneier, Bruce, Applied cryptography: protocols, algorithms, and source code in C, schneier2007applied,
19. 2007, john wiley & sons.