Proc. of The Sixth Intl. Conf. On Advances In Computing, Control And Networking - ACCN 2017

ISBN: 978-1-63248-117-7 doi: 10.15224/ 978-1-63248-117-7-52

QUANTUM ELGAMAL Cryptosystem

Vaibhav Gupta[1], Aditya Agrawal[1], K.K. Shukla[1] and Bhaskar Biswas[1]

Abstract*—Public key cryptography is extensively used for encryption, signing contracts and secure exchanges over the unreliable network. The findings of Shor in 1994, of a powerful algorithm which was based on quantum mechanics for computing discrete logarithms and factoring large integers sabotaged the security presumptions upon which the currently used public key cryptographic protocols are based, like ElGamal, RSA and ECC. However, few cryptosystems, known as post quantum cryptosystems, while not currently in wide use are considered to be resistant to such attacks. In this paper, a quantum version of ElGamal Cryptosystem is proposed whose security relies on the commutative rotation transformations and measurements in computational basis of qubits. An understanding of the new scheme over the quantum channels is provided. The proposed cryptosystem allows the party to send messages in the form of qubits over a quantum channel. Also the proposed protocol provides an opportunity for two parties to exchange keys which is considered as one of the major concerns while developing post quantum cryptosystems.

Keywords*—Quantum, elgamal, shor, post quantum, commutative rotation, qubits, cryptosystem.

I. Introduction

Cryptographic protocols present a significant role in the secure sharing of data or information over an unreliable network. Protocols such as ElGamal [12], Diffie- Hellman (DH) key agreement [13] and the RSA encryption schemes [3] consistently provide methods for secure encryption or key exchanges for many operations over the Internet. The security which these protocols guarantee is based on mathematical hypothesis such as difficulty of determining the discrete logarithm [4] or factoring large numbers into primes. However, since the discovery of the Shor's algorithm[5], these problems are vulnerable to quantum algorithms. Taking the example of the factoring problem, factoring a large number reduces to the problem of finding periods of certain functions which the quantum computers made possible by using the quantum fourier transform. Hence the security provided by these protocols seems to be short-lived with the arrival of quantum computers.

However, few cryptosystems, called quantum and post quantum cryptosystems, while not widely in use are considered to be resistant against quantum computing based attacks. Post quantum cryptosystems are the classically intractable cryptosystems that are proved to be secure against the attacks proposed by Shor [5]. These cryptosystems are not widespread as most of them are built on lattices, goppa codes, braids etc. and are tedious to implement in practicality. However these platforms are the reason behind the security of these cryptosystems against the quantum computing based attacks. Some of the popular post quantum cryptosystems are LWE, RLWE, NTRU, McEliece etc [6, 7, 8, 9]. Quantum cryptosystems are the parallels of classical cryptosystems in the quantum setting. Contrary to classical binary bits, quantum cryptosystems work on quantum bits or qubits that can take values 0, 1 or a superposition of the two. Working with qubits opens up large possibilities of algorithms that can be formulated over a quantum channel. Some of the recently proposed quantum cryptosystems are quantum diffie-hellman (QDH) [10], BB84 [11] etc. The quantum cryptosystems majorly consist of key distribution schemes over a quantum channel because there is a limit to the size of messages which can be sent over the quantum channel in the form of qubits.

In this paper, we propose a quantum version of the ElGamal protocol (QE(m)), m being the number of computational bases required in the protocol. Analogous to the classical version of the protocol, QE(m) is an encryption protocol as well where any one of the parties try to send an encrypted message to the other which is then decrypted by the other party and the actual message is retrieved. The computational basis is publically available to the two parties. The qubit sequences are manipulated by rotating them according to the set of basis and transmitted over a quantum channel. The received sequence of qubits are again rotated according to the bases and measured to recover the encrypted bits. The organisation of this paper is as follows. In section 2, we present the classical ElGamal cryptosystem [12] that is vulnerable to quantum computers. In section 3, we will look at the principles of quantum cryptosystems. In section 4, we review the quantum diffie-hellman protocol [11] on which our cryptosystem is based upon. In section 5, we present our quantum elgamal cryptosystem. In section 6, we provide the security analysis of the proposed protocol and finally we conclude the paper in Section 7.

II. ElGamal Cryptosystem

In 1985, ElGamal presented a new cryptosystem to the world which relied on the difficulty of finding a solution to the hard discrete logarithm problem in F_p.

Theorem 1 (Discrete Logarithm Problem) Given a primitive root g of the multiplicative group F_p and a random element a of F_p , the discrete logarithm problem (DLP) is the hard computational problem of finding x such that $a \equiv g^x (mod p)$.

Proc. of The Sixth Intl. Conf. On Advances In Computing, Control And Networking - ACCN 2017

ISBN: 978-1-63248-117-7 doi: 10.15224/ 978-1-63248-117-7-52

1. Department of Computer Science and Engineering, Indian Institute of Technology (BHU), Varanasi, India

The ElGamal cryptosystem can be briefly described as follows:

1. Key generation

• Select a large prime number p and a primitive root (generator) g of the multiplicative group $(Z/pZ)^*$.

• Randomly select an integer a such that $2 \leq a \leq p-2$.

• Compute $b \equiv g^a (mod p)$.

• Make the key (p, g, b) public and keep the key a as private.

2. Encryption

• Represent the message to be transmitted as a positive integer $m < p$.

• Randomly choose an integer k with $2 \leq k \leq p-2$.

• Encrypt m with the public key (p, g, b) using the rule

$$\gamma \equiv g^k (mod p)$$

$$\delta \equiv m b^k (mod p)$$

3. Decryption

• The receiver decrypts the message using the rule $m \equiv \gamma^{-a} \delta (mod p)$.

• Transform the positive integer m into the original message.

The correctness of the decryption in the El Gamal cryptosystem is as follows. We have

$$\gamma^{-a}\delta \equiv (g^k)^{-a} m b^k \equiv (g^k)^{-a} m (g^a)^k \equiv m (mod p)$$

The most common attack on an El Gamal cryptosystem is to solve the discrete logarithm problem. There are three basic types of discrete logarithm algorithm solvers: Pollard's rho algorithm, the Pohlig-Hellman algorithm, and the index calculus algorithm. The complexity of Pollard's rho algorithm and the Pohlig – Hellman algorithm are exponential while the expected running time of the index calculus algorithm is with a constant $c > 0$. For comparison, the running time of Shor's algorithm for discrete logarithm on a quantum computer is .

III. Quantum Diffie-Hellman Protocol

The Quantum Diffie – Hellman[10] (QDH(t)) is a key exchange scheme wherein Alice and Bob obtain a shared secret key based on the knowledge derived from each other. In QDH(t), Alice and Bob both control a sequence of qubits, whose states are shaped using the rotational quantum operations. These sequence of qubits are exchanged through a quantum channel. Each qubit upon receiving at each end is again manipulated and measured against the specified bases. Finally their values are stored by both the parties. In the protocol, QDH(t), t is the number of bases accessible to both Alice and Bob for the measurement of qubits at each step. Alice and Bob comply on the set of t bases, $B_1, B_2, ..., B_t$, $t>1$, to be used for measurement and the number of qubits to be utilised, m. The value of m depends on the required key length and the fact that some of the qubits will be discarded during detection of Eve's existence. Finally, they agree on the initial state of qubit to be $|\psi\rangle = |0\rangle$.

Phase 1:

• Alice independently and arbitrarily chooses m bases $B_1^a, B_2^a, ..., B_m^a$ out of the available t bases such that $B_i^a \in \{B_1, B_2, ..., B_t\}$.

• She also sets up a uniform and random bit sequence of length m : $a_1, a_2, ..., a_m$.

• Similarly, Bob independently and arbitrarily chooses m bases $B_1^b, B_2^b, ..., B_m^b$ out of the available t bases such that $B_i^b \in \{B_1, B_2, ..., B_t\}$.

• Bob also sets up a uniform and random bit sequence of length m : $b_1, b_2, ..., b_m$.

Transmission of Qubits:

1. Alice encodes the bit a_i in base B_i^a by applying the transformation U_i^a to $|0\rangle$, where $U_i^a = R(\theta_{ai})$ is a quantum rotation transformation and sends the qubit to Bob over a quantum channel.

2. Similarly Bob encodes the bit b_i in base B_i^b by applying the rotational transformation U_i^b to $|0\rangle$, where $U_i^b = R(\theta_{bi})$ and sends the qubit to Alice over the same quantum channel.

Measurements: Upon reception of the qubit from the other party, Alice and Bob execute the following operations.

1. Alice applies two rotation transformations to the qubit received from Bob: first she applies the transformation U_i^a to the qubit and then applies $U_{slack}(B_i^a)$ to the qubit.

2. Alice measures the qubit in basis B_i^a and stores the resulting bit as k_i.

3. Similarly, Bob applies two rotation transformations to the qubit received from Alice: first he applies the transformation U_i^b to the qubit and then applies $U_{slack}(B_i^b)$ to the qubit.

4. Bob measures the qubit in basis B_i^b and stores the resulting bit as k_i'.

Where $U_{slack}(B_j)$ is also a rotational transformation $R(90^\circ - \theta_0)$ for that basis.

Phase 2: Let $K = k_1, k_2, ..., k_m$ and $K' = k_1', k_2', ..., k_m'$ be the sequence of the bits recorded by Alice and Bob

Proc. of The Sixth Intl. Conf. On Advances In Computing, Control And Networking - ACCN 2017

ISBN: 978-1-63248-117-7 doi: 10.15224/ 978-1-63248-117-7-52

during the protocol stage, respectively. The following operations are performed to obtain a common shared key.

1. Alice and Bob disclose their respective sequence of bases B_i^a's and B_i^b's to each other over the public channel.

2. For each agreement i, where $B_i^a \neq B_i^b$, reject the values k_i and k_i' from K and K'.

3. Alice and Bob arbitrarily select k bits from the remaining sequence of bits and match their values. If Eve has hampered with their exchanges, they will witness error and can reject the key.

The number of matching bits and the size of the subset k may vary depending on the efficiency and the security of the executed protocol.

IV. Quantum ElGamal Cryptosystem

Diffie-Hellman key exchange algorithm was simplified by introducing a random exponent k which was the replacement for the private exponent of the receiving entity, and the algorithm thus obtained was ElGamal. This simplification made it possible for an entity to encrypt in one direction, without the requirement of the second entity to take actively part. In this section, a Quantum version of the ElGamal cryptosystem will be introduced to the reader.

A. Key Generation

The basic necessity for a cryptographic protocol is at least one key in symmetric algorithms and two keys in asymmetric. In ElGamal, only the receiving party is required to create a key beforehand and publish it. We will now follow Bob with his scheme of key generation in the Quantum version of the protocol.

1. Computational bases selection

First Bob needs to select a set of m bases, $B_1, B_2, ..., B_m$, $m > 1$, to use. The value of m is dependent on the number of qubits to be used which is further dependent on the desired length of a single block of message to be encrypted. For every basis B_i, there exists two rotation transformations $R(\theta_0)$ and $R(\theta_1)$ for bit 0 and bit 1, respectively. Also we have $\theta_1 = \theta_0 + 90^\circ$. For example, the bases can be of the form $\{0^\circ, 90^\circ\}$, $\{30^\circ, 120^\circ\}$, $\{41^\circ, 151^\circ\}$ and so on.

2. Private key generation

Bob generates m random and uniform bits $b_1, b_2, ..., b_m$ each time Alice creates a new session with him. This uniform bit sequence of length m acts as the private key for Bob.

3. Public key assembling

For every $1 \leq i \leq m$, Bob encodes b_i in base B_i by applying U_i^b to $|0\rangle$, where $U_i^b = R(\theta_{bi})$ and sends the qubit $|B\rangle$ to Alice through the quantum channel.

4. Public key publishing

The public key for Bob now consists of the set of m bases, $B_1, B_2, ..., B_m$, $m > 1$ and the rotated qubits $|B\rangle$ which is generated afresh and sent through the quantum channel each time Alice creates a new session.

B. Encryption Procedure

To be able to encrypt a message M to Bob, Alice first needs to create a fresh session with Bob and obtain his public key i.e. the qubit $|B\rangle$ along with the m computational bases. Alice has to follow the following steps for the encryption of the plaintext message M.

1. Obtain the public key

As mentioned above, Alice has to start by creating a new session with Bob and obatin the public key of Bob i.e. the qubit $|B\rangle$ through the quantum channel along with the m computational bases from a trusted keyserver.

2. Prepare M for encoding

Write M as set of sequence of uniform bits of length $m(m_1, m_2, ...)$. These sequence of bits will be encoded one by one, using the qubits and the computational bases.

3. Select random bit sequence

In this step, Alice has to select her own set of random and uniform bit sequence of length m, $a_1, a_2, ..., a_m$, which will act as the random exponent k of the classical ElGamal cryptosystem. The randomness is an important factor here as the possibility to guess the sequence of bits gives a sufficient amount of information to the attacker, necessary to decrypt the message.

4. Compute public key

To transmit the random bit sequence $a_1, a_2, ..., a_m$, to Bob, Alice computes the qubit $|A\rangle$ by applying U_i^a to $|0\rangle$ using the bases obtained from Bob, where $U_i^a = R(\theta_{ai})$ and sends it to Bob using the quantum channel.

5. Encrypt the plaintext

In this step, Alice encrypts the plaintext message M. For this, she iterates over the set of bit sequences created in step 2 and encodes each of the m_i as:

• Upon receiving the qubit $|B\rangle$ from Bob, Alice applies two rotation transformations: first she applies her U_i^a to the qubit and then she applies $U_{\text{slack}}(B_i)$ to the qubit. Then she measures the obtained qubit in basis B_i and records the resulting bit as k_i. $U_{\text{slack}}(B_i)$ is defined as $R(90^\circ - \theta_0)$ for that basis.

• Depending on k_i, we define the final bases for encryption of the plaintext. If k_i is 0, `we select the Basis` $\oplus = \{|\uparrow\rangle, |\rightarrow\rangle\}$ and if k_i is 1, `we select the Basis` $\otimes = \{|\nwarrow\rangle, |\nearrow\rangle\}$ for encoding the bits of the plaintext.

• Encoding of the bits of m_i is done as follows, Thus, Alice sends the m photons to Bob through the quantum channel, each in any one of the states $|\uparrow\rangle$, $|\rightarrow\rangle$, $|\nwarrow\rangle$ or $|\nearrow\rangle$ as shown in Table 1.

Proc. of The Sixth Intl. Conf. On Advances In Computing, Control And Networking - ACCN 2017

ISBN: 978-1-63248-117-7 doi: 10.15224/ 978-1-63248-117-7-52

C. *Decryption Procedure*

After receiving the qubit $|A\rangle$ followed by the set of qubits $|M_i\rangle$, Bob has to decode the photons to be able to read the plaintext M . Therefore the decryption algorithm can be divided in a few steps:

1. Compute shared key

Upon receiving the qubit $|A\rangle$ from Alice, Bob applies two rotation transformations: first he applies his U_i^b to the qubit and then he applies $U_{\text{slack}}(B_i)$ to the qubit. Then he measures the obtained qubit in basis B_i and records the resulting bit as k_i.

2. Decryption

Depending on k_i, Bob selects any one of the bases $\oplus$ $\otimes$ and measures the receiving photons in the respective basis to obtain the plaintext bit by bit.

After combining all of the m_i, Bob is able to read the message M sent by Alice.

V. Security Analysis

The security of the Quantum-Elgamal-type cryptosystems is based on the fact that measurement of a qubit or quantum bit destroys it's state that is the qubit is left in either of the two pure states. To decrypt the message sent by Alice, the eavesdropper, Eve has to decode or measure the quantum bits for which he requires to have the knowledge about the bases $\oplus$ $\otimes$ and for that he must know the shared key. Now suppose Eve tries to measure the sequence of qubits $|B\rangle$ against the m computational bases to gather knowledge about the secret bit sequence $b_1, b_2, ..., b_m$ of Bob, Alice would know about his presence as the qubits recepted at her end would be present in the pure states. Hence, the protocol is considered secure against a passive attacker. Also, in the situations where the protocol might be used as a key agreement protocol, it would present perfect forward secrecy as Bob generates fresh sequence of uniform bits each time Alice requests for a new session of key exchange.

TABLE I. ENCODING OF BITS

1	0	
$\|\rightarrow\rangle$	$\|\uparrow\rangle$	Basis $\oplus$= {$\|\uparrow\rangle$, $\|\rightarrow\rangle$ }
$\|\nearrow\rangle$	$\|\nwarrow\rangle$	Basis $\otimes$ = {$\|\nwarrow\rangle$, $\|\nearrow\rangle$ }

Conclusion

A new quantum elgamal cryptosystem is explained. We presented a cryptosystem that was derived from the quantum version of diffie-hellman as described before, but might be seen as an improvement as the elgamal cryptosystem can be used for signing messages or encryption in one direction without direct interaction between the parties. The protocol exchanges a pair of sequences of qubits between two parties over a quantum channel and uses computational bases as a parameter for commutative quantum rotation transformations to decrypt the message. Post quantum cryptography is an up-and-coming area of research that had come up after the introduction of Shor's algorithm. The classical cryptosystems like RSA, Diffie- Hellman and ElGamal will be completely obsolete with a quantum computer. Hence, the future studies require more research work in this field.

References

[1] *C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of IEEE International Conference on Computers, Systems & Signal Processing, Bangalore, India, 1984, pp. 175–179.*

[2] M. Hellman, "An overview of public key cryptography," Communications Society Magazine, IEEE, vol. 16, no. 6, pp. 24–32, November 1978.

[3] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[4] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, Handbook of Applied Cryptography, 1st ed. Boca Raton, FL, USA: CRC Press, Inc., 1996.

[5] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput., vol. 26, no. 5, pp. 1484–1509, Oct. 1997. [Online]. Available: http://dx.doi.org/10.1137/S0097539795293172

[6] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, STOC 2005, ACM (2005) p. 84–93.

[7] Bos, Joppe W., Craig Costello, Michael Naehrig, and Douglas Stebila. "Post quantum key exchange for the TLS protocol from the ring learning with errors problem." In Security and Privacy (SP), 2015 IEEE Symposium on, pp. 553-570. IEEE, 2015.

[8] J. Hoffstein, J. Pipher, and J. H. Silverman, NTRU: A Ring Based Public Key Cryptosystem in Algorithmic Number Theory. Lecture Notes in Computer Science 1423, Springer-Verlag, pp.267–288, 1998.

[9] McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. The Deep Space Network Progress Report 42–44, Jet Propulsion Laboratory, Pasadena, CA, (1978), 114–116.

[10] Subramaniam, Pranav, and Abhishek Parakh. "A Quantum Diffie-Hellman Protocol." In MASS, pp. 523-524. 2014.

[11] C.H. Bennett and G. Brassard. Quantum cryptography: Public-key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, IEEE Press, pp. 175–179, Bangalore, India, 1984.

[12] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In Proceedings of CRYPTO 84 on Advances in cryptology, pages 10–18. Springer-Verlag New York, Inc., 1985.

[13] Diffie, Whitfield, and Martin E. Hellman. "New directions in cryptography." Information Theory, IEEE Transactions on 22, no. 6 (1976): 644-654.

[14] Nitaj, Abderrahmane. "Quantum and post quantum cryptography.",Science and Information Systems (ICSIS'2014) (2014).

[15] Meier, Andreas V. "The ElGamal Cryptosystem." (2005).

ISBN: 978-1-63248-117-7 doi: 10.15224/ 978-1-63248-117-7-52

About Author (s):

Bhaskar Biswas received his Ph.D. in Computer Science and Engineering from Indian Institute of Technology (BHU), Varanasi. He is working as Assistant Professor at Indian Institute of Technology (BHU),Varanasi in the Computer Science and Engineering department. His research interests include Data Mining, Text Analysis, Machine Learning, Link Prediction, Social Network Analysis.

Dr. K. K. Shukla received Ph.D. And Mtech. from Banaras Hindu University. Working as the head of department of Computer Science and Engineering. His research interests are Information Security, Advanced Computer Networks, Computer Graphics, Graph Theory.

Vaibhav Gupta is currently pursuing his B.Tech, in Computer Science and Engineering from Indian Institute of Technology (BHU), Varanasi. His fields of interests are Cryptography, Machine Learning and Artificial Intelligence.

Aditya Agrawal is currently pursuing his B.Tech in Computer Science and Engineering from Indian Institute of Technology (BHU), Varanasi. His fields of interest are Cryptography, Machine Learning, AI, Deep Learning.