A Quantum Diffie-Hellman Protocol

Pranav Subramaniam
University of Nebraska, Omaha, NE
Email: submarine3.14159@gmail.com

Abhishek Parakh
Nebraska University Center for Information Assurance
University of Nebraska, Omaha, NE
Email: aparakh@unomaha.edu

***Abstract*—In this paper, a quantum version of Diffie-Hellman key agreement protocol is developed using the commutative rotation transformations.**

I. Introduction

Cryptographic protocols play an important role in the secure sharing of information over a network. Protocols such as Diffie-Hellman (DH) key agreement, ElGamal, and the RSA encryption schemes [1], [2], [3] routinely provide methods for secure key agreement or exchanges for many applications over the Internet. The security provided by these protocols is based on mathematical assumptions such as difficulty of factoring large numbers or determining the discrete logarithm [4]. However, as shown by Peter Shor in [5], these can be easily solved by using quantum algorithms. Hence the security provided by these protocols may be short-lived with the advent of quantum computers.

In this paper, we develop a quantum version of the Diffie-Hellman (DH) protocol (QDH(t)), where t is the number of computational bases used in the protocol. Analogous to the original protocol, QDH(t) is also a key agreement protocol where neither of the parties determines the encryption key in advance and both parties have equal amounts of input into the final encryption key. In each protocol step, a computational basis is randomly and independently chosen by the two parties from the available t bases. The current qubit of the sequence is rotated according to the chosen basis by each and exchanged over a quantum channel. The received qubits are further manipulated by rotating them and measured to retrieve the key bit.

Modular exponentiations performed in the Diffie-Hellman protocol are mapped to the commutative rotation operations over qubits. This also enables the proposed protocol to detect eavesdropping and provide additional security in comparison to the DH protocol. The probability of detecting Eve using a given number of exchanges and the number of exchanges needed to detect Eve with a given probability are determined to analyze the performance of the QDH(t) protocol. We also analyze the effect of the number of available bases, t, on the probability of detecting Eve for a given number of exchanges and the number of exchanges needed to detect Eve with a given probability. The performance of the protocol is compared with that of the BB84 protocol and it is shown that the QDH(t) protocol has a higher probability of detecting Eve for a given number of exchanges and bases t.

The proposed protocol enables Alice and Bob to input equal amounts of randomness into the final encryption key. Further, Diffie-Hellman type of key exchange provides opportunity to develop perfect forward secrecy [6] using quantum cryptography.

II. The Diffie-Hellman Key Agreement Protocol

Diffie and Hellman in their seminal work [7] developed a key agreement scheme between parties Alice and Bob over an insecure channel. Before the actual key exchange begins, both parties agree on a prime number p and its primitive root g. These are public knowledge.

1) Alice chooses a secret random number a from Z_p, computes g^a mod p, and sends the result to Bob,
2) Bob picks secret random number b from Z_p, computes g^b mod p, and sends the result to Alice,
3) On receipt of the transmission, Alice obtain the key, $K = (g^b)^a = g^{ba}$ mod p by using her number a and Bob obtains the exact same key $K = (g^a)^b = g^{ab}$ mod p computed by Bob using his number b on receiving data from Alice.

The security of the Diffie-Hellman protocol is based on how difficult it is for an eavesdropper, Eve, to construct the key using the public information exchanged between Alice and Bob. Eve has to find Alice's secret number a and/or Bob's secret number b using the prime number p, g, g^a mod p, and g^b mod p that she can obtain by intercepting their communications. This is also known as the discrete logarithm problem. However, discrete logarithm is a hard problem and is considered infeasible to solve using current computing technology when the prime p has more than 300 decimal digits and a and b have more than 100 decimal digits.

III. The Proposed Quantum Diffie-Hellman Protocol

The QDH(t) is a key agreement protocol wherein Alice and Bob derive a shared secret key based on the information obtained from each other. In QDH(t), Alice and Bob each maintain a sequence of qubits, which are manipulated using the rotation quantum operators and exchanged over a quantum channel. Each qubit upon reception at each end is further manipulated, measured, and their values are noted. In the protocol, QDH(t), the input t is the number of bases available to Alice and Bob to measure qubits in each step.

Public agreement: Alice and Bob agree on the set of t bases, $B_1, B_2, \ldots, B_t$, $t > 1$, to use and the number of qubits to be exchanged, m. The value of m is dependent on the desired key length and the number of qubits that will be discarded during detection of Eve's presence. Further, they agree on initial state of qubit $|\psi\rangle = |0\rangle$ that will be manipulated and exchanged.

Phase 1:

- Alice independently and randomly chooses m bases $B_1^a, B_2^a, \ldots, B_m^a$ such that $B_i^a \in \{B_1, B_2, \ldots, B_t\}$.
- She also generates a random and uniform bit sequence of length m: $a_1, a_2, \ldots, a_m$.
- Similarly, Bob independently and randomly chooses m bases $B_1^b, B_2^b, \ldots, B_m^b$ such that $B_i^b \in \{B_1, B_2, \ldots, B_t\}$.
- Bob also generates a random and uniform bit sequence of length m: $b_1, b_2, \ldots, b_m$.

From above, for every basis B_i, there are two possible rotation transformations $R(\theta_0)$ and $R(\theta_1)$ corresponding to bit 0 and bit 1, respectively. Therefore we have $\theta_1 = \theta_0 + 90°$. For example, possible choices for bases include $\{0°, 90°\}, \{30°, 120°\}, \{41°, 151°\}$ and so on.

Therefore, to encode bit 0 in basis $\{30, 120\}$ one could apply transformation $R(30°)$ to $|\psi\rangle = |0\rangle$. Similarly, in order to encode bit 1 in the same basis one could apply transformation $R(120°)$ to $|\psi\rangle = |0\rangle$.

Transmission of qubits:

1) Alice encodes a_i in base B_i^a by applying U_i^a to $|0\rangle$, where $U_i^a = R(\theta_{a_i})$ and sends the qubit to Bob.
2) Similarly Bob encodes b_i in base B_i^b by applying U_i^b to $|0\rangle$, where $U_i^b = R(\theta_{b_i})$ and sends the qubit to Alice.

Measurements:

Upon receiving the qubit from the other party, Alice and Bob perform the following operations:

1) Alice upon receiving the qubit from Bob, applies two rotation transformations: first she applies her U_i^a to the qubit and then she applies $U_{slack(B_i^a)}$ to the qubit.
2) Alice measures the received qubit in basis B_i^a and records the resulting bit as k_i.
3) Similarly, Bob upon receiving the qubit from Alice, applies two rotation transformations: first he applies his U_i^b to the qubit and then he applies $U_{slack(B_i^b)}$ to the qubit.
4) Bob measures the received qubit in basis B_i^b and records the resulting bit as k'_i.

Where $U_{slack(B_i^j)}$ is defined as $R(90 - \theta_0)$ for that basis. For example, for basis $\{30, 120\}$ the slack rotation is $R(90 - 30) = R(60)$.

a) Phase 2:: Let $K = \{k_1, k_2, \ldots, k_m\}$ and $K' = \{k'_1, k'_2, \ldots, k'_m\}$ be the sequence of random bits obtained by Alice and Bob, respectively. The following steps are performed to derive common shared key.

1) Alice and Bob announce their respective sequence of bases B_i^as and B_i^bs to each other over the public channel.
2) For each exchange i, where $B_i^a \neq B_i^b$, discard the values k_i and k'_i from K and K'.
3) Alice and Bob randomly choose k bits from the remaining set of bits and compare their values. If Eve has interfered with their transmissions, they will find error and can discard the key.

The size of the subset k and the number of bits that must match vary depending on the efficiency and the security of the protocol.

IV. Conclusions

A new quantum Diffie-Hellman protocol is presented. The protocol takes the number of computational bases as a parameter and exchanges a pair of sequences of qubits between two parties over a quantum channel. Commutative quantum rotation operators are used by both parties to derive shared secret key. In our future work, we will study the security provided by the protocol by comparing it to the well-known BB84 protocol and implement perfect forward secrecy using the proposed protocol.

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] W. Diffie, P. C. Van Oorschot, and M. J. Wiener, “Authentication and authenticated key exchanges,” *Des. Codes Cryptography*, vol. 2, no. 2, pp. 107–125, Jun. 1992. [Online]. Available: http://dx.doi.org/10.1007/BF00124891

[7] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE Trans. Inf. Theor.*, vol. 22, no. 6, pp. 644–654, Sep. 2006. [Online]. Available: http://dx.doi.org/10.1109/TIT.1976.1055638