Post-Quantum Diffie-Hellman and Symmetric Key Exchange Protocols

Xiangdong Li, Lin Leung, Andis Chi-Tung Kwan, Xiaowen Zhang, Damikka Kahanda, and Michael Anshel, Members, IEEE

Abstract—If an eavesdropper Eve is equipped with quantum computers, she can easily break the public key exchange protocols used today. In this paper we will discuss the post-quantum Diffie-Hellman key exchange and private key exchange protocols.

Index Terms—Post-quantum, Key Exchange, Diffie-Hellman, Quantum protocols, Teleportation, Quantum Clock.

I. INTRODUCTION

Diffie and Hellman proposed the first public-key agreement for key exchange in 1976. This protocol relies on the difficulty of computing discrete logarithms in a finite field. The most popular public key algorithm for encryption and digital signature is RSA. The security of RSA is based on the intractability of the integer factorization problem. There are a few other cryptographic schemes that are used in practice, for example, the Digital Signature Algorithm (DSA) and the Elliptic Curve Digital Signature Algorithm (ECDSA). The security of these schemes is based on the discrete logarithm problem in the multiplicative group of a prime field or in the group of points of an elliptic curve over a finite field.

But in 1994 Shor [1] showed that quantum computers can break all digital signatures that are used today. In 2001 Chuang et al [2] implemented Shor’s algorithm on a 7–qubit quantum computer. When quantum computers reach approximately 30 to 40 q–bits they will start to have the speed (parallelism) needed to attack the methods society uses to protect data and processes, including encryption, digital signatures, random number generators, key transmission, and other security algorithms.

Manuscript received March 12, 2006.

Dr. Xiangdong Li is the New York City College of Technology, The City University of New York (CUNY), CST, 300 Jay Street, Brooklyn, NY 11201 USA; e-mail: xli@citytech.cuny.edu.

Dr. Lin Leung is from Borough of Manhattan Community College, CUNY, CIS, 199 Chambers Street, NY, NY 10007.

Andis Chi-Tung Kwan, Xiaowen Zhang, and Damikka Kahanda are graduate students at the CS, Graduate Center, CUNY, 365 5th Ave, NY, NY 10016.

Dr. Michael Anshe is from The City College, CUNY, CS, 138th Street, NY, NY 10031.

We cannot predict exactly when this will happen because each advance in the number of q–bits has had radically different hardware architecture. Scientists believe quantum computers will surpass the speed of “Moore’s Law” computers in the next 20 years, break encryption in 25 years, and break the responding enhanced encryption (with much longer key lengths) in 30 to 50 years.

The scientists from RSA Laboratories have recently been considering quantum cryptanalysis more closely. RSA Laboratories has made it a priority to assess the impact of quantum information processing on IT security in general and on RSA Security’s products in particular as part of their research program.

Many quantum public key exchange protocols have been studied, for example BB84 [3] and B92 [4]. We will look at two schemes that achieve key agreement protocol.

The heart of our key exchange protocol is to use a public satellite – continually broadcasting random bits at a rate so high that no one could store more than a small fraction of them. Parties that want to communicate in privacy share a relatively short key that they both use to select a sequence of random bits from the public broadcast; the selected bits serve as an encryption key for their messages. An eavesdropper cannot decrypt an intercepted message without a record of the random broadcasts, and cannot keep such a record because it would be too voluminous. How much randomness would the satellite have to broadcast? Rabin and Ding [5] mention a rate of 50 gigabits per second, which would fill up some 800, 000 CD-ROMs per day.

II. POST-QUANTUM KEY EXCHANGE

<table>
<thead>
<tr>
<th>General Key Agreement Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Random source: a satellite sends random bit signals.</td>
</tr>
<tr>
<td>2. The two communicating parties Alice and Bob get these signals.</td>
</tr>
<tr>
<td>3. They need to know when they should count the bits as the key.</td>
</tr>
<tr>
<td>4. Two ways: Quantum Teleportation [6] or Quantum clock synchronization [7].</td>
</tr>
<tr>
<td>5. They agree to flip one bit or more.</td>
</tr>
</tbody>
</table>

1-4244-0130-5/06/$20.00 ©2006 IEEE 382
The general framework is shown in Figure 1:

![Diagram of quantum key exchange](image)

**Figure 1. General framework of the post-quantum key exchange scheme.**

**Symmetric Key Exchange:**

- At the beginning, Alice and Bob use quantum clock to synchronize their clocks.
- When Alice wants to send the message to Bob, she teleports a quantum particle state to Bob. Both of them understand they will start to count the bits at time \( t_1 \) (or after \( A \)) as a key. (It depends on the particle state which teleported between Alice and Bob.)
- The key vanishes after it is used by Alice and Bob.
- An eavesdropper Eve could not get this entangled information, so Eve could not know the key.

**Diffie-Hellman Key Exchange:**

- Alice and Bob use quantum clock to synchronize their clocks.
- When Alice wants to send the message to Bob, she publicly announces to Bob that they will start to count the bits at time \( t \). They also agree to use a prime number \( p \). Everyone can start to count the bits at time \( t \), including the eavesdropper Eve. The public key is \( g_1 \).
- Alice teleports a quantum particle state to Bob and tell Bob that she flips the \( n \)th bit of \( g_1 \). The position of the bit flipped depends on the quantum state teleported by Alice to Bob. So both Alice and Bob have the new key called \( g_2 \).
- Alice chooses her secret key \( a \), and Bob chooses his secret key \( b \). Alice sends Bob \( g_1^a \pmod{p} \), and Bob sends Alice \( g_2^b \pmod{p} \). Both Alice and Bob have arrived at the same value \( g_{ab} \).
- The key vanishes after it is used by Alice and Bob.

Only \( p \) is public, the eavesdropper Eve could intercept \( g_1^a \pmod{p} \) and \( g_2^b \pmod{p} \). All \( a \), \( b \) and \( g_2 \) are secret. Eve could not figure out the key even if she has quantum computer or this makes too hard for her to configure the key.

There are several passive quantum attacks and active eavesdropping on the quantum channel by beam splitter and phase shifters. To countermeasure weak impersonation attack, we propose to extend the current scheme to use a polarization QKD scheme that can reduce the transmission rate of errors and defeat man-in-the-middle attack. Our novel idea is that Alice and Bob use a quantum device to exchange an agreement operator at time \( t \). Then they apply the same operator on the random bits stream and yield to the same key. Presently, there is no realistic countermeasure against parallel timing attacks on physical device. Any advance against active impersonation attack and quantum denial-of-service attack is highly desirable.

**REFERENCES**


