Chapter 27
Sustainability of Public Key Cryptosystem in Quantum Computing Paradigm

Krishna Asawa
Jaypee Institute of Information Technology, India

Akanksha Bhardwaj
Jaypee Institute of Information Technology, India

ABSTRACT

With the emergence of technological revolution to host services over Internet, secure communication over World Wide Web becomes critical. Cryptographic protocols are being in practice to secure the data transmission over network. Researchers use complex mathematical problem, number theory, prime numbers etc. to develop such cryptographic protocols. RSA and Diffie Hellman public key crypto systems have proven to be secure due to the difficulty of factoring the product of two large primes or computing discrete logarithms respectively. With the advent of quantum computers a new paradigm shift on public key cryptography may be on horizon. Since superposition of the qubits and entanglement behavior exhibited by quantum computers could hold the potential to render most modern encryption useless. The aim of this chapter is to analyze the implications of quantum computing power on current public key cryptosystems and to show how these cryptosystems can be restructured to sustain in the new computing paradigm.

INTRODUCTION

Today is an era where a smart phone provides anytime anywhere services and stores personal data, including photos, messages, mails and documents. Instead of files and folders people use icloud, Microsoft one drive, Google cloud as backups. From small start-ups to Microsoft, Google, IBM, AT&T, Amazon store their data in data-centres and cloud. With the emergence of technological revolution to host services over internet, it has resulted in exponential growth of data stored in data-centres and cloud. Storing data in data-centres and cloud entails securing data from thieves, who secede valuable or sensitive data from storage centers and eavesdroppers, who listen or capture data on the communication

DOI: 10.4018/978-1-5225-0058-2.ch027

channel while it travels from provider to user over World Wide Web. Hence secure communication of this data becomes critical.

Cryptography is the collection of techniques to communicate data only to its intended user in presence of third parties. These techniques suggest that before the data enters the communication channel, hide the data using encryption techniques and then on reaching its destination unhide the data using decryption techniques. Hence cryptographic protocols are being in practice to secure the data transmission over network.

Traditionally cryptographic protocols involve use of a secret key, which is agreed upon by the sender and the receiver over a secure channel, to encrypt and decrypt this data. Ramification of this protocol is key distribution problem. To eliminate the use of a single key Diffie and Hellman devised a solution based on the concept given by Merkle(Merkle,1978). Merkle suggestion was to communicate the message over insecure channel by creating a puzzle and encrypting some information in the puzzle such that it requires exponentially more efforts from eavesdropper to solve the puzzle than the receiver.

Since the advent of quantum computing paradigm in 1980's, Richard Feynman and David Duetsch envisioned the massive computing power of quantum systems. Quantum computation provides parallelism because of phenomenal characteristics of quantum physics like superposition and entanglement to perform operations on data. Shor(1994) proposed a quantum algorithm that has severe implication on current classical algorithms for public key cryptography. The traditional cryptosystems are challenged to sustain and provide adequate security. So there is need to replace the existing cryptosystem with new protocols, resistant against the attacks due to quantum computing power. The only solution with us is to either switch to quantum cryptography algorithms or to reformulate the classical cryptosystem resistant to quantum paradigm.

BACKGROUND

Classical Computing Paradigm and Public Key Cryptography

Formally public key cryptography the term was first introduced by Diffie and Hellman (1976) which since then changed the cryptographic landscape forever. They presented a method to allow two parties to communicate and agree on a secret key without transmitting the secret key to each other. It exhibited only a little portion of number theory but motivated various researchers to start looking at applications of number theory and prime number that minimizes the need for secure key distribution channels.

In public key cryptographic protocols communicant secrete two keys, which are mathematically related to each other, and constructed in such a way that it is infeasible to obtain one key with the knowledge of another key. All users in the network generate two keys, public and private key. Public key is known to all while the private key is kept secret. Sender encrypts the data using receiver's public key while the decryption is done by the receiver using his private key. Although Encryption algorithm E is inverse of Decryption algorithm D, where E and D are easy to compute having knowledge of private key, but computationally difficult to derive D from E without the knowledge of private key. Here E is a "trapdoor one way function". One way; as it can be computed easily in one direction, trapdoor as it is infeasible to solve in other direction without the knowledge of trap door.

RSA cryptosystem, proposed by Ron Rivest, Adi Shamir and Len Adleman(1977), Diffie-Hellman key exchange, published by Whitfield Diffie and Martin Hellman(1976) and Elgamal key agreement