Chapter 11
Post-Quantum Cryptography and Quantum Cloning

Amandeep Singh Bhatia
Center for Quantum Computing, Peng Cheng Laboratory, China

Shenggen Zheng
Center for Quantum Computing, Peng Cheng Laboratory, China

ABSTRACT

In the last two decades, the field of post-quantum cryptography has had an overwhelming response among research communities. The ability of quantum computers to factorize large numbers could break many of well-known RSA cryptosystem and discrete log-based cryptosystem. Thus, post-quantum cryptography offers secure alternatives which are implemented on classical computers and is secure against attacks by quantum computers. The significant benefits of post-quantum cryptosystems are that they can be executed quickly and efficiently on desktops, smartphones, and the Internet of Things (IoTs) after some minor software updates. The main objective of this chapter is to give an outline of major developments in privacy protectors to reply to the forthcoming threats caused by quantum systems. In this chapter, we have presented crucial classes of cryptographic systems to resist attacks by classical and quantum computers. Furthermore, a review of different classes of quantum cloning is presented.

INTRODUCTION

In cryptography, several public-key cryptosystems are based on hard problems (not easily tractable on classical computers) such as discrete logarithms and integer factorization. Over the years, number of cryptography algorithms have been introduced and played a crucial role in cybersecurity such as Rivest-Shamir-Adleman (RSA) cryptosystem, Diffie-Hellman key exchange, elliptic curve cryptosystems (ECC) and digital signature algorithm (DSA). Nowadays, quantum computing is an exceptionally hot area of research. The era of quantum computing is nearly upon us, and quantum computers will be able to perform certain operations more quickly and efficiently than classical ones. It is based on quantum mechanical principles of superposition and entanglement. Feynman (1982) stated that the simulation

DOI: 10.4018/978-1-7998-8593-1.ch011

of quantum mechanics was performed on a classical computer. Initially, it was thought to be only a theoretical interest, but now the race to develop a truly useful quantum computer is on among major IT companies and research communities.

Shor (1994) developed a polynomial quantum algorithm which can solve the above intractable problems easily on a quantum computer. As the rapid advancement in quantum computers is catching up, Shor's factorization algorithm will completely end the RSA encryption. It take $O(\log n)$ space complexity and $O(\log n)^2 * \log \log n)$ time on a quantum computer and $O(\log n)$ time on a classical computer to find factors of a large number n. Therefore, current popular public-key cryptosystems can be attacked in polynomial time. Bernstein (2009) shown the status of several present public-key cryptosystems, given in Table 1.

Table 1. The present status of public-key cryptosystems

Cryptosystems	Cracked by Quantum algorithms?
Diffie-Hellman key-exchange by Diffie and Hellman (1976)	Yes
McEliece public-key encryption by McEliece (1978)	No
Algebraically Homomorphic by Rivest et al. (1978)	Yes
RSA public-key encryption by Rivest et al. (1978)	Yes
Algebraically Homomorphic by Rivest et al. (1978)	Yes
Elliptic curve cryptography by Koblitz (1987)	Yes
Buchmann-Williams key-exchange by Buchmann and Williams (1988)	Yes
Lattice-based public-key encryption by Cai and Cusick (1998)	No
NTRU public-key encryption by Hoffstein et al. (1998)	No

Till now, various public-key cryptosystems have been introduced to reply to security concerns with quantum systems in the post-quantum era. Post-quantum cryptography provides secure substitutes. The objective is to unfold different public-key cryptosystems, which can be adaptable to present communication networks and resist the attacks by both classical and quantum computers. Besides, RSA, DSA, and Elliptic curve digital signature algorithm (ECDSA), there exist several crucial classes of cryptographic systems which consist of code-based, hash-based, lattice-based, and multivariate-quadratic-equations. Indeed, Shor's algorithm has not been employed in these classes yet.

Although there exist several challenges for the implementation of the post-quantum algorithms. The requirement is to expand the effectiveness and make practicable these algorithms. Secondly, the time is required to get assuredness in post-quantum algorithms. Recently, Bhatia and Kumar (2019) mentioned that these challenges need to be focused before shifting completely to the post-quantum era. In this chapter, the details of different post-quantum cryptosystems to resist completely every attack are given. Moreover, the various classes of quantum cloning are described.

Basic Notations

In this section, some basic notations and terminologies are given, which will be used in the rest of this chapter.