Chapter 12
Pre-Quantum to Post-Quantum Cryptography Transition:
A Journey Connecting the Security and Challenges Eras

Sayan Das
https://orcid.org/0000-0002-9899-6664
St. Xavier's University, Kolkata, India

Arnav Das
https://orcid.org/0000-0003-3751-3056
India Internet Foundation, Kolkata, India

ABSTRACT

Quantum cryptography is a promising field for securing information against quantum computers. Shor's algorithm, a quantum algorithm, can factor large prime numbers in polynomial time and solve the discrete logarithm problem, which is the basis for classical cryptographic algorithms like Rivest-Shamir-Adleman algorithm (RSA), Diffie-Hellman key exchange (DHKE), and Elliptic Curve Diffie-Hellman algorithm(ECDH). These algorithms pose a significant threat to their security and reliability. Post-quantum cryptography techniques are being implemented by all industries to address the threat posed by quantum supremacy. The chapter discusses the potential threat of Shor's algorithm on classical cryptographic algorithms and discusses post-quantum cryptographic algorithms like lattice-based, multivariate, code-based, and Hash-based cryptography. It also discusses recent advancements that have improved the security and usefulness of these algorithms.

1. INTRODUCTION

With the advent of Quantum Computers and the democratization of access to Quantum hardware, numerous fields have experienced rapid and profound transformations. One domain significantly impacted is Cryptography, which previously relied heavily on mathematical principles. The effects have been so substantial that a clear distinction has emerged between Pre-Quantum and Post-Quantum cryptography. Pre-quantum cryptography included encryption techniques like RSA, a well-known scheme

DOI: 10.4018/979-8-3693-7076-6.ch012

that relies on the difficulty of determining the prime factors of a number. However, the dominant barrier had been eliminated by the emergence and utilization of Quantum Algorithms, making the entire RSA scheme invalid. This made the requirement for Post-Quantum Cryptography very necessary. Pre-Quantum Cryptography encompassed encryption methods such as RSA, a prominent scheme reliant on the inherent difficulty of calculating the prime factors of a number. Post-Quantum Cryptography comprises the development of increasingly sophisticated cryptographic schemes that rely on problems such as lattice theory, which even Quantum Computers find infeasible to solve. This exciting progress ensures the security of cryptographic systems in the face of Quantum Computing advancements. In the field of cryptography, classical cryptographic algorithms have been used for securing communication and data transfer for many years (Abdullah & Azad, 2014). However, with the emergence of quantum computers, the security of these classical cryptographic algorithms is at risk (Samta Gajbhiye et al., 2017). Shor's algorithm (Shor, 1999), introduced by Peter Shor in 1994, represents a pivotal computational advancement, enabling the efficient factorization of large numbers and resolution of the discrete logarithm problem. These mathematical challenges serve as foundational components within numerous classical cryptographic algorithms, including the renowned Rivest-Shamir-Adleman (RSA) (Rivest et al., 1978), the Diffie-Hellman Key Exchange (DHKE) (Diffie & Hellman, 1976), and the Elliptic Curve Diffie-Hellman (ECDH) (Barker et al., 2007) protocol. The considerable apprehension surrounding Shor's algorithm (Shor, 1999), (Shor, 1994) pertains to its potential to undermine classical cryptographic systems. Shor's algorithm capitalizes on the inherent quantum parallelism (superposition) and the ability of quantum computers to perform certain mathematical operations, surpassing their classical counterparts. It represents a significant breakthrough in quantum computing and has the potential to render many existing cryptographic protocols insecure. In response to the looming quantum threat, post-quantum cryptography has emerged as a new field of research. Post quantum cryptographic schemes are meticulously engineered to withstand attacks from both classical and quantum computers. These protective mechanisms based on mathematical conundrums deemed intrinsically complex, even for quantum computers. Exemplary instances encompass lattice-based cryptography (Regev, 2009), code-based cryptography (McEliece, 1978), and hash-based cryptography. While Shor's algorithm on huge primes cannot currently be executed by quantum computers, this may change in the near future. Consequently, it is imperative to scrutinize the resilience of classical cryptographic algorithms against potential quantum threats and to ascertain the ramifications of quantum computers on the security of data transmission and communication. In this chapter, we started with explaining the various commonly used pre-quantum algorithms like RSA, DHKE, and ECDH. We study the components of Shor's Algorithm and the kinds of mathematical problems it can answer in polynomial time, as it presents a challenge to the existing systems, especially RSA. The chapter also highlights different forms of encryption, such as the lattice-based approach, that are resistant to the quantum uprising.

2. BACKGROUND

Classical cryptography, fortified by the complexity of mathematical problems, has long been the cornerstone of secure communication. Algorithms like RSA (Rivest-Shamir Adleman), DHKE (Diffie-Hellman Key Exchange), and ECDH (Elliptic Curve Diffie-Hellman) have stood as stalwart guardians, preserving the sanctity of sensitive information. These cryptographic giants rely on intricate mathematical