Information Security in the Post Quantum Era for IoT

Abstract

With the advent of Quantum computing, more and more emphasis is on developing cyber-physical quantum-safe systems. Information-Theoretic security does not depend upon assumptions of computational hardness. Thus is quantum-safe if a framework is proved to be Information-Theoretic Secure. As networked devices' accessibility becomes more and more ubiquitous, groundbreaking applications of the Internet of Things (IoT) find their place in many aspects of our society. The exploitation of these devices is the main reason for the cyberattacks in IoT networks. Security design is still an open problem and a crucial step in making IoT applications successful. In dicey environments, such as e-health, smart grid, and smart cities, real-time commands must reach the end devices in the scale of milliseconds. Traditional public-key cryptosystem, albeit necessary in the context of general Internet security, falls short in establishing new session keys in the scale of milliseconds for critical messages. In this thesis, we proposed three frameworks that satisfy the cryptographic properties of cyber-physical systems. Firstly, a Blockchain User Authentication using zk-SNARKS is proposed to authenticate nodes wanted to join a network using a decentralized mechanism. Secondly, an information-theoretic key generation mechanism is proposed based on packet erasures and error correction codes. Thirdly, an information-theoretic secure message routing algorithms in software-defined networks (SDN) is proposed. The information-theoretic security of the latter two schemes is proved under the adversarial model. Our experimental results demonstrate our keystream generation's efficiency and Shamir's secret sharing (SSS)-based protocols and the validity of our mechanism design.

Keywords: *Information-Theoretic Security, Quantum, cyber, key stream, blockchain*

Ali