Lattice-based cryptography: the dots that provide information security

ABSTRACT

Since the novel discovery of Shor's quantum algorithm, current interest in cryptography is moving towards a new direction called Post-Quantum Cryptography. Once quantum computing technology is ready to be deployed effectively, the Shor's quantum algorithm would become a major threat on number-theoretical based cryptosystems that are widely used today such as the RSA, ElGamal, and Elliptic Curve cryptosystems. Alternatively, most of the current cryptographic schemes are developed based on hard mathematical problems believed to be as unaffected by Shor's quantum algorithm. One of the alternatives is lattice-based cryptography. 2-dimensional lattices could be represented pictorially as group of dots in periodic order. By manipulating the mathematical concept behind the lattices, these dots are surprisingly able to provide information security through cryptography. In this paper, the mathematical foundation regarding lattices will be discussed while the formation of hard-mathematical problems based on lattices will be emphasized. Then, several established lattice-based cryptosystems will be introduced, including our newly improved lattice-based cryptosystem named as GGH-MKA cryptosystem. On top of that, some further development of the scheme will also be proposed.