Attribute-based encryption in securing big data from post-quantum perspective: A survey

ABSTRACT

Attribute-based encryption (ABE) cryptography is widely known for its potential to solve the scalability issue of recent public key infrastructure (PKI). It provides a fine-grained access control system with high flexibility and efficiency by labeling the secret key and ciphertext with distinctive attributes. Due to its fine-grained features, the ABE scheme is a protection layer in securing users' data and privacy in big data processing and analytics. However, quantum computing, new technology on the horizon that will transform the security and privacy environment, has begun to appear. Like the conventional ABE schemes, present cryptography is not excluded from the impacts of quantum technology as they are not made to be quantum-resistant. While most recent surveys generally touched on the generic features of attribute-based encryption schemes such as user revocation, scalability, flexibility, data confidentiality, and scope in pairing-based ABE schemes, this survey investigated quantum-resistant ABE schemes in securing big data. This survey reviews the challenges faced by the recent ABE cryptography in the post-quantum era and highlights its differences from the conventional pairing-based ABE schemes. Subsequently, we defined the criteria of an ideal quantum-resistant ABE scheme. Additionally, existing works on quantum-resistant ABE schemes are reviewed based on their algorithms design, security and functionalities. Lastly, we summarized quantum-resistant ABE schemes' ongoing challenges and future works.