ABSTRACT OF THE DISCLOSURE

BLINDING TECHNIQUES FOR POST-QUANTUM PUBLIC KEYS

Blinding techniques can be used to obfuscate or otherwise modify a quantum-secure public key (and the corresponding private, or secret, key) such as a lattice-based public key. Blinding of a public key can include selecting a blinding parameter, which can be a vector or matrix, and applying the blinding parameter to the public key. A corresponding modification can be applied to the private key such that data encrypted using the blinded public key can be decrypted using the blinded public key. When a device needs to send a public key in the clear, e.g., in the course of establishing a secure communication session, the device can generate a blinded public key from its static public key and send the blinded key instead of the static public key.

FIG. 7