compromise of data, such as through key exhaustion. An encryption key is exhausted and thus exposed when it is used more times than it should be used because overuse of an encryption key can result in revealing information about the underlying plaintext or the secret values in the encryption key itself.

[0007] Furthermore, key rotation can be used to revoke old encryption keys, for example, that might have been compromised or to revoke data access, because once an encryption key has been replaced by a new encryption key, the older encryption key cannot access the data.

[0008] Accordingly, there is a need in the art for methods of key rotation for encryption key materials.

SUMMARY

[0009] A first aspect of the present disclosure provides a method for key rotation of an encryption key, including: generating a first ciphertext by encrypting a plaintext with a homomorphic probabilistic encryption scheme based on a first key; generating an updating token based on a difference between the homomorphic probabilistic encryption scheme based on the first key and the homomorphic probabilistic encryption scheme based on a second key; and generating a second ciphertext by encrypting the first ciphertext with the updating token.

[0009a] A second aspect of the present disclosure provides a method for verifiable key rotation of an encryption key, including: generating a first ciphertext by encrypting a plaintext with a homomorphic probabilistic encryption scheme based on a first key; generating an updating token based on a difference between the homomorphic probabilistic encryption scheme based on the first key and a homomorphic probabilistic encryption scheme based on a second key; generating a second ciphertext by encrypting the first ciphertext with the updating token; selecting a set of second ciphertext blocks from the second ciphertext; reverting the set of second ciphertext blocks with the updating token to a set of third ciphertext blocks; computing a Hamming distance between blocks of the set of second ciphertext blocks and the corresponding set of third ciphertext blocks; and in response to determining the Hamming distance is less than a threshold, validating the second ciphertext; and replacing the first key with the second key as the encryption key for the plaintext.

[0010] A third aspect of the present disclosure provides a processing system configured to perform the aforementioned methods as well as those described herein; non-transitory, computer-readable media comprising instructions that, when executed by a

processor of a processing system, cause the processing system to perform the aforementioned methods as well as those described herein; a computer program product embodied on a computer-readable storage medium comprising code for performing the aforementioned methods as well as those further described herein; and a processing system comprising means for performing the aforementioned methods as well as those further described herein.

[0011] The following description and the related drawings set forth in detail certain illustrative features of one or more aspects.

DESCRIPTION OF THE DRAWINGS

[0012] The appended figures depict certain aspects and are therefore not to be considered limiting of the scope of this disclosure.

[0013] **FIG. 1** depicts an example process flow for performing key rotation.