

CLAIMS

What is claimed is:

1. A method for encrypting an object such that the creator of the encrypted object can be identified comprising:

receiving, by a processor, an unencrypted object that comprises plaintext and metadata that describes the plaintext;

obtaining, by the processor in response to a request from a user, a data encryption key (DEK) and a nonce key for the unencrypted object, the nonce key being unique to the user;

encrypting, by the processor, the unencrypted object, the encrypting comprising:

generating a nonce based at least in part of the plaintext and the nonce key; and

generating ciphertext and a metadata authentication tag comprising a signature of the metadata, the generating based at least in part on the plaintext, the metadata, the DEK, and the nonce; and

creating an encrypted object that includes the ciphertext, the metadata, and the metadata authentication tag.

2. The method of claim 1, wherein the nonce is generated once, and in response to the encrypted object being created the nonce is linked to the encrypted object via a pointer to the nonce in the encrypted object or linked to the encrypted object via inclusion of the nonce in the encrypted object.

3. The method of claim 1, wherein the generating the nonce comprises executing a nonce encryption algorithm that takes as input the plaintext and the nonce key, and that outputs the nonce.

4. The method of claim 3, wherein the nonce encryption algorithm is an Advanced Encryption Standard with Cipher-based Message Authentication Code (AES-CMAC) encryption algorithm.

5. The method of claim 1, wherein a plurality of nonce keys correspond to the DEK and the nonce key is included in the plurality of nonce keys.

6. The method of claim 1, wherein the encrypting the unencrypted object is performed using an Advanced Encryption Standard with Galois/Counter Mode (AES-GCM) encryption algorithm.

7. The method of claim 1, further comprising:

receiving, by the processor, a second encrypted object, the second encrypted object having been previously generated by encrypting a second object based at least in part on the DEK and a second nonce;

obtaining a plurality of nonce keys correspond to the DEK, wherein each of the plurality of nonce keys corresponds to a specific user;

obtaining a copy of a second unencrypted object corresponding to the second encrypted object;

creating a plurality of nonces, each of the plurality of nonces being created using one of the plurality of nonce keys;

determining that one of the plurality of nonces that matches the second nonce and identifying the specific user associated with nonce key used to generate the one of the plurality of nonces as the creator of the second encrypted object.

8. The method of claim 7, wherein obtaining the copy of a second unencrypted object includes decrypting the second encrypted object using the DEK and the second nonce.

9. A system comprising:

one or more processors for executing computer-readable instructions, the computer-readable instructions controlling the one or more processors to perform operations comprising:

receiving an unencrypted object that comprises plaintext and metadata that describes the plaintext;

obtaining, in response to a request from a user, a data encryption key (DEK) and a nonce key for the unencrypted object, the nonce key being unique to the user;

encrypting the unencrypted object, the encrypting comprising:

generating a nonce based at least in part of the plaintext and the nonce key; and

generating ciphertext and a metadata authentication tag comprising a signature of the metadata, the generating based at least in part on the plaintext, the metadata, the DEK, and the nonce; and

creating an encrypted object that includes the ciphertext, the metadata, and the metadata authentication tag.

10. The system of claim 9, wherein the nonce is generated once, and in response to the encrypted object being created the nonce is linked to the encrypted object via a pointer to the nonce in the encrypted object or linked to the encrypted object via inclusion of the nonce in the encrypted object.

11. The system of claim 9, wherein the generating the nonce comprises executing a nonce encryption algorithm that takes as input the plaintext and the nonce key, and that outputs the nonce.

12. The system of claim 11, wherein the nonce encryption algorithm is an Advanced Encryption Standard with Cipher-based Message Authentication Code (AES-CMAC) encryption algorithm.

13. The system of claim 9, wherein a plurality of nonce keys correspond to the DEK and the nonce key is included in the plurality of nonce keys.

14. The system of claim 9, wherein the encrypting the unencrypted object is performed using an Advanced Encryption Standard with Galois/Counter Mode (AES-GCM) encryption algorithm.

15. The system of claim 9, wherein the operations further comprise:

receiving, by the processor, a second encrypted object, the second encrypted object having been previously generated by encrypting a second object based at least in part on the DEK and a second nonce;

obtaining a plurality of nonce keys correspond to the DEK, wherein each of the plurality of nonce keys corresponds to a specific user;

obtaining a copy of a second unencrypted object corresponding to the second encrypted object;

creating a plurality of nonces, each of the plurality of nonces being created using one of the plurality of nonce keys;

determining that one of the plurality of nonces that matches the second nonce and identifying the specific user associated with nonce key used to generate the one of the plurality of nonces as the creator of the second encrypted object.

16. The system of claim 15, wherein obtaining the copy of a second unencrypted object includes decrypting the second encrypted object using the DEK and the second nonce.

17. A computer program product comprising a computer-readable storage medium having program instructions embodied therewith, the program instructions executable by a processor to cause the processor to perform operations comprising:

receiving an unencrypted object that comprises plaintext and metadata that describes the plaintext;

obtaining, in response to a request from a user, a data encryption key (DEK) and a nonce key for the unencrypted object, the nonce key being unique to the user;

encrypting the unencrypted object, the encrypting comprising:

generating a nonce based at least in part of the plaintext and the nonce key; and

generating ciphertext and a metadata authentication tag comprising a signature of the metadata, the generating based at least in part on the plaintext, the metadata, the DEK, and the nonce; and

creating an encrypted object that includes the ciphertext, the metadata, and the metadata authentication tag.

18. The computer program product of claim 17, wherein the nonce is generated once, and in response to the encrypted object being created the nonce is linked to the encrypted object via a pointer to the nonce in the encrypted object or linked to the encrypted object via inclusion of the nonce in the encrypted object.

19. The computer program product of claim 17, wherein the generating the nonce comprises executing a nonce encryption algorithm that takes as input the plaintext and the nonce key, and that outputs the nonce.
20. The computer program product of claim 19, wherein the nonce encryption algorithm is an Advanced Encryption Standard with Cipher-based Message Authentication Code (AES-CMAC) encryption algorithm.