

WHAT IS CLAIMED IS:

1 1. A method comprising performing, by a computer system:
2 generating a commitment using a message and a random value;
3 transmitting a request including the commitment to each of a plurality of
4 cryptographic devices that store a plurality of secret shares that are generated from a secret
5 value and a plurality of verification shares generated from a verification value, wherein
6 contents of the request provide an indication, to each of the plurality of cryptographic
7 devices, that each of the plurality of cryptographic devices is to perform a cryptographic
8 function corresponding to encryption;
9 receiving from the plurality of cryptographic devices, a plurality of partial
10 computations, wherein the plurality of partial computations were generated by the plurality of
11 cryptographic devices using the plurality of secret shares and the commitment;
12 receiving, from the plurality of cryptographic devices, a plurality of partial
13 signatures, wherein the plurality of partial signatures were generated based on the indication
14 in the request that each of the plurality of cryptographic devices is to perform the
15 cryptographic function corresponding to the encryption, by the plurality of cryptographic
16 devices using the plurality of verification shares and the commitment;
17 generating a cryptographic key based on the plurality of partial computations;
18 generating a verification signature based on the plurality of partial signatures;
19 generating a ciphertext by encrypting the message and the random value using
20 the cryptographic key; and
21 generating a payload comprising the ciphertext, the verification signature, and
22 the commitment.

1 2. The method of claim 1, wherein:
2 transmitting the commitment to the plurality of cryptographic devices
3 comprises transmitting the commitment to a proxy device, wherein the proxy device
4 transmits the commitment to the plurality of cryptographic devices;
5 receiving the plurality of partial computations from the plurality of
6 cryptographic devices comprises receiving, from the proxy device, the plurality of partial
7 computations, wherein the proxy device receives the plurality of partial computations from
8 the plurality of cryptographic devices; and

receiving the plurality of partial signatures from the plurality of cryptographic devices comprises receiving, from the proxy device, the plurality of partial signatures, wherein the proxy device receives the plurality of partial signatures from the plurality of cryptographic devices.

3. The method of claim 1, wherein the plurality of cryptographic devices comprises at least a predetermined threshold number of cryptographic devices, and wherein the predetermined threshold number of cryptographic devices is less than a total number of cryptographic devices.

4. The method of claim 1, wherein generating the cryptographic key based on the plurality of partial computations comprises:
generating a key generation seed based on the plurality of partial computations; and
generating the cryptographic key by using the key generation seed as an input to a key generation function.

5. The method of claim 1, wherein generating the commitment comprises generating a hash value of the message and the random value using a hash function.

6. The method of claim 1, further comprising selecting the plurality of cryptographic devices from a network of cryptographic devices.

7. The method of claim 1, further comprising:
transmitting the verification signature and the commitment to a plurality of additional cryptographic devices, wherein the plurality of additional cryptographic devices verify the verification signature using a verification key and the commitment;
receiving a plurality of additional partial computations, wherein the plurality of additional partial computations were generated by the plurality of additional cryptographic devices using a plurality of additional secret shares and the commitment;
generating a second cryptographic key based on the plurality of additional partial computations; and
decrypting the ciphertext using the second cryptographic key to produce the message and the random value.

1 8. The method of claim 7, wherein one or more cryptographic devices of
2 the plurality of cryptographic devices are the same as one or more additional cryptographic
3 devices of a plurality of additional cryptographic devices, wherein one or more secret shares
4 of the plurality of secret shares are the same as one or more additional secret shares of a
5 plurality of additional secret shares.

1 9. A method comprising performing, by a computer system:
2 transmitting a request comprising a verification signature and a commitment to
3 a plurality of cryptographic devices, wherein the plurality of cryptographic devices verify the
4 verification signature using a verification key and the commitment;
5 receiving a plurality of partial computations, wherein the plurality of partial
6 computations were generated by the plurality of cryptographic devices using a plurality of
7 secret shares and the commitment;
8 generating a cryptographic key based on the plurality of partial computations;
9 and
10 decrypting a ciphertext using the cryptographic key to produce a message and
11 a random value.

1 10. The method of claim 9, wherein the verification signature indicates to
2 the plurality of cryptographic devices that the computer system intends to perform
3 decryption, and wherein the plurality of cryptographic devices verify the verification
4 signature by:
5 decrypting the verification signature using a verification key to produce an
6 additional commitment; and
7 determining if the additional commitment is the same as the commitment.

1 11. The method of claim 9, further comprising transmitting an indicator to
2 the plurality of cryptographic devices, wherein the indicator indicates to the plurality of
3 cryptographic devices that the computer system intends to perform decryption.

1 12. The method of claim 9, wherein:
2 transmitting the commitment to the plurality of cryptographic devices
3 comprises transmitting the commitment to a proxy device, wherein the proxy device
4 transmits the commitment to the plurality of cryptographic devices;

transmitting the verification signature to the plurality of cryptographic devices comprises transmitting the verification signature to the proxy device, wherein the proxy device transmits the verification signature to the plurality of cryptographic devices; and receiving the plurality of partial computations from the plurality of cryptographic devices comprises receiving, from the proxy device, the plurality of partial computations, wherein the proxy device receives the plurality of partial computations from the plurality of cryptographic devices.

13. The method of claim 9, wherein the plurality of cryptographic devices comprises at least a predetermined threshold number of cryptographic devices, wherein the predetermined threshold number of cryptographic devices is less than a total number of cryptographic devices.

14. The method of claim 9, wherein generating the cryptographic key based on the plurality of partial computations comprises:
generating a key generation seed based on the plurality of partial computations; and
generating the cryptographic key by using the key generation seed as an input to a key generation function.

15. The method of claim 9, further comprising selecting the plurality of cryptographic devices from a network of cryptographic devices.

16. A method comprising performing, by a cryptographic device:
receiving from a client computer, a request including a commitment generated using a message and a random value, wherein contents of the request provide an indication, to the cryptographic device, whether the client computer is to encrypt the message or to decrypt the message;
determining that the client computer intends to encrypt the message based on the contents of the request;
generating a partial computation based on a secret share and the commitment;
generating a partial signature based on a verification share and the commitment; and
transmitting the partial computation and the partial signature to the client computer, thereby enabling the client computer to: (1) generate a cryptographic key using

13 the partial computation, (2) encrypt the message using the cryptographic key, thereby
14 generating a ciphertext, (3) generate a verification signature using the partial signature, and
15 (4) generate a payload comprising the ciphertext, the verification signature, and the
16 commitment.

1 17. The method of claim 16, further comprising, prior to receiving the
2 request from the client computer, receiving the secret share from a trusted external server,
3 wherein the trusted external server also transmits one or more other secret shares to one or
4 more other cryptographic devices.

1 18. The method of claim 16, further comprising:
2 receiving from the client computer, the verification signature and the
3 commitment;
4 determining based on the verification signature and the commitment, that the
5 client computer intends to decrypt the message;
6 verifying the verification signature using a verification key and the
7 commitment;
8 generating the partial computation based on the commitment and the secret
9 share; and
10 transmitting the partial computation to the client computer, wherein the client
11 computer uses the partial computation to generate the cryptographic key and uses the
12 cryptographic key to decrypt the ciphertext to produce the message and the random value.

1 19. The method of claim 18, wherein verifying the verification signature
2 using the verification key and the commitment comprises:
3 decrypting the verification signature using the verification key to produce an
4 additional commitment; and
5 comparing the commitment to the additional commitment.

1 20. The method of claim 18, further comprising:
2 receiving, from the client computer, an indicator indicating that the client
3 computer intends to decrypt the message; and
4 recording that the client computer intends to decrypt the message in a log file.

21. A system comprising:
one or more processors; and

a computer readable medium storing a plurality of instructions that, when executed, cause the one or more processors to perform the method of any one of claims 1-20.