WHAT IS CLAIMED IS:

1. A method comprising performing, by a computer system:

generating a first commitment using a message and a first hash function;

generating a second commitment using the message and a second hash function;

transmitting a request including the first commitment and the second commitment to each of a plurality of cryptographic devices, the plurality of cryptographic devices storing a first plurality of secret shares that are generated from a first secret value and a second plurality of secret shares that are generated from a second secret value;

receiving, from the plurality of cryptographic devices, a plurality of partial computations, wherein each partial computation of the plurality of partial computations was generated by a respective one of the plurality of cryptographic devices using a respective first partial computation and a respective second partial computation, wherein the respective first partial computation is generated using a respective first secret share and the first commitment, and wherein the respective second partial computation is generated using a respective second secret share and the second commitment;

generating a cryptographic key based on the plurality of partial computations;

generating a ciphertext by encrypting the message using the cryptographic key; and

generating a payload comprising the ciphertext, the first commitment, and the second commitment.

2. The method of claim 1, wherein the payload additionally comprises a verification signature, and further comprising:

receiving, from the plurality of cryptographic devices, a plurality of partial signatures, wherein each partial signature of the plurality of partial signatures was generated by a respective one of the plurality of cryptographic devices using a respective verification share of a plurality of verification shares and the first commitment and/or the second commitment; and

generating the verification signature based on the plurality of partial signatures.

3. The method of claim 1, further comprising, after receiving the plurality of partial computations from the plurality of cryptographic devices:

retrieving a plurality of check values, the plurality of check values corresponding to the plurality of partial computations; and

verifying the plurality of partial computations using the plurality of check values.

4. The method of claim 1, wherein:

generating the first commitment using the message and the first hash function additionally comprises using a random value;

generating the second commitment using the message and the second hash function additionally comprises using the random value; and

generating a ciphertext by encrypting the message using the cryptographic key comprises generating a ciphertext by encrypting the message and the random value using the cryptographic key.

5. The method of claim 1, further comprising, prior to generating the first commitment and the second commitment:

randomly selecting the first hash function and the second hash function from a plurality of hash functions.

6. The method of claim 1, wherein:

transmitting the first commitment and the second commitment to the plurality of cryptographic devices comprises transmitting the first commitment and the second commitment to a proxy device, wherein the proxy device transmits the first commitment and the second commitment 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.

7. 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.

8. The method of claim 1, wherein generating the cryptographic key based on the plurality of partial computations comprises:

exponentiating each partial computation of the plurality of partial computations using a respective Lagrange coefficient, thereby generating a plurality of intermediate computations;

calculating a product of the plurality of intermediate computations; and

generating the cryptographic key based on the product of the plurality of intermediate computations.

9. The method of claim 1, further comprising:

transmitting the first commitment and the second commitment to each of a plurality of additional cryptographic devices, the plurality of additional cryptographic devices storing a third plurality of secret shares that are generated from the first secret value and a fourth plurality of secret shares that are generated from the second secret value;

receiving, from the plurality of additional cryptographic devices, a plurality of additional partial computations, wherein each of the plurality of additional partial computations was generated by a respective one of the plurality of additional cryptographic devices using a respective third partial computation and a respective fourth partial computation, wherein the respective third partial computation is generated using a respective third secret share and the first commitment, and wherein the respective fourth partial computation is generated using a respective fourth secret share and the second commitment.

generating the cryptographic key based on the additional plurality of partial computations; and

decrypting the ciphertext using the cryptographic key to produce the message.

10. The method of claim 9, wherein:

one or more cryptographic devices of the plurality of cryptographic devices are the same as one or more additional cryptographic devices of the plurality of additional cryptographic devices;

one or more first secret shares of the first plurality of secret shares are the same as one or more fourth secret shares of the fourth plurality of secret shares; and

one or more second secret shares of the second plurality of secret shares are the same as one or more fourth secret shares of the fourth plurality of secret shares.

11. A method comprising performing, by a computer system:

receiving a payload comprising a ciphertext, a first commitment, and a second commitment;

transmitting a request including the first commitment and the second commitment to each of a plurality of cryptographic devices, the plurality of cryptographic devices storing a first plurality of secret shares that are generated from a first secret value and a second plurality of secret shares that are generated from a second secret value;

receiving, from the plurality of cryptographic devices, a plurality of partial computations, wherein each partial computation of the plurality of partial computations was generated by a respective one of the plurality of cryptographic devices using a respective first partial computation and a respective second partial computation, wherein the respective first partial computation is generated using a respective first secret share and the first commitment, and wherein the respective second partial computation is generated using a respective second secret share and the second commitment;

generating a cryptographic key based on the plurality of partial computations; and

decrypting the ciphertext using the cryptographic key to produce a message.

12. The method of claim 11, wherein:

the payload additionally comprises a verification signature;

the request additionally comprises the verification signature; and

the plurality of cryptographic devices verify the verification signature using a verification key, the first commitment and/or the second commitment.

13. The method of claim 11, wherein the first commitment was generated using the message and a first hash function, wherein the second commitment was generated using the message and a second hash function, wherein the payload additionally comprises a hash indicator and wherein the method further comprises:

determining the first hash function and the second hash function using the hash indicator;

generating a third commitment using the message and the first hash function;

generating a fourth commitment using the message and the second hash function; and

verifying the message by comparing the first commitment to the third commitment and comparing the second commitment to the fourth commitment.

14. The method of claim 13, wherein:

the first commitment was generated using a random value in addition to the message and the first hash function;

the second commitment was generated using the random value in addition to the message and the second hash function;

the third commitment is generated using the random value in addition to the message and the first hash function; and

the fourth commitment is generated using the random value in addition to the message and the second hash function.

15. A method comprising performing, by a cryptographic device:

receiving, from a client computer, a request including a first commitment generating using a message and a first hash function, and a second commitment generated using the message and a second hash function;

generating a first partial computation based on a first secret share and the first commitment;

generating a second partial computation based on a second secret share and the second commitment;

generating a partial computation by combining the first partial computation and the second partial computation; and

transmitting the partial computation to the client computer, thereby enabling the client computer to: (1) generate a cryptographic key using the partial computation, (2) encrypt the message using the cryptographic key, thereby generating a ciphertext, and (3) generate a payload comprising the ciphertext, the first commitment, and the second commitment.

16. The method of claim 15, further comprising, prior to receiving the request from the client computer, receiving the first secret share and the second secret share from a trusted external server, wherein the trusted external server also transmits one or more other secret shares to one or more other cryptographic devices.

17. The method of claim 15, further comprising:

generating a partial signature based on the first commitment and/or the second commitment, and a verification share; and

transmitting the partial signature to the client computer, thereby enabling the client computer to generate a verification signature using the partial signature.

18. The method of claim 17, further comprising:

receiving, from the client computer, the verification signature, the first commitment, and the second commitment;

verifying the verification signature using a verification key and the first commitment and/or the second commitment;

generating the first partial computation based on the first commitment and the first secret share;

generating the second partial computation based on the second commitment and the second secret share;

generating the partial computation by combining the first commitment and the second commitment; and

transmitting the partial computation to the client computer, wherein the client computer uses the partial computation to generate the cryptographic key and uses the cryptographic key to decrypt the ciphertext to produce the message.

19. The method of claim 18, wherein verifying the verification signature using the verification key and the first commitment and/or second commitment comprises:

decrypting the verification signature using the verification key to produce an additional commitment; and

comparing the additional commitment to the first commitment, the second commitment, and/or a combination thereof.

20. The method of claim 18, further comprising:

receiving, from the client computer, an indicator indicating that the client computer intends to decrypt the message; and

recording that the client computer intends to decrypt the message in a log file.

21. A computer system comprising:

a processor; and

a non-transitory computer readable medium coupled to the processor, the non-transitory computer readable medium comprising code, executable by the processor for implementing the method of any one of claims 1-20.