WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a second computer node, a second key share from a key management computer;

receiving, by the second computer node, an initial message from a first computer node;

generating, by the second computer node, a second garbled circuit, a garbled second key share based on the second key share and the second garbled circuit, and a garbled message based on the initial message and the second garbled circuit; and

transmitting, by the second computer node to a third computer node, the second garbled circuit, the garbled second key share, and the garbled message, wherein the third computer node also receives, from the first computer node, a garbled first key share based on a first key share stored at the first computer node and a first garbled circuit,

which causes the third computer node to generate a subsequent message by inputting the first garbled key share, the second garbled key share, and the garbled message into either the first garbled circuit or the second garbled circuit, and transmit the subsequent message to the first computer node, wherein the first computer node transmits the subsequent message or a derivative thereof to a client computer.

2. The method of claim 1, wherein the garbled message is a second garbled message and wherein the third computer node also receives from the first computer node, a first garbled message based on the initial message and the first garbled circuit.

3. The method of claim 1, wherein receiving, by the second computer node, the second key share from the key management computer comprises:

retrieving, by the second computer node, the second key share from a second key share database, wherein the key management computer transmitted the second key share to the second key share database.

4. The method of claim 1, wherein the second computer node receives the second key share from the key management computer via a proxy.

5. The method of claim 1, wherein the initial message additionally comprises information about a requested operation, the information about the requested operation indicating whether the initial message should be encrypted or decrypted by the first computer node, the second computer node, and the third computer node.

6. The method of claim 1, wherein the key management computer generated the second key share from a key stored in a hardware security module.

7. The method of claim 1, further comprising:

storing, by the second computer node, the second key share in a secure memory element associated with the second computer node.

8. The method of claim 1, wherein, prior to receiving, by the second computer node, the second key share from the key management computer, the key management

computer verifies or authenticates the second computer node using a certificate corresponding to the second computer node.

9. The method of claim 1, wherein the initial message is ciphertext and the subsequent message or the derivative thereof is plaintext.

10. A second computer node 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 a method comprising:

receiving a second key share from a key management computer;

receiving an initial message from a first computer node;

generating a second garbled circuit, a garbled second key share based on the second key share and the second garbled circuit, and a garbled message based on the initial message and the second garbled circuit; and

transmitting to a third computer node, the second garbled circuit, the garbled second key share, and the garbled message, wherein the third computer node also receives, from the first computer node, a garbled first key share based on a first key share stored at the first computer node and a first garbled circuit,

which causes the third computer node to generate a subsequent message by inputting the first garbled key share, the second garbled key share, and the garbled message into either the first garbled circuit or the second garbled circuit, and transmit the subsequent message to the first computer node, wherein the first computer node transmits the subsequent message or a derivative thereof to a client computer.

11. The second computer node of claim 10, wherein the garbled message is a second garbled message and wherein the third computer node also receives from the first computer node, a first garbled message based on the initial message and the first garbled circuit.

12. The second computer node of claim 10, wherein receiving the second key share from the key management computer comprises:

retrieving the second key share from a second key share database, wherein the key management computer transmitted the second key share to the second key share database.

13. The second computer node of claim 10, wherein the second computer node receives the second key share from the key management computer via a proxy.

14. The second computer node of claim 10, wherein the initial message additionally comprises information about a requested operation, the information about the requested operation indicating whether the initial message should be encrypted or decrypted by the first computer node, the second computer node, and the third computer node.

15. The second computer node of claim 10, wherein the key management computer generated the second key share from a key stored in a hardware security module.

16. The second computer node of claim 10, wherein the second computer node additionally comprises a secure memory element, and wherein the method further comprises:

storing the second key share in the secure memory element.

17. The second computer node of claim 10, wherein in the method, prior to receiving the second key share from the key management computer, the key management computer verifies or authenticates the second computer node using a certificate corresponding to the second computer node.

18. A third computer node 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 a method comprising:

receiving, from a first computer node, a first garbled circuit, a garbled first key share, and a first garbled message;

receiving, from a second computer node, a second garbled circuit, a garbled second key share, and a second garbled message;

generating, by the third computer node, a subsequent message by inputting the first garbled key share, the second garbled key share and the first or second garbled message into either the first garbled circuit or the second garbled circuit; and

transmitting the subsequent message to the first computer node.

19. The third computer node of claim 18, wherein the method further comprises:

verifying that the first garbled circuit and the second garbled circuit match and that the first garbled message and the second garbled message match.

20. The third computer node of claim 18, wherein:

verifying that the first garbled circuit and the second garbled circuit match comprises performing a bitwise or bytewise comparison of first garbled circuit data corresponding to the first garbled circuit and second garbled circuit data corresponding to the second garbled circuit; and

verifying that the first garbled message and the second garbled message match comprises performing a bitwise comparison or bytewise comparison of first garbled message data corresponding to the first garbled message and second garbled message data corresponding to the second garbled message.