

WHAT IS CLAIMED IS:

1 ————— 1. ——— A method comprising:—
2 ————— receiving, by a first computer node, a first key share from a key
3 — management computer;—
4 ————— receiving, by the first computer node, an initial message from a client
5 — computer;—
6 ————— transmitting, by the first computer node, the initial message to a second
7 — computer node;—
8 ————— generating, by the first computer node, a garbled circuit, a garbled first key
9 — share based on the first key share and the garbled circuit, and a garbled message
10 — based on the initial message and the garbled circuit;—
11 ————— transmitting, by the first computer node to a third computer node, the
12 — garbled circuit, the garbled first key share, and the garbled message, wherein the third
13 — computer node also receives, from the second computer node, a garbled second key
14 — share based on a second key share stored at the second computer node and the
15 — garbled circuit,—
16 ————— which causes the third computer node to generate a subsequent message
17 — by inputting the first garbled key share, the second garbled key share, and the garbled
18 — message to the garbled circuit, and transmit the subsequent message to the first
19 — computer node; and
20 ————— transmitting, by the first computer node, the subsequent message or a
21 — derivative thereof to the client computer.

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

- 1 ————— 3. — The method of claim 2, wherein the third computer node
2 — determines that the first garbled circuit and the second garbled circuit match and the
3 — first garbled message and second garbled message match.
- 1 ————— 4. — The method of claim 1, further comprising:
2 — generating, by the first computer node, an ungarbled subsequent
3 — message based on the subsequent message and the garbled circuit.
- 1 ————— 5. — The method of claim 1, wherein the initial message is plaintext and
2 — the subsequent message or the derivative thereof is ciphertext.
- 1 ————— 6. — The method of claim 1, wherein the key management computer
2 — generated the first key share from a key stored in a hardware security module.
- 1 ————— 7. — The method of claim 1, wherein the key management computer
2 — forms the first key share and the second key share.
- 1 ————— 8. — The method of claim 1, wherein the first computer node, the second
2 — computer node, and the third computer node are all present at a same premises.
- 1 ————— 9. — The method of claim 1, wherein the first computer node, second
2 — computer node, and third computer node are part of a distributed computing network.
- 1 ————— 10. — A first computer node comprising:
2 — a processor; and
3 — a non-transitory computer readable medium coupled to the processor, the
4 — non-transitory computer readable medium comprising code, executable by the
5 — processor, for implementing a method comprising:
6 — receiving a first key share from a key management computer;
7 — receiving an initial message from a client computer;
8 — transmitting the initial message to a second computer node;
9 — generating a garbled circuit, a garbled first key share based on the first
10 — key share and the garbled circuit, and a garbled message based on the initial message
11 — and the garbled circuit;

transmitting to a third computer node, the garbled circuit, the garbled first key share, and the garbled message, wherein the third computer node also receives, from the second computer node, a garbled second key share based on a second key share stored at the second computer node and the 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 to the garbled circuit, and transmit the subsequent message to the first computer node; and transmitting the subsequent message or a derivative thereof to the client computer.

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

12. The first computer node of claim 11, wherein the third computer node determines that the first garbled circuit and the second garbled circuit match and that the first garbled message and the second garbled message match.

13. The first computer node of claim 10, wherein the method further comprises: generating an ungarbled subsequent message based on the subsequent message and the garbled circuit.

14. The first computer node of claim 10, wherein the initial message is plaintext and the subsequent message or the derivative thereof is ciphertext.

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

1 16. The first computer node of claim 10, wherein the key management
2 computer formed the first key share and the second key share.

1 17. The first computer node of claim 10, wherein the first computer
2 node, the second computer node, and the third computer node are all present at a same
3 premises.

1 18. A method comprising:
2 receiving, by a third computer node, from a first computer node, a first
3 garbled circuit, a garbled first key share, and a first garbled message;
4 receiving, by the third computer node, from a second computer node, a
5 second garbled circuit, a garbled second key share and a second garbled message;
6 generating, by the third computer node, a subsequent message by
7 inputting the first garbled key share, the second garbled key share, and the first or the
8 second garbled message to the first or the second garbled circuit; and
9 transmitting, by the third computer node, the subsequent message to the
10 first computer node.

1 19. The method of claim 18, further comprising verifying, by the third
2 computer node, that the first garbled circuit and the second garbled circuit match and
3 that the first garbled message and the second garbled message match.

1 20. The method of claim 18, wherein the first computer node ungarbles
2 the subsequent message and transmits the subsequent message to a client computer.

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.