

WHAT IS CLAIMED IS:

1 1. A method comprising:
2 receiving, by a first computer node in a distributed-computing network, a
3 first key share from a key management computer in an on-premises zone;
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 in the distributed-computing network;
8 generating, by the first computer node, a first garbled circuit, a garbled first
9 key share based on the first key share and the first garbled circuit, and a garbled
10 message based on the initial message and the first garbled circuit;
11 transmitting, by the first computer node to a third computer node in the
12 distributed-computing network, the first garbled circuit, the garbled first key share, and
13 the garbled message, wherein the third computer node also receives, from the second
14 computer node, a garbled second key share based on a second key share stored at the
15 second computer node and ~~the a second~~ 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 into either the first garbled circuit or the second garbled circuit ~~to the garbled~~
19 ~~circuit~~, and transmit the subsequent message to the first 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 the 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 first 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.~~

1 409. 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 in a distributed-computing network a first key share from a key
7 management computer in an on-premises zone;
8 receiving an initial message from a client computer;
9 transmitting the initial message to a second computer node in the
10 distributed-computing network;

11 generating a first garbled circuit, a garbled first key share based on the
12 first key share and the first garbled circuit, and a garbled message based on the initial
13 message and the first garbled circuit;

14 transmitting to a third computer node in the distributed-computing network,
15 the first garbled circuit, the garbled first key share, and the garbled message, wherein
16 the third computer node also receives, from the second computer node, a garbled
17 second key share based on a second key share stored at the second computer node
18 and ~~the~~ a second garbled circuit,
19 which causes the third computer node to generate a subsequent message
20 by inputting the first garbled key share, the second garbled key share, and the garbled
21 message into either the first garbled circuit or the second garbled circuit ~~to the garbled~~
22 ~~circuit~~, and transmit the subsequent message to the first computer node; and
23 transmitting the subsequent message or a derivative thereof to the client
24 computer.

1 ~~4110~~. The first computer node of claim ~~409~~, ~~wherein the garbled circuit is~~
2 ~~a first garbled circuit~~, wherein the garbled message is a first garbled message, and
3 wherein the third computer node also receives from the second computer node, ~~a~~
4 ~~second garbled circuit and a second garbled message based on the initial message and~~
5 the second garbled circuit.

1 ~~4211~~. The first computer node of claim ~~4110~~, wherein the third computer
2 node determines 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 ~~4312~~. The first computer node of claim ~~409~~, wherein the method further
2 comprises:
3 generating an ungarbled subsequent message based on the subsequent
4 message and the first garbled circuit.

1 ~~4413~~. The first computer node of claim ~~409~~, wherein the initial message is
2 plaintext and the subsequent message or the derivative thereof is ciphertext.

1 ~~4514~~. The first computer node of claim ~~409~~, wherein the key management
2 computer generated the first key share from a key stored in a hardware security
3 module.

1 ~~46~~15. The first computer node of claim ~~40~~9, wherein the key management
2 computer formed the first key share and the second key share.

1 ~~47~~16. The first computer node of claim ~~40~~9, wherein the first computer
2 node, the second computer node, and the third computer node are all present at a same
3 premises.

1 ~~48~~17. A method comprising:
2 receiving, by a third computer node in a distributed-computing network,
3 from a first computer node in the distributed-computing network, a first garbled circuit, a
4 garbled first key share, and a first garbled message;
5 receiving, by the third computer node, from a second computer node in the
6 distributed-computing network, a second garbled circuit, a garbled second key share
7 and a second garbled message;
8 generating, by the third computer node, a subsequent message by
9 inputting the first garbled key share, the second garbled key share, and the first or the
10 second garbled message into either ~~to~~ the first garbled circuit or the second garbled
11 circuit; and
12 transmitting, by the third computer node, the subsequent message to the
13 first computer node.

1 ~~49~~18. The method of claim ~~48~~17, 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~~19. The method of claim ~~48~~17, wherein the first computer node
2 ungarbles the subsequent message and transmits the subsequent message to a client
3 computer.