

CLAIMS

What is claimed is:

1. A method for secure out-of-band symmetric encryption key delivery, comprising:
 - receiving, at a first trusted node in a network, a request from a first one of a pair of user devices to deliver symmetric encryption keys to the pair of user devices;
 - delivering, from the first trusted node via the trusted nodes in the network, a second one of the symmetric encryption keys to a second one of the pair of user devices;
 - receiving, at the first trusted node, from one of the trusted nodes in the network, confirmation of delivery of the second one of the symmetric encryption keys to the second one of the pair of user devices; and
 - delivering, from the first trusted node in the network, a first one of the symmetric encryption keys to the first one of the pair of user devices, responsive to the confirmation of the delivery of the second one of the symmetric encryption keys to the second one of the pair of user devices.
2. The method of claim 1, wherein the first and second ones of the symmetric encryption keys are guaranteed by the trusted nodes to be delivered to only the first and second ones of the pair of user devices.
3. The method of claim 1, wherein the delivering the second one of the symmetric encryption keys comprises delivering the second one of the symmetric encryption keys through the network between nodes that are pre-configured to trust each other as trusted nodes.
4. The method of claim 1, wherein the trusted nodes in the network comprise nodes in a peer-to-peer or mesh network each in a one-to-one, one-to-many, or many-to-many configuration.
5. The method of claim 1, further comprising:
 - performing just-in-time optimal pathfinding during delivery of the first and second ones of the symmetric encryption keys.
6. The method of claim 1, further comprising:
 - performing just-in-time load-balancing during delivery of the second one of the symmetric encryption keys.

7. The method of claim 1, further comprising:
 - generating and delivering quantum keys to each of two or more trusted nodes in the network.
8. The method of claim 1, further comprising:
 - encrypting each of one or more node to node transmissions with a quantum key, during delivery of the first and second ones of the symmetric encryption keys.
9. The method of claim 1, further comprising:
 - performing just-in-time optimal pathfinding based on availability of quantum keys during delivery of the first and second ones of the symmetric encryption keys.
10. A tangible, non-transitory, computer-readable media having instructions thereupon which, when executed by a processor, cause the processor to perform a method comprising:
 - receiving, at a first trusted node in a network, a request from a first user device to deliver symmetric encryption keys to the first user device and a second user device;
 - delivering, from the first trusted node via trusted nodes in the network, a second symmetric encryption key to the second user device;
 - receiving, at the first trusted node, from one of the trusted nodes in the network, confirmation of delivery of the second symmetric encryption key to the second user device; and
 - delivering, from the first trusted node in the network, a first symmetric encryption key, first and second symmetric encryption keys being symmetric to each other, to the first user device, responsive to the confirmation of the delivery of the second symmetric encryption key to the second user device.
11. The tangible, non-transitory, computer-readable media of claim 10, wherein the method further comprises:
 - preconfiguring nodes in the network to trust each other as trusted nodes in a mesh network or peer-to-peer network.
12. The tangible, non-transitory, computer-readable media of claim 10, wherein the method further comprises:
 - performing just-in-time optimal pathfinding in the network.

13. The tangible, non-transitory, computer-readable media of claim 10, wherein the method further comprises:

performing just-in-time load-balancing in the network.

14. The tangible, non-transitory, computer-readable media of claim 10, wherein the method further comprises:

generating quantum keys in two or more neighboring trusted nodes; and

encrypting and decrypting the first or the second symmetric encryption key, using the quantum keys.

15. An apparatus for secure out-of-band symmetric encryption key delivery, comprising:

a plurality of nodes of a network to form trusted nodes in a peer-to-peer or mesh network; and

a first trusted node, of the trusted nodes, to:

receive a request from a first user device to deliver symmetric encryption keys to the first user device and a second user device;

deliver, from the first trusted node via the trusted nodes, a second symmetric encryption key to the second user device;

receive, from one of the trusted nodes, confirmation of delivery of the second symmetric encryption key to the second user device; and

deliver, from the first trusted node, a first symmetric encryption key that is symmetric to the second symmetric encryption key, to the first user device, responsive to the confirmation of the delivery of the second symmetric encryption key to the second user device.

16. The apparatus of claim 15, wherein the trusted nodes are further to:

perform just-in-time optimal pathfinding in the peer-to-peer or mesh network.

17. The apparatus of claim 15, wherein the trusted nodes are further to:

perform just-in-time load-balancing in the network.

18. The apparatus of claim 15, wherein the trusted nodes are further to:

generate quantum keys in two or more neighboring trusted nodes; and

encrypt and decrypt the first or the second symmetric encryption key during delivery, using the quantum keys.

19. The apparatus of claim 15, wherein the trusted nodes are further to:
 - use encryption and decryption with quantum keys, for each node to node transmission during delivery of the first and second symmetric encryption keys.
20. The apparatus of claim 15, wherein the trusted nodes are further to:
 - perform just-in-time optimal pathfinding based on availability of quantum keys during delivery of the first and second symmetric encryption keys.