

CLAIMS

What is claimed is:

1. A method, comprising:

collecting from each endpoint device of a plurality of endpoint devices a set of anonymized interactions of the corresponding endpoint device with other endpoint devices, wherein each anonymized interaction in the set of anonymized interactions is based on an ephemeral unique identifier of another endpoint device involved in a corresponding anonymized interaction with the corresponding endpoint device; and

for each endpoint device, resolving identities of the other endpoint devices with which the corresponding endpoint device has interacted from the corresponding set of anonymized interactions.

2. The method of claim 1, further comprising:

precomputing ephemeral unique identifiers for each endpoint device; and

storing the precomputed ephemeral unique identifiers for each endpoint device,

wherein:

each anonymized interaction includes an ephemeral unique identifier of a corresponding one of the other endpoint devices with which the corresponding device has interacted; and

resolving identities of the other endpoint devices with which the corresponding device has interacted comprises searching for ephemeral unique identifiers from the anonymized interactions in the stored precomputed ephemeral unique identifiers.

3. The method of claim 2, wherein resolving identities of the other endpoint devices with which the corresponding device has interacted further comprises, in response to a given anonymized interaction matching a given stored precomputed ephemeral unique identifier that is associated with a given endpoint device, determining that the corresponding endpoint device interacted with the given endpoint device.

4. The method of claim 2, wherein:

each endpoint device has a corresponding secret key known to a network operator;

and

each ephemeral unique identifier is precomputed based at least in part on a corresponding secret key and a counter.

5. The method of claim 4, wherein precomputing ephemeral unique identifiers comprises, for each endpoint device:

generating a plurality of deterministic seeds from the corresponding secret key and a plurality of counter values; and

generating a plurality of ephemeral public key pairs from the plurality of deterministic seeds, wherein each precomputed ephemeral unique identifier comprises a different one of the plurality of ephemeral public key pairs.

6. The method of claim 5, wherein generating the plurality of deterministic seeds comprises generating a plurality of hash values, each hash value being a hash of the corresponding secret key and a different counter value of the plurality of counter values.

7. The method of claim 5, wherein generating the plurality of ephemeral public key pairs comprises generating a plurality of Curve25519 public keys, each Curve25519 public key generated using a different deterministic seed of the plurality of deterministic seeds as input.

8. The method of claim 1, further comprising determining whether a first user of the corresponding endpoint device was exposed to a second user of another endpoint device based on whether an identity of the other endpoint device is among the resolved identities of the other endpoint devices with which the corresponding endpoint device has interacted.

9. The method of claim 1, wherein the plurality of endpoint devices are borne by users at a job site, the method further comprising determining, based on a plurality of interactions with endpoint devices having known locations within the job site, at least one of:

one or more patterns of movement of the users at the job site;

analytics regarding frequency of visits by users to each of one or more locations within the job site; or

analytics regarding number of interactions between the users at each of one or more locations within the job site.

10. A non-transitory computer-readable storage medium having computer-readable instructions stored thereon that are executable by a processor to perform or control performance of the method of claim 1.

11. A method, comprising:
- generating, over time, a plurality of ephemeral unique identifiers for a first endpoint device, wherein each of the plurality of ephemeral unique identifiers is specific to the first endpoint device and is configured to identify the first endpoint device;
 - scanning for other endpoint devices; and
 - in response to detecting a second endpoint device while scanning:
 - providing a current ephemeral unique identifier of the first endpoint device to the second endpoint device; and
 - receiving a current ephemeral unique identifier of the second endpoint device at the first endpoint device.
12. The method of claim 11, further comprising adding an anonymized interaction with the second endpoint device to a set of anonymized interactions of the first endpoint device with other endpoint devices, each anonymized interaction in the set of anonymized interactions based on a corresponding ephemeral unique identifier of the corresponding endpoint device received during a corresponding interaction between the first endpoint device and the corresponding endpoint device.
13. The method of claim 12, further comprising sharing the set of anonymized interactions of the first endpoint device with a backend server to resolve identities of the other endpoint devices with which the first endpoint device has interacted.
14. The method of claim 11, wherein:
- the first endpoint device has a secret key known to a network operator; and

each of the plurality of ephemeral unique identifiers for the first endpoint device is based on the secret key and a counter.

15. The method of claim 14, wherein generating, over time, the plurality of ephemeral unique identifiers comprises, for each of the plurality of ephemeral unique identifiers:

generating a deterministic seed from the secret key and a counter value that depends on a time at which the deterministic seed is generated; and

generating an ephemeral public key pair from the deterministic seed to use as a corresponding one of the plurality of ephemeral unique identifiers.

16. The method of claim 15, wherein generating the deterministic seed comprises generating a hash value as a hash of the secret key and the counter value.

17. The method of claim 15, wherein the counter value comprises a value of a difference between a current time and a reference time divided by a time step.

18. The method of claim 15, wherein generating the ephemeral public key pair comprises generating a Curve25519 public key using the deterministic seed as input.

19. The method of claim 11, further comprising:

determining a distance between the first endpoint device and the second endpoint device; and

in response to the distance being less than a threshold, outputting an alert to a user of the first endpoint device.

20. A non-transitory computer-readable storage medium having computer-readable instructions stored thereon that are executable by a processor to perform or control performance of the method of claim 11.