ECDH for more than two parties

Asked 3 years, 10 months ago Modified 3 years, 10 months ago Viewed 1k times

4

With classic diffie-hellman it's possible do it with more than two parties. Is this applicable to elliptic curve diffie hellman?

I'm guessing not.

With ECDH you have a scalar number as the private key and an x, y coordinate (or just x coordinate in the case of Curve25519) as the public key. You multiply the coordinate by the scalar and you get a new coordinate. The x coordinate of that is the shared secret.

If you had two public keys and one private / public ECDH key pair... if you didn't discard the y coordinate you could multiply one of the public key coordinates by the private key but then it's not clear what you would do with the other public key coordinate. Maybe there's nothing you can really do to facilitate ECDH for more than two parties?

elliptic-curves diffie-hellman

Share Improve this question Follow

asked Jul 27, 2019 at 21:35

neubert

2,855 1 25 50

1 Answer

Sorted by: Highest score (default)

5

You can do ECDH with more than two parties. See the below adaptation of the wikipedia example for an EC group -

1. The parties agree on the algorithm parameters, a curve over $E(\mathbb{F}_p)$ and base point G.
2. The parties generate their private keys, named a, b, and c (these are integers).
3. Alice computes aG and sends it to Bob.
4. Bob computes $(aG)b = (ab)G$ and sends it to Carol.
5. Carol computes $(abG)c = (abc)G$ and uses the x coordinate as her secret.
6. Bob computes bG and sends it to Carol.
7. Carol computes $(bG)c = (bc)G$ and sends it to Alice.
8. Alice computes $(bcG)a = (bca)G = (abc)G$ and uses the x coordinate as her secret.
9. Carol computes cG and sends it to Alice.
10. Alice computes $(cG)a = (ca)G$ and sends it to Bob.
11. Bob computes $(caG)b = (cab)G = (abc)G$ and uses the x coordinate as his secret.

A note about your concern with Montgomery curves (such as curve25519). Montgomery curves indeed only return the x coordinate but point multiplication only requires the x coordinate as input. Said another way, the Montgomery ladder which is used for point multiplication does not use the y coordinate in the algorithm. So the doing e.g. $(aG)b$ is fine since aG will return an x coordinate, and we can use the Montgomery ladder to multiply that by b.

In fact, multi party DH will work for any group that has a "combine" and a "scale" operations for its elements.

Share Improve this answer Follow

answered Jul 27, 2019 at 23:53

puzzlepalace
3,982 1 18 43

3 This answer was very useful for me! I made a Go implementation based on it: play.golang.org/p/avAJIL2ydui – Bukodi László Nov 12, 2020 at 22:46