US 20230231702A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2023/0231702 A1**

**Nix** (43) **Pub. Date: Jul. 20, 2023**

(54) **ECDHE KEY EXCHANGE FOR MUTUAL AUTHENTICATION USING A KEY SERVER**

(71) Applicant: **IoT and M2M Technologies, LLC**, Evanston, IL (US)

(72) Inventor: **John A. Nix**, Evanston, IL (US)

(73) Assignee: **IoT and M2M Technologies, LLC**, Evanston, IL (US)

(21) Appl. No.: **18/125,953**

(22) Filed: **Mar. 24, 2023**

**Related U.S. Application Data**

(63) Continuation of application No. 17/717,101, filed on Apr. 10, 2022, now Pat. No. 11,626,979, which is a continuation of application No. 17/254,849, filed on Dec. 21, 2020, now Pat. No. 11,316,672, filed as application No. PCT/US2019/039380 on Jun. 27, 2019.

(60) Provisional application No. 62/691,255, filed on Jun. 28, 2018.

**Publication Classification**

(51) **Int. Cl.**

| | |
|---|---|
| ***H04L 9/08*** | (2006.01) |
| ***H04L 9/30*** | (2006.01) |
| ***H04L 9/32*** | (2006.01) |

(52) **U.S. Cl.**

CPC ..... ***H04L 9/0841*** (2013.01); ***H04L 9/0825*** (2013.01); ***H04L 9/3066*** (2013.01); ***H04L 9/3242*** (2013.01); ***H04L 9/3252*** (2013.01)

(57) **ABSTRACT**

A server can record a device static public key (Sd) and a server static private key (ss). The server can receive a message with (i) a device ephemeral public key (Ed) and (ii) a ciphertext encrypted with key K1. The server can (i) conduct an EC point addition operation on Sd and Ed and (ii) send the resulting point/secret X0 to a key server. The key server can (i) perform a first elliptic curve Diffie-Hellman (ECDH) key exchange using X0 and a network static private key to derive a point/secret X1, and (ii) send X1 to the server. The server can conduct a second ECDH key exchange using the server static private key and point X0 to derive point X2. The server can conduct an EC point addition on X1 and X2 to derive X3. The server can derive K1 using X3 and decrypt the ciphertext.