US 20240214185A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2024/0214185 A1**

LI et al. (43) **Pub. Date: Jun. 27, 2024**

(54) **PROTECTING SECRET PROCESSING, SECRET INPUT DATA, AND SECRET OUTPUT DATA USING ENCLAVES**

(71) Applicants: **LI Zhiqiang**, Beijing (CN); **Daniel MIDDLETON**, Orono, MN (US); **Dan HE**, Shanghai (CN); **Yiqi CHEN**, Shanghai (CN); **Intel Corporation**, Santa Clara, CA (US)

(72) Inventors: **Zhiqiang LI**, Beijing (CN); **Daniel MIDDLETON**, Orono, MN (US); **Dan HE**, Shanghai (CN); **Yiqi CHEN**, Shanghai (CN)

(73) Assignee: **Intel Corporation**, Santa Clara, CA (US)

(21) Appl. No.: **18/556,022**

(22) PCT Filed: **Sep. 23, 2021**

(86) PCT No.: **PCT/CN2021/119882**

§ 371 (c)(1),
(2) Date: **Oct. 18, 2023**

Publication Classification

(51) **Int. Cl.**
H04L 9/08 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 9/0825*** (2013.01); ***H04L 9/083*** (2013.01); *H04L 9/0822* (2013.01)

(57) **ABSTRACT**

An apparatus and method of protect secret input data, secret processing, and secret output data by receiving a signed private enclave from a secret processing owner; receiving a signed manager enclave from a trusted third party (TTP); deploying the signed manager enclave; receiving a protected code loader (PCL) key encrypted with an encryption public key of the signed manager enclave from the secret processing owner; deploying the signed private enclave; running secret processing in the signed private enclave with secret input data to generate secret output data; and encrypting the secret output data in the signed private enclave using an ephemeral key, encrypting the ephemeral key in the signed private enclave using an encryption public key of the signed manager enclave, and sending the encrypted secret output data and the encrypted ephemeral key to the signed manager enclave.