US 20230231712A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2023/0231712 A1**

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

(54) **EMBEDDED TLS PROTOCOL FOR LIGHTWEIGHT DEVICES**

(71) Applicant: **Micron Technology, Inc.**, Boise, ID (US)

(72) Inventor: **Zhan Liu**, Cupertino, CA (US)

(21) Appl. No.: **17/576,889**

(22) Filed: **Jan. 14, 2022**

Publication Classification

(51) **Int. Cl.**

H04L 9/30	(2006.01)
H04L 9/08	(2006.01)
H04L 9/32	(2006.01)

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

CPC ***H04L 9/3066*** (2013.01); ***H04L 9/088*** (2013.01); ***H04L 9/3263*** (2013.01)

(57) **ABSTRACT**

The disclosure relates to improvements in secure channel establishment. In some aspects, the techniques described herein relate to a method including: issuing, by a client device to a server, a request to establish a secure connection; receiving, by the client device, a response to the request to establish a secure connection from the server, the response including a digital certificate associated with a public key stored by the server, the public key used to establish a symmetric key; validating, by the client device, the digital certificate; and computing, by the client device, a shared secret using the public key stored by the server and a private key generated by the client device.