US 20240214218A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2024/0214218 A1**

PETTIT (43) **Pub. Date: Jun. 27, 2024**

(54) **NESTED THRESHOLD SIGNATURES**

(71) Applicant: **nChain Licensing AG**, Zug (DE)

(72) Inventor: **Michaella PETTIT**, London (GB)

(21) Appl. No.: **18/288,555**

(22) PCT Filed: **Mar. 28, 2022**

(86) PCT No.: **PCT/EP2022/058085**

§ 371 (c)(1),
(2) Date: **Oct. 26, 2023**

(30) **Foreign Application Priority Data**

Apr. 27, 2021 (GB) 2105992.8

Publication Classification

(51) **Int. Cl.**
H04L 9/32 (2006.01)
H04L 9/08 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 9/3255*** (2013.01); ***H04L 9/085*** (2013.01); ***H04L 9/0869*** (2013.01)

(57) **ABSTRACT**

A computer-implemented method of requiring at least one of a sub-group of a group of participants to contribute to a threshold-optimal signature scheme, wherein the valid signature comprises a first signature component and a second signature component, wherein each participant has a respective private key share of a shared private key, a respective ephemeral private key share of a shared ephemeral private key, and the first signature component, wherein the shared private key can only be generated with at least a first threshold number of respective private key shares.