US012494897B2

(12) **United States Patent**
**Lee et al.**

(10) **Patent No.: US 12,494,897 B2**
(45) **Date of Patent: Dec. 9, 2025**

(54) **METHOD OF GENERATING RANDOMNESS BY PUBLIC PARTICIPATION**

(71) Applicants: **National Taiwan University**, Taipei (TW); **The Board of Trustees of the University of Illinois**, Urbana, IL (US)

(72) Inventors: **Hsun Lee**, Taipei (TW); **Yuming Hsu**, Taipei (TW); **Jing-Jie Wang**, Taipei (TW); **Hao Cheng Yang**, Taipei (TW); **Yu-Heng Chen**, Taipei (TW); **Yih-Chun Hu**, Urbana, IL (US); **Hsu-Chun Hsiao**, Taipei (TW)

(73) Assignees: **National Taiwan University**, Taipei (TW); **The Board of Trustees of the University of Illinois**, Urbana, IL (US)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 216 days.

(21) Appl. No.: **18/099,024**

(22) Filed: **Jan. 19, 2023**

(65) **Prior Publication Data**

US 2023/0299939 A1 Sep. 21, 2023

**Related U.S. Application Data**

(60) Provisional application No. 63/302,804, filed on Jan. 25, 2022.

(51) **Int. Cl.**
***H04L 9/06*** (2006.01)

(52) **U.S. Cl.**
CPC ..... ***H04L 9/0643*** (2013.01)

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 11,184,166 | B2 * | 11/2021 | Lampkins | H04L 9/0869 |
| 2018/0034636 | A1 * | 2/2018 | Benarroch Guenun | H04L 9/3073 |
| 2020/0252211 | A1 * | 8/2020 | Chen | H04L 9/0894 |
| 2023/0318857 | A1 * | 10/2023 | Nazarov | H04L 9/30 713/166 |

FOREIGN PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| CA | 2543796 C | * | 12/2015 | H04L 63/045 |
| CN | 113407156 A | * | 9/2021 | G06F 21/64 |

* cited by examiner

*Primary Examiner* — Jeffrey R Swearingen
(74) *Attorney, Agent, or Firm* — Chen Yoshimura LLP

(57) **ABSTRACT**

A method of generating randomness by public participation may comprise: communicating with the commodity devices to execute a protocol comprising a setup phase, a contribution phase and a result-generation phase, wherein: in the setup phase, parameters are initialized, a verifiable delay function is setup, and the parameters are published; the contribution phase is divided into at least one first stage, published parameters are provided, random values are received, and a Merkle tree root and Merkle tree audit paths are published in each of the first stage; and the result-generation phase is divided into at least one second stage of the same number as that of the first stage, each second stage is dedicated to one of the first stage ahead of the second stage for a period, and in each second stage, computation is performed to generate a result of randomness which is published.

**15 Claims, 8 Drawing Sheets**