US 20240214224A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2024/0214224 A1**

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

(54) **PSEUDO-HOMOMORPHIC AUTHENTICATION OF USERS WITH BIOMETRY**

(71) Applicant: **Arizona Board of Regents on Behalf of Northern Arizona University**, Flagstaff, AZ (US)

(72) Inventors: **Bertrand F. CAMBOU**, Flagstaff, AZ (US); **Michael L. GARRETT**, Flagstaff, AZ (US)

(21) Appl. No.: **18/397,975**

(22) Filed: **Dec. 27, 2023**

Related U.S. Application Data

(60) Provisional application No. 63/435,470, filed on Dec. 27, 2022.

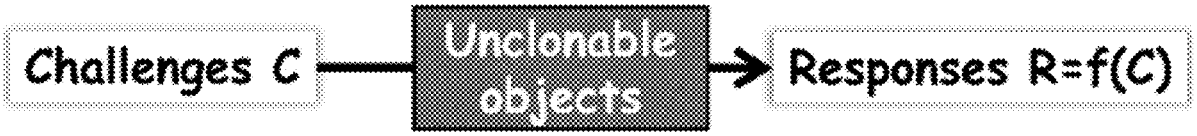
Publication Classification

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

(52) **U.S. Cl.**
CPC ***H04L 9/3278*** (2013.01); ***H04L 9/3231*** (2013.01); ***H04L 9/3239*** (2013.01)

(57) **ABSTRACT**

Methods for the generation and use of session keys for authentication of a user of a server device are disclosed. The methods use a biological objects of the user to generate responses to challenges. During enrollment, the server device receives a password, hashes it a first number of times, and sends the hash to the user. The user interprets the hash as a set of challenges for the biological object, applies the challenges, and stores the responses. During authentication, the server hashes the password a second number of times, less than the first number, and sends the hash to the user. The user iteratively applies second hash to the biological object, compares the responses to the stored responses, and if there is not a match, hashes the challenges again until there is a match. The number of hashes needed for a match is a session key or subkey.



Similarity with hash functions:

- **One way:** Hard to uncover C from R
- **Weak Collisions:** $C \neq C' \Rightarrow R \neq R'$ (most likely)
  $R \neq R' \Rightarrow C \neq C'$ (most likely)

Contrasts with hash functions:

- **Unclonable:** The objects are unclonable
- **Unique:** R_1 for object 1 $\neq$ R_2 for object 2
- **Stochasticity:** Presence of random effects
- **Sensitive:** Subject to environmental effects
- **Imperfect:** Subject to aging and drifts