US010979221B2

(12) **United States Patent**
Cambou

(10) **Patent No.: US 10,979,221 B2**
(45) **Date of Patent: Apr. 13, 2021**

(54) **GENERATION OF KEYS OF VARIABLE LENGTH FROM CRYPTOGRAPHIC TABLES**

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

(72) Inventor: **Bertrand F. Cambou**, Flagstaff, AZ (US)

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

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 341 days.

(21) Appl. No.: **16/237,366**

(22) Filed: **Dec. 31, 2018**

(65) **Prior Publication Data**

US 2019/0207758 A1 Jul. 4, 2019

Related U.S. Application Data

(60) Provisional application No. 62/613,166, filed on Jan. 3, 2018.

(51) **Int. Cl.**
H04L 9/08 (2006.01)
H04L 9/30 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC ***H04L 9/0863*** (2013.01); ***H04L 9/0618*** (2013.01); ***H04L 9/0643*** (2013.01); ***H04L 9/0662*** (2013.01); ***H04L 9/0866*** (2013.01); ***H04L 9/0869*** (2013.01); ***H04L 9/30*** (2013.01); ***H04L 63/0428*** (2013.01); ***H04L 63/061*** (2013.01); ***H04L 63/083*** (2013.01); *H04L 2463/061* (2013.01); *H04L 2463/081* (2013.01)

(58) **Field of Classification Search**
CPC ... H04L 9/0863; H04L 9/0618; H04L 9/0643; H04L 9/0662; H04L 9/0866; H04L 9/0869; H04L 9/30; H04L 63/0428; H04L 63/061; H04L 63/083; H04L 2463/061; H04L 2463/081
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,218,582 A * 8/1980 Hellman H04L 9/30 380/30
9,648,011 B1 * 5/2017 Mattsson H04L 9/3226
(Continued)

Primary Examiner — Peter C Shaw
Assistant Examiner — Zhe Liu
(74) *Attorney, Agent, or Firm* — Quarles & Brady LLP

(57) **ABSTRACT**

A cryptographic infrastructure, which provides a method for generating private keys of variable length from a cryptographic table and a public key. This infrastructure provides an approximation of the one-time pad scheme. The cryptographic table is shared between a message sender and a message recipient by a secure transfer. After sharing the cryptographic table, no new private keys need to be sent—the private keys are independently generated by each party from the data contained within the shared cryptographic tables, using the public key. After public keys are exchanged, private keys may be generated and used to encrypt and decrypt messages and perform authentication cycles, establishing a secure communication environment between the sender and the recipient.

20 Claims, 12 Drawing Sheets