US 20230231840A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2023/0231840 A1**

Wu et al. (43) **Pub. Date: Jul. 20, 2023**

(54) **ENCRYPTION AND DECRYPTION TECHNIQUES USING SHUFFLE FUNCTION**

(71) Applicant: **Jonetix Corporation**, Cupertino, CA (US)

(72) Inventors: **Paul Ying-Fung Wu**, Saratoga, CA (US); **Richard J. Nathan**, Gilroy, CA (US); **Harry Leslie Tredennick**, Los Gatos, CA (US)

(21) Appl. No.: **17/973,791**

(22) Filed: **Oct. 26, 2022**

Related U.S. Application Data

(63) Continuation of application No. 17/154,880, filed on Jan. 21, 2021, now Pat. No. 11,516,201, which is a continuation of application No. 16/533,024, filed on Aug. 6, 2019, now Pat. No. 10,931,658, which is a continuation of application No. 16/004,181, filed on Jun. 8, 2018, now Pat. No. 10,419,416, which is a continuation of application No. 15/461,384, filed on Mar. 16, 2017, now Pat. No. 10,021,085, which is a continuation of application No. 14/831,070, filed on Aug. 20, 2015, now Pat. No. 9,635,011.

(60) Provisional application No. 62/089,104, filed on Dec. 8, 2014, provisional application No. 62/099,446, filed on Jan. 3, 2015, provisional application No. 62/042,335, filed on Aug. 27, 2014.

Publication Classification

(51) **Int. Cl.**

H04L 9/40	(2006.01)
H04L 9/32	(2006.01)
H04L 9/08	(2006.01)
H04L 9/14	(2006.01)

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

CPC ***H04L 63/0807*** (2013.01); ***H04L 9/3242*** (2013.01); ***H04L 9/3297*** (2013.01); ***H04L 9/0861*** (2013.01); ***H04L 9/14*** (2013.01); ***H04L 9/3213*** (2013.01); ***H04L 9/3226*** (2013.01); ***H04L 63/0428*** (2013.01); ***H04L 63/083*** (2013.01); *H04L 2209/08* (2013.01); *H04L 2209/34* (2013.01)

(57) **ABSTRACT**

Encryption and decryption techniques based on one or more transposition vectors. A secret key is used to generate vectors that describe permutation (or repositioning) of characters within a segment length equal to a length of the transposition vector. The transposition vector is then inherited by the encryption process, which shifts characters and encrypts those characters using a variety of encryption processes, all completely reversible. In one embodiment, one or more auxiliary keys, transmitted as clear text header values, are used as initial values to vary the transposition vectors generated from the secret key, e.g., from encryption-to-encryption. Any number of rounds of encryption can be applied, each having associated headers used to "detokenize" encryption data and perform rounds to decryption to recover the original data (or parent token information). Format preserving encryption (FPE) techniques are also provided with application to, e.g., payment processing.