US009628266B2

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

(10) **Patent No.: US 9,628,266 B2**
(45) **Date of Patent: Apr. 18, 2017**

(54) **SYSTEM AND METHOD FOR ENCODING ENCRYPTED DATA FOR FURTHER PROCESSING**

(71) Applicant: **RAYTHEON BBN TECHNOLOGIES CORP.**, Cambridge, MA (US)

(72) Inventors: **Kurt Ryan Rohloff**, South Hadley, MA (US); **David Bruce Cousins**, Barrington, RI (US)

(73) Assignee: **RAYTHEON BBN TECHNOLOGIES CORP.**, Cambridge, MA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 525 days.

(21) Appl. No.: **14/191,021**

(22) Filed: **Feb. 26, 2014**

(65) **Prior Publication Data**

US 2017/0078086 A1 Mar. 16, 2017

(51) **Int. Cl.**

H04K 1/00	(2006.01)
H04L 9/00	(2006.01)
H04L 9/28	(2006.01)
H04L 9/06	(2006.01)

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

CPC ***H04L 9/06*** (2013.01)

(58) **Field of Classification Search**

CPC . H04L 9/008; H04L 63/0471; H04L 63/0428; H04L 63/0442; H04L 63/061; H04L 9/3093; H04L 65/403; H04K 1/00

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,324,505 B1 * 11/2001 Choy G10L 19/0204 704/201

2004/0017851 A1 * 1/2004 Haskell H04N 19/52 375/240.16

(Continued)

OTHER PUBLICATIONS

Real-time Adaptive Concepts in Acoustics, Blind Signal Separation and Multichannel Echo Cancellation, Daniel W.E. Schobben, 2001.*

(Continued)

Primary Examiner — Michael S McNally
Assistant Examiner — Amie C Lin
(74) *Attorney, Agent, or Firm* — Lewis Roca Rothgerber Christie LLP

(57) **ABSTRACT**

A method for encoding encrypted data for further processing includes: receiving an input data vector of length m; splitting the input data vector to k multiple vectors; multiplying each of the multiple vectors by a power of 2 to obtain k number of intermediate vectors; summing the k number of intermediate vectors to obtain a single summed vector; encrypting the single summed vector to obtain an encrypted vector; sending the encrypted vector to an operational unit to have the encrypted vector operated on to obtain a processed encrypted vector; receiving the processed encrypted vector; decrypting the received encrypted vector; dividing the processed decrypted vector by a power of 2, modulus a power of 2 to obtain multiple transitional vectors of the same dynamic range and the same length; and concatenating the multiple transitional vectors to obtain a recovered vector of length m.

11 Claims, 6 Drawing Sheets