US007362859B1

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

(10) **Patent No.: US 7,362,859 B1**
(45) **Date of Patent: Apr. 22, 2008**

(54) **ENHANCEMENT OF UTILIZATION OF ENCRYPTION ENGINE**

(75) Inventors: **Robert J. Robertson**, Albuquerque, NM (US); **Edward L. Witzke**, Edgewood, NM (US)

(73) Assignee: **Sandia Corporation**, Alb, NM (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 442 days.

(21) Appl. No.: **09/970,912**

(22) Filed: **Oct. 4, 2001**

Related U.S. Application Data

(60) Provisional application No. 60/238,678, filed on Oct. 6, 2000.

(51) **Int. Cl.**
H04K 1/04 (2006.01)
H04K 1/00 (2006.01)

(52) **U.S. Cl.** **380/37**; 380/29

(58) **Field of Classification Search** 380/37, 380/29

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,969,190 A * 11/1990 Takaragi et al. 380/43
5,432,849 A * 7/1995 Johnson et al. 380/280
5,633,934 A * 5/1997 Hember 713/192
5,671,283 A * 9/1997 Michener et al. 713/161
5,745,577 A * 4/1998 Leech 380/28
5,799,089 A * 8/1998 Kuhn et al. 380/37
5,835,599 A * 11/1998 Buer 380/29
6,055,316 A * 4/2000 Perlman et al. 380/262
6,269,163 B1 * 7/2001 Rivest et al. 380/28
6,870,929 B1 * 3/2005 Greene 380/28
6,920,562 B1 * 7/2005 Kerr et al. 713/189
2001/0038693 A1 * 11/2001 Luyster 380/37

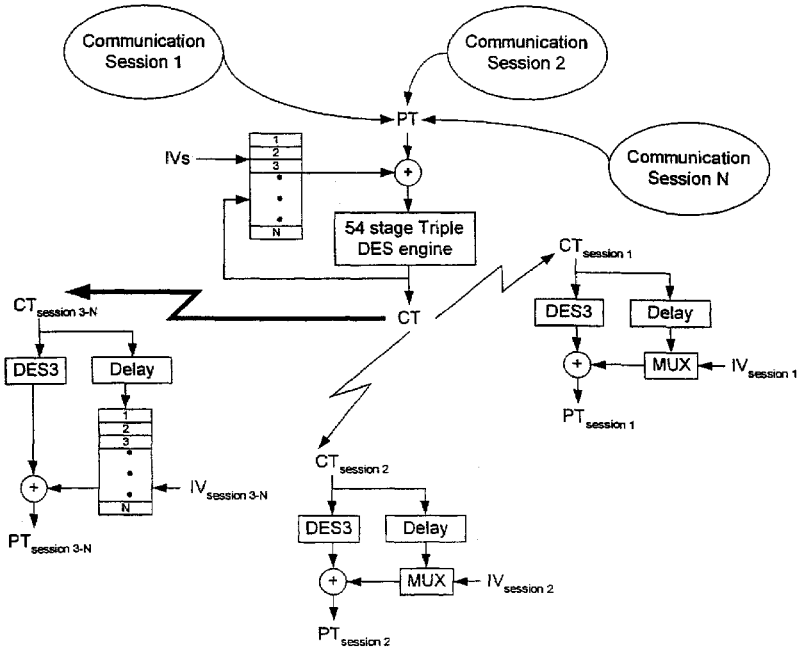
OTHER PUBLICATIONS

Bruce Schneier, 1996, Applied Cryptography , Second Edition p. 311.*
Michelle L. Hankins, Signal AFCEA's International Journal, Oct. 1999 "Integrated Circuit Chip Provides Secure, Rapid Data Encryption" pp. 1-3.*
Schaffer et al. "A flip-chip implementation of the data encryption standard (DES)" Feb. 1997, pp. 13-17.*
American National Standards Institute; Triple Data Encruption Algorithm Modes of Operation; Jul. 29, 1998; pp. 1-90.
ACM SIGCOMM, vol. 29, No. 1; ACM SIGCOMM Computer Communication Review Paper Retrieval; Jan. 1999.

* cited by examiner

Primary Examiner—Nasser Moazzami
Assistant Examiner—Eleni A Shiferaw
(74) *Attorney, Agent, or Firm*—Madelynne J. Farber

(57) **ABSTRACT**

A method of enhancing throughput of a pipelined encryption/decryption engine for an encryption/decryption process has a predetermined number of stages and provides feedback around the stages (and of such an encryption/decryption engine) by receiving a source datablock for a given stage and encryption/decryption context identifier; indexing according to the encryption/decryption context identifier into a bank of initial variables to retrieve an initial variable for the source datablock; and generating an output datablock from the source datablock and its corresponding initial variable.

8 Claims, 4 Drawing Sheets