



US006219421B1

(12) **United States Patent**
Backal

(10) **Patent No.:** **US 6,219,421 B1**
(45) **Date of Patent:** ***Apr. 17, 2001**

(54) **VIRTUAL MATRIX ENCRYPTION (VME)
AND VIRTUAL KEY CRYPTOGRAPHIC
METHOD AND APPARATUS**

OTHER PUBLICATIONS

(75) Inventor: **Shaul O. Backal**, 19528 Ventura Blvd.,
#317, Tarzana, CA (US) 91356

Schneier, Applied Cryptography 2e, pp. 170-177, 1996.*

Menezes, et al., Applied Cryptography, p. 172, 1996.*

(73) Assignee: **Shaul O. Backal**, Tarzana, CA (US)

Bruce Schneier, Applied cryptography, 2e, John Wiley pp.
183-184, 1996.*

(*) Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

* cited by examiner

Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

Primary Examiner—Gail Hayes
Assistant Examiner—James W Seal
(74) *Attorney, Agent, or Firm*—Burns, Doane, Swecker & Mathis, LLP

(21) Appl. No.: **08/957,288**

(57) **ABSTRACT**

(22) Filed: **Oct. 24, 1997**

A data security method and apparatus that provides an exceptional degree of security at low computational cost. The data security arrangement differs from known data security measures in several fundamental aspects. Most notably, the content of the message is not sent with the encrypted data. Rather, the encrypted data consists of pointers to locations within a virtual matrix, a large (arbitrarily large), continuously-changing array of values. The encryption technique is therefore referred to as Virtual Matrix Encryption. Furthermore, the data security arrangement uses a very large key of one million bits or more which creates a level of security much higher than any other existing method. The key is not transferred but is instead created from a file of any size that is available on both a computer used to send a secure message and a computer used to receive a secure message. The term Virtual Key Cryptographic as used herein to refer to techniques in which a key is recreated at a remote location from an electronic file without any transmission of the key itself. The file may be a system file, a file downloaded from the Internet, etc. A smaller, transaction-specific key, e.g., a 2,048 bit key, is sent end-to-end and is used in conjunction with the very large key to avoid a security hazard in instances where the same file is used repeatedly to create the very large key.

(51) **Int. Cl.**⁷ **A04K 1/00**

(52) **U.S. Cl.** **380/28; 380/28**

(58) **Field of Search** **380/28, 57**

(56) **References Cited**

U.S. PATENT DOCUMENTS

744,041	*	11/1903	Burke	380/57
3,250,855	*	5/1966	Vasseur	380/262
4,157,454		6/1979	Becker	178/22
4,740,890	*	4/1988	William	364/200
4,988,987	*	1/1991	Barrett et al.	
5,058,160	*	10/1991	Banker et al.	380/20
5,703,948	*	12/1997	Yanovsky	380/262
5,712,800		1/1998	Aucsmith	364/514 R
5,771,291	*	6/1998	Newton et al.	380/25
5,787,172	*	7/1998	Arnold	380/21
5,835,600		11/1998	Rivest	380/44

16 Claims, 11 Drawing Sheets

VME - Virtual Matrix Encryption

