



US006041122A

**United States Patent** [19]  
**Graunke et al.**

[11] **Patent Number:** **6,041,122**  
[45] **Date of Patent:** **Mar. 21, 2000**

[54] **METHOD AND APPARATUS FOR HIDING CRYPTOGRAPHIC KEYS UTILIZING AUTOCORRELATION TIMING ENCODING AND COMPUTATION**

Kocher, Paul C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems "Advances in Cryptology" Crypto '96.

[75] Inventors: **Gary L. Graunke**, Beaverton; **David W. Aucsmith**, Portland, both of Oreg.

"Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", by Paul C. Kocher, published in "Advances in Cryptology", Crypto '96, pp. 104-113, Lecture Notes in Computer Science #1109.

[73] Assignee: **Intel Corporation**, Santa Clara, Calif.

[21] Appl. No.: **09/032,594**

*Primary Examiner*—Gail O. Hayes

[22] Filed: **Feb. 27, 1998**

*Assistant Examiner*—Christopher M. Tucker

[51] **Int. Cl.**<sup>7</sup> ..... **H04L 9/00**

*Attorney, Agent, or Firm*—Blakely, Sokoloff, Taylor & Zafman LLP

[52] **U.S. Cl.** ..... **380/21; 380/1; 380/28**

[58] **Field of Search** ..... **380/21, 24, 23, 380/30, 44**

[57] **ABSTRACT**

[56] **References Cited**

A method and apparatus for hiding cryptographic keys based on autocorrelation timing attacks is provided. The method and apparatus of the present invention utilize a autocorrelation timing attack to allow independent software entities to authenticate themselves without storing a private cryptographic key. This is accomplished by storing timing statistics related to the evaluation of an equation in the software entity rather than the cryptographic key itself. When the software entity authenticates itself, the cryptographic key is derived based on information provided by the timing statistics contained in the software entity.

**U.S. PATENT DOCUMENTS**

4,649,233	3/1987	Bass et al. ....	380/21
4,878,246	10/1989	Pastor et al. ....	380/44
4,912,762	3/1990	Lee et al. ....	380/24
4,956,863	9/1990	Goss ....	380/30
5,201,000	4/1993	Matyas et al. ....	380/30
5,202,921	4/1993	Herzberg et al. ....	380/23
5,369,708	11/1994	Kawamura et al. .	

**OTHER PUBLICATIONS**

Kocher, Paul C. "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems" Advances in Cryptology Crypto '96, 1996.

**56 Claims, 11 Drawing Sheets**

