以四為基底之心脈式RSA加解密系統晶片

蔡秉諺、洪進華 程仲勝

E-mail: 9314948@mail.dyu.edu.tw

摘 要

基於改善蒙哥馬利的演算法，我們提出了適用於RSA 公開金 鑰密碼系統的位元階層之心脈式陣列。在指數演算法中，我們使用 插入平方運算與乘法運算的方式，使得乘法器的使用率可以達到 100%。 以修改過的布斯演算法為基礎，我們設計與實現了一個以四為 基底之位元插入心脈式陣列的RSA 密碼系統。藉由減少迭代的運 算次數，以及管線化的技術，我們的RSA 密碼系統比傳統的方法 要快上四倍，且運算一筆 512 位元的RSA 運算只需要大約平均 0.26M 個時脈週期，其RSA 密碼系統加解密的速度在工作頻率為 333M Hz 時可達到 656 Kb/s。

關鍵詞 : 心脈式 ; 密碼系統 ; 蒙哥馬利

目錄

參考文獻

[1] Diffie and M. E. Hellman, “ New Direction in Cryptography, ” IEEE Transaction on Information Theory, vol. IT-22, no. 6, pp. 644-654, 1976.

[2] R. L. Rivest, A. Shamir, and L. Adleman, “ A method for obtaining digital signatures and public-key cryptosystems, ” Communications of the ACM, vol. 21, pp. 120-126, Feb. 1978.

[3] Brickell, “ A First Modular Multiplication Algorithm with Application to Two Key Cryptography, ” in Advance in Cryptology (Proceeding of CRYPTO ’ 82), pp. 51-60, Academic Press, 1983.

[4] P. L. Montgomery, “ Modular multiplication without trial division, ” Math. Computation, vol. 44, pp. 519-521, 1985.

[5] Koc and C. Y. Hung, “ Bit-level Systolic Array for Modular Multiplication, ” Journal of VLSI Signal Processing, vol. 3, pp. 215-223, 1991.

[6] S. E. Eldridge and C. D. Walter, “ Hardware Implementation of Montgomery ’ s Modular Multiplication Algorithm, ” IEEE Transaction on Computers, vol. 42, no. 6, pp. 693-699, 1993.

[7] Colin D. Walter, “ Systolic Modular Multiplication, ” IEEE Trans. Computers, vol. 42, no. 3, Mar 1993.

[8] P.-S. Chen, S.-A. Hwang, and C.-W. Wu, “ A systolic RSA public key cryptosystem, ” in Proc. IEEE Int. Symp. Circuits and Systems (ISCAS), vol. 4, (Atlanta), pp. 408-411, May 1996.

[9] J.-H. Hong and C.-W. Wu, “ Radix-4 Modular Multiplication and Exponentiation Algorithms for the RSA Public-Key Cryptosystem, ” in Proc. Asia and South Pacific Design Automation Conf. (ASP-DAC), (Yokohama), pp. 565 -570, 2000.

[10] J.-H. Hong and C.-W. Wu, “ RSA public key crypto-processor core design and hierarchical system test using IEEE 1149 family, ” Phd Thesis, National Tsing-Hua University, Taiwan, June 2000.

[11] C.-C. Yang, T.-S. Chang, and C.-W. Jen, “ A new RSA cryptosystem hardware design based on Montgomery ’ s algorithm, ” IEEE Trans. Circuits and Systems II: Analog and Digital Signal Processing, vol. 45, no. 7, pp. 908-913, July 1998.

[12] F. Yingli, G. Zhiqiang, “ A New RSA Cryptosystem Hardware Implementation Based on High-Radix Montgomery ’ s Algorithm, ” 4th International ASIC conf., pp. 348 -351, 2001.

[13] Y.-H. Hsieh, “ Design and implementation of an RSA encryption /decryption processor on IC smart card, ” Master ’ s Thesis, National Taiwan University, Taiwan, June 1999.

[14] 曾希哲, “ RSA 加解密晶片之設計與分析, ” 國立海洋大學, 碩 士論文, 1999 [15] 吳哲漢, “ RSA 密碼系統之演算法研究與快速硬體實現, ” 雲林 科技大學, 碩士論文, 1999 [16] 李政德, “ 以Montgomery 演算法為基礎之RSA 密碼系統硬體 實作, ” 逢甲大學碩士論文, 2001 [17] 楊吳泉, “ 現代密碼學入門與程式設計, ” 全華科技圖書股份有 限公司, 1996.

[18] 賴溪松、韓亮、張真誠, “ 近代密碼學及其應用, ” 松崗電腦圖 書資料股份有限公司, 1995.

[19] 曾志光、巫坤品 譯, William Stallings 著, “ 密碼學與網路安全- 原理與實務(第二版), ” 碁峰資訊股份有限公司, 2001.

[20] 劉尊全, “ 數為時代密碼技術的現狀與未來, ” 松崗電腦圖書資 料股份有限公司, 2001.

[21] 曾志光、鄭光廷 譯, Patterson Hennessy 著 “ 計算機組織與設 計, ” 第二版 pp. 4-57~4-61, 碁峰資訊股份有限公司, 2002.

[22] Ribenboim, P. The New book of Prime Number Records. New York: Springer-Verlag, 1996.

[23] Kaliski, B., and Robshaw, M. “ The Secure Use of RSA. ” CryptoBytes, Autumn 1995.

[24] Wiener, M. “ Cryptanalysis of Short RSA Secret Exponents. ” IEEE Transactions on Information Theory, vol. IT-36, 1990.

[25] Kocher, P. “ Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other System. ” Proceedings, Crypto ’ 96, August 1996; published by Springer-Verlag.

[26] J.-J. Leu, and A.-Y. Wu, “ Design Methodology for Booth-Encoded Montgomery Module Design for RSA Cryptosystem, ” in Proc. IEEE International Symposium on Circuit and Systems, vol. 5, pp. 357-360, 2000.

[27] J.-H. Hong, and C.-W. Wu, “ Cellular Array Modular Multiplier for Fast RSA Public-Key Crypto-system Based on Modified Booth ’ s Algo-rithm, ” IEEE Trans. VLSI Systems, vol. 11, no.3, pp. 474-484, June 2003.

[28] 劉奇昌, “ 高效能RSA 密碼系統之硬體設計, ” 國立中正大學, 碩士論文, 2000.

[29] 劉俊麟, “ 以四為基底之高速RSA 加解密系統晶片, ” 大葉大學, 碩士論文,2002.

[30] C.-Y. Su, S.-A. Hwang, P.-S. Chen, and C.-W. Wu, “ An improved Montgomery's algorithm for high-speed RSA public-key cryptosystem, ” IEEE Trans. VLSI System, vol. 7, pp. 280-284, June 1999.

[31] S.-Y. Kung, VlSI Array Processors. Englewood Cliffs, New Jersey: Prentice-Hall Inc., 1988.