以四基底之高速RSA加解密系統晶片

劉俊麟、洪進華 ; 陳勛祥

E-mail: 9223665@mail.dyu.edu.tw

摘 要

現在已經進入了數位通訊的時代，大量的商業活動和個人信件，都經由網際網路來傳遞，因此資料保密、身分認證、數位簽署等安全需求便日益重要。RSA是1978年美國麻省理工學院 (MIT) 三位教授Rivest、Shamir及Adleman首先提出一種基於分解因數的指數函數密碼系統，為目前使用最廣泛的公開金鑰密碼系統。在RSA公鑰密碼系統中，每個使用者都擁有兩把鑰匙—公鑰與私鑰。公鑰公布給所有的人知道，私鑰則由自己秘密保存著。公鑰密碼系統的安全性在於幾乎無法由公鑰計算推導出私鑰，也就是靠這種計算不可行性 (computational infeasibility) 才得以保密。假如藉計算推導確實不易取得私鑰，那麼我們可以稱這系統是安全的。 RSA密碼系統就是利用大數因數分解相當困難的這個事實來製造公鑰與私鑰。基於安全性，隨著計算機技術的進步，金鑰的長度也不斷的增加。因 RSA 編解碼需做大量運算，當金鑰長度大於500位元時，比較適合以硬體來處理，以減低系統的負擔。　　本論文提出一個以四為基底的模乘法演算法，我們改善蒙哥馬利(Montgomery)演算法來設計模乘法器，並應用此模乘法器去實現一個 512 位元的 RSA 公開金鑰密碼系統晶片。本設計用 Avant! 0.35 μm standard cell library 來合成電路，並送至 CIC (國家晶片系統設計中心) 製作雛形晶片。本系統面積約六萬閘，當工作在 150 MHz 時脈時平均有196 Kbits/sec 的鮑率。

關鍵詞 : 蒙哥馬利演算法 ; 公開金鑰密碼系統 ; 模乘法

目錄

[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 Expoenets. ” 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.

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 Expoenets. ” 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.