[16]. M. Joye and S. M. Yen, "The Montgomery Powering Ladder," Cryptographic Hardware and Embedded Systems - CHES'2002, LNCS 2523, Springer-Verlag, pp. 291-302, 2003.

[17]. B. Chevallier-Mames, Mathieu Ciet, and Marc Joye, "Low-Cost Solutions for Preventing Simple Side-Channel Analysis：Side-Channel Atomicity," IEEE Trans. on Computers, vol. 53, no. 6, pp. 760-768, June 2004.

[18]. S. M. Yen, S. J. Kim, S. G. Lim and S. J. Moon, "RSA Speedup with Chinese Remainder Theorem Immune against Hardwarw Fault Cryptanalysis," IEEE Trans. on Computers, vol. 52, no. 4, pp. 461-472, Apr. 2003.

[19]. W. C. Yang, P. Y. Hsieh, and C. S. Laih, "Efficient Squaring of Large Integers," IEICE Transactions on Fundamentals, vol. E87-A, no. 5, pp. 1189-1192, May. 2004.

[20]. W. C. Yang, D. J. Guan, and C. S. Laih, "Fast Multi-Computations with Asynchronous Strategy," IEEE Trans. on Computers, vol. 56, no. 2, pp. 234-242, Feb. 2007.

[21]. W. C. Yang, "The Study of Multi-computation in Public Key Cryptography," Ph. D. dissertation of National Cheng Kung University, Jan. 2005.

[22]. D. C. Lou and C. C. Chang, "Fast exponentiation method obtained by folding the exponent in half," Electronics Letters, vol. 32, Issue 11, pp. 984-985, May 1996.

[23]. E. F. Brickelland, D. M. Gordon, K. S. McCurley, and D. Wilson, "Fast exponentiation with precomputation," Advances in Cryptology-Eurocrypt'92, LNCS 658, Springer-Verlag, pp. 200-207, 1992.

[24]. C. H. Lim and P. J. Lee, "More flexible exponentiation with precomputation," Advances in Cryptology-Crypto'94, LNCS 839, Springer-Verlag, pp. 95-107, 1994.

[25]. W. C. Yang, "New Strategy of Efficient SPA-resistant Exponentiations," The Fifth International Conference on Information Assurance and Security (IAS 2009), pp.348-351, 2009.08.

[26]. S. M. Yen, C. S. Laih, and A. K. Lenstra, "Multi-exponentiation," IEE Proceedings, Computers and Digital Techniques, vol. 141, no. 6, pp. 325-326, 1994.

Wu-Chuan Yang received his BS, MS, and Ph.D. degree all in Electrical Engineering from National Cheng Kung University, Tainan, Taiwan, in 1988, 1991, and 2006, respectively. From 1991 to 2005, he was with the Department of Electronic Engineering at Nan-Jeon Junior College of Technique and Commerce. In 2003, he obtained 2003 Annual Best Paper Award of JISE(Journal of Information Science and Engineering). From 2005 to 2007, he was with the Department of Technology Management at Aletheia University. Since 2007, he is an associate professor in the Department of Information Engineering at I-Shou University, located in Kaohsiung, Taiwan. His research interests include cryptography, algorithm, information security and software engineering.