[12] L. A. Tawalbeh, A. F. Tenca, and C. K. Koc,"A radix-4 scalable design," *IEEE Potentials*,vol.24, no.2, pp.16 – 18, 2005.

[13] C.K.Koc and C.Y.Hung, "Adaptive m-ary segmentation and canonical recoding algorithms for multiplication of large binary numbers," Computer mathematic application, vol.24, no.3, pp.3-12, 1992.

[14] B.Philips and N.Burgess, "Minimal weight digit set conversions," IEEE Trans. on computers, vol. 53, no.6 pp. 666-677, 2004.

[15] J.C. Ha, S.J. Moon, "A common-multiplicand method to the Montgomery algorithm for speeding up exponentiation," Information Processing Letters, vol.66, no.2, pp.105–107,1998.

[16] C.Wu, D.Lou and T.Chang, "An efficient Montgomery exponentiation algorithm for public-key cryptosystem," Proceedings of IEEE international conference on intelligence and security information, pp.284-285, June 2008.

[17] C.Wu, "An efficient common-multiplicand-multiplication method to the Montgomery algorithm for speeding up exponentiation," Information Sciences, vol.179, pp.410-421, 2009.

[18] L. Batina, et al. "Side channel attacks and fault attacks on cryptographic algorithm, " Revue HF Tijdschrift vol. 3, pp. 36-45, 2004.

 