World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:8, No:07, 2014

Low-Complexity Multiplication Using Complement and Signed-Digit Recoding Methods

Authors : Te-Jen Chang, I-Hui Pan, Ping-Sheng Huang, Shan-Jen Cheng

Abstract : In this paper, a fast multiplication computing method utilizing the complement representation method and canonical recoding technique is proposed. By performing complements and canonical recoding technique, the number of partial products can be reduced. Based on these techniques, we propose an algorithm that provides an efficient multiplication method. On average, our proposed algorithm is to reduce the number of k-bit additions from (0.25k+logk/k+2.5) to (k/6 +logk/k+2.5), where k is the bit-length of the multiplicand A and multiplier B. We can therefore efficiently speed up the overall performance of the multiplication. Moreover, if we use the new proposes to compute common-multiplicand multiplication, the computational complexity can be reduced from (0.5 k+2 logk/k+5) to (k/3+2 logk/k+5) k-bit additions.

Keywords : algorithm design, complexity analysis, canonical recoding, public key cryptography, common-multiplicand multiplication
Conference Title : ICISET 2014 : International Conference on Information Science, Engineering and Technology
Conference Location : Singapore, Singapore
Conference Dates : July 05-06, 2014