

Exponentiation Based on Binary-Fermat Number Representation

Vassil Dimitrov, Graham Jullien

ATIPS Laboratory, University of Calgary, Canada

Abstract: A new method for modular exponentiation based on representation of the exponent as a sum of products of Fermat numbers and powers of two is proposed. The algorithm can be effectively used in every cryptosystem based on $GF(2^n)$ arithmetic. The number of regular multiplications is 10% less than the best previously reported techniques. In terms of number of registers required for the algorithm, our approach is as good as the best methods found in the literature.

Resubmitted to IEEE Trans. on Computers

Index terms: Number Systems, Exponentiation, Cryptography, Computational Number Theory