Bit Forwarding 3-Bits Technique for Efficient Modular Exponentiation

Satyanarayana Vollala, National Institute of Technology, Tiruchirappalli, India
B. Shameedha Begum, National Institute of Technology, Tiruchirappalli, India
Amit D. Joshi, National Institute of Technology, Tiruchirappalli, India
N. Ramasubramanian, National Institute of Technology, Tiruchirappalli, India

ABSTRACT

It is widely recognized that the public-key cryptosystems are playing tremendously an important role for providing the security services. In majority of the cryptosystems the crucial arithmetic operation is modular exponentiation. It is composed of a series of modular multiplications. Hence, the performance of any cryptosystem is strongly depends on the efficient implementation of these operations. This paper presents the Bit Forwarding 3-bits(BFW3) technique for efficient implementation of modular exponentiation. The modular multiplication involved in BFW3 is evaluated with the help of Montgomery method. These techniques improves the performance by reducing the frequency of modular multiplications. Results shows that the BFW3 technique is able to reduce the frequency of multiplications by 18.20% for 1024-bit exponent. This reduction resulted in increased throughput of 18.11% in comparison with MME42_C2 at the cost of 1.09% extra area. The power consumption reduced by 8.53% thereby saving the energy up to 10.10%.

KEYWORDS

Bit Forwarding, Modular Exponentiation, Modular Multiplication, Montgomery Multiplication, Public-Key Cryptography

1. INTRODUCTION

It is widely recognized that security issues play a crucial role in the majority of today’s and the futures computer and communication systems. The explosive growth of data communications has made cryptographic algorithms and their implementations a crucial research topic to provide.

The need of security services such as confidentiality, authentication, data integrity, and/or non-repudiation. Public-key cryptosystem plays a crucial role for achieving higher level security (Stallings, 2003). The most popular public-key cryptosystems are Diffie-Hellman key exchange algorithm, Digital Signature Standard, RSA, and ElGamal public-key scheme. These schemes can be implemented in software as well as in hardware, but to provide adequate security and to achieve higher speed, hardware implementation will be the ultimate choice (Bar-El, 2002). All currently popular public key systems rely on modular exponentiation and modular multiplications (Batina, Örs, Preneel et al., 2003). A more serious challenge is to process the public-key cryptosystem in hardware, as it involves huge amount of computation, and there is a great demand for developing the efficient modular exponential and modular multiplication algorithms.

There are many well-known algorithms for modular exponentiation including binary method, the Mary method and sliding window method, but left-to-right binary method is extensively used.
for hardware implementation of modular exponentiation. This algorithm takes n+k number of modular multiplications for n-bit exponent, where k is the number of non-zero bits in the exponent. Sliding window method and M-ary methods increase the overhead and takes more space to store pre-computed values.

A significant problem is to devise modular exponential algorithms that takes less number of modular multiplications, so that the number of operational cycles to be reduced to improve the throughput without increasing the processor clock cycle speed, and power consumption can also be reduced. Cryptographic techniques can be implemented in software as well as in hardware. But hardware realization will be the ultimate choice for performance improvement and to attain higher level of security which is desirable in almost all the server based, banking, and military applications. This work proposes bit forwarding techniques for efficient implementation of modular exponential algorithms suitable for hardware implementation. Montgomery multiplication method is customized to suit the bit forwarding techniques and implemented with radix-2, named as Adaptable Montgomery Multiplication (AMM).

The content of this paper is structured as follows: Section 2 describes the brief work related to the public-key schemes, Montgomery multiplication and Modular exponentiation. Motivation is presented in Section 3, Proposed BFW3 algorithm is elaborated in section 4. Hardware realization of proposed algorithms is described in Section 5. Results and analysis is included in section 6. Finally, section 7 concludes the work.

2. LITERATURE REVIEW

To emphasis the relevance of the proposed work towards optimization of number of modular multiplications in modular exponential schemes, a detailed study of literature is made on existing modular exponential techniques, Montgomery method and presented in this section.

2.1. Public-Key Cryptography

To minimize the secure channel for exchanging the keys, Dieffie-Hellman introduced the theory of public-key cryptography (Diffie, & Hellman, 1976) first time in 1976, called as Diffie-Hellman key exchange algorithm. Two different but related keys are required for cryptographic transformations in public-key cryptography. One key is for encryption named public-key, another key is for decryption called private key or secrete key. The security of PKC is dependent on the difficulty of factoring the integers. The most well-known scheme called RSA was introduced by Rivest, Shamir and Adallman in 1978 (Rivest, Shamir, & Adleman, 1978). The encryption and decryption of RSA are both modular exponentiation \( \text{M}^E \mod N \) with different inputs. In Diffie-Hellman key exchange algorithm key generations are modular exponentiations like \( a \cdot b \mod N \) (Diffie, Van Oorschot, & Wiener, 1992). El Gamal proposed the El Gamal public-key scheme in 1985, applicable for both cryptographic transformations and digital signatures. In El Gamal scheme both key generation and cryptographic transformations involves modular exponentiations (El Gamal, 1984). For more security, the key length in all public-key schemes should be 1024-bits or greater. The central tool for all the public-key cryptographic schemes are modular exponentiation and modular multiplication. Computation of modular exponentiation in hardware with 1024-bit or of more bit length exponent is a challenging task.

2.2. Montgomery Multiplication

Modular multiplication is a complicated operation, these operations cannot be implemented directly in hardware, as it involves expensive trial division operations. To avoid this difficulty Peter L. Montgomery in 1985 has devised an efficient method to perform modular multiplication of two integers without trial divisions (Montgomery, 1985). His approach is based on residue number system,
Signature Restoration for Enhancing Robustness of FPGA IP Designs
www.igi-global.com/article/signature-restoration-for-enhancing-robustness-of-fpga-ip-designs/148302?camid=4v1a

A New Meta-Heuristic based on Human Renal Function for Detection and Filtering of SPAM
www.igi-global.com/article/a-new-meta-heuristic-based-on-human-renal-function-for-detection-and-filtering-of-spam/153528?camid=4v1a