

FPGA based DPA-resistant Unified Architecture for Signcryption

Yi Wang, Jussipekka Leiwo, Thambipillai Srikanthan and Yu Yu
Center for High Performance Embedded Systems, School of Computer Engineering
Nanyang Technological University, Singapore 639798

Abstract

Signcryption is a cryptographic primitive supporting both confidentiality and authentication. This paper proposes a DPA-resistant unified architecture for signing, encryption and signcryption with high performance and area-efficiency. Modular exponentiation is the main operation of RSA and ECC and also the key part of implementing signcryption. A unified signed adder is proposed to address the possible method to unify the modular exponentiation on $GF(p)$ field and $GF(2^p)$ field. Our simulation results show that the overall speed (maximum frequency of 1024 key length for RSA and 160 key length for ECC) can be increased approximately 28% of the existing design when our proposed design ported to FPGA with the utilization of 4355 CLBs.

1 Introduction

Signcryption is a cryptographic scheme providing confidentiality and authentication simultaneously, and the significant computation cost can be saved compared with "sign-then-encryption" scheme [7]. In this paper, we more concern about the public key cryptography as RSA [6] and ECC [5] and aim at a DPA-resistant unified hardware architecture.

2 Unified Architecture for Signcryption

A unified architecture for signcryption is proposed consisting of an encryption scheme, a signature scheme and signcryption scheme. $S = (SigGen, Sig, Ver)$, $E = (EncGen, Enc, Dec)$ and $SC = (Gen, SigEnc, VerDec)$ represents the signature, encryption and signcryption schemes respectively, where the sender is S and receiver is R . Therefore, it is possible to unify above three schemes into one as listed in Figure 1.

In Figure 1, we divide one security application into three levels: software level, firmware level and hardware

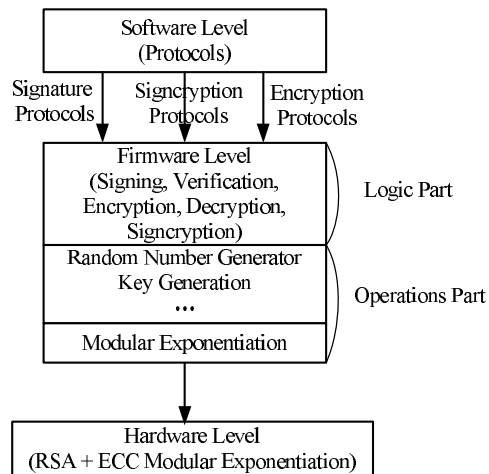


Figure 1. The overall architecture

level. The cryptographic protocols are at firmware level. Firmware level includes logic part and operations part, where the signing, encryption, and signcryption are at logic part and the key generation and the modular exponentiation are at operations part. Hardware level can support the operation part in firmware. Since modular exponentiation is main operation in RSA and ECC computations, we pick up this operation as an example to illustrate our proposed architecture.

3 DPA-resistant Public Key Cryptosystems

Public key cryptography provides the secure and authenticated communication in real world, where RSA and ECC are popularly used. But power analysis becomes a powerful attack to physical implementation of cryptographic algorithms.

In this paper, we are aiming at unified architecture for RSA and ECC with capability to resist DPA. The DPA-resistant algorithm for compute m^d is give in Algorithm 2 and Algorithm 1, where the $MM(A, B, M)$ and $MM(a(x), b(x), m(x))$ are the modular multiplication on $GF(p)$ field

and $GF(2^p)$ field respectively.

Algorithm 1. Algorithm to compute $s(x) = a(x) \cdot b(x)x^{-n} \bmod m(x)$ based on signed adder

Input: $a(x), b(x), m(x)$

Output: $s(x) = a(x) \cdot b(x)x^{-n} \bmod m(x)$

$a(x) = \sum_{i=0}^{n-1} a_i x^i, a_i \in GF(2), b(x) = \sum_{i=0}^{n-1} b_i x^i, b_i \in GF(2), m(x) = x^n + \sum_{i=0}^{n-1} m_i x^i, m_i \in \{0, 1\}$.

begin

$s(x)_0 = 0$;

for $i = 0$ *TO* $n - 1$ **do**

$s(x)_i = SXOR(s(x)_i, a_i b(x))$;

$q_i = s_0(x)_i$;

$s(x)_i = SXOR(s(x)_i, q_i m(x))$;

$s(x)_{i+1} = rightshift(s(x)_i)$

endfor

end

Algorithm 2. Algorithm to compute $A \cdot B \cdot R^{-1} \bmod M$ based on signed adder

Input: A, B, M

Output: $A \cdot B \cdot R^{-1} \bmod M$

$M = \sum_{i=0}^{n-1} 2^i m_i, m_i \in \{0, 1\}, B = \sum_{i=0}^{n-1} 2^i b_i, b_i \in \{0, 1\}, A = \sum_{i=0}^{n-1} 2^i a_i, a_i \in \{0, 1\}, A, B < M; M < R = 2^n; M' = -M^{-1} \bmod 2 = M; gcd(2, M) = 1$.

begin

$S_0 = 0$;

for $i = 0$ *TO* $n - 1$ **do**

$\tilde{S}_i = SADD(\tilde{S}_i, a_i B)$;

$q_i = \tilde{S}_{i0}$;

$\tilde{S}_i = SADD(\tilde{S}_i, q_i M)$;

$\tilde{S}_{i+1} = rightshift(\tilde{S}_i)$;

endfor

$S_n = convert(\tilde{S}_n)$;

end

The SXOR operation in Algorithm 1 and SADD operation in Algorithm 2 represent two functions of signed adder.

4 Results

We use VHDL coding, Synplify synthesis, Xilinx Virtex-E2000 devices for implementing the proposed unified architecture. Table 1 shows the computation time of modular exponentiation compared with previous alternatives.

Table 1. Modular exponentiation results

| | Operand Size(bits) | Operation Time(ms) | Clock Rate (MHZ) |
|-----------------|--------------------|--------------------|------------------|
| Goodman [3] | 1024/512 | 32.1/8.2 | 50 |
| Blum [1] | 1024/512 | 40.05/9.38 | 45.6 |
| Kim [4] | 1024 | 58.9 | 28 |
| Cilardo[2] | 1024 | 27.36 | 77.3 |
| Proposed Method | 1024/512 | 20.92/5.24 | 100.4 |

5 Conclusions

A DPA-resistant unified architecture for signing, encryption and signcryption is proposed to achieve high performance and area efficiency when ported to FPGA. Signcryption scheme becomes more and more hot topic in providing both confidentiality and authentication compared with previous method "sign-then-encryption" scheme. The DPA-resistant modular exponentiation has been proposed and a unified signed adder for modular multiplication on $GF(p)$ field and $GF(2^p)$ field has been applied to modular exponentiation for RSA and ECC. Our analysis shows that the whole design can reach the 100.4MHZ with the utilization of 4355 CLBs, and the speed of our design is 22.99% faster than Cilardo' one [2] and the area of our design is 35.09% smaller than his when ported to Virtex-E2000.

References

- [1] T. Blum and C. Paar. Brief contributions: high-radix Montgomery modular exponentiation on reconfigurable hardware. *IEEE Transactions on Computers*, 50(7):759–764, July 2001.
- [2] A. Cilardo, A. Mazzeo, N. Mazzocca, and L. Romano. A novel unified architecture for public-key cryptography. *DATE'05*, 3, 2005.
- [3] J. Goodman and A. P. Chandrakasan. An energy-efficient reconfigurable public-key cryptography processor. *IEEE Journal of Solid-State Circuit*, 36(11):1808–1820, Nov. 2001.
- [4] C. K. Kim, J. C. Ha, S. H. Kim, and S. Kim. A secure and practical CRT-based RSA to resist side channel attacks. *ICCSA 2004, LNCS 3043, Springer-Verlag*, pages 150–158, 2004.
- [5] P. L. Montgomery. Speeding the pollard and elliptic curve methods for factorizations. *Mathematics of Computation*, 48, 1987.
- [6] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.
- [7] Y. Zheng. Digital signcryption or how to achieve cost(signature & encryption) \ll cost(signature) + cost(encryption). *In Advance in Cryptology - CRYPTO'97, LNCS 1294. Springer-Verlag*, pages 165–179, 1997.