ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

# FPGA Design and Implementation of Secure Dual-Core Crypto Processor

J.Prabawathi[1], Mr.R.S.Karthic[2]

PG Scholar (M.E., VLSI Design), PSNA college of engineering and technology, Dindigul, Tamilnadu, India[1]

Assistant Professor, Dept. of ECE, PSNA college of engineering and technology, Dindigul, Tamilnadu, India[2]

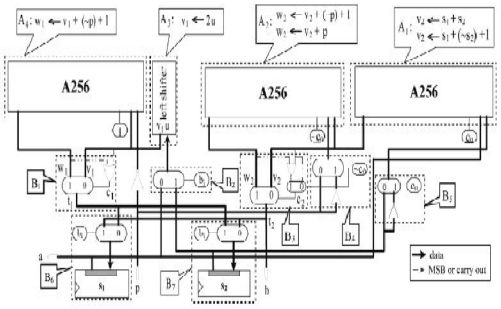
***Abstract*—This paper is devoted to the design and the physical security of a parallel dual-core flexible crypto processor for computing pairings over Barreto-Naehrig (BN) curves. The proposed design is specifically optimized for field-programmable gate-array (FPGA) platforms. The design explores the in-built features of an FPGA device for achieving an efficient crypto processor for computing 128-bit secure pairings. The work further pinpoints the vulnerability of those pairing computations against side-channel attacks and demonstrates experimentally that power consumptions of such devices can be used to attack these ciphers. Finally, we suggest a suitable countermeasure to overcome the respective weaknesses.**

## I. INTRODUCTION

Bilinear pairing first used in cryptography independently by Mitsunari *et al.* [7], Sakai *et al.* [8], and Joux [9] in 2000. One year later, Boneh and Franklin solved a long lasting problem of identity-based cryptography [10] based on pairing. Since then an impressive number of proposals arrived in the literature for designing cryptographic protocols based on pairings [11]. On the other hand, steep growth of the adversary's computation power demands increasing bit security in cryptographic protocols running in these applications. Practice has shown that one of the most efficient options to compute pairings for high bit security is to resort to Tate pairing operating on Barreto-Naehrig (BN) curves[12] defined over a 256-bit prime field having embedding degree k=12 .

Efficient computation of Tate pairing with linear complexity with respect to the size of the input was introduced long back in 1986 by Miller [13]. Significant improvements and the generalization of Miller's algorithm were independently proposed in 2002 by Barreto *et al.* [14] and Galbraith *et al.* [15]. Thereafter, intensive research has been carried out for further improvement. In this paper, we extend the work presented in [16] and propose a pairing crypto processor for BN curves. The design is flexible and resistant to side-channel attack. FPGA is one of the suitable platforms for implementing cryptographic algorithms. This paper proposes new implementation techniques of addition and multiplication on FPGAs. The in-built features available inside an FPGA device have been utilized to develop a high-speed 256-bit adder circuit. We show that when utilizing such adder circuits and adopting a parallelism technique, the multiplication in can be substantially improved. Based on such arithmetic cores, we develop a parallel configurable hardware for computing addition, subtraction, and multiplication. Existing techniques to speed up arithmetic in extension fields (see [17] and [18]) for fast computation in and are used on top of it.

## II.PROPOSED SYSTEM ARCHITECTURE




We propose an Lopez–Dahab scalar point multiplication architecture such that logic structures are

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

implemented in parallel and operations in the critical path are diverted to noncritical paths.

Scalar multiplication is by far the most important operation in elliptic curve cryptosystems. ECSM is an operation which, on input an integer *k* and a point *P* on an elliptic curve *C*, computes another point *Q* such that *Q* = *kP*. In our ECSM architecture, we use a variant of the algorithm due to Lopez and Dahab, which is an improvement of the traditional Montgomery ECSM algorithm [3]. The algorithm consists of three stages: 1) conversion of *P* from affine coordinate to projective coordinate; 2) computation of *Q* = *kP* in projective coordinate; and 3) conversion of *Q* from projective coordinate back to affine coordinate. The most important operations for designing an efficient ECC processor are finite field multiplication, inversion, and squaring. Field addition and subtraction in GF(2*m)* are not investigated since they are defined as polynomial addition and can be implemented simply as the XOR addition of the two *m*-bit operands [1]. Finite-field squarer over GF(2163*)* has been designed based on the proposal presented in [4]. For finite field multiplication, we have designed an efficient least significant digit finite-field multiplier as proposed in [5]. For inversion, an efficient inverter based on the Itoh–Tsujii multiplicative inverse algorithm [6] has been implemented. For the design of the architecture for ECSM, two different parts are considered: the first part involves calculations in the projective coordinate system, and the other part involves the calculations for converting projective coordinates to affine coordinates. For the projective calculations,parts 1 and 2 of the LD algorithm are considered. In the design of this part of the processor, as proposed in [7], the number of computational units is chosen in such a way that allows parallel computations to be performed. Hence, we use three field multipliers to implement the main loop of the algorithm in which point addition and doubling is carried out. So, according to Section 2.1 of the LD algorithm, in the the first stage, three multiplications *X*1 *Z*2, *X*2 *Z*1, and *T Z*2(*T* → *X*2) are performed in parallel by using three multipliers, and then three other multiplications *x p Z*1, *X*1*X*2*T Z*2 *(T* ← *Z*1*)*, and *bZ*4 2 are accomplished in parallel in the second stage, as shown in Fig. 1. Hence, the delay of each iteration is reduced from six field multiplication delays to two field multiplications delays. As mentioned, the most important modules in the design of an ECSM are the field multiplier, the field inverter, and the field squarer. The key point here is that the critical path must be placed on the longest path among these modules. Since in our design the inverter module is designed in such a way that its critical path coincides with that of the multiplier's and, since the multiplier's path is longer than the squarer's path, the critical path needs to be placed on the multiplier. Another important strategy in the design of the architecture for the projective calculations unit is that separate calculations are not performed for the use of the initial values of part 1 of the LD algorithm, because if further computational modules are designed for these calculations, the complexity of the critical path and the amount of required area will be increased.

*2.1.Stages in LD Algorithm:*

The algorithm consists of three stages:

- ✓ Conversion of P from affine coordinate to projective coordinate;
- ✓ Computation of Q = kP in projective coordinate; and
- ✓ Conversion of Q from projective coordinate back to affine coordinate.
- For the design of the architecture for ECSM, two different parts are considered: the first part involves calculations in the projective coordinate system(X1,X2,Z1 and Z2), and the other part involves the calculations for converting projective coordinates to affine coordinates($x_p$ , $y_p$ ).

*2.2.Computation of projective coordinate system(X1,X2,Z1 and Z2) for MSB=1*

- Assign initial values for X1,X2,Z1 and Z2.
- Consider a point 'P' on the curve 'C' is xp=4; yp=3;
- //initial values of LD algorithm
- X1=1; Z1=0;
- X2=xp; Z2=1;
- Let T=Z1;
- Z1=(X1*Z2+X2*Z1)^2;
- X1=xp*Z1+X1*X2*T*Z2;
- T=X2;
- Z2=T^2*Z2^2;
- b=1;//constant integer

X2=X2^4+b*Z2^4;

- According LD algorithm, in the the first stage, three multiplications X1 Z2, X2 Z1, and T $Z_2$

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

(T → X2) are performed in parallel by using three multipliers, and then three other multiplications x p Z1, X1X2T $Z_2$ (T ← Z1), and $bz_2^4$ are accomplished in parallel in the second stage,

- Hence, the delay of each iteration is reduced from six field multiplication delays to two field multiplications delays.

*2.3.Computation of projective coordinate system(X1,X2,Z1 and Z2) for MSB=0*

- Assign initial values for X1,X2,Z1 and Z2.
- Consider a point 'P' on the curve 'C' is xp=4; yp=3;
- //initial values of LD algorithm
- X1=1; Z1=0;
- X2=xp; Z2=1;
- Let T=Z2;
- Z2=(X1*Z2+X2*Z1)^2;
- X2=xp*Z2+X1*X2*T*Z1;
- T=X1;
- X1=X1^4+b*Z1^4;
- Z1=T^2*Z1^2

b=1;//constant integer

*2.4.Flow of LD Algorithm:*

INPUT: $k = (k_{t-1}, \ldots, k_1, k_0)_2$ with $k_{t-1} = 1$, $P = (x_P, y_P) \in E(F_2^m)$.
OUTPUT: $Q = kP = (x_3, y_3)$.
/*Affine to Projective */
1. $X_1 \leftarrow x_P$ $Z_1 \leftarrow 1$, $X_2 \leftarrow x_P^4 + b$, $Z_2 \leftarrow x_P^2$. {Compute (P,2P)}
/* Projective Scalar Multiplication */
2. For $i$ from $t-2$ downto 0 do
2.1 If $k_i = 1$ then
$T \leftarrow Z_1$, $Z_1 \leftarrow (X_1Z_2 + X_2Z_1)^2$, $X_1 \leftarrow x_P Z_1 + X_1X_2TZ_2$.
$T \leftarrow X_2$, $X_2 \leftarrow X_2^4 + bZ_2^4$, $Z_2 \leftarrow T^2Z_2^2$.
2.2 Else
$T \leftarrow Z_2$, $Z_2 \leftarrow (X_1Z_2 + X_2Z_1)^2$, $X_2 \leftarrow x_P Z_2 + X_1X_2Z_1T$.
$T \leftarrow X_1$, $X_1 \leftarrow X_1^4 + bZ_1^4$, $Z_1 \leftarrow T^2Z_1^2$.
/*Projective to Affine*/
3. $x_3 \leftarrow X_1/Z_1$.
4. $y_3 \leftarrow (x_P + X_1/Z_1)[(X_1 + x_P Z_1)(X_2 + x_P Z_2) + (x_P^2 + y)(Z_1 Z_2)](x_P Z_1 Z_2)^{-1} + y_P$.
5. Return $(x_3, y_3)$

## III. SIMULATION RESULTS

The proposed sphere decoder architecture is designed using verilog HDL,simulated using modelsim software and synthesized using Xilinx project navigator.The RTL schematic view is illustrated in fig 1 and its technology schematic view is displayed in fig 2.

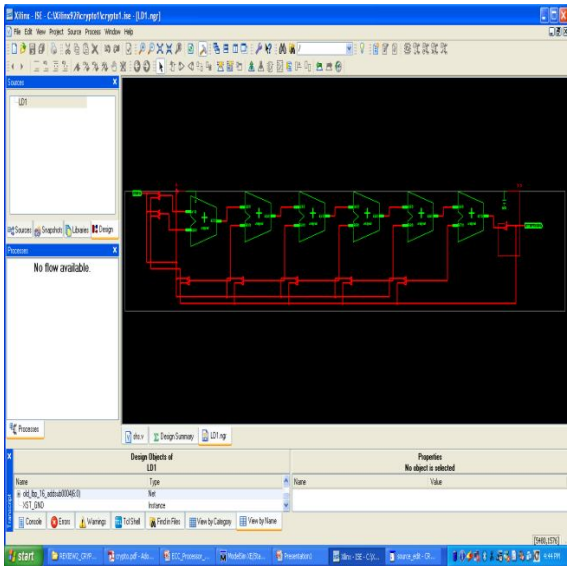


Fig1.RTL Schematic View

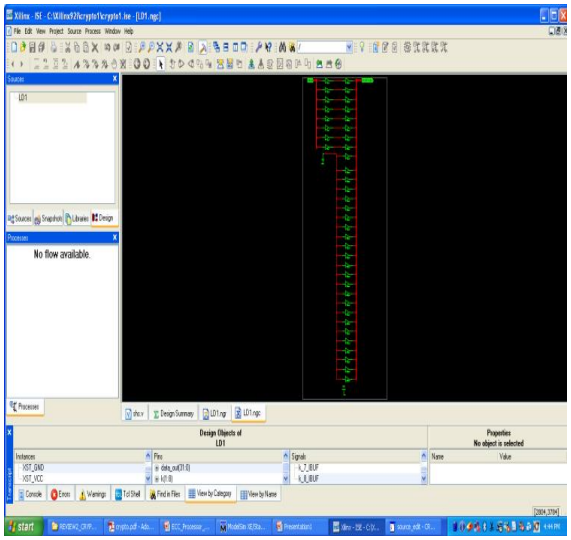


Fig2.Technology Schematic View

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

## Performance Analysis Graph:

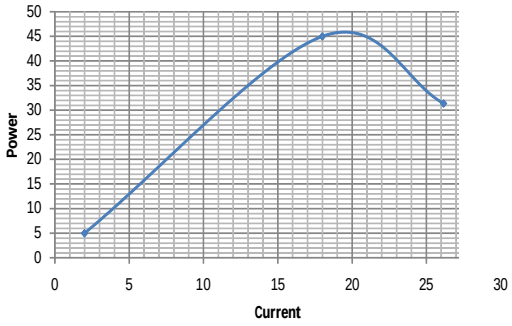



Fig3.Performance Analysis Graph

## Performance Analysis:

| Parameters | Current | Power |
|---|---|---|
| Quiescent form | 26.15mA | 31.37mW |
| Quiescent Vccaux at 2.5v | 18mA | 45mW |
| Quiescent Vcc025 at 2.5v | 2mA | 5mW |

Fig4.Performance Analysis

## REFERENCES

[1] F. Rodriguez-Henriquez, N. A. Saqib, A. D. Pérez, and C. K. Koc, *Cryptographic Algorithms on Reconfigurable Hardware*. New York: Springer-Verlag, 2006.

[2] J. Lopez and R. Dahab, "Fast multiplication on elliptic curves over GF(2m) without precomputation," in *Proc. 1st Int. Workshop Cryptograph.Hardw. Embedded Syst.*, 1999, pp. 316–327.

[3] D. Yong-Ping, Z. Xue-Cheng, L. Zheng-Lin, H. Yu, and Y. Li-Hua,"High-performance hardware architecture of elliptic curve cryptography processor over GF(2163)," *J. Zhejiang Univ. Sci. A*, vol. 10, no. 2, pp. 301–310, 2009.

[4] S. Kummar, T. Wollinger, and C. Paar, "Optimum digit serial GF(2m) multipliers for curve based cryptography," *IEEE Trans. Comput.*, vol. 55, no. 10, pp. 1306–1311, Oct. 2006.

[5] T. Itoh and S. Tsujii, "A fast algorithm for computing multiplicative inverses in GF(2m) using normal basis," *J. Inf. Comput.*, vol. 78, no. 3,pp. 171–177, 1988.

[6] C. H. Kim, S. Kwon, and C. P. Hong, "FPGA implementation of high performance elliptic curve cryptographic processor over GF(2163)," *J.Syst. Archit.*, vol. 54, no. 10, pp. 893–900, 2008.

[7] S. Mitsunari, R. Sakai, and M. Kasahara, "A new traitor tracing,"*IEICE Trans. Fundam.*, vol. 2, pp. 481–484, 2002.

[8] R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairing," in *Proc. SCIS*, 2000, pp. 26–28.

[9] A. Joux, "A one round protocol for tripartite diffie–hellman," in *Proc.ANTS*, 2000, pp. 385–394.

[10] D. Boneh andM.K. Franklin, "Identity based encryption fromtheWeil pairing," in *CRYPTO 2001, LNCS 2139*, 2001, pp. 213–229.

[11] R. Dutta, R. Barua, and P. Sarkar, "Pairing-based cryptographic protocols:A survey," Cryptology ePrint Archive, Tech. Rep. 2004/64, 2004.[Online]. Available: http://eprint.iacr.org.

[12] P. S. L. M. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order," in *SAC'05 LNCS 3897*, 2006, pp. 319–331.

[13] V. S. Miller, "The weil pairing, and its efficient calculation," *J. Cryptology*,vol. 17, pp. 235–261, 2004.

[14] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing–based cryptosystems," in *CRYPTO '02, LNCS 2442*,2002, pp. 354–368.

[15] S. D. Galbraith, K. Harrison, and D. Soldera, "Implementing the tate pairing," in *Proc. ANTS*, 2002, pp. 324–337.

[16] F. Vercauteren, "Optimal pairings," *IEEE Trans. Inf. Theory*, vol. 56,no. 1, pp. 455–461, Jan. 2010.

[17] A. J. Devegili, M. Scott, and R. Dahab, "Implementing cryptographic pairings over Barreto-Naehrig curves," *Pairing '07. LNCS 4575*, pp.197–207, 2007.

[18] A. Devegili, C. ÓhÉigeartaigh,M. Scott, and R.Dahab, "Multiplication and squaring on pairing-friendly fields," Cryptology ePrint Archive,Tech. Rep. 2006/471, 2006.