Design and Analysis of Pairing Based Cryptographic Hardware for Prime Fields

Santosh Ghosh
Department of Computer Sc. & Engineering, IIT Kharagpur, West Bengal, India, 721302.
Advisors: Dr. Debdeep Mukhopadhyay and Prof. Dr. Dipanwita Roy Chowdhury
{santosh}@cse.iitkgp.ernet.in

***Abstract*— This work deals with the design and implementation of pairing based cryptographic hardware and its security analysis against side-channel and fault attacks.**

1. Introduction

CRYPTOGRAPHIC HARDWARE is an emerging area of research where primary challenge lies in coping with progressively strong physical attacks commonly referred to as side-channel or covert-channel analysis. In general, a cryptographic scheme is developed against traditional algebraic attacks. On the other hand, a VLSI designer normally optimizes a hardware with respect to time, area, and power only. Let us consider a scenario depicted in Fig. 1. The decryption function $\mathcal{D}$ is assumed to be mathematically secure which is executed on an optimized cryptoprocessor. Instead of primary input/output, the cryptoprocessor releases several unwanted information through covert channels which are normally neglected by the design engineers. These hidden or side channels could be exploited to perform an attack on the decryption function, which differentiates cryptographic hardware from other hardwares. This type of attacks are commonly known as side-channel attacks which are applied physically on a cryptoprocessor during its execution. Designing cryptographic hardware against these physical attacks explores an area of research which is an overlap of cryptography and VLSI design.

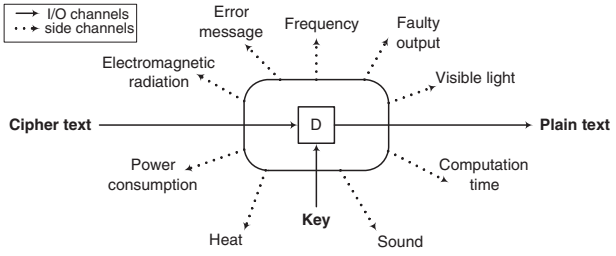

Fig. 1. Decryption on a cryptoprocessor.

2. Motivation and Scopes

The current dissertation [1] deals with the hardware design techniques of a relatively new cryptographic function known as *pairing* using which Boneh and Franklin [2] have solved a several years' open problem of *identity based cryptography* in 2001. A new area in this regard is identified as *pairing based cryptography*. Two complex operations are elliptic curve scalar multiplication (ECSM) and pairing computation which are often used in pairing based cryptographic schemes. Field programmable gate array (or FPGA) is one of the suitable platforms to develop hardware for accelerating cryptographic operations. Thus, it may be prudent at this point to look into the architecture design techniques on FPGA platform to improve the efficiency of ECSM and pairing computation.

Finite field arithmetic is the most important primitive of ECSM and pairing computation. Pairing based cryptography requires all the underlying finite field operations like addition, subtraction, multiplication, inversion, and division. In order to obtain an efficient design, the present work first focusses on introducing hardware sharing among the finite field operations. Modern FPGAs provide in-built features which may help in realizing optimized circuits. Thus, the proposed work also investigates FPGA features to accelerate the finite field primitives. Subsequently, the work focuses on exploiting scopes of parallelism in the finite field algorithms. It further explores the scope of parallelism in the computation of ECSM and pairing using multiple cores of underlying primitives.

On the other hand, as described before, the side-channel and fault attacks are two major threats on the implementation of a cryptographic algorithm. This is owing to the fact that the vulnerabilities of elliptic curve and pairing cryptoprocessors against actual attacks can be explored to furnish the scope of the current thesis. Thus, the algorithmic modifications and new counteracting techniques at different levels of pairing based cryptographic schemes are explored. Alongside, the effect of these techniques on the entire design and the final robustness of the design is evaluated.

3. Proposed Work

The overall contribution of current work is summed up concisely in this paper.

3.1. Design and Analysis of Elliptic Curve Cryptoprocessor

An elliptic curve cryptoprocessor is proposed by exploiting the concept of shared arithmetic hardware and explore its security against timing and power attacks. The contribution of this work is in three folds.

- **PGAU core:** It proposes a Programmable GF(p) Arithmetic Unit (PGAU) that performs GF(p) addition, subtraction, multiplication, inversion, and division. The PGAU reduces 18% area compared to that required of an integrated design where each arithmetic unit is a state-of-the-art stand alone implementation. The PGAU takes only 0.96 times slice area and achieves 2.67 times speedup compared to the GF(p) ALU described in [4].
- **ECC cryptoprocessor:** The saving in area of PGAU core is utilized to speed up the ECSM operation by developing an elliptic curve cryptoprocessor consisting of two PGAU-cores. The experimental result shows that

978-0-7695-4447-2/11 $26.00 © 2011 IEEE
DOI 10.1109/ISVLSI.2011.39

the proposed cryptoprocessor computes a 192-bit ECSM operation in $4.47ms$. The whole design demands 8972 CLB slices and runs at $43MHz$ on a Virtex-2 Pro FPGA. The same can run at $61MHz$ on a Virtex-4 FPGA.

- **Side-channel attacks:** It proposes a point blinding technique against DPA as well as doubling attack. Experimental results show that the proposed cryptoprocessor is secure against timing, SPA, DPA, and doubling attacks.

3.2. Fast $\mathbb{F}_p$ Adders and Multipliers on FPGA Platform

Finite field addition and multiplication are the most important operations in cryptography. Efficient techniques of these operations greatly affect the overall performance of a cryptoprocessor. This work explores the in-built features of an FPGA device to develop high-speed $\mathbb{F}_p$-primitives. The contributions of this research are briefly described here.

- **Fast carry chain (FCC):** FPGA provides special carry logic for addition. Through experimental results this work shows that the carry propagation adder (CPA) based on in-built carry logic for a 32-bit addition provides the minimum latency compared to all other known addition techniques. Experimental results show that the latency of CPA is only $6.6ns$ whereas the same of carry lookahead adder is $9.2ns$ on a Virtex-2 pro FPGA.
- **High-speed adder:** A hierarchical adder structure is proposed for large operands using above fast carry chain (FCC). The large operands are decomposed hierarchically upto 32-bit lengths based on Karatsuba technique. The experimental result shows that the proposed 256-bit adder provides 35% speedup from the best known technique [3].
- **$\mathbb{F}_p$-multiplier:** It exploits Montgomery ladder for improving the scope of parallelism of interleaved multiplication algorithm. Based on the high speed adders and the modified interleaved algorithm, we propose a parallel iterative architecture for $\mathbb{F}_p$-multiplication. Experimental results show 70% performance improvement over existing design and security against timing and SPA attacks.
- **Speedup of ECC cryptoprocessor:** In order to validate the proposed techniques, we redesigned the ECC cryptoprocessor based on the developed fast $\mathbb{F}_p$-primitives. The design is validated by matching the results with the previous ECC cryptoprocessor. Experimental results show that the modified design achieves 30% speedup.

3.3. High Speed Flexible Pairing Cryptoprocessor

This research proposes a cryptoprocessor for the computation of pairings over Barreto-Naehrig curves (BN curves). The BN curve : $Y^2 = X^3 + 3$ is defined over $\mathbb{F}_p$ with embedding degree k = 12. The major contributions of this work are highlighted here.

- **CFP design:** It introduces a configurable $\mathbb{F}_{p^k}$-primitive (CFP) based on the high-speed $\mathbb{F}_p$-primitives described above. The CFP has inherent configurability to perform arithmetic in $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ for any p less than the given length. Existing techniques to speed up arithmetic in extension fields for fast computation in $\mathbb{F}_{p^6}$ and $\mathbb{F}_{p^{12}}$ are implemented on top of it.
- **Pairing cryptoprocessor:** A pairing cryptoprocessor is designed with two CFP-cores. The advantages of dual core have been utilized by developing a parallel scheduling of the underlying $\mathbb{F}_p$-operations for pairing computation. The proposed cryptoprocessor also provides flexibility for curve parameters. Experimental results show a significant improvement in clock cycle counts for pairing computations compared to the similar design reported in [6]. Due to the above factor the speed of the proposed cryptoprocessor on a FPGA platform is comparable with the existing CMOS design.

The proposed configurable $\mathbb{F}_{p^k}$ arithmetic cores and parallel computation result in a significant improvement of the performance of Tate, ate, and R-ate pairing over BN curves.

3.4. Pairing Computations Against Fault and Power Attacks

This research deals with the fault and side-channel attacks on pairing computations which is another objective of this thesis. The contributions of this work are summarized here.

- **Fault attack on pairing:** The fault attacks on pairing computations described in [5] assumes that the fault is injected into a specific register. In this regard this work depicts an actual fault injection technique into a register by tuning the clock frequency of an FPGA prototype. It pinpoints the limitations of existing countermeasures against fault attacks. The work also proposes a new countermeasure to defend the same attack.
- **Fault attack on Miller's algorithm:** This work explores a vulnerability of the Miller's algorithm against fault attack. We propose an attack on pairing computations over BN curves and Edwards coordinates. A suitable technique is also proposed to counteract against such attack.
- **DPA on pairing:** The work discusses a DPA technique on pairing computations over $\mathbb{F}_p$. The vulnerability is suitably supported by experimental results on FPGA. A suitable technique is also proposed to counteract against such power attack.

4. Conclusion

In this work we explored the efficient design techniques of pairing cryptoprocessors exploiting inherent FPGA features. The work further addressed the security of proposed designs against side-channel attacks.

References

[1] S. Ghosh. Design and analysis of pairing based cryptographic hardware for prime fields. PhD thesis, 2011. http://www.facweb.iitkgp.ernet.in/∼drc/thesis/santosh_phd_thesis.pdf.

[2] D. Boneh and M.K. Franklin. Identity-based encryption from the Weil pairing. CRYPTO 2001, LNCS 2139, pp. 213–229, Springer, 2001.

[3] S. Hauck, M.M. Hosler, and T.W. Fry. High-performance carry chains for FPGAs. FPGA 98, pp. 223-233, 1998.

[4] A. Daly, W. Marnane, T. Kerins, and E. Popovici. An FPGA implementation of a GF(*p*) ALU for encryption processors. Microprocessors and Microsystems, Vol. 28, pp. 253–260, 2004.

[5] D. Page and F. Vercauteren. A Fault Attack on Pairing-Based Cryptography. IEEE TC, Vol. 55, No. 9, pp. 1075–1080, 2006.

[6] D. Kammler, D. Zhang, P. Schwabe, H. Scharwaechter, M. Langenberg, D. Auras, G. Ascheid, and R. Mathar. Designing an ASIP for cryptographic pairings over Barreto-Naehrig curves. CHES 2009, LNCS 5747, pp. 254–271, 2009.