Chapter 1

Introduction

BILINEAR PAIRING is a candidate for one-way functions defined on elliptic or hyperelliptic curve group. Pairing based cryptography is suitable for securing identity aware and ubiquitous computing devices. Major operations in pairing based cryptography are pairing computation and elliptic curve scalar multiplication. This research focuses on designing efficient hardware architectures for above mentioned operations on FPGA platform. Implementations of the respective algorithms may leak secret information during their execution through concealed channels, such as: power consumption, timing, and faults. The attacks based on the exploitation of such concealed channels are known as side-channel attacks. This research also focuses on the analysis and counteracts of elliptic curve and pairing implementations against side-channel attacks.

1.1 Motivation and Objective

In recent times, Pairing-based cryptography has attained lot of importance. As a natural consequence, its hardware implementation is extremely important. The implementations must be cost-effective, both in terms of time and space requirement. This thesis focuses on exploring several hardware design techniques which are employed in pairing based cryptography. Two complex operations are elliptic curve scalar multiplication (or 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 architectural 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, side-channel and fault attacks are the major threats on the implementation of any cryptographic algorithms. The present thesis explores not only these vulnerabilities but also counteracting techniques of pairing schemes. Finally, the effect of these techniques on the entire design and the final robustness of the design is evaluated.

In this thesis two broad aspects of the hardware for pairing based cryptography, namely, efficient implementation and security against side-channel attacks, have been separately studied. One of the main objectives of this thesis is to reduce the computation time of major operations of a pairing based scheme. This reduction in computation time is brought about by targeting the following aspects of FPGA implementation:

- Hardware sharing technique has been explored to develop an optimized programmable architecture for prime field arithmetic.
- The in-built carry chains of an FPGA device have been exploited to develop a high-speed adder circuit.
- A modified interleaved multiplication technique has been proposed to reduce the critical path of a prime field multiplier.
- Multiple functional cores have been incorporated into the proposed cryptoprocessors

for exploiting the parallelism of ECSM and pairing computations.

One more objective of this thesis is to provide the security of the proposed designs against side-channel attacks. In that respect the following techniques have been proposed:

- The proposed finite field primitives help to make the cryptoprocessors resistant against simple side-channel attacks.
- A new point blinding technique has been proposed which protects the secret parameter of ECSM operation against *simple power analysis* (SPA), *differential power analysis* (DPA), and *doubling attack* (DA).
- A new counteracting technique has been proposed to defend the fault attacks against pairing computations.
- Line function of pairings has been modified to defend differential power attacks.

1.2 Contributions

The contributions of the thesis are summarized below:

- **Design and Analysis of Elliptic Curve Cryptoprocessor.** We present an elliptic curve cryptoprocessor 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.

    1. **PGAU core:** We propose a Programmable GF(p) Arithmetic Unit (PGAU) that performs GF(p) addition, subtraction, multiplication, inversion, and division. The modular operations are performed directly in 2's complement number system. 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 but achieves 2.67 times speedup compared to the existing design [**?**].

2. **Elliptic curve cryptoprocessor:** We observe that the saving in area can be exploited by using multiple copies of PGAU for accelerating elliptic curve scalar multiplication. Thus, we attempt to speed up the ECSM operation by using two PGAU cores. The implementation of the proposed design is done on Xilinx Virtex-II Pro FPGA device. The experimental result shows that the proposed elliptic curve cryptoprocessor computes a 192-bit ECSM operation in $4.47ms$. The whole design demands 8972 CLB slices and runs at $43MHz$ clock on a Virtex-II Pro FPGA. The same can run at $61MHz$ clock on a Virtex-IV FPGA platform.

3. **Side-channel attacks:** The PGAU is designed in such a way that it does not provide any timing and power attack vulnerabilities during the execution of finite field operations. A new point blinding technique is proposed which is applied on the SPA resistant Montgomery ladder for ECSM computation. The analysis shows that the proposed cryptoprocessor is indeed secure against differential and non-differential timing and power attacks. In order to show its security against differential power analysis (or DPA) we first show an actual DPA result on an FPGA implementation without any DPA resistance scheme. This result ensures that the DPA is really capable to obtain the secret scalar multiplier. The same analysis have been performed on our proposed implementation. It is shown that with even ten times more power traces we could not find any significant DPA peak to guess the secret bits. The result ensures that the proposed design is capable to protect the secret against DPA attack. The proposed design is also capable to provide security against *doubling attack*.

- **Fast Prime Field 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. We explore the in-built features of an FPGA device to develop high-speed *prime field* (F_p) primitives. The contributions of this work are briefly described here.

  1. **Fast carry chain (FCC):** Modern FPGAs provide special carry logic for addition. The carry chains formed by the in-built carry logic are 32 bits long.

Through experimental results this chapter shows that the carry propagation adder (CPA) based on in-built carry logic for a 32-bit addition provides minimum latency compared to all other known addition techniques. Experimental results show that the latency of above CPA is only 6.6*ns* whereas the same of the carry lookahead adder is 9.2*ns* on a Virtex-II pro FPGA.

2. **High-speed adder:** Subsequently, we propose a hierarchical adder structure for large operands using above fast carry chains (FCCs). The large operands are decomposed hierarchically upto 32 bit-lengths based on Karatsuba technique. The experimental result shows that the proposed technique significantly reduces the routing delay as well as logic delay compared to the existing techniques. For a comparison we implement some existing addition techniques for 256 and 512 -bit operands using 32-bit FCC. Thus they are designed as their respective 8 and 16-bit structures where a single bit full-adder is now replaced by a 32-bit FCC. The proposed 256-bit adder provides 35% speedup from the best known carry lookahead technique on an FPGA platform.

3. $\mathbb{F}_p$**-multiplier:** A modification on interleaved multiplication algorithm is proposed for improving the scope of parallelism. The modified algorithm exploits the Montgomery ladder where doubling and addition within an iteration are independent to each other. On the other hand, both of the operations are computed at every iteration which provide a balanced execution and security against non-differential side-channel attacks.

   It further proposes a parallel iterative architecture based on the modified multiplication algorithm and high speed adders. It exploits the parallelism in two levels. One is in the addition level and other is in the algorithmic level. The extensive experimental results have been furnished to show its performance improvement of 70% over existing design and security against non-differential timing and power attacks.

4. **Speedup of ECC cryptoprocessor:** It is now essential to validate the proposed technique on elliptic curve and pairing computations. In case of elliptic curve computation, we redesign the PGAU and ECSM cryptoprocessor. The old adder circuits are now replaced by the proposed high speed adders in the new designs.

The experimental result shows that the modified designs achieve 30% speedup over the old designs. The same F_p-primitives are used to develop the pairing cryptoprocessor which is described later.

- **High Speed Flexible Pairing Cryptoprocessor.** In this work we propose a cryptoprocessor for the computation of pairings over Barreto-Naehrig curves (BN curves). The proposed pairing cryptoprocessor (PCP) supports random curve parameters including prime p. It supports all primes less than the given length (256 bits). We develop a parallel configurable hardware for computing addition, subtraction, and multiplication on $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ using high-speed $\mathbb{F}_p$-primitives described previously. Existing techniques to speed up arithmetic in extension fields [**?**] for fast computation in $\mathbb{F}_{p^6}$ and $\mathbb{F}_{p^{12}}$ are used on top of it. The major contributions of this work are highlighted here.

  1. **CFP design:** The chapter introduces a configurable $\mathbb{F}_{p^k}$-primitive (CFP) based on the high-speed $\mathbb{F}_p$-primitives described previously. 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.
  2. **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 [**?**]. 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 on the performance of Tate, ate, and R-ate pairing over BN curves. The result is demonstrated for a 256-bit BN curve which provides 128-bit security.

- **Pairing Computations Against Fault and Power Attacks.** This work deals with the fault and side-channel attacks on pairing computations which is another objective of this thesis. The contributions of this chapter are summarized here.

    1. **Fault attack on pairing:** It analyzes existing fault attacks and countermeasures on pairing computations that are described in [**?**]. The attack assumes that the respective fault is injected into a specific register inside the pairing cryptoprocessor. With experimental result this chapter depicts a fault injection technique into a register by tuning the clock frequency. The chapter finds out the limitations of the existing countermeasures. To overcome such limitations we propose a new countermeasure to defend fault attacks on pairing computations.
    2. **Fault attack on Miller's algorithm:** A new representation of the addition law on elliptic curves has been introduced by Edwards [**?**] in 2007, which provides efficient elliptic curve group operations [**?**]. Pairing computation in Edwards coordinates are proposed in [**?**]. This chapter analyzes the security of the pairing computation proposed in [?] against a new fault attack. This chapter shows a vulnerability against new fault attack on pairing computations over BN curves and Edwards coordinates [?]. A suitable technique is also proposed to counteract against such attack.
    3. **DPA on pairing:** The side-channel attack based on power analysis on pairing computation is another objective of the present work. We propose an attacking technique based on differential power analysis on pairing computations over $\mathbb{F}_p$. Through experimental results we show how the proposed attack actually works on an FPGA platform. A suitable technique is also proposed to counteract against such power attack.

1.3 Organization of the Thesis

The rest of the thesis is structured as follows:

Chapter 2 gives a brief overview with related techniques and algorithms of finite field operations. It also includes basic ideas of elliptic curve and pairing based cryptography. Backgrounds on side-channel and fault attacks are also provided in this chapter.

Chapter 3 reports some related works to present the state-of-art in connection to the thesis.

Chapter 4 presents an elliptic curve cryptoprocessor exploiting the concept of shared arithmetic hardware and explore its security against timing and power attacks.

Chapter 5 explores the in-built features of an FPGA device to develop high-speed prime field primitives. The multiplication algorithm has been modified to improve the scope of parallelism and proposed a high-speed F_p multiplier for 2's complement numbers.

Chapter 6 at first designs a configurable architecture for computing arithmetic in F_{p^k}. Then it proposes a cryptoprocessor for computing asymmetric pairings over BN curves that provide 128-bit security.

Chapter 7 deals with the security of pairing computations against fault and power attacks. Through experimental results the actual technique of fault induction has been shown. Actual DPA attacks on a pairing computation has been described. Suitable countermeasures have been proposed in this chapter.

Chapter 8 concludes the thesis and discusses some possible directions of future work.

1.4 Conclusion

This chapter has given an overview of the whole work. The motivation behind this research, objectives and scopes are described. In the next chapter we provide a background of the works described in this thesis.