A reconfigurable security architecture for wireless communication systems

Miguel Morales-Sandoval
National Institute for Astrophysics, Optics and Electronics
Computer Science Department
Luis Enrique Erro No. 1, Sta. Ma. Tonantzintla, 72840 Puebla, México
mmorales@inaoep.mx

Abstract

In this PhD. research it is proposed to analyze, design and evaluate a dynamically reconfigurable hardware architecture for elliptic curve cryptography (ECC). Such architecture is a proposal to solve the interoperability problem in ECC. Different to work reported in the literature, in which the ECC architecture needs to be reconfigured off line to support different security levels, the proposed architecture aims to make possible mobile devices can adapt to different security levels at runtime.

1. Motivation

Security and interoperability are two intrinsic requirements for mobile communications systems. An example of such systems are the Ad-Hoc networks, which are autonomous system of mobile routers connected by wireless links that form the network at the time they enter in their transmission range. This new paradigm of wireless communication imposes new challenges for network security. Current research is focusing on protocols for key establishment, confidentiality and authentication [2]. ECC is considered the most efficient public key technology to provide all these security services but at this moment, a state of the art implementation of ECC is unsuitable for such application because of the following points:

1. The tendency of future mobile systems is an integration of heterogeneous systems, so interoperability is necessary. ECC at this moment presents problems of interoperability [8], like the management of different elliptic curves, arithmetic in different finite fields and few standardized ECC algorithms.
2. The ECC solution must meet the security requirements of authentication and confidentiality and at the same time, it must be interoperable, to meet the constrains of mobile devices and to achieve the throughput expected for future communications (200 Mbps).
3. Since ECC can be implemented in different ways, different performances and area requirements may result. So, an efficient ECC implementation must be established for mobile applications.

Although there have been reported security hardware solutions based on ECC, only a few of them attempt to solve the interoperability problem by providing a generic architecture to manage some of the ECC parameters like the order of the finite field. Some of these solutions require higher area which makes them unsuitable for constrained devices. A careful study of which are the best choices to meet throughput and area requirements for mobile applications is not known, making it difficult to provide an efficient interoperable ECC security solution for future mobile communications.

2. Previous work

Reported works are concerned with hardware architectures for fast scalar multiplication computation, which is the most time consuming in the cryptographic schemes based on ECC. Table 2 summarizes some of the approaches taken in some architectures reported in the literature:

Ref.	m	kP method	Coordinates	Basis	Multiplier	Timing
[5]	163	D&A NAF	López-Dahab	Polynomial	D-S(41)	0.26
[1]	113	Montgomery	López-Dahab	ONB	Bit-serial (2)	0.27
[3]	K-163	Montgomery	López-Dahab	Polynomial	D-S	0.14
[4]	–	New 3 bits at a time	Projective	Polynomial	–	–

Table 1. Approaches taken in ECC hardware implementations in GF(2^m)

3. Questions research

This project aims to answer the following research questions:

1. *Is it possible to have an interoperable hardware architecture based on elliptic curve cryptography that can be integrated to mobile devices?*

2. *Is it possible that such architecture achieves a 200 Mbps throughput and at the same time addresses different security levels?*

3. *Is it possible to have a high performance ECC hardware architecture that reconfigures dynamically?*

4. Methodology

In order to achieve the goal of this research project, it is proposed the following methodology:

- Based on the reported work, to analyze the relation area/performance of ECC implementations. Complexities in area and time of reported work must be analyzed in order to select those algorithm combinations that are not suited for mobile applications.

- Classify the best algorithm combination (scalar multiplication algorithm, coordinates, finite field algorithms, implementation approaches) in order to select the best combinations suited for mobile devices.

- Based on the selected algorithm combination, to design the reconfigurable architecture that manage all the NIST recommended curves and support both finite fields. That is, an architecture that adapts to several security levels and also meets the constrains of the mobile devices. This implies the following task:

  [a] To design the architecture of the arithmetic modules, which must perform well for different finite field orders. Parallelism at algorithm and architecture will be applied as well as pipelining techniques in order to optimize the processing time.

  [b] The design of the architecture will be performed according to digital design methodologies, using high level hardware description languages (VHDL, Handel-C) and simulation software tools (Active-HDL, ModelSim).

  [c]To design the reconfiguration for the architecture based on reported methodologies. Partial designs will be tested on FPGA prototyping boards, like the RC200.

- Finally, to optimiz the architecture for an specific security level.

5. Preliminar results

At this moment, hardware arithmetic modules for different elliptic curves are being simulated, finite fields, and parallelism level. This is in order to find an area/performance trade off.

An ECC hardware architecture has been developed that can be used for testing arithmetic modules in order to evaluate the area/performance of selected algorithm-combination. The architecture is written in VHDL and simulated in Active-HDL. The architecture is organized in a modular way that allows the fast substitution of components for evaluation. Also, the source code available in [6] has been modified for hardware results verification.

The ECC system is defined on the binary field $GF(2^m)$ in polynomial basis and affine coordinates. The architecture is basically composed of two modules for dedicated point addition and doubling that internally incorporates modules for field arithmetic operation like multiplication, inversion, and squaring. These main modules are commanded by a finite state machine that implements the *Add and Double* method to compute the scalar multiplication. The arithmetic modules that have been considered until now are the the serial and digit-serial multipliers [5], the division algorithm [7] and the combinatorial squarer [5].

References

[1] R. Cheung, N. Telle, W. Luk, and P. Cheung. Customizable elliptic curve cryptosystems. *IEEE Trans. on VLSI Systems*, 13(9):1048–1059, Sept. 2005.

[2] L. Ertaul and N. Chavan. Security of Ad-Hoc Networks and Threshold Cryptography. In *International Conference on Wireless Networks, Communications and Mobile Computing*, IEEE Computer Society, pages 69– 74, 2005.

[3] N. Gura *et al.* An End to End Systems Approach to Elliptic Curve Cryptography. In *Proc. of CHES 2002*, volume 2523, pages 349–365. Springer, 2002.

[4] A. Hodjat, D. D. Hwang, and I. Verbauwhede. A scalable and high performance elliptic curve processor with resistance to timing attacks. In *ITCC'05: International Conference on Information Technology: Coding and Computing*, volume I, pages 538–543, 2005.

[5] J. Lutz and A. Hasan. High performance fpga based elliptic curve cryptographic co-processor. In *ITCC'04: International Conference on Information Technology: Coding and Computing*, volume 2, page 486, 2004.

[6] M. Rosing. *Implementing Elliptic Curve Cryptography*. Manning Publications, 1999.

[7] Shantz, S. C. From Euclid's GCD to Montgomery Multiplication to the Great Divide. Technical Report TR-2001-95, Sun Microsystems Laboratories, 2001.

[8] R. Zuccherato. Using a pki based upon elliptic curve cryptography. Entrust white paper, 2003. `http://www.entrust.com/resources`.