Fpga implementation of elliptic curve crypto processor over gf(2^{163}) : A Review

Anupama T[1]**, Dr. M. B. Manjunath** [2]

Abstract— **In the fast growing internet technology information security is very important, we can use the encryption to secure the information. So many different kinds of techniques are used to protect the information from unauthorized person. In this paper, we survey on text encryption techniques based on eigamal algorithm in elliptic curve i.e. ecc. Elliptic curve cryptography (ECC) has been identified and employed as an efficient and suitable scheme for public key cryptographic systems. The principal operation in elliptic curve cryptographic systems is point multiplication. Several effort in the literature have focused on developing efficient techniques to compute point multiplication**

Index Terms— **Elliptic curve cryptography, FPGA implementation, scalar point multiplication**

I. INTRODUCTION

In 1985, Miller [1] and Koblitz [2] independently showed that the group of rational points on elliptic curves over finite fields can be used for public-key cryptography. Since then, elliptic curve cryptography (ECC) has been identified and employed as an efficient and suitable scheme for public key cryptographic systems. The principal operation in elliptic curve cryptographic systems is point multiplication. Several effort in the literature have focused on developing efficient techniques to compute point multiplication on various forms of elliptic curves. Let elliptic curve E, together with a point at infinity, be an ordinary non-super singular elliptic curve defined over F2n. Given an integer k and a point $P \in E(\mathrm{F}2n)$, a *(single) point multiplication* algorithm computes $kP \in E(\mathrm{F}2n)$. Given two positive integers $k1$, $k2$ and two points $P, Q \in E(\mathrm{F}2n)$, a *double point multiplication* algorithm computes $k1P + k2Q \in E(\mathrm{F}2n)$. Double point multiplication can be used to obtain fast (single) point multiplication. Computational speed-up is achieved if the cost of performing a double point multiplication (plus the cost of evaluating Ψ) is less than twice the cost of performing a single point multiplication. In this paper a new algorithm, inserting redundancy into RNS Montgomery multiplication in order to provide efficient and cheap protection against fault attacks in the context of modular exponentiation/elliptic curve point addition, and compliant with a leak resistant arithmetic, is presented and analyzed. A formal analysis proves the detection of any single fault. Elliptic curve cryptography (ECC) is a public key cryptography system superior to the well-known RSA cryptography; for the same key size, it gives a higher security level than RSA [1]. Intuitively, there are numerous advantages of using field-programmable gate array (FPGA) technology to implement in hardware the computationally intensive operations needed for ECC. These advantages have been comprehensively studied and listed by Wollinger *et al.* [2]. Several recent FPGA-based hardware implementations of ECC have achieved high-performance throughput and efficiency. In this brief, we present a new architecture for efficient FPGA implementation of an ECC processor over GF(2163*)*, which has considerable advantages compared to other implementations as it regards to speed and area.

This paper is organized as follows In Section 1; Introduction about ECC and scalar point multiplication. In Section 2, we survey on already existing research paper. Finally, we conclude in section 3.

II. LITERATURE SURVEY

A New Double Point Multiplication Algorithm and its Application to Binary Elliptic Curves with Endomorphisms Reza Azarderakhsh, Koray Karabina[1] This paper present a new double point multiplication algorithm based on differential addition chains. Our proposed scheme has a uniform structure and has some degree of built-in resistance against side channel analysis attacks. We discuss deploying our scheme in a hardware implementation of single point multiplication on binary elliptic curves with efficiently computable endomorphisms. Based on operation counts, we expect to gain accelerations of 30% and 18% for computing single point multiplication with and without availability of parallel multipliers, respectively, and these results are verified in our implementations.

An End-to-End Systems Approach to Elliptic Curve Cryptography

Nils Gura , Sheueling Chang Shantz , Hans Eberle , Sumit Gupta , Vipul Gupta , Daniel Finchelstein , Edouard Goupy , Douglas Stebila , Daniel Finchelstein Edouard Goupy [2] Since its proposal by Victor Miller and Neal Koblitz in the mid 1980s, Elliptic Curve Cryptography (ECC) has evolved into a mature public-key cryptosystem. Offering the smallest key size and the highest strength per bit, its computational efficiency can benefit both client devices and server machines. We have designed a programmable hardware accelerator to speed up point multiplication for elliptic curves

Manuscript received April , 2014*.*

Anupama T, *4 th Sem, M.Tech(DECE)., Department of Electronics and Communication, Akshaya Institute of Technology , Tumkur, Karnataka, India. Mob. No.- 7795613527.*

Dr. Manjunath M. B., *principle, Department of Electronics and Communication, Akshaya Institute of Technology , Tumkur, Karnataka, India.*

over binary polynomial fields GF (2^m). The accelerator is based on a scalable architecture capable of handling curves of arbitrary field degrees up to m = 255. In addition, it delivers optimized performance for a set of commonly used curves through hard-wired reduction logic. A prototype implementation running in a Xilinx XCV2000E FPGA at 66.4 MHz shows a performance of 6987 point multiplications per second for GF(2^163). We have integrated ECC into OpenSSL, today's dominant implementation of the secure Internet protocol SSL, and tested it with the Apache web server and open-source web browsers.

Customizable elliptic curve cryptosystems

Ray C. C. Cheung, Nicolas Jean-baptiste Telle, Wayne Luk, Peter Y. K. Cheung[3] This paper presents a method for producing hardware designs for elliptic curve cryptography (ECC) systems over the finite field qp@P A, using the optimal normal basis for the representation of numbers. Our field multiplier design is based on a parallel architecture containing multiple-bit serial multipliers; by changing the number of such serial multipliers, designers can obtain implementations with different tradeoffs in speed, size and level of security. A design generator has been developed which can automatically produce a customised ECC hardware design that meets user-defined requirements. To facilitate performance characterization, we have developed a parametric model for estimating the number of cycles for our generic ECC architecture. The resulting hardware implementations are among the fastest reported: for a key size of 270 bits, a point multiplication in a Xilinx XC2V6000 FPGA at 35 MHz can run over 1000 times faster

FPGA implementation of high performance elliptic curve cryptographic processor over GF(2^{163})

Chang Hoon Kim, Soonhak Kwon, Chun Pyo Hong[4] In this paper, we propose a high performance elliptic curve cryptographic processor over GF(2^{163}), one of the five binary fields recommended by National Institute of Standards and Technology (NIST) for Elliptic Curve Digital Signature Algorithm (ECDSA). The proposed architecture is based on the López–Dahab elliptic curve point multiplication algorithm and uses Gaussian normal basis for GF(2^{163}) field arithmetic. To achieve high throughput rates, we design two new word-level arithmetic units over GF(2^{163}) and derive parallelized elliptic curve point doubling and point addition algorithms with uniform addressing based on the López–Dahab method. We implement our design using Xilinx XC4VLX80 FPGA device which uses 24,263 slices and has a maximum frequency of 143 MHz. Our design is roughly 4.8 times faster with two times increased hardware complexity compared with the previous hardware implementation proposed by Shu et al. Therefore, the proposed elliptic curve cryptographic processor is well suited to elliptic curve cryptosystems requiring high throughput rates such as network processors and web servers.

High-performance hardware architecture of elliptic curve cryptography processor over GF*(2^{163})*

Yong-ping Dan, Xue-cheng Zou, Zheng-lin Liu, Yu Han, Li-hua Yi [5] This paper propose a novel high-performance hardware architecture of processor for elliptic curve scalar multiplication based on the Lopez-Dahab algorithm over *GF*(2^{163}) in polynomial basis representation. The processor can do all the operations using an efficient modular arithmetic logic unit, which includes an addition unit, a square and a carefully designed multiplication unit. In the proposed architecture, multiplication, addition, and square can be performed in parallel by the decomposition of computation. The point addition and point doubling iteration operations can be performed in six multiplications by optimization and solution of data dependency. The implementation results based on Xilinx VirtexII XC2V6000 FPGA show that the proposed design can do random elliptic curve scalar multiplication *GF*(2^{163}) in 34.11 µs, occupying 2821 registers and 13 376 LUTs.

A Parallel and Uniform k-Partition Method for Montgomery Multiplication

Néto, J. ; University of São Paulo, Brazil ; Tenca, A. ; Ruggiero, W. [6] A way to speed up the Montgomery Multiplication by distributing the multiplier operand bits into k partitions is proposed. All of them process in parallel and use an identical algorithm. Each partition executes its task in n/k steps. Even though the computation step operates in radix 2^k, the complexity is reduced by the use of a limited digit set. Experiments with a 90nm cell library show that the hardware cost and its complexity have a linear growth according to the number of partitions. Besides the gain in speed, the proposal reduces power consumption for multiplication operands with 256, 512, 1024, and 2048 bits. The uniform treatment of partition hardware design enables the realization of a fault-tolerant hardware.

A scalable architecture for elliptic curve point multiplication

Jarvinen, K., Tommiska, M. ; Skytta, J.[7] An architecture for elliptic curve point multiplication, which is developed especially for FPGAs, is introduced. The point multiplication is the basic operation of any elliptic curve cryptosystem and, hence, it must be implemented efficiently. The architecture is designed to be flexible in terms of speed and logic requirements and it can be scaled to meet the demands of different applications. Implementations have proven to be very efficient in performance and they belong to the fastest published FPGA-based ECC designs for most elliptic curve parameters.

Efficient Elliptic Curve Point Multiplication Using Digit-Serial Binary Field Operations

Sutter, G.D. Deschamps, J. Imana, J.L. [8] This paper details the design of a new high-speed point multiplier for elliptic curve cryptography using either field-programmable gate array or application-specified integrated circuit technology. Different levels of digit-serial computation were applied to the data path of Galois field (GF) multiplication and division to explore the resulting performances and find out an optimal digit size. We provide results for the five National Institute of Standards and Technology recommended curves, outperforming the previous published results. In $GF(2^{163})$, we achieve a point multiplication in 19.38 μs in Xilinx Virtex-E. Using the modern Xilinx Virtex-5, the point multiplication times in $GF(2m)$ for m = 163, 233, 409, and 571 are 5.5, 17.8, 33.6, 102.6, 384μs, respectively, which are the fastest figures reported to date.

Fast Elliptic Curve Cryptography on FPGA

Chelton, W.N. ; Sheffield Univ., Sheffield ; Benaissa, M. [9] This paper details the design of a new high-speed pipelined application-specific instruction set processor (ASIP) for elliptic curve cryptography (ECC) using field-programmable gate-array (FPGA) technology. Different levels of pipelining were applied to the data path to explore the resulting performances and find an optimal pipeline depth. Three complex instructions were used to reduce the latency by reducing the overall number of instructions, and a new combined algorithm was developed to perform point doubling and point addition using the application specific instructions. An implementation for the United States Government National Institute of Standards and Technology-recommended curve over GF(2^{163}) is shown, which achieves a point multiplication time of 33.05 s at 91 MHz on a Xilinx Virtex-E FPGA-the fastest figure reported in the literature to date. Using the more modern Xilinx Virtex-4 technology, a point multiplication time of 19.55 s was achieved, which translates to over 51120 point multiplications per second.

Fault Detection in RNS Montgomery Modular Multiplication

Bajard, J., Eynard, J. , Gandino, F.[10] Recent studies have demonstrated the importance of protecting the hardware implementations of cryptographic functions against side channel and fault attacks. In last years, very efficient implementations of modular arithmetic have been done in RNS (RSA, ECC, pairings) as well on FPGA as on GPU. Thus the protection of RNS Montgomery modular multiplication is a crucial issue. For that purpose, some techniques have been proposed to protect this RNS operation against side channel analysis. Nevertheless, there are still no effective and generic approaches for the detection of fault injection, which would be additionally compatible with a leak resistant arithmetic. This paper proposes a new RNS Montgomery multiplication algorithm with fault detection capability. A mathematical analysis demonstrates the validity of the proposed approach. Moreover, an architecture that implements the proposed algorithm is presented.

III. CONCLUSION

We have proposed New and highly efficient architecture for elliptic curve scalar point multiplication is present by using a new double point multiplication algorithm for cryptography application. The hardware implementations of cryptographic functions against side channel and fault attacks. Our proposed scheme has a uniform structure and has some degree of built-in resistance and some techniques against side channel analysis attacks. To achieve the maximum architectural and timing improvements, we reorganize and reorder that logic structures are implemented in parallel and operations in the critical path are diverted to noncritical paths. Our proposed system representing a new double point multiplication algorithm based on differential addition chains and a new and highly efficient architecture for elliptic curve scalar point multiplication with fault detection capability.

REFERENCE

1] Reza Azarderakhsh, Koray Karabina, "A New Double Point Multiplication Algorithm and its Application to Binary Elliptic Curves with Endomorphisms," *IEEE Transactions on Computers*, vol. 99, no. 1, pp. 1, 5555.
2] Nils Gura and Sheueling Chang Shantz and Hans Eberle and Sumit Gupta and Vipul Gupta and Daniel Finchelstein and Edouard Goupy and Douglas Stebila and Daniel Finchelstein Edouard Goupy, "An End-to-End Systems Approach to Elliptic Curve Cryptography," In Cryptographic Hardware and Embedded Systems (CHES), 2002, pp. 349-365. Springer-Verlag
3] Ray C. C. Cheung, Nicolas Jean-baptiste Telle, Wayne Luk , Peter Y. K. Cheung, "Customizable elliptic curve cryptosystems," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2005, vol. 13, pp. 1048-1059
4] Chang Hoon Kim, Soonhak Kwon, Chun Pyo Hong, "FPGA implementation of high performance elliptic curve cryptographic processor over GF(2^{163})," Journal of System Architecture, Vol 54, issue 10, oct 2008, pp. 893-900
5] Yong-ping Dan, Xue-cheng Zou, Zheng-lin Liu, Yu Han, Li-hua Yi, " High-performance hardware architecture of elliptic curve cryptography processor over $GF(2^{163})$," Journal of Zhejiang University SCIENCE A, vol 10, issue 2, pp 301-310

6] Néto, J. ; University of São Paulo, Brazil ; Tenca, A. ; Ruggiero, W."A Parallel and Uniform k-Partition Method for Montgomery Multiplication," , IEEE Transactions on Computers, Volume:PP , Issue: 99.

7] Jarvinen, K. , Skytta, J., "A scalable architecture for elliptic curve point multiplication," IEEE International conference on Field Programmbale Technology, 2004, pp. 303-306.

8] Sutter, G.D. Deschamps, J. Imana, J.L., "Efficient Elliptic Curve Point Multiplication Using Digit-Serial Binary Field Operations," IEEE Transaction on Industrial Electronics, Vol. 60, Issue 1, pp. 217-225, Jan 2013.

9] Chelton, W.N. ; Sheffield Univ., Sheffield ; Benaissa, M., "Fast Elliptic Curve Cryptography on FPGA," IEEE Transaction on VLSI Systems, vol. 16, Issue 2, pp. 198-205, Feb 2008.

10] Bajard, J., Eynard, J. , Gandino, F., "Fault Detection in RNS Montgomery Modular Multiplication," IEEE Symposium on Computer Arithmatic, pp. 119-126, April 2013.

Anupama T
The author is currently pursuing M.tech in Digital Electronic and Communication Engineering at Akshaya Institute of Technology, Tumkur , Karnataka , affiliated to Visvesvaraya Technological University

.**Dr. M. B. Manjunath**
The author is principle at Akshaya Institute of Technology, Tumkur , Karnataka , affiliated to Visvesvaraya Technological University.