Scientific Journal Impact Factor (SJIF): 1.711

IJMTER

International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

EFFICIENT ALGORITHMS AND ARCHITECTURES FOR AVOIDING SIDE CHANNEL EFFECT USING ECC

A.Irfana[1],R.Anbarasan[2]

[1]PG Scholar department of ECE,srinivasan Engineering College,Perambalur,TamilNadu,India.
[2]Assistant professor,department of ECE ,Srinivasan Engineering College,Perambalur,TamilNadu ,India.

Abstract--A parallel processing crypto-processor for Elliptic Curve Cryptography (ECC) and EC point multiplication is used to increase the response. This system is continuously verifies the instruction-level parallelism (ILP) and multiple sets of modular arithmetic logic units accelerate modular operation. In this project think the two troubles surface channel attack. Curve crypto-processor over double fields on binary Edwards and generalized curves using Gaussian normal basis (GNB) optimization process. Its reduces the computation cost and also simplifies the critical paths present in the change structural plan. Working frequency improved by pipeline split lacking rising the cycle's rank. To eliminate the grave pathway by appear ahead clock gating technique used in the single bit memory storage device. It used to falling the power by the automatic seem ahead clock, delay, and area. Pipeline folding and partitioning method to well at least 256-bit modular multiplications on a single Xilinx FPGA used to implement large bit-length multiplications.

Keyword: ECC, ILP, GNB

I. INTRODUCTION

ECC is a lesser key range, falling storage space and transmission requirements that an elliptic curve group could give the same level of security afforded by an RSA-based system with a large modulus and likewise better key a 256-bit ECC public key be supposed to give similar security to a 3072-bit RSA free key. Cryptographic purpose, an elliptic curve is a plane curve over a limited field which consists of the point fulfilling the equation the length of by means of a illustrious point at time without end. The coordinates here are to be chosen from a fixed limited field of characteristic not equal to 2 or 3, or the curve equation will be rather more complicated.The generation of area parameter is not usually done by each member. Since this involves compute the numeral of point on a curve which is time overwhelming and worrying to execute. As a product more than a few standard bodies available area parameter of elliptic curves for several common field sizes. Such area limit are more often than not known as "normal curves" or "named curves"; a named curve be able to be referenced also by first name or by the unique thing identifier defined in the normal papers If one (despite the above) needs to construct one's own domain parameters, one should choose the fundamental field and then use one of the subsequent strategies to find a curve with suitable shape of point using one of the following method.

Elliptic curve operations the adding procedure on the points of an elliptic curve you have two points, R and S on an elliptic curve, and R + S = T. To verify T a line is drawn through points R and S, and the line will intersect the elliptic curve at a third point, which is –T. The point –T is then reflected in the axis to point R. For instance: present are two exceptions where sketch a line through points R and S will provide point –T. The first exception occurs when adding points R and –R, the second occurs when doubling point P. Since drawing a line through point R and –R will result in a vertical line (which will not cross through the elliptic curve at a third point), the point at infinity O is needed. By definition, R +

(-R) = O, therefore, R + O = R .Now on to doubling point R. To add P to itself, a tangent line to the curve is drawn at the point R. The tangent line will intersect the elliptic curve at the point –T, if the y value of R is not 0. –T is then reflected into the x-axis to provide T. If a point R is such that yR = 0, then the tangent line to the elliptic curve at R is vertical and does not intersect the elliptic curve at any other point.2R = 0 for such a point R”.Now is this done algebraically.

II. PROPOSED SYSTEM

A lot of amount of research is being conducted to find various approaches to accelerate ECC operations. The use of Residue Number System (RNS) to speed- up multiplications. To replace the intrinsic operation double-and-add by a new operation called quad-and-add expressed in radix-4 instead of the popular radix-2. Use of Instruction-level parallelism (ILP) and multiple modular arithmetic logic to speed-up ECC operations, assuming the popular binary algorithm. The dependency graphs presented here show that up to four processes can be run in parallel. To achieve the best performance, this amount of parallelism must be supported by adequate hardware resources. The point addition operation shows that in one level it requires four multipliers of two operands.

III. ARITHMETIC ANALYSIS

Scalar point multiplication, Q = k·P, is the underlying operation in the elliptic curve cryptosystems. P is the base point of ECs and k is a scalar used as private key. The resultant point Q will be used as a public key. According to ECDLP, if k is significantly large then it is very hard to retrieve k when the values of P and Q are given. The scalar point multiplication can be executed by point additions and point doublings, both of which involve many basic field arithmetic operations. In this paper, the EC is set as a generic Koblitz curve with the form of Equation (2), which is widely used in ECC, and the basic arithmetic operations are performed in the Galois fie ld (GF). The GFs are either prime field GF (p) or extension binary field GF (2m). The GF(2m) design is easier for hardware implementation and is adopted in this paper. Binary Method is a basic scalar point multiplication method, also called double and add method, as shown in Algorithm 1. The scalar point multiplication iterates through every bit of k. In each iteration, the point doubling is performed. When the particular bit of k is one, the point addition is also performed. It means that the execution time of one scalar point multiplication is correlated to the hamming weight of the key k, and then the Simple Power Analysis (SPA) attacks become a threat to reveal the key value through recording power traces over time.

IV. POINT MULTIPLICATION

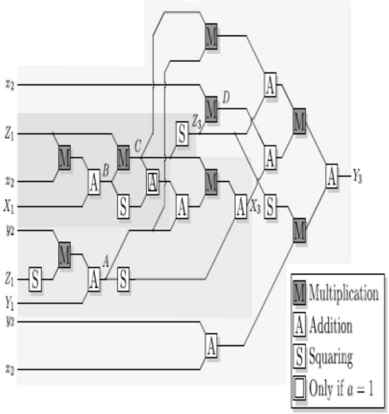


Fig.1. Point multiplication

We embed functionalities required for other field operations into the multiplier data path by adding two multiplexers. This increases the critical path of the multiplier only by a delay of a 2-input multiplexer. Based on the architecture of the proposed. Crypto-processor for point multiplication on Koblitz curves, the field operations are computed as follows: Addition : First, is loaded to by selecting with and setting and . Second, is selected with and the addition is computed by setting and which results in . Finally, is stored into . Thus, addition takes three clock cycles. If , then the second operand is not needed and the latency is two clock cycles. Squaring : First, is loaded to by selecting with and setting and . Second, the first operand of the adder is set to zero by selecting and the second operand is selected by setting .The routines implemented in the controller are collected in the controller takes in two most significant bits (MSB) of the register.

V. GNB MULTIPLIER

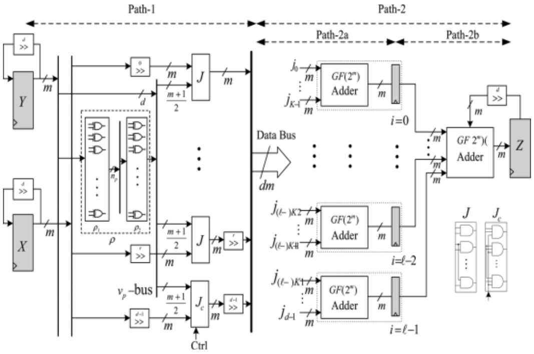


Fig .2.GNB multiplier

For our resource-constrained targets, we focus on minimizing the area as much as possible. Projective coordinates, where a point is represented with three coordinates (x,y,z), are commonly used for improving the speed of point multiplications because they allow trading expensive inversions to cheaper multiplications. On the other hand, traditional affine coordinates, where a point is represented with two coordinates , require simpler control structure and fewer registers to store the points and temporary variables and, as a result, lead to simpler and smaller (but, of course, slower) implementations An inversion in requires at least with all known algorithms based on Fermat's Little Theorem. Parallelism is an approach to reduce the number of field arithmetic operations, mainly multiplications, in the critical path by using multiple multipliers concurrently. In addition, merging point operations, i.e., the PA and PD, can result in less data dependency and can reduce the latency of the point multiplication over binary Edwards and generalized Hessian curves. Computing the -coordinates of PA and PD for BECs together in one step of the Montgomery's algorithm requires six general finite field multiplications and four field multiplications by constants, as reported in Table I. As summarized in this table, for GHCs, the cost of combined PA and PD is five field multiplications and two multiplications by constants. In the following, we explain how parallel field operations can be utilized to reduce the latency of the point multiplication operation.

VI. BINARY GENERIC CURVE

For the sake of comparison, we have included a data dependency graph for BCGs employing two multipliers. As seen from this figure, the latency of the combined PA and PD operations in parallel is. Incorporating three multipliers reduces the latency to with multiplier utilization of 100% . It is worth mentioning that employing more than three multipliers,i.e., , will not reduce the latency of point multiplication. This has been investigated in a different way with to parallelize PA and PD operations as well as parallelizing finite field operations in. We note that parallel computation of point multiplication over binary generic curves has been widely studied in the literature.

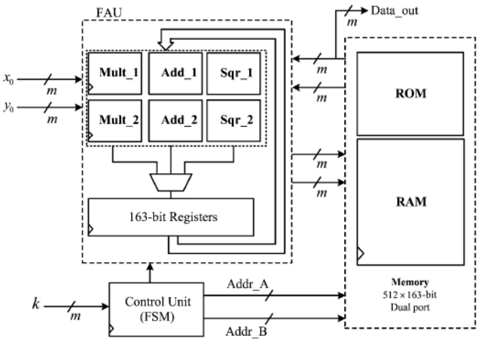


Fig.3.Binary generic curve

VII. LOOK AHEAD CLOCK GATING

The FF's master latch becomes transparent on the falling edge of the clock, where its output must stabilize no later than a setup time prior to the arrival of the clock's rising edge, when the master latch becomes opaque and the XOR gate indicates whether or not the slave latch should change its state. If it does not, its clock pulse is stopped and otherwise it is passed.

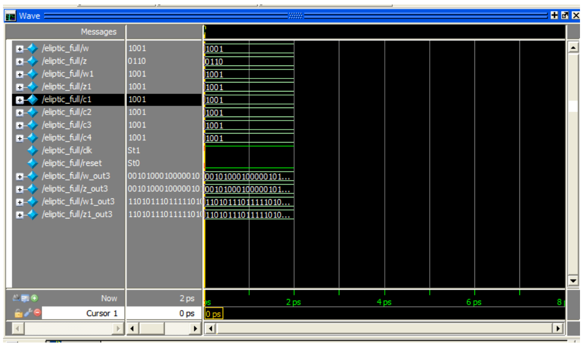
AGFF can also be used for general logic, but with two major drawbacks. Firstly, only the slave latches are gated, leaving half of the clock load not gated. Secondly, serious timing constraints are imposed on those FFs residing on critical paths, which avoid their gating.

LACG takes AGFF a leap forward, addressing three goals; stopping the clock pulse also in the master latch, making it applicable for large and general designs and avoiding the tight timing constraints. LACG is based on using the XOR output in figure 3.3 to generate clock enabling signals of other FFs in the system, whose data depend on that FF. There is a problem though.

VIII. IMPLEMENTATION RESULTS

I have examined the proposed stepping up techniques for the NIST optional Kobiltz curves K-233 and K- 283 on the Xilinx Virtex 4 FPGA. All those curve contain μ = −1 and hold up their safety principles. Operating frequencies achieve for the change system architectures based on the type of numeral adders plus on the optimization setting in the combination tools. This completion use general adders and subtracters. The projected optimizations decrease the number of adder and subtracter circuit but boost up the numeral of multiplexers. Employ of the parallel approach enhance the frequency radically. Because here no foam in the pipeline data- conduit, the necessities for scalar decline and translation stay behind roughly similar. Three set of point P, 2P, and 3P are pre-evaluated and worn intended for the left-to-right dual algorithm , one tip adding is forever execute following two point doublings are implemented. A modular reverse operation that is essential for a organize exchange is executed by means of Fermat's Little Theorem.

Curve	Coordinates	Area (um^2)	Power (uW)	Delay (ms)
BKC	Affine	13250	79.4	7.87
BEH	Affine	12580	68.6	5.2



```
/eliptic_full/w          1001                  1001
/eliptic_full/z          0110                  0110
/eliptic_full/w1         1001                  1001
/eliptic_full/z1         1001                  1001
/eliptic_full/c1         1001                  1001
/eliptic_full/c2         1001                  1001
/eliptic_full/c3         1001                  1001
/eliptic_full/c4         1001                  1001
/eliptic_full/clk        St1
/eliptic_full/reset      St0
/eliptic_full/w_out3     0010100010000010      0010100010000101...
/eliptic_full/z_out3     0010100010000010      0010100010000101...
/eliptic_full/w1_out3    1101011101111101      1101011101111010...
/eliptic_full/z1_out3    1101011101111101      1101011101111010...
Now                      2 ps
Cursor 1                 0 ps                  0 ps
```

IX. CONCLUSION

A highly parallel and fast crypto-processor for point multiplication on Binary Edwards and hessian curves. In this efficient, have to modified the point addition formulation to employ four parallel finite field multipliers and reduced the latency of point multiplication about 25% in comparison with the fastest one available in the literature. We have implemented the proposed ECC crypto-processor on an Altera Stratix FPGA for different digit sizes over GF targeting the applications where high speed is required and area usage should be considered as well. An efficient hardware architecture for point multiplication on koblitz curves incorporating higher level parallelization and optimum lower level scheduling. We have extended the digit-level architectures to a low-complexity bit-parallel architecture and compared it with the counterparts. we have implemented them on FPGA and ASIC and their area and timing results.

REFERENCES

[1] L.Batina, N.Mentens, K.Sakiyama, B.Preneel, and I.Verbauwhede, "low-cost elliptic curve cryptography for wireless sensor networks," in proc, security and privacy in ad-hoc and sensor networks, 2006, pp.6-17.

[2] V.Dimitrov and K.Jarvinen, "another look at inversions over binary fields," in proc, 21st IEEE int.symp, computer arithmetic (ARITH-21), 2013,pp-211-218

[3]Federal information processing standards publications, (FIPS 186-3), U.S. Departmentofcommerce/NIST,2009[online].available:csrc.nist.gov/publications/fips/fips186-3.pdf,Digital signature standards(DSS)

[4] D.Hein, J.Wolkerstrofer, and n.felber, "ECC is ready for RFID-A proof in silicon," in proc, workshop on selected areas in cryptography (SAC 2009), 2009, pp.401-413, springer.

[5] S.kumar, t.wollinger, and c. Paar, "optimum digit serial multipliers for curve-based cryptography," IEEE trans. Comput., vol.55,no. 10,pp. 1306-1311,2006.

[6] S. Kumar and C. Paar, "are standards compliant elliptic curve cryptosystems feasible on RFID," in proc, workshop RFID security (RFID sec 2006), 2006

[7] U.Kocabas, J.fan, and I.Verbauwhede, "Implementation of binary Edwards curves for very-constrained devices," in proc, 21st Int.conf.application-specific systems architectures and processors (ASAP 2010), 2010, pp. 185-191.

[8] Y.K.Lee, k.sakiyama, L.Batina, and I.Verbauwhede, "ellipticcurve-based security processor for RFID," IEEE trans. Comput., vol. 57, no.11,pp, 1514-1527, 2008.

[9] M.Mozaffari kermani and R. Azarderakhsh, " Efficient fault diagnosis schemes for reliable lightweight cryptographic ISO/IEC standard CLEFIA benchmarked on ASIC and FPGA," IEEE trans,ind, electron.,vol.60,no.12, pp.5925-5932,dec.2013.

[10] M.Mozaffari kermani and A.reyhani-masoleh, "a low-power high-performance concurrent fault detection approach for the composite field S-box," IEEE trans,comput., vol.60, no.9, pp.1327-1340,2011.