International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 13
October 2017

Serial-Out Bit-Stage Mastrovito Multiplers for High Speed Hybrid Double Multiplication Architecture

1.M KALPANA 2 M MAHESH

1.Pg Scholar, Department of ECE, Vaagdevi College of Engineering, Bollikunta Warangal, Telangana

2.Assosciate Professor, Department of ECE, Vaagdevi College of Engineering, Bollikunta Warangal, Telangana

ABSTRACT: Serial-bit level multiplication scheme has important internal feature. As a result of the multiplication of each clock cycle to generate a bit of it one has the ability to output. However, $ GF $ ($ 2 ^ m $) is based on the representation of the general use of the multipliers in the existing serial bit-level computational complexity, which limits its usefulness for many applications; Thus, the optimum use of the serial bit-level representation on the basis of polynomial coefficient is needed. In this paper, we propose a new serial bit-level Mastrovito multiplier schemes. We are in terms of the complexities of the time, the proposed multiplier schemes available in the literature have shown to outperform existing serial bitlevel schemes. In addition, the proposed use of multiple schemes, we present a new hybrid-double multiplication architectures. Best of our knowledge, this represents the first time using a polynomial coefficient of such a hybrid structure is proposed. The serial bit-level patterns and schemes presented by the proposed hybrid-double multiplication architectures (10 schemes in total) are implemented over both $ GF (2^{163})$ and $GF(2^{233})$, and experimental results are presented.

I INTRODUCTION:

It appears that Miller [1] and koblitz [2] limited to the fields of a group of elliptic curve points on elliptic curve cryptography (ECC) public-key cryptography that can be used independently Method. Compared to RSA, ECC offers the same level of employees in small key size [3]. Therefore, in terms of time-area trade is crucial to the effective implementation of the ECC. For server applications, high-speed implementations small and need to be considered for use in embedded devices is required, however, the main concern. As a field programmable gate array (FPGAs) and application specific integrated circuit, using a variety of hardware platforms. Edward and generalized Hessian binary curves recently and have been introduced. It is a generic elliptic curves in all the fields of binary input In addition to all of the pairs of unified principles for the work to obtain full and Edwards, and was written in a simple Hessian form. However, some of the works of literature of the curve is the multiplication, and wanted to run., in the multiplication of binary Edwards curves point in the ASIC implementation (BECs) has been submitted for resource constrained applications. finite field arithmetic, as well as a high degree of parallelization of the curvature of the compounds have been Page 953 investigated to

evaluate the low-level parallelization of time - in the area of trade - offs. Study results suggest that the level of parallelization curve, but the curve point multiplication unified and complete, but they compared the results of the multiplication of the point of the proposed binary generic curves and slow The four parallel finite field multipliers which employees need to be combined with the three levels of the product in addition to point (PA) and the doubling of computing the data dependency. pointed out that the binary normal curves point multiplication onrequire onlyt wolevels of multiplica tion santarin cukonnadi three or more parallel multiplier. Thus, new methods and structures of ECC computations are required to investigate all levels of parallelization and scalability. The main pupose of this paper is to point out the multiplication specifically targeted applications of high performance ECC cryptographic primitives provides a new structure in order to reduce the latency of the computation. In this paper, we propose a new scheme, a hybrid double-point multiplication Edwards reduce the latency binary multiplication techniqueproposedin [23] using the generalized Hessian curves. [23] as the level of conventional hybrid double-digit level of the coefficient multiplier to the same latency using the same measures in the two multiplications. This scheme reduces the latency of the curve point multiplication and hence increase the speed of the multiplication of the binary Edwards and generalized to the point hessian curves. In the proposed scheme is the only higher than presented in previous works should be noted that the merger. Putations ECC for data integrity in the field, such as various logic multipliers, adders and binary fields squarers not understand how the calculation is to move between the elements of the first data flow analysis. Then, an internal analysis to determine where and why we field multiplications double-double multiplier employ hybrid wecan. The results of the multiplication of the curve point in Curves, as well as the completeness of the usual binary speed is offering a contest. Practical, evaluate the performance of the proposed scheme, we are using the hybrid double multiplier using two crypto processors design and VHDL code and run it on Xilinx Virtex-4 and Virtex -7 FPGAs.

II LITERATURE SURVEY

A large number of errors, because they have the ability to correct the error correction described in this paper basically memory devices, the memory is used for the applications important to the majority logic decodable codes. However, the performance of the memory they need to have a big influence the decoding time. Technical standards, in memory devices become larger and more powerful error correction codes are needed. Euclidean geometry to overcome the problems in this paper as they use more modern codes. These codes can correct a number of errors, but usually requires complex decoders. Serially with the majority logic decoding circuitry can be implemented in a very simple, but it requires long periods of decoding. Memory, this is an important parameter for the access to the system can increase the time. Increase the size of the code, so the majority of the increase in the time of decoding the decoding logic (implemented serially), N iterations required. EGLDPC code, the code word is used in this method (Euclidean geometry -Low Density Parity Check), there is a majority One Step Logic Decodable code. It uses the algorithm to check the

code. There is nothing to check the algorithm, but code word is associated with a numerical value to be transmitted. The receiver then receives the code word at the end of the numerical values associated with the error identification is a Page 954 comparison of some numerical value. There. The method is easy to implement using existing hardware. This method is more time for decoding. As well as the power consumption and the need for the region are high. One step is to identify the shortcomings of the majority of serially MLDD serial technique uses Logic decoder. [2] In this article, the author of the noisy channel (Additive White Gaussian Noise) in the presence of PSK and FSK modulation techniques Reed Solomon code (RSC) of the bit error rate (BER) on performance analysis explains. In this paper, 32-FSK (frequency shift keying), PSK (phase shift keying) modulation coded communication system is used for the simulation. In addition to the use of Monte Carlo simulation and calculation of the rate of BER MATLAB / SIMULINK is done using the tool. The results are shown using BERTOOL. In order to compare the performance of the block length is fixed, we have taken a different code rates.Forward error correction technique used to detect and correct errors in the AWGN noise received from the channel. Burst errors or noise and improves performance by removing the received signal using Reed Solomon codes that can be encoded. AWGN channel satellite and in-depth information, but it is not a good model for multi-path interference as a good model for terrestrial links. FSK and PSK signal to detect and also do this in the calculation of this data leads to delay and is also a process for the circuit system are more complicated. The proposed system cannot cope with this problem. [3] The Reed-Solomon codes, sequential About the author explains the key equation solver algorithm is presented. This work is on-the-fly (OTF) error prevention storage devices with the highest data rate coding (ECC) is inspired by the need

III PROPOSED METHOD

New Technique For Latency Reduction In Point Multiplication: Point multiplication, ie the ability of Q = k. P, P, from a given point depends on finding the minimum number of steps to reach the KP. In addition to one of the differential and doubling formulas, Montgomery's ladder using w coordinate and generalized binary Edwards Hessi- effective multiplication of a point on the curves. In this case, the scalar K for each bit, each one-point addition and doubling are required to perform. The maximum parallelization over curves will not be considered for high-speed work practices. This idea is explored in depth investigation Page 955 for different applications in the area of time-off. Another idea is to optimize the different digit sizes in terms of the size of the finite field multipliers. In this effect, a different digit sizes (for small size and large digit sizes of some of the multipliers) is employed and further reduce the occupied area. In addition to the theoretically necessary is that we continue to reduce the latency remained unchanged, but in practice, with a large digit sizes and the maximum operating clock frequencies, reduce the number of multipliers will be dominated by the critical path. In this section, we first point of the product to achieve the maximum number of high-speed calculations, the study of multipliers. and employ a new hybrid-double multiplier. Reduces

the latency of the BECs and GHCs point multiplication.

IV BINARY EDWARDS CURVES:

Binary Edwards curves, mixed w coordinate the Montgomery Point multiplication addition and point to point, more than double the combined differential (PD) is a measure corporate. Differential In addition, Q, P, given the points, Q + P kamputation, and Q- is the P. Point P in terms of x and y coordinates in a linear and Toby, let's assume the same function, and w, is defined as w (P) = w (-p). Bernstein et al. w defined - differential w (P), W (Q + P) W (Q) computing, in addition to the co-ordination, and W (Q- P). Similarly, W-integrated differential doubling the w (2P) to w (P) calculation. Therefore, W-coordinates, doubling the principles w ((2n + 1) P), and W (2nP) using the differential in addition to W (NP) and W ((n + 1) P) can be computed by repeatedly C=w1.(z1+w1),D=w2.(z2+w2) ,E=Z1.Z2, F=w1.w2,V=C.D,w3=V+W0.Z3,

Z3=V+(c1.E+c2.F)^2 ,W4=D^2,

Z4=w4+((c3.z2+c4.w2)^2)^2 Where W0=X0+Y0,c1= $d1$,c2= $d2$ $d1$ +1,c3= $c1$, and C4 = $C2$,Also, $P1=(W1 ,Z1)$,$P2=(W2 ,Z2)$,$P3=P1+P2$, and $P4=2P2$,as seen from the above formulations, the cost of the combined PA and PD operations is 10M,where M is the cost of a multiplication for achieving highest degree of parallelization, we employ maximum number of parallel multipliers. The data dependency graph is depicted in the figure employing four DLPIPO multipliers. Therefore the multiplier utilization is (4+4+2)*100/(3*4)=83.33%.

V RESULTS:

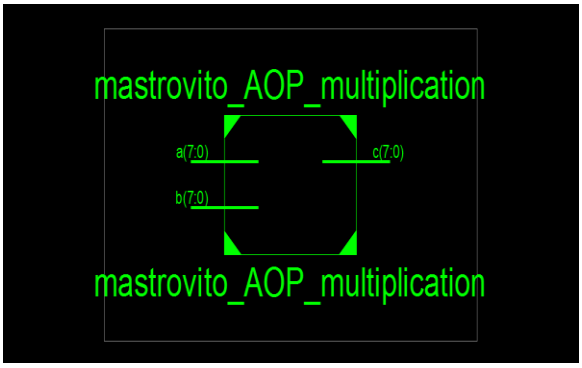
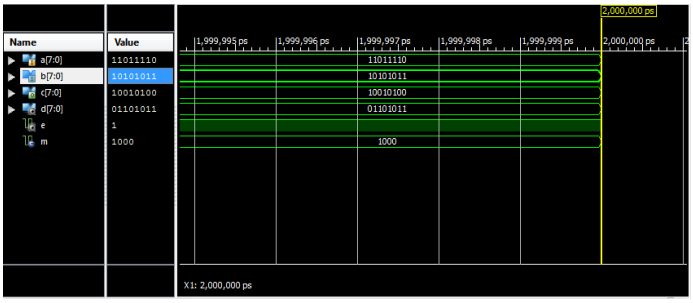


Fig :RTL SCHEMATIC

SIMULATION WAVE FORM:



V CONCLUSION

We have a variety of data, such as in the field of logic multipliers, adders and squarer's to understand how the calculation is to move between elements in a data flow analysis performed multiplication of the point. Then, we have to be employed to reduce the latency of the multiplication of hybrid double multiplier point investigated. We employ a multiple hybrid double Hessian binary Edwards and generalized curves point to reduce the latency of the product and the speed of the FPGA computation time. We crypto processors on the implementation of the different digit sizes in the proposed area, and the timing of the performance was analyzed and the

results reported. 25 per cent faster than the previous fastest results of our proposed common Hessian binary Edwards and curves as seen in the implementation of point multiplication.

REFERENCES:

[1] V. S. Miller, Use of elliptic curves in cryptography in Proc. Adv. Cryptol., 1986, pp.417–426.

[2]N. Koblitz, Elliptic curve crypto systems, Math. Comput, vol. 48,pp. 203–209, 1987.

[3]U.S. Department of Commerce/NIST, National Institute of Standards and technology, Digital signature Standard, FIPS Publications 1862.

[4] C. H. Kim, S. Kwon, and C. P. Hong, FPGA implementation of high performance elliptic curve cryptographic processor over J. Syst. Arch., vol. 54, no. 10, pp., 893–900, 2008.

[5] Y. K. Lee, K. Sakiyama, L. Batina, and I. Verbauwhede, Elliptic curve based security processor for RFID, IEEE Trans. Comput., vol. 57, no. 11, pp.,1514– 1527,Nov. 2008.

[6] J. Adikari, V. S. Dimitrov, and L. Imbert, Hybrid binary-ternary number system for elliptic curve cryptosystems, IEEE Trans. Comput., vol. 60, no.2,pp. 254–65, Feb. 2011.

[7] W. Chelton and M. Benaissa,Fast elliptic curve cryptography on FPGA, IEEE Trans. Very Large Scale Integr. Syst., vol. 16, no.2,pp. 198– 205, Feb. 2008.

[8] J. Adikari, V.Dimitrov, and K. Jarvinen, A fast Hardware architecture for integer to NAF conversion for koblitz curves, IEEE Trans. Comput., vol. 61, no. 5, pp. 732 – 737, May 2011. Page 958

[9] M. Keller, A. Byrne, and W. P. Marnane, Elliptic curve cryptography on FPGA for low-power applications, ACM Trans. Reconfigurable Technol. Syst., vol. 2, no. 1, pp. 1–20, 2009.

[10] G. Sutter and J. Deschamps and J.Imana, Efficient elliptic curve point multiplication using digit serial binary field operations, IEEE Trans. Ind. Electron., vol. 60, no.1, pp.,217–225, Jan. 2013.