RESEARCH ARTICLE OPEN ACCESS

FPGA Based Elliptical Cryptographic System Using Machine Learning Techniques

Karthikeyan S*, Soundappan V**
*ME VLSI, Mahendra Institute of Technology, Namakkal
Email: vskarthi18@gmail.com
** Professor, Mahendra Institute of Technology, Namakkal
Email: v.soundappan@gmail.com

--************************----------------------------------

Abstract:

Using modified block cyphers is one way to get both a greater performance yield and a shorter time duration for the necessary applications. This is possible by reducing the amount of time needed for the applications. Therefore, the necessary application may be categorised as implanted medical devices, compact devices, or wearable medical devices. It is expected that the severity of the algorithm would rise as a result of the availability of both intentional and natural defects. The new model that has been proposed is one that uses the lightweight block cypher known as Midori. The latency value of these proposed algorithms is the lowest possible value, and the complexity of their implementation in hardware will be the lowest possible value. The suggested system has a variety of diagnostic algorithms built into its work flow, each of which corresponds to a certain mode of the Midori model. The fault correcting strategy cannot achieve an accuracy of one hundred percent, but the value of the fault can be brought down to an acceptable minimum. Both 64-bit and 128-bit Midori symmetric key cyphers are supported by the fault diagnosis systems that are provided for the nonlinear S-box layer as well as for the beat structures. The aforementioned systems are evaluated using a field-programmable gate array as a benchmark, and their error coverage is determined using fault-injection simulations. The primary objective of the work that has been presented is to achieve a higher level of energy efficiency via the use of lightweight block cypher blocks.

Keywords **—Lower Efficiency, FPGA, Cipher blocks, Midori, Machine Learning techniques.**

--************************----------------------------------

I. INTRODUCTION

As a result of the fast breakthroughs in engineering and technology, significant aspects of electronic systems are receiving frequent updates. In the realm of communication, the conventional techniques mostly included the sending of handwritten letters, as well as conducting financial transactions through cash payments, demand draughts, and other similar practises. The top-secret documents were transported in suitcases equipped with the appropriate locks. Things are different now than they were before. The use of electronic means contributed to the development of these communication systems' approaches. E-mail and online banking both rose in popularity during this time period. Paperless strategies are becoming more popular in contemporary offices as a result of the growing popularity of paperless office environments. Despite the fact that communication over electronic platforms makes life more practical and less difficult, the potential for breaches in data security remains a [1] significant concern. The employment of cryptographic methods is what is done to make sure that the message that is received from illegal access points is kept secure.

The use of cryptography in a communication network makes it possible to send private messages and data while maintaining their confidentiality. The content of the message may be a file containing a document or a picture, an audio recording of a phone call, or any number of other types of information. Only the person who is supposed to receive the message and who has possession of the secret key will be able to read the encrypted data. By using cryptography to encrypt the text in question, the confidentiality of the communication may be preserved. When there are many people using a communication network system, such as the internet system, every user has their own unique password to ensure that their privacy is protected. On the internet, many users may run into various applications, such as electronic payment, online commerce, electronic mail, and so on, which call for the utilisation of cryptography in order to assist the users in protecting their private.

The following [2] services are expected to be brought about by the use of cryptographic techniques:

Confidentiality: Confidentiality is a service that maintains data such that it is only available to authorised users and is inaccessible to anybody else.

Integrity: Integrity is a service that assures that the message that was sent may only be altered in ways such as changing its status, postponing its delivery, replaying it, deleting it, or making new versions of itself by a user who is permitted to do so.

Authentication: Authentication is a service that gives the identification of the origin of data, the date of origin, the content of a message, the time that a message was delivered, and other such information.

Non-Repudiation: A service that assures the participation of an entity in a given communication and prohibits any party from disputing past commitments or acts. Non-Repudiation is also known as "non-repudiation."

Cryptography provides competent security engineers with the necessary tools to prevent unwanted data tampering, disguise messages and regulate accesses, check integrity, and authenticate themselves. It is impossible to accomplish safety without paying for it, just as it is impossible to acquire any other beneficial service. The execution of every cryptographic job requires an investment of time, effort, and money. The primary objective of this research is to investigate the many ways in which the performance of elliptic curve cryptosystems might be improved by focusing on their main capabilities.

The fast scalar point multiplication process may be used in a variety [3] of applications, including encryption/decryption employing elliptic curve operations, electronic signature authentication, and secure key exchange, to name a few of these possible uses. The scalar multiplication on Elliptic Curve Cryptography (ECC) consumes a lot of time, power, and space.

The following list contains the key goals of this thesis:

I To design and implement an effective Elliptic Curve Cryptosystem while taking into account various point multiplication techniques in relation to finite field operations.

(ii) To increase the efficiency of the system in terms of its performances, such as the use of available space, the power needs, and the level of safety.

The purpose of this study is to investigate the potential of elliptic curve cryptosystems in order to guarantee safe data transfer between portable devices in a way that uses less power, has a smaller key size, and makes better use of available [4] space.

The architecture that has been proposed for use with elliptic curve cryptography makes use of a variety of multipliers, including an array multiplier, a modified booth multiplier, and an encoding scheme that incorporates hybrid multiplication. This is done in order to reduce power consumption while simultaneously improving area utilization.

II. LITERATURE SURVEY

The methods that are appropriate for use in applications that use digital signatories rather than a handwritten signature were described in FIPS PUB 186-2 [5]. The formation of a digital signature is determined by specific regulations as well as certain criteria, which allow for the verification of the signatory's identity in addition to the data's continued integrity. E-mail, electronic data transmission, software distribution, electronic money transfer, and other applications that need data integrity and data authentication are examples of the types of uses that might benefit from the implementation of a digital signature method. The message data is hashed using a secure technique in order to facilitate both the production of signatures and the verification of signatures.

[6] developed an application-specific instruction set for processors, which made advantage of pipelining across many stages and was applied across the data stream. They experimented with the performance analysis using a variety of circles and found the ideal depth for pipelining. They employed three complicated instructions and devised a combined algorithm to carry out point addition and point doubling using the specified instructions in order to cut down on the latency of the system. This allowed them to accomplish their goal of reducing latency. The point multiplication was accomplished by using the Lopez – Dahab point multiplication as the basis. Reported a reduction in the amount of time needed to perform scalar multiplication as a result of the performance of a new combined algorithm to perform doubling and adding operations. Because this new algorithm requires only a smaller number of instructions, the latency has been reduced while the pipe line depth has been increased, which has resulted in an increase in the clock frequency.

[7] demonstrated performance-based elliptic curve cryptography over binary field. [Citation needed] The Montgomery scalar multiplication method was used as the foundation for the design. The execution of the design included the use of methods for converting coordinates. It was discovered that the system is both cost effective and efficient when compared to other systems currently in use, thus it was recommended to use advanced complementary metal oxide semi conductor technology to the design in order to bring throughput to the design in terms of area time product.

Two different techniques for performing multiplicative inverses in the Galois field were suggested by [8]. The first type is known as a sequential type, whereas the second type is known as a recursive type. In the study, a generalised approach for performing multiplicative inverses in Galois field was proposed (2 m). The circuit complexity was investigated for the sequential type fast method that was used, and it was established that it had simultaneous size and depth values of O(log2m), respectively.

[9] created a high performance elliptic curve co-processor that is designed for operations in binary field. They employed the projective coordinate system developed by Lopez and Dahab, which is designed to work well with Koblitz curves. When compared to the run time of applying NAF and F adic NAF, the architecture used field multiplication over extension field with degree 163 in 0.060 microseconds. The use of a co-processor brought to the excellent performance shown here. Several different digit sizes were used in order to carry out the scalar multiplication. For field sizes greater than 41, the co-field processor's multiplication function was unable to keep up with the required time. Because of this, 41 was the largest possible digit size.

An elliptic curve encryption scheme was devised by [10] and implemented in the Galois Field (2m). They have the capability of being re-configured in addition to being "scalable" in the cryptographic sense. According to the findings of the study, scalability can be implemented quite easily in various elliptic curve crypto accelerators; nevertheless, re-configurability over the reduction polynomial calls for a significant drop in performance. The strategy that was used for the job consisted of picking out hardware units and figuring out how to best optimise the scalar multiplication for the architecture.

[11] introduced a genetic kind of cryptographic processor. The architecture of this processor may be implemented with different limitations, such as the area size of a finite field, for example. This study addressed an examination of the speed trader algorithm with the purpose of realising an elliptic curve cryptosystem in hardware. They came to the conclusion that the polynomial basis was the most effective option for the implementation. If the area that is accessible is somewhat big and a Massey-Omura multiplier can be applied to it, then it will be beneficial to employ a representation with a normal foundation. The study investigated several performance limitations by leveraging certain degrees of freedom. These degrees of freedom concerned the degree of parallelism in the multiplier section, the number of functional units, the kind of controller, the coordinate representation, and other factors.

[12] examined the current state of the art of ECC and outlined the building technique for elliptic curves, as well as the security requirements for the implementation, picking the protocols, and selecting the finite field for the ECC set up, among other topics. In the study, a number of different assaults on cryptosystems and their subsequent effects were discussed. It spoke about how difficult the task was while taking into consideration the discrete logarithm problem. The primary benefits and drawbacks of elliptic curve cryptosystems were spoken about earlier in the article.

They compared the key generation process, in addition to encryption and decryption operations, using a variety of cryptosystems, such as the EI Gamal cryptosystem, the Massey Omura cryptosystem, the Menezes Vanstone cryptosystem, the RSA cryptosystem, and the ECRSA cryptosystem, amongst others. Additionally, a variety of digital signature schemes were discussed throughout the session.

III. PROPOSED WORK

The message digest will be estimated based on the specified input data after they have been processed by the hash algorithm. The input file may include any kind of data, but the machine would only read it as a string of bit values. The length of the message may be represented by the number of bits that are now accessible in the data. On the other hand, a length of 0 denotes an absence of data. Imagine for a moment that a data file stores the bit count as a product of eight. If this is the case, then hexadecimal notation may be used to record the data for the purpose of data compression. The length of the data will become equal to a product of five hundred and twelve when the padding operation has been completed. At this point, the length of each block is set at 512 bits, making it possible to create them. The hash method will generate the blocks in a sequential fashion while simultaneously computing the message digest. The procedure for padding the message is outlined in this section. Beginning with the number 1, it is followed by a "n" number of zeroes. This is followed by an integer that is sixty-four bits in length. These are included into the message at its concluding section. As a result, after padding, the data will have a length that is equal to the product of "n" and 500 + 12. "l" denotes the total length of the stored data. This is a number that has sixty-four bits in it. Following the step of padding, the data is then reconstructed using a hash technique that has a "n" number of blocks and a size that is equal to five hundred and twelve bits. Therefore, in the event that the total length of the data is less than 264, it will be appropriately padded just before it is sent through the hashing process.

The creation of the message digest thus mostly included the addition of real data with the necessary additional bits. In the end, the procedure is supposed to produce the structure of a message digest that has five hundred and twelve bits. The attachment of the padding bits in accordance with the appropriate length is the first step involved in the construction of the message digest. The padding of bits is often done in such a way that the bit-wise length will fit within the range of 440 to 512 modulo 448. This is because padding ensures that the length of the data remains constant. After padding, the length of the message will be sixty-four bits less than the product of five hundred and twelve and "n," where "n" is an integer. This will bring the total length of the message down to an acceptable level. Padding is always something that has to be done. Imagine if the message length begins with 448 bits, then an additional 512 bits are added to make the total length 960 bits. length initially started with 448 bits. Therefore, the amount of padding bits might vary anywhere from one to five hundred and twelve bits. As a result, it has zero bits followed by one bit. The next step, which comes after padding, is to increase length. The real message, which, before padding, had a size of 64 bits, is combined with the result of the step before it in such a manner that the least significant bit comes first. In the event that the data length is more than 264, only bits in the lowest order are used. After then, the length of the segment will equal the original data length divided by 2 64. Therefore, it can be deduced from the techniques described that the resulting data creates a bit size that is equal to the product of five hundred and twelve and "n," where "n" is an integer.

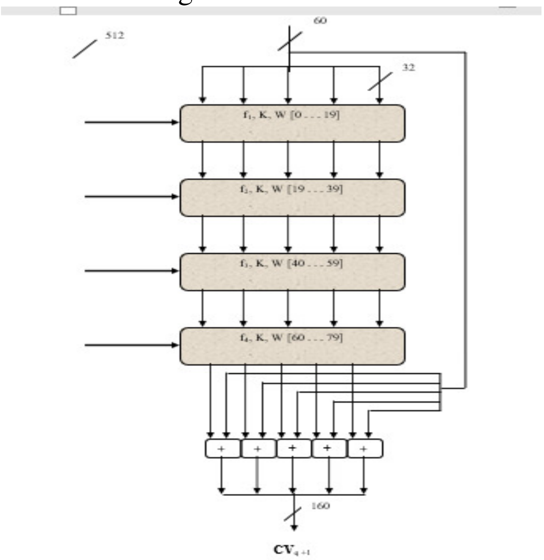

Fig1.Hashprocess

When compared to the other multipliers that were used, the encoding strategy that made use of a hybrid multiplication approach provided superior performance in terms of the amount of power that was saved as well as the amount of space that was utilised. The findings are presented in a nutshell in Figs. 7.3 and 7.4, respectively. ModelSim Simulator and Xilinx software 9.2i are used throughout the process of developing the architecture using the Spartan3E FPGA chip. The synthesis report generated by Xilinx software is used to analyse, and then compare and verify, the outcomes of the system's performance.

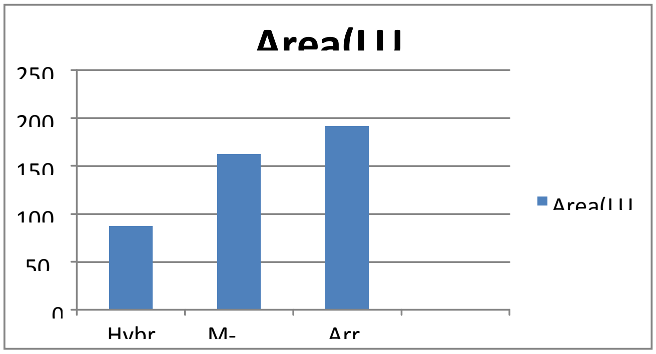

Fig.2Power Consumption of Various Multipliers.

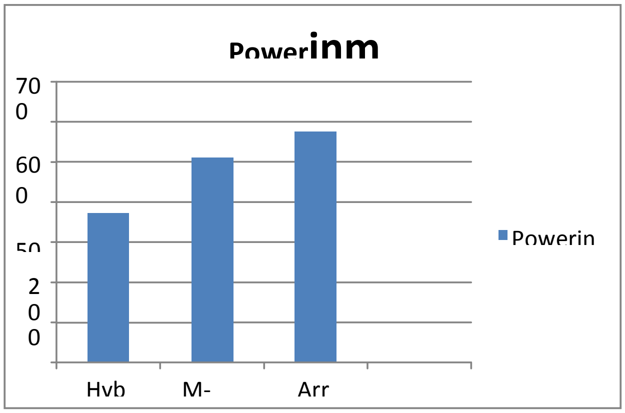

Fig.3Areautilization of Various Multipliers.

In comparison to the low power-based multiplication scheme carried out with a modified booth multiplier, the proposed architecture with hybrid multiplication based on an encoding scheme is significantly more effective with reduced partial products. This is due to the fact that the number of partial products is decreased.

In addition to this, the Elliptic Curve Cryptography protocol using the Elliptic Curve Digital Signature Algorithm (ECDSA) was investigated and examined for its compliance with the stipulated safety standards. In ECDSA, the procedures that are carried out are the production of key pairs, the generation of signatures, and the verification of signatures. The ECC Transmitter and Receiver portion was responsible for the production and verification of digital signatures using the ECDSA Algorithm as the underlying technology. Fig.3 displays the intermediate results that were produced when the ECDSA method was being implemented.

CONCLUSIONS

Both process used the Hash function of the message there by resulting in themessage digest. The transmitter sends the message, along with the digital signatures tothe receiver. The scheme and algorithm used for generation and verification of digitalsignatures with the ECC protocol enabled to develop a secured data communication. TheECDSAalgorithmconfirmedthesuitabilityforabettersecuredcommunicationenvironment.The transmitter and receiver sectionsare verified by the simulated outputofECC.

ACKNOWLEDGMENT

Thanks to the Reviewers and Editors for considering manuscript

REFERENCES

[1] Al-Khaleel.O, Papachristou. C, Wolff. F, An Elliptic Curve Cryptosystem Design Based on FPGA Pipeline Folding, IOLTS-07, July 2007, pp.71-78.

[2] Xiangu. A, Chao. W, The Application of Elliptic Curve Cryptosystem in Wireless Communication, IEEE International Symposium on Microwave, Antenna, Propogation and EMC Technologies Proceedings, 2005, pp.1602-1605.

[3] Kristin Lauther, The Advantages of Elliptic Curve Cryptography for wireless security, IEEE Wireless Communications, Feb.2004, pp.62-67.

[4] Chen. J, Shieh. M and Ming Wu, Concurrent Algorithm for High Speed Point Multiplication in Elliptic Curve Cryptography, IEEE, 2005, pp.5254-5257.

[5] Cheung. R, Nicholas, Luk. W, Customizable Elliptic Curve Cryptosystems, IEEE Transactions on VLSI Systems, vol.13, no.9, Sep 2005,pp.1048-1059.

[6] Deng Jian, Cheng Xiao, Gui, Design of Hyper Elliptic Curve Digital Signature, International Conference on Information Technology and Computer Science, IEEE Computer Society, 2009, pp.45-47.

[7] Rezai. A, Keshavarzi. P, High-performance implementation approach of elliptic curve cryptosystem for wireless network applications, IEEE, 2011, pp.1323- 1327.

[8] Vigila. S, Muneeswaran. K, Implementation of Text based Cryptosystem using Elliptic Curve Cryptography, IEEE, ICAC-09, 2009, pp.82-85.

[9] Yanlin. Q, Xiaoping Wu, New Digital Signature Scheme Based on both ECDLP and IFP, IEEE, 2009, pp.348-351.

[10] Kumar. P, Pipelined Computation of Scalar Multiplication in Elliptic Curve Cryptosystems, IEEE Transactions on Computers, vol.55, no.8, Aug 2006, pp.1000-1010.

[11] Nara. R, Togawa. N, Yanagisawa. M, Ohtsuki. T, Scan-Based Attack against Elliptic Curve Cryptosystems, IEEE, 2010, pp.407-412.

[12] Eberle. H, Gura. N, Shantz. S, Gupta. V, A Cryptographic Processor for Arbitrary Elliptic Curves over GF(2m), Sun Micro Systems, SMLI TR-2003- 123, May 2003.