ISSN: 2395-1680 (ONLINE)
DOI: 10.21917/ijme.2022.0221

HARDWARE SECURITY MODEL WITH VEDIC MULTIPLIER BASED ECC ALGORITHM ON HIGH-PERFORMANCE FPGA DEVICE

Saurabh Singh and Sunita Soni
Department of Computer Science and Engineering, Bhilai Institute of Technology, India

Abstract

The key problem that the world is most concerned about is security. Data security is the process of preventing unauthorized access to sensitive data. It includes all of the cybersecurity measures you take to keep your data safe from unauthorized access, such as encryption and access restrictions (both physical and digital). Data security has always been of the utmost importance. We utilize cryptographic methods to improve the services of data security. The application of cryptographic algorithms achieves data encryption. Therefore, we developed two versions of ECC algorithms on FPGA for improved hardware security in this study. The FPGA device employed here is Kintex-7, and there are two types of ECC: standard ECC and Vedic multiplier-based ECC. Vedic multiplier-based ECC has discovered that it consumes less space than standard ECC. Not only does Vedic multiplier-based ECC save space, but it also saves electricity. As a result, it is determined that for improved hardware security with ECC enabled, Vedic Multiplier-based ECC should be used over standard ECC.

Keywords:

ECC, Vedic Multiplier based ECC, Area, Power, and FPGA

1. INTRODUCTION

Security is the central issue regarding which the world is most concerned. Data security is the procedure of preventing unwanted access to sensitive information. It encompasses all of the cybersecurity methods you employ to protect your data from misuse, such as encryption, access controls (both physical and digital), and others [1]. Data security has always been a top priority. However, due to the present health crisis, more individuals work remotely (and cloud usage has surged to match). There is more potential for unwanted access to your data than ever before. And cybercriminals are taking advantage of it. Interpol and the US Chamber of Commerce, for example, both claim a substantial rise in the number of cyberattacks since the pandemic began.

To enhance data security services, we use the services of cryptography algorithms. Data encryption is accomplished through the use of cryptographic techniques. In general, there are two kinds of cryptography standards: symmetric standards and asymmetric standards [2-4]. Symmetric encryption techniques involve using a single key for both encryption and decryption of any data. Some symmetric encryption cryptographic algorithms include Data Encryption Standard (DES), Triple DES, and Advanced Encryption Standard (AES). Two keys are used for encryption and decryption in asymmetric encryption techniques. Asymmetric cryptographic techniques include the Rivest-Shamir-Adleman algorithm (RSA) and Elliptic Curve Cryptography (ECC), among others. In this work, to overcome the security issues, we have used the services of the ECC algorithm to encrypt our data. ECC is public-key cryptography. The intractability of some mathematical problems is the foundation of public-key cryptography. The security of early public-key systems was predicated on the idea that it is difficult to factor a huge integer consisting of two or more large prime factors [5]. The elliptic curve discrete logarithm issue is the foundation assumption for later elliptic-curve-based protocols: calculating the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is impossible (ECDLP).

The ability to compute a point multiplication while being unable to compute the multiplicand given the original and product points is required for elliptic curve cryptography to be secure. The complexity is determined by the size of the elliptic curve, which is defined by the total number of discrete integer pairs meeting the curve equation. There are several ways to implement and use the ECC algorithm. The major approaches are as software approach and hardware approach [6]. In this work, we have chosen the hardware approach instead of software. For the hardware approach, we have used the FPGA devices.

1.1 FPGA

FPGA is an abbreviation for Field Programmable Gate Arrays. FPGAs are semiconductor-based devices composed of Configurable Logic Blocks (CLBs) linked via programmable interconnects. FPGA devices are chosen over other systems such as ASIIC because they may be reconfigured after they are built. FPGA devices offer greater flexibility, are less complex to use, and deliver maximum throughput, frequency and speed [7]-[9]. The significant FPGA components are shown in Fig.1.

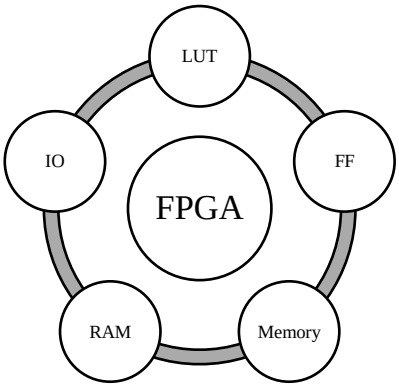

Fig.1. Major components of FPGA

2. RELATED WORK

In [10] authors have used ECC algorithm for enhancing the speed on FPGA devices. In [11] ECC algorithm multiplication techniques are compared for better hardware security. In [12] secure and quick approach of Vedic multiplier-based security algorithm is used on hardware FPGA devices. In [13] authors have designed efficient method of Vedic method for data security using ECC on FPGA. In [14] researchers have improved the

performance of ECC system using low power, Vedic multiplier-based logic. In [15] security has been provided with the help of Vedic approach on FPGA devices. In [16] researchers have implemented data security with Wallace Tree Approach Using ECC on FPGA. From the existing work it has been observed that there are several implementations of various cryptographic algorithms over FPGA is done. But no work has been done regarding the use of Vedic multiplier in the context ECC algorithm on FPGA. In this work we are making a comparative analysis of ECC algorithm and Vedic multiplier based ECC algorithm on FPGA.

3. IMPLEMENTATION OF ECC ALGORITHM ON FPGA

In this section we will discuss about the implementation of ECC algorithm on FPGA device. For the implementation we have used Kintex-7 FPGA. The RTL schematic of the ECC implementation is represented in Fig.2.

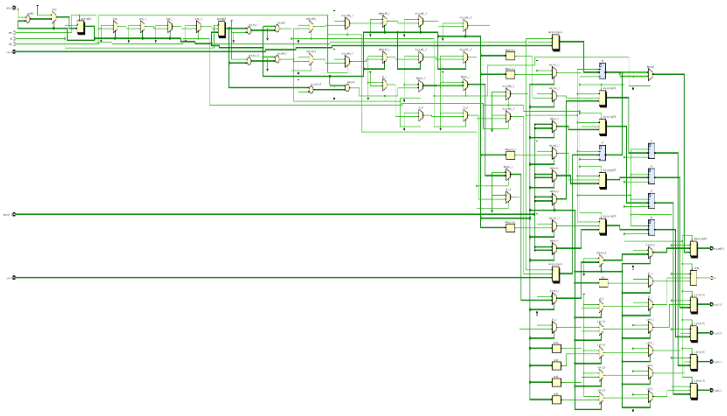

Fig.2. RTL of ECC on FPGA

3.1 RESOURCE UTILIZATION

In the implementation of ECC algorithm on FPGA, the following FPGA resources are utilized. These resources are such as Look Up Tables (LUTs), Flip Flop (FF), Global Buffer (BUFG), and Input Output (IO). The resource utilization of ECC algorithm is shown in Table.1, and its graphical representation is illustrated in Fig.3.

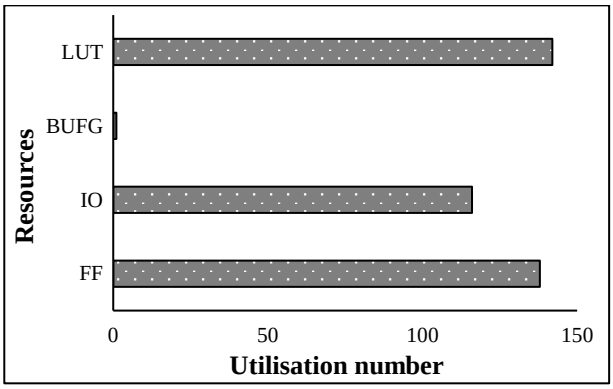

Fig.3. Graphical representation of utilized resource for ECC on Kintex-7

Table.1. Resource utilization for ECC on Kintex-7

Resources	Available	Utilization
FF	82000	138
IO	285	116
BUFG	32	1
LUT	41000	142

3.2 POWER ANALYSIS

Power consumption is a key factor for any device. In FPGA the Total Power Consumption (TPC) is the addition of Dynamic Power (DP) and Static Power (SP). The TPC for ECC on Kintex-7 is shown in Fig.4.

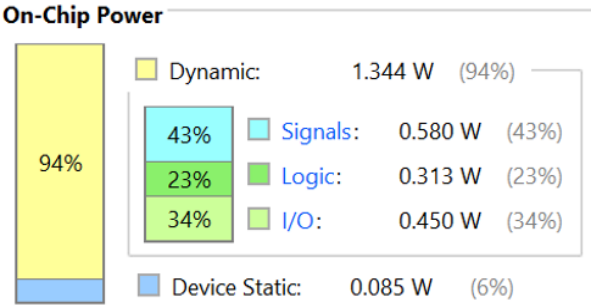

Fig.4. TPC for ECC on Kintex-7

From Fig.4, it is observed that the SP is 0.085 W. The SP counts 6% of the TPC. The DP is 1.344 W which is 94% of the TPC. Therefore, TPC is the sum of SP and DP (0.085+1.344) i.e., 1.428 W. The graphical representation of the on chips power is shown in Fig.5.

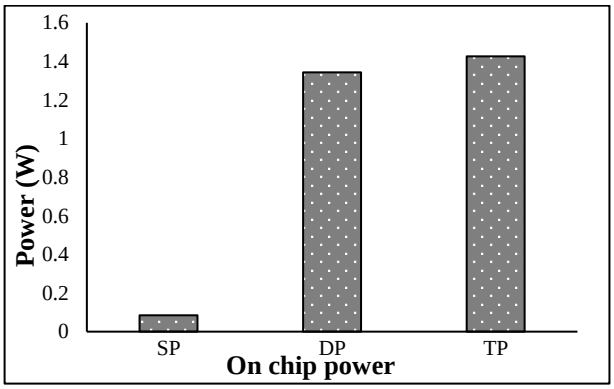

Fig.5. Graphical representation of TPC for ECC on Kintex-7

4. IMPLEMENTATION OF VEDIC MULTIPLIER BASED ECC ALGORITHM ON FPGA

In this section we will discuss about the implementation of Vedic Multiplier based ECC algorithm on FPGA device. For the implementation we have used Kintex-7 FPGA. The RTL schematic of the Vedic Multiplier based ECC implementation is represented in Fig.6.

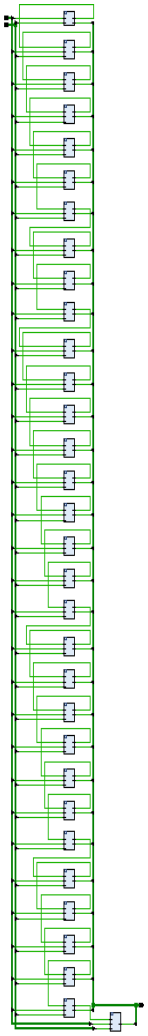

Fig.6. RTL schematic of Vedic Multiplier based ECC Algorithm

4.1 RESOURCE UTILIZATION

In the implementation of Vedic Multiplier based ECC algorithm on FPGA, the following FPGA resources are utilized. These resources are such as Look Up Tables (LUTs), Flip Flop (FF), Global Buffer (BUFG), and Input Output (IO). The resource utilization of Vedic Multiplier based ECC algorithm is shown in Table.2, and its graphical representation is illustrated in Fig.7.

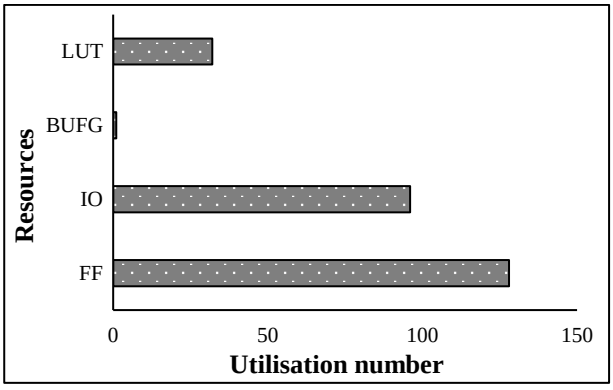

Fig.7. Graphical representation of utilized resource for Vedic Multiplier based ECC on Kintex-7

Table 2. Resource utilization for Vedic Multiplier based ECC on Kintex-7

Resources	Available	Utilization
FF	82000	128
IO	285	96
BUFG	32	1
LUT	41000	32

From Table.2, it is observed that for the implementation, 128 FF, 32 LUTs, 1 BUFG, and 96 IOs are required. While there are 82000 FF, 41000 LUTs, 32 BUFG, and 285 IOs are available on the device for utilization.

4.2 POWER ANALYSIS

Power consumption is a key factor for any device. In FPGA the TPC is the addition of DP and SP. The TPC for ECC on Kintex-7 is shown in Fig.8.

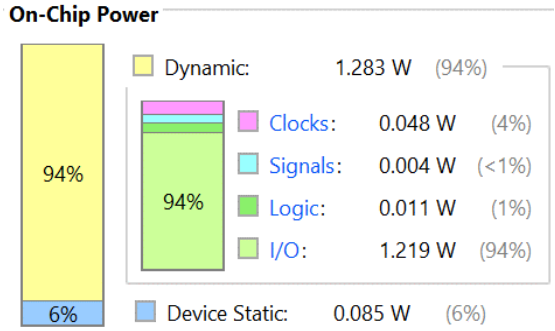

Fig.8. TPC for Vedic Multiplier based ECC on Kintex-7

From Fig.8, it is observed that the SP is 0.085 W. The SP counts 6% of the TPC. The DP is 1.283 W which is 94% of the TPC. Therefore, TPC is the sum of SP and DP (0.085+1.283) i.e., 1.367 W. The graphical representation of the on chips power is shown in Fig.9

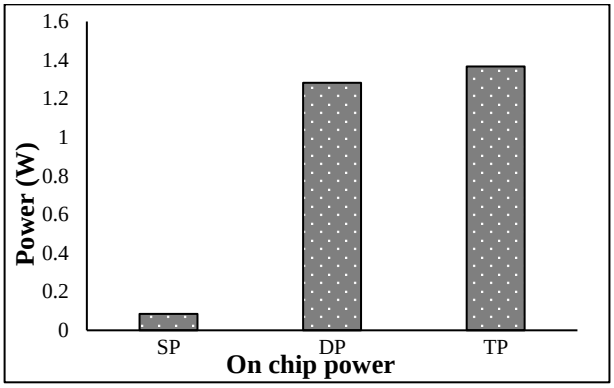

Fig.9. Graphical representation of TPC for Vedic Multiplier based ECC on Kintex-7

5. PERFORMANCE EVALUATION PARAMETERS

There are two important parameters for the comparison of traditional ECC with Vedic multiplier based ECC such as:

- **Area**: It is the number of FPGA resource utilized while implementing the algorithms on Kintex-7 device. It constitutes of the utilization of FF, IO, LUTs, and BUFG.
- **Power**: Power is the most important factor that plays the important role. The minimum the power consumption, the efficient working of the device and algorithm. In FPGA TPC is the sum of *SP* and *DP* (*TP= SP+DP*).

6. COMPARATIVE ANALYSIS

In this section a comparative analysis is done for both the traditional and Vedic multiplier based ECC. The comparison is done on the basis pf two factors such as: area and power. From the implementation sections of both the algorithms is observed that area consumption is reduced in Vedic multiplier based ECC in comparison to traditional ECC. There is the reduction in FF, IO, and LUTs utilization. The BUFG utilization is common for both. The comparative analysis of area is illustrated in Fig.10.

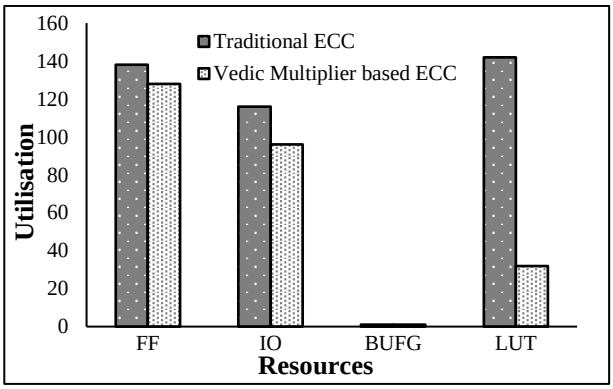

Fig.10. The comparative analysis of area

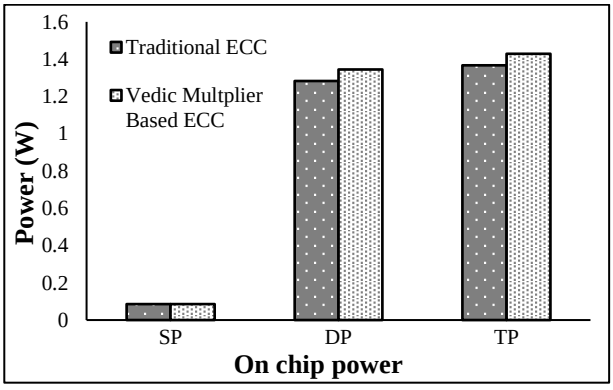

Fig.11. Comparative analysis of TPC

The TPC is also reduced for the Vedic multiplier based ECC as compared to traditional ECC. In both cases the SP are same. The change is observed only in DP. Therefore, the TPC of the both algorithms changes over Kintex-7 device. The comparative analysis of TPC is shown in Fig.11.

7. CONCLUSION

Security is the central issue regarding which the world is most concerned. Data security refers to the process of preventing unauthorized access to sensitive data. It comprises all of the cybersecurity techniques you use to protect your data from unauthorized access, including encryption, access controls (both physical and digital), and others. Data encryption is accomplished through the use of cryptographic techniques. In general, there are two kinds of cryptography standards: symmetric standards and asymmetric standards. Therefore, to enhance data security, we have implemented two versions of ECC algorithms on FPGA for better hardware security. The FPGA device used here is Kintex-7, and the two versions of ECC are such as traditional ECC and Vedic multiplier based ECC. It has been observed that the area consumption is reduced in Vedic multiplier based ECC as compared to traditional ECC. Not only area the power consumption is also reduced for Vedic multiplier based ECC. Hence it is concluded that for better hardware security with ECC on should chose Vedic Multiplier based ECC as compared to traditional ECC.

REFERENCES

[1] Keshav Kumar, K.R. Ramkumar and Amanpreet Kaur, “A Lightweight AES Algorithm Implementation for Encrypting Voice Messages using Field Programmable Gate Arrays”, *Journal of King Saud University-Computer and Information Sciences*, Vol. 83, pp. 1-18, 2020.

[2] Aryan Kaushik and Keshav Kumar, “Design and Implementation of Advanced Encryption Standard Algorithm on 7th Series Field Programmable Gate Array”, *Proceedings of International Conference on Smart Structures and Systems*, pp. 1-3, 2020.

[3] Keshav Kumar, K.R. Ramkumar and Amanpreet Kaur, “A Design Implementation and Comparative Analysis of Advanced Encryption Standard (AES) Algorithm on FPGA”, *Proceedings of International Conference on Reliability, Infocom Technologies and Optimization*, pp. 182-185, 2020.

[4] Keshav Kumar, K.R. Ramkumar and Amanpreet Kaur, “A Survey on Hardware Implementation of Cryptographic Algorithms Using Field Programmable Gate Array”, *Proceedings of International Conference on Communication Systems and Network Technologies*, pp. 189-194, 2020.

[5] K. Kumar, S. Malhotra and A. Kumar, “Design of Thermal-Aware and Power-Efficient LFSR on Different Nanometer Technology FPGA for Green Communication”, *Proceedings of International Conference on Communication Systems and Network Technologies*, pp. 236-240, 2021.

[6] K. Kumar, S. Malhotra and A. Kumar, 2019, "Frequency Scaling Based Low Power Oriya Unicode Reader (OUR) Design ON 40nm and 28nm FPGA”, *International Journal of Recent Technology and Engineering*, Vol. 7, No. 6, pp. 1-13, 2019.

[7] Bishwajeet Pandey, Keshav Kumar and Aiza Batool Shabeer Ahmad, “Implementation of Power-Efficient Control Unit on Ultra-Scale FPGA for Green Communication”, *3C Tecnologia*, Vol. 10, No. 1, pp. 93-105, 2021.

[8] Bishwajeet Pandey and Keshav Kumar, “Leakage Power Consumption of Address Register Interfacing with Different Families of FPGA”, *International Journal of Innovative*

Technology and Exploring Engineering, Vol. 9, No. 2, pp. 512-514, 2019.

[9] Keshav Kumar, Amanpreet Kaur, S.N. Panda, "Effect of Different Nano Meter Technology Based FPGA on Energy Efficient UART Design", *Proceedings of International Conference on Communication Systems and Network Technologies*, pp. 1-4, 2018.

[10] C.T. Poomagal, G.A. Sathish Kumar and D. Mehta, "Revisiting the ECM-KEEM Protocol with Vedic Multiplier for Enhanced Speed on FPGA Platforms", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 98, pp. 1-11, 2021.

[11] R.K. Kadu and D.S. Adane, "Hardware Implementation of Efficient Elliptic Curve Scalar Multiplication using Vedic Multiplier", *International Journal of Communication Networks and Information Security*, Vol. 11, No. 2, pp. 270-277, 2019.

[12] P. Ahuja, H. Soni and K. Bhavsar, "Fast, Secure and Efficient Vedic Approach for Cryptographic Implementations on FPGA", *Proceedings of International Conference on Electronics, Communication and Aerospace Technology*, pp. 1706-1710, 2018.

[13] P. Ahuja, H. Soni and K. Bhavsar, "High Performance Vedic Approach for Data Security using Elliptic Curve Cryptography on FPGA", *Proceedings of International Conference on Trends in Electronics and Informatics*, pp. 187-192, 2018.

[14] S. Karthikeyan and M. Jagadeeswari, "Performance Improvement of Elliptic Curve Cryptography System using Low Power, High Speed 16× 16 Vedic Multiplier based on Reversible Logic", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 12, No. 3, pp. 4161-4170, 2021.

[15] R.K. Kodali, S.S. Yenamachintala and L. Boppana, "FPGA Implementation of 160-Bit Vedic Multiplier", *Proceedings of International Conference on Devices, Circuits and Communications*, pp. 1-5, 2014.

[16] T.S. Reddy and Y.D.S.Raju, "Implementation of Data Security with Wallace Tree Approach using Elliptical Curve Cryptography on FPGA", *Turkish Journal of Computer and Mathematics Education*, Vol. 12, No. 6, pp. 1546-1553, 2021.