Comparative Study of Secure and Efficient Cryptography on FPGA

[1]Prashant Ahuja, [2]Prof. Hiren Soni
[1]Electronics & Communication Engineering, [2]Assistant Professor
[1]Vlsi & Embedded System Design, [2]Electronics & Communication Engineering
[1]GTU PG SCHOOL, Gandhinagar, Gujarat, India [2]A. D. Patel Institute of Technology, Gujarat, India

Abstract – Cryptography is the most preferred field for data security in security field. Today Data security is most preferred because each person needs their data in secured form. Cryptography provides security between sender and receiver. Cryptography has a number of algorithms & standards for security. In Asymmetric Cryptography there is issue of speed whereas Symmetric Cryptography is little bit poor in security. As far as hardware security is concerned, FPGA is the best tool in market. This Paper contains the survey about some security algorithms for data security on FPGA.

Index Terms – Cryptography, Security, Speed, FPGA, ECC.

I. INTRODUCTION –

In Today's generation, data security is Prime concern when we talk about data transmission from one end to another end. Today Data security is most preferred because each person needs their data in secure form. Security in term of no other unauthorised person can see our data when we communicate. This requirements are fulfilled by Cryptography. Cryptography has a number of algorithms and standards for data security on FPGA.

II. TYPES OF CRYPTOGRAPHY –

There are two fields in Cryptography named as Symmetric Cryptography and Asymmetric Cryptography. Symmetric Cryptography has same keys for encryption and decryption purpose as its name suggest. Because of this reason it provides less security (key exchange problem) but its advantage is speed for the same reason. Key exchange problem means in symmetric same key is used for both encryption and decryption, so before communication sender and receiver have to share their key for current session in one message. And if the message containing key is hacked by unauthorized person then there is no meaning of the whole cryptography. That's why it has poor security as compared to Asymmetric one. As we talk about same keys that means lesser area requirement for key storage and need to perform lesser operations to secure our data; so it offers great advantage of speed.

Whereas, Asymmetric Cryptography has different keys for encryption and decryption purpose. Because of this reason, it requires greater area for key storage so speed of this type of cryptography is very poor and more operations are performed for data security, so security is quite strong (no any key exchange problem) here as biggest advantage of these standards.

So when Speed is Prime concern then Symmetric Cryptography is preferred and of course when more security is Prime concern then Asymmetric Cryptography is most preferred. Symmetric Cryptography has certain standards like DES, 3DES, AES, IDEA, Blowfish, RC4, RC5 & RC6 and Asymmetric Cryptography has certain standards like Diffie-Hellman, RSA, ElGamal, **ECC**, DSA, and Knapsack. In Symmetric Cryptography AES (Advance Encryption Standard) is most widely used in industry because of its greater speed advantage whereas in Asymmetric Cryptography ECC (elliptic curve cryptography) is most widely used in industry because of it offering great Security. AES offering very poor security then ECC and 160-bit ECC encryption key provides the same security as a 1024-bit AES/RSA encryption key and can be up to 15 times faster, depending on the platform on which it is implemented. ECC is the best when security is the prime concern.

III. OVERVIEW OF CRYPTOGRAPHIC ALGORITHMS & STANDARDS ON FPGA –

As we know FPGA offers the best hardware security and higher processing power so it's the most preferred tool for implementation of Cryptography with taking the advantage of its hardware security. Many implementations done on FPGA in Both Symmetric as well as Asymmetric cryptography.

1. AES - Sub Bytes, Shift Row, Mix Column and Add Round Key –

One implementation done on FPGA in VHDL language used AES standard with Sub Bytes, Shift Row, Mix Column and Add Round Key technique. The AES cryptography algorithm is used to encrypt or decrypt the blocks of 128 bits. And also it is capable of using cipher keys of 128 bits (**AES 128**). Use of this algorithm will lead to an increase in the message encryption throughput. The biggest advantage of this technique is speed, system throughput and zero delay at output side. But again the disadvantages was less security then ECC. [1]

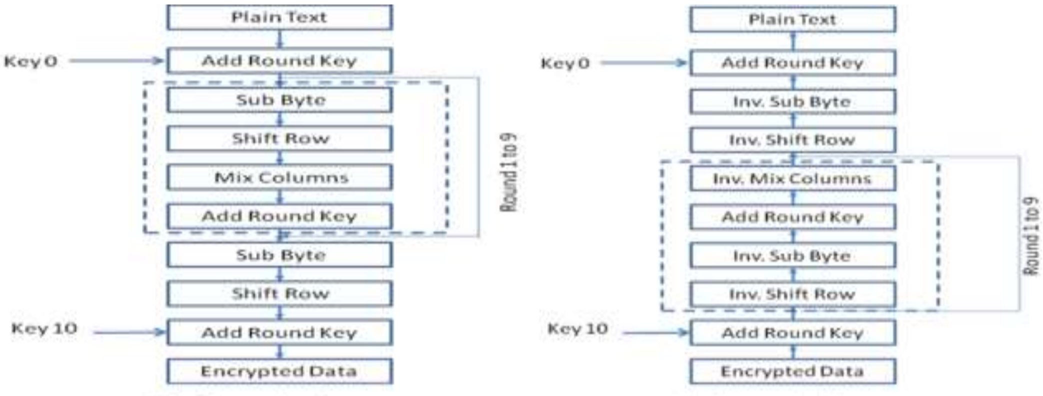

Fig: Encryption Structure *Fig: Decryption Structure*

Fig.1 AES Encryption-Decryption Process [1]

2. AES with Vedic multiplier (8 bit) –

Another implementation done on FPGA in Verilog language used AES standard with Vedic Multiplier as taking advantage of Vedic's greater speed and less area and power requirement as compare to other multipliers. They used 8 bit Vedic multiplier so it processed 8 bit at a time which improves the system performance in terms of speed. The disadvantages was offers security then ECC. [2]

Structure of Vedic multiplier (8 bit) is shown below

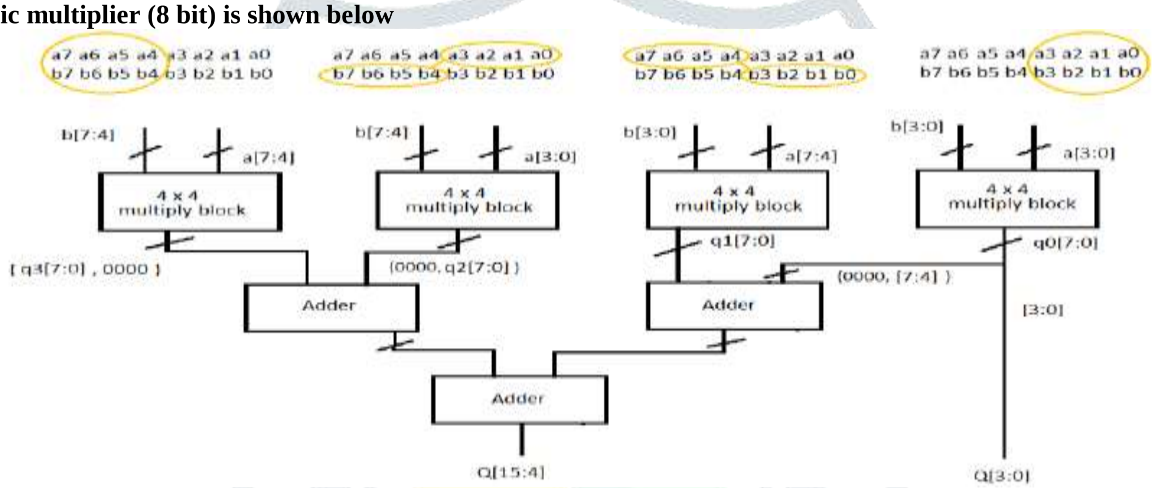

Fig.2 Vedic Multiplier (8 bit) [2]

3. Hardware implementation of ECC using FPGA –

One implementation done on **Spartan 3E** FPGA in Verilog language used ECC standard with offering greater security. They used 4 bit parallel multiplier which processed 4 bit at a time which improves the system performance in terms of speed as compared to normal ECC implementation. They have all advantages of ECC like it performs its process in less time, less memory, less computations and less power consumption. So they are more suitable for embedded environment. The hardware implementation of ECC using FPGA enhances the system performance since FPGA technology is faster by nature and much more secure than software implementations. The disadvantages was less performance in terms of speed then AES. [3]

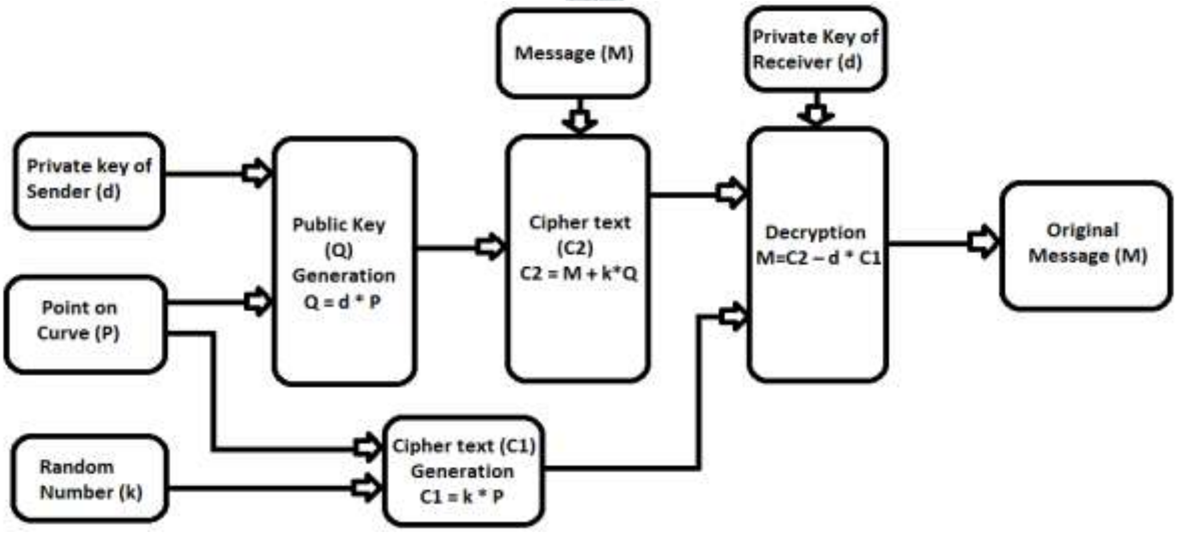
Message (M)
Private Key of Receiver (d)
Private key of Sender (d)
Public Key (Q) Generation Q = d * P
Cipher text (C2) C2 = M + k*Q
Decryption M=C2 – d * C1
Original Message (M)
Point on Curve (P)
Random Number (k)
Cipher text (C1) Generation C1 = k * P

Fig.3 ECC Implementation [3]

4. ECC with ElGamal encryption method –

Another implementation which done on FPGA in Verilog language used ECC standard with ElGamal standard for dual security which resulted in improved greater security but drastically reduction of speed. The point on curves are then encoded by ElGamal encryption technique and decoded to recover original message by ElGamal decryption technique. These system offers great security but makes system more complex and slower is their disadvantage. [4]

Key Generation :-
Generate large prime p and generator g, Select a random integer a, and compute g^a mod p.
Where, **A's Public key is (p, g, g^a); A's Private key is a.**
Alice chooses her **public key (17, 6, 7) :-**
Large Prime p = 17**, Generator** g = 6**,**
Private key part a = 5 (a=1, a=2 until 6^a mod 17= 7).
Public key part - g^a mod p = 6^5 mod 17 = 7.

Encryption :-
(Large Prime p = 17, Generator g = 6, Private key part a = 5)
Represent the **message as integers m** in the range {0, 1, . . . , p − 1}.

- **m = 13**

Select a **random integer k**, 1 ≤ k ≤ p − 2.

- **k = 10**

Compute γ = g^k mod p and δ = m ∗ (g^a)^k.

- **γ = g^k mod p = 6^10 mod 17 = 15 &**
- **δ = m ∗ (g^a)^k = (13 ∗ 7^10) mod 17 = 9.**

  where, (g^a mod p = 6^5 mod 17 = 7)

Send **cipher text c = (γ, δ) = (15, 9)** to A.

Decryption :-
A receives γ = 15 and δ = 9 from Bob.
Her public key is (p, g, g^a) = (17, 6, 7) & Her private key is a = 5.

Alice now decrypts the message using her private key:

Decryption factor = (γ^(p−1−a)) ∗ δ mod p

- **(γ^(p−1−a)) mod p = (15^(17-1-5)) mod 17**
  = 15^11 mod 17
  = 9.
- **(δ ∗ 9) mod p = (9 ∗ 9) mod 17 = 13**

Alice has now decrypted the message and received: **13**. [4]

5. ECC with double point multiplication algorithm –

They used ECC on FPGA with double point multiplication algorithm. So they had all ECC advantages, FPGA advantages and because of double point multiplication algorithm they offer great dual security then normal ECC without making system more complex. They used 16 bit parallel multiplier which processed 16 bit at a time for operations so improved in terms of speed as compared to previous ECC implementations. The disadvantage is System is still slower than symmetric type. [5]

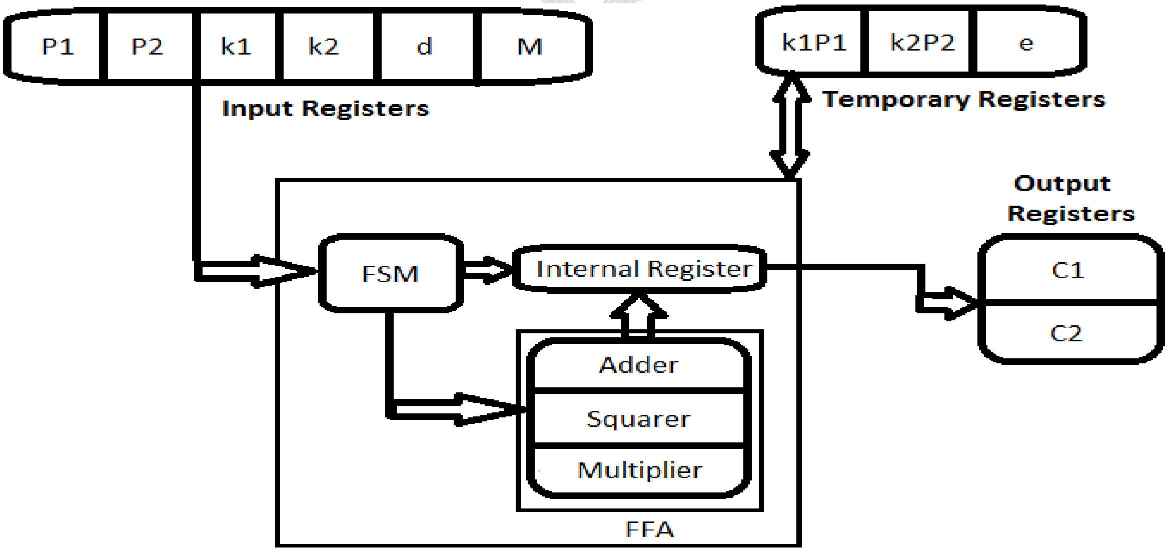

Fig.4 Elliptic curve cryptography Processor [5]

IV. CONCLUSION –

In Cryptography, there is always a trade-off between security and performance (speed). As we increase in security then complexity of system also gradually increases which resultant in more area consuming, degradation in performance (speed) of system. The future work is to find a solution which can maintain greater Security with efficient way in terms of improves speed, reduction in power and area requirements.

REFERENCES

[1] Nupur D. Vaidya, Dr. Yogesh. A. Surya wanshi & Dr. Manish Chavan "Design for Enhancing the Performance of Advance Encryption Standard Algorithm VHDL" International Conference on Green Engineering and Technologies (IC-GET), 2016.

[2] Amit Kumar, Hitesh P ahuja & Balwinder Singh "Design and Analysis of the high speed AES using Ancient Vedic Mathematics novel Approach" IEEE, 2016.

[3] Mustafa Nawari, Hazim Ahmed, Aisha Hamid, Mohamed Elkhidir "FPGA Based Implementation of Elliptic Curve Cryptography" IEEE, 2015.

[4] Balamurugan.R, Kamalakannan.V, Rahul Ganth.D & Tamilselvan.S "Enhancing Security in Text Messages Using Matrix based Mapping and ElGamal Method in Elliptic Curve Cryptography" IEEE, 2014.

[5] Sunil Devidas Bobade & Dr.Vijay R. Mankar "VLSI Architecture for an Area Efficient Elliptic Curve Cryptography Processor for Embedded Systems" International Conference on Industrial Instrumentation and Control (IClC), 2015.