International Journal of Research Studies in Science, Engineering and Technology
Volume 2, Issue 6, June 2015, PP 99-102
ISSN 2349-4751 (Print) & ISSN 2349-476X (Online)

FPGA Implementation of Hybrid Cryptographic Algorithm

Vinutha M, Dr. Siva Yellampalli

VTU, Extension center, UTL Technologies Limited
Bangalore, India

Abstract: *In this advanced computer network and communication technology, the internet attacks are also versatile so, security is a vital component of effective communication in a digital world, the traditional encryption algorithm [single data Encryption] is not much suitable for securing information over the network.*

The alternative is to design an algorithm that presents the need of high security with minimum computational effort. The Gold-Wasser-Micali cryptosystem is an asymmetric- key encryption algorithm developed by Shafi-Gold-Wasser-Micali has distinction of being the first Probabilistic public-Key encryption scheme. Which is proven by Secure under the Standard Cryptographic assumption. The main aim of this paper is to design and implementation of complexity involved in Gold-Wasser-Micali Probabilistic encryption and decryption algorithm. Hybrid cryptosystem is developed in this provides a shield against brute force attacks and cryptosystem mainly concentrate on increased level of security. This system is successfully implemented on Vertex 7 FPGA using Verilog as programming language. Synthesizing and implementation of the code is carried out on Xilinx-Project Navigator ISE 13.1 suite.

Keywords: *Elliptical Curve Cryptography, Multi-bit Pseudorandom Number Genarator, Gold-Wasser- Micali Probabilist encryption and decryption.*

1. Introduction

Rapid development on electronic technology security over the communication and networking is an big concern. During this time the internet provides essential communication between tens of millions of people and is being increasingly used, security becomes a tremendously important issue.

Cryptography is one of the essential aspects for secure communications. It is the art of achieving security by encoding messages to make them non-readable and also it is the practice and study of hiding information.

Mainly there are two types of cryptography: Symmetric key and Asymmetric key. Symmetric key algorithms are the quickest and most commonly used type of encryption. Here, a single key is used for both encryption and decryption. In Asymmetric key algorithm using two different keys one is public key and another one is private key for encryption and decryption.

Now a day Elliptic Curve Cryptography (ECC) is the most efficient public key encryption scheme based on elliptic curve concepts that can be used to create faster, smaller and efficient cryptographic keys. Security is the most attractive feature of elliptic curve cryptography.

1.1. Elliptical Curve Cryptography (ECC)

Elliptic curve cryptography (ECC) is a public key cryptosystem like RSA, Rabin, and El-Gamal encryption algorithm. Every user has a public and a private key. Public key is used for encryption and signature verification. Private Key is used for decryption and signature generation.

ECC has smaller public key sizes than both RSA and DSA/DH for most routine operations while offering security. The reason is that ECC provides greater efficiency in terms of computations overheads, key sizes and bandwidth. In Implementations, these savings means higher speeds, lower power consumption.

ECC provides level of security with a 164 bit key that RSA require a 1,024 bit key to achieve, Because ECC helps to establish equivalent security with lower computation power and battery resource usage. The ECC covers all primitives of public key cryptography like digital signature, key exchange, key transport, and key management. Presently ECC has been commercially adopted by many standardized organization such as NIST (National Institute of Standards and Technologies), and ANSI (American National Standard Institute).

1.2. Gold-Wasser-Micali Cryptosystem

The Gold-Wasser - Micali cryptosystem is an asymmetric key encryption algorithm developed by Shafi-Gold-wasser and Silvo Micali in 1982.

Traditional algorithms such as RSA and ECC generate the same cipher text each time for the same plain text message. This makes it is easy to see if the same message is sent more than once .With the above flaws in mind Gold-Wasser-Micali introducing the concept of 'randomness' there by generating of dynamic cipher text for the same plaintext, also known as Probabilistic encryption.

2. MULTIBIT LFSR PSEUDO RANDOM NUMBER SEQUENCE GENERATOR

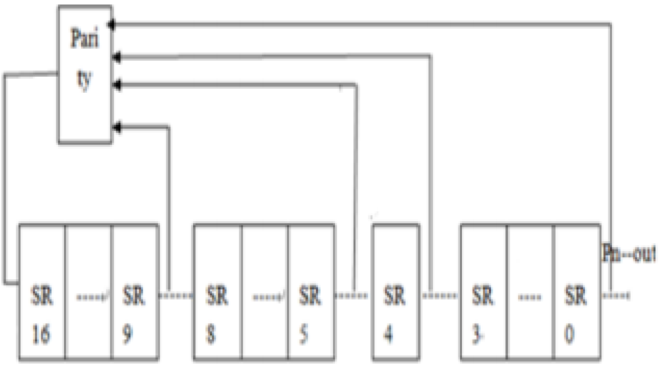

Fig1. *Multi bit LFSR Pseudo Random Number Sequence Generator*

Pseudo Random Number Sequence is generated in Verilog according to the following circuit based on the fig1 the concept of shift register. The linear feedback shift register is made up of two parts: a shift register and a feedback function. The shift register is initialized with n bits (called the key) and each time a key stream bit is required all of the bits in the register are shifted 1bit to the right. So the least significant bit is the output bit. The new left most bit is computed as the XOR of certain bits in the register. This arrangement can potentially produce 2^n-1 bit long Pseudo-Random Sequence before repeating.

The following polynomial equation is used for algorithm implementation.

$$I(X) = X^{17} + X^5 + 1 \qquad (1)$$

$$Q(X) = X^{17} + X^9 + X^5 + X^4 + \qquad (2)$$

Using LFSR Equation (1) and Equation (2) generates 64 bit Pseudo Random Number Sequence.

3. SYSTEM DESIGN

In any system, each component makes a complete system. In this Section establishing the connection between each component and understanding about their functions.

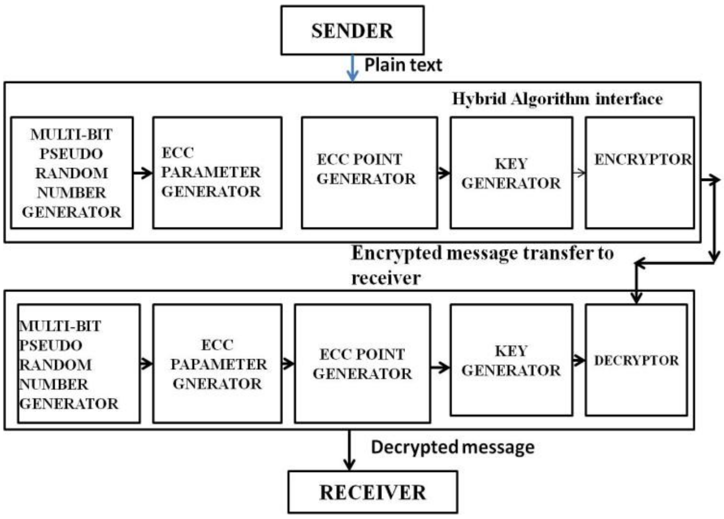

Fig2. *Shows the system design of Hybrid Algorithm*

3.1. Sender and Receiver

The Person who wants to send a message securely to receiver over the communication channel using hybrid Cryptosystem is called Sender. Data that can be read and understood without any special measures is called Plain text. The method of disguising plain text in such a way as to hide its substance is called Encryption. Encryption Plain text results in unreadable format called Cipher text. The Reverse process of cipher text to its original plain text is called Decryption. Finally the decrypted message will send to the Receiver.

3.2. Random Number Generator

The Random Number Generator is an important component of Hybrid Algorithm Interface. The 64bit pseudo random number sequence is generated using 16bit LFSR with the concept of shift register and provides it to Key generation process and ECC parameter generator.

3.3. ECC Parameter Generator

This module finds the suitable values for the Elliptic Curve Parameters: p, a and b. Parameter p is obtained using LFSR Pseudo Random Number Generator. Parameter a and b should be generated such that, they should satisfy the condition $(4A^3 + 27B^2) \bmod P \neq 0$.

3.4. ECC Point Generator

In this section, for achieving higher security, mapping the 8 bit input plain text to 164 bit .The point P(X, Y) are 164 bit each, It should lie on the ECC curve $Y^2 = X^3 + AX^2 + B$. Since ECC is implemented using prime field F (P), the condition: $Y^2 \bmod P = (X^3 + AX + B) \bmod P$ should be satisfied by the generated point.

3.5. Key Generator

This module generates ECC public key, and ECC private key for Encryption and Decryption. Using ECC parameter it generates ECC public key. The points co-ordinates are converted as nearest primes as (p,q) which is used as Gold Wasser-Micali algorithm private key, from private key , public key (n,y) is generated.

3.6. Encryptor and Decryptor

Using private key and public keys generated by key generator, encryptor will encrypt the message using 163 bit size encryption. Figure 3 shows the flowchart of encryption. Similarly, using 163 bit size decryption technique the original message is retrieved by receiver.

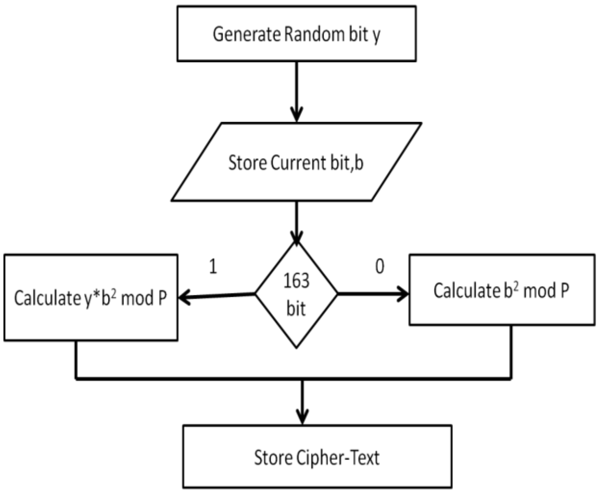

Fig3. *Flow chart of Encryption Algorithm*

4. Conclusion

The bitwise approach of probabilistic encryption has been criticized as not feasible to implement in practice because of message expansion resulting from the encryption of each bit. So, for faster encryption and decryption made some modifications in the existing algorithm and have been implemented in this project succefully. An effective random number generator has been developed to increase the strength of cryptosystem. The developed cryptographic algorithm uses 64bit key for encryption and decryption.

REFERENCES

[1] "Anjan Mathematiocal Model of Hybrid Cryptographic Algorithm- A^3 D Algorithm". International Journal of Advanced Research in Computer and Communication Engineering Vol.3, Issue 6, June 2014.

[2] Orhio Mark Creado, Xianping Wu, Yiling Wang, Phu Dung Le, "Probabilistic Encryption: A Practical Implementation", Proceeding of the Fourth International Conference on Computer Sciences and Convergence Information Technology, Melbourne, Australia, 2009,pp. 1130-1136.

[3] Shruthi R, Sumana P, Anjan Koundinya K, "Performance Analysis of Goldwasser-Micali Cryptosystem," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2(7), July 2013, pp. 2818-2822.

[4] Orhio Mark Creado, Xianping Wu, Yiling Wang, Phu Dung Le, "Probabilistic Encryption: A Comparative Analysis against RSA and ECC", Proceeding of the Fourth International Conference on Computer Sciences and Convergence Information Technology, 2009, pp. 1123-1129.

[5] Sonali Nimbhorkar, Dr.L.G. Mallik, "Prospective Utilization of Elliptic Curve Cryptography for Security Enhancement," International Journal of Application or Innovation in Engineering and Management, Vol 2, Issue 1, January 2013.

[6] Mr. Mahavir Jain, Mr. Arpit Agrawal, "Implementation of Hybrid Cryptographic Algorithm," International Journal of core Engineering and Mangement, vol 1, Issue 3, June 2014.

[7] Tarun Narayan Shankar, G.Sahoo, "Cryptography with Elliptic Curves,"International Journal of Computer Science and Applications, Vol. 2, No. 1, April/May 2009.