RESEARCH ARTICLE OPEN ACCESS

# FPGA Implementation of Key Exchange Algorithm

[1]Vadde SeethaRama Rao [2]Krishna Bharat Battala
*[1,2] Assistant Professor*
*Sreenidhi Institute of Science and Technology, Hyderabad.*

**ABSTRACT**
Due to rapid growth of Digital Communication, transmission of digital data plays a major role over in secured communication Channel. The main aim of this paper to establish Diffe Hellman key Exchange Algorithm which requires two keys one is for public and another one is for private key which establishes Asymmetric Cryptographic technique. This algorithm has several security applications such as secured socket layer (SSL), Internet Protocol Security (IPSec) etc. This technique is designed by using Verilog HDL with Xilinx ISE Design suite 13.2 version tool. The design is implemented in Xilinx Virtex 5 series device (XCVLX5110T) FPGA board. This project also includes Generation of ICON and VIO core for the design and on chip verification and analyzing using Chipscope Pro.

**Key words:** Chipscope pro, Cryptographic, Verilog HDL

---

Date of Submission: 23-11-2017 Date of acceptance: 02-12-2017

---

## I. INTRODUCTION

Due to rapid growth of Communication System exchanging of data plays a major role in entire system in secured manner. The demand of this security over communication channel has growing exponentially day to day. So, in the recent trends in communication system protection of data, Integrity of the data, Security of the data is needed. The major change that effected security was over, distributed systems and use of Networks. So, Network Security plays a major role in protection of data over in secured communication Channel. In order to protect the Network Security, this cryptographic techniques vital role. Cryptography derived from Greek word crypto means "hide" and graphic means "study".

### 1.1 Model for Network Security

Security aspects come into play when to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. The security related information can sent over the channel with the help of Encryption Technique and recollecting back original information with Decryption A model of Network Security is given as the fallowing 1.1.The fallowing terminologies are present in the Block Diagram are as follows: **Plain Text:** This is the original available message or data that is fed into Encryption Algorithm. **Encryption Algorithm:** The Conversion of plain into cipher test is known as Encrption.With the message X and the Encryption K key as input, the Encryption Algorithm forms the $\boldsymbol{Y = E_K(X)}$ Cipher text. **Decryption Algorithm:** Decryption is the Inverse process of Encryption. Conversion of cipher text to plain test is known as Decryption We can write this as $\boldsymbol{X = D_K(Y)}$

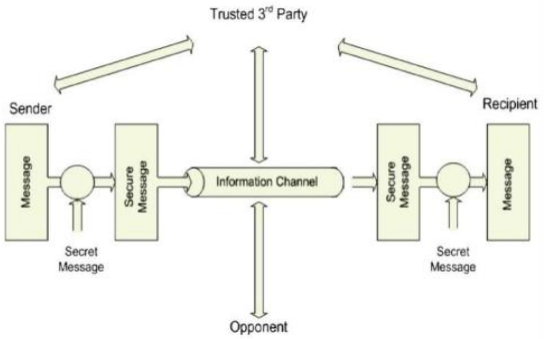


**Fig: Block Diagram for Network Security Model**

**Secret key:** The secret key is also input to the Encryption Algorithm. The key is a value independent of the Plain Text and of the Algorithm. The Algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the Algorithm depend on the key. **Cipher text:** The data obtained after Encryption is known as Cipher text data which is present in cipher text not detectable **Cryptanalysis:** Hacker **or** un trusted party is trying to retrieve the original message with knowing the key is called as Cryptanalysis

## II. DIFFIE HELLMAN KEY EXCHANGE ALGORITHM

Diffie–Hellman key exchange is one of Asymmetric Cryptographic Algorithm The Diffie–

Hellman key exchange method is used to exchange key between two members without knowing prior Knowledge of each other to jointly establish a shared secret key over an insecure communications channels. This Protocol mainly uses modulus theory with prime numbers from 1 to P-1 were p is the prime number .Diffie Hellman Algorithm is not for Encryption or Decryption but it enable two parties who are involved in communication to generate a shared secret key for exchanging information confidentially

**2.1 Steps in DH Algorithm**

1. Let p &g be the two prime numbers as a Public key.
2. Alice chooses a large random number x, such that 0<x <p and calculate $R_1 = g^x \bmod p$.
3. Bob chooses another large random number y, such that 0<y <p and calculate

$R_2 = g^y \bmod p$

4. Alice sends $R_1$to Bob.
5. Bob sends $R_2$to Alice.
6. Alice computes K Alice = $(R_2)^x \bmod p$.
7. Bob computes K Bob = $(R_1)^y \bmod p$.

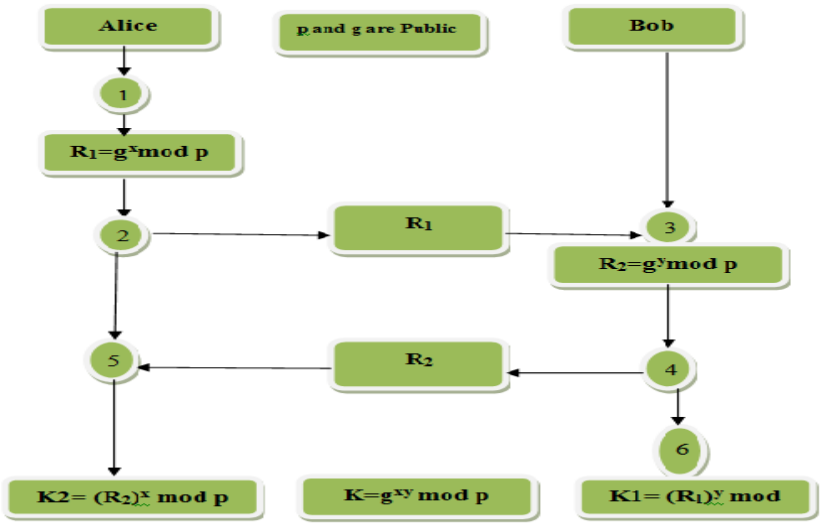


**Fig:** Flow Chart of DH Algorithm

**2.2 Advantages of DH Algorithm:**

DH Algorithm key agreement not limited to negotiating a key shared by only two Participants. Any number of users can take part in an agreement by performing iterations of the agreement protocol and exchanging intermediate data which does not itself need to be kept secret

**2.3 Disadvantages:**

DH Algorithm is susceptible to two types of attacks.

1. Discrete logarithmic attack.
2. Man in the middle attack

## III. SIMULATION RESULTS

This chapter presents Computer simulation results using Xilinx ISE (Integrated Software Environment) software for DH Algorithm Xilinx ISE Tools are mentioned below:

**Table3.1:** List of tools used

| Design action | Tool name |
|---|---|
| Design Entry | Verilog HDL |
| Synthesis | XilinxSynthesisTool(XST) |
| Simulation | ISE Simulator |
| FPGA Board | *XCVLX5110T* |

The design of DH Algorithm consists of basically two modules Power module and Division module In the power module basic inputs and out puts are base ,power and output. Based on the power, for every rise in clock edge power will be incremented according to our requirements till our count is satisfied.

**Inputs :**

a(31:0) -it is called as base

n(31:0) - it is called as power i.e. that number of times base is multiplied by itself.

Clk - it is clock for module

**Output:**

b(31:0)- the result of the $[a(31:0)]^{n(31:0)}$

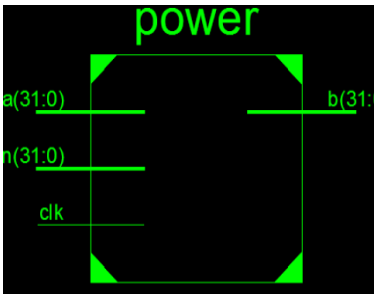


Fig:RTL Schematic for Power Module

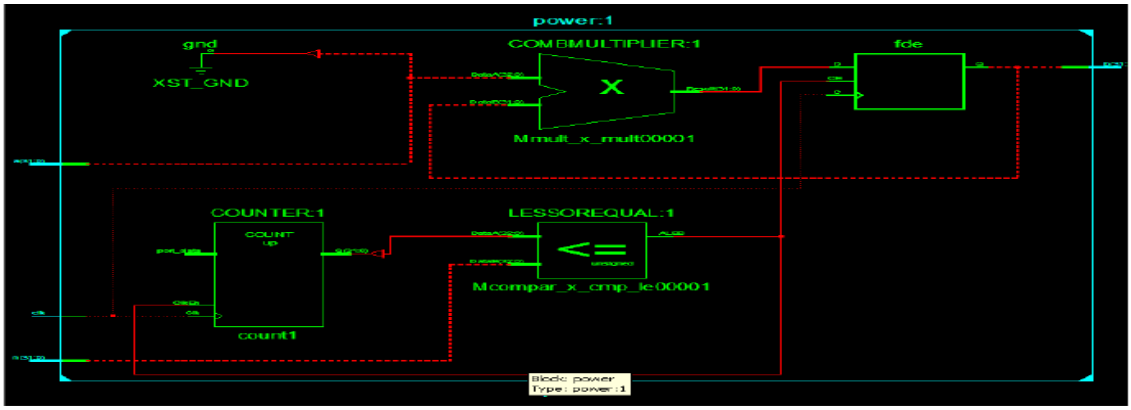


**Fig:** Technology Schematic for power module**.**

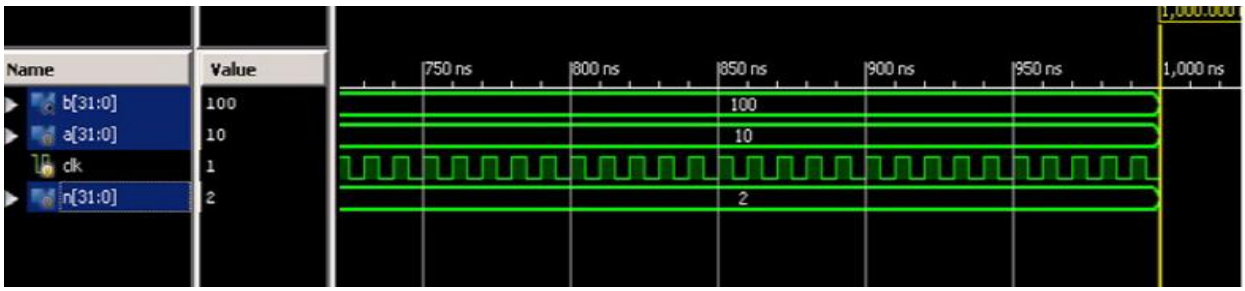


Fig: Simulation result for Power Module.

In order to calculate the key we have to do the modulo operation .This modulo operation can be obtained by taking remainder after the binary devision.So.in order to do the Division operation inputs are Dividend and Devisor .Out puts are Quotient and Remainder .It consists of two inputs &two outputs

| Inputs are | Outputs are: |
|---|---|
| Dividend (31:0) | Quotient (31:0) |
| Divisor (31:0) | Reminder (31:0) |

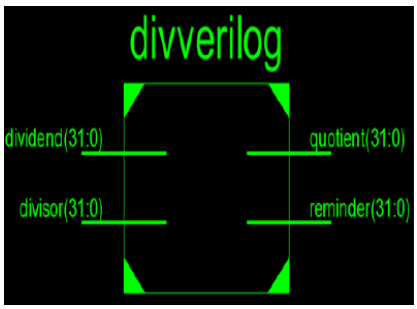


Fig: RTL Schematic for Division Module

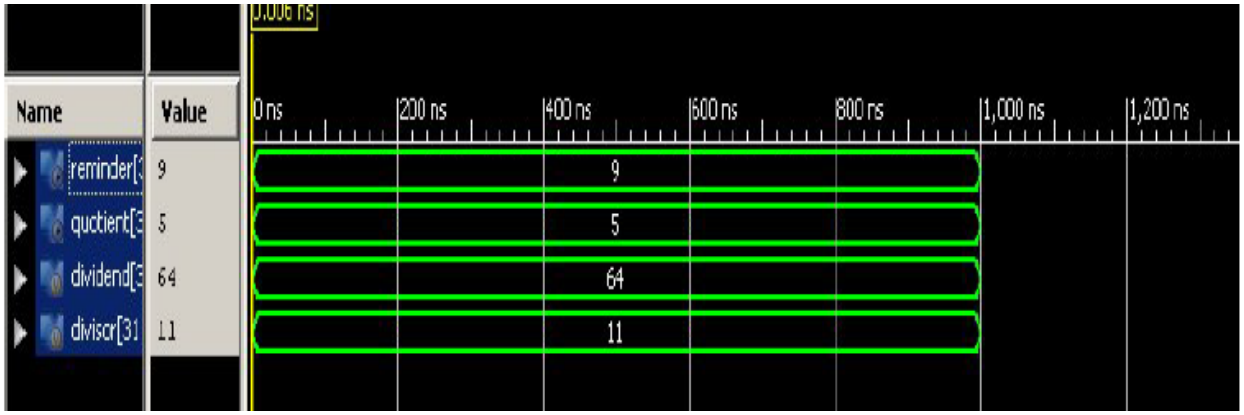

Fig: Simulation result for Division Module

**DH key Exchange Algorithm**

Diffie–Hellman key Exchange (D–H) is a Asymmetric method of exchanging Cryptographic keys. It is has two keys i.e. public key and Private key. In this Algorithm p &g are acting as public key inputs and the x&y are acting as private key inputs. Here **x** is acting as an Alice Private key and **y** is acting as a Bob's private ke

| **Inputs:** | **Outputs** |
|---|---|
| p(31:0)&g(31:0) are the Public key | K1(31:0)=Alice Secret key |
| X(31:0) is the Alice Private key | K2(31:0)=Bobs Secret key |
| Y (31:0)is the Bobs Private key | |

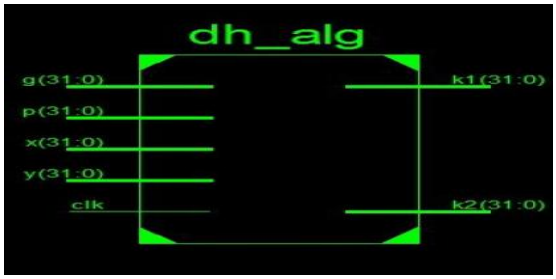

Fig: RTL Schematic for DH Algorithm

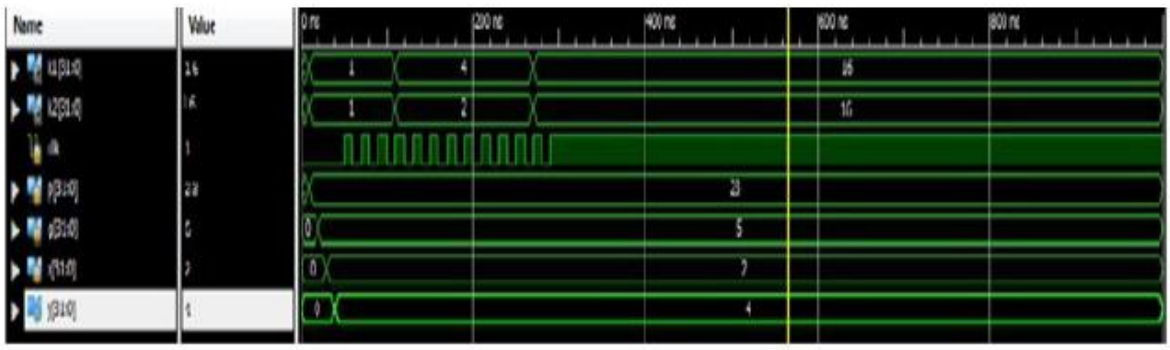

**Fig:** Simulation result for DH Algorithm.

## IV. CONCLUSION &FUTURE SCOPE

The proposed model can be improved by using Blow fish Algorithm, RSA Algorithm etc. With multiple Encryption and Decryption techniques.. Better Key length will provide better symmetric algorithm implementation and security.

## REFERENCES

[1]. Fischer, Michael J., (2010), "Cryptography and Computer Security", Department of Computer Science, Yale University, March 29, 2010.

[2]. Forouzan, Behrouz A. (2008), "Cryptography and Network Security", McGraw-Hill, Int. Ed. 2008.
[3]. Ibrahim M.K(2012)Modification of Diffie Hellman key exchange Algorithm for Zero Knowledge Proof Published in: future communication Networks (ICFCN)2012International conference.
[4]. Back, Amanda, (2009), "The Diffe-Hellman key Exchange", December 2,2009,.
[5]. Carts, David A., (2001), "A Review of the Diffie- Hellman Algorithm and its Use in Secure Internet Protocols", SANS Institute, 2001.

International Journal of Engineering Research and Applications (IJERA) is **UGC approved** Journal with Sl. No. 4525, Journal no. 47088. Indexed in Cross Ref, Index Copernicus (ICV 80.82), NASA, Ads, Researcher Id Thomson Reuters, DOAJ.

1Vadde SeethaRama Rao FPGA Implementation of Key Exchange Algorithm." International Journal of Engineering Research and Applications (IJERA) , vol. 7, no. 12, 2017, pp. 05-09.