International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 5, May - 2014

Design and Implementation of Stream Cipher Key Exchange in FPGA

Greeshma Vijayan[1],
ME Applied Electronics,VCEW, Dr.K.S.Lalmohan[2],HOD,VLSI dept,NIELIT,
Dr. A. Muruganandham[3],HOD,ECE dept.,VCEW

***Abstract*-With the advent of technology there are many applications that require secure data transmission like internet banking, e-mail, mobile telephones etc. These sensitive data need to be protected from being eavesdropped or else the result will be devastating. Today's demands of secure data exchange rely mostly on the use of cryptography. Cryptography provides a method for securing and authenticating the transmission of information over insecure channels. For encryption of data, stream ciphers are preferred to block ciphers because it consumes less power and hardware. The proposed system is a modification of the hash block in which it introduces a key exchange block similar to the Diffie Hellman key exchange system to exchange the value in the Key, between the sender and the receiver. The design of stream cipher based on hardware efficient hash function was reported earlier but the security of this stream cipher was proved to be very low in a paper which appeared later. In this paper, we made the design more secure to overcome this weakness and, without much increase in hardware complexity.**

***Index Terms*-Hash function, cryptosystems, Stream cipher, FPGA**

I. INTRODUCTION

A secure communication system contains a symmetric key encryption system, a hash algorithm and a method for providing digital signatures and key exchange using public key cryptography. The hardware used today makes use of three different algorithms operating independently there by increasing the hardware complexity.[1]Since the operations of key exchange, message encryption and hash generation are done sequentially an encryption and hash generation system built using the infrastructure available for key exchange will be highly acceptable.

This work aims to design and implement key exchange, message encryption and hash generation on a single field programmable gate array (FPGA).

The flexibility and high speed capability of FPGAs make them a suitable platform for cryptographic applications. Their structure allows complex arithmetic operations that are not suited to general purpose CPUs to be implemented more efficiently.

The remainder of the paper is organized as follows: In Section 2, review of stream cipher is discussed, Section 3,key exchange and hash generation are introduced. In section 4 Diffie hellman key exchange algorithm is presented. In Section 5, simulation result is discussed, and finally the paper is concluded in section 6 .

II. STREAM CIPHERS

Stream ciphers allow real time operation, which is usually not possible with block cipher encryption. The need for buffer space is very less in stream ciphers, since data is operated bit by bit. Most critical step in the design of a stream cipher is the design of a cryptographically strong pseudorandom bit sequence generator (CSPBSG). Two main approaches to implement CSPBSG are (i) using cryptographic one-way function and (ii) using Linear Feedback Shift Register (LFSR) based structures.

LFSR based systems are less complex in hardware compared to one-way function based structures. Even though one-way function based stream ciphers have increased hardware complexity compared to LFSR based structures, if the underlying one-way function is used for the implementation of some other cryptographic services such as authentication or key exchange, then the redundant hardware in the system can be reduced.The operations of key exchange, encryption and authentication are done sequentially. Thus an encryption system built using infrastructure available for key exchange or authentication is highly acceptable. This approach will reduce the overall hardware complexity of the cryptosystem.

III. Key Exchange And Hash Generation

Two kinds of cryptosystems that implement cryptographic algorithms are private key cryptosystem and public key cryptosystem. In a private key cryptosystem both communicating entities share a secret key through a secure and authenticated channel. This secret key is used for both encryption and decryption of data. Private Key cryptography is used for the encryption of data due to its speed and reduced complexity of operations. However, it has certain shortcomings that make it unsuitable for use in today's environment[11].

*Key Management Problem :*In a broadcast communication scenario, each user will have to communicate with many different ones. Thus, communication on a public network is not restricted to one-on-one. For a network of *n* users, *n*(*n*-1)/2 private keys need to be generated.. Larger the value of n, the number of keys becomes unmanageable.
*Key Distribution Problem :*With such a large number of keys that need to be generated on a network, the job of generating the keys and finding a secure channel to distribute them becomes a burden.

*No digital signatures possible :*A digital signature is an electronic analogue of a handwritten signature. If Alice sends an encrypted message to Bob, Bob should be able to verify that the received message is indeed from Alice. This can be done with Alice's signature; however, private key cryptography does not allow such a feature. In contrast, public key cryptography uses two keys. While keeping the private key secret for decryption ,each user on a network publishes a public encryption key that anyone can use to send them messages. On a network of *n* users, it only needs *n* public and *n* private keys. Furthermore, it allows the use of digital signatures, which ensures non-repudiation. However, public key cryptography does have its drawbacks.

In truth, public and private key cryptography work best together. Public key cryptography is ideal for key distribution and management, ensuring *data integrity*, providing *authentication* and *nonrepudiation*, while private key cryptography is ideal for ensuring *confidentiality*, such as encrypting data and communication channels. Thus in this hardware implementation public key cryptography is used for key exchange and private key cryptography is used for message encryption.[2].

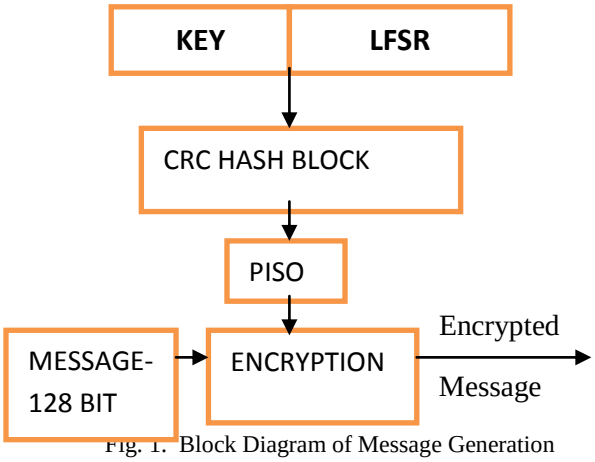

Fig. 1. Block Diagram of Message Generation

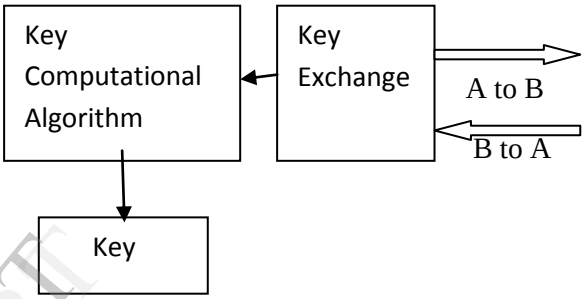

Fig.2. Block Diagram of Key Exchange

IV. Diffie-Hellman Key Exchange Algorithm

Two users can exchange a secret key without any prior secrets over an insecure medium using this protocol.

The Setup:

Suppose we have two people wishing to communicate: Alice and Bob. They do not want Eve (eavesdropper) to know their message. Alice and Bob agree upon and make public two numbers *g* and *p*, where *p* is a prime and *g* is a primitive root mod *p*.

The Exchange:

1. Alice chooses a random number *a* andcomputes $u = g^a \pmod p$, and sends *u* to Bob.
2. Bob chooses a random number *b* and computes $v = g^b \pmod p$, and sends *v* to Alice.
3.Bob computes the key,
$k = u^b = (g^a)^b \pmod p$.
4. Alice computes the key,
$k = v^a = (g^b)^a \pmod p$.
Now, both Alice and Bob have the same key,
namely$k = g^{ab} \pmod p$.

If Eve wants to compute *k*, then she would need either *a* or *b*.

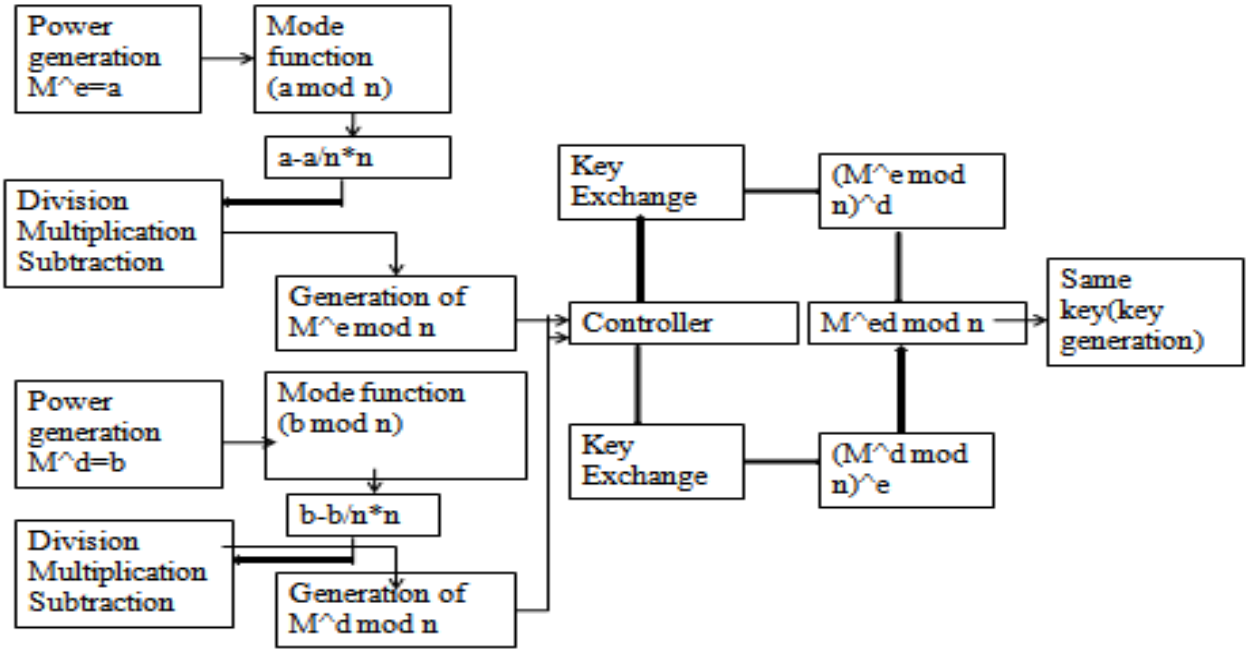

Fig.3. Structural Block Diagram of Hardware implemented

V. Simulation Result

Diffie hellman key exchange algorithm is synthesized in Xilinx. Division, subtraction and multiplication operation is used for synthesizing mode function and generated the key which is highly secure.

VI. Conclusion

Designed and implemented Secure Stream Cipher Key Exchange in FPGA. The proposed system is a modification of the hash block in which it introduces a key exchange block similar to the Diffie Hellman key exchange system to exchange the value in the Key, between the sender and the receiver. The proposed design is highly relevant in the implementation of secure communication system of low hardware complexity suitable for hand-held devices.

References

1. XunYi,San Ling and Huaxiong Wang, "*Efficient two- server password-only authenticated key exchange*",IEEE Transactions on Parallel and Distributed system,Vol.24,No.9,Sept 2013.
2. K S Lalmohan , Deepthi P P ,Sathidevi P S "*Design and Implementation of Secure Stream Cipher based on Elliptic Curves on Time Shared Basis* ", International Journal of Computer Applications (0975 – 8887) Volume 68– No.21, April 2013.
3. LalmohanK,Sreekumari, Deepthi P. Pattathil, JilnaPayingat, "*Hardware efficient implementation of encryption and key exchange based on elliptic curves*", Proceedings of the IASTED International Conference ,Signal and Image Processing and Applications (SIPA 2011),June 22 - 24, 2011 Crete, Greece
4. K.S.Lalmohan, Deepthi, Jithendra.K.B, "*FPGA implementation of secure time shared hash stream cipher*", 2011 International Conference on Computational Intelligence and Communication Systems.
5. D.B.Rane,SwetalR.Gund ,"*Hardware implementation of RC4 Stream Cipher using VLSI*," international journal of computer technology and electronics engineering, march-april 2013.
6. ShuklaAtuliika,Prof.SharmaSumit and Prof.Ravi Mohan "*Hardware Implementation of Advanced Cryptographic Hash function on FPGAs*",International Journal of Engineering and Computer Science,Vol.2,Jan 2013.
7. MoustafaM.Fouda,Zubair Md. Fadlullah,NeiKato,Rongxing Lu and XueminShen, "*A Lightweight Message Authentication Scheme for Smart Grid Communication*",IEEE Transactions on Smart Grid,Vol.2,No.4,Dec 2011.
8. IEEE 1363, *Standard Specifications for Publickey Cryptography*, 2000.
9. Deepthi.P.P, Sathidevi.P.S. *Design, implementation and analysis of hardware efficient stream ciphers using LFSR based hash functions*. Elsevier Computers and security.28, 229-241(2009).
10. PanagiotisRizomiliotis: *Misusing universal hash functions: security analysis of a hardware efficient stream cipher model using LFSR based hash function*, Information Theory Workshop(ITW), 2010 IEEE
11. Angelo P. E. Rosiello, "*Design of a Synchronous Stream Cipher from Hash Functions*", International Journal of Computer Science and Network Security, Vol.7 No.8, August 2007.
12. Yong Zhang, Xiamuniu, Juncao Li, Chunming Li, "*Research on a Novel Hashing Stream Cipher*", International Conference on Computational Intelligence and Security, 3-6 Nov 2006, Guangzhou, Vol. 2, 3-6, pp. 1339 – 1344, Nov 2006.