



FPGA IMPLEMENTATION OF HYBRID CRYPTOGRAPHY ENGINE FOR COMMUNICATION SYSTEMS

Shambhulingaiah C. M¹, Ravi Simha B. N², Dr. M.Z.Kurian³

PG Student [VLSI & Embedded systems], Sri Siddhartha Institute Of Technology, Tumkur, Karnataka, India¹

Asst. Professor, Dept. of ECE Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India²

HOD, Dept. of ECE, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India³

ABSTRACT: Security becomes increasingly important for many applications, such as video surveillance, confidential transmission military and medical applications. Data hiding has been used for several years to transmit data without being intercepted by unwanted viewers. The core of the system is two widely used cryptographic algorithm core: Secure Hash Algorithm SHA-256 and Advanced Encryption Standard AES-128. The system design is with hardware's effectiveness in mind. This cryptographic engine was used as an integral part of security data storage system. Cryptography algorithm is implemented on Software using computer. It has been observed that the performance of the software is not up to the mark. Moreover Security flaws were identified in Secure Hash Algorithm SHA-1, namely that a mathematical weakness exist, that indicating a stronger hash function would be desirable. So SHA-256 is used to overcome this.

Keywords: - Cryptography, SHA 256, AES 128.

I. INTRODUCTION

The term Cryptography is usually referred as "the study of secret", nowadays it is most attached to the definition of encryption. The term encryption is a process of converting plain text "unhidden" to a cryptic text "hidden" to secure it for against data thieves. The term decryption is reverse process of encryption, where cryptic text needs to be decrypted on the other end to be understood. In cryptographic systems, the term *key* refers to a numerical value used by an algorithm to alter the information so, making that information more secure and visible only to those who have the corresponding key to recover that information. The cryptography can be divided in to mainly two types. 1. Public key cryptography 2. Secret key cryptography. The Secret key cryptography is also called as *symmetric key* cryptography. Here both the sender and the receiver must know the same secret code, called as key. Messages can be encrypted by the sender using the key and decrypted by the receiver using the same key code. The Public key cryptography also referred as *asymmetric key cryptography*, which uses a two keys or pair of keys for encryption and decryption process. With the public key cryptography, keys work in pairs of matched private and public keys.

The traditional methods of Cryptography engine involve usage of single Cryptography algorithm. This has lead to chances of data being leak to the intruder, which has created lot of mishaps. In order to avoid this, to increase the data security, the Cryptographic level or Encryption level has been increased to an extent where such mishaps are not possible. In *hybrid cryptosystem*, the asymmetric key is used to encrypt the secret key and the secret key is used to encrypt the actual message.



II. HARDWARE IMPLEMENTATION

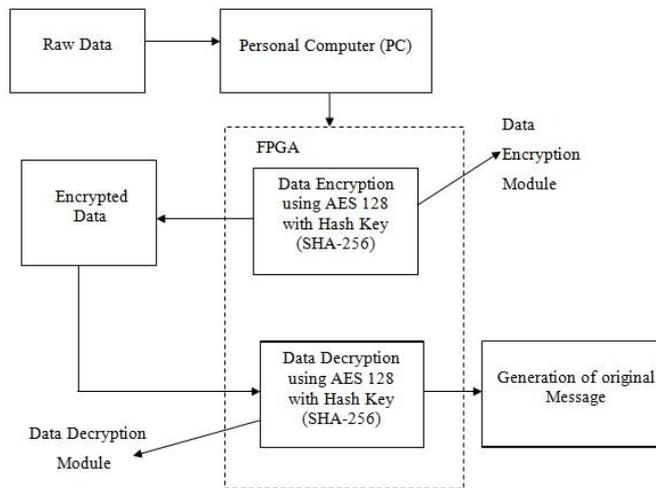


Fig. 1. Hybrid Cryptography Engine

Figure 1 shows the block diagram of Hybrid Cryptography Engine. The whole system is built up on a FPGA board and the core of the system is cryptographic cores implementing different cryptographic algorithm such as AES 128 and SHA 256. The cryptographic Engine is connected to computer through PCI port.

In Encryption process, plain text is converted in to cipher text, which is an output of AES Encryption. To encrypt the data, the key used is also encrypted by SHA-256 cryptographic algorithm. For SHA-256, a 32-bit key is given as an input. This SHA-256 algorithm gives the encrypted key. This key is used to encrypt the data in AES-128 algorithm. Finally, the output of AES algorithm produces the encrypted data of 128-bit.

During decryption process, the encrypted data is given to the data decryption module. The secret key is needed to decrypt the data which was used to encrypt the data. It is obtained by giving the public key to SHA 256, which gives the secret key. Now this secret key is used to decrypt the original data from the original data.

III. RESULT

The hybrid Cryptography Engine was implemented using Verilog hardware description language. These descriptions were then processed by standard Xilinx ISE 13.4 design tool suite, which performed synthesis, placement, and routing and bit stream (FPGA physical programming information) generation. The bit stream generated was dumped on to XC4VFX12 device of Xilinx Vertex 4 family. The number of slices used was 3791, number of slice flip flops used was 2384 and number of 4 input LUTs used was 7236, representing 69%, 21% and 66% of total resource available.

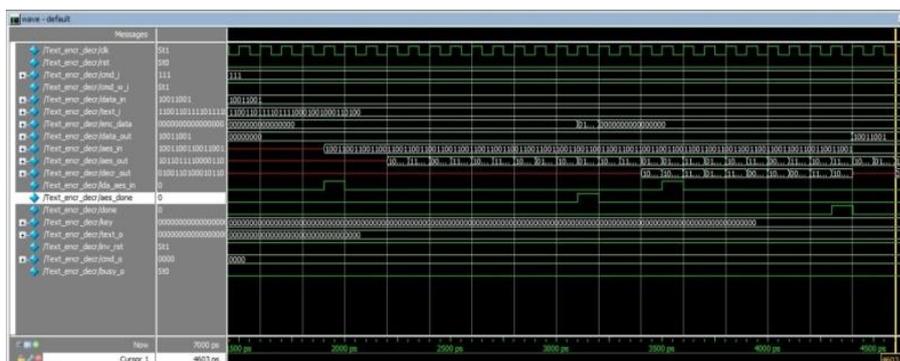


Fig. 2. Simulation Result



Figure 2 shows the simulation result of Hybrid Cryptography Engine. Here the data is of 128-bit and key is of 32-bit both of these are applied to the AES 128 algorithm. The 128-bit of encrypted data and decrypted data waveform has shown in above figure.

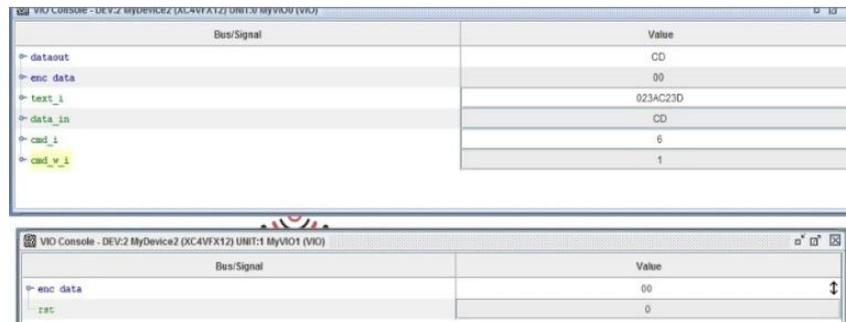


Fig. 3. FPGA Output

Figure 3 shows the FPGA output of implemented design. In the implementation as a reference, the data has been taken is of 8-bit of data instead of 128-bit and key size is same as of 32-bit. In the figure 3, Data_in is a input to the encryption and Data_out is a output from the decryption.

IV. CONCLUSION

In this paper, we implement a FPGA encrypt engine with SHA-256 and AES-128 IP cores. This hybrid cryptography engine uses SHA-256 algorithm to encrypt key and AES-128 algorithm is used to encrypt the data. This implementation shows that hardware implementation has better performance in terms of speed and power than software implementation. Also the use of SHA-256 Cryptographic algorithm for enhancing the Security has been proposed.

REFERENCES

- [1] Kaps, J. P. and Paar, C., "Fast DES implementation on FPGAs and its application to a universal key-search machine. In *Fifth Annual Workshop on Selected Area in Cryptography*, 1998.
- [2] Kaps, J. P., "High speed FPGA architectures for the data Encryption Standard", M.S. thesis, ECE department, Worcester Polytechnic Institute, Worcester, Massachusetts, USA. 1998.
- [3] Thomas Wollinger, Jorge Guajardo and Christof Paar, "Cryptography on FPGAs: State of the Art Implementations and Attacks." *ACM Special Issue Security and Embedded Systems* Vol. No. March 2003.
- [4] DATA ENCRYPTION STANDARD (DES), Federal Information Processing Standards Publication 46, 1999
- [5] Hui QIN, Tsutomu SASAO and Yukihiro IGUCHI, "A Design of AES Encryption Circuit with 128-bit Keys Using Look-Up Table Ring on FPGA", *IEICE TRANS. INF. & SYST.*, VOL.E89-D, NO.3 MARCH 2006.
- [6] Daemen, J., and Rijmen, R. *The Design of Rijndael: AES—The Advanced Encryption Standard*. New York: Springer-Verlag, 2002. New York: Springer, 2006.
- [7] LI Miao, XU Jinfu, YANG Xiaohui, YANG Zhifeng, "Design and Implementation of Reconfigurable Security Hash Algorithms based on FPGA", *IEEE Transaction on Information Engineering*, page no 381-384, 2009.
- [8] K. K. Ting, S. C. L. Yuen, K.-H. Lee and P. H. W. Leong. An FPGA based SHA-256 processor. In *FPL*, volume 2438 of *LNCS*, pages 577–585. Springer, 2002.
- [9] Robert P. McEvoy, Francis M. Crowe, Colin C. Murphy and William P. Marnane, "Optimisation of the SHA-2 Family of Hash Functions on FPGAs".
- [10] Chanjuan Li, Quingguo Zhou, Yuliliu, Qi Yao. "Cost efficient Data Cryptographic Engine Based on FPGA", *IEEE Transaction on Ubi-Media Computing*, page no 48-52, 2011.