IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 53-56
www.iosrjournals.org

Efficient Implementation of Hummingbird Cryptographic Algorithm

Mr. Shreyas D. Deshmukh [1], Ms. Priya More [2], Ms. Aditi Joshi [3],
Ms. Anushka Ayachit [4], Ms. Pooja Kawthekar [5]
[1] *(Asst. Professor, E&TC Department, RSCOE, Pune, India)*
[2,3,4,5] *(Student, E&TC Department, RSCOE, Pune, India)*

Abstract: *Hummingbird algorithm is a newly proposed lightweight cryptographic algorithm targeted for low-cost RFID low cost RFID tag. Hummingbird is a novel Ultra-light weight cryptographic encryption scheme used for RFID applications of privacy-preserving identification and mutual authentication protocols, motivated by the well known enigma machine. Hummingbird is expected to meet the stringent response time and power consumption requirements which can provide the designed security with a small block size. This algorithm shows resistant to the most common attacks like linear and differential cryptanalysis. In the proposed paper FPGA PROASIC3 has been used. FPGA is an Integrated Circuit designed to be configured by a customer or a designer after manufacturing. FPGA is used because it helps in power optimization which increases the efficiency and as it is programmable.*

Keywords*: FPGA (Field Programmable Gate Array), RFID (Radio Frequency Identification), LFSR (Linear Feedback Shift Register).*

I. Introduction

Low-cost smart devices like RFID tags and smart cards are used often in our daily life. Well known applications include electronic passports, contactless payments, product tracking, access control etc. But the small programmable chips that passively respond to every reader have raised concerns among researchers about privacy and security breaches. Cryptography is the art or science of hiding the information content using a key. Recently, a novel ultra-lightweight cryptographic algorithm, referred to as Hummingbird, is proposed for resource-constrained devices [2]. Light weight cryptography is a branch of modern cryptography, which covers cryptographic algorithms intended for use in devices with low or extremely low resources.

II. Hummingbird Cryptographic Algorithm

The design of the Hummingbird Cryptographic Algorithm is motivated by the well-known Enigma machine taking into account both security and efficiency. Hummingbird has a hybrid structure of block cipher and stream cipher and it has been shown to be resistant to the most common attacks to block ciphers and stream ciphers. Hummingbird can be used in high security required devices as it is resistant to most cryptographic attacks. The co-processor approach to FPGA implementation of the Hummingbird Cryptographic Algorithm is introduced. FPGAs are programmable logic devices which have proven to be highly feasible implementation platforms for cryptographic algorithm [2]. Simulation results show this design consumes less power than other symmetric cryptography algorithms and the area is small. As well as according to the research conducted FPGA is most compatible for the implementation of the Hummingbird Algorithm.

2.1 Plain text: Plain text is any text like numbers, alphabets which is the intended communication information or message referred to as plaintext is encrypted using encryption algorithm. The plain text is of 16 bits.

2.2 Encryption: Encryption is the most effective way to achieve data security. Encryption is a process of encoding message or information in such a way that only authorized parties can read it. Encryption is also used to protect data in transit for example data being transferred through networks (e.g. the internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices. Encryption scrambles the data which enhances the security of message.

2.3 Key: An encryption scheme usually uses a pseudo random encryption scheme generated by an algorithm. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not

to unauthorized interceptors. Without the key the algorithm would produce no useful results. Key is of 256 bits with four groups of 64bits each.

2.4 Cipher text: Cipher text is the result of encryption performed on plain text using an algorithm called as cipher. Cipher text contains a form of original plain text that is unreadable by a human or computer without the proper cipher to decrypt it.

2.5 Decryption: Decryption is the process of converting encrypted data back into its original form so that it can be understood. The authorized recipient should have the key to access the encrypted data and decrypt it. The cipher text produced in encryption is converted back to plain text by the decryption process.

III. Initialization

When using Hummingbird in practice, 4 16-bit random nonces(NONCEi) are first chosen to initialize the 4 internal state registers RSi(i=1,2,3,4) followed by 4 consecutive encryptions on the message RS1-RS4 by Hummingbird running in initialization mode.The final 16 bit cipher text TV is used to initialize the Linear Feedback Shift Register (LFSR). Moreover, the 13th bit of LFSR is always set to prevent a zero register. The LFSR is also stepped once before it is used to update the internal state register RS3.

IV. Encryption Process

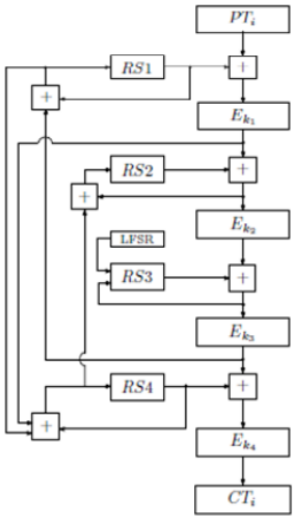

Fig. 1 Encryption Process Algorithm

After the system initialization process, a 16-bit plaintext block PTi is encrypted by first executing a modulo 216 addition of PTi [1] and the content of the first internal state register RS1. The result of the addition is then encrypted by the first block cipher Ek1. This procedure is repeated in corresponding manner and the output of Ek4 is the corresponding ciphertext PTi. The state of the four internal state registers will also be updated in an unpredictable way based on their current states, outputs of the three block ciphers and the status of LFSR [3] .

V. Decryption Process

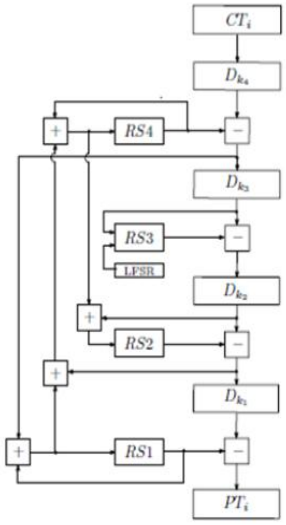

Fig. 2 Decryption Process Algorithm

The decryption process follows the same pattern that of encryption except that the ciphertext is given as input and we get plaintext as output, by performing the modulo 216 operation of the block cipher with the internal states RS1, RS2,RS3 and RS4.

VI. Results

The Hummingbird algorithm is implemented on the ProASIC 3 FPGA by means of VHDL language. The hardware performance of the Hummingbird cryptographic algorithm is studied where the lightweight architecture is based on loop unrolling of the inner 16-bit block ciphers. That implementation realizes all operations of the block cipher in one cycle consuming resources notably.

Table 1. Device Utilization Summery

Logic Utilization	Used	Available	Utilization
Number of slice register	4242	12480	33%
Number of slice LUT's	3504	12480	28%
number of bonded IOB's	278	172	161%
Number of fully used LUT-FF pair	1907	5839	32%
Number of BUFG/ BUFCTRLS	8	32	25%

VII. Conclusion

This work presents the smallest and the most efficient FPGA implementation of the ultra-lightweight cryptographic algorithm Hummingbird, to the coprocessor approach. The coprocessor approach is enabled due to the fact that FPGAs have dedicated memory blocks. The algorithm is serialized so that each step performs just one operation on the data. The datapath of the Hummingbird coprocessor is implemented in four stages and the instruction count is reduced via pipelining technique. With the hardware implementation improvement provided by this work, the Hummingbird will continue to be a favorite among the lightweight cryptographic algorithms for resource constrained devices like RFID tags and smart cards.

Reference

[1]. "Low Power Implementation of Hummingbird Cryptographic Algorithm for RFID tag", Meng-Qin Xiao, Xiang Shen, Yu-Qing Yang, Jun-Yu Wang.
[2]. "Lightweight Implementation of Hummingbird Cryptographic Algorithm on 4-bit Microcontrollers", Xinxin Fan, Honggang Hu.

[3]. "Implementation of Hummingbird Cryptographic Algorithm For Low Cost RFID Tags", Suresh N., Arun Prasad.
[4]. "Enhanced FPGA Implementation of the Hummingbird Cryptographic Algorithm", Ismail San and Nuray At.
[5]. "FPGA Implementation of Low Power and High Speed Hummingbird Cryptographic Algorithm", Nikita Arora, Yogita Gigras.