Design and Implementation of the High-End SAFER + Encryption Algorithm

V.Jeevan kanth
M.Tech. Student

P.Bujji babu
Assistant Professor

Abstract

In this paper, a VLSI design and implementation for the high-end SAFER+ encryption algorithm is presented. The combination of security, and high speed implementation, makes SAFER+ a very good choice for wireless systems. The SAFER+ algorithm is a basic component in the authentication Bluetooth mechanism. The relation between the algorithm properties and the VLSI architecture are described. Performance of the algorithm is evaluated based on the data throughput, frequency and security level. The results show that the modified SAFER plus algorithm has enhanced security compared to the existing algorithms.

Key words: Secure And Fast Encryption Routine, Pseudo Hadamard Transform, Encryption and description, Bluetooth.

1. Introduction

Wireless communication technology has advanced at a very fast pace during the last years, creating new applications and opportunities. In addition, the number of computing and telecommunications devices is increasing. Special attention has to be given in order to connect efficiently these devices. In the past, cable and infrared light connectivity methods were used. The cable solution is complicated since it requires special connectors, cables and space. This produces a lot of malfunctions and connectivity problems. The infrared solution requires line of sight. In order to solve these problems a new technology, named Bluetooth, has been developed. With this communication system, users are able to connect a wide range of computing and telecommunication devices easily and simply with out need for connecting cables. Unlike wireless LANs such as 802.11b, it was designed to be low power, operate over a short range, and support both data and voice services. It enables peer-to-peer communications among many types of handheld and mobile devices. Furthermore, it provides a conceptually simple communication model and lets these devices exchange information and work together to benefit the user.

2. Bluetooth Technology

Bluetooth is a technology for short range wireless data and real time two-way voice transfer providing data rates up to 3 Mb/s. It operates at 2.4 GHz frequency in the free ISM-band (Industrial, Scientific, and Medical) using frequency hopping Bluetooth can be used to connect almost any kind of device to another device. Typical range of Bluetooth communication varies from 10 to 100 meters indoors. Bluetooth technology and associated devices are susceptible to general wireless networking threats, such as denial of service attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation. They are also threatened by more specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Attacks against improperly secured Bluetooth implementations can provide attackers with unauthorized access to sensitive information and unauthorized usage of Bluetooth devices and other systems or networks to which the devices are connected.

There are several security algorithms available to ensure the security in wireless network devices. Some of the major methods are AES, DES, Triple DES, IDEA, BLOWFISH, SAFER+,ECDH etc. The SAFER+ algorithm is based on the existing SAFER family of ciphers. Although SAFER+ is the most widely used algorithm, it seems to have some vulnerabilities. This proves that proposed SAFER+ algorithm has better data throughput and frequency than the existing algorithms.

3. Description of SAFER + Algorithm

The SAFER+ (Secure And Fast Encryption Routine) algorithm is based on the existing SAFER family of ciphers, which comprises the ciphers SAFER K-64, SAFER K-128, SAFER SK-128. They have been developed by James L. Massey at the ETH Zurich. SAFER+ (as is also the case with all prior ciphers in the SAFER family) is neither a Feistel cipher nor a substitution-permutation cipher. There is no fundamental reason to alternate between substitutions and permutations to create good confusion and diffusion. All algorithms are byte-oriented block encryption algorithms, which are characterized by the following two properties. First, they use a non-orthodox linear transformation, which, is called Pseudo-Hadamard-Transformation (PHT) for the desired diffusion, and second, they use additive constant factors (Bias vectors) in the scheduling for weak keys avoidance.

SAFER + is an ***iterated*** cipher in the sense that encryption is performed by applying the same transformation repeatedly for r rounds, then applying an output transformation; r =6 is recommended but larger values of r can be used if desired for even greater security. Each round uses two 16-byte (128-bit) sub keys determined by a key schedule from the secret 16-byte user-selected key. The output transformation uses another 16-byte sub key determined by the key schedule. One unusual feature of SAFER + is that, in contrast to most recently proposed iterated block ciphers, encryption and decryption are slightly different (i.e., they differ by more than just the reversal of the key schedule).

Cryptographic strength of SAFER+ on most effective general attacks against ciphers are Differential cryptanalysis and Linear Cryptanalysis.

4. Architecture of SAFER + Algorithm

The architecture for the implementation of the SAFER+ algorithm consists of the two main components as shown in the figure 4.1, the data encryption path and the key scheduling. The plain text passes through the r rounds of encryption where r is determined by the key length chosen for the encryption. In our implementation we are using key size is 128 bits, so the no of rounds becomes eight. Two 16-byte round sub keys are used within the each round of encryption. These round sub keys are determined from the user-selected key according to a key scheduling. Finally the last round sub key "2r+1" is to Mixed XOR/Byte –Addition with the r rounds of encryption. This addition constitutes the output transformation for safer+ encryption. The encrypted text is a cipher text.

The input for the decryption of the safer+ is the cipher text block of 16-bytes.The decryption begins with the input transformation that undoes the output transform in the encryption process. This block then process through the r rounds of decryption, round1 of which undoes the round of encryption, round r undoes the encryption of round1 of encryption to produce the original plaintext. The round sub keys used for decryption used same as encryption but applied in reverse order.

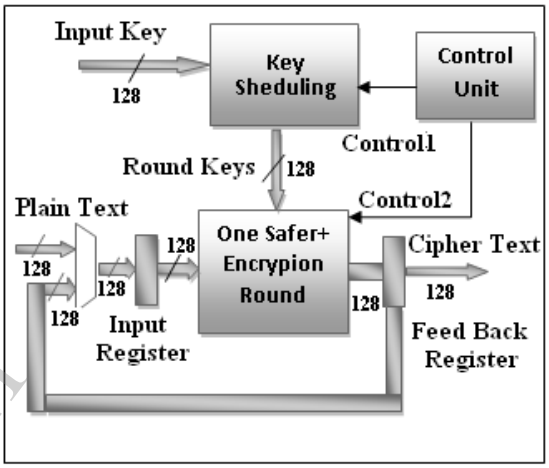

Fig 4.1. SAFER + Block Diagram Hardware Implementation

4.1. SAFER + Encryption Single Round

In this proposed design the whole single round of the SAFER+ algorithm is implemented. In order to run the whole SAFER+ algorithm eight loops of the single round implementation are needed .The single round implementation is chosen because the required system throughput can be achieved and in the same time the covered area is minimized. This block takes two 128 bit keys and 128-bit plain text as inputs and output will be 128-cipher.
A Safer+ single round has four subunits:

- The mixed XOR/addition subunit, which combines data with the appropriate round sub key *K*2*r*–1.

- The non-linear layer (use of the non-linear functions *e* and *l*). The *e* function is implemented as $y = 45^x$ in GF (257), except that 45128 = 0. The l function is implemented as $y = \log45(x)$ in GF (257), except that log45 (0) = 128.

• The mixed addition/XOR subunit, which combines data with the round sub key *K*2*r*

• The four linear Pseudo-Hadamard Transformation layers, connected through an "Armenian Shuffle"

The implementation of the non-linear layer using a *data-mapping* component that produces the X1 and X2 bytes is done. These bytes are the input of the non-linear functions *e* and *l*. During one round, we execute *e* and *l* eight times. This design significantly reduces the required silicon area. Each function is implemented using 256 bytes of ROM.

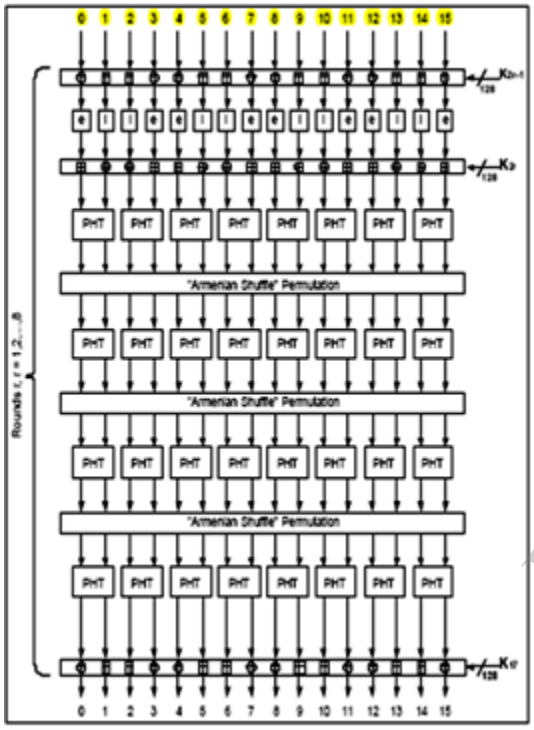

Fig 4.2. SAFER + Single Round

4.1.1 MODULAR ADDITION

Safer+ algorithm involves four layers of 8-bit modular additions. Modular adders and bitwise ex-or are interleaved alternatively in each of the four layers. This modular addition is performed over GF (256). Illustration of modular addition blocks interleaved with bit-wise ex-or blocks have been shown in figure 4.2.

4.1.2 BIT EX-OR

Bit-wise ex-or blocks are also used in the single round of safer+ algorithm in combination with modular addition blocks. This has been illustrated in figure 4.2.

4.1.3 Exponential and Logarithm in Nonlinear layer

Substitution box layer introduces non-linearity to the safer+ algorithm which is an essential feature in any of the security algorithms. Substitution box contains 'e' and 'l' non-linear functions and have been defined as follows.

Total eight 'e' and 'l' blocks are required for the algorithm. The choice of exptab (.) and logtab (.) as the mutually inverse nonlinear functions within the "nonlinear layer" of a round of SAFER+ was motivated by several factors. First of all, these are well-defined mathematical functions and their use obviates the suspicious of intentional weakness that might be raised if mutually inverse nonlinear functions defined only by "random looking' tables were chosen. The element 45 is a primitive element of this field, i.e., its first 256 powers generate all 256 non-zero field elements. The Data De-mapping unit performs the reverse function of the Data Mapping.

e is implemented as y1=45^x1 in GF(257)…...(1)

l is implemented as x1=log45(y1) in GF (257)…..(2)

With the exceptions that in e block implementation taking y1=0 when the x1=128 in eq(1).In l-block implementation taking x1=128 when the y1=0 in eq(2). Because the l and e block functions are reverse to each other. In the encryption one particular block is applied to the e block, the same block is applied to the l-block in the process of a decryption. In order to get the same plaintext.

4.1.4 Pseudo-Hadamard Transform (PHT)

PHT stands for Pseudo Hadamard Transform. If the two input bytes to a 2-PHT are (in1, in2), where in1 is the most significant byte, then the two output bytes are (out1, out2). The design of PHT element is shown in Fig.4.3. The PHT Implementation Multiplication by 2 can be achieved by one bit left wired shift.

PHT (in1, in2) = (2in1+ in2, in1+ in2).

The outputs of the PHT,

out1 = 2in1+ in2
out2 = in1+ in2

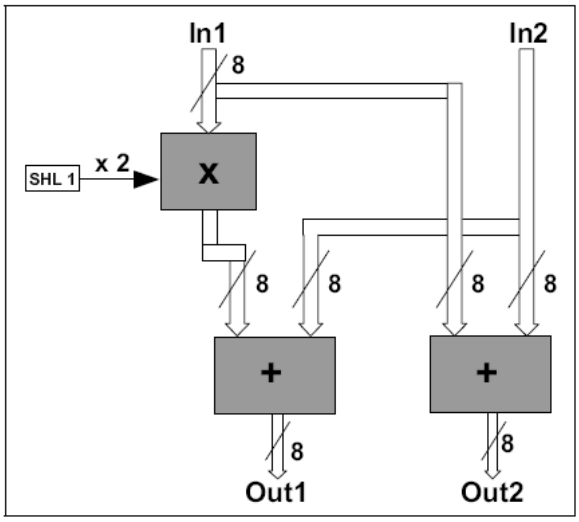

Fig 4.3 Design of Pseudo Hadamard Transform

The PHT boxes defined as

The four linear PHT layers connected through the permutations. The permutation boxes show how input byte indices are mapped into the output byte indices. Thus, position 0 (leftmost) is mapped on position 8; position 1 is mapped on position 11, etc.

5. Key Scheduling

The 2r+1 16-byte SAFER+ round sub keys required for the r rounds and for the output transformation of encryption (which are the same as those required for the input transformation and the r rounds of decryption) are produced from the input key according to a key. The key scheduling is shown in the figure 5.1

Calculation of biases for key schedules:

The key schedules of SAFER+ make use of 16-byte bias words to "randomize" the round sub keys produced .The required number of bias words is the same as the number 2r+1 of round sub keys, i.e., this number is 17,25 or 33 depending on whether the user-selected key length is 128 bits,192 bits or 256 bits respectively. The first bias word, however, is a "dummy" word that is never used but is convenient to have defined for programming purposes.

Let B_i denote the i-th bias word and let $B_{i,j}$ denote the j-th byte of this i-th bias word. For bias words B_2, B3…B_{17}, which are used in all the key schedules and are the only bias words needed for a 128-bit user-selected key, the bias bytes are computed in the following manner:

$$B_{i,\,j} = 45^{(45^{17i+j \bmod 257})} \bmod 257$$

where $B_{i,j}$ is represented as 0 in case this expression gives a value of 256 and) where this expression applies for i=2,3,…..17 and j=1,2,….16.The bias words B_{18},B_{19},…….B_{33}, of which only the first eight are needed for a 192-bit user –selected key but all sixteen of which are needed for a 256-bit user-selected key, are computed in the following manner.

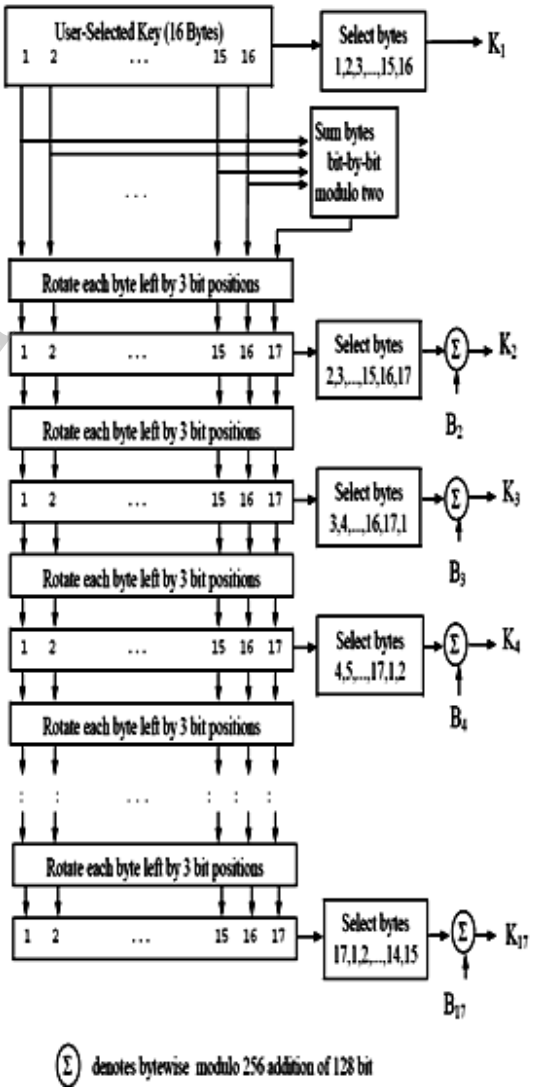

Figure 5.1. SAFER+ key schedule for 128 bit key

Conclusion

In this project, implementation of Safer+ algorithm (which is most important algorithm in Bluetooth security architecture) has been carried out successfully has been done. This project has helped me to become familiar with Verilog HDL, simulation tools, Modelsim and various synthesis tools. The whole design was captured entirely in the IEEE Verilog. VLSI implementation of the SAFER+ algorithm has been observed to work with a high throughput. The efficiency of the algorithm is evaluated by the analysis of parameters like encryption time, encryption frequency, and data throughput and security level. On comparison, the modified SAFER plus algorithm proved to be better for implementation in Bluetooth devices than the existing algorithms.

REFERENCES

[1] "*Specification of the Bluetooth System*", Specification Volume1, Version 1.1, February 22, 2001.

[2] J.L. Massey, G. H. Khachatrian, M. K. Kuregian, "Nomination of SAFER+ as Candidate Algorithm for the Advance Encryption Standard", *First Advanced Encryption Standard Candidate Conference*, Ventura, CA, August 20-22, 1998.

[3] J. L. Massey, "On the Optimality of SAFER+ Diffusion", *Second Advanced Encryption Standard Candidate Conference (AES2)*, Rome, Italy, March 22-23, on line available at http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm.

[4] J. L. Massey, "SAFER K-64: A Byte-Oriented Block Ciphering Algorithm", *Fast Software Encryption*, Proceedings of the Cambridge Security Workshop, Cambridge, U.K, 1998, pp. 1-17.

[5]Paraskevas Kitsos, Nicolas Sklavos, Kyriakos Papadomanolakis, and Odysseas Koufopavlou" Hardware Implementation of Bluetooth Security" *IEEE CS and IEEE Communications Society*, 2003

[6] P. Kitsos, N. Sklavos and O. Koufopavlou " HARDWARE IMPLEMENTATION OF THE SAFER+ ENCRYPTION ALGORITHM FOR THE BLUETOOTH SYSTEM" Proceedings of IEEE International Symposium on Circuits & Systems (ISCAS'02), Vol. IV, pp. 878-881, USA, May 26-29, 2002

[7] Xilinx, San Jose, California, USA, Virtex, 2.5 V Field Programmable Gate Arrays, 2001, www.xilinx.com

[8] D.Sharmila[1], R.Neelaveni[2]
"A Proposed SAFER Plus Security algorithm using Fast Walsh Hadamard transform for Bluetooth Technology" International Journal of Wireless & Mobile Networks (IJWMN), Vol 1, N0 2, November 2009