A Proposed SAFER Plus Security algorithm using Fast Walsh Hadamard transform for Bluetooth Technology

D.Sharmila[1], R.Neelaveni[2]

[1](Research Scholar),
Associate Professor,
Bannari Amman Institute of Technology, Sathyamangalam.
Tamil Nadu-638401.
sharmiramesh@rediffmail.com

[2] Asst.Prof. PSG College of Technology,
Coimbatore.Tamil Nadu -638401.
rnv@eee.psgtech.ac.in

ABSTRACT

In this paper, a modified SAFER plus algorithm is presented. Additionally, a comparison with various security algorithms like pipelined AES, Triple DES, Elliptic curve Diffie Hellman and the existing SAFER plus are done. Performance of the algorithms 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, Triple Data Encryption Standard, Pipelined Advanced Encryption Standard, Elliptic Curve Diffie Hellmann, Pseudo Hadamard Transform, Encryption and Decryption.*

1. Introduction

Bluetooth technology was developed to replace cumbersome wires in portable and personal electronic devices with radio frequency wireless communication. It has since found its way into numerous mobile applications as well as home and automobile use. Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth technology is used primarily to establish wireless personal area networks (WPAN), commonly referred to as ad hoc or peer-to-peer (P2P) networks. This allows users to form ad hoc networks between a wide variety of devices to transfer voice and data. There have been several versions of Bluetooth, with the most recent being 2.0 + Enhanced Data Rate (EDR) (November 2004) and 2.1 + EDR (July 2007). While 2.0 + EDR provided faster transmission speeds than previous versions (up to 3 Mbits/second), 2.1 + EDR provides a significant security improvement for link key generation and management in the form of Secure Simple Pairing (SSP). Bluetooth is a technology for short range wireless data and realtime 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 [18]. 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. [1]

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. The objective is to compare the various security algorithms like pipelined AES[14], triple DES [15][16], Elliptic Curve Diffie Hellman (ECDH), Existing SAFER+ and Proposed SAFER+ algorithm The Proposed SAFER+ algorithm has rotation block between every round of Existing SAFER+, PHT is replaced by Fast Psuedo Hadaamard transform (FPHT) and first round inputs are added or ored with the third round inputs and fifth round inputs are added or ored with the seventh round inputs. Thus the proposed SAFER+ has higher data throughput and frequency. This proves that proposed SAFER+ algorithm has better data throughput and frequency than the existing algorithms.

In this paper, section 2 describes the overview of Bluetooth technology and security. section 3 deals with the Existing SAFER+ algorithm. The Proposed SAFER+

algorithm is explained in section 4. A section 5 deal with the results, Section 6 refers the conclusion.

2. Bluetooth Security Architecture

Bluetooth architecture is described in Section 2.1. Section 2.2 explains the Bluetooth security. Bluetooth protocols are briefly described in Section 2.3

2.1 Bluetooth Architecture

Connection types define the possible ways Bluetooth devices can exchange data. Bluetooth has three connection types: ACL (Asynchronous Connection-Less), SCO (Synchronous Connection-Oriented) and eSCO. ACL links are for symmetric (maximum of 1306.9 kb/s for both directions) or asymmetric (maximum of 2178.1 kb/s for send and 177.1 kb/s for receive) data transfer. Retransmission of packets is used to ensure integrity of data. SCO links are symmetric (maximum of 64 kb/s for both directions) and they are used for transferring realtime two-way voice. Retransmission of voice packets is not used. Therefore, when the channel BER is high, voice can be distorted. eSCO links are also symmetric (maximum of 864 kb/s for both directions) and they are used for transferring realtime two-way voice. Retransmission of packets is used to ensure the integrity of data (voice). Because retransmission of packets is used, eSCO links can also carry data packets, but they are mainly used for realtime two-way voice. Only Bluetooth 1.2 or 2.0+EDR devices can use eSCO links, but SCO links must also be supported to provide backward-compatibility. Bluetooth devices that communicate with each other form a piconet. The device that initiates a connection is the piconet master. One piconet can have maximum of seven active slave devices and one master device. All communication within a piconet goes through the piconet master. The clock of the piconet master and frequency hopping information are used to synchronize the piconet slaves with the master. Two or more piconets together form a scatternet, which can be used to eliminate Bluetooth range restrictions. Scatternet environment requires that different piconets must have a common device, so-called scatternet member, to relay data between the piconets. [7] [8] [9].

The design goals for Bluetooth technology have been simplicity, compatibility, inexpensive and compact microchips, fast data transfer, globality, secure communication, and low power consumption. Simplicity means that a Bluetooth device must be as easy as possible to use for a user. Compatibility means manufacturer-independent interoperability between different Bluetooth devices, and it also means backward-compatibility with older Bluetooth versions. Bluetooth microchips are also very compact (roughly 5 mm × 5 mm of size) and cheap (roughly 2.50 dollars per microchip [Blu06d, Tan06]). The latest public version of Bluetooth specification, Bluetooth 2.0+EDR, supports data rates up to 3 Mb/s. The future version of Bluetooth specification (Seattle) is expected to provide data rates up to 480 Mb/s. Globality means that Bluetooth can be used all over the world using the same free ISM-band. Bluetooth has built-in security measures at the link level to provide the secure communication for the piconet. Bluetooth microchips have also low power consumption and therefore they are widely used in many different kinds of mobile devices. [17][19]

2.2 Bluetooth Security

This section provides Bluetooth specifications to illustrate their limitations and provide a foundation for some of the security recommendations A high-level example of the scope of the security for the Bluetooth radio path is depicted in Figure 2. In this example, Bluetooth security is provided only between the mobile phone and the laptop computer, while IEEE 802.11 security protects the wireless local area network link between the laptop and the IEEE 802.11 AP. However, the communications on the wired network are not protected by Bluetooth or IEEE 802.11 security capabilities. End-to-end security is not possible without using higher-layer security solutions in addition to the security features included in the Bluetooth specification and IEEE 802.11 standards. [2] The following are the three basic security services specified in the Bluetooth standard:

Authentication: verifying the identity of communicating devices. User authentication is not provided natively by Bluetooth.
Confidentiality: preventing information compromise caused by eavesdropping by ensuring that only authorized devices can access and view data.
Authorization: allowing the control of resources by ensuring that a device is authorized to use a service before permitting it to do so.
The three security services offered by Bluetooth and details about the modes of security are described below. Bluetooth does not address other security services such as audit and non-repudiation; if such services are needed, they must be provided through additional means.

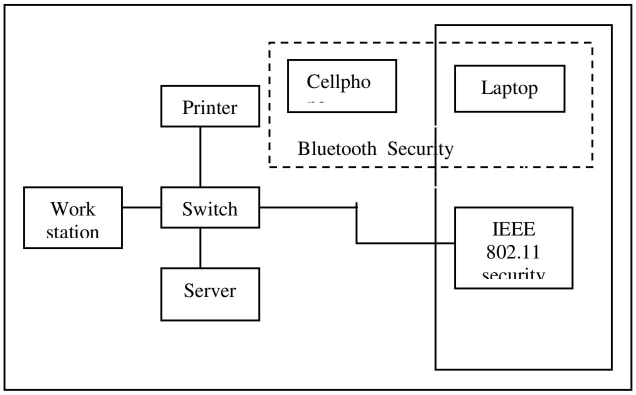


Figure1 Bluetooth Air-Interface Security

2.2.1 Authentication

The Bluetooth device authentication procedure is in the form of a challenge-response scheme. Each device interacting in an authentication procedure is referred to as either the claimant or the verifier.[3] The claimant is the device attempting to prove its identity, and the verifier is the device validating the identity of the claimant. The challenge-response protocol validates devices by verifying the knowledge of a secret key—the Bluetooth link key. The challenge-response verification scheme is depicted in Figure 2

The verifier transmits a 128-bit random challenge (AU_RAND) to the claimant. The claimant uses the E_1 algorithm to compute an authentication response using his unique 48-bit Bluetooth device address (BD_ADDR), the link key, and AU_RAND as inputs. The verifier performs the same computation. Only the 32 most significant bits of the E output are used for authentication purposes. The remaining 96 bits of the 128-bit output are known as the Authenticated Ciphering Offset (ACO) value, which will be used later to create the Bluetooth encryption key. The claimant returns the most significant 32 bits of the E_1 output as the computed response, SRES, to the verifier. The verifier compares the SRES from the claimant with the value that it computed. If the two 32-bit values are equal, the authentication is considered successful. If the two 32-bit values are not equal, the authentication has failed**.** Performing these steps once accomplishes one-way authentication. The Bluetooth standard allows both one-way and mutual authentication to be performed. For mutual authentication, the above process is repeated with the verifier and claimant switching roles. [20]

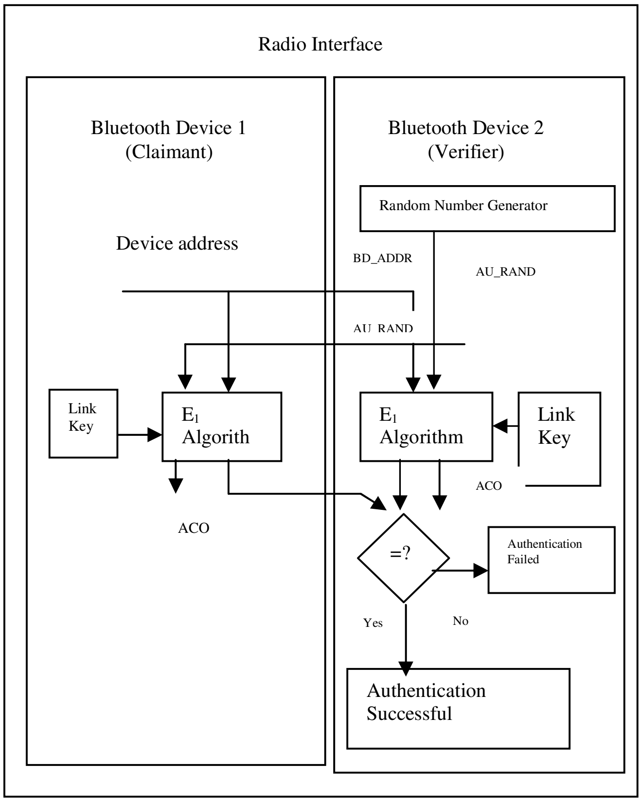


Figure 2 Bluetooth Authentication

2.2.2 Confidentiality

In addition to the Security Modes, Bluetooth provides a separate confidentiality service to thwart eavesdropping attempts on the payloads of the packets exchanged between Bluetooth devices. Bluetooth has three Encryption Modes, but only two of them actually provide confidentiality. The modes are as follows:

Encryption Mode 1—No encryption is performed on any traffic.

Encryption Mode 2—individually addressed traffic is encrypted using encryption keys based on individual link keys; broadcast traffic is not encrypted.

Encryption Mode 3—All traffic is encrypted using an encryption key based on the master link key. Encryption Modes 2 and 3 use the same encryption mechanism

2.3 Bluetooth protocols

Bluetooth protocol stack is illustrated in Figure 2. Protocols below HCI (Host Controller Interface) are built-in to the Bluetooth microchip and protocols above HCI are located as a part of the host device's software package. HCI is needed between the hardware and software protocols. The purpose of HCI is to enable manufacturer-independent combining of Bluetooth chips (Host Controller) and the actual host device. HCI takes care of security communication between the host and Bluetooth module. [3]

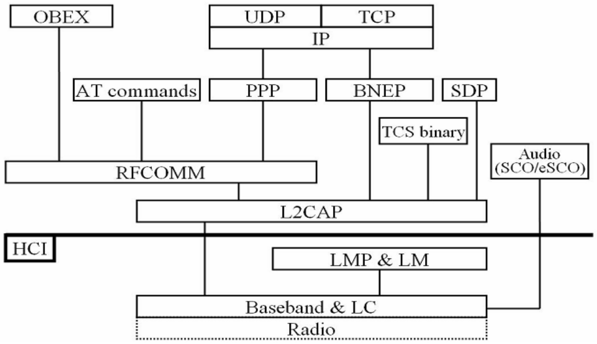


Figure 3. Bluetooth protocol stack

Baseband and LMP (Link Manager Protocol) together enable the physical RF connection. LC (Link Controller) is a state machine that defines the current state of Bluetooth device. Bluetooth device can be, for example, in low-power mode for saving batteries, in the connected state for normal piconet operation, or in the paging state for master to bring new slaves to the piconet. LC has pseudorandom number generation capability, the methods for managing security keys, and capability for providing the needed mathematical operations for authentication and encryption.

LM (Link Manager) acts as a liaison between the application and the LC on the local device, and it also communicates with the remote LM via PDUs (Protocol Data Units) using the LMP, i.e. the LM communicates with three different entities during a Bluetooth session: the local host through HCI, the local LC (local operations), and the remote LM (link configuration, link information, and link management operations). The PDU is acknowledged at the Baseband level, but it is acted upon by the LM. The local LM usually resides on the Bluetooth module as a complete host-module implementation. The remote LM can be defined as the LM at the other end of the Bluetooth link. LM has also several commands for handling security issues.

SCO and eSCO links are used for transferring realtime two-way voice (see Section 2.1). They are established directly from the Baseband level, so overhead of upper layer protocols is not causing any delays for realtime two-way voice connections.L2CAP (Logical Link Control and Adaptation Protocol) is a software module that normally resides on the host. It fits upper layer protocols to the Baseband, i.e. it acts as a conduit for data on the ACL link between Baseband and host applications. L2CAP also offers CO (Connection-Oriented; from master to one slave and from slave to master) and CL (Connection-Less; from master to multiple slaves) services, and it is defined only for ACL links. Lower layer protocols do not have to know how layers above L2CAP work and vice versa. L2CAP can initiate security procedures when a CO or a CL channel connection attempt is made.

SDP (Service Discovery Protocol) is used to find the services of Bluetooth devices in the range. RFCOMM (Radio Frequency Communication) emulates serial ports over L2CAP, and therefore it is possible to use existing serial port applications via Bluetooth. OBEX (Object Exchange Protocol) is used to exchange objects, such as calendar notes, business cards and data files, between devices by using the client-server model.

TCS (Telephony Control protocol Specification) binary defines the call control signalling for the establishment/release of speech and data calls between Bluetooth devices. It also provides functionality for exchanging signalling information that is unrelated to ongoing calls. Many AT commands are also supported for transmitting control signals for telephony control.[4]

BNEP (Bluetooth Network Encapsulation Protocol) is used to provide networking capabilities for Bluetooth devices. It allows that IP (Internet Protocol) packets can be carried in the payload of L2CAP packets. IP is a network layer protocol in the TCP/IP (Transmission Control Protocol / Internet Protocol) protocol suite. It contains both addressing information and some control information to enable routing of packets. TCP is one of the transport layer core protocols used in the TCP/IP protocol suite. It provides reliable transmission of data in IP network. UDP (User Datagram Protocol) is also one of the transport layer core protocols used in the TCP/IP protocol suite. It provides unreliable transmission of data in IP network, i.e. it does not provide reliability, flow-control, or error-recovery functions to IP. PPP (Point- to-Point Protocol) can also be used to provide TCP/IP networking capabilities for Bluetooth devices, but it is slower, i.e. it works over RFCOMM while BNEP works directly over L2CAP, and therefore it is rarely used anymore.

3. Description of SAFER Plus 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. 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. [5]

It consists of two main units: the encryption data path and the key-scheduling unit. The key-scheduling unit allows on-the-fly computation of the round keys. To reduce the silicon area, we used eight loops of a key scheduling single-round implementation. Round keys are applied in parallel in the encryption data path. The full Safer+ algorithm execution requires eight loops of the single round. We chose the single-round hardware implementation solution because, with this minimum silicon area, we could achieve the required throughput. The encryption data path's first component is an *input register*, which combines the *plaintext* and the *feedback data* produced in the previous round. The input register feeds the afer+ single round.

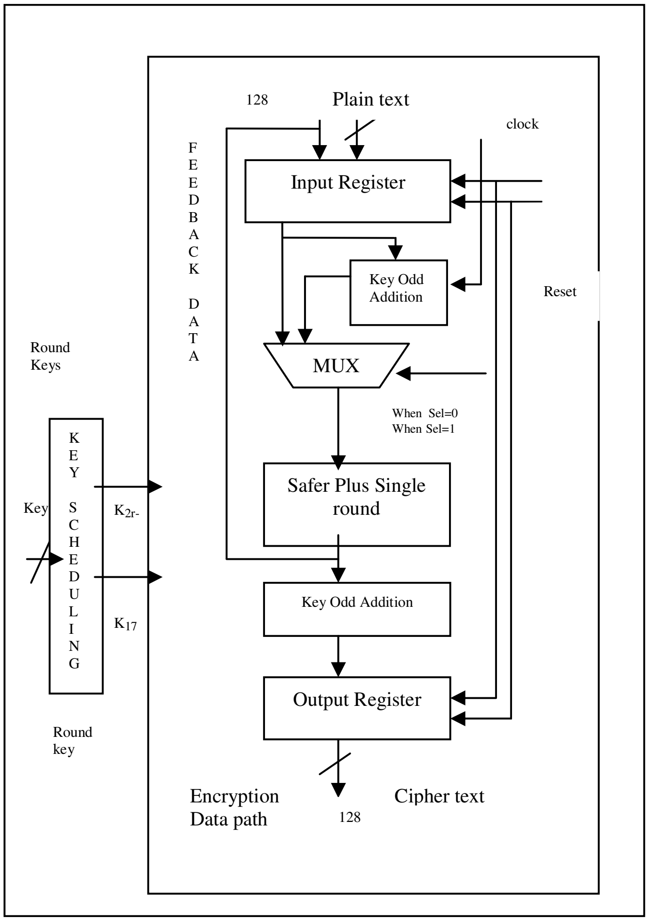
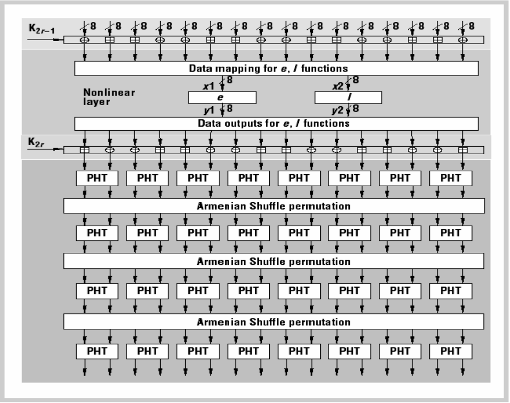


Figure.4 Safer + Implementation

3.1 SAFER + Single round

A Safer+ single round has four subunits:

- The mixed XOR/addition subunit, which combines data with the appropriate round sub key $K2r-1$.
- The non-linear layer (use of the non-linear functions *e* and *l*). The *e* function is implemented as $y = 45x$ 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 $K2r$
- The four linear Pseudo-Hadamard Transformation layers, connected through an “Armenian Shuffle” permutation.



K_{2r-1}
8
Data mapping for e, l functions
Nonlinear layer
x1
e
y1
x2
l
y2
Data outputs for e, l functions
K_{2r}
PHT
Armenian Shuffle permutation

Figure5. SAFER+ single round

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.

3.2 PHT Implementation

The design of PHT element is shown in Fig.6: The PHT Implementation Multiplication by 2 can be achieved by one bit left wired shift.

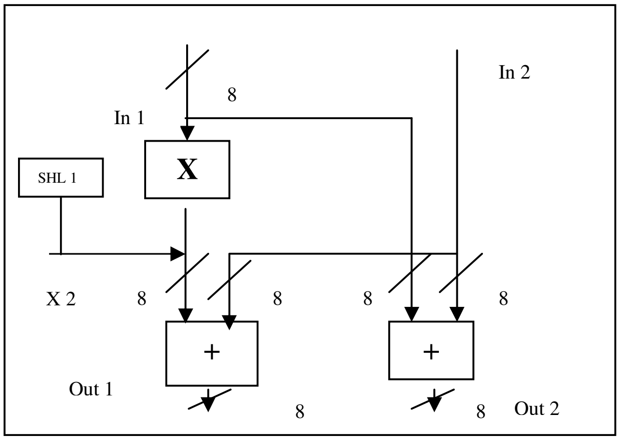


Figure 6 Psuedo Hadamard Transform

Out1=2 in1+in2 (1)

Out2=in1+in2 (2)

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.

4. Proposed SAFER Plus Algorithm

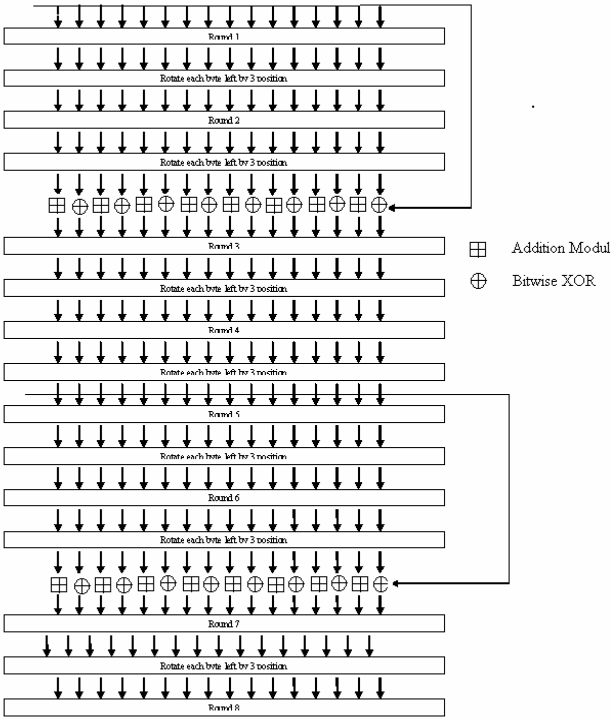
The Existing SAFER+ algorithm is modified to provide higher data throughput and frequency. The modified SAFER+ algorithm has three modifications when compared to the existing one.

(i) Rotation block is introduced between every round. Rotation is towards left for encryption and towards right for decryption

(ii) The input of round 1 and the output of round 2 are Xor/Add Modulo 16 byte-by-byte to form the input of round 3. Similarly the input of round 5 and the output of round 6 are Xor/Add Modulo 16 byte-by-byte to form the input of round 7.

(iii) Instead of PHT layer, Fast Walsh Hadamard Transform (FWHT) is used.

The Encryption and the Decryption block diagrams are given in the figure7 and figure 8.



Round 1
Rotate each byte left by 3 position
Round 2
Rotate each byte left by 3 position
Round 3
Rotate each byte left by 3 position
Round 4
Rotate each byte left by 3 position
Round 5
Rotate each byte left by 3 position
Round 6
Rotate each byte left by 3 position
Round 7
Rotate each byte left by 3 position
Round 8
⊞ Addition Modul
⊕ Bitwise XOR

Figure 8 Proposed SAFER+ for encryption

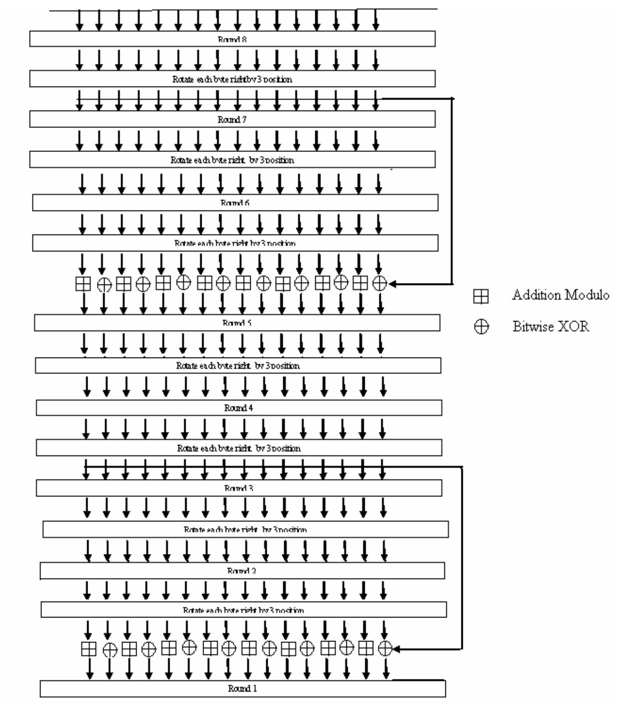

Round 8
Rotate each byte right by 3 position
Round 7
Rotate each byte right by 3 position
Round 6
Rotate each byte right by 3 position
Round 5
Rotate each byte right by 3 position
Round 4
Rotate each byte right by 3 position
Round 3
Rotate each byte right by 3 position
Round 2
Rotate each byte right by 3 position
Round 1
⊞ Addition Modulo
⊕ Bitwise XOR

Figure 9 Proposed SAFER+ for Decryption

The proposed work is to replace the Pseudo Hadamard Transform by Fast Walsh Hadamard transform.

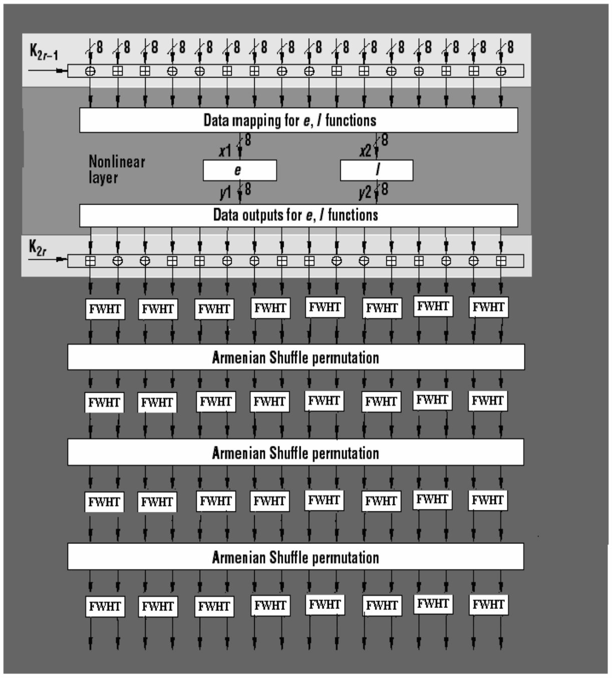

K_{2r-1}
8
Data mapping for e, l functions
Nonlinear layer
x1
x2
e
l
y1
y2
Data outputs for e, l functions
K_{2r}
FWHT
Armenian Shuffle permutation
FWHT
Armenian Shuffle permutation
FWHT
Armenian Shuffle permutation
FWHT

Figure 10 Proposed SAFER+ single round

Figure 10 shows the proposed SAFER+ single round architecture. In this, fast algorithms for Walsh Hadamard Transform on sliding windows are used to implement pattern matching most efficiently instead of PHT. The computational requirement of the proposed algorithm is about 1.5 additions per projection vector per sample which is the lowest among existing fast algorithms for Walsh Hadamard Transform on sliding windows.

4.1 Fast Algorithm for WHT

As any orthogonal (unitary) matrix can be used to define an orthogonal (unitary) transform, we define a Walsh-Hadamard transform of Hadamard order (WHT$_h$) as

$$\begin{cases} X = Hx \\ x = Hx \end{cases}$$

These are the forward and inverse transform pair.

$$x = [x[0], x[1], \ldots x[N-1]]^T$$

and

$X = [X[0], X[1], \ldots X[N-1]]^T$ are the signal and spectrum vectors, respectively. The K_{th} element of the transform can also be written as

$$X[k] = \sum_{m=0}^{N-1} h[k,m]x[m] = \sum_{m=0}^{N-1} x[m] \prod_{i=0}^{n-1} (-1)^{m_i k_i}$$

The complexity of WHT is O (N)$^{2.}$ Similar to FFT algorithm, Fast WHT algorithm with complexity of O (Nlog$_2$N) are derived assume n=3 and N=2^n =8 in the following derivation. An N=8 point WHTh of signal $x[m]$ is defined as

$$\begin{bmatrix} X[0] \\ \cdot \\ X[3] \\ X[4] \\ \cdot \\ X[7] \end{bmatrix} = \begin{bmatrix} \mathbf{H}_2 & \mathbf{H}_2 \\ \mathbf{H}_2 & -\mathbf{H}_2 \end{bmatrix} \begin{bmatrix} x[0] \\ \cdot \\ x[3] \\ x[4] \\ \cdot \\ x[7] \end{bmatrix}$$

This equation can be separated into two parts [13]. The first half of the X vector can be obtained as

$$\begin{bmatrix} X[0] \\ X[1] \\ X[2] \\ X[3] \end{bmatrix} = \mathbf{H}_2 \begin{bmatrix} x[0] \\ x[1] \\ x[2] \\ x[3] \end{bmatrix} + \mathbf{H}_2 \begin{bmatrix} x[4] \\ x[5] \\ x[6] \\ x[7] \end{bmatrix} = \mathbf{H}_2 \begin{bmatrix} x_1[0] \\ x_1[1] \\ x_1[2] \\ x_1[3] \end{bmatrix} \text{ -- (1)}$$

Where

$$x_1[i] \triangleq x[i] + x[i+4] \quad (i = 0, \cdots, 3) \qquad \text{-- (2)}$$

The second half of the X vector can be obtained as

$$\begin{bmatrix} X[4] \\ X[5] \\ X[6] \\ X[7] \end{bmatrix} = \mathbf{H}_2 \begin{bmatrix} x[0] \\ x[1] \\ x[2] \\ x[3] \end{bmatrix} - \mathbf{H}_2 \begin{bmatrix} x[4] \\ x[5] \\ x[6] \\ x[7] \end{bmatrix} = \mathbf{H}_2 \begin{bmatrix} x_1[4] \\ x_1[5] \\ x_1[6] \\ x_1[7] \end{bmatrix} \quad \text{-- (3)}$$

where

$$x_1[i] \overset{\triangle}{=} x[i] + x[i+4] \quad (i = 0, \cdots, 3) \quad \text{-- (4)}$$

Converting a WHT of size N=8 into two WHT of size N/2=4. Continuing this process recursively, we can rewrite Eq. (1) as the following (similar process for Eq. (3))

$$\begin{bmatrix} X[0] \\ X[1] \\ X[2] \\ X[3] \end{bmatrix} = \begin{bmatrix} \mathbf{H}_1 & \mathbf{H}_1 \\ \mathbf{H}_1 & -\mathbf{H}_1 \end{bmatrix} \begin{bmatrix} x_1[0] \\ x_1[1] \\ x_1[2] \\ x_1[3] \end{bmatrix}$$

$$\begin{bmatrix} X[0] \\ X[1] \end{bmatrix} = \mathbf{H}_1 \begin{bmatrix} x_1[0] \\ x_1[1] \end{bmatrix} + \mathbf{H}_1 \begin{bmatrix} x_1[2] \\ x_1[3] \end{bmatrix} = \mathbf{H}_1 \begin{bmatrix} x_2[0] \\ x_2[1] \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} x_2[0] \\ x_2[1] \end{bmatrix} = \begin{bmatrix} x_2[0] + x_2[1] \\ x_2[0] - x_2[1] \end{bmatrix} \quad \text{-- (5)}$$

where

$$x_2[i] \overset{\triangle}{=} x_1[i] + x_1[i+2] \quad (i = 0, 1) \quad \text{-- (6)}$$

The second half is

$$\begin{bmatrix} X[2] \\ X[3] \end{bmatrix} = \mathbf{H}_1 \begin{bmatrix} x_1[0] \\ x_1[1] \end{bmatrix} - \mathbf{H}_1 \begin{bmatrix} x_1[2] \\ x_1[3] \end{bmatrix} = \mathbf{H}_1 \begin{bmatrix} x_2[2] \\ x_2[3] \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} x_2[2] \\ x_2[3] \end{bmatrix} = \begin{bmatrix} x_2[2] + x_2[3] \\ x_2[2] - x_2[3] \end{bmatrix} \quad \text{-- (7)}$$

where

$$x_2[i+2] \overset{\triangle}{=} x_1[i] - x_1[i+2] \quad (i = 0, 1) \quad \text{-- (8)}$$

X (4) through X (7) of the second half can be obtained

$$X[0] = x_2[0] + x_2[1] \quad \text{-- (9)}$$

and

$$X[1] = x_2[0] - x_2[1] \quad \text{-- (10)}$$

Summarizing the above steps of Equations (2), (4), (6), (8), (9) and (10), we get the Fast WHT algorithm as illustrated below.

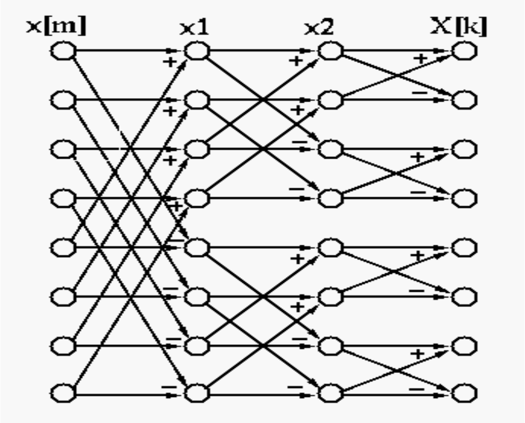


Figure 11 Fast WHT algorithm

5. Results

Various existing algorithms are analyzed and compared with the proposed algorithm based on the parameters such as encryption frequency, Data throughput and security level and the results are shown in the bar charts.

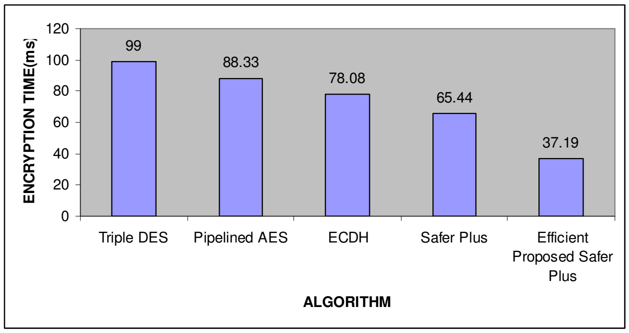


Figure 12 Encryption Time Vs Various Algorithms

Based on the analysis, the modified Safer Plus algorithm required minimum encryption time and maximum encryption frequency when compared to all the existing algorithms due to the inclusion of FWHT instead of PHT layer as shown in Figure 12 and Figure 13.

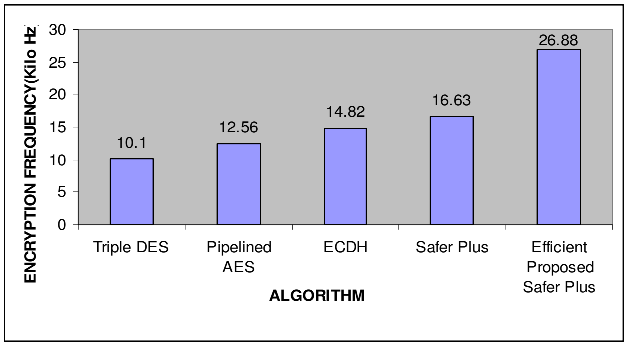


Figure 13 Encryption Frequency Vs Various Algorithms

The number of hits required to attack the various algorithms is also compared and shown in Figure14. The security level is much enhanced for the algorithm proposed since the number of hits is found to be maximum due to the introduction of the rotation block between every round.

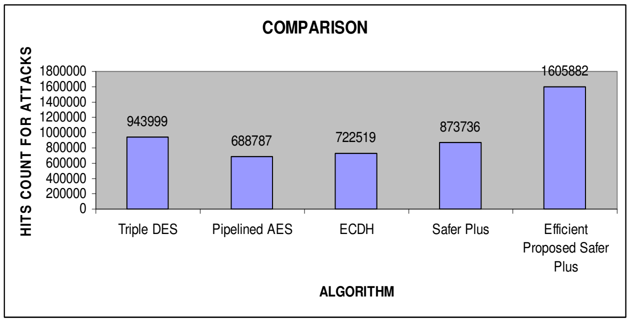


Figure 14 No. of Hit counts Vs Various algorithms

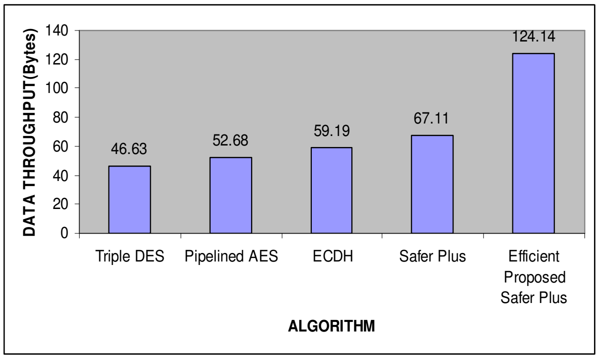


Figure 15 Data throughput Vs various algorithm

Figure 15 shows that modified Safer plus algorithm has higher data throughput comparatively because the input of round 1 and the output of round 2 are Xor/Add operation to form the input of round 3.

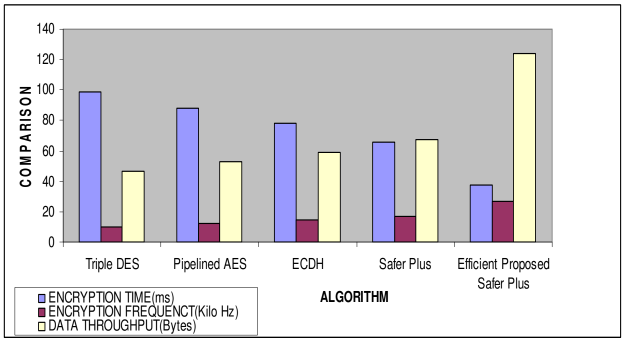


Figure 16 Encryption time, Encryption frequency and data throughput Vs various algorithms

Figure16 consolidates the performance of the proposed algorithm. It is observed that the modified Safer Plus is the best.

6. Conclusion

In this paper, a modified SAFER plus algorithm is proposed by replacing PH transform with FWH transform and introducing a rotation block for every round. The existing security algorithms are compared with the proposed Safer Plus algorithm. The entire design is captured in J2ME. 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.

7. References

[1] Paraskevas kitos, Nicolas sklavos, Kyriakos Papadomanolakis and Odysseas Koufopavlou university of patras, Greece," Hardware Implementation of Bluetooth Security" *IEEE CS and IEEE Communications Society* - January to March 2003. pp. 21 to 29.

[2] Karen Scarfone John Padgette, "Guide to Bluetooth security " National Institute of standards and technology Special Publication 800-121, U.S. Department of Commerce 43 pages.

[3] Vainio, Juha T. "Bluetooth Security," Helsinki University of Technology, 25 May 2000

[4] Gyongsu Lee, "Bluetooth Security Implementation based on Software Oriented Hardware-Software Partition" IEEE journal 2005. pp. 2070-2074.

[5] Kardach, James, "Bluetooth Architecture Overview," *Intel Technology Journal*, 2000

[6] Jyrki Oraskari, "Bluetooth versus wlan ieee 802.11x", Helsinki university of technology, october, 2001.

[7] A. Laurie and B.Laurie. serious flaws in blue tooth security lead to disclosure of personal data. http://bluestumbler.com.

[8] Brent A.Miller And Chatschik Bisdikian "Bluetooth revealed" – low price edition

[9] Wikipedia.org, "Bluetooth," Wikipedia.org, 5 March 2005, http://en.wikipedia.org/wiki/Bluetooth (21 February 2005)

[10] Vrije Universiteit Brussel, "Bluetooth security" phd thesis December 2004

[11] Keijo M.J. Haataja Licentiate Thesis January 2007 University of Kuopio

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

[13] Wanli Ouyang, W.K. Cham,"Fast Algorithm for Walsh Hadamard Transform on Sliding Windows" IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, MANUSCRIPT ID TPAMI-2008-06-0328

[14] NIST: Advanced Encryption Standard (AES) The Federal Information Processing Standards Publication 197. NIST, November 26, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (20.9.2006)

[15] NIST: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. NIST, May 2004. http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf (19.9.2006)

[16] NIST: Data Encryption Standard (DES) The Federal Information Processing Standards Publication 46-3. NIST, October 1999. http://www.cerberussystems. com/INFOSEC/stds/fip46-3.htm (19.9.2006)

[17]AlfonsoDeGregorio. Cryptographic Key ReliableLifetimes: Bounding the Risk of Key Exposure in the Presence of Faults. In Fault Diagnosis and Tolerance in Cryptography, volume 4236 of LNCS, pages 144–158. Springer, 2006.

[18] ARC Electronics (n.d.). DSSS and FHSS - Spread Spectrum modem. Retrieved March 24, 2004 from, Web site:http://www.arcelect.com/DSSS_FHSS-spead_spectrum.htm

D.Sharmila is presently working as Associate Professor, Department of ECE, Bannari Amman Institute of Technology, Sathyamangalam. She received B.E.(ECE) and M.E. (Applied Electronics) from Kongu Engineering College, Perundurai. She is now pursuing Phd in Wireless Security. She has 14 years of teaching experience and has guided several UG and PG projects. She is a life member of ISTE and Associate member of IE. Her area of interests are Wireless Security, Low power VLSI, Adhoc networks. She has published 4 International and National Journals and presented 20 research papers in International and National Conferences.

Dr.R. Neelaveni is presently working as Assistant Professor, Department of EEE, PSG College of Technology, Coimbatore. She has a Bachelor's degree in ECE, a Master's degree in Applied Electronics and PhD in Biomedical Instrumentation. She has 19 years of teaching experience and has guided many UG and PG projects. Her research and teaching interests includes Applied Electronics, Analog VLSI, Computer Networks, and Biomedical Engineering. She is a Life member of Indian Society for Technical Education (ISTE).She has published several research papers in national Journals and Conferences.