
Research Article

# FPGA Implementation of Hybrid Encryption Algorithm Based on Triple DES and RSA in Bluetooth Communication

*Authors*

[1] Veenanand Kakarla, [2] N.S.Govind

**Address for correspondence:**

[1, 2] E C E Department, ASR Institute of Engineering and Technology

**Abstract**

- In this paper, we propose the hybrid encryption algorithm based on Triple DES and RSA, to enhance the security of data transmission in wireless communication. The currently used encryption algorithm employed by the wireless devices to protect the confidentiality of data during transport between two or more devices may be broken under certain conditions. In the proposed hybrid encryption algorithm, Triple DES algorithm is used for data transmission because of its higher efficiency in block encryption, and RSA algorithm is used for the encryption of the key of the Triple DES because of its management advantages in key cipher. Under the dual protection with the Triple DES algorithm and the RSA algorithm, the data transmission will be more secure. Meanwhile, it is clear that the procedure of the entire encryption is still simple and efficient as ever.

**Key Words**:- Bluetooth,E0 key stream, Hybrid encryption algorithm, Data transmission

## 1 INTRODUCTION

Wireless communication is the transfer of information between two or more points that are not physically connected. Distances can be short, such as a few metres or as far as thousands of kilometres. Bluetooth technology is an emerging wireless networking standard, which is based on chip that provides short-range wireless frequency hopping communication. Now, Bluetooth technology is mainly applied to the communication between mobile terminal devices, such as palm computers, mobile phones, laptops and so on, and also can successfully simplify the communication among above devices and the Internet, so that the data transmission between these modern communication equipments and Internet has become more quickly and efficiently, and widen the road for wireless communications. It has the characteristic of wireless, openness, low-power and so on. However, the phenomenon of data-leaking frequently arise in using the Bluetooth technology for data transfer, since the emergence of Bluetooth, even if the Bluetooth takes the very robust security measures, there are still serious security risks. The encryption algorithm using in Bluetooth encryption process is the E0 stream cipher. However, this algorithm has some shortcomings, 128-bit E0 stream ciphers in some cases can be cracked by 0 ($2^{64}$) mode in some cases. So, for most applications that which need to give top priority to confidentiality, the data security is not enough if only use Bluetooth. Now I will introduce the Bluetooth mechanism, its disadvantages, and then propose a hybrid encryption algorithm to solve the current security risk in Bluetooth data transmission.

## 2 THE ENCRYPTION ALGORITHM IN BLUETOOTH SECURITY MECHANISM

### *A. Authentication and encryption process of Bluetooth*

Bluetooth security-mechanism is divided into three modules including key generation, authentication and encryption, and adopt four kinds of algorithms as E0 E1, E2, E3. Bluetooth system provides authentication, encryption and key management functions in Link layer. PIN code was entered by the

user, by means of the E2 algorithm for generating the link key, by means of E3 algorithm, getting encryption key, make use of E0 algorithm generated key stream, and encrypt plaintext, then get cipher text. Figure 1 is the process of Bluetooth encryption

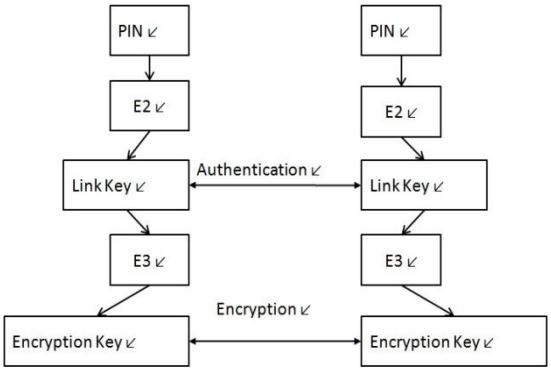


Figure 1

The three modules of Figure 1 are as follows: 1) key generation module, algorithm E2 is used for generating the link key, and its input parameter is a 4-digit passwords number which is entered by the user, the algorithm E3 calculates encryption key KC by the use of E2 link key encryption key as input parameters. 2) Encryption module, algorithm E0 can be used for generating keys stream to encrypt the original data. 3) Authentication module, algorithm E1 is the crucial algorithms in the authentication process, the two units in need of certification use each authentication algorithm E1 to generate identification word and compare, then complete certification.

### *B. Analysis of E0 Algorithms*

E0 algorithm is the encryption algorithms in Bluetooth link layer, which belongs to stream encryption method, that is to say it take data flow and the key bit stream Exclusive-or operation. The payload of each packet is encrypted separately, and the encryption occurs before MPE-FEC, after the cyclic redundancy check. The main principle is to use linear feedback shift register to generate pseudo-random sequence, after that form key stream that can be used for encryption, and then take the key stream and data stream that need encryption Exclusive-or operation, and achieve encryption. During decryption, the cipher text take Exclusive-or operation once more, re-plaintext can be obtained.

## 3 HIDDEN DANGER OF BLUETOOTH SECURITY SYSTEM

*A. The weakness of E0 stream cipher algorithm*

*B. Limited resources capacity of linear feedback shift register LFSR*

C. *Low credibility of PIN*

*D. High probability of non-link key cheat*

D. *Address Spoofing*

## 4 THE IDEAS AND PROCESSES OF HYBRID ENCRYPTION ALGORITHM

RSA algorithm is the first relatively complete public key algorithm. It can be used for data encryption, also can be used for digital signature algorithms. RSA cryptosystem is based on the difficulty of integer factorization in the group Zn, and its security establishes in the assumption that constructed by almost all

the important mathematicians, it is still a theorem that does not permit, which is lack of proof, but Mathematicians believe it is existent.

Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Triple DES uses a "key bundle" which comprises three DES keys, K1, K2 and K3, each of 56 bits (excluding parity bits). The encryption algorithm is:

ciphertext = EK3(DK2(EK1(plaintext)))

i.e., DES encrypts with K1, DES decrypt with K2, then DES encrypt with K3.

Decryption is the reverse:

plaintext = DK1(EK2(DK3(ciphertext)))

i.e., decrypt with K3, encrypt with K2, then decrypt with K1.Each triple encryption encrypts one block of 64 bits of data.In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm.

Seeing from the efficiency of encryption and decryption, Triple DES algorithm is better than the RSA algorithm. The speeds of Triple DES encryption is up to several M per second, it is suitable for encrypting large number of message; RSA algorithm is based on the difficulty of factoring, and its computing velocity is slower than Triple DES, and it is only suitable for encrypting a small amount of data, The RSA encryption algorithm used in the .NET, it encrypts data at most 117 bytes of once. Seeing from key management, RSA algorithm is more superior than the Triple DES algorithm. Because the RSA algorithm can distribute encryption key openly, it is also very easy to update the encryption keys, and for the different communication objects, just keep the decryption keys secret; Triple DES algorithm requires to distribute a secret key before communication, replacement of key is more difficulty, different communication objects, Triple DES need to generate and keep a different key. Based on the comparison of above Triple DES algorithm and RSA algorithms, in order to give expression to the advantages of the two algorithms, and avoid their shortcomings at the same time, we can conceive a new encryption algorithm, that is, Triple DES and RSA hybrid encryption algorithm. We will apply hybrid encryption algorithm to Bluetooth technology, we can solve the current security risks of Bluetooth technology effectively. The entire hybrid encryption process is as follows: Let the sender is A, the receiver is B, B's public key is eB, B's private key is dB, $K_2$ is Triple DES encryption session key (assuming that the two sides of communication know each RSA public key).

### *A. Process of encryption*

During the process of sending encrypted information, Triple DES, requires 168-bit key and encrypts each block three times. That is, each block of data is actually encrypted 48 times, it encrypt the plaintext to produce cipher text. On the other hand, the sender get debit’s public key from public key management center, and then using RSA to encrypt session key. Finally, the combination of the session key from RSA encryption and the cipher text from Triple DES encryption are sent out.

Triple DES encryption scheme is that encrypt the plaintext with K1, decrypt with K2, then encrypt with K3.

The second, RSA algorithm encrypts one of the three keys, i.e., Either $K_1$, $K_2$, $K_3$ of Triple DES algorithm.Let us consider key2 ($K_2$). Figure 2 is the whole mixed-encryption.

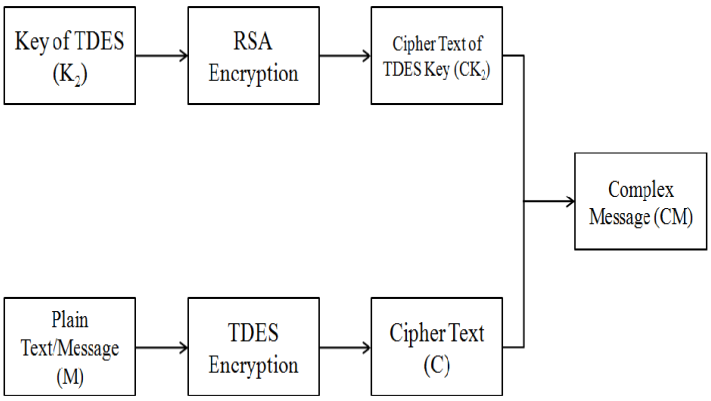


Figure 2. The whole mixed-encryption process.

B. *Process of decryption*

The decryption of hybrid encryption algorithm is as follows. The first, the receiver divide received cipher text CM into two parts, one is cipher text $CK_2$ from the RSA algorithm encryption, the other is cipher text C from the Triple DES algorithm encryption. The second, the receiver decrypt cipher text $CK_2$ by their own private key dB, receive the key $K_2$ which belongs TDES algorithm, then decrypt the cipher text C to the original M by keys $K_1$,$K_2$,$K_3$. Figure 3 is a decryption of hybrid encryption algorithm.

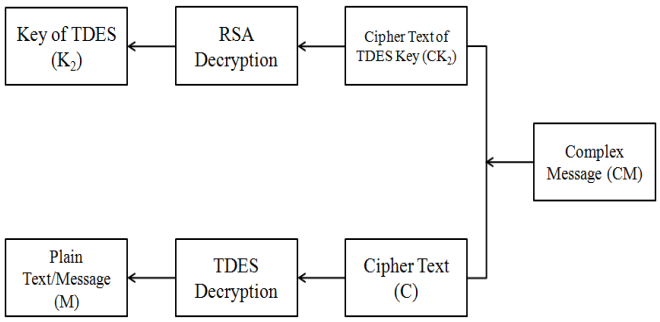


Figure 3. A decryption of hybrid encryption algorithm.

*C. The advantages of hybrid encryption algorithm*

• Using RSA algorithm and the TDES key for data transmission, so it is no need to transfer DES key secretly before communication;

• Management of RSA key is the same as RSA situation, only keep one decryption key secret;

• Using RSA to send keys, so it can also use for digital signature;

• The speed of encryption and decryption is the same as TDES. In other words, the time-consuming RSA just do with TDES keys;

D. *Safety analysis of hybrid encryption algorithm*

Safety of Hybrid encryption algorithm is based on the safety of RSA algorithm and Triple DES algorithm, operating efficiency of hybrid encryption algorithm depends on the speed and high efficiency of encryption and decryption by Triple DES algorithm. Of course, the Bluetooth based on hybrid

encryption algorithm, its data transmission security depend on the security of hybrid encryption algorithm. As long as we protect the key that encrypt original, and the security of entire file will be guaranteed. Because of the dual protection of Triple DES algorithm and RSA algorithm, the data in transit is safe.

## 5 CONCLUSIONS

Bluetooth technology is a new technology, which will change our transmission method. However, the Bluetooth technology has not fully considerate security issues in the standardization process. As communication networks, it uses wireless channel for the transmission medium. Compared to the fixed network Bluetooth network is more vulnerable to be attacked. For the applications that take data security as priority, achieving a high level of data security is essential. Currently, stream cipher E0 used in Bluetooth standard has many shortcomings, while the Triple DES and RSA hybrid encryption algorithm is relatively more secure and easier to achieve, thus ensures data transmission between the Bluetooth device safety and real-time.

## REFERENCES:

[ 1] Zheng Hu. Network and Information Security [M].Peking: Tsinghua University Pres, 2006.

[ 2] Man Young Rhee. Network Security Encryption Principle, algorithm and Protocol [M].Peking: Tsinghua University Pres, 2006.

[ 3] Suri , P. R . ; Rani , S.Bluetooth security Need to increase the efficiency in pairing [J ]. IEEE/ Southeastcon, 2008.

[ 4] Fengying Wang. Dynamic Key 3DES Algorithm of Discrete System Based on Multi-dimension Chaos[J]. Microelectronics and Computer,2005, 7: 25-28.

[ 5] Falk A. The IETF, the IRTF and the networking research community[C].Computer Communication Review,v35,n5,Oct.2005:6970.

[ 6] Yaniv Shaked , Avishai Wool . Cracking t he Bluetooth P[C]. 3rd USEN IX/ ACM Conf. Mobile Systems, Application and Services (MobiSys). Seattle, WA , J une 2005 :39250.

[ 7] A. Menezes, P. van Oorschot, S. Vanstone. Handbook of Applied Cryptography .CRC Press. 1996.

[ 8] M.Shnad and J.Vuillemin, “Fast implementation of RSA cryptography”, proceedings of the IEEE symposium on computer Arthematic,1993

[ 9] R.Rivest, .Shanir, L.Adleman, "A Method for obtaining DigitalSignatures and Public Key Cryptosystems," Comm. of ACM, 21(2), pp. 120-126, Feb. 1978

[ 10] Bluetooth CIG, Specification of the Bluetooth system, Version 1.1, February 22, 2001. Available from www.bluetooth.com.

[ 11] National Bureau of Standards, Data Encryption Standard, FIPS Publication 46, U.S. Department of Commerce, 1977.