A Middleware Design for Block Cipher Seamless Connected into Stream Cipher Mode

Lan Luo[1], ZhiGuang Qin[1], ShiJie Zhou[1], ShaoQuan Jiang[2], Juan Wang[1]
School of Computer Science and Technology, University of Electronic Science and Technology of China , Chengdu, 610054, China
Department of Computer Science University of Calgary 2500 University Drive, NW Calgary T2N 1N4, CANADA
E-mail: luolan@uestc.edu.cn

Abstract

In order to connect the block cipher into stream cipher mode, the middleware about output of the block cipher was designed according to flexible and scalable principle. The byte wise operation can be paralleled to more large scale such as 32bit wise or 16bit wise. Secure of this design was demonstrated by the block cipher algorithm itself and the complexity of mask algorithm. The middleware model and the block cipher algorithm model are seamless connected because of standardized block size and output size. Furthermore, such standardized size can be actively changed with the application environments. The approach of this paper is that a kind of complex mask was used in block cipher algorithm when embedded it into stream operation mode such as Cipher Feedback Mode , Output Feedback Mode and Counter Mode.

1. Introduction

One important development happened in the legal area and approximately at the same time when cipher Rijndael was chosen as the AES. These projects[1,2] produced portfolios of primitives recommended for ISO standards such as NESSIE or E-government. Since 2000 NIST has been running an effort for selection of modes of operation for block-ciphers. Recently, the PRESENT[3] block cipher already was published by this way. With the development of block cipher's design and analysis, the design of stream cipher is combining more character of block cipher. There are kinds of methods to use block cipher as stream cipher such as adopting block cipher's Output Feedback Mode (OFB mode) directly etc. The block cipher as a nonlinear part of stream cipher is also a trends in algorithm design. Such development in stream cipher has been shown in candidate of eSTREAM project. The rest of this paper is organized as follows. Section 2 contains overview of CFB, OFB and CTR modes of block cipher. Then a design for integrated the middleware between block cipher and stream cipher is shown in section 3. Section 4 contains conclusion about the design.

This work was partly supported by the National Nature Science Foundation of China under Grant No. 60673075, National 863 Program Grant No. 2006AA01Z428.

2. A design for integrated middleware between block cipher and stream cipher

The CFB mode (fig 1) and OFB (fig 2) mode are two kinds of synchronizing block cipher modes. Both of such two modes actually used as iterated nonlinear function in stream cipher's design. The block size and key size of block cipher which are at lest 128bits now decided the security level of this nonlinear function.

The cipher feedback mode, CFB, follows the second basic approach, namely to achieve a variant of the one-time key encryption mechanism: The required pseudorandom cipher key stream is generated by means of the encryption algorithm Block Encryption of the underlying block cipher, notably without employing the corresponding decryption algorithm. Hence, this mode

cannot be used for an asymmetric block cipher. Basically, the cipher key stream is extracted from the outputs of the block cipher encryption whose inputs are taken as a feedback from the ciphertext stream. At the beginning, before the feedback is available, an initialization vector is used as a seed, which must be used only once but can be communicated to the receiver without protection. The output feedback mode, OFB, follows the second basic approach too: The required pseudorandom cipher key stream is generated like for the cipher feedback mode, except that the block cipher encryption takes the feedback directly from its own outputs. There is CTR mode that also can convey block cipher to stream cipher. But the character of string generated by such kind of mode is not controlled by designers themselves when it was used as a nonlinear part of stream cipher.

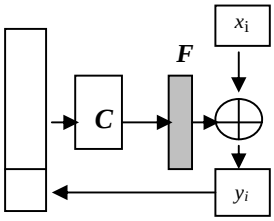

fig1. CFB mode

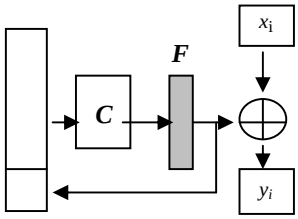

fig2. OFB mode

Obviously, the ciphertext of CFB mode can be directly effect by last clock's cipher state. On the contrary the ciphertext of OFB mode is only related to the key and the plaintext. Two kinds of operation modes' security were proved in many related thesis.

2.1. Kinds of attack to block cipher

There are two basic directions in block cipher algorithm design. The first one is designed based on security. The factors relate securities include length of block and key length etc. The essence principals also are confusion and diffusion. The confusion principle requests enough complexity relationship among key, plaintext and ciphertext so that this relationship cannot be used in cryptanalysis. The diffusion principle is that every key bit should change the ciphertext as much as possible to avoid slide attack the same as to make ciphertext's frequency becoming random. The second is that design faced to implementation. Block cipher algorithm can operate with both software and hardware. The hardware's merit is high-speed meanwhile the software is very flexible and cheap. This paper's idea is that the software implementation principles are module design and simple algorithm. Encryption algorithm is operated in module and the module length should suitable for the software programming. The required equality of the shift inputs on both sides is achieved by using the same initialization vector, and then inductively by employing the same operations and inputs to generate them. The key generation must against every kind of known attack. There are some attack methods to block cipher key and the design of this paper is a new idea to decrease such kinds of attack:

1. Linear attack[4,5,6]

This generalization of linear cryptanalysis uses the notion of binary I/O sums. An attacker attempts to find a statistic a limit balance that can be described as the result of some group operation on some function of the plaintext and some function of the ciphertext. Multiple linear approximations allow one to combine the bias of several high-probability linear approximations.

2. Differential attack[7,8]

The general idea of the attack is to force a characteristic for the F function to Occur in the second round. We realize this characteristic internally by causing the same low Hamming-weight xor difference to occur in the outputs of both g computations in the second round of the cipher. When this happens, and there are k bits in that xor difference, there is a 2^{-k} probability that the Output of the PHT will be unchanged in one of its two words. Until now such kind of attack method is one of most powerful methods to analysis a cryptography algorithm.

3. Differential-linear Cryptanalysis[9]

Differential-linear cryptanalysis uses a combination of techniques from both differential and linear crypt analysis. Due to the need to cover the last part of the cipher with two copies of a linear characteristic, the bias of the linear characteristic is likely to be extremely small unless the linear portion of the attack is confined to just three or four rounds. This means that the cryptanalyst would need to cover almost all of the rounds with the differential characteristic, making a

differential-linear analysis not much more powerful than a purely differential analysis.

4. Side-Channel Cryptanalysis and Fault Analysis [10,11]

Side-channel cryptanalysis uses information about the cipher in addition to the plaintext or ciphertext. Examples include timing, power consumption, NMR scanning, and electronic emanations. With many algorithms sit is possible to reconstruct the key from these side channels. Fault analysis can be used to successfully cryptanalyze this cipher. Again, we believe that total resistance to fault analysis is an impossible design constraint for a cipher. The resistance to fault analysis of any block cipher can be improved using classical fault tolerance techniques.

5. Interpolation Attack[12]

The interpolation attack is effective against ciphers that use simple algebraic functions. The principle of the attack is simple: if the cipher-text can be represented as a polynomial or rational express on of the plaintext, then the polynomial or rational expression can be reconstructed using N plaintext/ciphertext pairs. However, interpolation attacks are often only work-able against ciphers with a very small number of rounds, or against ciphers whose rounds functions have very low algebraic degree.

2.2. Overview of block cipher modes

A block cipher mode, or mode, for short, is an algorithm that features the use of a symmetric key block cipher algorithm to provide an information service, such as confidentiality or authentication. NIST is in the process of recommending modes in a series of special publications. Currently, there are seven block cipher modes that may be used with NIST's approved encryption algorithms: Five modes for confidentiality, one for authentication, and one combined mode for confidentiality and authentication. 1. ECB-Electronic Codebook: Every Block is treated independently. It does not hide patterns or Plaintext repetitions Error propagation: expansion within 1 block Limited number of applications. 2. CBC-Cipher Block Chaining: Ciphertext depends on all previous plaintext blocks Hides patterns and Plaintext repetitions Error propagation: expansion in 1 block, copied into next block Standard Mode for Block cipher before the AES Selection Process. 3. OFB-Output Feed Back: Synchronous Stream Cipher, No linking between subsequent blocks, No error propagation: errors are only copied. 4. CFB-Cyphertext Feed Back: Self-synchronizing Stream Cipher. Ciphertext depends on all previous plaintext blocks. Error propagation: error copied and propagated over 1 block. 5. CTR-Counter Mode: Every Block is treated independently. It hides patterns and Plaintext repetitions. Error propagation: expansion within 1 block. Mode allows Random Data Access. Security is comparable with CBC-Mode.

2.3. A design for integrate the middleware

So we design a F function in fig1 and fig2 to avoid kinds of attack. The F function was designed as flexible and scalable. The simplest design from our view is adopt a count figure to choose the m byte wise output use the block XOR iterated then math add 2^m which change the CFB mode's last clock ciphertext information leak. (fig3).

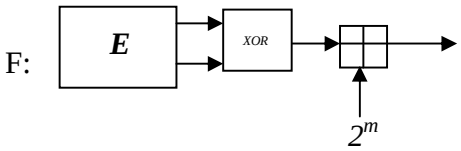

fig3 The middleware of F function

The block XOR is the algorithm that takes m bit E function output XOR directly. Such operation can confuse the n byte into m byte. The add algorithm is a nonlinear algorithm which let the XOR result more complex. This design can be implemented easily by both of software and hardware with little value. The F function take as a nonlinear function to adopt m bit output more complex and security as well as let the encrypt algorithm itself has far distance to ciphertext. The speed of such middleware was the same as adopt lest m bit directly. This kind of design is actually an implementation map of n bits to m bits.

2.3. The character of flexible and scalable about the design

Usually, F function is directly filtered the lowest or highest m bytes as the stream key or feedback to the

next E operation. Let the block size is n bytes. The iterated XOR in our design means that XOR the E function's output according stream key which is the same as the feedback size m bytes. Such linear algorithm can confuse all information of E function directly and simply, avoiding the leak of the information of n to m bytes. The information entropy increased $m\log 2^m$ to $n\log 2^n$. The result adds to counter figure 2^m change the linear character of XOR and can judge the steps of such system easily if necessary. Because the middleware cover the E function by a linear layer and a nonlinear layer, the CFB and OFB modes became more security. With enforcing the security the number of n and m can be changed as byte wise according implementation ability of hardware.

3. Conclusion

The area of symmetric key encryption has been very active recently due to growing interest from both academic and industry research, standardization efforts like AES, NESSIE and CRYPTREC, as well as due to ease of some governments control over export of cryptography. A block cipher algorithm is a type of cryptographic system that usually strengthen internet network and wireless networks more security directly. To enforce security factor the effective of algorithm may be decreased sometimes. Typically, this idea focused on published block cipher, such as DES, AES, Camellia, Serpent, Present etc. The middleware part is a simple design to solve the seamless connection that the block cipher algorithm operates as a stream cipher mode. In another view we can think this design as a simple nonlinear mask of block cipher's OFB operation mode. The mask changes the output character easily. Stream cipher or block cipher is lightweight, suitable to security of RFID as well as Internet environment. Sometimes, such flexible and scalable model can be named cryptography middleware, of cause, this is a visual name accepted by specialist. Furthermore, an obviously merit of cryptographic middleware is its character of upgrade because of its flexibility and scalable design.

References

[1] M.Walker T.Wright Security In F.Hillebr, GSM and UMTS: The creation of global mobile communication, NewYork, NY, JohnWiley& Sons, 2002, pp. 385–406.

[2] Daemen,J, Rijmen,V.: The Design of Rijndael: AES—The Advanced Encryption Standard. Berlin: Springer-Verlag, 2002.

[3] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, C. Vikkelsoe: PRESENT: An Ultra-Lightweight Block Cipher, Lecture Notes in Computer Science, Springer Berlin, Heidelberg , 2007.

[4] T. Kaneko, K. Koyama, R.T erada, Dy Ciphers, ETH Series on Information Pronamic Swapping Schemes and Differ entail cessing, v.7, HartungGorre Verlang Kon Cryptanalysis, IEICE Tranactions, v.E77-stanz, 1996. A,1994, pp.1328–1336.

[5] T. Jakobsen and C. Harpes, Bounds Cryptography Workshop Record, on Non-Uniformity Measures for General-School of Computer Science, Carleton Utilized Linear Cryptanalysis and Partitioning verisity, 1997, pp.201–212.

[6] M.Matsui, Linear cryptanalysis method for DES cipher. Advances in cryptology-Eurocrypt'93, LNCS 765, BerLin, Springer-Verlag, 1994, pp.17-26.

[7] M.Matsui T. Tokita. Cryptanalysis of a Reduced Version of the Block Cipher E2. In L. Knudsen, editor, Fast Software Encryption—6th International Workshop, FSE'99, Volume 1636 of Lecture Notes in computer Science, Berlin Heidelberg, New York, 1999. Springer-Verlag : pp71-80.

[8] Berbain, C.Gilbert, H. Patarin, J.QUAD: A Practical Stream Cipher with Provable Security. Vaudennay, S. EUROCRYPT 2006, LNCS, vol. 4004, Heidelberg, Springer, 2006, pp. 109-128.

[9] S. Langford and M. Hellman, Differential-Linear Cryptanalysis, Advances in Crypto. F.J. Mac Williams N.J.A. Sloane, "Theory CRYPTO'94 Proceedings, Springer-Theory of Error-Correcting Codes, North-Verlag, 1994, Holland, Amsterdam, 1977, pp. 17–26.

[10] J.Kelsey, B.Schneier, D.Wagner, L.Massey, SAFERK: A Byte-Hall, Side Channel Cryptanalysis of Prod-Oriented Block-Ciphering Algorithm, Fastuct Ciphers, ESORICS'98 Proceedings, Software Encryption, Cambridge Security Springer-Verlag, 1998. pp.87-89.

[11] D.Boneh, R. A. DeMillo, R.J.Lipt on On the Importance of Checking Crypto-graphic Protocols for Faults, Advances in Cryptology EUROCRYPT'97 Proceedings, Springer Verlag, 1997, pp.37–51.

[12] S. Moriai, T. Shimoyama, T. Kaneko, proceedings, Springer-Verlag, 1991.Interpolation Attacks of the Block Cipher: SNAKE, unpublished manuscript, 1998, pp.17–38.