Golden Fish: An Intelligent Stream Cipher Fuse Memory Modules

Lan Luo[2]，ZhengYao Wei[1]，ZhiGuang Qin[1]，WenZheng Zhang[2], ShiXiong Zhu[2]

1 School of Computer Science and Technology
University of Electronic Science Technology of China, ChengDu, China, 610054
2 No.30 Institute of CETC, No.810 box Chengdu, Sichuan, 610041, China

E-mail: lanneverlose@yahoo.com.cn

Abstract

In this paper, we use a high-order iterated function generated by block cipher as the nonlinear filter to improve the security of stream cipher. Moreover, by combining the published rounds function in block cipher and OFB as the nonlinear functional mode with an extra memory module, we enable to control the nonlinear complexity of the design. This new approach fuses the block cipher operation mode with two memory modules in one stream cipher. The security of this design is proven by the both periodic and nonlinear evaluation. The periods of this structure is guaranteed by the traditional Linear Feedback Shift Register design and the security of nonlinear characteristic is demonstrated by block cipher algorithm design itself, which is remarkably safer than the previous designs of stream cipher. We also can find such design style at SHA3.

Keywords: An intelligent golden Fish, LFSR & Block Cipher Modes as Stream Cipher, Memory Modules

1. Introduction

Recently, the area of symmetric key encryption is very active due to growing importance of both academic research and industrial applications. Despite of the standardization efforts (like AES [1], NESSIE [2] and CRYPTREC [3]) on the governmental controls over export of cryptography, stream cipher is seldom studied in public. The main idea of this paper is to replace the nonlinear function in stream ciphers by an equivalent operation mode in block cipher. Furthermore, we can intelligent design the ciphers according to different network environments [4-5]. In order to demonstrate our approach, we construct a simple synchronous stream cipher, which provides a significant flexibility for hardware implementations, with many desirable cryptographic advantages. The security of the encryption and decryption are based on the computational complexity, which is demonstrated by AES and NESSIE competition recently, where all the finalists fall into the category “no attack or weakness demonstrated”, in which people can go for the simplest, and most elegant design comparing an more complicate and non-transparent one. To implement the idea above, we take output feedback mode (OFB) of the block cipher as the nonlinear filter in stream cipher design. The rest part of this paper is as follows: Section 2 describes the typical structure of the block and stream cipher. A simple security proof is given for the new structure of stream cipher inspired by operation mode of block cipher afterwards. Section 3 summarizes the current results on the design based on information theory.

2. The Sketch Design: Fusing Block Cipher into Steam Cipher

One important approach is developed in the legal area at almost the same time when cipher Rijndael is chosen as the AES, which produce the portfolios of primitives recommended for ISO standards such as NESSIE or E-government. Since 2000, NIST has been making an effort for selection of modes of operation for block ciphers. The nonlinear feedback register is another interesting direction on the research of stream cipher design, which we will not discuss in this paper.

2.1 The typical structure of classical stream cipher

A typical stream cipher is incorporated by the state transition function computing a new state from the previous one, and the filter producing the output state. The state transition function is generated by a group of Linear Feedback Shift Registers （LFSR）, and the filter is generated nonlinearly by sorts of methods such as SBox, bent function, or some other combination flexibility functions (see Fig. 1）.

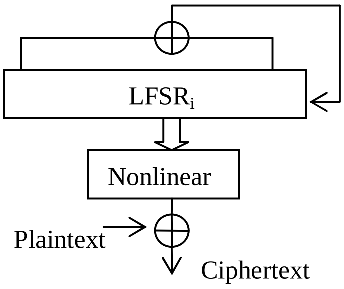

Figure 1. The typical stream cipher model

Current art on stream ciphers is less stable than on block ciphers, due to large variety of constructions, such as the difference between two basic models SPN (a stream ciphers) and Feistel cipher (a block cipher). In the area of the stream ciphers, Kasumi[6] provided a typical ciphers, which is a modification of a block cipher MISTY[7], as complementary standard A5/3 for 3GPP cellular phones in addition to the weak algorithms A5/1 and A5/2 used previously[8]. Trend of the stream ciphers' design turns into blockwise stream ciphers (i.e. output a block of bits, either one byte or 32-bits instead of a single bit), such as RC4, SNOW 2.0[9]. Stream cipher with part of structure from block cipher like round functions can intermix with more traditional LFSR-like structure such as MUGI [10].

2.2 A note to modes of block cipher operating as stream cipher

With the development of design and analysis of block cipher, there are many stream ciphers adopting the techniques from block ciphers such as Cipher Feedback mode (CFB mode) and Output Feedback Mode (OFB mode), which are two typical types of synchronizing block cipher modes and are used as iterated nonlinear function, of which the security level is determined by the block and key size of block cipher (at least 128bit in this study). The cipher feedback mode, CFB, follows the second basic approach, namely, an achievement of a variant of the one-time key encryption mechanism: the required pseudo-random cipher key stream is generated by the block encryption (an encryption algorithm) of the underlying block cipher, without employing the corresponding decryption algorithm. Thus, this mode cannot be used in an asymmetric block cipher. Basically, the cipher key stream is extracted from the outputs of the block cipher encryption whose inputs come from feedback of the ciphertext stream.

The collision of CFB mode is found with probability of $1/2^{s-t}$ if last clock's ciphertext is same, where *s* is the block size and *t* is the feedback size of CFB mode, which implies that under the ciphertext attack there are many same cipher chains in the ciphertext, and the cryptographic system can be recovered accordingly. Thus, CFB mode is not recommended as a nonlinear part of stream cipher or a key stream generator. On the contrary, OFB mode as an entire key stream of block cipher can be used as a feedback of the shift register, which can work as a high-order iterated nonlinear pseudorandom generator. Although CTR mode can convey block cipher to stream cipher as well, it suffers from the loss of key information and thus the generated string is out of control.

2.3 The new art of design inspired by OFB mode of block cipher

There are typical designs used technologies both for stream and block cipher. Some eSTREAM candidates and MUGI utilized arts of block cipher in stream cipher design as well. We summarize these designs in Table 1, showing that only SP structure is embedded in stream cipher.

*Table 1.*Updated Design of Stream Cipher

Algorithm	Stream cipher	Block Cipher
Trivium	NFSR	Design Principle
Sosemanuk	Snow2.0	Serpent
LEX	No	AES
MUGI	No	AES

The OFB mode of block cipher can be used as nonlinear function in stream cipher, which is another type of iterated structure based on simple round function of block cipher. The linear function module of the design adopts the uploadable and downloadable n LFSRs, with the period of 2^n-1. This memory module M_1 depends on both LFSR and OFB mode of block cipher (Fig. 2).

In Fig.2 we demonstrate the new architecture of stream cipher, where M_i modules are the memory designs, a store cells organized by some functions related to the last output's state, B module is a block cipher's OFB mode, and P module is the plaintext stream. The cipher stream is generated by key stream added the plain stream directly over the $GF(2^n)$. The key stream can be formularized as:

$$K(x) = B(F(M(x))), \text{ where } x \in GF(2^n),$$

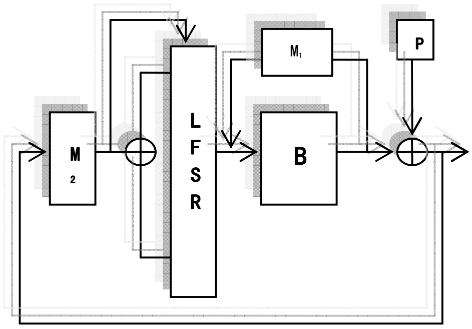

Figure2: Golden Fish: stream cipher fused with the block cipher design

Here, all the operations are accorded to bytewise technology. Function F denotes one of the LFSR's feedback n-order primitive polynomial, of which the hardware implementation is uploadable and down-loadable, with the periods at least 2^n-1. The value of n should choose as the times of minimum (CUP, OS), which usually as multi-32 or multi-64. The design model is against previous analysis, such as Linear attack [11,12,13], Differential attack [14,15], Differential linear Crypt analysis, Side-Channel Cryptanalysis and Fault Analysis [16,17,18] etc. Function B is the OFB mode of a block cipher, where the round number is determined by the secure requirement to the cipher system such as computing capacity. If the block cipher is Feistel structure, the design also can be named as an intelligent silver fish. Once the M_i modules are adopted, the chance of many updated known attack, Interpolation Attack decreases. The M_1 can control the round number of block cipher, in Trivium which is 2 and is ultra-lightweight. But with the more secure of such design the weight of the design is heavier. So the Trivium is even light than Present which is the new design instead of KeeLoq. In this demonstration, we omit the details of each module.

3. Conclusion

With the development of eSTREAM, the design and analysis of stream cipher attract more public's attention. Especially, the fuse of both high-order iterated function and memory modules tend to be one of the main future designs of stream cipher. In this study, we show that a design implementing the OFB mode of block cipher does improve the security of the cipher, despite of increasing the operation time cost in iterative transformation. Indeed, security trades off the efficiency for current algorithm. Practically, the block cipher is applied as nonlinear function, as an economic method to promote the security. Furthermore, the realization of modules M_i, Module B and LFSR is highly flexible and transformable. For instance, treating the reversible block cipher as the nonlinear function of stream cipher could be another useful design in low layers of wireless networks as well as Internet. Further hardware implementation can merge block cipher in stream cipher directly and increases speed of the stream cipher accordingly. In Shabal of SHA3, the mode2 shows the M_2=2circles memory while the mode1 is the M_2=1circle. The M_1 is implemented as the compression function of Keccak. Every part of golden fish can be achieved as intelligent level because M_1, M_2, LFSR and B are designed to highly changeable, flexible and transformable. Furthermore, the seamless connection of every part is a very difficult project. Maybe we name it as a stream cipher hopping.

References

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

[2] B.Preneel, A. Biryukov, C. De Canniere, Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption. https://www.cosic.esat.kuleuven.be/nessie/ 2008

[3] The CRYPTREC Advisory Committee, Cryptrec Report 2006; Report of the Cryptographic Technique Monitoring Subcommittee. http://www.cryptrec.jp/english/system.html 2008

[4] Luo, Lan, Qin, ZhiGuang, Wang, Juan, Intelligent Application Conversion of Block Ciphers for Different Network Layers, International Journal of Innovative Computing, Information and Control， Volume 3, Issue 1, 2009.3

[5] Luo, Lan, Qin, ZhiGuang, Jiang, ShaoQuan, The Intelligent Secure Structure Based on Active Block Ciphers for Application Layer of Internet. The 2008 International Congress on Image and Signal Processing, IEEE proceeding, 2008.5

[6] G. O. Partners, Specification of the 3GPP confidentiality and integrity algorithms: Kasumi algorithm specification–3GPP TS 35.202,

Technical report, http://www.3gpp.org/TB/Other/algorithms.htm, 2000

[7] M. Matsui, Block encryption algorithm MISTY, in Fast Software Encryption, FSE'97 (E.Bihamhed.), vol.1267 of Lecture Notes in Computer Science, pp.64– 74, Springer-Verlag, 1997

[8] 3GPP Standard. http://www.3gpp.org/ 2008

[9] P.Ekdahl T.Johansson.Anew version of the stream cipher SNOW In K.Nyberg and H.Heys, editors, Selected Areas in Cryptography, 9th Annual International Workshop, SAC2002, St.John's, New foundland, Canada, August15-16, 2002

[10] D.Watanabe, S.Furuya, H.Yoshida, K.Takaragi, B.Preneel. A new key stream generator MUGI. In J.Daemen V.Rijmen, editors, Fast Software Encryption, 9th International Workshop, FSE2002, Leuven, Belgium, February4-6,2002 ,Revised Papers, volume 2365 of Lecture Notes in Computer Science, pages179–194. Springer-Verlag, Berlin, 2002

[11] 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, , pp.1328–1336, v.E77-stanz, 1996.

[12] 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, pp.201–212, 1997.

[13] Akio Tsuneda, Sho Mitsuishi, Takahiro Inoue, A Study on Generation of Random Bit Sequences with Post-Processing by Linear Feedback Shift Registers, International Journal of Innovative Computing, Information and Control Volume 4, Number 10, October 2008 , pp.2631—2638

[14] Michel Abdalla, Xavier Boyen, C′eline Chevalier, David Pointcheval, Distributed Public-Key Cryptography from Weak Secrets, 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, CA, USA, March 18-20, 2009 Proceedings, pp.139-159.

[15] Manoj Prabhakaran, Rui Xue, Statistically Hiding Sets, The Cryptographers' Track at the RSA Conference 2009, San Francisco, CA, USA, April 20-24, 2009, Proceeding, pp.100-116

[16] Sung Jae Park, Jung-hak Nam, Dong-gyu Sim, Seoung Jun Oh, Jin Woo Hong, Reduced – Resultion Intra Block Cipher, ETRI Journal, vol.31, no.1, Feb. 2009, pp.80-82.

[17] 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, pp.37–51, Springer Verlag, 1997.

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