A New Approach to the Definition of Information Diffusion and Confusion of Boolean Transformation

Lin Li[1,*], Zhiyin Kong[2], Fengmei Liu[2], Kun Li[3] and Xiubin Fan[4]
[1]School of computer and information technology, Beijing Jiaotong University, China
[2]Science and Technology on Information Assurance Laboratory, China
[3]Institute of Information Technology, China
[4]Institute of Software, Chinese Academy of Sciences, China
[*]Corresponding author

Abstract—**Mass, energy and information are the three important quantities in the physical world. The diffusion and confusion of information is the guiding ideology of cipher algorithm coding. Linear transformation is generally used to realize the diffusion of information and S-box is used to realize the confusion. This paper presents the concept of the information diffusion and confusion degree in Boolean transformation and proves that the biggest information diffusion and confusion degrees are both $n-1$ in the n tuples Boolean linear invertible transform. Furthermore, we give the method to construct the maximum degree of diffusion and confusion degree for the structure of the reversible Boolean nonlinear transform. That is to say, the diffusion of information technology through reversible linear transformation in AES and SMS4, CAST is not optimal. The results presented in this paper, combined with the algebraic immune degree, balance, correlation immune, linear deviation and difference deviation, and other security cryptography parameters, can be used to design cryptographic algorithm with better properties.**

Keywords-diffusion; confusion; boolean function; boolean transformation

I. Introduction

Shannon information theory presents the basic concept and calculation formula of information. Since then, mass, energy and information become the three important quantities in the physical world. Shannon information theory is the foundation of source coding, channel coding, and cipher coding.

Cryptography is composed of cryptography design and cryptanalysis. Based on the principle of information theory, Shannon gives the concept of perfect security system in the paper "communication theory of secrecy system" [1], namely one-time pad; Also, he gives the cryptography design principles: the plaintext information diffusion and confusion under the control of key.

Under the guidance of Shannon information theory, a lot of symmetric cipher algorithm are designed based on the principle of diffusion and confusion, such as DES [2], AES [3], SMS4 [4], CAST [5], GOST [6], FLY [7], etc. Linear transformation is used to realize the design principle of information diffusion and nonlinear transformation is used to realize information confusion, which is the long-term experience for cryptography design in practice. But Shannon only pointed out the principles of diffusion and confusion in cryptography, and did not give their specific quantitative definition.

Webster and Tavares [8] proposed strict avalanche criterion, and Preneel [9] gave the concept of high-order diffusion. But the concept of vector Boolean function or permutation is not able to accurately depict the meaning and essence of Shannon information diffusion and confusion. Principle of information diffusion and confusion remains the foundation of symmetric cryptography design principle. So the further theory research is still needed.

The new definitions of Boolean function diffusion and confusion degrees are presented in this paper. In the future work, we will give the theory and application research.

II. Information diffusion of Boolean transformation

A. Basic Concept

The definition of Boolean function ring as follow.

For the binary domain $F_2 = \{0,1\}$, the n tuples Cartesian product of F_2 is $F_2^n = \underbrace{F_2 \times \cdots \times F_2}_{n}$ and the corresponding polynomial ring is $F_2[X_0, X_1, \cdots, X_{n-1}]$. The ideal generated by $X_0^2 - X_0, \cdots, X_{n-1}^2 - X_{n-1}$ is:

$$I =< X_0^2 - X_0, \cdots, X_{n-1}^2 - X_{n-1} > \tag{1}$$

Definition 1 The quotient ring about I is $F_2[X_0, X_1, \cdots, X_n]/I$, named n tuples Boolean function ring, commonly referred as B_n. The element in B_n is Boolean function, referred as $f(x_0, x_1, \cdots, x_{n-1})$.

Definition 2 The algebraic formal form of Boolean function is:

$$f(x_0 x_1) = \overline{x_0 x_1} + \overline{x_0} x_1 + x_0 \overline{x_1} . \tag{2}$$

Where $x^I = x_0^{i_0} \cdots x_{n-1}^{i_{n-1}}$, $I = (i_0, i_1, \cdots, i_{n-1})$, $a_I \in F_2$. It can be also denoted as:

$$f(x_0 x_1 \cdots x_{n-1}) = a_0 \oplus \cdots \oplus \sum_{0 \le i_0 < \cdots < i_{l-1} \le n-1} a_{i_0 \cdots i_{l-1}} x_{i_0} \cdots x_{i_{l-1}} \oplus \cdots \oplus a_{0 \cdots n-1} x_0 \cdots x_{n-1} \quad (3)$$

B. *The Information Diffusion of the Boolean Transformation*

In the algebraic formal form of n tuples Boolean function, let $\Omega_t, 1 \le i \le n$ denotes the collection of polynomials with the same order and nonzero coefficients. Obviously, $x_k \in \Omega_t$, there is at least one t times monomial which contains x_k .

Definition 3 If $x_k \notin \Omega$, then the variable x_k makes no effect for the Boolean function f .

Property 4 If the variable x_k makes no effect for the Boolean function f , $s = (0, \cdots 0, \underset{i-th\ position}{1}, 0 \cdots, 0)$ is the linear structure of $f(x)$ and $s \in U_f^{(0)}$, $f(x)$ is degradation function.

Proof: $\frac{\partial f(x)}{\partial s} = f(x+s) + f(x) = f(x) + f(x) = 0$, so property 4 holds.

Property 5 If $m(x_i) = 0$, then the variable x_k makes no effect for the Boolean function f .

Theorem 6 $m(x_i)$ is the translation invariant of Boolean function f input invariant.

Proof: Assume $m(x_i) = t$, there is at least one t times polynomial which contains x_k . Let all the t times polynomials with x_i be $x_i t_1, \cdots, x_i t_k$. Obviously, $t_1, \cdots, t_k$ are different monomials with the order $t-1$. $\forall v \in F_2^n$, after translation transformation of $x \oplus v$, $x_i t_1, \cdots, x_i t_k$ become polynomials. But the highest order item remains the same. For the item with the order greater than t in $f(x)$, after translation transformation of $x \oplus v$, there is no x_i . That is to say, no item can counteract $x_i t_1, \cdots, x_i t_k$.

Now, we can give the diffusion degree definition of the function:

$$F(x_0 x_1 \cdots x_{n-1}) = \left(f_0(x_0 x_1 \cdots x_{n-1}) \cdots f_{n-1}(x_0 x_1 \cdots x_{n-1}) \right) \quad (4)$$

In fact, such a vector Boolean function can be seen as Boolean transformation $F_2^n \to F_2^n$.

Definition 7 For a given i , if x_i makes effect about $f_j, 0 \le j \le n-1$, the information of x_i is diffused to f_j , then $\lambda_{ij} = 1$, else $\lambda_{ij} = 0$. The information diffusion degree of x_i in F is $d_i = \sum_{0 \le j \le n-1} \lambda_{ij}$. So the information diffusion degree of F is $d(F(x)) = \min_{0 \le i \le n-1} \{d_i\}$.

C. *The Information Confusion of the Boolean Transformation*

From the previous Boolean function f about $\Omega = \bigcup_{1 \le t \le n} \Omega_t$, we can define the confusion degree.

Definition 8 Let the Boolean transformation $F = F(f_0 \cdots f_{n-1})$: $F_2^n \to F_2^n$, every $f_i, 0 \le i \le n-1$ corresponding to Ω is Ω^i , then $\# \bigcap_{0 \le i \le n-1} \Omega$ is the confusion degree of Boolean transformation F , where $\#$ is the number of the set, referred as $c(F) = \# \bigcap_{0 \le i \le n-1} \Omega^i$.

Property 9 If there exists $0 \le j \le n-1$, $x_j \notin \bigcap_{0 \le i \le n-1} \Omega^i$, then x_i makes no effect for some $f_k, 0 \le k \le n-1$.

Proof: It can be proved by contradiction. If it make effect for any k , then there exists $x_j \notin \bigcap_{0 \le i \le n-1} \Omega^i$, which makes $f_k, 0 \le k \le n-1$ no effect to Boolean function f .

Proposition 10 If Boolean transformation F : $F_2^n \to F_2^n$ is linear invertible transform, then the confusion degree $c(F) < n$.

Proof: If the confusion degree $c(F) = n$, for every $\Omega^i = \{x_0, x_1, \cdots, x_{n-1}\}$, $0 \le i \le n-1$, since F is linear invertible transform, assume $F(x) = xA$, then A is

$$A = \begin{pmatrix} 111 \cdots 111 \\ 111 \cdots 111 \\ \vdots \\ 111 \cdots 111 \end{pmatrix}_{n \times n} \quad (5)$$

Namely, every element in matrix A is "1", $rank(A) = 1$. So A is not invertible matrix and the proposition holds.

What is the biggest confusion degree for nonlinear reversible transformation? The answer is given below.

Theorem 10 When $n \geq 4$, $g(x_0 x_1 \cdots x_{n-1}) = \sum_{0 \leq i \leq n-1} x_i x_{i+1}$,let:

$$\begin{cases} f_i\left(x_0 x_1 \cdots x_{n-1}\right) = g\left(x_0 x_1 \cdots x_{n-2}\right) + x_i + x_{n-1}, i = 0, \cdots, n-2; \\ f_{n-1}\left(x_0 x_1 \cdots x_{n-1}\right) = g\left(x_0 x_1 \cdots x_{n-2}\right) + x_{n-1}. \end{cases} \quad (6)$$

Then $c(F) = n$.

Proof: Since the constructed function is reversible Boolean transformation, from the standard form of Boolean algebraic function

$$\Omega^i = \Omega_1^i \bigcup \Omega_2^i = \left\{x_0, x_1, \cdots, x_{n-1}\right\}, 0 \leq i \leq n-1 \quad (7)$$

$$\text{So } \# \bigcap_{0 \leq i \leq n-1} \Omega^i = n$$

The conclusion in this section can be applied to the research of general vector Boolean function.

III. Conclusion

The concepts of information diffusion and confusion degrees of Boolean transform are given in this paper. We have proved the biggest information diffusion and confusion degrees of Boolean linear invertible transform are $n-1$. At the same time, we give the method to construct Boolean nonlinear invertible transform structure with the maximum degree of diffusion and confusion degree n. Under the guidance of the results in this paper, in combination with other cryptography security parameters, cryptographic algorithm can be designed with better properties.

Acknowledgment

Project supported by the Fundamental Research Funds for the Central Universities (Grant No.2014JBM033)and the National Natural Science Foundation of China (Grant No.61402035).

References

[1] C. E. Shannon, “A note on the concept of entropy,” Bell System Tech. J, vol. 27, pp. 379–423, 1948.

[2] D. E. Standard, “FIPS pub 46,” Appendix A, Federal Information Processing Standards Publication, 1977.

[3] J. Daemen and V. Rijmen, The design of Rijndael. Information security and cryptography. Springer Berlin, 2002.

[4] Lü S W, Fan X B,Wang Z S 2008 Complete Mapping and Application in Cryptog-raphy(Hefei: University of Science and Technoloqy of China Press) p241(in Chinese)

[5] C. Adams, “The CAST-128 encryption algorithm,” 1997.

[6] I. A. Zabotin, G. P. Glazkov, and V. B. Isaeva, “Cryptographic protection for information processing systems, Government Standard of the USSR, GOST 28147-89. Government Committee of the USSR for Standards,” Russian, translated to English at ftp. funet. fi/pub/crypt/cryptography/papers/gost/russian-des-preface. ps. gz, 1989.

[7] Lü S W, Fan X B, Zhou Y J. 2003, Design and analysis of stream cipher, Chinasoft elec-tronic publishing house, Beijing, pp.43.

[8] A. F. Webster and S. E. Tavares, “On the design of S-boxes,” in Advances in Cryptology—CRYPTO’85 Proceedings, 1986, pp. 523–534.

[9] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle, “Propagation characteristics of Boolean functions,” in Advances in Cryptology—EUROCRYPT’90, 1991, pp. 161–173.