Advanced Engineering Forum *Online: 2012-09-26*
ISSN: 2234-991X, Vols. 6-7, pp 54-57
doi:10.4028/www.scientific.net/AEF.6-7.54

Cryptographic Properties and Quadratic Equations of S-box in SMS4

Kuanjiang Xiong[1,a] Zhihua Hu[2,b]

[1] College of Mathematical and computer Sciences, Huanggang normal University, Hubei 438000, P. R.China

[2]FCollege of Mathematical and computer Sciences, Huanggang normal University, Hubei 438000, P. R.China

[a] 243675244@qq.com, [b]huzhihua123@126.com

Corresponding author: Zhihua Hu ,

Corresponding author E-mail:huzhihua123@126.com.

Keywords: SMS4, algebraic expressions, Quadratic Equations

Abstract. Analysis of the S-box password SMS4 algorithm characteristics, discussed the algorithm of S-box algebraic balance, nonlinearity, avalanche characteristics, diffusion characteristics, and XLS attack the related quadratic equation number. Compared with the S-box of AES, Camellia algorithm, algorithm SMS4 S-box design has reached the standards of Europe and the United States block cipher standard algorithm for the S-box design. However, the algorithm's overall security features remains to be further studied.

Introduction

In 2001, Nicolas and Pieprzyk designed a new algebraic attack –XSL(eXtended Sparse Linearization) attack[1] to attack Serpent and AES, simplifying cryptanalysis of Serpent and AES into the problem of solving multivariate quadratic equations (MQ problem). The key technique in XSL attack is to describe non-linear parts of block ciphers in the form of quadratic equation, overdetermine it through XSL and solve the equation with linear methods. However, it remains an open question as to whether this attack method is effective or not.

In 2005, Carlos Cid et al. revealed the essence of XSL[2] attack, pointing out that XSL attack is ineffective for equations constituted by Serpent and AES. Meanwhile, hidden equations in the non-linear parts of block ciphers found by Courtois et al. provided new directions for future research.

This paper analyzed hidden equations of non-linear parts in block cipher Serpent[3] while combining boomeran[4][5] attack and Rectangle[5][6] attack in order to design a new method called differential algebraic attack, and put forward algebraic attack of 10-round Serpent-128.

Well-designed S-box to ensure that the cryptographic algorithms better able to resist the differential cryptanalysis and linear cryptanalysis attacks, while the S-box of any defects that may affect the safety of the entire algorithm.

SMS4 algorithm principle

SMS4 algorithm S-box algebraic properties

S-box is the only non-linear structure of most of the block cipher algorithm, their passwords properties directly determine the performance of cryptographic algorithms.

S-box algebraic expression

If the password elements in the compact algebraic expressions, and these elements can be combined into control the complexity of the expression, then the interpolation method of attack is feasible for the password, the lower the number and complexity of transformation algebra .The password is particularly effective. To prevent injection attacks, usually require a password to transform the algebraic expression has a high enough frequency and complexity.

$$f(x)=\sum_{io0}^{255} y_i \prod_{j\neq i,j=0}^{255} \frac{x-x_j}{x_i-x_j} \tag{1}$$

Differential characteristics

Differential cryptanalysis is a chosen plaintext attack, the basic idea is the possibility to obtain the corresponding ciphertext through the analysis of the specific expressly poor key, it is one of the most effective ways to attack the block cipher. The S-box ability to anti differential cryptanalysis from the differential uniformity and differential distribution matrix approach: with a smaller differential uniformity is a necessary condition for the S-box against differential attacks.

Linearity characteristics

Linear cryptanalysis is a known plaintext attack, the goal is to find linear expressions and use between the number of bits of the plaintext P, ciphertext C and key K. Established by the expression probability and 1/2 deviation size is an important measure of linear cryptanalysis. Linear cryptanalysis thinking boils down to the core components of the S-box is to examine the relationship between the input and output bit can be linearly distributed matrix to characterize.

Table 1,is SMS4 algorithm for the calculation of the S-box of the AES algorithm and the Camellia algorithm of the data indicators, this expression, non-linear and anti-attack capability to conduct a comprehensive comparison.

Table 1 Cryptographic Properties

	SMS4	AES	Camellia			
			S1	S2	S3	S4
number of equations	254	254	254	254	254	254
number of items	255	9	254	253	254	255
Nonlinear degree	112	112	112	112	112	112

Although the number of SMS4 algorithm, AES algorithm and the Camellia algorithm S-box algebraic expression are 254, but up to 255 the number of SMS4 algorithm and Camellia algorithm, the AES algorithm is only 9.Visible SMS4 algorithm and the Camellia algorithm S-box algebraic expression is more complex than the AES, to some extent, to better ensure the security of the algorithm.

Quadratic Equations of S-box in SMS4

As S-boxes [8][9][10] are the most important non-linear parts in block cipher, how to utilize equations constructed by S-boxes to attack ciphers is an important study question of cryptanalysis. In 2011, Hu Zhi-Hua, Qin Zhong-Ping utilizes algebraic equations about input and output differentials as well as keys that can be constructed by S-box, which are combined with differential attack in order to put forward a new 8-round Serpent-128 differential algebraic attack. This method needs $2\times2^{95}\times2^{14}=2^{110}$ pairs of selective plaintexts, 2^{96} times of 8-round encryption and 2^{96} times of 8-round decipher, 2^{96} packets of memory store room to guess 12 bits of 8-round Serpent-128 encrypted keys[13,14].

Quadratic Equations

Definition 1: Set $(y_0,\cdots,y_{n-1})=S(x_0,\cdots,x_{m-1})$ as multi-output function of S-boxes with m as input and n as output, in which $x_i,y_j\in(0,1)$, $i\in(0,1,\cdots,m)$, $j\in(0,1,\cdots,n)$. Thus, multivariate coefficient matrix about x_i,y_j can be constructed according to the above function.

The multi-output function for S-boxes in Serpent encryption algorithm is $(y_0,\cdots,y_3)=S(x_0,\cdots,x_3)$, according to which full binary coefficient matrix of the size of 16×25 can be constructed, with array elements as $1,x_0,\cdots,x_3,y_0,\cdots,y_3,x_0x_1,\cdots,x_2x_3,y_0y_1,\cdots,y_2y_3,x_0y_0\cdots x_3y_3$.

Definition 2: After linearizing the formed binary coefficient matrix, we can obtain fundamental system of solutions in the form of the following equation:

$$\sum a_{ij}x_iy_j+\sum\beta_{ij}x_ix_j+\sum\chi_{ij}y_iy_j+\sum\delta_ix_i+\sum\phi_iy_i+\varepsilon=0$$

$$a,\beta,\delta,\chi,\varepsilon\in(0,1).$$

We call $\sum a_{ij}x_iy_j+\sum\beta_{ij}x_ix_j+\sum\chi_{ij}y_iy_j+\sum\delta_ix_i+\sum\phi_iy_i+\varepsilon=0$ the full quadratic algebraic equation of S-box; the equations that only contain a part of the above equation are called partially quadratic algebraic equations.

Theorem 1: For arbitrary S-boxes whose multi-output function is $(y_0,\cdots,y_n)=S(x_0,\cdots,x_m)$, if fundamental system of solutions constructed according to Definition 1 and Definition 2 contain equation of the following form:

$$\sum\beta_{ij}x_ix_j+\sum\delta_ix_i+\sum\phi_iy_i+\varepsilon=0. \tag{2}$$

Then we can make use of input differentials of two pairs of plaintexts to construct output differential and first order algebraic equation of the key.

Proving: Set $x(x_0,x_1\cdots,x_n)$, $y(y_0,y_1,\cdots,y_m)$ respectively as input and output of S-boxes, $z(z_0,z_1,\cdots,z_n)$ as plaintext, $k(k_0,k_1,\cdots,k_n)$ as the key, then $x=z\oplus k$ .Thus, the following can be obtained:

$$\begin{aligned}&\sum\beta_{ij}(z_iz_j+z_ik_j+z_jk_i+k_ik_j)+\\&\sum\delta_i(z_i+k_i)+\sum\phi_iy_i+\varepsilon=0\end{aligned} \tag{3}$$

Set $z^{\omega}(z_0,z_1,\cdots,z_n)$, $y^{\omega}(y_0,y_1,\cdots,y_m)$ as the first pair of plaintexts and ciphertexts, $z^{\omega}(z_0,z_1,\cdots,z_n)$, $y^{\omega}(y_0,y_1,\cdots,y_m)$ as the secondpair of plaintexts and ciphertexts. Thus, the following can be obtained:

$$\begin{aligned}&\sum\beta_{ij}((z^{(1)}{}_iz_j+z^{(0)}{}_iz_j)+(z^{(1)}{}_i+z^{(0)}{}_i)k_j+(z^{(1)}{}_j+z^{(0)}{}_j)k_i)+\\&\sum\delta_i(z^{(1)}{}_i+z^{(0)}{}_i)+\sum\phi_i(y^{(1)}{}_i+y^{(0)}{}_i)+\varepsilon=0\end{aligned} \tag{4}$$

Table 2 is the Quadratic Equations of the S-box of the AES algorithm, SMS4 algorithm and the Camellia algorithm .

Table 2 Quadratic Equations

	DES	SMS4	AES	Camellia			
				S1	S2	S3	S4
The number of some quadratic equation	0	23+1	23+1	23+1	23+1	23+1	23+1
The number of full quadratic equation	0	37	37	37	37	37	37

Table 2 compares the three major block cipher algorithm, which DES, the number of algebraic equations is zero, one of the reasons, we find that the box to teach difficult to construct algebraic equations, input and output unbalanced, 4 × 4,8 × 8 boxteach is easy to construct algebraic equations.

Conclusions

Analysis of the S-box password SMS4 algorithm characteristics, discussed the algorithm of S-box algebraic balance, nonlinearity, avalanche characteristics, diffusion characteristics, and XLS attack the related quadratic equation number. Compared with the S-box of AES, Camellia algorithm,

algorithm SMS4 S-box design has reached the standards of Europe and the United States block cipher standard algorithm for the S-box design. However, the algorithm's overall security features remains to be further studied.

Acknowledgments

This research was supported by the Hubei Province Natural Science Foundation 2010CDZ019, the outstanding young talents of the Hubei Provincial Department of Education project Foundation Q20122703, Corresponding author:Zhihua Hu , E-mail:huzhihua123@126.com.

References

[1] NICOLAS T, PIEPRZYK J. Cryptanalysis of block ciphers with overdefined systems of equations[C]// Proceedings of Cryptology—ASIACRYPT 2002. Berlin: Springer-Verlag, LNCS, 2002,2551:13-19.

[2] CARLOS C, LAURENT G. An Analysis of the XSL Algorithm[C]// Proceedings of ASIACRYPT 2005, Berlin: Springer-Verlag,LNCS,2005. 3788: 333–353.

[3] BIHAM E, BIRYUKOV A, SHAMIR A.Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials[C]// Proceedings of Eurocrypt'99. Berlin: Springer-Verlag, LNCS, 1999. 1592: 12—23.

[4] WANGER D. The boomerang attack[C]// Proceedings of Fast Software Encryption'99. Berlin: Springer-Verlag, LNCS, 1999.1636: 156—170.

[5] ZHANG Lei,WU Wen-lin.Rectangle and boomerang attacks on DES[J].Journal of Software, 2008, 10（19）:2659-2665. (in Chinese)

[6] J. Kelsey, T. Kohno, B. Schneier, Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent[C]// proceedings of Fast Software Encryption 2000, Berlin:Springer-Verlag, LNCS, 2001. 1978: 75—93.

[7] BIHAM E, DUNKELMAN O, NELLER N. The rectangle attack—rectangling the Serpent[C]// Proceedings of Eurocrypt'01. Berlin:Springer-Verlag, LNCS, 2001. 2045: 340—357.

[8] CLARK J A,JACOB J L,STEPNEY S. The design of S_boxs by simulated annealing[J]. New Generation Computing,2005,23(3):219-231.

[9] GUPTA K C, SARKAR P. Improved construction of nonlinear resilient S_boxes[J]. IEEE Trnsactions on Information Theory,2005,51(1):339-348.

[10] SANTIS A D,FERRARA A L,MASUCCI B. Enforcing the security of a time-bound hierarchical key assignment scheme[J]. Information Sciences,2006,176(12):1684-1694.

[11] LIU Jia, WEI Baodian,DAI Xianhua. Cryptographic Properties of S-box in SMS4,Computer Engineering,2008,34(5):158-160.

[12] Zhang Guo-ji,Xiao Huangpei. Quadratic Equations on S-Boxes and a New S-Box Design Criterion, Journal of South China University o f Technology,2008,36(8):140-144.

[13] Chen Wenlue, Li Boli, Hu Zhihua.Intelligence Information Processing and Trusted Computing (IPTC), 2010,573-576.

[14] Hu Zhihua.Differential Algebraic Attack of Serpent, JOURNAL OF BEIJING UNIVERSITY OF TECHNOLOGY,2010,36(5):651-653.