Trends in Mathematics
Information Center for Mathematical Sciences
Volume 8, Number 1, June, 2005, Pages 69–75

THE CONDITION OF XSL FOR A BLOCK CIPHER

BONWOOK KOO, HWANSEOK JANG, AND JUNGHWAN SONG

Abstract. In this paper, we introduce a modelling of generalized block cipher and try to solve using XSL with eliminating of obvious linear dependencies. And we count the number of monomials and equations so that verify their relationship and find the condition to XSL feasible. We conclude that the XSL is feasible if each system of linearized equations for every s-box is overdefined.

1. Introduction

Recently algebraic attack is given many attentions which make it possible to analyze a symmetric cipher with nonlinear but low degree equations describe its nonlinear core. This attack is very useful and powerful against stream ciphers with linear feedback and such a polynomial based stream ciphers. But there are some difficulties to attack block ciphers with this attack. Because the system of equation is very large to solve with usual methods. So XL and XSL are proposed by Courtois et.al. [1, 2] and it seems to be able to break block cipher like AES. However, no practical attack with this method published even on a small example, so far. Only there are a few research on comparing the expected susceptibility of well known block ciphers to hypothetical algebraic attack.

In this paper, we introduce a modelling of generalized block cipher and try to solve using XSL with eliminating of obvious linear dependencies. And we count the number of monomials and equations so that verify their relationship and find the condition to XSL feasible. We conclude that the XSL is feasible if each system of linearized equations for every s-box is overdefined.

2. Modelling of a Generalized Block cipher

We consider a general block cipher $\mathcal{A}$ which uses N S-boxes and M linear and key addition parts for a whole cipher. We assume that each S-box S_i should be described into q_i quadratic equations with m_i monomials where $i = 1, 2, \cdots, N$ and each linear and key addition part L_j should be described into l_j linear equations contain l_j key variables where $j = 1, 2, \cdots, M$.
Then the sets of monomials and equations for S_i are defined as follows.

$$X_i := \{x_{i,1}, x_{i,2}, \cdots, x_{i,m_i}\}, \quad |X_i| = m_i$$
$$F_i := \{f_{i,1}, f_{i,2}, \cdots, f_{i,q_i}\}, \quad |F_i| = q_i$$

where $i = 1, 2, \cdots, N$.

$x_{i,\bullet}$ is a monomial of degree 1 or 2 and X_i is the set of monomials in description of i-th S-box S_i. $f_{i,\bullet}$ is a quadratic equation with monomials in X_i and F_i is the set of quadratic equation in description of i-th S-box S_i.

And the sets of monomials and equations for L_j are defined as follows.

$$K_j := \{k_{j,1}, k_{j,2}, \cdots, x_{j,l_j}\}, \quad |K_j| = l_j$$
$$G_j := \{g_{j,1}, g_{j,2}, \cdots, g_{j,l_j}\}, \quad |G_j| = l_j$$

where $j = 1, 2, \cdots, M$.

$k_{j,\bullet}$ is a key variable and the K_j is a set of key variables in description of j-th linear and key addition part L_j. $g_{j,\bullet}$ is a linear equation with monomials in $(\cup_{i=1}^{n} X_i) \cup K_j$ and G_j is the set of linear equations in description of j-th linear and key addition part L_j.

Then, total number of monomials is

$$\begin{aligned} & m_1 + m_2 + \cdots + m_N + l_1 + l_2 + \cdots + l_M \\ &= \sum_{i=1}^{N} m_i + \sum_{j=1}^{M} l_j \end{aligned}$$

and total number of equations is

$$\begin{aligned} & q_1 + q_2 + \cdots + q_N + l_1 + l_2 + \cdots + l_M \\ &= \sum_{i=1}^{n} q_i + \sum_{j=1}^{m} l_j \end{aligned}$$

3. Using XSL to solve the system

Although a system of quadratic equations is overdefined, the linearized system of this equations can be underdefined. So, we generate new equations by multiplication of equations and monomials until the number of equations exceeds the number of monomials. That is XSL [2]. Courtois and Pieprzyk generate some new equations by multiplication of selected monomials and equations in their XSL simulation for the Toy Cipher in [2]. But there are obvious linear dependencies because the multiple of two equations are the linear combination of equations generated by multiplication of equations and monomials contained two equations. i.e.

The system

$$A + B = 0$$
$$C + D = 0$$

is extended to

$$A + B = 0$$
$$C + D = 0$$
$$AC + BC = 0 \tag{1}$$
$$AD + BD = 0 \tag{2}$$
$$AC + AD + BC + BD = 0 \tag{3}$$

But obviously (3)=(1)+(2). So we apply the XSL to our generalized block cipher $\mathcal{A}$ with eliminating such a obvious linear dependencies, count the number of equations and monomials and verify their relationship.

4. Extended system without redundancy

The initial system are as follows.

$$F_1, F_2, \cdots, F_N, \qquad G_1, G_2, \cdots, G_M$$

We generate new equations by multiplying of equations and monomials and adding them to the initial system. i.e.

$$y \cdot F_i := \{y \cdot f_{i,1}, y \cdot f_{i,2}, \cdots, y \cdot f_{i,q_i}\} \quad \forall y \in (\cup_{i'=i+1}^{N} X_{i'}) \cup (\cup_{j=1}^{M} K_j)$$

$$z \cdot G_j := \{z \cdot g_{j,1}, z \cdot g_{j,2}, \cdots, z \cdot g_{j,l_j}\} \quad \forall z \in (\cup_{j'=j+1}^{M} K_{j'})$$

$$\text{where} \quad i = 1, 2, \cdots, N \quad \text{and} \quad j = 1, 2, \cdots, M.$$

The number of monomials in extended system are calculated as follows;

$$\begin{aligned} & m_1 \cdot (m_2 + \cdots + m_N + l_1 + \cdots + l_M) + m_2 \cdot (m_3 + \cdots + i_N + l_1 + \cdots + l_M) \\ & + \cdots + m_{N-1} \cdot (m_N + l_1 + \cdots + l_M) + m_N \cdot (l_1 + \cdots + l_M) + l_1 \cdot (l_2 + \cdots + l_M) \\ & + l_2 \cdot (l_3 + \cdots + l_M) + \cdots + l_{M-1} \cdot l_M \\ & + (m_1 + m_2 + \cdots + m_N) + (l_1 + l_2 + \cdots + l_M) \\ & = \sum_{i=1}^{N} m_i (\sum_{i'=i+1}^{N} m_{i'} + \sum_{j=1}^{M} l_j) + \sum_{j=1}^{M} l_j \cdot (\sum_{j'=j+1}^{M} l_{j'}) + \sum_{i=1}^{N} m_i + \sum_{j=1}^{M} l_j \end{aligned} \tag{4}$$

And the number of equations in extended system are calculated as follows;

$$q_1 \cdot (m_2 + \cdots + m_N + l_1 + \cdots + l_M) + q_2 \cdot (m_3 + \cdots + m_N + l_1 + \cdots + l_M)$$

$$+ \cdots + q_{N-1} \cdot (m_N + l_1 + \cdots + l_M) + q_N \cdot (l_1 + \cdots + l_M) + l_1 \cdot (l_2 + \cdots + l_M)$$

$$+ l_2 \cdot (l_3 + \cdots + l_M) + \cdots + l_{M-1} \cdot l_M$$

$$+ (q_1 + q_2 + \cdots + q_N) + (l_1 + l_2 + \cdots + l_M)$$

$$= \sum_{i=1}^{N} q_i \Big(\sum_{i'=i+1}^{N} m_{i'} + \sum_{j=1}^{M} l_j \Big) + \sum_{j=1}^{M} l_j \cdot \Big(\sum_{j'=j+1}^{M} l_{j'} \Big) + \sum_{i=1}^{N} q_i + \sum_{j=1}^{M} l_j \tag{5}$$

An example can be found in Appendix A.

5. Feasibility for XSL

In Section 4, we get two equations (4) and (5) about the number of monomial and equation. So we are going to calculate the difference between (4) and (5).

Let D =(5)−(4). Then

$$\begin{aligned}
D &= \sum_{i=1}^{N} q_i \Big(\sum_{i'=i+1}^{N} m_{i'} + \sum_{j=1}^{M} l_j \Big) + \sum_{j=1}^{M} l_j \cdot \Big(\sum_{j'=j+1}^{M} l_{j'} \Big) + \sum_{i=1}^{N} q_i + \sum_{j=1}^{M} l_j \\
&\quad - \Big[\sum_{i=1}^{N} m_i \Big(\sum_{i'=i+1}^{N} m_{i'} + \sum_{j=1}^{M} l_j \Big) + \sum_{j=1}^{M} l_j \cdot \Big(\sum_{j'=j+1}^{M} l_{j'} \Big) + \sum_{i=1}^{N} m_i + \sum_{j=1}^{M} l_j \Big] \\
&= \sum_{i=1}^{N} (q_i - m_i) \Big(\sum_{i'=i+1}^{N} m_{i'} + \sum_{j=1}^{M} l_j \Big) + \sum_{i=1}^{N} (q_i - m_i) \\
&= \sum_{i=1}^{N} (q_i - m_i) \Big(\sum_{i'=i+1}^{N} m_{i'} + \sum_{j=1}^{M} l_j + 1 \Big)
\end{aligned}$$

If $q_i - m_i < 0$ for all $i = 1, 2, \cdots, N$, then $D < 0$. This means that the number of monomials is greater than the number of equations for each S-box. Therefore we conclude that if each linearized system of equation for S-boxes(after applying the Linearization method for a initial quadratic system of equations for S-box) is underdefined, then XSL can not find the unique solution for the system of equation.

We show whether the XSL for Toy cipher [2] and AES is feasible or not.

- Toy cipher(2-round version)
  Toy cipher uses 4 S-boxes but they are the same. By the simulation, the system of equation is consisted with 19 monomials and 14 quadratic equations [2]. $m_i = 19 > 14 = q_i$ for all $i = 1, 2, 3, 4$. So $D < 0$. Therefore the extension of XSL may not make it overdefined.

- AES
  AES(128) uses 160 S-boxes but they are the same too. We know that there are at least 24 quadratic equations for the AES S-box [2]. It is easy to find the equation have more monomials than the 24. Since the system of linearized equation for AES S-box is underdefined, therefore the XSL may not work with the 24 equations. If we find more equations which is linearly independent with the 24 equations above, then there are some possibility to make the system overdefined. But the complexity is still a obstacle to overcome.

6. Conclusion

We generalize a block cipher and calculate the numbers of monomials and equations of extended system of equations under some assumption about initial system of equations. In Section 5, we define D by subtraction of that two numbers as a parameter to decide whether XSL is feasible or not. If $D < 0$ then XSL fail since the extended system is underdefined. One of sufficient condition of $D < 0$ is that each system of linearized equations for every S-box is underdefined. So a block cipher using S-boxes which should not be described a overdefined system of linearlized equation is secure against the algebraic attack with XSL algorithms. Conversely if we find more quadratic equations than monomials for each S-box, then XSL works well for the block cipher using the S-box. However, the complexity of XSL is still a obstacle to overcome even if XSL is feasible.

References

[1] N. Coutois, A. Klimov, J. Partarin and A. Shamir, "Efficient algorithms for solving overdefined systems of multivariate polynomial equations,". in Proceedings of Eurocrypt'00(B. Preneel, ed.), n0. 1807 in Lecture Notes in Computer Science, pp. 392-407, Springer-Verlag, 2000.

[2] N. Coutois and J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of equations,". in Proceedings of Asiacrypt'02(Y. Zheng, ed.), n0. 2501 in Lecture Notes in Computer Science, Springer-Verlag, 2002. Earlier version available from `http://www.iacr.org`.

[3] A. Biryukov, C. De Cannière, "Block ciphers and systems of quadratic equations,". in Proceedings of FSE'03(Thomas Johansson, ed.), n0. 2887 in Lecture Notes in Computer Science, pp. 274 - 289, Springer-Verlag, 2003.

Appendix A. Example

The following example is just for showing how the extension works. Let the initial system of quadratic equations be as follows($N = 2, M = 1$).

$$X_1 := \{x_{13}, x_{14}, x_{11}x_{12}, x_{12}x_{13}\} \qquad |X_1| = m_1 = 4$$

$$F_1(X_1) := \begin{cases} f_{11}(X_1) = x_{11}x_{12} + x_{13} + x_{14} = 0 \\ f_{12}(X_1) = x_{12}x_{13} + x_{13} + x_{14} = 0 \end{cases} \qquad |F_1(X_1)| = q_1 = 2$$

$$X_2 := \{x_{21}, x_{23}, x_{24}, x_{22}x_{23}, x_{23}x_{24}\} \qquad |X_2| = m_2 = 5$$

$$F_2(X_2) := \begin{cases} f_{21}(X_2) = x_{22}x_{23} + x_{23}x_{24} + x_{21} + 1 = 0 \\ f_{22}(X_2) = x_{21} + x_{23} + x_{24} = 0 \end{cases} \qquad |F_2(X_2)| = q_2 = 2$$

$$K_1 := \{k_{11}, k_{12}\} \qquad |K_1| = l_1 = 2$$

$$G_1(\bullet,\bullet,K_1) := \begin{cases} g_{11}(\bullet,\bullet,K_1) = k_{11} + x_{13} + x_{23} + x_{14} = 0 \\ g_{12}(\bullet,\bullet,K_1) = k_{12} + x_{23} + x_{24} + x_{12} = 0 \end{cases} \qquad |G_1(\bullet,\bullet,K_1)| = l_1 = 2$$

Then the extended system is as follows;

$$F_1(X_1) := \begin{cases} f_{11}(X_1) = x_{11}x_{12} + x_{13} + x_{14} = 0 \\ f_{12}(X_1) = x_{11}x_{12} + x_{13} + x_{14} = 0 \end{cases}$$

$$x_{21} \cdot F_1(X_1) := \begin{cases} x_{21} \cdot f_{11}(X_1) = x_{21}x_{11}x_{12} + x_{21}x_{13} + x_{21}x_{14} = 0 \\ x_{21} \cdot f_{12}(X_1) = x_{21}x_{12}x_{13} + x_{21}x_{13} + x_{21}x_{14} = 0 \end{cases}$$

$$x_{23} \cdot F_1(X_1) := \begin{cases} x_{23} \cdot f_{11}(X_1) = x_{23}x_{11}x_{12} + x_{23}x_{13} + x_{23}x_{14} = 0 \\ x_{23} \cdot f_{12}(X_1) = x_{23}x_{12}x_{13} + x_{23}x_{13} + x_{23}x_{14} = 0 \end{cases}$$

$$x_{24} \cdot F_1(X_1) := \begin{cases} x_{24} \cdot f_{11}(X_1) = x_{24}x_{11}x_{12} + x_{24}x_{13} + x_{24}x_{14} = 0 \\ x_{24} \cdot f_{12}(X_1) = x_{24}x_{12}x_{13} + x_{24}x_{13} + x_{24}x_{14} = 0 \end{cases}$$

$$x_{22}x_{23} \cdot F_1(X_1) := \begin{cases} x_{22}x_{23} \cdot f_{11}(X_1) = x_{22}x_{23}x_{11}x_{12} + x_{22}x_{23}x_{13} + x_{22}x_{23}x_{14} = 0 \\ x_{22}x_{23} \cdot f_{12}(X_1) = x_{22}x_{23}x_{12}x_{13} + x_{22}x_{23}x_{13} + x_{22}x_{23}x_{14} = 0 \end{cases}$$

$$x_{23}x_{24} \cdot F_1(X_1) := \begin{cases} x_{23}x_{24} \cdot f_{11}(X_1) = x_{23}x_{24}x_{11}x_{12} + x_{23}x_{24}x_{13} + x_{23}x_{24}x_{14} = 0 \\ x_{23}x_{24} \cdot f_{12}(X_1) = x_{23}x_{24}x_{12}x_{13} + x_{23}x_{24}x_{13} + x_{23}x_{24}x_{14} = 0 \end{cases}$$

$$k_{11} \cdot F_1(X_1) := \begin{cases} k_{11} \cdot f_{11}(X_1) = k_{11}x_{11}x_{12} + k_{11}x_{13} + k_{11}x_{14} = 0 \\ k_{11} \cdot f_{12}(X_1) = k_{11}x_{12}x_{13} + k_{11}x_{13} + k_{11}x_{14} = 0 \end{cases}$$

$$k_{12} \cdot F_1(X_1) := \begin{cases} k_{12} \cdot f_{11}(X_1) = k_{12}x_{11}x_{12} + k_{12}x_{13} + k_{12}x_{14} = 0 \\ k_{12} \cdot f_{12}(X_1) = k_{12}x_{12}x_{13} + k_{12}x_{13} + k_{12}x_{14} = 0 \end{cases}$$

$$F_2(X_2) := \begin{cases} f_{21}(X_2) = x_{22}x_{23} + x_{23}x_{24} + x_{21} + 1 = 0 \\ f_{22}(X_2) = x_{21} + x_{23} + x_{24} = 0 \end{cases}$$

$$k_{11} \cdot F_2(X_2) := \begin{cases} k_{11} \cdot f_{21}(X_2) = k_{11}x_{22}x_{23} + k_{11}x_{23}x_{24} + k_{11}x_{21} + 1 = 0 \\ k_{11} \cdot f_{22}(X_2) = k_{11}x_{21} + k_{11}x_{23} + k_{11}x_{24} = 0 \end{cases}$$

$$k_{12} \cdot F_2(X_2) := \begin{cases} k_{12} \cdot f_{21}(X_2) = k_{12}x_{22}x_{23} + k_{12}x_{23}x_{24} + k_{12}x_{21} + 1 = 0 \\ k_{12} \cdot f_{22}(X_2) = k_{12}x_{21} + k_{12}x_{23} + k_{12}x_{24} = 0 \end{cases}$$

$$\begin{aligned}
&|X_1| = |\{x_{13}, x_{14}, x_{11}x_{12}, x_{12}x_{13}\}| = 4 \\
&|x_{21} \cdot X_1| = |\{x_{21}x_{13}, x_{21}x_{14}, x_{21}x_{11}x_{12}, x_{21}x_{12}x_{13}\}| = 4 \\
&|x_{23} \cdot X_1| = |\{x_{23}x_{13}, x_{23}x_{14}, x_{23}x_{11}x_{12}, x_{23}x_{12}x_{13}\}| = 4 \\
&|x_{24} \cdot X_1| = |\{x_{24}x_{13}, x_{24}x_{14}, x_{24}x_{11}x_{12}, x_{24}x_{12}x_{13}\}| = 4 \\
&|x_{22}x_{23} \cdot X_1| = |\{x_{22}x_{23}x_{13}, x_{22}x_{23}x_{14}, x_{22}x_{23}x_{11}x_{12}, x_{22}x_{23}x_{12}x_{13}\}| = 4 \\
&|x_{23}x_{24} \cdot X_1| = |\{x_{23}x_{24}x_{13}, x_{23}x_{24}x_{14}, x_{23}x_{24}x_{11}x_{12}, x_{23}x_{24}x_{12}x_{13}\}| = 4 \\
&|k_{11} \cdot X_1| = |\{k_{11}x_{13}, k_{11}x_{14}, k_{11}x_{11}x_{12}, k_{11}x_{12}x_{13}\}| = 4 \\
&|k_{12} \cdot X_1| = |\{k_{12}x_{13}, k_{12}x_{14}, k_{12}x_{11}x_{12}, k_{12}x_{12}x_{13}\}| = 4 \\
&|X_2| = |\{x_{21}, x_{23}, x_{24}, x_{22}x_{23}, x_{23}x_{24}\}| = 5 \\
&|k_{11} \cdot X_2| = |\{k_{11}x_{21}, k_{11}x_{23}, k_{11}x_{24}, k_{11}x_{22}x_{23}, k_{11}x_{23}x_{24}\}| = 5 \\
&|k_{12} \cdot X_2| = |\{k_{12}x_{21}, k_{12}x_{23}, k_{12}x_{24}, k_{12}x_{22}x_{23}, k_{12}x_{23}x_{24}\}| = 5 \\
&|K_1| = |\{k_{11}, k_{12}\}| = 2
\end{aligned}$$

So, the number of monomials in extended system is $4\cdot(5+2)+5\cdot 2+4+5+2 = 49$ and the number of equations in extended system is $2\cdot(5+2)+2\cdot 2+2+2+2 = 30$.

CAMP Lab. HanYang University 17 HaengDang-Dong SeongDong-Gu Seoul 133-791 Korea

E-mail address: {kidkoo, jhs1003}@ihanyang.ac.kr

E-mail address: camp123@hanyang.ac.kr