SCIENCE CHINA
Information Sciences

• LETTER •

September 2016, Vol. 59 099104:1–099104:3
doi: 10.1007/s11432-015-0345-0

Algebraic techniques in slender-set differential cryptanalysis of PRESENT-like cipher

Guo-Qiang LIU[1,2]* & Chen-Hui JIN[2]

[1] *Department of Mathematic and System Science, College of Science, National University of Defense Technology, Changsha* 410073*, China;*
[2] *Information Engineering University, Zhengzhou* 450000*, China*

Received September 15, 2015; accepted December 29, 2015; published online August 11, 2016

Citation Liu G-Q, Jin C-H. Algebraic techniques in slender-set differential cryptanalysis of PRESENT-like cipher. Sci China Inf Sci, 2016, 59(9): 099104, doi: 10.1007/s11432-015-0345-0

Dear editor,

Slender-set differential cryptanalysis, which is proposed by Borghoff et al. [1, 2], is an effective method of recovering the secret S-boxes of PRESENT-like cipher. And this differential method is improved by Liu et al. [3]. In [4], Courtois et al. proposed a novel algebraic cryptanalysis for block ciphers and stream ciphers. The algebraic attack requires only one or very few plaintext-ciphertext pairs. There are several algorithms for solving these equations, such as the Gröbner bases algorithms [5], the SAT solvers [1)], and Characteristic Set Algorithm [6].

In this letter, we focus on combining the algebraic technique with slender-set differential cryptanalysis of PRESENT-like cipher. Being different from Borghoff's original attack and Liu's improving attack, our attack makes use of the information from slender-pairs with weight one instead of the accurate partition of the slender-sets. Our contributions are twofold. First, for a slender-pair $\{x, y\}$, we investigate the algebraic properties from the perspective of the value $wt(S(x) \oplus S(y))$, and use them to set up the low degree multivariate system of equations. By solving the system of equations, we can recover the coordinate functions of the secret S-box. Second, we propose a filter method of detecting the wrong slender-sets and constructing the valid slender-sets for deriving the equations system. Our algebraic technique requires enough valid slender-pairs with weight one. However, to obtain the completely correct slender-sets requires more plaintext-ciphertext pairs. In order to reduce the data complexity, we construct the valid slender-pairs by using two filters, named the count filter and chain filter. In particular, we implemented a successful attack on the full round cipher Maya using Gröbner bases algorithms by Magma software.

Model and methodology. The diffusion layer in PRESENT-like cipher is designed as a bit-wise permutation (see Figure 1 and Algorithm A1 in Appendix A). To maximize diffusion, the output bits from the same S-box will map into four distinct S-boxes through the bit permutation. For one S-box, the weight of the output difference after the first S-box layer will determine the number of active S-boxes in the second round. That is to say, if the weight of output differential after the first S-box layer is equal to one, there must be one active S-box in the second round (see Figure 1, the active S-box denoted by white one). And the

* Corresponding author (email: liuguoqiang87@hotmail.com)

The authors declare that they have no conflict of interest.

[1)] Soos M. CryptoMiniSat—a SAT solver for cryptographic problems. http://planete.inrialpes.fr/∼soos/CryptoMiniSat2/index.php.

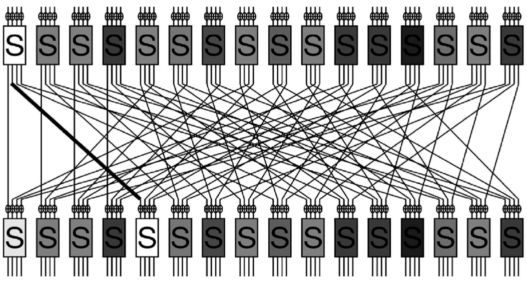

Figure 1 The differential path with weight one.

differential with weight two will case two active S-boxes in the next round (see Figure B1 in Appendix B).

This argument can be repeated for the following rounds. Hence, if the output of the first S-box layer has low weight difference, the characteristics through the whole cipher ending with a single active S-box will have the higher probability. In particular, weight-one differential is expected to have the highest probability. The basic idea of Borghoff's differential attack is to exploit which input pairs of the first S-box layer will lead to the low weight output differential after the first S-box layer by using the non-uniformity of output difference through the whole cipher.

Definition 1. [1,2] Given $e \in \mathbb{F}_2^m$ and $S : \mathbb{F}_2^m \to \mathbb{F}_2^m$, we denote the set of all pairs $\{x, y\}$ such that $S(x) \oplus S(y) = e$ by D_e. Here, we consider the pairs $\{x, y\}$ and $\{y, x\}$ to be identical. A pair $\{x, y\}$ belonging to a set D_e where e has Hamming weight '1' is called a slender-pair. A set consisting of slender-pairs is called a slender-set. We denote $wt_1(e)$ as the Hamming weight of e.

We attempt to derive the Boolean expressions the secret S-box as a set of low degree equations based on the differential information from the candidate slender-sets. First, we present the algebraic properties of output differences of coordinate functions of the S-box.

In one slender-set D_e, it holds that $e \in \{(0001)_2, (0010)_2, (0100)_2, (1000)_2\}$. In other words, we have $wt(e) = 1$. Let S-box $S : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ which is a bijective mapping. We denote $S(x) = (s_0(x), s_1(x), s_2(x), s_3(x))$. For every $0 \leqslant i < 4$, $s_i(x)$ is the i-th coordinate functions of the secret S-box $S(x)$. We present the sufficient and necessary condition for the slender-pair $\{x, y\}$ as the following theorem.

Theorem 1. Let S-box $S : \mathbb{F}_2^4 \to \mathbb{F}_2^4, x, y \in \mathbb{F}_2^4$, and $S(x) \oplus S(y) = e$. Then the sufficient and necessary condition of $wt(e) = 1$ is that

$$\begin{cases} s_0(x) \oplus s_0(y) \oplus s_1(x) \oplus s_1(y) \\ \oplus s_2(x) \oplus s_2(y) \oplus s_3(x) \oplus s_3(y) = 1; \\ (s_0(x) \oplus s_0(y))(s_1(x) \oplus s_1(y)) \\ \oplus (s_2(x) \oplus s_2(y))(s_3(x) \oplus s_3(y)) = 0. \end{cases}$$

According to Theorem 1, each slender-pair $\{x, y\}$ raises two equations which degrees are 1 and 2. Due to the secret S-box being a bijective mapping, for every $i \neq j$, we have $S(i) \neq S(j)$. That is $(s_0(i) \oplus s_0(j) \oplus 1) \cdot (s_1(i) \oplus s_1(j) \oplus 1) \cdot (s_2(i) \oplus s_2(j) \oplus 1) \cdot (s_3(i) \oplus s_3(j) \oplus 1) = 0$. Thus we have $C_{16}^2 = 120$ extra polynomials for extending the algebraic cryptanalysis as follows [2]:

$$\begin{cases} (s_0(0) \oplus s_0(1) \oplus 1) \cdot (s_1(0) \oplus s_1(1) \oplus 1) \\ \cdot (s_2(0) \oplus s_2(1) \oplus 1) \cdot (s_3(0) \oplus s_3(1) \oplus 1) = 0; \\ \qquad\qquad\qquad \vdots \\ (s_0(14) \oplus s_0(15) \oplus 1) \cdot (s_1(14) \oplus s_1(15) \oplus 1) \\ \cdot (s_2(14) \oplus s_2(15) \oplus 1) \cdot (s_3(14) \oplus s_3(15) \oplus 1) = 0. \end{cases}$$

By considering the entire 32 slender-pairs and the properties of bijective S-box, we have $64 + 120 = 184$ Boolean polynomials totally. There are 32 equations that are linear equations, 32 equations are nonlinear equations with degree '2', and 120 equations are nonlinear ones with degree '4' on the field $GF(2)$ (see Table C3 in Appendix C).

The valid pair $\{x, y\}$ for deriving the equations system should meet the condition $wt(S(x) \oplus S(y)) = 1$ in our algebraic techniques. The wrong equations will be constructed by these invalid pairs, which will cause incorrect secret S-box recovered. In this letter, we present a filter method of detecting the invalid pairs with low data complexity.

Let $\{x, y\} \in D_e$, because of the 4-bit S-box in PRESENT-like cipher being a bijective mapping, we have $\{x, z\} \notin D_e$. This means that each element will occur only once in one slender-set. Therefore, each element will occur four times in four slender-sets. In addition, given $\{x, y\} \in D_{e_1}$ and $\{y, z\} \in D_{e_2}$, we have $S(x) \oplus S(y) = e_1$ and $S(y) \oplus S(z) = e_2$. It must hold that $S(x) \oplus S(z) = e_1 \oplus e_2$. By using these two properties, the invalid pairs can be checked using the filtering methods described as follows.

Theorem 2. Let the set $\Omega \subset \{D_{e_1} \cup D_{e_2} \cup D_{e_3} \cup D_{e_4}\}$, where $wt(e_1) = wt(e_2) = wt(e_3) = wt(e_4) = 1$ and e_1, e_2, e_3, e_4 are distinct from each other. We have $N(x) = \#\{x : \{x, y\} \in \Omega\} \leqslant 4$. We call this filter the count filter.

Theorem 3. Given the slender-set D_{e_1}, D_{e_2}, where $wt(e_1) = wt(e_2) = 1$. Let $\{x, y\} \in D_{e_1}$

[2] Thank the anonymous reviewers for this useful improvements.

and $\{y, z\} \in D_{e_2}$. We have $wt(S(x) \oplus S(z)) \neq 1$. We call this filter the chain filter.

According to Theorem 2, for a pair $\{x, y\}$, if the value $N(x) > 4$ or $N(y) > 4$, we treat the pair $\{x, y\}$ as an invalid pair. According to Theorem 3, one can see that if the pairs $\{x, y\}$ and $\{y, z\}$ are valid pairs, the pair $\{x, z\}$ must be an invalid pair.

Now we describe the method of constructing the valid pairs with weight one by using the count filter and chain filter. We assume that the pairs at the top list would contain more differential information about the secret S-box. Let the set $\Omega = \emptyset$. We start with the first pair $\{x, y\}$ in the sorted list and add it into the set Ω. We check if the next pair $\{x, y\}$ passes the count filter and chain filter. If so, we consider this pair as a valid pair and add it to a collection of set Ω. We then look at the next pair and so forth. If not, we look at the next pair directly. We stop adding pairs when the number of elements of set Ω is equal to 32.

Experimental results. Slender-set attack is related with the differential properties of S-boxes. Throughout this section, the S-boxes in the PRESENT-like cipher are randomly generated.

In this section, we apply our attack against the PRESENT-like cipher. We use Gröbner basis algorithm by software Magma V2.20 [3)] to find the solutions of the equations system on IBM-System-x3650-m4 server (at Intel(R) Xeon(R) CPU E5-2667 V2 @ 3.30 GHz, RedHat Enterprise Linux 6.5). One possible solution for the equations system is listed by Table C1.

We have run experiments against 9 to 16 rounds PRESENT-like with randomly chosen S-boxes by using our attack based on 200 independent trials (see Table C2). Our attack can recover the secret S-box of full round (16 round) Maya with 2^{28} data complexity at a success rate of 100%. In [1, 2], Borghoff's attack can recover the secret S-boxes in versions up to 16-round cipher Maya with 2^{38} data complexity and 2^{38} time complexity successfully. To compare with the results of Borghoff's work, our algebraic technique can significantly reduce the data complexity from 2^{38} to 2^{28}. Compared with the improved slender-set differential cryptanalysis, the time complexity in our attack is much less than that of Liu's work in [3]. The average time consumption of solving the polynomials system is about 1 s.

Conclusion and future work. In this letter, we study the algebraic techniques in slender-set differential cryptanalysis on PRESENT-like cipher. We start with the algebraic properties from the perspective of the value of $wt(S(x) \oplus S(y))$ instead of the value of $S(x) \oplus S(y)$. Based on the slender-pairs, we build the low degree multivariate system equations, and use them to acquire the coordinate functions of the secret S-box. Furthermore, we present a method of constructing the valid slender-pairs by using two filters to reduce the data complexity. We run a practical attack to full round Maya. The experiments show that the correct S-box can be recovered with 2^{28} data complexity at a success rate of 100%. The time consumption is for about 1 s on a standard PC on average.

Our algebraic attack is a preliminary work and has some drawbacks. First of all, the filters for detecting the wrong slender-pairs are not strong enough with low data complexity. Secondly, the pairs $\{x, y\}$ with $wt(S(x) \oplus S(y)) \geqslant 2$ can be used in the algebraic cryptanalysis to reduce the data complexity. We leave it as a possible direction of future research.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61272488, 61402523), and Foundation of Science and Technology on Information Assurance Laboratory (Grant No. KJ-13-007).

Supporting information Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Borghoff J, Knudsen L, Leander G, et al. Cryptanalysis of PRESENT-like ciphers with secret S-boxes. Fast Softw Encryption, 2011, 6733: 270–289

2 Borghoff J, Knudsen L, Leander G, et al. Slender-set differential cryptanalysis. J Cryptol, 2013, 26: 11–38

3 Liu G-Q, Jin C-H. Differential cryptanalysis of PRESENT-like cipher. Design Code Cryptogr, 2015, 76: 385–408

4 Courtois N, Pieprzyk J. Cryptanalysis of block ciphers with overdefined systems of equations. In: Advances in Cryptology — ASIACRYPT 2002. Berlin: Springer, 2002. 267–287

5 Buchberger B. Gröbner-bases: an algorithmic method in polynomial ideal theory. In: Multidimensional Systems Theory. Dordrecht: Reidel Publishing Company, 1985. 184–232

6 Chai F, Gao X S, Yuan C. A characteristic set method for solving Boolean equations and applications in cryptanalysis of stream ciphers. J Syst Sci Complex, 2008, 21: 191–208

[3)] Magma. The Magma computational algebra system for algebra, number theory and geometry. http://magma.maths.usyd.edu.au/magma/.