

Cryptanalysis of Rijmen-Preneel Trapdoor Ciphers

Hongjun Wu* Feng Bao** Robert H. Deng** Qin-Zhong Ye*

*Department of Electrical Engineering
National University of Singapore
Singapore 119260

**Information Security Group
Kent Ridge Digital Labs
Singapore 119613

Abstract. Rijmen and Preneel recently proposed for the first time a family of trapdoor block ciphers [8]. In this family of ciphers, a trapdoor is hidden in S-boxes and is claimed to be undetectable in [8] for properly chosen parameters. Given the trapdoor, the secret key (used for encryption and decryption) can be recovered easily by applying Matsui's linear cryptanalysis [6].

In this paper, we break this family of trapdoor block ciphers by developing an attack on the S-boxes. We show how to find the trapdoor in the S-boxes and demonstrate that it is impossible to adjust the parameters of the S-boxes such that detecting the trapdoor is difficult meanwhile finding the secret key by trapdoor information is easy.

1 Introduction

In cryptography, design of secure trapdoor one-way functions has long been a challenging problem. Many previous proposals have been broken and the existing "secure" ones are mostly based on the few conjectures of hard problems in number theory.

Recently, Rijmen and Preneel proposed a family of trapdoor block ciphers [8] which we will call RP trapdoor ciphers. In such ciphers, a trapdoor is built into S-boxes. Knowledge of the trapdoor allows one to determine the correlation between output bits of the cipher's round function. This correlation is in turn used to find the secret key by performing Matsui's linear cryptanalysis on a small amount of known plaintexts [6]. In [8], it was claimed that the trapdoor with properly chosen parameters is undetectable and RP trapdoor ciphers may be used for public key encryption.

In this paper, we break RP trapdoor block ciphers by developing an attack on the trapdoor S-boxes. We first demonstrate that the trapdoor can be found from the S-boxes. We then show that RP trapdoor block ciphers can not be made secure by adjusting system parameters, since it is not possible for such ciphers to meet the following two contradicting requirements simultaneously: 1)

be resistance to our attack and, 2) be computationally efficient in finding the secret key using linear cryptanalysis once the trapdoor is known.

This paper is organized as follows. The trapdoor S-boxes and RP trapdoor ciphers are briefly reviewed in Section 2. In Section 3, we present our attack to RP trapdoor ciphers (more precisely, to the trapdoor S-boxes). In Section 4, we show that it is not possible to construct secure RP trapdoor ciphers by adjusting system parameters. We conclude the paper in Section 5.

2 RP Trapdoor Ciphers

RP trapdoor ciphers make use of the "type II" linear relations as defined in [7]: correlations that exist between output bits of a cipher's round function/S-boxes. Knowledge of the trapdoor reveals the correlations and allows linear cryptanalysis being carried out to determine the secret key from some known plaintexts.

2.1 Trapdoor $m \times n$ S-boxes

The trapdoor in RP trapdoor ciphers is built into S-boxes. An $m \times n$ S-box has m -dimensional and n -dimensional Boolean vectors as its inputs and outputs, respectively. It can be represented by 2^m n -dimensional Boolean vectors, i.e., $S = \{v_0, v_1, \dots, v_{2^m-1}\}$. For input $x \in \{0, 1, \dots, 2^m - 1\}$, the output of the S-box is defined as $S(x) = v_x$ where x can be treated as an m -dimensional vector. In the following, we denote the j th bit of v_i as $v_i[j]$. That is, $v_i = \langle v_i[1], v_i[2], \dots, v_i[n] \rangle$.

In a RP trapdoor cipher, the trapdoor $m \times n$ S-box is constructed as follows. First, choose a non-zero n -dimensional Boolean vector $\beta = \langle \beta[1], \beta[2], \dots, \beta[n] \rangle$ and let $\beta[q] = 1$. Then randomly choose the values of $v_i[j]$ for $i = 0, 1, \dots, 2^m - 1$ and $j = 1, \dots, q - 1, q + 1, \dots, n$. Finally, set the values of $v_i[q]$, $i = 0, 1, \dots, 2^m - 1$, such that

$$\beta[1]v_i[1] \oplus \dots \oplus \beta[q]v_i[q] \oplus \dots \oplus \beta[n]v_i[n] = v_i \cdot \beta = 0 \quad (1)$$

holds with probability p_T (which has a value very close to 1). Equation (1) is equivalent to a correlation

$$c_T = 2p_T - 1$$

between the constant zero function and $\beta \cdot S(x)$. The trapdoor is the Boolean vector β . It was claimed in [8] that finding β from published S-boxes is difficult for suitable parameters, say, $m = 10$, $n = 80$ and $p_T = 1 - 2^{-5}$. RP trapdoor ciphers are designed on this supposition.

2.2 Trapdoor Ciphers

RP trapdoor ciphers are based on the Feistel structure [4]. In a Feistel block cipher with $2n$ -bit block size and r rounds, plaintext and ciphertext consist of

two n -bit halves denoted as L_0, R_0 and L_r, R_r respectively. Each round operates as follows:

$$\begin{aligned} R_i &= L_{i-1} \oplus F(K_i \oplus R_{i-1}) \\ L_i &= R_{i-1} \end{aligned} \quad \text{for } i = 1, 2, \dots, r$$

where K_i is the i th round subkey and F is the round function. Note that after the last round, the swapping of the halves is undone to make encryption and decryption similar.

In [8], variants on both CAST [5] and LOKI91 [3] were studied. In this paper, we only consider trapdoor CAST ciphers since all the discussions here can be extended to trapdoor LOKI91 ciphers directly.

The CAST family of ciphers are 64-bit Feistel ciphers. Its round function F is based on four 8×32 S-boxes (i.e., for $m = 8, n = 32$), which have components that are either randomly chosen or are bent functions [1]. Mathematically, the round function is given by

$$F(x) = S_1(x_1) \oplus S_2(x_2) \oplus S_3(x_3) \oplus S_4(x_4)$$

where x , the 32-bit input, is the concatenation of 4 bytes $x = x_1 || x_2 || x_3 || x_4$ and where S_1, \dots, S_4 are four 8×32 S-boxes.

In a trapdoor CAST cipher, the four S-boxes use the same trapdoor β but possibly with different values of p_T , denoted as $p_T^{(1)}, \dots, p_T^{(4)}$. The following relation holds

$$\beta \cdot F(x) = \beta \cdot S_1(x_1) \oplus \beta \cdot S_2(x_2) \oplus \beta \cdot S_3(x_3) \oplus \beta \cdot S_4(x_4)$$

Hence the round function correlates with the constant zero function with a correlation equal to

$$c_F = \prod_{i=1}^4 c_T^{(i)}$$

It was stated in [8] that CAST should be extended in a natural way to a 128-bit block cipher by using 8×64 S-boxes. This, it claimed, will make the trapdoor undetectable. Unfortunately, this claim is false as we will show in the next section.

3 Attack on RP Trapdoor Ciphers

In this section, we show that the trapdoor in a RP trapdoor cipher can be found easily and directly from the S-boxes.

RP trapdoor ciphers as described in the last section has $l = \frac{n}{m}$ S-boxes, each consisting of 2^m n -dimensional Boolean vectors. By way of their construction as presented in Section 2.1, we know that vectors in S-boxes are randomly chosen; therefore, the total number of distinguishing vectors in the l S-boxes, denoted by N , should be very close to $l2^m$. We also know each S-box is associated with a probability $p_T^{(i)}$. Let

$$p_T = \frac{\sum_{i=1}^l p_T^{(i)}}{l}$$

denote the average of these probabilities.

Let all the N distinguishing vectors in the l S-boxes be denoted as $\{v_1, v_2, \dots, v_N\}$. From Section 2.1 we know that the trapdoor β satisfies

$$v_i \cdot \beta = 0$$

for $i = 1, 2, \dots, N$ with probability p_T . Hence, the problem of finding the trapdoor is to find a β such that

$$\begin{pmatrix} v_1[1] & v_1[2] & \cdots & v_1[n] \\ v_2[1] & v_2[2] & \cdots & v_2[n] \\ \vdots & \vdots & \ddots & \vdots \\ v_N[1] & v_N[2] & \cdots & v_N[n] \end{pmatrix} \begin{pmatrix} \beta[1] \\ \beta[2] \\ \vdots \\ \beta[n] \end{pmatrix} = \begin{pmatrix} \alpha[1] \\ \alpha[2] \\ \vdots \\ \alpha[N] \end{pmatrix} \quad (2)$$

for any Boolean vector $\alpha = \langle \alpha[1], \alpha[2], \dots, \alpha[N] \rangle$
of Hamming weight approximately equal to $N(1 - p_T)$

The following algorithm is used to determine the trapdoor β directly from the l S-boxes.

Algorithm 1.

Step 1. Choose n vectors, denoted as $v_{i_1}, v_{i_2}, \dots, v_{i_n}$, randomly from v_1, v_2, \dots, v_N .

Step 2. Solve the n equations for x_β :

$$v_{i_k} \cdot x_\beta = 0$$

for $k = 1, 2, \dots, n$

Step 3. If non-zero solutions do not exist, go to Step 1. If solutions, say $\beta_1, \beta_2, \dots, \beta_t$, are found, check whether they satisfy (2). If some β_j does satisfy (2), then it is the trapdoor β we are looking for; otherwise, go to Step 1.

Observations

1. If we happen to choose $v_{i_1}, v_{i_2}, \dots, v_{i_n}$ in Step 1 such that $v_{i_k} \cdot \beta = 0$ has non-zero solutions for $k = 1, 2, \dots, n$, then β must be among these solutions. By checking them one by one against (2), we can find this β .
2. If we can find another $\beta' (\neq \beta)$ also satisfying (2), this β' can also be used as trapdoor information in linear attack for finding the secret key.
3. Since $v_i \cdot \beta = 0$ with probability p_T , such “lucky choice” happens with probability about $(p_T)^n$. Hence, it is guaranteed to find a trapdoor with this probability. (The probability in fact should be $C_{Np_T}^n / C_N^n$. This number is very close to $(p_T)^n$ when N is much larger than n and p_T is close to 1. Here C_N^n denotes the number of ways of choosing n objects from N objects.)

4. The number of solutions t won't be very large. This is because the vectors of the S-boxes are randomly chosen except for one bit (at bit position q), therefore, the rank of the matrix in (2) is close to n with large probability.

Now let's look at a trapdoor CAST cipher with 128-bit block size ($n = 64$) and $p_T = 1 - 2^{-5}$ (this value of p_T was given in [8] as an example to illustrate the strength of the RP trapdoor cipher). The value of $(p_T)^n$ is about 0.1311. By repeating Steps 1 and 2 of the algorithm 32 times, we expect to get the value of β with probability 98.89%. This example shows clearly that RP trapdoor block ciphers are very vulnerable under our attack.

4 The Impossibility of Designing Secure RP Trapdoor Ciphers

In Section 3, we developed an attack to RP trapdoor ciphers. We demonstrated that the trapdoor can be determined easily from S-boxes. In this section, we show that it is impossible to design secure practical RP trapdoor ciphers.

We observe that there is a tradeoff between resisting our attack (i.e., Algorithm 1) and the effort required to find the secret key from trapdoor using linear cryptanalysis. This tradeoff can be adjusted by selecting system parameters r (number of rounds), m, n , and p_T . The smaller $(p_T - 0.5)$ is, the more difficult it is to succeed in Algorithm 1, but at the same time, the more difficult it is to find the secret key from the given trapdoor using linear cryptanalysis. Also, large values of m and n increases the computational complexity of Algorithm 1, as well as that of S-boxes. To simplify our notations and without loss of generality, in the following we assume that $p_T^{(1)} = p_T^{(2)} = \dots = p_T^{(t)}$.

Two basic requirements must be met in the design of a practical secure block cipher:

Requirement 1. The block cipher should be secure in the sense that it resists all the known attacks.

Requirement 2. The block cipher should be practical in the sense that the program size should not be too large.

To design a practical secure trapdoor cipher, two more requirements must be met:

Requirement 3. The trapdoor should be secure in the sense that it is hard to find the trapdoor even if its general form is known.

Requirement 4. The trapdoor should be practical in the sense that the secret key can be found easily once the trapdoor is given.

We now show that it is not possible to design a RP trapdoor cipher to satisfy the above four requirements simultaneously. We do this by showing that if a RP trapdoor cipher meets the first three requirements, then it can not meet the fourth requirement.

To satisfy the first requirement, the round number can not be too small. Thus, we expect that

$$r \geq 8 \quad (3)$$

To satisfy the second requirement, the total size of S-boxes is expected to be less than 128 Megabytes (i.e., 2^{30} bits). It is the same as to say that

$$\frac{n}{m}(n2^m) \leq 2^{30} \quad (4)$$

To satisfy the third requirement, we expect the following relation holds:

$$(p_T)^n \leq 2^{-64} \quad (5)$$

For a RP trapdoor cipher that **satisfies conditions (4), (5) and (6) simultaneously**, we evaluate the amount of known plaintexts required to carry out a successful linear cryptanalysis according to Matsui's algorithm 2 in [6]. The minimum numbers of plaintexts with respect to different value of m are listed in Table 1.

m	Number of plaintexts required	m	Number of plaintexts required
6	2^{175}	15	2^{74}
7	2^{150}	16	2^{70}
8	2^{132}	17	2^{67}
9	2^{118}	18	2^{65}
10	2^{107}	19	2^{64}
11	2^{97}	20	2^{65}
12	2^{90}	21	2^{78}
13	2^{84}	22	2^{126}
14	2^{78}	23	not exist since $p_T < 0.5$

Table 1. The number of known plaintexts required to carry out the linear cryptanalysis for a RP trapdoor cipher satisfying the first three requirements.

From table 1, we see that too many plaintexts are required to carried out the linear cryptanalysis based on knowledge of the trapdoor in order to discover the secret key. Although there may be some other methods to reduce the amount of known plaintexts (e.g., reducing the round number or increasing the size of S-boxes to a certain value), we believe that the number of known plaintexts required to carry out a successful linear cryptanalysis is still very large. Thus, we are forced to conclude that it is impossible to design practical secure RP trapdoor block ciphers.

5 Conclusions

Security of RP trapdoor block ciphers lies on the undetectability of a trapdoor built into S-boxes. It was claimed in [8] that it is hard to obtain the trapdoor from S-boxes and therefore RP trapdoor ciphers can be used for public key encryption. In this paper, we showed how to break such ciphers by finding the trapdoor directly from S-boxes. We demonstrated our attack to RP trapdoor ciphers based on "type II" linear relations.

In addition to trapdoors based on "type II" linear relations, trapdoors that make use of "type I" linear relations were also proposed in [8]. "Type I" linear relations are defined in [7] as the correlations between input and output bits of the round function. Unfortunately, this latter type of trapdoors is also vulnerable to our attack.

Other than hiding linear relations, another method proposed in [8] is to hide differentials into block ciphers in order to make them vulnerable to differential cryptanalysis [2]. However, construction of this kind of trapdoors was not given in [8] and it seems that hiding differentials is more difficult than hiding linear relations. So far, trapdoors based on hiding differentials remains an open problem

References

1. C.M. Adams, S.E. Tavares, "Designing S-boxes for ciphers resistant to differential cryptanalysis", Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, W. Wolkowicz, Ed., Fondazione Ugo Bordoni, 1993, pp. 181-190.
2. E. Biham, A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.
3. L. Brown, M. Kwan, J. Pieprzyk, J. Seberry, "Improving resistance against differential cryptanalysis and the redesign of LOKI", Advances in Cryptology, Proceedings Asiacrypt'91, LNCS 739, H. Imai, R. L. Rivest, and T. Matsumoto, Eds., Springer-Verlag, 1993, pp. 36-50.
4. H. Feistel, W.A. Notz, J.L. Smith, "Some cryptographic techniques for machine-to-machine data communications", Proceedings IEEE, Vol. 63, No. 11, November 1975, pp. 1545-1554.
5. H.M. Heys, S.E. Tavares, "On the security of the CAST encryption algorithm", Canadian Conference on Electrical and Computer Engineering, pp. 332-335, Sept. 1994, Halifax, Canada.
6. M. Matsui, "Linear cryptanalysis method for DES cipher", Advances in Cryptology, Proceedings Eurocrypt'93, LNCS 765, T. Helleseht, Ed., Springer-Verlag, 1994, pp. 386-397.
7. M. Matsui, "On correlation between the order of S-boxes and the strength of DES", Advances in Cryptology, Proceedings Eurocrypt'94, LNCS 950, A. De Santis, Ed., Springer-Verlag, 1995, pp. 366-375.
8. V. Rijmen, B. Preneel, "A family of trapdoor ciphers", Fast Software Encryption, LNCS 1267, E. Biham ed., Springer-Verlag, 1997, pp. 139-148.

This article was processed using the \LaTeX macro package with LLNCS style