Cryptanalysis of Strengthened Magenta

Orhun KARA

***Abstract*—In this paper we mount a reflection attack on a modified version of Magenta. Magenta was one of the block ciphers submitted for the AES contest. Indeed, Magenta has been already broken during the AES contest and hence has been disqualified. We first strengthen Magenta by double encryption and by adding two more rounds. We call this new cipher as MagentaP2. We claim that MagentaP2 is strong against any attack including the attack mounted on Magenta, except refection type attacks.**

One prevalent adoption in crypto community is that increasing the number of rounds of a block cipher enhances the security level. In fact, we give a counter example against this adoption. Magenta stands well against reflection attacks whereas MagentaP2 is vulnerable to reflection attacks even though its number of rounds is more than twice the number of original Magenta. The workloads of our attack are 2^{65}, 2^{131} and 2^{196} encryptions with at most 2^{66} known plaintexts for 128-bit, 192-bit and 256-bit key lengths, respectively.

***Keywords* —Block Cipher, Round Function, Round Key, Key Schedule, Cryptanalysis, Self-similarity.**

I. Introduction

In this paper we mount a reflection attack on a fortified version of Magenta by means of increasing its round numbers and double encryption. The reflection attack is a new type of self-similarity attack and the attack idea has been first appeared in [13]. The first applications with extensions have been presented in FSE 2007 [14] and in INDOCRYPT 2008 [12].

Apart from reflection attacks, there are two more generic attack types exploiting some degree of self-similarity among round functions: One of them is the slide attack [5], [6]. The typical slide attack can be applied if the sequence of round keys has a short period. The other attack type is the related-key attacks proposed by Biham [1]. Unlike slide attacks and related-key attacks, reflection attack exploits similarities of some round functions of encryption process with those of decryption. This is the main difference from the previous self-similarity attacks, which exploit the similarities among round functions only in encryption process. Consequently, some ciphers resistant to related-key attacks or slide attacks can be vulnerable to reflection attacks.

Magenta was one of the candidate algorithm for AES during NIST-AES contest and has been broken immediately after the commencement of the contest [2]. The major pitfall of the algorithm was not a weakness of the round function but was its extremely simple key-schedule algorithm. We strengthen Magenta by double encryption and by adding two more rounds in order to foil the attack in [2]. It is also interesting that slide attacks and related-key attacks are probably not applicable to the strengthened version. On the other hand, we mount a reflection attack on the strengthened version.

It is quite unusual that increasing the number of rounds may cause weaknesses in terms of reflection analysis in some cases. Magenta is strong against reflection analysis. However, reflection attack works quite well on MagentaP2, having more rounds. The attack exploits extremely large number of the fixed points produced by the encryption function of Magenta. The workloads are 2^{65}, 2^{131} and 2^{196} encryptions with at most 2^{66} known plaintexts for 128-bit, 192-bit and 256-bit key lengths, respectively.

Organization. We give a brief description of the algorithm Magenta in section II and then describe the modified version MagentaP2 in the forthcoming section. After giving preliminary results for the attack in Section IV, we explain the attack in Section V. Then, we conclude the paper.

II. A Brief Description of Magenta

Magenta is a block cipher submitted for the AES contest by Deutsche Telekom AG [10]. It is a Feistel cipher with 128 bit block size and 128, 192 or 256 bit key sizes. In this section we give a high level description of Magenta and construct a distinguisher for the whole cipher. This distinguisher does not assist key recovering. We modify Magenta and call it MagentaP2 (meaning Magenta Plus 2). MagentaP2 is double encryption of Magenta plus two more rounds. The modified Magenta is expected to be more secure than Magenta against most of the attack methods including the attack in [2] on Magenta. However, it is surprising that MagentaP2 is weaker than Magenta itself in terms of reflection attacks.

We give a short description of Magenta. We do not enter into details of round function since we do not exploit it in cryptanalysis. Magenta is a Feistel network where the last swap operation is included unlike DES. When the key length of Magenta is of 128, 192 or 256 bits then it is divided into two, three or four equal parts as (K_1, K_2), (K_1, K_2, K_3) or (K_1, K_2, K_3, K_4), respectively. The encryption functions are

$$E_K = \begin{cases} F^2_{K_1} F^2_{K_2} F^2_{K_1} & \text{if key size is 128,} \\ F_{K_1} F_{K_2} F^2_{K_3} F_{K_2} F_{K_1} & \text{if key size is 192,} \\ F_{K_1} F_{K_2} F_{K_3} F^2_{K_4} F_{K_3} F_{K_2} F_{K_1} & \text{if key size is 256.} \end{cases}$$

The author is supported in part by the European Commission through the project FP-7 ICE under the project grant number 206546.

O. KARA , TÜBİTAK UEKAE
National Research Institute of Electronics and Cryptology, Gebze 41470
Kocaeli/Turkey, orhun@uekae.tubitak.gov.tr

Each round function F_{K_i} is defined as

$$\begin{aligned} F_{K_i} : GF(2)^{128} &\longrightarrow GF(2)^{128} \\ F_{K_i}(x,y) &= (y, R_{K_i}(y) \oplus x) \end{aligned} \qquad (1)$$

where $\oplus$ is the "XOR" operation.

Magenta was cryptanalyzed during the AES conferences by Biham *et. al.* [2] and hence eliminated. The attack is a divide and conquer type attack. One can extract the outer keys, independently from the inner key. The complexity is $2^{m_k - 31}$ encryptions for a known plaintext attack where m_k is the key length.

III. Description of MagentaP2

The modified Magenta, which we call MagentaP2, is a double encryption of Magenta including two more rounds. Let $E_K^{(M)}$ and $E_K^{(MP2)}$ denote the encryption functions of Magenta and MagentaP2, respectively. Then, MagentaP2 encryption is defined as

$$E_K^{(MP2)}(x) = F_{(K_t \lll_m)} E_K^{(M)} E_K^{(M)} F_{K_t}(x) \qquad (2)$$

where F is the round function of Magenta and

$$K_t = \begin{cases} K_2 & \text{if key size is 128,} \\ K_2 \oplus K_3 & \text{if key size is 192,} \\ K_2 \oplus K_3 \oplus K_4 & \text{if key size is 256.} \end{cases}$$

$\lll_m$ is cyclic rotation to left by m bits where m can be chosen any positive integer less than 64. The new cipher depends on m, but we call all the ciphers simply as "MagentaP2" by abuse of terminology.

IV. Preliminary Work for the Attack

We give a general framework of the reflection attack on Feistel networks as a preliminary section for the next section where the attack is described. The extensions of the statements in this section can be found in [12].

Let a plaintext $x \in GF(2)^n$ be given as $x = (x_0, x_1); x_0, x_1 \in GF(2)^{n/2}$. The Feistel structure can be stated as a recursive function defined as $x_i = R_{k_{i-1}}(x_{i-1}) \oplus x_{i-2}$ with the initial conditions given by $x = (x_0, x_1)$. The function $R : GF(2)^{n/2} \to GF(2)^{n/2}$ is the encryption function. The i-th round operation is defined as

$$(x_i, x_{i+1}) = F_{k_i}(x_{i-1}, x_i) = (x_i, R_{k_i}(x_i) \oplus x_{i-1}) \qquad (3)$$

for $i \leq r$. In general, the swap operation is excluded in the last round and (x_{r+1}, x_r) is the corresponding ciphertext. With some abuse of terminology, R is also called the round function. We call the stream $x_0, x_1, ..., x_r, x_{r+1}$ the *encryption stream* of $x = (x_0, x_1)$ with respect to K.

Proposition 1: For a given natural number $m < r$, assume that $k_{m-i} = k_{m+i}$, $\forall i : 1 \leq i \leq \min\{r-m, m-1\}$. Let $x = (x_0, x_1)$ be encrypted and $x_0, x_1, ..., x_r, x_{r+1}$ be its encryption stream. If $R_{k_m}(x_m) = 0$, then $x_{m-i} = x_{m+i}$, $\forall i : 1 \leq i \leq \min\{r-m, m-1\}$. Conversely, if $x_{m-i} = x_{m+i}$ and $x_{m-i+1} = x_{m+i-1}$ for some i, then $R_{k_m}(x_m) = 0$.

Proposition 1 has already been known during the studies on cycle structures of DES (see [8], [19]). Hence, the notion of the fixed points of the weak keys of DES is well known. However, the studies were focused on algebraic properties of DES permutations and their short cycles rather than developing a key recovery attack [8], [19], [11], [18]. The following corollary points out the opposite direction of this old phenomenon.

Corollary 1: Assume that each round key k_i determines a round function R_{k_i} randomly. Let $x = (x_0, x_1)$ be encrypted and $x_0, x_1, ..., x_r, x_{r+1}$ be its encryption stream. Assume that the round number r is even, $r = 2r' > 4$, and $k_{r'-i} = k_{r'+i}$ $\forall i : 1 \leq i < r'$. Let $s_{r'}$ be the cardinality of the pre-image set, $R_{k_{r'}}^{-1}(0)$. Then, $\Pr(x_0 = x_r) = 2^{-\frac{n}{2}}(s_{r'} + 1 - 2^{-\frac{n}{2}} \cdot s_{r'})$ and

$$\Pr(R_{k_{r'}}(x_{r'}) = 0 \,|\, x_0 = x_r) = \frac{s_{r'}}{s_{r'} + 1 - 2^{-\frac{n}{2}} \cdot s_{r'}}.$$

Proof: Assume that the round function is random. Then, the probability that $x_0 = x_r$ is given as

$$\begin{aligned} \Pr(x_0 = x_r) = s_{r'} \cdot 2^{-n/2} &+ 2^{-n/2}(1 - s_{r'} \cdot 2^{-n/2}) \\ &= 2^{-\frac{n}{2}}(s_{r'} + 1 - s_{r'} \cdot 2^{-\frac{n}{2}}) \end{aligned}$$

since it is equal to

$$\begin{aligned} \Pr(x_0 = x_r \,|\, R_{k_{r'}}(x_{r'}) &= 0) \Pr(R_{k_{r'}}(x_{r'}) = 0) + \\ \Pr(x_0 = x_r \,|\, R_{k_{r'}}(x_{r'}) &\neq 0) \Pr(R_{k_{r'}}(x_{r'}) \neq 0). \end{aligned}$$

Note that $\Pr(x_0 = x_r \,|\, R_{k_{r'}}(x_{r'}) \neq 0) = 2^{-n/2}$ since $r > 4$. On the other hand, $\Pr(x_0 = x_r \,|\, R_{k_{r'}}(x_{r'}) = 0) = 1$ by Proposition 1. Hence, we conclude that

$$\begin{aligned} &\Pr(R_{k_{r'}}(x_{r'}) = 0 \,|\, x_0 = x_r) = \\ &\frac{\Pr(x_0 = x_r \,|\, R_{k_{r'}}(x_{r'}) = 0) \cdot \Pr(R_{k_{r'}}(x_{r'}) = 0)}{\Pr(x_0 = x_r)} \\ = \; &\frac{s_{r'}}{s_{r'} + 1 - 2^{-\frac{n}{2}} \cdot s_{r'}}. \end{aligned}$$

■

The following theorem illustrates the property exploited to mount an attack on a Feistel network with palindromic round keys.

Theorem 1: Assumptions are as in Corollary 1. Then the equality $x_0 = x_r$ implies that the equation

$$x_1 = R_{k_r}(x_r) \oplus x_{r+1}. \qquad (4)$$

is true with probability

$$\frac{s_{r'}}{s_{r'} + 1 - 2^{-\frac{n}{2}} \cdot s_{r'}}.$$

Proof: Assume that $x_0 = x_r$. Then by Corollary 1, we have $R_{k_{r'}}(x_{r'}) = 0$ with probability

$$\frac{s_{r'}}{s_{r'} + 1 - 2^{-\frac{n}{2}} \cdot s_{r'}}.$$

Thus the equality $x_1 = x_{r-1}$ is true with probability

$$\frac{s_{r'}}{s_{r'} + 1 - 2^{-\frac{n}{2}} \cdot s_{r'}}$$

by Proposition 1. On the other hand $x_{r+1} = R_{k_r}(x_r) \oplus x_{r-1}$. Thus, the probability that $x_1 = R_{k_r}(x_r) \oplus x_{r+1}$ is

$$\frac{s_{r'}}{s_{r'} + 1 - 2^{-\frac{n}{2}} \cdot s_{r'}}.$$

■

V. The Attack

Define an intermediate function

$$\begin{aligned} I_{K_i} &: GF(2)^{128} \longrightarrow GF(2)^{128} \\ I_{K_i}(x,y) &= (R_{K_i}(R_{K_i}(y) \oplus x) \oplus y, R_{K_i}(y) \oplus x). \quad (5) \end{aligned}$$

The function I_{K_i} is indeed two rounds of encryption with key K_i such that the second swap is ignored. That is, I_{K_i} is $F_{K_i}F_{K_i}$ without the last swap. We use this function as the intermediate function. It has many fixed points:

Lemma 1: The function I_{K_i} has 2^{64} fixed points.

Proof: The fixed points of the function I_{K_i} are those $(x,y) \in GF(2)^{128}$ such that

$$x = R_{K_i}(R_{K_i}(y) \oplus x) \oplus y \text{ and } y = R_{K_i}(y) \oplus x. \quad (6)$$

These are the same equations and the points $(R_{K_i}(y) \oplus y, y)$ are fixed points of I_{K_i} $\forall y \in GF(2)^{64}$.

■

The intermediate function of MagentaP2 chosen as

$$I_{K_1}(x,y) = (R_{K_1}(R_{K_1}(y) \oplus x) \oplus y, R_{K_1}(y) \oplus x) \quad (7)$$

also has 2^{64} fixed points by Lemma 1. If the first half of a plaintext is equal to second half of its corresponding ciphertext through encryption of Magenta, then the remaining other halves are also equal with probability nearly one half by Corollary 1. This distinguisher does not depend on the number of Magenta encryptions.

The reflection attack on MagentaP2 is to get an equation similar to Equation 4 and solve it to extract the subkey K_t. The following proposition leads to a reflection attack on MagentaP2.

Theorem 2: Assume that Magenta is a random function. Let a plaintext $x = (x_0, x_1)$ be encrypted by MagentaP2 and the ciphertext $y = (y_0, y_1)$ be produced. Assume that $x_1 = y_0$. Then x and y satisfy the equation

$$R_{K_t}(x_1) \oplus R_{K_{t \lll m}}(y_0) = x_0 \oplus y_1. \quad (8)$$

with probability

$$\frac{1}{2 - 2^{-64}}.$$

Proof: Observe that the equations $R_{K_t}(x_1) \oplus R_{K_{t \lll m}}(y_0) = x_0 \oplus y_1$ and $x_1 = y_0$ together come from a fixed point $(R_{K_t}(x_1) \oplus x_0, x_1)$ of double encryption Magenta function $E_K^{(M)} E_K^{(M)}$ without the last swap. We have the equality of probabilities:

$$\Pr(F_{K_t}(x) \text{ is fixed point } \mid x_1 = y_1) = \frac{\Pr(F_{K_t}(x) \text{ is fixed point})}{\Pr(x_1 = y_1)}$$

since $\Pr(x_1 = y_1 \,|\, F_{K_t}(x) \text{ is fixed point}) = 1$. On the other hand, $\Pr(x_1 = y_1) = 2^{-63} - 2^{-128}$ by Theorem 1 and the result follows.

■

Equation 8 in Theorem 2 leads to a divide and conquer type attack that can be mounted on MagentaP2. Encrypt a plaintext $x = (x_0, x_1)$ and obtain the corresponding ciphertext $y = (y_0, y_1)$. If $x_1 = y_0$ then Equation 8 is satisfied for x and y with probability nearly one half by Theorem 2. Solve the equation and extract the subkey K_t and then recover the remaining key bits by searching exhaustively. Let the key length be $64 \cdot i$ for $i = 2, 3, 4$. Then, by using $i \cdot 2^{64}$ plaintexts we obtain approximately $2i$ equations of the form Equation 8 and expect half of them to be correct by Proposition 2. By collecting the subsets of i equations and solving them we obtain a unique solution for K_t. Note that false alarm probability is almost zero since the probability that a false key is a solution of all the i equations is 2^{-64i}. The time complexity of recovering K_t is $\binom{2i}{i} \frac{i \cdot 2^{64i-63}}{r}$ where r is the number of rounds, namely 14 or 18 depending on the key size. The remaining key material (i.e., K_1) can be deduced by exhaustive search. As a result, one can recover the key by $2^{64.78}, 2^{131.1}$ and $2^{196.96}$ encryptions using $2^{65}, 2^{65.58}$ and 2^{66} known plaintexts for 128 bit, 192 bit and 256 bit key lengths, respectively.

VI. Conclusion and Discussion

The algorithm Magenta is doubled in the modified version. Indeed, the number of Magenta encryption does not affect the attack complexity. Therefore, one may use triple or more Magenta encryptions. Still, the attack will work. It is also interesting that other self-similarity attack methods whose complexities are independent of round number, such as related key attacks or slide attacks probably do not work for MagentaP2.

One design criterion introduced in [13] is the self similarity degree of functions. It is expected that the round functions of a block ciphers should not be similar of high degree with high probability. Indeed, the Magenta round functions are even same with probability one. This property results from the key schedule of Magenta and is exploited in the attack.

References

[1] E. Biham. New Types of Cryptanalytic Attacks Using Related Keys. *J. of Cryptology*, Vol.7, pp.229-246, 1994.

[2] E.Biham, A. Biryukov, N. Ferguson, L.R. Knudsen, B. Schneier and A. Shamir. Cryptanalysis of Magenta. In *Proc. Second AES conference*, NIST, 1999.

[3] E.Biham, O. Dunkelman and N. Keller. Improved Slide Attacks, In *Proc. FSE'07*, LNCS 4593, pp. 153-166, Springer, 2007.

[4] E. Biham and A. Shamir. *Differential Cryptanalysis of Data Encryption Standard*. Springer, 1993.

[5] A. Biryukov and D. Wagner. Slide Attacks. In *Proc. FSE'99*, LNCS 1636, pp.245-259, Springer, 1999.

[6] A. Biryukov and D. Wagner. Advanced Slide Attacks. In *Proc. EUROCRYPT 2000*, LNCS 1807, pp.589-606, Springer, 2000.

[7] G. Carter, E. Dawson and L. Nielsen. Key Schedules of Iterated Block Ciphers. In *Proc. Information Security and Privacy, ACISP'98*, LNCS 1438 pp. 80-89, Springer, 1998.

[8] D. Coppersmith. The Real Reason for Rivest's Phenomenon. In *Proc. CRYPTO'85*, LNCS 218, pp. 535-536, Springer, 1985.

[9] M. Henricksen. *Design, Implementation and Cryptanalysis of Modern Symmetric Ciphers*. PhD Thesis, ISRC, Faculty of Information Technology, Queensland University of Technology, 2005.

[10] M.J. Jacobson Jr. and K. Huber. The Magenta Block Cipher Algorithm. In *Proc. First AES conference*, NIST, 1998.

[11] B.S. Kaliski, R.L. Rivest and T. Sherman. Is DES a Pure Cipher? (Results of More Cycling Experiments on DES). In *Proc. CRYPTO'85*, LNCS 218, pp. 212-222, Springer, 1985.

[12] O. Kara. Reflection Cryptanalysis of Some Ciphers. In Proc. *INDOCRYPT 2008*, LNCS 5365, pp. 294-307, Springer, 2008.

[13] O. Kara. Self-Similarity Anlaysis of Block Ciphers. In Proc. II. National Cryptology Symposium, METU Ankara 2006.

[14] O. Kara and C. Manap. A new class of Weak Keys for Blowfish, In *Proc. FSE'07*, LNCS 4593, pp. 167-180, Springer, 2007.

[15] J. Kelsey and B. Schneier. Key-Schedule Cryptanalysis of DEAL. In *Proc. SAC'99*, pp.118-134, Springer, 2000.

[16] Y. Ko, S. Hong, W. Lee, S. Lee and J. Kang. Related Key Differential Attacks on 27 Rounds of XTEA and Full-Round GOST. In *Proc. FSE'04*, LNCS 3017, pp.299-316, Springer, 2004.

[17] M. Matsui. Linear Cryptanalysis Method of DES Cipher. In *Proc. EUROCRYPT'93*, LNCS 765, pp. 386-397, Springer, 1994.

[18] J.H. Moore and G.J. Simmons. Cycle Structure of the DES with Weak and Semi-Weak Keys. In *Proc. CRYPTO'86*, LNCS 263, pp.9-32, Springer, 1986.

[19] J.H. Moore and G.J. Simmons. Cycle Structure of the DES for Keys Having Palindromic (or Antipalindromic) Sequences of Round Keys. *IEEE Transactions on Software Engineering*, pp. 262-273,No 13,1987.