Research Article

Collision Attacks on AES-192/256, Crypton-192/256, mCrypton-96/128, and Anubis

Jinkeon Kang,¹ Kitae Jeong,¹ Jaechul Sung,² Seokhie Hong,¹ and Kyungho Lee¹

¹ Center for Information Security Technologies (CIST), Korea University, Anam-dong, Seongbuk-gu, Seoul 136-713, Republic of Korea

² Department of Mathematics, University of Seoul, Jeonnong-dong, Dongdaemun-gu, Seoul 130-743, Republic of Korea

Correspondence should be addressed to Kyungho Lee; kevinlee@korea.ac.kr

Received 19 July 2013; Accepted 22 August 2013

Academic Editor: Jongsung Kim

Copyright © 2013 Jinkeon Kang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

At AES'00, a collision attack on 7-round reduced AES was proposed. In this paper, we apply this idea to seven SPN block ciphers, AES-192/256, Crypton-192/256, mCrypton-96/128, and Anubis. Applying our attacks on AES-192/256, we improve the attack result based on meet-in-the-middle attack (AES-192) and the attack result proposed in AES'00 (AES-256), respectively. Our attack result on Anubis is superior to known cryptanalytic result on it. In the cases of Crypton-192/256 and mCrypton-96/128, our attacks are applicable to 8-round reduced versions. The attack results on mCrypton-96/128 are more practical than known cryptanalytic results on them.

1. Introduction

Recently, meet-in-the-middle attack has received attention. The attack procedure of meet-in-the-middle attack can be summarized as follows. Let $\mathcal{M}$ be the message space and $\mathcal{K}$ the key space. Suppose that G_K and $H_K : \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{M}$ are two block ciphers and let $F_K = H_K \circ G_K$. In this attack, an attacker tries to deduce K from a given plaintext/ciphertext pair $c = F_K(p)$ by trying to solve $G_K(p) = H_K^{-1}(c)$. In some cases, the equation is not tested for all the bits of the intermediate encryption value, but rather for only some of them. So far, many meet-in-the-middle attack results on block cipher have been proposed [1, 2]. On the other hand, Gilbert and Minier proposed a collision attack on 7-round of AES in [3]. This attack is a type of meet-in-the middle attack and exploits a 4-round distinguisher. In general, block cipher is completely deterministic, that is, if it is run again with the exact same input values, identical output values will be produced. Similarly, the different input values result in the different output values. However, it is possible that the different input values result in the output values of which the specific parts are the same. We call this case a collision.

In this paper, we apply the main idea of [3] to seven SPN block ciphers, such as AES-192/256 [4], Crypton [5], mCrypton-96/128 [6], and Anubis [7]. Table 1 shows our

attack results on them. Rijndael was announced as the Advanced Encryption Standard (AES) in 2001. After DES, it is one of the most widely used and analyzed ciphers in the world. AES is a 128-bit block cipher and accepts key sizes of 128, 192, and 256 bits. These versions of AES are called AES-128/192/256 and the number of rounds for these versions is 10, 12, and 14, respectively. Our attacks on AES-192/256 require a computational complexity of $2^{69.2}$ encryptions with 2^{32} chosen plaintexts and 2^{74} memory bytes, respectively. Though our attacks on them are not applicable to the full AES-192/256, these are superior to the attack results of [1] (AES-192) and [3] (AES-256), respectively.

Crypton is a 128-bit block cipher submitted as a candidate for the AES proposal of NIST. This algorithm has a 12-round SPN structure with 128/192/256-bit secret keys. According to the length of the secret keys, we call them Crypton-128/192/256, respectively. Our attack is applicable to 8-round reduced Crypton-192/256. To our knowledge, truncated differential cryptanalysis on 8-round reduced Crypton-192/256 has the best results on them, so far [8]. The attacks on an 8-round reduced Crypton-192/256 need the computational complexity of $2^{161.6}$ encryptions with 2^{96} chosen plaintexts and 2^{138} memory bytes, respectively. Compared to the attack results of [8], our attacks decrease the data complexity but increase the computational complexity.

S_{00}	S_{01}	S_{02}	S_{03}
S_{10}	S_{11}	S_{12}	S_{13}
S_{20}	S_{21}	S_{22}	S_{23}
S_{30}	S_{31}	S_{32}	S_{33}

FIGURE 1: Internal state of AES-192/256 and Anubis.

A 64-bit block cipher mCrypton was designed as a reduced version of Crypton for a ubiquitous environment. It provides low-resource hardware implementation, which is suitable for low-end devices such as RFID tags and wireless sensor network. Several security aspects related to RFID tags and wireless sensor network have already been studied. mCrypton has 12 rounds and supports the 64/96/128-bit secret keys. Our attack is applicable to mCrypton-96/128. We require the computational complexity of $2^{81.6}$ encryptions with 2^{48} chosen plaintexts and 2^{65} memory bytes. However, this is not the best result on them, since related-key impossible differential cryptanalysis on 9-round reduced mCrypton-96/128 was proposed in [9]. However, considering the attack assumption of a related-key attack, our attacks are more practical than it.

Anubis is a block cipher submitted to the NESSIE project and operates on data blocks of 128 bits, accepting keys of length $32N$ bits ($N = 4, \dots, 10$). It is a Rijndael variant that uses involutions for the various operations. Our attack is applicable to Anubis where the length of the secret key is longer than 192 bits. We need the computational complexity of $2^{161.6}$ encryptions with 2^{96} chosen plaintexts and 2^{138} memory bytes. This result is superior to known cryptanalytic results on this algorithm.

The rest of this paper is organized as follows. In Section 2, we propose collision attacks on AES-192/256. Collision attacks on Crypton-192/256 and mCrypton-96/128 are introduced in Section 3. In Section 4, we present a collision attack on Anubis. In each section, we start with a brief description of the block cipher concerned. Finally, we give our conclusion in Section 5.

2. Collision Attacks on 7-Round Reduced AES-192/256

First, we briefly present AES-192/256. And then we introduce collision attacks on AES-192/256. Note that the attack procedure on AES-192 is the same as that on AES-256. Thus, for the simplicity of notations, we just call them AES-192/256 AES.

2.1. AES-192/256. AES-192/256 are 128-bit block ciphers with 192/256-bit secret keys. According to the length of the

secret key, the number of rounds is 12 and 14, respectively. Each internal state is treated as a byte matrix of size 4×4 , where each byte represents a value in $\text{GF}(2^8)$ (see Figure 1).

In round r , input/output values and round key are denoted by I^r , O^r , and RK^r , respectively ($r = 1, \dots, 12$ (AES-192) or 14 (AES-256)). A whitening key is denoted by RK^0 . The round function of AES-192/256 applies the following four operations to the state matrix:

- (i) SubBytes (SB): applying the same 8×8 invertible S-box 16 times in parallel on each byte of the state;
- (ii) ShiftRows (SR): cyclic shift of each row (the i th row is shifted by i bytes to the left);
- (iii) MixColumns (MC): multiplication of each column by a constant 4×4 matrix over $\text{GF}(2^8)$;
- (iv) AddRoundKey (ARK): XORing the state with a 128-bit round key.

The SB, SR, MC, and ARK transformations are applied to each round except that MC is omitted in the last round. Besides, before the first round, an extra ARK is applied, which we call a whitening key step. For the more detailed descriptions of AES-192/256, we refer to [4]. We omit the key schedules of them, as they do not affect our attacks.

2.2. Finding a 4-Round Distinguisher of AES. In our attack on AES, we use a 4-round distinguisher of round 2~5. We consider an input value I^2 of round 2 in AES which is constructed as follows:

- (i) $(I_{00}^2, I_{10}^2, I_{20}^2, I_{30}^2)$: four 8-bit variables;
- (ii) I_{ij}^2 : a fixed 8-bit constant ($0 \leq i \leq 3, 1 \leq j \leq 3$).

By using I^2 , we can construct the following equations on I^3 ($i = 0, \dots, 3$). Here, a_{ij} means the entry of the coefficient matrix of MC ($j = 0, \dots, 3$):

$$\begin{aligned}
 I_{i0}^3 &= a_{i0} \circ \text{SB} [I_{00}^2] \oplus a_{i1} \circ \text{SB} [I_{11}^2] \oplus a_{i2} \circ \text{SB} [I_{22}^2] \\
 &\quad \oplus a_{i3} \circ \text{SB} [I_{33}^2] \oplus \text{RK}_{i0}^2, \\
 I_{i1}^3 &= a_{i0} \circ \text{SB} [I_{01}^2] \oplus a_{i1} \circ \text{SB} [I_{12}^2] \oplus a_{i2} \circ \text{SB} [I_{23}^2] \\
 &\quad \oplus a_{i3} \circ \text{SB} [I_{30}^2] \oplus \text{RK}_{i1}^2, \\
 I_{i2}^3 &= a_{i0} \circ \text{SB} [I_{02}^2] \oplus a_{i1} \circ \text{SB} [I_{13}^2] \oplus a_{i2} \circ \text{SB} [I_{20}^2] \\
 &\quad \oplus a_{i3} \circ \text{SB} [I_{31}^2] \oplus \text{RK}_{i2}^2, \\
 I_{i3}^3 &= a_{i0} \circ \text{SB} [I_{03}^2] \oplus a_{i1} \circ \text{SB} [I_{10}^2] \oplus a_{i2} \circ \text{SB} [I_{21}^2] \\
 &\quad \oplus a_{i3} \circ \text{SB} [I_{32}^2] \oplus \text{RK}_{i3}^2.
 \end{aligned} \tag{1}$$

Note that each I_{i0}^3 , I_{i1}^3 , I_{i2}^3 , and I_{i3}^3 depends on only one 8-bit variable and one 8-bit round key: $(I_{00}^2, \text{RK}_{i0}^2)$, $(I_{30}^2, \text{RK}_{i1}^2)$, $(I_{20}^2, \text{RK}_{i2}^2)$, and $(I_{10}^2, \text{RK}_{i3}^2)$.

Applying the above procedure repeatedly, as shown in (2), we can obtain an equation on an input value I_{00}^5 of round 5 by using I^2 . Here, bold characters indicate $(I_{10}^2, I_{20}^2, I_{30}^2)$

$$\begin{aligned}
I_{00}^5 = & a_{00} \circ \text{SB} \left[a_{00} \circ \text{SB} \left(a_{00} \circ \text{SB} \left[I_{00}^2 \right] \oplus a_{01} \circ \text{SB} \left[I_{11}^2 \right] \oplus a_{02} \circ \text{SB} \left[I_{22}^2 \right] \oplus a_{03} \circ \text{SB} \left[I_{33}^2 \right] \oplus \text{RK}_{00}^2 \right) \right. \\
& \oplus a_{01} \circ \text{SB} \left(a_{10} \circ \text{SB} \left[I_{01}^2 \right] \oplus a_{11} \circ \text{SB} \left[I_{12}^2 \right] \oplus a_{12} \circ \text{SB} \left[I_{23}^2 \right] \oplus a_{13} \circ \text{SB} \left[I_{30}^2 \right] \oplus \text{RK}_{11}^2 \right) \\
& \oplus a_{02} \circ \text{SB} \left(a_{20} \circ \text{SB} \left[I_{02}^2 \right] \oplus a_{21} \circ \text{SB} \left[I_{13}^2 \right] \oplus a_{22} \circ \text{SB} \left[I_{20}^2 \right] \oplus a_{23} \circ \text{SB} \left[I_{31}^2 \right] \oplus \text{RK}_{22}^2 \right) \\
& \left. \oplus a_{03} \circ \text{SB} \left(a_{30} \circ \text{SB} \left[I_{03}^2 \right] \oplus a_{31} \circ \text{SB} \left[I_{10}^2 \right] \oplus a_{32} \circ \text{SB} \left[I_{21}^2 \right] \oplus a_{33} \circ \text{SB} \left[I_{32}^2 \right] \oplus \text{RK}_{33}^2 \right) \oplus \text{RK}_{00}^3 \right] \\
& \oplus a_{01} \circ \text{SB} \left[a_{10} \circ \text{SB} \left(a_{00} \circ \text{SB} \left[I_{01}^2 \right] \oplus a_{01} \circ \text{SB} \left[I_{02}^2 \right] \oplus a_{12} \circ \text{SB} \left[I_{23}^2 \right] \oplus a_{03} \circ \text{SB} \left[I_{30}^2 \right] \oplus \text{RK}_{01}^2 \right) \right. \\
& \oplus a_{11} \circ \text{SB} \left(a_{10} \circ \text{SB} \left[I_{02}^2 \right] \oplus a_{11} \circ \text{SB} \left[I_{13}^2 \right] \oplus a_{12} \circ \text{SB} \left[I_{20}^2 \right] \oplus a_{13} \circ \text{SB} \left[I_{31}^2 \right] \oplus \text{RK}_{12}^2 \right) \\
& \oplus a_{12} \circ \text{SB} \left(a_{20} \circ \text{SB} \left[I_{03}^2 \right] \oplus a_{21} \circ \text{SB} \left[I_{10}^2 \right] \oplus a_{22} \circ \text{SB} \left[I_{21}^2 \right] \oplus a_{23} \circ \text{SB} \left[I_{32}^2 \right] \oplus \text{RK}_{23}^2 \right) \\
& \left. \oplus a_{13} \circ \text{SB} \left(a_{30} \circ \text{SB} \left[I_{00}^2 \right] \oplus a_{31} \circ \text{SB} \left[I_{11}^2 \right] \oplus a_{32} \circ \text{SB} \left[I_{22}^2 \right] \oplus a_{33} \circ \text{SB} \left[I_{33}^2 \right] \oplus \text{RK}_{30}^2 \right) \oplus \text{RK}_{11}^3 \right] \\
& \oplus a_{02} \circ \text{SB} \left[a_{20} \circ \text{SB} \left(a_{00} \circ \text{SB} \left[I_{02}^2 \right] \oplus a_{01} \circ \text{SB} \left[I_{13}^2 \right] \oplus a_{02} \circ \text{SB} \left[I_{20}^2 \right] \oplus a_{03} \circ \text{SB} \left[I_{31}^2 \right] \oplus \text{RK}_{02}^2 \right) \right. \\
& \oplus a_{21} \circ \text{SB} \left(a_{10} \circ \text{SB} \left[I_{03}^2 \right] \oplus a_{11} \circ \text{SB} \left[I_{10}^2 \right] \oplus a_{12} \circ \text{SB} \left[I_{21}^2 \right] \oplus a_{13} \circ \text{SB} \left[I_{32}^2 \right] \oplus \text{RK}_{13}^2 \right) \\
& \oplus a_{22} \circ \text{SB} \left(a_{20} \circ \text{SB} \left[I_{00}^2 \right] \oplus a_{21} \circ \text{SB} \left[I_{11}^2 \right] \oplus a_{22} \circ \text{SB} \left[I_{22}^2 \right] \oplus a_{23} \circ \text{SB} \left[I_{33}^2 \right] \oplus \text{RK}_{20}^2 \right) \\
& \left. \oplus a_{23} \circ \text{SB} \left(a_{30} \circ \text{SB} \left[I_{01}^2 \right] \oplus a_{31} \circ \text{SB} \left[I_{12}^2 \right] \oplus a_{32} \circ \text{SB} \left[I_{23}^2 \right] \oplus a_{33} \circ \text{SB} \left[I_{30}^2 \right] \oplus \text{RK}_{31}^2 \right) \oplus \text{RK}_{22}^3 \right] \\
& \oplus a_{03} \circ \text{SB} \left[a_{30} \circ \text{SB} \left(a_{00} \circ \text{SB} \left[I_{03}^2 \right] \oplus a_{01} \circ \text{SB} \left[I_{10}^2 \right] \oplus a_{02} \circ \text{SB} \left[I_{21}^2 \right] \oplus a_{03} \circ \text{SB} \left[I_{32}^2 \right] \oplus \text{RK}_{03}^2 \right) \right. \\
& \oplus a_{31} \circ \text{SB} \left(a_{10} \circ \text{SB} \left[I_{00}^2 \right] \oplus a_{11} \circ \text{SB} \left[I_{11}^2 \right] \oplus a_{12} \circ \text{SB} \left[I_{22}^2 \right] \oplus a_{13} \circ \text{SB} \left[I_{33}^2 \right] \oplus \text{RK}_{10}^2 \right) \\
& \oplus a_{32} \circ \text{SB} \left(a_{20} \circ \text{SB} \left[I_{01}^2 \right] \oplus a_{21} \circ \text{SB} \left[I_{12}^2 \right] \oplus a_{22} \circ \text{SB} \left[I_{23}^2 \right] \oplus a_{23} \circ \text{SB} \left[I_{30}^2 \right] \oplus \text{RK}_{21}^2 \right) \\
& \left. \oplus a_{33} \circ \text{SB} \left(a_{30} \circ \text{SB} \left[I_{02}^2 \right] \oplus a_{31} \circ \text{SB} \left[I_{13}^2 \right] \oplus a_{32} \circ \text{SB} \left[I_{20}^2 \right] \oplus a_{33} \circ \text{SB} \left[I_{31}^2 \right] \oplus \text{RK}_{32}^2 \right) \oplus \text{RK}_{33}^3 \right] \oplus \text{RK}_{00}^4.
\end{aligned} \tag{2}$$

Note that this equation consists of five parts as follows:

$$\begin{aligned}
I_{00}^5 = & (a_{00} \circ \text{SB} [\cdot]) \oplus (a_{01} \circ \text{SB} [\cdot]) \oplus (a_{02} \circ \text{SB} [\cdot]) \\
& \oplus (a_{03} \circ \text{SB} [\cdot]) \oplus \text{RK}_{00}^4.
\end{aligned} \tag{3}$$

If we find different $(I_{10}^{2'}, I_{20}^{2'}, I_{30}^{2'})$ and $(I_{10}^{2''}, I_{20}^{2''}, I_{30}^{2''})$ which satisfy that each subpart including $(I_{10}^{2'}, I_{20}^{2'}, I_{30}^{2'})$, that is, (2, 3, 4)th rows of the first part, (1, 2, 3)th rows of the second part, (1, 2, 4)th rows of the third part, and (1, 3, 4)th rows of the fourth part in (2), has the same value for a given I_{00}^2 , then $I_{00}^{5'}$ is equal to $I_{00}^{5''}$. That is, for all $I_{00}^2 \in \{0, \dots, 255\}$, these $(I_{10}^{2'}, I_{20}^{2'}, I_{30}^{2'})$ and $(I_{10}^{2''}, I_{20}^{2''}, I_{30}^{2''})$ result in the same 32-bit value of four subparts (the length of the value in each subpart is 8 bits). By the birthday paradox, we can obtain different $(I_{10}^{2'}, I_{20}^{2'}, I_{30}^{2'})$ and $(I_{10}^{2''}, I_{20}^{2''}, I_{30}^{2''})$ from $2^{16}(I_{10}^2, I_{20}^2, I_{30}^2)$ with the probability of 0.5.

We can express I^5 by using O^5 as follows. Here, f^{-1} means the inverse of a function f

$$\begin{aligned}
O^5 &= \text{ARK}_{\text{RK}^5} \circ \text{MC} \circ \text{SR} \circ \text{SB} [I^5] \\
&= \text{MC} \circ \text{SR} \circ \text{ARK}_{\text{SR}^{-1} \circ \text{MC}^{-1} [\text{RK}^5]} \circ \text{SB} [I^5]
\end{aligned} \tag{4}$$

$$\Rightarrow \text{SB} [I^5] = \text{ARK}_{\text{SR}^{-1} \circ \text{MC}^{-1} [\text{RK}^5]} \circ \text{SR}^{-1} \circ \text{MC}^{-1} [O^5].$$

If we obtain different $(I_{10}^{2'}, I_{20}^{2'}, I_{30}^{2'})$ and $(I_{10}^{2''}, I_{20}^{2''}, I_{30}^{2''})$ satisfying $I_{00}^{5'} = I_{00}^{5''}$, then $\text{SB}[I_{00}^{5'}]$ is also equal to $\text{SB}[I_{00}^{5''}]$. Thus, from the above equation, we can construct the following equation. Here, b_{ij} means the entry of the coefficient matrix of MC^{-1}

$$\begin{aligned}
\text{SB} [I_{00}^{5'}] &= b_{00} \circ O_{00}^{5'} \oplus b_{01} \circ O_{10}^{5'} \oplus b_{02} \circ O_{20}^{5'} \oplus b_{03} \circ O_{30}^{5'} \\
&= b_{00} \circ O_{00}^{5''} \oplus b_{01} \circ O_{10}^{5''} \oplus b_{02} \circ O_{20}^{5''} \oplus b_{03} \circ O_{30}^{5''} \\
&= \text{SB} [I_{00}^{5''}].
\end{aligned} \tag{5}$$

For all $I_{00}^2 \in \{0, \dots, 255\}$, we can check that $I_{00}^{5'}$ is equal to $I_{00}^{5''}$ by using (5). That is, with the probability of 0.5, we can find

TABLE 1: Our attack results on AES-192/256, Crypton-192/256, mCrypton-96/128, and Anubis.

Target Algorithm	Attack	Number of rounds	Data complexity	Computational complexity
AES-192	MitM [1]	7	2^{40}	2^{80}
	RKABA [10]	12	2^{123}	2^{176}
	CA (This paper)	7	2^{32}	$2^{69.2}$
AES-256	CA [3]	7	2^{32}	2^{140}
	RKBA [10]	14	$2^{99.5}$	$2^{99.5}$
	CA (This paper)	7	2^{32}	$2^{69.2}$
Crypton-192/256	TDC [8]	8	2^{126}	$2^{126.2}$
	CA (This paper)	8	2^{96}	$2^{161.6}$
mCrypton-96	RKIDC [9]	9	$2^{59.9}$	$2^{74.9}$
	CA (This paper)	8	2^{48}	$2^{81.6}$
mCrypton-128	RKIDC [9]	9	$2^{59.7}$	$2^{66.7}$
	CA (This paper)	8	2^{48}	$2^{81.6}$
Anubis	CA [11]	7	2^{32}	2^{140}
	Square [11]	7	$2^{128} \sim 2^{119}$	2^{120}
	CA (This paper)	8	2^{96}	$2^{161.6}$

MitM: meet-in-the-middle attack.

TDC: truncated differential cryptanalysis.

RKABA: related-key amplified boomerang attack.

RKBA: related-key boomerang attack.

RKIDC: related-key impossible differential cryptanalysis.

CA: collision attack.

different $(I_{10}^{2'}, I_{20}^{2'}, I_{30}^{2'})$ and $(I_{10}^{2''}, I_{20}^{2''}, I_{30}^{2''})$ satisfying (5) for all I_{00}^2 (among 2^{16} candidates).

On the other hand, our attack on AES recovers a 192-bit round key and the probability that (5) holds for one I_{00}^2 is 2^{-8} . So, if we use only 25 I_{00}^2 , the probability that (5) holds is $(2^{-8})^{25} = 2^{-200}$. Since $2^{-200} \cdot 2^{192} \ll 1$, we consider only 25 I_{00}^2 .

2.3. Collision Attack on a 7-Round Reduced AES. Now, we show how to exploit a 4-round distinguisher constructed in the previous subsection in order to attack a 7-round reduced AES.

Similarly to the previous subsection, O^5 can be expressed by using O^7 as follows:

$$\begin{aligned}
O^7 &= \text{ARK}_{\text{RK}^7} \circ \text{SR} \circ \text{SB} \circ \text{ARK}_{\text{RK}^6} \circ \text{MC} \circ \text{SR} \circ \text{SB} [O^5] \\
&= \text{SR} \circ \text{ARK}_{\text{SR}^{-1}[\text{RK}^7]} \circ \text{SB} \circ \text{MC} \circ \text{SR} \\
&\quad \circ \text{ARK}_{\text{SR}^{-1} \circ \text{MC}^{-1}[\text{RK}^6]} \circ \text{SB} [O^5] \\
\Rightarrow O^5 &= \text{SB}^{-1} \circ \text{ARK}_{\text{SR}^{-1} \circ \text{MC}^{-1}[\text{RK}^6]} \circ \text{SR}^{-1} \circ \text{MC}^{-1} \\
&\quad \circ \text{SB}^{-1} \circ \text{ARK}_{\text{SR}^{-1}[\text{RK}^7]} \circ \text{SR}^{-1} [O^7].
\end{aligned} \tag{6}$$

For the simplicity of notations, $\text{SR}^{-1} \circ \text{MC}^{-1}[\text{RK}^6]$ and $\text{SR}^{-1}[\text{RK}^7]$ in (6) are denoted by RK^{6*} and RK^{7*} , respectively.

Our attack procedure on AES is as follows (see Figure 2).

- (1) Construct 2^{32} plaintexts P^i , where all byte values except $(P_{00}^i, P_{11}^i, P_{22}^i, P_{33}^i)$ are fixed constants, and obtain the corresponding ciphertexts C^i ($i = 0, \dots, 2^{32} - 1$).

Sort C^i 's according to a 32-bit value $P_{00}^i \parallel P_{11}^i \parallel P_{22}^i \parallel P_{33}^i$.

- (2) For each $j (= 0, \dots, 3)$, guess 40-bit round keys $(\text{RK}_{j0}^{6*}, \text{RK}_{0((4-j) \bmod 4)}^{7*}, \text{RK}_{1((4-j) \bmod 4)}^{7*}, \text{RK}_{2((4-j) \bmod 4)}^{7*}, \text{RK}_{3((4-j) \bmod 4)}^{7*})$ and compute the corresponding O_{j0}^5 from the guessed round keys and C^i by using (6) (e.g., guess $(\text{RK}_{00}^{6*}, \text{RK}_{00}^{7*}, \text{RK}_{10}^{7*}, \text{RK}_{20}^{7*}, \text{RK}_{30}^{7*})$ to compute O_{00}^5). Sort O_{j0}^5 according to the guessed round keys, i and j , and keep them in a table.
- (3) Select 2^{16} sets S^k including 25 output values X of MC in round 1 ($k = 0, \dots, 2^{16} - 1$). Note that X_{mm} are fixed constants in all S^k ($0 \leq m \leq 3, 1 \leq n \leq 3$). In each S^k , 25 X_{00} have different values but all S^k contain the same X_{00} . In the case of (X_{10}, X_{20}, X_{30}) , they are different in each S^k but the same in all S^k .
- (4) Guess 32-bit round keys $(\text{RK}_{00}^0, \text{RK}_{11}^0, \text{RK}_{22}^0, \text{RK}_{33}^0)$ and construct 2^{16} sets Q^k including the corresponding $(P'_{00}, P'_{11}, P'_{22}, P'_{33})$ from each X in S^k , and do the following:
 - (i) choose different two sets Q^{k_1} and Q^{k_2} . By using the table constructed in Step 2, check that 25 pairs from Q^{k_1} and Q^{k_2} satisfy (5);
 - (ii) if all 25 pairs satisfy (5), then output the corresponding 192-bit guessed round keys as the right round keys of AES.

The data complexity of this attack is 2^{32} chosen plaintexts and the memory complexity is $2^{74} (\approx 4 \cdot 2^{32} \cdot 2^{40})$ memory

FIGURE 2: The attack procedure on AES-192/256.

bytes. The computational complexity depends on Step 2 heavily. Thus, it is about $2^{69.2} (\approx 2^{32} \cdot 2^{40} \cdot 1/7 \cdot 1/4 \cdot 4)$ encryptions. Though this attack is not applicable to the full AES-192/256, this result is superior to the attack results of [1] (AES-192) and [3] (AES-256), respectively.

3. Collision Attacks on 8-Round Reduced Crypton-192/256 and mCrypton-96/128

In this section, we present collision attacks on 8-round reduced Crypton-192/256 and mCrypton-96/128. Our attacks on 8-round reduced mCrypton-96/128 are similar to them on 8-round reduced Crypton-192/256. Thus, we mainly introduce the attacks on 8-round reduced Crypton-192/256. Furthermore, similarly to the attacks on AES-192/256, the attack procedure on Crypton-192 (mCrypton-96) is the same as that on Crypton-256 (mCrypton-128). Thus, for the simplicity of notations, we just call them Crypton-192/256 (mCrypton-96/128) and Crypton (mCrypton). First, we briefly present Crypton and mCrypton.

3.1. Crypton and mCrypton. As shown in Figure 3(a), a 128-bit block cipher Crypton has a 12-round SPN structure with 128/192/256-bit secret keys and processes blocks of 128 bits in the form of 4×4 byte array (see Figure 4). Note that indices used in the internal state of Crypton are different from that of AES.

Similarly to AES-192/256, in round r , we denote input/output values and round key I^r, O^r , and RK^r , respectively ($r = 1, \dots, 12$). The round function ρ of Crypton consists of the following four operations:

- (i) γ : applying four 4×4 S-boxes (S_0, S_1, S_2, S_3) 4 times in parallel on each byte of the state. Note that two versions (γ_o, γ_e) of γ are used according to rounds. In detail, γ_o is for odd rounds and γ_e is for even rounds;
- (ii) π : mixing each byte column of 4×4 array by using four masking bytes (m_0, m_1, m_2, m_3). Similarly to γ , two versions (π_o, π_e) of π are applied according to rounds (π_o is for odd rounds and π_e is for even rounds);
- (iii) τ : moving the byte at the (i, j) th position to the (j, i) th position;
- (iv) σ : XORing the state with an 128-bit round key.

The round function ρ consists of applying in sequence four operations, the S-box transformation γ , the bit permutation π , the byte transposition τ , and the key addition σ , to the 4×4 byte array. More specifically, the odd round function ρ_{oRK} and the even round function ρ_{eRK} are defined (for a round key RK) as follows:

- (i) $\rho_{oRK} = \sigma_{RK} \circ \tau \circ \pi_o \circ \gamma_o$ for odd rounds;
- (ii) $\rho_{eRK} = \sigma_{RK} \circ \tau \circ \pi_e \circ \gamma_e$ for even rounds.

For the more detailed descriptions of Crypton, we refer to [5]. Similarly to our attacks on AES-192/256, our attacks on Crypton do not also consider the key schedule of this algorithm. Thus, we omit its key schedules.

mCrypton is a 64-bit lightweight block cipher designed for use in low-cost and resource-constrained applications such as RFID tags and sensors in wireless sensor networks. As shown in Figure 3(b), it has a 12-round SPN structure and supports the 64/96/128-bit secret keys. The overall structure of mCrypton is similar to Crypton except that mCrypton is

FIGURE 3: (a) Crypton and (b) mCrypton.

S_{30}	S_{20}	S_{10}	S_{00}
S_{31}	S_{21}	S_{11}	S_{01}
S_{32}	S_{22}	S_{12}	S_{02}
S_{33}	S_{23}	S_{13}	S_{03}

FIGURE 4: Internal state of Crypton and mCrypton.

based on nibble-oriented operations (note that Crypton is based on byte-oriented operations).

3.2. Collision Attacks on an 8-Round Reduced Crypton. First, we explain the way to find a distinguisher of Crypton. By using a similar method in the attack on AES-192/256, we can

also construct a 4-round distinguisher of Crypton. Furthermore, because of the weak diffusion property of Crypton, we can extend this distinguisher to a 5-round distinguisher of it. In detail, our attacks on an 8-round reduced Crypton consider a 5-round distinguisher of round 2 ~ 6.

Recall that, in the attack on AES-192/256, an equation on O_{00}^5 can be constructed by using I^2 . We apply this method to Crypton. As a result, we obtain an equation on I_{30}^6 by using I^2 . Similarly to AES-192/256, this equation consists of five parts as follows. Here, m_i means a masking byte used in π and “ $\wedge$ ” is a bitwise AND operation

$$I_{30}^6 = (S_0 [\cdot] \wedge m_3) \oplus (S_1 [\cdot] \wedge m_0) \oplus (S_2 [\cdot] \wedge m_1) \oplus (S_3 [\cdot] \wedge m_2) \oplus RK_{30}^5. \quad (7)$$

On the other hand, I^6 can be written by using O^6 as follows:

$$\begin{aligned} O^6 &= \sigma_{RK^6} \circ \tau \circ \pi_e \circ \gamma_e [I^6] = \tau \circ \pi_e \circ \sigma_{\pi_e^{-1} \circ \tau^{-1}(RK^6)} \circ \gamma_e [I^6] \\ \Rightarrow \gamma_e [I^6] &= \sigma_{\pi_e^{-1} \circ \tau^{-1}(RK^6)} \circ \pi_e^{-1} \circ \tau^{-1} [O^6]. \end{aligned} \quad (8)$$

Thus, we use the following equation as a checking equation (note that, in the case of the attack on AES-192/256, a checking equation is (5))

$$\begin{aligned}
 \gamma_e [I_{30}^{6'}] &= (O_{03}^{6'} \wedge m_0) \oplus (O_{13}^{6'} \wedge m_3) \\
 &\quad \oplus (O_{23}^{6'} \wedge m_2) \oplus (O_{33}^{6'} \wedge m_1) \\
 &= (O_{03}^{6''} \wedge m_0) \oplus (O_{13}^{6''} \wedge m_3) \oplus (O_{23}^{6''} \wedge m_2) \quad (9) \\
 &\quad \oplus (O_{33}^{6''} \wedge m_1) \\
 &= \gamma_e [I_{30}^{6''}].
 \end{aligned}$$

The overall attack procedure is similar to the case of AES. Figure 5 presents our attack procedure on an 8-round reduced Crypton. The method to compute O^6 from O^8 is shown in

$$\begin{aligned}
 O^8 &= \tau \circ \pi_e \circ \tau \circ \sigma_{RK^8} \circ \tau \circ \pi_e \circ \gamma_e \circ \sigma_{RK^7} \circ \tau \circ \pi_o \circ \gamma_o [O^6] \\
 &= \tau \circ \pi_e \circ \tau \circ \tau \circ \pi_e \circ \sigma_{\pi_e^{-1} \circ \tau^{-1} [RK^8]} \circ \gamma_e \circ \tau \circ \pi_o \\
 &\quad \circ \sigma_{\pi_o^{-1} \circ \tau^{-1} [RK^7]} \circ \gamma_o [O^6] \\
 &= \tau \circ \sigma_{\pi_e^{-1} \circ \tau^{-1} [RK^8]} \circ \gamma_e \circ \tau \circ \pi_o \circ \sigma_{\pi_o^{-1} \circ \tau^{-1} [RK^7]} \circ \gamma_o [O^6] \\
 &= \sigma_{\tau \circ \pi_e^{-1} \circ \tau^{-1} [RK^8]} \circ \tau \circ \gamma_e \circ \tau \circ \pi_o \circ \sigma_{\pi_o^{-1} \circ \tau^{-1} [RK^7]} \circ \gamma_o [O^6] \\
 &= \sigma_{\tau \circ \pi_e^{-1} \circ \tau^{-1} [RK^8]} \circ \gamma_e \circ \pi_o \circ \sigma_{\pi_o^{-1} \circ \tau^{-1} [RK^7]} \circ \gamma_o [O^6]. \\
 \Rightarrow O^6 &= \gamma_o^{-1} \circ \sigma_{\pi_o^{-1} \circ \tau^{-1} [RK^7]} \circ \pi_o^{-1} \circ \gamma_e^{-1} \circ \sigma_{\tau \circ \pi_e^{-1} \circ \tau^{-1} [RK^8]} [O^8]. \quad (10)
 \end{aligned}$$

The complexities of this attack are as follows:

- (i) the data complexity: 2^{96} chosen plaintexts;
- (ii) the memory complexity: 2^{133} memory bytes;
- (iii) the computational complexity: $2^{161.6}$ encryptions.

So far, the best attack result was the truncated differential cryptanalysis on 8-round reduced Crypton-192/256 proposed in [8]. This attack requires the computational complexity of $2^{126.2}$ encryptions with 2^{126} chosen plaintexts, respectively. Compared to these results, our attack decreases the data complexity but increases the computational complexity.

3.3. Collision Attacks on an 8-Round Reduced mCrypton. As shown in Figure 5, the attack procedure on mCrypton is the same as that on Crypton except that it is based on nibble-oriented operations (recall that Crypton is based on byte-oriented operations). In detail, our attack on mCrypton uses (9) as a checking equation and O^6 is computed from O^8 by using (10).

Since the size of internal state of mCrypton is half of that in Crypton, the complexities of the attack on mCrypton are half of them on Crypton. The complexities of the attack on mCrypton are as follows:

- (i) the data complexity: 2^{48} chosen plaintexts;
- (ii) the memory complexity: $2^{81.6}$ memory bytes;
- (iii) the computational complexity: 2^{65} encryptions.

In [9], related-key impossible differential cryptanalysis on 9-round reduced mCrypton-96/128 was proposed. The attack on a 9-round reduced mCrypton-96 needs the computational complexity of $2^{74.9}$ encryptions with $2^{59.9}$ chosen plaintexts. In the case of a 9-round reduced mCrypton-128, we need the computational complexity of $2^{66.7}$ encryptions with $2^{59.7}$ chosen plaintexts. To our knowledge, these are the best results on mCrypton-96/128. However, considering the attack assumption of a related-key attack, our attacks are more practical than it.

4. Collision Attack on an 8-Round Reduced Anubis

First, we present Anubis, and then a collision attack on an 8-round reduced Anubis is introduced.

4.1. Anubis. As shown in Figure 6, Anubis is a 128-bit block cipher with variable-length keys from 128 bits to 320 bits in steps of 32 bits. The number of rounds depends on the length of the secret key: at least 12 (for the 128-bit secret key), plus one extra round for each additional 32 bits. For example, when the length of the secret key is 192(= 128 + 2 · 32) bits, the number of rounds is 14(= 12 + 2).

Anubis processes blocks of 128 bits in the form of 4×4 byte array and uses the same indices as AES (see Figure 1). Similarly to block ciphers concerned in the previous sections, in round r , we denote input/output values and round key I^r , O^r , and RK^r , respectively.

The round function of Anubis consists of sixteen 8×8 S-box parallel lookups, a linear transformation (matrix transposition followed by multiplication by a constant MDS diffusion matrix), and the round key addition. These transformations are defined as follows:

- (i) γ : applying the same 8×8 S-box 16 times in parallel on each byte of the state;
- (ii) τ : moving the byte at the (i, j) th position to the (j, i) th position;
- (iii) θ : multiplication of each column by a constant 4×4 matrix over $GF(2^8)$;
- (iv) σ : XORing the state with a 128-bit round key.

For the more detailed descriptions of Anubis, we refer to [7]. Similarly to the previous sections, we omit their key schedules, as they do not affect our attacks.

4.2. Collision Attacks on an 8-Round Reduced Anubis. Our attack on an 8-round reduced Anubis is similar to the attacks on AES-192/256, Crypton-192/256, and mCrypton-96/128. In collision attack on an 8-round reduced Anubis, we use a 5-round distinguisher of round 2~6. By using a similar

FIGURE 5: The attack procedure on Crypton-192/256 and mCrypton-96/128.

FIGURE 6: Anubis.

FIGURE 7: The attack procedure on Anubis.

method of the attack introduced in the previous sections, we can obtain the following equation on I_{00}^6 by using I^2 :

$$I_{00}^6 = (S[\cdot] \circ 01) \oplus (S[\cdot] \circ 02) \oplus (S[\cdot] \circ 04) \oplus (S[\cdot] \circ 06) \oplus \text{RK}_{00}^5. \quad (11)$$

On the other hand, I^6 can be written by using O^6 as follows:

$$O^6 = \sigma_{\text{RK}^6} \circ \theta \circ \tau \circ \gamma [I^6] = \theta \circ \tau \circ \sigma_{\tau^{-1} \circ \theta^{-1} [\text{RK}^6]} \circ \gamma [I^6] \Rightarrow \gamma [I^6] = \sigma_{\tau^{-1} \circ \theta^{-1} [\text{RK}^6]} \circ \tau^{-1} \circ \theta^{-1} [O^6]. \quad (12)$$

Thus, we use the following equation as a checking equation

$$\begin{aligned} \gamma [I_{00}^{6'}] &= (O_{00}^{6'} \circ 01) \oplus (O_{10}^{6'} \circ 02) \oplus (O_{20}^{6'} \circ 04) \oplus (O_{30}^{6'} \circ 06) \\ &= (O_{00}^{6''} \circ 01) \oplus (O_{10}^{6''} \circ 02) \oplus (O_{20}^{6''} \circ 04) \oplus (O_{30}^{6''} \circ 06) \\ &= \gamma_e [I_{00}^{6''}]. \end{aligned} \quad (13)$$

The attack procedure on an 8-round reduced Anubis is similar to that on block ciphers proposed in the previous

sections. Figure 7 presents our attack procedure on an 8-round reduced Anubis. In our attack, the method to compute O^6 from O^8 is

$$\begin{aligned} O^8 &= \sigma_{\text{RK}^8} \circ \tau \circ \gamma \circ \sigma_{\text{RK}^7} \circ \theta \circ \tau \circ \gamma [O^6] \\ &= \tau \circ \sigma_{\tau^{-1} [\text{RK}^8]} \circ \gamma \circ \sigma_{\text{RK}^7} \circ \theta \circ \tau \circ \gamma [O^6] \\ &= \tau \circ \sigma_{\tau^{-1} [\text{RK}^8]} \circ \theta \circ \tau \circ \sigma_{\tau^{-1} \circ \theta^{-1} [\text{RK}^7]} \circ \gamma [O^6] \\ &\Rightarrow O^6 = \gamma^{-1} \circ \sigma_{\tau^{-1} \circ \theta^{-1} [\text{RK}^7]} \circ \tau^{-1} \circ \theta^{-1} \circ \sigma_{\tau^{-1} [\text{RK}^8]} \circ \tau^{-1} [O^8]. \end{aligned} \quad (14)$$

The complexities of this attack is as follows:

- (i) the data complexity: 2^{96} chosen plaintexts;
- (ii) the memory complexity: 2^{133} memory bytes;
- (iii) the computational complexity: $2^{161.6}$ encryptions.

So far, the best attack results on Anubis are a collision attack and a square attack on a 7-round reduced version [11]. A collision attack on a 7-round reduced Anubis requires the computational complexity of 2^{140} encryptions with 2^{32} chosen plaintexts. In the case of a square attack on this algorithm, we need the computational complexity of 2^{120} encryptions with $2^{128} \sim 2^{119}$ chosen plaintexts. Thus, our attack result is superior to these cryptanalytic results.

5. Conclusion

In this paper, we have introduced collision attacks on seven SPN block ciphers, 7-round reduced AES-192/256, 8-round

reduced Crypton-192/256, 8-round reduced mCrypton-96/128, and an 8-round reduced Anubis. Our attacks are based on the idea of [3].

Our attacks on 7-round reduced AES-192/256 improve the attack results based on a type of meet-in-the-middle attack. Considering that the best attack results on Crypton-192/256 are those on 8-round reduced versions, our attacks on these algorithms are meaningful. Our attacks on 8-round reduced mCrypton-96/128 are not best results on mCrypton-96/128. However, considering that known best attack results on them are based on a related-key attack, our attacks are more practical than them. In the case of Anubis, our attack result is superior to known cryptanalytic result on this algorithm.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was supported by the Ministry of Science, ICT & Future Planning (MSIP), Korea, under the Convergence Information Technology Research Center (C-ITRC) Support Program (NIPA-2013-H0301-13-3007), supervised by the National IT Industry Promotion Agency (NIPA).

References

- [1] H. Demirci and A. Selçuk, "A meet-in-the-middle attack on 8-round AES," in *Proceedings of the FSE*, vol. 5086 of *Lecture Notes in Computer Science*, pp. 116–126, 2008.
- [2] O. Dunkelman, G. Sekar, and B. Preneel, "Improved meet-in-the-middle attacks on reduced-round DES," in *Proceedings of the Indocrypt*, vol. 4859 of *Lecture Notes in Computer Science*, pp. 86–100, Springer, Berlin, Germany, 2007.
- [3] H. Gilbert and M. Minier, "A collision attack on 7 rounds of Rijndael," in *Proceedings of the AES Candidate Conference*, pp. 230–241, 2000.
- [4] FIPS 197, "Advanced Encryption Standard (AES)," 2001, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.
- [5] C. Lim, "A revised version of crypton. Crypton Version 1.0," in *Proceedings of the FSE*, vol. 1638 of *Lecture Notes in Computer Science*, pp. 31–45, 1999.
- [6] C. Lim and T. Korkishko, "mCrypton—a lightweight block cipher for security of low-cost RFID tags and sensors," in *Proceedings of the WISA*, vol. 3786 of *Lecture Notes in Computer Science*, pp. 243–258, 2006.
- [7] P. Baretto and V. Rijmen, "The Anubis block cipher," *The NESSIE*, 2000.
- [8] J. Kim, S. Hong, S. Lee, J. H. Song, and H. Yang, "Truncated differential attacks on 8-round CRYPTON," in *Proceedings of the Information Security and Cryptology Conference (ICISC '03)*, vol. 2971 of *Lecture Notes in Computer Science*, pp. 446–456, Springer, Berlin, Germany, 2004.
- [9] H. Mala, M. Dakhilalian, and M. Shakiba, "Cryptanalysis of mCrypton—a lightweight block cipher for security of RFID tags and sensors," *International Journal of Communication Systems*, vol. 25, no. 4, pp. 415–426, 2012.
- [10] A. Biryukov and D. Khovratovich, "Related-key cryptanalysis of the full AES-192 and AES-256," in *Proceedings of the Asiacrypt*, vol. 5912 of *Lecture Notes in Computer Science*, pp. 1–18, Springer, Berlin, Germany, 2009.
- [11] A. Biryukov, "Analysis of involutory ciphers: Khazad and Anubis," in *Proceedings of the FSE*, vol. 2887 of *Lecture Notes in Computer Science*, pp. 45–53, 2003.