The Journal of Systems and Software xxx (2010) xxx–xxx

Contents lists available at ScienceDirect

The Journal of Systems and Software

journal homepage: www.elsevier.com/locate/jss

A differential cryptanalysis of Yen–Chen–Wu multimedia cryptography system

Chengqing Li [a,*], Shujun Li [b,**], Kwok-Tung Lo [a], Kyandoghere Kyamakya [c]

[a] Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China
[b] Fachbereich Informatik und Informationswissenschaft, Universität Konstanz, Fach M697, Universitätsstraße 10, 78457 Konstanz, Germany
[c] Universität Klagenfurt, Institut für Intelligente Systemtechnologien, Universitätsstraße 65-67, 9020 Klagenfurt, Austria

ARTICLE INFO

Article history:
Received 5 November 2009
Received in revised form 4 February 2010
Accepted 28 February 2010
Available online xxxx

Keywords:
Chaos
Cryptanalysis
Differential attack
Encryption
Multimedia
Security

ABSTRACT

Recently, Yen et al. presented a new chaos-based cryptosystem for multimedia transmission named "multimedia cryptography system" (MCS). No cryptanalytic results have been reported so far. This paper presents a differential attack to break MCS, which requires only seven chosen plaintexts. The complexity of the attack is $O(N)$, where N is the size of plaintext. Experimental results are also given to show the real performance of the proposed attack.

1. Introduction

The prevalence of multimedia data makes its security become more and more important. However, traditional cryptosystems can not protect multimedia data efficiently due to the big differences between texts and multimedia data, such as the bulky sizes and strong correlation between neighboring elements of uncompressed multimedia data. In addition, multimedia encryption schemes have some special requirements like high bitrate and easy concatenation of different components of the whole multimedia processing system. So, designing special encryption schemes protecting multimedia data becomes necessary. To meet this challenge, a great number of multimedia encryption schemes have been proposed in the past two decades (Bourbakis and Alexopoulos, 1992; Chung and Chang, 1998; Scharinger, 1998; Fridrich, 1998; Chen et al., 2004; Wu and Kuo, 2005; Flores-Carmona and Carpio-Valadez, 2006; Pareek et al., 2006; Xiao et al., 2006; Kim et al., 2007; Wong and Yuen, XXXX). Due to the subtle similarity between chaos and cryptography, some of multimedia encryption schemes were designed based on one or more chaotic systems (Scharinger, 1998; Fridrich, 1998; Chen et al., 2004; Pareek et al., 2006; Xiao et al., 2006; Wong and Yuen, XXXX). Meanwhile, a lot of cryptanalytic work has also been reported, showing that many encryption schemes were not designed carefully and are prone to various kinds of attacks (Jan and Tseng, 1996; Chang and Yu, 2002; Lian et al., 2005; Solak, 2005; Álvarez and Li, 2005; Wang et al., 2005; Arroyo et al., 2008; Zhou et al., 2007; Rhouma and Belghith, 2008; Jakimoski and Subbalakshmi, 2008; Zhou et al., 2009; Li et al., 2009).

In the past decade, a series of encryption schemes were proposed by Yen and Guo's research group (Yen and Guo, 2000; Guo et al., 2002; Chen and Yen, 2003; Chen et al., 2003; Yen et al., 2005). The main idea of these schemes is to combine some basic encryption operations, under the control of a pseudorandom bit sequence (PRBS) generated by iterating a chaotic system. Unfortunately, most of Yen–Guo multimedia encryption schemes have been successfully cryptanalyzed (Li et al., 2005, 2006a,b, 2008a,b).

This paper reports a security analysis of MCS (multimedia cryptography system) – the latest multimedia encryption scheme proposed by Yen et al. (2005). Another hardware implementation of MCS was proposed in Chen et al. (2007). Compared with other earlier designs, such as RCES (Chen and Yen, 2003) and TDCEA (Chen et al., 2003), which have been cryptanalyzed in (Li et al., 2008b, 2005), MCS combines more encryption operations of different kinds in a more complicated manner, in the hope that the security can be effectively enhanced. This paper shows that MCS is still vulnerable to a differential chosen plaintext attack. Only seven chosen plaintexts (or six specific plaintext differentials) are enough to break MCS, with a *divide-and-conquer* (DAC) strategy.

The rest of this paper is organized as follows. Section 2 briefly introduces how MCS works. The proposed differential attack is

* Corresponding author.
** Corresponding author.
E-mail address: zjulcq@gmail.com (C. Li).
URL: http://www.hooklee.com (S. Li).

0164-1212/$ - see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2010.02.039

detailed in Section 3 with experimental results. Finally the last section concludes the paper.

2. Multimedia cryptography system (MCS)

MCS encrypts the plaintext block by block, and each block contains 15 bytes. As the first step of the encryption process, each 15-byte plain-block is expanded to a 16-byte one by adding a secretly selected byte. Then, the expanded block is encrypted with the following four different operations: byte-swapping (permutation), value masking, horizontal and vertical bit rotations, which are all controlled by a secret PRBS.

Denote the plaintext by $f=(f(i))_{i=0}^{N-1}$, where $f(i)$ denotes the ith plain-byte. Without loss of generality, assume that N can be exactly divided by 15. Then, the plaintext has $N/15$ blocks: $f=(f^{(15)}(k))_{k=0}^{N/15-1}$, where $f^{(15)}(k)=(f^{(15)}(k,j))_{j=0}^{14}=(f(15k+j))_{j=0}^{14}$. Similarly, denote the ciphertext by $f'=(f'(i))_{i=0}^{(N/15)\cdot 16-1}=(f'^{(16)}(k))_{k=0}^{N/15-1}$, where $f'^{(16)}(k)=(f'^{(16)}(k,j))_{j=0}^{15}=(f'(16k+j))_{j=0}^{15}$ denotes the expanded cipher-block. With the above notations, MCS can be described as follows.

- *The secret key* includes five integers α_1, α_2, β_1, β_2, *Secret*, and a binary fraction $x(0)$, where $1\leqslant\alpha_1<\alpha_1+\beta_1\leqslant 7$, $1\leqslant\alpha_2<\alpha_2+\beta_2\leqslant 7$[1], $Secret\in\{0,\ldots,255\}$ and $x(0)=\sum_{j=-64}^{64}x(0)_j\cdot 2^j$, $x(0)_j\in\{0,1\}$.
- *A PRBG (pseudorandom bit generator)*
  A pseudorandom number sequence $(x(i))_{i=0}^{N/15+9}$ is generated by iterating the following equation from $x(0)$:

$$x(i+1)=T((419/2^8)\cdot(x(i)\oplus H(x(i)))\bmod 2^{64}), \qquad (1)$$

  where $x(i)=\sum_{j=-64}^{64}x(i)_j\cdot 2^j$, $x(i)_j\in\{0,1\}$, $H(x(i))=\sum_{j=-64}^{64}(\oplus_{k=-64}^{-1}x(i)_k)\cdot 2^j$, $T(x)=x-(x\bmod 2^{-64})$ and $\oplus$ denotes bitwise XOR. Then, the controlling PRBG $(b(i))_{i=0}^{129N/15-1}$ is derived from $(x(i))_{i=10}^{N/15+9}$ by extracting the 129 bits from each $x(i+10)$. The above PRBG is a special case of the second class of chaos-based PRBG proposed in Kocarev and Jakimoski (2003), with the parameters $p=419$, $m=8$, $M=k=64$.
- *The initialization process*
  (1) run the above PRBG to generate the controlling PRBS $(b(i))_{i=0}^{129N/15-1}$; (2) set $temp=Secret$.
- *The encryption procedure*
  For each plain-block $f^{(15)}(k)$, do the following operations consecutively:
  - *Step (a) Data expansion*
    Add *temp* to the 15-byte plain-block to get an expanded 16-byte block

$$f^{(16)}(k)=(f^{(16)}(k,j))_{j=0}^{15}=(f^{(15)}(k,0),\ldots,f^{(15)}(k,14),temp),$$

    and then set $temp=f^{(16)}(k,l(k))$, where $l(k)=\sum_{i=0}^{3}b(129k+i)\cdot 2^i$.
  - *Step (b) Byte-swapping*
    Define a pseudorandom byte-swapping operation, $Swap_b(129k+l)\ (f^{(16)}(k,i),f^{(16)}(k,j))$, which swaps $f^{(16)}(k,i)$ and $f^{(16)}(k,j)$ when $b(129k+l)=1$. Then, perform the byte-swapping operation for the following 32 values of (i,j,l) one after another: (0,8,4), (1,9,5), (2,10,6), (3,11,7), (4,12,8), (5,13,9), (6,14,10), (7,15,11), (0,4,12), (1,5,13), (2,6,14), (3,7,15), (8,12,16), (9,13,17), (10,14,18), (11,15,19), (0,2,20), (1,3,21), (4,6,22), (5,7,23), (8,10,24), (9,11,25), (12,14,26), (13,15,27), (0,1,28), (2,3,29), (4,5,30), (6,7,31), (8,9,32), (10,11,33), (12,13,34), (14,15,35). Denote the permuted 16-byte block by $f^{*(16)}(k)$.
  - *Step (c) Value masking*
    Determine two pseudorandom variables, $Seed1(k)=\sum_{i=0}^{15}(\oplus_{t=0}^{3}b(129k+4i+t))\cdot 2^i$ and $Seed2(k)=\sum_{i=16}^{31}(\oplus_{t=0}^{3}b(129k+4i+t))\cdot 2^{i-16}$, and then do the following masking operation for $j=0\sim 7$:

$$f^{**(16)}(k)_j=f^{*(16)}(k)_j\oplus Seed(k,j), \qquad (2)$$

    where $f^{*(16)}(k)_j$ and $f^{**(16)}(k)_j$ are composed of the jth bits of the 16 elements of $f^{*(16)}(k)$ and $f^{**(16)}(k)$, respectively,

$$Seed(k,j)=\begin{cases}Seed1(k), & B(k,j)=3,\\ \overline{Seed1(k)}, & B(k,j)=2,\\ Seed2(k), & B(k,j)=1,\\ \overline{Seed2(k)}, & B(k,j)=0,\end{cases} \qquad (3)$$

    and $B(k,j)=2\cdot b(129k+36+2j)+b(129k+37+2j)$.
  - *Step (d) Horizontal bit rotation*
    Construct an 8×8 matrix $\mathbf{M}_1$ by assigning $\mathbf{M}_1(i,j)$ as the j-th bit of $f^{**(16)}(k,i)$. Then, perform the following horizontal bit-rotation operations for $i=0,\ldots,7$ to get a new matrix $\widetilde{\mathbf{M}}_1$:

$$\widetilde{\mathbf{M}}_1(i,:)=RotateX^{p_{1,k,i},r_{1,k,i}}(\mathbf{M}_1(i,:)),$$

    which shifts $\mathbf{M}_1(i,:)$ (the ith row of $\mathbf{M}_1$) by $r_{1,k,i}$ elements (bits) to the left when $p_{1,k,i}=1$ and to the right when $p_{1,k,i}=0$. The values of the two parameters are as follows: $p_{1,k,i}=b(129k+65+2i)$, $r_{1,k,i}=\alpha_1+\beta_1\cdot b(129k+66+2i)$. Equivalently, the above process can be rewritten in the following way:

$$\widetilde{\mathbf{M}}_1(i,:)=RotateX^{0,\bar{r}_{1,k,i}}(\mathbf{M}_1(i,:)),$$

    where

$$\bar{r}_{1,k,i}=\begin{cases}\alpha_1+\beta_1\cdot b(129k+66+2i), & p_{1,k,i}=b(129k+65+2i)=0,\\ 8-(\alpha_1+\beta_1\cdot b(129k+66+2i)), & p_{1,k,i}=b(129k+65+2i)=1.\end{cases}$$

    In the following, we will use the latter form to simplify our further discussion.
    In a similar way, construct another 8×8 matrix $\mathbf{M}_2$ by assigning $\mathbf{M}_2(i,j)$ as the jth bit of $f^{**(16)}(k,8+i)$. Then, perform similar horizontal bit-rotation operations on $\mathbf{M}_2$ to get a new matrix $\widetilde{\mathbf{M}}_2$:

$$\widetilde{\mathbf{M}}_2(i,:)=RotateX^{0,\bar{r}_{2,k,i}}(\mathbf{M}_2(i,:)),$$

    where

$$\bar{r}_{2,k,i}=\begin{cases}\alpha_1+\beta_1\cdot b(129k+98+2i), & p_{2,k,i}=b(129k+97+2i)=0,\\ 8-(\alpha_1+\beta_1\cdot b(129k+98+2i)), & p_{2,k,i}=b(129k+97+2i)=1.\end{cases}$$

    After the above horizontal bit-rotation operations, represent the ith byte in the 16-byte block as follows:

$$f^{\star(16)}(k,i)=\begin{cases}\sum_{j=0}^{7}\widetilde{\mathbf{M}}_1(i,j)\cdot 2^j, & 0\leqslant i\leqslant 7,\\ \sum_{j=0}^{7}\widetilde{\mathbf{M}}_2(i-8,j)\cdot 2^j, & 8\leqslant i\leqslant 15.\end{cases}$$

  - *Step (e) Vertical bit rotation*
    For $j=0,\ldots,7$, do the following vertical bit-rotation operations on $\widetilde{\mathbf{M}}_1$ to get $\widehat{\mathbf{M}}_1$:

$$\widehat{\mathbf{M}}_1(:,j)=RotateY^{0,\bar{s}_{1,k,j}}(\widetilde{\mathbf{M}}_1(:,j)),$$

    which shifts $\widetilde{\mathbf{M}}_1(:,j)$ (the jth column of $\widetilde{\mathbf{M}}_1$) by $s_{1,k,j}$ elements (bits) downwards. The value of the parameter is as follows:

[1] In Yen et al. (2005), Yen et al. did not exclude the possibility of $\alpha_i=0$ and $\beta_i=0$, but to achieve the effect of encryption they should not be equal to 0.

Please cite this article in press as: Li, C., et al. A differential cryptanalysis of Yen–Chen–Wu multimedia cryptography system. J. Syst. Software (2010), doi:10.1016/j.jss.2010.02.039

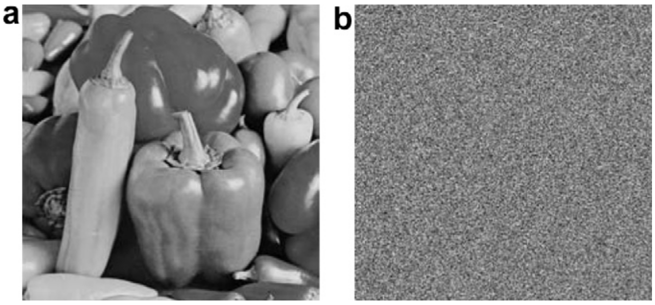

Fig. 1. The plain-image "Peppers" and the corresponding cipher-image: (a) the plain-image; (b) the cipher-image.

$$\bar{s}_{1,k,j} = \begin{cases} \alpha_1 + \beta_1 \cdot b(129k + 82 + 2j), & q_{1,k,j} = b(129k + 81 + 2j) = 0, \\ 8 - (\alpha_1 + \beta_1 \cdot b(129k + 82 + 2j)), & q_{1,k,j} = b(129k + 81 + 2j) = 1. \end{cases}$$

Similar vertical bit rotations are performed on $\widetilde{\mathbf{M}}_2$ to get $\widehat{\mathbf{M}}_2$ as follows:

$$\widehat{\mathbf{M}}_2(:, j) = RotateY^{0, \bar{s}_{2,k,j}}(\widetilde{\mathbf{M}}_2(:, j)),$$

where

$$\bar{s}_{2,k,j} = \begin{cases} \alpha_1 + \beta_1 \cdot b(129k + 114 + 2j), & q_{2,k,j} = b(129k + 113 + 2j) = 0, \\ 8 - (\alpha_1 + \beta_1 \cdot b(129k + 114 + 2j)), & q_{2,k,j} = b(129k + 113 + 2j) = 1. \end{cases}$$

Finally, the cipher-block $f'^{(16)}(k) = (f'^{(16)}(k, i))_{i=0}^{15}$ is derived from $\widehat{\mathbf{M}}_1$ and $\widehat{\mathbf{M}}_2$ as follows:

$$f'^{(16)}(k, i) = \begin{cases} \sum_{j=0}^{7} \widehat{\mathbf{M}}_1(i, j) \cdot 2^j, & 0 \leqslant i \leqslant 7, \\ \sum_{j=0}^{7} \widehat{\mathbf{M}}_2(i - 8, j) \cdot 2^j, & 8 \leqslant i \leqslant 15. \end{cases}$$

- *The decryption procedure* is simply the inverse of the above encryption procedure.

To show real performance of the above encryption scheme, a 512×512 plain-image "Peppers" and the corresponding cipher-image are shown in Fig. 1, where the randomly selected secret key is as follows: $\alpha_1 = 2$, $\beta_1 = 5$, $\alpha_2 = 3$, $\beta_2 = 4$, $Secret = 20$, and $x(0) = 0.251$. Note that the cipher-image is 1/16 higher than the plain-image due to the data expansion. To show how MCS works more clearly, encryption process of the second 15-byte block of the image shown in Fig. 1a is shown in Table 1.

3. Cryptanalysis

First of all, we point out that the sub-key *Secret* has no influence on the plaintext recovered from the decryption process. It is because *Secret* is only used to determine the expanded byte, and never used to change the value of any other byte in the plaintext. In fact, if we use a different value of *Secret* for the decryption process, the plaintext can still be correctly recovered. Furthermore, the probability that *Secret* becomes the expanded byte of $f^{(16)}(k)$ is $(15/16)^k$, which decreases exponentially with respect to k. As a consequence, we can simply ignore the (statistically tiny) influence of *Secret* on the encryption process after k become sufficiently large. As a whole, *Secret* should be excluded from the key. In the rest of this paper, we will not consider *Secret* as a sub-key.

3.1. Some properties of MCS

Define the XOR-differential ("differential" in short hereinafter) of two plaintexts f_0 and f_1 as $f_{0\oplus 1} = f_0 \oplus f_1$. When f_0 and f_1 are encrypted with the same secret key, it is easy to prove the following three properties of MCS, which will be the basis of the proposed attack.

Table 1
Encryption process of the second 16-byte block of the image shown in Fig. 1a.

$f^{(16)}(1)$	174, 184, 185, 191, 188, 190, 191, 185,	191, 190, 189, 190, 189, 187, 183, 113
$\overline{f^{*(16)}}(1)$	191, 184, 189, 190, 189, 187, 191, 185,	174, 190, 185, 191, 188, 190, 183, 113
$f^{*(16)}(1)$	184, 191, 190, 191, 185, 189, 189, 187,	113, 185, 174, 190, 183, 190, 188, 191
$\mathbf{M}_1, \mathbf{M}_2$	$\begin{bmatrix} 1,1,0,0,0,1,0,1 \\ 0,0,0,1,0,0,0,1 \\ 0,1,0,1,1,0,1,0 \\ 1,1,1,0,1,1,1,0 \\ 0,1,1,1,0,0,0,1 \\ 1,0,1,0,1,1,1,0 \\ 1,0,1,0,1,1,1,0 \\ 1,1,0,0,1,1,1,0 \end{bmatrix}$	$\begin{bmatrix} 0,1,0,1,0,1,1,0 \\ 1,0,0,0,1,1,1,0 \\ 1,0,1,0,1,1,0,1 \\ 1,0,0,1,0,0,0,1 \\ 1,1,0,0,1,0,1,0 \\ 1,0,0,1,0,0,0,1 \\ 1,1,1,0,0,1,0,1 \\ 0,0,1,0,0,1,0,1 \end{bmatrix}$
$f^{**(16)}(1)$	163, 136, 90, 119, 142, 117, 117, 115,	106, 113, 181, 137, 83, 137, 167, 164
$\bar{r}_{1,1,i}, \bar{r}_{2,1,i}$	1, 2, 2, 6, 6, 6, 7, 6	1, 2, 6, 2, 2, 6, 1, 6
$\widetilde{\mathbf{M}}_1, \widetilde{\mathbf{M}}_2$	$\begin{bmatrix} 1,1,1,0,0,0,1,0 \\ 0,1,0,0,0,1,0,0 \\ 1,0,0,1,0,1,1,0 \\ 1,0,1,1,1,0,1,1 \\ 1,1,0,0,0,1,0,1 \\ 1,0,1,1,1,0,1,0 \\ 0,1,0,1,1,1,0,1 \\ 0,0,1,1,1,0,1,1 \end{bmatrix}$	$\begin{bmatrix} 0,0,1,0,1,0,1,1 \\ 1,0,1,0,0,0,1,1 \\ 1,0,1,1,0,1,1,0 \\ 0,1,1,0,0,1,0,0 \\ 1,0,1,1,0,0,1,0 \\ 0,1,0,0,0,1,1,0 \\ 1,1,1,1,0,0,1,0 \\ 1,0,0,1,0,1,0,0 \end{bmatrix}$
$f^{\star(16)}(1)$	71, 34, 105, 221, 163, 93, 186, 220,	212, 197, 109, 38, 77, 98, 79, 41
$\bar{s}_{1,1,i}, \bar{s}_{2,1,i}$	1, 3, 5, 3, 5, 3, 5, 3	7, 3, 1, 3, 3, 1, 7, 7
$\widehat{\mathbf{M}}_1, \widehat{\mathbf{M}}_2$	$\begin{bmatrix} 0,0,1,1,1,0,1,0 \\ 1,1,0,1,0,1,0,1 \\ 0,0,1,1,1,0,1,1 \\ 1,1,0,0,1,0,0,0 \\ 1,1,1,0,1,1,1,0 \\ 1,0,1,1,0,1,1,0 \\ 1,0,0,1,0,0,0,1 \\ 0,1,0,0,0,1,1,1 \end{bmatrix}$	$\begin{bmatrix} 1,1,0,0,0,1,1,1 \\ 1,1,1,1,0,0,1,0 \\ 0,0,1,1,0,0,0,0 \\ 1,0,1,0,1,1,1,0 \\ 0,0,1,0,0,1,1,0 \\ 1,0,1,1,0,0,1,0 \\ 1,1,0,0,0,1,0,0 \\ 0,0,1,1,0,0,1,1 \end{bmatrix}$
$f'^{(16)}(1)$	92, 171, 220, 19, 119, 109, 137, 226,	227, 79, 12, 117, 100, 77, 35, 204

Please cite this article in press as: Li, C., et al. A differential cryptanalysis of Yen–Chen–Wu multimedia cryptography system. J. Syst. Software (2010), doi:10.1016/j.jss.2010.02.039

Property 1. *The random masking in Step (c) cannot change the differential value, i.e.,* $\forall\, k,\ j,\ f_{0\oplus 1}^{**(16)}(k,j) \equiv f_{0\oplus 1}^{*(16)}(k,j)$.

Proof. It is a straightforward result of the following property of XOR: $(a\oplus x)\oplus(b\oplus x)=a\oplus b$. □

Property 2. *Each expanded plain-block* $f_{0\oplus 1}^{(16)}(k)$ *is independent of the sub-key Secret.*

Proof. This can be proved with mathematical induction on k. When $k=0$ and $0\leqslant j\leqslant 15$, i.e., for the jth byte of the first 16-byte block,

$$f_{0\oplus 1}^{(16)}(0,j)=\begin{cases} f_{0\oplus 1}^{(15)}(0,j), & 0\leqslant j\leqslant 14,\\ Secret\oplus Secret=0, & j=15,\end{cases}$$

which is obviously independent of the value of *Secret*. Now assume the property holds for the first $k-1$ blocks. Then, for the kth 16-byte block,

$$f_{0\oplus 1}^{(16)}(k,j)=\begin{cases} f_{0\oplus 1}^{(15)}(k,j), & 0\leqslant j\leqslant 14,\\ f_{0\oplus 1}^{(16)}(k-1,l(k-1)), & j=15,\end{cases}$$

which is also independent from *Secret* according to the assumption. Thus, this property is proved. □

Property 3. *The byte-swapping in Step (b) cannot change each differential value, but its position in the 16-byte block.*

Property 4. *Both the horizontal bit rotation in Step (d) and the vertical bit rotation in Step (e) cannot change each differential bit itself, but its position in the binary presentation of the 8-byte block.*

The proofs of the above two properties are straightforward, so we omit them here.

3.2. The differential attack

Based on the above properties of MCS, the data expansion in *Step (a)*, the first 8-byte-swapping operations in *Step (b)*, the vertical bit rotation in *Step (e)*, the horizontal bit rotation in *Step (d)*, the other unknown byte-swapping operations in *Step (b)* and the value masking in *Step (c)* can be broken in order with a number of chosen plaintext differentials.

3.2.1. Breaking the secret data expansion in Step (a)

To facilitate the following discussion, let us denote the Hamming weight of a byte or a block x, i.e., the number of 1-bits in x, by $|x|$. From Properties 3 and 4, and the proof of Property 2, one can see that there are $8\cdot 15=120$ binary bits of $f_{0\oplus 1}^{\prime(16)}(k)$ come from $f_{0\oplus 1}^{(15)}(k)$ and other eight bits come from $f_{0\oplus 1}^{(15)}(k-1,l(k-1))$ for $k\geqslant 1$ (the eight expanded bits are all 0-bits when $k=0$). Since all the other steps do not change the Hamming weight of each 16-byte block, we can get $\left|f_{0\oplus 1}^{(15)}(k-1,l(k-1))\right|=\left|f_{0\oplus 1}^{\prime(16)}(k)\right|-\left|f_{0\oplus 1}^{(15)}(k)\right|$. In case $\left|f_{0\oplus 1}^{(15)}(k-1,l(k-1))\right|$ is unique in the last 15-byte block $f_{0\oplus 1}^{(15)}(k-1)$, we can uniquely determine the value of $l(k-1)$. Considering $\left|f_{0\oplus 1}^{(15)}(k-1,l(k-1))\right|\in\{0,\ldots,8\}$ but $l(k-1)\in\{0,\ldots,15\}$, at least two plain-bytes in each 15-byte block have the same Hamming weight. So, the value of $l(k-1)$ may not be uniquely determined sometimes. To make the unique determination of $l(k-1)$ possible, we can choose two plaintext differentials $f_{0\oplus 1}$ and $f_{0\oplus 2}$ (i.e., differentials of three chosen plaintexts f_0, f_1 and f_2) to fulfill the following two requirements: (1) $\forall\, k,\ j_1\neq j_2,\ \left(\left|f_{0\oplus 1}^{(15)}(k,j_1)\right|,\left|f_{0\oplus 2}^{(15)}(k,j_1)\right|\right)\neq\left(\left|f_{0\oplus 1}^{(15)}(k,j_2)\right|,\left|f_{0\oplus 2}^{(15)}(k,j_2)\right|\right)$; (2) $\forall\, k,\ j,\ \left(\left|f_{0\oplus 1}^{(15)}(k,j)\right|,\left|f_{0\oplus 2}^{(15)}(k,j)\right|\right)\neq(0,0)$. For example, the two plaintext differentials can be chosen to have the following Hamming weights:

$$\begin{aligned}(|f_{0\oplus 1}(i)|)_{i=1}^{N-1}&=(\overbrace{0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,1,\ldots,8,8,8,8,8,8,8,8,8}^{9\times 9-1=80\ \text{elements}},\ldots)\\ (|f_{0\oplus 2}(i)|)_{i=1}^{N-1}&=(1,2,3,4,5,6,7,8,0,1,2,3,4,5,6,7,8,\ldots,0,1,2,3,4,5,6,7,8,\ldots)\end{aligned}$$

With the above chosen plaintexts, it is obvious that the value of $l(k-1)$ can always be uniquely determined, except when

$$\left(\left|f_{0\oplus 1}^{(15)}(k-1,15)\right|,\left|f_{0\oplus 2}^{(15)}(k-1,15)\right|\right)\in\bigcup_{j=0}^{14}\left(\left|f_{0\oplus 1}^{(15)}(k-1,j)\right|,\left|f_{0\oplus 2}^{(15)}(k-1,j)\right|\right). \tag{4}$$

The exception (4) occurs when $l(k-n_0+1)\neq 15$ and $l(k-n_0+1)=l(k-n_0+2)=\cdots=l(k-1)$, where $n_0=\lfloor 80/15\rfloor-1$ and $k\geqslant n_0-1$. Assuming that the secret bits controlling $l(k-n_0+1),\ldots,l(k-1)$ distribute uniformly over {0,1}, the occurrence probability of the exception is less than $\frac{15}{16}\cdot\left(\frac{1}{16}\right)^{\lfloor 80/15\rfloor-1}\approx 1.4305\times 10^{-5}$. For a 512×512 image, this means that we will not be able to uniquely determine the value of $l(k-1)$ for less than $1.4305\times 10^{-5}\times 512\times 512/16\approx 0.2344$ blocks in an average sense. In other words, the value of $l(k-1)$ can be uniquely determined for almost all blocks. Note that breaking $l(k-1)$ implies breaking 4 controlling bits $(b(129(k-1)+i))_{i=0}^{3}$.

3.2.2. Breaking the first 8-byte-swapping operations in Step (b)

From Properties 3 and 4, one can see that all the $8\cdot 16=128$ bits of each 16-byte expanded plain-block $f_{0\oplus 1}^{(16)}(k)$ are the same as the ones of the corresponding 16-byte cipher-block $f_{0\oplus 1}^{\prime(16)}(k)$, except that their locations may change. Observing how the bit locations are changed in the whole encryption process, we can see the following 8-byte-swapping operations are the only encryption operations moving bits from one 8-byte half-block to another: $Swap_{b(129k+i+4)}(f^{(16)}(k,i),f^{(16)}(k,i+8))$, when $i=0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7$. Apparently, when the controlling bit is 1, each byte-swapping operation swaps the locations of one byte in the first half-block and the other byte in another half-block. This fact means that, by choosing the differences between the Hamming weights of the 8-bytes in the two half-blocks properly, we will be able to derive the values of the controlling bits $(b(129k+i+4))_{i=0}^{7}$. The simplest tactic is to choose $f_{0\oplus 1}^{(16)}(k)$ such that each half-block has only one byte with a different Hamming weight from the corresponding byte in the other half-block. If we assume all the values of $(l(k))_{k=0}^{N/15-2}$ have been recovered, which happens with high probability as shown in the previous subsection, the first 15 bytes in $f_{0\oplus 1}^{(16)}(k)$ can be freely chosen by choosing $f_{0\oplus 1}^{(15)}(k)$. The last byte in

Please cite this article in press as: Li, C., et al. A differential cryptanalysis of Yen–Chen–Wu multimedia cryptography system. J. Syst. Software (2010), doi:10.1016/j.jss.2010.02.039

each 16-byte block $f_{0\oplus1}^{(16)}(k,15)$ may not be chosen, if it is equal to *Secret*. Fortunately, this has no influence on the process of breaking the first 8-byte-swapping operations, because what is chosen for the last byte is $|f^{(16)}(k,15)| - |f^{(16)}(k,7)|$. Although we may not be able to choose $f_{0\oplus1}^{(16)}(k,15)$, we can always choose $f_{0\oplus1}^{(16)}(k,7)$ to have a different Hamming weight from that of $f_{0\oplus1}^{(16)}(k,7)$. One chosen-block $f_{0\oplus1}^{(16)}(k)$ will be able to derive the value of one controlling bit, which controls the possible swapping of the two bytes (in two half-blocks, respectively) with different Hamming weights. We need eight chosen plain-blocks (thus eight chosen plaintext differentials) to determine the values of all the eight controlling bits.

While eight chosen plaintext differentials are enough to recover all the bits controlling the first 8-byte-swapping operations, we actually need only two chosen plaintext differentials to achieve this goal. To see how it is possible, denote the difference between the Hamming weights of the two half-blocks of the kth cipher-block by $\Delta\left|\left(f_{0\oplus1}^{\prime(16)}(k)\right)_{i=0}^{7}\right|$. Then, we have the following equation:

$$\begin{aligned}\Delta\left|\left(f_{0\oplus1}^{\prime(16)}(k)\right)_{i=0}^{7}\right| &= \left|\left(f_{0\oplus1}^{\prime(16)}(k,i)\right)_{i=0}^{7}\right| - \left|\left(f_{0\oplus1}^{\prime(16)}(k,i+8)\right)_{i=0}^{7}\right| \\ &= \left|\left(f_{0\oplus1}^{*(16)}(k,i)\right)_{i=0}^{7}\right| - \left|\left(f_{0\oplus1}^{*(16)}(k,i+8)\right)_{i=0}^{7}\right| \\ &= \sum_{i=0}^{7}\left(\left|f_{0\oplus1}^{*(16)}(k,i)\right| - \left|f_{0\oplus1}^{*(16)}(k,i+8)\right|\right) \\ &= \sum_{i=0}^{7} b^{\pm}(k,i)\left(\left|f_{0\oplus1}^{(16)}(k,i)\right| - \left|f_{0\oplus1}^{(16)}(k,i+8)\right|\right),\end{aligned}$$

where

$$b^{\pm}(k,i) = 1 - 2b(129k+i+4) = \begin{cases} 1, & b(129k+i+4)=0, \\ -1, & b(129k+i+4)=1. \end{cases}$$

By choosing the values of $\left(\left|f_{0\oplus1}^{(16)}(k,i)\right| - \left|f_{0\oplus1}^{(16)}(k,i+8)\right|\right)_{i=0}^{7}$ to be a set of numbers such that every nonzero number can not be represented as a linear combination of other numbers in the set, the controlling bits corresponding to the nonzero numbers can be determined uniquely. For instance, to determine the values of $b^{\pm}(k,0),\ldots,b^{\pm}(k,3)$, we can choose a plaintext differential such that

- $\left|f_{0\oplus1}^{(16)}(k,i)\right| - \left|f_{0\oplus1}^{(16)}(k,i+8)\right| = \pm4, \pm5, \pm6, \pm8$ for $i = 0,\ 1,\ 2,\ 3$, respectively;
- $\left|f_{0\oplus1}^{(16)}(k,i)\right| - \left|f_{0\oplus1}^{(16)}(k,i+8)\right| = 0$ for $i = 4,\ 5,\ 6,\ 7$.

The above chosen plaintext differential leads to the following result:

$$\Delta\left|\left(f_{0\oplus1}^{\prime(16)}(k)\right)_{i=0}^{7}\right| \in \{\pm23, \pm15, \pm13, \pm11, \pm7, \pm5, \pm3, \pm1\}.$$

The 16 possible values of $\Delta\left|\left(f_{0\oplus1}^{\prime(16)}(k)\right)_{i=0}^{7}\right|$ correspond to the 16 possible values of $(b(129k+4+i))_{i=0}^{3}$. Choosing another plaintext differential such that

- $\left|f_{0\oplus1}^{(16)}(k,i)\right| - \left|f_{0\oplus1}^{(16)}(k,i+8)\right| = 0$ for $i = 0,\ 1,\ 2,\ 3$;
- $\left|f_{0\oplus1}^{(16)}(k,i)\right| - \left|f_{0\oplus1}^{(16)}(k,i+8)\right| = \pm4, \pm5, \pm6, \pm8$ for $i = 4,\ 5,\ 6,\ 7$, respectively,

we will be able to uniquely determine the other four controlling bits $(b(129k+4+i))_{i=4}^{7}$. As a whole, with only two chosen plaintext differentials, we can uniquely determine all the eight controlling bits $(b(129k+4+i))_{i=0}^{7}$.

3.2.3. Breaking the other part of MCS

For the kth block, denote the intermediate result of the first 8-byte-swapping operations by $\overline{f^{*(16)}(k)}$. Knowing $b(129k+4) \sim b(129k+11)$ allows us to choose $\overline{f_{0\oplus1}^{*(16)}(k)}$ by manipulating $f_{0\oplus1}^{(16)}(k)$. The other encryption operations to be further broken include the 9th to 35th byte-swapping operations, the value masking, and the horizontal/vertical bit rotations.

Different from the first 8 byte-swapping operations, the 9th to 35th ones in *Step (b)* only shuffle the locations of the 8-bytes inside each half-block. We found these byte-swapping operations cannot be uniquely determined, because some equivalent but different encryption operations exist. Roughly speaking, if we add an overall circularly byte shift operation to *Step (b)* and all the other steps afterwards, we will get an encryption scheme equivalent to but different from the real one. Therefore, in this sub-subsection we turn to find such an equivalent encryption scheme. To facilitate our discussion, in the following, we use the acronym "EES" to denote the equivalent encryption scheme that has the same encryption performance as all the four kinds of encryption operations to be further broken. The EES is also composed of four parts, which correspond to the four different kinds of encryption operations, respectively. Once again, we use a divide-and-conquer tactic to get all the four pars of an EES.

3.2.3.1. Obtaining the vertical bit-rotation part of the EES. To get the vertical bit-rotation part, we need to cancel the horizontal bit-rotation part and the byte-swapping part. The horizontal bit rotations can be done by choosing all bytes in $\overline{f_{0\oplus1}^{*(16)}(k)}$ to be either 0 or 255, i.e., all the bits in M_1 and M_2 are identical (either 0 or 1). The byte-swapping operations cannot be fully canceled. To minimize its interference with the vertical bit-rotation part, we can choose each half-block such that there is only one 0 or one 255. Without loss of generality, we choose one plaintext differential such that both half-blocks of each 16-byte block $\overline{f_{0\oplus1}^{*(16)}(k)}$ contains only one 255-byte but seven 0-bytes, i.e.,

$$\left(\overline{f_{0\oplus1}^{*(16)}(k,i)}\right)_{i=0}^{7} = \left(\overline{f_{0\oplus1}^{*(16)}(k,i)}\right)_{i=8}^{15} = (\overbrace{0,\ldots,0}^{a\ \text{zeros}},255,0,\ldots,0).$$

After the byte-swapping operations, assume $\overline{f_{0\oplus1}^{*(16)}(k,a)}$ is moved to $f_{0\oplus1}^{*(16)}(k,\tilde{s}_{1,k,a})$ and $\overline{f_{0\oplus1}^{*(16)}(k,8+a)}$ to $f_{0\oplus1}^{*(16)}(k,8+\tilde{s}_{2,k,a})$, where $\tilde{s}_{1,k,a}$, $\tilde{s}_{2,k,a} \in \{0,\ldots,7\}$. Since the horizontal bit rotations are canceled, by comparing $\left(\overline{f_{0\oplus1}^{*(16)}(k,i)}\right)_{i=0}^{7}$ and $\left(f_{0\oplus1}^{\prime(16)}(k,i)\right)_{i=0}^{7}$, we can observe that $RotateY^{0,\bar{s}_{1,k,j}+\tilde{s}_{1,k,a}}$ is performed for the jth bit of $\overline{f_{0\oplus1}^{*(16)}(k,0)}$. Similarly, for the second half-block, we can observe that $RotateY^{0,\bar{s}_{2,k,j}+\tilde{s}_{2,k,a}}$ is performed for the jth bit of $\overline{f_{0\oplus1}^{*(16)}(k,8)}$.

3.2.3.2. Obtaining the horizontal bit-rotation part of the EES. Now, we need to cancel the byte-swapping operations and the vertical bit rotations. The byte-swapping operations can be canceled by choosing a second plaintext differential such that all the bytes in each half-block are identical. To distinguish the horizontal bit shifts, we should choose the byte $x \in \{0,\ldots,255\}$ to satisfy the following property: $a_1 \not\equiv a_2 \bmod 8 \iff (x \ggg a_1) \neq (x \ggg a_2)$, or equivalently, $a_1 \equiv a_2 \bmod 8 \iff (x \ggg a_1) = (x \ggg a_2)$. The simplest choice of x is 2^i, where $i \in \{0,\ldots,7\}$. When $f^{(16)}(k,15) = temp$, either $\overline{f_{0\oplus1}^{*(16)}}(k,7)$ or $\overline{f_{0\oplus1}^{*(16)}}(k,15)$ will always be 0, so it will not be possible to obtain the horizontal bit-rotation part for this byte. Fortunately, this does not influence the decryption process, because the expanded byte is actually redundant and will be finally discarded. The vertical bit rotations cannot be canceled, since they are performed after the horizontal bit rotations. Since we have obtained the vertical bit-rotation part of the EES, we can apply it to $\left(f_{0\oplus1}^{\prime(16)}(k,i)\right)_{i=0}^{7}$ to get $\left(f_{0\oplus1}^{\star(16)}(k,i\dot{+}\tilde{s}_{1,k,a})\right)_{i=0}^{7}$, where $\dot{+}$ denotes addi-

Please cite this article in press as: Li, C., et al. A differential cryptanalysis of Yen–Chen–Wu multimedia cryptography system. J. Syst. Software (2010), doi:10.1016/j.jss.2010.02.039

tion modulo 8. Then, compare $\left(f^{\star(16)}_{0\oplus1}(k,i\dot{+}\tilde{s}_{1,k,a})\right)_{i=0}^{7}$ with $\left(\overline{f^{*(16)}_{0\oplus1}}(k,i)\right)_{i=0}^{7}$, one can observe that $RotateX^{0,\bar{r}_{1,k,(i\dot{+}\tilde{s}_{1,k,a})}}$ is performed for $\overline{f^{*(16)}_{0\oplus1}}(k,i)$. Similarly, we can observe $RotateX^{0,\bar{r}_{2,k,(i\dot{+}\tilde{s}_{2,k,a})}}$ is performed for $\overline{f^{*(16)}_{0\oplus1}}(k,8+i)$.

3.2.3.3. Obtaining the byte-swapping part of the EES. After obtaining the horizontal/vertical bit-rotation parts of the EES, we can apply the inverse horizontal/vertical bit rotations to $\left(f'^{(16)}_{0\oplus1}(k,j)\right)_{j=0}^{15}$ to get $\left(f^{*(16)}_{0\oplus1}(k,\tilde{s}_{1,k,a}\dot{+}i)\right)_{i=0}^{7}$ and $\left(f^{*(16)}_{0\oplus1}(k,8+(\tilde{s}_{2,k,a}\dot{+}i))\right)_{i=0}^{7}$. If we choose $f^{*(16)}_{0\oplus1}(k)$ such that all the 8-bytes of each half-block are different from each other, we will be able to obtain the following byte-swapping part of the EES. For the first half-block, the real byte-swapping operation moves $\overline{f^{*(16)}_{0\oplus1}}(k,i)$ to $f^{*(16)}_{0\oplus1}(k,\hat{s}_{1,k,i})$, the one we obtained for the EES will move it to $f^{*(16)}_{0\oplus1}(k,\hat{s}_{1,k,i}\dot{-}\tilde{s}_{1,k,a})$, where $\dot{-}$ denotes subtraction modulo 8. Similarly, for the second half-block, the real byte-swapping operation moves $\overline{f^{*(16)}_{0\oplus1}}(k,8+i)$ to $f^{*(16)}_{0\oplus1}(k,8+\hat{s}_{2,k,i})$, the one we obtained for the EES will move it to $f^{*(16)}_{0\oplus1}(k,8+(\hat{s}_{2,k,i}\dot{-}\tilde{s}_{2,k,a}))$.

3.2.3.4. Obtaining the value masking part of the EES. After obtaining the byte-swapping part of the EES, we can get $\{f^{*(16)}(k,i\dot{+}\tilde{s}_{1,k,a})\}_{i=0}^{7}$ and $\{f^{*(16)}(k,8+(i\dot{+}\tilde{s}_{1,k,a}))\}_{i=0}^{7}$ from any known plaintext. In addition, after obtaining both the horizontal and vertical bit-rotation parts, we can get $\{f^{**(16)}(k,i\dot{+}\tilde{s}_{1,k,a})\}_{i=0}^{7}$ and $\{f^{**(16)}(k,8+(i\dot{+}\tilde{s}_{1,k,a}))\}_{i=0}^{7}$ from any known ciphertext. We do not need to choose more plaintexts, but can simply reuse any chosen plaintext used in previous steps. Note that the value masking performed in *Step (c)* can be rewritten as the equivalent form: for $i=0,\ldots,15$,

$$f^{**(16)}(k,i)=f^{*(16)}(k,i)\oplus Seed^{*}(k,i), \tag{5}$$

where $Seed^{*}(k,i)=\sum_{j=0}^{7}Seed(k,j)_i\cdot 2^j$ and $Seed(k,j)_i$ is the i-th bit of $Seed(k,j)$. Then, by XORing $\{f^{*(16)}(k,i\dot{+}\tilde{s}_{1,k,a})\}_{i=0}^{7}$ and $\{f^{**(16)}(k,i\dot{+}\tilde{s}_{1,k,a})\}_{i=0}^{7}$, we can get $(Seed^{*}(k,i\dot{+}\tilde{s}_{1,k,a}))_{i=0}^{7}$. Similarly, by XORing $\{f^{*(16)}(k,8+(i\dot{+}\tilde{s}_{2,k,a}))\}_{i=0}^{7}$ and $\{f^{**(16)}(k,8+(i\dot{+}\tilde{s}_{2,k,a}))\}_{i=0}^{7}$, we can get $(Seed^{*}(k,8+(i\dot{+}\tilde{s}_{2,k,a})))_{i=0}^{7}$.

Observing the above four results, we can see all the fours parts of the ESS are related to the unknown parameters $\tilde{s}_{1,k,a}$ and $\tilde{s}_{2,k,a}$. If we choose different value of a in Section 3.2.3.1, we may have a different ESS. All the possible EESs are equivalent to each other (and to the real encryption scheme), so we can use any of them to decrypt any ciphertext encrypted with the same key, as long as the size of the ciphertext is not larger than N. In the next subsection, we will show the values of $\tilde{s}_{1,k,a}$ and $\tilde{s}_{2,k,a}$ can be uniquely determined if the sub-keys $\alpha_1,\ \alpha_2,\ \beta_1$ and β_2 satisfy some requirements.

3.2.4. Performance of the differential attack

To sum up, the differential attack outputs the following items as an equivalent key:

- for data expansion: $(l(k-1))_{1\leqslant k\leqslant N/15-1}$, which is equivalent to $(b(129(k-1)+i))_{\substack{1\leqslant k\leqslant N/15-1\\ 0\leqslant i\leqslant 3}}$;
- for the first 8-byte-swapping operations: $(b(129k+i))_{\substack{0\leqslant k\leqslant N/15-1\\ 4\leqslant i\leqslant 11}}$;
- for the vertical bit rotations:

$$\left(RotateY^{0,\bar{s}_{1,k,j}\dot{+}\tilde{s}_{1,k,a}}\right)_{\substack{0\leqslant k\leqslant N/15-1\\ 0\leqslant j\leqslant 7}}\quad\text{and}\quad\left(RotateY^{0,\bar{s}_{2,k,j}\dot{+}\tilde{s}_{2,k,a}}\right)_{\substack{0\leqslant k\leqslant N/15-1\\ 0\leqslant j\leqslant 7}};$$

- for the horizontal bit rotations:

$$\left(RotateX^{0,\bar{r}_{1,k,(i\dot{+}\tilde{s}_{1,k,a})}}\right)_{\substack{0\leqslant k\leqslant N/15-1\\ 0\leqslant j\leqslant 7}}\quad\text{and}\quad\left(RotateX^{0,\bar{r}_{2,k,(i\dot{+}\tilde{s}_{2,k,a})}}\right)_{\substack{0\leqslant k\leqslant N/15-1\\ 0\leqslant j\leqslant 7}};$$

- for the 9th to 35th byte-swapping operations:

$$\left\{\overline{f^{*(16)}_{0\oplus1}}(k,i)\to f^{*(16)}_{0\oplus1}(k,\hat{s}_{1,k,i}\dot{-}\tilde{s}_{1,k,a})\right\}_{\substack{0\leqslant k\leqslant N/15-1\\ 0\leqslant i\leqslant 7}}\quad\text{and}\quad\left\{\overline{f^{*(16)}_{0\oplus1}}(k,8+i)\to f^{*(16)}_{0\oplus1}(k,8+(\hat{s}_{2,k,i}\dot{-}\tilde{s}_{2,k,a}))\right\}_{\substack{0\leqslant k\leqslant N/15-1\\ 0\leqslant i\leqslant 7}};$$

- for the value masking:

$$\left(Seed^{*}(k,(i\dot{+}\tilde{s}_{1,k,a}))\right)_{\substack{0\leqslant k\leqslant N/15-1\\ 0\leqslant i\leqslant 7}}\quad\text{and}\quad\left(Seed^{*}(k,8+(i\dot{+}\tilde{s}_{1,k,a}))\right)_{\substack{0\leqslant k\leqslant N/15-1\\ 0\leqslant i\leqslant 7}}.$$

All the above items form an encryption system equivalent to MCS and can be used to decrypt any ciphertexts encrypted with the same secret key. The (equivalent) encryption operations performed on some expanded bytes $f^{(16)}(k,15)$ may not be recovered, but which does not influence the effectiveness of the differential attack, since those expanded bytes will finally be discarded.

The total number of chosen plaintexts is the sum of the following: (a) two differentials for breaking the data expansion; (b) two differentials for breaking the first 8-byte-swapping operations; (c) four differentials for obtaining the EES. Note that the plaintext differential needed in Section 3.2.3.3 can be replaced by the two differentials in Section 3.2.1. So, we only need two more differentials for obtaining the EES. As a whole, the differential attack requires $2+2+2=6$ plaintext differentials, or seven plaintexts, to break MCS.

The complexity of the differential attack is also very small. In each step, the equivalent sub-key can be directly derived from the plaintext and the ciphertext, so the complexity is proportional to the size of the plaintext, N. With 6 chosen plaintext differentials, the computational complexity of the attack is just $O(6N)=O(N)$, which is the same as that of the normal encryption/decryption process of MCS.

3.3. Breaking some sub-keys and more controlling bits

The differential attack described in the previous subsection outputs an equivalent key, which include some controlling bits $(b(129k+i))_{i=0}^{11}$, but does not include any part of the secret key. In this subsection, we show we may further derive more controlling bits and the following four sub-keys: $\alpha_1,\ \beta_1,\ \alpha_2$ and β_2. Although we have not found a way to break the underlying pseudorandom bit generator (PRBG) and then break the sub-key $x(0)$, breaking more controlling bits makes it easier to analyze more potential weaknesses of the PRBG and opens the door to a successful cryptanalysis in future.

We first try to break the two sets $\mathbb{R}_1=\{\alpha_1,8-\alpha_1,\alpha_1+\beta_1,8-(\alpha_1+\beta_1)\}$ and $\mathbb{R}_2=\{\alpha_2,8-\alpha_2,\alpha_2+\beta_2,8-(\alpha_2+\beta_2)\}$. Then, we may be able to further determine sub-keys $\alpha_1,\ \beta_1,\ \alpha_2,\ \beta_2,\ \tilde{s}_{1,k,a}$, $\tilde{s}_{2,k,a}$, and more controlling bits.

Please cite this article in press as: Li, C., et al. A differential cryptanalysis of Yen–Chen–Wu multimedia cryptography system. J. Syst. Software (2010), doi:10.1016/j.jss.2010.02.039

3.3.1. Breaking $\mathbb{R}_1$ and $\mathbb{R}_2$

In the differential attack, what we have obtained for the horizontal bit rotations are $(RotateX^{0,\bar{r}_{1,k,(i\dotplus\tilde{s}_{1,k,a})}})_{0\leqslant k\leqslant N/15-1,\ 0\leqslant j\leqslant 7}$ and $(RotateX^{0,\bar{r}_{2,k,(i\dotplus\tilde{s}_{2,k,a})}})_{0\leqslant k\leqslant N/15-1,\ 0\leqslant j\leqslant 7}$. According to how $\bar{r}_{1,k,i}$ and $\bar{r}_{1,k,i}$ are determined, it is obvious that

$$\mathbb{R}_{1,k}=\{\bar{r}_{1,k,(i\dotplus\tilde{s}_{1,k,a})}\}_{i=0}^{7}\subseteq\mathbb{R}_1\quad\text{and}\quad\mathbb{R}_{2,k}=\{\bar{r}_{2,k,(i\dotplus\tilde{s}_{2,k,a})}\}_{i=0}^{7}\subseteq\mathbb{R}_2.$$

Assuming the secret bits controlling $(\bar{r}_{1,k,i})_{i=0}^{7}$ and $(\bar{r}_{2,k,i})_{i=0}^{7}$ distribute uniformly over $\{0,1\}$, set $p=1/2$ and $n=8\cdot N/15$ in Proposition 1, we can get

$$\mathrm{Prob}\left(\mathbb{R}_1\neq\bigcup_{\substack{0\leqslant k\leqslant N/15-1\\0\leqslant i\leqslant 7}}\left\{\bar{r}_{1,k,(i\dotplus\tilde{s}_{1,k,a})},8-\bar{r}_{1,k,(i\dotplus\tilde{s}_{1,k,a})}\right\}\right)=\frac{1}{2}^{8\cdot N/15}+\left(1-\frac{1}{2}\right)^{8\cdot N/15}=1/2^{8N/15-1}$$

and

$$\mathrm{Prob}\left(\mathbb{R}_2\neq\bigcup_{\substack{0\leqslant k\leqslant N/15-1\\0\leqslant i\leqslant 7}}\left\{\bar{r}_{2,k,(i\dotplus\tilde{s}_{2,k,a})},8-\bar{r}_{2,k,(i\dotplus\tilde{s}_{2,k,a})}\right\}\right)=1/2^{8N/15-1}.$$

Since $8N/15-1$ is generally very large, the above two probability is extremely small, which means that $\mathbb{R}_1$ and $\mathbb{R}_2$ can be uniquely determined with very high probability.

Proposition 1. *Assume $1\leqslant\beta\leqslant 7$, $1\leqslant\alpha<\alpha+\beta\leqslant 7$ and $\mathbb{R}=\{\alpha,8-\alpha,\alpha+\beta,8-(\alpha+\beta)\}$. If for $i=1,\ldots,n$, random variable $r_i\in\mathbb{Z}$ satisfies $\mathrm{Prob}(r_i\in\{\alpha,8-\alpha\})=p$, then*

$$\mathrm{Prob}\left(\mathbb{R}\neq\bigcup_{i=1}^{n}\{r_i,8-r_i\}\right)=\begin{cases}0, & 2\alpha+\beta=8,\\ 1, & 2\alpha+\beta\neq 8\text{ and }n=1,\\ p^n+(1-p)^n, & 2\alpha+\beta\neq 8\text{ and }n\geqslant 2.\end{cases}$$

Proof. When $2\alpha+\beta=8$, we can get $\alpha=8-(\alpha+\beta)$ and $8-\alpha=\alpha+\beta$, which leads to $\mathbb{R}=\{\alpha,8-\alpha\}=\{\alpha+\beta,8-(\alpha+\beta)\}$. Hence, we can immediately get $\{r_i,8-r_i\}=\mathbb{R}$ and then $\bigcup_{i=1}^{n}\{r_i,8-r_i\}=\mathbb{R}$. This means that $\mathrm{Prob}(\mathbb{R}\neq\bigcup_{i=1}^{n}\{r_i,8-r_i\})=0$.

When $2\alpha+\beta\neq 8$, we have $\alpha\neq 8-(\alpha+\beta)$ and $8-\alpha\neq\alpha+\beta$. Since $\alpha\neq\alpha+8$ and $8-\alpha\neq 8-(\alpha+\beta)$, there are only the following $\binom{4}{2}-4=2$ pairs of elements that may be equal to each other to make $\#(\mathbb{R})<4$, where $\#(\cdot)$ denotes the cardinality of a set:

- $\alpha=8-\alpha:\ \alpha=4\Rightarrow 1\leqslant\beta\leqslant 3$ and $\mathbb{R}=\{4,4,4+\beta,4-\beta\}\Rightarrow\#(\mathbb{R})=3$;
- $\alpha+\beta=8-(\alpha+\beta):\ \alpha+\beta=4\Rightarrow 1\leqslant\alpha\leqslant 3$ and $\mathbb{R}=\{\alpha,8-\alpha,4,4\}\Rightarrow\#(\mathbb{R})=3$.

In case no any two elements in $\mathbb{R}$ are equal to each other, it is obvious that $\#(\mathbb{R})=4$. As a whole, we have $\#(\mathbb{R})\geqslant 3$. Then, when $n=1$, the proposition is obviously true since $\#(\{r_i,8-r_i\})<3\leqslant\#(\mathbb{R})$. When $n\geqslant 2$, we can see there are only two ways to make $\mathbb{R}\neq\bigcup_{i=1}^{n}\{r_i,8-r_i\}$:

- $\bigcup_{i=1}^{n}\{r_i,8-r_i\}=\{\alpha,8-\alpha\}$, which occurs with probability p^n;
- $\bigcup_{i=1}^{n}\{r_i,8-r_i\}=\{\alpha+\beta,8-(\alpha+\beta)\}$, which occurs with probability $(1-p)^n$.

As a whole, we have $\mathrm{Prob}(\mathbb{R}\neq\bigcup_{i=1}^{n}\{r_i,8-r_i\})=p^n+(1-p)^n$.

Combining the above three different cases, the proposition is thus proved. □

3.3.2. Determining sub-keys α_1, β_1, α_2 and β_2

After getting $\mathbb{R}_1$ and $\mathbb{R}_2$, the four sub-keys α_1, β_1, α_2 and β_2 may be uniquely determined. Following a similar process of the proof of Proposition 1, we consider the following three cases for $m=1,2$:

- $\#(\mathbb{R}_m)=2$: This case happens only when $2\alpha_m+\beta_m=8$. There are three possible sets $\mathbb{R}_m=\{1,7\},\ \{2,6\},\ \{3,5\}$, which corresponds to $(\alpha_m,\beta_m)=(1,6),\ (2,4),\ (3,2)$, respectively. Apparently, knowing $\mathbb{R}_m$ allows us to uniquely determine the values of α_m and β_m.
- $\#(\mathbb{R}_m)=3$: This case happens when $\alpha_m=8-\alpha_m=4$ or $\alpha_m+\beta_m=8-(\alpha_m+\beta_m)=4$. There are only three possible sets $\mathbb{R}_m$, each of which corresponds to two possible values of (α_m,β_m):
  - $\mathbb{R}_m=\{4,1,7\}:\ (\alpha_m,\beta_m)=(4,3)$ or $(1,3)$;
  - $\mathbb{R}_m=\{4,2,6\}:\ (\alpha_m,\beta_m)=(4,2)$ or $(2,2)$;
  - $\mathbb{R}_m=\{4,3,5\}:\ (\alpha_m,\beta_m)=(4,1)$ or $(3,1)$.

  It can be seen that α_m and β_m cannot be uniquely determined in this case.
- $\#(\mathbb{R}_m)=4$: This case includes three possible sets $\mathbb{R}_m$, each of which corresponds to four different values of (α_m,β_m):
  - $\mathbb{R}_m=\{1,2,6,7\}:\ (\alpha_m,\beta_m)=(1,1),\ (1,5),\ (2,5)$ or $(6,1)$;
  - $\mathbb{R}_m=\{1,3,5,7\}:\ (\alpha_m,\beta_m)=(1,2),\ (1,4),\ (3,4)$ or $(5,2)$;
  - $\mathbb{R}_m=\{2,3,5,6\}:\ (\alpha_m,\beta_m)=(2,1),\ (2,3),\ (3,3)$ or $(5,1)$.

3.3.3. Determining $\tilde{s}_{1,k,a}$ and $\tilde{s}_{2,k,a}$

In the differential attack, what we have obtained for the vertical bit rotations are

$$(RotateY^{0,\bar{s}_{1,k,j}\dotplus\tilde{s}_{1,k,a}})_{\substack{0\leqslant k\leqslant N/15-1\\0\leqslant j\leqslant 7}}\text{and}(RotateY^{0,\bar{s}_{2,k,j}\dotplus\tilde{s}_{2,k,a}})_{\substack{0\leqslant k\leqslant N/15-1\\0\leqslant j\leqslant 7}}.$$

According to how $\bar{s}_{1,k,j}$ and $\bar{s}_{2,k,j}$ are determined in the encryption process, we can get $\mathbb{S}_{1,k}=\{\bar{s}_{1,k,j}\dotplus\tilde{s}_{1,k,a}\}_{j=0}^{7}\subseteq\mathbb{S}_1=\{\alpha_1\dotplus\tilde{s}_{1,k,a},8-\alpha_1\dotplus\tilde{s}_{1,k,a},\alpha_1+\beta_1\dotplus\tilde{s}_{1,k,a},8-(\alpha_1+\beta_1)\dotplus\tilde{s}_{1,k,a}\}$ and $\mathbb{S}_{2,k}=\{\bar{s}_{2,k,j}\dotplus\tilde{s}_{2,k,a}\}_{j=0}^{7}\subseteq\mathbb{S}_2=\{\alpha_2\dotplus\tilde{s}_{2,k,a},8-\alpha_2\dotplus\tilde{s}_{2,k,a},\alpha_2+\beta_2\dotplus\tilde{s}_{2,k,a},8-(\alpha_2+\beta_2)\dotplus\tilde{s}_{2,k,a}\}$. Comparing $\mathbb{S}_1$, $\mathbb{S}_2$ with $\mathbb{R}_1$, $\mathbb{R}_2$, we may be able to determine the values of $\tilde{s}_{1,k,a}$ and $\tilde{s}_{2,k,a}$. There are four different cases:

- $\mathbb{S}_{m,k}\subset\mathbb{S}_m$: If $\mathbb{S}_{m,k}$ does not contain all elements in $\mathbb{S}_m$, it is generally impossible to uniquely determine $\tilde{s}_{m,k,a}$. From Proposition 1, the occurrence probability of this case is $2/2^8=1/2^7$.
- $\mathbb{S}_{m,k}=\mathbb{S}_m$ and $\mathbb{R}_m=\{2,6\}$: When $\tilde{s}_{m,k,a}\in\{1,2,3,5,6,7\}$, its value can be uniquely determined. When $\tilde{s}_{m,k,a}=0$ or 4, it is impossible to distinguish one value from the other.
- $\mathbb{S}_{m,k}=\mathbb{S}_m$ and $\mathbb{R}_m=\{1,7\},\{3,5\},\{4,1,7\},\{4,2,6\},\{4,3,5\},\{1,2,6,7\}$ or $\{2,3,5,6\}$: The value of $\tilde{s}_{m,k,a}$ can always be uniquely determine.
- $\mathbb{S}_{m,k}=\mathbb{S}_m$ and $\mathbb{R}_m=\{1,3,5,7\}$: The value of $\tilde{s}_{m,k,a}$ can never be uniquely determined. One can only determine which of the following two sets $\tilde{s}_{m,k,a}$ belongs to: $\{0,2,4,6\}$ and $\{1,3,5,7\}$.

Assuming the value of $\tilde{s}_{m,k,a}$ distributes uniformly over $\{0,\ldots,7\}$, the probability that each $\tilde{s}_{m,k,a}$ cannot be uniquely determined is $1/2^7+(1-1/2^7)((1/21)(2/8)+4/21)\approx 0.2086$. We may choose more different values of a in Section 3.2.3.1 to decrease this probability, but the probability has a lower bound $1/2^7+(1-1/2^7)(4/21)\approx 0.1968$. We can see this probability is always not sufficiently small, so we will not be able to uniquely determine the value of $\tilde{s}_{1,k,a}$ or that of $\tilde{s}_{2,k,a}$ for quite a lot of blocks.

Please cite this article in press as: Li, C., et al. A differential cryptanalysis of Yen–Chen–Wu multimedia cryptography system. J. Syst. Software (2010), doi:10.1016/j.jss.2010.02.039

3.3.4. Determining the secret bits controlling the 9th to 35th byte-swapping operations

In case $\tilde{s}_{1,k,a}$ and $\tilde{s}_{2,k,a}$ can be uniquely determined, we will be able to uniquely recover the 9th to 35th byte-swapping operations, i.e., we can determine the values of $(\hat{s}_{1,k,i})_{i=0}^{7}$ and $(\hat{s}_{2,k,i})_{i=0}^{7}$. Note $(\hat{s}_{1,k,i})_{i=0}^{7}$ and $(\hat{s}_{2,k,i})_{i=0}^{7}$ actually define two permutation maps over $\{0,\ldots,7\}$. Observing the 9th to 35th byte-swapping operations in *Step (b)*, one can notice that the permutation maps has a strong pattern: 12 byte-swapping operations for the first half-block and the other 12 ones for the second half-block, and each group of 12 byte-swapping operations can be divided into three phases. For the 12 byte-swapping operations performed on the first half-block, the three phases are as follows:

- *Phase 1*: $(i,j,a) = (0,4,12), (1,5,13), (2,6,14), (3,5,15)$;
- *Phase 2*: $(i,j,a) = (0,2,20), (1,3,21), (4,6,22), (5,7,23)$;
- *Phase 3*: $(i,j,a) = (0,1,28), (2,3,29), (4,5,30), (6,7,31)$.

Apparently, Phase 1 swaps the bytes in the two 4-byte quarter-block of the first 8-byte half-block, and Phases 2 and 3 only permute the bytes with each 4-byte quarter-block. Then, for $i = 0, 1, 2, 3$, we can check in which quarter-block $\overline{f^{(*16)}}(k,i)$ belongs to after the byte-swapping operations. In other words, we check if $\hat{s}_{1,k,i} \in \{0,1,2,3\}$ or $\{4,5,6,7\}$, which corresponds to $b(129k+12+i) = 0$ and 1, respectively. This allows us to completely determine $(b(129k+12+i))_{i=0}^{3}$, i.e., to break Phase 1. Then, we can derive a new permutation map represented by $(\hat{s}^*_{1,k,i})_{i=0}^{7}$, which consists of only Phases 2 and 3. Then, according to the byte-swapping operations involved in Phases 2 and 3, we can derive the following rule to break the 4 controlling bits involved in Phase 2:

- when $i = 0,1$: $b(129k+20+i) = \begin{cases} 0, & \hat{s}^*_{1,k,i} \in \{0,1\}, \\ 1, & \hat{s}^*_{1,k,i} \in \{2,3\}; \end{cases}$
- when $i = 2,3$: $b(129k+20+i) = \begin{cases} 0, & \hat{s}^*_{1,k,i} \in \{4,5\}, \\ 1, & \hat{s}^*_{1,k,i} \in \{6,7\}. \end{cases}$

After breaking both Phases 1 and 2, we can immediately break the 4 controlling bits $(b(129k+28+i))_{i=0}^{3}$ involved in Phase 3. Now, we completely break all the 12 controlling bits involved in the byte-swapping operations performed on the first half-block. The same process can be applied to the second half-block, and 12 controlling bits can be uniquely determined. As a whole, we will be able to break all the 24 controlling bits $(b(129k+i))_{i=12}^{35}$.

3.3.5. Determining the secret bits controlling value masking

In case $\tilde{s}_{1,k,a}$ and $\tilde{s}_{2,k,a}$ can be uniquely determined as described in Section 3.3.3, we will be able to determine $(Seed^*(k,j))_{j=0}^{15}$, or equivalently, $(Seed(k,j))_{j=0}^{8}$. This allows us to obtain $\{Seed(k,j)\}_{j=0}^{8} \subseteq \{Seed1(k), \overline{Seed1}(k), Seed2(k), \overline{Seed2}(k)\}$. To break the controlling bits, we need to recover $Seed1(k)$ and $Seed2(k)$, which are calculated from $(b(129k+i))_{i=0}^{63}$ and $(b(129k+64+i))_{i=0}^{63}$, respectively. Note that we can always break $(b(129k+i))_{i=0}^{35}$ if $\tilde{s}_{1,k,a}$ and $\tilde{s}_{2,k,a}$ are uniquely determined. This means that we can break the 36/4 = 9 least significant bits (LSBs) of $Seed1(k)$, since each bit of $Seed1(k)$ is determined by four controlling bits. Then, if the nine LSBs of $Seed1(k)$ are not all equal to those of $Seed2(k)$ or those of $\overline{Seed2}(k)$, we can uniquely determine $Seed1(k)$ and then $\overline{Seed1}(k)$. Assuming $Seed1(k)$ and $Seed2(k)$ are independent of each other and each bit distributes uniformly over $\{0,1\}$, the probability that $Seed1(k)$ cannot be uniquely determined is $2/2^9 = 1/2^8$. In case $Seed1(k)$ is uniquely determined, we have the following results:

- when $Seed(k,j) \in \{Seed1(k), \overline{Seed1}(k)\}$:

$$b(129k+36+2j) = 1;\quad b(129k+37+2j) = \begin{cases} 0, & Seed(k,j) = \overline{Seed1}(k), \\ 1, & Seed(k,j) = Seed1(k); \end{cases}$$

- when $Seed(k,j) \in \{Seed2(k), \overline{Seed2}(k)\}$:

$$b(129k+36+2j) = 1;\quad b(129k+37+2j) = \begin{cases} 0, & Seed(k,j) = \overline{Seed2}(k), \\ 1, & Seed(k,j) = Seed2(k). \end{cases}$$

Note that in this case, $Seed2(k)$ has to be guessed from the set $\{Seed2(k), \overline{Seed2}(k)\}$.

3.3.6. Determining the secret bits controlling horizontal/vertical bit rotations

In case $\tilde{s}_{1,k,a}$ and $\tilde{s}_{2,k,a}$ can be uniquely determined as described in Section 3.3.3, we will be able to uniquely determine the horizontal and vertical bit rotations exerted on $\mathbf{M}_1$, $\widetilde{\mathbf{M}}_1$, $\mathbf{M}_2$ and $\widetilde{\mathbf{M}}_2$. Depending on how well the values of α_1, β_1, α_2, β_2 are determined in Section 3.3.2, some information about the controlling bits involved in the bit rotations may be obtained, although it is always impossible to uniquely determine the value of any controlling bit involved. Since the determination process of the controlling bits are similar for $\mathbf{M}_1$, $\widetilde{\mathbf{M}}_1$, $\mathbf{M}_2$ and $\widetilde{\mathbf{M}}_2$, here we consider only the case of $\mathbf{M}_1$ (i.e., horizontal bit rotations exerted on the first half-block) to simplify the discussion. For this case, we get $(\bar{r}_{1,k,i})_{i=0}^{7}$ by substituting $\tilde{r}_{1,k,a}$ into $(\bar{r}_{1,k,(i+\tilde{r}_{1,k,a})})_{i=0}^{7}$. In *Step (d)*, $\bar{r}_{1,k,i}$ is determined by two controlling bits as follows:

$$\bar{r}_{1,k,i} = \begin{cases} \alpha_1, & (b(129k+65+2i), b(129k+66+2i)) = (0,0), \\ \alpha_1+\beta_1, & (b(129k+65+2i), b(129k+66+2i)) = (0,1), \\ 8-\alpha_1, & (b(129k+65+2i), b(129k+66+2i)) = (1,0), \\ 8-(\alpha_1+\beta_1), & (b(129k+65+2i), b(129k+66+2i)) = (1,1). \end{cases}$$

We have the following different cases.

- $\mathbb{R}_1 = \{1,7\}, \{2,6\}$ or $\{3,5\}$: In this case, α_1 and β_1 can be uniquely determined, but we cannot differentiate α_1 from $8-(\alpha_1+\beta_1)$, and $8-\alpha_1$ from $\alpha_1+\beta_1$. Hence, we can determine neither $b(129k+65+2i)$ nor $b(129k+66+2i)$, but just the following:

$$(b(129k+65+2i), b(129k+66+2i)) = \begin{cases} (0,0) \text{ or } (1,1), & \bar{r}_{1,k,i} \in \{1,2,3\}, \\ (0,1) \text{ or } (1,0), & \bar{r}_{1,k,i} \in \{5,6,7\}. \end{cases}$$

- $\mathbb{R}_1 = \{4,1,7\}, \{4,2,6\}$ or $\{4,3,5\}$: In this case, (α_1,β_1) has two possible values, so $(b(129k+65+2i), b(129k+66+2i))$ cannot be uniquely determined. What we can get is the following:

$$(b(129k+65+2i), b(129k+66+2i)) = \begin{cases} (0,0) \text{ or } (1,1), & \bar{r}_{1,k,i} \in \{1,2,3\}, \\ (0,1) \text{ or } (1,0), & \bar{r}_{1,k,i} \in \{5,6,7\}, \\ (0,0), (0,1), (1,0) \text{ or } (1,1), & \bar{r}_{1,k,i} = 4. \end{cases}$$

- $\mathbb{R}_1 = \{1,2,6,7\}$: In this case, (α_1,β_1) has four possible values (1,1), (1,5), (2,5) or (6,1), so $(b(129k+65+2i), b(129k+66+2i))$ cannot be uniquely determined, either. What we can get is the following:

$$(b(129k+65+2i), b(129k+66+2i)) = \begin{cases} (0,0) \text{ or } (1,1), & \bar{r}_{1,k,i} = 1, \\ (0,1) \text{ or } (1,0), & \bar{r}_{1,k,i} = 7, \\ (0,0), (0,1), (1,0) \text{ or } (1,1), & \bar{r}_{1,k,i} \in \{2,6\}. \end{cases}$$

- $\mathbb{R}_1 = \{1,3,5,7\}$: In this case, (α_1,β_1) has four possible values (1,2), (1,4), (3,4) or (5,2), so $(b(129k+65+2i), b(129k+66+2i))$ cannot be uniquely determined, either. What we can get is the following:

Please cite this article in press as: Li, C., et al. A differential cryptanalysis of Yen–Chen–Wu multimedia cryptography system. J. Syst. Software (2010), doi:10.1016/j.jss.2010.02.039

$$(b(129k+65+2i), b(129k+66+2i)) = \begin{cases} (0,0) \text{ or } (1,1), & \bar{r}_{1,k,i}=1, \\ (0,1) \text{ or } (1,0), & \bar{r}_{1,k,i}=7, \\ (0,0),(0,1),(1,0) \text{ or } (1,1), & \bar{r}_{1,k,i}\in\{3,5\}. \end{cases}$$

- $\mathbb{R}_1=\{2,3,5,6\}$: In this case, (α_1,β_1) has four possible values $(2,1)$, $(2,3)$, $(3,3)$ or $(5,1)$, so $(b(129k+65+2i), b(129k+66+2i))$ cannot be uniquely determined, either. What we can get is the following:

$$(b(129k+65+2i), b(129k+66+2i)) = \begin{cases} (0,0) \text{ or } (1,1), & \bar{r}_{1,k,i}=2, \\ (0,1) \text{ or } (1,0), & \bar{r}_{1,k,i}=6, \\ (0,0),(0,1),(1,0) \text{ or } (1,1), & \bar{r}_{1,k,i}\in\{3,5\}. \end{cases}$$

3.3.7. Summary

As a brief summary, based on the equivalent key obtained in the differential attack, we can further determine $\mathbb{R}_1=\{\alpha_1, 8-\alpha_1, \alpha_1+\beta_1, 8-(\alpha_1+\beta_1)\}$ and $\mathbb{R}_2=\{\alpha_2, 8-\alpha_2, \alpha_2+\beta_2, 8-(\alpha_2+\beta_2)\}$ with a very high probability $1-1/2^{8N/15-1}$. Then, we may be able to uniquely determine the value of (α_m,β_m) $(m=1,2)$ with probability 3/21 = 1/7, or narrow down the number of possible values to 2 (with probability 6/21 = 2/7) or to 4 (with probability 12/21 = 4/7). Based on $\mathbb{R}_m$ $(m=1,2)$, we may be able to recover $\tilde{s}_{m,k,a}$ with probability $\geqslant 1-0.1968=0.8032$ (see Section 3.3.3). In case $\tilde{s}_{1,k,a}$ and $\tilde{s}_{2,k,a}$ are uniquely determined, we have the following results:

- Controlling bits $(b(129k+i))_{i=12}^{35}$ can always be uniquely determined.
- In case the value of $Seed1(k)$ can be recovered, which happens with probability $1-1/2^8$, the controlling bits $(b(129k+36+2j))_{j=0}^{7}$ can always be uniquely determined, but $(b(129k+37+2j))_{j=0}^{7}$ can be uniquely determined only when $Seed(k,j)\in\{Seed1(k), \overline{Seed1}(k)\}$.
- None of the controlling bits involved in the bit rotations can be uniquely determined, but we may be able to narrow down the number of possible values of the two controlling bits determining each bit-rotation operation from 4 to 2 in some cases.

3.4. Experimental results

To verify the real performance of the differential attack proposed in this paper, some experiments were carried out with the secret key used in Section 2. The plain-image shown in Fig. 1a is used as one of the chosen plaintext f_0 to generate the required chosen plaintext differentials. The two differentials used for breaking secret data expansion are shown in Fig. 2. The two differentials used for breaking the first 8-byte-swapping operations, i.e., the secret bits $\{b(129k+i)\}_{\substack{0\leqslant k\leqslant N/15-1\\ 0\leqslant k\leqslant 7}}$, are shown in Fig. 3. The two differentials shown in Fig. 4 and those two shown in Fig. 2 were used to obtain an EES. The recovered equivalent key (i.e., all the items shown in Section 3.2.4) was used to decrypt a cipher-image as shown in Fig. 5a. The result is given in Fig. 5b. It can be seen that the secret plain-image was successfully recovered by the differential attack. To show the breaking process more clearly, the

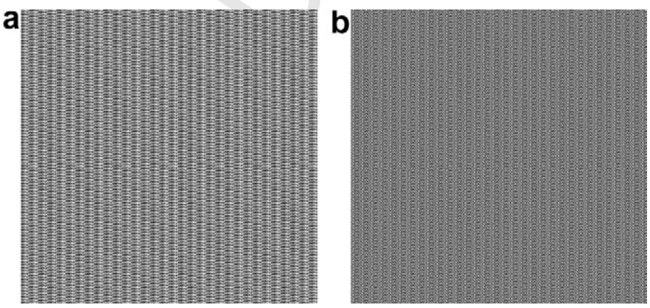

Fig. 2. The two plaintext differentials for breaking data expansion.

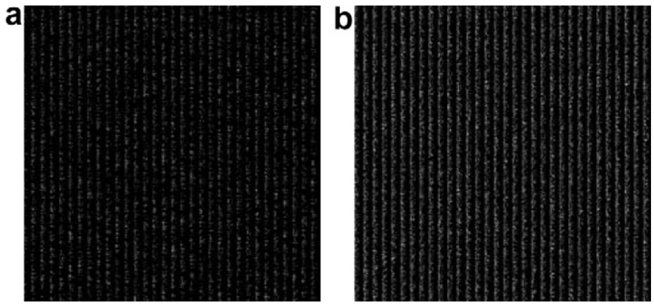

Fig. 3. The two plaintext differentials for breaking the first 8-byte-swapping operations.

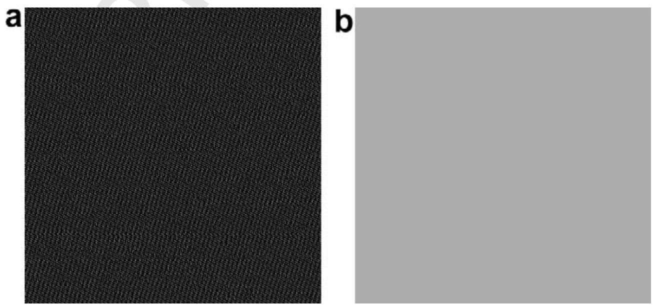

Fig. 4. The two plaintext differentials for obtaining the vertical and horizontal bit-operation part of the EES: (a) vertical bit-operation; (b) horizontal bit-operation.

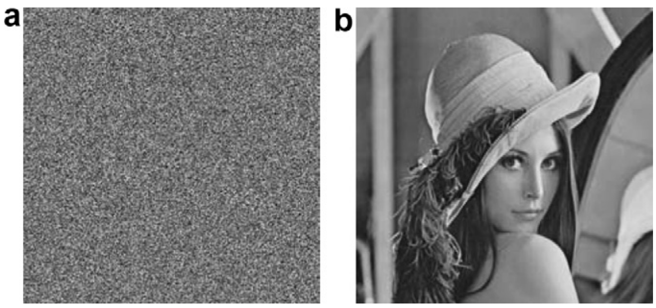

Fig. 5. The decryption result of another cipher-image encrypted with the same secret key: (a) cipher-image; (b) decrypted plain-image.

Table 2
The obtained items for breaking the second 16-byte block of the cipher-image shown in Fig. 1b.

Obtained items	The corresponding values
$l(1)$	5
$b(129+4)\sim b(129+11)$	2, 4, 6, 4, 6, 4, 6, 4
$\{\bar{s}_{1,1,j}\dot{+}\tilde{s}_{1,1,a}\}_{j=0}^{7}$	1, 5, 3, 5, 5, 3, 1, 1
$\{\bar{s}_{2,1,j}\dot{+}\tilde{s}_{2,1,a}\}_{j=0}^{7}$	2, 2, 6, 6, 6, 7, 6, 1
$\{\bar{r}_{1,1,j\dot{+}\tilde{s}_{1,1,a}}\}_{j=0}^{7}$	6, 2, 2, 6, 1, 6, 1, 2
$\{\bar{r}_{2,1,j\dot{+}\tilde{s}_{2,1,a}}\}_{j=0}^{7}$	7, 6, 1, 6, 7, 7, 1, 2
$\{\hat{s}_{1,1,j}\dot{-}\tilde{s}_{1,1,a}\}_{j=0}^{7}$	4, 3, 0, 5, 1, 2, 6, 7
$\{\hat{s}_{2,1,j}\dot{-}\tilde{s}_{2,1,a}\}_{j=0}^{7}$	4, 5, 3, 1, 0, 7, 6, 2
$\{Seed^*(1,(i\dot{+}\tilde{s}_{1,1,a}))\}_{i=0}^{7}$	55, 228, 200, 55, 200, 200, 200, 27
$\{Seed^*(1,8+(i\dot{+}\tilde{s}_{2,1,a}))\}_{i=0}^{7}$	27, 55, 228, 55, 27, 27, 27, 200

Please cite this article in press as: Li, C., et al. A differential cryptanalysis of Yen–Chen–Wu multimedia cryptography system. J. Syst. Software (2010), doi:10.1016/j.jss.2010.02.039

items determining the equivalent secret key of the second 16-byte block of cipher-image are shown in Table 2 also.

4. Conclusion

In this paper, we evaluate the security of a recently-proposed multimedia encryption system called MCS (Yen et al., 2005), and propose a differential attack to break it with a divide-and-conquer (DAC) strategy. The differential attack is very efficient in the sense that only seven chosen plaintexts are needed to get an equivalent key and the computational complexity is only $O(N)$, where N is the number of bytes in the plaintext. The real performance of the proposed attack was also verified with experiments. Similar to some other image encryption schemes proposed in the literature, the MCS was not designed by following some good principles of designing such systems. Some of these principles are discussed in (Alvarez and Li, 2006; Li et al., 2008b).

Acknowledgements

Chengqing Li was supported by The Hong Kong Polytechnic University's Postdoctoral Fellowships Scheme under Grant No. G-YX2L. Shujun Li was supported by a fellowship from the Zukunftskolleg of the University of Konstanz, Germany, which is part of the "Excellence Initiative" Program of the DFG (German Research Foundation). The work of Kwok-Tung Lo was supported by the Research Grant Council of the Hong Kong SAR Government under Project 523206 (PolyU 5232/06E).

References

Álvarez, G., Li, S., 2005. Breaking an encryption scheme based on chaotic baker map. Physics Letters A 352 (1-2), 78–82.
Alvarez, G., Li, S., 2006. Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos 16 (8), 2129–2151.
Arroyo, D., Rhouma, R., Alvarez, G., Li, S., Fernandez, V., 2008. On the security of a new image encryption scheme based on chaotic map lattices. Chaos 18 (3). Art. no. 03311.
Bourbakis, N., Alexopoulos, C., 1992. Picture data encryption using scan patterns. Pattern Recognition 25 (6), 567–581.
Chang, C.-C., Yu, T.-X., 2002. Cryptanalysis of an encryption scheme for binary images. Pattern Recognition Letters 23 (14), 1847–1852.
Chen, H.-C., Yen, J.-C., 2003. A new cryptography system and its VLSI realization. Journal of Systems Architecture 49 (7-9), 355–367.
Chen, H.-C., Guo, J.-I., Huang, L.-C., Yen, J.-C., 2003. Design and realization of a new signal security system for multimedia data transmission. EURASIP Journal on Applied Signal Processing 2003 (13), 1291–1305.
Chen, G., Mao, Y., Chui, C.K., 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals 21 (3), 749–761.
Chen, H.-C., Yen, J.-C., Juan, J.-H., Fan, K.-T., Wu, S.-M., 2007. A new cryptography system and its IP core design for multimedia application. In: Proceedings of IEEE International Symposium on Consumer Electronics, pp. 1–7.
Chung, K.-L., Chang, L.-C., 1998. Large encrypting binary images with higher security. Pattern Recognition Letters 19 (5-6), 461–468.
Flores-Carmona, N.J., Carpio-Valadez, M., 2006. Encryption and decryption of images with chaotic map lattices. Chaos 16 (3). Art. no. 03311.
Fridrich, J., 1998. Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and Chaos 8 (6), 1259–1284.
Guo, J.-I., Yen, J.-C., Pai, H.-F., 2002. New voice over internet protocol technique with hierarchical data security protection. IEE Proceedings – Vision Image and Signal Processing 149 (4), 237–243.
Jakimoski, G., Subbalakshmi, K., 2008. Cryptanalysis of some multimedia encryption schemes. IEEE Transactions on Multimedia 10 (3), 330–338.
Jan, J.-K., Tseng, Y.-M., 1996. On the security of image encryption method. Information Processing Letters 60 (5), 261–265.
Kim, H., Wen, J.T., Villasenor, J.D., 2007. Secure arithmetic coding. IEEE Transactions on Signal Processing 55 (5), C2263–C2272.
Kocarev, L., Jakimoski, G., 2003. Pseudorandom bits generated by chaotic maps. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 50 (1), 123–126.
Lian, S., Sun, J., Wang, Z., 2005. Security analysis of a chaos-based image encryption algorithm. Physica A: Statistical Mechanics and its Applications 351 (2-4), 645–661.
Li, C., Li, S., Chen, G., Chen, G., Hu, L., 2005. Cryptanalysis of a new signal security system for multimedia data transmission. EURASIP Journal on Applied Signal Processing 2005 (8), 1277–1288.
Li, C., Li, S., Lou, D.-C., 2006a. On the security of the Yen–Guo's domino signal encryption algorithm (DSEA). Journal of Systems and Software 79 (2), 253–258.
Li, C., Li, S., Zhang, D., Chen, G., 2006b. Cryptanalysis of a data security protection scheme for VoIP. IEE Proceedings – Vision Image and Signal Processing 153 (1), 1–10.
Li, S., Li, C., Chen, G., Bourbakis, N.G., Lo, K.-T., 2008a. A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Processing: Image Communication 23 (3), 212–223.
Li, S., Li, C., Chen, G., Mou, X., 2008b. Cryptanalysis of the RCES/RSES image encryption scheme. Journal of Systems and Software 81 (7), 1130–1143.
Li, C., Li, S., Asim, M., Nunez, J., Alvarez, G., Chen, G., 2009. On the security defects of an image encryption scheme. Image and Vision Computing 27 (9), 1371–1381.
Pareek, N., Patidar, V., Sud, K., 2006. Image encryption using chaotic logistic map. Image and Vision Computing 24 (9), 926–934.
Rhouma, R., Belghith, S., 2008. Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem. Physics Letters A 372 (36), 5790–5794.
Scharinger, J., 1998. Fast encryption of image data using chaotic Kolmogorov flows. Journal of Electronic Imaging 7 (2), 318–325.
Solak, E., 2005. Cryptanalysis of observer based discrete-time chaotic encryption schemes. International Journal of Bifurcation and Chaos 15 (2), 653–658.
Wang, K., Pei, W., Zou, L., Song, A., He, Z., 2005. On the security of 3D cat map based symmetric image encryption scheme. Physics Letters A 343, 432–439.
Wong, K.-W., Yuen, C.-H., XXXX. Embedding compression in chaos-based cryptography, IEEE Transactions on Circuits and Systems II: Express Brief 55(11). Q1
Wu, C.-P., Kuo, C.-C.J., 2005. Design of integrated multimedia compression and encryption systems. IEEE Transactions on Multimedia 7 (5), 828–839.
Xiao, D., Liao, X., Wong, K.-W., 2006. Improving the security of a dynamic look-up table based chaotic cryptosystem. IEEE Transactions on Circuits and Systems II: Express Briefs 53 (6), 502–506.
Yen, J.-C., Guo, J.-I., 2000. Efficient hierarchical chaotic image encryption algorithm and its VLSI realisation. IEE Proceedings – Vision Image and Signal Processing 147 (2), 167–175.
Yen, J.-C., Chen, H.-C., Wu, S.-M., 2005. Design and implementation of a new cryptographic system for multimedia transmission. In: Proceedings of IEEE International Symposium on Circuits and Systems, vol. 6, pp. 6126–6129.
Zhou, J., Liang, Z., Chen, Y., 2007. Security analysis of multimedia encryption schemes based on multiple Huffman table. IEEE Signal Processing Letters 14 (3), 201–204. A.O.C..
Zhou, J., Au, O.C., Wong, P.H.-W., 2009. Adaptive chosen-ciphertext attack on secure arithmetic coding. IEEE Transactions on Signal Processing 57 (5), 1825–1838.

Please cite this article in press as: Li, C., et al. A differential cryptanalysis of Yen–Chen–Wu multimedia cryptography system. J. Syst. Software (2010), doi:10.1016/j.jss.2010.02.039