Published in *Cryptologia*, Vol. XXVII, No. 4, October 2003.

Impossible Differential Cryptanalysis of Mini-AES

Raphael Chung-Wei **Phan**

ADDRESS: Swinburne Sarawak Institute of Technology, 1st Floor, State Complex, 93576 Kuching, Sarawak, Malaysia. rphan@swinburne.edu.my

ABSTRACT: Impossible differential cryptanalysis is one of the cryptanalysis methods that are applicable to the new Advanced Encryption Standard (AES). In this paper, we present an introduction to the method by applying it on Mini-AES, the mini version of the AES published in Cryptologia recently.

KEYWORDS: Advanced Encryption Standard, Rijndael, Mini-AES, Impossible Differential Cryptanalysis

1 Introduction

The Advanced Encryption Standard (AES) is the standard algorithm adopted by the National Institute of Standards and Technology (NIST) to replace the ageing Data Encryption Standard (DES) for encryption and protection of secure and non-classified information [1, 2]. The AES is expected to not only gain popular usage among the U.S but also among the international community, and will be implemented in various situations such as for the securing of online transactions, smart cards and dedicated hardware.

Foreseeing the importance of the AES, a mini version of the AES, Mini-AES was recently presented [3]. Mini-AES is proposed as a purely educational encryption algorithm to aid cryptography and cryptanalysis students to better understand the concepts behind the real AES. It is also intended that the Mini-AES be a testbed for cryptanalysis students to start their cryptanalytic efforts on. As an illustration, the Square attack was mounted on Mini-AES. This work is of great importance since there is an absence of suitable texts or reference books for field of cryptanalysis. Amateurs and aspirants new to the field have a hard time understanding the basic concepts from journal and conference papers which are the sole sources of cryptanalytic information.

In this paper, we extend on the effort by showing how another cryptanalysis method, the impossible differential cryptanalysis works. The impossible differential cryptanalysis is equally applicable to the AES, and we show the details step by step by mounting it on Mini-AES.

In section 2, we briefly describe Mini-AES. We introduce the notion of impossible differentials and apply it to an attack on Mini-AES in Section 3. We conclude in Section 4.

2 Mini-AES

In this section, we briefly describe Mini-AES. For further details, the reader should refer to [3]. Mini-AES is a 16-bit block cipher with a 16-bit secret key. It consists of 2 rounds, where each round is composed of 4 basic operations, namely *NibbleSub*, *ShiftRow*, *MixColumn* and *KeyAddition*. For ease of explanation of these operations, the 16-bit plaintext block, P is expressed as a matrix of 2 rows and 2 columns of nibbles (a nibble is 4 bits). Each nibble is denoted as a_{ij} where $i, j \in \{0,1\}$ are the row and column indices respectively. This is shown in Figure 1.

a_{00}	a_{01}
a_{10}	a_{11}

Figure 1: 2×2 Matrix Representation of the Mini-AES Block

The 16-bit block can sometimes also be expressed as a series of 4 nibbles, in which case, it is written as $a_{00}, a_{10}, a_{01}, a_{11}$. Note that in relating this to the matrix representation as in Figure 1, then the nibbles are read from the matrix column by column. When expressed as a series of 4 nibbles, then the leftmost nibble is referred to as the first nibble.

Example 1

Let P =

0100	*1110*
0011	*1001*

Then, we can also express P as P = 0100 0011 1110 1001. In this case, the first nibble is the leftmost nibble, which is 0100.

NibbleSub, γ substitutes each input nibble with an output nibble based on Table 1 of [3]. ShiftRow, π merely swaps the two nibbles in the second row, while the first row is left unchanged. MixColumn, θ takes each input column and multiplies it with a constant 2×2 matrix given in Figure 5 of [3] to obtain a new output column. Hence, each nibble in the output column depends on all the nibbles of the input column. KeyAddition, σ_{Ki} causes the 16-bit input block to be exclusive-ORed (XORed) with a 16-bit round key, K_i which is generated from the secret key.

In order to ensure that the same structure can be used for both encryption and decryption, an extra KeyAddition (called the 0^{th} round) is added prior to the first round, while MixColumn is removed from the last round.

In summary, the overall Mini-AES encryption is denoted by:

$$\text{Mini-AES}_{\text{Encrypt}} = \sigma_{K2} \circ \pi \circ \gamma \circ \sigma_{K1} \circ \theta \circ \pi \circ \gamma \circ \sigma_{K0}$$

3 Impossible Differential Cryptanalysis

The impossible differential cryptanalysis relies on finding an impossible event through a reduced part of a block cipher. Then, all possible secret keys are guessed, and those that suggest this impossible event are eliminated since the correct secret key would never cause such an event to occur. Currently, the most effective way of constructing an impossible event is by using the *miss-in-the-middle* technique, introduced by Biham et. al [4]. The miss-in-the-middle technique considers two events that always happen. By concatenating these events such that they cause a contradiction in the middle, an impossible event results.

3.1 A 4-round Impossible Differential of Mini-AES

Mini-AES has only 2 rounds [3], which makes it too trivial for an impossible differential attack, so we will consider more rounds of Mini-AES. In constructing an impossible event, we would like to have it cover as many rounds as possible. Nevertheless, similar to the case of the original AES [1, 2], 4 rounds is the maximum that an impossible event on Mini-AES

can cover. In this section, we will describe how such a 4-round impossible event is constructed.

Considering Mini-AES up to 4 rounds, suppose we choose two plaintexts, P and P' such that they differ in only one nibble and are equal in the other nibbles.

Example 2a

Let P = 0100 0011 1110 1001
P' = 1110 0011 1110 1001

The nibble in which P and P' differ is called the *active* nibble whereas the nibble in which they are equal is called a *passive* nibble. Hence, in Example 2a, there is one active nibble (the leftmost nibble) and three passive nibbles.

Let's observe how these two plaintexts behave as they go through the round components of Mini-AES.

Example 2b

NibbleSub:

After NibbleSub, the two outputs are

B = NibbleSub(0000), NibbleSub(0101), NibbleSub(1010), NibbleSub(1111)
= 1110 1111 0110 0111

B' = NibbleSub(0001), NibbleSub(0101), NibbleSub(1010), NibbleSub(1111)
= 0100 1111 0110 0111

We observe that after NibbleSub, the two outputs differ also in the same nibble, whereas the other nibbles are equal. Hence, NibbleSub does not affect the number nor the position of the active nibbles.

ShiftRow:

After ShiftRow, the outputs are

C = 1110 0111 0110 1111

C' = 0100 0111 0110 1111

From here, we see that ShiftRow does not affect the number of active nibbles. Nevertheless, two nibbles have been interchanged.

MixColumn:

After MixColumn, the outputs are

D = 1111 0110 0111 1110
D' = 0010 0001 0111 1110

With one active nibble at the input, MixColumn causes the output to have two active nibbles in that same column.

KeyAddition:

Suppose the round key is K_i, then after KeyAddition

E = 1111 0110 0111 1110 $\oplus K_i$

E' = 0010 0001 0111 1110 $\oplus K_i$

Given an input with two active nibbles, then regardless of the value of K_i, the output of KeyAddition will also have the same number of active nibbles in the same position, hence KeyAddition does not have any effect on the active nibbles.

To summarize, NibbleSub and KeyAddition do not affect the number nor the position of the active nibbles. ShiftRow only moves nibbles around but otherwise does not affect the number of active nibbles either. Finally, given an input with one active nibble, MixColumn causes an output with two active nibbles in that same column.

Consider again the 4-round Mini-AES. We will illustrate how a plaintext pair, P and P' with one active nibble will fare after going through the first two rounds of Mini-AES.

Example 3

Let

P = 0101 1111 0110 1100
P' = 0100 1111 0110 1100

Notice that only the leftmost nibble is active.

0th Round

***KeyAddition*:**

Supposing that K_0 = 0101 1010 1100 0011
After going through KeyAddition,

$A = P \oplus K_0$ = 0101 1111 0110 1100 ⊕ 0101 1010 1100 0011
= 0000 0101 1010 1111
$A' = P' \oplus K_0$ = 0100 1111 0110 1100 ⊕ 0101 1010 1100 0011
= 0001 0101 1010 1111

Observe that there is still only one active nibble. It is then proven that KeyAddition does not affect the number nor position of the active nibbles. We proceed to the first round.

1st Round

***NibbleSub*:**

After NibbleSub, the outputs are

B = NibbleSub(0000), NibbleSub(0101), NibbleSub(1010), NibbleSub(1111)
= 1110 1111 0110 0111

B' = NibbleSub(0001), NibbleSub(0101), NibbleSub(1010), NibbleSub(1111)
= 0100 1111 0110 0111

Again, this confirms our previous discussion that NibbleSub does not affect the number nor position of the active nibbles.

***ShiftRow*:**

After ShiftRow, the outputs are

C = 1110 0111 0110 1111
C' = 0100 0111 0110 1111

Clearly, there is still one active nibble, though two passive nibbles have been interchanged.

***MixColumn*:**

After MixColumn, the outputs are

D = 1111 0110 0111 1110

D' = 0010 0001 0111 1110

Notice that after MixColumn, we have two active nibbles in the same column instead of just one. Therefore, it is proven that MixColumn spreads one active nibble to two active nibbles in the same column.

***KeyAddition*:**
Supposing that K_1 = 1100 0011 0101 1010
After going through KeyAddition,

E = $D \oplus K_1$ = 1111 0110 0111 1110 ⊕ 1100 0011 0101 1010
= 0011 0101 0010 0100
E' = $D' \oplus K_1$ = 0010 0001 0111 1110 ⊕ 1100 0011 0101 1010
= 1110 0010 0010 0100

We see that at the output of KeyAddition, we still have two active nibbles in the same column. We then proceed to the second round.

2nd Round

***NibbleSub*:**
After NibbleSub, the outputs are

F = NibbleSub(0011), NibbleSub(0101), NibbleSub(0010), NibbleSub(0100)
= 0001 1111 1101 0010

F' = NibbleSub(1110), NibbleSub(0010), NibbleSub(0010), NibbleSub(0100)
= 0000 1101 1101 0010

The number of active nibbles remains at two, and in the same position.

***ShiftRow*:**
After ShiftRow, the outputs are

G = 0001 0010 1101 1111

G' = 0000 0010 1101 1101

The number of active nibbles is the same, but two nibbles have been interchanged. As a result of this, there is one active nibble in each column.

***MixColumn*:**
After MixColumn, the outputs are

H = 0111 0100 1001 1011
H' = 0100 0110 1101 1101

Hence, at the output of MixColumn, all nibbles are active.

***KeyAddition*:**
Supposing that K_2 = 1111 0010 1011 1100
After going through KeyAddition,

I = $H \oplus K_2$ = 0111 0100 1001 1011 ⊕ 1111 0010 1011 1100
= 1000 0110 0010 0111
I' = $H' \oplus K_2$ = 0100 0110 1101 1101 ⊕ 1111 0010 1011 1100
= 1011 0100 0110 0001

The output of KeyAddition also causes all active nibbles.

In summary, we have demonstrated that if we have two plaintexts such that they are equal in all nibbles except in the first nibble, then after the first round, we get outputs with two active nibbles in the first column. Proceeding through the second round, we see that we finally have two outputs that have all active nibbles.

Now, suppose we look at the other end, at the outputs of round 4, which is the last round of 4-round Mini-AES. Consider two ciphertexts, T and T' such that they are equal in only one nibble in each row and column.

Example 4a

Let T = 0100 0011 1001 0101
T' = 1110 0011 1001 1110

As can be seen, the ciphertexts have exactly one active nibble in each column, meaning they also have exactly one passive nibble in each column.

Let's see how the ciphertexts fare as they go through the last round in reverse.

Example 4b

***Inverse KeyAddition*:**

Supposing that K_4 = 0010 1011 1100 0111
After going through inverse KeyAddition,

$S = T \oplus K_4$ = 0100 0011 1001 0101 ⊕ 0010 1011 1100 0111
= 0110 1000 0101 0010

$S' = T' \oplus K_4$ = 1110 0011 1001 1110 ⊕ 0010 1011 1100 0111
= 1100 1000 0101 1001

We still have the two active and passive nibbles in the same positions.

***Inverse ShiftRow*:**

Recall that there is no MixColumn in the last round. Hence, the next operation would be Inverse ShiftRow, which is identical to ShiftRow. The corresponding outputs are

R = 0110 0010 0101 1000

R' = 1100 1001 0101 1000

The number of active and passive nibbles are the same, except that two nibbles have been interchanged, causing the active nibbles to appear solely in the first column while the passive nibbles are in the second column.

***Inverse NibbleSub*:**

After Inverse NibbleSub, the outputs are, according to Table 3 of [3]

Q = NibbleSub^{-1}(0110), NibbleSub^{-1}(0010), NibbleSub^{-1}(0101), NibbleSub^{-1}(1000)
= 1010 0100 1100 0111

Q' = NibbleSub^{-1}(1100), NibbleSub^{-1}(1001), NibbleSub^{-1}(0101), NibbleSub^{-1}(1000)
= 1011 1101 1100 0111

The number and position of the active and passive nibbles remain the same.

***Inverse KeyAddition*:**

Supposing that K_3 = 1011 1100 0111 1101
After going through inverse KeyAddition,

$P = Q \oplus K_3$ = 1010 0100 1100 0111 ⊕ 1011 1100 0111 1101

$$
\begin{aligned}
 & & = 0001\ 1000\ 1011\ 1010 \\
P' &= Q' \oplus K_3 & = 1011\ 1101\ 1100\ 0111 \oplus 1011\ 1100\ 0111\ 1101 \\
 & & = 0000\ 0001\ 1011\ 1010
\end{aligned}
$$

Again, the number and position of the active and passive nibbles are unchanged.

***Inverse MixColumn*:**
After Inverse MixColumn which is the same as MixColumn, the outputs are

O = 0000 1001 1001 1000
O' = 0010 0011 1001 1000

Hence, at the output, the number and position of the active and passive nibbles are unaffected.

***Inverse ShiftRow*:**
After Inverse ShiftRow, the outputs are

N = 0000 1000 1001 1001
N' = 0010 1000 1001 0011

We observe that the number of active nibbles are the same, except that two nibbles have been interchanged, causing one active and passive nibble in each column.

***Inverse NibbleSub*:**
After Inverse NibbleSub, the outputs are

M = NibbleSub^{-1}(0000), NibbleSub^{-1}(1000), NibbleSub^{-1}(1001), NibbleSub^{-1}(1001)
= 1110 0111 1101 1101
M' = NibbleSub^{-1}(0010), NibbleSub^{-1}(1000), NibbleSub^{-1}(1001), NibbleSub^{-1}(0011)
= 0100 0111 1101 1000

At the output of Inverse NibbleSub, we have the same number of active and passive nibbles, in the same positions.

Notice that we have gone through the last two rounds, Rounds 3 and 4 in reverse, and are now at the end of Round 2.

Therefore, as a consequence of Example 4a and 4b, we conclude that given two ciphertexts such that they are equal in exactly one nibble in each row and column, we will always get two outputs with one active and passive nibble in each column at the end of Round 2.

However, this contradicts with our previous argument derived from Example 3 about the behaviour two plaintexts through the first two rounds where we mentioned that at the output of round 2, all nibbles are active. Hence, we conclude that if we have two plaintexts, P and P' such that they differ in only one nibble, then after encryption with 4-round Mini-AES, we will never have ciphertexts, T and T' such that they differ in only one nibble in each row and column. This is illustrated in Figure 2, and is called a 4-round *impossible differential*.

By making use of this 4-round impossible differential, we can mount impossible differential attacks on Mini-AES with even more rounds. Simply place the impossible differential in the middle rounds, and then guess the round keys in the outer rounds and use them to verify if the impossible differential occurs. If so, then the guessed round key values are wrong and removed from the list of possible round keys. This is really the gist behind impossible differential cryptanalysis.

3.2 Attacking 5-round Mini-AES

In this section, we consider how to use the 4-round impossible differential to mount an impossible differential cryptanalysis on Mini-AES with up to 5 rounds. An attack on Mini-

AES up to 6 rounds works along the same lines and we leave it to the interested reader to work it out. As a hint, the attack is very much similar to the impossible differential attack on 6 rounds of the real AES presented in [8].

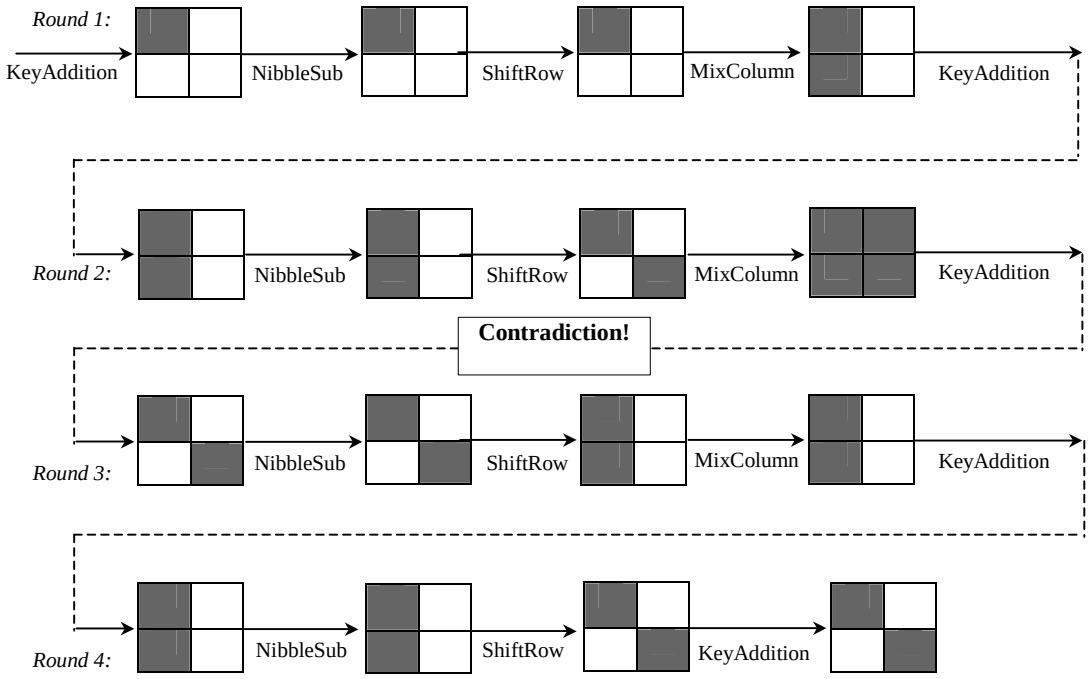

Figure 2: 4-round Impossible Differential of Mini-AES

We now describe how to mount an impossible differential cryptanalysis on Mini-AES up to 5 rounds. We apply the impossible differential to the last 4 rounds of this Mini-AES version. Then we make guesses of some nibbles of the 0^{th} round key, K_0 and partially encrypt plaintexts with K_0. If we discover that the impossible differential holds for the last 4 rounds, then the guessed key value is wrong since it caused an impossible condition that will never happen for the correct key. The attack proceeds as follows, with illustration in Figure 3:

1. Obtain 2^{11} plaintexts, P and P' which are equal in the second and third nibble and differ in the other nibbles. Since each P and P' forms a pair with passive second and third nibbles while the first and third nibbles are active, we then have 2^{11} such pairs.
2. Obtain the ciphertexts, C and C' corresponding to these plaintext pairs. Choose only the pairs whose ciphertext pairs differ in only one nibble in each column. We expect that out of 2^{11} pairs, we will get such ciphertext pairs with probability $(2^{-4} \times 2^{-4}) + (2^{-4} \times 2^{-4}) = 2^{-7}$, hence $2^{11} \times 2^{-7} = 2^4$ pairs will satisfy the requirement.
3. For all the remaining 2^4 pairs, do
   i. For all possible values ($2^4 \times 2^4 = 2^8$) of those two nibble positions of K_0, do
      a. Calculate the value of $X = \theta \circ \pi \circ \gamma \circ \sigma_{K0}(P)$ and $X' = \theta \circ \pi \circ \gamma \circ \sigma_{K0}(P')$.
      b. A randomly guessed key value would cause a pair X and X' that differs in only one nibble in the first column with probability $2^{-4} \times 2 = 2^{-3}$.
      c. This will ensure that the 4-round impossible differential as in Figure 1 will hold in the last 4 rounds. The guessed nibble values of K_0 that caused these pairs are wrong values and are discarded.
4. After analyzing 2^4 pairs, there are only about $2^8(1 - 2^{-3})^{2^4} \approx 2^8 e^{-2^1} \approx 2^5 \approx 0$ wrong values of the two nibbles of K_0 so only the right nibble value remains.

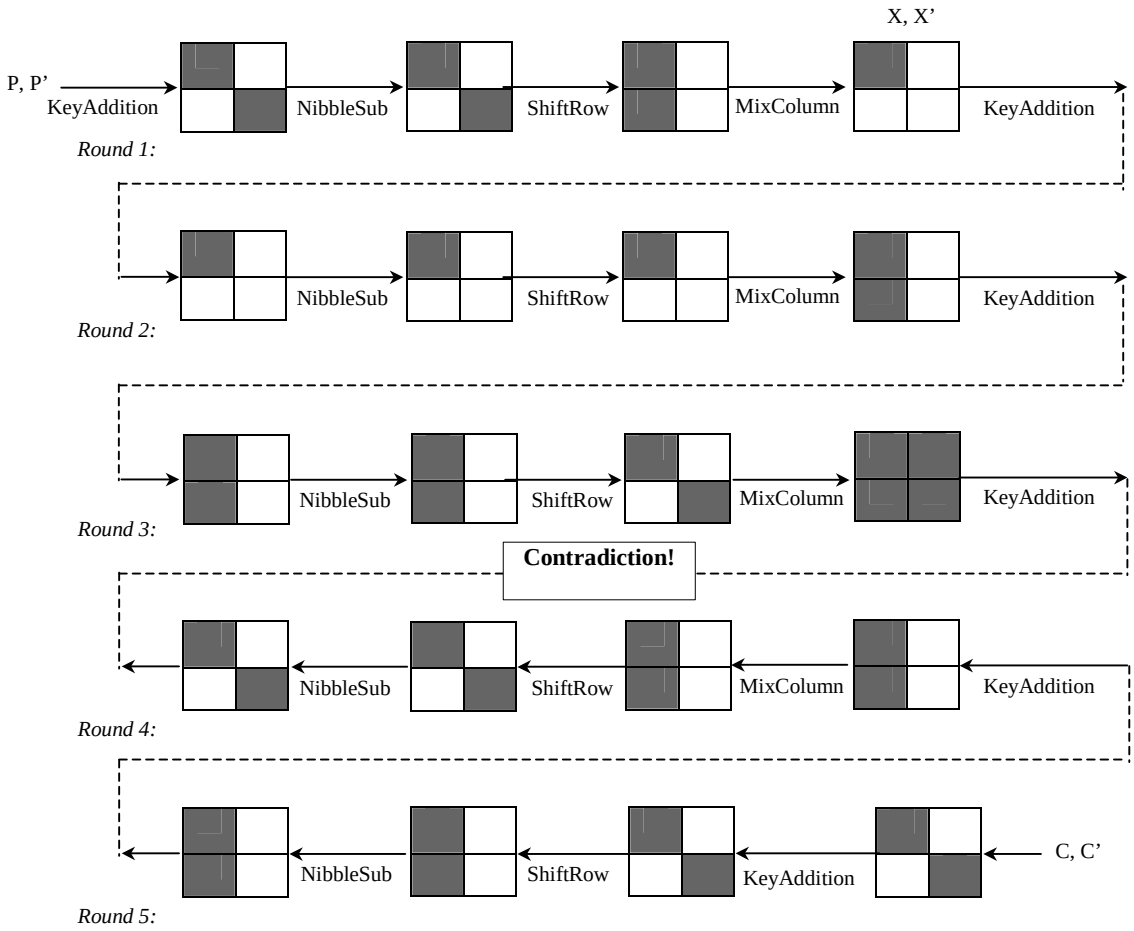

Figure 3: Attacking 5-round Mini-AES

4 Conclusion

We have presented an introduction to the impossible differential cryptanalysis by demonstrating step by step how a 4-round impossible differential of Mini-AES can be constructed. As a further step in understanding the concepts behind this attack, the reader is encouraged to verify the 4-round impossible differential by hand. This is an important part of impossible differential cryptanalysis because the difficulty mostly lies in trying to find impossible differentials before an impossible differential attack can be applied on encryption algorithms.

Once the reader is comfortable with the idea of the attack, he should refer to the following papers [5, 6, 7, 8] for details on how the impossible differential cryptanalysis is applied to the real AES.

References

1. NIST. 2001. *AES Homepage.* Available at: http://www.nist.gov/aes.

2. Stallings, W. 2002. The Advanced Encryption Standard. *Cryptologia.* 26(3).

3. Phan, R. C.-W. 2002. Mini Advanced Encryption Standard (Mini-AES): A Testbed for Cryptanalysis Students. *Cryptologia*. 26(4).

4. Biham, E., Biryukov, A. and Shamir, A. 2001. Miss in the Middle Attacks on IDEA and Khufu. In *Advances of Cryptology – FSE '99 (Lecture Notes in Computer Science No. 1636*). 124-138.

5. Biham, E. and Keller, N. 2000. *Cryptanalysis of Reduced Variants of Rijndael.* Submitted to 3rd AES Candidate Conference. Available at http://csrc.nist.gov/CryptoToolkit/aes/round2/conf3/papers/35-ebiham.pdf.

6. Phan, R. C. W. and Siddiqi, M. U. 2001. Generalised Impossible Differentials of Advanced Encryption Standard. *IEE Electronics Letters*. 37(14): 896-898.

7. Phan, R. C. W. 2002. Classes of Impossible Differentials of Advanced Encryption Standard. *IEE Electronics Letters*. 38(11): 508-510.

8. Cheon, J. H., Kim, M., Kim, K., Lee, J.-Y., Kang, S. 2002. Improved Impossible Differential Cryptanalysis of Rijndael and Crypton. In *International Conference on Information Security and Cryptology (ICISC) 2001 (Lecture Notes in Computer Science No. 2288*). 39-49.

BIOGRAPHICAL SKETCH

Raphael Chung-Wei Phan obtained his B. Eng (Hons) degree in Computer Engineering from the Multimedia University (MMU), Cyberjaya, Malaysia in 1999. He was a tutor at MMU's Faculty of Engineering and a researcher at MMU's Center for Smart Systems & Innovation (CSSI) from 1999 to 2001, where he also pursued his Master of Engineering Science degree by research in the "Cryptanalysis of the Advanced Encryption Standard (AES) and Skipjack". He is currently conducting his Ph.D research on the "Cryptanalysis of Block Ciphers: Generalization, Integration & Extensions" at MMU.

Since June 2001, Raphael has been a lecturer and researcher with the Department of Engineering, Swinburne Sarawak Institute of Technology, Kuching, Malaysia. His research interests include cryptanalysis, block ciphers, authentication protocols, smart card security, and other areas of computer security.