2011 International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11

Repeated Differential Properties of the AES-128 and AES-256 Key Schedules

Jianyong Huang, Willy Susilo, and Jennifer Seberry
Centre for Computer and Information Security Research,
School of Computer Science and Software Engineering,
University of Wollongong, Wollongong NSW 2522, Australia
Email: {jyh33, wsusilo, jennie}@uow.edu.au

***Abstract*—In this paper, we further study the key schedule of the AES algorithm and present some repeated differential properties of the AES-128 and AES-256 key schedules. We define the concept of repeated differential pattern for the AES-128 key schedule, and the notion of double-sized repeated differential pattern for the AES-256 key schedule. We show that if we use the key schedule to expand two 128-bit (or 256-bit) secret keys with the repeated differential pattern (or double-sized repeated differential pattern), the resultant 10-round (or 14-round) subkeys have a large number of bytes in common and the differential pattern has strong repeated features.**

***Keywords*-Advanced Encryption Standard, AES, Key Schedule, Repeated Differential Properties**

I. Introduction

The Advanced Encryption Standard (AES) is a block cipher adopted by the US government to replace the Data Encryption Standard (DES). The standard was announced by National Institute of Standards and Technology (NIST) on November 26, 2001 after a standardization process in which 15 competing designs were evaluated before Rijndael was selected as AES. AES has a 128-bit block size, with key sizes of 128, 192 and 256 bits, which are denoted by AES-128, AES-192 and AES-256, respectively.

The key schedule of the AES algorithm was designed for a few purposes. The first purpose is the introduction of asymmetry. Asymmetry in the key schedule prevents symmetry in the round transformation and between the rounds leading to weaknesses or allows attacks. The second purpose is the resistance against related-key attacks. The third purpose is the resistance against attacks in which the cipher key is (partially) known by or can be chosen by the attacker. This is the case if the cipher is used as the compression function of a hash function.

Since Rijndael became AES, there have been many research efforts aiming to attack this cipher. Some recent research results include the distinguisher and related-key attack on the full AES-256 [1], the related-key cryptanalysis of the full versions of AES-192 and AES-256 [2], key recovery attacks of practical complexity on AES-256 up to 10 rounds [3], and improved single-key attacks on 8-round AES-192 and AES-256 [4]. Some other related-key attacks of AES-192 and AES-256 can be found in [5], [6], [7] and [8]. An efficient search tool for finding differential characteristics in AES and other ciphers was presented in [9].

In this paper we analyze the AES-128 and AES-256 key schedules and describe some repeated differential properties of these two key expansion algorithms. We show that if two secret keys have a special difference pattern, the propagation of the difference via the key schedule produces a large number of identical round keys in 10 consecutive rounds for AES-128 and 14 consecutive rounds for AES-256, and the difference pattern has strong repeated features.

This paper is organized as follows. We provide a short description of the AES block cipher in Section II. In Section III, we present some repeated differential properties of the AES-128 key schedule. We describe some repeated differential features of the AES-256 key schedule in Section IV. We provide future research directions based on the differential properties in Section V. Finally, we conclude the paper in Section VI.

II. A Brief Description of AES

AES is a block cipher with a 128-bit block length and supports key lengths of 128, 192 and 256 bits. The plaintext is first copied to 4×4 array of bytes, which is called the state. After an initial round key addition, the state array is transformed by performing a round function 10, 12, or 14 times (for 128-bit, 192-bit or 256-bit keys, respectively), and the final state is the ciphertext. Each round of AES contains four transformations (the final round does not include MixColumns): SubBytes (SB), ShiftRows (SR), MixColumns (MC) and AddRoundKey (ARK). The SB operation is a non-linear byte substitution, and it operates independently on each byte of the state using a substitution table. In the SR transformation, the bytes of the state are cyclically shifted over different numbers of bytes, i.e., Row i is shifted to the left i byte cyclicly, $0 \leq i \leq 3$. The MC operation operates on the state column-by-column, and the columns are treated as polynomials and multiplied by a constant 4×4 matrix over $GF(2^8)$. In the ARK transformation, a round key is added to the state by a simple bitwise exclusive or (XOR) operation.

The AES algorithm takes the cipher key, and employs the key schedule to generate the round keys. The key schedule generates a total of $Nb(Nr + 1)$ words, where Nr is

978-0-7695-4600-1/11 $26.00 © 2011 IEEE
DOI 10.1109/TrustCom.2011.68

the number of rounds, and Nb is the number of columns comprising the state. The expanded key is an array of 4-byte words and is denoted by $w[Nb(Nr+1)]$. The first Nk (number of 32-bit words comprising the cipher key) words contain the cipher key. The pseudocode for the key expansion of the AES algorithm is shown below, where key is the cipher key, SubWord() applies the substitution operation to each byte of the word, RotWord() cyclically shifts the word to the left 8 bits, and $Rcon$ is an array of predefined constants.

```
KeyExpansion(byte key[4*Nk], word w[Nb*(Nr+1)], Nk)
begin
    word temp
    i = 0
    while (i < Nk)
        w[i] = word(key[4*i], key[4*i+1],
                    key[4*i+2], key[4*i+3])
        i = i+1
    end while
    i = Nk
    while (i < Nb * (Nr+1)]
        temp = w[i-1]
        if (i mod Nk = 0)
            temp = SubWord(RotWord(temp)) xor Rcon[i/Nk]
        else if (Nk > 6 and i mod Nk = 4)
            temp = SubWord(temp)
        end if
            w[i] = w[i-Nk] xor temp
            i = i + 1
    end while
end
```

Notations. An AES intermediate state, as well as an AES round key, is represented as a four-by-four array of bytes. A byte of an intermediate state is written as $a_{i,j}$, $0 \le i, j \le 3$, where i and j stand for the row and column index, respectively. The difference of two intermediate bytes, $a_{i,j}$ and $a'_{i,j}$, is denoted by $\Delta a_{i,j}$. A secret key is represented by K (in uppercase), a byte of the secret key K is written as $k_{i,j}$ (in lowercase), and a subkey byte of K in Round n is denoted by $k^n_{i,j}$ (in lowercase), where i is the row index and j is the column index. The difference of two key bytes in Round n, $k^n_{i,j}$ and $k'^n_{i,j}$, is represented as $\Delta k^n_{i,j}$.

III. Repeated Differential Properties of the AES-128 Key Schedule

In this section we show some repeated differential properties of the AES-128 key schedule. If two different keys start with a special difference pattern, the propagation of the difference generates a large set of identical round keys and the difference of the round keys has strong repeated patterns.

Definition 1. *A difference of two 128-bit keys is called an R differential pattern if the difference has the format*

$$\begin{pmatrix} x & 0 & x & 0 \\ y & y & 0 & 0 \\ z & 0 & 0 & 0 \\ v & v & v & v \end{pmatrix},$$

where x is an integer between 1 and 255, and y, z and v are integers between 0 and 255.

Definition 2. *A difference of two expanded 10-round subkeys is called a 10-round R differential pattern (whose format is shown in Figure 1) if the difference of the two 128-bit secret keys has the R differential pattern, where x is an integer between 1 and 255, and y, z, v, u, λ, ϕ, β, γ, α, t, d, w and q are integers between 0 and 255.*

In Figure 1, the leftmost part contains all bytes of K and its subkeys, the middle part lists all bytes of K' and its subkeys, and the rightmost part depicts the byte differences of K and K' and their subkeys.

Theorem 1. *For every 128-bit secret key K, there exist 255×256^3 different keys, K', such that the difference of K and K' has the R differential pattern, and the difference of the expanded 10-round subkeys has the 10-round R differential pattern with probability 1.*

Proof: Suppose two 128-bit secret keys, K and K', have the R differential pattern. We start with the difference of these two secret keys in Round 0, and analyze the propagation of the difference from Round 1 to Round 10 (see Figure 1 for the details of the differential pattern).

- Round 0.

$$\Delta K = K \oplus K' = \begin{pmatrix} x & 0 & x & 0 \\ y & y & 0 & 0 \\ z & 0 & 0 & 0 \\ v & v & v & v \end{pmatrix}.$$

- Round 1. Let $u = SB(k_{3,3}) \oplus z \oplus SB(k_{3,3} \oplus v)$, each byte difference is calculated as follows:

$$\begin{array}{llll} \Delta k^1_{0,0} = x, & \Delta k^1_{1,0} = y, & \Delta k^1_{2,0} = u, & \Delta k^1_{3,0} = v, \\ \Delta k^1_{0,1} = x, & \Delta k^1_{1,1} = 0, & \Delta k^1_{2,1} = u, & \Delta k^1_{3,1} = 0, \\ \Delta k^1_{0,2} = 0, & \Delta k^1_{1,2} = 0, & \Delta k^1_{2,2} = u, & \Delta k^1_{3,2} = v, \\ \Delta k^1_{0,3} = 0, & \Delta k^1_{1,3} = 0, & \Delta k^1_{2,3} = u, & \Delta k^1_{3,3} = 0. \end{array}$$

- Round 2. Let

$$\begin{aligned} \Omega^2_0 =& SB(k_{1,3} \oplus k_{1,2} \oplus k_{1,1} \oplus k_{1,0} \oplus SB(k_{2,3})) \\ & \oplus Rcon[2], \\ \Omega^2_1 =& SB(k_{2,3} \oplus k_{2,2} \oplus k_{2,1} \oplus k_{2,0} \oplus SB(k_{3,3})), \\ \Omega^2_2 =& SB(k_{3,3} \oplus k_{3,2} \oplus k_{3,1} \oplus k_{3,0} \oplus SB(k_{0,3})), \text{ and} \\ \Omega^2_3 =& SB(k_{0,3} \oplus k_{0,2} \oplus k_{0,1} \oplus k_{0,0} \oplus SB(k_{1,3}) \\ & \oplus Rcon[1]). \end{aligned}$$

  Ω^i_j is a variable used in Row j of Round i of K. Let $\Omega'^2_1 = SB(k_{2,3} \oplus k_{2,2} \oplus k_{2,1} \oplus k_{2,0} \oplus z \oplus SB(k_{3,3} \oplus v))$. Ω'^i_j is a variable used in Row j of Round i of K'. We use Ω^i_j and Ω'^i_j to avoid long expressions in our proof. Let $\lambda = \Omega^2_1 \oplus y \oplus \Omega'^2_1$, the key byte differences are listed below:

$$\begin{array}{llll} \Delta k^2_{0,0} = x, & \Delta k^2_{1,0} = \lambda, & \Delta k^2_{2,0} = u, & \Delta k^2_{3,0} = v. \\ \Delta k^2_{0,1} = 0, & \Delta k^2_{1,1} = \lambda, & \Delta k^2_{2,1} = 0, & \Delta k^2_{3,1} = v, \\ \Delta k^2_{0,2} = 0, & \Delta k^2_{1,2} = \lambda, & \Delta k^2_{2,2} = u, & \Delta k^2_{3,2} = 0, \\ \Delta k^2_{0,3} = 0, & \Delta k^2_{1,3} = \lambda, & \Delta k^2_{2,3} = 0, & \Delta k^2_{3,3} = 0. \end{array}$$

- Round 3. Let

$$\begin{aligned}\Omega_0^3 &= SB(k_{1,3} \oplus k_{1,1} \oplus \Omega_1^2) \oplus Rcon[3],\\ \Omega_1^3 &= SB(k_{2,3} \oplus k_{2,1} \oplus \Omega_2^2),\\ \Omega_2^3 &= SB(k_{3,3} \oplus k_{3,1} \oplus \Omega_3^2), \text{ and}\\ \Omega_3^3 &= SB(k_{0,3} \oplus k_{0,1} \oplus \Omega_0^2).\end{aligned}$$

Let $\Omega_0'^3 = SB(k_{1,3} \oplus k_{1,1} \oplus y \oplus \Omega_1'^2) \oplus Rcon[3]$, and $\phi = \Omega_0^3 \oplus x \oplus \Omega_0'^3$. The byte differences are represented as:

$$\begin{aligned}&\Delta k_{0,0}^3 = \phi, \quad \Delta k_{1,0}^3 = \lambda, \quad \Delta k_{2,0}^3 = u, \quad \Delta k_{3,0}^3 = v,\\ &\Delta k_{0,1}^3 = \phi, \quad \Delta k_{1,1}^3 = 0, \quad \Delta k_{2,1}^3 = u, \quad \Delta k_{3,1}^3 = 0,\\ &\Delta k_{0,2}^3 = \phi, \quad \Delta k_{1,2}^3 = \lambda, \quad \Delta k_{2,2}^3 = 0, \quad \Delta k_{3,2}^3 = 0,\\ &\Delta k_{0,3}^3 = \phi, \quad \Delta k_{1,3}^3 = 0, \quad \Delta k_{2,3}^3 = 0, \quad \Delta k_{3,3}^3 = 0.\end{aligned}$$

- Round 4. Let

$$\begin{aligned}\Omega_0^4 &= SB(k_{1,3} \oplus k_{1,2} \oplus \Omega_1^3) \oplus Rcon[4],\\ \Omega_1^4 &= SB(k_{2,3} \oplus k_{2,2} \oplus \Omega_2^3),\\ \Omega_2^4 &= SB(k_{3,3} \oplus k_{3,2} \oplus \Omega_3^3), \text{ and}\\ \Omega_3^4 &= SB(k_{0,3} \oplus k_{0,2} \oplus \Omega_0^3).\end{aligned}$$

Let $\Omega_3'^4 = SB(k_{0,3} \oplus k_{0,2} \oplus x \oplus \Omega_0'^3)$, and $\beta = \Omega_3^4 \oplus v \oplus \Omega_3'^4$, the key byte differences are computed as follows:

$$\begin{aligned}&\Delta k_{0,0}^4 = \phi, \quad \Delta k_{1,0}^4 = \lambda, \quad \Delta k_{2,0}^4 = u, \quad \Delta k_{3,0}^4 = \beta,\\ &\Delta k_{0,1}^4 = 0, \quad \Delta k_{1,1}^4 = \lambda, \quad \Delta k_{2,1}^4 = 0, \quad \Delta k_{3,1}^4 = \beta,\\ &\Delta k_{0,2}^4 = \phi, \quad \Delta k_{1,2}^4 = 0, \quad \Delta k_{2,2}^4 = 0, \quad \Delta k_{3,2}^4 = \beta,\\ &\Delta k_{0,3}^4 = 0, \quad \Delta k_{1,3}^4 = 0, \quad \Delta k_{2,3}^4 = 0, \quad \Delta k_{3,3}^4 = \beta.\end{aligned}$$

- Round 5. Let

$$\begin{aligned}\Omega_0^5 &= SB(k_{1,3} \oplus \Omega_1^4) \oplus Rcon[5],\\ \Omega_1^5 &= SB(k_{2,3} \oplus \Omega_2^4),\\ \Omega_2^5 &= SB(k_{3,3} \oplus \Omega_3^4), \text{ and}\\ \Omega_3^5 &= SB(k_{0,3} \oplus \Omega_0^4).\end{aligned}$$

Let $\Omega_2'^5 = SB(k_{3,3} \oplus v \oplus \Omega_3'^4)$, and $\gamma = \Omega_2^5 \oplus u \oplus \Omega_2'^5$, the key byte differences are provided below:

$$\begin{aligned}&\Delta k_{0,0}^5 = \phi, \quad \Delta k_{1,0}^5 = \lambda, \quad \Delta k_{2,0}^5 = \gamma, \quad \Delta k_{3,0}^5 = \beta,\\ &\Delta k_{0,1}^5 = \phi, \quad \Delta k_{1,1}^5 = 0, \quad \Delta k_{2,1}^5 = \gamma, \quad \Delta k_{3,1}^5 = 0,\\ &\Delta k_{0,2}^5 = 0, \quad \Delta k_{1,2}^5 = 0, \quad \Delta k_{2,2}^5 = \gamma, \quad \Delta k_{3,2}^5 = \beta,\\ &\Delta k_{0,3}^5 = 0, \quad \Delta k_{1,3}^5 = 0, \quad \Delta k_{2,3}^5 = \gamma, \quad \Delta k_{3,3}^5 = 0.\end{aligned}$$

- Round 6. Let

$$\begin{aligned}\Omega_0^6 &= SB(k_{1,3} \oplus k_{1,2} \oplus k_{1,1} \oplus k_{1,0} \oplus SB(k_{2,3}) \oplus \Omega_1^5)\\ &\quad \oplus Rcon[6],\\ \Omega_1^6 &= SB(k_{2,3} \oplus k_{2,2} \oplus k_{2,1} \oplus k_{2,0} \oplus SB(k_{3,3}) \oplus \Omega_2^5),\\ \Omega_2^6 &= SB(k_{3,3} \oplus k_{3,2} \oplus k_{3,1} \oplus k_{3,0} \oplus SB(k_{0,3}) \oplus \Omega_3^5),\\ &\quad \text{and}\\ \Omega_3^6 &= SB(k_{0,3} \oplus k_{0,2} \oplus k_{0,1} \oplus k_{0,0} \oplus SB(k_{1,3}) \oplus\\ &\quad Rcon[1] \oplus \Omega_0^5).\end{aligned}$$

Let $\Omega_1'^6 = SB(k_{2,3} \oplus k_{2,2} \oplus k_{2,1} \oplus k_{2,0} \oplus z \oplus SB(k_{3,3} \oplus v) \oplus \Omega_2'^5)$, and $\alpha = \Omega_1^6 \oplus \lambda \oplus \Omega_1'^6$, we have the following byte differences:

$$\begin{aligned}&\Delta k_{0,0}^6 = \phi, \quad \Delta k_{1,0}^6 = \alpha, \quad \Delta k_{2,0}^6 = \gamma, \quad \Delta k_{3,0}^6 = \beta,\\ &\Delta k_{0,1}^6 = 0, \quad \Delta k_{1,1}^6 = \alpha, \quad \Delta k_{2,1}^6 = 0, \quad \Delta k_{3,1}^6 = \beta,\\ &\Delta k_{0,2}^6 = 0, \quad \Delta k_{1,2}^6 = \alpha, \quad \Delta k_{2,2}^6 = \gamma, \quad \Delta k_{3,2}^6 = 0,\\ &\Delta k_{0,3}^6 = 0, \quad \Delta k_{1,3}^6 = \alpha, \quad \Delta k_{2,3}^6 = 0, \quad \Delta k_{3,3}^6 = 0.\end{aligned}$$

- Round 7. Let

$$\begin{aligned}\Omega_0^7 &= SB(k_{1,3} \oplus k_{1,1} \oplus \Omega_1^2 \oplus \Omega_1^6) \oplus Rcon[7],\\ \Omega_1^7 &= SB(k_{2,3} \oplus k_{2,1} \oplus \Omega_2^2 \oplus \Omega_2^6),\\ \Omega_2^7 &= SB(k_{3,3} \oplus k_{3,1} \oplus \Omega_3^2 \oplus \Omega_3^6), \text{ and}\\ \Omega_3^7 &= SB(k_{0,3} \oplus k_{0,1} \oplus \Omega_0^2 \oplus \Omega_0^6).\end{aligned}$$

Let $\Omega_0'^7 = SB(k_{1,3} \oplus k_{1,1} \oplus y \oplus \Omega_1'^2 \oplus \Omega_1'^6) \oplus Rcon[7]$, and $t = \Omega_0^7 \oplus \phi \oplus \Omega_0'^7$, the byte differences are calculated as follows:

$$\begin{aligned}&\Delta k_{0,0}^7 = t, \quad \Delta k_{1,0}^7 = \alpha, \quad \Delta k_{2,0}^7 = \gamma, \quad \Delta k_{3,0}^7 = \beta.\\ &\Delta k_{0,1}^7 = t, \quad \Delta k_{1,1}^7 = 0, \quad \Delta k_{2,1}^7 = \gamma, \quad \Delta k_{3,1}^7 = 0,\\ &\Delta k_{0,2}^7 = t, \quad \Delta k_{1,2}^7 = \alpha, \quad \Delta k_{2,2}^7 = 0, \quad \Delta k_{3,2}^7 = 0,\\ &\Delta k_{0,3}^7 = t, \quad \Delta k_{1,3}^7 = 0, \quad \Delta k_{2,3}^7 = 0, \quad \Delta k_{3,3}^7 = 0.\end{aligned}$$

- Round 8. Let

$$\begin{aligned}\Omega_0^8 &= SB(k_{1,3} \oplus k_{1,2} \oplus \Omega_1^3 \oplus \Omega_1^7) \oplus Rcon[8],\\ \Omega_1^8 &= SB(k_{2,3} \oplus k_{2,2} \oplus \Omega_2^3 \oplus \Omega_2^7),\\ \Omega_2^8 &= SB(k_{3,3} \oplus k_{3,2} \oplus \Omega_3^3 \oplus \Omega_3^7), \text{ and}\\ \Omega_3^8 &= SB(k_{0,3} \oplus k_{0,2} \oplus \Omega_0^3 \oplus \Omega_0^7).\end{aligned}$$

Let $\Omega_3'^8 = SB(k_{0,3} \oplus k_{0,2} \oplus x \oplus \Omega_0'^3 \oplus \Omega_0'^7)$, and $d = \Omega_3^8 \oplus \beta \oplus \Omega_3'^8$, the byte differences are listed below:

$$\begin{aligned}&\Delta k_{0,0}^8 = t, \quad \Delta k_{1,0}^8 = \alpha, \quad \Delta k_{2,0}^8 = \gamma, \quad \Delta k_{3,0}^8 = d,\\ &\Delta k_{0,1}^8 = 0, \quad \Delta k_{1,1}^8 = \alpha, \quad \Delta k_{2,1}^8 = 0, \quad \Delta k_{3,1}^8 = d,\\ &\Delta k_{0,2}^8 = t, \quad \Delta k_{1,2}^8 = 0, \quad \Delta k_{2,2}^8 = 0, \quad \Delta k_{3,2}^8 = d,\\ &\Delta k_{0,3}^8 = 0, \quad \Delta k_{1,3}^8 = 0, \quad \Delta k_{2,3}^8 = 0, \quad \Delta k_{3,3}^8 = d.\end{aligned}$$

- Round 9. Let

$$\begin{aligned}\Omega_0^9 &= SB(k_{1,3} \oplus \Omega_1^4 \oplus \Omega_1^8) \oplus Rcon[9],\\ \Omega_1^9 &= SB(k_{2,3} \oplus \Omega_2^4 \oplus \Omega_2^8),\\ \Omega_2^9 &= SB(k_{3,3} \oplus \Omega_3^4 \oplus \Omega_3^8), \text{ and}\\ \Omega_3^9 &= SB(k_{0,3} \oplus \Omega_0^4 \oplus \Omega_0^8).\end{aligned}$$

Let $\Omega_2'^9 = SB(k_{3,3} \oplus v \oplus \Omega_3'^4 \oplus \Omega_3'^8)$, and $w = \Omega_2^9 \oplus \gamma \oplus \Omega_2'^9$, each byte difference can be computed as:

$$\begin{aligned}&\Delta k_{0,0}^9 = t, \quad \Delta k_{1,0}^9 = \alpha, \quad \Delta k_{2,0}^9 = w, \quad \Delta k_{3,0}^9 = d.\\ &\Delta k_{0,1}^9 = t, \quad \Delta k_{1,1}^9 = 0, \quad \Delta k_{2,1}^9 = w, \quad \Delta k_{3,1}^9 = 0,\\ &\Delta k_{0,2}^9 = 0, \quad \Delta k_{1,2}^9 = 0, \quad \Delta k_{2,2}^9 = w, \quad \Delta k_{3,2}^9 = d,\\ &\Delta k_{0,3}^9 = 0, \quad \Delta k_{1,3}^9 = 0, \quad \Delta k_{2,3}^9 = w, \quad \Delta k_{3,3}^8 = 0.\end{aligned}$$

- Round 10. Let

$$\begin{aligned}
\Omega_0^{10} &= SB(k_{1,3} \oplus k_{1,2} \oplus k_{1,1} \oplus k_{1,0} \oplus SB(k_{2,3}) \oplus \\
&\quad \Omega_1^5 \oplus \Omega_1^9) \oplus Rcon[10], \\
\Omega_1^{10} &= SB(k_{2,3} \oplus k_{2,2} \oplus k_{2,1} \oplus k_{2,0} \oplus SB(k_{3,3}) \oplus \\
&\quad \Omega_2^5 \oplus \Omega_2^9), \\
\Omega_2^{10} &= SB(k_{3,3} \oplus k_{3,2} \oplus k_{3,1} \oplus k_{3,0} \oplus SB(k_{0,3}) \oplus \\
&\quad \Omega_3^5 \oplus \Omega_3^9), \text{ and} \\
\Omega_3^{10} &= SB(k_{0,3} \oplus k_{0,2} \oplus k_{0,1} \oplus k_{0,0} \oplus SB(k_{1,3}) \oplus \\
&\quad Rcon[1] \oplus \Omega_0^5 \oplus \Omega_0^9).
\end{aligned}$$

  Let $\Omega_1'^{10} = SB(k_{2,3} \oplus k_{2,2} \oplus k_{2,1} \oplus k_{2,0} \oplus z \oplus SB(k_{3,3} \oplus v) \oplus \Omega_2'^5 \oplus \Omega_2'^9)$, and $q = \Omega_1^{10} \oplus \alpha \oplus \Omega_1'^{10}$, the byte differences are shown below:

$$\begin{array}{llll}
\Delta k_{0,0}^{10} = t, & \Delta k_{1,0}^{10} = q, & \Delta k_{2,0}^{10} = w, & \Delta k_{3,0}^{10} = d. \\
\Delta k_{0,1}^{10} = 0, & \Delta k_{1,1}^{10} = q, & \Delta k_{2,1}^{10} = 0, & \Delta k_{3,1}^{10} = d, \\
\Delta k_{0,2}^{10} = 0, & \Delta k_{1,2}^{10} = q, & \Delta k_{2,2}^{10} = w, & \Delta k_{3,2}^{10} = 0, \\
\Delta k_{0,3}^{10} = 0, & \Delta k_{1,3}^{10} = q, & \Delta k_{2,3}^{10} = 0, & \Delta k_{3,3}^{10} = 0.
\end{array}$$

- The number of different keys. Since there is no constraint on choosing the values of x, y, z, and v, we can choose 255 possible values for x, 256 possible values for y, 256 possible values for z, and 256 possible values for v. Therefore, for any secret key K, there exist 255×256^3 possible values for K'.

■

We would like to emphasize that the 10-round R differential pattern has the following interesting features (see Figure 1).

1) There are (at least) 7 zero differences in each round. For example, in Round 2, there are 3 zero differences in the first row, 2 zero differences in the third row, and 2 zero differences in the fourth row.
2) There are 4 character variables in each round, and these 4 variables appear in 9 different locations. For example, in Round 1, x appears twice in the first row, y appears once in the second row, u appears four times in the third row and v appears twice in the fourth row.
3) The same differential pattern repeats every 4 rounds. The differential pattern includes the byte positions and the values of the differences. For instance, we consider the differential pattern of Round 1 is same as the differential pattern of Round 5.
4) The differences, denoted by character variables, are identical in each row. For example, in the second row of Round 2, the differences denoted by character variables are all equal to λ, and in the third row of Round 2, the differences denoted by character variables are equal to u.
5) The key schedule introduces a new difference value in each round. For instance, there are four character variables in Round 3 (ϕ, λ, u and v), and a new difference value, β, is introduced to Round 4.

IV. Repeated Differential Properties of the AES-256 Key Schedule

Definition 3. *A difference of two 256-bit keys is called a double-sized R differential pattern if the difference has the format*

$$\begin{pmatrix}
X & 0 & X & 0 & 0 & 0 & 0 & 0 \\
Y & Y & 0 & 0 & 0 & 0 & 0 & 0 \\
Z & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
V & V & V & V & 0 & 0 & 0 & 0
\end{pmatrix},$$

where X is an integer between 1 and 255, and Y, Z and V are integers between 0 and 255.

Definition 4. *A difference of two expanded 14-round subkeys is called a 14-round R differential pattern (whose format is shown in Figure 2) if the difference of the two 256-bit secret keys has the double-sized R differential pattern, where X is an integer between 1 and 255, and Y, Z, V, U, Λ, Φ, Γ, Θ, Ψ, Υ, T, D, S, Q and J are integers between 0 and 255.*

In Figure 2, the leftmost part shows all bytes of K and its expanded subkeys, the middle part holds all bytes of K' and its expanded subkeys, and the rightmost part contains the byte differences of K and K' and their subkeys.

Theorem 2. *For every 256-bit secret key K, there exist 255×256^3 different keys, K', such that the difference of K and K' has the double-sized R differential pattern, and the difference of the two expanded 14-round subkeys has the 14-round R differential pattern with probability 1.*

Proof: Assume that two 256-bit secret keys, K and K', have the double-sized R differential pattern. We begin with the difference of these two keys in Round 0 and 1, and trace the propagation of the difference from Round 2 to Round 14.

- Round 0 and 1. We have the following equation:

$$\Delta K = K \oplus K' = \begin{pmatrix}
X & 0 & X & 0 & 0 & 0 & 0 & 0 \\
Y & Y & 0 & 0 & 0 & 0 & 0 & 0 \\
Z & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
V & V & V & V & 0 & 0 & 0 & 0
\end{pmatrix}.$$

- Round 2. The byte differences are computed as follows:

$$\begin{array}{llll}
\Delta k_{0,0}^{2} = X, & \Delta k_{1,0}^{2} = Y, & \Delta k_{2,0}^{2} = Z, & \Delta k_{3,0}^{2} = V, \\
\Delta k_{0,1}^{2} = X, & \Delta k_{1,1}^{2} = 0, & \Delta k_{2,1}^{2} = Z, & \Delta k_{3,1}^{2} = 0, \\
\Delta k_{0,2}^{2} = 0, & \Delta k_{1,2}^{2} = 0, & \Delta k_{2,2}^{2} = Z, & \Delta k_{3,2}^{2} = V, \\
\Delta k_{0,3}^{2} = 0, & \Delta k_{1,3}^{2} = 0, & \Delta k_{2,3}^{2} = Z, & \Delta k_{3,3}^{2} = 0.
\end{array}$$

- Round 3. Let $U = SB(k_{2,3}^2) \oplus SB(k_{2,3}'^2)$, the byte differences are listed below:

$$\begin{array}{llll}
\Delta k_{0,0}^{3} = 0, & \Delta k_{1,0}^{3} = 0, & \Delta k_{2,0}^{3} = U, & \Delta k_{3,0}^{3} = 0, \\
\Delta k_{0,1}^{3} = 0, & \Delta k_{1,1}^{3} = 0, & \Delta k_{2,1}^{3} = U, & \Delta k_{3,1}^{3} = 0, \\
\Delta k_{0,2}^{3} = 0, & \Delta k_{1,2}^{3} = 0, & \Delta k_{2,2}^{3} = U, & \Delta k_{3,2}^{3} = 0, \\
\Delta k_{0,3}^{3} = 0, & \Delta k_{1,3}^{3} = 0, & \Delta k_{2,3}^{3} = U, & \Delta k_{3,3}^{3} = 0.
\end{array}$$

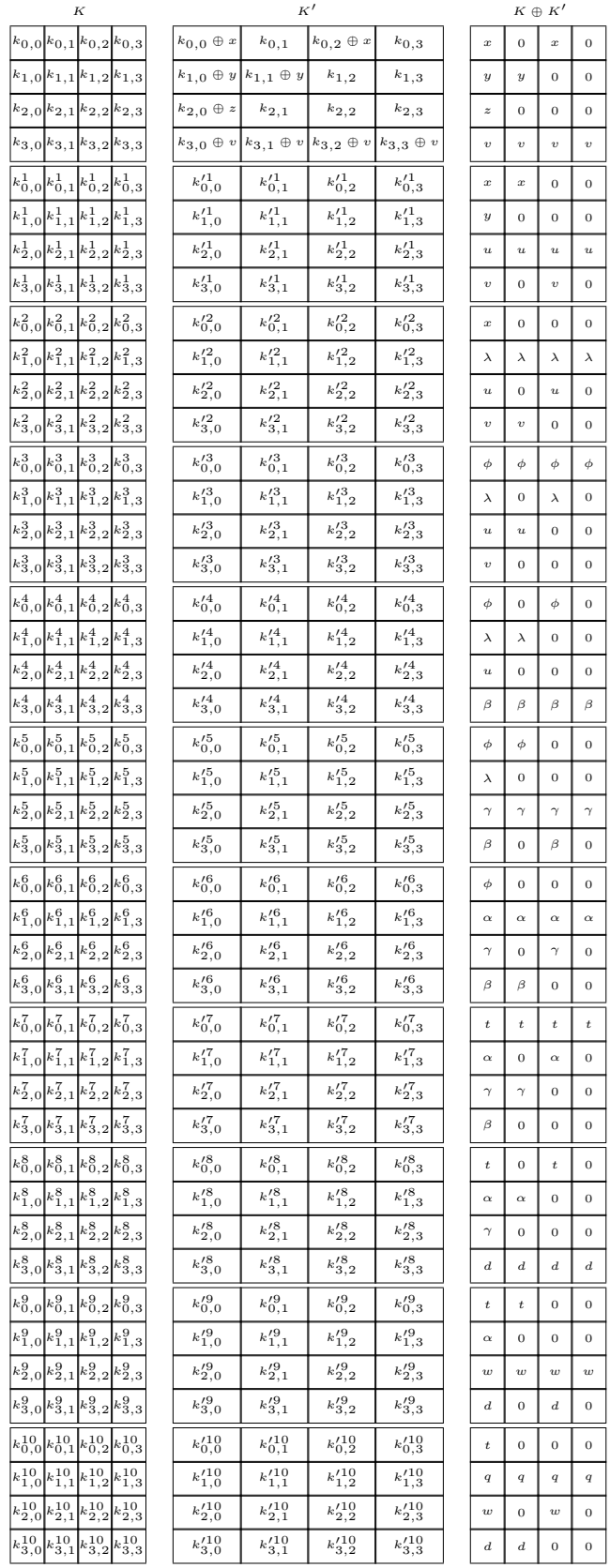

Figure 1. The 10-round R differential pattern

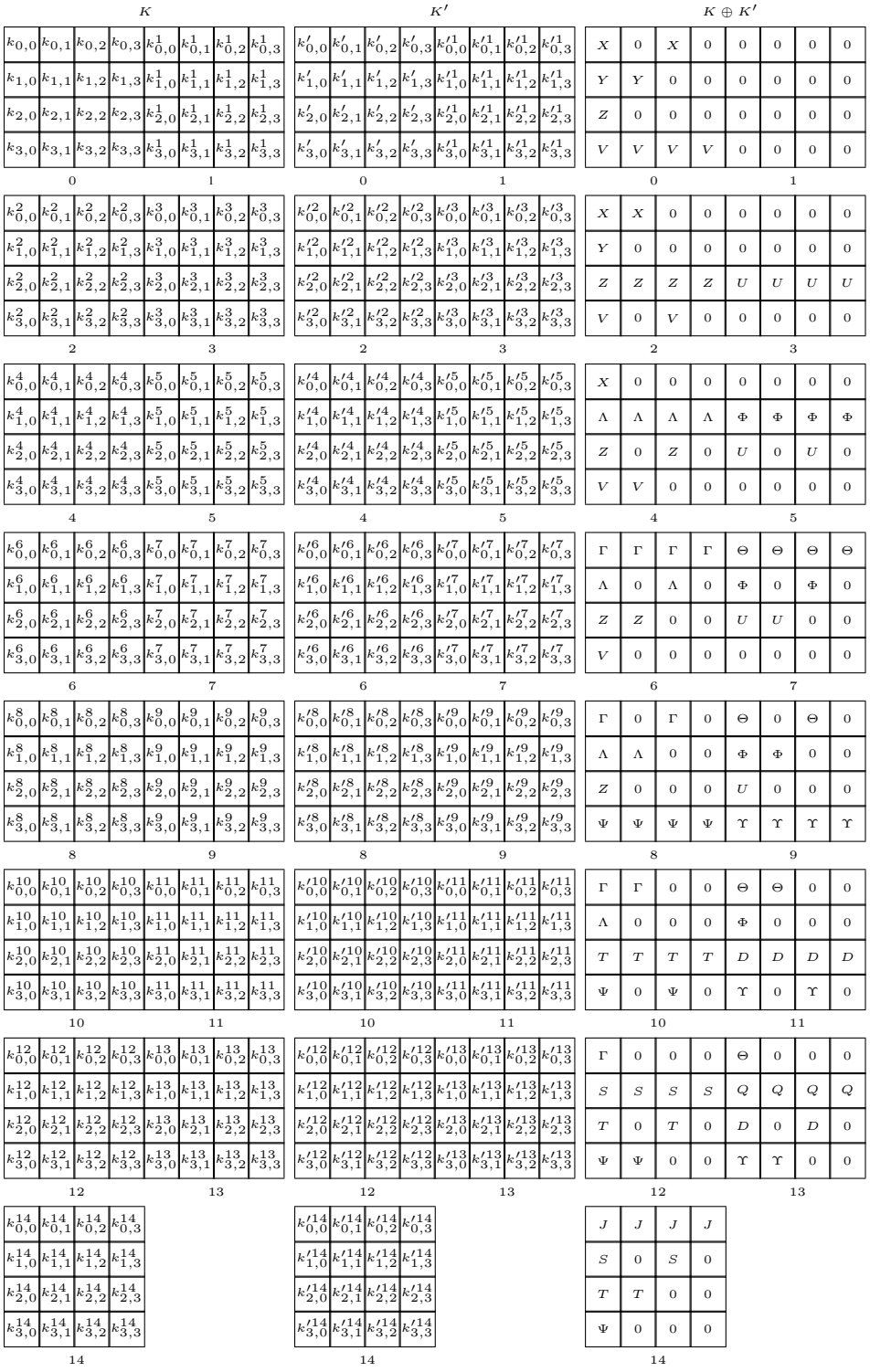

Figure 2. The 14-round R differential pattern

- Round 4. Let $\Lambda = k^2_{1,0} \oplus SB(k^3_{2,3}) \oplus k'^2_{1,0} \oplus SB(k'^3_{2,3})$, all byte differences are provided below.

$$\begin{array}{llll} \Delta k^4_{0,0} = X, & \Delta k^4_{1,0} = \Lambda, & \Delta k^4_{2,0} = Z, & \Delta k^4_{3,0} = V, \\ \Delta k^4_{0,1} = 0, & \Delta k^4_{1,1} = \Lambda, & \Delta k^4_{2,1} = 0, & \Delta k^4_{3,1} = V, \\ \Delta k^4_{0,2} = 0, & \Delta k^4_{1,2} = \Lambda, & \Delta k^4_{2,2} = Z, & \Delta k^4_{3,2} = 0, \\ \Delta k^4_{0,3} = 0, & \Delta k^4_{1,3} = \Lambda, & \Delta k^4_{2,3} = 0, & \Delta k^4_{3,3} = 0. \end{array}$$

- Round 5. Let $\Phi = SB(k^4_{1,3}) \oplus SB(k'^4_{1,3})$, the byte differences can be represented as:

$$\begin{array}{llll} \Delta k^5_{0,0} = 0, & \Delta k^5_{1,0} = \Phi, & \Delta k^5_{2,0} = U, & \Delta k^5_{3,0} = 0, \\ \Delta k^5_{0,1} = 0, & \Delta k^5_{1,1} = \Phi, & \Delta k^5_{2,1} = 0, & \Delta k^5_{3,1} = 0, \\ \Delta k^5_{0,2} = 0, & \Delta k^5_{1,2} = \Phi, & \Delta k^5_{2,2} = U, & \Delta k^5_{3,2} = 0, \\ \Delta k^5_{0,3} = 0, & \Delta k^5_{1,3} = \Phi, & \Delta k^5_{2,3} = 0, & \Delta k^5_{3,3} = 0. \end{array}$$

- Round 6. Let $\Gamma = k^4_{0,0} \oplus SB(k^5_{1,3}) \oplus k'^4_{0,0} \oplus SB(k'^5_{1,3})$, the byte differences are shown below:

$$\begin{array}{llll} \Delta k^6_{0,0} = \Gamma, & \Delta k^6_{1,0} = \Lambda, & \Delta k^6_{2,0} = Z, & \Delta k^6_{3,0} = V, \\ \Delta k^6_{0,1} = \Gamma, & \Delta k^6_{1,1} = 0, & \Delta k^6_{2,1} = Z, & \Delta k^6_{3,1} = 0, \\ \Delta k^6_{0,2} = \Gamma, & \Delta k^6_{1,2} = \Lambda, & \Delta k^6_{2,2} = 0, & \Delta k^6_{3,2} = 0, \\ \Delta k^6_{0,3} = \Gamma, & \Delta k^6_{1,3} = 0, & \Delta k^6_{2,3} = 0, & \Delta k^6_{3,3} = 0. \end{array}$$

- Round 7. Let $\Theta = SB(k^6_{0,3}) \oplus k^5_{0,0} \oplus SB(k'^6_{0,3}) \oplus k'^5_{0,0}$, the byte differences are calculated as follows:

$$\begin{array}{llll} \Delta k^7_{0,0} = \Theta, & \Delta k^7_{1,0} = \Phi, & \Delta k^7_{2,0} = U, & \Delta k^7_{3,0} = 0, \\ \Delta k^7_{0,1} = \Theta, & \Delta k^7_{1,1} = 0, & \Delta k^7_{2,1} = U, & \Delta k^7_{3,1} = 0, \\ \Delta k^7_{0,2} = \Theta, & \Delta k^7_{1,2} = \Phi, & \Delta k^7_{2,2} = 0, & \Delta k^7_{3,2} = 0, \\ \Delta k^7_{0,3} = \Theta, & \Delta k^7_{1,3} = 0, & \Delta k^7_{2,3} = 0, & \Delta k^7_{3,3} = 0. \end{array}$$

- Round 8. Let $\Psi = k^6_{3,0} \oplus SB(k^7_{0,3}) \oplus k'^6_{3,0} \oplus SB(k'^7_{0,3})$, the byte differences are listed below:

$$\begin{array}{llll} \Delta k^8_{0,0} = \Gamma, & \Delta k^8_{1,0} = \Lambda, & \Delta k^8_{2,0} = Z, & \Delta k^8_{3,0} = \Psi, \\ \Delta k^8_{0,1} = 0, & \Delta k^8_{1,1} = \Lambda, & \Delta k^8_{2,1} = 0, & \Delta k^8_{3,1} = \Psi, \\ \Delta k^8_{0,2} = \Gamma, & \Delta k^8_{1,2} = 0, & \Delta k^8_{2,2} = 0, & \Delta k^8_{3,2} = \Psi, \\ \Delta k^8_{0,3} = 0, & \Delta k^8_{1,3} = 0, & \Delta k^8_{2,3} = 0, & \Delta k^8_{3,3} = \Psi. \end{array}$$

- Round 9. Let $\Upsilon = SB(k^8_{3,3}) \oplus k^7_{3,0} \oplus SB(k'^8_{3,3}) \oplus k'^7_{3,0}$, the byte differences are represented as:

$$\begin{array}{llll} \Delta k^9_{0,0} = \Theta, & \Delta k^9_{1,0} = \Phi, & \Delta k^9_{2,0} = U, & \Delta k^9_{3,0} = \Upsilon, \\ \Delta k^9_{0,1} = 0, & \Delta k^9_{1,1} = \Phi, & \Delta k^9_{2,1} = 0, & \Delta k^9_{3,1} = \Upsilon, \\ \Delta k^9_{0,2} = \Theta, & \Delta k^9_{1,2} = 0, & \Delta k^9_{2,2} = 0, & \Delta k^9_{3,2} = \Upsilon, \\ \Delta k^9_{0,3} = 0, & \Delta k^9_{1,3} = 0, & \Delta k^9_{2,3} = 0, & \Delta k^8_{3,3} = \Upsilon. \end{array}$$

- Round 10. Let $T = k^8_{2,0} \oplus SB(k^9_{3,3}) \oplus k'^8_{2,0} \oplus SB(k'^9_{3,3})$, the byte differences are listed below:

$$\begin{array}{llll} \Delta k^{10}_{0,0} = \Gamma, & \Delta k^{10}_{1,0} = \Lambda, & \Delta k^{10}_{2,0} = T, & \Delta k^{10}_{3,0} = \Psi, \\ \Delta k^{10}_{0,1} = \Gamma, & \Delta k^{10}_{1,1} = 0, & \Delta k^{10}_{2,1} = T, & \Delta k^{10}_{3,1} = 0, \\ \Delta k^{10}_{0,2} = 0, & \Delta k^{10}_{1,2} = 0, & \Delta k^{10}_{2,2} = T, & \Delta k^{10}_{3,2} = \Psi, \\ \Delta k^{10}_{0,3} = 0, & \Delta k^{10}_{1,3} = 0, & \Delta k^{10}_{2,3} = T, & \Delta k^{10}_{3,3} = 0. \end{array}$$

- Round 11. Let $D = SB(k^{10}_{2,3}) \oplus k^9_{2,0} \oplus SB(k'^{10}_{2,3}) \oplus k'^9_{2,0}$, we have:

$$\begin{array}{llll} \Delta k^{11}_{0,0} = \Theta, & \Delta k^{11}_{1,0} = \Phi, & \Delta k^{11}_{2,0} = D, & \Delta k^{11}_{3,0} = \Upsilon, \\ \Delta k^{11}_{0,1} = \Theta, & \Delta k^{11}_{1,1} = 0, & \Delta k^{11}_{2,1} = D, & \Delta k^{11}_{3,1} = 0, \\ \Delta k^{11}_{0,2} = 0, & \Delta k^{11}_{1,2} = 0, & \Delta k^{11}_{2,2} = D, & \Delta k^{11}_{3,2} = \Upsilon, \\ \Delta k^{11}_{0,3} = 0, & \Delta k^{11}_{1,3} = 0, & \Delta k^{11}_{2,3} = D, & \Delta k^{11}_{3,3} = 0. \end{array}$$

- Round 12. Let $S = k^{10}_{1,0} \oplus SB(k^{11}_{2,3}) \oplus k'^{10}_{1,0} \oplus SB(k'^{11}_{2,3})$, the byte differences are provided below:

$$\begin{array}{llll} \Delta k^{12}_{0,0} = \Gamma, & \Delta k^{12}_{1,0} = S, & \Delta k^{12}_{2,0} = T, & \Delta k^{12}_{3,0} = \Psi, \\ \Delta k^{12}_{0,1} = 0, & \Delta k^{12}_{1,1} = S, & \Delta k^{12}_{2,1} = 0, & \Delta k^{12}_{3,1} = \Psi, \\ \Delta k^{12}_{0,2} = 0, & \Delta k^{12}_{1,2} = S, & \Delta k^{12}_{2,2} = T, & \Delta k^{12}_{3,2} = 0, \\ \Delta k^{12}_{0,3} = 0, & \Delta k^{12}_{1,3} = S, & \Delta k^{12}_{2,3} = 0, & \Delta k^{12}_{3,3} = 0. \end{array}$$

- Round 13. Let $Q = SB(k^{12}_{1,3}) \oplus k^{11}_{1,0} \oplus SB(k'^{12}_{1,3}) \oplus k'^{11}_{1,0}$, the byte differences are represented as:

$$\begin{array}{llll} \Delta k^{13}_{0,0} = \Theta, & \Delta k^{13}_{1,0} = Q, & \Delta k^{13}_{2,0} = D, & \Delta k^{13}_{3,0} = \Upsilon, \\ \Delta k^{13}_{0,1} = 0, & \Delta k^{13}_{1,1} = Q, & \Delta k^{13}_{2,1} = 0, & \Delta k^{13}_{3,1} = \Upsilon, \\ \Delta k^{13}_{0,2} = 0, & \Delta k^{13}_{1,2} = Q, & \Delta k^{13}_{2,2} = D, & \Delta k^{13}_{3,2} = 0, \\ \Delta k^{13}_{0,3} = 0, & \Delta k^{13}_{1,3} = Q, & \Delta k^{13}_{2,3} = 0, & \Delta k^{13}_{3,3} = 0. \end{array}$$

- Round 14. Let $J = k^{12}_{0,0} \oplus SB(k^{13}_{1,3}) \oplus k'^{12}_{0,0} \oplus SB(k'^{13}_{1,3})$, the byte differences are computed as follows:

$$\begin{array}{llll} \Delta k^{14}_{0,0} = J, & \Delta k^{14}_{1,0} = S, & \Delta k^{14}_{2,0} = T, & \Delta k^{14}_{3,0} = \Psi, \\ \Delta k^{14}_{0,1} = J, & \Delta k^{14}_{1,1} = 0, & \Delta k^{14}_{2,1} = T, & \Delta k^{14}_{3,1} = 0, \\ \Delta k^{14}_{0,2} = J, & \Delta k^{14}_{1,2} = S, & \Delta k^{14}_{2,2} = 0, & \Delta k^{14}_{3,2} = 0, \\ \Delta k^{14}_{0,3} = J, & \Delta k^{14}_{1,3} = 0, & \Delta k^{14}_{2,3} = 0, & \Delta k^{14}_{3,3} = 0. \end{array}$$

- Since there is no limit on choosing X, Y, Z, and V, we can choose 255 possible values for X, 256 possible values for Y, 256 possible values for Z, and 256 possible values for V. Thus, for any 256-bit secret key K, there exist 255×256^3 possible values for K'.

■

The 14-round R differential pattern has some repeated features, which are described below.

1) The layout of the left half 16 bytes of the double-sized R differential is same as the layout of the 16 bytes of the R differential defined in Section III, and the right half 16 bytes of the double-sized R differential are all equal to zero.

2) The differential patterns of Round 2, 4, 6, 8, 10, 12 and 14 in the 14-round R differential pattern are same as the differential patterns of Round 1, 2, 3, 4, 5, 6 and 7 in the 10-round R differential pattern, respectively.
3) There are (at least) 7 zero differences in Round 0, 2, 4, 6, 8, 9, 10, 11, 12, 13 and 14. Round 1 has 16 zero differences, and Round 3 contains (at least) 12 zero differences. There are (at least) 10 zero differences in Round 5, and (at least) 8 zero differences in Round 7.

V. Future Work

The Rijndael submission document (Section 7.5, Page 28) [10] states that "A necessary condition for resistance against related-key attacks is that there should not be two different cipher keys that have a large set of round keys in common". The repeated differential properties demonstrated in this paper show that the AES-128 and AES-256 key schedules do not seem to meet this requirement. If two 128-bit secret keys have the R differential pattern (there are at least 7 zero differences in this differential pattern), the expanded round keys contain at least 7 zero differences in each round. If two 256-bit secret keys have the double-sized R differential pattern (there are at least 23 zero differences in this differential pattern), the expanded round keys have (at least) 7 zero differences in Round 0, 2, 4, 6, 8, 9, 10, 11, 12, 13 and 14, 16 zero differences in Round 1, (at least) 12 zero differences in Round 3, (at least) 10 zero differences in Round 5, and (at least) 8 zero differences in Round 7.

The potential application of the repeated differential properties is related to the related-key attacks against AES-128 and AES-256. Related-key cryptanalysis assumes that the attacker knows or chooses two (or even several) keys with certain relationship, and learns the encryptions of some plaintexts under these keys. The attacker knows only the relation between the keys, but not the actual key values. The target of the attacker is to find the keys. Since the attacks exploit the weaknesses of key schedules, a cipher with a weak key scheduling algorithm may be vulnerable to these attacks. This seems to be an interesting area for future research.

VI. Conclusion

We described some repeated differential patterns of the AES-128 and AES-256 key schedules in this paper. Our results showed that these two key scheduling algorithms are not ideal because if we use the key schedules to expand two different cipher keys with a special differential pattern, the key expansion will generate a large set of round keys in common. We also provided future research directions for investigating the potential application of the repeated differential properties.

References

[1] Biryukov, A., Khovratovich, D., Nikolić, I.: Distinguisher and Related-Key Attack on the Full AES-256. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 231-249. Springer, Heidelberg (2009)

[2] Biryukov, A., Khovratovich, D.: Related-Key Cryptanalysis of the Full AES-192 and AES-256. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 1-18. Springer, Heidelberg (2009)

[3] Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D., Shamir, A.: Key Recovery Attacks of Practical Complexity on AES-256 Variants with up to 10 Rounds. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 299-319. Springer, Heidelberg (2010)

[4] Dunkelman, O., Keller, N., Shamir, A.: Improved Single-Key Attacks on 8-Round AES-192 and AES-256. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 158-176. Springer, Heidelberg (2010)

[5] Biham, E., Dunkelman, O., Keller, N.: Related-Key Boomerang and Rectangle Attacks. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 507-525. Springer, Heidelberg (2005)

[6] Ferguson, N., Kelsey, J., Lucks, S., Schneier, B., Stay, M., Wagner, D., Whiting, D.: Improved Cryptanalysis of Rijndael. In: Schneier, B. (ed.) FSE 2000. LNCS, vol. 1978, pp. 213-230. Springer, Heidelberg (2001)

[7] Jakimoski, G., Desmedt, Y.: Related-Key Differential Cryptanalysis of 192-bit Key AES Variants. In: Matsui, M., Zuccherato, R.J. (eds.) SAC 2003. LNCS, vol. 3006, pp. 208-221. Springer, Heidelberg (2003)

[8] Kim, J., Hong, S., Preneel, B.: Related-Key Rectangle Attacks on Reduced AES-192 and AES-256. In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 225-241. Springer, Heidelberg (2007)

[9] Biryukov, A., Nikolić:, I.: Automatic Search for Related-Key Differential Characteristics in Byte-Oriented Block Ciphers: Application to AES, Camellia, Khazad and Others. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 322-344. Springer, Heidelberg (2010)

[10] Daemen, J., Rijmen, V.: AES Proposal: Rijndael. In: First Advanced Encryption Standard (AES) Candidate Conference (1998)