Algebraic Analysis of LEX

Muhammad Reza Z'aba[1] **Håvard Raddum**[2] **Leonie Simpson**[1] **Ed Dawson**[1]
Matt Henricksen[3] **Kenneth Wong**[1]

[1] Information Security Institute, Queensland University of Technology,
GPO Box 2434, Brisbane, Queensland 4001, Australia
Email: m.zaba@isi.qut.edu.au, {lr.simpson,e.dawson,kk.wong}@qut.edu.au

[2] Selmersenteret , University of Bergen, Norway
Email: haavardr@ii.uib.no

[3] Institute for Infocomm Research, A*STAR,
1 Fusionopolis Way, 21-01 Connexis, South Tower, Singapore 138632
Email: mhenricksen@i2r.a-star.edu.sg

Abstract

LEX is a stream cipher that progressed to Phase 3 of the eSTREAM stream cipher project. In this paper, we show that the security of LEX against algebraic attacks relies on a small equation system not being solvable faster than exhaustive search. We use the byte leakage in LEX to construct a system of 21 equations in 17 variables. This is very close to the requirement for an efficient attack, i.e. a system containing 16 variables. The system requires only 36 bytes of keystream, which is very low.

Keywords: LEX, Advanced Encryption Standard, Stream Cipher.

1 Introduction

LEX (Biryukov 2007) is a stream cipher submitted by Biryukov to eSTREAM, the ECRYPT stream cipher project. The basic idea of LEX is to use a block cipher as a keystream generator for a binary additive stream cipher. The keystream is formed by extracting part of the internal state at certain rounds. The security of the stream cipher is consequently linked to the way the block cipher is used in the construction.

In the LEX proposal, an example is given where the Advanced Encryption Standard (AES) (Daemen & Rijmen 2002) is chosen as the block cipher. The AES was selected because it is a standard adopted by the US National Institute of Standards and Technology (NIST) and has been extensively analyzed without any major flaws. As a keystream generator, LEX is 2.5 times faster than the block cipher AES because after 10 rounds, LEX encrypts 320 bits of data whereas the AES encrypts only 128 bits. In the remainder of this paper, the term LEX is used to refer to this specific instance based on the AES with 128-bit key.

The AES has a rich algebraic structure and the possibility of mounting algebraic attacks is still being explored. In particular, the AES has been described as a system of continued fractions over $GF(2^8)$ (Ferguson et al. 2001). It has also been studied under the so-called XSL attack using a system of equations over $GF(2)$ (Courtois & Pieprzyk 2002). Furthermore, simple multivariate quadratic equations over $GF(2^8)$ can also be derived by embedding the AES in the larger cipher BES (Murphy & Robshaw 2002). It is therefore natural to study LEX from the perspective of algebraic attacks.

This paper demonstrates that the security of LEX against algebraic attacks depends on the difficulty of solving a very small equation system. The equations are derived by linking the output keystream bytes with the unknown internal state bytes of a specific iteration and the round subkeys. As far as we know, this is the first attempt at creating a solvable equation system from the LEX technique.

This paper is organized as follows. Section 2 defines some terminologies and notations and Section 3 describes the LEX cipher. The equation systems arising from LEX are discussed in Section 4. Section 5 presents some discussions and concludes the paper.

2 Terminology and Notation

LEX is a generic method of constructing a stream cipher from a block cipher. As the modes of operation of block and stream ciphers are quite different, some terminologies need to be clarified.

A block cipher accepts a fixed-size input block and repeatedly applies a key-dependent *round function* to the block. The number of repetitions is referred to as the number of *rounds* of a block cipher. Each round function takes a *round subkey* to process the input block. The round subkeys are generated by the *key scheduling algorithm*. A block cipher is considered stateless because it does not store any information at a particular time.

A stream cipher is considered as stateful because it has an *internal state* which stores the current value of the state. The internal state is updated by the state *update function* until it reaches the specified number of *iterations*. In each iteration, the *output function* produces the output *keystream* based on the current value of the internal state.

To simplify notation, the number of rounds of the block cipher is denoted by n and the number of iterations of the stream cipher is denoted by t. In LEX, the application of one iteration means the application of one round of the block cipher's round function.

3 Description of LEX

Our investigation is restricted to LEX based on the AES with 128-bit key. The number of block cipher rounds is 10. The size of the internal state is 256 bits, which is composed of the 16-byte block A and the 16-byte secret key block K. The functions which

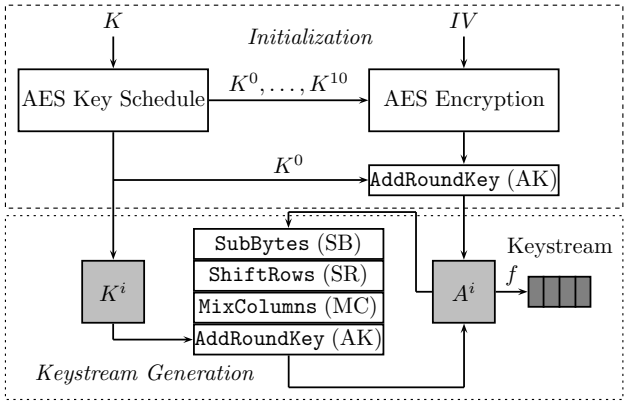

Figure 1: Initialization and keystream generation of LEX

LEX uses to initialize the internal state and how the keystream is generated are described in the following subsections, and illustrated in Figure 1.

3.1 Key Schedule and Initializaton

The 128-bit secret key K is expanded using the key scheduling algorithm to produce 11 128-bit round subkeys, denoted $K^0, \ldots, K^{10}$. All 11 round subkeys are used in the initialization process but only 10 round subkeys are used by the state update function during keystream generation. The key scheduling algorithm will be discussed in greater detail in Section 4.

The internal state is initialized by encrypting an IV with K using the full 10-round AES. According to Biryukov (2007), the encrypted IV is concatenated with K to form the initial 256-bit state of LEX, i.e. (A, K). However, as explained in the next subsection, only A is updated in each iteration. Let A^i denote the value of the block A at iteration i, E_K denote the AES encryption using the key K and $\oplus$ denote addition modulo 2 (XOR). The initialization process is as follows:

$$A^0 = E_K(IV) \oplus K^0$$

3.2 Keystream Generation

The 16-byte internal state $A = (a_0, \ldots, a_{15})$ is depicted as a 4×4 matrix. The content of this state is updated using the round function of the AES denoted by F_{K^i}. The t iterations of LEX can be described by the following algorithm:

$$A^i = F_{K^i \bmod 10}(A^{i-1}) \quad i = 1, \ldots, t$$

After the state is updated, four bytes of A^i are leaked directly by the output function f to form the keystream. The positions of the leaked bytes depend on whether the round number is odd or even. Figure 2 shows the different leak positions, which are shaded in gray. The output function f can also be described by the following equations.

$$f(A^i) = \begin{cases} (a_0^i, a_2^i, a_8^i, a_{10}^i) & \text{if } i \text{ is odd} \\ (a_4^i, a_6^i, a_{12}^i, a_{14}^i) & \text{if } i \text{ is even} \end{cases}$$

The round function F_{K^i} is composed of the following invertible transformations (Daemen & Rijmen 2002): `SubBytes` (SB), `ShiftRows` (SR), `MixColumns` (MC) and `AddRoundKey` (AK).

`SubBytes` (SB). This transformation is composed of the application of the function $S[a_j]$ to each byte a_j of the state A. Its inverse, denoted SB^{-1}, is composed of the function $S^{-1}[a_j]$.

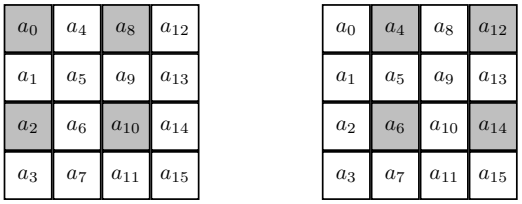

Figure 2: Different leaks in odd and even rounds

`ShiftRows` (SR). Each row of the state matrix is rotated by different offsets. The first row is not rotated. The second, third and fourth rows are rotated to the left by one, two and three bytes. The inverse, denoted SR^{-1}, applies the previous operations in reverse.

`MixColumns` (MC). Each column in the state matrix is multiplied with a fixed 4×4 matrix. Multiplication is performed in the AES $GF(2^8)$ field. If (a_0, a_1, a_2, a_3) and (b_0, b_1, b_2, b_3) are the input and output column of MC, respectively, the multiplication is done as follows:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}.$$

The inverse operation, denoted MC^{-1}, is given by the following:

$$\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} \texttt{E} & \texttt{B} & \texttt{D} & \texttt{9} \\ \texttt{9} & \texttt{E} & \texttt{B} & \texttt{D} \\ \texttt{D} & \texttt{9} & \texttt{E} & \texttt{B} \\ \texttt{B} & \texttt{D} & \texttt{9} & \texttt{E} \end{bmatrix} \times \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

where the elements in the 4×4 matrix are in hexadecimal.

`AddRoundKey` (AK). All bytes in the state A are XORed with the current round subkey bytes.

In LEX, the state update function is the AES round function, which transforms A^i to A^{i+1}. The round function is key-dependent, and makes use of 10 round subkeys $K^0, \ldots, K^9$. After 10 iterations, the state update function reuses the 10 subkeys, provided the secret key has remained unchanged. Every 10th 4-byte output is therefore produced using the same subkey. In a more secure variant of LEX, the secret key K is changed at least every 2^{32} IV setups and the IV is changed every $t = 500$ iterations.

4 Forming Equations to Describe LEX

The algebraic approach presented in this paper assumes that an attacker knows some plaintext and ciphertext pairs. For a binary additive stream cipher, this is equivalent to knowing the keystream output. This knowledge means that portions of the internal state are also known because the keystream is extracted directly from the internal state. No output filtering is used. The keystream bytes are considered as constants and the unknown portions are considered as variables to form the equations. The equations basically link the bytes of the state in a particular iteration to the bytes of the state from previous and subsequent iterations.

The following subsections will explore the equations arising from LEX. Section 4.1 discusses the equations from the encryption and decryption of the

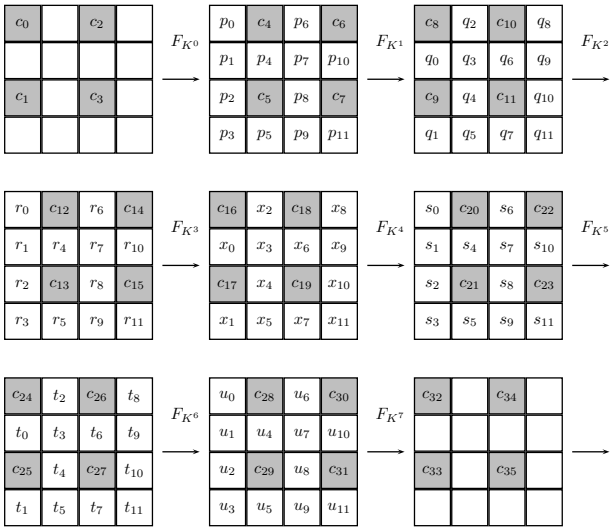

Figure 3: State byte variables and constants involved in building the system of equations.

AES. Section 4.2 explores the key schedule algorithm and Section 4.3 explains the final set of equations. Section 4.4 investigates other methods for obtaining the equations.

4.1 Encryption and Decryption Equations

Recall that 4 bytes from the 16-byte state A^i at iteration i are extracted to form the keystream. For clarity, let us fix the iteration to be $i = 3$ and let $c_{16}, \ldots, c_{19}$ represent these 4 constants. The remaining 12 variables from A^3 can be labelled as $x_0, \ldots, x_{11}$. Furthermore, let the 16 constant bytes from 4 backward (decryption) iterations be denoted by $c_0, \ldots, c_{15}$ and the 16 constant bytes from forward (encryption) iterations be denoted by $c_{20}, \ldots, c_{35}$. Each round generates four equations and hence, there are 32 equations in 12 state variables. In total, the equations span 8 rounds of the AES. The number of subkey variables is ignored for the moment.

Let $K^l = (k_{16l}, \ldots, k_{16l+15})$ denote the subkey variables. The keystream bytes involved in forming the equations are depicted in Figure 3. The figure shows the variables and constants of the internal state after they are updated using the key-dependent update function F_{K^l}. The values for the subkey variables and the temporary variables p_j,q_j,r_j,s_j,t_j,u_j are given in Appendix A. These temporary variables can be described in terms of only the x_j's and the subkey variables.

As noted earlier, the equations are built by using 12 state variables in a fixed iteration to describe constants in previous and subsequent iterations. An example is shown in Figure 4 where two equations are constructed where the variables are in an odd iteration. The upper half of the figure depicts the forming of an equation using a constant in the previous iteration. The lower half of the figure shows the forming of an equation using a constant in the subsequent iteration. Only affected variables and constants are shown.

The figure clearly shows that if a constant from a subsequent iteration is used, one byte of the round subkey is involved. If, however, a constant from a previous iteration is used, four bytes of round subkeys are involved. This is due to the order of operations in the forward and backward direction. In the forward direction, the MC operation is performed before the state is XORed with the current round subkey. In the backward direction, the current round subkey is XORed with the state before the MC^{-1} operation is performed. In essence, each byte of the current state depends on the values of 4 diagonal bytes of the state in the previous iteration. On the other hand, each byte of the same column of the state in the subsequent iteration.

At the start, the system contains 32 equations in 12 state variables and $8 + 96 + 4 = 108$ subkey variables. The subkey variables consists of 8 bytes from K^0, $6 \times 16 = 96$ bytes from $K^1, \ldots, K^6$ and 4 bytes from K^7. Note that if we do not fix the 12 state variables, the number of state variables will be $8+60+8 = 76$. These variables consists of $p_0, \ldots, p_3, p_6, \ldots, p_9$ (8 variables), $5 \times 12 = 60$ from q_j, r_j, x_j, s_j, t_j where $0 \leq j < 12$, and $u_0, u_4, u_8, u_{11}, u_6, u_{10}, u_2, u_5$ (8 variables).

The following shows 8 equations that are generated from one forward and one backward iteration. It is assumed that the x_j's are variables in an odd iteration[1]. The equations are:

$$c_{20} = \Theta(x_2, x_6, x_{10}, x_1) \oplus k_{68} \quad (1)$$
$$c_{21} = \Theta(x_{10}, x_1, x_2, x_6) \oplus k_{70} \quad (2)$$
$$c_{22} = \Theta(x_8, x_0, x_4, x_7) \oplus k_{76} \quad (3)$$
$$c_{23} = \Theta(x_4, x_7, x_8, x_0) \oplus k_{78} \quad (4)$$
$$S[c_{12}] = \Pi(x_2, x_3, x_4, x_5) \oplus \Pi(k_{52}, k_{53}, k_{54}, k_{55}) \quad (5)$$
$$S[c_{13}] = \Pi(x_{10}, x_{11}, x_8, x_9) \oplus \Pi(k_{62}, k_{63}, k_{60}, k_{61}) \quad (6)$$
$$S[c_{14}] = \Pi(x_8, x_9, x_{10}, x_{11}) \oplus \Pi(k_{60}, k_{61}, k_{62}, k_{63}) \quad (7)$$
$$S[c_{15}] = \Pi(x_4, x_5, x_2, x_3) \oplus \Pi(k_{54}, k_{55}, k_{52}, k_{53}) \quad (8)$$

where Θ and Π are defined as follows where the coefficients are in hexadecimal notation, both of which represent the operation of `MixColumns` and its inverse, respectively:

- $\Theta(z_0, z_1, z_2, z_3) = \mathtt{2}S[z_0] \oplus \mathtt{3}S[z_1] \oplus S[z_2] \oplus S[z_3]$.
- $\Pi(z_0, z_1, z_2, z_3) = \mathtt{E}z_0 \oplus \mathtt{B}z_1 \oplus \mathtt{D}z_2 \oplus \mathtt{9}z_3$.

The above equations can be used to eliminate 8 state variables using substitution. Say that the following variables are to be eliminated: $x_0, x_1, x_3, x_5, x_6, x_7, x_9$ and x_{11}. Then, the eight equations used for substitutions are:

$$x_6 = S^{-1}[\theta(S[x_2], S[x_{10}], k_{68}, k_{70}, c_{20}, c_{21})] \quad (9)$$
$$x_1 = S^{-1}[\theta(S[x_{10}], S[x_2], k_{70}, k_{68}, c_{21}, c_{20})] \quad (10)$$
$$x_0 = S^{-1}[\theta(S[x_8], S[x_4], k_{76}, k_{78}, c_{22}, c_{23})] \quad (11)$$
$$x_7 = S^{-1}[\theta(S[x_4], S[x_8], k_{78}, k_{76}, c_{23}, c_{22})] \quad (12)$$
$$x_3 = \pi(x_2, x_4, k_{52}, k_{53}, k_{54}, S[c_{12}], S[c_{15}]) \quad (13)$$
$$x_{11} = \pi(x_{10}, x_8, k_{62}, k_{63}, k_{60}, S[c_{13}], S[c_{14}]) \quad (14)$$
$$x_9 = \pi(x_8, x_{10}, k_{60}, k_{61}, k_{62}, S[c_{14}], S[c_{13}]) \quad (15)$$
$$x_5 = \pi(x_4, x_2, k_{54}, k_{55}, k_{52}, S[c_{15}], S[c_{12}]) \quad (16)$$

where θ and π are defined as follows:

- $\theta(z_0, z_1, z_2, z_3, z_4, z_5) = \mathtt{47}z_0 \oplus \mathtt{CB}(z_1 \oplus z_3 \oplus z_5) \oplus \mathtt{46}(z_2 \oplus z_4)$.
- $\pi(z_0, z_1, z_2, z_3, z_4, z_5, z_6) = \mathtt{47}(z_0 \oplus z_2) \oplus \mathtt{CB}(z_1 \oplus z_4) \oplus z_3 \oplus \mathtt{44}z_5 \oplus \mathtt{C9}z_6$.

[1] Similar equations can be generated for an even iteration number by modifying the appropriate byte positions.

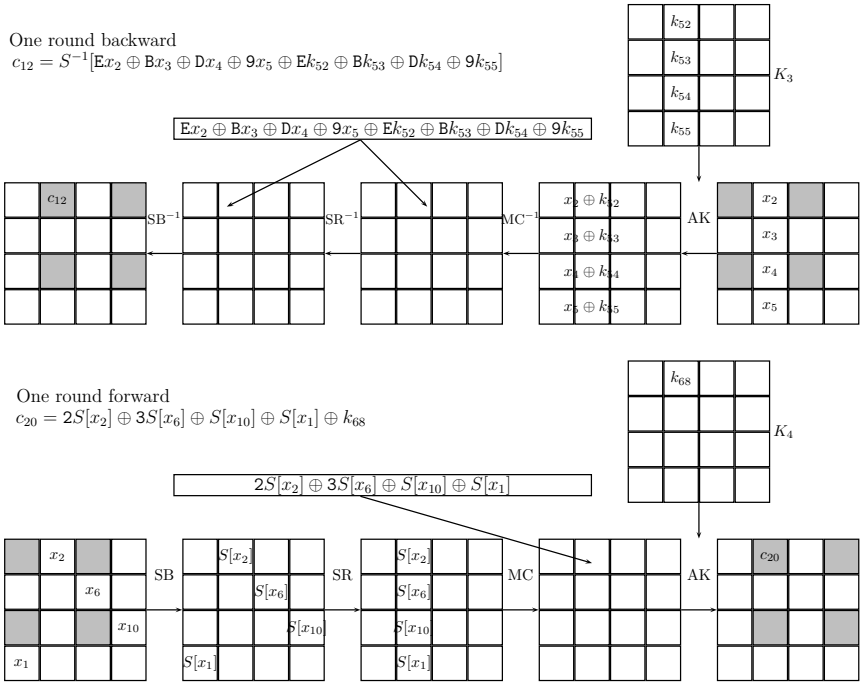

Figure 4: Example of forming 1 equation using a constant in one round backward and one round forward. Known keystream bytes (constants) are denoted in gray.

The step-by-step procedure to obtain Equations (9)–(16) is outlined in Appendix B.

The above relations are then substituted into the following remaining $32 - 8 = 24$ equations:

$$c_{24} = \Theta(s_0, s_4, s_8, s_{11}) \oplus k_{80} \quad (17)$$
$$c_{25} = \Theta(s_8, s_{11}, s_0, s_4) \oplus k_{82} \quad (18)$$
$$c_{26} = \Theta(s_6, s_{10}, s_2, s_5) \oplus k_{88} \quad (19)$$
$$c_{27} = \Theta(s_2, s_5, s_6, s_{10}) \oplus k_{90} \quad (20)$$
$$c_{28} = \Theta(t_2, t_6, t_{10}, t_1) \oplus k_{100} \quad (21)$$
$$c_{29} = \Theta(t_{10}, t_1, t_2, t_6) \oplus k_{102} \quad (22)$$
$$c_{30} = \Theta(t_8, t_0, t_4, t_7) \oplus k_{108} \quad (23)$$
$$c_{31} = \Theta(t_4, t_7, t_8, t_0) \oplus k_{110} \quad (24)$$
$$c_{32} = \Theta(u_0, u_4, u_8, u_{11}) \oplus k_{112} \quad (25)$$
$$c_{33} = \Theta(u_8, u_{11}, u_0, u_4) \oplus k_{114} \quad (26)$$
$$c_{34} = \Theta(u_6, u_{10}, u_2, u_5) \oplus k_{120} \quad (27)$$
$$c_{35} = \Theta(u_2, u_5, u_6, u_{10}) \oplus k_{122} \quad (28)$$

$$S[c_0] = \Pi(p_0, p_1, p_2, p_3) \oplus \Pi(k_0, k_1, k_2, k_3) \quad (29)$$
$$S[c_1] = \Pi(p_8, p_9, p_6, p_7) \oplus \Pi(k_{10}, k_{11}, k_8, k_9) \quad (30)$$
$$S[c_2] = \Pi(p_6, p_7, p_8, p_9) \oplus \Pi(k_8, k_9, k_{10}, k_{11}) \quad (31)$$
$$S[c_3] = \Pi(p_2, p_3, p_0, p_1) \oplus \Pi(k_2, k_3, k_0, k_1) \quad (32)$$
$$S[c_4] = \Pi(q_2, q_3, q_4, q_5) \oplus \Pi(k_{20}, k_{21}, k_{22}, k_{23}) \quad (33)$$
$$S[c_5] = \Pi(q_{10}, q_{11}, q_8, q_9) \oplus \Pi(k_{30}, k_{31}, k_{28}, k_{29}) \quad (34)$$
$$S[c_6] = \Pi(q_8, q_9, q_{10}, q_{11}) \oplus \Pi(k_{28}, k_{29}, k_{30}, k_{31}) \quad (35)$$
$$S[c_7] = \Pi(q_4, q_5, q_2, q_3) \oplus \Pi(k_{22}, k_{23}, k_{20}, k_{21}) \quad (36)$$
$$S[c_8] = \Pi(r_0, r_1, r_2, r_3) \oplus \Pi(k_{32}, k_{33}, k_{34}, k_{35}) \quad (37)$$
$$S[c_9] = \Pi(r_8, r_9, r_6, r_7) \oplus \Pi(k_{42}, k_{43}, k_{40}, k_{41}) \quad (38)$$
$$S[c_{10}] = \Pi(r_6, r_7, r_8, r_9) \oplus \Pi(k_{40}, k_{41}, k_{42}, k_{43}) \quad (39)$$
$$S[c_{11}] = \Pi(r_2, r_3, r_0, r_1) \oplus \Pi(k_{34}, k_{35}, k_{32}, k_{33}) \quad (40)$$

There are only $12 - 8 = 4$ state variables left, i.e. x_2,x_4,x_8 and x_{10}. After substituting the 8 variables, no more state variables can be eliminated using substitution due to the linear diffusion layers and the nesting of S-boxes. This system is constructed using only $9 \times 4 = 36$ bytes of the keystream, generated under the same secret key.

4.2 Key Schedule Equations

Note that the generation of round subkeys is performed independently to the keystream generation. Every byte of subkey K^i in Round i is affected by at least one subkey byte K^{i-1} in Round $i-1$ where $1 \leq i < 10$. Each of the first four subkey bytes is composed of the XOR of two different subkey bytes in the previous round. The remaining 12 subkey bytes are composed of the XOR of one subkey byte in the current round and one subkey byte from the previous round. The algorithm to compute the i-th round subkey of LEX is given by the following equations.

$$\begin{array}{ll|ll}
k^{\acute{i}}_i & = k^{\hat{i}}_i \oplus S[k^{\hat{i}}_{i+13}] \oplus R^i & k^{\acute{i}}_{i+8} & = k^{\hat{i}}_{i+8} \oplus k^{\acute{i}}_{i+4} \\
k^{\acute{i}}_{i+1} & = k^{\hat{i}}_{i+1} \oplus S[k^{\hat{i}}_{i+14}] & k^{\acute{i}}_{i+9} & = k^{\hat{i}}_{i+9} \oplus k^{\acute{i}}_{i+5} \\
k^{\acute{i}}_{i+2} & = k^{\hat{i}}_{i+2} \oplus S[k^{\hat{i}}_{i+15}] & k^{\acute{i}}_{i+10} & = k^{\hat{i}}_{i+10} \oplus k^{\acute{i}}_{i+6} \\
k^{\acute{i}}_{i+3} & = k^{\hat{i}}_{i+3} \oplus S[k^{\hat{i}}_{i+12}] & k^{\acute{i}}_{i+11} & = k^{\hat{i}}_{i+11} \oplus k^{\acute{i}}_{i+7} \\
k^{\acute{i}}_{i+4} & = k^{\hat{i}}_{i+4} \oplus k^{\acute{i}}_i & k^{\acute{i}}_{i+12} & = k^{\hat{i}}_{i+12} \oplus k^{\acute{i}}_{i+8} \\
k^{\acute{i}}_{i+5} & = k^{\hat{i}}_{i+5} \oplus k^{\acute{i}}_{i+1} & k^{\acute{i}}_{i+13} & = k^{\hat{i}}_{i+13} \oplus k^{\acute{i}}_{i+9} \\
k^{\acute{i}}_{i+6} & = k^{\hat{i}}_{i+6} \oplus k^{\acute{i}}_{i+2} & k^{\acute{i}}_{i+14} & = k^{\hat{i}}_{i+14} \oplus k^{\acute{i}}_{i+10} \\
k^{\acute{i}}_{i+7} & = k^{\hat{i}}_{i+7} \oplus k^{\acute{i}}_{i+3} & k^{\acute{i}}_{i+15} & = k^{\hat{i}}_{i+15} \oplus k^{\acute{i}}_{i+11}
\end{array}$$

where $K^i = (k_{16i}, \ldots, k_{16i+15})$, $\acute{i} = 16i$, $\hat{i} = 16(i-1)$, $1 \leq i < 10$ and R^i is the round constant.

During keystream generation, LEX uses the same set of 10-round subkeys every 10-iteration block, provided that the secret key is unchanged. Building equations that link all the output keystream of r rounds ($r \geq 2$) involves $16(r-1)$ subkey variables. Due to the simple structure of the key schedule, the equations can be rearranged so that only 16 variables remain, even though $r > 2$.

Let $K^0, \ldots, K^7$ represent the $8 \times 16 = 128$ subkey variables involved in the equations that link the output keystream of 9 rounds. The equations can be

constructed in terms of the 16 subkey variables in K^3. Recall that in the AES, K^i is described in terms of K^{i-1} and K^i. We can rearrange this so that for instance, $K^2 = (k_{32}, \ldots, k_{47})$ can be written in terms of $K^3 = (k_{48}, \ldots, k_{63})$ only, as follows:

$$\begin{array}{ll} k_{32} = k_{48} \oplus S[k_{61} \oplus k_{57}] \oplus R^3 & k_{40} = k_{56} \oplus k_{52} \\ k_{33} = k_{49} \oplus S[k_{62} \oplus k_{58}] & k_{41} = k_{57} \oplus k_{53} \\ k_{34} = k_{50} \oplus S[k_{63} \oplus k_{59}] & k_{42} = k_{58} \oplus k_{54} \\ k_{35} = k_{51} \oplus S[k_{60} \oplus k_{56}] & k_{43} = k_{59} \oplus k_{55} \\ k_{36} = k_{52} \oplus k_{48} & k_{44} = k_{60} \oplus k_{56} \\ k_{37} = k_{53} \oplus k_{49} & k_{45} = k_{61} \oplus k_{57} \\ k_{38} = k_{54} \oplus k_{50} & k_{46} = k_{62} \oplus k_{58} \\ k_{39} = k_{55} \oplus k_{51} & k_{47} = k_{63} \oplus k_{59} \end{array}$$

In the general case, additional substitutions are required. For instance, the following describes $K^4 = (k_{64}, \ldots, k_{79})$ in terms of K^3 only:

$$\begin{aligned} k_{64} &= k_{48} \oplus S[k_{61}] \oplus R^4 \\ k_{65} &= k_{49} \oplus S[k_{62}] \\ k_{66} &= k_{50} \oplus S[k_{63}] \\ k_{67} &= k_{51} \oplus S[k_{60}] \\ k_{68} &= k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4 \\ k_{69} &= k_{53} \oplus k_{49} \oplus S[k_{62}] \\ k_{70} &= k_{54} \oplus k_{50} \oplus S[k_{63}] \\ k_{71} &= k_{55} \oplus k_{51} \oplus S[k_{60}] \\ k_{72} &= k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4 \\ k_{73} &= k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}] \\ k_{74} &= k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}] \\ k_{75} &= k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}] \\ k_{76} &= k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4 \\ k_{77} &= k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}] \\ k_{78} &= k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}] \\ k_{79} &= k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}] \end{aligned}$$

Using the above logic, the variables in K^0, K^1, K^5, K^6, K^7 can be described in terms of K^3 in similar way. The full subkey substitution is given in Appendix A.3. These key schedule equations are then substituted in the encryption and decryption equations and thus, only 16 subkey variables remain.

4.3 The Final Equation System

After substituting the subkey variables, Equations (17) and (19), respectively have the following form.

$$\Theta(v_0, v_1, v_2, k_{59} \oplus v_3) \oplus K_0^* \oplus c_{24} = 0 \qquad (41)$$
$$\Theta(w_0, w_1, w_2, k_{51} \oplus w_3) \oplus K_1^* \oplus c_{26} = 0 \qquad (42)$$

where the temporary variables v_j,w_j and K_j^* are defined in Appendix A.4.

A careful examination of the above equations reveals that two more round subkey variables can be eliminated. The first one can be removed as follows.

By looking at Equation (41) we find that it contains only a single k_{59}. Isolating this variable results in the following equation:

$$k_{59} = S^{-1}[\Theta(v_0, v_1, v_2, 0) \oplus K_0^* \oplus c_{24}] \oplus v_3$$

The above equation is then substituted into the remaining 23 equations. The second subkey variable can be eliminated by using the fact that Equation (42) does not contain k_{59} which consequently means that Equation (42) is not affected by the previous substitution. It turns out that the subkey variable k_{51} only appears once in Equation (42) and can be isolated and described in terms of the other variables as follows:

$$k_{51} = S^{-1}[\Theta(w_0, w_1, w_2, 0) \oplus K_1^* \oplus c_{26}] \oplus w_3$$

The above equation is substituted into the remaining 22 equations, where only 4 state and $16 - 2 = 14$ subkey variables remain (18 variables in total).

Further examination reveals that one more subkey variable can be eliminated. After substituting the previous subkey variables, Equation (18) becomes the following:

$$y_0 \oplus y_1 \oplus y_2 \oplus S[y_3 \oplus \mathtt{CB}k_{56}] \oplus K_2^* \oplus c_{25} = 0$$

where the temporary variables y_j and K_2^* are defined in Appendix A.4.

It can be noted that the above equation contains only a single k_{56}. This subkey variable can be isolated and described in terms of other variables as follows:

$$k_{56} = \mathtt{4}S^{-1}[y_0 \oplus y_1 \oplus y_2 \oplus K_2^* \oplus c_{25}] \oplus \mathtt{4}y_3$$

The right hand side of the above equation contains all the remaining 17 variables. The subkey variable k_{56} also occurs in every remaining equation; moreover, there are 1233 occurences of k_{56} detected throughout all equations. After performing the substitution, there are $22 - 1 = 21$ equations in 4 state and $14 - 1 = 13$ subkey variables left in the system (17 variables in total).

We could not find any more key variables that can be isolated this way after these substitutions. This is because the same variable occurs inside and outside of the S-box in the same equation. For instance, if we have an equation of the form $x \oplus S[x] \oplus \ldots = 0$, where x is a variable, it is not possible to isolate x.

In forming the equation system, we managed to reduce the number of variables from $12 + 16 = 28$ to 17. This is only one variable away from the limit of an exhaustive search, i.e., 16. The equation system is also very straightforward to construct. Recall from Section 4.1 that the system requires only 36 bytes of known keystream, generated under the same secret key. In terms of required number of keystream, this is very low. The final set of equations are given in Appendix A.5.

Note that for an efficient attack, the effort required to break the cipher must be less than performing an exhaustive search of the key space. One way of solving the system of equations is to guess the value of all variables and discard guesses for which the equations are inconsistent. We have 21 equations, which is 4 more than the number of variables in the system and thus, with very high probability, there is only one solution to the system. This solution must correspond to the correct key. If the number of variables is less than the number of key bytes (in our case, 16), solving the system can be faster than exhaustive search.

Another possible way of solving the equations is to only guess certain variables. The reasoning for this is that the equations might be significantly simplified if the partial guess is made. The simplified equations are expected to be much easier to solve than the original equation system. In order for this to work, we must be able to determine which subset of variables provide the greatest simplification for the equation system, and to be able to verify whether the partial guess is right or wrong, with high probability.

In the system of equations, there are many expressions that occur frequently. These frequent expressions are made up of the sum of some key or/and

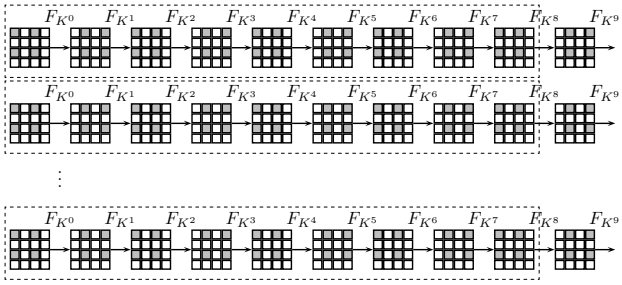

Figure 5: Keystream involved in forming system of equations.

state variables. The common expressions are denoted as W_j, Y_j and Z_j in the final set of equations given in Appendix A.5. Some of these expressions contain as few as four variables; however, almost all of them contain the entire 17 variables. For example, consider the following equation, which is the last of the 21 equations given in Appendix A.5:

$$\hat{\Pi}(Z_{10}, Z_{11}, Z_8, Z_9) \oplus T_{60} \oplus S[c_{11}] = 0$$

where Z_j are expressions, $\hat{\Pi}(z_0, z_1, z_2, z_3) = \mathtt{E}S^{-1}[z_0] \oplus \mathtt{B}S^{-1}[z_1] \oplus \mathtt{D}S^{-1}[z_2] \oplus \mathtt{9}S^{-1}[z_3]$ and T_{60} is composed of the sum of some state and key variables. The expressions Z_9 and Z_{11} contain four variables while Z_8 and Z_{10} contain the entire 17 variables. Even if the variables in Z_9 and Z_{11} are guessed, there are still $17 - 4 = 13$ variables left in Z_8 and Z_{10}. In this case, the guesses do not simplify the equation. As a result of this, we were unable to identify any subset of state or/and key variables that can be guessed to simplify any equation.

4.4 Alternative Methods for Obtaining Equations

The fact that the same subkey is used in every 10th round can be used to obtain additional equations by repeating the previous system as much as needed, across 10-round blocks. For each repetition, both the number of equations and state variables increase. The number of round subkey variables, however, remains unchanged.

This is illustrated in Figure 5 where the dotted lines represent the keystream and state update functions involved in forming the equations. It can be clearly seen that the previous system of equations span 8 rounds of the AES, i.e. two rounds short of the full AES. However, the system needs the output keystream of 9 rounds of the AES.

Since LEX uses the same set of 10 round subkeys repeatedly, the number of round subkeys remains unchanged if the same system of equations is formed for the next 10-round block. Each repetition of the system only adds another 21 equations and 4 state variables to the current system. For instance, repeating the same system another 2 times gives $3 \times 21 = 63$ equations in $13 + 3 \times 4 = 25$ variables.

Another method of obtaining equations is to use only the constants that appear in the iterations that include 2 forward and 2 backward iterations from a fixed iteration. This system spans 4 rounds of the AES and uses the output keystream of 5 rounds. Initially, this system has $4 \times 4 = 16$ equations in 12 state variables and $8 + 2 \times 16 + 4 = 44$ subkey variables. If the same fixed state variables are used as before, the system starts at the output of F_K^1 and ends at the output of F_K^5. Refer again to Figure 5 for illustration.

Assuming the same notations for variables and constants as before, we can use Equations (9) to (16) to substitute into the remaining $16 - 8 = 8$ equations. After substitution, $12 - 8 = 4$ state variables are left. As explained in Section 4.2, the subkey variables can be substituted so that only 16 remain. We can use the same technique to eliminate 3 more subkey variables as outlined in Section 4.3. Assuming no more variables can be eliminated, there are $8 - 3 = 5$ equations in $4 + 13 = 17$ variables which span 4 rounds of the AES. As before, the system can be repeated as much as needed, by going across 10-round blocks. Each repetition adds 5 equations and 4 variables. The initial equations are constructed using only $5 \times 4 = 20$ bytes of keystream.

Similarly, we can use constants that appear in the iteration which includes 3 forward and 3 backward iterations from a fixed iteration. The resulting equations span 6 rounds of the AES and uses the output keystream of 7 rounds. After the same elimination as before is performed, we are left with $6 \times 4 - 11 = 13$ equations in $4 + 13 = 17$ variables. This system can also be repeated as much as needed, by going across 10-round blocks. Each repetition adds 13 equations and 4 variables. The amount of known keystream needed to construct the initial system is $7 \times 4 = 28$ bytes.

The final form for the sets of equations that span 4 and 6 rounds of the AES are expected to be simpler compared to the previous system that spans 8 rounds. If only the base equations are used (without repeating the system by going across 10-round blocks), the two systems (which span 4 and 6 rounds of the AES) are underdefined since the number of variables are greater than the number of equations. If, however, the systems are repeated, the additional number of known keystream is still considerably low.

5 Discussion and Conclusion

There are two versions of LEX. The first version uses the full AES in both the IV setup and the state update function. It was therefore vulnerable to a slide attack, where a particular key can be recovered if used with about 2^{61} random IVs (Wu & Preneel 2006). In order to resist this attack, a second version (Biryukov 2007) of LEX was proposed. This version uses the full AES in the IV setup but a slightly modified AES in the state update function. This variant was subjected to a key recovery attack by Dunkelman & Keller (2008) which requires $2^{36.3}$ bytes of keystream and 2^{112} operations. They also note that their attack can also be adopted to the first version of LEX. This attack was one of the reasons LEX was dropped from the final eSTREAM portfolio (Babbage et al. 2008). The variant of LEX examined in this paper is based on this second version.

In this paper, it is shown that the security of LEX relies on the solution of a small system of equations. It contains 21 equations in 4 state and 13 subkey variables. This system spans eight rounds of the AES, which at the start involves 32 equations in 12 state and 108 subkey variables. It is a massive reduction in terms of the number of variables and is very close to the limit for an efficient attack, i.e. 16 variables.

Although the work presented in this paper does not provide a key recovery attack, and the work of Dunkelman & Keller (2008) does, this paper is still important for two reasons. First, as always with algebraic attacks, we need very little known keystream. This makes an attack by solving an equation system needing 36 bytes of known keystream more threatening in a real-world situation than attacks needing almost 85 billion ($2^{36.3}$) bytes of known keystream. Note that the LEX specification states that the amount of keystream to be produced from

one key and IV pair should not exceed 2000 bytes for a secure LEX variant. Our work, therefore, can be applied to this variant while previous attacks cannot. Second, the constructed equation system is almost sufficient for an efficient attack. Guessing 16 bytes is the limit for an efficient attack, we need to guess 17 in order to solve our system. Traditionally, attacks on block ciphers have been classified as to how many rounds a particular attack is able to break, out of the full number of rounds. The small difference between 17 and 16 leads us to think that the attack presented here has the same strength as an attack on a block cipher that falls only one or two rounds short of breaking the full cipher.

We did not use any clever tricks in constructing our equation system in this paper. It is a tedious but straightforward job to construct the system and then start eliminating variables. In particular, we did not make any use of the algebraic properties of the S-box. As known from literature (Daemen & Rijmen 2002), the S-box can be replaced with the following polynomial equation:

$$S[x] = \mathtt{5}x^{254} \oplus \mathtt{9}x^{253} \oplus \mathtt{F9}x^{251} \oplus \mathtt{25}x^{247} \oplus \mathtt{F4}x^{239} \oplus \mathtt{B5}x^{223} \oplus \mathtt{B9}x^{191} \oplus \mathtt{8F}x^{127} \oplus \mathtt{63}$$

The inverse S-box polynomial equation, however, is denser than the above equation. It contains 247 terms and is given in Appendix A of the paper by Buchmann et al. (2006). The complicated structure of the inverse equations makes solving the equations very hard. The degree of the resulting equation system is also expected to be very high. This leaves room for further research. It is fully possible that one can improve on the results we obtained.

Finally, note that LEX is intended as a generic method of constructing a stream cipher from a block cipher. In this paper, a specific instance of LEX which uses the AES has been explored in terms of building a small system of equations. The AES is known to be a very strong cipher. Yet we have shown that the resulting equation system is very close to the threshold for key recovery. If other possibly weak block ciphers are used in this manner, the security of the stream cipher is surely questionable. This remains an area of further investigation, and we think that the result in this paper shows that one must thoroughly investigate algebraic attacks when using the LEX design with a different block cipher than the AES.

References

Babbage, S., De Cannière, C., Canteaut, A., Cid, C., Gilbert, H., Johansson, T., Parker, M. & Preneel, B., (2008), The eSTREAM Portfolio, *in* 'eSTREAM, ECRYPT Stream Cipher Project', `http://www.ecrypt.eu.org/stream/`.

Biryukov, A. (2007), The Design of a Stream Cipher LEX, *in* Biham, E. & Youssef, A.M., eds, 'Selected Areas in Cryptography, 13th International Workshop, SAC 2006', Vol. 4356, LNCS Springer, Heidelberg, pp. 67–75.

Buchmann, J., Pyshkin, A. & Weinmann, R-.P. (2006), A Zero-Dimensional Gröbner Basis for AES-128, *in* Robshaw, M.J.B., ed, 'Fast Software Encryption: 13th International Workshop, FSE 2006', Vol. 4047, LNCS Springer, Heidelberg, pp. 78–88.

Cid, C., Murphy, S. & Robshaw, M.J.B. (2005), Small Scale Variants of the AES, *in* Gilbert, H & Handschuh, H., eds, 'Fast Software Encryption: 12th International Workshop, FSE 2005', Vol. 3557, LNCS Springer, Heidelberg, pp. 145–162.

Courtois, N.T. & Pieprzyk, J. (2002), Cryptanalysis of Block Ciphers with Overdefined Systems of Equations, *in* 'Advances in Cryptology – ASIACRYPT 2002: 8th International Conference on the Theory and Application of Cryptology and Information Security', Vol. 2501, LNCS Springer, Heidelberg, pp. 267–287.

Daemen, J. & Rijmen, V. (2002), *The Design of Rijndael, AES – The Advanced Encryption Standard*, Springer, Heidelberg.

Dunkelman, O. & Keller, N. (2008), A New Attack on the LEX Stream Cipher, *in* 'eSTREAM, ECRYPT Stream Cipher Project, Report 2008/016', `http://www.ecrypt.eu.org/stream/`.

Ferguson, N., Schroeppel, R. & Whiting, D. (2001), A Simple Algebraic Representation of Rijndael, *in* 'Selected Areas in Cryptography: 8th Annual International Workshop', Vol. 2259, LNCS Springer, Heidelberg, pp. 103–111.

Murphy, S. & Robshaw, M.J.B. (2002), Essential Algebraic Structure within the AES, *in* 'Advances in Cryptology – CRYPTO 2002', Vol. 2442, LNCS Springer, Heidelberg, pp. 1–16.

Wu, H. & Preneel, B. (2006), Resynchronization Attacks on WG and LEX, *in* 'Fast Software Encryption: 13th International Workshop, FSE 2006', Vol. 4047, LNCS Springer, Heidelberg, pp. 422–432.

A Equations

The following list the relations of the temporary variables p_i,q_i,r_i,s_i,t_i,u_i in the forward and backward directions. These variables are substituted so that only the x_i variables remain.

A.1 Forward Direction

- $s_0 = \Theta(c_{16}, x_3, c_{19}, x_{11}) \oplus k_{64}$
- $s_1 = \Theta(x_3, c_{19}, x_{11}, c_{16}) \oplus k_{65}$
- $s_2 = \Theta(c_{19}, x_{11}, c_{16}, x_3) \oplus k_{66}$
- $s_3 = \Theta(x_{11}, c_{16}, x_3, c_{19}) \oplus k_{67}$
- $s_4 = \Theta(x_6, x_{10}, x_1, x_2) \oplus k_{69}$
- $s_5 = \Theta(x_1, x_2, x_6, x_{10}) \oplus k_{71}$
- $s_6 = \Theta(c_{18}, x_9, c_{17}, x_5) \oplus k_{72}$
- $s_7 = \Theta(x_9, c_{17}, x_5, c_{18}) \oplus k_{73}$
- $s_8 = \Theta(c_{17}, x_5, c_{18}, x_9) \oplus k_{74}$
- $s_9 = \Theta(x_5, c_{18}, x_9, c_{17}) \oplus k_{75}$
- $s_{10} = \Theta(x_0, x_4, x_7, x_8) \oplus k_{77}$
- $s_{11} = \Theta(x_7, x_8, x_0, x_4) \oplus k_{79}$
- $t_0 = \Theta(s_4, s_8, s_{11}, s_0) \oplus k_{81}$
- $t_1 = \Theta(s_{11}, s_0, s_4, s_8) \oplus k_{83}$
- $t_2 = \Theta(c_{20}, s_7, c_{23}, s_3) \oplus k_{84}$
- $t_3 = \Theta(s_7, c_{23}, s_3, c_{20}) \oplus k_{85}$
- $t_4 = \Theta(c_{23}, s_3, c_{20}, s_7) \oplus k_{86}$
- $t_5 = \Theta(s_3, c_{20}, s_7, c_{23}) \oplus k_{87}$
- $t_6 = \Theta(s_{10}, s_2, s_5, s_6) \oplus k_{89}$

- $t_7 = \Theta(s_5, s_6, s_{10}, s_2) \oplus k_{91}$
- $t_8 = \Theta(c_{22}, s_1, c_{21}, s_9) \oplus k_{92}$
- $t_9 = \Theta(s_1, c_{21}, s_9, c_{22}) \oplus k_{93}$
- $t_{10} = \Theta(c_{21}, s_9, c_{22}, s_1) \oplus k_{94}$
- $t_{11} = \Theta(s_9, c_{22}, s_1, c_{21}) \oplus k_{95}$
- $u_0 = \Theta(c_{24}, t_3, c_{27}, t_{11}) \oplus k_{96}$
- $u_1 = \Theta(t_3, c_{27}, t_{11}, c_{24}) \oplus k_{97}$
- $u_2 = \Theta(c_{27}, t_{11}, c_{24}, t_3) \oplus k_{98}$
- $u_3 = \Theta(t_{11}, c_{24}, t_3, c_{27}) \oplus k_{99}$
- $u_4 = \Theta(t_6, t_{10}, t_1, t_2) \oplus k_{101}$
- $u_5 = \Theta(t_1, t_2, t_6, t_{10}) \oplus k_{103}$
- $u_6 = \Theta(c_{26}, t_9, c_{25}, t_5) \oplus k_{104}$
- $u_7 = \Theta(t_9, c_{25}, t_5, c_{26}) \oplus k_{105}$
- $u_8 = \Theta(c_{25}, t_5, c_{26}, t_9) \oplus k_{106}$
- $u_9 = \Theta(t_5, c_{26}, t_9, c_{25}) \oplus k_{107}$
- $u_{10} = \Theta(t_0, t_4, t_7, t_8) \oplus k_{109}$
- $u_{11} = \Theta(t_7, t_8, t_0, t_4) \oplus k_{111}$

A.2 Backward Direction

- $r_0 = S^{-1}[\Pi(c_{16}, x_0, c_{17}, x_1) \oplus \Pi(k_{48}, k_{49}, k_{50}, k_{51})]$
- $r_1 = S^{-1}[\Pi(x_9, x_{10}, x_{11}, x_8) \oplus \Pi(k_{61}, k_{62}, k_{63}, k_{60})]$
- $r_2 = S^{-1}[\Pi(c_{19}, x_7, c_{18}, x_6) \oplus \Pi(k_{58}, k_{59}, k_{56}, k_{57})]$
- $r_3 = S^{-1}[\Pi(x_5, x_2, x_3, x_4) \oplus \Pi(k_{55}, k_{52}, k_{53}, k_{54})]$
- $r_4 = S^{-1}[\Pi(x_0, c_{17}, x_1, c_{16}) \oplus \Pi(k_{49}, k_{50}, k_{51}, k_{48})]$
- $r_5 = S^{-1}[\Pi(x_7, c_{18}, x_6, c_{19}) \oplus \Pi(k_{59}, k_{56}, k_{57}, k_{58})]$
- $r_6 = S^{-1}[\Pi(c_{18}, x_6, c_{19}, x_7) \oplus \Pi(k_{56}, k_{57}, k_{58}, k_{59})]$
- $r_7 = S^{-1}[\Pi(x_3, x_4, x_5, x_2) \oplus \Pi(k_{53}, k_{54}, k_{55}, k_{52})]$
- $r_8 = S^{-1}[\Pi(c_{17}, x_1, c_{16}, x_0) \oplus \Pi(k_{50}, k_{51}, k_{48}, k_{49})]$
- $r_9 = S^{-1}[\Pi(x_{11}, x_8, x_9, x_{10}) \oplus \Pi(k_{63}, k_{60}, k_{61}, k_{62})]$
- $r_{10} = S^{-1}[\Pi(x_6, c_{19}, x_7, c_{18}) \oplus \Pi(k_{57}, k_{58}, k_{59}, k_{56})]$
- $r_{11} = S^{-1}[\Pi(x_1, c_{16}, x_0, c_{17}) \oplus \Pi(k_{51}, k_{48}, k_{49}, k_{50})]$
- $q_0 = S^{-1}[\Pi(r_{10}, c_{15}, r_{11}, c_{14}) \oplus \Pi(k_{45}, k_{46}, k_{47}, k_{44})]$
- $q_1 = S^{-1}[\Pi(r_5, c_{12}, r_4, c_{13}) \oplus \Pi(k_{39}, k_{36}, k_{37}, k_{38})]$
- $q_2 = S^{-1}[\Pi(c_{12}, r_4, c_{13}, r_5) \oplus \Pi(k_{36}, k_{37}, k_{38}, k_{39})]$
- $q_3 = S^{-1}[\Pi(r_1, r_2, r_3, r_0) \oplus \Pi(k_{33}, k_{34}, k_{35}, k_{32})]$
- $q_4 = S^{-1}[\Pi(c_{15}, r_{11}, c_{14}, r_{10}) \oplus \Pi(k_{46}, k_{47}, k_{44}, k_{45})]$
- $q_5 = S^{-1}[\Pi(r_9, r_6, r_7, r_8) \oplus \Pi(k_{43}, k_{40}, k_{41}, k_{42})]$
- $q_6 = S^{-1}[\Pi(r_4, c_{13}, r_5, c_{12}) \oplus \Pi(k_{37}, k_{38}, k_{39}, k_{36})]$
- $q_7 = S^{-1}[\Pi(r_{11}, c_{14}, r_{10}, c_{15}) \oplus \Pi(k_{47}, k_{44}, k_{45}, k_{46})]$
- $q_8 = S^{-1}[\Pi(c_{14}, r_{10}, c_{15}, r_{11}) \oplus \Pi(k_{44}, k_{45}, k_{46}, k_{47})]$
- $q_9 = S^{-1}[\Pi(r_7, r_8, r_9, r_6) \oplus \Pi(k_{41}, k_{42}, k_{43}, k_{40})]$
- $q_{10} = S^{-1}[\Pi(c_{13}, r_5, c_{12}, r_4) \oplus \Pi(k_{38}, k_{39}, k_{36}, k_{37})]$
- $q_{11} = S^{-1}[\Pi(r_3, r_0, r_1, r_2) \oplus \Pi(k_{35}, k_{32}, k_{33}, k_{34})]$
- $p_0 = S^{-1}[\Pi(c_8, q_0, c_9, q_1) \oplus \Pi(k_{16}, k_{17}, k_{18}, k_{19})]$
- $p_1 = S^{-1}[\Pi(q_9, q_{10}, q_{11}, q_8) \oplus \Pi(k_{29}, k_{30}, k_{31}, k_{28})]$
- $p_2 = S^{-1}[\Pi(c_{11}, q_7, c_{10}, q_6) \oplus \Pi(k_{26}, k_{27}, k_{24}, k_{25})]$
- $p_3 = S^{-1}[\Pi(q_5, q_2, q_3, q_4) \oplus \Pi(k_{23}, k_{20}, k_{21}, k_{22})]$
- $p_4 = S^{-1}[\Pi(q_0, c_9, q_1, c_8) \oplus \Pi(k_{17}, k_{18}, k_{19}, k_{16})]$
- $p_5 = S^{-1}[\Pi(q_7, c_{10}, q_6, c_{11}) \oplus \Pi(k_{27}, k_{24}, k_{25}, k_{26})]$
- $p_6 = S^{-1}[\Pi(c_{10}, q_6, c_{11}, q_7) \oplus \Pi(k_{24}, k_{25}, k_{26}, k_{27})]$
- $p_7 = S^{-1}[\Pi(q_3, q_4, q_5, q_2) \oplus \Pi(k_{21}, k_{22}, k_{23}, k_{20})]$
- $p_8 = S^{-1}[\Pi(c_9, q_1, c_8, q_0) \oplus \Pi(k_{18}, k_{19}, k_{16}, k_{17})]$
- $p_9 = S^{-1}[\Pi(q_{11}, q_8, q_9, q_{10}) \oplus \Pi(k_{31}, k_{28}, k_{29}, k_{30})]$
- $p_{10} = S^{-1}[\Pi(q_6, c_{11}, q_7, c_{10}) \oplus \Pi(k_{25}, k_{26}, k_{27}, k_{24})]$
- $p_{11} = S^{-1}[\Pi(q_1, c_8, q_0, c_9) \oplus \Pi(k_{19}, k_{16}, k_{17}, k_{18})]$

A.3 Subkey Variables Substitution

The following substitutions are performed so that only 16 subkey variables remain.

- $k_0 = k_{48} \oplus S[k_{61} \oplus k_{57}] \oplus S[k_{61} \oplus k_{53}] \oplus S[k_{61} \oplus k_{53} \oplus k_{57} \oplus k_{49}] \oplus R^1 \oplus R^2 \oplus R^3$
- $k_1 = k_{49} \oplus S[k_{62} \oplus k_{58}] \oplus S[k_{62} \oplus k_{54}] \oplus S[k_{62} \oplus k_{54} \oplus k_{58} \oplus k_{50}]$
- $k_2 = k_{50} \oplus S[k_{63} \oplus k_{59}] \oplus S[k_{63} \oplus k_{55}] \oplus S[k_{63} \oplus k_{55} \oplus k_{59} \oplus k_{51}]$
- $k_3 = k_{51} \oplus S[k_{60} \oplus k_{56}] \oplus S[k_{60} \oplus k_{52}] \oplus S[k_{60} \oplus k_{52} \oplus k_{56} \oplus k_{48}]$
- $k_4 = k_{48} \oplus k_{52} \oplus S[k_{61} \oplus k_{53}] \oplus R^2$
- $k_5 = k_{49} \oplus k_{53} \oplus S[k_{62} \oplus k_{54}]$
- $k_6 = k_{50} \oplus k_{54} \oplus S[k_{63} \oplus k_{55}]$
- $k_7 = k_{51} \oplus k_{55} \oplus S[k_{60} \oplus k_{52}]$
- $k_8 = k_{48} \oplus k_{52} \oplus k_{56} \oplus S[k_{61} \oplus k_{57}] \oplus R^3$
- $k_9 = k_{49} \oplus k_{53} \oplus k_{57} \oplus S[k_{62} \oplus k_{58}]$
- $k_{10} = k_{50} \oplus k_{54} \oplus k_{58} \oplus S[k_{63} \oplus k_{59}]$
- $k_{11} = k_{51} \oplus k_{55} \oplus k_{59} \oplus S[k_{60} \oplus k_{56}]$
- $k_{12} = k_{48} \oplus k_{52} \oplus k_{56} \oplus k_{60}$
- $k_{13} = k_{49} \oplus k_{53} \oplus k_{57} \oplus k_{61}$
- $k_{14} = k_{50} \oplus k_{54} \oplus k_{58} \oplus k_{62}$
- $k_{15} = k_{51} \oplus k_{55} \oplus k_{59} \oplus k_{63}$

- $k_{16} = k_{48} \oplus S[k_{61} \oplus k_{57}] \oplus S[k_{61} \oplus k_{53}] \oplus R^2 \oplus R^3$
- $k_{17} = k_{49} \oplus S[k_{62} \oplus k_{58}] \oplus S[k_{62} \oplus k_{54}]$
- $k_{18} = k_{50} \oplus S[k_{63} \oplus k_{59}] \oplus S[k_{63} \oplus k_{55}]$
- $k_{19} = k_{51} \oplus S[k_{60} \oplus k_{56}] \oplus S[k_{60} \oplus k_{52}]$
- $k_{20} = k_{52} \oplus S[k_{61} \oplus k_{57}] \oplus R^3$
- $k_{21} = k_{53} \oplus S[k_{62} \oplus k_{58}]$
- $k_{22} = k_{54} \oplus S[k_{63} \oplus k_{59}]$
- $k_{23} = k_{55} \oplus S[k_{60} \oplus k_{56}]$
- $k_{24} = k_{48} \oplus k_{56}$
- $k_{25} = k_{49} \oplus k_{57}$
- $k_{26} = k_{50} \oplus k_{58}$
- $k_{27} = k_{51} \oplus k_{59}$
- $k_{28} = k_{52} \oplus k_{60}$
- $k_{29} = k_{53} \oplus k_{61}$
- $k_{30} = k_{54} \oplus k_{62}$
- $k_{31} = k_{55} \oplus k_{63}$
- $k_{32} = k_{48} \oplus S[k_{61} \oplus k_{57}] \oplus R^3$
- $k_{33} = k_{49} \oplus S[k_{62} \oplus k_{58}]$
- $k_{34} = k_{50} \oplus S[k_{63} \oplus k_{59}]$
- $k_{35} = k_{51} \oplus S[k_{60} \oplus k_{56}]$
- $k_{36} = k_{48} \oplus k_{52}$
- $k_{37} = k_{49} \oplus k_{53}$
- $k_{38} = k_{50} \oplus k_{54}$
- $k_{39} = k_{51} \oplus k_{55}$
- $k_{40} = k_{52} \oplus k_{56}$
- $k_{41} = k_{53} \oplus k_{57}$
- $k_{42} = k_{54} \oplus k_{58}$
- $k_{43} = k_{55} \oplus k_{59}$
- $k_{44} = k_{56} \oplus k_{60}$
- $k_{45} = k_{57} \oplus k_{61}$
- $k_{46} = k_{58} \oplus k_{62}$
- $k_{47} = k_{59} \oplus k_{63}$
- $k_{64} = k_{48} \oplus S[k_{61}] \oplus R^4$
- $k_{65} = k_{49} \oplus S[k_{62}]$
- $k_{66} = k_{50} \oplus S[k_{63}]$
- $k_{67} = k_{51} \oplus S[k_{60}]$
- $k_{68} = k_{48} \oplus k_{52} \oplus S[k_{61}] \oplus R^4$
- $k_{69} = k_{49} \oplus k_{53} \oplus S[k_{62}]$
- $k_{70} = k_{50} \oplus k_{54} \oplus S[k_{63}]$
- $k_{71} = k_{51} \oplus k_{55} \oplus S[k_{60}]$
- $k_{72} = k_{48} \oplus k_{52} \oplus k_{56} \oplus S[k_{61}] \oplus R^4$
- $k_{73} = k_{49} \oplus k_{53} \oplus k_{57} \oplus S[k_{62}]$
- $k_{74} = k_{50} \oplus k_{54} \oplus k_{58} \oplus S[k_{63}]$
- $k_{75} = k_{51} \oplus k_{55} \oplus k_{59} \oplus S[k_{60}]$
- $k_{76} = k_{48} \oplus k_{52} \oplus k_{56} \oplus k_{60} \oplus S[k_{61}] \oplus R^4$
- $k_{77} = k_{49} \oplus k_{53} \oplus k_{57} \oplus k_{61} \oplus S[k_{62}]$
- $k_{78} = k_{50} \oplus k_{54} \oplus k_{58} \oplus k_{62} \oplus S[k_{63}]$
- $k_{79} = k_{51} \oplus k_{55} \oplus k_{59} \oplus k_{63} \oplus S[k_{60}]$
- $k_{80} = k_{48} \oplus S[k_{61}] \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus R^4 \oplus R^5$
- $k_{81} = k_{49} \oplus S[k_{62}] \oplus S[k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}]]$
- $k_{82} = k_{50} \oplus S[k_{63}] \oplus S[k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}]]$
- $k_{83} = k_{51} \oplus S[k_{60}] \oplus S[k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4]$
- $k_{84} = k_{52} \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus R^5$
- $k_{85} = k_{53} \oplus S[k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}]]$
- $k_{86} = k_{54} \oplus S[k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}]]$
- $k_{87} = k_{55} \oplus S[k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4]$
- $k_{88} = k_{48} \oplus k_{56} \oplus S[k_{61}] \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus R^4 \oplus R^5$
- $k_{89} = k_{49} \oplus k_{57} \oplus S[k_{62}] \oplus S[k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}]]$
- $k_{90} = k_{50} \oplus k_{58} \oplus S[k_{63}] \oplus S[k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}]]$
- $k_{91} = k_{51} \oplus k_{59} \oplus S[k_{60}] \oplus S[k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4]$
- $k_{92} = k_{52} \oplus k_{60} \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus R^5$
- $k_{93} = k_{53} \oplus k_{61} \oplus S[k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}]]$
- $k_{94} = k_{54} \oplus k_{62} \oplus S[k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}]]$
- $k_{95} = k_{55} \oplus k_{63} \oplus S[k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4]$
- $k_{96} = k_{48} \oplus S[k_{61}] \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus S[k_{61} \oplus k_{53} \oplus S[k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}]]] \oplus R^4 \oplus R^5 \oplus R^6$
- $k_{97} = k_{49} \oplus S[k_{62}] \oplus S[k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}]] \oplus S[k_{62} \oplus k_{54} \oplus S[k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}]]]$
- $k_{98} = k_{50} \oplus S[k_{63}] \oplus S[k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}]] \oplus S[k_{63} \oplus k_{55} \oplus S[k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4]]$
- $k_{99} = k_{51} \oplus S[k_{60}] \oplus S[k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4] \oplus S[k_{60} \oplus k_{52} \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus R^5]$
- $k_{100} = k_{48} \oplus k_{52} \oplus S[k_{61}] \oplus S[k_{61} \oplus k_{53} \oplus S[k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}]]] \oplus R^4 \oplus R^6$
- $k_{101} = k_{49} \oplus k_{53} \oplus S[k_{62}] \oplus S[k_{62} \oplus k_{54} \oplus S[k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}]]]$
- $k_{102} = k_{50} \oplus k_{54} \oplus S[k_{63}] \oplus S[k_{63} \oplus k_{55} \oplus S[k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4]]$
- $k_{103} = k_{51} \oplus k_{55} \oplus S[k_{60}] \oplus S[k_{60} \oplus k_{52} \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus R^5]$
- $k_{104} = k_{52} \oplus k_{56} \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus S[k_{61} \oplus k_{53} \oplus S[k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}]]] \oplus R^5 \oplus R^6$

- $k_{105} = k_{53} \oplus k_{57} \oplus S[k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}]] \oplus S[k_{62} \oplus k_{54} \oplus S[k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}]]]$
- $k_{106} = k_{54} \oplus k_{58} \oplus S[k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}]] \oplus S[k_{63} \oplus k_{55} \oplus S[k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4]]$
- $k_{107} = k_{55} \oplus k_{59} \oplus S[k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4] \oplus S[k_{60} \oplus k_{52} \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus R^5]$
- $k_{108} = k_{56} \oplus k_{60} \oplus S[k_{61} \oplus k_{53} \oplus S[k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}]]] \oplus R^6$
- $k_{109} = k_{57} \oplus k_{61} \oplus S[k_{62} \oplus k_{54} \oplus S[k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}]]]$
- $k_{110} = k_{58} \oplus k_{62} \oplus S[k_{63} \oplus k_{55} \oplus S[k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4]]$
- $k_{111} = k_{59} \oplus k_{63} \oplus S[k_{60} \oplus k_{52} \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus R^5]$
- $k_{112} = k_{48} \oplus S[k_{61}] \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus S[k_{61} \oplus k_{53} \oplus S[k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}]]] \oplus S[k_{61} \oplus k_{57} \oplus S[k_{62} \oplus k_{54} \oplus S[k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}]]]] \oplus R^4 \oplus R^5 \oplus R^6 \oplus R^7$
- $k_{113} = k_{49} \oplus S[k_{62}] \oplus S[k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}]] \oplus S[k_{62} \oplus k_{54} \oplus S[k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}]]] \oplus S[k_{62} \oplus k_{58} \oplus S[k_{63} \oplus k_{55} \oplus S[k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4]]]$
- $k_{114} = k_{50} \oplus S[k_{63}] \oplus S[k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}]] \oplus S[k_{63} \oplus k_{55} \oplus S[k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4]] \oplus S[k_{63} \oplus k_{59} \oplus S[k_{60} \oplus k_{52} \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus R^5]]$
- $k_{115} = k_{51} \oplus S[k_{60}] \oplus S[k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4] \oplus S[k_{60} \oplus k_{52} \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus R^5] \oplus S[k_{60} \oplus k_{56} \oplus S[k_{61} \oplus k_{53} \oplus S[k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}]]] \oplus R^6]$
- $k_{116} = k_{52} \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus S[k_{61} \oplus k_{57} \oplus S[k_{62} \oplus k_{54} \oplus S[k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}]]]] \oplus R^5 \oplus R^7$
- $k_{117} = k_{53} \oplus S[k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}]] \oplus S[k_{62} \oplus k_{58} \oplus S[k_{63} \oplus k_{55} \oplus S[k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4]]]$
- $k_{118} = k_{54} \oplus S[k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}]] \oplus S[k_{63} \oplus k_{59} \oplus S[k_{60} \oplus k_{52} \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus R^5]]$
- $k_{119} = k_{55} \oplus S[k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4] \oplus S[k_{60} \oplus k_{56} \oplus S[k_{61} \oplus k_{53} \oplus S[k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}]]] \oplus R^6]$
- $k_{120} = k_{56} \oplus S[k_{61} \oplus k_{53} \oplus S[k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}]]] \oplus S[k_{61} \oplus k_{57} \oplus S[k_{62} \oplus k_{54} \oplus S[k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}]]]] \oplus R^6 \oplus R^7$
- $k_{121} = k_{57} \oplus S[k_{62} \oplus k_{54} \oplus S[k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}]]] \oplus S[k_{62} \oplus k_{58} \oplus S[k_{63} \oplus k_{55} \oplus S[k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4]]]$
- $k_{122} = k_{58} \oplus S[k_{63} \oplus k_{55} \oplus S[k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4]] \oplus S[k_{63} \oplus k_{59} \oplus S[k_{60} \oplus k_{52} \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus R^5]]$
- $k_{123} = k_{59} \oplus S[k_{60} \oplus k_{52} \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus R^5] \oplus S[k_{60} \oplus k_{56} \oplus S[k_{61} \oplus k_{53} \oplus S[k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}]]] \oplus R^6]$
- $k_{124} = k_{60} \oplus S[k_{61} \oplus k_{57} \oplus S[k_{62} \oplus k_{54} \oplus S[k_{63} \oplus k_{59} \oplus k_{55} \oplus k_{51} \oplus S[k_{60}]]]] \oplus R^7$
- $k_{125} = k_{61} \oplus S[k_{62} \oplus k_{58} \oplus S[k_{63} \oplus k_{55} \oplus S[k_{60} \oplus k_{56} \oplus k_{52} \oplus k_{48} \oplus S[k_{61}] \oplus R^4]]]$
- $k_{126} = k_{62} \oplus S[k_{63} \oplus k_{59} \oplus S[k_{60} \oplus k_{52} \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus R^5]]$
- $k_{127} = k_{63} \oplus S[k_{60} \oplus k_{56} \oplus S[k_{61} \oplus k_{53} \oplus S[k_{62} \oplus k_{58} \oplus k_{54} \oplus k_{50} \oplus S[k_{63}]]] \oplus R^6]$

A.4 Temporary Variables

Temporary variables from Section 4.3 are defined here. Note that multiplication is performed in the AES $GF(2^8)$ field and the coefficients are in hexadecimal format.

- $v_0 = \Theta(c_{16}, 47x_2 \oplus \texttt{CB}x_4 \oplus 47k_{52} \oplus k_{53} \oplus \texttt{CB}k_{54} \oplus 44S[c_{12}] \oplus \texttt{C9}S[c_{15}], c_{19}, \texttt{CB}x_8 \oplus 47x_{10} \oplus \texttt{CB}k_{60} \oplus 47k_{62} \oplus k_{63} \oplus \texttt{C9}S[c_{14}] \oplus 44S[c_{13}]) \oplus k_{48} \oplus S[k_{61}] \oplus R^4$
- $v_1 = 44S[x_2] \oplus \texttt{C9}S[x_{10}] \oplus 47k_{48} \oplus k_{49} \oplus \texttt{CB}k_{50} \oplus 47k_{52} \oplus k_{53} \oplus \texttt{CB}k_{54} \oplus 47S[k_{61}] \oplus S[k_{62}] \oplus \texttt{CB}S[k_{63}] \oplus 47R^4 \oplus 47c_{20} \oplus \texttt{CB}c_{21}$
- $v_2 = \Theta(c_{17}, \texttt{CB}x_2 \oplus 47x_4 \oplus \texttt{CB}k_{52} \oplus 47k_{54} \oplus k_{55} \oplus \texttt{C9}S[c_{12}] \oplus 44S[c_{15}], c_{18}, 47x_8 \oplus \texttt{CB}x_{10} \oplus 47k_{60} \oplus k_{61} \oplus \texttt{CB}k_{62} \oplus 44S[c_{14}] \oplus \texttt{C9}S[c_{13}]) \oplus k_{50} \oplus k_{54} \oplus k_{58} \oplus S[k_{63}]$
- $v_3 = \texttt{C9}S[x_8] \oplus 44S[x_4] \oplus \texttt{CB}k_{48} \oplus 47k_{50} \oplus k_{51} \oplus \texttt{CB}k_{52} \oplus 47k_{54} \oplus k_{55} \oplus \texttt{CB}k_{56} \oplus 47k_{58} \oplus \texttt{CB}k_{60} \oplus S[k_{60}] \oplus \texttt{CB}S[k_{61}] \oplus 47k_{62} \oplus k_{63} \oplus 47S[k_{63}] \oplus \texttt{CB}R^4 \oplus \texttt{CB}c_{22} \oplus 47c_{23}$
- $w_0 = \Theta(c_{18}, 47x_8 \oplus \texttt{CB}x_{10} \oplus 47k_{60} \oplus k_{61} \oplus \texttt{CB}k_{62} \oplus 44S[c_{14}] \oplus \texttt{C9}S[c_{13}], S[c_{17}], \texttt{CB}x_2 \oplus 47x_4 \oplus \texttt{CB}k_{52} \oplus 47k_{54} \oplus k_{55} \oplus \texttt{C9}S[c_{12}] \oplus 44S[c_{15}]) \oplus k_{48} \oplus k_{52} \oplus k_{56} \oplus S[k_{61}] \oplus R^4$
- $w_1 = 44S[x_8] \oplus \texttt{C9}S[x_4] \oplus 47k_{48} \oplus k_{49} \oplus \texttt{CB}k_{50} \oplus 47k_{52} \oplus k_{53} \oplus \texttt{CB}k_{54} \oplus 47k_{56} \oplus k_{57} \oplus \texttt{CB}k_{58} \oplus 47k_{60} \oplus k_{61} \oplus 47S[k_{61}] \oplus \texttt{CB}k_{62} \oplus S[k_{62}] \oplus \texttt{CB}S[k_{63}] \oplus 47R^4 \oplus 47c_{22} \oplus \texttt{CB}c_{23}$
- $w_2 = \Theta(c_{19}, \texttt{CB}x_8 \oplus 47x_{10} \oplus \texttt{CB}k_{60} \oplus 47k_{62} \oplus k_{63} \oplus \texttt{C9}S[c_{14}] \oplus 44S[c_{13}], c_{16}, 47x_2 \oplus \texttt{CB}x_4 \oplus 47k_{52} \oplus k_{53} \oplus \texttt{CB}k_{54} \oplus 44S[c_{12}] \oplus \texttt{C9}S[c_{15}]) \oplus k_{50} \oplus S[k_{63}]$
- $w_3 = \texttt{C9}S[x_2] \oplus 44S[x_{10}] \oplus \texttt{CB}k_{48} \oplus 47k_{50} \oplus \texttt{CB}k_{52} \oplus 47k_{54} \oplus k_{55} \oplus S[k_{60}] \oplus \texttt{CB}S[k_{61}] \oplus 47S[k_{63}] \oplus \texttt{CB}R^4 \oplus \texttt{CB}c_{20} \oplus 47c_{21}$
- $y_0 = 7S[2S[c_{16}] \oplus 3S[47x_2 \oplus \texttt{CB}x_4 \oplus 47k_{52} \oplus k_{53} \oplus \texttt{CB}k_{54} \oplus 44S[c_{12}] \oplus \texttt{C9}S[c_{15}]] \oplus S[c_{19}] \oplus S[\texttt{CB}x_8 \oplus 47x_{10} \oplus \texttt{CB}k_{60} \oplus 47k_{62} \oplus k_{63} \oplus \texttt{C9}S[c_{14}] \oplus 44S[c_{13}]] \oplus k_{48} \oplus S[k_{61}] \oplus R^4]$
- $y_1 = 4S[44S[x_2] \oplus \texttt{C9}S[x_{10}] \oplus 47k_{48} \oplus k_{49} \oplus \texttt{CB}k_{50} \oplus 47k_{52} \oplus k_{53} \oplus \texttt{CB}k_{54} \oplus 47S[k_{61}] \oplus S[k_{62}] \oplus \texttt{CB}S[k_{63}] \oplus 47R^4 \oplus 47c_{20} \oplus \texttt{CB}c_{21}]$
- $y_2 = S[S[c_{18}] \oplus S[47x_8 \oplus \texttt{CB}x_{10} \oplus 47k_{60} \oplus k_{61} \oplus \texttt{CB}k_{62} \oplus 44S[c_{14}] \oplus \texttt{C9}S[c_{13}]] \oplus 2S[c_{17}] \oplus 3S[\texttt{CB}x_2 \oplus 47x_4 \oplus \texttt{CB}k_{52} \oplus 47k_{54} \oplus k_{55} \oplus \texttt{C9}S[c_{12}] \oplus 44S[c_{15}]] \oplus k_{50} \oplus k_{54} \oplus k_{58} \oplus S[k_{63}]]$
- $y_3 = 44S[x_4] \oplus \texttt{C9}S[x_8] \oplus \texttt{CB}k_{48} \oplus 47k_{50} \oplus \texttt{CB}k_{52} \oplus 47k_{54} \oplus 47k_{58} \oplus \texttt{CB}k_{60} \oplus \texttt{CB}S[k_{61}] \oplus k_{63} \oplus 47S[k_{63}] \oplus \texttt{CB}R^4 \oplus 47k_{62} \oplus k_{63} \oplus \texttt{CB}c_{22} \oplus 47c_{23} \oplus S^{-1}[2S[2S[c_{16}] \oplus 3S[47x_2 \oplus \texttt{CB}x_4 \oplus 47k_{52} \oplus k_{53} \oplus \texttt{CB}k_{54} \oplus 44S[c_{12}] \oplus \texttt{C9}S[c_{15}]] \oplus S[c_{19}] \oplus S[\texttt{CB}x_8 \oplus 47x_{10} \oplus \texttt{CB}k_{60} \oplus 47k_{62} \oplus k_{63} \oplus \texttt{C9}S[c_{14}] \oplus 44S[c_{13}]] \oplus k_{48} \oplus S[k_{61}] \oplus R^4] \oplus 3S[44S[x_2] \oplus \texttt{C9}S[x_{10}] \oplus 47k_{48} \oplus k_{49} \oplus \texttt{CB}k_{50} \oplus 47k_{52} \oplus k_{53} \oplus \texttt{CB}k_{54} \oplus 47S[k_{61}] \oplus S[k_{62}] \oplus \texttt{CB}S[k_{63}] \oplus 47R^4 \oplus 47c_{20} \oplus \texttt{CB}c_{21}] \oplus S[S[c_{18}] \oplus S[47x_8 \oplus \texttt{CB}x_{10} \oplus 47k_{60} \oplus k_{61} \oplus$

$\mathtt{CB}k_{62} \oplus \mathtt{44}S[c_{14}] \oplus \mathtt{C9}S[c_{13}]] \oplus \mathtt{2}S[c_{17}] \oplus \mathtt{3}S[\mathtt{CB}x_2 \oplus \mathtt{47}x_4 \oplus \mathtt{CB}k_{52} \oplus \mathtt{47}k_{54} \oplus k_{55} \oplus \mathtt{C9}S[c_{12}] \oplus \mathtt{44}S[c_{15}]] \oplus k_{50} \oplus k_{54} \oplus k_{58} \oplus S[k_{63}]] \oplus k_{48} \oplus S[k_{61}] \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus R^4 \oplus R^5 \oplus c_{24}]$

The temporary key variables are:

- $K_0^* = k_{48} \oplus S[k_{61}] \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus R^4 \oplus R^5$
- $K_1^* = k_{48} \oplus k_{56} \oplus S[k_{61}] \oplus S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus R^4 \oplus R^5$
- $K_2^* = \mathtt{3}k_{48} \oplus k_{50} \oplus \mathtt{3}S[k_{61}] \oplus S[k_{63}] \oplus \mathtt{3}S[k_{61} \oplus k_{57} \oplus k_{53} \oplus k_{49} \oplus S[k_{62}]] \oplus \mathtt{3}R^4 \oplus \mathtt{3}R^5 \oplus \mathtt{3}c_{24}$

A.5 Final Equation System

The final system of 21 equations in 17 variables are given here. The expressions W_j, Y_j, Z_j and T_j contain subkey and/or key variables which are defined later. Note that Θ is defined in Section 4.1 and $\hat{\Pi}(z_0, z_1, z_2, z_3) = \mathtt{E}S^{-1}[z_0] \oplus \mathtt{B}S^{-1}[z_1] \oplus \mathtt{D}S^{-1}[z_2] \oplus \mathtt{9}S^{-1}[z_3]$. Note that multiplication is performed in the AES $GF(2^8)$ field and the coefficients are in hexadecimal format.

1. Based on Equation (25):

$$\begin{aligned}\Theta(\Theta(\ & c_{24}, \Theta(Y_0, c_{23}, Y_1, c_{20}) \oplus T_0,\\ & c_{27}, \Theta(Y_3, c_{22}, Y_2, c_{21}) \oplus T_1) \oplus T_2,\\ \Theta(\ & \Theta(W_2, W_0, W_1, 0) \oplus T_4,\\ & \Theta(c_{21}, Y_3, c_{22}, Y_2) \oplus T_5,\\ & \mathtt{7}S[W_4] \oplus \mathtt{7}S[W_5] \oplus \mathtt{3}S[W_6] \oplus T_6 \oplus T_{61},\\ & \Theta(c_{20}, Y_0, c_{23}, Y_1) \oplus T_3) \oplus T_7,\\ \Theta(\ & c_{25}, \Theta(Y_1, c_{20}, Y_0, c_{23}) \oplus T_9,\\ & c_{26}, \Theta(Y_2, c_{21}, Y_3, c_{22}) \oplus T_8) \oplus T_{10}\\ \Theta(\ & \mathtt{7}S[W_0] \oplus \mathtt{7}S[W_1] \oplus \mathtt{3}S[W_2] \oplus T_{14} \oplus T_{62},\\ & \Theta(c_{22}, Y_2, c_{21}, Y_3) \oplus T_{11},\\ & \mathtt{3}S[W_4] \oplus S[W_5] \oplus \mathtt{2}S[W_6] \oplus T_{12},\\ & \Theta(c_{23}, Y_1, c_{20}, Y_0) \oplus T_{13}) \oplus T_{15})\\ & \oplus T_{16} \oplus c_{32} = 0\end{aligned}$$

2. Based on Equation (26):

$$\begin{aligned}\Theta(\Theta(\ & c_{25}, \Theta(Y_1, c_{20}, Y_0, c_{23}) \oplus T_9,\\ & c_{26}, \Theta(Y_2, c_{21}, Y_3, c_{22}) \oplus T_8) \oplus T_{10},\\ \Theta(\ & \mathtt{7}S[W_0] \oplus \mathtt{7}S[W_1] \oplus \mathtt{3}S[W_2] \oplus T_{14} \oplus T_{62},\\ & \Theta(c_{22}, Y_2, c_{21}, Y_3) \oplus T_{11},\\ & \Theta(W_6, W_4, W_5, 0) \oplus T_{12},\\ & \Theta(c_{23}, Y_1, c_{20}, Y_0) \oplus T_{13}) \oplus T_{15},\\ \Theta(\ & c_{24}, \Theta(Y_0, c_{23}, Y_1, c_{20}) \oplus T_0,\\ & c_{27}, \Theta(Y_3, c_{22}, Y_2, c_{21}) \oplus T_1) \oplus T_2\\ \Theta(\ & \Theta(W_2, W_0, W_1, 0) \oplus T_4,\\ & \Theta(c_{21}, Y_3, c_{22}, Y_2) \oplus T_5,\\ & \mathtt{7}S[W_4] \oplus \mathtt{7}S[W_5] \oplus \mathtt{3}S[W_6] \oplus T_6 \oplus T_{61},\\ & \Theta(c_{20}, Y_0, c_{23}, Y_1) \oplus T_3) \oplus T_7)\\ & \oplus T_{17} \oplus c_{33} = 0\end{aligned}$$

3. Based on Equation (27):

$$\begin{aligned}\Theta(\Theta(\ & c_{26}, \Theta(Y_2, c_{21}, Y_3, c_{22}) \oplus T_8,\\ & c_{25}, \Theta(Y_1, c_{20}, Y_0, c_{23}) \oplus T_9) \oplus T_{18},\\ \Theta(\ & \Theta(W_6, W_4, W_5, 0) \oplus T_{12},\\ & \Theta(c_{23}, Y_1, c_{20}, Y_0) \oplus T_{13},\\ & \Theta(c_{22}, Y_2, c_{21}, Y_3) \oplus T_{14} \oplus T_{62},\\ & \mathtt{7}S[W_0] \oplus \mathtt{7}S[W_1] \oplus \mathtt{3}S[W_2] \oplus T_{11}) \oplus T_{19},\\ \Theta(\ & c_{27}, \Theta(Y_3, c_{22}, Y_2, c_{21}) \oplus T_1,\\ & c_{24}, \Theta(Y_0, c_{23}, Y_1, c_{20}) \oplus T_0) \oplus T_{20}\\ \Theta(\ & \mathtt{7}S[W_4] \oplus \mathtt{7}S[W_5] \oplus \mathtt{3}S[W_6] \oplus T_6 \oplus T_{61},\\ & \Theta(c_{20}, Y_0, c_{23}, Y_1) \oplus T_3,\\ & \Theta(W_2, W_0, W_1, 0) \oplus T_4,\\ & \Theta(c_{21}, Y_3, c_{22}, Y_2) \oplus T_5) \oplus T_{21})\\ & \oplus T_{22} \oplus c_{34} = 0\end{aligned}$$

4. Based on Equation (28):

$$\begin{aligned}\Theta(\Theta(\ & c_{27}, \Theta(Y_3, c_{22}, Y_2, c_{21}) \oplus T_1,\\ & c_{24}, \Theta(Y_0, c_{23}, Y_1, c_{20}) \oplus T_0) \oplus T_{20},\\ \Theta(\ & \mathtt{7}S[W_4] \oplus \mathtt{7}S[W_5] \oplus \mathtt{3}S[W_6] \oplus T_6 \oplus T_{61},\\ & \Theta(c_{20}, Y_0, c_{23}, Y_1) \oplus T_3,\\ & \Theta(W_2, W_0, W_1, 0) \oplus T_4,\\ & \Theta(c_{21}, Y_3, c_{22}, Y_2) \oplus T_5,\\ \Theta(\ & c_{26}, \Theta(Y_2, c_{21}, Y_3, c_{22}) \oplus T_8,\\ & c_{25}, \Theta(Y_1, c_{20}, Y_0, c_{23}) \oplus T_9) \oplus T_{18}\\ \Theta(\ & \Theta(W_6, W_4, W_5, 0) \oplus T_{12},\\ & \Theta(c_{23}, Y_1, c_{20}, Y_0) \oplus T_{13},\\ & \mathtt{7}S[W_0] \oplus \mathtt{7}S[W_1] \oplus \mathtt{3}S[W_2] \oplus T_{14} \oplus T_{62},\\ & \Theta(c_{22}, Y_2, c_{21}, Y_3) \oplus T_{11}) \oplus T_{19})\\ & \oplus T_{23} \oplus c_{35} = 0\end{aligned}$$

5. Based on Equation (29):

$$\begin{aligned}\hat{\Pi}(\hat{\Pi}(\ & S[c_8], \hat{\Pi}(Y_6, S[c_{15}], Y_7, S[c_{14}]) \oplus T_{24},\\ & S[c_9], \hat{\Pi}(Y_5, S[c_{12}], Y_4, S[c_{13}]) \oplus T_{25}) \oplus T_{26},\\ \hat{\Pi}(\ & \hat{\Pi}(Z_{13}, Z_{14}, Z_{15}, Z_{12}) \oplus T_{28},\\ & \hat{\Pi}(S[c_{13}], Y_5, S[c_{12}], Y_4) \oplus T_{29},\\ & \hat{\Pi}(Z_{11}, Z_8, Z_9, Z_{10}) \oplus T_{30},\\ & \hat{\Pi}(S[c_{14}], Y_6, S[c_{15}], Y_7) \oplus T_{27}) \oplus T_{31},\\ \hat{\Pi}(\ & S[c_{11}], \hat{\Pi}(Y_7, S[c_{14}], Y_6, S[c_{15}]) \oplus T_{33},\\ & S[c_{10}], \hat{\Pi}(Y_4, S[c_{13}], Y_5, S[c_{12}]) \oplus T_{32}) \oplus T_{34}\\ \hat{\Pi}(\ & \hat{\Pi}(Z_{15}, Z_{12}, Z_{13}, Z_{14}) \oplus T_{38},\\ & \hat{\Pi}(S[c_{12}], Y_4, S[c_{13}], Y_5) \oplus T_{35},\\ & \hat{\Pi}(Z_9, Z_{10}, Z_{11}, Z_8) \oplus T_{36},\\ & \hat{\Pi}(S[c_{15}], Y_7, S[c_{14}], Y_6) \oplus T_{37}) \oplus T_{39})\\ & \oplus T_{40} \oplus S[c_0] = 0\end{aligned}$$

6. Based on Equation (30):

$$\begin{aligned}\hat{\Pi}(\hat{\Pi}(& S[c_9], \hat{\Pi}(Y_5, S[c_{12}], Y_4, S[c_{13}]) \oplus T_{25},\\ & S[c_8], \hat{\Pi}(Y_6, S[c_{15}], Y_7, S[c_{14}]) \oplus T_{24}) \oplus T_{43},\\ \hat{\Pi}(& \hat{\Pi}(Z_{11}, Z_8, Z_9, Z_{10}) \oplus T_{30},\\ & \hat{\Pi}(S[c_{14}], Y_6, S[c_{15}], Y_7) \oplus T_{27},\\ & \hat{\Pi}(Z_{13}, Z_{14}, Z_{15}, Z_{12}) \oplus T_{28},\\ & \hat{\Pi}(S[c_{13}], Y_5, S[c_{12}], Y_4) \oplus T_{29}) \oplus T_{44},\\ \hat{\Pi}(& S[c_{10}], \hat{\Pi}(Y_4, S[c_{13}], Y_5, S[c_{12}]) \oplus T_{32},\\ & S[c_{11}], \hat{\Pi}(Y_7, S[c_{14}], Y_6, S[c_{15}]) \oplus T_{33}) \oplus T_{41}\\ \hat{\Pi}(& \hat{\Pi}(Z_9, Z_{10}, Z_{11}, Z_8) \oplus T_{36},\\ & \hat{\Pi}(S[c_{15}], Y_7, S[c_{14}], Y_6) \oplus T_{37},\\ & \hat{\Pi}(Z_{15}, Z_{12}, Z_{13}, Z_{14}) \oplus T_{38},\\ & \hat{\Pi}(S[c_{12}], Y_4, S[c_{13}], Y_5) \oplus T_{35}) \oplus T_{42})\\ & \oplus T_{45} \oplus S[c_1] = 0\end{aligned}$$

7. Based on Equation (31):

$$\begin{aligned}\hat{\Pi}(\hat{\Pi}(& S[c_{10}], \hat{\Pi}(Y_4, S[c_{13}], Y_5, S[c_{12}]) \oplus T_{32},\\ & S[c_{11}], \hat{\Pi}(Y_7, S[c_{14}], Y_6, S[c_{15}]) \oplus T_{33}) \oplus T_{41},\\ \hat{\Pi}(& \hat{\Pi}(Z_9, Z_{10}, Z_{11}, Z_8) \oplus T_{36},\\ & \hat{\Pi}(S[c_{15}], Y_7, S[c_{14}], Y_6) \oplus T_{37},\\ & \hat{\Pi}(Z_{15}, Z_{12}, Z_{13}, Z_{14}) \oplus T_{38},\\ & \hat{\Pi}(S[c_{12}], Y_4, S[c_{13}], Y_5) \oplus T_{35},\\ \hat{\Pi}(& S[c_9], \hat{\Pi}(Y_5, S[c_{12}], Y_4, S[c_{13}]) \oplus T_{25},\\ & S[c_8], \hat{\Pi}(Y_6, S[c_{15}], Y_7, S[c_{14}]) \oplus T_{24}) \oplus T_{43}\\ \hat{\Pi}(& \hat{\Pi}(Z_{11}, Z_8, Z_9, Z_{10}) \oplus T_{30},\\ & \hat{\Pi}(S[c_{14}], Y_6, S[c_{15}], Y_7) \oplus T_{27},\\ & \hat{\Pi}(Z_{13}, Z_{14}, Z_{15}, Z_{12}) \oplus T_{28},\\ & \hat{\Pi}(S[c_{13}], Y_5, S[c_{12}], Y_4) \oplus T_{29}) \oplus T_{44})\\ & \oplus T_{46} \oplus S[c_2] = 0\end{aligned}$$

8. Based on Equation (32):

$$\begin{aligned}\hat{\Pi}(\hat{\Pi}(& S[c_{11}], \hat{\Pi}(Y_7, S[c_{14}], Y_6, S[c_{15}]) \oplus T_{33},\\ & S[c_{10}], \hat{\Pi}(Y_4, S[c_{13}], Y_5, S[c_{12}]) \oplus T_{32}) \oplus T_{34},\\ \hat{\Pi}(& \hat{\Pi}(Z_{15}, Z_{12}, Z_{13}, Z_{14}) \oplus T_{38},\\ & \hat{\Pi}(S[c_{12}], Y_4, S[c_{13}], Y_5) \oplus T_{35},\\ & \hat{\Pi}(Z_9, Z_{10}, Z_{11}, Z_8) \oplus T_{36},\\ & \hat{\Pi}(S[c_{15}], Y_7, S[c_{14}], Y_6) \oplus T_{37}) \oplus T_{39},\\ \hat{\Pi}(& S[c_8], \hat{\Pi}(Y_6, S[c_{15}], Y_7, S[c_{14}]) \oplus T_{24},\\ & S[c_9], \hat{\Pi}(Y_5, S[c_{12}], Y_4, S[c_{13}]) \oplus T_{25}) \oplus T_{26}\\ \hat{\Pi}(& \hat{\Pi}(Z_{13}, Z_{14}, Z_{15}, Z_{12}) \oplus T_{28},\\ & \hat{\Pi}(S[c_{13}], Y_5, S[c_{12}], Y_4) \oplus T_{29},\\ & \hat{\Pi}(Z_{11}, Z_8, Z_9, Z_{10}) \oplus T_{30},\\ & \hat{\Pi}(S[c_{14}], Y_6, S[c_{15}], Y_7) \oplus T_{27}) \oplus T_{31})\\ & \oplus T_{47} \oplus S[c_3] = 0\end{aligned}$$

9. Based on Equation (21):

$$\begin{aligned}&\Theta(\Theta(c_{20}, Y_0, c_{23}, Y_1) \oplus T_3, \Theta(W_2, W_0, W_1, 0) \oplus T_4,\\ &\quad \Theta(c_{21}, Y_3, c_{22}, Y_2) \oplus T_5,\\ &\quad 7S[W_4] \oplus 7S[W_5] \oplus 3S[W_6] \oplus T_6 \oplus T_{61})\\ &\quad \oplus T_{48} \oplus c_{28} = 0\end{aligned}$$

10. Based on Equation (22):

$$\begin{aligned}&\Theta(\Theta(c_{21}, Y_3, c_{22}, Y_2) \oplus T_5,\\ &\quad 7S[W_4] \oplus 7S[W_5] \oplus 3S[W_6] \oplus T_6 \oplus T_{61},\\ &\quad \Theta(c_{20}, Y_0, c_{23}, Y_1) \oplus T_3, \Theta(W_2, W_0, W_1, 0) \oplus T_4)\\ &\quad \oplus T_{49} \oplus c_{29} = 0\end{aligned}$$

11. Based on Equation (23):

$$\begin{aligned}&\Theta(\Theta(c_{22}, Y_2, c_{21}, Y_3) \oplus T_{11}, \Theta(W_6, W_4, W_5, 0) \oplus T_{12},\\ &\quad \Theta(c_{23}, Y_1, c_{20}, Y_0) \oplus T_{13},\\ &\quad 7S[W_0] \oplus 7S[W_1] \oplus 3S[W_2] \oplus T_{14} \oplus T_{62})\\ &\quad \oplus T_{50} \oplus c_{30} = 0\end{aligned}$$

12. Based on Equation (24):

$$\begin{aligned}&\Theta(\Theta(c_{23}, Y_1, c_{20}, Y_0) \oplus T_{13},\\ &\quad 7S[W_0] \oplus 7S[W_1] \oplus 3S[W_2] \oplus T_{14} \oplus T_{62},\\ &\quad \Theta(c_{22}, Y_2, c_{21}, Y_3) \oplus T_{11}, \Theta(W_6, W_4, W_5, 0) \oplus T_{12})\\ &\quad \oplus T_{51} \oplus c_{31} = 0\end{aligned}$$

13. Based on Equation (5):

$$\begin{aligned}&\hat{\Pi}(\hat{\Pi}(S[c_{12}], Y_4, S[c_{13}], Y_5) \oplus T_{35},\\ &\quad \hat{\Pi}(Z_9, Z_{10}, Z_{11}, Z_8) \oplus T_{36},\\ &\quad \hat{\Pi}(S[c_{15}], Y_7, S[c_{14}], Y_6) \oplus T_{37},\\ &\quad \hat{\Pi}(Z_{15}, Z_{12}, Z_{13}, Z_{14}) \oplus T_{38}) \oplus T_{52} \oplus S[c_{12}] = 0\end{aligned}$$

14. Based on Equation (6):

$$\begin{aligned}&\hat{\Pi}(\hat{\Pi}(S[c_{13}], Y_5, S[c_{12}], Y_4) \oplus T_{29},\\ &\quad \hat{\Pi}(Z_{11}, Z_8, Z_9, Z_{10}) \oplus T_{30},\\ &\quad \hat{\Pi}(S[c_{14}], Y_6, S[c_{15}], Y_7) \oplus T_{27},\\ &\quad \hat{\Pi}(Z_{13}, Z_{14}, Z_{15}, Z_{12}) \oplus T_{28}) \oplus T_{53} \oplus S[c_{13}] = 0\end{aligned}$$

15. Based on Equation (7):

$$\begin{aligned}&\hat{\Pi}(\hat{\Pi}(S[c_{14}], Y_6, S[c_{15}], Y_7) \oplus T_{27},\\ &\quad \hat{\Pi}(Z_{13}, Z_{14}, Z_{15}, Z_{12}) \oplus T_{28},\\ &\quad \hat{\Pi}(S[c_{13}], Y_5, S[c_{12}], Y_4) \oplus T_{29},\\ &\quad \hat{\Pi}(Z_{11}, Z_8, Z_9, Z_{10}) \oplus T_{30}) \oplus T_{54} \oplus S[c_{14}] = 0\end{aligned}$$

16. Based on Equation (8):

$$\begin{aligned}&\hat{\Pi}(\hat{\Pi}(S[c_{15}], Y_7, S[c_{14}], Y_6) \oplus T_{37},\\ &\quad \hat{\Pi}(Z_{15}, Z_{12}, Z_{13}, Z_{14}) \oplus T_{38},\\ &\quad \hat{\Pi}(S[c_{12}], Y_4, S[c_{13}], Y_5) \oplus T_{35},\\ &\quad \hat{\Pi}(Z_9, Z_{10}, Z_{11}, Z_8) \oplus T_{36}) \oplus T_{55} \oplus S[c_{15}] = 0\end{aligned}$$

17. Based on Equation (20):

$$7S[W_0] \oplus 4S[W_1] \oplus S[W_2] \oplus T_{56} \oplus c_{27} = 0$$

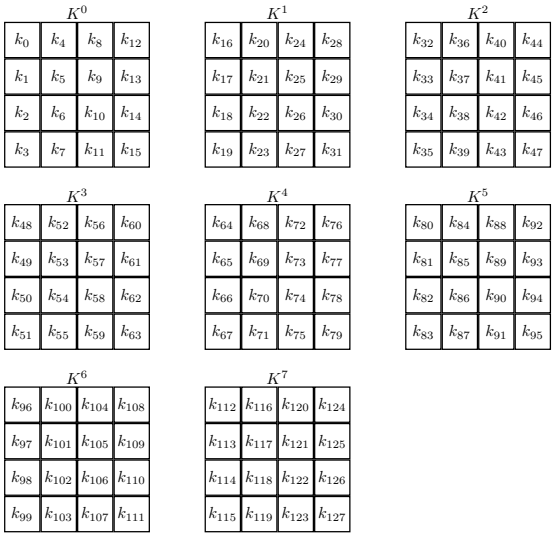

Figure 6: Key variables in Figure 3.

18. Based on Equation (37):

$$\hat{\Pi}(Z_8, Z_9, Z_{10}, Z_{11}) \oplus T_{57} \oplus S[c_8] = 0$$

19. Based on Equation (38):

$$\hat{\Pi}(Z_{14}, Z_{15}, Z_{12}, Z_{13}) \oplus T_{58} \oplus S[c_9] = 0$$

20. Based on Equation (39):

$$\hat{\Pi}(Z_{12}, Z_{13}, Z_{14}, Z_{15}) \oplus T_{59} \oplus S[c_{10}] = 0$$

21. Based on Equation (40):

$$\hat{\Pi}(Z_{10}, Z_{11}, Z_8, Z_9) \oplus T_{60} \oplus S[c_{11}] = 0$$

The W_j, Y_j, Z_j and T_j expressions in the above equations are composed of the sum of the remaining state, key variables and constants.

B Step-by-Step Procedure to Produce Equations for Substitution

The following details the step-by-step procedure to produce Equations (9) to (16). These equations are used in the initial substitution process to eliminate 8 state variables.

1. Describe x_6 in Eq. (1) in terms of x_1, x_2, x_{10}.
2. Describe x_1 in Eq. (2) in terms of x_2, x_6, x_{10}.
3. Substitute x_6 in Step 2 with x_6 in Step 1. Now x_1 is described only in terms of x_2, x_{10} (Refer to Eq. (9)).
4. Substitute x_1 in Step 1 with x_1 in the previous step. Now x_6 is described only in terms of x_2, x_{10} (Refer to Eq. (10)).
5. Describe x_0 in Eq. (3) in terms of x_4, x_7, x_8.
6. Describe x_7 in Eq. (4) in terms of x_0, x_4, x_8.
7. Substitute x_0 in Step 6 with x_0 in Step 5. Now x_7 is described only in terms of x_4, x_8 (Refer to Eq. (12)).
8. Substitute x_7 in Step 5 with x_7 the previous step. Now x_0 is described only in terms of x_4, x_8 (Refer to Eq. (11)).
9. Describe x_3 in Eq. (5) in terms of x_2, x_4, x_5.
10. Describe x_{11} in Eq. (6) in terms of x_8, x_9, x_{10}.
11. Describe x_9 in Eq. (7) in terms of x_8, x_{10}, x_{11}.
12. Describe x_5 in Eq. (8) in terms of x_2, x_3, x_4.
13. Substitute x_5 in Step 9 with x_5 in Step 12. Now x_3 is described only in terms of x_2, x_4 (Refer to Eq. (13).
14. Substitute x_9 in Step 10 with x_9 in Step 11. Now x_{11} is described only in terms of x_8, x_{10} (Refer to Eq. (14).
15. Substitute x_{11} in Step 11 with x_{11} in Step 14. Now x_9 is described only in terms of x_8, x_{10} (Refer to Eq. (15).
16. Substitute x_3 in Step 12 with x_3 in Step 13. Now x_5 is described only in terms of x_2, x_4 (Refer to Eq. (16).