Published in IET Information Security
Received on 6th March 2009
doi: 10.1049/iet-ifs.2009.0118

ISSN 1751-8709

# Algebraic cryptanalysis of a small-scale version of stream cipher Lex

V. Velichkov[1,2] V. Rijmen[1,2,3] B. Preneel[1,2]

[1]Department of Electrical Engineering ESAT/SCD-COSIC, Katholieke Universiteit Leuven, Kasteelpark Arenberg 10, B-3001 Heverlee, Belgium
[2]Interdisciplinary Institute for BroadBand Technology (IBBT), Gent-Ledeberg, B-9050, Belgium
[3]Institute for Applied Information Processing and Communications, Graz University of Technology, A-8010 Graz, Austria
E-mail: vesselin.velichkov@esat.kuleuven.be

**Abstract:** In this study, the authors analyse with respect to algebraic attacks a small-scale version of the stream cipher Lex. They base it on a small-scale version of the block cipher advanced encryption standard (AES) with 16-bit state and 16-bit key. They represent the small-scale Lex and its key schedule in two alternative ways: as a system of cubic boolean equations and as a system of quadratic boolean equations. The authors use Gröbner bases to solve the two systems for different number of rounds and sizes of the leak. They obtain the best results for the quadratic representation of the cipher. For this case they are able to recover the secret key in time less than 2 min by solving a system of 374 quadratic boolean equations in 208 unknowns resulting from 5 rounds of the cipher.

## 1 Introduction

Lex is a 128-bit key stream cipher proposed by Alex Biryukov in [1–3]. Lex was selected for phase 3 of the eSTREAM competition. It was not chosen for the eSTREAM portfolio. Lex is based on the notion of 'leak extraction', which is first defined in [1].

The motivation for the current work is the following citation from the design of Lex [3, Section 3.3]: 'Applicability of these [algebraic attacks] to Lex is to be carefully investigated. If one could write a non-linear equation in terms of the outputs and the key – that could lead to an attack.'

There are four cryptanalytic results on Lex published so far [4–7]. Of them only [7] exploits the algebraic structure of the cipher. With the presented work we complement the results of [7].

The paper is organised as follows. In Section 2, we give an overview of the existing attacks on Lex. In Section 3, we give a short description of stream cipher Lex. In Section 4, we propose Lex(2,2,4) – a small-scale version of Lex. In Section 5, we represent Lex(2,2,4) and its key schedule as a system of cubic and quadratic boolean equations. In Section 6, we describe a modification of the Gröbner bases attack algorithm presented in [8], which we apply for a key recovery attack on Lex(2,2,4). In Section 7, we give information on the experimental setting in which we perform our experiments. In Section 8, we describe our results and in Section 10 we conclude. In the Appendix, we provide the explicit equations for one round of Lex(2,2,4) and two round keys.

## 2 Previous work

Wu and Preneel [4] presented a slide attack on the original version of Lex [1]. The attack exploits the initialisation phase of the cipher. It requires 500 × 320 bits of key stream, each generated from $2^{60.8}$ different IVs under the same key. As a result of finding three collisions in the output key stream, 96 bits of the key can be recovered. The remaining 32 bits of the key are recovered by exhaustive search. Subsequently, Lex was tweaked [2] to resist the attack by using a full AES encryption during initialisation (instead of the modified version of AES used before). No change was made to the stream generation.

Johansson *et al.* [5] present an attack on Lex in which it is possible to decrypt some ciphertext without recovering the key. The attack requires $2^{65.66}$ key stream bits produced by one IV and the first approx. 320 bits from $2^{65.66}$ other IVs. This attack is not applicable to the tweaked version of Lex [3], where the maximum number of IVs used under the same key is required to be $2^{32}$.

The most recent successful attack on Lex is the one proposed by Dunkelman and Keller [6]. The attack identifies special states in two AES encryptions, which satisfy a certain difference pattern. The secret key is retrieved in time of $2^{112}$ operations using $2^{36.3}$ bytes of key stream produced by the same key. The attack is applicable also to the tweaked version of Lex.

The only result so far that explores the algebraic structure of Lex is [7]. This result also bears most relevence to the presented work. In [7], a system of 21 equations in 17 variables is constructed based on the byte leakage of eight rounds of the full-scale Lex. A middle state of Lex is selected from which 12 state variables are chosen. By running the cipher from the middle state for four rounds forward and for four rounds backward 32 equations in the 12 state variables and 108 key variables are obtained. By writing equations for the key schedule all key variables are expressed in terms of the 16 variables of the initial key. Thus the total number of key variables is lowered to 16. By using dependence relations between variables and equations the final system of 21 equations in 17 variables is constructed. In order to solve the system, $2^{17}$ bytes have to be guessed. This being one byte more than exhaustive key search of $2^{16}$ causes the attack to fail.

The motivation for the current work is very similar to [7] namely: exploit the algebraic structure of Lex in order to recover the key. However the approach which we take differs from [7] in several significant ways:

- While [7] work at byte level we base our algebraic representation of Lex on bit level. This allows us to exploit algebraic relations not only between bytes but also between bits.

- [7] do not explore the algebraic structure of the AES Sbox. As it is the main source of non-linearity the Sbox is a very important component of Lex. Being defined as the modular inverse in $GF(2^8)$ the AES Sbox is a source of rich algebraic structure. In our approach we extensively explore this structure by representing the Sbox as systems of cubic and quadratic equations over $GF(2)$ (also see next).

- [7] admit that 'if we have an equation $x \oplus Sbox(x) \oplus \ldots = 0$ where $x$ is a variable, it is not possible to isolate $x$'. In our approach, $Sbox\ (x)$ is an algebraic expression and so the mentioned problem is naturally solved.

- Another significant difference between [7] and the presented work is the method that is used for solving the system of equations which describe Lex. The method used in [7] is guessing variables and discarding those guesses for which the equations are not consistent. In our approach we use Gröbner bases [19] to compute the solutions to our system. Gröbner bases are a standard way to approach the problem of solving systems of non-linear equations. We believe that the use of Gröbner bases allows us to explore more fully the algebraic structure of the cipher. Furthermore the Gröbner bases technique can be seen as a one level more complex approach over guessing variables.

For the reasons stated above we believe that the presented work can be seen as complementary to [7]. We believe that the two results together provide a rich picture of the algebraic structure of Lex and can facilitate further investigations in the algebaric cryptanalysis of the cipher.

## 3 Lex

In this section, we give a short overview of stream cipher Lex. From now on whenever we refer to Lex we shall mean its 128-bit version – Lex-128.

Lex has 128-bit key and 128-bit IV. During initialisation the key of Lex is expanded into 11 round keys by a standard AES key schedule. Next, the IV is encrypted with AES-128 [17, 18], the first round key is *exor*-ed with the output and the result becomes the input to the first round of Lex. The input to every round of Lex is transformed to the output by the AES round transformation circularly using the first 10 of the 11 round keys. After every round, four bytes of the output (the 'leaks') are extracted as four bytes of the key stream produced by Lex. At odd rounds the four bytes of the leak are extracted at positions (0, 0), (0, 2), (2, 0), (2, 2); at even rounds the four bytes of the leak are extracted at positions (0, 1), (0, 3), (2, 1), (2, 3). The output of every round is fed as the input to the next round. The operation of Lex is shown in Fig. 1.

## 4 Lex(2,2,4)

With Lex(2,2,4) we designate a small-scale version of stream cipher Lex based on the block cipher SR(10,2,2,4). SR(10,2,2,4) is one of the small-scale versions of AES proposed in [9]. Lex(2,2,4) has a state of 2 × 2 words of size 4 bits each. Thus Lex(2,2,4) has 16-bit state and 16-bit key. At every round Lex(2,2,4) leaks 4 bits, which is one-fourth of the whole state as is also the case for Lex. At odd rounds the byte of the leak is extracted at position (0, 0); at even rounds the byte of the leak is extracted at position (0, 1). The operation of Lex(2,2,4) is identical to the one of Lex and is shown in Fig. 2. A summary of the parameters of Lex and Lex(2,2,4) is given in Table 1.

doi: 10.1049/iet-ifs.2009.0118

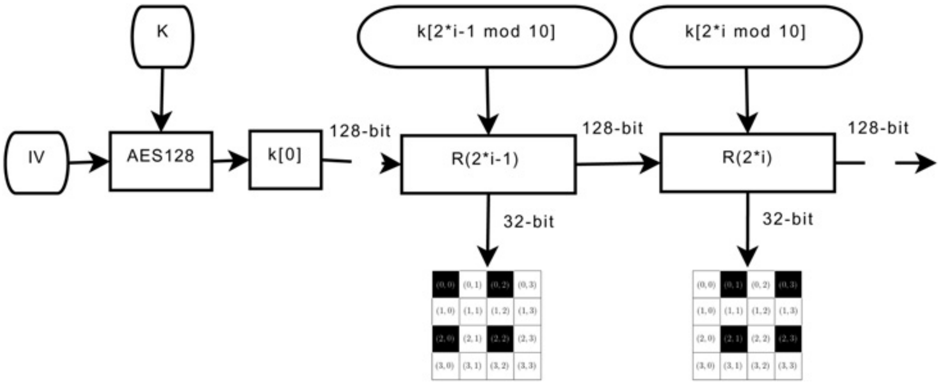

**Figure 1** *Lex: R is the round transformation of AES-128, i ≥ 1*

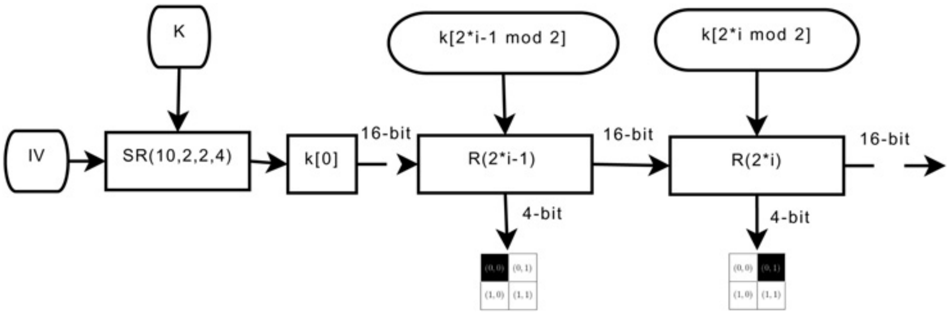

**Figure 2** *Lex(2,2,4): R is the round transformation of SR(10,2,2,4), i ≥ 1*

# 5 Constructing equations for Lex(2,2,4)

In this section, we describe how we represent the cipher Lex(2,2,4) and its key schedule as a system of boolean equations. The polynomials composing the equations are in the ring of boolean polynomials $GF(2^4) \equiv GF(2)[z]/\langle z^4 + z + 1\rangle$. We use two alternative representations of Lex(2,2,4): as a system of cubic equations and as a system of quadratic equations. We base our second representation on the quadratic equations representation of Rijndael described in [10]. We keep the structure of this section consistent with the presentation structure of [10]. The information presented next is summarised in Table 2. The equations are given in explicit form in Appendix 1 and 2.

**Table 1** Lex against Lex(2,2,4)

| Parameter | Lex | Lex(2,2,4) |
|---|---|---|
| word size, bits | 8 | 4 |
| words in state | 16 | 4 |
| state size, bits | 128 | 16 |
| round leak, bits | 32 | 4 |
| round keys | 10 | 2 |
| underlying cipher | AES-128 | SR(10,2,2,4) |

## 5.1 Cubic equations

Cipher equations for one round:

*Variables:* The variables are the input and output bits to one round of the cipher. Note that the output bits from the round are also the input bits to the next round. In total we have 32 variables.

*Linear equations:* There are four linear equations arising from the leak after the round.

**Table 2** Equations for one round of Lex(2,2,4) and two keys

| | Lex(2,2,4) | Cubic | Quadratic |
|---|---|---|---|
| cipher | variables | 32 | 48 |
| | linear eqs. | 4 | 20 |
| | non-linear eqs. | 16 | 44 |
| key schedule | variables | 32 | 32 |
| | linear eqs. | 8 | 8 |
| | non-linear eqs. | 8 | 22 |
| total | variables | 64 | 80 |
| | equations | 36 | 94 |

doi: 10.1049/iet-ifs.2009.0118

*Non-linear equations:* The non-linear equations describe the operation of SR(10,2,2,4) round function, which transforms the input bits into the output bits. In total we have 16 non-linear equations.

Key schedule equations for two keys:

*Variables:* The variables are the bits of the round keys. For two round keys we have 32 variables.

*Linear equations:* There are eight linear equations arising from the key schedule (see next).

*Non-linear equations:* The non-linear equations describe the operation of the key schedule of SR(10,2,2,4), which produces the second round key from the first. Initially, we have 16 non-linear equations. By adding the first half of the 16 equations to the second half, the initial 16 non-linear equations can be easily transformed into eight non-linear and eight linear equations. Thus the total number of non-linear equations arising from the key schedule is eight.

### 5.2 Quadratic equations

In [10] the cipher Rijndael is represented as a system of multivariate quadratic equations. This representation uses the fact that each Rijndael S-box is completely defined by a system of 23 quadratic equations [11]. In a similar way we construct a system of multivariate quadratic equations representing one round of Lex(2,2,4) and its key schedule for two round keys. We describe each 4-bit S-box of Lex(2,2,4) as a system of 11 quadratic equations.

Cipher equations for one round:

*Variables:* The variables are the input and output bits of each of the four S-boxes of the round. Note that the input bits to the S-boxes of one round are also the output bits from the previous round. In total we have 48 variables.

*Linear equations:* Similarly to Rijndael, the linear layer of the SR(10,2,2,4) round function is composed of the ShiftRows, MixColumns and AddRoundKey operations. It corresponds to a system of 16 linear equations. There are also four additional linear equations arising from the bits of the leak after the round. In total we have 20 linear equations.

*Non-linear equations:* The non-linear equations are the equations of the S-boxes. Each S-box is defined with 11 quadratic equations. In total we have 44 non-linear equations.

Key schedule equations for two keys:

*Variables:* The variables are the inputs and the outputs of the S-boxes in the key schedule. The round key of SR(10,2,2,4) is composed of two columns of two 4-bit words each. In the key schedule the SubBytes transformation is applied to the first column. We choose our variables to be the inputs and the outputs of the two S-boxes in the computed round key and the inputs to the two S-boxes for the next round key (which are also the bits of the second column of the computed round key). For two round keys we have 32 variables in total.

*Linear equations:* The linear equations arise from the linear relations binding the outputs of the S-boxes of the computed round key to the inputs of the S-boxes of the next round key. For two round keys we have eight linear equations.

*Non-linear equations:* The non-linear equations are the S-box equations of the key schedule. For two round keys of which the second is derived from the first we have two applications of the SR(10,2,2,4) 4-bit S-box. In total we have 22 non-linear equations.

## 6 Key recovery attack on Lex(2,2,4) using Gröbner bases

In [8], a general Gröbner bases attack algorithm is presented. It is applied for key recovery attacks on instances of block ciphers FLURRY and CURRY. This algorithm is also discussed in [12]. In this section, we adapt the algorithm from [8] for the case of Lex(2,2,4). We describe the modified algorithm next.

1. Set up a polynomial system $\mathcal{E} = \{e_i = 0\}$ for $R$ rounds of Lex(2,2,4), starting from round 1 (so that we can use the bits of the leak after round 0). The equations $\{e_i = 0\}$ are obtained for each round as discussed in Section 5. The system $\mathcal{E}$ consists of cipher equations, key schedule equations and leak equations.

2. Set the number of bits $L$, which are guessed at the output of every round (it is possible that $L = 0$). In this way the total number of leaked bits per round becomes $4 + L$. Because we have constructed $\mathcal{E}$ starting from round 1, for $R$ rounds we have $(R + 1)$ leaks of size $(4 + L)$ bits each. The total number of guessed bits for $R$ rounds is $(R + 1)L$.

3. For all possible $2^{(R+1)L}$ values of all guessed bits do:

3a. Get the next value of the guessed bits $l_0, l_1, \ldots, l_{(R+1)(L-1)}$. Compose the system $\mathcal{D} = \{d_i = 0\}$ of $(R+1)L$ additional linear equations arising from the guessed bits

$$x_0^{(0)} + l_0 = 0$$

$$x_1^{(0)} + l_1 = 0$$

$$\ldots$$

$$x_{L-1}^{(R)} + l_{(R+1)(L-1)} = 0$$

where $x_i^{(r)}$, $0 \le r \le R$, $0 \le i \le L-1$, are the variables corresponding to the guessed bits from the leak after round $r$.

Let $\mathcal{I}$ be the ideal generated by the set of polynomials $\mathcal{P} = (\bigcup_i e_i) \cup (\bigcup_i d_i)$. Following the terminology of [8] we call $\mathcal{I}$ the key recovery ideal.

3b. Compute the dimension $dim(\mathcal{I})$ of $\mathcal{I}$. If $dim(\mathcal{I}) = 0$ (a finite number of solutions exist) then do:

3bi. Compute a degree-reverse lexicographic Gröbner basis $G$ of $\mathcal{I}$.

3bii. Compute the variety $V$ of $G$. $V$ contains the solutions to the system $\mathcal{E} \cup \mathcal{D}$, including the key bits. Store the key bits of the solutions in a list $T$ of possible key candidates.

4. For all entries $t_i$ in $T$ do: use $t_i$ as a key for Lex(2,2,4) and produce output for $r > R$ rounds. Compare the outputs from the last $r - R$ rounds with the output for the same rounds produced by Lex(2,2,4) under the secret key. If the outputs match, then $t_i$ is the secret key – store it in $k$ and go to next step.

5. Return $k$ and terminate.

Note on step 3b.: $\dim(\mathcal{I})$ represents the dimension of the solution set. The algebraic system has a finite number of solutions only when $\dim(\mathcal{I}) = 0$. This is why in the algorithm we proceed to computing the Gröbner basis and the variety only when $\dim(\mathcal{I}) = 0$.

**Table 3** Cubic equations for Lex(2,2,4)

| r | leak | guess | eqs | var | odef | sol | gb, s | variety, s |
|---|---|---|---|---|---|---|---|---|
| 1 | 16 | 24 | 64 | 64 | 1.000 | 1 | 0.144 | 0.35 |
| | 15 | 22 | 62 | 64 | 0.969 | 4 | 0.144 | 0.60 |
| | 14 | 20 | 60 | 64 | 0.937 | n/a | n/a | n/a |
| 2 | 12 | 24 | 84 | 80 | 1.050 | 1 | 0.200 | 0.730 |
| | 11 | 21 | 81 | 80 | 1.012 | 1 | 0.212 | 0.730 |
| | 10 | 18 | 78 | 80 | 0.975 | 5 | 0.228 | 1.460 |
| | 9 | 15 | 75 | 80 | 0.938 | n/a | n/a | n/a |
| 3 | 11 | 28 | 108 | 96 | 1.125 | 1 | 0.260 | 1.450 |
| | 10 | 24 | 104 | 96 | 1.083 | 1 | 0.276 | 1.450 |
| | 9 | 20 | 100 | 96 | 1.041 | 1 | 0.256 | 1.480 |
| | 8 | 16 | 96 | 96 | 1 | n/a | n/a | n/a |
| 4 | 10 | 30 | 130 | 112 | 1.160 | 1 | 0.336 | 2.880 |
| | 9 | 25 | 125 | 112 | 1.116 | 1 | 0.328 | 2.800 |
| | 8 | 20 | 120 | 112 | 1.071 | 1 | 0.328 | 2.810 |
| | 7 | 15 | 115 | 112 | 1.027 | n/a | n/a | n/a |
| 5 | 9 | 30 | 150 | 128 | 1.171 | 1 | 0.424 | 8.52 |
| | 8 | 24 | 144 | 128 | 1.125 | 1 | 0.436 | 10.55 |
| | 7 | 18 | 138 | 128 | 1.078 | 1 | 0.412 | 10.63 |
| | 6 | 12 | 132 | 128 | 1.031 | n/a | n/a | n/a |
| 6 | 9 | 35 | 175 | 144 | 1.215 | 1 | 0.512 | 18.71 |
| | 8 | 28 | 168 | 144 | 1.166 | 1 | 0.508 | 19.08 |
| | 7 | 21 | 161 | 144 | 1.118 | 1 | 0.536 | 19.28 |
| | 6 | 14 | 154 | 144 | 1.069 | n/a | n/a | n/a |

## 7 Experimental setting

We have performed our experiments using the open-source computer algebra system Sage [13] on a machine with

**Table 4** Quadratic equations for Lex(2,2,4)

| r | leak | guess | eqs | var | odef | sol | gb, s | variety, s |
|---|---|---|---|---|---|---|---|---|
| 1 | 8 | 8 | 114 | 80 | 1.425 | 256 | 0.256 | 41.18 |
| | 7 | 6 | 111 | 80 | 1.387 | n/a | n/a | n/a |
| 2 | 8 | 12 | 190 | 112 | 1.696 | 1 | 0.364 | 2.79 |
| | 7 | 9 | 185 | 112 | 1.651 | 1 | 0.352 | 2.77 |
| | 6 | 6 | 180 | 112 | 1.607 | 4 | 0.360 | 3.68 |
| | 5 | 5 | 175 | 112 | 1.562 | n/a | n/a | n/a |
| 3 | 8 | 16 | 266 | 144 | 1.847 | 1 | 0.592 | 15.14 |
| | 7 | 12 | 259 | 144 | 1.799 | 1 | 0.572 | 14.93 |
| | 6 | 8 | 252 | 144 | 1.750 | 1 | 0.564 | 15.09 |
| | 5 | 4 | 245 | 144 | 1.701 | 2 | 0.524 | 15.38 |
| | 4 | 0 | 238 | 144 | 1.653 | n/a | n/a | n/a |
| 4 | 8 | 20 | 342 | 176 | 1.943 | 1 | 0.784 | 39.77 |
| | 7 | 15 | 333 | 176 | 1.892 | 1 | 0.768 | 39.99 |
| | 6 | 10 | 324 | 176 | 1.841 | 1 | 0.744 | 40.05 |
| | 5 | 5 | 315 | 176 | 1.789 | 1 | 0.740 | 40.12 |
| | 4 | 0 | 306 | 176 | 1.739 | n/a | n/a | n/a |
| 5 | 8 | 24 | 418 | 208 | 2.009 | 1 | 1.012 | 84.67 |
| | 7 | 18 | 407 | 208 | 1.957 | 1 | 1.004 | 84.42 |
| | 6 | 12 | 396 | 208 | 1.904 | 1 | 1.032 | 84.27 |
| | 5 | 6 | 385 | 208 | 1.851 | 1 | 1.024 | 84.43 |
| | **4** | **0** | **374** | **208** | **1.798** | **1** | **1.024** | **85.01** |
| 6 | 8 | 28 | 494 | 240 | 2.058 | 1 | 1.364 | 168.92 |
| | 7 | 21 | 481 | 240 | 2.004 | 1 | 1.400 | 157.73 |
| | 6 | 14 | 468 | 240 | 1.950 | 1 | 1.312 | 157.49 |
| | 5 | 7 | 455 | 240 | 1.895 | 1 | 1.300 | 157.36 |
| | 4 | 0 | 442 | 240 | 1.841 | 1 | 1.316 | 157.72 |

2.2 GHz CPU AMD Opteron(tm) Processor 275 and 4 GB RAM with OS GNU/Linux. For computation of Gröbner bases in the boolean polynomial ring, Sage uses the open-source library PolyBoRi [14].

## 8 Results

For different number of rounds and sizes of the leak we construct a system of equations as discussed in Section 5. We solve the system using the algorithm described in Section 6. The results from our experiments are shown in Tables 3 and 4. Before we explain the data in the tables, we would like first to elaborate a bit on what it means to vary the number of rounds and the sizes of the leak.

When we increase the number of rounds for which we run the cipher, we also increase the total number of equations and unknowns in the algebraic system. On the one hand this increases the overall complexity of the system and so it becomes harder to be solved. On the other hand, with the increase of the number of rounds the number of equations grows faster than the number of unknowns and so the system becomes more and more over-defined. This in turn makes it easier to be solved. As to the number of leaked bits: when we increase the sizes of the leaks on one hand we decrease the number of unknowns in the system and so it becomes easier to be solved. On the other hand for every leak size bigger than 4 bits we have to guess the values of the additional bits. For every guessed value of additional leaked bits we have to solve a separate algebraic system, which increases the overall work. To summarise: more rounds means more equations and unknowns but also more over-defined-*ness*; bigger size of the leaks means less unknowns, but also more time and work. Next we proceed with explaining the data in the tables.

Each row of Tables 3 and 4 gives information on constructing and solving the system of equations resulting from Lex(2,2,4) for a given number of rounds and a given size of the leak after each round. For a fixed number of rounds only the results from the last several experiments are presented. For example when results for sizes of the leak 12, 11, 10, 9 bits are shown, it means that we are also able to solve the system for leak sizes 16, 15, 14 and 13 bits but we are not able to solve it for leak sizes 9 bits and less. The fact that the system resulting from a certain size of the leak (9 bits in the last example) cannot be solved is indicated by the abbreviation ‘n/a’ (not available) in the last three columns of the tables. The rest of the information in the tables is the following:

*R:* Number of rounds for which equations are generated: between 1 and 6. We chose to limit our experiments to the first six rounds because at round 5 (for the quadratic case) we are already able to recover the key without guessing any bits from the leaks.

*Leak:* The number of bits which are leaked after every round. Four bits of every leak are known by design. The remaining bits of each leak are guessed by exhaustive search. For example when a leak has size 16 bits, 4 of the 16 bits are known while the remaining 12 bits are guessed by searching through all possible $2^{12}$ values (see also Step 2 of the algorithm described in Section 6).

*Guess:* Total number of guessed bits for the specified number of rounds and size of the leak.

*Eqs:* The number of equations in one system resulting for the specific number of rounds and leaks.

*Var:* The number of variables participating in the equations in one system.

*Odef:* A measure of the extent to which the algebraic system is over-defined. This value is obtained by dividing the number of equations by the number of variables.

*Sol:* Number of solutions to the given system.

*Gb:* The time (in seconds) necessary for the computation of the Gröbner basis of the polynomials composing the given system.

*Variety:* The time (in seconds) necessary for the computation of the algebraic variety of the given system.

From the data in Tables 3 and 4 it can be seen that the best result is obtained for the quadratic representation of Lex(2,2,4) (Table 4) for five rounds and 4-bit leak (in

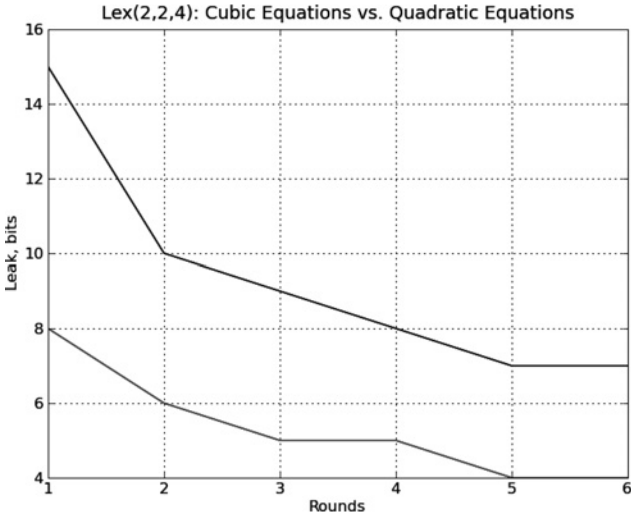

**Figure 3** *Smallest leak sizes for which it was computationally possible to solve the systems of cubic (upper graph) and quadratic (lower graph) equations for different number of rounds*

doi: 10.1049/iet-ifs.2009.0118

bold). In this case we solve a system of 374 equations in 208 variables. We obtain one solution, which contains the bits of the secret key. The times necessary for the computation of the Gröbner basis and the variety are 1.024 and 85.01 s, respectively. Given the fact that those are the two most computationally expensive operations we can estimate the total timing of the attack to be less than 2 min.

In Fig. 3 are plotted the smallest leak sizes for which it was computationally possible to solve the systems of cubic (upper graph) and quadratic (lower graph) equations for different number of rounds.

## 9 Implications for the full-scale Lex

In this section, we estimate the complexity of solving a system of equations describing the full-scale cipher Lex according to the method presented in Sections 5 and 6. We use the quadratic representation of Lex described in Section 5.2, because for this case we obtain the best experimantal results (as was shown in Section 8). We obtain the following expressions for calculating the number of boolean quadratic equations $m$ and the number of variables $n$ for a given number of rounds $r$ of the original Lex

$$m = 528r + 1084$$
$$n = 256r + 800$$

The constants 1084 and 800 come mostly from the equations and variables of the key schedule which are not dependent on $r$ when $r > 9$ (as mentioned Lex has 10 round keys which are used circularly). To estimate the complexity of solving a system with the above number of quadratic boolean equations $m$ in $n$ variables we use the results of [15, 16]. In particular, we use the upper bounds on the complexities of solving systems of boolean equations using Gröbner bases given in [15]. Three complexity classes are defined depending on the ratio between $m$ and $n$ ($N$ is a constant)

- Exponential: $m \sim Nn$
- Sub-exponenial: $n \leq m \leq n^2$
- Polynomial: $m \sim Nn^2$

From the expressions for $m$ and $n$ for Lex given in the beginning of the section it can be easily checked that $m \sim 2n$. Thus the complexity of the system for Lex falls into the first class – exponential complexity. Therefore the recovery of the key for the full-scale cipher Lex using our method will have exponential complexity. Based on the above analysis we can conclude that the security of the full-scale cipher Lex against algebraic attacks is not threatened.

## 10 Conclusion

In this paper we analysed a small-scale version of the stream cipher Lex [3] with respect to algebraic attacks. We call the small-scale version – Lex(2,2,4). We represented Lex(2,2,4) algebraically in two alternative ways: as a system of boolean quadratic equations and as a system of boolean cubic equations. We experimented with solving the two systems for different number of rounds and leak sizes. We obtain the best results for the quadratic representation of Lex(2,2,4). For this case we are able to recover the secret key in time less than 2 min by solving a system of 374 quadratic boolean equations in 208 unknowns resulting from five rounds of the cipher. Although mathematically successful, this result cannot be classified as an attack in the cryptographic sense, because the measured time is greater than the time for exhaustive search on $2^{16}$ values. Estimations for applying our method to the full-scale version of Lex showed exponential growth in computational complexity. Although faster implementations of the Gröbner basis algorithm as well as future advances in computing technology may lower the time complexity of our method, for the moment we consider Lex not vulnerable to algebraic attacks.

## 11 Acknowledgments

The authors thank Martin Albrecht for proofreading and insightful comments on the preliminary draft as well as for his extremely helpful suggestions for improving the efficiency of the Gröbner basis computation in Sage. They thank also Frederik Vercauteren for pointing us to important results on the complexities of solving systems of equations using Gröbner basis. This work was supported in part by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government, by the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy), and in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT.

## 12 References

[1] BIRYUKOV A.: 'A new 128-bit key stream cipher Lex'. eSTREAM, ECRYPT Stream Cipher Project, Report 2005/013

[2] BIRYUKOV A.: 'The tweak for Lex-128, Lex-192, Lex-256; Lex (Phase 2)'. eSTREAM, ECRYPT Stream Cipher Project, Report 2006/037

[3] BIRYUKOV A.: 'The design of a stream cipher Lex', *Sel. Areas Cryptogr.*, 2006, **4356**, pp. 67–75

[4] PRENEEL B., WU H.: 'Resynchronization attacks on WG and Lex', *FSE*, 2006, pp. 422–432

doi: 10.1049/iet-ifs.2009.0118

[5] ENGLUND H., HELL M., JOHANSSON T.: 'A note on distinguishing attacks, information theory for wireless networks'. 2007 IEEE Information Theory Workshop, 1–6 July 2007, vol. 4047, pp. 1–4

[6] DUNKELMAN O., KELLER N.: 'A new attack on the Lex stream cipher', *ASIACRYPT*, 2008, **5350**, pp. 539–556

[7] Z'ABA R.M., RADDUM H., SIMPSON L., DAWSON E., HENRICKSEN M., WONG K.: 'Algebraic analysis of Lex'. Proc. Seventh Australasian Information Security Conf. AISC 2009, Wellington, New Zealand, CRPIT, 98, (BRANKOVIC L, SUSILO W. EDS), pp. 33–45

[8] BUCHMANN J., PYSHKIN A., WEINMANN R.-P.: 'Block ciphers sensitive to Gröbner basis attacks', *CT-RSA*, 2006, **3860**, pp. 313–331

[9] CID C., MURPHY S., ROBSHAW M.J.B.: 'Small scale variants of the AES', *FSE*, 2005, **3557**, pp. 145–162

[10] BIRYUKOV A., DE CANNIERE C.: 'Block ciphers and systems of quadratic equations', *FSE*, 2003, **2887**, pp. 274–289

[11] COURTOIS N., PIEPRZYK J.: 'Cryptanalysis of block ciphers with overdefined systems of equations'. ASIACRYPT, 2002, pp. 267–287

[12] ALBRECHT M.: 'Algebraic attacks on the Courtois Toy cipher', *J. Cryptol.*, 2008, **32**, (3), pp. 220–276

[13] WILLIAM S.: 'Sage: Open source mathematical software (Version 3.1.4)' (The Sage Group, 2008), http://www.sagemath.org

[14] BRICKENSTEIN M., DREYER A.: 'PolyBoRi: A framework for Gröbner basis computations with Boolean polynomials'. Electronic Proc. MEGA 2007 – Effective Methods in Algebraic Geometry, Strobl, Austria, June 2007

[15] BARDET M., FAUGERE J.C., SALVY B.: 'On the complexity of Gröbner basis computation of semi-regular overdetermined sequences over F2 with solutions in F2'. Rapport de recherche de l'INRIA, December 2003, p. 19

[16] BARDET M., FAUGERE J.C., SALVY B.: 'On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations'. Proc. Int. Conf. on Polynomial System Solving, 2004, pp. 71–74

[17] DAEMEN J., RIJMEN V.: 'AES proposal: Rijndael' (NIST AES proposal, 1998)

[18] DAEMEN J., RIJMEN V.: 'The design of Rijndael: AES – the advanced encryption standard' (Springer-Verlag, 2002)

[19] BUCHBERGER B.: 'An algorithmical criterion for the solvability of algebraic systems of equations', *Aequationes Math.*, 1970, **4**, (3), 374–383

# 13 Appendix: A Cubic equations

Cubic Equations for Lex(2,2,4)

1 Round, 2 leaks of size 4 bits, 2 Round keys

## 13.1 Actual values with which the experiments were performed

Round key 0 (initial key)

$$[x_0, x_1, \ldots, x_{15}] = [1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0]$$

Round key 1 (calculated from key 0)

$$[x_{16}, x_{31}, \ldots, x_{31}] = [1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0]$$

Actual values of the round input

$$[x_{32}, x_{33}, \ldots, x_{47}] = [1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1]$$

Actual values of the round output

$$[x_{48}, x_{49}, \ldots, x_{63}] = [0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1]$$

## 13.2 Key variables

$x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}, x_{17}, x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{31}$

## 13.3 Key variables outlay

Round key 0 (initial key)

$x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}$

Round key 1 (calculated from Round key 0)

$x_{16}, x_{17}, x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{31}$

doi: 10.1049/iet-ifs.2009.0118

## 13.4 Key schedule equations

$$\begin{aligned}
0 &= x_0 + x_{12}x_{13}x_{14} + x_{12}x_{13}x_{15} + x_{12}x_{14}x_{15} \\
&\quad + x_{12}x_{14} + x_{12}x_{15} + x_{12} + x_{13}x_{14}x_{15} \\
&\quad + x_{13}x_{15} + x_{13} + x_{15} + x_{16} \\
0 &= x_1 + x_{12}x_{13}x_{15} + x_{12}x_{14}x_{15} + x_{13}x_{14}x_{15} \\
&\quad + x_{13}x_{14} + x_{13} + x_{14}x_{15} + x_{15} + x_{17} \\
0 &= x_2 + x_{12}x_{13}x_{14} + x_{12}x_{13} + x_{12}x_{14}x_{15} + x_{12} + x_{13}x_{14} \\
&\quad + x_{13}x_{15} + x_{14}x_{15} + x_{14} + x_{15} + x_{18} + 1 \\
0 &= x_3 + x_{12}x_{13}x_{14} + x_{12}x_{13}x_{15} + x_{12}x_{13} + x_{12}x_{15} \\
&\quad + x_{12} + x_{14}x_{15} + x_{15} + x_{19} \\
0 &= x_4 + x_8x_9x_{10} + x_8x_9x_{11} + x_8x_{10}x_{11} + x_8x_{10} + x_8x_{11} + x_8 \\
&\quad + x_9x_{10}x_{11} + x_9x_{11} + x_9 + x_{11} + x_{20} \\
0 &= x_5 + x_8x_9x_{11} + x_8x_{10}x_{11} + x_9x_{10}x_{11} + x_9x_{10} \\
&\quad + x_9 + x_{10}x_{11} + x_{11} + x_{21} + 1 \\
0 &= x_6 + x_8x_9x_{10} + x_8x_9 + x_8x_{10}x_{11} + x_8 + x_9x_{10} \\
&\quad + x_9x_{11} + x_{10}x_{11} + x_{10} + x_{11} + x_{22} + 1 \\
0 &= x_7 + x_8x_9x_{10} + x_8x_9x_{11} + x_8x_9 + x_8x_{11} + x_8 \\
&\quad + x_{10}x_{11} + x_{11} + x_{23} \\
0 &= x_0 + x_8 + x_{12}x_{13}x_{14} + x_{12}x_{13}x_{15} + x_{12}x_{14}x_{15} + x_{12}x_{14} \\
&\quad + x_{12}x_{15} + x_{12} + x_{13}x_{14}x_{15} + x_{13}x_{15} + x_{13} + x_{15} + x_{24} \\
0 &= x_1 + x_9 + x_{12}x_{13}x_{15} + x_{12}x_{14}x_{15} \\
&\quad + x_{13}x_{14}x_{15} + x_{13}x_{14} + x_{13} + x_{14}x_{15} + x_{15} + x_{25} \\
0 &= x_2 + x_{10} + x_{12}x_{13}x_{14} + x_{12}x_{13} + x_{12}x_{14}x_{15} + x_{12} \\
&\quad + x_{13}x_{14} + x_{13}x_{15} + x_{14}x_{15} + x_{14} + x_{15} + x_{26} + 1 \\
0 &= x_3 + x_{11} + x_{12}x_{13}x_{14} + x_{12}x_{13}x_{15} \\
&\quad + x_{12}x_{13} + x_{12}x_{15} + x_{12} + x_{14}x_{15} + x_{15} + x_{27} \\
0 &= x_4 + x_8x_9x_{10} + x_8x_9x_{11} + x_8x_{10}x_{11} + x_8x_{10} + x_8x_{11} + x_8 \\
&\quad + x_9x_{10}x_{11} + x_9x_{11} + x_9 + x_{11} + x_{12} + x_{28} \\
0 &= x_5 + x_8x_9x_{11} + x_8x_{10}x_{11} \\
&\quad + x_9x_{10}x_{11} + x_9x_{10} + x_9 + x_{10}x_{11} + x_{11} + x_{13} + x_{29} + 1 \\
0 &= x_6 + x_8x_9x_{10} + x_8x_9 + x_8x_{10}x_{11} + x_8 + x_9x_{10} + x_9x_{11} \\
&\quad + x_{10}x_{11} + x_{10} + x_{11} + x_{14} + x_{30} + 1 \\
0 &= x_7 + x_8x_9x_{10} + x_8x_9x_{11} + x_8x_9 + x_8x_{11} + x_8 \\
&\quad + x_{10}x_{11} + x_{11} + x_{15} + x_{31}
\end{aligned}$$

By adding the first half of the key equations to the second half, the above system is transformed into

$$\begin{aligned}
0 &= x_0 + x_{12}x_{13}x_{14} + x_{12}x_{13}x_{15} + x_{12}x_{14}x_{15} \\
&\quad + x_{12}x_{14} + x_{12}x_{15} + x_{12} + x_{13}x_{14}x_{15} \\
&\quad + x_{13}x_{15} + x_{13} + x_{15} + x_{16} \\
0 &= x_1 + x_{12}x_{13}x_{15} + x_{12}x_{14}x_{15} + x_{13}x_{14}x_{15} + x_{13}x_{14} \\
&\quad + x_{13} + x_{14}x_{15} + x_{15} + x_{17} \\
0 &= x_2 + x_{12}x_{13}x_{14} + x_{12}x_{13} + x_{12}x_{14}x_{15} + x_{12} + x_{13}x_{14} \\
&\quad + x_{13}x_{15} + x_{14}x_{15} + x_{14} + x_{15} + x_{18} + 1 \\
0 &= x_3 + x_{12}x_{13}x_{14} + x_{12}x_{13}x_{15} + x_{12}x_{13} + x_{12}x_{15} \\
&\quad + x_{12} + x_{14}x_{15} + x_{15} + x_{19} \\
0 &= x_4 + x_8x_9x_{10} + x_8x_9x_{11} + x_8x_{10}x_{11} + x_8x_{10} + x_8x_{11} + x_8 \\
&\quad + x_9x_{10}x_{11} + x_9x_{11} + x_9 + x_{11} + x_{20} \\
0 &= x_5 + x_8x_9x_{11} + x_8x_{10}x_{11} + x_9x_{10}x_{11} + x_9x_{10} \\
&\quad + x_9 + x_{10}x_{11} + x_{11} + x_{21} + 1 \\
0 &= x_6 + x_8x_9x_{10} + x_8x_9 + x_8x_{10}x_{11} + x_8 + x_9x_{10} \\
&\quad + x_9x_{11} + x_{10}x_{11} + x_{10} + x_{11} + x_{22} + 1 \\
0 &= x_7 + x_8x_9x_{10} + x_8x_9x_{11} + x_8x_9 + x_8x_{11} + x_8 + x_{10}x_{11} \\
&\quad + x_{11} + x_{23} \\
0 &= x_8 + x_{16} + x_{24} \\
0 &= x_9 + x_{17} + x_{25} \\
0 &= x_{10} + x_{18} + x_{26} \\
0 &= x_{11} + x_{19} + x_{27} \\
0 &= x_{12} + x_{20} + x_{28} \\
0 &= x_{13} + x_{21} + x_{29} \\
0 &= x_{14} + x_{22} + x_{30} \\
0 &= x_{15} + x_{23} + x_{31}
\end{aligned}$$

## 13.5 State variables

$$\begin{gathered}
x_{32}, x_{33}, x_{34}, x_{35}, x_{36}, x_{37}, x_{38}, x_{39}, x_{40}, x_{41}, x_{42}, x_{43}, \\
x_{44}, x_{45}, x_{46}, x_{47}, x_{48}, x_{49}, x_{50}, x_{51}, x_{52}, x_{53}, x_{54}, \\
x_{55}, x_{56}, x_{57}, x_{58}, x_{59}, x_{60}, x_{61}, x_{62}, x_{63}
\end{gathered}$$

## 13.6 State variables outlay

Input to the round

$$\begin{gathered}
x_{32}, x_{33}, x_{34}, x_{35}, x_{36}, x_{37}, x_{38}, x_{39}, \\
x_{40}, x_{41}, x_{42}, x_{43}, x_{44}, x_{45}, x_{46}, x_{47}
\end{gathered}$$

Output from the round (input to the next round)

$$\begin{gathered}
x_{48}, x_{49}, x_{50}, x_{51}, x_{52}, x_{53}, x_{54}, x_{55}, x_{56}, x_{57}, x_{58}, x_{59}, x_{60}, \\
x_{61}, x_{62}, x_{63}
\end{gathered}$$

## 13.7 Cipher equations

$$\begin{aligned}
0 &= x_0 + x_{32}x_{33} + x_{32}x_{34}x_{35} + x_{32}x_{34} + x_{33}x_{34}x_{35} + x_{33}x_{35} \\
&\quad + x_{33} + x_{34}x_{35} + x_{44}x_{45}x_{46} + x_{44}x_{45}x_{47} + x_{44}x_{45} \\
&\quad + x_{44}x_{47} + x_{44} + x_{46}x_{47} + x_{47} + x_{48} \\
0 &= x_1 + x_{32}x_{33}x_{35} + x_{32}x_{33} + x_{32}x_{34} + x_{33}x_{34} + x_{33}x_{35} \\
&\quad + x_{35} + x_{44}x_{45} + x_{44}x_{46}x_{47} + x_{44}x_{46} + x_{45}x_{46}x_{47} \\
&\quad + x_{45}x_{47} + x_{45} + x_{46}x_{47} + x_{49} + 1 \\
0 &= x_2 + x_{32}x_{33}x_{34} + x_{32}x_{33}x_{35} + x_{32}x_{33} + x_{32} + x_{33}x_{34}x_{35} \\
&\quad + x_{33}x_{35} + x_{33} + x_{34} + x_{44}x_{45}x_{47} + x_{44}x_{46}x_{47} \\
&\quad + x_{45}x_{46}x_{47} + x_{45}x_{46} + x_{45} + x_{46}x_{47} + x_{47} + x_{50} + 1
\end{aligned}$$

$$\begin{aligned}
0 &= x_3 + x_{32}x_{33}x_{35} + x_{32}x_{34}x_{35} + x_{32}x_{35} + x_{33}x_{34}\\
&\quad + x_{33}x_{35} + x_{34} + x_{44}x_{45}x_{46} + x_{44}x_{45} + x_{44}x_{46}x_{47}\\
&\quad + x_{44} + x_{45}x_{46} + x_{45}x_{47} + x_{46}x_{47} + x_{46} + x_{47} + x_{51}\\
0 &= x_4 + x_{36}x_{37} + x_{36}x_{38}x_{39} + x_{36}x_{38} + x_{37}x_{38}x_{39} + x_{37}x_{39}\\
&\quad + x_{37} + x_{38}x_{39} + x_{40}x_{41}x_{42} + x_{40}x_{41}x_{43} + x_{40}x_{41}\\
&\quad + x_{40}x_{43} + x_{40} + x_{42}x_{43} + x_{43} + x_{52}\\
0 &= x_5 + x_{36}x_{37}x_{39} + x_{36}x_{37} + x_{36}x_{38} + x_{37}x_{38} + x_{37}x_{39}\\
&\quad + x_{39} + x_{40}x_{41} + x_{40}x_{42}x_{43} + x_{40}x_{42}\\
&\quad + x_{41}x_{42}x_{43} + x_{41}x_{43} + x_{41} + x_{42}x_{43} + x_{53} + 1\\
0 &= x_6 + x_{36}x_{37}x_{38} + x_{36}x_{37}x_{39} + x_{36}x_{37} + x_{36} + x_{37}x_{38}x_{39}\\
&\quad + x_{37}x_{39} + x_{37} + x_{38} + x_{40}x_{41}x_{43} + x_{40}x_{42}x_{43}\\
&\quad + x_{41}x_{42}x_{43} + x_{41}x_{42} + x_{41} + x_{42}x_{43} + x_{43} + x_{54} + 1\\
0 &= x_7 + x_{36}x_{37}x_{39} + x_{36}x_{38}x_{39} + x_{36}x_{39} + x_{37}x_{38} + x_{37}x_{39}\\
&\quad + x_{38} + x_{40}x_{41}x_{42} + x_{40}x_{41} + x_{40}x_{42}x_{43} + x_{40} + x_{41}x_{42}\\
&\quad + x_{41}x_{43} + x_{42}x_{43} + x_{42} + x_{43} + x_{55}\\
0 &= x_8 + x_{32}x_{33}x_{34} + x_{32}x_{33}x_{35} + x_{32}x_{33} + x_{32}x_{35} + x_{32}\\
&\quad + x_{34}x_{35} + x_{35} + x_{44}x_{45} + x_{44}x_{46}x_{47} + x_{44}x_{46}\\
&\quad + x_{45}x_{46}x_{47} + x_{45}x_{47} + x_{45} + x_{46}x_{47} + x_{56}\\
0 &= x_9 + x_{32}x_{33} + x_{32}x_{34}x_{35} + x_{32}x_{34} + x_{33}x_{34}x_{35} + x_{33}x_{35}\\
&\quad + x_{33} + x_{34}x_{35} + x_{44}x_{45}x_{47} + x_{44}x_{45} + x_{44}x_{46}\\
&\quad + x_{45}x_{46} + x_{45}x_{47} + x_{47} + x_{57} + 1\\
0 &= x_{10} + x_{32}x_{33}x_{35} + x_{32}x_{34}x_{35} + x_{33}x_{34}x_{35} + x_{33}x_{34} + x_{33}\\
&\quad + x_{34}x_{35} + x_{35} + x_{44}x_{45}x_{46} + x_{44}x_{45}x_{47} + x_{44}x_{45} + x_{44}\\
&\quad + x_{45}x_{46}x_{47} + x_{45}x_{47} + x_{45} + x_{46} + x_{58} + 1\\
0 &= x_{11} + x_{32}x_{33}x_{34} + x_{32}x_{33} + x_{32}x_{34}x_{35} + x_{32} + x_{33}x_{34}\\
&\quad + x_{33}x_{35} + x_{34}x_{35} + x_{34} + x_{35} + x_{44}x_{45}x_{47} + x_{44}x_{46}x_{47}\\
&\quad + x_{44}x_{47} + x_{45}x_{46} + x_{45}x_{47} + x_{46} + x_{59}\\
0 &= x_{12} + x_{36}x_{37}x_{38} + x_{36}x_{37}x_{39} + x_{36}x_{37} + x_{36}x_{39} + x_{36}\\
&\quad + x_{38}x_{39} + x_{39} + x_{40}x_{41} + x_{40}x_{42}x_{43} + x_{40}x_{42}\\
&\quad + x_{41}x_{42}x_{43} + x_{41}x_{43} + x_{41} + x_{42}x_{43} + x_{60}\\
0 &= x_{13} + x_{36}x_{37} + x_{36}x_{38}x_{39} + x_{36}x_{38} + x_{37}x_{38}x_{39}\\
&\quad + x_{37}x_{39} + x_{37} + x_{38}x_{39} + x_{40}x_{41}x_{43}\\
&\quad + x_{40}x_{41} + x_{40}x_{42} + x_{41}x_{42} + x_{41}x_{43} + x_{43} + x_{61} + 1\\
0 &= x_{14} + x_{36}x_{37}x_{39} + x_{36}x_{38}x_{39} + x_{37}x_{38}x_{39} + x_{37}x_{38} + x_{37}\\
&\quad + x_{38}x_{39} + x_{39} + x_{40}x_{41}x_{42} + x_{40}x_{41}x_{43} + x_{40}x_{41} + x_{40}\\
&\quad + x_{41}x_{42}x_{43} + x_{41}x_{43} + x_{41} + x_{42} + x_{62} + 1\\
0 &= x_{15} + x_{36}x_{37}x_{38} + x_{36}x_{37} + x_{36}x_{38}x_{39} + x_{36} + x_{37}x_{38}\\
&\quad + x_{37}x_{39} + x_{38}x_{39} + x_{38} + x_{39} + x_{40}x_{41}x_{43} + x_{40}x_{42}x_{43}\\
&\quad + x_{40}x_{43} + x_{41}x_{42} + x_{41}x_{43} + x_{42} + x_{63}
\end{aligned}$$

### 13.8 Leak equations

Leak equations after round 0

$$\begin{aligned}
0 &= x_{32} + 1\\
0 &= x_{33}\\
0 &= x_{34}\\
0 &= x_{35} + 1
\end{aligned}$$

Leak equations after round 1

$$\begin{aligned}
0 &= x_{48}\\
0 &= x_{49} + 1\\
0 &= x_{50}\\
0 &= x_{51} + 1
\end{aligned}$$

## 14 Appendix: Quadratic equations

Quadratic Equations for Lex(2,2,4)

1 Round, 2 leaks of size 4 bits, 2 Round keys

### 14.1 Actual values with which the experiments were performed

Round key 0 (initial key)

$$[x_0, x_1, \ldots, x_{15}] = [1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0]$$

Outputs from the S-boxes of the key schedule for key 1

$$[x_{16}, x_{17}, \ldots, x_{23}] = [0, 1, 0, 1, 1, 1, 0, 1]$$

Outputs from the linear part of the key schedule for key 1

$$[x_{24}, x_{25}, \ldots, x_{31}] = [0, 1, 1, 1, 0, 0, 0, 0]$$

Actual value of the round input

$$[x_{32}, x_{33}, \ldots, x_{47}] = [0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1]$$

Actual values of the round input after the S-boxes

$$[x_{48}, x_{49}, \ldots, x_{63}] = [1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0]$$

Actual value of the round output

$$[x_{64}, x_{65}, \ldots, x_{79}] = [1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1]$$

### 14.2 Key variables

$$\begin{aligned}
&x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13},\\
&\quad x_{14}, x_{15}, x_{16}, x_{17}, x_{18}, x_{19}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, x_{26},\\
&\quad x_{27}, x_{28}, x_{29}, x_{30}, x_{31}
\end{aligned}$$

doi: 10.1049/iet-ifs.2009.0118

## 14.3 Key variables outlay

Round key 0 (initial key)

$$x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}$$

The last 8 bits of the initial key are inputs to the two S-boxes of the key schedule

Input to S-box 0 of the key schedule

$$x_{12}, x_{13}, x_{14}, x_{15}$$

Input to S-box 1 of the key schedule

$$x_8, x_9, x_{10}, x_{11}$$

Round key 1

Output from S-box 0 of the key schedule

$$x_{16}, x_{17}, x_{18}, x_{19}$$

Output from S-box 1 of the key schedule

$$x_{20}, x_{21}, x_{22}, x_{23}$$

Outputs from the linear part of the key schedule (inputs to the two S-boxes of the next round key)

$$x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{31}$$

## 14.4 Key schedule equations

Key schedule equations: S-box 0

$$\begin{aligned}
0 = {} & x_{12}x_{16} + x_{12}x_{17} + x_{12}x_{19} + x_{12} + x_{13}x_{16} + x_{13}x_{17} \\
& + x_{13} + x_{14}x_{16} + x_{14}x_{19} + x_{15}x_{18} + x_{15}x_{19} + x_{15} \\
0 = {} & x_{12}x_{16} + x_{12}x_{17} + x_{12}x_{18} + x_{13}x_{16} + x_{13}x_{17} + x_{13}x_{19} \\
& + x_{13} + x_{14}x_{16} + x_{14}x_{17} + x_{14} + x_{15}x_{16} + x_{15}x_{19} \\
0 = {} & x_{12}x_{17} + x_{12}x_{18} + x_{12}x_{19} + x_{13}x_{16} + x_{13}x_{17} + x_{13}x_{18} \\
& + x_{14}x_{16} + x_{14}x_{17} + x_{14}x_{19} + x_{14} + x_{15}x_{16} + x_{15}x_{17} + x_{15} \\
0 = {} & x_{12}x_{16} + x_{12}x_{18} + x_{12}x_{19} + x_{13}x_{16} + x_{13}x_{17} + x_{13}x_{18} \\
& + x_{14}x_{16} + x_{14}x_{17} + x_{14} + x_{15}x_{18} + x_{15}x_{19} + x_{15} \\
0 = {} & x_{12}x_{16} + x_{12}x_{17} + x_{12}x_{19} + x_{12} + x_{13}x_{16} + x_{13}x_{19} \\
& + x_{13} + x_{14}x_{19} + x_{15}x_{16} + x_{15}x_{18} + x_{15} \\
0 = {} & x_{12}x_{16} + x_{12}x_{17} + x_{12}x_{18} + x_{13}x_{16} + x_{13}x_{17} + x_{13} \\
& + x_{14}x_{18} + x_{14}x_{19} + x_{15}x_{17} + x_{15}x_{19} + x_{15} \\
0 = {} & x_{12}x_{17} + x_{12}x_{18} + x_{12}x_{19} + x_{13}x_{16} + x_{13}x_{17} + x_{13}x_{19} \\
& + x_{13} + x_{14}x_{16} + x_{14}x_{19} + x_{15}x_{19} + x_{15} \\
0 = {} & x_{12}x_{17} + x_{12}x_{19} + x_{12} + x_{13}x_{17} + x_{13}x_{18} + x_{13}x_{19} \\
& + x_{14}x_{16} + x_{14}x_{18} + x_{14} + x_{15}x_{16} + x_{15}x_{17} \\
& + x_{15}x_{18} + x_{16} + x_{18} + x_{19} + 1 \\
0 = {} & x_{12}x_{16} + x_{12}x_{17} + x_{12}x_{18} + x_{13}x_{18} + x_{13} + x_{14}x_{16} + x_{14}x_{17} \\
& + x_{14}x_{19} + x_{14} + x_{15}x_{17} + x_{15} + x_{16} + x_{17} + x_{19} + 1 \\
0 = {} & x_{12}x_{16} + x_{12}x_{18} + x_{12} + x_{13}x_{16} + x_{13}x_{17} + x_{13}x_{18} + x_{14}x_{18} \\
& + x_{14} + x_{15}x_{16} + x_{15}x_{17} + x_{15}x_{19} + x_{15} + x_{16} + x_{17} + x_{18} \\
0 = {} & x_{12}x_{17} + x_{12}x_{18} + x_{12}x_{19} + x_{13}x_{16} + x_{13}x_{18} + x_{13} + x_{14}x_{16} \\
& + x_{14}x_{17} + x_{14}x_{18} + x_{15}x_{18} + x_{15} + x_{17} + x_{18} + x_{19}
\end{aligned}$$

Key schedule equations: S-box 1

$$\begin{aligned}
0 = {} & x_8x_{20} + x_8x_{21} + x_8x_{23} + x_8 + x_9x_{20} + x_9x_{21} + x_9 \\
& + x_{10}x_{20} + x_{10} + x_{23} + x_{11}x_{22} + x_{11}x_{23} + x_{11} \\
0 = {} & x_8x_{20} + x_8x_{21} + x_8x_{22} + x_9x_{20} + x_9x_{21} + x_9x_{23} + x_9 \\
& + x_{10}x_{20} + x_{10}x_{21} + x_{10} + x_{11}x_{20} + x_{11}x_{23} \\
0 = {} & x_8x_{21} + x_8x_{22} + x_8x_{23} + x_9x_{20} + x_9x_{21} + x_9x_{22} + x_{10}x_{20} \\
& + x_{10}x_{21} + x_{10}x_{23} + x_{10} + x_{11}x_{20} + x_{11}x_{21} + x_{11} \\
0 = {} & x_8x_{20} + x_8x_{22} + x_8x_{23} + x_9x_{20} + x_9x_{21} + x_9x_{22} + x_{10}x_{20} \\
& + x_{10}x_{21} + x_{10} + x_{11}x_{22} + x_{11}x_{23} + x_{11} \\
0 = {} & x_8x_{20} + x_8x_{21} + x_8x_{23} + x_8 + x_9x_{20} + x_9x_{23} + x_9 \\
& + x_{10}x_{23} + x_{11}x_{20} + x_{11}x_{22} + x_{11} \\
0 = {} & x_8x_{20} + x_8x_{21} + x_8x_{22} + x_9x_{20} + x_9x_{21} + x_9 + x_{10}x_{22} \\
& + x_{10}x_{23} + x_{11}x_{21} + x_{11}x_{23} + x_{11} \\
0 = {} & x_8x_{21} + x_8x_{22} + x_8x_{23} + x_9x_{20} + x_9x_{21} + x_9x_{23} + x_9 \\
& + x_{10}x_{20} + x_{10}x_{23} + x_{11}x_{23} + x_{11} \\
0 = {} & x_8x_{21} + x_8x_{23} + x_8 + x_9x_{21} + x_9x_{22} + x_9x_{23} + x_{10}x_{20} \\
& + x_{10}x_{22} + x_{10} + x_{11}x_{20} + x_{11}x_{21} + x_{11}x_{22} + x_{20} \\
& + x_{22} + x_{23} + 1 \\
0 = {} & x_8x_{20} + x_8x_{21} + x_8x_{22} + x_9x_{22} + x_9 + x_{10}x_{20} + x_{10}x_{21} \\
& + x_{10}x_{23} + x_{10} + x_{11}x_{21} + x_{11} + x_{20} + x_{21} + x_{23} + 1 \\
0 = {} & x_8x_{20} + x_8x_{22} + x_8 + x_9x_{20} + x_9x_{21} + x_9x_{22} + x_{10}x_{22} \\
& + x_{10} + x_{11}x_{20} + x_{11}x_{21} + x_{11}x_{23} + x_{11} + x_{20} + x_{21} + x_{22} \\
0 = {} & x_8x_{21} + x_8x_{22} + x_8x_{23} + x_9x_{20} + x_9x_{22} + x_9 + x_{10}x_{20} \\
& + x_{10}x_{21} + x_{10}x_{22} + x_{11}x_{22} + x_{11} + x_{21} + x_{22} + x_{23}
\end{aligned}$$

Key schedule equations: linear part

$$\begin{aligned}
0 &= x_0 + x_8 + x_{16} + x_{24} \\
0 &= x_1 + x_9 + x_{17} + x_{25} + 1 \\
0 &= x_2 + x_{10} + x_{18} + x_{26} \\
0 &= x_3 + x_{11} + x_{19} + x_{27} \\
0 &= x_4 + x_{12} + x_{20} + x_{28}
\end{aligned}$$

$$
\begin{aligned}
0 &= x_5 + x_{13} + x_{21} + x_{29}\\
0 &= x_6 + x_{14} + x_{22} + x_{30}\\
0 &= x_7 + x_{15} + x_{23} + x_{31}
\end{aligned}
$$

## 14.5 State variables

$x_{32}, x_{33}, x_{34}, x_{35}, x_{36}, x_{37}, x_{38}, x_{39}, x_{40}, x_{41}, x_{42}, x_{43}, x_{44}, x_{45}, x_{46}, x_{47}, x_{48}, x_{49}, x_{50}, x_{51}, x_{52}, x_{53}, x_{54}, x_{55}, x_{56}, x_{57}, x_{58}, x_{59}, x_{60}, x_{61}, x_{62}, x_{63}, x_{64}, x_{65}, x_{66}, x_{67}, x_{68}, x_{69}, x_{70}, x_{71}, x_{72}, x_{73}, x_{74}, x_{75}, x_{76}, x_{77}, x_{78}, x_{79}$

## 14.6 State variables outlay

Inputs to the four S-boxes of the state

$$
\begin{gathered}
x_{32}, x_{33}, x_{34}, x_{35}\\
x_{36}, x_{37}, x_{38}, x_{39}\\
x_{40}, x_{41}, x_{42}, x_{43}\\
x_{44}, x_{45}, x_{46}, x_{47}
\end{gathered}
$$

Outputs from the four S-boxes of the state

$$
\begin{gathered}
x_{48}, x_{49}, x_{50}, x_{51}\\
x_{52}, x_{53}, x_{54}, x_{55}\\
x_{56}, x_{57}, x_{58}, x_{59}\\
x_{60}, x_{61}, x_{62}, x_{63}
\end{gathered}
$$

Outputs from the round (inputs to the S-boxes of the next round)

$$
\begin{gathered}
x_{64}, x_{65}, x_{66}, x_{67}\\
x_{68}, x_{69}, x_{70}, x_{71}\\
x_{72}, x_{73}, x_{74}, x_{75}\\
x_{76}, x_{77}, x_{78}, x_{79}
\end{gathered}
$$

## 14.7 Cipher Equations

Cipher equations: S-box 0

$$
\begin{aligned}
0 &= x_{32}x_{48} + x_{32}x_{49} + x_{32}x_{51} + x_{32} + x_{33}x_{48} + x_{33}x_{49} + x_{33}\\
&\quad + x_{34}x_{48} + x_{34}x_{51} + x_{35}x_{50} + x_{35}x_{51} + x_{35}\\
0 &= x_{32}x_{48} + x_{32}x_{49} + x_{32}x_{50} + x_{33}x_{48} + x_{33}x_{49} + x_{33}x_{51}\\
&\quad + x_{33} + x_{34}x_{48} + x_{34}x_{49} + x_{34} + x_{35}x_{48} + x_{35}x_{51}\\
0 &= x_{32}x_{49} + x_{32}x_{50} + x_{32}x_{51} + x_{33}x_{48} + x_{33}x_{49} + x_{33}x_{50}\\
&\quad + x_{34}x_{48} + x_{34}x_{49} + x_{34}x_{51} + x_{34} + x_{35}x_{48}\\
&\quad + x_{35}x_{49} + x_{35}\\
0 &= x_{32}x_{48} + x_{32}x_{50} + x_{32}x_{51} + x_{33}x_{48} + x_{33}x_{49} + x_{33}x_{50}\\
&\quad + x_{34}x_{48} + x_{34}x_{49} + x_{34} + x_{35}x_{50} + x_{35}x_{51} + x_{35}\\
0 &= x_{32}x_{48} + x_{32}x_{49} + x_{32}x_{51} + x_{32} + x_{33}x_{48} + x_{33}x_{51} + x_{33}\\
&\quad + x_{34}x_{51} + x_{35}x_{48} + x_{35}x_{50} + x_{35}\\
0 &= x_{32}x_{48} + x_{32}x_{49} + x_{32}x_{50} + x_{33}x_{48} + x_{33}x_{49} + x_{33}\\
&\quad + x_{34}x_{50} + x_{34}x_{51} + x_{35}x_{49} + x_{35}x_{51} + x_{35}\\
0 &= x_{32}x_{49} + x_{32}x_{50} + x_{32}x_{51} + x_{33}x_{48} + x_{33}x_{49} + x_{33}x_{51}\\
&\quad + x_{33} + x_{34}x_{48} + x_{34}x_{51} + x_{35}x_{51} + x_{35}\\
0 &= x_{32}x_{49} + x_{32}x_{51} + x_{32} + x_{33}x_{49} + x_{33}x_{50} + x_{33}x_{51}\\
&\quad + x_{34}x_{48} + x_{34}x_{50} + x_{34} + x_{35}x_{48} + x_{35}x_{49} + x_{35}x_{50}\\
&\quad + x_{48} + x_{50} + x_{51} + 1\\
0 &= x_{32}x_{48} + x_{32}x_{49} + x_{32}x_{50} + x_{33}x_{50} + x_{33} + x_{34}x_{48}\\
&\quad + x_{34}x_{49} + x_{34}x_{51} + x_{34} + x_{35}x_{49} + x_{35} + x_{48}\\
&\quad + x_{49} + x_{51} + 1\\
0 &= x_{32}x_{48} + x_{32}x_{50} + x_{32} + x_{33}x_{48} + x_{33}x_{49} + x_{33}x_{50}\\
&\quad + x_{34}x_{50} + x_{34} + x_{35}x_{48} + x_{35}x_{49} + x_{35}x_{51} + x_{35}\\
&\quad + x_{48} + x_{49} + x_{50}\\
0 &= x_{32}x_{49} + x_{32}x_{50} + x_{32}x_{51} + x_{33}x_{48} + x_{33}x_{50} + x_{33}\\
&\quad + x_{34}x_{48} + x_{34}x_{49} + x_{34}x_{50} + x_{35}x_{50}\\
&\quad + x_{35} + x_{49} + x_{50} + x_{51}
\end{aligned}
$$

Cipher equations: S-box 1

$$
\begin{aligned}
0 &= x_{36}x_{52} + x_{36}x_{53} + x_{36}x_{55} + x_{36} + x_{37}x_{52} + x_{37}x_{53} + x_{37}\\
&\quad + x_{38}x_{52} + x_{38}x_{55} + x_{39}x_{54} + x_{39}x_{55} + x_{39}\\
0 &= x_{36}x_{52} + x_{36}x_{53} + x_{36}x_{54} + x_{37}x_{52} + x_{37}x_{53} + x_{37}x_{55}\\
&\quad + x_{37} + x_{38}x_{52} + x_{38}x_{53} + x_{38} + x_{39}x_{52} + x_{39}x_{55}\\
0 &= x_{36}x_{53} + x_{36}x_{54} + x_{36}x_{55} + x_{37}x_{52} + x_{37}x_{53} + x_{37}x_{54}\\
&\quad + x_{38}x_{52} + x_{38}x_{53} + x_{38}x_{55} + x_{38} + x_{39}x_{52} + x_{39}x_{53} + x_{39}\\
0 &= x_{36}x_{52} + x_{36}x_{54} + x_{36}x_{55} + x_{37}x_{52} + x_{37}x_{53} + x_{37}x_{54}\\
&\quad + x_{38}x_{52} + x_{38}x_{53} + x_{38} + x_{39}x_{54} + x_{39}x_{55} + x_{39}\\
0 &= x_{36}x_{52} + x_{36}x_{53} + x_{36}x_{55} + x_{36} + x_{37}x_{52} + x_{37}x_{55} + x_{37}\\
&\quad + x_{38}x_{55} + x_{39}x_{52} + x_{39}x_{54} + x_{39}\\
0 &= x_{36}x_{52} + x_{36}x_{53} + x_{36}x_{54} + x_{37}x_{52} + x_{37}x_{53} + x_{37}\\
&\quad + x_{38}x_{54} + x_{38}x_{55} + x_{39}x_{53} + x_{39}x_{55} + x_{39}\\
0 &= x_{36}x_{53} + x_{36}x_{54} + x_{36}x_{55} + x_{37}x_{52} + x_{37}x_{53} + x_{37}x_{55}\\
&\quad + x_{37} + x_{38}x_{52} + x_{38}x_{55} + x_{39}x_{55} + x_{39}\\
0 &= x_{36}x_{53} + x_{36}x_{55} + x_{36} + x_{37}x_{53} + x_{37}x_{54} + x_{37}x_{55}\\
&\quad + x_{38}x_{52} + x_{38}x_{54} + x_{38} + x_{39}x_{52}\\
&\quad + x_{39}x_{53} + x_{39}x_{54} + x_{52} + x_{54} + x_{55} + 1\\
0 &= x_{36}x_{52} + x_{36}x_{53} + x_{36}x_{54} + x_{37}x_{54} + x_{37} + x_{38}x_{52} + x_{38}\\
&\quad \times x_{53} + x_{38}x_{55} + x_{38} + x_{39}x_{53} + x_{39} + x_{52} + x_{53} + x_{55} + 1\\
0 &= x_{36}x_{52} + x_{36}x_{54} + x_{36} + x_{37}x_{52} + x_{37}x_{53} + x_{37}x_{54}\\
&\quad + x_{38}x_{54} + x_{38} + x_{39}x_{52} + x_{39}x_{53} + x_{39}x_{55} + x_{39}\\
&\quad + x_{52} + x_{53} + x_{54}\\
0 &= x_{36}x_{53} + x_{36}x_{54} + x_{36}x_{55} + x_{37}x_{52} + x_{37}x_{54} + x_{37} + x_{38}x_{52}\\
&\quad + x_{38}x_{53} + x_{38}x_{54} + x_{39}x_{54} + x_{39} + x_{53} + x_{54} + x_{55}
\end{aligned}
$$

doi: 10.1049/iet-ifs.2009.0118

Cipher equations: S-box 2

$$\begin{aligned}
0 &= x_{40}x_{56} + x_{40}x_{57} + x_{40}x_{59} + x_{40} + x_{41}x_{56} + x_{41}x_{57} + x_{41}\\
&\quad + x_{42}x_{56} + x_{42}x_{59} + x_{43}x_{58} + x_{43}x_{59} + x_{43}\\
0 &= x_{40}x_{56} + x_{40}x_{57} + x_{40}x_{58} + x_{41}x_{56} + x_{41}x_{57} + x_{41}x_{59}\\
&\quad + x_{41} + x_{42}x_{56} + x_{42}x_{57} + x_{42} + x_{43}x_{56} + x_{43}x_{59}\\
0 &= x_{40}x_{57} + x_{40}x_{58} + x_{40}x_{59} + x_{41}x_{56} + x_{41}x_{57} + x_{41}x_{58}\\
&\quad + x_{42}x_{56} + x_{42}x_{57} + x_{42}x_{59} + x_{42} + x_{43}x_{56} + x_{43}x_{57} + x_{43}\\
0 &= x_{40}x_{56} + x_{40}x_{58} + x_{40}x_{59} + x_{41}x_{56} + x_{41}x_{57} + x_{41}x_{58}\\
&\quad + x_{42}x_{56} + x_{42}x_{57} + x_{42} + x_{43}x_{58} + x_{43}x_{59} + x_{43}\\
0 &= x_{40}x_{56} + x_{40}x_{57} + x_{40}x_{59} + x_{40} + x_{41}x_{56} + x_{41}x_{59}\\
&\quad + x_{41} + x_{42}x_{59} + x_{43}x_{56} + x_{43}x_{58} + x_{43}\\
0 &= x_{40}x_{56} + x_{40}x_{57} + x_{40}x_{58} + x_{41}x_{56} + x_{41}x_{57}\\
&\quad + x_{41} + x_{42}x_{58} + x_{42}x_{59} + x_{43}x_{57} + x_{43}x_{59} + x_{43}\\
0 &= x_{40}x_{57} + x_{40}x_{58} + x_{40}x_{59} + x_{41}x_{56} + x_{41}x_{57}\\
&\quad + x_{41}x_{59} + x_{41} + x_{42}x_{56} + x_{42}x_{59} + x_{43}x_{59} + x_{43}\\
0 &= x_{40}x_{57} + x_{40}x_{59} + x_{40} + x_{41}x_{57} + x_{41}x_{58} + x_{41}x_{59}\\
&\quad + x_{42}x_{56} + x_{42}x_{58} + x_{42} + x_{43}x_{56} + x_{43}x_{57}\\
&\quad + x_{43}x_{58} + x_{56} + x_{58} + x_{59} + 1\\
0 &= x_{40}x_{56} + x_{40}x_{57} + x_{40}x_{58} + x_{41}x_{58} + x_{41}\\
&\quad + x_{42}x_{56} + x_{42}x_{57} + x_{42}x_{59} + x_{42} + x_{43}x_{57} + x_{43}\\
&\quad + x_{56} + x_{57} + x_{59} + 1\\
0 &= x_{40}x_{56} + x_{40}x_{58} + x_{40} + x_{41}x_{56} + x_{41}x_{57} + x_{41}x_{58}\\
&\quad + x_{42}x_{58} + x_{42} + x_{43}x_{56} + x_{43}x_{57} + x_{43}x_{59} + x_{43} + x_{56}\\
&\quad + x_{57} + x_{58}\\
0 &= x_{40}x_{57} + x_{40}x_{58} + x_{40}x_{59} + x_{41}x_{56} + x_{41}x_{58} + x_{41}\\
&\quad + x_{42}x_{56} + x_{42}x_{57} + x_{42}x_{58}\\
&\quad + x_{43}x_{58} + x_{43} + x_{57} + x_{58} + x_{59}
\end{aligned}$$

Cipher equations: S-box 3

$$\begin{aligned}
0 &= x_{44}x_{60} + x_{44}x_{61} + x_{44}x_{63} + x_{44} + x_{45}x_{60} + x_{45}x_{61} + x_{45}\\
&\quad + x_{46}x_{60} + x_{46}x_{63} + x_{47}x_{62} + x_{47}x_{63} + x_{47}\\
0 &= x_{44}x_{60} + x_{44}x_{61} + x_{44}x_{62} + x_{45}x_{60} + x_{45}x_{61} + x_{45}x_{63}\\
&\quad + x_{45} + x_{46}x_{60} + x_{46}x_{61} + x_{46} + x_{47}x_{60} + x_{47}x_{63}\\
0 &= x_{44}x_{61} + x_{44}x_{62} + x_{44}x_{63} + x_{45}x_{60} + x_{45}x_{61} + x_{45}x_{62}\\
&\quad + x_{46}x_{60} + x_{46}x_{61} + x_{46}x_{63} + x_{46} + x_{47}x_{60} + x_{47}x_{61} + x_{47}\\
0 &= x_{44}x_{60} + x_{44}x_{62} + x_{44}x_{63} + x_{45}x_{60} + x_{45}x_{61} + x_{45}x_{62}\\
&\quad + x_{46}x_{60} + x_{46}x_{61} + x_{46} + x_{47}x_{62} + x_{47}x_{63} + x_{47}\\
0 &= x_{44}x_{60} + x_{44}x_{61} + x_{44}x_{63} + x_{44} + x_{45}x_{60} + x_{45}x_{63} + x_{45}\\
&\quad + x_{46}x_{63} + x_{47}x_{60} + x_{47}x_{62} + x_{47}\\
0 &= x_{44}x_{60} + x_{44}x_{61} + x_{44}x_{62} + x_{45}x_{60} + x_{45}x_{61} + x_{45}\\
&\quad + x_{46}x_{62} + x_{46}x_{63} + x_{47}x_{61} + x_{47}x_{63} + x_{47}\\
0 &= x_{44}x_{61} + x_{44}x_{62} + x_{44}x_{63} + x_{45}x_{60} + x_{45}x_{61} + x_{45}x_{63}\\
&\quad + x_{45} + x_{46}x_{60} + x_{46}x_{63} + x_{47}x_{63} + x_{47}\\
0 &= x_{44}x_{61} + x_{44}x_{63} + x_{44} + x_{45}x_{61}\\
&\quad + x_{45}x_{62} + x_{45}x_{63} + x_{46}x_{60} + x_{46}x_{62} + x_{46}\\
&\quad + x_{47}x_{60} + x_{47}x_{61} + x_{47}x_{62} + x_{60} + x_{62} + x_{63} + 1\\
0 &= x_{44}x_{60} + x_{44}x_{61} + x_{44}x_{62} + x_{45}x_{62} + x_{45} + x_{46}x_{60}\\
&\quad + x_{46}x_{61} + x_{46}x_{63} + x_{46} + x_{47}x_{61} + x_{47} + x_{60} + x_{61}\\
&\quad + x_{63} + 1\\
0 &= x_{44}x_{60} + x_{44}x_{62} + x_{44} + x_{45}x_{60} + x_{45}x_{61} + x_{45}x_{62}\\
&\quad + x_{46}x_{62} + x_{46} + x_{47}x_{60} + x_{47}x_{61} + x_{47}x_{63} + x_{47} + x_{60}\\
&\quad + x_{61} + x_{62}\\
0 &= x_{44}x_{61} + x_{44}x_{62} + x_{44}x_{63} + x_{45}x_{60}\\
&\quad + x_{45}x_{62} + x_{45} + x_{46}x_{60}\\
&\quad + x_{46}x_{61} + x_{46}x_{62} + x_{47}x_{62}\\
&\quad + x_{47} + x_{61} + x_{62} + x_{63}
\end{aligned}$$

Cipher equations: linear part

$$\begin{aligned}
0 &= x_0 + x_{16} + x_{48} + x_{51} + x_{63} + x_{64}\\
0 &= x_1 + x_{17} + x_{48} + x_{49} + x_{51} + x_{60} + x_{63} + x_{65} + 1\\
0 &= x_2 + x_{18} + x_{49} + x_{50} + x_{61} + x_{66}\\
0 &= x_3 + x_{19} + x_{50} + x_{51} + x_{62} + x_{67}\\
0 &= x_4 + x_{20} + x_{52} + x_{55} + x_{59} + x_{68}\\
0 &= x_5 + x_{21} + x_{52} + x_{53} + x_{55} + x_{56} + x_{59} + x_{69}\\
0 &= x_6 + x_{22} + x_{53} + x_{54} + x_{57} + x_{70}\\
0 &= x_7 + x_{23} + x_{54} + x_{55} + x_{58} + x_{71}\\
0 &= x_{24} + x_{51} + x_{60} + x_{63} + x_{72}\\
0 &= x_{25} + x_{48} + x_{51} + x_{60} + x_{61} + x_{63} + x_{73}\\
0 &= x_{26} + x_{49} + x_{61} + x_{62} + x_{74}\\
0 &= x_{27} + x_{50} + x_{62} + x_{63} + x_{75}\\
0 &= x_{28} + x_{55} + x_{56} + x_{59} + x_{76}\\
0 &= x_{29} + x_{52} + x_{55} + x_{56} + x_{57} + x_{59} + x_{77}\\
0 &= x_{30} + x_{53} + x_{57} + x_{58} + x_{78}\\
0 &= x_{31} + x_{54} + x_{58} + x_{59} + x_{79}
\end{aligned}$$

## 14.8 Leak equations

Leak equations after round 0

$$\begin{aligned}
0 &= x_{32}\\
0 &= x_{33} + 1\\
0 &= x_{34}\\
0 &= x_{35} + 1
\end{aligned}$$

S-box output equations from the leak after round 0

$$\begin{aligned}
0 &= x_{48} + 1\\
0 &= x_{49} + 1\\
0 &= x_{50} + 1\\
0 &= x_{51} + 1
\end{aligned}$$

Leak equations after round 1

$$\begin{aligned}
0 &= x_{64} + 1\\
0 &= x_{65} + 1\\
0 &= x_{66}\\
0 &= x_{67} + 1
\end{aligned}$$