On Linear Hulls and Trails

Tomer Ashur and Vincent Rijmen

Dept. Electrical Engineering, ESAT/COSIC, KU Leuven, and iMinds, Belgium
[tomer.ashur,vincent.rijmen] @ esat.kuleuven.be

Abstract. This paper improves the understanding of linear cryptanalysis by highlighting some previously overlooked aspects. It shows that linear hulls are sometimes formed already in a single round, and that overlooking such hulls may lead to a wrong estimation of the linear correlation, and thus of the data complexity. It shows how correlation matrices can be used to avoid this, and provides a tutorial on how to use them properly. By separating the input and output masks from the key mask it refines the formulas for computing the expected correlation and the expected linear potential. Finally, it shows that when the correlation of a hull is not properly estimated (e.g., by using the correlation of a single trail as the correlation of the hull), the success probability of Matsui's Algorithm 1 drops, sometimes drastically. It also shows that when the trails composing the hull are properly accounted for, more than a single key bit can be recovered using Algorithm 1. All the ideas presented in this paper are followed by examples comparing previous methods to the corrected ones, and verified experimentally with reduced-round versions of Simon32/64.

Keywords: Linear cryptanalysis, linear hulls, Simon

1 Introduction

Linear cryptanalysis is introduced by Matsui and applied to DES in [10]. The formalism of linear cryptanalysis is extended in [3, 5, 12]. These works emphasise the similarity with the formalism for differential cryptanalysis that existed before. The *linear hull* is introduced as the counterpart of a differential. It is often used to prove the security of block ciphers against cryptanalysis, e.g. in [9]. A critical study of the *linear hull effect* is presented in [11]. A different framework for linear cryptanalysis, called *correlation matrices*, is introduced in [6].

In this paper, we revisit [6] and apply it to the block cipher Simon reduced to 3 rounds. Firstly, Simon's simple structure allows to construct simple and illustrative examples to highlight the similarities and differences between the two formalisms for linear cryptanalysis in practice. Secondly, the structure of Simon is sufficiently different from other mainstream ciphers to highlight the impact of some theoretical observations.

In Section 3 we follow the 'classical' formalism and show that the round function of Simon exhibits one-round hulls. In Section 4 we repeat the analysis using correlation matrices and illustrate that these matrices can facilitate the automatic analysis of ciphers, even when one-round hulls exist.

In Section 5 we present our first theoretical observation. We use the theoretical contributions of [6] to discuss the validity of a popular method to compute the *potential* of a linear hull.

In Section 6 we present our second theoretical observation. When several trails with correlation contributions of comparable magnitude and different signs exist, the performance of Matsui's Algorithm 1 strongly depends on the values of some roundkey bits. When this dependency is taken into account, the algorithm can be extended to recover multiple roundkey bits [13]. When this fact is neglected, the average success rate of Algorithm 1 drops, sometimes dramatically. Furthermore, we show a case where increasing the number of known plaintexts beyond a certain value, leads to a *decrease* in the success probability of the attack.

2 Notation and terminology

In this section, we recall some definitions and terminology of linear cryptanalysis [3, 5, 6, 9, 10, 12].

2.1 Boolean functions

We denote the field with two elements by GF(2) and the vector space of dimension n over this field by $\mathrm{GF}(2)^n$. We use $+$ to denote addition in some field. The field in which the addition is made is always clear from the context.

A boolean function $y = f(x)$ is a function $f : \mathrm{GF}(2)^n \to \mathrm{GF}(2)$ mapping a vector of size n with binary components into a single bit. A boolean vector function $y = F(x)$ is a function $F : \mathrm{GF}(2)^n \to \mathrm{GF}(2)^m$ that maps a binary vector of size n into a binary vector of size m. A permutation is an invertible boolean vector function. A boolean vector function $y = F(x)$ with output size m can be viewed as the parallel execution of m boolean functions such that $y_i = F_i(x)$ where $0 \leq i \leq m-1$ denotes the bit position.

A keyed boolean vector function $y = F(x,k) = F_k(x)$ is a family of boolean vector functions, indexed by a key k. An iterative block cipher with r rounds is a composition of r permutations $F_{k_{r-1}} \circ F_{k_{r-2}} \circ \ldots \circ F_{k_0}(x)$. Observe that many r-round ciphers contain in fact a reduced extra round, consisting only of an extra key addition. We will ignore this. In this paper we will assume that the roundkeys k_i are independent. Hence the key of a block cipher, denoted by k, is defined as the vector consisting of the concatenation of the r roundkeys k_i.

2.2 Masks and approximations

Let a, b be two vectors of size n. Then $a^t x = \sum_{i=0}^{n-1} a_i \cdot x_i$. We will call a the mask of x. In practical examples, the masks will often contain many zero bits. In order to emphasize which bits are nonzero, we will sometimes use the following set notation:

$$a = \{i_1, i_2, \ldots, i_u\} \Leftrightarrow \begin{cases} a_j = 1, \forall j \in \{i_1, i_2, \ldots, i_u\} \\ a_j = 0, \forall j \notin \{i_1, i_2, \ldots, i_u\} \end{cases}$$

Using this notation, the addition (XOR) of two masks corresponds to the symmetric difference operation on the sets.

A linear approximation for a keyed boolean permutation is a tuple (a, b, c) such that a, b and c are masks for the input, the output and the key, respectively. Let p be the fraction of inputs x for which the equation $a^t x + b^t F_k(x) + c^t k = 0$ holds. The correlation of the linear approximation (a, b, c) is defined as $\mathrm{cor}(a, b, c) = 2 \cdot (p - \frac{1}{2}) = 2p - 1$. In general, both p and $\mathrm{cor}(a, b, c)$ will depend on the value of k. When $c = 0$, we abbreviate the notation $(a, b, 0)$ and $\mathrm{cor}(a, b, 0)$ to (a, b) and $\mathrm{cor}(a, b)$.

2.3 Linear hulls and trails

A (linear) trail Ω covering r rounds of an iterative block cipher is a concatenation of linear approximations each covering a single round such that the output mask of round i equals the input mask of round $i + 1$. Hence we can identify the trail with a vector of $r + 1$ masks $\omega_i, 0 \leq i \leq r$ $\Omega = (\omega_0, \omega_1, \ldots, \omega_r)$. Round i has input mask ω_i and output mask ω_{i+1}. The correlation contribution of a trail Ω is the product of the correlations of the individual rounds: $\mathrm{cor_p}(\Omega) = \prod_{i=0}^{r-1} \mathrm{cor_{round}}\ _i(\omega_i, \omega_{i+1})$. In a key-alternating cipher the round consists of a fixed part g followed by an addition with the round key. We can write:

$$\mathrm{cor_{round}}\ _i(\omega_i, \omega_{i+1}) = (-1)^{\omega_i^t k_i} \mathrm{cor}_g(\omega_i, \omega_{i+1}). \tag{1}$$

Note, however, that this notation implicitly assumes that to each bit of the round input a different bit of the roundkey is added . We will say more on this in Section 5.3. We obtain:

$$\mathrm{cor_p}(\Omega) = \prod_i (-1)^{\omega_i^t k_i} \mathrm{cor}_g(\omega_i, \omega_{i+1}) = |\mathrm{cor_p}(\Omega)| \cdot (-1)^{d_\Omega + \sum_i \omega_i^t k_i}, \tag{2}$$

with $d_\Omega = 1$ if $\prod_i \mathrm{cor}_g(\omega_i, \omega_{i+1})$ is negative; otherwise $d_\Omega = 0$.

A linear hull covering r rounds of a block cipher is a tuple (α, β). The hull is composed of a set of linear trails all having the same input mask and output mask but that can differ in the intermediate masks. The correlation of a linear hull is

$$\mathrm{cor}(\alpha, \beta) = \sum_{\substack{\Omega \\ \omega_0 = \alpha, \omega_r = \beta}} \mathrm{cor_p}(\Omega) \tag{3}$$

3 One-round hulls in Simon

In this section, we briefly recall the definition of Simon's round function. We prove the existence of one-round hulls, which impact the computation of correlations of multi-round hulls.

3.1 Simon

Simon is a family of lightweight block ciphers designed by the US National Security Agency and published in 2013 [2]. The Simon$2n/mn$ family of lightweight block ciphers has 10 members differing in the block and key sizes. All members of the family have a Feistel structure with round function R employing a non-linear function f. In each round i, R receives two n-bit input words X^i and Y^i, and outputs two n-bit words X^{i+1} and Y^{i+1}. The round function uses three operations: addition in GF$(2)^n$, bitwise AND, and a left circular shift by j positions, which we denote by $+, \&$, and $\lll j$, respectively. The internal non-linear function f is defined as:

$$f(X^i) = [(X^i \lll 1) \& (X^i \lll 8)] + (X^i \lll 2).$$

The output of the round function R on input block (X^i, Y^i) is: $R^i(X^i, Y^i) = (Y^i + f(X^i) + k^i, X^i)$, where i is the round number. The entire cipher is $R^{r-1} \circ R^{r-2} \circ \ldots \circ R^0(X^0, Y^0)$. The structure of the round function of Simon is depicted in Fig. 1.

3.2 Linear hulls and trails through one round of Simon

We use the notation (a, b, c, d, e) to describe a linear trail through one round of Simon. Here a and b denote the left and right input masks; c and d denote the masks at the outputs of the two topmost rotations; e and b denote the left and right output masks (before the swap operation), cf. Fig. 1.

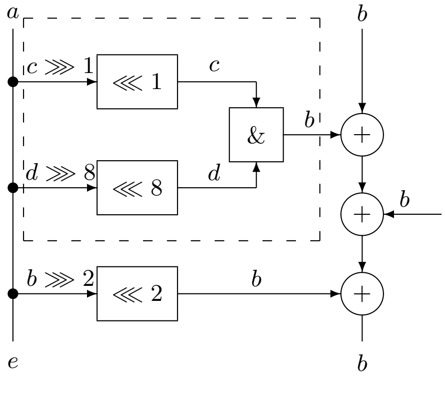

Fig. 1. Trail through one round of Simon (without the final swap operation). The dashed box indicates the part of the round that we discuss in Section 4.

We now study the behavior of linear trails over one round of Simon using the rules of propagation of linear trails introduced in [3, 5]. The rule for trail propagation over the branch operation implies the following constraint on a, b, c, d, e:

$$a + e = (b \ggg 2) + (c \ggg 1) + (d \ggg 8) \tag{4}$$

Note that the rule for trail propagation over the addition operation is already implicit in the way we propagate the b mask through Fig. 1. The output bit z of a bitwise AND operation $z = x$ AND y is correlated to the 4 linear functions of the two input bits:

$$\mathrm{cor}(z, 0) = \mathrm{cor}(z, x) = \mathrm{cor}(z, y) = 1/2,\ \mathrm{cor}(z, x + y) = -1/2.$$

It follows that the AND operation in Simon leads to the following constraints on b, c, d: if a bit in c or d is set, then the bit in b at the corresponding position needs to be set. This translates to:

$$\bar{c} \text{ OR } b = 1 \tag{5}$$

$$\bar{d} \text{ OR } b = 1 \tag{6}$$

The following lemma expresses that some one-round trails come in groups.

Lemma 1. *Let* (a, b, c, d, e) *be a one-round trail over Simon. If there exists an index* i *such that* $b_i = b_{i+7} = 1$*, then the trail* (a, b, c, d, e) *satisfies the constraints* (4)–(6) *if and only if the trail* $(a, b, c + (1 \lll i), d + (1 \lll (i + 7)), e)$ *satisfies the constraints* (4)–(6)*.*

Proof. For constraint (4) we have:

$$\begin{aligned} &((c + (1 \lll i)) \ggg 1) + ((d + (1 \lll (i + 7))) \ggg 8) \\ &\qquad = (c \ggg 1) + (1 \lll (i - 1)) + (d \ggg 8) + (1 \lll (i + 7 - 8)) \\ &\qquad = (c \ggg 1) + (d \ggg 8) \end{aligned}$$

Hence both satisfy (4) or neither does. For constraint (5) we see that if bit i of b is set, then the value of c at position i does not matter. Hence both c and $c + (1 \lll i)$ satisfy (5), or they both don't satisfy (5). Similar for constraint (6) and $d + (1 \lll (i + 7))$. □

Since the trails in Lemma 1 have the same input masks (a, b) and the same output masks (e, b), they are in the same one-round linear hull. Fig. 2–Fig. 4 each show two trails derived from one another by means of Lemma 1. Notice that in each set both trails select exactly the same bits of the roundkeys.

3.3 Correlations and correlation contributions

We now want to compute the correlation contributions of the trails of Fig. 2–Fig. 4. The usual rule is to assume that all nonlinear functions act independently and to multiply all the correlations. This results in the following values for the

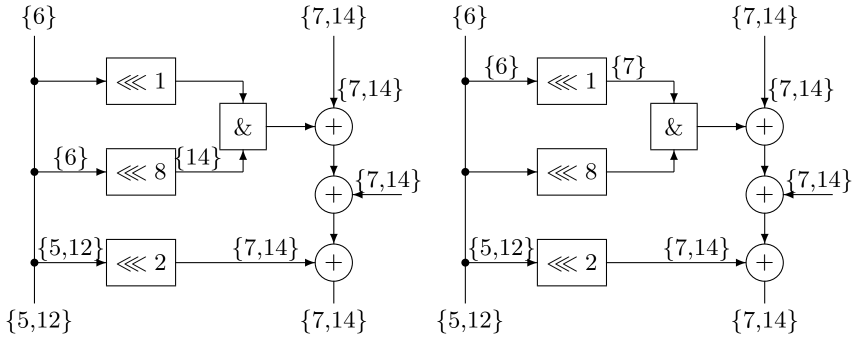

Fig. 2. Two trails of a one-round hull.

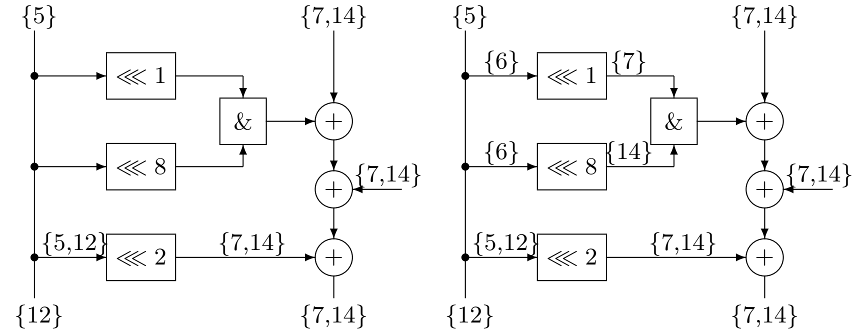

Fig. 3. Two trails of a second one-round hull.

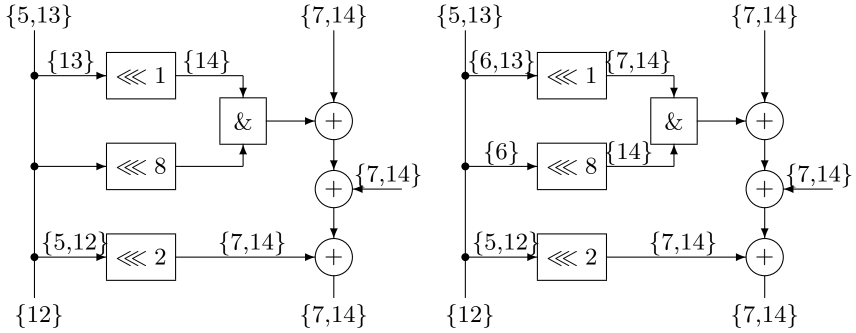

Fig. 4. Two trails of a third one-round hull. The trails have nonzero contributions of the same magnitude and opposite sign. The hull has correlation zero.

correlation contributions of the six trails:

	c	d	cor
Fig. 2	$\varnothing$	$\{14\}$	2^{-2}
	$\{7\}$	$\varnothing$	2^{-2}
Fig. 3	$\varnothing$	$\varnothing$	2^{-2}
	$\{7\}$	$\{14\}$	2^{-2}
Fig. 4	$\{14\}$	$\varnothing$	2^{-2}
	$\{7, 14\}$	$\{14\}$	-2^{-2}

In each case by adding the correlation contributions of the two trails we obtain the correct correlation of the hull. However, starting from the observation that when $b_i = b_{i+7} = 1$, there are pairs of AND gates that share one input bit, we can follow a different approach. Let

$$s = x \text{ AND } y,\ t = y \text{ AND } z$$

Then we have

$$s + t = y \text{ AND } (x + z),$$

which implies the following:

$$\begin{aligned} \operatorname{cor}(s+t, x+z) = \operatorname{cor}(s+t, 0) = \operatorname{cor}(s+t, y) &= 1/2 \\ \operatorname{cor}(s+t, x+y+z) &= -1/2 \\ \operatorname{cor}(s+t, x+y) = \operatorname{cor}(s+t, y+z) &= 0 \\ \operatorname{cor}(s+t, x) = \operatorname{cor}(s+t, z) &= 0 \end{aligned}$$

These values can be used to derive immediately the exact correlations of the linear hulls of Fig. 2–Fig. 4. Observe that the linear hull of Fig. 4 has correlation zero, while both trails have a nonzero correlation contribution. Hence, mounting an attack and using the correlation contribution of a trail as an estimate for the correlation of this linear hull will likely lead to wrong results.

4 Correlation matrices

In this section, we follow the alternative approach of [6] to compute correlations and correlation contributions.

4.1 Correlation matrix for Simon

In order not to repeat too much from the previous approach, we concentrate on the most interesting part of the round function: the AND function combined with the preceding expanding linear function $\operatorname{lin}(x) = (x \lll 1, x \lll 8)$. This part is indicated by a dashed box in Fig. 1. The correlation matrix of a map f is defined as follows:

Definition 1 (Correlation matrix [6]).

$$\mathbf{C}^f_{uw} := \mathrm{cor}(u^t f(x), w^t x)$$

For a linear map $y = \mathbf{M}x$, we have: $\mathbf{C}_{uw} = \delta(\mathbf{M}^t u + w)$, where δ is the Kronecker-delta function (which is defined by $\delta(0) = 1$ and $\delta(x) = 0, \forall x \neq 0$). This gives for $\mathrm{lin}(x)$:

$$\mathbf{C}^{\mathrm{lin}}_{uv,w} = \delta(w + (u \ggg 1) + (v \ggg 8)),$$

where we denote the row index of $\mathbf{C}^{\mathrm{lin}}$ by uv in order to make it more clear from the notation this is an expansion function, and hence, the row index of the matrix (i.e., the output) is twice as long as the column index.

The correlation matrix for a 1-bit AND operation $z = x$ AND y is given by:

$$\mathbf{C}^{\mathrm{A}} = \begin{bmatrix} \mathrm{cor}(0,0) & \mathrm{cor}(0,x) & \mathrm{cor}(0,y) & \mathrm{cor}(0,x+y) \\ \mathrm{cor}(z,0) & \mathrm{cor}(z,x) & \mathrm{cor}(z,y) & \mathrm{cor}(z,x+y) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{bmatrix}$$

We can express the matrix elements by means of the following formula:

$$\mathbf{C}^{\mathrm{A}}_{a,bc} = (1-a)(1-b)(1-c) + \frac{1}{2}a(-1)^{bc}$$

The 16-bit parallel AND operation is a special case of the boxed map discussed in [6]. Hence, we obtain:

$$\mathbf{C}^{\mathrm{AND}}_{a,bc} = \prod_i \mathbf{C}^{\mathrm{A}}_{a_i,b_ic_i} = \prod_i \left((1-a_i)(1-b_i)(1-c_i) + \frac{1}{2}a_i(-1)^{b_ic_i} \right)$$

In order to compute the correlation matrix for a combined map, we only have to multiply the correlation matrices of its components [6]:

$$\mathbf{C}^{f_2 \circ f_1} = \mathbf{C}^{f_2} \times \mathbf{C}^{f_1}$$

For the combination of $\mathrm{lin}(x)$ and AND, we obtain:

$$\begin{aligned} \mathbf{C}_{u,w} &= \sum_{xy} \mathbf{C}^{\mathrm{AND}}_{u,xy} \mathbf{C}^{\mathrm{lin}}_{xy,w} \\ &= \sum_{xy} \prod_i \left((1-u_i)(1-x_i)(1-y_i) + \frac{1}{2}u_i(-1)^{x_iy_i} \right) \delta(w + (x \ggg 1) + (y \ggg 8)) \end{aligned}$$

The δ-function is nonzero only when $y = (w \lll 8) + (x \lll 7)$. Hence, we obtain:

$$\mathbf{C}_{u,w} = \sum_x \prod_i \left((1-u_i)(1-x_i)(1-(w_{i-8} + x_{i-7})) + \frac{1}{2}u_i(-1)^{x_i(w_{i-8}+x_{i-7})} \right) \tag{7}$$

4.2 Examples

We now apply (7) to compute the correlations and correlation contributions of the linear hulls, respectively trails, shown in Fig. 2–4. Remember that we consider only the combination of the linear map lin and the AND operation. We denote the input mask for this combined map by w and the output mask by u. They are related as follows to the masks (a, b, c, d, e) defining a trail over one round, cf. Fig. 1:

$$\begin{aligned} w &= a + e + (b \ggg 2) \\ u &= b \end{aligned}$$

The hull of Fig. 2 has input $w = \{6\} = 0040_{\mathrm{x}}$ and output $u = \{7, 14\} = 4080_{\mathrm{x}}$. Filling out these values in (7), we obtain

$$\mathbf{C}_{4080,0040} = \sum_x \prod_{i=7,14} \left(\frac{1}{2}(-1)^{x_i(w_{i-8}+x_{i-7})}\right) \prod_{i\neq 7,14} (1 - x_i)(1 - (w_{i-8} + x_{i-7})) \ .$$

From the first factor of the product on the right, we see that in order to obtain a nonzero contribution, x_i must equal 0 for all i except $i = 7, 14$. Combined with the second factor we obtain that x_7 is free and all other $x_i = 0$. Hence we obtain:

$$\begin{aligned} \mathbf{C}_{4080,0040} &= \sum_{x_7} \prod_{i=7,14} \frac{1}{2}(-1)^{x_i(w_{i-8}+x_{i-7})} \\ &= \underbrace{\frac{1}{4}(-1)^0(-1)^0}_{x_7=0,\text{trail of Fig. 2, left}} + \underbrace{\frac{1}{4}(-1)^0(-1)^0}_{x_7=1,\text{trail of Fig. 2, right}} = \frac{1}{2} \end{aligned}$$

The two terms in the sum are the correlation contributions of the two trails that are shown in Fig. 2 and that together form the one-round hull.

The hull of Fig. 3 has $w = \varnothing = 0000_{\mathrm{x}}$ and $u = \{7, 14\} = 4080_{\mathrm{x}}$. We obtain:

$$\mathbf{C}_{4080,0000} = \sum_x \prod_{i=7,14} \left(\frac{1}{2}(-1)^{x_i x_{i-7}}\right) \prod_{i\neq 7,14} (1 - x_i)(1 - x_{i-7})$$

From the product on the right, we obtain that x_7 is free and all other $x_i = 0$. Hence we obtain

$$\begin{aligned} \mathbf{C}_{4080,0000} &= \sum_{x_7} \prod_{i=7,14} \frac{1}{2}(-1)^{x_i x_{i-7}} \\ &= \underbrace{\frac{1}{4}(-1)^0(-1)^0}_{x_7=0,\text{trail of Fig. 3, left}} + \underbrace{\frac{1}{4}(-1)^0(-1)^0}_{x_7=1,\text{trail of Fig. 3, right}} = \frac{1}{2} \end{aligned}$$

The hull of Fig. 4 has $w = \{13\} = 2000_{\mathtt{x}}$ and $u = \{7, 14\} = 4080_{\mathtt{x}}$. We obtain:

$$\mathbf{C}_{4080,2000} = \sum_x \prod_{i=7,14} \left(\frac{1}{2}(-1)^{x_i(w_{i-8}+x_{i-7})}\right) \prod_{i\neq 7,14} (1 - x_i)(1 - (w_{i-8} + x_{i-7}))$$

From the product on the right, we obtain that x_7 is free, $x_{14} = 1$ and all other $x_i = 0$.

$$\begin{aligned}\mathbf{C}_{4080,2000} &= \sum_{x_7} \prod_{i=7,14} \frac{1}{2}(-1)^{x_i(w_{i-8}+x_{i-7})} \\ &= \frac{1}{4}(-1)^0(-1)^0 + \frac{1}{4}(-1)^0(-1)^1 = 0\end{aligned}$$

We see that the two trails of this hull have opposite contributions, resulting in a correlation zero for the hull.

4.3 Conclusion

As expected, this method gives the same results as the method of Section 3. However, observe that by using correlation matrices, the dependence between the inputs of the AND operation is taken care of automatically. Observe also that while the end result of this method is the correlation of the linear hull, we also obtain the correlation contributions of all the individual trails as the nonzero terms in the final sum.

5 Expected correlation and potential

Several recent works provide bounds for the security of ARX ciphers and other ciphers defined at bit-level against linear cryptanalysis by bounding the potential of linear hulls [15–17]. The bounds on the hulls are computed by summing the squares of the expected values of the correlation contributions of the linear trails, which are constructed automatically using mixed-integer linear programming (MILP) techniques.

Several of these works mention the problem that may arise in the computation of the correlation contribution of a linear trail when non-linear functions share inputs. We showed in Section 4 that correlation matrices don't have this problem.

In this section we address a second problem with the computation of the potential. Note that this problem doesn't occur for differential characteristics and differentials. It is one reason why we do not agree that differential and linear trails can be treated in exactly the same way, as is claimed e.g. in [17].

5.1 Expected correlation

For a key-alternating cipher, the expected value (over all roundkeys) of the correlation contribution of a linear trail equals

$$\mathrm{E}[\mathrm{cor_p}(\Omega)] = 0 \tag{8}$$

This follows directly by taking the expectation of (2). Intuitively, (8) might look contradictory to [10], in particular to Algorithm 1. The apparent contradiction can be solved as follows. Although [6] writes:

> *The multiple-round linear expressions described in [10] correspond with what we call linear trails.*

there is in fact a difference. The approximations of [10] are linear expressions in terms of plaintext bits, ciphertext bits and roundkey bits. In the trails of [6], the roundkey bits are left out of the expression. It follows that the expected value of the correlation contribution becomes zero. By (3) we obtain that the expected value over all roundkeys of the correlation of a linear hull is

$$\mathrm{E}[\mathrm{cor}(a,b)] = 0 \ .$$

5.2 Potential

Since the data complexity of a linear attack is inversely proportional to the square of the correlation, it is of importance to know or to bound the value $\mathrm{E}[(\mathrm{cor}(a,b))^2]$. In [12], Nyberg calls this quantity the *potential* of the linear hull, and gives the following formula to compute it:

$$\mathrm{E}[(\mathrm{cor}(a,b))^2] = \sum_{\substack{\Omega \\ \omega_0=a,\omega_r=b}} (\mathrm{cor}_{\mathrm{p}}(\Omega))^2 \tag{9}$$

The potential is also called the Expected Linear Probability (ELP). We briefly recall here the proof for (9), using our own notation. By definition of expectation, we have:

$$\mathrm{E}[(\mathrm{cor}(a,b))^2] = \frac{1}{K}\sum_k \left(\sum_{\substack{\Omega \\ \omega_0=a,\omega_r=b}} \mathrm{cor}_{\mathrm{p}}(\Omega) \right) \left(\sum_{\substack{\Omega' \\ \omega'_0=a,\omega'_r=b}} \mathrm{cor}_{\mathrm{p}}(\Omega') \right)$$

Using (2):

$$= \frac{1}{K}\sum_{\Omega}\sum_{\Omega'}\left(\sum_k (-1)^{d_\Omega + d_{\Omega'} + \sum_i (\omega_i+\omega'_i)^t k_i} |\mathrm{cor}_{\mathrm{p}}(\Omega)||\mathrm{cor}_{\mathrm{p}}(\Omega')|\right)$$

Since

$$\sum_k (-1)^{\sum_i (\omega_i+\omega'_i)^t k_i} = \begin{cases} K & \text{if } \omega_i = \omega'_i, \forall i, \\ 0 & \text{else,} \end{cases} \tag{10}$$

we have:

$$\mathrm{E}[(\mathrm{cor}(a,b))^2] = \sum_{\Omega} (\mathrm{cor}_{\mathrm{p}}(\Omega))^2 \ . \tag{11}$$

□

5.3 Additions/corrections

We will now show that if a cipher exhibits one-round hulls as described in Section 3, Formula (11) is no longer correct. The existence of one-round hulls implies that we can have more than one trail corresponding to the same linear mask of the roundkey. For example, Fig. 2–Fig. 4 each show two different trails corresponding to the same linear mask of the roundkey.

In order to explain the consequences, (1) has to be slightly rewritten, using a different notation. In fact, we need to distinguish between *trails* and *masks for the roundkey*. From now on, we use κ_i to denote the mask for the roundkey of round i, and $\mathcal{K}$ to denote the vector of roundkey masks. We use W to denote the vector of the data masks required to uniquely define the trail: $W = (w_0, w_1, \ldots, w_r)$. Note that the domain of the w_i may be larger than the domain of the κ_i. For example, in Fig. 1, the data mask w_i contains a, b, c and d, while the roundkey mask κ_i needs to contain only b.

We denote by l, respectively L, the functions mapping w_i to the corresponding κ_i, respectively W to the corresponding $\mathcal{K}$. These functions are specific to the cipher. With this notation, (1) becomes:

$$\mathrm{cor}_{\mathrm{round}\ i}(w_i, w_{i+1}) = (-1)^{\kappa_i^t k_i} \mathrm{cor}_g(w_i, w_{i+1}), \text{ with } \kappa_i = l(w_i).$$

When L is one-to-one, formula (11) applies without modifications. However, if L is a non-injective map, then the sum of (10) become nonzero as soon as $\mathcal{K} = \mathcal{K}'$, which still allows $W \neq W'$. Hence (11) becomes:

$$\mathrm{E}[(\mathrm{cor}(a,b))^2] = \sum_{\mathcal{K}} \sum_{\substack{W,W' \\ L(W)=L(W')=\mathcal{K}}} (\mathrm{cor}_{\mathrm{p}}(W))(\mathrm{cor}_{\mathrm{p}}(W')) \ .$$

Converting back, we obtain:

$$\mathrm{E}[(\mathrm{cor}(a,b))^2] = \sum_{\mathcal{K}} \left(\sum_{\substack{W \\ L(W)=\mathcal{K}}} \mathrm{cor}_{\mathrm{p}}(W) \right)^2 \tag{12}$$

Comparing (9) to (12), we see that the difference between the two values can take positive as well as negative values. In particular when there are several trails with correlation contributions of comparable magnitude, the difference can be significant. Applied to the one-round hulls of Fig. 2–Fig. 4, we get the following results:

(a,b)	$\mathrm{E}[(\mathrm{cor}(a,b))^2]$ with (9)	$\mathrm{E}[(\mathrm{cor}(a,b))^2]$ with (12)
$(\{6;7,14\},\{5,12;7,14\})$	2^{-3}	2^{-2}
$(\{5;7,14\},\{12;7,14\})$	2^{-3}	2^{-2}
$(\{5,13;7,14\},\{12;7,14\})$	2^{-3}	0

We performed practical experiments and confirmed the values in the rightmost column.

5.4 Conclusion

Finally, we would like to discuss when (12) has to be used instead of (11), or in other words: "For which ciphers is the map L from data-input masks to roundkey masks not one-to-one?" We already demonstrated that Simon is such a cipher. Also Speck and ciphers using Substitution-Permutation-Substitution (SPS) round functions like Camellia [1] are in this category.

Perhaps we should conclude that the difference between (11) and (12) points to a problem with the methodology being used to construct linear trails. Indeed, it would be possible to define a linear trail by its roundkey mask, and then adapt the method to compute its correlation contribution to make sure that all terms are included.

6 On Matsui's Algorithm 1

In this section, we investigate how the success rate of Matsui's Algorithm 1 is influenced by all the trails in the same linear hull. As described already in [13], this phenomenon can be used to extend Matsui's Algorithm 1 and to extract multiple key-bits. We illustrate this for reduced Simon in Section 6.5.

In Section 6.3 and Section 6.4 we study another consequence of this phenomenon: sometimes, the success rate of Matsui's Algorithm 1 will be worse than the estimate based on the study of a single trail. Somewhat counter-intuitively, the success rate of an attack may even decrease when the number of known plaintexts is increased! As far as we know, this is the first time that an explanation for such an effect is provided.

First, we describe the background for this special phenomenon: the 4 trails that constitute a hull over three rounds of Simon (Section 6.1) and the key-dependence of their correlations (Section 6.2).

6.1 Four trails through three rounds of Simon

Fig. 5 shows two trails through three rounds of Simon-32. Both trails start from the plaintext bits $\{8, 10, 16, 28\}$ and end in the ciphertext bit $\{16\}$. Hence they belong to the same 3-round linear hull. Fig. 6 in Appendix A shows two more trails belonging to this 3-round linear hull. It can be shown that this 3-round hull doesn't have any other trails with nonzero correlation contribution. These 4 linear trails are linearly dependent: denoting the vector of roundkey masks of Trail i by Ω_i, we have

$$\Omega_1 + \Omega_2 + \Omega_3 + \Omega_4 = 0$$

All trails involve bits $\{0, 12\}$ from the first roundkey, bit $\{14\}$ from the second, and bit $\{0\}$ from the third roundkey. Additionally, each of these trails have the following bits involved:

Trail 1: $\emptyset$
Trail 2: bit 8
Trail 3: bit 15
Trail 4: bits $8, 15$

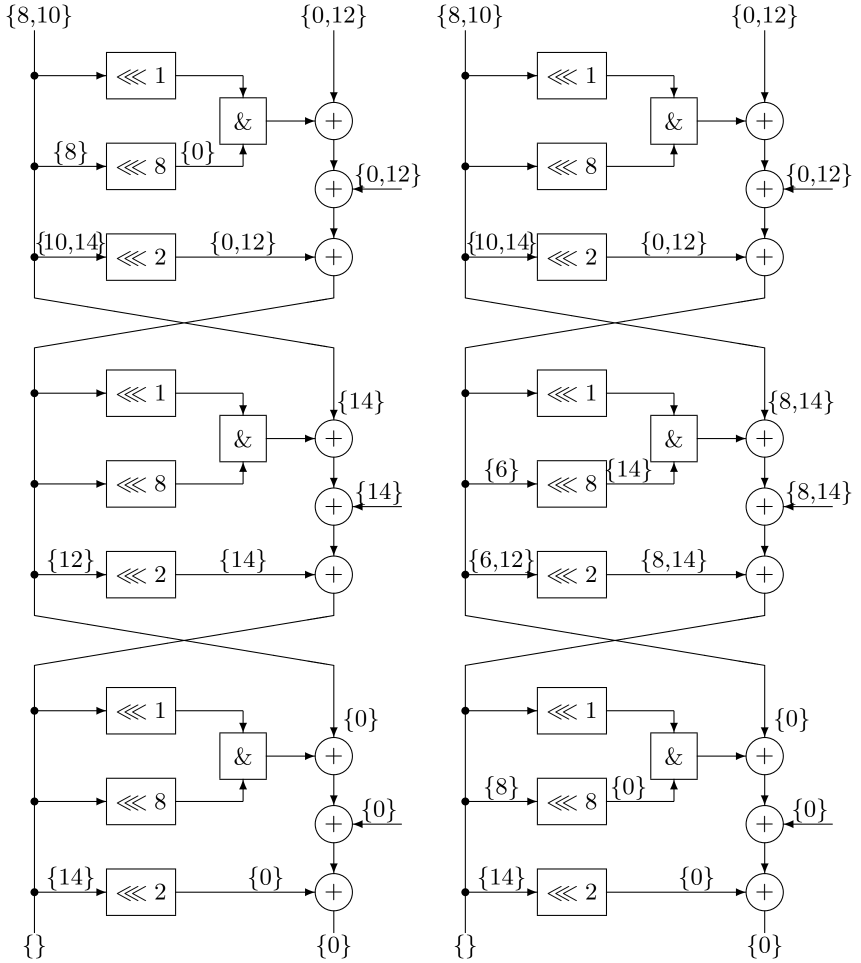

Fig. 5. Two trails in a 3-round linear hull. Trail 1 is shown on the left, Trail 2 on the right.

We denote by Z the sum of the roundkey bits involved in all trails. The sum of the roundkey bits involved in Trail 2, 3 and 4, we denote respectively by $Z + z_0$, $Z + z_1$ and $Z + z_0 + z_1$.

6.2 Correlation contributions of the trails

Straightforward computations similar to the computations in Section 3 and Section 4 show that the trails have the following correlation contributions:

$$\begin{aligned}
\text{Trail 1: } \mathrm{cor}_{\mathrm{p}}^{(1)} &= (-1)^{Z} \cdot 2^{-4} \\
\text{Trail 2: } \mathrm{cor}_{\mathrm{p}}^{(2)} &= (-1)^{Z+z_0} \cdot 2^{-5} \\
\text{Trail 3: } \mathrm{cor}_{\mathrm{p}}^{(3)} &= (-1)^{Z+z_1+1} \cdot 2^{-5} \\
\text{Trail 4: } \mathrm{cor}_{\mathrm{p}}^{(4)} &= (-1)^{Z+z_0+z_1} \cdot 2^{-5}
\end{aligned}$$

Note that these correlation contributions exist only as intermediate mathematical results. An attacker who can observe only plaintext and ciphertext bits, can measure only the sum of the four correlation contributions, i.e. the correlation of the hull. We suspect that this fact forms the basis of Murphy's argument against *the probability statements made in the usual definition of a linear hull* [11]. We denote the correlation of the hull by cor_h and obtain:

$$\begin{aligned}
\mathrm{cor}_h &= (-1)^{Z} \cdot 2^{-4} + (-1)^{Z+z_0} 2^{-5} + (-1)^{Z+z_1+1} 2^{-5} + (-1)^{Z+z_0+z_1} 2^{-5} && (13) \\
&= (-1)^{Z} \cdot 2^{-5} \left(2 + (-1)^{z_0} + (-1)^{z_1+1} + (-1)^{z_0+z_1}\right) && (14) \\
&= (-1)^{Z+z_0} \cdot 2^{-5} \left((-1)^{z_0} \cdot 2 + 1 + (-1)^{z_1+z_0+1} + (-1)^{z_1}\right) && (15) \\
&= (-1)^{Z+z_1} \cdot 2^{-5} \left((-1)^{z_1} \cdot 2 + (-1)^{z_0+z_1} - 1 + (-1)^{z_0}\right) && (16) \\
&= (-1)^{Z+z_0+z_1} \cdot 2^{-5} \left((-1)^{z_0+z_1} \cdot 2 + (-1)^{z_1} + (-1)^{z_0+1} + 1\right) && (17)
\end{aligned}$$

From (13) we see that the correlation is determined by the values of $Z, Z + z_0, Z + z_1 + 1$, and $Z + z_0 + z_1$. Table 1 considers the 8 possible assignments for these variables and their correlations. We see that for a fixed Z, the value $(-1)^Z \cdot 3 \cdot 2^{-5}$ is three times more likely to occur than the value $(-1)^{Z+1} \cdot 2^{-5}$. In the following, we will investigate how likely each value is, and show how different values affect the success rate of Matsui's Algorithm 1 when different trails are considered as if they are the only trails.

6.3 Knowing Trail 1 only

We adopt the figures of [10, Table 2] to express the relation between correlation of a hull, the number of known plaintext and the success rate. Concretely, we derive from the table that if the hull has correlation c, then using c^{-2}, $4c^{-2}$ and $8c^{-2}$ known plaintexts, the algorithm achieves success rates of respectively 84%, 98% and 100%.

In order to apply Algorithm 1 using Trail 1, the adversary first computes the correlation contribution of Trail 1:

$$\mathrm{cor}_{\mathrm{p}}^{(1)} = (-1)^{Z} \cdot 2^{-4} \qquad (18)$$

Table 1. The possible values for cor_h obtained from (13).

Z	z_0	z_1	cor_h
0	0	0	$3 \cdot 2^{-5}$
0	0	1	$3 \cdot 2^{-5}$
0	1	0	-2^{-5}
0	1	1	$3 \cdot 2^{-5}$
1	0	0	$-3 \cdot 2^{-5}$
1	0	1	$-3 \cdot 2^{-5}$
1	1	0	2^{-5}
1	1	1	$-3 \cdot 2^{-5}$

Using the assumption that the correlation of the hull is approximately equal to the correlation contribution of Trail 1, the adversary concludes that a sample of $N = 2^{10}$ known plaintexts should be sufficient to estimate Z with a success rate of 98%.

Subsequently, the adversary collects a sample of N known plaintexts and uses them to compute the experimental correlation $\hat{c}$. Depending on the value of $\hat{c}$, the adversary "guesses" a value for the sum (XOR) of the roundkey bits associated with the trail. Using (18) the adversary is led to believe that the actual bias can only take the values 2^{-4} and -2^{-4} and so the obvious decision rule is to guess for the XOR of the roundkey bits the value 1 if $\hat{c} < 0$, and the value 0 if $\hat{c} > 0$. From (14), however, we obtain:

$$\begin{aligned} z_0 = 0, z_1 = 0 &\rightarrow \mathrm{cor}_h = (-1)^Z \cdot 3 \cdot 2^{-5} \\ z_0 = 0, z_1 = 1 &\rightarrow \mathrm{cor}_h = (-1)^Z \cdot 3 \cdot 2^{-5} \\ z_0 = 1, z_1 = 0 &\rightarrow \mathrm{cor}_h = (-1)^Z \cdot (-1) \cdot 2^{-5} \\ z_0 = 1, z_1 = 1 &\rightarrow \mathrm{cor}_h = (-1)^Z \cdot 3 \cdot 2^{-5} \end{aligned}$$

In the first, the second and the last case, the actual correlation is $(-1)^Z \cdot 3 \cdot 2^{-5}$, which is 50% larger than the value that was obtained using Trail 1 only. Using 2^{10} known plaintexts, the success rate of Algorithm 1 increases from the predicted 98% to 100%.

In the third case, however, not only the magnitude of the correlation has decreased, but also the sign has changed. This means that Algorithm 1's estimate for Z will be *usually wrong*! The success rate drops from the predicted 98% to $100 - 84 = 16\%$. We conclude that the average success rate of Matsui's Algorithm 1 drops from the predicted 98% to

$$0.75 \cdot 100\% + 0.25 \cdot 16\% = 79\%.$$

When the data complexity is increased, the estimate of the actual correlation through the sample correlation is improved. This means that the first term in the sum increases, while the second one decreases. The success probability in the general case is given by:

$$1 - 0.75 \cdot \phi \left(\frac{-\left(\frac{N}{2} + 3 \cdot N \cdot 2^{-6} - \frac{N}{2}\right)}{\sqrt{\frac{N}{4} - 9 \cdot N \cdot 2^{-12}}} \right) + 0.25 \cdot \phi \left(\frac{-\left(\frac{N}{2} - N \cdot 2^{-6} - \frac{N}{2}\right)}{\sqrt{\frac{N}{4} + \cdot N \cdot 2^{-12}}} \right)$$

Differentiating with respect to N shows that the function is maximised with a success rate of 80% when $N = 2^{9.12}$, and tends to 75% as N tends to 2^{32}. So we get the following observation.

Observation: In an attack based on (the original, non-extended version of) Matsui's Algorithm 1 the optimal number of plaintexts can be smaller than the full codebook. Increasing the number of plaintexts beyond this optimal number may *decrease* the success rate of the attack.

6.4 Knowing only one of the Trails 2–4

Similar to the case of Trail 1, we can use the individual correlations presented in Subsection 6.2. Hence, for Trail 2, the adversary will compute

$$\mathrm{cor}_{\mathrm{p}}^{(2)} = (-1)^{Z+z_0} 2^{-5}$$

and conclude that 2^{12} known plaintexts should be sufficient to estimate $Z + z_0$ with a success rate of 98%. Since the predicted correlation differs only in sign, the decision rule for the guessed sum of the roundkey bits is as before. Repeating the success rate analysis and using the numbers from Table 1, we learn that the success rate with 2^{12} known plaintexts drops from the predicted 98% to

$$0.5 \cdot 100\% + 0.25 \cdot 98\% + 0.25 \cdot 0\% = 74.5\%$$

The success rate is maximised and saturates with 75% when N grows beyond $2^{12.1}$ as the middle term tends to 100% and the others stay steady. Similar computations give for Trail 4 the same result as for Trail 2. For Trail 3, setting $N = 2^{12}$ gives a reduced success rate of:

$$0.25 \cdot 100\% + 0.5 \cdot 0\% + 0.25 \cdot 2\% = 25.5\%.$$

A success rate below 50% means that Algorithm 1 will more often produce the wrong answer.

6.5 Knowing all Trails

When all trails are taken into account, Matsui's Algorithm 1 can be extended and recover more than a single bit, cf. also [13]. The approach can be summarized as follows. The adversary knows now that the correlation of the hull can take 4 values, distanced $2 \cdot 2^{-5}$ apart, cf. (13) and Table 1. The adversary divides the space of possible $\hat{c}$ outcomes into four regions instead of just two. After collecting N plaintexts, the adversary computes $\hat{c}$ and guesses for the key bits the values that produce the correlation the closest to $\hat{c}$. We can compute the success rate as follows.

If $Z = 0$ **and** $z_0z_1 \in \{00, 01, 11\}$**,** then $\mathrm{cor}_h = 3 \cdot 2^{-5}$. The attack will be successful if $\hat{c} > 2^{-4}$. When $N = 2^{12}$, this happens with probability 0.98. The adversary obtains $1 + 3(-1/3 \log_2(1/3)) = 1 + \log_2(3) \approx 2.6$ bits of information.

If $Z = 0$ **and** $z_0z_1 = 10$**,** then $\mathrm{cor}_h = -1 \cdot 2^{-5}$. The attack will be successful if $-2^{-4} < \hat{c} < 0$. When $N = 2^{12}$, this happens with probability 0.95. The adversary obtains 3 bits of information.

If $Z = 1$ **and** $z_0z_1 = 10$**,** then $\mathrm{cor}_h = 2^{-5}$. The attack will be successful if $0 < \hat{c} < 2^{-4}$. When $N = 2^{12}$, this happens with probability 0.95. The adversary obtains 3 bits of information.

If $Z = 1$ **and** $z_0z_1 \in \{00, 01, 11\}$**,** then $\mathrm{cor}_h = -3 \cdot 2^{-5}$. The attack will be successful if $\hat{c} < -2^{-4}$. When $N = 2^{12}$, this happens with probability 0.98. The adversary obtains 2.6 bits of information.

6.6 Conclusion

It has been observed before that the accuracy of linear attacks can be improved if multiple trails are taken into account [4,7,8]. The example that we treated in this section illustrates this for the specific case where we use Matsui's Algorithm 1 and all trails are in the same linear hull.

When we take the dependencies on the roundkey bits into account, we can use Algorithm 1 to recover more than 1 key bit as in [13]. However, when we do not take into account these dependencies, there are cases where Algorithm 1 systematically provides the wrong outcome, no matter how much we increase the number of known plaintexts. In fact, there are cases where increasing the number of known plaintexts beyond a certain value will result in a decrease of the attack's success rate. Future work should revisit attacks that were using the correlation of a single trail as an estimate for the correlation of the hull, as well as attacks using Matsui's Algorithm 1, to see whether the data complexity needs to be modified, and whether more key bits can be recovered. In previous sections we showed how this can be done using correlation matrices, taking into account conflicting effects that were previously overlooked.

It remains to be investigated how we can extend this analysis to hulls over more rounds, when it becomes infeasible to enumerate all the trails. Secondly, it would be interesting to investigate the consequences for Matsui's Algorithm 2. Algorithm 2 tries to find the last-round keys that minimise the distance between the correlation over $R - x$ rounds that is predicted by the adversary and the experimental correlation computed from ciphertexts and known plaintexts. If the actual correlation is very far from the predicted correlation, as we observed here, there could be many wrong keys ranked above the correct key.

ACKNOWLEDGMENTS. The authors would like to thank Kaisa Nyberg and the anonymous reviewers for their comments. This work was partially supported by the Research Council KU Leuven, OT/13/071.

References

1. Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., Tokita, T.: Camellia: A 128-bit block cipher suitable for multiple platforms - design and analysis. In: Stinson, D.R., Tavares, S.E. (eds.) Selected Areas in Cryptography, 7th Annual International Workshop, SAC 2000, Waterloo, Ontario, Canada, August 14-15, 2000, Proceedings. Lecture Notes in Computer Science, vol. 2012, pp. 39–56. Springer (2000), http://dx.doi.org/10.1007/3-540-44983-3_4
2. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404 (2013), http://eprint.iacr.org/
3. Biham, E.: On Matsui's linear cryptanalysis. In: Santis [14], pp. 341–355, http://dx.doi.org/10.1007/BFb0053449
4. Biryukov, A., Cannière, C.D., Quisquater, M.: On multiple linear approximations. In: Franklin, M.K. (ed.) Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings. Lecture Notes in Computer Science, vol. 3152, pp. 1–22. Springer (2004), http://dx.doi.org/10.1007/978-3-540-28628-8_1
5. Chabaud, F., Vaudenay, S.: Links between differential and linear cryptanalysis. In: Santis [14], pp. 356–365, http://dx.doi.org/10.1007/BFb0053450
6. Daemen, J., Govaerts, R., Vandewalle, J.: Correlation matrices. In: Preneel, B. (ed.) Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings. Lecture Notes in Computer Science, vol. 1008, pp. 275–285. Springer (1994), http://dx.doi.org/10.1007/3-540-60590-8_21
7. Hermelin, M., Cho, J.Y., Nyberg, K.: Multidimensional linear cryptanalysis of reduced round Serpent. In: Mu, Y., Susilo, W., Seberry, J. (eds.) Information Security and Privacy, 13th Australasian Conference, ACISP 2008, Wollongong, Australia, July 7-9, 2008, Proceedings. Lecture Notes in Computer Science, vol. 5107, pp. 203–215. Springer (2008), http://dx.doi.org/10.1007/978-3-540-70500-0_15
8. Jr., B.S.K., Robshaw, M.J.B.: Linear cryptanalysis using multiple approximations. In: Desmedt, Y. (ed.) Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings. Lecture Notes in Computer Science, vol. 839, pp. 26–39. Springer (1994), http://dx.doi.org/10.1007/3-540-48658-5_4
9. Keliher, L., Meijer, H., Tavares, S.E.: New method for upper bounding the maximum average linear hull probability for SPNs. In: Pfitzmann, B. (ed.) EUROCRYPT. Lecture Notes in Computer Science, vol. 2045, pp. 420–436. Springer (2001)
10. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings. Lecture Notes in Computer Science, vol. 765, pp. 386–397. Springer (1993), http://dx.doi.org/10.1007/3-540-48285-7_33
11. Murphy, S.: The effectiveness of the linear hull effect. J. Mathematical Cryptology 6(2), 137–147 (2012), http://dx.doi.org/10.1515/jmc-2011-0025
12. Nyberg, K.: Linear approximation of block ciphers. In: Santis [14], pp. 439–444, http://dx.doi.org/10.1007/BFb0053460
13. Röck, A., Nyberg, K.: Generalization of Matsui's Algorithm 1 to linear hull for key-alternating block ciphers. Des. Codes Cryptography 66(1-3), 175–193 (2013), http://dx.doi.org/10.1007/s10623-012-9679-1

14. Santis, A.D. (ed.): Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings, Lecture Notes in Computer Science, vol. 950. Springer (1995)
15. Shi, D., Hu, L., Sun, S., Song, L.: Linear (hull) cryptanalysis of round-reduced versions of KATAN. Cryptology ePrint Archive, Report 2015/964 (2015), http://eprint.iacr.org/
16. Shi, D., Hu, L., Sun, S., Song, L., Qiao, K., Ma, X.: Improved linear (hull) cryptanalysis of round-reduced versions of SIMON. Cryptology ePrint Archive, Report 2014/973 (2014), http://eprint.iacr.org/
17. Sun, S., Hu, L., Wang, M., Wang, P., Qiao, K., Ma, X., Shi, D., Song, L., Fu, K.: Towards finding the best characteristics of some bit-oriented block ciphers and automatic enumeration of (related-key) differential and linear characteristics with predefined properties. Cryptology ePrint Archive, Report 2014/747 (2014), http://eprint.iacr.org/

A Two more trails

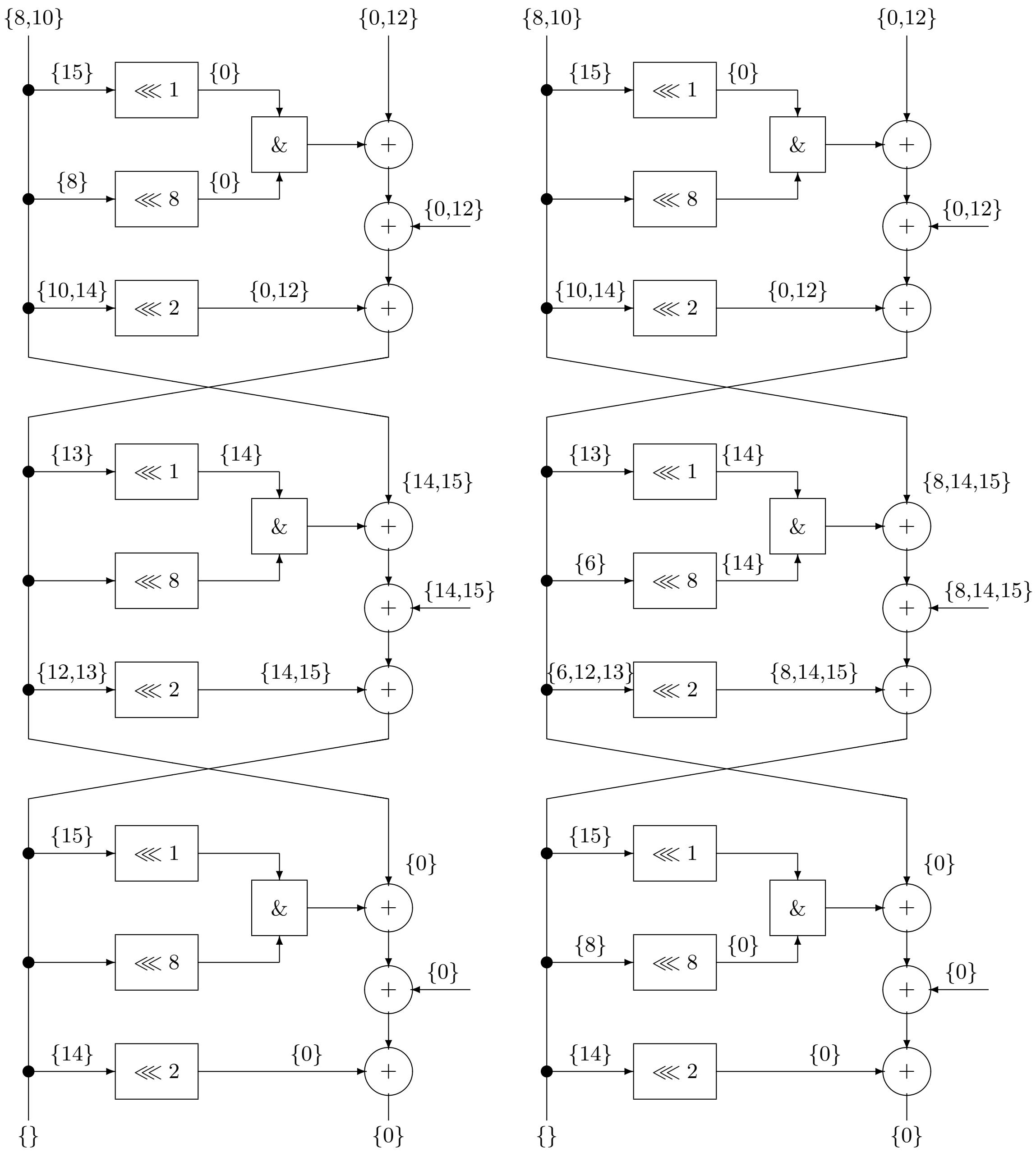

Fig. 6. Two more trails in the same 3-round linear hull as Figure 5. Trail 3 is shown on the left, Trail 4 on the right.