

The Maiorana-McFarland Structure Based Cryptanalysis for Simon

Hao Chen *

December 28, 2021

Abstract

In this paper we propose the linear hull construction for block ciphers with quadratic Maiorana-McFarland structure round functions. The search for linear trails with high squared correlations from our Maiorana-McFarland structure based constructive linear cryptanalysis is linear algebraic. Hence from this linear algebraic essence, the space of all linear trails has the structure such that good linear hulls can be constructed. We apply our method to construct better linear hulls for the Simon and Simeck block cipher family. Then for Simon $2n$ and its variants, the linear hull with the fixed input and output masks at arbitrary long rounds, and with the potential bigger than $\frac{1}{2^{2n}}$ can be constructed.

On the other hand we propose the Maiorana-McFarland structure based constructive differential cryptanalysis for symmetric-key primitives. The new search for good differential trails for Simon variants is linear algebraic. The problem of real existent differential trails is reduced to the finding of a solution of algebraic equations. We apply our method to the Simon $2n$ variants with arbitrary long rounds and prove that the expected differential probability is bigger than $\frac{1}{2^{\frac{n}{2}}}$ under the independence assumptions. It seems that at least theoretically Simon $2n$ is insecure for the key-recovery attack based on our new constructed linear hulls and key-recovery attack based on our constructed differential trails.

Keywords: Maiorana-McFarland structure, Linear hull construction, Potential, Expected differential probability, Simon, Simeck.

*Hao Chen is with the College of Information Science and Technology/Cyber Security, Jinan University, Guangzhou, Guangdong Province, 510632, China, haochen@jnu.edu.cn. This research was supported by the NSFC Grant 62032009.

1 Introduction

In symmetric-key primitives, in particular in recent permutation based hash constructions and the candidates in NIST lightweight cryptography competition, the algebraic degree of many round functions is two. For example in Keccak, Subterranean, Gimli, Ascon, Simon and Simeck, see [11, 21, 10, 23, 8, 30, 32, 5, 56, 50], the round functions or the nonlinear layers are algebraic degree two Boolean permutations. In this paper we propose the Maiorana-McFarland structure based linear cryptanalysis for block ciphers, which is suitable to algebraic degree two Boolean round functions with the Maiorana-McFarland structure.

Linear cryptanalysis was proposed and applied to key-recovery attack on DES in 1993-1994 by M. Matsui in [42, 43]. The basic ingredient in linear key-recovery attack on the block ciphers is the linear approximations with high correlations. The idea of the linear hull of an approximations was introduced by Nyberg in [49] and analysed in [47, 2, 6, 35], such that the required plaintext-ciphertext pairs for key-recovery attack decreased significantly. We refer to [3, 4, 5, 20, 24] for linear cryptanalysis of block ciphers such as Simon and PRESENT. In particular the linear attack in [24] gave a first attack on the 28 round PRESENT, and the attack on the 45 round Simon96/144 in [34].

Differential cryptanalysis was initiated from the classical paper [13] and has been one of the basic analysis tool to evaluate the security margin of block ciphers. We refer to [33, 25] for independence assumptions and expected differential probability calculation. There have been many works [15, 30, 39, 41] on differential cryptanalysis of Simon based on computer-aided search of good differential trails.

The Maiorana-McFarland class of bent functions was given in the paper [44]. The concept of Maiorana-McFarland class Boolean functions in [44, 48, 17, 16] was introduced basically for the construction of good cryptographic Boolean functions. However our motivation in this paper is to establish good linear hulls and construct many differential trails with the fixed input and output differences from the Maiorana-McFarland structure of Boolean round functions. In the Maiorana-McFarland structure based linear cryptanalysis for degree two restricted Boolean round functions, the search of good linear trails is linear algebraic. Then linear trails with high squared correlations can be constructed and searched more efficiently than

previous approaches. We apply our method to construct the linear hulls for the Simon variants and the Simeck block cipher. It is possible that this method can also be partially extended to higher degree round function block ciphers. We also propose the Maiorana-McFarland structure based constructive differential cryptanalysis such that many good differential trails with fixed input and output differences can be constructed and the expected differential probability can be lower bounded. This paper is the first work to apply the Maiorana-McFarland structure of round functions to cryptanalysis of block ciphers systematically.

Simon is a lightweight block cipher designed and presented by NSA in 2013. NSA did not provide security analysis and design rationale. For the description of Simon block cipher family we refer to [8]. Its version Simon $2n$, where $n \in \{16, 24, 32, 48, 64\}$, is defined as follows. The Boolean mapping $f : \mathbf{F}_2^n \rightarrow \mathbf{F}_2^n$ is a permutation defined by

$$f(\mathbf{x}) = S^1(\mathbf{x}) \cdot S^8(\mathbf{x}) + S^2(\mathbf{x}),$$

where $\mathbf{x} \in \mathbf{F}_2^n$, \cdot is the bit-wise multiplication, S^i is the shift of bits to the left by i positions. The round function on \mathbf{F}_2^{2n} is defined by

$$L_i = f(L_{i-1}) + R_{i-1} + k_i,$$

$$R_i = L_{i-1}.$$

Then (L_0, R_0) is the plaintext, after r rounds, (L_{r-1}, R_{r-1}) is the ciphertext. When the parameter $(1, 8, 2)$ is replaced by (a, b, c) the Simon variant with the parameter triple (a, b, c) using

$$f_{a,b,c}(\mathbf{x}) = S^a(\mathbf{x}) \cdot S^b(\mathbf{x}) + S^c(\mathbf{x})$$

was considered in [30]. Notice that there are

$$\binom{n}{2} \cdot n$$

possibilities of parameter triples (a, b, c) 's. For Simon $2n$ the sizes of master keys are mn bits where $2 \leq m \leq 4$. For Simon $32/64$ the designed number of rounds is 32, for Simon $48/72$ and Simon $48/96$ the designed number of rounds is 36. For Simon $64/96$ the designed number of rounds is 42, for Simon $64/128$ the designed number of rounds is 44. For Simon $96/96$ the designed number of rounds is 52 and 54 for Simon $96/144$. For Simon $128/128$

the designed number of rounds is 68, 69 for Simon128/192 and 72 for Simon128/256.

When the parameter triple is $(5, 0, 1)$ this is the Simeck block cipher family, see [56]. The designed numbers of rounds for Simeck32/64, Simeck48/96, Simeck64/128 are 32, 36 and 44.

The Simon and Simeck are key-alternating block ciphers. We refer the description of key scheduling to [8, 9, 56]. The round keys for Simon k_0, k_1, k_2, \dots , are produced from the master keys k_0, k_1, \dots, k_{m-1} , where $m = 2, 3, 4$, as follows

$$\begin{aligned} k_{i+2} &= k_i \oplus (I \oplus S^{-1})S^{-3}k_{i+1} \oplus C_i, \\ k_{i+3} &= k_i \oplus (I \oplus S^{-1})S^{-3}k_{i+2} \oplus D_i, \\ k_{i+4} &= k_i \oplus (I \oplus S^{-1})(S^{-3}k_{i+3} \oplus k_{i+1}) \oplus E_i, \end{aligned}$$

where C_i , D_i and E_i are round-dependent constants. Notice that the key schedule for Simon is linear. We refer to [56] for key scheduling for Simeck. The recursion is defined by $k^{i+4} = k^i \oplus f(k^{i+1}) \oplus C \oplus z^i$, where C and z^i are constants depending on block size and f is the same function $f_{(5,0,10)}$ used in the data path. This key scheduling is not linear.

2 Previous results and our contribution

2.1 Previous cryptanalysis of Simon and Simeck

We refer to [1, 3, 4, 5, 20, 39, 34] for the linear and differential cryptanalysis of Simon. For differential cryptanalysis and rotational-XOR cryptanalysis of Simon, see [15, 41]. Integral attack and impossible differential attack on Simon were presented in [32]. The most successful attacks on Simon and Simeck are from linear (hull) cryptanalysis and differential cryptanalysis in [34]. In [30] exact and explicit-computable differential and linear behaviour of Simon-like round functions are derived and optimal differential and linear characteristics of Simon variants are searched by computer-aided SAT/SMT solvers. The optimal differential and linear trails were searched by their explicit calculations of differential probability formula in Theorem 3 and explicit expression of squared correlation in Theorem 5 of [30]. For general parameters (a, b, c) satisfying $\gcd(a-b, n) = 1$ and $a < b$ optimal differential

trails for 10 rounds of Simon32, Simon48 and Simon64 were searched and presented in Appendix D of [30]. As analysed by Kölbl-Leander-Teissen in [30], 20 parameter triples are optimal for Simon32, Simon48 and Simon64 with respect to 10 rounds differential attack. The computer-aided search results about differential trails in [30] was verified in [39]. In [32] it was argued that $(4, 1, 7)$ and $(12, 5, 3)$ belong to the above parameter triples with optimal security against differential attack have the same security level against integral and impossible differential attacks as the original Simon. We refer linear hull cryptanalysis and linear analysis using super rounds of Simon to [4, 20, 5, 40, 3]. For the latest and known best linear and differential cryptanalysis of Simon and Simeck, we refer to [7, 31, 50, 52, 34]. For a nice survey on various attacks on Simon family before 2017, we refer to [9]. The present best attack results are key-recovery attacks due to [34] based on linear hulls, for example, an attack against 45-round Simon96/144, an attack against 42 round Simeck64.

2.2 Our contribution

We present the Maiorana-McFarland structure based linear cryptanalysis and differential cryptanalysis. In particular when the round functions are of algebraic degree two the squared correlation can be expressed directly from the restricted Maiorana-McFarland structure. The search of good linear trails is reduced to a search for target vectors satisfying some linear algebraic properties. In this framework linear hulls can be constructed by linear algebra techniques. This leads to better attacks based on linear hull for Simon2n and its variants. To the best of our knowledge this is the first effort to construct good linear hulls from the structures of round functions, not from the search.

Based on our linear algebraic search of linear trails of the Simon, better linear hulls than the best previous known results in [3, 20, 34] can be constructed directly. The space of all linear trails in our presentation has the structure such that linear trails for Simon variants can be operated. We apply our method to construct better linear hulls for the Simon and Simeck block cipher family. Then for Simon2n with the linear key schedule, the linear hull with the fixed input mask and the output mask at arbitrary rounds can be constructed. The potentials of our new constructed linear hulls are bigger than $\frac{1}{2^{2n}}$. Then it seems that theoretically Simon2n and its variants using linear key schedule are insecure for the key-recovery attack based on

our new constructed linear hulls. This method seems possible to extend to multiply linear or multidimensional linear cryptanalysis.

As indicated in [45, 38, 37] some discovered differential trails by computer-aided search/solver are always invalid since contradictions may easily occur in the set of conditions implied in the discovered differential trails. However we can check that if the Maiorana-McFarland structure based differential trails are compatible by algebraic equations. The inconsistency problem of Maiorana-McFarland structure based differential trails is reduced to the finding of a solution of algebraic equations. This is analysed in Section 8.

We apply the Maiorana-McFarland structure constructive differential cryptanalysis to Simon variants. Then we prove that the expected differential probability (EDP) of Simon $2n$ of arbitrary rounds is bigger than $\frac{1}{2^{\frac{n}{2}}}$ under independence assumption. Then even when lower bound EDP over realistic differential trails, the lower bound is bigger than $\frac{1}{2^{2n}}$. Combining with the Maiorana-McFarland structure based linear hull construction described as above, at least theoretically Simon is not secure because of its degree two Maiorana-McFarland structure round function.

Actually from our Maiorana-McFarland structure based linear and differential cryptanalysis, for a Feistel block cipher with a degree two restricted Maiorana-McFarland structure round function, the space of all effective linear trails and differential trails can be described almost explicitly. Therefore operations on linear trails and differential trails are possible. Such operations on linear trails and differential trails can help to give better potential and EDP lower bounds. From a linear algebraic and counting argument the linear hull with the big potential can be constructed, though the complexity to list all linear trails in the hull is high. Similarly EDP can be nicely lower bounded.

2.3 Outline of our arguments

The main results in this paper are the lower bounds on the potential and the expected differential probability (EDP) for Simon $2n$ and its variants, under the following two independent assumptions, we refer to [33, 25].

- 1) The linear approximations or differentials of different rounds are independent;
- 2) The linear trails or differential trails are independent.

If these two assumptions are assumed, we prove that the lower bound $\frac{1}{2^n}$ on the potential and the lower bound $\frac{1}{2^{\frac{n}{2}}}$ on EDP for Simon2n of arbitrary long rounds. However for key-alternating block ciphers such as Simon the above assumptions are not realistic. We argue that by the average method that the lower bound of potential for the linear key schedule Simon2n, is strictly bigger than $\frac{1}{2^{2n}}$. And the EDP for Simon2n with linear key schedule is much bigger than $\frac{1}{2^{2n}}$. The basic point is that though the realistic potential and EDP is not so big when the above two assumptions are assumed, they are still larger than the threshold.

2.4 No dominant trail

From the construction of linear hull and many differential trails with the fixed input and output differences, it is easy to see that for a given trail there are many trails produced from this trail with probabilities not much decreased. This is easy to verify under the above two independent assumptions. Even in the realistic case, this non-dominant property seems true.

3 The Maiorana-McFarland structures and the structure finding algorithm

Definition 3.1. Let $\Phi : \mathbf{F}_2^m \rightarrow \mathbf{F}_2^n$ be a Boolean mapping. If there exists some variables x_{i_1}, \dots, x_{i_h} , where i_1, \dots, i_h are distinct indices in the set $\{1, 2, \dots, m\}$ such that for each component

$$\Phi = (\Phi_1, \dots, \Phi_n),$$

we have

$$\Phi_t(x_1, \dots, x_m) = \sum_{j=1}^h G_t^j x_{i_j} + G_t,$$

where G_t^j, G_t are Boolean functions of variables in the set $\{x_1, \dots, x_m\} - \{x_{i_1}, \dots, x_{i_h}\}$, we say that the Boolean mapping Φ has a Maiorana-McFarland structure at the variables x_{i_1}, \dots, x_{i_h} . The variables in $\{x_1, \dots, x_m\} - \{x_{i_1}, \dots, x_{i_h}\}$ are called non-Maiorana-McFarland variables. We call the number h the Maiorana-McFarland number of Φ . The Boolean mapping G^j is $G^j = (G_t^j)_{t=1, \dots, n} : \mathbf{F}_2^{m-h} \rightarrow \mathbf{F}_2^m$.

Definition 3.2. Let $\Phi : \mathbf{F}_2^m \rightarrow \mathbf{F}_2^n$ be a Boolean mapping. If there exists some variables x_{i_1}, \dots, x_{i_h} , where i_1, \dots, i_h are distinct indices in the set $\{1, 2, \dots, m\}$ such that for each component

$$\Phi = (\Phi_1, \dots, \Phi_n),$$

we have

$$\Phi_t(x_1, \dots, x_m) = \sum_{j=1}^H G_t^j f_j + G_t,$$

where G_t^j, G_t are Boolean functions of variables in the set $\{x_1, \dots, x_m\} - \{x_{i_1}, \dots, x_{i_h}\}$ and f_1, \dots, f_H are functions of variables in the set $\{x_{i_1}, \dots, x_{i_h}\}$, we say that the Boolean mapping Φ has a generalized Maiorana-McFarland structure at the variables x_{i_1}, \dots, x_{i_h} . The variables in $\{x_1, \dots, x_m\} - \{x_{i_1}, \dots, x_{i_h}\}$ are called non-Maiorana-McFarland variables. We call the number h the Maiorana-McFarland number of Φ . The Boolean mapping G^j is $G^j = (G_t^j)_{t=1, \dots, m} : \mathbf{F}_2^{m-h} \rightarrow \mathbf{F}_2^m$.

It is obvious that a linear Boolean mapping $\mathbf{L} : \mathbf{F}_2^n \rightarrow \mathbf{F}_2^n$ has the full Maiorana-McFarland structure and the Maiorana-McFarland number is n . An arbitrary Boolean mapping has at least the Maiorana-McFarland number 1. If $\Phi : \mathbf{F}_2^m \rightarrow \mathbf{F}_2^n$ has a Maiorana-McFarland structure at the variables x_{i_1}, \dots, x_{i_h} , then when the variables in $\{x_1, \dots, x_m\} - \{x_{i_1}, \dots, x_{i_h}\}$ are given fixed values, Φ is an affine mapping from \mathbf{F}_2^h to \mathbf{F}_2^n .

If some Boolean permutations in a symmetric-key primitives have large Maiorana-McFarland number h , this is a weakness of this symmetric-key primitive to the adversary. We now establish an algorithm to find the Maiorana-McFarland structures of Boolean mappings. It is clear that there is a one-variable Maiorana-McFarland structure for an arbitrary Boolean mapping. Hence it is a goal for our algorithm to find the Maiorana-McFarland number h **as large as possible** for a Boolean mapping $\Phi : \mathbf{F}_2^m \rightarrow \mathbf{F}_2^n$,

$$\Phi(x_1, \dots, x_m) = (\phi_1(x_1, \dots, x_m), \dots, \phi_n(x_1, \dots, x_m)).$$

Route. Write

$$\Phi = \Phi_1(x_1, \dots, \hat{x}_{i_1}, \dots, x_m)x_{i_1} + \Phi'_1(x_1, \dots, \hat{x}_{i_1}, \dots, x_m),$$

where Φ_1 and Φ'_1 are just Boolean mappings from \mathbf{F}_2^{m-1} to \mathbf{F}_2^n . Here $x_1, \dots, \hat{x}_{i_1}, \dots, x_m$ are $m - 1$ variables $x_1, \dots, x_{i_1-1}, x_{i_1+1}, \dots, x_m$. In this step the target is to find an index i_1 such that Φ_1 is a Boolean mapping

from $\mathbf{F}_2^{m-j_1}$ to \mathbf{F}_2^m with the maximal possible j_1 .

When $j_1 = 1$ then the Maiorana-McFarland number of Φ is (at least) 1 and the algorithm stops.

When $j_1 > 1$ we continue the Route for the Boolean mapping Φ'_1 for an index x_{i_2} which does not appear in Φ_1 . Hence after this step we have $\Phi = \Phi_1(x_1, \dots, \hat{x}_{i_1}, \dots, \hat{x}_{i_2}, \dots, x_m)x_{i_1} + \Phi_2(x_1, \dots, \hat{x}_{i_1}, \dots, \hat{x}_{i_2}, \dots, x_m)x_{i_2} + \Phi'_2(x_1, \dots, \hat{x}_{i_1}, \dots, \hat{x}_{i_2}, \dots, x_m)$. The Maiorana-McFarland number of Φ is (at least) 2. Here Φ_1 is a Boolean mapping from $\mathbf{F}_2^{m-j_1}$ to \mathbf{F}_2^n , Φ_2 is a Boolean mapping from $\mathbf{F}_2^{m-j_2}$ to \mathbf{F}_2^n , Φ'_2 is a Boolean mapping from \mathbf{F}_2^{m-2} to \mathbf{F}_2^n .

If $j_1 = 2$ or $j_2 = 2$ the algorithm stops. Otherwise we repeat the Route to Φ'_2 . This process can continue to one step and we get h Maiorana-McFarland structure variables of the Boolean mapping Φ .

Let g be a fixed round function $g : \mathbf{F}_2^n \rightarrow \mathbf{F}_2^n$, the block cipher can be modeled as follow.

$$\begin{aligned} \mathbf{x} &= w^0, \\ w^1 &= g(w^0, K_1), \\ w^2 &= g(w^1, K_2), \\ &\dots\dots, \\ w^{N_r} &= g(w^{N_r-1}, K_{N_r}), \\ \mathbf{y} &= w^{N_r}, \end{aligned}$$

where N_r is number of rounds, K_1, K_2, \dots, K_{N_r} are N_r round keys in \mathbf{F}_2^m , \mathbf{w} is the plaintext and \mathbf{y} is the ciphertext.

We consider the following Boolean mapping $G_t : \mathbf{F}_2^{n+tm} \rightarrow \mathbf{F}_2^n$ defined by

$$G_t(x, K_1, \dots, K_t) = g(G_{t-1}(G_{t-2}, K_1, \dots, K_{t-1}), K_t)$$

and check if these G_t 's have the Maiorana-McFarland structures at many variables. If many Maiorana-McFarland structure variables can be found in G_t , by fixing the values of not many non -Maiorana-McFarland variables, G_t is linear. This weakness can be used to cryptanalysis this block cipher.

From the previous analysis the following Maiorana-McFarland criterion for the compositions of block ciphers seems reasonable.

The Maiorana-McFarland structure criterion for block ciphers.

The Maiorana-McFarland number of G_{r_1} 's should be 1 for $r_1 \leq r$, where r is the real round of this block cipher. Hence for any given G_{r_1} , we should take random fixed values of some random variables and then apply the Maiorana-McFarland structure finding algorithm to check the Maiorana-McFarland number of above G_{r_1} 's with these fixed values, for $r_1 = 1, 2, \dots, r$. These Maiorana-McFarland numbers can not be large.

However it is difficult to get a compact algebraic normal form for several round compositions of round functions, the above Maiorana-McFarland structure finding algorithm is not so help to find the real such structures of these compositions. The problem of Maiorana-McFarland structure finding in block ciphers without the ANF is interesting and important. We calculate the compositions of Simon block ciphers of very few rounds and found that the Maiorana-McFarland numbers are small.

4 The Maiorana-McFarland structure based linear cryptanalysis

4.1 General facts

For a Boolean mapping $f : \mathbf{F}_2^n \rightarrow \mathbf{F}_2^n$, the Walsh coefficient of f with the input mask α and the output mask β in \mathbf{F}_2^n is defined by

$$\hat{f}(\alpha, \beta) = \sum_{\mathbf{x} \in \mathbf{F}_2^n} (-1)^{\langle \beta, f(\mathbf{x}) \rangle + \langle \alpha, \mathbf{x} \rangle}.$$

The squared correlation is

$$C^2(\alpha, \beta) = \left(\frac{\hat{f}(\alpha, \beta)}{2^n} \right)^2.$$

For independent assumptions we refer to [33, 25].

Given input mask α and output mask β the potential of a linear hull with the fixed input mask α and output mask β is

$$ELP(\alpha, \beta) = \sum_{(\gamma_0, \dots, \gamma_r)} C^2(\alpha, \beta, \gamma_0, \dots, \gamma_r),$$

we refer to [49, 20, 34]. In general linear hull attack requires $O(\frac{1}{ELP(\alpha,\beta)})$ plaintext-ciphertext pairs to succeed. Linear hull effect means that this potential is significantly larger than the squared correlation of individual linear trail with fixed intermediate masks. As proved in Theorem 1 of [49] (or see [6] Section 5), if the plaintext X and the key K are independent and the key K is uniformly distributed, the the bias of the linear approximation with the input mask at the plaintext and output mask at the ciphertext is indeed the sum of all correlation squares over all linear trails over all keys. We refer to [14, 26, 27, 28, 46, 2, 35] for multiply linear cryptanalysis and multidimensional linear cryptanalysis. For Simon block ciphers, we refer to [6] for analysing of linear hulls and dependent linear trail contribution calculation, as compared to the paper [53].

4.2 Squared correlation calculation

The following restricted Maiorana-McFarland structure of the Boolean mapping f of algebraic degree two makes the calculation of Walsh coefficients and squared correlation directly. Suppose that the algebraic degree two Boolean mapping f has the Maiorana-McFarland number h and has the Maiorana-McFarland structure expansion $f(x_1, \dots, x_n) = F_1x_1 + \dots + F_hx_h + F_{h+1} + F_{h+2}$, where $F_i : \mathbf{F}_2^{n-h} \rightarrow \mathbf{F}_2^n$ are Boolean mapping of the $(n-h)$ variables $\{x_{h+1}, \dots, x_n\}$ for $i = 1, \dots, h+1$. F_{h+2} is a linear mapping from the variables x_1, \dots, x_h to \mathbf{F}_2^n . Here for general degree two Boolean mapping f with the Maiorana-McFarland structure, F_{h+1} need not to be linear and there are possible some degree two terms in F_{h+1} . We restrict ourselves to the case \mathbf{F}_{h+1} is linear. The round functions of Simon variants are typical such degree two restricted Maiorana-McFarland Boolean mappings.

For such a restricted Maiorana-McFarland degree two Boolean mapping f , when $(x_1, \dots, x_h) \in \mathbf{F}_2^h$ is fixed,

$$(-1)^{\sum_{j=1}^h x_h \langle \beta, F_j \rangle + \langle \alpha_1, \mathbf{x}_1 \rangle + \langle \beta \cdot F_{h+2}, \mathbf{x}_1 \rangle + \langle \alpha_2, \mathbf{x}_2 \rangle + \langle \beta \cdot F_{h+1}, \mathbf{x}_2 \rangle},$$

where $\mathbf{x}_1 = (x_1, \dots, x_h)$ and $\mathbf{x}_2 = (x_{h+1}, \dots, x_n)$, can be calculated. Here α_1 and α_2 are the first h bit vector and the last $n-h$ bit vector of α . F_j , $j = 1, \dots, h$ are considered as length n vectors with entries of linear functions of x_{h+1}, \dots, x_n . F_{h+1} is considered as $n \times (n-h)$ matrix and F_{h+2} is considered as $n \times h$ matrix. When the Maiorana-McFarland structure variables x_1, \dots, x_h are fixed $\langle \alpha_1, \mathbf{x}_1 \rangle + \langle \beta \cdot F_{h+2}, \mathbf{x}_1 \rangle$ is a fixed 0 or 1. When the round function f is of degree two the Maiorana-McFarland

structure-based calculation of Walsh coefficients and squared correlation is direct as follows.

When the round function f is of algebraic degree two, then F_1, \dots, F_h are linear mappings from \mathbf{F}_2^{n-h} to \mathbf{F}_2^n . They are considered as $n \times (n-h)$ matrices. For any given nonzero $\beta \in \mathbf{F}_2^n$, we define a linear mapping B_β as follows

$$B_\beta(F) = (\langle \beta, F_j \rangle)_{1 \leq j \leq h}.$$

This is a $h \times (n-h)$ matrix. For 2^h possibilities of $x_1 F_1 + \dots + x_h F_h$ when x_1, \dots, x_h take over all vectors in \mathbf{F}_2^h , we denote the linear subspace of \mathbf{F}_2^h of $(x_1, \dots, x_h) \in \mathbf{F}_2^h$ such that $x_1 F_1 + \dots + x_h F_h$ satisfying $\beta \cdot (x_1 F_1 + \dots + x_h F_h) = 0$, that is, (x_1, \dots, x_h) is in the kernel of the linear mapping $\mathbf{F}_2^h \rightarrow \mathbf{F}_2^{n-h}$ defined by $B_\beta(F)$, by $W_{\beta, F_1, \dots, F_h}$. The dimension of this subspace is $h - \text{rank}(B_\beta(F))$.

For fixed \mathbf{x}_1 , when $\alpha_2 + \beta \cdot F_{h+1}$ is not in the image of B_β , then

$$(-1)^{\sum_{j=1}^h x_j \langle \beta, F_j \rangle + \langle \alpha_1, \mathbf{x}_1 \rangle + \langle \beta \cdot F_{h+2}, \mathbf{x}_1 \rangle + \langle \alpha_2, \mathbf{x}_2 \rangle + \langle \beta \cdot F_{h+1}, \mathbf{x}_2 \rangle}$$

is zero since

$$\sum_{j=1}^h x_j \langle \beta, F_j \rangle + \langle \alpha_2, \mathbf{x}_2 \rangle + \langle \beta \cdot F_{h+1}, \mathbf{x}_2 \rangle + \langle \alpha_1, \mathbf{x}_1 \rangle + \langle \beta \cdot F_{h+2}, \mathbf{x}_1 \rangle$$

is a nonzero linear function on \mathbf{F}_2^{n-h} . When $\alpha_2 + \beta \cdot F_{h+1}$ is in the image of B_β , then

$$\hat{f}(\alpha, \beta) = 2^{n-h} \sum_{\mathbf{x}_1 \in \mathbf{x}_1^0 + W_{\beta, F_1, \dots, F_h}} (-1)^{\langle \alpha_1, \mathbf{x}_1 \rangle + \langle \beta \cdot F_{h+2}, \mathbf{x}_1 \rangle},$$

where \mathbf{x}_1^0 satisfies

$$\sum_{i=1}^h x_i^0 \beta \cdot F_i = \alpha_2 + \beta \cdot F_{h+1}.$$

In this case if $\alpha_1 + \beta \cdot F_{h+2} = 0$, then we have

$$\hat{f}(\alpha, \beta) = 2^{n - \text{rank}(B_\beta(F))}.$$

More importantly when $\langle \alpha_1 + \beta \cdot F_{h+2}, \mathbf{x}_1 \rangle = 0$ for any given $\mathbf{x}_1 \in \mathbf{x}_1^0 + W_{\beta, F_1, \dots, F_h}$ we also have

$$\hat{f}(\alpha, \beta) = 2^{n - \text{rank}(B_\beta(F))}.$$

From the above analysis we have the following result.

Theorem 4.1. *When $\alpha_2 + \beta F_{h+1}$ is not in the image of B_β , then $\hat{f}(\alpha, \beta) = 0$, when $\alpha_2 + \beta F_{h+1}$ is in the image of B_β , we have*

$$\hat{f}(\alpha, \beta) = 2^{n-h} \sum_{\mathbf{x}_1 \in \mathbf{x}_1^0 + W_{\beta, F_1, \dots, F_h}} (-1)^{\langle \alpha_1, \mathbf{x}_1 \rangle + \langle \beta \cdot F_{h+2}, \mathbf{x}_1 \rangle},$$

where \mathbf{x}_1^0 satisfies

$$\sum_{i=1}^h x_i^0 \beta \cdot F_i = \alpha_2 + \beta \cdot F_{h+1}.$$

Moreover we have $|\hat{f}(\alpha, \beta)| \leq 2^{n-\text{rank}(B_\beta(F))}$.

Corollary 4.1. *Only when $\alpha_1 + \beta \cdot F_{h+2}$ has zero inner product with each vector in the affine space $\mathbf{x}_1^0 + W_{\beta, F_1, \dots, F_h}$ and $\alpha_2 + \beta \cdot F_{h+1}$ is in the image of B_β , we have*

$$|\hat{f}(\alpha, \beta)| = 2^{n-\text{rank}(B_\beta(F))}.$$

We have

$$\hat{f}(\alpha, \beta) = 0$$

in other cases.

The following statement is direct from Theorem 4.1.

Corollary 4.2. *Only when $(\alpha_1 + \beta \cdot F_{h+2})$ is in the linear span of $n - h$ columns of B_β , and $\alpha_2 + \beta \cdot F_{h+1}$ is in the linear span of $\beta F_1, \dots, \beta F_h$, we have*

$$|\hat{f}(\alpha, \beta)| = 2^{n-\text{rank}(B_\beta(F))}.$$

We have

$$\hat{f}(\alpha, \beta) = 0$$

in other cases.

Proof. If $(\alpha_1 + \beta \cdot F_{h+2})$ is in the linear span of $n - h$ columns of B_β , then $\langle \alpha_1 + \beta \cdot F_{h+2}, \mathbf{x}_1 \rangle = 0$ for all $\mathbf{x}_1 \in W_{\beta, F_1, \dots, F_h}$. Then the exponent of -1 is fixed and determined by \mathbf{x}_1^0 . The conclusion follows.

4.3 Feistel round function

In the case that the round function \mathbf{T} of is a Feistel map $\mathbf{T} : \mathbf{F}_2^{2n} \longrightarrow \mathbf{F}_2^{2n}$ defined by

$$\mathbf{F}(\mathbf{x}, \mathbf{y}) = (f(\mathbf{x}) + \mathbf{y}, \mathbf{x}).$$

We need to compute the squared correlation of this function \mathbf{T} . Applying Corollary 4.1 to this round function we have the following result. Here γ_1 and γ_2 are the Maiorana-McFarland structure variable part and the remaining variable part of a vector $\gamma \in \mathbf{F}_2^n$. Here we only need the restricted Maiorana-McFarland structure of the algebraic degree two Boolean mapping f .

Theorem 4.3. *Set $\alpha = (L(\alpha), R(\alpha)) \in \mathbf{F}_2^{2n}$ and $\beta = (L(\beta), R(\beta)) \in \mathbf{F}_2^{2n}$. Only when*

- 1) $L(\alpha)_1 + L(\beta) \cdot F_{h+2} + R(\beta)_1$ is in the linear span of $n-h$ columns of $B_{L(\beta)}$;
 - 2) $L(\alpha)_2 + L(\beta) \cdot F_{h+1} + R(\beta)_2$ is in the linear span of h rows of $B_{L(\beta)}$;
 - 3) $L(\beta) + R(\alpha) = 0$,
- Then we have $\hat{T}(\alpha, \beta) = 2^{2n - \text{rank}(B_{L(\beta)}(F))}$.

Proof. From the formula

$$\hat{T}(\alpha, \beta) = \sum_{\mathbf{y}} (-1)^{\langle L(\beta) + R(\alpha), \mathbf{y} \rangle} \sum_{\mathbf{x}} (-1)^{\langle L(\beta), f(\mathbf{x}) \rangle + \langle R(\beta) + L(\alpha), \mathbf{x} \rangle},$$

we get the conclusion immediately.

4.4 Computer-aided search

Optimal linear trail. Then the search for optimal r -round linear trails is equivalent to the following problem to find vectors $\beta^0, \beta^1, \dots, \beta^r$ satisfying the following conditions. Here F_1, \dots, F_{h+1} are considered as $n \times (n-h)$ binary matrices and F_{h+2} is considered as an $n \times h$ binary matrix.

- 1) $(\beta_1^i + \beta^{i+1} \cdot F_{h+2})$ is in the linear span of $n-h$ columns of $B_{\beta^{i+1}}$, and

$$\beta_2^i + \beta^{i+1} \cdot F_{h+1}$$

is in the linear span of $\beta^{i+1} \cdot F_1, \dots, \beta^{i+1} \cdot F_h$;

Here β_1^i is the Maiorana-McFarland structure variable part of the vector β^i and β_2^i is the non-Maiorana-McFarland structure variable part of the vector β^i .

- 2) $\sum_{i=1}^r \text{rank}(B_{\beta^i})$ is as small as possible. The squared correlation is

$$\frac{1}{2^{2(\sum \text{rank}(B_{\beta^i}))}}.$$

Local optimal. Find one β^1 with $\text{rank}(B_{\beta^1})$ as small as possible, such that there is another β^2 satisfying 1) and $\text{rank}(B_{\beta^2})$ is as small as possible. Then for each given β^i we need to find one β^{i+1} satisfying 1) with smallest possible $\text{rank}(B_{\beta^{i+1}})$.

It seems that in almost all cases the local optimal does not lead to the global optimal. Hence the reasonable search strategy for global optimal linear trail is to restrict to these β_i 's such that the ranks of corresponding B_{β_i} 's are smaller than a certain threshold.

4.5 Computer-aided search for Feistel round function

Linear trail. Then the search for optimal r -round linear trails is equivalent to the following problem to find vectors $(\beta^0, \mathbf{0}) \rightarrow (\mathbf{0}, \beta^0) \rightarrow (\beta^0, \beta^1) \rightarrow (\beta^1, \beta^2) \rightarrow \dots \rightarrow (\beta^i, \beta^{i+1}) \rightarrow (\beta^{i+1}, \beta^{i+2}) \rightarrow \dots$ satisfying the following conditions.

1) $(\beta_1^i + \beta^{i+1} \cdot F_{h+2}) + \beta_1^{i+2}$ is in the linear span of $n - h$ columns of $B_{\beta^{i+1}}$, $(\beta_2^i + \beta^{i+1} \cdot F_{h+1}) + \beta_2^{i+2}$ is in the linear span of h rows of $B_{\beta^{i+1}}$.

2) $\sum_{i=1} \text{rank}(B_{\beta^i})$ is as small as possible. The squared correlation of this linear trail is

$$\frac{1}{2^{2(\sum \text{rank}(B_{\beta^i}))}}.$$

5 The Maiorana-McFarland structure based linear cryptanalysis for Simon variants

In this Section we apply the Maiorana-McFarland structure-based linear cryptanalysis to the Simon variants. Around $\frac{1}{n}$ of all Simon variant parameter triples are figured out as weakest. We construct linear trails of arbitrary r rounds of Simon variants Simon $2n$ with probability $\frac{1}{2^{2r-2}}$ for these weakest parameter triples. Our results show that for some parameter triples, the constructive arbitrary round good linear trails from the Maiorana-McFarland structure-based linear cryptanalysis can be obtained directly. This is out of reach of the computer-aided search/solver used in [30].

For the Simon variant parameter triple (a, b, c) , since $\gcd(a - b, n) = 1$ we can assume that a is odd and b is even. We now expand the function

$$f_{a,b,c}(\mathbf{x}) = S^a(\mathbf{x}) \cdot S^b(\mathbf{x}) + S^c(\mathbf{x})$$

where $\mathbf{x} = (x_1, \dots, x_n)^\tau \in \mathbf{F}_2^n$, as

$$x_1F_1 + x_3F_3 + \dots + x_{n-1}F_{n-1} + G_1 + G_2,$$

where F_1, F_3, \dots, F_{n-1} are functions of x_2, x_4, \dots, x_n , and G_1 is the odd-position part of $S^c(\mathbf{x})$ and G_2 is even-position part of $S^c(\mathbf{x})$. The bit at the i -th position of $f_{a,b,c}(\mathbf{x})$ is

$$x_{i+a}x_{i+b} + x_{i+c}.$$

Then it is clear we can take the Maiorana-McFarland coordinates $i_1, i_2, \dots, i_{n/2}$ as all odd position coordinates. The coefficient vector F_i of x_i is

$$(0, \dots, x_{i+a-b}, 0, \dots, 0, \dots, 0, x_{i+b-a}, 0, \dots, 0)^\tau$$

where only nonzero coordinates are x_{i+a-b} at the $i - b$ position and x_{i+b-a} at the $i - a$ position.

Proposition 5.1 *We assume that $\gcd(a - b, n) = 1$. Then $\text{rank}(B_\beta) = 1$ when and only when $\text{wt}(\beta) = 1$ or $\text{wt}(\beta) = 2$ and the difference of the two nonzero positions of β is $|a - b|$. Suppose that $\text{wt}(\beta) = t$ and there are exactly $u \leq \lfloor \frac{t}{2} \rfloor$ pairs of nonzero positions with difference $|a - b|$ with each nonzero position counted once, then*

$$\text{rank}(B_\beta) = t - u.$$

Proof. This is direct computation. We assume a is odd and b is even. In the case β has only one non-zero i -th position, there are the following two possibilities. If i is odd, B_β has only one non-zero entry at $\frac{i+a}{2}$ column and $\frac{i+b+1}{2}$ row. If i is even, B_β has only one non-zero entry at $\frac{i+b}{2}$ column and $\frac{i+a+1}{2}$ row. The indices should be calculated module n . The conclusion follows directly.

Here the pairs of positions means that these pairs of indices are $i_1, i_2, \dots, i_l, \dots, j_1, j_2, \dots, j_l$ satisfy $j_1 - i_1 = b - a = 7, \dots, j_l - i_l = b - a = 7$, and

j_1, j_2, \dots, j_l is out of the set $\{i_1, \dots, i_l\}$. That is, each index can not be counted more than once in pairs.

Proposition 5.2. *In one of the following cases we have one arbitrary r -round linear trail of probability $\frac{1}{2^{\frac{1}{r}-2}}$ for the Simon variant with the parameter triple (a, b, c) .*

- 1) $2c \equiv 0 \pmod n$ or;
- 2) $b \equiv c \pmod n$ or;
- 3) $b + c \equiv 0 \pmod n$.

Proof. We construct the linear trail in the case 3). Let $\beta \in \mathbf{F}_2^n$ be a vector supported only at an arbitrary odd-position. Then the following linear characteristic satisfies the requirement. $(\beta, \mathbf{0}) \rightarrow (\mathbf{0}, \beta) \rightarrow (\beta, S^c(\beta)) \rightarrow (S^c(\beta), S^{2c}(\beta)) \rightarrow (S^{2c}(\beta), S^{3c}(\beta)) \rightarrow (S^{3c}(\beta), S^{4c}(\beta)) \rightarrow (S^{4c}(\beta), S^{5c}(\beta)) \rightarrow \dots$.

The linear trail in case 1) can be constructed as follows. $(\beta, \mathbf{0}) \rightarrow (\mathbf{0}, \beta) \rightarrow (\beta, S^c(\beta)) \rightarrow (S^c(\beta), \mathbf{0}) \rightarrow (\mathbf{0}, S^c(\beta)) \rightarrow (S^c(\beta), S^{2c}(\beta)) \rightarrow (S^{2c}(\beta), \mathbf{0}) \rightarrow \dots$.

The linear trail in case 2) can be constructed as follows. $(\beta, \mathbf{0}) \rightarrow (\mathbf{0}, \beta) \rightarrow (\beta, S^c(\beta)) \rightarrow (S^c(\beta), \beta) \rightarrow (\beta, \mathbf{0}) \rightarrow (\mathbf{0}, \beta) \rightarrow (\beta, S^c(\beta)) \rightarrow (S^c(\beta), \beta) \rightarrow (\beta, \mathbf{0}) \rightarrow \dots$.

Computer-aided search of linear trails for the Simon variants

We assume that a is odd and b is even. $\beta \in \mathbf{F}_2^n$ and B_β is a $\frac{n}{2} \times \frac{n}{2}$ matrix which is determined as follows. Suppose that β has only one non-zero i -th position. If i is odd, B_β has only one non-zero entry at $\frac{i+a}{2}$ column and $\frac{i+b+1}{2}$ row. If i is even, B_β has only one non-zero entry at $\frac{i+b}{2}$ column and $\frac{i+a+1}{2}$ row. The indices should be calculated module $\frac{n}{2}$. Then B_β is determined from the linearity.

Then $\text{rank}(B_\beta) = 1$ when and only when $\text{wt}(\beta) = 1$ or $\text{wt}(\beta) = 2$ and the difference of the two nonzero positions of β is $b - a = 7$.

Example 1. For $\beta = (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$, the matrix B_β is a rank 2 matrix as follows.

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Search. The search for optimal r -round linear trails for the Simon variants are equivalent to the following problem to find vectors $(\beta^1, \mathbf{0}) \rightarrow (\mathbf{0}, \beta^1) \rightarrow (\beta^1, \beta^2) \rightarrow (\beta^2, \beta^3) \rightarrow \dots \rightarrow (\beta^i, \beta^{i+1}) \rightarrow (\beta^{i+1}, \beta^{i+2}) \rightarrow \dots$ satisfying the following conditions.

1) The odd-position part of the vector $(\beta^i + S^c(\beta^{i+1}) + \beta^{i+2})$ is in the linear span of $\frac{n}{2}$ columns of $B_{\beta^{i+1}}$, the even-position part of $(\beta^i + S^c(\beta^{i+1}) + \beta^{i+2})$ is in the linear span of $\frac{n}{2}$ rows of $B_{\beta^{i+1}}$.

2) $\Sigma rank(B_{\beta^i})$ is as small as possible, where $rank(B_{\beta^i})$ can be calculated from Proposition 5.1. Then the squared correlation of the corresponding linear trail is

$$\frac{1}{2^{2(\Sigma rank(B_{\beta^i}))}}.$$

Our search strategy is to restrict to these masks such that their corresponding ranks are smaller than a certain threshold. This is reasonable not only for the Simon variants including the Simeck but also for other lightweight block cipher families. On the other hand we observe that the above search has no structural connection for various parameters $n = 16, 24, 32, 48, 64$ since S^2 and the formation of the matrix B_β . It has to search for each n and there is no transformation from chains of vectors in \mathbf{F}_2^n satisfying connecting condition 1) to chains of vectors in \mathbf{F}_2^{2n} satisfying connecting condition 1).

Proposition 5.3. *Around $\frac{3n}{2^{n+1}}$ fraction vectors of all nonzero vectors β in \mathbf{F}^n have their B matrices with their ranks 1. Around $\frac{9n(n-2)}{2^{n+2}}$ fraction vectors of all nonzero vectors β in \mathbf{F}^n have their B matrices with their ranks 2. Around $\frac{9n(n-1)(n-2)}{2^{n+1}}$ fraction vectors of all nonzero vectors β in \mathbf{F}^n have their B matrices with their ranks 3.*

Proof. This is direct from Proposition 5.1.

For Simon32, $n = 16$, around $\frac{1}{256}$ fractions of vectors in \mathbf{F}_2^{16} have their B matrices with rank 2. For Simon48, $n = 24$ around $\frac{297}{2^{22}}$ fractions of vectors in \mathbf{F}_2^{24} have their B matrices with rank 2.

6 Linear hull construction

The connecting condition 1) in the search for linear trails for Simon variant block ciphers as showed in the previous section is totally linear-algebraic. Hence this gives some "structures" on the whole set of linear trails, which is suitable to do linear hull, multiple linear or multidimensional linear cryptanalysis, see [49, 14, 26, 27, 28]. As noticed in [6, 2] for Simon block ciphers, linear trails with intermediate masks should be counted carefully to grantee the potential formula in [49] is correctly used. In our counting of different linear trails for Simon variant block ciphers, only linear trails with different intermediate masks on the left sides are counted. Hence the potential formula in [49] can be used in our linear hull construction.

6.1 Operations on linear trails

Proposition 6.1. *Let $\beta : (\beta^1, \mathbf{0}) \longrightarrow (\mathbf{0}, \beta^1) \longrightarrow (\beta^1, \beta^2) \longrightarrow (\beta^2, \beta^3) \longrightarrow \dots \longrightarrow (\beta^{t-1}, \beta^t)$ be a chain of vectors satisfying the connecting condition 1). The operation $S^c(\mathbf{x}) = (x_c, x_{c+1}, \dots, x_1, \dots, x_{c-1})$, where $\mathbf{x} = (x_1, \dots, x_n) \in \mathbf{F}_2^n$. For positive integer c , $S^c(\beta)$ is the chain of vectors $s^c(\beta^i)$. When c is even, $S^c(\beta)$ is another chain of vectors satisfying the condition 1).*

Proof. From Proposition 5.1 the contribution of rows and columns from B matrices are shifted by S^c , therefore the conclusion follows.

Proposition 6.2. *Let $\beta : (\beta^1, \mathbf{0}) \longrightarrow (\mathbf{0}, \beta^1) \longrightarrow (\beta^1, \beta^2) \longrightarrow (\beta^2, \beta^3) \longrightarrow \dots \longrightarrow (\beta^{t-1}, \beta^t)$ and $\gamma : (\gamma^1, \mathbf{0}) \longrightarrow (\mathbf{0}, \gamma^1) \longrightarrow (\gamma^1, \gamma^2) \longrightarrow (\gamma^2, \gamma^3) \longrightarrow \dots \longrightarrow (\gamma^{t-1}, \gamma^t)$ be two chains of t vectors in \mathbf{F}_2^n satisfying the connecting condition 1). Suppose that for any 1 coordinate in the $\text{supp}(\beta^{i+1}) \cap \text{supp}(\gamma^{i+1})$, the columns and rows corresponding to this 1 in $B_{\beta^{i+1}}$ and $B_{\gamma^{i+1}}$ are not used to construct β^{i+2} or γ^{i+2} for all $i = 0, \dots, t-2$. Then the sum of these two chains of vectors $\beta + \gamma : (\beta^1 + \gamma^1, \mathbf{0}) \longrightarrow (\mathbf{0}, \beta^1 + \gamma^1) \longrightarrow (\beta^1 + \gamma^1, \beta^2 + \gamma^2) \longrightarrow \dots$*

$(\beta^2 + \gamma^2, \beta^3 + \gamma^3) \longrightarrow \dots \longrightarrow (\beta^{t-1} + \gamma^{t-1}, \beta^t + \gamma^t)$ satisfies the connecting condition 1). In particular if $\text{supp}(\beta^{i+1}) \cap \text{supp}(\gamma^{i+1}) = \emptyset$, for $i = 0, \dots, t-2$, the sum of two chains of vectors satisfies the connecting condition 1).

Proof. This is direct from the condition 1).

Proposition 6.3. Let $\beta : (\beta^1, \beta^2) \longrightarrow (\beta^2, \beta^3) \longrightarrow \dots \longrightarrow (\beta^{t-1}, \beta^t)$ be a chain of vectors satisfying the connecting condition 1). Then $\beta^{\text{reverse}} : (\beta^t, \beta^{t-1}) \longrightarrow (\beta^{t-1}, \beta^{t-2}) \longrightarrow \dots \longrightarrow (\beta^2, \beta^1)$ is a chain of vectors satisfying the connecting condition 1).

Proof. This is direct from the condition 1).

From Proposition 6.3 we can glue two chains of vectors such that the first and the last two vectors are fixed arbitrary vectors in \mathbf{F}_2^{2n} . Then we can get a linear trail with the arbitrary input mask and output mask.

Proposition 6.1, Proposition 6.2 and Proposition 6.3 can be used to construct many linear trails with the same input mask and output mask, the correlation squares have to be calculated for each such linear trails. This can be completed with the aid of computer search about the condition

$$\text{supp}(\beta^{i+1}) \cap \text{supp}(\gamma^{i+1}) = \emptyset$$

and the squared correlation calculations. The "structures" of the whole set of linear trails can be used to do better linear hull construction. Notice our method is essentially different with the papers [24, 34].

Computer-aided search for linear hull construction 1.

For Simon2n we do the the following several steps to construct a good linear hull.

The 1st step: Construct a chain of vectors satisfying connecting condition 1), of length equal to the required round number, such that the Hamming weights of each vector in this chain is small, for example, upper bounded by 3 or 4. Operation in Proposition 6.3 can help to get such a chain of vectors. Set γ_{main} is the squared correlation of this main linear trail. For example, γ_{main} might be $\frac{1}{2^{6n}}$.

The 2nd step: Construct many short chains of vectors satisfying the connecting condition 1), of the length smaller than $\frac{n}{2}$ with vectors with low Hamming weights. The first vector is of the form $(\mathbf{0}, \beta^1)$ and the last vector is of the form $(\beta^u, \mathbf{0})$, where $u \leq \frac{n}{2}$. In many cases long linear trail in the 1st step is the glue of short chains of vectors found in the second step. That is, search of short chains of vectors satisfying the connecting condition 1) and with the small rank sum is sufficient.

The 3rd step: Using Proposition 6.2, to check if the intersection of supports of vectors in short chains in the 2nd step and some intervals of the 1st step chain is empty. If it is, we can add short chains to this interval of the main chain constructed in the 1st step, to get a new chain of vectors satisfying the connecting condition 1) from Proposition 6.2. If the intersection is not empty, using the operation S^c with an even positive integer c to move the supports of these short chains and test if the intersection is empty. Then in this way, a lot of new chains of vectors satisfying the connecting condition 1) and with the same input mask and output mask as the main linear trail constructed in the 1st step can be obtained.

In general the squared correlations of these Proposition 6.2 operated new linear trails are lower bounded by $\frac{\gamma_{main}}{2^T}$ for some positive integer T , if the number of new linear trails is very large, the good linear hull is obtained. More importantly, the linear trails in this hull has low Hamming weight intermediate masks.

Example 2. Consider the following 7 vectors in \mathbf{F}_2^{16} ,

$$\beta^1 = (0000000100000000),$$

$$\beta^2 = (0000010010000000),$$

$$\beta^3 = (1001000100000000),$$

$$\beta^4 = (0000000010010011),$$

$$\beta^5 = (1000000000000100),$$

$$\beta^6 = (0000010000000001),$$

$$\beta^7 = \mathbf{0}.$$

This is a chain of vectors satisfying the connecting condition 1) and the B matrices have their ranks at most 3. The rank sum of B matrices is 11.

Since β^6 is of Hamming weight 1 we can operate on this short chain $S^c(\beta)$ of vectors by Proposition 6.1, where c is an even number, and then glue to get long chain of vectors. We also can add some short chains of vectors of the form $S^c(\beta)$ to the long chain of vectors from Proposition 6.2.

6.2 Linear hull construction

We observe that if the input mask is fixed, in each step to construct β^{i+2} the columns and rows of the matrix $B_{\beta^{i+1}}$ can be used span a linear subspace of \mathbf{F}_2^n of the dimension equal to $2\text{rank}(B_{\beta^{i+1}})$. We only need the output mask is the same.

The construction of linear trails is as follows. From arbitrary first α^1 , the chains of vectors satisfying 1) are constructed in each step by using all possible α^{i+2} of the form

$$\alpha^i + S^c(\alpha^{i+1}) + \mathbf{v},$$

where \mathbf{v} takes all $2^{2\text{rank}(B_{\alpha^{i+1}})}$ possible vectors in the linear subspace of \mathbf{F}_2^n spanned by rows and columns of the matrix $B_{\alpha^{i+1}}$ as in the condition 1). Then we have a lot of chains of vectors as in the following Proposition 6.4.

Proposition 6.4. *For Simon $2n$ or Simon variant with cipher size $2n$, from an arbitrary input mask $(\mathbf{0}, \alpha^1)$ after arbitrary round R , we can construct a linear hull with the fixed output mask (α^R, α^{R+1}) . The potential is bigger than or equal to $\frac{1}{2^{2n}}$. The complexity to list all linear trails in this linear hull is $2^{2\sum_{i=1}^R(\text{rank}(B_{\alpha^i}))}$, where $\alpha : (\mathbf{0}, \alpha^1) \rightarrow (\alpha^1, \alpha^2) \rightarrow (\alpha^2, \alpha^3) \rightarrow \dots \rightarrow (\alpha^R, \alpha^{R+1})$ is a chain of vectors in \mathbf{F}_2^n satisfying the condition 1).*

Proof. For intermediate masks we only use different linear trails with different left components. Hence the problem indicated in [6] does not happen in our linear hull construction. From the first α^1 , in each step to construct α^{i+2} from α^i and α^{i+1} we use contributions from the linear span of rows and columns in the matrix $B_{\alpha^{i+1}}$ such that $B_{\alpha^{i+2}}$ has the maximal possible rank. Then we have a chain of vectors $\alpha : (\mathbf{0}, \alpha^1) \rightarrow (\alpha^1, \alpha^2) \rightarrow (\alpha^2, \alpha^3) \rightarrow \dots \rightarrow (\alpha^R, \alpha^{R+1})$ is a chain of vectors in \mathbf{F}_2^n satisfying the condition 1). For any other possible choices of α^{i+2} , the corresponding linear trails has squared correlations not smaller than the potential of this chain. Then the

squared correlation of each such linear trail is at least

$$\frac{1}{2^{2\sum_{i=1}^R(\text{rank}(B_{\alpha^i}))}}.$$

Notice that the number of linear trails constructed as above is upper bounded by

$$2^{2\sum_{i=1}^R(\text{rank}(B_{\alpha^i}))}.$$

We give the proof that the sum of squared correlations of above linear trails is 1. First of all we fixed all $\alpha^1, \dots, \alpha^R$, then there exact $2^{2\text{rank}(B_{\alpha^R})}$ possible α^{R+1} , the sum of all these $2^{2\text{rank}(B_{\alpha^R})}$ linear trails is

$$\frac{2^{2\text{rank}(B_{\alpha^R})}}{2^{\sum_{i=1}^R 2\text{rank}(B_{\alpha^i})}} = \frac{1}{2^{\sum_{i=1}^{R-1} 2\text{rank}(B_{\alpha^i})}}.$$

Then we fixed all $\alpha^1, \dots, \alpha^{R-1}$ and sum all squared correlations over all possible (α^R, α^{R+1}) . Notice the number of all such possible (α^R, α^{R+1}) is upper bounded by $2^{2(\text{rank}(B_{\alpha^{R-1}})+\text{rank}(B_{\alpha^R}))}$. The sum of squared correlations is exact

$$\frac{2^{2\text{rank}(B_{\alpha^{R-1}})}}{2^{\sum_{i=1}^{R-1} 2\text{rank}(B_{\alpha^i})}} = \frac{1}{2^{\sum_{i=1}^{R-2} 2\text{rank}(B_{\alpha^i})}}.$$

Continue this process the sum of all linear trails is exact 1.

There are at most 2^{2n} output masks (α^R, α^{R+1}) 's in \mathbf{F}_2^{2n} . By collecting linear trails with the same last two vectors in the chain of vectors among all above linear trails, we get a linear hull with the same input and output mask. The potential is at least $\frac{1}{2^{2n}}$. The conclusion follows.

Computer-aided listing of all linear trails in the hull 2.

Set $a = 1$, $b = 8$ and $c = 2$. $\beta \in \mathbf{F}_2^n$ and B_β is a $\frac{n}{2} \times \frac{n}{2}$ matrix defined as follows. Suppose that β has only one non-zero i -th position. If i is odd, B_β has only one non-zero entry at $\frac{i+1}{2}$ column and $\frac{i+9}{2}$ row. If i is even, B_β has only one non-zero entry at $\frac{i+8}{2}$ column and $\frac{i+2}{2}$ row. The indices should be calculated module $\frac{n}{2}$. Then B_β is determined from the linearity.

Search. To find a chain of vectors $(\mathbf{0}, \alpha^1) \rightarrow (\alpha^1, \beta^2) \rightarrow (\alpha^2, \alpha^3) \rightarrow \dots \rightarrow (\alpha^i, \alpha^{i+1}) \rightarrow (\alpha^{i+1}, \alpha^{i+2}) \rightarrow \dots$ satisfying the following conditions.

1) The odd-position part of the vector $(\alpha^i + S^c(\alpha^{i+1}) + \alpha^{i+2})$ is in the linear span of $\frac{n}{2}$ columns of $B_{\alpha^{i+1}}$, the even-position part of $(\alpha^i + S^c(\alpha^{i+1}) + \alpha^{i+2})$ is in the linear span of $\frac{n}{2}$ rows of $B_{\alpha^{i+1}}$.

2) In each step to construct α^{i+2} from the condition 1), we want find one such α^{i+2} with the maximal possible $rank(B_{\alpha^{i+2}})$.

3) Collecting linear trails with the last two vectors fixed.

4) Among 2^{32} possible last two vectors or output masks, there is at least one such output mask such the sum of squared correlations of linear trails with this fixed last two vectors or output mask, is at least $\frac{1}{2^{32}}$.

Using this search the required chains (linear trails) of vectors with the fixed two first vectors (input mask) and last two vectors (output mask) in Theorem 6.1 can be found. However there are too many linear trails and this search in Theorem 6.1 is not good enough to construct a nice linear hull.

We observe that if for some α^{i+1} , the matrix $B_{\alpha^{i+1}}$ is of rank $\frac{n}{2}$, then α^{i+2} can be an arbitrary vector in \mathbf{F}_2^n . In the above Proposition 6.4 the α^{i+2} after this vector in the chain can have the maximal rank. Hence the total rank sum in Proposition 6.4 and the complexity to list all linear trails in Proposition 6.4 is large. However if α^R is chosen as a fixed vector with smallest possible rank 1, this will help us to get the fixed right component α^{R+1} of the output mask among 2^n vectors in \mathbf{F}_2^n . The following result follows.

Corollary 6.1. *Let $t \leq \frac{n}{2}$ be a positive integer. In Proposition 6.4, among all chains of vectors with one fixed α^R with the property that $rank(B_{\alpha^R}) \leq t$, we collect linear trails with the same α^{R+1} , there is a linear hull with the fixed output mask (α^R, α^{R+1}) . The potential is at least $\frac{1}{2^{n+2t}}$.*

Hence it is proved that the input mask can be arbitrary and the left component of the output mask can be arbitrary. If a lot of chain of vectors are found such that the $R - 1$ -th vector α^{R-1} 's in all these chains of vectors have their $B_{\alpha^{R-1}}$ matrices of the full rank $\frac{n}{2}$, many chains of vectors with the above property can be constructed such that the final α^R of the maximal $rank(B_{\alpha^R})$ can be fixed as in Corollary 6.1. Then the last fixed α^{R+1} , the right component of the output mask can be an arbitrary fixed vector in \mathbf{F}_2^n . The potential is at least $\frac{1}{2^{2n}}$.

6.3 Glue of chains of vectors and the sum of the squared correlations

Let $\alpha : (\mathbf{0}, \alpha^1) \rightarrow (\alpha^1, \alpha^2) \rightarrow (\alpha^2, \alpha^3) \rightarrow \dots \rightarrow (\alpha^R, \alpha^{R+1})$ be a chain of vectors satisfying the connecting condition 1), and $\beta : (\mathbf{0}, \beta^1) \rightarrow (\beta^1, \beta^2) \rightarrow \dots \rightarrow (\beta^{R'}, \beta^{R'+1})$ be another chain of vectors satisfying the connecting condition 1). Assume that $(\alpha^R, \alpha^{R+1}) = (\beta^{R'+1}, \beta^{R'})$. From Proposition 6.3 we have a glued chain of vectors $\alpha \odot \beta : (\mathbf{0}, \alpha^1) \rightarrow (\alpha^1, \alpha^2) \rightarrow (\alpha^2, \alpha^3) \rightarrow \dots \rightarrow (\alpha^R, \alpha^{R+1}) = (\beta^{R'+1}, \beta^{R'}) \rightarrow (\beta^{R'}, \beta^{R'-1}) \rightarrow \dots \rightarrow (\beta^1, \mathbf{0})$. Using these glued chains of vectors linear trails with the same input mask and the same output mask can be obtained. We need to calculate the sum of squared correlations of all such glued linear trails.

We start from an arbitrary α^1 and reach a vector α^R with that the property the $\text{rank}(B_{\alpha^R}) = \frac{n}{2}$. Similarly we start from an arbitrary $(\mathbf{0}, \beta^1)$ and reach vector $\beta^{R'}$ with the property the $\text{rank}(B_{\beta^{R'}}) = \frac{n}{2}$. Then $(\alpha^{R+1}, \alpha^{R+2})$ can be an arbitrary vector in \mathbf{F}_2^{2n} and $(\beta^{R'+1}, \beta^{R'+2})$ can be an arbitrary vector in \mathbf{F}_2^{2n} . Then the above glued chains of vectors can be done for any two such chain of vectors.

Theorem 6.1. *From an arbitrary nonzero fixed first two vectors in \mathbf{F}_2^n , after at most $\frac{n}{2}$ vectors we have a chain of vectors satisfying the connecting condition 1) such that the B matrices of the last two vectors are of the full rank $\frac{n}{2}$. The sum of the squared correlations of above glued linear trails with the fixed input mask $(\mathbf{0}, \alpha^1)$, where $\alpha^1 \in \mathbf{F}_2^n$ is an arbitrary nonzero vector, and the fixed output mask of the the form $(\beta^1, \mathbf{0})$ where $\beta^1 \in \mathbf{F}_2^n$ is an arbitrary nonzero vector, is at least $\frac{1}{2^{2\text{rank}(B_{\alpha^{R+2}})}} = \frac{1}{2^{2\text{rank}(B_{\beta^{R'+1}})}} \geq \frac{1}{2^n}$.*

Proof. The first conclusion follows from a direct calculation. As in the proof of Proposition 6.4 we sum over fixed previous vectors, the only missing vector is $\alpha^{R+2} = \beta^{R'+1}$. The conclusion follows.

Notice that at the glue round, $\text{rank}(B_{\alpha^{R+2}}) = \text{rank}(B_{\beta^{R'+1}})$ can be from 1 to $\frac{n}{2}$, hence the real lower bound is much larger.

This glue method give us a better linear hull than Corollary 6.1. However the difference is only $\frac{1}{4}$. From Proposition 5.3 the fraction of linear trails with these intermediate masks with low rank B matrices in the hull is

significant. Since low rank B matrix implies that the low Hamming weight of the intermediate masks, it seems that in both Proposition 6.4 and Theorem 6.1, the fraction of linear trails with low Hamming weight masks in the constructed linear hull is not small.

Secondly for Simon2n, for a fixed squared correlation product (fixed rank sum), there are many linear trails (chain of vectors satisfying the connecting condition 1)) with the same rank sum. This observation shows that it seems not good to pick up only several linear trails with the largest squared correlation product, we should search a batch of linear trails with large squared correlation product.

6.4 Independent linear trails for linear key schedules

In this subsection we show hoe to construct linear trails which are independent for key schedule in the Simon. The main point of the construction is the linearity of the key schedule of Simon round keys.

Notice that the round keys are only XORed at left n bits and the key schedule is linear, then from Lemma 1 in [2], if two linear trails are not equal then they are independent. Hence for two linear trail with masks of the form $(\mathbf{a}_1, \dots, \mathbf{a}_R)$ and $(\mathbf{a}'_1, \dots, \mathbf{a}'_R)$, if $(a_1 \cdot \mathbf{A}_1 + \dots + \mathbf{a}_R \mathbf{A}_R) \cdot (k_0, \dots, k_{mn-1})^\tau \in \mathbf{F}_2^n$ is not equal to $(a'_1 \cdot \mathbf{A}_1 + \dots + \mathbf{a}'_R \mathbf{A}_R) \cdot (k_0, \dots, k_{mn-1})^\tau \in \mathbf{F}_2^n$, where $\mathbf{A}_1, \dots, \mathbf{A}_R$ are 16×64 matrices determined from the linear key schedule of Simon or its variants and k_0, \dots, k_{mn-1} are the mask keys, then these two linear trails are independent. Notice that there are 2^n possible values. Hence if for each such a value of $(a_1 \cdot \mathbf{A}_1 + \dots + \mathbf{a}_R \mathbf{A}_R) \cdot (k_0, \dots, k_{mn-1})^\tau$, pick up only a linear trail among the linear trails constructed in Theorem 6.2, with the maximal squared correlation. Then the sum of squared correlations of such independent linear trails is at least $\frac{1}{2^n} = \frac{1}{2^{2n}}$. However the potential is $\frac{1}{2^{2n}}$ only when for each value of $(a_1 \cdot \mathbf{A}_1 + \dots + \mathbf{a}_R \mathbf{A}_R) \cdot (k_0, \dots, k_{mn-1})^\tau \in \mathbf{F}_2^n$, the squared correlations of all these linear trails are the same. This is not true from a direct computation for Simon2n block cipher. Hence we have the following result. Actually from the above argument the realistic potential should be much larger.

Theorem 6.2. *For Simon 2n and its variants of at least n rounds, with the linear key schedule, we can construct a linear hull with the fixed input mask $(\mathbf{0}, \alpha^1)$, where $\alpha^1 \in \mathbf{F}_2^n$ is an arbitrary nonzero vector, and the fixed*

output mask of the the form $(\beta^1, \mathbf{0})$ where $\beta^1 \in \mathbf{F}_2^n$ is an arbitrary nonzero vector. These linear trails in this linear hull are independent for rounds keys. The potential of this linear hull is bigger than $\frac{1}{2^{2n}}$.

Actually in the process to pick out the linear trail of the largest squared correlation for each value in \mathbf{F}_2^n of the intermediate sum, only the average lower bound in given in the above argument of Theorem 6.3, hence the real potential should be much larger than $\frac{1}{2^{2n}}$. Observe Proposition 5.3 the low Hamming weight requirement is reasonable.

Computer-aided search for liner hull construction 3.

The 1st Step: Using Proposition 6.3 to get many chain of low Hamming weight vectors in \mathbf{F}_2^n . The length is the number of required round in the design. In this way, the input mask and the output mask is the same.

The 2nd Step: Check if the sum of the intermediate masks and round keys as above is the same, if the value is the same, only the linear trail with the largest squared correlation is picked out.

Finally we try to find such chain of vectors as more as possible. Then we get a linear hull consisting of linear trails which are independent for round keys. To calculate the potential of this linear hull to check if it is bigger than $\frac{4}{2^{2n}}$.

From the theoretical argument in Theorem 6,3 if without the low Hamming weight requirement in the 1st step, the potential should be large than $\frac{1}{2^{2n}}$.

6.5 Independence for different rounds

We observe that for a linear trail such that $\alpha_0 \cdot \mathbf{k}_0, \dots, \alpha_R \cdot \mathbf{k}_R$ are linear independent linear forms on \mathbf{F}_2^{mn} of master keys, where $\mathbf{k}_0, \dots, \mathbf{k}_R$ are round keys from the master keys, then the linear approximation of different rounds are linear independent, because the key schedule of Simon is linear. Hence the chains of vectors satisfying the connecting condition 1) lead to linear dependent form of master keys is at most $\frac{1}{2}$ in all summation in Proposition 6.4, Theorem 6.1 and 6.2. Thus the summation in potential over these round-linear-independent linear trails of the constructed linear hull should

be half of the summation as above. From this argument the real potential summing over round-linear-independent linear trails is also bigger than $\frac{1}{2^{2n}}$.

7 Linear hull construction for Feistel block ciphers with degree two restricted Maiorana-McFarland structure round functions

We observe the connecting condition 1) for the Feistel block ciphers with the degree two restricted Maiorana-McFarland round functions in Section 4.3.

Connecting condition 1). The search for optimal r -round linear trails is equivalent to the following problem to find vectors in \mathbf{F}_2^n , $(\beta^0, \mathbf{0}) \rightarrow (\mathbf{0}, \beta^0) \rightarrow (\beta^0, \beta^1) \rightarrow (\beta^1, \beta^2) \rightarrow \dots \rightarrow (\beta^i, \beta^{i+1}) \rightarrow (\beta^{i+1}, \beta^{i+2}) \rightarrow \dots$ satisfying the following conditions.

1) $(\beta_1^i + \beta^{i+1} \cdot F_{h+2}) + \beta_1^{i+2}$ is in the linear span of $n - h$ columns of $B_{\beta^{i+1}}$, $(\beta_2^i + \beta^{i+1} \cdot F_{h+1}) + \beta_2^{i+2}$ is in the linear span of h rows of $B_{\beta^{i+1}}$.

Similarly as the case for Simon we can consider the similar results as Theorem 6. 1 and 6.2 for this block cipher. In general the sum of squared correlations of all glued linear trails is at least $\frac{1}{2^n}$. The main problem is if the conclusion in Theorem 6.3 is true for the key-scheduling. The case of Simon and variants with linear key schedule are showed that linear hull with the large ELP can be constructed and the linear trails in the hull are independent.

Theorem 7.1. *Let $\mathbf{Feistel}(f)$ be a key-alternating Feistel block cipher with the degree two restricted Maiorana-McFarland round function f . The length of this block cipher is $2n$. Suppose the required number of rounds is large and the key schedule is linear. Then there is a linear hull with its potential at least $\frac{1}{2^{2n}}$.*

We speculate that the Feistel structure is not the key for the construction of above linear hull. It seems that the degree two restricted Maiorana-McFarland round functions lead to the existence of this kind of linear hull.

8 The Maiorana-McFarland structure based constructive differential cryptanalysis

8.1 General facts

For a Boolean permutation $\Phi : \mathbf{F}_2^m \rightarrow \mathbf{F}_2^m$ and two given difference α and β , the differential probability is

$$P(\alpha \rightarrow \beta) = \frac{|\{\mathbf{x} \in \mathbf{F}_2^m : \Delta_\alpha(\mathbf{x}) = \beta\}|}{2^m},$$

where $\Delta_\alpha(\mathbf{x}) = \Phi(\mathbf{x} + \alpha) + \Phi(\mathbf{x})$. Then the differential probability of several rounds with differences $\alpha_1, \dots, \alpha_r$ is

$$P(\alpha_1 \rightarrow \dots \rightarrow \alpha_r) = P(\alpha_1 \rightarrow \alpha_2)P(\alpha_2 \rightarrow \alpha_3) \cdots P(\alpha_{r-1} \rightarrow \alpha_r)$$

if α_i is transformed to α_{i+1} by the round function. For the fixed input difference α_1 and the output difference α_r , the expected differential probability is

$$EDP(\alpha_1 \rightarrow \alpha_r) = \sum_{\alpha_2, \dots, \alpha_{r-1}} P(\alpha_1 \rightarrow \alpha_2)P(\alpha_2 \rightarrow \alpha_3) \cdots P(\alpha_{r-1} \rightarrow \alpha_r)$$

if the round keys are assumed independent and uniformly random, we refer to [33, 25].

The following simple result means that the difference at the Maiorana-McFarland structure coordinates leads to simple function difference.

Theorem 8.1. *Let Φ be a Boolean mapping with the Maiorana-McFarland structure at the variables x_{i_1}, \dots, x_{i_h} . Set*

$$\mathbf{v}_{\mathbf{I}} = (0, \dots, 1, \dots, 1, 0)$$

the vector in \mathbf{F}_2^m only supported at subset $\mathbf{I} \subset \{i_1, \dots, i_h\}$. We have

$$\Delta_{\mathbf{v}}(\mathbf{x}) = \Phi_t(x_1, \dots, x_{i_1} + 1, \dots, x_{i_h} + 1, \dots, x_m) + \Phi_t(x_1, \dots, x_m) = \sum_{j \in \mathbf{I}} G_t^j.$$

Proof. This is direct from the expansion in the Definition 3.1.

In the case that the Maiorana-McFarland structure coordinates can be distinguished from a Boolean permutation f , Theorem 5.1 can be used to establish the output differential

$$(\dots \sum_{j \in \mathbf{I}} G_t^j \dots)$$

at the positions

$$\{t : \sum_{j \in \mathbf{I}} G_t^j \neq 0\}$$

with the input difference $\mathbf{v}_{\mathbf{I}}$. There are 2^h such input differences. The advantage of such input-output differential pairs is as follows, the identity

$$\Phi((x_1, \dots, x_m) + \mathbf{v}_{\mathbf{I}}) + \Phi(x_1, \dots, x_m) = (\dots \sum_{j \in \mathbf{I}} G_t^j \dots)$$

is valid for all Maiorana-McFarland structure variable coordinates x_{i_1}, \dots, x_{i_h} .

Probability calculation. Let $\mathbf{G}_{\mathbf{I}} = \sum_{j \in \mathbf{I}} G^j$, for any given \mathbf{v} in the image $\mathfrak{S}\mathbf{G}_{\mathbf{I}} \subset \mathbf{F}_2^m$, let $\mathbf{G}_{\mathbf{I}, \mathbf{v}} = \{\hat{\mathbf{x}} : \mathbf{G}_{\mathbf{I}}(\hat{\mathbf{x}}) = \mathbf{v}\}$, where $\hat{\mathbf{x}}$ is the vector of variables in $\{x_1, \dots, x_m\} - \{x_{i_1}, \dots, x_{i_h}\}$. The probability that a vector $\mathbf{x} \in \mathbf{F}_2^m$ leads to the the input-output difference relation

$$f(\mathbf{x} + \mathbf{v}_{\mathbf{I}}) + f(\mathbf{x}) = \mathbf{v}$$

is

$$P(\mathbf{v}_{\mathbf{I}} \longrightarrow \mathbf{v}) = \frac{|\mathbf{G}_{\mathbf{I}, \mathbf{v}}| \cdot 2^h}{2^m} = \frac{|\mathbf{G}_{\mathbf{I}, \mathbf{v}}|}{2^{m-h}},$$

where $\frac{|\mathbf{G}_{\mathbf{I}, \mathbf{v}}|}{2^{m-h}}$ is just the probability about the variables in the set $\{x_1, \dots, x_m\} - \{x_{i_1}, \dots, x_{i_h}\}$. Here it is very interesting to notice that the probability only depends on the variables in the set $\{x_1, \dots, x_m\} - \{x_{i_1}, \dots, x_{i_h}\}$. This is because the Maiorana-McFarland structure-based input-output relation Theorem 6.1 holds for any given inputs of variables of $\{x_{i_1}, \dots, x_{i_h}\}$. It is clear that when the Maiorana-McFarland number h becomes bigger the probability as above becomes bigger. Then the high Maiorana-McFarland number perhaps leads to high probability differential characteristics.

8.2 The Maiorana-McFarland structure based differential trails when the algebraic degree of round functions is 2

When the Boolean permutations with the Maiorana-McFarland structure are of algebraic degree two, it is obvious that Boolean mappings G_t^j and G_t are algebraic degree one Boolean mappings from $\mathbf{F}_2^{m-h} \rightarrow \mathbf{F}_2^n$. Hence G_t^j, G_t 's are linear. This in this case establishing the Maiorana-McFarland structure based differential trails from Theorem 8.1 is easy.. Let $\mathbf{I} \subset \{i_1, \dots, i_h\}$ and

$$\mathbf{G}_{\mathbf{t}, \mathbf{I}} = \sum_{j \in \mathbf{I}} G_t^j$$

be the mapping from \mathbf{F}_2^{m-h} to \mathbf{F}_2^n . The image $\mathfrak{S}(\mathbf{G}_{\mathbf{I}})$ of $\mathbf{G}_{\mathbf{I}}$ is the main point in the Maiorana-McFarland structure-based differential cryptanalysis.

8.3 Establishing t -round differential trails

The following result is direct from the Maiorana-McFarland structure computation.

Corollary 8.1. *Let $\Phi : \mathbf{F}_2^m \rightarrow \mathbf{F}_2^m$ be an algebraic degree two Boolean mapping. It has the Maiorana-McFarland structure at the variables x_{i_1}, \dots, x_{i_h} . Suppose that there exists a subset $\mathbf{I} \subset \{i_1, \dots, i_h\}$ such that $\mathbf{G}_{\mathbf{I}}$ be a linear mapping on variables in the set $\{x_1, \dots, x_m\} - \{x_{i_1}, \dots, x_{i_h}\}$. For any given $\mathbf{v} \in \mathfrak{S}\mathbf{G}_{\mathbf{I}} \subset \mathbf{F}_2^b$, let $\mathbf{G}_{\mathbf{I}, \mathbf{v}} = \{\hat{\mathbf{x}} : \mathbf{G}_{\mathbf{I}}(\hat{\mathbf{x}}) = \mathbf{v}\}$, where $\hat{\mathbf{x}}$ is the vector of variables in $\{x_1, \dots, x_b\} - \{x_{i_1}, \dots, x_{i_h}\}$. Then we have a message space $\mathbf{E}_{(M, M')} = \{(M, M') : M \in \mathbf{G}_{\mathbf{I}, \mathbf{v}}, M' = M + \mathbf{v}\}$ such that $\Phi(M) + \Phi(M') = \mathbf{v}$ for each $(M, M') \in \mathbf{E}_{(M, M')}$. $\mathbf{E}_{(M, M')}$ is an affine space of dimension $\dim(\mathbf{G}_{\mathbf{I}, \mathbf{v}})$.*

For the purpose to get t -round algebraic equations of the differential trails for the Boolean mapping $\Phi : \mathbf{F}_2^m \rightarrow \mathbf{F}_2^m$, where Φ is a composition of degree two Boolean permutations, we need to do the Maiorana-McFarland structure based differential consecutively as follows.

First at the last t -round, we need to find as more Maiorana-McFarland structure variables $x_{i_1}, \dots, x_{i_{h_t}}$ as possible and a subset $\mathbf{I}_t \subset \{i_1, \dots, i_{h_t}\}$, such that $\mathbf{v} \in \mathfrak{S}(\mathbf{G}_{\mathbf{I}_t})$. Then the t -round condition of the form

$$\mathbf{G}_{\mathbf{I}_t}(\mathbf{x} + \mathbf{k}_{t-1}) = \mathbf{v}$$

for $\mathbf{x} + \mathbf{k}_{t-1} \in \mathbf{F}_2^{m-h_t}$ is imposed, where \mathbf{k}_{t-1} is the non Maiorana-McFarland part of the $t - 1$ -th round keys.

Secondly at the $t - 1$ -round, we need to find as more Maiorana-McFarland structure variables $x_{i_1}, \dots, x_{i_{h_{t-1}}}$ as possible and a subset $\mathbf{I}_{t-1} \subset \{i_1, \dots, i_{h_{t-1}}\}$, such that $\mathbf{v}_{\mathbf{I}_t} \in \mathfrak{S}(\mathbf{G}_{\mathbf{I}_{t-1}})$. Then the $(t - 1)$ -round condition of the form

$$\mathbf{G}_{\mathbf{I}_{t-1}}(\mathbf{x} + \mathbf{k}_{t-2}) = \mathbf{v}_{\mathbf{I}_t}$$

for $\mathbf{x} + \mathbf{k}_{t-2} \in \mathbf{F}_2^{m-h_{t-1}}$ is imposed, where \mathbf{k}_{t-2} is the non Maiorana-McFarland part of the $t - 2$ -th round keys. Here $\mathbf{v}_{\mathbf{I}_t} \in \mathbf{F}_2^m$ is the support vector of the coordinate positions of the subset $\mathbf{I}_t \subset \{i_1, \dots, i_{h_t}\}$.

Thirdly at the $t - 2$ -round, we need to find as more Maiorana-McFarland structure variables $x_{i_1}, \dots, x_{i_{h_{t-2}}}$ as possible and a subset $\mathbf{I}_{t-2} \subset \{i_1, \dots, i_{h_{t-2}}\}$,

such that $\mathbf{v}_{\mathbf{I}_{t-1}} \in \mathfrak{S}(\mathbf{G}_{\mathbf{I}_{t-2}})$. Then the $(t-2)$ -round condition of the form

$$\mathbf{G}_{\mathbf{I}_{t-2}}(\mathbf{x} + \mathbf{k}_{t-3}) = \mathbf{v}_{\mathbf{I}_{t-1}}$$

for $\mathbf{x} \in \mathbf{F}_2^{m-h_{t-2}}$ is imposed, where \mathbf{k}_{t-3} is the non Maiorana-McFarland part of the $t-3$ -th round keys. Here $\mathbf{v}_{\mathbf{I}_{t-1}} \in \mathbf{F}_2^m$ is the support vector of the coordinate positions of the subset $\mathbf{I}_{t-1} \subset \{i_1, \dots, i^{h_{t-1}}\}$.

We can continue this process to the the first round. Combining all round conditions

$$\begin{aligned} \mathbf{G}_{\mathbf{I}_t}(\Phi^{t-1}(\mathbf{x}) + \mathbf{k}_{t-1}) &= \mathbf{v}, \\ \mathbf{G}_{\mathbf{I}_{t-1}}(\Phi^{t-2}(\mathbf{x}) + \mathbf{k}_{t-2}) &= \mathbf{v}_{\mathbf{I}_t}, \\ \mathbf{G}_{\mathbf{I}_{t-2}}(\Phi^{t-3}(\mathbf{x}) + \mathbf{k}_{t-3}) &= \mathbf{v}_{\mathbf{I}_{t-1}}, \\ &\dots\dots, \\ \mathbf{G}_{\mathbf{I}_1}(\mathbf{x} + \mathbf{k}_0) &= \mathbf{v}_{\mathbf{I}_2}. \end{aligned}$$

This is a system of algebraic equations on the initial input bits in \mathbf{F}_2^m .

Here it is important to notice that though in the $(t-i)$ -round conditions where $i < t$, it is linear, the linear conditions $\mathbf{G}_{\mathbf{I}_{t-i}}$ is imposed on $\Phi_{t-i-1} \circ \dots \circ \Phi_1(\mathbf{x})$. Hence this system of equations is not linear.

8.4 Independent condition and inconsistency

When the above algebraic equations are independent, then the probability of the above Maiorana-McFarland structure based differential characteristic is

$$P(\mathbf{v}_{\mathbf{I}_1} \longrightarrow \mathbf{v}_{\mathbf{I}_2} \longrightarrow \dots \longrightarrow \mathbf{v}) = \frac{|\mathbf{G}_{\mathbf{I}_t, \mathbf{v}}|}{2^{m-h}} \cdot \frac{|\mathbf{G}_{\mathbf{I}_{t-1}, \mathbf{v}_{\mathbf{I}_t}}|}{2^{m-h}} \dots \frac{|\mathbf{G}_{\mathbf{I}_1, \mathbf{v}_{\mathbf{I}_2}}|}{2^{m-h}}.$$

If $\mathbf{G}_{\mathbf{I}_t}, \mathbf{G}_{\mathbf{I}_{t-1}}, \dots, \mathbf{G}_{\mathbf{I}_1}$ are independent linear mappings, then the above algebraic equations are independent.

As indicated in [45, 37, 38], some discovered differential trails of permutation based hash functions by computer-aided search/solver are always invalid since contradictions may easily occur in the set of conditions implied in the discovered differential trails. In the above Maiorana-McFarland

structure based differential trails the existence of real differential trail is formulated by a system of algebraic equations as follows.

$$\begin{aligned}
\mathbf{G}_{\mathbf{I}_t}(\Phi^{t-1}(\mathbf{x}) + \mathbf{k}_{t-1}) &= \mathbf{v}, \\
\mathbf{G}_{\mathbf{I}_{t-1}}(\Phi^{t-2}(\mathbf{x}) + \mathbf{k}_{t-2}) &= \mathbf{v}_{\mathbf{I}_t}, \\
\mathbf{G}_{\mathbf{I}_{t-2}}(\Phi^{t-3}(\mathbf{x}) + \mathbf{k}_{t-3}) &= \mathbf{v}_{\mathbf{I}_{t-1}}, \\
&\dots\dots, \\
\mathbf{G}_{\mathbf{I}_1}(\mathbf{x} + \mathbf{k}_0) &= \mathbf{v}_{\mathbf{I}_2}.
\end{aligned}$$

If we can find a solution of this system of algebraic equations, then we get a desired real differential trail. When the round number is not big, this method is efficient. The Maiorana-McFarland structure based differential cryptanalysis can be thought as deterministic and constructive. If the above algebraic conditions are independent, the differential probability of a difference trail is indeed the product of round differential probability, that is, the conditions at each round is indeed independent.

8.5 Computer-aided search

Global optimal. The optimal Maiorana-McFarland structure based r -round differential trail problem can be formulated as follows. Find subsets $\mathbf{I}_1, \dots, \mathbf{I}_r$ satisfying that

$$\sum_{j=1}^{r-1} |\mathbf{G}_{\mathbf{I}_j, \mathbf{v}_{\mathbf{I}_{j+1}}}|$$

is as small as possible.

Local optimal. For given $\mathbf{v}_{\mathbf{I}_{r+1}}$ we find one subset $\mathbf{I}_t \subset \{i_1, \dots, i_t\}$ such that

$$|\mathbf{G}_{\mathbf{I}_t, \mathbf{v}_{\mathbf{I}_{r+1}}}|$$

is as small as possible. Then for given subset \mathbf{I}_r and the vector $\mathbf{v}_{\mathbf{I}_r}$ we find one subset $\mathbf{I}_{r-1} \subset \{i_1, \dots, i_t\}$ such that

$$|\mathbf{G}_{\mathbf{I}_{r-1}, \mathbf{v}_{\mathbf{I}_r}}|$$

is as small as possible.

In general local optimal does not give the global optimal. Hence the search complexity is large.

9 The Maiorana-McFarland structure based differential cryptanalysis of the Simon variants

9.1 Difference vectors

In this Section we apply the Maiorana-McFarland structure-based differential cryptanalysis to the Simon variants. Around $\frac{1}{n}$ of all Simon variant parameter triples are figured out as weakest. We construct linear and differential characteristics of arbitrary r rounds of Simon variants Simon $2n$ with probability $\frac{1}{2^{2r-2}}$ for these weakest parameter triples. Our results show that for some parameter triples, the constructive arbitrary round good linear and differential characteristics from the Maiorana-McFarland structure-based cryptanalysis can be obtained directly. Much better linear hull effect with more rounds is also presented.

For the Simon variant parameter triple (a, b, c) , since $\gcd(a - b, n) = 1$ we can assume that a is odd, b is even and c is even. Consider the Boolean permutation

$$f_{a,b,c}(\mathbf{x}) = S^a(\mathbf{x}) \cdot S^b(\mathbf{x}) + s^c(\mathbf{x}),$$

we can take the Maiorana-McFarland coordinates $i_1, i_2, \dots, i_{n/2}$ as all odd-position coordinates or all even position coordinates. For each Maiorana-McFarland coordinate x_i the coefficient vector G^i of x_i is

$$(0, \dots, x_{i+a-b}, 0, \dots, 1, 0, \dots, x_{i+b-a}, 0, \dots, 0)^T$$

where only nonzero coordinates are x_{i+a-b} at the $i-b$ position, 1 at the $i-c$ position and x_{i+b-a} at the $i-a$ position. Let $\mathbf{e} = (0000000100000000)$, then $\Delta_{\mathbf{e}}(f) = f(\mathbf{x} + \mathbf{e}) + f(\mathbf{x}) = (000001x_{15}00000000x_1)$. This simple example shows that for an input difference vector α , the output difference vector β can non be arbitrary since the 6-th coordinate is always 1.

Therefore if we take even number position coordinates as Maiorana-McFarland variable and construct differential trail as in Theorem 8.1, for each difference vector α supported only at even number positions, in the image $\mathfrak{S}(\Delta_{\alpha}(f))$, for $i \in \text{supp}(\alpha)$, the coordinate at the odd number $i - a$ position has to be zero. Hence we need impose $wt_H(\alpha)$ conditions on the coordinates at odd number position variables such that the next round difference vector is always supported at even number positions.

The differential trail is of the form $(\alpha^2, \alpha^1) \longrightarrow (\alpha^3, \alpha^2) \longrightarrow \dots \longrightarrow (\alpha^{i+1}, \alpha^i) \longrightarrow (\alpha^{i+2}, \alpha^{i+1})$, where $\alpha^i \in \mathbf{F}_2^n$. The connecting condition is as follows,

$$\alpha^{i+2} = \mathbf{v} + \alpha^i,$$

where f is the round function in Simon variant block cipher, $\mathbf{v} \in \mathfrak{S}(\Delta_{\alpha^{i+1}}(f))$. Here $\Delta_{\alpha^{i+1}}(f)$ is the affine mapping from $\mathbf{F}_2^{\frac{n}{2}}$ of non Maiorana-McFarland variables, that is, the affine mapping from $\frac{n}{2}$ odd position variables to \mathbf{F}_2^n . We call such a chain of difference vectors admissible if all α^i 's are supported only at even number positions, such that the Maiorana-McFarland structure based differential trails can be constructed as in Theorem 8.1. The differential probability of an admissible chain of difference vectors is

$$\frac{1}{2^{\sum_{j=1}^R wt_H(\alpha^j)}}$$

We figure out some Simon variant parameter triples with large differential probability.

Theorem 9.1. *For Simon variant with block size $2n$ and parameter triple (a, b, c) , suppose that (a, b, c) satisfies one of the following conditions*

- 1) $a \equiv c \pmod n$ or;
- 2) $b \equiv c \pmod n$ or
- 3) $b + c \equiv a \pmod n$.

Then there is a differential trail of arbitrary round r with the probability $\frac{1}{2^{2r-2}}$.

Proof. In the case of Simon variants with parameter triple (a, b, c) satisfying $a \equiv c \pmod n$ or $b \equiv c \pmod n$. The above G^i of x_i is $(0, \dots, x_{i+b-a} + 1, 0, \dots, x_{i+a-b}, 0, \dots, 0)^\tau$ where only nonzero coordinates are x_{i+a-b} at the $i - b$ position, $1 + x_{i+b-a}$ at the $i - a$ position if $a = c$, or the G^i is $(0, \dots, x_{i+b-a}, 0, \dots, x_{i+a-b} + 1, 0, \dots, 0)^\tau$ where only nonzero coordinates are $x_{i+b-a} + 1$ at the $i - b = i - c$ position, x_{i+a-b} at the $i - b$ position if $b = c$. In both cases we have a long differential characteristic of arbitrary r round with probability $\frac{1}{2^{2r-2}}$ of the difference chain $(Left : 0, \dots, 1, \dots, 0, Right : 0, 0, \dots, 0) \longrightarrow (Left : 0, \dots, 0, Right : 0, \dots, 1, \dots, 0) \longrightarrow (Left : 0, \dots, 1, \dots, 0, Right : 0, 0, \dots, 0) \longrightarrow (Left : 0, \dots, 0, Right : 0, \dots, 1, \dots, 0) \longrightarrow \dots$.

In case 3) we consider the following chain of Maiorana-McFarland variable positions

$$(i|i-c) \longrightarrow (i-b+a|i) \longrightarrow (i-2b+2a|i-b+a) \longrightarrow (i-3b+3a|i-2b+2a) \longrightarrow \dots$$

In this process the nonzero coordinates 1's at the positions $i-c$, $i-b+a-c$, $i-2b-c+2a$, $i-3b-c+3a$, \dots are vanished by the 1's from the right positions i , $i-b+a$, $i-2b+2a$, \dots from the fact $i-hb-c+h)a \equiv i-(h-1)b+(h-1)a \pmod n$. The conclusion follows immediately.

9.2 Operations on differential trails

Then we have the following operations on differential trails as in the linear hull case.

Proposition 9.1. *For an admissible chain of difference vectors α , $S^c(\alpha)$ is another admissible chain of difference vectors if c is an even number. For two admissible chain of difference vectors $\alpha : (\alpha^2, \alpha^1) \longrightarrow (\alpha^3, \alpha^2) \longrightarrow \dots \longrightarrow (\alpha^{i+1}, \alpha^i) \longrightarrow (\alpha^{i+2}, \alpha^{i+1})$ and $\beta : (\beta^2, \beta^1) \longrightarrow (\beta^3, \beta^2) \longrightarrow \dots \longrightarrow (\beta^{i+1}, \beta^i) \longrightarrow (\beta^{i+2}, \beta^{i+1})$, if $\text{supp}(\alpha^i) \cap \text{supp}(\beta^i) = \emptyset$, then the sum $\alpha + \beta : (\alpha^2 + \beta^2, \alpha^1 + \beta^1) \longrightarrow (\alpha^3 + \beta^3, \alpha^2 + \beta^2) \longrightarrow \dots \longrightarrow (\alpha^{i+1} + \beta^{i+1}, \alpha^i + \beta^i) \longrightarrow (\alpha^{i+2} + \beta^{i+2}, \alpha^{i+1} + \beta^{i+1})$ is another admissible chain of difference vectors.*

Proof. The first conclusion is obvious. The second conclusion follows from $\Delta_{\alpha+\beta}(f) = \Delta_\alpha(f) + \Delta_\beta(f)$ when α and β are only supported at even number positions. If $\text{supp}(\alpha^i) \cap \text{supp}(\beta^i) = \emptyset$, the sum of images of two affine mappings is the direct sum of affine subspaces.

Proposition 9.2. *Let $\beta : (\beta^2, \beta^1) \longrightarrow (\beta^3, \beta^2) \longrightarrow \dots \longrightarrow (\beta^t, \beta^{t-1})$ be an admissible chain of difference vectors. Then $\beta^{\text{reverse}} : (\beta^{t-1}, \beta^t) \longrightarrow (\beta^{t-2}, \beta^{t-1}) \longrightarrow \dots \longrightarrow (\beta^2, \beta^1)$ is another admissible chain of difference vectors.*

9.3 EDP lower bound under independence assumptions

From an arbitrary nonzero fixed input difference vector supported only at even positions, at the first round the input difference vector is $(\alpha^2, \alpha^1) \neq \mathbf{0}$, at each next round connecting, we impose the conditions that the odd position coordinates of $\Delta_{\alpha^{i+1}}(f)$ are zero, and the even position coordinates

can be 0 and 1. Then we imposed $wt_H(\alpha^{i+1})$ linear conditions, and the output difference vector can be nonzero vector in an affine space of dimension $wt_H(\alpha^{i+1})$. Hence the probability is $\frac{1}{2^{wt_H(\alpha^{i+1})}}$ and we get

$$2^{\sum_{i=1}^R wt_H(\alpha^i)}$$

admissible chains of difference vectors.

Proposition 9.3. *The sum of differential probabilities over all above admissible chains of difference vectors is 1.*

Proof. The proof is similar to the proof of Proposition 6.4. If we fix the first $j - 1$ vectors in the admissible chain, in the step to get the j -th vector, the $wt_H(\alpha^{j-1})$ linear conditions are imposed and we get $wt_H(\alpha^{j-1})$ next round nonzero difference vectors. Hence the sum is always 1.

We start from an arbitrary (α^2, α^1) supported only at even positions, and reach a vector (α^t, α^{t-1}) with the property that the dimension of $\mathfrak{S}(\Delta_{\alpha^{t-2}}(f))$ is $\frac{n}{2}$. Similarly we start from an arbitrary (α^{R+1}, α^R) and reach vector $(\alpha^{t'}, \alpha^{t'-1})$ with the property that the dimension of $\mathfrak{S}(\Delta_{\alpha^{t'-2}}(f))$ is $\frac{n}{2}$. Then (α^{t+1}, α^t) and $(\alpha^{t'+1}, \alpha^{t'})$ can be arbitrary vectors in \mathbf{F}_2^{2n} supported at even positions. From Proposition 9.2 the above two admissible chains of difference vectors can be glued to an admissible chain of difference vectors.

Theorem 9.2. *For an arbitrary fixed nonzero input difference vector $(\alpha^2, \alpha^1) \in \mathbf{F}_2^{2n}$ supported only at even positions, and an arbitrary nonzero output difference vector $(\alpha^{R+1}, \alpha^R) \in \mathbf{F}_2^{2n}$ supported at even positions, we have a set of admissible chains of difference vectors with input difference vector (α^2, α^1) at the 1st round and output difference vector (α^{R+1}, α^R) at the R -th round, such that the sum of all differential probability is at least $\frac{1}{2^{\frac{n}{2}}}$.*

Proof. This is similar to the proof of Theorem 6.1, we sum over fixed previous vectors, the only missing vector is $\alpha^{t+1} = \alpha^{t'+1}$. The conclusion follows.

9.4 Real EDP lower bound for key scheduling

It is obvious for two different admissible chains of difference vectors, the set of points satisfying the input-output difference relation is disjoint. Hence

the main problem is the existence of the real difference trails, that is, we need to prove the expected differential probability over all real differential trails is at least $O(\frac{1}{2^{2n}})$ for Simon2n. As argued in the previous section, when the EDP is only summed over all admissible chains of difference vectors in which the algebraic equations establishing this differential trail are independent, this is very close to the real probability when the key schedule is used. We observe that there are $2n + mn$ free variables used in Simon2n. Therefore, if the total number of algebraic equations to establish the differential trail is smaller than $2n + mn$ the differential trail seems realistic. In algebraic equations in Subsection 8.3-8.4, if there is a new degree one variable for each new algebraic equation, it is reasonable to assume that the independence of these algebraic equations and the realistic existence of the differential trail. Notice that the key scheduling in Simon2n is linear, new degree one master keys are involved in the different rounds. Therefore in Theorem 9.2, we only sum over such admissible chains of difference vectors such that in these algebraic equations of Subsection 8.3-8.4, there is a new degree one variable among these $2n + mn$ free variables in each algebraic equation. It seems even EDP is only summed over such realistic difference trails, the lower bound is still bigger than $\frac{1}{2^{2n}}$.

10 Conclusion

Linear cryptanalysis initiated from [42] is a general method to analyze block ciphers, and the key-recovery attack based on linear hull proposed in [49] is a powerful extended version. In this paper we show that when the round functions of the block ciphers have the restricted Maiorana-McFarland structure and of degree two, the search of linear trails of these block ciphers are essentially linear algebraic and better linear hull can be constructed. Theoretically Simon2n with linear key schedule is insecure for the key-recovery attack from our new constructed linear hulls of the potential bigger than $\frac{1}{2^{2n}}$.

Similarly the lower bound $\frac{1}{2^{\frac{n}{2}}}$ on the expected differential probability over all admissible chains of difference vectors, that is, over all Maiorana-McFarland structure based differential trails with the fixed input and output differences for Simon2n, is given under independence assumptions. We then argue that even when EDP is summed over all low dimension $\mathfrak{S}(\Delta_\alpha(f))$ realistic difference vectors, it is bigger than $\frac{1}{2^{2n}}$. Both linear hull construction and EDP lower bound shows that at least theoretically Simon2n with linear

key schedule is insecure.

The key-recovery attack based on linear hull and differential trails on Simon2n constructed from the restricted Maiorana-McFarland structure of round functions presented in this paper illustrates that the Maiorana-McFarland structure of the round function or the compositions of several rounds of round functions is indeed a weakness for the cryptanalyst to utilize. Hence it is interesting and necessary to understand the possible Maiorana-McFarland structures of compositions of round functions of lightweight cryptography primitives.

References

- [1] F. Abed, E. List, S. Lucks and J. Wenzel, Differential Cryptanalysis of Round-Reduced Simon and Speck, FSE 2014, LNCS 8540, pp. 525-545, 2014.
- [2] M. A. Abdelraheem, M. Ågren, P. Beelen and G. Leander, On the distributions of linear biases: Three instructive examples, Crypto 2012, LNCS 7417, pp. 50-67, 2012.
- [3] M. A. Abdelraheem, J. Alizadeh, H. A. Alkhzaimi, M. R. Aref, N. Bagheri and P. Gauravaram, Improved linear cryptanalysis of reduced-round Simon-32 and Simon-48, Indocrypt 2015, LNCS 9462, pp. 153-179, Cryptology ePrint, 2015/988, 2015.
- [4] J. Alizadeh, H. A. Alkhzaimi, M. R. Aref, N. Bagheri, P. Gaurawaram, A. Kumar, M. M. Lauridsen and S. K. Sanadhya, Cryptanalysis of the SIMON variants with connections, RFIDSec., LNCS 8651, pp. 90-107, 2014.
- [5] R. Almkhelifi and P. Vora, Linear cryptanalysis of round-reduced Simon using super rounds, Cryptology ePrint Archive 2020/290, 2020.
- [6] T. Ashur and V. Rijmen, On linear hulls and trails, Indocrypt 2016, LNCS 10095, pp. 269-286, 2016.
- [7] N. Bagheri, Linear cryptanalysis of reduced-round simeck variants, Indocrypt 2015, LNCS 9462, pp. 140-152, 2015.

- [8] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks and L. Wingers, The SIMON and SPECK families of lightweight block ciphers, *Cryptology ePrint 2013/404*, 2013, 2015 52nd ACM/EDSC/IEEE Design Automation Conference (DAC), pp. 1-6, 2015.
- [9] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks and L. Wingers, Notes on the design and analysis of SIMON and SPECK, *Cryptology ePrint 2017/560*, 2017.
- [10] D. J. Bernstein, S. Kölbl, S. Lucks, P. M. C. Massolino, F. Mendel, K. Nawaz, T. Schneider, P. Schwabe, F. Standaert, Y. Todo, and B. Vigiuer, Gimli : A cross-platform permutation. In *Cryptographic Hardware and Embedded Systems, CHES 2017, LNCS 10529*, pp. 299-320, 2017.
- [11] G. Bertoni, J. Daemen, M. Peeters and G. Van Assche, The Keccak reference, <http://keccak.noekeon.org>, January 2011, version 3.0.
- [12] T. Beyne, A geometric approach to linear cryptanalysis, *Asiacrypt 2021*, 2021.
- [13] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, *Journal of Cryptology*, Vol. 4, pp. 3-72, 1991.
- [14] A. Biryukov, C. De Cannière and M. Quisquater, On mutiple linear approximations, *Crypto 2004, LNCS 3152*, pp. 1-22, 2004.
- [15] A. Biryukov, A. Roy and V. Velichkov, Differential Analysis of Block Ciphers SIMON and SPECK, *FSE 2014, LNCS 8540*, pp. 546-570, 2014.
- [16] C. Boura and A. Canteaut, A new criterion for avoiding the propagation of linear relations through an S-box (Full version), *Cryptology ePrint 2013/211*, 2013.
- [17] C. Carlet, Vectorial Boolean functions for cryptography, Chapter 9, *Boolean models and methods in mathematics, computer science and engineering*, Edited by Y. Crama and P. L. Hammer, Cambridge University Press.
- [18] P. Charpin, Normal Boolean functions, *Journal of Complexity*, Vol. 20, pp. 245-265, 2004.
- [19] Hao Chen, The Maiorana-McFarland structure based differential cryptanalysis: Collision attacks on round-reduced SHA-3, Gimli, Ascon, Work in progress, 2020-2021.

- [20] H. Chen and X. Wang, Improved linear hull attack on round-reduced Simon with dynamic key-guessing techniques, FSE 2016, LNCS 9783, pp. 428-449, 2016.
- [21] J. Daemen, P. M. C. Massolino, and Y. Rotella, The Subterranean 2.0 cipher suite, 2019. <https://csrc.nist.gov/Projects/Lightweight-Cryptography/Round-1-Candidates>, 2019.
- [22] H. Dobbertin, Construction of bent functions and balanced Boolean functions with high nonlinearity, FSE 1994, LNCS 1008, pp. 61-74, 1994.
- [23] C. Dobraunig, M. Eichlseder, F. Mendel and M. Schl affer, Ascon. Submission to the CAESAR competition: <http://ascon.iaik.tugraz.at>, 2014.
- [24] A. Fl orez-Guti errez and M. Naya-Plasencia, Improving key-recovery attack in linear attacks: Applications to 28-round PRESENT, Eurocrypt 2020, LNCS 12105, pp. 221-249, 2020.
- [25] M. Eichlseder, G. Leander and S. Rasoolzadeh, Computing expected differential probability of (truncated) differentials and expected linear potential of (multidimensional) linear hulls in SPN block ciphers, Indocrypt 2020, LNCS 12578, pp. 345-369, 2020.
- [26] M. Hermelin, J. Y. Choo and K. Nyberg, Multidimensional linear cryptanalysis of reduced round surpent, ACISP 2008, LNCS 5107, pp. 203-215, 2008.
- [27] M. Hermelin, J. Y. Choo and K. Nyberg, Multidimensional extension of Matsui's algorithm, FSE 2009, LNCS 5665, pp. 209-227, 2009.
- [28] M. Hermelin, J. Y. Choo and K. Nyberg, Multidimensional linear cryptanalysis, Journal of Cryptology, Vol. 32, pp. 1-34, 2019.
- [29] J. Jean, M. Naya-Plasencia and T. Peyrin, Improved Cryptanalysis of AES-like Permutations. Journal of Cryptology, Vol. 27, pp. 772-798, 2014.
- [30] S. K obl, G. Leander and T. Tiessen, Observations on the SIMON block cipher family, CRYPTO 2015, LNCS 9215, pp. 161-185. 2015.
- [31] S. K obl and A. Roy, A brief comparison of simon and simeck, 5th LightSec 2016, LNCS 10098, pp. 69-88, 2016.

- [32] K. Kondo, Y. Sasaki and T. Iwata, On the Design Rationale of Simon Block Cipher: Integral Attacks and Impossible Differential Attacks against Simon Variants, ACNS 2016, LNCS 9696, pp. 518-536, 2016.
- [33] X. Lai, J. Massey, and S. Murphy, Markov ciphers and differential cryptanalysis, Eurocrypt 1991, LNCS 547, pp. 17-38, 1991.
- [34] G. Leurent, C. Pernot and A. Schrottenloher, Clustering effect in Simon and Simeck, Asiacrypt 2021.
- [35] G. Leander, On linear hulls, statistical saturation attacks, PRESENT and a cryptanalysis of PUFFIN, Eurocrypt 2011, LNCS 6632, pp. 303-322, 2011.
- [36] F. Liu, T. Isobe and W. Meier, Cube-Based Cryptanalysis of Subterranean-SAE, Cryptology ePrint, 2019/879, 2019.
- [37] F. Liu, T. Isobe and W. Meier, Automatic Verification of Differential Characteristics: Application to Reduced Gimli, Crypto 2020, 219-248, 2020.
- [38] Y. Liu, W. Zheng, B. Sun, V. Rijmen, G. Liu, C. Li, S. Fu and M. Cao, The phantom of differential characteristics, Designs, Codes and Cryptography, Vol. 88, pp. 2289-2311, 2020.
- [39] Z. Liu, Y. Li and M. Wang, Optimal Differential Trails in SIMON-like Ciphers. IACR Trans. Symmetric Cryptol. Vol. 1, pp. 358-379, 2017.
- [40] Z. Liu, Y. Li and M. Wang, The Security of SIMON-like Ciphers Against Linear Cryptanalysis, Cryptology ePrint 2017/576, 2017.
- [41] J. Lu, Y. Liu, T. Ashur, B. Sun and C. Li, Rotational-XOR Cryptanalysis of Simon-like Block Ciphers, Cryptology ePrint Archive 2020/486, 2020.
- [42] M. Matsui, Linear cryptanalysis method for DES cipher, Eurocrypt 1993, LNCS 765, pp. 386-397, 1993.
- [43] M. Matsui, The first experimental cryptanalysis of the data encryption standard, Crypto 1994, LNCS 839, pp. 1-11, 1994.
- [44] R. L. McFarland, A family of noncyclic difference sets, Journal of Combinatorial Theory, Ser. A, 15, 1-10, 1973.

- [45] F. Mendel, T. Nad, and M. Schlaffer. Finding SHA-2 characteristics: Searching through a minefield of contradictions, ASIACRYPT 2011, 288-307, 2011.
- [46] S. Murphy, The independence of linear approximations in symmetric cryptology, IEEE Transactions on Information Theory, Vol. 52, pp. 5510-5518, 2006.
- [47] S. Murphy, The effectiveness of linear hull effect, Technical Report RHUL-MA-2009-19, 2009.
- [48] K. Nyberg, Perfect nonlinear S-boxes, Eurocrypt 91, LNCS 547, pp. 378-385, 1991.
- [49] K. Nyberg, Linear approximation of block ciphers, Eurocrypt 1994, LNCS 950, pp. 439-444, 1994.
- [50] R. Rohit and G. Gong, Correlated Sequence Attack on Reduced-Round Simon-32/64 and Simeck-32/64, Cryptology ePrint 2018/699, 2018.
- [51] A. A. Selçuk, On the probability of success in linear and differential cryptanalysis, Journal of Cryptology, Vol. 21, pp. 131-147, 2008.
- [52] L. Qin, H. Chen and X. Wang, Linear hull attack on round-reduced Simeck with dynamic key-guessing techniques, ACISP 16, LNCS 9723, pp. 409-424, 2016.
- [53] S. Sun, L. Hu, M. Wang, P. Wang, K. Qiao, X. Ma, D. Ma, L. Song, K. Fu, Towards finding the best characteristics of some bit-oriented block ciphers and automatic enumeration of (related-key) differential and linear characteristics with predefined properties and its applications, IACR Cryptology ePrint 2014/747, 2014.
- [54] N. Wang, X. Wang, K. Jia and J. Zhao, Differential attacks on reduced Simon versions with dynamic key-guessing techniques, Sci. China, Information Science, Vol. 61, pp. 098103.1-098103.3, 2018.
- [55] X. Wang, B. Wu, L. Hou and D. Lin, Automatic search for related-key differential trails in Simon-like block ciphers based on MILP, ISC 2018, LNCS 11060, pp. 116-131, 2018.
- [56] G. Yang, B. Zhu, V. Suder, M. D. Aagaard and Gong, G. The Simeck family of lightweight block ciphers, CHES 2015, LNCS 9293, pp. 307-329, 2015.