Related-Key Linear Hull Distinguishers for Key-Alternating Block Ciphers

Andrey Bogdanov, Vincent Rijmen, Elmar Tischhauser

Related-Key Linear Hull Distinguishers for Key-Alternating Block Ciphers

Andrey Bogdanov[1], Vincent Rijmen[2], and Elmar Tischhauser[1]

[1] Department of Applied Mathematics and Computer Science, Technical University of Denmark
[2] ESAT/COSIC, Katholieke Universiteit Leuven, Belgium
{anbog,ewti}@dtu.dk

Abstract. In this paper, we describe work in progress on novel related-key distinguishers applicable to key-alternating block ciphers, a wide class of symmetric-key primitives. This class includes the AES finalists Rijndael and Serpent as well as many other block ciphers having SPN structure, including many Feistel networks. Unlike the known differential related-key techniques, our distinguishers are essentially of linear nature and make use of how exactly that linear hulls of key-alternating ciphers are structured when encrypting under different keys.
By partitioning the linear trails contained in these hulls into a "signal" part (known enumerated trails) and a "noise" part (the unknown remainder of the hull), we develop statistical models for differences and sums of linear hull correlations when evaluated under different keys. We then observe that for concrete key-alternating ciphers, the differences or sums of correlations tend to differ from the ideal behaviour, admitting a structural distinguisher.
Unlike the key-difference invariant bias technique from ASIACRYPT 2013, our models allow for an intersection of the key difference with active bits of trails contained in the linear hull under consideration. This opens up possibilities for more powerful and generally applicable distinguishers.
Keywords: block cipher, distinguisher, linear hull, related-key attack, correlation, key-schedule, substitution-permutation network, key-invariant bias

1 Introduction

Block ciphers have developed to the basis of symmetric-key cryptography: Many sound and efficient cryptographic constructions can be built upon them, such as stream ciphers, message authentication codes, hash functions or entropy extractors for random number generators.

1.1 Motivation

Design strategies such as the wide trail design strategy [13] by Daemen and Rijmen or the decorrelation theory [25] by Vaudenay allow to construct block ciphers for which we can state with high confidence that they will resist crucial analysis methods such as differential [6] and linear [20] cryptanalysis for the case of *a fixed random secret key.* However, in *related-key* [2] or even *known-key* [19] attack scenarios, these strategies provide only limited evidence of resistance. Indeed, only few recently proposed block ciphers have been broken in the classical attack model with a fixed secret key, most of the successful analysis being performed in the related-key model [4], [17], [16], [27] including the differential related-key cryptanalysis [8], [7] of AES designed according to the wide trail strategy.

While a great deal of research effort has recently been devoted to developing efficient differential related-key attacks, e.g. by combining them with boomerang techniques [5], [7], practically no related-key attacks are known so far in the framework of linear cryptanalysis, with the exception of the key-difference invariant bias attacks proposed at ASIACRYPT 2013 [9].

In this paper, we aim to further bridge this gap by enriching the cryptanalytic toolbox of related-key attacks exploiting the key-dependent linear properties of the wide class of key-alternating block ciphers in a more general way than in [9].

1.2 Contributions

In this work in progress, related-key distinguishers are proposed, based on the properties of the linear hulls of key-alternating block ciphers. The idea is to inspect the joint distribution of (signed) correlations for the same linear approximation obtained for different keys. More specifically, we propose to look at differences or sums of two correlations C and C' corresponding to two distinct keys κ and κ' for some linear hull.

This is motivated by the fact that in key-alternating ciphers, the linear trails constituting a given linear hull are themselves independent of the key value. The signs of correlation values for these linear trails are, however, key-dependent. By choosing a proper combination of related keys, we try to manipulate the signs of individual linear trail contributions so that the joint distribution of the corresponding correlations behaves non-ideally. As opposed to the key-difference invariant bias technique, our approach does not require the two correlations to be equal, which in turn essentially requires to have active bits in the expanded key difference at nonintersecting positions with the bit positions participating in all trails in the linear hulls.

We extend furthermore on the key-difference invariant bias technique by partitioning the linear trails contained in these hulls into a "signal" part (known enumerated trails) and a "noise" part (the unknown remainder of the hull), we develop statistical models for differences and sums of linear hull correlations when evaluated under different keys. These extensions open up possibilities for more powerful and generally applicable distinguishers.

1.3 Background

Key-Alternating Block Ciphers. A block cipher encrypts an n-bit plaintext block with a k-bit key to obtain an n-bit ciphertext block. As a rule, the block cipher encryption is the iterative application of r similar invertible transformations (called rounds) to the plaintext. In a *key-alternating block cipher* (see Figure 1) [14], the key material in round i is introduced by XORing the subkey k_i to the state at the end of the round. Additionally, the subkey k_0 is XORed with the plaintext before round 1.

The $r + 1$ round subkeys $k_0, k_1, \ldots, k_{r-1}, k_r$ form the *expanded key* K which is derived from the used-supplied key κ using a key-schedule algorithm φ.

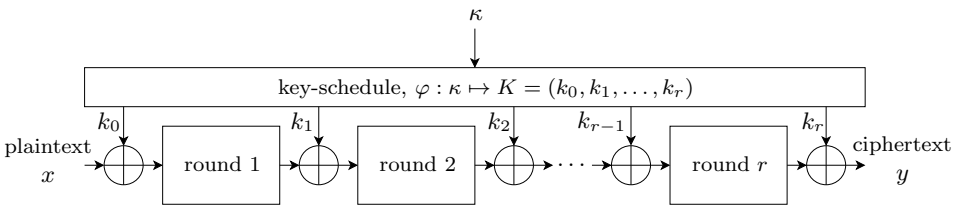

Fig. 1. Key-alternating block cipher

Numerous popular and widely used block ciphers belong to the class of key-alternating block ciphers. Among others, most substitution-permutation networks (SPNs) such as AES [14], Serpent [3], SHARK [23], and PRESENT [10] are key-alternating.

Linear Cryptanalysis, Linear Hulls, Correlation. Linear cryptanalysis [20] uses linear approximations of block ciphers to build a distinguisher. A linear approximation is given by input and output selection patterns, α and β. The probability π that the equality of scalar products[3] over $\mathbb{F}_2$

$$\alpha \diamond x = \beta \diamond y$$

on plaintexts x and ciphertexts y holds is usually the measure of approximation goodness: The more significantly π deviates from $1/2$, the better the linear approximation is for linear cryptanalysis. Following [14] and [21], we prefer to operate in terms of *correlation* $C = 2\pi - 1$.

The input selection pattern α propagates to β through the rounds of the cipher along *linear trails*. The set of all linear trails from α to β is referred to as a *linear hull*, a concept introduced by Nyberg [21].

As opposed to the linear cryptanalysis, our attacks do not take into account how much π deviates from $1/2$ for a given linear approximation and work equally well with each nontrivial linear hull. That is, an increase in the number of rounds per se does not improve the resistance of a block cipher to our attacks. Our distinguishers strongly depend on the fact that the correlation of one linear hull is the sum of many contributions belonging to different trails. Although our distinguishers are typically not very sensitive towards the particular choice of hull, we see currently no way to benefit from using more than one hull simultaneously, as is done in [18].

Correlation for Random Permutations. The correlation C of a linear approximation for a randomly drawn permutation is distributed as follows [22]:

$$\Pr\left\{C = z \cdot 2^{2-n}\right\} = \frac{\binom{2^{n-1}}{2^{n-2}+z}^2}{\binom{2^n}{2^{n-1}}}. \tag{1}$$

Thus, for an ideal cipher, C can be approximated by a normal distribution $\mathcal{N}(0, 2^{-n})$ with mean 0 and variance 2^{-n} [15]. The sum or difference of correlation values for two different randomly drawn permutations on n bits can be then approximated by $\mathcal{N}(0, 2^{(1-n)})$, which is the sum of two normal distributions for C and C'. Now if we obtain a distribution $C - C'$ or $C + C'$ substantially deviating from this, then we have a distinguisher.

Correlation for Key-Alternating Ciphers. Let us fix a linear hull defined by input and output selection patterns α and β for a key-alternating cipher. Many linear trails U_i contribute to the same linear hull. Each linear trail U_i has its correlation $2\pi_i - 1$, where π_i is the probability that α propagates to β along the linear trail U_i. As in [14], we denote its sign by $(-1)^{d_{U_i}}$ and the absolute value by C_{U_i}, $2\pi_i - 1 = (-1)^{d_{U_i}} C_{U_i}$. Moreover, we consider U_i as a concatenation of selection patterns at input, output and between the round transformations. Respectively, U_i consists of $\ell = n(r+1)$ bits which we will address by $U_{i,j}$. It has been

[3] For $a = (a_n, \ldots, a_1) \in \mathbb{F}_2^n$ and $b = (b_n, \ldots, b_1) \in \mathbb{F}_2^n$ with $a_i, b_i \in \mathbb{F}_2$, $a \diamond b = \bigoplus_{i=1}^n a_i b_i$

shown in [14] that, for key-alternating ciphers, the correlation for an expanded key K can be computed as:

$$C = \sum_i (-1)^{U_i \diamond K + d_{U_i}} C_{U_i}. \tag{2}$$

2 Towards General Related-Key Linear Hull Distinguishers

We choose input and output linear selection patterns, α and β, for a block cipher. Let C and C' be the correlations between α and β for the block cipher with (expanded) keys K and K', respectively, $K \oplus K' = \Delta$. For distinguishing between an ideal cipher and a key-alternating cipher, we consider the joint distribution of C and C'. More specifically, the distinguishers are based on inspecting $C - C'$ or $C + C'$.

For the difference of two correlations for two distinct keys, the following can be derived from equation (2):

$$C - C' = \sum_i \left[(-1)^{U_i \diamond K} - (-1)^{U_i \diamond K'} \right] (-1)^{d_{U_i}} C_{U_i}. \tag{3}$$

All correlations for a given linear hull share the linear trails U_i as well as the values of C_{U_i} and d_{U_i}. The difference between C and C' originates from the varying signs which in turn depend only on the relation between of K and K'.

More specifically, the difference between C and C' is due to the value of $(-1)^{U_i \diamond K} - (-1)^{U_i \diamond K'}$:

$$(-1)^{U_i \diamond K} - (-1)^{U_i \diamond K'} = \begin{cases} 0, & \text{if } U_i \diamond K = U_i \diamond K' \Leftrightarrow U_i \diamond \Delta = 0, \\ \pm 2, & \text{if } U_i \diamond K \neq U_i \diamond K' \Leftrightarrow U_i \diamond \Delta = 1. \end{cases}$$

This connection between the correlation difference $C - C'$ for a given linear hull and the key difference Δ is crucial to our distinguishers. In the following, we discuss the question of how balanced $U_i \diamond \Delta$ is as a Boolean function of Δ.

Linear Hull Biases. The expanded key difference Δ is a value choosing certain positions in linear trail U_i. To explore its balancedness, we are interested in the probability

$$p = \Pr\{U_i \diamond \Delta = 0\}. \tag{4}$$

We conjecture that ideally, $p = 1/2$. So one needs to tell how far p is from $1/2$ for the cipher in question, which can be done by measuring the bias

$$\delta = 2p - 1$$

for a given key difference Δ. Let $j \in \{1, \ldots, \ell\}$ a bit position in U_i with ℓ the length of a linear trail/expanded key. Define

$$p_j = \Pr\{U_{i,j} = 0\} \tag{5}$$

to be the probability that U_i has a zero bit in position j in the given linear hull, computed over all linear trails i.

Relation to Key-Difference Invariant Bias. We briefly note that the key-difference invariant bias technique can be seen as a special case where $C = C'$ which generally requires $p = 1$ for the entire linear hull.

Signal-Noise Decomposition of Linear Hulls. For any realistic key-alternating cipher, it quickly becomes infeasible to enumerate all linear trails in a given linear hull as the number of rounds increases. Inspection of the distribution (3) of the correlation difference or computation of the linear hull bias δ is therefore computationally infeasible. In order to cope with this difficulty, we propose to consider a decomposition of the sum over all trails according to the significance of their contributions to the overall correlation. This approach has been successfully used in the context of estimating the complexity of Matsui's Algorithm 2 [11]; and considering only the "dominant" part of a hull has turned out to be fruitful in the context of Matsui's Algorithm 1 [24].

The idea is a follows: When evaluating a concrete cipher, one typically manages to enumerate a certain number of high-probability trails, but not the entire linear hull. Suppose that t dominant trails are known, the contribution of the remainder of the hull is then modeled by a random permutation as in (1):

$$C \approx \sum_{j=1}^{t} (-1)^{d_{U_j} + U_j \diamond K} C_{U_j} + \mathcal{N}\big(0,\, 2^{-n}\big)\,. \tag{6}$$

The probabilities p and p_j and the bias δ are then accordingly defined over the known set of trails instead of the entire linear hull.

2.1 Statistical model for correlation difference

We now develop a statistical model for the behaviour of $C - C'$ for expanded keys K and K', using the signal-noise decomposition outlined above.

If $\Delta \diamond U_i = 0$ for some trails U_i and $\Delta \diamond U_i = 1$ for the other trails constituting the linear hull (in other words: $p \neq 1$), $C - C'$ will behave non-deterministically. Intuitively, the value of $C - C'$ is mainly determined by the distribution of $(-1)^{U_i \diamond K} - (-1)^{U_i \diamond K'}$, which in turn depends on how often $U_i \diamond K = U_i \diamond K'$ is fulfilled or, in other words, how often $U_i \diamond \Delta = 0$.

We start with (3) and split the sum first according to the trail bits d_{U_i}:

$$\begin{aligned} C - C' &= \sum_i \left[(-1)^{U_i \diamond K} - (-1)^{U_i \diamond K'}\right] (-1)^{d_{U_i}} C_{U_i} \\ &= \sum_{i : d_{U_i} = 0} \left((-1)^{U_i \diamond K} - (-1)^{U_i \diamond K'}\right) C_{U_i} \\ &\quad - \sum_{j : d_{U_j} = 1} \left((-1)^{U_j \diamond K} - (-1)^{U_j \diamond K'}\right) C_{U_j}. \end{aligned}$$

and then repartition it according to the different correlation values C_{U_i} that occur:

$$\begin{aligned} &= C_{U_1} \left(\sum_i \chi(U_i) - \sum_j \chi(U_j) \right) \\ &\quad + \cdots \\ &\quad + C_{U_m} \left(\sum_i \chi(U_i) - \sum_j \chi(U_j) \right), \end{aligned}$$

with $\chi(U_i) \stackrel{\text{def}}{=} (-1)^{U_i \diamond K} - (-1)^{U_i \diamond K'}$ and assuming that there are m possible different nonzero correlation values. Denoting the number of trails with correlation value C_{U_i} and trail bits d_{U_i} as $N_i^{(d_{U_i})}$ (with $d_{U_i} = 0, 1$), this yields

$$\begin{aligned} C - C' = C_{U_1} &\left(\sum_{i=1}^{N_1^{(0)}} \chi(U_i) - \sum_{j=1}^{N_1^{(1)}} \chi(U_j) \right) \\ &+ \cdots \\ &+ C_{U_m} \left(\sum_{i=1}^{N_m^{(0)}} \chi(U_i) - \sum_{j=1}^{N_m^{(1)}} \chi(U_j) \right). \end{aligned} \tag{7}$$

We now consider the quantity $\chi(U_i)$ statistically. We have $\chi(U_i)$ equal to

- 0, if $U_i \diamond K = U_i \diamond K'$,
- 2, if $U_i \diamond K = 0$ and $U_i \diamond K' = 1$, or
- -2, if $U_i \diamond K = 1$ and $U_i \diamond K' = 0$.

Note that when the U_i range over all trails in the hull, the first event happens with probability p as defined in (4). Since we are now partitioning the hull according to correlation value, we analogously define

$$p_i^{(b)} \stackrel{\text{def}}{=} \Pr_{U_j : C_{U_j} = i, d_{U_j} = b} \{ U_j \diamond \Delta = 0 \}$$

for $b = 0, 1$. The second and third events are then assumed to occur with probabilities $(1 - p_i^{(b)})/2$ each. This yields

$$\chi(U_i) \sim 2\,\mathrm{Bern}(\frac{(1 - p_i^{(b)})}{2}) - 2\,\mathrm{Bern}(\frac{(1 - p_i^{(b)})}{2}).$$

Since we can consider these Bernoulli distributions as indepenent, each of the sums in (7) is therefore distributed as

$$\begin{aligned} \sum_{i=1}^{N_j^{(b)}} \chi(U_i) &\sim 2 \left(\sum_{i=1}^{N_j^{(b)}} \mathrm{Bern}(\frac{(1 - p_i^{(b)})}{2}) - \mathrm{Bern}(\frac{(1 - p_i^{(b)})}{2}) \right) \\ &= 2\,\mathrm{Bin}(N_j^{(b)}, \frac{(1 - p_i^{(b)})}{2}) - 2\,\mathrm{Bin}(N_j^{(b)}, \frac{(1 - p_i^{(b)})}{2}), \end{aligned}$$

with $\mathrm{Bin}(N,p)$ denoting a Binomial distribution with success probability p and N repetitions. If the $N_j^{(b)}$'s are large enough, the Binomial distributions can be approximated by normal distributions $\mathcal{N}\big(\mu,\ \sigma^2\big)$:

$$\begin{aligned}\sum_{i=1}^{N_j^{(b)}} \chi(U_i) &\sim 2\mathcal{N}\left(N_j^{(b)}\frac{(1-p_j^{(b)})}{2},\ N_j^{(b)}\frac{(1-p_j^{(b)})}{2}\frac{(1+p_j^{(b)})}{2}\right)\\ &\quad - 2\mathcal{N}\left(N_j^{(b)}\frac{(1-p_j^{(b)})}{2},\ N_j^{(b)}\frac{(1-p_j^{(b)})}{2}\frac{(1+p_j^{(b)})}{2}\right)\\ &= 2\mathcal{N}\left(0,\ N_j^{(b)}\frac{1-{p_i^{(b)}}^2}{2}\right)\\ &= \mathcal{N}\left(0,\ 2N_j^{(b)}(1-{p_i^{(b)}}^2)\right).\end{aligned}$$

Since it is infeasible to explicitly calculate these sums for all trails for all possible correlation values C_{U_i}, we now apply the signal-noise decomposition and model the sum (7) as an exact part for $t \ll m$ correlation values and a statistical approximation for the remainder of the hull. According to (1), the correlation of an n-bit permutation is distributed approximately as $\mathcal{N}(0,\ 2^{-n})$, therefore we assume that for $C-C'$, the unknown part of the linear hull behaves as $\mathcal{N}\big(0,\ 2^{1-n}\big)$. This yields

$$\begin{aligned}C - C' \sim\ & C_{U_1}\left[\mathcal{N}\left(0,\ 2N_1^{(0)}(1-{p_1^{(0)}}^2)\right) - \mathcal{N}\left(0,\ 2N_1^{(1)}(1-{p_1^{(1)}}^2)\right)\right]\\ &+\cdots\\ &+ C_{U_t}\left[\mathcal{N}\left(0,\ 2N_t^{(0)}(1-{p_t^{(0)}}^2)\right) - \mathcal{N}\left(0,\ 2N_t^{(1)}(1-{p_t^{(1)}}^2)\right)\right]\\ &+\mathcal{N}\big(0,\ 2^{1-n}\big)\end{aligned}$$

which can be reformulated to

$$\begin{aligned}=\ & \mathcal{N}\left(0,\ 2C_{U_1}^2N_1^{(0)}(1-{p_1^{(0)}}^2)\right) - \mathcal{N}\left(0,\ 2C_{U_1}^2N_1^{(1)}(1-{p_1^{(1)}}^2)\right)\\ &+\cdots\\ &+\mathcal{N}\left(0,\ 2C_{U_t}^2N_t^{(0)}(1-{p_t^{(0)}}^2)\right) - \mathcal{N}\left(0,\ 2C_{U_t}^2N_t^{(1)}(1-{p_t^{(1)}}^2)\right)\\ &+\mathcal{N}\big(0,\ 2^{1-n}\big)\end{aligned}$$

which finally gives

$$= \mathcal{N}\big(0,\ \sigma_t^2\big)$$

with

$$\begin{aligned}\sigma_t^2 = 2\sum_{i=1}^{t} C_{U_i}^2\left(N_i^{(0)}(1-{p_i^{(0)}}^2) + N_i^{(1)}(1-{p_i^{(1)}}^2)\right)\\ + 2^{1-n}.\end{aligned} \tag{8}$$

Note that the first summand of (8) is an exact and explicitly computable value corresponding to the available signal, whereas the second summand accounts for the noise stemming from the unknown remainder of the hull.

The difference of correlations for a fixed linear hull for two random permutations is approximately $\mathcal{N}\big(0,\, 2^{1-n}\big)$. It can now be tested by a comparison of variances whether the corresponding distribution $\mathcal{N}\big(0,\, \sigma_t^2\big)$ as given in (8) for concrete ciphers differs from the ideal case, yielding a distinguisher.

2.2 Statistical model for sums of correlations

For the case that $p = 1$ for all known signal trails, the difference between C and C' does not yield interesting information about the cipher in question, since independent of the used keys, all signal deterministically cancels out. In such a scenario, we propose to instead consider sums of correlations in an attempt to amplify the signal provided by the fact that the correlation will be invariant for the known trails (but vary for the unknown and uncontrolled part). Denoting by t the number of known trails, we therefore have

$$\begin{aligned} C_K &= \sum_i C_{U_i}(-1)^{U_i \diamond K + d_{U_i}} \\ &\approx \sum_i^t C_{U_i}(-1)^{U_i \diamond K + d_{U_i}} + \mathcal{N}\big(0,\, 2^{-n}\big) = C_0 + \mathcal{N}\big(0,\, 2^{-n}\big) \end{aligned}$$

for some fixed correlation value C_0 and analogously

$$\begin{aligned} C_{K'} &= \sum_i C_{U_i}(-1)^{U_i \diamond K' + d_{U_i}} \\ &\approx \sum_i^t C_{U_i}(-1)^{U_i \diamond K' + d_{U_i}} + \mathcal{N}\big(0,\, 2^{-n}\big) = C_0 + \mathcal{N}\big(0,\, 2^{-n}\big)\,. \end{aligned}$$

Note that the correlation C_0 for the known part of the hull is the same for any two keys K and K' here. We therefore conclude that the sum of any two such correlations is distributed as

$$\begin{aligned} C_K + C_{K'} &\sim C_0 + C_0 + \mathcal{N}\big(0,\, 2^{1-n}\big) \\ &= \mathcal{N}\big(2C_0,\, 2^{1-n}\big)\,. \end{aligned}$$

A distinguisher can now be based on a test of means between $\mathcal{N}\big(2C_0,\, 2^{1-n}\big)$ for the cipher in question and $\mathcal{N}\big(0,\, 2^{1-n}\big)$ for the ideal cipher.

It is worth noting that this scenario explicitly allows for $p \neq 1$ in the noise part, as long as $p = 1$ for the signal trails. This was not the case for the invariant bias technique, which essentially required $p = 1$ for the entire linear hull.

2.3 Experimental results

The ability to apply the techniques from either Sect. 2.1 or 2.2 depends on identifying linear hulls for block ciphers that give rise to distributions of $C - C'$ or $C + C'$ which differ from the ideal cipher. We specified several 10-round small-scale SHARK-ciphers [23] using the 4-bit S-box and MDS submatrices of the 4x4 diffusion matrix over $\mathbb{F}_2^4$ from [12], where AES-variants for algebraic cryptanalysis are proposed. We performed experiments with block sizes of 8, 12 and 16 bits. Note that SHARK-type ciphers have the highest single-round diffusion in the class of SPNs.

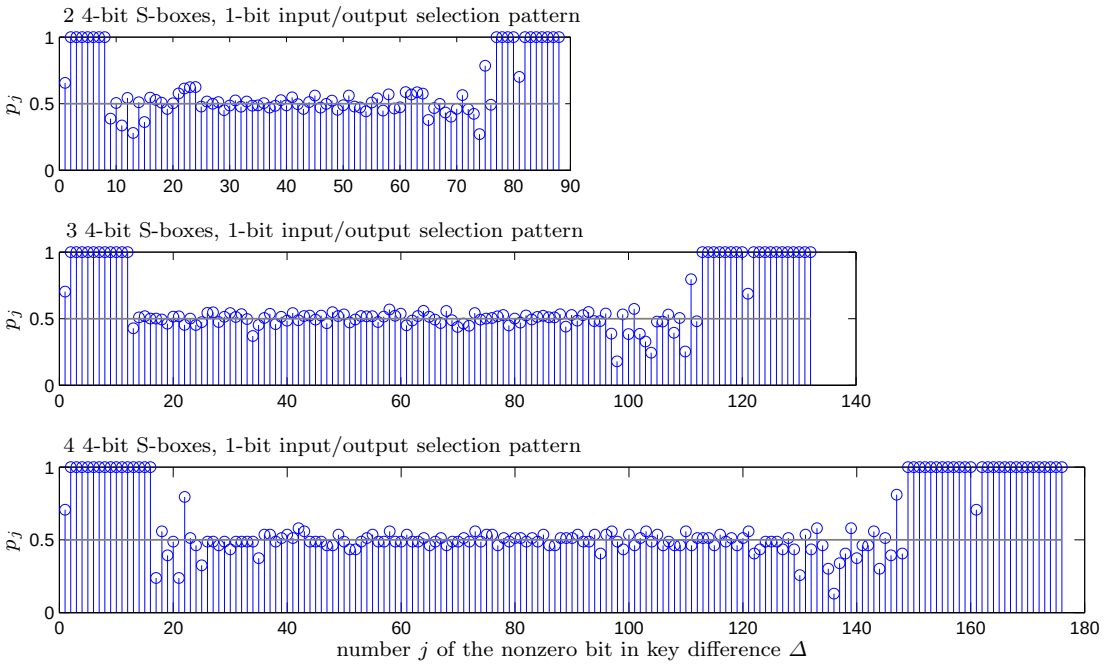

Fig. 2. p_j for small-scale SPN ciphers with 10 rounds, p_j=0.5 for an ideal cipher

Existence of Biased Bits in Linear Hulls. We experimentally analyzed the linear hull biases for these ciphers with single-bit expanded key differences. The results are given in Figure 2.

We observe that for all three block sizes, after a certain number of rounds (from the end and from the beginning), the values of δ_j stop decreasing and become stable: Linear hull biases δ_j in the middle do not depend on the number of rounds. How fast the stabilization occurs, depends on the sparseness of input/output linear selection patterns. The results indicate that most p_j are not prohibitive and can allow for distinguishing.

3 Conclusions

In this paper, we report work in progress towards novel related-key distinguishers for key-alternating block ciphers which are based on exploiting structural properties of linear hulls. Our approach extends the key difference invariant bias technique in two ways: First, it allows intersections between key differences and active linear trail bits. Second, by adopting a signal-noise decomposition of the linear hulls in question, it allows detecting non-ideal properties when only partial knowledge about the composition of linear hulls is available.

References

1. Bellare, M., Kohno, T.: A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications. In: Biham, E. (ed.) EUROCRYPT'03. LNCS, vol. 2656, pp. 491–506. Springer-Verlag (2003)
2. Biham, E.: New Types of Cryptoanalytic Attacks Using Related Keys (Extended Abstract). In: EUROCRYPT'93. pp. 398–409. LNCS, Springer-Verlag (1993)
3. Biham, E., Anderson, R.J., Knudsen, L.R.: Serpent: A New Block Cipher Proposal. In: Vaudenay, S. (ed.) FSE'98. LNCS, vol. 1372, pp. 222–238. Springer-Verlag (1998)

4. Biham, E., Dunkelman, O., Keller, N.: A Related-Key Rectangle Attack on the Full Kasumi. In: Roy, B.K. (ed.) ASIACRYPT'05. LNCS, vol. 3788, pp. 443–461. Springer-Verlag (2005)
5. Biham, E., Dunkelman, O., Keller, N.: Related-Key Boomerang and Rectangle Attacks. In: Cramer, R. (ed.) EUROCRYPT'05. LNCS, vol. 3494, pp. 507–525. Springer-Verlag (2005)
6. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO'90. LNCS, vol. 537, pp. 2–21. Springer-Verlag (1990)
7. Biryukov, A., Khovratovich, D.: Related-Key Cryptanalysis of the Full AES-192 and AES-256. In: Matsui, M. (ed.) ASIACRYPT'09. LNCS, vol. 5912, pp. 1–18. Springer-Verlag (2009), http://dx.doi.org/10.1007/978-3-642-10366-7
8. Biryukov, A., Khovratovich, D., Nikolic, I.: Distinguisher and Related-Key Attack on the Full AES-256. In: Halevi, S. (ed.) CRYPTO'09. LNCS, vol. 5677, pp. 231–249. Springer-Verlag (2009), http://dx.doi.org/10.1007/978-3-642-03356-8
9. Bogdanov, A., Boura, C., Rijmen, V., Wang, M., Wen, L., Zhao, J.: Key difference invariant bias in block ciphers. In: Sako, K., Sarkar, P. (eds.) Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I. Lecture Notes in Computer Science, vol. 8269, pp. 357–376. Springer (2013), http://dx.doi.org/10.1007/978-3-642-42033-7_19
10. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES'07. LNCS, vol. 4727, pp. 450–466. Springer-Verlag (2007)
11. Bogdanov, A., Tischhauser, E.: On the wrong key randomisation and key equivalence hypotheses in matsui's algorithm 2. In: Moriai, S. (ed.) Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers. Lecture Notes in Computer Science, vol. 8424, pp. 19–38. Springer (2013), http://dx.doi.org/10.1007/978-3-662-43933-3_2
12. Cid, C., Murphy, S., Robshaw, M.J.B.: Small Scale Variants of the AES. In: Gilbert, H., Handschuh, H. (eds.) FSE'05. LNCS, vol. 3557, pp. 145–162. Springer-Verlag (2005)
13. Daemen, J., Rijmen, V.: AES and the Wide Trail Design Strategy. In: Knudsen, L.R. (ed.) EUROCRYPT'02. LNCS, vol. 2332, pp. 108–109. Springer-Verlag (2002)
14. Daemen, J., Rijmen, V.: The Design of Rijndael: AES – The Advanced Encryption Standard. Springer-Verlag (2002)
15. Daemen, J., Rijmen, V.: Probability Distributions of Correlation and Differentials in Block Ciphers. Journal of Mathematical Cryptology 1(3), 221–242 (2007)
16. Dunkelman, O., Fleischmann, E., Gorski, M., Lucks, S.: Related-Key Rectangle Attack of the Full HAS-160 Encryption Mode. In: Roy, B.K., Sendrier, N. (eds.) INDOCRYPT'09. LNCS, vol. 5922, pp. 157–168. Springer-Verlag (2009), http://dx.doi.org/10.1007/978-3-642-10628-6
17. Fleischmann, E., Gorski, M., Lucks, S.: Memoryless Related-Key Boomerang Attack on the Full Tiger Block Cipher. In: Bao, F., Li, H., Wang, G. (eds.) ISPEC'09. LNCS, vol. 5451, pp. 298–309. Springer-Verlag (2009), http://dx.doi.org/10.1007/978-3-642-00843-6
18. Hermelin, M., Nyberg, K.: Dependent Linear Approximations: The Algorithm of Biryukov and Others Revisited. In: Pieprzyk, J. (ed.) CT-RSA'10. LNCS, vol. 5985, pp. 318–333. Springer-Verlag (2010), http://dx.doi.org/10.1007/978-3-642-11925-5
19. Knudsen, L.R., Rijmen, V.: Known-Key Distinguishers for Some Block Ciphers. In: Kurosawa, K. (ed.) ASIACRYPT'07. LNCS, vol. 4833, pp. 315–324. Springer-Verlag (2007)
20. Matsui, M.: Linear Cryptoanalysis Method for DES Cipher. In: EUROCRYPT'93. pp. 386–397. LNCS, Springer-Verlag (1993)
21. Nyberg, K.: Linear Approximation of Block Ciphers. In: EUROCRYPT'94. pp. 439–444. LNCS, Springer-Verlag (1994)
22. O'Connor, L.: Properties of Linear Approximation Tables. In: Preneel, B. (ed.) FSE'94. LNCS, vol. 1008, pp. 131–136. Springer-Verlag (1994)
23. Rijmen, V., Daemen, J., Preneel, B., Bosselaers, A., De Win, E.: The Cipher SHARK. In: Gollmann, D. (ed.) FSE'96. LNCS, vol. 1039, pp. 99–111. Springer-Verlag (1996)
24. Röck, A., Nyberg, K.: Generalization of matsui's algorithm 1 to linear hull for key-alternating block ciphers. Des. Codes Cryptography 66(1-3), 175–193 (2013), http://dx.doi.org/10.1007/s10623-012-9679-1
25. Vaudenay, S.: Decorrelation: A Theory for Block Cipher Security. J. Cryptology 16(4), 249–286 (2003)
26. Vora, P.L., Mir, D.: Related-Key Linear Cryptanalysis. In: IEEE International Symposium on Information Theory 2006. pp. 1609–1613 (2006)
27. Zhang, W., Zhang, L., Wu, W., Feng, D.: Related-Key Differential-Linear Attacks on Reduced AES-192. In: Srinathan, K., Rangan, C.P., Yung, M. (eds.) INDOCRYPT'07. LNCS, vol. 4859, pp. 73–85. Springer-Verlag (2007)