Key Difference Invariant Bias in Block Ciphers

Andrey Bogdanov[1⋆], Christina Boura[1⋆], Vincent Rijmen[2⋆], Meiqin Wang[3⋆],
Long Wen[3⋆], Jingyuan Zhao[3⋆]

[1] Technical University of Denmark, Denmark
[2] KU Leuven ESAT/SCD/COSIC and iMinds, Belgium
[3] Shandong University, Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China

Abstract. In this paper, we reveal a fundamental property of block ciphers: There can exist linear approximations such that their biases ε are deterministically *invariant under key difference*. This behaviour is highly unlikely to occur in idealized ciphers but persists, for instance, in 5-round AES. Interestingly, the property of key difference invariant bias is independent of the bias value ε itself and only depends on the form of linear characteristics comprising the linear approximation in question as well as on the key schedule of the cipher.

We propose a statistical distinguisher for this property and turn it into an key recovery. As an illustration, we apply our novel cryptanalytic technique to mount related-key attacks on two recent block ciphers — LBlock and TWINE. In these cases, we break 2 and 3 more rounds, respectively, than the best previous attacks.

Keywords: block ciphers, key difference invariant bias, linear cryptanalysis, linear hull, key-alternating ciphers, LBlock, TWINE

1 Introduction

1.1 Linear cryptanalysis, linear approximations, and bias

Linear cryptanalysis is a central and indispensable attack on block ciphers. Having been proposed as early as in 1992 [23–25], it forms an established research field within symmetric-key cryptology. Since then, many interesting results have been obtained in the area, among others including correlation matrices by Daemen et al. [8], multiple linear cryptanalysis by Kaliski and Robshaw [15], linear hull effect by Nyberg [29], multidimensional cryptanalysis by Hermelin et al. [13], comprehensive bounds on linear properties by Keliher and Sui [18], as well as success probability estimations by Selçuk [35].

The basis of linear cryptanalysis is a *linear approximation* of a function f. If the linear approximation holds with probability $1/2 + \varepsilon$, ε is called its *bias*. A linear approximation can comprise numerous linear characteristics θ, each contributing their linear characteristic bias ε_θ to the linear approximation bias ε.

[⋆] All authors are corresponding authors.

There are essentially two standard approaches to deal with the key-dependency of these biases: they are either averaged over all keys or evaluated for a fixed key. Both cases have been studied in great detail and these approaches have turned out to be very fruitful: While the average behaviour of the bias is vital to the foundations of linear cryptanalysis and the demonstration of the linear hull effect, Murphy has demonstrated [27] that there can be keys for which the linear distinguisher might not apply. The latter observation is more inline with the fixed-key correlation-matrix approach, which also, among others, has lead to zero-correlation attacks by Bogdanov et al. [3–5] and improved linear attacks on PRESENT by Cho [6].

Apart from the average case and the fixed-key case, recently, Abdelraheem et al. [1] have managed to compute the distribution of linear characteristic bias for several interesting examples. Moreover, there has been quite some interest towards deducing key information from the value of the bias [7,28,30]. Kim [19] studies the combined related-key linear-differential attacks on block ciphers. Interestingly, a linear-hull version of Matsui's Algorithm 1 by Röck and Nyberg [32] uses the fact that, in some ciphers, the linear characteristic biases ε_θ are the same for different keys.

At the same time, much less is known about the even more fundamental question of how *the bias* ε *of the entire linear approximation behaves under a change of key.* This is not least due to the fact that the entire linear hull is notoriously difficult to analyze for the immense number of linear characteristics θ comprising it. In this paper, we tackle this problem and reveal a property for many block ciphers, namely, that *the bias* ε *of a linear approximation can be actually invariant under the modification of the key.*

1.2 Our contributions

The contributions of this paper are as follows.

Bias invariant under key difference in iterative block ciphers. We investigate the bias of a linear approximation in *key-alternating ciphers* (iterative SPN ciphers with XOR addition of subkeys) under a change of the key. By looking at the composition of the fixed-key linear hull from individual characteristics, we derive a sufficient condition on the keys and linear approximations such that *the bias remains unaffected by a change of key.* The class of key-alternating ciphers is already broad enough to include AES, most of the other SPN ciphers, and some Feistel ciphers. After recalling some background on linear cryptanalysis in Section 2, we describe these findings in Section 3.

An instructive example with AES. With our technique, the key difference invariant bias property is easy to construct over (a part of) susceptible ciphers since it mainly depends on the differential diffusion in the key schedule and on the linear diffusion in the data transform of a cipher. We use AES to show how the property can be derived. Namely, we demonstrate a key difference invariant bias property holding deterministically over 5 rounds of the original AES-256. This serves as a pedagogical illustration. See Section 3.3.

Statistical distinguisher and generic key recovery. The probability to have the key difference invariant bias property in an idealized block cipher with block size n, is about $\frac{1}{\sqrt{2\pi}} 2^{\frac{3-n}{2}}$. This forms the basis for a statistical distinguisher that can be used for key recovery. Here, we use the fact that the *key difference invariant bias property is actually truncated*, i.e., there are many linear approximations with key difference invariant bias in most susceptible ciphers. In our distinguisher, for two keys, we compute the sample biases of a set of approximations with this property (using the part of the plaintext-ciphertext pairs available to the adversary) and test their collective proximity. We demonstrate that it is possible to efficiently distinguish this from an idealized cipher, under some basic independency assumptions. The distinguisher can be used for hash functions and block ciphers. In the related-key setting, we propose a key recovery procedure for block ciphers which is similar to Matsui's Algorithm 2. These techniques are given in Section 4.

Applications to block ciphers LBlock and TWINE. As an illustration, we apply our new cryptanalytic technique of key difference invariant bias to the recently proposed block ciphers LBlock [39] and TWINE [37] . LBlock was designed by Wu et al. and presented in ACNS 2011. Its state and key sizes are 64 and 80 bits respectively. LBlock has received the attention of many cryptographers and various attacks have been published so far on some reduced versions [16, 20–22, 26, 33, 34]. The best attack breaks 22 rounds of the cipher. TWINE is a block cipher proposed in SAC 2012 by Suzaki et al. that is operating on a 64-bit state that is parameterized by keys of length 80 or 128 bits. The total number of rounds is 36. The best known attack on TWINE-128, is an impossible differential attack given in [37], that breaks 24 rounds of the cipher.

We identify key difference invariant bias properties over 16 rounds of LBlock and 17 rounds of TWINE-128. This allows us to attack 24-round LBlock and 27-round TWINE-128 in the classical related-key model with differences in the user-supplied master keys. Thus, our attacks improve upon the state-of-the-art cryptanalysis for both LBlock and TWINE by breaking 2 and 3 more rounds, respectively, than the best previous attacks. Our cryptanalysis is provided in Sections 5 and Section 6.

2 Preliminaries

2.1 Key-alternating ciphers

A *block cipher* operating on n-bit blocks with a k-bit key can be seen as a subset of cardinality 2^k of the set of all $2^n!$ permutations over the space of n-bit strings. In an *idealized block cipher*, this subset is randomly chosen. In all practical settings, however, one is concerned with efficiently implementable block ciphers. So all block ciphers used in practice contain at their core the iterative application of r similar invertible transformations (called *rounds*). *Key-alternating block ciphers* form a special but important subset of the modern block ciphers (see Figure 1):

Definition 1 (Key-alternating block cipher [9]). *Let each round i, $1 \leq i \leq r$, of a block cipher have its own n-bit subkey k_i. This block cipher is* key-alternating, *if 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 the first round.*

The $r+1$ round subkeys $k_0, k_1, \ldots, k_{r-1}, k_r$ build the *expanded key* K (of length $n(r+1)$ bits) which is derived from the user-supplied key κ using a key-schedule algorithm φ. Numerous popular and widely used block ciphers belong to the class of key-alternating block ciphers. Among others, almost all SPNs (including AES) and some Feistel ciphers are key-alternating [11].

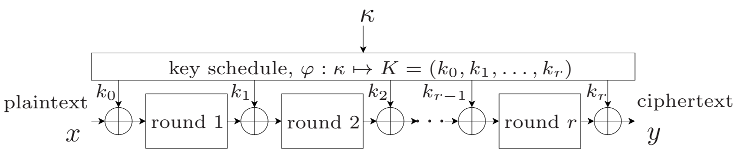


Fig. 1. Key-alternating cipher

2.2 Linear approximations and bias

We briefly recall the concepts of linear approximations and bias. We denote the scalar product of binary vectors by $a^t x = \bigoplus_{i=1}^{n} a_i x_i$. Linear cryptanalysis is based on *linear approximations* determined by input mask a and output mask b. A linear approximation (a, b) of a vectorial function f has a *bias* defined by

$$\varepsilon_{a,b}^{f} = \Pr_{x}\{b^t f(x) \oplus a^t x\} - 1/2$$

to which we also refer simply as ε if its assignment to function and linear approximation is clear from the context. We call a linear approximation *trivial* if both a and b are zero. Otherwise, with both $a \neq 0$ and $b \neq 0$, it is *non-trivial.*

2.3 Linear characteristics and linear hulls

A linear approximation (a, b) of an iterative block cipher (e.g. a key-alternating block cipher of Definition 1) is called a *linear hull* in [29]. The linear hull contains all possible sequences of the linear approximations over individual rounds, with input mask a and output mask b. These sequences are called *linear characteristics* which we denote by θ. Now we recall the relations between the bias of a linear characteristic and the bias of the entire linear hull it belongs to, for key-alternating block ciphers.

Given a linear hull (a, b), a linear characteristic θ is the concatenation of an input mask $a = \theta_0$ before the first round, an output mask $b = \theta_r$ after the last round, and $r - 1$ intermediate masks θ_i between rounds $i - 1$ and i:

$$\theta = (\theta_0, \theta_1, \dots, \theta_{r-1}, \theta_r). \tag{1}$$

Thus, each linear characteristic consists of $n(r + 1)$ bits (cf. the length of the expanded key K). The *bias ε_θ of the linear characteristic θ* is defined as the scaled product of the individual biases $\varepsilon_{\theta_{i-1},\theta_i}$ over each round:

$$\varepsilon_\theta = 2^{r-1} \prod_{i=1}^{r} \varepsilon_{\theta_{i-1},\theta_i}.$$

In a key-alternating cipher, only the sign of ε_θ depends on the key value, while the absolute bias value $|\varepsilon_\theta|$ remains exactly the same for all keys. As a reference point, we denote by $d_\theta \in \{0, 1\}$ the sign of the linear characteristic bias with expanded key $K = 0$:

$$\varepsilon_\theta[0] = (-1)^{d_\theta} |\varepsilon_\theta|.$$

Now we formulate the following central proposition that deterministically connects the linear approximation bias with the individual linear characteristic biases through a fixed key value:

Proposition 1 ([9, Subsection 7.9.2]). *For a key-alternating block cipher, the bias ε of a non-trivial linear hull (a, b) is*

$$\varepsilon = \sum_{\theta:\theta_0=a,\theta_r=b} (-1)^{d_\theta + \theta^t K} |\varepsilon_\theta|.$$

We will be relying on Proposition 1 in the next section to determine when ε is invariant under a change of key.

3 Towards bias invariant under key difference

For a non-trivial linear hull (a, b) of a block cipher, let ε and ε' be two biases under two distinct keys κ and κ', respectively. Now we consider when $\varepsilon = \varepsilon'$ with $\kappa \neq \kappa'$, that is, when the bias is invariant under a change of key.

3.1 Key difference invariant bias in key-alternating ciphers

In a key-alternating block cipher, let K and K' be the expanded keys corresponding to two user-supplied keys κ and κ', $K = \varphi(\kappa)$ and $K' = \varphi(\kappa')$ for key schedule φ as in Section 2, such that $K' = K \oplus \varDelta$ where the difference $\varDelta$ describes a connection between K and K'. We will now derive a condition on $\varDelta$ and θ such that the value of linear approximation bias $\varepsilon = \varepsilon'$ is unaffected by the key change $\kappa \neq \kappa'$.

In a key-alternating cipher, the bias for an expanded key can be computed due to Proposition 1. That is:

$$\varepsilon = \sum_{\theta:\theta_0=a,\theta_r=b} (-1)^{d_\theta+\theta^t K}|\varepsilon_\theta| \text{ and } \varepsilon' = \sum_{\theta:\theta_0=a,\theta_r=b} (-1)^{d_\theta+\theta^t K'}|\varepsilon_\theta|. \qquad (2)$$

We want to attain the equality $\varepsilon = \varepsilon'$, so we study when both sides of (2) are equal: One can observe that the only part that is different are *the signs of the individual linear characteristic biases*. Therefore, the equation will hold if all the signs are equal, that is, if the following is satisfied for each θ:

$$d_\theta + \theta^t K = d_\theta + \theta^t K'. \qquad (3)$$

Since d_θ is the same, (3) holds if and only if $\theta^t(K \oplus K') = 0$. Recalling that we denote $K \oplus K'$ by $\varDelta$, we have the following statement:

Theorem 1 (Key difference invariant bias for key-alternating ciphers). *Let (a,b) be a non-trivial linear hull of a key-alternating block cipher. Its biases ε for expanded key K and ε' for expanded key K' with $K = K' \oplus \varDelta$ have exactly equal values $\varepsilon = \varepsilon'$, if $\theta^t \varDelta = 0$ for each linear characteristic θ of the linear hull (a,b) with $\varepsilon_\theta \neq 0$.*

Theorem 1 yields a sufficient condition on the relation between the masks of linear characteristics and the expanded key difference for the key difference invariant bias property to hold. We will deal with this in the next subsection.

3.2 Sufficient condition for key difference invariant bias

For a fixed pair of keys K and K', the difference $\varDelta$ connecting them is also constant. At the same time, the linear masks θ will be different for each linear characteristic in the given linear hull (a,b). Thus, $\varDelta$ can be seen as a linear mask itself on θ that *chooses* certain positions in characteristics θ, cf. (1).

In a linear characteristic θ, we address each of the $n(r+1)$ bits by $\theta(j)$, $j = 1, \ldots, n(r+1)$. We focus on bit positions $\theta(j)$ in linear characteristics θ such that $\theta(j) = 0$ for all θ with $\varepsilon_\theta \neq 0$. We call such positions **zero positions**. Otherwise, a position is called a **nonzero position**.

Now we are ready to formulate a more explicit sufficient condition for deterministically keeping $\theta^t \varDelta = 0$:

Condition 1 (Sufficient condition for key difference invariant bias) *For a fixed non-trivial linear approximation (a,b) of a key-alternating block cipher, the relation between a pair of the user-supplied keys κ and κ' is such that the expanded key difference $\varDelta = K \oplus K'$ chooses an arbitrary number of zero positions and no nonzero positions in the linear characteristics θ of the linear hull, with $\varepsilon_\theta \neq 0$.*

Once Condition 1 is fulfilled, Theorem 1 becomes applicable with $\theta^t \varDelta = 0$ and yields $\varepsilon = \varepsilon'$.

In the next subsection, for instructive and pedagogical purposes, we show one example of key difference invariant bias property using Condition 1 with AES.

3.3 The instructive example of AES

Here we provide an illustration of the key difference invariant bias property for AES. The goal of this section is mainly pedagogical and we simply aim to show how such a property can be derived in practice. We demonstrate a key difference invariant bias property for reduced-round AES-256. We provide an example where Condition 1 is satisfied, which in turn makes Theorem 1 applicable.

For AES-256, let the two user-supplied 32-byte keys be connected by

$$\kappa \oplus \kappa' = \begin{bmatrix} 0\,0\,0\,0\,0\,0\,\delta\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0 \end{bmatrix} \tag{4}$$

with the first byte $\delta \neq 0$ of the 7-th column being the only non-zero byte. Furthermore, let the (truncated) linear approximation be defined by the 16-byte input/output masks:

$$a = \begin{bmatrix} a\,0\,0\,0 \\ 0\,0\,0\,0 \\ 0\,0\,0\,0 \\ 0\,0\,0\,0 \end{bmatrix} \text{ and } b = \begin{bmatrix} b\,0\,0\,0 \\ 0\,0\,0\,0 \\ 0\,0\,0\,0 \\ 0\,0\,0\,0. \end{bmatrix} \tag{5}$$

The masks define a linear hull for any non-zero byte values a and b. We show that the key difference (4) and the linear hulls (5) result in the key difference invariant bias property for 5 rounds of AES-256.

The AES data transform diffuses a single-byte input mask to the full state only after two rounds. Analogously, a single-byte output mask applies to the full state only after three rounds of backward computations. This fact makes Condition 1 applicable to AES. The byte positions involved into the propagation of linear patterns over 5 rounds of AES with a and b above as input/output masks are shown as ■ in Figure 2. Correspondingly, byte positions not involved are depicted as □. Since AddRoundKey is addition with constant and MixColumns is an affine operation, one can exchange their order under the suitable modification of the subkey value. In this case, ShiftRows is followed directly by the modified AddRoundKey (AK') which is the case in the last round of Figure 2.

We track the propagation of the difference in the user-supplied key to the expanded key difference which is shown as ╳ in Figure 2. $\kappa \oplus \kappa'$ specified above satisfies Condition 1. In Figure 2, all non-zero bytes ╳ of Δ are only concentrated in impossible positions □ of θ and do not interfere with ■.
Thus, $\varepsilon = \varepsilon'$ is fulfilled with probability 1 and the key difference invariant bias property holds deterministically.

3.4 Key difference invariant bias and idealized cipher

In random block ciphers, the bias ε under a fixed key is the bias for a fixed randomly drawn permutation. Using [10, Theorem 4.7], one can demostrate that

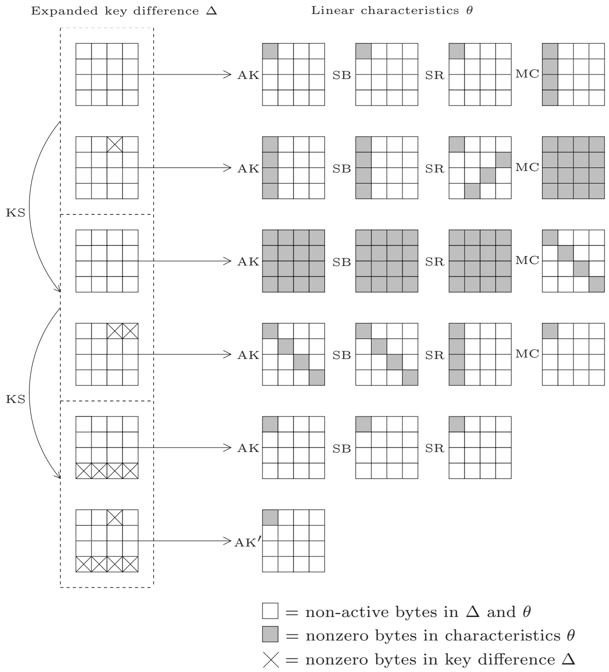

Expanded key difference Δ
Linear characteristics θ
KS
KS
AK
SB
SR
MC
AK
SB
SR
MC
AK
SB
SR
MC
AK
SB
SR
MC
AK
SB
SR
AK′
□ = non-active bytes in Δ and θ
▨ = nonzero bytes in characteristics θ
☒ = nonzero bytes in key difference Δ

Fig. 2. Key difference invariant bias for 5 rounds of AES-256

the probability for the biases with two different keys to be exactly equal is $\Pr\{\varepsilon = \varepsilon' | \kappa \neq \kappa'\} \approx \frac{1}{\sqrt{2\pi}} 2^{\frac{3-n}{2}}$ for block sizes $n \geq 5$. Thus, the key difference invariant property for idealized block ciphers is a rare event, which yields a distinguisher for susceptible ciphers outlined in the next section.

4 Statistical distinguisher and key recovery with key difference invariant bias

In this section, we present the statistical distinguisher based on the key difference invariant bias for an n-bit block cipher, followed by a generic key recovery procedure.

4.1 Distinguisher

In the distinguisher, our aim is to tell if we deal with the target cipher featuring the property or an idealized cipher. The setup for the statistical test is as follows. Suppose that we are given N plaintext-ciphertext pairs and λ linear approximations under a pair of expanded keys (K, K') connected by Δ in the way described in Condition 1. Then, for each one of these linear approximations we compute and store in counters S_i and S'_i, $1 \leq i \leq \lambda$, which account for the number of times these approximations are satisfied for K and K' with the N texts. The counters S_i and S'_i suggest empirical biases $\hat{\varepsilon}_i = \frac{S_i}{N} - \frac{1}{2}$ and $\hat{\varepsilon}'_i = \frac{S'_i}{N} - \frac{1}{2}$ respectively. We evaluate consequently the following statistic s:

$$s = \sum_{i=1}^{\lambda} \left[\left(\frac{S_i}{N} - \frac{1}{2} \right) - \left(\frac{S'_i}{N} - \frac{1}{2} \right) \right]^2 .$$

We expect the statistic s to be lower for the target cipher, featuring the key difference invariant bias property, than for a random cipher. As we aim to perform key-recovery with this test, we will derive the distribution of this statistic for the right key guess (assuming the target structure) and for the wrong key guess (assuming a random cipher).

Right key guess. The empirical bias value $\hat{\varepsilon}_i$ for the i-th linear approximation approximately follows the normal distribution with the exact value of bias ε_i as mean and variance $1/4N$ with good precision (cf., e.g., [14,35]) for sufficiently large N:

$$\hat{\varepsilon}_i \sim \mathcal{N}(\varepsilon_i, 1/4N).$$

In this case, the following proposition holds:

Proposition 2 (Distribution of statistic s for the right key). *Consider λ nontrivial linear approximations for a block cipher under a pair of expanded keys (K, K') connected by Δ conforming to Condition 1. If N is the number of known plaintext-ciphertext pairs, S_i and S'_i are the numbers of times such a linear approximation is fulfilled for K and K', respectively, $i \in \{1, \ldots, \lambda\}$, and λ is high enough, then, assuming the counters S_i and S'_i are all independent, the following approximate distribution holds for sufficiently large N and n:*

$$s \sim \mathcal{N}\left(\frac{\lambda}{2N}, \frac{\lambda}{2N^2} \right).$$

Proof. See the full version of this paper [2].

Wrong key guess. In this case, we base upon the hypothesis that for a wrong key, we deal with a random cipher consisting of permutations drawn at random. Then, each of the values $\hat{\varepsilon}_i$ can be approximated by a normal distribution with mean ε_i and variance $1/4N$ for sufficiently large N:

$$\hat{\varepsilon}_i \sim \mathcal{N}(\varepsilon_i, 1/4N) \text{ with } \varepsilon_i \sim \mathcal{N}(0, 1/2^{n+2}),$$

where ε_i is the exact value of the bias which is itself distributed over n-bit random permutations for $n \geq 5$ [10,31].

Then we have then the following proposition for the distribution of the statistic s:

Proposition 3 (Distribution of statistic s for the wrong key). *Consider λ nontrivial linear approximations for two randomly drawn permutations. If N is the number of known plaintext-ciphertext pairs, S_i and S'_i are the numbers of times a linear approximation is fulfilled for these two permutations,*

$i \in \{1, \ldots, \lambda\}$, and λ is high enough, then, assuming the independency of all S_i and S'_i, the following approximate distribution holds for sufficiently large N and n:

$$s \sim \mathcal{N}\left(\frac{\lambda}{2N} + \frac{\lambda}{2^{n+1}}, \frac{\lambda}{2N^2} + \frac{\lambda}{2^{2n+1}} + \frac{\lambda}{N2^n}\right).$$

Proof. See the full version of this paper [2].

Data complexity of distinguisher. In the two above cases, we have seen that the statistic s will follow, depending on if we deal with the right or the wrong key, two different normal distributions. In the first case, it follows the normal distribution with mean $\mu_0 = \frac{\lambda}{2N}$ and variance $\sigma_0^2 = \frac{\lambda}{2N^2}$, while in the second case it follows the normal distribution with mean $\mu_1 = \frac{\lambda}{2N} + \frac{\lambda}{2^{n+1}}$ and variance $\sigma_1^2 = \frac{\lambda}{2N^2} + \frac{\lambda}{2^{2n+1}} + \frac{\lambda}{N2^n}$. It has to be decided if the obtained statistic s is from $\mathcal{N}(\mu_0, \sigma_0^2)$ or from $\mathcal{N}(\mu_1, \sigma_1^2)$. To do that, we perform a test that compares the statistic s to a threshold value τ. This test says that s belongs to $\mathcal{N}(\mu_0, \sigma_0^2)$ if $s \leq \tau$ and that s belongs to $\mathcal{N}(\mu_1, \sigma_1^2)$, otherwise.

As in any statistical test, one has to deal with two types of error probabilities here. The first one – denoted by α_0 – is the probability to reject the right key, whereas the second one – denoted by α_1 – is the probability to accept a wrong key. The decision threshold used is $\tau = \mu_0 + \sigma_0 q_{1-\alpha_0} = \mu_1 - \sigma_1 q_{1-\alpha_1}$, where $q_{1-\alpha_1}$ and $q_{1-\alpha_0}$ are the quantiles of the standard normal distribution $\mathcal{N}(0, 1)$. This simple test is visualized in Figure 3.

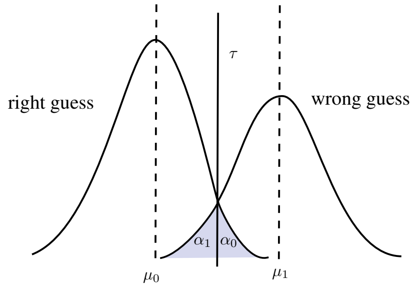


Fig. 3. Statistical test for key difference invariant bias in key recovery

It is well known [12] that in order for such a test to have error probabilities of at most α_0 and α_1, the parameters μ_0, σ_0^2, μ_1 and σ_1^2 should be such that $q_{1-\alpha_1}\sigma_1 + q_{1-\alpha_0}\sigma_0 = |\mu_1 - \mu_0|$.

Now, using Proposition 2 and Proposition 3, we obtain the following equation that determines the amount of data needed by the distinguisher:

$$N = \frac{2^{n+0.5}}{\sqrt{\lambda} - q_{1-\alpha_1}\sqrt{2}} \left(q_{1-\alpha_0} + q_{1-\alpha_1}\right). \tag{6}$$

4.2 How to recover the key with key difference invariant bias

Here, we describe a generic key recovery attack approach that can be applied to block ciphers for which a key difference invariant bias property for r rounds has been identified. This procedure is described in Algorithm 1. We will feed this algorithm with the related key differential paths that are going to be used for the attack. Other entries to the algorithm will be the number of rounds of the distinguisher r, the number of rounds r_{top} that we are going to append at the top of the distinguisher and the number of rounds r_{bot} that we are going to add at the bottom of the distinguisher. In Algorithm 1, $V[x]$ and $V'[x']$ are the counters containing the number of times the partial state values x and x' (values corresponding to non-zero mask of linear approximations) occur for N plaintext-ciphertext pairs under the key pair.

Algorithm 1 Generic Attack Procedure

```
Require: A set of linear approximations $(a, b)$ and master key difference $\delta = \kappa \oplus \kappa'$
    with the key difference invariant bias property holding.
for all related-key differential paths with a difference $\delta$ on the master-key do
    Collect $N$ plaintext-ciphertext pairs $(P, C)$ under a key $\kappa$.
    Collect $N$ plaintext-ciphertext pairs $(P', C')$ under $\kappa' = \kappa \oplus \delta$.
    Partially encrypt $r_{top}$ rounds and partially decrypt $r_{bot}$ rounds, obtain partial
    state values $x$ and $x'$ covered by the input/output masks of $(a, b)$ and compute
    $V[x]$ and $V'[x']$ (number of times these partial state values occur).
    Allocate a counter $s$.
    for all linear approximations $(a, b)$ do
        Allocate counters $S$ and $S'$ and set them to zero.
        for all values of $x$ and $x'$ do
            if the linear approximation holds then
                Add $V[x]$ and $V[x']$ to $S$ and $S'$, respectively.
            end if
        end for
        Compute $s = s + \left[\left(\frac{S}{N} - \frac{1}{2}\right) - \left(\frac{S'}{N} - \frac{1}{2}\right)\right]^2$.
    end for
    if $s \leq \tau$ then
        The guessed subkey is a possible subkey value.
        Check exhaustively the remaining keys against several plaintext-ciphertext
        pairs.
    end if
end for
return encryption key.
```

5 Attack on 24-round LBlock

LBlock is a lightweight block cipher presented at ACNS 2011 by Wu and Zhang [39]. It uses 64-bit block and 80-bit key and is based on a modified 32-round Feistel structure. Its description is provided in the full version of this paper [2].

5.1 Previous cryptanalysis

Despite its recent proposal, LBlock has already been extensively analyzed. For example, impossible differential attacks have been mounted in the single-key model [16, 21, 39] as well as attacks in the related-key model [26]. A related-key truncated differential attack on 22-round LBlock was given in [22]. Some other results concern integral cryptanalysis [20, 33, 34, 39]. A zero-correlation linear attack was equally mounted against 22 rounds of LBlock [36]. Finally, biclique attacks [17, 40] provide only a small gain against exhaustive search. So the currently best non-exhaustive attacks against LBlock can break at most 22 rounds.

In this paper, we propose an attack on 24 rounds of LBlock. Our results are summarized and compared to previous cryptanalysis in Table 1.

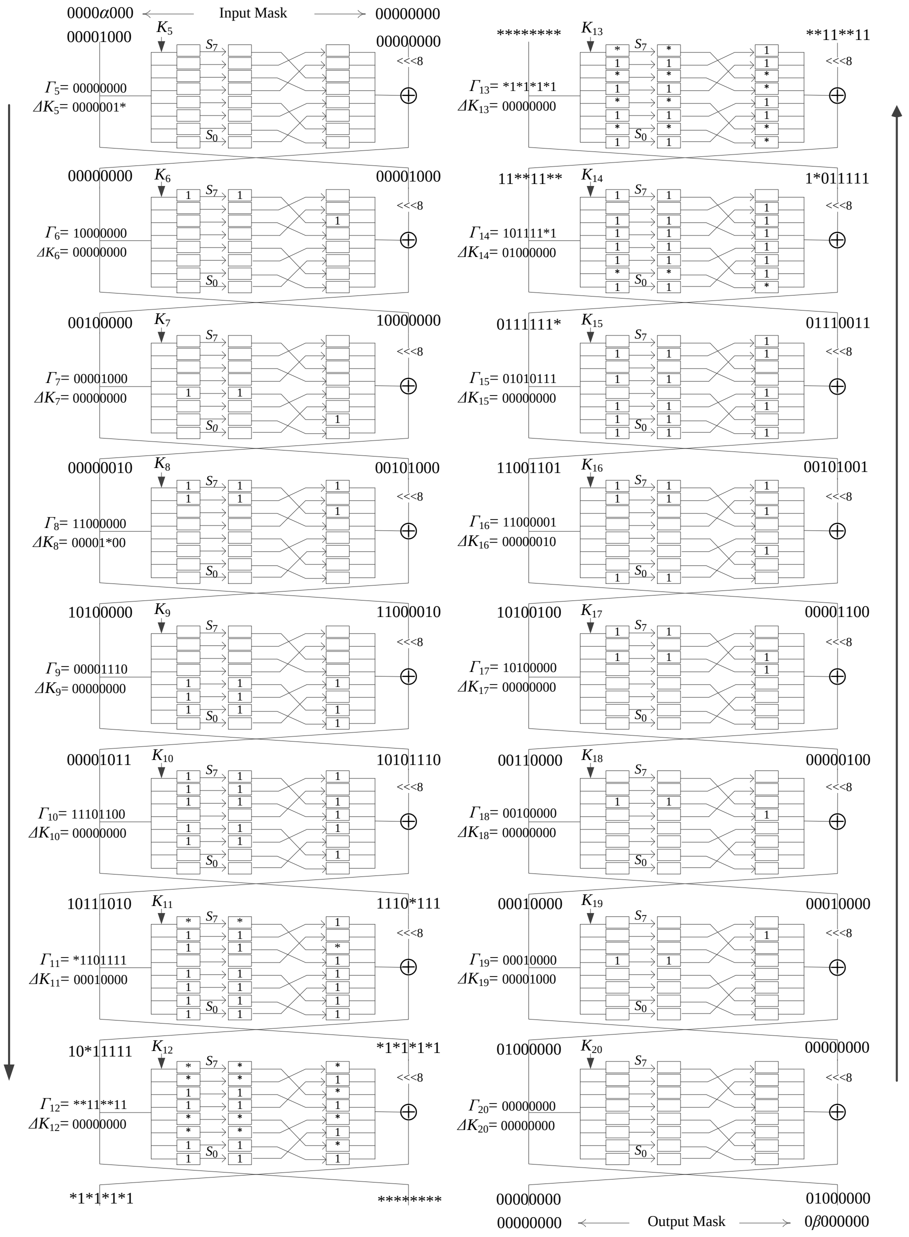
Table 1. Summary of attacks on LBlock

Model	Attack	#Rounds	#keys	Data per key	Time	Memory	Ref.
SK	Imp. Diff	20	1	2^{63} CP	$2^{72.7}$	2^{68}	[39]
	Imp. Diff	21	1	$2^{62.5}$CP	$2^{73.7}$	$2^{55.5}$	[21]
	Imp. Diff	21	1	2^{63}CP	$2^{69.5}$	2^{75}	[16]
	Imp. Diff	22	1	2^{58}CP	$2^{79.28}$	2^{76}	[16]
	Integral	20	1	$2^{63.7}$CP	$2^{63.7}$	N/A	[39]
	Integral	20	1	$2^{63.6}$CP	$2^{39.6}$	2^{35}	[33]
	Integral	22	1	$2^{61.6}$CP	$2^{71.2}$	N/A	[20]
	Integral	21	1	$2^{61.6}$CP	$2^{54.1}$	$2^{51.58}$	[34]
	Integral	22	1	2^{61}CP	2^{70}	2^{63}	[34]
	Zero-Correlation	22	1	2^{64}KP	$2^{70.54}$	2^{64}	[36]
	Zero-Correlation	22	1	$2^{62.1}$KP	$2^{71.27}$	2^{64}	[36]
	Zero-Correlation	22	1	2^{60}KP	2^{79}	2^{64}	[36]
RK	Imp. Diff	22	8	2^{47}RKCP	2^{70}	N/A	[26]
	Differential	22	2	$2^{63.1}$RKCP	2^{67}	N/A	[22]
	Key Diff Inv Bias	**24**	32	$2^{62.29}$ **RKKP**	$2^{74.59}$	2^{61}	**Here**
	Key Diff Inv Bias	**24**	32	$2^{62.95}$ **RKKP**	$2^{70.67}$	2^{61}	**Here**

5.2 Linear approximations with key difference invariant bias for LBlock

We start by presenting the linear approximations with key difference invariant bias under two keys related by a difference on a single nibble of the master key. These linear approximations depicted in Figure 4, hold for 16 rounds (from round 5 to round 20) under the related-key differential paths depicted in the full version of this paper [2]. The input mask of the 5-th round is $(0000\alpha00000000000)$ and the output mask of the 20-th round is $(000000000\beta000000)$, $\alpha \neq 0, \beta \neq 0$. There are in total $(2^4 - 1) \cdot (2^4 - 1) \approx 2^{7.81}$ such linear approximations.

We can see from Figure 4 that the relations $\Gamma_r \cdot \Delta K_r = 0$, for $5 \leq r \leq 20$ hold for all the related-key differential paths listed in the full version of this paper [2]. Therefore Condition 1 is satisfied, so the linear approximations in Figure 4 have a key difference invariant bias under the related-key differential paths listed in the full version of this paper [2].



$\Gamma_r, 5 \leq r \leq 20$: input mask value for the S-boxes in round r.
$\Delta K_r, 5 \leq r \leq 20$: the subkey difference in round r.
In masks, '0', '1' and '*': zero, nonzero and arbitrary mask for a nibble, resp.
In differences, '0' , '1' and '*': zero, nonzero and arbitrary difference for a nibble, resp.

Fig. 4. 16-round linear approximations with key difference invariant bias for LBlock

The related-key differential paths that we used for our attack are presented in the full version of this paper [2].

5.3 Key recovery for 24-round LBlock

The 16-round linear approximations with key difference invariant bias that we used for our attack start before round 5 and end after round 20. The initial four rounds, round 1 to round 4, are added before the linear approximations and the final four rounds, round 21 to round 24, are appended after the linear approximations. The details of this stage, and the nibbles to be computed in the initial and the final four rounds are shown in the full version of this paper [2]. For this attack, $r = 16$, $r_{top} = 4$ and $r_{bot} = 4$. These elements will be input to Algorithm 1.

Attack procedure for 24-round LBlock. The attack for LBlock will follow the attack procedure described in Algorithm 1. For this reason the Steps 2 and 3 of Algorithm 1 do not have to be executed for every path of Step 1. The Step 4 of Algorithm 1 for LBlock is composed itself of 14 consecutive steps. The details of Step 4 are presented in the full version of this paper [2].

After proceeding from Step 5 to Step 15, we obtain the counter s containing the χ^2 statistics for the subkey guess. The right value of guessed 53-bit subkey is likely to be among the candidates with the statistic s lower than or equal to the threshold $\tau = \frac{\sqrt{\lambda}}{N\sqrt{2}} q_{1-\alpha_0} + \frac{\lambda}{2N}$. All cipher keys it is compatible with are tested exhaustively against a maximum of 2 plaintext-ciphertext pairs.

Complexity estimation. We start by evaluating the complexity of Step 4. From Step 4.1 to Step 4.14, the time complexity is $T_1 = N \cdot 2^4 \cdot 2 + 2^{60} \cdot 2^8 \cdot 2 + 2^{56} \cdot 2^{12} \cdot 2 + 2^{52} \cdot 2^{13} \cdot 2 + 2^{48} \cdot 2^{17} \cdot 2 + 2^{44} \cdot 2^{21} \cdot 2 + 2^{40} \cdot 2^{25} \cdot 2 + 2^{36} \cdot 2^{29} \cdot 2 + 2^{32} \cdot 2^{33} \cdot 2 + 2^{28} \cdot 2^{37} \cdot 2 + 2^{24} \cdot 2^{41} \cdot 2 + 2^{20} \cdot 2^{45} \cdot 2 + 2^{16} \cdot 2^{49} \cdot 2 + 2^{12} \cdot 2^{53} \cdot 2 = N \cdot 2^5 + 2 \cdot 2^{69} + 11 \cdot 2^{66}$.

We will compute N by using Equation (6), after choosing the values of α_0 and α_1. Here, the number of linear approximations is $\lambda = 2^{7.81}$ and $n = 64$. Different choices of α_0 and α_1 will provide a time-complexity trade-off. We start by choosing some concrete values for α_0 and α_1 that lead to an optimized time complexity. By setting $\alpha_0 = 2^{-2.7}$ and $\alpha_1 = 2^{-8.5}$, we have $q_{1-\alpha_0} \approx 1.02$ and $q_{1-\alpha_1} \approx 2.77$. In this way $N \approx 2^{62.95}$ (Note that the same N (P, C) pairs or N (P', C') pairs can be reused for different related-key differential paths under the condition that $\Delta\kappa_{14\sim17}$ remains the same.) and the threshold value gets $\tau \approx 2^{-55.02}$. Then, $T_1 \approx 2^{70.95}$ times of $\frac{1}{8}$ round encryption which is equivalent to $2^{63.37}$ times of 24-round encryptions. Note that the time complexity of the procedure described in Steps 6$\sim$14 is negligible. Under each related-key differential path, the value of $\kappa_{14\sim17}$ is already known, so the time complexity of Steps 16-19 is about $2^{76} \cdot 2^{-8.5} = 2^{67.5}$ times of 24-round encryption. Therefore, the total complexity from Step 2 to Step 18 is about $2^{67.58}$ encryptions. After proceeding from Step 2 to Step 18, if we can not succeed, this means that the value of the right key does not belong to the values corresponding to the related-key differential path tested. We can then use another related-key differential path to proceed the above attack. All possible values of the master key bits $\kappa_{4\sim21}$ are covered by the related-key differential paths, so we could always find the right key where in the worst case, all the related-key differential paths have to be tested. So the expected time complexity of our attack on 24-round LBlock is about $2^{67.58}\cdot[1+(1-\frac{1}{16})+\cdots+(1-\frac{15}{16})]\approx 2^{70.67}$ 24-round encryptions. The data complexity is $2^{62.95}$ known plaintexts under each master key, while $2^{60}\cdot 2=2^{61}$ bytes of memory are required to store the counters.

Another possible choice of α_0 and α_1 can lead to a different time-data complexity trade-off. For example, if we set $\alpha_0 = 2^{-2.7}$ and $\alpha_1 = 2^{-4.5}$, then $q_{1-\alpha_0}\approx 1.01$ and $q_{1-\alpha_1}\approx 1.70$, we get $N\approx 2^{62.29}$. For these parameters the expected time complexity is about $2^{74.59}$ encryptions and the expected data complexity is $2^{62.29}$ known plaintexts for each master key. The memory requirements are the same as in the previous attack.

Other possible time-data trade-offs with $\beta_0 = 2^{-2.7}$ for the attack on LBlock can be visualized in Figure 6.

6 Attack on 27-round TWINE-128

TWINE is a lightweight block cipher proposed by Suzaki, Minematsu, Morioka and Kobayashi in [37]. Its structure is based on a modified Type-2 generalized Feistel scheme. The cipher's description is given in the full version of this paper.

6.1 Previous cryptanalysis

In the original proposal of TWINE [37], the authors analyze the resistance of TWINE against various types of attacks, such as impossible differential and saturation attacks. The best analysis in this proposal is an impossible differential attack against 23 rounds of TWINE-80 and against 24 rounds of TWINE-128. Moreover, biclique attacks have been mounted in [17] for both full-round versions of TWINE, but the time complexity of these attacks is only marginally lower than exhaustive search.

6.2 Linear approximations with key difference invariant bias for TWINE-128

We present 17-round (from round 6 to round 22) linear approximations with key difference invariant bias under related-key differential paths for TWINE-128 in Figure 5. In our attack, the input mask of the 6-th round is $00000000000\alpha000$ and the output mask of the 22-th round is $0000000\beta00000000$, $\alpha,\beta\neq 0$. Thus, there are $15*15\approx 2^{7.81}$ such linear approximations, exactly as in the case of LBlock. We start by describing the related-key truncated differential path that we use in our attack. This differential path was found by considering only differences in only one nibble of the master key and by searching exhaustively over all such configurations.

This path is described in the full version of this paper [2]. More precisely, we consider a difference equal to 1 in the 22nd nibble of the master key. This differential path covers all the possible key values and is sufficient to recover the right key value. From Figure 5, we can see that $\Gamma_r \cdot \Delta K_r = 0$, $6 \leq r \leq 22$ (where K_r and ΔK_r denote the subkey value and the subkey difference for the round r respectively) and thus Condition 1 is satisfied.

6.3 Key recovery for 27-round TWINE-128

We utilize the 17-round distinguisher in Figure 5 to attack 27 rounds of TWINE-128. The initial five rounds from round 1 to round 5 are added before the distinguisher and the final five rounds from round 23 to round 27 are appended after the distinguisher, as shown in the full version of this paper. In such a way, the first 27 rounds of TWINE-128 are covered. The attack is proceeded by following Algorithm 1. The parameters are $r = 17$, $r_{top} = 5$, $r_{bot} = 5$, see the full version of this paper.

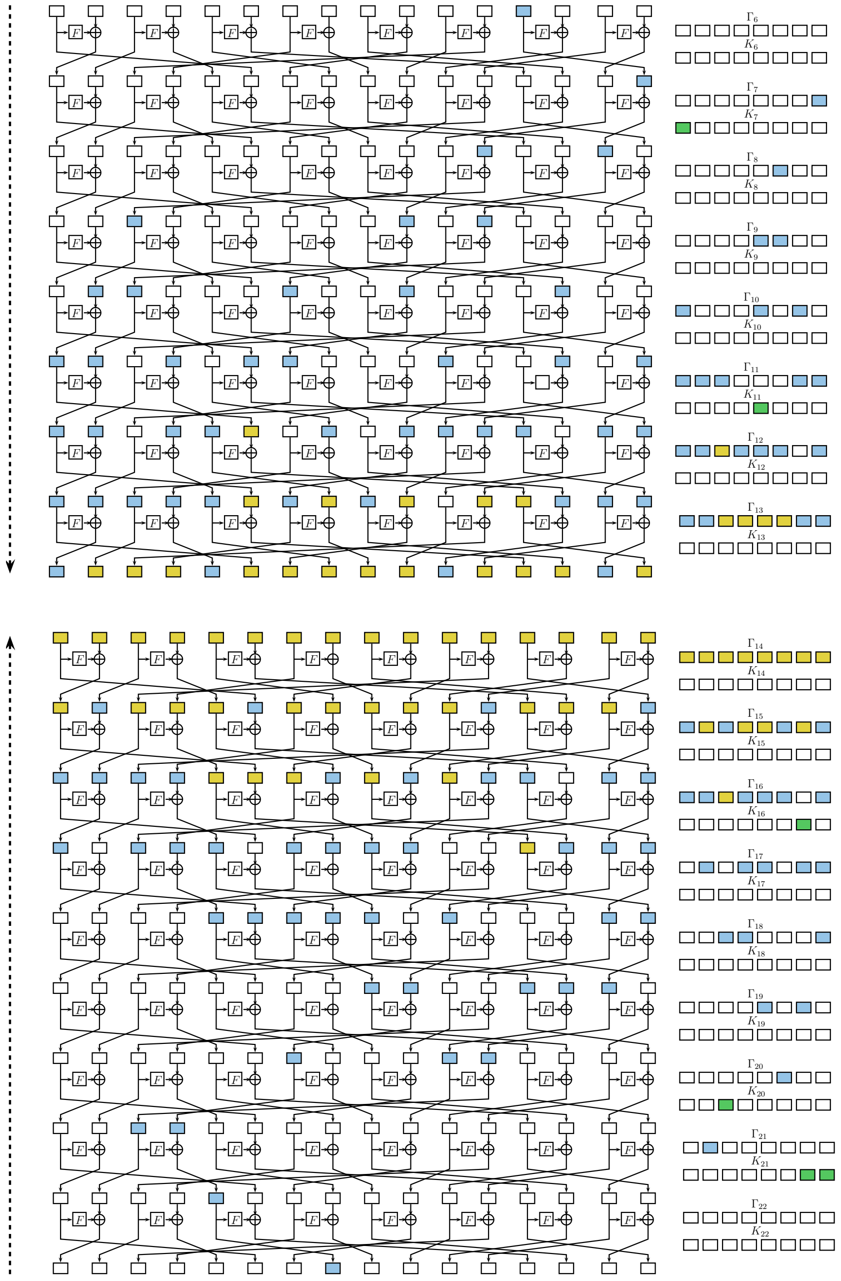
After proceeding from Step 5 to Step 15, we obtain the counter s containing the χ^2 statistics for the subkey guess. The right value of guessed 96-bit subkey is likely to be among the candidates with the statistic s lower than or equal to the threshold $\tau = \frac{\sqrt{\lambda}}{N\sqrt{2}} q_{1-\alpha_0} + \frac{\lambda}{2N}$. All cipher keys it is compatible with are tested exhaustively against a maximum of 2 plaintext-ciphertext pairs.

Complexity estimation. We start by evaluating the complexity T_1 of Steps 4.1-4.17. $T_1 = N \cdot 2^{20} \cdot 2 + N \cdot 2^{32} \cdot 15 \cdot 2 + N \cdot 2^{40} \cdot 15 \cdot 2 + 2^{60} \cdot 2^{44} \cdot 2 \cdot 15 + 2^{56} \cdot 2^{48} \cdot 2 \cdot 15 + 2^{52} \cdot 2^{52} \cdot 2 \cdot 15 + 2^{48} \cdot 2^{56} \cdot 2 \cdot 15 + 2^{44} \cdot 2^{60} \cdot 2 \cdot 15 + 2^{40} \cdot 2^{64} \cdot 2 \cdot 15 + 2^{36} \cdot 2^{68} \cdot 2 \cdot 15 + 2^{36} \cdot 2^{72} \cdot 2 \cdot 15 + 2^{32} \cdot 2^{76} \cdot 2 \cdot 15 + 2^{28} \cdot 2^{80} \cdot 2 \cdot 15 + 2^{24} \cdot 2^{84} \cdot 2 \cdot 15 + 2^{20} \cdot 2^{88} \cdot 2 \cdot 15 + 2^{16} \cdot 2^{92} \cdot 2 \cdot 15 + 2^{12} \cdot 2^{96} \cdot 2 \cdot 15 = N \cdot 2^{20} \cdot 2 + N \cdot 2^{32} \cdot 15 \cdot 2 + N \cdot 2^{40} \cdot 15 \cdot 2 + 7 \cdot 2^{104} \cdot 2 \cdot 15 + 7 \cdot 2^{108} \cdot 2 \cdot 15$.

To compute N, we will use Equation (6). Here, the number of linear approximations is $\lambda = 2^{7.81}$ and $n = 64$. Therefore N will be computed after choosing the values of α_0 and α_1. Different choices of these values will provide a data-time trade-off. We start by choosing some concrete values for α_0 and α_1 that lead to an optimized time complexity.

Consider for example $\alpha_0 = 2^{-2.7}$ and $\alpha_1 = 2^{-8.5}$. Then $q_{1-\alpha_0} \approx 1.02$ and $q_{1-\alpha_1} \approx 2.77$. By replacing these values to Equation (6), we obtain $N \approx 2^{62.95}$. The threshold value gets $\tau = \frac{\sqrt{\lambda}}{N\sqrt{2}} q_{1-\alpha_0} + \frac{\lambda}{2N} \approx 2^{-55.02}$. Thus $T_1 \approx 2^{115.81}$ times of 1/8 encryption, which is equivalent to $2^{108.05}$ times of 27-round encryption. The complexity of computing the counters S and S' is negligible. The complexity of the last step is $2^{128} \cdot 2^{-8.5} = 2^{119.5}$ times of 27-round encryption. Thus the total time complexity of the attack is about $2^{119.5}$ 27-round TWINE-128 encryptions. The data complexity is $N \approx 2^{62.95}$ known plaintexts per key and the memory requirements are 2^{61} bytes to store the counters.

In the same way, if we want to optimize the data complexity, we choose $\alpha_0 = 2^{-2.7}$ and $\alpha_1 = 2^{-4.5}$. Then $q_{1-\alpha_0} \approx 1.02$ and $q_{1-\alpha_1} = 1.70$. Equation (6) gives now $N = 2^{62.29}$ and the threshold is $2^{-54.38}$. The time complexity of the attack is $2^{123.5}$ and the data complexity is $N = 2^{62.29}$ known plaintexts per key. Figure 7 depicts different possible data-time trade-offs with $\beta_0 = 2^{-2.7}$.



Vectors Γ_r, $6 \leq r \leq 22$: input mask value of S-box.
Green nibbles: nibbles with nonzero difference in the subkeys.
Blue nibbles: nibbles w/nonzero mask
Yellow nibbles: nibbles w/undetermined mask.
White nibbles: nibbles w/zero mask or 0 subkey difference.

Fig. 5. 17-round linear approximations for key difference invariant bias for TWINE-128

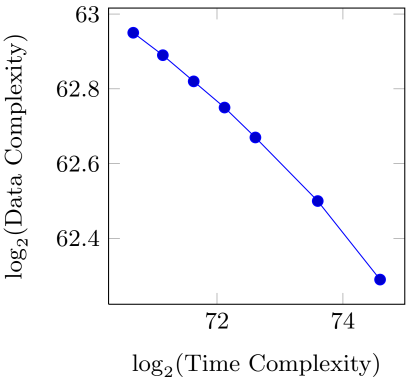


Fig. 6. Data-time trade-off for the attack on 24-round LBlock

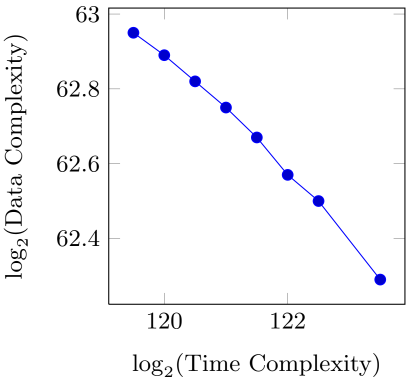


Fig. 7. Data-time trade-off for the attack on 27-round TWINE-128

7 Conclusions

In this paper, we reveal the fundamental property of key difference invariant bias in key-alternating block ciphers. We show how to identify this property efficiently. We propose a statistical distinguisher for the property and demonstrate the property for 5 rounds of AES. As an illustration, using our novel cryptanalytic technique, under related keys, we attack more rounds of LBlock and TWINE than the best previous cryptanalysis.

Acknowledgements. This work was partially supported by the Research Fund KU Leuven, OT/13/071, 973 program (No. 2013CB834205), NSFC Projects (No. 61133013 and No. 61070244), as well as Interdisciplinary Research Foundation of Shandong University (No.2012JC018).

References

1. M. A. Abdelraheem, M. Agren, P. Beelen, G. Leander. On the Distribution of Linear Biases: Three Instructive Examples. CRYPTO 2012, LNCS, vol. 7417, pp. 50–67, Springer-Verlag, 2012.
2. A. Bogdanov, C. Boura, V. Rijmen, M. Wang, L. Wen, J. Zhao. Key Difference Invariant Bias in Block Ciphers. IACR Eprint report, 2013.
3. A. Bogdanov, V. Rijmen. Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers. Accepted to Designs, Codes and Cryptography, in press, Springer-Verlag, 2012.
4. A. Bogdanov, M. Wang. Zero Correlation Linear Cryptanalysis with Reduced Data Complexity. FSE 2012, LNCS, vol. 7549, pp. 29–48, Springer-Verlag, 2012.
5. A. Bogdanov, G. Leander, K. Nyberg, M. Wang. Integral and Multidimensional Linear Distinguishers with Correlation Zero. ASIACRYPT 2012, LNCS, vol. 7658, pp. 244–261, Springer-Verlag, 2012.
6. J. Y. Cho. Linear Cryptanalysis of Reduced-Round PRESENT. CT-RSA 2010, LNCS, vol. 5985, pp. 302–317, Springer-Verlag, 2010.

7. B. Collard, F.-X. Standaert. Experimenting Linear Cryptanalysis. Advanced Linear Cryptanalysis of Block and Stream Ciphers, P. Junod, A. Canteaut (eds.), ISO Press, 2011.
8. J. Daemen, R. Govaerts, J. Vandewalle. Correlation Matrices. FSE 1994, LNCS, vol. 1008, pp. 275–285, Springer-Verlag, 1995.
9. J. Daemen, V. Rijmen. The Design of Rijndael: AES - The Advanced Encryption Standard. Springer-Verlag, ISBN 3-540-42580-2, 2002.
10. J. Daemen, V. Rijmen. Probability Distributions of Correlations and Differentials in Block Ciphers. Journal of Mathematical Cryptology 1(3), pp. 221–242, 2007.
11. J. Daemen, V. Rijmen. Probability Distributions of Correlation and Differentials in Block Ciphers. Tech. Rep. 212, IACR ePrint Report 2005/212 (2005), http://eprint.iacr.org/2005/212.
12. W. Feller. An Introduction to Probability Theory and Its Applications, 1971.
13. M. Hermelin, J.Y. Cho, K. Nyberg. Multidimensional Extension of Matsui's Algorithm 2. FSE 2009, LNCS, vol. 5665, pp. 209–227, Springer-Verlag, 2009.
14. P. Junod. On the Complexity of Matsui's Attack. SAC 2001, LNCS, vol. 2259, pp. 199–211, Springer-Verlag, 2001.
15. B. Kaliski, M. Robshaw, Linear Cryptanalysis Using Multiple Approximations. CRYPTO 1994, LNCS, vol. 839, pp. 26–39, Springer-Verlag, 1994.
16. F. Karakoç, H. Demirci, A. Harmanci. Impossible Differential Cryptanalysis of Reduced-Round LBlock. WISTP 2012, LNCS, vol. 7322, pp. 179–188, Springer-Verlag, 2012.
17. F. Karakoç, H. Demirci, A. Harmanci. Biclique Cryptanalysis of LBlock and TWINE. Inf. Process. Lett. 113(12), pp. 423–429, 2013.
18. L. Keliher, J. Sui. Exact Maximum Expected Differential and Linear Probability for Two-Round Advanced Encryption Standard. IET Information Security 1(2), pp. 53–57, 2007.
19. J. Kim. Combined Differential, Linear and Related-Key Attacks on Block Ciphers and MAC Algorithms. Ph.D. thesis, K.U.Leuven, 2006.
20. Y. Li. Integral Cryptanalysis on Block Ciphers (in Chinese). [D]. Beijing: Institute of Software, Chinese Academy of Sciences, 2012.
21. Y. Liu, D. Gu, Z. Liu, W. Li. Impossible Differential Attacks on Reduced-Round LBlock. ISPEC 2012, LNCS, vol. 7232, pp. 97–108, Springer-Verlag, 2012.
22. S. Liu, Z. Gong, L. Wang. Improved Related-Key Differential Attacks on Reduced-Round LBlock. ICICS 2012, LNCS, vol. 7618, pp. 58–69, Springer-Verlag, 2012.
23. M. Matsui. Linear Cryptanalysis Method for DES Cipher. EUROCRYPT 1993, vol. 765, pp. 386–397, Springer-Verlag, 1993.
24. M. Matsui. The First Experimental Cryptanalysis of the Data Encryption Standard. CRYPTO 1994, LNCS, vol. 839, pp. 1–11, Springer-Verlag, 1994.
25. M. Matsui, A. Yamagishi. A New Method for Known Plaintext Attack of FEAL Cipher. EUROCRYPT 1992, LNCS, vol. 658, pp. 81–91, Springer-Verlag, 1993.
26. M. Minier, M. Naya-Plasencia. A Related Key Impossible Differential Attack against 22 Rounds of the Lightweight Block Cipher LBlock. Inf. Process. Lett., 112(16), 624–629, 2012.
27. S. Murphy. The Effectiveness of the Linear Hull Effect. J. Mathematical Cryptology 6(2), pp. 137–147, 2012.
28. K. Nyberg, R. Hakala. A Key-Recovery Attack on SOBER-128, Symmetric Cryptography Dagstuhl Seminar No. 07021, 2007.
29. K. Nyberg. Linear Approximation of Block Ciphers. EUROCRYPT 1994, LNCS, vol. 950, pp. 439–444, Springer-Verlag, 1994.

30. K. Nyberg. Linear Cryptanalysis Using Multiple Linear Approximations. Early Symmetric Crypto (ESC 2010) seminar, Remich, Luxembourg, 2011. https://cryptolux.org/mediawiki.esc/images/5/52/Esc_nyberg.pdf
31. L. O'Connor. Properties of Linear Approximation Tables. FSE 1994, LNCS, vol. 1008, pp. 131–136, Springer-Verlag, 1995.
32. A. Röck, K. Nyberg. Generalization of Matsui's Algorithm 1 to Linear Hull for Key-Alternating Block Ciphers. Designs, Codes and Cryptography, 66(1-3), pp. 175–193, Springer-Verlag, 2013.
33. Y. Sasaki, L. Wang. Meet-in-the-Middle Technique for Integral Attacks against Feistel Ciphers. SAC 2012, LNCS, vol. 7707, pp. 234–251, Springer-Verlag, 2013.
34. Y. Sasaki, L. Wang. Comprehensive Study of Integral Analysis on 22-Round LBlock. ICISC 2012, LNCS, vol. 7839, pp. 156–169, Springer-Verlag, 2013.
35. A.A. Selçuk. On Probability of Success in Linear and Differential Cryptanalysis. Journal of Cryptology, Volume 21(1), pp. 131–147, Springer-Verlag, 2008.
36. H. Soleimany, K. Nyberg. Zero-Correlation Linear Cryptanalysis of Reduced-Round LBlock. Accepted to WCC 2013. To appear. http://eprint.iacr.org/2012/570.pdf, 2012.
37. T. Suzaki, K. Minematsu, S. Morioka, E. Kobayashi. TWINE : A Lightweight Block Cipher for Multiple Platforms. SAC 2012, LNCS, vol. 7707, pp. 339–354, Springer-Verlag, 2012.
38. D. Wagner. The Boomerang Attack. FSE 1999, LNCS, vol. 1636, pp.156–170, Springer-Verlag, 1999.
39. W. Wu, L. Zhang. LBlock: A Lightweight Block Cipher. ACNS 2011, LNCS, vol. 6715, pp. 327–344, Springer-Verlag, 2011.
40. X. Yu, Y. Wang, W. Wu, L. Zhang. Security on LBlock against Biclique Cryptanalysis. WISA 2012, LNCS, vol. 7690, pp. 1–14, Springer-Verlag, 2012.