Cao and Zhang *Cybersecurity* (2021) 4:32
https://doi.org/10.1186/s42400-021-00096-4

Cybersecurity

RESEARCH Open Access

Multidimensional linear cryptanalysis with key difference invariant bias for block ciphers

Wenqin Cao[1,2,3] and Wentao Zhang[1,2*]

Abstract

For block ciphers, Bogdanov et al. found that there are some linear approximations satisfying that their biases are deterministically invariant under key difference. This property is called key difference invariant bias. Based on this property, Bogdanov et al. proposed a related-key statistical distinguisher and turned it into key-recovery attacks on LBlock and TWINE-128. In this paper, we propose a new related-key model by combining multidimensional linear cryptanalysis with key difference invariant bias. The main theoretical advantage is that our new model does not depend on statistical independence of linear approximations. We demonstrate our cryptanalysis technique by performing key recovery attacks on LBlock and TWINE-128. By using the relations of the involved round keys to reduce the number of guessed subkey bits. Moreover, the partial-compression technique is used to reduce the time complexity. We can recover the master key of LBlock up to 25 rounds with about $2^{60.4}$ distinct known plaintexts, $2^{78.85}$ time complexity and 2^{61} bytes of memory requirements. Our attack can recover the master key of TWINE-128 up to 28 rounds with about $2^{61.5}$ distinct known plaintexts, $2^{126.15}$ time complexity and 2^{61} bytes of memory requirements. The results are the currently best ones on cryptanalysis of LBlock and TWINE-128.

Keywords: Key-alternating cipher, Key difference invariant bias, Multidimensional linear cryptanalysis, LBlock, TWINE

Introduction

Linear cryptanalysis introduced by Matsui in 1993 has become one of the most important cryptanalysis method of block ciphers. After being introduced a quarter of a century ago, linear cryptanalysis has been extended to various more evolved statistical attacks, including multiple linear cryptanalysis (Kaliski and Robshaw 1994) and multidimensional linear cryptanalysis (Hermelin et al. 2008; Hermelin et al. 2009; Cho et al. 2008; Blondeau and Nyberg 2017). Various authors have previously presented different approaches to exploit multiple linear approximations to enhance linear cryptanalysis. In multiple linear cryptanalysis, a fundamental assumption was that the approximations are statistically independent. The theoretically restrictive assumption of independence of linear approximations was removed in the multidimensional linear cryptanalysis on the cost of taking into account a family of linear approximations which covers a linear space excluding zero. In Hermelin et al. (2009), presented the log-likelihood ratio and χ^2 statistical distinuishers that can be used to perform key recovery attacks. The aim of a statistical key-recovery attack is to search the right value for some bits of the round-key based on a known statistical property of the cipher. This property is expected to be detected only for the right key candidate, while wrong key candidates which are far from satisfying the property can be discarded. To estimate the data complexity of a statistical attack, the probability distributions of the involved random variables for the right and wrong keys are analyzed. These distributions depend on both the data sample

*Correspondence: zhangwentao@iie.ac.cn
[1]State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, No. 89 Minzhuang Road, Haidian District, 100093 Beijing, China
[2]School of Cyber Security, University of Chinese Academy of Sciences, No. 19 Yuquan Road, Shijingshan District, 100049 Beijing, China
Full list of author information is available at the end of the article

used to compute it as well as the encryption key and the key candidate. Selçuk gave a formal probabilistic model in linear and differential cryptanalysis in Selçuk and Biçak (2002). The probabilistic model provided efficient formulations that can be used to estimate the success probability of a given attack or to find the data complexity to achieve a certain success level.

In Bogdanov et al. (2013), revealed a fundamental property of block ciphers: there can exist linear approximations such that their biases are deterministically invariant under key difference. This property is called key difference invariant bias. They proposed a statistical related-key distinguisher for this property and turned it into key recovery attacks on LBlock and TWINE-128. Under some basic independency assumptions, they computed the sample biases of a set of approximations with this property for two keys, and constructed an efficiently statistical related-key distinguisher. In their model, a fundamental assumption was that the linear approximations are statistically independent. But this assumption is hard to verify in practice. In this paper, we propose a multidimensional related-key distinguisher for the key difference invariant bias property, which can remove the independence assumption on the linear approximations.

To decrease key set-up time and to reduce the cost of hardware, the key schedule of lightweight ciphers are usually simple. As is known to us, the diffusion of the key schedule plays an important role on the security of the block cipher, so we should spend more effort on the key schedules of lightweight block ciphers. Wang et al. improved multidimensional zero-correlation linear attack in Wang and Wu (2014). They have taken the key schedule into consideration and used the relations that existed in the involved round keys of key recovery attack to reduce the number of round keys that need to be guessed. They carefully chose the order of guessing keys and guessed each subkey nibble one after another. By using the partial-compression technique to reduce the time complexity.

In Blondeau and Nyberg (2017), developed distinct-known-plaintext (DKP) that was first introduced in the context of multidimensional zero-correlation attacks[11]. The DKP sample can improve the data complexity of multiple linear attacks, multidimensional linear attacks and key difference invariant bias attacks.

Our contributions

The contributions of this paper are as follows.

New model with key difference invariant bias

In this paper, we take into account multidimensional cryptanalysis with key difference invariant bias. The main motivation of this method is that the dependencies of linear approximations need not be measured explicity. We present a multidimensional statistical related-key distinguisher for the key difference invariant bias property of key-alternating block ciphers. Our new model has the two following advantages:

(1). Does not assume statistical independence of linear approximations, i.e. the assumption about statistical independence of linear approximations can be removed.
(2). Consider all linear approximations of linear subspace with key difference invariant bias property excluding zero. The new model can increase the freedom of the model, thus the data complexity is reduced.

We analyze the probability distribution of the new related-key statistic Q both in the right-key and wrong-key case and derive the formula of the data complexity for given attack. In addition, the new statistical model takes into account whether the data sample is obtained by the usually known plaintext (KP) sampling or the considered distinct known plaintext (DKP) sampling.

Key Recovery Attack for LBlock and TWINE-128

By using the new related-key statistic Q, we give the first key-recovery attack on 25-round LBlock. We put the 16-round 8-dimensional linear approximations with key difference invariant bias in round 5 to 20. We partially encrypt the first 4 rounds and partially decrypt the last 5 rounds. The attack is affected by 32 bits of a plaintext, 48 bits of a ciphertext and 76 bits of round keys. Because the attack involves too many plaintext bits, ciphertext bits and round key bits, the data complexity and time complexity are both too huge. In order to reduce the data complexity and the time complexity, we take the key schedule of LBlock into consideration and obtain the relations that exist in the involved round keys. Thus the involved round keys can reduce 17 bits key information that need to be guessed. We carefully choose the order of guessing key bits and use partial-compression technique to reduce the time complexity. Our attack can recover the 80-bit master key of LBlock with about $2^{60.4}$ distinct known plaintexts, $2^{78.85}$ time complexity and 2^{61} bytes of memory requirements. Similary, using the same multidimensional linear approximation, we can give 24-round attack on LBlock which is better than that in Bogdanov et al. (2013). In Table 1, we present a comparison of our attack results and the best known ones.

We apply the new related-key model to perform a 28-round attack on TWINE-128. We put the 17-round 8-dimensional linear approximations with key difference invariant bias in round 6 to 22. We partially encrypt the first 5 rounds and partially decrypt the last 6 rounds. We take the key schedule of TWINE-128 into consideration and obtain the relations that exist in the involved round keys. By using the partial-compression technique to reduce the time complexity. Our attack can recover the

Table 1 Comparison of key-recovery attacks on LBlock

Model	Attack	rounds	Data per key	Time	Memory	Ref.
RK	Differential	22	$2^{64.1}$RKKP	2^{67}	N/A	(Liu et al. 2012)
	Imp.Diff	22	2^{47}RKCP	2^{70}	N/A	(Minier and Naya-Plasencia 2012)
	Imp.Diff	23	$2^{64.1}$RKKP	$2^{78.3}$	$2^{61.4}$	(Wen et al. 2014)
	Key Diff Inv Bias	24	$2^{62.95}$RKKP	$2^{70.67}$	2^{61}	(Bogdanov et al. 2013)
	Key Diff Inv Bias	24	$2^{62.83}$RKKP	$2^{68.08}$	2^{61}	this paper
	Key Diff Inv Bias	24	$2^{62.3}$RKDKP	$2^{68.07}$	2^{61}	this paper
	Key Diff Inv Bias	25	$2^{60.4}$RKDKP	$2^{78.85}$	2^{61}	this paper
SK	Integral	20	$2^{63.6}$CP	$2^{39.6}$	2^{35}	(Sasaki and Wang 2013a)
	Integral	21	$2^{61.6}$CP	$2^{54.16}$	$2^{51.58}$	(Sasaki and Wang 2013b)
	Integral	22	2^{61}CP	2^{70}	2^{63}	(Sasaki and Wang 2013b)
	Zero-Correlation	22	2^{62}DKP	$2^{71.27}$	2^{64}	(Soleimany and Nyberg 2014)
	Zero-Correlation	22	2^{60}DKP	2^{79}	2^{64}	(Soleimany and Nyberg 2014)
	Zero-Correlation	23	$2^{62.1}$KP	2^{76}	2^{60}	(Wang and Wu 2014)
	Imp.Diff	24	2^{59}CP	$2^{77.5}$	2^{75}	(Wang et al. 2016)

128-bit master key of TWINE-128 with about $2^{61.5}$ distinct known plaintexts, $2^{126.15}$ time complexity and 2^{61} bytes of memory requirements, with success probability 0.85. Similary, using the same multidimensional linear approximation, we can give 27-round attack on TWINE-128 which is better than that in Bogdanov et al. (2013). In addition, we combine all differential paths of the 15 key differences that satisfy the property of invariant bias. So we propose a combined model and perform the 27-round attack on TWINE-128 with about $2^{60.44}$ distinct known plaintexts, $2^{119.5}$ time complexity and $15 \cdot 2^{61}$ bytes of memory requirements. Our attacks are compared to previous attacks on TWINE-128 in Table 2.

Preliminaries

Linear cryptanalysis with key difference invariant bias

In Bogdanov et al. (2013), analysed the fundamental question of how the bias of the entire linear approximation behaves under a change of key. They revealed a property for many block ciphers, namely, that the bias of a linear approximation can be actually invariant with a modified key. Based on the fact, they proposed a statistical related-key distinguisher and demonstrated that it can be used to efficiently distinguish the cipher from an idealized cipher under some basic independency assumptions. As an illustration, they applied the cryptanalytic technique of key difference invariant bias to LBlock and TWINE-128. In this section, we introduce some definitions and main results in Bogdanov et al. (2013).

Consider an n-bit block cipher f with a k-bit key. Linear cryptanalysis is based on a linear approximation determined by input mask a and output mask b. The bias of the linear approximation (a, b) of f is defined by

$$\varepsilon(a,b) = Pr_x[\, a^t x \oplus b^t f(x) = 0] - 1/2$$

The value $c(a, b) = 2\varepsilon(a, b)$ is called correlation of the linear approximation (a, b). A linear approximation (a, b) of an iterative block cipher is called a linear hull. The linear hull contains all possible sequences of the linear approximations over individual rounds with input mask a and

Table 2 Comparison of key-recovery attacks on TWINE-128

Model	Attack	rounds	Data per key	Time	Memory	Ref.
RK	Key Diff Inv Bias	27	$2^{62.95}$RKKP	$2^{119.5}$	2^{61}	(Bogdanov et al. 2013)
	Key Diff Inv Bias	27	$2^{62.3}$RKDKP	$2^{119.5}$	2^{61}	this paper
	Key Diff Inv Bias	27	$2^{60.44}$RKDKP	$2^{119.5}$	$15 \cdot 2^{61}$	this paper
	Key Diff Inv Bias	28	$2^{61.5}$RKDKP	$2^{126.15}$	2^{61}	this paper
SK	Saturation	23	$2^{62.81}$CP	$2^{106.14}$	2^{103}	(Suzaki et al. 2012)
	Imp.Diff	24	$2^{52.21}$CP	$2^{115.10}$	2^{118}	(Suzaki et al. 2012)
	Meet-in-the-Middle	25	2^{48}CP	2^{122}	2^{125}	(Boztas et al. 2013)
	Zero-Correlation	25	$2^{62.1}$KP	$2^{122.12}$	2^{60}	(Wang and Wu 2014)

output mask b. These sequences are called linear trails which we denote by θ. Given a linear hull (a, b), a linear trail 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:

$$\theta = (\theta_0, \theta_1, ..., \theta_r).$$

Thus, each linear trail consists of $(r+1)$ n-bit masks. The bias ε_θ of the linear trail θ is defined as the scaled product of the individual biases $\varepsilon_{\theta_{i-1},\theta_i}$ over each round,

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

Key alternating block ciphers form a special but important subset of modern block ciphers. Its definition is as follows.

Definition 1 ((Daemen and Rijmen 2002)). *Let each round $i, 1 \le i \le r$, 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 round subkeys $K_0, K_1, \ldots, K_r$, build the expanded key K (of length $n(r+1)$ bits) which is derived from the master key κ using a key-schedule algorithm φ. From Daemen and Rijmen (2002), for a key-alternating block cipher, the bias $\varepsilon(a, b)$ of the linear hull (a, b) is

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

where d_θ is a key-independent constant .

In an n-bit key-alternating block cipher, let φ be key schedule, K and K' be the expanded keys corresponding to two master keys κ and κ', $K = \varphi(\kappa)$ and $K' = \varphi(\kappa')$ satisfying $K = K' \oplus \Delta$, where the difference Δ describes a connection between K and K'. Let ε and ε' are two biases under two keys κ and κ', with $\kappa \neq \kappa'$, then

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

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

When does the equality $\varepsilon = \varepsilon'$ hold? The equality holds if $d_\theta \oplus \theta \cdot K = d_\theta \oplus \theta \cdot K'$, that is, $\theta \cdot \Delta = 0$. In the following, we give a short summary of the contributions in Bogdanov et al. (2013).

Theorem 1 ((Bogdanov et al. 2013), Key difference invariant bias for key-alternating ciphers). *Let (a, b) be a non-trivial linear approximation of a key-alternating block cipher. Its biases ε for expanded key K and ε' for expanded key K' with $K' = K \oplus \Delta$ have exactly equal values $\varepsilon = \varepsilon'$, if $\theta \cdot \Delta = 0$ for each linear characteristic θ of the linear hull (a, b) with $\varepsilon_\theta \neq 0$.*

Given a linear approximation (a, b), we denote by $\theta_j, j = 1, ..., n(r+1)$ the j-th bit of linear characteristics θ. If bit positions j 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. Next we give a more explicit sufficient condition for keeping $\theta \cdot \Delta = 0$.

Corollary 1. *[(Bogdanov et al. 2013), **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 $\Delta = K \oplus K'$ chooses an arbitrary number of zero positions and no nonzero positions in the linear characteristics θ of the linear approximation, with $\varepsilon_\theta \neq 0$.*

For random block ciphers and block sizes $n \ge 5$, the bias ε of a linear approximation follows a normal distribution with mean 0 and variance 2^{-n-2} from Daemen and Rijmen (2007), that is, $\varepsilon \sim \mathcal{N}(0, 2^{-n-2})$. Then, the probability for biases with two different keys to be equal is $Pr\{\varepsilon = \varepsilon' | \kappa \neq \kappa'\} \approx \frac{1}{\sqrt{2\pi}} 2^{\frac{3-n}{2}}$.

Given N plaintext-ciphertext pairs and λ linear approximations under a pair of expanded keys K, K', $\Delta = K \oplus K'$, Δ satisfies the condition 1 for key difference invariant bias. For each of these linear approximations we allocate counters S_i and S'_i, $i = 1, ..., \lambda$, which account for the number of times that these linear approximations are satisfied under K and K' for each of the N known-plaintexts. The statistic s is as follows:

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

Assume the counters S_i and S'_i, $i = 1, ..., \lambda$, are all independent, s approximately follows normal distribution with mean $\frac{\lambda}{2N}$ and variance $\frac{\lambda}{2N^2}$ for the right key, that is,

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

Similarly, s approximately follows normal distribution for the wrong key as follows:

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

In the two above cases, we have seen that the statistic s follows two different normal distributions. When testing the key candidates, the cryptanalysts face with the task of statistical hypothesis. Consider two normal distributions $\mathcal{N}(\mu_0, \sigma_0^2)$ and $\mathcal{N}(\mu_1, \sigma_1^2)$. Without loss of generality, assume that $\mu_0 < \mu_1$. A sample t is drawn from either $\mathcal{N}(\mu_0, \sigma_0^2)$ or $\mathcal{N}(\mu_1, \sigma_1^2)$. The hypothesis test is performed to determine which distribution the sample comes from. Compare the value t with some threshold value τ, if $t \le \tau$, the test returns $t \in \mathcal{N}(\mu_0, \sigma_0^2)$; if $t > \tau$, the test returns $t \in \mathcal{N}(\mu_1, \sigma_1^2)$. There are two types error

of probabilities. The type I error is the probability of the sample t comes from $\mathcal{N}\left(\mu_1, \sigma_1^2\right)$ when t actually comes from $\mathcal{N}\left(\mu_0, \sigma_0^2\right)$. The type II error is the probability of the sample t comes from $\mathcal{N}\left(\mu_0, \sigma_0^2\right)$ when t actually comes from $\mathcal{N}\left(\mu_1, \sigma_1^2\right)$. The two errors are denoted by α_0 and α_1 as follows.

$$\alpha_0 = Pr\left\{t > \tau | t \in \mathcal{N}\left(\mu_0, \sigma_0^2\right)\right\},$$
$$\alpha_1 = Pr\left\{t < \tau | t \in \mathcal{N}\left(\mu_1, \sigma_1^2\right)\right\}.$$

The decision threshold 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 $\mathcal{N}(0,1)$.

Corollary 2 ((Bogdanov et al. 2013), Data Complexity of Distinguisher)**.** *Using the s distributions for the right and wrong key, we obtain the following equation that determines the amount of data needed by the distinguisher s:*

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

where α_0 is the probability to reject the right key, whereas α_1 is the probability to accept a wrong key.

The statistical cryptanalysis attack also depends on the way to obtain the data sample. In known plaintext (KP) attack, the plaintext-ciphertext pair (P, C) is done with replacement. If the plaintext-ciphertext pairs are sampled randomly without replacement, the attack is called distinct-known-plaintext (DKP) attack. Suppose N plaintext-ciphertext pairs are sampled randomly, let us denote by Z the random variable corresponding to the number of plaintext-ciphertext pairs that satisfy linear approximation equation. In the cases of KP and DKP sampling, the variable Z follows a binomial and hypergeometric distributions, respectively. The two distributions have the same expectation Np, but variance is $BNp(1-p)$, where p is the probability that the linear approximation holds, the constant B is defined by

$$B = \begin{cases} 1, & \text{for KP} \\ \frac{2^n - N}{2^n - 1}, & \text{for DKP.} \end{cases}$$

Multidimensional approximation of boolean functions

In this section, we introduce two lemmas of multidimensional linear cryptanalysis (Hermelin et al. 2008) that will be needed in next section.

Let $f : V_n \to V_l$ be a vector Boolean function, and binary vectors $v_i \in V_l$ and $u_i \in V_n$, $i = 1, 2, ..., m$, be linear masks such that the paired masks (u_i, v_i) are linearly independent. Define functions g_i by

$$g_i(\xi) := v_i \cdot f(\xi) + u_i \cdot \xi$$

and assume g_i have correlations c_i, $i = 1, ..., m$. We will call these correlations base-correlations, and the corresponding linear approximations of f the base-approximations. We want to find the probability distribution of the m-dimensional linear approximation

$$g(\xi) := Vf(\xi) + U\xi$$

where $V = (v_1, ..., v_m)$, $U = (u_1, ..., u_m)$ and $g = (g_1, ..., g_m)$. Let the probability distribution of g be $p = (p_0, ..., p_M), M = 2^m - 1$. Assume that we have the correlations $c(a)$ of all the linear mappings $a \cdot g$ of g, We will call the correlations $c(a)$ the combined correlations of f and the corresponding approximations the combined approximations.

Definition 2. *The capacity between two probability distributions p and q is defined by*

$$C(p, q) = \sum_{\eta=0}^{2^m-1} \frac{(p_\eta - q_\eta)^2}{q_\eta}.$$

Let us consider m-dimensional linear attack whose m base approximations construct an m-dimensional vectorial boolean function f. Let $p = (p_0, ..., p_{2^m-1})$ denote the probability distribution of f, and γ is the discrete uniform distribution, the capacity of the m-dimensional linear approximations as below:

$$C(p, \gamma) = \sum_{\eta=0}^{2^m-1} \frac{(p_\eta - 2^{-m})^2}{2^{-m}}.$$

For simplicity, let $C(p)$ denotes the capacity of the probability distribution of m-dimensional linear approximations.

Lemma 1. *[(Hermelin et al. 2008)] Let $g : F_2^n \to F_2^m$ be a Boolean function with probability distribution p and one-dimensional correlations $c(a)$ of $a \cdot g$. Then*

$$p_\eta = 2^{-m} \sum_{a \in F_2^m} (-1)^{a \cdot \eta} c(a),$$
$$c(a) = \sum_{\eta \in F_2^m} (-1)^{a \cdot \eta} p_\eta, \ \eta \in F_2^m, \ a \in F_2^m.$$

Lemma 2. *[(Hermelin et al. 2008)] Let $g : F_2^n \to F_2^m$ be the Boolean function with probability distribution p. Then the capacity $C(p)$ of p such that*

$$C(p) = 2^m \sum_{\eta \in F_2^m} (p_\eta - 2^{-m})^2 = \sum_{\substack{a \neq 0 \\ a \in F_2^m}} c(a)^2.$$

Note 1. If a random variable X has the χ^2 distribution with l degrees of freedom, then X approximately follows normal distribution with mean l and variance $2l$ when l is sufficiently large, that is, $X \to \mathcal{N}(l, 2l)$.

Note 2. Suppose X is d-dimensional normal random vector with mean vector μ and covariance Σ, $X \sim \mathcal{N}_d(\mu, \Sigma)$, then $(X - \mu)^T \Sigma^{-1} (X - \mu)$ follows a χ^2 distribution with r degrees of freedom, $r = rank(\Sigma)$.

We will need the above results in next section where we study how multidimensional linear statistic is applied in key difference invariant bias linear cryptanalysis.

Improved statistical distinguisher with key difference invariant bias

In this section, we firstly consider multidimensional linear attacks with key difference invariant bias and present a new statistic Q. Then we analyse the probability distribution of statistic Q for the right/wrong key guess, and give the data complexity of an attack to achieve a certain success level under KP and DKP cases, respectively. Finally, the key recovery attack procedure which uses our new model is described.

A new statistical distinguisher

We analyse the relation between correlations and probability distributions of multidimensional linear approximation under two distinct round keys. Suppose a block cipher $f : F_2^n \to F_2^n$, we consider m-dimension linear cryptanalysis of f. Assume the base-approximations of m-dimensional linear approximation is $g = (g_1, ..., g_m)$. Let us denote by $c(a)$ and $c'(a)$ the correlations of $a \cdot g$ under master keys κ and κ', respectively, and denote by p_η and p'_η the probability distributions of g under master keys κ and κ', respectively. We can obtain the next lemma.

Lemma 3.

$$\sum_{\substack{a\neq 0\\ a\in F_2^m}} \left(c(a)-c'(a)\right)^2 = 2^m \cdot \sum_{\eta\in F_2^m} \left[\left(p_\eta - 2^{-m}\right) - \left(p'_\eta - 2^{-m}\right)\right]^2.$$

Proof According to Lemma 2, we have:

$$2^m \sum_{\eta\in F_2^m} (p_\eta - 2^{-m})^2 = \sum_{\substack{a\neq 0\\ a\in F_2^m}} c(a)^2,$$

$$2^m \sum_{\eta\in F_2^m} (p'_\eta - 2^{-m})^2 = \sum_{\substack{a\neq 0\\ a\in F_2^m}} c'(a)^2.$$

So it suffices to show that

$$\sum_{\substack{a\neq 0\\ a\in F_2^m}} c(a)c'(a) = 2^m \sum_{\eta\in F_2^m} \left(p_\eta - 2^{-m}\right)\left(p'_\eta - 2^{-m}\right). \quad (1)$$

Using Lemma 1, we have:

$$p_\eta = 2^{-m} \sum_{a\in F_2^m} (-1)^{a\cdot\eta} c(a), \quad p'_\eta = 2^{-m} \sum_{b\in F_2^m} (-1)^{b\cdot\eta} c'(b).$$

Substituting p_η and p'_η in (1) as follows:

$$\begin{aligned}
&2^m \cdot \sum_{\eta\in F_2^m} \left[\left(p_\eta - 2^{-m}\right)\cdot\left(p'_\eta - 2^{-m}\right)\right] \\
&= 2^{-m} \cdot \sum_{\eta\in F_2^m} \left[\left(\sum_{a\in F_2^m} (-1)^{a\cdot\eta} c(a) - 1\right)\left(\sum_{b\in F_2^m} (-1)^{b\cdot\eta} c'(b) - 1\right)\right] \\
&= 2^{-m} \sum_{\eta\in F_2^m} \left[\sum_{a,b\in F_2^m} (-1)^{(a+b)\cdot\eta} c(a)c'(b) - \sum_{a\in F_2^m} (-1)^{a\cdot\eta} c(a) \right. \\
&\qquad \left. - \sum_{b\in F_2^m} (-1)^{b\cdot\eta} c'(b) + 1\right].
\end{aligned}$$

Because

$$\sum_{\eta\in F_2^m} (-1)^{a\cdot\eta} = \begin{cases} 2^m, & \text{for } a = 0, \\ 0, & \text{for } a \neq 0. \end{cases}$$

therefore,

$$2^{-m} \cdot \sum_{\eta\in F_2^m} \sum_{a\in F_2^m} (-1)^{a\cdot\eta} c(a) = 2^{-m} \cdot \sum_{a\in F_2^m} \sum_{\eta\in F_2^m} (-1)^{a\cdot\eta} c(a) = 1.$$

Similarly,

$$2^{-m} \cdot \sum_{\eta\in F_2^m} \sum_{b\in F_2^m} (-1)^{b\cdot\eta} c'(b) = 1,$$

$$2^{-m} \sum_{\eta\in F_2^m} \sum_{a,b\in F_2^m} (-1)^{(a+b)\cdot\eta} c(a)c'(b) = \sum_{\substack{a=b,\\ a,b\in F_2^m}} c(a)c'(b)$$

$$= \sum_{\substack{a\neq 0\\ a\in F_2^m}} c(a)c'(a) + 1.$$

Thus, the Eq. (1) holds, the Lemma 3 as desired. □

Thus we can present a new statistic based on the key difference invariant bias property by using an m-dimensional linear approximation for an n-bit block cipher. Suppose the data sample is randomly selected, the sample size is N. $V(\eta)$ and $V'(\eta)$, $\eta = 0, ..., 2^m - 1$, denote the number of occurrences of value η of the observed data distribution for master keys κ and κ' with the N plaintexts. We propose a new statistic Q:

$$Q = 2^m \cdot \sum_{\eta=0}^{2^m-1} \left[\left(\frac{V(\eta)}{N} - 2^{-m}\right) - \left(\frac{V'(\eta)}{N} - 2^{-m}\right)\right]^2.$$

As we aim to perform a key recovery attack with this statiatic Q, we will derive the distribution of Q for the right key guess and for the wrong key guess.

In the case of right key guess, we obtain the following result.

Proposition 1. *[Distribution of Statistic Q for the Right Key] Consider an m-dimensional linear approximation for a block cipher under a pair of expanding keys (K, K') connected by Δ conforming to condition 1. Let N is the number of KP or DKP pairs, $V(\eta)$ and $V'(\eta)$ are the frequency of value η of the observed data distribution for K and*

K′, respectively, and m is high enough. Then the following approximate distribution holds for sufficiently large N and m:

$$Q \sim \mathcal{N}\left(\frac{2Bl}{N}, \frac{8B^2 l}{N^2}\right)$$

where $l = 2^m - 1$, $B = \begin{cases} 1, & for\ KP \\ \frac{2^n-N}{2^n-1}, & for\ DKP \end{cases}$.

Proof We first consider KP case. For m-dimensional linear attack, let $l = 2^m - 1$, N is the number of random KP pairs, $V(\eta)$ and $V'(\eta)$, $\eta = 0, ..., 2^m - 1$, denote the number of occurrences of value η of the observed data distribution for master keys κ and κ'. The random vector $(V(0), ..., V(l))^T$ follows a multinomial distribution with parameter N and $p(\kappa)$, where $p(\kappa) = (p_0(\kappa), ..., p_l(\kappa))$ with $\sum_{\eta=0}^{l} p_\eta(\kappa) = 1$. The variance of $V(i)$ is $Np_i(\kappa)(1 - p_i(\kappa)) \approx N2^{-m}(1 - 2^{-m})$. The covariance of $V(i)$ and $V(j)$ is $Cov(V(i), V(j)) = -Np_i(\kappa)p_j(\kappa)) \approx N2^{-2m}$. The counters $V(\eta)$ and $V'(\eta)$ suggest empirical probability $\hat{p}_\eta(\kappa) = \frac{V(\eta)}{N}$ and $\hat{p}_\eta(\kappa') = \frac{V'(\eta)}{N}$ respectively. Let $\hat{p}(k) = (\hat{p}_0(\kappa), ..., \hat{p}_{l-1}(\kappa))^T$, $\hat{p}(\kappa') = (\hat{p}_0(\kappa'), ..., \hat{p}_{l-1}(\kappa'))^T$, for sufficiently large N, the random vector $\hat{p}(\kappa)$ approximately follows l-dimensional normal distribution with mean vector $p(\kappa) = (p_0(\kappa), ..., p_{l-1}(\kappa))^T$ and covariance matrix $\Sigma = N^{-1}2^{-m}(I_l - 2^{-m}E)$, where I_l is an identity matrix, E is a $l \times l$ matrix with all entries are equal one, that is,

$$\hat{p}(\kappa) \sim \mathcal{N}_l(p(\kappa), \Sigma).$$

Similarly, $\hat{p}(\kappa') \sim \mathcal{N}_l(p(\kappa'), \Sigma)$.

The expanded keys $K = \varphi(\kappa)$ and $K' = \varphi(\kappa')$ satisfying $K = K' \oplus \Delta$, Δ satisfies the condition 1 for key difference invariant bias, so $p(\kappa) = p(\kappa')$. Then, $\hat{p}(\kappa) - \hat{p}(\kappa') \sim \mathcal{N}_l(0, 2\Sigma)$. From Note 2, we know

$$\left(\hat{p}(\kappa) - \hat{p}(\kappa')\right)^T (2\Sigma)^{-1} \left(\hat{p}(\kappa) - \hat{p}(\kappa')\right) \sim \chi^2(l).$$

Because $\Sigma^{-1} = N2^m(I_l + E)$, therefore,

$$\begin{aligned}
&(\hat{p}(\kappa) - \hat{p}(\kappa'))^T (2\Sigma)^{-1} (\hat{p}(\kappa) - \hat{p}(\kappa')) \\
&= N2^{m-1}\left[\sum_{\eta=0}^{l-1} \left(\hat{p}_\eta(\kappa) - \hat{p}_\eta(\kappa')\right)^2 + \left(\sum_{\eta=0}^{l-1} (\hat{p}_\eta(\kappa) - \hat{p}_\eta(\kappa'))\right)^2\right] \\
&= N2^{m-1}\left[\sum_{\eta=0}^{l-1} \left(\hat{p}_\eta(\kappa) - \hat{p}_\eta(\kappa')\right)^2 + \left(1 - \hat{p}_l(\kappa) - (1 - \hat{p}_l(\kappa'))\right)^2\right] \\
&= N2^{m-1} \sum_{\eta=0}^{l} \left(\hat{p}_\eta(\kappa) - \hat{p}_\eta(\kappa')\right)^2 = \frac{N}{2} Q.
\end{aligned}$$

Thus we obtain $Q \sim \frac{2}{N}\chi^2(l)$. Using the Note 1, the following approximate distribution holds for sufficiently large N and m:

$$Q \sim \mathcal{N}\left(\frac{2l}{N}, \frac{8l}{N^2}\right).$$

In the case of DKP sample, the random vector $(V(0), ..., V(l))^T$ follows a multivariate hypergeometric distribution. The variance of $V(i)$ is $\frac{2^n-N}{2^n-1}Np_i(\kappa)(1 - p_i(\kappa)) \approx \frac{2^n-N}{2^n-1}N2^{-m}(1 - 2^{-m})$. The covariance of $V(i)$ and $V(j)$ is

$$Cov(V(i), V(j)) = -\frac{2^n - N}{2^n - 1}Np_i(\kappa)p_j(\kappa)) \approx \frac{2^n - N}{2^n - 1}N2^{-2m}.$$

The following steps of the proof are similar to those in the KP case. □

In the case of wrong key guess, we base upon the hypothesis that for a wrong key, i.e., the cipher is a permutation drawn at random. Suppose the m-dimensional linear approximation with the probability distribution $p_\eta(k)$, $\eta = 0, ..., 2^m - 1$, independent and identical distribution to a normal distribution $\mathcal{N}\left(2^{-m}, \sigma^2\right)$. According to Lemma 1, for $a \neq 0$,

$$\begin{aligned}
c_a(k) &= \sum_{\eta \in F_2^m} (-1)^{a \cdot \eta} \left[p_\eta(k) - 2^{-m} + 2^{-m}\right] \\
&= \sum_{\eta \in F_2^m} (-1)^{a \cdot \eta} \left[p_\eta(k) - 2^{-m}\right]
\end{aligned}$$

we have $c_a(k) \sim \mathcal{N}\left(0, 2^m\sigma^2\right)$. In Daemen and Rijmen (2007), Daemen and Rijmen show that the correlation distribution of an ideal cipher is normal with mean zero and variance 2^{-n}, i.e., $c_a(k) \sim \mathcal{N}\left(0, 2^{-n}\right)$. So we obtain $2^m\sigma^2 = 2^{-n}$, $p_\eta(k) \sim \mathcal{N}\left(2^{-m}, 2^{-m-n}\right)$. Then we have the following proposition for the distribution of Q.

Proposition 2. *[Distribution of Statistic Q for the Wrong Key] Consider an m-dimensional linear approximation for two randomly drawn permutations. Let N is the number of KP or DKP pairs, $V(\eta)$ and $V'(\eta)$ are the frequency of value η of the observed data distribution for two permutations, respectively, and m is high enough. Then the following approximate distribution holds for sufficiently large N and n:*

$$Q \sim \mathcal{N}\left(\left(\frac{2B}{N} + 2^{-n+1}\right) \cdot l, \left(\frac{2B}{N} + 2^{-n+1}\right)^2 \cdot 2l\right)$$

where $l = 2^m - 1$, $B = \begin{cases} 1, & for\ KP \\ \frac{2^n-N}{2^n-1}, & for\ DKP \end{cases}$.

The proof of proposition 2 is similar to proposition 1.

In the two above cases, we have seen that the statistic Q will follow two different normal distributions. Using statistical hypothesis, we obtain the following data complexity under KP and DKP data sample, respectively.

$$N^{KP} = \frac{2^{n+0.5}\left(q_{1-\alpha_0} + q_{1-\alpha_1}\right)}{\sqrt{l} - \sqrt{2} \cdot q_{1-\alpha_1}}; \tag{2}$$

$$N^{DKP} = \frac{2^{n+0.5}\left(q_{1-\alpha_0} + q_{1-\alpha_1}\right)}{\sqrt{l} + \sqrt{2} \cdot q_{1-\alpha_0}}. \tag{3}$$

where α_0 is the probability to reject the right key, α_1 is the probability to accept a wrong key.

Procedure of key recovery attack

We describe the key recovery attack procedure which uses the statistic Q. The attack procedure is as follows:

Step1: For all related-key differential paths (a, b) with a difference $\delta = \kappa \oplus \kappa'$ on the master-key that satisfy key difference invariant bias condition. We collect N plaintext-ciphertext pairs (P, C) under the keys κ and $\kappa' = \kappa \oplus \delta$.

Step2: 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) under κ and κ', respectively. Compute the number of times $N[x]$ and $N[x']$ that partial state values occur.

Step3: For all state values of x and x', we compute the value η and allocate counters $V(\eta)$ and $V'(\eta)$ and set their initial values to zero. If the value η occurs, then add $N[x]$ and $N[x']$ to $V(\eta)$ and $V'(\eta)$, respectively. Compute

$$Q = Q + 2^m \cdot \sum_{\eta=0}^{2^m-1} \left[\left(\frac{V(\eta)}{N} - 2^{-m} \right) - \left(\frac{V'(\eta)}{N} - 2^{-m} \right) \right]^2 .$$

Step4: If $Q < \tau$, then the guessed subkey is a possible right subkey candidate.

Step5: Do exhaustive search for all right subkey candidates.

Attack on LBlock

In this section, we will evaluate the security of LBlock against multidimensional linear attack with key difference invariant bias by using the new statistic Q.

A brief description of LBlock

Encryption Algorithm. The general structure of LBlock is a variant of Feistel Network. The number of iterative rounds is 32. The round function of LBlock includes three basic functions: AddRoundKey, confusion function S and diffusion function P. The confusion function S consists of eight 4×4 S-boxes in parallel. The diffusion function P is defined as a permutation of eight 4-bit nibbles (see Wu and Zhang (2011)).

Key Schedule Algorithm. The key schedule of LBlock is rather simple. The 80-bit master key κ is stored in a key register, denoted by $\kappa = k_{79}k_{78}...k_1k_0$. At round i, the leftmost 32 bits of current contents of register κ are output as the round key K_i, i.e., $K_i = k_{79}k_{78}...k_{48}$. The key schedule of LBlock can be shown as follows:

1. $K_1 = \kappa[79, 78, ..., 48]$;
2. For $i \leftarrow 2$ to 32,

   (a) $\kappa = \kappa <<< 29$
   (b) $\kappa[79, 78, 77, 76] = S_9(\kappa[79, 78, 77, 76])$,
   $\kappa[75, 74, 73, 72] = S_8(\kappa[75, 74, 73, 72])$;
   (c) $\kappa[50, 49, 48, 47, 46] = \kappa[50, 49, 48, 47, 46] \oplus [i]_2$;
   (d) $K_i = \kappa[79, 78, ..., 48]$.

Multidimensional linear approximations with key difference invariant bias for LBlock

Let K and K' be the expanded keys corresponding to two master keys κ and κ', $K = \varphi(\kappa)$ and $K' = \varphi(\kappa')$ for key schedule φ, such that $K = K' \oplus \Delta$. Firstly, we introduce the notations that need to be used.

$i : j$ denotes an integer range from i to j;
$\delta = \kappa \oplus \kappa'$: the difference of master key κ and κ';
$\delta_{14:17}$ denotes a 4-bit nibble of δ, the bit position is $j = 14 : 17$;
$k_{14:17}$ denotes a 4-bit nibble of κ, the bit position is $j = 14 : 17$;
$k'_{14:17}$ denotes a 4-bit nibble of κ', the bit position is $j = 14 : 17$;
$k_{18:21}$ denotes a 4-bit nibble of κ, the bit position is $j = 18 : 21$
$k'_{18:21}$ denotes a 4-bit nibble of κ', the bit position is $j = 18 : 21$;
$S(x) = \left(S(x)^0, S(x)^1, S(x)^2, S(x)^3\right)$, $S_8(k_{14:17}) = S_8(k_{17}, k_{16}, k_{15}, k_{14})$;
$\Delta S(k_{14:17}) = S(k_{14:17}) \oplus S(k'_{14:17})$, and analogously, the other difference notation can be similarly represented;
$\Gamma_r, 5 \le r \le 20$: input mask value for the S-boxes in round r;
$\Delta K_r, 5 \le r \le 20$: the subkey difference in round r;
$\Delta K_r^i, 5 \le r \le 20$: the i-th nibble of subkey difference in round r, the 0-th nibble is the leftmost nibble;

In masks, '0', '1' and '$*$' denote zero, nonzero and arbitrary mask for a nibble, respectively; In differences, '0', '1' and '$*$' denote zero, nonzero and arbitrary difference for a nibble, respectively.

In Bogdanov et al. (2013), Bogdanov et al. found 16-round linear approximations that satisfy key difference invariant bias property. But they didn't identify the master key difference such that condition 1. In this section, we find the master key difference that satisfy invariant bias for 16-round 8-dimensional linear approximations. The 16 rounds 8-dimensional linear approximations with 4-bit input and 4-bit output. We put the 16 rounds 8-dimensional linear approximation in round 5 to 20. The input mask of the 5-th round is $(0000\alpha 00000000000)$ and the output mask of the 20-th round is $(000000000\beta 000000)$, $(\alpha, \beta) \neq 0$. Next, we determine the master key difference that satisfy condition 1.

For all cases of input mask $\Gamma_r, 5 \le r \le 20$, if the relations $\Gamma_r \cdot \Delta K_r = 0$ hold, then, the sufficient condition for key difference invariant bias is fulfilled according to the condition 1 in corollary 1. Now we determine all the

related-key differential paths, that is, we find the specific master key difference δ that satisfy the sufficient condition of invariant bias.

We get all the input mask $\Gamma_r, 5 \leq r \leq 20$ from (Bogdanov et al. 2013). Because $\Gamma_{12} = **11**11, \Gamma_{13} = *1*1*1*1, \Gamma_{11} = *1101111$, let $\Delta K_{12} = 00000000$, $\Delta K_{13} = 00000000$, $\Delta K_{11}^i = 0, i = 0, 1, 2, 4, 5, 6, 7$. According to the key schedule of LBlock, round keys K_{12}, K_{13}, K_{11}^i are functions of master key $k_j, j \in (0:79), j \neq 14, 15, 16, 17$. So the master key difference δ satisfy $\delta_{14:17} \neq 0000, \delta_j = 0, j \in (0:79), j \neq 14, 15, 16, 17$. Next, we determine the value of $\delta_{14:17}$.

According to the propagation property of the linear mask, the 14-round and 16-round input masks are obtained (see Bogdanov et al. (2013)), $\Gamma_{14} = 101111 * 1, \Gamma_{16} = 11000001$. In order for the equations $\Gamma_r \cdot \Delta K_r = 0$ hold, let $\Gamma_r^j \cdot \Delta K_r^j = 0, j = 0, 1, ..., 7$. On the basis of key schedule, the key $\Delta K_{14}^2, \Delta K_{16}^7$ are functions of the master key $k_{14:17}$, so we just need the next equation holds.

$$\begin{cases} \Delta K_{14}^2 = 0 \\ \Delta K_{16}^7 = 0 \end{cases} \tag{4}$$

Equation (4) can be turned to

$$\begin{cases} \Delta S_9\left(S_8\left(k_{14:17}\right)^3, k_{13}, k_{12}, k_{11}\right) = 0000 \\ \Delta S_8\left(S_9\left(k_{18:21}\right)^3, S_8\left(k_{14:17}\right)^0, S_8\left(k_{14:17}\right)^1 S_8\left(k_{14:17}\right)^2\right) = **00 \end{cases} \tag{5}$$

For every value of $k_{14:17}$ and $S_9\left(k_{18:21}\right)^3$, we can obtain only single nonzero difference $\delta_{14:17}$ by solving the Eq. (5) (see in Table 3). So we get all the key difference that satisfy the condition 1 in Corollary 1.

Table 3 Master key difference satisfy invariant bias condition 1

$k_{14:17}$	$S_9\left(k_{18:21}\right)^3$	$\delta_{14:17}$	$k_{14:17}$	$S_9\left(k_{18:21}\right)^3$	$\delta_{14:17}$
0000	0	1100	0010	1	0100
0111	0	1100	1001	1	0100
1011	0	1100	1101	1	0100
1100	0	1100	0110	1	0100
0000	1	0111	0010	0	1111
0011	0	0111	1001	0	1111
1111	1	0111	1101	0	1111
0100	0	0111	0110	0	1111
0111	1	0111	0101	0	1011
1000	1	0111	1010	1	1011
1011	1	0111	1110	0	1011
1100	1	0111	0001	1	1011
0100	1	1010	0001	0	1001
1110	1	1010	1000	0	1001
0011	1	0110	1010	0	0101
0101	1	0110	1111	0	0101

Key recovery for 25-Round LBlock

In order to attack 25-round LBlock, we follow the multidimensional linear cryptanalysis with key difference invariant bias property. The attack utilizes the 16-round key difference invariant bias linear approximations described in the above section from round 5 to 20. We append 4 rounds at the top of the distinguisher and add 5 rounds at the bottom of the distinguisher. After collecting sufficient plaintext-ciphertext pairs, we guess corresponding subkeys for the first four rounds and the last five rounds and compute the statistic Q of the linear approximations. Next, we decide if the guessed key is right or not. Finally, we exhaustively search all right subkey candidates. If we directly guess the subkeys bits involved in the key recovery process, then the time complexity will be greater than exhaustive search. Therefore, in order to reduce the time complexity, we express the two target values of attack by using the related round keys and plaintexts or ciphertexts, then, we use the partial-compression technique to reduce the time complexity significantly. The attack process is shown as the following Fig. 1.

Let X_0 denote the 64 bits plaintext, X_r^j denote the 4-bit nibble of the r-th ciphertext, the 0-th nibble is the leftmost nibble. As shown in Fig. 2, the nibble X_4^4 is affected by 32 bits of plaintext X_0 and 28 bits of round keys and the expression can be shown:

$$\begin{aligned} X_4^4 = X_0^0 \oplus S\left(X_0^{14} \oplus S\left(X_0^5 \oplus K_1^5\right) \oplus K_2^4\right) \oplus S\left(X_0^9 \oplus S\left(X_0^6\right.\right. \\ \left.\left. \oplus K_1^6\right) \oplus S\left(X_0^1 \oplus S\left(X_0^8 \oplus S\left(X_0^4 \oplus K_1^4\right) \oplus K_2^6\right) \oplus K_3^7\right)\right. \\ \left. \oplus K_4^5\right) \end{aligned}$$

Similarly, the nibble X_{20}^9 is affected by 48 bits of ciphertext X_{25} and 48 bits of round keys and the expression can be shown:

$$\begin{aligned} X_{20}^9 = X_{25}^3 \oplus S\left(X_{25}^{10} \oplus K_{25}^2\right) \oplus S\left(X_{25}^{13} \oplus S\left(X_{25}^5 \oplus S\left(X_{25}^{15}\right.\right.\right. \\ \left.\left.\left. \oplus K_{25}^7\right) \oplus K_{24}^7\right) \oplus K_{23}^7\right) \oplus S\left(X_{25}^{10} \oplus S\left(X_{25}^6 \oplus S\left(X_{25}^{12}\right.\right.\right. \\ \left.\left.\left. \oplus K_{25}^4\right) \oplus K_{24}^0\right) \oplus S\left(X_{25}^1 \oplus S\left(X_{25}^{11} \oplus K_{25}^3\right) \oplus S\left(X_{25}^8\right.\right.\right. \\ \left.\left.\left. \oplus S\left(X_{25}^7 \oplus S\left(X_{25}^{14} \oplus K_{25}^6\right) \oplus K_{24}^1\right) \oplus K_{23}^2\right) \oplus K_{22}^5\right) \\ \left. \oplus K_{21}^6\right) \end{aligned}$$

After analyzing the key schedule of LBlock, we find the following relations in the round keys:
$K_{24}^0 \Rightarrow K_{23}^7[1:3]$; $K_{24}^0, K_{24}^1, K_1^6 \Rightarrow K_4^5[0, 2, 3]$; $K_{25}^7 \Rightarrow K_{23}^2[0:1]$;
$K_{25}^3 \Rightarrow K_{22}^5[0:2]$; $K_{25}^4 \Rightarrow K_{22}^5[3]$; $K_{23}^2, K_{25}^6, K_{25}^7 \Rightarrow K_3^7$ only has two possible values; $K_2^6 \Rightarrow K_{24}^7$ has 2^3 possible values; $k_{14:17}, S_9\left(k_{18:21}\right)^3 \Rightarrow K_{25}^2$ has 2^3 possible values. According to these relations, the involved 76 bits round keys can reduce 17 bits information of subkeys, then we just need guess 59 bits subkey in the key recovery attack.

Assuming that N distinct known plaintext-ciphertext pairs are sampled, the partial encryption and decryption using the partial-compression technique are proceeded as

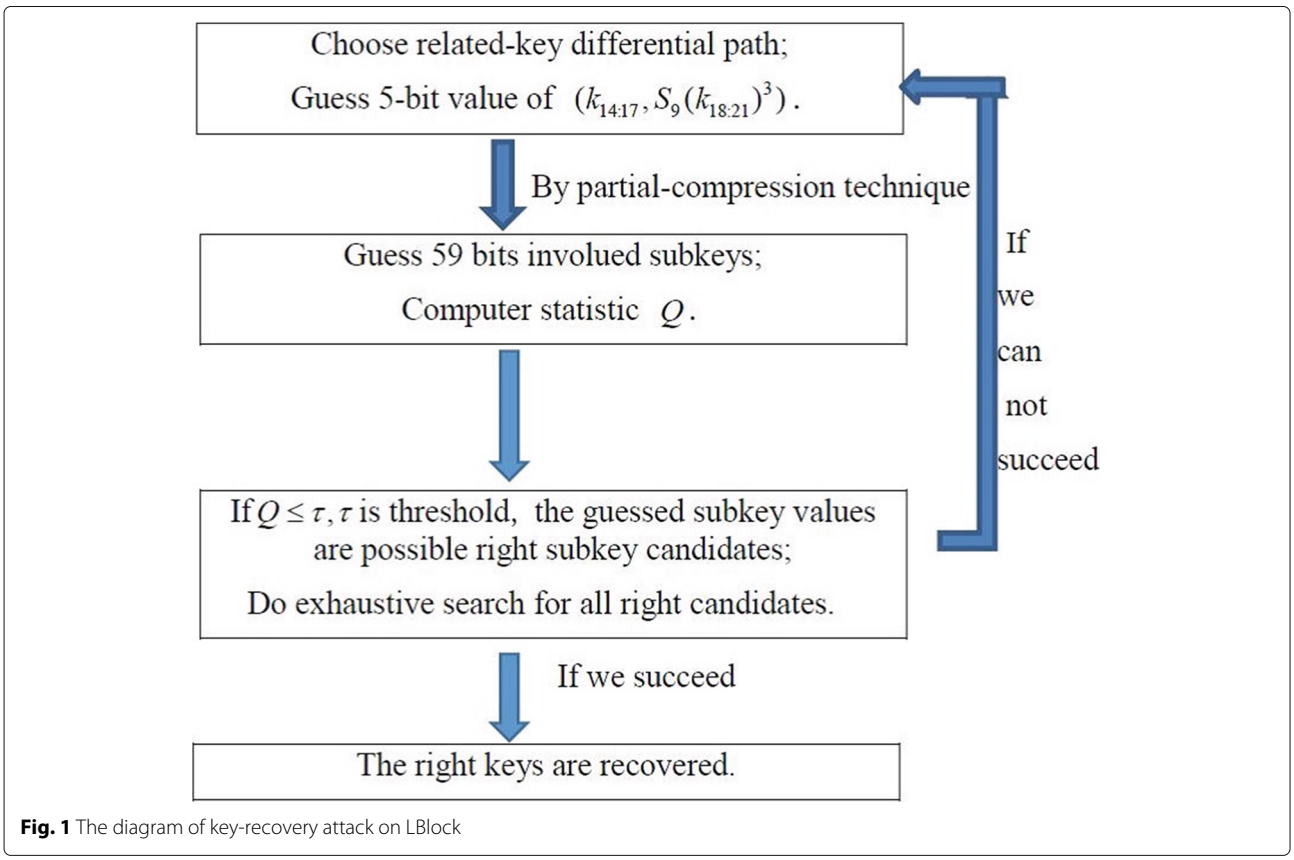

Fig. 1 The diagram of key-recovery attack on LBlock

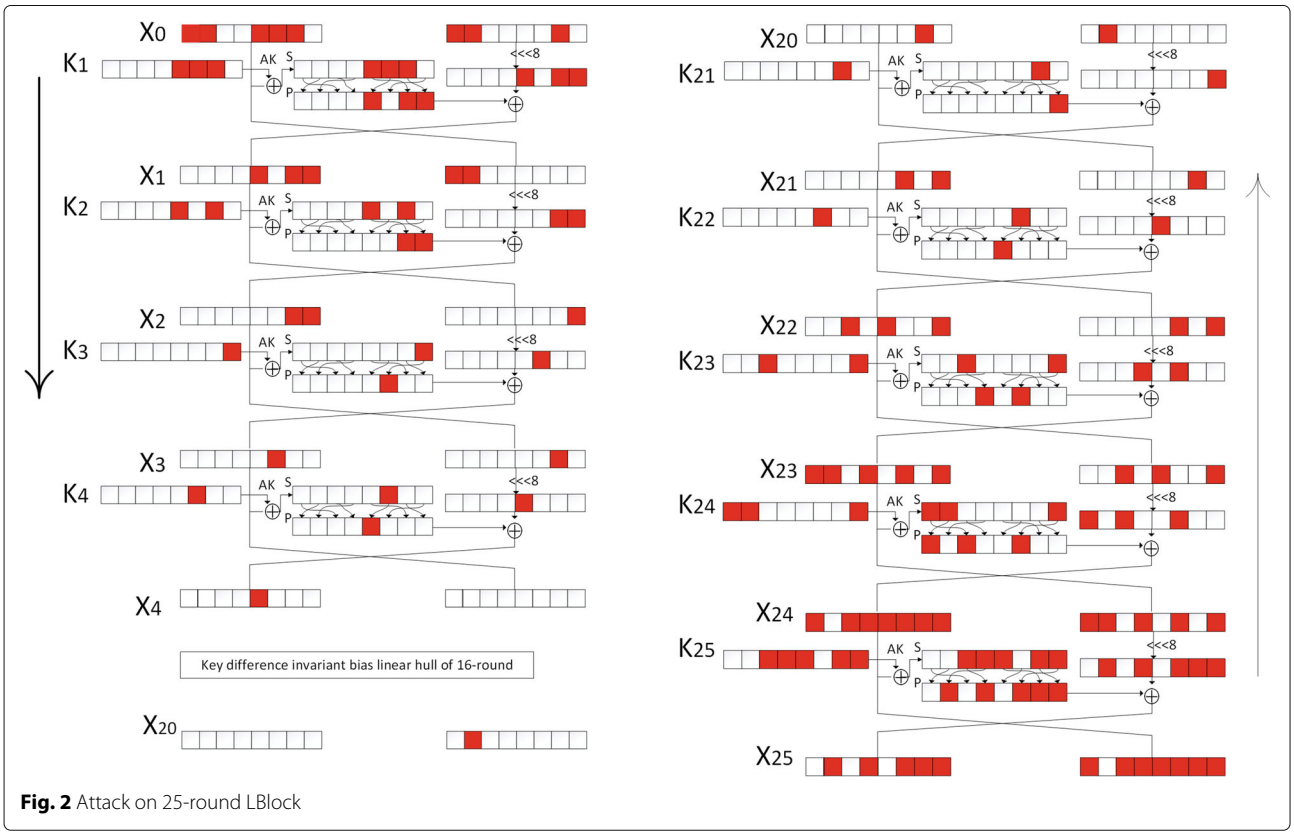

Fig. 2 Attack on 25-round LBlock

in Table 4. Under master key κ and κ', the subkey nibbles that have to be guessed in the second column. The Step 2's time complexity that is measured in S-box access in the third column. The "Obtained States" are saved during the encryption and decryption process in the fourth colum. Let x_i and x_i' $(1 \leq i \leq 14)$ denote the possible obtained states under the master key κ and κ', respectively, the counter $N_i[x_i]$ and $N_i[x_i']$ will record how many plaintext-ciphertext pairs can produce the corresponding intermediate state x_i and x_i', respectively. The counter size for x_i and x_i' is shown in the last column.

To be more clear, we explain some steps in Table 4 in detail.

Step 1. In the process of attack, the target values $X_4^4|X_{20}^9$ are affected by 32 bits of plaintext and 48 bits of ciphertext. They are represented by

$$x_0 = X_0^0|X_0^{14}|X_0^5|X_0^9|X_0^6|X_0^1|X_0^8|X_0^4|X_{25}^3|X_{25}^{10}|X_{25}^{13}|X_{25}^5|X_{25}^{15}|X_{25}^6|X_{25}^{12}|X_{25}^1|X_{25}^{11}|X_{25}^8|X_{25}^7|X_{25}^{14}.$$

We guess 18 bits subkeys $K_{25}^7|K_{25}^3|K_{25}^6|K_{24}^1|K_{23}^2[2:3]$ for the master key κ and κ' respectively. The following two equtions are true for LBlock.

$$\begin{cases} X_{23}^7 = X_{25}^5 \oplus S(X_{25}^{15} \oplus K_{25}^7), \\ X_{21}^5 = X_{25}^1 \oplus S(X_{25}^{11} \oplus K_{25}^3) \oplus S(X_{25}^8 \oplus S(X_{25}^7 \oplus S(X_{25}^{14} \oplus K_{25}^6) \oplus K_{24}^1) \oplus K_{23}^2). \end{cases}$$

So we can update the expression of X_{20}^9:

$$\begin{aligned} X_{20}^9 = {} & X_{25}^3 \oplus S(X_{25}^{10} \oplus K_{25}^2) \oplus S\left[X_{25}^3 \oplus S\left(X_{23}^7 \oplus K_{24}^7\right) \oplus K_{23}^7\right] \\ & \oplus S\left\{\left[X_{25}^{10} \oplus S\left(X_{25}^6 \oplus S\left(X_{25}^{12} \oplus K_{25}^4\right) \oplus K_{24}^0\right)\right]\right. \\ & \left. \oplus S\left(X_{21}^5 \oplus K_{22}^5\right) \oplus K_{21}^6\right\}. \end{aligned}$$

The 80-bit x_0 and x_0' can be reduced to 60-bit x_1 and x_1' after guessing the 18 bits round keys. We allocate two 60-bit counters $N_1[x_1]$ and $N_1[x_1']$ for the master key κ and κ', respectively, and initialize them to zero. We then guess 18-bit keys and partially decrypt N ciphertexts to compute x_1 and x_1' under master key κ and κ', respectively, and increment the corresponding counters.

Step 2. We first allocate 56-bit counter $N_2[x_2]$ and $N_2[x_2']$ for the master key κ and κ', respectively, and initialize them to zero. We then guess 4-bit K_1^4 for the master key κ and κ', respectively, and partially encrypt x_1 and x_1' to compute x_2 and x_2', respectively, and increment the corresponding counters. As the equation $X_1^6 =$

Table 4 Partial encryption and decryption on 25-round LBlock

Step	Guess	Time	Obtained States	Size
1	K_{25}^6, K_{25}^7 $K_{23}^2[2:3]$ K_{24}^1, K_{25}^3	$N \cdot 2^{18} \cdot 10$	$x_1(x_1') = X_0^0\|X_0^{14}\|X_0^5\|X_0^9\|X_0^6\|X_0^1\|X_0^8\|X_0^4$ $X_{25}^3\|X_{25}^{10}\|X_{25}^{13}\|X_{23}^7\|X_{25}^6\|X_{25}^{12}\|X_{21}^5$	$2^{60} \cdot 2$
2	K_1^4	$2^{60} \cdot 2^{18+4} \cdot 2$	$x_2(x_2') = X_0^0\|X_0^{14}\|X_0^5\|X_0^9\|X_0^6\|X_0^1\|X_1^6\|$ $X_{25}^3\|X_{25}^{10}\|X_{25}^{13}\|X_{23}^7\|X_{25}^6\|X_{25}^{12}\|X_{21}^5$	$2^{56} \cdot 2$
3	K_2^6	$2^{56} \cdot 2^{22+4} \cdot 2$	$x_3(x_3') = X_0^0\|X_0^{14}\|X_0^5\|X_0^9\|X_0^6\|X_2^7\|X_{25}^3\|$ $X_{25}^{10}\|X_{25}^{13}\|X_{23}^7\|X_{25}^6\|X_{25}^{12}\|X_{21}^5$	$2^{52} \cdot 2$
4	K_{24}^7 2^3 possible values	$2^{52} \cdot 2^{26+3} \cdot 2$	$x_4(x_4') = X_0^0\|X_0^{14}\|X_0^5\|X_0^9\|X_0^6\|X_2^7\|X_{25}^3\|$ $X_{25}^{10}\|X_{22}^7\|X_{25}^6\|X_{25}^{12}\|X_{21}^5$	$2^{48} \cdot 2$
5	K_1^6	$2^{48} \cdot 2^{29+4} \cdot 2$	$x_5(x_5') = X_0^0\|X_0^{14}\|X_0^5\|X_1^7\|X_2^7\|X_{25}^3\|X_{25}^{10}\|$ $X_{22}^7\|X_{25}^6\|X_{25}^{12}\|X_{21}^5$	$2^{44} \cdot 2$
6	K_3^7 2 possible values	$2^{44} \cdot 2^{33+1} \cdot 2$	$x_6(x_6') = X_0^0\|X_0^{14}\|X_0^5\|X_3^5\|X_{25}^3\|X_{25}^{10}\|X_{22}^7\|$ $X_{25}^6\|X_{25}^{12}\|X_{21}^5$	$2^{40} \cdot 2$
7	K_{25}^4	$2^{40} \cdot 2^{34+4} \cdot 2$	$x_7(x_7') = X_0^0\|X_0^{14}\|X_0^5\|X_3^5\|X_{25}^3\|X_{25}^{10}\|X_{22}^7\|$ $X_{23}^0\|X_{21}^5$	$2^{36} \cdot 2$
8	$K_{24}^0(K_{22}^5)$	$2^{36} \cdot 2^{38+4} \cdot 4$	$x_8(x_8') = X_0^0\|X_0^{14}\|X_0^5\|X_3^5\|X_{25}^3\|X_{25}^{10}\|X_{22}^7\|$ X_{20}^6	$2^{32} \cdot 2$
9	K_{25}^2 2^3 possible values	$2^{32} \cdot 2^{42+3} \cdot 2$	$x_9(x_9') = X_0^0\|X_0^{14}\|X_0^5\|X_3^5\|X_{23}^5\|X_{22}^7\|X_{20}^6$	$2^{28} \cdot 2$
10	$K_{23}^7[0]$	$2^{28} \cdot 2^{45+1} \cdot 2$	$x_{10}(x_{10}') = X_0^0\|X_0^{14}\|X_0^5\|X_3^5\|X_{21}^7\|X_{20}^6$	$2^{24} \cdot 2$
11	K_1^5	$2^{24} \cdot 2^{46+4} \cdot 2$	$x_{11}(x_{11}') = X_0^0\|X_1^4\|X_3^5\|X_{21}^7\|X_{20}^6$	$2^{20} \cdot 2$
12	K_2^4	$2^{20} \cdot 2^{50+4} \cdot 2$	$x_{12}(x_{12}') = X_3^{14}\|X_3^5\|X_{21}^7\|X_{20}^6$	$2^{16} \cdot 2$
13	$K_4^5[1]$	$2^{16} \cdot 2^{54+1} \cdot 2$	$x_{13}(x_{13}') = X_4^4\|X_{21}^7\|X_{20}^6$	$2^{12} \cdot 2$
14	K_{21}^6	$2^{12} \cdot 2^{55+4} \cdot 2$	$x_{14}(x_{14}') = X_4^4\|X_{20}^9$	$2^8 \cdot 2$

$X_0^8 \oplus S\left(X_0^4 \oplus K_1^4\right)$ holds, the expression of X_4^4 is update as:

$$X_4^4 = X_0^0 \oplus S\left(X_0^{14} \oplus S\left(X_0^5 \oplus K_1^5\right) \oplus K_2^4\right) \oplus S\Big(X_0^9 \oplus S\left(X_0^6 \oplus K_1^6\right) \oplus S\left(X_0^1 \oplus S\left(X_1^6 \oplus K_2^6\right) \oplus K_3^7\right) \oplus K_4^5\Big).$$

Because the following steps are similar to the above two steps, we do not explain in details. Besides, we note that the numbers of guessed keys in step 8 of Table 4 is 4 bits. However, the numbers of known keys are 8 bits, that is because the key in the "( )" can be obtained by using the relations of round keys. To recover the secret key, the following steps are performed:

1. Allocate two counters $V[\eta]$ and $V'[\eta]$ for 8-bit $X_4^4|X_{20}^9 = \eta$.
2. For 2^8 values of x_{14} and x'_{14}:
(a) Evaluate all 8 basis masks on x_{14} and x'_{14} and get η;
(b) Update the counters $V(\eta)$ and $V'(\eta)$ by $V(\eta) = V(\eta) + N_{14}[x_{14}]$ and $V'(\eta) = V'(\eta) + N_{14}[x_{14}]$.
3. For each guessing key, compute

$$Q = 2^m \cdot \sum_{\eta=0}^{2^m-1} \left[\left(\frac{V(\eta)}{N} - 2^{-m}\right) - \left(\frac{V'(\eta)}{N} - 2^{-m}\right)\right]^2$$

4. If $Q \le \tau$, then the guessed subkey values are possible right subkey candidates.
5. Do exhaustive search for all right candidates.

After processding of attack procedure from step 1 to 5, 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 $k_{14:17}$ and $S_9\left(k_{18:21}\right)^3$ 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. For example, we choose master key difference $\delta_{14:17} = 0111$, then $k_{14:17}$ and $S_9\left(k_{18:21}\right)^3$ have 8 possible values. We need to guess one by one and determine which one is the right key. The average number of guesses is $\frac{1}{8}(1+2+3+4+5+6+7+8) = 4.5$. Similarly, when $\delta_{14:17} = 1100, 0100, 1111$ or 1011 the average number of guesses is 2.5; when $\delta_{14:17} = 1010, 0110, 1001$ or 0101, the average number of guesses is 1.5. The key difference $\delta_{14:17}$ has 9 possible values, its probability distribution of $\delta_{14:17}$ is as follows (see Table 3).

$\delta_{14:17}$	1100,	0111,	1010,	0110,	0100,	1111,	1011,	1001,	0101
p	$\frac{4}{32}$,	$\frac{8}{32}$,	$\frac{2}{32}$,	$\frac{2}{32}$,	$\frac{4}{32}$,	$\frac{4}{32}$,	$\frac{4}{32}$,	$\frac{2}{32}$,	$\frac{2}{32}$

According to the above discussion, then,the total average number of guesses is $4.5 \cdot \frac{8}{32} + 2.5 \cdot \frac{4\times4}{32} + 1.5 \cdot \frac{2\times4}{32} = \frac{88}{32}$.

Complexity Now we evaluate the time complexity of the key recovery on 25-round LBlock. By setting $\alpha_0 = 2^{-2.7}, \alpha_1 = 0.5$, we have $q_{1-\alpha_0} \approx 1.02$ and $q_{1-\alpha_1} = 0$. Since $n = 64$ and $l = 255$, then according to Eq. (3), the data complexity $N^{DKP} \approx 2^{60.4}$. Now we evaluate the time complexity of the key recovery on 25-round LBlock. We start by evaluating the complexity of step 1 to step 14 in the process of partial computation(see Table 4), the time complexity is $T_1 = N \cdot 2^{19} \cdot 5 + 2 \cdot 2^{83} + 2 \cdot 2^{82} + 2 \cdot 2^{79} + 2^{80} + 2^{78} + 3 \cdot 2^{75} + 2 \cdot 2^{72} \approx 2^{84.89}$ S-box access, which is about $T = T_1 \cdot \frac{1}{8} \cdot \frac{1}{25} = 2^{77.25}$ 25-round LBlock encryptions. Under each related-key differential path,the values $k_{14:17}$ and $S_9\left(k_{18:21}\right)^3$ are known, so the time complexity of Step 5 of key recovery attack is about $2^{75} \cdot \alpha_1 = 2^{74}$ times of 25-round encryption. Therefore, the total time complexity is about $2^{74} + 2^{77.25} \approx 2^{77.39}$ 25-round LBlock encryptions. Since the given value $k_{14:17}$ and $S_9\left(k_{18:21}\right)^3$ may not be the right key, the average number of guesses to the value of $k_{14:17}$ and $S_9\left(k_{18:21}\right)^3$ is $\frac{88}{32}$, so the expected time complexity of our attack on 25-round LBlock is about $2^{77.39} \cdot \frac{88}{32} \approx 2^{78.85}$ 25-round encryptions. The memory requirements are about 2^{61} bytes.

Key recovery for 24-Round LBlock

Similarly, we can perform key recover attack on 24-round LBlock by using the same linear approximations from round 5 to 20. We append 4 rounds at the top of the distinguisher and add 4 rounds at the bottom of the distinguisher.

We express the two target values of attack by using the related round keys and plaintexts or ciphertexts, then use the partial-compression technique to reduce the time complexity significantly (see Table 5). The nibble X_4^4 is affected by 32 bits of plaintext X_0 and 28 bits of round keys and the expression can be shown:

$$X_4^4 = X_0^0 \oplus S\left(X_0^{14} \oplus S\left(X_0^5 \oplus K_1^5\right) \oplus K_2^4\right) \oplus S\left(X_0^9 \oplus S\left(X_0^6 \oplus K_1^6\right) \oplus S\left(X_0^1 \oplus S\left(X_0^8 \oplus S\left(X_0^4 \oplus K_1^4\right) \oplus K_2^6\right) \oplus K_3^7\right) \oplus K_4^5\right)$$

Similarly, the nibble X_{20}^9 is affected by 32 bits of ciphertext X_{24} and 28 bits of round keys and the expression can be shown:

$$X_{20}^9 = X_{24}^{13} \oplus S\left(X_{24}^5 \oplus S\left(X_{24}^{15} \oplus K_{24}^7\right) \oplus K_{23}^7\right) \oplus S\left(X_{24}^2 \oplus S\left(X_{24}^8 \oplus K_{24}^0\right) \oplus S\left(X_{24}^{11} \oplus S\left(X_{24}^0 \oplus S\left(X_{24}^9 \oplus K_{24}^1\right) \oplus K_{23}^2\right) \oplus K_{21}^6\right)\right)$$

After analyzing the key schedule of LBlock, we find the following relations in the round keys: $K_{24}^0 \Rightarrow K_{23}^7[1:3]; K_{24}^0, K_{24}^1, K_1^6 \Rightarrow K_4^5[0,2,3]$.

Assuming that N distinct known plaintexts are used, the partial encryption and decryption using the partial-compression technique are proceeded as in Table 5. The process can be referred to 25-round attack on LBlock.

Table 5 Partial encryption and decryption on 24-round LBlock

Step	Guess	Time	Obtained States	Size
1	K_{24}^{7}	$N \cdot 2^{4} \cdot 2$	$X_0^0 \mid X_0^{14} \mid X_0^5 \mid X_0^9 \mid X_0^6 \mid X_0^1 \mid X_0^8 \mid X_0^4 \mid X_{24}^{13} \mid$ $X_{22}^7 \mid X_{24}^2 \mid X_{24}^8 \mid X_{24}^{11} \mid X_{24}^0 \mid X_{24}^9$	$2^{60} \cdot 2$
2	K_{24}^{0}	$2^{60} \cdot 2^{8} \cdot 2$	$X_0^0 \mid X_0^{14} \mid X_0^5 \mid X_0^9 \mid X_0^6 \mid X_0^1 \mid X_0^8 \mid X_0^4 \mid X_{24}^{13} \mid$ $X_{22}^7 \mid X_{22}^4 \mid X_{24}^{11} \mid X_{24}^0 \mid X_{24}^9$	$2^{56} \cdot 2$
3	$K_{23}^{7}[0]$	$2^{56} \cdot 2^{8+1} \cdot 2$	$X_0^0 \mid X_0^{14} \mid X_0^5 \mid X_0^9 \mid X_0^6 \mid X_0^1 \mid X_0^8 \mid X_0^4 \mid X_{21}^7 \mid$ $X_{22}^4 \mid X_{24}^{11} \mid X_{24}^0 \mid X_{24}^9$	$2^{52} \cdot 2$
4	K_{1}^{4}	$2^{52} \cdot 2^{9+4} \cdot 2$	$X_0^0 \mid X_0^{14} \mid X_0^5 \mid X_0^9 \mid X_0^6 \mid X_0^1 \mid X_0^1 \mid X_1^6 \mid X_{21}^7 \mid X_{22}^4 \mid$ $X_{24}^{11} \mid X_{24}^0 \mid X_{24}^9$	$2^{48} \cdot 2$
5	K_{2}^{6}	$2^{48} \cdot 2^{13+4} \cdot 2$	$X_0^0 \mid X_0^{14} \mid X_0^5 \mid X_0^9 \mid X_0^6 \mid X_2^7 \mid X_{21}^7 \mid X_{22}^4 \mid X_{24}^{11} \mid$ $X_{24}^0 \mid X_{24}^9$	$2^{44} \cdot 2$
6	K_{1}^{6}	$2^{44} \cdot 2^{17+4} \cdot 2$	$X_0^0 \mid X_0^{14} \mid X_0^5 \mid X_1^7 \mid X_2^7 \mid X_{21}^7 \mid X_{22}^4 \mid X_{24}^{11} \mid$ $X_{24}^0 \mid X_{24}^9$	$2^{40} \cdot 2$
7	K_{1}^{5}	$2^{40} \cdot 2^{21+4} \cdot 2$	$X_0^0 \mid X_1^4 \mid X_1^7 \mid X_2^7 \mid X_{21}^7 \mid X_{22}^4 \mid X_{24}^{11} \mid X_{24}^0 \mid X_{24}^9$	$2^{36} \cdot 2$
8	K_{2}^{4}	$2^{36} \cdot 2^{25+4} \cdot 2$	$X_3^{14} \mid X_1^7 \mid X_2^7 \mid X_{21}^7 \mid X_{22}^4 \mid X_{24}^{11} \mid X_{24}^0 \mid X_{24}^9$	$2^{32} \cdot 2$
9	K_{3}^{7}	$2^{32} \cdot 2^{29+4} \cdot 2$	$X_3^{14} \mid X_3^5 \mid X_{21}^7 \mid X_{22}^4 \mid X_{24}^{11} \mid X_{24}^0 \mid X_{24}^9$	$2^{28} \cdot 2$
10	$K_{24}^{1}, K_{4}^{5}[1]$	$2^{28} \cdot 2^{33+5} \cdot 4$	$X_4^4 \mid X_{21}^7 \mid X_{22}^4 \mid X_{24}^{11} \mid X_{22}^2$	$2^{20} \cdot 2$
11	K_{23}^{2}	$2^{20} \cdot 2^{38+4} \cdot 2$	$X_4^4 \mid X_{21}^7 \mid X_{22}^4 \mid X_{21}^5$	$2^{16} \cdot 2$
12	K_{22}^{5}	$2^{16} \cdot 2^{42+4} \cdot 2$	$X_4^4 \mid X_{21}^7 \mid X_{20}^6$	$2^{12} \cdot 2$
13	K_{21}^{6}	$2^{12} \cdot 2^{46+4} \cdot 2$	$X_4^4 \mid X_{20}^9$	$2^{8} \cdot 2$

Complexity By setting $\alpha_0 = 2^{-2.7}, \alpha_1 = 2^{-8.5}$, then according to Eq. (2), the data complexity is $N^{KP} \approx 2^{62.83}$, the time complexity is about $2^{68.08}$ 24-round LBlock encryptions and the memory requirements are about 2^{61} bytes.

In the DKP case, we set $\alpha_0 = 2^{-2.7}, \alpha_1 = 2^{-8.5}$, then according to Eq. (3), the data complexity is $N^{DKP} \approx 2^{62.3}$, the time complexity is about $2^{68.07}$ 24-round LBlock encryptions and the memory requirements are about 2^{61} bytes. Figure 3 depicts different possible data time tradeoffs with $\alpha_0 = 2^{-2.7}$.

Attack on TWINE-128

In this section, we will evaluate the security of TWINE-128 against multidimensional linear attack with key difference invariant bias by using the new distinguisher Q.

A brief description of TWINE

TWINE is a 64-bit lightweight block cipher with 80 or 128-bit key. It was proposed by Suzaki et al in 2012. The structure of TWINE is a modified Type-2 generalized Feistel network. Its round function consists of AddRoundkey, 4-bit S-boxes and a diffusion layer. This round function is iterated for 36 times for both TWINE-80 and TWINE-128, where the diffusion layer of the last round is omitted.

The key schedule of TWINE is quite simple. S-boxes, XOR operations and a series of constants are used in the key schedule. Due to the page limit, see the specific key schedule algorithms in Suzaki et al. (2012).

Key recovery for 28-round TWINE-128

We consider 17-round (from round 6 to round 22) linear approximations with key difference invariant bias for TWINE-128 that have been identified in Bogdanov et al. (2013). The input mask of the 6-th round is $(000000000000\alpha000)$ and the output mask of the 22-th round is $(0000000\beta00000000)$, $(\alpha, \beta) \neq 0$. Let K and K' be the expanded keys corresponding to two the master keys κ and κ', $K = \varphi(\kappa)$ and $K' = \varphi(\kappa')$ for key schedule φ, such that $K = K' \oplus \Delta$. Let us denote by $\delta = \kappa \oplus \kappa'$ the difference of masker keys κ and κ'. Let ΔK_r and Γ_r denote the subkey difference and input mask value for the S-boxes in round r, respectively. To make the relations

$$\Gamma_r \cdot \Delta K_r = 0, 6 \leq r \leq 22 \tag{6}$$

hold, it suffices to let $\delta_{20:23} \neq 0000$, $\delta_j = 0, j = 0, 1, ..., 79$ and $j \neq 20, 21, 22, 23$.

Thus sufficient condition for key difference invariant bias is satisfied. There are 15 possible nonzero values $\delta_{20:23}$ that satisfy the Eq. (6). We can choose any nonzero $\delta_{20:23}$, and $\delta_j = 0, j = 0, 1, ..., 79$ and $j \neq 20, 21, 22, 23$, to obtain the differential path which covers all the possible key values and is sufficient to recovery the right key value.

We utilize the 17-round distinguisher to attack 28 rounds of TWINE-128. The initial five rounds from 1 to

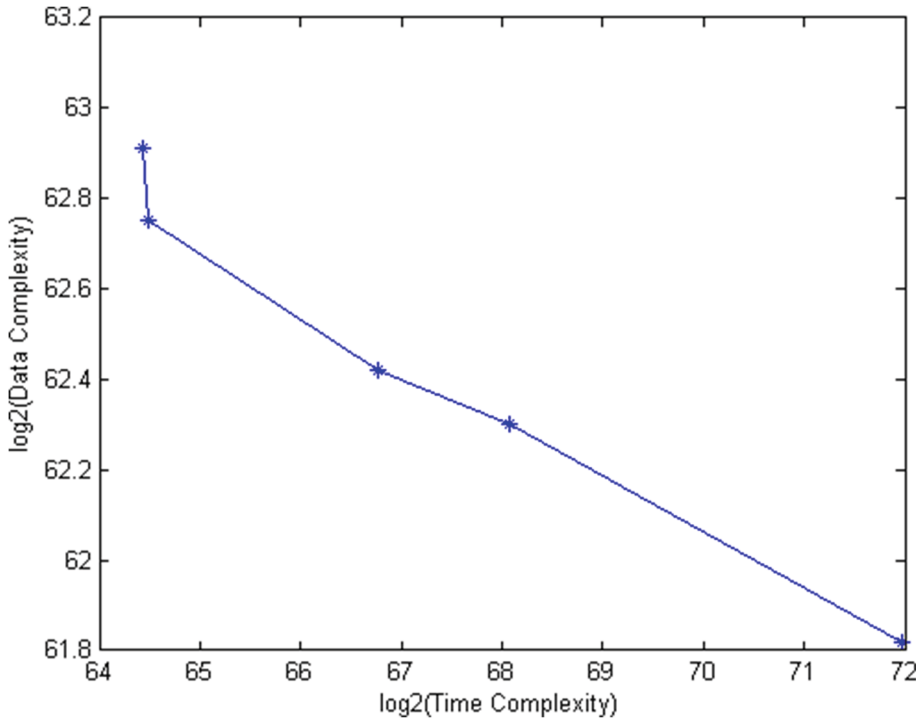

Fig. 3 Data-time tradeoff for the attack on 24-round LBlock

round 5 are added before the distinguisher and the finial six rounds from 23 to round 28 are appended after the distinguisher. Similary, we express the two target values and then guess the keys one nibble after another to reduce the time complexity of partial computation. The nibble X_5^{12} is affected by 48 bits of plaintext X_0 and 48 bits of round keys and the expression can be shown as:

$$\begin{aligned} X_5^{12} = & X_0^{11} \oplus S\left(X_0^{10} \oplus K_1^5\right) \oplus S\left(X_0^2 \oplus S\left(X_0^1 \oplus S\left(X_0^0 \oplus K_1^0\right)\right.\right. \\ & \left.\oplus K_2^0\right) \oplus K_3^0\right) \oplus S\left(X_0^{10} \oplus S\left(X_0^7 \oplus S\left(X_0^6 \oplus K_1^3\right) \oplus K_2^4\right)\right. \\ & \oplus S\left(X_0^{15} \oplus S\left(X_0^{14} \oplus K_1^7\right) \oplus S\left(X_0^8 \oplus S\left(X_0^5 \oplus S\left(X_0^4\right.\right.\right. \\ & \left.\left.\left.\left.\oplus K_1^2\right) \oplus K_2^6\right) \oplus K_3^5\right) \oplus K_4^1\right) \oplus K_5^2\right) \end{aligned} \tag{7}$$

Similarly, the nibble X_{22}^7 is affected by 60 bits of ciphertext X_{28} and 76 bits of round keys:

$$\begin{aligned} X_{22}^7 = & X_{28}^3 \oplus S\left(X_{28}^{10} \oplus S\left(X_{28}^{15} \oplus K_{28}^6\right) \oplus K_{27}^4\right) \oplus S\left(X_{28}^2\right. \\ & \oplus S\left(X_{28}^9 \oplus K_{28}^5\right) \oplus S\left(X_{28}^1 \oplus S\left(X_{28}^6 \oplus S\left(X_{28}^{13} \oplus K_{28}^4\right)\right.\right. \\ & \left.\left.\oplus K_{27}^5\right) \oplus K_{26}^7\right) \oplus K_{25}^6\right) \oplus S\left(X_{28}^{10} \oplus S\left(X_{28}^{15} \oplus K_{28}^6\right)\right. \\ & \oplus S\left(X_{28}^7 \oplus S\left(X_{28}^0 \oplus S\left(X_{28}^5 \oplus K_{28}^0\right) \oplus K_{27}^1\right) \oplus K_{26}^3\right) \\ & \oplus S\left(X_{28}^{15} \oplus S\left(X_{28}^8 \oplus S\left(X_{28}^3 \oplus K_{28}^3\right) \oplus K_{27}^2\right)\right. \\ & \oplus S\left(X_{28}^{14} \oplus S\left(X_{28}^{11} \oplus K_{28}^7\right) \oplus S\left(X_{28}^{13} \oplus S\left(X_{28}^4\right.\right.\right. \\ & \left.\left.\left.\oplus S\left(X_{28}^1 \oplus K_{28}^1\right) \oplus K_{27}^3\right) \oplus K_{26}^2\right) \oplus K_{25}^0\right) \oplus K_{24}^1\right) \\ & \left.\oplus K_{23}^3\right) \end{aligned}$$

The following relations exist in the related round keys:

$$K_1^3 \Leftrightarrow K_4^1, K_{28}^5 \Leftrightarrow K_{24}^1.$$

Thus, we just need guess 116 bits subkeys in the attack.

Assuming that N distinct known plaintexts are used, the partial encryption and decryption using the partial-compression technique are proceeded as in Table 6.

Complexity We set $\alpha_0 = 2^{-2.7}, \alpha_1 = 2^{-3}$, so we have $q_{1-\alpha_0} \approx 1.02$ and $q_{1-\alpha_1} = 1.15$. Since $n = 64$ and $l = 255$, then according to Eq. (3), the data complexity $N^{DKP} \approx 2^{61.5}$. Now we evaluate the time complexity of the key recovery on 28-round TWINE-128. We start by evaluating the complexity of step 1 to step 14 in the process of partial-compression (see Table 6), the time complexity is $T_1 = N \cdot 2^{65} \cdot 17 + 12 \cdot 2^{129} + 2^{130} \approx 2^{133.09}$ S-box access, which is about $T = T_1 \cdot \frac{1}{8} \cdot \frac{1}{28} = 2^{125.28}$ 28-round TEINE-128 encryptions. Note that the time complexity of Step 3, 4 is negligible. The time complexity of Step 5 of key recovery attack is about $2^{128} \cdot \alpha_1 = 2^{125}$ times of 25-round encryption. Therefore, the total time complexity is about $2^{125} + 2^{125.28} \approx 2^{126.15}$ 28-round TWINE encryptions. The memory requirements are about 2^{61} bytes.

Key recovery for 27-round TWINE-128

We use the 17-round 8-dimension linear approximations with key difference invariant bias to give an attack on 27-round TWINE-128. By putting the 17-round 8-dimension

Table 6 Partial encryption and decryption on 28-round TWINE-128

Step	Guess	Time	Obtained States	Size
1	$K_{28}^5, K_{28}^3, K_{27}^2$ $K_{28}^7, K_{28}^1, K_{27}^3$ $K_{26}^2, K_{25}^0, K_{28}^0$ $K_{27}^1, K_{28}^6, K_{26}^3$ $(K_{24}^1), K_{27}^4$ $(K_{28}^5), K_{27}^5, K_{26}^7$	$N \cdot 2^{64} \cdot 2 \cdot 17$	$y_1\,(y_1') = X_0^{11}\,\lvert X_0^{10}\rvert\, X_0^2\,\lvert X_0^1\rvert\, X_0^0\,\lvert X_0^7\rvert$ $X_0^6\,\lvert X_0^{15}\rvert\, X_0^{14}\,\lvert X_0^8\rvert\, X_0^5\,\lvert X_0^4\rvert\, X_{25}^{10}\,\lvert X_{25}^{15}\rvert$ X_{23}^3	$2^{60} \cdot 2$
2	K_1^2	$2^{60} \cdot 2^{64+4} \cdot 2$	$y_2\,(y_2') = X_0^{11}\,\lvert X_0^{10}\rvert\, X_0^2\,\lvert X_0^1\rvert\, X_0^0\,\lvert X_0^7\rvert$ $X_0^6\,\lvert X_0^{15}\rvert\, X_0^{14}\,\lvert X_0^8\rvert\, X_1^{12}\,\lvert X_{25}^{10}\rvert\, X_{25}^{15}\rvert X_{23}^3$	$2^{56} \cdot 2$
3	K_2^6	$2^{56} \cdot 2^{68+4} \cdot 2$	$y_3\,(y_3') = X_0^{11}\,\lvert X_0^{10}\rvert\, X_0^2\,\lvert X_0^1\rvert\, X_0^0\,\lvert X_0^7\rvert$ $X_0^6\,\lvert X_0^{15}\rvert\, X_0^{14}\,\lvert X_2^{10}\,X_{25}^{10}\,\lvert X_{25}^{15}\rvert\, X_{23}^3$	$2^{52} \cdot 2$
4	K_1^7	$2^{52} \cdot 2^{72+4} \cdot 2$	$y_4\,(y_4') = X_0^{11}\,\lvert X_0^{10}\rvert\, X_0^2\,\lvert X_0^1\rvert\, X_0^0\,\lvert X_0^7\rvert$ $X_0^6\,\lvert X_1^{14}\rvert\, X_2^{10}\,\lvert X_{25}^{10}\rvert\, X_{25}^{15}\rvert X_{23}^3$	$2^{48} \cdot 2$
5	K_3^5	$2^{48} \cdot 2^{76+4} \cdot 2$	$y_5\,(y_5') = X_0^{11}\,\lvert X_0^{10}\rvert\, X_0^2\,\lvert X_0^1\rvert\, X_0^0\,\lvert X_0^7\rvert$ $X_0^6\,\lvert X_3^2\rvert\, X_{25}^{10}\,\lvert X_{25}^{15}\rvert\, X_{23}^3$	$2^{44} \cdot 2$
6	K_1^3	$2^{44} \cdot 2^{80+4} \cdot 2$	$y_6\,(y_6') = X_0^{11}\,\lvert X_0^{10}\rvert\, X_0^2\,\lvert X_0^1\rvert\, X_0^0\,\lvert X_1^8\rvert$ $X_3^2\,\lvert X_{25}^{10}\rvert\, X_{25}^{15}\rvert X_{23}^3$	$2^{40} \cdot 2$
7	$K_2^4\,(K_4^1)$	$2^{40} \cdot 2^{84+4} \cdot 4$	$y_7\,(y_7') = X_0^{11}\,\lvert X_0^{10}\rvert\, X_0^2\,\lvert X_0^1\rvert\, X_0^0\,\lvert X_4^4\rvert$ $X_{25}^{10}\,\lvert X_{25}^{15}\rvert\, X_{23}^3$	$2^{36} \cdot 2$
8	K_1^5	$2^{36} \cdot 2^{88+4} \cdot 2$	$y_8\,(y_8') = X_1^2\,\lvert X_0^2\rvert\, X_0^1\,\lvert X_0^0\rvert\, X_4^4\,\lvert X_{25}^{10}\rvert$ $X_{25}^{15}\rvert X_{23}^3$	$2^{32} \cdot 2$
9	K_1^0	$2^{32} \cdot 2^{92+4} \cdot 2$	$y_9\,(y_9') = X_1^2\,\lvert X_0^2\rvert\, X_1^0\,\lvert X_4^4\rvert\, X_{25}^{10}\,\lvert X_{25}^{15}\rvert$ X_{23}^3	$2^{28} \cdot 2$
10	K_2^0	$2^{28} \cdot 2^{96+4} \cdot 2$	$y_{10}\,(y_{10}') = X_1^2\,\lvert X_2^0\rvert\, X_4^4\,\lvert X_{25}^{10}\rvert\, X_{25}^{15}\rvert X_{23}^3$	$2^{24} \cdot 2$
11	K_3^0	$2^{24} \cdot 2^{100+4} \cdot 2$	$y_{11}\,(y_{11}') = X_4^5\,\lvert X_4^4\rvert\, X_{25}^{10}\,\lvert X_{25}^{15}\rvert\, X_{23}^3$	$2^{20} \cdot 2$
12	K_5^2	$2^{20} \cdot 2^{104+4} \cdot 2$	$y_{12}\,(y_{12}') = X_5^{12}\,\lvert X_{25}^{10}\rvert\, X_{25}^{15}\rvert X_{23}^3$	$2^{16} \cdot 2$
13	K_{25}^6	$2^{16} \cdot 2^{108+4} \cdot 2$	$y_{13}\,(y_{13}') = X_5^{12}\,\lvert X_{23}^8\rvert\, X_{23}^3$	$2^{12} \cdot 2$
14	K_{23}^3	$2^{12} \cdot 2^{112+4} \cdot 2$	$y_{14}\,(y_{14}') = X_5^{12}\rvert X_{22}^7$	$2^8 \cdot 2$

linear approximations in round 6 to 22, we can perform key recovery attack on 27-round TWINE-128. Similary, we can express the two target values X_5^{12} and X_{22}^7, the values X_5^{12} is the same as (7), the nibble X_{22}^7 can be shown as:

$$\begin{aligned} X_{22}^7 = X_{27}^6 \oplus S\left(X_{27}^{13} \oplus K_{27}^4\right) \oplus S\left(X_{27}^{11} \oplus S\left(X_{27}^2 \oplus S\left(X_{27}^9\right.\right.\right. \\ \left.\left.\left. \oplus K_{27}^5\right) \oplus K_{26}^7\right) \oplus K_{25}^6\right) \oplus S\left(X_{27}^{13} \oplus S\left(X_{27}^4 \oplus S\left(X_{27}^1\right.\right.\right. \\ \left.\left.\left. \oplus K_{27}^1\right) \oplus K_{26}^3\right) \oplus S\left(X_{27}^{12} \oplus S\left(X_{27}^7 \oplus K_{27}^2\right) \oplus S\left(X_{27}^{15}\right.\right.\right. \\ \left.\left.\left. \oplus S\left(X_{27}^8 \oplus S\left(X_{27}^3 \oplus K_{27}^3\right) \oplus K_{26}^2\right) \oplus K_{25}^0\right) \oplus K_{24}^1\right) \\ \left. \oplus K_{23}^3\right) \end{aligned}$$

The nibble X_5^{12} is affected by 48 bits of plaintext X_0 and 48 bits of round keys, the nibble X_{22}^7 is affected by 48 bits of ciphertext X_{27} and 48 bits of round keys. The following relations exist in the related round keys:

$$K_1^3 \Leftrightarrow K_4^1.$$

Assuming that N distinct known plaintexts are used, the partial encryption and decryption using the partial-compression technique are proceeded as in Table 7.

Complexity We set $\alpha_0 = 2^{-2.7}, \alpha_1 = 2^{-8.5}$, according to Eq. (3), the data complexity $N^{DKP} \approx 2^{62.3}$. The time complexity of partial computation about is $2^{107.27}$ S-box access, which is about $2^{107.27} \cdot \frac{1}{8} \cdot \frac{1}{27} = 2^{99.52}$ 27-round TEINE-128 encryptions. The number of remaining key candidates is about $2^{128} \cdot \alpha_1 = 2^{119.5}$ times of 27-round encryption. Thus, the total time complexity is about $2^{99.52} + 2^{119.5} \approx 2^{119.5}$ 27-round TWINE encryptions. Meanwhile, the memory requirements are about 2^{61} bytes. Figure 4 depicts different possible data time trade-offs with $\alpha_0 = 2^{-2.7}$.

Combined Model. In order to reduced the data complexity of attacks, we can perform 27-round key recovery attack which use all differential paths of 15 key difference

Table 7 Partial encryption and decryption on 27-round TWINE-128

Step	Guess	Time	Obtained States	Size
1	K_1^3, K_1^5, K_2^4 K_1^7, K_1^2, K_2^6 $K_3^5, (K_4^1)$ K_1^0, K_2^0	$N \cdot 2^{4\times 9} \cdot 2 \cdot 10$	$X_1^2 \mid X_2^0 \mid X_4^4 \mid X_{27}^6 \mid X_{27}^{13} \mid X_{27}^{11} \mid X_{27}^2 \mid X_{27}^9 \mid$ $X_{27}^4 \mid X_{27}^1 \mid X_{27}^{12} \mid X_{27}^7 \mid X_{27}^{15} \mid X_{27}^8 \mid X_{27}^3$	$2^{60} \cdot 2$
2	K_3^0	$2^{60} \cdot 2^{36+4} \cdot 2$	$X_4^5 \mid X_4^4 \mid X_{27}^6 \mid X_{27}^{13} \mid X_{27}^{11} \mid X_{27}^2 \mid X_{27}^9 \mid X_{27}^4 \mid$ $X_{27}^1 \mid X_{27}^{12} \mid X_{27}^7 \mid X_{27}^{15} \mid X_{27}^8 \mid X_{27}^3$	$2^{56} \cdot 2$
3	K_5^2	$2^{56} \cdot 2^{40+4} \cdot 2$	$X_5^{12} \mid X_{27}^6 \mid X_{27}^{13} \mid X_{27}^{11} \mid X_{27}^2 \mid X_{27}^9 \mid X_{27}^4 \mid X_{27}^1 \mid$ $X_{27}^{12} \mid X_{27}^7 \mid X_{27}^{15} \mid X_{27}^8 \mid X_{27}^3$	$2^{52} \cdot 2$
4	K_{27}^5	$2^{52} \cdot 2^{44+4} \cdot 2$	$X_5^{12} \mid X_{27}^6 \mid X_{27}^{13} \mid X_{27}^{11} \mid X_{26}^{11} \mid X_{27}^4 \mid X_{27}^1 \mid X_{27}^{12} \mid$ $X_{27}^7 \mid X_{27}^{15} \mid X_{27}^8 \mid X_{27}^3$	$2^{48} \cdot 2$
5	K_{26}^7	$2^{48} \cdot 2^{48+4} \cdot 2$	$X_5^{12} \mid X_{27}^6 \mid X_{27}^{13} \mid X_{25}^{15} \mid X_{27}^4 \mid X_{27}^1 \mid X_{27}^{12} \mid X_{27}^7 \mid$ $X_{27}^{15} \mid X_{27}^8 \mid X_{27}^3$	$2^{44} \cdot 2$
6	K_{27}^3	$2^{44} \cdot 2^{52+4} \cdot 2$	$X_5^{12} \mid X_{27}^6 \mid X_{27}^{13} \mid X_{25}^{15} \mid X_{27}^4 \mid X_{27}^1 \mid X_{27}^{12} \mid X_{27}^7 \mid$ $X_{27}^{15} \mid X_{26}^7$	$2^{40} \cdot 2$
7	K_{26}^2	$2^{40} \cdot 2^{56+4} \cdot 2$	$X_5^{12} \mid X_{27}^6 \mid X_{27}^{13} \mid X_{25}^{15} \mid X_{25}^4 \mid X_{27}^1 \mid X_{27}^{12} \mid X_{27}^7 \mid$ X_{25}^5	$2^{36} \cdot 2$
8	K_{27}^2	$2^{36} \cdot 2^{60+4} \cdot 2$	$X_5^{12} \mid X_{27}^6 \mid X_{27}^{13} \mid X_{25}^{15} \mid X_{27}^4 \mid X_{27}^1 \mid X_{26}^5 \mid X_{25}^5$	$2^{32} \cdot 2$
9	K_{27}^1	$2^{32} \cdot 2^{64+4} \cdot 2$	$X_5^{12} \mid X_{27}^6 \mid X_{27}^{13} \mid X_{25}^{15} \mid X_{26}^3 \mid X_{26}^5 \mid X_{25}^5$	$2^{28} \cdot 2$
10	K_{25}^0	$2^{28} \cdot 2^{68+4} \cdot 2$	$X_5^{12} \mid X_{27}^6 \mid X_{27}^{13} \mid X_{25}^{15} \mid X_{26}^3 \mid X_{24}^1$	$2^{24} \cdot 2$
11	K_{27}^4	$2^{24} \cdot 2^{72+4} \cdot 2$	$X_5^{12} \mid X_{26}^9 \mid X_{27}^{13} \mid X_{25}^{15} \mid X_{26}^3 \mid X_{24}^1$	$2^{24} \cdot 2$
12	K_{26}^3	$2^{24} \cdot 2^{76+4} \cdot 2$	$X_5^{12} \mid X_{26}^9 \mid X_{25}^{15} \mid X_{25}^7 \mid X_{24}^1$	$2^{20} \cdot 2$
13	K_{25}^6	$2^{20} \cdot 2^{80+4} \cdot 2$	$X_5^{12} \mid X_{23}^8 \mid X_{25}^7 \mid X_{24}^1$	$2^{16} \cdot 2$
14	K_{24}^1	$2^{16} \cdot 2^{84+4} \cdot 2$	$X_5^{12} \mid X_{23}^8 \mid X_{23}^3$	$2^{12} \cdot 2$
15	K_{23}^3	$2^{12} \cdot 2^{88+4} \cdot 2$	$X_5^{12} \mid X_{22}^7$	$2^8 \cdot 2$

that satisfy condition of key difference invariant bias together. Let $\delta^{(i)}, 1 \le i \le 15$ denote the i-th master key difference that satisfy condition of key difference invariant bias. $V_i(\eta)$ and $V_i'(\eta)$, $\eta = 0, ..., 2^m - 1$ denote the number of occurrences of value η of the observed data distribution for master keys κ and κ' such that $\kappa \oplus \kappa' = \delta^{(i)}$ with the N texts. Let $Q^{(i)}$ be the i-th $i = 1, ..., 15$ statistic under master key difference $\delta^{(i)}$, then

$$Q^{(i)} = 2^m \cdot \sum_{\eta=0}^{2^m-1} \left[\left(\frac{V_i(\eta)}{N} - 2^{-m} \right) - \left(\frac{V_i'(\eta)}{N} - 2^{-m} \right) \right]^2.$$

Define statistic $T = \sum_{i=1}^{15} Q^{(i)}$, then, for the right key guess, T approximately follows the normal distribution for sufficiently large N and n:

$$T \sim \mathcal{N}\left(15\left(\frac{2B}{N}\right) \cdot l, 15\left(\frac{2B}{N}\right)^2 \cdot 2l \right).$$

Similary, for the wrong key guess, we have:

$$T \sim \mathcal{N}\left(15 \cdot \left(\frac{2B}{N} + 2^{-n+1}\right) \cdot l, 15 \cdot \left(\frac{2B}{N} + 2^{-n+1}\right)^2 \cdot 2l \right)$$

Then, under the KP and DKP cases, the amount of data needed by the distinguisher T are

$$\begin{aligned} N^{KP} &= \frac{2^{n+0.5}\left(q_{1-\alpha_0} + q_{1-\alpha_1}\right)}{\sqrt{15l} - \sqrt{2} \cdot q_{1-\alpha_1}}, \\ N^{DKP} &= \frac{2^{n+0.5}\left(q_{1-\alpha_0} + q_{1-\alpha_1}\right)}{\sqrt{15l} + \sqrt{2} \cdot q_{1-\alpha_0}} \end{aligned} \tag{8}$$

Complexity By setting $\alpha_0 = 2^{-2.7}, \alpha_1 = 2^{-8.5}$, according to Eq. (8), the data complexity $N^{DKP} \approx 2^{60.44}$, the total time complexity is about $2^{119.5}$ 27-round TWINE encryptions, and the memory requirements are about $15 \cdot 2^{61}$ bytes.

Conclution

In this paper, we propose a new statistical related-key distinguisher under the scenario of key difference invariant bias for multidimensional linear cryptanalysis. Compared with the model in Bogdanov et al. (2013), our new model has the following two main advantages: One is that the assumption about statistical independence of

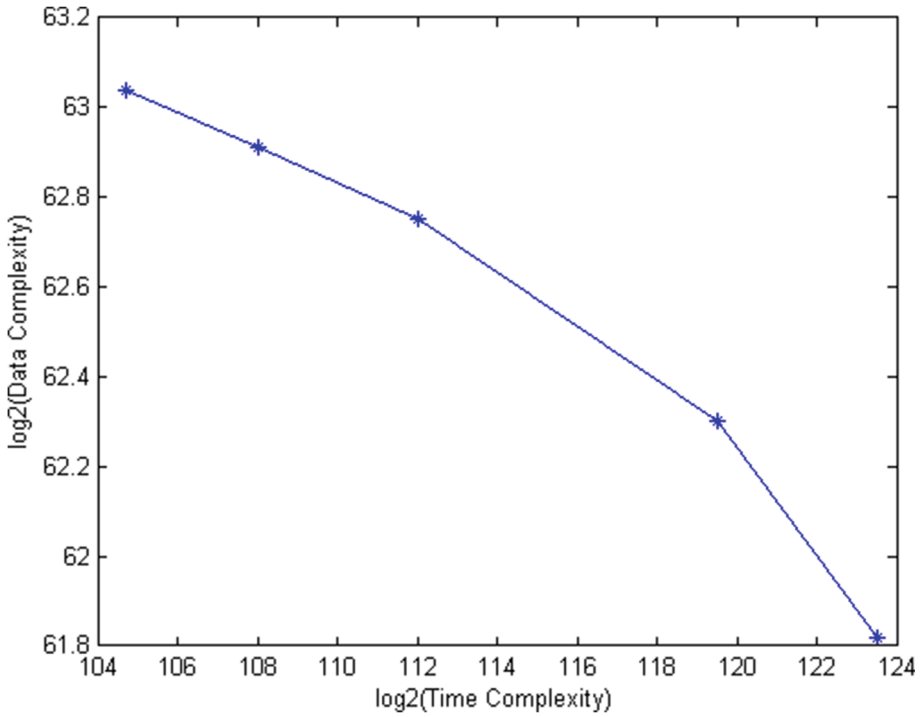

Fig. 4 Data-time tradeoff for the attack on 27-round TWINE-128

linear approximations can be removed, and the other is that our model considers all linear approximations of linear subspace with key difference invariant bias property excluding zero, so our new model can increase the freedom. Moreover partial-compression technique is used to reduce the time complexity. We carefully choose the order of guessing keys and guess each subkey nibble one after another. Besides, we take the key schedule into consideration and use the relations in the related round keys to reduce the number of round keys that need to be guessed. In order to illustrate the new attack model, we evaluate the security of LBlock and TWINE-128 block ciphers against our cryptanalysis technique. For LBlock cipher, based on 16-round key difference invariant bias distinguisher, we present a 25-round key recovery attack. For TWINE-128 cipher, we apply 17-round key difference invariant bias distinguisher to 28-round key recovery attack. We attack more rounds than the best previous cryptanalysis. While previous attack can break 24-round LBlock and 27-round TWINE-128, our attack break the same number of rounds that use the less time complexity and data complexity.

Acknowledgements
Not applicable.

Authors' contributions
The first author conceived the idea of the study and wrote the paper; both authors discussed the results and revised the final manuscript. Both authors read and approved the final manuscript.

Funding
This work was supported by the National Natural Science Foundation of China (Grant No.61379138).

Availability of data and materials
Not applicable.

Declarations

Competing interests
The authors declare that they have no competing interests.

Author details
[1]State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, No. 89 Minzhuang Road, Haidian District, 100093 Beijing, China. [2]School of Cyber Security, University of Chinese Academy of Sciences, No. 19 Yuquan Road, Shijingshan District, 100049 Beijing, China. [3]School of Mathematics and Statistics, Shandong University of Technology, No. 266Xincunxi Road, Zhangdian District, 255000 Zibo, Shandong, China.

Received: 24 March 2021 Accepted: 20 July 2021
Published online: 01 October 2021

References

Blondeau C, Nyberg K (2017) Joint data and key distribution of simple, multiple, and multidimensional linear cryptanalysis test statistic and its impact to data complexity. Des Codes Crypt 82(1-2):319–349

Bogdanov A, Boura C, Rijmen V, Wang M, Wen L, Zhao J (2013) Key difference invariant bias in block ciphers. In: Sako K, Sarkar P (eds). 19th International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg Vol. 8269. pp 357–376

Boztas Ö, Karakoç F, Çoban M (2013) Multidimensional meet-in-the-middle attacks on reduced-round TWINE-128. In: Avoine G, Kara O (eds). Second International Workshop Lightweight Cryptography for Security and Privacy. Springer, Berlin, Heidelberg Vol. 8162. pp 55–67

Cho JY, Hermelin M, Nyberg K (2008) A new technique for multidimensional linear cryptanalysis with applications on reduced round serpent. In: Lee PJ, Cheon JH (eds). 11th International Conference Information Security and Cryptology. Springer, Berlin, Heidelberg Vol. 5461. pp 383–398
Daemen J, Rijmen V (2002) The Design of Rijndael: AES - The Advanced Encryption Standard. Springer, Berlin, Heidelberg
Daemen J, Rijmen V (2007) Probability distributions of correlation and differentials in block ciphers. J Math Cryptol 1(3):221–242
Hermelin M, Cho JY, Nyberg K (2008) Multidimensional linear cryptanalysis of reduced round serpent. In: Mu Y, Susilo W, Seberry J (eds). 13th Australasian Conference Information Security and Privacy. Springer, Berlin, Heidelberg Vol. 5107. pp 203–215
Hermelin M, Cho JY, Nyberg K (2009) Multidimensional extension of Matsui's algorithm 2. In: Dunkelman O (ed). Fast Software Encryption. Springer, Berlin, Heidelberg Vol. 5665. pp 209–227
Kaliski BS, Robshaw MJB (1994) Linear cryptanalysis using multiple approximations. In: Desmedt Y (ed). 14th Annual International Cryptology Conference. Springer, Berlin, Heidelberg Vol. 839. pp 26–39
Liu S, Gong Z, Wang L (2012) Improved related-key differential attacks on reduced-round LBlock. In: Chim TW, Yuen TH (eds). 14th International Conference Information and Communications Security. Springer, Berlin, Heidelberg Vol. 7618. pp 58–69
Matsui M (1993) Linear cryptanalysis method for DES cipher. In: Helleseth T (ed). Advances in Cryptology - EUROCRYPT '93. Springer, Berlin, Heidelberg Vol. 765. pp 386–397
Minier M, Naya-Plasencia M (2012) A related key impossible differential attack against 22 rounds of the lightweight block cipher Iblock. Inf Process Lett 112(16):624–629
Sasaki Y, Wang L (2013) Meet-in-the-middle technique for integral attacks against feistel ciphers. In: Knudsen LR, Wu H (eds). Selected Areas in Cryptography. Springer, Berlin, Heidelberg. pp 234–251
Sasaki Y, Wang L (2013) Comprehensive study of integral analysis on 22-round Iblock. In: Kwon T, Lee M-K, Kwon D (eds). Information Security and Cryptology – ICISC 2012. Springer, Berlin, Heidelberg. pp 156–169
Selçuk AA, Biçak A (2002) On probability of success in linear and differential cryptanalysis. In: Cimato S, Galdi C, Persiano G (eds). Third International Conference Security in Communication Networks. Springer, Berlin, Heidelberg Vol. 2576. pp 174–185
Soleimany H, Nyberg K (2014) Zero-correlation linear cryptanalysis of reduced-round Iblock. Des Codes Crypt 73(2):683–698
Suzaki T, Minematsu K, Morioka S, Kobayashi E (2012) TWINE: A lightweight block cipher for multiple platforms. In: Knudsen LR, Wu H (eds). 19th International Conference Selected Areas in Cryptography. Springer, Berlin, Heidelberg Vol. 7707. pp 339–354
Wang N, Wang X, Jia K (2016) Improved impossible differential attack on reduced-round Iblock. In: Kwon S, Yun A (eds). Information Security and Cryptology - ICISC 2015. Springer International Publishing, Berlin, Heidelberg. pp 136–152
Wang Y, Wu W (2014) Improved multidimensional zero-correlation linear cryptanalysis and applications to Iblock and TWINE. In: Susilo W, Mu Y (eds). 19th Australasian Conference Information Security and Privacy. Springer, Berlin, Heidelberg Vol. 8544. pp 1–16
Wen L, Wang M-Q, Zhao J-Y (2014) Related-key impossible differential attack on reduced-round Iblock. J Comput Sci Technol 29(1):165–176
Wu W, Zhang L (2011) LBlock: A lightweight block cipher. In: López J, Tsudik G (eds). 9th International Conference Applied Cryptography and Network Security Vol. 6715. pp 327–344

Publisher's Note