Key Difference Invariant Bias in Block Ciphers

Andrey Bogdanov, Christina Boura, Vincent Rijmen, Meiqin Wang, Long Wen and Jingyuan Zhao

Asiacrypt 2013, Bangalore, India

December 3, 2013

Linear cryptanalysis

Linear cryptanalysis was introduced by Matsui in 1992.

Based on the notion of linear approximations:

Linear approximation (a, b) of a vectorial function F:

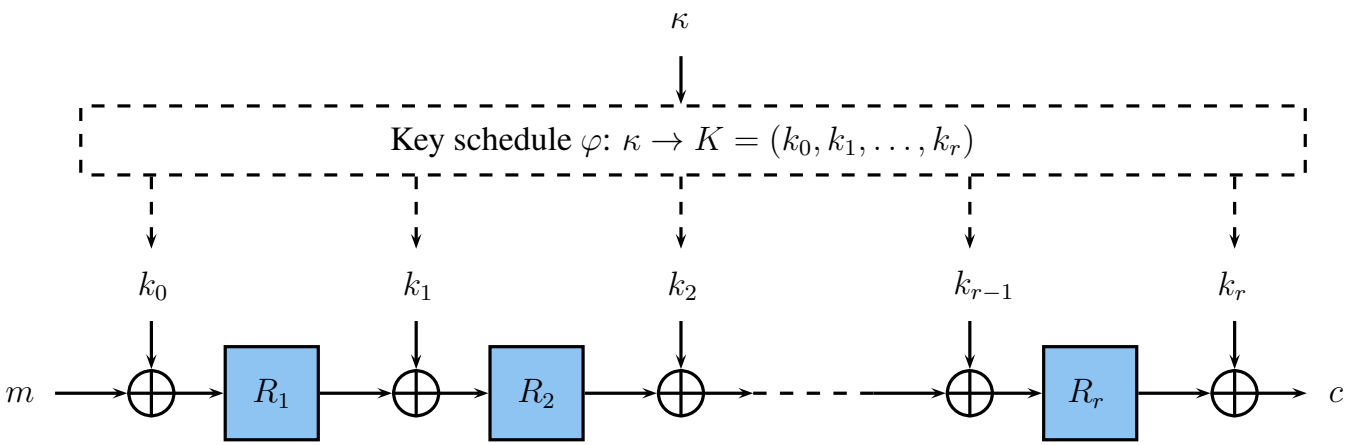
$$b \cdot F(x) \oplus a \cdot x.$$

Bias of (a, b):

$$\varepsilon_{a,b}^{F} = Pr_x\{b \cdot F(x) \oplus a \cdot x\} - \frac{1}{2}$$

Key-alternating block ciphers

Many block ciphers belong to this class: AES, PRESENT,...



- κ: user-supplied key
- K: expanded key
- $k_0, \ldots, k_r$: round subkeys
- n: block size

Linear characteristics and linear hulls

A linear approximation (a, b) of an iterated block cipher is called a

linear hull.

Composed of all the linear approximations θ over individual rounds, with input mask a and output mask b:

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

with $\theta_0 = a$ and $\theta_r = b$.
Bias ε_θ of the linear characteristic θ:

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

Case of key-alternating ciphers

Only the sign of ε_θ depends on the key value.

Proposition [DR02]: For a key-alternating block cipher, the bias ε of a linear hull (a, b) is

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

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

Fundamental Question

How does the bias of a linear hull behave under a change of key?

Our contribution:

The bias of a linear hull can be invariant
under a change of the key.

Towards bias invariance under key difference

- Let a linear hull (a, b)
- Let ε and ε' two biases under two keys κ and κ', with $\kappa \neq \kappa'$.

When $\varepsilon = \varepsilon'$?

- Let $K = \varphi(\kappa)$, $K' = \varphi(\kappa')$ and $K \oplus K' = \Delta$.

Then,

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

Equality holds if

$$d_\theta + \theta \cdot K = d_\theta + \theta \cdot K'.$$

Towards bias invariance under key difference

- Let a linear-hull (a, b)
- Let ε and ε' two biases under two keys κ and κ', with $\kappa \neq \kappa'$.

When $\varepsilon = \varepsilon'$?

- Let $K = \varphi(\kappa)$, $K' = \varphi(\kappa')$ and $K \oplus K' = \Delta$.

Then,

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

Equality holds if

$$\theta \cdot (K \oplus K') = 0.$$

Towards bias invariance under key difference

- Let a linear hull (a, b).
- Let ε and ε' two biases under two keys κ and κ', with $\kappa \neq \kappa'$.

When $\varepsilon = \varepsilon'$?

- Let $K = \varphi(\kappa)$, $K' = \varphi(\kappa')$ and $K \oplus K' = \Delta$.

Then,

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

Equality holds if

$$\theta \cdot \Delta = 0.$$

Key-difference invariant bias for key-alternating ciphers

Theorem

Let (a, b) with $a, b \neq 0$ be a linear hull of a key-alternating block cipher. Let ε and ε' be the biases for the expanded keys K and K' respectively, with $K \oplus K' = \Delta$. Then

$$\varepsilon = \varepsilon' \quad \textit{if} \quad \theta \cdot \Delta = 0$$

for each *linear characteristic θ of the linear hull (a, b) with $\varepsilon_\theta \neq 0$.*

How to construct the property in practice?

Call zero position a bit position $\theta(j), j = 1, \ldots, n(r+1)$ such that

$$\theta(j) = 0 \text{ for all linear approximations } \theta \text{ with } \varepsilon_\theta \neq 0.$$

Choose $\Delta = K \oplus K'$ in a way that $\Delta(j)$ is

- active in some zero-positions and
- non-active in all nonzero-positions.

The example of AES-256 (1)

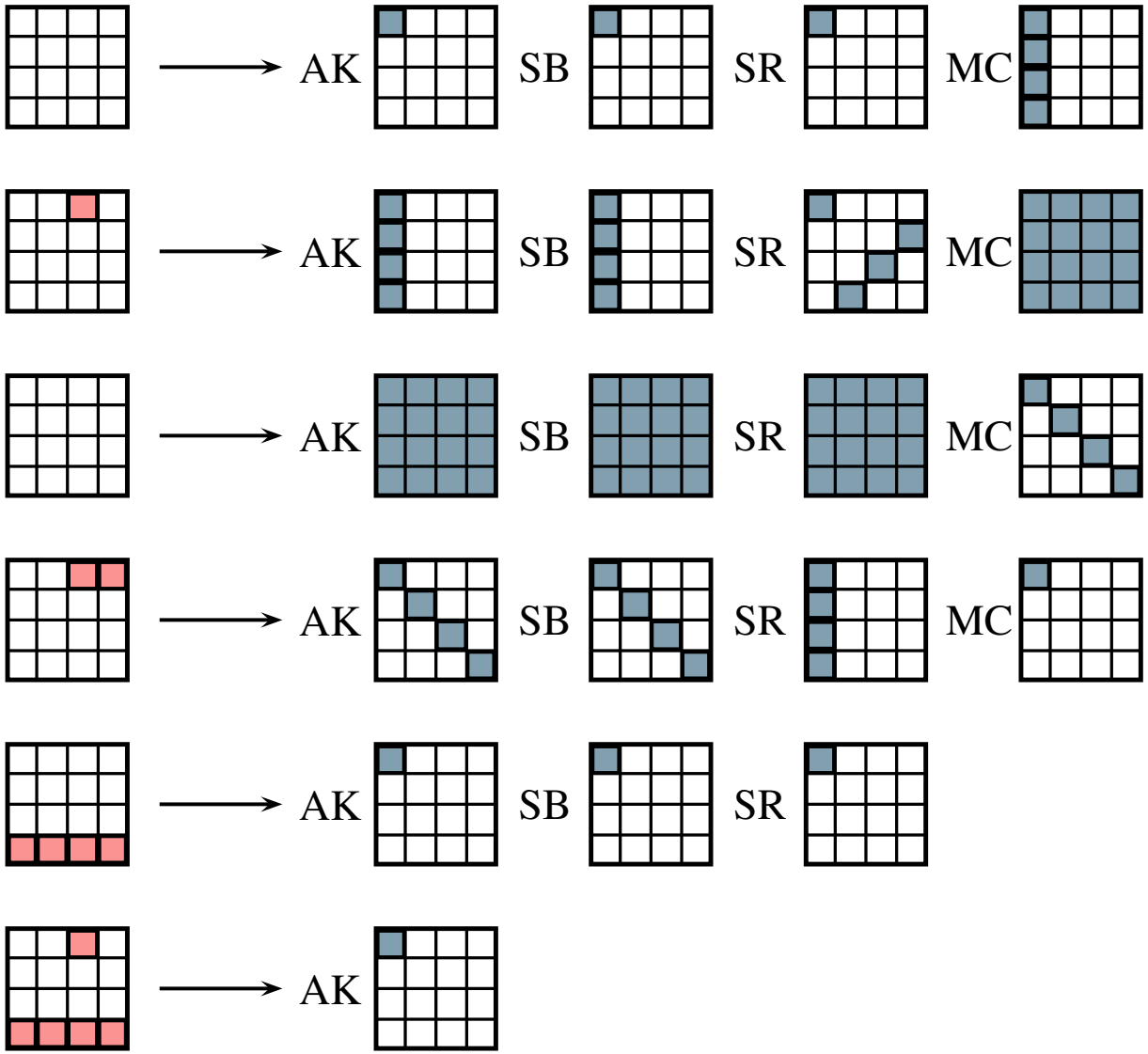
Consider two 32-byte master keys κ and κ' with

$$\kappa \oplus \kappa' = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & \boldsymbol{\delta} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Define the input mask a and the output mask b as:

$$a = \begin{bmatrix} \boldsymbol{\alpha} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \text{ and } b = \begin{bmatrix} \boldsymbol{\beta} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0. \end{bmatrix}$$

The example of AES-256 (2)



Key invariance bias and idealized cipher

For a randomly selected cipher:

$$\Pr\{\varepsilon = \varepsilon' | \kappa \neq \kappa'\} \approx \frac{1}{\sqrt{2\pi}} 2^{\frac{3-n}{2}}, \text{ for } n \geq 5.$$

Distinguisher

Underlying statistic:

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

- N: # of plaintexts/ciphertexts
- ℓ: # linear approximations under (K, K') with $K \oplus K' = \Delta$.
- S_i, S_i': counters.

Two distinct distributions:

- $s \sim \mathcal{N}\left(\frac{\ell}{2N}, \frac{\ell}{2N^2} \right)$ for the right key.
- $s \sim \mathcal{N}\left(\frac{\ell}{2N} + \frac{\ell}{2^{n+1}}, \frac{\ell}{2N^2} + \frac{\ell}{2^{2n+1}} + \frac{\ell}{N2^n} \right)$ for the wrong key.

Data complexity of the distinguisher

Condition for the distinguisher to work:

$$q_{1-\alpha_1}\left(\frac{\ell}{2N^2}+\frac{\ell}{2^{2n+1}}+\frac{\ell}{N2^n}\right)+q_{1-\alpha_0}\frac{\ell}{2N^2}=\frac{\ell}{2^{n+1}}.$$

- $q_{1-\alpha_1}$ and $q_{1-\alpha_0}$: quartiles of standard normal distribution.
- α_0: failure probability of the attack.
- α_1: proportion of surviving keys.

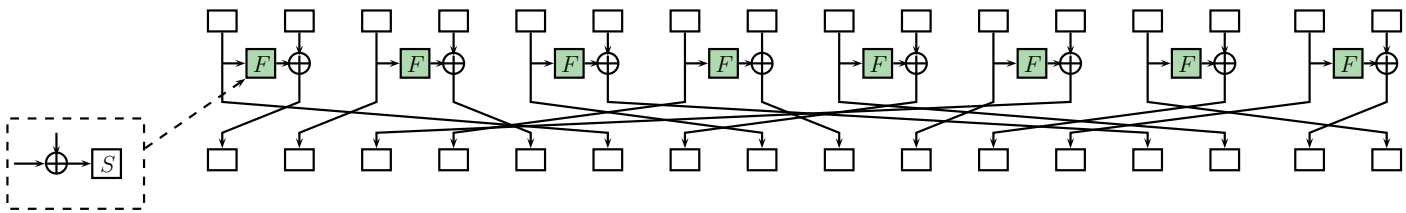
Data complexity:

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

TWINE-128

Proposed by Suzaki, Minematsu, Morioka and Kobayashi [SAC '12].

- 64-bit blocks, 128-bit keys.
- 36 rounds.



Key schedule: Non-linear, nibble-oriented.

Best previous cryptanalysis: 24-round impossible differential attack in the single key model [SMMK '12].

Linear approximations with key difference invariant bias

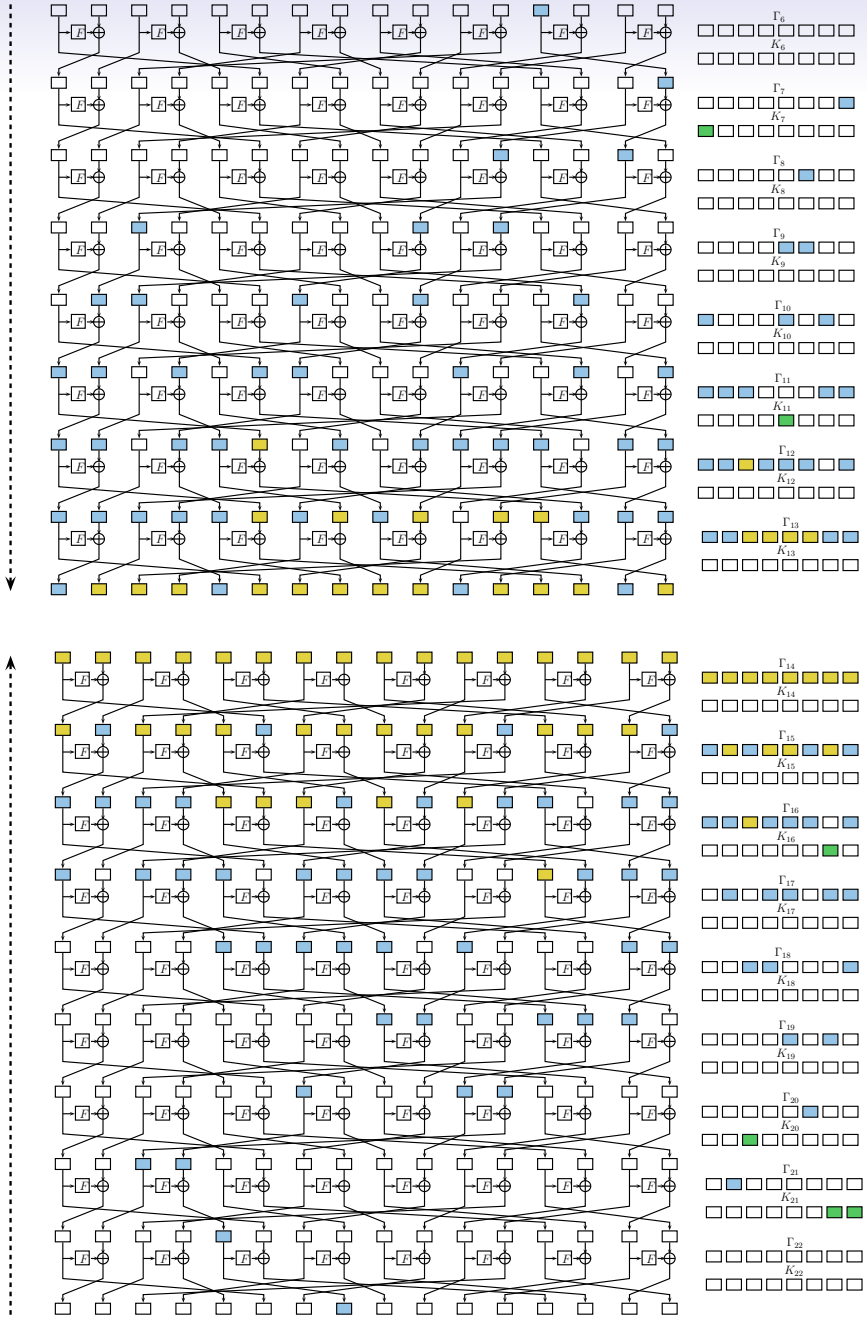
- 17-round linear approximations with key invariant bias under related-key differential paths.
- Input/output masks :

$$(000000000000\alpha 000, 0000000\beta 00000000),$$

with $\alpha, \beta \neq 0$.

$\Rightarrow 15 * 15 \approx 2^{7.81}$ linear approximations.

- Key difference on bits $104 - 107$ of the master key.


Γ_6
K_6
Γ_7
K_7
Γ_8
K_8
Γ_9
K_9
Γ_{10}
K_{10}
Γ_{11}
K_{11}
Γ_{12}
K_{12}
Γ_{13}
K_{13}
Γ_{14}
K_{14}
Γ_{15}
K_{15}
Γ_{16}
K_{16}
Γ_{17}
K_{17}
Γ_{18}
K_{18}
Γ_{19}
K_{19}
Γ_{20}
K_{20}
Γ_{21}
K_{21}
Γ_{22}
K_{22}

Key-recovery for 27-round TWINE

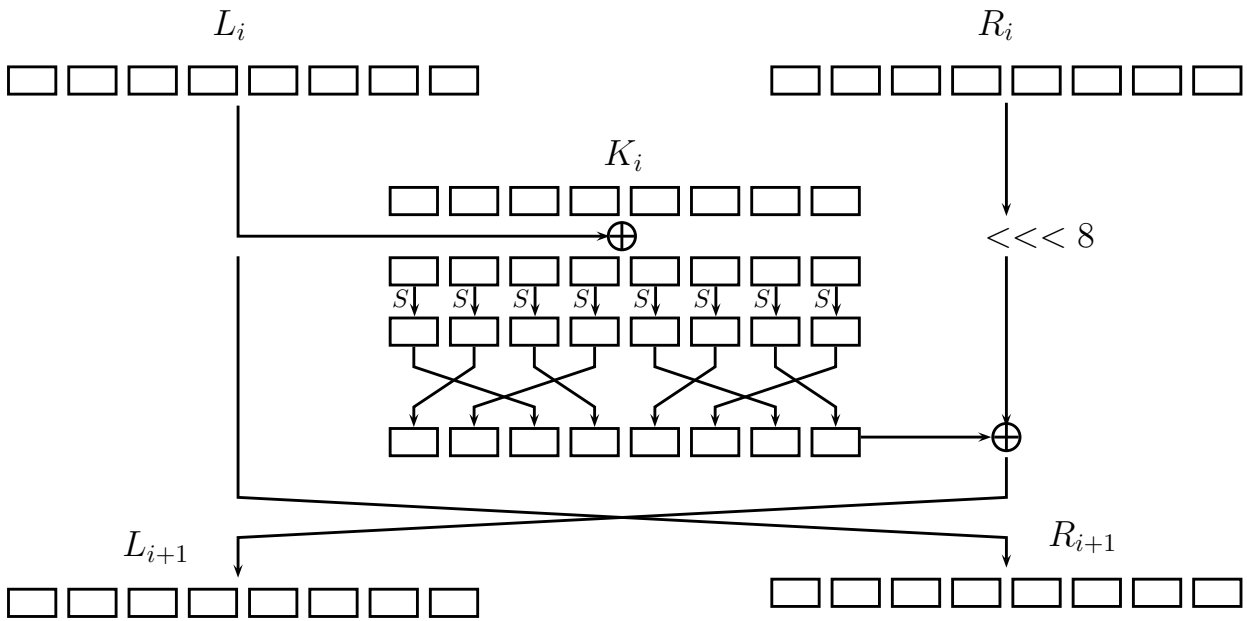
- Append 5 rounds at the beginning and 5 rounds at the end of the characteristic.

α_0	α_1	Data (KP/key)	Time (27R enc.)	Memory (Bytes)
$2^{-2.7}$	$2^{-8.5}$	$2^{62.95}$	$2^{119.5}$	2^{61}
$2^{-2.7}$	$2^{-4.5}$	$2^{62.29}$	$2^{123.5}$	2^{61}

LBlock

Designed by Wu and Zhang, (ACNS 2011).

- 80-bit key and 64-bit state.
- 32 rounds.



LBlock-Summary of Attacks

Model	Attack	#Rounds	Data per key	Time	Memory	Ref.
Single-key	Imp. Diff	20	2^{63} CP	$2^{72.7}$	2^{68}	[WZ11]
	Imp. Diff	21	$2^{62.5}$ CP	$2^{73.7}$	$2^{55.5}$	[LGLL12]
	Imp. Diff	22	2^{58} CP	$2^{79.28}$	2^{76}	[KDH12]
	Integral	20	$2^{63.7}$ CP	$2^{63.7}$	N/A	[WZ11]
	Integral	20	$2^{63.6}$ CP	$2^{39.6}$	2^{35}	[SW12a]
	Integral	22	2^{61} CP	2^{70}	2^{63}	[SW12b]
	Zero-Correlation	22	$2^{62.1}$ KP	$2^{71.27}$	2^{64}	[SN12]
Related-key	Imp. Diff	22	2^{47} RKCP	2^{70}	N/A	[MN12]
	Differential	22	$2^{63.1}$ RKCP	2^{67}	N/A	[LGW12]
	Key Invariant Bias	**24**	$2^{62.29}$ **RKKP**	$2^{74.59}$	2^{61}	**This paper**
	Key Invariant Bias	**24**	$2^{62.95}$ **RKKP**	$2^{70.67}$	2^{61}	**This paper**

LBlock-Summary of Attacks

Model	Attack	#Rounds	Data per key	Time	Memory	Ref.
Single-key	Imp. Diff	20	2^{63} CP	$2^{72.7}$	2^{68}	[WZ11]
	Imp. Diff	21	$2^{62.5}$ CP	$2^{73.7}$	$2^{55.5}$	[LGLL12]
	Imp. Diff	22	2^{58} CP	$2^{79.28}$	2^{76}	[KDH12]
	Integral	20	$2^{63.7}$ CP	$2^{63.7}$	N/A	[WZ11]
	Integral	20	$2^{63.6}$ CP	$2^{39.6}$	2^{35}	[SW12a]
	Integral	22	2^{61} CP	2^{70}	2^{63}	[SW12b]
	Zero-Correlation	22	$2^{62.1}$ KP	$2^{71.27}$	2^{64}	[SN12]
Related-key	Imp. Diff	22	2^{47} RKCP	2^{70}	N/A	[MN12]
	Differential	22	$2^{63.1}$ RKCP	2^{67}	N/A	[LGW12]
	Key Invariant Bias	**24**	$2^{62.29}$ **RKKP**	$2^{74.59}$	2^{61}	**This paper**
	Key Invariant Bias	**24**	$2^{62.95}$ **RKKP**	$2^{70.67}$	2^{61}	**This paper**

- 16-round linear approximations with key invariant bias.

Conclusion

- New fundamental property of key invariant bias in key-alternating ciphers.
- Propose a statistical distinguisher for the property.
- News attacks in the related-key setting against LBlock and TWINE-128 covering more rounds than all previous attacks.

Conclusion

- New fundamental property of key invariant bias in key-alternating ciphers.
- Propose a statistical distinguisher for the property.
- News attacks in the related-key setting against LBlock and TWINE-128 covering more rounds than all previous attacks.

Thanks for you attention!