

Zero Correlation Linear Cryptanalysis with Reduced Data Complexity

Andrey Bogdanov¹ and Meiqin Wang²

¹KU Leuven

²Shandong University

FSE'12, 19 March 2012

Linear Cryptanalysis:

Approximations and Correlation

Action of an n -bit block cipher on plaintext P :

$$C = f_K(P)$$



Input and output linear masks:

$$\chi_P, \chi_C$$



Linear approximation $\chi_P \rightarrow \chi_C$:

$$\chi_P^T P \oplus \chi_C^T C = 0$$

Probability of linear approximation:

$$p_{\chi_P, \chi_C} = \Pr_{P \in \mathbb{F}_2^n} \{ \chi_P^T P \oplus \chi_C^T C = 0 \}$$

Correlation of linear approximation:

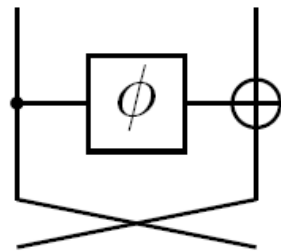
$$c_{\chi_P, \chi_C} = 2p_{\chi_P, \chi_C} - 1$$

Towards Zero-Correlation Cryptanalysis

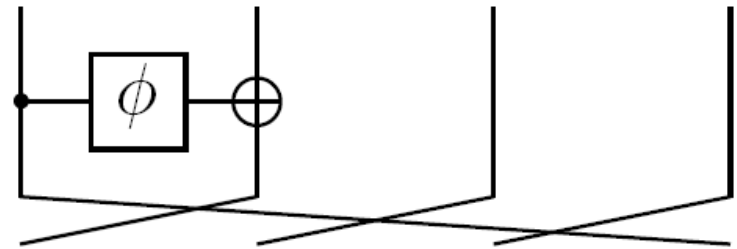
- Standard linear cryptanalysis tries to make use of linear approximations with highly nonzero correlation values
- Zero correlation linear cryptanalysis by B.-Rijmen [BR11] uses linear approximations with correlation exactly zero for all keys
- It is the counterpart of impossible differential cryptanalysis in the domain of linear cryptanalysis
- Cf. [ER10], [CS11], [RN11]

Susceptible Structures [BR11]

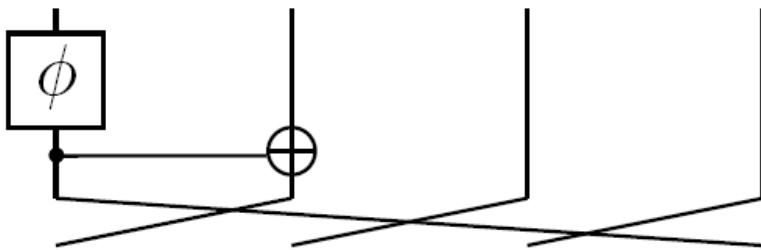
- Zero correlation linear hulls exist in many popular cipher constructions:
 - Feistel networks, round-reduced Rijndael-type ciphers, ...



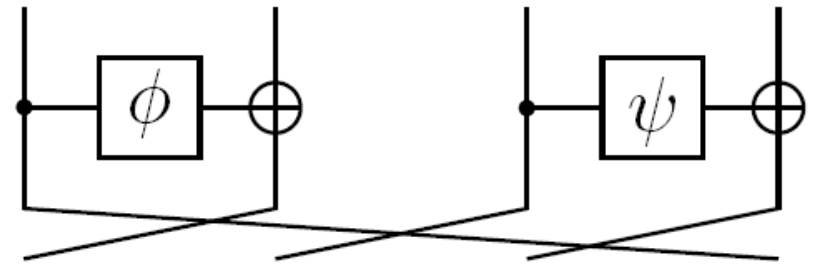
Balanced Feistel



CAST256



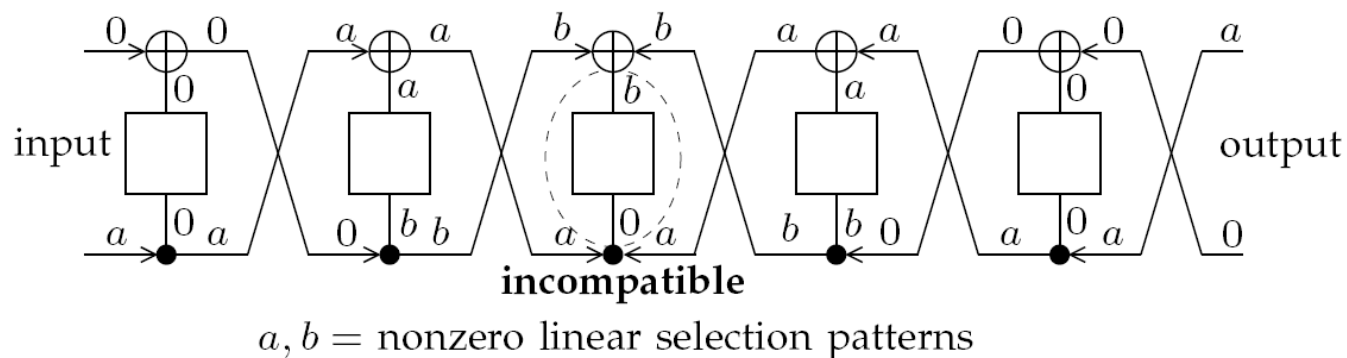
Skipjack (Rule A)



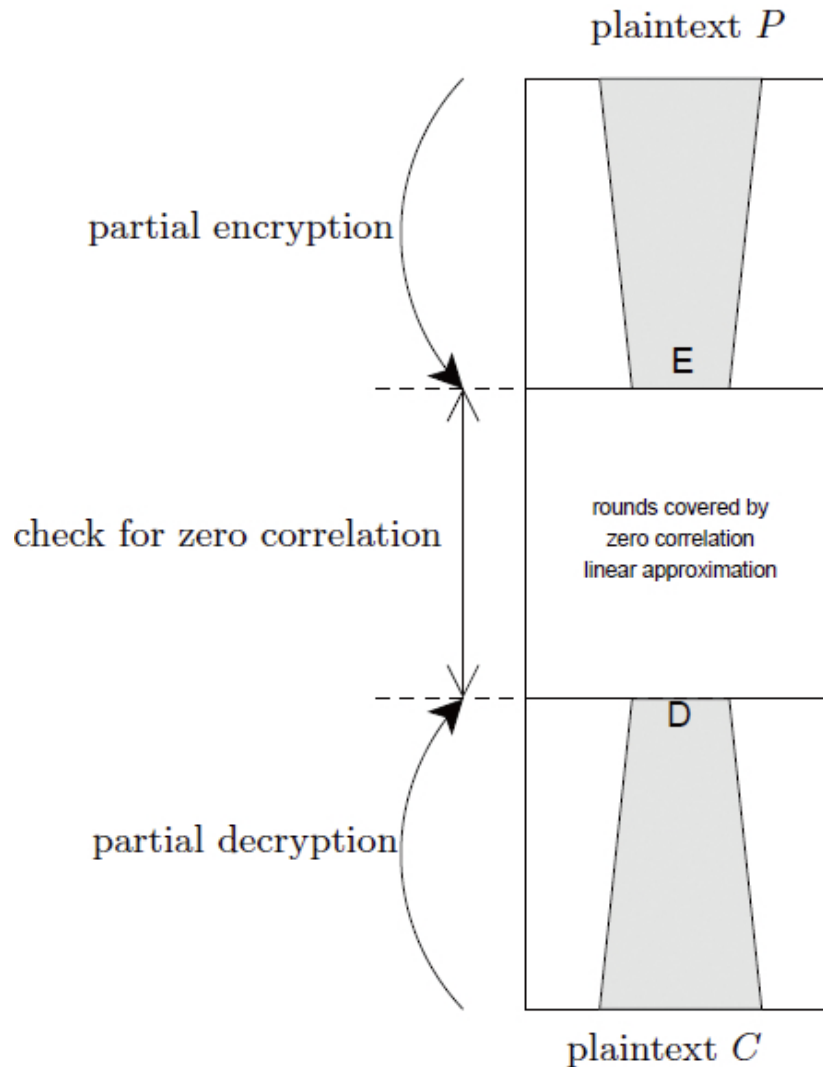
CLEFIA

Zero-Correlation Linear Hulls [BR11]

- 5 rounds of balanced Feistel with bijective functions:



Zero-Correlation Key Recovery



Reduction of Data Complexity I

- High data complexity has been a limitation of zero-correlation approach
- So far zero correlation cryptanalysis did not use the large number of linear approximations available
- A statistical approach addresses the data complexity problem if many zero-correlation approximations are available for each key:
 - for 4R AES: $>2^{20}$ zero-correlation linear hulls
 - for 9R CLEFIA: about 2^{32} zero-correlation linear hulls

Reduction of Data Complexity II

- Underlying statistic:
$$\sum_{i=1}^{\ell} C_i^2 = \sum_{i=1}^{\ell} \left(2\frac{T_i}{N} - 1\right)^2$$
 - N = number of known PC pairs available
 - ℓ = number of zero-correlation linear hulls used
 - T_i = counter for approximation i
- Two distinct distributions:
 - $$\sum_{i=1}^{\ell} \left(2\frac{T_i}{N} - 1\right)^2 \sim \mathcal{N}\left(\frac{\ell}{N} + \frac{\ell}{2^n}, \frac{\sqrt{2\ell}}{N} + \frac{\sqrt{2\ell}}{2^n}\right)$$
 for wrong keys
 - $$\sum_{i=1}^{\ell} \left(2\frac{T_i}{N} - 1\right)^2 \sim \mathcal{N}\left(\frac{\ell}{N}, \frac{\sqrt{2\ell}}{N}\right)$$
 for the right key

Reduction of Data Complexity III

- Condition for the distinguisher to work:

$$\frac{2^{n+0.5}}{N\sqrt{\ell}} (z_{1-\beta_0} + z_{1-\beta_1}) + \frac{z_{1-\beta_1}\sqrt{2}}{\sqrt{\ell}} = 1$$

- $z_{1-\beta_1}$ and $z_{1-\beta_0}$ = quantiles of std. norm. dist.
 - β_0 = failure probability of attack
 - β_1 = proportion of surviving keys
- For instance, for $\beta_0 \approx 0.023$ and $\beta_1 \approx 2^{-50.5}$

$$N \geq \frac{2^{n+3.82}}{\sqrt{\ell}}$$

Applications: TEA and XTEA

attack	#rounds	data	comp. compl.	memory	Pr[success]	reference
TEA						
impossible differential	11	$2^{52.5}$ CP	2^{84}	NA	NA	[MHLLL02]
truncated differential	17	1920 CP	$2^{123.37}$	NA	NA	[HHKCLL04]
impossible differential	17	2^{57} CP	$2^{106.6}$	2^{49}	NA	[CWP11]
zero correlation linear	21	$2^{62.62}$ KP	$2^{121.52}$	negligible	0.846	this paper
zero correlation linear	23	2^{64}	$2^{119.64}$	negligible	1	this paper
XTEA						
impossible differential	14	$2^{62.5}$ CP	2^{85}	NA	NA	[MHLLL02]
truncated differential	23	$2^{20.55}$ CP	$2^{120.65}$	NA	0.969	[HHKCLL04]
meet-in-the-middle	23	18 KP	2^{117}		$1 - 2^{-1025}$	[SMVP11]
impossible differential	23	$2^{62.3}$ CP	$2^{114.9}$	$2^{94.3}$	NA	[CWP11]
impossible differential	23	2^{63}	2^{101} MA + $2^{105.6}$	2^{103}	NA	[CWP11]
zero correlation linear	25	$2^{62.62}$ KP	$2^{124.53}$	2^{30}	0.846	this paper
zero correlation linear	27	2^{64}	$2^{120.71}$	negligible	1	this paper

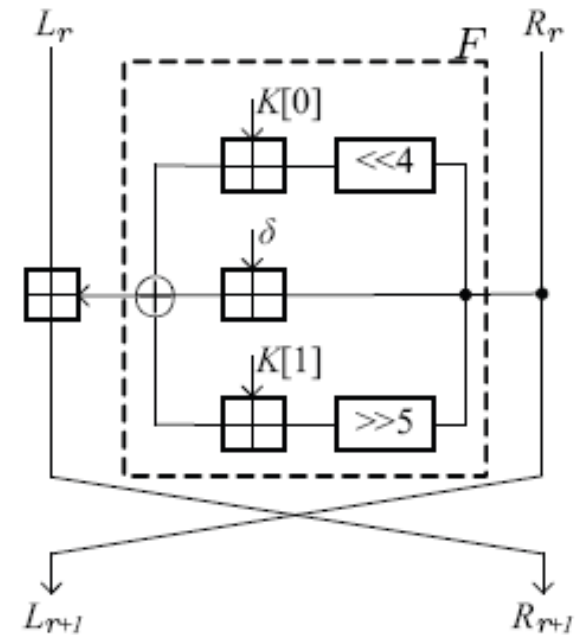
CP: Chosen Plaintexts, KP: Known Plaintexts.

Memory: the number of 32-bit words.

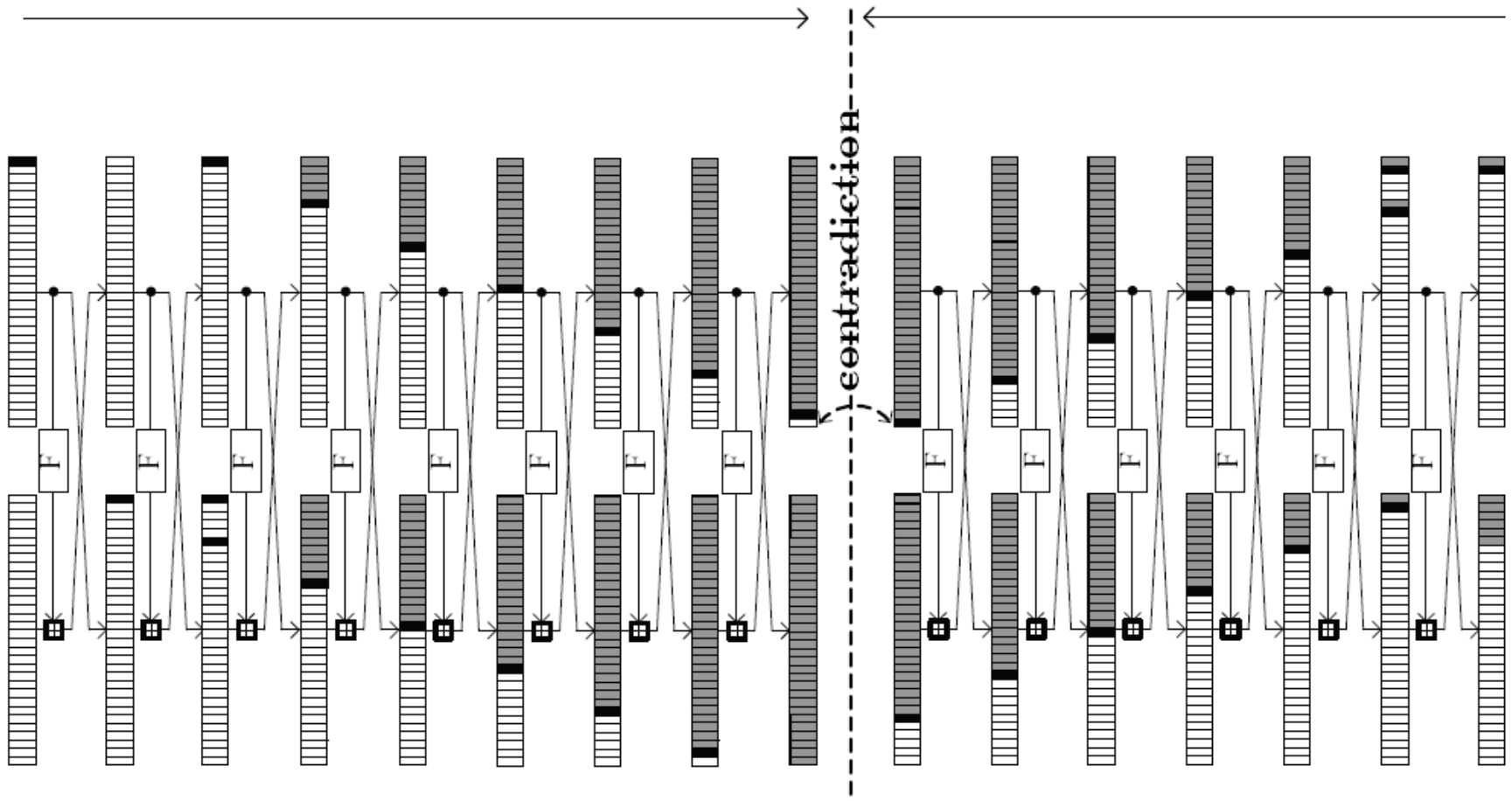
*The effective key length for TEA is 126 bit

TEA

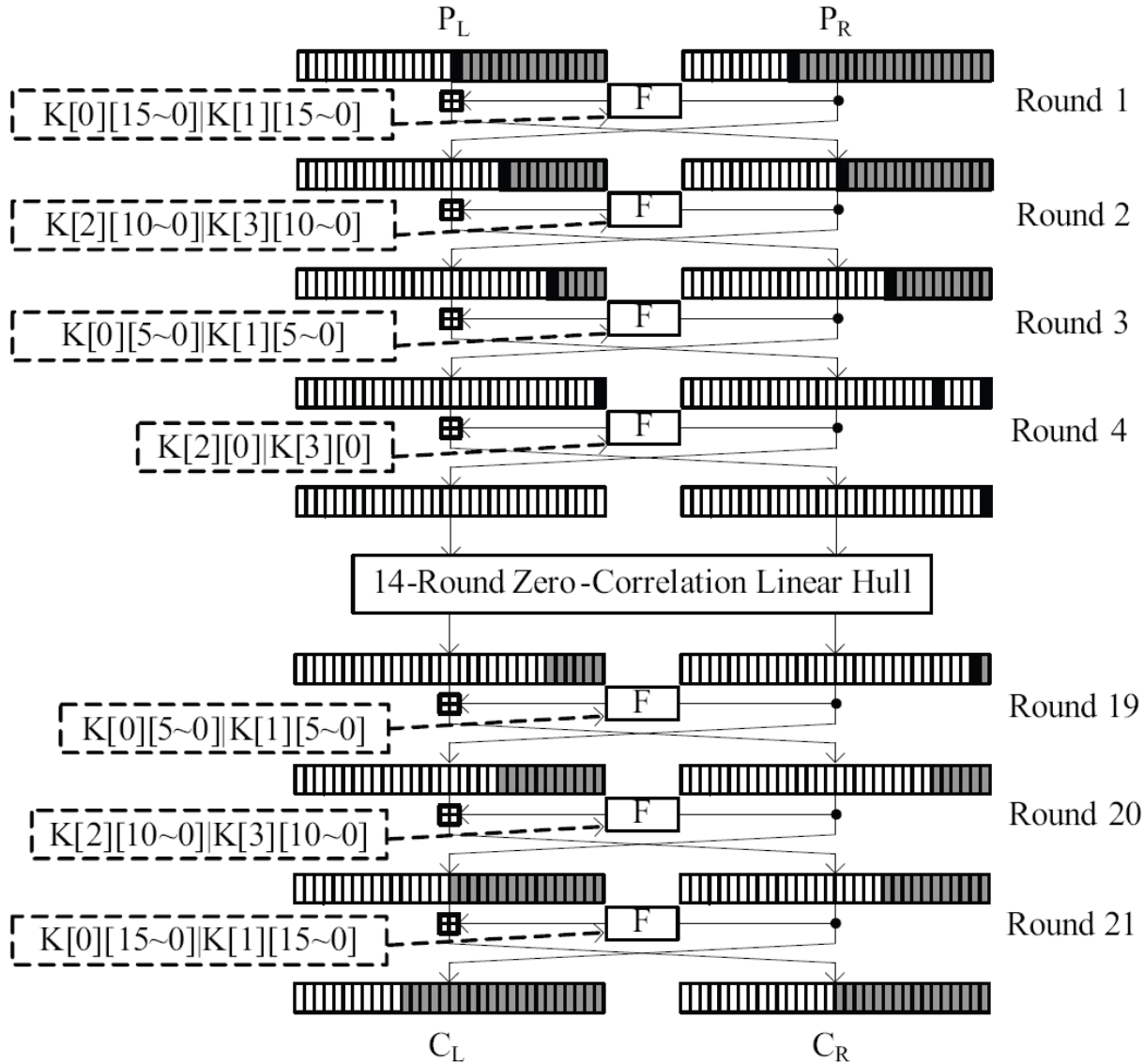
- 64 rounds
- Feistel-type network with ARX
- by Wheeler and Needham at FSE'94
- key length 128 bit
- effective key length 126 bit



14R ZC Linear Hulls for TEA/XTEA



21R ZC Linear Attack on TEA



Summary of Attacks on TEA and XTEA

attack	#rounds	data	comp. compl.	memory	Pr[success]	reference
TEA						
impossible differential	11	$2^{52.5}$ CP	2^{84}	NA	NA	[MHLLL02]
truncated differential	17	1920 CP	$2^{123.37}$	NA	NA	[HHKCLL04]
impossible differential	17	2^{57} CP	$2^{106.6}$	2^{49}	NA	[CWP11]
zero correlation linear	21	$2^{62.62}$ KP	$2^{121.52}$	negligible	0.846	this paper
zero correlation linear	23	2^{64}	$2^{119.64}$	negligible	1	this paper
XTEA						
impossible differential	14	$2^{62.5}$ CP	2^{85}	NA	NA	[MHLLL02]
truncated differential	23	$2^{20.55}$ CP	$2^{120.65}$	NA	0.969	[HHKCLL04]
meet-in-the-middle	23	18 KP	2^{117}		$1 - 2^{-1025}$	[SMVP11]
impossible differential	23	$2^{62.3}$ CP	$2^{114.9}$	$2^{94.3}$	NA	[CWP11]
impossible differential	23	2^{63}	2^{101} MA + $2^{105.6}$	2^{103}	NA	[CWP11]
zero correlation linear	25	$2^{62.62}$ KP	$2^{124.53}$	2^{30}	0.846	this paper
zero correlation linear	27	2^{64}	$2^{120.71}$	negligible	1	this paper

CP: Chosen Plaintexts, KP: Known Plaintexts.

Memory: the number of 32-bit words.

*The effective key length for TEA is 126 bit

Conclusions

- Zero-correlation linear cryptanalysis is the counterpart of impossible differential cryptanalysis in the domain of linear cryptanalysis
- Zero-correlation linear approximations are sometimes longer than impossible differentials
- Data complexity can be limited by using statistics
- Zero correlation can result in faster attacks for some ciphers