Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA

Andrey Bogdanov,
Huizheng Geng, Meiqin Wang, Long Wen,
Baudoin Collard

Technical University of Denmark, Denmark
Shandong University, China
Université Catholique de Louvain, Belgium

Presented by Yu Sasaki
SAC 2013
August 15, 2013

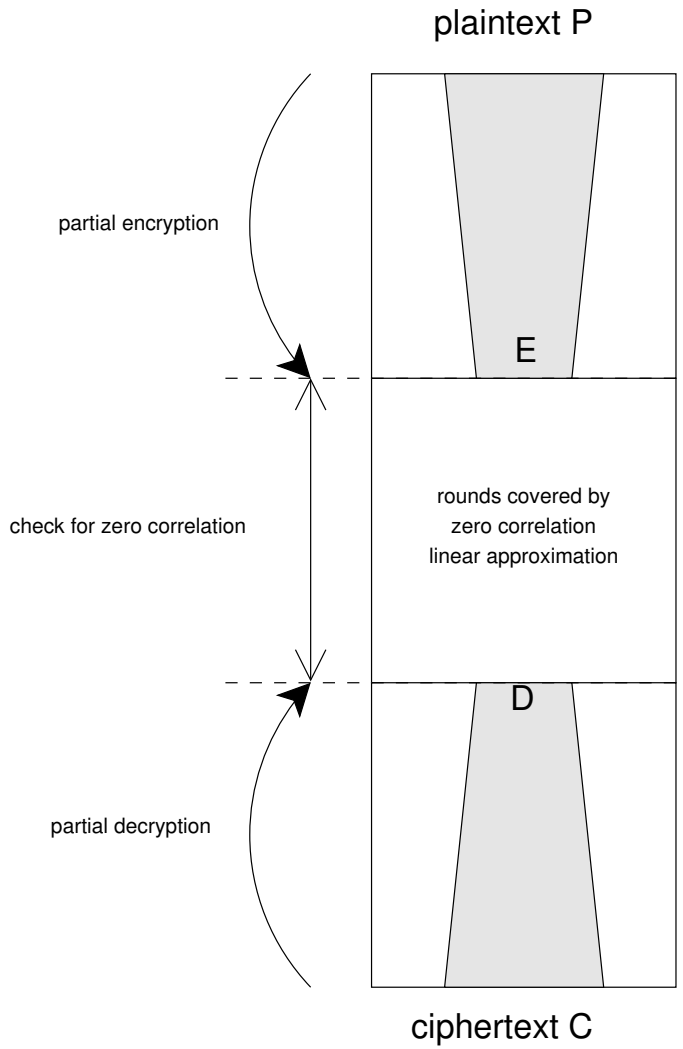
Outline

Zero Correlation Cryptanalysis: Overview

- The idea due to Bogdanov and Rijmen (to appear in DCC, see also IACR eprint report 2011/123):
  - Use linear approximations with probability $p{=}1/2$, or correlation $c = 2p - 1 = 0$
- Bogdanov and Wang in FSE'12:
  - Use multiple approximations of correlation 0
  - Applications to TEA and XTEA (best attack on TEA!)
- Bogdanov, Leander, Nyberg, Wang in Asiacrypt'12:
  - Multidimenstional distinguisher proposed
  - Integrals are a special case of zero correlation
  - Applications to CAST-256 (best attack on CAST-256!)

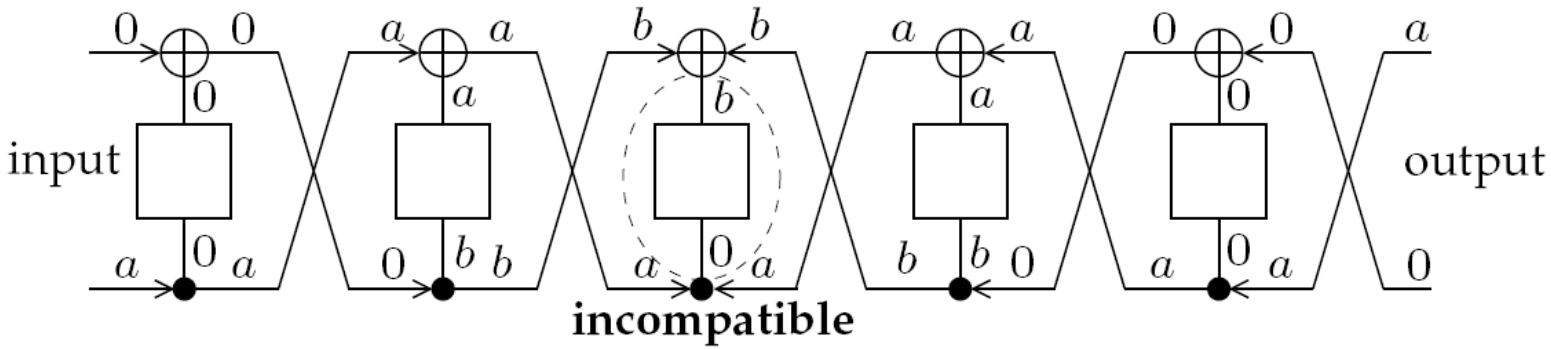
Zero Correlation Cryptanalysis: Overall Procedure

- Identify linear approximations
- For each subkey guess:
  - Partially encrypt/decrypt
  - Check the zero correlation property
  - If correct, output a subkey candidate



Zero Correlation Cryptanalysis: Example

- 5-round zero-correlation for Feistel with balanced F-functions



Motivation

- Time complexity is often an obstacle in attacks on more rounds
- Discrete Fast Fourier Transform for zero correlation cryptanalysis
- $\Rightarrow$ Break stronger ciphers!

Outline

Towards FFT: Algorithm 2 [Matsui'93]:

Linear approximation $\chi_P \rightarrow \chi_D$ for $R-1$ rounds of R-round block cipher, k subkey bits κ, N PT/CT pairs needed

- Decrypt one round for every ciphertext by guessing κ
- Complexity $\mathcal{O}(N2^k)$

Towards FFT: Improved Algorithm 2 [Matsui'94]

- Data counting phase
  1. Initialize an array counter $V[x]$ for 2^k possible values of x
  2. For N texts, take k-bit ciphertext x (output from active S-boxes) and evaluate $\chi_P^T P$
  3. Compute $V[x] += (-1)^{\chi_P^T P}$
- Key counting phase
  1. Guess k-bit subkey κ, decrypt 2^k x to get $\chi_D D$, $M[\kappa, x] = \chi_D D$
  2. For each κ, $T_\kappa = \sum_{x=0}^{2^k-1} M[\kappa, x]\, V[x]$, use T to compute bias ϵ_κ
- Complexity $\mathcal{O}(2^k \cdot 2^k)$ if $N \gg 2^k$

FFT by Collard-Standaert-Quisquater in ICISC'07

- Vector bias through matrix-vector product $M \cdot V$
- Structure of matrix M

$$M(i,j) = parity(S^{-1}(i \oplus j)) \triangleq f(i \oplus j)$$

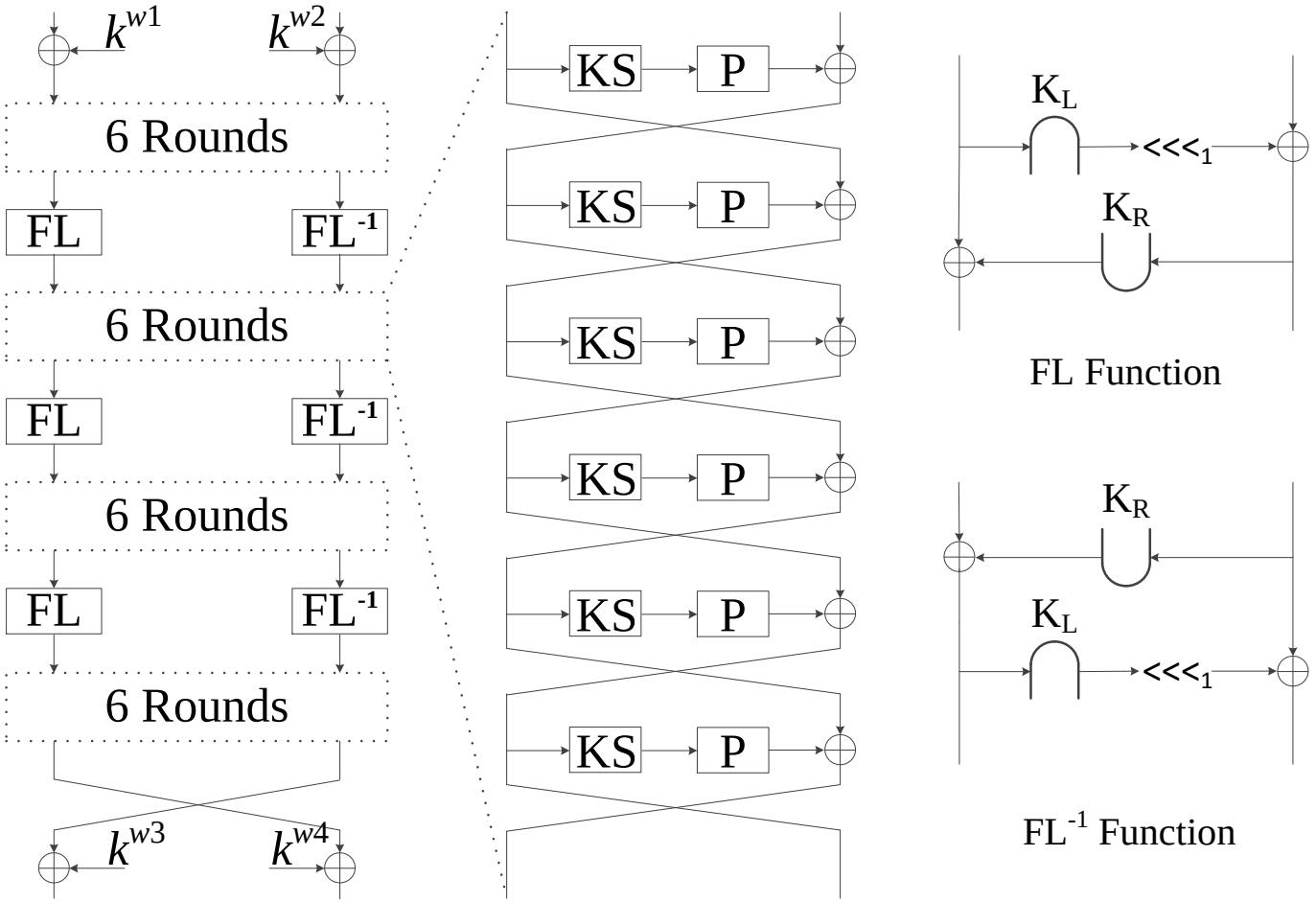
  where $S^{-1}(\cdot)$ represents a partial decryption of the last round
- M has a level-circulant structure $\Rightarrow M \cdot V$ by Fast Walsh-Hadamard Transform in $\mathcal{O}(3k \cdot 2^k)$ complexity
- M is a function of $C \oplus K$ or $P \oplus K$

Outline

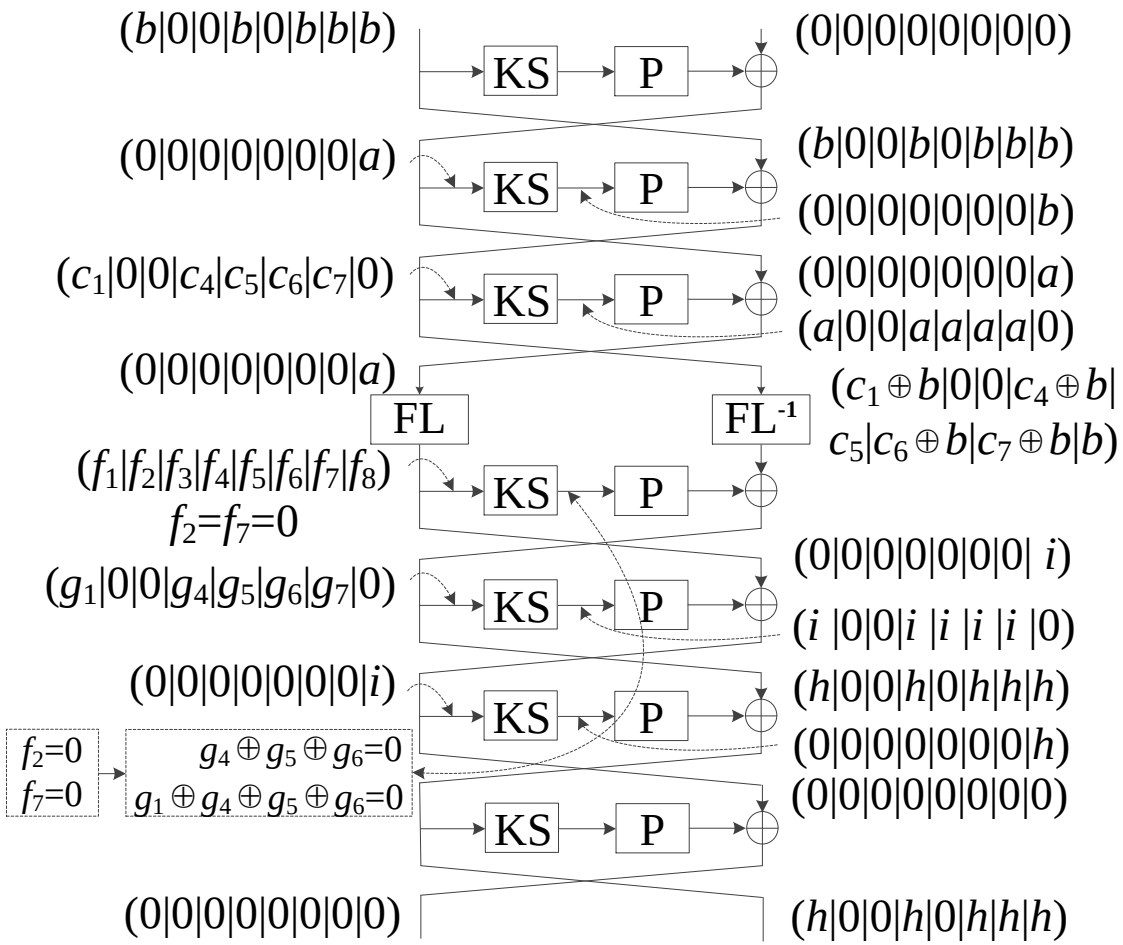
Camellia Block Cipher

- ISO/IEC standard, proposed by NTT and Mitsubishi
- Block size: 128 bits
- Key sizes: 128, 192 or 256 bits
- Round number: 18, 24, 24
- Feistel structure with keyed functions FL/FL^{-1}
- With whitening key at the top and bottom of the cipher

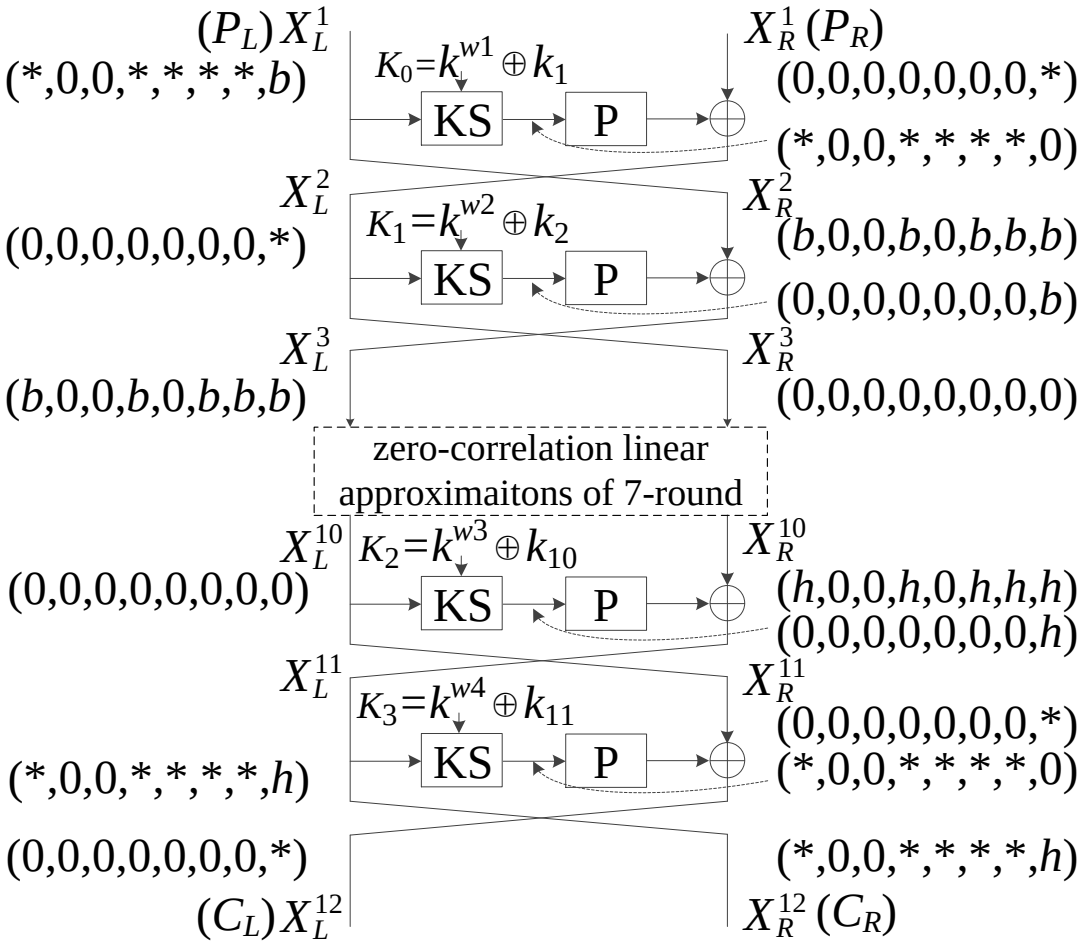
Structure of Camellia



Zero-correlation approximations over 7 rounds



Attack on 11-round Camellia-128 with FFT



Summary of attacks on Camellia-128 and -192

With FL/FL^{-1} and starting from the 1st round

Key Size	R	Attack Type	Data	Time (Encs)	Memory (Bytes)	Ref
128	10	Imp. Diff	$2^{113.8}$CPs	2^{120}	$2^{84.8}$	[LLGWLCL'12]
	11	**ZC FFT**	$\mathbf{2^{125.3}}$**KPs**	$\mathbf{2^{124.8}}$	$\mathbf{2^{112.0}}$	**This paper**
192	10	Imp. Diff	2^{121}CPs	2^{175}	$2^{155.2}$	[CJYW'11]
	10	Imp. Diff	$2^{118.7}$CPs	$2^{130.4}$	2^{132}	[LCW'11]
	11	Imp. Diff	$2^{114.64}$CPs	2^{184}	$2^{141.64}$	[LLGWLCL'12]
	12	**ZC FFT**	$\mathbf{2^{125.7}}$**KPs**	$\mathbf{2^{188.8}}$	$\mathbf{2^{112.0}}$	**This paper**

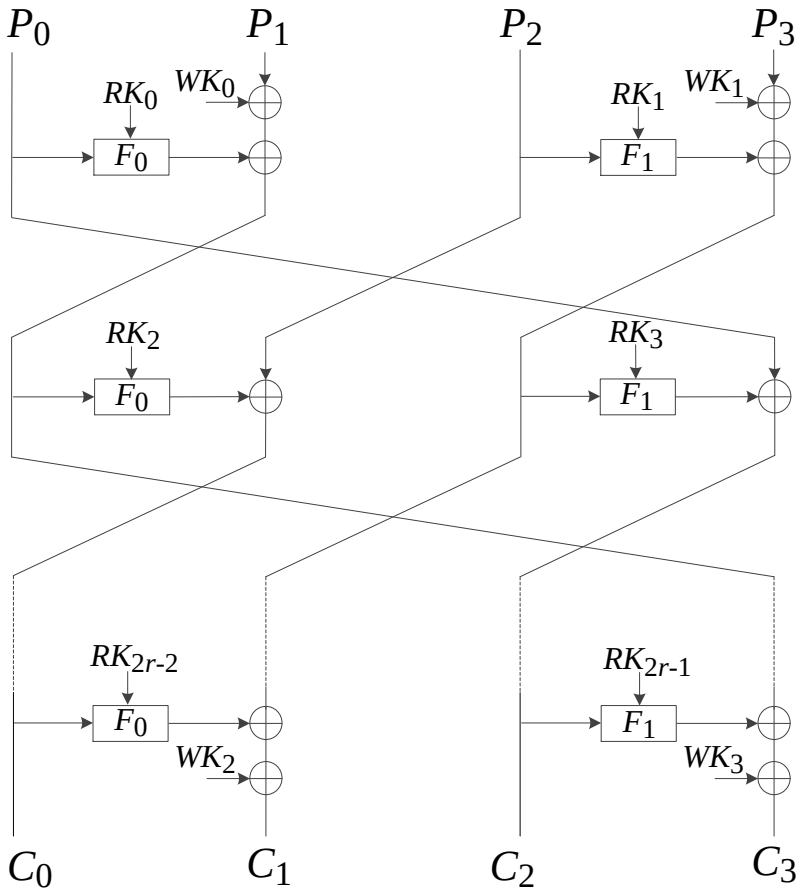
[LLGWLCL'12]: Liu, Li, Gu, Wang, Liu, Chen, and Li in FSE 2012

Outline

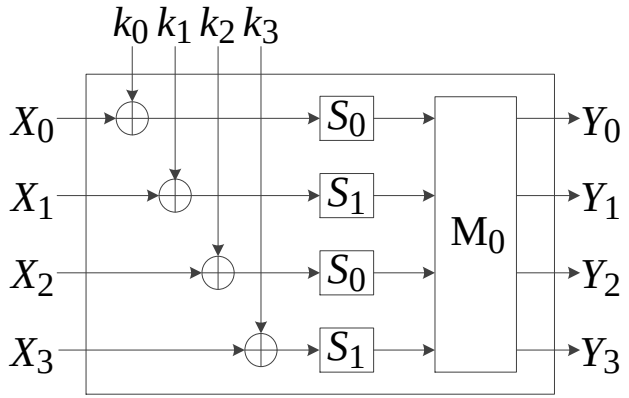
CLEFIA Block Cipher

- ISO/IEC standard for lightweight encryption, proposed by Sony
- Block size: 128 bits
- Key sizes: 128, 192 or 256 bits
- Round number: 18, 22, 26
- 4-Branch Generalized Feistel Structure
- With whitening key at top and bottom

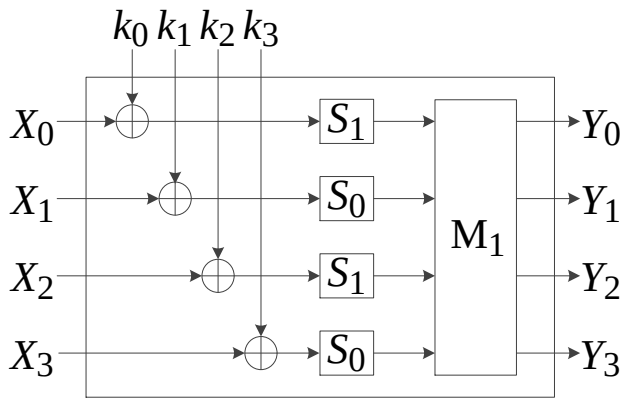
Structure of CLEFIA



(a) Encryption Process of CLEFIA



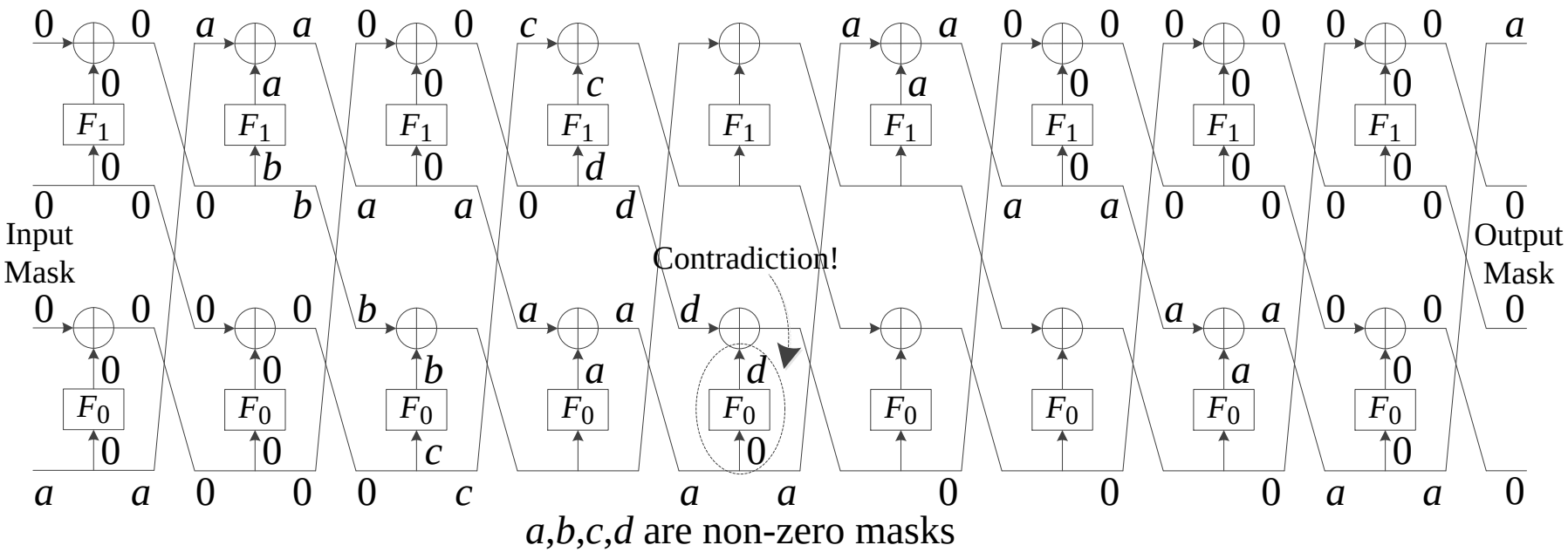
(b) F_0



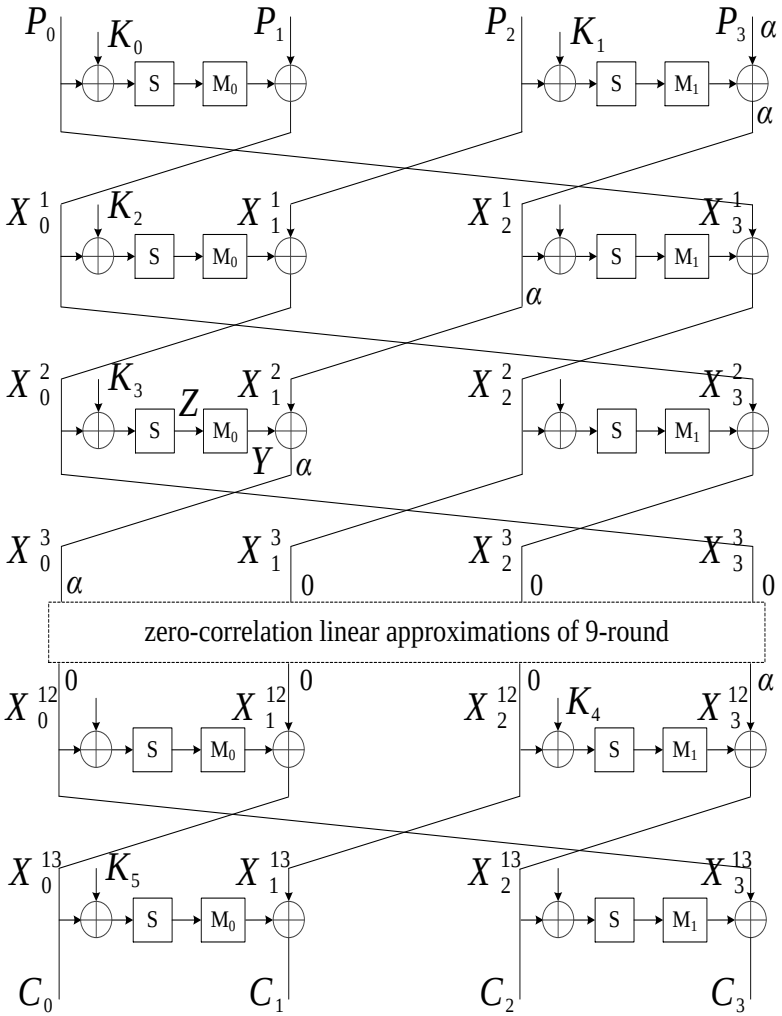
(c) F_1

Zero-correlation approximations over 9 rounds

Bogdanov-Rijmen in DCC



Key recovery attack on 14-round CLEFIA-192



Complexity:

- Data Complexity: $2^{127.5}$ KPs
- Memory Complexity: 2^{115} Bytes
- Time Complexity: $2^{180.2}$ Encs

Summary of Attacks on CLEFIA-192 and -256

Key size	Attack	R	Data	Time (Ens)	Memory (Bytes)	Source
192	Integral	13	2^{113}CPs	$2^{180.5}$	NA	[LWYD'11]
	Impossible	13	$2^{119.8}$CPs	2^{146}	2^{120}	[YEMTTH'08]
	Improbable	14	$2^{127.0}$CPs	$2^{183.2}$	$2^{127.0}$	[Tezcan'10]
	Multidim. ZC	**14**	$\mathbf{2^{127.5}}$**KPs**	$\mathbf{2^{180.2}}$	$\mathbf{2^{115}}$	**This paper**
256	Integral	14	2^{113}CPs	$2^{244.5}$	NA	[LWYD'11]
	Impossible	14	$2^{120.3}$CPs	2^{212}	2^{121}	[YEMTTH'08]
	Improbable	15	$2^{127.4}$CPs	$2^{247.5}$	$2^{127.4}$	[Tezcan'10]
	Multidim. ZC	**15**	$\mathbf{2^{127.5}}$**KPs**	$\mathbf{2^{244.2}}$	$\mathbf{2^{115}}$	**This paper**

Note that the validity of the improbable differential cryptanalysis has been recently challenged by Celine Blondeau:

http://users.ics.aalto.fi/blondeau/PDF/improbable.pdf

Outline

Conclusions

- FFT technique to improve the time complexity of zero correlation attacks
- ZC attacks with FFT 1 more round of Camellia-128 and Camellia-192 with FL/FL^{-1} and starting from the first round
- Multidimensional ZC attacks on the same number of rounds in CLEFIA-192 and CLEFIA-256 with improved memory complexities and similar time and data complexities if improbable differential cryptanalysis turns out correct and on 1 more round otherwise

Thanks!