Zero-Correlation Linear Cryptanalysis of Reduced-Round LBlock

Hadi Soleimany and Kaisa Nyberg

Department of Information and Computer Science,
Aalto University School of Science, Finland

WCC 2013

Outline

Zero-correlation Linear Attack

Matrix Method

Description of LBlock

Zero-correlation Linear Attack on LBlock

Conclusion

Linear attack

Consider a function $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ and let the input of the function be $x \in \mathbb{F}_2^n$. A linear approximation with an input mask u and an output mask v is the following function:

$$x \mapsto u \cdot x \oplus v \cdot f(x).$$

Linear attack

Consider a function $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ and let the input of the function be $x \in \mathbb{F}_2^n$. A linear approximation with an input mask u and an output mask v is the following function:

$$x \mapsto u \cdot x \oplus v \cdot f(x).$$

The linear approximation has probability

$$p(u; v) = Pr(u \cdot x \oplus v \cdot f(x) = 0)$$

Linear attack

Consider a function $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ and let the input of the function be $x \in \mathbb{F}_2^n$. A linear approximation with an input mask u and an output mask v is the following function:

$$x \mapsto u \cdot x \oplus v \cdot f(x).$$

The linear approximation has probability

$$p(u; v) = Pr(u \cdot x \oplus v \cdot f(x) = 0)$$

and its correlation is defined as follows:

$$c_f(u; v) = 2p(u; v) - 1.$$

Extensions of Linear Cryptanalysis

- Exploit several linear approximations with high correlation simultaneously:
  - Multiple linear approximations with the same key mask (Kaliski and Robshaw 1994)
  - Several linear approximations with the same input and output masks (Nyberg 1994)
  - Multiple independent linear approximations (Biryukov et al. 2004)
  - Multidimensional linear approximations (Hermelin et al. 2009)
  - Zero-correlation linear approximations (Bogdanov et al. 2012)

Zero-correlation Linear Cryptanalysis

- It can be seen as the counterpart of impossible differential cryptanalysis.

Zero-correlation Linear Cryptanalysis

- It can be seen as the counterpart of impossible differential cryptanalysis.
- We are interested in linear approximation with correlation (exactly) zero.

Zero-correlation Linear Cryptanalysis

- It can be seen as the counterpart of impossible differential cryptanalysis.
- We are interested in linear approximation with correlation (exactly) zero.
- The original proposal had the disadvantage to require almost the full codebook of data.

Zero-correlation Linear Cryptanalysis

- It can be seen as the counterpart of impossible differential cryptanalysis.
- We are interested in linear approximation with correlation (exactly) zero.
- The original proposal had the disadvantage to require almost the full codebook of data.
- Bogdanov et al. suggested to use several independent zero-correlation linear approximations to reduce data complexity (FSE2012).

Zero-correlation Linear Cryptanalysis

- It can be seen as the counterpart of impossible differential cryptanalysis.
- We are interested in linear approximation with correlation (exactly) zero.
- The original proposal had the disadvantage to require almost the full codebook of data.
- Bogdanov et al. suggested to use several independent zero-correlation linear approximations to reduce data complexity (FSE2012).
- Based on the multidimensional linear attack, a new distinguisher was recently proposed to eliminate the independence assumption (ASIACRYPT2012)

Zero-correlation Linear Cryptanalysis

- It can be seen as the counterpart of impossible differential cryptanalysis.
- We are interested in linear approximation with correlation (exactly) zero.
- The original proposal had the disadvantage to require almost the full codebook of data.
- Bogdanov et al. suggested to use several independent zero-correlation linear approximations to reduce data complexity (FSE2012).
- Based on the multidimensional linear attack, a new distinguisher was recently proposed to eliminate the independence assumption (ASIACRYPT2012)

This Work:

How to use the matrix method as an automatic tool to find zero-correlation approximations

Zero-correlation Linear Attack

Matrix Method

Description of LBlock

Zero-correlation Linear Attack on LBlock

Conclusion

Matrix Method

- A cryptanalytic tool for finding impossible differential characteristics in block ciphers by using the miss-in-the-middle approach systematically (Kim et.al 2003 and 2010).
- The technique involves constructing systematically two minimal truncated differential paths with probability one, one from the first round the block cipher down towards the middle and one from the last round up.
- Scan the midmost round for contradiction.

Matrix Method to Find Zero-correlation Linear Approximation

The state is partitioned into n words (usually of the same length). In the linear approximation, the linear masks applied to the words can be of the following five types:

Matrix Method to Find Zero-correlation Linear Approximation

The state is partitioned into n words (usually of the same length). In the linear approximation, the linear masks applied to the words can be of the following five types:

1. zero mask, denoted by 0,
2. an arbitrary non-zero mask, denoted by $\overline{0}$,
3. non-zero mask with a fixed value a, denoted by a,
4. the exclusive-or of a fixed non-zero mask a and an arbitrary non-zero mask, denoted by $\bar{a}$, that is, any mask different from a,
5. any mask, denoted by $*$.

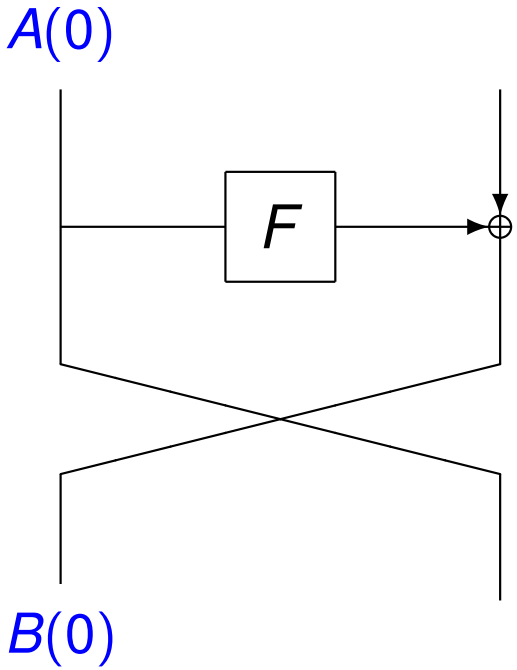
Matrix Method to Find Zero-correlation Linear Approximation

- Describe the encryption round as a $n \times n$ matrix M which shows how a linear mask of each output word is affected by the linear mask of an input word.

Example on Simple Feistel

If linear mask $B(j)$ is not affected by linear mask $A(i)$, the value $M(i,j)$ is set to 0.

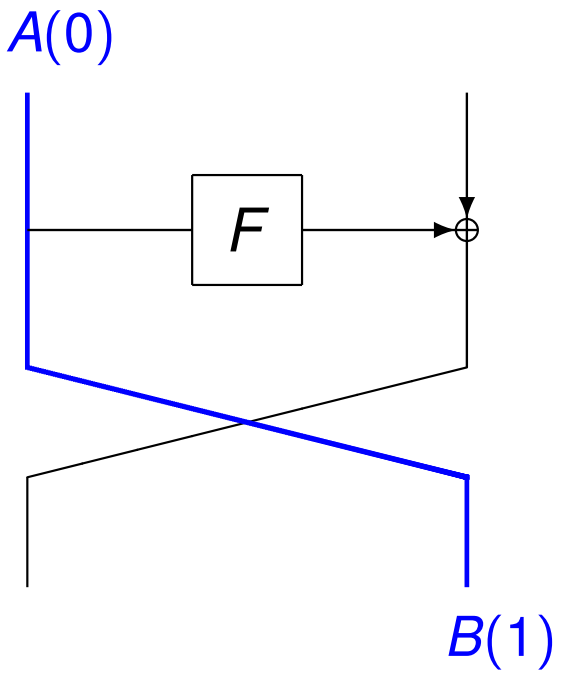
$$M = \begin{pmatrix} 0 & \\ & \end{pmatrix}$$



Example on Simple Feistel

If linear mask $A(i)$ affects linear mask $B(j)$ directly, the value $M(i,j)$ is set to 1.

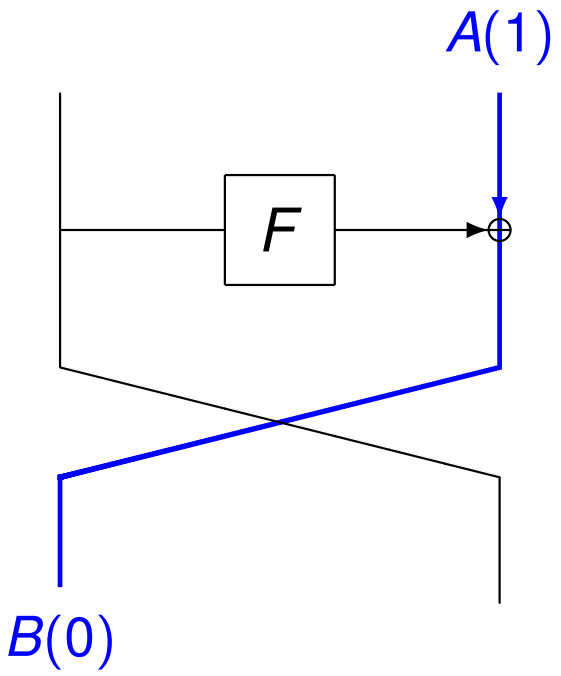
$$M = \begin{pmatrix} 0 & 1 \\ & \end{pmatrix}$$



Example on Simple Feistel

If linear mask $A(i)$ affects linear mask $B(j)$ directly, the value $M(i,j)$ is set to 1.

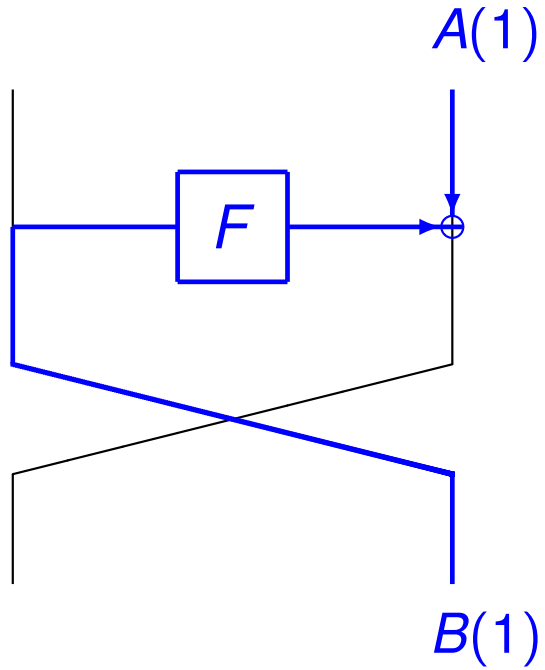
$$M = \begin{pmatrix} 0 & 1 \\ 1 & \end{pmatrix}$$



Example on Simple Feistel

If linear mask $B(j)$ is affected by linear mask $A(i)$ after the round function, the value $M(i,j)$ set to 1_F.

$$M = \begin{pmatrix} 0 & 1 \\ 1 & 1_F \end{pmatrix}$$



Arithmetics Operations

$+$	0	$\bar{0}$	b	$\bar{b}$	$*$
0					
$\bar{0}$					
a					
$\bar{a}$					
$*$					

	0	1	1_F
0			
$\bar{0}$			
a			
$\bar{a}$			
$*$			

Arithmetics Operations

$+$	0	$\bar{0}$	b	$\bar{b}$	$*$
0	0				
$\bar{0}$	$\bar{0}$				
a	a				
$\bar{a}$	$\bar{a}$				
$*$	$*$				

	0	1	1_F
0			
$\bar{0}$			
a			
$\bar{a}$			
$*$			

Arithmetics Operations

$+$	0	$\bar{0}$	b	$\bar{b}$	$*$
0	0	$\bar{0}$			
$\bar{0}$	$\bar{0}$	$*$			
a	a	$\bar{a}$			
$\bar{a}$	$\bar{a}$	$*$			
$*$	$*$	$*$			

	0	1	1_F
0			
$\bar{0}$			
a			
$\bar{a}$			
$*$			

Arithmetics Operations

$+$	0	$\bar{0}$	b	$\bar{b}$	$*$
0	0	$\bar{0}$	b		
$\bar{0}$	$\bar{0}$	$*$	$\bar{b}$		
a	a	$\bar{a}$	$a+b$		
$\bar{a}$	$\bar{a}$	$*$	$\overline{a+b}$		
$*$	$*$	$*$	$*$		

	0	1	1_F
0			
$\bar{0}$			
a			
$\bar{a}$			
$*$			

Arithmetics Operations

$+$	0	$\bar{0}$	b	$\bar{b}$	$*$
0	0	$\bar{0}$	b	$\bar{b}$	
$\bar{0}$	$\bar{0}$	$*$	$\bar{b}$	$*$	
a	a	$\bar{a}$	$a+b$	$\overline{a+b}$	
$\bar{a}$	$\bar{a}$	$*$	$\overline{a+b}$	$*$	
$*$	$*$	$*$	$*$	$*$	

	0	1	1_F
0			
$\bar{0}$			
a			
$\bar{a}$			
$*$			

Arithmetics Operations

$+$	0	$\bar{0}$	b	$\bar{b}$	$*$
0	0	$\bar{0}$	b	$\bar{b}$	$*$
$\bar{0}$	$\bar{0}$	$*$	$\bar{b}$	$*$	$*$
a	a	$\bar{a}$	$a+b$	$\overline{a+b}$	$*$
$\bar{a}$	$\bar{a}$	$*$	$\overline{a+b}$	$*$	$*$
$*$	$*$	$*$	$*$	$*$	$*$

	0	1	1_F
0			
$\bar{0}$			
a			
$\bar{a}$			
$*$			

Arithmetics Operations

$+$	0	$\bar{0}$	b	$\bar{b}$	$*$
0	0	$\bar{0}$	b	$\bar{b}$	$*$
$\bar{0}$	$\bar{0}$	$*$	$\bar{b}$	$*$	$*$
a	a	$\bar{a}$	$a+b$	$\overline{a+b}$	$*$
$\bar{a}$	$\bar{a}$	$*$	$\overline{a+b}$	$*$	$*$
$*$	$*$	$*$	$*$	$*$	$*$

	0	1	1_F
0	0		
$\bar{0}$	0		
a	0		
$\bar{a}$	0		
$*$	0		

For a bijection function F

Arithmetics Operations

$+$	0	$\bar{0}$	b	$\bar{b}$	$*$
0	0	$\bar{0}$	b	$\bar{b}$	$*$
$\bar{0}$	$\bar{0}$	$*$	$\bar{b}$	$*$	$*$
a	a	$\bar{a}$	$a+b$	$\overline{a+b}$	$*$
$\bar{a}$	$\bar{a}$	$*$	$\overline{a+b}$	$*$	$*$
$*$	$*$	$*$	$*$	$*$	$*$

	0	1	1_F
0	0	0	
$\bar{0}$	0	$\bar{0}$	
a	0	a	
$\bar{a}$	0	$\bar{a}$	
$*$	0	$*$	

For a bijection function F

Arithmetics Operations

$+$	0	$\bar{0}$	b	$\bar{b}$	$*$
0	0	$\bar{0}$	b	$\bar{b}$	$*$
$\bar{0}$	$\bar{0}$	$*$	$\bar{b}$	$*$	$*$
a	a	$\bar{a}$	$a+b$	$\overline{a+b}$	$*$
$\bar{a}$	$\bar{a}$	$*$	$\overline{a+b}$	$*$	$*$
$*$	$*$	$*$	$*$	$*$	$*$

	0	1	1_F
0	0	0	0
$\bar{0}$	0	$\bar{0}$	$\bar{0}$
a	0	a	$\bar{0}$
$\bar{a}$	0	$\bar{a}$	$*$
$*$	0	$*$	$*$

For a bijection function F

Zero-correlation Linear Attack

Matrix Method

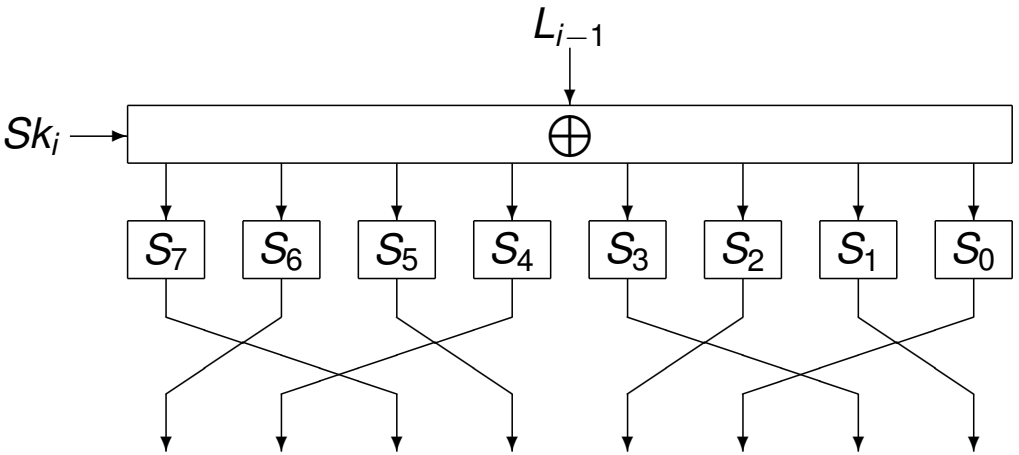
Description of LBlock

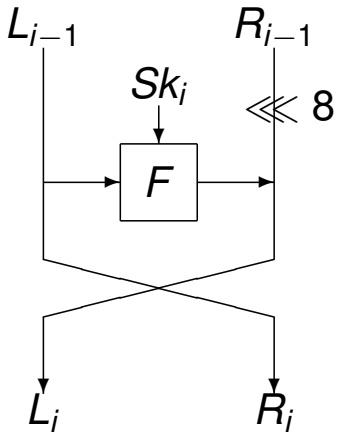
Zero-correlation Linear Attack on LBlock

Conclusion

Description of LBlock

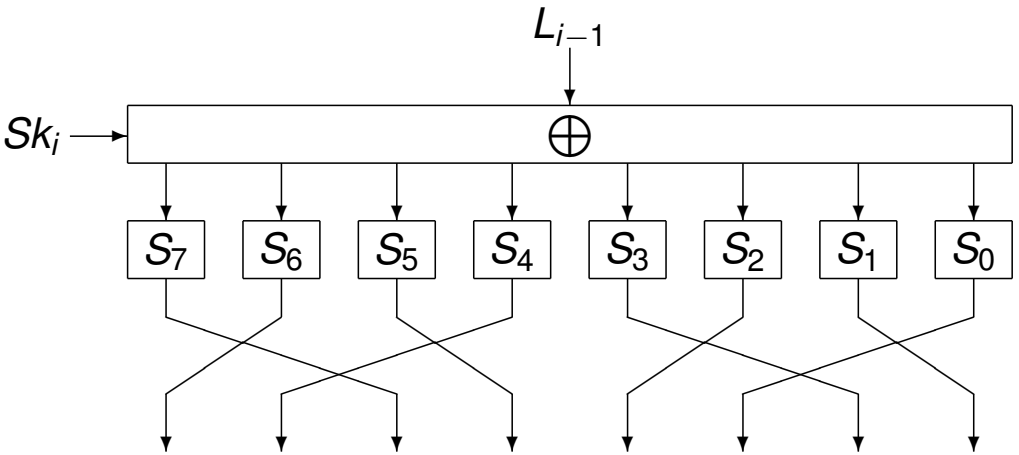
- Lightweight block cipher with semi-Feistel structure
- 32 rounds
- Supports 80 secret key bits and the block size is $b = 64$ bits.

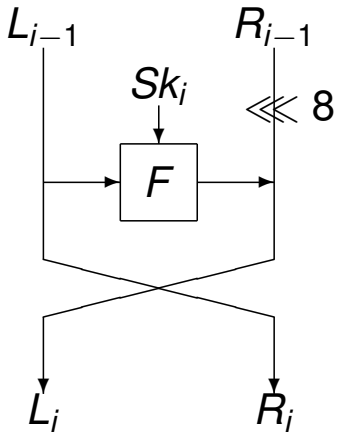




Description of LBlock

- Lightweight block cipher with semi-Feistel structure
- 32 rounds
- Supports 80 secret key bits and the block size is $b = 64$ bits.





- After biclique attacks on LBlock revealed weaknesses in its key schedule, its designers presented a new version of the cipher with a revised key schedule.

Zero-correlation Linear Attack

Matrix Method

Description of LBlock

Zero-correlation Linear Attack on LBlock

Conclusion

Zero-Correlation Linear Approximation for 14-rounds of LBlock

Round	Γ_{L_r}	Γ_{R_r}
0	000a0000	00000000
1		
2		
3		
4		
5		
6		
7		
7		
8		
9		
10		
11		
12		
13		
14		

Zero-Correlation Linear Approximation for 14-rounds of LBlock

Round	Γ_{L_r}	Γ_{R_r}
0	000a0000	00000000
1	00000000	000a0000
2		
3		
4		
5		
6		
7		
7		
8		
9		
10		
11		
12		
13		
14		

Zero-Correlation Linear Approximation for 14-rounds of LBlock

Round	Γ_{L_r}	Γ_{R_r}
0	000a0000	00000000
1	00000000	000a0000
2	0a000000	000$\bar{0}$0000
3		
4		
5		
6		
7		
7		
8		
9		
10		
11		
12		
13		
14		

Zero-Correlation Linear Approximation for 14-rounds of LBlock

Round	Γ_{L_r}	Γ_{R_r}
0	000a0000	00000000
1	00000000	000a0000
2	0a000000	000$\bar{0}$0000
3	0$\bar{0}$000000	0a0$\bar{0}$0000
4		
5		
6		
7		
7		
8		
9		
10		
11		
12		
13		
14		

Zero-Correlation Linear Approximation for 14-rounds of LBlock

Round	Γ_{L_r}	Γ_{R_r}
0	000a0000	00000000
1	00000000	000a0000
2	0a000000	000$\bar{0}$0000
3	0$\bar{0}$000000	0a0$\bar{0}$0000
4	0$\bar{0}$00000a	0$\bar{0}$0$\bar{0}$0$\bar{0}$0
5		
6		
7		
7		
8		
9		
10		
11		
12		
13		
14		

Zero-Correlation Linear Approximation for 14-rounds of LBlock

Round	Γ_{L_r}	Γ_{R_r}
0	000a0000	00000000
1	00000000	000a0000
2	0a000000	000$\bar{0}$0000
3	0$\bar{0}$000000	0a0$\bar{0}$0000
4	0$\bar{0}$00000a	0$\bar{0}$0$\bar{0}$00$\bar{0}$0
5	0$\bar{0}$000$\bar{0}$00$\bar{0}$	0$\bar{0}$00$\bar{0}$0$\bar{0}a$
6		
7		
7		
8		
9		
10		
11		
12		
13		
14		

Zero-Correlation Linear Approximation for 14-rounds of LBlock

Round	Γ_{L_r}	Γ_{R_r}
0	000a0000	00000000
1	00000000	000a0000
2	0a000000	000$\bar{0}$0000
3	0$\bar{0}$000000	0a0$\bar{0}$0000
4	0$\bar{0}$00000a	0$\bar{0}$0$\bar{0}$00$\bar{0}$0
5	0$\bar{0}$00$\bar{0}$000$\bar{0}$	0$\bar{0}$00$\bar{0}$0$\bar{0}$$\bar{0}$$a$
6	0$\bar{0}$0$\bar{0}$$\bar{0}$$a0\bar{0}$	0$\bar{0}$$\bar{0}$$\bar{0}$$\bar{0}$$\bar{0}$$\bar{0}$$*$
7		
7		
8		
9		
10		
11		
12		
13		
14		

Zero-Correlation Linear Approximation for 14-rounds of LBlock

Round	Γ_{L_r}	Γ_{R_r}
0	$000a0000$	00000000
1	00000000	$000a0000$
2	$0a000000$	$000\bar{0}0000$
3	$0\bar{0}000000$	$0a0\bar{0}0000$
4	$0\bar{0}00000a$	$0\bar{0}0\bar{0}00\bar{0}0$
5	$0\bar{0}00\bar{0}00\bar{0}$	$0\bar{0}0\bar{0}0\bar{0}\bar{0}a$
6	$0\bar{0}0\bar{0}\bar{0}a0\bar{0}$	$0\bar{0}\bar{0}\bar{0}\bar{0}\bar{0}\bar{0}*$
7	$\bar{0}\bar{0}\bar{0}\bar{0}\bar{0}*0\bar{0}$	$\bar{0}*\bar{0}*0\bar{a}\bar{0}*$
7		
8		
9		
10		
11		
12		
13		
14		

Zero-Correlation Linear Approximation for 14-rounds of LBlock

Round	Γ_{L_r}	Γ_{R_r}
0	000a0000	00000000
1	00000000	000a0000
2	0a000000	000$\bar{0}$0000
3	0$\bar{0}$000000	0a0$\bar{0}$0000
4	0$\bar{0}$00000a	0$\bar{0}$0$\bar{0}$00$\bar{0}$0
5	0$\bar{0}$000$\bar{0}$00$\bar{0}$	0$\bar{0}$00$\bar{0}$0$\bar{0}$$a$
6	0$\bar{0}$00$\bar{0}$$\bar{0}$$a0\bar{0}$	0$\bar{0}$0$\bar{0}$0$\bar{0}$$\bar{0}$$*$
7	$\bar{0}$$\bar{0}$$\bar{0}$$\bar{0}$$\bar{0}$$*0\bar{0}$	$\bar{0}*\bar{0}*0\bar{a}\bar{0}*$
7		
8		
9		
10		
11		
12		
13		
14	00000000	0b000000

Zero-Correlation Linear Approximation for 14-rounds of LBlock

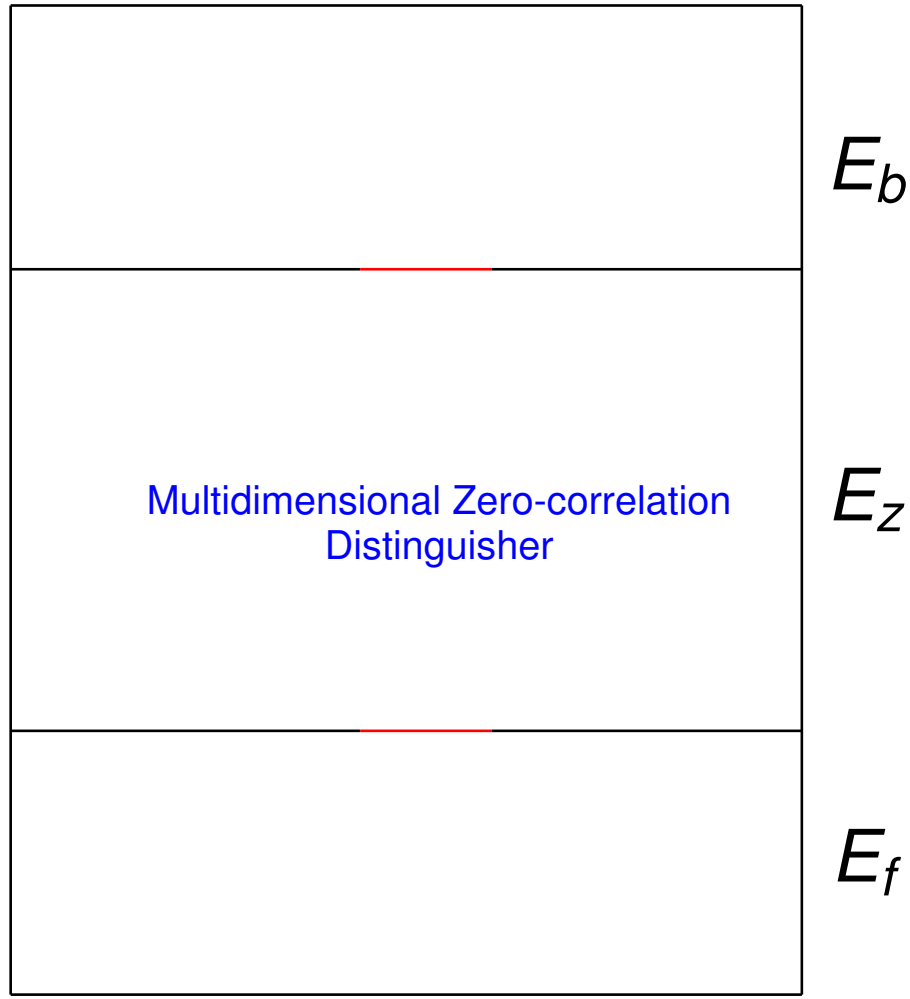
Round	Γ_{L_r}	Γ_{R_r}
0	$000a0000$	00000000
1	00000000	$000a0000$
2	$0a000000$	$000\bar{0}0000$
3	$0\bar{0}000000$	$0a0\bar{0}0000$
4	$0\bar{0}00000a$	$0\bar{0}0\bar{0}00\bar{0}0$
5	$0\bar{0}00\bar{0}00\bar{0}$	$0\bar{0}0\bar{0}0\bar{0}a$
6	$0\bar{0}0\bar{0}\bar{0}a0\bar{0}$	$0\bar{0}\bar{0}\bar{0}\bar{0}\bar{0}\bar{0}*$
7	$\bar{0}\bar{0}\bar{0}\bar{0}\bar{0}*0\bar{0}$	$\bar{0}*\bar{0}*0\bar{a}\bar{0}*$
7	$\bar{0}\bar{0}**\bar{0}\bar{0}*\bar{b}$	$\bar{0}*0\bar{0}\bar{0}\bar{0}\bar{0}\bar{0}$
8	$0\bar{0}\bar{0}\bar{0}\bar{0}\bar{0}\bar{0}*$	$0\bar{0}\bar{0}\bar{0}000\bar{b}$
9	$\bar{0}\bar{0}000\bar{b}0\bar{0}$	$00\bar{0}0\bar{0}000\bar{0}$
10	$\bar{0}0\bar{0}000\bar{0}00$	$0000\bar{b}00$
11	$00\bar{b}0000$	$0000\bar{0}00$
12	$000\bar{0}0000$	$000b0000$
13	$0b000000$	00000000
14	00000000	$0b000000$

Zero-Correlation Linear Approximation for 14-rounds of LBlock

If the input mask would be exactly one non zero nibble in L_r and the output mask after 14 rounds would be one non zero nibble in R_{r+14}, then the linear approximation has correlation zero.

Key Recovery

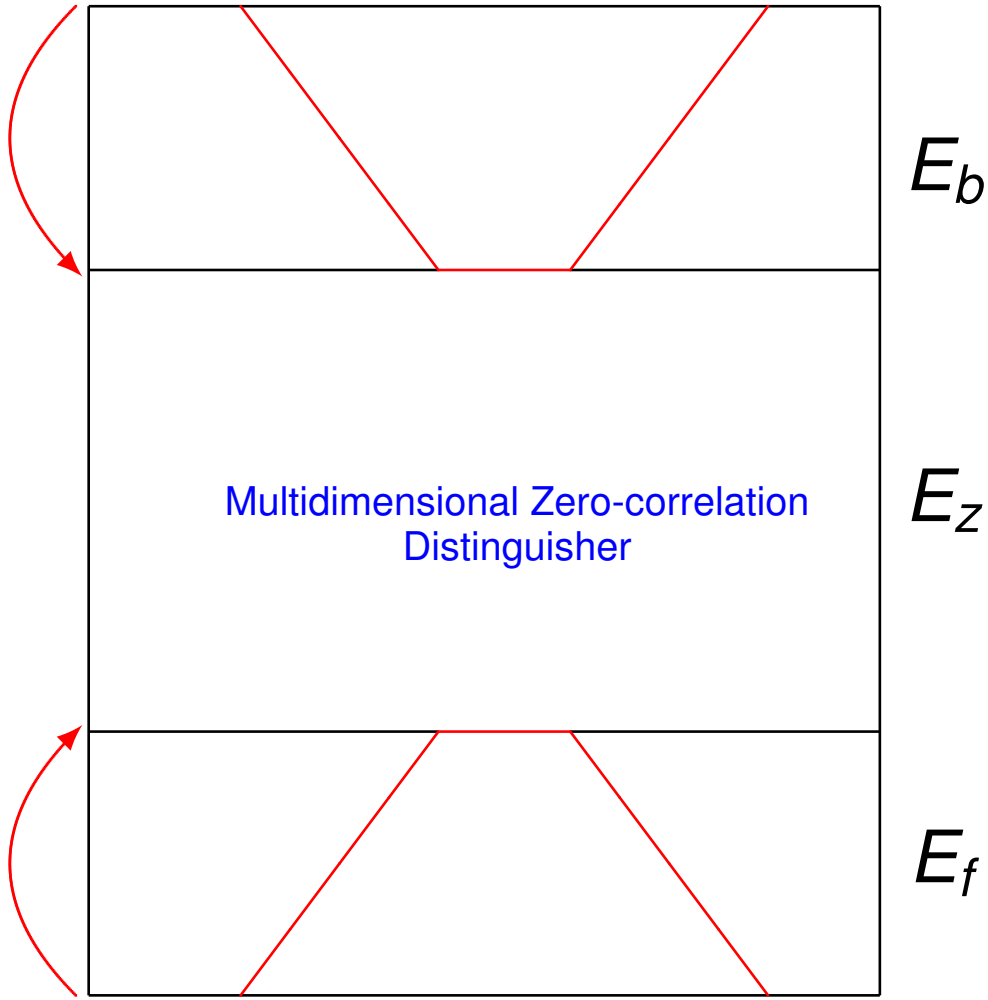
- Split n-bit block cipher E as a cascade $E = E_f \circ E_z \circ E_b$.
- Assume there exists m independent linear approximations for E_z such that all $\ell = 2^m - 1$ nonzero linear combinations of them have correlation zero.



Key Recovery

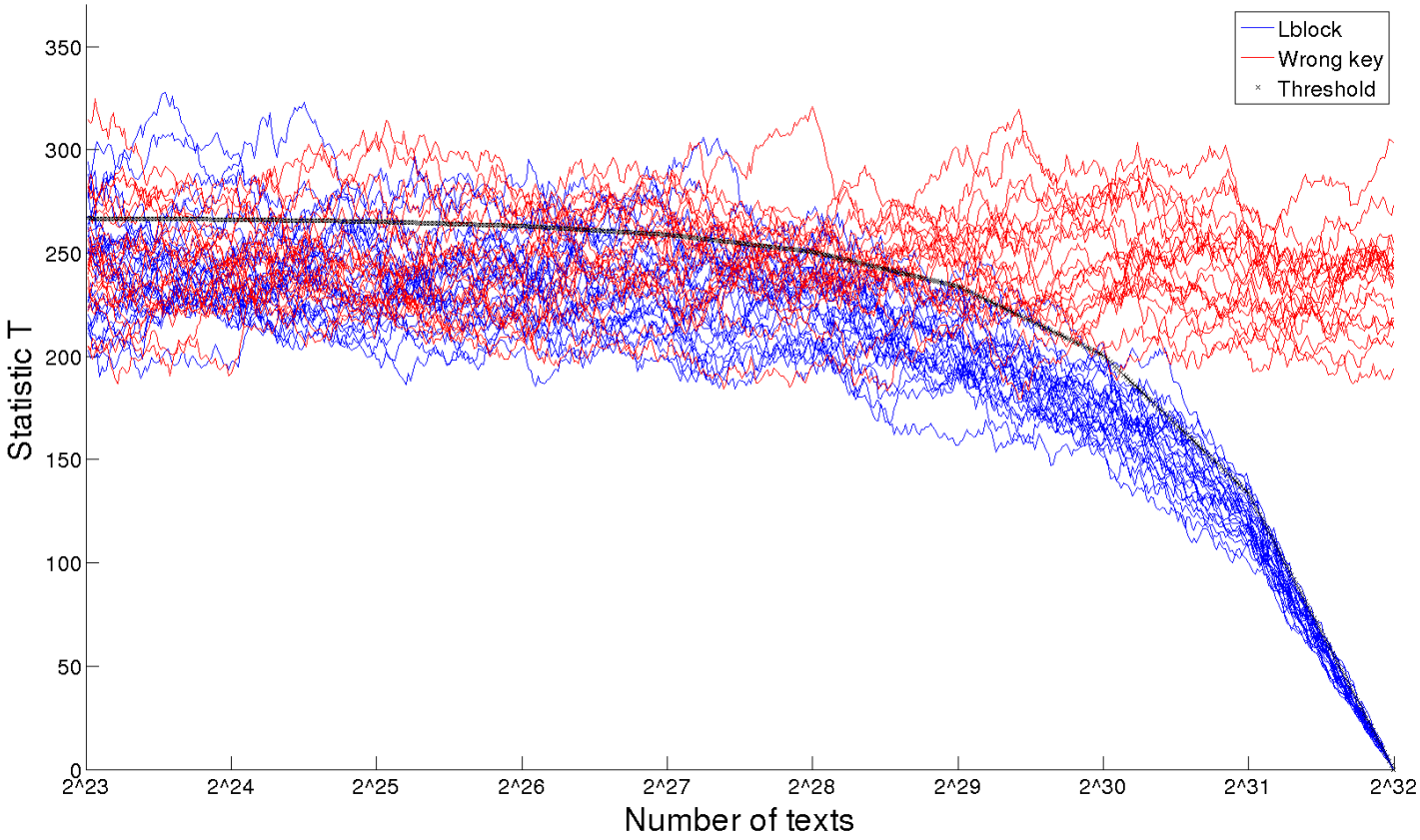
- For each key candidate, encrypt the plaintexts for E_b and decrypt the ciphertexts for E_f.
- For each of $i \in \mathbb{F}_2^m$ allocate a counter T_i and computes the number of times which the corresponding data value is equal to i.
- Compute the statistic T value:

$$T = \sum_{i=0}^{2^m-1} \frac{(T_i - N2^{-m})^2}{N2^{-m}(1-2^{-m})}.$$



Simulations for a Small Variant of LBlock

- Similar multidimensional zero-correlation distinguisher for 10 rounds of the small variant of LBlock cipher ($n = 32, m = 8$).



Summary of the Attacks on LBlock

Attack	Rounds	Data	Time	Memory (Bytes)	Source
Integral Attack (CP)	20	$2^{63.7}$	$2^{63.7}$	Not Specified	WZ11
Impossible Differential (CP)	20	2^{63}	$2^{72.7}$	2^{60}	WZ11
Impossible Differential† (CP)	21	$2^{62.5}$	$2^{73.7}$	2^{64}	LG12
Impossible Differential† (CP)	21	2^{63}	$2^{69.5}$	2^{68}	KD12
Impossible Differential† (CP)	22	2^{58}	$2^{79.28}$	2^{68}	KD12
Zero Correlation (DKP)	22	2^{64}	$2^{70.54}$	2^{64}	This paper
Zero Correlation (DKP)	22	$2^{62.1}$	$2^{71.27}$	2^{64}	This paper
Zero Correlation (DKP)	22	2^{60}	2^{79}	2^{64}	This paper
Biclique (KP)†	Full	2^{52}	$2^{78.4}$	Negligible	WWZ12

Zero-correlation Linear Attack

Matrix Method

Description of LBlock

Zero-correlation Linear Attack on LBlock

Conclusion

Conclusion

- Show how to use the matrix method to establish zero-correlation linear approximations automatically.
- Obtain several zero-correlation linear approximations over 14 rounds of LBlock.
- Present an attack on 22 rounds of LBlock independent from key schedule.
- Implement the attack for an small variant of LBlock and run simulations to experimentally validate the statistical model of zero-correlation linear cryptanalysis.

Thanks for your attention!