On the Construction of Partial Difference Distribution Tables for ARX Ciphers

A. Biryukov V. Velichkov

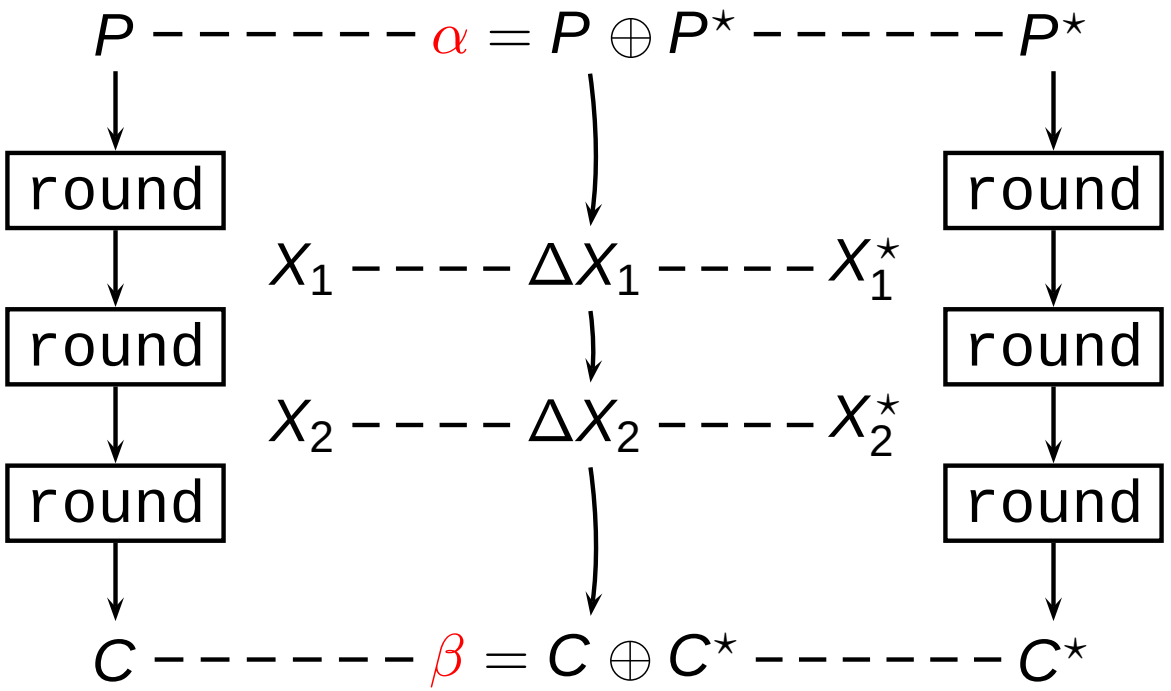
LACS, Luxembourg University

ESC 2013, January 14-18,
Mondorf-les-Bains, Luxembourg

Outline

Outline

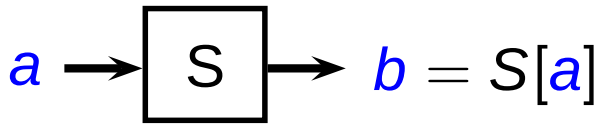
Differential Cryptanalysis [Biham,Shamir,1991]



$$\mathrm{DP}(\alpha \to \beta) = ?$$

Substitution Box (S-box): a Source of Non-linearity

- An example 4-bit S-box:



a	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[a]$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

- The differential probability of an S-box:

$$\mathrm{DP}(\alpha \to \beta) = \frac{\#\{a : S[a \oplus \alpha] \oplus S[a] = \beta\}}{\#\{a\}} \ .$$

- S-boxes make differential cryptanalysis harder

Difference Distribution Table (DDT) for 4-bit S-box

α, β	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
1	.	.	.	2	.	.	.	2	.	2	4	.	4	2	.	.
2	.	.	.	2	.	6	2	2	.	2	.	.	.	.	2	.
3	.	.	2	.	2	.	.	.	.	4	2	.	2	.	.	4
4	.	.	.	2	.	.	6	.	.	2	.	4	2	.	.	.
5	.	4	.	.	.	2	2	.	.	.	4	.	2	.	.	2
6	.	.	.	4	.	4	.	.	.	.	.	.	2	2	2	2
7	.	.	2	2	2	.	2	.	.	2	2	.	.	.	.	4
8	.	.	.	.	.	.	2	2	.	.	.	4	.	4	2	2
9	.	2	.	.	2	.	.	4	2	.	2	2	2	.	.	.
A	.	2	2	.	.	.	.	.	6	.	.	2	.	.	4	.
B	.	.	8	.	.	2	.	2	.	.	.	.	.	2	.	2
C	.	2	.	.	2	2	2	.	.	.	.	2	.	6	.	.
D	.	4	.	.	.	.	.	4	2	.	2	.	2	.	2	.
E	.	.	2	4	2	.	.	.	6	.	.	.	.	.	2	.
F	.	2	.	.	6	.	.	.	.	4	.	2	.	.	2	.

DDT: Analyzing the Differential Properties of an S-box

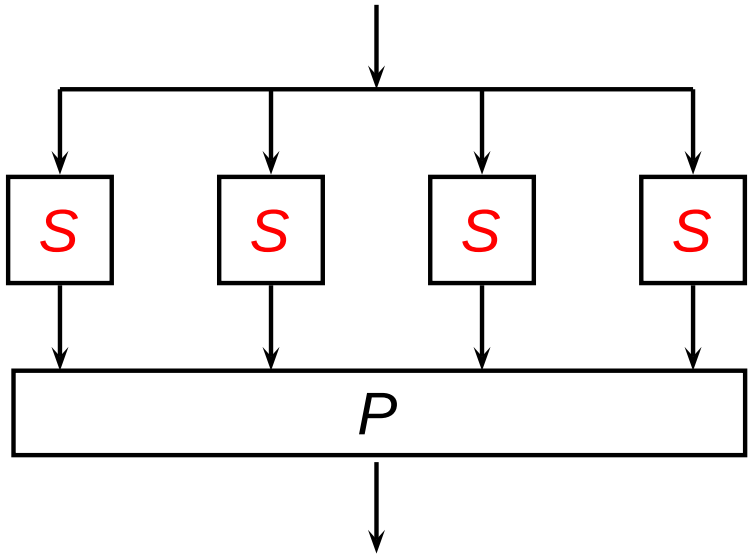
- A DDT *reflects* the differential properties of an S-box
- Many useful parameters can be computed from the DDT e.g. the maximum differential probability:

$$\max_{\alpha,\beta} \mathrm{DP}(\alpha \to \beta) = \mathrm{DP}(\texttt{0xB} \to \texttt{0x2}) = \frac{8}{16} = 0.5 \ .$$

- Used to estimate the strength against DC e.g. set upper bound on the max. probability of a differential

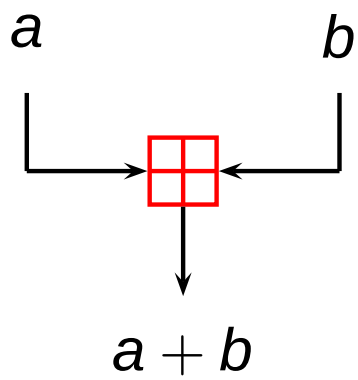
Cipher Designs that Use S-boxes

- Many cipher designs use S-boxes as a component

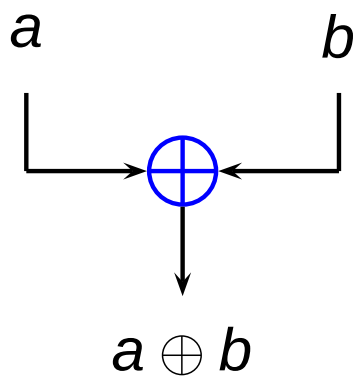


Examples: DES, AES, PRESENT, etc.

Modular Addition and XOR as Sources of Non-linearity



ADD



XOR

- ADD is non-linear w.r.t. XOR differences:

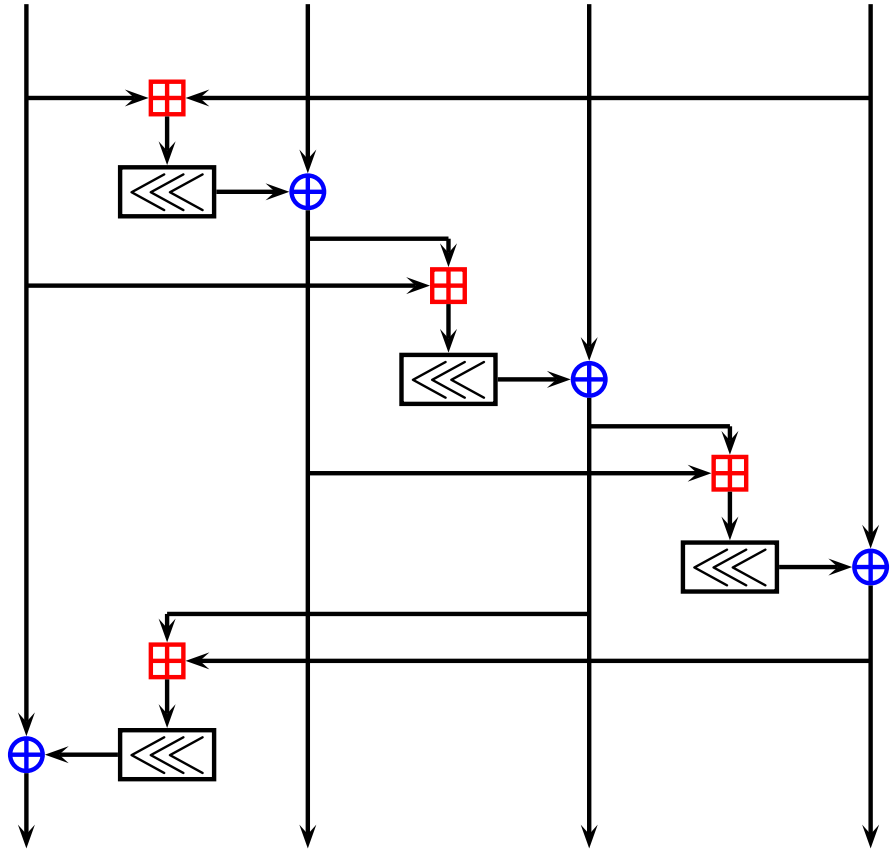
$$(a \oplus \alpha) + (b \oplus \beta) \neq (a + b) \oplus (\alpha + \beta) \ .$$

- XOR is non-linear w.r.t. ADD differences

$$(a + \alpha) \oplus (b + \beta) \neq (a \oplus b) + (\alpha \oplus \beta) \ .$$

Designs Based on ADD and XOR (ARX)

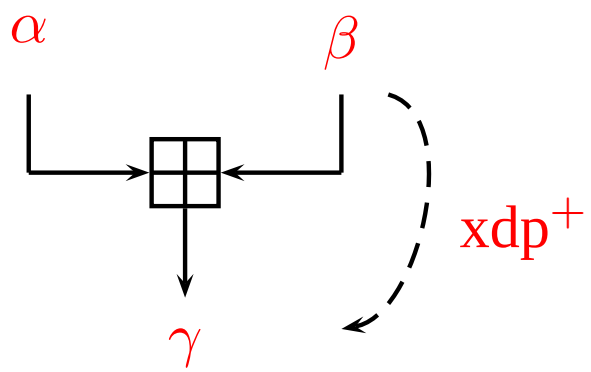
- ADD and XOR provide **non-linearity** similarly to an S-box



Examples: FEAL, MD4, MD5, Salsa20, Skein, etc.

The XOR Differential Probability of Modular Addition

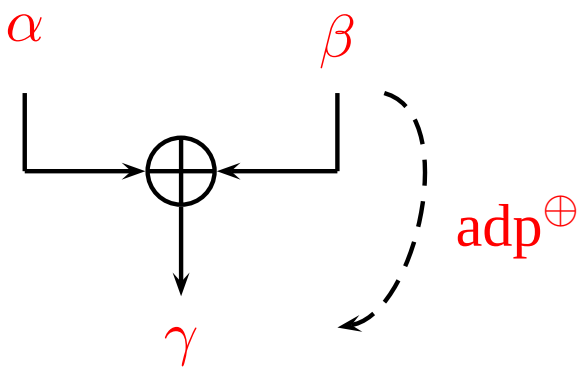
α, β, γ are XOR differences:



$$\mathrm{xdp}^+(\alpha, \beta \to \gamma) = \frac{\#\{(a,b) : ((a \oplus \alpha) + (b \oplus \beta) \oplus (a+b)) = \gamma\}}{\#\{(a,b)\}} \ .$$

The Additive Differential Probability of XOR

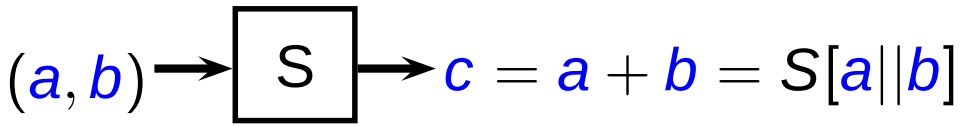
α, β, γ are additive (ADD) differences:



$$\mathrm{adp}^{\oplus}(\alpha, \beta \to \gamma) = \frac{\#\{(a,b) : ((a+\alpha) \oplus (b+\beta)) - (a+b) = \gamma\}}{\#\{(a,b)\}} \ .$$

A DDT for ADD (resp. XOR)?

- Viewing the ADD operation as an S-box:



- The DDT of this S-box is huge: $2^{64} \times 2^{32}$
- Infeasible to compute and store the full table!
- Maybe we can only store part of the DDT, say, the top k differentials:

$$k \ll 2^{64} \times 2^{32} \quad . \tag{1}$$

- A partial DDT?

Outline

Partial DDT for XOR and ADD

Definition

A partial difference distribution table D for ADD (resp. XOR) is a DDT that contains all XOR (resp. ADD) differentials $(\alpha, \beta \to \gamma)$ whose probabilities are larger than or equal to a pre-defined threshold $\mathbf{p}_{\text{thres}}$:

$$(\alpha, \beta, \gamma) \in D \iff \text{DP}(\alpha, \beta \to \gamma) \geq \mathbf{p}_{\text{thres}} \ .$$

Computation of a Partial DDT

Proposition

The differential probabilities (DP) of ADD and XOR (resp. xdp^{+} *and* $\mathrm{adp}^{\oplus}$*) are monotonously decreasing with the word size n of the differences* α, β, γ*:*

$$p_n \leq \ldots \leq p_{k+1} \leq p_k \leq p_{k-1} \leq \ldots \leq p_1 \ ,$$

where

$$p_k = \mathrm{DP}(\alpha_k, \beta_k \rightarrow \gamma_k) \ , \ n \leq k \leq 1 \ ,$$

and x_k *denotes the k LSB-s of the difference x.*

The DP of ADD and XOR is Decreasing with n

- For ADD, the proposition follows from a result by [LM01]:

$$\mathrm{xdp}^{+}(\alpha, \beta \to \gamma) = 2^{-\sum_{i=0}^{n-2} \neg\mathrm{eq}(\alpha[i],\beta[i],\gamma[i])} \quad ,$$

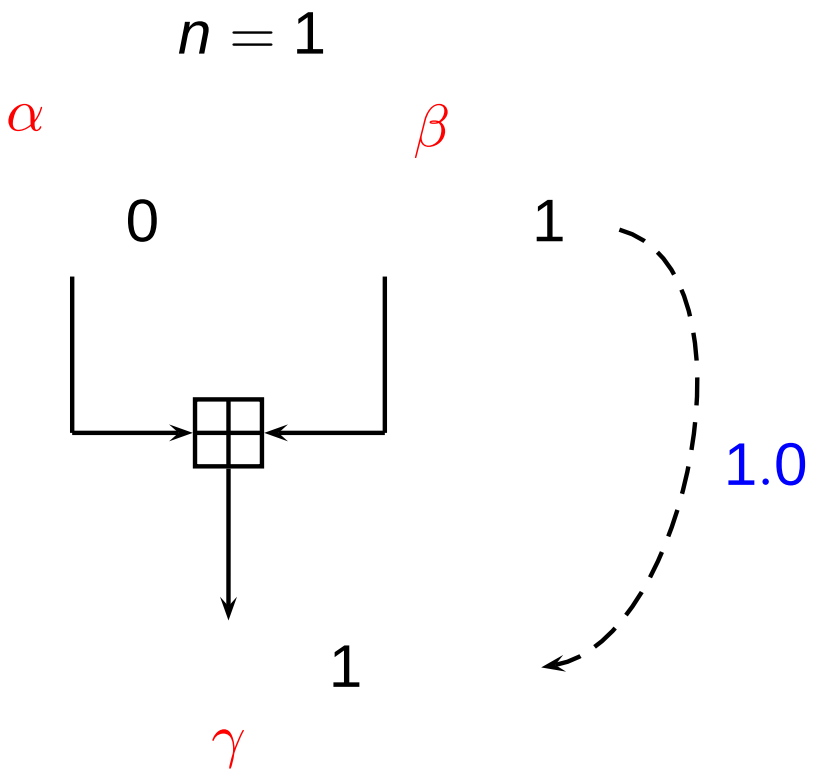
  where

$$\mathrm{eq}(\alpha[i], \beta[i], \gamma[i]) = 1 \iff \alpha[i] = \beta[i] = \gamma[i] \quad .$$

- Is also true for $\mathrm{adp}^{\oplus}$.

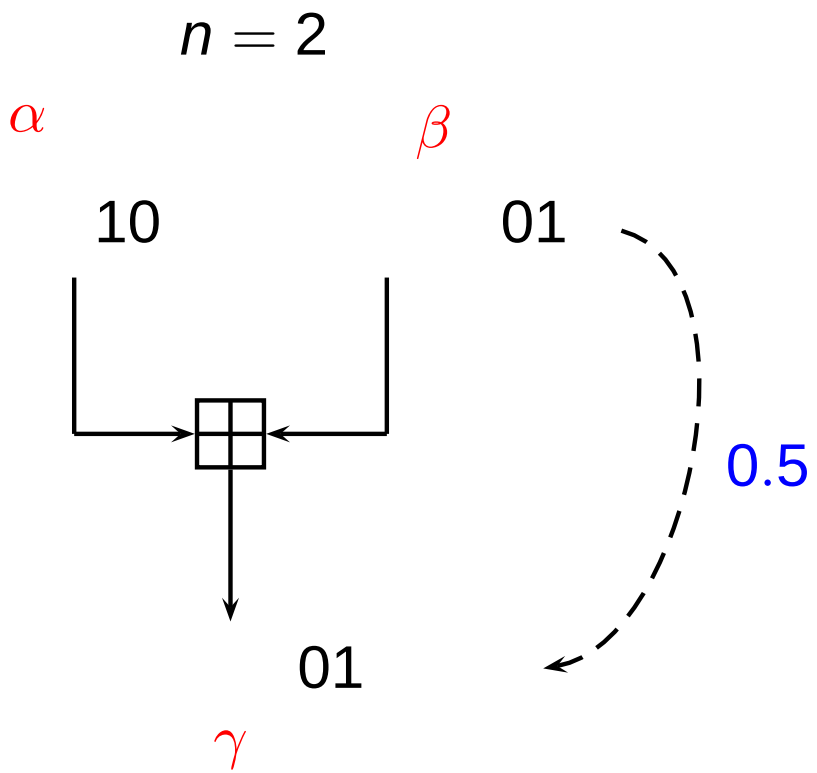
[LM01] Lipmaa, Moriai: Efficient Algorithms for Computing Differential Properties of Addition. FSE 2001: 336-350

Example: the DP of ADD is Decreasing with n



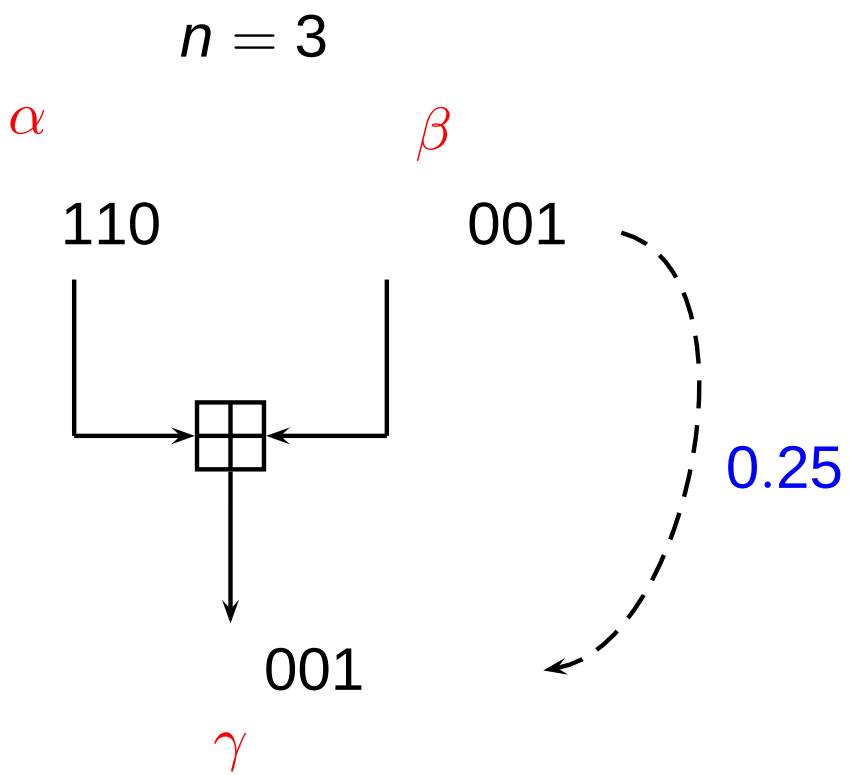
1.0

Example: the DP of ADD is Decreasing with n



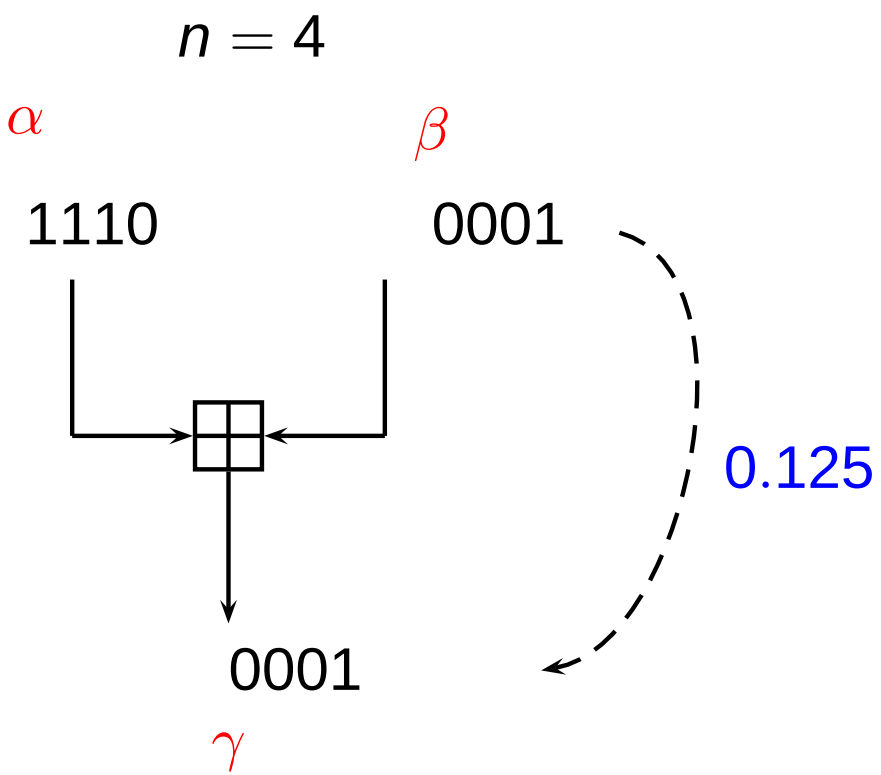
$0.5 \leq 1.0$

Example: the DP of ADD is Decreasing with n



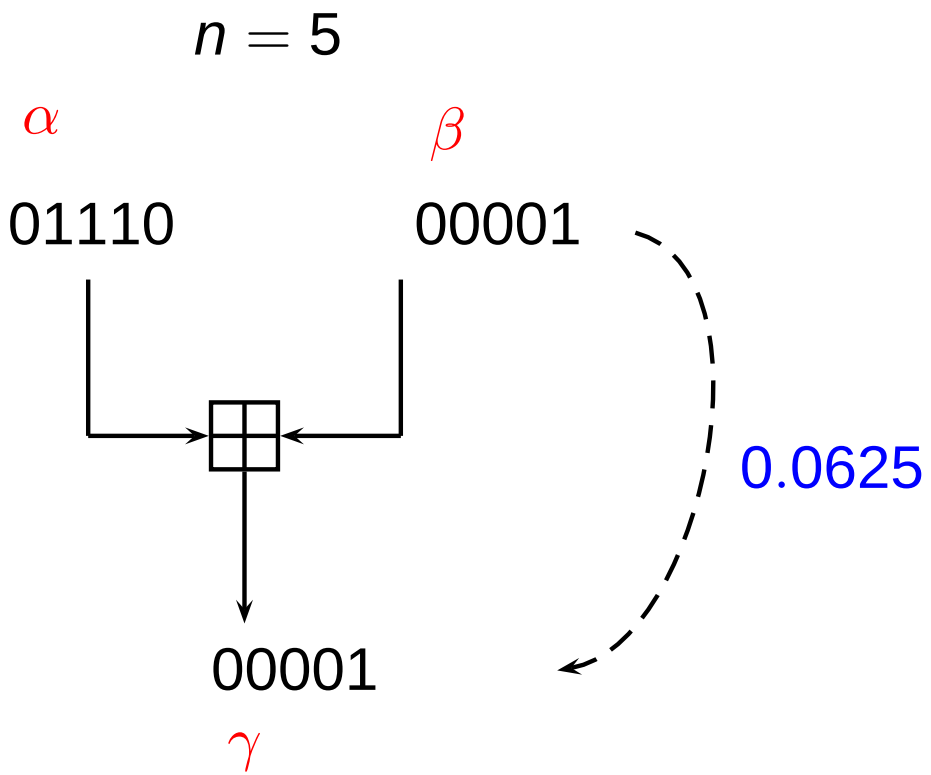
$0.25 \leq 0.5 \leq 1.0$

Example: the DP of ADD is Decreasing with n



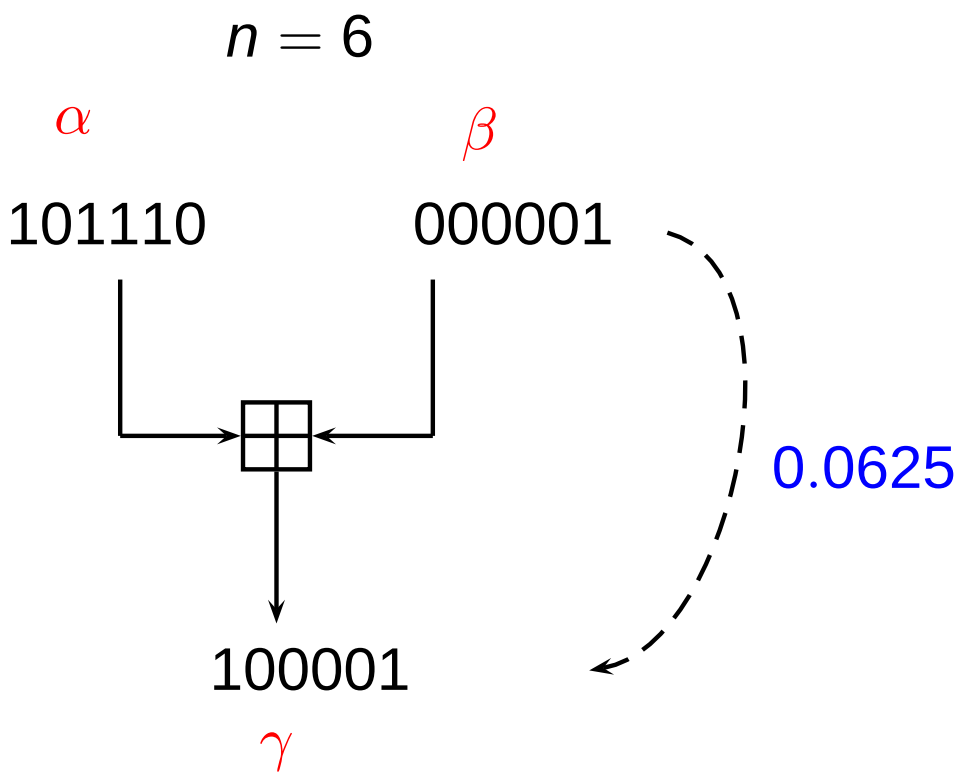
$0.125 \leq 0.25 \leq 0.5 \leq 1.0$

Example: the DP of ADD is Decreasing with n



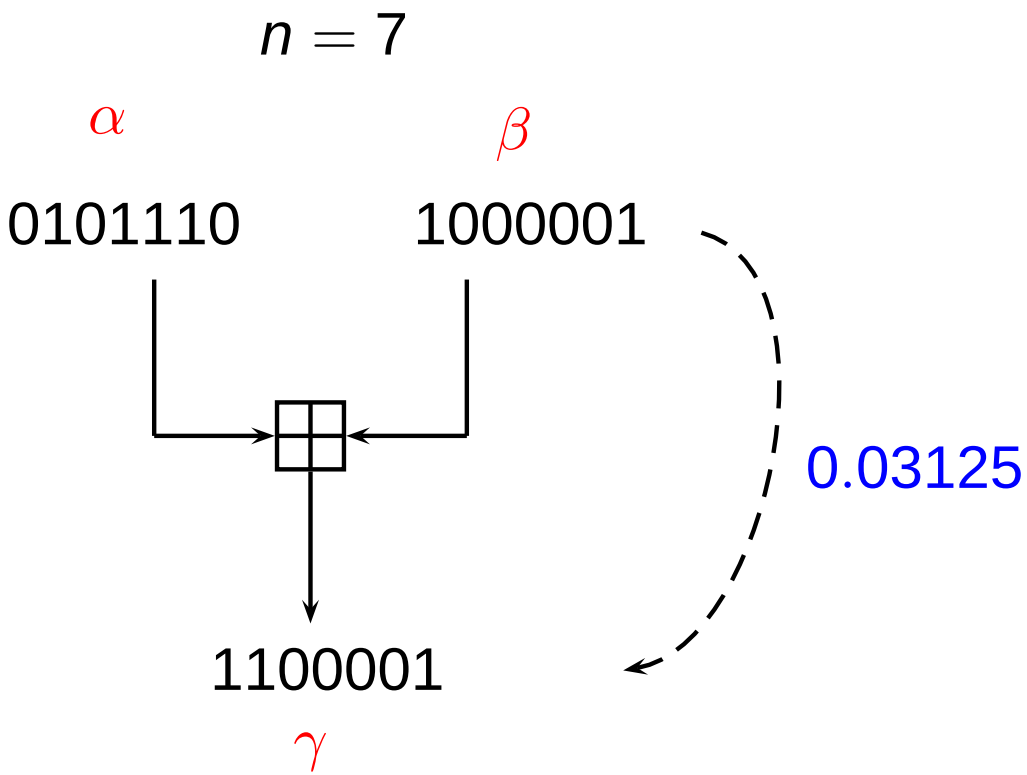
$0.0625 \leq 0.125 \leq 0.25 \leq 0.5 \leq 1.0$

Example: the DP of ADD is Decreasing with n



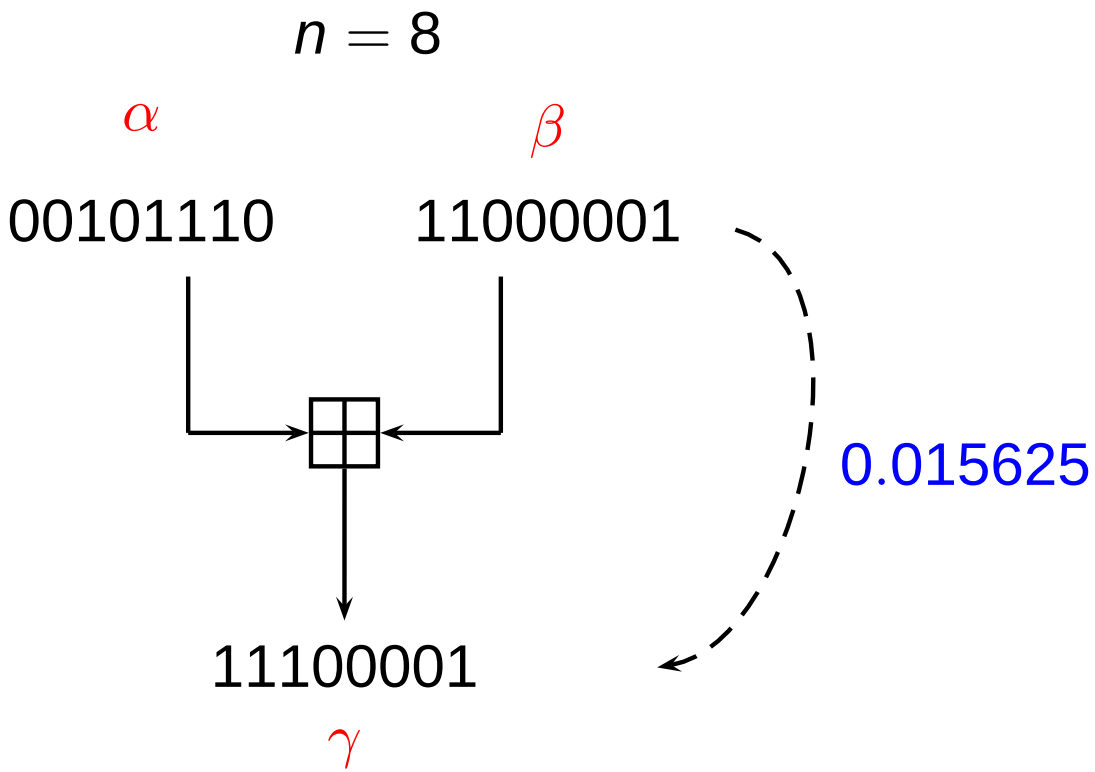
$$0.0625 \leq 0.0625 \leq 0.125 \leq 0.25 \leq 0.5 \leq 1.0$$

Example: the DP of ADD is Decreasing with n



$$0.03125 \leq 0.0625 \leq 0.0625 \leq 0.125 \leq 0.25 \leq 0.5 \leq 1.0$$

Example: the DP of ADD is Decreasing with n



$$0.015625 \leq 0.03125 \leq 0.0625 \leq 0.0625 \leq 0.125 \leq 0.25 \leq 0.5 \leq 1.0$$

Computing a Partial DDT for ADD and XOR

Procedure 1 Compute partial DDT for ADD or XOR.

Input: $n, p_{\text{thres}}, k, p_k, \alpha_k, \beta_k, \gamma_k$.

Output: Partial DDT D: $(\alpha, \beta, \gamma) \in D : \text{DP}(\alpha, \beta \rightarrow \gamma) \geq p_{\text{thres}}$.

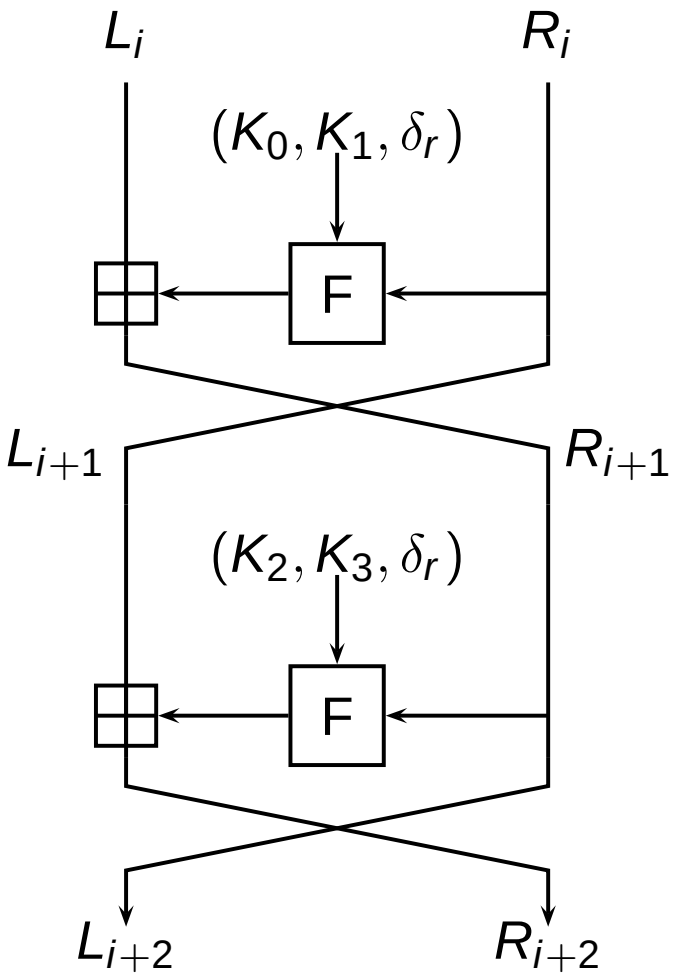
1: **if** $n = k$ **then**
2: Add $(\alpha, \beta, \gamma) \leftarrow (\alpha_k, \beta_k, \gamma_k)$ to D
3: **return**
4: **for** $x, y, x \in \{0, 1\}$ **do**
5: $\alpha_{k+1} \leftarrow x|\alpha_k, \quad \beta_{k+1} \leftarrow y|\beta_k, \quad \gamma_{k+1} \leftarrow z|\gamma_k \quad .$
6: $p_{k+1} = \text{DP}(\alpha_{k+1}, \beta_{k+1} \rightarrow \gamma_{k+1})$
7: **if** $p_{k+1} \geq p_{\text{thres}}$ **then**
8: **Procedure 1**$(n, p_{\text{thres}}, k+1, p_{k+1}, \alpha_{k+1}, \beta_{k+1}, \gamma_{k+1})$

Outline

Computation of Partial DDT: Timings, $n = 32$

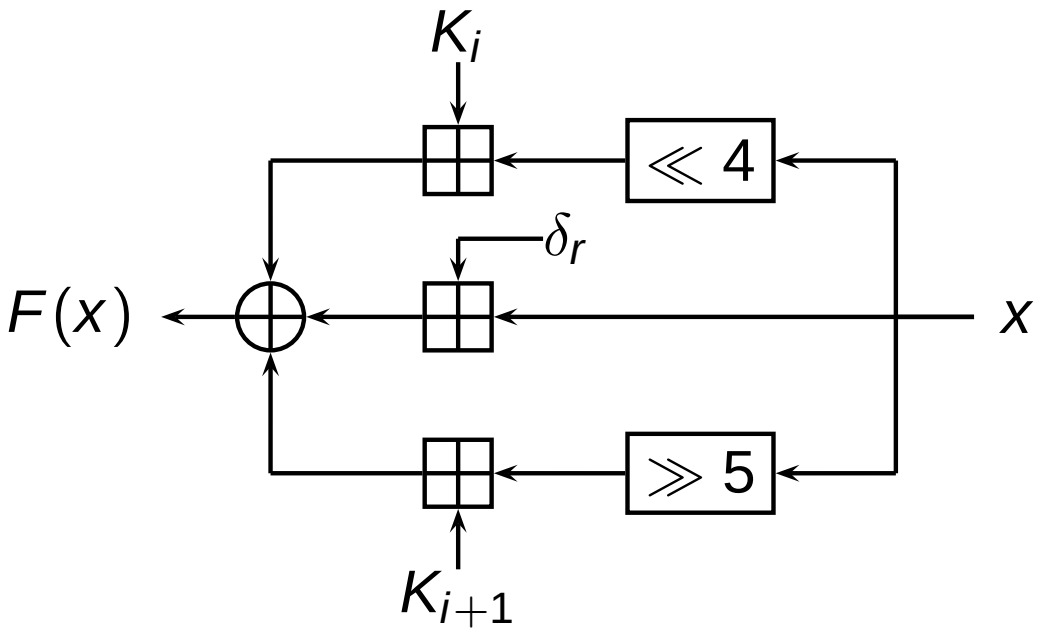
	ADD		XOR	
$\mathbf{p}_{\text{thres}}$	**DDT size**	**Time**	**DDT size**	**Time**
0.1	252, 940	36, *sec.*	3, 951, 388	2.29, *min.*
0.7	361, 420	37, *sec.*	3, 951, 388	1.23, *min.*
0.05	3, 038, 668	5.35, *min.*	167, 065, 948	44.36, *min.*
0.01	2, 715, 532, 204	17.46, *hours.*	–	–

Block Cipher TEA



- 64-round Feistel network
- 64-bit blocks: $L_i||R_i$
- 128-bit key: $K_0||K_1||K_2||K_3$
- δ_r : 32 32-bit round constants (updated every 2-nd round)
- F : round function

The F-function of TEA



Current Status of TEA

- Best attack: 23 rounds, zero-correlation [BW12]
- Best differential attack: 17 rounds, impossible differential [CWP12]

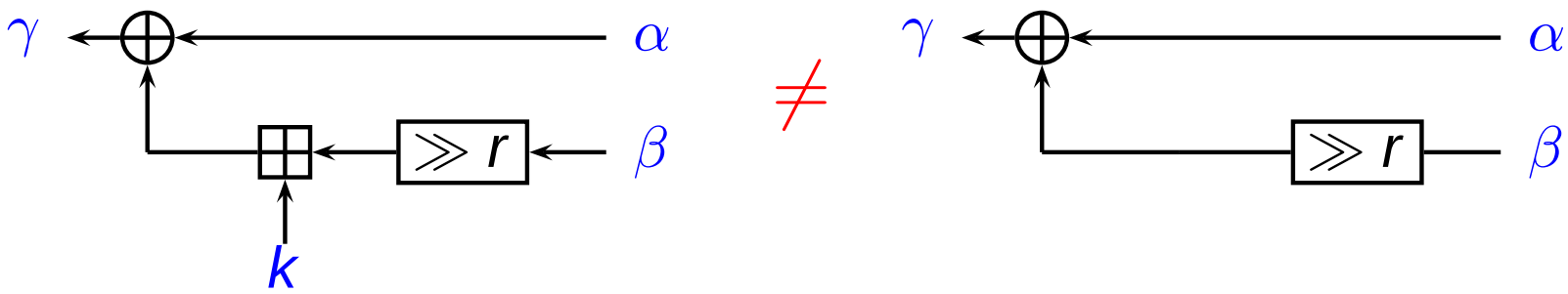
[BW12] Bogdanov, Wang: Zero Correlation Linear Cryptanalysis with Reduced Data Complexity. FSE 2012: 29-48
[CWP12] Chen, Wang, Preneel: Impossible Differential Cryptanalysis of the Lightweight Block Ciphers TEA, XTEA and HIGHT. AFRICACRYPT 2012: 117-137

UNIVERSITÉ DU LUXEMBOURG

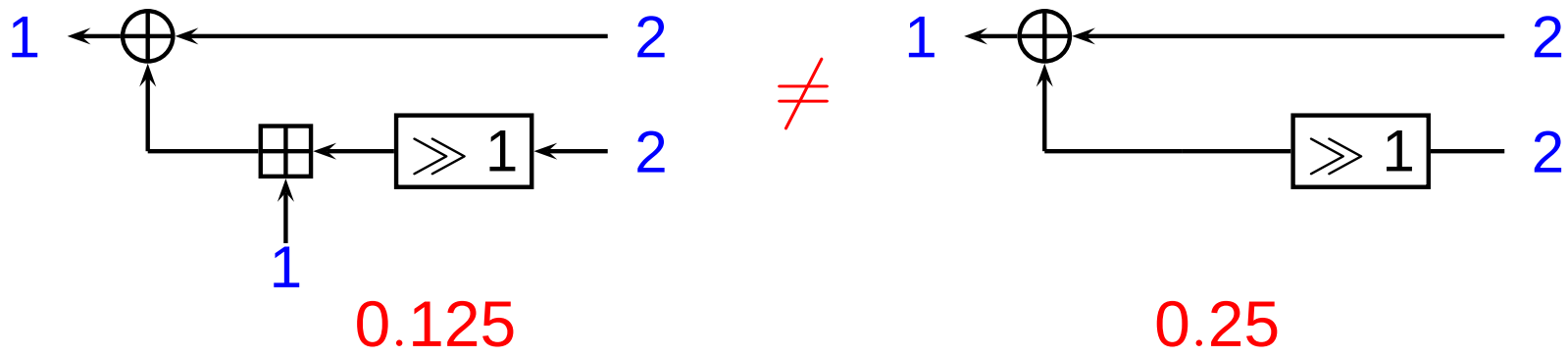
Automatic Search for ADD Differentials in TEA

- Main idea (sketch):
  - Work with ADD differences.
  - Compute a partial DDT for the XOR operation of F.
  - Extend the partial DDT to the full F.
  - Apply Matsui search strategy using the partial DDT.

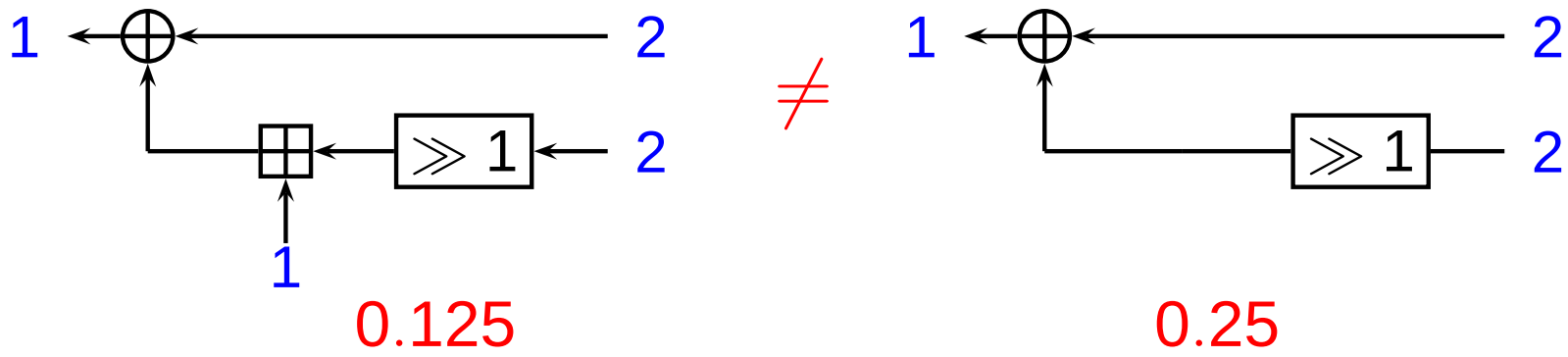
Key Dependence of the DP of the F-function



Key Dependence of the DP of the F-function, $n = 3$

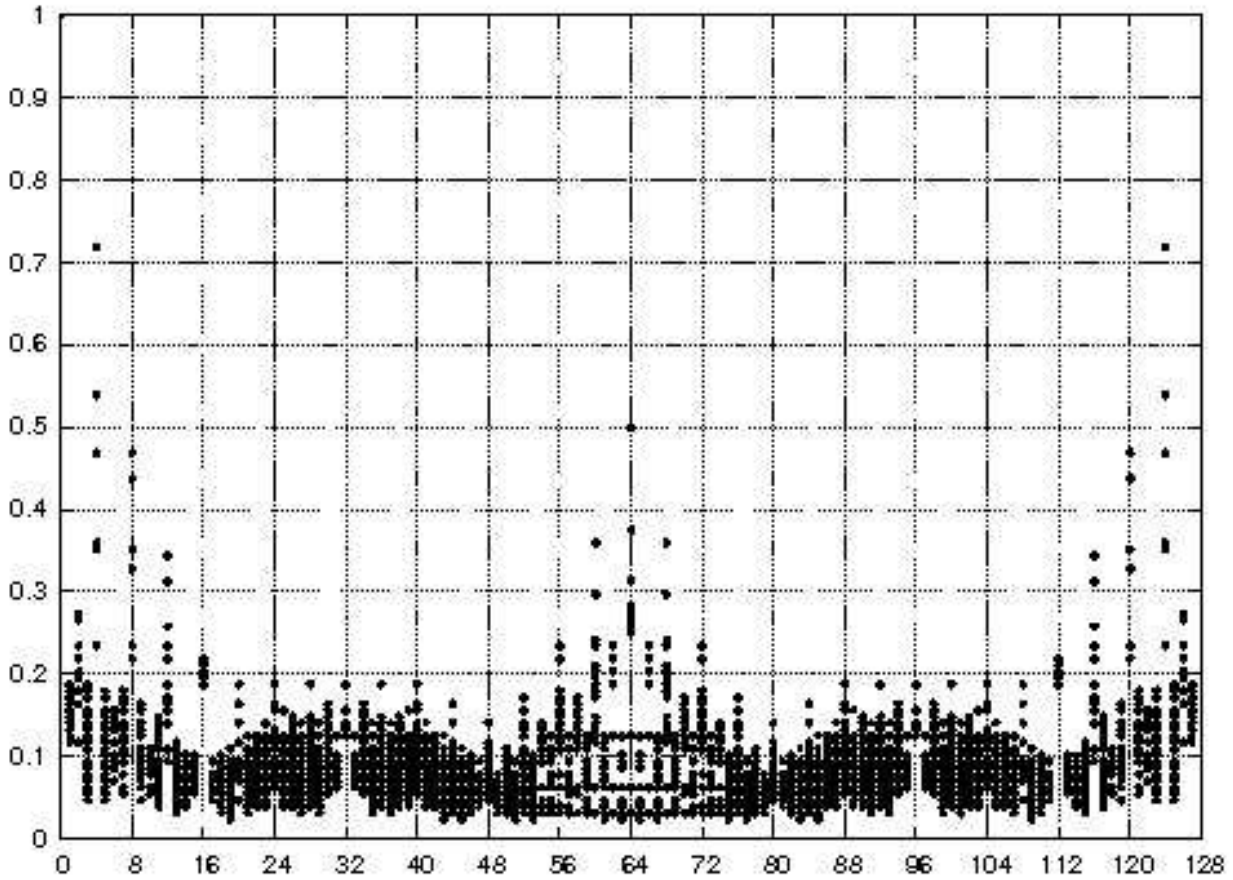


Key Dependence of the DP of the F-function, $n = 3$

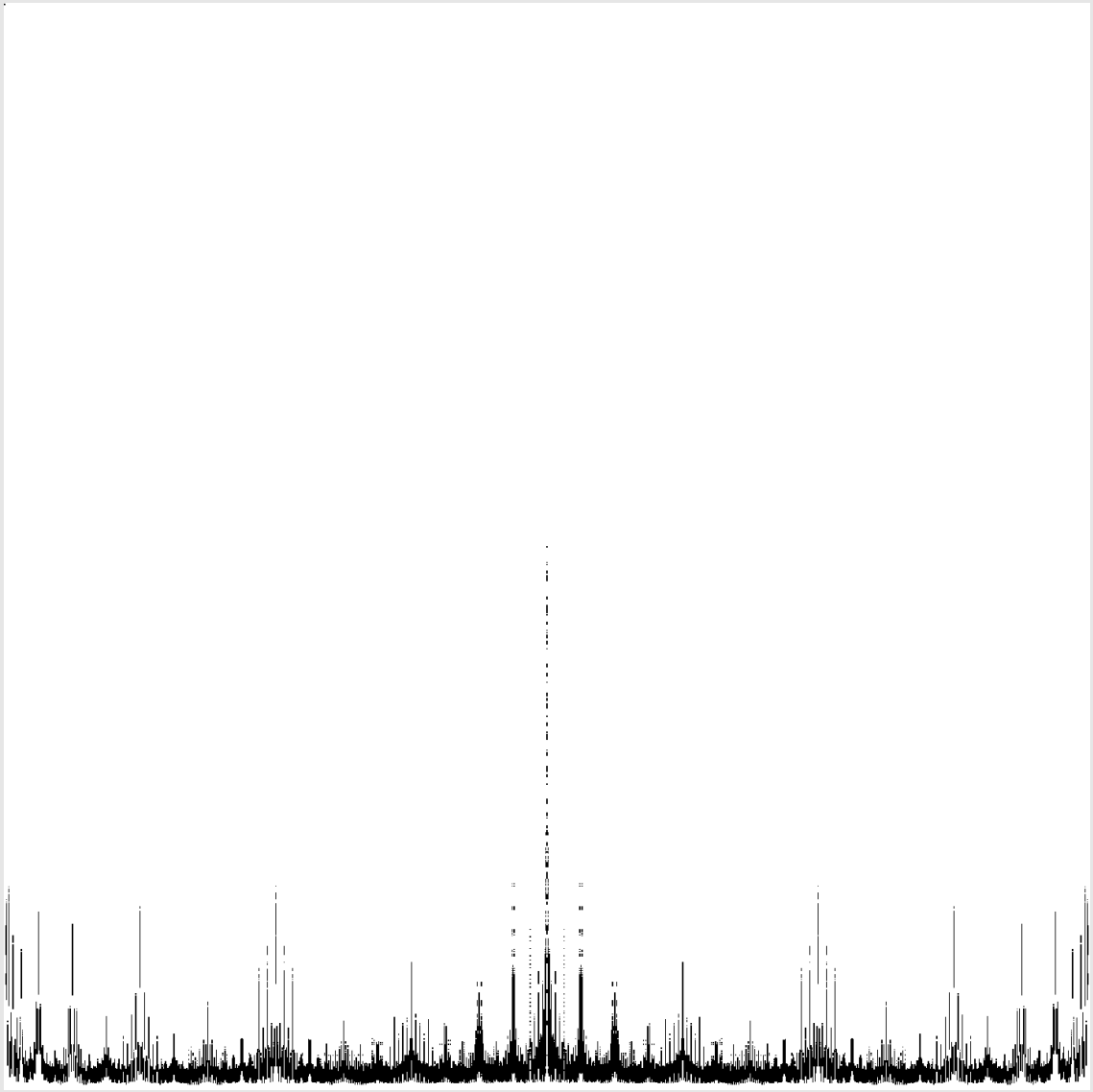


- Similar dependence for the $\ll$ operation
- In the TEA F-function, the input differences α and β are also dependent

Key Dependence of the DP of the F-function, $n = 7$



Key Dependence of the DP of the F-function, $n = 10$



Credit: Yann Le Corre, LACS

Key Dependence: More Issues

- The same keys are used every 2-nd round
- Does it make sense to assume independent round keys in this case (as is usually done)?
- Are average probabilities (over all keys) still a good estimation of the actual probability of differentials (cf. hypothesis of stochastic equivalence)?
- Seems that TEA is not a key-alternating cipher – further complicates analysis:

Definition (DR07)

A key-alternating cipher consists of an alternating sequence of unkeyed rounds and simple bitwise key additions.

[DR07] Daemen, Rijmen: Probability distributions of correlation and differentials in block ciphers. J. Mathematical Cryptology 1(3): 221-242 (2007)

TEA, $n = 11$, all δ, $p_{\text{thres}} = 0.01$: pDDT vs. full DDT

r	Δ^+y		Δ^+x	p	Δ^+y		Δ^+x	p
0	0	$\leftarrow$	0	1	378	$\leftarrow$	80	0.094727
1	388	$\leftarrow$	80	0.085785	0	$\leftarrow$	0	1
2	780	$\leftarrow$	388	0.027191	378	$\leftarrow$	80	0.117676
3	0	$\leftarrow$	0	1	780	$\leftarrow$	378	0.041992
4	80	$\leftarrow$	388	0.037476	0	$\leftarrow$	0	1
5	478	$\leftarrow$	80	0.131866	0	$\leftarrow$	378	0.049316
6	0	$\leftarrow$	0	1	0	$\leftarrow$	0	1
7	388	$\leftarrow$	80	0.093323	0	$\leftarrow$	378	0.021484
8	780	$\leftarrow$	388	0.023865	0	$\leftarrow$	0	1
9	0	$\leftarrow$	0	1	80	$\leftarrow$	378	0.034668
10	0	$\leftarrow$	388	0.038422	488	$\leftarrow$	80	0.112305
11	0	$\leftarrow$	0	1	0	$\leftarrow$	0	1
$\prod_r$				$2^{-29.92}$				$2^{-28.95}$

key = 4E1 193 1D5 34

TEA, $n = 16$, one δ, $p_{\text{thres}} = 0.01$: pDDT vs. full DDT

r	Δ^+y		Δ^+x	p	Δ^+y		Δ^+x	p
0	0	←	0	1	0	←	0	1
1	0	←	1108	0.013123	0	←	F08	0.014404
2	0	←	0	1	0	←	0	1
3	0	←	1108	0.013123	0	←	F08	0.014404
4	0	←	0	1	0	←	0	1
5	0	←	1108	0.013123	0	←	F08	0.014404
6	0	←	0	1	0	←	0	1
7	0	←	1108	0.013123	0	←	F08	0.014404
8	0	←	0	1	0	←	0	1
9	0	←	1108	0.013123	0	←	F08	0.014404
10	0	←	0	1	0	←	0	1
11	0	←	1108	0.013123	0	←	F08	0.014404
12	0	←	0	1	0	←	0	1
13	100	←	1108	0.015442	FF00	←	F08	0.014267
14	EEF8	←	100	0.039978	F0F8	←	FF00	0.042694
15	0	←	0	1	0	←	0	1
$\prod_r$				$2^{-48.17}$				$2^{-47.39}$

key = E1A5 37E3 8FCF FB5A

TEA, $n = 32$, all δ, $p_{\text{thres}} = 0.01$

r	$\Delta^+ y$		$\Delta^+ x$	p	$p, \log_2$
0	0	$\leftarrow$	0	1	$2^{-0.00}$
1	F	$\leftarrow$	FFFFFFFF	0.082794	$2^{-3.59}$
2	0	$\leftarrow$	F	0.000458	$2^{-11.09}$
3	FFFFFFF1	$\leftarrow$	FFFFFFFF	0.139893	$2^{-2.84}$
4	0	$\leftarrow$	0	1	$2^{-0.00}$
5	11	$\leftarrow$	FFFFFFFF	0.081909	$2^{-3.61}$
6	0	$\leftarrow$	11	0.000092	$2^{-13.42}$
7	FFFFFFEF	$\leftarrow$	FFFFFFFF	0.133881	$2^{-2.90}$
8	0	$\leftarrow$	0	1	$2^{-0.00}$
9	11	$\leftarrow$	FFFFFFFF	0.077576	$2^{-3.69}$
10	0	$\leftarrow$	11	0.000122	$2^{-13.00}$
11	FFFFFFEF	$\leftarrow$	FFFFFFFF	0.139709	$2^{-2.84}$
12	0	$\leftarrow$	0	1	$2^{-0.00}$
13	FFFFFFF1	$\leftarrow$	FFFFFFFF	0.083771	$2^{-3.58}$
$\prod_r$					$2^{-60.56}$

key = E028DF9A 8819B4C3 3AB116AF 3C50723

TEA, $n = 32$, single δ, $p_{\text{thres}} = 0.01$

r	$\Delta^+ y$		$\Delta^+ x$	p	$p, \log_2$
0	FFFFFFF1	$\leftarrow$	1	0.137390	$2^{-2.86}$
1	0	$\leftarrow$	0	1	$2^{-0.00}$
2	F	$\leftarrow$	1	0.135712	$2^{-2.88}$
3	0	$\leftarrow$	F	0.001984	$2^{-8.98}$
4	FFFFFFF1	$\leftarrow$	1	0.133148	$2^{-2.91}$
5	0	$\leftarrow$	0	1	$2^{-0.00}$
6	F	$\leftarrow$	1	0.138214	$2^{-2.86}$
7	0	$\leftarrow$	F	0.002533	$2^{-8.62}$
8	FFFFFFF1	$\leftarrow$	1	0.137360	$2^{-2.86}$
9	0	$\leftarrow$	0	1	$2^{-0.00}$
10	F	$\leftarrow$	1	0.130371	$2^{-2.94}$
11	0	$\leftarrow$	F	0.001984	$2^{-8.98}$
12	FFFFFFF1	$\leftarrow$	1	0.131958	$2^{-2.92}$
13	0	$\leftarrow$	0	1	$2^{-0.00}$
14	F	$\leftarrow$	1	0.137543	$2^{-2.86}$
15	0	$\leftarrow$	F	0.002228	$2^{-8.81}$
16	FFFFFFF1	$\leftarrow$	1	0.136597	$2^{-2.87}$
17	0	$\leftarrow$	0	1	$2^{-0.00}$
$\prod_r$					$2^{-61.36}$

Outline

Summary of Contributions

- Presented partial DDT-s + algorithm for their computation
- An attempt to quantify the resistance of ARX ciphers against DC, similarly to S-box-based ciphers
- Makes possible to apply Matsui algorithm (originally proposed for S-box ciphers) to automatically search for differentials in ARX designs
- Showed preliminary results from application to TEA:
  - Differential on 14 rounds, $p = 2^{-60.56}$, original TEA
  - Differential on 18 rounds, $p = 2^{-61.36}$, modified TEA (use the same constant δ at every round)

Thank you for your attention!

UNIVERSITÉ DU LUXEMBOURG