Truncated Differential Analysis of Reduced-Round LBlock

Sareh Emami, Cameron McDonald, Josef Pieprzyk and Ron Steinfeld

Joint work between **Macquarie University**, **Qualcomm Inc. Australia** and **Monash University**

CANS 2013, Paraty, Brazil

Outline

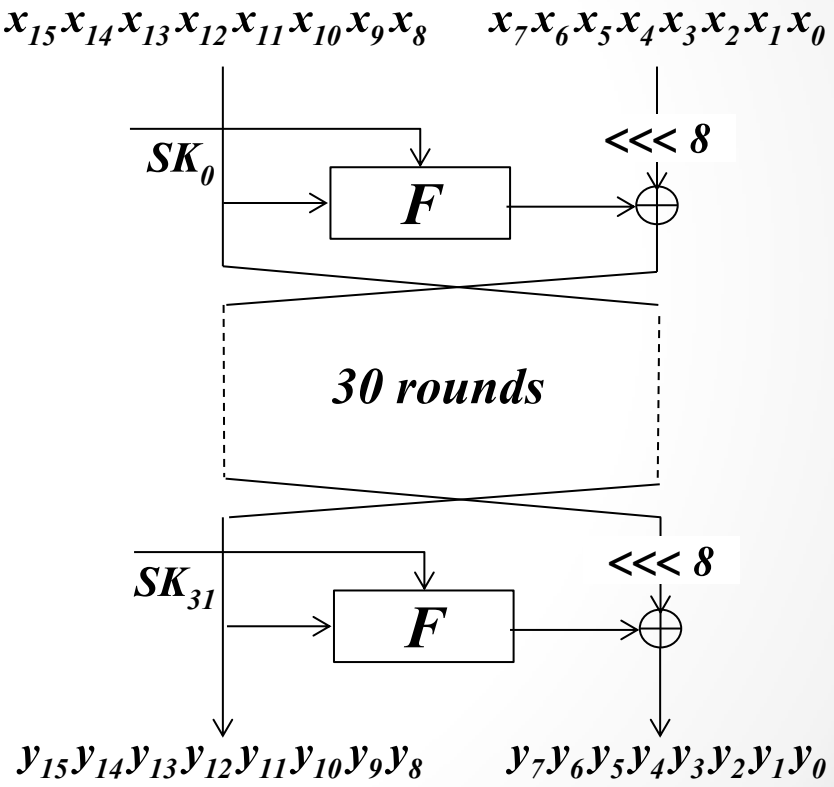
- Preliminaries
- Truncated differential distribution
- Truncated differential analysis of LBlock
- Complexity Analysis
- Experiments
- Results

Our Contribution

- Truncated differential analysis
  - Differential probability distributions
  - Log-likelihood ratio (LLR) test
- Presented framework
  - Merges the truncated differential distributions with classical differential analysis
- Application to LBlock
  - Single-key attack - 18 rounds
  - Related-key attacks – 21 rounds

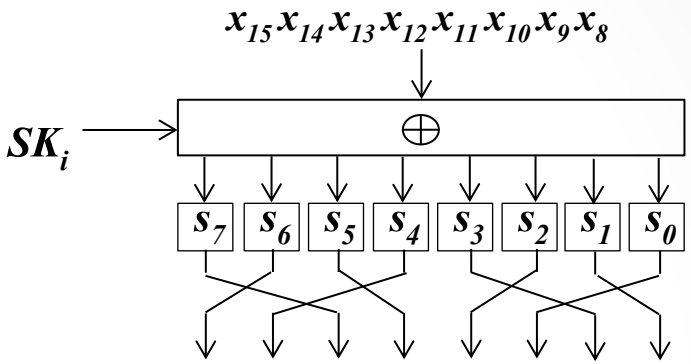
LBlock

- Was submitted to ACNS 2011
- Lightweight block cipher
  - 64-bit block
  - 80-bit secret key
- Balanced Feistel network
  - 32-round

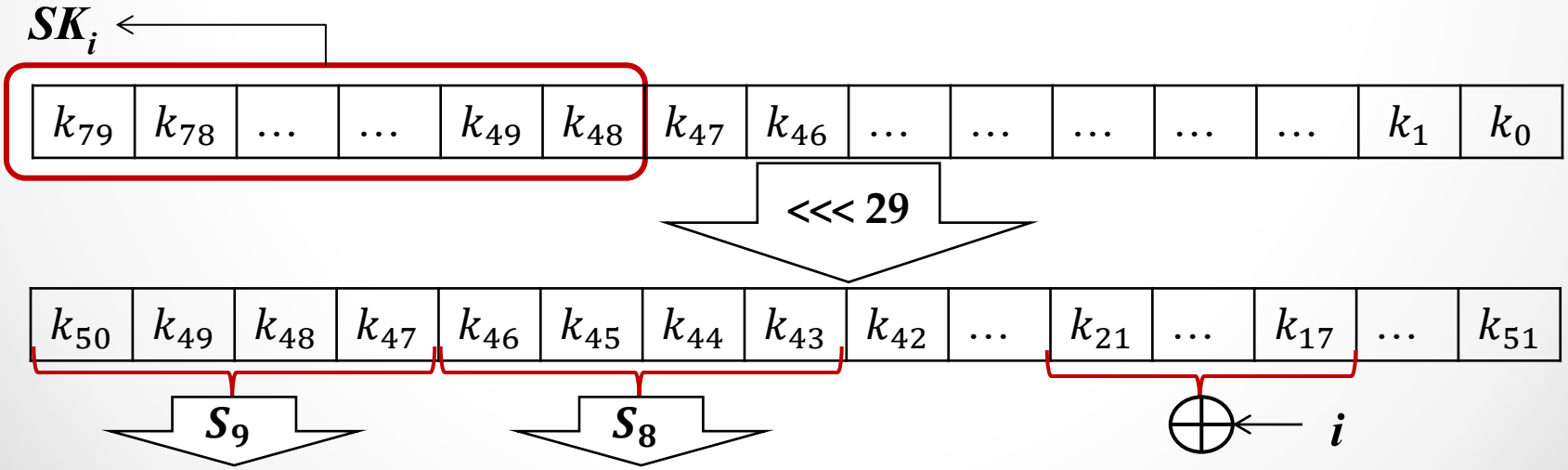


LBlock

- SPN round function



- Key Schedule
  - 32-bit sub-keys: $SK_0, SK_1, \ldots, SK_{31}$



Likelihood test

- Statistical test which compares two distributions
- Let P and Q be two discrete probability distributions
- Kullback-Leibler (KL) divergence
  - Measures the distance between P and Q
- The log-likelihood ratio (LLR)
  - Empirical dataset x taken from N samples
  - Determines the probability distribution (P or Q) that the sample data x belongs to

Related Work

- All-in-one approach to differential analysis of lightweight block ciphers
  - Albrecht and Leander (SAC 2012)
- Multiple differential cryptanalysis using the LLR and χ^2 tests
  - Blondeau *et. al.* (SCN 2012)
- Both analyses work on ciphers with *small* block sizes

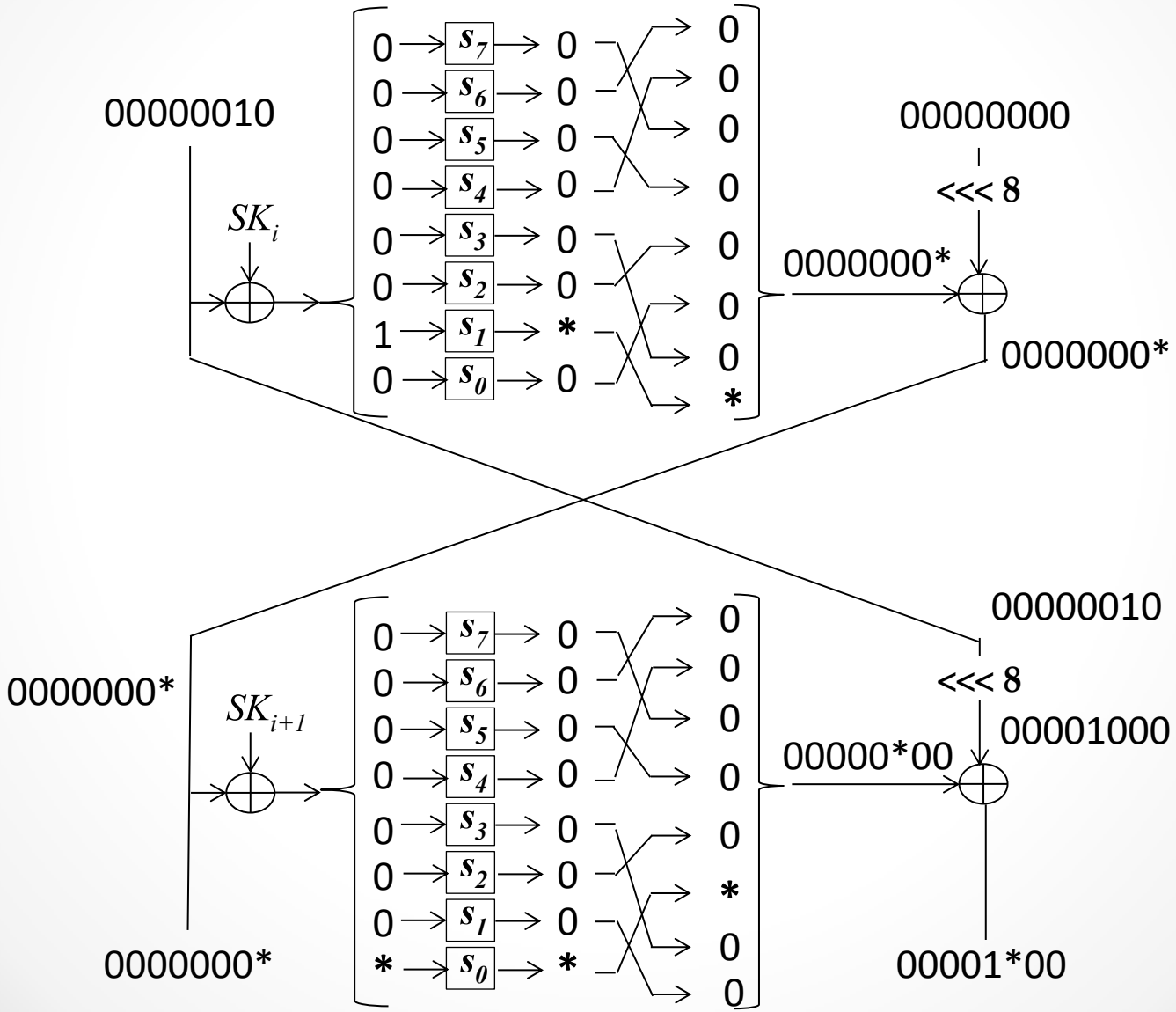
Outline

- Preliminaries
- Truncated differential distribution
- Truncated differential analysis of LBlock
- Complexity Analysis
- Experiments
- Results

Truncated Differential Distribution (TDD)

- Assumes the cipher follows the Marcov assumption
  - The probability distribution of round r only depends on round $r-1$
- Finds the differential distribution for the state symbols
  - Nibbles in LBlock
- Starts from a fixed differential
  - Propagates the differences through r rounds
  - Finds the probability of every difference for each nibble

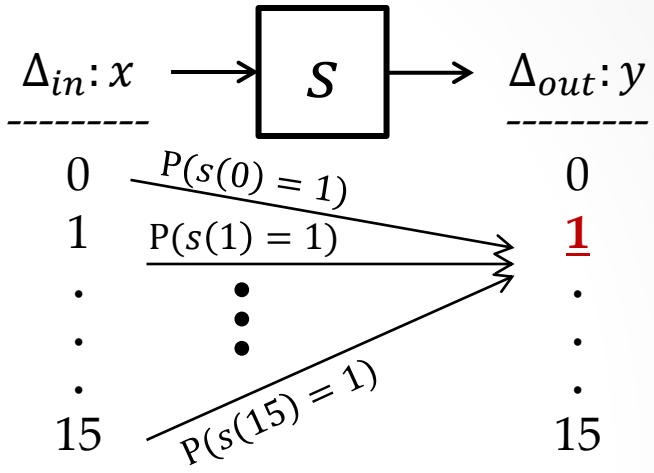
Truncated Differential



Computing TDD

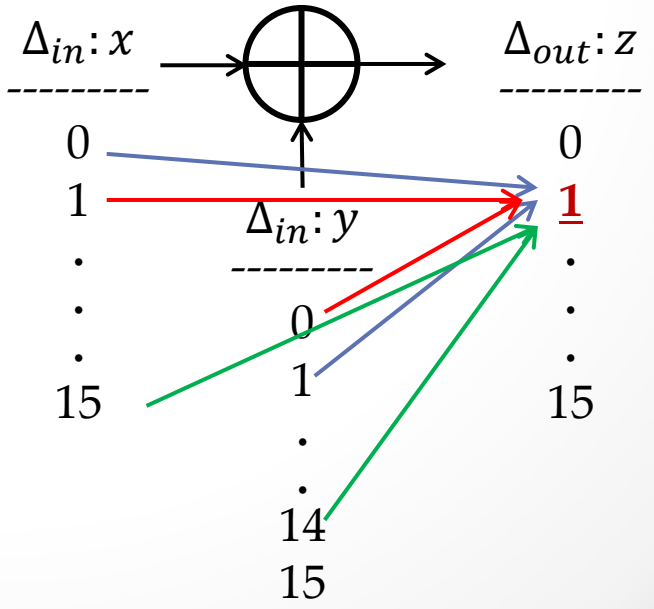
- S-box transformation

$$y^i = \sum_{j=0}^{15} x^j \cdot \mathrm{P}(s(j) = i)$$



- XOR addition

$$z^i = \sum_{j=0}^{15} x^j \cdot y^{i \oplus j}$$



Sample TDD

- Input difference: 00000000 10000000
- TDD is computed through 8 rounds of LBlock encryption
  - The right-hand half truncated differential distribution is:

Diff\Nibble	Γ_7	Γ_6	Γ_5	Γ_4	Γ_3	Γ_2	Γ_1	Γ_0
0	0.0610	0.0654	0.0000	0.0000	0.0667	0.0667	0.0000	0.0000
1	0.0000	0.0592	0.0312	0.0693	0.0625	0.0625	0.0625	0.0645
2	0.0649	0.0620	0.1562	0.0732	0.0626	0.0624	0.0312	0.0635
3	0.0649	0.0619	0.0312	0.0684	0.0623	0.0626	0.0938	0.0649
4	0.0610	0.0608	0.0469	0.0698	0.0620	0.0625	0.0625	0.0654
5	0.0732	0.0646	0.0469	0.0610	0.0626	0.0625	0.0625	0.0664
6	0.0703	0.0657	0.0781	0.0649	0.0622	0.0624	0.1250	0.0654
7	0.0684	0.0604	0.1094	0.0698	0.0625	0.0625	0.0625	0.0688
8	0.0703	0.0588	0.0625	0.0635	0.0617	0.0646	0.0625	0.0649
9	0.0679	0.0663	0.0625	0.0649	0.0618	0.0583	0.0625	0.0757
A	0.0659	0.0627	0.0469	0.0635	0.0623	0.0604	0.0312	0.0659
B	0.0649	0.0626	0.0469	0.0728	0.0619	0.0626	0.0312	0.0684
C	0.0615	0.0615	0.0781	0.0659	0.0621	0.0646	0.0625	0.0649
D	0.0679	0.0634	0.1094	0.0654	0.0619	0.0583	0.0625	0.0728
E	0.0693	0.0591	0.0625	0.0620	0.0626	0.0645	0.1250	0.0630
F	0.0684	0.0656	0.0312	0.0654	0.0623	0.0626	0.0625	0.0654
$D(P\|\|U)$	**6.59e-2**	**7.37e-4**	**1.81e-1**	**6.59e-2**	**1.55e-4**	**5.6e-4**	**1.46e-1**	**6.57e-2**

KL-divergence (distance from the uniform distribution)

Outline

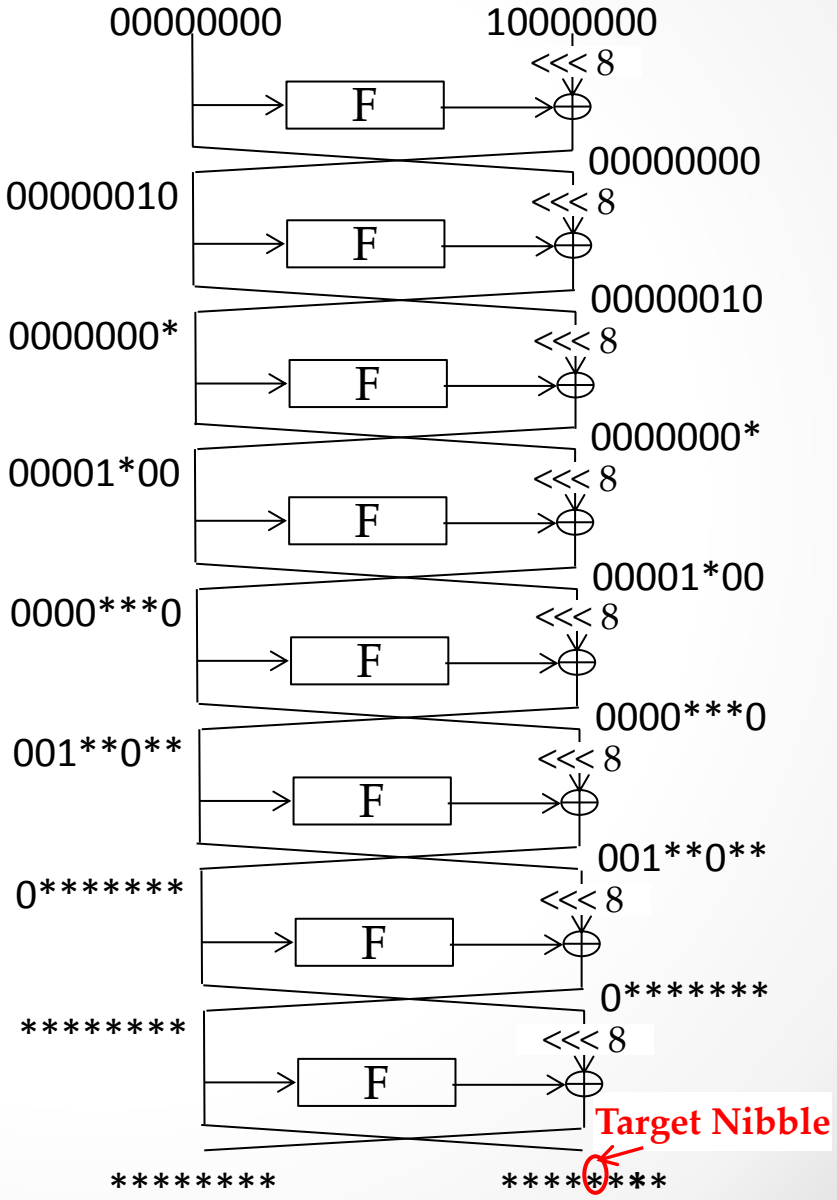
- Preliminaries
- Truncated differential distribution
- Truncated differential analysis of LBlock
- Complexity Analysis
- Experiments
- Results

LBlock Attack

- The TDD is extended on both sides
  - Benefits from the key schedule properties
- The attack model
  - Standard differential phase (SD)
  - Truncated differential distribution phase (TDD)
  - Partial-key recovery phase (PKR)

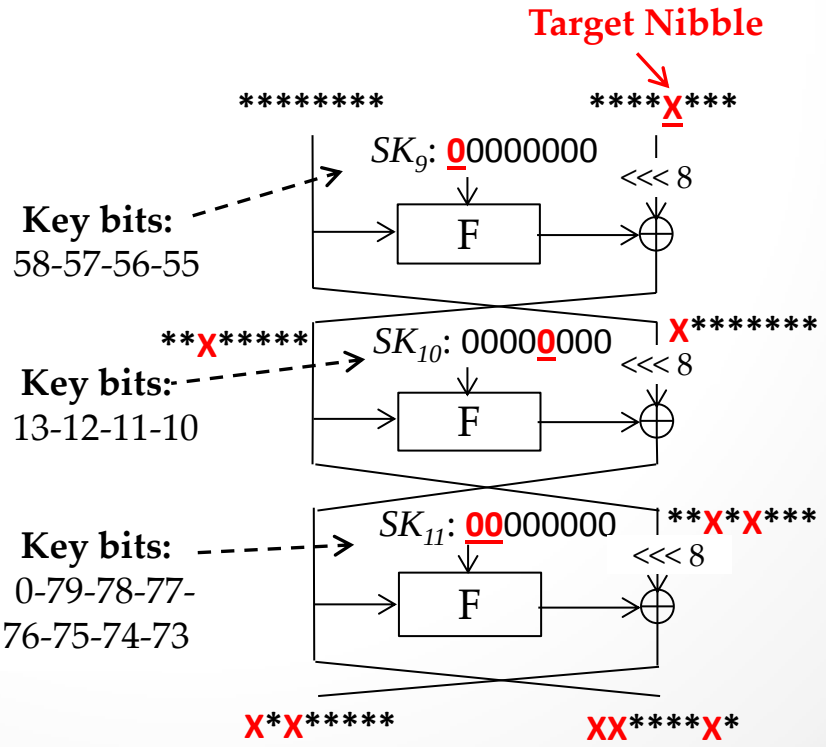
TDD Phase

- 8-round truncated differential distribution
- Target nibble
  - Its distribution has a relatively high distance from the uniform



PKR Phase

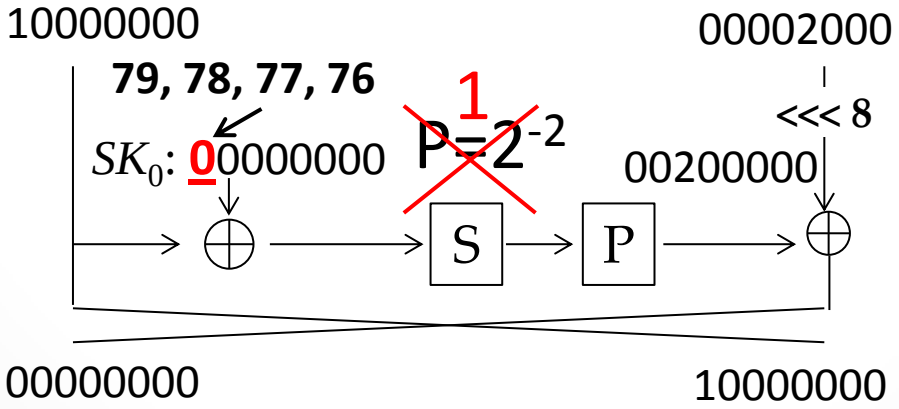
- Additional rounds added to the end of TDD rounds
- Partially decrypt the ciphertexts
  - Finds the differential distribution for the target nibble
- LLR test
- Example 3 rounds



SD Phase

- High probability differential characteristic
  - Assume we know some key-bits
- Example 1-round differential:

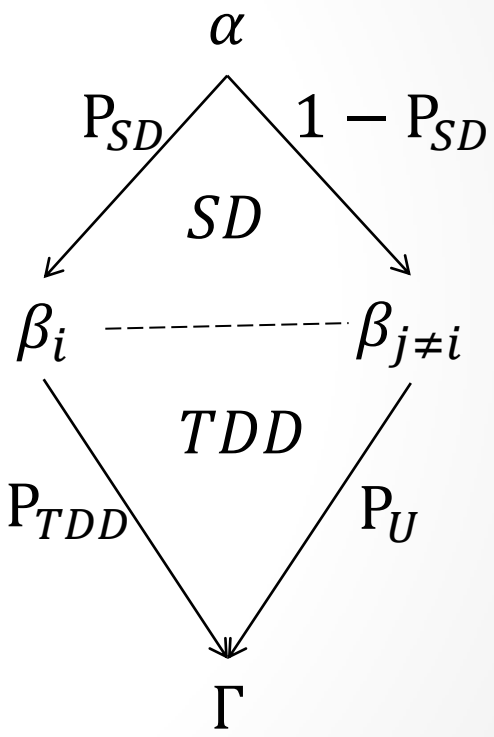
$$(10000000\ 00002000) \rightarrow (00000000\ 10000000)$$



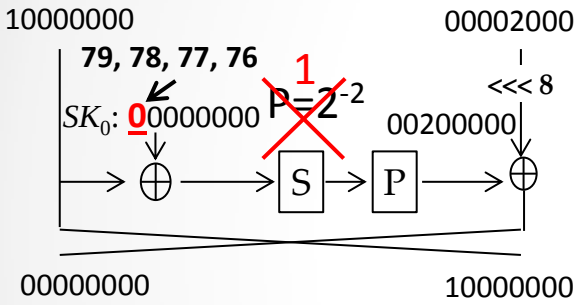
Merging Phase

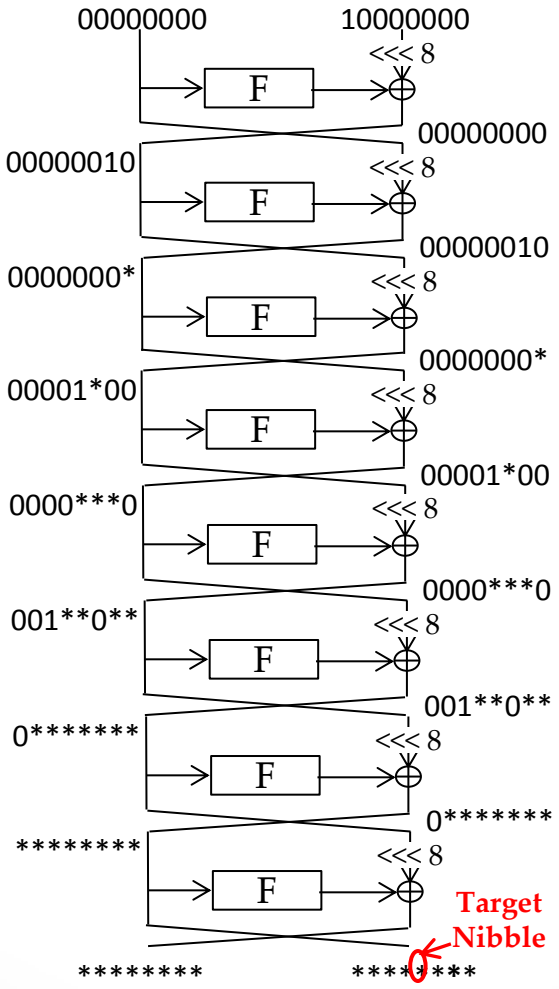
- Assume
  - $\mathrm{P}_{SD} = \mathrm{P}\,(\alpha \rightarrow \beta_i)$
  - $\mathrm{P}_{TDD} = \mathrm{P}\,(\beta_i \rightarrow \Gamma)$
  - P_U is the random probability

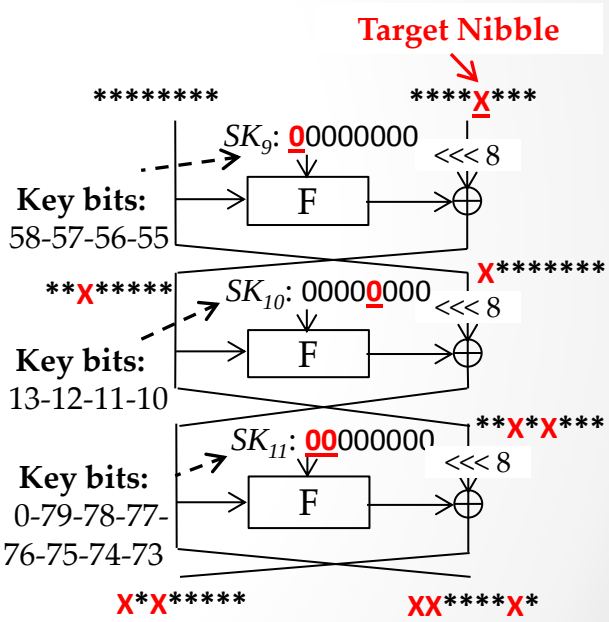
$$\mathrm{P}(\alpha \rightarrow \Gamma) = \mathrm{P}_{SD} \cdot \mathrm{P}_{TDD} + (1 - \mathrm{P}_{SD}) \cdot \mathrm{P}_U$$



12-Round Example





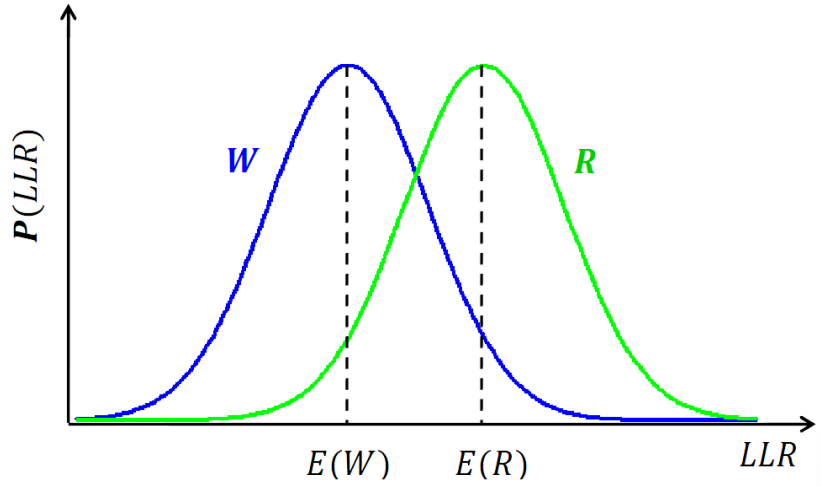


Outline

- Preliminaries
- Truncated differential distribution
- Truncated differential analysis of LBlock
- Complexity Analysis
- Experiments
- Results

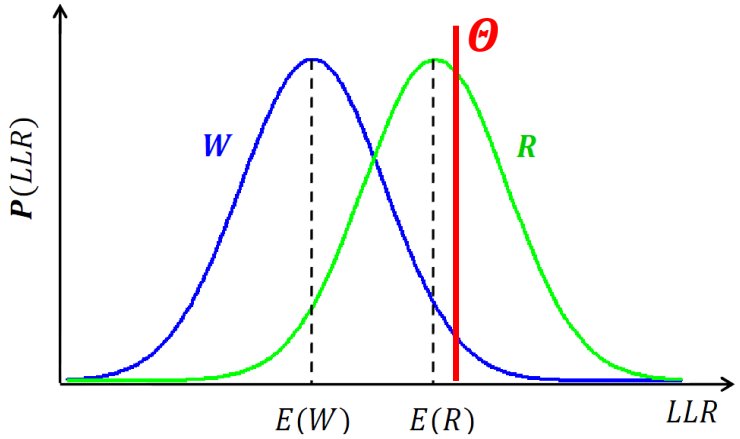
LLR Distributions

- W is a random variable for the LLR of the wrong keys
  - Wrong key randomization hypothesis
- R is a random variable for the LLR of the right key
  - Is a binomial distribution



Complexity Analysis

- Cumulative distribution function (CDF)
  - Probability of X falling into the interval $[x, \infty)$:
- Denote Θ a threshold for the LLR
  - Success rate : $\mathrm{P}(R \geq \Theta)$
  - Probability of a wrong key LLR becomes higher than Θ : $\mathrm{P}(W \geq \Theta)$



Complexity

- Number of wrong keys ranked higher than Θ

$$N_{wk} = N_K \cdot \mathrm{P}(W \geq \Theta)$$

- We have to adjust Θ and N (number of samples)
  - Compromise between the success rate and the complexity

- Complexity of the full key-recovery

$$C = N2^b + (N_{wk} + 1)2^{80-b}$$

Outline

- Preliminaries
- Truncated differential distribution
- Truncated differential analysis of LBlock
- Complexity Analysis
- Experiments
- Results

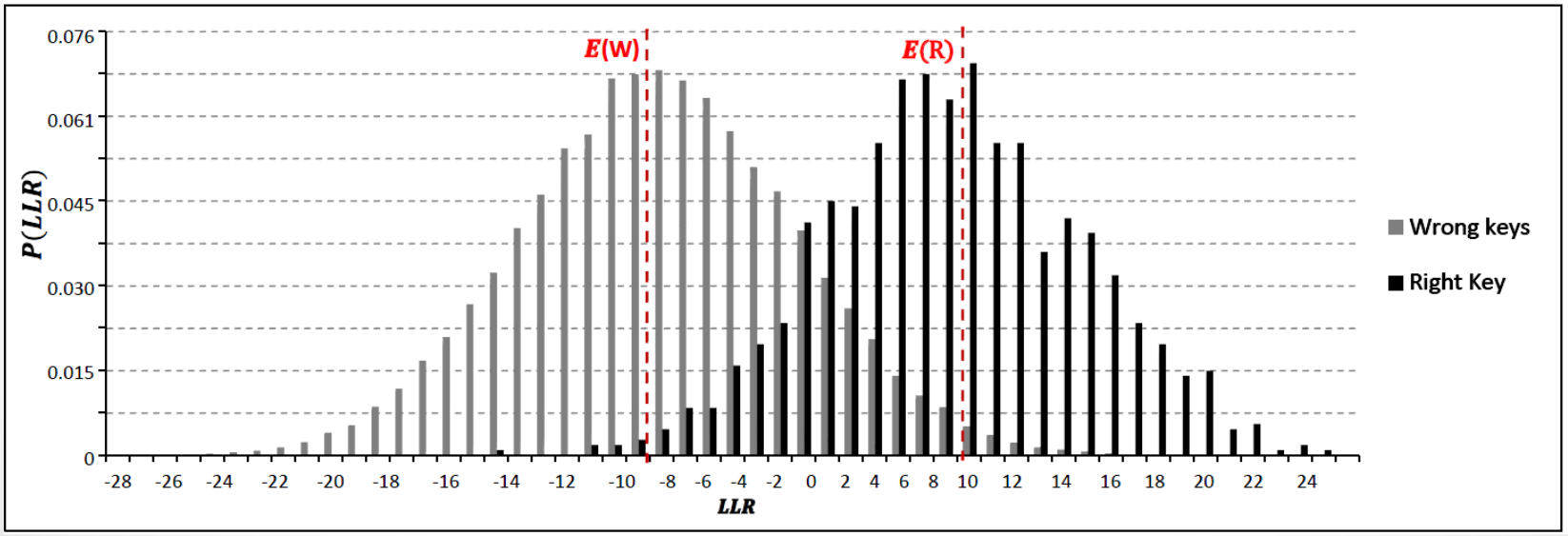
Experiments

- 12-round sample attack
  - $N = 2^{16}$ samples
  - The attack is repeated 100 times

Θ	$\mathbf{P}(R \geq \Theta)$	$\mathbf{P}(W \geq \Theta)$	N_{wk}	Empirical $\mathbf{P}(R \geq \Theta)$	Average empirical N_{wk}
2.6189	0.95	0.0021	143	0.94	154.07
5.6610	0.84	0.0002	14	0.87	15.16
7.1821	0.74	5.25e-05	4	0.73	3.68
8.7032	0.63	1.21e-05	0.79	0.61	0.92
10.2242	0.5	2.51e-06	0.16	0.45	0.19

Experiments

- The attack is repeated 1000 times
  - LLR distribution of the right key
  - The average LLR distribution of the wrong keys

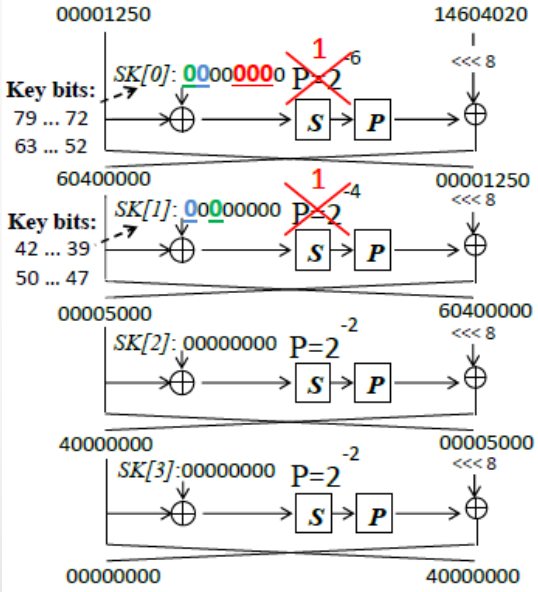


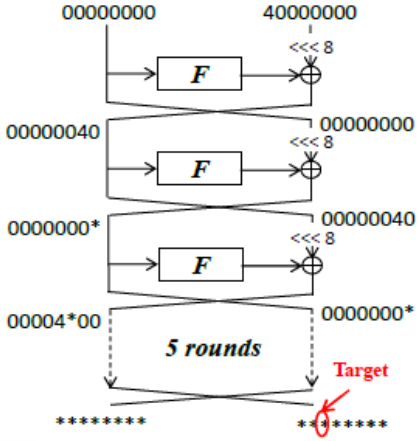
Outline

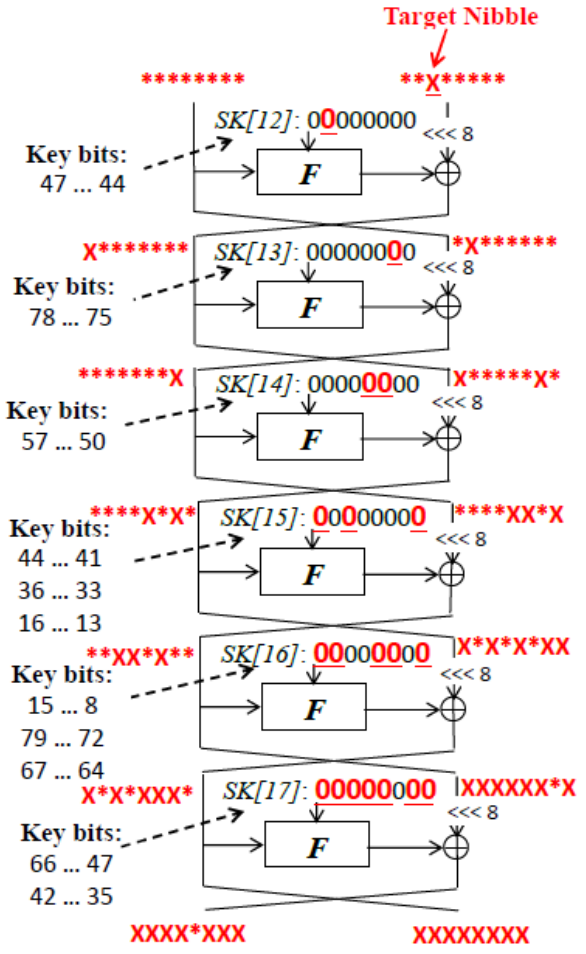
- Preliminaries
- Truncated differential distribution
- Truncated differential analysis of LBlock
- Complexity Analysis
- Experiments
- Results

Results

- 18-round single key attack
  - Data: 2^{23} plaintext/ciphertext pairs
  - Time: $2^{68.71}$ encryptions

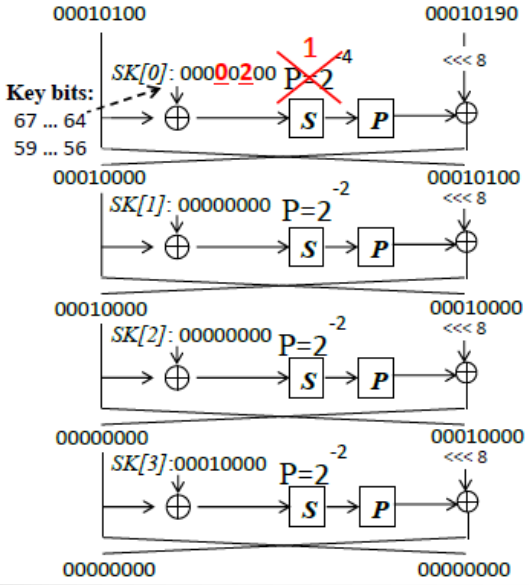


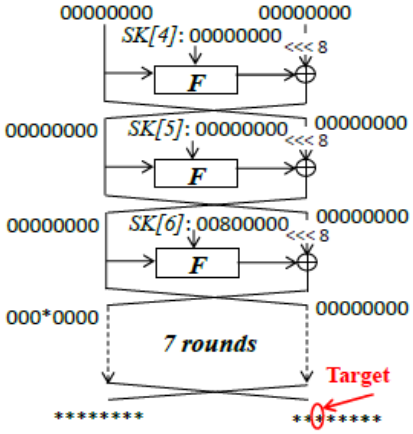


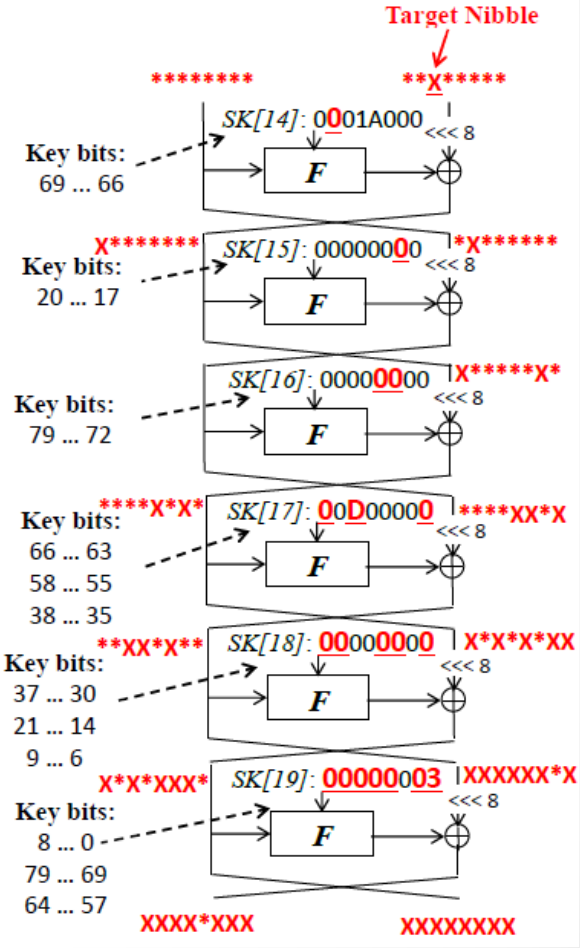


Results

- Related-key attacks
  - 20 rounds: Data: 2^{27}, time: $2^{74.55}$
  - 21 rounds: Data: 2^{30}, time: $2^{77.56}$







Thank you for your attention