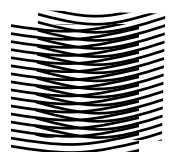
Differential Cryptanalysis in the Fixed-Key Model

Tim Beyne and Vincent Rijmen

imec-COSIC, ESAT, KULeuven

August 17, 2022

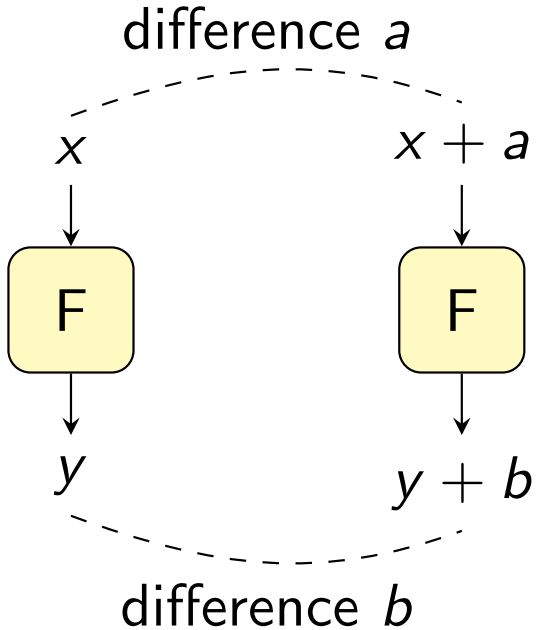


COSIC

Differential cryptanalysis

Differentials [Biham and Shamir, 1991]

- Differential $a \to b$ for a function $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$



How to estimate $p_{a \to b}$?

- Ideally, many x such that $\mathsf{F}(x + a) = \mathsf{F}(x) + b$
- 'Probability' of the differential $a \to b$:

$$p_{a \to b} = |\{x \in \mathbb{F}_2^n \mid \mathsf{F}(x + a) = \mathsf{F}(x) + b\}|/2^n$$

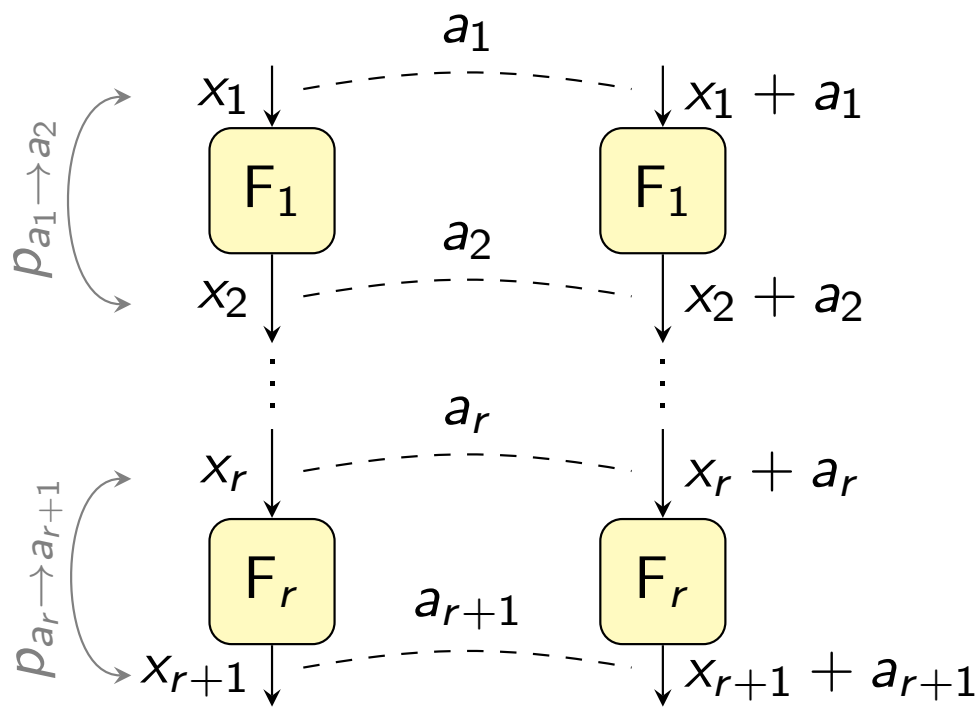
Differential cryptanalysis

Differential characteristics

- Sequence of intermediate differences for $F = F_r \circ \cdots \circ F_2 \circ F_1$
- Sum of probabilities of characteristics $(a_1, a_2, \ldots, a_{r+1})$:

$$p_{a_1 \to a_{r+1}} = \sum_{a_2,\ldots,a_r} p_{a_1 \to a_2 \to \cdots \to a_{r+1}}$$

- Heuristic: $p_{a_1 \to a_2 \to \cdots \to a_{r+1}} \approx p_{a_1 \to a_2} \times p_{a_2 \to a_3} \times \cdots \times p_{a_r \to a_{r+1}}$



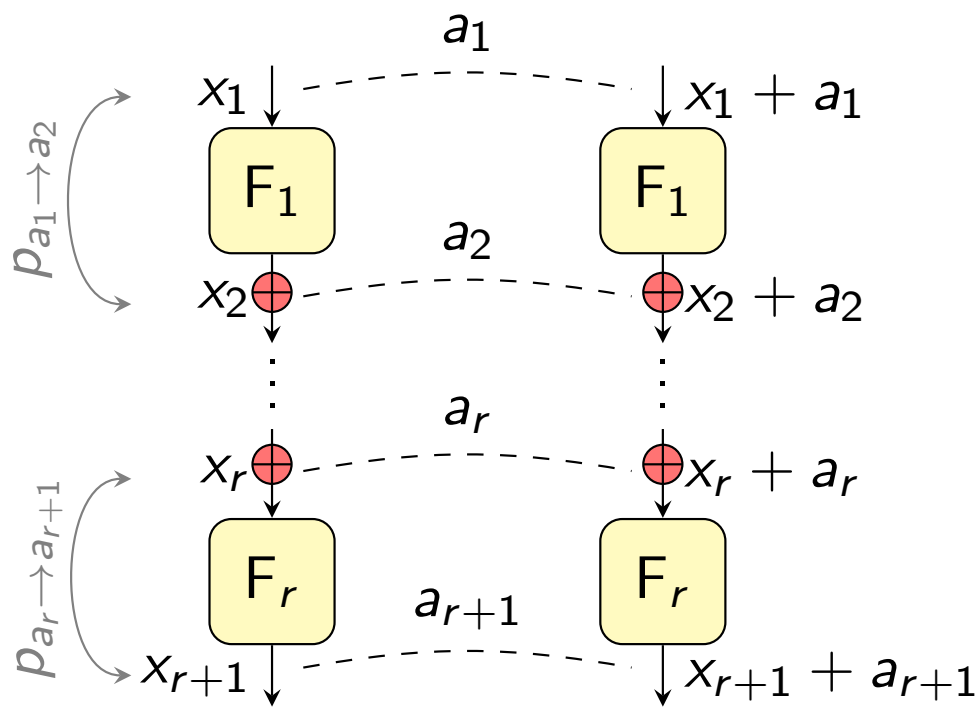
Differential cryptanalysis

Differential characteristics

- Sequence of intermediate differences for $F = F_r \circ \cdots \circ F_2 \circ F_1$
- Sum of probabilities of characteristics $(a_1, a_2, \ldots, a_{r+1})$:

$$p_{a_1 \to a_{r+1}} = \sum_{a_2,\ldots,a_r} p_{a_1 \to a_2 \to \cdots \to a_{r+1}}$$

- Heuristic: $p_{a_1 \to a_2 \to \cdots \to a_{r+1}} \approx p_{a_1 \to a_2} \times p_{a_2 \to a_3} \times \cdots \times p_{a_r \to a_{r+1}}$



Key-average is equal (for Markov ciphers)

$\overset{*}{\downarrow}$

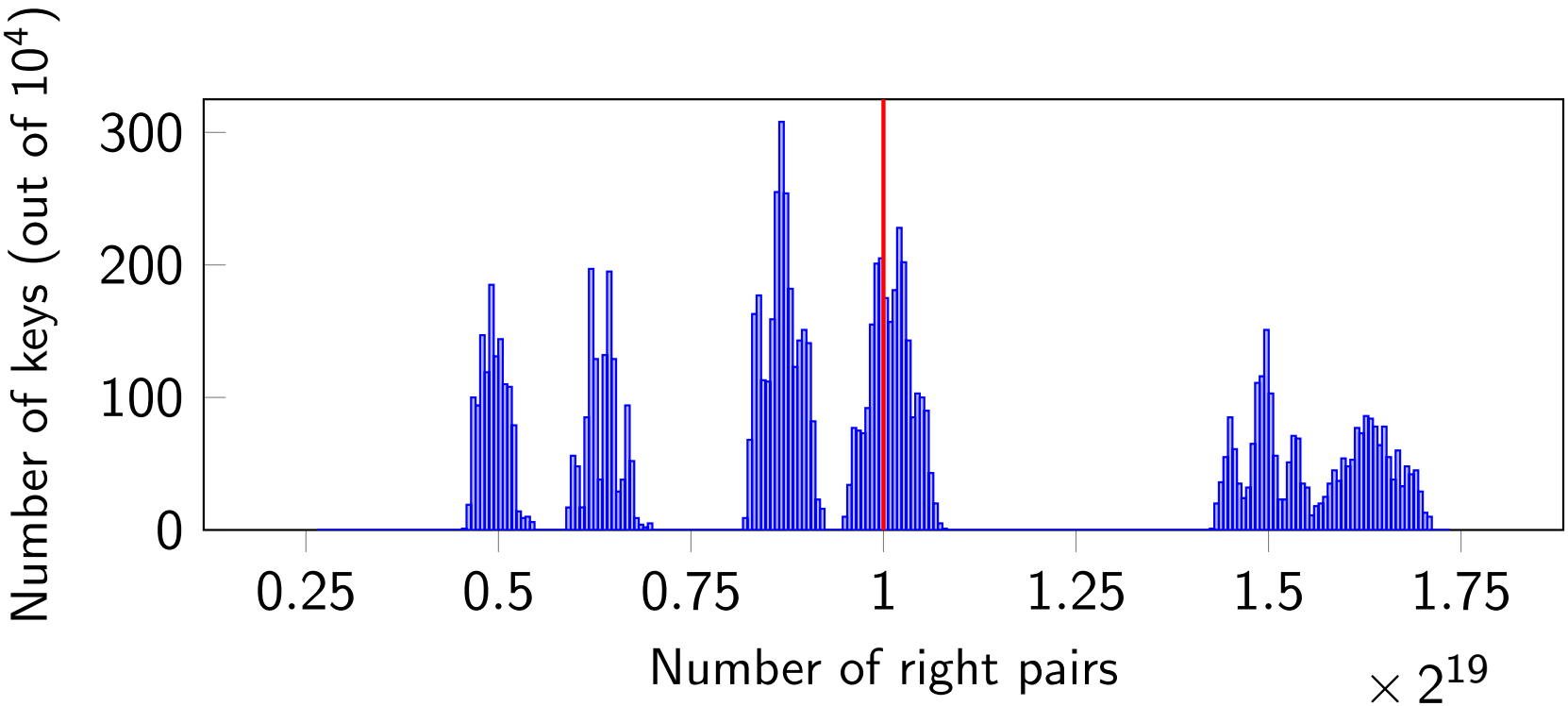
Fixed-key probability

*Hypothesis of stochastic equivalence

Differential cryptanalysis

Hypothesis of stochastic equivalence

- Six-round differential for SPECK-32 with $p_{a \to b} \approx 2^{-13}$



- For most keys, $p_{a \to b}$ *not* close to the average
- Using the average can lead to incorrect conclusions

Round key dependencies?

Overview

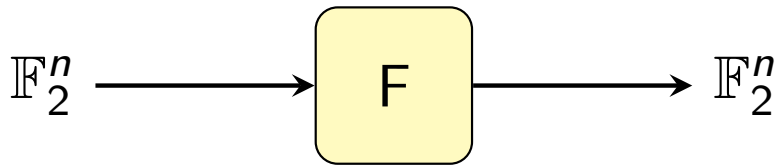
1. Quasidifferential transition matrices
2. Quasidifferential trails
3. Applications

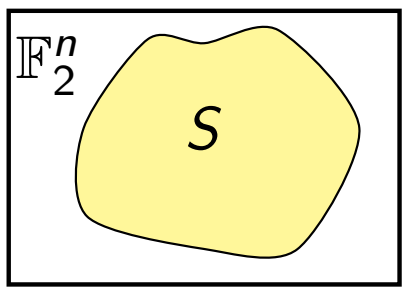
Quasidifferential transition matrices

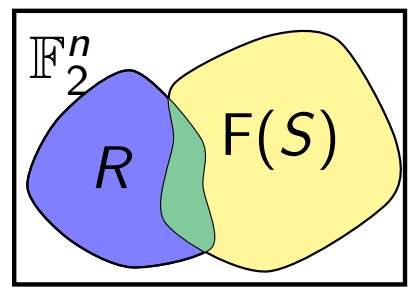
Recipe: geometric approach

- Permutation F on $\mathbb{F}_2^n$ (general case is similar)

- Counting using inner products of indicator functions







$\mathbb{1}_S : \mathbb{F}_2^n \to \mathbb{R}$

$$\mathbb{1}_S(x) = \begin{cases} 1 \text{ if } x \in S \\ 0 \text{ else} \end{cases}$$

$\mathbb{1}_R : \mathbb{F}_2^n \to \mathbb{R}$

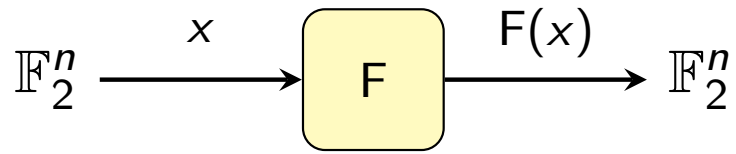
$$\mathbb{1}_R(x) = \begin{cases} 1 \text{ if } x \in R \\ 0 \text{ else} \end{cases}$$

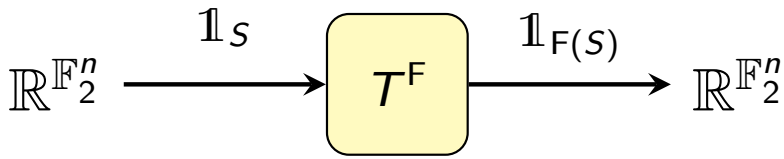
$$|R \cap \mathsf{F}(S)| = \sum_{x \in \mathbb{F}_2^n} \mathbb{1}_R(x) \mathbb{1}_{\mathsf{F}(S)}(x) = \langle \mathbb{1}_R, \mathbb{1}_{\mathsf{F}(S)} \rangle$$

Quasidifferential transition matrices

Transition matrices

- Permutation F on $\mathbb{F}_2^n$ (general case is similar)
- Propagation of indicator functions of sets





Matrix T^{F}: $T^{\mathsf{F}}\delta_x = \delta_{\mathsf{F}(x)}$

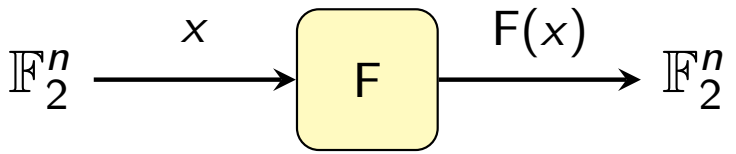
with $\delta_x(z) = \begin{cases} 1 \text{ if } z = x \\ 0 \text{ else} \end{cases}$

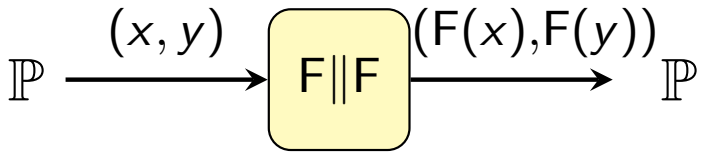
Quasidifferential transition matrices

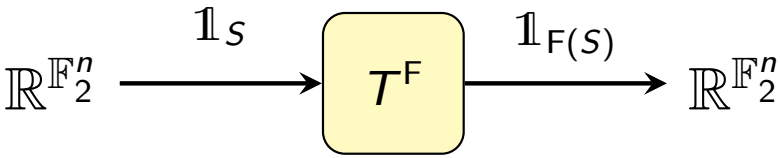
Transition matrices for pairs

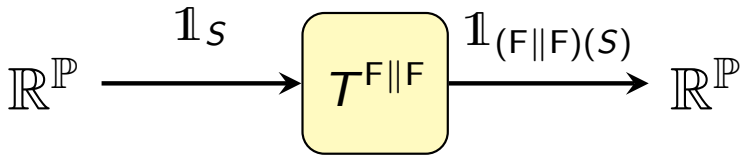
- Permutation F on $\mathbb{F}_2^n$ (general case is similar)
- Propagation of indicator functions of sets of pairs

$$\mathbb{P} = \mathbb{F}_2^n \times \mathbb{F}_2^n$$









Matrix T^{F}: $T^{\mathsf{F}}\delta_x = \delta_{\mathsf{F}(x)}$

with $\delta_x(z) = \begin{cases} 1 \text{ if } z = x \\ 0 \text{ else} \end{cases}$

Matrix $T^{\mathsf{F}\|\mathsf{F}}$: $T^{\mathsf{F}\|\mathsf{F}}\delta_{(x,y)} = \delta_{(\mathsf{F}(x),\mathsf{F}(y))}$

$T^{\mathsf{F}\|\mathsf{F}} = T^{\mathsf{F}} \otimes T^{\mathsf{F}}$

Quasidifferential transition matrices

Change-of-basis

- Transition matrix $T^{\mathsf{F}} \otimes T^{\mathsf{F}}$

  👍 Fully describes the propagation of sets of pairs

  👎 Not a practical way to compute the probablity of differentials

→ Change-of-basis to obtain a workable theory

Quasidifferential transition matrices

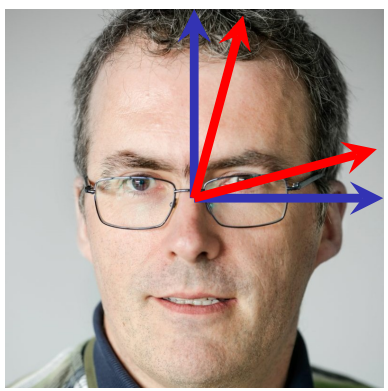
Change-of-basis

- Transition matrix $T^{\mathsf{F}} \otimes T^{\mathsf{F}}$

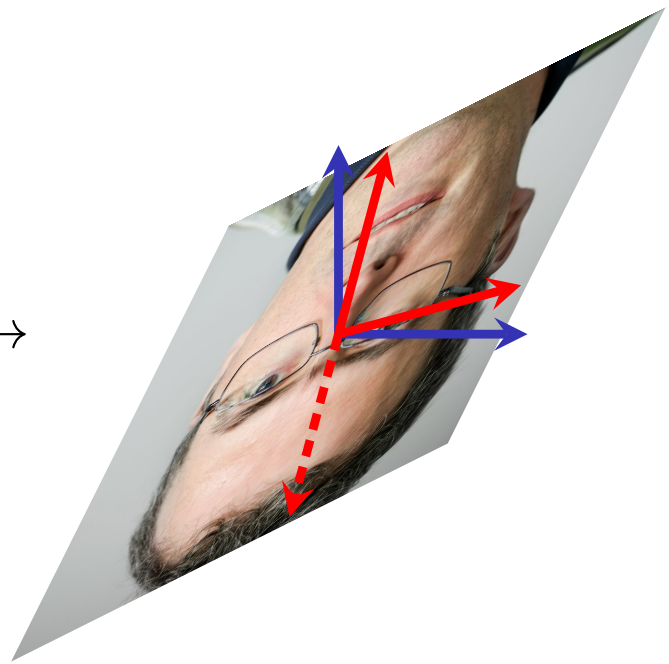
  👍 Fully describes the propagation of sets of pairs

  👎 Not a practical way to compute the probablity of differentials

➔ Change-of-basis to obtain a workable theory



$$\begin{bmatrix} 1.15 & -0.58 \\ 0.58 & -1.15 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



Quasidifferential transition matrices

Quasidifferential basis

- The new basis for $\mathbb{R}^{\mathbb{F}_2^n \times \mathbb{F}_2^n}$ should...
  - $\cdots$ include the functions $(x, y) \mapsto \delta_a(x + y)$, $a \in \mathbb{F}_2^n$
  - $\cdots$ be invariant under translation $(x, y) \mapsto (x + k, y + k)$, $k \in \mathbb{F}_2^n$

Quasidifferential transition matrices

Quasidifferential basis

- The new basis for $\mathbb{R}^{\mathbb{F}_2^n \times \mathbb{F}_2^n}$ should...
  - $\cdots$ include the functions $(x, y) \mapsto \delta_a(x + y)$, $a \in \mathbb{F}_2^n$
  - $\cdots$ be invariant under translation $(x, y) \mapsto (x + k, y + k)$, $k \in \mathbb{F}_2^n$
- Basis $\{\beta_{u,a} \mid (u, a) \in \mathbb{F}_2^n \times \mathbb{F}_2^n\}$ with

$$\beta_{u,a}(x, y) = \chi_u(x)\delta_a(x + y)$$

where $\chi_u(x) = (-1)^{u^\mathsf{T} x}$ is an additive character of $\mathbb{F}_2^n$

Quasidifferential transition matrices

Quasidifferential basis

- The new basis for $\mathbb{R}^{\mathbb{F}_2^n \times \mathbb{F}_2^n}$ should...
  - $\cdots$ include the functions $(x, y) \mapsto \delta_a(x + y)$, $a \in \mathbb{F}_2^n$
  - $\cdots$ be invariant under translation $(x, y) \mapsto (x + k, y + k)$, $k \in \mathbb{F}_2^n$
- Basis $\{\beta_{u,a} \mid (u, a) \in \mathbb{F}_2^n \times \mathbb{F}_2^n\}$ with

$$\beta_{u,a}(x+k, y+k) = \chi_u(k)\chi_u(x)\delta_a(x + y)$$

where $\chi_u(x) = (-1)^{u^\mathsf{T} x}$ is an additive character of $\mathbb{F}_2^n$

Quasidifferential transition matrices

Definition

- Quasidifferential transition matrix of $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ $= T^{\mathsf{F}} \otimes T^{\mathsf{F}}$ expressed in the basis consisting of $\beta_{u,a}$

$$D^{\mathsf{F}} = Q_m (T^{\mathsf{F}} \otimes T^{\mathsf{F}}) Q_n^{-1}$$

with Q_n and Q_m the change-of-basis matrices

- Coordinates of D^{F} are indexed by 'mask-difference pairs' (u, a)

$$D^{\mathsf{F}}_{(v,b),(u,a)} = \left(2 \Pr_{\boldsymbol{x}}[u^{\mathsf{T}}\boldsymbol{x} + v^{\mathsf{T}}\mathsf{F}(\boldsymbol{x}) = 0 \mid \mathsf{F}(\boldsymbol{x}+a) = \mathsf{F}(\boldsymbol{x}) + b] - 1\right) p_{a \to b}\,,$$

with $\boldsymbol{x}$ uniform random on $\mathbb{F}_2^n$

Quasidifferential transition matrices

Definition

- Quasidifferential transition matrix of $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ $= T^{\mathsf{F}} \otimes T^{\mathsf{F}}$ expressed in the basis consisting of $\beta_{u,a}$

$$D^{\mathsf{F}} = Q_m (T^{\mathsf{F}} \otimes T^{\mathsf{F}}) Q_n^{-1}$$

with Q_n and Q_m the change-of-basis matrices

- Coordinates of D^{F} are indexed by 'mask-difference pairs' (u, a)

$$D^{\mathsf{F}}_{(v,b),(u,a)} = \left(2 \Pr_{\boldsymbol{x}}[u^{\mathsf{T}}\boldsymbol{x} + v^{\mathsf{T}}\mathsf{F}(\boldsymbol{x}) = 0 \mid \mathsf{F}(\boldsymbol{x}+a) = \mathsf{F}(\boldsymbol{x}) + b] - 1\right) p_{a \to b},$$

with $\boldsymbol{x}$ uniform random on $\mathbb{F}_2^n$

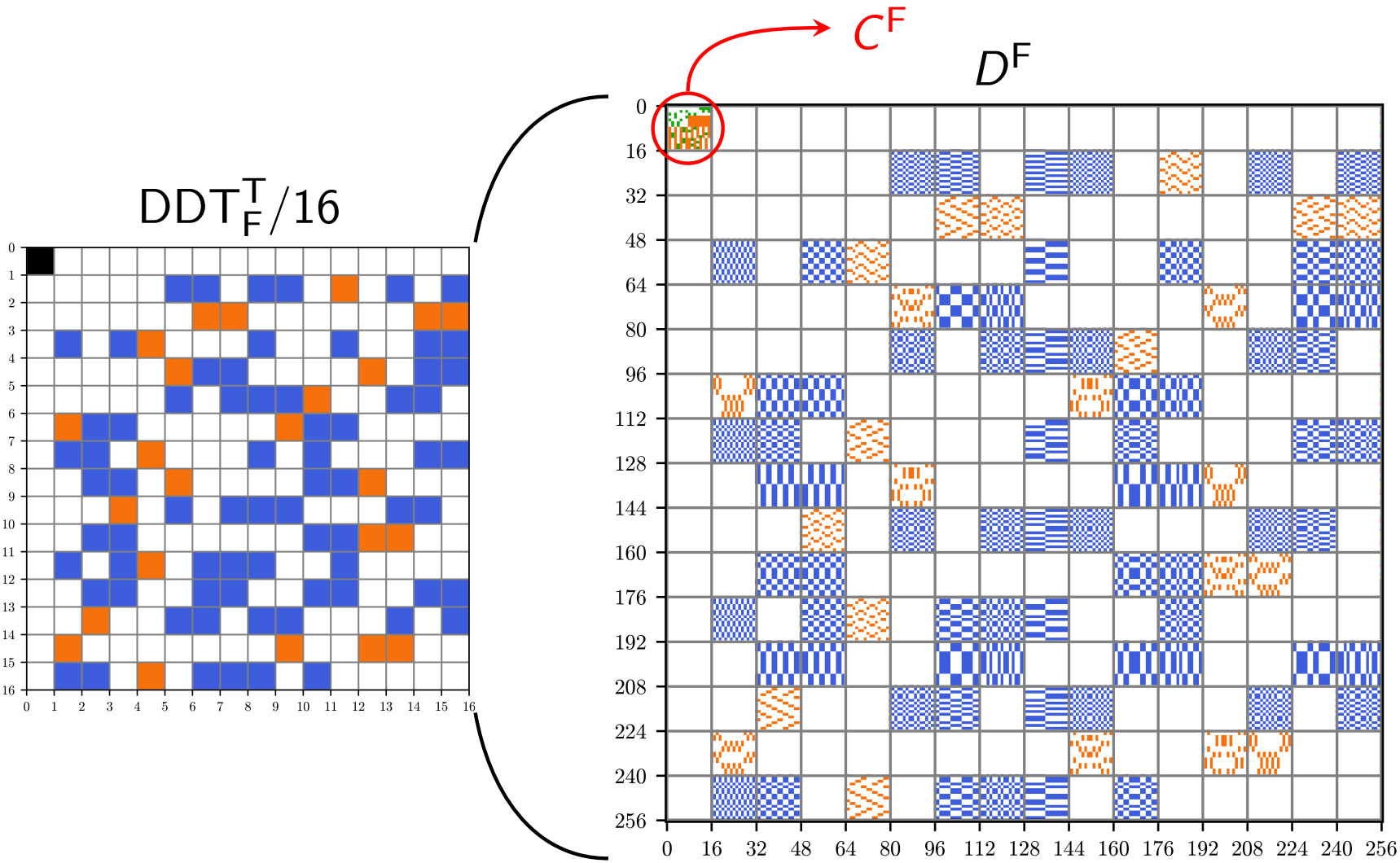
'Linear cryptanalysis on the set of right values'

Quasidifferential transition matrices

Properties

- D^{F} contains difference-distribution table: $D^{\mathsf{F}}_{(0,b),(0,a)} = p_{a \to b}$

correlation matrix C^{F}



Overview

1. Quasidifferential transition matrices
   Transition matrix for pairs w.r.t. the quasidifferential basis

2. Quasidifferential trails

3. Applications

Quasidifferential trails

Probability of a differential

- Quasidifferential trail for $\mathsf{F} = \mathsf{F}_r \circ \cdots \circ \mathsf{F}_2 \circ \mathsf{F}_1$:
  sequence $\varpi_1, \ldots, \varpi_{r+1}$ of mask-difference pairs $\varpi_i = (u_i, a_i)$
- Correlation of a trail: $\prod_{i=1}^{r} D^{\mathsf{F}_i}_{\varpi_{i+1},\varpi_i}$
- From $D^{\mathsf{F}} = D^{\mathsf{F}_r} \cdots D^{\mathsf{F}_2} D^{\mathsf{F}_1}$, it follows that

$$D^{\mathsf{F}}_{\varpi_{r+1},\varpi_1} = \sum_{\varpi_2,\ldots,\varpi_r} \prod_{i=1}^{r} D^{\mathsf{F}_i}_{\varpi_{i+1},\varpi_i}$$

- With $\varpi_1 = (0, a)$ and $\varpi_{r+1} = (0, b)$, this gives $p_{a \to b}$
- Consider only trails with $u_i = 0 \rightarrow$ standard theory

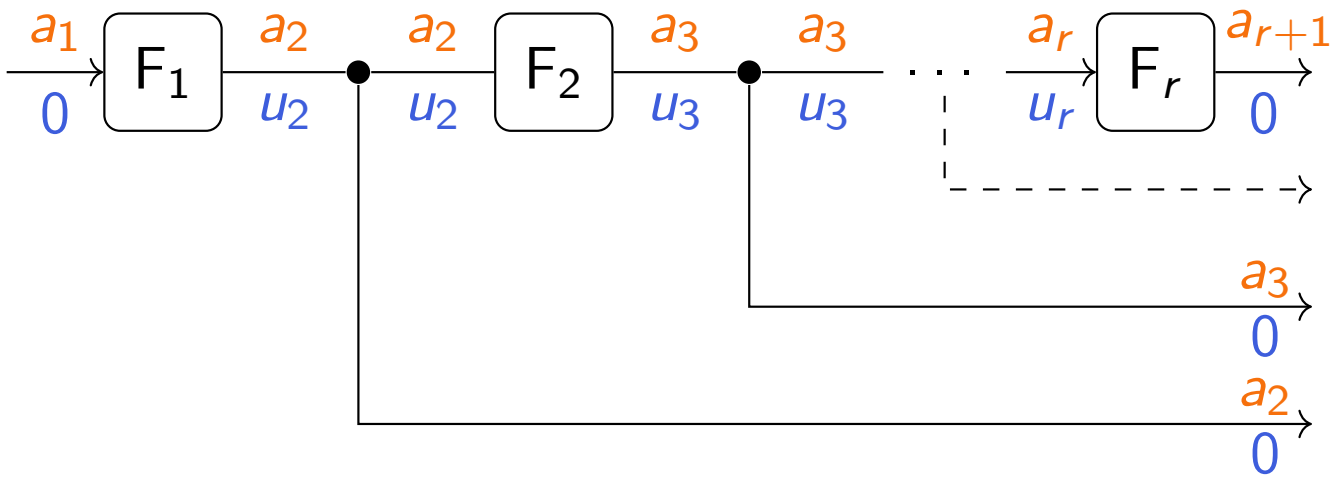
Quasidifferential trails

Probability of a differential characteristic

- Probability of a *characteristic* $a_1 \to a_2 \to \cdots \to a_{r+1}$:

$$p_{a_1 \to a_2 \to \cdots \to a_{r+1}} = \sum_{u_2,\ldots,u_r} \prod_{i=1}^{r} D^{\mathsf{F}_i}_{(u_{i+1},a_{i+1}),(u_i,a_i)}$$

- Graphical proof



$$D^{\mathsf{L}}_{(v,b),(u,a)} = \delta_u(\mathsf{F}^{\mathsf{T}}(v))\delta_b(\mathsf{F}(a)) \text{ for linear L}$$

Overview

1. Quasidifferential transition matrices
   Transition matrix for pairs w.r.t. the quasidifferential basis

2. Quasidifferential trails
   Sequences $\varpi_1, \ldots, \varpi_{r+1}$ of mask-difference pairs

3. Applications

Applications
Overview

- Search problem is similar to finding linear trails
  - In this paper: SMT modelling
  - For n to m bit functions: $\mathcal{O}((n+m)2^{2n+2m})$-time algorithm
  - Formula for modular additions

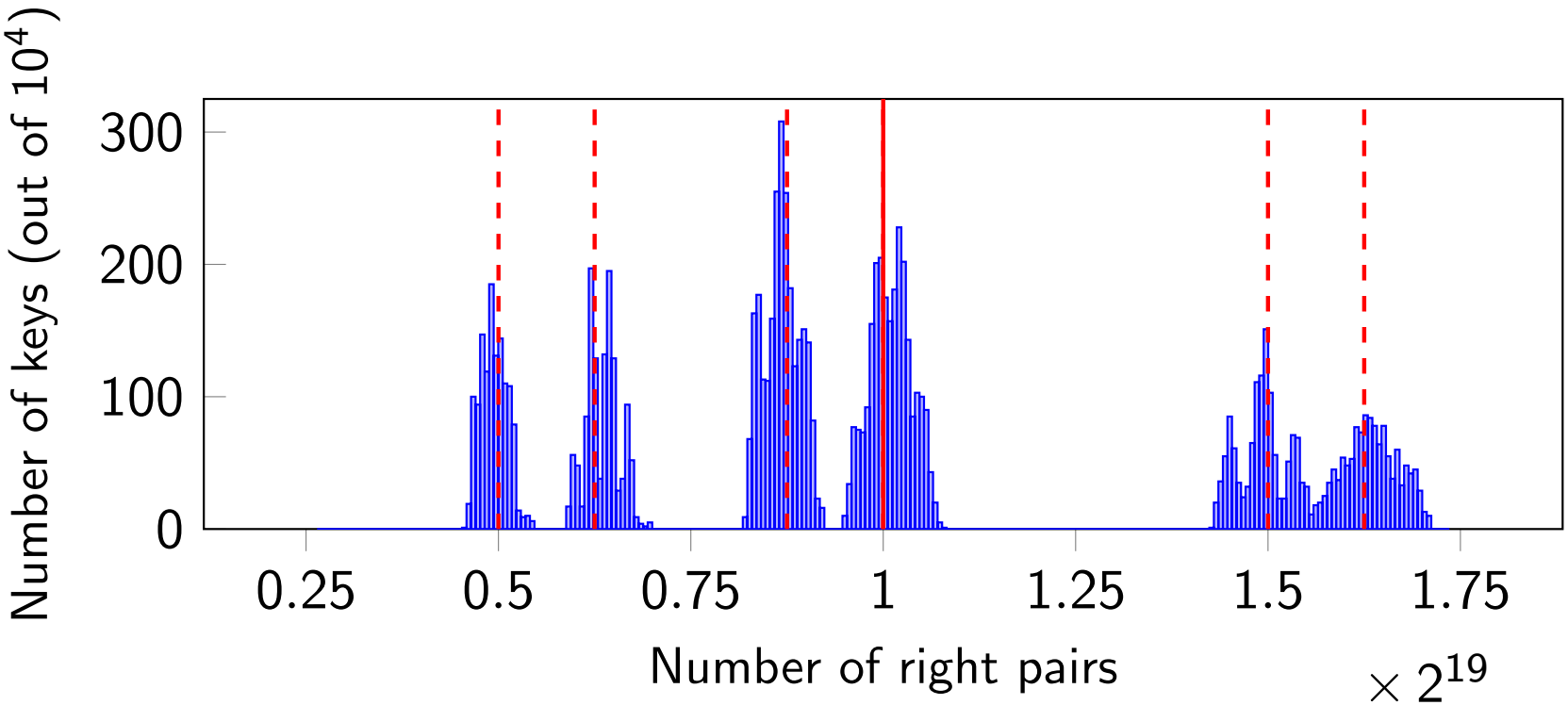
- Examples:
  - RECTANGLE
    best-known attack does not work [Zhang et al., 2015]
  - KNOT
    proposed collision attacks do not work [Zhang et al., 2020]
  - SPECK (next slides)
    analysis of key-recovery attacks [Dinur, 2014] and follow-up

Applications

Six round differential for SPECK-32

- Five quasidifferential trails with largest absolute correlation:

$$p_{a\to b} \approx 2^{-13} + (-1)^{0003^{\mathsf{T}}k_5}\, 2^{-15} + (-1)^{0180^{\mathsf{T}}k_5}\, 2^{-15} + (-1)^{0183^{\mathsf{T}}k_5}\, 2^{-17} + (-1)^{0102^{\mathsf{T}}k_5}\, 2^{-17}$$



Applications

SPECK

- Experiments from [Ankele and Kölbl, 2019]:
  explanation with two quasidifferential trails

- Analysis of several key-recovery several attacks
  [Dinur, 2014, Abed et al., 2015, Song et al., 2016]

  - Most attacks work only for some keys (typically $\leq 1/4$)
    ❗ SPECK-96: only $1/64$ keys

  - For these keys, the data-complexity is lower than expected

ℹ Selection of the differentials was only based on their use in the best known attacks on different variants of SPECK

Conclusions

1. Quasidifferential transition matrices
   Transition matrix for pairs w.r.t. the quasidifferential basis
2. Quasidifferential trails
   Sequences $\varpi_1, \ldots, \varpi_{r+1}$ of mask-difference pairs
3. Applications
   Automated analysis (SMT) of RECTANGLE, KNOT and SPECK

- Future work: analyze attacks, improve tools, clustering, ...


`https://github.com/TimBeyne/quasidifferential-trails`


`tim.beyne@esat.kuleuven.be`