A geometric approach to symmetric-key cryptanalysis

Tim Beyne

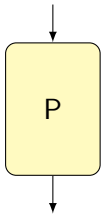
tim@cryptanalysis.info

KU Leuven

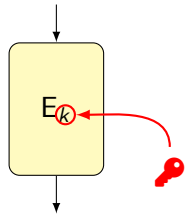
August 18, 2023

Primitives

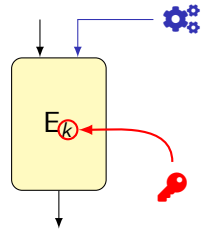
Permutations



Block ciphers

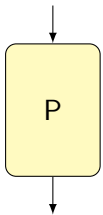


Tweakable block ciphers

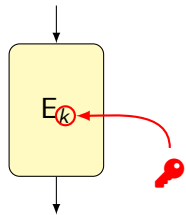


Primitives

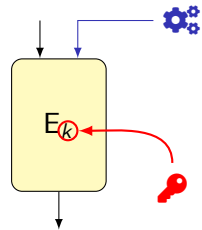
Permutations



Block ciphers



Tweakable block ciphers



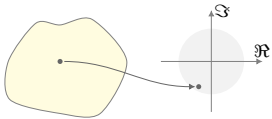
How do we know these are secure?

Cryptanalysis

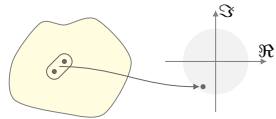
Overview

Geometric approach

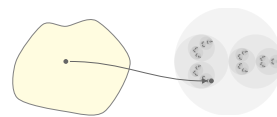
Linear cryptanalysis



Differential cryptanalysis



Integral cryptanalysis



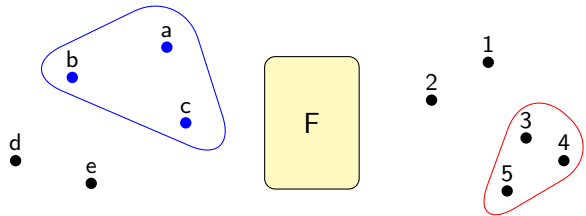
Failures of (academic) cryptanalysis

1. Lack of unification
   - ➔ Duplication of effort

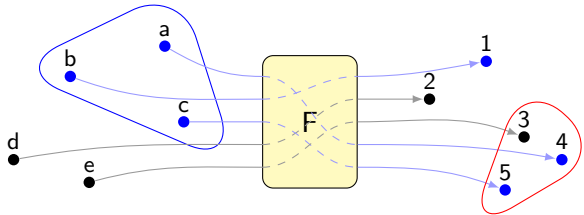
2. Lack of urgency to investigate assumptions
   - ➔ Errors, missed opportunities

3. Lack of perspective
   - ➔ Few proposals of general cryptanalytic methods

Geometric approach

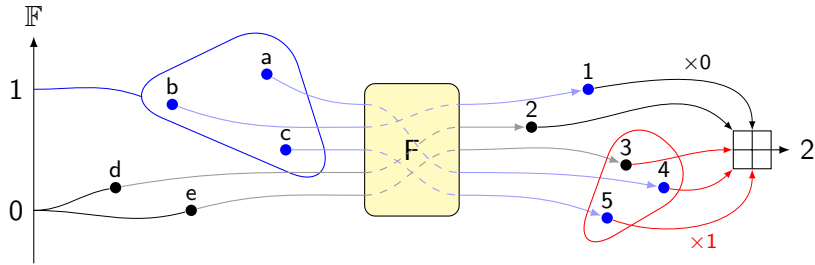


Geometric approach



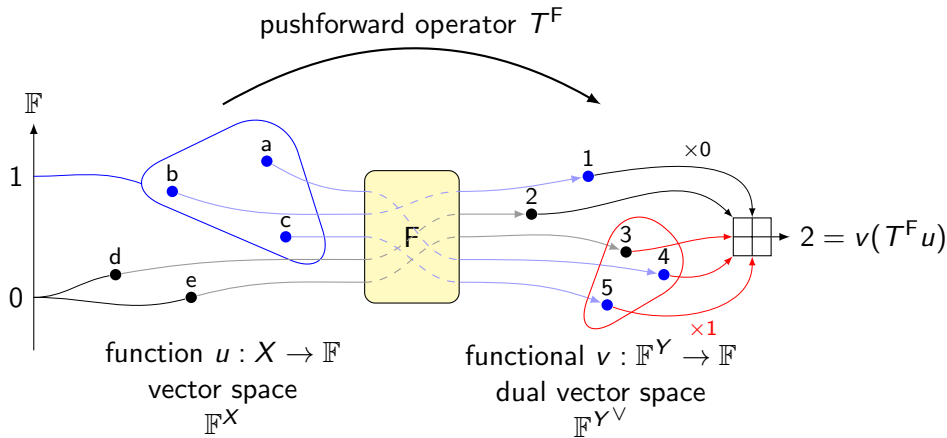
Geometric approach

- Assign a weight to every possible input in $X = \{a, b, c, d, e\}$
- Compute weighted combinations of the outputs in $Y = \{1, 2, 3, 4, 5\}$



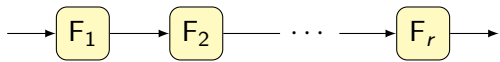
Geometric approach

- Assign a weight to every possible input in $X = \{a, b, c, d, e\}$
- Compute weighted combinations of the outputs in $Y = \{1, 2, 3, 4, 5\}$



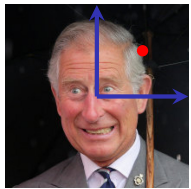
Pushforward operator

- Evaluating $v(T^{\mathsf{F}}u)$ directly is not feasible for real ciphers
- Iterated structure of F:

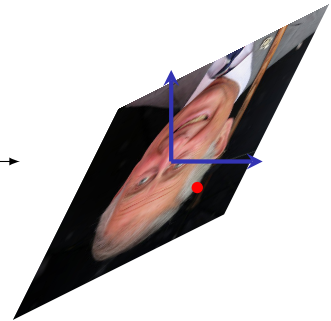


$$T^{\mathsf{F}} = T^{\mathsf{F}_r} \dots T^{\mathsf{F}_2} T^{\mathsf{F}_1}$$

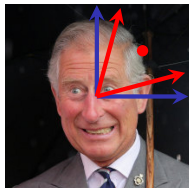
Change-of-basis



$$\begin{bmatrix} 1.15 & -0.58 \\ 0.58 & -1.15 \end{bmatrix}$$

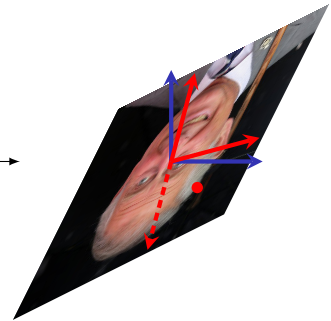


Change-of-basis

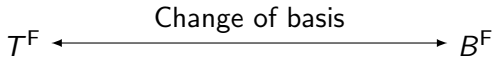


$$\begin{bmatrix} 1.15 & -0.58 \\ 0.58 & -1.15 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



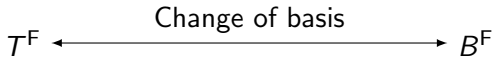
Relative pushforward operators



$$T^{\mathsf{F}} = T^{\mathsf{F}_r} \dots T^{\mathsf{F}_2} T^{\mathsf{F}_1} \qquad B^{\mathsf{F}} = B^{\mathsf{F}_r} \dots B^{\mathsf{F}_2} B^{\mathsf{F}_1}$$

- With the right change of basis, this makes it easier to estimate $v(T^{\mathsf{F}} u) = \widehat{v}(B^{\mathsf{F}} \widehat{u})$

Relative pushforward operators



$$T^{\mathsf{F}} = T^{\mathsf{F}_r} \dots T^{\mathsf{F}_2} T^{\mathsf{F}_1} \qquad B^{\mathsf{F}} = B^{\mathsf{F}_r} \dots B^{\mathsf{F}_2} B^{\mathsf{F}_1}$$

- With the right change of basis, this makes it easier to estimate $v(T^{\mathsf{F}} u) = \widehat{v}(B^{\mathsf{F}} \widehat{u})$
- When $u = b_{\beta_1}$ and $v = b^{\beta_{r+1}}$ are basis functions:

$$b^{\beta_{r+1}}(T^{\mathsf{F}} b_{\beta_1}) = B^{\mathsf{F}}_{\beta_{r+1},\beta_1} = \sum_{\beta_2,\dots,\beta_r} \prod_{i=1}^{r} B^{\mathsf{F}_i}_{\beta_{i+1},\beta_i}$$

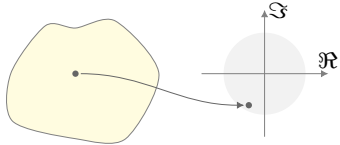
Trail correlation

- A sequence $(\beta_1, \dots, \beta_{r+1})$ of basis function labels is a 'trail'

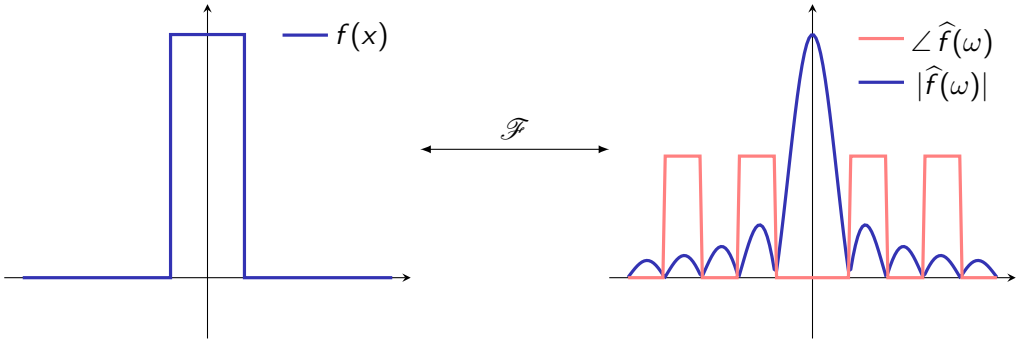
Multidimensional theory

- Cryptanalytic property of $\mathsf{F} : X \to Y$ is a pair (U, V)
  - Vector space of functions $U \subseteq \mathbb{F}^X$
  - Vector space of linear functionals $V \subseteq \mathbb{F}^{Y^\vee}$
- Evaluation at $u \in U$ and $v \in V$ is $v\left(T^{\mathsf{F}} u\right)$
- 'Basis-free' definition of trails will not be discussed today

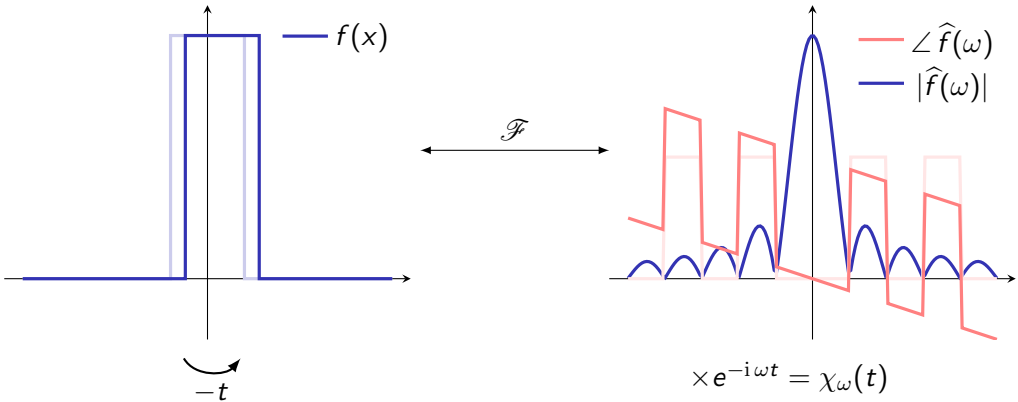
Linear cryptanalysis



Fourier transformation



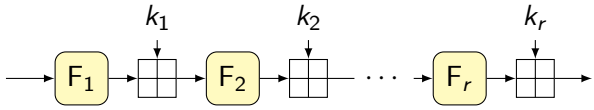
Fourier transformation



Fourier transformation diagonalizes translation

Geometric approach to linear cryptanalysis

- Fourier transformation exists for any finite Abelian group (e.g. $\mathbb{Z}/N\mathbb{Z}$)



$$T^{\mathsf{F}} = T^{k_r} T^{\mathsf{F}_r} \cdots T^{k_2} T^{\mathsf{F}_2} T^{k_1} T^{\mathsf{F}_1}$$

$$\Updownarrow \mathscr{F}$$

$$C^{\mathsf{F}} = C^{k_r} C^{\mathsf{F}_r} \cdots C^{k_2} C^{\mathsf{F}_2} C^{k_1} C^{\mathsf{F}_1}$$

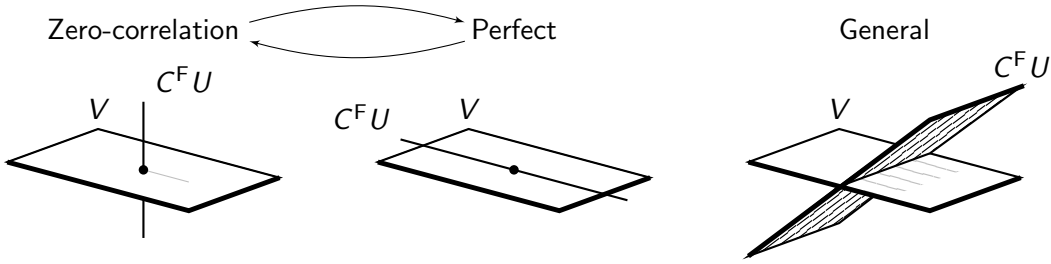
- Correlation matrices C^{F_i}
- Expanding the matrix product gives linear trails

$$C^{\mathsf{F}}_{\chi_{r+1},\chi_1} = \sum_{\chi_2,\cdots,\chi_r} \prod_{i=1}^{r} \chi_{i+1}(k_i) C^{\mathsf{F}_i}_{\chi_{i+1},\chi_i}$$

Lack of unification

Geometric approach to linear cryptanalysis

Multidimensional theory



$C^{\mathsf{F}}U \perp V$

- Zero-correlation linear approximations
- Multidimensional $\sim$

$C^{\mathsf{F}}U \subseteq V$

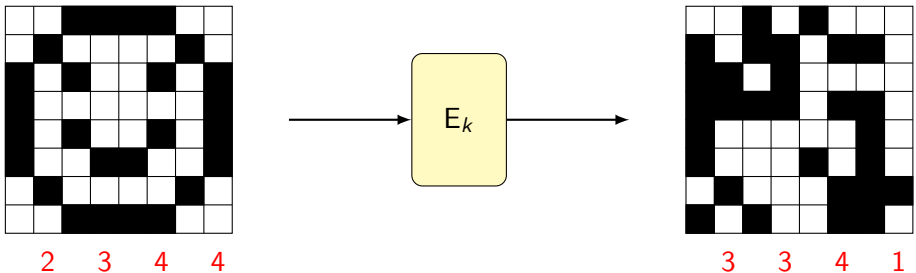
- Saturation attacks
- Invariant subspaces
- Nonlinear invariants

$\langle V, U \rangle_{\mathsf{F}}$

- (Non)linear approximations
- Multiple $\sim$
- Multidimensional $\sim$
- Partitioning

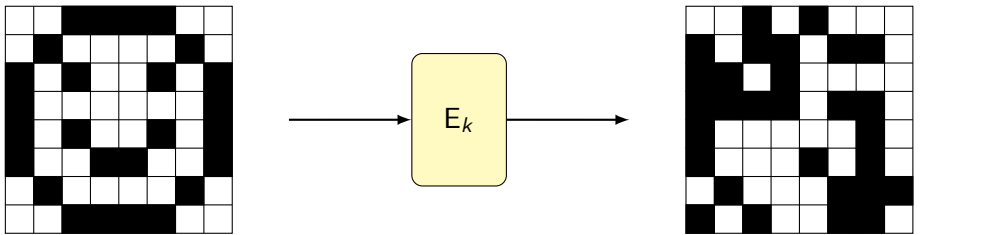
Invariants

Example: Midori-64*



Invariants

Example: Midori-64*

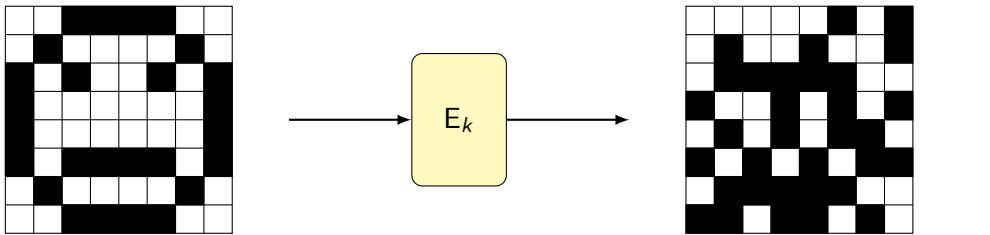


$2 + 3 + 4 + 4 = \text{odd}$

$3 + 3 + 4 + 1 = \text{odd}$

Invariants

Example: Midori-64*

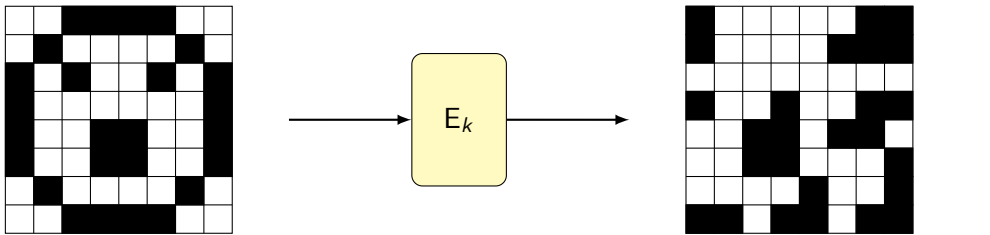


$2 + 3 + 4 + 4 = \text{odd}$
$2 + 3 + 4 + 4 = \text{odd}$

$3 + 3 + 4 + 1 = \text{odd}$
$5 + 5 + 5 + 4 = \text{odd}$

Invariants

Example: Midori-64*

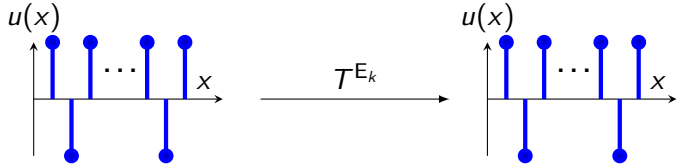


$2 + 3 + 4 + 4 = \text{odd}$
$2 + 3 + 4 + 4 = \text{odd}$
$2 + 4 + 3 + 4 = \text{odd}$

$3 + 3 + 4 + 1 = \text{odd}$
$5 + 5 + 5 + 4 = \text{odd}$
$1 + 4 + 2 + 6 = \text{odd}$

Invariants

Geometric approach

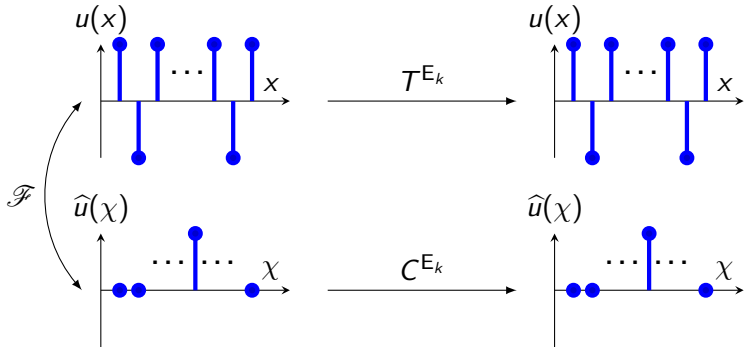


$$\begin{bmatrix} & T^{\mathsf{E}_k} & \end{bmatrix} \begin{bmatrix} u \end{bmatrix} = \begin{bmatrix} u \end{bmatrix}$$

invariants are eigenvectors

Invariants

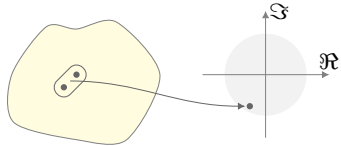
Geometric approach



$$\begin{bmatrix} \\ C^{\mathsf{E}_k} \\ \\ \end{bmatrix} \begin{bmatrix} \\ \widehat{u} \\ \\ \end{bmatrix} = \begin{bmatrix} \\ \widehat{u} \\ \\ \end{bmatrix}$$

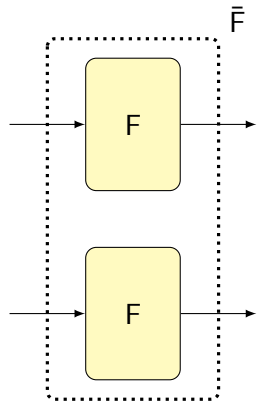
invariants are eigenvectors

Differential cryptanalysis



Pairs of values

- Assign weights (complex numbers) to all pairs of values

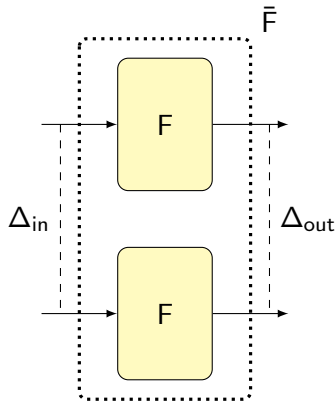


$T^{\bar{\mathsf{F}}} = T^{\mathsf{F}} \otimes T^{\mathsf{F}}$

pushforward operator for pairs

Pairs of values

- Assign weights (complex numbers) to all pairs of values



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

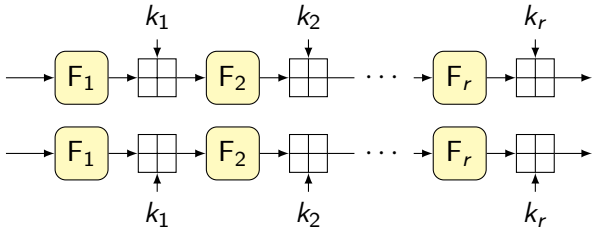
pushforward operator for pairs

Geometric approach to differential cryptanalysis

- Quasidifferential basis functions $(x, y) \mapsto \chi(x)\delta_a(y - x)$

Constant-difference pairs

Fourier basis



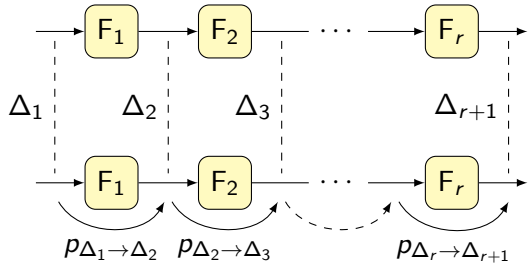
$$T^{\bar{\mathsf{F}}} = T^{\bar{k}_r} T^{\bar{\mathsf{F}}_r} \cdots T^{\bar{k}_2} T^{\bar{\mathsf{F}}_2} T^{\bar{k}_1} T^{\bar{\mathsf{F}}_1}$$

$$\Updownarrow \mathscr{D}$$

$$D^{\mathsf{F}} = D^{k_r} D^{\mathsf{F}_r} \cdots D^{k_2} D^{\mathsf{F}_2} D^{k_1} D^{\mathsf{F}_1}$$

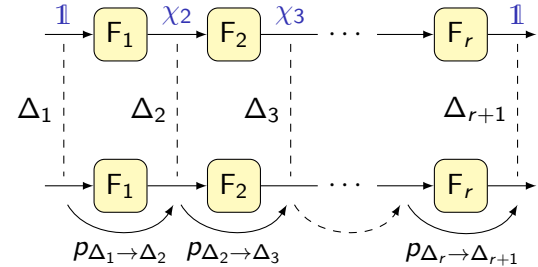
Lack of urgency to investigate assumptions

Independence assumptions



$$\text{probability} = \sum_{\Delta_2,\ldots,\Delta_r} p_{\Delta_1\to\Delta_2} \times p_{\Delta_2\to\Delta_3} \times \cdots \times p_{\Delta_r\to\Delta_{r+1}}$$

Independence assumptions



$$\text{probability} = \sum_{\Delta_2,\ldots,\Delta_r} \cancel{p_{\Delta_1 \to \Delta_2} \times p_{\Delta_2 \to \Delta_3} \times \cdots \times p_{\Delta_r \to \Delta_{r+1}}}$$

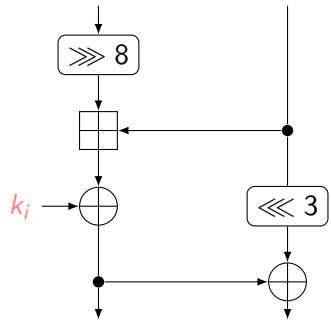
$$= \sum_{\substack{\Delta_2,\ldots,\Delta_r \\ \chi_2,\ldots,\chi_r}} D^{F_1}_{(\chi_2,\Delta_2),(\mathbb{1},\Delta_1)} \times D^{F_2}_{(\chi_3,\Delta_3),(\chi_2,\Delta_2)} \times \cdots \times D^{F_r}_{(\mathbb{1},\Delta_{r+1}),(\chi_r,\Delta_r)}$$

Independence assumptions

[Ankele and Kölbl (SAC 2018)]

Example: differential for 7-round Speck-64

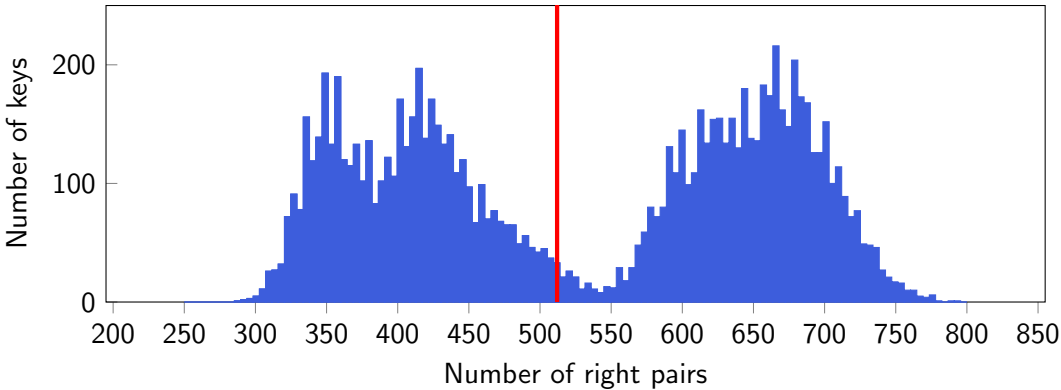
- Differential (4004092 104204, 8080a080 8481a4a) for 7-round Speck-64
- Dominant characteristic with naive probability 2^{-21}



Independence assumptions

Example: differential for 7-round Speck-64

$$4004092\ \ 1042004 \xrightarrow{\text{Probability } 2^{-21}?} 8080a080\ \ 8481a4a$$

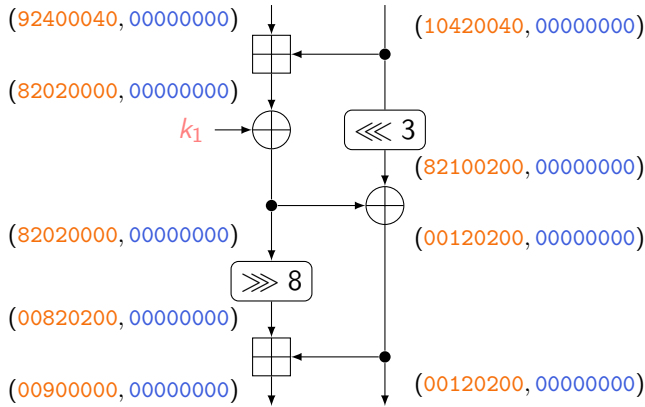


- 10000 keys, 2^{30} pairs per key

Independence assumptions

Example: differential for 7-round Speck-64

- Quasidifferential trails over the first two rounds

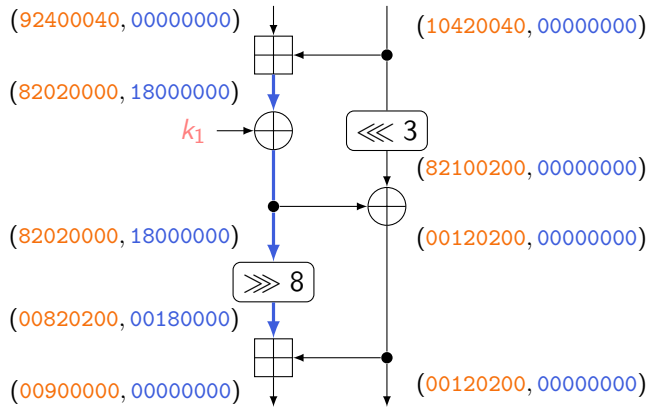


2^{-9}

Independence assumptions

Example: differential for 7-round Speck-64

- Quasidifferential trails over the first two rounds

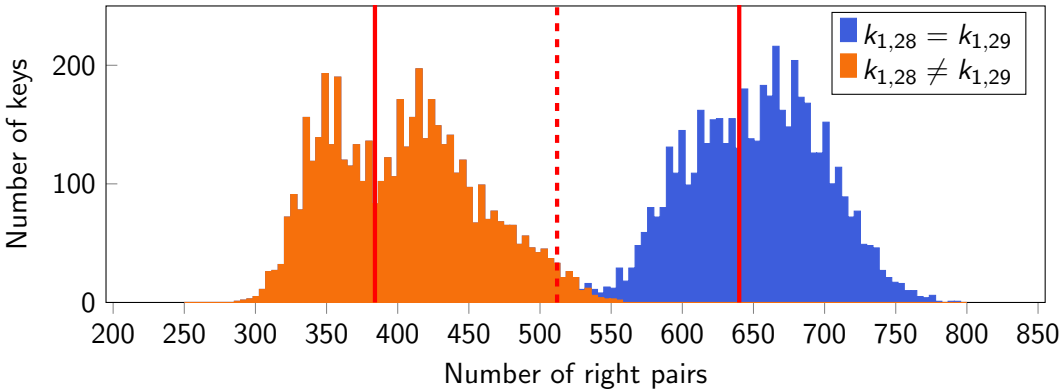


$$2^{-9} + (-1)^{k_{1,28}+k_{1,29}}\, 2^{-11}$$

Independence assumptions

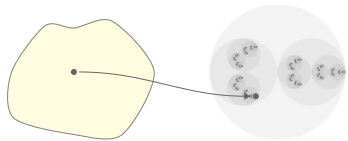
Example: differential for 7-round Speck-64

4004092 1042004 $\xrightarrow{\text{Probability } 2^{-21} + (-1)^{k_{1,28}+k_{1,29}} 2^{-23}}$ 8080a080 8481a4a



- 10000 keys, 2^{30} pairs per key

Integral cryptanalysis

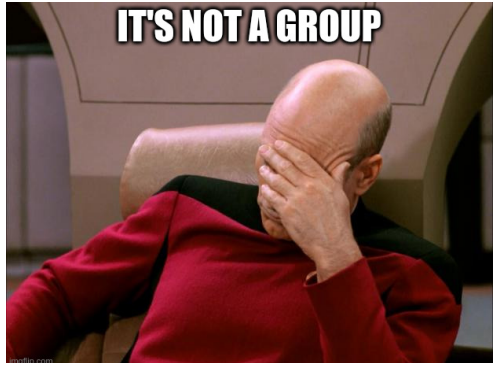


Geometric approach to integral cryptanalysis

- The Fourier transformation simplifies additions
  What about multiplications?

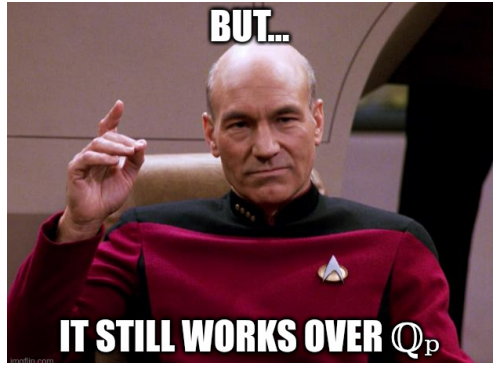
Geometric approach to integral cryptanalysis

- The Fourier transformation simplifies additions
  What about multiplications?



Geometric approach to integral cryptanalysis

- The Fourier transformation simplifies additions
  What about multiplications?

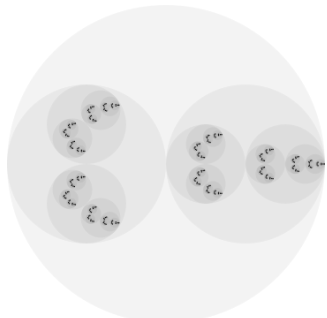


- Use weights in the p-adic numbers $\mathbb{Q}_p$
- 'Multiplicative' Fourier transformation that still preserves distances
  ... for some definiton of distance

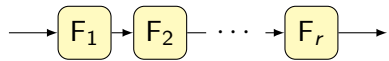
p-adic numbers

- $\mathbb{Q}_p$ contains the integers, but with a different distance:

$$\text{distance between 7 and } 1 = |7-1|_2 = |6|_2 = 1/2$$
$$\text{distance between 9 and } 1 = |9-1|_2 = |8|_2 = 1/8$$



Geometric approach to integral cryptanalysis



$$T^{\mathsf{F}} = T^{\mathsf{F}_r} \cdots T^{\mathsf{F}_2} T^{\mathsf{F}_1}$$
$$\Updownarrow \mathscr{U}$$
$$A^{\mathsf{F}} = A^{\mathsf{F}_r} \cdots A^{\mathsf{F}_2} A^{\mathsf{F}_1}$$

- Expanding the matrix product gives trails

$$A^{\mathsf{F}}_{\chi_{r+1},\chi_1} = \sum_{\chi_2,\ldots,\chi_r} \prod_{i=1}^{r} A^{\mathsf{F}_i}_{\chi_{i+1},\chi_i}$$

Lack of perspective

Ultrametric integral cryptanalysis

- For $\mathbb{F}_q^n$ with $\psi : x \mapsto \tau(x^u)$ and $\chi : x \mapsto \tau(x^v)$:

$$A^{\mathsf{F}}_{\chi,\psi} \equiv \text{coefficient of } x^u \text{ in the algebraic normal form of } F^v \pmod{p}$$

τ is the Teichmüller lift – nothing special for $q \in \{2, 3\}$

Ultrametric integral cryptanalysis

- For $\mathbb{F}_q^n$ with $\psi : x \mapsto \tau(x^u)$ and $\chi : x \mapsto \tau(x^v)$:

$$A^{\mathsf{F}}_{\chi,\psi} \equiv \text{coefficient of } x^u \text{ in the algebraic normal form of } F^v \pmod{p}$$

  τ is the Teichmüller lift – nothing special for $q \in \{2, 3\}$

- 'Approximate' zero-correlation properties

$$A^{\mathsf{F}}_{\chi_{r+1},\chi_1} = \sum_{\chi_2,\ldots,\chi_r} \prod_{i=1}^{r} A^{\mathsf{F}_i}_{\chi_{i+1},\chi_i} \approx 0$$

  Divisible by p^N

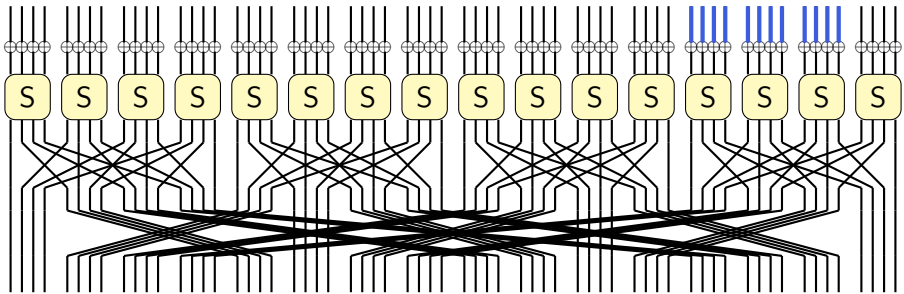
- Ordinary integral cryptanalysis: take $p = 2$ and $N = 1$

Ultrametric integral cryptanalysis

Example: integral property for 4-round Present

- Boura and Canteaut (Crypto 2016)

$$\sum_{x \preccurlyeq 0000000000000\texttt{fff}0} \tau(\mathsf{F}_1(x)) \equiv 0 \pmod 2$$

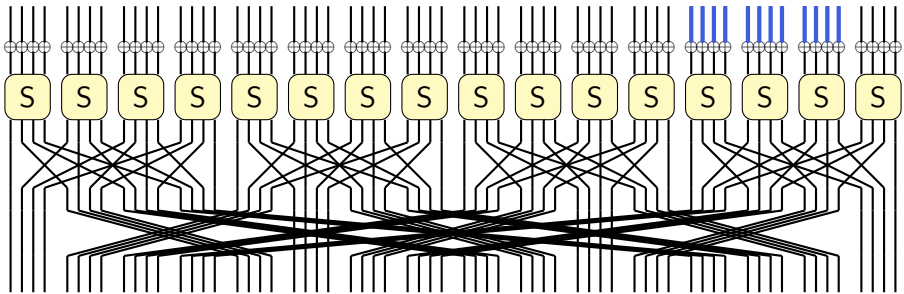


Ultrametric integral cryptanalysis

Example: integral property for 4-round Present

- Boura and Canteaut (Crypto 2016)

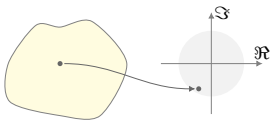
$$\sum_{x \preccurlyeq 000000000000\texttt{fff}0} \tau(\mathsf{F}_1(x)) \equiv 0 \pmod{32}$$



Conclusions

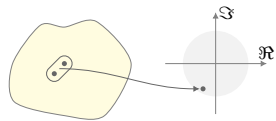
Geometric approach

Linear cryptanalysis



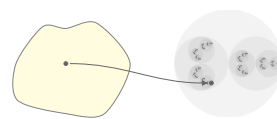
Fourier basis

Differential cryptanalysis



Quasidifferential basis

Integral cryptanalysis



Ultrametric basis

http://tim.cryptanalysis.info/

tim@cryptanalysis.info