A geometric approach to symmetric-key cryptanalysis

Tim Beyne

tim@cryptanalysis.info

KU Leuven

October 3, 2024

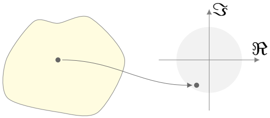
Overview

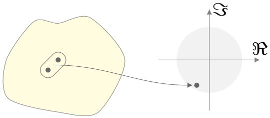
Geometric approach

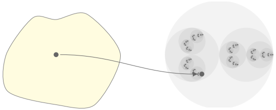
Linear cryptanalysis

Differential cryptanalysis

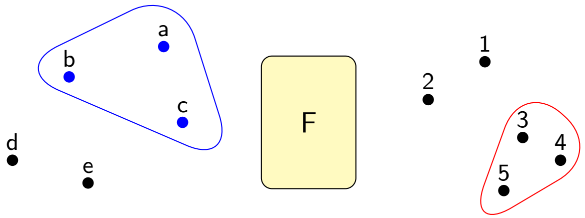
Integral cryptanalysis



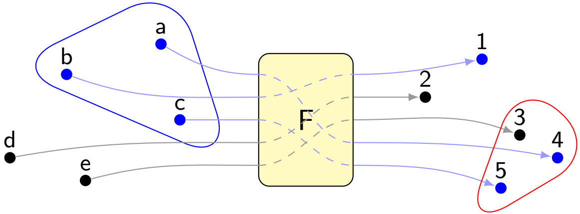




Geometric approach

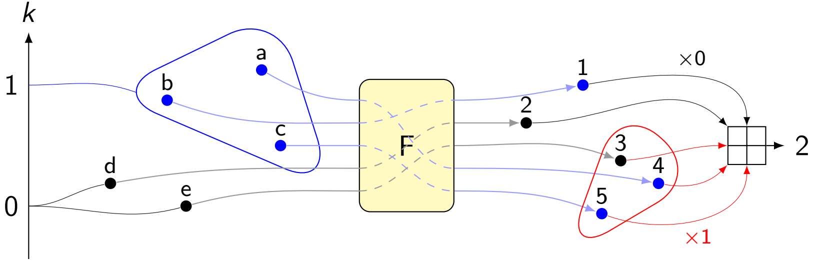


Geometric approach



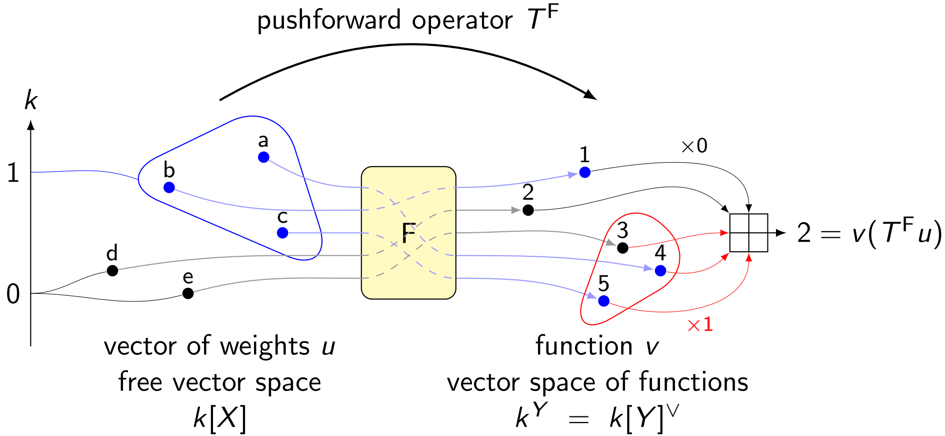
Geometric approach

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



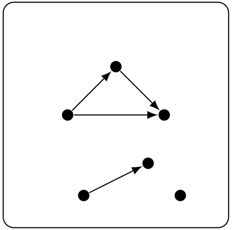
Geometric approach

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

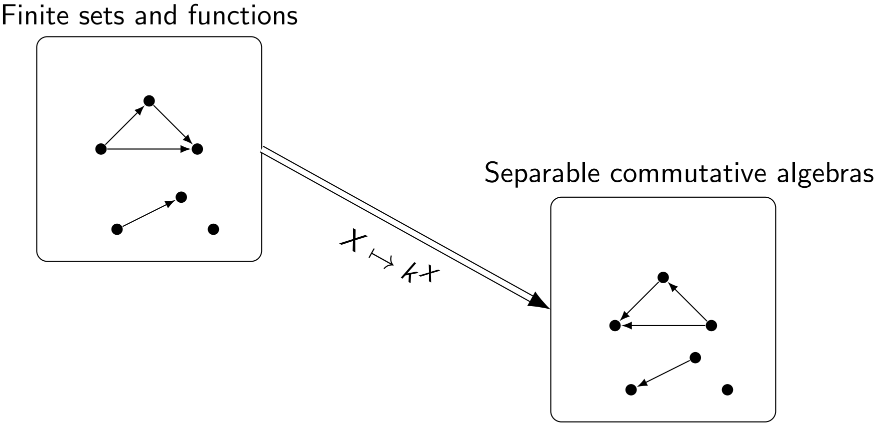


Geometric approach

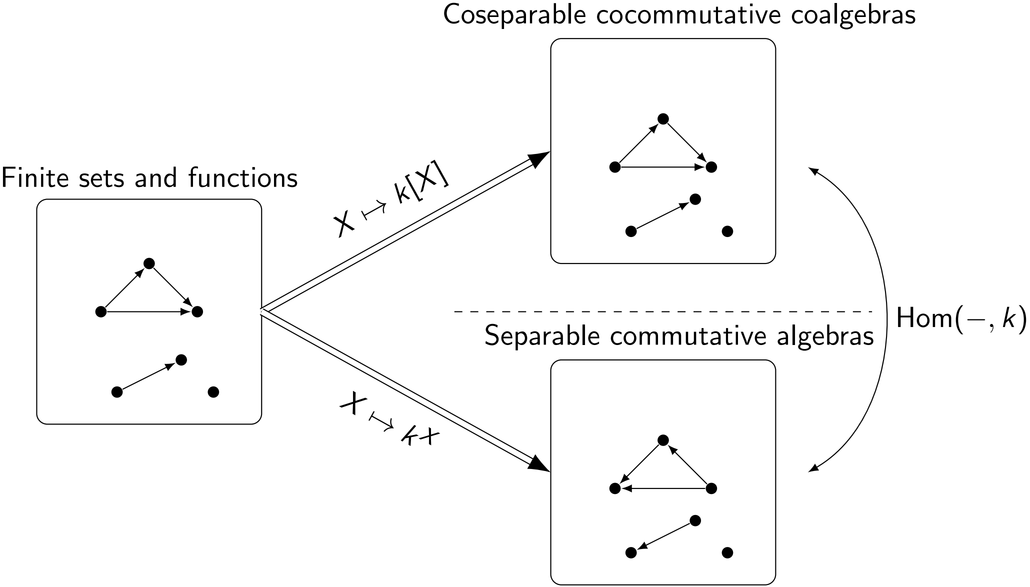
Finite sets and functions



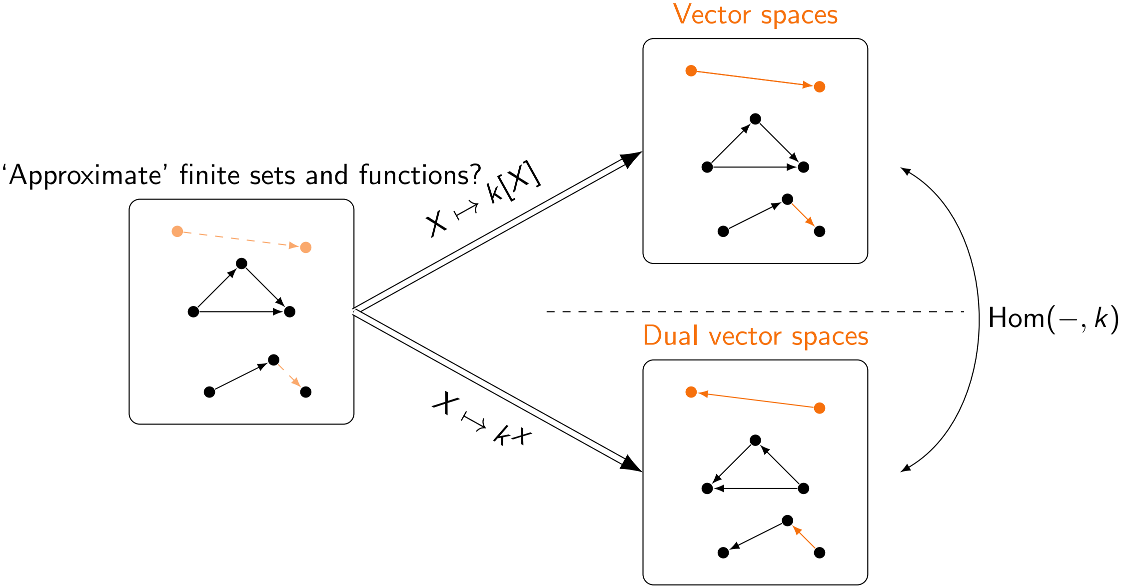
Geometric approach



Geometric approach



Geometric approach



Cryptanalytic properties

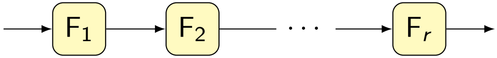
- Cryptanalytic property of a function $\mathsf{F} : X \to Y$ consists of
  - A subspace $U \subset k[X]$
  - A subspace $V \subset k^Y$
- Cryptanalysis is about evaluating properties:

$$\text{estimating } v(T^{\mathsf{F}} u) \text{ for } u \in U \text{ and } v \in V$$

- These data are equivalent to a map $U \to k[Y]/V^0$ or dually $V \to k^X/U^0$

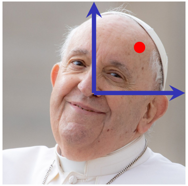
Pushforward operator

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

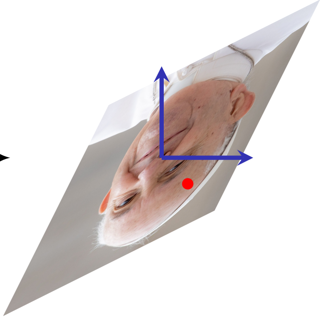


$$T^{\mathsf{F}} = T^{\mathsf{F}_r} \cdots T^{\mathsf{F}_2} T^{\mathsf{F}_1}$$

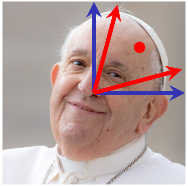
Change-of-basis



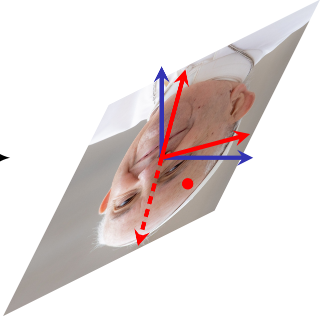
$$\begin{bmatrix} 1.15 & -0.58 \\ 0.58 & -1.15 \end{bmatrix}$$



Change-of-basis



$$\xrightarrow[\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}]{\begin{bmatrix}1.15 & -0.58\\ 0.58 & -1.15\end{bmatrix}}$$



Relative pushforward operators

$$T^{\mathsf{F}} \xleftrightarrow{\text{Change of basis}} B^{\mathsf{F}}$$

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

- 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

$$T^{\mathsf{F}} \xleftrightarrow{\text{Change of basis}} B^{\mathsf{F}}$$

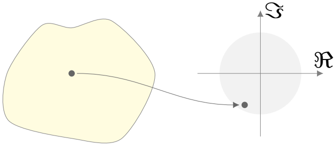
$$T^{\mathsf{F}} = T^{\mathsf{F}_r} \cdots T^{\mathsf{F}_2} T^{\mathsf{F}_1} \qquad B^{\mathsf{F}} = B^{\mathsf{F}_r} \cdots B^{\mathsf{F}_2} B^{\mathsf{F}_1}$$

- 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:

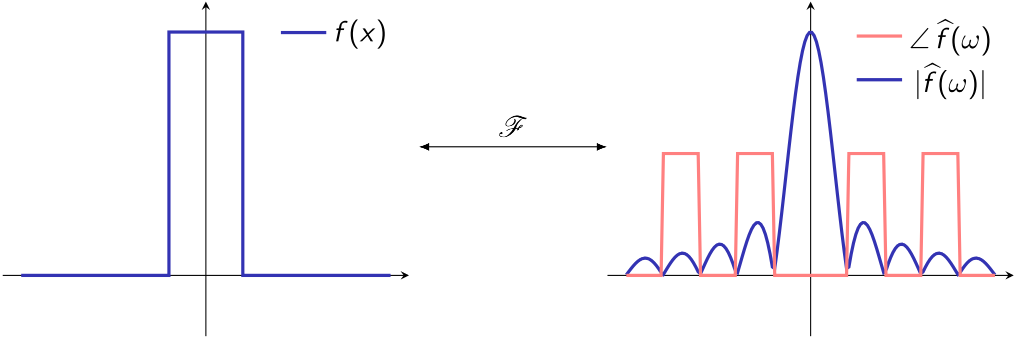
$$b^{\beta_{r+1}}\left(T^{\mathsf{F}} b_{\beta_1}\right) = B^{\mathsf{F}}_{\beta_{r+1},\beta_1} = \sum_{\beta_2,\ldots,\beta_r} \underbrace{\prod_{i=1}^{r} B^{\mathsf{F}_i}_{\beta_{i+1},\beta_i}}_{\text{Trail correlation}}$$

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

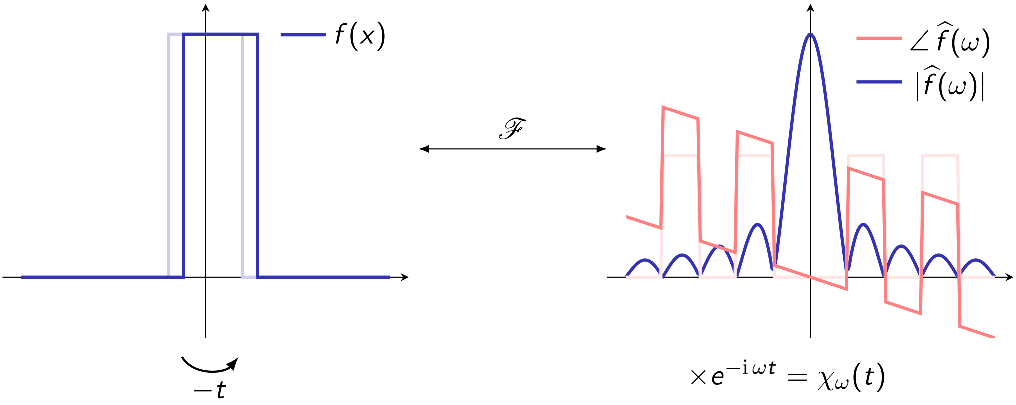
Linear cryptanalysis



Fourier transformation



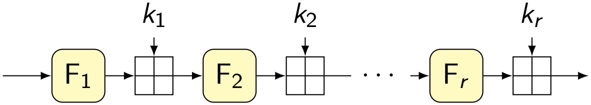
Fourier transformation



Fourier transformation diagonalizes translation

Geometric approach to linear cryptanalysis

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



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

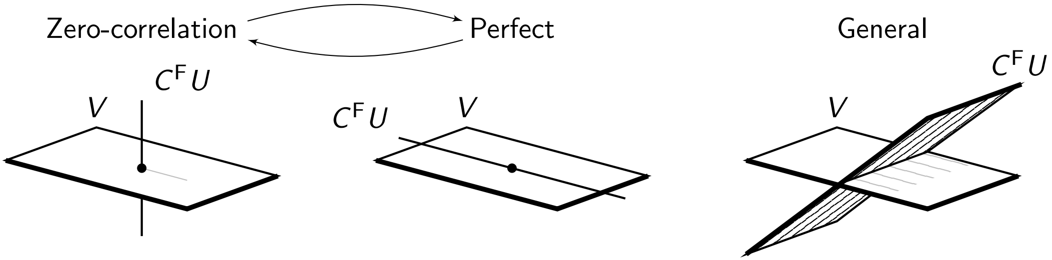
$$\Updownarrow \mathscr{F}$$

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

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

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

Geometric approach to linear cryptanalysis



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

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

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

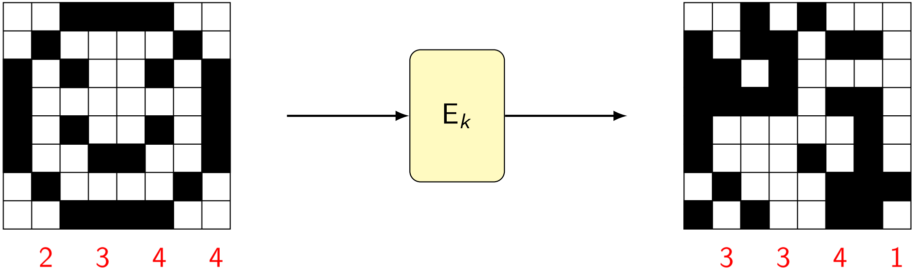
- Saturation attacks
- Invariant subspaces
- Nonlinear invariants

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

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

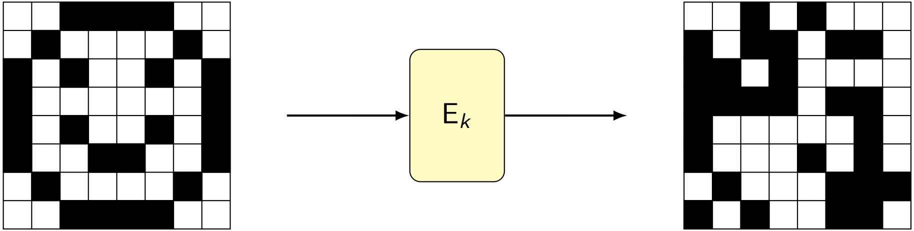
Invariants

Example: Midori-64*



Invariants

Example: Midori-64*

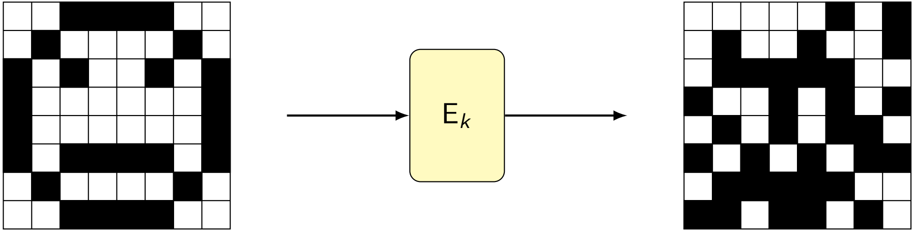


$2 + 3 + 4 + 4 \;=$ odd

$3 + 3 + 4 + 1 \;=$ odd

Invariants

Example: Midori-64*

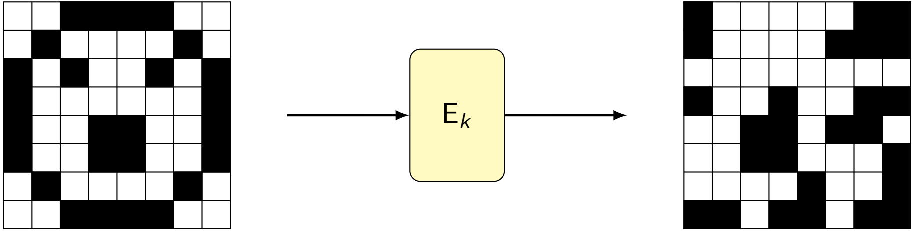


$2 + 3 + 4 + 4 \;= \text{odd}$
$2 + 3 + 4 + 4 \;= \text{odd}$

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

Invariants

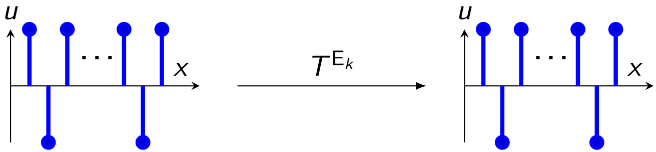
Example: Midori-64*



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

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

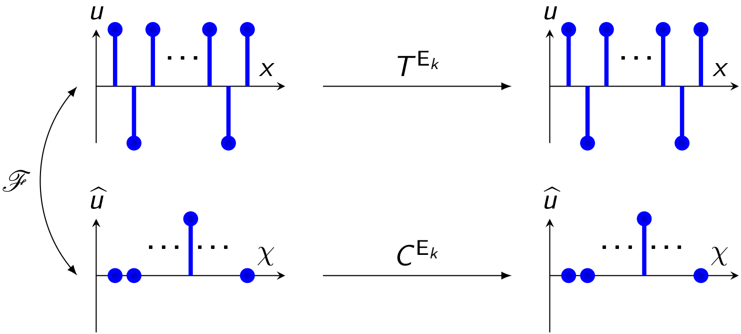
Invariants



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

invariants are eigenvectors

Invariants

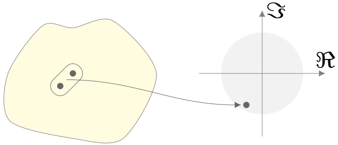


$$\begin{bmatrix} & & \\ & C^{\mathsf{E}_k} & \\ & & \end{bmatrix} \begin{bmatrix} \\ \widehat{u} \\ \\ \end{bmatrix} = \begin{bmatrix} \\ \widehat{u} \\ \\ \end{bmatrix}$$

invariants are eigenvectors

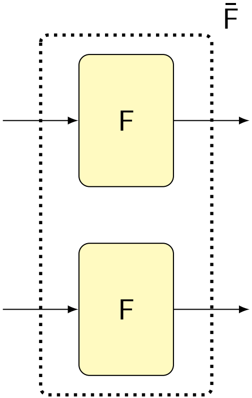
https://eprint.iacr.org/2018/763

Differential cryptanalysis



Pairs of values

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

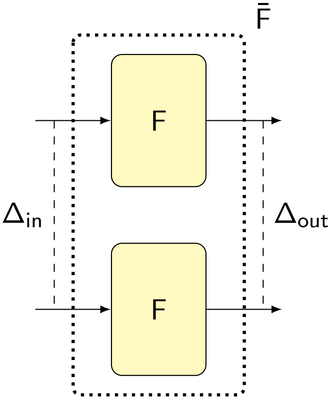


$$T^{\bar{\mathsf{F}}} = T^{\mathsf{F}} \otimes T^{\mathsf{F}}$$

pushforward operator for pairs

Pairs of values

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

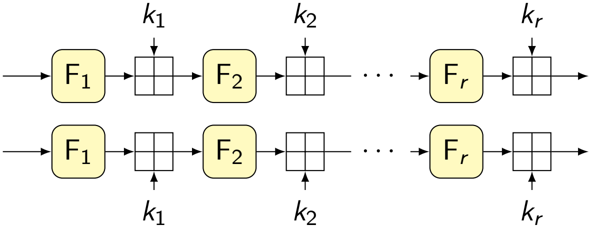


$$T^{\bar{\mathsf{F}}} = T^{\mathsf{F}} \otimes T^{\mathsf{F}}$$

pushforward operator for pairs

Geometric approach to differential cryptanalysis

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



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

$$\Updownarrow \mathscr{Q}$$

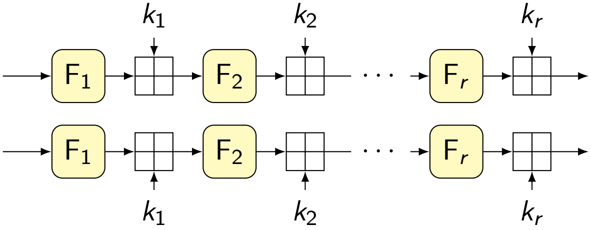
$$D^{\mathsf{F}} = D^{k_r} D^{\mathsf{F}_r} \cdots D^{k_2} D^{\mathsf{F}_2} D^{k_1} D^{\mathsf{F}_1}$$

Geometric approach to differential cryptanalysis

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

Constant-difference pairs

Fourier basis



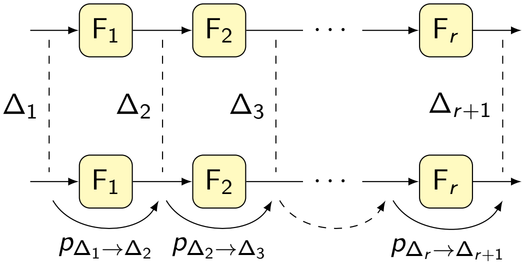
$$T^{\bar{\mathsf{F}}} = T^{\bar{k}_r}\, T^{\bar{\mathsf{F}}_r} \cdots T^{\bar{k}_2}\, T^{\bar{\mathsf{F}}_2}\, T^{\bar{k}_1}\, T^{\bar{\mathsf{F}}_1}$$

$$\Updownarrow \mathscr{Q}$$

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

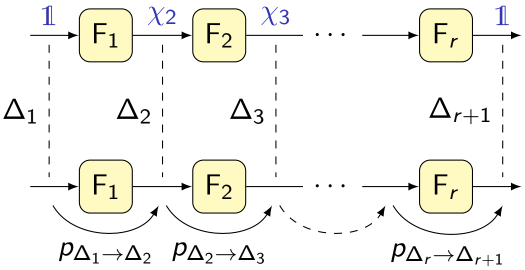
https://eprint.iacr.org/2022/837 (with V. Rijmen)

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



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

$$= \sum_{\substack{\Delta_2,\dots,\Delta_r \\ \chi_2,\dots,\chi_r}} D^{\mathsf{F}_1}_{(\chi_2,\Delta_2),(\mathbb{1},\Delta_1)} \times D^{\mathsf{F}_2}_{(\chi_3,\Delta_3),(\chi_2,\Delta_2)} \times \cdots \times D^{\mathsf{F}_r}_{(\mathbb{1},\Delta_{r+1}),(\chi_r,\Delta_r)}$$

Quasidifferential trails

Example: SPEEDY

- *Better Steady than Speedy: Full Break of* SPEEDY*-7-192* (Eurocrypt 2023)
  Boura, David, Boissier, Naya-Plasencia
- Four-round core-characteristic with claimed probability 2^{-42}

Quasidifferential trails

Example: SPEEDY

- *Better Steady than Speedy: Full Break of* SPEEDY-*7-192* (Eurocrypt 2023)
  Boura, David, Boissier, Naya-Plasencia

- Four-round core-characteristic with claimed probability 2^{-42}

- Inspection of quasidifferential trails shows that the probability is actually

$$2^{-42} - 2^{-42} = 0$$

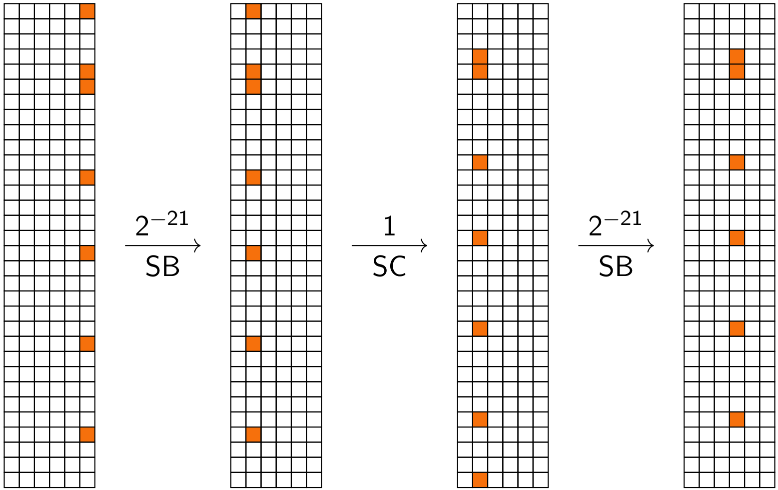
- Many other invalid attacks on SPEEDY in other papers

https://eprint.iacr.org/2024/262 (with A. Neyt)

Quasidifferential trails

Example: SPEEDY

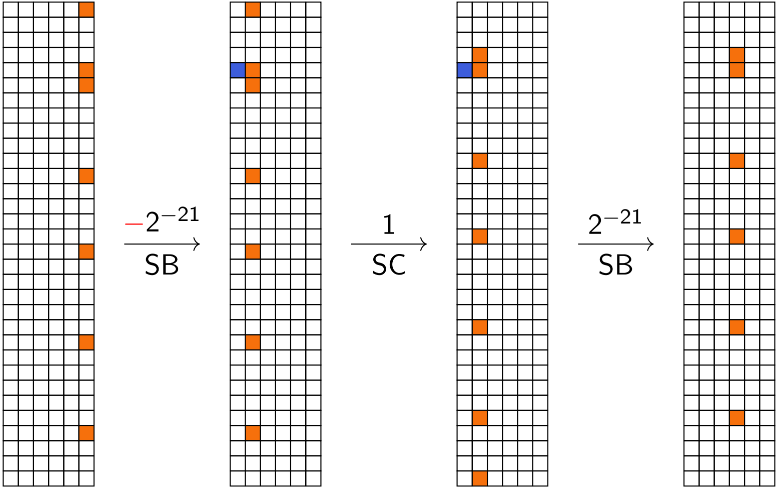
- First quasidifferential trail for SPEEDY: correlation 2^{-42}



Quasidifferential trails

Example: SPEEDY

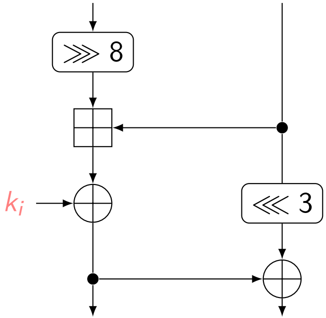
- Second quasidifferential trail for SPEEDY: correlation -2^{-42}



Quasidifferential trails

Example: 7-round Speck-64

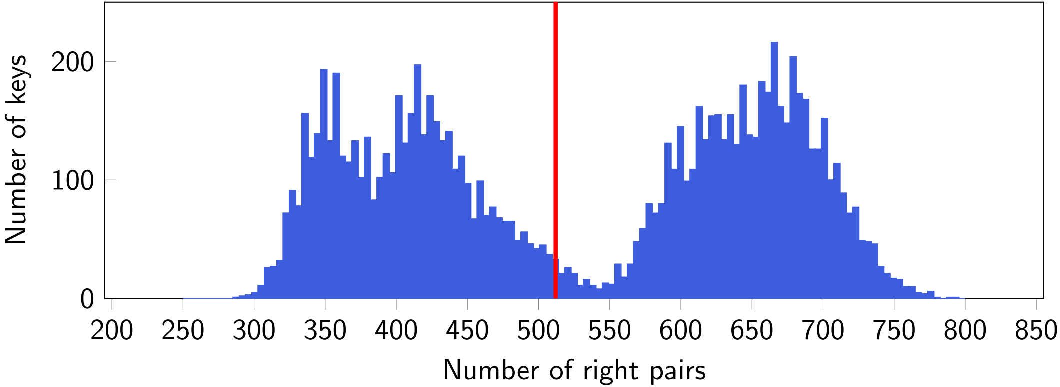
- Ankele and Kölbl (SAC 2018)
- Differential $(\texttt{4004092 104204}, \texttt{8080a080 8481a4a})$ for 7-round Speck-64
- Dominant characteristic estimated probability 2^{-21}



Quasidifferential trails

Example: 7-round Speck-64

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

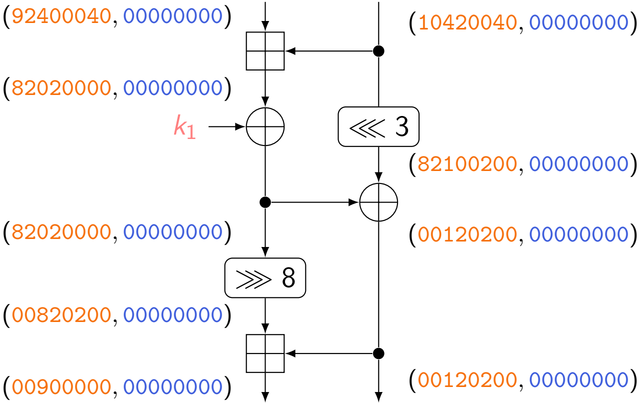


- 10000 keys, 2^{30} pairs per key

Quasidifferential trails

Example: 7-round Speck-64

- Quasidifferential trails over the first two rounds

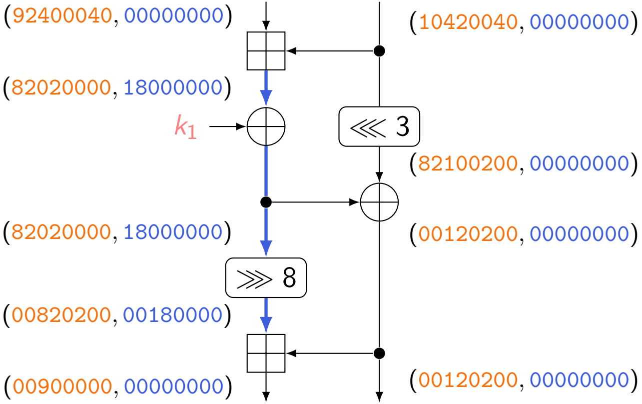


2^{-9}

Quasidifferential trails

Example: 7-round Speck-64

- Quasidifferential trails over the first two rounds

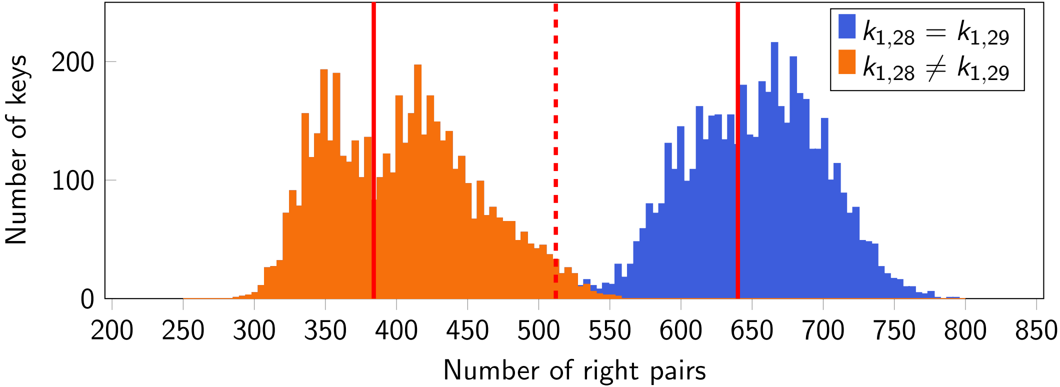


$$2^{-9} + (-1)^{k_{1,28}+k_{1,29}}\, 2^{-11}$$

Differential cryptanalysis

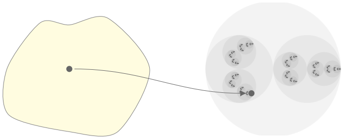
Example: 7-round Speck-64

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



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

Integral cryptanalysis

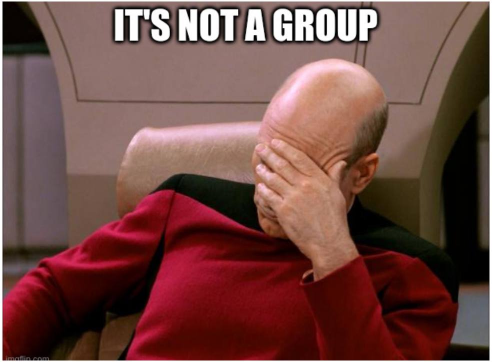


Geometric approach to integral cryptanalysis

- The Fourier transformation simplifies additions
  What about multiplications?

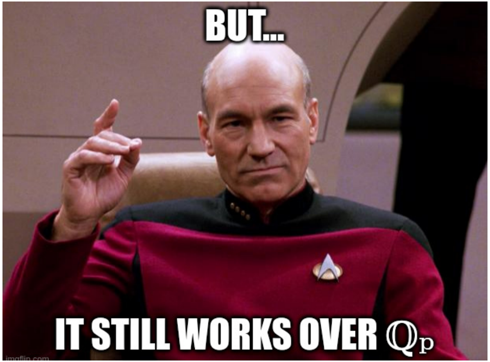
Geometric approach to integral cryptanalysis

- The Fourier transformation simplifies additions
  What about multiplications?



Geometric approach to integral cryptanalysis

- The Fourier transformation simplifies additions
  What about multiplications?



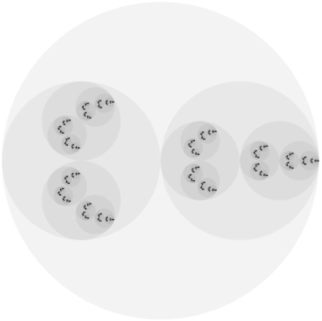
- Use weights in the p-adic numbers $\mathbb{Q}_p$

➔ '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

$$\longrightarrow \boxed{\mathsf{F}_1} \rightarrow \boxed{\mathsf{F}_2} \text{---} \cdots \rightarrow \boxed{\mathsf{F}_r} \longrightarrow$$

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

$$\Updownarrow \mathscr{U}$$

$$A^{\mathsf{F}} = A^{\mathsf{F}_r} \cdots A^{\mathsf{F}_2} A^{\mathsf{F}_1}$$

- Expanding the matrix product gives trails

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

https://eprint.iacr.org/2024/722 (with M. Verbauwhede)

Ultrametric integral cryptanalysis

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

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

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

Ultrametric integral cryptanalysis

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

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

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

- 'Approximate' zero-correlation properties

Divisible by p^N

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

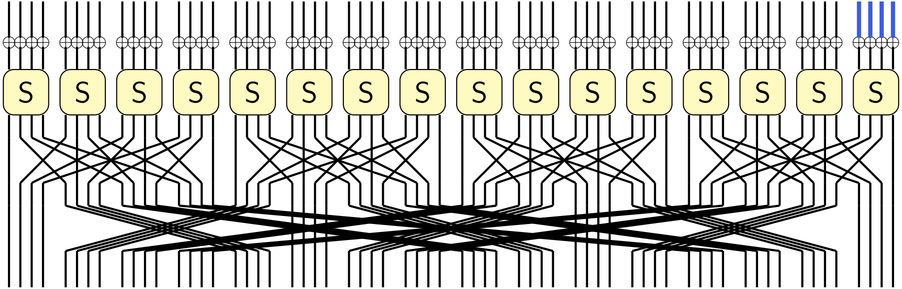
- Ordinary integral cryptanalysis: take $p = 2$ and $N = 1$

Ultrametric integral cryptanalysis

Example: 4-round Present

- Boura and Canteaut (Crypto 2016)

$$\sum_{x \preccurlyeq \mathtt{000000000000000f}} \tau(\mathsf{F}_2(x)) \equiv 0 \pmod 2$$

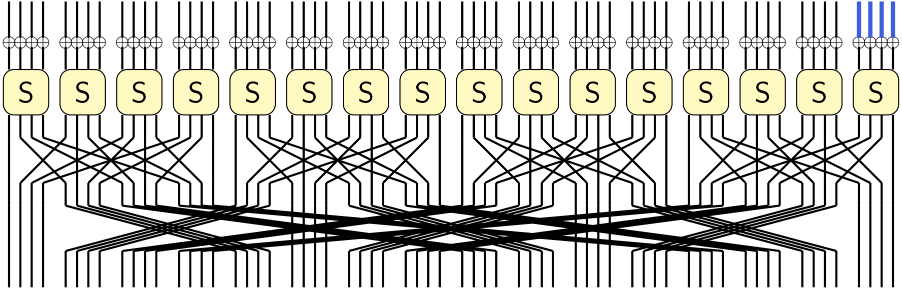


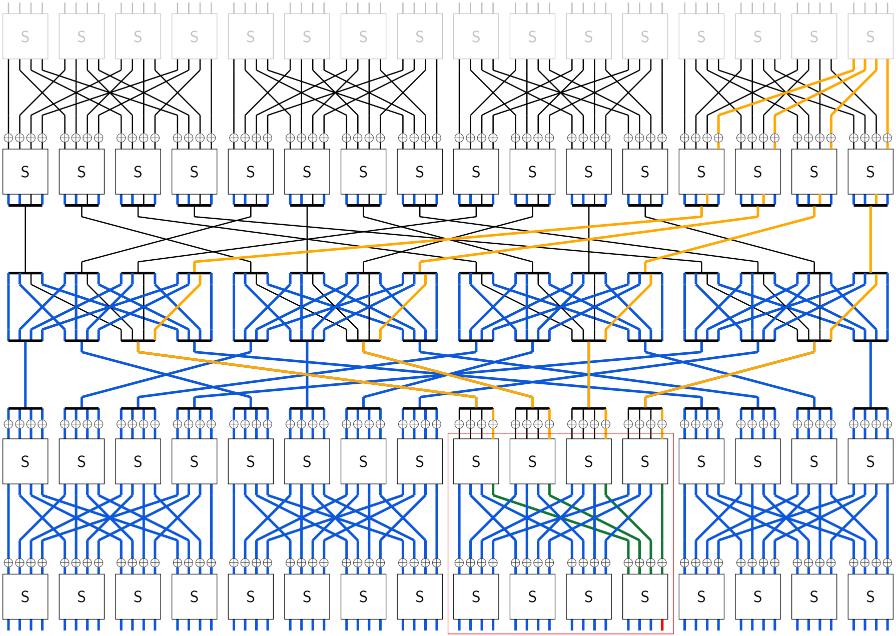
Ultrametric integral cryptanalysis

Example: 4-round Present

- Boura and Canteaut (Crypto 2016)

$$\sum_{x \preccurlyeq \texttt{000000000000000f}} \tau(\mathsf{F}_2(x)) \equiv 0 \pmod{4}$$




S

Ultrametric integral cryptanalysis

Example from mathematics: planar functions

- A function $\mathsf{F} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is called planar if

$$x \mapsto \mathsf{F}(x + \alpha) - \mathsf{F}(x)$$

  is a permutation for all α in $\mathbb{F}_{p^n}^{\times}$

- Dembowski-Ostrom conjecture: if F is planar, then $\deg_p \mathsf{F} = 2$ (for $p > 3$)

Ultrametric integral cryptanalysis

Example from mathematics: planar functions

- A function $\mathsf{F} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is called planar if

$$x \mapsto \mathsf{F}(x + \alpha) - \mathsf{F}(x)$$

  is a permutation for all α in $\mathbb{F}_{p^n}^{\times}$

- Dembowski-Ostrom conjecture: if F is planar, then $\deg_p \mathsf{F} = 2$ (for $p > 3$)

- Theorem (with C. Beierle): If F is planar, then for all nonzero $\mathsf{G} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$,

$$\deg_p \mathsf{G} \circ \mathsf{F} - \deg_p \mathsf{G} \leq \frac{n(p-1)}{2}$$

- We show this implies the conjecture for $\mathsf{F}(x) = x^d$ and $n = 2^k$ and $p \geq 7$

Ultrametric integral cryptanalysis

Example from mathematics: planar functions

- Planarity is additive: $\left|C^{\mathsf{F}}_{\chi,\psi}\right| = 1/\sqrt{p^n}$ for nontrivial χ
- Degree is multiplicative: $A^{\mathsf{F}}_{\mu,\lambda} \pmod{p}$ contains the algebraic normal form of F
- C^{F} and A^{F} represent the same linear map

$$C^{\mathsf{F}} = \left(\mathscr{F}\mathscr{U}^{-1}\right) A^{\mathsf{F}} \left(\mathscr{F}\mathscr{U}^{-1}\right)^{-1}$$

- p-adic absolute value

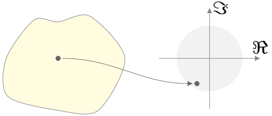
$$\left|A^{\mathsf{F}}_{\mu,\lambda}\right|_p \leq p^{\frac{\deg \mu - \deg \lambda}{p-1}} \max_{\chi,\psi \neq 1} \underbrace{\left|C^{\mathsf{F}}_{\chi,\psi}\right|_p}_{\sqrt{p^n}}$$

https://arxiv.org/abs/2407.04570 (with C. Beierle)

Conclusions

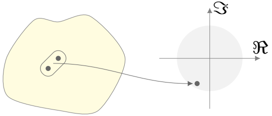
Geometric approach

Linear cryptanalysis



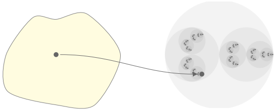
Fourier basis

Differential cryptanalysis



Quasidifferential basis

Integral cryptanalysis



Ultrametric basis

🌐 `https://tim.cryptanalysis.info/`

✉ `tim@cryptanalysis.info`