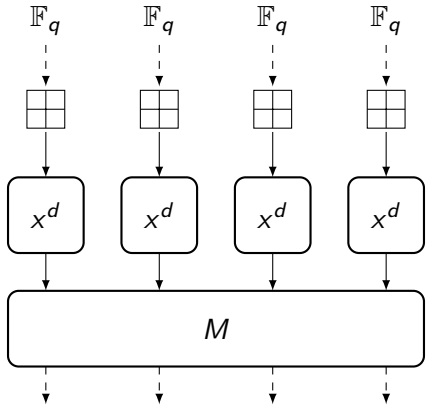
Security analysis of arithmetization-oriented primitives

Tim Beyne

May 10, 2026

Arithmetization-oriented primitives



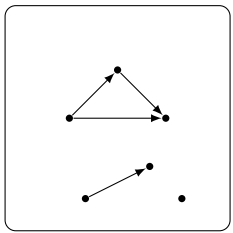
Arithmetization-oriented primitives

Questions for security analysis

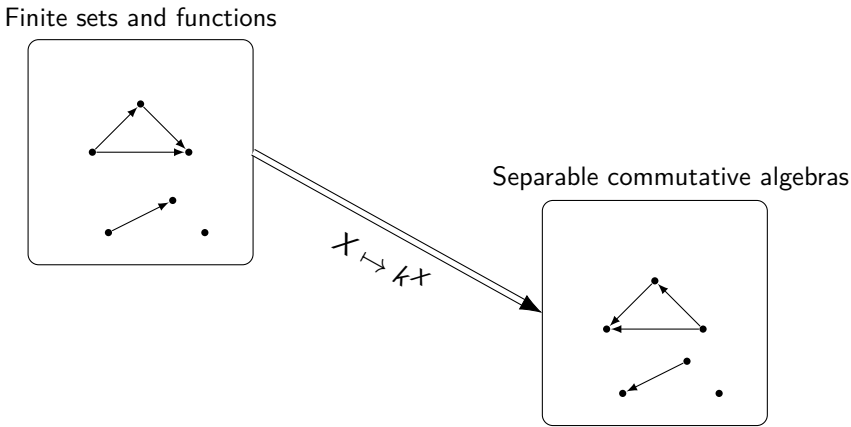
- How do cryptanalysis techniques generalize from $\mathbb{F}_2$ to $\mathbb{F}_q$?
- Impact of arithmization-friendly operations on security?
- Impact on security arguments?

Geometric approach to cryptanalysis

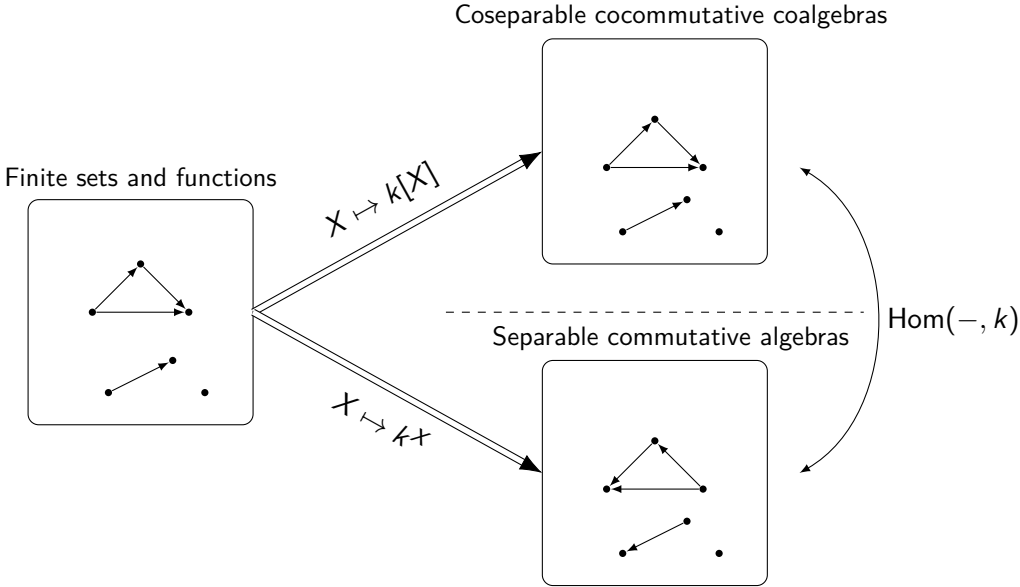
Finite sets and functions



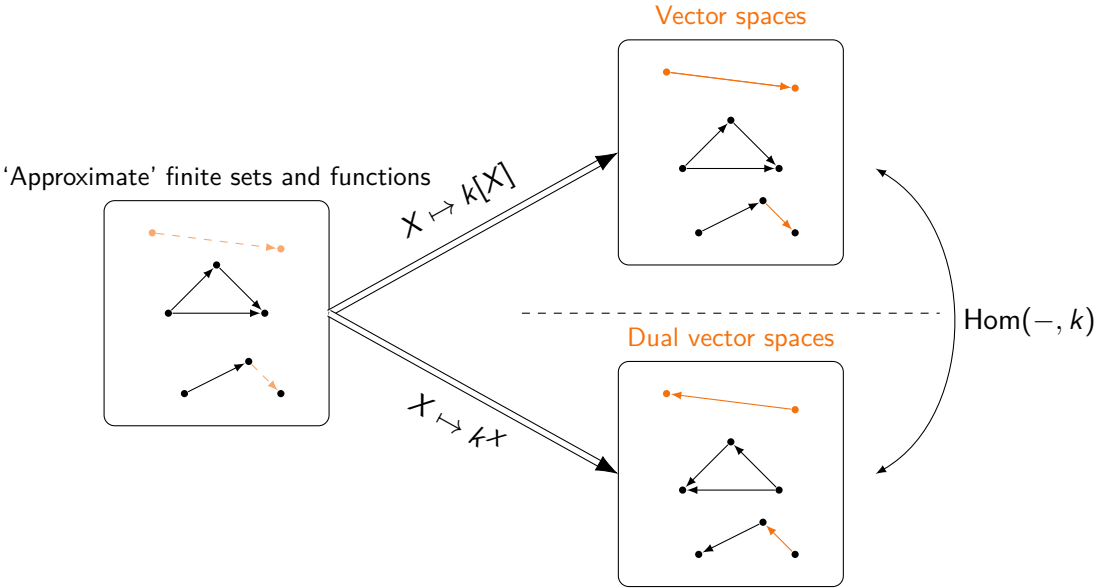
Geometric approach to cryptanalysis



Geometric approach to cryptanalysis



Geometric approach to cryptanalysis

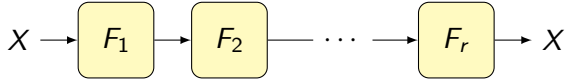


Geometric approach to cryptanalysis

- Solve combinatorial problems (cryptanalysis) using linear algebra!
- Function $F\colon X \to Y$ corresponds to a linear map

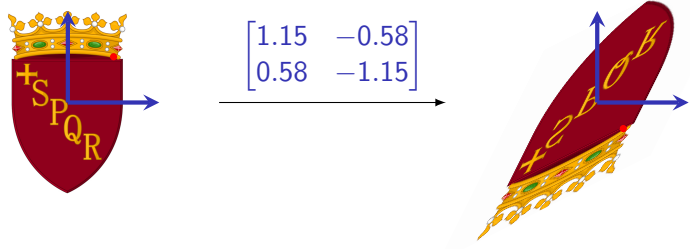
$$\begin{aligned} T^F\colon k[X] &\to k[Y] \\ \delta_x &\mapsto \delta_{F(x)} \end{aligned}$$

- Composition of functions

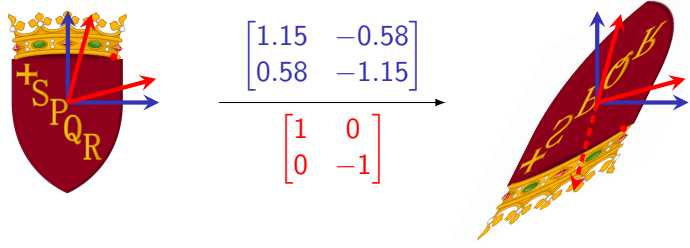


$$T^{F_r \circ \cdots \circ F_2 \circ F_1} = T^{F_r} \dots T^{F_2} T^{F_1}$$

Geometric approach to cryptanalysis



Geometric approach to cryptanalysis



Part I

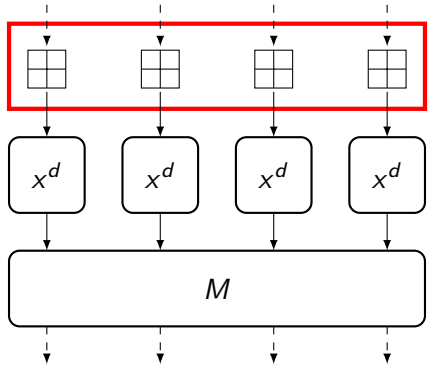
Archimedean techniques

$k = \mathbb{R}$ or $\mathbb{C}$

Overview

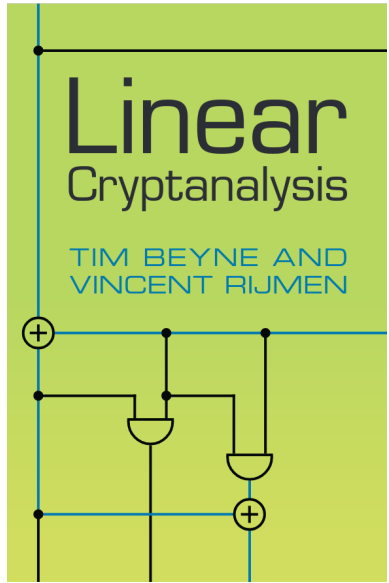
- Linear and differential cryptanalysis
- Security arguments in the key-averaged setting
- Security arguments in the fixed-key setting

Linear and differential cryptanalysis

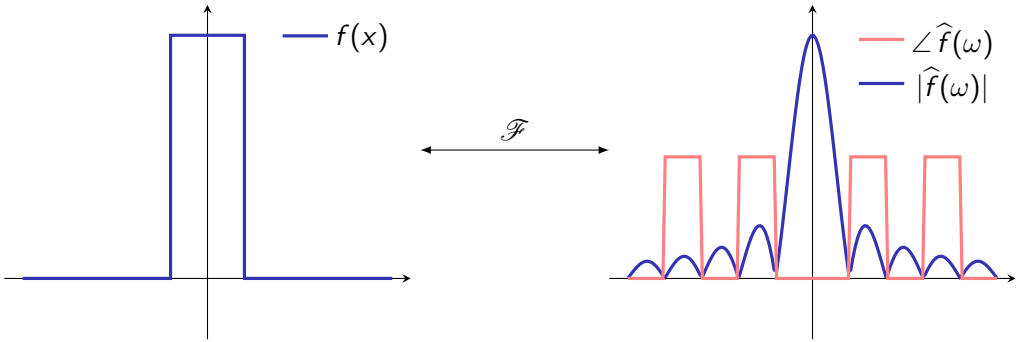


- These techniques only depend on the group structure
- Focus on linear cryptanalysis in this talk

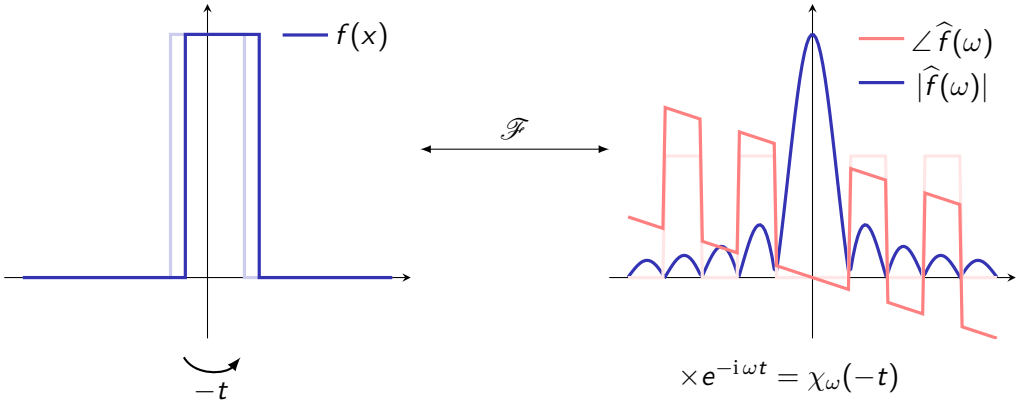
Linear cryptanalysis



Fourier transformation

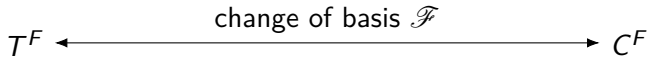


Fourier transformation



Fourier transformation diagonalizes translation

Linear cryptanalysis on $\mathbb{F}_q^n$



- Change of basis or Fourier transformation $\mathscr{F}\colon \mathbb{C}[\mathbb{F}_q^n] \to \mathbb{C}[\widehat{\mathbb{F}_q^n}]$
- Correlation matrix $C^F = \mathscr{F} T^F \mathscr{F}^{-1}$
- Linear approximation (ψ, χ) of F

$$C^F_{\chi,\psi} = \frac{1}{q^n} \sum_{x \in \mathbb{F}_q^n} \chi(F(x))\, \psi(-x)$$

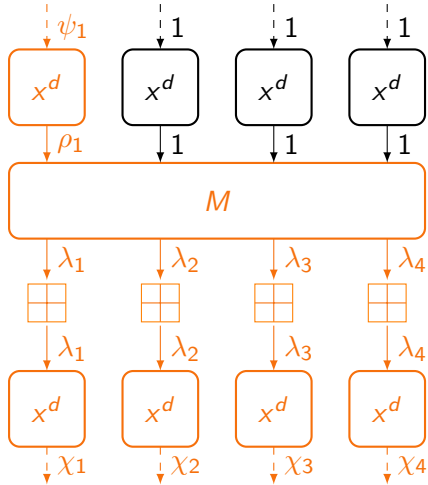
Linear approximations and trails

- If $F = F_r \circ \cdots \circ F_2 \circ F_1$, then $C^F = C^{F_r} \cdots C^{F_2} C^{F_1}$
- Linear trails

$$C^F_{\chi_{r+1},\chi_1} = \sum_{\chi_2,\ldots,\chi_r} \underbrace{C^{F_r}_{\chi_{r+1},\chi_r} \cdots C^{F_1}_{\chi_2,\chi_1}}_{\text{Trail correlation}}$$

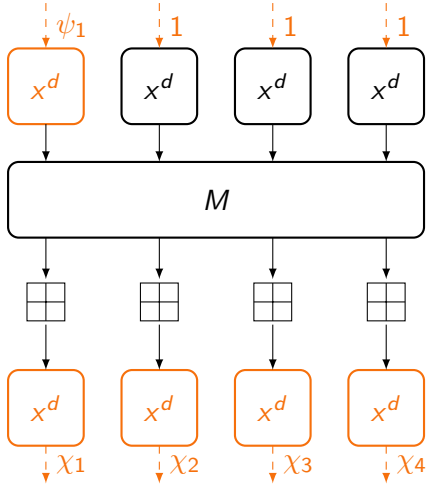
- A sequence $(\chi_1, \ldots, \chi_{r+1})$ of basis vector labels is a 'trail'

Linear trails



$$\left| C^S_{\rho_1,\psi_1} \times \lambda(k) \times C^S_{\chi_1,\lambda_1} \times C^S_{\chi_2,\lambda_2} \times C^S_{\chi_3,\lambda_3} \times C^S_{\chi_4,\lambda_4} \right| \leq \left(\frac{d-1}{\sqrt{q}} \right)^{B_L}$$

Linear approximations

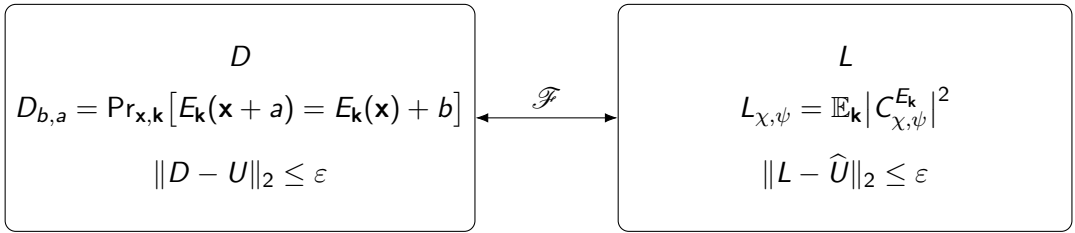


$$\sqrt{\mathbb{E}_{\mathbf{k}} \left| C^{E_{\mathbf{k}}}_{\chi,\psi} \right|^2} \leq \left(\frac{d-1}{\sqrt{q}} \right)^{B_L - 1}$$

Overview

- Linear and differential cryptanalysis
  Trail bounds; bounds for approximations in the key-averaged setting
- Security arguments in the key-averaged setting
- Security arguments in the fixed-key setting

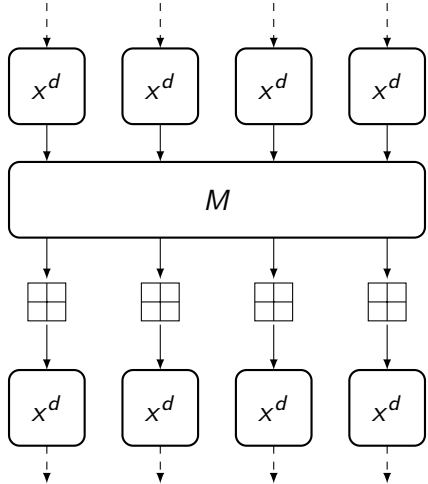
Pairwise independence of AES-like primitives



- Multiple approximations, zero-correlation properties, ...
- Pairwise independence: $\|D - U\|_1 \leq 2\varepsilon$
- Interpretation without keys: security against translation-invariant pairwise attacks

T. B., I. Schütt, G. Leander. *Pairwise independence of AES-like ciphers*. Eurocrypt 2026.

Example: SHARK construction

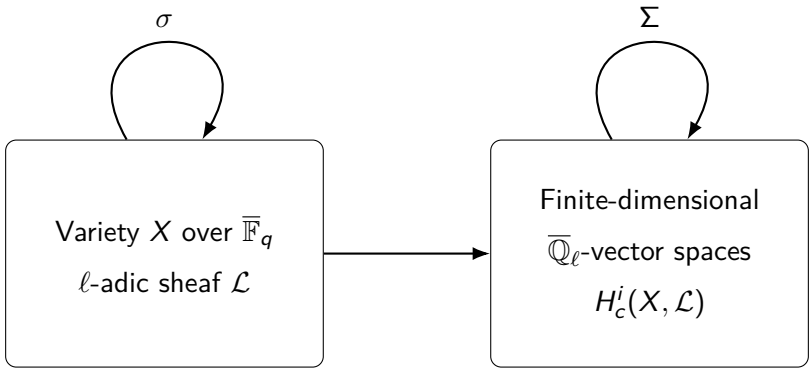


$$\|L - \widehat{U}\|_2 \leq \left(\frac{4(d-2)}{\sqrt{q}-1}\right)^4$$

Overview

- Linear and differential cryptanalysis
  Trail bounds; bounds for approximations in the key-averaged setting
- Security arguments in the key-averaged setting
  Pairwise independence bounds for AES-like ciphers
- Security arguments in the fixed-key setting

Cohomological framework



T. B., C. Bouvier. *Exponential sums in linear cryptanalysis*. Journal of Cryptology, 2026.

Cohomological framework

- Action of geometric Frobenius σ on an ℓ-adic sheaf $\mathcal{L}$ on $\mathbb{A}^n$

$$\mathrm{Tr}\big(\sigma_x \mid \mathcal{L}_x\big) = \frac{1}{q^n}\,\chi\big(F(x)\big)\,\psi(-x)$$

- Sum over fixed points of Frobenius

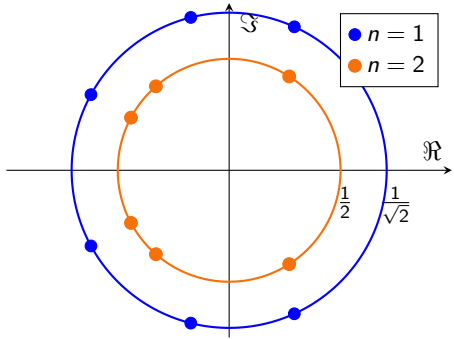
$$C^F_{\chi,\psi} = \sum_{x\in\mathbb{F}_q^n} \mathrm{Tr}\big(\sigma_x \mid \mathcal{L}_x\big) = \sum_{\substack{x\in\mathbb{A}^n \\ x^q = x}} \mathrm{Tr}\big(\sigma_x \mid \mathcal{L}_x\big)$$

- Grothendieck-Lefschetz trace formula

$$C^F_{\chi,\psi} = \sum_{i=0}^{2n} (-1)^i\,\mathrm{Tr}\Big(\Sigma \mid H^i_c(\mathbb{A}^n, \mathcal{L})\Big)$$

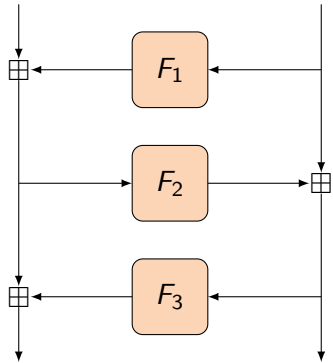
Example: $F(x) = x^7$ over $\mathbb{F}_{2^n}$

- $H_c^0 = H_c^2 = 0$, $\dim H_c^1 = 6$
- Eigenvalues of $\Sigma \mid H_c^1$: $\lambda_1, \lambda_2 \ldots, \lambda_6$ with $|\lambda_i| = 2^{-n/2}$



$$C^F_{\chi,\psi} = -\sum_{i=1}^{6} \lambda_i$$
$$= -2^{1-\frac{n}{2}} \Big(\cos(n\, 2.64\ldots) + \cos(n\, 1.81\ldots) + \cos(n\, 1.14\ldots) \Big) \text{ for } \chi, \psi \colon x \mapsto (-1)^{\mathrm{Tr}\, x}$$

Example: Feistel cipher using results of Denef-Loeser (1991)



$$\left|C^F_{\chi,\psi}\right| \leq \frac{(\max\{d_1, d_3\} - 1)(d_2 \min\{d_1, d_3\} - 1)}{q}$$

Overview

- Linear and differential cryptanalysis
  Trail bounds; bounds for approximations in the key-averaged setting
- Security arguments in the key-averaged setting
  Pairwise independence bounds for AES-like ciphers
- Security arguments in the fixed-key setting
  Fixed-key bounds for approximations using cohomology

Part II

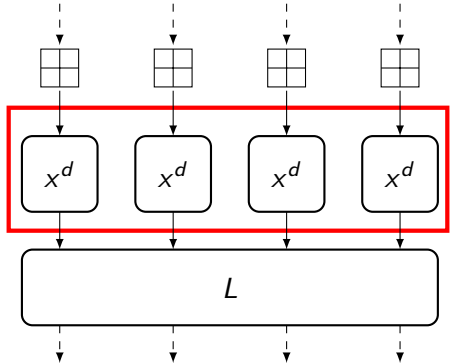
Non-Archimedean techniques

$k = \mathbb{Q}_p$ or $\mathbb{Q}_p(\zeta_{q-1})$

Overview

- Integral cryptanalysis
- Ultrametric integral cryptanalysis

Integral cryptanalysis

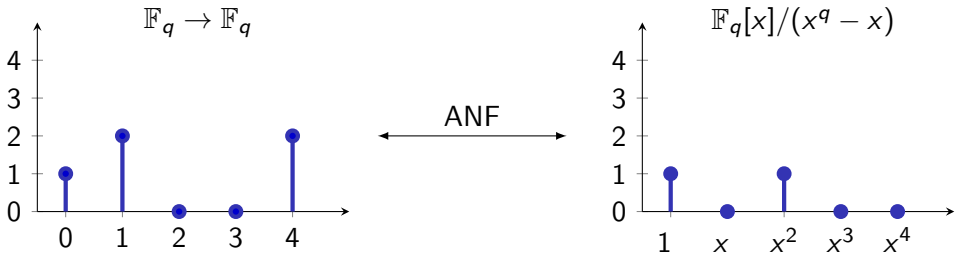


- Coordinate-wise multiplicative structure of $\mathbb{F}_q^n$
- Start with $k = \mathbb{F}_q$, but natural setting is $k = \mathbb{Q}_p(\zeta_{q-1})$

T. B., M. Verbauwhede. *Integral cryptanalysis in characteristic p.* Asiacrypt 2025.

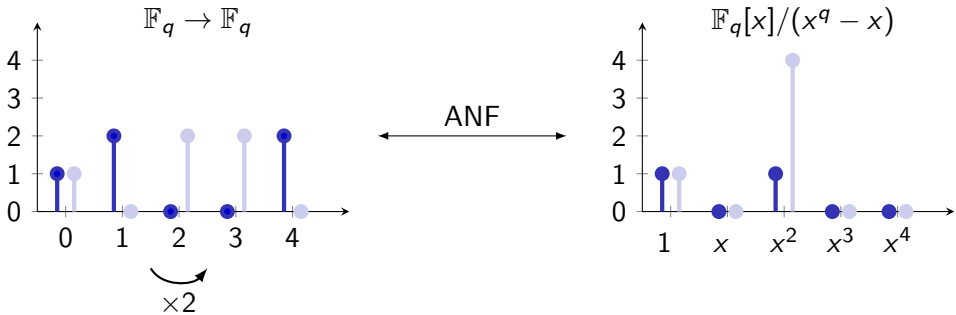
Multiplicative Fourier transformation on $\mathbb{F}_q$

- $\mathbb{F}_q$ is not a group, but close enough ('inverse monoid')
- For $k = \mathbb{F}_q$, this is related to the 'polynomial representation' of a function

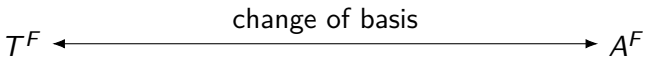


Multiplicative Fourier transformation on $\mathbb{F}_q$

- $\mathbb{F}_q$ is not a group, but close enough ('inverse monoid')
- For $k = \mathbb{F}_q$, this is related to the 'polynomial representation' of a function



Integral cryptanalysis on $\mathbb{F}_q^n$



- Change of basis or multiplicative Fourier transformation $\mathscr{U} : \mathbb{C}[\mathbb{F}_q^n] \to \mathbb{C}[\widehat{\mathbb{F}_q^n}]$

$$A^F = \begin{bmatrix} & & x^u \downarrow & & \\ & & & & \\ & \text{coefficient of } x^u \text{ in the ANF of } F^v & & & \leftarrow y^v \\ & & & & \end{bmatrix}$$

Integral trails

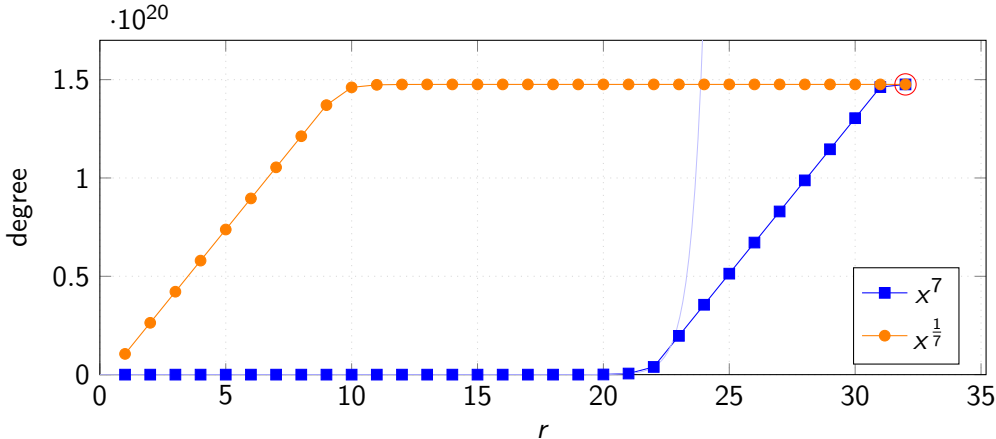
- If $F = F_r \circ \cdots \circ F_2 \circ F_1$, then

$$A^{F}_{\chi_{r+1},\chi_1} = \sum_{\chi_2,\ldots,\chi_r} \underbrace{A^{F_r}_{\chi_{r+1},\chi_r} \cdots A^{F_1}_{\chi_2,\chi_1}}_{\text{Trail correlation}}$$

- A sequence $(\chi_1, \ldots, \chi_{r+1})$ of basis vector labels is a 'trail'
- Interpretation as sequences of monomials *and* special input sets
- Currently the best way to study polynomial representations of composite functions

Example: degree growth in HadesMiMC partial rounds

$p = 2^{64} - 2^{32} + 1$, $t = 8$

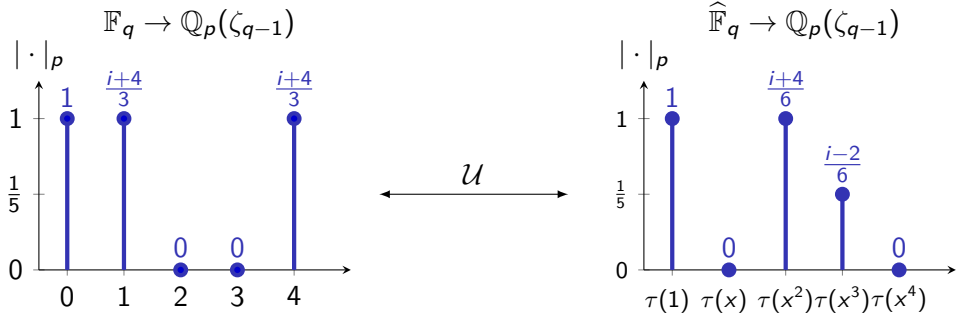


Overview

- Integral cryptanalysis
  Propagation of structured sets and polynomial representations
- Ultrametric integral cryptanalysis

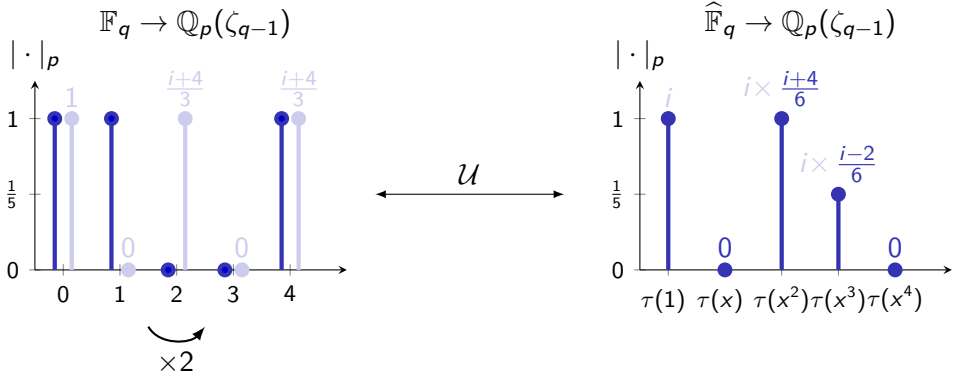
Multiplicative Fourier transformation on $\mathbb{F}_q$

- Choose $k = \mathbb{Q}_p(\zeta_{q-1})$ to express any 'integer' pointwise property
- p-adic absolute value $|x|_p = p^{-\nu}$ if $x = up^\nu$ with u a unit

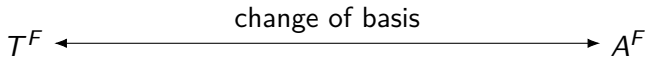


Multiplicative Fourier transformation on $\mathbb{F}_q$

- Choose $k = \mathbb{Q}_p(\zeta_{q-1})$ to express any 'integer' pointwise property
- p-adic absolute value $|x|_p = p^{-\nu}$ if $x = up^\nu$ with u a unit



Ultrametric integral cryptanalysis



- Comparison theorems with e.g. linear cryptanalysis
  C. Beierle, T. Beyne. *A degree bound for planar functions.* Combinatorial Theory 2025.

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

- Higher divisibility (zero sums modulo p^l)

Overview

- Integral cryptanalysis
  Propagation of structured sets and polynomial representation
- Ultrametric integral cryptanalysis
  Lift of integral cryptanalysis to characteristic zero

Conclusion

- Archimedean cryptanalysis ($k/\mathbb{R}$)
  - Security arguments against translation-invariant attacks
  - Fixed-key security arguments for linear cryptanalysis (cohomological framework)

  B., Leander, Schütt. *Pairwise independence of AES-like ciphers.* Eurocrypt 2026.
  B., Bouvier. *Exponential sums in linear cryptanalysis* Journal of Cryptology 2026.

- Non-Archimedean cryptanalysis ($k/\mathbb{Q}_p$)
  - Integral cryptanalysis to understand polynomial representations
  - Ultrametric integral cryptanalysis in characteristic zero

  B., Verbauwhede. *Integral cryptanalysis in characteristic p.* Asiacrypt 2025.

`https://tim.cryptanalysis.info`