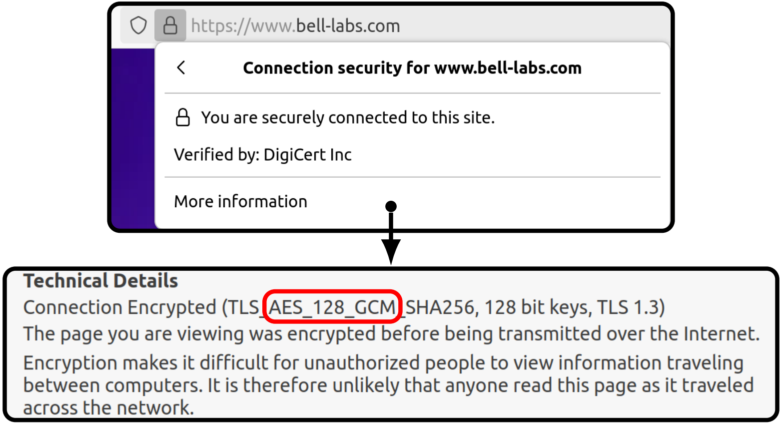
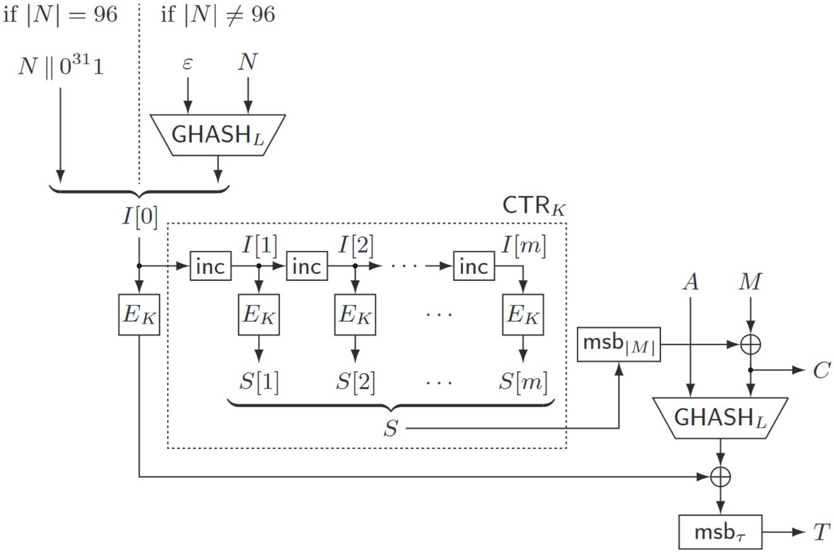
A geometric approach to symmetric-key cryptanalysis

Tim Beyne

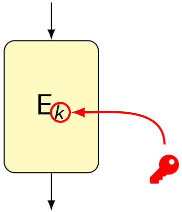
October 24, 2024

KU LEUVEN


https://www.bell-labs.com
Connection security for www.bell-labs.com
You are securely connected to this site.
Verified by: DigiCert Inc
More information
Technical Details
Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.


if $|N| = 96$
if $|N| \neq 96$
$N \,\|\, 0^{31}1$
ε
N
GHASH_L
$I[0]$
CTR_K
$I[1]$
$I[2]$
$I[m]$
inc
inc
inc
E_K
E_K
E_K
E_K
$S[1]$
$S[2]$
$S[m]$
S
$\mathsf{msb}_{|M|}$
A
M
C
GHASH_L
msb_τ
T

Block ciphers



e.g. AES-128

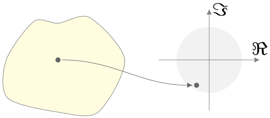
Cryptanalysis

Cryptanalysis

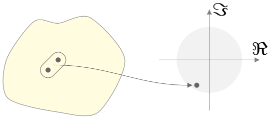
Overview

Geometric approach

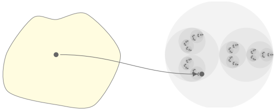
Linear cryptanalysis



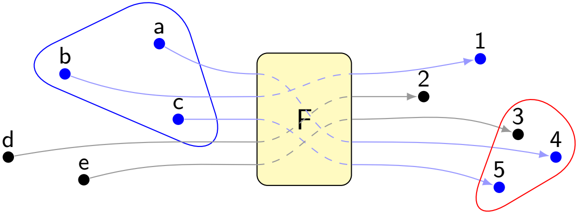
Differential cryptanalysis



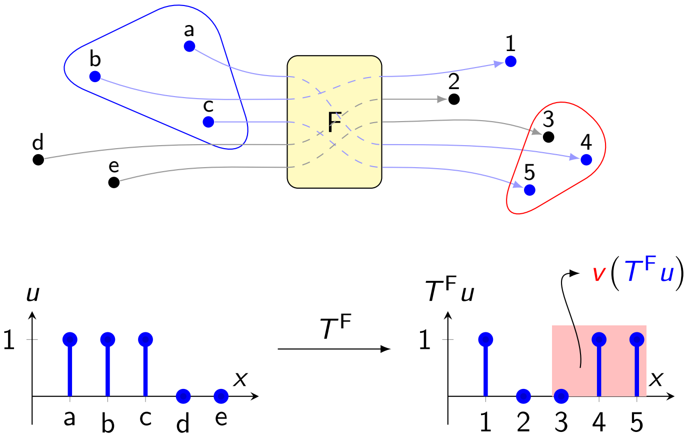
Integral cryptanalysis



Geometric approach

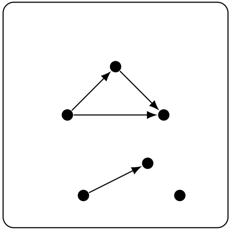


Geometric approach

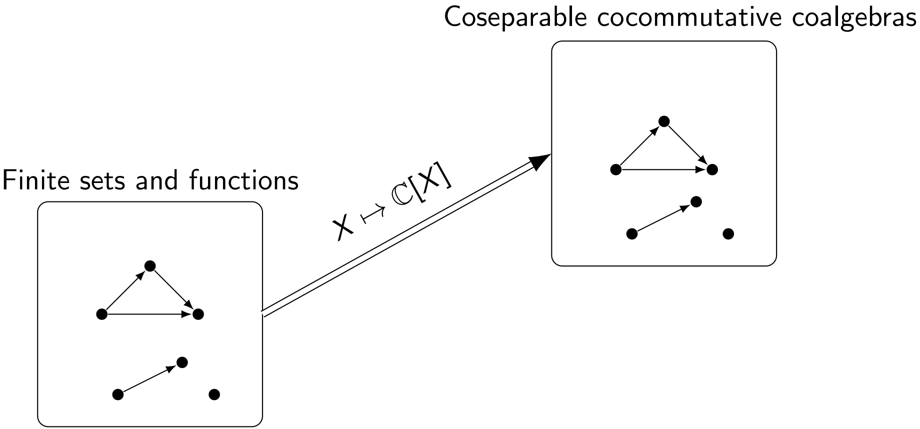


Geometric approach

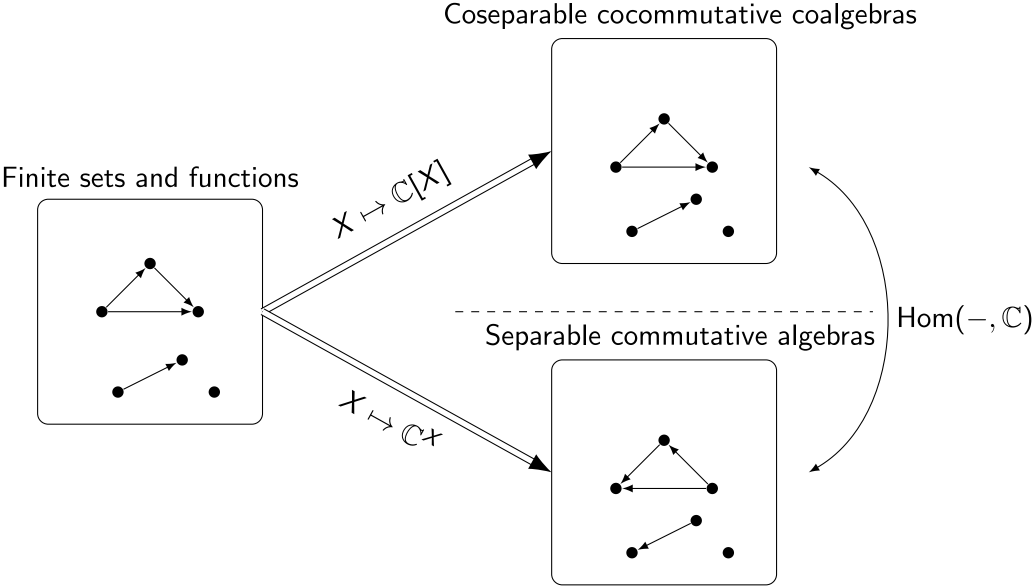
Finite sets and functions



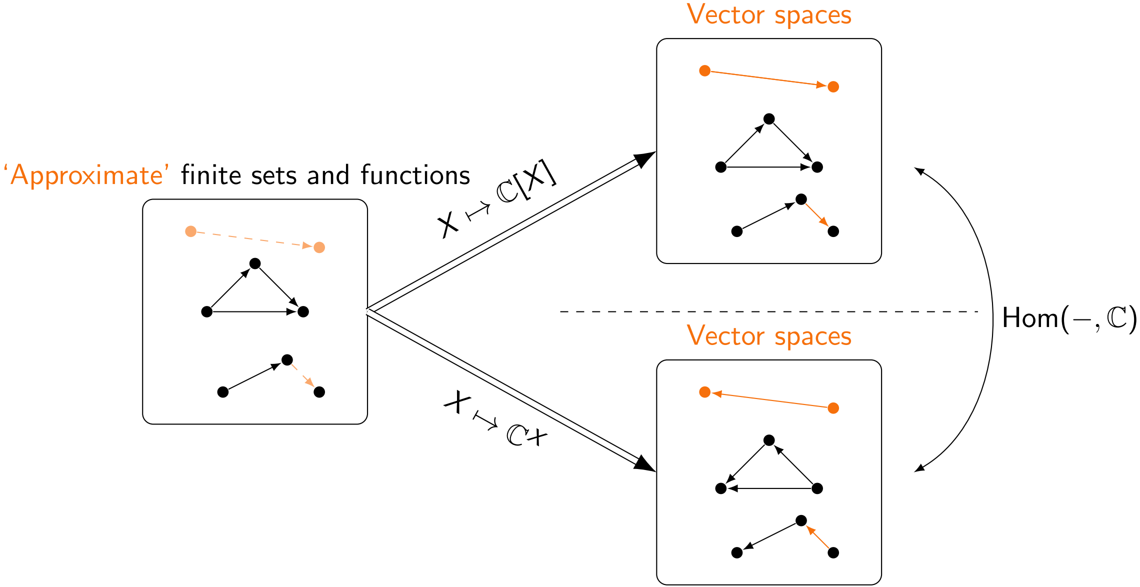
Geometric approach



Geometric approach

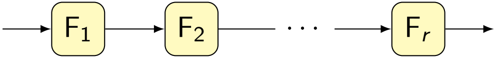


Geometric approach



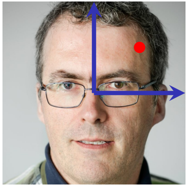
Iterated functions

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

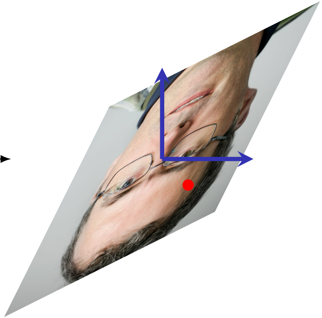


$$T^{\mathsf{F}} = T^{\mathsf{F}_r} \cdots T^{\mathsf{F}_2} T^{\mathsf{F}_1}$$

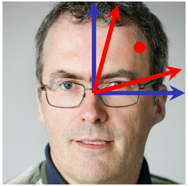
Change-of-basis



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



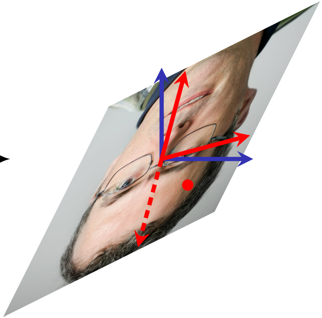
Change-of-basis



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

$$\longrightarrow$$

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



One-dimensional trails

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

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

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

One-dimensional trails

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

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

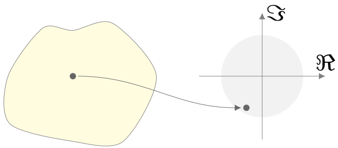
- With the right change of basis, this makes it easier to estimate $v(T^{\mathsf{F}} u) = \widehat{v}(B^{\mathsf{F}} \widehat{u})$
- When $u = b_{\beta_1}$ and $v = b^{\beta_{r+1}}$ are basis vectors:

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

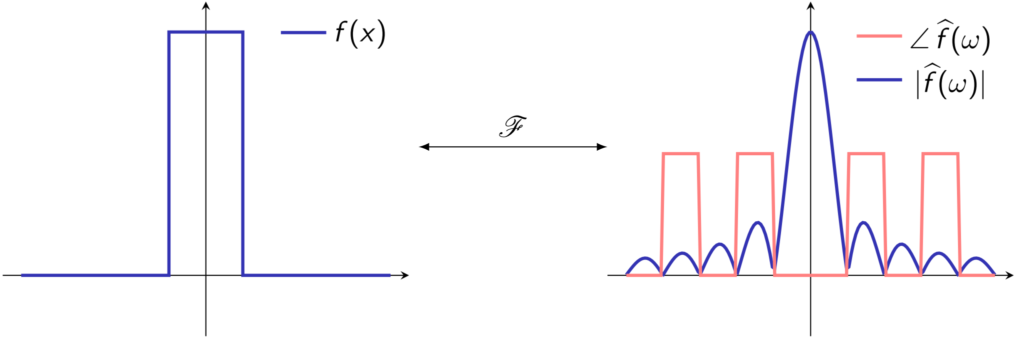
Trail correlation

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

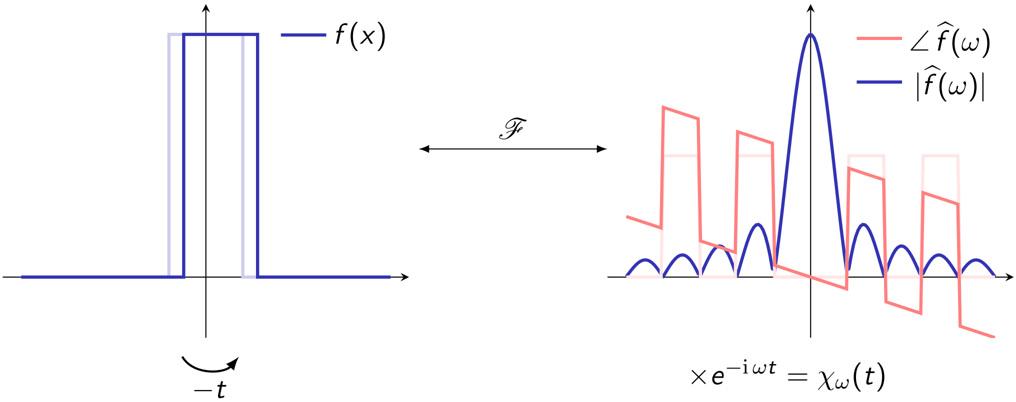
Linear cryptanalysis



Fourier transformation



Fourier transformation

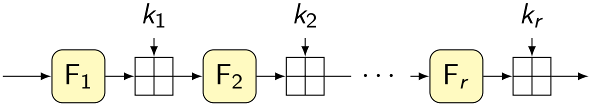


Fourier transformation diagonalizes translation

Geometric approach to linear cryptanalysis

[Asiacrypt 2021]

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



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

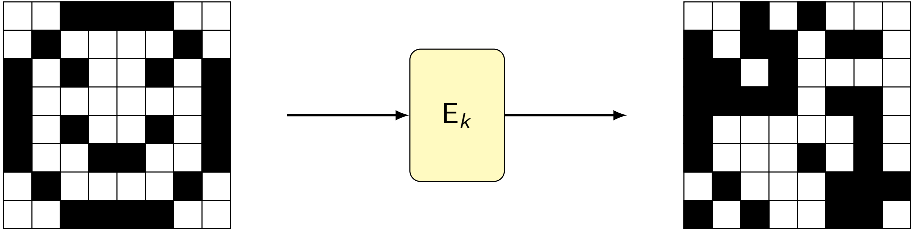
$$\Updownarrow \mathscr{F}$$

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

Invariants

[Asiacrypt 2018, JoC 2020]

Example: Midori-64*

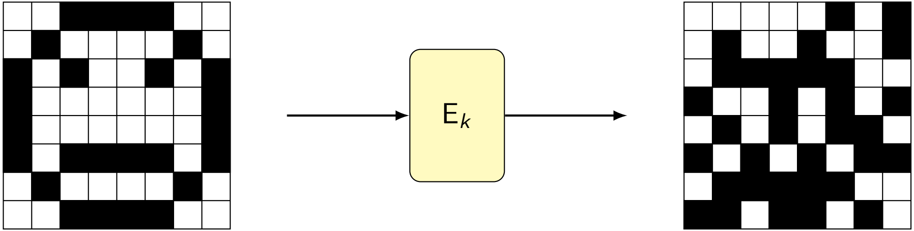


$2 + 3 + 4 + 4 \;= \text{odd}$ $\qquad$ $3 + 3 + 4 + 1 \;= \text{odd}$

[Asiacrypt 2018, JoC 2020]

Invariants

Example: Midori-64*



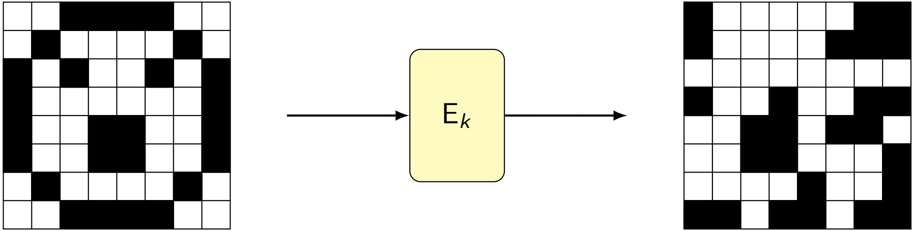
$2 + 3 + 4 + 4 = \text{odd}$
$2 + 3 + 4 + 4 = \text{odd}$

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

Invariants

[Asiacrypt 2018, JoC 2020]

Example: Midori-64*



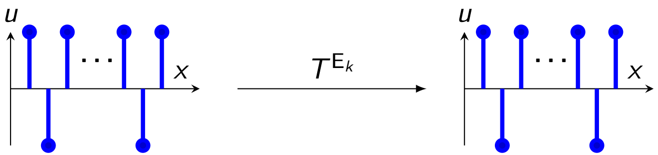
$2 + 3 + 4 + 4 = \text{odd}$
$2 + 3 + 4 + 4 = \text{odd}$
$2 + 4 + 3 + 4 = \text{odd}$

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

Invariants

Geometric approach

[Asiacrypt 2018, JoC 2020]

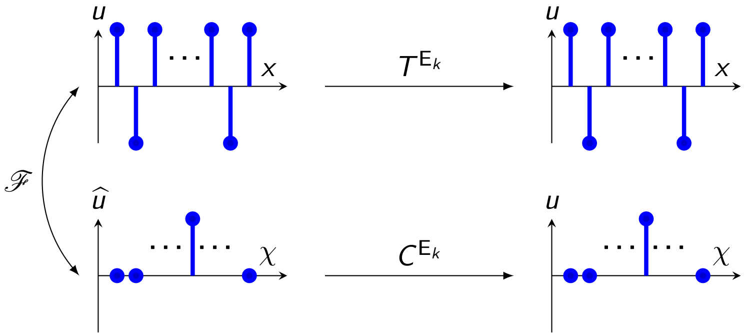


$$\begin{bmatrix} & & \\ & T^{E_k} & \\ & & \end{bmatrix} \begin{bmatrix} \\ u \\ \\ \end{bmatrix} = \begin{bmatrix} \\ u \\ \\ \end{bmatrix}$$

invariants are eigenvectors

Invariants

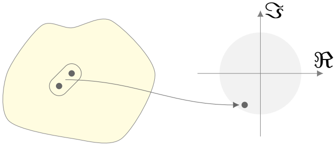
Geometric approach



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

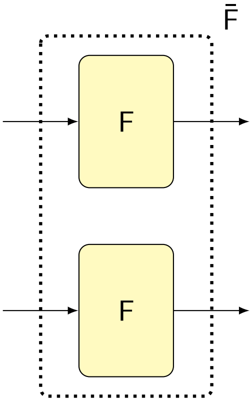
invariants are eigenvectors

Differential cryptanalysis



Pairs of values

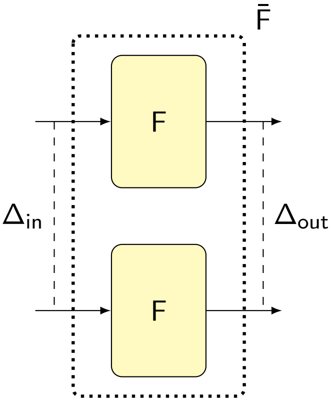
- Assign weights (complex numbers) to all pairs of values



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

Pairs of values

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



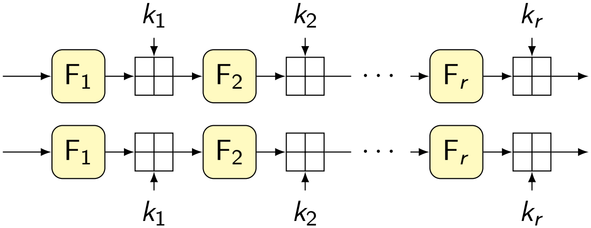
$$T^{\bar{\mathsf{F}}} = T^{\mathsf{F}} \otimes T^{\mathsf{F}}$$

Geometric approach to differential cryptanalysis

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

Constant-difference pairs

Fourier basis



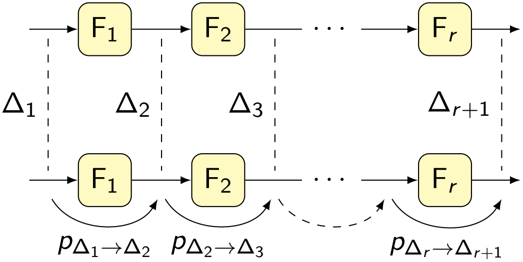
$$T^{\bar{\mathsf{F}}} = T^{\bar{k}_r} T^{\bar{\mathsf{F}}_r} \cdots T^{\bar{k}_2} T^{\bar{\mathsf{F}}_2} T^{\bar{k}_1} T^{\bar{\mathsf{F}}_1}$$

$$\Updownarrow \mathscr{Q}$$

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

Reevaluating differential attacks

Independence assumptions

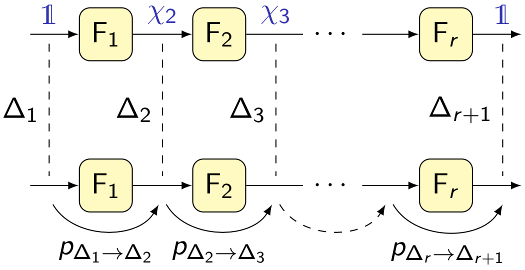


$$\text{probability} = \sum_{\Delta_2, \ldots, \Delta_r} p_{\Delta_1 \to \Delta_2} \times p_{\Delta_2 \to \Delta_3} \times \cdots \times p_{\Delta_r \to \Delta_{r+1}}$$

Reevaluating differential attacks

Independence assumptions

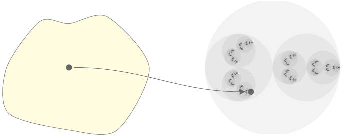
[Crypto 2022]



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

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

Integral cryptanalysis

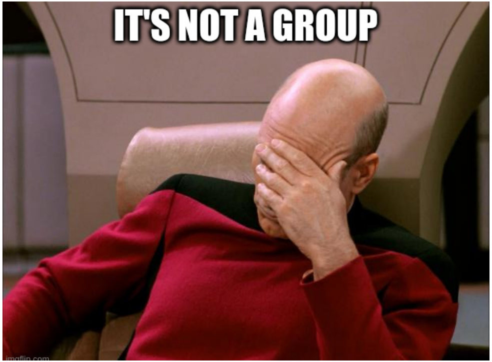


Geometric approach to integral cryptanalysis

- The Fourier transformation simplifies additions
  What about multiplications?

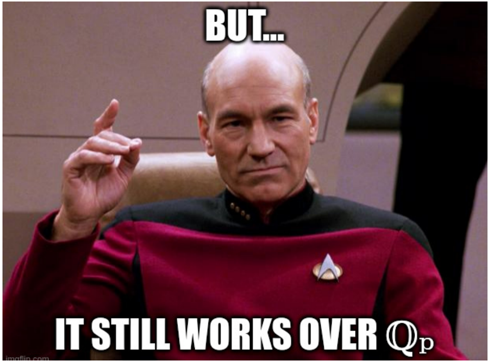
Geometric approach to integral cryptanalysis

- The Fourier transformation simplifies additions
  What about multiplications?



Geometric approach to integral cryptanalysis

- The Fourier transformation simplifies additions
  What about multiplications?



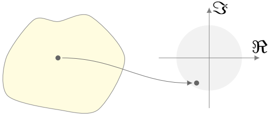
- Use weights in the p-adic numbers $\mathbb{Q}_p$

➜ 'Multiplicative' Fourier transformation that still preserves distances
… for some definiton of distance

Conclusions

Geometric approach

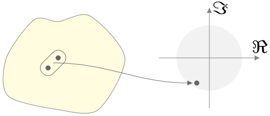
Linear cryptanalysis



Fourier basis

- Invariants of Midori & Mantis
- Attacks on FEA-$\{1,2\}$ & FF3-1
- Backdoored ciphers
- Side-channel countermeasures

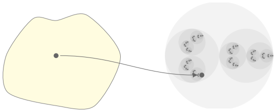
Differential cryptanalysis



Quasidifferential basis

- Re-evaluation of attacks (Speck, Rectangle, KNOT)
- Attacks on SM4 & GMiMC-crf
- Attacks on LowMC-M

Integral cryptanalysis



Ultrametric basis

- Ultrametric analysis of Present
- Attacks on Midori & Mantis
- Distinguishers for HadesMiMC

(other results: preimage attack on HadesMiMC, cryptanalysis of the Legendre PRF)