Unlocking Mix-Basis Potential: Geometric Approach for Combined Attacks

Kai Hu, Chi Zhang, Chengcheng Chang, Jiashu Zhang, Meiqin Wang and Thomas Peyrin

Shandong University
Nanyang Technological University

August 17, 2025, CRYPTO 2025

https://eprint.iacr.org/2025/403.pdf

Overview

1. **Motivation and background**

2. **Geometric approach by Beyne**

3. **Use different bases in geometric approach**

4. **Summary**

An elephant of current cryptanalysis

- So/too many attacks
  - differential, linear, integral, diff-linear...
- Need to resist all known attacks
  - Where the confidence on security of a cipher comes
- Tedious
  - to test all known attacks
- Not enough
  - Potential new attacks
  - Example: Multiple-of-*n* property for 5-round AES [GRR, EC 17]. Division property [Todo, EC 15]
- Possible explanation
  - Imperical
    Cryptanalysis is a task heavily based on the experience/intuition of cryptanalysts
  - Rather than
    Systematical methods
- Beneficial to have a unified method to describe/predict many attacks

Geometric approach by Beyne [Beyne, thesis]

- $\mathbb{K}$-Free vector space
  - Regard elements in $\mathbb{F}_2^n$ as 2^n basis vectors, choose a field $\mathbb{K}$

$$\mathbb{K}[\mathbb{F}_2^n] = \left\{ \sum_u k_u \delta_u : u \in \mathbb{F}_2^n, k_u \in \mathbb{K} \right\}$$

  - $\mathbb{K}[\mathbb{F}_2^n]$ is a linear space, as

$$\sum_u k_u \delta_u + \sum_u k'_u \delta_u = \sum_u (k_u + k'_u) \delta_u \in \mathbb{K}[\mathbb{F}_2^n]; \quad b \sum_u k_u \delta_u = \sum_u (b k_u) \, \delta_u \in \mathbb{K}[\mathbb{F}_2^n]$$

- Linear extension
  - For nonlinear $\mathsf{E} : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$, we define T^{E} as

$$\mathsf{T}^{\mathsf{E}} : \mathbb{K}[\mathbb{F}_2^n] \to \mathbb{K}[\mathbb{F}_2^n]; \quad \sum_u k_u \delta_u \mapsto \sum_u k_u \delta_{\mathsf{E}(u)}$$

  - T^{E} is a linear map, as

$$\mathsf{T}^{\mathsf{E}} \left(\sum_u a_u \delta_u + \sum_u b_u \delta_u \right) = \sum_u (a_u + b_u) \, \delta_{\mathsf{E}(u)} = \mathsf{T}^{\mathsf{E}} \left(\sum_u a_u \delta_u \right) + \mathsf{T}^{\mathsf{E}} \left(\sum_u b_u \delta_u \right)$$

$$\mathsf{T}^{\mathsf{E}} \left(k \sum_u a_u \delta_u \right) = k \sum_u a_u \delta_{\mathsf{E}(u)} = k \mathsf{T}^{\mathsf{E}} \left(\sum_u a_u \delta_u \right)$$

Notations in this work

- Let $f_u(\cdot) : \mathbb{F}_2^n \to \mathbb{K}$ be a function.
- A vector $f_u = (f_u(x), x = 0, \ldots, 2^n - 1)$
- A basis (a set of basis vectors) $(f_u, u = 0, \ldots, 2^n - 1)$ is written as $[f_u(x)]_{x,u}$ (if it can be written in such a compact way)

$$[f_u(x)]_{x,u} = \begin{array}{cc} u & \\ \begin{bmatrix} \ddots & & \\ & f_u(x) & \\ & & \ddots \end{bmatrix} & x \end{array}$$

Functions used in this work

Let $\mathbb{K} := \mathbb{Q}$

- $\delta_u(\cdot) : \mathbb{F}_2^n \to \mathbb{Q}; \quad \delta_u(x) = \begin{cases} 1 & \text{if } u = x \\ 0 & \text{otherwise} \end{cases}$
- $(-1)^{u^\top(\cdot)} : \mathbb{F}_2^n \to \mathbb{Q}; \quad (-1)^{u^\top x} = \begin{cases} 1 & \text{if } \sum_i u_i x_i \equiv 0 \bmod 2 \\ -1 & \text{otherwise} \end{cases}$
- $(\cdot)^u : \mathbb{F}_2^n \to \mathbb{Q}; \quad x^u = \begin{cases} 1 & \text{if } x \succeq u \quad (x \succeq u \text{ iff } x_i \geq u_i \text{ for all } i) \\ 0 & \text{otherwise} \end{cases}$
- $u^{(\cdot)} : \mathbb{F}_2^n \to \mathbb{Q}; \quad u^x = \begin{cases} 1 & \text{if } u \succeq x \\ 0 & \text{otherwise} \end{cases}$

Remark. The monomial function $x^u \in \mathbb{F}_2^n$, so we should apply a Teichmüller lift to it

$$\tau : \mathbb{F}_2^n \to \mathbb{Q}; \quad 0 \mapsto 0, 1 \mapsto 1$$

Since this work only focuses on values in $\mathbb{Q}$, we will omit τ

Transition Matrix and change-of-basis [Beyne, thesis]

- $\mathrm{T}^{\mathrm{E}} : \mathbb{Q}[\mathbb{F}_2^n] \to \mathbb{Q}[\mathbb{F}_2^n]$ is a linear map. Fixing bases for the input/output spaces, we will get a matrix w.r.t the bases
- Regard $[\delta_u(x)]_{x,u}$ as the standard basis for the input and output spaces, the corresponding transition matrix has elements as

$$T^{\mathrm{E}}_{v,u} = \delta_v^\top \mathrm{T}^{\mathrm{E}}(\delta_u) = \delta_v(\mathrm{E}(u))$$

- What is the transition matrix when choosing another basis $[f_u(x)]_{x,u}$?

$$\begin{tikzcd}\mathbb{K}[\mathbb{F}_2^n] = Span\left([\delta_u(x)]_{x,u}\right) \arrow[r, "T^{\mathrm{E}}"] & \mathbb{K}[\mathbb{F}_2^n] = Span\left([\delta_u(x)]_{x,u}\right)\end{tikzcd}$$

$$\begin{tikzcd}\mathbb{K}[\mathbb{F}_2^n] = Span\left([f_u(x)]_{x,u}\right) \arrow[r, "A^{\mathrm{E}} =?"] & \mathbb{K}[\mathbb{F}_2^n] = Span\left([f_u(x)]_{x,u}\right)\end{tikzcd}$$

Transition Matrix and change-of-basis [Beyne, thesis]

- $\mathsf{T}^{\mathsf{E}} : \mathbb{Q}[\mathbb{F}_2^n] \to \mathbb{Q}[\mathbb{F}_2^n]$ is a linear map. Fixing bases for the input/output spaces, we will get a matrix w.r.t the bases
- Regard $[\delta_u(x)]_{x,u}$ as the standard basis for the input and output spaces, the corresponding transition matrix has elements as
$$T^{\mathsf{E}}_{v,u} = \delta_v^\top \mathsf{T}^{\mathsf{E}}(\delta_u) = \delta_v(\mathsf{E}(u))$$
- What is the transition matrix when choosing another basis $[f_u(x)]_{x,u}$?

$$\begin{tikzcd}
{[\delta_u(x)]_{x,u}\ F^{-1}\ x} \arrow[r, "T^{\mathsf{E}}"] & {[\delta_u(x)]_{x,u}\ T^{\mathsf{E}}\ \ F^{-1}\ x} \arrow[d, "{[\delta_u(x)]_{x,u} = [f_u(x)]_{x,u} F}"] \\
{X = [f_u(x)]_{x,u} x} \arrow[u, "{[f_u(x)]_{x,u} = [\delta_u(x)]_{x,u} F^{-1}}"] \arrow[r, "A^{\mathsf{E}} = ?"] & {A^{\mathsf{E}} X = [f_u(x)]_{x,u} F\ T^{\mathsf{E}(u)}\ F^{-1}\ x}
\end{tikzcd}$$

- The transition matrix under $[f_u(x)]_{x,u}$ is

$$A^{\mathsf{E}} = F\ T^{\mathsf{E}}\ F^{-1} = [f_u(x)]_{x,u}^{-1}\ T^{\mathsf{E}}\ [f_u(x)]_{x,u}$$

A^{E} is a similar matrix of T^{E}

Use different bases for input/output spaces (new)

- Choose $[f_u(x)]_{x,u}$ as the input basis, and $[g_u(x)]_{x,u}$ as the output basis

$$\begin{tikzcd}
\mathbb{K}[\mathbb{F}_2^n] = Span\left([\delta_u(x)]_{x,u}\right) \arrow[rr, "T^{\mathrm{E}}"] \arrow[d, leftrightarrow, "{[\delta_u(x)]_{x,u} = [f_u(x)]_{x,u}F}"] & & \mathbb{K}[\mathbb{F}_2^n] = Span\left([\delta_u(x)]_{x,u}\right) \arrow[d, leftrightarrow, "{[\delta_u(x)]_{x,u} = [g_u(x)]_{x,u}G}"] \\
\mathbb{K}[\mathbb{F}_2^n] = Span\left([f_u(x)]_{x,u}\right) \arrow[rr, "A^{\mathrm{E}} =?"] & & \mathbb{K}[\mathbb{F}_2^n] = Span\left([g_u(x)]_{x,u}\right)
\end{tikzcd}$$

Use different bases for input/output spaces (new)

- Choose $[f_u(x)]_{x,u}$ as the input basis, and $[g_u(x)]_{x,u}$ as the output basis

$$\begin{tikzcd}
\mathbb{K}[\mathbb{F}_2^n] = Span\left([\delta_u(x)]_{x,u}\right) \arrow[r, "T^{\mathsf{E}}"] \arrow[d, leftrightarrow, "{[\delta_u(x)]_{x,u} = [f_u(x)]_{x,u}F}"] & \mathbb{K}[\mathbb{F}_2^n] = Span\left([\delta_u(x)]_{x,u}\right) \arrow[d, leftrightarrow, "{[\delta_u(x)]_{x,u} = [g_u(x)]_{x,u}G}"] \\
\mathbb{K}[\mathbb{F}_2^n] = Span\left([f_u(x)]_{x,u}\right) \arrow[r, "A^{\mathsf{E}} =?"] & \mathbb{K}[\mathbb{F}_2^n] = Span\left([g_u(x)]_{x,u}\right)
\end{tikzcd}$$

- The transition matrix can be constructed in a similar way

$$\begin{tikzcd}
{[\delta_u(x)]_{x,u}\ F^{-1}\ x} \arrow[r, "T^{\mathsf{E}}"] & {[\delta_u(x)]_{x,u}\ T^{\mathsf{E}}\ \ F^{-1}\ x} \arrow[d, "{[\delta_u(x)]_{x,u} = [g_u(x)]_{x,u}G}"] \\
X = [f_u(x)]_{x,u}x \arrow[u, "{[f_u(x)]_{x,u} = [\delta_u(x)]_{x,u}F^{-1}}"] \arrow[r, "A^{\mathsf{E}}"] & A^{\mathsf{E}}X = [g_u(x)]_{x,u}G\ T^{\mathsf{E}(u)}\ F^{-1}\ x
\end{tikzcd}$$

Use different bases for input/output spaces (new)

- Choose $[f_u(x)]_{x,u}$ as the input basis, and $[g_u(x)]_{x,u}$ as the output basis

$$\begin{tikzcd}
\mathbb{K}[\mathbb{F}_2^n] = Span([\delta_u(x)]_{x,u}) \arrow[r, "T^{\mathrm{E}}"] \arrow[d, leftrightarrow, "{[\delta_u(x)]_{x,u} = [f_u(x)]_{x,u} F}"] & \mathbb{K}[\mathbb{F}_2^n] = Span([\delta_u(x)]_{x,u}) \arrow[d, leftrightarrow, "{[\delta_u(x)]_{x,u} = [g_u(x)]_{x,u} G}"] \\
\mathbb{K}[\mathbb{F}_2^n] = Span([f_u(x)]_{x,u}) \arrow[r, "A^{\mathrm{E}} =?"] & \mathbb{K}[\mathbb{F}_2^n] = Span([g_u(x)]_{x,u})
\end{tikzcd}$$

- The transition matrix can be constructed in a similar way

$$\begin{tikzcd}
{[\delta_u(x)]_{x,u}\ F^{-1}\ x} \arrow[r, "T^{\mathrm{E}}"] & {[\delta_u(x)]_{x,u}\ T^{\mathrm{E}}\ \ F^{-1}\ x} \arrow[d, "{[\delta_u(x)]_{x,u} = [g_u(x)]_{x,u} G}"] \\
X = [f_u(x)]_{x,u} x \arrow[u, "{[f_u(x)]_{x,u} = [\delta_u(x)]_{x,u} F^{-1}}"] \arrow[r, "A^{\mathrm{E}}"] & A^{\mathrm{E}} X = [g_u(x)]_{x,u} G\ T^{\mathrm{E}(u)}\ F^{-1}\ x
\end{tikzcd}$$

- The transition matrix under $[f_u(x)]_{x,u}$ and $[g_u(x)]_{x,u}$: $A^{\mathrm{E}} = G\ T^{\mathrm{E}}\ F^{-1} = [g_u(x)]_{x,u}^{-1}\ T^{\mathrm{E}}\ [f_u(x)]_{x,u}$.

Use different bases for input/output spaces (new)

- Choose $[f_u(x)]_{x,u}$ as the input basis, and $[g_u(x)]_{x,u}$ as the output basis

$$\begin{tikzcd}
\mathbb{K}[\mathbb{F}_2^n] = Span\left([\delta_u(x)]_{x,u}\right) \arrow[rr, "T^{\mathrm{E}}"] \arrow[d, leftrightarrow, "{[\delta_u(x)]_{x,u} = [f_u(x)]_{x,u}F}"] & & \mathbb{K}[\mathbb{F}_2^n] = Span\left([\delta_u(x)]_{x,u}\right) \arrow[d, leftrightarrow, "{[\delta_u(x)]_{x,u} = [g_u(x)]_{x,u}G}"] \\
\mathbb{K}[\mathbb{F}_2^n] = Span\left([f_u(x)]_{x,u}\right) \arrow[rr, "A^{\mathrm{E}} =?"] & & \mathbb{K}[\mathbb{F}_2^n] = Span\left([g_u(x)]_{x,u}\right)
\end{tikzcd}$$

- The transition matrix can be constructed in a similar way

$$\begin{tikzcd}
{[\delta_u(x)]_{x,u}}\ F^{-1}\ x \arrow[rr, "T^{\mathrm{E}}"] & & {[\delta_u(x)]_{x,u}}\ T^{\mathrm{E}}\ \ F^{-1}\ x \arrow[d, "{[\delta_u(x)]_{x,u} = [g_u(x)]_{x,u}G}"] \\
X = [f_u(x)]_{x,u}x \arrow[u, "{[f_u(x)]_{x,u} = [\delta_u(x)]_{x,u}F^{-1}}"] \arrow[rr, "A^{\mathrm{E}}"] & & A^{\mathrm{E}}X = [g_u(x)]_{x,u}G\ T^{\mathrm{E}(u)}\ \ F^{-1}\ x
\end{tikzcd}$$

- The transition matrix under $[f_u(x)]_{x,u}$ and $[g_u(x)]_{x,u}$: $A^{\mathrm{E}} = G\ T^{\mathrm{E}}\ F^{-1} = [g_u(x)]_{x,u}^{-1}\ T^{\mathrm{E}}\ [f_u(x)]_{x,u}$.

  Remark. The possibility of using different bases in geometric approach had been mentioned in Beyne's thesis, but no one really explored it in cryptanalysis.

Calculate coordinates of a transition matrix

Assume that $[g_u(x)]^{-1}_{x,u} = [g^\star_u(x)]_{x,u}$ (only for a compact representation).

- The specific coordinate of A^{E}:

$$\begin{aligned}
A^{\mathrm{E}}_{v,u} &= \delta_v^\top \; [g^\star_u(x)]_{x,u} \; T^{\mathrm{E}} \; [f_u(x)]_{x,u} \; \delta_u \\
&= [g^\star_x(v), 0 \le x < 2^n]^\top \, T^{\mathrm{E}} \; [f_u(x), 0 \le x < 2^n] \\
&= \left[\sum_x g^\star_x(v)\delta_x(E(y)), 0 \le y < 2^n\right]^\top \; [f_u(x), 0 \le x < 2^n] \\
&= \sum_{x \in \mathbb{F}_2^n} g^\star_{\mathrm{E}(x)}(v) f_u(x)
\end{aligned}$$

Known bases and rules for generating new ones

- Three known bases for $\mathbb{Q}[\mathbb{F}_2^n]$
  - Standard basis $[\delta_u(x)]_{x,u}$ [Beyne, AC 21]
  - Linear basis $[(-1)^{u^\top x}]_{x,u}$ [Beyne, AC 21]
  - Ultrametric integral basis $[(-1)^{\mathsf{wt}(x \oplus u)} u^x]$ [BV, AC 24]
- Three rules for generating new bases (any preserving-rank operation can be a rule)
  - Inverse: If $[\alpha_u(x)]_{x,u}$ is a basis, $[\alpha_u(x)]_{x,u}^{-1}$ is also a basis
  - Transpose: If $[\alpha_u(x)]_{x,u}$ is a basis, $[\alpha_u(x)]_{x,u}^{\top}$ is also a basis
  - Scale: If $[\alpha_u(x)]_{x,u}$ is a basis, $[k\alpha_u(x)]_{x,u}$ is a basis, where $k \in \mathbb{K} \backslash \{0\}$
- Four new bases
  - Inverse of linear basis: $[2^{-n}(-1)^{u^\top x}]_{x,u}$
  - Inverse of ultrametric integral basis: $[u^x]_{x,u}$
  - Transpose of ultrametric integral basis: $[(-1)^{\mathsf{wt}(u \oplus x)} x^u]_{x,u}$
  - Inverse and transpose of ultrametric integral basis: $[x^u]_{x,u}$

Seven Bases and effects

Choose different bases, we get different attacks

$$A^{\mathsf{E}}_{v,u} = \sum_{x \in \mathbb{F}_2^n} g^{\star}_{\mathsf{E}(x)}(v) f_u(x)$$

Index	Basis	Effect of input $f_u(x)$	Effect of output $g^{\star}_{\mathsf{E}(x)}(v)$
0	$[\delta_u(v)]_{v,u}$	$\delta_u(x)$	$\delta_{\mathsf{E}(x)}(v)$
1	$[(-1)^{u^\top v}]_{v,u}$	$(-1)^{u^\top x}$	$2^{-n}(-1)^{\mathsf{E}(x)^\top v}$
2	$[2^{-n}(-1)^{u^\top v}]_{v,u}$	$2^{-n}(-1)^{u^\top x}$	$(-1)^{\mathsf{E}(x)^\top v}$
3	$[u^v]_{v,u}$	u^x	$(-1)^{\mathrm{wt}(v \oplus \mathsf{E}(x))}\mathsf{E}^v(x)$
4	$[(-1)^{\mathrm{wt}(u \oplus v)} u^v]_{v,u}$	$(-1)^{\mathrm{wt}(u \oplus x)} u^x$	$\mathsf{E}^v(x)$
5	$[v^u]_{v,u}$	x^u	$(-1)^{\mathrm{wt}(v \oplus \mathsf{E}(x))} v^{\mathsf{E}(x)}$
6	$[(-1)^{\mathrm{wt}(u \oplus v)} v^u]_{v,u}$	$(-1)^{\mathrm{wt}(u \oplus x)} x^u$	$v^{\mathsf{E}(x)}$

Same-basis and Mix-basis Attacks

Definition (Same-basis and mix-basis attack)

An attack on $\mathsf{E} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called a same-basis attack if the bases for the input/output spaces are the same; otherwise, a mix-basis attack.

- Divide $\mathsf{E} = \mathsf{E}_2 \circ \mathsf{E}_1 \circ \mathsf{E}_0$. $[f_u(x)]_{x,u}/[f_u(x)]_{x,u}$ for E_0, $[f_u(x)]_{x,u}/[g_u(x)]_{x,u}$ for E_1, $[g_u(x)]_{x,u}/[g_u(x)]_{x,u}$ for E_2

$$\begin{tikzcd}
\mathbb{Q}[(\mathbb{F}_2^n)^d] \arrow[r, "T^{\mathsf{E}_0}"] \arrow[d, leftrightarrow] & \mathbb{Q}[(\mathbb{F}_2^n)^d] \arrow[r, "T^{\mathsf{E}_1}"] \arrow[d, leftrightarrow] & \mathbb{Q}[(\mathbb{F}_2^n)^d] \arrow[r, "T^{\mathsf{E}_2}"] \arrow[d, leftrightarrow] & \mathbb{Q}[(\mathbb{F}_2^n)^d] \arrow[d, leftrightarrow] \\
\mathbb{Q}[(\mathbb{F}_2^n)] \arrow[r, "A^{\mathsf{E}_0} = {[f_u(x)]_{x,u}^{-1}} T^{\mathsf{E}_0} {[f_u(x)]_{x,u}}"'] & \mathbb{Q}[(\mathbb{F}_2^n)] \arrow[r, "A^{\mathsf{E}_1} = {[g_u(x)]_{x,u}^{-1}} T^{\mathsf{E}_1} {[f_u(x)]_{x,u}}"] & \mathbb{Q}[(\mathbb{F}_2^n)] \arrow[r, "A^{\mathsf{E}_2} = {[g_u(x)]_{x,u}^{-1}} T^{\mathsf{E}_2} {[g_u(x)]_{x,u}}"'] & \mathbb{Q}[(\mathbb{F}_2^n)]
\end{tikzcd}$$

Finally,

$$\begin{aligned} A^{\mathsf{E}} = A^{\mathsf{E}_2} A^{\mathsf{E}_1} A^{\mathsf{E}_0} &= [g_u(x)]_{x,u}^{-1} T^{\mathsf{E}_2} \left([g_u(x)]_{x,u} [g_u(x)]_{x,u}^{-1} \right) T^{\mathsf{E}_1} \left([f_u(x)]_{x,u} [f_u(x)]_{x,u}^{-1} \right) T^{\mathsf{E}_0} [f_u(x)]_{x,u} \\ &= [g_u(x)]_{x,u}^{-1} T^{\mathsf{E}_2} T^{\mathsf{E}_1} T^{\mathsf{E}_0} [f_u(x)]_{x,u} \end{aligned}$$

Several Examples

- Linear cryptanalysis (same-basis) [Beyne, AC 21]. Input basis: $[(-1)^{u^\top x}]_{x,u}$, output basis $[(-1)^{u^\top x}]_{x,u}$

$$A^{\mathsf{E}}_{v,u} = \sum_{x\in\mathbb{F}_2^n} (-1)^{u^\top x} 2^{-n} (-1)^{v^\top \mathsf{E}(x)} = 2^{-n} \sum_{x\in\mathbb{F}_2^n} (-1)^{u^\top x \oplus v^\top \mathsf{E}(x)}$$

- Ultrametric integral cryptanalysis (same-basis) [BV, AC 24]. Input basis $[(-1)^{\mathrm{wt}(u\oplus x)} u^x]_{x,u}$, output basis $[(-1)^{\mathrm{wt}(u\oplus x)} u^x]_{x,u}$

$$A^{\mathsf{E}}_{v,u} = \sum_{x\in\mathbb{F}_2^n} (-1)^{\mathrm{wt}(u\oplus x)} u^x \mathsf{E}^v(x) = \sum_{x\preceq u} (-1)^{\mathrm{wt}(u\oplus x)} \mathsf{E}^v(x)$$

- Subspace propagation (mix-basis, new). Input basis $[u^x]_{x,u}$, output basis $[(-1)^{\mathrm{wt}(u\oplus x)} x^u]_{x,u}$

$$A^{\mathsf{E}}_{v,u} = \sum_{x\in\mathbb{F}_2^n} u^x v^{\mathsf{E}(x)} = \sum_{x\preceq u, \mathsf{E}(x)\preceq v} 1$$

Orders of Attacks

Definition (Order)

Suppose a space $\mathbb{S} \cong (\mathbb{F}_2^n)^d$, we call the smallest d the order of $\mathbb{S}$. If an attack on $\mathsf{E} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ take plaintext/ciphertext samples from d-th-order space, we call this attack a d-th-order attack.

- A d-th-attack works on

$$\mathsf{E}^{\times d} : (\mathbb{F}_2^n)^d \to (\mathbb{F}_2^n)^d; (x, \Delta_1, \ldots, \Delta_{d-1}) \mapsto \big(\mathsf{E}(x), D_{\Delta_1}(\mathsf{E}(x)), D_{\Delta_2}(\mathsf{E}(x)), \ldots, D_{\Delta_{d-1}}(\mathsf{E}(x))\big)$$

- $[f_u(x)]_{x,u}^{(i)}$ is a basis for the i-th $\mathbb{K}[\mathbb{F}_2^n]$, a basis for $\mathbb{K}[(\mathbb{F}_2^n)^d]$ is $\bigotimes_{0 \le i < d} [f_u(x)]_{x,u}^{(i)}$.

Several Examples

- Differential attack (same-basis, 2nd order) [BR, C 22]. Input basis $[(-1)^{u^\top x}]_{x,u} \otimes [\delta_u(x)]_{x,u}$, output basis $[(-1)^{u^\top x}]_{x,u} \otimes [\delta_u(x)]_{x,u}$

$$A^{\mathsf{E}}_{(v_0,v_1),(u_0,u_1)} = \sum_{x\in\mathbb{F}_2^n,\Delta\in\mathbb{F}_2^n} (-1)^{u_0^\top x}\delta_{u_1}(\Delta)2^{-n}(-1)^{v_0^\top \mathsf{E}(x)}\delta_{v_1}(D_\Delta(x))$$

$$= \sum_{\substack{x\in\mathbb{F}_2^n\\ \mathsf{E}(x)\oplus\mathsf{E}(x\oplus u_1)=v_1}} (-1)^{u_0^\top x\oplus v_0^\top \mathsf{E}(x)} \xrightarrow{u_0=v_0=0} \sum_{\substack{x\in\mathbb{F}_2^n\\ \mathsf{E}(x)\oplus\mathsf{E}(x\oplus u_1)=v_1}} 1$$

- d-differential (same-basis, d-th order) [WSW+, TIT 23]. Input/output basis $[(-1)^{u^\top x}]_{x,u} \bigotimes_{1\le i\le d}[\delta_u(x)]_{x,u}$

$$A^{\mathsf{E}}_{(v_0,\dots,v_d),(u_0,\dots u_d)} = \;= \sum_{\substack{x\in\mathbb{F}_2^n\\ \mathsf{E}(x)\oplus\mathsf{E}(x\oplus u_i)=v_i,0\le i\le d}} (-1)^{u_i^\top x\oplus v_0^\top \mathsf{E}(x)} \xrightarrow{u_0=v_0=0} \sum_{\substack{x\in\mathbb{F}_2^n\\ \mathsf{E}(x)\oplus\mathsf{E}(x\oplus u_i)=v_i,0\le i\le d}} 1$$

- Differential-linear attack (mix-basis, 2nd order, new). Input/output basis $[(-1)^{u^\top x}]_{x,u} \otimes [\delta_u(x)]_{x,u}/2^{-n}[(-1)^{u^\top x}]_{x,u} \otimes [(-1)^{u^\top x}]_{x,u}$

$$A^{\mathsf{E}}_{(v_0,v_1),(u_0,u_1)} = 2^{-n} \sum_{x\in\mathbb{F}_2^n,\Delta=u_1} (-1)^{u_0^\top x\oplus v_0^\top \mathsf{E}(x)\oplus v_1^\top D_\Delta(x)} \xrightarrow{u_0=v_0=0} 2^{-n} \sum_{x\in\mathbb{F}_2^n,\Delta=u_1} (-1)^{v_1^\top D_\Delta(x)}$$

Example applications

- An alternative method of studying the same property in ultrametric integral cryptanalysis [BV, AC 24]
  - Choose $[u^x]_{x,u}/[(-1)^{\mathrm{wt}(u \oplus x)} u^x]_{x,u}$ for input/output spaces
  - Attacking expression: $A^{\mathsf{E}}_{v,u} = \sum_{x \preceq u} \mathsf{E}^v(x)$

Example applications

- An alternative method of studying the same property in ultrametric integral cryptanalysis [BV, AC 24]
  - Choose $[u^x]_{x,u}/[(-1)^{\mathrm{wt}(u \oplus x)} u^x]_{x,u}$ for input/output spaces
  - Attacking expression: $A^{\mathsf{E}}_{v,u} = \sum_{x \preceq u} \mathsf{E}^v(x)$

- Automatic search models for the multiple-of-n property for SKINNY-64 [GRR, EC 17][BCC, ToSC 19]
  - (First-order method) Choose $[u^x]_{x,u}/[(-1)^{\mathrm{wt}(u \oplus x)} x^u]_{x,u}$ for input/output spaces
    Attacking expression:

$$A^{\mathsf{E}}_{v,u} = \sum_{x \preceq u, \mathsf{E}(x) \preceq v} 1$$

$A^{\mathsf{E}}_{v,u}(A^{\mathsf{E}}_{v,u} - 1)/2$ is the number of unordered pairs

Example applications

- An alternative method of studying the same property in ultrametric integral cryptanalysis [BV, AC 24]
  - Choose $[u^x]_{x,u}/[(-1)^{\mathrm{wt}(u \oplus x)} u^x]_{x,u}$ for input/output spaces
  - Attacking expression: $A^{\mathsf{E}}_{v,u} = \sum_{x \preceq u} \mathsf{E}^v(x)$

- Automatic search models for the multiple-of-n property for SKINNY-64 [GRR, EC 17][BCC, ToSC 19]
  - (First-order method) Choose $[u^x]_{x,u}/[(-1)^{\mathrm{wt}(u \oplus x)} x^u]_{x,u}$ for input/output spaces
    Attacking expression:
    $$A^{\mathsf{E}}_{v,u} = \sum_{x \preceq u, \mathsf{E}(x) \preceq v} 1$$
    $A^{\mathsf{E}}_{v,u}(A^{\mathsf{E}}_{v,u} - 1)/2$ is the number of unordered pairs
  - (Second-order method) Choose $[u^x]_{x,u} \otimes [u^x]_{x,u}/[(-1)^{\mathrm{wt}(u \oplus x)} x^u]_{x,u} \otimes [(-1)^{\mathrm{wt}(u \oplus x)} x^u]_{x,u}$ for input/output spaces
    Attacking expression:
    $$A^{\mathsf{E}}_{(v_0,v_1),(u_0,u_1)} = \sum_{x \preceq u_0, \Delta \preceq u_1, \mathsf{E}(x) \preceq v_0, D_\Delta(\mathsf{E}(x)) \preceq v_1} 1$$
    (Set $u_0 = u_1 = u$, $v_0 = \mathbf{1}$, $A^{\mathsf{E}}_{(v_0,v_1),(u_0,u_1)}$ is the number of unordered pairs)

Example applications

- An alternative method of studying the same property in ultrametric integral cryptanalysis [BV, AC 24]
    - Choose $[u^x]_{x,u}/[(-1)^{\mathrm{wt}(u\oplus x)}u^x]_{x,u}$ for input/output spaces
    - Attacking expression: $A^{\mathsf{E}}_{v,u} = \sum_{x\preceq u} \mathsf{E}^v(x)$

- Automatic search models for the multiple-of-n property for SKINNY-64 [GRR, EC 17][BCC, ToSC 19]
    - (First-order method) Choose $[u^x]_{x,u}/[(-1)^{\mathrm{wt}(u\oplus x)}x^u]_{x,u}$ for input/output spaces
      Attacking expression:
      $$A^{\mathsf{E}}_{v,u} = \sum_{x\preceq u, \mathsf{E}(x)\preceq v} 1$$
      $A^{\mathsf{E}}_{v,u}(A^{\mathsf{E}}_{v,u}-1)/2$ is the number of unordered pairs
    - (Second-order method) Choose $[u^x]_{x,u}\otimes[u^x]_{x,u}/[(-1)^{\mathrm{wt}(u\oplus x)}x^u]_{x,u}\otimes[(-1)^{\mathrm{wt}(u\oplus x)}x^u]_{x,u}$ for input/output spaces
      Attacking expression:
      $$A^{\mathsf{E}}_{(v_0,v_1),(u_0,u_1)} = \sum_{x\preceq u_0, \Delta\preceq u_1, \mathsf{E}(x)\preceq v_0, D_\Delta(\mathsf{E}(x))\preceq v_1} 1$$
      (Set $u_0=u_1=u$, $v_0=\mathbf{1}$, $A^{\mathsf{E}}_{(v_0,v_1),(u_0,u_1)}$ is the number of unordered pairs)
- Verification for 2 differential-linear distinguishers of SIMON-32 and -48 [HDE, C 24] without the round independence assumption

Summary

- We explored the possibility to use different bases in Beyne's geometric approach
- The geometric approach becomes more flexible, and can be applied to more attacks, especially combined ones
- All attacks can be studied in the unified automatic search method
- We applied mix-basis geometric approach to several known attacks, and provided new methods to study them

Summary

- We explored the possibility to use different bases in Beyne's geometric approach
- The geometric approach becomes more flexible, and can be applied to more attacks, especially combined ones
- All attacks can be studied in the unified automatic search method
- We applied mix-basis geometric approach to several known attacks, and provided new methods to study them

Thank you for your attention!

References

[GRR, EC 17] L. Grassi, C. Rechberger, S. Rønjom: A new structural-differential property of 5-round AES. EUROCRYPT 2017

[Todo, EC 15] Y. Todo, Structural evaluation by generalized integral property. EUROCRYPT 2015

[Beyne, thesis] T. Beyne: A geometric approach to symmetric-Key cryptanalysis. PHD Thesis

[Bey, AC 21] T. Beyne: A geometric approach to linear cryptanalysis. ASIACRYPT 2021

[BR, AC 22] T. Beyne, V. Rijmen: Differential cryptanalysis in the fixed-key model. CRYPTO 2022

[BV, AC 24] T. Beyne, M. Verbauwhede: Ultrametric integral cryptanalysis. ASIACRYPT 2024

[WSW+, TIT 24] L. Wang, L. Song, B. Wu, M. Rahman, and T. Isobe.

[BCC, ToSC 19] C. Boura, A. Canteaut, D. Coggia: A general proof framework for recent AES distinguishers. ToSC 2019 Revisiting the boomerang attack from a perspective of 3-differential. IEEE TIT 2024

[HDE24] H. Hadipour, P. Derbez and M. Eichlseder: Revisiting Differential-Linear Attacks via a