# Pairwise independence of AES-like block ciphers

Tim Beyne

COSIC, KU Leuven

April 13, 2026


*based on joint work with Gregor Leander and Immo Schütt*

# Motivation

- Most important problem in (symmetric?) cryptography:

  *Prove that our primitives are secure, or show that they are not.*

- Progress so far?
  - Limited set of general cryptanalytic techniques
  - Limited security arguments

- Solution to all cryptanalytic problems: the geometric approach
  *Maybe it also works for security arguments?*

# Backstory

## A Short Note on a Weight Probability Distribution Related to SPNs

Sondre Rønjom

Department of Informatics
University of Bergen, Norway

**Abstract.** We report on a simple technique that supports some recent developments on AES by Grassi and Rechberger and Bao, Guo and List. We construct a weight transition probability matrix related to AES that characterises fixed configurations of active bytes in differences of ciphertexts when plaintext differences are fixed to some (possibly other) configuration of active bytes. The construction is very simple and requires only a little bit of linear algebra. The derived probabilities are essentially identical to recent results on 5- and 6-rounds AES derived through more sophisticated means, indicating that it might be worth a further investigation.

ePrint 2019/750

# Backstory

- Truncated differentials for the AES
  Singular values of the difference-distribution matrix
- Application to pairwise independence
  Masters' thesis of Immo Schütt (Ruhr University Bochum, March 2025)
- Joint paper with Gregor Leander and Immo Schütt (ePrint 2025/1495)
- Independent work of Itai Dinur (ePrint 2025/1326)

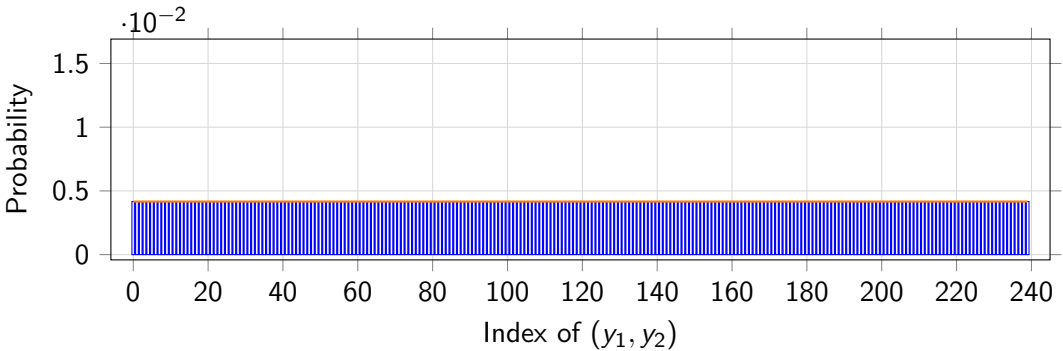
# Almost pairwise independence

- Pairwise decorrelation (Vaudenay)
- Almost $\varepsilon$-pairwise independence of a block cipher $E_k \colon \mathbb{F}_q^n \to \mathbb{F}_q^n$
- Definition: for all $(x_1, x_2)$ with $x_1 \neq x_2$,

$$\frac{1}{2} \sum_{y_1 \neq y_2} \left| \Pr_{\boldsymbol{k}} \left[ (E_{\boldsymbol{k}}(x_1), E_{\boldsymbol{k}}(x_2)) = (y_1, y_2) \right] - \frac{1}{q^n} \times \frac{1}{q^n - 1} \right| \leq \varepsilon$$

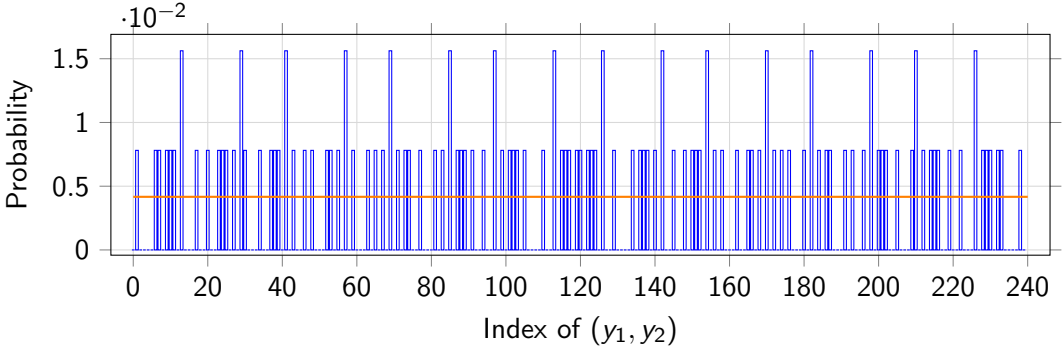
# Almost pairwise independence

## Example: $x \mapsto k_1\, x + k_2$ on $\mathbb{F}_{2^4}$ with $k_1 \neq 0$



# Almost pairwise independence

## Example: $x \mapsto (x + k_1)^{-1} + k_2$ on $\mathbb{F}_{2^4}$




- For most block ciphers, $\varepsilon$ is large (barely enough randomness)
- Relevance of pairwise independence for cryptanalysis?

# Overview

- Pairwise independence from the point of view of cryptanalysis
- Proof strategy
- Pairwise independence of the AES

# Pairwise independence from the point of view of cryptanalysis

- Difference-distribution matrix $D$ of a *random function* $\boldsymbol{F}$:

$$D_{b,a} = \Pr_{\boldsymbol{F},\boldsymbol{x}}\big[\boldsymbol{F}(\boldsymbol{x}+a) = \boldsymbol{F}(\boldsymbol{x}) + b\big]$$

- Difference-distribution matrix $U$ of a uniform random permutation:

$$U_{b,a} = \begin{cases} 1 & \text{if } a = 0 \text{ and } b = 0\,, \\ 1/(q^n - 1) & \text{if } a \neq 0 \text{ and } b \neq 0\,, \\ 0 & \text{else}\,. \end{cases}$$

- A (whitened) block cipher $\boldsymbol{F} = E_{\boldsymbol{k}}$ is $\varepsilon$-pairwise independent iff $\|D - U\|_1 \leq 2\varepsilon$

# Composition of functions

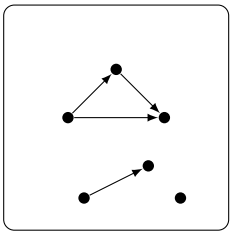
- Let $D_1, \ldots, D_r$ be difference-distribution matrices of independent random functions $\boldsymbol{F}_1, \ldots, \boldsymbol{F}_r$ with input- and output whitening key additions
- If $D$ is the difference-distribution matrix of $\boldsymbol{F}_r \circ \cdots \circ \boldsymbol{F}_1$, then

$$D = D_r \cdots D_2 D_1$$

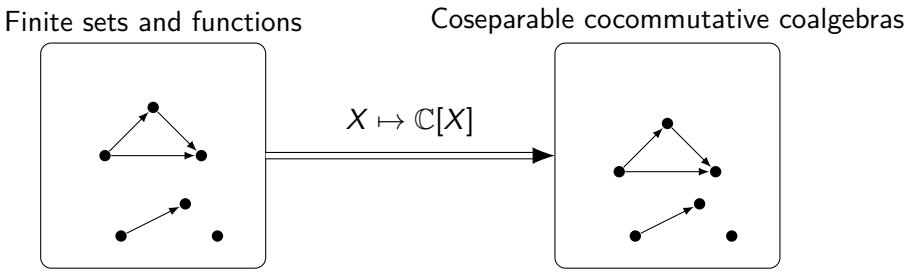
Assumption that $\boldsymbol{F}_1, \ldots, \boldsymbol{F}_r$ are independent random functions is **void**
Pairwise independence is (mostly) not about differential cryptanalysis

# Geometric approach

Finite sets and functions



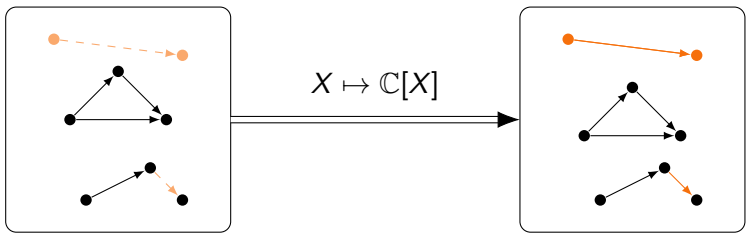
# Geometric approach



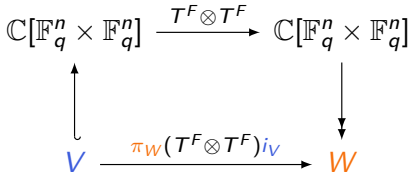
# Geometric approach

'Approximate' finite sets and functions

Vector spaces



# Pairwise attacks in the geometric approach




- Subspaces $V$ and $W$ define a (cryptanalytic) property
- 'Approximation map' for subspaces $V$ and $W$ of $\mathbb{C}[\mathbb{F}_q^n]$

$$\pi_W(T^F \otimes T^F) i_V$$

# Pairwise attacks in the geometric approach

## Translation-invariant properties

- $\mathbb{F}_q^n$ acts on $\mathbb{C}[\mathbb{F}_q^n \times \mathbb{F}_q^n]$ by addition: $\delta_x \otimes \delta_y \mapsto \delta_{x+k} \otimes \delta_{y+k}$
- For translation-invariant properties, $V$ and $W$ are fixed under this action:

$$V, W \subseteq \mathrm{Fix}_{\mathbb{F}_q^n}\big(\mathbb{C}[\mathbb{F}_q^n \times \mathbb{F}_q^n]\big) = \mathrm{Span}\left\{\sum_{x \in \mathbb{F}_q^n} \delta_x \otimes \delta_{x+a} \;\middle|\; a \in \mathbb{F}_q^n\right\} \cong \mathbb{C}[\mathbb{F}_q^n]$$

- Difference-distribution matrix of $F$:

$$D = \pi_W\big(T^F \otimes T^F\big) i_V \quad \text{for } V = W = \mathrm{Fix}_{\mathbb{F}_q^n}\big(\mathbb{C}[\mathbb{F}_q^n \times \mathbb{F}_q^n]\big)$$

# Characterizing the class of techniques ruled out by pairwise independence

- Trails $(V_1, V_2, \ldots, V_{r+1})$ with $V_1, V_2, \ldots, V_{r+1} \subseteq \mathbb{C}[\mathbb{F}_q^n \times \mathbb{F}_q^n]$
- A trail is translation-invariant if $V_i \subseteq \mathrm{Fix}_{\mathbb{F}_q^n}\big(\mathbb{C}[\mathbb{F}_q^n \times \mathbb{F}_q^n]\big)$
- Composition of difference-distribution matrices is the 'piling-up principle':

$$\pi_{V_{r+1}}\big(T^{F_r} \otimes T^{F_r}\big) i_{V_r} \times \cdots \times \pi_{V_2}\big(T^{F_1} \otimes T^{F_1}\big) i_{V_1}$$

- Equivalent (basis-dependent) descriptions
  - Quasidifferential basis: masks are zero
  - Double linear basis: value masks are zero

# Overview

- Pairwise independence from the point of view of cryptanalysis
  Ruling out translation-invariant 'pairwise methods' over $\mathbb{C}$ (Archimedean)
- Proof strategy
- Pairwise independence of the AES

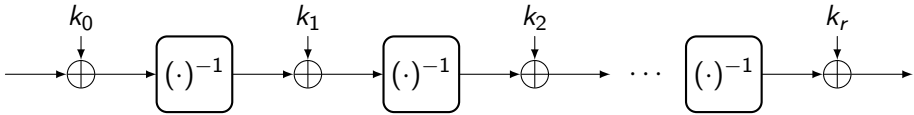
# Proof strategy

- Since $D_i U = U = U D_i$ and $U^2 = U$,

$$D - U = (D_r - U) \cdots (D_2 - U)(D_1 - U)$$

- High-level proof strategy:
  - Bound $\|D_r \cdots D_2 - U\|_2$
  - Bound $\|D_1 - U\|_{2,1}$
  - $\|D - U\|_1 \leq \|D_r \cdots D_2 - U\|_2 \, \|D_1 - U\|_{2,1}$

# Example: key-alternating cipher with inverse round function




- Maximum differential probability for one round: $p_{\max} \leq 4/q$
- 'Spectral uniformity' for one round: $\|D - U\|_2 \leq 1/\sqrt{q} + 2/q$
  Proof: ask GPT 5.4 (nice argument from circulant structure)
- Pairwise independence bound for $r + 1$ rounds:

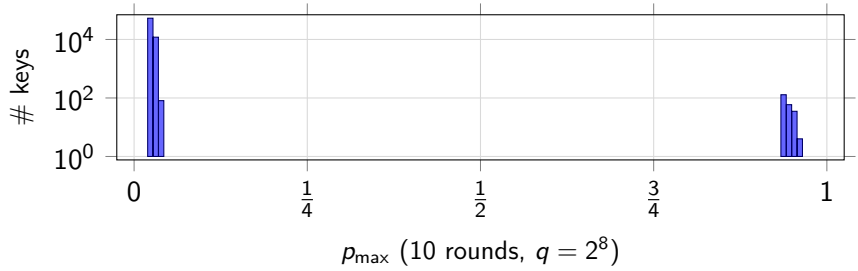
$$\|D - U\|_1 \leq \|D_2 - U\|_2 \, \|D_1 - U\|_{2,1} \leq 4\sqrt{q} \left( \frac{1}{\sqrt{q}} + \frac{2}{q} \right)^r \asymp q^{1-r/2}$$

# Example: key-alternating cipher with inverse round function

- Rational interpolation attack (Jakobsen & Knudsen)

$$E(x) = \frac{x + a}{bx + c} \quad \text{for most } x$$

- Not a pairwise attack
- Intricately related to fixed-key probabilities:

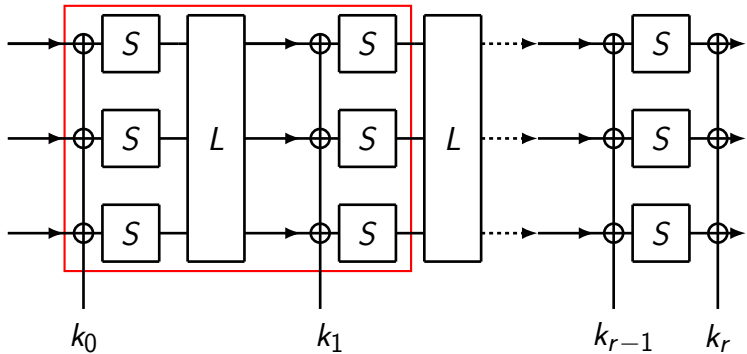


# Overview

- Pairwise independence from the point of view of cryptanalysis
  Ruling out translation-invariant 'pairwise methods' over $\mathbb{C}$ (Archimedean)
- Proof strategy
  Bounding the operator norm $\|D - U\|_2$ (no randomness needed)
- Pairwise independence of the AES

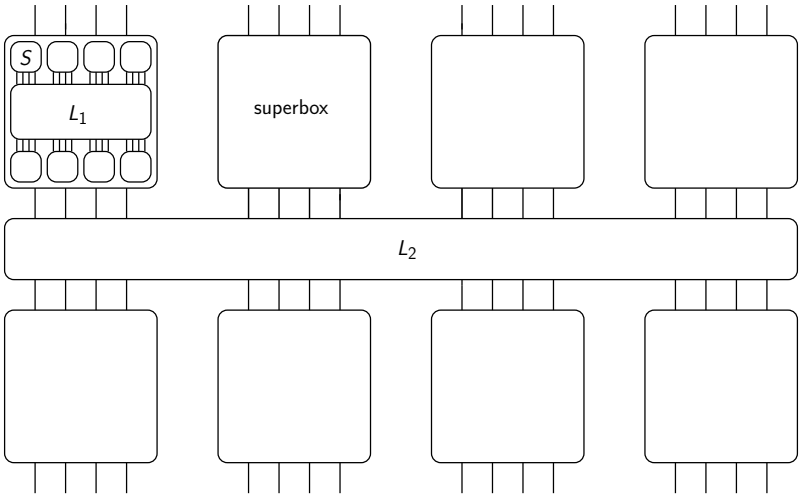
# Pairwise independence of the AES

## SHARK structure



# Pairwise independence of the AES

## SHARK structure



# Pairwise independence of the AES

## High-level proof strategy

- $D = (D^S)^{\otimes n} D^L (D^S)^{\otimes n}$

- For $z \in \{0,1\}^n$, define $[z] = [z_1] \times [z_2] \times \cdots \times [z_n]$ with $[0] = \{0\}$ and $[1] = \mathbb{F}_q$
- Truncated differentials defined by activity patterns:

$$V = \mathrm{Span}\left\{ \delta_{[z]} = \textstyle\sum_{x \in [z]} \delta_x \;\middle|\; z \in \{0,1\}^n \right\} \subset \mathbb{R}[\mathbb{F}_q^n]$$

- Strategy: split translation-invariant trails using $\mathbb{R}[\mathbb{F}_q^n] = V \oplus V^\perp$

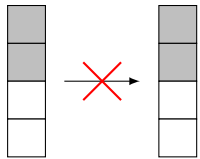
$$\|D - U\|_2 \leq \left\| \begin{bmatrix} \|\pi_V \ (D-U) i_V\|_2 & \|\pi_V \ (D-U)\, i_V \ \|_2 \\ \|\pi_{V^\perp} (D-U)\, i_V\|_2 & \|\pi_{V^\perp} (D-U)\, i_{V^\perp}\|_2 \end{bmatrix} \right\|_2$$

# Pairwise independence of the AES

## Truncated differentials: $\|\pi_V(D-U)i_V\|_2$

- $2^n$ activity patterns: compute norm of $2^n \times 2^n$ matrix (easy)
  - $n = 4$ and $q = 2^8$: $\|\pi_V(D-U)i_V\|_2 \approx 2^{-13}$
  - $n = 4$ and $q = 2^{32}$: $\|\pi_V(D-U)i_V\|_2 \approx 2^{-61}$

- Corresponding property ($\sim 6/2^{16}$):



- Closed-form bound:

$$\|\pi_V(D-U)i_V\|_2 \leq \left(\frac{2}{\sqrt{q}-1}\right)^n$$

# Pairwise independence of the AES

## Spectral terms

- More analysis required:

$$V^{\perp} = W_1 \oplus W_2 \oplus \cdots \oplus W_n$$

If $w_1 \otimes \cdots \otimes w_n \in W_I$, then $w_i \perp \{\delta_0, \delta_{\mathbb{F}_q}\}$ for at least $I$ choices of $i$

- Key result for $I_1 + I_2 = I$:

$$\|\pi_{W_{I_1}}(D - U)\, i_{W_{I_2}}\|_2 \leq C \left(\frac{1}{\sqrt{q}-1}\right)^{n-I} \sigma^I$$

Strategy: bound $\|\pi_{W_{I_1}}(D^L - U)\, i_{W_{I_2}}\|_2$ using MDS properties
handle the S-box layers using $\|D^S - U\|_2 \leq \sigma$

# Pairwise independence of the AES

## Putting everything together

- One AES superbox:

$$\|D - U\|_2 \leq \left\| \begin{bmatrix} 2^{-13.098} & 2^{-11.178} \\ 2^{-11.178} & 2^{-10.845} \end{bmatrix} \right\|_2 \leq 2^{-10.268}$$

- Four AES rounds: $\|D - U\|_2 \leq 2^{-40}$

- Using maximum key-averaged probability of differentials (Keliher & Sui):

$$\|D - U\|_1 \leq 2^{128} \times (53 \cdot 2^{-34})^4 \times 2^{-40 \lfloor \frac{r-4}{4} \rfloor} \leq 2^{15} \times 2^{-40 \lfloor \frac{r-4}{4} \rfloor}$$

# Conclusions

- Pairwise independence from the point of view of cryptanalysis
  Ruling out translation-invariant 'pairwise methods' over $\mathbb{C}$ (Archimedean)
- Proof strategy
  Bounding the operator norm $\|D - U\|_2$ (no randomness needed)
- Pairwise independence of the AES
  20 rounds are enough for $\varepsilon \leq 2^{-128}$ (further improvements expected)