Revisiting Integral Distinguishers using Subspace Trails and Generalized Derivatives

Noureddine El-Asri, **Kirpa Garg**, and Valentin Suder

University of Rouen Normandy – LITIS

SAC 2026, Ottawa

Integral distinguishers

Definition (Daemen–Knudsen–Rijmen 1997; Knudsen–Wagner 2002)

Let $\mathcal{E} = \{\mathcal{E}_K : \mathbb{F}_p^n \to \mathbb{F}_p^n\}_{K \in \mathbb{F}_p^\kappa}$ be an ℓ-round iterated cipher and $X \subseteq \mathbb{F}_p^n$. If

$$\sum_{x \in X} \mathcal{E}_K(x) = c \qquad \text{with } c \text{ independent of the key } K,$$

then X is an *integral distinguisher* for $\mathcal{E}$. If $c = 0$: a *zero-sum* integral distinguisher.

Subspace trails: three definitions in the literature

Definition

$F : \mathbb{F}_p^n \to \mathbb{F}_p^n$, subspaces $U_0, \ldots, U_r$ with $\dim_{\mathbb{F}_p} U_i \leq \dim_{\mathbb{F}_p} U_{i+1}$: for each i and each $a_i \in \mathcal{A}_i$ there exists $a_{i+1} \in \mathcal{B}_{i+1}$ with

$$F(U_i + a_i) \subseteq U_{i+1} + a_{i+1}.$$

Subspace trails: three definitions in the literature

Definition

$F : \mathbb{F}_p^n \to \mathbb{F}_p^n$, subspaces $U_0, \ldots, U_r$ with $\dim_{\mathbb{F}_p} U_i \leq \dim_{\mathbb{F}_p} U_{i+1}$: for each i and each $a_i \in \mathcal{A}_i$ there exists $a_{i+1} \in \mathcal{B}_{i+1}$ with

$$F(U_i + a_i) \subseteq U_{i+1} + a_{i+1}.$$

	$\mathcal{A}_i$	$\mathcal{B}_{i+1}$	Reference
Orthogonal	$U_i^\perp$	$U_{i+1}^\perp$	Grassi–Rechberger–Rønjom 2016
Complete	$\mathbb{F}_p^n$	$\mathbb{F}_p^n$	Leander–Tezcan–Wiemer 2018
Complement	$\mathbb{F}_p^n$	$\mathbb{F}_p^n \setminus U_{i+1}$	Grassi–Rechberger–Schofnegger 2021

Subspace trails: three definitions in the literature

Definition

$F : \mathbb{F}_p^n \to \mathbb{F}_p^n$, subspaces $U_0, \ldots, U_r$ with $\dim_{\mathbb{F}_p} U_i \leq \dim_{\mathbb{F}_p} U_{i+1}$: for each i and each $a_i \in \mathcal{A}_i$ there exists $a_{i+1} \in \mathcal{B}_{i+1}$ with

$$F(U_i + a_i) \subseteq U_{i+1} + a_{i+1}.$$

	$\mathcal{A}_i$	$\mathcal{B}_{i+1}$	Reference
Orthogonal	$U_i^\perp$	$U_{i+1}^\perp$	Grassi–Rechberger–Rønjom 2016
Complete	$\mathbb{F}_p^n$	$\mathbb{F}_p^n$	Leander–Tezcan–Wiemer 2018
Complement	$\mathbb{F}_p^n$	$\mathbb{F}_p^n \setminus U_{i+1}$	Grassi–Rechberger–Schofnegger 2021

Often used interchangeably — but they are not equivalent!

Exact complete subspace trails

Our setting

A subspace trail is *exact* if all inclusions hold with equality. Our distinguisher uses exact complete trails:

$$U_0 \overset{F}{\Longrightarrow} \cdots \overset{F}{\Longrightarrow} U_r, \qquad F(U_i + a_i) = U_{i+1} + a_{i+1} \ \ \forall\, a_i \in \mathbb{F}_p^n.$$

Derivatives and higher-order derivatives

Derivative

For $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and a direction $\alpha \in \mathbb{F}_{p^n}$,

$$\Delta_\alpha F(x) := F(x + \alpha) - F(x).$$

Higher-order derivative (Lai 1994)

Along directions $\alpha_1, \ldots, \alpha_s \in \mathbb{F}_{p^n}$,

$$\Delta_{\alpha_1,\ldots,\alpha_s} F(x) := \Delta_{\alpha_1} \cdots \Delta_{\alpha_s} F(x).$$

Generalized derivatives

Generalized derivatives (Kuroda–Tsujie 2017; Özbudak–Sălăgean 2021)

For $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and $\alpha \in \mathbb{F}_{p^n}$,

$$\nabla_\alpha F(x) := \sum_{i \in \mathbb{F}_p} F(x + i\alpha)$$

Generalized derivatives

Generalized derivatives (Kuroda–Tsujie 2017; Özbudak–Sălăgean 2021)

For $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and $\alpha \in \mathbb{F}_{p^n}$,

$$\nabla_\alpha F(x) := \sum_{i \in \mathbb{F}_p} F(x + i\alpha) \;=\; \Delta_{\underbrace{\alpha,\ldots,\alpha}_{p-1}} F(x) \qquad (\text{for } p = 2\colon\ \nabla_\alpha = \Delta_\alpha).$$

Generalized derivatives

Generalized derivatives (Kuroda–Tsujie 2017; Özbudak–Sălăgean 2021)

For $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and $\alpha \in \mathbb{F}_{p^n}$,

$$\nabla_\alpha F(x) := \sum_{i \in \mathbb{F}_p} F(x + i\alpha) \;=\; \Delta_{\underbrace{\alpha,\ldots,\alpha}_{p-1}} F(x) \qquad (\text{for } p = 2\colon\ \nabla_\alpha = \Delta_\alpha).$$

Higher-order generalized derivative

Along $\mathbb{F}_p$-linearly independent $\alpha_1, \ldots, \alpha_s$, with $U = \langle \alpha_1, \ldots, \alpha_s \rangle_{\mathbb{F}_p}$,

$$\nabla_{\alpha_1,\ldots,\alpha_s} F(x) \;=\; \sum_{u \in U} F(x + u) \;=:\; \nabla_U F(x).$$

Generalized derivatives

Generalized derivatives (Kuroda–Tsujie 2017; Özbudak–Sălăgean 2021)

For $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and $\alpha \in \mathbb{F}_{p^n}$,

$$\nabla_\alpha F(x) := \sum_{i \in \mathbb{F}_p} F(x + i\alpha) \;=\; \Delta_{\underbrace{\alpha,\ldots,\alpha}_{p-1}} F(x) \qquad (\text{for } p = 2\text{:}\;\; \nabla_\alpha = \Delta_\alpha).$$

Higher-order generalized derivative

Along $\mathbb{F}_p$-linearly independent $\alpha_1, \ldots, \alpha_s$, with $U = \langle \alpha_1, \ldots, \alpha_s \rangle_{\mathbb{F}_p}$,

$$\nabla_{\alpha_1,\ldots,\alpha_s} F(x) \;=\; \sum_{u \in U} F(x + u) \;=:\; \nabla_U F(x).$$

$\nabla_U F \equiv 0$ makes every coset of U a zero-sum integral distinguisher.

Why generalized derivatives?

Let $s = \dim_{\mathbb{F}_p}(U)$. To compute $\nabla_U F(x)$:

Via higher-order derivatives

Unfold into $s(p-1)$ simple Δ's:

$2^{s(p-1)}$ evaluations of F.

Directly

Use $\nabla_U F(x) = \sum_{u \in U} F(x+u)$:

p^s evaluations of F.

Why generalized derivatives?

Let $s = \dim_{\mathbb{F}_p}(U)$. To compute $\nabla_U F(x)$:

Via higher-order derivatives

Unfold into $s(p-1)$ simple Δ's:

$2^{s(p-1)}$ evaluations of F.

Directly

Use $\nabla_U F(x) = \sum_{u \in U} F(x+u)$:

p^s evaluations of F.

p	s	Via higher-order	directly
3	2	$2^4 = 16$	$3^2 = 9$
5	2	$2^8 = 256$	$5^2 = 25$
7	3	$2^{18} \approx 2.6 \cdot 10^5$	$7^3 = 343$

Algebraic degree

Algebraic degree

For $F = (F_1, \ldots, F_n) : \mathbb{F}_p^n \to \mathbb{F}_p^n$, the algebraic degree is

$$\deg_p(F) := \max_{1 \le i \le n} \deg_p(F_i),$$

where $\deg_p(F_i)$ is the (total) degree of F_i as a reduced multivariate polynomial in $\dfrac{\mathbb{F}_p[x_1, \ldots, x_n]}{\langle x_1^p - x_1, \ldots, x_n^p - x_n \rangle}$.

Algebraic degree

Algebraic degree

For $F = (F_1, \ldots, F_n) : \mathbb{F}_p^n \to \mathbb{F}_p^n$, the algebraic degree is

$$\deg_p(F) := \max_{1 \le i \le n} \deg_p(F_i),$$

where $\deg_p(F_i)$ is the (total) degree of F_i as a reduced multivariate polynomial in $\dfrac{\mathbb{F}_p[x_1, \ldots, x_n]}{\langle x_1^p - x_1, \ldots, x_n^p - x_n \rangle}$.

Degree bound

$$\deg_p(\nabla_U F) \;\le\; \deg_p(F) - \dim_{\mathbb{F}_p}(U)\,(p-1)$$

Main observation

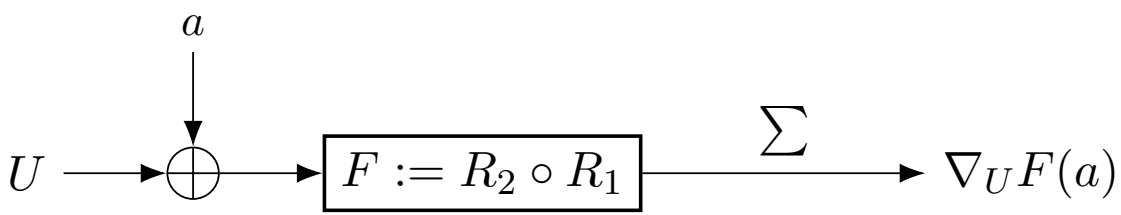
Let $F = R_2 \circ R_1$ with $R_1, R_2 : \mathbb{F}_p^n \to \mathbb{F}_p^n$, and let U, V be subspace of $\mathbb{F}_p^n$ such that $U \overset{R_1}{\Longrightarrow} V$ is an exact complete subspace trail. Then

$$\forall\, a \in \mathbb{F}_p^n \;\; \exists\, b_a \in \mathbb{F}_p^n : \qquad \nabla_U F(a) \;=\; \nabla_V R_2(b_a).$$

Main observation

Let $F = R_2 \circ R_1$ with $R_1, R_2 : \mathbb{F}_p^n \to \mathbb{F}_p^n$, and let U, V be subspace of $\mathbb{F}_p^n$ such that $U \overset{R_1}{\Longrightarrow} V$ is an exact complete subspace trail. Then

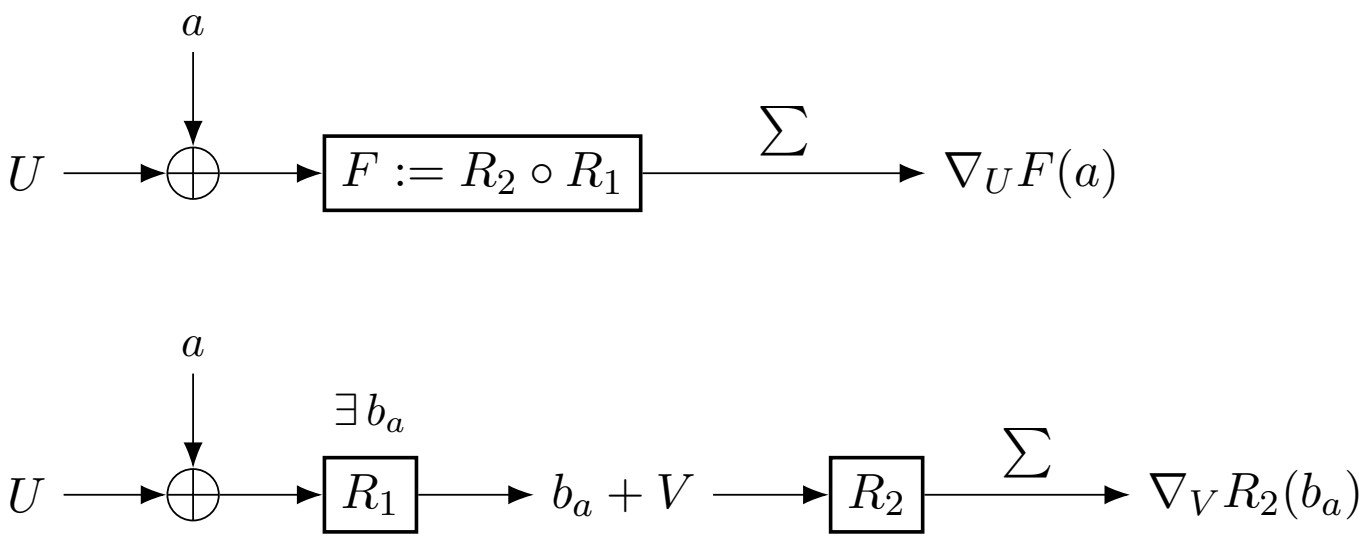
$$\forall\, a \in \mathbb{F}_p^n \;\; \exists\, b_a \in \mathbb{F}_p^n : \qquad \nabla_U F(a) \;=\; \nabla_V R_2(b_a).$$



Main observation

Let $F = R_2 \circ R_1$ with $R_1, R_2 : \mathbb{F}_p^n \to \mathbb{F}_p^n$, and let U, V be subspace of $\mathbb{F}_p^n$ such that $U \overset{R_1}{\Longrightarrow} V$ is an exact complete subspace trail. Then

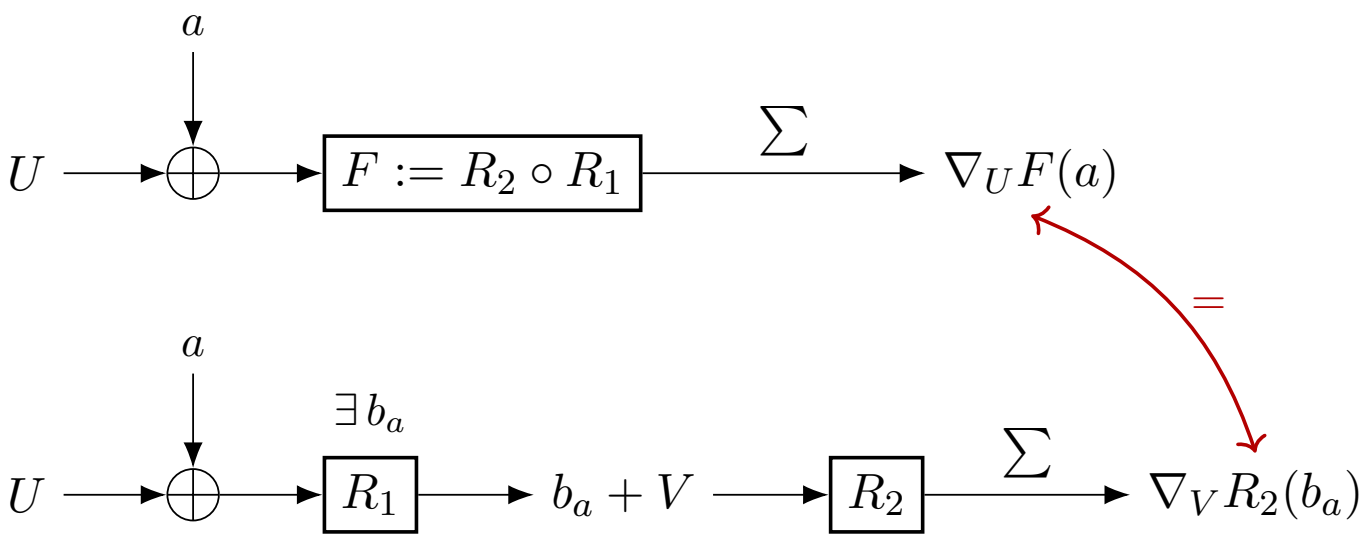
$$\forall\, a \in \mathbb{F}_p^n \;\; \exists\, b_a \in \mathbb{F}_p^n : \qquad \nabla_U F(a) \;=\; \nabla_V R_2(b_a).$$



Main observation

Let $F = R_2 \circ R_1$ with $R_1, R_2 : \mathbb{F}_p^n \to \mathbb{F}_p^n$, and let U, V be subspace of $\mathbb{F}_p^n$ such that $U \overset{R_1}{\Longrightarrow} V$ is an exact complete subspace trail. Then

$$\forall\, a \in \mathbb{F}_p^n \;\; \exists\, b_a \in \mathbb{F}_p^n : \qquad \nabla_U F(a) \;=\; \nabla_V R_2(b_a).$$



Zero-sum integral distinguisher ($\mathcal{R}_k(x) = \mathcal{R}(x+k)$)

Theorem (Asri-G.-Suder)

Let $\mathcal{E}_K = \mathcal{R}_{k_\ell} \circ \cdots \circ \mathcal{R}_{k_1}$ be an ℓ-round cipher on $\mathbb{F}_p^n$, for any round keys $k_1, \ldots, k_\ell$. Suppose

- an exact complete trail through the first m rounds, with all $\dim_{\mathbb{F}_p} U_i = s$:

$$U_0 \xrightarrow{\mathcal{R}_{k_1}} U_1 \xrightarrow{\mathcal{R}_{k_2}} \cdots \xrightarrow{\mathcal{R}_{k_m}} U_m,$$

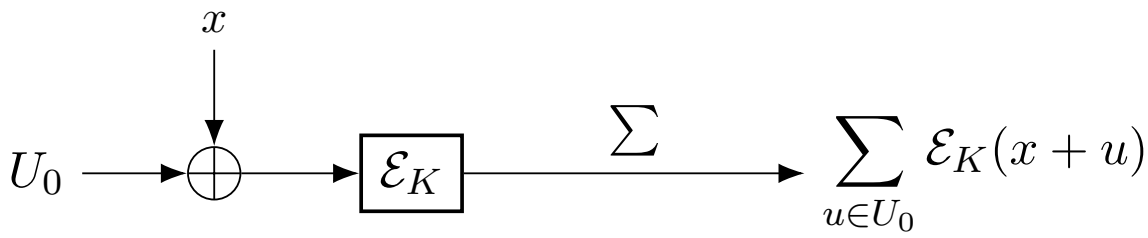
- the remaining $\ell - m$ rounds have algebraic degree:

$$\deg_p \left(\mathcal{R}_{k_\ell} \circ \cdots \circ \mathcal{R}_{k_{m+1}} \right) < s\,(p-1).$$

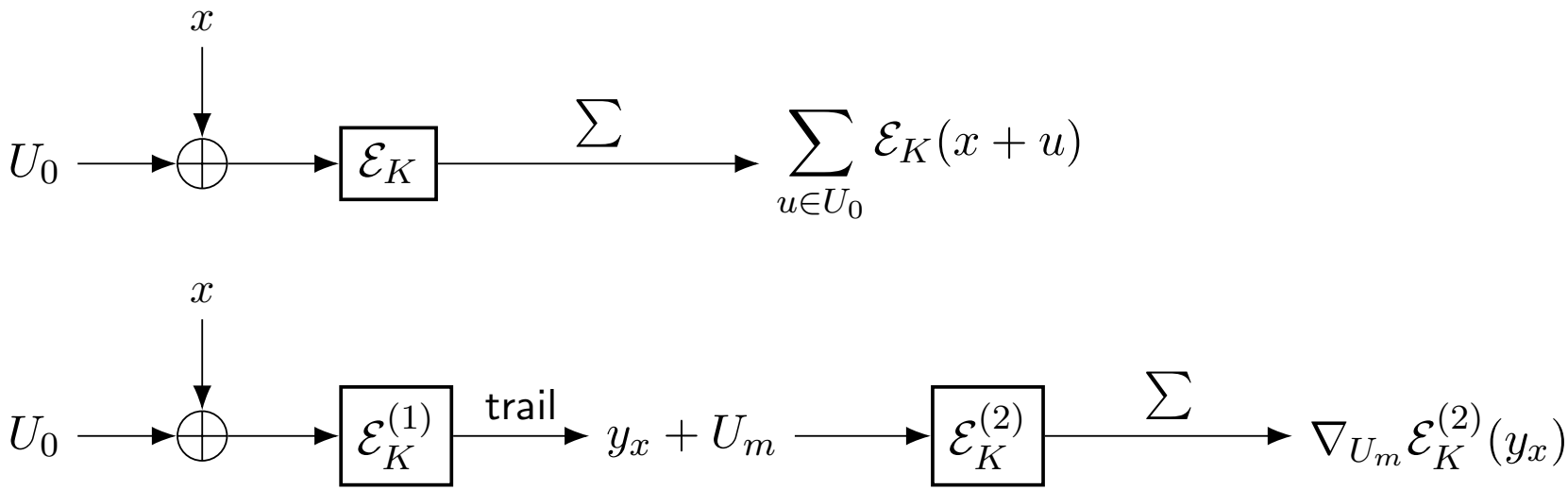
Then for *every* $x \in \mathbb{F}_p^n$,

$$\sum_{u \in U_0} \mathcal{E}_K(x+u) = 0.$$

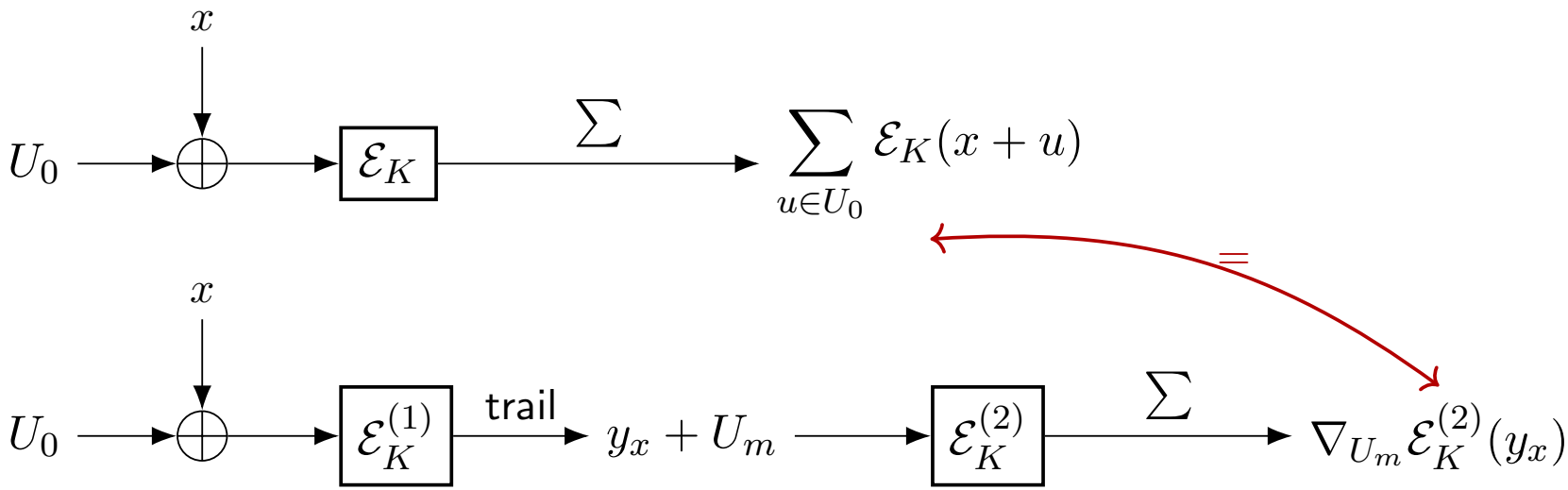
Idea of the proof



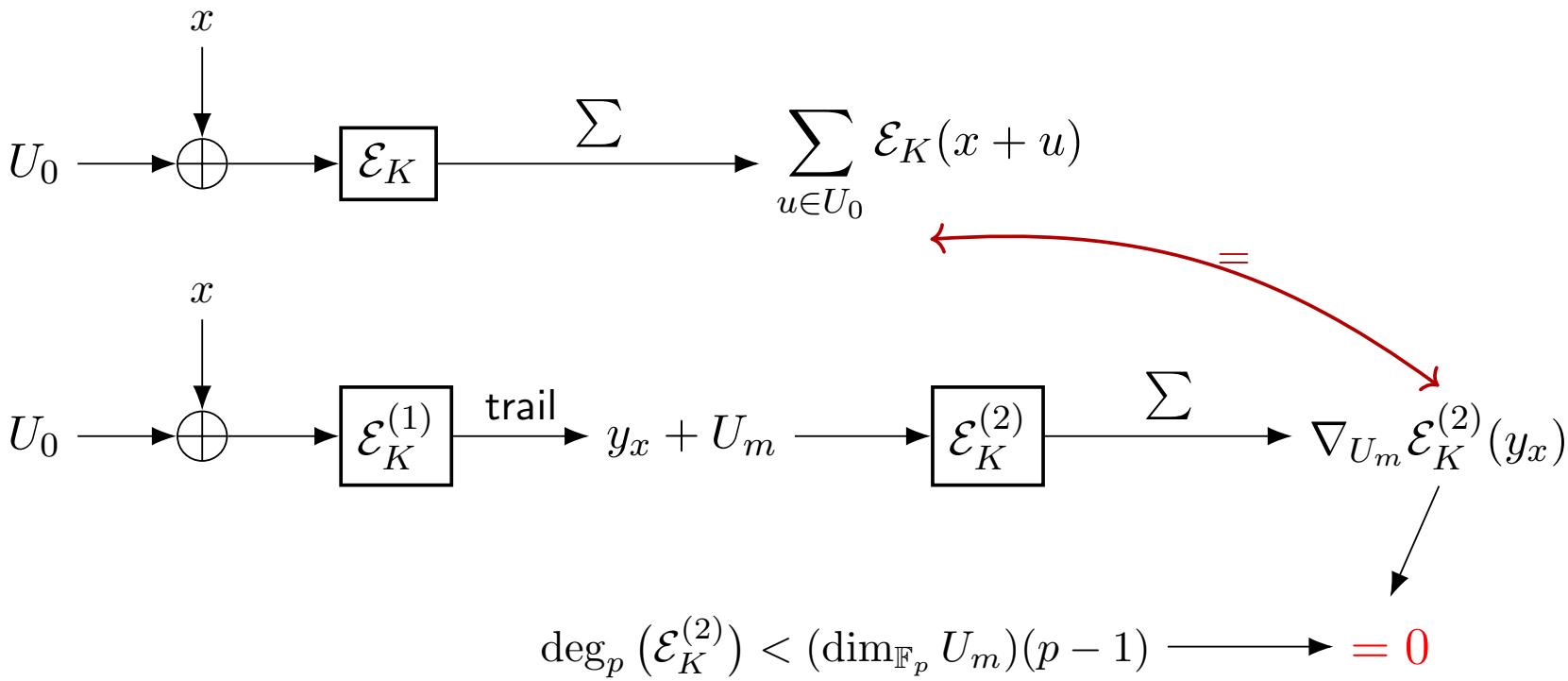
Idea of the proof



Idea of the proof



Idea of the proof



A lower bound on the number of rounds

Result (Asri-G.-Suder)

The tail has $\ell - m$ rounds, so $\deg_p\left(\mathcal{E}_K^{(2)}\right) \leq d^{\ell-m}$ with $d := \deg_p(\mathcal{R})$.

$$d^{\ell-m} < s\,(p-1) \quad \Longleftrightarrow \quad \ell \leq m + \log_d\left(s\,(p-1)\right).$$

A lower bound on the number of rounds

Result (Asri-G.-Suder)

The tail has $\ell - m$ rounds, so $\deg_p\left(\mathcal{E}_K^{(2)}\right) \leq d^{\ell-m}$ with $d := \deg_p(\mathcal{R})$.

$$d^{\ell-m} < s\,(p-1) \quad \Longleftrightarrow \quad \ell \leq m + \log_d\left(s\,(p-1)\right).$$

Example

$p = 2^{31} - 1, \quad d = 5, \quad s = 12, \quad m = 2$

$$\Longrightarrow \quad \ell \leq 2 + \log_5\big(12(p-1)\big) \approx 16.9 \qquad \Rightarrow \qquad \ell \leq 16 \text{ rounds.}$$

Application: AES-like SPN ciphers

Cipher	$\deg_2(\mathcal{R})$	Rounds ℓ	m	$\ell - m$	$\deg_2((\ell-m)$-rounds)	Data
AES	7	4	2	2	≤ 49	2^{64}
Midori-64	3	5	2	3	≤ 27	2^{32}
Klein-64	3	5	2	3	≤ 27	2^{32}
Skinny-64	3	5	2	3	≤ 27	2^{32}
Skinny-64	3	7	2	5	≤ 47	2^{48}

Key-independent zero-sum integral distinguisher

AES (Daemen–Knudsen–Rijmen, 1997); KLEIN-64 (Yu-Wu-Li-Zhang, 2012); Midori-64, Skinny-64 (Derbez–Fouque, 2020).

Application: AES-prime

AES-like SPN over $\mathbb{F}_p$, $p = 2^7 - 1$: state $\in \mathbb{F}_p^{4\times 4}$, $\deg_p(\mathcal{R}) = 5$.

Application: AES-prime

AES-like SPN over $\mathbb{F}_p$, $p = 2^7 - 1$: state $\in \mathbb{F}_p^{4\times 4}$, $\deg_p(\mathcal{R}) = 5$.

	Rounds ℓ	Data	Keys
Known results Beyne–Verbauwhede 2025	1–4	p	all
	5	p^4	all
	6	p^8	all

Key-independent zero-sum integral distinguisher

Extending the subspace trail

Germs of a subspace (Asri-G.-Suder)

$$\Gamma_F(U) = \{\, a \in \mathbb{F}_p^n : F(a+U) \text{ is an } \mathbb{F}_p\text{-affine subspace} \,\}.$$

$\Gamma_F(U)$ either empty, or of size $\geq |U|$.

Why: a trail needs *every* coset to map to a coset; a germ asks only that one coset does — enough to buy one more round.

One more round

Setting

$\mathcal{E}_K = \mathcal{R}_{k_\ell} \circ \cdots \circ \mathcal{R}_{k_1}$ be an ℓ-round cipher on $\mathbb{F}_q^n$, and $\mathcal{R}_k(x) := \mathcal{R}(x + k)$ for any round keys $k_1, \ldots, k_\ell$.

One more round

Setting

$\mathcal{E}_K = \mathcal{R}_{k_\ell} \circ \cdots \circ \mathcal{R}_{k_1}$ be an ℓ-round cipher on $\mathbb{F}_q^n$, and $\mathcal{R}_k(x) := \mathcal{R}(x+k)$ for any round keys $k_1, \ldots, k_\ell$.

Theorem (Asri-G.-Suder)

Suppose

- exact complete trail $U_0 \overset{\mathcal{R}}{\Longrightarrow} U_1 \overset{\mathcal{R}}{\Longrightarrow} \cdots \overset{\mathcal{R}}{\Longrightarrow} U_m$, all $\dim_{\mathbb{F}_p} U_i = s$;
- $\Gamma_{\mathcal{R}}(U_m) \neq \emptyset$;
- $\deg_p\left(\mathcal{R}^{\ell-m-1}\right) < s\,(p-1)$.

Then for every $x \in \mathbb{F}_p^n$ there are $|\Gamma_{\mathcal{R}}(U_m)|$ keys K with

$$\sum_{u \in U_0} \mathcal{E}_K(x+u) = 0.$$

Application: AES-prime

	Rounds ℓ	Data	Keys
Known Beyne–Verbauwhede 2025	1–4	p	all
	5	p^4	all
	6	p^8	all
Ours one more round	1–5	p	$\geq p^{13}$
	6	p^4	$\geq N_I$

$\mathcal{M}_I = \mathrm{MC}(\mathcal{D}_I)$ is the mixed space of dimension $4|I|$, for $I \subseteq \{0,1,2,3\}$, and

$$N_I = \left|\{k \in \mathbb{F}_p^{4\times 4} \,:\, \mathcal{R}(\mathcal{R}(k)+k)+k \in \mathcal{M}_I\}\right|.$$

Conclusion

- One framework: exact subspace trails + higher-order generalized derivatives give integral distinguishers.
- Known distinguishers explained.
- One more round on AES-prime, in a weak-key setting.
- Also yields a lower bound on the number of rounds needed for security.

Conclusion

- One framework: exact subspace trails + higher-order generalized derivatives give integral distinguishers.
- Known distinguishers explained.
- One more round on AES-prime, in a weak-key setting.
- Also yields a lower bound on the number of rounds needed for security.

Future directions

- Extend to arbitrary subspace trails, not only exact complete ones.
- Develop tools to analyse block ciphers through properties of higher-order generalized derivatives.
- Apply these techniques to key-recovery attacks.
- Extend beyond AES-like SPNs — Feistel ciphers.

References

- T. Beyne, A. Canteaut, I. Dinur, M. Eichlseder, G., Leander, G. Leurent, M. Naya-Plasencia, Y. Sasaki, Y. Todo, F. Wiemer, *Out of oddity– new cryptanalytic techniques against symmetric primitives optimized for integrity proof systems.* In: Advances in Cryptology – CRYPTO 2020 – 40th Annual International Cryptology Conference, Proceedings. Lecture Notes in Computer Science, vol. 12172, pp. 299–328. Springer (2020).
- T. Beyne, M., Verbauwhede, *Integral cryptanalysis in characteristic p.* In: Hanaoka, G., Yang, B.Y. (eds.) Advances in Cryptology – ASIACRYPT 2025. LNCS, vol. 16245, pp. 66–96. Springer Nature Singapore (2026).
- J. Daemen, L. R. Knudsen, V. Rijmen. *The Block Cipher Square*. FSE 1997, LNCS 1267, pp. 149–165.
- P. Derbez, P.-A. Fouque. *Increasing Precision of Division Property*. IACR Trans. Symmetric Cryptol. 2020.
- L. Grassi, C. Rechberger, S. Rønjom. *Subspace Trail Cryptanalysis and its Applications to AES*. IACR Trans. Symmetric Cryptol. 2016(2), pp. 192–225.
- L. Grassi, C. Rechberger, M. Schofnegger. *Proving Resistance Against Infinitely Long Subspace Trails: How to Choose the Linear Layer*. IACR Trans. Symmetric Cryptol. 2021(2), pp. 314–352.

References

- P. Hebborn, B. Lambin, G. Leander, Y. Todo. *Lower Bounds on the Degree of Block Ciphers*. ASIACRYPT 2020, pp. 537–566.
- L. R. Knudsen, D. Wagner. *Integral Cryptanalysis*. FSE 2002, LNCS 2365, pp. 112–127.
- M. Kuroda, S. Tsujie. *A Generalization of APN Functions for Odd Characteristic*. Finite Fields Appl. 47 (2017), pp. 46–59.
- X. Lai. *Higher Order Derivatives and Differential Cryptanalysis*. Communications and Cryptography, Kluwer, 1994, pp. 227–233.
- G. Leander, C. Tezcan, F. Wiemer. *Searching for Subspace Trails and Truncated Differentials*. IACR Trans. Symmetric Cryptol. 2018(1), pp. 74–100.
- F. Özbudak, A. Sălăgean. *New Generalized Almost Perfect Nonlinear Functions*. Finite Fields Appl. 70 (2021).
- X. Yu, W. Wu, Y. Li, L. Zhang. *Cryptanalysis of Reduced-Round KLEIN Block Cipher*. Inscrypt 2011, LNCS 7537, pp. 237–250.

Thank you!