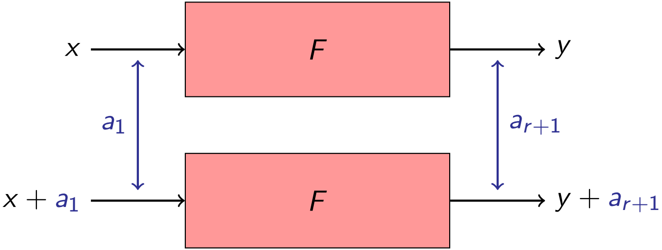
On the validity of differential distinguishers: extensions of the quasidifferential framework

Baptiste Germon

Univ Rennes, Inria, CNRS, IRISA

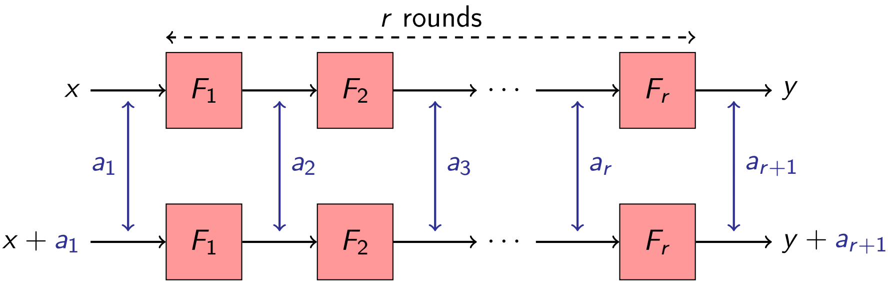
Differential Cryptanalysis

- Introduced by Biham and Shamir in 1990 [BS91].



Distinguisher: differential (a_1, a_{r+1}) such that $\Pr[a_1 \to a_{r+1}] \gg \frac{1}{2^n}$.

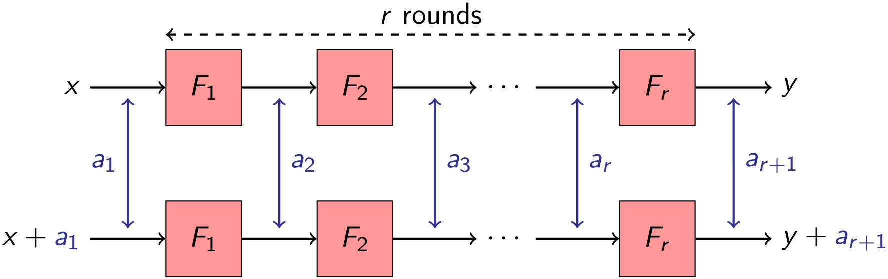
Differential Characteristics



Distinguisher probability estimation: characteristic $(a_1, a_2, \ldots, a_{r+1})$ such that

$$\Pr[a_1 \to a_{r+1}] \geq \Pr[a_1 \to a_2 \to \cdots \to a_{r+1}] \gg \frac{1}{2^n}.$$

Differential Characteristics



Distinguisher probability estimation: characteristic $(a_1, a_2, \ldots, a_{r+1})$ such that the fixed-key probability satisfies $\Pr[a_1 \rightarrow a_2 \rightarrow \cdots \rightarrow a_{r+1} | K = k] \gg \frac{1}{2^n}$ for any given key.

Classical Assumptions

Stochastic Equivalence Hypothesis

$$\Pr[a_1 \to a_2 \to \cdots \to a_{r+1} | K = k^*] \approx \underbrace{\frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} \Pr[a_1 \to a_2 \to \cdots \to a_{r+1} | K = k]}_{\text{Expected Differential Probability}} \quad \forall k^* \in \mathcal{K}$$

Round Independence

$$\mathrm{EDP}[a_1, \ldots, a_{r+1}] \approx \prod_{i=1}^{r} \Pr[a_i \to a_{i+1}]$$

Reasonable Hypotheses?

- Deviation of the fixed-key probability already observed by Knudsen in 1992 [Knu93].
- Most of AES characteristics are plateau characteristics (up to 4 rounds) [DR07].
- Only **1 out of 43** published characteristics on SKINNY is valid for more than 50% of the keys [PT22].

[BR22]'s quasidifferential framework:

$$p_k = \prod_{i=1}^{r} \left(\frac{1120}{64^3} - (-1)^{k_{2i,12}+k_{2i,14}} \frac{672}{64^3} \right)$$

They provide a general framework to evaluate the fixed-key probability.

Quasidifferential Framework

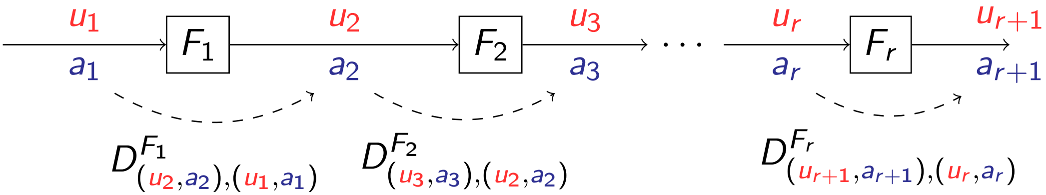
$$
\begin{tikzcd}
{} \arrow[r, "u_1", "a_1"'] & \boxed{F_1} \arrow[r, "u_2", "a_2"'] & \boxed{F_2} \arrow[r, "u_3", "a_3"'] & \cdots \arrow[r, "u_r", "a_r"'] & \boxed{F_r} \arrow[r, "u_{r+1}", "a_{r+1}"'] & {}
\end{tikzcd}
$$

$$
D^{F_1}_{(u_2,a_2),(u_1,a_1)} \qquad D^{F_2}_{(u_3,a_3),(u_2,a_2)} \qquad D^{F_r}_{(u_{r+1},a_{r+1}),(u_r,a_r)}
$$

where

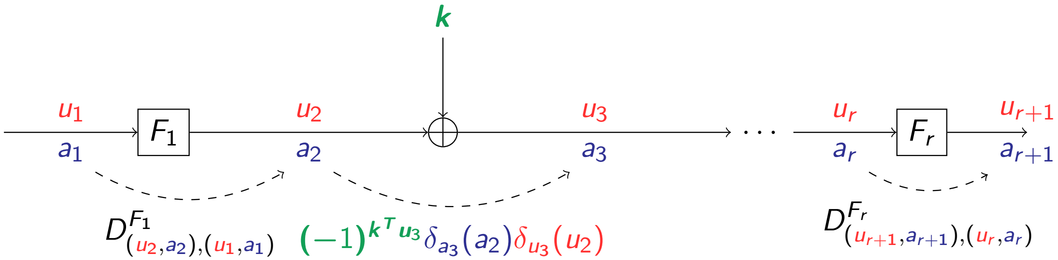
$$
\begin{aligned}
D^{F_i}_{(u_{i+1},a_{i+1}),(u_i,a_i)} = & \left(2 \Pr[u_{i+1}^{\mathsf{T}} F_i(\boldsymbol{x}) \oplus u_i^{\mathsf{T}} \boldsymbol{x} = 0 | F_i(\boldsymbol{x} \oplus a_i) \oplus F_i(\boldsymbol{x}) = a_{i+1}] - 1\right) \\
& \times \Pr[F_i(\boldsymbol{x} \oplus a_i) \oplus F_i(\boldsymbol{x}) = a_{i+1}]
\end{aligned}
$$

Quasidifferential Framework



$$\mathrm{Corr}\Big((u_1, a_1), \ldots, (u_{r+1}, a_{r+1})\Big) = \prod_{i=1}^{r} D^{F_i}_{(u_{i+1},a_{i+1}),(u_i,a_i)}$$

Quasidifferential Framework - Key Addition



$$\mathrm{Corr} = D^{F_1}_{(u_2,a_2),(u_1,a_1)} \times (-1)^{k^T u_3}\delta_{a_3}(a_2)\delta_{u_3}(u_2) \times \cdots \times D^{F_r}_{(u_{r+1},a_{r+1}),(u_r,a_r)}$$

Fixed-key Probability As Sum Of Correlations

Theorem 4.1 [BR22]

$$\Pr\left[\bigwedge_{i=1}^{r} F_i(\boldsymbol{x}_i \oplus a_i) \oplus F_i(\boldsymbol{x}_i) = a_{i+1}\right] = \sum_{u_2,\ldots,u_r} \prod_{i=1}^{r} D^{F_i}_{(u_{i+1},a_{i+1}),(u_i,a_i)}$$

with $u_1 = u_{r+1} = 0$, $\boldsymbol{x}_i = F_{i-1}(\boldsymbol{x}_{i-1})$, $\boldsymbol{x}_1$ uniform.

No assumptions needed!

Our Contributions (published in ToSC[1])

Related-key setting

The original framework applies the same function on both elements of the pairs. Not compatible with the related-key setting.

We extend the original framework to treat pairs asymmetrically.

[1] [BDG25] Boura, Derbez, Germon *Extending the Quasidifferential Framework: From Fixed-Key to Expected Differential Probability.* ToSC 2025

Our Contributions (published in ToSC[1])

Related-key setting

The original framework applies the same function on both elements of the pairs. Not compatible with the related-key setting.

We extend the original framework to treat pairs asymmetrically.

Analysing clusters of differential characteristics

- Exhausting all quasidifferential trails for a characteristic can be hard or infeasible.
- Analysing cluster leads to complex formulas which can be heavy to manipulate.

- Extend [BR22] framework to obtain an **exact formula for the EDP**.
- Takes the key-schedule into account for the first time!

[1] [BDG25] Boura, Derbez, Germon *Extending the Quasidifferential Framework: From Fixed-Key to Expected Differential Probability.* ToSC 2025

Applications: AES and SKINNY

Developed a practical MILP implementation to search for quasidifferential trails.

AES: EDP matches the heuristical estimation.

Version	Rounds	Estimated proba.	EDP	Source
AES-128	2	2^{-7}	2^{-7}	[FJP13]
AES-128	4	2^{-81}	2^{-81}	[FJP13]
AES-128	4	2^{-81}	2^{-81}	[FJP13]
AES-128	5	2^{-105}	2^{-105}	[FJP13]
AES-256	14	2^{-154}	2^{-154}	[GLMS18]
AES-256	14	2^{-146}	2^{-146}	[GLMS18]
AES-192	9	2^{-146}	2^{-146}	[GLMS18]

[1] [FJP13] Fouque et al. *Structural Evaluation of AES and Chosen-Key Distinguisher of 9-round AES-128.* CRYPTO 2013

[2] [GLMS18] Gérault et al. *Revisiting AES Related-Key Differential Attacks with Constraint Programming.* Inf. Process. Lett. 2018

Applications: AES and SKINNY

SKINNY: More precise results than Peyrin and Tan on SKINNY-64 in fixed-key model.
More accurate estimation of EDP.

SKINNY	Estimated prob.	EDP	[PT22] Key Space	[PT22] Prob. Range
64-64	2^{-52} 2^{-46}	2^{-52} (1) 0 (8)	2^{-6} 0	2^{-46} —
64-128	2^{-55} 2^{-44}	2^{-55} (1) 2^{-44} (4)	2^{-4} Not given	2^{-51} 2^{-39} – $2^{-35.415}$
64-192	2^{-54}	2^{-54} (1)	$2^{-6.19}$	2^{-48} – 2^{-47}
128-128	2^{-123} 2^{-120}	0 (16) $2^{-119.05}$ **(44)**	0 $2^{-7.66}$	— $2^{-122.39}$ – $2^{-106.88}$ (E)
128-256	$2^{-127.66}$	$2^{-126.41}$ **(26)**	$2^{-6.11}$	$2^{-133.80}$ – $2^{-112.15}$(E)

Applications: AES and SKINNY

SKINNY: Analysed a cluster of 114 688 characteristics with EDP computation:
More than a half of the characteristics are invalid.
Improved Diff-MitM attack on SKINNY-128-384 by a factor $2^{2.9}$.

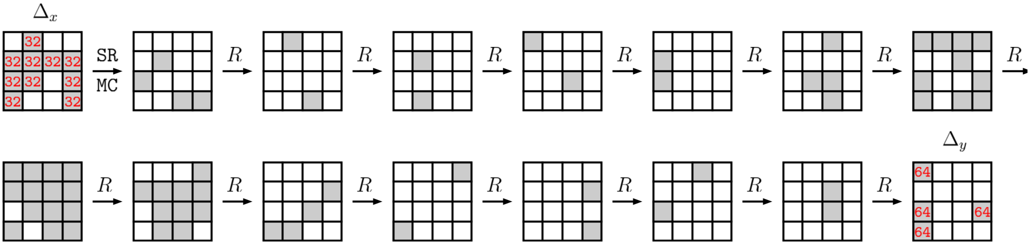


Figure: Truncated differential trail of the attack on 25-round SKINNY-128-384 [BDD+23]

[1] [BDD+23] Boura et al. *Differential meet-in-the-middle cryptanalysis.* CRYPTO 2023

Summary & Future work

- Extend the quasidifferential framework to the related-key setting.
- Provide for the **first time** a formula for the EDP that takes the key-schedule into account.
- Practical MILP model.
- New results on `AES` and `SKINNY`.

Summary & Future work

- Extend the quasidifferential framework to the related-key setting.
- Provide for the **first time** a formula for the EDP that takes the key-schedule into account.
- Practical MILP model.
- New results on `AES` and `SKINNY`.

Future work

- Extend the framework to other types of differential-based distinguishers.
- Improve the modeling of the framework.
- Use the EDP computation to design a robust key-schedule.

Summary & Future work

Future work

- Extend the framework to other types of differential-based distinguishers.
- Improve the modeling of the framework.
- Use the EDP computation to design a robust key-schedule.

Thanks for your attention!

Christina Boura, Nicolas David, Patrick Derbez, Gregor Leander, and María Naya-Plasencia.
Differential meet-in-the-middle cryptanalysis.
In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part III*, volume 14083 of *LNCS*, pages 240–272. Springer, Cham, August 2023.

Tim Beyne and Vincent Rijmen.
Differential cryptanalysis in the fixed-key model.
In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part III*, volume 13509 of *LNCS*, pages 687–716. Springer, Cham, August 2022.

Eli Biham and Adi Shamir.
Differential cryptanalysis of DES-like cryptosystems.
In Alfred J. Menezes and Scott A. Vanstone, editors, *CRYPTO'90*, volume 537 of *LNCS*, pages 2–21. Springer, Berlin, Heidelberg, August 1991.

Joan Daemen and Vincent Rijmen.
Plateau characteristics.
IET Inf. Secur., 1(1):11–17, 2007.

Pierre-Alain Fouque, Jérémy Jean, and Thomas Peyrin.
Structural evaluation of AES and chosen-key distinguisher of 9-round AES-128.
In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 183–203. Springer, Berlin, Heidelberg, August 2013.

David Gérault, Pascal Lafourcade, Marine Minier, and Christine Solnon.
Revisiting AES related-key differential attacks with constraint programming.
Inf. Process. Lett., 139:24–29, 2018.

Lars R. Knudsen.
Iterative characteristics of DES and s^2-DES.
In Ernest F. Brickell, editor, *CRYPTO'92*, volume 740 of *LNCS*, pages 497–511. Springer, Berlin, Heidelberg, August 1993.

Thomas Peyrin and Quan Quan Tan.
Mind your path: On (key) dependencies in differential characteristics.
IACR Trans. Symm. Cryptol., 2022(4):179–207, 2022.