New perspectives in Differential Cryptanalysis of SPN's

Merlin Fruchon [1,2], Anne Canteaut[1]

[1]Inria, France, [2]DGA, France

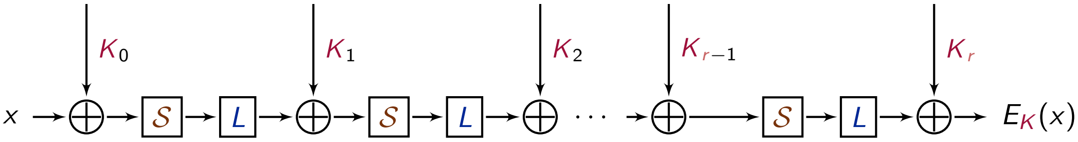
01/04/2025

Outline

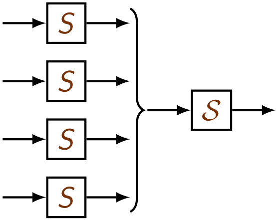
Plan of this Section

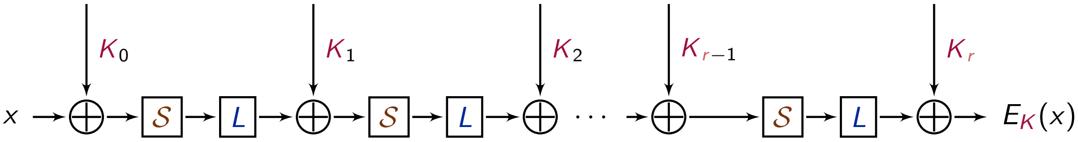
Plan of this Section

Substitution Permutation Networks

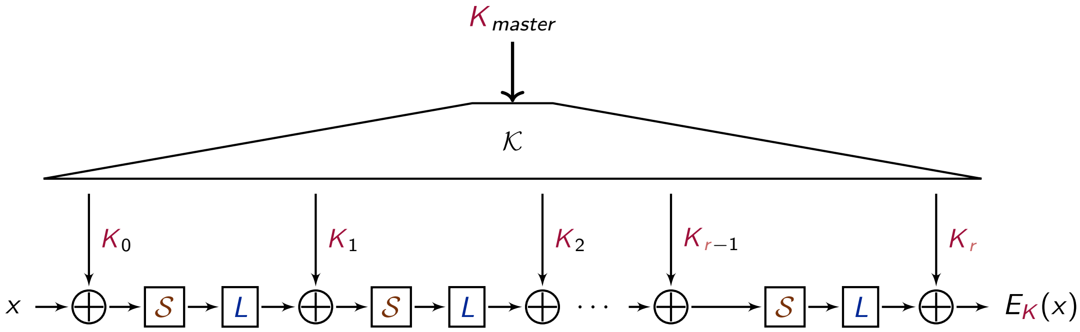


Substitution Permutation Networks





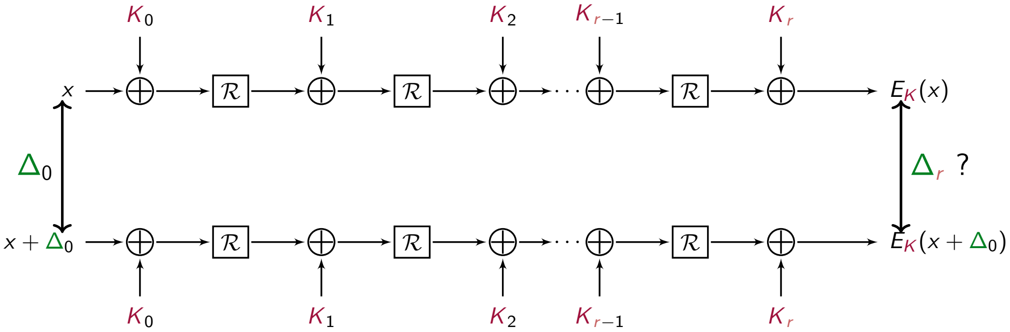
Substitution Permutation Networks



Plan of this Section

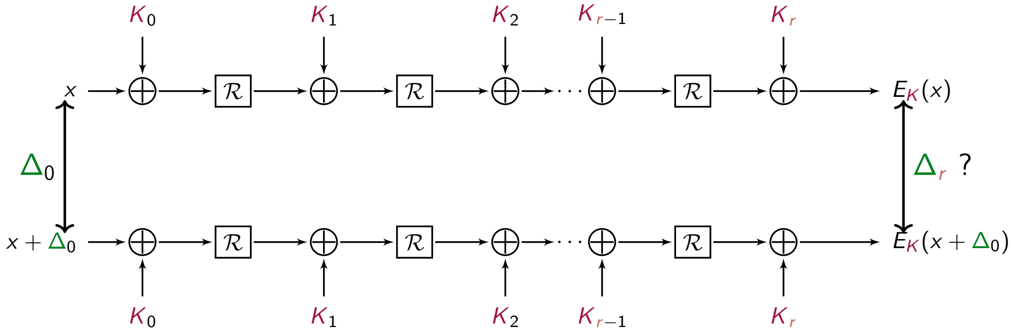
Differentials [BS91]

$\mathcal{R} = L \circ \mathcal{S}$



Differentials [BS91]

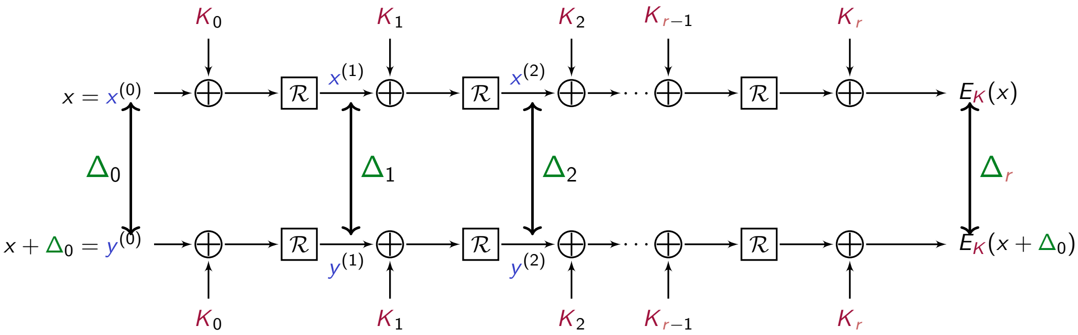
$\mathcal{R} = L \circ \mathcal{S}$



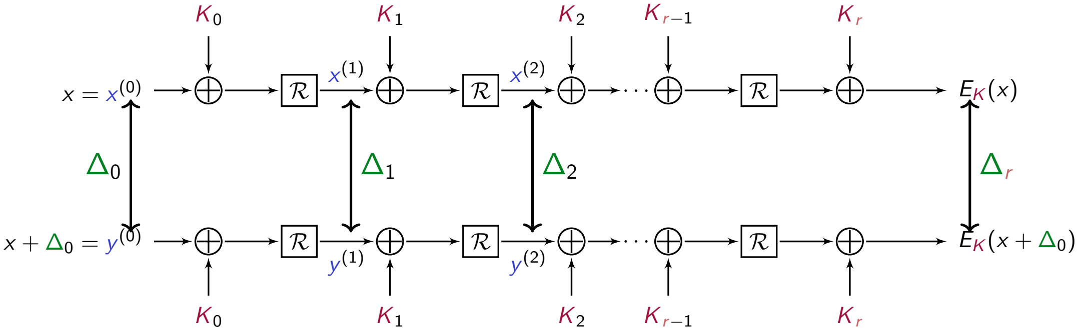
Probability of a differential

$$\mathbb{P}(K, \Delta_0, \Delta_r) := \frac{\#\{x \in \mathbb{F}_2^n \mid E_K(x + \Delta_0) + E_K(x) = \Delta_r\}}{2^n}$$

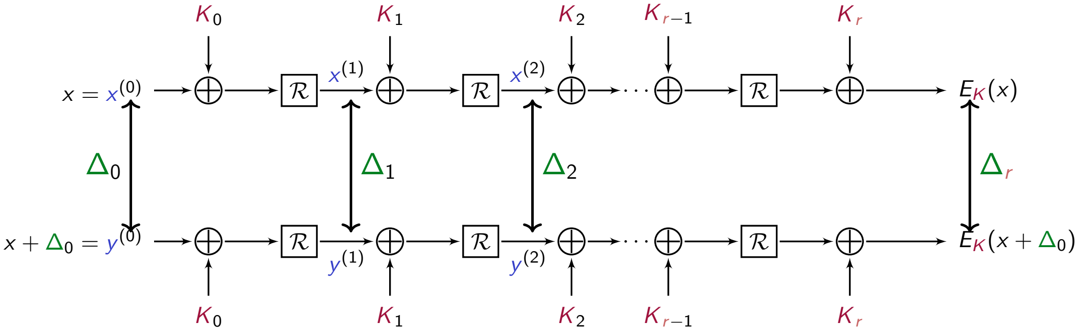
Differential characteristics



Differential characteristics



Differential characteristics



Probability of a differential characteristic

$$\mathbb{P}(K, \Delta_{0\leq j\leq r}) := \frac{\#\{x \in \mathbb{F}_2^n \mid \forall j \in [\![0, r]\!], x^{(j)} + y^{(j)} = \Delta_j\}}{2^n}$$

Plan of this Section

Plan of this Section

Usual assumptions [LMM91]

Expected Differential Probability

$$EDP(\Delta_0, \Delta_r) := \frac{1}{2^n} \sum_{K \in \mathbb{F}_2^n} \mathbb{P}(K, \Delta_0, \Delta_r)$$

Usual assumptions [LMM91]

Expected Differential Probability

$$EDP(\Delta_0, \Delta_r) := \frac{1}{2^n} \sum_{K \in \mathbb{F}_2^n} \mathbb{P}(K, \Delta_0, \Delta_r)$$

1. Stochastic equivalence : $\forall K, \mathbb{P}(K, \Delta_0, \Delta_r) \approx EDP(\Delta_0, \Delta_r)$

Usual assumptions [LMM91]

Expected Differential Probability

$$EDP(\Delta_0, \Delta_r) := \frac{1}{2^n} \sum_{K \in \mathbb{F}_2^n} \mathbb{P}(K, \Delta_0, \Delta_r)$$

1. Stochastic equivalence : $\forall K, \mathbb{P}(K, \Delta_0, \Delta_r) \approx EDP(\Delta_0, \Delta_r)$
2. Round keys are independent and uniformly distributed

Usual assumptions [LMM91]

Expected Differential Probability

$$EDP(\Delta_0, \Delta_r) := \frac{1}{2^n} \sum_{K \in \mathbb{F}_2^n} \mathbb{P}(K, \Delta_0, \Delta_r)$$

1. Stochastic equivalence : $\forall K, \mathbb{P}(K, \Delta_0, \Delta_r) \approx EDP(\Delta_0, \Delta_r)$
2. Round keys are independent and uniformly distributed
3. Dominant trail: the probability of the differential is close to the probability of the most probable characteristic.

Validity of these assumptions

- For the DES, $EDP = 2^{-47.22}$ but equal to $2^{-43.16}$ for some keys and $2^{-55.16}$ for other keys [Knu93].

Validity of these assumptions

- For the DES, $EDP = 2^{-47.22}$ but equal to $2^{-43.16}$ for some keys and $2^{-55.16}$ for other keys [Knu93].
- Good approximation when the key-schedule is complex.

Validity of these assumptions

- For the DES, $EDP = 2^{-47.22}$ but equal to $2^{-43.16}$ for some keys and $2^{-55.16}$ for other keys [Knu93].
- Good approximation when the key-schedule is complex.

Validity for lightweight designs

In $\textsc{Midori64}$, for some weak keys there are characteristics of probability $> 2^{-32}$ for any number of rounds.

Plan of this Section

A framework to study fixed-key behavior [BR22]

Quasi-differential framework

- Analyzes the fixed-key behavior of differential characteristics.

A framework to study fixed-key behavior [BR22]

Quasi-differential framework

- Analyzes the fixed-key behavior of differential characteristics.
- Stochastic equivalence and independence of the keys are not needed.

A framework to study fixed-key behavior [BR22]

Quasi-differential framework

- Analyzes the fixed-key behavior of differential characteristics.
- Stochastic equivalence and independence of the keys are not needed.
- Lots of characteristics found using the usual assumptions are in fact invalid.

A framework to study fixed-key behavior [BR22]

Quasi-differential framework

- Analyzes the fixed-key behavior of differential characteristics.
- Stochastic equivalence and independence of the keys are not needed.
- Lots of characteristics found using the usual assumptions are in fact invalid.

Drawback

Matrices of size $2^{2^n} \times 2^{2^n}$ hence computation infeasible in general.

Plan of this Section

Generalization of planar pairs : [DR07]

Super planar pairs

(a, b) is a super planar pair for an Sbox S if

$$\left\{ \begin{pmatrix} x \\ S(x) \end{pmatrix} \mid S(x) + S(x+a) = b \right\}$$

is an affine space.

Remark

If $\# \{x \mid S(x) + S(x+a) = b\} \in \{2, 4\}$, (a, b) is super planar.

Our starting point

Consider a SPN consisting of r rounds with linear layer L and a non-linear layer which applies S in parallel.

Our starting point

Consider a SPN consisting of r rounds with linear layer L and a non-linear layer which applies S in parallel.

Theorem

Let Δ be a differential characteristic such that, for each intermediate Sbox, the pair (input difference, output difference) is super planar. Then :

$$\mathbb{P}(K, \Delta) = \begin{cases} p_0 \times 2^{\dim(W)} & \text{if } K \in c + W^{\perp} \\ 0 & \text{otherwise} \end{cases}$$

- p_0 is the probability that we obtain using the usual assumptions.
- $W \subset \mathbb{F}_2^{n(r-1)}$ is a vector space depending on Δ, L and S.
- $c + W^{\perp}$ is an affine subspace whose linear part is $W^{\perp}$.

Plan of this Section

Confirming known (but surprising) results

- MIDORI64 is a light-weight block cipher proposed by [BBI+15]
- Linear key-schedule

Confirming known (but surprising) results

- MIDORI64 is a light-weight block cipher proposed by [BBI+15]
- Linear key-schedule

Baudrin et al. proved the following result using *commutative cryptanalysis*.

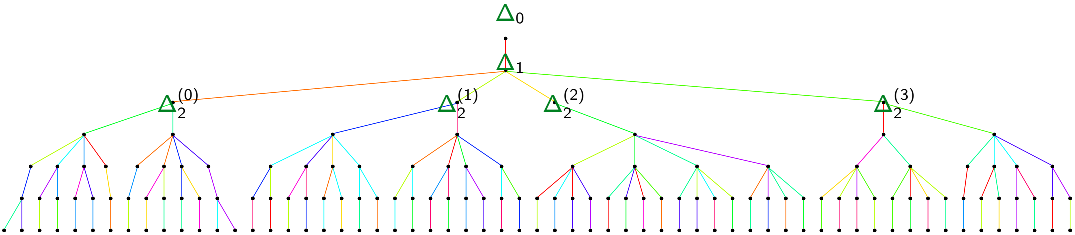
Proposition [BFL+23]

Let $\Delta_0 \in \{\texttt{0xa},\texttt{0xf}\}^{16}$ and $K_i \in \langle \texttt{0x2},\texttt{0x5},\texttt{0x8}\rangle^{16}$. Then for any r,

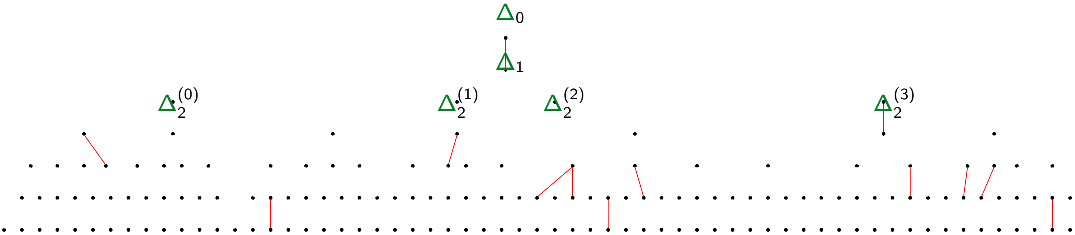
$$\sum_{\Delta_r \in \{\texttt{0xa},\texttt{0xf}\}^{16}} \mathbb{P}(K, \Delta_0, \Delta_r) \geq 2^{-16}$$

Our framework allows us to confirm and extend this result.

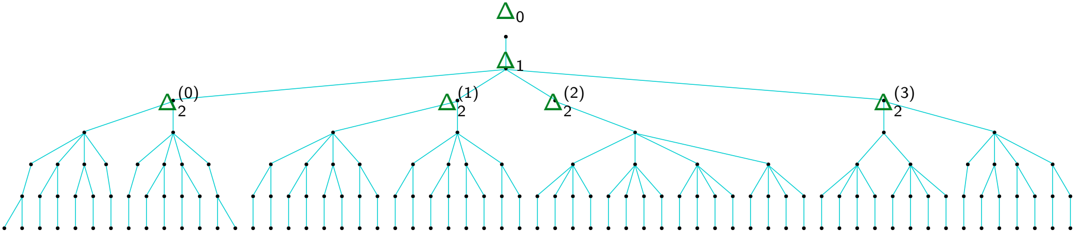
How we thought it behaved



How we thought it behaved



How it really behaves



All characteristics are valid for the same keys !

Conclusion

- Analyzing the fixed-key behavior is crucial ...

Conclusion

- Analyzing the fixed-key behavior is crucial ... but difficult in general

Conclusion

- Analyzing the fixed-key behavior is crucial … but difficult in general
- Our work gives a partial answer.

Conclusion

- Analyzing the fixed-key behavior is crucial ... but difficult in general
- Our work gives a partial answer.

Some more applications

- The result holds for modified MIDORI64 with non-involutive Sboxes.
- Our framework confirms a similar result on SCREAM.

Conclusion

- Analyzing the fixed-key behavior is crucial ... but difficult in general
- Our work gives a partial answer.

Some more applications

- The result holds for modified MIDORI64 with non-involutive Sboxes.
- Our framework confirms a similar result on SCREAM.

Thank you for listening !

Bibliography I

- Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni.
  Midori: A block cipher for low energy.
  In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part II*, volume 9453 of *LNCS*, pages 411–436. Springer, Berlin, Heidelberg, November / December 2015.
- Jules Baudrin, Patrick Felke, Gregor Leander, Patrick Neumann, Léo Perrin, and Lukas Stennes.
  Commutative cryptanalysis made practical.
  IACR Trans. Symm. Cryptol., 2023(4):299–329, 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.

Bibliography II

Eli Biham and Adi Shamir.
Differential cryptanalysis of DES-like cryptosystems.
Journal of Cryptology, 4(1):3–72, January 1991.

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

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.

Xuejia Lai, James L. Massey, and Sean Murphy.
Markov ciphers and differential cryptanalysis.
In Donald W. Davies, editor, *EUROCRYPT'91*, volume 547 of *LNCS*, pages 17–38. Springer, Berlin, Heidelberg, April 1991.