Differential Meet-in-the-Middle Cryptanalyis

Christina Boura[1], Nicolas David[2], **Patrick Derbez**[3], Gregor Leander[4], and María Naya-Plasencia[2]

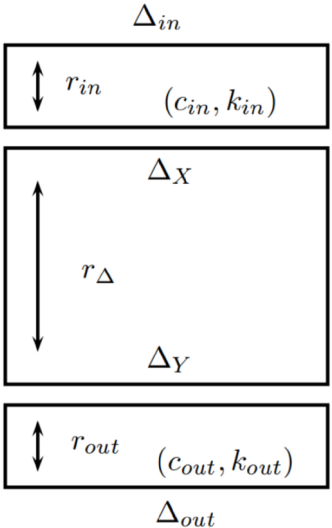
[1] Université Paris-Saclay, UVSQ, CNRS, Laboratoire de mathématiques de Versailles
[2] Inria
[3] Univ Rennes, Inria, CNRS, IRISA
[4] Ruhr University Bochum

Question

Université de Rennes

Can we use meet-in-the-middle related techniques to improve differential attacks?

Differential Attack



top $P[\Delta_{in} \to \Delta_X] = 2^{-c_{in}}$

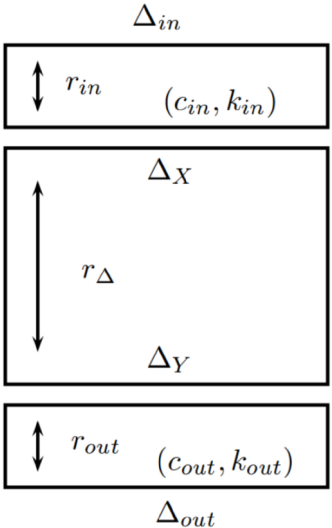
middle $P[\Delta_X \to \Delta_Y] = 2^{-p}$

bottom $P[\Delta_{out} \to \Delta_Y] = 2^{-c_{out}}$

Main idea

Given $\alpha 2^{c_{in}} 2^p$ pairs with difference Δ_{in}, we expect on average α pairs following the differential in the middle rounds and thus the **right value** for $k_{in} \cup k_{out}$ should appear α times.

Differential Attack



top $P[\Delta_{in} \to \Delta_X] = 2^{-c_{in}}$

middle $P[\Delta_X \to \Delta_Y] = 2^{-p}$

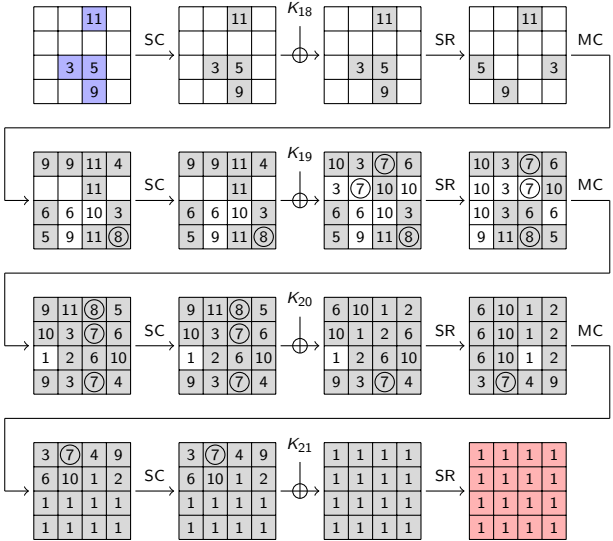
bottom $P[\Delta_{out} \to \Delta_Y] = 2^{-c_{out}}$

Main idea

Given $\alpha 2^{c_{in}} 2^p$ pairs with difference Δ_{in}, we expect on average α pairs following the differential in the middle rounds and thus the **right value** for $k_{in} \cup k_{out}$ should appear α times.

Given one pair of data, how to determine possible values for $k_{in} \cup k_{out}$?

Differential Attack - Retrieving Key Candidates

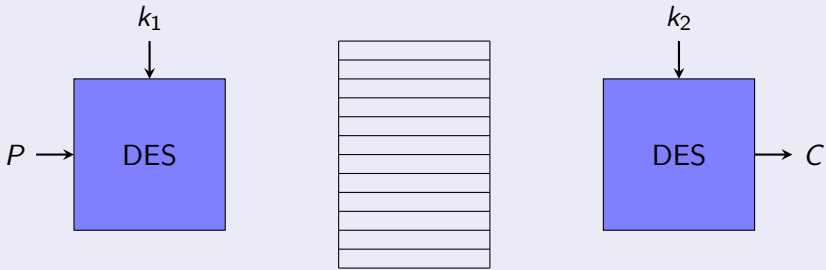


- Early abort technique
- Rebound-like procedure
- Knowing both input/output differences around an Sbox leads to the actual values
- Might be **very complex** depending on the key schedule and the cipher

A Well-Known MitM Attack

$$2DES_{k_1,k_2} = DES_{k_2} \circ DES_{k_1}$$

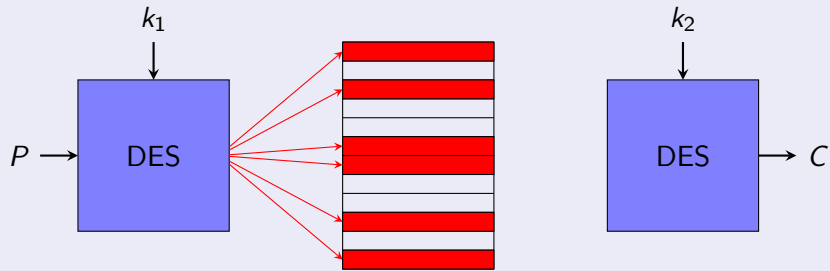
A Well-Known MitM Attack



$$2DES_{k_1,k_2} = DES_{k_2} \circ DES_{k_1}$$

- Initialize a Hash Table

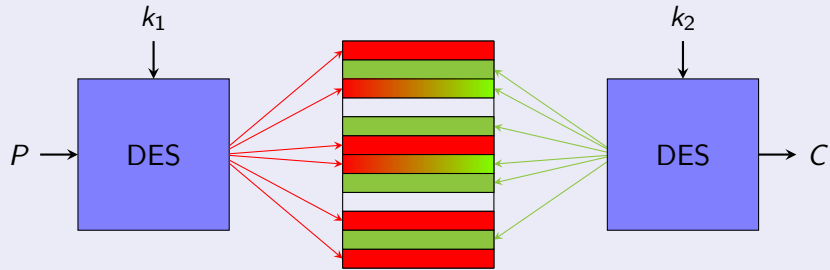
A Well-Known MitM Attack



$$2DES_{k_1,k_2} = DES_{k_2} \circ DES_{k_1}$$

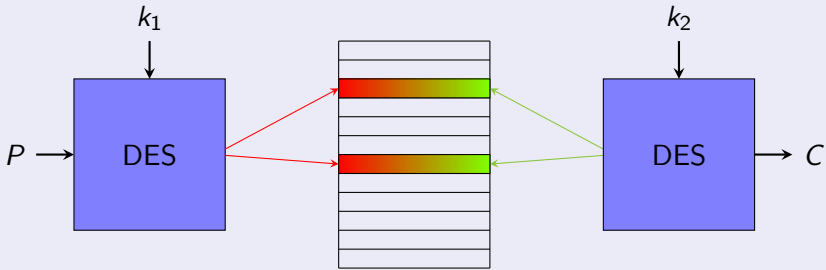
- Initialize a Hash Table
- For all k_1, store $M = DES_{k_1}(P) \rightarrow k_1$

A Well-Known MitM Attack



- Initialize a Hash Table
- For all k_1, store $M = DES_{k_1}(P) \rightarrow k_1$
- For all k_2, look-up $M = DES^{-1}_{k_2}(C)$

A Well-Known MitM Attack

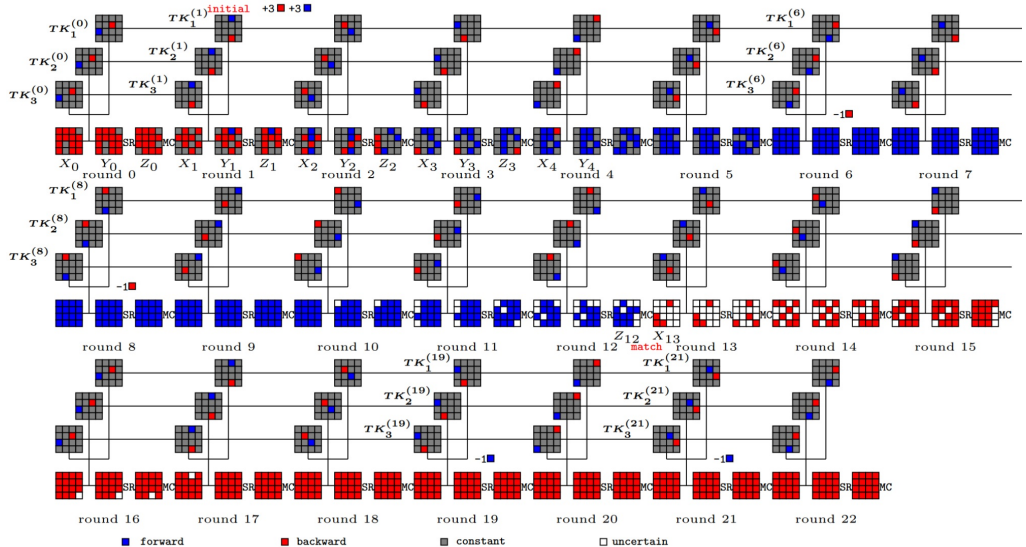


$$2DES_{k_1,k_2} = DES_{k_2} \circ DES_{k_1}$$

- Initialize a Hash Table
- For all k_1, store $M = DES_{k_1}(P) \rightarrow k_1$
- For all k_2, look-up $M = DES^{-1}_{k_2}(C)$

Time complexity $\approx 2^k$ encryptions, with $2k$-bit keys!

More complicated (Dong et al., CRYPTO'21)

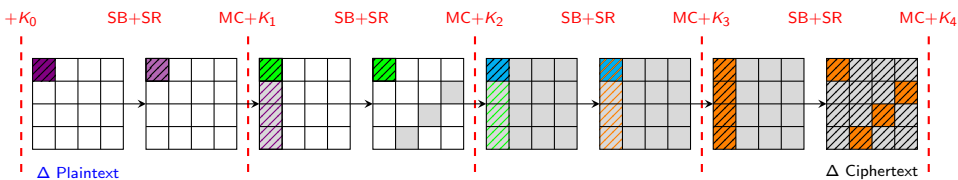


Differential and MitM

- Can we combine ideas from both differential and MitM attacks?

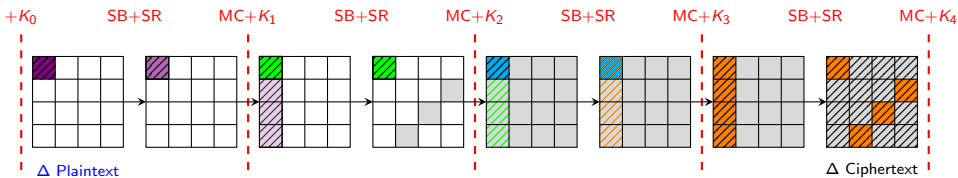
Differential and MitM

- Can we combine ideas from both differential and MitM attacks? Yes!
  - Consider plaintexts/states in structures
  - Differential Enumeration Technique (Demirci-Selçuk attacks)



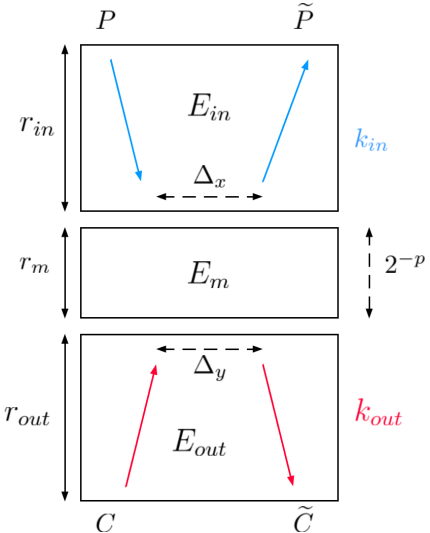
Differential and MitM

- Can we combine ideas from both differential and MitM attacks? Yes!
  - Consider plaintexts/states in structures
  - Differential Enumeration Technique (Demirci-Selçuk attacks)



- Reduce complexities of MitM attacks
- Rely on **truncated** differential characteristics only

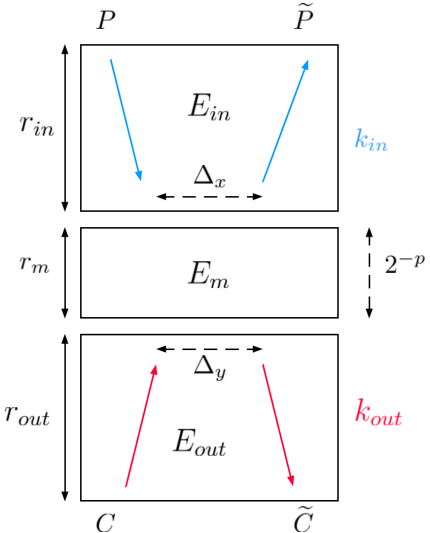
Our New Framework



Procedure:

1. Ask for one plaintext/ciphertext pair (P, C)
2. Construct the set of the $|k_{in}|$ possible plaintexts $\mathcal{P}$
3. Construct the set of the $|k_{out}|$ possible ciphertexts $\mathcal{C}$
4. Search for valid $(P', C') \in \mathcal{P} \times \mathcal{C}$ by looking for a collision

Our New Framework



Procedure:

1. Ask for one plaintext/ciphertext pair (P, C)
2. Construct the set of the $|k_{in}|$ possible plaintexts $\mathcal{P}$
3. Construct the set of the $|k_{out}|$ possible ciphertexts $\mathcal{C}$
4. Search for valid $(P', C') \in \mathcal{P} \times \mathcal{C}$ by looking for a collision

Pro:
- Much easier to deal with the key
- Specific improvement for ciphers with partial key addition

Con:
- More memory than for classical differential attacks

Two Targets - New Results

- **SKINNY-128-384:** First attack against 25 rounds in the single tweakey model!
- **AES-256:** First attack against 12 rounds requiring only 2 related keys!

Two Targets - New Results

- **SKINNY-128-384:** First attack against 25 rounds in the single tweakey model!
- **AES-256:** First attack against 12 rounds requiring only 2 related keys!

Seem to work well when the key size is larger than the block size

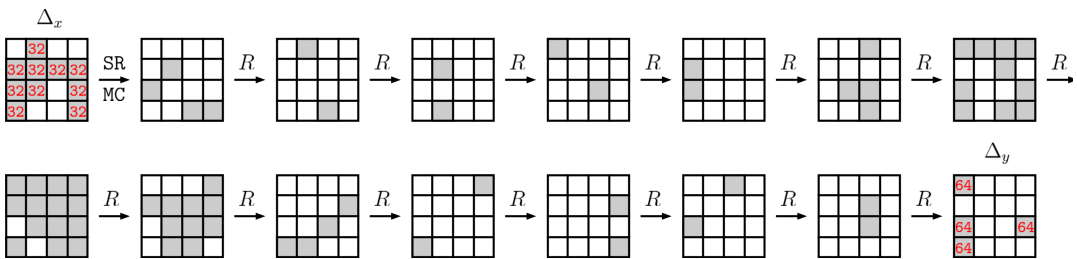
Two Targets - New Results

- **SKINNY-128-384:** First attack against 25 rounds in the single tweakey model!

# Rounds	Data	Time	Memory	Type	Ref.
21	2^{123}	$2^{353.6}$	2^{341}	ID	Yang et al.
21	$2^{122.89}$	$2^{347.35}$	2^{336}	ID	Hadipour et al.
22	2^{96}	$2^{382.46}$	$2^{330.99}$	DS-MITM	Shi et al.
22	$2^{92.22}$	$2^{373.48}$	$2^{147.22}$	ID	Tolba et al.
23	2^{104}	2^{376}	2^{8}	MITM	Dong et al.
23	2^{117}	$2^{361.9}$	$2^{118.5}$	Diff. MITM	new
24	2^{117}	$2^{361.9}$	2^{183}	Diff. MITM	new
24	$2^{122.3}$	$2^{372.5}$	$2^{123.8}$	Diff. MITM	new
25	$2^{122.3}$	$2^{372.5}$	$2^{188.3}$	Diff. MITM	new

Differential on SKINNY-128

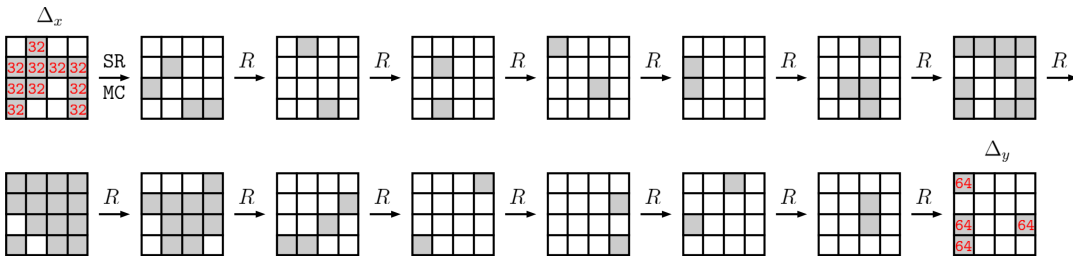
- For the 25-round attack, we use the following differential on 15 rounds:



- CP model from Delaune et al. (2021) to estimate its probability: $2^{-p} \geq 2^{-116.5}$
  - Note that the best differential characteristic has probability 2^{-131}

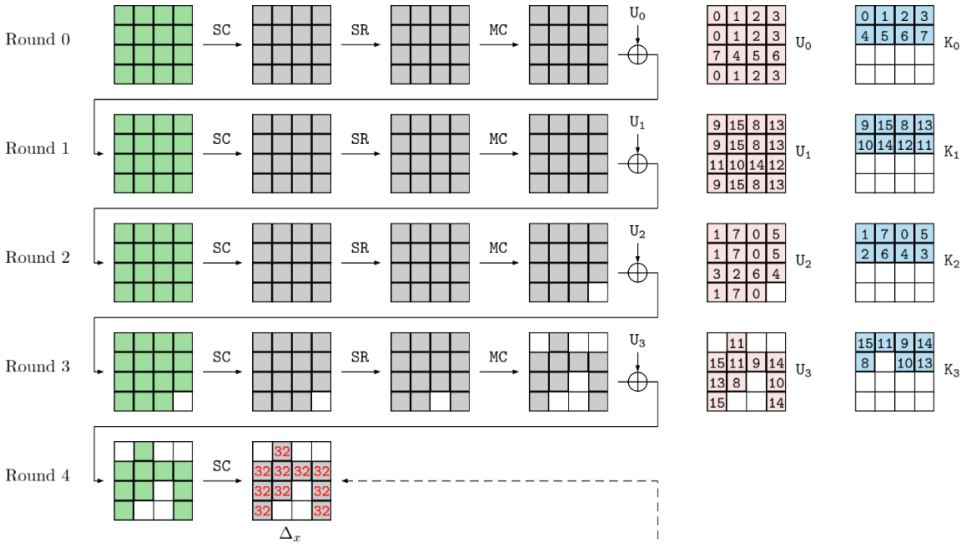
Differential on SKINNY-128

- For the 25-round attack, we use the following differential on 15 rounds:

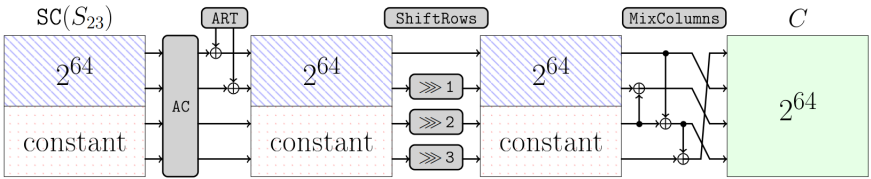


- CP model from Delaune et al. (2021) to estimate its probability: $2^{-p} \geq 2^{-116.5}$
  - Note that the best differential characteristic has probability 2^{-131}
- Extended by adding 4 rounds to the plaintext, 5 rounds to the ciphertext and one extra free round

4 rounds to the plaintext

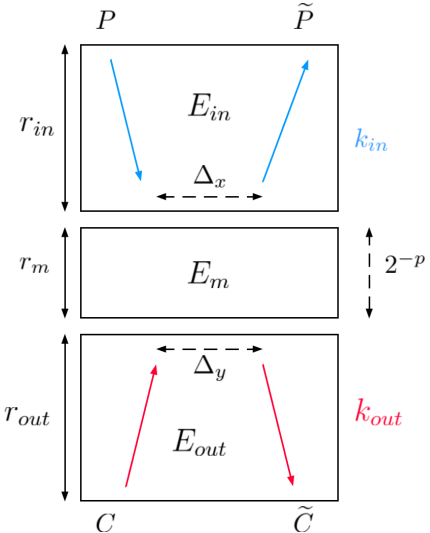


Extra Free Round



- The round key is only applied to the first two rows
- Consider structure of 2^{64} plaintext/ciphertext pairs
- The attack is performed on the 2^{64} pairs in parallel

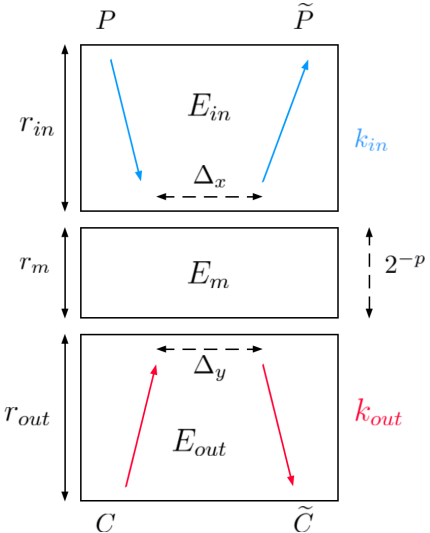
Our New Framework



Procedure:

1. Ask for one structure of 2^{64} plaintext/ciphertext pair (P, C)
2. Construct the set of the $|k_{in}|$ possible plaintexts $\mathcal{P}$
3. Construct the set of the $|k_{out}|$ possible ciphertexts $\mathcal{C}$
4. Search for valid $(P', C') \in \mathcal{P} \times \mathcal{C}$ by looking for a collision

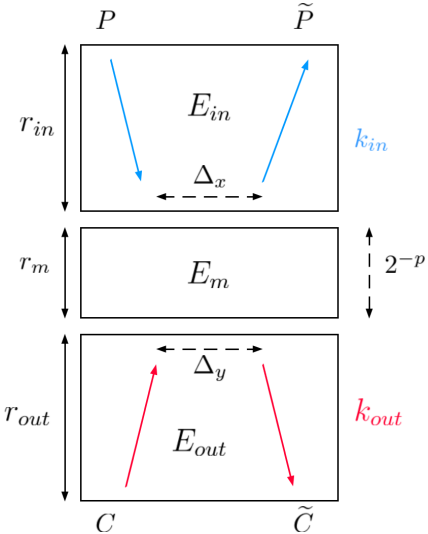
Our New Framework



Procedure: repeat 2^p times

1. Ask for one structure of 2^{64} plaintext/ciphertext pair (P, C)
2. Construct the set of the $|k_{in}|$ possible plaintexts $\mathcal{P}$
3. Construct the set of the $|k_{out}|$ possible ciphertexts $\mathcal{C}$
4. Search for valid $(P', C') \in \mathcal{P} \times \mathcal{C}$ by looking for a collision

Our New Framework



Procedure: repeat $2^p/2^{64}$ times

1. Ask for one structure of 2^{64} plaintext/ciphertext pair (P, C)
2. Construct the set of the $|k_{in}|$ possible pairs of plaintexts $\mathcal{P}$
3. Construct the set of the $|k_{out}|$ possible pairs of "ciphertexts" $\mathcal{C}$
4. Search for valid $((P, P'), (C, C')) \in \mathcal{P} \times \mathcal{C}$ by looking for a collision

Conclusion

- New cryptanalysis technique: **the Differential MITM attack**
- More improvements described in the paper (e.g. data reduction)
- First attack against 25-round SKINNY-128-384 in the single tweakey model
- First attack against 12-round AES-256 with only two related keys

- Many open questions and future works:
  - When is this framework better than classical differential attacks?
  - Can we automatize the search of such attacks?
  - Can this framework work with truncated differentials?
  - Can we combine MitM attacks with other cryptanalysis techniques?
  - ...

Conclusion

- New cryptanalysis technique: **the Differential MITM attack**
- More improvements described in the paper (e.g. data reduction)
- First attack against 25-round SKINNY-128-384 in the single tweakey model
- First attack against 12-round AES-256 with only two related keys

- Many open questions and future works:
  - When is this framework better than classical differential attacks?
  - Can we automatize the search of such attacks?
  - Can this framework work with truncated differentials?
  - Can we combine MitM attacks with other cryptanalysis techniques?
  - ...

Thank you for your attention!