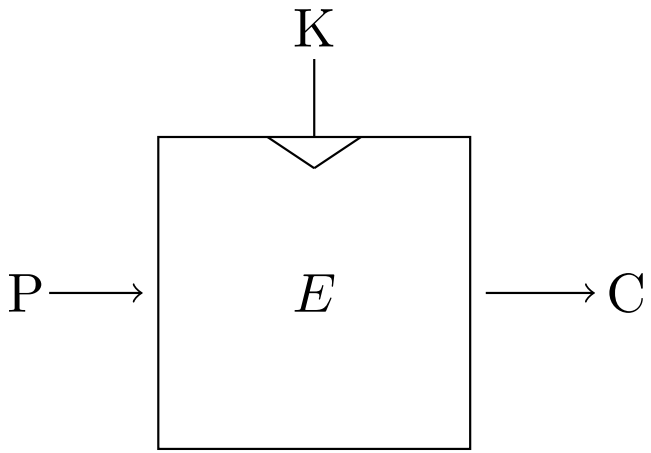
Improvements of the differential MITM attack

M'foukh Dounia

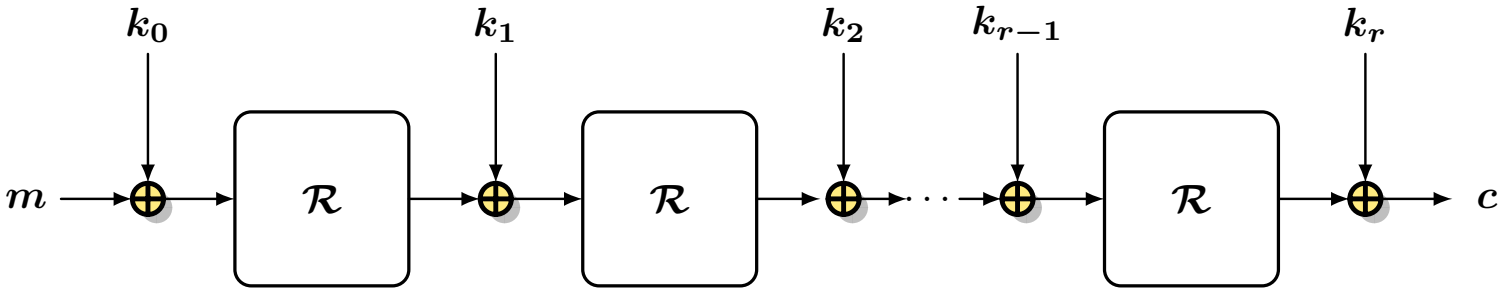
Table of contents

Block Cipher

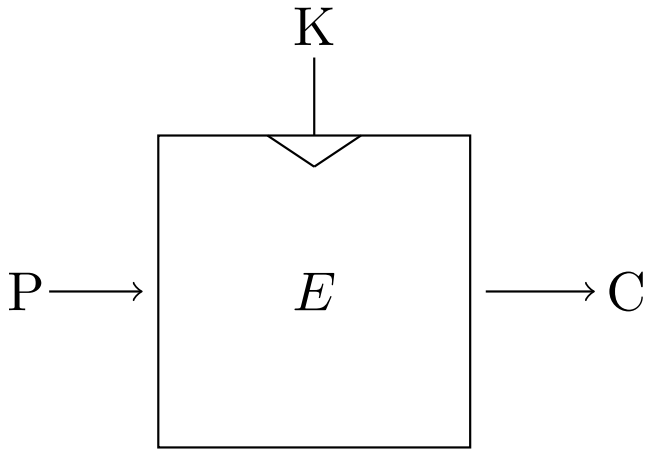


- Block of size n of 64 or 128 bits in general.
- Key size k of 128 or 256 bits in general.

Example of a round function :

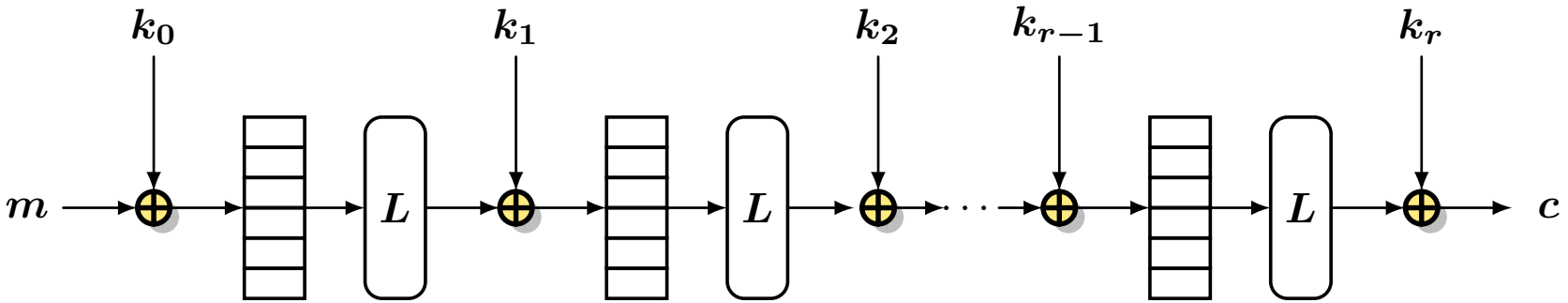


Block Cipher



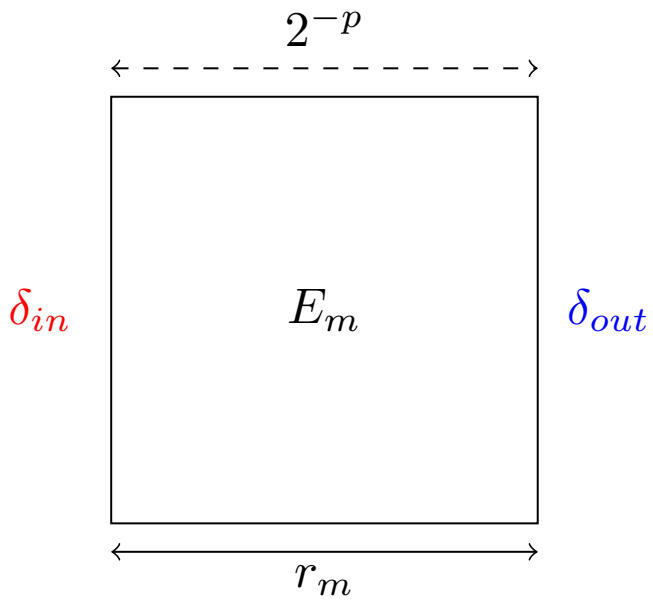
- Block of size n of 64 or 128 bits in general.
- Key size k of 128 or 256 bits in general.

Example of a round function :



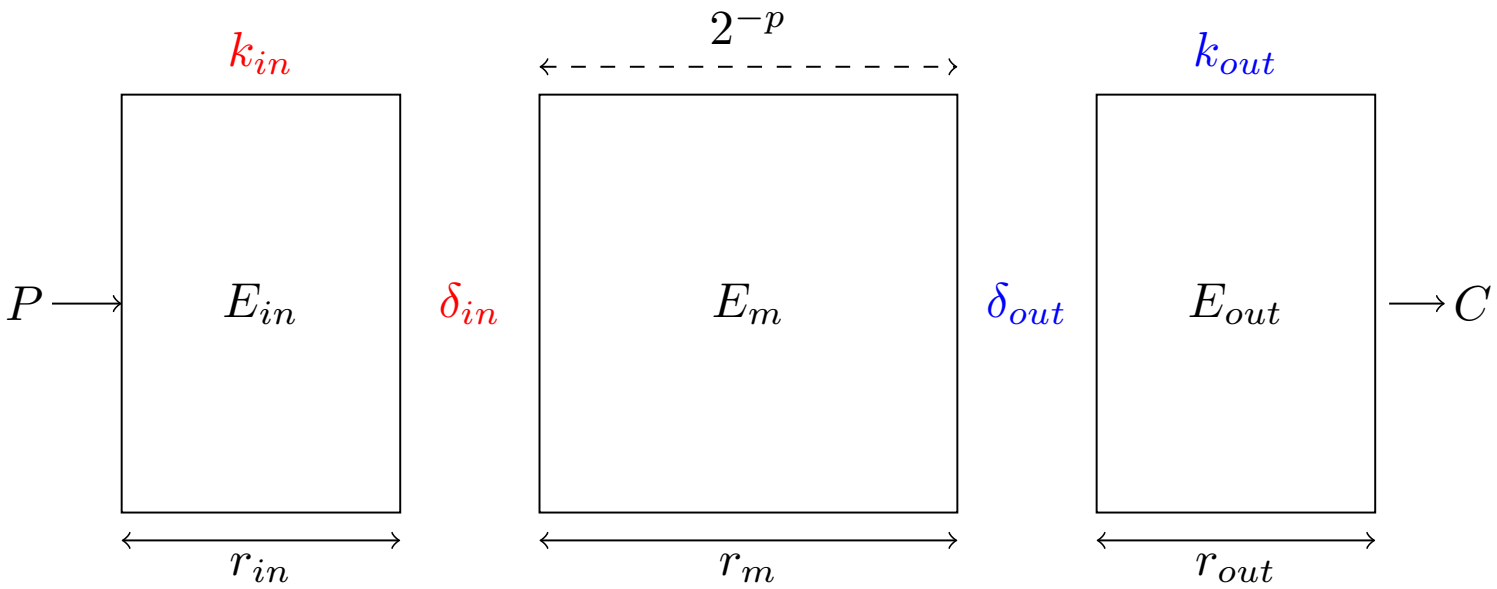
Differential cryptanalysis

Introduced to the public by Biham and Shamir in 1990 in [BS90]



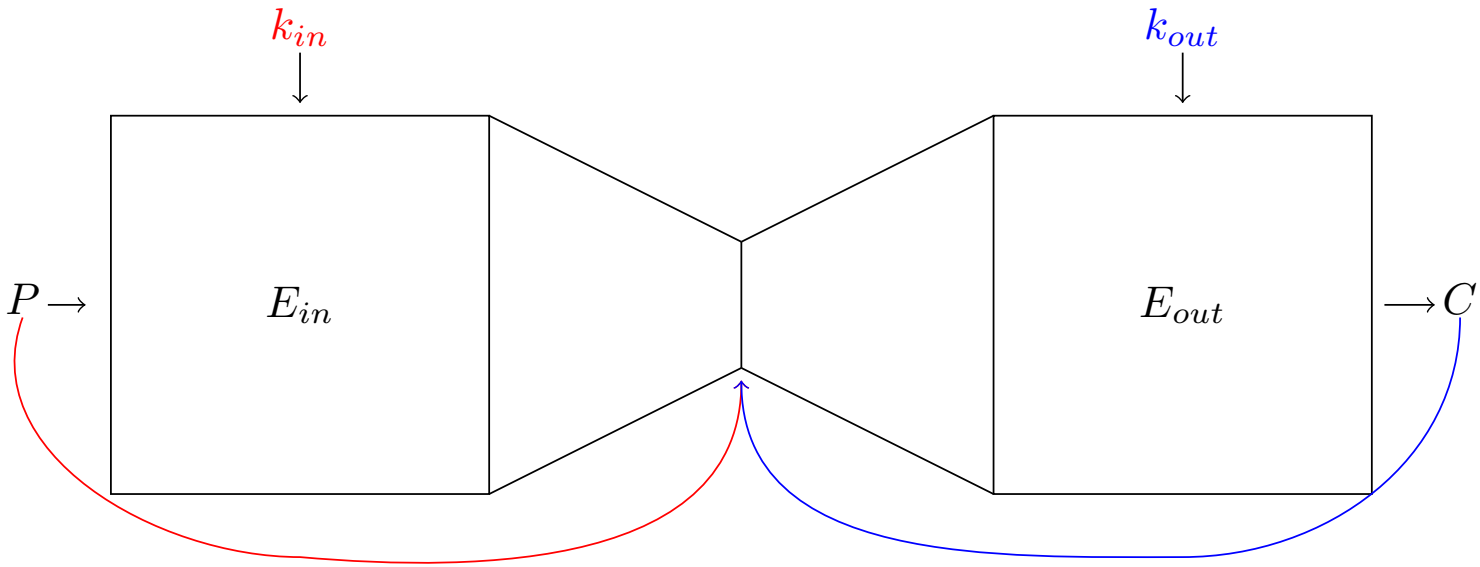
Differential cryptanalysis

Introduced to the public by Biham and Shamir in 1990 in [BS90]

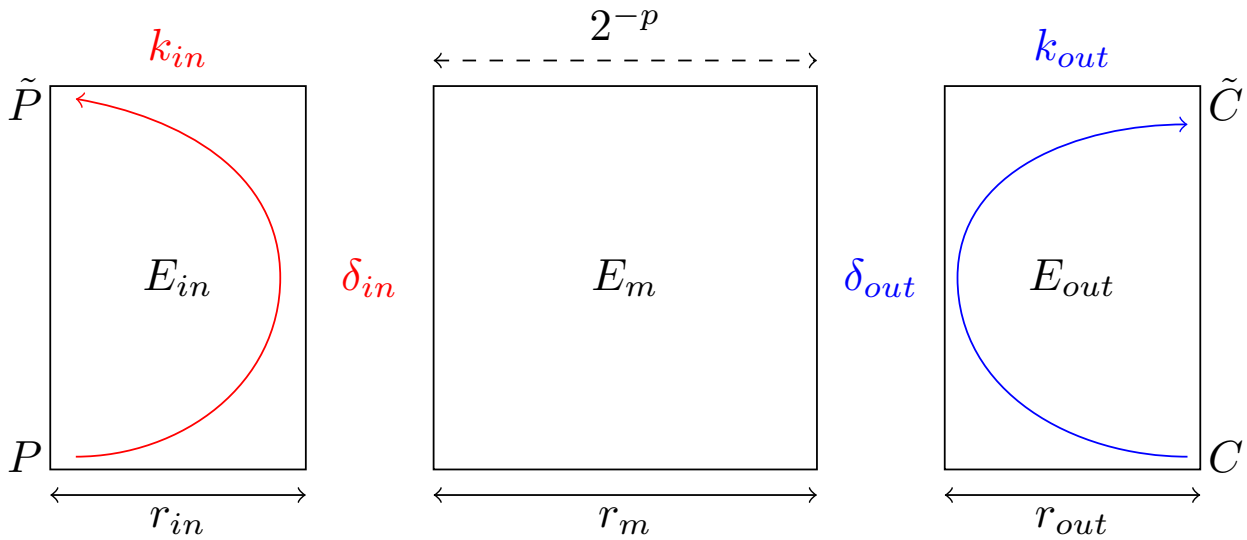


Meet-In-The-Middle (MITM) attack

Introduced by Diffie and Hellman in 1977 in [DH77]



Differential Meet-In-The-Middle [BDD+23]



We generate 2^p pairs (P, C).

$$P \to 2^{|k_{in}|}\tilde{P} \text{ and } C \to 2^{|k_{out}|}\tilde{C}.$$

We keep k_{in} and k_{out} such that $\tilde{P} = E^{-1}(\tilde{C})$.

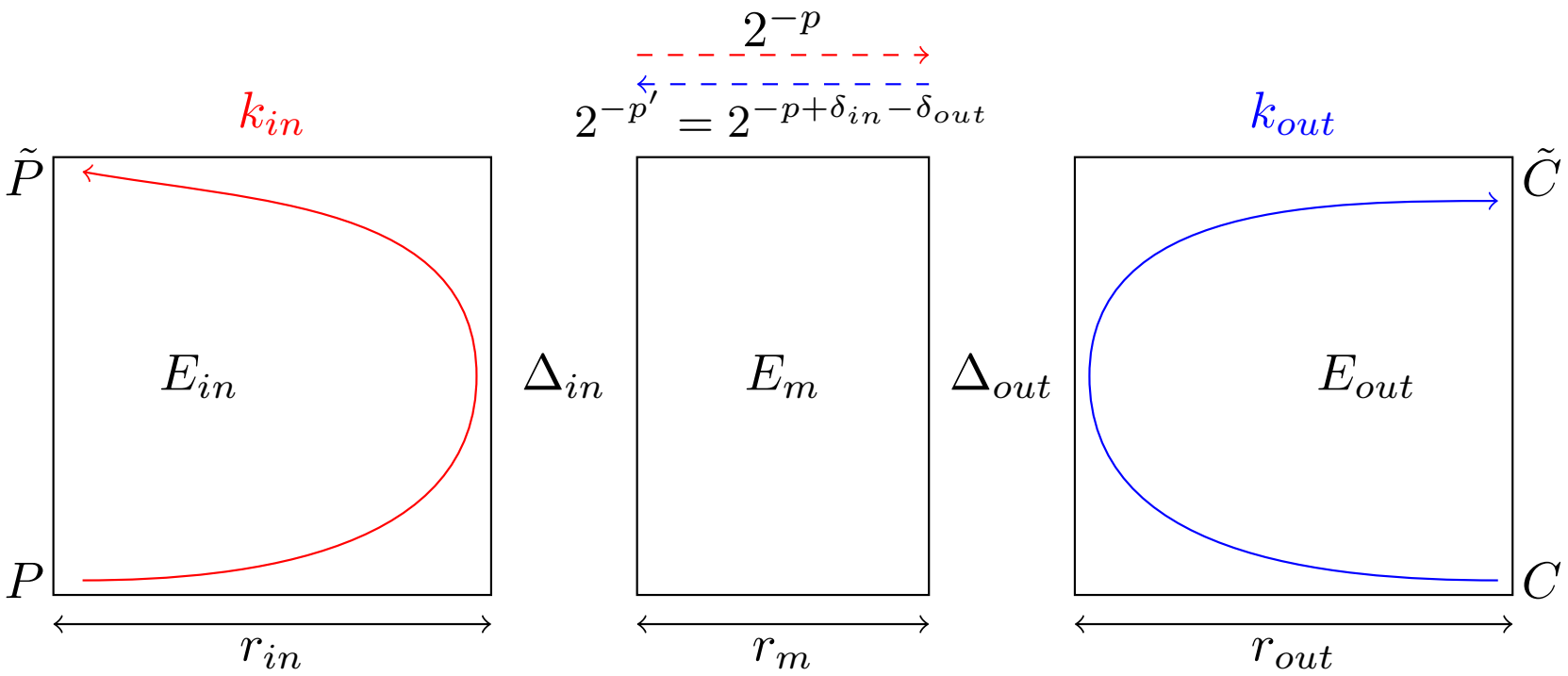
Improvement of the differential MITM attack

Improvement of the differential MITM attack

- Extension to truncated differential MITM attack.
- Improved structures.
- State-test technique.
- Probability in the key recovery part.

Truncated differential MITM

Instead of fixed differences δ_{in} and δ_{out}, we consider sets of differences Δ_{in} and Δ_{out}.

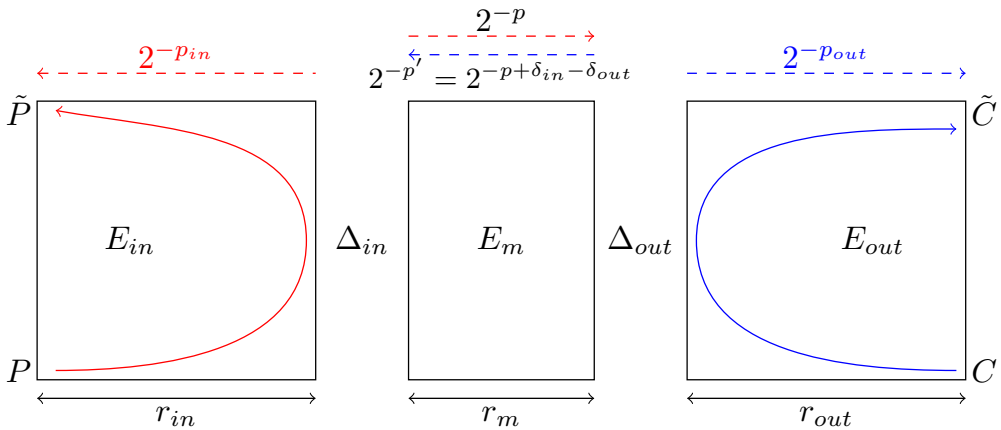


Key guessing improvement : Probability and State-test technique

1. State test technique :
   - Technique inherited from impossible differential cryptanalysis in [BLNS18]
   - Test a part of the internal state defining a partition of the involved key bits.

Key guessing improvement : Probability and State-test technique

1. State test technique :
   - Technique inherited from impossible differential cryptanalysis in [BLNS18]
   - Test a part of the internal state defining a partition of the involved key bits.
2. Probabilistic key recovery



The probability for a random pair to follow the differential path is now $2^{-p-p_{in}-p_{out}}$.

Application of the improvements

Application of the improvements

- 23 rounds of SKINNY-64-192;
- 25 rounds of SKINNY-128-384;
- 23 rounds out of 31 rounds of CRAFT.

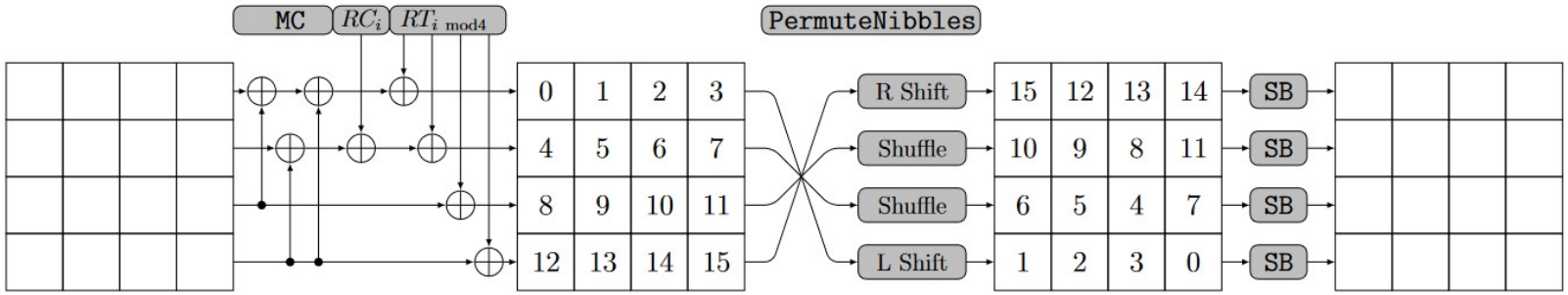
Cipher	Rounds	Time	Data	Memory	Attack	Ref.
CRAFT	21	$2^{106.53}$	$2^{60.99}$	2^{100}	ID	[HSE23]
	23	2^{125}	2^{60}	2^{68}	Tr-Diff-MITM	
SKINNY-64-192	23	2^{188}	2^{52}	2^{4}	MITM	[DHS+21]
	23	2^{184}	2^{60}	2^{8}	MITM	[DHS+21]
	23	2^{188}	2^{56}	2^{104}	Tr-Diff-MITM	
SKINNY-128-384	24	$2^{361.9}$	2^{117}	2^{183}	Diff-MITM	[BDD+23]
	25	$2^{372.5}$	$2^{122.3}$	$2^{188.3}$	Diff-MITM	[BDD+23]
	25	$2^{378.9}$	2^{117}	2^{165}	Diff-MITM	
	25	2^{366}	$2^{122.3}$	$2^{188.3}$	Diff-MITM	

MITM: Meet In the Middle
Diff-MITM: Differential MITM
ID: Impossible Differential
Tr-Diff-MITM: Truncated Differential MITM

Table: Summary of the best known cryptanalysis on CRAFT, SKINNY-64-192 and SKINNY-128-384 in the single tweak setting.

Description of CRAFT

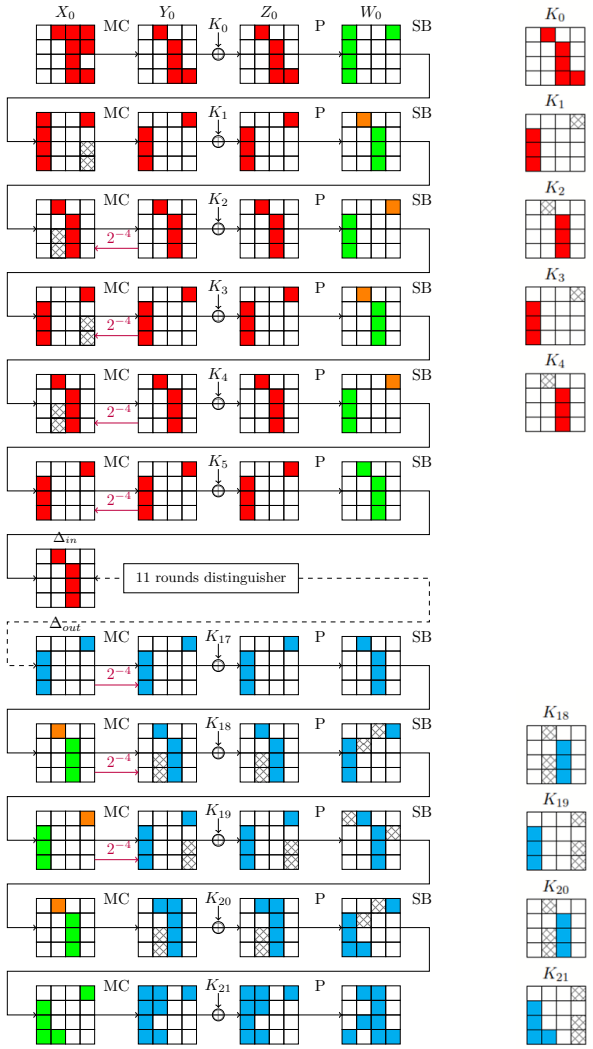
CRAFT [BLMR19], published in TOSC in 2019, is a lightweight tweakable block cipher operating on a 64-bit block, a 128-bit key $(K_0||K_1)$, and a 64-bit tweak T.



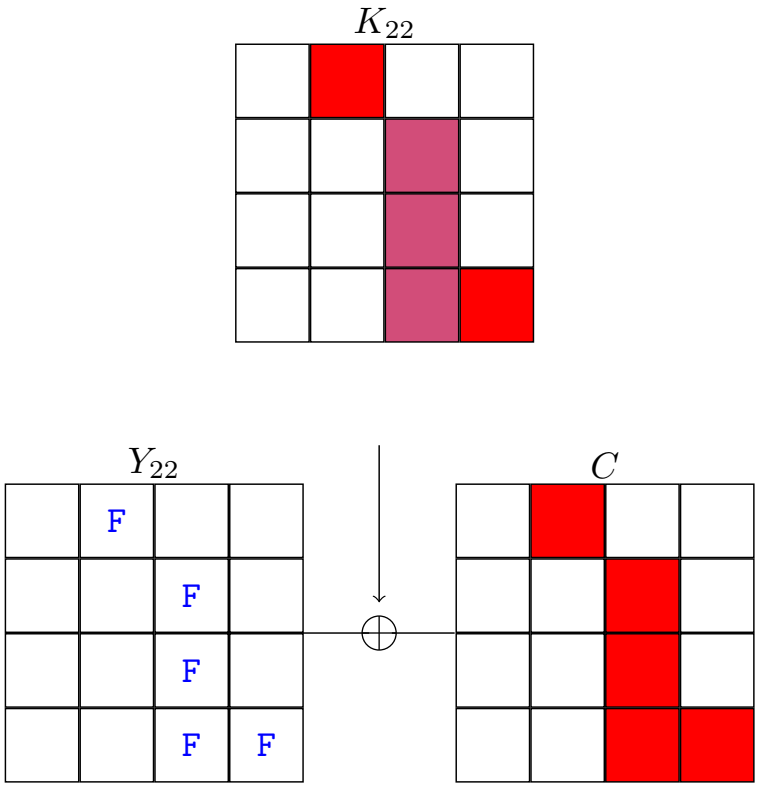
Attack against 22+1 rounds of CRAFT

We use a truncated differential characteristic over 11 rounds.
Parameters :

$$p = 44,$$
$$p_{in} = 16,\ p_{out} = 12,$$
$$|\Delta_{in}| = |\Delta_{out}| = 16,$$
$$|k_{in}| = 48,\ |k_{out}| = 44$$
$$\text{and } |k_{in} \cap k_{out}| = 24.$$



Extension of one round



We fix the 5 words F, thus the structure will be of size 2^{44}. The purple subkey words are already known for both the lower and upper part and the red subkey words are known for the upper part.

Complexities

Time complexity to recover information on the key

$$\begin{aligned}\mathcal{T} &= 2^{12} \times 2^{24}(2^{44} \times 2^{24} \times 2^{16-16} + 2^{44} \times 2^{20} \times 2^{16-12} + 2^{68+68-20-44}) \\ &= 2^{108}.\end{aligned}$$

The time complexity to recover the whole key is finally $\mathcal{T} = 2^{125}$.

Complexities

Time complexity to recover information on the key

$$\begin{aligned}\mathcal{T} &= 2^{12} \times 2^{24}(2^{44} \times 2^{24} \times 2^{16-16} + 2^{44} \times 2^{20} \times 2^{16-12} + 2^{68+68-20-44}) \\ &= 2^{108}.\end{aligned}$$

The time complexity to recover the whole key is finally $\mathcal{T} = 2^{125}$.

Memory and data complexities

$\mathcal{M} = 2^{68}$ and $\mathcal{D} = 2^{60}$.

Conclusion

Conclusion

- Several new attacks leading to best known applications.
- Differential MITM attacks have a different nature than differential attacks.

Reference I

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, *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part III*, volume 14083 of *Lecture Notes in Computer Science*, pages 240–272. Springer, 2023.

Christof Beierle, Gregor Leander, Amir Moradi, and Shahram Rasoolzadeh.
CRAFT: lightweight tweakable block cipher with efficient protection against DFA attacks.
IACR Trans. Symmetric Cryptol., 2019(1):5–45, 2019.

Reference II

Christina Boura, Virginie Lallemand, María Naya-Plasencia, and Valentin Suder.
Making the impossible possible.
J. Cryptol., 31(1):101–133, 2018.

Eli Biham and Adi Shamir.
Differential cryptanalysis of des-like cryptosystems.
In Alfred Menezes and Scott A. Vanstone, editors, *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer, 1990.

Whitfield Diffie and Martin E. Hellman.
Special feature exhaustive cryptanalysis of the NBS data encryption standard.
Computer, 10(6):74–84, 1977.

Reference III

Xiaoyang Dong, Jialiang Hua, Siwei Sun, Zheng Li, Xiaoyun Wang, and Lei Hu.
Meet-in-the-middle attacks revisited: Key-recovery, collision, and preimage attacks.
In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part III*, volume 12827 of *Lecture Notes in Computer Science*, pages 278–308. Springer, 2021.

Reference IV

Hosein Hadipour, Sadegh Sadeghi, and Maria Eichlseder.
Finding the impossible: Automated search for full impossible-differential, zero-correlation, and integral attacks.
In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part IV*, volume 14007 of *Lecture Notes in Computer Science*, pages 128–157. Springer, 2023.