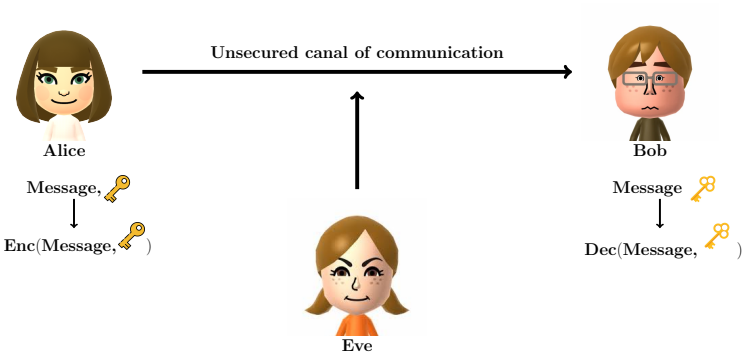
Differential cryptanalysis

Dounia M'foukh[1]

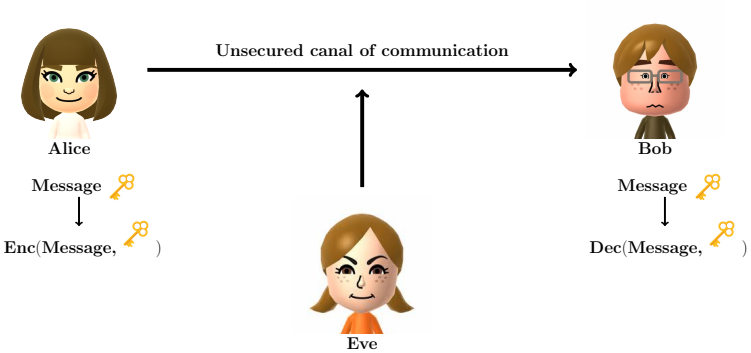
[1]Inria Paris

Symmetric encryption



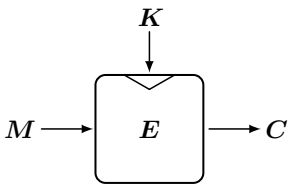
- Goal: Ensure that only the authorized entities has access to the message.
- Secret key shared beforehand.

Symmetric encryption



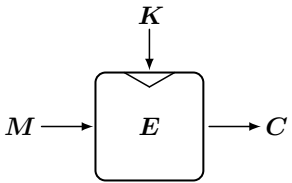
- Goal: Ensure that only the authorized entities has access to the message.
- Secret key shared beforehand.

Block ciphers



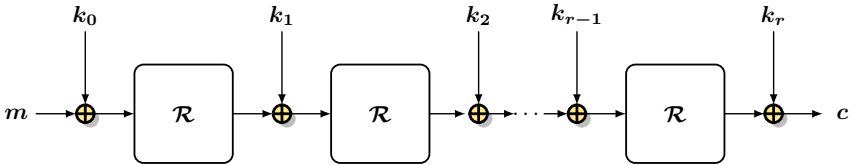
- E is a function $\mathbb{F}_2^n \times \mathbb{F}_2^k \to \mathbb{F}_2^n$.
- Block of size n of 64 or 128 bits in general.
- Key of size k of 128 or 256 bits in general.

Block ciphers

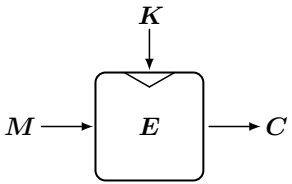


- E is a function $\mathbb{F}_2^n \times \mathbb{F}_2^k \to \mathbb{F}_2^n$.
- Block of size n of 64 or 128 bits in general.
- Key of size k of 128 or 256 bits in general.

Usual structure of a block cipher:

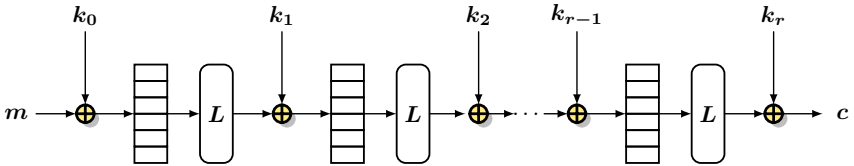


Block ciphers



- E is a function $\mathbb{F}_2^n \times \mathbb{F}_2^k \to \mathbb{F}_2^n$.
- Block of size n of 64 or 128 bits in general.
- Key of size k of 128 or 256 bits in general.

Usual structure of a block cipher:



Security of a Block cipher

The security is defined by the best generic attack.

$\rightsquigarrow$ Exhaustive search of the secret key.

- Best attack against an ideal cipher.
- Test all the possible key with a known pair (M, C).
- Cost 2^k encryption.
- The size k of the key need to be big enough.

Security of a Block cipher

The security is defined by the best generic attack.

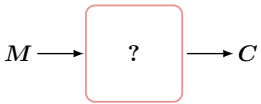
$\rightsquigarrow$ Exhaustive search of the secret key.

- Best attack against an ideal cipher.
- Test all the possible key with a known pair (M, C).
- Cost 2^k encryption.
- The size k of the key need to be big enough.

$\rightsquigarrow$ Cryptanalysis is needed to trust the security of the ciphers.

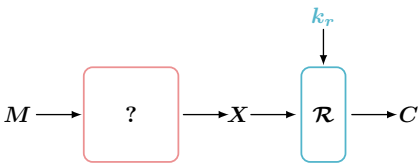
What is an attack?

1. Distinguisher



- Find property to distinguish a block cipher from a random permutation with a high probability.
- Number of queries $\rightsquigarrow$ complexity of the distinguisher.

2. Last round attack



- Transform the distinguisher into key-recovery attack.
- For each guess of $k_r \rightarrow$ check if (M, X) verify the distinguisher properly.
- Can add more than one round.

How to measure the efficiency of an attack?

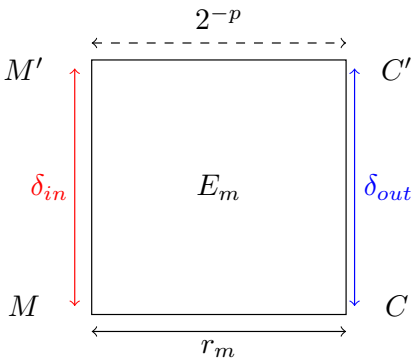
Three complexities to measure an attack:

- Time complexity: number of computations to succeed $\rightsquigarrow < 2^k$ encryptions.
- Data complexity: number of queries used $\rightsquigarrow < 2^n$.
- Memory complexity: size of memory used.

$\rightsquigarrow$ Many possible Trade-offs.

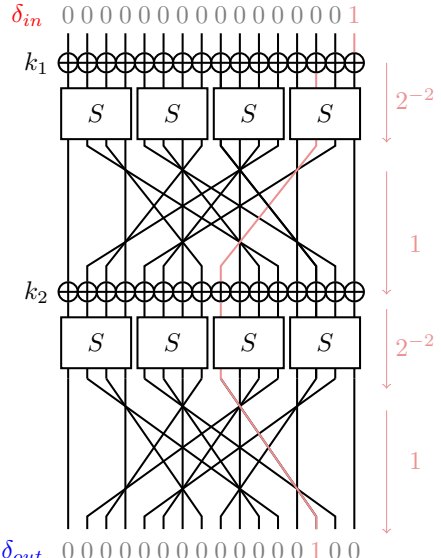
Differential Cryptanalysis

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



- Distinguishes if $2^{-p} >> 2^{-n}$.
- (δ_{in},δ_{in}) is called a differential.

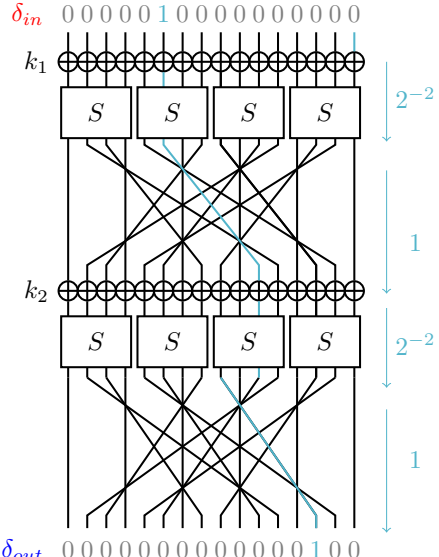
An example



- Probability of the path $2^{-4} >> 2^{16}$.
- Difference distribution table:

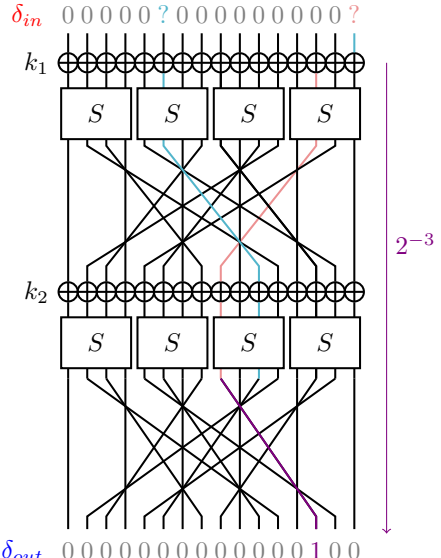
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	4	4	4	4	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	4	0	0	4	2	2	2	2
3	0	0	0	0	0	0	0	0	4	0	0	4	2	2	2	2
4	0	4	0	0	0	0	4	0	0	2	2	0	2	0	0	2
5	0	4	0	0	0	4	0	0	0	2	2	0	2	0	0	2
6	0	4	0	0	4	0	0	0	0	2	2	0	0	2	2	0
7	0	4	0	0	0	0	0	4	0	2	2	0	0	2	2	0
8	0	0	4	4	0	0	0	0	4	0	4	0	0	0	0	0
9	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
a	0	0	0	0	2	2	2	2	4	0	4	0	0	0	0	0
b	0	0	4	4	0	0	0	0	0	0	0	0	2	2	2	2
c	0	0	2	2	2	2	0	0	0	2	0	2	2	0	2	0
d	0	0	2	2	0	0	2	2	0	2	0	2	0	2	0	2
e	0	0	2	2	0	0	2	2	0	2	0	2	2	0	2	0
f	0	0	2	2	2	2	0	0	0	2	0	2	0	2	0	2

An example



- Probability of the path $2^{-4} >> 2^{16}$.
- Same output as other path.

An example

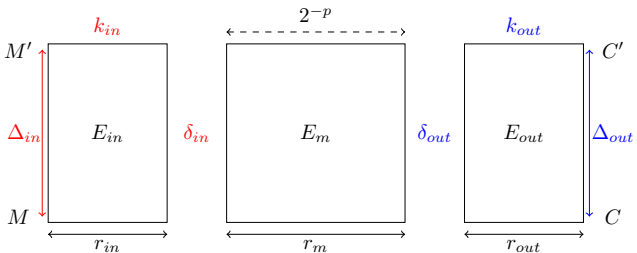


- Probability of the path $2^{-4} >> 2^{16}$.
- Same output as other path.
- Combine both differential characteristic $\rightsquigarrow$ probability increases.
-  This probability might be wrong (quasi-differential...).

1. Symmetric cryptography
2. Differential Cryptanalysis
3. Key recovery attack

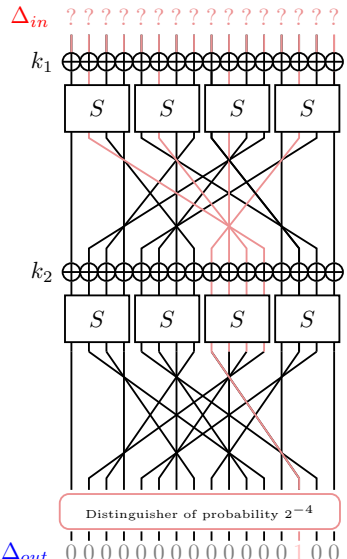
Key-recovery attack

Let $E = E_{out} \circ E_m \circ E_{in}$ be a block cipher.



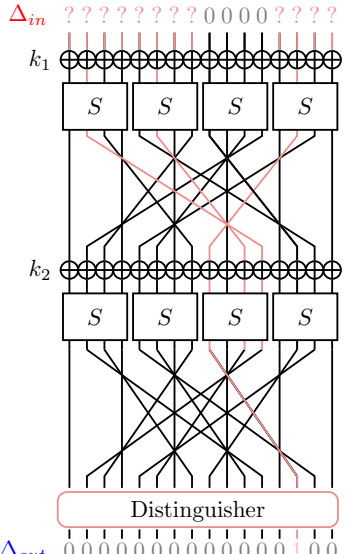
- Δ_{in} and Δ_{out} are the sets of differences that can lead to δ_{in} and δ_{out}.
- Find candidate triplets $(P, P', k_{in} \cup k_{out})$ that imply δ_{in} and δ_{out}.
- The time complexity depends in part on the size of k_{in} and k_{out}.

An example



- Propagate the differences δ_{in} and δ_{out}.
- Build "structure" of plaintexts, the space of pairs of plaintext taking all the possible values for the ? bits.
- Filter when their corresponding ciphertexts using Δ_{out}.
- Guess the all the bits of k_1 and 4 bits of k_2.

Improving key-recovery attacks



- Study the possible weaknesses of the Sbox.
- Other existing techniques to improve key-recovery attacks $\rightsquigarrow$ State-test technique: guess the bit of the state instead of the key.
- Recover information on the key through non-linear equations.

Conclusion

Conclusion

- Still need to study known attacks.
- Cryptanalysis is essential to trust the ciphers used.

Conclusion

Conclusion

- ⇝ Still need to study known attacks.
- ⇝ Cryptanalysis is essential to trust the ciphers used.

Thank you for your attention !