Division Property: a New Attack Against Block Ciphers

Christina Boura

(joint on-going work with Anne Canteaut)

Séminaire du groupe Algèbre et Géometrie, LMV
November 24, 2015

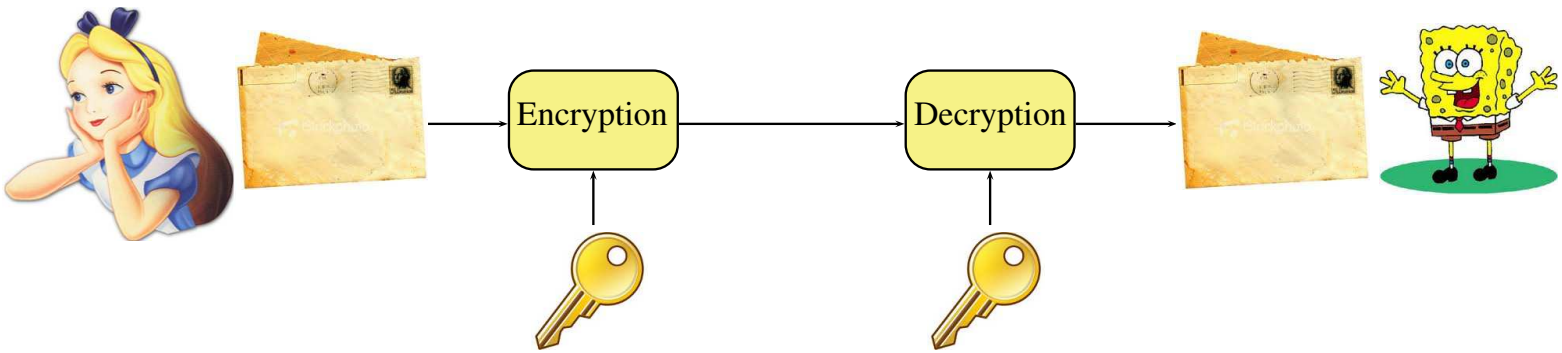
UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

université PARIS-SACLAY

informatics mathematics Inria

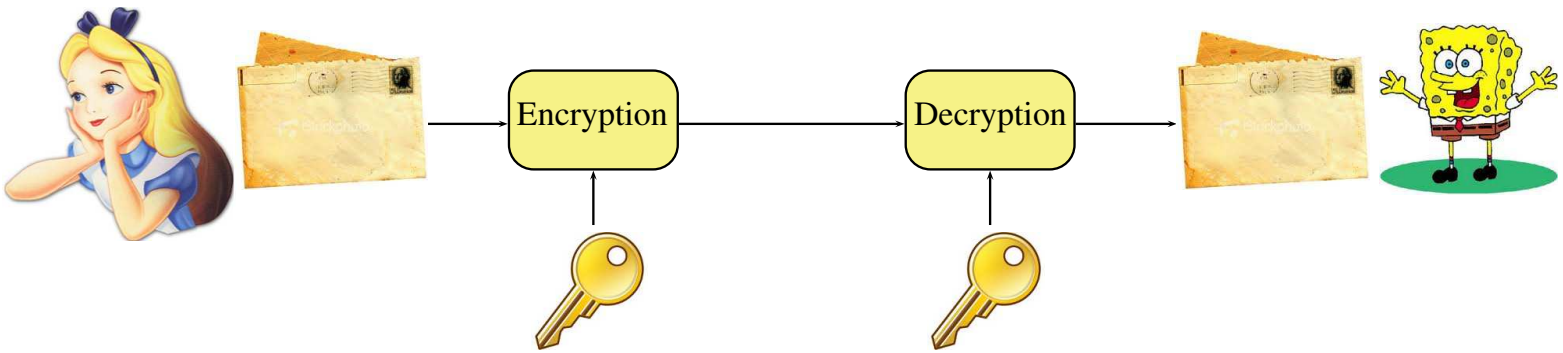
Symmetric-key encryption

Alice and Bob exchange the secret key through a **secure channel**.



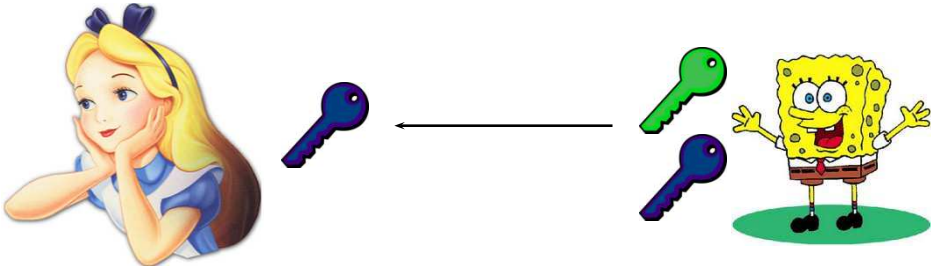
Symmetric-key encryption

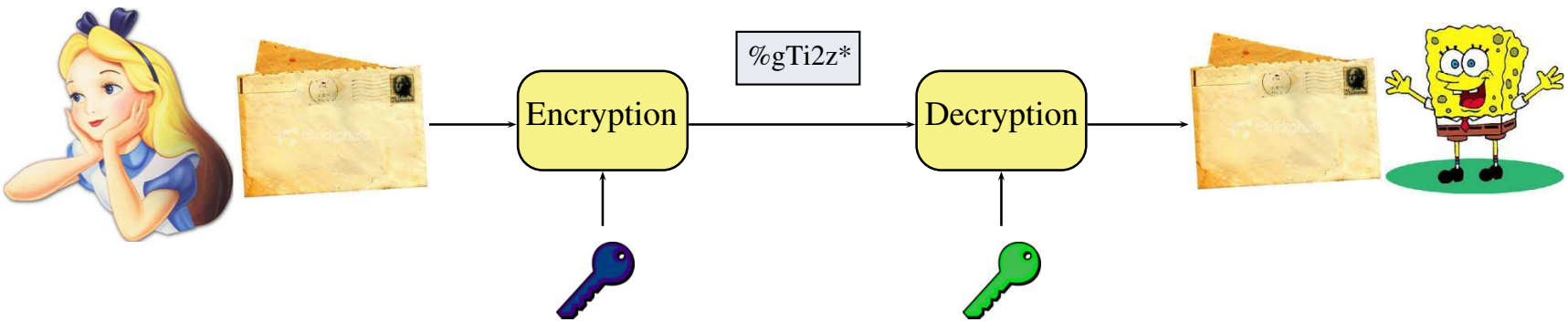
Alice and Bob exchange the secret key through a **secure channel**.



Key-exchange problem $\Rightarrow$ birth of the public-key cryptography.

Public-key encryption



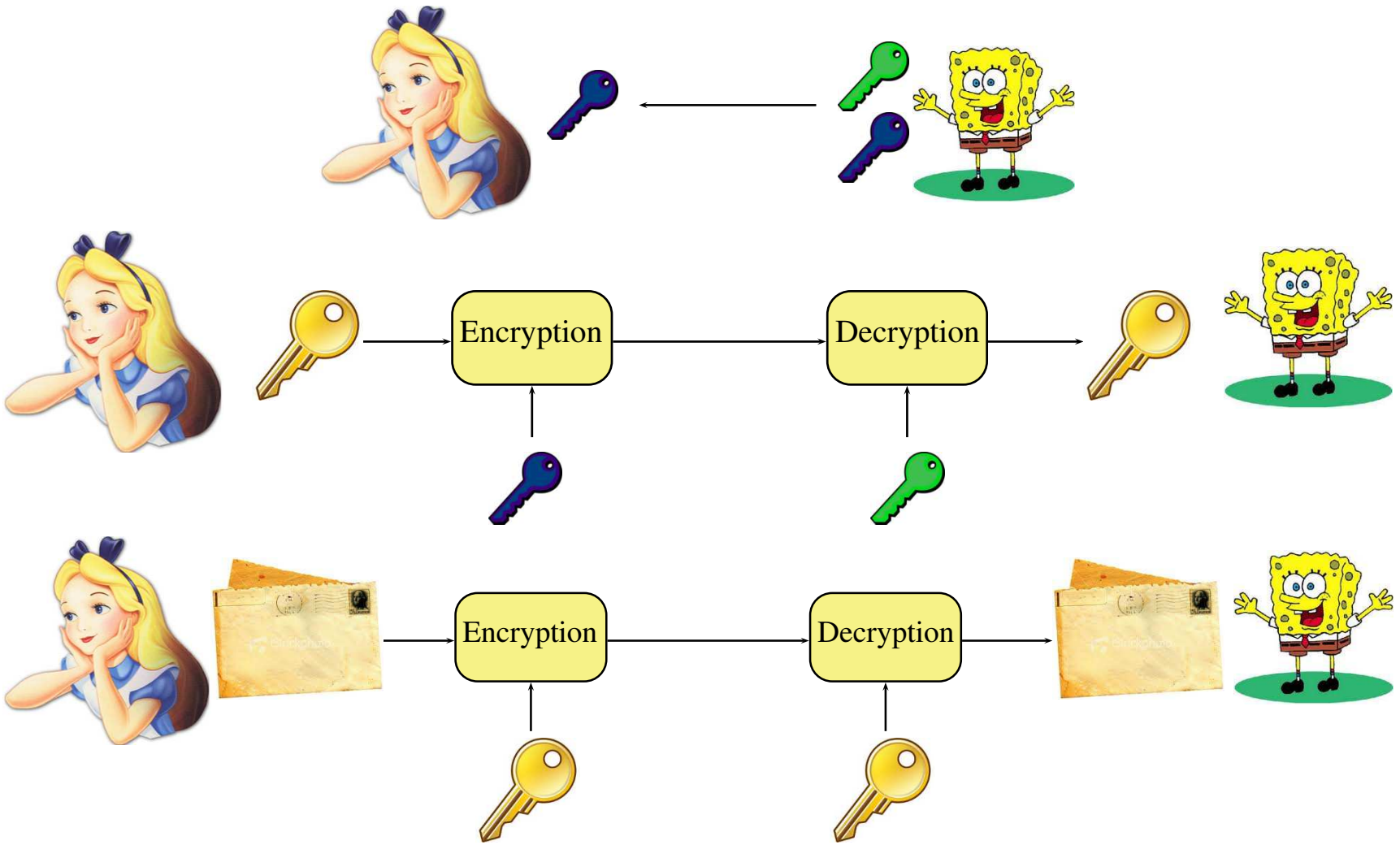


Advantages and disadvantages of each system

	Advantages	**Disadvantages**
Secret-key	Fast systems Relatively short-keys	Need secure key-exchange n users: n^2 keys
Public-key	No key-exchange needed n users: $2n$ keys	Slow systems Relatively long-keys

Hybrid encryption

Idea: Use a combination of asymmetric and symmetric encryption to benefit from the strengths of every system.



Hybrid encryption

- Use a public-key cryptosystem to exchange a key (session key).
- Use the exchanged key to encrypt data by using a symmetric-key cryptosystem.

Advantages:

- Slow public-cryptosystem is used to encrypt a short string only.
- Fast symmetric-key cryptosystem is used to encrypt the longer communication session.

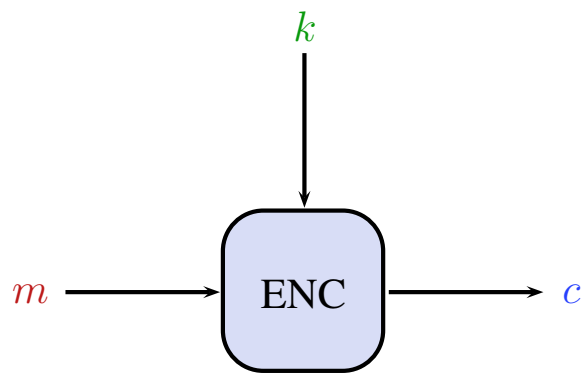
Used for example in the SSL protocol.

Outline

Block ciphers

Encrypt a block of **message** m into a block of **ciphertext** c under the action of the **key** k.

$$\begin{aligned} \text{ENC} : \{0,1\}^n \times \{0,1\}^\kappa &\rightarrow \{0,1\}^n \\ (m,k) &\mapsto ENC(m,k) = c \end{aligned}$$

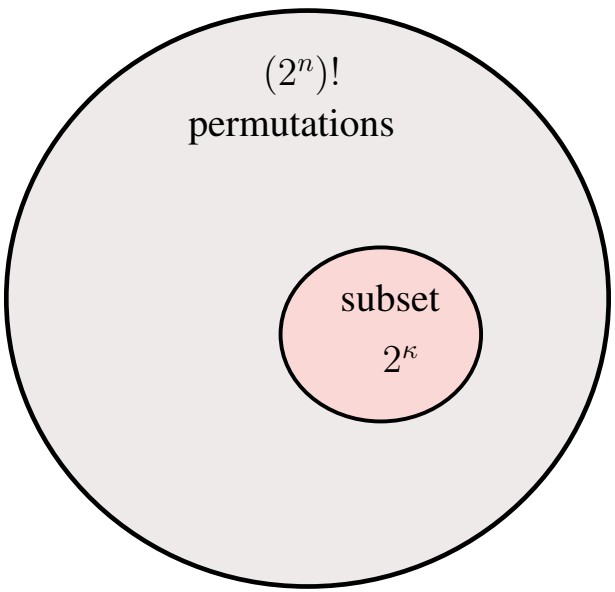


- Given k, it must be easy to compute c from m.
- Given m, c it must be hard to compute k such that $ENC(m,k) = c$.

Two important parameters:

- block size, n
- key size, κ

A block cipher generates a family of permutations indexed by a key k.



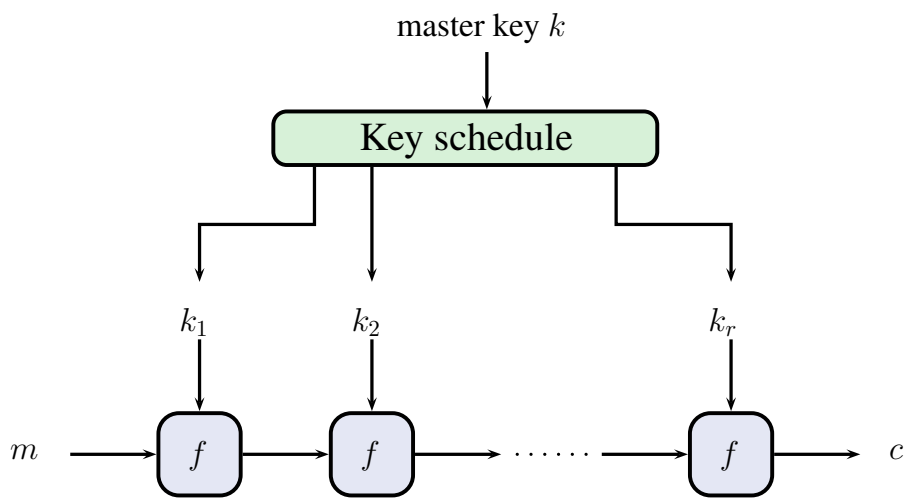
Ideal design: 2^κ permutations chosen uniformly at random from all $2^n! \approx 2^{(n-1)2^n}$ permutations.

Iterated block ciphers

Idea: Iterate a round function f several times. The function f^r is waited to be strong for large r.

Advantages:

- Compact implementation.
- Easier analysis.



Use a key schedule to extend the user-supplied (or master) key to a sequence of r subkeys.

How to build the round function?

Two major approaches:

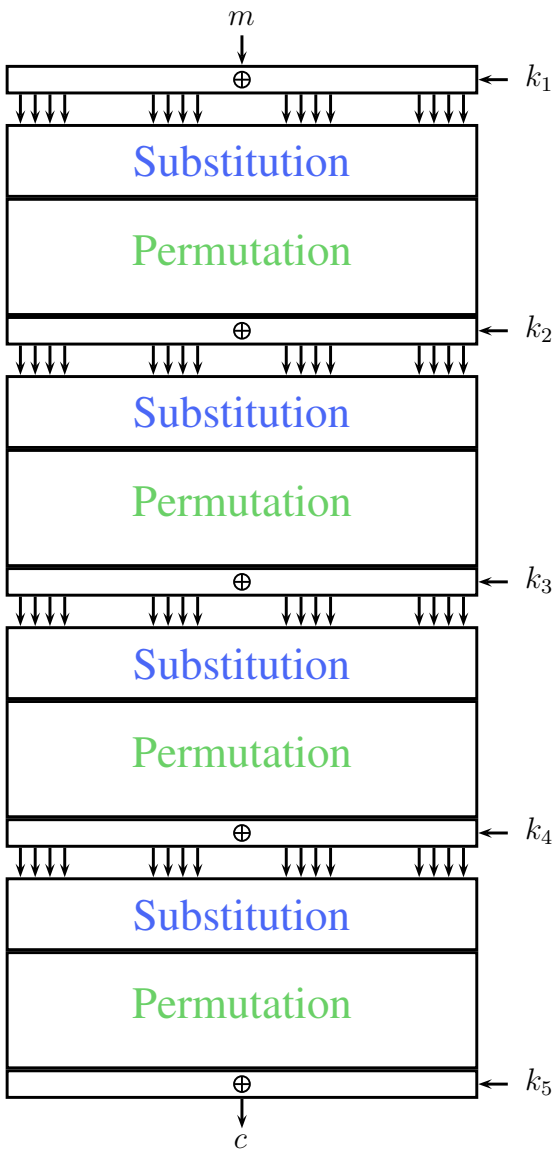
- Feistel network.
- Substitution-Permutation Network (SPN).

How to build the round function?

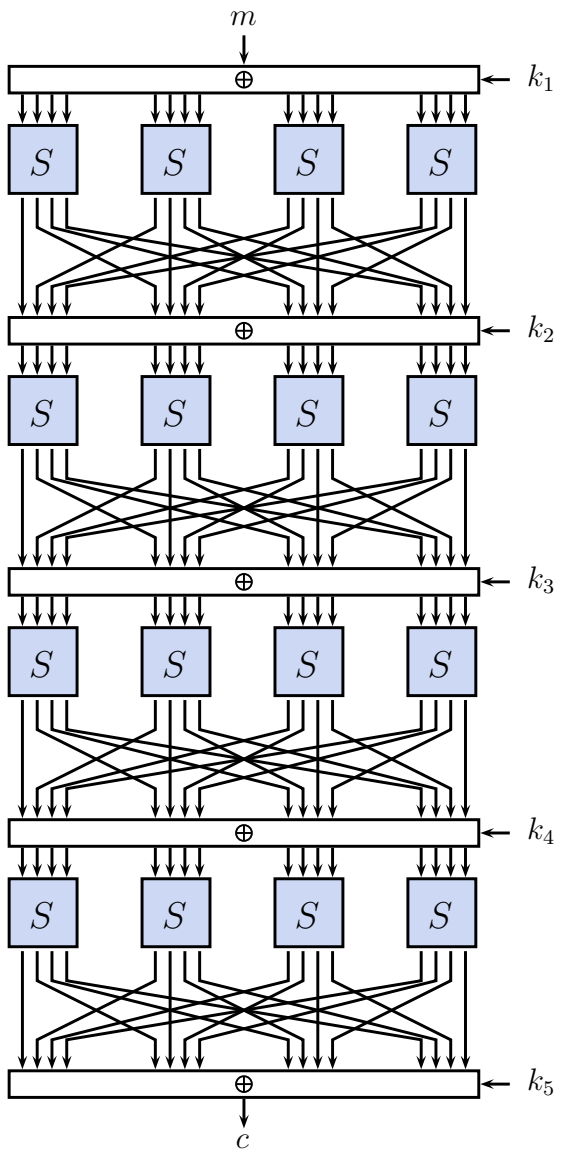
Two major approaches:

- Feistel network.
- Substitution-Permutation Network (SPN).

Substitution Permutation Network (SPN)



Substitution Permutation Network (SPN)



Cryptanalysis of block ciphers

Problem: Design block ciphers that are fast and secure at the same time.

In symmetric key cryptography, security proofs are partial and insufficient.

Only mean of proving that a design is secure:

cryptanalysis.

- An algorithm is secure as long there is no attack against it.
- The more an algorithm is analysed without being broken, the more reliable it is.

What does "broken" mean?

No attack faster than exhaustive search should exist.

If a block cipher encrypts messages with a k-bit key, no attack with time complexity less than 2^k should be known.

Otherwise, the cipher is considered as broken (even if the complexity of the attack is not practical).

Outline

A new property for block ciphers

- In Eurocrypt 2015, Yosuke Todo introduces a new property, called the division property.
- Combination (in some sense) of higher-order differential and saturation attacks.
- Construction of more powerful generic distinguishers for both SPN and Feistel constructions.
- Use of this new property for breaking full MISTY-1 (best paper award at CRYPTO 2015).

Notation

If $x, u \in \mathbf{F}_2^n$, we denote

$$x^u = \prod_{i=1}^{n} x_i^{u_i}$$

Example: $(n = 4)$

$x = (x_1, x_2, x_3, x_4) = (1, 1, 0, 1)$,
$u = (u_1, u_2, u_3, u_4) = (1, 0, 1, 0)$

$$x^u = {x_1}^{u_1} {x_2}^{u_2} {x_3}^{u_3} {x_4}^{u_4} = 1^1 1^0 0^1 1^0 = 0.$$

Division property

Let X be a multiset of elements in $\mathbf{F}_2^n$.

For $0 \leq k \leq n$, we say that X has the division property $\mathcal{D}_k^n$ if

$$\bigoplus_{x \in X} x^u = 0,$$

for all $u \in \mathbf{F}_2^n$ such that $wt(u) < k$.

Division property - Example

$$X = \{\texttt{0x0}, \texttt{0x3}, \texttt{0x3}, \texttt{0x3}, \texttt{0x5}, \texttt{0x6}, \texttt{0x8}, \texttt{0xB}, \texttt{0xD}, \texttt{0xE}\}.$$

Compute $\bigoplus_{x \in X} x^u$ for all $u \in \mathbf{F}_2^4$.

$$\bigoplus_{x \in X} x^u = 1,$$

for $u = 1011$, $u = 1101$ and $u = 1110$.

So, $\bigoplus_{x \in X} x^u = 0$ for all u with $wt(u) < 3$.

X has the division property $\mathcal{D}_3^4$.

Using the division property in practice

- Prepare a set of plaintexts and evaluate its division property.
- Propagate the input texts and evaluate the division property of the output set after one round.
  - Use rules to propagate the property through the different cipher components (Sboxes, XOR, etc..)
- Repeat the procedure and compute the division property of the set of texts after several rounds.
- If after several rounds some exploitable information is found, then we get a distinguisher.

Distinguisher and key recovery attack

Distinguisher: A property that permits to distinguish the target block cipher from an ideal permutation.

Division property:

$$\bigoplus_{y \in Y} E_K(y) \text{ has the division property } \mathcal{D}_k^n \text{ for } k \geq 1.$$

Key recovery: Exploit this property to recover the key by targeting first the subkey of the last round.

Outline

What is an Sbox?

Main component for providing non-linearity.

Can be seen as a vectorial Boolean function $S : \mathbf{F}_2^n \to \mathbf{F}_2^m$ (usually $m = n$).

Algebraic Normal Form (ANF) of an Sbox

$$
\begin{aligned}
y_0 &= x_0x_2 + x_1 + x_2 + x_3 \\
y_1 &= x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_0x_3 + x_2x_3 + x_0 + x_2 \\
y_2 &= x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_0 + x_1 + x_3 \\
y_3 &= x_0x_1x_2 + x_1x_3 + x_0 + x_1 + x_2 + 1.
\end{aligned}
$$

Algebraic degree of an Sbox

$$(y_0, y_1, y_2, y_3) = S(x_0, x_1, x_2, x_3)$$

$$\begin{aligned}
y_0 &= x_0x_2 + x_1 + x_2 + x_3 \\
y_1 &= x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_0x_3 + x_2x_3 + x_0 + x_2 \\
y_2 &= x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_0 + x_1 + x_3 \\
y_3 &= x_0x_1x_2 + x_1x_3 + x_0 + x_1 + x_2 + 1.
\end{aligned}$$

The algebraic degree of S is 3.

Propagation of the division property through an Sbox

- Let S be a permutation of $\mathbf{F}_2^n$ of algebraic degree d.
- Let X be a multiset having the division property $\mathcal{D}_k^n$.

Question: What is the division property of $Y = S(X)$?

- If $k = n$, then Y has the division property $\mathcal{D}_n^n$.

Proposition (Todo):

Y has the division property $\mathcal{D}^n_{\lceil \frac{k}{d} \rceil}$.

Example - MISTY S_7

MISTY's Sbox S_7 is a 7-bit Sbox of degree 3.

- The input set X has the property $\mathcal{D}_k^7$.
- The output set Y has the property $\mathcal{D}_{k'}^7$, with $k' = \lceil \frac{k}{3} \rceil$.

k	0	1	2	3	4	5	6	7
k'	0	1	1	1	2	2	2	7

Proof Sketch

Let the input set X have the division property $\mathcal{D}_k^n$. Then,

$$\bigoplus_{x \in X} x^u = 0, \text{ for all } u \in \mathbf{F}_2^n \text{ with } wt(u) < k.$$

Goal: Evaluate for which $v \in \mathbf{F}_2^n$, $\bigoplus_{x \in X} S(x)^v$ vanishes.

- If $\deg(S^v) < k$ then $\bigoplus_{x \in X} S(x)^v = 0$.
- If $\deg(S^v) \geq k$, $\bigoplus_{x \in X} S(x)^v$ is undetermined.

Obviously, $\deg(S^v) \leq wt(v) \times d$, so the sum becomes unknown if

$$wt(v) \times d \geq k.$$

An improvement idea

In the previous proof, the degree was bounded by

$$\deg(S^v) \leq wt(v) \times d$$

This bound is not tight!

The inverse permutation influences the degree

Let S be a permutation on $\mathbf{F}_2^n$.

Denote by $\delta_k(S)$ the max. degree of the product of k coordinates of S.

Theorem [B.–Canteaut 2013]. For any k and ℓ,

$$\delta_\ell(S) < n - k \text{ if and only if } \delta_k(S^{-1}) < n - \ell.$$

Getting a tighter result

Use the previous theorem to better estimate $\deg(S^v)$:

$$\deg(S^v) \leq \delta_{wt(v)}(S).$$

Then,

$$\delta_{wt(v)}(S) < k \text{ iff } \delta_{n-k}(S^{-1}) < n - wt(v).$$

By re-writing the second inequality we get

$$\delta_{wt(v)}(S) < k \text{ iff } wt(v) < n - \delta_{n-k}(S^{-1}).$$

The quantity $\bigoplus_{x \in X}(S^v)(x)$ becomes unknown when

$$wt(v) \geq n - \delta_{n-k}(S^{-1}).$$

So Y has the division property $\mathcal{D}^n_{n-\delta_{n-k}(S^{-1})}$.

Example - Back to MISTY S_7

MISTY's inverse Sbox S_7^{-1} is a 7-bit Sbox of degree 3.

k	1	2	3	4	5	6	7
$\delta_k(S_7^{-1})$	3	5	5	6	6	6	7

- The input set X has the property $\mathcal{D}_k^7$.
- The output set Y has the property $\mathcal{D}_{k'}^7$, with
  - $k' = \lceil \frac{k}{3} \rceil$ (Todo's estimation)
  - $k' = 7 - \delta_{7-k}(S_7^{-1})$ (our estimation)

k	0	1	2	3	4	5	6	7
k' (Todo's)	0	1	1	1	2	2	2	7
k' (our)	0	1	1	1	2	2	**4**	7

For $k = 6$: $k' = 7 - \delta_{7-6}(S_7^{-1}) = 7 - 3 = 4$

Outline

Reduced set of a multiset

Let X be a multiset of elements in $\mathbf{F}_2^n$.

The corresponding reduced set $\tilde{X}$ is the set composed of all elements in X having an odd multiplicity.

Example: If $X = \{\texttt{0x0}, \texttt{0x3}, \texttt{0x3}, \texttt{0x3}, \texttt{0x5}, \texttt{0x7}, \texttt{0x7}, \texttt{0xB}, \texttt{0xC}\}$ then

$$\tilde{X} = \{\texttt{0x0}, \texttt{0x3}, \texttt{0x5}, \texttt{0xB}, \texttt{0xC}\}.$$

A multiset X fulfills $\mathcal{D}_k^n$ if and only if $\tilde{X}$ fulfills $\mathcal{D}_k^n$.

Parity set of a multiset

Let X be a multiset of elements in $\mathbf{F}_2^n$. The set $\mathcal{U}(X)$ is the subset of $\mathbf{F}_2^n$ defined by

$$\mathcal{U}(X) = \{u \in \mathbf{F}_2^n : \bigoplus_{x \in X} x^u = 1\},$$

is called the parity set of X.

Obviously $\mathcal{U}(X) = \mathcal{U}(\widetilde{X})$.

The parity set provides a complete characterization of the reduced set of a multiset.

Incidence vector of $\mathcal{U}(X)$

Lemma. Let G be the $2^n \times 2^n$ binary matrix whose entries are indexed by n-bit vectors and defined by

$$G_{u,a} = a^u, \ a, u \in \mathbf{F}_2^n \ .$$

For any subset X of $\mathbf{F}_2^n$, the incidence vector of $\mathcal{U}(X)$ is equal to the product of G by the incidence vector of X.

An example ($n = 3$)

$$G = \begin{pmatrix} 0^0 & 1^0 & 2^0 & 3^0 & 4^0 & 5^0 & 6^0 & 7^0 \\ 0^1 & 1^1 & 2^1 & 3^1 & 4^1 & 5^1 & 6^1 & 7^1 \\ 0^2 & 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 \\ 0^3 & 1^3 & 2^3 & 3^3 & 4^3 & 5^3 & 6^3 & 7^3 \\ 0^4 & 1^4 & 2^4 & 3^4 & 4^4 & 5^4 & 6^4 & 7^4 \\ 0^5 & 1^5 & 2^5 & 3^5 & 4^5 & 5^5 & 6^5 & 7^5 \\ 0^6 & 1^6 & 2^6 & 3^6 & 4^6 & 5^6 & 6^6 & 7^6 \\ 0^7 & 1^7 & 2^7 & 3^7 & 4^7 & 5^7 & 6^7 & 7^7 \end{pmatrix}$$

An example ($n = 3$)

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

An example ($n = 3$)

$X = \{1, 3, 4\}$

$$\mathcal{U}(X) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$\mathcal{U}(X) = \{0, 2, 3, 4\}$.

Reed-Muller codes

$\mathbf{F}_2^m = \{z_0, \ldots, z_{2^m-1}\}$. Let $f : \mathbf{F}_2^m \to \mathbf{F}_2$. We define

$c_f = (f(z_0), \ldots, f(z_{2^m-1}))$.

The Reed-Muller code $RM(d, m)$ of order d and length 2^m is defined as

$$RM(d, m) := \{c_f : \deg(f) \leq d\}.$$

Correspondance of X and $\mathcal{U}(X)$

Corollary. For any subset U of $\mathbf{F}_2^n$, there exists a unique set $X \subset \mathbf{F}_2^n$ such that $\mathcal{U}(X) = U$.

Proof.

- The matrix G is a generator matrix of the Reed-Muller code of length 2^n and order n.
- Dimension of the code : $2^n \Rightarrow G$ is invertible.
- The mapping matching the incidence vector of a set X, v_X to the incidence vector of $\mathcal{U}(X)$ is an isomorphism of the set of 2^n vectors.

Parity set and the division property

Let E_k be a keyed permutation.

- The division property is a distinguishing property of the multiset $E_k(X)$ for a given choice of the input multiset X.
- We can now reformulate the division property $\mathcal{D}_k^n$ of $E_k(X)$ by a simple property of $\mathcal{U}(E_k(X))$. Indeed, $\mathcal{D}_k^n$ characterizes a multiset X by a lower bound on the weight of all elements in $\mathcal{U}(X)$.

Proposition. Let X be a multiset of elements in $\mathbf{F}_2^n$ and k be an integer $0 \leq k \leq n$. Then,the following assertions are equivalent:

(i) X fulfills the division property $\mathcal{D}_k^n$.

(ii)
$$\mathcal{U}(X) \subseteq \{u \in \mathbf{F}_2^n : wt(u) \geq k\} .$$

(iii) The incidence vector of the corresponding reduced set $\widetilde{X}$ belongs to the Reed-Muller code of length 2^n and order $(n-k)$.

Outline

Some specific values of k

Question: What can be said about a multiset X that verifies a property $\mathcal{D}_k^n$, for some value of k?

- The cases $\mathcal{D}_1^n$, $\mathcal{D}_2^n$, $\mathcal{D}_n^n$, have been characterized.
  - [Todo 2015], [Sun et al. 2015]
- The cases $\mathcal{D}_k^n$, for $k \neq \{1, 2, n\}$ had not been exploited before.
  - We provide some insight on these cases **here** by using the above introduced new vision and some well known properties of Reed-Muller codes.

The property $\mathcal{D}_1^n$

Let X be a multiset of elements in $\mathbf{F}_2^n$.

X fulfills $\mathcal{D}_1^n$ **if and only if** its cardinality is even.

Indeed,

- X has the property $\mathcal{D}_1^n$: For $u = (0, \ldots, 0) : \bigoplus_{x \in X} x^u = 0$

$$\Leftrightarrow \bigoplus_{x \in X} x_1^0 \ldots x_n^0 = \bigoplus_{x \in X} 1 = \#X \mod 2 = 0$$

- The inverse can be easily deduced.

The property $\mathcal{D}_2^n$

Let X be a multiset of elements in $\mathbf{F}_2^n$.

X fulfills $\mathcal{D}_2^n$ **if and only if** its cardinality is even and it has the Balance property.

Balance property: For any i, $1 \leq i \leq n$ $\bigoplus_{x \in X} x_i = 0$.

Indeed, if X has the property $\mathcal{D}_2^n$:

- $\bigoplus_{x \in X} x_1^0 \dots x_n^0 = 0 \Rightarrow X$ has even cardinality.
- For all u with $wt(u) = 1$:
  $\bigoplus_{x \in X} x^u = \bigoplus_{x \in X} x_1^0 \dots x_{i-1}^0 x_i^1 \dots x_n^0 = \bigoplus_{x \in X} x_i = 0$
  $\Rightarrow X$ has the Balance property.

The inverse is proven easily.

The property $\mathcal{D}_n^n$

Let X be a multiset of elements in $\mathbf{F}_2^n$.

X fulfills $\mathcal{D}_n^n$ **if and only if** its reduced set $\tilde{X}$ is either empty or equal to $\mathbf{F}_2^n$.

Let v be the incidence vector of $\tilde{X}$.

Proof. X satisfies $\mathcal{D}_n^n$ iff $v \in R(0, n)$. Thus, either v is the all-zero vector, i.e., $\widetilde{X}$ is empty or v is the all-one vector i.e. $\widetilde{X} = \mathbf{F}_2^n$.

The property $\mathcal{D}_{n-1}^n$

Let X be a multiset of elements in $\mathbf{F}_2^n$.

Proposition. X satisfies $\mathcal{D}_{n-1}^n$ **if and only if** $\tilde{X}$ is an (affine) subspace of dimension $(n-1)$.

Proof. X satisfies $\mathcal{D}_{n-1}^n$ iff $v \in R(1,n)$.
$R(1,n)$ consists of the incidence vectors of all (affine) hyperplanes of $\mathbf{F}_2$.
Then, this equivalently means that $\widetilde{X}$ is an (affine) hyperplane.

Example [Todo, Eurocrypt 2015]

For the multiset of elements of $\mathbf{F}_2^4$

$$X = \{\texttt{0x0}, \texttt{0x3}, \texttt{0x3}, \texttt{0x3}, \texttt{0x5}, \texttt{0x6}, \texttt{0x8}, \texttt{0xB}, \texttt{0xD}, \texttt{0xE}\},$$

the corresponding reduced set

$$\tilde{X} = \{\texttt{0x0}, \texttt{0x3}, \texttt{0x5}, \texttt{0x6}, \texttt{0x8}, \texttt{0xB}, \texttt{0xD}, \texttt{0xE}\}$$

is a linear subspace of dimension 3 spanned by $\{\texttt{0x3}, \texttt{0x5}, \texttt{0x8}\}$.

So, it can be directly deduced (**without computation**) that

X has the property $\mathcal{D}_3^4$.

The property $\mathcal{D}_k^n$

Proposition. Let X be a multiset of elements in $\mathbf{F}_2^n$ satisfying $\mathcal{D}_k^n$ such that $\widetilde{X}$ is not empty. Then

$$|\widetilde{X}| \geq 2^k \ ,$$

and equality holds iff $\widetilde{X}$ is an affine subspace of dimension k.

Proof. X satisfies $\mathcal{D}_k^n$ iff $v_{\widetilde{X}}$ belongs to $R(n-k,n)$. The minimum distance of $R(n-k,n)$ is 2^k and that the minimum-weight codewords in this code are the incidence vectors of the affine subspaces of dimension k.

Conclusion

- We have reformulated the division property to captivate more information.
- Complete characterisation of the property $\mathcal{D}_k^n$ for different values of k.
- More powerful distinguishers for a high number of block ciphers.
- Work in progress...

Conclusion

- We have reformulated the division property to captivate more information.
- Complete characterisation of the property $\mathcal{D}_k^n$ for different values of k.
- More powerful distinguishers for a high number of block ciphers.
- Work in progress...

Thanks for your attention!