Structural weaknesses of mappings with a low differential uniformity

Anne Canteaut and Maria Naya-Plasencia

INRIA Paris-Rocquencourt, France

Fq9, July 16, 2009

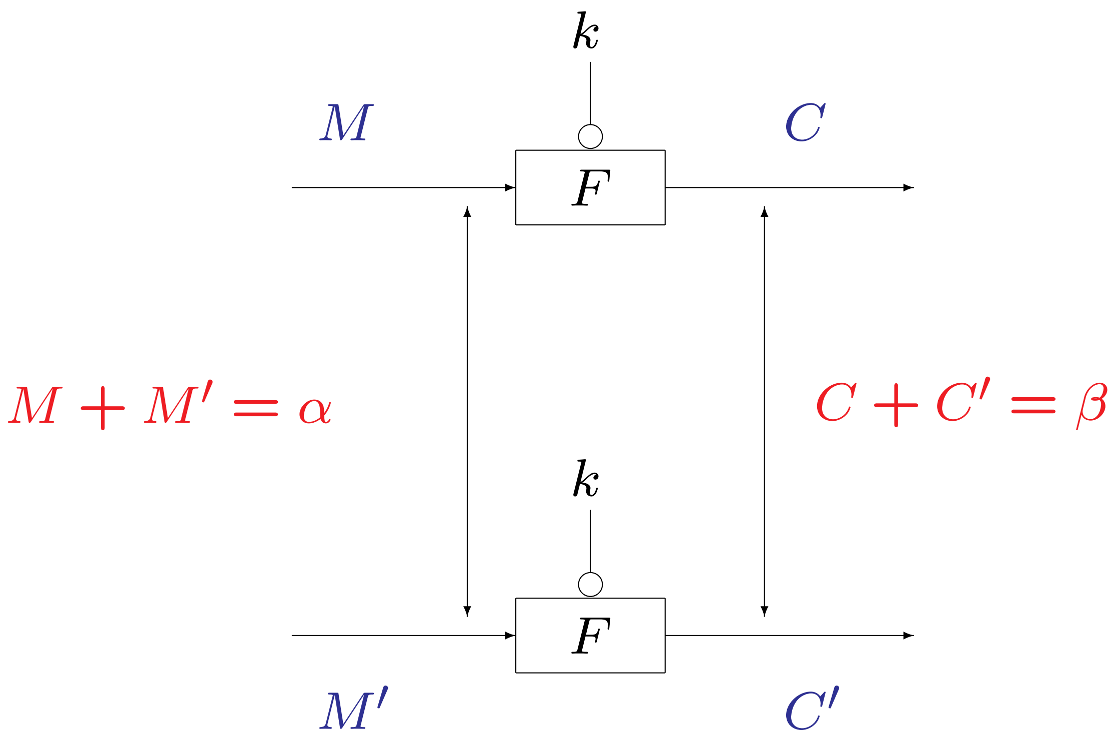
Outline

1. An (unsuitable) property of the permutations which guarantee a high resistance to differential cryptanalysis.

2. An attack on a new hash function proposal based on this property.

3. Impact of the algebraic structure of the image sets of the derivatives; link with crooked functions.

Differential cryptanalysis [Biham-Shamir 91]



Differential cryptanalysis exploits the existence of (α, β) such that

$$F(M + \alpha) + F(M) = \beta \text{ for many values of } M.$$

Differential uniformity of $F : \mathbf{F}_2^n \to \mathbf{F}_2^n$ [Nyberg 93]

$$\Delta(\alpha,\beta) = \#\{x \in \mathbf{F}_2^n,\ \ F(x+\alpha)+F(x)=\beta\}.$$

$\Delta_F = \max_{\alpha\neq 0,\beta} \Delta(\alpha,\beta)$ is the differential uniformity of F.

Proposition For any $F : \mathbf{F}_2^n \longrightarrow \mathbf{F}_2^n$,

$$\Delta_F \geq 2$$

and equality holds for APN (almost perfect nonlinear) functions.

When n is even and $n \geq 8$, no APN permutation of $\mathbf{F}_2^n$ is known.

$\longrightarrow$ permutations with $\Delta_F = 4$ are used,
e.g., $x \mapsto x^{2^n-2}$ over $\mathbf{F}_{2^n}$.

A related quantity

$$D(\beta) = \{\alpha \in \mathbf{F}_2^n, \ \ \exists x \in \mathbf{F}_2^n \text{ with } F(x+\alpha) + F(x) = \beta\}.$$

$$D_F = \max_{\beta \in \mathbf{F}_2^n} \#D(\beta).$$

Proposition Let F be a permutation of $\mathbf{F}_2^n$. Then, for any $\beta \in \mathbf{F}_2^n$,

$$\begin{aligned} D(\beta) &= \{\alpha \in \mathbf{F}_2^n, \ \ \exists x \in \mathbf{F}_2^n \text{ with } F(x+\alpha) + F(x) = \beta\} \\ &= \{F^{-1}(x+\beta) + F^{-1}(x), \ \ x \in \mathbf{F}_2^n\}. \end{aligned}$$

Link between D_F and Δ_F

Proposition For any nonzero $\beta \in \mathbf{F}_2^n$,

$$\#D(\beta) \geq \frac{2^n}{\Delta_F}$$

with equality if and only if all equations

$$F(x+\alpha) + F(x) = \beta,\ \alpha \neq 0$$

have either 0 or Δ_F solutions.

Corollaries.

- $D_F = \max_\beta \#D(\beta) = 1$ if and only if F has degree 1.
- If F is APN, then $\#D(\beta) = 2^{n-1}$ for all $\beta \neq 0$.

An attack against a hash function exploiting a high D_F

Cryptographic hash functions

$$H : \{0,1\}^* \longrightarrow \mathbf{F}_2^h, \text{ e.g. } h = 256, 512.$$

Collision resistance.

Find (x, x') such that $H(x) = H(x')$.

Generic algorithm: a set of $2^{\frac{h}{2}}$ random inputs contains a collision with probability more than $1/2$.

Security requirement: the generic algorithm must be the most efficient method for finding a collision.

Maraca [Jenkins Jr 08]

submitted to the SHA-3 competition (among 64 candidates).

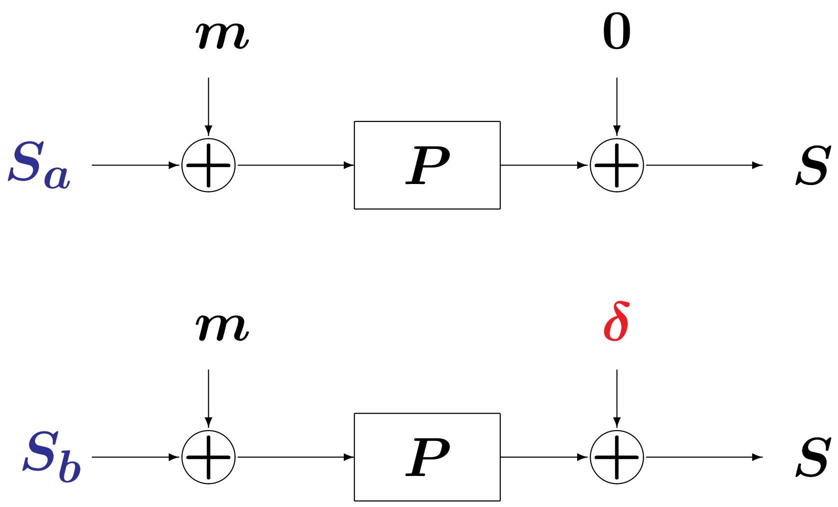
internal state: $\boldsymbol{n} = \mathbf{1024}$ bits

Underlying permutation P:

permutation of $\mathbf{F}_2^n$, concatenation of $\mathbf{128}$ copies of a quadratic permutation of $\mathbf{F_2^8}$.

Finding an internal collision for Maraca

Beginning of the last round.



where δ and m are fixed, but chosen by the attacker.

Internal collision:

$$P(S_a + m) = P(S_b + m) + \delta.$$

Finding an internal collision for Maraca (2)

Find (S_a, S_b) such that there exists $m \in \mathbf{F}_2^n$ satisfying

$$P(S_a + m) + P(S_b + m) = \delta.$$

or equivalently such that

$$S_a + S_b \in D(\delta),$$

since $D(\delta) = \{\alpha \in \mathbf{F}_2^n, \ \exists x \in \mathbf{F}_2^n \text{ with } F(x + \alpha) + F(x) = \delta\}$.

Data complexity:

$$N = \frac{2^{\frac{n}{2}}}{\sqrt{\#D(\delta)}} \text{ values of } S_a \text{ and } S_b.$$

Finding an internal collision for Maraca (3)

for N values of a **do**
  compute S_a.
end for
for N values of b **do**
  compute S_b.
end for
for all pairs (S_a, S_b) **do**
  if $S_a + S_b \in D(\delta)$ **then**
    find m such that $P(m + S_a + S_b) + P(m) = \delta$.
  end if
end for

Time complexity:

$$\frac{\log(\#D(\delta))}{\#D(\delta)} \times 2^n.$$

$\rightarrow$ faster than the generic algorithm if $D(\delta) > 2^{n-\frac{h}{2}}$.

If P is based on the inverse function

P: 128 copies of the inverse function π over $\mathbf{F}_{2^8}$.

$$D_\pi(\delta) = \{(x+\delta)^{-1} + x^{-1},\ \ x \in \mathbf{F}_{2^m}\}$$

For any nonzero $\delta \in \mathbf{F}_{2^m}$, $\#D_\pi(\delta) = 2^{m-1} - 1$.

For the parameters of Maraca:

$$\#D_P(\delta) = (2^7 - 1)^{128} = 2^{895}$$

leading to an attack with 2^{65} hash computations and time complexity 2^{146}.

For the original permutation used in Maraca

$$\max_{\delta} D_P(\delta) = (21)^{128} = 2^{461} < 2^{768}.$$

Problem: Can we find a faster method for determining all pairs (S_a, S_b) such that $S_a + S_b \in D(\delta)$?

$\longrightarrow$ use the algebraic structure of $D(\delta)$.

$D(\delta)$ is an affine subspace

$$D(\delta) = \{F^{-1}(x+\delta) + F^{-1}(x),\ \ x \in \mathbf{F}_2^n\}.$$

Suppose that $D(\delta) = \gamma + V$ where $\dim(V) = d$.

Decompose all S_a (resp. S_b) with respect to $V \times W$

Sort both lists according to $(S_a)_W$ (resp. $(S_b)_W$).

for all S_a **do**

determine whether there exists S_b in the list with $(S_b)_W = (S_a)_W + \gamma$.

end for

Time complexity:

$$2(n-d)2^{\frac{n-d}{2}}.$$

$\longrightarrow$ faster than the generic algorithm if $d > n - h$.

$D(\delta)$ is included in an (affine) subspace

Suppose that there is an (affine) subpace V such that $D(\delta) \subset V$.

Then, V can used for sieving the pairs (S_a, S_b).

For Maraca:

For π over $\mathbb{F}_2^8$, $D_\pi(\delta)$ is included in an affine subspace of dimension 5.

For P over $\mathbb{F}_2^{1024}$, $D_P(\delta)$ is included in an affine subspace of dimension 640.

$\longrightarrow$ attack with time complexity 2^{240}.

Examples of functions for which all $D(\delta)$ have a particular structure

$$D(\delta) = \{F^{-1}(x+\delta) + F^{-1}(x), \ \ x \in \mathbf{F}_2^n\}.$$

Inverse of a quadratic permutation:

If F^{-1} has degree 2, then $D(\delta)$ is an affine subspace for any δ.

Crooked functions [Bending, Fon-der-Flaas 98][Kyureghyan 07]:

F is crooked if for any nonzero δ, $\{F(x+\delta) + F(x), \ \ x \in \mathbf{F}_2^n\}$ is an (affine) hyperplane.

$\Rightarrow$ If F^{-1} is crooked, then $D(\delta)$ is an affine hyperplane for any nonzero δ.

Conjecture. All crooked functions are quadratic.
[Kyureghyan 07], [Bierbrauer, Kyureghyan 08]

Related problems

Open problem. Is there a permutation F with $\deg(F^{-1}) > 2$ such that $D(\delta)$ is an affine subspace for any nonzero δ?

Proposition For monomial permutations, $x \mapsto x^s$, these functions are exactly the inverses of the quadratic permutations.

Open problem. Characterize the permutations F over $\mathbf{F}_2^n$ such that, there exists an input difference $\delta \neq 0$ for which

$$\{F(x+\delta) + F(x),\ x \in \mathbf{F}_2^n\}$$

is a large affine subspace.

Conclusions

[Indesteege 09]: linear cryptanalysis of Maraca
$\Rightarrow$ "the weakness of Maraca is due to the use of a bad permutation regarding linear and differential attacks".

But:

- The functions which guarantee a good resistance to differential cryptanalysis may introduce unexpected weaknesses.
- The algebraic structure of $\boldsymbol{D(\delta)}$ may be relevant for the security.