Internal collision attack on Maraca

Anne Canteaut and Maria Naya-Plasencia

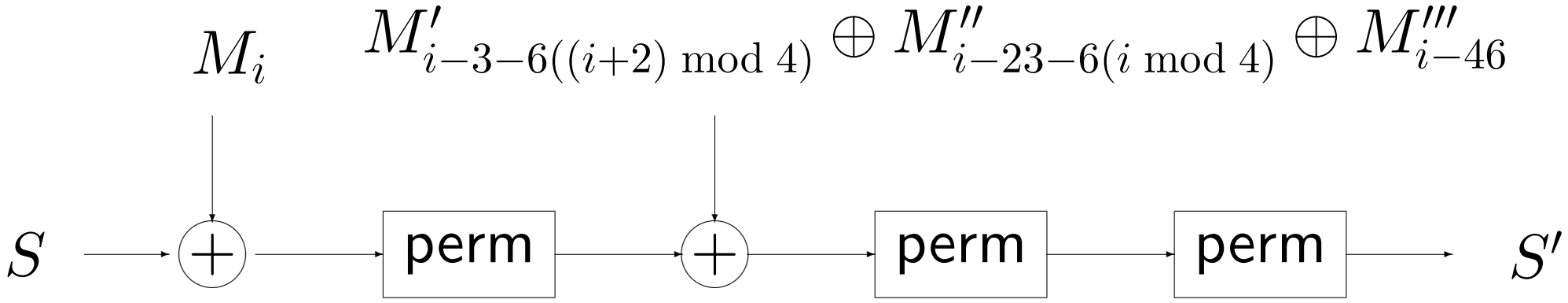
INRIA Paris-Rocquencourt
SECRET team (SEcurité, CRyptologie Et Transmissions)
Domaine de Voluceau
78153 Le Chesnay - France

Outline

Maraca [Jenkins 08]

- Keyed hash function submitted by Robert J. Jenkins Jr.
- Message padded with the key and length
- Internal state of 1024 bits
- Message blocks of 1024 bits used at 4 rounds (until 46 rounds later)
- h-bit digest: extracted from the internal state after 30 more iterations of perm.

Round function of Maraca



Permutation $perm$

- 128 parallel applications of an unique 8X8 bit permutation, P.
- First 3 output bits of P are linear. The others of higher degree.
- A constant is added.
- A bit permutation is applied (for mixing).

Differential property of $perm$

- We look at the 8X8 bit permutation P:

- One output difference β may be obtained from several input differences α, i.e.

  $D(\beta) = \{\alpha, \exists x, P(x \oplus \alpha) \oplus P(x) = \beta\}$ may contain several elements.

- Which output difference is associated to the highest number of input differences?

- There are 20 output differences β(Ox03, for example) associated to 21 input differentials, i.e. with $|D(\beta)| = 21$.

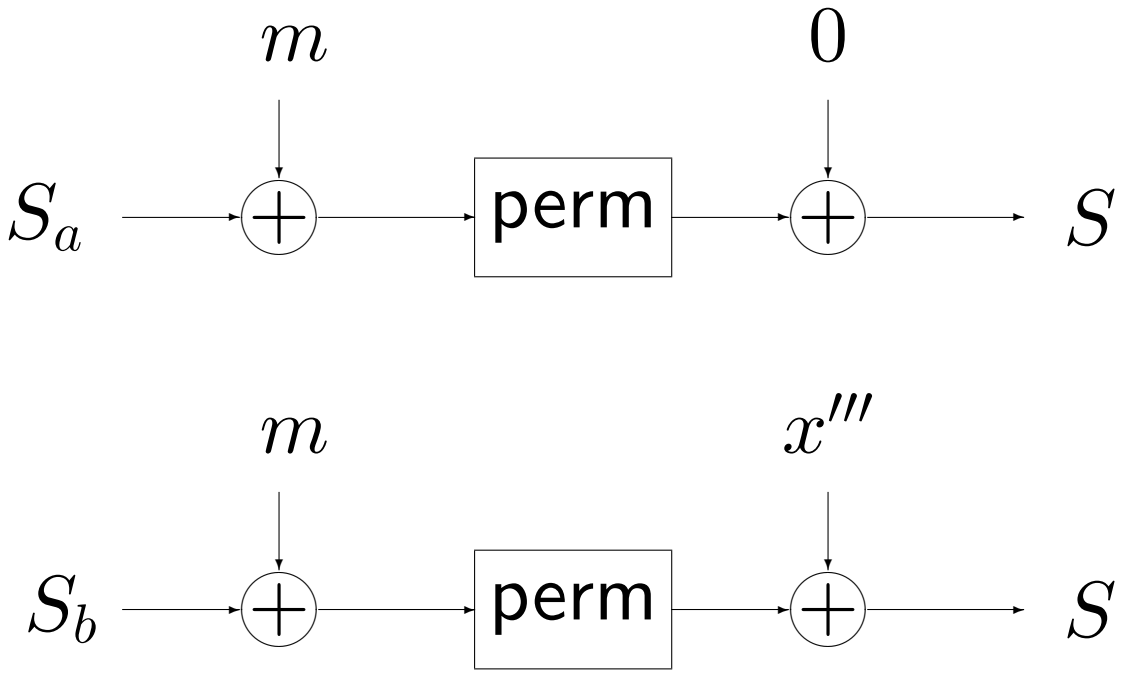
Internal collision attack on Maraca

We will use two sets of paded messages:

$$\mathcal{A} = \{M_a = (K, a, 0^{47}, m, pad), a \in \{0,1\}^{1024}\}$$

$$\mathcal{B} = \{M_b = (K, b, 0, x, 0^{45}, m, pad), b \in \{0,1\}^{1024}\}$$

Beginning of round 49.



Internal collision attack on Maraca

- x is chosen so that all 128 bytes of x''' corresponding to the outputs of P are equal to a β with $|D(\beta)| = 21$.

Let D be the set of input differences so that the output differential can be x'''.

- If $S_a \oplus S_b \in D$, then:
  there exists m such that

$$perm(m \oplus S_a) = perm(m \oplus S_b) \oplus x'''$$

  and it is easy to find it.

Data complexity

Which sizes N_a and N_b for the two sets of messages do we need to find a pair such that $S_a \oplus S_b \in D$?

- Probability of finding one favorable $(S_a, S_b) = (\frac{21}{256})^{128}$
- So we want $N_a \times N_b = (\frac{256}{21})^{128}$, that means:

$$N_a = N_b = 2^{230.5}.$$

Exploiting the algebraic structure of $D(\beta)$

- Using the fact that the 3 first output bits of P are linear enables us to make a sieving phase: we use that D is included in a 5×128-dimensional affine subspace.

- We compute and store the table of the N_a states S_a and the 128×3 output linear bits L_a for each of them.

- We compute S_b for each M_b and the 128×3 output linear bits L_b for each of them. We check wether $L_b \oplus (\beta)^{128}$ is in the table.

Exploiting the algebraic structure of $D(\beta)$

- Probability for one M_b of finding an M_a in the table matching for the linear part:

$$2^{230.5} \times 2^{-3\times 128} = 2^{-153.5}$$

- How many "linear matches" should we find for all the N_b messages M_b?

$$2^{230.5} \times 2^{-153.5} = 2^{77}$$

- Probability of finding (S_a, S_b) with $(S_a \oplus S_b) \in D$ once we have found the "linear match":

$$(\tfrac{21}{2^5})^{128} = 2^{-77}.$$

Final step

- Once we have found the pair of "sub-messages" M_a and M_b that gives us a desired input difference, we only have to pick up a value of m for which:

$$perm(m \oplus S_a) = perm(m \oplus S_b) \oplus x'''$$

and messages leading to colliding internal states have been found.

Time complexity

- Finding an internal collision in S means a collision at any step further and, so, on the hash value.

- Time complexity:
  2^{237} call to the round function.
  ($2^{261.5}$ for the generic attack)

- Memory complexity:
  $2^{230.5}$ bits.

$D(\beta)$ and link with differential cryptanalysis

- **Proposition 1.** *Let F be a permutation over $\mathbf{F_2^n}$. For any $\beta \in \mathbf{F_2^n}$ we have:*

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

- Let $\Delta_F = \max_{\alpha,\beta \in \mathbf{F}_2^n, n \neq 0} \Delta(\alpha, \beta)$ with

$$\Delta(\alpha, \beta) = |\{x \in \mathbf{F}_2^n, F(x \oplus \alpha) \oplus F(x) = \beta\}|,$$

a function with $\Delta_F = \Delta$ is said to be differentially Δ-uniform.

$D(\beta)$ and link with differential cryptanalysis

Theorem 1. *Let F be a permutation over $\mathbf{F_2^n}$. If F is differentially Δ-uniform, then, for any $\beta \in \mathbf{F_2^n}$, $\beta \neq 0$ we have*

$$|D(\beta)| \geq \frac{2^n}{\Delta}$$

Example: P the inverse function over $\mathbf{F}_{2^8}$

- Then:

  $|D_P(\beta)| = 2^{m-1} - 1$, with $m = 8$, and so
  $|D_{perm}| = |D_P(\beta)|^{128} = 2^{894.5}$.

- Our attack requires then $N_a = N_b = 2^{64.7}$.

- Complexity

  2^{146} operations.

  2^{76} bits of memory.

Conclusion

- When $h \geq 512$, better than the generic attack in the sense that we divide by a factor 2^{24} the number of calls to the round function.
- We find not only a collision attack, but an internal collision in 2^{237} calls to the round function instead of 2^{512}.
- The attack exploits some properties that are in contradiction with the usual security criterion for differential attacks.
- Attack acknowledged by the author (Maraca-512 is broken)