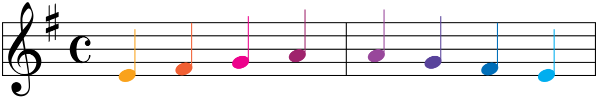
♫ Let's play music with MiMC ♫

Clémence Bouvier ♪,♫
joint work with Anne Canteaut♫ and Léo Perrin♫

♪Sorbonne Université, ♫Inria Paris, team COSMIQ

Rump session, EUROCRYPT, 2021



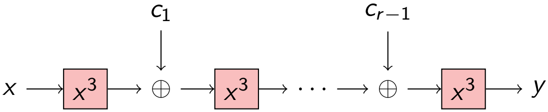
The block cipher MiMC

- Minimize the number of multiplications in a large finite field.
- Construction of MiMC [Albrecht et al., EC16]:
  - n-bit blocks (n odd ≈ 127)
  - n-bit key k
  - decryption : replacing x^3 by x^s where $s = (2^{n+1} - 1)/3$

$$x \longrightarrow \overset{k}{\oplus} \longrightarrow \boxed{x^3} \longrightarrow \overset{k \oplus c_1}{\oplus} \longrightarrow \boxed{x^3} \longrightarrow \cdots \longrightarrow \overset{k \oplus c_{r-1}}{\oplus} \longrightarrow \boxed{x^3} \longrightarrow \overset{k}{\oplus} \longrightarrow y$$

The block cipher MiMC

- Minimize the number of multiplications in a large finite field.
- Construction of MiMC [Albrecht et al., EC16]:
  - n-bit blocks (n odd ≈ 127)
  - n-bit key k
  - decryption : replacing x^3 by x^s where $s = (2^{n+1} - 1)/3$



Algebraic degree of MiMC

- Preliminary study: [Eichlseder et al., AC20]
- Our study: plateaus on the algebraic degree

Round 1 : deg $= 2$

$$\mathcal{P}_1(x) = x^3$$

$$3 = [11]_2$$

Round 2 : deg $= 2$

$$\mathcal{P}_2(x) = x^9 + c_1 x^6 + c_1^2 x^3 + c_1^3$$

$$9 = [1001]_2 \quad 6 = [110]_2 \quad 3 = [11]_2$$

Algebraic degree of MiMC

- Preliminary study: [Eichlseder et al., AC20]
- Our study: plateaus on the algebraic degree

Round 1 : deg = 2

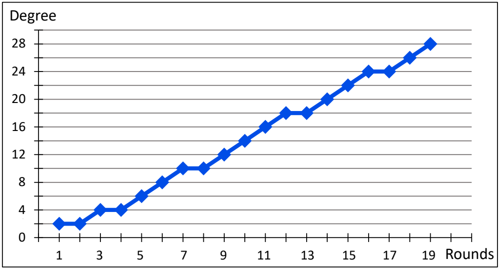
$$\mathcal{P}_1(x) = x^3$$

$$3 = [11]_2$$

Round 2 : deg = 2

$$\mathcal{P}_2(x) = x^9 + c_1 x^6 + c_1^2 x^3 + c_1^3$$

$$9 = [1001]_2 \quad 6 = [110]_2 \quad 3 = [11]_2$$



Bounding the degree

Proposition

Set of exponents that might appear in the polynomial :

$$\mathcal{E}_r = \{3j \bmod (2^n - 1) \text{ where } j \preceq i,\ i \in \mathcal{E}_{r-1}\}$$

No exponent $\equiv 5, 7 \bmod 8$ $\Rightarrow$ No exponent $2^{2k} - 1$

$$\mathcal{E}_r \subseteq \{ \begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & \cancel{5} & 6 & \cancel{7} \\ 8 & 9 & 10 & 11 & 12 & \cancel{13} & 14 & \cancel{15} \\ 16 & 17 & 18 & 19 & 20 & \cancel{21} & 22 & \cancel{23} \\ & & & & & & & \\ \dots & 3^r \} & & & & & & \end{array}$$

Exact degree

Maximum-weight exponents :

Let $k_r = \lfloor r \log_2 3 \rfloor$.

$\forall r \in \mathcal{R} = \{4, ..., 16265\} \backslash \mathcal{F}$
with $\mathcal{F} = \{465, 571, \ldots\}$:

- if k_r is odd,

$$2^{k_r} - 5 \in \mathcal{E}_r ,$$

- if k_r is even,

$$2^{k_r} - 7 \in \mathcal{E}_r .$$

$r-7$	$2^{2k-10}-7$
$r-6$	$2^{2k-9}-5$
$r-5$	$2^{2k-7}-5$
$r-4$	$2^{2k-6}-7$
$r-3$	$2^{2k-4}-7$
$r-2$	$2^{2k-3}-5$
$r-1$	$2^{2k-1}-5$
r	$2^{2k+1}-5$

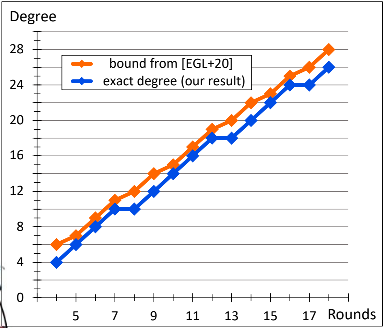
Constructing exponents.

$\Rightarrow$ plateau when k_r is odd and k_{r+1} is even

Integral Attacks

After r rounds of MIMC_3:

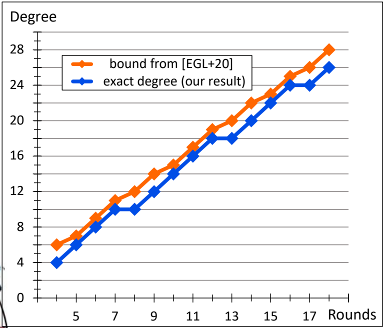
$$\deg = 2 \times \lceil k_r/2 - 1 \rceil \ .$$



Integral Attacks

After r rounds of MIMC_3:

$$\deg = 2 \times \lceil k_r/2 - 1 \rceil \ .$$



For $n = 129$, $\text{MIMC}_3 = 82$ rounds

Rounds	Time	Data	Source
80/82	2^{128}XOR	2^{128}	[EGL+20]
81/82	2^{128}XOR	2^{128}	New
80/82	2^{125}XOR	2^{125}	New

Secret-key distinguishers ($n = 129$)

Music in MiMC

- Patterns in sequence $(k_r)_{r>0}$:
  $\Rightarrow$ denominators of semiconvergents of $\log_2(3) \simeq 1.5849625$

$$\mathfrak{D} = \{1, 2, 3, 5, 7, 12, 17, 29, 41, 53, 94, 147, 200, 253, 306, 359, \ldots\},$$

$$\log_2(3) \simeq \frac{a}{b} \quad \Leftrightarrow \quad 2^a \simeq 3^b$$

- **Music theory:**
  - perfect octave 2:1
  - perfect fifth 3:2

$$2^{19} \simeq 3^{12} \quad \Leftrightarrow \quad 2^7 \simeq \left(\frac{3}{2}\right)^{12} \quad \Leftrightarrow \quad \text{7 octaves} \sim \text{12 fifths}$$

Thanks for your attention !

$$
\begin{tikzcd}[column sep=small]
 & k \arrow[d] & & k \oplus c_1 \arrow[d] & & k \oplus c_2 \arrow[d] & & & & k \oplus c_{r-1} \arrow[d] & & k \arrow[d] & \\
x \arrow[r] & \oplus \arrow[r] & \boxed{x^3} \arrow[r] & \oplus \arrow[r] & \boxed{x^3} \arrow[r] & \oplus \arrow[r] & \boxed{x^3} \arrow[r] & \cdots \arrow[r] & & \oplus \arrow[r] & \boxed{x^3} \arrow[r] & \oplus \arrow[r] & y
\end{tikzcd}
$$