Analyse de la sécurité de primitives symétriques dédiées à diverses techniques de preuve

Soutenance de Stage
Clémence Bouvier
stage encadré par Anne Canteaut et Léo Perrin

2 septembre 2020

Stage à l'INRIA

INRIA : Institut National de Recherche en Informatique et en Automatique
Équipe-projet **COSMIQ**
Stage encadré par Anne Canteaut et Léo Perrin

Plan

Analyse de la sécurité de primitives symétriques dédiées à diverses techniques de preuve

Usages émergents en cryptographie symétrique

Cryptographie symétrique :

- chiffrement à flots
- chiffrement par blocs : indistinguable d'une permutation aléatoire

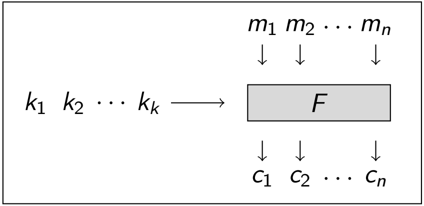


FIGURE – Chiffrement par blocs

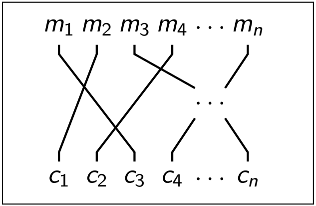


FIGURE – Permutation aléatoire

Usages émergents en cryptographie symétrique

Problématique : Analyser la sécurité de nouvelles primitives symétriques

Protocoles nécessitant de nouvelles primitives :

- calcul multi-partite (MPC)
- chiffrement homomorphe (FHE)
- systèmes de preuve à apport nul de connaissance (zk-SNARK, zk-STARK)

Déploiement de la Blockchain

Primitives conçues pour minimiser le nb de multiplications dans un corps fini
$\Rightarrow$ utilisation de fonctions non-linéaires sur un corps finis $\mathbb{F}_q$ de grande taille (tel que $\mathbb{F}_{2^n}$ où $n \sim 128$, ou des corps premiers)

Degré algébrique

Soit $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, il existe alors une **unique représentation polynomiale univariée** sur $\mathbb{F}_{2^n}$ de degré au plus $2^n - 1$:

$$F(x) = \sum_{i=0}^{2^n-1} b_i x^i ;\, b_i \in \mathbb{F}_2^n$$

Définition

Degré algébrique de $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$:

$$\deg(F) = \max\{wt(i),\ 0 \leq i < 2^n,\ \text{et}\ \ b_i \neq 0\}$$

Proposition [BC13]

Si $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ est une permutation, alors

$$\deg(F^{-1}) = n - 1 \iff \deg(F) = n - 1$$

Le chiffrement par bloc MiMC

Construction de MiMC [AGR+16] :

- blocs de n bits ($n \approx 127$)
- clé k de n bits
- déchiffrement : remplacer x^3 par x^s où $s = (2^{n+1} - 1)/3$

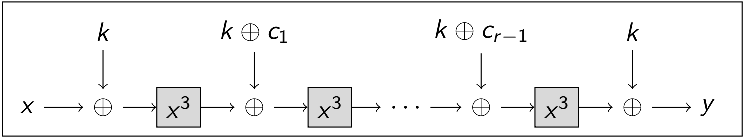


FIGURE – Chiffrement MiMC avec r tours

Analyser la sécurité du chiffrement : Cryptanalyse

$\Rightarrow$ Étudier l'évolution du **degré algébrique** de la transformation

Analyse de la sécurité

Un premier palier :

- Tour 1 : deg $= 2$

$$\mathcal{P}_1(x) = (x+k)^3 = x^3 + kx^2 + k^2x + k^3$$

$1 = [1]_2$ $2 = [10]_2$ $3 = [11]_2$

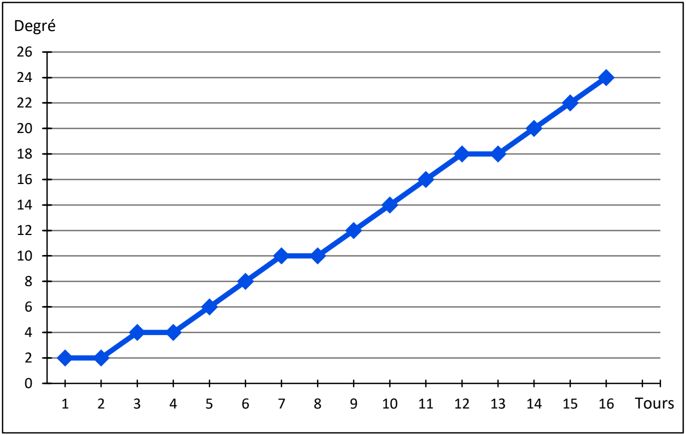
- Tour 2 : deg $= 2$

$$\begin{aligned}\mathcal{P}_2(x) &= ((x+k)^3 + k_1)^3 \\ &= x^9 + kx^8 + k_1x^6 + k^2k_1x^4 + k_1^2x^3 + (k^4k_1 + kk_1^2)x^2 \\ &+ (k^8 + k^2k_1^2)x + (k^3 + k_1)^3 \qquad \text{où } k_1 = k + c_1\end{aligned}$$

$1 = [1]_2$ $2 = [10]_2$ $3 = [11]_2$ $4 = [100]_2$ $6 = [110]_2$ $8 = [1000]_2$ $9 = [1001]_2$

Observation du degré algébrique de MiMC

FIGURE – Évolution du degré algébrique de la fonction de chiffrement (pgm Sage et C)



Étude du degré algébrique de MiMC

Proposition

Liste des exposants susceptibles d'apparaître dans le polynôme :

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

Si $3^r < 2^n - 1$:
borne max $= 2 \times \lfloor \log_2(3^r)/2 \rfloor$
borne min $= wt(3^r)$

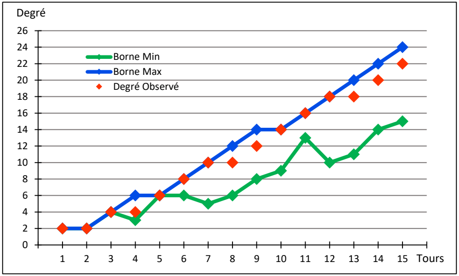


FIGURE – Comparaison du degré observé avec les bornes (pour $n = 25$)

Étude du degré algébrique de MiMC

Conjecture : Évolution du degré algébrique : $2 \times \lceil \lfloor \log_2(3^r) \rfloor / 2 - 1 \rceil$

Étude des monômes absents dans le polynôme :

- aucun exposant $\equiv 5, 7 \mod 8$ donc absence des exposants $2^{2k} - 1$
  Exemple $63 = 2^{2\times 3} - 1 \notin \mathcal{M}_4 = \{0, 3, \ldots, 81\}$
  $\Rightarrow deg < 6 = wt(63)$
- si $k = \lfloor \log_2(3^r) \rfloor$, pour tout $r > 4$, $2^{k+1} - 5 > 3^r$
  Exemple $\lfloor \log_2(3^8) \rfloor = 12$ et $3^8 = 6561 < 8187 = 2^{13} - 5$
  $\Rightarrow deg < 12 = wt(8187)$

Étude du degré algébrique de MiMC

Conjecture : Évolution du degré algébrique : $2 \times \lceil \lfloor \log_2(3^r) \rfloor /2 - 1 \rceil$

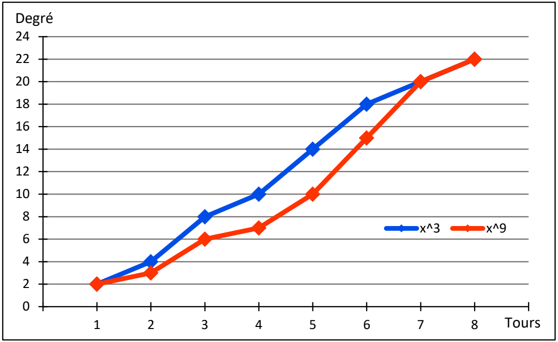
Étude des monômes d'exposant de poids maximal, présents dans le polynôme :

- $2^{2k-1} - 5$ et $2^{2k} - 7$ si $\lfloor \log_2(3^r) \rfloor = 2k$
  Exemple $27 = 2^{2\times 3 - 1} - 5, 57 = 2^{2\times 3} - 7 \in \mathcal{M}_4 = \{0, 3, \ldots, 81\}$
  $\Rightarrow deg = 4 = wt(27) = wt(57)$
- $2^{2k+1} - 5$ si $\lfloor \log_2(3^r) \rfloor = 2k + 1$
  Exemple $123 = 2^{2\times 3+1} - 5 \in \mathcal{M}_5 = \{0, 3, \ldots, 243\}$
  $\Rightarrow deg = 6 = wt(123)$

$\boxed{\Rightarrow \text{palier lorsque } \lfloor \log_2(3^r) \rfloor = 2k - 1 \text{ et } \lfloor \log_2(3^{r+1}) \rfloor = 2k}$

Forme des coefficients

FIGURE – Comparaison du degré algébrique pour les tours r de MiMC avec x^9 et pour les tours $2r$ de MiMC avec x^3 ($n = 23$)

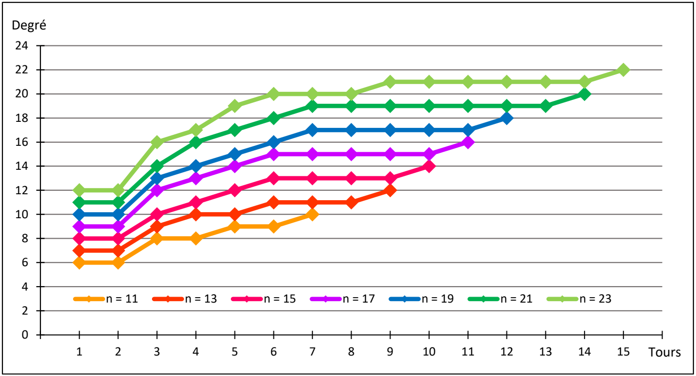


Exemple : coefficients des monômes d'exposant de poids maximal au tour 4

$$27 : c_1^{18} + c_3^2 \quad 30 : c_1^{17} \quad 51 : c_1^{10} \quad 54 : c_1^9 + c_3 \quad 57 : c_1^8 \quad 75 : c_1^2 \quad 78 : c_1$$

Étude la transformation inverse

FIGURE – Évolution du degré algébrique de la fonction de déchiffrement



Fonction inverse : $F : x \mapsto x^s, s = (2^{n+1} - 1)/3$

Quelques pistes étudiées

$s = (2^{n+1} - 1)/3 = [101..01]_2$

- Palier entre les tours 1 et 2
  - Tour 1 : $deg = wt(s) = (n+1)/2$
  - Tour 2 : $deg = \max\{wt(js),\ \text{pour } j \preceq s\} = (n+1)/2$

Proposition

pour $j \preceq s$ tel que $wt(j) \geq 2$:

$$wt(js) \in \begin{cases} [wt(j) - 1, (n-1)/2] & \text{si} \quad wt(j) \equiv 2 \mod 3 \\ [wt(j), (n+1)/2] & \text{sinon} \end{cases}$$

Quelques pistes étudiées

$s = (2^{n+1} - 1)/3 = [101..01]_2$

- Palier entre les tours 1 et 2
  - Tour 1 : $deg = wt(s) = (n+1)/2$
  - Tour 2 : $deg = \max\{wt(js),\ \text{pour } j \preceq s\} = (n+1)/2$

Proposition

pour $j \preceq s$ tel que $wt(j) \geq 2$:

$$wt(js) \in \begin{cases} [wt(j) - 1, (n-1)/2] & \text{si} \quad wt(j) \equiv 2 \mod 3 \\ [wt(j), (n+1)/2] & \text{sinon} \end{cases}$$

- Comportement sur les tours suivants :
  Conjecture : si $2 \leq j \leq 2^n - 2$ on a

$$wt(js) \in \begin{cases} [k, (n+2k-3)/2] & \text{si} \quad wt(j) = 2k \\ [k+2, (n+2k+1)/2] & \text{si} \quad wt(j) = 2k+1 \end{cases}$$

Autres permutations

Autres permutations avec un palier entre les tours 1 et 2 :

Proposition

Soit $F : \mathbb{F}_2^n \to \mathbb{F}_2^n, x \mapsto x^d$ où $d = 2^k - 1$. Si $d^2 < 2^n - 1$, alors :

$$deg((x^d + c)^d) = deg(x^d) \quad \text{où } c \text{ est une constante}$$

Mais pas de palier entre les tours 1 et 2 pour l'inverse de ces permutations !

Exemple (dans $\mathbb{F}_{2^{11}}$)

- chiffrement : $15 = 2^4 - 1 \Rightarrow$ palier
- déchiffrement : $15^{-1} = 273$ donc
  - degré algébrique au tour 1 : $3 = wt(273)$
  - degré algébrique au tour 2 : $5 = wt(273 \times 273 \mod 2^n - 1)$

Conclusion

Bilan du stage

- paliers dans l'évolution du degré de la fonction de chiffrement MiMC

$$2 \times \lceil \lfloor \log_2(3^r) \rfloor / 2 - 1 \rceil$$

- transformation inverse
  - palier entre les tours 1 et 2
  - tours suivants ?

Conclusion

Bilan du stage

- paliers dans l'évolution du degré de la fonction de chiffrement MiMC

$$2 \times \lceil \lfloor \log_2(3^r) \rfloor / 2 - 1 \rceil$$

- transformation inverse
  - palier entre les tours 1 et 2
  - tours suivants ?

Perspectives

Thèse à l'INRIA sous la direction d'Anne Canteaut et Léo Perrin

- structure algébrique univariée simple
  - étudier l'impact sur la résistance aux attaques classiques
  - rechercher de nouvelles techniques d'attaques
- primitive définie sur un corps premier

Merci pour votre attention