Propriétés « de base » des fonctions quadratiques aléatoires

Charles Bouillaguet

22 avril 2025

Plan

Plan

Plan

Fonctions quadratiques

Définition

- Corps fini $\mathbb{F}_q$
  - Choix courants : $q \in \{2, 16, 31, 256\}$
- Générer aléatoirement m polynômes quadratique en n variables (un polynôme $\approx n^2$ coefficients sur $\mathbb{F}_q$)
- Évaluer les polynômes sur l'entrée x
  x : vecteur de taille n sur $\mathbb{F}_q$

$$f_1(x) = x_1 + x_1x_3 + x_2x_3 + x_2x_4 + x_3 + x_3x_4 + 1$$
$$f_2(x) = x_1 + x_1x_2 + x_1x_3 + x_2 + x_2x_4 + x_3 + x_4 + 1$$
$$f_3(x) = x_1x_2 + x_1x_4 + x_2x_3 + x_2x_4 + x_3 + x_3x_4 + x_4$$
$$f_4(x) = x_1x_2 + x_1x_3 + x_2 + x_2x_3 + x_3x_4$$

Fonctions quadratiques

$F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ est une **fonction quadratique** si $\mathbf{y} = F(\mathbf{x})$ signifie :

$$\mathbf{y}_1 = \sum_{i=1}^{n}\sum_{j=1}^{n} A_{ij}[1]\mathbf{x}_i\mathbf{x}_j + \sum_{i=1}^{n} b_i[1]\mathbf{x}_i + c[1]$$

$$\mathbf{y}_2 = \sum_{i=1}^{n}\sum_{j=1}^{n} A_{ij}[2]\mathbf{x}_i\mathbf{x}_j + \sum_{i=1}^{n} b_i[2]\mathbf{x}_i + c[2]$$

$$\vdots$$

$$\mathbf{y}_m = \sum_{i=1}^{n}\sum_{j=1}^{n} A_{ij}[m]\mathbf{x}_i\mathbf{x}_j + \sum_{i=1}^{n} b_i[m]\mathbf{x}_i + c[m]$$

Fonctions quadratiques

$F : \mathbb{K}^n \to \mathbb{K}^m$ est une **fonction quadratique** si $\mathbf{y} = F(\mathbf{x})$ signifie :

$$
\begin{aligned}
\mathbf{y}_1 &= {}^t\mathbf{x}A[1]\mathbf{x} + \mathbf{b}[1]\mathbf{x} + c[1] \\
\mathbf{y}_2 &= {}^t\mathbf{x}A[2]\mathbf{x} + \mathbf{b}[2]\mathbf{x} + c[2] \\
&\vdots \\
\mathbf{y}_m &= {}^t\mathbf{x}A[m]\mathbf{x} + \mathbf{b}[m]\mathbf{x} + c[m]
\end{aligned}
$$

Fonctions quadratiques : facilité d'implantation

- m polynômes quadratiques en n variables modulo 2

```
for (int k = 0; k < m; k++) {
    y[k] = 0;
    for (int i = 0; i < n; i++)
        for (int j = i; j < n; j++)
            y[k] ^= a[k][i][j] & x[i] & x[j];
}
```

- « Stupid simple » 😘
- $\mathcal{O}\left(mn^2\right)$ opérations
- Des instructions SIMD peuvent servir
  - Tous les polynômes en parallèle
- PAS de grands entiers, exponentiation rapide, groupes cycliques, groupe de classe, corps quadratiques qui n'existent que dans l'imaginaire de certains farfelus, etc.

Systèmes polynomiaux : difficulté supposée

$$
\begin{aligned}
f_1(x) &= x_1 + x_1x_3 + x_2x_3 + x_2x_4 + x_3 + x_3x_4 + 1 \\
f_2(x) &= x_1 + x_1x_2 + x_1x_3 + x_2 + x_2x_4 + x_3 + x_4 + 1 \\
f_3(x) &= x_1x_2 + x_1x_4 + x_2x_3 + x_2x_4 + x_3 + x_3x_4 + x_4 \\
f_4(x) &= x_1x_2 + x_1x_3 + x_2 + x_2x_3 + x_3x_4
\end{aligned}
$$

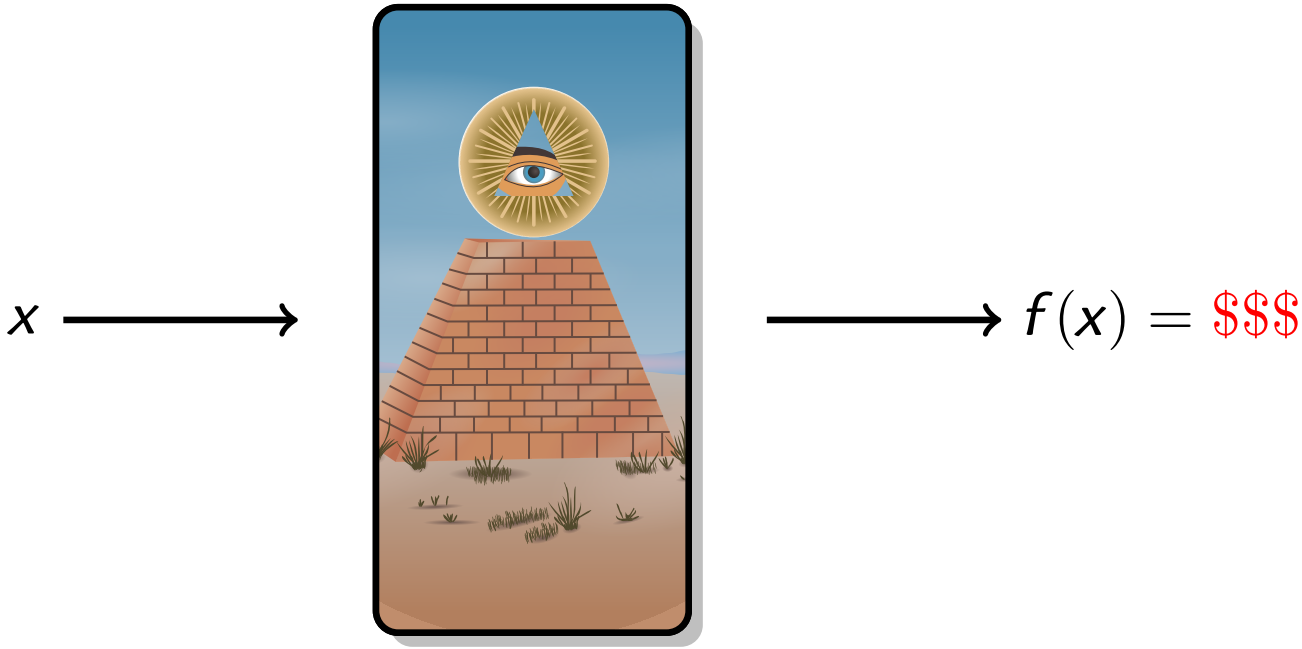
Sens-unique

- Résoudre le système est **NP-dur** sur n'importe quel $\mathbb{F}_q$
- Tous les algos connus sont exponentiels (en m)
  - Recherche exhaustive : q^m
  - Bases de Gröbner (F5) : $2^{4.3n}$ si $m \leq n$ (moins sinon)
- Intuition : les systèmes aléatoires sont durs
  - Pas de preuve

Plan

Fonctions aléatoires

- Une fonction $\{0,1\}^n \to \{0,1\}^m$...
- ... qui renvoie des chaînes de bits aléatoires



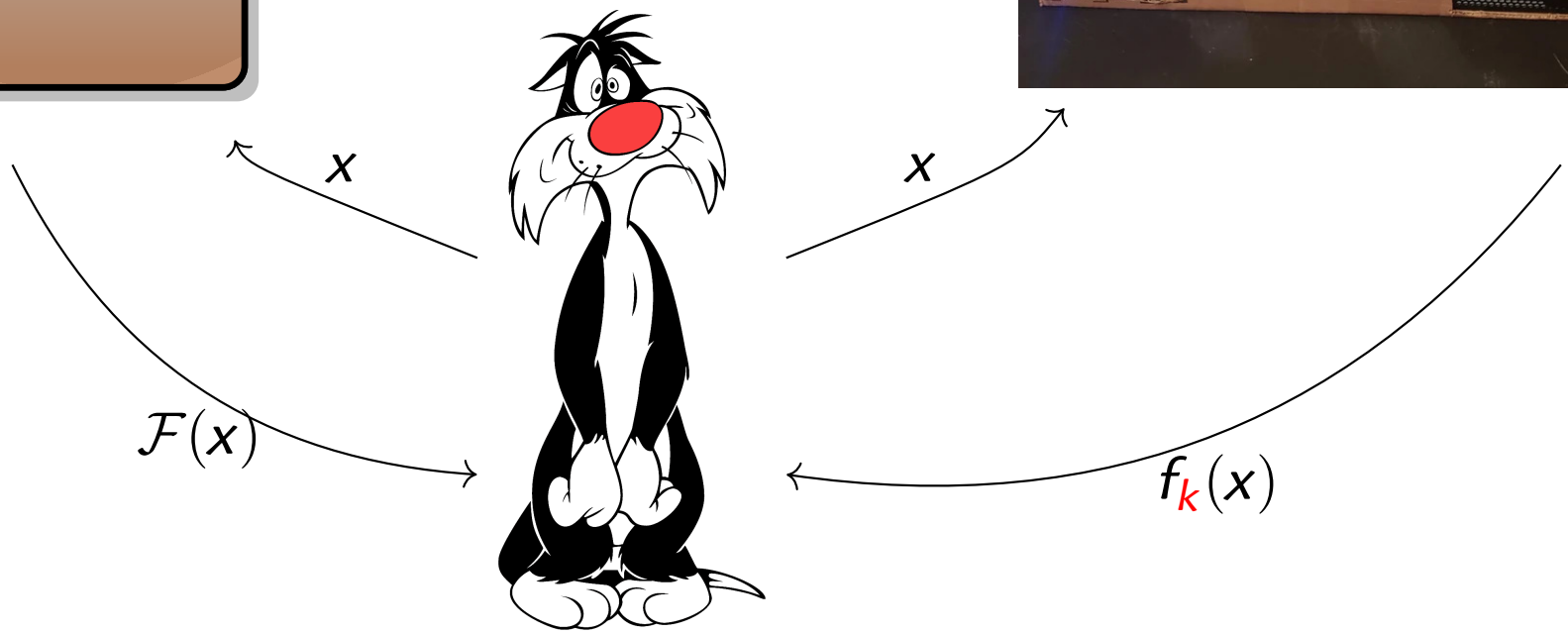
Fonction aléatoire $\{0,1\}^3 \to \{0,1\}^{32}$

x	$f(x)$
000	0110 1001 0000 1111 1101 1110 1110 0001
001	0011 1101 0001 0101 1111 1100 1010 0111
010	0000 1000 1000 0000 0000 1100 1001 1110
011	0010 0000 0011 1010 0010 1011 0011 1011
100	1010 0110 0100 0100 0100 1010 1100 1110
101	0000 1001 1111 0110 1111 0111 0011 1100
110	1010 0011 1110 1100 1011 1110 1010 1001
111	1011 0010 0111 0111 0010 0110 1110 1000

- Obtenue en tirant $2^3 \times 32$ bits aléatoires
  - Chaque sortie est tirée au hasard
  - $\{0,1\}^n \to \{0,1\}^m \rightsquigarrow 2^n$ sorties de m bits
  - 2^{m2^n} fonctions différentes possibles

Fonction aléatoire

PRF



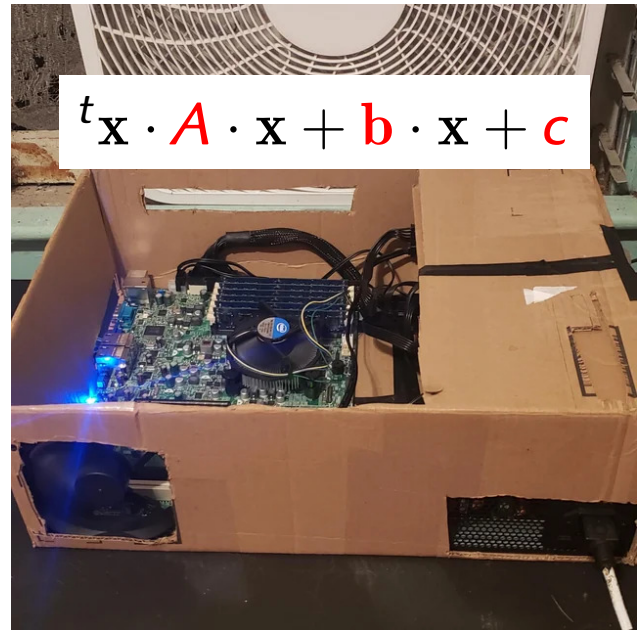
La question que je voudrais discuter 🤔

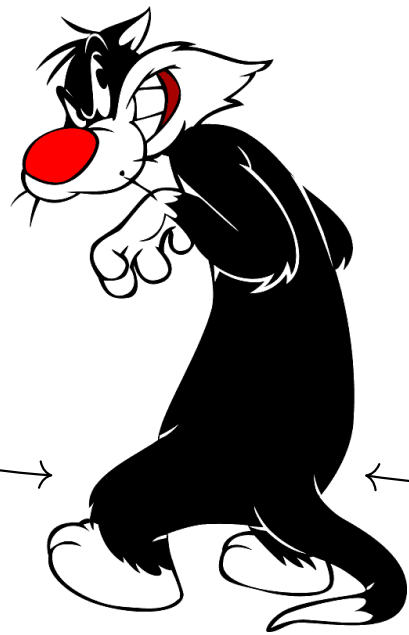
Peut-on utiliser une fonction quadratique à la place d'une fonction aléatoire ?

fonction aléatoire

fonction quadratique

$A, \mathbf{b}, c$





x

x

$\mathcal{F}(x)$

$f_{A,\mathbf{b},c}(x)$

Distingueurs faciles

8 requêtes suffisent pour distinguer

- $f(\mathbf{x}) = {}^t\mathbf{x}A\mathbf{x} + \mathbf{b}\mathbf{x} + c$
- On a

$$f(\mathbf{x}+\mathbf{y}+\mathbf{z}) = f(\mathbf{x}+\mathbf{y})+f(\mathbf{x}+\mathbf{z})+f(\mathbf{y}+\mathbf{z})-f(\mathbf{x})-f(\mathbf{y})-f(\mathbf{z})+f(0)$$

Pas une PRF sûre, mais alors pas **DU TOUT**... 😬

- 1 requête aléatoire $\rightsquigarrow$ 1 équation linéaire en $A, \mathbf{b}, c$

$\Rightarrow$ $\approx n^2 + n + 1$ requêtes permettent d'interpoler $A, \mathbf{b}, c$

Des fonctions quadratiques (aléatoires) au lieu de fonctions aléatoires ?

En général, ça ne marche pas

- Merci d'avoir suivi cet exposé ! 😋

Des fonctions quadratiques (aléatoires) au lieu de fonctions aléatoires ?

En général, ça ne marche pas

- Merci d'avoir suivi cet exposé ! 😋

Cependant, les fonctions quadratiques sont...

1. Des fonctions de hachage universelles
2. Des générateurs pseudo-aléatoires

Et ça, c'est parfois suffisant.

Plan

Plan

Approche

Fonctions quadratiques

$F : \mathbb{F}_q^n \to \mathbb{F}_q^m$:

$$
\begin{aligned}
&{}^t\mathbf{x}A[1]\mathbf{x} + \mathbf{b}[1]\mathbf{x} + c[1] \\
&{}^t\mathbf{x}A[2]\mathbf{x} + \mathbf{b}[2]\mathbf{x} + c[2] \\
&\vdots \\
&{}^t\mathbf{x}A[m]\mathbf{x} + \mathbf{b}[m]\mathbf{x} + c[m]
\end{aligned}
$$

- Tirer F au hasard
  - C.a.d. choisir les coefficients de $A, \mathbf{b}, c$ uniformément dans $\mathbb{F}_q$
- Évaluer $F(\mathbf{x})$ $\rightsquigarrow$ on obtient un vecteur aléatoire dans $\mathbb{F}_q^m$
  - À cause des coefficients constants aléatoires (c)

Approche

Fonctions quadratiques

$F : \mathbb{F}_q^n \to \mathbb{F}_q^m$:

$$
\begin{aligned}
&{}^t\mathbf{x}A[1]\mathbf{x} + \mathbf{b}[1]\mathbf{x} + c[1] \\
&{}^t\mathbf{x}A[2]\mathbf{x} + \mathbf{b}[2]\mathbf{x} + c[2] \\
&\vdots \\
&{}^t\mathbf{x}A[m]\mathbf{x} + \mathbf{b}[m]\mathbf{x} + c[m]
\end{aligned}
$$

- Tirer F au hasard
  - C.a.d. choisir les coefficients de $A, \mathbf{b}, c$ uniformément dans $\mathbb{F}_q$
- Évaluer $F(\mathbf{x})$ $\rightsquigarrow$ on obtient un vecteur aléatoire dans $\mathbb{F}_q^m$
  - À cause des coefficients constants aléatoires (c)
- Évaluer $F(\mathbf{y})$ $\rightsquigarrow$ on obtient... quoi ?

Universal Classes of Hash Functions

J. Lawrence Carter et Mark N. Wegman (J. Comp. and Sys. Sciences, 1979)

Soit $\mathcal{H}$ une famille de fonctions de $A \to B$ telle que

i) il est facile de sélectionner $f \xleftarrow{\$} \mathcal{H}$

ii) il est facile d'évaluer $f(x)$

Famille de fonctions de hachage universelle

iii) Pour tout $x \neq y \in A$,

$$\Pr[f(x) = f(y)] = \frac{1}{|B|}$$ (sur le choix aléatoire de f)

Famille de fonctions de hachage fortement universelle

iii) pour tout $x \neq y \in A$ et tous $u, v \in B$,

$$\Pr[f(x) = u \wedge f(y) = v] = \frac{1}{|B|^2}$$ (sur le choix aléatoire de f)

Fonctions de hachage (fortement) universelles (suite)

Classique : les fonctions affines sont fortement universelles

$$\begin{array}{rccc} H_{a,b} : & \mathbb{F}_q & \to & \mathbb{F}_q \\ & x & \mapsto & ax + \mathbf{b} \end{array}$$

Theorem

Les fonctions quadratiques sont fortement universelles.

Démonstration (grandes lignes).

- $f = {}^{x}Ax + \mathbf{b}x + c$, avec $f(\mathbf{x}) = u$ et $f(\mathbf{y}) = v$
- Il y a un indice i tel que $x_i \neq y_i$
- c et b_i sont fixés de manière unique par tout le reste
- Tout le reste peut être choisi librement

□

Plan

Régularité

Soit $\mathcal{H}$ est une famille de fonctions de hachage fortement universelle $A \to B$ et soit $u \in B$ arbitraire.
On note $N_a(f)$ le nombre d'antécédents de a par f, c.a.d. $\left|f^{-1}(a)\right|$.

Alors pour $h \xleftarrow{\$} \mathcal{H}$:

$$\begin{array}{rrcl} i) & \mathrm{E}\, N_u(h) & = & |A|/|B| \\ ii) & \mathrm{Var}\, N_u(h) & = & |A|/|B| \end{array}$$

Démonstration

- Pour tout $x \in A$, considérons l'évènement $[h(x) = u]$.
- Loi de Bernoulli de paramètre $1/|B|$
- fortement universel $\mapsto [h(x) = u]$ et $[h(y) = u]$ sont deux-à-deux indépendants
- $N_u(h) = \sum_{x \in A} [h(x) = u]$
- Linéarité de l'espérance permet de conclure pour $i)$
- Indépendance deux-à-deux permet de conclure pour $ii)$

Phase Transition of Multivariate Polynomial Systems

Giordano Fusco et Eric Bach (TAMC 2007)

Résultat (asymptotique) plus précis

- q premier
- $f : \mathbb{Z}_q^n \to \mathbb{Z}_q^{n+\alpha}$ de degré $d \geq 2$
- $n \to +\infty$
- $N_u(f)$ tend vers une **loi de poisson** de paramètre $q^{-\alpha}$

Autrement dit :

- $N_u(f) = 0$ (pas de solution) avec probabilité $\approx e^{-q^{-\alpha}}$
- $N_u(f) = s$ avec proba qui tend vers $\lambda^s e^{-\lambda}/s!$ avec $\lambda = q^{-\alpha}$

Injectivité / survectivité

Soit $\mathcal{H}$ est une famille de fonctions de hachage fortement universelle $A \to B$. Et $h \xleftarrow{\$} \mathcal{H}$.

i) h est injective avec probabilité au moins 1 - $|A|^2/|B|$

ii) h est surjective avec probabilité au moins 1 - $|B|^2/|A|$

Preuve (injectivité)

- h pas injective $\iff \exists x \neq y.\, h(x) = h(y)$. Et alors :

$$\begin{aligned} \Pr[\exists x \neq y.\, h(x) = h(y)] &\leq \sum_{x \neq y} \Pr[h(x) = h(y)] && \text{(Boole)} \\ &\leq \sum_{x \neq y} 1/|B| && \text{(universel)} \\ &\leq |A|^2/|B| \end{aligned}$$

Injectivité / survectivité (suite)

Soit $\mathcal{H}$ est une famille de fonctions de hachage fortement universelle $A \to B$. Et $h \xleftarrow{\$} \mathcal{H}$.

i) h est injective avec probabilité au moins 1 - $|A|^2/|B|$

ii) h est surjective avec probabilité au moins 1 - $|B|^2/|A|$

Preuve (surjectivité)

- Inégalité du 2ème moment : $\Pr[X > 0] \geq (\mathrm{E}\, X)^2/(\mathrm{E}\, X^2)$
  - $\Pr[X = 0] \leq 1 - (\mathrm{E}\, X)^2/(\mathrm{E}\, X^2)$
  - $\mathrm{E}\, X^2 = \mathrm{Var}\, X + (\mathrm{E}\, X)^2$:
  - $\Pr[X = 0] \leq \mathrm{Var}\, X/(\mathrm{Var}\, X + (\mathrm{E}\, X)^2) \leq \mathrm{Var}\, X/(\mathrm{E}\, X)^2$
- h pas surjective $\iff \exists u \in B.\ N_u(h) = 0$. Et alors :

$$\Pr[\exists u \in B.\ N_u(h) = 0] \leq \sum_{u \in B} \Pr[N_u(h) = 0] \qquad \text{(Boole)}$$

$$\leq \sum_{u \in B} |B|/|A| = |B|^2/|A|$$

Injectivité / survectivité (fin)

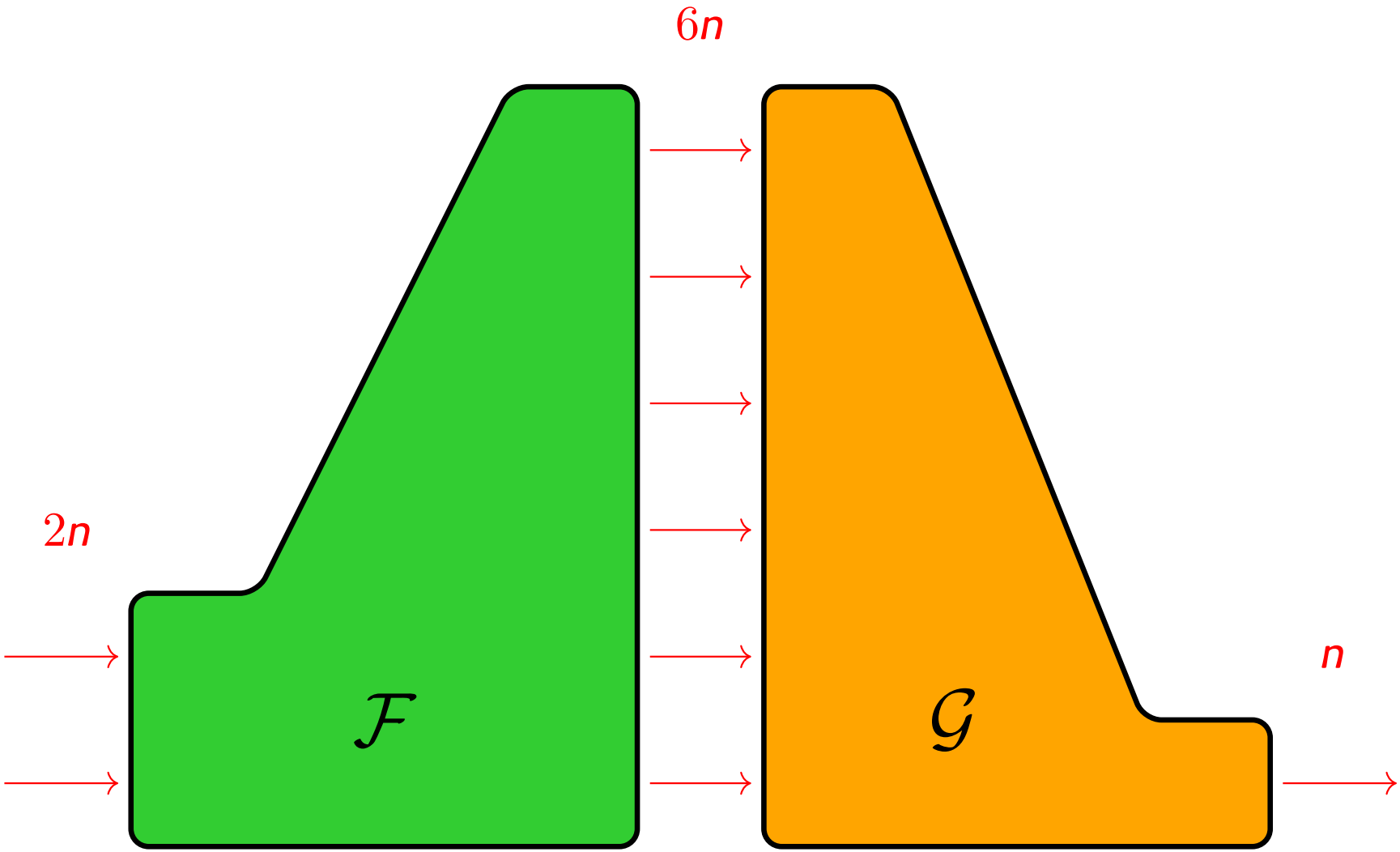
Conclusion

Si on tire au hasard une fonction quadratique $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$

- Si $m \gg 2n$ (expansive), alors elle est sûrement injective
- Si $n \gg 2m$ (contractante), alors elle est sûrement surjective

On Building Hash Functions from Multivariate Quadratic Equations

Olivier Billet, Matt Robshaw et Thomas Peyrin (ACISP 2007)



Injectivité / survectivité (fin)

Conclusion

Si on tire au hasard une fonction quadratique $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$

- Si $m \gg 2n$ (expansive), alors elle est sûrement injective
- Si $n \gg 2m$ (contractante), alors elle est sûrement surjective

Question subsidiaire

Si on nous donne (les coefficients de) $\mathcal{F}$, peut-on tester si elle est injective / surjective ?

Injectivité / survectivité (fin)

Conclusion

Si on tire au hasard une fonction quadratique $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$

- Si $m \gg 2n$ (expansive), alors elle est sûrement injective
- Si $n \gg 2m$ (contractante), alors elle est sûrement surjective

Question subsidiaire

Si on nous donne (les coefficients de) $\mathcal{F}$, peut-on tester si elle est injective / surjective ?

Theorème (inédit)

Le problème suivant est **NP-complet** :

- En entrée : les coefficients d'une fonction quadratique $\mathcal{F}$
- Existe-t-il $\mathbf{x} \neq \mathbf{y}$ tels que $\mathcal{F}(\mathbf{x}) = \mathcal{F}(\mathbf{y})$?

Plan

Universal One-Way Hash Functions and their Cryptographic Applications

Moni Naor et Moti Young (STOC 1989)

x

$h \xleftarrow{\$} \mathcal{K}$

Adversary

Challenger

y

$$\mathbf{Adv}_{TCR}(\mathcal{A}) = \Pr[H_k(x) = H_k(y)]$$

Sufficient for Hash-and-Sign

- *Collision-resistant hashing : towards making UOWHFs practical*
  - M. Bellare et P. Rogaway (Crypto 1997)
- Signature de $M = (k, \mathrm{Sign}(k, H_k(M)))$

Les fonctions quadratiques sont-elles des UOWHFs ?

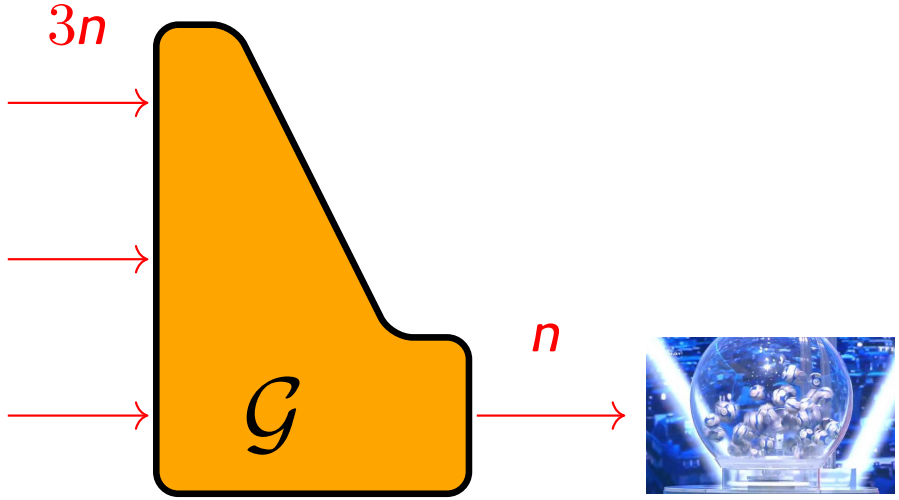
- Surtout intéressant dans le cas $m \leq n$
  - Contractant, pour pouvoir hacher
- Ça a l'air vrai mais **comment le prouver** ? 🧐

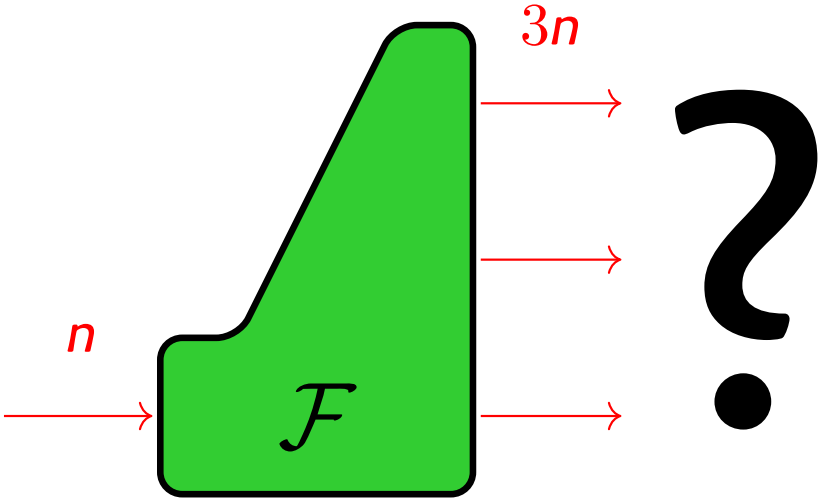
Le problème

- On dispose d'un adversaire en deux parties :
  - $\mathit{state}, \mathbf{x} \leftarrow \mathrm{Marvin}_1(1^n)$
  - Une fonction quadratique $f : \mathbb{F}_q^n \to \mathbb{F}_q^m$ est tirée aléatoirement
  - $\mathbf{y} \leftarrow \mathrm{Marvin}_2(\mathit{state}, f)$ avec $f(\mathbf{x}) = f(\mathbf{y})$
- La construction précédente donne une fonction structurée
  - 😭
  - (et en plus $\mathbf{x}$ devrait nous être imposé)

Plan

Fonction quadratique aléatoire évaluée sur un vecteur aléatoire ?





Les fonction quadratiques sont pseudo-aléatoires

Intuition

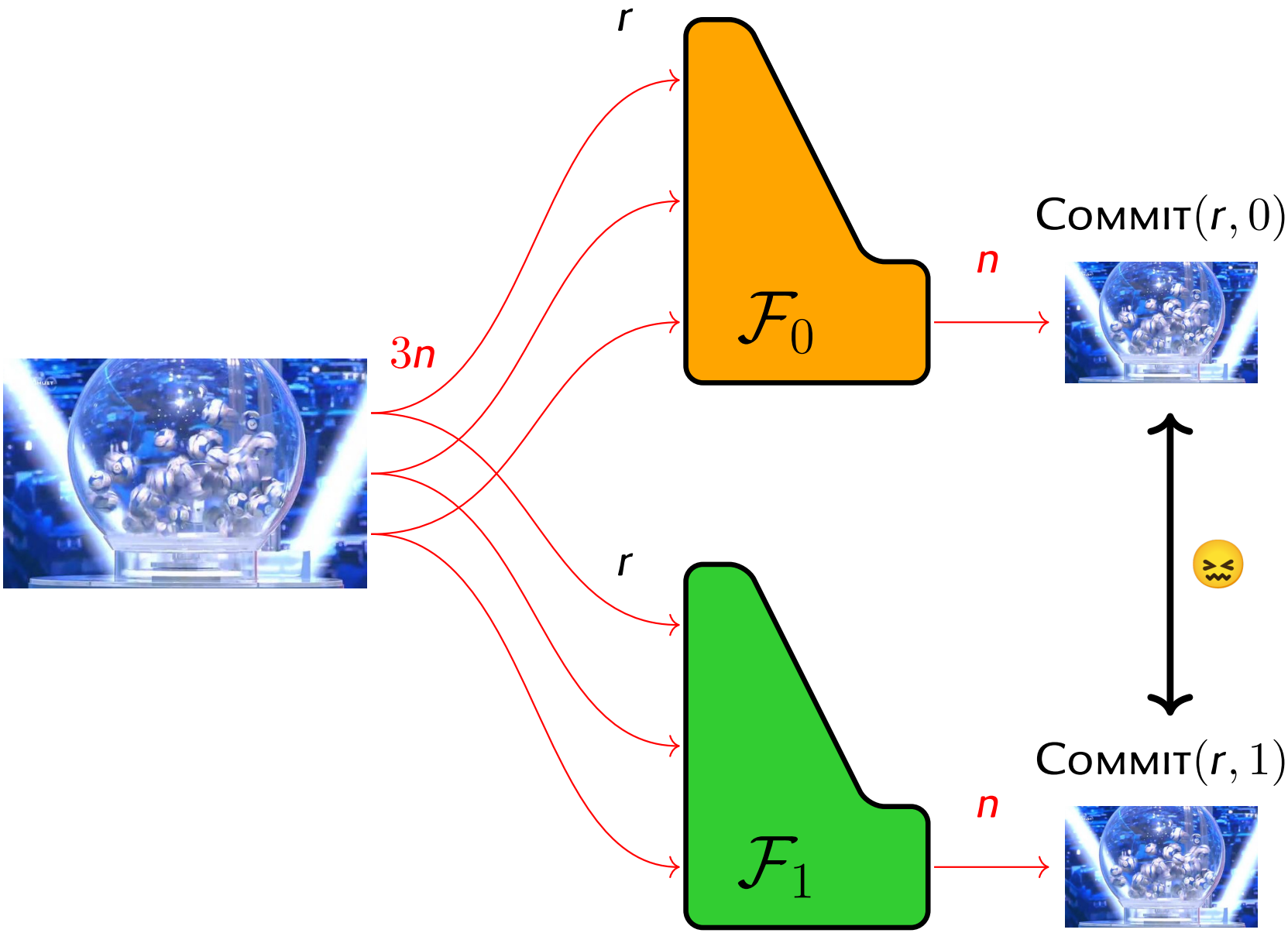
Si $\mathcal{F}$ est une fonction quadratique aléatoire et $\mathbf{x}$ un vecteur aléatoire, alors $\mathcal{F}(x)$ devrait avoir l'air aléatoire.

Dans le détail...

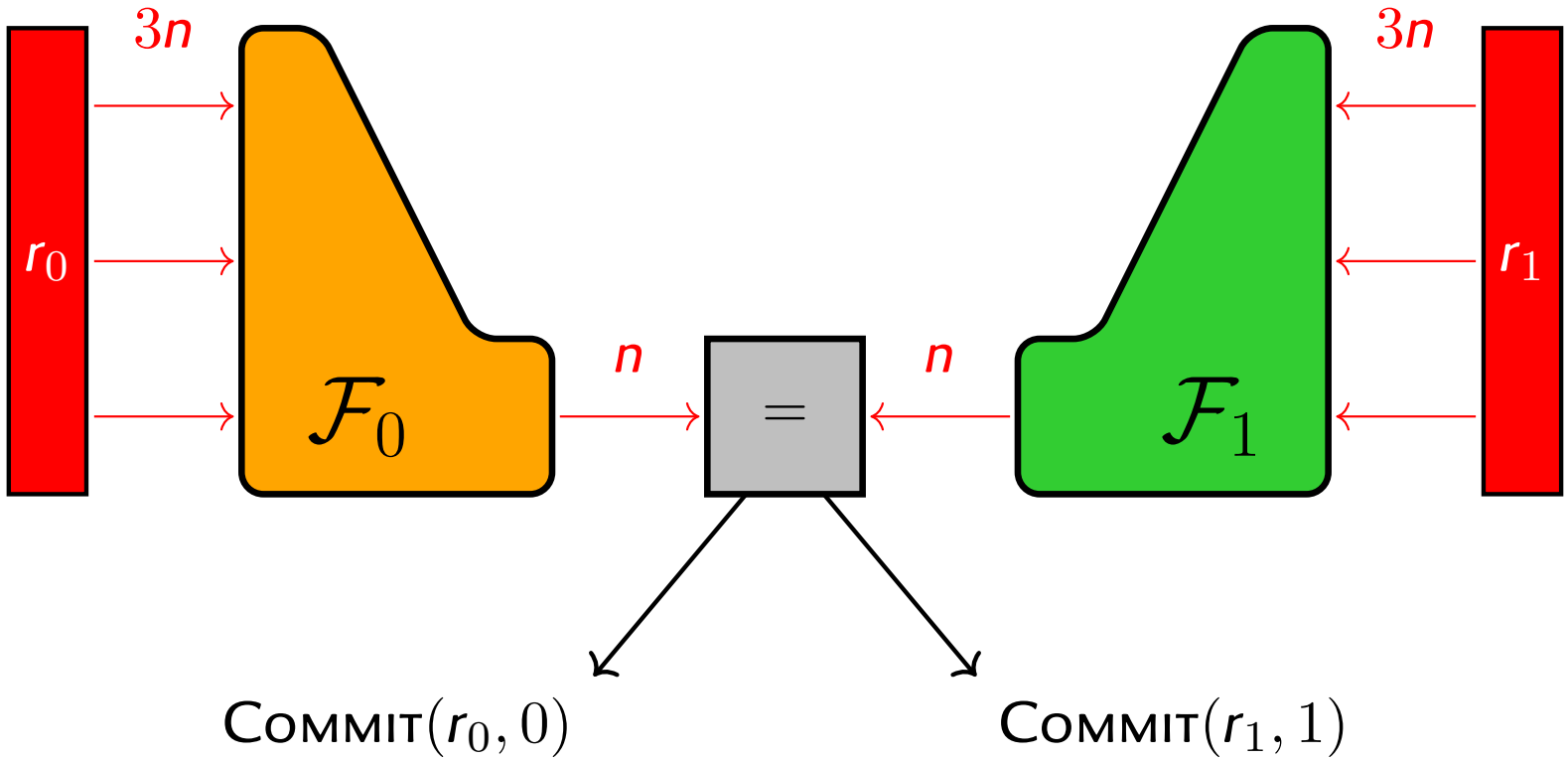
- $\mathcal{F}(x)$ est statistiquement indistinguable de la distribution uniforme si $\mathcal{F}$ est (suffisamment) contractante
  - Argument simple ☺️
  - Valable pour toutes les fonctions de hachage universelles

How to Construct Constant-Round Zero-Knowledge Proof Systems for NP

Oded Goldreich et Ariel Kahan (J. of crypto 1988–1996)



Est-il *binding* ? *Claw-freeness* des fonctions quadratiques...



Attaque contre le *binding*

- Résoudre $\mathcal{F}_0(\mathbf{x}) = \mathcal{F}_1(\mathbf{y})$
- Système structuré, pas évident d'étudier la complexité...

Plan

Les fonction quadratiques sont pseudo-aléatoires

Intuition

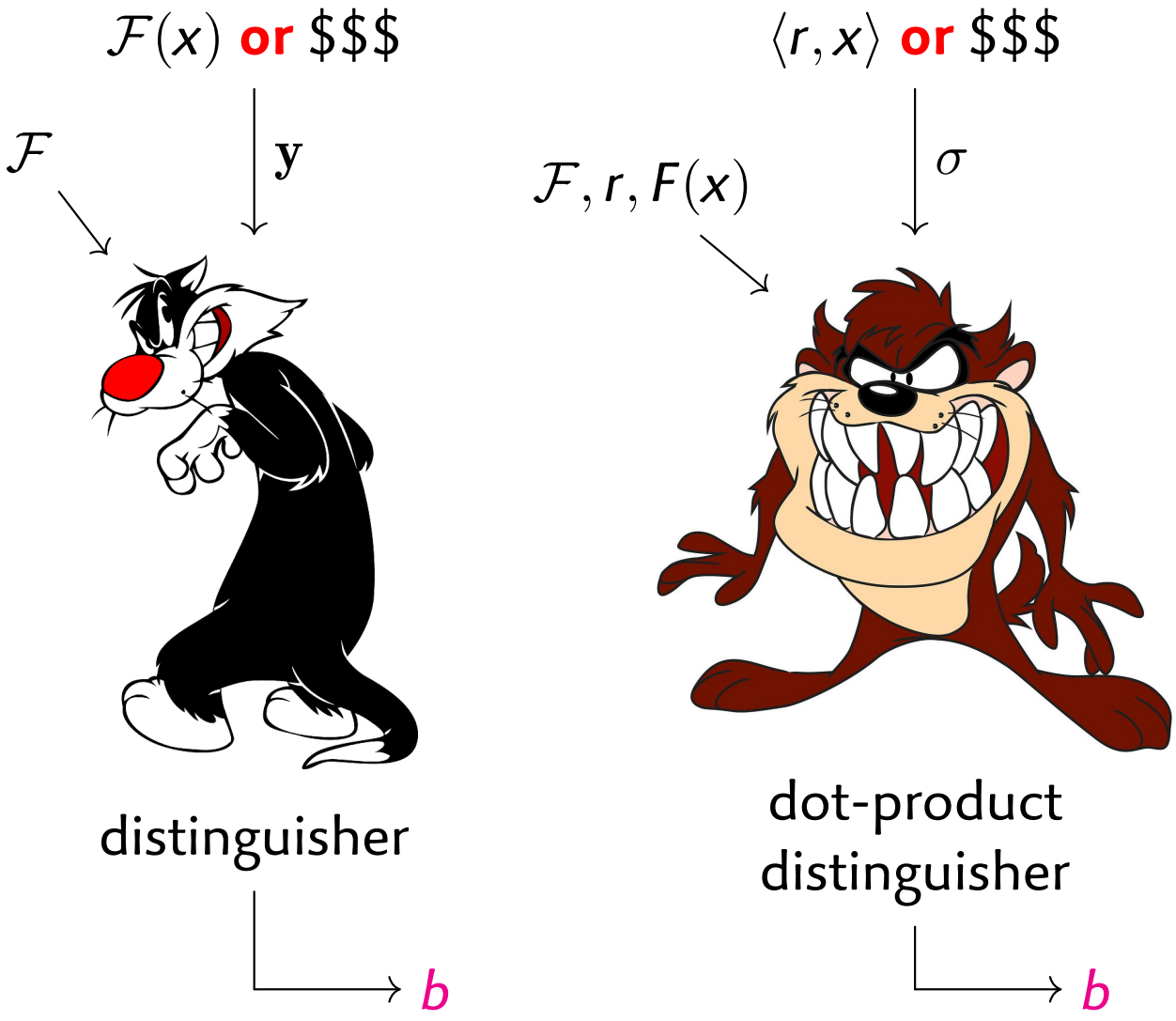
Si $\mathcal{F}$ est une fonction quadratique aléatoire et $\mathbf{x}$ un vecteur aléatoire, alors $\mathcal{F}(x)$ devrait avoir l'air aléatoire.

Dans le détail...

- $\mathcal{F}(x)$ est statistiquement indistinguable de la distribution uniforme si $\mathcal{F}$ est (suffisamment) contractante
  - Argument simple ☺️
  - Valable pour toutes les fonctions de hachage universelles
- $\mathcal{F}(x)$ est calculatoirement indistinguable de la distribution uniforme si $\mathcal{F}$ est (pas trop) expansive
  - Attaque simple : résoudre $\mathbf{y} = \mathcal{F}(\mathbf{x})$
    - Succès $\rightsquigarrow$ PRG / échec $\rightsquigarrow$ \$\$\$
  - Preuve ? Argument difficile 😖 « à la Goldreich-Levin »
  - *QUAD : A Practical Stream Cipher with Provable Security*
    - Côme Berbain, Henri Gilbert, Jacques Patarin (Eurocrypt 2006)

Idée générale

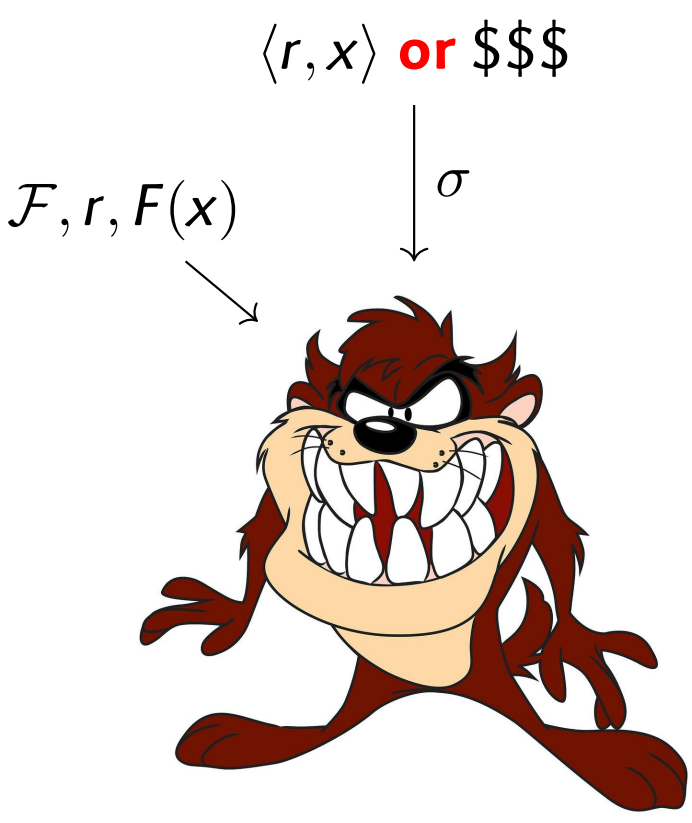
Idée générale



Idée générale

distinguisher

$\rightarrow b$



dot-product distinguisher

$\rightarrow b$

inverter

$\rightarrow x$

Phase 1 (la facile)

$\mathcal{F}(\mathbf{x})$ **or** \$\$\$

$\mathbf{y}$

$\mathcal{F}$

distinguisher

b

$\langle \mathbf{r}, \mathbf{x} \rangle$ **or** \$\$\$

σ

$\mathcal{F}, \mathbf{r}, \mathcal{F}(\mathbf{x})$

dot-product
distinguisher

b

Phase 1 (la facile)

$\mathcal{F}(\mathbf{x})$ **or** \$\$\$

$\mathbf{y}$

$\mathcal{F}$

distinguisher

b

$\langle \mathbf{r}, \mathbf{x} \rangle$ **or** \$\$\$

σ

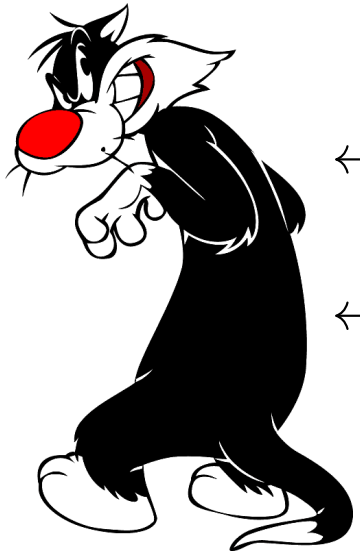
$\mathcal{F}, \mathbf{r}, \mathcal{F}(\mathbf{x})$

$\mathbf{a} \xleftarrow{\$} \mathbb{F}_q^m$

dot-product distinguisher

b

Phase 1 (la facile)



distinguisher

$\langle \mathbf{r}, \mathbf{x} \rangle$ or \$\$\$

σ

$\mathcal{F}, \mathbf{r}, \mathcal{F}(\mathbf{x})$

$\mathcal{F}'(\mathbf{z}) := \mathcal{F}(\mathbf{z}) + \langle \mathbf{r}, \mathbf{z} \rangle \cdot \mathbf{a}$

$\mathbf{y}' := \mathbf{y} + \sigma \cdot \mathbf{a}$

$\mathbf{a} \xleftarrow{\$} \mathbb{F}_q^m$

dot-product distinguisher

b

If $\sigma = \langle \mathbf{r}, \mathbf{x} \rangle$, then $\mathbf{y}' = \mathcal{F}'(\mathbf{x})$, otherwise $\mathbf{y}' = \$\$\$$

Public-key encryption schemes with auxiliary inputs

Y. Dodis, S. Goldwasser, Y. Tauman Kalai, C. Peikert et V. Vaikuntanathan (TCC 2010)

function INVERTER(n, ϵ, y)
  Set c to the smallest integer such that $q^c \geq 128qn/\epsilon^2$. ▷ note that $c \geq 2$
  Set $N \leftarrow 0$. ▷ Estimate $\beta_{x,y}$
  for $i = 1, \ldots, 192n/\epsilon^2$ **do**
    Sample a vector $r \xleftarrow{\$} \mathbb{F}_q^n$ and a scalar $u \xleftarrow{\$} \mathbb{F}_q$.
    if $\mathcal{D}(y, r, u) = 1$ **then** increment N.
  end for
  Set $e \leftarrow N\epsilon^2/n/192$. ▷ $\Pr[|e - \beta| \geq \epsilon/8] \leq 2^{-n}$ as soon as $n \geq 3$
  Set $\gamma \leftarrow e + \epsilon/4$. ▷ $\beta_{x,y} + \epsilon/8 \leq \gamma \leq \alpha_{x,y} - \epsilon/8$.
  Choose c random vectors $z_1, \ldots, z_c$ in $\mathbb{F}_q^n$ and c random scalars $g_1, \ldots, g_c$ from $\mathbb{F}_q$.
    ▷ g_i is a "guess" for the value of $\langle z_i, x \rangle$
  Set $m \leftarrow 128qn/\epsilon^2$. Sample a random m-subset S of $\mathbb{F}_q^c/\{0\}$.
  for every $\rho = (\rho_1, \ldots, \rho_c) \in S$ **do**
    Compute $r_\rho = \sum_{j=1}^{c} \rho_j z_j$ and $h_\rho = \sum_{j=1}^{c} \rho_j g_j$.
  end for
    ▷ if the "guesses" g_i are all correct, then $h_\rho = \langle r_\rho, x \rangle$ for every ρ
  for $i = 1, 2, \ldots, n$ **do**
    Set $x_i \leftarrow \perp$. ▷ the following tries to determine x_i
    for $a \in \mathbb{F}_q$ **do** ▷ assume that $x_i = a$; the following checks if this is correct
      Set $N \leftarrow 0$.
      for $\rho \in S$ **do**
        Pick a random scalar $\tau \xleftarrow{\$} \mathbb{F}_q$.
        if $\mathcal{D}(y, r_\rho + \tau \cdot e_i, h_\rho + \tau \cdot a) = 1$ **then** increment N.
      end for
      if $N \geq m\gamma$ **then** set $x_i \leftarrow a$.
    end for
    if $x_i = \perp$ **then abort** the algorithm. ▷ could not determine x_i
  end for
  return x
end function

Phase 2 (la difficile)

$\langle \mathbf{r}, \mathbf{x} \rangle$ **or** \$\$\$

σ

$\mathcal{F}, \mathcal{F}(\mathbf{x}), \mathbf{r}$

dot-product distinguisher

b

$\mathcal{F}(x)$

y

$\mathcal{F}$

inverter

x

Phase 2 (la difficile)

$\langle \mathbf{r}, \mathbf{x} \rangle$ **or** \$\$\$

σ

$\mathcal{F}, \mathcal{F}(\mathbf{x}), \mathbf{r}$

dot-product distinguisher

b

$$\mathbf{r}_1, \ldots, \mathbf{r}_c \xleftarrow{\$} \mathbb{F}_q^n$$
$$g_1, \ldots, g_c \xleftarrow{\$} \mathbb{F}_q$$
assume $\langle \mathbf{r}_i, \mathbf{x} \rangle = g_i$

$\mathcal{F}(x)$

y

$\mathcal{F}$

inverter

x

Phase 2 (la difficile)

$\langle \mathbf{r}, \mathbf{x} \rangle$ **or** \$\$\$

σ

$\mathcal{F}, \mathcal{F}(\mathbf{x}), \mathbf{r}$

dot-product distinguisher

$\longrightarrow b$

$$\mathbf{r}_1, \ldots, \mathbf{r}_c \xleftarrow{\$} \mathbb{F}_q^n$$
$$g_1, \ldots, g_c \xleftarrow{\$} \mathbb{F}_q$$
assume $\langle \mathbf{r}_i, \mathbf{x} \rangle = g_i$

$$u_1, \ldots, u_c \xleftarrow{\$} \mathbb{F}_q$$
$$\left\langle \sum_i u_i \mathbf{r}_i, \mathbf{x} \right\rangle = \sum_i u_i g_i$$

$\mathcal{F}(x)$

y

$\mathcal{F}$

inverter

$\longrightarrow x$

Phase 2 (la difficile)

$\langle \mathbf{r}, \mathbf{x} \rangle$ **or** \$\$\$

σ

$\mathcal{F}, \mathcal{F}(\mathbf{x}), \mathbf{r}$

dot-product distinguisher

b

$$\mathbf{r}_1, \ldots, \mathbf{r}_c \xleftarrow{\$} \mathbb{F}_q^n$$
$$g_1, \ldots, g_c \xleftarrow{\$} \mathbb{F}_q$$
assume $\langle \mathbf{r}_i, \mathbf{x} \rangle = g_i$

$$u_1, \ldots, u_c \xleftarrow{\$} \mathbb{F}_q$$
$$\left\langle \sum_i u_i \mathbf{r}_i, \mathbf{x} \right\rangle = \sum_i u_i g_i$$

Test if $\mathbf{x}_i = a$

$$\tau \xleftarrow{\$} \mathbb{F}_q$$
$$\left\langle \sum_i u_i \mathbf{r}_i + \tau \mathbf{e}_i, \mathbf{x} \right\rangle = \sum_i u_i g_i + \tau a$$

$\mathcal{F}(x)$

y

$\mathcal{F}$

inverter

x

Phase 2 (la difficile)

$$\mathbf{r}_1, \ldots, \mathbf{r}_c \xleftarrow{\$} \mathbb{F}_q^n$$
$$g_1, \ldots, g_c \xleftarrow{\$} \mathbb{F}_q$$
assume $\langle \mathbf{r}_i, \mathbf{x} \rangle = g_i$

$$u_1, \ldots, u_c \xleftarrow{\$} \mathbb{F}_q$$
$$\left\langle \sum_i u_i \mathbf{r}_i, \mathbf{x} \right\rangle = \sum_i u_i g_i$$

Test if $\mathbf{x}_i = a$
$$\tau \xleftarrow{\$} \mathbb{F}_q$$
$$\left\langle \sum_i u_i \mathbf{r}_i + \tau \mathbf{e}_i, \mathbf{x} \right\rangle = \sum_i u_i g_i + \tau a$$

dot-product distinguisher

$\mathcal{F}, y, \mathbf{r} := \sum_i u_i \mathbf{r}_i + \tau \mathbf{e}_i$ ←

$\sigma := \sum_i u_i g_i + \tau a$ ←

b →

$\mathcal{F}(x)$ → y → $\mathcal{F}$

inverter

x →

Phase 2 (la difficile)

$\mathbf{r}_1, \ldots, \mathbf{r}_c \xleftarrow{\$} \mathbb{F}_q^n$

$g_1, \ldots, g_c \xleftarrow{\$} \mathbb{F}_q$

assume $\langle \mathbf{r}_i, \mathbf{x} \rangle = g_i$

$u_1, \ldots, u_c \xleftarrow{\$} \mathbb{F}_q$

$\left\langle \sum_i u_i \mathbf{r}_i, \mathbf{x} \right\rangle = \sum_i u_i g_i$

Test if $\mathbf{x}_i = a$

$\tau \xleftarrow{\$} \mathbb{F}_q$

$\left\langle \sum_i u_i \mathbf{r}_i + \tau \mathbf{e}_i, \mathbf{x} \right\rangle = \sum_i u_i g_i + \tau a$

dot-product distinguisher

$\mathcal{F}, y, \mathbf{r} := \sum_i u_i \mathbf{r}_i + \tau \mathbf{e}_i$

$\sigma := \sum_i u_i g_i + \tau a$

b

$\mathcal{F}(x)$

y

$\mathcal{F}$

inverter

x

Si les $\mathbf{r}_i, g_i$ et a sont corrects, alors b est **biaisé**

Au final

Theorem

Si *il existe un algorithme $\mathcal{D}$ qui (T, ϵ)-distingue $\mathcal{F}(x)$ de la distribution uniforme, où $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ est une fonction quadratique aléatoire et $x \xleftarrow{\$} \mathbb{F}_{q'}^n$*

alors *il existe un algorithme qui (T', ϵ')-inverse $\mathcal{F}$ avec*

$$T' = 128\frac{q^2n^2}{\epsilon^2}T + [\textit{termes négligeables}] \qquad \textit{et} \qquad \epsilon' \geq \frac{\epsilon^3}{512nq^2}$$

Paramètres sûrs pour $m = 2n$ (étirement $\times 2$) et $q = 256$

- $n = 96 \rightsquigarrow$ résolution de $\mathcal{F}(x) = 0$ coûte $\geq 2^{128}$
- $n = 896 \rightsquigarrow$ pas de distingueur avec $T \leq 2^{128}$ et $\epsilon \geq 2^{-128}$

Plan

How to construct random functions ?

Oded Goldreich, Shafi Goldwasser et Silvio Micali (J. ACM 1984)

- $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^{2n}$ une fonction quadratique aléatoire
  - $\mathcal{F}_0(x)$ est la première moitié de $\mathcal{F}(x)$
  - $\mathcal{F}_1(x)$ est le deuxième moitié de $\mathcal{F}(x)$