Générateurs pseudo-aléatoires à base de courbes elliptiques

(Aymen Landolsi) Bruno Martin

Université de Nice-Sophia Antipolis, laboratoire I3S, équipe MC3

Journées C2, Fréjus, le 9 octobre 2009

Plan de l'exposé

Quelques notations

Alphabet $\Sigma = \{0, 1\} = \mathbf{2}$
Mot fini $m \in \mathbf{2}^*$,

$\sharp w$: longueur de w
$w[1..n]$: n-préfixe de w (ou lsb_n)
On considère des distributions de probabilités.
(description valeurs et proba prises par un évènement)

$\mathcal{U}_{\mathbf{2}^n}$: distribution uniforme sur $\mathbf{2}^n$

$e \leftarrow D$: tirer e selon D
$Pr[\mathcal{P}(e)/e \leftarrow D]$ proba que e vérifie $\mathcal{P}$ pour e tiré selon D

Gedankenexperiment

Suites pseudo-aléatoires vues comme des "expériences de pensée" de la physique quantique

Goldreich : expériences sur le résultat d'un tirage à pile ou face. Celui qui doit deviner le résultat du tirage en fait l'annonce soit a priori, soit pendant l'expérience. Dans ce second cas, peut faire appel à des moyens techniques sophistiqués pour prendre sa décision.

Celui qui doit deviner le résultat du tirage peut améliorer substantiellement son choix. Voir [Diaconis, 2007].

Formalisation intuitive

[Blum et Micali] et [Yao] à l'origine de la théorie des GPA fondés sur la complexité

[Goldreich] $x \in \mathbf{2}^*$ pseudo-aléatoire si elle ne peut pas être distinguée efficacement d'une suite aléatoire parfaite.

- Utilise des suites infinies de distributions où chaque distribution est à support fini : ensemble de distributions.
- Indiscernabilité : deux suites sont indiscernables si aucune procédure efficace ne peut les distinguer.

(Ensemble de) Distributions

Distribution : associe à toute VA une fonction définie sur l'ensemble de ses événements élémentaires muni d'une distribution de probabilité qui attribue une probabilité à chacun des sous-ensembles (mesurables) d'événements élémentaires.

Ensemble de distributions : ℓ un polynôme. $\{D_n\}_{n\in\mathbb{N}}$ ens. de distributions où les $D_n \subseteq \mathbf{2}^{\ell(n)}$

Notion de distingueur

D algorithme PPT qui cherche à distinguer une distribution pseudo-aléatoire A de $\mathcal{U}$.

- p : proba de succès de D (répond que la distribution est A)
- $p^\star$ la proba correspondante pour $\mathcal{U}$,

on étudie l'avantage :

$$\mathrm{Adv}_D(A,\mathcal{U}) = |p - p^\star|$$

Si l'avantage est négligeable (1/poly), les distributions sont indiscernables (noté IND).

Distribution pseudo-aléatoire

Définition
Une distribution de probabilité est pseudo-aléatoire s'il n'y a pas de procédure efficace qui la distingue d'une uniforme.

Autre point de vue équivalent :

Théorème (Yao)

Une suite est pseudo-aléatoire si et seulement si on ne peut prédire la valeur du bit suivant.

Distribution pseudo-aléatoire

Définition
Une distribution de probabilité est pseudo-aléatoire s'il n'y a pas de procédure efficace qui la distingue d'une uniforme.

Autre point de vue équivalent :

Théorème (Yao)

Une suite est pseudo-aléatoire si et seulement si on ne peut prédire la valeur du bit suivant.

Applications :

- GPA
- génération de r pour méthode de Monte-Carlo
- techniques de dérandomisation

Générateur pseudo-aléatoire

Définition
$G \in$ FP GPA, s'il existe une fonction d'extension $\ell : \mathbb{N} \to \mathbb{N}$ telle que $\{G_n\}_{n\in\mathbb{N}}$ IND $\{\mathcal{U}_{\mathbf{2}^{\ell(n)}}\}_{n\in\mathbb{N}}$ où G_n est la sortie de G sur un germe tiré uniformément dans $\mathbf{2}^n$.

Plan de l'exposé

Suites pseudo-aléatoires

Petite histoire (DEC PRG)

Golreich-Levin

Retour aux courbes elliptiques

Notations (courbes elliptiques)

E : courbe elliptique définie par l'équation $y^2 = x^3 + ax + b$
$E(\mathbb{F}_p)$: ensemble des points $\mathbb{F}_p$ -rationnels de E :

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 = x^3 + ax + b\} \cup \mathcal{O}$$

$P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$ deux points de $E(\mathbb{F}_p)$ tq

$$P = \alpha \cdot Q$$

Trouver α est difficile (résoudre ECDLP)

$\mathrm{x} : E(\mathbb{F}_p) \to \mathbb{F}_p$: projection de l'abcisse d'un point
$\mathrm{y} : E(\mathbb{F}_p) \to \mathbb{F}_p$: projection de l'ordonnée d'un point

DEC PRG

[Barker and Kelsey, 2005] : Dual Elliptic Curve PRG (NIST)

Input : $s_0 \xleftarrow{\mathcal{U}} \{0, 1, \ldots, \sharp E(\mathbb{F}_p) - 1\}$, $k > 0$
Output : $240.k$ bits pseudo-aléatoires
for $i = 1$ à k **do**
$s_i = \mathrm{x}(s_{i-1}P)$
$r_i = \text{lsb}_{240}(\mathrm{x}(s_iQ))$
end for
return $r_1, \ldots, r_k$

avec $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$, a et b de 150 chiffres.

Distingueur de DEC PRG

[Schoenmakers et al., 2006] construisent un distingueur

- d'avantage $0,00156$ pour un bloc de 240 bits
- d'avantage $0,09757$ sur plusieurs blocs

avec une attaque de complexité 2^{16}
Ils contredisent l'affirmation

$$\text{lsb}_{240}(\mathrm{x}(s_iQ)) \text{ IND } \mathcal{U}_{240}$$

Plan de l'exposé

Suites pseudo-aléatoires

Petite histoire (DEC PRG)

Golreich-Levin

Retour aux courbes elliptiques

Fonction à sens unique

Définition
$f : \{0,1\}^\star \to \{0,1\}^\star$ est à sens unique (OW) si :

- *il existe un algo en temps polynomial pour calculer $f(x)$*
- *pour tout adversaire A PPT, il existe $negl.$ tq :*

$$Pr[\textit{Invert}_{A,\,f}(n)] \leq negl(n)$$

$\text{Invert}_{A,\,f}(n)$ formalise l'attaque contre f OW :

1. $x \xleftarrow{u} 2^n$; $y := f(x)$
2. A reçoit 1^n et y et renvoie x'
3. A réussit (i.e. renvoie 1) ssi $f(x') = y$

Hard-core predicate

Définition
Un prédicat calculable en temps polynomial $b : \{0,1\}^\star \to \{0,1\}$ est la fève (hard-core predicate) d'une fonction OW f si pour tout adversaire A PPT, il existe $negl$:

$$Pr[A(f(x)) = b(x)] \leq \frac{1}{2} + negl(n)$$

où la proba est prise pour $x \xleftarrow{u} \mathbf{2}^n$ et l'ens. des tirages de A.

généralise une notion d'imprédictibilité obtenue de l'impossibilité d'inverser f :

$$Pr\big[A(i, f(x)) = x[i]\big] \leq \frac{1}{2} + negl(n)$$

Goldreich-Levin

Théorème ([Goldreich and Levin, 1989])
Soit f OW. Il existe g OW et gl une fève pour g. Si f est une permutation, g aussi.

$$g(x,r) = (f(x), r) \text{ avec } \sharp x = \sharp r$$
$$gl(x,r) = \bigoplus_{i=1}^{n} x[i]r[i]$$

$r \subsetneq \{1, \ldots, n\}$ parfaitement aléatoire.

Attention, trouver une fève n'est pas facile.

Sauter l'intuition de GL

Intuition de GL

Proposition
S'il existe A PPT tel que, pour une infinité de n,

$$Pr_{x,r \leftarrow \mathcal{U}_n}\big[A(f(x), r) = gl(x,r)\big] = 1$$

alors il existe A' PPT qui inverse f pour une infinité de n :

$$Pr\big[A'(f(x)) \in f^{-1}(f(x))\big] = 1$$

Preuve : construction de A' donné A : soit $e_i \in \mathbf{2}^n$ le mot $0 \cdots 0$ sauf 1 en position i. A', sur l'entrée $y \in \mathbf{2}^n$, calcule

$$x[i] = A(y, e_i) = A(f(x), e_i) = \bigoplus_{j=1}^{n} x[j]e_i[j] = y[i]$$

de proba de succès 1 pour tout i $\square$

Par hyp. f OW. Il est impossible, pour tout algo PPT, d'inverser f avec une proba. non négligeable.

On en conclut qu'il n'existe pas d'algo PPT calculant toujours correctement $gl(x,r)$ étant donné $(f(x), r)$ pour une infinité de valeurs de n.

On est encore loin du résultat pour lequel on veut que $gl(x,r)$ ne puisse être déterminé avec proba $> 1/2$.

Il faut faire baisser la proba de succès de A petit à petit.

Construire un GPA

A partir de f OW selon [Goldreich, 2008].

Théorème

L'existence de permutations à sens unique implique celle de GPA. Et, pour tout polynôme $Q(n)$, il existe un GPA d'extension $Q(n)$.

Se fait en 2 lemmes :

- construire un bit
- étendre un nombre polynomial de fois

Construire un bit

Lemme

L'existence de permutations à sens unique implique celle d'un GPA qui étend son entrée d'un bit.

f permutation OW de fève gl. On construit la fonction G_1 :

$$G_1(x) = f(x).gl(x)$$

On peut montrer par l'absurde que G_1 est un GPA.

Répéter $Q(n)$ fois

Lemme

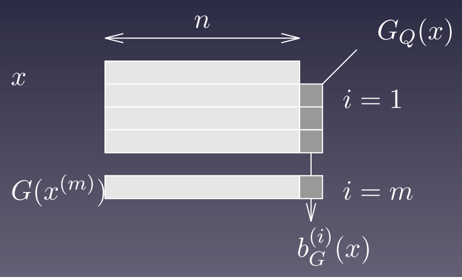
L'existence de GPA qui étendent leur entrée d'un bit implique que, pour tout polynôme $Q(n)$, il existe un GPA qui étend des entrées de taille n en des sorties de longueur $Q(n)$.

G_1 étend son entrée. Soit $m = Q(n)$ et $G_Q(x) = b_G^{(1)}(x) \ldots b_G^{(m)}(x)$

$$b_G^{(i)}(x) := \text{rmb}(G_1(x^{(i)}))$$

$x^{(i)}$ défini par réc. :

$$\begin{cases} x^{(0)} = x = x_1 \ldots x_n \\ x^{(i+1)} = G_1(x^{(i)})[1..n] \end{cases}$$



Plan de l'exposé

Suites pseudo-aléatoires

Petite histoire (DEC PRG)

Golreich-Levin

Retour aux courbes elliptiques

Kaliski, 1986

[Kaliski, 1986] : GPA basé sur la difficulté du problème du log. discret sur des courbes elliptiques.
Méthode comparable à GL :

- itérer une fonction OW
- extraire un bit

[Lercier, 2004] : courbes préconisées sont supersingulières.

Kaliski, 1986 : $\{b(f^i(s))\}_i$

Groupe des points $E(\mathbb{F}_p)$ engendrés par G
Itérées de la fonction : Germe : P un point de la courbe. On itère la fonction $\phi(P).G$ pour

$$\phi(P) = \begin{cases} \mathrm{y}(P) \text{ pour un point } P = (x, y) \\ p \text{ pour le point à l'infini} \end{cases}$$

Hard-core predicate :
G groupe abélien fini d'ordre N engendré par g. Kaliski définit

$$\mathrm{b}_{G,g}(x) = \begin{cases} 1 \text{ si } \mathrm{ord}_{G,g}(x) \geq N/2 \\ 0 \text{ sinon} \end{cases}$$

analogue à $\mathrm{umsb}_p(x) = \lfloor 2x/p \rfloor$ du prédicat de Blum et Micali pour l'exponentiation modulaire.

Kaliski, 1989

[Kaliski, 1991] : OWP f basée sur le problème elliptique du log. discret dans un groupe d'ordre n.
injection l des points rationnels de E dans les entiers modulo n

$$f(i) = l(i \cdot G)$$

pour G un point d'ordre maximum de la courbe dans les cas

1. $y^2 \equiv x^3 + b \mod p$ pour $p \equiv 2 \mod 3$
2. $y^2 \equiv x^3 + ax \mod p$ pour $p \equiv 3 \mod 4$ et $(a/p) = 1$

pour (a/p) le symbole de Legendre (i.e. a est un carré)

Généralise à des paires composées d'une courbe elliptique et de sa tordue.

Questions

1. OWP de Kaliski utilisable avec GL ?

Questions

1. OWP de Kaliski utilisable avec GL ?
2. Aussi bon que Kaliski, 1985 (M. Girault) ?

Questions

1. OWP de Kaliski utilisable avec GL ?
2. Aussi bon que Kaliski, 1985 (M. Girault) ?
3. Sur l'application de la construction de Goldreich...

Questions

1. OWP de Kaliski utilisable avec GL ?
2. Aussi bon que Kaliski, 1985 (M. Girault) ?
3. Sur l'application de la construction de Goldreich...

Merci !

Barker, E. and Kelsey, J. (2005).
Recommandation for random number generations using deterministic random bit generators.
NIST Special publications (SP) 800-90.

Diaconis, P. (2007).
The search for randomness.
http://www-sop.inria.fr/colloquium/diaconis/index.html.

Goldreich, O. (2008).
Computational Complexity.
Cambridge University Press.

Goldreich, O. and Levin, L. A. (1989).
A hard core predicate for any one way function.
In 21st STOC, pages 25–32.

Kaliski, B. (1986).
A pseudo-random bit generator based on elliptic logarithms.
In Crypto'86, volume 263 of LNCS, pages 84–103. Springer Verlag.

Kaliski, B. (1991).
One-way permutations on elliptic curves.
J. Cryptology, 3(3) :187–199.

Lercier, R. (2004).
Courbes elliptiques et cryptographie.
Revue Scientifique et Technique de la Défense, 64 :59–67.

Schoenmakers, B., Sidorenko, A., and Eidhoeven, T. (2006).
Cryptanalysis of the dual elliptic curve pseudorandom generator.
eprint.iacr, (190) :1–5.