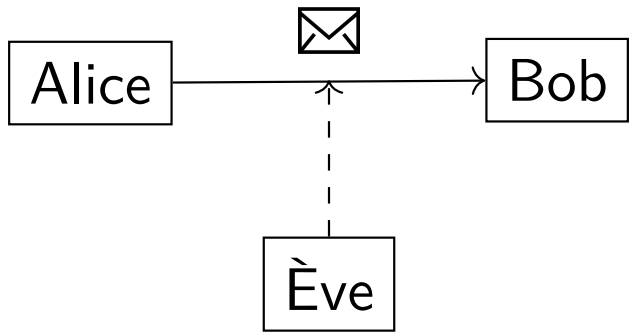
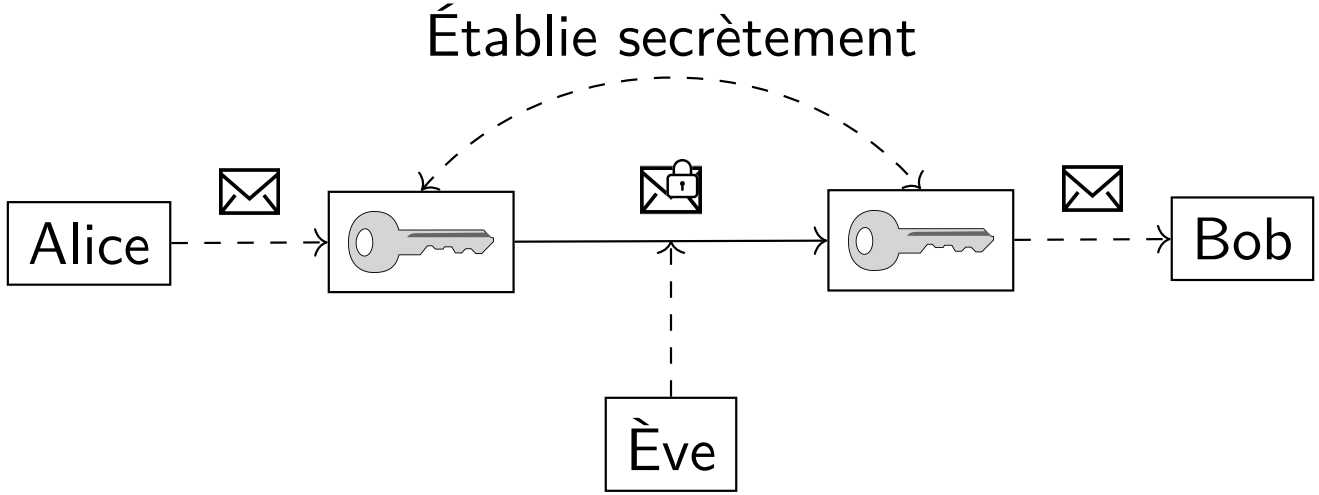
Générateurs pseudo-aléatoires et cryptographie

Elie Le Vaillant, SCEI n°49854

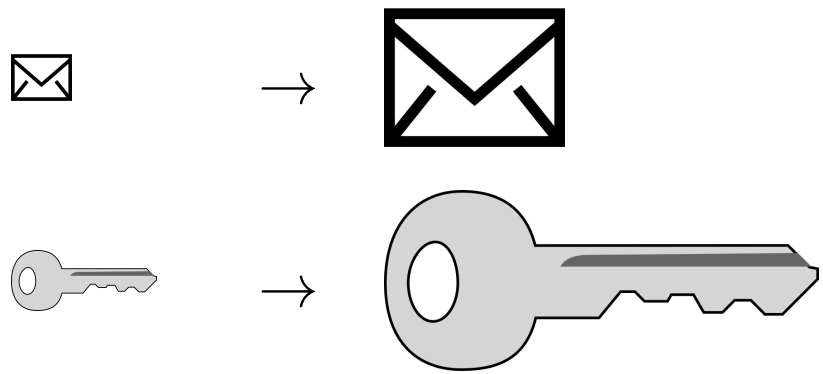
Session 2026



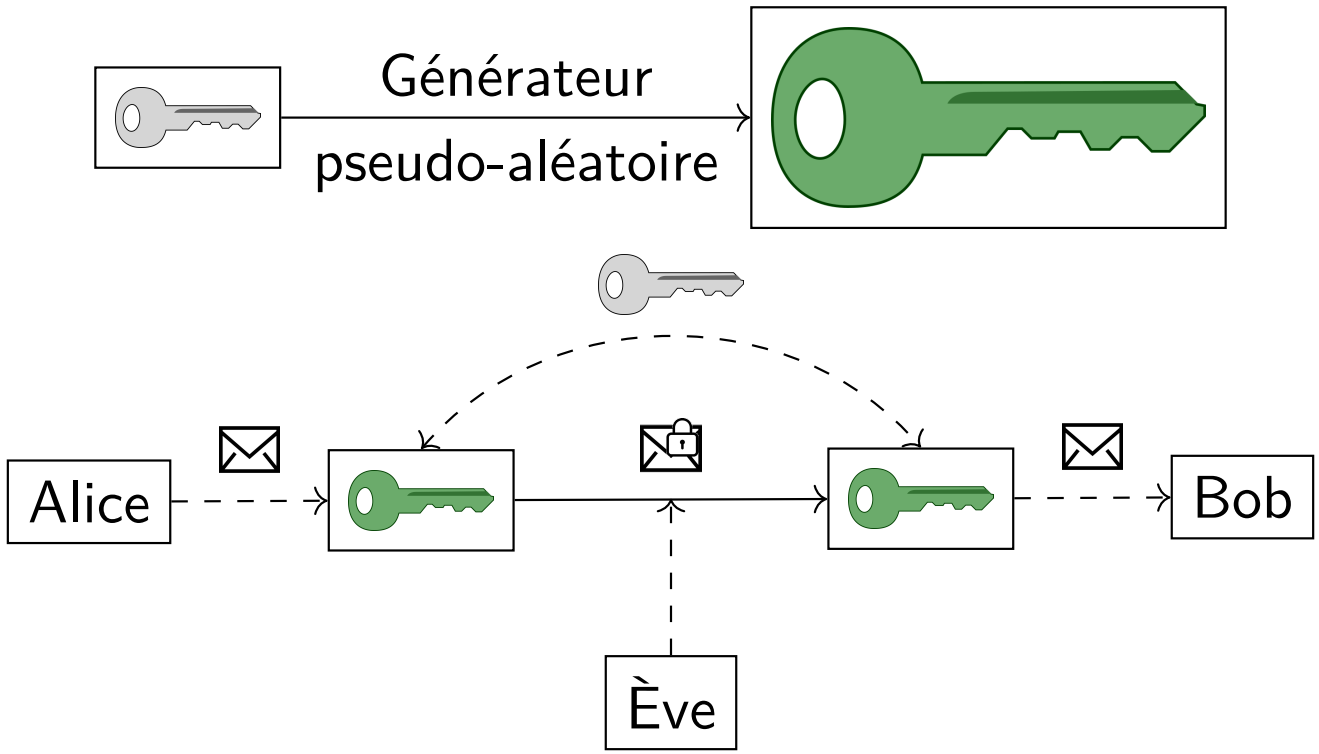
Les messages ne doivent pas être lisibles pour des agents extérieurs



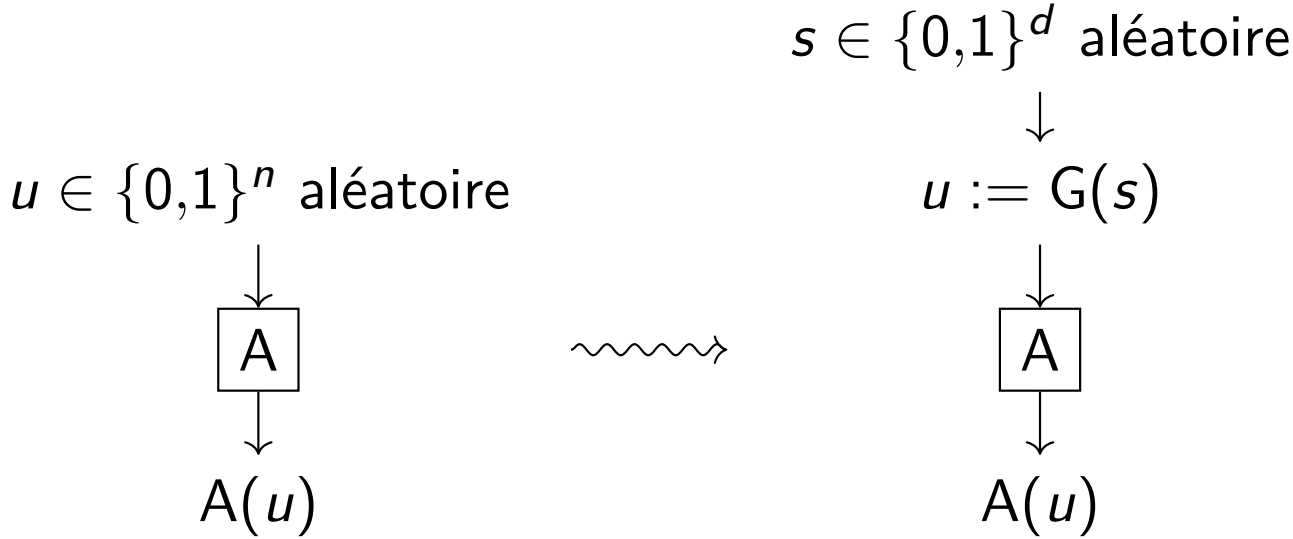
Protocole d'encryption à clé symétrique



Si sécurité parfaite, alors la clé doit être au moins aussi longue que le message



Principe d'un générateur pseudo-aléatoire cryptographique



Générateur pseudo-aléatoire : algorithme déterministe
$\mathsf{G} : \{0,1\}^d \to \{0,1\}^n$ avec $n > d$

Comment construire un générateur pseudo-aléatoire qui assure une sécurité cryptographique ?

1. Les LCGs

2. Générateur pseudo-aléatoire cryptographique

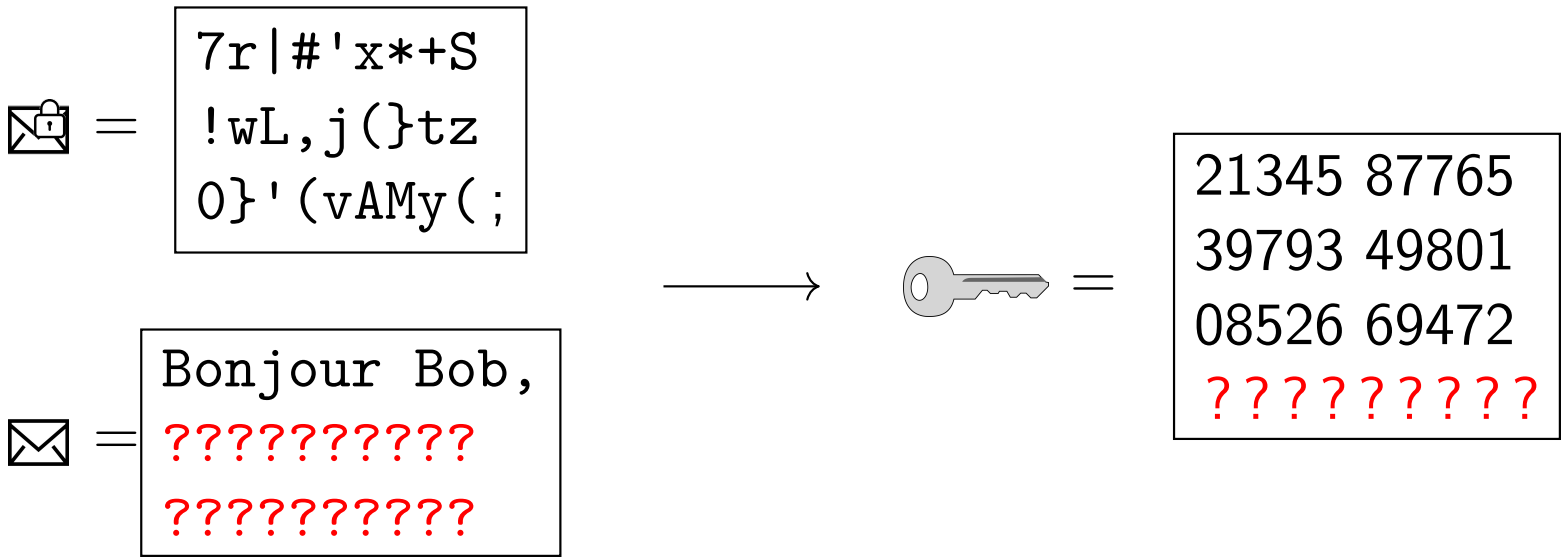
LCG = Linear Congruential Generator

Représentation binaire $\rightsquigarrow \{0,1\}^{32} \cong \{0,1,...,2^{32}-1\} =: \mathrm{N}$.

On définit alors le générateur $\mathrm{G} : \mathrm{N}^4 \to \mathrm{N}^{2^{16}}$ comme suit :

Pour $s, m, a, b \in \mathrm{N}$, on définit :

- $s_1 = s$, et $s_{n+1} = (as_n + b) \mod m$
- $\mathrm{G}(s, m, a, b) = (s_1, s_2, ..., s_{2^{16}})$



On peut retrouver des fragments de la clé

fragment de $s_1, s_2, \ldots$ (la clé)

$\rightsquigarrow$ reconstruction de **toute la clé** en retrouvant a, b, m, par une méthode *spécifique aux LCGs*

$\rightsquigarrow$ **décryptage de tout le message** (!!!)

On pose $t_n := s_{n+1} - s_n$

Alors
$$\begin{aligned} t_{n+1} &\equiv (as_{n+1} + b) - (as_n + b) \quad [m] \\ &\equiv at_n \quad [m] \end{aligned}$$

On pose
$$\begin{aligned} u_n &:= t_n t_{n+2} - t_{n+1}^2 \\ &\equiv t_n a^2 t_n - a^2 t_n^2 \quad [m] \\ &\equiv 0 \quad [m] \end{aligned}$$

$k+3$ termes consécutifs de $(s_n)_n$
$\rightsquigarrow$ k termes $a_1, ..., a_k$ de $(u_n)_n$, multiples de m
$\rightsquigarrow$ $\text{pgcd}(a_1, ..., a_k) = m$, très probablement

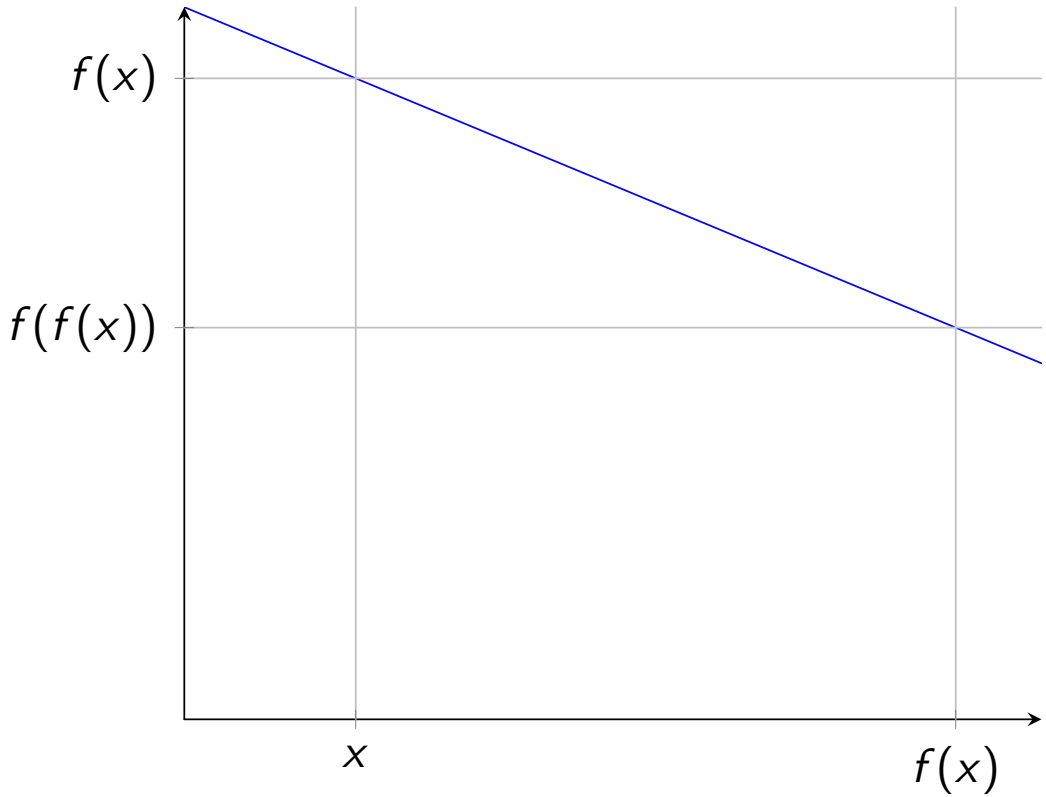
Théorème.

Soit $\mathrm{N}_k(n) = \{(a_1, ..., a_k) \in [\![1, n]\!]^k \,;\, \mathrm{pgcd}(a_1, ..., a_k) = 1\}$. *Alors :*

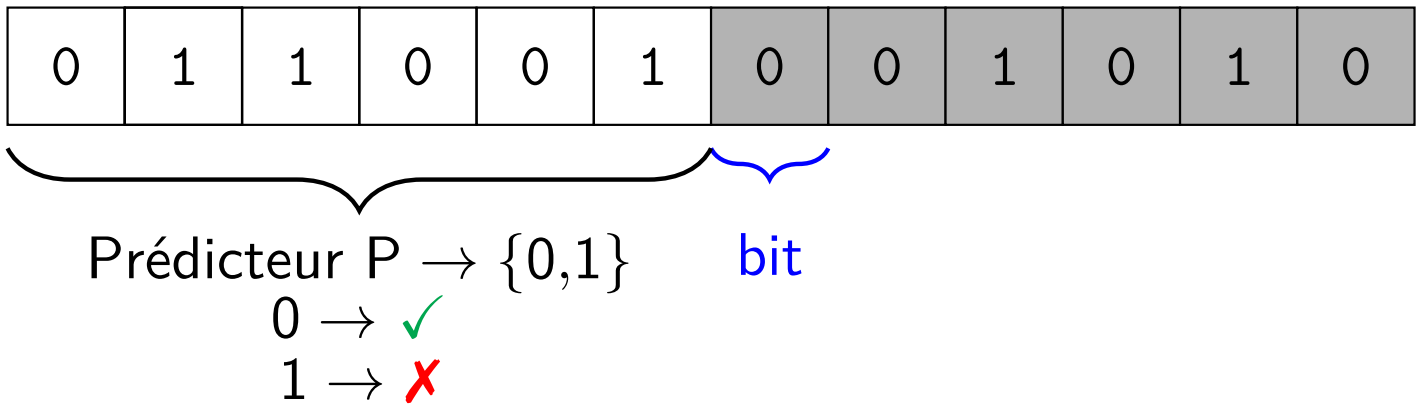
$$\frac{|\mathrm{N}_k(n)|}{n^k} \xrightarrow[n\to\infty]{} \prod_{p\in\mathcal{P}} \left(1 - \frac{1}{p^k}\right) = \frac{1}{\zeta(k)} = 1 - \frac{1}{2^k} + \mathrm{O}\left(\frac{1}{3^k}\right)$$

Corollaire : la densité des multiples de m $a_1, ..., a_k$ tels que $\mathrm{pgcd}(a_1, ..., a_k) \neq m$ est équivalente à $\frac{1}{2^k}$ quand $k \to \infty$, ce qui justifie l'argument précédent.

En connaissant m, 3 termes consécutifs de $(s_n)_n$ suffisent

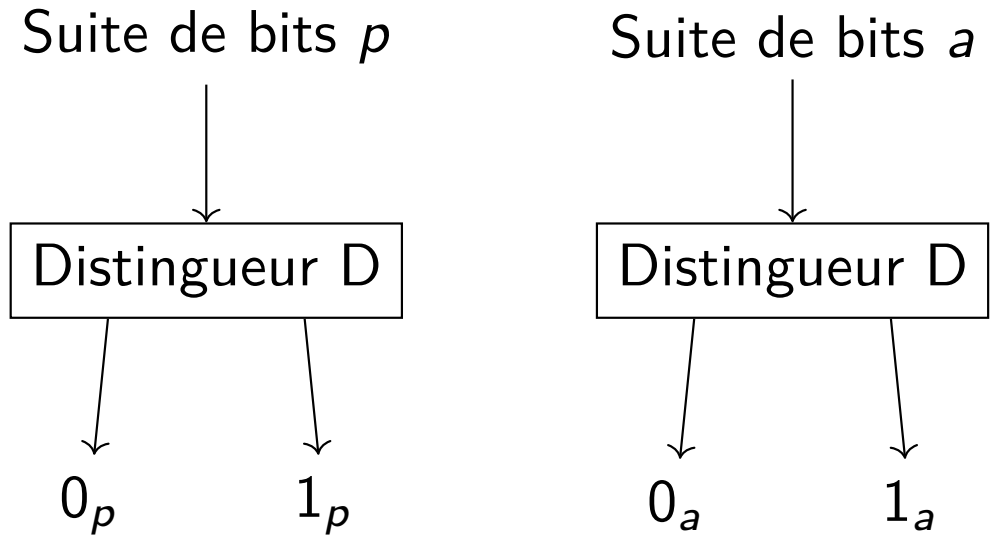


Résolution d'une équation affine avec 3 termes consécutifs



On dit que P *prédit le prochain bit mieux que le hasard* quand $\left|\mathbb{P}(\checkmark) - \frac{1}{2}\right|$ est non-négligeable.

But sur le générateur : aucun prédicteur « efficace » ne prédit le prochain bit mieux que le hasard

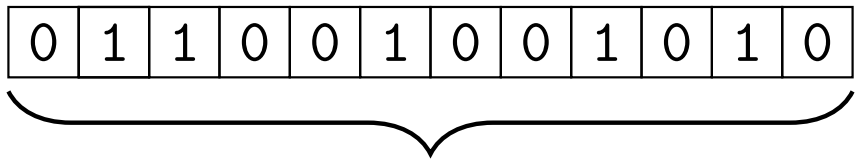


On dit que D *distingue p et a* quand $|\mathbb{P}(1_p) - \mathbb{P}(1_a)|$ est non-négligeable.

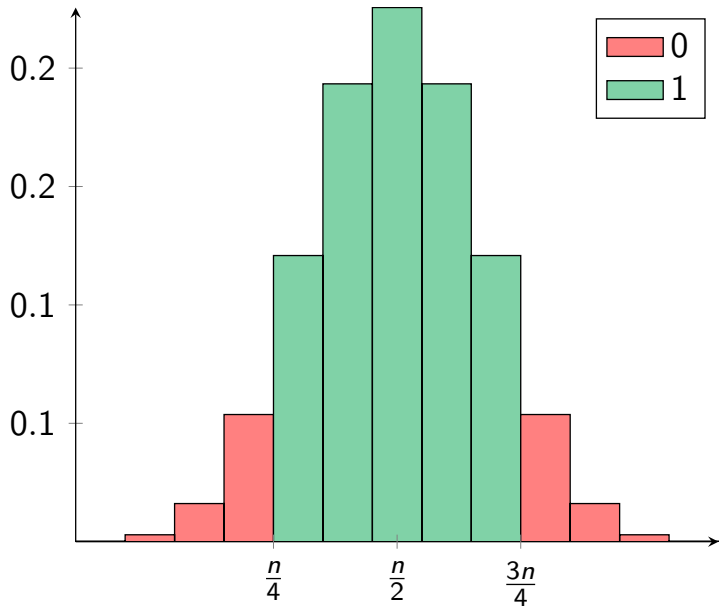
But sur le générateur : aucun distingueur « efficace » ne distingue les bits pseudo-aléatoires des bits aléatoires

2. Générateur pseudo-aléatoire cryptographique

Exemple de distingueur : compter les « 1 »



$\rightarrow$ 5 « 1 »



$n = 12$

On note $\{0,1\}^* := \bigcup_{n=0}^{+\infty} \{0,1\}^n$, et si $x \in \{0,1\}^*$, on note $|x|$ sa longueur

Définition.

- *Un algorithme (probabiliste)* $\mathsf{A} : \{0,1\}^* \to \{0,1\}^*$ *est* ***efficace*** *quand il existe un polynôme* p *tel que, pour tout* $x \in \{0,1\}^*$, $\mathsf{A}(x)$ *termine après au plus* $p(|x|)$ *étapes*
- *Une fonction* $\mu : \mathbb{R} \to \mathbb{R}$ *est* ***négligeable*** *quand, pour tout* $k \in \mathbb{N}$, $\mu(x) \underset{x \to \infty}{=} o\left(\frac{1}{x^k}\right)$

$(X_n)_{n\in\mathsf{I}}$: suite de va avec X_n à valeurs dans $\{0,1\}^n$

Si $x := (b_1, ..., b_n) \in \{0,1\}^n$, $x^i := b_i$, et $x^{\leq i} := (x^1, ..., x^i)$

Définition.

$(X_n)_{n\in\mathsf{I}}$ *est* ***imprédictible*** *quand pour tout prédicteur efficace* $A : \{0,1\}^* \to \{0,1\}$, *pour tout algorithme efficace de choix* $\pi : \{0,1\}^* \to \mathbb{N}$ *avec* $\pi(\{0,1\}^n) \subset [\![0, n-1]\!]$, *il existe* μ *négligeable tel que, pour tout* $n \in \mathsf{I}$,

$$i := \pi(X_n), \left| \mathbb{P}\left[A\left(X_n^{\leq i}, 1^n \right) = X_n^{i+1} \right] - \frac{1}{2} \right| \leq \mu(n)$$

U_n : va distribuée uniformément dans $\{0,1\}^n$

Définition.

$(X_n)_{n\in I}$ *est* ***pseudoaléatoire*** *quand pour tout distingueur efficace* $D : \{0,1\}^* \to \{0,1\}$, *il existe* μ *négligeable tel que, pour tout* $n \in I$,

$$|\mathbb{P}[D(X_n) = 1] - \mathbb{P}[D(U_n) = 1| \leq \mu(n)$$

Théorème.

$(X_n)_{n\in I}$ *est imprédictible*

$\iff$

$(X_n)_{n\in I}$ *est pseudoaléatoire*

Démonstration.

A, π : prédicteur efficace $\rightsquigarrow$ D : distingueur efficace

Soit $n \in \mathsf{I}$, D(x) où $x \in \{0,1\}^n$ l'algorithme défini par :

- Soit $i := \pi(x)$
- Si $\mathsf{A}(x^{\leq i}, 1^n) = x^i$, alors renvoyer 1
- Sinon, renvoyer 0

Alors $\mathbb{P}[\mathsf{D}(\mathsf{U}_n) = 1] = \frac{1}{2}$, et :

$$\left|\mathbb{P}\left[\mathsf{A}\left(\mathsf{X}_n^{\leq i}, 1^n\right) = \mathsf{X}_n^{i+1}\right] - \frac{1}{2}\right| = |\mathbb{P}[\mathsf{D}(\mathsf{X}_n) = 1] - \mathbb{P}[\mathsf{D}(\mathsf{U}_n) = 1]|$$
$$\leq \mu(n).$$

□

Démonstration.

D : distingueur efficace $\rightsquigarrow$ A, π : prédicteur efficace

Soit $n \in \mathbb{N}$, $\pi(x)$ où $x \in \{0,1\}^n$ l'algorithme défini par :

- Tirer i aléatoirement dans $[\![0, n-1]\!]$
- Renvoyer i

Et A$(x,1^n)$ défini par :

- Compléter $x = x^1 ... x^i$ par des bits tirés aléatoirement $r^{i+1}, ..., r^n$
- Si D$(x^1 ... x^i r^{i+1} ... r^n) = 1$, renvoyer r^{i+1}
- Sinon, renvoyer $\overline{r^{i+1}}$

Démonstration.

Fixons $i \in [\![0, n-1]\!]$.

Alors, $\mathbb{P}[r^i = X_n^i] = \frac{1}{2}$, et :

$$\begin{aligned}
\mathbb{P}\left[A\left(X_n^{\leq i}, 1^n\right) = X_n^{i+1}\right] &= \mathbb{P}\left[D\left(X_n^1 ... X_n^i r^{i+1} ... r^n\right) = 1 \text{ et } r^{i+1} = X_n^{i+1}\right] \\
&+ \mathbb{P}\left[D\left(X_n^1 ... X_n^i r^{i+1} ... r^n\right) = 0 \text{ et } r^{i+1} = \overline{X_n^{i+1}}\right] \\
&= \frac{1}{2}\mathbb{P}\left[D\left(X_n^1 ... X_n^i X_n^{i+1} r^{i+2} ... r^n\right) = 1\right] \\
&+ \frac{1}{2}\left(1 - \mathbb{P}\left[D\left(X_n^1 ... X_n^i \overline{X_n^{i+1}} r^{i+2} ... r^n\right) = 1\right]\right)
\end{aligned}$$

Démonstration.

Or
$$\begin{aligned}
&\mathbb{P}\left[\mathsf{D}\left(\mathsf{X}_n^1 \ldots \mathsf{X}_n^i r^{i+1} \ldots r^n\right) = 1\right] \\
&\quad = \frac{1}{2}\mathbb{P}\left[\mathsf{D}\left(\mathsf{X}_n^1 \ldots \mathsf{X}_n^i \mathsf{X}_n^{i+1} r^{i+2} \ldots r^n\right) = 1\right] \\
&\quad + \frac{1}{2}\mathbb{P}\left[\mathsf{D}\left(\mathsf{X}_n^1 \ldots \mathsf{X}_n^i \overline{\mathsf{X}_n^{i+1}} r^{i+2} \ldots r^n\right) = 1\right]
\end{aligned}$$

Donc
$$\begin{aligned}
&\mathbb{P}\left[\mathsf{A}\left(\mathsf{X}_n^{\leq i}, 1^n\right) = \mathsf{X}_n^{i+1}\right] \\
&\quad = \frac{1}{2} + \mathbb{P}\left[\mathsf{D}\left(\mathsf{X}_n^1 \ldots \mathsf{X}_n^{i+1} r^{i+2} \ldots r^n\right) = 1\right] \\
&\quad - \mathbb{P}\left[\mathsf{D}\left(\mathsf{X}_n^1 \ldots \mathsf{X}_n^i r^{i+1} \ldots r^n\right) = 1\right]
\end{aligned}$$

Démonstration.

Alors
$$\begin{aligned}\mathbb{P}\left[A\left(X_n^{\leq \pi(X_n)}, 1^n\right) = X_n^{\pi(X_n)+1}\right] &= \sum_{i=0}^{n-1} \mathbb{P}[A(X_n^{\leq i}, 1^n) = X_n^{i+1}]\frac{1}{n} \\ &= \frac{1}{2} + \frac{1}{n}\left(\mathbb{P}\left[D\left(X_n^1 ... X_n^n\right) = 1\right] - \mathbb{P}\left[D\left(r^1 ... r^n\right) = 1\right]\right)\end{aligned}$$

Donc
$$\begin{aligned}|\mathbb{P}\left[D\left(X_n\right) = 1\right] - \mathbb{P}\left[D\left(U_n\right) = 1\right]| &= n\left|\mathbb{P}\left[A\left(X_n^{\leq \pi(X_n)}, 1^n\right) = X_n^{\pi(X_n)+1}\right] - \frac{1}{2}\right| \\ &\leq n\mu(n) \text{ qui est négligeable.}\end{aligned}$$

□

Définition.

*Un **générateur pseudo-aléatoire** est un algorithme déterministe efficace* $\mathsf{G} : \{0,1\}^* \to \{0,1\}^*$ *où :*

- G *étire son entrée :* $\forall x \in \{0,1\}^*$, $|\mathsf{G}(x)| = l(|x|)$, *où* $l : \mathbb{N} \to \mathbb{N}$ *avec* $l(n) > n$ *pour tout* n
- *La suite* $(\mathsf{X}_{l(n)})_n := (\mathsf{G}(\mathsf{U}_n))_n$ *est pseudo-aléatoire*

Existe-t-il un générateur pseudo-aléatoire ?

On ne sait pas.

Théorème.

S'il existe un générateur pseudo-aléatoire, alors $\mathsf{P} \neq \mathsf{NP}$.