Comment produire des nombres vraiment aléatoires ?

Arnaud Tisserand

CNRS, IRISA, équipe-projet CAIRN

Fête de la science, octobre 2011






Plan de l'exposé

- Définition
  Qu'est-ce que c'est ?
- Domaines d'utilisation
  À quoi ça sert ?
- Générateurs de nombres aléatoires
  Comment produire des nombres aléatoires ?
- Exemples de générateurs de nombres vraiment aléatoires
  Quelles solutions dans l'histoire et maintenant ?
- Notre solution
  Comment et pourquoi nos travaux de recherche ?

Définition du mot (adjectif) *aléatoire*

dictionnaire	définition
petit Larousse (2002)	qui relève du hasard qui dépend d'un événement incertain
CNRTL `http://www.cnrtl.fr/`	ce qui est soumis à un aléa
Littré	soumis aux chances du hasard

Étymologie : du latin *aleatorius*, de *alea*, hasard, jeu de dés

Dictionnaires en ligne : `http://www.lexilogos.com/`

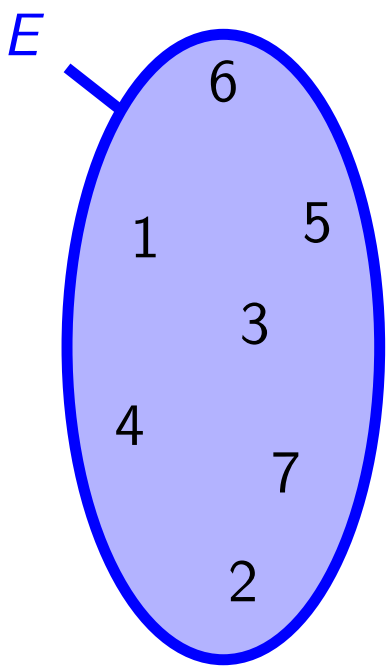
Synonymes et antonymes du mot (adjectif) *aléatoire*

Synonymes : hasardeux, incertain, risqué, chanceux, hasardé, dangereux, aventureux, problématique, éventuel, périlleux, hypothétique, douteux, contingent, arbitraire, aventuré, casuel, improbable, précaire, stochastique

Antonymes : assuré, certain, déterminé, infaillible, palpable, sûr

Source : `http://www.cnrtl.fr/`

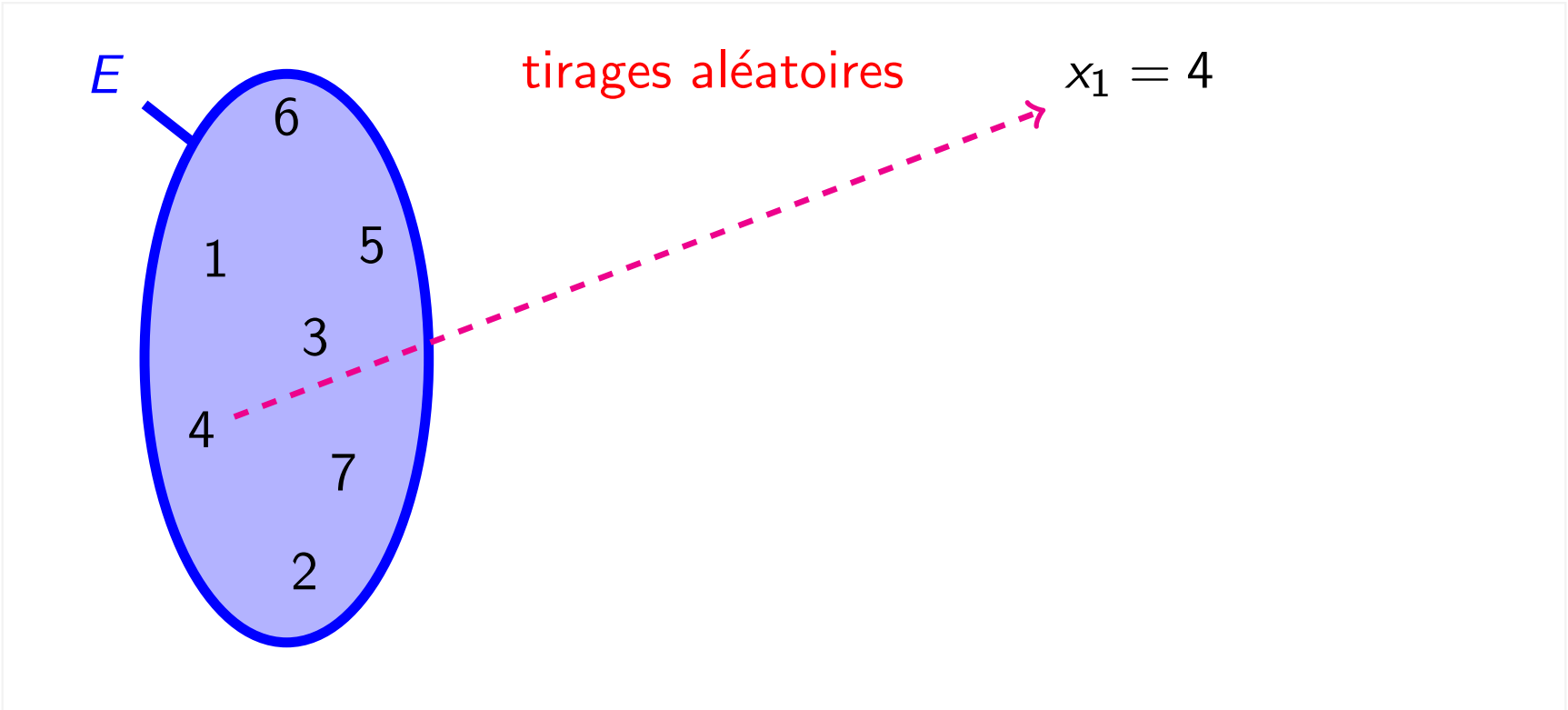
Définition plus « mathématique » des nombres aléatoires



tirages aléatoires

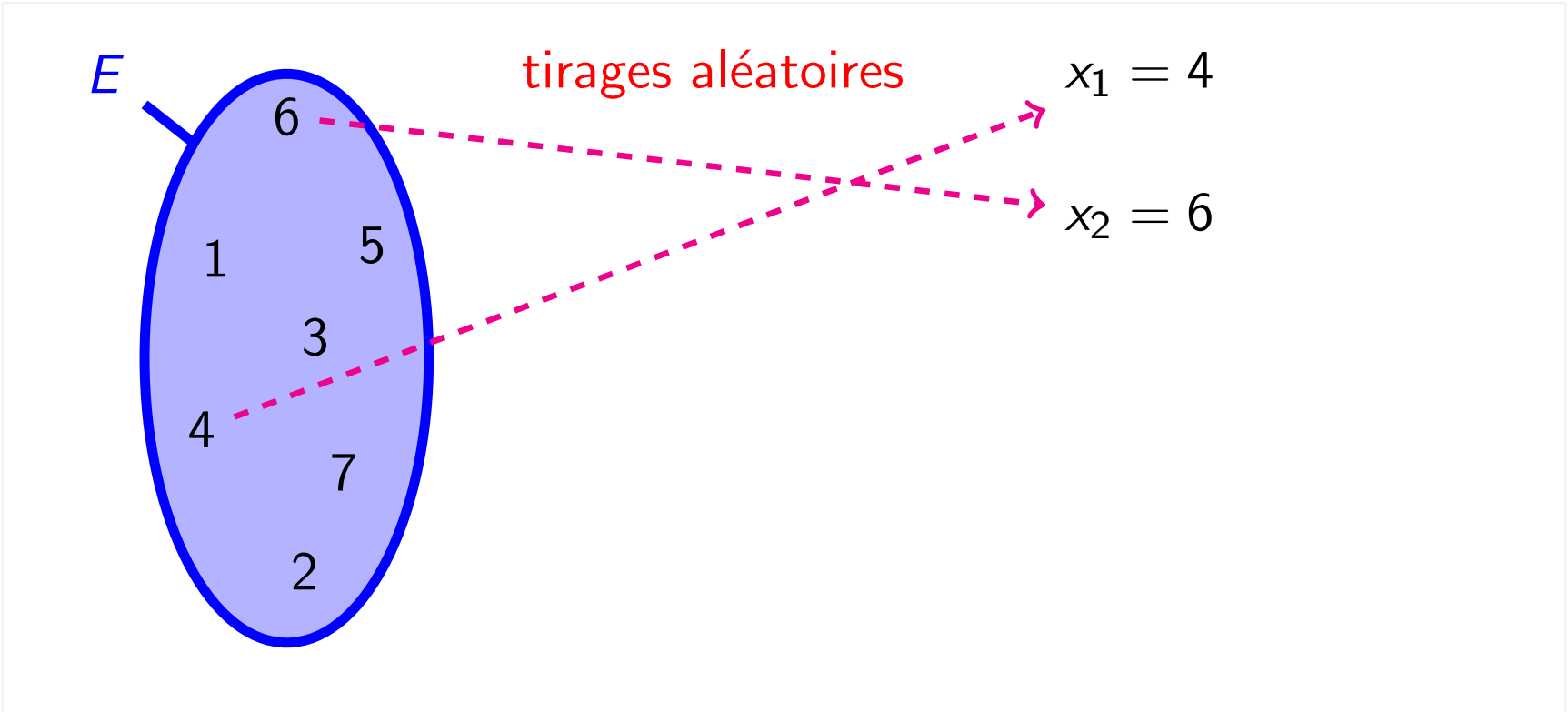
- E ensemble (fini) de nombres, la taille de E est n

Définition plus « mathématique » des nombres aléatoires



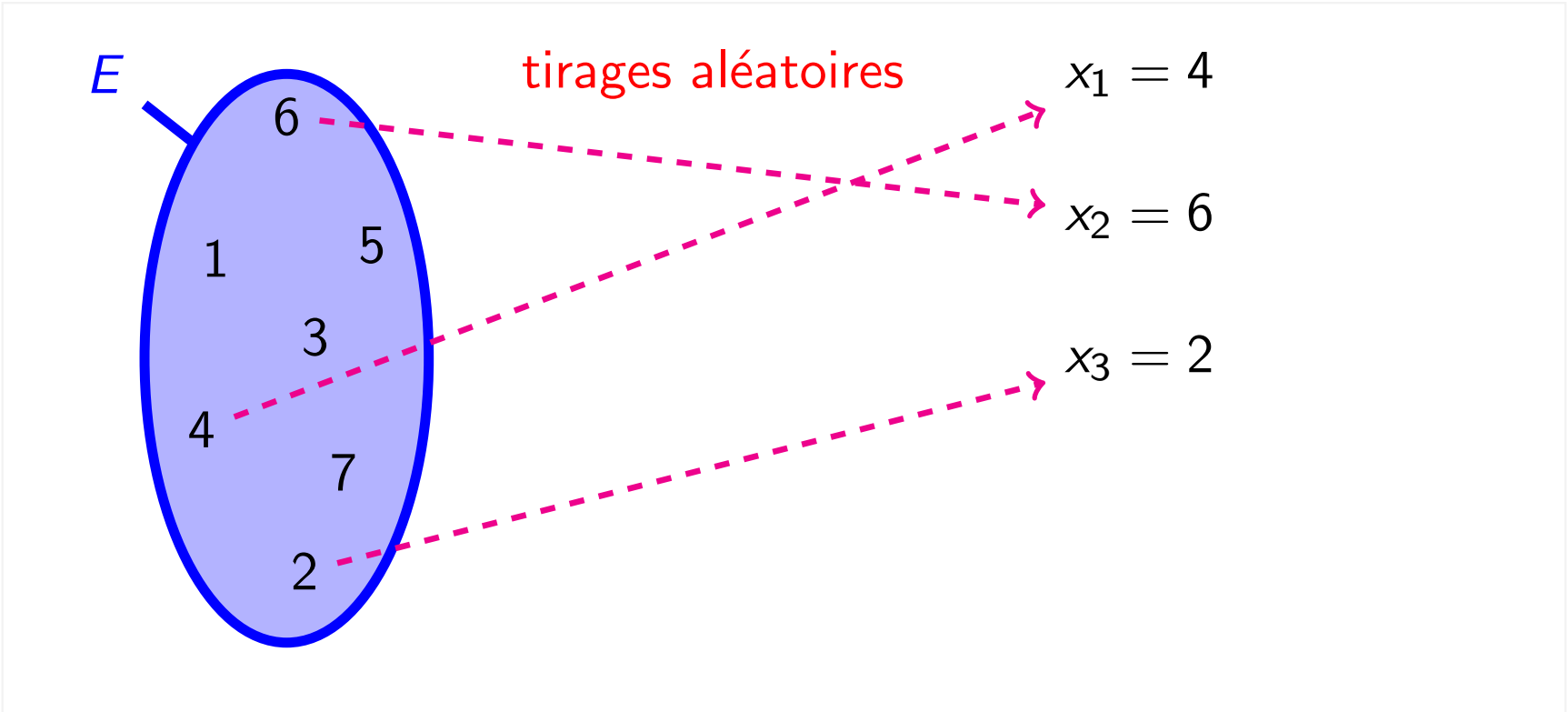
- E ensemble (fini) de nombres, la taille de E est n
- x_i les nombres tirés aléatoirement

Définition plus « mathématique » des nombres aléatoires



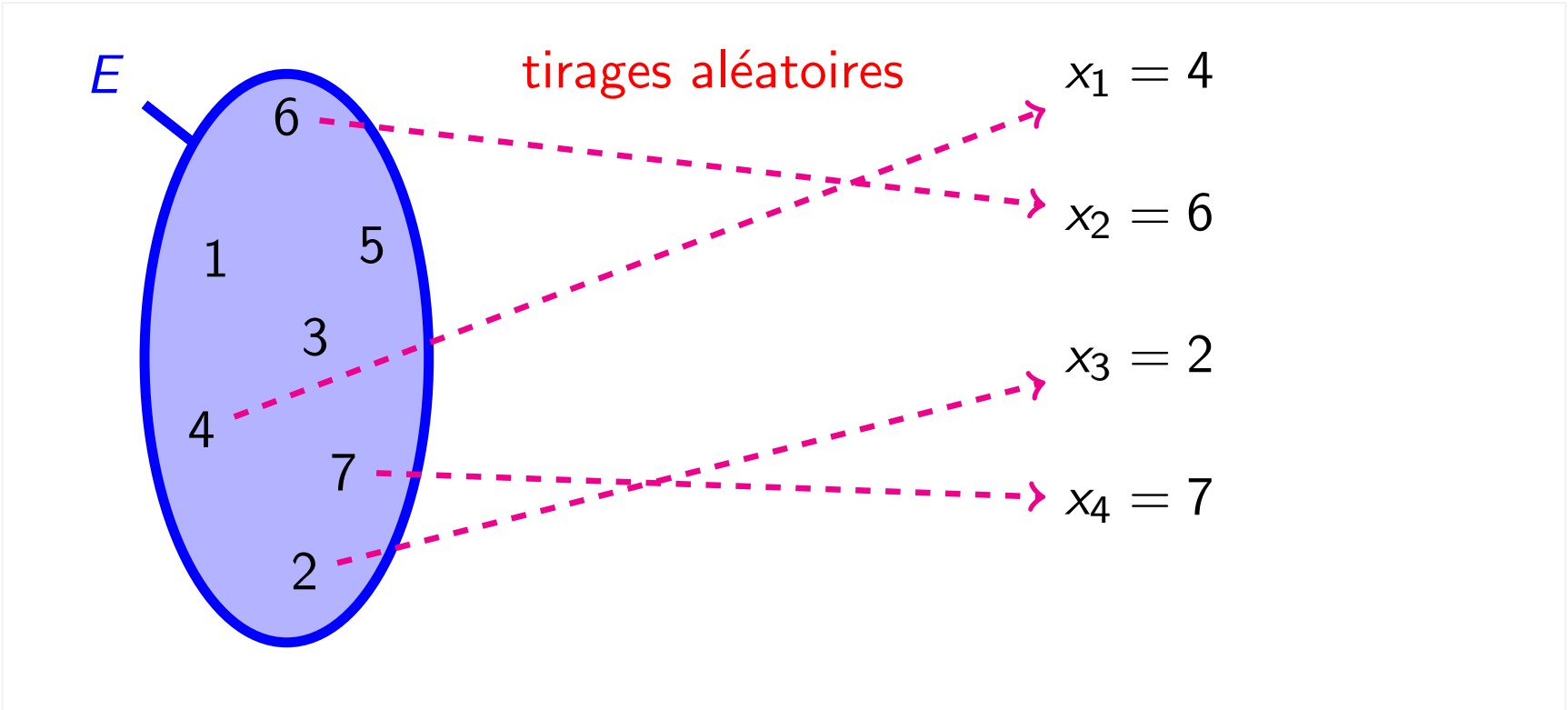
- E ensemble (fini) de nombres, la taille de E est n
- x_i les nombres tirés aléatoirement

Définition plus « mathématique » des nombres aléatoires



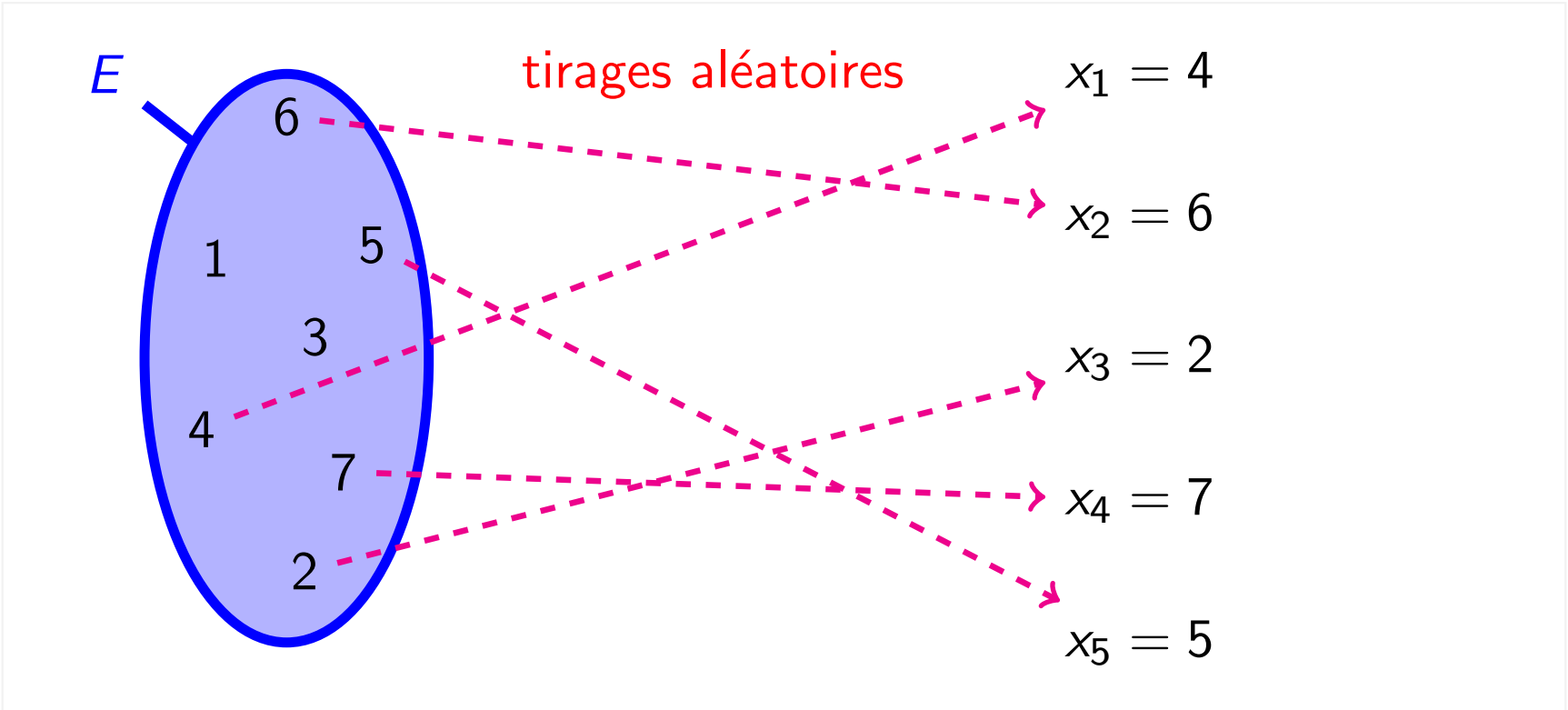
- E ensemble (fini) de nombres, la taille de E est n
- x_i les nombres tirés aléatoirement

Définition plus « mathématique » des nombres aléatoires



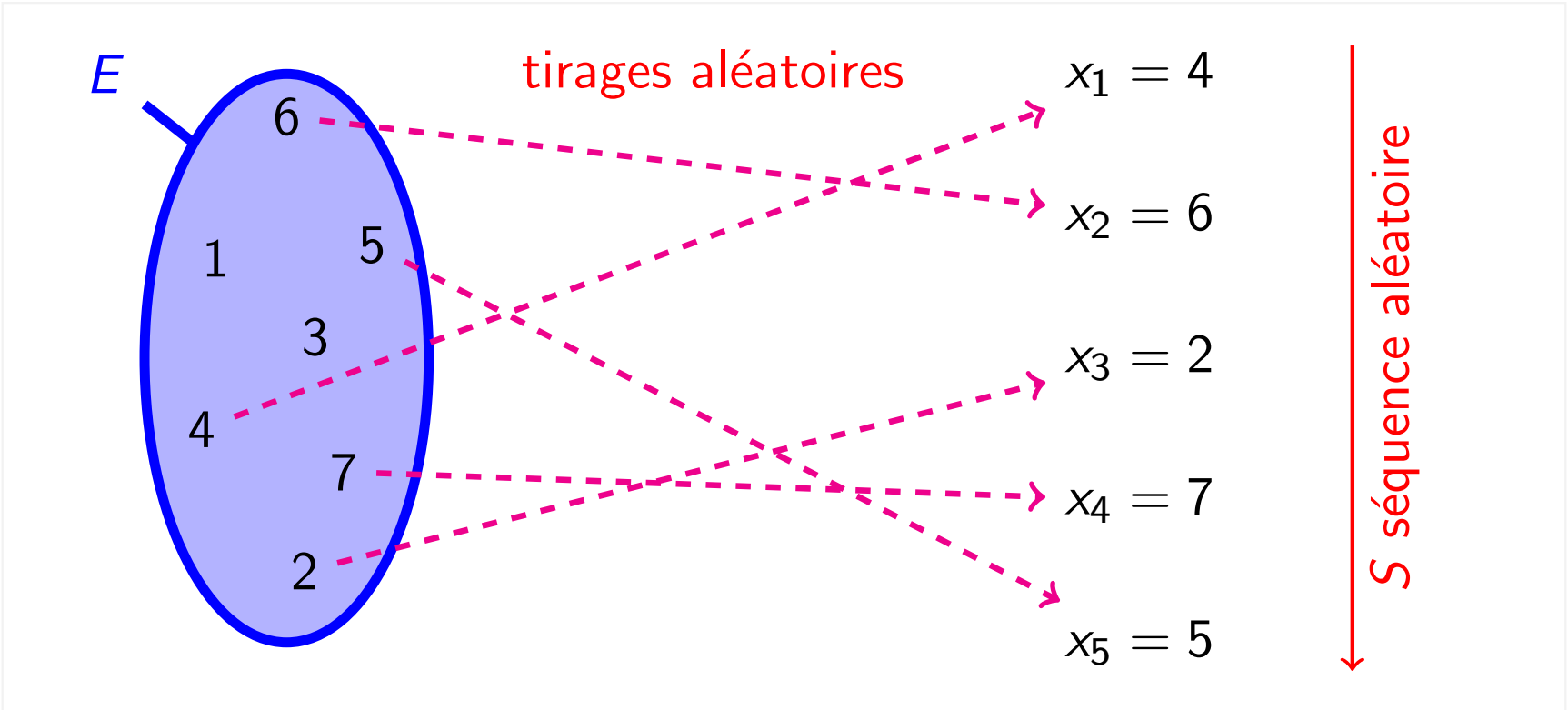
- E ensemble (fini) de nombres, la taille de E est n
- x_i les nombres tirés aléatoirement

Définition plus « mathématique » des nombres aléatoires



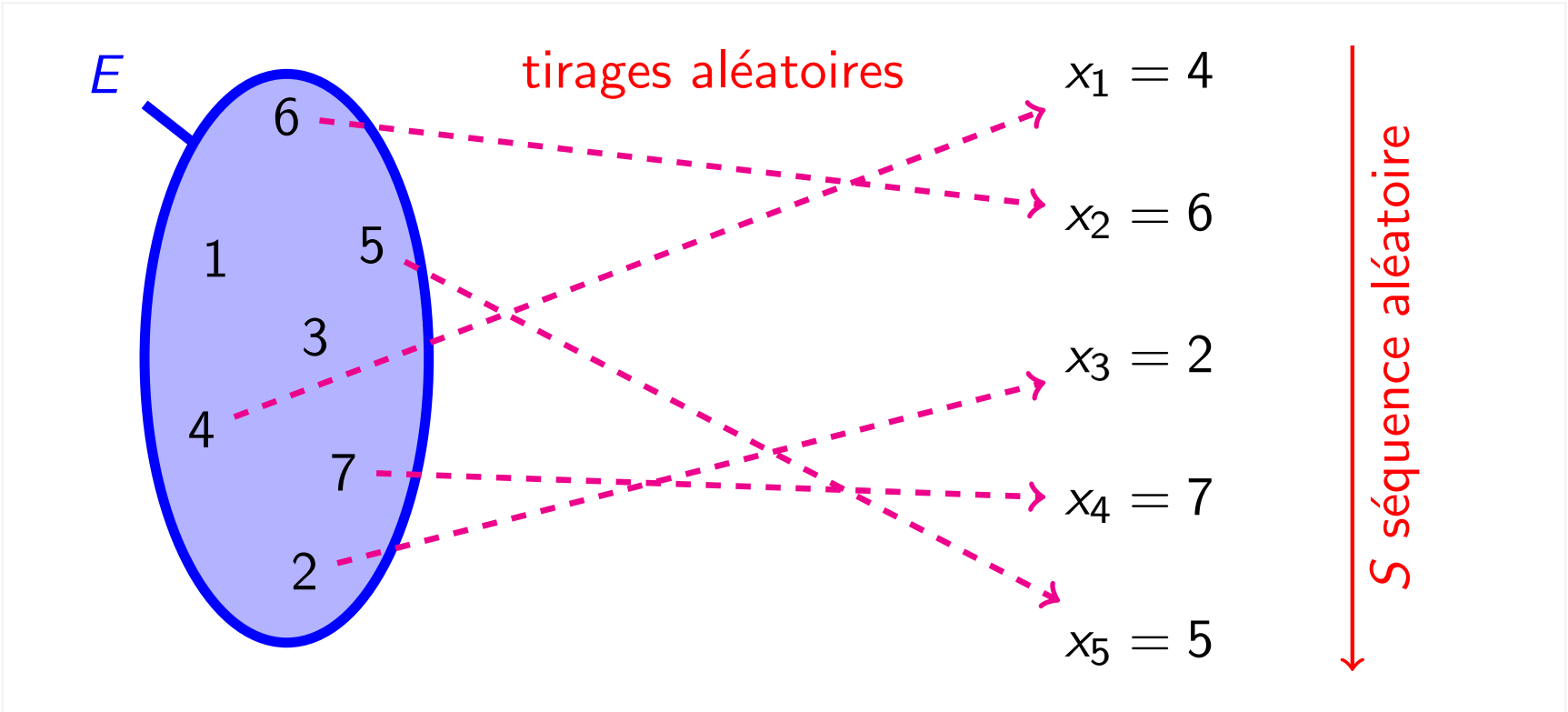
- E ensemble (fini) de nombres, la taille de E est n
- x_i les nombres tirés aléatoirement

Définition plus « mathématique » des nombres aléatoires



- E ensemble (fini) de nombres, la taille de E est n
- x_i les nombres tirés aléatoirement
- S séquence (ou suite) aléatoire de nombres

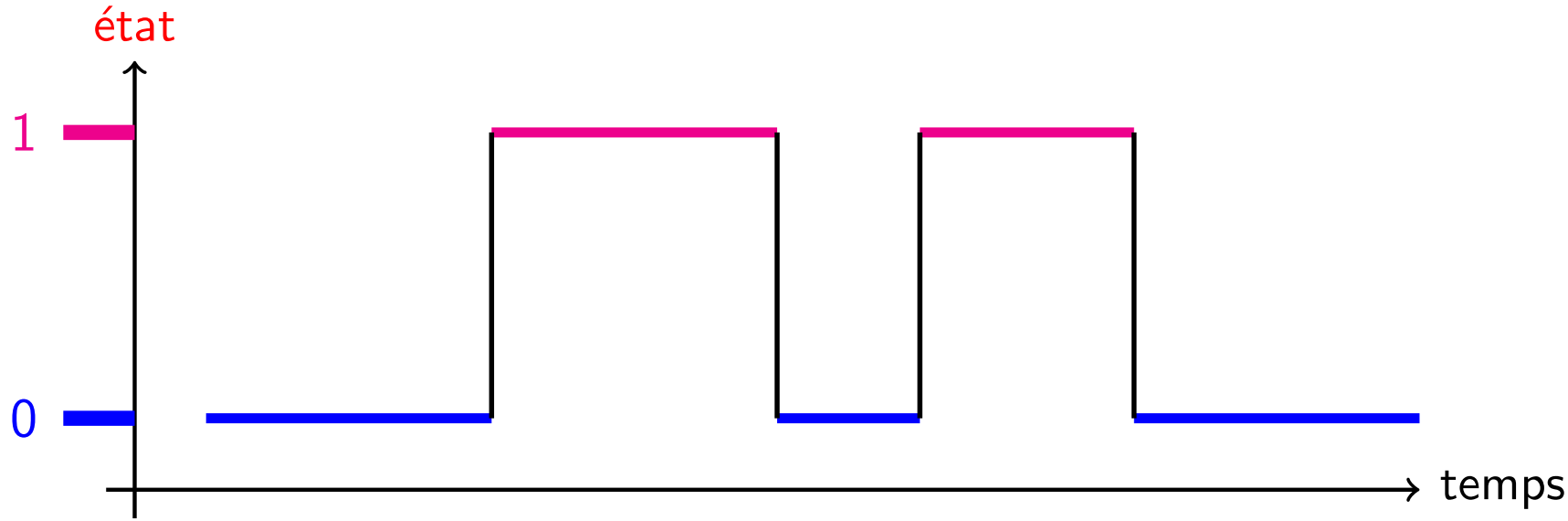
Définition plus « mathématique » des nombres aléatoires



- E ensemble (fini) de nombres, la taille de E est n
- x_i les nombres tirés aléatoirement
- S séquence (ou suite) aléatoire de nombres
- S de bonne qualité : probabilité$(x_i = k) = \frac{1}{n}$ pour tout k dans E

Séquences aléatoires dans une puce électronique

Deux états (électriques) possibles sur un fil : 0 et 1 (code binaire)



Condition d'un aléa de « bonne qualité » (équiprobabilité) :

$$\text{Proba}(x_i = 0) \quad = \quad \text{Proba}(x_i = 1) \quad = \quad \frac{1}{2}$$

Vers une définition un peu plus précise

Une séquence est aléatoire quand les nombres sont :

- équiprobables

  50 % de chance d'avoir 0 ou 1

Vers une définition un peu plus précise

Une séquence est aléatoire quand les nombres sont :

- équiprobables
  50 % de chance d'avoir 0 ou 1
- uniformément distribués
  la probabilité est la même dans le temps pour chaque tirage

Vers une définition un peu plus précise

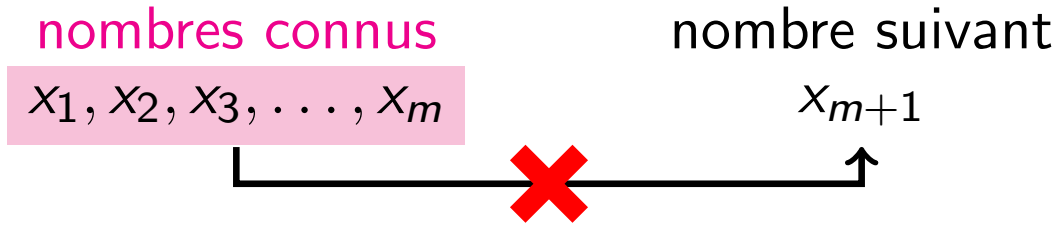
Une séquence est aléatoire quand les nombres sont :

- équiprobables
  50 % de chance d'avoir 0 ou 1
- uniformément distribués
  la probabilité est la même dans le temps pour chaque tirage
- statistiquement indépendants

Vers une définition un peu plus précise

Une séquence est aléatoire quand les nombres sont :

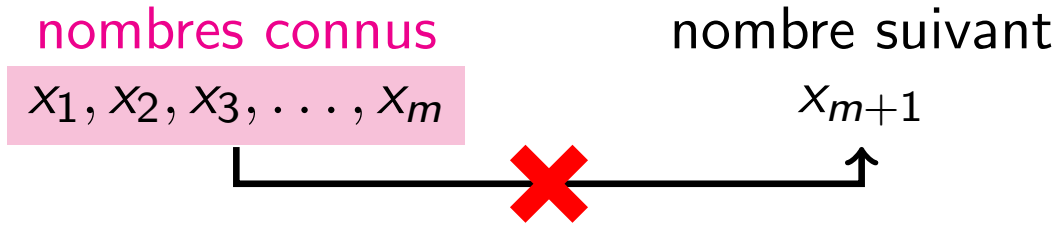
- équiprobables
  50 % de chance d'avoir 0 ou 1
- uniformément distribués
  la probabilité est la même dans le temps pour chaque tirage
- statistiquement indépendants
- non prédictibles



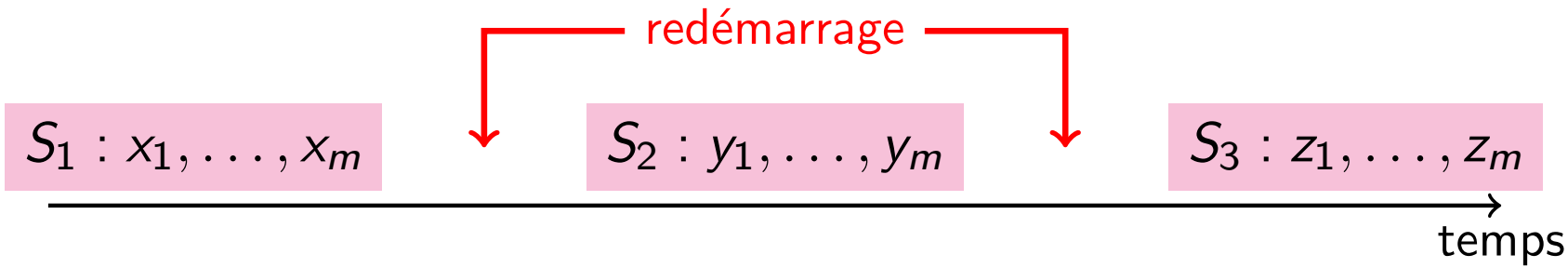
Vers une définition un peu plus précise

Une séquence est vraiment aléatoire quand les nombres sont :

- équiprobables
  50 % de chance d'avoir 0 ou 1
- uniformément distribués
  la probabilité est la même dans le temps pour chaque tirage
- statistiquement indépendants
- non prédictibles



- non reproductibles (c.-à-d. $S_1 \neq S_2 \neq S_3$)

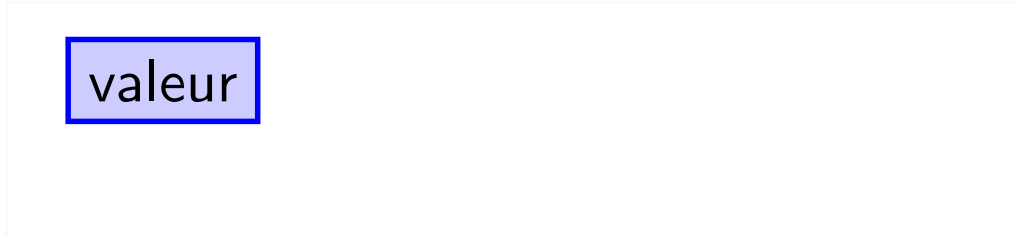


Domaines d'utilisation des nombres aléatoires

- Loteries
- Jeux vidéo
- Cryptographie et sécurité
- Communications numériques
- Simulation numérique
- Informatique (algorithmes « randomisés »)
- ...

Générateurs de nombres aléatoires

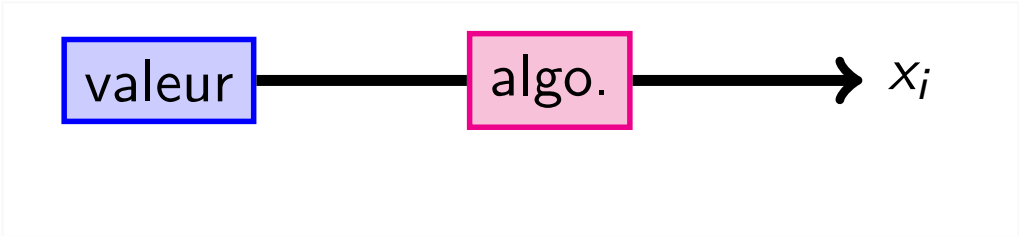
- Générateur pseudo aléatoire : (*PRNG en anglais*)



Principe : algorithme (programme) informatique/mathématique
Avantages : très rapide et simple à utiliser
Inconvénient : déterministe (prédictible dans certains cas)

Générateurs de nombres aléatoires

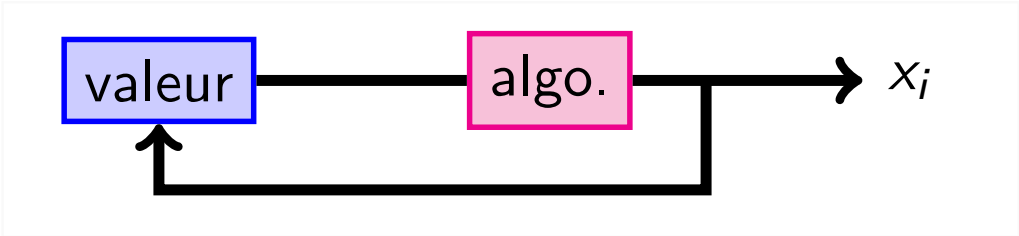
- Générateur pseudo aléatoire : (*PRNG en anglais*)



Principe : algorithme (programme) informatique/mathématique
Avantages : très rapide et simple à utiliser
Inconvénient : déterministe (prédictible dans certains cas)

Générateurs de nombres aléatoires

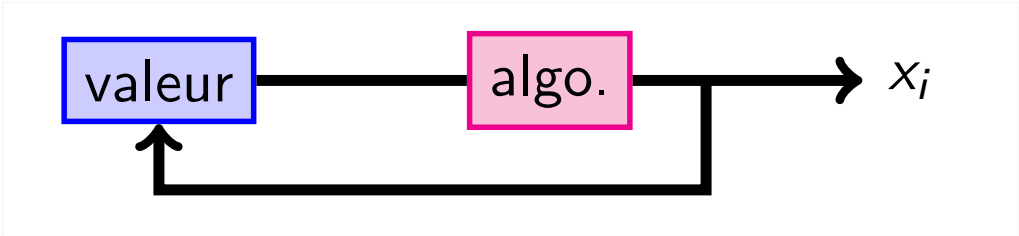
- Générateur pseudo aléatoire : (*PRNG en anglais*)



Principe : algorithme (programme) informatique/mathématique
Avantages : très rapide et simple à utiliser
Inconvénient : déterministe (prédictible dans certains cas)

Générateurs de nombres aléatoires

- Générateur pseudo aléatoire : (*PRNG en anglais*)



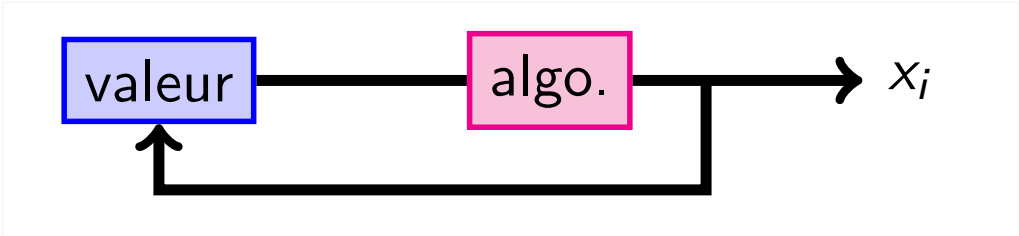
Principe : algorithme (programme) informatique/mathématique
Avantages : très rapide et simple à utiliser
Inconvénient : déterministe (prédictible dans certains cas)

- Générateur vraiment aléatoire : (*TRNG en anglais*)

Principe : source physique de bruit
Avantage : non déterministe $\Longrightarrow$ vraiment aléatoire
Inconvénients : lent et intégration complexe

Générateurs de nombres aléatoires

- Générateur pseudo aléatoire : (*PRNG en anglais*)



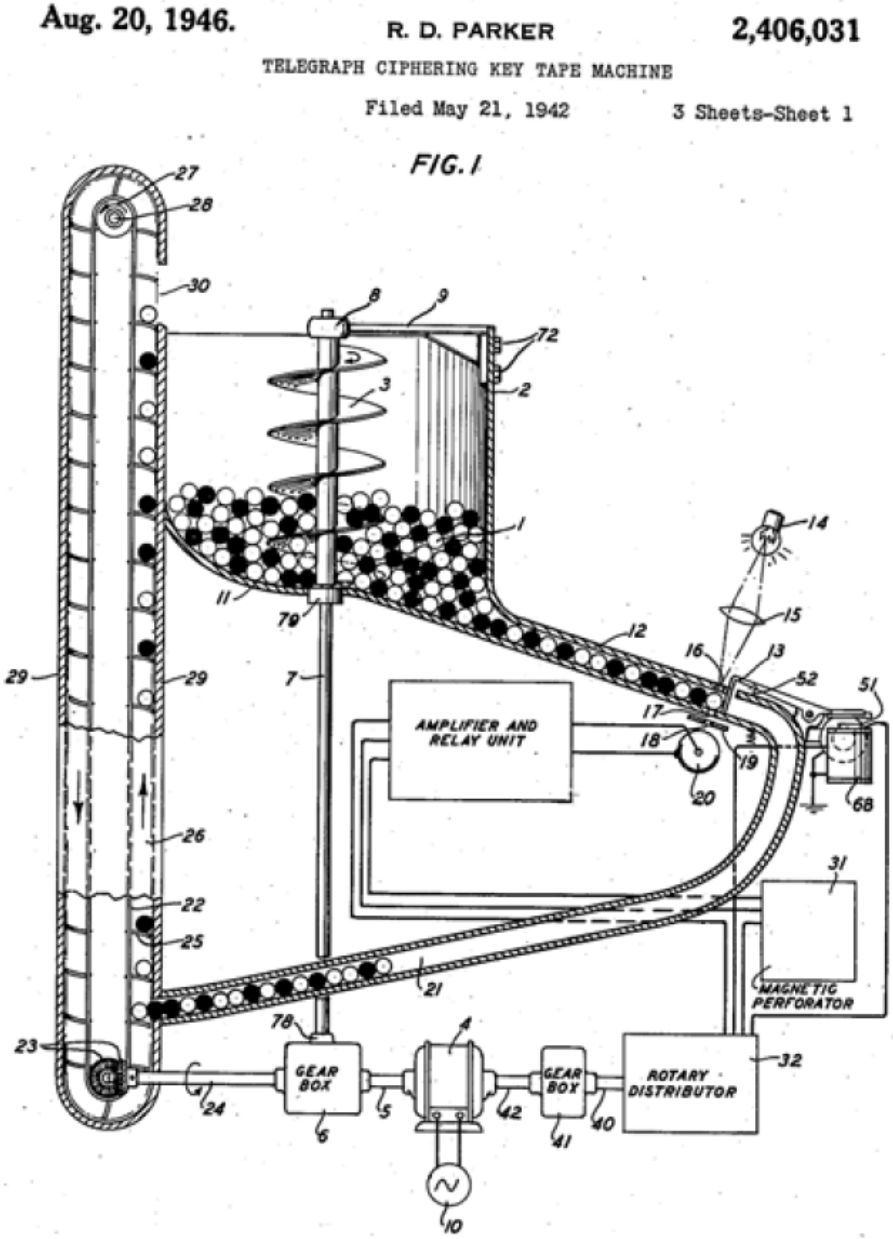
Principe : algorithme (programme) informatique/mathématique
Avantages : très rapide et simple à utiliser
Inconvénient : déterministe (prédictible dans certains cas)

- Générateur vraiment aléatoire : (*TRNG en anglais*)

Principe : source physique de bruit
Avantage : non déterministe $\Longrightarrow$ vraiment aléatoire
Inconvénients : lent et intégration complexe

- Générateur hybride : TRNG → PRNG → sortie

Exemples de générateurs de nombres vraiment aléatoires

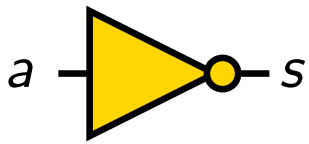


Sources de bruit physique

- Phénomènes quantiques
- Désintégration radioactive
- Bruits atmosphériques et thermiques
- Circuits électroniques : gigue de phase d'oscillateurs libres, méta-stabilité, $1/f$, *shot*, popcorn...

Notre solution : éléments électroniques

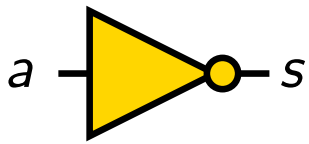
- Inverseur :



a	0	1
s	1	0

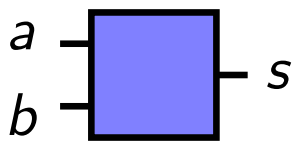
Notre solution : éléments électroniques

- Inverseur :



a	0	1
s	1	0

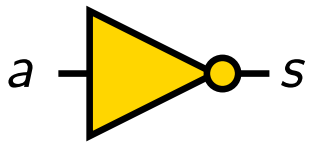
- XOR :



a	0	0	1	1
b	0	1	0	1
s	0	1	1	0

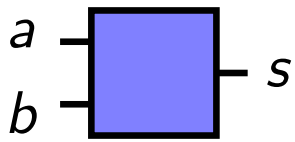
Notre solution : éléments électroniques

- Inverseur :



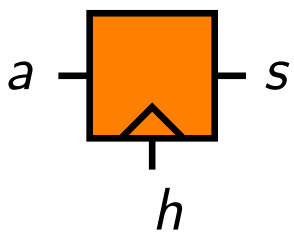
a	0	1
s	1	0

- XOR :



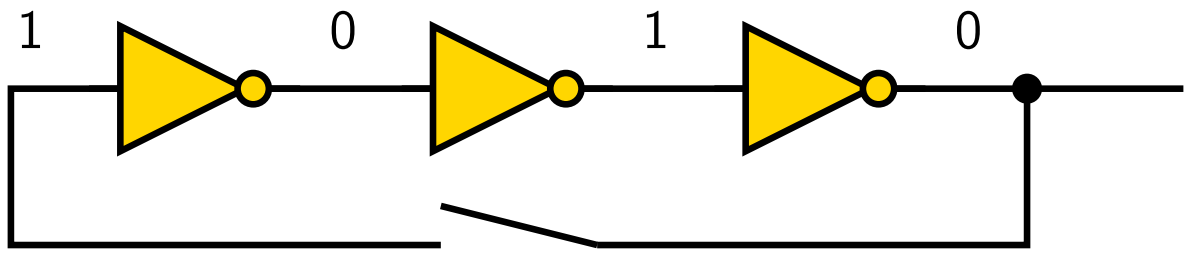
a	0	0	1	1
b	0	1	0	1
s	0	1	1	0

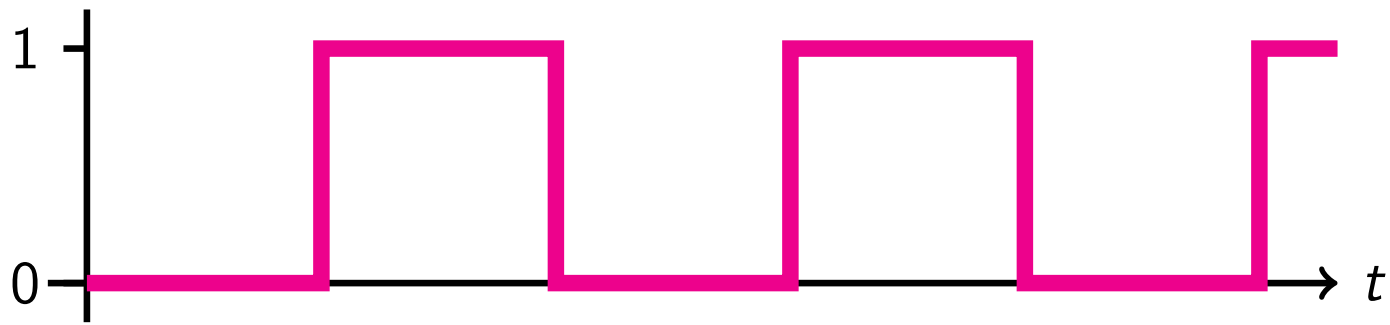
- Bascule :



h passe de 0 à 1 : $s(t+1) = a(t)$

Notre solution : oscillateur en anneau libre

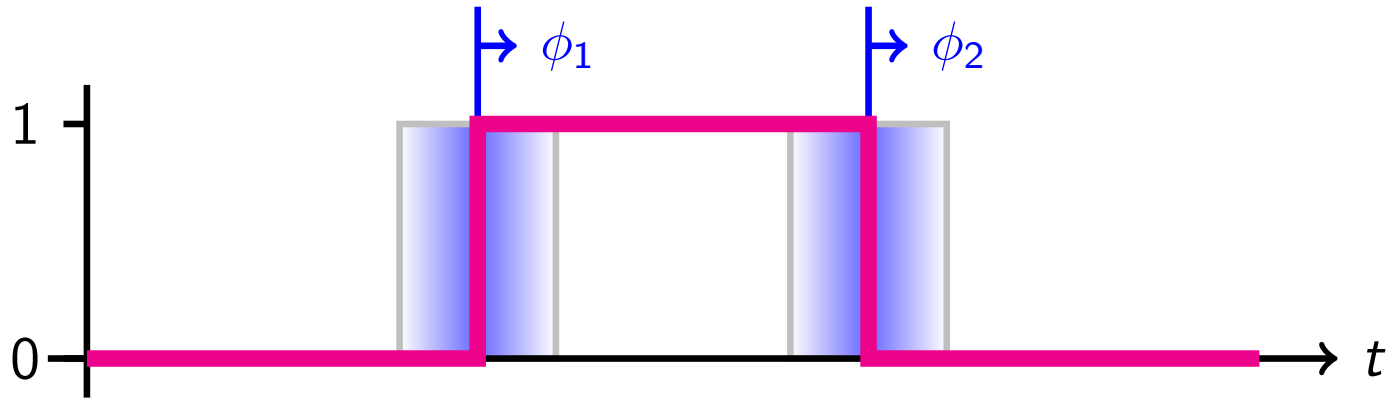




Contrainte : nombre impair d'inverseurs (3,5,7,9,11...)

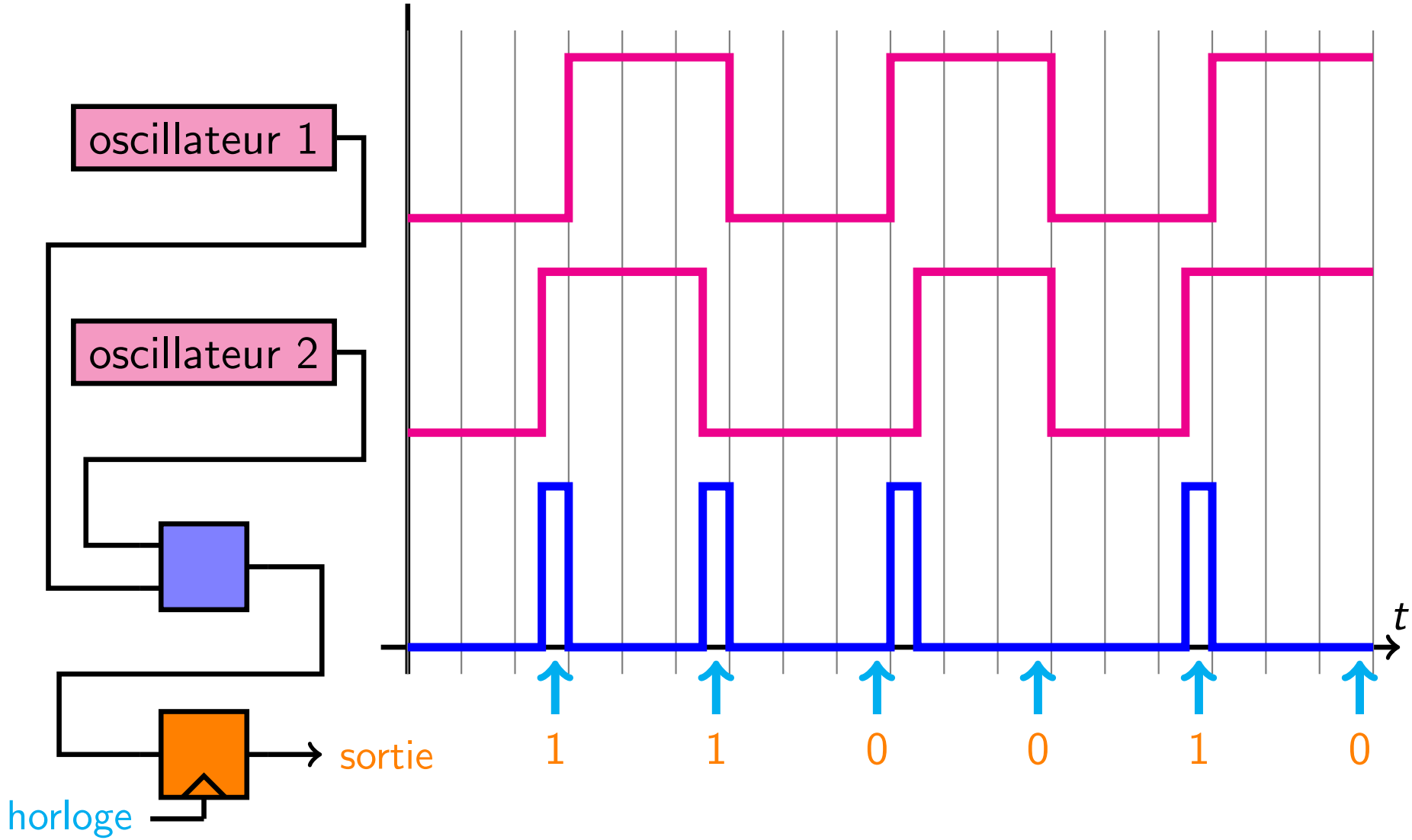
Notre solution : gigue de phase aléatoire

Petit décalage aléatoire des transitions dans le temps



Source de bruit physique interne au circuit

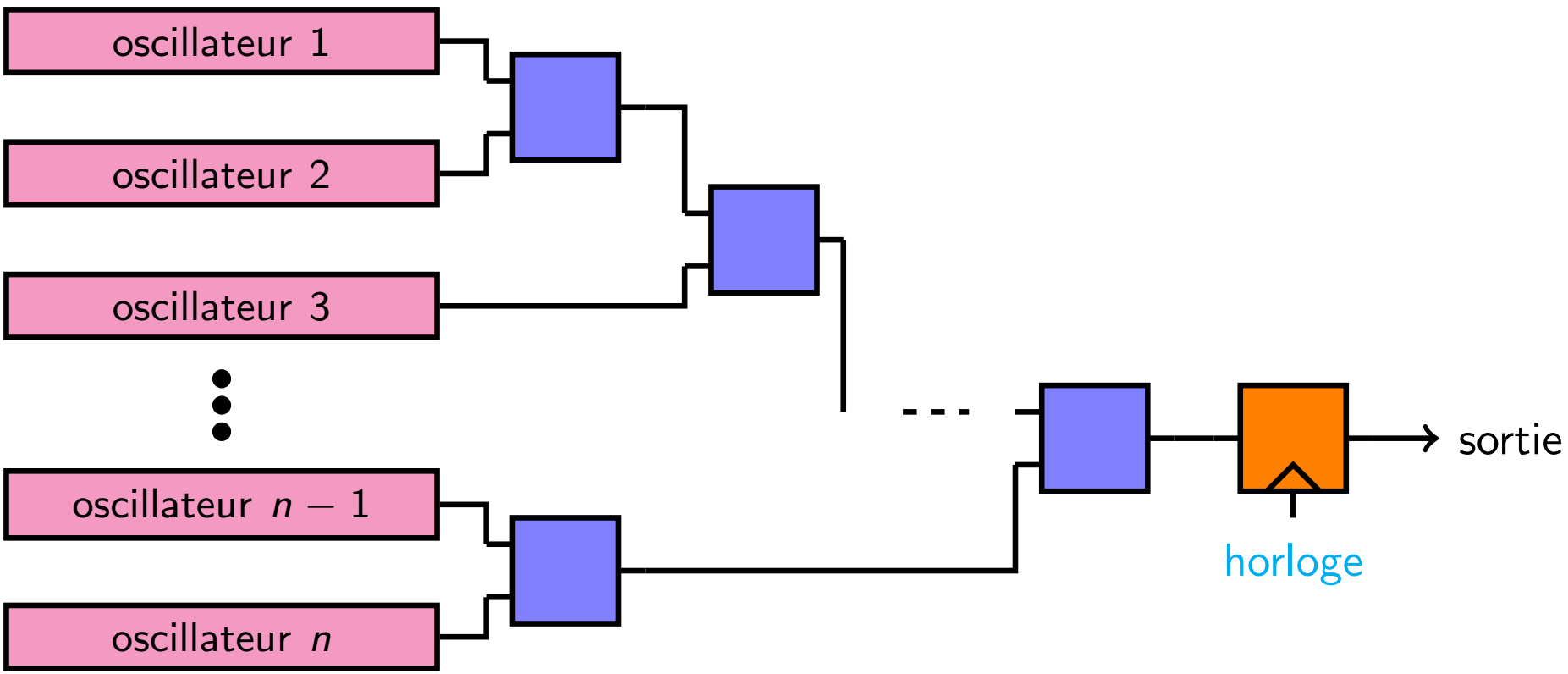
Notre solution : version avec 2 oscillateurs



Remarque : aléa très faible avec seulement 2 oscillateurs

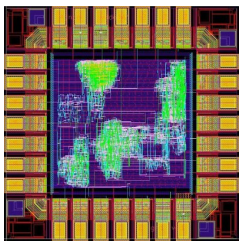
Notre solution

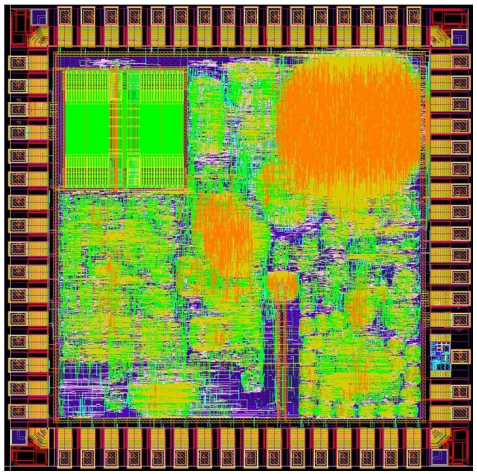
- Utiliser de nombreux oscillateurs libres (≈ 100)
- Composer les différentes sorties avec des portes XOR
- Échantillonner la sortie finale avec une bascule ayant une fréquence fixe (signal d'horloge)



Nos circuits TRNG

- Technologie CMOS 130 nm
- Conception à Lannion
- Fabrication à Grenoble
- Surfaces : 1 et 4 mm^2
- Vitesses : de 150 à 700 MHz





Point fort : surveillance automatique dans le circuit, en temps réel, de la qualité de l'aléa par des tests statistiques (alarme en cas de problème, p. ex. en cas d'attaque physique)

Fin, des questions ?

Contact:

- mailto:arnaud.tisserand@irisa.fr
- http://www.irisa.fr/prive/Arnaud.Tisserand/
- Equipe-projet CAIRN http://www.irisa.fr/cairn/
- Laboratoire IRISA, CNRS–INRIA–Univ. Rennes 1
  6 rue Kérampont, BP 80518, F-22305 Lannion cedex, France

Merci