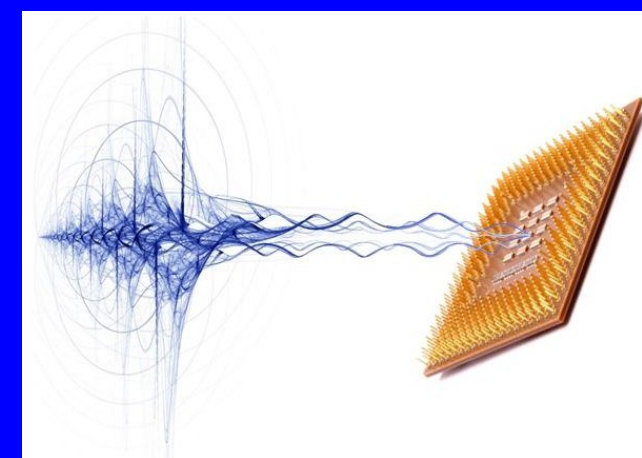


Comment produire des nombres vraiment aléatoires ?

Équipe de recherche CAIRN



1. Utilisations des nombres aléatoires

- ▶ Loteries
- ▶ Jeux vidéo
- ▶ Cryptographie et sécurité
- ▶ Simulation numérique
- ▶ ...



2. Générateurs de nombres aléatoires

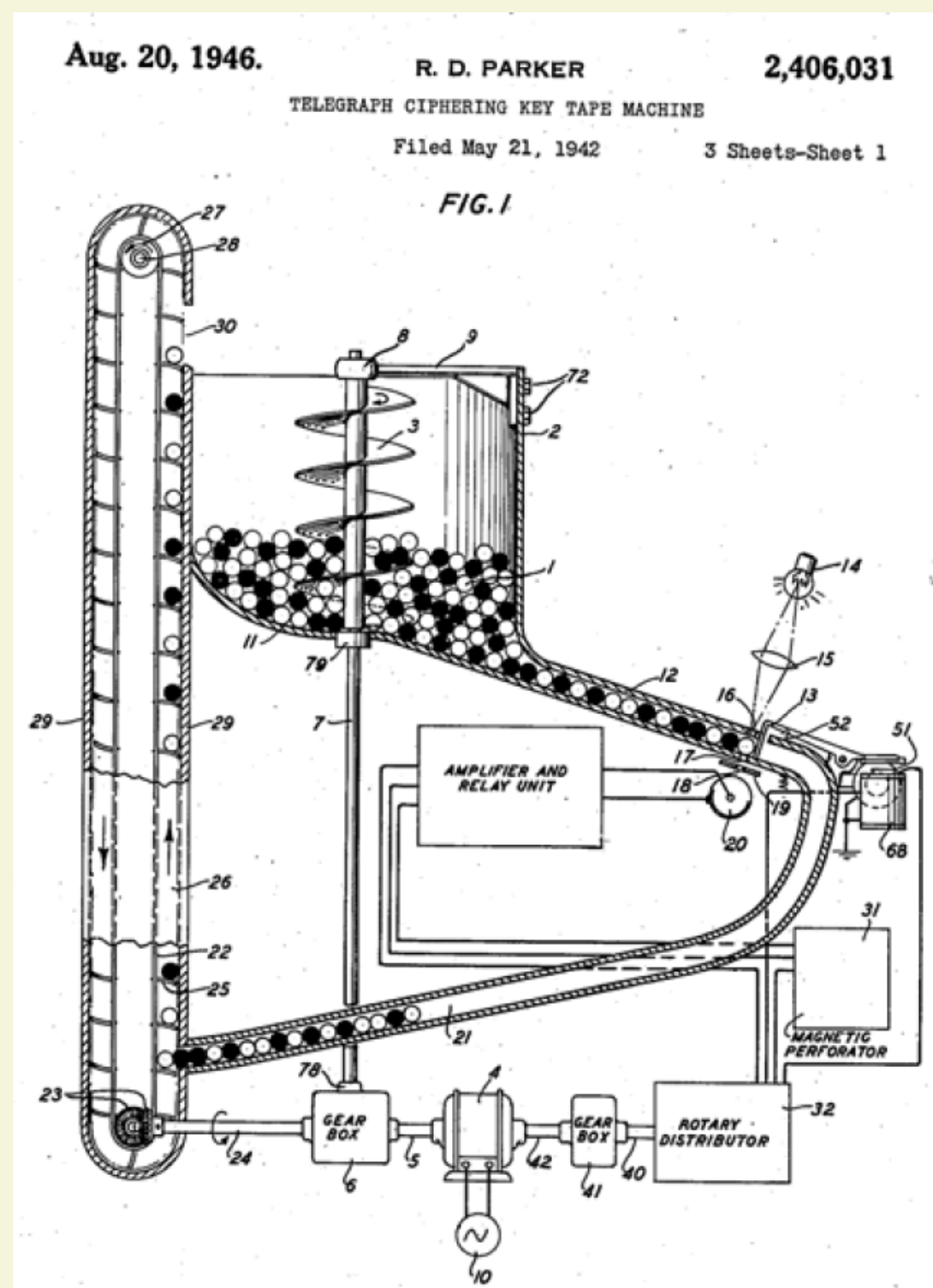
- ▶ Générateur **pseudo** aléatoire : (PRNG en anglais)
Principe : algorithme (programme) mathématique
Avantages : très rapide et simple à utiliser
Inconvénient : déterministe (prédictible dans certains cas)
- ▶ Générateur **vraiment** aléatoire : (TRNG en anglais)
Principe : source physique de bruit
Avantage : non déterministe $\Rightarrow$ vraiment aléatoire
Inconvénients : lent et intégration complexe
- ▶ Générateur **hybride** :



3. Exemples de sources de bruit physique

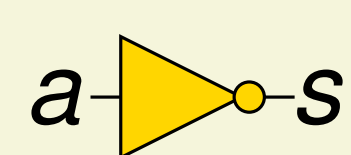
- ▶ Phénomènes quantiques
- ▶ Désintégration radioactive
- ▶ Bruits atmosphériques et thermiques
- ▶ Circuits électroniques : **gigue de phase** d'oscillateurs libres, méta-stabilité, $1/f$, shot, popcorn...

4. Exemples « historiques »



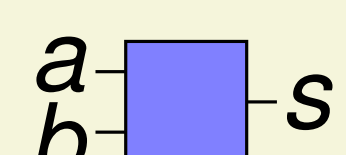
5. Portes logiques utilisées

Inverseur :



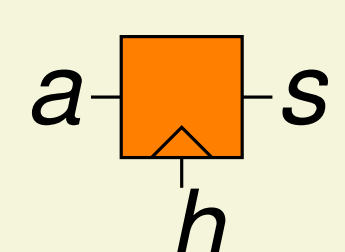
a	0	1
s	1	0

XOR :



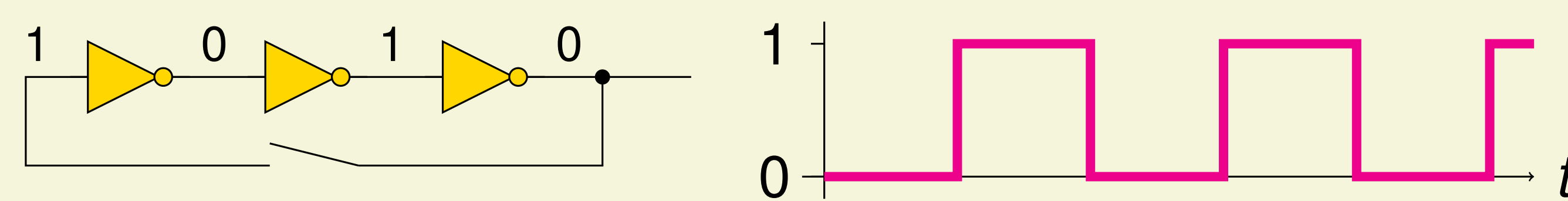
a	0	0	1	1
b	0	1	0	1
s	0	1	1	0

Bascule :



h passe de 0 à 1 :
 $s(t+1) = a(t)$

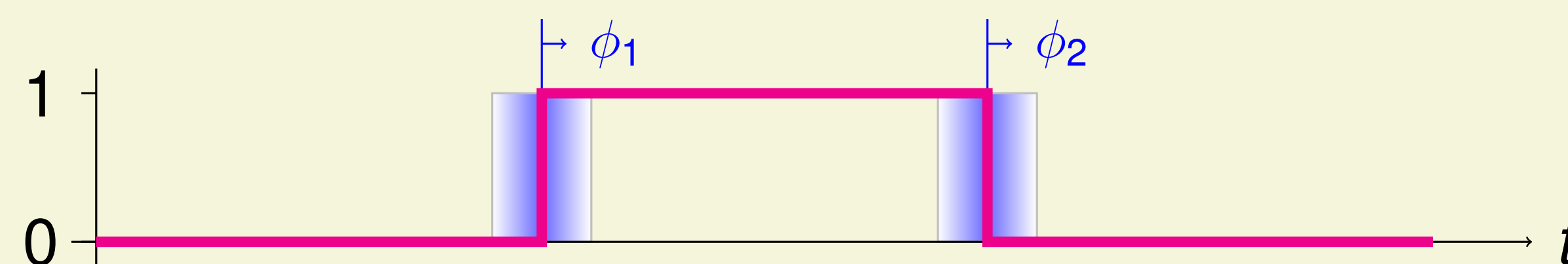
6. Oscillateur en anneau libre



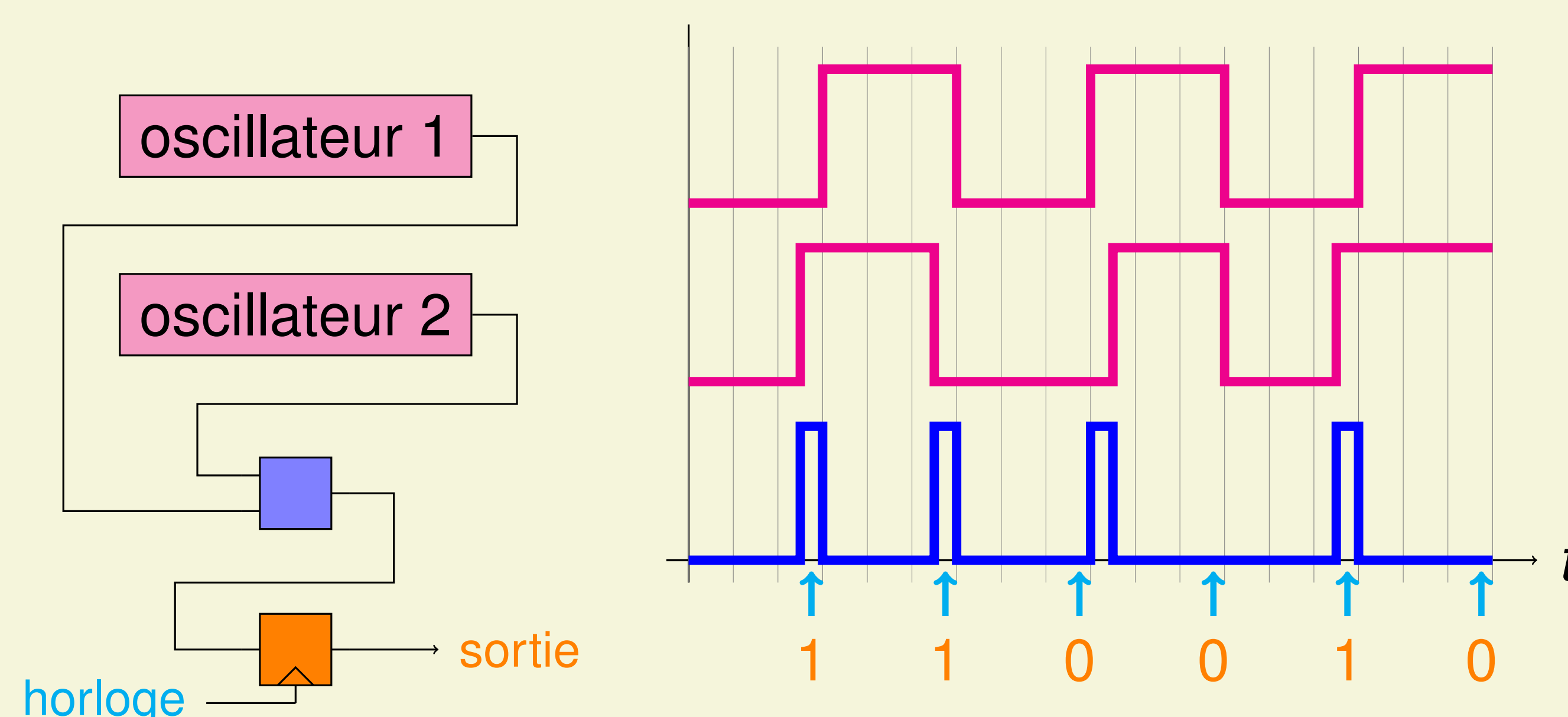
Contrainte : nombre **impair** d'inverseurs (3,5,7,9,11...)

7. Gigue de phase

Petit décalage **aléatoire** des **transitions** dans le temps



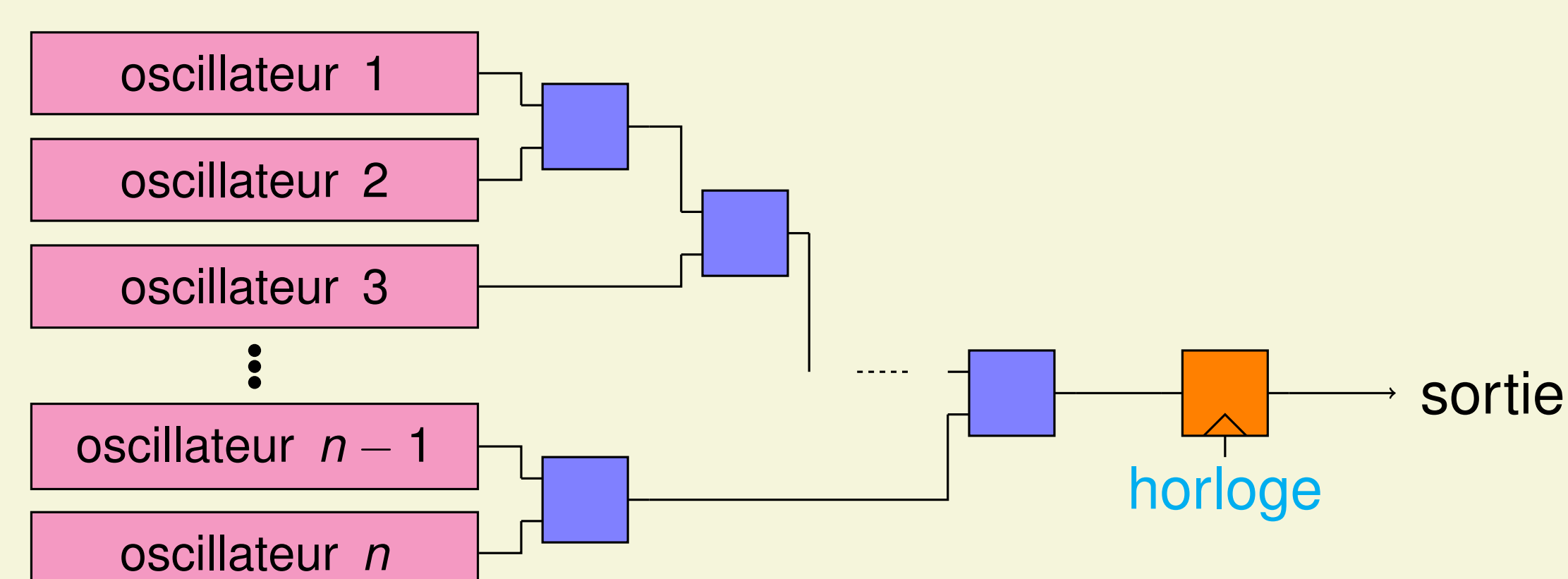
8. Illustration du principe



Remarque : aléa limité avec seulement 2 oscillateurs

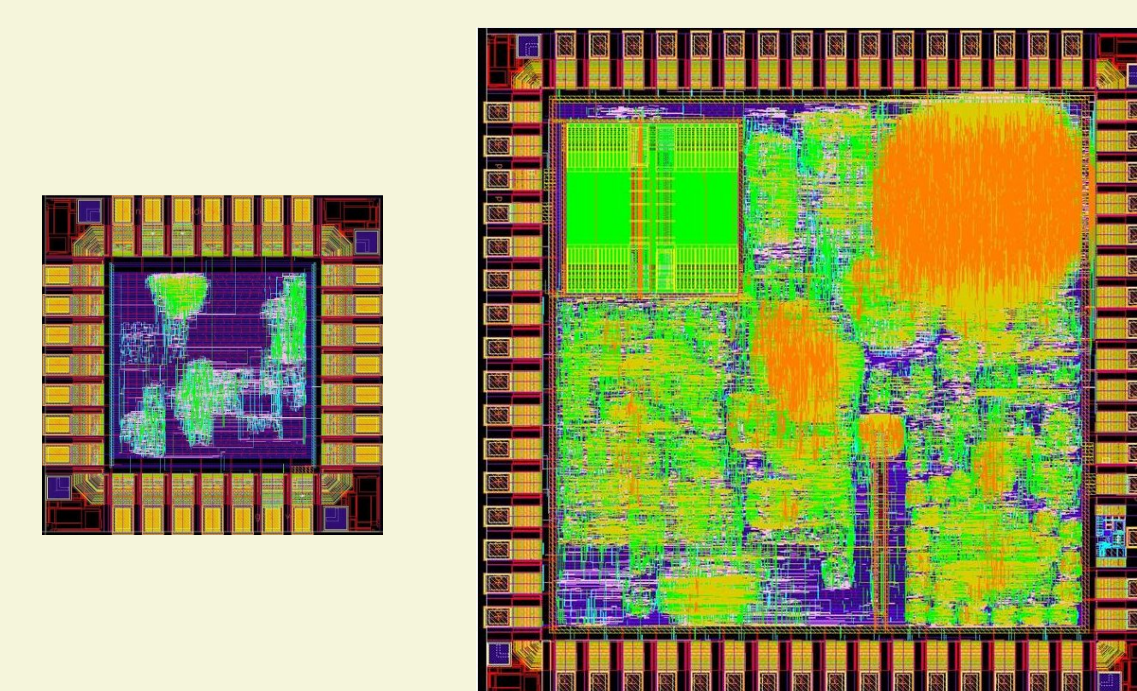
9. TRNG à base d'oscillateurs libres

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



10. Nos circuits intégrés TRNG

- ▶ Technologie CMOS 130 nm
- ▶ Conception à Lannion
- ▶ Fabrication à Grenoble
- ▶ Surfaces : 1 et 4 mm²
- ▶ 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)

<http://www.irisa.fr/cairn/>