rateur aléatoire cryptographique sûr». Est sûr un générateur dont la période est trop grande pour être explorée exhaustivement, et tel qu'en plus les moyens exigés pour mener une analyse conduisant à en prévoir le comportement sont inacceptablement coûteux.

Il faut remarquer qu'en cryptographie on accepte parfois qu'un générateur ne soit pas uniforme (par exemple, qu'il donne 45 pour cent de '0' contre 55 pour cent de '1') s'il est imprévisible, alors qu'en simulation la situation est inverse : l'uniformité est plus importante que l'imprévisibilité.

Existe-t-il des générateurs cryptographiquement sûrs? Vraisemblablement oui, et le générateur BBS décrit sur la figure 4 est un bon candidat comme générateur cryptographiquement sûr. Pourquoi vraisemblablement? Parce que les mathématiciens ont seulement réussi à établir que le BBS est sûr en admettant qu'une certaine conjecture est vraie (il s'agit de la conjecture sur la difficulté du calcul de la *résiduosité quadratique*). La conjecture est jugée très vraisemblable, et donc on est presque certain que BBS est un bon générateur aléatoire... mais pas absolument.

Cette situation où un résultat, conjecturé et jugé vraisemblable par les spécialistes, reste non démontré est fréquente en théorie de la complexité. Bien d'autres conjectures attendent le génie mathématique qui saura les élucider. La situation est inconfortable : les cryptographes utilisent des méthodes vraisemblablement bonnes, sans avoir d'assurances fermes à leur sujet. Cette remarque s'applique en particulier aux systèmes utilisés pour la carte à puce ou les transactions entre banques.

Qui a dit qu'on faisait trop de mathématiques? La création de suites aléatoires sûres est un exemple parmi d'autres (qu'on trouverait en physique) où apparaît l'insuffisance du développement des mathématiques contemporaines face aux besoins de l'industrie. Même sur des sujets économiquement cruciaux, car liés au commerce électronique et à la sécurité bancaire, on attend des avancées mathématiques.

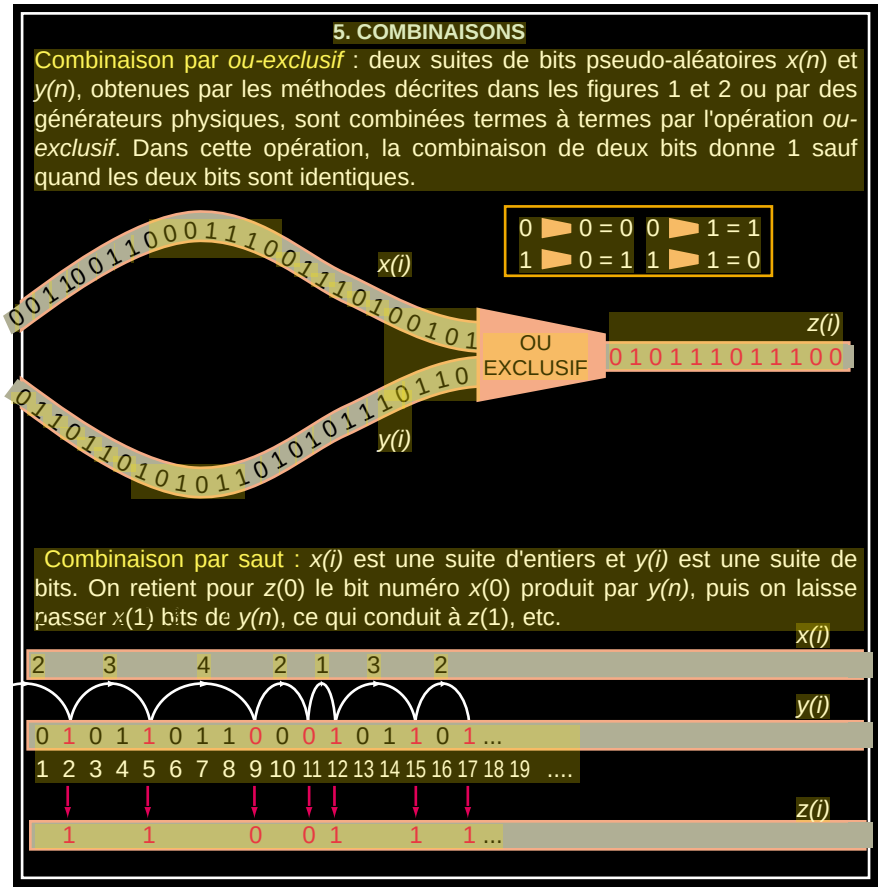
LE HASARD FORT

Ce hasard cryptographique (défini par la difficulté de la prédiction), sans doute atteint pas BBS, est le *hasard moyen*. Le *hasard fort* est défini par l'impossibilité absolue de la prédiction, quelle que soit la puissance de calcul utilisée. On a démontré, il y a quelques années, que cette impossibilité absolue est équivalente à l'impossibilité de la compression des données : une suite de nombres est aléatoire au sens fort s'il est impossible de la décrire en utilisant moins de place que celle qu'elle occupe.

Le malheur de ce hasard fort défini en 1965 par le mathématicien suédois Pier Martin-Löf est que, par nature, aucun programme déterministe d'ordinateur ne peut l'engendrer. Une procédure d'ordinateur (par nature déterministe) n'engendrera jamais de suites aléatoires au sens fort.

Dès 1951, avant même qu'elle n'ait pris un sens mathématique précis, von Neumann, conscient de cette difficulté fondamentale, écrivait : «Quiconque envisage une méthode arithmétique pour produire des chiffres aléatoires est en état de péché.»

À côté de l'impossibilité pour un programme déterministe d'engendrer une suite aléatoire au sens fort, on démontre que, si l'on réussit à disposer d'un phénomène physique non déterministe équiréparti (produisant des 0 et des 1 en proportion égale), alors en faisant travailler ce générateur on tombera presque certainement sur une suite aléatoire au sens de P. Martin-Löf (donc au sens le plus fort). Ce résultat semble être un jeu de mots – l'indéterminisme produit le hasard –, mais mathématiquement il lui correspond un énoncé précis qui n'est ni évident ni une boutade.



RÉALISATION DE TABLES DE NOMBRES ALÉATOIRES

Toutes ces raisons expliquent pourquoi on s'est souvent tourné vers des mécanismes physiques de production du hasard.

Il n'y a pas si longtemps, on éditait des tables de nombres aléatoires. En 1927, une table de 40 000 chiffres aléatoires fut publiée par L. Tippett. En 1939, un mécanisme physique fut utilisé par M. Kendal et B. Babington-Smith pour produire une table de 100 000 chiffres aléatoires. En 1955, la *RAND Corporation* publia une table d'un million de chiffres aléatoires engendrés, là encore, par une machine. Les tests statistiques utilisés pour mettre cette table à l'épreuve furent repris par J. Guilloud et M. Bouyer quand, en 1973, ils calculèrent un million de décimales de π. Le nombre π passa les tests. Cela ne signifie par que π est aléatoire au sens fort : le cryptographe saura reconnaître la suite des décimales de π et calculer les suivantes pour déchiffrer le message.

Les chiffres de π, contrairement à une légende tenace, ne conviennent donc ni comme hasard faible pour la simulation (trop compliqués à calculer), ni comme hasard moyen en cryptographie, où ils ne possèdent pas les propriétés d'imprévisibilité souhaitées.