tirés du bruit atmosphérique capté par radio. On peut par exemple obtenir, à la demande, le résultat d'un lancer de deux dés, ou le mélange d'un paquet de 52 cartes, ou même une image aléatoire faite de pixels noirs et blancs.

Random.org affirme extraire 12000 bits par seconde du bruit atmosphérique, et c'est à partir d'eux que les autres services sont fournis. Si on le souhaite, les nombres que le site communique sont mémorisés, mais ce n'est pas très facile car le site n'est pas conçu pour jouer le rôle de balise aléatoire sécurisée émettant périodiquement. Par ailleurs, on ne sait pas vraiment comment le bruit atmosphérique est capté et transformé en données aléatoires. Utiliser random.org pour les applications n'exigeant pas une certitude d'honnêteté et de sécurité totale sera une assez bonne solution, mais, tel qu'il est conçu, ce site internet n'est pas en mesure de fournir assez de garanties pour des applications où par exemple des sommes importantes d'argent seraient en jeu.

LA BALISE DU NIST: UNE LISTE DE 512 BITS CHAQUE MINUTE

C'est sans doute pourquoi l'institut américain des normes et de la technologie, le NIST (National Institute of Standards and Technology), travaille sur ce problème depuis 2011 et propose une balise aléatoire, conçue cette fois comme un émetteur public et périodique d'aléas dont les données produites sont protégées et restent consultables sans limitation de temps. La balise du NIST publie chaque minute une liste de 512 bits aléatoires (*voir* https://beacon.nist.gov/home). Et le NIST encourage la création d'autres balises indépendantes.

Le NIST utilise les bits émis par un dispositif quantique. Il fournit un moyen de vérifier que les bits publiés ne sont pas modifiés une fois publiés et affirme que son site est protégé contre toute intervention extérieure, ce qui assure que personne ne manipule le mécanisme de production ou de publication.

Si l'on considère que le NIST est un tiers de confiance parfait, on peut utiliser ce qu'émet sa balise. Par exemple, si des sites de jeux qui utilisent des nombres aléatoires vont les y rechercher en indiquant comment, on pourra avoir confiance en eux et vérifier qu'il n'y a pas tricherie, car il est improbable que le NIST se laisse corrompre par eux. Malgré tout, comme le notent de nombreux spécialistes, le NIST ne donne aucun moyen pour contrôler que les bits qu'il publie sont produits par des phénomènes quantiques et qu'aucune manipulation n'est opérée par l'institut sur ce qu'il émet. Le NIST ayant déjà été soupçonné de tentatives de trucage liées à des outils de génération d'aléas (*voir* https://en.wikipedia.org/wiki/Dual_EC_DRBG), il est impossible de recommander d'utiliser sa balise pour les applications exigeant une sécurité absolue.

Remarquons que, sur sa page, le NIST indique en rouge qu'il ne faut pas utiliser sa balise pour choisir des mots de passe. La recommandation est tout à fait justifiée et s'applique à tous les générateurs publics d'aléas. En effet, les données publiées restent accessibles (c'est nécessaire pour mener des contrôles *a posteriori*), ce qui signifie que si votre mot de passe a été engendré par une balise publique, quelqu'un cherchant à le deviner a accès aux mêmes nombres aléatoires, ce qui facilite son travail. Pour vos mots de passe, utilisez des générateurs privés et si possible indépendants de votre machine!

D'autres sites se présentent comme des balises aléatoires sécurisées et réussissent à faire mieux que la balise du NIST.

Le Laboratoire de sécurité computationnelle et de cryptographie appliquée de l'université du Chili (https://random.uchile.cl/en/) propose une balise dont les bits dépendent à la fois d'une source quantique locale et de données extérieures (données sismiques, radio de l'université du Chili, blockchain Ethereum, Twitter). Ce site est l'une des meilleures balises actuelles: il utilise le principe décrit plus loin et dans l'encadré 3.

Le site brésilien d'Inmetro, l'Institut national de la métrologie et de la qualité (www4.inmetro.gov.br/) et le projet collaboratif *League of entropy* (www.cloudflare.com/leagueofentropy/) offrent divers outils de génération de hasard privé et public. Là encore, ils s'appuient >

AUTHENTIFICATION SANS CONSERVATION DES MOTS DE PASSE

Première connexion : enregistrement de l'identifiant de l'utilisateur et de l'empreinte du mot de passe

Jean-Paul choisit le mot de passe JP1234 et le communique au serveur

Le serveur calcule l'empreinte du mot de passe reçu, trouve X2e9qq92 et mémorise le couple Jean-Paul/X2e9qq92.

Connexion ultérieure : vérification par le serveur que celui qui se connecte est la bonne personne

Jean-Paul se connecte au serveur et indique son identifiant ainsi que son mot de passe

Le serveur calcule l'empreinte du mot de passe reçu et vérifie qu'elle est bien la même que celle du couple qu'il a enregistré Jean-Paul/X2e9qq92