à la guerre moderne. Dorénavant, les savants serviront en tant que scientifiques, ou du moins dans les armes techniques, où ils seront moins exposés.

À la rentrée solennelle du 24 mars 1919, on commence à cultiver le souvenir de la Grande Guerre sur une double base : d'une part, le rappel du sacrifice de l'École et des promesses brisées que chaque vie perdue représente ; d'autre part, la réaffirmation de la mission de l'École en faveur de « la recherche libre et de la science désintéressée » et de la mission « pacifique et civilisatrice » de la France. Par contraste, l'École polytechnique représentera les ajustements qui doivent être apportés à ces idéaux à la suite de la guerre, notamment un investissement profond dans le développement de nouvelles applications des sciences pour l'industrie ou la guerre.

Dans les années 1920, les jeunes gens qui formeront plus tard Bourbaki sont abreuvés de ces discours. Quelques années plus tard, vers 1935, les membres du groupe entament la rédaction d'un nouveau traité de mathématiques très ambitieux, qu'ils veulent avant tout abstrait et défini par les seuls besoins internes aux mathématiques. Cette vision qu'ils promeuvent de plus en plus activement dans divers écrits à destination de larges publics jusque dans les années 1970 s'oppose de front à la conception promue par leurs aînés qui avaient plutôt tendance, comme on l'a vu, à penser les mathématiques dans la continuité des sciences de la nature.

Malgré cette opposition, ils entonnent volontiers le discours de leur *alma mater*. La mort de tant de mathématiciens pendant la guerre ne semble plus rien d'autre qu'un immense gâchis ; dorénavant, le but de la génération montante paraît clair : ils se doivent avant tout à la recherche mathématique pure. Les récits à propos des mathématiciens morts au combat, même si les membres de Bourbaki choisissent de ne pas s'en souvenir, ont rempli leur rôle : alors même que la recherche militaire est fortement promue par l'État, un large espace pour une science pure, neutre, s'est ouvert pour eux. C'est là, sans aucun doute, l'une des conséquences les plus durables de cette terrible guerre. ■

BIBLIOGRAPHIE

D. Aubin, L'Élite sous la mitraille, Rue d'Ulm, 2018.

D. Aubin et C. Goldstein (éd.), The War of Guns and Mathematics, American Mathematical Society, 2014.

P. Painlevé, L'École normale supérieure et la guerre, *Revue scientifique*, vol. 54, p. 193-195, 1916.

Notices nécrologiques de normaliens morts à la guerre : https://www.presses.ens.fr/client/document/aubin_notices_834.pdf

R
ENDEZ-VOUS

ENVOYER DES MESSAGES À RETARDEMENT

La science cryptographique étudie les moyens de livrer une information en fixant une date avant laquelle elle restera cachée et inaccessible. Un problème de mieux en mieux résolu.

L'AUTEUR

JEAN-PAUL DELAHAYE
professeur émérite à l'université de Lille et chercheur au laboratoire Cristal (Centre de recherche en informatique, signal et automatique de Lille)

Le 29 mai 1875, au milieu de la nuit, Frederick Deland, caissier à la Grand Mahawie Bank, est pris en otage par quatre individus qui se sont introduits chez lui. Conduit sur place à la banque, on lui demande d'ouvrir le coffre dont les malfrats savent qu'il connaît la combinaison. Il leur explique qu'un nouveau dispositif, empêchant d'ouvrir la porte du coffre avant une heure donnée, a été installé. Les menaces ne servent à rien et les voleurs repartent bredouilles.

Ce fut le premier succès des serrures à horlogerie, devenues alors d'usage courant et dont il existe une multitude de modèles différents, que les collectionneurs s'arrachent (*voir l'encadré 1*). Les banques en utilisent toujours, mais aujourd'hui vous en trouverez aussi pour les usages individuels sous le nom, en France, de serrures et coffres «à retardement». Il existe aussi des boîtes de rangement munies de tels dispositifs pour aider les victimes d'addiction à résister à leurs démons. On peut y déposer des téléphones portables, des paquets de cigarettes, de la drogue, de la nourriture, etc., qui, tant qu'ils sont dans la boîte fermée, empêchent qu'on y accède et en abuse.

CAPSULES TEMPORELLES POUR LE MONDE NUMÉRIQUE

Et dans le monde numérique? Existe-t-il des «capsules temporelles» qui permettraient de chiffrer un message sous la forme d'un fichier informatique qu'on laisserait circuler, qu'on pourrait dupliquer et qui resterait illisible jusqu'à une certaine date, à partir de laquelle l'information cachée deviendrait accessible? La cryptographie moderne a abordé la question et les plus anciens travaux remontent à 1993. Le problème est assez délicat et les diverses solutions proposées ne réussissent que partiellement à créer ces capsules temporelles.

Pourtant de tels mécanismes de chiffrement à retardement seraient susceptibles de nombreuses applications. En voici quelques exemples.

– Vous voulez faire un cadeau à un proche pour son anniversaire. Vous lui envoyez un message chiffré qui se libère le jour venu et dans lequel est indiqué l'endroit où est caché son cadeau, ou les données pour accéder au compte où vous lui avez laissé une somme d'argent.

– Vous êtes un lanceur d'alerte… ou un maître chanteur. Vous déposez des informations compromettantes dans un endroit secret, peut-être sur internet, que vous ne voulez rendre publiques que si l'on vous arrête ou vous assassine. Vous faites circuler l'information sur le lieu du dépôt sous la forme d'un fichier temporairement chiffré jusqu'à une date que vous avez choisie. Si vous êtes arrêté ou tué, l'information sera libérée à la date choisie et tous ceux ayant reçu le fichier sauront, sans que vous ayez à intervenir, où sont les informations que vous vouliez rendre publiques.

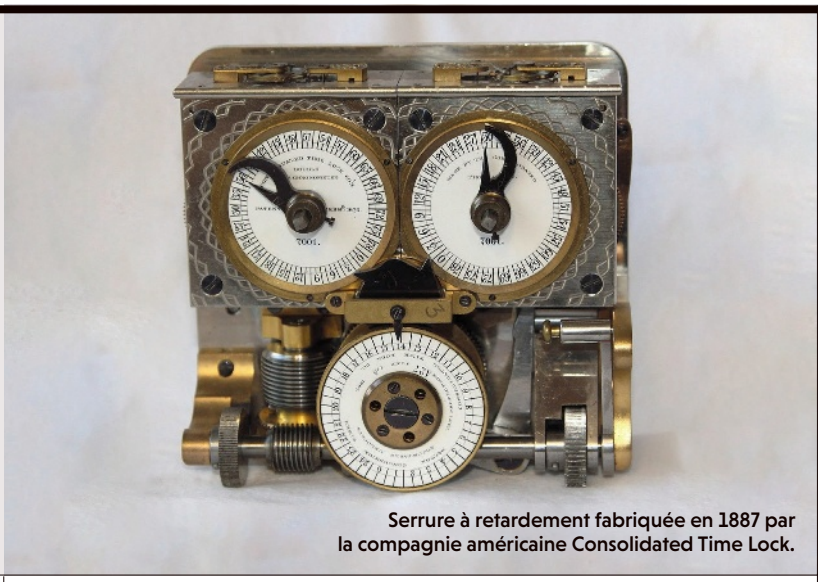
– Pour organiser une enchère, chaque acheteur intéressé dépose le prix qu'il est prêt à payer dans un message chiffré qui ne se libère qu'à la date de clôture des enchères. Plus généralement l'idée fonctionne pour les procédures

Jean-Paul Delahaye a notamment publié : **Les Mathématiciens se plient au jeu**, une sélection de ses chroniques parues dans *Pour la Science* (Belin, 2017).

SERRURES À RETARDEMENT

1

Les serrures à retardement (*time lock boxes* en anglais), une fois enclenchées, ne peuvent pas s'ouvrir avant une heure programmée. Utilisées par les banques depuis plus d'un siècle, elles empêchent quiconque réussissant à entrer dans la salle des coffres, et même s'il connaît la combinaison d'un coffre, de l'ouvrir. Les modèles sont nombreux et intéressent les collectionneurs comme Mark Frank, qui a créé un magnifique site internet pour présenter sa collection, dont la photo ci-contre montre un exemplaire (www.my-time-machines.net/my_time_lock_collection.htm).



Serrure à retardement fabriquée en 1887 par la compagnie américaine Consolidated Time Lock.

de vote (non secret) où les électeurs sont éloignés et ne souhaitent dévoiler leur choix que lorsque chaque électeur a déposé le sien.

– Vous organisez un examen ou un concours dont les participants sont dispersés dans le monde entier. Sans avoir à vous soucier des délais et erreurs de transmission, vous leur envoyez la capsule temporelle contenant le sujet. Vous contrôlez que tous l'ont reçue et, à l'heure voulue, le sujet d'examen se dévoilera à tous.

COFFRES ET ORDINATEURS À RETARDEMENT

L'utilisation d'un coffre à retardement permet de maintenir secret un message jusqu'à la date programmée d'ouverture. Toutefois, le message n'est pas accessible à tout le monde à la date voulue. Un acteur puissant pourrait contrôler le coffre, l'ouvrir le premier et empêcher la diffusion de l'information déposée.

Pour éviter ce risque, vous pouvez mettre l'information dans plusieurs coffres en ne donnant l'information de leur emplacement qu'à certaines personnes. L'acteur puissant qui souhaite empêcher la diffusion de l'information ne connaîtra pas tous les emplacements des coffres.

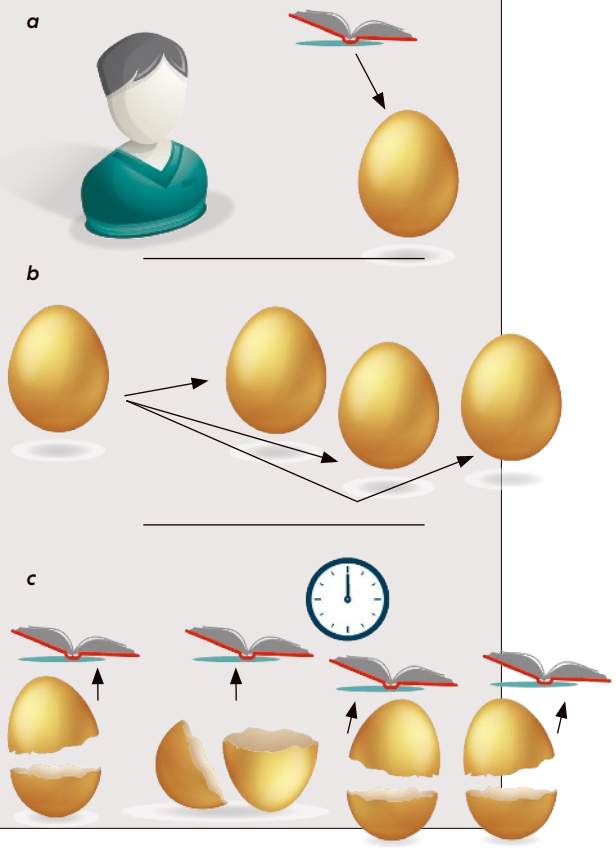
On peut aussi imaginer qu'avec une serrure à retardement, on envoie un message à une date donnée, par un téléphone portable où un ordinateur, à une série de numéros de téléphone donnés, ou, mieux, on dépose à une adresse internet le message souhaité qui sera alors lisible dans le monde entier. Un ordinateur portable caché dans un coffre fermé (qui laisse passer les ondes !) et convenablement >

2 UNE CAPSULE TEMPORELLE IDÉALE

Monsieur Dupont veut cacher l'histoire de sa vie qu'il a soigneusement rédigée et déposée dans un fichier informatique de façon à ce que personne de son vivant ne puisse en prendre connaissance. Il fixe la date de levée du secret au 1er janvier 2100. Il crée un fichier informatique (capsule temporelle) programmé pour cette date *(a)*.

Il fait ensuite circuler la capsule temporelle, qui est multipliée sur le réseau, sans que personne ne puisse prendre connaissance du contenu *(b)*.

Le 1er janvier 2100, ceux qui détiennent la capsule réussissent sans mal à l'ouvrir et à prendre connaissance du document de M. Dupont, qui est mort depuis longtemps *(c)*.



En haut : © Frank Mark (http://www.my-time-machines.net/)
En bas : © Shutterstock.com/Naida Jazmin Ochoa/Meilun/NeMaria/Pour la Science

3

UN SECRET PARTAGÉ EN MORCEAUX

Il est possible de partager un message M en n morceaux $M_1, M_2, \ldots, M_n$ de telle façon que l'on n'ait aucune information sur M tant que l'on ne dispose pas de tous les n morceaux. Expliquons comment. On suppose M donné sous forme binaire et ayant la longueur L.

Pour $M_1, M_2, \ldots, M_{n-1}$, on prend des suites de 0 et de 1 aléatoires, différentes et indépendantes, chacune de longueur L. Pour définir M_n, on procède bit par bit.

Pour le premier bit de M_n, on prend un 0 ou un 1 de façon que le nombre de 1 en première position dans les messages $M_1, M_2, \ldots, M_n$ soit pair si le premier bit de M est 0, et impair sinon.

Pour le deuxième bit de M_n, on procède de la même façon à partir des bits en deuxième position de M et de $M_1, M_2, \ldots, M_{n-1}$. Et ainsi de suite (la procédure est illustrée ci-dessous pour $n = 10$, sur un message court).

Connaître $M_1, M_2, \ldots, M_n$ permet de reconstituer M, mais connaître $n - 1$ de ces messages ne donne aucune information sur M.

On peut faire mieux et partager un message M en n morceaux de telle façon que :
– connaître k morceaux, quels qu'ils soient ($k < n$), redonne M ;
– connaître moins de k morceaux ne donne aucune information sur M.

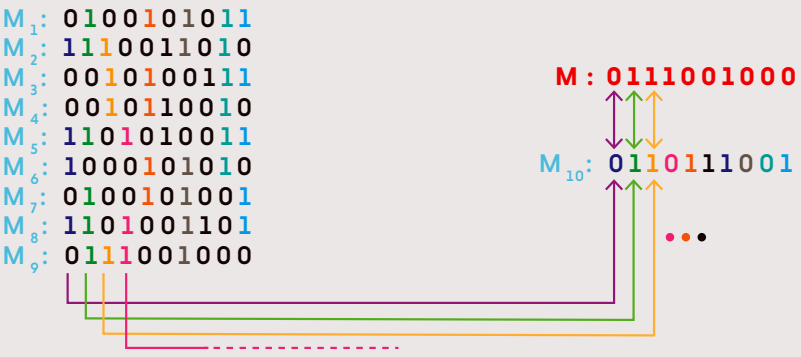
Plusieurs méthodes ont été proposées, dont celle d'Adi Shamir (« How to share a secret », *Communications of the ACM*, vol. 22(11), pp. 612-613, 1979).

Son idée repose sur le fait que disposer de k valeurs d'un polynôme P de degré $k - 1$ permet de le déterminer, mais que c'est impossible si l'on en connaît moins.

Le premier bit de M étant d_1, on commence par trouver un polynôme P_1 de degré $k - 1$ dont la valeur en 0 est d_1. Ensuite, pour chaque i de 1 à n, on fixe comme premier élément du message M_i la valeur $P_1(i)$.

On fait de même avec le second bit d_2 de M : on choisit un polynôme P_2 de degré $k - 1$ dont la valeur en 0 est d_2. Puis, pour chaque i de 1 à n, on fixe comme second élément du message M_i la valeur $P_2(i)$. Et ainsi de suite.

En conséquence :
– celui qui connaît k messages parmi $M_1, M_2, \ldots, M_n$ connaîtra le 1er bit de M, car il peut calculer le polynôme P_1. Il connaîtra le 2e bit de M, car il peut calculer le polynôme P_2. Etc.
– celui qui connaît moins de k messages parmi $M_1, M_2, \ldots, M_n$ ne peut rien connaître de M.



> programmé fera l'affaire : vous délivrerez le message à la date voulue.

Ces méthodes sont intéressantes, mais uniquement pour des délais assez courts ne dépassant pas quelques mois ou années, car les batteries du téléphone ou de l'ordinateur caché doivent tenir jusqu'au moment du déclenchement. Elles ne permettent pas d'envoyer un message un siècle à l'avance.

De plus, les solutions avec téléphone ou ordinateurs cachés ne produisent pas un fichier informatique qu'on laisse circuler et qui est tel que tous ceux le détenant à l'heure voulue en découvrent le message sans avoir à interagir avec autre chose. Elles ont aussi l'inconvénient d'être lourdes à mettre en œuvre, sans parler du risque que le dispositif caché soit découvert et arrêté ou détruit par accident. Réfléchissons à mieux.

FAIRE APPEL À UN OU PLUSIEURS TIERS DE CONFIANCE

Une idée évidente est celle du tiers de confiance. Vous confiez le message, placé dans une enveloppe cachetée par exemple, à un huissier en lui indiquant la date à laquelle il devra ouvrir l'enveloppe et en délivrer le contenu. Vous pouvez améliorer la robustesse du procédé en utilisant plusieurs tiers de confiance dont aucun ne pourra divulguer seul le message avant l'instant choisi par vous. Voici la méthode.

Vous découpez le message en n morceaux dont aucun ne permet d'avoir la moindre idée du message complet et dont même la connaissance de $n-1$ morceaux ne révèle rien (*voir l'encadré 3*). Vous confiez ces n morceaux à n tiers de confiance en leur demandant de se contacter les uns les autres à la date voulue pour s'échanger les bouts du message, le reconstituer et le rendre public.

Le risque sera cependant que l'un des tiers de confiance soit indisponible le jour voulu, malade ou décédé par exemple. Cela empêcherait que le message soit reconstitué et délivré. Mais il existe des procédés de découpage d'une information, inventés en 1979 par Adi Shamir et George Blakley, qui résolvent le problème. Le message est découpé en n morceaux qui ont la propriété que dès que l'on dispose de k morceaux ($k<n$) du découpage, il devient possible de retrouver tout le message, et qu'avec moins de k morceaux, rien ne peut être dévoilé du message découpé (*voir l'encadré 3*).

Ces idées résolvent sans doute un certain nombre de cas, mais, comme précédemment, ce ne sont que des méthodes partiellement satisfaisantes : elles ne produisent pas une capsule temporelle, c'est-à-dire un message qui libère seul son information à la date voulue à ceux qui le détiennent.

Explorons d'autres idées. Ronald Rivest

(le R du protocole de chiffrement à double clé RSA), Adi Shamir (le S de RSA) et David Wagner ont proposé en 1996 une méthode consistant à utiliser un protocole de chiffrement dont on efface volontairement la clé de déchiffrement. La seule façon de lire le message chiffré est alors de mener une attaque par calculs massifs dont on évalue la durée. Le message est illisible pendant tout le temps nécessaire aux calculs. Ceux qui les effectuent obtiennent au bout du temps prévu le moyen de déchiffrer le message. Cette fois, on a bien un message chiffré qui peut circuler et même être dupliqué et qui est protégé en lui-même par un système ne permettant pas d'en lire le contenu avant une certaine date. La méthode est astucieuse, mais on doit noter deux points.

UN RETARD IMPOSÉ PAR DES CALCULS NON PARALLÉLISABLES

Tout d'abord, le message ne sera déchiffré que par ceux qui effectueront le calcul massif et l'auront poursuivi pendant la durée nécessaire. C'est coûteux et cela demande des compétences; le message ne sera donc accessible qu'à certains acteurs très particuliers ayant accepté de s'en occuper en continu. De plus, si vous ne vous occupez pas de la capsule temporelle dès qu'elle est émise, vous ne pourrez disposer du message qu'avec retard.

Ensuite, on ne connaît pas à ce jour de méthode permettant d'ajuster avec précision la difficulté de la recherche de la clé. On peut d'ailleurs remarquer que, en 1996, les trois chercheurs ont décrit leurs idées en évoquant un système où le calcul massif consistait à calculer successivement des carrés de nombres entiers.

En 1999, un défi a été lancé concernant ce procédé, le « LCS35 Time Capsule Crypto-Puzzle ». Le message caché ne devait pouvoir se libérer que trente-cinq ans plus tard environ, donc vers 2034. Cette évaluation de la résistance du problème tenait compte de la loi de Moore, selon laquelle nos capacités de calcul doublent tous les dix-huit à vingt-quatre mois environ. Mais les progrès en matière de calcul de carrés de nombres entiers ont été plus rapides que prévu et le défi est tombé en 2019, quinze ans plus tôt que ce qui était programmé. Ronald Rivest a dû reconnaître qu'il s'était trompé dans son anticipation.

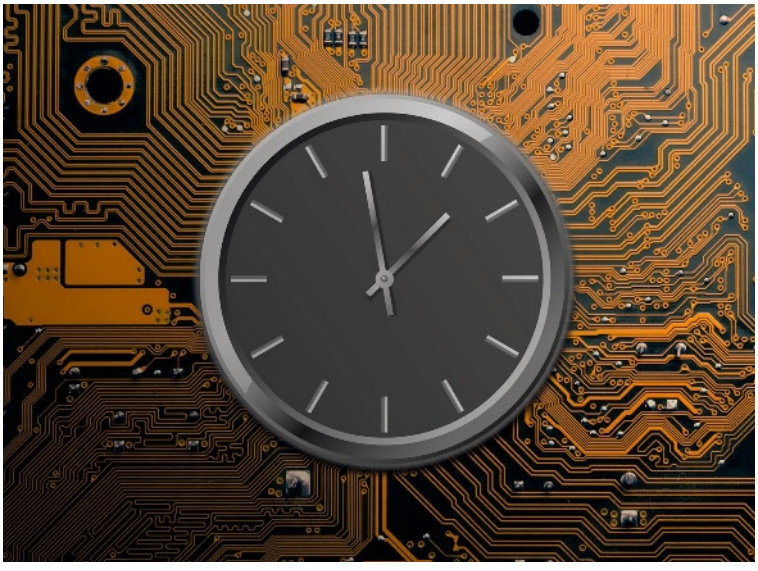
L'erreur ne provient pas de la loi de Moore, mais de la réalisation de puces spécialisées dans le calcul de carrés et des progrès faits par les algorithmes de calcul du carré d'un nombre entier. Les informaticiens et les mathématiciens travaillent en effet à des avancées en termes d'algorithmes ou dans la conception des dispositifs de calcul qui accélèrent la résolution de certains problèmes particuliers indépendamment des progrès de l'électronique de base, lesquels sont les seuls que la loi de Moore prend en compte.

Le calcul de carrés successifs était pourtant « intrinsèquement séquentiel », ce qui signifie que l'utilisation de calculs parallèles ne pouvait pas aider à accélérer sa réalisation. Aujourd'hui, d'autres méthodes – les VDF ou fonctions vérifiables à délai – ont été proposées pour concevoir des énigmes dont la résolution exige une quantité de calcul impossible à mener en parallèle et donc demandent un temps de calcul impossible à raccourcir sensiblement. Cependant, la durée minimale que de tels calculs exigent reste imprécise. >

4 UN DÉFI DE CALCUL TROP VITE RÉSOLU

Une idée pour concevoir des capsules temporelles est de chiffrer le message avec un procédé dont la clé de déchiffrement ne se découvre qu'en menant un long calcul dont la durée amènera à la date fixée pour la libération du message. Proposée par Ronald Rivest, Adi Shamir et David Wagner en 1996, cette idée ne permet pas de fixer avec une grande précision la date de libération du message, car selon qu'on aura consacré beaucoup de moyens ou non pour mener le calcul, on arrivera plus ou moins vite au résultat provoquant l'ouverture.

Les calculs nécessairement longs proposés par les chercheurs étaient des calculs enchaînés de carrés de nombres entiers. Un problème de ce type fut proposé en 1999 à titre de défi (https://en.wikipedia.org/wiki/LCS35) ; il devait tenir trente-cinq ans, mais il a été résolu en moitié moins de temps car on a su améliorer les algorithmes de calcul de carrés et créer des processeurs spécialisés (voir « Programmers solve MIT's 20-year-old cryptographic puzzle », laboratoire CSAIL du MIT, avril 2019 : https://www.csail.mit.edu/news/programmers-solve-mits-20-year-old-cryptographic-puzzle).



> Pour atteindre l'objectif recherché, on peut s'appuyer sur les techniques d'« offuscation » de programmes et sur l'existence d'horloges publiques sécurisées ou aux propriétés particulières.

DES PROGRAMMES OFFUSQUÉS QUI SURVEILLENT L'HEURE

L'offuscation de programmes consiste à écrire des programmes informatiques que tout le monde peut avoir et faire fonctionner, mais dont la logique de fonctionnement est tellement embrouillée et masquée que même en étudiant soigneusement le programme, on ne saura pas bien ce qu'il fait. Cela empêche qu'on les modifie ou qu'on exploite les idées qui ont conduit à leur mise au point.

Si l'on maîtrise l'offuscation, on peut créer un programme à retardement livrant un message à une date fixée par le créateur: une fois lancé sur une machine ayant accès à internet, le programme offusqué lit l'heure sur un ou plusieurs sites qui la publient en continu. Quand l'heure trouvée dépasse la date programmée, le programme déchiffre l'information qui est cachée en lui et la fait alors apparaître en clair. Si l'information qu'on veut libérer est très volumineuse, l'information libérée sera la clé de déchiffrement du fichier chiffré contenant cette information, le programme offusqué ne servant qu'à cacher la clé de déchiffrement.

Il existe de nombreux sites publiant l'heure, en particulier l'horloge parlante (http://www.horlogeparlante.com). On peut imaginer qu'ils fonctionneront encore longtemps et suivront le même mode de publication. Si l'on craint qu'ils soient compromis ou simplement arrêtés, l'utilisation de plusieurs horloges dispersées en des endroits divers du monde fournira une garantie renforcée. Le programme consultera par exemple n horloges et considérera comme certain que le moment attendu est atteint seulement si k horloges parmi n l'indiquent.

Cette méthode est moins risquée que celle où l'on confie le message à un tiers de confiance: les horloges utilisées ne sont pas informées du message caché dans le programme offusqué, et ne savent même pas qu'on les utilise. Toutefois, certains résultats théoriques semblent indiquer qu'aucune méthode parfaite d'offuscation n'existe. D'autres résultats récents utilisant une définition moins stricte de l'offuscation montrent qu'on peut réussir, mais au prix d'un ralentissement du fonctionnement du programme offusqué.

C'est pourquoi on a recherché des méthodes ne faisant pas appel à l'offuscation. L'une d'elles, décrite en 2004 par Aldar Chan et Ian Blake, et perfectionnée en 2006 par Julien Cathalo, Benoît Libert et Jean-Jacques Quisquater, décrit comment une horloge de référence fiable peut produire et publier des informations qui permettront à quelqu'un voulant émettre un message à retardement de le faire sans que l'horloge ait à connaître le message temporairement chiffré ni même savoir qu'un tel message existe.

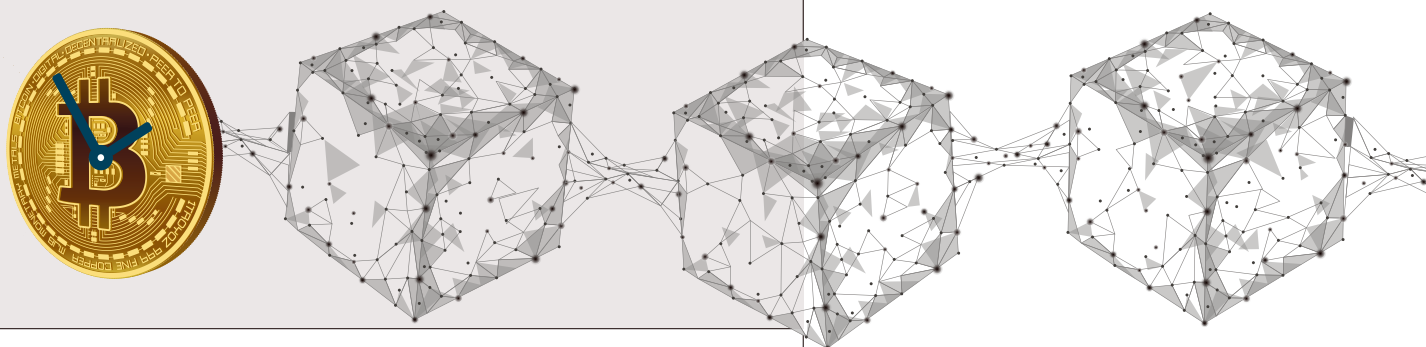
L'horloge produit à la date voulue des informations permettant de déchiffrer les fichiers secrets. Ni le créateur de la capsule temporelle ni ceux à qui elle est adressée n'ont à interagir avec l'horloge qui diffuse les messages permettant de déchiffrer les capsules temporelles ayant atteint l'instant de libération. Ces méthodes permettent aussi de préserver l'anonymat des utilisateurs qui créent les capsules temporelles ou les lisent l'heure venue.

Malheureusement, celui qui fait fonctionner horloge peut produire avant l'heure les clés de déchiffrement des capsules temporelles. La solution est donc encore imparfaite.

5 LA SOLUTION BLOCKCHAIN

La technologie des blockchains qui est utilisée pour émettre et faire circuler des cryptomonnaies telles que le Bitcoin met à la disposition de tous une horloge décentralisée dont le fonctionnement ne peut être perturbé par personne.

Cette technologie permet de concevoir des capsules temporelles dont la sûreté n'est pas liée à la confiance accordée à un acteur particulier. Cette dernière avancée dans la conception de capsules temporelles de plus en plus proches de l'idéal, décrit dans l'encadré 2, est due à Jia Liu, de l'université de Surrey, Tibor Jager et Saqib Kakvi, de l'université de Paderborn, et Bogdan Warinschi, de l'université de Bristol, et a été publiée en 2018 *(voir la bibliographie)*.



© Shutterstock.com/Iurii Motov/LuckyStep

Depuis quelques années, il est devenu possible de disposer de l'équivalent d'une horloge de référence sans avoir à craindre qu'elle puisse être utilisée en avance. La méthode publiée en 2018 par Jia Liu, Tibor Jager, Saqib Kakvi et Bogdan Warinschi s'appuie sur les blockchains (ou chaînes de blocs) publiques, comme celle de la monnaie cryptographique Bitcoin en fonctionnement depuis 2009.

La blockchain du Bitcoin est un fichier recopié à l'identique en chaque nœud d'un réseau informatique, ce fichier étant géré et surveillé par chaque nœud de ce réseau. Le fichier évolue toutes les dix minutes environ par l'ajout d'une nouvelle page (ou bloc) et c'est cet ajout périodique qui fixe l'avancée de l'horloge. Son fonctionnement n'est pas extrêmement précis, car l'intervalle de dix minutes n'est qu'une moyenne.

UNE BLOCKCHAIN POUR UNE HORLOGE DÉCENTRALISÉE

Cependant, cette horloge décentralisée n'est aux mains de personne en particulier. C'est donc l'ensemble des nœuds du réseau, environ 10 000 répartis dans le monde entier, qu'il faudrait soudoyer pour fausser le signal qu'elle émet. En perturber le fonctionnement est pratiquement impossible, car l'ajout d'une nouvelle page exige que le réseau fasse une quantité colossale de calculs, aujourd'hui environ 10^{20} calculs de la fonction SHA256 par seconde. Il y a donc bien, comme pour les méthodes proposées par Adi Shamir et ses collègues, un calcul important à faire qui régule l'horloge. Cependant, la situation est très différente pour trois raisons rassurantes.

Tout d'abord, ce ne sont pas ceux qui créent ou veulent lire le contenu des capsules temporelles en s'appuyant sur cette horloge qui font les calculs, mais les nœuds du réseau qui sont motivés par les gains payés en nouveaux bitcoins créés pour cette participation au fonctionnement du réseau.

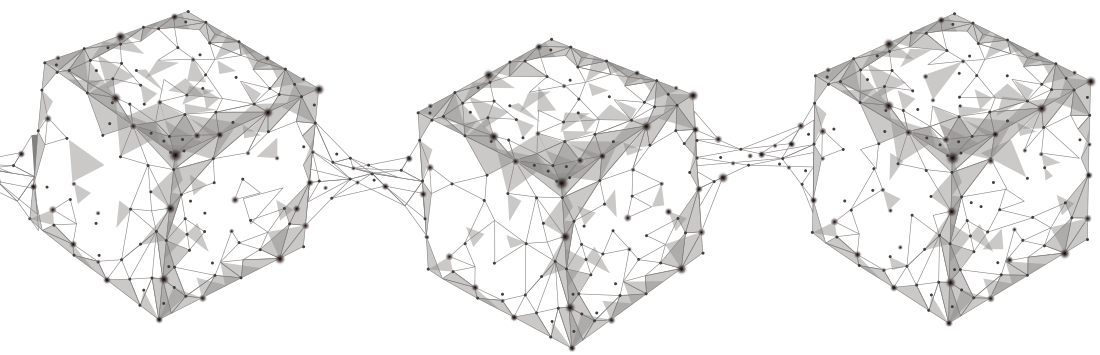
Ensuite, la difficulté du calcul à mener pour faire avancer l'horloge d'une étape de dix minutes se réajuste automatiquement tous les quatorze jours pour prendre en compte l'évolution de la capacité totale du réseau: la difficulté augmente si le réseau a accru sa capacité à calculer, elle diminue sinon. Ce réajustement annule l'évolution de puissance du réseau et maintient sur le long terme la durée moyenne d'une étape à dix minutes. Les progrès de l'électronique, ou d'autres natures n'accéléreront pas l'horloge.

Enfin, quelqu'un qui voudrait seul accélérer brusquement le calcul pour produire de nombreuses étapes rapprochées de l'horloge doit disposer d'une capacité de calcul propre de l'ordre de grandeur de celle cumulée de tous les nœuds validateurs du réseau, ce qui est très difficile à imaginer. Une dernière raison rend improbable la manipulation de l'horloge du bitcoin par un seul acteur: celui qui pourrait le faire pourrait aussi exploiter cette capacité de calcul pour s'approprier une grande partie des nouveaux bitcoins créés, dont la valeur équivaut à plusieurs milliards de dollars par an… ce qu'il préférera sans doute!

La blockchain semble donc nous approcher de l'idéal souhaité. Le système ne repose pas sur des tiers de confiance et il assure l'anonymat des créateurs de capsules temporelles et de ceux qui veulent les lire. Le message secret circule et se libère indépendamment de celui qui l'a émis, personne qui peut avoir disparu au moment de l'ouverture. Et lire le message une fois la date atteinte ne demande pas de capacité de calcul particulière et n'exige pas de s'en être occupé depuis son émission.

D'autres idées s'appuyant sur la notion de *smart-contract* du réseau Ethereum ont aussi été proposées. Ces méthodes ne sont malheureusement sans doute pas assez sûres à très long terme. En effet, comment être certain que, dans dix ans ou plus, les réseaux Bitcoin et Ethereum continueront de fonctionner, qu'ils auront résisté à toutes les attaques et n'auront pas été délaissés pour de meilleurs modèles de blockchain?

Le problème est difficile, mais la science cryptographique avance, en produisant d'année en année d'étonnants résultats! ■



BIBLIOGRAPHIE

W.-J. Lai *et al.*, **A fully decentralized time-lock encryption system on blockchain**, *2019 IEEE International Conference on Blockchain*, IEEE, 2019.

G. Branwen, **Time-Lock Encryption**, 2019 (https://www.gwern.net/Self-decrypting-files).

J. Liu *et al.*, **How to build time-lock encryption**, *Designs, Codes and Cryptography*, vol. 86, pp. 2549-2586, 2018 (https://bit.ly/36Rrx0u).

J. Cathalo *et al.*, **Efficient and non-interactive timed-release encryption**, *International Conference on Information and Communications Security*, Springer, 2005.

A. Chan et I. F. Blake, **Scalable, server-passive, user-anonymous timed release cryptography**, *25th IEEE International Conference on Distributed Computing Systems (ICDCS'05)*, IEEE, 2005.

R. Rivest, **Description of the LCS35 Time Capsule Crypto-Puzzle**, 1999 (https://bit.ly/3jKRQt1).

R. Rivest *et al.*, **Time-lock puzzles and timed-release crypto**, Technical Report MIT/LCS/TR-684, MIT Laboratory for Computer Science, 1996 (https://bit.ly/3nvdu72).

LES AUTEURS

JEAN-MICHEL COURTY et ÉDOUARD KIERLIK
professeurs de physique à Sorbonne Université, à Paris

BENOÎT SEMIN
chercheur CNRS au laboratoire PMMH (Physique et mécanique des milieux hétérogènes), à Paris

BIEN VENTILER POUR BIEN RESPIRER

Pour limiter la propagation du Covid-19, il faut aérer les lieux clos. Mais quand et pendant combien de temps ? Pour répondre, à défaut de mesurer la quantité de microbes dans l'air, on peut s'appuyer sur la concentration de dioxyde de carbone de l'air que l'on respire.

Renouveler l'air dans les lieux clos : ce thème a resurgi dans le débat public avec la pandémie de Covid-19. En effet, le virus impliqué se transmet notamment par voie aérienne, d'où la recommandation actuelle de bien ventiler les lieux clos pour contrer sa propagation. Cependant, bien au-delà de la crise épidémique, une bonne ventilation est importante pour la santé et le bien-être en général. Comment s'assurer qu'elle est satisfaisante ? En mesurant le taux de dioxyde de carbone, le CO_2, dans l'air. Ce gaz carbonique est produit par notre respiration et son taux permet donc d'estimer la qualité de l'aération.

ÉVITER DE DÉPASSER 1000 PPM DE CO_2

Dans l'air extérieur, la concentration moyenne de CO_2 est d'environ 0,04 %, c'est-à-dire que 1 molécule sur 2500 est une molécule de CO_2. Pour éviter d'avoir à manipuler des chiffres décimaux, on utilise plutôt la « partie par million », ou ppm en abrégé : on a donc ici une concentration d'environ 400 ppm, avec, en ville, des variations de quelques dizaines de ppm dues à la pollution ou à la situation météorologique.

Lorsque nous sommes à l'extérieur, l'air que nous expirons se dilue rapidement dans l'immensité de l'air ambiant ; notre respiration n'a donc aucune conséquence sur la concentration de CO_2. Tel n'est pas le cas dans un espace clos. Dans l'air expiré, la concentration de CO_2 atteint environ 40 000 ppm (soit 4 %). On estime ainsi que lors d'une respiration normale, un adulte rejette 18 litres de CO_2 par heure à pression atmosphérique. Dans un espace clos, la concentration de CO_2 augmente donc progressivement.

Pour fixer les idées, considérons une pièce où chaque personne dispose de 10 mètres cubes d'air. Cela correspond par exemple à 5 personnes dans un salon de 20 mètres carrés et 2,5 mètres de hauteur. Si la pièce est étanche et non ventilée, la concentration de CO_2 augmente linéairement avec le temps. Au bout de 1 heure, 18 litres de CO_2 s'ajouteront aux 10 mètres cubes (soit 10 000 litres) d'air par personne : la concentration sera donc augmentée de 1800 ppm et atteindra 2200 ppm si l'air de la pièce avait initialement la même composition que l'air extérieur.

Dans un lieu clos, la respiration des personnes présentes accroît assez vite la concentration en CO_2 de l'air. Pour rester à moins de 1 500 ppm de CO_2 dans une salle offrant une dizaine de mètres cubes d'air par personne, il faut renouveler l'air à peu près toutes les demi-heures. À cette fin, ouvrir grand les fenêtres quelques minutes suffit.

Or des études ont montré qu'au-delà d'une teneur en CO_2 de 2000 ppm, nos capacités cognitives commencent à s'altérer, et cela d'autant plus qu'elles sont de niveau élevé (prise de décision, réflexion…). C'est pourquoi les valeurs maximales conseillées pour la concentration de CO_2 en intérieur se situent d'habitude entre 1000 et 1500 ppm ; elles s'appliquent notamment aux bâtiments résidentiels et aux bureaux.

Comment ne pas dépasser ces seuils ? Par exemple en faisant appel à une ventilation mécanique. La norme européenne de ventilation dans les locaux non résidentiels (EN 13779) préconise un débit de 29 mètres cubes par heure et par personne pour que la qualité de l'air soit « modérée ». D'où sort ce chiffre ?

Après une phase transitoire où elle varie, la teneur en CO_2 se stabilise lorsque