Bomba Kryptologiczna

de Matthieu Walraet

« J'ai quelque chose à te montrer. » J'ai pris place devant mon ordinateur. Il était déjà allumé pour passer de la musique. En bas de l'écran, l'horloge affichait 01:47. La soirée était terminée, il n'en restait plus que des bouteilles vides, quelques restes de nourriture et Michel, toujours le dernier à partir. J'ai ouvert la page de Michel sur le site de l'université. J'ai récupéré son certificat et je l'ai exporté au format PKCS#7. J'ai ouvert une fenêtre de commande et tapé *cer2pvk* suivit du nom du fichier contenant le certificat.

« Laisse-moi deviner, c'est une commande pour extraire la clé privée d'un certificat, c'est ça ? » dit Michel d'un ton incrédule.

J'ai pris une photo avec la webcam : Michel et moi, l'air un peu ahuris, dans un éclairage trop rouge. J'ai copié la photo dans un document, je l'ai sauvegardé en PDF et je l'ai signé avec le certificat et sa clé privée. J'ai ouvert à nouveau le document pour vérifier que la signature électronique était bien valide.

Michel n'était pas encore convaincu. Il m'a fait recommencer l'opération avec un autre certificat, appartenant à un spécialiste en sécurité informatique que je ne connaissais pas. Il a copié les deux fichiers signés sur une clé USB et les a vérifiés sur son propre ordinateur portable.

« C'est impossible, il y a un truc. Si tu as trouvé une faille de sécurité dans RSA, les conséquences sont...

- C'est plus fondamental qu'une faille de sécurité.
- Je vois deux possibilités, j'ai du mal à évaluer laquelle est la moins impossible. Un, tu as trouvé un algorithme polynomial pour la factorisation des nombres entiers, à la stupéfaction de la communauté mathématique. Deux, tu disposes d'un ordinateur quantique. Les plus performants jusqu'à présent ne manipulent qu'une poignée de qubits. Ils sont à peine capables de factoriser le nombre quinze.
- J'ai fabriqué l'ordinateur quantique du pauvre, regarde. »

J'ai ouvert un tiroir. Là, relié au PC par un câble et un circuit électronique, se trouvait un pain de plastic et son détonateur. Le visage de Michel vira au blanc. Il tremblait, sa respiration était difficile. Pour briser le silence, je me suis lancé dans l'explication détaillée du dispositif.

« Une clé publique RSA est constituée de deux nombres : un module et un exposant. Le module est la multiplication de deux nombres premiers. Décomposer le module en ses facteurs premiers permet de déduire la clé privée et donc de casser RSA. Pour une clé publique de 2048 bits, comme celle de ton certificat, chacun des facteurs est un nombre de plus de trois cent chiffres. La factorisation d'un module de cette taille est hors de portée des moyens traditionnels.

Ce boîtier est générateur quantique de nombres aléatoires. Ce genre d'équipement est utilisé par des casinos en ligne et des sites de poker. J'ai écrit un programme qui utilise le générateur pour choisir au hasard un nombre entier de 1024 bit. Il fait une division entière du module RSA par ce nombre. Si le reste est nul, c'est gagné, il peut calculer la clé privée facilement. Sinon, il déclenche l'explosion de la bombe.

Nous ne survivons que dans les cas où la factorisation est réussie. Subjectivement, cela marche à tous les coups.

- Tu as fait ça... juste pour avoir raison. »

Nous étions revenu à notre éternel débat sur la physique quantique. Je suis un farouche partisan de l'interprétation d'Everett, dites des mondes multiples. Michel défend l'approche de Bohr. Il considère que les différentes interprétations sont vaines : une théorie physique sert à expliquer les observations et ne dévoile rien de la nature de la réalité.

« Oui, et alors ? J'avais raison et j'en ai enfin la preuve.

- Tu n'avais pas le droit de me faire subir cette expérience. C'est criminel !
- Nous sommes vivants, non ? La bombe n'a pas explosé.
- De notre point de vue c'est vrai. Pour nos amis, pour nos familles, la probabilité que la bombe explose était quasiment de un. Pour eux, nous sommes morts.
- C'est le cas, dans des mondes parallèles complètement inaccessibles.

- Ces mondes représentent la quasi-totalité des branches qui ont divergées depuis une demi-heure. Nous avions environ une chance sur dix puissance trois cents de survivre. Non, il faut mettre ça au carré, parce que j'ai commis l'erreur de te demander de refaire ta démonstration. Enfin au point où nous en sommes, c'est tout aussi epsilonesque.
- Sauf que j'ai effectué un premier essai seul. Si nous considérons les branches qui ont divergées depuis huit heures, tu as survécu dans la quasi-totalité.
- Super... Dans ces mondes-là, c'est moi qui ai raison et je pleure devant ta maison en ruines. De toute façon un jour ou l'autre, tu vas faire ta démo à quelqu'un d'autre et vous allez vous tuer. Promets-moi que tu n'utiliseras plus jamais ce truc.
- Je peux te promettre de ne jamais l'utiliser sans te prévenir, pour que tu puisses venir sur place. Comme cela tu n'en verras jamais les aspects négatifs.
- Bien sûr, il vaut mieux se faire tuer avec toi. Si c'est vrai pour moi, pourquoi cela ne serait pas vrai pour les autres, tout le reste de l'humanité qui ne peut pas *bénéficier* de ta machine ? Il faudrait faire venir tout le monde chez toi.
- Pas forcément, il serait possible d'utiliser les stocks d'ogives nucléaires, de les placer uniformément sur la surface de la terre et de les connecter à mon PC. Bon, cela risque d'être difficile de convaincre la population de l'opportunité d'annihiler toute vie sur terre pour décomposer un nombre en facteurs premiers, mais je peux adapter le système à des applications plus pratiques : l'optimisation de réseaux, la démonstration automatique de théorèmes...
- Attends... Il y a quelque chose que je ne comprends pas. Quand tu as effectué ton premier test, je n'étais pas près de la bombe. Les chances que tu réussisses la factorisation étaient quasi-nulles et je n'avais pas l'effet de sélection par suicide quantique pour compenser. Pourtant, tu as réussi quand même.
- C'est normal. Il y a forcément des branches historiques dans lesquelles j'ai réussi, et je n'existe plus dans les autres. Cette conversation ne peut avoir lieu que dans la situation où j'ai survécu. La personne que tu es à présent, qui possède l'expérience de cette conversation, ne peux exister que dans les très rares cas où la

factorisation a réussi. Tu bénéficies ainsi de l'effet de la bombe à posteriori. Autrement dit, si tu considères le point de vue global, englobant toute les branches possibles, une telle situation n'est pas paradoxale.

- D'accord, je comprends tout cela. Enfin, j'ai compris le principe, mais je n'arrive pas à me l'approprier. J'ai l'impression que l'idée même de probabilité n'est qu'une illusion. Si je lance une pièce de monnaie trente fois de suite, mon expérience me permettait de prédire qu'elle allait tomber sur pile la moitié des jets environ. Je ne peux plus lui faire confiance. Dans mon futur, il existe une version de moi qui a obtenu pile trente fois de suite. Il existe une branche où je vais continuer à avoir pile tout le reste de ma vie. Alors au bout de quarante ans, quand je vais lancer une pièce je serai certain qu'elle tombera sur pile. Pourtant elle aura toujours autant de chances de tomber sur face. Une prédiction toute simple, basée sur une expérience acquise durant toute une vie, n'a absolument aucune signification. J'ai l'impression d'être cette personne, qui obtient le côté face après quarante ans et pour qui cela signifie que le monde s'effondre. »

Michel s'arrêta de parler. Au bout d'une minute il prit place devant l'ordinateur. Il débrancha le détonateur et recommença la manipulation sur un troisième certificat. Il obtint une nouvelle photo avec une signature valide.

« Comment est-ce possible ? J'ai déconnecté la bombe, la probabilité que la factorisation réussisse était infinitésimale. Pourtant... elle n'est pas nulle. Dans la multitude des branches possibles, une toute petite partie contient des versions de nous-mêmes qui sont étonnées de voir un résultat positif. Les autres obtiennent un échec, mais cela ne change rien. En fait la bombe ne sert à rien !

- Je sais bien. D'ailleurs, ce n'est pas une bombe. C'est de la pâte à modeler, regarde. Où veux-tu que je trouve du plastic ? Tu croyais vraiment que je pouvais risquer de nous tuer simplement pour te convaincre que l'interprétation d'Everett est la bonne ? »

J'ai détaché un morceau de la soi-disant bombe et l'ai donné à Michel. La consistance et l'odeur étaient caractéristiques d'une simple pâte à modeler.

« En fait tout est faux. J'ai triché. Mon programme ne calcule pas la clé privée correspondant à la clé publique. Il créé une nouvelle clé privée et remplace la clé publique. Il signe le nouveau certificat avec un faux certificat racine de l'autorité de certification. J'ai configuré mon système pour qu'il accepte ce certificat racine, afin qu'il juge la signature valide.

- Je vois. Toute la chaîne de certification est bidon, tu peux faire ce que tu veux tant que cela reste chez toi. Par contre, comment as-tu fait pour que la signature soit valide sur mon PC portable ?
- Eh bien... Je sais que tu visites mon blog régulièrement. Or tu n'as pas patché le dernier zero-day d'Internet Explorer. J'en ai profité pour installer mon faux certificat racine sur ton ordinateur. »

Michel se met rarement en colère, mais quand il y va, c'est pour de bon. Il a très mal pris que je pirate son ordinateur. Il a dit ce qu'il pensait de mon canular et est parti en claquant la porte.

Le lendemain, j'ai tenté à plusieurs reprises de lui téléphoner pour m'excuser mais je n'avais que sa messagerie. Ce qui me semblait une bonne blague quand je l'ai mise au point me paraissait à présent une idée stupide. Comment ai-je pu imaginer un seul instant que Michel allait trouver cela drôle? Je commençais à m'inquiéter de n'avoir aucune nouvelle. Le soir, j'ai enfin reçu un appel.

« Salut, c'est Michel. Je suis sur la côte, là. J'ai fait une grande balade, j'avais éteint mon téléphone. C'est moi qui dois m'excuser. J'étais vexé de m'être fait piéger, j'y ai vraiment cru. Tu as dû passer un temps fou à tout préparer. Grâce à cela, j'ai compris quelque chose. Je faisais un blocage sur l'interprétation d'Everett, pour des raisons irrationnelles. Mon appréhension du futur, un sentiment naturel, se trouvait démultipliée par le nombre des avenirs possibles jusqu'à devenir inacceptable. Quand je me suis retrouvé dans la situation où l'interprétation des mondes multiples était un fait prouvé, j'ai compris que l'univers n'avait rien à faire de nos états d'âme et qu'il fallait l'accepter tel qu'il est.

Bien entendu, la preuve était fausse. Cependant mon blocage est tombé. Je me rends compte maintenant que l'interprétation de Copenhague n'est qu'une façon de se mettre des œillères. La vision d'Everett me semble une évidence. Tout me paraît plus clair, plus simple, plus vrai, plus juste. C'est extraordinaire ! »

Quelques références:

Factorization of a 768-bit RSA modulus
http://eprint.iacr.org/2010/006.pdf

Code-breaking quantum algorithm run on a silicon chip
http://www.newscientist.com/article/dn17736-codebreaking-quantum-algorithm-run-on-a-silicon-chip.html

The Everett FAQ
http://www.hedweb.com/everett/everett.htm