11. Les mondes d'Impagliazzo

Le développement d'une théorie de la complexité des algorithmes fait suite aux travaux de Turing sur la calculabilité. Son développement au cours de la deuxième moitié du vingtième siècle a conduit à distinguer plusieurs classes de problèmes selon la complexité des algorithmes pour les résoudre sur une machine de Turing.

La qualité d'un chiffre revendiquant l'impossibilité d'éclaircir un cryptogramme en l'absence de la clé de chiffrement, les cryptologues se sont naturellement penchés cette théorie. Ainsi la classe P est celle des problèmes pour lesquels il existe un algorithme de résolution efficace, c'est-à-dire s'exécutant sur une machine de Turing déterministe, et dont la complexité est bornée par un polynôme de la taille des données d'entrée. Ces problèmes sont ceux qui sont résolubles en pratique. Cela doit être le cas du chiffrement ou du déchiffrement en connaissance de la clé. Une autre classe remarquable est la classe NP, pour *Non-deterministic Polynomial.* Elle est celle des problèmes pour lesquels il existe un algorithme efficace s'exécutant sur une machine de Turing *non déterministe*, c'est-à-dire une machine qui, à chaque pas de son exécution, comporte de plusieurs continuations possibles.

Après avoir démontré l'équivalence des automates à mémoire finis déterministes et non déterministes, la théorie s'est naturellement penchée sur cette question d'équivalence entre déterminisme et non déterminisme pour les machines de Turing, et, en l'absence de réponse, aboutir finalement à la fameuse conjecture P=NP ? qui est l'un des grands problèmes encore non résolus du prix du millénaire. Une machine non déterministe peut être vue comme guidée par un oracle qui lui indique la marche à suivre, la direction à prendre parmi tous les choix ouverts à chaque pas du programme afin aboutir au plus vite au résultat. Lorsque la solution au problème est connue, elle peut tenir lieu d'oracle, de telle sorte qu'un problème NP peut être vu comme un problème dont la vérification peut se faire avec un algorithme efficace. Mais les problèmes difficiles qui présentent un intérêt pratique sont précisément ceux dont la solution est vérifiable en temps raisonnable, c'est-à-dire les problèmes NP.

Il existe encore aujourd'hui des problèmes, comme la factorisation des entiers, qui sont difficiles à résoudre, mais facilement vérifiables. Cette difficulté est-elle intrinsèque au problème, ou bien n'est-elle due qu'à notre ignorance ? Découvrirons-nous dans l'avenir un algorithme efficace de factorisation ? Ou bien prouverons-nous que ce problème est d'une difficulté telle qu'il est illusoire de chercher un tel algorithme ?

Nous sommes ainsi aujourd'hui en pratique dans un monde où P ≠ NP. Mais cette appartenance reset virtuelle dans la mesure où elle n'est peut-être que provisoire – ou définitive – en attendant que ne soit prouvée – ou infirmée – l'identité des classes P et NP.

Un problème NP est appelé *complet* si tous les problèmes NP peuvent s'y ramener efficacement. Ils apparaissent ainsi parmi les problèmes les plus difficiles de cette classe. Mais ce niveau de difficulté est insuffisant pour traiter de ce qui survient en cryptographie. Dans leur article fondateur de la cryptographie à clé publique, Diffie et Hellmann ont invité les chercheurs à fonder leur nouvelle cryptographie sur des problèmes NP complets, en proposant l'exemple du problème du sac à dos. Plusieurs propositions en ont résulté, mais qui ont toutes été successivement cassées, les instances pratiques de ce problème étant toujours faciles à résoudre, jusqu'à ce que les chercheurs abandonnent finalement toute recherche dans cette direction.

La difficulté attendue des problèmes cryptographiques est une difficulté *en moyenne*, théorie développée par Lenoid Levin (né en 1948) et qui a inspiré au chercheur Russel Impagliazzo (né en 1963) la possibilité de cinq mondes qui diffèrent selon le type de problèmes qu'il y est possible de résoudre avec efficacité. Impagliazzo a vulgarisé cette théorie en illustrant sa visite guidée des cinq mondes par l'usage de la cryptographie, mais aussi en mettant en scène Grouse1, professeur imaginaire du jeune élève Gauss, qui voulait poser une colle en lui demandant la somme des entiers de 1 à 100. Après avoir été humilié devant toute la classe par la réponse rapide du brillant élève, le malheureux professeur a passé le reste de sa vie à chercher sans succès un problème qui pourrait mettre fin à l'arrogant succès de son élève pour finir misérablement sa vie dans un asile d'aliénés.

(c) http://eecs.umich.edu/cse/fischer_symposium/index.html

Algorithmica.

Ce monde est celui dans lequel P=NP. Il y existe une méthode pour produire la solution d'un problème à partir d'un algorithme de vérification de la solution. Grouse ne peut pas coller Gauss avec un problème dont il pourrait présenter la solution à toute la classe, puisque ce dernier peut trouver la solution directement avec l'algorithme de vérification. L'informatique s'en trouve

révolutionnée. L'ordinateur peut se charger de toutes les tâches dévolues aux humains. Parler une langue naturelle se réduit à savoir lire et interpréter un corpus réduit de textes. Savoir multiplier revient à savoir factoriser, déchiffrer et décrypter, avec ou sans la clé, sont des problèmes de difficultés équivalentes, et aucune cryptographie n'y est possible autre que le masque jetable du téléphone rouge. Dans ce monde, il est impossible de réserver à l'accès à une information à certaines personnes seulement sans que tous ne puissent également y accéder. Le prix à payer à savoir résoudre tous les problèmes algorithmiques de la vie courante est l'impossibilité d'y conduire la moindre cryptographie efficace.

Heuristica.

Heuristica est un monde ou les problèmes NP ne sont difficiles que dans le pire des cas, mais sont en moyenne faciles. Les instances difficiles des problèmes NP existent, mais sont également difficiles à trouver. Le temps moyen pour résoudre un problème NP reste comparable à celui pour en concevoir l'énoncer. Grouse peut coller Gauss avec un problème difficile, mais il lui faudra au moins deux fois plus de temps pour l'établir qu'à Gauss pour le résoudre – n'oublions pas qu'il est un élève particulièrement brillant. En pratique, ce monde est en presque tout point comparable à Algorithmica. La différence réside dans l'existence de rares problèmes pratiquement insolubles. Supposons par exemple que la recherche d'un problème mathématique prennent un temps t, et sa résolution un temps $2t$. Comme tout chercheur le sait, la réponse à un problème conduit invariablement à un nouveau problème. En Heuristica, ce deuxième problème, qui survient au bout d'un temps $3t$ prend un temps $6t$ à être résolu. La récurrence est exponentielle, et en quelques itérations, la frontière de l'infaisable est rapidement atteinte. D'un point de vue cryptographique, le temps passé à trouver un chiffre correspond au temps pendant lequel le secret et garanti. En Heuristica, il n'y a pas plus d'espoir qu'en Algoritmica de trouver une cryptographie efficace.

Pessiland.

Selon Impagliazzo, ce monde est le pire qui soit. Il existe des problèmes difficiles à résoudre en moyenne, mais pour toute fonction efficacement calculable, il existe une façon efficace de trouver un antécédent à une valeur donnée. En d'autres termes, il n'existe pas de fonction à sens unique. En Pessiland, il est facile de produire des instance difficiles de problèmes NP, mais il n'est pas possible de produire des instances difficiles de problème dont la solution soit connue. En Pessiland, Grouse peut poser à Gauss une colle insoluble, mais personne, y compris la grande force intuitive de Gauss, ne pourra en pratique conduire à une solution. L'humiliation de Grouse restera entière lorsque la classe demandera la réponse au professeur qui aura toute les difficultés du monde pour en exhiber une. La théorie cryptographique fonde le chiffrement symétrique – celui où les deux participants partagent la même clé – sur un axiome d'existence de fonction à sens unique. En Pessiland, de nombreux problèmes de la vie courante restent difficile, mais aucun d'entre eux ne peut être utilisé à des fins cryptographiques. Ce monde agaçant cumule tous les désavantages.

Minicrypt.

Dans Minicrypt, les fonctions à sens unique existent. La cryptographie symétrique est possible, mais pas la cryptographie à clé publique. Deux correspondants devront préalablement s'accorder sur une clé secrète, fusse-t-elle de taille réduite, pour pouvoir échanger par la suite de façon tout à fait discrète une très grande quantité d'informations sur un canal public. Une fonction à sens unique *f* peut être utilisée pour produire un problème difficile dont ont connaît une solution, par exemple en tirant un élément *x* au hasard, en calculant *y=f(x)* et en posant le défi de trouver un antécédent à *y*. Dans ce monde, Grouse garde la tête haute, car il peut poser à Gauss un problème qu'il aura bien du mal à résoudre. Il pourra même exhiber fièrement la solution à la classe ébahie et emporter une certaine victoire. La théorie cryptographique montre qu'en Minicrypt, il est aussi possible de produire des signatures à clés asymétriques, une clé privée pour produire la signature et ne clé publique pour sa vérification. Contrairement à ce que pensaient Diffie et Hellman dans leur article fondateur de la cryptographie à clé publique, la frontière des mondes n'est pas entre cryptographie symétrique et cryptographie asymétrique, mais seulement avec le chiffrement asymétrique qui, lui, appartient au monde suivant.

Cryptomania.

Cryptomania est le monde le plus proche de celui dans lequel nous vivons aujourd'hui. La cryptologie à clé publique y est possible. Deux correspondants peuvent s'accorder sur un secret partagé commun à partir de données qu'ils s'échangent publiquement. Cette cryptographie à clé publique repose sur la notion de *fonction à sens unique à porte dérobée*. Il s'agit d'une fonction dont les valeurs sont efficacement calculables, les antécédents sont difficiles à exhiber sauf pour les détenteurs d'une information supplémentaire qui constitue la porte dérobée. Ainsi, tout le monde peut chiffrer un message, mais le déchiffrement reste réservé au seul détenteur de la porte dérobée qui tient lieu de clé privée. En Cryptomania, Grouse peut enfin asseoir son autorité en posant à la classe entière un problème pratiquement impossible à résoudre. Mieux, il peut humilier Gauss en révélant au reste de la classe une indication qui leur permet d'accéder à la solution, alors que pour le pauvre Gauss resté dans l'ignorance de cette indication, le problème restera définitivement insoluble. En Cryptomania, les possibilités de la cryptologie n'ont de limites que celles de l'imagination des concepteurs : vote électronique, monnaie digitale anonyme, manipulation de données chiffrées. Le niveau d'intimité de la sphère privée n'est pas limité limité par la technique, mais seulement par des décisions sociales ou politiques qui dictent la détention des portes dérobées.

Ces mondes constituent une hiérarchie de mondes possibles ou impossibles selon que la théorie de la complexité démontrera l'existence de problèmes difficiles ou infirmera leur existence en découvrant des algorithmes efficaces pour les résoudre.

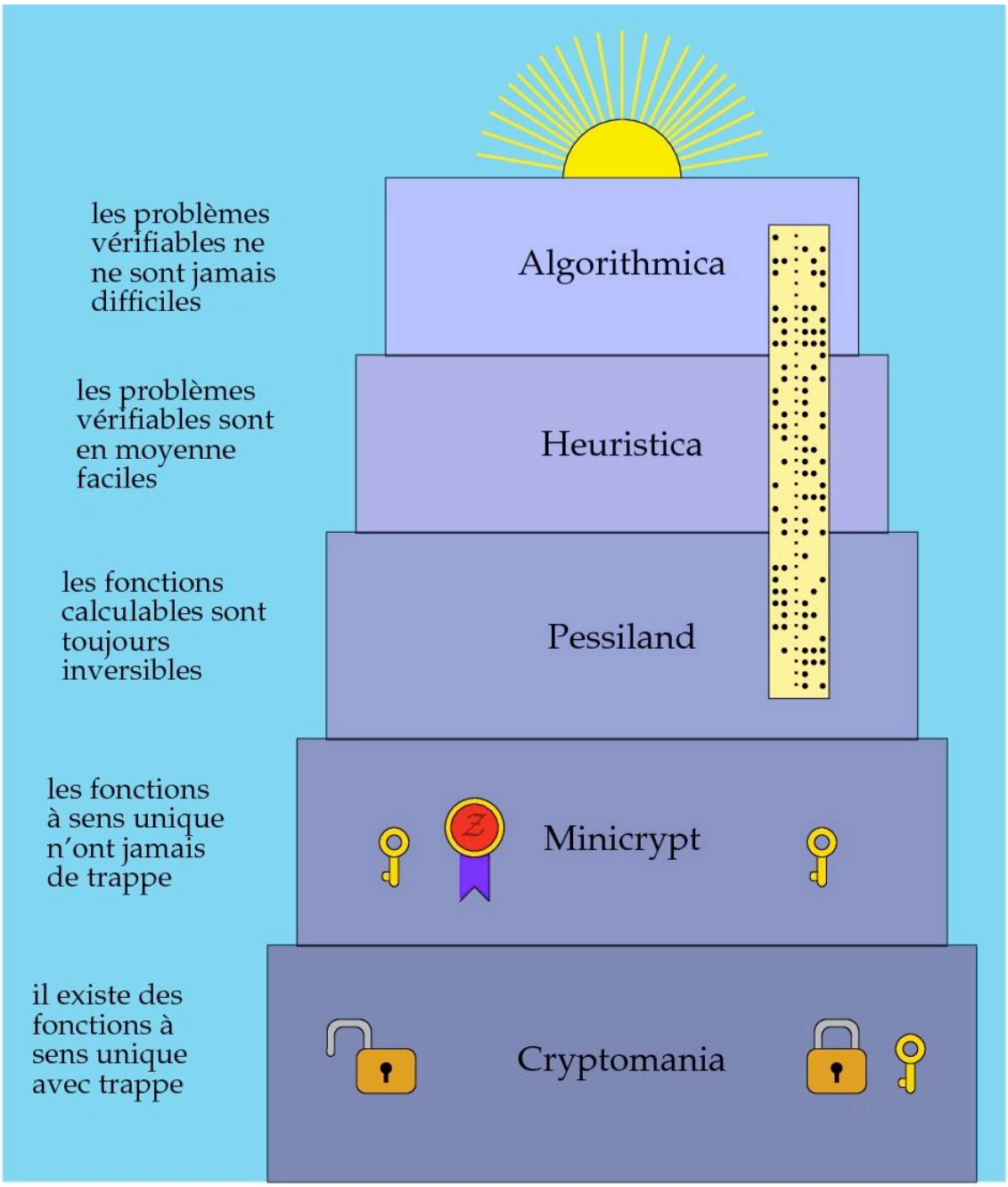

Fig. 6.7 Les cinq mondes d'Impagliazzo. Ces mondes sont des mondes imaginaires possibles en l'état actuel de nos connaissances. Le développement de la théorie pourrait, soit les rendre réels et non plus imaginaires, soit les faire disparaître. Toute la cryptographie, et en particulier le chiffrement à clé publique appartient au monde Cryptomania qui est notre monde empirique actuel. Le chiffrement symétrique et la signature à clé publique appartiennent au monde Minicrypt. La seule cryptographie utilisable dans les autres mondes est la cryptographie inconditionnellement sûre comme le chiffre de Vernam avec bande aléatoire. Il est étonnant de noter que la signature à clé publique appartient au monde Minicrypt, alors que le chiffrement à clé publique appartient, lui, au monde Cryptomania.

Cette visite guidée d'Impagliazzo se termine sur un cri d'alarme : Si un façon efficace de factoriser ou de calculer des logarithme discrets venait à être découverte, alors non seulement les plus

populaires des systèmes cryptographiques à clé publique viendraient à être cassés, mais il n'y aurait aucun autre candidat, ni de méthode systématique applicable pour concevoir une alternative sûre. Il n'y aucune raison théorique connue à la difficulté intrinsèque de la factorisation ou du logarithme discret. Notre confiance dans leur difficulté repose sur notre ignorance de méthode efficace de résolution, après plus de vingt années d'intense recherches sur cette question. Mais les progrès accomplis – surtout des progrès dans la puissance de calcul des ordinateurs – ont frappé d'obsolescence les clés publiques produites aux débuts de cette nouvelle cryptographie, et il est impossible de dire quelle taille de clé est convenable aujourd'hui pour garantir une sécurité pour les vingt prochaines années.

L'édifice de la cryptographie à clé publique est bâti sur du sable. Cet avenir semble inquiéter jusqu'en haut lieu, en témoigne depuis 2014, la tenue du congrès annuel *catacrypt2,* parrainé par les plus grandes organisations dont la cryptologie à clé publique est au cœur de l'activité.