# ASSOCIATION des RÉSERVISTES du CHIFFRE

Document interne à l'Association réservé aux adhérents

*Nouvelle série*
*N° 17 - 1989*

Le dernier cri des études et recherches de cryptologie

# « La preuve sans transfert de connaissances »

Cattieuw

La société moderne s'automatise, s'informatise, se télématise toujours davantage ; de nouveaux outils de communication et de traitement des informations apparaissent et prolifèrent et, peu à peu, les systèmes d'information envahissent notre vie. Cette évolution s'accompagne de problèmes cruciaux de protection de l'information : des données vitales de toute sorte sont massivement traitées par ordinateurs, des informations sensibles s'accumulent dans les mémoires informatisées, des transactions traduisant des opérations économiques ou financières considérables se multiplient au travers des réseaux ; cet état de chose ne manque pas de stimuler la convoitise et l'imagination des indiscrets et fraudeurs de tout poil.

Fondamentalement, protéger un système d'information revient à vérifier qui fait quoi et pour quoi faire et, tout d'abord, à savoir qui est qui afin de reconnaître les « ayants droits » aux ressources informatiques. Pour cela, lorsqu'ils accèdent à un système sensible, ces derniers doivent faire connaître leur identité puis la prouver en s'authentifiant. De son côté le système doit authentifier l'utilisateur présumé : il vérifie, à l'aide d'un mécanisme approprié que l'identité prétendue de l'utilisateur est correcte et qu'il n'a pas affaire à un imposteur. Ce mécanisme fonctionne selon trois approches classiques visant à vérifier une caractéristique, une chose ou une information que :

1 - la personne possède physiologiquement
2 - la personne est seule à détenir
3 - la personne est seule à connaître.

La première approche repose sur la vérification de caractéristiques physiques (empreintes digitales, empreintes vocales, géométrie de la main, dynamique de la signature, etc). Théoriquement très efficace, elle se révèle souvent peu fiable et, en tout cas, difficile à mettre en œuvre du point de vue technique.

La deuxième recourt, par exemple, à des clefs physiques, à des badges de divers types lisibles par une machine parmi lesquels se rangent les cartes à pistes magnétiques et les fameuses cartes à microprocesseur.
Quant à la troisième approche, elle couvre l'emploi de « mots de passe » et de « codes confidentiels », solution la plus banale et la plus communément utilisée

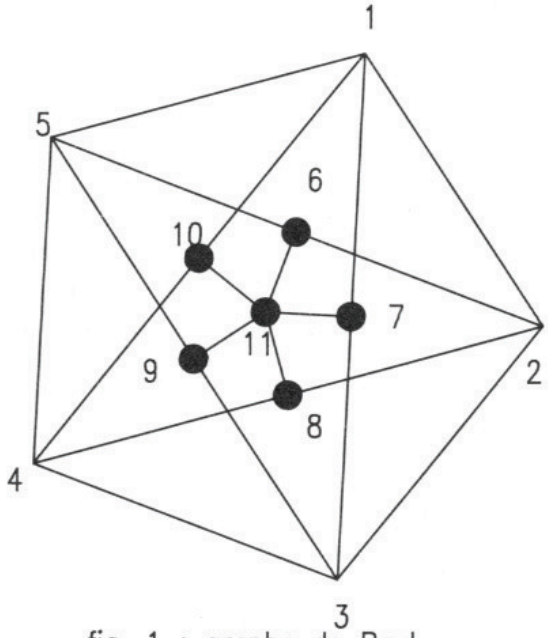
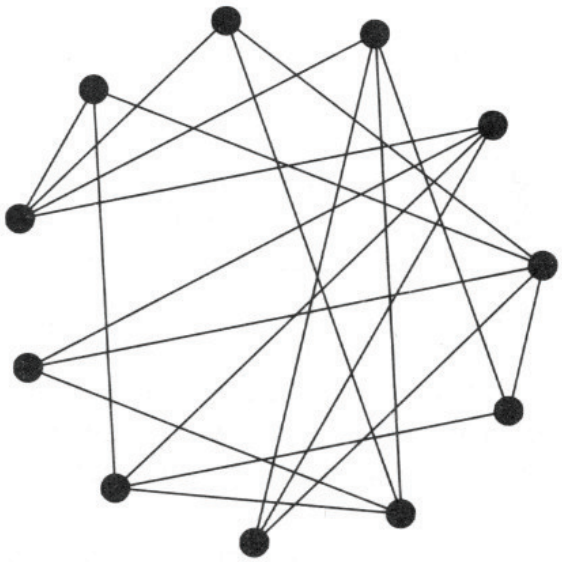
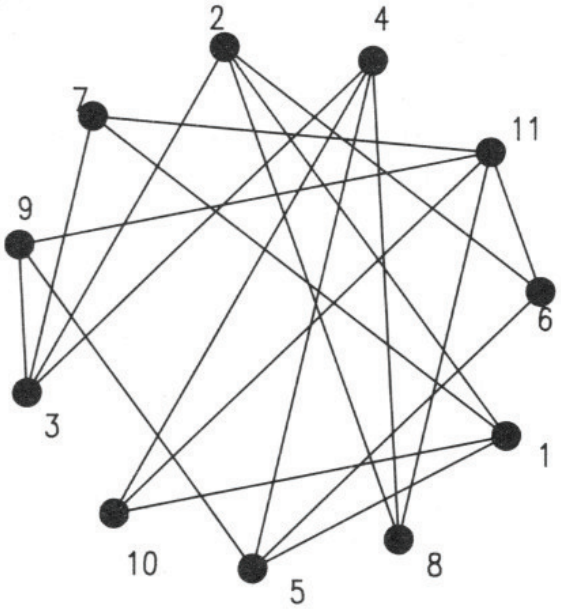


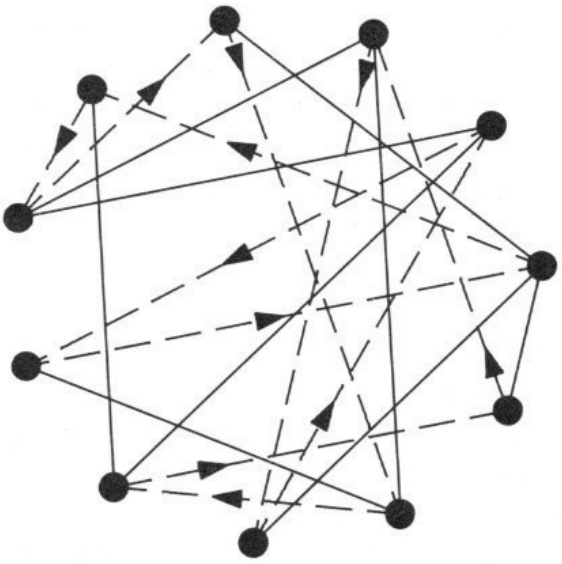

fig. 1 : graphe de Paul
inscrit a l'annuaire



schema A
Schema de test presente par Paul
pour repondre aux deux demandes
possibles de Pierre.




schema B
Reponse de Paul a la demande
de numerotation des sommets.



schema C
Reponse de Paul a la demande
de revelation du circuit

mais qui est loin d'être efficace. Un mot de passe peut être oublié, perdu ou volé ; il peut être communiqué à un tiers non autorisé, il peut être facilement compromis. Il suffit pour s'en convaincre d'observer le peu de précaution que prennent la plupart des porteurs de cartes bancaires pour pianoter leur « code secret » sur le clavier d'un distributeur de billets ou de la machine comptable d'un commerçant.

Non seulement l'emploi du mot de passe pêche par son insécurité mais son principe même offre une contradiction flagrante : le mot de passe doit être tenu secret par son détenteur. Mais celui-ci, pour s'authentifier, doit l'exhiber à un tiers qui en prend connaissance. Celui-ci peut donc, s'il est malhonnête, s'en servir pour se faire passer pour qui il n'est pas.

Placés devant cette contradiction, les mathématiciens-cryptologues ont tenté d'imaginer un mot de passe que l'on ne montrerait jamais. Pour cela ils ont été conduits, en 1985, à poser la question paradoxale suivante : peut-on vérifier, sans en prendre connaissance, qu'une personne connaît une information secrète ? ou encore, exprimé de façon plus technique ; peut-on, sans en donner la démonstration, prouver à un mathématicien que l'on a découvert la solution d'un problème réputé difficile ?
Pour répondre à la question les mathématiciens ont défini une notion nouvelle appelée « zéro knowledge proof » – traduisez « preuve sans transfert de connaissance », ce qui signifie, preuve, avec apport nul de connaissance, de la véracité d'une affirmation – notion qui se révèle riche de retombées potentielles en cryptologie.

Lors d'un congrès de mathématiques tenu en août 1986 à l'université de Berkeley une réponse affirmative a été donnée à la question posée un an auparavant. La réalité de l'existence de la « preuve sans transfert de connaissance » a été démontrée, en termes accessibles par des non spécialistes, par exemple simple issu de la théorie des graphes. Pour comprendre cet exemple quelques explications très élémentaires suffisent.

### *Circuit hamiltonien dans un graphe.*

Un graphe (voir fig. 1) est un ensemble de points, encore dénommés « sommets », reliés de façon précise par des lignes appelées « arêtes ». Des exemples de graphes se trouvent aisément dans la vie pratique : une carte routière est un graphe dont les villes sont les sommets et les routes qui les relient les arêtes. De même les cases d'un organigramme contituent les sommets d'un graphe dont les arêtes sont les traits traduisant les relations hiérarchiques et fonctionnelles.

Partant d'un sommet on peut en rejoindre d'autres en parcourant une succession d'arêtes du graphe, un trajet de ce genre est un « chemin », et, un chemin dont le sommet de départ coincide avec le sommet d'arrivée constitue un « circuit ». Enfin, un circuit passant une seule fois par chaque

sommet d'un graphe est un « circuit hamiltonien ».

Il faut bien voir qu'il est facile à n'importe qui de bâtir un graphe comportant un circuit hamiltonien. Mais, à l'inverse, placé devant un graphe quelconque comptant un grand nombre de sommets et d'arêtes (disons de l'ordre du millier par exemple) répondre à la question « ce graphe possède t-il, ou non, un circuit hamiltonien ? » est très difficile. En effet, la première idée qui vient à l'esprit pour y répondre est de rechercher le circuit demandé en dressant, de façon systématique, la liste de tous les circuits possibles du graphe afin de constater si elle y inclut un circuit hamiltonien. On s'aperçoit alors que le nombre élevé de sommets et d'arêtes rend cette façon de faire effrayante de complexité car la liste des circuits devient vite trop longue pour être traitée. Les mathématiciens, et parmi eux les meilleurs, sont nombreux depuis plus d'un siècle à avoir médité ce problème, néanmoins les méthodes de résolution les plus performantes connues aujourd'hui ne sont pas fondamentalement meilleures que cette recherche systématique : toutes exigent une puissance colossale de traitement par ordinateur ou un temps de calcul prohibitif. Bien qu'aucune méthode rapide de solution n'ait été trouvée, il n'a cependant pas été prouvé qu'il n'en existait pas une et, si elle existe, un mathématicien génial la découvrira peut-être demain, ou dans mille ans, sans qu'il soit possible de le prévoir aujourd'hui. Trouver la solution à la question de savoir si un graphe de grande taille possède, ou non, un circuit hamiltonien est donc, en pratique, impossible dans l'état actuel des connaissances. En revanche, si l'on connait la solution il est très facile de le prouver en énumérant tout simplement les arêtes successives du circuit hamiltonien. C'est sur cette constatation – impossibilité de résoudre le problème mais facilité de prouver qu'on en connait la solution – qu'est fondée l'idée des nouveaux procédés d'authentification basés sur le concept de « preuve par transfert nul de connaissance ».

Pour s'en rendre compte, imaginons un jeu à deux partenaires, Paul et Pierre : Paul désire prouver son identité à Pierre qui veut la vérifier :

***Paul, sans dire ce qu'il sait, doit convaincre Pierre qu'il sait ce qu'il prétend savoir.***

Paul a construit le graphe de la fig. 1 en s'arrangeant pour qu'il possède un circuit hamiltonien (celui-ci relie successivement les sommets 1 - 5 - 6 - 2 - 8 - 4 - 10 - 11 - 9 - 3 - 7 - 1). Seul Paul connait le circuit hamiltonien et il le garde précieusement secret. Il dispose donc d'une information secrète exclusive qui est la solution au problème complexe de la recherche du circuit hamiltonien dans ce graphe, problème qu'en principe personne ne sait résoudre.

Paul s'adresse à l'autorité gérant la sécurité d'un système d'information ; celle-ci a pour rôle de tenir à jour scrupuleusement un annuaire public d'identification et

d'authentification des usagers que chacun peut consulter. Paul y fait inscrire son identité (par exemple son nom, son numéro de téléphone, son « pseudo », etc) et son graphe personnel (de la fig. 1).

Cette inscription faite à l'annuaire, Paul proclame son identité à Pierre et le processus d'authentification, suivant, à trois étapes, commence et est répété autant de fois que Pierre le désire.

***1re étape : Paul présente un shéma de test.***

Secrètement Paul dispose en cercle, régulièrement espacés autant de points qu'en comporte son graphe inscrit à l'annuaire (ici 11). Il numérote ces points au hasard en prenant soin d'écrire les nombres légèrement au crayon. Puis il trace les arêtes reliant les mêmes sommets que sur son graphe personnel. Enfin il gomme, sans laisser de trace, la numérotation des points et obtient le schéma de test, identique au schéma A, qu'il présente à Pierre.

***2e étape : Pierre fait un demande à Paul.***

Selon un jeu à pile ou face, Pierre, en présence du schéma de test, demande à Paul :

- soit de lui révéler les numéros des sommets (schéma B) : Pierre pourra donc vérifier en comparant le schéma B au graphe de l'annuaire que ceux-ci sont bien identiques, les mêmes arêtes reliant les mêmes sommets deux à deux.
- soit de lui indiquer le circuit hamiltonien sans indiquer la numérotation des sommets (schéma C) : Pierre pourra donc vérifier l'existence du circuit hamiltonien sans que celui-ci soit révélé puisqu'il ne connaîtra pas l'ordre de parcours des points.

***3e étape : Paul répond à la demande de Pierre.***

Selon la demande, Paul révèle le schéma B ou le schéma C.

Le processus est recommencé autant de fois que la réponse de Paul satisfait Pierre mais, si Paul ne répond pas de façon satisfaisante à une demande, Pierre arrête le processus d'authentification et considère que le prétendu Paul est un imposteur. En effet, si Paul n'est pas un bluffeur, il doit répondre sans erreur à l'une ou à l'autre demande de Pierre aussi longtemps que Pierre le désire.

Examinons la situation de plus près :

Si Paul est, en réalité, un intrus voulant se faire passer pour Paul. Il lui faut convaincre Pierre qu'il connaît le circuit hamiltonien alors qu'il ne le connaît pas et qu'il est incapable (...dans l'état des connaissances actuelles) de le trouver au vu du graphe publié à l'annuaire.

Il peut tenter de répondre à la demande de numérotation des sommets. Pour celà il lui suffit, à partir du graphe de l'annuaire public, de construire le schéma de test mais il sera démasqué si Pierre lui demande le schéma B.

A contrario, s'il veut pouvoir dévoiler le circuit hamiltonien du schéma C, il est contraint de bâtir un graphe possédant un tel circuit (le seul moyen d'y échapper serait d'avoir résolu le problème). De ce graphe il dérive aisément le schéma de test mais sa supercherie sera découverte si Pierre lui réclame la numérotation des sommets car le faux schéma de test numéroté ne correspondra pas au graphe de l'annuaire.

En définitive, l'imposteur est placé dans la situation délicate de devoir choisir, sans connaître à l'avance la demande de Pierre, laquelle des deux demandes il satisfaira sachant que s'il répond correctement à l'une sa réponse pour l'autre est fausse. Il doit donc tenter sa chance en étant conscient qu'il n'a qu'une chance sur deux de berner Pierre à chacune de ses demandes.

Combien de fois Pierre va-t-il recommencer le processus ?

C'est à lui d'en décider selon ses exigences de sécurité.

La 1re fois Pierre a une chance sur deux (1/2) d'être trompé et de confondre un imposteur avec Paul, la 2e fois une chance sur quatre (1/4) = $(1/2)^2$, la 3e fois une chance sur huit (1/8) = $(1/2)^3$ ... La 50e fois environ une chance sur un million de milliards $(1/2)^{50}$. Pierre admettra sûrement que 50 réponses correctes de Paul réduisent la possibilité d'être trompé à un niveau assez faible pour se déclarer convaincu que Paul connait bien ce qu'il prétend connaître et qu'il est bien celui qu'il déclare être.

Cependant Pierre, comme toute autre personne qui aurait assisté à l 'entretien et aurait enregistré les demandes et les réponses, n'a obtenu aucun renseignement sur le circuit hamiltonien de Paul et se trouve tout aussi ignorant qu'auparavant. Chaque vérification s'est limitée à comparer deux graphes (celui de l'annuaire et le schéma B) ou bien à observer un circuit reliant les sommets anonymes du schéma C, elle n'a fourni aucune connaissance réelle sur le circuit hamiltonien lui-même. Pierre n'a donc obtenu rien de plus que ce qu'il aurait pu connaître lui-même avant le déroulement du processus d'authentification.

Avec un peu de réflexion, on observe que :

- La connaissance simultanée du schéma B et du schéma C donne directement le circuit tant convoité : Paul devra y veiller et ne jamais laisser coexister ces deux schémas.

- l'imposteur qui, tel un oracle, devinerait à l'avance les demandes de Pierre le tromperait à coup sûr : Pierre doit prendre soin de choisir ses demandes au hasard selon un jeu de pile ou face joué avec une pièce honnête et loyale.

- si Pierre découvrait une loi utilisée par Paul pour numéroter les sommets il pourrait percevoir le secret de Paul par une suite de demandes judicieuses. De même si Paul choisissait deux fois la même numérotation au cours du processus et que Pierre s'en aperçoive dès l'apparition du schéma

de test de la seconde tentative, il lui serait facile de poser la demande qui lui permettrait de connaître exactement le circuit de Paul : Paul doit donc choisir sa numérotation au hasard pour éviter de divulguer indirectement son secret.

- un observateur neutre examinant le déroulement du processus n'acquiert aucune certitude car il peut soupçonner avoir affaire à une paire de complices qui se seraient entendus, à l'avance, sur de prétendus choix au hasard : si Pierre est convaincu de l'identité de Paul, un observateur ne l'est pas.

- un imposteur qui parviendrait à falsifier l'annuaire public en remplaçant le graphe de Paul par un graphe de son cru se ferait passer pour Paul auprès de quiconque et Paul ne pourrait plus se faire reconnaître de personne : l'autorité responsable de l'annuaire doit veiller jalousement à son intégrité et s'en porter garante.

### *Les applications.*

Sitôt démontrée l'existence de la preuve par transfert nul de connaissance, les mathématiciens cryptologues se sont empressés de rechercher les problèmes mathématiques, analogues à celui de la recherche du circuit hamiltonien d'un graphe, susceptibles d'une réalisation pratique. La première application envisagée, compte tenu de ses implications commerciales importantes, est la preuve de l'authenticité des cartes à micro- circuit dont l'utilisation à l'échelle mondiale sera généralisée en monétique.
L'authentification basée sur la « preuve par transfert nul de connaissance », si elle peut être réalisée grâce au microcircuit d'une carte bancaire, ouvre en effet la voie à la conception de cartes inimitables capables de prouver elles-mêmes leur authenticité. Des faussaires même très astucieux ne pourront pas contrefaire de vraies fausses cartes bancaires.

Dès l'été 1986 une équipe de chercheurs a déposé aux Etats-Unis une demande de brevet dans ce domaine et de Département de la Défense (DOD) en a demandé la mise au secret dans l'intérêt de la défense nationale des Etats-Unis. Au delà des intérêts commerciaux en jeu, la communauté des mathématiques a mal accepté l'idée que les recherches de mathématiques fondamentales et, même leurs applications, puissent être assimilées aux technologies sensibles contrôlées par l'Etat. Quoi qu'il est soit le DOD dut se rendre à l'évidence que la recherche mathématique, même touchant à la cryptologie, était une affaire internationale : les auteurs de l'invention, avant l'intervention du DOD, avaient déjà abondamment commenté et exposé leur trouvaille à l'occasion de séminaires internationnaux ; certains d'entre eux ne possédaient pas la nationalité américaine et leurs recherches avaient été financées par des universités étrangères ce qui a conduit le DOD à lever son interdiction.
En France nous ne sommes pas en retard, en 1987 une demande de brevet analogue a été déposée conjointement par le Centre

Commun d'Etudes de Télédiffusion et Télécommunications (G.I.E commun au CNET et à TDF) et le laboratoire de recherche de Philips ; elle permettra de maintenir et de consolider notre position dans l'âpre combat qui se livre au niveau international pour la normalisation de la carte à microcircuit, invention française et l'un des fleurons de la télématique française.

Cattieuw