Introduction

"L*ES sanglots longs des violons de l'automne, blessent mon coeur d'une langueur monotone"*. Durant la dernière guerre mondiale, à l'écoute de cette phrase, extraite d'un poème de Paul Verlaine, de nombreux réseaux de résistance surent que le débarquement était proche. Ce message chiffré est sûrement l'un des plus célèbres de l'histoire contemporaine française, et illustre parfaitement le principe de base de la cryptographie : modifier un message de façon à ce que son contenu soit inintelligible pour quiconque, sauf pour son destinataire.

La cryptographie est une science qui a occupé les esprits depuis la haute antiquité. Les méthodes de cryptage n'ont cessé d'évoluer de pair avec la puissance de calcul des ordinateurs. La cryptographie n'est plus un domaine réservé aux hommes d'Etat, aux ambassadeurs ou aux militaires, elle s'utilise aussi dans les milieux bancaires et industriels.

Avec l'avènement des réseaux informatiques internationaux, le problème de la sécurité, lors de l'échange de données, est plus que jamais au goût du jour. Il ne se passe pas un jour sans que les médias vantent les mérites des "autoroutes de l'information" et du réseau Internet. Le développement exponentiel du réseau nécessite la mise au point de protocoles de sécurité sûrs, aussi bien pour contrôler l'identité d'un individu, que pour valider, et certifier, une quelconque transaction entre deux personnes.

Une étude menée aux Etats-Unis, a montré que le réseau Internet a provoqué une augmentation de 400% de l'espionnage étranger, et une propagation, sans précédent, de virus et autres chevaux de Troie. En 1992, il y aurait eu un million d'effractions "virtuelles", sans compter les centaines de milliers de mots de passe et autres codes d'accès volés chaque année.

Les journaux relatent de plus en plus souvent les "exploits" de pirates informatiques ayant réussi à s'infiltrer sur des serveurs plus ou moins sensibles.

Plus que jamais, protéger les informations confidentielles et s'assurer de leur intégrité (ainsi que de leur provenance) relève de l'impératif catégorique, au sens kantien : à mesure que s'affirme l'omniprésence des ordinateurs, au bureau comme au foyer, et que s'accroît la compétence informatique des utilisateurs, les données circulent toujours plus librement...

A une époque où l'information constitue une arme véritable, et la plus terrible de toutes, la divulgation de données bien choisies ou de fausses informations, peut provoquer des catastrophes pour un particulier comme pour une entreprise. Le remède s'appelle *cryptographie*.

Parmi les nombreux domaines d'application de la cryptographie, nous nous sommes plus particulièrement intéressés à celui de *l'identification*, où un individu (le prouveur) doit convaincre un interlocuteur (le vérifieur) de son identité.

Comme c'est souvent le cas en cryptographie, de nombreux schémas d'identification, dont la sécurité dépend d'un problème issu de la théorie des nombres, ont été élaborés. Pour ces derniers, un processus d'identification nécessite l'exécution de calculs complexes (multiplications et exponentiations modulaires) coûteux en temps et puissance machine. La difficulté des problèmes utilisés (factorisation et logarithme discret) n'est pas prouvée, et de nombreuses attaques, de plus en plus performantes, menacent la solidité de ces problèmes.

Par ailleurs, dans le cadre d'une application de type carte à puce, le prouveur est représenté par un support mobile possédant un faible volume mémoire et une puissance de calcul limitée.

La théorie des codes, conjointement avec la théorie de la complexité, ont permis l'élaboration de schémas d'identification performants n'utilisant que des opérations de base sur le corps $\mathbb{F}_2$ et dont la sécurité dépend de la difficulté de résolution d'une instance quelconque d'un problème $\mathcal{NP}$-complet (le problème du décodage du syndrome ou problème SD).

C'est S. Harari [Har] qui, le premier, en 1988, a proposé un schéma d'identification utilisant les codes correcteurs d'erreurs. Depuis d'autres schémas ont été proposés [Gir, Ste_2, Ste_3].

Dans cette thèse, nous proposons d'autres schémas d'identification utilisant les codes correcteurs d'erreurs. Le principe de base est le suivant : le prouveur connaît une solution s d'une instance d'un problème $\mathcal{NP}$-complet. Pour établir son identité, il doit convaincre le vérifieur qu'il détient effectivement cette quantité.

La preuve est interactive, c'est-à-dire qu'il y a un échange d'informations entre le vérifieur et le prouveur afin d'établir cette preuve de connaissance. Comparativement, on est plus facilement convaincu de la preuve d'un théorème quand un professeur l'explique au tableau que lorsqu'on la découvre dans un livre.

D'après les travaux de Goldwasser, Micali et Rackoff [GMR], une telle preuve peut s'effectuer sans ne jamais dévoiler une seule information concernant le secret s. C'est-à-dire que lors d'une interaction avec le prouveur, le vérifieur n'apprend pas plus de choses qu'il ne connaissait avant le début de la transaction.

Un tel protocole s'appelle un système interactif de preuve à divulgation nulle (zéro-knowledge). L'un des schémas que nous proposons possède cette propriété. Il se peut qu'un protocole révèle une quelconque information concernant le secret s mais que celle-ci soit totalement inexploitable. On dit alors que le protocole est un système interactif de preuve à divulgation minimale.

Lors de la mise au point des schémas proposés, nous nous sommes particulièrement préoccupés de trois critères :

- le volume mémoire nécessaire au prouveur,
- la complexité des calculs effectués par le prouveur,
- le nombre de bits devant être échangés lors d'un processus d'identification (*débit de transaction*).

Tous les schémas seront évalués selon ces trois critères.

Nous décrivons aussi dans cette thèse, une cryptanalyse efficace du schéma de S. Harari. Trois attaques sont proposées. Les deux premières montrent comment un prouveur malhonnête peut satisfaire, en moyenne, une fois sur deux, le protocole. De nouveaux paramètres sont proposés afin d'augmenter la sécurité du schéma.

La dernière attaque permet, dans certains cas, à un vérifieur malhonnête de retrouver, en un nombre moyen de 2^{45} étapes, le secret s d'un prouveur honnête. De plus, l'efficacité de cette dernière attaque montre qu'il est nécessaire d'augmenter la valeur des paramètres du système (notamment la taille de la matrice) afin de renforcer la sécurité du schéma.

Une autre étude a été menée concernant les codes de Goppa. Généralement, le calcul de la dimension et de la distance minimale de ces codes est un problème difficile. Nous nous sommes plus particulièrement intéressés à une sous-classe des codes à poids pair, celle définie par le polynôme $g(z) = \mathrm{Tr}_{\mathbb{F}_{2^{2s}}:\mathbb{F}_{2^s}}(z)$. La dimension de ces codes n'atteint jamais la borne classique. Une étude plus générale a été réalisée, en considérant les codes définis par le polynôme $g(z) = a(z)\mathrm{Tr}_{\mathbb{F}_{p^{ms}}:\mathbb{F}_{p^s}}(b(z))$. De nouveaux résultats sont obtenus, concernant la dimension de ces codes, selon le cas considéré : cas général, cas quadratique ($m = 2$), cas binaire-quadratique ($m = 2, p = 2$). Il est démontré que, dans le cas binaire, ces codes sont à poids pair et que selon la valeur des polynômes $a(z)$ et $b(z)$, l'orthogonal de ces codes est aussi à poids pair.