François-Xavier Standaert

Sécurité des communications en présence de fuites physiques d'information.

Soit le jeu suivant. Deux boîtes, *A* et *B*, contiennent 100 et 42 euros. Un joueur doit trouver celle qui contient 100 euros. Pour ce faire, il peut demander à un arbitre de calculer (10 x *A* + 7 x *B*) et d'indiquer si le résultat est pair ou impair. À première vue, cette question semble inutile car les deux résultats possibles sont pairs (10 x 42 + 7 x 100 = 1120, 10 x 100 + 7 x 42 = 1294). Pourtant, si l'arbitre effectue ses calculs mentalement et que le joueur observe son temps de réaction, il y a bien de l'information cachée dans sa réponse. Un long délai correspond probablement au calcul de 7 x 42. Il permettrait de déduire que *A* = 100 et *B* = 42. Imaginons maintenant que l'arbitre soit une carte à puce effectuant une opération bancaire et le joueur un pirate essayant de casser un code. Le jeu qui vient d'être décrit se transforme alors en un problème cryptographique !

La cryptographie évoque traditionnellement l'art de rendre des messages inintelligibles à tout autre que leur destinataire. Elle se base notamment sur les notions d'information et de calcul. On dit qu'un système de chiffrement est "inconditionnellement sûr" si un adversaire ne dispose pas de l'information suffisante pour déchiffrer les messages. En cryptographie classique, l'information correspond aux mots échangés sur un canal de communication. Dans le jeu qui précède, il s'agit de la réponse de l'arbitre (pair ou impair). Le défi de la cryptographie physique est d'intégrer d'autres canaux d'information à l'analyse classique. Dans le jeu qui précède, il s'agit du temps de calcul de l'arbitre. On parle ensuite de sécurité calculatoire lorsque l'information est suffisante pour attaquer un système, mais que son exploitation se révèle difficile. La modélisation d'une attaque s'apparente alors à une partie de Mastermind où l'on trouve un compromis entre la quantité d'information disponible (c'est-à-dire le nombre de questions permises au joueur) et la puissance de calcul (c'est-à-dire la stratégie du joueur).

Les recherches de François-Xavier Standaert, Docteur en Sciences appliquées de l'Université Catholique de Louvain, ont pour but d'évaluer la sécurité physique de systèmes cryptographiques, à partir de bornes raisonnables sur l'information et le calcul. Ceci impose de travailler à la fois sur des questions théoriques (*Comment formaliser ces notions ?*) et pratiques (*Que considère-t-on comme raisonnable ?*). À l'instar du cerveau humain, plus ou moins habile en calcul mental, les circuits électroniques sont plus ou moins rapides pour effectuer des opérations de chiffrement. Il faut donc tenir compte de cette multiplicité de contextes. De plus, le temps de calcul n'est qu'un exemple de canal caché d'information : la consommation énergétique des circuits ou leur rayonnement électromagnétique constituent autant de défis supplémentaires. Au final, il faut aussi que les solutions envisagées soient utilisables : la cryptographie ne doit pas ralentir les communications. Il en résulte un équilibre subtil entre efficacité et sécurité qui nécessite une adaptation constante aux évolutions technologiques.

François-Xavier Standaert, 30 ans, Laboratoire de Microélectronique, Pr. J.-J. Quisquater, UCL.

Trois questions...

Quel est le moteur de vos recherches ?
Leurs applications au sens large et donc l'homme comme utilisateur. À cet égard, le caractère parfois intrusif des technologies de l'information implique une réflexion en termes d'éthique, de respect de la vie privée, ...

Quel personnage (historique ou fictif) incarne le mieux l'esprit de vos recherches ?
Dédale. Beaucoup de codes ressemblent à des labyrinthes : inextricables pour le profane mais parfois étonnamment simples pour qui sait les contourner.

Quels rêves d'aboutissement pour vos recherches ?
Qu'elles sortent des laboratoires, aient un impact sociétal et rencontrent les sciences humaines dans un dialogue interdisciplinaire sur la modernité.