CRYPTANALYSE DE FONCTIONS DE HACHAGE DES SOLVEURS-SAT

Type de contenu : Images animées

Titre(s) : CRYPTANALYSE DE FONCTIONS DE HACHAGE DES SOLVEURS-SAT ; PARRAUD, Patrice ; SLT NAMOR, Anthony|SLT SIONNEAU, Edouard ; VAN HEULE, Dirk ; LAFITTE, Frédéric

Autre(s) responsabilité(s) : PARRAUD, Patrice (Directeur de thèse)
SLT NAMOR, Anthony|SLT SIONNEAU, Edouard (Secrétaire)
VAN HEULE, Dirk ; LAFITTE, Frédéric (Directeur de thèse)

Editeur, producteur : Ecoles Militaires de Saint-Cyr Coëtquidan

Note de thèses et écrits académiques : Filière Scientifique - Option Informatique Promotion Chef d'Escadron Francoville Date de soutenance : 01/01/2011

Résumé ou extrait : > Etude : POSITION DU PROBLEME : Nous proposons une cryptanalyse des fonctions de hachage à l'aide d'un solveur SAT. Il s'agit là d'obtenir des résultats en cryptographie, en s'appuyant sur un outil d'intelligence artificielle. LES FONCTIONS DE HACHAGE : Les premières fonctions de hachage cryptographiques ont été inventées par Ronald Rivest au début des années 90, avec notamment MD4 en 1991. Ces fonctions permettent de générer, à partir d'une information de taille arbitraire, une empreinte unique, appelée haché, de taille fixe, et ce de manière quasi-irréversible. Leur usage, d'abord dans les structures de données (tables de hachage), s'est rapidement montré indispensable dans le domaine de la cryptographie. De nos jours, elles sont présentes dans la plupart des systèmes sécurisés, du stockage de mots de passe sous Windows aux certificats numériques (norme X.509), en passant par la sécurité des transactions bancaires en ligne (SHA-1 dans SSL). Une fonction de hachage est utilisée en cryptographie si elle possède deux propriétés fondamentales: une bonne résistance aux collisions (il est impossible de trouver deux mots clairs ayant le même haché en un temps raisonnable), et une bonne résistance au calcul de préimage (il est impossible de calculer un mot clair correspondant à un haché donné en un temps raisonnable). Les fonctions MD4 et MD5 créées par Ronald Rivest en 1990-91 ont longtemps été considérées sûres, vérifiant ces propriétés, et sont encore utilisées de nos jours (notamment MD5, pour stocker les mots de passe sous Windows). De même la fonction SHA-1, conçue par la National Security Agency (NSA) et classifiée en 1995 comme standard cryptographique pour les agences non militaires des Etats Unis, est encore utilisée notamment dans les transactions bancaires sécurisées (SSL). Lors de la conférence CRYPTO 2005, Wang et Al. annoncent avoir trouvé des collisions pour ces fonctions, rendant leur usage beaucoup moins sûr. Suite à ces découvertes, le National Institute of Standard and Technology (NIST) lance une compétition visant à remplacer ces fonctions de hachage peu sûres en promouvant un nouveau standard, la fonction SHA-3. Cette compétition, qui prendra fin en 2012, évalue différentes fonctions proposées par près de 64 candidats. L'une d'elle, SHAvite-3, a été l'objet de notre étude. Nous avons également mis à l'épreuve la résistance aux préimages des fonctions MD4, MD5 et SHA-1 et avons amélioré des résultats existants. La satisfiabilité : D'autre part, les problèmes dits de satisfiabilité, où l'on cherche à donner une valeur à un ensemble de variables booléenne afin que soit vérifiée une formule propositionnelle, prennent une ampleur considérable dans de nombreuses applications. Ce problème NP (ne pouvant être traité de manière déterministe en un temps

polynomial), attire l'attention de la communauté scientifique depuis que Stephen Cook a démontré, en 1971, que tous les problèmes NP pouvaient être modélisé par une instance de problème SAT. L'algorithme Davis-Putnam, proposant une méthode de résolution de ce type de problème, a connu de nombreuses optimisations ces derniers temps, notamment par l'ajout de techniques d'intelligence artificielle (apprentissage). Diverses compétitions internationales déterminent, chaque année, le meilleur algorithme de résolution de problème SAT, appelé solveur SAT . Leur intérêt est de fournir aux domaines industriels, de l'électronique de pointe (vérification de microprocesseurs), des mathématiques (preuve automatique de théorèmes), et de la cryptologie, des solveurs SAT de plus en plus efficaces. Un des problèmes rencontrés par les organisateurs de ces compétitions est de générer des instances difficiles de problèmes SAT pour évaluer la puissance des algorithmes candidats, les générateurs aléatoires créant des problèmes trop faciles en général, et les générateurs basés sur des problèmes réels présentant peu de possibilités de moduler la difficulté du problème créé. NOS TRAVAUX :

Sujet(s) : algèbre de Boole
cryptage
cryptographie
hachage : informatique
intelligence artificielle
sécurité informatique