CRYPTANALYSE DE LA FONCTION DE HACHAGE MD4 PAR LES ALGORITHMES DE SATISFAISABILITE

Type de contenu : Texte

Titre(s) : CRYPTANALYSE DE LA FONCTION DE HACHAGE MD4 PAR LES ALGORITHMES DE SATISFAISABILITE ; PARRAUD, Patrice ; SLT CHAMPSEIX, Loïc|SLT DERIVE, Maximilien ; VAN HEULE, Dirk

Autre(s) responsabilité(s) : PARRAUD, Patrice (Directeur de thèse)
SLT CHAMPSEIX, Loïc|SLT DERIVE, Maximilien (Secrétaire)
VAN HEULE, Dirk (Directeur de thèse)

Editeur, producteur : Ecoles Militaires de Saint-Cyr Coëtquidan

Description matérielle : 1 CD

Note sur le contenu : mémoire

Note de thèses et écrits académiques : Filière Scientifique - Option Informatique Promotion Capitaine de Cacqueray Date de soutenance : 01/01/2012

Résumé ou extrait : INTRODUCTION Le papier a été le principal support de l'information depuis l'invention de l'imprimerie jusqu'à ces dernières années. Mais depuis quelques dizaines d'années, celui-ci a été « dématérialisé ». Cette dématérialisation est d'autant plus répandue dans les économies modernes en raison de l'informatisation croissante des entreprises et des administrations. En effet, aujourd'hui l'information est sauvegardée sur support électronique. Le manque de sécurité autour des systèmes de communication et des supports qu'ils utilisent pourrait entraîner un libre accès à l'information. Or, les données qui transitent peuvent être extrêmement sensibles et faire l'objet de convoitises. Elles ont donc besoin d'être protégées lorsqu'elles sont stockées, consultées ou expédiées électroniquement. La sécurité de l'information numérique doit donc être assurée à tout moment et mérite une attention toute particulière. C'est la raison pour laquelle certains algorithmes cryptographiques ont été développés. Protéger des données en modifiant leurs aspects visuels fut l'une des premières méthodes employées. Le chiffrement par clés est apparu par la suite mais souleva le problème de la sécurité lors de l'échange de ces clés. Les fonctions de hachage se sont alors présentées comme un outil incontournable pour protéger l'information en interdisant un quelconque retour en arrière (principale différence avec la méthode de chiffrement). Depuis, la communauté cryptographique ne cesse de travailler sur la sécurité de ces fonctions. La recherche de solutions à ces algorithmes donne naissance à un grand nombre d'équations où les variables sont les bits secrets. Une nouvelle approche en cryptanalyse consiste à exprimer non pas des équations algébriques (entre bits publics et bits privés) mais des contraintes logiques dont les variables sont à valeur dans {0,1} correspondent aux bits. Il s'agit désormais d'un problème décisionnel pour lequel des algorithmes plus performants ont été développés. Trouver une valeur aux variables est ici équivalent à résoudre le système algébrique. Notre objectif est donc, notamment grâce à ces algorithmes, de réduire le temps nécessaire à la recherche d'un message clair haché par l'algorithme MD4, mais aussi de voir dans

quelle mesure certains critères pouvaient influencer la performance de ces algorithmes. LIMITES Les fonctions de hachage cryptographiques ont la particularité de vérifier deux propriétés qui rendent leur utilisation très pratique dans le domaine de la sécurité de l¹information : d'une part leur résistance aux collisions (deux entrées ne doivent pas aboutir à la même sortie), d'autre part leur résistance aux pré-images (étant donné une sortie, il doit être impossible de trouver un autre objet conduisant à la même sortie). La fonction de hachage cryptographique MD4, apparue en 1990, est l'une des pionnières. En effet, elle a donné naissance à bien d'autres comme, par exemple, MD5 (1991), RIPEMD (1992), SHA-0 (1993), SHA-1 (1995), SHA-2 (2002). C'est la raison pour laquelle de nombreux chercheurs se sont attaqués à cet algorithme. Cela étant, seule la résistance aux collisions a été cassée ; la résistance aux pré-images reste d'actualité et c'est d'ailleurs la propriété que nous avons étudiée. Dans ce cadre-ci, nous ne pouvions pour le moment nous attaquer qu'à une version restreinte de l'algorithme MD4. En d'autres termes, nous avons du procéder comme suit : d'une part, travailler sur la version complète de MD4, mais avec des messages très courts (entre 10 et 32 bits) ; d'autre part, travailler sur des messages de 512 bits, mais en ne considérant qu'une partie restreinte de l'algorithme, c'est-à-dire en n'effectuant pas toutes les étapes de celui-ci. CONCLUSION Ces deux mois et demi de recherches sur les possibilités d'avancées dans le domaine de la cryptanalyse des fonctions de hachage cryptographiques ont constitué un travail des plus intéressants nécessitant une perpétuelle remise en question de la démarche emp

Sujet(s) : codage de données
cryptage
fichier informatique
programme informatique
protection de l'information