Projet SFPN

Titre. Implantation de l'attaque générique contre le chiffrement double.

Encadrants. Charles Bouillaguet (`charles.bouillaguet@univ-lille.fr`)

Laboratoire d'accueil. Laboratoire d'Informatique de Paris 6 (LIP6), Sorbonne Université (campus de Jussieu).

Mots clés. Cryptanalyse, attaque générique, double-DES, parallel collision search, compromis temps-mémoire

Contexte. Le *chiffrement double* consiste à utiliser le même dispositif de chiffrement par blocs deux fois de suite, avec deux clefs de chiffrement différentes. Cette technique n'est pas utilisée en pratique car elle n'offre pas le niveau de sécurité désiré.

Plus précisément, avec un système de chiffrement par bloc $E_k(x)$ qui chiffre un bloc x avec une clef k. on peut former $E^2_{k,k'} = E_k \circ E_{k'}$ — ça veut dire qu'on chiffre d'abord avec la clef k puis avec la clef k'. Si les clefs de E font n bits de long, alors les clefs de E^2 font $2n$ bits. On aimerait donc que les meilleures attaques contre E^2 nécessitent environ 2^{2n} opérations.

Le chiffrement *triple* fonctionne de manière analogue avec 3 clefs. Le triple-DES a été standardisé par le gouvernement américain pour son propre usage. En effet, le DES avait des clefs de 56 bits, ce qui est devenu trop court, et le chiffrement triple augmente ceci à 168 bits.

Le triple-DES est sûr et largement utilisé. Par contre une attaque générique assez simple « casse » le chiffrement double E^2 en 2^n opérations, en utilisant $n2^n$ bits de mémoire, ce qui est sensiblement plus rapide qu'attendu. On pourrait envisager de la réaliser en pratique sur le double-DES... à ceci prêt qu'il faudrait 512Po de mémoire, ce qui n'est pas réaliste.

À la place, on peut utiliser un compromis temps-mémoire, l'algorithme de recherche de collisions parallèle de van Oorschot et Wiener. En utilisant M bits de mémoire, ceci nécessite $2^{1.5n}/\sqrt{M}$ opérations, et c'est facilement parallelisable.

Description détaillée du travail attendu. Il s'agit de programmer, en C, l'algorithme de recherche de collision parallèle et de s'en servir pour réaliser l'attaque contre le chiffrement double. Plutôt que le DES, on utilisera par exemple le système de chiffrement par bloc RC5, qui permet de choisir la taille de la clef, et donc de faire tourner l'attaque « en pratique » avec de petites clefs. Une parallélisation sur plusieurs machines est attendue. L'implantation doit, dans la mesure du possible, être « haute-performance ».

Le résultat du projet, outre le code lui-même, consiste à faire apparaître tous les problèmes théoriques ou pratiques qui pourraient survenir (probabilité de succès, gestion du volume de données, communications, facteurs limitant les performances, etc.), et de parvenir à une estimation du temps de calcul nécessaire à la réalisation de l'attaque sur le double-DES.

Référence. `https://people.scs.carleton.ca/~paulv/papers/JoC97.pdf`