

Univesity of Bordeaux
College of Science & Technology
351 Cours de la Liberation
33400 Talence

- TER Oral -

Sponge Function's Implementation

Amelie GUEMON & Ida TUCKER

Master 1 CSI — Cryptology & Computer Security

April 23, 2016

En faisant subir une suite de traitements reproductibles à une entrée, une fonction de hachage génère une empreinte servant à identifier la donnée initiale. Cette identification par le biais de fonctions de hachage est un outil indispensable pour de nombreux protocoles cryptographique, du stockage de mots de passes à l'authentification en passant par l'intégrité de messages de grande taille, ils présentent de nombreux intérêts.

Nous nous sommes intéressées à l'évolution des fonctions de hachage, dû à la publication en Août dernier d'une nouvelle famille de fonctions de hachage par le NIST.

Le NIST est l'organisme de normalisation des standards et de la technologie aux USA.

La particularité de cette nouvelle famille est qu'elle repose sur des principes fondamentalement différents de toutes les familles de fonctions ayant été standardisées au part avant. Nous nous sommes donc demandées ce qui a poussé le NIST à chercher une telle différence radicale.

Chapter 1

INTRODUCTION

1.1 Qu'est-ce qu'une fonction de hachage

Une fonction de hachage prend en entrée un message de taille quelconque, applique une série de transformations et réduit ces données. On obtient à la sortie une chaîne de caractères hexadécimaux, le condensé, ou haché, qui résume en quelque sorte le fichier.

Cette sortie a une taille fixe qui varie selon les algorithmes (128 bits pour MD5 et 160 bits pour SHA-1).

Remarquons qu'elles ne peuvent être injectives, par conséquent il y aura forcément plusieurs messages menant aux mêmes hachés.

1.2 Fonctions de hachage cryptographiques

Pour qu'une fonction de hachage soit utilisée à des fins cryptographiques, (il s'agit alors d'une fonction de hachage cryptographique) elle doit satisfaire certaines contraintes.

- Il doit être difficile de retrouver ou générer un texte à partir de l'empreinte:
Résistance à la première pré-image. Il est alors difficile pour qu'un attaquant puisse trouver un message qui mène à un haché donné (signatures falsifiées si Oscar a une liste de signatures que Bob acceptera et qu'il trouve un message qui est valide pour cette signature, la fonction de hachage ne garantit plus l'intégrité).
- La moindre modification dans le fichier original doit engendrer un condensé totalement différent. En outre, le hachage doit rendre impossible la création d'un fichier qui donne la même empreinte qu'un autre préalablement fixé: **Résistance à la seconde pré-image.** La résistance à la seconde pré-image garantit l'intégrité d'un fichier: si elle n'est pas respectée, on pourrait facilement générer un fichier corrompu mais valide aux yeux de l'utilisateur.
- De même il doit être difficile pour un attaquant de trouver deux messages ayant le même haché, car il pourrait alors substituer un message par un autre, ou nier avoir envoyé un message (intégrité et non répudiation): **Résistance aux collisions.**

Chapter 2

MERKLE DAMGARD

2.1 Idée

On peut utiliser des fonctions de compression résistantes aux collisions pour construire des fonctions de hachage, elles-aussi résistantes aux collisions. C'est sur ce principe que repose la construction de Merkle-Damgard. L'approche traditionnelle pour construire des fonctions de Hachage a été de se reposer sur une construction appelée la construction de Merkle-Damgard.

2.2 Construction

Chapter 3

ATTAQUES

3.1 Attaque par force brute: l'attaque des anniversaires

Si l'on suppose que l'ensemble de messages \mathcal{E} est choisi de façon aléatoire et uniforme parmi tous les messages possibles, on peut montrer que le nombre de messages à tester afin d'avoir une probabilité donnée de trouver des collisions ne dépend que de la taille des condensés.

Ainsi, afin d'avoir une probabilité supérieure à 50% de trouver des collisions, il suffit de tester aléatoirement peu plus de \sqrt{N} messages.

Dans le cas de SHA1 et MD5, puisque les condensés sont de 128 et 160 bits respectivement, l'attaque par force brute se fait de façon naïve en 2^{56} et 2^{80} essais.

Pour donner une idée en temps, 8 cartes graphiques NVidia Titan X peuvent calculer 115840 millions de condensés MD5 par seconde. Cela prendrait donc ≈ 5 ans afin de trouver une collision avec un tel dispositif. Ainsi avec une armée de machines dédiées à cette tâche, il serait relativement facile de trouver des collisions pour MD5 en un temps raisonnable.

L'attaque par force brute fournit donc une taille minimale nécessaire pour la taille des condensés afin de garantir une certaine sécurité de base.

Il est recommandé de prendre $n \geq 128$, voir $n \geq 160$. Ces recommandations sont cependant relatives aux performances actuelles des ordinateurs; elles ne sont que provisoires et ne correspondent en aucun cas à un seuil théorique de sécurité.

3.2 Quand une fonction de hachage est-elle considérée cassée?

Une fonction de hachage est dite **cassée** lorsqu'il existe une attaque connue permettant de trouver des collisions ayant une complexité moindre que l'attaque par force brute.

3.3 MD5 et SHA1: cassés en 2004

Il existe des algorithmes aujourd'hui capables de trouver des collisions pour MD5 en quelques secondes, et l'attaque de SHA1 découverte par l'équipe de Wang en 2004 a une probabilité supérieure à 50% de trouver des collisions en 2^{69} opérations, c'est à dire plus rapide qu'une attaque par force brute (2^{80}) d'un facteur 2000. Si 2^{69} reste à l'heure actuelle hors de portée du commun des ordinateurs, cette attaque reste un résultat important dans le domaine de la cryptanalyse, et est suffisant pour qu'il soit déconseillé d'utiliser SHA1 aujourd'hui. Le nombre de fonctions de hachage cryptographique sûres a réduit considérablement dans la dernière décennie, d'autant que l'on suspecte SHA-2 de n'être plus aussi sécurisée qu'on a pu le croire. En effet, bien que SHA-2 ne soit pas cassée, et que son implémentation reste recommandée par le NIST il existe des attaques contre des versions réduites de SHA-2 (la fonction de compression est itérée sur 46 tours au lieu de 64).

Quoi qu'il en soit, ces progrès importants dans la cryptanalyse des fonctions de hachage ont poussé le NIST à développer de nouveaux algorithmes de hachage standards. La recherche de cette nouvelle norme s'est faite sous la forme d'un concours, comme pour AES, la communauté cryptographique était invitée à proposer des algorithmes et parmi eux un ou plusieurs seront sélectionnés à l'issue du processus.

Le NIST souhaitait un algorithme reposant sur une construction complètement différente que Merkle-Damgård, ainsi, même si une attaque est découverte contre ce type de construction, remettant en question la sécurité de SHA2, l'algorithme pour SHA3 ne serait pas affecté.

L'algorithme qui fut sélectionné pour SHA3, en Août dernier, à l'issue de ce concours repose sur une construction dite en éponge.

Chapter 4

FONCTIONS EN ÉPONGE

4.1 Sponge construction

4.2 Keccak

4.3 SHA-3