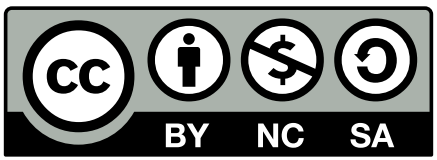
université de BORDEAUX

Implémentation de fonctions en éponge

Amélie Guémon
Ida Tucker
<amelie.guemon@etu.u-bordeaux.fr>

Master CSI, Université de Bordeaux, France

22 avril 2016



Plan

Définition : fonction de hashage

Une fonction de hashage est une application qui associe à un ensemble de départ infini $\{0,1\}^*$ un ensemble d'arrivée fini $\{0,1\}^n$ constitué de chaînes de bits de taille n.

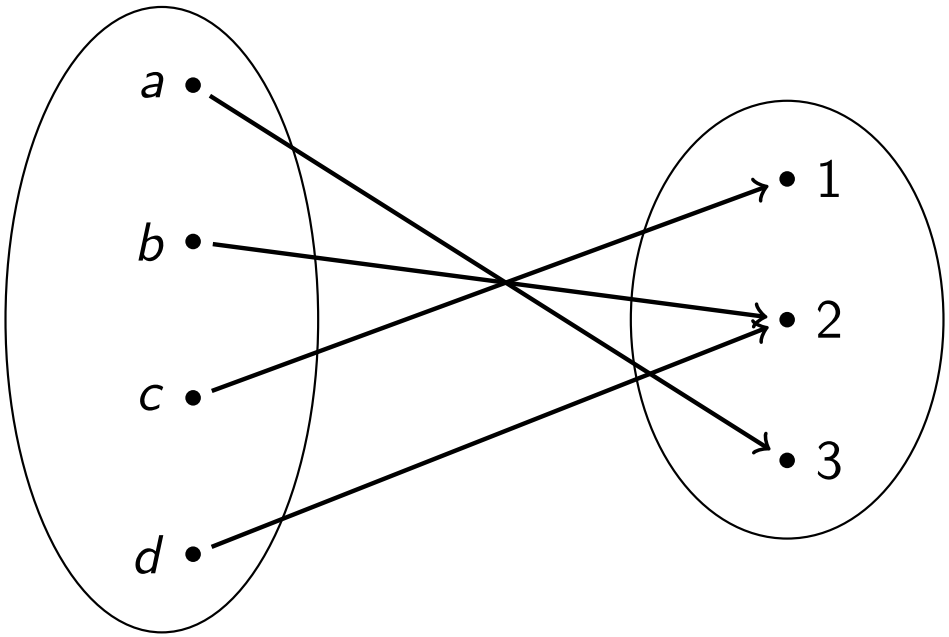


Figure: Collision dans une fonction de Hachage

Propriétés requises

- **Résistance à la Pré-image** : Pour un hash y donné, il est dur de trouver une pré-image $x \in f^{-1}(H)$ tel que $y = H(x)$.
- **Résistance à la Seconde Pré-image** : Pour un clair x, il est dur de trouver un autre clair x', $x' \neq x$ tel que $H(x) = H(x')$.
- **Résistance aux Collisions** : Il est dur de trouver 2 messages clairs x et x' avec $x \neq x'$ tel que $H(x) = H(x')$.

Padding

- **Padding Simple** : Représenté par $10*$, il faut rajouter un 1, puis un nombre fini de 0, de telle sorte que la longueur du resultat soit un multiple de le taille des blocks que l'on doit utiliser.

Figure: Simple padding.

Padding

- **Merkle-Damgård Padding** : Représenté par $10*1|M|$, il faut rajouter un 1, puis un nombre fini de 0, de telle sorte que la longueur du resultat soit congru à 448 mod 512. Ensuite, on y ajoute la longueur du message, sur 64 bits.

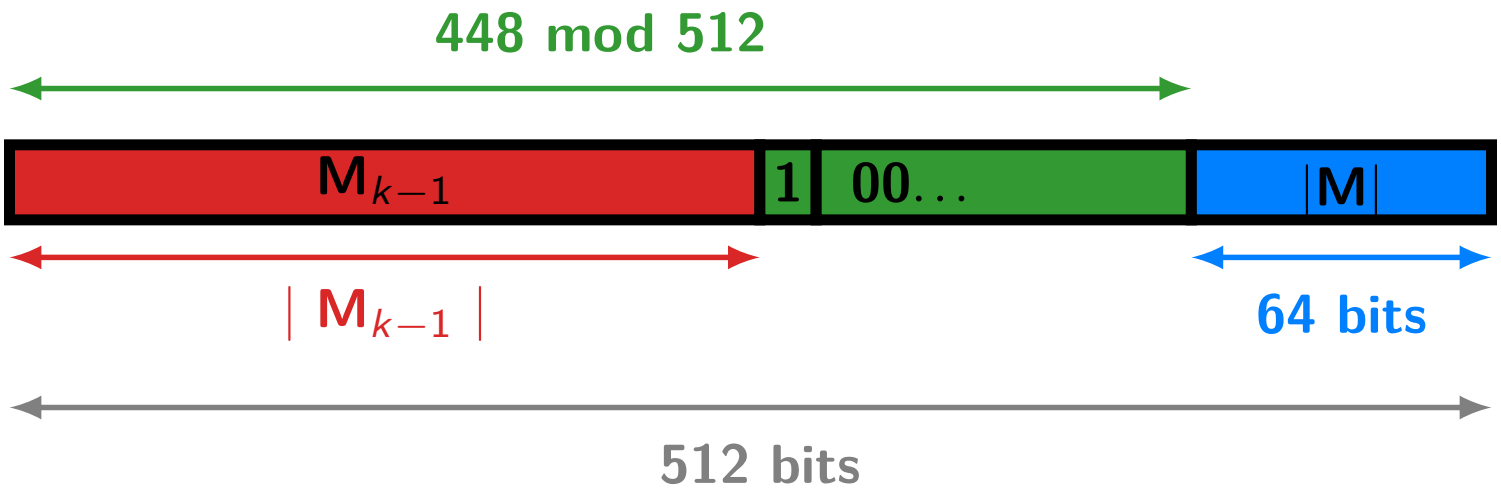


Figure: Merkle-Damgård padding.

Plan

Construction de Merkle-Damgård

La construction de Merkle-Damgård permet de définir des fonctions de hachage en itérant des fonctions de compression.

- Une fonction de compression part d'un ensemble fini vers un ensemble fini.
- Une fonction de hachage part d'un ensemble infini vers un ensemble fini.

Construction de Merkle-Damgård

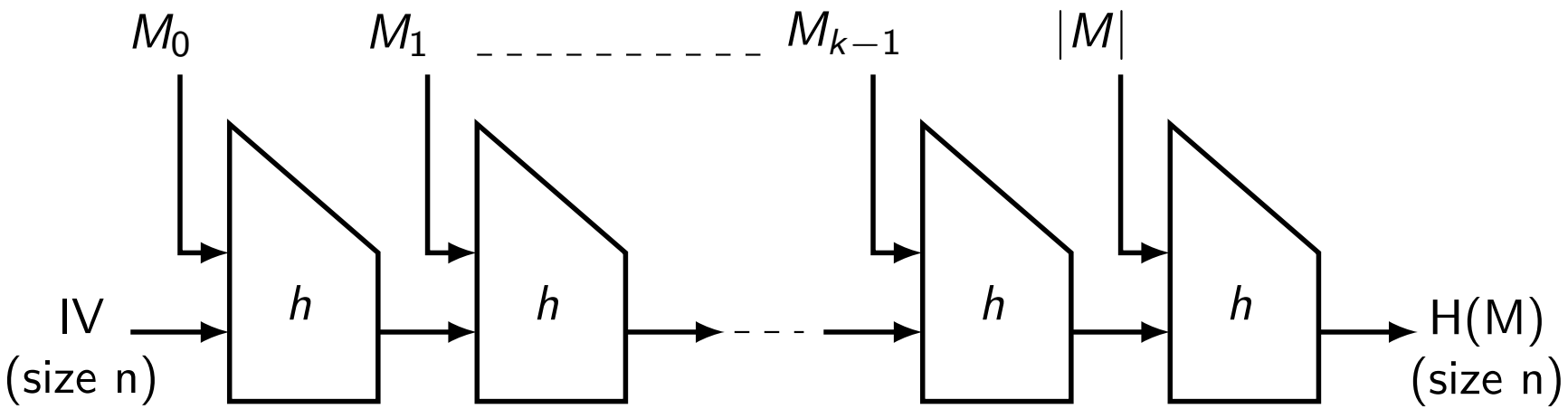


Figure: Merkle-Damgård construction.

- Théorème : Si la fonction de compression h utilisée par la fonction de hachage H l'est aussi.

Applications

- MD5
- SHA1

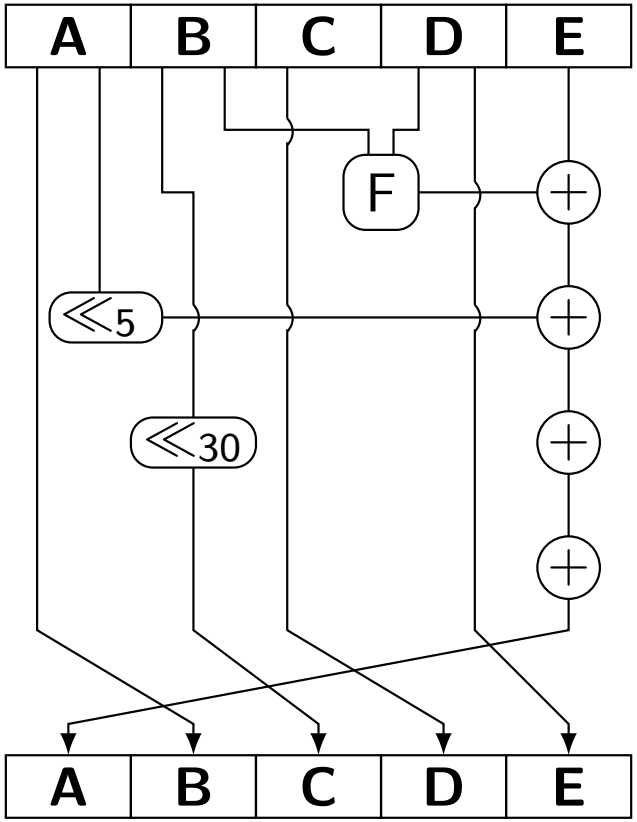


Figure: The i^{th} round in SHA-1 ($0 \leq i \leq 79$).

Plan

On continue ! ! !

Ce slide est quasiment vide !

Plan

Livres et références I


Ida Tucker Amelie Guemon.
Hashing algorithms.
https://github.com/pouwapouwa/HachingAlgo, 2016.


NIST Computer Security Division.
SHA-3 Standard : Permutation-Based Hash and Extendable-Output Functions.
Number 202. May 2014.


Jean-Guillaume Dumas, Jean-Louis Roch, Eric Tannier, and Sébastien Varrette.
Théorie des codes : Compression, cryptage, correction.
DUNOD, 2007.


Hashcat performance tests.
`http://hashcat.net/oclhashcat/`.
Accessed : 2016-04-13.

Livres et références II


Tadayoshi Kohno John Kelsey.
Herding hash functions and the nostradamus attack.
Technical report, National Institute of Standards and Technology,CSE Department, 2006.


Antoine Joux.
Multicollisions in iterated hash functions. application to cascaded constructions.
Technical report, DCSSI Crypto Lab, 2004.


Marc Stevens.
Attacks on Hash Functions and Applications.
PhD thesis, Amsterdam, 2012.


Douglas Stinson.
CRYPTOGRAPHIE Théorie et pratique.
vuibert, 5 edition, 1996.

Livres et références III

Christopher Swenson.
Modern Cryptanalysis : Techniques for advanced code breaking.
WILEY, 2008.

Xuejia Lai Xiaoyun Wang, Dengguo Feng and Hongbo Yu.
Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD.
Cryptology ePrint Archive : Report 2004/199, 2004.

Questions ?