Funzioni hash crittografiche

Una buona funzione hash $f : X \to Y$ (con $|X| \gg |Y|$) ha le seguenti caratteristiche:

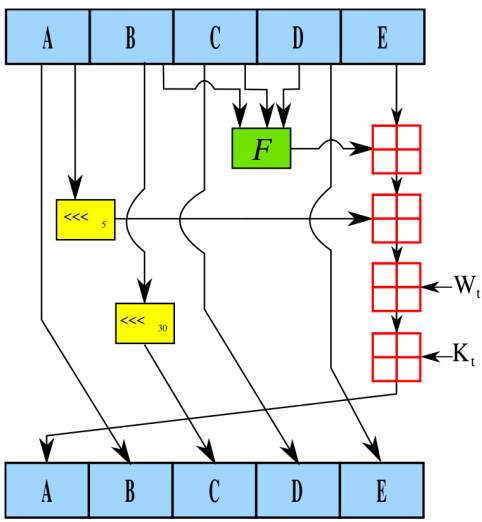
- le controimmagini degli elementi di Y hanno circa la stessa cardinalità, ovvero due elementi presi a caso da X hanno probabilità $\simeq \frac{1}{|Y|}$ di avere la stessa immagine;
- elementi di X simili (e.g. interi vicini) tra loro hanno immagini diverse.

Per applicazioni crittografiche è richiesto anche che:

- $f(x)$ è facile da calcolare;
- *one-way*: dato y, trovare un $x \in f^{-1}(y)$ è difficile;
- *claw-free*: difficile trovare una coppia con lo stesso hash ($f(x_1) = f(x_2)$).

SHA1

Calcola un hash da 160 bit di sequenze lunghe fino a $2^{64} - 1$ bit. Opera su blocchi di 160 bit, divisi in 5 registri da 32 bit.



Un'iterazione all'interno della funzione di compressione di SHA-1. A, B, C, D ed E sono parole di stato a 32 bit; F è una funzione non lineare che varia; $\lll_n$ denota una rotazione del bit di sinistra di n posti; n varia per ogni operazione. $\boxplus$ denota l'addizione modulo 2^{32}. K_t è una costante.

W_t blocco di 32 bit ottenuto tagliando e rimescolando i blocchi di messaggio

A, B, C, D, E sono inizializzati con valori fissi, e il messaggio viene caricato 32 bit alla volta attraverso W_t. È stato applicato il principio di diffusione per garantire che piccole modifiche all'input provochino grandi cambiamenti nell'hash.