Generatori crittograficamente sicuri basati su funzioni one-way

Funzioni one-way: computazionalmente facili da calcolare ma difficili da invertire. Permettono di definire generatori crittograficamente sicuri.

Data la funzione one-way f e il seme x_0, possiamo generare la sequenza

$$x_i = f^i(x_0) = f(x_{i-1})$$

e consumarla in ordine inverso, visto che l'inversione di f è difficile. Se restituissimo in ordine si potrebbe calcolare il valore successivo applicando f al precedente.

Generatore binario

$b(x)$ è un predicato hard-core della funzione one-way $f(x)$ se:

- $b(x)$ è facile da calcolare conoscendo x;
- è difficile da calcolare o prevedere con probabilità $> 1/2$ se si conosce $f(x)$ (che è il valore a cui corrisponde l'ultimo bit restituito)

b permette di trasformare in modo sicuro la sequenza di numeri in una sequenza di bit.

Esempio

- $f(x) = x^2 \bmod m$ con m composto (radice modulo un composto è difficile);
- $b(x) = x \bmod 2$.

Se $x = 10$, $m = 77$:

$$f(10) = 23 \qquad b(10) = 0$$

facili da calcolare, ma a partire da 23 trovare la parità della radice modulo 77 è difficile.