

Theoretical Constructions of Pseudorandom Objects

Yu Zhang

HIT/CST/NIS

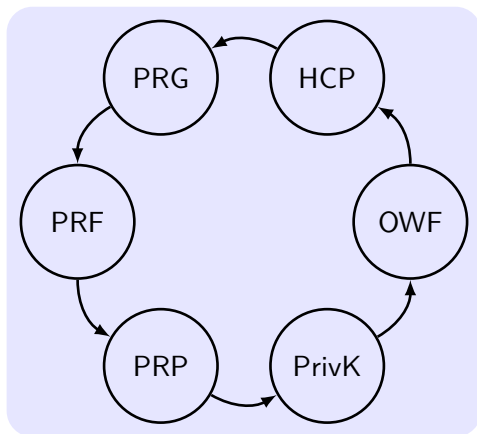
Cryptography, Autumn, 2014

1 One-Way Functions

2 From OWF to PRP (FYI)

1 One-Way Functions

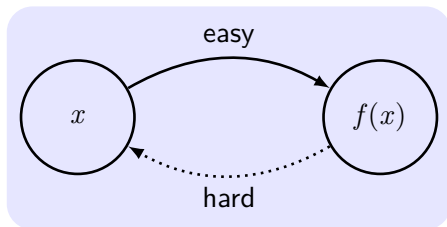
2 From OWF to PRP (FYI)



One of contributions of modern cryptography

The existence of one-way functions is equivalent to the existence of all (non-trivial) private-key cryptography.

One-Way Functions (OWF)



The inverting experiment $\text{Invert}_{\mathcal{A},f}(n)$:

- 1 Choose input $x \leftarrow \{0, 1\}^n$. Compute $y := f(x)$.
- 2 \mathcal{A} is given 1^n and y as input, and outputs x' .
- 3 $\text{Invert}_{\mathcal{A},f}(n) = 1$ if $f(x') = y$, otherwise 0.

Definitions of OWF/OWP [Yao]

For polynomial-time algorithm M_f and \mathcal{A} .

Definition 1

A function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ is **one-way** if:

- 1 (Easy to compute): $\exists M_f: \forall x, M_f(x) = f(x)$.
- 2 (Hard to invert): $\forall \mathcal{A}, \exists \text{negl}$ such that

$$\Pr[\text{Invert}_{\mathcal{A},f}(n) = 1] \leq \text{negl}(n).$$

or

$$\Pr_{x \leftarrow \{0,1\}^n} [\mathcal{A}(f(x)) \in f^{-1}(f(x))] \leq \text{negl}(n).$$

Definition 2

Let $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ be length-preserving, and f_n be the restriction of f to the domain $\{0, 1\}^n$. A OWP f is a **one-way permutation** if $\forall n, f_n$ is a bijection.

Candidate One-Way Function

- **Multiplication and factoring:**

$f_{\text{mult}}(x, y) = (xy, \|x\|, \|y\|)$, x and y are equal-length primes.

- **Modular squaring and square roots:**

$f_{\text{square}}(x) = x^2 \bmod N$.

- **Discrete exponential and logarithm:**

$f_{g,p}(x) = g^x \bmod p$.

- **Subset sum problem:**

$f(x_1, \dots, x_n, J) = (x_1, \dots, x_n, \sum_{j \in J} x_j)$.

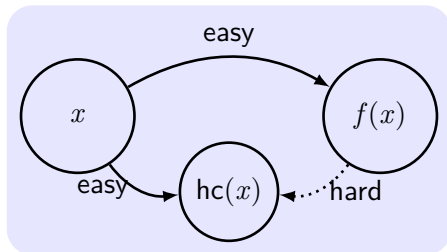
- **Cryptographically secure hash functions:**

Practical solutions for one-way computation.

f is OWF. Is f' OWF?

- $f'(x) = f(x) \| x$
- $f'(x) = f(x) \oplus 1^{|x|}$
- $f'(x \| x') = f(x) \| x'$
- $f'(x) = f(x) \oplus f(x)$
- $f'(x) = \begin{cases} f(x) & \text{if } x[0, 1, 2, 3] \neq 1010 \\ x & \text{otherwise} \end{cases}$

Hard-Core Predicates (HCP) [Blum-Micali]



Definition 3

A function $hc : \{0, 1\}^* \rightarrow \{0, 1\}$ is a **hard-core predicate of a function** f if (1) hc can be computed in polynomial time, and (2) \forall PPT \mathcal{A} , \exists negl such that

$$\Pr_{x \leftarrow \{0,1\}^n} [\mathcal{A}(f(x)) = hc(x)] \leq \frac{1}{2} + \text{negl}(n).$$

A HCP for Any OWF

Theorem 4

f is OWF. Then \exists an OWF g along with an HCP gl for g . If f is a permutation then so is g .

Q: is $gl(x) = \bigoplus_{i=1}^n x_i$ the HCP of any OWF?

$g(x, r) \stackrel{\text{def}}{=} (f(x), r)$, for $|x| = |r|$, and define

$$gl(x, r) \stackrel{\text{def}}{=} \bigoplus_{i=1}^n x_i \cdot r_i.$$

r is a random subset of $\{1, \dots, n\}$. [Goldreich and Levin]

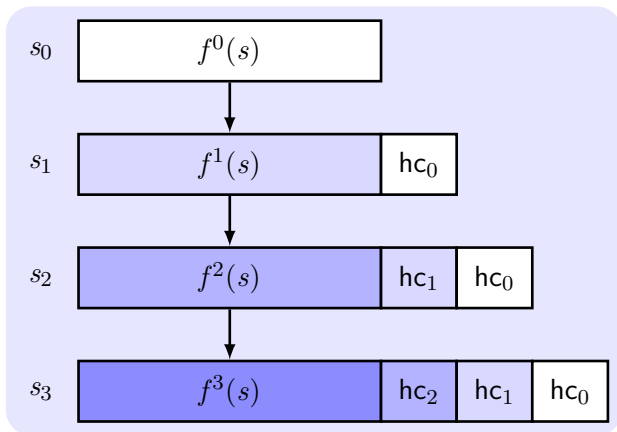
1 One-Way Functions

2 From OWF to PRP (FYI)

PRG from OWP: Blum-Micali Generator

Theorem 5

f is an OWP and hc is an HCP of f . Then $G(s) \stackrel{\text{def}}{=} (f(s), hc(s))$ constitutes a PRG with expansion factor $\ell(n) = n + 1$, then \forall polynomial $p(n) > n$, \exists a PRG with expansion factor $\ell(n) = p(n)$.

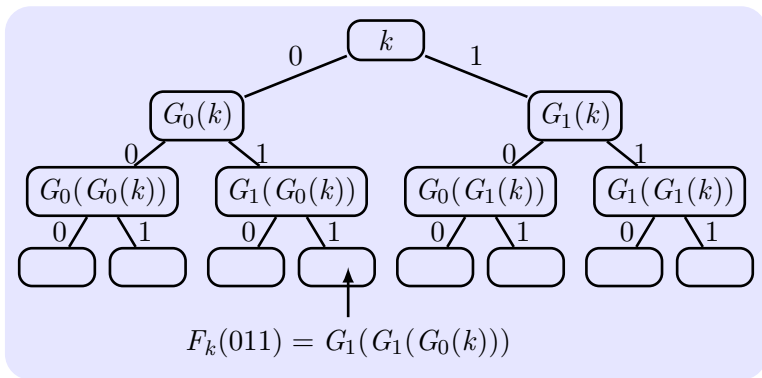


PRF from PRG [Goldreich, Goldwasser, Micali]

Theorem 6

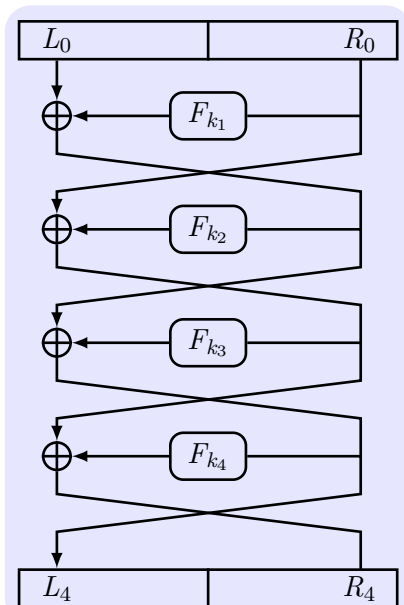
If \exists a PRG with expansion factor $\ell(n) = 2n$, then \exists a PRF.

$$G(k) = G_0(k) \parallel G_1(k)$$



$$F_k(x_1 x_2 \cdots x_n) = G_{x_n}(\cdots (G_{x_2}(G_{x_1}(k))) \cdots), \quad G(s) = (G_0(s), G_1(s)).$$

PRP from PRF [Lucy, Rackoff]



$F^{(r)}$ is an r -round Feistel network with the mangler function F .

Theorem 7

If F is a length-preserving PRF, then $F^{(3)}$ is a PRP that maps $2n$ -bit strings to $2n$ -bit strings (and uses a key of length $3n$).

Theorem 8

If F is a length-preserving PRF, then $F^{(4)}$ is a strong PRP that maps $2n$ -bit strings to $2n$ -bit strings (and uses a key of length $4n$).

Necessary Assumptions

Theorem 9

Assume that \exists OWP. Then \exists PRG, PRF, strong PRP, CCA-secure private-key encryption schemes, and secure MAC.

Proposition 10

If \exists a private-key encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper, then \exists an OWF.

Proof.

$$f(k, m, r) \stackrel{\text{def}}{=} (\text{Enc}_k(m, r), m).$$



- OWF implies secure private-key encryption scheme and MAC.
- Secure private-key encryption scheme/MAC implies OWF.