

# Theoretical Constructions of Pseudorandom Objects

Yu Zhang

HIT/CST/NIS

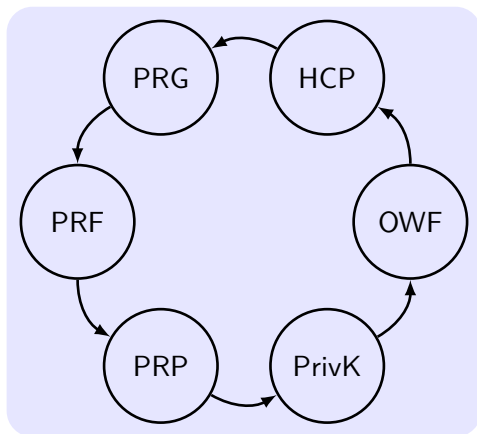
Cryptography, Autumn, 2014

**1** One-Way Functions

**2** From OWF to PRP (FYI)

## **1** One-Way Functions

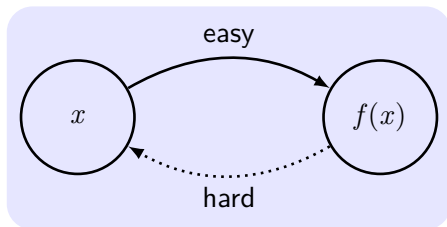
## **2** From OWF to PRP (FYI)



## 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

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

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

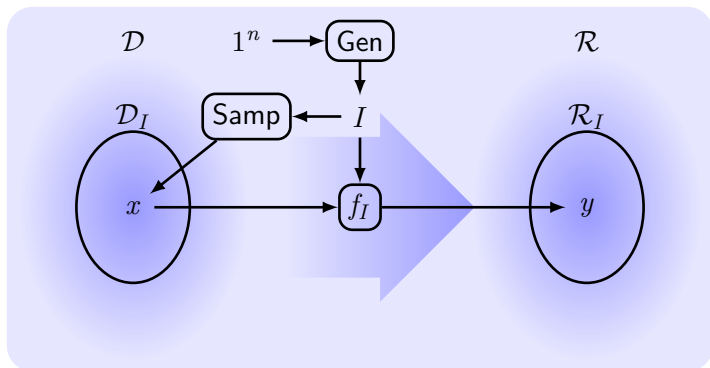
or

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

## 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.

# Families of Functions



## Definition 3

$\Pi = (\text{Gen}, \text{Samp}, f)$  is a **family of functions** if:

- 1 **Parameter-generation** algorithm:  $I \leftarrow \text{Gen}(1^n)$ .
- 2 **sampling** algorithm:  $x \leftarrow \text{Samp}(I)$ .
- 3 The deterministic **evaluation** algorithm:  $y := f_I(x)$ .

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

- 1  $\text{Gen}(1^n)$  obtains  $I$ ,  $\text{Samp}(I)$  obtains a random  $x \leftarrow \mathcal{D}_I$ .  
 $y := f_I(x)$ .
- 2  $\mathcal{A}$  is given  $I$  and  $y$  as input, and outputs  $x'$ .
- 3  $\text{Invert}_{\mathcal{A}, \Pi}(n) = 1$  if  $f_I(x') = y$ , and 0 otherwise.

## Definition 4

a function/permutation family  $\Pi$  is **one-way** if  $\forall$  PPT  $\mathcal{A}$ ,  $\exists \text{negl}$  such that

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



# 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:**

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

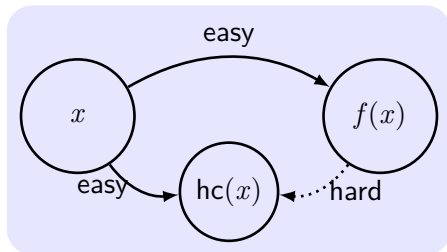
- **Subset sum problem:**

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

- **Cryptographically secure hash functions:**

Practical solutions for one-way computation.

# Hard-Core Predicates (HCP)



## Definition 5

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  $\mathcal{A}$ ,  $\exists$   $\text{negl}$  such that

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

## 1 One-Way Functions

## 2 From OWF to PRP (FYI)

## Theorem 6

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

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

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

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

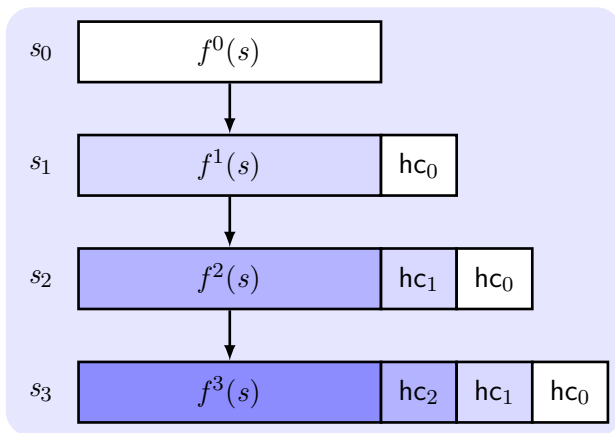
## Theorem 7

*$f$  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  $\ell(n) = n + 1$ .*

## Theorem 8

*If  $\exists$  a PRG with expansion factor  $\hat{\ell}(n) = n + 1$ , then  $\forall$  polynomial  $p(n) > n$ ,  $\exists$  a PRG with expansion factor  $\ell(n) = p(n)$ .*

# Blum-Micali Generator



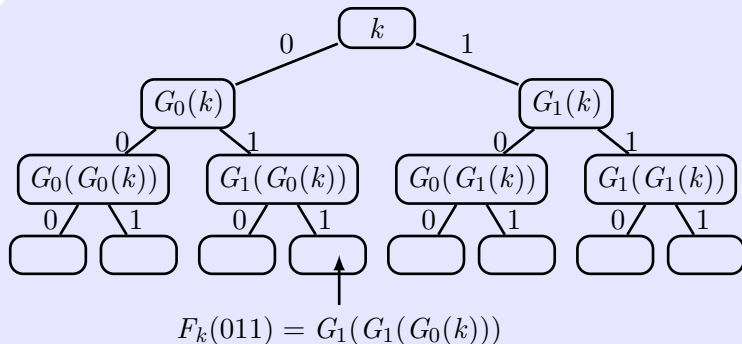
$$G(s) = (f^{p'(n)}(s), hc_{[p'(n)-1]}(f^{[p'(n)-1]}(s)), \dots, hc_0(s)),$$

is a PRG with expansion factor  $p(n) = n + p'(n)$ .

# Constructing PRF from PRG

## Theorem 9

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



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

# Constructing PRP from PRF

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

## Theorem 10

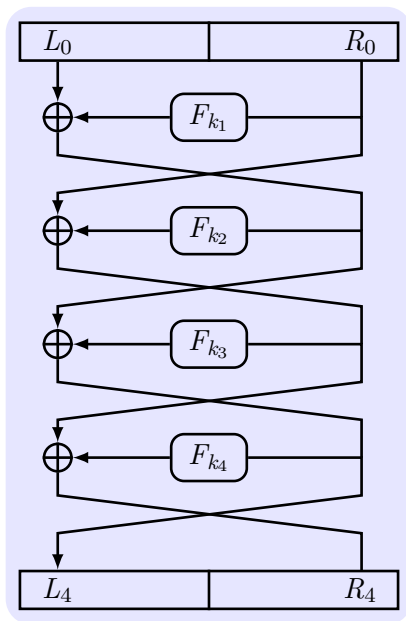
*If  $F$  is a length-preserving PRF, then  $F^{(3)}$  is a PRP that maps  $2n$ -bit strings to  $2n$ -bit strings (and uses a key of length  $3n$ ).*

## Theorem 11

*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  $4n$ ).*



# A Four-Round Feistel Network



# Necessary Assumptions

## Theorem 12

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

## Proposition 13

*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.