Katz, Lindell
Introduction to Modern Cryptrography
Slides Chapter 7

Markus Bläser, Saarland University

One-way functions

$f : \{0,1\}^* \to \{0,1\}^*$ shall be

- easy to compute, but
- hard to invert.

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

1. Choose $x \in \{0,1\}^n$ uniformly at random and set $y := f(x)$.
2. $\mathcal{A}$ gets 1^n and y and outputs x'.
3. The result of the experiment is 1 if $f(x') = y$ and 0 otherwise.

One-way functions (2)

Definition (7.1)

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

1. There exists a deterministic polynomial-time algorithm computing f.
2. For every ppt $\mathcal{A}$,

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

One-way permutation:

- length-preserving
- bijective

Function families

Most candidate one-way functions work differently, they are parameterized by some parameters.

Definition (7.2)

A tuple $\Pi = (\mathrm{Gen}, \mathrm{Samp}, \mathrm{f})$ of ppt algorithms is a *function family* if:

1. Gen on input 1^n generates some parameters I. I defines the domain $\mathrm{D_I}$ and $\mathrm{R_I}$ of a function $\mathrm{f_I}$.
2. Samp on input I outputs an element of $\mathrm{D_I}$ uniformly at random.
3. f on input I and $x \in \mathrm{D_I}$ outputs an element $\mathrm{f_I}(x) \in \mathrm{R_I}$. f is deterministic.

permutation family:

- $\mathrm{D_I} = \mathrm{R_I}$
- $\mathrm{f_I}$ bijective

One-way functions (3)

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

1. Generate parameters I using $\mathsf{Gen}(1^n)$.
   Run $\mathsf{Samp}(I)$ to generate a uniform $x \in D_I$.
   Finally, set $y := f_I(x)$.
2. $\mathcal{A}$ gets 1^n and y and outputs x'.
3. The result of the experiment is 1 if $f(x') = y$ and 0 otherwise.

Definition

A function family Π is *one-way* if for all ppt $\mathcal{A}$,

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

Hard-core predicates

Definition (7.4)

$\mathsf{hc} : \{0,1\}^* \to \{0,1\}$ is a *hard-core predicate* of a function f, if

1. hc can be computed deterministically in polynomial time and
2. for any ppt $\mathcal{A}$,

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

Goldreich-Levin Theorem

Theorem (7.5, Goldreich–Levin)

Assume that one-way functions exist. Then there is a one-way function g *with a hardcore predicate* hc *for* g.

- Let f be a one-way function. We set

$$g(x, r) = (f(x), r) \qquad \text{for } |r| = |x|.$$

- and

$$\mathrm{hc}(x, r) = \bigoplus_{i=1}^{n} x_i \cdot r_i.$$

"XOR of random subset"

From one-way functions to pseudorandomness

Theorem (7.6)

Let f *be a one-way permutation with hard-core predicate* hc. *Then* $\mathrm{G}(s) := \mathrm{f}(s)||\mathrm{hc}(s)$ *is a prg (with expansion factor* $n+1$*).*

Theorem (7.7)

If there is a prg with expansion factor $n+1$, *then there is a prg with expansion factor* $p(n)$ *for any polynomial* p.

Theorem (7.8)

If there is a prg with expansion factor $2n$, *then there exists a prf.*

Theorem (7.9)

If there is a prf, then there exists a strong prp.

and back . . .

Proposition (7.28)

If there is a prg, then there is a one-way function.

In fact, any prg with expansion factor $2n$ it self is one-way.