Introduction to Modern Cryptography Recitation 4

Orit Moskovich
Tel Aviv University
November 23, 2016

One Way Function (OWF)

Definition. A function $f\colon \{0,1\}^n \rightarrow \{0,1\}^m$ is a **ε-one way function (ε-OWF)** if for any polynomial time adversary A:

$$\Pr_{x \leftarrow \{0,1\}^n}\left[A\big(f(x)\big) = x\right] < \varepsilon$$

- What if f is not one-to-one?
- What is ε?

DL → OWF

Definition. **The discrete logarithm problem**:
Let G be a cyclic group of order $|G| = m$ and a generator $g \in G$.
Given: $h = g^x$ for $x \in \mathbb{Z}_m = \{0, \ldots, m-1\}$
Output: x such that $g^x = h$

Definition. **The discrete logarithm assumption**:
There exists a cyclic group G for which the DL problem is hard

- Let p be a prime and a generator $g \in \mathbb{Z}_p^*$ (in which DL is hard)
- Define the OWF: $f(x) = g^x \ mod \ p$

Hard-Core Predicates

- Motivation:
  - A OWF f is hard to invert
  - Given $f(x)$, the value of x is hard to discover
  - However, a OWF f may disclose some information about its input

- Example:
  - Let f be a OWF
  - Define $g(x_1, x_2) = (f(x_1), x_2)$
  - g is also a OWF, and in the same time reveals x_2 completely

Hard-Core Predicates

Claim. If $f: \{0,1\}^n \to \{0,1\}^n$ is a OWF, then $g: \{0,1\}^{n+1} \to \{0,1\}^{n+1}$
$g(x_1, x_2) = (f(x_1), x_2)$ is also a OWF

- Assume g is not a OWF
- Then, there exist an efficient adversary A_g such that

$$\Pr_{x_1 \leftarrow \{0,1\}^n, x_2 \leftarrow \{0,1\}}\left[A_g\big(g(x_1, x_2)\big) = x_1, x_2\right] > \varepsilon$$

- We'll construct an efficient adversary A_f that inverts f w.p. $> \varepsilon$

1. The adversary A_f is given $f(x)$
2. A_f chooses at random $u' \leftarrow U_1$
3. A_f runs $A_g\big((f(x), u')\big)$ and returns the first n bits of the output

Hard-Core Predicates

- A hard-core predicate of a function f is:
  - A function $hc: \{0,1\}^n \to \{0,1\}$ such that:
  - Given $f(x)$ it is hard to guess $hc(x)$ w.p. $> \frac{1}{2} + \varepsilon$

Definition. A polynomial-time computable predicate $hc: \{0,1\}^n \to \{0,1\}$ is called a hard-core of a function f if for every PPT algorithm A:

$$\Pr_{x \leftarrow \{0,1\}^n}\left[A\big(f(x)\big) = hc(x)\right] \leq \frac{1}{2} + \varepsilon$$

- $hc(x)$ is called the hard core bit (HCB)

Hard-Core Predicates

Definition. A polynomial-time computable predicate $hc: \{0,1\}^n \to \{0,1\}$ is called a hard-core of a function f if for every PPT algorithm A:

$$\Pr_{x \leftarrow \{0,1\}^n}\left[A\big(f(x)\big) = hc(x)\right] \le \frac{1}{2} + \varepsilon$$

Equivalent Definition. A polynomial-time computable predicate $hc: \{0,1\}^n \to \{0,1\}$ is called a hard-core of a function f if

$$f(U_n), hc(U_n) \approx_{c,\varepsilon} f(U_n), U_1$$

Hard-Core Predicates

- We'll show one direction:
  $f(U_n), hc(U_n) \approx_{c,\varepsilon} f(U_n), U_1 \Rightarrow$
  for every PPT algorithm A, $\Pr_{x \leftarrow \{0,1\}^n}\left[A\big(f(x)\big) = hc(x)\right] \leq \frac{1}{2} + \varepsilon$
- Assume there exists a PPT algorithm A_1 such that
  $\Pr_{x \leftarrow \{0,1\}^n}\left[A_1\big(f(x)\big) = hc(x)\right] > \frac{1}{2} + \varepsilon$
- Construct the following PPT A_2

1. A_2 is given (u, b) (either from $\big(f(U_n), hc(U_n)\big)$ or $(f(U_n), U_1)$)
2. A_2 returns 1 $\Leftrightarrow A_1(u) = b$

Hard-Core Predicates

- Construct the following PPT A_2

1. A_2 is given (u, b) (either from $\left(f(U_n), hc(U_n)\right)$ or $(f(U_n), U_1)$)
2. A_2 returns 1 $\Longleftrightarrow A_1(u) = b$

- Let's analyze the result:

- $$\left| \underbrace{\Pr_{d_0 \leftarrow f(U_n), hc(U_n)}[A_2(d_0) = 1]}_{> \frac{1}{2} + \varepsilon} - \underbrace{\Pr_{d_1 \leftarrow f(U_n), U_1}[A_2(d_1) = 1]}_{= \frac{1}{2}} \right| > \varepsilon$$

Hard-Core Predicates

- Let‘s try $hc(x) = \bigoplus_{i=1}^{n} x_i$ where $x = x_1 x_2 \dots x_n$
- Is this a HCP for every OWF function f?
  - No!

- Let f be a OWF
- Define $g(x) = (f(x), \bigoplus_{i=1}^{n} x_i)$
- g is also a OWF, and at the same time reveals $hc(x)$ completely

Goldreich-Levin Theorem

- Every OWF can be trivially modified to obtain a OWF that has a specific hard-core predicate

OWP → PRG

Theorem. Let $f: \{0,1\}^n \rightarrow \{0,1\}^n$ be a OWP and let hc be a hard-core predicate of f.
Define $G: \{0,1\}^n \rightarrow \{0,1\}^{n+1}$ as follows: $G(s) = \big(f(s), hc(s)\big)$.
Then, G is a PRG.

Reminder: DL → OWF

- Let p be a prime and a generator $g \in \mathbb{Z}_p^*$ (in which DL is hard)
- Define the OWF: $f(x) = g^x \; mod \; p$

HCB for: DL → OWF

- Let p be a prime and a generator $g \in \mathbb{Z}_p^*$ (in which DL is hard)
- Define the OWF: $f(x) = g^x \; mod \; p$

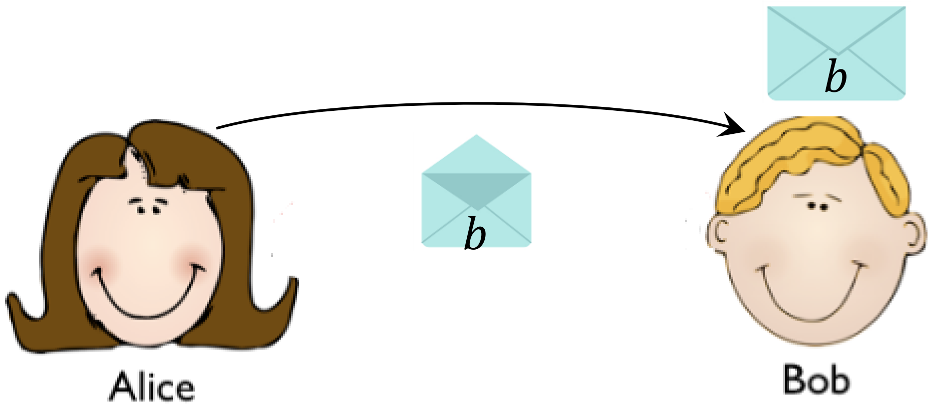
- First attempt:
- $hc(x) = parity(x) = x \; mod \; 2$
- We will prove in HW that this function is not a HCP

- Blum-Micali (without proof):
- Define $Half(x) = \begin{cases} 1 & x \in \left[1, \frac{p-1}{2}\right] \\ 0 & \text{otherwise} \end{cases}$

Bit Commitment

- A two party protocol between computationally bound Alice and Bob

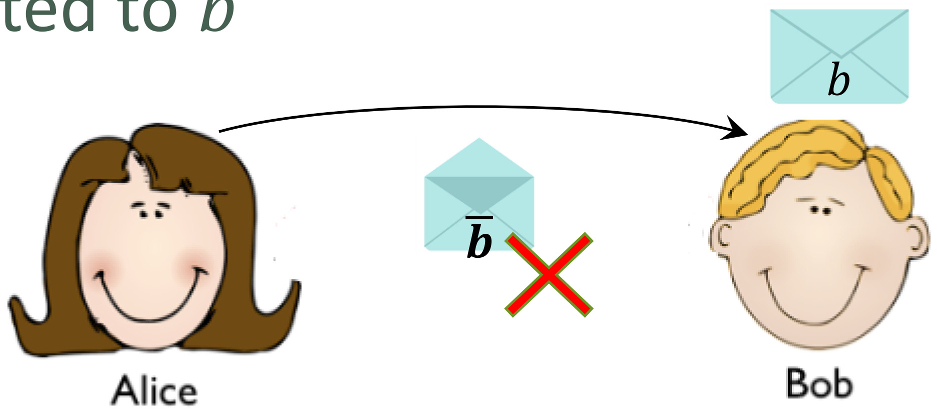
- Alice **commits** to a bit b (which she is chooses)
- Bob cannot tell what b is after the commitment phase
- At a decommit phase, Alice **reveals** b, and Bob is convinced this is indeed the bit Alice committed to



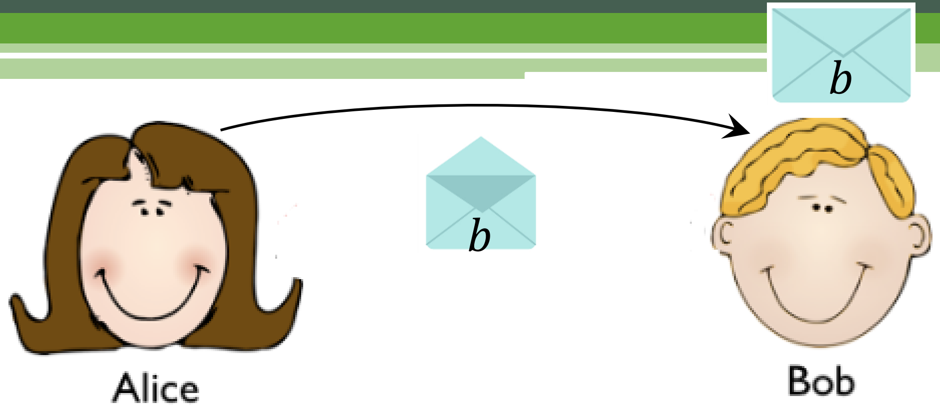
Bit Commitment

- A two party protocol between computationally bound Alice and Bob

- Alice **commits** to a bit b (which she is chooses)
- Bob cannot tell what b is after the commitment phase
- At a decommit phase, Alice **reveals** b, and Bob is convinced this is indeed the bit Alice committed to
- Alice cannot convince Bob she committed to $\bar{b}$



Bit Commitment



- Commit Stage:
  - The sender S (Alice) has private input $\sigma \in \{0,1\}$
  - S chooses a private random input r
  - S sends to the receiver R (Bob) the commitment $C(\sigma, r)$
- Decommit Stage:
  - S sends σ, r to R
  - R either accepts or rejects

- Hiding property: $\forall \sigma_1, \sigma_2 \in \{0,1\}. C(\sigma_1, r) \approx_\varepsilon C(\sigma_2, r)$
- Binding property: $\nexists \sigma_1, r_1, \sigma_2, r_2$ s.t $C(\sigma_1, r_1) = C(\sigma_2, r_2)$ and $\sigma_1 \neq \sigma_2$

OWP → Bit Commitment

- Let $f: \{0,1\}^n \to \{0,1\}^n$ be a OWP with a HCP $hc: \{0,1\}^n \to \{0,1\}$

- Commit Stage:
  - The sender S has private input $\sigma \in \{0,1\}$
  - S chooses a private random input $r \leftarrow \{0,1\}^n$
  - S sends to the receiver R the commitment $C(\sigma, r) = (f(r), hc(r) \oplus \sigma)$
- Decommit Stage:
  - S sends σ, r to R
  - R verifies the correctness either accepts or rejects

✓Binding property: $\nexists \sigma_1, r_1, \sigma_2, r_2$ s.t $C(\sigma_1, r_1) = C(\sigma_2, r_2)$ and $\sigma_1 \neq \sigma_2$

✓Hiding property: $\forall \sigma_1, \sigma_2 \in \{0,1\}. C(\sigma_1, r) \approx_{c,\varepsilon} C(\sigma_2, r)$

OWP ➔ Bit Commitment

- Let $f: \{0,1\}^n \to \{0,1\}^n$ be a OWP with a HCP $hc: \{0,1\}^n \to \{0,1\}$

- Commit Stage:
  - The sender S has private input $\sigma \in \{0,1\}$
  - S chooses a private random input $r \leftarrow \{0,1\}^n$
  - S sends to the receiver R the commitment $C(\sigma, r) = (f(r), hc(r) \oplus \sigma)$
- Decommit Stage:
  - S sends σ, r to R
  - R verifies the correctness either accepts or rejects

tradeoff

✓Binding property: $\nexists \sigma_1, r_1, \sigma_2, r_2$ s.t $C(\sigma_1, r_1) = C(\sigma_2, r_2)$ and $\sigma_1 \neq \sigma_2$

✓Hiding property: $\forall \sigma_1, \sigma_2 \in \{0,1\}. C(\sigma_1, r) \approx_{c,\varepsilon} C(\sigma_2, r)$

Coin Flipping Over the Phone

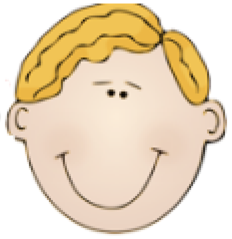
- Let $f: \{0,1\}^n \to \{0,1\}^n$ be a OWP with a HCP $hc: \{0,1\}^n \to \{0,1\}$
- Let $C(x,r) = (f(r), hc(r) \oplus x)$

Alice

1. Alice chooses a random bit x and sends $C(x,r)$

2. Bob chooses a random bit x' and send it to Alice

3. Alice sends x, r



Bob

The outcome of the coin flip is $x \oplus x'$