EECS 575: Advanced Cryptography
Fall 2021
Lecture 7

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- More on discrete log
- OWF(P) based on discrete log
- Hardcore predicates + (Blum-Micali)

Agenda for this lecture

- Announcements
- Recap from last time
- More on discrete log
- OWF(P) based on discrete log
- Blum-Micali/Hardcore predicates

Announcements

- Homework 3 is due 10/4.
  - Take-home exam 1 will be released that day!
- Lecture topic vote, current standings:
  1. Cryptocurrencies/Blockchains
  2. Lattice-based cryptography
  3. fully-homomorphic encryption
  4. Advanced ZK (zkSNARKs)
  5. Verifiable computation

Ask on Piazza or email for info

Agenda for this lecture

- Announcements
- Recap from last time
- More on discrete log
- OWF(P) based on discrete log
- Blum-Micali/Hardcore predicates

Recap from last time: PRGs

$G : \{0,1\}^* \to \{0,1\}^*$ is a PRG if:

- Efficiently evaluated: $\exists$ deterministic ppt evaluator
- Expands its $\ell(|x|) > |x|$
- pseudorandom: $G(U_n) \approx_c U_{\ell(n)}$

Recap from last time: number theory

- Euler's theorem: Take finite abelian group G

$$a^{|G|} = 1$$

Proof in notes. Special case: $a \in \mathbb{N}$, $a^{p-1} \equiv 1 \bmod p$

- "Structure" of $\mathbb{Z}_p^*$: $\mathbb{Z}_p^*$ is cyclic. $\exists g$ (generator)

$$\underbrace{\{g^1, g^2, \ldots g^{p-1}\}}_{\text{not cyclic: this set's size} < p-1} = \{1, \ldots, p-1\}$$

Agenda for this lecture

- Announcements
- Recap from last time
- More on discrete log
- OWF(P) based on discrete log
- Blum-Micali/Hardcore predicates

The Discrete Logarithm Problem

Param. gen $S(1^n)$ outputs prime p, generator $g \in \mathbb{Z}_p^*$

Given $y \in \mathbb{Z}_p^*$ along w/ (p, g), compute $g^x \equiv y \bmod p$. (x discrete log)

Discrete log assumption: $\forall$ nuppt A,

$$\Pr_{\substack{(p,g) \leftarrow S(1^n) \\ x \leftarrow \mathbb{Z}_p^*}}[A(p, g, y) = x \text{ s.t. } g^x = y \bmod p] = \text{negl}(n)$$

OWP from discrete log

$f_{p,g}(x) = g^x \bmod p$. $f_{p,g} : \{1, \ldots, p-1\} \to \mathbb{Z}_p^*$

$f_{p,g}$ is a permutation! One-way permutation based on hardness of dlog.

$f_{p,g}$ efficient to evaluate?

One idea: $f_{p,g}(x) =$

```
For i = 1 to x:
    result *= g mod p
Return result
```

Not efficient!
Requires $\approx |\mathbb{Z}_p^*|$ mults

OWP from discrete log

Evaluate $f_{p,g}(x)$: result $\leftarrow g$
For $i = 1$ to $\log |x|$
result $\leftarrow$ (result)^2
Return result

exponentiates in $\log |\mathbb{Z}_p^*|$ multiplications

How to choose a generator of $\mathbb{Z}_p^*$?

Generate p along with factorization of $p-1$.

Primes $q_1, q_2 \ldots q_k$; order of $a \in G$ must divide $p-1$

Choose random elt, check $a^{q_1} \ldots a^{q_k} \stackrel{?}{=} 1$

Special case: $p = 2q+1$ prime q.

$p-1 = \mathbb{Z}_p^* = 2q$

Agenda for this lecture

- Announcements
- Recap from last time
- More on discrete log
- OWF(P) based on discrete log
- Blum-Micali/Hardcore predicates

Blum-Micali PRG

$G_{p,g} : \mathbb{Z}_p^* \to \mathbb{Z}_p^* \times \{0,1\}$ ← expands by one bit

$S(1^n)$ from dlog assumption. outputs (p, g)

$$G_{p,g}(x) = (f_{p,g}(x), h(x))$$ — $h(x)$: some function

Can expand as many bits as we want!

what is h? Function $h(x)$ should "look random" even given $f_{p,g}(x)$

$h(x)$ some bit definitely hidden by $f_{p,g}$

Hardcore Predicates

Function h is a hardcore predicate of $f_{p,g}$

Define:

A predicate $h: \{0,1\}^* \to \{0,1\}$ is a hardcore predicate for F if $\forall$ nuppt A,

$$\Pr_X[A(f(X)) = h(X)] - \frac{1}{2} = \text{negl}(n).$$

Claim: $h(x) = \left[x > \frac{p-1}{2}\right]$ (boolean output) is hardcore for $f_{p,g}$.

So $F_{p,g}(x) = \left(g^x \bmod p, \left[x > \frac{p-1}{2}\right]\right)$ is a PRG!

OWP+HCP yields a PRG

Theorem: Given a OWP $F: D \to D$ with hcp h,

(1) $(F(x), h(x)) \approx_c (F(x), b)$ (0)

where $x \leftarrow D$ and $b \leftarrow \{0,1\}$. Implies that $(F(x), h(x))$ is a PRG.

Proof idea: Turn distinguisher D for two distributions into a predictor for $h(x)$ given $f(x)$.

$D(y, b) \in \{0,1\}$

$A^D(y)$:

$b \leftarrow \{0,1\}$

$b' \leftarrow D(y, b)$

If $b' = 1$

  Ret b

Else

  Ret $\neg b$

OWP+HCP yields a PRG

$A^D(y)$:

$b \leftarrow \{0,1\}$

$b' \leftarrow D(y, b)$

If $b' = 1$

  Ret b

Else

  Ret $\neg b$

$$Adv^{hcp}(A) = \Pr_x[A(f(x)) = h(x)] - \frac{1}{2}$$

$$= \frac{1}{2}\left(\Pr_x[D(f(x), h(x)) = 1] + \Pr[D(f(x), \overline{h(x)}) = 0] - 1\right)$$

$$= \frac{1}{2}\left(\Pr_x[D(f(x), h(x)) = 1] - (1 - \Pr[D(f(x), \overline{h(x)}) = 0])\right)$$

$$= \frac{1}{2}\left(\Pr_x[D(f(x), h(x)) = 1] - \Pr[D(f(x), \overline{h(x)}) = 1]\right)$$

OWP+HCP yields a PRG

Define $P_U = \Pr_{\substack{x \in D \\ b \in \{0,1\}}}[D(f(x), b) = 1]$ $\quad P_G = \Pr[D(f(x), h(x)) = 1]$

$$= \frac{1}{2}\left(\Pr_x[D(f(x), h(x)) = 1] + \Pr_x[D(f(x), \overline{h(x)}) = 1]\right)$$

Claim $P_G - P_U = Adv^{dist}(D) = Adv^{hcp}(A)$

$(f(x), h(x)) \approx_c (f(x), b)$

In words: hcp "looks" random even given $f(x)$.