Lecture 20: Goldreich-Levin Hardcore Predicate & Applications

Observation on Bijections

- Let $f \colon \{0,1\}^n \to \{0,1\}^n$ be a bijection
- Suppose we sample $x \xleftarrow{\$} \{0,1\}^n$
- For any $y \in \{0,1\}^n$, what is the probability that $f(x) = y$?
  - Note that there is a unique x' such that $f(x') = y$, because f is a bijection
  - $f(x) = y$ if and only if $x = x'$, i.e. the probability that $f(x) = y$ is $1/2^n$.
- So, the distribution of $f(x)$, where $x \xleftarrow{\$} \{0,1\}^n$, is a uniform distribution over $\{0,1\}^n$

- We define the inner product of $r \in \{0,1\}^n$ and $x \in \{0,1\}^n$ as $\langle r, x \rangle = \sum_{i=1}^{n} r_i x_i$
- We will state the Goldreich-Levin Hardcore Predicate without proof

Theorem (Goldrecih-Levin Hardcore Predicate)

If $f\{0,1\}^n \to \{0,1\}^n$ is a one-way function then the bit $b = \langle r, x \rangle$ cannot be predicted given $(r, f(x))$.

A note on "Predicting a bit"

- Note that it is trivial to correctly predict any bit with probability $1/2$. (Guess a uniformly random bit z. The probability that z is identical to the hidden bit is $1/2$)

- To <u>non-trivially</u> predict a hidden bit, the adversary has to correctly predict it with probability at least $1/2 + \varepsilon$, where $\varepsilon = 1/\mathrm{poly}(n)$
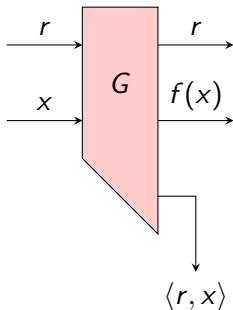
One-bit Extension PRG I

- Recall: A pseudorandom generator (PRG) is a function $G_{n,n+\ell} \colon \{0,1\}^n \to \{0,1\}^{n+\ell}$ such that, for $x \xleftarrow{\$} \{0,1\}^n$, the output $G_{n,n+\ell}(x)$ *looks like* a random $(n+\ell)$-bit string.

- A one-bit extension PRG has $\ell = 1$

- Suppose $f \colon \{0,1\}^n \to \{0,1\}^n$ is a OWP (i.e., f is a OWF and it is a bijection)

- Note that the mapping $(r, x) \mapsto (r, f(x))$ is a bijection

- So, the output $(r, f(x))$ is a uniform distribution if $(r, x) \xleftarrow{\$} \{0,1\}^{2n}$

- Now, the output $(r, f(x), \langle r, x \rangle)$ looks like a random $(2n+1)$-bit string if f is a OWF (because of Goldreich-Levin Hardcore Predicate result)

One-bit Extension PRG II

- Consider the function $G_{2n,2n+1}: \{0,1\}^{2n} \to \{0,1\}^{2n+1}$ defined as follows

$$G_{2n,2n+1}(r,x) = (r, f(x), \langle r, x \rangle)$$

- This is a one-bit extension PRG if f is a OWP
- This construction will be pictorially represented as follows

- In the previous step, we saw how to construct a one-bit extension PRG G

- Now, we use the previous step iteratively to construct arbitrarily long pseudorandom bit-strings

- The next slide, using the one-bit extension PRG, provides the intuition to construct $G_{2n,\ell} \colon \{0,1\}^{2n} \to \{0,1\}^{\ell}$, for arbitrary $\ell = \mathrm{poly}(n)$.

- The example shows only $\ell = 5$ but can be extended naturally to arbitrary $\ell = \mathrm{poly}(n)$
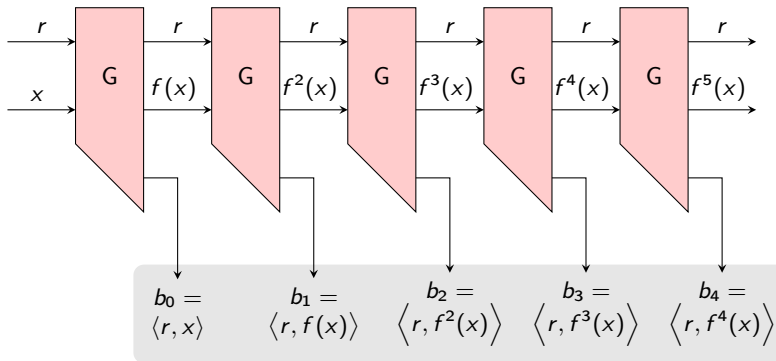
- This is a PRG that takes n-bit seed and outputs $2n$-bit string
- $G_{n,2n}$ is a length-doubling PRG if $G_{n,2n} \colon \{0,1\}^n \to \{0,1\}^{2n}$ and $G_{n,2n}$ is a PRG
- We can use the iterated construction in the previous slide to construct a length-doubling PRG from one-bit extension PRG

- Design secret-key encryption schemes where the message is much longer than the secret key