

CS 276: Homework 3

Due Date: Friday September 27th, 2024 at 8:59pm via Gradescope

1 A Pseudorandom Function Based on Diffie-Hellman

Let us construct a more efficient variant of the Naor-Reingold PRF.

Definition 1.1 (PRF Construction) Let \mathbb{G} be a cryptographic group of prime order p . Let $\ell \in \mathbb{N}$ be polynomial in λ . Next, let $s^{*n} = (s_1, \dots, s_n, h)$ be sampled from $\mathcal{S}^{*n} := \mathbb{Z}_p^n \times \mathbb{G}$, and let $x^{*n} = (x_1, \dots, x_n)$ be drawn from $\mathcal{X}^{*n} = [\ell]^n$. Finally, define $F^{*n} : \mathcal{S}^{*n} \times \mathcal{X}^{*n} \rightarrow \mathbb{G}$ as follows:

$$F^{*n}(s^{*n}, x^{*n}) = \begin{cases} 1, & \prod_{i \in [n]} (s_i + x_i) = 0 \\ h^{1/\prod_{i \in [n]} (s_i + x_i)}, & \text{else} \end{cases}$$

This construction is more efficient than Naor-Reingold's PRF. F^{*n} can handle an input x^{*n} of length $n \cdot \lg(\ell)$ bits, whereas the same seed in the Naor-Reingold PRF would handle inputs of length n bits.

Question: Prove that the function F^{*n} given in definition 1.1 is a secure PRF assuming the ℓ -DDH assumption (assumption 1.2).

Assumption 1.2 (ℓ -DDH Assumption) Let \mathbb{G} be a cryptographic group of prime order p , and let $\ell < p$. Then for any PPT adversary \mathcal{A} , the following two hybrids are indistinguishable:

- \mathcal{G}_0 : The challenger samples $(\alpha, g) \xleftarrow{\$} \mathbb{Z}_p \times \mathbb{G}$ and then gives the adversary $(g, g^\alpha, g^{\alpha^2}, \dots, g^{\alpha^\ell}, g^{1/\alpha})$.
- \mathcal{G}_1 : The challenger samples $(\alpha, g, r) \xleftarrow{\$} \mathbb{Z}_p \times \mathbb{G} \times \mathbb{G}$ and then gives the adversary $(g, g^\alpha, g^{\alpha^2}, \dots, g^{\alpha^\ell}, r)$.

Finally, when $\alpha = 0$, then define $g^{1/\alpha} = 1$.

Note that p must be super-polynomial in λ because otherwise ℓ -DDH does not hold.

Hint: You may wish to use the following strategy. First, let us define a PRF f over a smaller domain $[\ell]$. Let f take a seed $(s, h) \in \mathbb{Z}_p \times \mathbb{G}$ and an input $x \in [\ell]$ and output:

$$f((s, h), x) = \begin{cases} 1, & s + x = 0 \\ h^{1/(s+x)}, & \text{else} \end{cases}$$

First prove that f is a secure PRF when ℓ is polynomial in the security parameter λ .

Second, note that F^{*n} is an n -fold composition of f , where the output of one invocation of f becomes the h -value of the next invocation of f .

$$F^{*n}((s_1, \dots, s_n, h), (x_1, \dots, x_n)) = f((s_n, \dots, f((s_2, f((s_1, h), x_1)), x_2) \dots), x_n)$$

Then use a similar proof technique to the one used for Naor-Reingold's PRF to prove that the composition of this small-domain PRF f is also a PRF.

References