CS171 HW8

Q1.1) Construction of B that solves mCDH(n, G, B):

(i) Challenger of mCDH samples $(G, q, g) \leftarrow \mathcal{G}(1^n)$ and $x \leftarrow \mathbb{Z}_q$, then sends to B the inputs (G, q, g, g^x)

(ii) B gives $(G, q, g, g^x, g^y = g^x)$ to A, as if these inputs were given by challenger of CDH(n, G, A)

(iii) A outputs $h \in G$ such that $h = g^{x \cdot y} = g^{x \cdot x} = g^{x^2}$

(iv) B outputs the same h

Because B simulates the environment for CDH(n, G, A) successfully, the probability $Pr[mCDH(n, G, A) \to 1] = Pr[CDH(n, G, B) \to 1]$ which is non-negligible.

Q1.2) Construction of A that solves CDH(n, G, B):

(i) Challenger of CDH samples $(G, q, g) \leftarrow \mathcal{G}(1^n)$ and $x, y \leftarrow \mathbb{Z}_q$, then sends to A the inputs (G, q, g, g^x, g^y)

(ii) A use B to find $\left\{ \begin{array}{l} g^{x^2} \\ g^{y^2} \\ g^{(x+y)^2} \end{array} \right\}$ via inputs $\left\{ \begin{array}{l} (G, q, g, g^x) \\ (G, q, g, g^y) \\ (G, q, g, g^x \cdot g^y = g^{x+y}) \end{array} \right.$

(iii) A outputs $h = g^{x \cdot y} = \dfrac{g^{x^2} \cdot g^{2xy} \cdot g^{y^2}}{2; g^{x^2} \cdot g^{y^2}} = \dfrac{g^{(x+y)^2}}{2g^{x^2} \cdot g^{y^2}}$

Because A simulates the environment for mCDH(n, G, B) successfully, the $Pr[CDH(n, G, B) \to 1] = Pr[mCDH(n, G, A) \to 1]$ which is non-negligible.

Q2e) $$y = \frac{x_t \sum_{j=1}^{t-1} a_j x_j - x_t' \sum_{j=1}^{t-1} a_j x_j'}{x_i' - x_i} \quad \text{for } j \neq i$$

Q2 Proof) If A breaks the collision-resistence of H, then we have

$$H^s(x_1 \cdots x_t) = H^s(x_1' \cdots x_t')$$

$$g^{x_t} \cdot \left(\prod_{j=1}^{j=t-1} (g^{a_j})^{x_j}\right) \cdot h^{x_t} = g^{x_t'} \cdot \left(\prod_{j=1}^{j=t-1} (g^{a_j})^{x_j'}\right) \cdot h^{x_t'}$$

which rearranges to our expression for y in the previous part

∴ B solves the dlog with same prob as A breaking CRHF

Q3. If there exists A' that breaks unforgeability of Π', we can construct A that uses A' to break unforgeability of Π

A is constructed:

(i) When A' requests a signature on message m from challenger of Π', A sample $r \leftarrow \{0,1\}^n$ and request $\sigma_0 = Sign(sk, m \oplus r)$ & $\sigma_1 = Sign(sk, r)$ from challenger of Π, then give $\sigma = (r, \sigma_0, \sigma_1)$ to A

(ii) When A' outputs m^* & $\sigma^* = (r^*, \sigma_0^*, \sigma_1^*)$, A outputs $m^* \oplus r^*$ & σ_0^* to challenger of Π

If A' successes, then $Verify(pk, m^* \oplus r^*, \sigma_0^*) = 1$, and so as A should succeess.

The $Pr[Forge_{A,\Pi} = 1] = Pr[Forge_{A',\Pi'} = 1] - Pr[(m^* \oplus r^*) \in M_\Pi]$

$$\underbrace{Pr[Forge_{A',\Pi'} = 1]}_{\text{by assumption}, \geq negl(n)} \qquad \underbrace{Pr[(m^* \oplus r^*) \in M_\Pi]}_{\leq negl}$$

∴ For A' to be successful, it must not have queried m^* before, so $Pr[(m^* \oplus r^*) \in M_\Pi]$ is as small as $\frac{|M|}{2^n}$ which could be assumed to be negligible

∴ $Pr[Forge_{A,\Pi} = 1]$ is ~~nonnegligible~~ non-negligible if $Pr[Forge_{A',\Pi'} = 1]$ is non-negigible, a contradiction.