# Homework 3

Advanced Tools From Modern Cryptography
CS 758 : Spring 2018

Released: November 17 Friday
Due: December 1 Friday

## Bi-Linear Pairings [Total 50 pts]

**Notation:** In this assignment, we consider a bilinear pairing operation $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_t$ where $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t$ are prime order groups. We use multiplicative notation for all groups. We write $e$ to also denote a specification of the pairing operation, along with the specification of the groups $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t)$. Assumptions will refer to an algorithm BiGen to sample $(e, g_1, g_2)$ where $g_1, g_2$ are generators for $\mathbb{G}_1, \mathbb{G}_2$ respectively.

The naming of the assumptions (other than DDH) are non-standard.

1. **Bi-Linear Pairing and DDH - I** [25 pts]

   Consider the following assumption for a distribution over groups with bilinear pairings:

   **xCDH Assumption** for BiGen: For any PPT adversary $A$, the following probability is negligible:

$$\Pr_{\substack{(e,g_1,g_2)\leftarrow \mathsf{BiGen} \\ a\leftarrow \mathbb{Z}_{|\mathbb{G}_1|}}}[(h_1, h_1', h_2, h_2') \leftarrow A(e, g_1, g_2, g_1^a)] \text{s.t. } \exists r \in \mathbb{Z}_p \setminus \{0\} \ \ (h_1, h_1', h_2, h_2') = (g_1^r, g_1^{ar}, g_2^r, g_2^{ar})$$

   (a) Show that xCDH Assumption is falsifiable. That is, show how to check if a tuple $(h_1, h_1', h_2, h_2')$ returned by an adversary meets the requirement that $\exists r \in \mathbb{Z}_p \setminus \{0\}$ $(h_1, h_1', h_2, h_2') = (g_1^r, g_1^{ar}, g_2^r, g_2^{ar})$. You should show how to check this given only $(e, g_1, g_2, g_1^a)$ (i.e., only $g_1^a$ rather than $a$ itself), so that an adversary can itself check its answer.

   (b) Consider the DDH assumption, restated for bilinear groups (essentially the DDH for $\mathbb{G}_1$, when the adversary is also given $(\mathbb{G}_2, g_2)$):

   **DDH Assumption** for BiGen:

$$\{(e, g_1, g_2, g_1^a, g_1^b, g_1^{ab})\}_{\substack{(e,g_1,g_2)\leftarrow \mathsf{BiGen} \\ a,b\leftarrow \mathbb{Z}_{|\mathbb{G}_1|}}} \approx \{(e, g_1, g_2, g_1^a, g_1^b, g_1^c)\}_{\substack{(e,g_1,g_2)\leftarrow \mathsf{BiGen} \\ a,b,c\leftarrow \mathbb{Z}_{|\mathbb{G}_1|}}}$$

   Show that the DDH assumption for BiGen implies the xCDH Assumption for BiGen.

   Hint: You need to construct a DDH adversary given an adversary $A$ that breaks the xCDH Assumption. Recall that if $\mathbb{G}_1 = \mathbb{G}_2$, then DDH does not hold. Here, $\mathbb{G}_1 \neq \mathbb{G}_2$, but the adversary that breaks the xCDH Assumption can be used to "transfer" the exponent $a$ from $g_1$ to $g_2$.

2. **Bi-Linear Pairing and DDH - II** [25 pts]

   Consider another assumption for groups with bilinear pairings.

**Hardness of Orthogonal Pairing (HOP) Assumption** for $\mathsf{BiGen}$: For any PPT adversary $A$, the following probability is negligible (where $1$ denotes the identity element in $\mathbb{G}_t$):

$$\Pr_{\substack{(e,g_1,g_2)\leftarrow\mathsf{BiGen}\\ h_1,h_1'\leftarrow\mathbb{G}_1}}[(h_2,h_2')\leftarrow A(e,g_1,g_2,h_1,h_1')]\text{s.t. } e(h_1,h_2)e(h_1',h_2')=1 \text{ and } h_2'\neq 1.$$

(a) Show that DDH for $\mathsf{BiGen}$ implies HOP for $\mathsf{BiGen}$.

(b) Recall vector commitment of group elements. It uses a trusted setup consisting of a bilinear pairing operator $e$, a vector of generators of $\mathbb{G}_1$, $\mathbf{t}=(t_0,t_1,\ldots,t_n)$. To commit to a message $\mathbf{m}\in\mathbb{G}_2^n$, sample $\rho\leftarrow\mathbb{G}_2$ and let $\mathsf{Com}_{h,\mathbf{t}}(\mathbf{m};\rho)=e(t_0,\rho)\prod_{i=1}^n e(t_i,m_i)$. Opening the commitment involves revealing $(\mathbf{m},\rho)$.

Show that HOP for $\mathsf{BiGen}$ implies binding for the above commitment scheme. That is, a PPT adversary $A$ that produces an equivocation $(c,\mathbf{m},\rho,\mathbf{m}',\rho')$ such that $c=e(t_0,\rho)\prod_{i=1}^n e(t_i,m_i)=e(t_0,\rho')\prod_{i=1}^n e(t_i,m_i')$ and $\mathbf{m}\neq\mathbf{m}'$ can be used to define an adversary that breaks HOP assumption.

*Hint:* First try a HOP adversary that invokes the commitment adversary with $t_0=h_1'$ and $t_i=h_1^{\alpha_i}$ for $i>0$. Show that an equivocation can be turned into $h_2,h_2'$ such that $e(h_1,h_2)e(h_1',h_2')=1$. But this leaves open the possibility that $h_2=h_2'=1$, if (somehow) the equivocated messages are appropriately correlated with $\alpha_i$. To fix this, show that taking $t_i=h_1^{\alpha_i}{h_1'}^{\beta_i}$ (and keeping $h_2$ to the same as before, while updating $h_2'$ suitably), for $i>0$ makes the probability of this happening negligible.