CS276: Cryptography	November 17, 2015

Amplification of Indistinguishability Obfuscation

Instructor: Alessandro Chiesa — *Scribe: Linyue Zhu*

1 Amplification

Theorem 1 *IO for* $NC_2 + FHE$ *with* $Dec \in NC_1 \to$ *IO for all poly-size circuit.*

Proof: Say $\mathcal{O}$ in IO for NC_1.

$$\begin{aligned}\tilde{\mathcal{O}} :&= 1.\ (pk_1, sk_1) \leftarrow G(1^k), (pk_2, sk_2) \leftarrow G(1^k)\\ &= 2.\ e_1 \leftarrow Enc(pk_1, c),\ e_2 \leftarrow Enc(pk_2, c)\\ &= 3.\ \hat{P} \leftarrow \mathcal{O}(P_{pk_1,pk_2,sk_1,e_1,e_2})\\ &= 4.\ \text{output } (e_1, e_2, pk_1, pk_2, \hat{D})\end{aligned}$$

$\hat{P}_{pk_1,pk_2,sk_1,e_1,e_2}(x, e_1^*, e_2^*, aux_1, aux_2) :=$

1. check that $e_1^* = Eval(pk_1, u_x, e_1)$ via aux_1, $e_2^* = Eval(pk_2, u_x, e_2)$ via aux_2
2. $c(x) \leftarrow Dec_{sk_1}(e_1^*)$

$$\begin{aligned}\hat{c}(x) :&= 1.\ e_1^* \leftarrow Eval(pk_1, u_x, e_1),\ e_2^* \leftarrow Eval(pk_2, u_x, e_2)\\ &= 2.\ aux_1 = \text{transcript of } Eval(pk_1, u_x, e_1),\ aux_2 = \text{transcript of } Eval(pk_2, u_x, e_2)\\ &= 3.\ c(x) \leftarrow \hat{P}(x, e_1^*, e_2^*, aux_1, aux_2)\end{aligned}$$

We want to show that $\forall c_1, c_2, c_1 = c_2, |c_1| = |c_2|,\ \tilde{O}(c_1) \overset{c}{=} \tilde{O}(c_2)$.

$H_0 :\ \tilde{\mathcal{O}}(c_1)$

$H_1 :$
1. $(pk_1, sk_1) \leftarrow G(1^k),\ (pk_2, sk_2) \leftarrow G(1^k)$
2. $e_1 \leftarrow Enc(pk_1, c_1),\ e_2 \leftarrow Enc(pk_2, c_2)$
3. $\hat{P} \leftarrow \mathcal{O}(P_{pk_1,pk_2,e_1,e_2,sk_1})$

$H_2 :$
1. $(pk_1, sk_1) \leftarrow G(1^k),\ (pk_2, sk_2) \leftarrow G(1^k)$
2. $e_1 \leftarrow Enc(pk_1, c_1),\ e_2 \leftarrow Enc(pk_2, c_2)$
3. $\hat{P} \leftarrow \mathcal{O}(P_{pk_1,pk_2,e_1,e_2,sk_2})$

$H_3 :$
1. $(pk_1, sk_1) \leftarrow G(1^k),\ (pk_2, sk_2) \leftarrow G(1^k)$
2. $e_1 \leftarrow Enc(pk_1, c_2),\ e_2 \leftarrow Enc(pk_2, c_2)$
3. $\hat{P} \leftarrow \mathcal{O}(P_{pk_1,pk_2,e_1,e_2,sk_2})$

$H_4: \ \tilde{\mathcal{O}}(c_2)$

Using the property of IO security, H_1 and H_2 are indistinguishable. Using the property of FHE security, H_2 and H_3 are indistinguishable. Again, using the property of IO security, H_3 and H_4 are indistinguishable. □

Lemma 2 ~~$IO \nrightarrow OWFs$.~~

Proof: ~~Suppose that $IO \rightarrow OWFs$.~~

~~Then $IO \rightarrow P \neq NP$, i.e., $P = NP \rightarrow \overline{IO}$.~~

~~But actually if $P = NP$,~~

~~$\mathcal{O}(c)$:="output lexically first circuit with $|c|$ gates that outputs c".~~ □

This lemma should be formalized as below.

Lemma 3

If $P = NP$, then $OWFs$ do not exist.
If $P = NP$, then IO exists.

Thus we cannot prove that $IO \rightarrow OWFs$, because this statement depends on the answer of whether P equals NP or not.

Ideal Lemma 4

$IO + P = NP \rightarrow \overline{OWFs}$. *This is true even without IO.*
$IO + P \neq NP \rightarrow OWFs$. (?)

We do not prove how to prove $IO + P \neq NP \rightarrow OWFs$. But we prove the following similar statement.

Actual Lemma 5 $IO + coRP \neq NP \rightarrow OWFs$.

Proof: Assume IO. We prove that $coRP \neq NP \rightarrow OWFs$, i.e., $\overline{OWFs} \rightarrow coRP \supseteq NP$.

$$\underline{WTS}: \text{Circuit } SAT \in coRP, i.e., \exists \text{ ppt } D \text{ such that}$$
$$\forall c^* \in \text{Circuit } SAT \rightarrow \Pr[D(c^*) = 1] = 1$$
$$\forall c^* \notin \text{Circuit } SAT \rightarrow \Pr[D(c^*) = 1] \leq \frac{1}{2}$$

How to construct D?

Construct $F = \{f_k : \{0,1\}^k \rightarrow \{0,1\}^k\}$ where $f_k(x) := \mathcal{O}(Z_{k,n}, x)$.

Since $\overline{OWFs}$, $\exists$ ppt A that inserts Fsuch that

$\Pr[f(A(\mathcal{O}(Z,x))) = \mathcal{O}(Z,x)] \geq \delta(k)$.

Given circuit C,

$\triangle(C,Z) := |\Pr_x[f(A(\mathcal{O}(C,x))) = \mathcal{O}(C,x)] - \Pr_x[f(A(\mathcal{O}(Z,x))) = (Z,x)]|$

For every $C : \{0,1\}^k \to \{0,1\}^k$ with n gates:

if $C \equiv 0$ then $\triangle(C,z) \geq negl(K)$
if $\not\equiv 0$ then $\Pr_x[f(A(\mathcal{O}(C,x))) = \mathcal{O}(C,x)] = 0$

$\square$