CS276: Cryptography November 19, 2015

IO and One-way functions

Instructor: Alessandro Chiesa *Scribe: Akshay Ram*

1 Introduction

Last time we talked about Indistinguishability obfuscation from NC^1 to all circuits. We also began to look at the strength of obfuscation, IO and VBB, as an assumption compared to that of the existence, which till now has been the weakest object we have seen (in that all other constructions imply their existence). We also cover a different version of obfuscation based on a different equality constraint for messages that are obfuscated.

2 Indistinguishability Obfuscation and One Way functions

Theorem 1 *IO + (coRP $\neq$ NP) $\implies$ OWF*

Proof: Assume IO and show the contrapositive: $\overline{OWF} \implies (NP \subseteq coRP)$
Let L be the NP relation defined by Circuit-SAT. Then we need to show:
There exists a probabilistic polynomial time algorithm D such that:

$$\forall C \in L : \mathbb{P}[D(C) = 1] = 1$$

$$\forall C \notin L : \mathbb{P}[D(C) = 1] \leq 1/2$$

Consider the family of functions $F = \{f_k : \{0,1\}^k \to \{0,1\}^*\}_k$ where $f_k(x) = \theta(Z_{k,n}, x)$.
Here $Z_{k,n}$ is the identically zero circuit with n gates on k bits of input, and θ is an IO obfuscator.
Since OWF does not exist by assumption, $\exists$ ppt A that can invert f_k with non-negligible success:

$$\mathbb{P}[f_k(A(\theta(Z_{k,n}, x))) = \theta(Z_{k,n}, x)] \geq \delta(k)$$

Let $\Delta(C, Z) := |\mathbb{P}[f(A(\theta(C, x))) = \theta(C, x)] - \mathbb{P}[f(A(\theta(Z, x))) = \theta(Z, x)]|$. Then for any circuit with n gates $C : \{0,1\}^k \to \{0,1\}^*$:

$$(C \equiv False) \equiv (C \notin L) \implies \Delta(C, Z) \leq 1/p(k)$$

because IO security guarantees that no such distinguisher can exist between equivalent circuits.

$$(C \not\equiv False) \equiv (C \in L) \implies \mathbb{P}[f(A(\theta(C, x))) = \theta(C, x)] = 0$$

because $\theta(C)$ is not in the range of f, so there is no pre-image. Now we can construct the ppt decider for Circuit-SAT

```
def D(C): /* Decides if circuit C can be satisfied for some inputs */
        Sample x randomly such that |x| = k;
        Run the obfuscator y := O(C,x)
        Run the inverter x' := A(y)
        if f(x') == y: return 0
        else: return 1
```

In this algorithm, if C is satisfiable, A will never find a pre-image: $\mathbb{P}[D(C) = 1] = 1$
Otherwise, C is equivalent to Z: $\mathbb{P}[D(C) = 0] \geq \delta(k) - negl(k)$ □

3 Virtual Black-box Obfuscation and One way function

Theorem 2 *$VBB \implies OWF$*

Proof: Let θ be a VBB Obfuscator
Consider $\alpha \in \{0,1\}^k, \beta \in \{0,1\}$, and the point function $C_{\alpha,\beta}(x) := \beta \cdot \delta_\alpha(x)$. Then the function $f(\alpha, \beta, x) := \theta(C_{\alpha,\beta}, x)$ is OWF, because the only success comes from randomly guessing the output or finding α:

$$\mathbb{P}[S^{C_{\alpha,\beta}}(1^k) = \beta] = \frac{1}{2} + negl(k)$$

Then by the definition of f, and the VBB assumption:

$$\mathbb{P}[A(\theta(C_{\alpha,\beta}, x)) = \beta] = \mathbb{P}[A(f(\alpha, \beta, x)) = \beta] = \frac{1}{2} + negl(k)$$

So f has a hard-core bit β which means that f is OWF. □

4 The Five Worlds of Impagliazzo

- Algorithmica: NP is easy in the worst case, $NP \subseteq P; NP \subseteq BPP$; OWF don't exist
- Heuristica: NP is easy on average, $NP \neq P; NP \neq BPP$; OWF don't exist
- Pessiland: NP is hard on average, but also OWF don't exist
- Minicrypt: OWF exist, but no public key cryptography (for example)
- Cryptomania: OWF exist, and Public key crypto systems exist

5 Differing Input Obfuscation

Now we define another type of obfuscation on circuits that can computationally be distinguished on their outputs, in order to produce a new idea of encryption.

Definition 3 *A ppt θ is DIO if*

1. *Correctness:* $\forall C \forall x : \theta(C)(x) = C(x)$
2. *Efficiency:* $\forall C : |\theta(C)| \in poly(|C|)$
3. *Security: $\forall$ ppt A, $\exists$ ppt E such that $\forall C_1, C_2$ with $|C_1| = |C_2|$:*
   Suppose $|\mathbb{P}[A(\theta(C_1)) = 1] - \mathbb{P}[A(\theta(C_2)) = 1]| \geq 1/p(k)$
   Then for circuits $C_1' \equiv C_1, C_2' \equiv C_2, |C_1'| = |C_1| = |C_2'| = |C_2|$,
   $x \leftarrow E(C_1', C_2')$ *such that* $C_1'(x) \neq C_2'(x)$.
   In other words, if it is computationally hard to find a point at which two circuits differ, then it is computationally hard to distinguish between obfuscated versions of those circuits.

Definition 4 *An EWE scheme for an NP-relation R is a pair (E,D) such that*

1. *Correctness:* $\forall k \in \mathbb{N}, \forall m \in \{0,1\}, \forall (x,w) \in R :$
   $\mathbb{P}[D(1^k, E(1^k, x, m), w) = m] = 1$

2. *Extractable Security:* $\forall$ *ppt A,* $\exists$ *ppt Ext:*
   $|\mathbb{P}[A(E(1^k, x, 0)) = 1] - \mathbb{P}[A(E(1^k, x, 1)) = 1]| \geq 1/p(k) \implies$
   $w \leftarrow Ext(1^k, x)$ *such that* $(x, w) \in R$*.*
   In other words, if an adversary can decrypt under some NP input x, then the adversary can also produce a witness for that input.

$IO \implies DIO$ for circuits that differ at polynomial number of inputs.

Theorem 5 *Last time, we showed that* $IO \implies WE$ *(Witness Encryption). Now we can analogously show that* $DIO \implies EWE$*.*

Proof: Given DIO θ:
$E(1^k, x, m) = \theta(C_{x,m})$ where $C_{x,m}(y) = m \cdot \delta_{(x,y)\in R}$ and $\perp$ otherwise
$D(1^k, c, w) = c(w)$
Now if $y \leftarrow Ext(\theta(C_{x,0}), \theta(C_{x,1}))$ such that $\theta(C_{x,0})(y) \neq \theta(C_{x,1})(y)$, then y is the witness for the input x, because the circuits return $\perp$ for every non-witness by construction. $\square$