Foundation of Cryptography (0368-4162-01), Fall 2011 Iftach Haitner

Final Exam

6.2.2012

Time Limit: 3 hours
Instructions:

- The exam is open book, you might use any written material.
- Please write clearly, and prove your answers. In case you are using an unproven "fact", please state the fact clearly, and explain why you are not proving it ("lack of time","easy to see", etc.).
- There are three questions, each contributes up to 33 points (hence, the minimal grade is 1).

  Each question has three sub-questions. The best solved sub-question contributes up to 20 points, the second best contributes up to 10 points, and the last good one up to 3 points.

Good Luck!

1. Recall the definition of hardcore predicate we've seen in class:

   Definition 1 (hardcore predicate)**.** *A function* $b\colon \{0,1\}^{\ell(n)} \mapsto \{0,1\}$ *is an* hardcore predicate *of a function* $f\colon \{0,1\}^{\ell(n)} \mapsto \{0,1\}^{m(n)}$,[1] *if*

   $$\mathsf{Pr}_{x \leftarrow \{0,1\}^{\ell(n)}}[\mathsf{P}(1^n, f(x)) = b(x)] \leq \frac{1}{2} + \operatorname{neg}(n),$$

   for any PPT P *and large enough* n.

   (a) Show the existence of a polynomial-time computable functions $b\colon \{0,1\}^n \mapsto \{0,1\}$ and $f\colon \{0,1\}^n \mapsto \{0,1\}^n$, such that b is an hardcore predicate of f. You are **not** allowed to rely on assumptions (e.g., one-way functions exist).

   (b) Assuming OWFs (one-way functions) exist, prove that for any polynomial-time computable function $b\colon \{0,1\}^n \mapsto \{0,1\}$, there exists a OWF $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ such that b is **not** an hardcore predicate of f.

   (c) Given a function $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ and $\ell\colon \mathbb{N} \mapsto \mathbb{N}$, define $f^\ell\colon \{0,1\}^{\ell(n)n} \mapsto \{0,1\}^{\ell(n)n}$ as

   $$f^\ell(x_1, \ldots, x_{\ell(n)}) := (f(x_1) \ldots, f(x_{\ell(n)})),$$

   for any $n \in \mathbb{N}$ and $x_1, \ldots, x_{\ell(n)} \in \{0,1\}^n$. Similarly, given a function $b\colon \{0,1\}^n \mapsto \{0,1\}$, define $b^{\oplus \ell}\colon \{0,1\}^{\ell(n)n} \mapsto \{0,1\}$ as

   $$b^{\oplus \ell}(x_1, \ldots, x_{\ell(n)}) := b(x_1) \oplus b(x_2) \ldots \oplus b(x_{\ell(n)}).$$

   Given a OWF $f\colon \{0,1\}^n \mapsto \{0,1\}^n$, prove that there exists $\ell \in \operatorname{poly}$ and polynomial-time computable $b\colon \{0,1\}^{\ell(n)n} \mapsto \{0,1\}$, such that b is an hardcore predicate of f^ℓ.

   You might use the following fact:

   Definition 2 (weak hardcore predicate)**.** *A function* $b\colon \{0,1\}^{\ell(n)} \mapsto \{0,1\}$ *is an* δ-hardcore predicate *of* $f\colon \{0,1\}^{\ell(n)} \mapsto \{0,1\}^{m(n)}$*, where* $\delta\colon \mathbb{N} \mapsto [0, \frac{1}{2}]$*, if*

   $$\mathsf{Pr}_{x \leftarrow \{0,1\}^{\ell(n)}}[\mathsf{P}(1^n, f(x)) = b(x)] \leq 1 - \delta(n),$$

   for any PPT P *and large enough* n.

   Fact 3. *Let* $b\colon \{0,1\}^n \mapsto \{0,1\}$ *and* $f\colon \{0,1\}^n \mapsto \{0,1\}^n$*, be polynomial-time computable functions. Assume that* b *is a* $\frac{1}{p}$*-hardcore predicate of* f *for some* $p \in \operatorname{poly}$*, and let* $\ell(n) := \lceil n/p(n) \rceil$*. Then* $b^{\oplus \ell}$ *is an hardcore predicate of* f^ℓ*.*

[1] Recall that by $f\colon \{0,1\}^{\ell(n)} \mapsto \{0,1\}^{m(n)}$, we mean that f maps strings of length $\ell(n)$ to strings of length $m(n)$, for any $n \in \mathbb{N}$.

2. (a) Let $\mathcal{L} \in$ NP be a single witness language – for every $(x, w) \in R_{\mathcal{L}}$, there exists no $w' \neq w$ with $(x, w') \in R_{\mathcal{L}}$. Consider a relaxation of the CZKP (computational zero knowledge proof) notion we gave in class, which allows inefficient simulators (the simulator is not required to run in polynomial time). Is it true that under this relaxed definition, $\mathcal{L}$ has a single-message[2] CZKP?

   (b) Let (P, V) be a NIZK for a language $\mathcal{L}$. Consider the following two-message proof system:

   Protocol 4 $((\mathsf{P}', \mathsf{V}'))$**.**
   Common input: $x \in \{0,1\}^*$
   P'***'s private input:*** $w \in R_{\mathcal{L}}(x)$

   i. V' *sends* $r \leftarrow \{0,1\}^{\ell|x|}$ *to* P'*, where* $\ell(|x|)$ *is the CRS length used by* (P, V) *for statements of length* $|x|$*.*
   ii. P' *sends* $\pi \leftarrow \mathsf{P}(x, w, r)$ *to* V'*.*
   iii. V' *accepts iff* $\mathsf{V}(x, \pi, r)$ *does.*

   Is $(\mathsf{P}', \mathsf{V}')$ an IP (interactive proof system) for $\mathcal{L}$?

   (c) Is $(\mathsf{P}', \mathsf{V}')$, defined above, a CZKP (according to the standard definition) for $\mathcal{L}$? (you might assume that NP $\not\subseteq$ BPP)

[2]The protocol consists on a single message sent from the prover to the verifier.

(a) Show that a semantically-secure *public*-key encryption scheme, cannot have a deterministic encryption algorithm.[3]

(b) Recall the private-key encryption scheme we presented in class:

Construction 5.

- $\mathsf{G}(1^n)$*: output* $e \leftarrow \mathcal{F}_n$*,*
- $\mathsf{E}_e(m)$*: choose* $r \leftarrow \{0,1\}^n$ *and output* $(r, e(r) \oplus m)$
- $\mathsf{D}_e(r,c)$*: output* $e(r) \oplus c$

where $\mathcal{F}$ *is a (non-uniform) length-preserving PRF.*

Prove that the above scheme is private-key CPA secure. You can use the fact that the inefficient variant of Construction 5 where $\mathcal{F}_n$ is replaced with Π_n – the set of all functions from $\{0,1\}^n$ to $\{0,1\}^n$ – is CPA secure.

(c) Is it true that *any* existential unforgeable signature scheme (a signature scheme, according to the terminology used in class), is also *strong* existential unforgeable signature scheme? [4]

[3] An encryption algorithm is deterministic, if encrypting the same message twice, with the same encryption key, always yields the same ciphertext.

[4] Recall that a signature scheme is strong existential unforgeable, if it is hard for an attacker to output a pair (M, σ), s.t. σ is a valid signature for M, unless it has queried the signing oracle on M, and replied with σ.