Foundation of Cryptography (0368-4162-01), Spring 2014 Iftach Haitner

Final Exam

23.6.2014

Time Limit: 3 hours
Instructions:

- The exam is with open books — 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).

Good Luck!

1. Prove that the existence of existential unforgeable signature scheme implies the existence of one-way functions.

2. Let $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ and $b\colon \{0,1\}^n \mapsto \{0,1\}$ be efficient functions, and assume there exists an efficient algorithm P such that $\Pr_{x \leftarrow \{0,1\}^n}\left[\mathsf{P}(f(x), x_1) = b(x)\right] \geq \frac{1}{2} + \frac{1}{q(n)}$, for some $q \in \mathrm{poly}$.[1]

   (a) Can b be an hardcore predicate of f? (for some specific choice of f and b).

   (b) What would be the answer if b is defined by $b(x) = \langle x_{1,\ldots,n/2}, x_{n/2+1,\ldots,n}\rangle_2$ (i.e., the inner product of the first half of x with its second half).[2]

[1] x_i stands for the i'th bit of x.

[2] We assume here that f is only defined over *even* length inputs.

3. Let HAMILTONIAN be the $\mathcal{NP}$ language consists of all (undirected) graphs in which there exist an hamiltonian path (a path that visit all nodes in the graph without visiting any node twice). Consider the following protocol for proving membership in HAMILTONIAN.

   Let $\mathsf{Com} = (\mathsf{Snd}, \mathsf{Rcv})$ be a perfectly binding commitment.

   Given an n-node graph $G = ([n] = \{1, \ldots, n\}, E)$, let M_E be its $[n] \times [n]$ adjacency matrix (i.e., $M_E[i,j] = 1$ iff $(i,j) \in E$). Let Π_n be the set of all permutations over $[n]$, and given $\pi \in \Pi_n$, let $\pi(G) = ([n], \{(\pi(i), \pi(j)) \colon (i,j) \in E\})$.

   Protocol 1 ((P, V))**.**

   Common input: undirected graph $\mathsf{G} = ([n], E)$.

   P*'s input: an hamiltonian path* $C = (c_1, \ldots, c_n)$ *in* G.

   (a) P *chooses* $\pi \leftarrow \Pi_n$ *and sets* $G' = ([n], E') = \pi(G)$.

   (b) For each $(i,j) \in [n] \times [n]$*:*
   P *commits to* $M_{E'}[i,j]$ *using* Com*, with security parameter* 1^n.

   (c) V *sends* $b \leftarrow \{0,1\}$ *to* P.

   (d) If $b = 0$*:*

      i. P *sends* π *to* V *and decommits* all *entries of* $M_{E'}$.

      ii. V *accepts if all decommitment are valid, and* $M_{E'}$ *is the adjacency matrix of* $\pi(G)$.

   Otherwise (b=1):

      i. P *sends* $C' = (c'_1 = \pi(c_1), \ldots, c'_n = \pi(c_n))$ *to* V*, and decommits the values corresponds to the edges of* C' *in* E' *(i.e., the entries* $\{(c'_i, c'_{i+1})\}_{i \in [n-1]}$ *in* $M_{E'}$*).*

      ii. V *accepts if all decommitment are valid,* $C' = (c'_1, \ldots, c'_n)$ *is permutation of the elements of* $[n]$*, and all edges of* C' *appear in* $M_{E'}$*.*[3]

   Prove that for the language HAMILTONIAN, protocol (P, V) is:

   (a) Perfectly complete, and $\frac{1}{2}$ sound.

   (b) Zero knowledge against *honest* verifiers. On input G, your simulator running time should be in the *same order* (i.e., bounded by a constant factor of) as the running time of $(\mathsf{P}(\cdot), \mathsf{V})(G)$.

   (c) Zero knowledge against *arbitrary non-aborting* PPT verifiers.
   Given a verifier V^*, you might like to define an intermediate (inefficient) simulator, whose output is *statically close* to V^*'s output in $(\mathsf{P}(\cdot), \mathsf{V}^*)(G)$, and *computationally close* to the your final efficient simulator.

   For this question, it suffices to give only the *high level arguments* of the proofs. I.e., when arguing that violating a property of the protocol translates to violating a property of Com, no need to define the hybrid formally.

[3] $(c_i, c'_{i+1}) \in M_{E'}$ for all $i \in [n-1]$.