Problem set 6

January 19, 2017

Due: Feb 2 (optional)

- Please submit the handout in class, or email me, in case you write in LaTeX.

- Write clearly and shortly using sub claims if needed. The emphasize in most questions is on the proofs (no much point is writing a “solution” w/o proving its correctness).

- For Latex users, a solution example can be found in the course web site.

- It is ok to work in (small) groups, but please write the id list of your partners in the solution file, and each student should write her solution by herself (joint effort is only allowed in the “thinking phase”).

- The notation we use appears in the introduction part of the first lecture (Notation section).
1. Consider the following variant of construction 19 in Lecture 9 (Encryption Schemes).
   Let \((G_T, f, \text{Inv})\) be a (non-uniform) TDP, and let \(b\) be hardcore predicate for it.

   **Construction 1** (bit encryption).
   
   - \(G(1^n)\): output \((e, d) \leftarrow G_T(1^n)\).
   - \(E_e(m)\): choose \(r \leftarrow \{0, 1\}^n\) conditioned that \(b(r) = m\), and output \(f_e(r)\) (output \(m\) if no such \(r\) exists).
   - \(D_d(y)\): output \(b(\text{Inv}_d(y))\).

   (a) Describe a PPT \(E'\) such that \(\text{SD} \left( \left( (e, E'_e(m))_{(e, r) \leftarrow G(1^n)}, (e, E_e(m))_{(e, r) \leftarrow G(1^n)} \right), \leq \text{neg}(n) \right)\), for every \(m \in \{0, 1\}\).

   (b) Prove that \((G, E', D)\) has public-key indistinguishable encryptions for a multiple messages.

2. Assume we change Algorithm 30 in Lecture 8 so that \(j\) is Step 1 is always set to 0 (rather than being chosen at random). Is Claim 31 still true?