Foundation of Cryptography, Fall 2016 Beny Applebaum and Iftach Haitner

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, Inv) be a (non-uniform) TDP, and let b be hardcore predicate for it.

   Construction 1 (bit encryption)**.**

   - $\mathsf{G}(1^n)$*: output* $(e, d) \leftarrow \mathsf{G}_T(1^n)$.
   - $\mathsf{E}_e(m)$*: choose* $r \leftarrow \{0,1\}^n$ *conditioned that* $b(r) = m$*, and output* $f_e(r)$ *(output* m *if no such* r *exists).*
   - $\mathsf{D}_d(y)$*: output* $b(\mathrm{Inv}_d(y))$.

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

   (b) Prove that $(\mathsf{G}, \mathsf{E}', \mathsf{D})$ 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?