COMP-647B Advanced Cryptography

Problem set #3

due on ***Thursday March 29, 2007***

9. "Static" Interactive Hashing.

Let G be a subset of $\{0,1\}^n$, a set of "good" strings. The notion of a "good" string will be application dependent. If Alice and Bob honestly enter into an Interactive Hashing protocol so that Alice enforces that one of the two output strings is from G, then with probability $(|G|-1)/2^n$ the second string will also be an element of G by accident (assuming the second string is uniformly distributed among the other strings). My student George Savvides proved in his PhD thesis that even if Alice is dishonest and try her best to get both strings to be from G, her success probability is only a constant times more than the honest case $\leq 16\,|G|/2^n$. You may use this fact for free.

Remember the Naor protocol for bit commitment based on the existence of a pseudo-random bit generator. His construction used a generator from n-bit strings to 3n-bit strings. Let $e>1$ be any expansion factor and assume that you are given an e-generator from n-bit strings to en-bit strings. Show how you can use Interactive Hashing to construct a Bit Commitment scheme similar to Naor's directly from the e-generator. (you are not allowed to transform your e-generator into a e'-generator for $e' > e$)

10. BBCM, HILL and NOV…

Prove that the Generalized Privacy Amplification Theorem 3 of [BBCM95], and the left-over hash Lemma 4.8 of [HILL99] and Lemma 4.1 of [NOV06] are all equivalent statements.

11. Privacy Amplification/Left-over Hash VS Erasure Channel

Suppose Alice and Bob have access to a binary erasure channel with erasure probability ε, that is a channel such that on input b the output is b with probability $1-\varepsilon$ and a special erasure symbol Δ otherwise. The sender does not find out whether the output was b or Δ, while the receiver learns nothing about b when Δ is received. Let $\rho,\delta>0$ be positive real constants. Consider an $[n,\rho n,\delta n]$ linear error-correcting code C, i.e. a set of $2^{\rho n}$ codewords from $\{0,1\}^n$, such that $D(w,w')\geq\delta n$ for all pair of distinct codewords $w,w'\in C$. (the distance D(x,y) between two codewords x,y is the number of positions where they differ). Let $t := \delta n-\varepsilon n$ be a security parameter. A basic result of coding theory is the Singleton bound stating that if there exists an $[n,\rho n,\delta n]$ linear error-correcting code then $\rho+\delta<1$.

11.A Calculate the Renyi uncertainty $\mathbf{H_2}(w)$ of Bob, when Alice sends him a random codeword w through the erasure channel.

11.B Using **11.A** and the Privacy Amplification/Left-over Hash Lemma, show how Alice can use the erasure channel (with Bob) n times to commit to a string of size $\Theta(n)$. (Construct a BCSS)

12. Simplified Interactive Hashing

Remember that we saw in class that the interactive hashing protocol of NOVY is a gradual way for the receiver of disclosing a random string $u\in\{0,1\}^n$ and for the sender a gradual way of disclosing y and $y\oplus u$. Consider a simplification of the Interactive Hashing protocol in which u is revealed in a bit-by-bit fashion to the sender. Accordingly the sender discloses the bits of y, $y\oplus u$ in a bit-by-bit fashion to the receiver.

12.A Show that this is a special case of the NOVY protocol.

12.B Show that there exists a set G of "good" strings from $\{0,1\}^n$ of size $2^{\gamma n}$ with $\frac{1}{2} < \gamma < 1$, such that the probability for a dishonest sender to end up with $y\in G$ and $y\oplus u\in G$ is non negligeable. (i.e. this simplification is not secure in the so-called static case.)