CAS CS 548. Problem Set 2

Due 5 pm Friday, March 24, 2006, in the drop box near the CS office.

Problem 1. Consider the Boneh-Boyen selective-ID-secure IBE scheme (the scheme as presented in the paper is a HIBE scheme, but we will consider only one level of the hierarchy). This problem attempts to explain why it is hard to prove that the scheme is fully (as opposed to selective-ID) secure. Suppose the adversary could somehow, after seeing the public key $(P, \alpha P, Q, R)$, find a pair of values x, y such that $x = \log_{\alpha P}(yQ - R)$. Show then that the adversary could find an ID for which it could break the encryption scheme.

Problem 2. This problem asks you to make the connection between IBE and digital signatures more formal. Namely, show how, given an IBE scheme, to construct a digital signature scheme. Prove that the digital signature scheme you construct is secure in the usual sense (existentially unforgeable under adaptive chosen message attacks) assuming IBE is secure. Hint: the difficulty in this problem lies in designing the signature verification algorithm.

Problem 3. This is an exercise to get you a bit more comfortable with the random oracle model. Consider the following digital signature scheme: $\mathrm{Gen}(1^k)$ generates a trapdoor permutation f with domain $D = \{0,1\}^k$ and sets $\mathrm{pk} = f$, $\mathrm{sk} = f^{-1}$. Let $H : \{0,1\}^* \to \{0,1\}^k$ be a hash function. $\mathrm{Sig}_{\mathrm{sk}}(m) = f^{-1}(H(m))$ and $\mathrm{Ver}_{\mathrm{pk}}(m, \sigma)$ checks if $f(\sigma) = H(m)$. Prove that this is a secure digital signature scheme (assuming the hardness of inverting f) if H is modeled as a random oracle.