This problem set is due by the start of lecture on Tuesday, March 10. The problem set should be typed up in LaTeX and compiled into pdf. Please both bring in a physical copy and email to bwaters@gmail.com (for backup purposes). Please clearly indicate your collaborators for each problem. Or explicitly note if there were no collaborators. Note that the email address given is not one I check often and it is only used for backup. You should also keep your own problem set saved.

1. Show that one can build a secure “hash-and-sign” signature scheme from any secure IBE system. Assume that you are given any IBE system with algorithms: Setup, KeyGen, Encrypt, and Decrypt. Then: 1) Describe a signature system (i.e. describe 3 algorithms). 2) Prove it secure under the assumption that the IBE system is secure. You should use the definitions of security given in class. Note — since you might be given any IBE system you cannot rely on any particular construction. Your solution should not mention bilinear maps at all! You may assume that the message space for the IBE scheme is \{0, 1\}^\lambda, where \lambda is the security parameter.

2. Let’s consider two weaker notions of signature security and think how they might be useful for building our traditional strong notion. First, a weak signature scheme is one where the attacker tells the challenger all of the messages he wants signed before the attacker sees the verification key — the message the attacker forges on can still be dynamically chosen though. Second, a one-time signature scheme allows the attacker to only make one signing query. However, this can be chosen after seeing the public verification key.

While these two security properties seem to be weak, you should show that they surprisingly can be combined to produce a signature system of standard security. Assume you are given both a weak and a one-time signature scheme (for message space of arbitrary length). Show how to build a standard secure signature scheme.

Let (\text{Setup}_W, \text{Sign}_W, \text{Verify}_W) be the algorithms for the weak signature scheme and let (\text{Setup}_O, \text{Sign}_O, \text{Verify}_O) be the algorithms for the one time signature system.

First describe, your new system in terms of three algorithms. It should be built using the existing algorithms. Then give a proof of security.

3. Consider the following signature system that is intended to be secure under the RSA scheme in the standard model (i.e. no random oracles).

Setup: Let \( N = p \cdot q \) where \( p, q \) are two randomly chosen primes of equal length. Also choose random \( e < \phi(N) \) and \( u, h \in \mathbb{Z}_N \), where \( e \) is relatively prime to \( \phi(N) \). Let the message space be \( \{0, 1\}^\ell \) where \( \ell \) is less than the bit length of \( p, q \). The public key is \( N, e, u, h \) and the secret key is \( e^{-1} \mod \phi(N) \).

Sign(m) : Compute \( \sigma = (u^m h)^{1/e} \).
Verify(M, VK): Test if $\sigma = u^m h$.

Either prove this secure under the RSA assumption or show how to break it. Note that since you don’t know $\phi(N)$ you cannot compute $x^{a-1}$ for arbitrary $a, x$. This might apply either to an attack or a proof.

4. Several times we will need to encrypt a message to multiple recipients. Consider if I encrypt the same message $M$ to user 1 under $PK_1$ and user 2 under $PK_2$. (Assume the message spaces of the two encryption schemes are the same). Show that if both encryption systems are secure under our Chosen Plaintext Attack definition, that no attacker can break CPA security for when I encrypt the same message to both systems.

5. Bonus Question: I have not worked out the answer to this yet. This is the most challenging one, it is suggested that you start on the other problems first.

Let’s consider a new type of “geometrical” encryption system that is a generalization of the type of IBE systems we have considered. For encryption, suppose that you encrypt a message $M$ and tag it with a point $t \in \mathbb{Z}_p$. We can let $p$ be the order of the group used in a system. The key generation algorithm will take as input the master secret key and another point $x \in \mathbb{Z}_p$. Decryption will work if the user’s key has “identity” $x$ that is not equal to the ciphertext identity $t$. In some sense this is the opposite of IBE. I can only decrypt if I have a key identity not equal to the ciphertext identity.

First, provide a security definition. The definition may include discussion of $p$, but not of bilinear groups, since it should be a general definition. Next, design a system; you may use bilinear groups. Then prove it secure under the decisional Bilinear Diffie-Hellman assumption. You may prove it under a selective model where the ciphertext “identity” $t^*$ is decided by the attacker before he sees the system public parameters.

Now try to generalize the scheme. In the generalization the ciphertext will be associated with a point $(t_1, t_2)$ in a two dimensional space $\mathbb{Z}_p^2$. A private key is now associated with values $(x_1, x_2) \in \mathbb{Z}_p$. The decryption functionality should be that a user can decrypt a ciphertext to $t_1, t_2$ if and only if he has a key for subspace $(x_1, x_2)$ such that there does not exist a value $c \in \mathbb{Z}_p$ such that $(t_1, t_2) = (cx_1, cx_2)$. In other words $x_1, x_2$ defines a one dimensional subspace and a user can decrypt if the ciphertext point is outside of the key’s subspace. You should define a new security model, create a system and prove it selectively secure.