Assignment 3

Due: Tuesday April 25, 2006, in class.

Rules: This assignment should be done alone, without discussion with other students in the class. (Exception: Undergraduate students may work in pairs. You must however turn in individual writeups on which you name your collaborator.) You may of course use your course materiels, meaning your notes or the course notes. I encourage you not to refer to the literature either: one learns more by doing on one’s own. You are, however, allowed to consult papers we have referred to in class. You are not allowed to consult other papers or sources.

Note: Some words of warning. I have thought about this problem only to the extent that I feel it is plausible. I did not check all the details. I did this on purpose, because, as a step towards research, I want you to get used to tackling problems that are not guaranteed solvable. In solving the problem you will have to make decisions, for example with regard to how strong to make your definition. If you do not solve the problem, try tweaking it or relaxing the definition, or doing something that will give you some result. In any case write up what you got and, if you got stuck, say where and explain the problem you encountered. If I get stuck at the same place, you won’t lose credit. If you use a weak definition and I can do it with a strong one, you lose credit.

Let \( e: G_1 \times G_2 \to G_T \) be a bilinear map and let \( p \) be the common prime order of the groups. Let \( H \) be a hash function with range \( G_1 \). Consider the signature scheme where the secret key is \( sk = (g_1^s, g_2) \) and the public key is \( pk = (g_1, g_2^g, g_2^s) \) where \( g_1 \in_G G_1^*, g_2 \in_G G_2^* \) and \( s \in \mathbb{Z}_p \). The signing and verifying algorithms are as follows:

Algorithm \( \text{SGN}(sk, M) \):

\[
\begin{align*}
& r \leftarrow \mathbb{Z}_p \\
& A \leftarrow g_1^r H(M)^r \\
& B \leftarrow g_2^g \\
& \text{Return } (A, B)
\end{align*}
\]

Algorithm \( \text{VF}(pk, M, (A, B)) \):

\[
\begin{align*}
& \text{If } A \notin G_1 \text{ or } B \notin G_2 \text{ then return } 0 \\
& \text{If } e(A, g_2) = e(g_1, g_2^g) e(H(M), B) \text{ then return } 1 \\
& \text{Else return } 0
\end{align*}
\]

In the security analysis, you may assume \( H \) is a random oracle.

1. **[25 points]** Present a multisignature scheme based on the above base signature scheme. (That is, the signature of an individual signer in the multisignature scheme should be the same as in the base scheme.)

2. **[55 points]** Prove your multisignature scheme is secure if the CDH problem is hard. As part of this, you should present a definition of security for multisignatures, state a theorem involving a concrete security reduction, and prove your theorem.

3. **[5 points]** Do we want an isomorphism \( \psi: G_2 \to G_1 \)? Yes? No? Doesn’t matter?
4. [15 points] Compare this multisignature scheme to others we have studied. Does it have any advantages?