
Assignment 4

Due: Tuesday May 9, 2006, in class.

Rules: You may work with another student in the class, but not more, meaning the size of your group must be at most two. You must however write your solutions yourself, in your own words, and turn in individual writeups on which you name your partner. You may of course use your course materials, meaning your notes or the course notes. You may also use any CSE 207 materials. I encourage you not to refer to the literature: 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: As with the previous homework, I have thought about this problem only to the extent that I feel it is plausible. If you get stuck and feel it is not solvable in the stated form, try some combination of the following: weakening the goals, modifying the scheme, changing the assumptions, telling me about it.

Let $\mathbf{e}: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ be a bilinear map and let p be the common prime order of the groups. You may assume there is an efficiently computable isomorphism $\psi: \mathbb{G}_2 \rightarrow \mathbb{G}_1$. The Gap-BDH assumption states that the CBDH problem remains hard even given an oracle for the DBDH problem. Let H_1 be a hash function with range \mathbb{G}_1 and H_2 a hash function with range $\{0, 1\}^k$. Let $\mathcal{SE} = (\mathcal{K}, \mathcal{SE}, \mathcal{SD})$ be an IND-CCA secure symmetric encryption scheme whose key-generation algorithm returns a random k -bit string. Consider the variant of the BF-IBE scheme whose master key generation, user key generation and encryption algorithms work as follows:

Algorithm \mathcal{MK} $g_2 \xleftarrow{\$} \mathbb{G}_2^*$; $s \xleftarrow{\$} \mathbb{Z}_p$ $msk \leftarrow s$; $mpk \leftarrow (g_2, g_2^s)$ Return (mpk, msk)	Algorithm $\mathcal{UK}(msk, I)$ $sk(I) \leftarrow H_1(I)^s$ Return $sk(I)$	Algorithm $\mathcal{E}(mpk, I, M)$ $r \xleftarrow{\$} \mathbb{Z}_p$; $R \leftarrow g_2^r$ $K \leftarrow H_2(I, R, \mathbf{e}(H_1(I)^r, g_2^s))$ $C_s \xleftarrow{\$} \mathcal{SE}(K, M)$ $C \leftarrow (R, C_s)$ Return C
--	---	---

In the security analysis, you may assume H_1, H_2 are random oracles.

1. **[5 points]** Present a decryption algorithm for this scheme. It should take inputs $mpk, I, sk(I), C$ and return either a message or the symbol \perp .
2. **[5 points]** Recall some formalization of IND-CCA security of \mathcal{SE} to use below.
3. **[15 points]** Provide a definition of IND-CCA security of an IBE scheme.

4. **[15 points]** Formalize the Gap-BDH assumption.
 5. **[60 points]** Prove that this IBE scheme is IND-CCA secure in the RO model assuming Gap-BDH is hard and \mathcal{SE} is IND-CCA secure. Given an adversary A against the IBE scheme, you should define an adversary B against Gap-BDH and an adversary S against \mathcal{SE} such that the advantage of A is bounded above by a linear combination of the advantages of B and S , with the factor weighting the first being at most $O(q_c)$, where q_c is the number of CORRUPT queries that A makes.
-