LELEC2770 – Practical Sessions

Practical Session 4: Anonymous Credentials

1. Consider the different groups G_1, G_2, G_T of prime order q and a bilinear map $e : G_1 \times G_2 \leftarrow G_T$. Prove that if one has a polynomial time algorithm $\mathcal{A}$ that extracts the discrete logarithm in G_T, then the El Gamal encryption scheme is not semantically secure in G_1.

2. The verification algorithm of the Boneh-Boyen signature checks the following equality :

$$e(\sigma, \mathbf{a}^{\mathbf{m}} b^r c) \stackrel{?}{=} e(g, \hat{g})$$

   Consider the simpler case of $e(g, A) \stackrel{?}{=} T$, design a proof of knowledge of A. In order to make your proof as efficient as possible, keep in mind that computations are more costly in G_T than in G_2.

3. Consider a polynomial time algorithm $\mathcal{A}$ that, given B and T, produces A such that $e(A, B) = T$. Use $\mathcal{A}$ to forge a Boneh-Boyen signature.

4. Suppose that one of the attribute of $\mathbf{m} = (m_1, .., m_l)$ say m_1 is the birth year and consider the commitment $A := g^{m_1} h^r$. Getting access to some service provider requires the user to prove that he is older than 18 years old. How can we actually make such proof in zero-knowledge which means that the service provider learns only one bit of information? In practice, how can we perform such proof on the commitment $B := \mathbf{a}^{\mathbf{m}} b^r c$ of the Boneh-Boyen signature?

5. Consider the modified Camenish-Lysyanskaya signature scheme:

   - $vk = (N, \mathbf{a}, b)$,
   - in the signature algorithm $v = (\mathbf{a}^{\mathbf{m}} b^r)^{1/e} \mod N$,
   - and in the verification algorithm, one checks that $v^e \stackrel{?}{=} \mathbf{a}^{\mathbf{m}} b^r \mod N$.

   This modified version is not secure, show why.

6. In Figure 1 what happens if we use an encryption scheme instead of a commitment scheme?

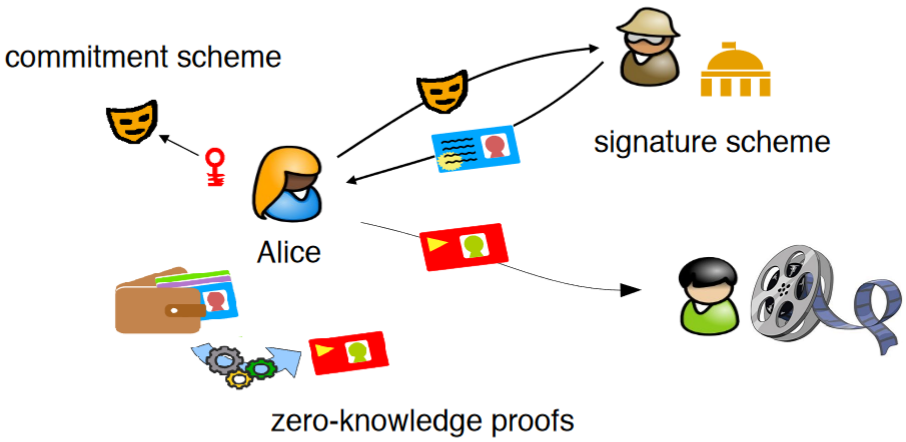

Figure 1: Anonymous Credentials