

Exercises “Anonymous Credentials II”

Exercise 1. Pedersen Commitment Scheme.

The discrete logarithm problem is to compute an integer x given g and y such that $y = g^x$ will hold. In the lecture we claimed that the Pedersen commitment scheme (i.e., the commitment to a value m is the group element $C = g^m h^r$, where r is chosen randomly) is computationally binding. Show that if there exists an algorithm that can break the binding property of the Pedersen commitment scheme, then there exists an algorithm that can solve the discrete logarithm problem.

Exercise 2. Off-Line E-Cash with Camenisch-Lysyanskaya Signatures

Try to design an *off-line* e-cash scheme, i.e., a scheme where the bank is not involved in the spending-transaction between the user and the merchant. The requirements of such a scheme are as follows:

1. A user shall be able to spend a coin anonymously once, i.e., when the merchant hands the coin to the bank for deposit, the bank shall not be able to tell which user the money originates from.
2. If the user spends the coin a second time with any merchant, the bank shall be able figure out the the coin was spent twice and identify the user.
3. Of course, the user shall be protected against merchant who try to deposit a coin twice

Hint:

- Embed secret values in the signature (aka coin) that the user obtains from the bank.
- Make use of the fact that if there are two unknown variables x and y , then given values a, b, c such that $a = b x + c y$ does not reveal any information about x and y , but given two set of such values allows one to solve the equation system, i.e., to determine x and y .