

## Exercises “Anonymous Credentials I”

### Exercise 1. Anonymous Credentials.

Come up with two use cases of anonymous credentials (so think of authentication with privacy requirements) and

1. Describe the requirements of the participants in terms of what information needs to be available to whom at what time.
2. How would you meet these requirements, given a digital signatures scheme, a public key encryption scheme and zero-knowledge proofs

Hint: Think of an electronic passport and a visit to a disco or of digital cash.

### Exercise 2. Zero Knowledge Protocols for Discrete Logarithms.

Show how and why the protocols denoted

1.  $PK\{(\alpha, \beta): u = g^{\beta} h^{\alpha}\}$
2.  $PK\{(\alpha, \beta): y = g^{\alpha} \wedge u = g^{\beta} h^{\alpha}\}$

are secure proofs of knowledge of the quantities  $\alpha$  and  $\beta$  (and, for the second one, why we can conclude that  $\alpha$  is the same integer in both term).