Advanced Topics on Privacy-Enhancing Technologies
CS-523
Anonymous Authentication Exercises

1 Zero-knowledge color-blindness

Alice has two pens. They are identical, except that one pen is red and the other blue. Bob is colorblind, so to him the pens look the same. Alice wants to convince Bob that she can distinguish these pens, without revealing to Bob which pen is red and which is blue. To this end, Alice and Bob run the following protocol:

1. (commitment) Alice shuffles the pens and gives them, in a specific order, to Bob. One pen for each hand.
2. (challenge) Bob hides the pens from Alice's view and either (a) swaps the pens, or (b) keeps each pen in the same hand. Each with probability $\frac{1}{2}$. Bob shows the pens to Alice again.
3. (response) Alice tells Bob whether he swaps the pens or not. Bob rejects if Alice's answer is wrong and accepts otherwise.

Prove that this protocol is *complete*, *sound*, and *zero-knowledge*. What is the soundness error?

2 Proving knowledge of a Pedersen commitment

Let $\mathbb{G}$ be a cyclic group of prime order q, generated by g. Let h be another random generator of $\mathbb{G}$.

1. Construct the Sigma protocol for proving knowledge of a Pedersen commitment $\mathsf{com} = g^x h^r$ to the value $x \in \mathbb{Z}_p$. What are the prover's secrets? What are the public values that both the prover and verifier know?
2. Prove completeness, special-soundness and honest-verifier zero-knowledge.
3. Apply the Fiat-Shamir heuristic to your protocol to obtain a non-interactive version.

3 Domain-specific pseudonyms

Consider a credential scheme with a single attribute – the users private key x – that is constructed using blind signatures. In this exercise, a credential then takes the form of a signatures σ on a commitments $C = g^x h^r$ where x is the user's private key.

In this exercise we will work with domain specific pseudonyms to ensure that users will always derive the same pseudonym for the same service provider (but pseudonyms between service providers are unlinkable). The pseudonym nym for a service provider at domain domain is computed as:

$$\mathsf{nym} = H(\mathsf{domain})^x$$

where $H : \{0,1\}^* \to \mathbb{G}$ maps strings to group elements.

Suppose a user wants to use her signature σ to convince a service provider that nym computed as before is her pseudonym. What protocol do the user and the service provider run? If you need to use a zero-knowledge proof, give both the high-level description, and the low level details.

4 What if verifiers are dishonest

The sigma protocols we constructed in the previous questions assume that the verifier is honest. What goes wrong if the verifier in question 2 is not honest. (Think about how you would construct a trace that cannot be easily simulated.) Could you extend the protocol to make it zero-knowledge even against malicious verifiers?