Privacy Enhancing Technologies FS2025
Exercise Sheet 2 (version 1)

Florian Tramèr

Problem 1: Conceptual Questions. For each of the following statements, say whether it is TRUE or FALSE. Write at most one sentence to justify your answer.

(a) If $\mathtt{P} = \mathtt{NP}$, then ZK-proofs exist for all $\mathtt{NP}$ languages.

(b) Let $\langle P, V \rangle$ be a zero-knowledge interactive protocol for some language. The protocol has perfect completeness and soundness error $1/3$. Which of the following are true:

i) A malicious verifier interacting with an honest prover will always accept a true statement.

ii) An honest verifier interacting with a malicious prover will "learn nothing" besides the statement's validity.

(c) In the standard model (without random oracles), there exist non-interactive zero-knowledge proofs for languages in P.

Problem 2: Composing ZK Protocols. Consider the ZK protocol for Hamiltonian Cycle from the lecture. Recall that this protocol has perfect completeness and soundness error $1/2$. We now want to amplify soundness to get a soundness error of $1/2^\lambda$ by running the protocol λ times. The verifier will accept if and only if all λ instances accept.

(a) We first consider running the protocol λ times in *sequence*. Show that the resulting protocol is still zero-knowledge.

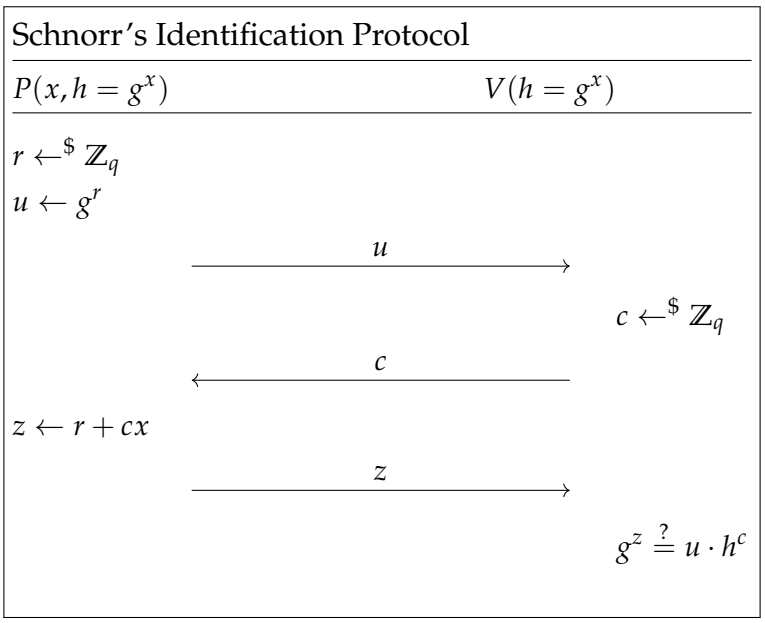
(b) We now consider running the protocol λ times in *parallel*. Can you still show that the resulting protocol is zero-knowledge? Why or why not?

Note that it can be shown that the *proof of knowledge* property is preserved under both types of composition strategies. We do not show this here.

(c) Show that *Honest-verifier* zero-knowledge is preserved under parallel composition for this protocol (in fact, honest-verifier zero-knowledge is preserved under parallel composition for any Sigma protocol).

Problem 3: Schnorr's Identification Protocol Let $\mathbb{G}$ be a group of prime order q, and let g be a generator of $\mathbb{G}$. Suppose that a prover wants to prove it knows the discrete logarithm x of some element $h = g^x \in \mathbb{G}$.

The following protocol, due to Schnorr, achieves this:



(a) Show that the protocol has perfect completeness.

(b) Show that the protocol is honest-verifier zero-knowledge. [**Hint:** Simulate the protocol "in reverse" by first picking z and c uniformly at random, and then picking u. Argue that the resulting transcript is distributed *identically* to the verifier's view in the real protocol.]

(c) Show that the protocol is a proof of knowledge of x. For your proof, you can assume a prover P^* that can successfully respond to any challenge from the verifier. Show that there exists an extractor E that extracts x from P^* with probability $1 - 1/q$.

Hint: Recall how to break a discrete log from the lecture on commitments.

Problem 4: Sigma Protocol for Circuit Satisfiability Let CSAT be the language of satisfiable Boolean circuits[1] :

$$\text{CSAT} = \{C \colon \{0,1\}^n \to \{0,1\} \mid n \in \mathbb{N},\ \exists (x_1, \ldots, x_n) \in \{0,1\}^n \text{ such that } C(x_1, \ldots, x_n) = 1\}\ .$$

Let $\texttt{Commit} \colon \{0,1\} \times \mathcal{R} \to \mathcal{C}$ be a perfectly-binding and computationally-hiding commitment scheme with message space $\{0,1\}$, randomness space $\mathcal{R}$, and commitment space $\mathcal{C}$. Suppose that there exist Sigma protocols $(P_{\text{XOR}}, V_{\text{XOR}})$ and $(P_{\text{AND}}, V_{\text{AND}})$ for languages L_{XOR} and L_{AND}, respectively, where:

$$L_{\text{XOR}} = \left\{ (c_1, c_2, c_3) \in \mathcal{C}^3 \;\middle|\; \begin{array}{c} \exists (m_1, m_2, m_3) \in \{0,1\}^3, (r_1, r_2, r_3) \in \mathcal{R}^3 \text{ such that} \\ \forall i \in \{1,2,3\}\ c_i = \texttt{Commit}(m_i; r_i) \text{ and } m_1 \oplus m_2 = m_3 \end{array} \right\}$$

$$L_{\text{AND}} = \left\{ (c_1, c_2, c_3) \in \mathcal{C}^3 \;\middle|\; \begin{array}{c} \exists (m_1, m_2, m_3) \in \{0,1\}^3, (r_1, r_2, r_3) \in \mathcal{R}^3 \text{ such that} \\ \forall i \in \{1,2,3\}\ c_i = \texttt{Commit}(m_i; r_i) \text{ and } m_1 \wedge m_2 = m_3 \end{array} \right\}.$$

The prover shows that (c_1, c_2, c_3) are commitments to some bits m_1, m_2, m_3 such that $m_1 \oplus m_2 = m_3$ for XOR gates and $m_1 \wedge m_2 = m_3$ for AND gates.

(a) Describe a Sigma protocol for CSAT that runs N parallel instances of the above Sigma protocol for either XOR or AND, where N is the number of gates in the circuit.

[1] You can assume without loss of generality that a Boolean circuit consists of only XOR and AND gates.

(b) Prove that your protocol is sound. In particular, show that if the prover can convince the verifier that an unsatisfiable circuit is satisfiable with non-negligible probability, then it must have broken the soundness of one of the underlying Sigma protocols.

(c) Describe a simulator `Sim` that simulates the verifier's view in the protocol. Argue (informally) that your protocol is honest-verifier zero-knowledge.