Privacy Enhancing Technologies FS2025
Exercise Sheet 3 (version 1.1)

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 an interactive proof system has soundness error greater than $\frac{1}{3}$, then it cannot be a proof of knowledge with knowledge error less than $\frac{1}{3}$.

(b) In the standard model (without a random oracle), we can build NIZKs for $\mathtt{NP}$ languages.

(c) The polynomial $f(X) = 2X^2 + 4X$ has at most two roots in $\mathbb{Z}_6$.

(d) The Fiat-Shamir transform applied to a Sigma protocol yields a NIZK with statistical zero-knowledge.

Problem 2: More on Schnorr. Recall Schnorr's identification protocol from the previous homework:

Schnorr's Identification Protocol		
$P(x, h = g^x)$		$V(h = g^x)$
$r \xleftarrow{\$} \mathbb{Z}_q$ $u \leftarrow g^r$		
	$\xrightarrow{\quad u \quad}$	
		$c \xleftarrow{\$} \mathbb{Z}_q$
	$\xleftarrow{\quad c \quad}$	
$z \leftarrow r + cx$		
	$\xrightarrow{\quad z \quad}$	
		$g^z \stackrel{?}{=} u \cdot h^c$

(a) Build a NIZK from this protocol in the random oracle model. What is the proof π?

(b) Write down the verifier algorithm $\mathcal{V}(\pi, h)$ for the NIZK.

(c) What is the soundness error of this NIZK? Assume that the prover makes at most Q queries to the random oracle.

(d) Suppose a verifier V was convinced by a NIZK proof for some statement x. Can they then go on to convince another verifier V' of the same statement x? What about if V was convinced by an interactive ZK proof for the same statement x?

Problem 3: Understanding Fiat-Shamir. Let Σ be a Sigma protocol.

(a) Show that if Σ has soundness error $1/2$, then applying the Fiat-Shamir transform *directly* to Σ yields a non-interactive zero-knowledge proof (NIZK) that is unsound. In particular, demonstrate an efficient attack that breaks the soundness of this NIZK.

(b) Use Σ to construct a Sigma protocol Σ' that has negligible soundness error, and prove that its soundness error is negligible. Then explain how to apply the Fiat-Shamir transform to this protocol.

Problem 4: SNARGs in the Random Oracle Model. In this problem, we will show how to leverage probabilistically-checkable proofs (PCPs) to construct a succinct non-interactive argument (SNARG) in the random oracle model. We will rely on the following adaptation of the famous PCP theorem:

> **Theorem 1** (PCP). Let L be an $\texttt{NP}$ language. There exists two efficient algorithms $(\mathcal{P}, \mathcal{V})$ defined as follows:
>
> - The prover algorithm $\mathcal{P}$ is a deterministic algorithm that takes as input a statement $x \in \{0,1\}^n$, a witness $w \in \{0,1\}^h$ and outputs a bitstring $\pi \in \{0,1\}^m$, where $h, m = \mathsf{poly}(n)$. We refer to π as the proof string.
> - The verifier algorithm $\mathcal{V}^\pi$ is a *randomized* algorithm that takes as input a statement $x \in \{0,1\}^n$ and has oracle access to a proof string $\pi \in \{0,1\}^m$. The verifier reads $O(1)$ bits of π. The verifier chooses the bits it reads *nonadaptively* (i.e., they can depend on the statement x, but *not* on the values of any bit in π).
>
> Moreover, $(\mathcal{P}, \mathcal{V})$ satisfy the following properties:
>
> - **Completeness:** For all $x \in L$, if w is a valid witness for x, then
>
> $$\Pr[\mathcal{V}^\pi(x) = 1 \colon \pi \leftarrow \mathcal{P}(x, w)] = 1.$$
>
> - **Soundness:** If $x \notin L$, then for all $\pi \in \{0,1\}^m$,
>
> $$\Pr[\mathcal{V}^\pi(x) = 1] \leq 1/2.$$

Recall that in homework 1, we constructed a computationally-binding vector commitment scheme with the following syntax:

> - $\texttt{Commit}(x) \to c$: The commitment algorithm takes a message $x \in \{0,1\}^n$ and outputs a succinct commitment $c \in \{0,1\}^\lambda$.
> - $\texttt{Open}(c, i, x_i) \to \sigma$: The open algorithm takes a bit $x_i \in \{0,1\}$, a commitment $c \in \{0,1\}^\lambda$, and an index $i \in [n]$, and outputs a proof σ of length $O(\lambda \cdot \log n)$.
> - $\texttt{Verify}(c, i, x_i, \sigma) \to \{0,1\}$: The verification algorithm takes a commitment $c \in \{0,1\}^\lambda$, an index $i \in [n]$, a value $x_i \in \{0,1\}$, and a proof σ, and outputs a bit.

(a) Let L be an $\texttt{NP}$ language (with statements of length m). Show how to construct a 3-round succinct argument system for L using your commitment scheme. Specifically, your argument system should satisfy perfect completeness, have soundness error $\mathsf{negl}(\lambda)$ against computationally-bounded provers, and the total communication complexity between the prover and the verifier should be $\mathsf{poly}(\lambda, \log m)$. In particular, the communication complexity scales *polylogarithmically* with the length of the $\texttt{NP}$ statement. **[Hint:**

Use the PCP theorem.]

(b) Explain briefly how to convert your succinct argument from Part (a) into a SNARG in the random oracle model.