CS 395T: Topics in Cryptography **Spring 2024**

Exercise Set 4

Due: March 19, 2024 at 11:59pm (Submit on Gradescope) **Instructor:** David Wu

Instructions. You **must** typeset your solution in LaTeX using the provided template:

https://www.cs.utexas.edu/~dwu4/courses/sp24/static/homework.tex

You must submit your problem set via Gradescope (accessible through Canvas).

Collaboration Policy. You may discuss your general approach with other students, but you may not share written documents. You should not search online for solutions to these problems. If you do consult external sources, you must cite them in your submission. You must include the names of all of your collaborators with your submission. Refer to the official course policies for the full details.

Problem 1: NIZKs with a Subverted CRS [20 points]. In the Groth-Ostrovsky-Sahai NIZK scheme presented in class, the common reference string consists of

$$\mathsf{crs} = \big((\mathbb{G}, \mathbb{G}_T, e), N, g, h\big),$$

where $(\mathbb{G}, \mathbb{G}_T, e)$ is a pairing group of composite-order $N = pq$, g is a generator of $\mathbb{G}$, and $h \xleftarrow{R} \mathbb{G}_q$, where $\mathbb{G}_q$ is the subgroup of $\mathbb{G}$ of order q. The key building block in the Groth-Ostrovsky-Sahai construction is a way to prove in zero-knowledge that a commitment $c = g^m h^r \in \mathbb{G}$ is a commitment to a message $m \in \{0,1\}$. As shown in class, the proof in this case is the tuple

$$\pi = (\pi_1, \pi_2, \pi_3) = \big(h^\alpha, (g^{2m-1} h^r)^{\alpha^{-1} r}, g^\alpha\big),$$

where $\alpha \xleftarrow{R} \mathbb{Z}_N$. The verifier accepts if the following holds:

$$e(g, \pi_1) = e(h, \pi_3) \quad \text{and} \quad e(c, cg^{-1}) = e(\pi_1, \pi_2),$$

where $g, h \in \mathbb{G}$ are the components in the CRS. In this problem, we will show that security of this scheme critically relies on the assumption that the CRS is *honestly* generated. Specifically, your goal is to describe an algorithm that generates a "subverted CRS" that allows the prover to convince the verifier of *false* statements. Importantly, the "subverted CRS" should look computationally indistinguishable from a real CRS (namely, an honest user should not be able to detect that anything went wrong). Using the subverted CRS, you will then show that the malicious prover can produce a commitment $c \in \mathbb{G}$, randomness $r \in \mathbb{Z}_N$ and a proof $\pi = (\pi_1, \pi_2, \pi_3)$ such that the following hold:

$$c = g^2 h^r \quad \text{and} \quad e(g, \pi_1) = e(h, \pi_3) \quad \text{and} \quad e(c, cg^{-1}) = e(\pi_1, \pi_2). \tag{1}$$

Namely, even though the prover *opened* the commitment to the value 2, it is nonetheless able to also produce a proof that c is a commitment to a 0/1 value. This can be extended to break soundness of the NIZK as a whole. Note that the subverted CRS should remain indistinguishable from the real CRS even *given* the commitment c and the opening r.

(a) Describe an efficient algorithm for constructing a subverted CRS that allows a malicious prover to break soundness. The subverted CRS should be computationally indistinguishable from the real CRS.

(b) Explain (informally) why your subverted CRS is computationally indistinguishable from a real CRS. (Depending on your construction, you may be able to answer this in one sentence.)

(c) Show how the malicious prover can efficiently come up with (c, r, π) that satisfy Eq. (1) with respect to the subverted CRS.

Optional Feedback. Please answer the following *optional* questions to help design future exercise sets. You do not need to answer these questions. However, we do encourage you to provide us feedback on how to improve the course experience.

(a) How long did you spend on this exercise set?

(b) Do you have any feedback for this exercise set?

(c) Do you have any feedback on the course so far?

(d) Are there specific topics that you are interested in seeing in this course?

Challenge Problem: Groth-Ostrovsky-Sahai in Prime-Order Groups [Optional]. Show how to construct an analog of the Groth-Ostrovsky-Sahai NIZK scheme in prime-order pairing groups. For security, you should use the 2-Lin assumption. For any $k \in \mathbb{N}$, the k-Lin assumption states that $\left(g^{\mathbf{M}}, g^{\mathbf{Mv}}\right)$ is computationally indistinguishable from $\left(g^{\mathbf{M}}, g^{\mathbf{u}}\right)$, where

$$\mathbf{M} = \begin{bmatrix} r_1 & & & \\ & r_2 & & \\ & & \ddots & \\ & & & r_k \\ 1 & 1 & \cdots & 1 \end{bmatrix} \in \mathbb{Z}_p^{(k+1)\times k},$$

and $r_1, \ldots, r_k \xleftarrow{R} \mathbb{Z}_p$, $\mathbf{v} \xleftarrow{R} \mathbb{Z}_p^k$, and $\mathbf{u} \xleftarrow{R} \mathbb{Z}_p^{k+1}$. Observe that the special case where $k = 1$ coincides with the DDH assumption. For larger k, this assumption is *weaker* than the DDH assumption. Show how to adapt your construction so soundness holds even if the adversary gets to choose the CRS (i.e., defend against the attack developed in the previous problem). The latter approach can be realized by having the prover choose two *correlated* common reference strings (which the verifier can validate). Your resulting construction will no longer be zero-knowledge, but will satisfy a weaker property of *witness indistinguishability*.

Challenge Problem: Functional Commitments for all Circuits [Optional]. Show how to adapt the Choudhuri-Jain-Jin RAM delegation scheme to obtain a functional commitment scheme for all circuits. Prove the security of your scheme. For this problem, you will need to adapt the proof strategy from the Choudhuri-Jain-Jin construction.