Zero-Knowledge Proofs
Exercise 13 (graded)

Submission Deadline: 15/12/2022, 23:59 CEST

Note: Solutions must be typeset in LaTeX. Make sure to name the pdf file of your solutions in the following format:

"*<Legi Number>_13.pdf*"

13.1 Non-Interactive Shuffle Proofs (20 marks)

Recall the setup algorithm for the Boneh-Goh-Nissim cryptosystem

- $\mathsf{Setup}\left(1^\lambda, t\right) \to pp$: Sample two large distinct primes p and q, cyclic groups $\mathbb{G}, \mathbb{G}_T$ of order $n = pq$, and a generator G of $\mathbb{G}$, with a non-degenerate bilinear map $e\colon \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, corresponding to the Type 1 setting.
  If $t = \texttt{Hiding}$, sample $s \leftarrow \mathbb{Z}_n^*$. Set $H = s \cdot G$.
  If $t = \texttt{Binding}$, sample $s \leftarrow \mathbb{Z}_n^*$. Set $H = sp \cdot G$.
  Output $pp = (e, \mathbb{G}, \mathbb{G}_T, G, H, n)$.

Let $\bar{A}_0 \neq \bar{A}_1$ and $\bar{A}_0' \neq \bar{A}_1'$ lie in $\mathbb{G}$. We say that $\bar{A}_0', \bar{A}_1'$ are a *rerandomised shuffle* of $\bar{A}_0, \bar{A}_1$ with respect to $b \in \{0, 1\}$, $r_0, r_1 \in \mathbb{Z}_n$ if $\bar{A}_0' = \bar{A}_b + r_b \cdot H$ and $\bar{A}_1' = \bar{A}_{1-b} + r_{1-b} \cdot H$.

a) Consider a setup with $t = \texttt{Hiding}$. Let $\bar{A}_0', \bar{A}_1'$ be a rerandomised shuffle of $\bar{A}_0, \bar{A}_1$ with respect to $b \in \{0, 1\}$, $r_0, r_1 \in \mathbb{Z}_n$. Let $r \in \mathbb{Z}_n$ and $A = b \cdot G + r \cdot H$.
Give explicit expressions for the unique values of $\Pi_0, \Pi_1 \in \mathbb{G}$ which satisfy the following equations, writing your answers in terms of $\bar{A}_0, \bar{A}_1, b, r_0, r_1, r, G$ and H.

$$e(\bar{A}_0, G - A) + e(\bar{A}_1, A) = e(\bar{A}_0', G) + e(\Pi_0, H) \ ,$$
$$e(\bar{A}_0, A) + e(\bar{A}_1, G - A) = e(\bar{A}_1', G) + e(\Pi_1, H) \ .$$

[2 marks]

Consider the following non-interactive proof system:

Inputs: The prover P receives CRS pp, instance $x := (\bar{A}_0, \bar{A}_1, \bar{A}_0', \bar{A}_1') \in \mathbb{G}^4$ with $\bar{A}_0 \neq \bar{A}_1$ and $\bar{A}_0' \neq \bar{A}_1'$, and witness $w := (r_0, r_1, b) \in \mathbb{Z}_n^2 \times \{0, 1\}$ as input. The verifier V receives pp and x.

Prover algorithm:

- Sample $r \leftarrow \mathbb{Z}_n$ and compute $A := b \cdot G + r \cdot H \in \mathbb{G}$.
- Compute $\Pi_0, \Pi_1 \in \mathbb{G}$ as in part a).
- Compute $\Pi_2 := (2b - 1)r \cdot G + r^2 \cdot H \in \mathbb{G}$.
- For each $i = 0, 1, 2$, sample $\rho_i \leftarrow \mathbb{Z}_n^*$, and compute

$$\pi_i := \rho_i^{-1} \cdot \Pi_i \ , \qquad \hat{\pi}_i := \rho_i \cdot H \ , \qquad \tilde{\pi}_i := \rho_i \cdot G \ .$$

- Output $(A, (\pi_i, \hat{\pi}_i, \tilde{\pi}_i)_{i=0,1,2}) \in \mathbb{G}^{10}$.

Verifier algorithm: Output 1 if and only if all of the following checks pass.

$$
\begin{aligned}
e(\bar{A}_0, G - A) + e(\bar{A}_1, A) &= e(\bar{A}'_0, G) + e(\pi_0, \hat{\pi}_0) \ , & e(G, \hat{\pi}_0) &= e(\tilde{\pi}_0, H) \ , \\
e(\bar{A}_0, A) + e(\bar{A}_1, G - A) &= e(\bar{A}'_1, G) + e(\pi_1, \hat{\pi}_1) \ , & e(G, \hat{\pi}_1) &= e(\tilde{\pi}_1, H) \ , \\
e(A, A - G) &= e(\pi_2, \hat{\pi}_2) \ , & e(G, \hat{\pi}_2) &= e(\tilde{\pi}_2, H) \ .
\end{aligned}
$$

b) Show that the verifier always accepts proofs produced by the honest prover when $\bar{A}'_0, \bar{A}'_1$ are a rerandomised shuffle of $\bar{A}_0, \bar{A}_1$ with respect to $b \in \{0, 1\}$, $r_0, r_1 \in \mathbb{Z}_n$. [4 marks]

c) Assume $t = \texttt{Binding}$. Show that if there exist $(A, (\pi_i, \hat{\pi}_i, \tilde{\pi}_i)_{i=0,1,2}) \in \mathbb{G}^{10}$ satisfying all of the verification checks, then there exist $b \in \{0, 1\}$, $r_0, r_1 \in \mathbb{Z}_n$ such that $\bar{A}'_0, \bar{A}'_1$ are a rerandomised shuffle of $\bar{A}_0, \bar{A}_1$ with respect to b, r_0 and r_1. You may not assume without justification that $(A, (\pi_i, \hat{\pi}_i, \tilde{\pi}_i)_{i=0,1,2}) \in \mathbb{G}^{10}$ are of the form produced by the honest prover algorithm. [7 marks]

d) Assume $t = \texttt{Hiding}$ and consider a trapdoor setup algorithm which additionally outputs s. Show that the protocol satisfies adaptive zero-knowledge with respect to this setup algorithm. [6 marks]

e) Describe an efficient algorithm which, given pp, x and an accepting proof $(A, (\pi_i, \hat{\pi}_i, \tilde{\pi}_i)_{i=0,1,2}) \in \mathbb{G}^{10}$ as input, *but not the witness*, produces a new accepting proof. [1 mark]