CS 276: Homework 10

Due Date: Friday December 13th, 2024 at 8:59pm via Gradescope

1 Succinct Arguments from Folding

Succinct argument systems are a valuable tool to compress a long witness into a short proof of the same statement. In recent years, folding has become a popular technique to construct succinct argument systems. Each iteration of the folding algorithm halves the length of the witness, and after $\log |w|$ iterations, the witness is constant-sized and can be published directly.

In this homework, we will use folding to succinctly prove that the inner product of two long vectors is equal to the claimed value. Crucially, the communication complexity of the protocol is $\mathsf{poly}\log n$, where n is the length of each vector, so it is more communication-efficient than publishing the two vectors directly. You are asked to prove lemma 1.4, which is a form of special soundness used in the proof of knowledge soundness.

1.1 Preliminaries

Let $\mathbb{G}$ be a cryptographic group of prime order p, where $\frac{1}{p} = \mathsf{negl}(\lambda)$. Let $n \in \mathbb{N}$ be a power of 2. For any vector $\mathbf{g}$ with n components and for any $i \in [n]$, let $\mathbf{g}_{[i]} = (g_1, \ldots, g_i)$, let $\mathbf{g}_L = (g_1, \ldots, g_{\frac{n}{2}})$, and let $\mathbf{g}_R = (g_{\frac{n}{2}+1}, \ldots, g_n)$.

Let us define four vectors $\mathbf{g} = (g_1, \ldots, g_n) \in \mathbb{G}^n$, $\mathbf{h} = (h_1, \ldots, h_n) \in \mathbb{G}^n$, $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{Z}_p^n$, and $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{Z}_p^n$. Let the inner product of $\mathbf{a}, \mathbf{b}$ be $\langle \mathbf{a}, \mathbf{b} \rangle = \sum_{i \in [n]} a_i \cdot b_i$, and let the component-wise product of $\mathbf{g}, \mathbf{h}$ be $\mathbf{g} * \mathbf{h} = (g_1 \cdot h_1, \ldots, g_n \cdot h_n)$. Also, let $\mathbf{g}^{\mathbf{a}} = \prod_{i \in [n]} g_i^{a_i}$.

Let us make the following hardness assumption, which is a variant of the discrete log assumption.

Definition 1.1 (Discrete Log Relation Assumption) *For any PPT adversary $\mathcal{A}$ and any $n \in \mathbb{N}$, the probability that $\mathcal{A}$ wins the following game is $\mathsf{negl}(\lambda)$.*

1. *Sample $(\mathbf{g}, \mathbf{h}, u) \xleftarrow{\$} \mathbb{G}^n \times \mathbb{G}^n \times \mathbb{G}$.*
2. *$\mathcal{A}(\mathbf{g}, \mathbf{h}, u)$ outputs $(\mathbf{a}, \mathbf{b}, c) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^n \times \mathbb{Z}_p$.*
3. *$\mathcal{A}$ wins if $\mathbf{g}^{\mathbf{a}} \cdot \mathbf{h}^{\mathbf{b}} \cdot u^c = 1$ and $(\mathbf{a}, \mathbf{b}, c) \neq \mathbf{0}$. $\mathcal{A}$ loses otherwise.*

The Inner Product Language Given a commitment P and a scalar c, the statement being proved is that there is some witness $(\mathbf{a}, \mathbf{b})$ – committed to by P – for which $c = \langle \mathbf{a}, \mathbf{b} \rangle$. Now we will state this more formally.

The following *public parameters* are sampled beforehand: $(\mathbf{g}, \mathbf{h}, u) \xleftarrow{\$} \mathbb{G}^n \times \mathbb{G}^n \times \mathbb{G}$. Next, an *instance* of the language is any tuple $(P, c) \in \mathbb{G} \times \mathbb{Z}_p$ such that there exists a *witness* $(\mathbf{a}, \mathbf{b}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^n$ such that $c = \langle \mathbf{a}, \mathbf{b} \rangle$ and $P = \mathbf{g}^{\mathbf{a}} \cdot \mathbf{h}^{\mathbf{b}}$. We can view P as a binding commitment to $(\mathbf{a}, \mathbf{b})$.

1.2 The Protocol

The following protocol Π is a succinct argument system for the inner product language defined above.

1. **Inputs:** The verifier's input is $(\mathbf{g}, \mathbf{h}, u, P, c)$, and the prover's input is the verifier's input as well as $(\mathbf{a}, \mathbf{b})$.
2. **Preprocessing:**
   (a) The verifier samples $x \xleftarrow{\$} \mathbb{Z}_p \backslash \{0\}$ and sends it to the prover.
   (b) The prover and verifier each compute $u' = u^x$ and $P' = P \cdot u^{x \cdot c}$.
3. **Folding:** Let n be the number of components of $\mathbf{g}$, and let n be a power of 2. If $n = 1$, then skip to the **verification** step. Otherwise, for each $i \in [\lg n]$, do the following:
   (a) The prover computes the following:
   $$L = \mathbf{g}_R^{\mathbf{a}_L} \cdot \mathbf{h}_L^{\mathbf{b}_R} \cdot u'^{\langle \mathbf{a}_L, \mathbf{b}_R \rangle}$$
   $$R = \mathbf{g}_L^{\mathbf{a}_R} \cdot \mathbf{h}_R^{\mathbf{b}_L} \cdot u'^{\langle \mathbf{a}_R, \mathbf{b}_L \rangle}$$
   and sends (L, R) to the verifier.
   (b) The verifier samples $y \xleftarrow{\$} \mathbb{Z}_p \backslash \{0\}$ and sends y to the prover.
   (c) The prover and verifier each compute the following:
   $$\mathbf{g} \leftarrow \mathbf{g}_L^{y^{-1}} * \mathbf{g}_R^{y}$$
   $$\mathbf{h} \leftarrow \mathbf{h}_L^{y} * \mathbf{h}_R^{y^{-1}}$$
   $$P' \leftarrow P' \cdot L^{y^2} \cdot R^{y^{-2}}$$
   (d) The prover additionally computes the following:
   $$\mathbf{a} \leftarrow \mathbf{a}_L \cdot y + \mathbf{a}_R \cdot y^{-1}$$
   $$\mathbf{b} \leftarrow \mathbf{b}_L \cdot y^{-1} + \mathbf{b}_R \cdot y$$
   Note that each iteration of folding halves the length of $\mathbf{g}, \mathbf{h}, \mathbf{a}, \mathbf{b}$.
4. **Verification**
   (a) The prover sends $(\mathbf{a}, \mathbf{b})$ to the verifier. *By this time,* $\mathbf{g}, \mathbf{h}, \mathbf{a}, \mathbf{b}$ *are scalars.*
   (b) The verifier checks whether:
   $$P' = \mathbf{g}^{\mathbf{a}} \cdot \mathbf{h}^{\mathbf{b}} \cdot u'^{\langle \mathbf{a}, \mathbf{b} \rangle}$$
   The verifier outputs 1 (accept) if the check passes and 0 (reject) if not.

1.3 Knowledge Soundness

Π satisfies knowledge soundness, assuming the discrete log relation problem is hard (def. 1.1). The proof of knowledge soundness is somewhat involved, so we'll walk through the proof sketch and just ask you to prove a core lemma, which is stated in lemma 1.4 below.

Definition 1.2 (Knowledge Soundness) *There exists an extractor E that runs in expected polynomial time such that for any $(P, c) \in \mathbb{G} \times \mathbb{Z}_p$ and any PPT adversarial prover $\mathcal{P}^*$, if $\Pr[\langle \mathcal{P}^*, \mathcal{V}\rangle(P, c) \to \mathsf{accept}] = \mathsf{nonnegl}(\lambda)$, then $\Pr[c = \langle \mathbf{a}, \mathbf{b}\rangle \wedge P = \mathbf{g}^{\mathbf{a}} \cdot \mathbf{h}^{\mathbf{b}} : (\mathbf{a}, \mathbf{b}) \leftarrow E^{\mathcal{P}^*}] = \mathsf{nonnegl}(\lambda)$ as well.*

Theorem 1.3 *If the discrete log relation assumption holds (def. 1.1), then Π satisfies knowledge soundness (def. 1.2).*

Proof Sketch. Let us run Π with $n = 2$ and public inputs $(\mathbf{g}, \mathbf{h}, u, P, c)$. An accepting transcript for the protocol is a tuple $\mathsf{tr} := (x, L, R, y, \mathbf{a}', \mathbf{b}')$ for which

$$P \cdot u^{x\cdot c} \cdot L^{y^2} \cdot R^{y^{-2}} = \left(\mathbf{g}_L^{y^{-1}} * \mathbf{g}_R^{y}\right)^{\mathbf{a}'} \cdot \left(\mathbf{h}_L^{y} * \mathbf{h}_R^{y^{-1}}\right)^{\mathbf{b}'} \cdot u^{x\cdot\langle \mathbf{a}', \mathbf{b}'\rangle}$$

Given a prover $\mathcal{P}^*$ that produces an accepting transcript with non-negligible probability, we can rewind the prover several times to obtain 8 accepting transcripts:

$$\begin{aligned}
\mathsf{tr}_1 &= (x_1, L_1, R_1, y_1, \mathbf{a}'^1, \mathbf{b}'^1)\\
\mathsf{tr}_2 &= (x_1, L_1, R_1, y_2, \mathbf{a}'^2, \mathbf{b}'^2)\\
\mathsf{tr}_3 &= (x_1, L_1, R_1, y_3, \mathbf{a}'^3, \mathbf{b}'^3)\\
\mathsf{tr}_4 &= (x_1, L_1, R_1, y_4, \mathbf{a}'^4, \mathbf{b}'^4)\\
\mathsf{tr}_5 &= (x_2, L_2, R_2, y_5, \mathbf{a}'^5, \mathbf{b}'^5)\\
\mathsf{tr}_6 &= (x_2, L_2, R_2, y_6, \mathbf{a}'^6, \mathbf{b}'^6)\\
\mathsf{tr}_7 &= (x_2, L_2, R_2, y_7, \mathbf{a}'^7, \mathbf{b}'^7)\\
\mathsf{tr}_8 &= (x_2, L_2, R_2, y_8, \mathbf{a}'^8, \mathbf{b}'^8)
\end{aligned}$$

with the following properties: $x_1 \neq x_2$, and for every $i, j \in [8]$ such that $i \neq j$: $y_i \neq y_j$ and $y_i \neq -y_j$. Lemma 1.4 says that from these accepting transcripts, we can extract a valid witness $(\mathbf{a}, \mathbf{b})$.

Lemma 1.4 (Special Soundness) *There is a PPT algorithm that takes the accepting transcripts $(\mathsf{tr}_1, \ldots, \mathsf{tr}_8)$ defined above, and either wins the discrete log relation game (def. 1.1) or computes a witness $(\mathbf{a}, \mathbf{b})$ for which*

$$\begin{aligned}
c &= \langle \mathbf{a}, \mathbf{b}\rangle\\
P &= \mathbf{g}^{\mathbf{a}} \cdot \mathbf{h}^{\mathbf{b}}
\end{aligned}$$

■

Question: Prove lemma 1.4.

Solution This problem is based on [BBB+17].

Lemma 1.5 *There is a PPT algorithm that takes* $(\mathsf{tr}_1, \ldots, \mathsf{tr}_4)$ *and either computes a solution to the discrete log relation game or computes values* $(\mathbf{a}^1, \mathbf{b}^1) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^n$ *such that*

$$P \cdot u^{x_1 \cdot c} = \mathbf{g}^{\mathbf{a}^1} \cdot \mathbf{h}^{\mathbf{b}^1} \cdot u^{x_1 \cdot \langle \mathbf{a}^1, \mathbf{b}^1 \rangle}$$

Proof.

1. Since $(\mathsf{tr}_1, \ldots, \mathsf{tr}_4)$ are accepting transcripts, the following equation holds for each $i \in [4]$:

$$P \cdot u^{x_1 \cdot c} \cdot L_1^{y_i^2} \cdot R_1^{y_i^{-2}} = \left(\mathbf{g}_L^{y_i^{-1}} * \mathbf{g}_R^{y_i}\right)^{\mathbf{a'}^i} \cdot \left(\mathbf{h}_L^{y_i} * \mathbf{h}_R^{y_i^{-1}}\right)^{\mathbf{b'}^i} \cdot u^{x_1 \cdot \langle \mathbf{a'}^i, \mathbf{b'}^i \rangle} \tag{1.1}$$

2. We will take linear combinations of equation 1.1 for $i \in [3]$ to separate the left-hand side into the factors $P \cdot u^{x_1 \cdot c}$, L_1, R_1.

   (a)

   $$\text{Let } M = \begin{bmatrix} y_1^2 & y_2^2 & y_3^2 \\ 1 & 1 & 1 \\ y_1^{-2} & y_2^{-2} & y_3^{-2} \end{bmatrix}$$

   Since y_1, y_2, y_3 are distinct, M is full-rank, so M^{-1} exists.

   (b)

   $$\begin{aligned} \text{Let } \mathbf{v}^L &= M^{-1} \cdot \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}^T = M^{-1} \cdot \hat{\mathbf{e}}_1 \\ \mathbf{v}^P &= M^{-1} \cdot \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}^T = M^{-1} \cdot \hat{\mathbf{e}}_2 \\ \mathbf{v}^R &= M^{-1} \cdot \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}^T = M^{-1} \cdot \hat{\mathbf{e}}_3 \end{aligned}$$

   (c) Now take a linear combination of equation 1.1 for $i \in [3]$ with coefficients given by $\mathbf{v}^L$. This yields:

   $$\prod_{i \in [3]} \left(P \cdot u^{x_1 \cdot c} \cdot L_1^{y_i^2} \cdot R_1^{y_i^{-2}}\right)^{\mathbf{v}_i^L} = \prod_{i \in [3]} \left[\left(\mathbf{g}_L^{y_i^{-1}} * \mathbf{g}_R^{y_i}\right)^{\mathbf{a'}^i} \cdot \left(\mathbf{h}_L^{y_i} * \mathbf{h}_R^{y_i^{-1}}\right)^{\mathbf{b'}^i} \cdot u^{x_1 \cdot \langle \mathbf{a'}^i, \mathbf{b'}^i \rangle}\right]^{\mathbf{v}_i^L} \tag{1.2}$$

   The left-hand side can be simplified as follows:

   $$\begin{aligned} \prod_{i \in [3]} \left(P \cdot u^{x_1 \cdot c} \cdot L_1^{y_i^2} \cdot R_1^{y_i^{-2}}\right)^{\mathbf{v}_i^L} &= (P \cdot u^{x_1 \cdot c})^{\sum_{i \in [3]} \mathbf{v}_i^L} \cdot L_1^{\sum_{i \in [3]} y_i^2 \cdot \mathbf{v}_i^L} \cdot R_1^{\sum_{i \in [3]} y_i^{-2} \cdot \mathbf{v}_i^L} \\ &= (P \cdot u^{x_1 \cdot c})^{\hat{\mathbf{e}}_2^T \cdot M \cdot \mathbf{v}^L} \cdot L_1^{\hat{\mathbf{e}}_1^T \cdot M \cdot \mathbf{v}^L} \cdot R_1^{\hat{\mathbf{e}}_3^T \cdot M \cdot \mathbf{v}^L} \\ &= (P \cdot u^{x_1 \cdot c})^{\langle \hat{\mathbf{e}}_2, \hat{\mathbf{e}}_1 \rangle} \cdot L_1^{\langle \hat{\mathbf{e}}_1, \hat{\mathbf{e}}_1 \rangle} \cdot R_1^{\langle \hat{\mathbf{e}}_3, \hat{\mathbf{e}}_1 \rangle} \\ &= L_1 \end{aligned}$$

Next,

$$\begin{aligned}
\text{let } \mathbf{a}^L &= \left(\sum_{i\in[3]} \mathbf{v}_i^L \cdot y_i^{-1} \cdot \mathbf{a}'^i\right) \mid\mid \left(\sum_{i\in[3]} \mathbf{v}_i^L \cdot y_i \cdot \mathbf{a}'^i\right) \\
\mathbf{b}^L &= \left(\sum_{i\in[3]} \mathbf{v}_i^L \cdot y_i \cdot \mathbf{b}'^i\right) \mid\mid \left(\sum_{i\in[3]} \mathbf{v}_i^L \cdot y_i^{-1} \cdot \mathbf{b}'^i\right) \\
c^L &= \sum_{i\in[3]} \mathbf{v}_i^L \cdot \langle \mathbf{a}'^i, \mathbf{b}'^i \rangle
\end{aligned}$$

Note that $\left(\sum_{i\in[3]} \mathbf{v}_i^L \cdot y_i^{-1} \cdot \mathbf{a}'^i\right)$ and $\left(\sum_{i\in[3]} \mathbf{v}_i^L \cdot y_i \cdot \mathbf{a}'^i\right)$ are vectors in $\mathbb{Z}_p^{n/2}$, so $\mathbf{a}^L \in \mathbb{Z}_p^n$. The right-hand side of equation 1.2 is simplified as follows:

$$\begin{aligned}
\text{Then } \prod_{i\in[3]} &\left[\left(\mathbf{g}_L^{y_i^{-1}} * \mathbf{g}_R^{y_i}\right)^{\mathbf{a}'^i} \cdot \left(\mathbf{h}_L^{y_i} * \mathbf{h}_R^{y_i^{-1}}\right)^{\mathbf{b}'^i} \cdot u^{x_1 \cdot \langle \mathbf{a}'^i, \mathbf{b}'^i\rangle}\right]^{\mathbf{v}_i^L} \\
&= \left(\mathbf{g}_L^{\sum_{i\in[3]} \mathbf{v}_i^L \cdot y_i^{-1} \cdot \mathbf{a}'^i} \cdot \mathbf{g}_R^{\sum_{i\in[3]} \mathbf{v}_i^L \cdot y_i \cdot \mathbf{a}'^i}\right) \cdot \left(\mathbf{h}_L^{\sum_{i\in[3]} \mathbf{v}_i^L \cdot y_i \cdot \mathbf{b}'^i} \cdot \mathbf{h}_R^{\sum_{i\in[3]} \mathbf{v}_i^L \cdot y_i^{-1} \cdot \mathbf{b}'^i}\right) \\
&\quad \cdot u^{\sum_{i\in[3]} \mathbf{v}_i^L \cdot x_1 \cdot \langle \mathbf{a}'^i, \mathbf{b}'^i \rangle} \\
&= \mathbf{g}^{\mathbf{a}^L} \cdot \mathbf{h}^{\mathbf{b}^L} \cdot u^{x_1 \cdot c^L}
\end{aligned}$$

In total, we've constructed $\mathbf{a}^L, \mathbf{b}^L \in \mathbb{Z}_p^n$ and $c^L \in \mathbb{Z}_p$ such that:

$$L_1 = \mathbf{g}^{\mathbf{a}^L} \cdot \mathbf{h}^{\mathbf{b}^L} \cdot u^{x_1 \cdot c^L} \tag{1.3}$$

(d) Likewise, take a linear combination of equation 1.1 for $i \in [3]$ with coefficients given by $\mathbf{v}^P$ and another linear combination with coefficients given by $\mathbf{v}^R$. This yields:

$$\prod_{i\in[3]} \left(P \cdot u^{x_1 \cdot c} \cdot L_1^{y_i^2} \cdot R_1^{y_i^{-2}}\right)^{\mathbf{v}_i^P} = \prod_{i\in[3]} \left[\left(\mathbf{g}_L^{y_i^{-1}} * \mathbf{g}_R^{y_i}\right)^{\mathbf{a}'^i} \cdot \left(\mathbf{h}_L^{y_i} * \mathbf{h}_R^{y_i^{-1}}\right)^{\mathbf{b}'^i} \cdot u^{x_1 \cdot \langle \mathbf{a}'^i, \mathbf{b}'^i\rangle}\right]^{\mathbf{v}_i^P} \tag{1.4}$$

$$\prod_{i\in[3]} \left(P \cdot u^{x_1 \cdot c} \cdot L_1^{y_i^2} \cdot R_1^{y_i^{-2}}\right)^{\mathbf{v}_i^R} = \prod_{i\in[3]} \left[\left(\mathbf{g}_L^{y_i^{-1}} * \mathbf{g}_R^{y_i}\right)^{\mathbf{a}'^i} \cdot \left(\mathbf{h}_L^{y_i} * \mathbf{h}_R^{y_i^{-1}}\right)^{\mathbf{b}'^i} \cdot u^{x_1 \cdot \langle \mathbf{a}'^i, \mathbf{b}'^i\rangle}\right]^{\mathbf{v}_i^R} \tag{1.5}$$

Then define the following variables:

$$\begin{aligned}
\mathbf{a}^P &= \left(\sum_{i\in[3]} \mathbf{v}_i^P \cdot y_i^{-1} \cdot \mathbf{a}'^i\right) \mid\mid \left(\sum_{i\in[3]} \mathbf{v}_i^P \cdot y_i \cdot \mathbf{a}'^i\right)\\
\mathbf{b}^P &= \left(\sum_{i\in[3]} \mathbf{v}_i^P \cdot y_i \cdot \mathbf{b}'^i\right) \mid\mid \left(\sum_{i\in[3]} \mathbf{v}_i^P \cdot y_i^{-1} \cdot \mathbf{b}'^i\right)\\
c^P &= \sum_{i\in[3]} \mathbf{v}_i^P \cdot \langle \mathbf{a}'^i, \mathbf{b}'^i\rangle
\end{aligned}$$

$$\begin{aligned}
\mathbf{a}^R &= \left(\sum_{i\in[3]} \mathbf{v}_i^R \cdot y_i^{-1} \cdot \mathbf{a}'^i\right) \mid\mid \left(\sum_{i\in[3]} \mathbf{v}_i^R \cdot y_i \cdot \mathbf{a}'^i\right)\\
\mathbf{b}^R &= \left(\sum_{i\in[3]} \mathbf{v}_i^R \cdot y_i \cdot \mathbf{b}'^i\right) \mid\mid \left(\sum_{i\in[3]} \mathbf{v}_i^R \cdot y_i^{-1} \cdot \mathbf{b}'^i\right)\\
c^R &= \sum_{i\in[3]} \mathbf{v}_i^R \cdot \langle \mathbf{a}'^i, \mathbf{b}'^i\rangle
\end{aligned}$$

Then equations 1.4 and 1.5 simplify to:

$$P \cdot u^{x_1 \cdot c} = \mathbf{g}^{\mathbf{a}^P} \cdot \mathbf{h}^{\mathbf{b}^P} \cdot u^{x_1 \cdot c^P} \tag{1.6}$$

$$R_1 = \mathbf{g}^{\mathbf{a}^R} \cdot \mathbf{h}^{\mathbf{b}^R} \cdot u^{x_1 \cdot c^R} \tag{1.7}$$

3. We can extract a system of equations relating $(\mathbf{a}^L, \mathbf{a}^P, \mathbf{a}^R, \mathbf{b}^L, \mathbf{b}^P, \mathbf{b}^R)$ or else we can find a solution to the discrete log relation problem.

   (a) For each $i \in [4]$, equation 1.1 implies the following:

$$\begin{aligned}
P \cdot u^{x_1 \cdot c} \cdot L_1^{y_i^2} \cdot R_1^{y_i^{-2}} &= \left(\mathbf{g}_L^{y_i^{-1}} * \mathbf{g}_R^{y_i}\right)^{\mathbf{a}'^i} \cdot \left(\mathbf{h}_L^{y_i} * \mathbf{h}_R^{y_i^{-1}}\right)^{\mathbf{b}'^i} \cdot u^{x_1 \cdot \langle \mathbf{a}'^i, \mathbf{b}'^i\rangle}\\
&= \mathbf{g}_L^{y_i^{-1} \cdot \mathbf{a}'^i} \cdot \mathbf{g}_R^{y_i \cdot \mathbf{a}'^i} \cdot \mathbf{h}_L^{y_i \cdot \mathbf{b}'^i} \cdot \mathbf{h}_R^{y_i^{-1} \cdot \mathbf{b}'^i} \cdot u^{x_1 \cdot \langle \mathbf{a}'^i, \mathbf{b}'^i\rangle}
\end{aligned}$$

(b) Next, equations 1.3, 1.6, 1.7 imply that:

$$\begin{aligned} P \cdot u^{x_1 \cdot c} \cdot L_1^{y_i^2} \cdot R_1^{y_i^{-2}} &= \left(\mathbf{g}^{\mathbf{a}^P} \cdot \mathbf{h}^{\mathbf{b}^P} \cdot u^{x_1 \cdot c^P}\right) \cdot \left(\mathbf{g}^{\mathbf{a}^L} \cdot \mathbf{h}^{\mathbf{b}^L} \cdot u^{x_1 \cdot c^L}\right)^{y_i^2} \cdot \left(\mathbf{g}^{\mathbf{a}^R} \cdot \mathbf{h}^{\mathbf{b}^R} \cdot u^{x_1 \cdot c^R}\right)^{y_i^{-2}} \\ &= \mathbf{g}^{\mathbf{a}^P + y_i^2 \cdot \mathbf{a}^L + y_i^{-2} \cdot \mathbf{a}^R} \cdot \mathbf{h}^{\mathbf{b}^P + y_i^2 \cdot \mathbf{b}^L + y_i^{-2} \cdot \mathbf{b}^R} \cdot u^{x_1 \cdot \left(c^P + y_i^2 \cdot c^L + y_i^{-2} \cdot c^R\right)} \\ &= \mathbf{g}_L^{\mathbf{a}_L^P + y_i^2 \cdot \mathbf{a}_L^L + y_i^{-2} \cdot \mathbf{a}_L^R} \cdot \mathbf{g}_R^{\mathbf{a}_R^P + y_i^2 \cdot \mathbf{a}_R^L + y_i^{-2} \cdot \mathbf{a}_R^R} \\ &\quad \cdot \mathbf{h}_L^{\mathbf{b}_L^P + y_i^2 \cdot \mathbf{b}_L^L + y_i^{-2} \cdot \mathbf{b}_L^R} \cdot \mathbf{h}_R^{\mathbf{b}_R^P + y_i^2 \cdot \mathbf{b}_R^L + y_i^{-2} \cdot \mathbf{b}_R^R} \\ &\quad \cdot u^{x_1 \cdot \left(c^P + y_i^2 \cdot c^L + y_i^{-2} \cdot c^R\right)} \end{aligned}$$

$$\begin{aligned} 1 &= \mathbf{g}_L^{\mathbf{a}_L^P + y_i^2 \cdot \mathbf{a}_L^L + y_i^{-2} \cdot \mathbf{a}_L^R - y_i^{-1} \cdot \mathbf{a}'^i} \cdot \mathbf{g}_R^{\mathbf{a}_R^P + y_i^2 \cdot \mathbf{a}_R^L + y_i^{-2} \cdot \mathbf{a}_R^R - y_i \cdot \mathbf{a}'^i} \\ &\quad \cdot \mathbf{h}_L^{\mathbf{b}_L^P + y_i^2 \cdot \mathbf{b}_L^L + y_i^{-2} \cdot \mathbf{b}_L^R - y_i \cdot \mathbf{b}'^i} \cdot \mathbf{h}_R^{\mathbf{b}_R^P + y_i^2 \cdot \mathbf{b}_R^L + y_i^{-2} \cdot \mathbf{b}_R^R - y_i^{-1} \cdot \mathbf{b}'^i} \\ &\quad \cdot u^{x_1 \cdot \left(c^P + y_i^2 \cdot c^L + y_i^{-2} \cdot c^R - \langle \mathbf{a}'^i, \mathbf{b}'^i \rangle\right)} \end{aligned}$$

(c) The exponents of $(\mathbf{g}_L, \mathbf{g}_R, \mathbf{h}_L, \mathbf{h}_R, u)$ can be computed from $(\mathsf{tr}_1, \ldots, \mathsf{tr}_4)$, and if any of them is non-zero, then they represent a solution to the discrete log relation problem. Let us assume that the discrete log relation problem is hard, so from now onward, all of the exponents must be zero, and the following equations are satisfied:

$$\begin{aligned} \mathbf{a}'^i &= y_i^1 \cdot \mathbf{a}_L^P + y_i^3 \cdot \mathbf{a}_L^L + y_i^{-1} \cdot \mathbf{a}_L^R \\ \mathbf{a}'^i &= y_i^{-1} \cdot \mathbf{a}_R^P + y_i^1 \cdot \mathbf{a}_R^L + y_i^{-3} \cdot \mathbf{a}_R^R \\ \mathbf{b}'^i &= y_i^{-1} \cdot \mathbf{b}_L^P + y_i^1 \cdot \mathbf{b}_L^L + y_i^{-3} \cdot \mathbf{b}_L^R \\ \mathbf{b}'^i &= y_i^1 \cdot \mathbf{b}_R^P + y_i^3 \cdot \mathbf{b}_R^L + y_i^{-1} \cdot \mathbf{b}_R^R \\ \langle \mathbf{a}'^i, \mathbf{b}'^i \rangle &= c^P + y_i^2 \cdot c^L + y_i^{-2} \cdot c^R \end{aligned} \tag{1.8}$$

(d) Next, we combine the equations above:

$$\begin{aligned} y_i^1 \cdot \mathbf{a}_L^P + y_i^3 \cdot \mathbf{a}_L^L + y_i^{-1} \cdot \mathbf{a}_L^R = \mathbf{a}'^i &= y_i^{-1} \cdot \mathbf{a}_R^P + y_i^1 \cdot \mathbf{a}_R^L + y_i^{-3} \cdot \mathbf{a}_R^R \\ 0 &= y_i^{-3} \cdot \mathbf{a}_R^R + y_i^{-1} \cdot (\mathbf{a}_R^P - \mathbf{a}_L^R) + y_i^1 \cdot (\mathbf{a}_R^L - \mathbf{a}_L^P) - y_i^3 \cdot \mathbf{a}_L^L \end{aligned}$$

Let us define some Laurent polynomials:

$$\begin{aligned} \text{Let } f_{\mathbf{a}}(Y) &= \mathbf{a}_R^R + Y^2 \cdot (\mathbf{a}_R^P - \mathbf{a}_L^R) + Y^4 \cdot (\mathbf{a}_R^L - \mathbf{a}_L^P) - Y^6 \cdot \mathbf{a}_L^L \\ g_{\mathbf{a}}(Y) &= Y^{-3} \cdot f_{\mathbf{a}}(Y) \\ &= Y^{-3} \cdot \mathbf{a}_R^R + Y^{-1} \cdot (\mathbf{a}_R^P - \mathbf{a}_L^R) + Y^1 \cdot (\mathbf{a}_R^L - \mathbf{a}_L^P) - Y^3 \cdot \mathbf{a}_L^L \end{aligned}$$

Then $g_{\mathbf{a}}(y_i) = 0$ for every $i \in [4]$.

(e) **Claim 1.6** $f_{\mathbf{a}}(Y) = 0$

Proof. We have already shown that $g_{\mathbf{a}}(y_i) = 0$ for every $i \in [4]$. Furthermore, $g_{\mathbf{a}}(-y_i) = -g_{\mathbf{a}}(y_i) = 0$. That implies that $f_{\mathbf{a}}(y_i) = f_{\mathbf{a}}(-y_i) = 0$. Next, $\{y_1, -y_1, y_2, -y_2, y_3, -y_3, y_4, -y_4\}$ are 8 distinct values, and they are all roots of $f_{\mathbf{a}}(Y)$. $f_{\mathbf{a}}$ has degree-6, so the only way that $f_{\mathbf{a}}$ has more than 6 roots is if $f_{\mathbf{a}}(Y) = 0$.

(f) Since $f_{\mathbf{a}}(Y) = 0$, the following equations hold:

$$\begin{aligned} \mathbf{a}_R^R &= \mathbf{a}_L^L = 0 \\ \mathbf{a}_R^P &= \mathbf{a}_L^R \\ \mathbf{a}_L^P &= \mathbf{a}_R^L \end{aligned}$$

(g) By similar reasoning, we can show that:

$$\begin{aligned} \mathbf{b}_L^R &= \mathbf{b}_R^L = 0 \\ \mathbf{b}_R^P &= \mathbf{b}_L^L \\ \mathbf{b}_L^P &= \mathbf{b}_R^R \end{aligned}$$

4. **Claim 1.7** $\langle \mathbf{a}^P, \mathbf{b}^P \rangle = c^P$

Proof.

(a) By equations 1.8, for each $i \in [4]$,

$$\begin{aligned} \mathbf{a}'^i &= y_i \cdot \mathbf{a}_L^P + y_i^3 \cdot \mathbf{a}_L^L + y_i^{-1} \cdot \mathbf{a}_L^R \\ &= y_i \cdot \mathbf{a}_L^P + y_i^{-1} \cdot \mathbf{a}_R^P \end{aligned}$$

$$\begin{aligned} \mathbf{b}'^i &= y_i^{-1} \cdot \mathbf{b}_L^P + y_i^1 \cdot \mathbf{b}_L^L + y_i^{-3} \cdot \mathbf{b}_L^R \\ &= y_i^{-1} \cdot \mathbf{b}_L^P + y_i^1 \cdot \mathbf{b}_R^P \end{aligned}$$

$$\begin{aligned} c^P + y_i^2 \cdot c^L + y_i^{-2} \cdot c^R &= \langle \mathbf{a}'^i, \mathbf{b}'^i \rangle \\ &= \langle (y_i \cdot \mathbf{a}_L^P + y_i^{-1} \cdot \mathbf{a}_R^P), (y_i^{-1} \cdot \mathbf{b}_L^P + y_i \cdot \mathbf{b}_R^P) \rangle \\ &= y_i^{-2} \cdot \langle \mathbf{a}_R^P, \mathbf{b}_L^P \rangle + \langle \mathbf{a}_L^P, \mathbf{b}_L^P \rangle + \langle \mathbf{a}_R^P, \mathbf{b}_R^P \rangle + y_i^2 \cdot \langle \mathbf{a}_L^P, \mathbf{b}_R^P \rangle \\ &= y_i^{-2} \cdot \langle \mathbf{a}_R^P, \mathbf{b}_L^P \rangle + \langle \mathbf{a}^P, \mathbf{b}^P \rangle + y_i^2 \cdot \langle \mathbf{a}_L^P, \mathbf{b}_R^P \rangle \\ 0 &= y_i^{-2} \cdot \left(\langle \mathbf{a}_R^P, \mathbf{b}_L^P \rangle - c^R \right) + \left(\langle \mathbf{a}^P, \mathbf{b}^P \rangle - c^P \right) + y_i^2 \cdot \left(\langle \mathbf{a}_L^P, \mathbf{b}_R^P \rangle - c^L \right) \end{aligned}$$

(b) Let us define some Laurent polynomials:

$$\begin{aligned} f_{\langle\rangle}(Y) &= \left(\langle \mathbf{a}_R^P, \mathbf{b}_L^P \rangle - c^R \right) + Y^2 \cdot \left(\langle \mathbf{a}^P, \mathbf{b}^P \rangle - c^P \right) + Y^4 \cdot \left(\langle \mathbf{a}_L^P, \mathbf{b}_R^P \rangle - c^L \right) \\ g_{\langle\rangle}(Y) &= Y^{-2} \cdot f_{\langle\rangle}(Y) \\ &= Y^{-2} \cdot \left(\langle \mathbf{a}_R^P, \mathbf{b}_L^P \rangle - c^R \right) + \left(\langle \mathbf{a}^P, \mathbf{b}^P \rangle - c^P \right) + Y^2 \cdot \left(\langle \mathbf{a}_L^P, \mathbf{b}_R^P \rangle - c^L \right) \end{aligned}$$

(c) We know that for any $i \in [4]$, $g_{\langle\rangle}(y_i) = 0$. Furthermore, $g_{\langle\rangle}(-y_i) = g_{\langle\rangle}(y_i) = 0$, and $f_{\langle\rangle}(y_i) = f_{\langle\rangle}(-y_i) = 0$. This means that on 8 distinct points, $\{y_1, -y_1, y_2, -y_2, y_3, -y_3, y_4, -y_4\}$, $f_{\langle\rangle}(Y) = 0$. Since $f_{\langle\rangle}(Y)$ has degree 4, the only way that $f_{\langle\rangle}(Y)$ has 8 roots is if $f_{\langle\rangle}(Y) = 0$.

(d) Since $f_{\langle\rangle}(Y) = 0$, the following equations are true:

$$\begin{aligned} c^R &= \langle \mathbf{a}_R^P, \mathbf{b}_L^P \rangle \\ c^P &= \langle \mathbf{a}^P, \mathbf{b}^P \rangle \\ c^L &= \langle \mathbf{a}_L^P, \mathbf{b}_R^P \rangle \end{aligned}$$

5. Let us set $(\mathbf{a}^1, \mathbf{b}^1) = (\mathbf{a}^P, \mathbf{b}^P)$, then we can rewrite equation 1.6 as follows:

$$\begin{aligned} P \cdot u^{x_1 \cdot c} &= \mathbf{g}^{\mathbf{a}^P} \cdot \mathbf{h}^{\mathbf{b}^P} \cdot u^{x_1 \cdot c^P} \\ P \cdot u^{x_1 \cdot c} &= \mathbf{g}^{\mathbf{a}^1} \cdot \mathbf{h}^{\mathbf{b}^1} \cdot u^{x_1 \cdot \langle \mathbf{a}^1, \mathbf{b}^1 \rangle} \end{aligned}$$

Lemma 1.8 *There is a PPT algorithm that takes* $(\mathsf{tr}_5, \ldots, \mathsf{tr}_8)$ *and either computes a solution to the discrete log relation game or computes values* $(\mathbf{a}^2, \mathbf{b}^2) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^n$ *such that*

$$P \cdot u^{x_2 \cdot c} = \mathbf{g}^{\mathbf{a}^2} \cdot \mathbf{h}^{\mathbf{b}^2} \cdot u^{x_2 \cdot \langle \mathbf{a}^2, \mathbf{b}^2 \rangle}$$

The proof of lemma 1.8 is similar to the proof of lemma 1.5.

Lemma 1.9 *Given values* $\mathbf{a}^1, \mathbf{b}^1, \mathbf{a}^2, \mathbf{b}^2 \in \mathbb{Z}_p^n$ *such that*

$$P \cdot u^{x_1 \cdot c} = \mathbf{g}^{\mathbf{a}^1} \cdot \mathbf{h}^{\mathbf{b}^1} \cdot u^{x_1 \cdot \langle \mathbf{a}^1, \mathbf{b}^1 \rangle} \tag{1.9}$$

$$P \cdot u^{x_2 \cdot c} = \mathbf{g}^{\mathbf{a}^2} \cdot \mathbf{h}^{\mathbf{b}^2} \cdot u^{x_2 \cdot \langle \mathbf{a}^2, \mathbf{b}^2 \rangle} \tag{1.10}$$

and $x_1 \neq x_2$*, there is a PPT algorithm that computes a pair* $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_p^n$ *such that*

$$\begin{aligned} c &= \langle \mathbf{a}, \mathbf{b} \rangle \\ P &= \mathbf{g}^{\mathbf{a}} \cdot \mathbf{h}^{\mathbf{b}} \end{aligned} \tag{1.11}$$

Proof. We will show that $\mathbf{a}^1 = \mathbf{a}^2$, $\mathbf{b}^1 = \mathbf{b}^2$, and $\langle \mathbf{a}^1, \mathbf{b}^1 \rangle = c$, or else we can compute a solution to the discrete log relation problem. Then we set $(\mathbf{a}, \mathbf{b}) = (\mathbf{a}^1, \mathbf{b}^1)$, so $(\mathbf{a}, \mathbf{b})$ satisfies 1.11.

1. Let us take a linear combination of equations 1.9 and 1.10 with coefficients 1 and -1:

$$\begin{aligned} P^{1-1} \cdot u^{(x_1 - x_2) \cdot c} &= \mathbf{g}^{\mathbf{a}^1 - \mathbf{a}^2} \cdot \mathbf{h}^{\mathbf{b}^1 - \mathbf{b}^2} \cdot u^{x_1 \cdot \langle \mathbf{a}^1, \mathbf{b}^1 \rangle - x_2 \cdot \langle \mathbf{a}^2, \mathbf{b}^2 \rangle} \\ 1 &= \mathbf{g}^{\mathbf{a}^1 - \mathbf{a}^2} \cdot \mathbf{h}^{\mathbf{b}^1 - \mathbf{b}^2} \cdot u^{x_1 \cdot \langle \mathbf{a}^1, \mathbf{b}^1 \rangle - x_2 \cdot \langle \mathbf{a}^2, \mathbf{b}^2 \rangle - (x_1 - x_2) \cdot c} \end{aligned}$$

2. Then we can compute a solution to the discrete log relation problem unless the following conditions are satisfied:

$$\begin{aligned} \mathbf{a}^1 &= \mathbf{a}^2 \\ \mathbf{b}^1 &= \mathbf{b}^2 \\ 0 &= x_1 \cdot \langle \mathbf{a}^1, \mathbf{b}^1 \rangle - x_2 \cdot \langle \mathbf{a}^2, \mathbf{b}^2 \rangle - (x_1 - x_2) \cdot c \end{aligned}$$

   The final condition simplifies to the following:

$$\begin{aligned} 0 &= (x_1 - x_2) \cdot \langle \mathbf{a}^1, \mathbf{b}^1 \rangle - (x_1 - x_2) \cdot c \\ c &= \langle \mathbf{a}^1, \mathbf{b}^1 \rangle \end{aligned}$$

3. Let us assume that the discrete log relation problem is hard, so the conditions above are satisfied. Then we can set $(\mathbf{a}, \mathbf{b}) = (\mathbf{a}^1, \mathbf{b}^1)$. Then $c = \langle \mathbf{a}, \mathbf{b} \rangle$, and:

$$\begin{aligned} P \cdot u^{x_1 \cdot c} &= \mathbf{g}^{\mathbf{a}^1} \cdot \mathbf{h}^{\mathbf{b}^1} \cdot u^{x_1 \cdot \langle \mathbf{a}^1, \mathbf{b}^1 \rangle} \\ &= \mathbf{g}^{\mathbf{a}} \cdot \mathbf{h}^{\mathbf{b}} \cdot u^{x_1 \cdot c} \\ P &= \mathbf{g}^{\mathbf{a}} \cdot \mathbf{h}^{\mathbf{b}} \end{aligned}$$

■

References

[BBB+17] Benedikt Bnz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for confidential transactions and more. Cryptology ePrint Archive, Paper 2017/1066, 2017.