Zero-knowledge proof for Lattice-based group signature schemes with Verifier-local Revocation

Maharage Nisansala Sevwandi Perera and Takeshi Koshiba

[1] Graduate School of Science and Engineering
Saitama University, Japan
perera.m.n.s.119@ms.saitama-u.ac.jp,
[2] Faculty of Education and Integrated Arts and Sciences
Waseda University, Japan
tkoshiba@waseda.jp

Abstract. In group signature schemes, signers prove verifiers, their validity of signing through an interactive protocol in zero-knowledge. In lattice-based group signatures with Verifier-local revocation (VLR), group members have both secret signing key and revocation token. Thus, the members in VLR schemes should show the verifiers, that he has a valid secret signing key and his token is not in the revoked members list. These conditions are satisfied in the underlying interactive protocol provided in the first lattice-based group signature scheme with VLR suggested by Langlois et al. in PKC 2014. In their scheme, member revocation token is a part of the secret signing key and has an implicit tracing algorithm to trace signers. For a scheme which generates member revocation token separately, the suggested interactive protocol by Langlois et al. is not suitable. Moreover, if the group manager wants to use an explicit tracing algorithm to trace signers instead the implicit tracing algorithm given in VLR schemes, then the signer should encrypt his index at the time of signing, and the interactive protocol should show signer's index is correctly encrypted. This work presents a combined interactive protocol that signer can use to prove his validity of signing, his separately generated revocation token is not in the revocation list, and his index is correctly encrypted required for such kind of schemes.

Keywords: lattice-based group signatures, verifier-local revocation, zero-knowledge proof, interactive protocol

1 Introduction

Commitment schemes are one of the leading primitives of group signature schemes. Commitment schemes allow a prover (signer) to commit to a value while keeping it in secret and later the prover provides additional information to open the commitment. A commitment scheme has three requirements, namely, *Hiding property*, *Binding property*, and *Viability.* The hiding property requires the receiver (verifier) cannot learn anything about the committed value. The binding property requires the prover cannot change the committed value after the commit step. The viability ensures if both parties, the signer and the verifier follow the protocol honestly, the verifier will always recover the committed value. Kawachi et al. [?] proposed a simple construction from lattices for string commitment scheme. Let COM be the statistically hiding and computationally binding commitment scheme. The statistically hiding requirement ensures any cheating verifier (adversary) cannot distinguish the commitments of two different strings and the computationally binding requirement ensures any polynomial time cheating signer cannot change the committed string after the commitment phase.

In 2014, Langlois et al. [?] presented the first lattice-based group signature scheme with member revocation while employing most flexible revocation approach, *Verifier-local revocation*. Their scheme operates within the structure of a *Bonsai tree* of hard random lattices, specified by a matrix $\mathbf{A}$ and a vector $\mathbf{u}$. In the proof of knowledge system, the signer with identity d has to prove in zero-knowledge that he knows a vector $\mathbf{z}$ which is a solution to the Inhomogeneous Short Integer Solution instance $(\mathbf{A}_d \cdot \mathbf{z})$ while hiding $\mathbf{z}$, where the vector $\mathbf{z}$ is the Bonsai signature issued on the prover's identity d. In other words, the signer has to prove, $||\mathbf{z}||_\infty \leq \beta$ and $\mathbf{A}_d \cdot \mathbf{z} = \mathbf{u} \mod q$ in zero-knowledge while hiding $\mathbf{z}$, where $\mathbf{A}_d = [\mathbf{A}_0|\mathbf{A}_1^0|\mathbf{A}_1^1|\ldots|\mathbf{A}_\ell^0|\mathbf{A}_\ell^1] \in \mathbb{Z}_q^{n\times(2\ell+1)m}$. As a solution for the above problem. they use a masking method. The masking method extends the given vector by adding zero-blocks. In the scheme in [?], they extended the vector $\mathbf{z}$ by adding ℓ suitable *zero-blocks* of size m to obtain a vector $\mathbf{x} = (\mathbf{x}_0||\mathbf{x}_1^0||\mathbf{x}_1^1||\ldots||\mathbf{x}_\ell^0||\mathbf{x}_\ell^1) \in \mathbb{Z}^{(2\ell+1)m}$, such that $||\mathbf{x}||_\infty \leq \beta$, and $\mathbf{A}\cdot\mathbf{x} = \mathbf{u} \mod q$, where $\mathbf{x}_1^{1-d[1]}, \ldots, \mathbf{x}_\ell^{1-d[\ell]}$ are added zero-blocks. To prove in zero-knowledge the possession of $\mathbf{x}$, Langlois et al. [?] adapted the 'Stren Extension' argument system provided in [?]. Moreover, they have generated the revocation token of each user by using the first block of user's secret signing key and the first block of the corresponding Bonsai tree. Thus the revocation token $\mathbf{grt}$ is $(\mathbf{A}_0 \cdot \mathbf{x}_0) \mod q$. At the time of signing, the signer computes $\mathbf{v} = \mathbf{V} \cdot \mathbf{grt} + \mathbf{e}_1 \mod q$, where $\mathbf{V} \in \mathbb{Z}_q^{m\times n}$ is a uniformly random matrix which is drawn from a random oracle and $\mathbf{e}_1 \in \mathbb{Z}^m$ is a small vector which is sampled from the Learning With Error distribution. At the zero-knowledge argument system, the signer additionally proves that the vector $\mathbf{v}$ is honestly generated.

However, in case of separating the revocation token creation from the secret signing key, the generation of the vector $\mathbf{v}$ cannot prove using the interactive protocol given in [?]. Moreover, the scheme in [?] uses an implicit tracing algorithm which requires to execute Verify with the tracing message-signature pair (M, Σ) for each member until the signer is traced. For a large group, this is not a convenient method. The group manager may require to find the signer quickly using an explicit tracing algorithm. For the explicit tracing algorithm, the signer should encrypt his index d at the time of signing, and he should prove his index d correctly encrypted in a ciphertext $\mathbf{c}$. This yields a new zero-knowledge interactive protocol since the protocol given in [?] cannot satisfy those conditions.

Our Contribution

The underlying interactive protocol in Langlois's scheme allows a signer to prove his validity using two vectors of the witness. One vector is for witnessing his Bonsai signature and the other vector is for witnessing he is not being revoked.

However, for a situation that revocation token is not deriving from the secret signing key, the interactive protocol given in [?] cannot be employed. Moreover, we take into account schemes which require the signers to encrypt their index at the signature generation such that the group manager can open signatures and trace the signers using the explicit tracing algorithm. Thus we need a protocol to show that the given ciphertext is correct encryption of the signer's index. As an answer for those requirements, we present a combined protocol which proves that the signer is a certified group member possessing a signature on his secret index with respect to the Bonsai tree signature, the signer's revocation token is correctly committed via an LWE function, and the signer's index is correctly encrypted based on LWE.

2 Preliminaries

2.1 Notations

For any integer $k \geq 1$, we denote the set of integers $\{1, \ldots, k\}$ by $[k]$. We denote matrices by bold upper-case letters such as $\mathbf{A}$, and vectors by bold lower-case letters, such as $\mathbf{x}$. We assume that all vectors are in column form. The concatenation of matrices $\mathbf{A} \in \mathbb{R}^{n \times m}$ and $\mathbf{B} \in \mathbb{R}^{n \times k}$, is denoted by $[\mathbf{A}|\mathbf{B}] \in \mathbb{R}^{n \times (m+k)}$. The concatenation of vectors $\mathbf{x} \in \mathbb{R}^m$ and $\mathbf{y} \in \mathbb{R}^k$ is denoted by $(\mathbf{x}\|\mathbf{y}) \in \mathbb{R}^{m+k}$. If S is a finite set, $b \xleftarrow{\$} S$ means that b is chosen uniformly at random from S. The Euclidean norm of $\mathbf{x}$ is denoted by $||\mathbf{x}||$ and the infinity norm is denoted by $||\mathbf{x}||_\infty$. Let χ be a b-bounded distribution over $\mathbb{Z}$ (i.e., samples that output by χ is with norm at most b with overwhelming probability where $b \geq \sqrt{n}\omega(\log n)$).

$\mathsf{Secret}_\beta(d)$ and $\mathsf{SecretExt}_\beta(d)$ are specific sets of vectors defined in [?] and obtained by appending ℓ *zero−blocks* of size 0^m and 0^{3m} respectively to vectors $\mathbf{x} \in \mathbb{Z}^{(2\ell+1)m}$ and $\mathbf{x} \in \mathbb{Z}^{(2\ell+1)3m}$.

2.2 Lattice-based Functions

Definition 1 (Learning With Errors (LWE) [?]). *For a vector $\boldsymbol{s} \in \mathbb{Z}_q^n$ and χ, the distribution $\mathrm{A}_{\boldsymbol{s},\chi}$ is obtained by sampling $\boldsymbol{a} \in \mathbb{Z}_q^n$ uniformly at random and choosing $\mathrm{e} \leftarrow \chi$, and outputting the pair $(\boldsymbol{a}, \boldsymbol{a}^T \cdot \boldsymbol{s} + \mathrm{e})$, where integers $n, m \geq 1$, and $q \geq 2$.*

Definition 2 (Inhomogeneous Short Integer Solution Problem ($\mathbf{ISIS}_{n,m,q,\beta}$) [?]). *Given matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ with m uniformly random vectors $\boldsymbol{a}_i \in \mathbb{Z}_q^n$ and a uniformly random vector $\mathbf{u} \in \mathbb{Z}_q^n$, $\mathbf{ISIS}_{n,m,q,\beta}$ asks to find a vector $\boldsymbol{x} \in \Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A})$ such that $||\boldsymbol{x}|| \leq \beta$.*

3 Underlying Interactive Protocol

Our Stern-like [**?**] interactive argument system allows a signer (prover) to convince the verifier about his validity in zero-knowledge, that the signer is a valid group member that posses a signature generated using his secret key and both his revocation token and his index are correctly committed via an LWE function.

Let n be the security parameter and ℓ be the message length. Let modulus $q = \omega(n^2 \log n)$ be prime, dimension $m \geq 2n \log q$, and Gaussian parameter $\sigma = \omega(\sqrt{n \log q \log n})$. The infinity norm bound $\beta = \lceil \sigma \cdot \log m \rceil$ s.t $(4\beta + 1)^2 \leq q$ and norm bound for LWE noises is b s.t $q/b = \ell\tilde{\mathcal{O}}(n)$. Let $k_1 := m + \ell$ and $k_2 := n + m + \ell$.

- The common inputs: Matrices $\mathbf{A} = [\mathbf{A}_0|\mathbf{A}_1^0|\mathbf{A}_1^1|...|\mathbf{A}_\ell^0|\mathbf{A}_\ell^1] \in \mathbb{Z}_q^{n \times (2\ell+1)m}$, $\mathbf{B} \in \mathbb{Z}^{n \times m}$, $\mathbf{V} \in \mathbb{Z}_q^{m \times n}$, and $\mathbf{P} \in \mathbb{Z}_q^{k_1 \times k_2}$ and vectors $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{v} \in \mathbb{Z}_q^m$, and $\mathbf{c} \in \mathbb{Z}_q^{k_1}$.
- The prover's inputs: A vector $\mathbf{x} = (\mathbf{x}_0||\mathbf{x}_1^0||\mathbf{x}_1^1||...||\mathbf{x}_\ell^0||\mathbf{x}_\ell^1) \in \mathsf{Secret}_\beta(d)$ for some secret $d \in \{0,1\}^\ell$, vector $\mathbf{e}_1 \in \mathbb{Z}^m$, vector $\mathbf{r} \in \mathbb{Z}_q^n$, and a vector $\mathbf{e} \in \mathbb{Z}^{k_2}$. We use $\mathbf{f}$ instead of $\mathbf{e}_1$ hereunder to discard the confusing $\mathbf{e}_1$with $\mathbf{e}$.
- The prover's goal is to convince the verifier in zero-knowledge that:
  - $\mathbf{A} \cdot \mathbf{x} = \mathbf{u} \mod q$ and $\mathbf{x} \in \mathsf{Secret}_\beta(d)$.
  - $||\mathbf{f}||_\infty \leq \beta$ and $\mathbf{V} \cdot (\mathbf{B} \cdot \mathbf{r}) + \mathbf{f} = \mathbf{v} \mod q$. (Here the revocation token is created separately with a matrix $\mathbf{B}$ and a vector $\mathbf{r}$ instead of using $\mathbf{A}_0$ and $\mathbf{x}_0$).
  - $||\mathbf{e}||_\infty \leq b$ and $\mathbf{Pe} + (0^{k_1-\ell}||\lfloor q/2 \rfloor d) = \mathbf{c} \mod q$ (b is the norm bound for LWE noises and $\bar{p} = \lfloor \log b \rfloor + 1$).

Before the interaction, both the prover and the verifier form the public matrices: $\mathbf{A}^* \leftarrow \mathsf{MatrixExt}(\mathbf{A})$, $\mathbf{V}^* = \mathbf{V} \cdot \mathbf{B} \in \mathbb{Z}_q^{m \times m}$, $\mathbf{I}^* \in \{0,1\}^{m \times 3m}$ ($\mathbf{I}^*$ is obtained by appending *2m zero-columns* to the identity matrix of order m), $\mathbf{P}^* = [\mathbf{P} \mid 0^{k_1 \times 2k_2}] \in \mathbb{Z}_q^{k_1 \times 3k_2}$, and

$$Q = \left(\begin{array}{c|c} 0^{(k_1-\ell)\times\ell} & 0^{(k_1-\ell)\times\ell} \\ \hdashline \lfloor q/2 \rfloor \mathbf{I}_\ell & 0^{\ell\times\ell} \end{array}\right) \in \{0, \lfloor q/2 \rfloor\}^{k_1 \times 2\ell}.$$

Then the prover uses the Decomposition-Extension technique provided in [**?**] with his witness vectors as below.

- Let $\mathbf{z}_1, \ldots, \mathbf{z}_p \leftarrow \mathsf{WitnessDE}(\mathbf{x})$.
- Let $\tilde{\mathbf{f}}_1, \ldots, \tilde{\mathbf{f}}_p \leftarrow \mathsf{EleDec}(\mathbf{f})$, then for each $i \in [p]$, let $\mathbf{f}_i \leftarrow \mathsf{EleExt}(\tilde{\mathbf{f}}_i)$.
- Let $\tilde{\mathbf{r}}_1, \ldots, \tilde{\mathbf{r}}_p \leftarrow \mathsf{EleDec}(\mathbf{r})$, then for each $i \in [p]$, let $\mathbf{r}_i \leftarrow \mathsf{EleExt}(\tilde{\mathbf{r}}_i)$.
- Let $\tilde{\mathbf{e}}_1, \ldots, \tilde{\mathbf{e}}_{\bar{p}} \leftarrow \mathsf{EleDec}(\mathbf{e})$, then for each $i \in [p]$, let $\mathbf{e}_i \leftarrow \mathsf{EleExt}(\tilde{\mathbf{e}}_i)$.

At the interactive protocol, the prover instead convince the verifier that he knows $\mathbf{z}_1, \ldots, \mathbf{z}_p \in \mathsf{Secret}_\beta(d)$, $\tilde{\mathbf{f}}_1, \ldots, \tilde{\mathbf{f}}_p \in \mathsf{B}_{3m}$, $\tilde{\mathbf{r}}_1, \ldots, \tilde{\mathbf{r}}_p \in \mathsf{B}_{3m}$, and $\tilde{\mathbf{e}}_1, \ldots, \tilde{\mathbf{e}}_p \in \mathsf{B}_{3k_2}$, such that:

$$\begin{cases} \mathbf{A}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{z}_j) = \mathbf{u} \mod q; \\ \mathbf{V}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{r}_j) + \mathbf{I}^* \cdot (\sum_{j=1}^{P} \beta_j \cdot \mathbf{f}_j) = \mathbf{v} \mod q. \\ \mathbf{P}^* \cdot (\sum_{j=1}^{\bar{p}} b_j \cdot \mathbf{e}_j) + \mathbf{Q} \cdot d^* = \mathbf{Pe} + (0^{k_1-\ell}||\lfloor q/2 \rfloor d) = \mathbf{c} \mod q. \end{cases}$$

Description of the protocol:

1. **Commitment**: The prover samples randomness ρ_1, ρ_2, ρ_3 for COM and the following uniformly random objects:

$$\begin{cases} c \xleftarrow{\$} \{0,1\}^{\ell}; \\ \pi_{z,1}, \ldots, \pi_{z,p} \xleftarrow{\$} S; \pi_{f,1}, \ldots, \pi_{f,p} \xleftarrow{\$} S_{3m}; \pi_{r,1}, \ldots, \pi_{r,p} \xleftarrow{\$} S_{3m}; \\ \quad \pi_{e,1}, \ldots, \pi_{e,\bar{p}} \xleftarrow{\$} S_{3k_2}; \tau \xleftarrow{\$} S_{2\ell}; \\ \mathbf{k}_{z,1}, \ldots, \mathbf{k}_{z,p} \xleftarrow{\$} \mathbb{Z}_q^{(2\ell+1)3m}; \mathbf{k}_{f,1}, \ldots, \mathbf{k}_{f,p} \xleftarrow{\$} \mathbb{Z}_q^{3m}; \\ \quad \mathbf{k}_{r,1}, \ldots, \mathbf{k}_{r,p} \xleftarrow{\$} \mathbb{Z}_q^{3m}; \mathbf{k}_{e,1}, \ldots, \mathbf{k}_{e,\bar{p}} \xleftarrow{\$} \mathbb{Z}_q^{3k_2}; \mathbf{k}_d \xleftarrow{\$} \mathbb{Z}_q^{2\ell}. \end{cases} \tag{1}$$

Then the prover sends the following commitment $\mathbf{CMT} = (\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$ to the verifier.

$$\begin{cases} \mathbf{c}_1 = \mathsf{COM}(c, \{\pi_{z,j}, \pi_{f,j}, \pi_{r,j}\}_{j=1}^{p}), \mathbf{A}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{k}_{z,j}); \\ \quad \mathbf{V}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{k}_{r,j}) + \mathbf{I}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{k}_{f,j}); \\ \quad \{\pi_{e,j}, \}_{j=1}^{\bar{p}}; \mathbf{P}^*(\sum_{j=1}^{\bar{p}} b_j \mathbf{k}_{e,j}) + \mathbf{Q}\mathbf{k}_d; \tau; \rho_1), \\ \mathbf{c}_2 = \mathsf{COM}(\{T_c \circ \pi_{z,j}(\mathbf{k}_{z,j}), \pi_{f,j}(\mathbf{k}_{f,j}), \pi_{r,j}(\mathbf{k}_{r,j})\}_{j=1}^{p}; \\ \quad \{\pi_{e,j}(\mathbf{k}_{e,j})\}_{j=1}^{\bar{p}}; \tau(\mathbf{k}_d); \rho_2), \\ \mathbf{c}_3 = \\ \mathsf{COM}(\{T_c \circ \pi_{z,j}(\mathbf{z}_j + \mathbf{k}_{z,j}), \pi_{f,j}(\mathbf{f}_j + \mathbf{k}_{f,j}), \pi_{r,j}(\mathbf{r}_j + \mathbf{k}_{r,j})\}_{j=1}^{p}; \\ \quad \{\pi_{e,j}(\mathbf{e}_j + \mathbf{k}_{e,j})\}_{j=1}^{\bar{p}}; \tau(d^* + \mathbf{k}_d); \rho_3). \end{cases} \tag{2}$$

2. **Challenge:** The verifier sends a challenge $Ch \xleftarrow{\$} \{1,2,3\}$ to the prover.
3. **Response:** Depending on the challenge, the prover sends the response RSP computed as follows.
   - Case $Ch = 1$: Let $d_1 = d \oplus c$. For each $j \in [p]$, let $\mathbf{u}_{z,j} = T_c \circ \pi_{z,j}(\mathbf{z}_j); \mathbf{w}_{z,j} = T_c \circ \pi_{z,j}(\mathbf{k}_{z,j}); \mathbf{u}_{f,j} = \pi_{f,j}(\mathbf{f}_j); \mathbf{w}_{f,j} = \pi_{f,j}(\mathbf{k}_{f,j}); \mathbf{u}_{r,j} = \pi_{r,j}(\mathbf{r}_j); \mathbf{w}_{r,j} = \pi_{r,j}(\mathbf{k}_{r,j})$. For each $j \in [\bar{p}]$, let $\mathbf{u}_{e,j} = \pi_{e,j}(\mathbf{e}_j); \mathbf{w}_{e,j} = \pi_{e,j}(\mathbf{k}_{e,j})$. Let $\mathbf{u}_d = \tau(d^*); \mathbf{w}_d = \tau(\mathbf{k}_d)$. Then send,

$$RSP = (d_1, \{\mathbf{u}_{z,j}, \mathbf{w}_{z,j}, \mathbf{u}_{f,j}, \mathbf{w}_{f,j}, \mathbf{u}_{r,j}, \mathbf{w}_{r,j}\}_{j=1}^{p}, \\ \{\mathbf{u}_{e,j}, \mathbf{w}_{e,j}\}_{j=1}^{\bar{p}}, \mathbf{u}_d, \mathbf{w}_d, \rho_2, \rho_3). \tag{3}$$

   - Case $Ch = 2$: Let $d_2 = c$. For each $j \in [p]$, let $\phi_{z,j} = \pi_{z,j}; \phi_{f,j} = \pi_{f,j}; \phi_{r,j} = \pi_{r,j}; \mathbf{s}_{z,j} = \mathbf{z}_j + \mathbf{k}_{z,j}; \mathbf{s}_{f,j} = \mathbf{f}_j + \mathbf{k}_{f,j}; \mathbf{s}_{r,j} = \mathbf{r}_j + \mathbf{k}_{r,j}$. For each $j \in [\bar{p}]$, let $\phi_{e,j} = \pi_{e,j}; \mathbf{s}_{e,j} = \mathbf{e}_j + \mathbf{k}_{e,j}$. Let $\hat{\tau} = \tau$ and $\mathbf{s}_d = d^* + \mathbf{k}_d$. Then send,

$$RSP = (d_2, \{\phi_{z,j}, \phi_{f,j}, \phi_{r,j}, \mathbf{s}_{z,j}, \mathbf{s}_{f,j}, \mathbf{s}_{k,j}\}_{j=1}^{p}, \\ \{\phi_{e,j}, \mathbf{s}_{e,j}\}_{j=1}^{\bar{p}}, \hat{\tau}, \mathbf{s}_d, \rho_1, \rho_3) \tag{4}$$

- Case $Ch = 3$: Let $d_3 = c$. For each $j \in [p]$, let $\psi_{z,j} = \pi_{z,j}; \psi_{f,j} = \pi_{f,j}; \psi_{r,j} = \pi_{r,j}; \mathbf{h}_{z,j} = \mathbf{k}_{z,j}; \mathbf{h}_{f,j} = \mathbf{k}_{f,j}; \mathbf{h}_{r,j} = \mathbf{k}_{r,j}$. For each $j \in [\bar{p}]$, let $\psi_{e,j} = \pi_{e,j}; \mathbf{h}_{e,j} = \mathbf{k}_{e,j}$. Let $\tilde{\tau} = \tau$ and $\mathbf{h}_d = \mathbf{k}_d$. Then send,

$$\begin{aligned} RSP = (d_3, \{\psi_{z,j}, \psi_{f,j}, \psi_{r,j}, \mathbf{h}_{z,j}, \mathbf{h}_{f,j}, \mathbf{h}_{k,j}\}_{j=1}^{p}, \\ \{\psi_{e,j}, \mathbf{h}_{e,j}\}_{j=1}^{\bar{p}}, \tilde{\tau}, \mathbf{h}_d, \rho_1, \rho_2) \end{aligned} \quad (5)$$

4. Receiving the response RSP, the verifier proceeds as follows:
   - $Ch = 1$: Parse RSP as in (**??**).
     Check that $\forall \in [p] : \mathbf{u}_{z,j} \in \mathsf{SecretExt}(d_1), \mathbf{u}_{f,j} \in \mathsf{B}_{3m},\ \mathbf{u}_{r,j} \in \mathsf{B}_{3m}$, $\forall j \in [\bar{p}] : \mathbf{u}_d \in \mathsf{B}_{2\ell}, \mathbf{u}_{e,j} \in \mathsf{B}_{3k_2}$, and

$$\begin{cases} \mathbf{c}_2 = \mathsf{COM}(\{\mathbf{w}_{z,j}, \mathbf{w}_{f,j}, \mathbf{w}_{r,j}\}_{j=1}^{p}; \{\mathbf{w}_{e,j}\}_{j=1}^{\bar{p}}; \mathbf{w}_d; \rho_2), \\ \mathbf{c}_3 = \mathsf{COM}(\{\mathbf{u}_{z,j} + \mathbf{w}_{z,j}, \mathbf{u}_{f,j} + \mathbf{w}_{f,j}, \mathbf{u}_{r,j} + \mathbf{w}_{r,j}\}_{j=1}^{p}; \\ \qquad \{\mathbf{u}_{e,j} + \mathbf{w}_{e,j}\}_{j=1}^{\bar{p}}; \{\mathbf{u}_d + \mathbf{w}_d\}; \rho_3). \end{cases} \quad (6)$$

   - $Ch = 2$: Parse RSP as in (**??**). Check that :

$$\begin{cases} \mathbf{c}_1 = \mathsf{COM}(d_2, \{\phi_{z,j}, \phi_{f,j}, \phi_{r,j}\}_{j=1}^{p}, \mathbf{A}^*(\sum_{j=1}^{p} \beta_j \cdot \mathbf{s}_{z,j}) - \mathbf{u}; \\ \quad \mathbf{V}^*(\sum_{j=1}^{p} \beta_j \cdot \mathbf{s}_{r,j}) + \mathbf{I}^*(\sum_{j=1}^{p} \beta_j \cdot \mathbf{s}_{f,j}) - \mathbf{v}; \\ \quad \{\phi_{e,j}\}_{j=1}^{\bar{p}}; \mathbf{P}^* \cdot (\sum_{j=1}^{\bar{p}} b_j \cdot \mathbf{s}_{e,j}) + \mathbf{Q}\mathbf{s}_d - \mathbf{c}; \hat{\tau}; \rho_1), \\ \mathbf{c}_3 = \mathsf{COM}(\{T_{d_2} \circ \phi_{z,j}(\mathbf{s}_{z,j}), \phi_{f,j}(\mathbf{s}_{f,j}), \phi_{r,j}(\mathbf{s}_{r,j})\}_{j=1}^{p}; \\ \quad \{\phi_{e,j}(\mathbf{s}_{e,j})\}_{j=1}^{\bar{p}}; \hat{\tau}(\mathbf{s}_d); \rho_3). \end{cases} \quad (7)$$

   - $Ch = 3$:Parse RSP as in (**??**). Check that :

$$\begin{cases} \mathbf{c}_1 = \mathsf{COM}(d_3, \{\psi_{z,j}, \psi_{f,j}, \psi_{r,j}\}_{j=1}^{p}, \mathbf{A}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{h}_{z,j}); \\ \quad \mathbf{V}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{h}_{r,j}) + \mathbf{I}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{h}_{f,j}); \\ \quad \{\phi_{e,j}\}_{j=1}^{\bar{p}}; \mathbf{P}^* \cdot (\sum_{j=1}^{\bar{p}} b_j \cdot \mathbf{h}_{e,j}) + \mathbf{Q}\mathbf{h}_d; \tilde{\tau}; \rho_1), \\ \mathbf{c}_2 = \mathsf{COM}(\{T_{d_3} \circ \psi_{z,j}(\mathbf{h}_{z,j}), \psi_{f,j}(\mathbf{h}_{f,j}), \psi_{r,j}(\mathbf{h}_{r,j})\}_{j=1}^{p}; \\ \quad \{\psi_{e,j}(\mathbf{h}_{e,j}), \}_{j=1}^{\bar{p}}; \tilde{\tau}(\mathbf{h}_d); \rho_2). \end{cases} \quad (8)$$

The verifier outputs Valid if and only if all the conditions hold. Otherwise, he outputs Invalid.

4 Analysis of the protocol

Theorem 1. *Let* **COM** *be a statistically hiding and computationally binding string commitment scheme. The interactive protocol is a zero-knowledge argument of knowledge with perfect completeness and soundness error 2/3 with* $(\mathcal{O}(\ell m) \log \beta + \mathcal{O}(k_2) \log b) \log q$ *communication cost. Thus it satisfies the followings.*

- *There exists an efficient simulator that, on input* $(\mathbf{A}, \mathbf{u}, \mathbf{B}, \mathbf{V}, \mathbf{v}, \mathbf{P}, \mathbf{c})$*, outputs an accepted transcript which is statistically close to that produced by the real prover.*
- *There exists an efficient knowledge extractor that, on input a commitment CMT and 3 valid responses* $(RSP^{(1)}, RSP^{(2)}, RSP^{(3)})$ *corresponding to all 3 possible values of the challenging Ch, outputs vectors* $(\mathbf{y}, \mathbf{f}', \mathbf{r}', \mathbf{e}')$ *such that:*
  1. $\mathbf{y} = (\mathbf{y}_0||\mathbf{y}_1^0||\mathbf{y}_1^1||\dots||\mathbf{y}_\ell^0||\mathbf{y}_\ell^1) \in \mathsf{Secret}_\beta(d)$ *for some* $d \in \{0,1\}^\ell$*, and* $\mathbf{A} \cdot \mathbf{y} = \mathbf{u} \mod q$.
  2. $||\mathbf{f}'||_\infty \leq \beta$ *and* $\mathbf{V} \cdot (\mathbf{B} \cdot \mathbf{r}) + \mathbf{f}' = \mathbf{v} \mod q$.
  3. $||\mathbf{e}'||_\infty \leq b$ *and* $\mathbf{P}\mathbf{e}' + (0^{k_1-\ell}||\lfloor q/2 \rfloor d) = \mathbf{c} \mod q$.

4.1 Completeness and Soundness

An honest prover, with a valid witness $(\mathbf{x}, \mathbf{f}, \mathbf{r}, \mathbf{e})$ for some $d \in \{0,1\}^\ell$, can always obtain $\mathbf{z}_1, \dots, \mathbf{z}_p \in \mathsf{Secret}_\beta(d), \mathbf{f}_1, \dots, \mathbf{f}_p \in \mathsf{B}_{3m}, \mathbf{r}_1, \dots, \mathbf{r}_p \in \mathsf{B}_{3m}$, and $\mathbf{e}_1, \dots, \mathbf{e}_{\bar{p}} \in \mathsf{B}_{3k_2}$ via the Decomposition-Extension technique [?]. If he follows the protocol, he should always be accepted by the verifier. In this manner, the protocol has perfect completeness.

The protocol admits a soundness error 2/3, which is natural for typical Stern-like protocols. However, this error can be made negligible by repeating the protocol $t = \omega(\log n)$ times in parallel.

4.2 Communication Cost

The KTX scheme [?] COM outputs an element of $\mathbb{Z}_q^n$. Therefore the commitment CMT has bit-size $3n \log q = \tilde{\mathcal{O}}(n)$. The response RSP is executed by, p permutations in S, p permutations in S_{3m}, $\bar{p}$ permutations in S_{3k_2}, one permutation in 2ℓ, p vectors in $\mathbb{Z}_q^{(2\ell+1)3m}$, p vectors in $\mathbb{Z}_q^{3m}$, $\bar{p}$ vectors in $\mathbb{Z}_q^{3k_2}$, and one vector in $\mathbb{Z}_q^{2\ell}$.

In this manner, the bit size of RSP is bounded by $(\mathcal{O}(\ell m)p + \mathcal{O}(k_2)\bar{p}) \log q$, where $p = \lfloor \log \beta \rfloor + 1$ and $p = \lfloor \log b \rfloor + 1$. Thus the overall communication cost of the protocol is bounded by $(\mathcal{O}(\ell m) \log \beta + \mathcal{O}(k_2) \log b) \log q$.

4.3 Zero-Knowledge Property

If **COM** is statistically hiding, we can prove that, the interactive protocol is statistical zero-knowledge argument.

First, construct a PPT simulator *SIM* interacting with a verifier V such that, by giving only the public inputs, *SIM* outputs with probability close to 2/3 a simulated transcript that is statistically close to the outputs of an honest prover in the real interaction. From the public input ($\mathbf{A}$, $\mathbf{u}$, $\mathbf{B}$, $\mathbf{V}$, $\mathbf{v}$, $\mathbf{P}$, $\mathbf{c}$) given by the protocol, both *SIM* and V acquire matrices, $\mathbf{A}^*, \mathbf{V}^*$, $\mathbf{I}^*$, $\mathbf{P}^*$, and $\mathbf{Q}$. Then *SIM* starts simulation by selecting a random $\overline{Ch} \in \{1, 2, 3\}$. This is a prediction of the challenge value that V will not choose.

Case $\overline{Ch} = 1$: *SIM* computes the vectors $\mathbf{z}'_1, \ldots, \mathbf{z}'_p \in \mathbb{Z}_q^{(2\ell+1)3m}$ such that $\mathbf{A}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{z}'_j) = \mathbf{u} \mod q$, $\mathbf{r}'_1, \ldots, \mathbf{r}'_p \in \mathbb{Z}_q^{3m}$ and $\mathbf{f}'_1, \ldots, \mathbf{f}'_p \in \mathbb{Z}_q^{3m}$ such that $\mathbf{V}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{r}'_j) + \mathbf{I}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{f}'_j) = \mathbf{v} \mod q$, and $\mathbf{e}'_1, \ldots, \mathbf{e}'_{\bar{p}} \in \mathbb{Z}_q^{3k}$ and $d' \in \mathbb{Z}_q^{2\ell}$, such that $\mathbf{P}^* \cdot (\sum_{j=1}^{\bar{p}} b_j \cdot \mathbf{e}'_j) + \mathbf{Q} \cdot d' = \mathbf{c} \mod q$ by using linear algebra.

Then *SIM* samples objects as in equation (**??**) and sends commitment $\mathbf{CMT} = (\mathbf{c}'_1, \mathbf{c}'_2, \mathbf{c}'_3)$ to V, where

$$\begin{cases} \mathbf{c}'_1 = \mathsf{COM}(c, \{\pi_{z,j}, \pi_{f,j}, \pi_{r,j}\}_{j=1}^{p}, \mathbf{A}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{k}_{z,j}); \\ \qquad \mathbf{V}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{k}_{r,j}) + \mathbf{I}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{k}_{f,j}) \\ \qquad \{\pi_{e,j}\}_{j=1}^{\bar{p}}, \mathbf{P}^* \cdot (\sum_{j=1}^{\bar{p}} b_j \cdot \mathbf{k}_{e,j}) + \mathbf{Q}\mathbf{k}_d; \tau; \rho_1), \\ \mathbf{c}'_2 = \mathsf{COM}(\{T_c \circ \pi_{z,j}(\mathbf{k}_{z,j}), \pi_{f,j}(\mathbf{k}_{f,j}), \pi_{r,j}(\mathbf{k}_{r,j})\}_{j=1}^{p}; \\ \qquad \{\pi_{e,j}(\mathbf{k}_{e,j})\}_{j=1}^{\bar{p}}; \tau(\mathbf{k}_d); \rho_2), \\ \mathbf{c}'_3 = \mathsf{COM}(\{T_c \circ \pi_{z,j}(\mathbf{z}'_j + \mathbf{k}_{z,j}), \pi_{f,j}(\mathbf{f}'_j + \mathbf{k}_{f,j}), \pi_{r,j}(\mathbf{r}'_j + \mathbf{k}_{r,j})\}_{j=1}^{p}; \\ \qquad \{\pi_{e,j}(\mathbf{e}'_j + \mathbf{k}_{e,j})\}_{j=1}^{\bar{p}}; \tau(d' + \mathbf{k}_d); \rho_3). \end{cases} \tag{9}$$

For a challenge Ch from V, *SIM* responds as follows:
- If $Ch = 1$: Output $\perp$ and abort.
- If $Ch = 2$: Send,
RSP $= (c, \{\pi_{z,j}, \pi_{f,j}, \pi_{r,j}, \mathbf{z}'_j + \mathbf{k}_{z,j}, \mathbf{f}'_j + \mathbf{k}_{f,j}, \mathbf{r}'_j + \mathbf{k}_{r,j}\}_{j=1}^{p}$, $\{\pi_{e,j}, \mathbf{e}'_j + \mathbf{k}_{e,j}\}_{j=1}^{\bar{p}}, d' + \mathbf{k}_d, \tau, \rho_1, \rho_3)$.
- If $Ch = 3$: Send, RSP $= (c, \{\pi_{z,j}, \pi_{f,j}, \pi_{r,j}, \mathbf{k}_{z,j}, \mathbf{k}_{f,j}, \mathbf{k}_{r,j}\}_{j=1}^{p}$, $\{\pi_{e,j}, \mathbf{k}_{e,j}\}_{j=1}^{\bar{p}}, \tau, \rho_1, \rho_2)$.

Case $\overline{Ch} = 2$: *SIM* samples randomness ρ_1, ρ_2, ρ_3 for **COM** and

$$\begin{cases} \hat{d} \xleftarrow{\$} \{0,1\}^{\ell}, c \xleftarrow{\$} \{0,1\}^{\ell}; d' \xleftarrow{\$} \mathsf{B}_{2\ell}; \\ \mathbf{z}'_1, \ldots, \mathbf{z}'_p \xleftarrow{\$} \mathsf{SecretExt}(d); \mathbf{f}'_1, \ldots, \mathbf{f}'_p \xleftarrow{\$} \mathsf{B}_{3m}; \mathbf{r}'_1, \ldots, \mathbf{r}'_p \xleftarrow{\$} \mathsf{B}_{3m}; \\ \qquad \mathbf{e}'_1, \ldots, \mathbf{e}'_{\bar{p}} \xleftarrow{\$} \mathsf{B}_{3k}; \\ \pi_{z,1}, \ldots, \pi_{z,p} \xleftarrow{\$} S; \pi_{f,1}, \ldots, \pi_{f,p} \xleftarrow{\$} S_{3m}; \pi_{r,1}, \ldots, \pi_{r,p} \xleftarrow{\$} S_{3m}; \\ \qquad \pi_{e,1}, \ldots, \pi_{e,\bar{p}} \xleftarrow{\$} S_{3k}; \\ \mathbf{k}_{z,1}, \ldots, \mathbf{k}_{z,p} \xleftarrow{\$} \mathbb{Z}_q^{(2\ell+1)3m}; \mathbf{k}_{f,1}, \ldots, \mathbf{k}_{f,p} \xleftarrow{\$} \mathbb{Z}_q^{3m}; \mathbf{k}_{r,1}, \ldots, \mathbf{k}_{r,p} \xleftarrow{\$} \mathbb{Z}_q^{3m}; \\ \qquad \mathbf{k}_{e,1}, \ldots, \mathbf{k}_{e,\bar{p}} \xleftarrow{\$} \mathbb{Z}_q^{3k}; \mathbf{k}_d \xleftarrow{\$} \mathbb{Z}_q^{2\ell}, \tau \xleftarrow{\$} S_{2\ell}. \end{cases}$$

Next *SIM* forms and sends commitment CMT as the same manner as in (**??**).

For a challenge Ch from V, *SIM* responds as follows:
- If $Ch = 1$: $(\hat{d} \oplus c \; \{T_c \circ \pi_{z,j}(\mathbf{z}'_j), T_c \circ \pi_{z,j}(\mathbf{k}_{z,j}), \pi_{f,j}(\mathbf{f}'_j), \pi_{f,j}(\mathbf{k}_{f,j}),$ $\pi_{r,j}(\mathbf{r}'_j), \pi_{r,j}(\mathbf{k}_{r,j})\}_{j=1}^{p}, \{\pi_{e,j}(\mathbf{e}'_j), \pi_{e,j}(\mathbf{k}_{e,j})\}_{j=1}^{\bar{p}}, \tau(d'), \tau(\mathbf{k}_d))$.
- If $Ch = 2$: Output $\perp$ and abort.
- If $Ch = 3$: Send, RSP computed as in the case $(\overline{Ch} = 1, Ch = 3)$.

Case $\overline{Ch} = 3$: *SIM* samples randomness as in $\overline{Ch} = 2$ and sends the commitment $\mathbf{CMT} = (\mathbf{c}_1', \mathbf{c}_2', \mathbf{c}_3')$ to V, where $\mathbf{c}_2', \mathbf{c}_3'$ are computed as in (**??**), and

$$\mathbf{c}_1' = \mathsf{COM}\ (c, \{\pi_{z,j}, \pi_{e,j}, \pi_{r,j}\}_{j=1}^{p}, \mathbf{A}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot (\mathbf{z}_j' + \mathbf{k}_{z,j})) - \mathbf{u};$$
$$\mathbf{V}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot (\mathbf{r}_j' + \mathbf{k}_{r,j})) + \mathbf{I}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot (\mathbf{f}_j' + \mathbf{k}_{f,j})) - \mathbf{v};$$
$$\{\pi_{e,j}\}_{j=1}^{\bar{p}}; \mathbf{P}^* \sum_{j=1}^{\bar{p}} b_j(\mathbf{e}_j' + \mathbf{k}_{e,j}) + \mathbf{Q}(d' + \mathbf{k}_d) - \mathbf{c}; \tau; \rho_1).$$

For a challenge Ch from V, *SIM* responds as follows:
- If $Ch = 1$: Send, RSP computed as in the case $(\overline{Ch} = 2, Ch = 1)$.
- If $Ch = 2$: Send, RSP computed as in the case $(\overline{Ch} = 1, Ch = 2)$.
- If $Ch = 3$: Output $\perp$ and abort.

Since **COM** is statistically hiding, the distribution of the commitment CMT and the distribution of the challenge Ch from V for every case considered above are statistically close to those in the real interaction. Hence, the probability that the simulator outputs $\perp$ is negligibly close to 1/3. Thus, the simulator *SIM* can successfully imitate the honest prover with probability negligibly close to 2/3.

4.4 Argument of Knowledge

Here we prove that, if COM is computationally binding, then the given protocol is an argument of knowledge. For a given commitment CMT and three valid responses $RSP^{(1)}, RSP^{(2)}, RSP^{(3)}$ to all three possible values of the challenge Ch, a valid witness can be extracted.

$$\begin{cases}
\mathbf{c}_1 & = \mathsf{COM}(d_2, \{\phi_{z,j}, \phi_{f,j}, \phi_{r,j}\}_{j=1}^{p}, \mathbf{A}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{s}_{z,j}) - \mathbf{u}; \\
& \qquad \mathbf{V}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{s}_{r,j}) + \mathbf{I}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{s}_{f,j}) - \mathbf{v}; \\
& \qquad \{\phi_{e,j}\}_{j=1}^{\bar{p}}; \mathbf{P}^* \cdot (\sum_{j=1}^{\bar{p}} b_j \cdot \mathbf{s}_{e,j}) + \mathbf{Q}\mathbf{s}_d - \mathbf{c}; \hat{\tau}; \rho_1) \\
& = \mathsf{COM}(d_3, \{\psi_{z,j}, \psi_{f,j}, \psi_{r,j}\}_{j=1}^{p}, \mathbf{A}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{h}_{z,j}); \\
& \qquad \mathbf{V}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{h}_{r,j}) + \mathbf{I}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot \mathbf{h}_{f,j}); \\
& \qquad \{\psi_{e,j}\}_{j=1}^{\bar{p}}; \mathbf{P}^* \cdot (\sum_{j=1}^{\bar{p}} b_j \cdot \mathbf{h}_{e,j}) + \mathbf{Q}\mathbf{h}_d; \tilde{\tau}; \rho_1), \\
\mathbf{c}_2 & = \mathsf{COM}(\{\mathbf{w}_{z,j}, \mathbf{w}_{f,j}, \mathbf{w}_{r,j}\}_{j=1}^{p}, \{\mathbf{w}_{e,j}\}_{j=1}^{\bar{p}}, \mathbf{w}_d; \rho_2) \\
& = \mathsf{COM}(\{T_{d_3} \circ \psi_{z,j}(\mathbf{h}_{z,j}), \psi_{f,j}(\mathbf{h}_{f,j}), \psi_{r,j}(\mathbf{h}_{r,j})\}_{j=1}^{p}; \\
& \qquad \{\psi_{e,j}(\mathbf{h}_{e,j})\}_{j=1}^{\bar{p}}, \tilde{\tau}(\mathbf{h}_d); \rho_2), \\
\mathbf{c}_3 & = \mathsf{COM}(\{\mathbf{u}_{z,j} + \mathbf{w}_{z,j}, \mathbf{u}_{f,j} + \mathbf{w}_{f,j}, \mathbf{u}_{r,j} + \mathbf{w}_{r,j}\}_{j=1}^{p}; \\
& \qquad \{\mathbf{u}_{e,j} + \mathbf{w}_{e,j}\}_{j=1}^{\bar{p}}, \{\mathbf{u}_d + \mathbf{w}_d\}; \rho_3) \\
& = \mathsf{COM}(\{T_{d_2} \circ \phi_{z,j}(\mathbf{s}_{z,j}), \phi_{f,j}(\mathbf{s}_{f,j}), \phi_{r,j}(\mathbf{s}_{r,j})\}_{j=1}^{p}; \\
& \qquad \{\phi_{e,j}(\mathbf{s}_{e,j})\}_{j=1}^{\bar{p}}, \hat{\tau}(\mathbf{s}_d); \rho_3).
\end{cases}$$

The computational binding property of **COM** implies that:

$$\begin{cases} d_2 = d_3; \\ \mathbf{u}_d \in \mathsf{B}_{2\ell}; \hat{\tau} = \tilde{\tau}; \mathbf{w}_d = \tilde{\tau}(\mathbf{h}_d); \mathbf{u}_d + \mathbf{w}_d = \hat{\tau}(\mathbf{s}_d); \\ \forall j \in [p] : \phi_{z,j} = \psi_{z,j}; \mathbf{w}_{z,j} = T_{d_2} \circ \phi_{z,j}(\mathbf{h}_{z,j}) \ and \\ \qquad \mathbf{u}_{z,j} + \mathbf{w}_{z,j} = T_{d_2} \circ \phi_{z,j}(\mathbf{s}_{z,j}); \\ \forall j \in [p] : \phi_{f,j} = \psi_{f,j}; \mathbf{w}_{f,j} = \phi_{f,j}(\mathbf{h}_{f,j}) \ and \ \mathbf{u}_{f,j} + \mathbf{w}_{f,j} = \phi_{f,j}(\mathbf{s}_{f,j}); \\ \forall j \in [p] : \phi_{r,j} = \psi_{r,j}; \mathbf{w}_{r,j} = \phi_{r,j}(\mathbf{h}_{r,j}) \ and \ \mathbf{u}_{r,j} + \mathbf{w}_{r,j} = \phi_{r,j}(\mathbf{s}_{r,j}); \\ \forall j \in [\bar{p}] : \phi_{e,j} = \psi_{e,j}; \mathbf{w}_{e,j} = \phi_{e,j}(\mathbf{h}_{e,j}) \ and \ \mathbf{u}_{e,j} + \mathbf{w}_{e,j} = \phi_{e,j}(\mathbf{s}_{e,j}); \\ \mathbf{A}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot (\mathbf{s}_{z,j} - \mathbf{h}_{z,j})) = \mathbf{u} \mod q; \\ \mathbf{V}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot (\mathbf{s}_{r,j} - \mathbf{h}_{r,j})) + \mathbf{I}^* \cdot (\sum_{j=1}^{p} \beta_j \cdot (\mathbf{s}_{f,j} - \mathbf{h}_{f,j})) = \mathbf{v} \mod q; \\ \mathbf{P}^* \cdot (\sum_{j=1}^{\bar{p}} b_j \mathbf{s}_{e,j}) + \mathbf{Q}\mathbf{s}_d - \mathbf{c} = \mathbf{P}^* \cdot (\sum_{j=1}^{\bar{p}} b_j \mathbf{h}_{e,j}) + \mathbf{Q}\mathbf{h}_d \mod q. \end{cases}$$

For each $j \in [p]$, let $\mathbf{y}'_j = (\mathbf{s}_{z,j} - \mathbf{h}_{z,j})$. Then $T_{d_2} \circ \phi_{z,j}(\mathbf{y}'_j) = T_{d_2} \circ \phi_{z,j}(\mathbf{s}_{z,j}) - T_{d_2} \circ \phi_{z,j}(\mathbf{h}_{z,j}) = \mathbf{u}_{z,j} \in \mathsf{SecretExt}(d_1)$. Thus, $\phi_{z,j}(\mathbf{y}'_j) \in \mathsf{SecretExt}(d_1 \oplus d_2)$. Let $\bar{d} = d_1 \oplus d_2$, then for all $j \in [p]$, $\mathbf{y}'_j \in \mathsf{SecretExt}(\bar{d})$, since the permutation $\phi_{z,j} \in S$ preserves the arrangements of the blocks of $\mathbf{y}'_j$. By removing the last $2m$ coordinates in each $3m$-block of $\mathbf{y}'$ obtain vectors $\mathbf{y}' \sum_{j=1}^{p} \beta_j \cdot \mathbf{y}'_j \in \mathbb{Z}_q^{(2\ell+1)3m}$, and $\mathbf{y} \in \mathbb{Z}^{(2\ell+1)m}$. Now we can declare

$$||\mathbf{y}||_\infty \leq ||\mathbf{y}'||_\infty \leq \sum_{j=1}^{p} \beta_j \cdot ||\mathbf{y}_j||_\infty = \sum_{j=1}^{p} \beta_j \cdot 1 = \beta.$$

Moreover, since $\mathbf{y}'_j \in \mathsf{SecretExt}(\bar{d})$ for all $j \in [p]$, we have that $\mathbf{y} \in \mathsf{Secret}_\beta(\bar{d})$ and, $\mathbf{A} \cdot \mathbf{y} = \mathbf{A}^* \cdot \mathbf{y}' = \mathbf{A}^* \cdot \sum_{j=1}^{p} \beta_j \cdot \mathbf{y}_j = \mathbf{A}^*(\sum_{j=1}^{p} \beta_j \cdot (\mathbf{s}_{z,j} - \mathbf{h}_{z,j})) = \mathbf{u} \mod q$.

For each $j \in [p]$, let $\mathbf{f}'_j = (\mathbf{s}_{f,j} - \mathbf{h}_{f,j})$. Then $\phi_{f,j}(\mathbf{f}'_j) = \phi_{f,j}(\mathbf{s}_{f,j}) - \phi_{e,j}(\mathbf{h}_{f,j}) = \mathbf{u}_{f,j} \in \mathsf{B}_{3m}$, which implies that $\mathbf{f}'_j \in \mathsf{B}_{3m}$. Let $\hat{\mathbf{f}} = \sum_{j=1}^{p} \beta_j \cdot \mathbf{f}'_j \in \mathbb{Z}^{3m}$ and by dropping the last $2m$ coordinates from $\hat{\mathbf{f}}$ obtain $\mathbf{f}' \in \mathbb{Z}^m$. We can declare,

$$||\mathbf{f}'||_\infty \leq ||\hat{\mathbf{f}}||_\infty \leq \sum_{j=1}^{p} \beta_j \cdot ||\mathbf{f}'_j||_\infty = \sum_{j=1}^{p} \beta_j \cdot 1 = \beta.$$

Moreover, for each $j \in [p]$, let $\mathbf{r}'_j = (\mathbf{s}_{r,j} - \mathbf{h}_{r,j})$. Then $\phi_{r,j}(\mathbf{r}'_j) = \phi_{r,j}(\mathbf{s}_{r,j}) - \phi_{r,j}(\mathbf{h}_{r,j}) = \mathbf{u}_{r,j} \in \mathsf{B}_{3m}$, which implies that $\mathbf{r}'_j \in \mathsf{B}_{3m}$. Let $\hat{\mathbf{r}} = \sum_{j=1}^{p} \beta_j \cdot \mathbf{r}'_j \in \mathbb{Z}^{3m}$ and by dropping the last $2m$ coordinates from $\hat{\mathbf{r}}$ obtain $\mathbf{r}' \in \mathbb{Z}^m$. We can declare,

$$||\mathbf{r}'||_\infty \leq ||\hat{\mathbf{r}}||_\infty \leq \sum_{j=1}^{p} \beta_j \cdot ||\mathbf{r}'_j||_\infty = \sum_{j=1}^{p} \beta_j \cdot 1 = \beta.$$

We can obtain the relation:

$$\mathbf{V}^* \cdot \hat{\mathbf{r}} + \mathbf{I}^* \cdot \hat{\mathbf{f}} = \mathbf{v} \mod q \iff \mathbf{V}^* \cdot (\mathbf{B} \cdot \mathbf{r}') + \mathbf{f}' = \mathbf{v} \mod q.$$

Let $d^* = \mathbf{s}_d - \mathbf{h}_d = \hat{\tau}^{-1}(\mathbf{u}_d)$. Then it follows that $d^* \in \mathsf{B}_{2\ell}$. Now let $d^* = (d_1, \ldots, d_\ell, d_{\ell+1}, \ldots, d_{2\ell})$ and let $d = (d_1, \ldots, d_\ell) \in 0, 1^\ell$.

For each $j \in [\bar{p}]$, let $\mathbf{e}'_j = (\mathbf{s}_{e,j} - \mathbf{h}_{e,j})$. Then $\phi_{e,j}(\mathbf{e}'_j) = \phi_{e,j}(\mathbf{s}_{e,j}) - \phi_{e,j}(\mathbf{h}_{e,j}) = \mathbf{u}_{e,j} \in \mathsf{B}_{3k}$, which implies that $\mathbf{e}'_j \in \mathsf{B}_{3k}$. Let $\hat{\mathbf{e}} = \sum_{j=1}^{\bar{p}} b_j \cdot \mathbf{e}'_j$ and by dropping the last $2k$ coordinates from $\hat{\mathbf{e}}$ obtain $\mathbf{e}' \in \mathbb{Z}^k$. We can declare,

$$||\mathbf{e}'||_\infty \leq ||\hat{\mathbf{e}}||_\infty \leq \sum_{j=1}^{\bar{p}} b_j \cdot ||\mathbf{e}'_j||_\infty = \sum_{j=1}^{p} b_j \cdot 1 = b.$$

Now, $||\mathbf{e}'||_\infty \leq b$, and $\mathbf{P}^*\mathbf{e}' + \mathbf{Q}d^* = \mathbf{P}\mathbf{e}' + (0^{k-\ell}||\lfloor q/2 \rfloor d) = \mathbf{c} \mod q$.

In conclusion, the constructed efficient knowledge extractor which satisfies all the conditions stated in Theorem **??** outputs vectors $(\mathbf{y}, \mathbf{f}', \mathbf{r}', \mathbf{e}')$.The vector $\mathbf{f}'(\mathbf{e}_1)$ can extract from $\mathbf{e}$. But, for the ease of understanding and to reduce the complexity we prove the witness of $\mathbf{f}'(\mathbf{e}_1)$ and extraction separately.

5 Conclusion

This paper presents a combined interactive protocol that signer can use to prove his validity of signing, his revocation token which is generated separately without deriving from secret signing key is not in the revocation list, and his index is correctly encrypted. Since the proofs in proposed protocol not relying on each other this can be used in any scheme with slight modifications. For instance, the schemes like [**?**] can use the proposed protocol by adding member registration.

Acknowledgments. This work is supported in part by JSPS Grant-in-Aids for Scientic Research (A) JP16H01705 and for Scientic Research (B) JP17H01695.

References

1. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: ACM 2008. pp. 197–206. ACM (2008)
2. Kawachi, A., Tanaka, K., Xagawa, K.: Concurrently secure identification schemes based on the worst-case hardness of lattice problems. In: ASIACRYPT 2008, LNCS. vol. 5350, pp. 372–389. Springer (2008)
3. Langlois, A., Ling, S., Nguyen, K., Wang, H.: Lattice-based group signature scheme with verifier-local revocation. In: PKC 2014, LNCS. vol. 8383, pp. 345–361. Springer (2014)
4. Ling, S., Nguyen, K., Stehle, D., Wang, H.: Improved zero-knowledge proofs of knowledge for isis problem, and applications. PKC volume 7778 of *LNCS*, pages 107–124 (2013)
5. Peikert, C.: A decade of lattice cryptography. Foundations and Trends in Theoretical Computer Science 10(4), 283–424 (2016), https://doi.org/10.1561/0400000074
6. Perera, M.N.S., Koshiba, T.: Achieving almost-full security for lattice-based fully dynamic group signatures with verifier-local revocation. In: ISPEC 2018, LNCS (to appear)
7. Stern, J.: A new paradigm for public key identification. IEEE Transactions on Information Theory 42(6), 1757–1768 (1996)