Efficient Zero-Knowledge Arguments for Some Matrix Relations over Rings and Non-malleable Enhancement

Yuan Tian

[1] Software School, Dalian University of Technology, Dalian, Liao Ning, P.R.China,
tianyuan_ca@dlut.edu.cn

Abstract Various matrix relations widely appeared in data-intensive computations, as a result their efficient zero-knowledge proofs/arguments are naturally required in large-scale private computing applications. In the first part of this paper, we concretely establish efficient zero-knowledge arguments for linear matrix relation **AU** = **B** and bilinear relation $\mathbf{U}^{\mathrm{T}}\mathbf{QV}$ = **Y** over the residue ring Z_m with logarithmic message complexity. We take a direct, matrix-oriented (rather than vector-oriented in usual) approach to such establishments on basis of the elegant commitment scheme over finite ring recently established by Attema et al[16]. The constructed commit-and-proof protocols are public-coin and in c.r.s paradigm (c.r.s used only as the public-key of the commitment scheme), suitable for any size matrices and significantly outperform the protocols constructed in usual approach with smaller-sized c.r.s.(e.g., decreased by a factor of d for linear and by n^2d for bilinear relation where d is the extension degree of Galois ring and n is the order of the witness square), fewer rounds (decreased by a fraction > log$d$/2log$n$ for linear and > 1/2 for bilinear relation) and lower message complexity (e.g., number of ring elements decreased by a fraction > log$d$/log$n$ for linear and >1/6 for bilinear relation) for large-size squares. The on-line computational complexities are almost the same in both approaches. In the second part, on basis of the simulation-sound tag-based trapdoor commitment scheme we establish a general compiler to transform any public coin proof/argument protocol into the one which is concurrently non-malleable with unchanged number of rounds, properly increased message and computational complexity. Such enhanced protocols, e.g., the versions compiled from those constructed in the first part of this work, can run in parallel while keeping all their security properties, particularly resisting man-in-the-middle attacks.

Keywords: Zero-Knowledge, Linear Matrix Equation, Bilinear Matrix Equation, ∑-Protocol, Concurrent Non-malleability, Galois Ring.

1 Introduction

1.1 Basic Problems and Related Works

Efficient zero-knowledge proofs for various relations are crucial techniques to support multiparty private computing tasks[1,2], secure distributed ledger systems[3,4,5] and many other cryptographic applications. In data-intensive private computation, lots of data relations appear in the form of high dimensional vector or large-size matrix equations[3,4] and efficient zero-knowledge proof/argument protocols (ZKP/ZKA) with low message complexity are highly valuable to support these applications in complicated network environment.

Recently, some innovative techniques have been developed in [6,7] to construct highly efficient ZKAs for linear vector relation $\boldsymbol{a}^{\mathrm{T}}\boldsymbol{u}=b$ and inner product relation $\boldsymbol{u}^{\mathrm{T}}\boldsymbol{v} = w$ over finite field. The constructed ZKAs have message complexity of only O(log$n$) where n is the dimension of witness space, significantly improving previous works in performance. This approach was further developed in [8] to construct ZKA for vectors' quadratic relation $\boldsymbol{u}^{\mathrm{T}}\mathbf{A}\boldsymbol{u}+\boldsymbol{b}^{\mathrm{T}}\boldsymbol{u}=c$ over finite field with logarithmic message complexity and lots of other improvements in performance. This approach was also applied to constructing ZKAs with logarithmic message complexity for bilinear relations on groups with pairing structure[9,10] and partial-knowledge proofs[11].

The critical idea initiated in [6,7] for compressing the argument is on basis of an observation that the normally constructed commit-and-proof arguments (for relations discussed there) have some intrinsic recursive structure. With the aid of homomorphism of the commitment scheme and smart witness space decomposition, such recursive structure can be used to expand the original arguments to multiple rounds. In such expansion the total message complexity is highly compressed while the number of rounds only increases as slowly as the logarithm of the dimension of witness space. Such idea was generalized in [12] within the widely used Σ-protocol framework and a very general theory for linear and nonlinear relations was henceforth established.

After succeeding in developing efficient ZKAs for linear vector relations over finite field, it is natural to establish efficient ZKAs for nonlinear relations over finite field and other arithmetic systems, e.g., finite rings Z_m or integer ring Z.

In the first direction, bilinear relation is the simplest non-linear relation which efficient ZKA construction was partially solved, e.g., [6-8] has established the protocols with logarithmic message complexity in some special cases. More specifically, the protocols constructed in [6,7] are only for inner-product relation, and the protocols in [8] are only for quadratic relation with 1-rank coefficient matrix. So far with the author's knowledge there is no direct work on bilinear relation $\boldsymbol{u}^{\mathrm{T}}\mathbf{Q}\boldsymbol{v} = y$ with general $\mathbf{Q}$ or with witnesses not only $\boldsymbol{u}$ and $\boldsymbol{v}$ but also $\mathbf{Q}$ and y. These relations naturally appear in contemporary cryptographic applications. For non-linear relations, so far the most common and effective approach is linearization[12]. In this approach, any relation over the finite field can be equivalently transformed into a (maybe very high dimensional) linear relation through secrete sharing techniques. On the other hand, as indicated in [9], the compilation from nonlinear to linear relation comes at the price of losing conceptual simplicity and modularity in protocol design. Therefore, developing direct approach for specific non-linear relation is still useful in cryptography theory and applications. [9-11] are heuristic examples in this direction.

In the second direction, recently a ZKA with polynomial-logarithmic message complexity was constructed in [13] for a linear relation over the integer ring Z. [16] established a family of general and elegant commitment schemes for vectors over Galois ring, and the ZKA with logarithmic message complexity is constructed by generalizing techniques in [12] for linear relations over the ring. The ZKA for any nonlinear relation over Galois ring can be also constructed via the linearization approach and related techniques developed in multiparty private computation over the ring. However, a straightforward generalization of ZKA construction from the finite field to finite ring does not sufficiently make use of all flexibilities provided by this scheme. There are new and interesting problems for applying this new commitment scheme in ZKA-construction, even for linear relations.

Contributions Our contributions in this paper have two parts. In the first part (Sec. 3 and 4) we concretely establish efficient commit-and-proof zero-knowledge argument (ZKA) protocols for linear matrix relation $\mathbf{AU} = \mathbf{B}$ and bilinear relation $\mathbf{U^TQV} = \mathbf{Y}$ over the residue ring Z_m with logarithmic message complexity. In private computing applications various data relations can be represented by or reduced to some matrix relation, e.g., the (private) isomorphic relation between two lattices or graphs; multiplicative, inverse or similarity relations between two private matrices, etc. In addition, Z_m is one of the most widely used arithmetic systems in practice. One of the main challenges in constructing ZKA protocols for relations over a ring is how to ensure sufficient number of challenges to fulfill the necessary soundness requirements. This is elegantly achieved in [16] by committing over the extended ring S, which elements are polynomials of some finite degree d over Z_m. As a direct result, a Z_m-vector is regarded as a special S-vector and the ZKA protocol for a relation over Z_m is simply constructed as a ZKA protocol for a relation over S, by generalizing techniques (e.g., amortization, compression, etc.) from Galois fields to Galois rings. However, in private computing applications, what is actually needed is to prove relations over, e.g., Z_m, rather than over its extension S, so when establishing the ZKA protocol for a matrix relation this vector-oriented approach (dealing with a matrix just as a collection of vectors) is not as efficient as desired.

We take a matrix-oriented approach on basis of an observation that a n-dimensional vector over the Galois ring S can be effectively related with a Z_m-matrix in various ways. For example, by re-arranging a large-size, n-by-td Z_m-matrix $\mathbf{U}$ to be a nt-by-d matrix $\mathbf{U}^*$, it can be equivalently regarded as a nt-dimensional S-vector $\boldsymbol{u}^*$ so its commitment can be always valued in G^d, i.e., its commitment size can be independent of its total size and only determined by the targeted knowledge-error in ZKA. Furthermore, how to transform the original relation for **matrices** over Z_m into an equivalent relation for the correspondent **vectors** over S while keeping the commitment size fixed (e.g., d) or as slowly-increasing as possible is crucial to make use of these observations. This is simple in linear case but technically involved in non-linear case. Details are elaborated in sec. 3 and 4.

Our matrix-oriented approach to ZKA for matrix relations is able to deal with Z_m-matrix in any size. The constructed protocols have almost the same on-line computational complexity as those constructed in vector-oriented approach. It begins to outperform the vector-oriented approach when number of columns > log(number of rows) with smaller c.r.s, shorter commitments, fewer rounds and lower message complexity. For example, for linear relation with the witness of n-by-n Z_m-matrix, number of rounds can be reduced from $4\log n$ to $4\log n - 2\log d$ and message complexity can be reduced from $4d\log n$ to $4d\log n - 2d\log d$(for number of group elements) and from $6d\log n$ to $6d\log n - 3d\log d$(for number of ring elements). In addition, the number of group elements in c.r.s can be reduced by a factor of d (see tab. 1 & 2 in sec.3). For bilinear matrix relation, the matrix-oriented approach also outperforms the general linearization approach in almost all aspects, e.g., the number of rounds can be reduced by > 1/2; size of c.r.s. reduced by > n^2d times; total number of ring elements in messages reduced by > 1/6 and total number of group elements asymptotically the same but decreased by $4d\log d$ (n is the number of rows in the witness square, see tab. 3 & 4 in sec.4). Such advantages are not only helpful for interactive but also for non-interactive argument constructions. This is a result of making use of specific structural features of the commitment scheme and matrix equations. The same approach can also deal with more complicated matrix relations such as eigenvalue relation $\mathbf{U}\boldsymbol{a} = \lambda\boldsymbol{a}$, $\mathbf{AUB}^T = \mathbf{C}$, $\mathbf{U}^T\mathbf{QV} + \mathbf{AUB}^T + \mathbf{CVD}^T = \mathbf{R}$(with witnesses **U** and **V**) with similar performance advantages.

All constructed protocols in this paper are public-coin and in c.r.s paradigm, where the c.r.s is only used as the commitment scheme's public key.

In the second part (Sec.5), on basis of the general and formal public-coin protocol structure, we establish a general compiler to transform any such proof/argument protocol into the protocol which is *concurrently non-malleable* with unchanged number of rounds, properly increased message and computational complexity (by nearly constant times). The innovative approach developed in [20-22] for 3-round protocols is generalized to multi-round public-coin protocols via some recent analysis and results in [13]. The basic tool is the simulation-sound trap-door commitment scheme introduced in [20-22]. Such enhanced protocols, e.g., all the enhanced versions of protocols in sec. 3 and 4, can run in parallel environment while keeping all its security properties, particularly resisting man-in-the-middle attacks.

Some Notes on Terminologies In second part of our work, we simply inherit the terminology *non-malleability* from [22] but it is strictly weaker than the "*non-malleability*" in [20-21] which is actually equivalent to *universal composability*. In addition, "*tag-based*" and "*simulation soundness*" for the trapdoor commitment scheme are terminologies inherited from [20] which are similar (but not exactly the same) as the properties proposed in [22] in different names.

2 Preliminaries

Notations and Conventions λ usually represents the security parameter, poly(λ) represents a polynomial in λ. A function $\varepsilon(\lambda)$ is called *asymptotically negligible* or simply negligible if $\lim_{\lambda\to\infty} poly(\lambda)\varepsilon(\lambda) = 0$.

P.P.T. means Probabilistic Polynomial Time.

$u\overset{R}{\leftarrow}J$ means a random variable u is sampled on a set J under uniform distribution.

Two random variable ensembles $\{X_\lambda\}$ and $\{Y_\lambda\}$ are called *statistically indistinguishable* if the differences of their distribution is negligible:

$$\sum_u |P[X_\lambda = u] - P[Y_\lambda = u]| \le \varepsilon(\lambda)$$

$\{X_\lambda\}$ and $\{Y_\lambda\}$ are called *computationally indistinguishable* if for any P.P.T. algorithm A the following inequality holds where the function $\varepsilon(\lambda)$ is negligible.

$$|P[A(X_\lambda)=1] - P[A(Y_\lambda)=1]| \le \varepsilon(\lambda)$$

2.1 Zero-knowledge Proofs/Arguments

A binary relation R is NP-class if there exists a polynomial-time algorithm A to decide whether (x,w) is in R. $L_R \equiv \{ x$: there exists $(x,w) \in R\}$.

In an interactive proof system (P,V) where P and V are P.P.T prover and verifier, σ represents the common reference string(c.r.s.), x represents the public information for P and V, w represents the private information only for P, i.e., the witness, $<P(w);\underline{V}>_\sigma(x)$ represents the output of V valued in {0,1} after the interaction with P on input x and c.r.s. σ, $Tr<P,V>_\sigma(x)$ the trace during the interaction between P and V. These notations have the same meaning for any interactive algorithms A and B.

Definition 1 (**Zero-knowledge Proof**) For a relation R and some given function $\kappa(\lambda)$, an interactive proof system (P,V) is defined as a *zero-knowledge proof of knowledge* for R, **ZKPoK** hereafter, if it has all the following properties:
(1) **Complete** For any $(x,w) \in R$ there holds $P[<P(w);\underline{V}>_\sigma(x) = 1] = 1$.
(2) **Knowledge-sound with knowledge-error $\kappa(\lambda)$** There exists a polynomial q(.) and an algorithm Ext (called *extractor*) with expected polynomial time complexity, such that for any (maybe dishonest) prover P^* which can be rewound by Ext there holds

$$P[w^* \leftarrow Ext^{P^*}(\sigma, x, Tr<P^*,V>_\sigma(x)): (x,w^*) \in R] \ge (\mu(x) - \kappa(|x|))/q(|x|)$$

where $\mu(x) \equiv P[<P^*;\underline{V}>_\sigma(x)=1] \ge \kappa(|x|)$.
(3) **Zero-knowledge** There exists a P.P.T. algorithm S, called *simulator*, such that for any (maybe dishonest) verifier V^*, the output of $S(\sigma,x)$ and $Tr<P,V^*>_\sigma(x)$ are statistically indistinguishable for any $x \in L_R$.

For knowledge soundness, there is an equivalent definition ([18] sec. 4.7) that on input of x and $Tr<P^*,V>_\sigma(x)$ with $<P^*,\underline{V}>_\sigma(x)=1$ and Ext can rewind P^*, Ext outputs a witness w^*: $(x,w^*) \in R$ with the expected time at most $q(|x|)/(\mu(x)-\kappa(|x|))$.

If knowledge soundness only holds for P.P.T. prover P^*, the proof system is called *knowledge argument*, notated by **ZKAoK** hereafter.

Definition 2 (**∑-Protocol and generalized ∑-Protocol**) An interactive proof system (P,V) for relation R is called a ∑-protocol, if it has 3 rounds with the first message from P to V and the second message just being a random coin from V to P independent of the session context.

An interactive proof system (P,V) for relation R is called a *generalized* ∑-protocol, if it has $2k+1$ rounds with the first message from P to V and any messages from V to P just being random coins independent of each other and session context.

A generalized ∑-protocol for relation R is called *special honest verifier zero-knowledge* (**SHVZK**) if there exists a P.P.T. algorithm S such that for any verifier V^*, the real trace $Tr<P,V^*>_\sigma(x)$ and the output of S on input $(\sigma,x;e_1,...,e_k)$ have the same distribution for any $x \in L_R$ and independent random coins $e_1,...,e_k$.

Definition 3 (**($\mu_1,\ldots,\mu_k$)-special soundness and session-tree for a generalized ∑-Protocol**) A ($\mu_1,\ldots,\mu_k$)-*session-tree*, denoted by $T_\sigma(x)$, for the proof system of relation R with c.r.s. σ is a tree in which:

(1) Each node is associated with a message instance from P to V in the interaction between P and V with public information x, in particular the root is with the first message in the interaction.

(2) Each edge is a random coin from V to P.

(3) At level-i (the root being at level-1) each node α has μ_i edges and the random coin instances $e_{\alpha/1},\ldots, e_{\alpha/\mu i}$ associated with these edges are distinct. The downstream node of each edge is associated with the message instance of P in response to the random coin.

Each integer μ_i is called the *soundness factor* of the i-th round.

Obviously, each path from the root to a leaf in the tree $T_\sigma(x)$ is a complete session instance, i.e., a trace. The number of paths in a tree $T_\sigma(x)$ is $\mu_1\ldots\mu_k$. If the verifier V outputs 1 on all these paths, the tree $T_\sigma(x)$ is called ***accepting***.

A generalized ∑-protocol is called ($\mu_1,\ldots,\mu_k$)-*special sound*, if there exists a P.P.T. algorithm (*extractor*) which with overwhelming probability outputs a witness w^*: $(x,w^*)\in R$ on input of σ, x and the accepting tree $T_\sigma(x)$.

Recently [13] proved a fundamental fact that ($\mu_1,\ldots,\mu_k$)-soundness implies knowledge soundness, a general fact without imposing any restrictions on the challenge set where the random coins are sampled.

2.2 Commitment Scheme

Definition 4 (**Commitment Scheme**) A Commitment scheme CS ≡ (CGen, Cmt, Cvf) is composed of three P.P.T. algorithms with the following properties:

(1) **Complete** For any message x there holds

$$P[pk\leftarrow \mathrm{CGen}(\lambda);\ (c,d)\leftarrow \mathrm{Cmt}(pk,x):\ \mathrm{Cvf}(pk,c,x,d)=1]=1$$

(2) **Binding** There exists a negligible function $\varepsilon(\lambda)$ s.t. for any P.P.T. algorithm A:

$$P[pk\leftarrow \mathrm{CGen}(\lambda);(c,x_1,x_2,d_1,d_2)\leftarrow A(pk):\mathrm{Cvf}(pk,c,x_1,d_1)=1\wedge \mathrm{Cvf}(pk,c,x_2,d_2)=1\wedge x_1\neq x_2]\leq\varepsilon(\lambda)$$

(3) **Hiding** For any pk generated by CGen and any messages x_1, x_2 in the same size, the variables c_1 : $(c_1,d_1)\leftarrow \mathrm{Cmt}(pk,x_1)$ and c_2 : $(c_2,d_2)\leftarrow \mathrm{Cmt}(pk,x_2)$ has the same distribution.

2.3 Basic Facts about Galois Ring

Formally, a Galois ring is a finite ring with multiplicative unit 1 such that all of its zero divisors (including 0) forms a principal ideal ($p1$) for some prime number p.

One of the most important examples for Galois ring is the residue ring Z_m where $m = p^s$ and p is a prime number. Another important example is $Z_m[X]/(f(X))$ where Z_m is as before and $f(X)$ is a monic irreducible polynomial of degree d over Z_m. This ring is the extended ring of Z_m of degree d, notated as GR(m,d) hereafter.

The most important facts about Galois ring useful in this paper are stated here. All details and proofs can be seen, e.g., in Chapter 14 of [17], particularly its theorem 14.1, 14.6, 14.8 and lemma 14.20 and 14.29.

Fact 1 Let S be a Galois ring of characteristic p^s (i.e., $p^s1 = 0$ and $N1 \neq 0$ for any integer $N \neq 0 \bmod p^s$) and cardinality p^{sd} where p is a prime, s and d are positive integers. Then S is isomorphic to the ring GR(m,d) ≡ $Z_m[X]/(f(X))$ for $m = p^s$ and any irreducible polynomial $f(X)$ of degree d over Z_m.

Fact 2 In Galois ring GR(m,d) ≡ $Z_m[X]/(f(X))$ with $m = p^s$:

(1) There is an element ξ of order p^d-1 such that $f(\xi) = 0$ and $f(X)$ is the unique monic polynomial of degree $\leq d$ over Z_m with ξ as its root .

(2) $X^{p^{d-1}}$ - 1 = 0 mod $f(X)$ and X^N -1 $\neq$ 0 mod $f(X)$ for $0<N<p^d-1$.

(3) GR(m,d) = $Z_m[\xi] \equiv \{a_0+a_1\xi+ a_2\xi^2+\ldots+ a_{d-1}\xi^{d-1}$: $a_0, a_1, a_2,\ldots,a_{d-1}$ in Z_m }

(4) Let $E_{GR(m,d)} \equiv \{\xi^i$: $i = 0,1,2,\ldots, p^d-2\}$ then any u in GR(m,d) has a unique p-adic representation as

$$u = A_0 + A_1p + A_2p^2 + \ldots + A_{s-1}p^{s-1}$$

with each A_i in $E_{GR(m,d)}\cup\{0\}$. Furthermore, u is invertible in GR(m,d) iff $A_0\neq0$.

(4) $E_{GR(m,d)}$ is called the *exceptional set* of Galois ring G(m,d). $E_{GR(m,d)}$ is a cyclic multiplicative group of order p^d-1 and is isomorphic to the multiplicative subgroup of finite field F_{p^d}. ξ^i - ξ^j is in $E_{GR(m,d)}$ for any $i\neq j$, i.e., ξ^i - ξ^j is always invertible in GR(m,d).

(5) $f(X)$ has roots ξ, ξ^p, ξ^{p^2} ,…, $\xi^{p^{d-1}}$in GR(m,d).

Fact 3 Let S be GR(m,d) and $l < p^d$-1, then any non-identically zero polynomial $\varphi(X)\in S[X]$ of degree $\leq l$ cannot have more than l roots in the exceptional set E_S.

Fact 4 Let S be GR(m,d) with $m = p^s$, $\bar{S}$ be S/(p) and h be a monic polynomial in S[X]. If there are pairwise coprime monic polynomials $\overline{g_1}$,…, $\overline{g_r}$ in $\bar{S}$ [X] such that $h = \overline{g_1}\ldots\overline{g_r}$ mod (p), then there exist pairwise coprime monic polynomials g_1, …, g_r in S[X] such that $f = g_1\ldots g_r$ and $g_i = \overline{g_\iota}$ mod (p) for each i.

Although the commitment schemes established in [16] is not limited to ring Z_m or its extensions with special m, in this paper we only consider Z_m and its extensions GR(m,d) with $m = p^s$ where p = 2 or any odd prime, the most important Galois ring family in applications.

2.4 Vector Commitments over Galois Ring

Attema T., et al in [16] established a family of general and elegant commitment schemes for vectors over any finite ring. Let S be GR(m,d) ≡ $Z_m[X]/(f(X))$ and $\boldsymbol{u}$ be a n-dimensional S-vector, i.e.,

$$\boldsymbol{u} = \begin{bmatrix} u_1(X) \\ \cdot \\ \cdot \\ u_n(X) \end{bmatrix} \in S^n \tag{2.1}$$

where each component $u_k(X)$ ∈S is a polynomial $u_1(k)+u_2(k)X+u_3(k)X^2+\ldots+u_d(k)X^{d-1}$. Let R be the set on which to select the random element for hiding, then the commitment to $\boldsymbol{u}$ is an element in product group G^d where G is the commitment-friendly group, e.g., $G = Z_N^*$ (for m odd) or $J^+(N)$ (for m even) with some strong RSA module N (detailed discussions on G are in sec.3.2[16]). The commitment to $\boldsymbol{u}$ is computed by:

$$\mathrm{Cmt}(\sigma|\boldsymbol{u};\boldsymbol{r}) = \begin{bmatrix} \mathrm{cmt}_\sigma(u_1(1),\ldots,u_1(n);r_1) \\ \cdot \\ \cdot \\ \mathrm{cmt}_\sigma(u_d(1),\ldots,u_d(n);r_d) \end{bmatrix} \in G^d\text{: } S^n\times R^d \rightarrow G^d \quad (2.2)$$

where $\mathrm{cmt}_\sigma(\boldsymbol{w};r)$: $Z_m^n \times R \rightarrow G$ is a basic commitment scheme for any n-dimensional Z_m-vector $\boldsymbol{w}$. A general method is provided to construct the basic scheme $\mathrm{cmt}_\sigma(.;.)$ in [16] to ensure the properties of unconditional completeness, perfect hiding and computational binding. Specifically, given the commitment key $\sigma \equiv [G, \boldsymbol{g}, m]$ with $\boldsymbol{g} \equiv (g_1,\ldots,g_n)$ being group elements[1], for $\boldsymbol{w} = [w_1,\ldots,w_n] \in Z_m^n$ with m odd then:

$$\mathrm{cmt}_\sigma(\boldsymbol{w};r) = r^m\boldsymbol{g}[\boldsymbol{w}] \equiv r^m g_1^{w_1}\ldots g_n^{w_n} \text{ where } r\in R \quad (2.3)$$

For m even:

$$\mathrm{cmt}_\sigma(\boldsymbol{w};r) = r^m(-1)^b\boldsymbol{g}[\boldsymbol{w}] \equiv r^m(-1)^b g_1^{w_1}\ldots g_n^{w_n} \text{ where } (b,r)\in\{0,1\}\times R \quad (2.4)$$

Note that we denote $g_1^{w_1}\ldots g_n^{w_n}$ as $\boldsymbol{g}[\boldsymbol{w}]$, $g_1^e\ldots g_n^e$ as $\boldsymbol{g}[e]$ to simplify the expressions.

Besides security properties, homomorphism is also crucial for these commitment scheme's applications. It is straightforward to show that (2.3) and (2.4) have the usual homomorphism properties required for a commitment. Furthermore, scheme $\mathrm{Cmt}(\sigma|.;.)$: $S^n\times R^d \rightarrow G^d$ has a algebraic property useful in protocol construction.

Lemma 1 Let e be in Galois ring $S=GR(m,d)\equiv Z_m[X]/(f(X))$ and $M_e\in Z_m^{d\times d}$ be its associated matrix, i.e., for any

$$u = u_1+u_2X+u_3X^2+\ldots+u_dX^{d-1}\in S$$

there holds

$$eu = \sum_{i=1}^d\left(\sum_{j=1}^d M_e(i,j)u_j\right)X^{i-1} \bmod f(X) \quad (2.5)$$

Also let

$$\mathrm{Cmt}(\sigma|\boldsymbol{u};\boldsymbol{r}) = \begin{bmatrix} C_1 \\ \cdot \\ \cdot \\ C_d \end{bmatrix} \in S^d$$

and $\boldsymbol{u}$ be the S-vector in (2.1), then

[1] Each g_i is the m-th power of some element in G, as a result the commitment to any message is always in G^m(except for a random factor -1 in case of even m) [16].

$$\mathrm{Cmt}(\sigma|\boldsymbol{eu};\, \boldsymbol{s}) = \begin{bmatrix} \prod_{j=1}^{d} C_j^{M_e(1,j)} \\ \cdot \\ \cdot \\ \prod_{j=1}^{d} C_j^{M_e(d,j)} \end{bmatrix} \qquad (2.6)$$

where $\boldsymbol{s}$ can be efficiently computed from $\boldsymbol{u}$, $\boldsymbol{r}$, e[2] and is uniformly distributed if $\boldsymbol{r}$ or e are uniformly distributed. Equality (2.6) is denoted as $\mathrm{Cmt}(\sigma|\boldsymbol{eu};\boldsymbol{s}) = \mathrm{Cmt}(\sigma|\boldsymbol{u};\, \boldsymbol{s})^e$.

Proof For each k =1,…, n let

$$u_k = \sum_{j=1}^{d} u_j\,(k)X^{j-1}$$

so by (2.5) one has $eu_k = \sum_{i=1}^{d}(\sum_{j=1}^{d} M_e\,(i,j)u_j(k))X^{i-1}$ mod $f(X)$, hence

$$\boldsymbol{eu} = \begin{bmatrix} \sum_{i=1}^{d}(\sum_{j=1}^{d} M_e\,(i,j)u_j(1))X^{i-1} \\ \cdot \\ \cdot \\ \sum_{i=1}^{d}(\sum_{j=1}^{d} M_e\,(i,j)u_j(n))X^{i-1} \end{bmatrix}$$

$$= \begin{bmatrix} \sum_{j=1}^{d} M_e(1,j)u_j(1), \dots\dots, \sum_{j=1}^{d} M_e(d,j)u_j(1) \\ \cdot \\ \cdot \\ \sum_{j=1}^{d} M_e(1,j)u_j(n), \dots\dots, \sum_{j=1}^{d} M_e(d,j)u_j(n) \end{bmatrix} \begin{bmatrix} 1 \\ X \\ \cdot \\ X^{d-1} \end{bmatrix}$$

$$= \begin{bmatrix} u_1(1) & \cdots & u_d(1) \\ \vdots & \ddots & \vdots \\ u_1(n) & \cdots & u_d(n) \end{bmatrix} \begin{bmatrix} M_e(1,1) & \cdots & M_e(d,1) \\ \vdots & \ddots & \vdots \\ M_e(1,d) & \cdots & M_e(d,d) \end{bmatrix} \begin{bmatrix} 1 \\ X \\ \cdot \\ X^{d-1} \end{bmatrix} = \boldsymbol{W} \begin{bmatrix} 1 \\ X \\ \cdot \\ X^{d-1} \end{bmatrix} \bmod f(X)$$

where the Z_m-matrix $\boldsymbol{W} = \mathbf{UM}_e^{\mathbf{T}} = [\boldsymbol{u}_1,\dots,\boldsymbol{u}_d]\mathbf{M}_e^{\mathbf{T}} \equiv [\boldsymbol{w}_1,\dots,\boldsymbol{w}_d]$ with column vectors $\boldsymbol{w}_k$:

$$\boldsymbol{w_k} = \sum_{j=1}^{d} M_e\,(k,j)\boldsymbol{u}_j \quad k=1,\dots,d$$

By commitment scheme cmt_σ's homomorphism property, the k-th component of $\mathrm{Cmt}(\sigma|\boldsymbol{eu})$ is (for simplicity we omit all random numbers' expressions):

$$\mathrm{Cmt}(\sigma|\boldsymbol{eu})_k = \mathrm{cmt}_\sigma(\boldsymbol{w_k}) = \mathrm{cmt}_\sigma(\sum_{j=1}^{d} M_e\,(k,j)\boldsymbol{u}_j) = \prod_{j=1}^{d} cmt_\sigma\,(\boldsymbol{u_j})^{M_e(k,j)}$$

$$\text{i.e., } \mathrm{Cmt}(\sigma|\boldsymbol{eu})_k = \prod_{j=1}^{d} Cmt\,(\sigma|\boldsymbol{u})_j^{M_e(k,j)}$$

which proves (2.6).

Remark 1 This result was basically established in [16] and lemma 2.1 presents it in a more explicit formulism (2.6). Furthermore, when the commitment (2.2) to a S-vector $\boldsymbol{u}$ in (2.1) is equivalently regarded as a commitment to a Z_m-matrix

$$\mathbf{U} = \begin{bmatrix} u_1(1) & \cdots & u_d(1) \\ \vdots & \ddots & \vdots \\ u_1(n) & \cdots & u_d(n) \end{bmatrix} \in Z_m^{n\times d}$$

[2] For simplicity, here and in the following arguments we always omit the long expressions for random objects which can be easily derived from basic formulas in sec.3.1 in [16].

and denoted by Cmt(σ|**U**), then (2.6) implies

$$\mathrm{Cmt}(\sigma|\mathbf{U}\mathbf{M}_e^{\mathbf{T}}) = \mathrm{Cmt}(\sigma|\mathbf{U})^e \qquad (2.7)$$

This view of equalizing S-vectors and Z_m-matrices is useful in the following work.

2.5 Probabilistic Equivalence Reduction

Two relations R(α;u) and S(β;v) (where α, β are public information while u, v are witnesses) are called *probabilistically equivalent* with each other if there exists negligible functions $\varepsilon_1(\lambda)$ and $\varepsilon_2(\lambda)$ such that

$$P[\ R(\alpha;u)\ |\ S(\beta;v)] \geq 1\text{-}\ \varepsilon_1(\lambda) \ \text{ and } \ P[\ S(\beta;v)\ |\ R(\alpha;u)] \geq 1\text{-}\ \varepsilon_2(\lambda)$$

This equivalence is denoted by $R(\alpha;u)\overset{P}{\leftrightarrow}S(\beta;v)$. Usually one of $\varepsilon_1(\lambda)$ or $\varepsilon_2(\lambda)$ is 0, i.e., the reduction is deterministic in one direction but probabilistic in the other.

Let the reduction from R to S is deterministic, i.e., P[S(β;v)| R(α;u)]=1, while on the other direction it is probabilistic: P[R(α;u) | S(β;v_ρ)] ≥ 1- $\varepsilon_1(\lambda)$ where ρ is a random variable. If there exists a P.P.T. algorithm A which can compute the witness u of R from at most m witnesses $v_{\rho 1},\ldots, v_{\rho m}$ of S with overwhelming probability, we say this reduction has *soundness factor m* and denote this fact by $R \overset{P/m}{\longleftrightarrow} S$.

Some detailed analysis and useful examples of probabilistic reduction in zero-knowledge proofs for relations in Galois fields can be seen in [12]. Fact 3 in sec. 2.3 is the foundation to generalize these techniques from Galois fields to Galois rings.

3 Efficient ZKA Protocol for Matrix Relation AU = B

Consider the matrix equation **AU** = **B** in residue ring Z_m where matrices $\mathbf{U}\in Z_m^{n\times h}$, $\mathbf{A}\in Z_m^{l\times n}$ and $\mathbf{B}\in Z_m^{l\times h}$. Both n and h are sufficiently large and $h = td$ for some integer t. The extension degree of Galois ring S over Z_m is d and determined by p^{-d} log$n$ < the target knowledge error. Matrix **U** is the witness while **A** and **B** are public.

3.1 Basics

To present the main idea explicitly, let's consider the case t =1 at first, i.e., **AU** = **B** in residue ring Z_m where matrices $\mathbf{U}\in Z_m^{n\times d}$, $\mathbf{A}\in Z_m^{l\times n}$ and $\mathbf{B}\in Z_m^{l\times d}$. There is no performance advantage in this case in comparison with the standard, vector-oriented approach. The objective of this section is to present the main ideas and techniques in our matrix-oriented approach.

In order to construct an efficient proof protocol with commitment to Z_m-matrix **U**, the first step is to find some relation over S which is equivalent to the original linear matrix relation over Z_m.

For S ≡ $Z_m[X]/(f(X))$ = GR(m,d) with degree-d irreducible monic polynomial $f(X)$ and matrix $\mathbf{A}\in Z_m^{l\times n}$, define a S-linear operator:

$$\mathbf{L}_A\text{: } S^n \to S^l\text{: } L_A(\boldsymbol{u})_i \equiv \textstyle\sum_{k=1}^{n} a_{ik}\, u_k(X) \bmod f(X),\ i = 1,\ldots, l \qquad (3.1)$$

where $u_k(X)\in S$ is the k-th component of vector $\boldsymbol{u}$ in S^n.

For the Z_m-matrices

$$\mathbf{U} = \begin{bmatrix} u_1(1) & \cdots & u_d(1) \\ \vdots & \ddots & \vdots \\ u_1(n) & \cdots & u_d(n) \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} b_1(1) & \cdots & b_d(1) \\ \vdots & \ddots & \vdots \\ b_1(l) & \cdots & b_d(l) \end{bmatrix} \qquad (3.2)$$

and each $i = 1,\ldots, l$, $k = 1,\ldots, n$, let:

$$b_i(X) \equiv \sum_{j=1}^{d} b_j(i)\, X^{j-1} = b_1(i) + b_2(i)X + \cdots + b_d(i)X^{d-1}$$

$$u_k(X) \equiv u_1(k) + u_2(k)X + \cdots + u_d(k)X^{d-1}$$

Regard $\mathbf{U}$ and $\mathbf{B}$ as vectors with components $u_k(X)$'s and $b_i(X)$'s in S, the corresponding S-vectors are:

$$\boldsymbol{u} = \begin{bmatrix} u_1(X) \\ \cdot \\ \cdot \\ u_n(X) \end{bmatrix} \in S^n, \ \boldsymbol{b} = \begin{bmatrix} b_1(X) \\ \cdot \\ \cdot \\ b_l(X) \end{bmatrix} \in S^l \qquad (3.3)$$

This correspondence is very useful and can be transformed by:

$$\boldsymbol{u} = \mathbf{U}\begin{bmatrix} 1 \\ X \\ X^2 \\ \cdot \\ X^{d-1} \end{bmatrix}, \ \boldsymbol{b} = \mathbf{B}\begin{bmatrix} 1 \\ X \\ X^2 \\ \cdot \\ X^{d-1} \end{bmatrix} \qquad (3.4)$$

Then for the S-vector $\boldsymbol{u}$ corresponding to Z_m-matrix $\mathbf{U}$ in (3.2) one has, for each i:

$$\mathrm{L}_{\mathrm{A}}(\boldsymbol{u})_i = \sum_{k=1}^{n} a_{ik}\, u_k(X) = \sum_{j=1}^{d}\Big(\sum_{k=1}^{n} a_{ik}\, u_j\,(k)\Big)X^{j-1} \bmod f(X)$$

As a result, it's easy to show the fact that:

$$\mathbf{L}_{\mathrm{A}}(\boldsymbol{u}) = \boldsymbol{b} \text{ over S}$$

$$\text{if and only if } \sum_{k=1}^{n} a_{ik}u_j\,(k) = b_j(i) \text{ for all } i, j, \text{ i.e., } \mathbf{AU} = \mathbf{B} \text{ over } Z_m \qquad (3.5)$$

Based on the fact (3.5), the problem of constructing a ZKA protocol for a linear matrix relation over Z_m can be transformed into a problem of constructing a ZKA protocol for a linear relation over Galois ring S. For this purpose, we define a formal linear relation over S.

Let Galois ring S ≡ GR(m,d), let σ be the public key of the S-vector commitment scheme and be used as c.r.s. of the proof protocol. The commitment is valued in product group G^d where G is commitment-friendly. The linear relation **SLR** on space S^n is defined as(all variables in the frame stand for witnesses):

$$\mathbf{SLR}(\sigma|\ U, \boldsymbol{b}, \mathbf{A}; \boxed{\boldsymbol{r}, \boldsymbol{u}}): \qquad (3.6)$$

$$U = \mathrm{Cmt}(\sigma|\boldsymbol{u}; \boldsymbol{r}) \wedge \mathbf{L}_{\mathrm{A}}(\boldsymbol{u}) = \boldsymbol{b}$$

where $\mathbf{L}_{\mathrm{A}}$ is defined in (3.1) with $\mathbf{A}\in Z_m^{l\times n}$, $\boldsymbol{b}\in S^l$; witnesses $\boldsymbol{u}$ is a n-dimensional S-vector, $\boldsymbol{r}$ is a d-dimensional random vector with components in set R.

In the above formulation, the commitment to S-vector $\boldsymbol{u}$

$$U=\mathrm{Cmt}(\sigma|\boldsymbol{u};\boldsymbol{r})=\mathrm{Cmt}(\sigma|\begin{bmatrix} u_1(1) & \cdots & u_d(1) \\ \vdots & \ddots & \vdots \\ u_1(n) & \cdots & u_d(n) \end{bmatrix}, \begin{bmatrix} r_1 \\ . \\ . \\ r_d \end{bmatrix})=\begin{bmatrix} \mathrm{cmt}_\sigma(u_1(1),\dots,u_1(n);r_1) \\ . \\ . \\ \mathrm{cmt}_\sigma(u_d(1),\dots,u_d(n);r_d) \end{bmatrix}$$

can be reasonably regarded as the commitment to Z_m-matrix $\mathbf{U}$, so also notated as $\mathrm{Cmt}(\sigma|\mathbf{U};\boldsymbol{r})$. All these basics are summarized in theorem 1 which is the starting point to construct ZKA protocol for linear matrix relation in Z_m .

Theorem 1 The linear matrix relation over Z_m :

$$\mathbf{MLR}(\sigma|U, \mathbf{B}, \mathbf{A}; \boxed{\boldsymbol{r}, \mathbf{U}}):$$

$$U= \mathrm{Cmt}(\sigma|\mathbf{U};\boldsymbol{r}) \wedge \mathbf{AU} = \mathbf{B} \qquad (3.7)$$

with $\mathbf{U}\in Z_m^{n\times d}$(witness), $\mathbf{A}\in Z_m^{l\times n}$, $\mathbf{B}\in Z_m^{l\times d}$ is equivalent to the linear relation over Galois ring S = GR(m,d) = $Z_m[X]/(f(X))$:

$$\mathbf{SLR}(\sigma| V, \boldsymbol{b}, \mathbf{L}_A; \boxed{\boldsymbol{r}, \boldsymbol{u}}):$$

$$V= \mathrm{Cmt}(\sigma|\boldsymbol{u};\boldsymbol{r}) \wedge \mathbf{L}_A(\boldsymbol{u}) = \boldsymbol{b} \qquad (3.8)$$

where $\boldsymbol{u}\in S^n$(witness), $\mathbf{L}_A$ is the linear operator defined in (3.1), $b_i=\sum_{j=1}^{d} b_j(i)X^{j-1}$ and $V = U$. These two relations' witnesses have the simple correspondence

$$\mathbf{U} \cong \boldsymbol{u}$$

where ≅ means that n-dimensional S-vectors $\boldsymbol{u}$ is equivalently regarded as a n-by-d matrix in Z_m (see (3.2)~(3.4).

3.2 Compressed Protocol with Logarithmic Message Complexity

S-linear relation SLR in (3.8) is the starting point to construct the efficient proof protocol for linear Z_m-matrix relation MLR in (3.7). However, $\mathbf{L}_A(\boldsymbol{u}) = \boldsymbol{b}$ in (3.8) is actually a system of l linear equations in S. For the sake of efficiency, this equation system can be further reduced to just one linear equation via standard probabilistic equivalence reduction techniques.

Define a polynomial $\varphi(T)$ as

$$\varphi(T) \equiv \sum_{i=1}^{l}(\mathrm{L}_A(\boldsymbol{u})_i - b_i)T^{i-1} \in S[T] \qquad (3.9)$$

Let ρ be randomly sampled from the exceptional set E_S in ring S. If there exists a $\boldsymbol{u}\in S^n$ such that $\mathbf{L}_A(\boldsymbol{u}) = \boldsymbol{b}$, i.e., $\mathrm{L}_A(\boldsymbol{u})_i = b_i$ for each i = 1,…, l, then

$$\sum_{i=1}^{l}(\mathrm{L}_A(\boldsymbol{u})_i - b_i)\rho^{i-1} = \varphi(\rho) = 0$$

On the other hand, if $\varphi(\rho) = 0$ for φ defined in (3.9) and ρ in E_S, then ρ is a zero of $\varphi(T)$ in E_S. Since $\varphi(T)$ has at most l-1 zeroes in E_S, for S ≡ GR(m,d), $m = p^s$ and $l < p^d$ one has the conclusion that $\varphi(T) \equiv 0$ with probability > $1 - lp^{-d}$. Since $\varphi(T) \equiv 0$ implies $\mathbf{L}_A(\boldsymbol{u}) = \boldsymbol{b}$, we have got the following result:

Theorem 2 Linear relation **SLR**(σ|V, $\boldsymbol{b}$, $\mathbf{L}_{\mathrm{A}}$**;** $\boxed{\boldsymbol{r}, \boldsymbol{u}}$) in (3.8) is probabilistically equivalent to the linear relation (3.10) with soundness factor l:

$$\text{sl-R}(\sigma|\ V, \boldsymbol{b}, l_{A,\rho}; \boxed{\boldsymbol{r}, \boldsymbol{u}}):$$

$$V = \mathrm{Cmt}(\sigma|\boldsymbol{u};\boldsymbol{r}) \wedge l_{\mathrm{A},\rho}(\boldsymbol{u}) = b_\rho \tag{3.10}$$

where $b_\rho \equiv \sum_{i=1}^{l} b_{\mathrm{i}}\rho^{i-1} \in \mathrm{S}$ and the S-linear functional $l_{\mathrm{A},\rho}$ is defined as

$$l_{\mathrm{A},\rho}(\boldsymbol{w}) \equiv \sum_{i=1}^{l} \sum_{k=1}^{n} a_{ik}\, w_k\, \rho^{i-1}: \mathrm{S}^n \rightarrow \mathrm{S}$$

The efficient protocol for linear Z_m-matrix relation (3.7) can now be constructed equivalently for the simple S-linear relation (3.10), via compressed techniques [6,7,12]. In fact, [16] has presented such a protocol framework with O(log$n$) message complexity and provided detailed analysis about its completeness, zero-knowledge and knowledge soundness properties so we don't repeat it here.

3.3 Vector-oriented Approach and Comparisons

According to the basic result in [16], for $n = 2^k$ the compressed protocol for matrix relation **AU = B** in Z_m is $2k$+1 round, complete, (2,3,…,3)-special sound henceforth knowledge sound with knowledge error $\leq kp^{-d}$ and total message complexity O(dk).

A standard, vector-oriented approach to constructing the efficient protocol for **AU = B** is the amortization method. Let $\mathbf{U} = [\boldsymbol{u}_1,\ldots,\boldsymbol{u}_d]$ and B= $[\boldsymbol{b}_1,\ldots,\boldsymbol{b}_d]$ where columns $\boldsymbol{u}_i \in Z_m^n$, $\boldsymbol{b}_i \in Z_m^l$, then **AU = B** is a system of d linear equations $\mathbf{A}\boldsymbol{u}_i = \boldsymbol{b}_i$. For any randomness ρ in $\mathrm{E}_{\mathrm{S},}$ it is equivalently reduced to a single vector equation:

$$\mathbf{A}\boldsymbol{u}_\rho = \boldsymbol{b}_\rho \text{ where } \boldsymbol{u}_\rho = \sum_{i=1}^{d} \boldsymbol{u}_i\, \rho^{i-1} \in S^n,\ \ \boldsymbol{b}_\rho = \sum_{i=1}^{d} \boldsymbol{b}_i\, \rho^{i-1} \in S^l$$

and furthermore, by left-multiplying the row-vector $(1, \delta, \delta^2,\ldots, \delta^{l-1})$ for an independent randomness δ in E_{S} on both sides, the above equality is equivalent to a scalar equation in S:

$$\boldsymbol{a}(\delta)^{\mathrm{T}}\boldsymbol{u}_\rho = b_{\rho,\delta} \tag{3.11}$$

where $\boldsymbol{a}(\delta)^{\mathrm{T}} = (1, \delta, \delta^2,\ldots, \delta^{l-1})\mathbf{A}$ and $b_{\rho,\delta} = (1, \delta, \delta^2,\ldots, \delta^{l-1})\boldsymbol{b}_\rho$. In this way the linear matrix relation **AU = B** in Z_m is (probabilistically) equivalent to the relation (3.11) with witness $\boldsymbol{u}_\rho$. If all Z_m-vectors $\boldsymbol{u}_i$'s have been individually committed to, then the commitment to $\boldsymbol{u}_\rho$ can be computed by (see (2.6)):

$$\mathrm{Cmt}(\sigma|\boldsymbol{u}_\rho) = \prod_{i=1}^{d} Cmt(\sigma|\boldsymbol{u}_i)^{\rho^{i-1}} \tag{3.12}$$

Here we can see one of the main differences between our (matrix-oriented) approach and the standard (vector-oriented) one: if a private computing task is vector-oriented and each Z_m-vector has to be committed individually, then the standard approach works well and needs totally d G-elements for commitments[3] and some additional computations like (3.12); however, if all Z_m-vectors can be committed in a

[3] By (2.2), the commitment to a $\boldsymbol{u}$ in S^n is formally comprised of d elements in G, however, for $\boldsymbol{u}$ in $\mathrm{Z}_m{}^n$ all components are 1 in G except for the first component, so actually only 1 nontrivial G-element is needed for a commitment to $\boldsymbol{u}$. See also sec.3 in [16].

batch or the computation is naturally matrix-oriented instead of just dealing with “a collection of vectors”, then our approach works well. The total number of G-elements needed for commitments to **U** is also *d*.

It’s easy to see that in this case these two approaches also have the same message complexity and the same on-line computational complexity. In summary, there are no significant differences in performance for $t = 1$.

However, in case of $t > 1$ the standard approach either (by regarding matrix **U** simply as a collection of *td* *n*-dimensional Z_m-vectors and committing to these vectors individually) needs totally *td* G-elements for commitments and *n* G-elements in c.r.s., or (by regarding **U** as a *ntd*-dimensional Z_m-vector) needs 1 G-elements for commitments and *ntd* G-elements in c.r.s. On the other hand, by carefully making use of the commitment scheme, the matrix-oriented approach can implement the protocol with proper number of G-elements in both commitments and c.r.s while improving the performance.

3.4 Matrix-oriented Construction

Consider $t = 2$, i.e., the equation $\mathbf{AU} = \mathbf{B}$ with $\mathbf{A} \in Z_m^{l\times n}$, $Z_m^{n\times 2d} \ni \mathbf{U} \equiv [\mathbf{U}_1,\mathbf{U}_2]$ with each $\mathbf{U}_i \in Z_m^{n\times d}$; $Z_m^{l\times 2d} \ni \mathbf{B} \equiv [\mathbf{B}_1,\mathbf{B}_2]$ with each $\mathbf{B}_i \in Z_m^{l\times d}$ and:

$$\mathbf{U}_1 = \begin{bmatrix} u_1(1) & \cdots & u_d(1) \\ \vdots & \ddots & \vdots \\ u_1(n) & \cdots & u_d(n) \end{bmatrix}, \quad \mathbf{U}_2 = \begin{bmatrix} v_1(1) & \cdots & v_d(1) \\ \vdots & \ddots & \vdots \\ v_1(n) & \cdots & v_d(n) \end{bmatrix}$$

In this case we take $\boldsymbol{g}$ of $2n$ elements in G for committing to **U**, i.e., let $\sigma \equiv [G, \boldsymbol{g}, m]$ with $\boldsymbol{g} \equiv (g_1,\ldots, g_{2n})$ (see (2.3) or (2.4)). Since the equation $\mathbf{A}[\mathbf{U}_1,\mathbf{U}_2] = [\mathbf{B}_1,\mathbf{B}_2]$ is equivalent to $\mathbf{AU}_i = \mathbf{B}_i$, i=1,2, i.e.,

$$\begin{bmatrix} \boldsymbol{A} & \boldsymbol{O} \\ \boldsymbol{O} & \boldsymbol{A} \end{bmatrix} \begin{bmatrix} \boldsymbol{U}_1 \\ \boldsymbol{U}_2 \end{bmatrix} = \begin{bmatrix} \boldsymbol{B}_1 \\ \boldsymbol{B}_2 \end{bmatrix} \quad \text{i.e., } \mathbf{A}^*\mathbf{U}^* = \mathbf{B}^* \tag{3.13}$$

where $\mathbf{A}^* \epsilon Z_m^{2l\times 2n}$ and $\mathbf{U}^* \epsilon Z_m^{2n\times d}$ are the matrices on the left side and $\mathbf{B}^*$ is the matrix on the right side. If committing to $\mathbf{U}^*$ (which is actually our definition of “the commitment to matrix **U**”) then with public key σ we have 1 commitment in G^d with its *j*-th component as ($\boldsymbol{u}_j$ and $\boldsymbol{v}_j$ are the *j*-th column in $\mathbf{U}_1$ and $\mathbf{U}_2$):

$$\mathrm{Cmt}(\sigma|\mathbf{U}^*)_j = \mathrm{cmt}_\sigma([\boldsymbol{u}_j^{\mathrm{T}}, \boldsymbol{v}_j^{\mathrm{T}}]) \in G, \ \ j = 1,\ldots, d \tag{3.14}$$

Now the ZKA protocol construction in sec.3.1 and 3.2 can be applied to equation (3.13) which (by theorem 1 and 2) corresponding linear relation is on S^{2n} with commitments (3.14). More generally, for any $t > 1$: $Z_m^{n\times td} \ni \mathbf{U} \equiv [\mathbf{U}_1,\ldots,\mathbf{U}_t]$ and $\mathbf{AU} = \mathbf{B}$ we can apply the efficient ZKA protocol construction to the equivalent linear relation

$$\begin{bmatrix} \mathbf{A} & .. & \boldsymbol{O} \\ .. & .. & .. \\ \boldsymbol{O} & .. & \boldsymbol{A} \end{bmatrix} \begin{bmatrix} \boldsymbol{U}_1 \\ \ldots \\ \boldsymbol{U}_t \end{bmatrix} = \begin{bmatrix} \boldsymbol{B}_1 \\ \ldots \\ \boldsymbol{B}_t \end{bmatrix}, \ \mathbf{U}^* \equiv \begin{bmatrix} \boldsymbol{U}_1 \\ \ldots \\ \boldsymbol{U}_t \end{bmatrix} \epsilon Z_m^{tn\times d} \tag{3.15}$$

with *nt* group elements in c.r.s. σ and the commitments

$$\mathrm{Cmt}(\sigma|\mathbf{U}^*)_j = \mathrm{cmt}_\sigma([\boldsymbol{u}_j^{(1)\mathrm{T}},\ldots, \boldsymbol{u}_j^{(t)\mathrm{T}}]) \in G, \ \ j = 1,\ldots, d \tag{3.16}$$

where each $\boldsymbol{u}_j^{(k)}$ is the *j*-th column Z_m-vector in $\mathbf{U}_k$. The corresponding S-linear relation of (3.15) is on space S^{nt}.

Table 1 summaries the performance comparisons for different approaches (on basis of sec.4.4 in [16]). Note that when $\mathbf{U}\epsilon\mathrm{Z}_m^{n\times td}$ is regarded as a *ntd*-dimensional vector then *ntd* G-elements are needed in c.r.s. while when regarded as a collection of *td n*-dimensional vectors then *n* G-elements needed in c.r.s. Table 2 provides the special case for square **U**: *td* = *n*.

Table 1. Performance of different approaches to constructing ZKA for linear matrix relation

	Vector-oriented (e.g., [12][16])	Matrix-oriented (ours)
	Both with targeted knowledge error $\le p^{-d}\log n$ and $\mathbf{U}\epsilon\mathrm{Z}_m^{n\times td}$	
number of G-elements in c.r.s.	①*ntd* or ②*n*	*nt*
number of G-elements for commitment.	①: 1 ②: *td*	*d*
number of rounds	①: 2log*n* + 2log*t* + 2log*d* – 1 ②: 2log*t* + 2log*d* – 1	2log*n* + 2log*t* – 1
message complexity	①: (2log(*ntd*)-3)*d* G-element 1+2log(*ntd*) S-elements log(*ntd*) – 1 $\mathrm{E_S}$-element ②: (2log*n*–3)*d* G-element 1+2log*n* S-elements log*n* – 1 $\mathrm{E_S}$-element	(2log(*nt*)–3)*d* G-element. 1+2log(*nt*) S-elements log(*nt*) – 1 $\mathrm{E_S}$-element

Table 2. Performance of different approaches to constructing ZKA for linear matrix relation(square witness)

	Vector-oriented (e.g., [12][16])	Matrix-oriented (ours)
	Both with targeted knowledge error $\le p^{-d}\log n$ and $\mathbf{U}\epsilon\mathrm{Z}_m^{n\times n}$	
number of G-elements in c.r.s.	① n^2 or ②*n*	n^2/d
number of G-elements for commitment.	①: 1 ②: *n*	*d*
number of rounds	①: 4log*n* – 1 ②: 2log*n* – 1	4log*n* – 2log*d* – 1
message complexity	①: (4log*n* – 3)*d* G-element 1+4log*n* S-elements 2log*n* – 1 $\mathrm{E_S}$-element ②: (2log*n*-3)*d* G-element 1+2log*n* S-elements log*n* – 1 $\mathrm{E_S}$-element	(4log*n*–2log*d*–3)*d* G-element; 1+4log*n*–2log*d* S-elements; 2log*n* – log*d* – 1 $\mathrm{E_S}$-element

Note that in the second sub-case in vector-oriented approach (regarding matrix **U** as a collection of *td n*-dimensional Z_m-vectors so that each column is committed individually) there may be too many (totally td) commitments needed, so this sub-approach becomes inefficient when $td > \log n$. In particular, for square **U** ($td = n$) the matrix-oriented approach is greatly superior to the vector-oriented one. For example, the number of rounds is reduced from $4\log n$ to $4\log n–2\log d$ and message complexity is reduced from $4d\log n$ to $4d\log n–2d\log d$(for number of group elements) and from $6d\log n$ to $6d\log n–3d\log d$(for number of ring elements). In addition, the number of group elements in c.r.s is reduced by a factor of d (see tab. 1 & 2).

Some ZKA constructions for more complicated linear matrix relations over Zm, are presented in Appendix C. All these relations can be equivalently reduced to the form of (3.8).

4 Efficient ZKA Protocol for Matrix Relation $\mathbf{U}^{\mathrm{T}}\mathbf{QV} = \mathbf{Y}$

Consider the matrix bilinear equation

$$\mathbf{U}^{\mathrm{T}}\mathbf{QV} = \mathbf{Y} \tag{4.1}$$

in residue ring Z_m where matrices **U**, $\mathbf{V} \in Z_m^{n\times td}$, $\mathbf{Q} \in Z_m^{n\times n}$ and diagonal, $\mathbf{Y} \in Z_m^{td\times td}$. The extension degree of Galois ring S over Z_m is d and is determined by $p^{-d} \log n <$ the targeted knowledge error. Furthermore matrices **U** and **V** are private (witnesses) while **Q** and **Y** are public.

For simplicity, **Q** is assumed to be diagonal in sec. 4.1. Non-diagonal case will be treated in sec. 4.2.

4.1 Basics

Consider $t = 1$ at first. If in this case the bilinear equation (4.1) is regarded as a collection of vector bilinear equations $\wedge_{i,j=1}^{d} \boldsymbol{u_i}^{\mathrm{T}}\mathbf{Q}\boldsymbol{v}_j = \mathrm{Y}_{i,j}$ where $\boldsymbol{u_i}$ and $\boldsymbol{v}_j$ are column vectors of **U** and **V** and apply the standard amortization techniques, then this relation can be probabilistically equivalently reduced to a bilinear relation over the ring S:

$$\boldsymbol{u}_\rho^{\mathrm{T}}\mathbf{Q}\boldsymbol{v}_\delta = \sum_{i,j=1}^{d} Y_{ij}\, \rho^{i-1}\delta^{j-1} \tag{4.2}$$

where the independent randomness $\rho, \delta \overset{R}{\leftarrow} \mathrm{E}_S$ are sampled by the verifier:

$$\boldsymbol{u}_\rho = \sum_{i=1}^{d} \boldsymbol{u}_i\, \rho^{i-1},\ \ \boldsymbol{v}_\delta = \sum_{i=1}^{d} \boldsymbol{v}_i\, \delta^{i-1} \tag{4.3}$$

The commitments are (see (2.6) and (2.7)):

$$U_\rho = \prod_{i=1}^{n} Cmt(\sigma|\boldsymbol{u}_i)^{\rho^{i-1}},\ V_\delta = \prod_{i=1}^{n} Cmt(\sigma|\boldsymbol{v_i})^{\delta^{i-1}},\ i{=}1,\ldots,d \tag{4.4}$$

Totally $2d$ elements in G are needed for commitment(see the footnote 4).

Now consider the case t =2 where $Z_m^{n\times 2d} \ni \mathbf{U} \equiv [\mathbf{U}_1,\mathbf{U}_2]$, $\mathbf{V} \equiv [\mathbf{V}_1,\mathbf{V}_2]$, each $\mathbf{U}_{\boldsymbol{i}}$ and $\mathbf{V}_{\boldsymbol{i}} \in Z_m^{n\times d}$.

Note that (4.1) in this case is formulated as :

$$\begin{bmatrix} \boldsymbol{U}_1^{\mathrm{T}} \\ \boldsymbol{U}_1^{\mathrm{T}} \end{bmatrix} \mathbf{Q}[\mathbf{V}_1,\mathbf{V}_2] = \begin{bmatrix} Y_{11} & Y_{12} \\ Y_{21} & Y_{22} \end{bmatrix}$$

where Y_{ij}'s are d-by-d blocks in $\mathbf{Y}$. This equation is just $\wedge_{i,j=1}^{2}\, \boldsymbol{U}_{\boldsymbol{i}}^{\mathrm{T}}\mathbf{Q}\boldsymbol{V}_j = \mathbf{Y}_{i,j}$ and for any randomness $\rho \overset{R}{\leftarrow} \mathrm{E}_S$ sampled by the verifier, it is equivalent to the following matrix bilinear relation with probability $> 1- 3p^{-d}$:

$$(\mathbf{U}_1+\rho\mathbf{U}_2)^{\mathrm{T}}\mathbf{Q}(\mathbf{V}_1+\rho^2\mathbf{V}_2) = \mathbf{Y}_{11}+\rho\mathbf{Y}_{21}+\rho^2\mathbf{Y}_{12}+\rho^3\mathbf{Y}_{22} \equiv \mathbf{Y}_\rho$$

Also this can be reformulated in a $2n$-by-$2n$ matrix form with witness matrices in Z_m:

$$[\mathbf{U}_1^{\mathrm{T}}, \mathbf{U}_2^{\mathrm{T}}] \begin{bmatrix} \mathbf{Q} & \rho^2\mathbf{Q} \\ \rho\mathbf{Q} & \rho^3\mathbf{Q} \end{bmatrix} \begin{bmatrix} \mathbf{V_1} \\ \mathbf{V_2} \end{bmatrix} = \mathbf{Y}_\rho \in S^{d\times d} \qquad (4.5)$$

Let $\mathbf{U}^*, \mathbf{V}^* \in \mathrm{Z}_m^{2n\times d}$ and $\mathbf{Q}_\rho{}^* \in S^{2n\times 2n}$ be the matrices on left side of (4.5), i.e.,

$$\mathbf{U}^* \equiv \begin{bmatrix} \boldsymbol{U}_1 \\ \boldsymbol{U}_2 \end{bmatrix} = \begin{bmatrix} u_{1,1}(1), & \dots & u_{1,d}(1) \\ \vdots & & \vdots \\ u_{1,1}(n) & \ddots & u_{1,d}(n) \\ u_{2,1}(1) & & u_{2,d}(1) \\ \vdots & \cdots & \vdots \\ u_{2,1}(n) & & u_{2,d}(n) \end{bmatrix}, \ \mathbf{Q}_\rho{}^* \equiv \begin{bmatrix} \mathbf{Q} & \rho^2\mathbf{Q} \\ \rho\mathbf{Q} & \rho^3\mathbf{Q} \end{bmatrix}$$

By applying the methods presented in the first paragraph of this section, i.e., (4.3)~(4.4), relation (4.5) can be reduced to a bilinear relation (4.2) over the ring S. In order to achieve this goal, we take $2n$ elements $\boldsymbol{g}$ in G for committing $\mathbf{U}^*$ and $\mathbf{V}^*$, i.e., set $\sigma \equiv [\mathrm{G}, \boldsymbol{g}, m]$ with $\boldsymbol{g} \equiv (g_1,\dots, g_{2n})$ and compute the commitments to $\mathbf{U}^*$, $\mathbf{V}^*$ (which are actually our definition of "the commitments to matrix $\mathbf{U}$ and $\mathbf{V}$") just as done in (3.16). These commitments have totally $2d$ G-elements and the dimension of the corresponding S-vectors under commitment is $2n$. For example:

$$\mathrm{Cmt}(\sigma|\mathbf{U}^*) = \begin{bmatrix} cmt_\sigma(u_{1,1}(1), & \cdots, u_{1,1}(n), u_{2,1}(1), \dots & u_{2,1}(n)) \\ \vdots & . & \vdots \\ cmt_\sigma(u_{1,d}(1), & \cdots, u_{1,d}(n), u_{2,d}(1), \dots & u_{2,d}(n)) \end{bmatrix} \text{ in } \mathrm{G}^d$$

In general, for any t>1 where $Z_m^{n\times td} \ni \mathbf{U} \equiv [\mathbf{U}_1,\dots,\mathbf{U}_t]$, $\mathbf{V} \equiv [\mathbf{V}_1,\dots,\mathbf{V}_t]$ with each $\mathbf{U}_{\boldsymbol{i}}$, $\mathbf{V}_{\boldsymbol{i}} \in Z_m^{n\times d}$, by the above method relation (4.1) can be probabilistic-equivalently reduced to the form like:

$$\mathbf{U}^{*\mathrm{T}}\mathbf{Q}_\rho{}^*\mathbf{V}^* = \mathbf{Y}_\rho \qquad (4.6)$$

where $\mathbf{U}^*, \mathbf{V}^* \in \mathrm{Z}_m^{tn\times d}$ and $\mathbf{Q}_\rho{}^* \in S^{tn\times tn}$ as:

$$\mathbf{U}^* \equiv \begin{bmatrix} \boldsymbol{U}_1 \\ \vdots \\ \boldsymbol{U}_t \end{bmatrix} = \begin{bmatrix} u_{1,1}(1), & & u_{1,d}(1) \\ \vdots & \cdots & \vdots \\ u_{1,1}(n) & & u_{1,d}(n) \\ \vdots & \ddots & \vdots \\ u_{t,1}(1) & & u_{t,d}(1) \\ \vdots & \cdots & \vdots \\ u_{t,1}(n) & & u_{t,d}(n) \end{bmatrix}, \ \mathbf{Q}_\rho{}^* \equiv \begin{bmatrix} \mathbf{Q} & \rho^{\boldsymbol{t}}\mathbf{Q} & \dots & \rho^{(\boldsymbol{t}-\mathbf{1})\boldsymbol{t}}\mathbf{Q} \\ \rho\mathbf{Q} & \rho^{\boldsymbol{t}+\mathbf{1}}\mathbf{Q} & \dots & \rho^{(\boldsymbol{t}-\mathbf{1})\boldsymbol{t}+\mathbf{1}}\mathbf{Q} \\ \vdots & \vdots & & \vdots \\ \rho^{\boldsymbol{t}-\mathbf{1}}\mathbf{Q} & \rho^{\mathbf{2}\boldsymbol{t}-\mathbf{1}}\mathbf{Q} & \dots & \rho^{\boldsymbol{t}^{\mathbf{2}}-\mathbf{1}}\mathbf{Q} \end{bmatrix}$$

By applying the methods presented in (4.3)~(4.4), relation (4.6) can be reduced to a bilinear relation (4.2) over the ring S. In order for this, we take *tn* elements $\boldsymbol{g}$ in G for committing $\mathbf{U}^*$ and $\mathbf{V}^*$, i.e., set $\sigma \equiv [\mathrm{G}, \boldsymbol{g}, m]$ with $\boldsymbol{g} \equiv (g_1, \dots, g_{nt})$ and compute the commitments to $\mathbf{U}^*$, $\mathbf{V}^*$ as done in the above. The dimension of the corresponding S-vectors under commitment is *tn*, which commitments have totally 2*d* G-elements.

In order to construct the efficient protocol for bilinear relation (4.2), **Q**'s diagonality is important (see sec. 4.4). However, $\mathbf{Q}_\rho^*$ in (4.6) (which will be inherited in the bilinear relation over S) is no longer diagonal even **Q** is diagonal. This can be handled in the following way on basis of a helpful observation that $\mathbf{Q}_\rho^* \in S^{nt\times nt}$ is actually a tensor product as:

$$\mathbf{Q}_\rho^* = \boldsymbol{\Delta}(\rho)\hat{\otimes}\mathbf{Q} \qquad (4.7)$$

where:

$$\boldsymbol{\Delta}(\rho) \equiv [\boldsymbol{\rho}(t), \rho^t\boldsymbol{\rho}(t), \rho^{2t}\boldsymbol{\rho}(t), \dots, \rho^{t(t\text{-}1)}\boldsymbol{\rho}(t)] \in E_S^{t\times t}$$

and the column vector $\boldsymbol{\rho}(t)^{\mathrm{T}} \equiv [1, \rho, \rho^2, \dots, \rho^{t\text{-}1}] \in \mathrm{E}_S^t$.

Recall that $\mathrm{E_S}$ is the exceptional set in Galois ring S = GR(*m*,*d*) with $m = p^s$ which is actually (with 0 added in it) isomorphic to Galois field F_p^d. With overwhelming probability, there are efficiently computable non-singular matrices $\boldsymbol{\Phi}_\rho$, $\boldsymbol{\Psi}_\rho \in E_S^{t\times t}$ and a diagonal matrix $\mathbf{D}_\rho$ such that:

$$\boldsymbol{\Delta}(\rho) = \boldsymbol{\Phi}_\rho^{\mathrm{T}}\mathbf{D}_\rho\boldsymbol{\Psi}_\rho \qquad (4.8)$$

Indeed, for *i*,*j*=1,…,*t* note that $\boldsymbol{\Delta}_{ij}(\rho) = \rho^{i-1+(j-1)t} = \sum_{k,l=1}^{t} \rho_k^{i-1}\delta_{k1}\,\delta_{l1}\rho_l^{(j-1)t}$ where δ_{kl} is the Kronecker symbol and $\rho_k \equiv \rho^k$, $\rho_l \equiv \rho^l$, so $\mathbf{D}_\rho$=diag(1,0,…0) and $\boldsymbol{\Phi}_\rho$, $\boldsymbol{\Psi}_\rho$ are Vandermonde matrices with determinants $\det\boldsymbol{\Phi}_\rho = \prod_{1\le\mu<\nu\le t}(\rho^\mu - \rho^\nu)$, $\det\boldsymbol{\Psi}_\rho = \prod_{1\le\mu<\nu\le t}(\rho^{\mu t} - \rho^{\nu t})$. Obviously $\boldsymbol{\Phi}_\rho$ or $\boldsymbol{\Psi}_\rho$ is singular only if the randomness ρ is a root of the equation $\rho^k = 1$ or $\rho^{kt} = 1$ for some *k*: $1\le k\le t\text{-}1$. Since $t = \mathrm{poly}(\lambda)$ but $|\mathrm{E_S}| = p^d\sim2^\lambda$ so this occurs with probability negligible in security parameter λ. As a result, the diagonalization (4.8) holds with overwhelming probability. Combining (4.7), (4.8) and the well-known identity $(\mathbf{AB})\hat{\otimes}(\mathbf{CD}) = (\mathbf{A}\hat{\otimes}\mathbf{C})(\mathbf{B}\hat{\otimes}\mathbf{D})$, one obtains the diagonalization for $\mathbf{Q}_\rho^*$:

$$\mathbf{Q}_\rho^* = (\boldsymbol{\Phi}_\rho\hat{\otimes}\mathbf{I}_{\boldsymbol{n}})^{\mathrm{T}}(\mathbf{D}_\rho\hat{\otimes}\mathbf{Q})(\boldsymbol{\Psi}_\rho\hat{\otimes}\mathbf{I}_{\boldsymbol{n}}) \qquad (4.9)$$

In summary, the large matrix $\mathbf{Q}_\rho^*$ can be efficiently diagonalized and the computational complexity of its diagonalization only depends on diagonalizing a special and relatively small-size matrix $\boldsymbol{\Delta}(\rho)$, which can be pre-calculated by the verifier.

For notational simplicity, reformulate (4.9) as follows with diagonal $\mathbf{D_Q} \in E_S^{nt\times nt}$:

$$\mathbf{Q}_\rho^* = \boldsymbol{\Phi}^{\mathrm{T}}\mathbf{D_Q}\boldsymbol{\Psi}$$

Set new witness matrices $\overline{\mathbf{U}}$ and $\overline{\mathbf{V}}$ over S such that $\overline{\mathbf{U}} = \boldsymbol{\Phi}\mathbf{U}^*$ and $\overline{\mathbf{V}} = \boldsymbol{\Psi}\mathbf{V}^*$ then by simple calculations one has:

$$\mathrm{U}^{*\mathrm{T}}\mathbf{Q}_\rho^*\mathbf{V}^* = \overline{\mathbf{U}}^{\mathbf{T}}\mathbf{D_Q}\overline{\mathbf{V}}$$

Hence the bilinear relation (4.6) $\mathrm{U}^{*\mathrm{T}}\mathbf{Q}_\rho^*\mathbf{V}^* = \mathbf{Y}_\rho$ with witness Z_m-matrices U^* and $\mathbf{V}^*$ is probabilistically equivalent to the diagonal bilinear relation $\overline{\mathbf{U}}^{\mathbf{T}}\mathbf{D_Q}\overline{\mathbf{V}} = \mathbf{Y}_\rho$ with witness

S-matrices $\overline{\mathbf{U}}$ and $\overline{\mathbf{V}}$: $\overline{\mathbf{U}}^{\mathrm{T}}\mathbf{D}_{\mathrm{Q}}\overline{\mathbf{V}} = \mathbf{Y}_{\rho}$. Left-multiply this equation by vector $[1, \omega, \omega^2,\ldots, \omega^{d\text{-}1}]$ and right-multiply it by column vector $[1, \theta, \theta^2,\ldots, \theta^{d\text{-}1}]^{\mathrm{T}}$ for any independent randomness ω and θ sampled by the verifier in the exceptional set $\mathrm{E_S}$, one reduces it furthermore to a bilinear relation with *nt*-dimensional S-vector witness $\boldsymbol{u}(\omega)$ and $\boldsymbol{v}(\theta)$:

$$\boldsymbol{u}(\omega)^{\mathrm{T}}\mathbf{D}_{\mathrm{Q}}\boldsymbol{v}(\theta) = \textstyle\sum_{i,j=1}^{d} Y_\rho\,(i,j)\omega^{i-1}\theta^{j-1} \qquad (4.10)$$

where $\boldsymbol{u}(\omega)^{\mathrm{T}} = [1, \omega, \omega^2,\ldots, \omega^{d\text{-}1}]\overline{\mathbf{U}}^{\mathbf{T}}$ and $\boldsymbol{v}(\theta)^{\mathrm{T}} = [1, \theta, \theta^2,\ldots, \theta^{d\text{-}1}]\overline{\mathbf{V}}^{\mathbf{T}}$. The overall reduction from relation (4.1) to relation (4.10) is of equivalence with overwhelming probability ($> 1 - \mathrm{O}(np^{-d})$).

The remaining problem is how to efficiently calculate the commitments to S-vectors $\boldsymbol{u}(\omega)$ and $\boldsymbol{v}(\theta)$ from those to Z_m-matrices U^* and $\mathbf{V}^*$. Let $\overline{\mathbf{U}} = [\overline{\boldsymbol{u}_1},\ldots, \overline{\boldsymbol{u}_d}]$, $\overline{\mathbf{V}} = [\overline{\boldsymbol{v}_1},\ldots, \overline{\boldsymbol{v}_d}]$ with columns $\overline{\boldsymbol{u}}_\iota$, $\overline{\boldsymbol{v}}_\iota \in E_S^{nt}$, note that

$$\boldsymbol{u}(\omega) = \textstyle\sum_{i=1}^{d} \omega^{i-1}\,\overline{\boldsymbol{u}}_\iota,\ \boldsymbol{v}(\theta) = \sum_{i=1}^{d} \theta^{i-1}\,\overline{\boldsymbol{v}}_\iota \qquad (4.11)$$

so for any public-key τ the commitments to S-vectors $\boldsymbol{u}(\omega)$ and $\boldsymbol{v}(\theta)$ are:

$$\mathrm{Cmt}(\tau|\boldsymbol{u}(\omega)) = \textstyle\prod_{i=1}^{d} Cmt(\tau|\overline{\boldsymbol{u}}_i)^{\omega^{i-1}},\ \mathrm{Cmt}(\tau|\boldsymbol{v}(\theta)) = \prod_{i=1}^{d} Cmt(\tau|\overline{\boldsymbol{v}}_i)^{\theta^{i-1}} \qquad (4.12)$$

In order to present how to calculate, e.g., $\mathrm{Cmt}(\tau|\overline{\boldsymbol{u}}_\iota)$ from the commitment to $\mathbf{U}^*$, we prove the following fact.

Lemma 2 Let $S^{nt} \ni \overline{\boldsymbol{w}}$ with each component $\overline{w}_i = \sum_{k=1}^{d} \overline{w}_k\,(i)X^{k-1}$ and $\overline{w}_k(i)$ in $\mathrm{Z}_m[X]$ (recall that the ring $\mathrm{S} = \mathrm{GR}(m,d) = \mathrm{Z}_m[X]/(f(X))$, $\mathbf{E}\in E_S^{nt\times nt}$ be any matrix over Es, $\mathbf{M}_{ij} \in Z_m^{d\times d}$ is the multiplicative matrix associated with the matrix element E_{ij} (see lemma 2.1 in sec.2.4), then
(*i*)The *l*-th component (an element in group G) of the commitment to $\boldsymbol{w} = \mathbf{E}\overline{\boldsymbol{w}}$ is:

$$\mathrm{Cmt}(\sigma|\boldsymbol{w})_l == \textstyle\prod_{j=1}^{nt}\prod_{k=1}^{d} cmt_\sigma\,([M_{1j}(l,k),\ldots,M_{nt,j}(l,k)])^{\overline{w}_k(j)},\ l=1,\ldots,.d \qquad (4.13)$$

(*ii*) For $\boldsymbol{w} \in Z_m^{nt}$ one furthermore has:

$$\mathrm{Cmt}(\sigma|\boldsymbol{w}) = \mathrm{Cmt}(\overline{\sigma}|\overline{\boldsymbol{w}}) \qquad (4.14)$$

where the public-key $\overline{\sigma} \equiv [\mathrm{G}, \overline{g_1},\ldots, \overline{g_{nt}}, m]$ has:

$$\overline{g_J} \equiv \mathrm{cmt}_\sigma([\mathrm{M}_{1j}(1,1),\ldots, \mathrm{M}_{nt,j}(1,1)]) \qquad (4.15)$$

Proof (*i*) $\mathrm{S}^{nt}\ni\boldsymbol{w} = \mathbf{E}\overline{\boldsymbol{w}}$ has its *i*-th component as:

$$w_i = \textstyle\sum_{\boldsymbol{j=1}}^{\boldsymbol{nt}} E_{ij}\,\overline{w_J} = \sum_{l=1}^{d}(\sum_{j=1}^{nt}\sum_{k=1}^{d} M_{ij}\,(l,k)\overline{w}_k\,(j))X^{l-1},\ i=1,\ldots, nt$$

hence the *l*-th component of the commitment to $\overline{\boldsymbol{w}}$ is:

$$\begin{aligned}\mathrm{Cmt}(\sigma|\boldsymbol{w})_l &= \mathrm{cmt}_\sigma(\text{the } nt\text{-dimensional coefficient-vector of monomial } X^{l\text{-}1} \text{ in } \boldsymbol{w})\\ &= \mathrm{cmt}_\sigma([\textstyle\sum_{j=1}^{nt}\sum_{k=1}^{d} M_{1j}(l,k)\,\overline{w}_k(j),\ldots,\sum_{j=1}^{nt}\sum_{k=1}^{d} M_{nt,j}(l,k)\,\overline{w}_k(j)])\\ &= \textstyle\prod_{j=1}^{nt}\prod_{k=1}^{d} cmt_\sigma\,([M_{1j}(l,k),\ldots,M_{nt,j}(l,k)])^{\overline{w}_k(j)},\ l=1,\ldots,.d\end{aligned}$$

(*ii*) For $\boldsymbol{w} \in Z_m^{nt}$, the 1-st ($l = 1$) component in its commitment carries complete information of the committed vector (other *d*-1components are randomness or simply 1 in G) and the value of $\mathrm{cmt}_\sigma(.)$ is always in G^m(up to a random factor -1 in case of even *m*)

[16], so by separating the factor related with $\overline{\boldsymbol{w}}_l$ in (4.13), appropriately re-arrange some factors to keep the equality and reduce all other factors to the random factor (always in a form of r^m in the commitment scheme), (4.13) becomes:

$$\mathrm{Cmt}(\sigma|\boldsymbol{w})_l = r_l^m \prod_{j=1}^{nt} cmt_\sigma\left([M_{1j}(1,1),\dots,M_{nt,j}(1,1)]\right)^{\overline{w}_l(j)} \qquad (4.16)$$

As a result, we have $\mathrm{Cmt}(\sigma|\boldsymbol{w}) = \mathrm{Cmt}(\overline{\sigma}|\overline{\boldsymbol{w}})$ where the public-key $\overline{\sigma} \equiv [\mathrm{G}, \overline{g_1},\dots, \overline{g_{nt}}, m]$ with $\overline{g_j} \equiv \mathrm{cmt}_\sigma([\mathrm{M}_{1j}(1,1),\dots, \mathrm{M}_{nt,j}(1,1)])$. This proves the lemma.

Applying this lemma to column vectors of $\overline{\mathbf{U}}$, $\overline{\mathbf{V}}$ and $\mathbf{U}^*$, $\mathbf{V}^*$, the commitments to the original Z_m-matrices **U** and **V** with public-key σ is just the commitments to S-matrices $\overline{\mathbf{U}}$ and $\overline{\mathbf{V}}$ with public-key $\overline{\sigma_1}$, $\overline{\sigma_2}$ respectively(each key dependent on the randomness sampled by the verifier), which can be efficiently computed by both prover and verifier (by (4.15) where matrix **M** substituted with $\mathbf{\Phi}^{-1}$ and $\mathbf{\Psi}^{-1}$ respectively).

In summary, the matrix bilinear relation (4.1) over Z_m with witness matrices in any size can be probabilistic-equivalently reduced to a bilinear vector relation (4.10) over S = GR(m,d) which coefficient matrix is diagonal. This reduction is summarized more accurately in next theorem, which is the starting point to constructing ZKA protocol for bilinear matrix relation in Z_m.

Theorem 3 For Galois ring S ≡ GR(m,d) with $m = p^s$ and p being prime, let the bilinear matrix relation in Z_m (variables in the frame are witnesses) be:

$$\mathbf{MBLR}(\sigma|\, U_1, V_1, \mathbf{Y}, \mathbf{Q};\, \boxed{\boldsymbol{r},\boldsymbol{t},\mathbf{U},\mathbf{V}}):$$

$$U_1 = \mathrm{Cmt}(\sigma|\mathbf{U}^*;\boldsymbol{r}) \wedge V_1 = \mathrm{Cmt}(\sigma|\mathbf{V}^*;\boldsymbol{t}) \wedge \mathbf{U}^{\mathrm{T}}\mathbf{Q}\mathbf{V} = \mathbf{Y} \qquad (4.17)$$

with c.r.s. σ being a public key of the S-vector commitment scheme, witness matrices $Z_m^{n\times td} \ni \mathbf{U} \equiv [\mathbf{U}_1,\dots,\mathbf{U}_t]$, $\mathbf{V} \equiv [\mathbf{V}_1,\dots,\mathbf{V}_t]$ with each $\mathbf{U}_i$, $\mathbf{V}_i \in Z_m^{n\times d}$, $\mathbf{Q} \in Z_m^{n\times n}$ diagonal, $\mathbf{Y} \in Z_m^{td\times td}$ and:

$$\mathbf{U}^* \equiv \begin{bmatrix} \boldsymbol{U}_1 \\ \vdots \\ \boldsymbol{U}_t \end{bmatrix} = \begin{bmatrix} u_{1,1}(1), & & u_{1,d}(1) \\ \vdots & \cdots & \vdots \\ u_{1,1}(n) & & u_{1,d}(n) \\ \vdots & \ddots & \vdots \\ u_{t,1}(1) & & u_{t,d}(1) \\ \vdots & \cdots & \vdots \\ u_{t,1}(n) & & u_{t,d}(n) \end{bmatrix}, \mathbf{V}^* \equiv \begin{bmatrix} \boldsymbol{V}_1 \\ \vdots \\ \boldsymbol{V}_t \end{bmatrix} = \begin{bmatrix} v_{1,1}(1), & & v_{1,d}(1) \\ \vdots & \cdots & \vdots \\ v_{1,1}(n) & & v_{1,d}(n) \\ \vdots & \ddots & \vdots \\ v_{t,1}(1) & & v_{t,d}(1) \\ \vdots & \cdots & \vdots \\ v_{t,1}(n) & & v_{t,d}(n) \end{bmatrix} \qquad (4.18)$$

then **MBLR** is probabilistic-equivalent with soundness factor $2d+t^2$ to the bilinear relation in Galois ring S:

$$\mathbf{SBLR}(\overline{\sigma}_1,\overline{\sigma}_2|U_2,V_2,\, y_\rho(\omega,\theta),\, \mathbf{D}_{\mathbf{Q}};\, \boxed{\boldsymbol{r},\boldsymbol{s},\boldsymbol{u}(\omega),\boldsymbol{v}(\theta)}):$$

$$U_2 = \mathrm{Cmt}(\overline{\sigma}_1|\boldsymbol{u}(\omega);\, \boldsymbol{r}) \wedge V_2 = \mathrm{Cmt}(\overline{\sigma}_2|\boldsymbol{v}(\theta);\, \boldsymbol{s}) \wedge \boldsymbol{u}(\omega)^{\mathrm{T}}\mathbf{D}_{\mathbf{Q}}\boldsymbol{v}(\theta) = y_\rho(\omega,\theta) \qquad (4.19)$$

where ρ, ω, θ are sampled randomly and independently in E_S by the verifier, $\boldsymbol{u}(\omega)$, $\boldsymbol{v}(\theta) \in \mathrm{S}^{tn}$(witnesses) and $y_\rho(\omega,\theta)$ are specified in relation (4.10), $\mathbf{D}_{\mathbf{Q}} = \mathbf{D}_\rho \hat{\otimes} \mathbf{Q}$ is diagonal and specified in (4.9), $\overline{\sigma}_1$and $\overline{\sigma}_2$ specified in (4.15), U_2, $V_2 \in \mathrm{G}^d$ are computed from U_1, $V_1 \in \mathrm{G}^d$ by the component wise formula: $l = 1, \dots, d$

$$G \ni U_{2,l} = \prod_{i,j=1}^{d} U_{1,l}^{M(\omega^{i-1}|l,j)}$$

$$G \ni V_{2,l} = \prod_{i,j=1}^{d} V_{1,l}^{M(\theta^{i-1}|l,j)}$$

where $M(e|i,j)$ stands for the (i,j)-element in the multiplicative matrix $\mathbf{M}_e$ associated with e in S.
Proof The probabilistic-equivalent reduction from relation MLBR to SLBR has been elaborated in the above. The computational relation between the witnesses $\boldsymbol{u}(\omega)$, $\boldsymbol{v}(\theta)$ of relation SLBR and witnesses **U**, **V** of MLBR is completely implied by specifications for (4.6), (4.9) and (4.10) from which it's easy to derive the soundness factor of this reduction is $2d+t^2$. Finally the above formulas to compute U_2, V_2 from U_1, V_1 is the result of combining the formulas of (2.6), (4.12), (4.14) and (4.15) .

4.2 Non-diagonal Matrix Q

In many applications, a non-diagonal coefficient matrix in bilinear form is usually symmetric, i.e., $\mathbf{Q}^T = \mathbf{Q}$. If **Q**'s elements are regarded as numbers in rational field Q, there exists (according to the general theory of quadratic forms over any field[24]) a matrix $\mathbf{W} \in Q^{n\times n}$ non-singular in Q which can be efficiently computed such that

$$\mathbf{W}^T\mathbf{Q}\mathbf{W} = \text{diagonal matrix } \mathbf{D}_Q$$

Rescaling this equality by some integer, matrices **W** and $\mathbf{D}_Q$ can be both integral. If the above equality holds in Z_m, i.e., there exist matrix **W** and diagonal matrix $\mathbf{D}_Q$ such that g.c.d.(m, det**W**) = 1and:

$$\mathbf{W}^T\mathbf{Q}\mathbf{W} = \mathbf{D}_Q \bmod m \tag{4.20}$$

set new witness matrices $\widetilde{\mathbf{U}}$ and $\widetilde{\mathbf{V}}$ such that $\mathbf{U} = \mathbf{W}\widetilde{\mathbf{U}}$ and $\mathbf{V} = \mathbf{W}\widetilde{\mathbf{V}}$ then by simple calculations via the explicit commitment expressions in sec. 2.4 one obtains:

$$\mathbf{U}^T\mathbf{Q}\mathbf{V} = \widetilde{\mathbf{U}}^T\mathbf{D}_Q\widetilde{\mathbf{V}} \tag{4.21}$$

Let $Z_m^{n\times td} \ni \mathbf{U} \equiv [\mathbf{U}_1,\ldots,\mathbf{U}_t]$, $\widetilde{\mathbf{U}} \equiv [\widetilde{\mathbf{U}}_1,\ldots,\widetilde{\mathbf{U}}_t]$ with each $\mathbf{U}_i$, $\widetilde{\mathbf{U}}_i \in Z_m^{n\times d}$, then $\mathbf{U}_i = \mathbf{W}\widetilde{\mathbf{U}}_i$ and by notations in (4.18) one has:

$$u_{il}(j) = \sum_{k=1}^{n} W_{jk}\,\tilde{u}_{il}(k) \quad i = 1,\ldots,t,\ l = 1,\ldots,d,\ j=1,\ldots,n$$

For c.r.s. $\sigma \equiv [G, \boldsymbol{g}, m]$ with $\boldsymbol{g} \equiv \{g_{ij}: i = 1,\ldots,t; j=1,\ldots,n\}$ in G, the l-th component of the commitment to **U** is (see (3.16) and here $g[x]$ stands for g^x):

$$\begin{aligned}\mathrm{Cmt}(\sigma|\mathbf{U};\boldsymbol{r})_l &= r_l^m \prod_{i=1}^{t}\prod_{j=1}^{n} g_{ij}\,[u_{il}(j)] = r_l^m \prod_{i=1}^{t}\prod_{j=1}^{n} g_{ij}\,[\textstyle\sum_{k=1}^{n} W_{jk}\,\tilde{u}_{il}(k)]\\ &= r_l^m \prod_{i=1}^{t}\prod_{k=1}^{n}(\prod_{j=1}^{n} g_{ij}[W_{jk}])^{\tilde{u}_{il}(k)}\\ &= r_l^m \prod_{i=1}^{t}\prod_{k=1}^{n} \tilde{g}_{ik}\,[\tilde{u}_{il}(k)] = \mathrm{Cmt}(\tilde{\sigma}|\widetilde{\mathbf{U}};\boldsymbol{r})_l\end{aligned}$$

i.e., $$\mathrm{Cmt}(\sigma|\mathbf{U};\boldsymbol{r}) = \mathrm{Cmt}(\tilde{\sigma}|\widetilde{\mathbf{U}};\boldsymbol{r}) \text{ and } \mathrm{Cmt}(\sigma|\mathbf{V};\boldsymbol{s}) = \mathrm{Cmt}(\tilde{\sigma}|\widetilde{\mathbf{V}};\boldsymbol{s}) \tag{4.22}$$

where $\tilde{g}_{ik} = \prod_{j=1}^{n} g_{ij}^{W_{jk}}$, $i = 1,\ldots,t$, $k=1,\ldots,n$ and $\tilde{\sigma} = [G, \tilde{\boldsymbol{g}}, m]$.

As a result, in this case the bilinear matrix relation $\mathbf{MBLR}(\sigma|U,V,\mathbf{Y},\mathbf{Q};\ \boxed{\boldsymbol{r},\boldsymbol{s},\mathbf{U},\mathbf{V}})$ with c.r.s. σ and symmetric $\mathbf{Q} \in Z_m^{n\times n}$ is equivalent to a bilinear relation $\mathbf{MBLR}(\tilde{\sigma}\ |U, V, \mathbf{Y}, \mathbf{D}_\mathrm{Q};\ \boxed{\boldsymbol{r}, \boldsymbol{s}, \widetilde{\mathbf{U}},\widetilde{\mathbf{V}}})$ with c.r.s. $\tilde{\sigma}$ and diagonal matrix $\mathbf{D}_\mathrm{Q}$. Both prover and verifier can compute $\mathbf{W}$ and $\tilde{\sigma}$ from public information and these calculations can be done at initialization phase or off-line for the verifier, not degrading the verifier's online performance. Moreover, this equivalent transformation preserves the witness space dimension so the message complexity of the proof protocol is unchanged.

Another method to deal with non-diagonal $\mathbf{Q}$ is by Smith Normal Form. For any (asymmetric) $\mathbf{Q}$ and regarding it as a matrix over Z, there exist matrices $\mathbf{W},\mathbf{M} \in GL_n(Z)$ which can be efficiently computed such that:

$$\mathbf{W}^\mathrm{T}\mathbf{Q}\mathbf{M} = \text{diagonal matrix } \mathbf{D}_\mathrm{Q}$$

If this equality also holds over Z_m, i.e., $\mathbf{W},\mathbf{M} \in GL_n(Z_m)$ such that

$$\mathbf{W}^\mathrm{T}\mathbf{Q}\mathbf{M} = \mathbf{D}_\mathrm{Q} \bmod m \tag{4.23}$$

we can similarly set new witness matrices $\widetilde{\mathbf{U}}$ and $\widetilde{\mathbf{V}}$ such that $\mathbf{U} = \mathbf{W}\widetilde{\mathbf{U}}$ and $\mathbf{V} = \mathbf{M}\widetilde{\mathbf{V}}$ then by the same calculations one obtains (4.21) and:

$$\mathrm{Cmt}(\sigma|\mathbf{U};\boldsymbol{r}) = \mathrm{Cmt}(\tilde{\sigma}|\widetilde{\mathbf{U}};\boldsymbol{r}),\ \ \mathrm{Cmt}(\sigma|\mathbf{V};\boldsymbol{s}) = \mathrm{Cmt}(\tilde{\tau}|\widetilde{\mathbf{V}};\boldsymbol{s}) \tag{4.24}$$

where $\tilde{g}_{ik} = \prod_{j=1}^{n} g_{ij}^{W_{jk}}$, $\tilde{h}_{ik} = \prod_{j=1}^{n} g_{ij}^{M_{jk}}$, $i = 1,\ldots,t$, $k=1,\ldots,n$; $\tilde{\sigma} = [\mathrm{G}, \tilde{\boldsymbol{g}}, m]$ and $\tilde{\tau} = [\mathrm{G}, \tilde{\boldsymbol{h}}, m]$. In this case the bilinear matrix relation $\mathbf{MBLR}(\sigma|U,V,\mathbf{Y},\mathbf{Q};\ \boxed{\boldsymbol{r},\boldsymbol{s},\mathbf{U},\mathbf{V}})$ with c.r.s. σ and arbitrary $\mathbf{Q} \in Z_m^{n\times n}$ is equivalent to a bilinear relation $\mathbf{MBLR}(\tilde{\sigma}, \tilde{\tau}|U,V, \mathbf{Y}, \mathbf{D}_\mathrm{Q};\ \boxed{\boldsymbol{r}, \boldsymbol{s}, \widetilde{\mathbf{U}},\widetilde{\mathbf{V}}})$ with c.r.s. $\tilde{\sigma}$, $\tilde{\tau}$ and diagonal matrix $\mathbf{D}_\mathrm{Q}$. Applying the methods in sec.4.1 to relation $\mathbf{MBLR}(\tilde{\sigma}, \tilde{\tau}|U,V, \mathbf{Y}, \mathbf{D}_\mathrm{Q};\ \boxed{\boldsymbol{r}, \boldsymbol{s}, \widetilde{\mathbf{U}},\widetilde{\mathbf{V}}})$, the matrix bilinear relation can be reduced to (4.19) since in this reduction the commitments to $\mathbf{U}$ and $\mathbf{V}$ are processed independently.

4.3 ∑-Protocol

On basis of the efficient equivalence between the bilinear matrix relation (4.17) over Z_m and the bilinear relation (4.19) over S, now we construct the efficient ZKA protocol for the latter. The relation is reformulated here with simplified notations:

$$\mathbf{SBLR}(\sigma,\tau|U,V,y,\mathbf{Q};\ \boxed{\boldsymbol{r},\boldsymbol{s},\boldsymbol{u},\boldsymbol{v}}):$$

$$U = \mathrm{Cmt}(\sigma|\boldsymbol{u};\boldsymbol{r}) \wedge V = \mathrm{Cmt}(\tau|\boldsymbol{v};\boldsymbol{s}) \wedge \boldsymbol{u}^\mathrm{T}\mathbf{Q}\boldsymbol{v} = y \tag{4.25}$$

where $\mathbf{Q}$ is a n-by-n diagonal matrix, y is an element in S; witnesses $\boldsymbol{u}$ and $\boldsymbol{v}$ are n-dimensional S-vectors, $\boldsymbol{r}$ and $\boldsymbol{s}$ are d-dimensional random vectors with components in set R. Note that in the following protocol, actually $\mathbf{Q}$ can be any diagonal matrix over S, unnecessarily limited to Z_m.

$\boxed{\text{Protocol } \sum\textbf{-ZKA/SBLR}}$

P→V: P samples $\boldsymbol{\rho}_1, \boldsymbol{\rho}_2 \overset{R}{\leftarrow} \mathrm{R}^d$, $\boldsymbol{x}_1, \boldsymbol{x}_2 \overset{R}{\leftarrow} \mathrm{S}^n$ at random;

P computes:

$\eta_1 = \boldsymbol{u}^{\mathrm{T}}\mathbf{Q}\boldsymbol{x}_2 + \boldsymbol{x}_1^{\mathrm{T}}\mathbf{Q}\boldsymbol{v}$, $\eta_2 = \boldsymbol{x}_1^{\mathrm{T}}\mathbf{Q}\boldsymbol{x}_2$, $K_1 = \mathrm{Cmt}(\sigma|\, \boldsymbol{x}_1, \boldsymbol{\rho}_1)$, $K_2 = \mathrm{Cmt}(\tau|\boldsymbol{x}_2, \boldsymbol{\rho}_2)$.

P sends message $[K_1, K_2, \eta_1, \eta_2]$ to V.

P←V: V samples $e \overset{R}{\leftarrow} \mathrm{E}_S$ from the exceptional set at random and sends e to P.

P→V: P computes $\boldsymbol{z}_1 = e\boldsymbol{u}+\boldsymbol{x}_1$, $\boldsymbol{z}_2 = e\boldsymbol{v}+\boldsymbol{x}_2$.

P computes randomness $\boldsymbol{\beta}_1, \boldsymbol{\beta}_2$ from $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{r}, \boldsymbol{s}, e, \boldsymbol{x}_1, \boldsymbol{x}_2$[4].

P sends message $[\boldsymbol{z}_1, \boldsymbol{z}_2, \boldsymbol{\beta}_1, \boldsymbol{\beta}_2]$ to V.

V: V verifies

$$K_1U^e = \mathrm{Cmt}(\sigma|\boldsymbol{z}_1; \boldsymbol{\beta}_1) \wedge K_2V^e = \mathrm{Cmt}(\tau|\boldsymbol{z}_2; \boldsymbol{\beta}_2) \wedge \boldsymbol{z}_1^{\mathrm{T}}\mathbf{Q}\boldsymbol{z}_2 = \eta_2 + e\eta_1 + e^2y \quad (4.26)$$

Theorem 4. The protocol ∑-ZKA/SBLR is unconditionally complete, special honest verifier zero-knowledge (SHVZK) and computationally 3-special-sound.

Proof In Appendix A.

4.4 Compressed Protocol with Logarithmic Message Complexity

In protocol ∑-ZKA/SBLR, the prover P convinces the verifier the following relation

$$\mathrm{SBLR}(\sigma,\tau|K_1U^e, K_2V^e, \eta_2+e\eta_1+e^2y, \mathbf{Q}; \boxed{\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \boldsymbol{z}_1, \boldsymbol{z}_2}) \quad (4.27)$$

by the last message $[\boldsymbol{z}_1,\boldsymbol{z}_2,\boldsymbol{\beta}_1,\boldsymbol{\beta}_2]$. Similar as the approach in [6][7], a dimension-reduction transformation in the witness space is introduced to establish a recursive proof of (4.27). Since $[\boldsymbol{z}_1,\boldsymbol{z}_2,\boldsymbol{\beta}_1,\boldsymbol{\beta}_2]$ perfectly hides the original witnesses, this proof is unnecessarily zero-knowledge.

In order to simplify the formulism, the following protocol NoZKA/SBLR is specified for relation (4.25) instead of (4.27), but notational correspondence is trivial. In case of $n = 2^k$ where n is dimension of the witness vector space, when the third message in protocol ∑-ZKA/SBLR is substituted with the following protocol NoZKA/SBLR and recursively expanded with $n \leftarrow n/2$ up to $n = 1$, a ZKA protocol with $2k+1$ rounds and $\mathrm{O}(k)$ message complexity for relation SBLR is obtained.

For reading convenience, relation SBLR is reformulated here with random numbers $\boldsymbol{r}$, $\boldsymbol{s}$ removed to simplify the formulism (they are not really needed for hiding since here the proof is unnecessarily zero-knowledge).

$$\mathrm{SBLR}(\sigma,\tau|U,V,y,\mathbf{Q}; \boxed{\boldsymbol{u}, \boldsymbol{v}}):$$

$$U = \mathrm{Cmt}(\sigma|\boldsymbol{u}) \wedge V = \mathrm{Cmt}(\tau|\boldsymbol{v}) \wedge \boldsymbol{u}^{\mathrm{T}}\mathbf{Q}\boldsymbol{v} = y \quad (4.28)$$

Notations for the compressed protocol:

Dimension of the witness vectors $\boldsymbol{u}$ and $\boldsymbol{v}$: $n = 2^k$.

c.r.s $\sigma \equiv [\mathrm{G}, \boldsymbol{g}, m]$, $\tau \equiv [\mathrm{G}, \boldsymbol{h}, m]$ where the group elements $\boldsymbol{g} \equiv (g_1,\ldots, g_n)$, $\boldsymbol{h} \equiv (h_1,\ldots, h_n)$are divided into two parts :

$\boldsymbol{g}_{\mathrm{L}} \equiv (g_1,\ldots, g_{n/2})$, $\boldsymbol{g}_{\mathrm{R}} \equiv (g_{n/2+1},\ldots, g_n)$, $\boldsymbol{h}_{\mathrm{L}} \equiv (h_1,\ldots, h_{n/2})$, $\boldsymbol{h}_{\mathrm{R}} \equiv (h_{n/2+1},\ldots, h_n)$.

n-dimensional vectors are decomposed into a direct-sum of $n/2$-dimensional parts:

[4] For notational simplification we always omit the long expressions to compute the randomness β_1 and β_2, which can be easily derived from the formulas in sec. 2 and 3 in [16].

$$\boldsymbol{u} = \boldsymbol{u}_{\mathrm{L}} \dot{+} \boldsymbol{u}_{\mathrm{R}},\ \boldsymbol{v} = \boldsymbol{v}_{\mathrm{L}} \dot{+} \boldsymbol{v}_{\mathrm{R}} \tag{4.29}$$

The n-by-n diagonal matrix $\mathbf{Q}$ is decomposed into submatrices as:

$$\mathbf{Q} = \begin{bmatrix} \boldsymbol{Q_L} & \boldsymbol{O} \\ \boldsymbol{O} & \boldsymbol{Q_R} \end{bmatrix} \tag{4.30}$$

where $\mathbf{Q}_{\mathrm{L}}$ and $\mathbf{Q}_{\mathrm{R}}$ are $n/2$-by-$n/2$ diagonal.

$\boxed{\text{Protocol } \textbf{NoZKA/SBLR}}$

P→V: P performs the computations in group G^d:

A_1=Cmt($\sigma|\boldsymbol{u}_{\mathrm{R}}\dot{+}\mathbf{0}$), A_2=Cmt($\tau|\boldsymbol{v}_{\mathrm{R}}\dot{+}\mathbf{0}$), B_1=Cmt($\sigma|\mathbf{0}\dot{+}\boldsymbol{u}_{\mathrm{L}}$), B_2=Cmt($\tau|\mathbf{0}\dot{+}\boldsymbol{v}_{\mathrm{L}}$) (4.31)

P performs the computations in Galois ring S:

$C_1=\boldsymbol{u}_{\mathrm{R}}^{\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{L}}+\boldsymbol{u}_{\mathrm{L}}^{\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{R}}$, $C_2=\boldsymbol{u}_{\mathrm{R}}^{\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{L}}+\boldsymbol{u}_{\mathrm{L}}^{\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{R}}$, $D_1=\boldsymbol{u}_{\mathrm{R}}^{\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{R}}$, $D_2=\boldsymbol{u}_{\mathrm{L}}^{\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{L}}$(4.32)

P sends message $[A_1,A_2,B_1,B_2,C_1,C_2,D_1,D_2]$ to V.

P←V: V samples $e\overset{R}{\leftarrow}\mathrm{E}_S$ at random and sends to P.

V computes:

$$U_e = A_1^{e^{-1}}U^eB_1^{e^3},\ \ V_e = A_2^{e^{-1}}V^eB_2^{e^3} \tag{4.33}$$

$$\mathbf{Q}_e = e^{-2}\mathbf{Q}_{\mathrm{L}}+e^2\mathbf{Q}_{\mathrm{R}} \ \text{ and } \ r_e = C_1e^{-2} + C_2e^2 + D_1e^{-4} + D_2e^4 \tag{4.34}$$

If n = 1(in this case the message received from P is $[u_e, v_e]$) then V verifies

$$U_e = \mathrm{Cmt}(\sigma|\,\boldsymbol{u}_e\dot{+}e^2\boldsymbol{u}_e) \wedge V_e = \mathrm{Cmt}(\tau|\boldsymbol{v}_e\dot{+}e^2\boldsymbol{v}_e)^5 \wedge u_e\mathrm{Q}_ev_e = y+r_e \tag{4.35}$$

otherwise n is substituted with $n/2$, U substituted with U_e, V with V_e, σ with σ_e= [G, $\boldsymbol{g}_{\mathrm{L}}$, m], τ with τ_e= [G, $\boldsymbol{h}_{\mathrm{L}}$, m] respectively.

P: On receiving the challenge e (in $\mathrm{E_S}$) from V, P performs:
computing σ_e= [G, $\boldsymbol{g}_{\mathrm{L}}$, m], τ_e= [G, $\boldsymbol{h}_{\mathrm{L}}$, m] and substituting σ with σ_e, τ with τ_e;

$\boldsymbol{u}_e = e\boldsymbol{u}_{\mathrm{L}}+e^{-1}\boldsymbol{u}_{\mathrm{R}}$, $\boldsymbol{v}_e = e\boldsymbol{v}_{\mathrm{L}}+e^{-1}\boldsymbol{v}_{\mathrm{R}}$, $\mathbf{Q}_e = e^{-2}\mathbf{Q}_{\mathrm{L}}+e^2\mathbf{Q}_{\mathrm{R}}$;

if n = 1 then P sends $[u_e, v_e]$ to V, otherwise P decomposes $\boldsymbol{u}_e$, $\boldsymbol{v}_e$ and $\boldsymbol{Q}_e$ according to (4.29) and (4.30), performs computations according to (4.33) and (4.34), sends message to V and then substitutes n with $n/2$.

Theorem 5 The protocol NoZKA/SBLR is $2k$-1 round, unconditionally complete and computationally (5, 5,…, 5)-special-sound.

Proof In Appendix A.

Remark 2 On basis of a general theorem proved in [13] that (μ_1,…, μ_k)-spacial soundness implies knowledge soundness, the above constructed protocol is ZKAoK.

[5] Actually U_e = Cmt($\sigma_e|u_e$) and V_e = Cmt($\tau_e|v_e$) which can be verified by the explicit expressions of the commitment in sec.2.4 and straightforward calculations.

4.5 Performance and Comparisons against Linearization Approach

There are $2n$ witnesses in S in the relation SBLR(4.25). For n=2^k, the whole protocol is $2k$+1 round, unconditionally complete and (3,5,5,…,5)-special sound (on basis of the commitment scheme's binding property) where:

The first message (P→V and also the first one in protocol ∑-ZKA/SBLR) is composed of $2d$ elements in group G and 2 elements in Galois ring S.

For the 2nd,4th, 6th, …, $2k$th messages (P←V), each one is composed of just 1 element in Galois ring's exceptional set E_S.

For the 3rd, 5th, 7th,…, $2k$-1th messages (P→V and all are messages of protocol NoZKA/SBLR), each one is composed of $4d$ elements in G and 4 elements in S.

The $2k$+1th (P→V and also the last message) is composed of 2 elements in S.

Totally, the whole protocol needs $4dk$ G-elements, $5k$ S-elements in its communication where $k = \log_2 n$.

Currently there are no other works on matrix bilinear relation over Galois ring comparable, so we make a comparison between the above results and the general linearization approach, which compiles any non-linear arithmetic relation (circuit) into a linear one via secret-sharing techniques (which works originally over Galois fields and can be directly generalized to Galois ring, see. Sec. 6 in [12]). In the following tables, the performance results are derived from the results of linearization approach [12] and those of linear relation over Galois ring (sec.4 in [13]), while the performance results about our approach is from the above analysis with (including the costs in reduction) 3 S-elements and 1 message added, and n (dimension of S-vectors in (4.25)) substituted with nt (dimension of S-vectors in (4.19)).

Table 3. Performance of ZKA for matrix bilinear relation in different approaches

	Linearization (e.g., [12][16])	Matrix-oriented (ours)
	Both with targeted knowledge error ≤ $p^{-d}\log n$ and $\mathbf{U},\mathbf{V}\in Z_m^{n\times td}$	
number of G-elements in c.r.s.	$4n^2t^2d^2 + 3$	nt
number of G-elements for commitment.	d	$2d$
number of rounds	$2\log(n^2+(1+2n^2)t^2d^2+4)+7$	$2+2\log(nt)$
message complexity	$2d\log(n^2+(1+2n^2)t^2d^2+4)$ G-element $3\log(n^2+(1+2n^2)t^2d^2+4)-1$ S-elements	$4d\log(nt)$ G-element. $3+5\log(nt)$ S-elements

In summary, by specifically making use of structural features of the commitment scheme and matrix equations, the matrix-oriented approach outperforms the general one for bilinear matrix relation in all aspects, e.g., for large-size n-by-n square witnesses the size of c.r.s. is reduced by > n^2d times; the number of rounds is reduced by > $1/2+\log d/2\log n$; total number of ring elements in messages reduced by > $1/6+5\log d/12\log n$; total umber of group elements asymptotically the same but decreased by a number of $4d\log d$ (see tab. 4). These improvements for bilinear relation are even better than those for the linear relation.

Table 4. Performance of ZKA for matrix bilinear relation in different approaches(square witness)

	Linearization (e.g., [12][16])	Matrix-oriented (ours)
	Both with targeted knowledge error $\leq p^{-d}\log n$ and $\mathbf{U},\mathbf{V}\epsilon Z_m^{n\times n}$	
number of G-elements in c.r.s.	$4n^4 + 3$	n^2/d
number of G-elements for commitment.	d	$2d$
number of rounds	$2\log(n^2+(1+2n^2)n^2+4)+7$ $\geq 8\log n$	$2+4\log n - 2\log d$
message complexity	$2d\log(n^2+(1+2n^2)n^2+4) \geq 8d\log n$ G-element $3\log(n^2+(1+2n^2)n^2+4)-1 \geq 12\log n$ S-elements	$8d\log n - 4d\log d$ G-element $3+10\log n - 5\log d$ S-elements

As an example, the ZKA protocol for bilinear matrix relation is used in private 2D spectrum reconstruction where **U** and **V** are (private) transformation squares. In this application n = 512, p = 2, s = 64 (so $m = 2^{64}$), G ≡ $J^+(N)$ = {a in Z_N: the Jacobi symbol (a/N)=1} (see sec.3.3[16] for details on this commitment-friendly group) with N=PQ where large primes P and Q are selected such that $(P\text{-}1)(Q\text{-}1)/4$ is odd. For knowledge-error $\varepsilon = 2^{-56} \approx 10^{-16}$ and the matched d = 64 ($\varepsilon \approx p^{-d}\log n$), the number of rounds is reduced by ≈ 85%; total number of ring elements reduced by ≈ 44%; total umber of group elements is decreased by 1536 (33%).

5 Concurrently Non-malleable Enhancement

In various private computing applications, zero-knowledge proof protocols need to be composed in complicated running environment. However, the protocols established in sec.3 and 4 can only ensure security in sequential composition. The concurrent non-malleable ZKA protocol[22] has such a property that, even a dishonest prover playing man-in-the-middle role by concurrently interacting with multiple honest provers, it still cannot efficiently generate a new statement and convince the verifier without knowing its witness. Such property enhances zero-knowledge proof protocol's security in concurrent environment. [20-22] developed a general approach to compile any ∑-protocol into a non-malleable one. In this section, we extend this method to compile any $2k$+1-round argument protocol into a non-malleable one with the same number of rounds and properly increased message and computational complexity.

5.1 Basic Tools

One of the crucial tools needed is the tag-based simulation-sound trapdoor commitment scheme. This is a trapdoor commitment scheme with input (x,t) where x is plaintext and t is a tag variable(usually some identity). Intuitively, its security ensures that an adversary cannot efficiently destroy the binding property even after collecting arbitrary number of commitments and related plaintexts, so its security is stronger than ordinary commitment schemes.

Definition 5(**Tag-based Commitment Scheme**[20]) CS ≡ (CGen,Cmt,Cvf) is called a *Tag-based Commitment Scheme* if CGen, Cmt, Cvf are all P.P.T algorithms and have the following properties:

(1) **Complete** For any (x,t) there holds

$$\mathrm{P}[pk\leftarrow \mathrm{CGen}(\lambda);\ (y,d)\leftarrow \mathrm{Cmt}(pk,x,t)\text{: }\mathrm{Cvf}(pk,y,x,t,d)=1] = 1$$

(2) **Binding** There exists a negligible function $\varepsilon(\lambda)$ s.t. for any P.P.T algorithm A:

$$\mathrm{P}[pk\leftarrow \mathrm{CGen}(\lambda);\ (y,t,x_1,x_2,d_1,d_2)\leftarrow \mathrm{A}(pk)\text{:}$$

$$\mathrm{Cvf}(pk,y,x_1,t,d_1)=1 \wedge \mathrm{Cvf}(pk,y,x_2,t,d_2)=1 \wedge x_1\neq x_2] \le \varepsilon(\lambda)$$

(3) **Hiding** For any pk generated by CGen, any x_1, x_2 in the same bit-size and any tag t, the output c_1 : $(c_1,d_1)\leftarrow\mathrm{Cmt}(pk,x_1,t)$ and c_2 : $(c_2,d_2)\leftarrow\mathrm{Cmt}(pk,x_2,t)$ are computationally indistinguishable.

In the following definition, the algorithm TCGen outputs public and private key-pair, i.e., $(pk,sk)\leftarrow\mathrm{CGen}(\lambda)$. The symbol TCGen_{pk} notates such a algorithm the same as TCGen but only outputs pk.

Definition 6 (Tag-based Trapdoor Commitment Scheme[20]) TC ≡ (TCGen, TCmt, TCvf, TCFakeCmt, TCFakeDmt) is a *tag-based trapdoor commitment scheme*, if all the five algorithms are P.P.T with (TCGen_{pk}, TCmt, TCvf) satisfying properties (1)~(3) in definition 5. In addition, for any (x,t) the two outputs

(pk,x,t,y^*,d^*):

$$(pk,sk)\leftarrow\mathrm{TCGen}(\lambda);\ (y^*,\delta)\leftarrow\mathrm{TCFakeCmt}(pk,sk,t);\ d^*\leftarrow\mathrm{TCFakeDmt}(\delta,y^*,x,t);$$

and (pk,x,t,y,d):

$$(pk,sk)\leftarrow\mathrm{TCGen}(\lambda);\ (y,d)\leftarrow\mathrm{TCmt}(pk,x,t);$$

are computationally indistinguishable.

Definition 7 (**Simulation Soundness of Tag-based Trapdoor Commitment Scheme**[20]) The scheme in definition 6 is called *simulation sound* if there exists a negligible function $\varepsilon(\lambda)$ such that for any P.P.T. algorithm A:

$$\mathrm{Adv}_{TC}^{SS}(\lambda) \equiv \mathrm{P}[(pk,sk)\leftarrow\mathrm{TCGen}(\lambda);\ (y,t,x_1,x_2,d_1,d_2)\leftarrow \mathrm{A}^{\mathrm{O}(\,.\,|\,sk)}(pk)\text{:}$$

$$\mathrm{TCvf}(pk,y,x_1,t,d_1)=1 \wedge \mathrm{TCvf}(pk,y,x_2,t,d_2)=1 \wedge x_1\neq x_2 \wedge t\notin \mathrm{Q}] \le \varepsilon(\lambda)$$

where the oracle $\mathrm{O}(.|sk)$ with the private key sk works in the following way:

(1) Initialize Q to be empty.

(2)For each query [“commit”, t]:

O(. | sk) computes $(y^*,\delta) = \mathrm{TCFakeCmt}(pk,sk,t)$; Store (y^*,t,δ); $\mathrm{Q} = \mathrm{Q}\cup\{t\}$;
Output y^*.

(3) For each query [“decommit”, y^*, x]:

```
IF some $(y^*,t,\delta)$ exists in current storage
THEN
        $d^*$=TCFakeDmt($\delta,y^*,x,t$); output $d^*$;
END
```

For efficient constructions of simulation sound trapdoor commitment(SSTC hereafter) scheme, see[20-22].

Another tool required for constructing the compiler is the strongly unforgeable one-time signature scheme, which constructions can be seen in , e.g., [19][23].

5.2 Concurrently Non-malleable ZKA protocol

For a given interactive algorithm M, let $\boxed{M}$ be a set of multiple instances of M running in any concurrent way. $\boxed{M}$ receives two classes of input instructions:

Instruction [START, *id, x,w*]: start a new instance of M, assign identifier *id* and input (σ, *x, w*) to it, where σ is the c.r.s.

Instruction [MSG, *id, m*]: send message *m* to the instance M(*id*) and return the output of this instance.

Given three interactive algorithms S, A≡(A_1,A_2) and B, let <S, A_1|A_2, B)> denote the interactions of A_1 with S and A_2 with B where (A_1,A_2) are coordinated, any information obtained by A_1 can be used by A_2 to generate the message sent to B and vice versa.

In any interaction, a trace is defined as a sequence of messages $Tr = [+m_1\text{-}m_2+m_3\text{-}m_4\ldots]$ where + and – represent the opposite message transmission directions. Two traces Tr_1 and Tr_2 are called *matched* if they have the same message terms but in opposite directions, e.g., $Tr_1 = [+m_1\text{-}m_2+m_3\text{-}m_4\ldots]$ and $Tr_2 = [\text{-}m_1+m_2\text{-}m_3+m_4\ldots]$.

Definition 8 (**Concurrent Non-Malleability of Zero Knowledge Proof /Argument**[22]) (D,P,V,(S_1,S_2)) is called a concurrently non-malleable zero knowledge argument protocol for a relation R if all algorithms D, P, V, S_1, S_2 are P.P.T. and have the following properties:

(1) **Completeness** For σ←D(λ) and (*x*, *w*) ∊ R there holds $P[<P(w); \underline{V}>_\sigma(x) = 1] = 1$.

(2) **Witness Extraction** For P.P.T algorithm $P^*\equiv(P_1^*,P_2^*)$ consider the game $Exp^{P^*}(\lambda)$:

```
$(\sigma,\tau) \leftarrow S_1(\lambda)$;
$(x^*,Tr^*,b^*) \leftarrow <\boxed{S^*(\tau)}, P_1^*| P_2^*,V>_\sigma$;
$Q\leftarrow\boxed{S^*(\tau)}$'s traces during the interactions;
IF $b^*= 1 \wedge_{Tr\in Q} Tr^*$ is unmatched with any $Tr$
THEN output 1;
ELSE output 0;
```

(*Tr* is the trace between interactions of P_1^* and $\boxed{S^*}$; b^* is the output of V on trace Tr^*; *unmatched* means Tr^* cannot be a copy of any trace appeared in the interactions between P_1^* and $\boxed{S^*}$.)

On each input (*x*,*w*), $\boxed{S^*(\tau)}$ decides whether R(*x*,*w*)=1: if true then it starts an instance $S_2(\tau,\sigma,x)$ otherwise does nothing. Let

$$\pi(P^*|\lambda) \equiv P[Exp^{P^*}(\lambda) = 1]$$

There exists an expected polynomial time algorithm Ext, a positive valued function κ and a negligible function ε such that, if $\pi(P^*|\lambda) > \kappa(\lambda)$ then Ext with rewind access to P^* can compute a w^* such that $(x^*,w^*)\in R$ with probability $\geq \pi(P^*|\lambda)-\kappa(\lambda)-\varepsilon(\lambda)$ where x^* is the output of P^* in Exp^{P^*}.

(3) **Zero-knowledge** For any P.P.T. algorithm V^* there has the computational indistinguishability

$$Tr<\boxed{P}, V^*>_\sigma(x) \overset{C}{\leftrightarrow} Tr<\boxed{S^{**}(\tau)}, V^*>_\sigma(x)$$

where σ on the left side is generated by D: $\sigma\leftarrow D(\lambda)$ and σ on the right side is generated by S_1: $(\sigma,\tau)\leftarrow S_1(\lambda)$. On each input (x,w), S^{**} decides whether $R(x,w)=1$: if true then it starts an instance $S_2(\tau,\sigma,x)$ otherwise does nothing. Note that S_2 always has the input $x\in L_R$ but not *w*.

5.3 Concurrently Non-Malleable ZKA Protocol's Construction

Let $R(\sigma|x,w)$ be the relation with c.r.s. σ, public input *x* and witness *w*; ZKAoK/R be the public-coin argument protocol for R with logarithmic message complexity and $2k+1$ rounds; A, A_i, B_i and ψ be polynomial-time algorithms in the protocol.

Protocol **ZKAoK/R**

```
P→V: P computes $(x_1,\xi_1) = A(\sigma,x,w)$ and sends $x_1$ to V;
//The 1st session
P←V: V samples $e_1$ at random and sends it to P;
     V computes $(b_2,\eta_2) = B_1(\sigma,x_1,e_1)$;
P→V: P computes $(x_2,\xi_2) = A_1(\xi_1,e_1)$ and sends $x_2$ to V;
//2nd session
P←V: V samples $e_2$ at random and sends it to P;
     V computes $(b_3,\eta_3) = B_2(\eta_2,x_2,e_2)$;
P→V: P computes $(x_3,\xi_3) = A_2(\xi_2,e_2)$ and sends $x_3$ to V;
 …………
// i-th session
P←V: V samples $e_i$ at random and sends it to P;
     V computes $(b_{i+1},\eta_{i+1}) = B_i(\eta_i,x_i,e_i)$;
P→V: P computes $(x_{i+1},\xi_{i+1}) = A_i(\xi_i,e_i)$ and sends $x_{i+1}$ to V;
………….
//The last session
P←V: V samples $e_k$ at random and sends it to P;
     V computes $(b_{k+1},\eta_{k+1}) = B_k(\eta_k,x_k,e_k)$;
P→V: P computes $x_{k+1} = A_k(\xi_k,e_k)$ and sends $x_{k+1}$ to V;
 V:  V verifies $\psi(\sigma,b_{k+1},x_{k+1},x) = 1$.
```

Let SSTC ≡ (TCGen, TCmt,TCvf, TCFakeCmt, TCFakeDmt) be the simulation-sound tag-based trapdoor commitment scheme defined in sec. 5.1; SG ≡ (KG,Sgn,Vf) be the strongly unforgeable one-time signature scheme with key generator KG, signing algorithm Sgn and verification algorithm Vf; H be a collision-resistant hash function. With these basic cryptographic schemes, a new argument protocol for relation R is compiled from protocol ZKAoK/R with new c.r.s. $\sigma^* \equiv [\sigma, pk]$ where σ is the original protocol's c.r.s. and pk is the public key of scheme SSTC.

Protocol **CNM-ZKAoK/R**

```
P→V: P computes: $(s\_vk, s\_sk) = \mathrm{KG}(\lambda)$;
                 $(x_1, \xi_1) = A(\sigma, x, w)$;
                 $(y_1, d_1) \leftarrow \mathrm{TCmt}(pk, x_1, \mathrm{H}(s\_vk||1))$;
     //Here $x_1$ in the original protocol is committed to with $\mathrm{H}(s\_vk||1)$ used as a tag.
     P sends message $[s\_vk, y_1]$ to V;
//1st session
P←V: V samples $e_1$ at random and sends it to P;
P→V: P computes $(x_2, \xi_2) = A_1(\xi_1, e_1)$; $(y_2, d_2) \leftarrow \mathrm{TCmt}(pk, x_2, \mathrm{H}(s\_vk||2))$;
     P sends $y_2$ to V;
//2nd session
P←V: V samples $e_2$ at random and sends it to P;
P→V: P computes $(x_3, \xi_3) = A_2(\xi_2, e_2)$; $(y_3,d_3) \leftarrow \mathrm{TCmt}(pk, x_3, \mathrm{H}(s\_vk||3))$;
     P sends $y_3$ to V;
//$i$-th session
P←V: V samples $e_i$ at random and sends it to P;
P→V: P computes $(x_{i+1}, \xi_{i+1}) = A_i(\xi_i, e_i)$; $(y_{i+1}, d_{i+1}) \leftarrow \mathrm{TCmt}(pk, x_{i+1}, \mathrm{H}(s\_vk||i+1))$;
     P sends $y_{i+1}$ to V;
//the last session
P←V: V samples $e_k$ at random and sends it to P;
P→V: P computes $x_{k+1} = A_k(\xi_k, e_k)$; $\boldsymbol{z} = (x_1, d_1, \ldots, x_k, d_k, x_{k+1})$;
                 $\boldsymbol{u} = (y_1, e_1, \ldots, y_k, e_k)$; $s = \mathrm{Sgn}(s\_sk, s\_vk||\boldsymbol{u}||\boldsymbol{z})$;
     //operator "||" means joining the string
     P sends $[\boldsymbol{z},s]$ to V;
V: On receiving the last message $\boldsymbol{z}$ from P, V computes:
        $(b_2,\eta_2) = B_1(\sigma,x_1,e_1)$; $(b_{i+1},\eta_{i+1}) = B_i(\eta_i,x_i,e_i)$, $i=2,\ldots,k$;
   then verifies $\psi(\sigma,b_{k+1},x_{k+1},x) = 1 \wedge \mathrm{Vf}(s\_vk, s\_vk||(y_1,e_1,\ldots, y_k,e_k)||\boldsymbol{z}, s) = 1$
        $\wedge_{i=1}^{k} T\mathrm{Cvf}(pk, y_i, x_i, \mathrm{H}(s\_vk||i),d_i) = 1$
```

Remark 3 As long as each y_i and d_i is in constant-size, total message size $\sum_{i=1}^{k}(|y_i| + |x_i| + |d_i|)+\mathrm{O}(1)$ of the new protocol will be only constant times that of the original protocol. Relative to the original protocol, the prover adds the workload to compute commitments in each round, while the verifier delays all intermediate computations to the last round with some additional verification computation. With efficient implementation of SSTC scheme, the total computational workload in new protocol is approximately constant times the original.

About the new protocol's properties, we have the following conclusions.

Lemma 3 If ZKAoK/R has SHVZK property, then CNM-ZKAoK/R is zero-knowledge in the sense of definition 8(3).

Proof In Appendix B.

Lemma 4 Suppose the protocol ZKAoK/R is ($\mu_1,\ldots,\mu_k$)-special sound, then there exists an extractor Ext for protocol CNM-ZKAoK/R as specified in def.8. Let the event EXT be "Ext outputs a w^* s.t. $(x^*,w^*)\in$R for an accepting statement x^*", |E| be the cardinality of the space for the verifier to sample challenges, then:

$$\mathrm{P[EXT]} > \pi(\mathrm{P}^*|\lambda) - \sum_{i=1}^{k}\mu_i/|\mathrm{E}| - \mathrm{Adv}_{TC}^{SS}(\lambda)\prod_{i=1}^{k}\mu_i + \mathrm{poly}(\lambda)\mathrm{Adv}_{SG}^{UF(1)}(\lambda)$$

(Adv_{TC}^{SS} specified in def. 7, $\pi(\mathrm{P}^*|\lambda)$ in def. 8) and Ext's running time is poly(λ).

Proof In Appendix B.

Remark 4 For Galois ring GR(m,d) with $m = p^s$, we have $|\mathrm{E}| = p^{-d}$. For non-malleable enhanced protocols over GR(m,d) with μ = O(1) and k = O(log$n$), if $k\mu/|\mathrm{E}| \sim 2^{-\lambda}$ then d should take the value > (λ+log$k\mu$)/log$p$.

In summary, one obtains the general result:

Theorem 6 If ZKAoK/R is an argument protocol for relation R with special soundness and SHVZK property (in terms of def. 2 and 3), then CNM-ZKAoK/R is a concurrently non-malleable zero knowledge argument protocol for R in terms of def. 10.

References

1 I Damagard, R. Cramer, J.B.Nielsen. Secure multiparty computation and secret sharing. Cambridge: Cambridge University Press, 2015.

2 J. Furukawa, Y. Lindell. Two-thirds honest-majority MPC for malicious adversaries at Almost the Cost of Semi-Honest. In: 26th ACM CCS, 1557-1571, 2019.

3 A Kosba, C. Papamanthou, E.Shi. xJsnark: A framework for efficient verifiable computation. IEEE Symposium on Privacy & Security, 2018, 128-149.

4 E. Cecchetti, F. Zhang, Y Ji, A. Kosba, A. Juels, E.Shi. Solidus: Confidential distributed ledger transactions via PVORM. ACM Computer & Communication Security, Dalas U.S.A., 2017, 701-718.

5 B.Bunz, B.Fish, A. Szeieniec. Transparent SNARKS froms DARK compilers, Eurocrypt, Heidelberg: Springer, Lecture Notes in Computer Science, Vol. 12115, 677-706. 2020.

6 J. Bootle, A. Cerulli, P. Chaidos, J. Groth, and C. Petit. Efficient zero-knowledge arguments for arithmetic circuits in the discrete log setting. EUROCRYPT 2016, Heidelberg: Springer, Lecture Notes in Computer Science, Vol. 9666, 327–357. 2016.

7 B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell. Bulletproofs: Short proofs for confidential transactions and more. IEEE Symposium on Security and Privacy, 315–334. IEEE Computer Society Press, 2018.

8 Hoffmann M, Klooß M, Rupp A: Efficient zero- knowledge arguments in discrete log setting, revisited. ACM Conference on Computer and Communication Security, 2019.

9 Attema T, Cramer R, Rambaud M. Compressed Σ-Protocols for bilinear group arithmetic circuits and application to logarithmic transparent threshold signatures. Advances in Cryptology - ASIACRYPT 2021, 526–556.

10 Russell W, Lai F, G Malavolta, V Ronge. Succinct arguments for bilinear group arithmetic: Practical structure -preserving cryptography. ACM Conference on Computer and Communications Security, 2057–2074. 2019.

11 Attema T, Cramer R, Fehr S. Compressing proofs of k-out-of-n partial knowledge. Heidelberg: Springer, Advances in Cryptology, 2021, 65–89.

12 Attema T, Cramer M. Compressed Σ-protocol theory and practical application to plug and play secure algorithms. CRYPTO, Heidelberg: Springer, Lecture Notes in Computer Science, 513–543, 2020. Full-version available at IACR ePrint 2020/152.

13 Attema T, Cramer R, Kohl L. A compressed Σ-Protocol theory for lattices, CRYPTO, Lecture Notes in Computer Science Vol. 12826, 549-579, 2021.

14 Geoffroy Couteau, Thomas Peters, and David Pointcheval. Removing the strong RSA assumption from arguments over the integers, EUROCRYPT, Heidelberg: Springer, Lecture Notes in Computer Science, Vol. 10211, 321-350, 2017.

15 Ivan Damgard and Eiichiro Fujisaki. A statistically-hiding integer commitment scheme based on groups with hidden order. ASIACRYPT 2002, Heidelberg: Springer, Lecture Notes in Computer Science, Vol. 2501, 125–142, 2002.

16 Attema T, Cascudo I, Cramer R, Damgard I, Escudero D. Vector commitments over rings and compressed Sigma-protocols. Theory of Cryptography Conference, 173-202, 2022.

17 Wan, Z.: Lectures on Finite Fields and Galois Rings. Academy of Sciences Press, Beijing. (2006). .

18 Goldreich O. Foundations of Cryptography. Vol 1.Basic Techniques. Cambridge: Cambridge University Press, 2005.

19 Katz J, Lindell Y. Introduction to Modern Cryptography. Chapman Hall/CRC Press, 2020.

20 Mackenzie P, Yang Ke. On simulation sound trapdoor commitments. Advances in Cryptology, Lecture Notes in Computer Science Vol. 3027, 382-400, 2003.

21 Garay J.A., Mackenzie P, Yang Ke. Strengthening zero-knowledge protocols using Signature. Journal of Cryptology, 2006, 19(1):169-209.

22 Gennaro R. Multi-trapdoor commitments and their applications to non-malleable protocols. CRYPTO 2004, Lecture Notes in Computer Science Vol. 3152: 220-236, 2004.

23 D. Bleichenbacher, U. Maurer. On the efficiency of one-time digital signatures. ASIACRYPT'96, Lecture Notes in Compter Science, Vol.1163, 145–158, Springer 1996.

24 Elman R, Karpenko N and Merkurjev A. Algebraic and geometric theory of quadratic forms[M]. New York: American Mathematical Society, 2017.

APPENDIX A. Proofs of Theorem 4 and 5

Theorem 4. The protocol ∑-ZKA/SBLR* is unconditionally complete, special honest verifier zero-knowledge (SHVZK) and computationally 3-special-sound.

Proof If P has all the witnesses ***r***, ***s***, ***u***, ***v*** then:

$$z_1^{\mathrm{T}}\mathbf{Q}z_2 = (e\boldsymbol{u}+\boldsymbol{x}_1)^{\mathrm{T}}\mathbf{Q}(e\boldsymbol{v}+\boldsymbol{x}_2) = \boldsymbol{x}_1^{\mathrm{T}}\mathbf{Q}\boldsymbol{x}_2+e(\boldsymbol{x}_1^{\mathrm{T}}\mathbf{Q}\boldsymbol{v}+\boldsymbol{u}^{\mathrm{T}}\mathbf{Q}\boldsymbol{x}_2)+e^2\boldsymbol{u}^{\mathrm{T}}\mathbf{Q}\boldsymbol{v} = \eta_2+e\eta_1+e^2y$$

Other two equalities in (4.26) can be easily confirmed by the homomorphic property of the commitment scheme, so the completeness is proved.

The protocol's SHVZK property can be proved by constructing the following simulator which on input of (σ,e) performs the computation:

samples $\eta_1\overset{R}{\leftarrow}\mathrm{S}$; $\boldsymbol{\beta}_1, \boldsymbol{\beta}_2 \overset{R}{\leftarrow}\mathrm{S}^d$ and $z_1, z_2 \overset{R}{\leftarrow}\mathrm{S}^n$ at random;

$K_1 = U^{-e}\mathrm{Cmt}(\sigma|z_1, \boldsymbol{\beta}_1)$, $K_2 = V^{-e}\mathrm{Cmt}(\tau|z_2, \boldsymbol{\beta}_2)$, $\eta_2 = z_1^{\mathrm{T}}\mathbf{Q}z_2–e\eta_1–e^2y$;

output(K_1, K_2, η_1, η_2, e, z_1, z_2, $\boldsymbol{\beta}_1$, $\boldsymbol{\beta}_2$).

It's straightforward to verify that the trace output by the simulator has the same distribution as the real trace in the interactions between the honest prover and the verifier, so the SHVZK property holds.

To prove the 3-special soundness, consider three accepting traces Tr_i=[K_1, K_2, η_1, η_2, e_i, z_{i1}, z_{i2}, $\boldsymbol{\beta}_{i1}$, $\boldsymbol{\beta}_{i2}$] with distinct challenges e_1, e_2, e_3 sampled from E_{S}.

For Tr_1 和 Tr_2, there exist μ_1 and μ_2 in S which can be efficiently computed as solutions to the equations:

$$\mu_1 + \mu_2 = 0,\ e_1\mu_1 + e_2\mu_2 = 1 \qquad \text{(A.1)}$$

From the equations K_1U^e = Cmt(σ|z_1, $\boldsymbol{\beta}_1$) i=1,2 in (4.26), one can get

$$U = \prod_{i=1}^{2}(K_1U^{e_i})^{\mu_i} = \prod_{i=1}^{2}\mathrm{Cmt}(\sigma|\boldsymbol{z}_{i1},\boldsymbol{\beta}_{i1})^{\mu_i} = \mathrm{Cmt}(\sigma|\boldsymbol{u}^*, \boldsymbol{r}^*) \qquad \text{(A.2)}$$

where $$\boldsymbol{u}^* = \sum_{i=1}^{2}\mu_i\,\boldsymbol{z}_{i1}$$

In the same way we also have

$$V = \mathrm{Cmt}(\tau|\boldsymbol{v}^*, \boldsymbol{s}^*) \text{ where } \boldsymbol{v}^* = \sum_{i=1}^{2}\mu_i\,\boldsymbol{z}_{i2} \qquad \text{(A.3)}$$

Now we claim that there exist $\boldsymbol{x}_1$, $\boldsymbol{x}_2$ which are independent of i satisfying:

$$z_{i1} = e_i\boldsymbol{u}^*+\boldsymbol{x}_1,\ z_{i2} = e_i\boldsymbol{v}^*+\boldsymbol{x}_2,\ i=1,2 \qquad \text{(A.4)}$$

Indeed, let $z_{i1} = e_i\boldsymbol{u}^* + \xi_i$, i=1,2 then by

$$\boldsymbol{u}^* = \sum_{i=1}^{2}\mu_i\,\boldsymbol{z}_{i1}=\sum_{i=1}^{2}\mu_i\,(e_i\boldsymbol{u}^* + \xi_i) = \boldsymbol{u}^*\sum_{i=1}^{2}\mu_i\,e_i+\mu_1\xi_1+\mu_2\xi_2 = \boldsymbol{u}^*+\mu_1(\xi_1–\xi_2)$$

and $\mu_1\neq0$ one gets $\xi_1 = \xi_2$ and denote this by $\boldsymbol{x}_1$. In a similar way one can confirm the existence of $\boldsymbol{x}_2$ satisfying (A.4).

Substituting z_{i1} and z_{i2} in (4.26)'s equations $z_{i1}^{\mathrm{T}}\mathbf{Q}z_{i2}=\eta_2+e_i\eta_1+e_i^2y$ i =1,2 with the expressions in (A.4), after simple algebraic calculations one gets

$$\eta_2 - \boldsymbol{x}_1{}^{\mathrm{T}}\mathbf{Q}\boldsymbol{x}_2 + (\eta_1 - \boldsymbol{x}_1{}^{\mathrm{T}}\mathbf{Q}\boldsymbol{v}^* - \boldsymbol{u}^{*\mathrm{T}}\mathbf{Q}\boldsymbol{x}_2)e_i + (y - \boldsymbol{u}^{*\mathrm{T}}\mathbf{Q}\boldsymbol{v}^*)e_i^2 = 0 \quad i = 1,2 \qquad \text{(A.5)}$$

which shows that e_1 and e_2 are roots of the degree-2 polynomial $\eta_2 - \boldsymbol{x}_1{}^{\mathrm{T}}\mathbf{Q}\boldsymbol{x}_2 + (\eta_1 - \boldsymbol{x}_1{}^{\mathrm{T}}\mathbf{Q}\boldsymbol{v}^* - \boldsymbol{u}^{*\mathrm{T}}\mathbf{Q}\boldsymbol{x}_2)T + (y^* - \boldsymbol{u}^{*\mathrm{T}}\mathbf{Q}\boldsymbol{v}^*)T^2$. This result is obtained from traces Tr_1 and Tr_2 with the resulted "witnesses"

$$\boldsymbol{r}^*, \boldsymbol{s}^*, \boldsymbol{u}^*, \boldsymbol{v}^*, \boldsymbol{x}_1, \boldsymbol{x}_2 \qquad \text{(A.6)}$$

When the same analysis is applied to traces Tr_2 and Tr_3, another group of "witnesses"

$$\boldsymbol{r}', \boldsymbol{s}', \boldsymbol{u}', \boldsymbol{v}', \boldsymbol{x}_1{}', \boldsymbol{x}_2{}' \qquad \text{(A.7)}$$

can be obtained which also satisfy equations (A. 2)~(A.3), i.e.,

$$\mathrm{Cmt}(\sigma|\boldsymbol{u}^*, \boldsymbol{r}^*) = U = \mathrm{Cmt}(\sigma|\boldsymbol{u}', \boldsymbol{r}'),\ \mathrm{Cmt}(\tau|\boldsymbol{v}^*, \boldsymbol{s}^*) = V = \mathrm{Cmt}(\tau|\boldsymbol{v}', \boldsymbol{s}')$$

Under the binding property of the commitment scheme, these equalities imply

$$\boldsymbol{u}^* = \boldsymbol{u}', \boldsymbol{v}^* = \boldsymbol{v}'$$

Note that equalities in (A.4) hold at i = 2 for both "witnesses" in (A.6) and (A.7), which implies

$$\boldsymbol{x}_1 = \boldsymbol{x}_1{}',\ \ \boldsymbol{x}_2 = \boldsymbol{x}_2{}'$$

Equation (A.5) with coefficients y', $\boldsymbol{u}'$, $\boldsymbol{v}'$, $\boldsymbol{x}_1{}'$, $\boldsymbol{x}_2{}'$ also hold for e_2 and e_3. As a result, the coefficients in (A.5) are independent of i = 1,2,3, which means the degree-2 polynomial $\eta_2 - \boldsymbol{x}_1{}^{\mathrm{T}}\mathbf{Q}\boldsymbol{x}_2 + (\eta_1 - \boldsymbol{x}_1{}^{\mathrm{T}}\mathbf{Q}\boldsymbol{v}^* - \boldsymbol{u}^{*\mathrm{T}}\mathbf{Q}\boldsymbol{x}_2)T + (y - \boldsymbol{u}^{*\mathrm{T}}\mathbf{Q}\boldsymbol{v}^*)T^2$ has at least three distinct roots e_1, e_2, e_3 in the exceptional set E_S, so it must be identically zero. In particular, $y = \boldsymbol{u}^{*\mathrm{T}}\mathbf{Q}\boldsymbol{v}^*$. This proves that $\boldsymbol{u}^*$, $\boldsymbol{v}^*$ are correctly extracted witnesses.

Theorem 5 The protocol NoZKA/SBLR is 2k-1 round, unconditionally complete and computationally (5, 5,…, 5)-special-sound.

Proof Completeness can be confirmed by straightforward algebraic calculations. In order to prove (5, 5,…, 5)-special-soundness, we construct an extractor which outputs the witness $\boldsymbol{u}$, $\boldsymbol{v}$ and all variables $[A_1,A_2,B_1,B_2,C_1,C_2,D_1,D_2]$ from 5 accepting traces with $e_i^2 \neq e_j^2$ in E_S, i=1,2,3,4,5:

$$\mathrm{Tr}_i \equiv [[A_1,A_2,B_1,B_2,C_1,C_2,D_1,D_2], e_i, [\boldsymbol{u}_{ei}, \boldsymbol{v}_{ei}]]$$

where each trace satisfies

$$U_{ei} = \mathrm{Cmt}(\sigma|\ \boldsymbol{u}_{ei} \dot{+} e_i^2\boldsymbol{u}_{ei}) \wedge V_{ei} = \mathrm{Cmt}(\tau|\ \boldsymbol{v}_{ei} \dot{+} e_i^2\boldsymbol{v}_{ei}) \wedge \boldsymbol{u}_{ei}{}^{\mathrm{T}}\mathbf{Q}_{ei}\boldsymbol{v}_{ei} = y + r_{ei} \qquad \text{(A.8)}$$

If this claim can be proved for each recursive step, the whole protocol is (5,…,5)-special sound.

Consider three traces Tr_i: i=1,2,3 at first. For these traces μ_1, μ_2, μ_3 can be efficiently calculated as solution to the equations:

$$\textstyle\sum_{i=1}^{3} e_i^{-1}\,\mu_i = 0,\ \ \sum_{i=1}^{3} e_i\ \ \mu_i = 1,\ \ \sum_{i=1}^{3} e_i^3\,\mu_i = 0 \qquad \text{(A.9)}$$

For notational simplicity, all variables with subscript e_i will be subscripted only by i, e.g., U_{e_i} is simply notated as U_i. Combining the verification equation $U_i = \mathrm{Cmt}(\sigma|$

$\boldsymbol{u}_{ei}\dot{+}e_i^2\boldsymbol{u}_{ei})$, i=1,2,3 in (A.8) with (4.33) and (A.9) one can get:

$$U = \prod_{i=1}^{3}(A_1^{e_i^{-1}}\,U^{e_i}\;B_1^{e_i^3})^{\mu_i} = \prod_{i=1}^{3} U_i^{\mu_i} = \prod_{i=1}^{3} \mathrm{Cmt}(\sigma|\,\boldsymbol{u}_{ei}\dot{+}e_i^2\boldsymbol{u}_{ei})^{\mu_i}$$

Using the commitment scheme's explicit expressions in sec. 2.4, one obtains:

$$U = \mathrm{Cmt}(\sigma|[\boldsymbol{u}_{\mathrm{L}}^{*}\dot{+}\boldsymbol{u}_{\mathrm{R}}^{*}])\text{ where }\boldsymbol{u}_{\mathrm{L}}^{*}=\sum_{i=1}^{3}\mu_i\,\boldsymbol{u}_i,\ \boldsymbol{u}_R^{*}=\sum_{i=1}^{3}e_i^2\,\mu_i\boldsymbol{u}_i \qquad \text{(A.10)}$$

Similarly, one can also obtains:

$$V = \mathrm{Cmt}(\tau|[\boldsymbol{v}_{\mathrm{L}}^{*}\dot{+}\boldsymbol{v}_{\mathrm{R}}^{*}])\text{ where }\boldsymbol{v}_{\mathrm{L}}^{*} = \sum_{i=1}^{3}\mu_i\,\boldsymbol{v}_i,\ \ \boldsymbol{v}_R^{*} =\sum_{i=1}^{3}e_i^2\,\mu_i\boldsymbol{v}_i \qquad \text{(A.11)}$$

Also ν_1,ν_2,ν_3 and $\gamma_1,\gamma_2,\gamma_3$ can be efficiently calculated as solutions to the following equations:

$$\sum_{i=1}^{3}e_i^{-1}\,\nu_i= 1,\ \ \sum_{i=1}^{3}e_i\nu_i= 0,\ \ \sum_{i=1}^{3}e_i^3\,\nu_i= 0 \qquad \text{(A.12)}$$

$$\sum_{i=1}^{3}e_i^{-1}\,\gamma_i= 0,\ \ \sum_{i=1}^{3}e_i\gamma_i= 0, \sum_{i=1}^{3}e_i^3\,\gamma_i= 1 \qquad \text{(A.13)}$$

Combining U_i= Cmt(σ| $\boldsymbol{u}_{ei}\dot{+}e_i^2\boldsymbol{u}_{ei}$), i=1,2,3 in (A.8) with (4.33), (A.12), there derives:

$$A_1 = \prod_{i=1}^{3}(A_1^{e_i^{-1}}\,U^{e_i}\;B_1^{e_i^3})^{\nu_i} = \prod_{i=1}^{3} U_i^{\nu_i} = \prod_{i=1}^{3}\mathrm{Cmt}(\sigma|\ \boldsymbol{u}_{ei}\dot{+}e_i^2\boldsymbol{u}_{ei})^{\nu_i}$$

i.e., $A_1 = \mathrm{Cmt}(\sigma|[\boldsymbol{w}_{\mathrm{L}}^{*}\dot{+}\boldsymbol{w}_{\mathrm{R}}^{*}])$ where $\boldsymbol{w}_{\mathrm{L}}^{*} = \sum_{i=1}^{3}\nu_i\,\boldsymbol{u}_i$, $\boldsymbol{w}_R^{*} =\sum_{i=1}^{3}e_i^2\,\nu_i\boldsymbol{u}_i$ (A.14)

In a similar way, one can also get:

$$B_1 = \mathrm{Cmt}(\sigma|[{}^*\boldsymbol{w}_{\mathrm{L}}\dot{+}{}^*\boldsymbol{w}_{\mathrm{R}}])\text{ where }{}^*\boldsymbol{w}_{\mathrm{L}}= \sum_{i=1}^{3}\gamma_i\,\boldsymbol{u}_i,\ {}^*\boldsymbol{w}_R=\sum_{i=1}^{3}e_i{}^2\,\gamma_i\boldsymbol{u}_i \qquad \text{(A.15)}$$

$$A_2 = \mathrm{Cmt}(\sigma|[\boldsymbol{q}_{\mathrm{L}}^{*}\dot{+}\boldsymbol{q}_{\mathrm{R}}^{*}])\text{ where }\ \boldsymbol{q}_{\mathrm{L}}^{*} = \sum_{i=1}^{3}\nu_i\,\boldsymbol{v}_i,\ \ \boldsymbol{q}_R^{*}=\sum_{i=1}^{3}e_i{}^2\,\nu_i\boldsymbol{v}_i$$

$$B_2 = \mathrm{Cmt}(\sigma|[{}^*\boldsymbol{q}_{\mathrm{L}}\dot{+}{}^*\boldsymbol{q}_{\mathrm{R}}])\text{ where }{}^*\boldsymbol{q}_{\mathrm{L}} = \sum_{i=1}^{3}\gamma_i\,\boldsymbol{v}_i,\ \ {}^*\boldsymbol{q}_R=\sum_{i=1}^{3}e_i{}^2\,\gamma_i\boldsymbol{v}_i$$

By the equality $U_i = A_1^{e_i^{-2}}\,U^{e_i}\;B_1^{e_i^3}$ in (4.33) and U_i= Cmt(σ|[$\boldsymbol{u}_i\dot{+}e_i^2\boldsymbol{u}_i$]) in (A.8) for i=1,2,3, we get:

$$A_1^{e_i^{-1}}\,U^{e_i}\;B_1^{e_i^3} = \mathrm{Cmt}(\sigma|[\boldsymbol{u}_i\dot{+}e_i^2\boldsymbol{u}_i])$$

Put A_1, U, B_1's expressions (A.14), (A.10), (A.15) into the above expression, the obtained equality implies

$$\boldsymbol{u}_i = e_i\boldsymbol{u}_{\mathrm{L}}^{*} + e_i^{-1}\boldsymbol{w}_{\mathrm{L}}^{*} + e_i^{3}\,{}^*\boldsymbol{w}_{\mathrm{L}}\,,\quad e_i{}^2\boldsymbol{u}_i = e_i\,\boldsymbol{u}_{\mathrm{R}}^{*} + e_i^{-1}\boldsymbol{w}_{\mathrm{R}}^{*} + e_i^{3}\,{}^*\boldsymbol{w}_{\mathrm{R}}\quad i=1,2,3 \qquad \text{(A.16)}$$

due to the commitment's binding property. After eliminating $\boldsymbol{u}_i$ one has

$$\boldsymbol{w}_{\mathrm{R}}^{*} + (\boldsymbol{u}_{\mathrm{R}}^{*}-\boldsymbol{w}_{\mathrm{L}}^{*})e_i^{2} + ({}^*\boldsymbol{w}_{\mathrm{R}}-\boldsymbol{u}_{\mathrm{L}}^{*})e_i^{4} - {}^*\boldsymbol{w}_{\mathrm{L}}e_i^{6} = 0 \qquad \text{(A.17)}$$

Equation (A.17) is satisfied by $\boldsymbol{u}_{\mathrm{L}}^{*}$, $\boldsymbol{u}_{\mathrm{R}}^{*}$, $\boldsymbol{w}_{\mathrm{L}}^{*}$, ${}^*\boldsymbol{w}_{\mathrm{R}}$ which can be efficiently calculated from Tr_1, Tr_2, Tr_3 with challenges e_i in $\mathrm{E_S}$: i=1,2,3. When the derivation is applied to Tr_3, Tr_4, Tr_5, one can also calculate $\boldsymbol{u}_{\mathrm{L}*}$, $\boldsymbol{u}_{\mathrm{R}*}$, ${}_*\boldsymbol{w}_{\mathrm{L}}$, ${}_*\boldsymbol{w}_{\mathrm{R}}$ which satisfy the same equations with e_i in $\mathrm{E_S}$: i=3,4,5. These two groups of calculated results all satisfy

$$\mathrm{Cmt}(\sigma|\boldsymbol{u}_{\mathrm{L}}^{*}\dot{+}\boldsymbol{u}_{\mathrm{R}}^{*}) = U = \mathrm{Cmt}(\sigma|\boldsymbol{u}_{\mathrm{L}*}\dot{+}\boldsymbol{u}_{\mathrm{R}*})$$

$$\mathrm{Cmt}(\sigma|\boldsymbol{w}_{\mathrm{L}}{}^{*}\dotplus\boldsymbol{w}_{\mathrm{R}}{}^{*}) = A_1 = \mathrm{Cmt}(\sigma|\boldsymbol{w}_{\mathrm{L}*}\dotplus\boldsymbol{w}_{\mathrm{R}*})$$

$$\mathrm{Cmt}(\sigma|{}^{*}\boldsymbol{w}_{\mathrm{L}}\dotplus{}^{*}\boldsymbol{w}_{\mathrm{R}}) = B_1 = \mathrm{Cmt}(\sigma|{}_{*}\boldsymbol{w}_{\mathrm{L}}\dotplus{}_{*}\boldsymbol{w}_{\mathrm{R}})$$

Due to binding property of the commitment scheme, these equalities imply:

$$\boldsymbol{u}_{\mathrm{L}}{}^{*} = \boldsymbol{u}_{\mathrm{L}*},\ \boldsymbol{u}_{\mathrm{R}}{}^{*} = \boldsymbol{u}_{\mathrm{R}*},\ {}^{*}\boldsymbol{w}_{\mathrm{L}} = {}_{*}\boldsymbol{w}_{\mathrm{L}},\ {}^{*}\boldsymbol{w}_{\mathrm{R}} = {}_{*}\boldsymbol{w}_{\mathrm{R}} \tag{A.18}$$

As a result, (A.17) holds for more than 4 challenges e_i, i.e., degree-3 polynomial $\boldsymbol{w}_{\mathrm{R}}{}^{*}+(\boldsymbol{u}_{\mathrm{R}}{}^{*}-\boldsymbol{w}_{\mathrm{L}}{}^{*})T+({}^{*}\boldsymbol{w}_{\mathrm{R}}-\boldsymbol{u}_{\mathrm{L}}{}^{*})T^2-{}^{*}\boldsymbol{w}_{\mathrm{L}}T^3$ in T has more than 4 distinct zeros e_i^2 ($e_i^2 \neq e_j^2$, i=1,2,3,4,5) in $\mathrm{E_S}$, which implies all its coefficients are zero:

$$\boldsymbol{w}_{\mathrm{R}}{}^{*} = 0,\ \boldsymbol{u}_{\mathrm{R}}{}^{*} = \boldsymbol{w}_{\mathrm{L}}{}^{*},\ {}^{*}\boldsymbol{w}_{\mathrm{R}} = \boldsymbol{u}_{\mathrm{L}}{}^{*},\ {}^{*}\boldsymbol{w}_{\mathrm{L}} = 0 \tag{A.19}$$

Combining (A.19) with (A.14) and (A.15) one obtains

$$A_1 = \mathrm{Cmt}(\sigma|\boldsymbol{u}_{\mathrm{R}}{}^{*}\dotplus\boldsymbol{0}),\ \ B_1 = \mathrm{Cmt}(\sigma|\boldsymbol{0}\dotplus\boldsymbol{u}_{\mathrm{L}}{}^{*}) \tag{A.20}$$

Combining (A.19) with (A.16) and (A.18) one obtains

$$\boldsymbol{u}_i = e_i\boldsymbol{u}_{\mathrm{L}}{}^{*} + e_i^{-1}\boldsymbol{u}_{\mathrm{R}}{}^{*}\ \ i=1,\ldots,5 \tag{A.21}$$

In a similar way one can also obtain

$$A_2 = \mathrm{Cmt}(\tau|\boldsymbol{v}_{\mathrm{R}}{}^{*}\dotplus\boldsymbol{0}),\ \ B_2 = \mathrm{Cmt}(\tau|\boldsymbol{0}\dotplus\boldsymbol{v}_{\mathrm{L}}{}^{*}) \tag{A.22}$$

$$\boldsymbol{v}_i = e_i\boldsymbol{v}_{\mathrm{L}}{}^{*} + e_i^{-1}\boldsymbol{v}_{\mathrm{R}}{}^{*}\ \ i=1,\ldots,5 \tag{A.23}$$

Combining the equation $\boldsymbol{u}_e{}^{\mathrm{T}}\mathbf{Q}_e\boldsymbol{v}_e = y + r_e$ in (A.8) with equalities (A.21), (A.23) and $\mathbf{Q}_e = e^{-2}\mathbf{Q}_{\mathrm{L}}+e^2\mathbf{Q}_{\mathrm{R}}$ in (4.34), one has (for each i = 1,…,5):

$$\begin{aligned} y + r_i = \boldsymbol{u}_i{}^{\mathrm{T}}\mathbf{Q}_i\boldsymbol{v}_i &= (e_i\boldsymbol{u}_{\mathrm{L}}{}^{*}+e_i^{-1}\boldsymbol{u}_{\mathrm{R}}{}^{*})^{\mathrm{T}}(e^{-2}\mathbf{Q}_{\mathrm{L}}+e^2\mathbf{Q}_{\mathrm{R}})(e_i\boldsymbol{v}_{\mathrm{L}}{}^{*}+e_i^{-1}\boldsymbol{v}_{\mathrm{R}}{}^{*}) \\ &= \boldsymbol{u}_{\mathrm{L}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{L}}{}^{*}+\boldsymbol{u}_{\mathrm{R}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{R}}{}^{*} + (\boldsymbol{u}_{\mathrm{R}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{L}}{}^{*}+\boldsymbol{u}_{\mathrm{L}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{R}}{}^{*})e_i^{-2} \\ &\quad + (\boldsymbol{u}_{\mathrm{R}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{L}}{}^{*}+\boldsymbol{u}_{\mathrm{L}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{R}}{}^{*})e_i^{2} + \boldsymbol{u}_{\mathrm{R}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{R}}{}^{*}e_i^{-4} + \boldsymbol{u}_{\mathrm{L}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{L}}{}^{*}e_i^{4} \end{aligned} \tag{A.24}$$

Put r_i's expression (4.34) into (A.24) and after simple calculations, one gets:

$$\begin{aligned} &\boldsymbol{u}_{\mathrm{L}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{L}}{}^{*}+\boldsymbol{u}_{\mathrm{R}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{R}}{}^{*}-y+(\boldsymbol{u}_{\mathrm{R}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{L}}{}^{*}+\boldsymbol{u}_{\mathrm{L}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{R}}{}^{*}-C_1)e_i^{-2} \\ &+ (\boldsymbol{u}_{\mathrm{R}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{L}}{}^{*}+\boldsymbol{u}_{\mathrm{L}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{R}}{}^{*}-C_2)e_i^{2}+(\boldsymbol{u}_{\mathrm{R}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{R}}{}^{*}-D_1)e_i^{-4}+(\boldsymbol{u}_{\mathrm{L}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{L}}{}^{*}-D_2)e_i^{4}=0 \end{aligned} \tag{A.25}$$

i.e., the degree-4 polynomial in T

$$\begin{aligned} &\boldsymbol{u}_{\mathrm{R}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{R}}{}^{*}-D_1 + (\boldsymbol{u}_{\mathrm{R}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{L}}{}^{*}+\boldsymbol{u}_{\mathrm{L}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{R}}{}^{*}-C_1)T+(\boldsymbol{u}_{\mathrm{L}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{L}}{}^{*}+\boldsymbol{u}_{\mathrm{R}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{R}}{}^{*}-y)T^2 \\ &+ (\boldsymbol{u}_{\mathrm{R}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{L}}{}^{*}+\boldsymbol{u}_{\mathrm{L}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{R}}{}^{*}-C_2)T^3 + (\boldsymbol{u}_{\mathrm{L}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{L}}{}^{*}-D_2)T^4 \end{aligned}$$

has 5 distinct zeros e_i^2 in $\mathrm{E_S}$: i = 1,…,5, which implies all its coefficients are zero:

$$\begin{aligned} &C_1 = \boldsymbol{u}_{\mathrm{R}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{L}}{}^{*} + \boldsymbol{u}_{\mathrm{L}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{R}}{}^{*},\ \ C_2 = \boldsymbol{u}_{\mathrm{R}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{L}}{}^{*} + \boldsymbol{u}_{\mathrm{L}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{R}}{}^{*} \\ &D_1 = \boldsymbol{u}_{\mathrm{R}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{R}}{}^{*},\ \ D_2 = \boldsymbol{u}_{\mathrm{L}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{L}}{}^{*},\ \ y = \boldsymbol{u}_{\mathrm{L}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{L}}\boldsymbol{v}_{\mathrm{L}}{}^{*}+\boldsymbol{u}_{\mathrm{R}}{}^{*\mathrm{T}}\mathbf{Q}_{\mathrm{R}}\boldsymbol{v}_{\mathrm{R}}{}^{*} = \boldsymbol{u}^{*\mathrm{T}}\mathbf{Q}\boldsymbol{v}^{*} \end{aligned} \tag{A.26}$$

where

$$\boldsymbol{u}^{*} = \boldsymbol{u}_{\mathrm{L}}{}^{*}\dotplus\boldsymbol{u}_{\mathrm{R}}{}^{*},\ \boldsymbol{v}^{*} = \boldsymbol{v}_{\mathrm{L}}{}^{*}\dotplus\boldsymbol{v}_{\mathrm{R}}{}^{*} \tag{A.27}$$

These results show that $\boldsymbol{u}^{*}$, $\boldsymbol{v}^{*}$ satisfy the bilinear equation $y = \boldsymbol{u}^{*\mathrm{T}}\mathbf{Q}\boldsymbol{v}^{*}$ and the two commitments. The above arguments also provides an efficient knowledge extractor which computes the witness $(\boldsymbol{u}^*,\boldsymbol{v}^*)$ and all related variables in consistency with the protocol's specification from 5 accepting traces$\{\mathrm{Tr}_i$: $e_i^2 \neq e_j^2$, i=1,2,3,4,5$\}$. Since this fact is true for each recursive step, the whole protocol is (5,…,5)-special-sound.

APPENDIX B. Proofs of lemma 3 and 4

Lemma 3 If ZKAoK/R has SHVZK property, then CNM-ZKAoK/R is zero-knowledge in the sense of definition 8(3).

Proof Let S^0 be zero-knowledge simulator of ZKAoK/R, the simulator $S \equiv (S_1,S_2)$ for CNM-ZKAoK/R is constructed in the following:

```
S_1(λ):
    Generate the c.r.s. $\sigma$ for ZKAoK/R;
    Compute $(pk, sk)$ = TCGen($\lambda$);  $\sigma^* = [\sigma, pk]$;
    Output($\sigma^*$, $sk$)
    //SSTC's private key $sk$ will be used as the trapdoor $\tau$
S_2($\tau$, $\sigma^*$, $x$):
    Compute $(s\_vk, s\_sk)$ = KG($\lambda$);
    For each $1 \le i \le k$:
        Compute $t_i$ = H($s\_vk||i$); $(Y_i, \delta_i)$=TCFakeCmt($pk, sk, t_i$);        (B.1)
        Send message $[s\_vk, Y_1]$ to $V^*$;
        For the $i$-th challenge $e_i$ from $V^*$, $1 \le i \le k$-1, response $V^*$ with $Y_{i+1}$;
        For the $k$-th challenge $e_k$ from $V^*$, compute:
            $(X_1,\ldots,X_k, X_{k+1}) = S^0(\sigma, x; e_1,\ldots, e_k)$;
            $D_i$ = TCFakeDmt($\delta_i, Y_i, X_i, t_i$); $1 \le i \le k$-1        (B.2)
            $\boldsymbol{Z}^* = (X_1, D_1,\ldots, X_k, D_k, X_{k+1})$;
            $\boldsymbol{U}^* = (Y_1, e_1,\ldots, Y_k, e_k)$;
            $s^*$ = Sgn($s\_sk, s\_vk||\boldsymbol{U}^*||\boldsymbol{Z}^*$);
        Then Send $[\boldsymbol{Z}^*, s^*]$ to $V^*$.
```

According to the above construction, the $P \rightarrow V^*$ trace simulated by S is TR = $[s\_vk, Y_1,\ldots, Y_k, (X_1, D_1,\ldots,X_k, D_k, X_{k+1}), s^*]$. Now we claim that TR is computationally indistinguishable with the real $P \rightarrow V^*$ trace tr = $[s\_vk, y_1,\ldots,y_k,(x_1,d_1,\ldots,x_k, d_k,x_{k+1}), s]$.

Obviously in TR and tr both s_vk's are in the same distribution, furthermore the tags t_i = H($s\_vk||i$) in TR and tr are in the same distribution.

Due to (B.1), (B.2) and SSTC's trapdoor property(definition 8), for each $1 \le i \le k$ there is the following computational indistinguishability:

$$(X_i, t_i, Y_i, D_i) \overset{C}{\leftrightarrow} (X_i, t_i, \overline{y_\iota}, \overline{d_\iota})$$

where $$(\overline{y_\iota}, \overline{d_\iota}) = \mathrm{TCmt}(pk, X_i, t_i) \tag{B.3}$$

hence $$\mathrm{TR} \overset{C}{\leftrightarrow} \overline{\mathrm{tr}} \tag{B.4}$$

where $\overline{\mathrm{tr}} \equiv [s\_vk, \overline{y_1},\ldots,\overline{y_k},(X_1,\overline{d_1},\ldots, X_k,\overline{d_k}, X_{k+1}),\bar{s}]$, $\bar{s} \equiv$ Sgn($s\_sk, s\_vk||\overline{\boldsymbol{U}}||\overline{\boldsymbol{Z}}$), $\overline{\boldsymbol{U}}$ and $\overline{\boldsymbol{Z}}$ are the expressions resulted from replacing Y_i with $\overline{y_\iota}$, D_i with $\overline{d_\iota}$ in $\boldsymbol{U}^*$'s and $\boldsymbol{Z}^*$'s expressions(see (B.2)).

For simulator S^0 there holds:

$$(X_1,\ldots,X_k, X_{k+1}) \overset{C}{\leftrightarrow} (x_1,\ldots,x_k, x_{k+1}) \qquad \text{(B.5)}$$

where $(x_1,\ldots,x_k, x_{k+1})$ is the real message sequence output from P. In CNM-ZKAoK/R each x_i has the commitment:

$$(y_i, d_i) = \mathrm{TCmt}(pk, x_i, \mathrm{H}(s\_vk||i)) \qquad \text{(B.6)}$$

So (B.3)~(B.6) implies:

$$\mathrm{TR} \overset{C}{\leftrightarrow} \mathrm{tr} \qquad \text{(B.7)}$$

where tr ≡ $[s\_vk, y_1, \ldots, y_k,(x_1, d_1,\ldots, x_k, d_k, x_{k+1}),s]$, $s \equiv \mathrm{Sgn}(s\_sk, s\_vk||\boldsymbol{U}||\boldsymbol{Z})$, $\boldsymbol{U}$ and $\boldsymbol{Z}$ are the expressions resulted from replacing $\overline{y_i}$ with y_i, X_i with x_i, $\overline{d_i}$ with d_i in the expressions of $\overline{\boldsymbol{U}}$ and $\overline{\boldsymbol{Z}}$. Obviously, tr and the real trace are in the same distribution.

Lemma 4 Suppose the protocol ZKAoK/R is $(\mu_1,\ldots, \mu_k)$-special sound, then there exists an extractor Ext for protocol CNM-ZKAoK/R as specified in def.8. Let the event EXT be "Ext outputs a w^* s.t. $(x^*,w^*)\in$R for an accepting statement x^*", |E| be the cardinality of the space for the verifier to sample challenges, then:

$$\mathrm{P[EXT]} > \pi(\mathrm{P}^*|\lambda) - \textstyle\sum_{i=1}^{k} \mu_i/|\mathrm{E}| - \mathrm{Adv}_{TC}^{SS}(\lambda) \prod_{i=1}^{k} \mu_i + \mathrm{poly}(\lambda)\mathrm{Adv}_{SG}^{UF(1)}(\lambda)$$

(Adv_{TC}^{SS} specified in def. 7, $\pi(\mathrm{P}^*|\lambda)$ in def. 8) and Ext's running time is poly(λ).

Proof Let $\mathrm{P}^*\equiv(\mathrm{P}_1^*,\mathrm{P}_2^*)$ be a P.P.T. algorithm which convinces the verifier with a statement x^* in the game $\mathrm{Exp}^{\mathrm{P}*}$ in definition 8, i.e:

$$(x^*,\mathrm{Tr}^*,b^*) = <\boxed{\mathrm{S}^*(\tau)}, \mathrm{P}_1^*|\, \mathrm{P}_2^*,\mathrm{V}>_\sigma$$

$$\text{with } b^* = 1 \wedge_{\mathrm{Tr}\in\mathrm{Q}} \mathrm{Tr}^* \text{ is unmatched with any Tr.}$$

where $\mathrm{Tr}^* \equiv [s\_vk^*, y_1^*,\ldots, y_k^*, (x_1^*, d_1^*,\ldots, x_k^*, d_k^*, x_{k+1}^*), s^*]$, S ≡ $(\mathrm{S}_1,\mathrm{S}_2)$ be the simulator constructed in lemma 3's proof. For presentational simplicity, let $\mu_1 = \ldots = \mu_k \equiv \mu$, otherwise for $\mu \equiv \max \mu_i$ the following argument is still valid.

We construct a P.P.T. extractor **Ext** which calls P^* and interacts with it both in the role of prover (via its component algorithm Ext::P) and the role of verifier (via the component algorithm Ext:V). Since Ext can rewind P^*(mainly P_2^* in the following) to any state, for presentational simplicity we take an equivalent view in concurrent environment that Ext can *fork* P^* instance at any state. The forked instance inherits its parent state and proceeds as specified in the protocol from that state on.

Ext executes the interactions with P^* in the follow way:

In the role of prover, Ext::P calls the simulator S to interact with P_1^*. Note that S_1 calls SSTC's key-generator TCGen to generate and output the public/secret key pair (pk, sk) so Ext can obtain this key pair from S.

In the role of verifier, each time right before Ext::V sends the first challenge e_1 to P_2^*, Ext forks it into μ P_2^*-instances and sends randomly independent and pairwise distinct challenges $e_i^{(1)}$, $i = 1,\ldots, \mu$ to each P_2^*-instance.

Every time right before Ext::V sends the second challenge e_2 to some P_2^*-instance, Ext forks it into μ P_2^*-instances, sends independent and pairwise distinct challenges $e_1^{(2)},\ldots, e_\mu^{(2)}$ to each instance.

Every instance inherits its parent's state and proceeds after receiving its challenge. Such operations proceed until all rounds are finished in protocol CNM-ZKAoK/R.

Let $\mathrm{T}(x^*)$ be a tree constructed as stated in definition 3 for the above interactions, with $[s\_vk^*, y_1^*]$ as its root. According to the above operation, $\mathrm{T}(x^*)$ is a session tree and each path γ in the tree is a trace $\mathrm{Tr}{<}\mathrm{P}_2^*,\mathrm{V}{>}(x^*)$.

Since the verifier generates k challenges in CNM-ZKAoK/R, i.e., each path in $\mathrm{T}(x^*)$ has k edges along it, so in the tree:

Total number of edges $\mathrm{N} = \mu+\mu^2+\ldots+\mu^k < \mu^{k+1}$

Total number of nodes $\mathrm{M} = 1+\mu+\mu^2+\ldots+\mu^{k-1} < \mu^k$ (B.8)

Total number of paths K = total number of leaves = μ^k

Define a event $\boxed{\mathrm{Succ}}$ as:

Tree $\mathrm{T}(x^*)$ is accepting, i.e., $b^*(\gamma) = 1$ for every path γ in the tree.

Consider two subevents $\mathrm{P}[\mathrm{Succ}\wedge\mathrm{T}^0(x^*)]$ and $\mathrm{P}[\mathrm{Succ}\wedge\sim\mathrm{T}^0(x^*)]$.

In the event of $\boxed{\mathrm{Succ}\wedge\mathrm{T}^0(x^*)}$, Succ occurs and all session variables x_i associated with nodes $y_i(\gamma)$ ($y_i(\gamma)$ stands for a node on path γ and at level i) in the accepting tree $\mathrm{T}(x^*)$ are in consistency with each other, i.e., $x_i(\gamma) = x_i(\beta)$ for any path γ and β bifurcating at node $y_i(\gamma)$ (so $y_i(\gamma) = y_i(\beta) \equiv y_i$, $i\geq 1$), so after replacing each node y_i with x_i one can obtain an accepting session tree of protocol ZKAoK/R., denoted as $\mathrm{T}^0(x^*)$.

Since ZKAoK/R is $(\mu_1, \ldots, \mu_k)$-special sound, its P.P.T. extractor Ext^0 can be called by Ext to output a w^* s.t. $(x^*,w^*)\in\mathrm{R}$. In particular:

$$\mathrm{P}[\mathrm{Succ} \wedge\mathrm{T}^0(x^*)] \leq \mathrm{P}[\mathrm{Ext\ outputs\ a\ } w^* \mathrm{\ s.t.\ } (x^*,w^*)\in\mathrm{R}] \qquad \text{(B.9)}$$

and note that the event on the right side is just $\boxed{\mathrm{EXT}}$.

For arguments on the complimentary event $\boxed{\mathrm{Succ}\wedge\sim\mathrm{T}^0(x^*)}$, i.e., no session tree for protocol ZKAoK/R can be successfully derived from $\mathrm{T}(x^*)$ in the abovementioned way, we consider two further subcases.

Case I: *s_vk^* does not appear in any message output from* S_2

We construct a P.P.T. algorithm **A** on basis of P^* to destroy SSTC's simulation soundness in this case. **A** has SSTC's public key pk as one of its input, has access to oracle-$\mathrm{O}(.|sk)$ and controls interactions of S (in role of prover) and V with P^* similarly as Ext does. During the interactions, whenever S_2 needs to generate the message Y_i or D_i in the protocol(see (B.1) and (B.2)), **A** queries its oracle-$\mathrm{O}(.|sk)$ with ["commit", t_i] or ["decommit", Y_i, X_i] and returns the oracle's response to S_2.

In the event of $\mathrm{Succ}\wedge\sim\mathrm{T}^0(x^*)$, there exist at least two paths γ^* and β^* in $\mathrm{T}(x^*)$ which bifurcate at some node $y_i(\gamma^*) = y_i(\beta^*) \equiv y_i^*$ $(i\geq 1)$ with the associated session variables unequal: $x_i(\gamma^*) \neq x_i(\beta^*)$. On the other hand, $b(\gamma^*) = b(\beta^*) = 1$ so

$$\mathrm{TCvf}(pk, y_i^*, x_i(\gamma^*), t_i, d_i(\gamma^*)) = 1 \wedge \mathrm{TCvf}(pk, y_i^*, x_i(\beta^*), t_i, d_i(\beta^*)) = 1$$

where $t_i = \mathrm{H}(s\_vk^*||i)$ is independent with any path.

In case I s_vk^* does not appear in any message output from S_2 and H is collision-resistant, no t_i can be in the set of tags once received by oracle-$\mathrm{O}(.|sk)$. As a result, the algorithm **A** generates a output destroying scheme SSTC's simulation soundness with the probability

$$p_{\mathrm{I}} \equiv \mathrm{P}[\mathrm{Succ} \wedge\sim\mathrm{T}^0(x^*) \wedge\mathrm{Case\ I}] \leq \mathrm{M}\,\mathrm{Adv}_{TC}^{SS}(\lambda) < \mu^k\mathrm{Adv}_{TC}^{SS}(\lambda) \qquad \text{(B.10)}$$

Case II: s_vk^* *does appear in some message output from* S_2

On basis of P^*, we construct a P.P.T. algorithm **B** to destroy strong unforgeability of the one-time signature scheme SG in this case. **B** has the signature verification key s_vk^* as one of its input and has access to the signing oracle-OSgn(. $|s\_sk^*$) at most one-time.

Let T be total number of message sequences output from S_2 during interactions with P^*. B selects a $m\in\{1,2,\ldots,T\}$ uniformly, inserts s_vk^* into the m-th message sequence during the interactions between S_2 and P_1^*, and generates the signature of this trace required by CNM-ZKAoK/R via accessing oracle-OSgn(.$|s\_sk^*$).

If the m-th sequence Tr_m is the one where s_vk^* appeared, then B makes P^* succeed in generating an accepting trace $Tr^*\neq Tr_m$. The fact that Tr^* contains a signature s^* satisfying $Vf(s\_vk^*, Tr^*, s^*)=1$ implies B's success in destroying SG's one-time unforgeability. Obviously:

$$p_{II} \equiv P[Succ \wedge\sim T^0(x^*) \wedge Case\ II] \leq T Adv_{SG}^{UF(1)}(\lambda) \quad (B.11)$$

Since Case I and II are complementary, from (B.10) and (B.11) one obtains

$$P[Succ \wedge\sim T^0(x^*)] = p_I + p_{II} \leq \mu^k Adv_{TC}^{SS}(\lambda) + T Adv_{SG}^{UF(1)}(\lambda) \quad (B.12)$$

Combining (B.9) and (B.12) one has:

$$P[Succ] = P[Succ\wedge T^0(x^*)] + P[Succ\wedge\sim T^0(x^*)]$$

$$\leq P[EXT] + \mu^k Adv_{TC}^{SS}(\lambda) + T Adv_{SG}^{UF(1)}(\lambda) \quad (B.13)$$

On the other hand, one can apply an analysis similar as that in sec.3 in [13](see lemma 5 there) to obtain a lower-bound of P[Succ] as[6]:

$$P[Succ] > \pi(P^*|\lambda) - k\mu/|E| \quad (B.14)$$

So $$P[EXT] > \pi(P^*|\lambda) - k\mu/|E| - \mu^k Adv_{TC}^{SS}(\lambda) + T Adv_{SG}^{UF(1)}(\lambda) \quad (B.15)$$

Note that n,T = poly(λ), μ = O(1) and k = O(log$n$) so the third and fourth terms in (B.15) are both negligible in λ. According to Ext's construction, its running time is μ^kpoly(n) = O(poly(n)) = O(poly(λ)). This completes the proof.

APPENDIX C. More about ZKA for Matrix Linear Relations

C.1 ZKA for Eigenvalue Relation: A$\boldsymbol{u}$ = λ$\boldsymbol{u}$

Consider the eigenvalue relation over residue ring Z_m for matrix $\mathbf{A}\in Z_m^{n\times n}$, vector $\boldsymbol{u}\in Z_m^n$ and eigenvalue λ in Z_m: A$\boldsymbol{u}$ = λ$\boldsymbol{u}$ where **A** is the witness (otherwise the problem is trivial), $\boldsymbol{u}$ and λ are public. $n = td$ is a power of 2 and d is the extension degree

[6] Event Succ implies that Ext successfully outputs a witness of x^* which probability's lower bound established in lemma 5 in [13] is ε–κ, where ε is the success probability of a dishonest prover P^* to cheat the verifier. By definitions and notations in this paper, ε is just $\pi(P^*|\lambda)$ (see def.8 in sec.5). Furthermore the expression of M in our notations here is $\kappa = 1 - \prod_{i=1}^{k}(1-\mu)/|E|$. Since $\kappa < \mu k/|E|$ so $P[Succ] > \pi(P^*|\lambda) - k\mu/|E|$.

of Galois ring S ≡ GR(m,d) = Z_m[X]/(f(X)) which value is determined by the target knowledge-error.

Let $\mathbf{A} = \begin{bmatrix} \boldsymbol{A}_1 \\ \vdots \\ \boldsymbol{A}_t \end{bmatrix}$ with each $\mathbf{A}_i \in Z_m^{d\times n}$, the equation A$\boldsymbol{u}$ = λ$\boldsymbol{u}$ is equivalent to

$$\mathbf{A}_i \boldsymbol{u} = \lambda \boldsymbol{u}^{(i)} \equiv \lambda \begin{bmatrix} u_{1+(i-1)d} \\ \vdots \\ u_{id} \end{bmatrix},\ i = 1,\ldots, t \qquad \text{(C.1)}$$

For randomness ρ in E_S the relation (C.1) is equivalent with probability > 1- t/p^d to the relation:

$$\textstyle\sum_{i=1}^{t} \mathbf{A}_i\, \rho^{i-1}\boldsymbol{u} = \lambda \sum_{i=1}^{t} \rho^{i-1}\, \boldsymbol{u}^{(i)} \equiv \lambda \boldsymbol{u}_\rho$$

i.e.,

$$[\mathbf{A}_1, \ldots, \mathbf{A}_t] \begin{bmatrix} \boldsymbol{u} \\ \rho\boldsymbol{u} \\ \vdots \\ \rho^{t-1}\boldsymbol{u} \end{bmatrix} = \lambda \boldsymbol{u}_\rho \qquad \text{(C.2)}$$

This is a collection of d linear relations over S. Let $\mathbf{A}^*$ and $\boldsymbol{u}_\rho^*$ be the matrix and vector on left side of (C.2), left-multiplying this equality by [1,δ, δ^2,…, δ^{d-1}] furthermore equivalently reduces it to the following relation with probability > 1– t/p^d:

$$[1,\delta, \delta^2,\ldots, \delta^{d-1}]\mathbf{A}^*\boldsymbol{u}_\rho^* = \lambda[1,\delta, \delta^2,\ldots, \delta^{d-1}]\boldsymbol{u}_\rho \equiv \lambda\bar{u}_{\rho,\delta}$$

i.e.,

$$\boldsymbol{a}_\delta^{*T}\boldsymbol{u}_\rho^* = \lambda\bar{u}_{\rho,\delta} \qquad \text{(C.3)}$$

where $\boldsymbol{a}_\delta^{*T} \equiv [1,\delta, \delta^2,\ldots, \delta^{d-1}]\mathbf{A}^* \in S^{tn}$, $\boldsymbol{u}_\rho^* \in S^{tn}$ and $\lambda\bar{u}_{\rho,\delta}$ in S. Let σ ≡ [G, $\boldsymbol{g}$, m] be the public-key for the commitment scheme with nt G-elements in $\boldsymbol{g}$ and used as the c.r.s, A is the commitment to matrix **A**:

$$G^d \ni A = \mathrm{Cmt}(\sigma|[\mathbf{A}_1, \ldots, \mathbf{A}_t])$$

$$= \begin{bmatrix} cmt_\sigma(A_1(1,1),\ldots,A_1(1,n),\ldots,A_t(1,1),\ldots,A_t(1,n)) \\ \vdots \\ cmt_\sigma(A_1(d,1),\ldots,A_1(d,n),\ldots,A_t(d,1),\ldots,A_t(d,n)) \end{bmatrix} \qquad \text{(C.4)}$$

then (C.3) is a linear relation over S with witness $\boldsymbol{a}_\delta^{*T} \in S^{tn}$ which commitment can be computed from the commitment to matrix **A** by(see (2.7)~(2.7)):

$$\mathrm{Cmt}(\sigma|\, \boldsymbol{a}_\delta^*) = A^{\Gamma\delta} \qquad \text{(C.5)}$$

where $\Gamma_\delta \in Z_m^{d\times d}$ is the coefficient matrix of polynomials 1, δ, δ^2,…, δ^{d-1}in S:

$$\begin{bmatrix} 1 \\ \delta \\ \vdots \\ \delta^{t-1} \end{bmatrix} = \Gamma_\delta \begin{bmatrix} 1 \\ X \\ \vdots \\ X^{t-1} \end{bmatrix} \bmod f(X) \qquad \text{(C.6)}$$

In summary, if the eigenvalue relation over Z_m is defined as:

$$\mathrm{SEVR}(\sigma|A, \boldsymbol{u}, \lambda;\ \boxed{\mathbf{A}, \boldsymbol{\gamma}}): \qquad \text{(C.7)}$$

$$A = \mathrm{Cmt}(\sigma|\mathbf{A}; \boldsymbol{\gamma}) \wedge \mathbf{A}\boldsymbol{u} = \lambda\boldsymbol{u}$$

where **A**∈ $Z_m^{n\times n}$, ***u***∈ Z_m^n, λ∈Z$_m$ and Cmt(σ|**A**) is specified by (C.4), then for independent randomness ρ, δ in E$_S$ it is probabilistic-equivalent to the linear relation (C.3) over Galois ring S with witness $\boldsymbol{a}_\delta^*$∈S^{nt} which commitment is computed by (C.5) from A and the reduction soundness factor is t+d (= n/d+d). The compressed ZKA protocol constructed for (C.3) has 4log$n$–2log$d$–1 rounds, (4log$n$–2log$d$–3)d G-elements and totally 6log$n$–3log$d$ S-elements in its messages, reducing the costs of vector-oriented approach by the amounts similar as indicated in table 2.

C.2 ZKA for Linear Matrix Relation: AUB^T = C

Consider the linear relation over residue ring Z$_m$ for matrix **A,B,C,U** ∈ $Z_m^{n\times n}$ where **U** is the witness, n = td is a power of 2 and d is the extension degree of Galois ring S ≡ GR(m,d) which value is determined by the target knowledge-error. Let

$$\mathbf{U} = [\mathbf{U}_1,\ldots,\mathbf{U}_t],\ \mathbf{C} = [\mathbf{C}_1,\ldots,\mathbf{C}_t] \text{ with each } \mathbf{U}_i,\ \mathbf{C}_i \in Z_m^{n\times d}$$

$$\mathbf{U}^* \equiv \begin{bmatrix}\mathbf{U}_1\\ \vdots\\ \mathbf{U}_t\end{bmatrix},\ \mathbf{C}^* \equiv \begin{bmatrix}\mathbf{C}_1\\ \vdots\\ \mathbf{C}_t\end{bmatrix} \in Z_m^{nt\times d}$$

Both **U*** and **C*** can be regarded as the matrices with row-index (kl) and column-index h for k=1,…,n, l=1,…,t, h=1,…,d:

$$U^*_{kl,h} = U_{k,(l-1)d+h},\ \ C^*_{kl,h} = C_{k,(l-1)d+h}$$

By reformulating the indices, the component-wise form of the equation **AUB^T** = **C** can be represented as:

$$C_{i,(j-1)d+q} = \sum_{k=1}^{n}\sum_{l=1}^{t}\sum_{h=1}^{d} A_{ik}\, B_{(j-1)d+q,(l-1)d+h} U_{k,(l-1)d+h}$$

$$i = 1,\ldots,n,\ j = 1,\ldots,t,\ q = 1,\ldots,d$$

$$\text{i.e., } \tilde{\mathbf{C}} = \mathbf{\Omega}(\mathbf{A},\mathbf{B})\mathbf{U}^* \qquad \text{(C.8)}$$

where $\tilde{\mathbf{C}}$ ∈ $Z_m^{n^2\times d}$ has entries $\tilde{C}_{ij,q}$ ≡ $C_{i,(j-1)d+q}$ and **Ω(A,B)** ∈$Z_m^{n^2\times nt}$ has entries:

$$\mathbf{\Omega}(\mathbf{A},\mathbf{B})_{ijq,\,klh} \equiv A_{ik}B_{(j-1)d+q,\,(l-1)d+h} \quad i, k=1,\ldots,n;\ j,l =1,\ldots,t \qquad \text{(C.9)}$$

In summary, the relation **AUB^T** = **C** with witness **U** ∈ $Z_m^{n\times n}$ is equivalent to the relation (C.8) with witness **U***∈ $Z_m^{nt\times d}$. The ZKA protocol for the former can be equivalently constructed for the latter with the method presented in sec.3.1~3.2, with performance indicated in the second column in tab.2.

C.3 ZKA for Linear Matrix Relation: AU + UB^T = C

Consider the linear relation over residue ring Z$_m$ for matrix **A,B,C,U** ∈ $Z_m^{n\times n}$ where **U** is the witness, n = td is a power of 2 and d is the extension degree of Galois ring S ≡ GR(m,d) which value is determined by the target knowledge-error.

Let **U*** and **C*** be specified as in C.2, obviously in the same way as that in C.2 **AU** + **UB^T** = **C** is equivalent to the equation

$$\tilde{\mathbf{C}} = (\mathbf{\Omega}(\mathbf{A},\mathbf{I}_n) + \mathbf{\Omega}(\mathbf{I}_n,\mathbf{B}))\mathbf{U}^* \qquad \text{(C.10)}$$

where **Ω(A,B)** is specified in (C.9) for any given matrix **A** and **B**. The ZKA protocol for $\mathbf{AU} + \mathbf{UB}^{\mathrm{T}} = \mathbf{C}$ can be equivalently constructed for(C.10) with the method presented in sec.3.1~3.2. The performance is indicated in the second column in tab.2.

C.4 Some Special Cases

Matrix-oriented approach can have some additional advantages in some special cases. Consider two linear matrix relations **AU** = **B** and **CV** = **D** where **A**, $\mathbf{C}\in Z_m^{l\times n}$ and **B**, $\mathbf{D}\in Z_m^{d\times d}$. Of course they can be proved independently by running the proof protocols over GR(m,d) established in sec.3.1-3.2., each with knowledge-error ≈ $p^{-d}\log n$. However, under some conditions there is more efficient way to prove **AU**=**B** ∧ **CV**=**D** by running a single protocol instance with significantly lower knowledge-error ≈ $p^{-2d}\log n$ over the ring GR(m,2d).

Let $\mathbf{M}\in Z_m^{l\times l}$ be a non-singular matrix such that **C** = **MA**. In this case the above two linear matrix equations are equal to just one equation:

$$\mathbf{AW} = \mathbf{Y} \text{ where } \mathbf{W} = [\mathbf{U}, \mathbf{V}] \in Z_m^{n\times 2d},\ \mathbf{Y} = [\mathbf{B}, \mathbf{M}^{-1}\mathbf{D}] \in Z_m^{l\times 2d} \qquad \text{(C.11)}$$

If the ring S=GR(m,2d) instead of GR(m,d) is used to generate the commitment to **W**:

$$\mathrm{Cmt}(\sigma|W) = \begin{bmatrix} u_1(1) & \cdots, u_d(1), v_1(1), \ldots & v_d(1) \\ \vdots & . & \vdots \\ u_1(n) & \cdots, u_d(n), v_1(n), \ldots & v_d(n) \end{bmatrix}$$

The relation (C.11) can be proved via the compressed ZKA protocol with knowledge error ≈ $p^{-2d}\log n$ (approximately squaring the knowledge-error over the ring GR(m,d)) and message complexity ≈ $2d\log n$ (same as the total message complexity of independent running two proofs over GR(m,d)).

In particular, if l = d and there exists a matrix $\mathbf{M}\in Z_m^{d\times d}$ associated with some element e in the exceptional set E of GR(m,d) = $Z_m[X]/(g(X))$ such that **C** = **MA**, then the above method is feasible since in this case **M** is always non-singular (in fact $\mathbf{M}^{-1}$ is the matrix associated with e^{-1}).

Now we present a more explicit formulism about the condition **C** = **MA** where **M** is associated with some element $e(X)$ in E. Note that **C** = **MA** in Z_m if and only if in GR(m,d):

$$\textstyle\sum_{i=1}^{d} C_{ij}X^{i-1} = \sum_{i=1}^{d}(\sum_{k=1}^{d} M_{ik}a_{kj})X^{i-1} = e(X)\sum_{j=1}^{d} a_{ij}X^{i-1} \bmod g(X).\ \ j=1,\ldots,d$$

i.e., $$(1,X,X^2,\ldots,X^{d-1})\mathbf{C}^{\mathrm{T}} = e(X)(1,X,X^2,\ldots,X^{d-1})\mathbf{A}^{\mathrm{T}} \bmod g(X) \qquad \text{(C.12)}$$

Let $(1,X,X^2,\ldots,X^{d-1})\mathbf{C}^{\mathrm{T}}=(c_1(X),\ldots,c_d(X))$ and $(1,X,X^2,\ldots,X^{d-1})\mathbf{A}^{\mathrm{T}}=(a_1(X),\ldots,a_d(X))$, the above condition is just the existence of some $e(X)$ in E such that

$$c_j(X) = e(X)a_j(X) \bmod g(X) \text{ for } j=1,\ldots,d \qquad \text{(C.13)}$$

For $m = p^s$, let $\bar{c}_j(X) = c_j(X) \bmod p$, $\bar{a}_j(X) = a_j(X) \bmod p$. Since GR($m$,$d$)/($p$) is isomorphic to E∪{0} and also isomorphic to Galois field F_{p^d} (Fact 2 in sec.2.3), $\bar{c}_j(X)$ and $\bar{a}_j(X)$ are polynomials over the field F_p. If (C.13) holds in GR(m,d) then obviously it also holds in Galois field F_{p^d}, i.e., as polynomials over F_p:

$$\overline{c}_j(X) = \bar{e}(X)\bar{a}_j(X) \text{ for all } j=1,\ldots,d \qquad \text{(C.14)}$$

On the other hand, it can be proved by Hensel's lemma (fact 4 in sec.2.3) that (C.14) implies (C.13) and $e(X)$ can be efficiently computed for properly large d.

In summary, in order to check the condition that there exists a matrix $\mathbf{M}\in Z_m^{d\times d}$ associated with some e in the exceptional set E of ring GR(m,d) such that $\mathbf{C} = \mathbf{MA}$, it is sufficient to check (C.12) modulo p.

More generally, in case that there exist $\mathbf{A}\in Z_m^{l\times n}$ and non-singular matrices $\mathbf{M}_k\in Z_m^{l\times l}$, k=1,…,q such that $\mathbf{A}_k = \mathbf{M}_k\mathbf{A}$ for each k, then k linear matrix equations

$$\wedge_{k=1}^{q} \mathbf{A}_{\boldsymbol{k}}\mathbf{U}_k = \mathbf{B}_k$$

can be equivalently proved for just one linear equation

$$\mathbf{AW} = \mathbf{Y} \text{ where } \mathbf{W} = [\mathbf{U}_1,\ldots,\mathbf{U}_q] \in Z_m^{n\times qd},\ \mathbf{Y}= [\mathbf{M}_1^{-1}\mathbf{B}_1,\ldots,\ \mathbf{M}_q^{-1}\mathbf{B}_q] \in Z_m^{l\times qd}$$

over the ring GR(m,qd) with the commitment to $\mathbf{W}$:

$$\mathrm{Cmt}(\sigma|W) = \begin{bmatrix} cmt_\sigma(u_{1,1}(1), & \cdots, u_{1,d}(1),\ldots, u_{q,1}(1),\ldots & u_{q,d}(1)) \\ \vdots & . & \vdots \\ cmt_\sigma(u_{1,1}(n), & \cdots, u_{1,d}(n),\ldots, u_{q,1}(n),\ldots & u_{q,d}(n)) \end{bmatrix}$$

The proof has knowledge error ≈ $p^{-qd}\log n$ (approximately q-th power of the knowledge-error over the ring GR(m,d)) and message complexity ≈ $qd\log n$ (same as the total message complexity of running q independent proofs over GR(m,d)). The number of G-elements for commitment is dq.

APPENDIX D: Generalized Compression via Dimension-Reduction Chain

In this section we introduce a class of mapping-sequence acting on witness space which maps high dimensional space into lower dimensional subspaces while reversible on basis of multi-images. This notion is an abstraction of constructing efficient ZKA protocols in current approach.

D.1 Dimension-Reduction Chain in Witness Space

Let $\{W_\lambda\}$ be a family of witness spaces where λ is the security parameter, $\{J_\lambda\}$ be a family of Abel groups, $\{\sum_\lambda\}$ be a family of common reference strings (c.r.s.), $\{E_\lambda\}$ be a family of random variables. For notation simplification, parameter λ is usually omitted.

F: $\sum\times W\to W\times J$ is a function which output can be efficiently computed from its input. For $X\in J$, $\boldsymbol{w}\in W$ and $\sigma\in\sum$, define the pre-image relation $R_{\sigma,F}$ with σ as the c.r.s. as:

$$F(\sigma,\boldsymbol{w}) = (\boldsymbol{w},X) \qquad \text{(D.1)}$$

And let F_σ be the function $F(\sigma,.)$: $W\to W\times J$ with σ fixed.

Definition D.1 (**Dimension-reduction chain**) Let γ >1 be a real number, μ and m be positive integers. A finite sequence of 4-tuples $\Pi_{\gamma,\mu}[W] \equiv \{[W_i,\Omega_i,\Psi_i,\Phi]: i=1, 2,\ldots,m\}$

in linear space W is called a *dimension-reduction chain* (DRC) with *reduction factor* γ, *soundness factor* μ for relation family $\{R_{\sigma,F}\}$, if there hold the following properties:

(1) $\{W_i\}$ is a decreasing sequence for subspaces, i.e., $W=W_1 \supset W_2 \supset \ldots \supset W_m$ and $\dim W \geq \gamma \dim W_1 \geq \gamma \dim W_2 \geq \ldots \geq \gamma \dim W_m$.

(2) For each i, the associated input/output algorithms for function Ψ_i: $\sum \times E \times W_i \times J \to W_{i+1} \times J$, function Φ: $\sum \times E \to \sum$ and function Ω_i: $E \times W_i \to W_{i+1}$ are all of polynomial time complexity.

For any $e \in E$, let $\Omega_{i,e}$ represent the function $\Omega_i(e,.)$:$W_i \to W_{i+1}$, $\Psi_{i,\sigma,e}$ represent the function $\Psi_i(\sigma,e,.)$: $W_i \times J \to W_{i+1} \times J$ and $f \circ g$ represent function composition.

(3) For any $\sigma \in \sum$,$e \in E$ and each I there always hold:

$$F_{\Phi(\sigma,e)} \circ \Omega_{i,e} = \Psi_{i,\sigma,e} \circ F_\sigma \tag{D.2}$$

i.e., $$F_{\Phi(\sigma,e)}(\Omega_i(e,\boldsymbol{w})) = \Psi_{i,\sigma,e}(F_\sigma(\boldsymbol{w})) \text{ for any } \boldsymbol{w} \text{ in } W_i$$

Equivalently, figure 1 is commutative.

(4) Ther exists a P.P.T algorithm Ext such that for any i and $(\boldsymbol{w}, X) \in W_i \times J$, if there are $(e_j,\boldsymbol{w}_j) \in E \times W_{i+1}$: $j = 1,\ldots, \mu$ satisfying

$$F_{\Phi(\sigma,e_j)}(\boldsymbol{w}_j) = \Psi_{i,\sigma,e_j}(\boldsymbol{w},X) \quad j = 1,\ldots,\mu \tag{D.3}$$

then Ext(σ, i, X,$\{e_j,\boldsymbol{w}_j$: $j = 1,\ldots, \mu\}$) outputs a $\boldsymbol{w}^* \in W_i$ satisfying

$$F(\sigma,\boldsymbol{w}^*) = (\boldsymbol{w}^*, X) \tag{D.4}$$

with probability $\geq 1 - \varepsilon(\lambda)$ where $\varepsilon(\lambda)$ is a negligible function in λ.

$$\begin{tikzcd}
W_i \arrow[r, "F_\sigma"] \arrow[d, "\Omega_{i,e}"'] & W_i \times J \arrow[d, "\Psi_{i,\sigma,e}"] \\
W_{i+1} \arrow[r, "F_{\Phi(\sigma,e)}"'] & W_{i+1} \times J
\end{tikzcd}$$

Fig.1 Commutative diagram of dimension-reduction chain

According to property (1) the chain $\Pi_{\gamma,\mu}[W]$'s length m always has the inequality

$$\log_\gamma(\dim W/\dim W_m) \leq m \leq \log_\gamma \dim W.$$

For a dimension-reduction chain $\Pi_{\gamma,\mu}[W]$, property (3) implies relation $R_{\sigma,F}$'s invariance under the mappings $[\Omega_i,\Psi_i]$ along the chain, i.e., if $R_{\sigma,F}$ is true in space W_i then $R_{\Phi(\sigma,e),F_{\Phi(\sigma,e)}}$ is true in its subspace W_{i+1}. This property ensures completeness in ZKA protocol's construction. Property (4) implies the reversibility of mappings $[\Omega_i,\Psi_i]$, i.e., as long as there are sufficient number of e and the associated relation instances $R_{\Phi(\sigma,e),F_{\Phi(\sigma,e)}}$ are true in subspace W_{i+1}, then a relation $R_{\sigma,F}$'s instance is true in super-space W_i and its witness can be efficiently computed from the witnesses of $\mathrm{R}_{\Phi(\sigma,\mathrm{e}),F_{\Phi(\sigma,\mathrm{e})}}$. This property ensures special-soundness for constructing ZKA protocol.

D.2 General Compressive Protocol's Construction

In proof protocol's construction, we can assign the operations specified by $\Omega_{i,e}$ (on the left side of Fig.1) to the verifier, the operations specified by $\Psi_{i,\sigma,e}$ (on the right side) to the prover and use challenges e's to relate the operations on both sides. In this view, the fact that dimension-reduction chain's properties (3) and (4) hold for every neighbor subspace pair $\mathrm{W}_i/\mathrm{W}_{i+1}$ implies that the proof can be recursively constructed along the subspace chain from $\mathrm{W}(=\mathrm{W}_1)$ to the terminal subspace W_m. Since $m \approx \log_\gamma(\dim\mathrm{W}/\dim\mathrm{W}_m)$, if the message is almost constant-size in each recursion, then the total message complexity is O(log(dimW).

Let $\pi_\mathrm{J}(.)$ be the projection to the set J. With this notation, for the function

$$\Psi_i\text{: } \sum\times\mathrm{E}\times\mathrm{W}_i\times\mathrm{J}\rightarrow\mathrm{W}_{i+1}\times\mathrm{J}\text{: } \Psi_i(\sigma,e,\boldsymbol{w}^{(i)},X^{(i)})\rightarrow(\boldsymbol{w}^{(i+1)},X^{(i+1)})$$

we have

$$X^{(i+1)} = \pi_\mathrm{J}\Psi_i(\sigma,e,\boldsymbol{w}^{(i)},X^{(i)}) \tag{D.5}$$

In order to make the above ideas practical, the chain $\Pi_{\gamma,\mu}[\mathrm{W}]$ must have some additional properties specified in the following.

Definition D.2 In a dimension-reduction chain, function Ψ_i is called *separable* if there exist efficiently computable functions Θ_i, Δ_i and Γ_i such that

$$\pi_\mathrm{J}\Psi_i(\sigma,e,\boldsymbol{w}^{(i)},X^{(i)}) = \Theta_i(\sigma,e,X^{(i)},\Delta_i) \tag{D.6}$$

$$\Delta_i = \Gamma_i(\sigma,e,\boldsymbol{w}^{(i)}) \tag{D.7}$$

Usually $X^{(i+1)}$ and $X^{(i)}$ are some derived commitments or parameters necessary for recursive computations in protocol. Separable Ψ_i makes it feasible for the verifier to compute $X^{(i+1)}$ from $X^{(i)}$ via two parts of information: one part is $[\sigma,e,X^{(i)}]$ which is public so can be directly obtained, the other part is Δ_i which depends on witness $\boldsymbol{w}^{(i)}$ so can be only obtained through the results computed by the prover via $\Gamma_i(\sigma,e,\boldsymbol{w}^{(i)})$ and then sent to the verifier.

One of the effective approach to constructing the compressed protocol from the original ∑-protocol for relation $\mathrm{R}_{\sigma,\mathrm{F}}$ (D.1) is to recursively expand its last message. Since the first message in ∑-protocol hides the witness perfectly, the expanded protocol is unnecessarily zero-knowledge. Based on the dimension-reduction chain's properties including separability (D.6) and (D.7), the basic module for proving relation $\mathrm{R}_{\sigma,\mathrm{F}}$ in space W is constructed in the following. The whole proof protocol can be obtained by combining the first two rounds in the original ∑-protocol and all the module instances here along the subspace chain.

The i-th session module of non-zero knowledge proof protocol for relation $\mathrm{R}_{\sigma,\mathrm{F}}$ $1\leq i \leq m$

P←V: V's current input is $X^{(j)} \in \mathrm{J}$, $\sigma^{(j)} \in \sum$ and $\Delta_j, 1\leq j \leq i$

(where $X^{(1)} = X$ is the commitment specified in $\mathrm{R}_{\sigma,\mathrm{F}}$, $X^{(j)}$'s and $\sigma^{(j)}$'s were computed by V and Δ_j's were received from P in last sessions)

```
    IF $i$+1 = $m$
    THEN($\Delta_m = \boldsymbol{w}^{(m)}$ is the last message received by V）
        V verifies $\mathrm{F}(\sigma^{(m)},\boldsymbol{w}^{(m)}) = (\boldsymbol{w}^{(m)}, X^{(m)})$
    ELSE
        V samples $e \overset{R}{\leftarrow} \mathrm{E}$ and send $e$ to P;
        V computes $X^{(i+1)} = \Theta_i(\sigma^{(i)},e, X^{(i)},\Delta_i)$; $\sigma^{(i+1)} = \Phi(\sigma^{(i)},e)$; $i = i+1$;
    ENDIF
P→V: P's current input is $X^{(j)} \in \mathrm{J}$, $\sigma^{(j)} \in \sum$和 $\boldsymbol{w}^{(j)} \in \mathrm{W}_{\mathrm{j}}, 1\le j \le i$ (where $\boldsymbol{w}^{(1)} = \boldsymbol{w}$ is
    The initial witness in $\mathrm{R}_{\sigma,\mathrm{F}}$).
    P receives $e$ from V;
    P computes $\sigma^{(i+1)} = \Phi(\sigma^{(i)},e)$ and $\boldsymbol{w}^{(i+1)} = \Omega_i(e,\boldsymbol{w}^{(i)})$;
    IF $i$+1 = $m$  (the last session)
    THEN   P sends $\boldsymbol{w}^{(m)}$ to V;
    ELSE
        P computes $\Delta_{i+1} = \Gamma_i(\sigma^{(i+1)},e,\boldsymbol{w}^{(i+1)})$;
        P sends $\Delta_{i+1}$ to V;
        $i = i+1$;
    ENDIF
```

Let NoZKA/$\mathrm{R}_{\sigma,\mathrm{F}}[\Pi_{\gamma,\mu}[\mathrm{W}]]$ be the protocol constructed by combining all the module instances along the subspace chain, then we have:

Theorem D.1 If all the messages are in constant-size (independent of dimensions of witness spaces), then NoZKA/$\mathrm{R}_{\sigma,\mathrm{F}}[\Pi_{\gamma,\mu}[\mathrm{W}]]$ is of $\mathrm{O}(log_\gamma \mathrm{dimW})$ message complexity, completeness and $(\mu_1,\ldots, \mu_m)$-special soundness.

Remark Combining the $(\mu_1,\ldots, \mu_m)$-special soundness and the results proved in [13], we have the conclusion that the whole proof protocol constructed via dimension-reduction chain, for instance all those in this paper, are ZKA protocols.

D.3 An Example

The concept of dimension-reduction chain covers all current compressed protocols' constructions, among which the case of linear relation's protocol is the simplest example. Here we present the construction in sec.4 as a relatively more complicated example, where:

W_λ is the vector space of witness $\boldsymbol{w} \equiv (r,s,\boldsymbol{u},\boldsymbol{v})$ over the ring S.

$\mathrm{J}_\lambda \equiv \mathrm{G}^d\times\mathrm{G}^d$ where G is a commitment-friendly group.

$\mathrm{E}_\lambda \equiv \mathrm{E}_S$, the exceptional set in ring S.

$\sigma \equiv [\mathrm{G}, \boldsymbol{g}, m]$.

Given diagonal matrix **Q** and witness $\boldsymbol{w} = (\boldsymbol{r},\boldsymbol{s},\boldsymbol{u},\boldsymbol{v})$, function $\mathrm{F}(\sigma,\boldsymbol{w})$ is defined as:

$$\mathrm{F}(\sigma, \boldsymbol{w}) \equiv (\boldsymbol{w}, \mathrm{Cmt}(\sigma_1|\boldsymbol{u}; \boldsymbol{r}), \mathrm{Cmt}(\sigma_2|\boldsymbol{v}; \boldsymbol{s}))$$

For $X = (U,V) \in \mathrm{J}_\lambda$, $\mathrm{R}_{\sigma,\mathrm{F}}$ is the relation specified in (4.25).

For $\sigma \equiv [\mathrm{G}, \boldsymbol{g}, m]$ and $\boldsymbol{g} \equiv (g_1,\ldots, g_n)$, the function Φ is defined as

$$\Phi(\sigma,e) \equiv [\mathrm{G}, \boldsymbol{g}_e, m]$$

where $\boldsymbol{g}_e$ is specified in (4.28).

For $\boldsymbol{w} = (\boldsymbol{r},\boldsymbol{s},\boldsymbol{u},\boldsymbol{v}) \in \mathrm{W}_\mathrm{i}$, $\boldsymbol{u}=\boldsymbol{u}_\mathrm{L} \dotplus \boldsymbol{u}_\mathrm{R}$, $\boldsymbol{v}=\boldsymbol{v}_\mathrm{L} \dotplus \boldsymbol{v}_\mathrm{R}$, the function Ω_i is defined as

$$\Omega_i(e,\boldsymbol{w}) \equiv \boldsymbol{u}_e \dotplus \boldsymbol{v}_e$$

where $\boldsymbol{u}_e = e\boldsymbol{u}_\mathrm{L}+e^{-1}\boldsymbol{u}_\mathrm{R}$, $\boldsymbol{v}_e = e\boldsymbol{v}_\mathrm{L}+e^{-1}\boldsymbol{v}_\mathrm{R}$.

For $\boldsymbol{w} = (\boldsymbol{r},\boldsymbol{s},\boldsymbol{u},\boldsymbol{v}) \in \mathrm{W}_\mathrm{i}$ and $X=(U,V) \in \mathrm{J}$, the function Ψ_i is defined as :

$$\Psi_i(\sigma,e,\boldsymbol{w},X) \equiv (\Omega_i(e,\boldsymbol{w}),U_e,V_e,)$$

where $U_e = A_1^{e^{-1}} U^e \; B_1^{e^3}$, $V_e = A_2^{e^{-1}} V^e \; B_2^{e^3}$(i.e., (4.33)). All the coefficients A_1, A_2, B_1, B_2 are computed according to (4.31-4.32).

According to these formulas, $\pi_\mathrm{J}\Psi_i(\sigma,e,\boldsymbol{w},X) \equiv (U_e,V_e)$ as the component of output of $\Psi_i(\sigma,e,\boldsymbol{w},X)$ only depends on public information and the coefficients A_1, A_2, ..., D_1, D_2. These coefficients are completely determined by witness $\boldsymbol{w}$ and algorithms (4.31-4.32) defines $\Gamma_i(\sigma,e,\boldsymbol{w}^{(i)})$ in definition D.2. As a result, function Ψ_i is separable.

In this dimension-reduction chain, each subspace has 1/2-dimension of its upstream neighbor, so the reduction factor $\gamma = 2$.

Property (3) for this chain, i.e., $\mathrm{F}_{\Phi(\sigma,\mathrm{e})}(\Omega_i(e,\boldsymbol{w})) = \Psi_{i,\sigma,e}(\mathrm{F}_\sigma(\boldsymbol{w}))$, can be verified straightforwardly which is just the homomorphic property of the commitment scheme. Property (4) is essentially proved in Theorem 5, i.e., the efficient algorithm Ext specified in definition 5 exists and the related soundness factor $\mu \leq 5$.

This example also shows that the dimension-reduction chain is not unique, e.g., there exists the chain with reduction factor γ=4 or any $\gamma=2^s(<m)$. Protocol's construction needs reasonable balance in selecting the appropriate chain. The higher the value of γ is, the fewer the number of rounds in the proof protocol while the higher the extractor's complexity and the value of soundness factors will be.