Efficient Zero Knowledge Arguments for Bilinear Matrix Relations over Finite Fields and Knowledge-Soundness Enhancement via Operations over Extended Field

Yuan Tian[1]

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

Abstract. In data-intensive private computing applications various relations appear as or can be reduced to matrix relations**.** In this paper we investigate two problems related to constructing the zero-knowledge argument (ZKA) protocols for matrix relations (in commit-and-prove paradigm).

In the first part, we establish the ZKA for some bilinear matrix relations over F_p. The relations in consideration include (1) general forms of bilinear relations with two witness matrices and some most important special cases. (2) some special forms of bilinear relations with three or four witness matrices. (3) eigenvalue relation. In private computing tasks various important relations are instances or special cases of these relations, e.g., matrix multiplicative relation, inverse relation, similarity relation, some structure decomposition relation and some isomorphic relations for lattices and graphs, etc. Instead of applying the general linearization approach to dealing with these non-linear relations, our approach is matrix-specific. The matrix equation is treated as a tensor identity and probabilistic-equivalent reduction techniques (amortization) are widely applied to reduce non-linear matrix relations to vector nonlinear relations. With the author's knowledge, currently there are no other systematic works on ZKA for nonlinear matrix relations. Our approach significantly outperforms the general linearization approach in all important performances, e.g., for n-by-t matrix witnesses the required size of c.r.s (only used as the public-key for commitment) can be compressed by $2nt$ times and the number of rounds, group and field elements in messages are all decreased by ~1/2 for large-size matrix.

In the second part, we enhance knowledge-soundness of ZKA for the linear matrix relation over the ground field F_p. By treating the matrix in $F_p^{n\times td}$ as a nt-dimensional vector over the d-th extended field over F_p and applying appropriate reductions, we decrease the knowledge-error of the original ZKA over F_p from $O(1/p)$ down to $O(1/p^d)$. This is comparable to the general parallel repetition approach which improves knowledge-error to the same degree, but our approach (matrix-specific) at the same time significantly improves other performances, e.g., smaller-sized c.r.s., fewer rounds and shorter messages.

Keywords: Zero-Knowledge, Matrix Equations, ∑-Protocols, Knowledge-error

1 Introduction

1.1 Motivations and Related Works

Efficient zero-knowledge proofs for various relations are crucial techniques to support multiparty private computing tasks[1-5]. 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 protocols (ZKP) with low message complexity are highly valuable to support these applications in complicated network environment or transformation into non-interactive schemes.

Recently, some innovative techniques have been developed in [6][7] to construct highly efficient ZKPs 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 ZKPs have message complexity of only O(log$n$) were n is the dimension of witness space, significantly improving previous works in performance. This approach was further developed in [8] to construct ZKP for 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 ZKPs with logarithmic message complexity for bilinear relations on groups with pairing structure[9][10] and partial-knowledge proof protocols[11].

After succeeding in developing efficient ZKPs for linear vector relations over finite field, it is natural to establish efficient ZKPs for nonlinear relations over finite field and other arithmetic systems, e.g., finite rings Z_M or integer ring Z. In this direction, bilinear relation is the simplest non-linear relation which efficient ZKP 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 rank-1 coefficient matrix. So far with the author's knowledge there are no direct and systematic works on non-linear vector or matrix relations. In addition, although any (linear or non-linear) matrix relation can be dealt with by simply treating the matrix as a vector, some more direct, matrix-oriented approach may be still necessary to significantly improve the performance relative to the general approach. For non-linear relations, currently 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 nonlinear relation is still valuable in theory and applications. [9][10][11] are heuristic examples in this direction.

In many situations, parallel repetition is a simple and effective way to enhance the interactive proof/argument protocols' knowledge-soundness. Recently [21] proved that t-fold parallel repetition of any special-sound multi-round public-coin interactive proof/argument indeed (and optimally) reduces the knowledge-error from κ down to κ^t. This elegant result is general, particularly valuable for those public-coin protocols operating over relatively small challenge spaces. However, in some special situations

is there any simpler way to (flexibly and significantly) decrease the knowledge-error just in a single protocol invocation? Another motivation to investigate this problem is due to the fact recently proved in [22]: when applying Fiat-Shamir transform to t-fold parallel repetition of a $(k_1,\ldots,k_\mu)$-special-sound interactive proof/argument to get the non-interactive scheme, there exists an attack resulting a security loss $\sim Q^{\mu}/\mu^{\mu+t}$ in knowledge-error (Q is the number of oracle-queries by the attacker) , while the transform of one-invocation of the protocol only suffers a loss linearly in Q. Therefore, the method to significantly decrease knowledge-error other than by parallel-repetition will be helpful for constructing efficient non-interactive proof/argument schemes in practice. In the second part of this work we present a positive and efficient solution to this question for linear matrix relations over F_p.

1.2 Contributions

In the first part of this paper, we establish the zero-knowledge argument (ZKA) protocols for a family of bilinear matrix relations over $F_{p.}$ The investigated matrix relations include:

(1) General forms of bilinear relations with two witness matrices and some most important special cases:

$$\mathbf{U}^{\mathrm{T}}\mathbf{QV} + \mathbf{V}^{\mathrm{T}}\mathbf{RU} + \mathbf{AUB} + \mathbf{CVD} = \mathbf{S},\ \mathbf{UQV} + \mathbf{VRU} + \mathbf{AUB} + \mathbf{CVD} = \mathbf{S}$$

where **U** and **V** are witnesses (sec.3.1~3.4).

(2) Some special forms of bilinear relations with three or four witness matrices:

$$\mathbf{U}^{\mathrm{T}}\mathbf{QW} = \mathbf{W}^{\mathrm{T}}\mathbf{RV}+\mathbf{S},\ \mathbf{UQW} = \mathbf{WRV}+\mathbf{S},\ \mathbf{U}_1{}^{\mathrm{T}}\mathbf{QU}_2 = \mathbf{V}_1{}^{\mathrm{T}}\mathbf{RV}_2 + \mathbf{S}$$

where $\mathbf{U},\mathbf{V},\mathbf{W}$ or $\mathbf{U}_1,\mathbf{U}_2,\mathbf{V}_1,\mathbf{V}_2$ are witnesses (sec. 3.5~3.6).

(3) Eigenvalue relation $\mathbf{U}\boldsymbol{x} = \lambda\boldsymbol{x}$ where **U** and $\boldsymbol{x}$ are witnesses (sec.3.7).

In private computing tasks various important relations are instances or special cases of these matrix relations, e.g., the isomorphic relation between two lattices is a special case of relation $\mathbf{U}^{\mathrm{T}}\mathbf{QV} = \mathbf{S}$ (sec.3.1) with $\mathbf{U} = \mathbf{V}$ while **Q** and **S** being the Graham matrices of the lattices; the multiplicative and inverse relations of matrices **U** and **V** are special cases of $\mathbf{UQV} = \mathbf{S}$(sec.3.2) when $\mathbf{Q} = \mathrm{I}_n$ and $\mathbf{Q} = \mathbf{S} = \mathrm{I}_n$ respectively; the similarity relation between matrices **U** and **V** is a special case of $\mathbf{UQW} = \mathbf{WRV}+\mathbf{S}$ (sec.3.5) when $\mathbf{S} = \mathbf{O}$ and $\mathbf{Q} = \mathbf{R} = \mathrm{I}_n$. The relation with four witness matrices discussed in sec.3.6 is useful for proving some matrix decomposition with special structural features, e.g., diagonalization, upper/lower triangular decomposition, etc. where all factor matrices are in privacy.

Instead of applying the general linearization approach to dealing with nonlinear relations, our approach is matrix-specific. In our approach a nonlinear matrix equation is regarded as a tensor identity and probabilistic-equivalence reduction techniques (amortization) are widely applied to reduce these relations to a simple vector bilinear relation $\boldsymbol{u}^{\mathrm{T}}\mathbf{D}\boldsymbol{v} = y$ in a space of higher dimension where $\boldsymbol{u}$, $\boldsymbol{v}$ are vector witnesses, **D**, y are public and **D** is diagonal. On basis of the ZKA protocol for this vector bilinear relation, all the investigated matrix relations can be completely established.

With the author's knowledge, currently there is no other direct and systematic works on ZKA for nonlinear matrix relations. Compared with the general linearization approach, important performances of these ZKA protocols for matrix bilinear relations constructed in our approach are significantly improved, as indicated by table 2

and 3. For example, for n-by-t matrix witnesses the required size of c.r.s (only used as the public-key for commitment) can be compressed by $2nt$ times; when $n >> t$ or $t>>n$, the number of rounds, group and field elements in messages are all decreased by ~ 1/2; when $n \sim t >> 1$ (e.g., square witnesses) these are also decreased by ~1/2. In summary, our approach significantly outperforms the general linearization approach in all aspects, a result of making use of specific features of matrix algebra.

In the second part of this work (sec.5), by extending the tensorization technique used in sec.3 we present a simple method to flexibly and significantly decrease the knowledge-error of the ZKA for matrix relation over F_p just in a single protocol invocation. As the most fundamental relation, we investigate the linear matrix relation over F_p with matrix witness in $F_p^{N\times td}$(d determined by the target knowledge-error). Compared with the general parallel repetition approach, (with the same knowledge-error ~ $1/p^d$) our approach outperforms it with the number of rounds decreased by $2logd$, total number of F_p elements decreased by $dlogd$ and G elements decreased by $2dlogd$. Also the size of c.r.s in our approach is reduced by d times. Although specific to linear matrix relation, this positive result is interesting and it is worthwhile to investigate non-linear matrix relations in the same direction in future works.

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.

$u \xleftarrow{R} J$ 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, $\langle P(w);\underline{V}\rangle_\sigma(x)$ represents the output of V valued in {0,1} after the interaction with P on input x and c.r.s. σ, $Tr\langle P,V\rangle_\sigma(x)$ 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

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

where $\mu(x) \equiv P[<P^*;\underline{V}>_\sigma(x)=1] \geq \kappa(|x|)$.
(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 $\mathrm{Tr}<P,V^*>_\sigma(x)$ 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 $\mathrm{Tr}<P^*,V>_\sigma(x)$ 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 (**$\sum$-Protocol and generalized $\sum$-Protocol**) An interactive proof system (P,V) for relation R is called a $\sum$-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* $\sum$-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 $\sum$-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 $\mathrm{Tr}<P,V^*>_\sigma(x)$ and the output of S on input $(\sigma,x;e_1,\ldots,e_k)$ have the same distribution for any $x\in L_R$ and independent random coins $e_1,\ldots,e_k$.

Definition 3 (**$(\mu_1,\ldots,\mu_k)$-special soundness and session-tree for a generalized $\sum$-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 $\sum$-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

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

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

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

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

2.3 Discrete Logarithm Hardness and Pedersen Commitment Scheme

This paper deals with zero-knowledge arguments for linear algebraic relations over finite fields on basis of discrete logarithm problem(DLP)'s hardness. More exactly, all our ZKAoK protocols are established on the ensemble of groups $\{G_\lambda\}$ where each G_λ is a cyclic group of prime order and there exists a negligible function $\varepsilon(\lambda)$ s.t. for any P.P.T. algorithm A there holds

$$P[g,h \overset{R}{\leftarrow} G_\lambda; u \leftarrow A(g,h): h = g^u] \leq \varepsilon(\lambda)$$

For n-dimensional vector $\boldsymbol{u} \equiv (u_1,\ldots, u_n)$ over finite field F_p and n-tuple $\boldsymbol{g} \equiv (g_1,\ldots, g_n)$ over group G, we frequently denote the expression $g_1^{u_1} \ldots g_n^{u_n}$ as $\boldsymbol{g}[\boldsymbol{u}]$; for scalar e in F_p, we denote $g_1^e \ldots g_n^e$ *as* $\boldsymbol{g}[e]$. With this notation, DLP hardness is equivalent to the following hardness statement where 1 is the unit element in group G, A is any P.P.T. algorithm and $<G_\lambda>$ is the information encoded for the operations on G_λ:

$$P[\boldsymbol{g} \overset{R}{\leftarrow} G_\lambda; \boldsymbol{u} \leftarrow A(<G_\lambda>, \boldsymbol{g}): \boldsymbol{g}[\boldsymbol{u}] = 1 \text{ and } \boldsymbol{u} \neq \boldsymbol{0} \bmod |G_\lambda|] \leq \varepsilon(\lambda)$$

Frequently we say "group G with DLP-hardness property" instead of the above exact but long statement. Under this statement, Pedersen commitment scheme [19] has all properties specified in definition 4. In Pedersen scheme, CGen(λ) outputs $pk = (h,\boldsymbol{g})$ and Cmt(pk,(r,$\boldsymbol{u}$)) outputs (c,d) where $c = h^r\boldsymbol{g}[\boldsymbol{u}]$ and $d = (r,\boldsymbol{u})$.

Besides the security properties, the algebraic homeomorphism properties of Pedersen scheme are also fundamental to all our ZKAoK protocol constructions.

Generalization to Matrix Commitment Pedersen scheme can be straightforwardly generalized to committing to the matrix. Formally, let:

CGen(λ) outputs the public-key $pk = (h,\boldsymbol{g})$ as a system of randomly independent elements in G where:

$$\boldsymbol{g} = [g_{ij}: i=1,\ldots,n, j=1,\ldots,t]$$

Cmt($pk|\mathbf{U},r$) outputs (c,d) on input of the matrix $\mathbf{U} = [\boldsymbol{u}_1,\ldots,\mathbf{u}_t] \in F_p^{n\times t}$ and randomness r where:

$$c = h^r \prod_{i=1}^{n} \prod_{j=1}^{n} g_{ij}^{U_{ij}},\ d = (\mathbf{U},r) \tag{2.1}$$

Cmt($pk|c,\mathbf{U},d$) outputs 1 if the equality (2.1) holds for (pk, c, $\mathbf{U}$, d).

Note that there is a bijective correspondence between a matrix $\mathbf{U} = [\boldsymbol{u}_1,\ldots,\mathbf{u}_t] \in F_p^{n\times t}$ and a column vector

$$\boldsymbol{u}^* = \begin{bmatrix} \boldsymbol{u}_1 \\ \vdots \\ \boldsymbol{u}_t \end{bmatrix} \in F_p^{nt} \tag{2.2}$$

i.e., $u_k^* = U_{ij}$ with the bijective correspondence between each $\{1,\ldots,nt\} \ni k = i\text{-}1+(j\text{-}1)n$ and (i,j): $i = 1,\ldots,n$, $j=1,\ldots,t$. On basis of this fact and the correspondence $g_k^* = g_{ij}$, we have :

$$\text{Cmt}(pk|\mathbf{U},r) = \text{Cmt}(pk^*|(\boldsymbol{u}^*,r) \tag{2.3}$$

It's easy to prove that generalized commitment scheme is perfect-hiding and computational-binding. Properties (2.1)~(2.3) will be widely used in subsequent derivations. Both notations Cmt($pk|\mathbf{U},r$) and Cmt($pk^*|(\boldsymbol{u}^*,r$) will be used inter-changeably.

2.4 Probabilistic Equivalence Reduction

Two relations $R(\alpha|x;u)$ and $S(\beta|y;v)$ are called probabilistically equivalent to each other if there exists negligible functions $\varepsilon_1(\lambda)$ and $\varepsilon_2(\lambda)$ such that

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

This equivalence is denoted by $R(\alpha|x;u) \overset{P}{\leftrightarrow} S(\beta|y;v)$. In sections 3 and 5 probabilistic equivalence reductions are widely used where frequently 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., $P[S(\beta|y;v)|\ R(\alpha|x;u)]=1$, while on the other direction it is probabilistic: $P[R(\alpha|x;u) \mid S(\beta|y_\rho;v_\rho)] \geq 1\text{-}\ \varepsilon_1(\lambda)$ where ρ is the 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 by $R \overset{P/m}{\longleftrightarrow} S$.

Some detailed analysis and useful examples of probabilistic reduction in zero-knowledge proofs can be seen in [12].

3 Equivalence Reductions for Bilinear Matrix Relations

In this section we reduce a family of bilinear matrix relations over F_p to the bilinear vector relation $\boldsymbol{u}^{\mathrm{T}}\mathbf{D}\boldsymbol{v} = y$ where $\boldsymbol{u}$, $\boldsymbol{v}$ are vector witnesses, $\mathbf{D}$ and y are public and $\mathbf{D}$ is diagonal. Many frequently appeared important relations in private computations are instances or special cases of these matrix relations, e.g., the isomorphic relation between two lattices is a special case of relation $\mathbf{U}^{\mathrm{T}}\mathbf{Q}\mathbf{V} = \mathbf{Y}$ (sec.3.1) with $\mathbf{U} = \mathbf{V}$ while $\mathbf{Q}$ and $\mathbf{Y}$ being the Graham matrices of the lattices; the multiplicative and inverse relations of matrices $\mathbf{U}$ and $\mathbf{V}$ are special cases of $\mathbf{UQV} = \mathbf{Y}$(sec.3.2) when $\mathbf{Q} = \mathrm{I}_n$ and $\mathbf{Q} = \mathbf{Y} = \mathrm{I}_n$ respectively; the similarity relation between matrices $\mathbf{U}$ and $\mathbf{V}$ is a special case of $\mathbf{UQW} = \mathbf{WRV+S}$ (sec.3.5) when $\mathbf{S} = \mathbf{O}$ and $\mathbf{Q} = \mathbf{R} = \mathrm{I}_n$.

We work in the commit-and-prove paradigm that all commitments to witnesses are published prior to running any protocols. Since the commitments are independent of specific parameter values used by any protocol instance, they can be reused in different protocol invocation when necessary.

3.1 Equivalence Reduction for $\mathbf{U}^{\mathrm{T}}\mathbf{QV} = \mathbf{Y}$

Consider the bilinear matrix relation:

$$\mathbf{U}^{\mathrm{T}}\mathbf{Q}\mathbf{V} = \mathbf{Y} \tag{3.1}$$

where $\mathbf{U},\mathbf{V} \in F_p^{n\times t}$, $\mathbf{Q} \in F_p^{n\times n}$, $\mathbf{Y} \in F_p^{t\times t}$, n and t are any integer. $\mathbf{U}$ and $\mathbf{V}$ are witnesses while $\mathbf{Q}$ and $\mathbf{Y}$ are public.

For simplicity, $\mathbf{Q}$ is assumed diagonal in this and next section. However, this assumption is not essential. Non-diagonal case will be dealt with in sec. 3.3.

Note that for $t = 1$, (3.1) is just a bilinear vector relation over F_p. For $t = 2$, i.e., $F_p^{n\times 2}$ $\exists \mathbf{U} \equiv [\boldsymbol{u}_1,\boldsymbol{u}_2]$ and $\mathbf{V} \equiv [\boldsymbol{v}_1,\boldsymbol{v}_2]$ with $\boldsymbol{u}_i,\boldsymbol{v}_i \in F_p^n$, (3.1) has the form:

$$\begin{bmatrix}\boldsymbol{u}_1^{\mathrm{T}}\\ \boldsymbol{u}_1^{\mathrm{T}}\end{bmatrix}\mathbf{Q}[\mathbf{v}_1,\mathbf{v}_2] = \begin{bmatrix}y_{11} & y_{12}\\ y_{21} & y_{22}\end{bmatrix} \tag{3.2}$$

or equivalently $\wedge_{i,j=1}^{2}\, \boldsymbol{u}_i^{\mathrm{T}}\mathbf{Q}\boldsymbol{v}_j = y_{i,j}$. Given any $\rho \xleftarrow{R} F_p$ randomly sampled by the verifier, this relation is equivalent with probability $> 1-3/p$ to the following bilinear equation:

$$(\boldsymbol{u}_1+\rho\boldsymbol{u}_2)^{\mathrm{T}}\mathbf{Q}(\boldsymbol{v}_1+\rho^2\boldsymbol{v}_2) = y_{11}+\rho y_{21}+\rho^2 y_{12}+\rho^3 y_{22} \equiv y_\rho$$

which is furthermore equivalent to:

$$[\boldsymbol{u}_1^{\mathrm{T}}, \boldsymbol{u}_2^{\mathrm{T}}]\begin{bmatrix}\mathbf{Q} & \rho^2\mathbf{Q}\\ \rho\mathbf{Q} & \rho^3\mathbf{Q}\end{bmatrix}\begin{bmatrix}\boldsymbol{v}_1\\ \boldsymbol{v}_2\end{bmatrix} = y_\rho \tag{3.3}$$

Let $\boldsymbol{u}^*,\boldsymbol{v}^* \in F_p^{2n}$ and $\mathbf{Q}_\rho{}^* \in F_p{}^{2n\times 2n}$ be the vectors and matrix in (3.3), i.e.:

$$\boldsymbol{u}^* \equiv \begin{bmatrix}\boldsymbol{u}_1\\ \boldsymbol{u}_2\end{bmatrix} = \begin{bmatrix}\boldsymbol{u}_1(1)\\ \vdots\\ \boldsymbol{u}_1(n)\\ \boldsymbol{u}_2(1)\\ \vdots\\ \boldsymbol{u}_2(n)\end{bmatrix},\ \boldsymbol{v}^* \equiv \begin{bmatrix}\boldsymbol{v}_1\\ \boldsymbol{v}_2\end{bmatrix} = \begin{bmatrix}\boldsymbol{v}_1(1)\\ \vdots\\ \boldsymbol{v}_1(n)\\ \boldsymbol{v_2}(1)\\ \vdots\\ \boldsymbol{v}_2(n)\end{bmatrix},\ \mathbf{Q}_\rho{}^* \equiv \begin{bmatrix}\mathbf{Q} & \rho^2\mathbf{Q}\\ \rho\mathbf{Q} & \rho^3\mathbf{Q}\end{bmatrix}$$

As a result, the bilinear matrix relation (3.1) is reduced to a bilinear vector relation (3.3).

For any $t>1$, i.e., $F_p^{n\times t} \ni \mathbf{U} \equiv [\boldsymbol{u}_1,\ldots,\boldsymbol{u}_t]$ and $\boldsymbol{v} \equiv [\boldsymbol{v}_1,\ldots,\boldsymbol{v}_t]$ with $\boldsymbol{u_i}, \boldsymbol{v_i} \in F_p^n$, applying the above approach (probabilistic-equivalently) reduces (3.1) to:

$$\boldsymbol{u}^{*\mathrm{T}}\mathbf{Q}_\rho{}^*\boldsymbol{v}^* = y_\rho \tag{3.4}$$

where $\boldsymbol{u}^*, \boldsymbol{v}^* \in F_p^{tn}, \mathbf{Q}_\rho{}^* \in F_p^{tn\times tn}$:

$$\boldsymbol{u}^* \equiv \begin{bmatrix}\boldsymbol{u}_1\\ \vdots\\ \boldsymbol{u}_t\end{bmatrix} = \begin{bmatrix}\boldsymbol{u}_1(1)\\ \vdots\\ \boldsymbol{u}_1(n)\\ \vdots\\ \boldsymbol{u}_t(1)\\ \vdots\\ \boldsymbol{u}_t(n)\end{bmatrix},\ \boldsymbol{v}^* \equiv \begin{bmatrix}\boldsymbol{v}_1\\ \vdots\\ \boldsymbol{v}_t\end{bmatrix} = \begin{bmatrix}\boldsymbol{v}_1(1)\\ \vdots\\ \boldsymbol{v}_1(n)\\ \vdots\\ \boldsymbol{v}_t(1)\\ \vdots\\ \boldsymbol{v}_t(n)\end{bmatrix},\ \mathbf{Q}_\rho{}^* \equiv \begin{bmatrix}\mathbf{Q} & \rho^{\boldsymbol{t}}\mathbf{Q} & \ldots & \rho^{(\boldsymbol{t-1})\boldsymbol{t}}\mathbf{Q}\\ \rho\mathbf{Q} & \rho^{\boldsymbol{t+1}}\mathbf{Q} & \ldots & \rho^{(\boldsymbol{t-1})\boldsymbol{t+1}}\mathbf{Q}\\ \vdots & \vdots & & \vdots\\ \rho^{\boldsymbol{t-1}}\mathbf{Q} & \rho^{\boldsymbol{2t-1}}\mathbf{Q} & \ldots & \rho^{\boldsymbol{t^2-1}}\mathbf{Q}\end{bmatrix} \tag{3.5}$$

The above reductions also indicate that committing to vectors $\boldsymbol{u}^*, \boldsymbol{v}^*$ is a reasonable way to commit to the matrix witnesses **U** and **V**, so the generalized scheme for matrix specified in sec.2.4 is used here and hereafter. Formally, we set the c.r.s $\sigma \equiv [G, \boldsymbol{g}, \boldsymbol{h}, h, p]$ with $\boldsymbol{g} \equiv (g_{1,1},\ldots, g_{t,n})$ and $\boldsymbol{h} \equiv (h_{1,1},\ldots, h_{t,n})$, compute the commitment W to witnesses $(\mathbf{U},\mathbf{V})$ as:

$$W = \mathrm{Cmt}(\sigma|\mathbf{U},\mathbf{V};r) \equiv \mathrm{Cmt}(\sigma|\boldsymbol{u}^*,\boldsymbol{v}^*;r)$$
$$\equiv h^r g_{1,1}[u_1(1)]\ldots g_{t,n}[u_t(n)]h_{1,1}[v_1(1)]\ldots h_{t,n}[v_t(n)] \tag{3.6}$$

In order to construct the efficient ZKA protocol for (3.4), $\mathbf{Q}_\rho{}^*$'s diagonality is important. However, in general $\mathbf{Q}_\rho{}^*$ is not diagonal even **Q** is. This issue can be handled in the following way with the observation that it is actually a tensor product:

$$\mathbf{Q}_\rho{}^* = \boldsymbol{\Delta}(\rho)\hat{\otimes}\mathbf{Q} \tag{3.7}$$

where:

$$\boldsymbol{\Delta}(\rho) \equiv [\boldsymbol{\rho}(t), \rho^t\boldsymbol{\rho}(t), \rho^{2t}\boldsymbol{\rho}(t),\ldots, \rho^{t(t-1)}\boldsymbol{\rho}(t)] \in F_p^{t\times t},\ \boldsymbol{\rho}(t)^{\mathrm{T}} \equiv [1, \rho, \rho^2,\ldots, \rho^{t-1}] \in \mathrm{F}_p^t$$

According to the general theory on quadratic forms over arbitrary fields[20], there exist non-singular matrices $\boldsymbol{\Phi}_\rho, \boldsymbol{\Psi}_\rho \in F_p^{t\times t}$ and a diagonal matrix $\mathbf{D}_\rho$ all of which can be efficiently computed such that (called *Smith* form):

$$\boldsymbol{\Delta}(\rho) = \boldsymbol{\Phi}_\rho{}^{\mathrm{T}}\mathbf{D}_\rho\boldsymbol{\Psi}_\rho \tag{3.8}$$

Combining (3.8)~(3.9) and the well-known tensor identity $(\mathbf{AB})\hat{\otimes}(\mathbf{CD}) = (\mathbf{A}\hat{\otimes}\mathbf{C})(\mathbf{B}\hat{\otimes}\mathbf{D})$, one can obtain the diagonal decomposition of $\mathbf{Q}_\rho{}^*$ as:

$$\mathbf{Q}_\rho^* = (\mathbf{\Phi}_\rho \hat{\otimes} \mathbf{I}_n)^{\mathrm{T}} (\mathbf{D}_\rho \hat{\otimes} \mathbf{Q})(\mathbf{\Psi}_\rho \hat{\otimes} \mathbf{I}_n) \tag{3.9}$$

In summary, not only can $\mathbf{Q}_\rho^*$ be diagonalized but also its diagonalization complexity only depends on that of diagonalizing a relatively small matrix $\mathbf{\Delta}(\rho)$. Note that $\mathbf{\Delta}(\rho)$ is of rank 1 so its Smith form has only one non-zero entry and its diagonalization can be even pre-computed off-line by the verifier.

Now we use simplified notations to represent (3.9) as:

$$\mathbf{Q}_\rho^* = \mathbf{\Phi}^{\mathrm{T}} \mathbf{D}_\mathbf{Q} \mathbf{\Psi} \tag{3.10}$$

where $\mathbf{D}_\mathbf{Q} \in F_p^{nt \times nt}$ is diagonal. Let the new witnesses $\bar{\boldsymbol{u}}$ and $\bar{\boldsymbol{v}}$ be:

$$\bar{\boldsymbol{u}} = \mathbf{\Phi} \boldsymbol{u}^*, \bar{\boldsymbol{v}} = \mathbf{\Psi} \boldsymbol{v}^* \tag{3.11}$$

Simple calculations demonstrate:

$$\boldsymbol{u}^{*\mathrm{T}} \mathbf{Q}_\rho^* \boldsymbol{v}^* = \bar{\boldsymbol{u}}^{\mathrm{T}} \mathbf{D}_\mathbf{Q} \bar{\boldsymbol{v}} \tag{3.12}$$

$$\bar{\boldsymbol{g}}[\bar{\boldsymbol{u}}] = \boldsymbol{g}[\boldsymbol{u}^*], \bar{\boldsymbol{h}}[\bar{\boldsymbol{v}}] = \boldsymbol{h}[\boldsymbol{v}^*] \tag{3.13}$$

where: $$\bar{g}_\mu = \prod_{\nu=1}^{nt} g_\nu^{\Phi^{-1}(\mu,\nu)}, \ \bar{h}_\mu = \prod_{\nu=1}^{nt} h_\nu^{\Psi^{-1}(\mu,\nu)} \tag{3.14}$$

$\mu, \nu = 1,\ldots,nt$, each $\mu = i - 1 + (j-1)n$ one-to-one corresponds to (i,j): $i = 1,\ldots,n$, $j = 1,\ldots,t$ and similarly for ν. Note that if DLP is hard for $(\boldsymbol{g},\boldsymbol{h},h)$ so is it for $(\bar{\boldsymbol{g}},\bar{\boldsymbol{h}},h)$, which means both of them are valid public-keys for the commitment scheme (or c.r.s.). Therefore the bilinear relation (3.4) with witnesses $\boldsymbol{u}^*$ and $\boldsymbol{v}^*$ is probabilistic-equivalently reduced to a relation with witnesses $\bar{\boldsymbol{u}}$, $\bar{\boldsymbol{v}}$ and diagonal coefficient matrix $\mathbf{D}_\mathbf{Q}$:

$$\bar{\boldsymbol{u}}^{\mathrm{T}} \mathbf{D}_\mathbf{Q} \bar{\boldsymbol{v}} = y_\rho \tag{3.15}$$

As a result, the bilinear matrix relation (3.1) is equivalently reduced with probability > 1- nt/p to a bilinear vector relation in space F_p^{nt}. More formally:

Theorem 1 Define the bilinear matrix relation over F_p as (variables in the frame are witnesses):

$$\mathbf{MBLR}^{\mathrm{I}}(\sigma|W,\mathbf{Y},\mathbf{Q};\boxed{r,\mathbf{U},\mathbf{V}}): W = \mathrm{Cmt}(\sigma|\mathbf{U},\mathbf{V};r) \wedge \mathbf{U}^{\mathrm{T}}\mathbf{Q}\mathbf{V} = \mathbf{Y} \tag{3.16}$$

where Cmt is the Pedersen commitment scheme with public-key $\sigma \equiv [G, \boldsymbol{g}, \boldsymbol{h}, h, p]$ (also used as c.r.s.), $F_p^{n\times t} \ni \mathbf{U} \equiv [\boldsymbol{u}_1,\ldots,\boldsymbol{u}_t]$ and $\mathbf{V} \equiv [\boldsymbol{v}_1,\ldots,\boldsymbol{v}_t]$ with $\boldsymbol{u}_i, \boldsymbol{v}_i \in F_p^n$, $\mathbf{Q} \in F_p^{n\times n}$ is diagonal, $\mathbf{Y} \in F_p^{t\times t}$, then $\mathbf{MBLR}^{\mathrm{I}}$ is probabilistic-equivalent to the following relation with soundness factor nt:

$$\mathbf{VBLR}^{\mathrm{I}}(\bar{\sigma}|\bar{W}, y_\rho, \mathbf{D}_\mathbf{Q};\boxed{r, \bar{\boldsymbol{u}}, \bar{\boldsymbol{v}}}): \ \bar{W} = \mathrm{Cmt}(\bar{\boldsymbol{\sigma}}|\bar{\boldsymbol{u}},\bar{\boldsymbol{v}};\ r) \wedge \bar{\boldsymbol{u}}^{\mathrm{T}}\mathbf{D}_\mathbf{Q}\bar{\boldsymbol{v}} = y_\rho \tag{3.17}$$

where ρ is a randomness sampled by the verifier, $\bar{\boldsymbol{u}}, \bar{\boldsymbol{v}} \in \mathrm{F}_p^{\ tn}$, $y_\rho \equiv \sum_{i,j=1}^{t} y_{i,j}\, \rho^{i-1+(j-1)t}$, diagonal $\mathbf{D}_\mathbf{Q} = \mathbf{D}_\rho \hat{\otimes} \mathbf{Q}$ is specified in (3.10), $\bar{\sigma} \equiv [G, \bar{\boldsymbol{g}}, \bar{\boldsymbol{h}}, h, p]$ with $\bar{\boldsymbol{g}}$ and $\bar{\boldsymbol{h}}$ computed via (3.14), $W = \bar{W}$. The witnesses of $\mathrm{MBLR}^{\mathrm{I}}$ and $\mathrm{VBLR}^{\mathrm{I}}$ are computationally related via (3.11) and (3.5).

3.2 Equivalence Reduction for UQV = Y

Consider the relation with witnesses $\mathbf{U},\mathbf{V}\in F_p^{n\times n}$ and $\mathbf{Q}\in F_p^{n\times n}$ diagonal:

$$\mathbf{UQV} = \mathbf{Y} \tag{3.18}$$

which component-wise form is:

$$\sum_{k,l=1}^{n} Q_{kl}\, U_{ik} V_{lj} = y_{ij} \quad i,j = 1,\ldots,n \tag{3.19}$$

Given any random element ρ sampled in the field, by multiplying each equality on both sides with $\rho^{i-1+(j-1)n}$ and then making a summation, one has:

$$\sum_{k,i,l,j=1}^{n} \rho^{i-1+(j-1)n} Q_{kl}\, U_{ik} V_{lj} = \mathrm{Y}_\rho \tag{3.20}$$

where

$$\mathrm{Y}_\rho \equiv \sum_{i,j=1}^{n} y_{ij}\ \rho^{i-1+(j-1)n} \tag{3.21}$$

In summary, bilinear matrix relation (3.18) is equivalent with probability > $1-n^2/p$ to a bilinear vector relation:

$$\boldsymbol{u}^{*\mathrm{T}} \widetilde{\mathbf{Q}_\rho} \boldsymbol{v}^{*} = \mathrm{Y}_\rho \tag{3.22}$$

where the square $\widetilde{\mathbf{Q}}_\rho$ of order n^2 has its entries:

$$(\widetilde{\mathbf{Q}}_\rho)_{il,kj} \equiv \mathrm{Q}_{kl}\rho^{i-1+(j-1)n} \quad k,\, l,\, i,\, j = 1,\ldots,n$$

Each double index il, kj is correspondent with the single index in the way specified in (2.2). Note that

$$\widetilde{\mathbf{Q}}_\rho = \mathbf{Q}^{\mathrm{T}} \hat{\otimes} \boldsymbol{\Delta}(\rho) \tag{3.23}$$

So with the same method presented in sec.3.1 to diagonalize $\widetilde{\mathbf{Q}}_\rho$, the relation (3.22) can be furthermore reduced to a bilinear vector relation with n^2-dimensional witnesses and diagonal coefficient matrix, a result similar as that of theorem 1.

3.3 The Case of Non-diagonal Matrix Q

In matrix relations $\mathbf{U}^{\mathrm{T}}\mathbf{QV}=\mathbf{Y}$ or $\mathbf{UQV}=\mathbf{Y}$, usually a non-diagonal $\mathbf{Q}$ has some other algebraic feature such as symmetry: $\mathbf{Q}^{\mathrm{T}}=\mathbf{Q}$. According to the general theory on quadratic forms over arbitrary fields[20], there exist non-singular matrix $\mathbf{W}\in F_p^{n\times n}$ and diagonal matrix $\mathbf{D}_\mathbf{Q}$ which can be efficiently computed such that:

$$\mathbf{Q} = \mathbf{W}^{\mathrm{T}}\mathbf{D}_{\mathrm{Q}}\mathbf{W}$$

As an example, for the relation $\mathbf{U}^{\mathrm{T}}\mathbf{QV}=\mathbf{Y}$ we set the new witness matrices $\widetilde{\mathbf{U}},\widetilde{\mathbf{V}}$: $\widetilde{\mathbf{U}} = \mathbf{WU}$, $\widetilde{\mathbf{V}} = \mathbf{WV}$ and simple calculation shows that:

$$\mathbf{U}^{\mathrm{T}}\mathbf{QV} = \widetilde{\mathbf{U}}^{\mathrm{T}}\mathbf{D}_{\mathbf{Q}}\widetilde{\mathbf{V}}$$

and

$$\mathrm{Cmt}(\sigma|\mathbf{U},\mathbf{V};r) = \mathrm{Cmt}(\breve{\sigma}|\widetilde{\mathbf{U}},\widetilde{\mathbf{V}};r)$$

where the original c.r.s. $\sigma = [\mathrm{G},\boldsymbol{g},\boldsymbol{h},p]$ and the new one $\breve{\sigma} = [\mathrm{G},\widetilde{\boldsymbol{g}},\breve{\boldsymbol{h}},p]$ are related by:

$$\widetilde{\boldsymbol{g}}_{kj} = \prod_{i=1}^{n} g_{ij}^{W^{-1}(i,k)},\ \breve{\boldsymbol{h}}_{kj} = \prod_{i=1}^{n} h_{ij}^{W^{-1}(i,k)} \quad k,j=1,\ldots,n \tag{3.24}$$

Even if **Q** is non-symmetric, we can still apply the diagonalization method in sec.3.1 to diagonalize **Q** as:

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

where **W** and **M** are both non-singular. Set the new witness matrices $\widetilde{\mathbf{U}}$, $\widetilde{\mathbf{V}}$: $\widetilde{\mathbf{U}}$ = **WU**, $\widetilde{\mathbf{V}}$ = **WV**, then $\mathbf{U}^{\mathrm{T}}\mathbf{Q}\mathbf{V} = \widetilde{\mathbf{U}}\mathbf{D}_{\mathbf{Q}}\widetilde{\mathbf{V}}$ and the commitments are still unchanged. The c.r.s. $\breve{\sigma}$ is still computed by (3.24) with a slight modification that $W(i,k)$ in the expression of $\widetilde{\boldsymbol{h}}_{kj}$ is replaced by $M(i,k)$.

Since **Q** is public, the above pre-processing can be done off-line by the verifier. As a result, the relation $\mathbf{MBLR}^{\mathrm{I}}(\sigma|W,\mathbf{Y},\mathbf{Q};\ r,\mathbf{U},\mathbf{V})$ with arbitrary matrix **Q** is equivalent to the relation $\mathbf{MBLR}^{\mathrm{I}}(\breve{\sigma}|W,\mathbf{Y},\mathbf{D}_{\mathrm{Q}};\ r,\widetilde{\mathbf{U}},\widetilde{\mathbf{V}})$ with diagonal $\mathbf{D}_{\mathbf{Q}}$. This transformation keeps the dimension of witness so the message complexity is not changed.

For relation **UQV**=**Y**, the pre-processing can be done in a similar way as the above: make diagonalization **Q** = $\mathbf{W}\mathbf{D}_{\mathrm{Q}}\mathbf{M}$ and set new witnesses $\widetilde{\mathbf{U}}$=**UW**, $\widetilde{\mathbf{V}}$=**MV**. As a result $\mathbf{U}\mathbf{Q}\mathbf{V} = \widetilde{\mathbf{U}}\mathbf{D}_{\mathbf{Q}}\widetilde{\mathbf{V}}$ and $\mathrm{Cmt}(\sigma|\mathbf{U},\mathbf{V};r) = \mathrm{Cmt}(\breve{\sigma}|\widetilde{\mathbf{U}},\widetilde{\mathbf{V}};r)$ where G-elements in $\breve{\sigma}$ is computed by:

$$\widetilde{\boldsymbol{g}}_{kj} = \prod_{i=1}^{n} g_{ki}^{W^{-1}(j,i)},\ \widetilde{\boldsymbol{h}}_{kj} = \prod_{i=1}^{n} h_{ij}^{M^{-1}(i,k)} \tag{3.25}$$

3.4 Equivalence Reduction for General Bilinear Relation with Two Witnesses

Consider the general bilinear relation with two witness matrices **U**, $\mathbf{V} \in F_p^{n\times n}$:

$$\mathbf{U}^{\mathrm{T}}\mathbf{Q}\mathbf{V} + \mathbf{V}^{\mathrm{T}}\mathbf{R}\mathbf{U} + \mathbf{A}\mathbf{U}\mathbf{B} + \mathbf{C}\mathbf{V}\mathbf{D} = \mathbf{S} \tag{3.26}$$

where **Q**,**R**,**S**,**A**,**B**,**C**,**D** are public and have appropriate orders. Following the methods in sec.3.1, it can be probabilistic-equivalently reduced to a bilinear vector relation:

$$\boldsymbol{u}^{*\mathrm{T}}\mathbf{Q}_{\rho}^{*}\boldsymbol{v}^{*} + \boldsymbol{v}^{*\mathrm{T}}\mathbf{R}_{\rho}^{*}\boldsymbol{u}^{*} + \boldsymbol{m}_{\rho}\boldsymbol{u}^{*} + \boldsymbol{k}_{\rho}\boldsymbol{v}^{*} = s_{\rho}$$

where matrices $\mathbf{Q}_{\rho}^{*}$, $\mathbf{R}_{\rho}^{*}$ are computed similarly as in (3.7), $\boldsymbol{m}_{\rho} \equiv [\rho^{i\text{-}1+(j\text{-}1)n}]^{\mathrm{T}}(\mathbf{A}\hat{\otimes}\mathbf{B})_{\rho}$, $\boldsymbol{k}_{\rho} \equiv [\rho^{i\text{-}1+(j\text{-}1)n}]^{\mathrm{T}}(\mathbf{C}\hat{\otimes}\mathbf{D})_{\rho}$, $s_{\rho} \equiv \sum_{i,j=1}^{t} S_{ij}\ \rho^{i-1+(j-1)t}$. This can be also represented as :

$$[\boldsymbol{u}^{*\mathrm{T}}, \boldsymbol{v}^{*\mathrm{T}}]\begin{bmatrix}\mathbf{0} & \mathbf{Q}_{\rho}^{*}\\ \mathbf{R}_{\rho}^{*} & \mathbf{0}\end{bmatrix}\begin{bmatrix}\boldsymbol{u}^{*}\\ \boldsymbol{v}^{*}\end{bmatrix} + [\boldsymbol{m}_{\rho}{}^{\mathrm{T}}, \boldsymbol{k}_{\rho}{}^{\mathrm{T}}]\begin{bmatrix}\boldsymbol{u}^{*}\\ \boldsymbol{v}^{*}\end{bmatrix} = s_{\rho}$$

Let $\boldsymbol{w}^{*\mathrm{T}} \equiv [\boldsymbol{u}^{*\mathrm{T}}, \boldsymbol{v}^{*\mathrm{T}}] \in F_p^{2nt}$ so this equation becomes:

$$\boldsymbol{w}^{*\mathrm{T}}\boldsymbol{\Omega}_{\rho}\boldsymbol{w}^{*} + \boldsymbol{\chi}_{\rho}{}^{\mathrm{T}}\boldsymbol{w}^{*} = s_{\rho} \tag{3.27}$$

and is also equivalent to the symmetric quadratic form[1]:

$$\boldsymbol{w}^{*\mathrm{T}}(\boldsymbol{\Omega}_{\rho}+\boldsymbol{\Omega}_{\rho}{}^{\mathrm{T}})\boldsymbol{w}^{*} + 2\boldsymbol{\chi}_{\rho}{}^{\mathrm{T}}\boldsymbol{w}^{*} = 2s_{\rho} \tag{3.28}$$

With the diagonalization method similar as in sec.3.3, (3.28) is equivalent to a bilinear relation with diagonal $\mathbf{D}_{\boldsymbol{\rho}}$:

$$\overline{\boldsymbol{w}}^{\mathrm{T}}\mathbf{D}_{\rho}\overline{\boldsymbol{w}} + 2\overline{\boldsymbol{\chi}}_{\rho}{}^{\mathrm{T}}\overline{\mathbf{w}} = \mathrm{S}_{\rho} \tag{3.29}$$

---

[1] $\boldsymbol{w}^{*\mathrm{T}}\boldsymbol{\Omega}_{\rho}\boldsymbol{w}^{*} = \boldsymbol{w}^{*\mathrm{T}}\boldsymbol{\Omega}_{\rho}{}^{\mathrm{T}}\boldsymbol{w}^{*}$ and $\boldsymbol{w}^{*\mathrm{T}}\boldsymbol{\chi} = \boldsymbol{\chi}^{\mathrm{T}}\boldsymbol{w}^{*}$ so (3.27) and (3.28) implies each other.

where $\mathbf{\Omega}_\rho+\mathbf{\Omega}_\rho^{\mathrm{T}}=\mathbf{W}_{\boldsymbol{\rho}}{}^{\mathrm{T}}\mathbf{D}_{\boldsymbol{\rho}}\mathbf{W}_{\boldsymbol{\rho}}$ and $\mathbf{W}_{\boldsymbol{\rho}}$ is non-singular. Let the new witness $\overline{\boldsymbol{w}} \in F_p^{2nt}$ be:

$$\overline{\boldsymbol{w}} \equiv \mathbf{W}_{\boldsymbol{\rho}}\boldsymbol{w}^* \tag{3.30}$$

and let $\sigma \equiv [G, \boldsymbol{g}, \boldsymbol{h}, h, p]$ be the c.r.s. with $1+2nt$ G-elements used as the public-key to commit to matrices $\mathbf{U},\mathbf{V}$ (actually commit to the vector $\boldsymbol{w}^*$):

$$\mathrm{Cmt}(\sigma|\mathbf{U},\mathbf{V};r) \equiv \mathrm{Cmt}(\sigma|\boldsymbol{w}^*;r) = h^r\boldsymbol{g}[\boldsymbol{u}^*]\boldsymbol{h}[\boldsymbol{v}^*]$$

Note that

$$\mathrm{Cmt}(\overline{\sigma}|\overline{\boldsymbol{w}};r) = \mathrm{Cmt}(\sigma|\boldsymbol{w}^*;r)$$

and $\overline{\sigma} \equiv [G,\overline{\boldsymbol{g}},\overline{\boldsymbol{h}},h,p]$ can be computed from $\mathbf{M}_\rho$ and σ by (3.24).

The bilinear form with witness sqaures $\mathbf{U},\mathbf{V} \in F^{n\times n}$:

$$\mathbf{UQV} + \mathbf{VRU} + \mathbf{AUB} + \mathbf{CVD} = \mathbf{S}$$

can be reduced in a similar way as in sec.3.2 and the above.

3.5 Equivalence Reduction for Bilinear Relations with Three Witness Matrices

In this section we consider two classes of bilinear relations with three witness matrices, i.e., $\mathbf{U}^{\mathrm{T}}\mathbf{QW} = \mathbf{W}^{\mathrm{T}}\mathbf{RV}+\mathbf{S}$ and $\mathbf{UQW} = \mathbf{WRV}+\mathbf{S}$.

Reduction for the Relation $\mathbf{U}^{\mathrm{T}}\mathbf{QW} = \mathbf{W}^{\mathrm{T}}\mathbf{RV}+\mathbf{S}$

$$\mathbf{U}^{\mathrm{T}}\mathbf{QW} = \mathbf{W}^{\mathrm{T}}\mathbf{RV} + \mathbf{S} \tag{3.31}$$

In this relation the witnesses $\mathbf{U}$, $\mathbf{V}$, $\mathbf{W} \in F_p^{n\times t}$, public matrices $\mathbf{Q}$, $\mathbf{R} \in F_p^{n\times n}$, $\mathbf{S} \in F_p^{t\times t}$. Let $\mathbf{U} = [\boldsymbol{u}_1,\ldots,\boldsymbol{u}_t]$, $\mathbf{V} = [\boldsymbol{v}_1,\ldots,\boldsymbol{v}_t]$, $\mathbf{W} = [\boldsymbol{w}_1,\ldots,\boldsymbol{w}_t]$ with columns $\boldsymbol{u}_i,\boldsymbol{v}_i,\boldsymbol{w}_i \in F_p^n$ and let $\boldsymbol{u}^*$, $\boldsymbol{v}^*$, $\boldsymbol{w}^*$ be vectors corresponding to these matrices respectively (see e.g. (3.5)). (3.31) can be reduced to a bilinear relation with the $3nt$-dimensional vector witness

$$\boldsymbol{\xi}^{\mathrm{T}} \equiv [\boldsymbol{u}^{*\mathrm{T}},\boldsymbol{v}^{*\mathrm{T}},\boldsymbol{w}^{*\mathrm{T}}] \tag{3.32}$$

Indeed, on basis of the component-wise form of (3.31):

$$\textstyle\sum_{k,l=1}^{n} Q_{kl}\,U_{ki}W_{lj} = \sum_{k,l=1}^{n} R_{kl}\,W_{ki}V_{lj}+\mathrm{S}_{ij} \qquad i,j = 1,\ldots,t \tag{3.33}$$

Given any randomness ρ multiplying these equalities by $\rho^{i-1+(j-1)t}$ on both sides and then making a summation, one has:

$$\textstyle\sum_{k,i}\sum_{l,j}\rho^{i-1+(j-1)t}(Q_{kl}\,U_{ki}W_{lj} - R_{kl}W_{ki}V_{lj}) = \mathrm{S}_\rho \equiv \sum_{i,j=1}^{t} S_{ij}\;\rho^{i-1+(j-1)t} \tag{3.34}$$

The reduction from (3.31) to (3.34) has probability $> 1-nt/p$ and (3.34) also has a form:

$$[\boldsymbol{u}^{*\mathrm{T}},\boldsymbol{v}^{*\mathrm{T}},\boldsymbol{w}^{*\mathrm{T}}]\begin{bmatrix}\mathbf{0} & \mathbf{0} & \mathbf{Q}_\rho\\ \mathbf{0} & \mathbf{0} & \mathbf{0}\\ \mathbf{0} & -\mathbf{R}_\rho & \mathbf{0}\end{bmatrix}\begin{bmatrix}\boldsymbol{u}^*\\ \boldsymbol{v}^*\\ \boldsymbol{w}^*\end{bmatrix} = \mathrm{S}_\rho \tag{3.35}$$

where the squares $\mathbf{Q}_\rho$ and $\mathbf{R}_\rho$ of order nt has their entries as:

$$(\mathbf{Q}_\rho)_{ki,lj} \equiv Q_{lk}\rho^{i-1+(j-1)t},\ (\mathbf{R}_\rho)_{ki,lj} \equiv R_{lk}\rho^{i-1+(j-1)t}\quad k, l=1,\ldots,n;\ i, j=1,\ldots,t$$

Each double-index *ki*, *lj* one-to-one corresponds to the single-index as specified in (2.1). Let the coefficient matrix in (3.35) denoted by $\boldsymbol{\Omega}_\rho$, $\boldsymbol{\xi}$ be the 3*nt*-dimensional vector defined in (3.32), then the bilinear matrix equation (3.31) is probabilistic-equivalently reduced to a vector quadratic relation:

$$\boldsymbol{\xi}^{\mathrm{T}}\boldsymbol{\Omega}_\rho\boldsymbol{\xi} = S_\rho \tag{3.36}$$

This relation is furthermore equivalent to a symmetric one [2]:

$$\boldsymbol{\xi}^{\mathrm{T}}(\boldsymbol{\Omega}_\rho+\boldsymbol{\Omega}_\rho^{\mathrm{T}})\boldsymbol{\xi} = 2S_\rho \tag{3.37}$$

Let $\sigma \equiv [G, \boldsymbol{g},\boldsymbol{h},\boldsymbol{k},h,p]$ be the c.r.s with 1+3*nt* G-elements and used as the public-key to commit to the witness matrices **U**,**V**,**W**:

$$\mathrm{Cmt}(\sigma|\mathbf{U},\mathbf{V},\mathbf{W};r) \equiv \mathrm{Cmt}(\sigma|\boldsymbol{\xi};r) = h^r\boldsymbol{g}[\boldsymbol{u}^*]\boldsymbol{h}[\boldsymbol{v}^*]\boldsymbol{k}[\boldsymbol{w}^*]$$

Diagonalizaing $\boldsymbol{\Omega}_\rho+\boldsymbol{\Omega}_\rho^{\mathrm{T}}$ in the method as in sec.3.1, (3.37) is equivalently transformed to be:

$$\bar{\boldsymbol{\xi}}^{\mathrm{T}}\mathbf{D}_\rho\bar{\boldsymbol{\xi}} = S_\rho \tag{3.38}$$

where $\boldsymbol{\Omega}_\rho+\boldsymbol{\Omega}_\rho^{\mathrm{T}} = \mathbf{M}_{\boldsymbol{\rho}}^{\mathrm{T}}\mathbf{D}_{\boldsymbol{\rho}}\mathbf{M}_{\boldsymbol{\rho}}$, $\mathbf{D}_{\boldsymbol{\rho}}$ is diagonal and $\mathbf{M}_{\boldsymbol{\rho}}$ is non-singular. Set the new witness $\bar{\boldsymbol{\xi}} \in F_p^{3nt}$ to be:

$$\bar{\boldsymbol{\xi}} \equiv \mathbf{M}_{\boldsymbol{\rho}}\boldsymbol{\xi} \tag{3.39}$$

Its commitment is related with the original commitment by:

$$\mathrm{Cmt}(\bar{\sigma}|\bar{\boldsymbol{\xi}};r) = \mathrm{Cmt}(\sigma|\boldsymbol{\xi};r)$$

where the new c.r.s. $\bar{\sigma} \equiv [G,\bar{\boldsymbol{g}},\bar{\boldsymbol{h}},\bar{\boldsymbol{k}},h,p]$ is computed from $\mathbf{M}_\rho$ and σ by an algorithm similar as (3.24). Formally:

Theorem 2 Define the bilinear matrix relation over F_p as (variables in the frame are witnesses):

$$\mathbf{MBLR}^{\mathrm{II}}(\sigma|K,\mathbf{S},\mathbf{Q},\mathbf{R};\boxed{r,\mathbf{U},\mathbf{V},\mathbf{W}}):\ K=\mathrm{Cmt}(\sigma|\mathbf{U},\mathbf{V},\mathbf{W};r)\wedge\mathbf{U}^{\mathrm{T}}\mathbf{Q}\mathbf{W}=\mathbf{W}^{\mathrm{T}}\mathbf{R}\mathbf{V}+\mathbf{S} \tag{3.40}$$

where Cmt is the Pedersen commitment scheme with public-key $\sigma \equiv [G, \boldsymbol{f}, h, p]$ (also used as c.r.s.) with 1+3*nt* G-elements in $\boldsymbol{f}$, $F_p^{n\times t} \ni \mathbf{U} \equiv [\boldsymbol{u}_1,\ldots,\boldsymbol{u}_t]$, $\mathbf{V} \equiv [\boldsymbol{v}_1,\ldots,\boldsymbol{v}_t]$, $\mathbf{W} \equiv [\boldsymbol{w}_1,\ldots,\boldsymbol{w}_t]$ with columns $\boldsymbol{u}_i, \boldsymbol{v}_i, \boldsymbol{w}_i \in F_p^n$, matrix $\mathbf{Q}$, $\mathbf{R}\in F_p^{n\times n}$, $\mathbf{S}\in F_p^{t\times t}$, then $\mathbf{MBLR}^{\mathrm{II}}$ is probabilistic-equivalent to the following relation with soundness factor *nt*:

$$\mathbf{VBLR}^{\mathrm{II}}(\tilde{\sigma}|\bar{K},\ S_\rho,\ \mathbf{D}_\rho;\ \boxed{r,\ \bar{\boldsymbol{\xi}}}):\ \bar{K} = \mathrm{Cmt}(\tilde{\boldsymbol{\sigma}}|\bar{\boldsymbol{\xi}};\ r)\wedge\bar{\boldsymbol{\xi}}^{\mathrm{T}}\mathbf{D}_\rho\bar{\boldsymbol{\xi}} = S_\rho \tag{3.41}$$

where ρ is a randomness sampled by the verifier, $\bar{\boldsymbol{\xi}}\in F_p^{3tn}$, S_ρ, $\mathbf{D}_\rho$ are specified in (3.34) and (3.38) , G-elements in $\tilde{\sigma}$ are computed from σ by the algorithm in (3.24), $\bar{K} = K$ and $\bar{\boldsymbol{\xi}}$ is computationally related with (**U**,**V**,**W**) by (3.32) and (3.39).

Reduction for the Relation UQW = WRV+S

---

[2] $\boldsymbol{\xi}^{\mathrm{T}}\boldsymbol{\Omega}_\rho\boldsymbol{\xi} = \boldsymbol{\xi}^{\mathrm{T}}\boldsymbol{\Omega}_\rho^{\mathrm{T}}\boldsymbol{\xi}$ so (3.36) and (3.37) implies each other.

$$\mathbf{UQW} = \mathbf{WRV} + \mathbf{S} \tag{3.42}$$

In this relation the witnesses **U**, **V**, **W**$\in F_p^{n\times n}$ and public matrices **Q**, **R**, **S**$\in F_p^{n\times n}$. The same method as in the above can reduce this relation to

$$[\boldsymbol{u}^{*\mathrm{T}},\boldsymbol{v}^{*\mathrm{T}},\boldsymbol{w}^{*\mathrm{T}}]\begin{bmatrix}\mathbf{0} & \mathbf{0} & \mathbf{0}\\ \mathbf{0} & \mathbf{0} & -\mathbf{R}_\rho^T\\ \mathbf{Q}_\rho^T & \mathbf{0} & \mathbf{0}\end{bmatrix}\begin{bmatrix}\boldsymbol{u}^*\\ \boldsymbol{v}^*\\ \boldsymbol{w}^*\end{bmatrix} = \mathrm{S}_\rho \tag{3.43}$$

and furthermore a similar result as in Theorem 2 can be obtained.

3.6 Equivalence Reduction for $\mathbf{U_1}^{\mathrm{T}}\mathbf{QU_2} = \mathbf{V_1}^{\mathrm{T}}\mathbf{RV_2} + \mathbf{S}$

Here we consider a bilinear relation with four witness matrices, which instances and special cases can be used for proving some matrix structural decompositions with all factors in privacy:

$$\mathbf{U}_1^{\mathbf{T}}\mathbf{QU}_2 = \mathbf{V}_1^{\mathbf{T}}\mathbf{RV}_2 + \mathbf{S} \tag{3.44}$$

where $\mathbf{U}_i,\mathbf{V}_i \in F_p^{n\times t}$ are witnesses while **Q**, **R**$\in F_p^{n\times n}$ and **S**$\in F_p^{t\times t}$ are public. Given any randomness ρ in F_p, for $i,j = 1,\ldots,t$; $k, l = 1,\ldots,n$ let:

$$S_\rho \equiv \sum_{i,j=1}^{t} S_{ij}\ \rho^{i-1+(j-1)t} \in F_p$$

$$(\mathbf{Q}_\rho)_{ki,lj} \equiv \mathrm{Q}_{lk}\rho^{i\text{-}1+(j\text{-}1)t},\ (\mathbf{R}_\rho)_{ki,lj} \equiv \mathrm{R}_{lk}\rho^{i\text{-}1+(j\text{-}1)t} \tag{3.45}$$

In the same techniques as before, the relation (3.44) is equivalent with probability > 1 – *nt/p* to the relation:

$$\boldsymbol{u_1}^{*\mathrm{T}}\mathbf{Q}_\rho\boldsymbol{u_2}^* = \boldsymbol{v_1}^{*\mathrm{T}}\mathbf{R}_\rho\boldsymbol{v_2}^* + S_\rho \tag{3.46}$$

which also has the form:

$$\boldsymbol{\xi}^{\mathrm{T}}\begin{bmatrix}\mathbf{Q}_\rho & \mathbf{0}\\ \mathbf{0} & -\boldsymbol{R}_\rho\end{bmatrix}\boldsymbol{\eta} = S_\rho$$

where $\boldsymbol{\xi}^{\mathrm{T}} \equiv [\boldsymbol{u_1}^{*\mathrm{T}},\boldsymbol{v_1}^{*\mathrm{T}}]$, $\boldsymbol{\eta}^{\mathrm{T}} \equiv [\boldsymbol{u_2}^{*\mathrm{T}},\boldsymbol{v_2}^{*\mathrm{T}}]$. The relation (3.46) is a bilinear vector relation in space F_p^{2nt} with witnesses $(\boldsymbol{\xi},\boldsymbol{\eta})$ which commitment is also used as the commitment to witness matrices $(\mathbf{U}_1,\mathbf{U}_2,\mathbf{V}_1,\mathbf{V}_2)$ in relation (3.44). By diagonalization techniques this relation can be further reduced to a bilinear one with diagonal coefficient matrix.

In private computing applications, one of the important usage of relation (3.44) is to prove structural decomposition of some private matrix **A** while all factors **U**, **D**, **V** must be kept in secrecy:

$$\mathbf{A} = \mathbf{UDV} \tag{3.47}$$

When **U** and **V** are non-singular, this decomposition can be expressed as

$$\mathbf{WA} = \mathbf{DV}$$

which is a special case of (3.44). Usually **D** is some canonical form of **A** and should be proved having some structural feature, e.g., diagonal (in Smith decomposition), upper/lower triangle (in Schur decomposition), etc. This structure features may be represented via some additional equations, fro example, diagonality of D can be represented by a family of linear relations:

$$\boldsymbol{e}_{ki}^{*\mathrm{T}}\boldsymbol{d}^{*} = 0,\ k \neq i$$

where $\boldsymbol{e}_{ki}^{*}$ is the vector corresponding to the standard base matrix $\mathbf{E}_{ki}$. With probability $\geq 1-(n^2-n)/p > n^2/\mathrm{p}$ and soundness factor $n(n-1)$, these linear equations can be further reduced to a single linear equation:

$$\sum_{i,k=1,i\neq k}^{n} \rho^{i-1+(k-1)n} d_{i\text{-}1+(j\text{-}1)n} = 0$$

As a result, the diagonalization relation (3.47) can be reduced to a bilinear vector relation together with a linear relation in (3.48).

Another interesting special case of relation (3.44) is Schur decomposition, which can be reduced to a bilinear vector relation with an additional linear relation as:

$$\sum_{i,k=1,i>k}^{n} \rho^{i-1+(k-1)n} d_{i\text{-}1+(j\text{-}1)n} = 0$$

3.7 Equivalence Reduction for Eigenvalue Relation $\mathbf{U}\boldsymbol{x} = \lambda\boldsymbol{x}$

Consider the eigenvalue relation over F_p:

$$\mathbf{U}\boldsymbol{x} = \lambda\boldsymbol{x} \tag{3.48}$$

where $\mathbf{U} \in F_p^{n\times n}$ and $\boldsymbol{x} \in F_p^n$ are witnesses while λ is public (If **U** is public then the proof will be trivial since both $\boldsymbol{x}$ and λ can be efficiently computed from **U**; on the other hand if $\boldsymbol{x}$ and λ are public then this relation is just linear). Let:

$$\boldsymbol{x}^{*\mathrm{T}} \equiv [x_1,\ldots,x_1,\ldots,x_n,\ldots,x_n] \tag{3.49}$$

which is the n^2-dimensional vector corresponding to $\boldsymbol{x}$, $\boldsymbol{u}^{*}$ be the vector corresponding to matrix $\mathbf{U} = [\boldsymbol{u}_1,\ldots,\boldsymbol{u}_n]$ in the way specified in (2.2) and $\boldsymbol{b}^{*}$ the vector corresponding to matrix $\mathbf{B} \equiv \mathbf{U} - \lambda\mathbf{I}_n = [\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n]$. Note that (3.48) is equivalent to the form:

$$[x_1\mathbf{I}_n,\ldots,x_n\mathbf{I}_n]\boldsymbol{b}^{*} = \sum_{i=1}^{n} x_i\boldsymbol{b}_i = \mathbf{0}$$

Given any randomness ρ, left-multiplying the above equality with $\boldsymbol{\rho}(n)^{\mathrm{T}} \equiv [1, \rho, \rho^2,\ldots, \rho^{n-1}]$ on both sides leads to:

$$\boldsymbol{x}_{\rho}^{\mathrm{T}}\boldsymbol{b}^{*} = \mathbf{0} \tag{3.50}$$

where $\boldsymbol{x}_{\rho}^{\mathrm{T}} \equiv [x_1\boldsymbol{\rho}(n),\ldots,x_n\boldsymbol{\rho}(n)]$. (3.50) is an inner-product relation and the commitment to witness **U** and $\boldsymbol{x}$ on the public-key $\sigma \equiv [\mathrm{G}, \boldsymbol{g}, \boldsymbol{h}, h, p]$ is:

$$\mathrm{Cmt}(\sigma \mid \mathbf{U}, \boldsymbol{x}; r) \equiv \mathrm{Cmt}(\sigma \mid \boldsymbol{u}^{*}, \boldsymbol{x}^{*}; r) = h^{r}\prod_{i,j=1}^{n} g_{ij}^{x_i} \prod_{i,j=1}^{n} h_{ij}^{U_{ij}}$$

Note that:

$$\mathrm{Cmt}(\overline{\sigma}|\, \boldsymbol{b}^*, \boldsymbol{x}_\rho{}^*; r) = \mathrm{Cmt}(\sigma \,|\, \boldsymbol{u}^*, \boldsymbol{x}^*; r)(\textstyle\prod_{i=1}^{n} h_{ii}^{-1})^{\lambda}$$

where $\overline{\sigma} \equiv [\mathrm{G}, \overline{\boldsymbol{g}}, \overline{\boldsymbol{h}}, h, p]$ is computed by:

$$\overline{g_{ij}} \equiv g_{ij}^{\rho^{i-j}}, \ \overline{h_{ij}} \equiv h_{ij} \ \ i, j = 1,\ldots,n \tag{3.51}$$

In summary, the eigenvalue relation with witness matrix $\mathbf{U} \in F_p^{n\times n}$ and eigenvector $\boldsymbol{x} \in F_p^n$:

$$\mathbf{U}\boldsymbol{x} = \lambda\boldsymbol{x} \wedge W = \mathrm{Cmt}(\sigma \,|U, \boldsymbol{x}; r)$$

is probabilistic-equivalent to a bilinear relation with witness $\boldsymbol{b}^*$ and $\boldsymbol{x}_\rho{}^* \in F_p^{n^2}$:

$$\boldsymbol{x}_\rho{}^{\mathrm{T}}\, \boldsymbol{b}^* = \mathbf{0} \wedge W(\textstyle\prod_{i=1}^{n} h_{ii}^{-1})^{\lambda} = \mathrm{Cmt}(\overline{\sigma}|\, \boldsymbol{b}^*, \boldsymbol{x}_\rho{}^*; r) \tag{3.52}$$

where $\overline{\sigma}$ is computed by (3.51).

4 Complete ZKA Construction and Performances

Now we can complete the ZKA protocols construction for all the relations in sec.3 on basis of the efficient ZKA protocol for the bilinear vector relation $\boldsymbol{u}^{\mathrm{T}}\mathbf{D}\boldsymbol{v} = y$ where $\mathbf{D}$ is diagonal. It is shown in sec.3 that various bilinear matrix relations can be reduced to this relation. Table 1 presents performances of such a protocol constructed by linearization method[12].

Table 1. Performances of ZKA for $\boldsymbol{u}^{\mathrm{T}}\mathbf{D}\boldsymbol{v} = \boldsymbol{y}$: $\boldsymbol{u},\boldsymbol{v} \in F_p^k$, $\mathbf{D}$ diagonal

	Linearization Approach[12]
# G-elements in c.r.s.	$4k$+3
# G-elements in commitment	1
# Rounds	2log(3k+5)+7
Message complexity	# G: 2log(3k +5) # F_p: log(3k +5)+9

Currently there are no other works on ZKA for matrix bilinear relations over Galois fields comparable, so we make a comparison between our results and the general linearization approach which compiles any non-linear arithmetic relation (circuit) into a linear one via secret-sharing techniques (see Sec.6 in [12] for details). In the following tables, performance results of linearization approach are straightforwardly derived from the results in [12] while the performance results about our approach is from combination of the above results (table.1) on ZKA protocol for vector bilinear relation and the reduction results in sec.3 with (considering the costs in reduction) at most 2 extra F_p-elements and 1 message added.

As demonstrated in table 2 and 3, for n-by-t matrix witnesses the required size of c.r.s can be compressed by $2tn$ times. As demonstrated in table 4, when $n >> t$ or $t >> n$, the number of rounds, group and field elements in messages for our approach are all decreased by ~ 1/2; when $n \sim t >> 1$(e.g., square witnesses) these are also decreased

by ~1/2. In summary, the matrix-oriented approach significantly outperforms the general linearization approach in all aspects, a result of making use of special features of matrix algebra.

Table 2. Performances of ZKA for $\mathbf{U}^{\mathrm{T}}\mathbf{QV}=\mathbf{Y}$: $\mathbf{U}, \mathbf{V} \in F_p^{n\times t}$

	Linearization Approach[12]	Our Approach (3.17)
# G-elements in c.r.s.	$4n^2t^2+3$	$2nt+1$
# G-elements in Commitment	1	1
# Rounds	$2\log(n^2+(1+2n^2)t^2+4)+7$ $\sim 2\log(n^2+t^2+2n^2t^2)$	$8+2\log(4nt+5)$ $\sim 2\log n + 2\log t$
Message Complexity	# G: $2\log(n^2+(1+2n^2)t^2+4)$ $\sim 2\log(n^2+t^2+2n^2t^2)$ # F_p: $\log(n^2+(1+2n^2)t^2+4)+9$ $\sim \log(n^2+t^2+2n^2t^2)$	# G: $2\log(3nt+5)$ $\sim 2\log n + 2\log t$ # F_p: $\log(3nt+5)+10$ $\sim \log n + \log t$

Table 3. Performances of ZKA for $\mathbf{U}^{\mathrm{T}}\mathbf{QW}=\mathbf{W}^{\mathrm{T}}\mathbf{RV}+\mathbf{S}$: $\mathbf{U},\mathbf{V},\mathbf{W} \in F_p^{n\times t}$

	Linearization Approach[12]	Our Approach (3.41)
# G-elements in c.r.s.	$8n^2t^2+3$	$3nt+1$
# G-elements in commitment	1	1
# Rounds	$2\log(2n^2+(1+4n^2)t^2+4)+7$ $\sim 2\log(2n^2+t^2+4n^2t^2)$	$8+2\log(9nt+5)$ $\sim 2\log n + 2\log t$
Message Complexity	# G: $2\log(2n^2+(1+4n)t^2+4)$ $\sim 2\log(2n^2+t^2+4n^2t^2)$ # F_p: $\log(2n^2+(1+4n)t^2+4)+9$ $\sim \log(2n^2+t^2+4n^2t^2)$	# G: $2\log(9nt+5)$ $\sim 2\log n + 2\log t$ # F_p: $\log(9nt+5)+9$ $\sim \log n + \log t$

Table 4. Asymptotic performances of ZKA for bilinear relations with witness matrices in $F_p^{n\times t}$

		Linearization Approach	Our Approach
# Rounds	$n \sim t >> 1$	$\sim 8\log n$	$\sim 4\log n$
	$n >> t$	$\sim 4\log n$	$\sim 2\log n$
	$t >> n$	$\sim 4\log t$	$\sim 2\log t$
# G elements	$n \sim t >> 1$	$\sim 8\log n$	$\sim 2\log n$
	$n >> t$	$\sim 4\log n$	$\sim 2\log n$
	$t >> n$	$\sim 4\log t$	$\sim 2\log t$
# F_p elements	$n \sim t >> 1$	$\sim 4\log n$	$\sim 2\log n$
	$n >> t$	$\sim 2\log n$	$\sim \log n$
	$t >> n$	$\sim 2\log t$	$\sim \log t$

5 Decreasing Knowledge-Error via Operations on Extended Field: Arguments for Linear Matrix Relations

We now present a approach to enhancing knowledge-soundness of the ZKA's for matrix relations over the ground field F_p. In this approach, we treat any matrix **U** in $F_p^{n\times td}$ equivalently as a nt-dimensional vector over the d-th extended field GF(p,d) ≡ $F_p[X]/(f(X))$ and then, by appropriate reductions, we can decrease the knowledge-error of the original ZKA over F_p from O(1/p) down to O(1/p^d) while significantly improving other performances.

GF(p,d) ≡ $F_p[X]/(f(X))$ is a finite field which elements are polynomials of degree < d in $F_p[X]$ and $f(X)$ is a monic irreducible polynomial of degree d. In particular, GF(p,d) is of cardinality p^d. All analysis and results in the following does not depend on any special selection of the extension degree d or $f(X)$. In practice, d can be completely determined by the target knowledge-error ε (approximately by $p^{-d} < \varepsilon$).

5.1 Generalized Pedersen Scheme for Vectors over Extended Galois Field

At first we generalize the Pedersen commitment scheme from committing to F_p-vectors to committing to GF(p,d)-vectors. Let G be a cyclic group of order p with DLP-hardness property, $\mathrm{cmt}_\sigma(\boldsymbol{w};\ r)$: $F_p^n \times F_p \rightarrow$ G be the Pedersen commitment scheme for any n-dimensional F_p-vector $\boldsymbol{w}$, S be the extended Galois field GR(p,d), $\boldsymbol{u}$ be any n-dimensional S-vector, i.e.,

$$\boldsymbol{u} = \begin{bmatrix} u_1(X) \\ \vdots \\ u_n(X) \end{bmatrix} = \begin{bmatrix} u_1(1) \\ \vdots \\ u_1(n) \end{bmatrix} + \begin{bmatrix} u_2(1) \\ \vdots \\ u_2(n) \end{bmatrix} X + \cdots + \begin{bmatrix} u_d(1) \\ \vdots \\ u_d(n) \end{bmatrix} X^{d-1} \in S^n \qquad (5.1)$$

with each $u_i(k)$ in F_p, k=1,…, n. define

$$\mathrm{Cmt}(\sigma|\boldsymbol{u};\ \boldsymbol{r}) \equiv \begin{bmatrix} \mathrm{cmt}_\sigma(u_1(1),\ldots,u_1(n);r_1) \\ \vdots \\ \mathrm{cmt}_\sigma(u_d(1),\ldots,u_d(n);r_d) \end{bmatrix} \in G^d\text{: } \mathrm{S}^n \times {F_p}^d \rightarrow \mathrm{G}^d \quad (5.2)$$

as the commitment to the vector $\boldsymbol{u}$. More explicitly, given the public-key σ ≡ [G, $\boldsymbol{g}$, h, p] with $\boldsymbol{g} \equiv (g_1,\ldots, g_n)$, g_i and h being group elements, the commitment to $\boldsymbol{u}$ is

$$\mathrm{Cmt}(\sigma|\boldsymbol{u};\ \boldsymbol{r}) = \begin{bmatrix} h^{r_1} g_1^{u_1(1)} \ldots g_n^{u_1(n)} \\ \vdots \\ h^{r_d} g_1^{u_d(1)} \ldots g_n^{u_d(n)} \end{bmatrix} \in G^d \qquad (5.3)$$

As before we frequently denote $g_1^{w_1} \ldots g_n^{w_n}$ as $\boldsymbol{g}[\boldsymbol{w}]$ and $g_1^e \ldots g_n^e$ as $\boldsymbol{g}[e]$ to simplify the expressions.

For any matrix $F_p^{n\times td}$ ∋**U** ≡ [**U**$_1$,…,**U**$_t$] with each block **U**$_i$ in $F_p^{n\times d}$ we associate a S-vector $\boldsymbol{u}^*$ with **U** as:

$$\boldsymbol{u}^* \equiv \begin{bmatrix} \boldsymbol{U}_1 \\ \vdots \\ \boldsymbol{U}_t \end{bmatrix} \begin{bmatrix} 1 \\ X \\ X^2 \\ \vdots \\ X^{d-1} \end{bmatrix} \in S^{tn} \tag{5.4}$$

On basis of this association (which is obviously one-to-one) and given the public-key $\sigma \equiv [G, \boldsymbol{g}, h, p]$ with $\boldsymbol{g} \equiv (g_{ij}) = (g_{11}, \ldots, g_{n,t})$, we define the commitment to matrix **U** as the commitment to the *nt*-dimensional vector $\boldsymbol{u}^*$:

$$\text{Cmt}(\sigma|\boldsymbol{U}; \boldsymbol{r}) \equiv \text{Cmt}(\sigma|\boldsymbol{u}^*; \boldsymbol{r}) \tag{5/5}$$

More explicitly, for the matrix:

$$\mathbf{U} = \begin{bmatrix} u_{11}(1), \ldots, u_{1d}(1), \ldots, u_{t1}(1), \ldots, u_{td}(1) \\ \vdots \\ u_{11}(n), \ldots, u_{1d}(n), \ldots, u_{t1}(n), \ldots, u_{td}(n) \end{bmatrix} \in F_p^{n \times td} \tag{5.6}$$

its associated S-vector is:

$$\boldsymbol{u}^* = \begin{bmatrix} u_{11}(1) + u_{12}(1)X + \cdots + u_{1d}(1)X^{d-1} \\ \vdots \\ u_{11}(n) + u_{12}(n)X + \cdots + u_{1d}(n)X^{d-1} \\ \vdots \\ u_{t1}(1) + u_{t2}(1)X + \cdots + u_{td}(1)X^{d-1} \\ \vdots \\ u_{t1}(n) + u_{t2}(n)X + \cdots + u_{td}(n)X^{d-1} \end{bmatrix} \in S^{nt}$$

and the commitment is computed as:

$$\text{Cmt}(\sigma|\boldsymbol{U}; \boldsymbol{r}) = \begin{bmatrix} cmt_\sigma(u_{11}(1), \ldots, u_{11}(n), \ldots, u_{t1}(1), \ldots, u_{t1}(n)) \\ \vdots \\ cmt_\sigma(u_{1d}(1), \ldots, u_{1d}(n), \ldots, u_{td}(1), \ldots, u_{td}(n)) \end{bmatrix} \in G^d \tag{5.7}$$

Note that this definition of commitment to matrix is consisted with the definition in (2.2)-(2.3) in case of $d = 1$.

Both generalized commitment schemes for vectors over GF(*p*,*d*) and matrices over F_p are perfect-hiding and computational-binding. Hiding property is easy to confirm. To prove binding property of the scheme for GF(*p*,*d*)-vectors, suppose some P.P.T. algorithm A can output $\boldsymbol{u}$ and $\boldsymbol{v}$ such that $\boldsymbol{u} \neq \boldsymbol{v}$ but $\text{Cmt}(\sigma|\boldsymbol{u};\boldsymbol{r}) = \text{Cmt}(\sigma|\boldsymbol{v};s)$. By (5.2), this implies that there is some k such that $(u_k(1), \ldots, u_k(n)) \neq (v_k(1), \ldots, v_k(n))$ but their commitments (the *k*-th component of $\text{Cmt}(\sigma|\boldsymbol{u};\boldsymbol{r})$ and $\text{Cmt}(\sigma|\boldsymbol{v};s)$ are equal to each other:

$$\text{cmt}_\sigma(u_k(1), \ldots, u_k(n); r_k) = \text{cmt}_\sigma(v_k(1), \ldots, v_k(n); s_k)$$

which ruins (computational) binding property of the underlying Pedersen commitment scheme $\text{cmt}_\sigma(.)$, a contradiction. Similar analysis can prove that binding-property holds for matrix commitment scheme (5.5).

It is also straightforward to show that these generalized schemes have the usual homomorphism properties. In addition, the scheme Cmt(σ|.;.): $S^n \times F_p{}^d \to G^d$ has an algebraic property helpful in protocol construction.

Lemma 1 Let e be in Galois field S=GF(p,d)≡$F_p[X]/(f(X))$ and $\mathbf{M}_e \in F_p^{d\times d}$ be its associated multiplicative matrix, i.e., for any

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

there holds

$$eu = \sum_{i=1}^{d}(\sum_{j=1}^{d} M_e(i,j)u_j)X^{i-1} \tag{5.8}$$

Also let the commitment to $\boldsymbol{u}$ be:

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

and $\boldsymbol{u}$ be the S-vector in (5.1), then :

$$\text{Cmt}(\sigma|e\boldsymbol{u};\boldsymbol{s}) = \begin{bmatrix} \prod_{j=1}^{d} C_j^{M_e(1,j)} \\ \cdot \\ \cdot \\ \prod_{j=1}^{d} C_j^{M_e(d,j)} \end{bmatrix},\ \boldsymbol{s} = \mathbf{M}_e\boldsymbol{r},\ \text{i.e.},\ s_l = \sum_{j=1}^{d} M_e(l,j)r_j\ l=1,\ldots,d \tag{5.9}$$

Equality (5.9) is denoted by Cmt(σ|$e\boldsymbol{u}$;$\boldsymbol{s}$) = Cmt(σ|$\boldsymbol{u}$;r)^e.

Proof For each k =1,…, n let $\boldsymbol{u}$'s k-th component be:

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

so by (5.8) one has $eu_k = \sum_{i=1}^{d}(\sum_{j=1}^{d} M_e(i,j)u_j(k))X^{i-1}$, hence

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

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

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

where $\mathbf{U} \equiv \begin{bmatrix} u_1(1) & \cdots & u_d(1) \\ \vdots & \ddots & \vdots \\ u_1(n) & \cdots & u_d(n) \end{bmatrix} \in F_p^{n\times d}$ and the F_p-matrix $\boldsymbol{W} = \mathbf{U}\mathbf{M}_e^{\mathbf{T}} = [\boldsymbol{u}_1,\ldots,\boldsymbol{u}_d]\mathbf{M}_e^{\mathbf{T}}$ ≡ [$\boldsymbol{w}_1$,…,$\boldsymbol{w}_d$] with column vectors $\boldsymbol{w}_k$:

$$\boldsymbol{w_k} = \sum_{j=1}^{d} M_e\,(k,j)\boldsymbol{u}_j \quad k=1,\ldots,\, d \tag{5.10}$$

By Pedersen scheme cmt_σ's homomorphism property, the k-th component of $\mathrm{Cmt}(\sigma|e\boldsymbol{u})$ is (for simplicity we omit the randomness expressions):

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

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

which proves the first equality in (5.9). The second equality $\boldsymbol{s} = \mathbf{M}_e\boldsymbol{r}$ is easy to be confirmed by the same calculation.

Remark 1 For any e in S and F_p-matrix $\mathbf{U} \in F_p^{n\times d}$ this proof also shows that $\mathrm{Cmt}(\sigma|\mathbf{U}\mathbf{M}_e^{\mathbf{T}}) = \mathrm{Cmt}(\sigma|\mathbf{U})^e$.

Remark 2 According to the equality between randomness $\boldsymbol{r}$, e and $\boldsymbol{s}$ in (5.9) and the fact that $\mathbf{M}_e$ is non-singular (actually $\mathbf{M}_e^{-1} = \mathbf{M}_{e^{-1}}$ for any $e \neq 0$), $\boldsymbol{r}$ is uniformly distributed over $F_p^{\,d}$ if and only if $\boldsymbol{s}$ is uniformly distributed over $F_p^{\,d}$.

5.2 Knowledge-Soundness Enhanced ZKA for Linear Matrix Relations over $\mathbf{F}_p$

Consider the linear matrix relation $\mathbf{AU} = \mathbf{B}$ over F_p with matrix witness $\mathbf{U} \in F_p^{N\times d}$ and public matrices $\mathbf{A} \in F_p^{l\times N}$, $\mathbf{B} \in F_p^{l\times d}$. To construct the efficient argument protocol for this relation with commitment to F_p-matrix $\mathbf{U}$ and operations on S = GF(p,d), the first step is to establish a relation over S which is equivalent to the given linear matrix relation over F_p.

For $\mathrm{S} \equiv F_p[X]/(f(X)) = \mathrm{GF}(p,d)$ with degree-d irreducible monic polynomial $f(X)$ and matrix $\mathbf{A} \in F_p^{l\times N}$, define a S-linear operator:

$$\mathbf{L}_\mathrm{A}\colon \mathrm{S}^N \to \mathrm{S}^l\colon \mathrm{L}_\mathrm{A}(\boldsymbol{u})_i \equiv \sum_{k=1}^{N} a_{ik}\,u_k(X) \bmod f(X),\ i = 1,\ldots,\, l \tag{5.11}$$

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

For F_p-matrices

$$\mathbf{U} = \begin{bmatrix} u_1(1) & \cdots & u_d(1) \\ \vdots & \ddots & \vdots \\ u_1(N) & \cdots & u_d(N) \end{bmatrix},\quad \mathbf{B} = \begin{bmatrix} b_1(1) & \cdots & b_d(1) \\ \vdots & \ddots & \vdots \\ b_1(l) & \cdots & b_d(l) \end{bmatrix} \tag{5.12}$$

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, their corresponding S-vectors are:

$$\boldsymbol{u}^* = \begin{bmatrix} u_1(X) \\ \cdot \\ \cdot \\ u_n(X) \end{bmatrix} = \mathbf{U}\begin{bmatrix} 1 \\ X \\ X^2 \\ \vdots \\ X^{d-1} \end{bmatrix} \in S^N,\ \ \boldsymbol{b}^* = \begin{bmatrix} b_1(X) \\ \vdots \\ \vdots \\ b_l(X) \end{bmatrix} = \mathbf{B}\begin{bmatrix} 1 \\ X \\ X^2 \\ \vdots \\ X^{d-1} \end{bmatrix} \in S^l \tag{5.13}$$

Then for the S-vector $\boldsymbol{u}^*$ corresponding to F_p-matrix **U** in (5.12) one has, for each *i*:

$$\mathrm{L_A}(\boldsymbol{u}^*)_i = \sum_{k=1}^{N} a_{ik}\, u_k(X) = \sum_{j=1}^{d}(\sum_{k=1}^{N} a_{ik}\, u_j\,(k))X^{j-1} \bmod f(X)$$

As a result, there is the fact that:

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

$$\text{if and only if } \sum_{k=1}^{N} a_{ik} u_j\,(k) = b_j(i) \text{ for all } i, j, \text{ i.e., } \mathbf{AU} = \mathbf{B} \text{ over } F_p \qquad (5.14)$$

Based on the fact (5.14), the problem of constructing a ZKA protocol for the linear matrix relation over F_p can be transformed into a problem of constructing a ZKA protocol for a linear relation over the extended field S.

Let S ≡ GR(*p*,*d*), σ be the public-key of the S-vector commitment scheme and used as c.r.s. of the argument protocol, the linear relation **SLR** on space S^N is defined as (variables in the frame are witnesses):

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

where $\mathbf{L}_\mathrm{A}$ is defined in (5.11) with $\mathbf{A} \in F_p^{l\times N}$, $\boldsymbol{b} \in S^l$; witnesses $\boldsymbol{u}$ is a *N*-dimensional S-vector, $\boldsymbol{r}$ is a random vector in $F_p^{\,d}$. The commitment to S-vector $\boldsymbol{u}$ is:

$$U=\mathrm{Cmt}(\sigma|\boldsymbol{u};\boldsymbol{r})=\mathrm{Cmt}(\sigma|\begin{bmatrix} u_1(1) & \cdots & u_d(1) \\ \vdots & \ddots & \vdots \\ u_1(N) & \cdots & u_d(N) \end{bmatrix}, \begin{bmatrix} r_1 \\ . \\ . \\ r_d \end{bmatrix})=\begin{bmatrix} \mathrm{cmt}_\sigma(u_1(1), \ldots, u_1(N); r_1) \\ . \\ . \\ \mathrm{cmt}_\sigma(u_d(1), \ldots, u_d(N); r_d) \end{bmatrix} \qquad (5.15)$$

which is also the commitment to a F_p-matrix **U**, i.e., $U = \mathrm{Cmt}(\sigma|\mathbf{U}; \boldsymbol{r})$ (see (5.5)). This reduction is the starting point to construct ZKA protocol for linear matrix relation over F_p. Formally, the linear matrix relation over F_p :

$$\mathbf{MLR}(\sigma|U, \mathbf{B}, \mathbf{A}; \boxed{\boldsymbol{r}, \mathbf{U}}): U = \mathrm{Cmt}(\sigma|\mathbf{U};\boldsymbol{r}) \wedge \mathbf{AU} = \mathbf{B} \qquad (5.16)$$

with $\mathbf{U} \in F_p^{N\times d}$(witness), $\mathbf{A} \in F_p^{l\times N}$, $\mathbf{B} \in F_p^{l\times d}$ is equivalent to the linear relation over Galois field S = GF(*p*,*d*) ≡ $F_p[X]/(f(X))$:

$$\mathbf{SLR}(\sigma|V, \boldsymbol{b}, \mathbf{L_A}; \boxed{\boldsymbol{r}, \boldsymbol{u}^*}): V = \mathrm{Cmt}(\sigma|\boldsymbol{u}^*;\boldsymbol{r}) \wedge \mathbf{L}_\mathrm{A}(\boldsymbol{u}^*) = \boldsymbol{b}^* \qquad (5.17)$$

where $\boldsymbol{u}^* \in S^N$(witness), $\mathbf{L}_\mathrm{A}$ is the linear operator defined in (5.11), $b^*_i = \sum_{j=1}^{d} b_j\,(i)X^{j-1}$ and $V = U$. These two relations' witnesses are related by the first equality in (5.13).

Note that $\mathbf{L}_\mathrm{A}(\boldsymbol{u}) = \boldsymbol{b}$ in (5.17) is a system of *l* linear equations in S which can be further reduced to only one linear equation via the standard amortization technique, i.e., given any randomness ρ sampled by the verifier, with probability > $1 - lp^{-d}$ the vector equation $\mathbf{L}_\mathrm{A}(\boldsymbol{u}) = \boldsymbol{b}$ is equivalent to the scalar equation:

$$\sum_{\mathrm{i}=1}^{l}(\mathrm{L_A}(\boldsymbol{u})_\mathrm{i} - b_\mathrm{i})\,\rho^{\mathrm{i}-1} = 0$$

Obviously this reduction has soundness factor *l*. In summary, we have:

Theorem 5 Linear matrix relation $\mathbf{MLR}(\sigma|U, \boldsymbol{B}, \mathbf{A}; \boxed{\boldsymbol{r}, \boldsymbol{U}})$ in (5.16) is probabilistically equivalent to the linear relation (5.18) with soundness factor *l*:

$$sl\text{-R}(\sigma|U, b_\rho, l_{A,\rho}; \boxed{\boldsymbol{r}, \boldsymbol{u}^*}): U = \mathrm{Cmt}(\sigma|\boldsymbol{u}^*;\boldsymbol{r}) \wedge l_{\mathrm{A},\rho}(\boldsymbol{u}^*) = b_\rho \qquad (5.18)$$

where $\boldsymbol{u}^* \in S^N$, ρ is a randomness sampled by the verifier, $b_\rho \equiv \sum_{i=1}^{l} b_i^* \rho^{i-1} \in S$ and the S-linear functional $l_{A,\rho}$ is defined as:

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

The efficient ZKA protocol for linear matrix relation (5.16) over F_p can now be constructed equivalently for the linear vector relation (5.18) over the extended field S via compressed techniques in [6][7][12]. For example, [12] presented such a protocol framework with logarithmic message complexity and provided complete analysis about its completeness, zero-knowledge and knowledge soundness properties. The protocol will not be repeated here. The only modification is that in our approach all arithmetic operations are in the extended field S so for any e in S and $U \equiv (U_1,\ldots,U_d)$ in G^d, U^e is computed by(see (5.9) in lemma 1):

$$U^e = \begin{bmatrix} \prod_{j=1}^{d} U_j^{M_e(1,j)} \\ \cdot \\ \cdot \\ \prod_{j=1}^{d} U_j^{M_e(d,j)} \end{bmatrix} \tag{5.19}$$

and all multiplications on G^d is component-wise.

In general, for any $t > 1$: $\mathbf{U} \equiv [\mathbf{U}_1,\ldots,\mathbf{U}_t] \in F_p^{n\times td}$, $\mathbf{A} \in F_p^{l\times n}$, $\mathbf{B} \equiv [\mathbf{B}_1,\ldots,\mathbf{B}_t] \in F_p^{l\times t}$ and $\mathbf{AU} = \mathbf{B}$ we can apply the efficient ZKA protocol construction to the equivalent linear relation $\mathbf{A}^*\mathbf{U}^* = \mathbf{B}^*$, i.e.,

$$\begin{bmatrix} \mathbf{A} & .. & \boldsymbol{O} \\ .. & .. & .. \\ \boldsymbol{O} & .. & \boldsymbol{A} \end{bmatrix} \begin{bmatrix} \boldsymbol{U}_1 \\ ... \\ \boldsymbol{U}_t \end{bmatrix} = \begin{bmatrix} \boldsymbol{B}_1 \\ ... \\ \boldsymbol{B}_t \end{bmatrix},\ \mathbf{U}^* \equiv \begin{bmatrix} \boldsymbol{U}_1 \\ ... \\ \boldsymbol{U}_t \end{bmatrix} \in F_p^{tn\times d} \tag{5.20}$$

with $1+nt$ group elements in c.r.s. σ and the commitment to $\mathbf{U}$ (equivalently, to $\mathbf{U}^*$):

$$\mathrm{Cmt}(\sigma|\mathbf{U})_j = \mathrm{cmt}_\sigma([\boldsymbol{u}_j^{(1)\mathrm{T}},\ldots,\boldsymbol{u}_j^{(t)\mathrm{T}}]) \in G,\ j = 1,\ldots,d \tag{5.21}$$

where each F_p-vector $\boldsymbol{u}_j^{(k)}$ is the j-th column in $\mathbf{U}_k$. The corresponding S-linear relation of (5.20) is specified on space S^{nt} (see (5.18)).

Table 5 summaries the performance comparisons between our approach and the d-fold parallelism one. Both approaches use the same ZKA protocol with logarithmic message complexity.

In our approach the protocol operates over the extended field S = GF(p,d) with a nt-dimensional witness vector over S and only 1 running instance, while in the parallel repetition approach the protocol operates over the ground field F_p with d running instances in parallel and each with a ntd-dimensional witness vector (actually a n-by-td matrix) over F_p. The cardinality of challenge space in our approach is p^d while in parallel repetition approach is p. Since both protocols have exactly the same (3,3,…,3)-special-soundness property, according to the general result in [21], our protocol has the knowledge-error(theorem 3 in sec.3 of [21]):

$$\kappa_{(\mathrm{ours})} = 1 - \prod_{j=t}^{\mu}\left(1 - \frac{2}{p^d}\right) \sim 2\mu/p^d \ \text{ with } \mu = \log(nt) \tag{5.21}$$

while the d-fold parallel repetition approach has its knowledge-error (theorem 4 [21]):

$$\kappa_{(\text{para.rept.})} = [1-\prod_{j=t}^{\mu}(1-\frac{2}{p})]^d \sim (2\mu/p)^d \text{ with } \mu = \log(ntd) \quad (5.22)$$

In particular, for squares of order-n (in this case $t = n/d$) we have the simpler and more explicit result that:

$$\kappa_{(\text{ours})} \sim (4\log n - 2\log d)/p^d,\ \kappa_{(\text{para.rept.})} \sim (4\log n/p)^d \quad (5.23)$$

Since n is poly($\log p$), we have $\kappa_{(\text{ours})} \sim 1/p^d \sim \kappa_{(\text{para.rept.})}$.

Remark 3 By the inequality $1-(1-x_1)\ldots(1-x_N) < x_{1+}\ldots+x_N$ for any x_i in [0,1], all the terms on the right sides of (5.21~23) are upper-bounds of their left sides respectively.

Communication performances of both approaches are evaluated via the same statement (e.g., theorem 2 in [12]). Note that due to reduction one extra message and one S-element should be added in our approach.

In our approach, the objects under operations are polynomials of (d–1)-degree with coefficients in F_p which can be processed equivalently and efficiently as d-dimensional vectors over F_p, and the commitments are valued in G^d, so the total number of G and S elements are d times those over F_p. For the parallel repetition approach, the same d factor also appears but due to d-fold parallelism. On the other hand, since our approach is for the linear relation on nt-dimensional space (over S) while the parallel repetition approach is for the relation on ntd-dimensional space (over F_p), the number of rounds in our approach is decreased by $\log d$. It is interesting that due to the gap in dimensions our approach outperforms the parallel repetition one by 2$\log d$ in number of rounds, $d\log d$ in total number of F_p elements and 2$d\log d$ in total number of G elements.

Our approach needs d G-elements for commitment, d times more than the parallel one while the latter needs larger-sized c.r.s than ours by d times.

In summary, compared with the general parallel repetition approach, our approach (matrix-specific) to linear relation can reach the knowledge-error $O(1/p^d)$ with almost the same computational complexity while significantly improving communication performances, i.e., smaller c.r.s., fewer rounds and shorter messages in total.

Table 5. Performances of different approaches for linear matrix relation **AU**=**B**: **U**$\in F_p^{n\times td}$

	d-fold parallel repetition over F_p	single invocation over GF(p,d)
	Both with knowledge error ~ $\boldsymbol{p^{-d}}$	
#of G-elements in c.r.s.	1+ntd	1+nt
# of G-elements for commitment	1	d
# of rounds	2log$n$ + 2log$t$ + 2log$d$ – 1	2log$n$ + 2log$t$
# of G elements in message	(2log(ntd) – 2)d	(2log(nt)–2)d
# of F_p elements in message	(1+log(ntd))d	(2+log(nt))d

Table 6 presents the special case of table 5 where **U** is a square with $n = td$.

Table 6. Performance of different approaches for linear matrix relation **AU**=**B**: **U**$\in F_p^{n\times n}$

	d-fold parallel repetition over F_p	single invocation over GF(p,d)	Improvement in fraction
	Both with knowledge error ~ $\boldsymbol{p^{-d}}$		≈
#of G-elements in c.r.s.	$1+n^2$	$1+n^2/d$	d
# of G-elements for commitment.	1	d	$1/d$
# of rounds	$4\log n - 1$	$4\log n - 2\log d$	$\log d/2\log n$
# of G elements in message	$(4\log n - 2)d$	$(4\log n - 2\log d - 2)d$	$\log d/2\log n$
# of F_p elements in message	$(1+2\log n)d$	$(2+2\log n - \log d)d$	$\log d/2\log n$

5.3 More Linear Matrix Relations

Relation AUB$^{\mathbf{T}}$ = C Consider the linear relation over F_p for matrix $\mathbf{A,B,C,U} \in F_p^{n\times n}$ where **U** is the witness, $n = td$ is a power of 2 and d is the extension degree of Galois field S ≡ GR(p,d) which value is determined by the target knowledge-error. Let:

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

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

Both $\mathbf{U}^*$ and $\mathbf{C}^*$ 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$^{\mathbf{T}}$** = **C** can be represented as:

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

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

$$\text{i.e.,}\ \ \tilde{\mathbf{C}} = \boldsymbol{\Omega}(\mathbf{A},\mathbf{B})\mathbf{U}^* \qquad (5.22)$$

where $\tilde{\mathbf{C}} \in F_p^{n^2\times d}$ has the entry $\tilde{C}_{iqj} \equiv C_{i,(j-1)d+q}$ and $\boldsymbol{\Omega} \in F_p^{n^2\times nt}$ has its entry:

$$\boldsymbol{\Omega}_{ijq,\,klh} \equiv A_{ik}B_{(j-1)d+q,\,(l-1)d+h} \quad i,k=1,\ldots,n;\ j,l=1,\ldots,t \qquad (5.23)$$

In summary, the relation **AUB$^{\mathbf{T}}$** = **C** with witness $\mathbf{U} \in F_p^{n\times n}$ is equivalent to the relation (5.22) with witness $\mathbf{U}^* \in F_p^{nt\times d}$. The ZKA protocol for the former relation can

be equivalently constructed for the latter with the method presented in sec.5.2, with the same performances indicated in tab.6.

Relation $\mathbf{AU + UB^T = C}$ Consider the linear relation over residue ring Z_m for matrix $\mathbf{A,B,C,U} \in F_p^{n\times n}$ where $\mathbf{U}$ is the witness, $n = td$ is a power of 2 and d is the extension degree of $S \equiv GF(p,d)$ over F_p which value is determined by the target knowledge-error.

Let $\mathbf{U}^*$ and $\mathbf{C}^*$ be specified as before, obviously in the same way as before equation $\mathbf{AU + UB^T = C}$ is equivalent to the equation

$$\tilde{\mathbf{C}} = (\mathbf{\Omega}(\mathbf{A},\mathbf{I}_n) + \mathbf{\Omega}(\mathbf{I}_n,\mathbf{B}))\mathbf{U}^* \tag{5.24}$$

where $\mathbf{\Omega(A,B)}$ is specified in (5.23) for any given matrix $\mathbf{A}$ and $\mathbf{B}$. The ZKA protocol for $\mathbf{AU + UB^T = C}$ can be equivalently constructed for (5.24) with the method presented in sec.5.2, which performances are the same as in tab.6.

Relation $\mathbf{A_1UB_1^T + \ldots + A_kUB_k^T = C}$ On basis of the above methods, the efficient ZKA protocol for this general linear relation can be also constructed which performances are the same as indicated in tab. 6.

Remark 4 Since any relation over F_p can be reduced to a linear relation (via linearization), as a result any relation which can be reduced to a linear matrix relation can be enhanced in knowledge-error by the above result.

Remark 5 The same approach can apply to some non-linear matrix relations, e.g., bilinear matrix relation $\mathbf{U^TQV = Y}$ but will be more technically complicated, which will be completed in future works.

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. IACR. ePrint, 2022:181, 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 Elman R, Karpenko N and Merkurjev A. Algebraic and geometric theory of quadratic forms[M]. New York: American Mathematical Society, 2017.

21 Attema T, Fehr S. Parallel repetition of $(k_1, ..,k_u)$-special-sound multi-round interactive proofs. Advances in Cryptology - CRYPTO 2022, LNCS Vol. 13507, 415–443, 2022.

22 Attema T, Fehr S, Kloos M. Fiat-Shamir transformation of multi-round interactive proofs, eprint.iacr.org/2021/137, 2021.