ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/228965324

Key Exchange Protocol using Matrix Algebras and its Analysis

Article *in* Journal of the Korean Mathematical Society · November 2005

DOI: 10.4134/JKMS.2005.42.6.1287

CITATIONS
4

READS
206

4 authors, including:

Soojin Cho
Ajou University, Suwon, South Korea
23 PUBLICATIONS **127** CITATIONS

SEE PROFILE

Kil-Chan Ha
Sejong University
42 PUBLICATIONS **678** CITATIONS

SEE PROFILE

All content following this page was uploaded by Soojin Cho on 22 April 2014.

The user has requested enhancement of the downloaded file.

J. Korean Math. Soc. **42** (2005), No. 6, pp. 1287–1309

KEY EXCHANGE PROTOCOL USING MATRIX ALGEBRAS AND ITS ANALYSIS

Soojin Cho*, Kil-Chan Ha,
Young-One Kim*, and Dongho Moon

Abstract. A key exchange protocol using commutative subalgebras of a full matrix algebra is considered. The security of the protocol depends on the difficulty of solving matrix equations $XRY = T$, with given matrices R and T. We give a polynomial time algorithm to solve $XRY = T$ for the choice of certain types of subalgebras. We also compare the efficiency of the protocol with the Diffie-Hellman key exchange protocol on the key computation time and the key size.

1. Introduction

Many key exchange protocols have been proposed [2, 3, 14, 16, 19] since the Diffie-Hellman protocol was proposed in [5], which is most popularly used. One of them is the protocol using commutative subsemigroups of some noncommutative semigroup by Sidelnikov, Cherepnev and Yashchenko[4] which can be described as follows:

Let H and R be commutative subsemigroups of a noncommutative semigroup $(G, \star)$, and σ be a fixed element of G. Alice chooses $h_A \in H$, $r_A \in R$ and send $h_A \star \sigma \star r_A$ to Bob, while Bob chooses $h_B \in H$, $r_B \in R$ and send $h_B \star \sigma \star r_B$ to Alice. The shared key is $h_B \star (h_A \star \sigma \star r_A) \star r_B = h_A \star (h_B \star \sigma \star r_B) \star r_A$. The security of the protocol depends on the difficulty of the factorization: Write an element $g \in G$ as a product $x \star \sigma \star y$ for $x \in \widetilde{H}, y \in \widetilde{R}$, where $\widetilde{H} \supseteq H$ and $\widetilde{R} \supseteq R$ are commutative subsemigroups of G. If G is a groups rather than a semigroup, then

Received January 20, 2005.
2000 Mathematics Subject Classification: 15A24, 94A60.
Key words and phrases: key exchange protocol, matrix algebra, Diffie-Hellman key exchange.
*This work was supported by the Korea Research Foundation Grant(KRF-2002-015-CP0049).

the factorization problem is to find x, y satisfying $x \star g = \sigma \star y$ and the inverse of x.

In [4], the case when G is a cyclic subgroup of a finite general linear group is considered, and the analysis shows that this case is not secure since the equation $x \star g = \sigma \star y$ becomes a system of linear equations.

In this article, we consider a key exchange protocol using matrix *algebras* over finite fields, not just a multiplicative group of nonsingular matrices. We started our work as an attempt to find a more efficient key exchange protocol on the key computation time than Diffie-Hellman type, and came up with a protocol using matrix algebras. We, however, found out that the basic idea of construction is exactly the same as that of Sidelnikov et al.[4], whereas we also realized that there are many differences that should be considered. Since we consider the *full matrix algebra* rather than the general linear group, matrices do not have to be nonsingular and this makes the analysis of the protocol with respect to the man-in-the-middle attack complicated. In our case, the problem is to solve the matrix equation of X, Y given by $XRY = T$, while in [4], the equation is given by $RY = X^{-1}T$. Note that the equations are quadratic in our case.

Even though the main part of the article is on the analysis, we made efforts to examine the protocol in as many aspects as possible. We consider possible ways to choose commutative subalgebras, analysis with respect to the man-in-the-middle attack, and we also compare the efficiency of the protocol with that of Diffie-Hellman type protocol.

We should mention that the number of solutions to the matrix equation $XRY = T$ with predetermined values of $\mathrm{rank}(R)$, $\mathrm{rank}(T)$ has been known [10, 11, 20]. Our case, however, has more restriction than general matrix equations since X and Y must be in certain commutative subalgebras. It also should be noted that we may use known methods using algorithms to find Gröbner basis of quadratic equations(polynomials) [6, 7] to do the analysis. However, the complexity of those algorithms are not explicitly calculated, and in general it is expected to be exponential. A purpose of this article is to find a polynomial time algorithm to solve $XRY = T$, when X and Y are of certain type of matrices using properties of commutative matrix subalgebras. For that purpose, we use Jordan canonical forms of matrices, for which we must extend the base field $\mathbb{F}_q$ to the splitting field of characteristic polynomials of generators of commutative subalgebras. Thus, without the assumption that generators are given in their Jordan forms, we may not conclude that the algorithm has polynomial time complexity. In that sense, our analysis

does not show the insecurity of the protocol in full, but it tells us about some cases that should be avoided when one wants to use the protocol.

We describe the protocol using matrix algebras and consider some practical issues on the protocol in section 2. Even though the basic idea is exactly the same as that of Sidelnikov et. al., there are some practical issues that should be considered when the full matrix algebra is used. In section 3, we restate the man-in-the-middle attack for our case and review some preliminaries that will be needed to analyze our protocol. In section 4, we formulate problems to be solved to analyze the protocol. In section 5, a polynomial time algorithm is given to solve $XRY = T$ when two commutative subalgebras are cyclic. In section 6, we consider the analysis of more general type and suggest a direction to solve the system, but we were not able to do the full analysis. In the final section, we compare the efficiency of the protocol and Diffie-Hellman type protocol, especially on the key computation time and key size. Then we conclude with several remarks.

2. The protocol

Let $\mathbb{F}_q$ be the Galois field of size q, and $M_n(q)$ be the matrix algebra of $n \times n$ matrices over $\mathbb{F}_q$. The protocol relies on the choice of two subsets $\mathcal{S}_1, \mathcal{S}_2$ of $M_n(q)$, the algebra of all $n \times n$ matrices over $\mathbb{F}_q$, which satisfy the following conditions:

- $(*)$ For any $A_1, B_1 \in \mathcal{S}_1$ and $A_2, B_2 \in \mathcal{S}_2$, $A_1B_1 = B_1A_1$ and $A_2B_2 = B_2A_2$.
- $(**)$ For $A_1 \in \mathcal{S}_1$ and $A_2 \in \mathcal{S}_2$, $A_1A_2 \neq A_2A_1$.

The following is the description of the protocol we are considering, that is exactly the same protocol of Sidelnikov, et. al. except that we use a matrix algebra rather than a semigroup. In the following, we assume that $\mathcal{S}_1, \mathcal{S}_2$ are subsets of $M_n(q)$ satisfying $(*)$ and $(**)$.

Key exchange protocol using matrix algebras
COMMON INPUT $\mathcal{S}_1, \mathcal{S}_2$
OUTPUT An element in $M_n(q)$ shared between Alice and Bob.
1. Alice picks $A_1 \in \mathcal{S}_1$, $A_2 \in \mathcal{S}_2$; sends the product A_1A_2 to Bob.
2. Bob picks $B_1 \in \mathcal{S}_1$, $B_2 \in \mathcal{S}_2$; sends the product B_1B_2 to Alice.
3. Alice computes $K_A = A_1(B_1B_2)A_2$.
4. Bob computes $K_B = B_1(A_1A_2)B_2$.

From the assumption, $K_A = A_1(B_1B_2)A_2 = B_1(A_1A_2)B_2 = K_B$; hence Alice and Bob have computed the same value that is the shared key. Property $(**)$ is essential, otherwise $(A_1A_2)(B_1B_2)$ can be the shared key. The main concern of the protocol is on the choice of $\mathcal{S}_1$ and $\mathcal{S}_2$.

2.1. $\mathcal{S}_1$ and $\mathcal{S}_2$

For a moment, let us assume that $\mathcal{S}_i$'s are commutative subalgebras of $M_n(q)$. Then we may think of at least two ways of describing $\mathcal{S}_1, \mathcal{S}_2$. One is to give an explicit characterization, for example, we may use Schur algebra(see [12, 21]) that is known to be the commutative subalgebra of $M_n(q)$ of the maximum possible dimension. Another is to give generators to define $\mathcal{S}_i$'s. Based on our preliminary investigations, we believe that the first way is not appropriate for the protocol from the security point of view. Thus we assume that $\mathcal{S}_i$'s are given by generators commuting with each other.

Recall that any nonzero unital subalgebra of $M_n(q)$ contains scalar multiples of the identity matrix I_n, which commute with any matrix in $M_n(q)$. This will cause a problem because of the condition $(**)$. Thus we no longer may not make an assumption that $\mathcal{S}_i$'s are subalgebras of $M_n(q)$. To make the condition $(**)$ satisfied, we suggest that one uses the subsets obtained by deleting the multiples of the identity matrix from each commutative subalgebra. The probability that two arbitrarily chosen matrices from $M_n(q) - \{\alpha I_n \mid \alpha \in \mathbb{F}_q\}$ commute is $p(q)/(q^{n^2}-q)^2$, where p is a polynomial in q of degree n^2+n (see [9]). Note that as q or n gets larger, the probability becomes smaller for fixed n and q respectively. Our calculation shows that the probability is about 0.13×10^{-89} when $n = 5$, $q = 2^{15}$. For this reason, once we disregard scalar matrices, we may disregard the possibility for two matrices from $\mathcal{S}_1$ and $\mathcal{S}_2$ commute. For matrices $M_1, \ldots, M_m \in M_n(q)$, let $\langle M_1, \ldots, M_m \rangle$ be the subalgebra of $M_n(q)$ generated by M_i's, that is the set of linear sums of powers of M_i's. We finally can write down our suggestion for the choice of $\mathcal{S}_i$'s: $\mathcal{S}_1 = \langle G_1, \ldots, G_k \rangle - \{\alpha I_n \mid \alpha \in \mathbb{F}_q\}$, $\mathcal{S}_2 = \langle H_1, \ldots, H_l \rangle - \{\alpha I_n \mid \alpha \in \mathbb{F}_q\}$, where G_i's commute with each other, H_j's commute with each other, and $G_iH_j \neq H_jG_i$ for all i, j.

3. A possible attack and preliminaries on matrix algebras

Suppose that Alice and Bob want to share a key using the protocol described in section 2, and they use two subsets $\mathcal{S}_1, \mathcal{S}_2$ of $M_n(q)$. Assume

that the products A_1A_2 and B_1B_2 are intercepted while transmitted. Recall that we have assumed $A_1, B_1 \in \mathcal{S}_1$ and $A_2, B_2 \in \mathcal{S}_2$. Following is the man-in-the-middle attack to our protocol.

(C) If one finds $A_1', A_2' \in M_n(q)$ such that $A_1A_2 = A_1'A_2'$ and A_1', A_2' commute with B_1, B_2 respectively, then the shared key can be computed;

$$A_1'(B_1B_2)A_2' = B_1(A_1'A_2')B_2 = B_1(A_1A_2)B_2\,.$$

Note that in **(C)**, there is no need for A_i' to be contained in $\mathcal{S}_i$, $i = 1, 2$, and finding B_1' and B_2' with appropriate properties must work also.

If one wants to analyze the protocol through the attack **(C)**, it will be needed to understand the structure of commutative subalgebras of $M_n(q)$. We investigate some known results on commutative subalgebras of $M_n(q)$. We use results of this section to analyze our protocol in section 5 and section 6.

3.1. Preliminaries on commutative subalgebras of $M_n(q)$

First, we set up some notations. For a matrix $G \in M_n(q)$, let $J(G)$ denote the Jordan canonical form of G, that can be calculated over the algebraic closure of $\mathbb{F}_q$ (or the splitting field of the characteristic polynomial of G over $\mathbb{F}_q$). For a subalgebra $\mathcal{S}$ of $M_n(q)$ or a matrix A in $M_n(q)$, we let

$$Z(\mathcal{S}) = \{X \in M_n(q) \,|\, XG = GX \text{ for all } G \in \mathcal{S}\}\,,$$

$$Z(A) = \{X \in M_n(q) \,|\, XA = AX\}\,.$$

For $\lambda \in \mathbb{F}_q$ and $(\nu_1, \ldots, \nu_l)$, a sequence of positive integers in decreasing order, we let $J_\lambda(\nu_1, \ldots, \nu_l)$ denote the Jordan block with the diagonal entry λ and each small block is of size ν_i. For example,

$$J_\lambda(3,2) = \begin{bmatrix} \lambda & 1 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 \\ 0 & 0 & \lambda & 0 & 0 \\ 0 & 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & 0 & \lambda \end{bmatrix}.$$

We call $X = (x_{ij})$, an m by n matrix, a *regular upper triangular* matrix if the following conditions are satisfied;

1. $x_{ij} = x_{i'j'}$, whenever $i - j = i' - j'$.
2. $x_{ij} = 0$, if $\min\{m, n\} - n + 1 \le i - j \le m - 1$.

For example, $\begin{bmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix}$ is a regular upper triangular matrix.

The following propositions can be found in [8].

PROPOSITION 1. *$Z(J_\lambda(\nu_1,\ldots,\nu_l))$ is*

$$\{X=(B_{ij})_{1\le i,j\le l} \mid B_{ij} \text{ is an } \nu_i\times\nu_j \text{ regular upper triangular matrix }\}.$$

PROPOSITION 2. *Let A be a block diagonal matrix with diagonal blocks $J_1,\ldots,J_k$, where $J_i=J_{\lambda_i}(\nu_{i1},\ldots,\nu_{il_i})$, and $\lambda_i\neq\lambda_{i'}$ if $i\neq i'$. Then*

$$Z(A)=\{diag(X_1,\ldots,X_k) \mid X_i\in Z(J_i) \text{ for all } i=1,\ldots,k\}.$$

For example, if $A=\mathrm{diag}(J_{\lambda_1}(3,2),J_{\lambda_2}(2,1))$, $\lambda_1\neq\lambda_2$, then elements of $Z(A)$ are of the form $\begin{bmatrix} A & 0\\ 0 & B\end{bmatrix}$, where $A=\left[\begin{array}{cccccc} a & b & c & | & d & e\\ 0 & a & b & | & 0 & d\\ 0 & 0 & a & | & 0 & 0\\ - & - & - & - & - & -\\ 0 & f & g & | & p & q\\ 0 & 0 & f & | & 0 & p\end{array}\right]$ and $B=\left[\begin{array}{cccc} r & s & | & t\\ 0 & r & | & 0\\ - & - & - & -\\ 0 & w & | & z\end{array}\right]$, $a,b,\ldots,z\in\mathbb{F}_q$.

3.2. Cyclic subalgebras

In general, it is not easy to characterize all elements in a commutative subalgebra of $M_n(q)$. It, however, is possible to find a pattern of the elements of $\mathcal{S}$, when $\mathcal{S}$ is a subalgebra of $M_n(q)$ generated by only one matrix (and hence commutative), if we extend the field $\mathbb{F}_q$ so that the Jordan form of the generator can be computed over the extension field. We call $X=(x_{ij})$, an n by n matrix, a *block regular upper triangular matrix of type* $(\mu_1,\ldots,\mu_k)$, $\mu_1\ge\cdots\ge\mu_k$, if the following conditions are satisfied;

1. $\sum_{i=1}^k\mu_i=n$ and X is a block matrix whose (i,j)th block size is $\mu_i\times\mu_j$.
2. If $i\neq j$, (i,j)-block is 0.
3. (i,i)-block is a regular upper triangular matrix.
4. (i,i)-block is the upper left $\mu_i\times\mu_i$ submatrix of $(1,1)$-block.

LEMMA 3. *For a matrix $A\in M_n(q)$, let $\widetilde{\mathbb{F}}_q$ be the splitting field of the characteristic polynomial of A over $\mathbb{F}_q$, and let $J(A)=P^{-1}AP=diag(J_{\lambda_1},\ldots,J_{\lambda_k})$, where the Jordan block J_{λ_i} is of type $(\mu_{i_1},\ldots,\mu_{i_{k_i}})$. If $\mathcal{S}=\langle A\rangle_{\widetilde{\mathbb{F}}_q}$ is the cyclic subalgebra generated by A over $\widetilde{\mathbb{F}}_q$, then*

$$\begin{aligned}\mathcal{S}=\{&PXP^{-1} \mid X=diag(X_1,\ldots,X_k), \text{ where } X_i \text{ is a block regular}\\ &\text{upper triangular matrix over } \widetilde{\mathbb{F}}_q \text{ of type } (\mu_{i_1},\ldots,\mu_{i_{k_i}})\}\end{aligned}$$

Proof. Let $\mathcal{A}$ be the set on the right hand side of the equation in the Lemma. Then $\mathcal{A}$ is a subalgebra of $M_n(\widetilde{\mathbb{F}}_q)$, and $\sum_{i=0}^{m(A)-1} \alpha_i A^i \in \mathcal{A}$ for every $\alpha_i \in \widetilde{\mathbb{F}}_q$. Moreover, $\dim_{\widetilde{\mathbb{F}}_q}(\mathcal{A}) = \dim_{\widetilde{\mathbb{F}}_q}(\mathcal{S})$ is the degree of the minimal polynomial of A. Hence, we conclude that $\mathcal{S} = \mathcal{A}$. □

For example, if $P^{-1}AP = J(A) = \mathrm{diag}(J_{\lambda_1}(3,2), J_{\lambda_2}(2))$, $\lambda_1 \neq \lambda_2$, then the minimal polynomial of A is of degree 5; it is $(x-\lambda_1)^3(x-\lambda_2)^2$. Moreover, elements of $\langle A \rangle_{\widetilde{\mathbb{F}}_q}$ are PXP^{-1}, where $X = \begin{bmatrix} X_1 & 0 \\ 0 & X_2 \end{bmatrix}$, $X_1 = \begin{bmatrix} x_1 & x_2 & x_3 & 0 & 0 \\ 0 & x_1 & x_2 & 0 & 0 \\ 0 & 0 & x_1 & 0 & 0 \\ 0 & 0 & 0 & x_1 & x_2 \\ 0 & 0 & 0 & 0 & x_1 \end{bmatrix}$ and $X_2 = \begin{bmatrix} x_4 & x_5 \\ 0 & x_4 \end{bmatrix}$, $x_1, x_2, x_3, x_4, x_5 \in \widetilde{\mathbb{F}}_q$.

4. Problems to be solved

Suppose that Alice and Bob use the key exchange protocol described in section 2. In this section, we reformulate the problem that is to be solved when someone tries to know the shared key through the attack **(C)**. Therefore, we assume that the product A_1A_2 that Alice sends to Bob and B_1B_2 that Bob sends to Alice are intercepted while transmitted, and the problem to be solved is to find A_1' and A_2' satisfying the conditions $A_1'A_2' = A_1A_2$, $A_1'B_1 = B_1A_1'$, and $A_2'B_2 = B_2A_2'$. We also make a strong assumption that the Jordan form and a similarity transformation matrix of each generator of $\mathcal{S}_i$, $i = 1, 2$ are known. Therefore, we work over the splitting field of characteristic polynomials of generator matrices.

4.1. Simple cases

Suppose that $\mathcal{S}_1 = \langle G \rangle - \{\alpha I_n \,|\, \alpha \in \mathbb{F}_q\}$, $\mathcal{S}_2 = \langle H \rangle - \{\alpha I_n \,|\, \alpha \in \mathbb{F}_q\}$ for $G, H \in M_n(q)$, $GH \neq HG$. That is, each of $\mathcal{S}_1$ and $\mathcal{S}_2$ is generated by only one matrix. let $\widetilde{\mathbb{F}}_q$ be the splitting field of characteristic polynomials of G and H over $\mathbb{F}_q$. Moreover, let us assume that $J(G) = P^{-1}GP = \mathrm{diag}(J_{\lambda_1}, \ldots, J_{\lambda_k})$ and $J(H) = Q^{-1}HQ = \mathrm{diag}(J_{\chi_1}, \ldots, J_{\chi_l})$ denote Jordan canonical forms of G and H, where P, Q and $J(G), J(H)$ are matrices over $\widetilde{\mathbb{F}}_q$, and J_{λ_s} is the Jordan block with respect to the eigenvalue λ_s. Then, by Lemma 3, we may let $A_1' = PXP^{-1}$ and $A_2' = QYQ^{-1}$, where $X = \mathrm{diag}(X_1, ..., X_k)$, $Y = \mathrm{diag}(Y_1, ..., Y_l)$ with X_s, Y_t are block regular upper triangular matrices of corresponding type of J_{λ_s} and J_{χ_t},

respectively. Thus, the equation to be solved is

$$XRY = T\,, \tag{1}$$

where $R = P^{-1}Q$, $T = P^{-1}A_1A_2Q$ and X, Y are block matrices of certain form with unknown entries to be determined. One should note that we are working over an extension field $\widetilde{\mathbb{F}}_q$ of $\mathbb{F}_q$. That is, we are considering $\widetilde{\mathcal{S}}_1 = \langle G\rangle_{\widetilde{\mathbb{F}}_q} - \{\alpha I_n \,|\, \alpha \in \widetilde{\mathbb{F}}_q\}$, $\widetilde{\mathcal{S}}_2 = \langle H\rangle_{\widetilde{\mathbb{F}}_q} - \{\alpha I_n \,|\, \alpha \in \widetilde{\mathbb{F}}_q\}$ rather than $\mathcal{S}_1$ or $\mathcal{S}_2$ itself. Note that R and T are known. Hence, in general, we have quadratic equations with $(\mu_{1_1} + \cdots + \mu_{k_1}) + (\nu_{1_1} + \cdots + \nu_{l_1})$ many variables. For example, if

$$J(G) = \begin{bmatrix} \lambda_1 & 1 & 0 & 0 & 0 & 0 \\ 0 & \lambda_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_1 & 1 & 0 & 0 \\ 0 & 0 & 0 & \lambda_1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \lambda_2 & 1 \\ 0 & 0 & 0 & 0 & 0 & \lambda_2 \end{bmatrix}, \text{ and } J(H) = \begin{bmatrix} \chi_1 & 1 & 0 & 0 & 0 & 0 \\ 0 & \chi_1 & 1 & 0 & 0 & 0 \\ 0 & 0 & \chi_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \chi_2 & 1 & 0 \\ 0 & 0 & 0 & 0 & \chi_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & \chi_2 \end{bmatrix},$$

for $\lambda_i, \chi_j \in \widetilde{\mathbb{F}}_q$, then we may let

$$X = P^{-1}A_1'P = \begin{bmatrix} x_1 & x_2 & 0 & 0 & 0 & 0 \\ 0 & x_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & x_1 & x_2 & 0 & 0 \\ 0 & 0 & 0 & x_1 & 0 & 0 \\ 0 & 0 & 0 & 0 & x_3 & x_4 \\ 0 & 0 & 0 & 0 & 0 & x_3 \end{bmatrix},$$

$$Y = Q^{-1}A_2'Q = \begin{bmatrix} y_1 & y_2 & y_3 & 0 & 0 & 0 \\ 0 & y_1 & y_2 & 0 & 0 & 0 \\ 0 & 0 & y_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & y_4 & y_5 & 0 \\ 0 & 0 & 0 & 0 & y_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & y_4 \end{bmatrix},$$

where x_i, y_j are variables to be decided.

If we look at the equation in (1) block by block according to the size of J_{λ_s}'s and J_{χ_t}'s, then we have

$$X_sR_{st}Y_t = T_{st}\,, 1 \le s \le k, 1 \le t \le l\,, \tag{2}$$

where R_{st}, T_{st} are the (s,t)th partitioned block of R and T. Note that X_s and Y_t are block regular upper triangular matrices of certain type.

Now, let us look at just one equation in (2), say the case $(s,t) = (1,1)$, and let J_{λ_1} and J_{χ_1} be of type $(\mu_1, \ldots, \mu_\alpha)$ and $(\nu_1, \ldots, \nu_\beta)$. Then we may write the equation $X_1R_{11}Y_1 = T_{11}$ as the system of equations

$$X_{\mu_s}R_{\mu_s\nu_t}Y_{\nu_t} = T_{\mu_s\nu_t},\ 1 \le s \le \alpha,\ 1 \le t \le \beta\ , \text{ where} \tag{3}$$

$$X_{\mu_s} = \begin{bmatrix} x_1 & x_2 & x_3 & \cdots & x_{\mu_s} \\ 0 & x_1 & x_2 & \cdots & x_{\mu_s-1} \\ 0 & 0 & x_1 & \cdots & x_{\mu_s-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & x_1 \end{bmatrix}, Y_{\nu_j} = \begin{bmatrix} y_1 & y_2 & y_3 & \cdots & y_{\nu_t} \\ 0 & y_1 & y_2 & \cdots & y_{\nu_t-1} \\ 0 & 0 & y_1 & \cdots & y_{\nu_t-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & y_1 \end{bmatrix}, \text{ with}$$

x_s, y_t's the variables to be determined, and $R_{\mu_s\nu_t}$, $T_{\mu_s\nu_t}$ are the corresponding submatrices of R_{11} and T_{11} respectively.

4.2. General cases

If the number of generators for each $\mathcal{S}_i$, $i = 1, 2$, is more than one, then unlike the cyclic case, it is not easy to characterize the elements in $\mathcal{S}_i$ as in Lemma 3. Note that $\dim(Z(\mathcal{S}_i))$ need not equal to $\dim(\mathcal{S}_i)$ anymore, and therefore we have to consider more variables than in one generator case. We make an observation on the system: If one of the generators of $\mathcal{S}_i$ has at least two different eigenvalues, then we can do the analysis for each eigenvalue separately, hence we assume that each generator has only one eigenvalue.

Suppose that $\mathcal{S}_1 = \langle G_1, \ldots, G_g \rangle - \{\alpha I_n\}$ and $\mathcal{S}_2 = \langle H_1, \ldots, H_h \rangle - \{\alpha I_n\}$ for $G_i, H_j \in M_n(q)$, where G_i's commute each other and H_j's commute each other. Without loss of generality, we assume that the Jordan canonical form $J(G_1) = P^{-1}G_1P$ is of type $\mu_1, \ldots, \mu_k$ and $J(H_1) = Q^{-1}H_1Q$ is of type $\nu_1, \ldots, \nu_l$. Again, we work on the splitting field of characteristic polynomial of G_1 and H_1 over $\mathbb{F}_q$. Remember that we are assuming that the product A_1A_2 that Alice sends to Bob and B_1B_2 that Bob sends to Alice are intercepted, and we are looking for A_1', A_2'(or B_1', B_2') such that $A_1A_2 = A_1'A_2'$(or $B_1B_2 = B_1'B_2'$). Therefore we may let $X = P^{-1}A_1'P$ be a matrix in $Z(J(G_1))$ and $Y = Q^{-1}A_2'Q$ be a matrix in $Z(J(H_1))$. Then, the system we have to solve is

(4)
$$\begin{cases} XRY = T, & \text{where } R = P^{-1}Q,\ T = P^{-1}A_1A_2P, \\ X(P^{-1}G_iP) = (P^{-1}G_iP)X & \text{for all } i = 2, \ldots, g, \\ Y(Q^{-1}H_jQ) = (Q^{-1}H_jQ)Y & \text{for all } j = 2, \ldots, h. \end{cases}$$

EXAMPLE 1. *If $J(G_1)$ is of type $(3, 3)$, and $J(H_1)$ is of type $(2, 2, 2)$, then we may let*

$$X = \begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{21} & x_{22} & x_{23} \\ 0 & x_{11} & x_{12} & 0 & x_{21} & x_{22} \\ 0 & 0 & x_{11} & 0 & 0 & x_{21} \\ x_{31} & x_{32} & x_{33} & x_{41} & x_{42} & x_{43} \\ 0 & x_{31} & x_{32} & 0 & x_{41} & x_{42} \\ 0 & 0 & x_{31} & 0 & 0 & x_{41} \end{bmatrix}, Y = \begin{bmatrix} y_{11} & y_{12} & y_{21} & y_{22} & y_{31} & y_{32} \\ 0 & y_{11} & 0 & y_{21} & 0 & y_{31} \\ y_{41} & y_{42} & y_{51} & y_{52} & y_{61} & y_{62} \\ 0 & y_{41} & 0 & y_{51} & 0 & y_{61} \\ y_{71} & y_{72} & y_{81} & y_{82} & y_{91} & y_{92} \\ 0 & y_{71} & 0 & y_{81} & 0 & y_{91} \end{bmatrix},$$

where x_{ij}'s, y_{ij}'s are variables to be decided.

REMARK 4. If there is an evidence that X or Y is nonsingular in (1) or (4), then equations are linear on the entries of X^{-1} and Y (or X and Y^{-1}). Hence we only care about the case that X and Y are both singular.

5. Analysis(cyclic subalgebras)

Note that we are assuming that the equations we derived in section 4 are solvable, and we always can find a solution of the equations by exhaustive search. The main concern, however, is if there is a polynomial time algorithm to find a solution of each equation. In this section, we show that there exists a polynomial time algorithm if $\mathcal{S}_i$'s are cyclic subalgebras of $M_n(q)$, under the assumption that the dimension of $\widetilde{\mathbb{F}}_q$ over $\mathbb{F}_q$ is reasonably small. Through the sections 5 and 6, we use q in the place $q^d = |\widetilde{\mathbb{F}}_q|$ should be, which connote the assumption that Jordan forms and transformation matrices are defined over the field of q elements already.

5.1. Simplest case

As the first step, we consider the simplest case, that is an equation from (3) ;

$$X_\mu R Y_\nu = T, \tag{5}$$

where R and T are given $\mu \times \nu$ matrices and

$$X_\mu = \begin{bmatrix} x_1 & x_2 & x_3 & \cdots & x_\mu \\ 0 & x_1 & x_2 & \cdots & x_{\mu-1} \\ 0 & 0 & x_1 & \cdots & x_{\mu-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & x_1 \end{bmatrix}, Y_\nu = \begin{bmatrix} y_1 & y_2 & y_3 & \cdots & y_\nu \\ 0 & y_1 & y_2 & \cdots & y_{\nu-1} \\ 0 & 0 & y_1 & \cdots & y_{\nu-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & y_1 \end{bmatrix}.$$

DEFINITION 5.

1. For a column vector $\mathbf{a} = [a_1, \ldots, a_\mu]^t$, we let $S(\mathbf{a})$ be the $\mu \times \mu$ matrix defined as follows:
$$(S(\mathbf{a}))_{ij} = \begin{cases} a_{i+j-1} & \text{if } i+j \le \mu+1, \\ 0 & \text{otherwise.} \end{cases}$$
2. Let $\mathcal{R}_i$, $\mathcal{T}_i$ denote the ith column of R and T respectively, and let $\mathcal{R}'_j$, $\mathcal{T}'_j$ denote the jth row of R and T respectively.

For example, if $\mathbf{a} = [1,2,3]^t$, then $S(\mathbf{a}) = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 0 \\ 3 & 0 & 0 \end{bmatrix}$. Note that $\operatorname{rank}(S(\mathbf{a})) = \max\{j \mid a_j \neq 0\}$.

5.2. When $\mathcal{T}_1 \neq 0$(or $\mathcal{T}'_\mu \neq 0$)

If $\mathcal{T}_1 \neq 0$ then $y_1 \neq 0$ and Y_ν is nonsingular.(The case that $\mathcal{T}'_\mu \neq 0$ that is X_μ is nonsingular can be solved by the dual argument, so we only consider the case $\mathcal{T}_1 \neq 0$.) Without loss of generality, we assume that $y_1 = 1$. In this case, since Y_ν is nonsingular, we may write equation (5) as

$$X_\mu R = TY_\nu^{-1}, \tag{6}$$

with $Y_\nu^{-1} = \begin{bmatrix} y'_1 & y'_2 & y'_3 & \cdots & y'_\nu \\ 0 & y'_1 & y'_2 & \cdots & y'_{\nu-1} \\ 0 & 0 & y'_1 & \cdots & y'_{\nu-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & y'_1 \end{bmatrix}$, where $y'_1 = 1$ and y_j are polynomials of $y'_1, ..., y'_j$ of degree $j-1$.

If we write $\mu \times \nu$ equations read off from the equation (6), column by column, then we have

$$\mathcal{M}\mathcal{X} = 0, \tag{7}$$

where

$$\mathcal{M} = \begin{bmatrix} S(\mathcal{R}_1) & -\mathcal{T}_1 & 0 & \cdots & 0 \\ S(\mathcal{R}_2) & -\mathcal{T}_2 & -\mathcal{T}_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ S(\mathcal{R}_\nu) & -\mathcal{T}_\nu & -\mathcal{T}_{\nu-1} & \cdots & -\mathcal{T}_1 \end{bmatrix},$$

and $\mathcal{X} = [x_1, \ldots, x_\mu, y'_1, \ldots, y'_\nu]^t$. Using Gaussian algorithm, we will need $\mathcal{O}((\mu + \nu^2)\mu\nu)$ many multiplications to solve (7). Then, $\mathcal{O}(\nu^2)$ many multiplications to find y_j's will be needed.

5.3. When $\mathcal{T}_1 = 0$ and $\mathcal{T}'_\mu = 0$

When $\mathcal{T}_1 = 0$ and $\mathcal{T}'_\mu = 0$, we define two constants a, b from T as follows:

If $T = 0$, then $a = \mu$ and $b = \nu$.

If $T \neq 0$, then let $a < \mu$ and $b < \nu$ be nonnegative integers that satisfy the following conditions:

$\mathcal{T}_1 = \cdots = \mathcal{T}_b = 0$ but $\mathcal{T}_{b+1} \neq 0$,

$\mathcal{T}'_\mu = \cdots = \mathcal{T}'_{\mu-(a-1)} = 0$ but $\mathcal{T}'_{\mu-a} \neq 0$.

For each $0 \leq i \leq \mu$, let f_i be the function from the set of $\mu \times \nu$ matrices to itself moving each row upward i times and filling in the last i rows by 0's.

For each $0 \leq j \leq \nu$, let g_j be the function from the set of $\mu \times \nu$ matrices to itself moving each column rightward j times and filling in the first j columns by 0's. If $(a, b) \neq (\mu, \nu)$, let

$$A = \{(i,j) | \text{ The last } a \text{ rows and the first } b \text{ columns of } g_j f_i(R) \text{ are all zero, but the } (b+1)\text{th column and the } (\mu - a)\text{th row of } g_j f_i(R) \text{ are not zero } \}.$$

When $(a,b) = (\mu,\nu)$, A is just the set of (i,j)'s such that $g_j f_i(R) = T = 0$.

The following lemma is immediate from the definition.

LEMMA 6. *When $T = 0$, A satisfies the following properties:*

1. *A is nonempty.*
2. *For $(i,j) \in A$, if $i \le i'$, $j \le j'$ and $i + j < i' + j'$ then $(i',j') \in A$.*

We say that a solution of the equation (5) is of *type* (i,j) if $x_1 = \cdots = x_i = 0$, $y_1 = \cdots = y_j = 0$, but $x_{i+1} \neq 0$ and $y_{j+1} \neq 0$. Then, we have the following lemma.

LEMMA 7. *A solution of the equation* (5) *is of type (i,j) for some $(i,j) \in A$.*

Proof. If $T = 0$ that is $(a,b) = (\mu,\nu)$, there is nothing to prove. Hence we assume that $T \neq 0$. Let a solution of the system (5) be of type (I,J) but $(I,J) \notin A$. Consider $g_J f_I(R)$. Since $(I,J) \notin A$, there are two cases to be considered. The first case is that either the $(b+1)$th column or the $(\mu - a)$th row of $g_J f_I(R)$ is zero. In this case, either the $(b+1)$th column or the $(\mu - a)$th row of XRY is 0, but none of the $(b+1)$th column and the $(\mu - a)$th row of T is 0. Hence this case can not occur. The second case is that either the last a rows or the first b columns of $g_J f_I(R)$ are not all zero. Assume that the first nonzero column of $g_J f_I(R)$ is the j'th column and the first nonzero entry, say ζ, of that column is in the i' th row of $g_J f_I(R)$, then $j' \le b$. It is clear that the (i',j')-entry of XRY is $x_{I+1}\zeta y_{J+1}$ which is nonzero. Since $j' \le b$ we have a contradiction. We also get a contradiction if we assume that there is a nonzero row in the last a rows of $g_J f_I(R)$. This completes the proof. □

LEMMA 8. *When $T \neq 0$, A satisfies the following properties:*

1. *A is nonempty.*
2. *If $(i,j) \in A$, then $0 \le i \le a$ and $0 \le j \le b$.*
3. *For $(i,j) \in A$,if $i' \le i$, $j' \le j$ and $i' + j' < i + j$ then $(i',j') \notin A$.*
4. *$|A| \le \min\{a,b\} + 1 \le \min\{\mu,\nu\}$.*

Proof. Nonemptiness of A follows from Lemma 7, since we are assuming that the equation (5) has a solution. If $j > b$ then the $(b+1)$th

column of $g_i f_j(R)$ is zero, and if $i > a$ then the $(\mu - a)$th row of $g_i f_j(R)$ is zero. Hence, the second property must be satisfied. If $(i,j) \neq (i',j')$, $i' \leq i$, $j' \leq j$ and $(i,j),(i',j') \in A$, then either $(b+1)$th column or the $(\mu - a)$th row of $g_i f_j(R)$ is zero, which proves the third property. The fourth property is immediate from the second and the third properties. □

If $x_1 = \cdots = x_i = 0$ and $y_1 = \cdots = y_j = 0$ in equation (5), then we may rewrite the equation as $X'_\mu R' Y'_\nu = T'$, where R' is the lower left $(\mu - i) \times (\nu - j)$ submatrix of R, T' is the upper right $(\mu - i) \times (\nu - j)$ submatrix of T and

$$X'_\mu = \begin{bmatrix} x_{i+1} & x_{i+2} & \cdots & x_\mu \\ 0 & x_{i+1} & \cdots & x_{\mu-1} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & x_{i+1} \end{bmatrix}, Y'_\nu = \begin{bmatrix} y_{j+1} & y_{j+2} & \cdots & y_\nu \\ 0 & y_{j+1} & \cdots & y_{\nu-1} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & y_{j+1} \end{bmatrix}.$$

Note that, if $T = 0$ then $x_1 = \cdots = x_i = 0$, $y_1 = \cdots = y_j = 0$ with other variables arbitrary, for any $(i,j) \in A$, will be a solution of (5). Hence, in the next Algorithm, we only care about the case $T \neq 0$. Because of Lemma 7, when $T \neq 0$, we may write the procedure to solve (5) as follows;

Algorithm 1 (When $T \neq 0$)
For each $(i,j) \in A$ do

1. Let $x_1 = \cdots = x_i = 0$, $y_1 = \cdots = y_j = 0$ and $y_{j+1} = 1$.
2. If $X'_\mu R' = T'(Y')^{-1}_\nu$ is a consistent linear system, solve for x_i's and y'_j's. Then, calculate y_j's.

Enddo
End of Algorithm 1

In the above Algorithm, at most $\mu\nu$ many linear equations of at most $(\mu + \nu)$ variables are solved at most $|A| \leq \min\{\mu, \nu\}$ many times. Therefore, we have the following theorem.

THEOREM 9. *Following the Algorithm 1, we can solve the equation* (5) *with* $\mathcal{O}(\chi^5 (\log_2 q)^2)$ *many bit operations, where* $\chi = \max\{\mu, \nu\}$.

Moreover, we can count the number of solutions of $X'_\mu R' = T'(Y')^{-1}_\nu$ for each $(i,j) \in A$ if it is consistent:

THEOREM 10. *For a given element* $(i,j) \in A$, *suppose that the corresponding system of linear equations* $X'_\mu R' = T'(Y')^{-1}_\nu$ *is consistent. Then, there are* $q^{a-i} q^{b-j}$ *many solutions of the equation* (5) *after we fix the value* y_{j+1} *as* 1.

Proof. By the definition of A, if $(i,j) \in A$ then $i \le a$, $j \le b$, and $\mu - a \le \mu - i$, $\nu - b \le \nu - j$. Moreover, the $(\mu - a)$th row of R' is nonzero and the $(\nu - b)$th column from the right of R' is nonzero, whereas the last $(a-i)$ rows and the first $(j-b)$ columns of R' are all zero. Also, the same is true for the matrix T'. In this situation, the last $(a-i)$ many x variables and the last $(b-j)$ many y variables may be arbitrary values. If we write the equation $X'_\mu R' = T'(Y')^{-1}_\nu$ in the form of (7), then since at least one $S(\mathcal{R}'_c)$ is of rank $\mu - a$ and the $(\nu - b)$th column from the right of T' is nonzero we have at least $(\mu - a) + (\nu - b) - 1$ many linearly independent equations in $(\mu - a) + (\nu - b) - 1$ many variables by fixing the value of y_{j+1} as 1. Hence if the system of linear equations is consistent then there exists only one solution for the remaining variables $x_{i+1}, ..., x_{\mu+i-a}, y_{j+2}, ..., y_{\nu+j-b}$. □

Example 2. Suppose that $\mu = \nu = 5$ and

$$R = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 & 2 \\ 0 & 3 & 3 & 3 & 3 \\ 0 & 0 & 0 & 4 & 4 \\ 0 & 0 & 0 & 5 & 5 \end{bmatrix}, \; T = \begin{bmatrix} 0 & 0 & 0 & 8 & 24 \\ 0 & 0 & 0 & 3 & 9 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

over the field $\mathbb{F}_{31}$, then $(a,b) = (3,3)$ and $A = \{(1,2),(3,0)\}$.

When $(i,j) = (1,2)$, $X'_\mu = \begin{bmatrix} x_2 & x_3 & x_4 & x_5 \\ 0 & x_2 & x_3 & x_4 \\ 0 & 0 & x_2 & x_3 \\ 0 & 0 & 0 & x_2 \end{bmatrix}$, $Y'_\nu = \begin{bmatrix} 1 & y_4 & y_5 \\ 0 & 1 & y_4 \\ 0 & 0 & 1 \end{bmatrix}$ and $R' = \begin{bmatrix} 0 & 2 & 2 \\ 0 & 3 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $T' = \begin{bmatrix} 0 & 8 & 24 \\ 0 & 3 & 9 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$. If we write the equation $X'_\mu R' = T'(Y')^{-1}_\nu$ in the form of (7), then we have $\mathcal{M}[x_2\, x_3\, x_4\, x_5\, y'_3\, y'_4\, y'_5]^t = 0$, where

$$\mathcal{M} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 3 & 0 & 0 & -8 & 0 & 0 \\ 3 & 0 & 0 & 0 & -3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 3 & 0 & 0 & -24 & -8 & 0 \\ 3 & 0 & 0 & 0 & -9 & -3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Therefore, x_4, x_5, y'_5(hence y_5) can be arbitrary values and x_2, x_3, y'_4 are uniquely determined if the system is consistent.

5.4. System (3)

For more general cases given by the system (3), since the system consists of several equations of type (5), we basically can follow Algorithm 1 to solve each system, while we have to consider subsystems simultaneously. Recall that the system (3) is defined as follows:

$$X_{\mu_s} R_{\mu_s\nu_t} Y_{\nu_t} = T_{\mu_s\nu_t},\ 1 \le s \le \alpha,\ 1 \le t \le \beta\ ,\ \text{where}$$

$$X_{\mu_s} = \begin{bmatrix} x_1 & x_2 & x_3 & \cdots & x_{\mu_s} \\ 0 & x_1 & x_2 & \cdots & x_{\mu_s-1} \\ 0 & 0 & x_1 & \cdots & x_{\mu_s-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & x_1 \end{bmatrix},\ Y_{\nu_j} = \begin{bmatrix} y_1 & y_2 & y_3 & \cdots & y_{\nu_t} \\ 0 & y_1 & y_2 & \cdots & y_{\nu_t-1} \\ 0 & 0 & y_1 & \cdots & y_{\nu_t-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & y_1 \end{bmatrix},\ \text{with}$$

x_s, y_t's the variables to be determined, and $R_{\mu_s\nu_t}$, $T_{\mu_s\nu_t}$ are the corresponding submatrices of R_{11} and T_{11} respectively. Also, recall that we assumed that $\mu_1 \ge \mu_2 \ge \cdots \ge \mu_\alpha$ and $\nu_1 \ge \nu_2 \ge \cdots \ge \nu_\beta$. We let $\mu = \mu_1$, $\nu = \nu_1$. For each s and t, $X_{\mu_s} R_{\mu_s\nu_t} Y_{\nu_t} = T_{\mu_s\nu_t}$ is just an equation of type (5). Hence we can define the set A for each case indexed by s, t, as we did in the previous subsection, and let them A_{st}. When $T_{\mu_s\nu_t} = 0$, we let A_{st} be extended to a subset of $\{1, 2, \ldots, \mu\} \times \{1, 2, \ldots, \nu\}$ from a subset of $\{1, 2, \ldots, \mu_s\} \times \{1, 2, \ldots, \nu_t\}$. Take the intersection of all A_{st}'s and let us call it *A of the system (3)*. Note again that A is nonempty.

If $T_{\mu_s\nu_t} = 0$ for every s and t, then the corresponding solution of any element of A will be a solution of (3). If $T_{\mu_s\nu_t} \ne 0$ for some s and t, then $|A| \le \min\{\mu, \nu\}$. For each $(i, j) \in A$, if we let $x_1 = \cdots = x_i = 0$, $y_1 = \cdots = y_j = 0$ and $y_{j+1} = 1$, then for each (s, t), we obtain a system of linear equations of $x_{i+1}, ..., x_{\mu_s}$ and $y_{j+2}, ..., y_{\nu_t}$. Consider all of these equations together as a system of linear equations with variables $x_{i+1}, ..., x_\mu$, $y_{j+2}, ..., y_\nu$. If it is consistent, then solve for the variables, otherwise try another element of A. If we use Gaussian algorithm, we have the following theorem.

THEOREM 11. *We can solve system* (3) *with* $\mathcal{O}(\eta^3(\sum_{i=1}^{\alpha} \mu_i)(\sum_{j=1}^{\beta} \nu_j)(\log_2 q)^2)$ *many bit operations, where* $\eta = \max\{\mu, \nu\}$.

5.5. System (2)

Recall that the system (2) is given as follows:

$$X_s R_{st} Y_t = T_{st}\,, 1 \le s \le k, 1 \le t \le l\,,$$

where each equation indexed by (s, t) is an equation of type (3). Note that X_s and Y_t are block regular upper triangular matrices of corresponding type. For each Y_t, solve $X_s R_{st} Y_t = T_{st}$, $1 \le s \le k$, to have

solutions $(X_1, X_2, \ldots, X_k)_t$ corresponding to Y_t (so that the first nonzero y variable is 1). There are at most $|Y_t|$ many types of solution (spaces) $(X_1, X_2, \ldots, X_k)_t$, depending on the type of the solution Y_t, where Y_t is a $|Y_t| \times |Y_t|$ matrix. Now, we find an intersection of $(X_1, X_2, \ldots, X_k)_t$'s where t varies. There are $\prod |Y_t|$ many such intersections to be considered and any constant multiple of $(X_1, X_2, \ldots, X_k)_t$, $t \neq 0$, should be considered since the first nonzero of y-variables for each Y_t was fixed as 1.

Now, we may collect all the work needed, and conclude as follows, which is the final conclusion about the cyclic subalgebra case. Note that n is the dimension of matrices X, R, Y, and T, given in the equation (1), which is equivalent to (2).

THEOREM 12. *We can solve the system* (2) *with* $\mathcal{O}(n^5(\log_2 q)^2)$ *many bit operations.*

6. Analysis(General cases)

In this section, we consider a special case of the most general case given as system (4) of equations. Unlike the cyclic subalgebra case, it is not easy to find an (polynomial time) algorithm for general cases. We only consider a special case and exhibit a way to write the system (4) as a system of linear equations of variables $x_i y_j$'s. Then, we suggest a method to solve (4), without explicit calculation of the complexity, which seems to be impossible to do in general case.

Recall that the system (4) is given by

$$\begin{cases} XRY = T & \text{where } R = P^{-1}Q,\ T = P^{-1}A_1A_2P, \\ X(P^{-1}G_iP) = (P^{-1}G_iP)X & \text{for all } i = 2, \ldots, g, \\ Y(Q^{-1}H_jQ) = (Q^{-1}H_jQ)Y & \text{for all } j = 2, \ldots, h, \end{cases}$$

where $\mathcal{S}_1 = \langle G_1, \ldots, G_g \rangle - \{\alpha I_n\}$ and $\mathcal{S}_2 = \langle H_1, \ldots, H_h \rangle - \{\alpha I_n\}$. In the following we state some assumptions we make on the system.

1. The number of generators of the system $\mathcal{S}_i$ is restricted to small numbers. It is because that we can not describe the system if there are too many generators.
2. Degrees of minimal polynomials of generators of the system are not so small compared to n. If all the degrees of minimal polynomials are less than d, for some fixed d, then we can do the exhaustive search with a generator set(or basis) of the system.

3. If one of the generators of $\mathcal{S}_i$ has at least two different eigenvalues, then we can do the analysis for each eigenvalue separately, hence we assume that each generator has only one eigenvalue.
4. Let $J(G_1) = J_\lambda(\mu_1, \mu_2, \cdots, \mu_k)$ and $J(H_1) = J_\chi(\nu_1, \nu_2, \cdots, \nu_l)$. We assume that $\mu_1 = \mu_2 = \cdots = \mu_k$, $\nu_1 = \nu_2 = \cdots = \nu_l$ and k and l are relatively small compared to n. Moreover we assume that $k \leq l$ hence $\mu_i \geq \nu_j$.
5. As we mentioned earlier, if either X or Y is nonsingular, then it is easy to solve the system (4). Therefore, we assume that X and Y are singular matrices.

Note that $P^{-1}G_iP \in Z(J(G_1))$ and $Q^{-1}H_jQ \in Z(J(H_1))$, hence $P^{-1}G_iP$ and $Q^{-1}H_jQ$ are block matrices with regular upper triangular blocks of size $\mu_1 \times \mu_1$ and $\nu_1 \times \nu_1$ respectively. Note that $k\mu_1 = l\nu_1 = n$, and there are $k^2\mu_1 = kn$ many variables in X and $l^2\nu_1 = ln$ many variables in Y. We will give indices to the variables in X and Y as in Example 1.

For a column vector $\mathbf{a} = [a_1, \ldots, a_n]^t$, and a partition $(\mu_1, \mu_2, \ldots, \mu_k)$, $\mu_i = \frac{n}{k}$, of n, we divide $\mathbf{a}$ into a block matrix with each block size μ_i. Let $\mathbf{a}_i$ be the ith block of $\mathbf{a}$. Then we let $S_\mu(\mathbf{a})$ be the $\mu_1 \times n$ matrix defined as

$$S_\mu(\mathbf{a}) = \begin{bmatrix} S(\mathbf{a}_1) & \cdots & S(\mathbf{a}_k) \end{bmatrix},$$

and $D_\mu(\mathbf{a})$ be the $\frac{n}{\mu_1} \times \frac{n}{\mu_1}$ block diagonal matrix with diagonal blocks $S_\mu(\mathbf{a})$. Then $D_\mu(\mathbf{a})$ is an $n \times (nk)$ matrix.

In the following, we rewrite the first equation in (4) in a matrix form. Remember that $\mathcal{R}_i$ denote the ith column of R. For each $c = 1, \ldots, l$, we let B_c be the matrix given as follows

$$\begin{bmatrix} D_\mu(\mathcal{R}_{(c-1)\nu+1}) & 0 & 0 & \cdots & 0 \\ D_\mu(\mathcal{R}_{(c-1)\nu+2}) & D_\mu(\mathcal{R}_{(c-1)\nu+1}) & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ D_\mu(\mathcal{R}_{(c-1)\nu+\nu-1}) & D_\mu(\mathcal{R}_{(c-1)\nu+\nu-2}) & \cdots & D_\mu(\mathcal{R}_{(c-1)\nu+1}) & 0 \\ D_\mu(\mathcal{R}_{(c-1)\nu+\nu}) & D_\mu(\mathcal{R}_{(c-1)\nu+\nu-1}) & \cdots & D_\mu(\mathcal{R}_{(c-1)\nu+2}) & D_\mu(\mathcal{R}_{(c-1)\nu+1}) \end{bmatrix}$$

and $\mathcal{M}_c$ be a $l \times l$ block diagonal matrix with diagonal blocks B_c.

Now let

$$\mathcal{M} = \begin{bmatrix} \mathcal{M}_1 & \cdots & \mathcal{M}_l \end{bmatrix}, \mathcal{X} = var(Y) \otimes var(X),$$

where $var(Y)$($var(X)$, respectively) is a column vector having y_{ij}(x_{ij}, respectively) as its entries in order. We also let

$\mathcal{T} = [T_{11}, T_{21}, \ldots, T_{n1}, T_{12}, \ldots, T_{n2}, \ldots, T_{1n}, \ldots, T_{nn}]^t$. Then, finally, we can rewrite the first equation in (4):

$$\mathcal{M}\mathcal{X} = \mathcal{T}. \tag{8}$$

EXAMPLE 3. As in Example 1, suppose that $J(G_1)$ is of type $\mu = (3,3)$, and $J(H_1)$ is of type $\nu = (2,2,2)$, then $k = 2$, $l = 3$. If the first column $\mathcal{R}_1$ of R is given by $[2,5,12,15,3,7]^t$ then

$$S_\mu(\mathcal{R}_1) = \begin{bmatrix} 2 & 5 & 12 & 15 & 3 & 7 \\ 5 & 12 & 0 & 3 & 7 & 0 \\ 12 & 0 & 0 & 7 & 0 & 0 \end{bmatrix}, \; D_\mu(\mathcal{R}_1) = \begin{bmatrix} S_\mu(\mathcal{R}_1) & 0 \\ 0 & S_\mu(\mathcal{R}_1) \end{bmatrix},$$

$$B_1 = \begin{bmatrix} D_\mu(\mathcal{R}_1) & 0 \\ D_\mu(\mathcal{R}_2) & D_\mu(\mathcal{R}_1) \end{bmatrix}, \; \mathcal{M}_1 = \begin{bmatrix} B_1 & 0 & 0 \\ 0 & B_1 & 0 \\ 0 & 0 & B_1 \end{bmatrix}.$$

Moreover, $6^2 \times (18 \cdot 12)$ matrix $\mathcal{M} = [\mathcal{M}_1\, \mathcal{M}_2\, \mathcal{M}_3]$ is given as follows:

$$\mathcal{M}_1 = \begin{array}{|cccccc|} \hline y_{11} & y_{12} & y_{21} & y_{22} & y_{31} & y_{32} \\ \hline D_1 & 0 & 0 & 0 & 0 & 0 \\ D_2 & D_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & D_1 & 0 & 0 & 0 \\ 0 & 0 & D_2 & D_1 & 0 & 0 \\ 0 & 0 & 0 & 0 & D_1 & 0 \\ 0 & 0 & 0 & 0 & D_2 & D_1 \\ \hline \end{array}, \; \mathcal{M}_2 = \begin{array}{|cccccc|} \hline y_{41} & y_{42} & y_{51} & y_{52} & y_{61} & y_{62} \\ \hline D_3 & 0 & 0 & 0 & 0 & 0 \\ D_4 & D_3 & 0 & 0 & 0 & 0 \\ 0 & 0 & D_3 & 0 & 0 & 0 \\ 0 & 0 & D_4 & D_3 & 0 & 0 \\ 0 & 0 & 0 & 0 & D_3 & 0 \\ 0 & 0 & 0 & 0 & D_4 & D_3 \\ \hline \end{array}$$

$$\mathcal{M}_3 = \begin{array}{|cccccc|} \hline y_{71} & y_{72} & y_{81} & y_{82} & y_{91} & y_{92} \\ \hline D_5 & 0 & 0 & 0 & 0 & 0 \\ D_6 & D_5 & 0 & 0 & 0 & 0 \\ 0 & 0 & D_5 & 0 & 0 & 0 \\ 0 & 0 & D_6 & D_5 & 0 & 0 \\ 0 & 0 & 0 & 0 & D_5 & 0 \\ 0 & 0 & 0 & 0 & D_6 & D_5 \\ \hline \end{array},$$

where $D_i = D_\mu(\mathcal{R}_i)$ and each y_{ij} represents $y_{ij}(var(X))$, a vector of length 12. Note that each $D_\mu(\mathcal{R}_i)$ is a 6×12 matrix.

When $\mathcal{S}_1$ and $\mathcal{S}_2$ are cyclic, singularity of X and Y are equivalent to $x_1 = 0$ and $y_1 = 0$. However, in the general case, it is more complicated, and it is not possible to use the same method as in Section 5.

LEMMA 13. *Let $Y = (Y_{ij})$, $1 \le i, j \le k$, be a block matrix with*

$$Y_{ij} = \begin{bmatrix} y_{(i-1)k+j,1} & y_{(i-1)k+j,2} & \cdots & y_{(i-1)k+j,\frac{n}{k}} \\ 0 & y_{(i-1)k+j,1} & \cdots & y_{(i-1)k+j,\frac{n}{k}-1} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & y_{(i-1)k+j,1} \end{bmatrix}.$$

Then Y is singular if and only if $Y' = \begin{bmatrix} y_{1,1} & \cdots & y_{k,1} \\ y_{k+1,1} & \cdots & y_{2k,1} \\ \vdots & \cdots & \vdots \\ y_{(k-1)k+1,1} & \cdots & y_{k^2,1} \end{bmatrix}$ is singular.

Proof. This is immediate from the shape of each block of Y. □

Therefore, we first may fix the values for Y' so that Y' is singular and then try to solve the system. Following is a well-known theorem which gives the number of possible Y' (see [10]).

PROPOSITION 14. *The number of $k \times k$ matrices in $M_k(q)$ of rank r is*

$$q^{\binom{r}{2}} \prod_{i=1}^{r} \frac{(q^{k-i+1}-1)^2}{(q^i-1)}\,.$$

Proposition 14 tells us that there are $\sum_{r=0}^{k-1} \left(q^{\binom{r}{2}} \prod_{i=1}^{r} \frac{(q^{k-i+1}-1)^2}{(q^i-1)} \right)$ many choices for Y' to be singular, which is a polynomial in q of degree $\frac{k(k-1)(4k+1)}{6}$. Note that k is a small integer by our assumption, so it is plausible to make arbitrary choice for Y'.

Now our suggestion is to solve for the x variables first with preassumed values of Y':

By assuming the values for Y', we will have $l \times n$ many linear equations of x_{ij}'s from (8), moreover the second part of system (4) gives more linear equations of x_{ij}'s. Since there are $k \times n$ manyx_{ij}'s and we assume that $k \leq l$, we can expect that x_{ij}'s will be uniquely determined. If the solution is not uniquely determined then we may choose arbitrary values for free variables.

Then use values of x_{ij}'s to solve for y_{ij}'s using equations in (8) and the third part of the system (4). If we obtain inconsistent system of linear equations then try another value for free x variables. Then try another value of Y'.

The method we suggest must have exponential time complexity in worst case, but it should work quite well for many cases, we believe.

Of course, the number of linearly independent equations(hence the number of free x variables) depends on the shape of R and the rank of Y'. It was not possible for us to estimate the number of free variables, which will be the most important affecting factor on the time complexity.

7. Efficiency issues and concluding remarks

The security of Diffie-Hellman key exchange protocol relies on the difficulty of the discrete logarithm problem on the multiplicative group $\mathbb{F}_q^*$, where $\mathbb{F}_q$ is the Galois field of order q. In Diffie-Hellman key exchange, the bit operation complexity of computing the shared key is $O((\log q)^3)$ which is quite expensive for for some special instances.

For now, we do not have any evidence that the protocol using matrix algebras is secure in terms of relative difficulty to a well known hard problem, and do not have any proof that the protocol is breakable in general case in polynomial time either. Even though we do not have

full analysis of our protocol, in the following, we try to compare the key computation complexity and the key size of Diffie-Hellman protocol and the protocol using matrix algebras.

In Diffie-Hellman key exchange, keys are elements of $\mathbb{F}_q^*$, the bit operation complexity of computing the shared key is $O((\log_2 q)^3)$, and at present, the breaking time complexity is known to be

$$O(e^{(c+o(1))(\log_2 q)^{1/2}(\log_2 \log_2 q)^{1/2}}),$$

where c is a positive constant [18]. In our case, the keys are $n \times n$ matrices with entries in $\mathbb{F}_q$, and the shared key is computed by multiplying three such matrices. Thus the key size is $n^2 \log q$ and the key computation complexity is $O(n^3(\log_2 q)^2)$, and the exhaustive search complexity is $O(n^3(\log_2 q)^2 q^d)$ for some integer d with $2 \leq d \leq n^2/2$, if we make an assumption that one knows bases of commutative algebras. One may notice that, unlike Diffie-Hellman protocol, there are two parameters n and q which control the important features of our protocol. In Diffie-Hellman protocol, q is usually taken to be a prime power of about 1024-bit. With this, we may obtain the conditions for n and q in our protocol so that our protocol has advantages on the key computation time and the key size over Diffie-Hellman type, while 2^{80}-breaking time complexity is guaranteed with respect to the exhaustive search. If we let $q = 2^x$ and $d = 2n$, then we obtain the following conditions:

$$n^3 x^2 \geq 2^{80-2nx}, \tag{9}$$

$$n^2 x \leq 2^{10}. \tag{10}$$

For example, if $q = 2^8$ and $n = 8$, then above conditions are satisfied and the key computation time is about $1/2^{15}$ of the computation time in Diffie-Hellman protocol, whereas the key size is about $1/2$ of the key size of Diffie-Hellman type. Moreover, if one wants to use $n = 10$, then q can be a number between 2^4 and 2^{10}. If a more efficient attack other than the exhaustive search is developed, the condition (9) must be replaced with a more restrictive one; and if the conditions were too restrictive to have solutions, then our protocol would lose the advantages over Diffie-Hellman type.

Remark 15.

1. Remember that we need Jordan forms and transformation matrices of the generators of $\mathcal{S}_i$ to set up problems in Section 4. In general, it is costly to find Jordan forms and transformation matrices; due to [17], the worst case complexity is $O(n^{12} + n^9 \log(q)^3)$,

where the given matrix is in $M_n(q)$. Moreover, we need to extend the base field to to the splitting field of characteristic polynomials of generators so that the Jordan forms and transformation matrices can be dealt with. Hence, our q in the analysis should be power of q, which can be large enough to make our algorithm an exponential one, depending on the given matrices. However, without Jordan forms, it does not look possible to do systematic analysis. In conclusion, the (polynomial time) algorithm we develop can be applied only for very restricted cases.

2. It is known that the dimension of a commutative subalgebra of $M_n(q)$ generated by two matrices is at most n, while there is no known fact on the dimension of commutative subalgebra generated by more than two matrices (see [1, 13, 15]). It might also be possible to find a polynomial time algorithm to solve system (4), when $\mathcal{S}_1$ and $\mathcal{S}_2$ are generated by one or two matrices.
3. We considered a key exchange protocol using matrix algebras and its analysis in this article, yet there is no satisfactory analysis in the sense that we made very strong assumption about Jordan forms. The verification of the usefulness of the protocol is open. We believe that to find effective algorithms and calculation of its complexity to solve problems described in section 4 is itself an interesting work.

References

[1] J. Barria and P. R. Halmos, *Vector bases for two commuting matrices*, Linear Multilinear Algebra **27** (1990), 147–157.

[2] J. A. Buchmann, R. Scheidler, and H. C. Williams, *A key-exchange protocol using real quadratic fields*, J. Cryptology **7** (1994), 171–199.

[3] M. A. Cherepnev, *Schemes of public distribution of keys based on a noncommutative group*, Discrete Math. Appl. **13** (2003), no. 3, 265–269.

[4] M. A. Cherepnev, V. M. Sidelnikov, and V. V. Yashchenko, *Systems of open distribution of keys on the basis of noncommutative semigroups*, Russian Acad. Sci. Dokl. Math. **48** (1994), no. 2, 384–386.

[5] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Trans. Inform Theory **22** (1976), 644–654.

[6] J.-C. Faugére, *A new efficient algorithm for computing gröbner bases (F_4)*, J. Pure Appl. Algebra **139** (1999), 61–88.

[7] ———, *A new efficient algorithm for computing gröbner bases without reduction to zero (F_5)*, In Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation.

[8] F. Gantmacher, *The Theory of Matrices Vol. 1*, A.M.S. Chelsea publishing, 1977.

[9] J. A. Green, *The character of finite general linear groups*, Trans. Amer. Math. Soc. **80** (1955), 402–447.
[10] J. H. Hodges, *A bilinear matrix equations over a finite field*, Duke Math. J. **31** (1964), 661–666.
[11] ———, *Representation by bilinear forms in a finite field*, Duke Math. J. **22** (1955), 497–510.
[12] N. Jacobson, *Schur's theormes on commutative matrices*, Bull. Amer. Math. Soc. **50** (1944), 431–436.
[13] T. Laffey and S. Lazarus, *Two-generated commutative matrix subalgebras*, Linear Algebra Appl. **147** (1991), 249–273.
[14] S. M. Mollevi, C. Pardo, I. Gracia, and P. Morillo, *Linear key predistribution schemes*, Des. Codes Cryptogr. **25** (2002), 281–298.
[15] M. Neubauer and D. Saltman, *Two-generated commutative subalgebras of* $M_n(f)$, J. Algebra **164** (1994), 545–562.
[16] M. Qu, J. Solinas, L. Law, A. Menezes, and S. Vanstone, *An efficient protocol for authenticated key agreement*, Des. Codes Cryptogr. **28** (2003), no. 2, 119–134.
[17] N. Strauss, *Algorithm and implementation for computation of Jordan form over* $A[x_1, \cdots, x_m]$, In Computers and mathematics, Springer, 1989, 21–26.
[18] P. C. van Oorschot, A. J. Menezes, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.
[19] V. Varadharajan, R. W. K. Odoni, and P. W. Sanders, *Public key distribution in matrix rings*, Electronic Letters, **20** (1974), no. 9, 386–387.
[20] Hongzeng Wei and Xingfen Zheng, *The number of solutions to the bilinear matrix equation over a finite field*, J. Statist. Plann. Inference **94** (2001), 359–369.
[21] Wan Zhe-xian and Li Gen-dao, *The two theorems of Schur on commutative matrices*, Chinese Math. **5** (1964), 156–164.

Soojin Cho
Department of Mathematics
Ajou University
Suwon 443-749, Korea
E-mail: chosj@ajou.ac.kr

Young-One Kim
Department of Mathematics
Seoul National University
Seoul 151-747, Korea
E-mail: kimyo@math.snu.ac.kr

View publication stats

Kil-Chan Ha and Dongho Moon
Department of Applied Mathematics
Sejong University
Seoul 143-747, Korea
E-mail: kcha@sejong.ac.kr
dhmoon@sejong.ac.kr