# A Note on Two Schemes for Secure Outsourcing of Linear Programming

Zhengjun Cao[1], Lihua Liu[2]

(Corresponding author: Lihua Liu)

Department of Mathematics, Shanghai University[1]

No.99, Shangda Road, Shanghai, China.

Department of Mathematics, Shanghai Maritime University[2]

No. 1550, Haigang Ave, Pudong New District, Shanghai, China.

(Email: liulh@shmtu.edu.cn)

(Received Jan. 26, 2016; revised and accepted Apr. 23 & May 31, 2016)

## Abstract

Recently, Wang et al. [IEEE INFOCOM 2011, 820-828], and Nie et al. [IEEE AINA 2014, 591-596] have proposed two schemes for secure outsourcing of linear programming (LP). They did not consider the standard form: minimize $\mathbf{c}^T\mathbf{x}$, subject to $\mathbf{A}\mathbf{x} = \mathbf{b}, \mathbf{x} \geq 0$. Instead, they studied a peculiar form: minimize $\mathbf{c}^T\mathbf{x}$, subject to $\mathbf{A}\mathbf{x} = \mathbf{b}, \mathbf{B}\mathbf{x} \geq 0$, where $\mathbf{B}$ is a non-singular matrix. In this note, we stress that the proposed peculiar form is unsolvable and meaningless. The two schemes have confused the *functional inequality constraints* $\mathbf{B}\mathbf{x} \geq 0$ with the *nonnegativity constraints* $\mathbf{x} \geq 0$ in the linear programming model. But the condition $\mathbf{x} \geq 0$ is indispensable to LP. Thus, both two schemes failed.

*Keywords: Cloud computing, functional inequality constraints, linear programming, nonnegativity constraints, simplex method.*

## 1 Introduction

Cloud computing makes use of the massive resources of computing and storage systems via the Internet to efficiently deal with information processing. It supports a paradigm shift from local to network-centric computing and network-centric content [10, 17], and benefits scientific and engineering applications, such as data mining, computational financing, and many other computational and data-intensive activities [14, 18]. Cloud computing makes it possible to enable customers with limited computational resources to outsource large-scale computational tasks to the cloud, including linear equations (LE), linear programming (LP), matrix multiplication computation, and matrix inversion computation.

In 2011, Dreier and Kerschbaum [4] put forth a method for secure outsourcing of LP. In order to protect the solution $\mathbf{x}$, the Dreier-Kerschbaum scheme uses the affine transformation

$$\mathbf{z} = \mathbf{Q}^{-1}\mathbf{x} + \mathbf{r},$$

where $\mathbf{Q}$ is a positive monomial matrix (a monomial matrix contains exactly one non-zero entry per row and column), and $\mathbf{r}$ is a random vector picked by the client. Wang et al. [15] also presented a scheme for outsourcing of LP based on the transformation $\mathbf{y} = \mathbf{M}^{-1}(\mathbf{x} + \mathbf{r})$, where $\mathbf{M}$ is a random non-singular matrix and $\mathbf{r}$ is a random vector. In 2014, Nie et al. [11] proposed another scheme for outsourcing of LP based on the same transformation as that used in [15].

In 2013, Lei et al. [8] have proposed a scheme for outsourcing matrix inversion computation over the field $\mathbb{R}$ of real numbers. After that, they [7] proposed another scheme for outsourcing matrix multiplication computation over $\mathbb{R}$. But the verifying equations in [7, 8] do not hold over $\mathbb{R}$ because the computational errors, especially rounding errors, are not considered carefully. That means the client cannot check whether the cloud server is cheating him.

Wang et al. [16] have ever proposed a scheme for outsourcing large-scale systems of linear equations to cloud, which enables a client to securely harness the cloud for iteratively finding successive approximations to the LE solution, while keeping both the sensitive input and output of the computation private. Recently, Cao and Liu [1] pointed out that the Wang et al.'s scheme fails because the involved homomorphic encryption system [2, 12] is invalid in the context of the scheme. In 2014, Chen et al. [3] proposed two computation outsourcing schemes for LE and LP. Both two schemes are insecure because the technique of masking a vector with a diagonal matrix is vulnerable to statistical analysis attacks. In 2015, Salinas et al. [13] proposed a scheme for outsourcing LE, which makes use of the conjugate gradient method to solve the equivalent quadratic program in the client-server scenario. Recently, Hsien et al. [6, 9] presented two surveys of public auditing for secure data storage in cloud computing.

In this note we would like to stress that the proposed peculiar form by Wang et al. [15] and Nie et al. [11] is unsolvable and meaningless. In fact, they did not consider the standard form:

$$\text{Minimize } \mathbf{c}^T\mathbf{x}, \text{ subject to } \mathbf{A}\mathbf{x} = \mathbf{b}, \mathbf{x} \geq 0.$$

Instead, they studied a peculiar form:

$$\text{Minimize } \mathbf{c}^T\mathbf{x}, \text{ subject to } \mathbf{A}\mathbf{x} = \mathbf{b}, \mathbf{B}\mathbf{x} \geq 0,$$

where $\mathbf{A}$ is an $m \times n$ matrix, $\mathbf{c}$ is an $n \times 1$ vector, $\mathbf{b}$ is an $m \times 1$ vector, $\mathbf{x}$ is an $n \times 1$ vector of variables, and $\mathbf{B}$ is an $n \times n$ non-singular matrix.

They have confused the *functional inequality constraints* $\mathbf{B}\mathbf{x} \geq 0$ with *nonnegativity constraints* $\mathbf{x} \geq 0$ in the linear programming model. In nature, the condition $\mathbf{x} \geq 0$ is indispensable to LP. Thus, both two schemes failed. We also review the possible method for secure outsourcing of LP, which is due to Dreier and Kerschbaum.

# 2 Preliminaries

Linear programming has numerous important applications. Among these allocating resources to activities is the most common type of application. The *standard form* for a linear programming problem can be described as follows [5]. Select the values for $x_1, \cdots, x_n$ so as to

$$\text{maximize} \quad c_1x_1 + c_2x_2 + \cdots + c_nx_n,$$

subject to the restrictions

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & \leq & b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n & \leq & b_2 \\ & \vdots & \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & \leq & b_m \end{array}$$

and

$$x_1 \geq 0, x_2 \geq 0, \cdots, x_n \geq 0.$$

$c_1x_1 + c_2x_2 + \cdots + c_nx_n$ is called the *objective function*. The first $m$ constraints are sometimes called *functional constraints*. The restrictions $x_j \geq 0$ are called *nonnegativity constraints*.

The simplex method, a general procedure for solving linear programming problems, is based on solving systems of equations. Therefore, it has to firstly convert the functional inequality constraints to *equivalent equality constraints*. This conversion is accomplished by introducing *slack variables*. After the conversion, the original linear programming model can now be replaced by the equivalent model (called the *augmented form*).

Using matrices, the standard form for the general linear programming model becomes

$$\text{maximize } \mathbf{c}^T\mathbf{x}, \text{ subject to } \mathbf{A}\mathbf{x} \leq \mathbf{b}, \mathbf{x} \geq 0$$

where $\mathbf{A}$ is an $m \times n$ matrix, $\mathbf{c}$ is an $n \times 1$ vector, $\mathbf{b}$ is an $m \times 1$ vector, and $\mathbf{x}$ is an $n \times 1$ vector of variables. To obtain the augmented form of the problem, introduce the column vector of slack variables $\mathbf{x}_s = (x_{n+1}, \cdots, x_{n+m})^T$ so that the constraints become

$$[\mathbf{A}, \mathbf{I}] \begin{bmatrix} \mathbf{x} \\ \mathbf{x}_s \end{bmatrix} = \mathbf{b} \text{ and } \begin{bmatrix} \mathbf{x} \\ \mathbf{x}_s \end{bmatrix} \geq \mathbf{0},$$

where $\mathbf{I}$ is the $m \times m$ identity matrix, and the null vector $\mathbf{0}$ now has $n + m$ elements.

Notice that the nonnegativity constraints are left as inequalities because they are used to determine the *leaving basic variable* according to the *minimum ratio test*.

# 3 Analysis of Two Schemes for Outsourcing of LP

## 3.1 Review

We now take the scheme in [15] as the example to show the incorrectness of the proposed peculiar form (see page 822 of [15] and page 592 of [11]). In the scheme, there are two entities, the client and the cloud server. The client has the original problem

$$\min \mathbf{c}^T\mathbf{x}, \text{ s.t. } \mathbf{A}\mathbf{x} = \mathbf{b}, \ \mathbf{B}\mathbf{x} \geq 0 \tag{1}$$

where $\mathbf{A}$ is an $m \times n$ matrix, $\mathbf{c}$ is an $n \times 1$ vector, $\mathbf{b}$ is an $m \times 1$ vector, $\mathbf{x}$ is an $n \times 1$ vector of variables, $\mathbf{B}$ is an $n \times n$ non-singular matrix.

To ensure the privacy of input and output, the client transforms the original problem into the following problem

$$\min \mathbf{c}'^T\mathbf{y}, \text{ s.t. } \mathbf{A}'\mathbf{y} = \mathbf{b}', \ \mathbf{B}'\mathbf{y} \geq 0 \tag{2}$$

where

$$\begin{cases} \mathbf{A}' = \mathbf{QAM} \\ \mathbf{B}' = (\mathbf{B} - \mathbf{PQA})\mathbf{M} \\ \mathbf{b}' = \mathbf{Q}(\mathbf{b} + \mathbf{Ar}) \\ \mathbf{c}' = \gamma\mathbf{M}^T\mathbf{c} \\ \mathbf{y} = \mathbf{M}^{-1}(\mathbf{x} + \mathbf{r}) \end{cases}$$

satisfying

$$|\mathbf{B}'| \neq 0, \mathbf{P}\mathbf{b}' = \mathbf{B}\mathbf{r}, \mathbf{b} + \mathbf{A}\mathbf{r} \neq 0, \gamma > 0,$$

where $\mathbf{P}$ is an $n \times m$ matrix, $\mathbf{Q}$ is a random $m \times m$ non-singular matrix, $\mathbf{M}$ is a random $n \times n$ non-singular matrix, and $\mathbf{r}$ is an $n \times 1$ vector. The client then sends Problem (2) to the server.

## 3.2 Analysis

Upon receiving Problem (2), the server has to introduce the nonnegativity conditions $\mathbf{y} \geq 0$ into it and solve the following problem

$$\min \mathbf{c}'^T\mathbf{y}, \text{ s.t. } \mathbf{A}'\mathbf{y} = \mathbf{b}', \ \mathbf{B}'\mathbf{y} \geq 0, \ \mathbf{y} \geq 0 \tag{3}$$

This is because the constraints $\mathbf{B}'\mathbf{y} \geq 0$ should be viewed as a part of the functional constraints, not the necessary nonnegativity constraints, unless

$$\mathbf{B}' = (\mathbf{B} - \mathbf{PQA})\mathbf{M}$$

can be rewritten as a diagonal matrix where the entries on the main diagonal are strictly positive (in such case, $\mathbf{B}'\mathbf{y} \geq 0$ implies $\mathbf{y} \geq 0$).

Unfortunately, the solution of the following problem

$$\min \mathbf{c}^T\mathbf{x}, \text{ s.t. } \mathbf{Ax} = \mathbf{b}, \ \mathbf{Bx} \geq 0, \ \mathbf{x} \geq 0 \quad (4)$$

cannot be derived from the solution of Problem (3), because the transformation

$$\mathbf{y} = \mathbf{M}^{-1}(\mathbf{x} + \mathbf{r}), \text{ where } \mathbf{x} \geq 0$$

cannot ensure that $\mathbf{y} \geq 0$.

The authors of [11, 15] have confused the functional inequality constraints $\mathbf{Bx} \geq 0$ with the nonnegativity constraints $\mathbf{x} \geq 0$. In fact, the proposed peculiar form is meaningless and unsolvable, unless $\mathbf{Bx} \geq 0$ can be rewritten as $\mathbf{x} \geq 0$.

# 4 A Possible Method for Secure Outsourcing of LP

In 2011, Dreier and Kerschbaum [4] have already presented a possible method for secure outsourcing of LP. The scheme can be briefly described as follows.

Given the original LP problem

$$\min \mathbf{c}^T\mathbf{x}, \text{ s.t. } \mathbf{M}_1\mathbf{x} = \mathbf{b}_1, \mathbf{M}_2\mathbf{x} \leq \mathbf{b}_2, \mathbf{x} \geq 0,$$

the client uses *a positive monomial matrix* $\boldsymbol{Q}$ (a monomial matrix contains exactly one non-zero entry per row and column) to hide $\mathbf{c}$ and obtains

$$\begin{aligned} & \min \mathbf{c}^T\mathbf{Q}\mathbf{Q}^{-1}\mathbf{x}, \\ \text{s.t.} \quad & \mathbf{M}_1\mathbf{Q}\mathbf{Q}^{-1}\mathbf{x} = \mathbf{b}_1, \\ & \mathbf{M}_2\mathbf{Q}\mathbf{Q}^{-1}\mathbf{x} \leq \mathbf{b}_2, \\ & \mathbf{Q}^{-1}\mathbf{x} \geq 0. \end{aligned}$$

He then uses *a positive vector* $\boldsymbol{r}$ to hide $\mathbf{x}$ and obtains

$$\begin{aligned} & \min \mathbf{c}^T\mathbf{Q}(\mathbf{Q}^{-1}\mathbf{x} + \mathbf{r}), \\ \text{s.t.} \quad & \mathbf{M}_1\mathbf{Q}(\mathbf{Q}^{-1}\mathbf{x} + \mathbf{r}) = \mathbf{b}_1 + \mathbf{M}_1\mathbf{Q}\mathbf{r}, \\ & \mathbf{M}_2\mathbf{Q}(\mathbf{Q}^{-1}\mathbf{x} + \mathbf{r}) \leq \mathbf{b}_2 + \mathbf{M}_2\mathbf{Q}\mathbf{r}, \\ & (\mathbf{Q}^{-1}\mathbf{x} + \mathbf{r}) \geq \mathbf{r}. \end{aligned}$$

Setting $\mathbf{z} = \mathbf{Q}^{-1}\mathbf{x} + \mathbf{r}$ and taking a strictly positive diagonal matrix $\mathbf{S}$ (a diagonal matrix where the entries on the main diagonal are strictly positive), the client obtains

$$\begin{aligned} & \min \mathbf{c}^T\mathbf{Q}\mathbf{z}, \\ \text{s.t.} \quad & \mathbf{M}_1\mathbf{Q}\mathbf{z} = \mathbf{b}_1 + \mathbf{M}_1\mathbf{Q}\mathbf{r}, \\ & \mathbf{M}_2\mathbf{Q}\mathbf{z} \leq \mathbf{b}_2 + \mathbf{M}_2\mathbf{Q}\mathbf{r}, \\ & \mathbf{S}\mathbf{z} \geq \mathbf{S}\mathbf{r}, \\ & \mathbf{z} \geq 0 \text{ (see the above definitions of } \mathbf{Q} \text{ and } \mathbf{r}). \end{aligned}$$

Set $\mathbf{c}'^T = \mathbf{c}^T\mathbf{Q}$ and

$$\mathbf{M}' = \begin{pmatrix} \mathbf{M}_1\mathbf{Q} & 0 \\ \mathbf{M}_2\mathbf{Q} & \mathbf{A} \\ -\mathbf{S} & \end{pmatrix}, \ \mathbf{b}' = \begin{pmatrix} \mathbf{b}_1 + \mathbf{M}_1\mathbf{Q}\mathbf{r} \\ \mathbf{b}_2 + \mathbf{M}_2\mathbf{Q}\mathbf{r} \\ -\mathbf{S}\mathbf{r} \end{pmatrix}$$

where $\mathbf{A}$ is a permutation matrix representing slack-variables. Hence, the client can rewrite the program as follows:

$$\min \mathbf{c}_s'^T\mathbf{z}_s, \text{ s.t. } \mathbf{M}'\mathbf{z}_s = \mathbf{b}', \ \mathbf{z}_s \geq 0,$$

where $\mathbf{c}_s'$ is $\mathbf{c}'$ with added zeros for the slack-variables and $\mathbf{z}_s$ is the variable vector ($\mathbf{z}$ with added slack-variables). To hide the contents of $\mathbf{M}'$ and $\mathbf{b}'$, the client uses a nonsingular matrix $\mathbf{P}$ and with $\widehat{\mathbf{M}} = \mathbf{PM}'$ and $\widehat{\mathbf{b}} = \mathbf{Pb}'$ and obtains

$$\begin{aligned} & \min \mathbf{c}_s'^T\mathbf{z}_s, \\ \text{s.t.} \quad & \widehat{\mathbf{M}}\mathbf{z}_s = \widehat{\mathbf{b}}, \\ & \mathbf{z}_s \geq 0. \end{aligned}$$

Finally, the client outsources the above problem to the cloud server. As

$$\mathbf{z} = \mathbf{Q}^{-1}\mathbf{x} + \mathbf{r},$$

the resulting $\mathbf{x}$ can be obtained from $\mathbf{z}$ by calculating

$$\mathbf{x} = \mathbf{Q}(\mathbf{z} - \mathbf{r}).$$

Notice that in the Dreier-Kerschbaum scheme the nonnegativity constraints $\mathbf{z}_s \geq 0$ has explicitly specified. But it is a pity that the authors [11] did not pay more attentions to the specification although they cited the Dreier-Kerschbaum's work.

The designing art in the scheme can be depicted as follows

$$\mathbf{x} \quad \xrightarrow{\text{affine transformation}} \quad \mathbf{z} = \mathbf{Q}^{-1}\mathbf{x} + \mathbf{r}$$
$$\xrightarrow{\text{adding slack-variables}} \quad \mathbf{z}_s = (\mathbf{z}^T, z_{n+1}, \cdots, z_{n+k})^T.$$

Clearly, the cloud server cannot recover $\mathbf{x}$ from $\mathbf{z}_s$ because $\mathbf{Q}, \mathbf{r}$ are the session keys randomly picked by the client.

# 5 Conclusion

We point out that the procedure for determining the leaving basic variable in the simplex method requires that all variables are subject to nonnegativity. One must draw a clear distinction between the functional inequality constraints and the nonnegativity constraints.

Notice that deriving the augmented form of a standard form for a linear programming problem is very easy. It can be solely done by the client himself even though who is assumed to be of weak computational capability.

## Acknowledgments

This work is supported by the National Natural Science Foundation of China (Project 61303200, 61411146001). The authors gratefully acknowledge the reviewers for their valuable suggestions.

## References

[1] Z. J. Cao and L. H. Liu, "Comment on 'harnessing the cloud for securely outsourcing large-scale systems of linear equations'," *IEEE Transactions on Parallel Distribution Systems*, vol. 27, no. 5, pp. 1551–1552, 2016.

[2] Z. J. Cao and L. H. Liu, "The paillier's cryptosystem and some variants revisited," *International Journal of Network Security*, vol. 19, no. 1, pp. 89–96, 2017.

[3] F. Chen, T. Xiang, and Y. Y. Yang, "Privacy-preserving and verifiable protocols for scientific computation outsourcing to the cloud," *Journal of Parallel Distribution Computing*, vol. 74, pp. 2141–2151, 2014.

[4] J. Dreier and F. Kerschbaum, "Practical privacy-preserving multiparty linear programming based on problem transformation," in *Proceedings of IEEE International Conference on Privacy, Security, Risk, and Trust*, pp. 916–924, Boston, MA, USA, Oct. 2011.

[5] F. Hillier and G. Lieberman, *Introduction to Operations Resarch (9th edition)*. USA: McGraw-Hill Higher Education, 2010.

[6] W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133–142, 2016.

[7] X. Y. Lei, X. F. Liao, T. W. Huang, and F. Heriniaina, "Achieving security, robust cheating resistance, and high-efficiency for outsourcing large matrix multiplication computation to a malicious cloud," *Information Sciences*, vol. 280, pp. 205–217, 2014.

[8] X. Y. Lei, X. F. Liao, T. W. Huang, H. Q. Li, and C. Q. Hu, "Outsourcing large matrix inversion computation to a public cloud," *IEEE Transactions on Cloud Computing*, vol. 1, no. 1, pp. 78–87, 2013.

[9] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing," *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.

[10] D. Marinescu, *Cloud Computing Theory and Practice*. USA: Elsevier, 2013.

[11] H. X. Nie, X. F. Chen, J. Li, J. Liu, and W. J. Lou, "Efficient and verifiable algorithm for secure outsourcing of large-scale linear programming," in *Proceedings of 28th IEEE International Conference on Advanced Information Networking and Applications (AINA'14)*, pp. 591–596, Victoria, BC, Canada, May 2014.

[12] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proceedings of Advances in Cryptology (EUROCRYPT'99)*, pp. 223–238, Prague, Czech Republic, May 1999.

[13] S. Salinas, C. Q. Luo, X. H. Chen, and P. Li, "Efficient secure outsourcing of large-scale linear systems of equations," in *Proceedings of 2015 IEEE Conference on Computer Communications (INFOCOM'15)*, pp. 1035–1043, Hong Kong, China, Apr. 2015.

[14] J. Singh, "Cyber-attacks in cloud computing: A case study," *International Journal of Electronics and Information Engineering*, vol. 1, no. 2, pp. 78–87, 2014.

[15] C. Wang, K. Ren, and J. Wang, "Secure and practical outsourcing of linear programming in cloud computing," in *Proceedings of 2011 IEEE Conference on Computer Communications (INFOCOM'11)*, pp. 820–828, Shanghai, China, Apr. 2011.

[16] C. Wang, K. Ren, J. Wang, and Q. Wang, "Harnessing the cloud for securely outsourcing large-scale systems of linear equations," *IEEE Transactions on Parallel Distrib. Syst.*, vol. 24, no. 6, pp. 1172–1181, 2013.

[17] Z. Wang, Y. Lu, G. Sun, "A policy-based deduplication mechanism for securing cloud storage," *International Journal of Electronics and Information Engineering*, vol. 2, no. 2, pp. 70–79, 2015.

[18] M. Zareapoor, P. Shamsolmoali, and M. A. Alam, "Establishing safe cloud: Ensuring data security and performance evaluation," *International Journal of Electronics and Information Engineering*, vol. 1, no. 2, pp. 88–99, 2014.

**Zhengjun Cao** is an associate professor of Department of Mathematics at Shanghai University. He received his Ph.D. degree in applied mathematics from Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He served as a post-doctor in Computer Sciences Department, Université Libre de Bruxelles, from 2008 to 2010. His research interests include cryptography, discrete logarithms and quantum computation.

**Lihua Liu** is an associate professor of Department of Mathematics at Shanghai Maritime University. She received her Ph.D. degree in applied mathematics from Shanghai Jiao Tong University. Her research interests include combinatorics, cryptography and information security.