J Syst Sci Complex (2018) 31: 946–963

Information Security Protocol Based System Identification with Binary-Valued Observations*

XU Changbao · ZHAO Yanlong · ZHANG Ji-Feng

DOI: 10.1007/s11424-017-7075-7
Received: 16 March 2017 / Revised: 15 May 2017

Abstract Traditional control does not pay much attention to information security problems in system identification enough, which are important in practical applications. This paper focuses on the security problem of input information in a class of system identification problems with noise and binary-valued observations, presents a cryptography based security protocol, and improves it in the range of allowed errors. During solving the identification problem, the improved security protocol can ensure that the input information is not leaked, and thus, can deal with passive attacks effectively. Besides, a quantitative relationship among the input information, the public key in encryption and the number of participants in the improved protocol is shown. Finally, the simulation results show that, the identification algorithm can still achieve the estimation accuracy by adding the improved security protocol. However, compared with the original identification algorithm, the time complexity of the algorithm with the improved security protocol increases.

Keywords Cryptography, identification algorithm, information security, passive attacks, security protocol, time complexity.

1 Introduction

Traditional information security mainly protects information and information systems from unauthorized access, use, destruction, modification, inspection, records, etc. In practice, private companies have accumulated a large number of information about their employees, customers, products, research, financial data, new product lines and other confidential information. If this kind of information is mastered by competitors, the loss of such security may result in economic losses, legal proceedings and even the bankruptcy of the enterprise. In addition, for individuals, information security has significant impact on their personal privacy. Therefore, security for

XU Changbao · ZHAO Yanlong · ZHANG Ji-Feng
Key Laboratory of Systems and Control, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190*, China; School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing* 100049*, China.* Email: xuchangbao@amss.ac.cn; ylzhao@amss.ac.cn; jif@iss.ac.cn.
*This research was supported by the National Key Basic Research Program of China (973 Program) under Grant No. 2014CB845301 and the National Natural Science Foundation of China under Grant No. 61227902.
◇ *This paper was recommended for publication by Editor SUN Jian.*

protection of confidential information is not only a business requirement, but also a moral and legal requirement in many situations[1, 2].

The field of information security has experienced tremendous growth and evolution in recent years, see [3], [4] and [5]. It involves many special research fields, including: Security network, application software and database, safety test, evaluation of information systems, enterprise security planning and digital forensics technology, etc.

With the development of computer and network technology, most confidential information is collected and stored in computers, and transmitted to other terminals through communication networks. Therefore, the information security problem of computers and communication networks is particularly important. System control is now in the field of information technology, such as communications (see [6, 7]). As a result, security problems of system control can be related to important information security problems. The control systems have many mature methods and techniques, however, the problem based on information security has not been fully investigated.

In the traditional control problems, operations of the controllers do not set security measures, and the corresponding observation information is also disclosed. In this case, attackers can easily steal, tamper with or add information, thereby affecting the normal operation of the system and resulting in loss. Therefore, it is very important to improve the security of control systems, so that it can deal with a certain degree of active or passive attacks. Actually, existing security work in control systems (see [8, 9]) is mainly based on encoding/decoding algorithms, which is not enough to ensure the security to a certain extent.

In this paper, we start with a class of system identification problems with noise, based on binary-valued output information with multi-party cooperation. In fact, in identification with multi-party cooperation, the input information is likely to involve their privacy or confidences. For example, in commercial cooperation, it may be related to the sources of information, marketing strategy, customer information and other important information. And the corresponding output information is often related to the embodiment of the confidential information and feedback results. If the information is invested into identification protocols without security guarantee, although identification results is got, such as parameters, cooperative production process development coordinates, confidential information can easily be stolen by others in identification process, resulting in confidential input information leakage and a huge loss. Therefore, the security of identification protocols is particularly important in system identification problems.

In this paper, for simplicity, we assume that the attacker only uses passive attacks[10] in the identification problem discussed, the attacker at most bought $n-1$ participants $R_2, R_3, \cdots, R_n$, and R_1 is honest. Under these conditions, there is no secure protocol in the sense of information theory (see [11]), and we can only design secure protocols in the sense of cryptography, that is, simply relying on communication encoding/decoding algorithms can not guarantee the security of protocols, so that encryption/decryption algorithms are needed and make sense. To this end, the following are discussed in the sense of cryptography.

The main contributions of this paper can be concluded as follows. First, according to the traditional identification algorithm, we propose a security protocol in the sense of cryptography based on a linear topology structure[12]. Furthermore, we improve the security protocol in order to reduce its implementation complexity. To a certain extent, we improve security of the identification algorithm. Finally, we give the relationship among the public key, the input matrix and the number of parameters, and analyze the limitation of the security protocol.

The rest of this paper is organized as follows. Section 2 gives the formulation of the security problem in the system identification problem. Section 3 describes the treatment of encryption scheme and error. In Section 4, we design the security protocol. And we improve it in Section 5. Section 6 gives the main result of this paper and analyze the limitation of the security protocol. Related simulations are presented in Section 7. In Section 8, we conclude this paper and discuss further topics.

2 Problem Formulation

Assume that, there are n participants $R_1, R_2, \cdots, R_n$ cooperate to solve the following identification problem:

$$y(k) = \sum_{i=1}^{n} a_i u_i + d(k), \tag{1}$$

where $a_1, a_2, \cdots, a_n$ are parameters to be estimated, and $\{d(k)\}_{k=1}^{\infty}$ is a white noise sequence.

Input and output of Participant R_j $(j = 1, 2, \cdots, n)$ satisfy

$$y^j(k) = \sum_{i=1}^{n} a_i u_i^j + d(k). \tag{2}$$

In order to introduce the security problem, we need the following assumption.

Assumption 2.1 u_i^j $(i = 1, 2, \cdots, n)$, the input information of Participant R_j $(j = 1, 2, \cdots, n)$, are independent with time k, that is, the input information is fixed.

So, the n participants $R_1, R_2, \cdots, R_n$ need to cooperate to solve the identification problem. Furthermore, the solving process requires to ensure no leakage of their own input information.

In addition, the following assumption is also needed.

Assumption 2.2 In this paper, in order to deal with specific conditions, the identification method based on binary values is adopted. For Participant R_j $(j = 1, 2, \cdots, n)$, denote

$$S^j(k) = I_{\{y^j(k) \le C\}}, \quad \xi^j(k) = \frac{1}{k}\sum_{i=1}^{k} S^j(i), \tag{3}$$

where C is a threshold.

Then, $\left\{S^j(k)\right\}_{k=1}^{\infty}$ is a sequence of i.i.d. Bernoulli random variables, with success probability

$$\begin{aligned} \mathrm{P}\left\{S^j(k) = 1\right\} &= \mathrm{P}\left\{y^j(k) \le C\right\} = \mathrm{P}\left\{\sum_{i=1}^{n} a_i u_i^j + d(k) \le C\right\} \\ &= \mathrm{P}\left\{d(k) \le C - \sum_{i=1}^{n} a_i u_i^j\right\} = \Phi\left(C - \sum_{i=1}^{n} a_i u_i^j\right), \end{aligned} \tag{4}$$

where Φ is the standard normal distribution function. By Kolmogorov Strong Law of Large Numbers, we have

$$\xi^j(k) = \frac{1}{k}\sum_{i=1}^{k} S^j(i) \xrightarrow{\text{a.c.}} \Phi\left(C - \sum_{i=1}^{n} a_i u_i^j\right), \quad k \to \infty. \tag{5}$$

Therefore,

$$C - \Phi^{-1}\left(\xi^j(k)\right) \xrightarrow{\text{a.c.}} \sum_{i=1}^{n} a_i u_i^j, \quad k \to \infty. \tag{6}$$

Then, n participants only need to jointly solve the following linear equations to get estimates of $a_1, a_2, \cdots, a_n$:

$$\begin{cases} \widehat{a_1}(k)u_1^1 + \cdots + \widehat{a_n}(k)u_n^1 = C - \Phi^{-1}\left(\xi^1(k)\right), \\ \qquad\qquad \vdots \qquad\qquad\qquad\qquad \vdots \\ \widehat{a_1}(k)u_1^n + \cdots + \widehat{a_n}(k)u_n^n = C - \Phi^{-1}\left(\xi^n(k)\right), \end{cases} \tag{7}$$

where a_i's estimate $\widehat{a_i}(k) \xrightarrow{\text{a.c.}} a_i, i = 1, 2, \cdots, n$.

It can be seen that the original problem is transformed into a problem to jointly solve a set of linear equations with privacy protection, where the privacy refers to the participants' respective equations, that is, R_j's equation $\widehat{a_1}(k)u_1^j + \widehat{a_2}(k)u_2^j + \cdots + \widehat{a_n}(k)u_n^j = C - \Phi^{-1}\left(\xi^j(k)\right)$ is secret to other participants, $j = 1, 2, \cdots, n$. In this way, we can use the method of secure multi-party computation to solve the problem in the sense of cryptography.

3 Approximation Algorithm and Error Analysis

As mentioned earlier, only security protocols in the sense of cryptography can be designed in the situation of Section 2. So we need to use an encryption scheme on the integer ring and positive integer inputs. Since the range of Φ^{-1} is all real numbers, we need to replace irrational numbers by rational numbers approximately. The main idea is based on that any irrational number can be approximated by a sequence of rational numbers. The sequence of rational numbers can be constructed as follows.

For any irrational number x, given positive integer s, there is an integer r_s satisfying

$$\frac{r_s}{s} < x < \frac{r_s + 1}{s}. \tag{8}$$

In fact, interval $(r_s/s, (r_s + 1)/s)$ covers x. Such coverage exists, because, when r_s takes all integers, the union of all intervals like $[r_s/s, (r_s + 1)/s)$ can cover the whole real axis. As s increases, the length of interval $(r_s/s, (r_s + 1)/s)$ becomes smaller and smaller. So,

$$\frac{r_s}{s} \to x, \quad s \to \infty, \tag{9}$$

and $\{r_s/s\}_{s=1}^{\infty}$ is the sequence of rational numbers. That is, any given irrational number can be replaced by a rational number approximately, and the error can be made arbitrarily small.

Assume that the right side of R_j's equation $C - \Phi^{-1}\left(\xi^j(k)\right)$ can be replaced by rational number $r_{s^j}(k)/s^j(k), j = 1, 2, \cdots, n$. Then, (7) becomes

$$\begin{cases} \widehat{a_1}(k)u_1^1 + \cdots + \widehat{a_n}(k)u_n^1 = r_{s^1}(k)/s^1(k), \\ \qquad \vdots \qquad\qquad\qquad \vdots \\ \widehat{a_1}(k)u_1^n + \cdots + \widehat{a_n}(k)u_n^n = r_{s^n}(k)/s^n(k), \end{cases} \tag{10}$$

that is,

$$\begin{cases} \widehat{a_1}(k)u_1^1 s^1(k) + \cdots + \widehat{a_n}(k)u_n^1 s^1(k) = r_{s^1}(k), \\ \qquad \vdots \qquad\qquad\qquad \vdots \\ \widehat{a_1}(k)u_1^n s^n(k) + \cdots + \widehat{a_n}(k)u_n^n s^n(k) = r_{s^n}(k). \end{cases} \tag{11}$$

In this way, (11) is a set of linear equations with integral coefficients, and we use it to discuss instead of (7).

Rewrite (11) in matrix form

$$\widetilde{\boldsymbol{M}}(k)\widehat{\theta}(k) = \widetilde{\boldsymbol{b}}(k), \tag{12}$$

where

$$\widetilde{\boldsymbol{M}}(k) = \begin{pmatrix} u_1^1 s^1(k) & \cdots & u_n^1 s^1(k) \\ \vdots & \ddots & \vdots \\ u_1^n s^n(k) & \cdots & u_n^n s^n(k) \end{pmatrix}, \quad \widehat{\theta}(k) = \begin{pmatrix} \widehat{a_1}(k) \\ \vdots \\ \widehat{a_n}(k) \end{pmatrix}, \quad \widetilde{\boldsymbol{b}}(k) = \begin{pmatrix} r_{s^1}(k) \\ \vdots \\ r_{s^n}(k) \end{pmatrix}.$$

Similarly, rewrite (7) in matrix form $\boldsymbol{M}\widehat{\theta}(k) = \boldsymbol{b}(k)$, where

$$\boldsymbol{M} = \begin{pmatrix} u_1^1 & \cdots & u_n^1 \\ \vdots & \ddots & \vdots \\ u_1^n & \cdots & u_n^n \end{pmatrix}, \quad \boldsymbol{b}(k) = \begin{pmatrix} C - \Phi^{-1}\left(\xi^1(k)\right) \\ \vdots \\ C - \Phi^{-1}\left(\xi^n(k)\right) \end{pmatrix}. \tag{13}$$

Rewrite (10) as $\boldsymbol{M}\widehat{\theta}(k) = \overline{\boldsymbol{b}}(k)$, where

$$\overline{\boldsymbol{b}}(k) = [r_{s^1}(k)/s^1(k), r_{s^2}(k)/s^2(k), \cdots, r_{s^n}(k)/s^n(k)]'.$$

Denote $\delta^j(k) = \left[C - \Phi^{-1}\left(\xi^j(k)\right)\right] - r_{s^j}(k)/s^j(k), j = 1, 2, \cdots, n, \boldsymbol{\delta}(k) = [\delta^1(k), \delta^2(k), \cdots, \delta^n(k)]'$, and then, (7) satisfies

$$\boldsymbol{M}\widehat{\theta}(k) = \boldsymbol{b}(k) = \overline{\boldsymbol{b}}(k) + \boldsymbol{\delta}(k). \tag{14}$$

If $\boldsymbol{M}$ is nondegenerate, the solution of (7) satisfies

$$\widehat{\theta}(k) = \boldsymbol{M}^{-1}\overline{\boldsymbol{b}}(k) + \boldsymbol{M}^{-1}\boldsymbol{\delta}(k). \tag{15}$$

Besides, $\boldsymbol{M}^{-1}\overline{\boldsymbol{b}}(k)$ is the solution of (10), so $\boldsymbol{M}^{-1}\boldsymbol{\delta}(k)$ is the error term, that is, the error of the two kind of estimations.

From the previous analysis,

$$\delta^j(k) = \left[C - \Phi^{-1}\left(\xi^j(k)\right)\right] - \frac{r_{s^j}(k)}{s^j(k)} < \frac{1}{s^j(k)}, \quad j = 1, 2, \cdots, n. \tag{16}$$

For simplicity, take $s^j(k) = k, j = 1, 2, \cdots, n$. Then,

$$\delta^j(k) < \frac{1}{s^j(k)} = \frac{1}{k}, \quad j = 1, 2, \cdots, n. \tag{17}$$

So,

$$\boldsymbol{\delta}(k) = \begin{pmatrix} \delta^1(k) \\ \vdots \\ \delta^n(k) \end{pmatrix} < \frac{\mathbf{1}}{k} \to \mathbf{0}, \quad k \to \infty, \tag{18}$$

where $\mathbf{1} = (1, 1, \cdots, 1)'$.

This shows that the estimates obtained by the solution of (11) converge to the same values as that of (7), that is, the estimates obtained by the solution of (11) converge to real values.

Convergence rate of the estimates obtained by the solution of (7) is $O(1/k)$. $\boldsymbol{\delta}(k)$'s convergence rate is higher than $O(1/k)$, so, by (15), convergence rate of the estimates obtained by the solution of (11) is $O(1/k)$. That is, the two kinds of estimations have the same convergence rate.

So, we can solve (11) by using secure multi-party computation method.

4 Security Protocol

In this section, we adopt a threshold Paillier cryptographic system[13]. Denote $\mathbb{Z}_N = \{m \in \mathbb{Z} | 0 \leq m < N\}$ is the plain text space, Paillier cryptographic system has the following homomorphic property (see [14]).

$$E(m_1 + m_2) = E(m_1)E(m_2) \mod N^2, \tag{19}$$

where E is an encryption function, and $m_1, m_2 \in \mathbb{Z}_N$. In order to make only n participants be able to jointly decrypt and any $n-1$ (or less) participants be unable to, we need to add a threshold to this cryptographic system, namely (n, n)-threshold. The specific key generation process is as follows.

Select primes p, q, RSA module $N = pq$, $p_1 = (p-1)/2, q_1 = (q-1)/2$, and $M = p_1 q_1$, satisfying p_1, q_1 are prime and N, M are coprime. Select d, e satisfying $d \equiv 0 \mod M, de \equiv 1 \mod N$. Let $g = (1+N)^e$, and the public key is (N, g), the private key is d. Select $d_1, d_2, \cdots, d_n$ satisfying $d = d_1 + d_2 + \cdots + d_n$. Send $d_1, d_2, \cdots, d_n$ to the participants $R_1, R_2, \cdots, R_n$ as the private keys, respectively, to complete the private key distribution.

For $\forall m \in \mathbb{Z}_N$, the encryption function is as follows.

$$E(m) = g^m \mod N^2. \tag{20}$$

Denote $c = E(m)$ is the cipher text. The corresponding decryption process requires participant R_i to use his own private key to calculate $c_i = c^{d_i} \mod N^2$, and then all participants joint to decrypt. The decryption function is

$$m = D(c) = \frac{\left(\prod_{i=1}^{n} c_i \mod N^2\right) - 1}{N} \mod N. \tag{21}$$

At time k, the participants perform the following secure multi-party computation protocol.

Step 1 Encrypt the coefficients of the equations in (11), and get the following encrypted matrices.

$$E\left(\widetilde{\boldsymbol{M}}(k)\right) = \begin{pmatrix} E(u_1^1 s^1(k)) & \cdots & E(u_n^1 s^1(k)) \\ \vdots & \ddots & \vdots \\ E(u_1^n s^n(k)) & \cdots & E(u_n^n s^n(k)) \end{pmatrix}, \quad E\left(\widetilde{\boldsymbol{b}}(k)\right) = \begin{pmatrix} E(r_{s^1}(k)) \\ \vdots \\ E(r_{s^n}(k)) \end{pmatrix}.$$

Step 2 Participant R_i select n-order matrices $U_i, V_i \in \mathbb{Z}_N^{n\times n}$ secretly, $i = 1, 2, \cdots, n$. Pass the encrypted coefficient matrices in Step 1 in turn to the n participants, and each participant operates them, respectively, as shown in the following figure.

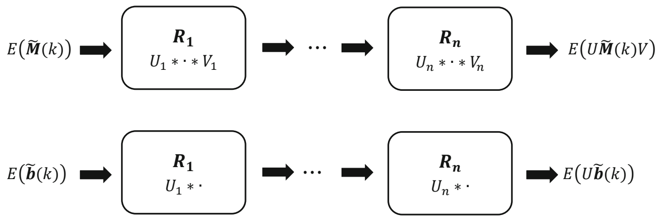


Figure 1 Cipher text transfer process

Where $U = U_n U_{n-1} \cdots U_1, V = V_1 V_2 \cdots V_n$, and the operation "$*$" is defined as follows.

$$\begin{aligned} &A = [a_{ij}]_{m_1\times m_2}, \quad E(B) = [E(b_{ij})]_{m_2\times m_3}, \quad A * E(B) = \left[\prod_{l=1}^{m_2} E(b_{lj})^{a_{il}}\right]_{m_1\times m_3}, \\ &E(B) = [E(b_{ij})]_{m_1\times m_2}, \quad A = [a_{ij}]_{m_2\times m_3}, \quad E(B) * A = \left[\prod_{l=1}^{m_2} E(b_{il})^{a_{lj}}\right]_{m_1\times m_3}. \end{aligned} \tag{22}$$

By (19), the output on the right side in the figure can be obtained.

Step 3 The n participants joint to decrypt the cipher text $E\left(U\widetilde{\boldsymbol{M}}(k)V\right), E\left(U\widetilde{\boldsymbol{b}}(k)\right)$. Here, we require that N is big enough so that $U\widetilde{\boldsymbol{M}}(k)V \in \mathbb{Z}_N^{n\times n}, U\widetilde{\boldsymbol{b}}(k) \in \mathbb{Z}_N^n$. Then, by decryption, $U\widetilde{\boldsymbol{M}}(k)V$, $U\widetilde{\boldsymbol{b}}(k)$ is obtained.

Step 4 Solve equation $U\widetilde{\boldsymbol{M}}(k)V\vartheta(k) = U\widetilde{\boldsymbol{b}}(k)$. It can be seen that $V\vartheta(k) = \widehat{\theta}(k)$, so, by the following procedure, $\widehat{\theta}(k)$ can be given.

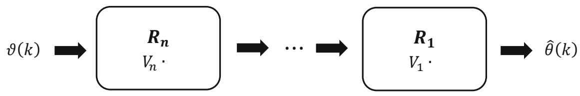


Figure 2 Plain text transfer process

Finally, the participant R_1 can make the result $\widehat{\theta}(k)$ public.

5 Protocol Improvement

In Step 3 of the protocol in the above section, we require the public key N of the encryption algorithm to satisfy $U\widetilde{\boldsymbol{M}}(k)V \in \mathbb{Z}_N^{n\times n}, U\widetilde{\boldsymbol{b}}(k) \in \mathbb{Z}_N^n$. This leads to that, as k increases, N will be very large beyond the actual computing ability of computers, and a lot of limitations in practical applications. To this end, we need to weaken the impact of k on the execution of the protocol.

Under the premise of allowed estimation error, let $s^j(k) = s_0, \forall j, k$, satisfying $1/s_0 < \varepsilon$ (allowed estimation error). By (17) and (18), the estimation error is within the allowed range. Correspondingly, there is a similar protocol.

In fact, the protocol's implementation complexity is positively related to n, and the actual implementation process is cumbersome. In order to reduce the implementation complexity of the protocol, we improve the protocol as follows. Take $n = 2$ in the original cryptographic system, and, under the premise of the participant R_1's honesty, let other participants to execute the protocol with R_1 separately, that is, each protocol execution process has only two participants. Then, the intersection of solution spaces of each execution result is just $\widehat{\theta}(k)$. In this way, we need to execute the protocol $n-1$ times, which can be processed in parallel. So, the implementation complexity of the protocol is reduced greatly. In fact, the cipher text transfer in Step 2 of the improved protocol can be described as the following figure.

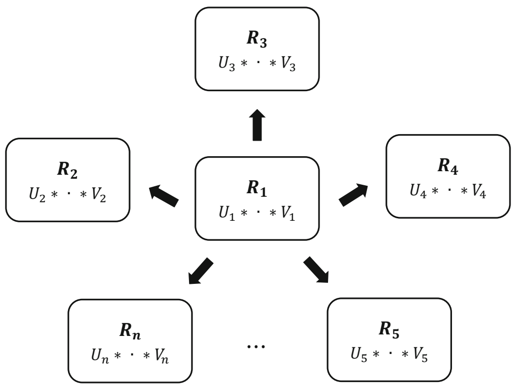


Figure 3 Cipher text transfer process in the improved protocol

Similarly, the plain text transfer in Step 4 can be described as follows.

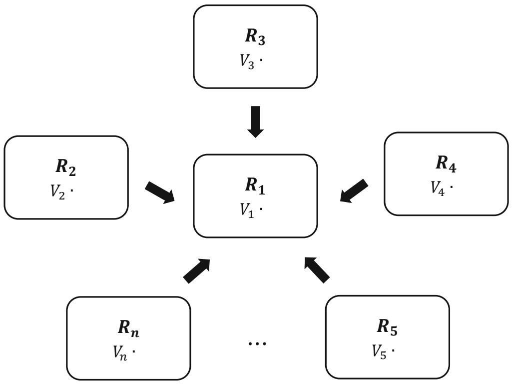


Figure 4 Plain text transfer process in the improved protocol

6 Main Result

For the improved protocol in Section 5, the public key N must satisfy the following condition.

Theorem 6.1 *In practice, the improved security protocol requires that the public key N, the input matrix $\boldsymbol{M}$ and the number of participants n must meet the following relationship:*

$$N > 4n^2 u_m^5, \tag{23}$$

where u_m is the maximum element of $\boldsymbol{M}$.

Proof Generally speaking, in the improved protocol, for every two participants $R_1, R_i, i = 2, 3, \cdots, n$, the protocol's requirement

$$U\widetilde{\boldsymbol{M}}_{1,i}(k)V \in \mathbb{Z}_N^{2\times n}, \quad U\widetilde{\boldsymbol{b}}_{1,i}(k) \in \mathbb{Z}_N^2 \tag{24}$$

can be met by $U\boldsymbol{M}_{1,i}V \in \mathbb{Z}_N^{2\times n}$, where $\widetilde{\boldsymbol{M}}_{1,i}(k)$ is the matrix consisting of the 1st and the i-th rows of $\widetilde{\boldsymbol{M}}(k)$, $\widetilde{\boldsymbol{b}}_{1,i}(k)$ is the vector consisting of the 1st and the i-th elements of $\widetilde{\boldsymbol{b}}(k)$, $\boldsymbol{M}_{1,i}$ is the matrix consisting of the 1st and the i-th rows of $\boldsymbol{M}$, $U = U_iU_1$ and $V = V_1V_i$. This can be guaranteed in practical applications. In detail, error requirements generally make

$$U\boldsymbol{M}_{1,i}V \in \mathbb{Z}_N^{2\times n} \Rightarrow U\widetilde{\boldsymbol{b}}_{1,i}(k) \in \mathbb{Z}_N^2, \tag{25}$$

and $U\widetilde{\boldsymbol{M}}_{1,i}(k)V \in \mathbb{Z}_N^{2\times n}$ can be replaced by $U\boldsymbol{M}_{1,i}V \in \mathbb{Z}_N^{2\times n}$ in the algorithm design.

In addition, with security guarantee, participants can select U_i, V_j with all elements smaller than u_m. Therefore, according to $U\boldsymbol{M}_{1,i}V \in \mathbb{Z}_N^{2\times n}$ and the number of participants in the improved protocol, by property of matrix multiplication and relation of dimension, we can get

$$\{[(u_m^2 \cdot 2) \cdot u_m \cdot 2] \cdot (u_m^2 \cdot n)\} \cdot n < N, \tag{26}$$

which leads to (23). The proof is completed. ∎

Further, we can give the constraint between the identification input and the number of parameters as follows.

Corollary 6.2 *Traditional computing ability of 64-bit computers restricts that, in this protocol, the number of participants n (the number of parameters to be estimated in the identification problem) and the maximum element of the input matrix u_m must satisfy*

$$n^2 u_m^5 < 2^{14}. \tag{27}$$

Proof In the encryption process, by (20), there are computations of $N^2 \times N^2 = N^4$ order of magnitude in the algorithm. Traditional computing ability of 64-bit computers is less than 2^{64}, so, by Theorem 6.1,

$$(4n^2 u_m^5)^4 < N^4 < 2^{64} \Rightarrow n^2 u_m^5 < 2^{14}. \tag{28}$$

The proof is completed. ∎

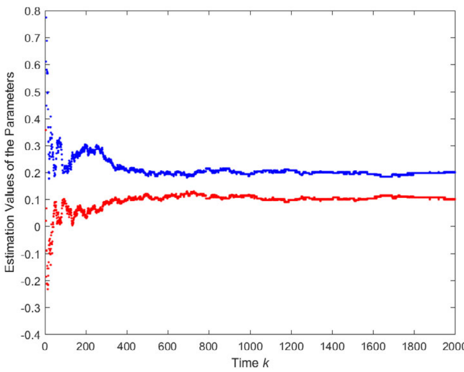
7 Simulation

For System (1), parameters of the algorithm with the improved security protocol take values as follows.

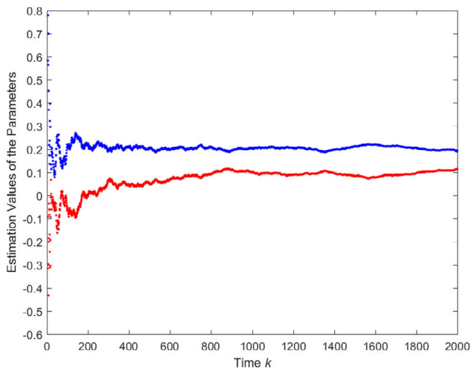
$$n = 2, \quad s_0 = 100, \quad T = 2000, \quad \theta = \begin{pmatrix} 0.2 \\ 0.1 \end{pmatrix}, \quad \boldsymbol{M} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \quad C = 0.4, \tag{29}$$

where T is the algorithm time.

For comparison, we simulate the original algorithm without the security protocol with the same parameters, and get the following result.



(a) The algorithm with the improved protocol



(b) The original algorithm

Figure 5 Result of the two algorithms with $u_m = 2$

Time used by the algorithm with the improved protocol is

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
begin	1	6.714 s	0.002 s	
Estimation	1	6.677 s	2.904 s	
newplot	1997	1.373 s	0.682 s	
hold	1997	1.122 s	0.907 s	
ishold	1997	0.452 s	0.452 s	
gobjects	3994	0.362 s	0.362 s	
Encryption	1998	0.314 s	0.314 s	
Equation	1997	0.284 s	0.087 s	
newplot>ObserveAxesNextPlot	1997	0.240 s	0.235 s	
markFigure	1997	0.176 s	0.176 s	
Decryption	1998	0.170 s	0.170 s	

Figure 6 Time spent by functions in the algorithm with the improved protocol

It can be seen that time is about 6.71 seconds.

Time used by the original algorithm is

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
begin	1	5.972 s	0.001 s	
Estimation	1	5.972 s	2.896 s	
newplot	1997	1.198 s	0.484 s	
hold	1997	1.136 s	0.916 s	
ishold	1997	0.456 s	0.456 s	
gobjects	3994	0.368 s	0.368 s	
Equation	1997	0.286 s	0.088 s	

Figure 7 Time spent by functions in the original algorithm

It can be seen that time is about 5.97 seconds. By comparison, time complexity of the algorithm becomes larger by the introduction of the encryption protocol.

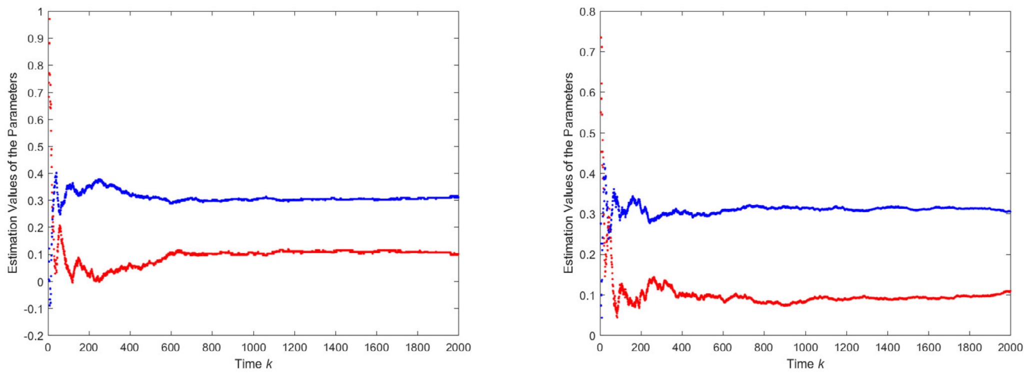
In the simulation, the maximum element of the input matrix $u_m = 2$. By Corollary 6.2, the protocol can deal with the identification problems with at most 22 participants and 22 parameters.

To show the increase of time complexity of the algorithm due to the introduction of the encryption protocol more clearly, we take different sets of parameters and get more simulation results as follows.

Take

$$\theta = \begin{pmatrix} 0.3 \\ 0.1 \end{pmatrix}, \quad \boldsymbol{M} = \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}, \quad C = 0.7,$$

and let other parameters remain unchanged.



(a) The algorithm with the improved protocol (b) The original algorithm

Figure 8 Result of the two algorithms with $u_m = 3$

Corresponding time used by the algorithm with the improved protocol is

Function Name	Calls	**Total Time**	Self Time*	Total Time Plot (dark band = self time)
begin	1	10.635 s	0.035 s	
Estimation	1	10.471 s	3.067 s	
Encryption	1998	2.354 s	2.354 s	
Decryption	1998	1.610 s	1.610 s	
newplot	1997	1.421 s	0.667 s	
hold	1997	1.166 s	0.939 s	
ishold	1997	0.463 s	0.463 s	
gobjects	3994	0.383 s	0.383 s	
Equation	1997	0.325 s	0.105 s	

Figure 9 Time spent by functions in the algorithm with the improved protocol

For the original algorithm, we have

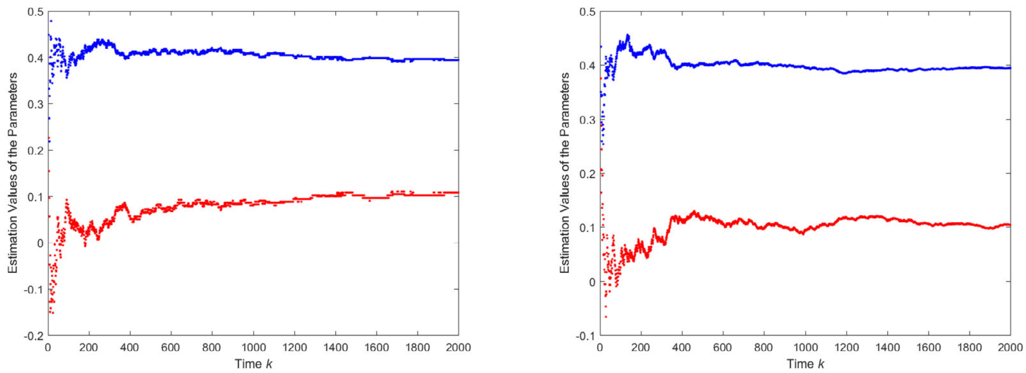
Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
begin	1	6.589 s	0.012 s	
Estimation	1	6.576 s	3.113 s	
newplot	1997	1.496 s	0.746 s	
hold	1997	1.176 s	0.953 s	
ishold	1997	0.462 s	0.462 s	
gobjects	3994	0.380 s	0.380 s	
Equation	1997	0.329 s	0.113 s	

Figure 10 Time spent by functions in the original algorithm

Take

$$\theta = \begin{pmatrix} 0.4 \\ 0.1 \end{pmatrix}, \quad \boldsymbol{M} = \begin{pmatrix} 4 & 1 \\ 1 & 2 \end{pmatrix}, \quad C = 1.1,$$

and let other parameters remain unchanged.



(a) The algorithm with the improved protocol (b) The original algorithm

Figure 11 Result of the two algorithms with $u_m = 4$

Corresponding time used by the algorithm with the improved protocol is

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
begin	1	20.236 s	0.003 s	
Estimation	1	20.188 s	3.090 s	
Encryption	1998	8.207 s	8.207 s	
Decryption	1998	5.472 s	5.472 s	
newplot	1997	1.380 s	0.615 s	
hold	1997	1.173 s	0.940 s	
ishold	1997	0.473 s	0.473 s	
gobjects	3994	0.391 s	0.391 s	
Equation	1997	0.321 s	0.100 s	

Figure 12 Time spent by functions in the algorithm with the improved protocol

For the original algorithm, we have

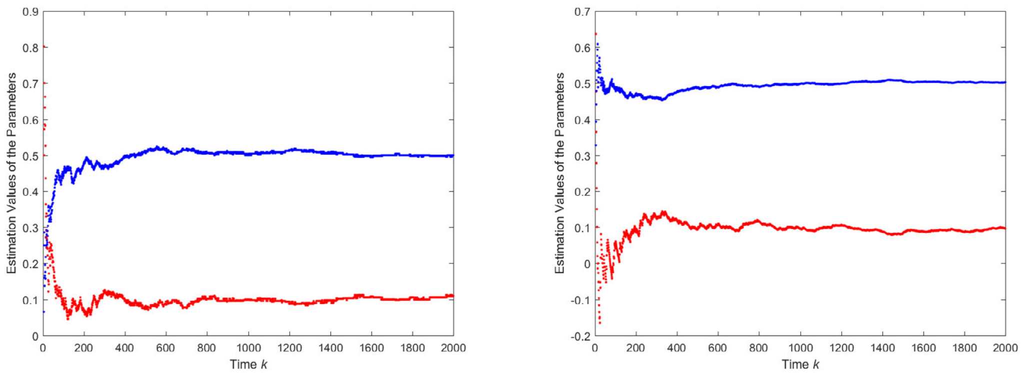
Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
begin	1	6.248 s	0.002 s	
Estimation	1	6.246 s	2.906 s	
newplot	1997	1.405 s	0.680 s	
hold	1997	1.173 s	0.948 s	
ishold	1997	0.467 s	0.467 s	
gobjects	3994	0.380 s	0.380 s	
Equation	1997	0.295 s	0.090 s	

Figure 13 Time spent by functions in the original algorithm

Take

$$\theta = \begin{pmatrix} 0.5 \\ 0.1 \end{pmatrix}, \quad \boldsymbol{M} = \begin{pmatrix} 5 & 1 \\ 1 & 2 \end{pmatrix}, \quad C = 1.6,$$

and let other parameters remain unchanged.



(a) The algorithm with the improved protocol (b) The original algorithm

Figure 14 Result of the two algorithms with $u_m = 5$

Corresponding time used by the algorithm with the improved protocol is

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
begin	1	62.350 s	0.053 s	
Estimation	1	62.161 s	3.468 s	
Encryption	1998	28.444 s	28.444 s	
Decryption	1998	26.626 s	26.626 s	
newplot	1997	1.504 s	0.683 s	
hold	1997	1.183 s	0.950 s	
ishold	1997	0.488 s	0.488 s	
gobjects	3994	0.410 s	0.410 s	
Equation	1997	0.357 s	0.115 s	

Figure 15 Time spent by functions in the algorithm with the improved protocol

For the original algorithm, we have

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
begin	1	6.267 s	0.001 s	
Estimation	1	6.265 s	2.921 s	
newplot	1997	1.398 s	0.667 s	
hold	1997	1.180 s	0.953 s	
ishold	1997	0.467 s	0.467 s	
gobjects	3994	0.381 s	0.381 s	
Equation	1997	0.300 s	0.093 s	

Figure 16 Time spent by functions in the original algorithm

However, when we take

$$\theta = \begin{pmatrix} 0.6 \\ 0.1 \end{pmatrix}, \quad \boldsymbol{M} = \begin{pmatrix} 6 & 1 \\ 1 & 2 \end{pmatrix}, \quad C = 2.2,$$

and let other parameters remain unchanged, we find the algorithm with the improved security protocol failed.

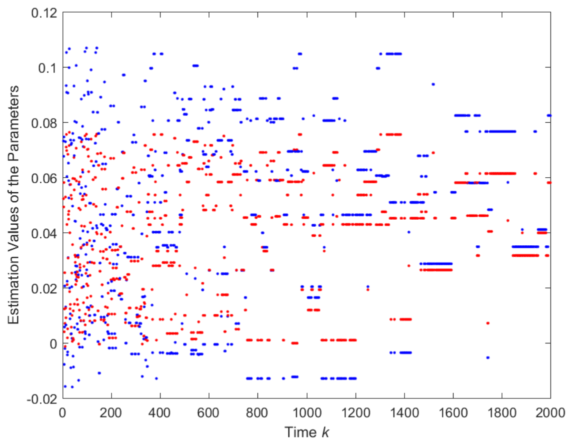


Figure 17 Result of the algorithm with the improved protocol

Actually, by Corollary 6.2, $u_m = 6$ leads to $n \leq 1$, which contradicts with the parameter setting in (29). That is, the improved security protocol is not able to deal with this set of parameters, which reflects the limitation of the protocol.

We summarize the above simulation results in Table 1.

Table 1 Simulation results

Set of parameters	Time spent by the algorithm with the improved protocol	Time spent by the original algorithm
$\theta = \left(\begin{smallmatrix}0.2\\0.1\end{smallmatrix}\right), \boldsymbol{M} = \left(\begin{smallmatrix}2&1\\1&2\end{smallmatrix}\right), C = 0.4$	6.71	5.97
$\theta = \left(\begin{smallmatrix}0.3\\0.1\end{smallmatrix}\right), \boldsymbol{M} = \left(\begin{smallmatrix}3&1\\1&2\end{smallmatrix}\right), C = 0.7$	10.64	6.59
$\theta = \left(\begin{smallmatrix}0.4\\0.1\end{smallmatrix}\right), \boldsymbol{M} = \left(\begin{smallmatrix}4&1\\1&2\end{smallmatrix}\right), C = 1.1$	20.24	6.25
$\theta = \left(\begin{smallmatrix}0.5\\0.1\end{smallmatrix}\right), \boldsymbol{M} = \left(\begin{smallmatrix}5&1\\1&2\end{smallmatrix}\right), C = 1.6$	62.35	6.27

From the above table, we can see that, as u_m increases, the algorithm with the improved security protocol costs more and more time, but the time spent by the original algorithm remains stable. In addition, as u_m increases, the difference between the time cost by the two algorithm becomes larger and larger.

8 Summary and Prospect

This paper proposes a security protocol in the sense of cryptography based on the traditional identification algorithm. We improve the security protocol to reduce its implementation complexity. Besides, the relationship among the public key, the input matrix and the number of parameters is given, and the limitation and the simulation results are analysed.

In the problem of this paper, the protocol based on star topology has obvious advantages than linear topology case. Actually, from Figures 1 and 3, the improved protocol essentially changes the linear topology structure in the original protocol to star type. So, we can study topology structures of multi-agent (participant) network for further study of the problem in this paper and it is expected to reduce the limitation of the protocol (Figure 21 and Corollary 6.2). In addition, the protocol in this paper is based on solving linear equations, which is not necessarily applicable to other types of identification problems. This may lead to further study. In other fields of control theory, there are still many problems involved in security, which are of great significance and need to be solved.

References

[1] Wang D and Wang Y, Optimal military spending, trade and stochastic economic growth, *Journal of Systems Science and Complexity*, 2016, **29**(3): 736–751.

[2] Zhang L, Jin L, Luo W, et al., Robust secure transmission for multiuser MISO systems with probabilistic QoS constraints, *Science China: Information Sciences*, 2016, **59**(2): 1–13.

[3] Gordon L A and Loeb M P, The economics of information security investment, *Journal ACM Transactions on Information and System Security* (*TISSEC*), 2002, **5**(4): 438–457.

[4] Catteddu D, Cloud computing: Benefits, risks and recommendations for information security, *Communications in Computer and Information Science*, 2010, **72**: 17–17.

[5] Bulgurcu B, Cavusoglu H, and Benbasat I, Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, *Journal MIS Quarterly*, 2010, **34**(3): 523–548.

[6] Li T, Fu M, Xie L, et al., Distributed consensus with limited communication data rate, *IEEE Transactions on Automatic Control*, 2011, **56**(2): 279–292.

[7] Cheng H and Wong W S, Application of protocol sequences in wireless networked control systems, *Proc. of the* 33*rd Chinese Control Conference*, 2014, 5666–5671.

[8] Ding K, Li Y, Quevedo D, et al., A multi-channel transmission schedule for remote state estimation under DoS attacks, *Automatica*, 2017, **78**: 194–201.

[9] Li Y, Quevedo D E, Dey S, et al., A game-theoretic approach to fake-acknowledgment attack on cyber-physical systems, *IEEE Transactions on Signal and Information Processing over Networks*, 2017, **3**(1): 1–11.

[10] Serjantov A and Sewell P, Passive attack analysis for connection-based anonymity systems, *Lecture Notes in Computer Science*, 2003, **2808**: 116–131.

[11] Hirt M and Maurer U, Player simulation and general adversary structures in perfect multiparty computation, *Journal of Cryptology*, 2000, **13**(1): 31–60.

[12] Zhang Z, Privacy preserving cooperative solving system of linear equations, *ChinaCrypt*, 2007, 217–224.

[13] Paillier P, Public-key cryptosystems based on discrete logarithms residues, *Eurocrypt*'99, *Lecture Notes in Computer Science* 1592, Springer-Verlag, 1999, 223–238.

[14] Gentry C, Fully homomorphic encryption using ideal lattices, *STOC*, 2009, 169–178.