An Innovative Encryption Method for Agriculture Intelligent Information System based on Cloud Computing Platform *

Tan, Wen Xue[1,2,3] Zhao, Chun Jiang* [1,3] Wu, Hua Rui [1] Wang, Xi Ping [4]

1. National Engineering Research Center for Information Technology in Agriculture, Beijing, 100097, China
2. College of Computer Science and Technology, Hunan University of Arts and Science, Changde, 415000, China
3. College of Computer Science, Beijing University of Technology, Beijing, 100022, China
4. College of Economy and Management, Hunan University of Arts and Science, Changde, Hunan, 415000, China
Email: {twxpaper,zhaocjnercita}@163.com; wuhr@nercita.org.cn; wxp7973@163.com

Abstract— **Along with a rapid growth of cloud computing technology and its deep application in Agriculture Intelligent Information System, Agriculture Industry information security and privacy has become a highlight of the issue about Agriculture Cloud Information System. Encrypting is a conventional information security means, however, hitherto almost all encryption scheme cannot support the operation based on cipher-text. As a result, it is a difficult to build up the corporate and individual information security and privacy-securing in the information system based on cloud computing platform. In order to construct the information security and privacy of cloud computing infrastructure, down to the practicality of Agriculture Information System the project crew brings forward An Innovative Encryption Method for Agriculture Intelligent Information System based on Cloud Computing Platform, OCEVMO for short, which takes root in the theory of matrix, and supports a series of cipher-text-operation essential to build a secure communication protocol between user, owner and cloud server. Beside the conventional encryption-decryption operation, OCEVMO implements 4 operations of cipher-text-numerical-value data such as adding, subtracting, multiplying and dividing. Theoretical analysis and experimental performance estimation demonstrates that OCEVMO is of IND-CCA security, capable of performing crypo-function with a moderate speed. Its favorable versatile performance gives promise of the interactive operation Securing corporate-individual privacy in the area of Agriculture Intelligent Information System.**

Index Terms— **Cloud computing; Agriculture Intelligent System; Data Encryption; Matrix-Operation; Privacy-Securing; IND-CCA.**

Submitted date: 2012-09-01;Revised date: 2013-06-25.

(*) This work is funded by Chinese National Natural Science Foundation (61271257, 61102126); Chinese National Science and Technology Support Program (2013BAJ04B04, 2011BAD21B02, 2012BAD52G01); Beijing Natural Science Foundation (4122034); Hunan Provincial Natural Science Foundation of China (12JJ9020); Hunan Provincial Science and Technology Plan(2013GK3135, 2012GK3125); Project of the Education Department of Hunan Province No. 11C0900 and Project of Hunan University of Arts and Science, No. JGYB1223.

(⋆) Corresponding Author: Zhao, Chun Jiang. China National Engineering Research Center for Information Technology in Agriculture(NERCITA) , Beijing Agriculture Science and Technology Building A, Room A320, Beijing Shuguang Garden Middle Road No. 11, Haidian District West Suburb, Beijing,China.

I. INTRODUCTION

Cloud computing has become a welcome computing mode based on Internet by providing user with more economical and flexible IT service such as the ability of storage, computing and network access in demand than the traditional IT technology. Since the idea of cloud computing caters to the current social trend of " Green-Computing " and " Low-Carbon Economy " [1], governments and corporations all over the world are trying their best to advocate and develop the cloud computing oriented traditional and basic industries, which activates some outstanding innovation in the area of computation and commerce in turn.

A. Status of Corporate and Individual Cloud Security

However, in the cloud computing system which has been constructed and in operation, the crux of privacy-security has been annoying people,which has become one of main factors that hold back its development and generalization.

Corporative privacy may be some data whereby to identify an individual corporation or an aggregate corporation itself such as phone number, corporation address, credit card number. In addition,some sensitive information and some expensive digital information asset of Agriculture Intelligent System and of the like system all belongs to the focus of security concern [2], [3]. For examples, the individual health reports from Diagnosing System, the Knowledge Rules of Agriculture Expert System [4], [5] and financial records from Stock System and so on.

Cloud privacy-security originates from data-trusting and service-leasehold which are 2 outstanding characteristics of cloud platform. Once people trust the third part with their data which then is stored in the cloud-server and lose the manipulative ability to their data. As a result, the event of revealing or abusing user's sensitive information occurs frequently. In recent years, some cases of cloud service provider losing or revealing user's data happened to Google and MediaMax, which

doi:10.4304/jsw.9.1.1-10

suggests people's concern about cloud privacy securing be far from unwanted [6].

Encryption is a conventional method to secure privacy. But, nowadays most of the encryption algorithm cannot support cipher-text operation such as fuzzy indexing-comparing,similarity distance calculating in encrypted document, and arithmetic operating or encrypted financial data items for Statistical Analysis Report. These operations are essential to Agriculture Cloud Intelligent System sustaining open access [7], [8].

B. Related Work and Our Contribution

According to present research , the encryption scheme addressed to sustaining cipher-text-operation, it may be classified into two classes: the search-sustaining and the compute-sustaining.

[6] brought forward a cipher-text searching method based symmetric encryption, and [9] proposed an algorithm with alike function based public encryption.However, these schemes is effective only to exact-search and is out of action when spelling errors and format mistakes occur.

[1] designed the encryption scheme based product of scalar quantity, which is compatible with K-Nearest-Neighbor (KNN) computing toward the encrypted database. In addition, some well-known homomorphic schemes such as Elgamal, Pailler and Unpadded-RSA only compatible with one homomorphic operation either homomorphic addition or homomorphic multiplication [10], [11]. As to fully homomorphic algorithm, these existed algorithms are too high computational complex to be applied in cloud computing system [12], [13].

To the issues listed above, in this paper, a novel Homomorphic Encryption Scheme oriented to Cloud Computing System is brought forward, which is rooted in the theory of vector and matrix, and supports cipher-text computation and is a promising scheme to secure privacy in the course of cloud-storing and cloud-computing.

II. Formulation of Problem

A. Privacy-Securing Model of Cloud Platform

Let abstract the cloud computing model supporting privacy-securing to Figure 1, which depicts the interaction between the Owner of data, the User of data,and Service Provider (SP for short) which is a trustee of contracted data. The following steps are introduction details.

Step 1. Owner encrypts the private-sensitive data items denoted by m_i, and returns $\mathcal{E}(m_i)$, then trust service provider with $\mathcal{E}(m_i)$ and which is stored on the server.

step 2. After being permitted or empowered by Owner, User encrypts the $para$ which denotes the operation type and the data in User's care and involved into computation, then submits all the encryption result to SP.

Step 3. Responding to the User's request, SP authenticates the User's privilege then computes $\mathcal{E}(m_i)$ in the scope denoted by $para$ according to the operation type and $para$. At last, the output denoted by $\mathcal{E}(Output)$ is returned to User.

Step 4. Use decrypts $\mathcal{E}(Output)$ and gets $Output$ in state of plain-text.

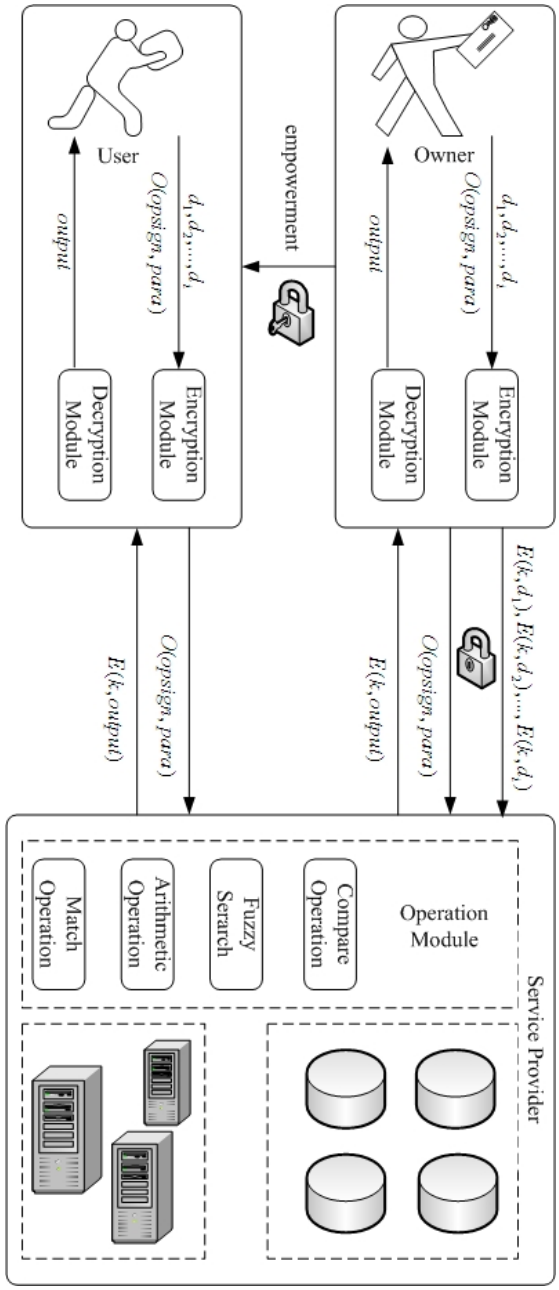

Figure 1. Privacy-Securing Model of Cloud Platform.

In this flow, both User and Owner encrypt the trusted sensitive data, the operation parameter respectively and hide their privacy in good condition. However, it is a fresh question to arise subsequently how SP operates the encrypted data and maintains operation output equivalent [14]. If it were not solved effectively, Owner and User could not exert the computer resource of cloud computing system to process sensitive data, and its advantage would be out of action [14], [15]. In such background, this literature proposes an innovative encryption scheme which may be a potential to reverse such a predicament.

B. Related Definitions

Definition 1. **Operable-Cipher-text Encryption Scheme** (OCES for short) $\bigsqcup = (\mathcal{E}, \mathcal{D}, \mathcal{G}, \mathcal{O})$, which is composed of 4 algorithms as follows.

Key-Generating algorithm $\mathcal{G}$, which is called to generate secret key k from User's random secure parameter $para$ and is denoted by (1).

$$\mathcal{G}(para) \rightarrow k \tag{1}$$

Encryption algorithm $\mathcal{E}$. Let $\widehat{X}$ and $\widehat{Y}$ denote the domain and range of $\mathcal{E}$. Address to a message $m \in \widehat{X}$, $c \in \widehat{Y}$, it is defined as (2) which is maybe either a determinate algorithm or a probable algorithm.

$$\mathcal{E}(m, k) \rightarrow \ c \tag{2}$$

Decryption algorithm $\mathcal{D}$ is defined as (3), and ϕ indicates the rootlessness of $\mathcal{D}$ operated on cipher-text. $\mathcal{D}$ must be a determinate algorithm.

$$\mathcal{D}(c, k) \rightarrow \{m\} \bigcup \{\phi\} \tag{3}$$

Cipher-text operation algorithm $\mathcal{O}$. Given a set $\{c_1, c_2, ...c_i\}, c_i \in \widehat{Y}$, (4) expresses the mathematic implication of $\mathcal{O}$, and $opsign$ represents the operation type, maybe anyone of Fuzzy-Matching and arithmetic operation $+$, $-$,$\times$,$\div$.

$$\begin{aligned} &\mathcal{D}(\mathcal{O}(c_1, c_2, ...c_i, opsign)) \rightarrow \mathcal{O}(\mathcal{D}(c_1, k) \\ &\mathcal{D}(c_2, k), ...\mathcal{D}(c_i, k), opsign) \end{aligned} \tag{4}$$

Definition 2. **Correctness** of $\bigsqcup$. OCES is defined to be correct where (5) is satisfied.

$$\begin{aligned} &I. \forall m \in \widehat{X}, \mathcal{D}(\mathcal{E}(m, k)) = m \\ &II. \exists \mathcal{O}(m_1, m_2, ...m_i, opsign) = \mathcal{D}(\mathcal{O}(\mathcal{E}(m_1, k), \\ &\mathcal{E}(m_2, k), ...\mathcal{E}(m_i, k), opsign), k) \end{aligned} \tag{5}$$

Definition 3. **Security** of $\bigsqcup$ OCES is defined to be secure subject to 2 items as follows. (1) $\bigsqcup$ is able to maintain security of Indistinguishability Against Chosen Cipher-text Attack (IND-CCA for short) in the event that the oracle of cipher-text and the oracle of plain-text about the trusted data are provided. (2). $\bigsqcup$ assures that it is impossible for SP to deduce any knowledge about original plain-text or intermediate result or the last result during the course of running $\mathcal{O}$ for operating cipher-text [14].

Definition 4. Given $c_1, c_2, c_3 \in \widehat{Y}$, a binary operant as $opsign$ defined in the above text denoted by $\circ$ so that for all $m_1, m_2, m_3 \in \widehat{X}$ it holds that $m_3 = m_1 \circ m_2$ and $c_1 = \mathcal{E}(m_1, k)$,$c_2 = \mathcal{E}(m_2, k)$ then (6) is negligible. Then it is defined that scheme $\mathcal{E}$ is homomorphic to operant $\circ$, so-called the **Homomorphic Property**.

$$Prob[\mathcal{D}(c_1 \circ c_2, k) \neq m_3] \tag{6}$$

III. Operable Cipher-text Encryption based on Vector-Matrix Operation

In this Section, an Operable Cipher-text Encryption Scheme based on Vector-Matrix Operation is constructed, which is abbreviated to OCEVMO. OCEVMO realizes the cipher-text computing such as addition, substraction, multiplication and dividing of numeric digital data under the condition that information security of both User and Owner of data is warranted.

A. Formal Definition of OCEVMO

Definition 5. $\mathbf{OCEVMO} = \{\mathcal{G}, \mathcal{E}, \mathcal{D}, \mathcal{C}\}$,which covers 4 algorithm as follows.

$\mathcal{G}$ is a key generation algorithm which is defined as (7). $para$ denotes Users' secure parameter. A key $\mathbf{K}$ is a $d \times d$ reversible matrix.

$$\mathcal{G}(para) \rightarrow \{\mathbf{K}\} \tag{7}$$

$\mathcal{E}$ is an encryption algorithm. Let $\widehat{X}$ and $\widehat{Y}$ denote the domain and range of $\mathcal{E}$. $\mathbf{m} \in \widehat{X}$ which is a d-dimension vector transformed from plain-text message, define $\mathcal{E}$ as (8), $\mathbf{c} \in \widehat{Y}$, which is a d-dimension vector and is the cipher-text of m .

$$\mathcal{E}(\mathbf{m}, \mathbf{K}) \rightarrow \mathbf{c} \tag{8}$$

$\mathcal{D}$ is a decryption algorithm which is defined as (9), $opsign$ indicates the the type of operation operated on cipher-text. $opsign = null$ denotes the operation is to decrypt the cipher-text $\mathbf{c}$ which is a direct encryption result of $\mathbf{m}$; $opsign = +$ denotes the cipher-text to be decrypted is a addition-operation result of some 2 cipher-text; $opsign = -$ denotes the cipher-text to be decrypted is a subtraction-operation result of some 2 cipher-text; $opsign = \times$ denotes the cipher-text to be decrypted is a multiplication-operation result of some 2 cipher-text; $opsign = \div$ denotes the cipher-text to be decrypted is the quotient result of some 2 cipher-text.

$$\mathcal{D}(\mathbf{c}, \mathbf{K}, opsign) \rightarrow \{\mathbf{m}\} \tag{9}$$

$\mathcal{O}$ is a cipher-text operation algorithm. Its form is as (10), which operates $\mathbf{c_1}, \mathbf{c_2}, ...\mathbf{c_i}, \mathbf{c_i} \in \widehat{Y}$, and outputs corresponding result according to $opsign$ defined in the above text. $\mathbf{c}'$ is subjected to $\mathbf{c}' \in \widehat{Y}$.

$$\mathcal{O}(\mathbf{c_1}, \mathbf{c_2}, ...\mathbf{c_i}, opsign) \rightarrow \mathbf{c}' \tag{10}$$

B. Transformation of Numeric Data

Data of cloud computing system is divided into 2 parts: numeric data and character data or string data, which is an primary idea of OCEVMO. Numeric data is often operated some mathematic operation such as addition and multiplication, while query and fuzzy-indexing is fit to character data [16]. In this literature, the former is the focus of the discussion.

Operations fit to numeric data are arithmetic operation, as is referred in the above text. In order to implement these operations, message m is preprocessed into the

vector $\mathbf{m}$. The elements of vector are partitioned into 2 parts, the adding factor which is a computation array, denoted by $FAdd$ used to implement addition of cipher-text and the multiplication factor which is also a computation array, denoted by $FMul$, used to construct multiplication of cipher-text. The dimension of $FAdd$ and $FMul$ are denoted by d_a, d_m, subject to $d_a \in N, d_a > 2, d_m \in N, d_m > 3$. No doubt, process is to be a reversible course.

Let m be a plain-text numeric data, the process whereby it is transformed into a d dimension vector is composed of following steps. At first, select d_a-1 random real number $(r_{+1}, r_{+2}, ..., r_{+d_a-1}), r_{+i} \in \mathcal{R}, i \in [1, d_a - 1]$, and extract another element by (11). So a d_a dimension vector denoted by $\mathbf{m}$ is returned as (12). Choose d_a random real number $\{r_1, r_2, ..., r_{d_a}\}, r_i \in \mathcal{R}, i \in [1, d_a]$ a second time, by which $\mathbf{m}$ is transformed into $\mathbf{m}'$ as (13).

$$r_{+d_a} = m - \sum_{i=1}^{d_a-1} r_{+i} \tag{11}$$

$$\mathbf{m} = (r_{+1}, r_{+2}, ..., r_{+d_a-1,}, r_{+d_a})^T \tag{12}$$

$$\mathbf{m}' = (r_{+1} + r_1, r_{+2} + r_2, ..., r_{+d_a} + r_{d_a})^T \tag{13}$$

Secondly, select d_m-1 random real number $(r_{\times 1}, r_{\times 2}, ..., r_{\times d_m-1}), r_{\times i} \in \mathcal{R}, i \in [1, d_m - 1]$, the multiplication inverse of $r_{\times i}$ is a limited fraction and extract another element $r_{\times d_m}$ by (14). Thus the owner of data can transform $\mathbf{m}'$ into $\mathbf{m}''$ as (16), what should be noticed is the dimension of $\mathbf{m}''$ is $d_m + d_a$.

$$r_{\times d_m} = m \div \prod_{i=1}^{d_m-1} r_{\times i} \tag{14}$$

$$\begin{aligned}\mathbf{m}'' = (&r_{+1} + r_1, r_{+2} + r_2, ..., r_{+d_a} + r_{d_a},\\ &r_{\times 1}, r_{\times 2}, ..., r_{\times d_m})^T\end{aligned} \tag{15}$$

Thirdly, by tailing a random computation array, the owner extends $\mathbf{m}''$ into a $d_m + d_a + k$ dimension vector denoted by $\mathbf{m}'''$ which is a final vector of preprocess of encryption as (16), random number $r_{\phi i} \in \mathcal{R}, k \in N, k > 2$ and $r_{\phi k}$ subjected to (17).

$$\begin{aligned}\mathbf{m}''' = (&r_{+1} + r_1, r_{+2} + r_2, ..., r_{+d_a} + r_{d_a},\\ &r_{\times 1}, r_{\times 2}, ..., r_{\times d_m}, r_{\phi 1}, r_{\phi 2}, ..., r_{\phi k-1}, r_{\phi k})^T\end{aligned} \tag{16}$$

$$r_{\phi k} = -\sum_{i=1}^{d_a} r_i \tag{17}$$

At last, Owner encrypts $\mathbf{m}'''$ and get $\hat{\mathbf{c}}$ by (18) with which is trusted SP and saved on the storage system of server by its Owner. Decryption of $\hat{\mathbf{c}}$ is an inverse process of encryption obviously, as is omitted here [17], [18].

$$\hat{\mathbf{c}} = \mathbf{K} \times \mathbf{m}''' \tag{18}$$

The steps whereby users transform query parameter into vector is similar with the course above. So, whether the trust data or query parameter is to be preprocessed through the same procedure and the result will be a vector.

From the course aforementioned, preprocessing of vector transforming scatters and hides the original information into all components of the vector. In the meantime, through an ingenious designment of each component, it becomes practical to maintain arithmetic operation equivalence between plain-text and cipher-text.

However, the computation complexity similar to " dimension curse " will arise, which means that computation workload increases in proportion to the growth of vector dimension.

Let m_p, m_q be 2 plain-text numeric data, and their corresponding final vectors be $\mathbf{p}''', \mathbf{q}'''$, and their corresponding cipher-text vectors be $\hat{\mathbf{p}}, \hat{\mathbf{q}}$. In the next text, how to implement various operation of cipher-text will be discussed in detail.

C. Addition Operation

SP operates addition on $\hat{\mathbf{p}}, \hat{\mathbf{q}}$ directly as (19).

$$\begin{aligned}&\hat{\mathbf{p}} + \hat{\mathbf{q}} = \mathbf{K} \times \mathbf{p}''' + \mathbf{K} \times \mathbf{q}'''\\ &= \mathbf{K} \times [(p_{+1} + p_1, p_{+2} + p_2, ..., p_{+d_a} + p_{d_a},\\ &p_{\times 1}, p_{\times 2}, ..., p_{\times d_m}, p_{\phi 1}, p_{\phi 2}, ..., p_{\phi k-1}, p_{\phi k})^T +\\ &(q_{+1} + q_1, q_{+2} + q_2, ..., q_{+d_a} + q_{d_a}, q_{\times 1}, q_{\times 2}, ...,\\ &q_{\times d_m}, q_{\phi 1}, q_{\phi 2}, ..., q_{\phi k-1}, q_{\phi k})^T]\\ &= \mathbf{K} \times [(p_{+1} + p_1 + q_{+1} + q_1, p_{+2} + p_2 + q_{+2} +\\ &q_2, ..., p_{+d_a} + p_{d_a} + q_{+d_a} + q_{d_a}, p_{\times 1} + q_{\times 1}, p_{\times 2} +\\ &q_{\times 2}, ..., p_{\times d_m} + q_{\times d_m}, p_{\phi 1} + q_{\phi 1}, p_{\phi 2} + q_{\phi 2}, ...,\\ &p_{\phi k-1} + q_{\phi k-1}, p_{\phi k} + q_{\phi k})^T = \mathbf{K} \times (\mathbf{p}''' + \mathbf{q}''')\end{aligned} \tag{19}$$

Then, SP returns it to User. User decrypts it as (20).

$$\begin{aligned}&\mathbf{K^{-1}} \times (\hat{\mathbf{p}} + \hat{\mathbf{q}}) = \mathbf{K^{-1}} \times \mathbf{K} \times [(p_{+1} + p_1 + q_{+1}\\ &+q_1, p_{+2} + p_2 + q_{+2} + q_2, ..., p_{+d_a} + p_{d_a} + q_{+d_a} +\\ &q_{d_a}, p_{\times 1} + q_{\times 1}, p_{\times 2} + q_{\times 2}, ..., p_{\times d_m} + q_{\times d_m}, p_{\phi 1} +\\ &q_{\phi 1}, p_{\phi 2} + q_{\phi 2}, ..., p_{\phi k-1} + q_{\phi k-1}, p_{\phi k} + q_{\phi k})^T\\ &= (p_{+1} + p_1 + q_{+1} + q_1, p_{+2} + p_2 + q_{+2} + q_2, ...,\\ &p_{+d_a} + p_{d_a} + q_{+d_a} + q_{d_a}, p_{\times 1} + q_{\times 1}, p_{\times 2} + q_{\times 2},\\ &..., p_{\times d_m} + q_{\times d_m}, p_{\phi 1} + q_{\phi 1}, p_{\phi 2} + q_{\phi 2}, ...,\\ &p_{\phi k-1} + q_{\phi k-1}, p_{\phi k} + q_{\phi k})^T = \mathbf{p}''' + \mathbf{q}'''\end{aligned} \tag{20}$$

After getting a d-dimension vector $\mathbf{p}''' + \mathbf{q}'''$, according to preprocess procedure expressed by (11),(16) and (17) from message to vector, User sums its the former d_a elements and the last element, then the result is returned which just is the addition of m_p, m_q as (21).

Multi-Adding operation of cipher-text is supported in this scheme under the condition of not being decrypted.

$$\begin{aligned}&p_{\phi k} + q_{\phi k} + \sum_{i=1}^{d_a} (p_{+i} + p_i + q_{+i} + q_i) = -\sum_{i=1}^{d_a} (p_i)\\ &-\sum_{i=1}^{d_a} (q_i) + [\sum_{i=1}^{d_a} (p_{+i}) + \sum_{i=1}^{d_a} (p_i) + \sum_{i=1}^{d_a} (q_{+i})\\ &+\sum_{i=1}^{d_a} (q_i)] = \sum_{i=1}^{d_a} (p_{+i}) + \sum_{i=1}^{d_a} (q_{+i}) = m_p + m_q\end{aligned} \tag{21}$$

D. Subtraction Operation

SP subtracts $\hat{\mathbf{q}}$ from $\hat{\mathbf{q}}$ by (22).

$$\begin{aligned}&\hat{\mathbf{p}}-\hat{\mathbf{q}}=\mathbf{K}\times\mathbf{p}'''-\mathbf{K}\times\mathbf{q}'''\\&=\mathbf{K}\times[(p_{+1}+p_1,p_{+2}+p_2,...,p_{+d_a}+p_{d_a},\\&p_{\times1},p_{\times2},...,p_{\times d_m},p_{\phi1},p_{\phi2},...,p_{\phi k-1},p_{\phi k})^T-\\&(q_{+1}+q_1,q_{+2}+q_2,...,q_{+d_a}+q_{d_a},q_{\times1},q_{\times2},...,\\&q_{\times d_m},q_{\phi1},q_{\phi2},...,q_{\phi k-1},q_{\phi k})^T]\\&=\mathbf{K}\times[(p_{+1}+p_1-q_{+1}-q_1,p_{+2}+p_2-q_{+2}-\\&q_2,...,p_{+d_a}+p_{d_a}-q_{+d_a}-q_{d_a},p_{\times1}-q_{\times1},p_{\times2}-\\&q_{\times2},...,p_{\times d_m}-q_{\times d_m},p_{\phi1}-q_{\phi1},p_{\phi2}-q_{\phi2},...,\\&p_{\phi k-1}-q_{\phi k-1},p_{\phi k}-q_{\phi k})^T=\mathbf{K}\times(\mathbf{p}'''-\mathbf{q}''')\end{aligned}\tag{22}$$

Its result is returned and User can decrypt it as (23).

$$\begin{aligned}&\mathbf{K^{-1}}\times(\hat{\mathbf{p}}-\hat{\mathbf{q}})=\mathbf{K^{-1}}\times\mathbf{K}\times[(p_{+1}+p_1-q_{+1}\\&-q_1,p_{+2}+p_2-q_{+2}-q_2,...,p_{+d_a}+p_{d_a}-q_{+d_a}-\\&q_{d_a},p_{\times1}-q_{\times1},p_{\times2}-q_{\times2},...,p_{\times d_m}-q_{\times d_m},p_{\phi1}-\\&q_{\phi1},p_{\phi2}-q_{\phi2},...,p_{\phi k-1}-q_{\phi k-1},p_{\phi k}-q_{\phi k})^T\\&=(p_{+1}+p_1-q_{+1}-q_1,p_{+2}+p_2-q_{+2}-q_2,...,\\&p_{+d_a}+p_{d_a}-q_{+d_a}-q_{d_a},p_{\times1}-q_{\times1},p_{\times2}-q_{\times2},\\&...,p_{\times d_m}-q_{\times d_m},p_{\phi1}-q_{\phi1},p_{\phi2}-q_{\phi2},...,\\&p_{\phi k-1}-q_{\phi k-1},p_{\phi k}-q_{\phi k})^T=\mathbf{p}'''-\mathbf{q}'''\end{aligned}\tag{23}$$

User totals its the former d_a elements and the last element and the output is returned, which just is the difference between m_p and m_q as (24). Multi-Subtracting operation of cipher-text is acceptable in this scheme before being decrypted.

$$\begin{aligned}&p_{\phi k}-q_{\phi k}+\sum_{i=1}^{d_a}(p_{+i}+p_i-q_{+i}-q_i)=-\sum_{i=1}^{d_a}(p_i)\\&+\sum_{i=1}^{d_a}(q_i)+[\sum_{i=1}^{d_a}(p_{+i})+\sum_{i=1}^{d_a}(p_i)-\sum_{i=1}^{d_a}(q_{+i})\\&-\sum_{i=1}^{d_a}(q_i)]=\sum_{i=1}^{d_a}(p_{+i})-\sum_{i=1}^{d_a}(q_{+i})=m_p-m_q\end{aligned}\tag{24}$$

E. Multiplication Operation

At first, introduce the principle of implementing multiplication in this scheme by a specific case. Let m_p, m_q be 2 plain-text numeric data, and their corresponding final vectors be 2 6-dimension vector $\mathbf{p}''', \mathbf{q}'''$ as (25) and (26).

Obviously $m_p = p_{+1} + p_{+2} = p_{\times1} \times p_{\times2}$ and $m_q = q_{+1} + q_{+2} = q_{\times1} \times q_{\times2}$ according to (11) and (14). $p_1, p_2, q_1, q_2, p_{\phi1}, q_{\phi1}$ be random real number. Then, watch the multiplication result of ${\mathbf{p}'''}^T$ and $\mathbf{q}'''$ denoted by 6×6 Matrix $\mathbf{R}$ as (31) and (32) and its column components as expressed by (27) $\sim$ (30).

$$\mathbf{p}'''=(p_{+1}+p_1,p_{+2}+p_2,p_{\times1},p_{\times2},p_{\phi1},p_{\phi2})^T\tag{25}$$

$$\mathbf{q}'''=(q_{+1}+p_1,q_{+2}+q_2,q_{\times1},q_{\times2},q_{\phi1},q_{\phi2})^T\tag{26}$$

$$\mathbf{R_{*1}}=\begin{bmatrix}p_{+1}q_{+1}+p_{+1}q_1+p_1q_{+1}+p_1q_1\\p_{+2}q_{+1}+p_{+2}q_1+p_2q_{+1}+p_2q_1\\p_{\times1}q_{+1}+p_{\times1}q_1\\p_{\times2}q_{+1}+p_{\times2}q_1\\p_{\phi1}q_{+1}+p_{\phi1}q_1\\p_{\phi2}q_{+1}+p_{\phi2}q_1\end{bmatrix}\tag{27}$$

$$\mathbf{R_{*2}}=\begin{bmatrix}p_{+1}q_{+2}+p_{+1}q_2+p_1q_{+2}+p_1q_2\\p_{+2}q_{+2}+p_{+2}q_2+p_2q_{+2}+p_2q_2\\p_{\times1}q_{+2}+p_{\times1}q_2\\p_{\times2}q_{+2}+p_{\times2}q_2\\p_{\phi1}q_{+2}+p_{\phi1}q_2\\p_{\phi2}q_{+2}+p_{\phi2}q_2\end{bmatrix}\tag{28}$$

$$\mathbf{R_{*3,*4}}=\begin{bmatrix}p_{+1}q_{\times1}+p_1q_{\times1}&p_{+1}q_{\times2}+p_1q_{\times2}\\p_{+2}q_{\times1}+p_2q_{\times1}&p_{+2}q_{\times2}+p_2q_{\times2}\\p_{\times1}q_{\times1}&p_{\times1}q_{\times2}\\p_{\times2}q_{\times1}&p_{\times2}q_{\times2}\\p_{\phi1}q_{\times1}&p_{\phi1}q_{\times2}\\p_{\phi2}q_{\times1}&p_{\phi2}q_{\times2}\end{bmatrix}\tag{29}$$

$$\mathbf{R_{*5,*6}}=\begin{bmatrix}p_{+1}p_{\phi1}+p_1p_{\phi1}&p_{+1}p_{\phi2}+p_1p_{\phi2}\\p_{+2}p_{\phi1}+p_2p_{\phi1}&p_{+2}p_{\phi2}+p_2p_{\phi2}\\p_{\times1}p_{\phi1}&p_{\times1}p_{\phi2}\\p_{\times2}p_{\phi1}&p_{\times2}p_{\phi2}\\p_{\phi1}p_{\phi1}&p_{\phi1}p_{\phi2}\\p_{\phi2}p_{\phi1}&p_{\phi2}p_{\phi2}\end{bmatrix}\tag{30}$$

$$\mathbf{R}=(R_{*1},R_{*2},R_{*3,*4},R_{*5,*6})\tag{31}$$

$$\mathbf{p}'''\times{\mathbf{q}'''}^T=\mathbf{R}\tag{32}$$

It is found that if we multiply $\mathbf{R}[3][3]$ and $\mathbf{R}[4][4]$ the product of m_p, m_q will be extracted as (30).

$$\begin{aligned}&\prod_{i=3}^{4}\mathbf{R}[i][i]=p_{\times1}q_{\times1}\times p_{\times2}q_{\times2}\\&=p_{\times1}p_{\times2}\times q_{\times2}q_{\times1}=m_p\times m_q\end{aligned}\tag{33}$$

So, the product of any cipher-text-pair may be computed similarly. According to the analysis above, SP operates the cipher-text-pair $\hat{\mathbf{p}}, \hat{\mathbf{q}}$ as (34).

$$\begin{aligned}&\hat{\mathbf{p}}\times\hat{\mathbf{q}}^{\mathbf{T}}=\mathbf{K}\times\mathbf{p}'''\times(\mathbf{K}\times\mathbf{q}''')^T\\&=\mathbf{K}\times\mathbf{p}'''\times{\mathbf{q}'''}^T\times\mathbf{K}^T\\&=\mathbf{K}\times(p_{+1}+p_1,p_{+2}+p_2,...,p_{+d_a}+p_{d_a},\\&p_{\times1},p_{\times2},...,p_{\times d_m},p_{\phi1},p_{\phi2},...,p_{\phi k-1},p_{\phi k})^T\times\\&(q_{+1}+q_1,q_{+2}+q_2,...,q_{+d_a}+q_{d_a},q_{\times1},q_{\times2},...,\\&q_{\times d_m},q_{\phi1},q_{\phi2},...,q_{\phi k-1},q_{\phi k})\times\mathbf{K}^T\end{aligned}\tag{34}$$

The result of (34) is a $d \times d$ matrix which is to be returned to User by SP. User can decrypt it as (35).

$$\begin{aligned}&\mathbf{K}^{-1} \times \mathbf{K} \times (p_{+1} + p_1, p_{+2} + p_2, ..., p_{+d_a} + p_{d_a},\\ &p_{\times 1}, p_{\times 2}, ..., p_{\times d_m}, p_{\phi 1}, p_{\phi 2}, ..., p_{\phi k-1}, p_{\phi k})^T \times\\ &(q_{+1} + q_1, q_{+2} + q_2, ..., q_{+d_a} + q_{d_a}, q_{\times 1}, q_{\times 2}, ...,\\ &q_{\times d_m}, q_{\phi 1}, q_{\phi 2}, ..., q_{\phi k-1}, q_{\phi k}) \times \mathbf{K}^T \times \mathbf{K^{-1}}^T\\ &= (p_{+1} + p_1, p_{+2} + p_2, ..., p_{+d_a} + p_{d_a},\\ &p_{\times 1}, p_{\times 2}, ..., p_{\times d_m}, p_{\phi 1}, p_{\phi 2}, ..., p_{\phi k-1}, p_{\phi k})^T \times\\ &(q_{+1} + q_1, q_{+2} + q_2, ..., q_{+d_a} + q_{d_a}, q_{\times 1}, q_{\times 2}, ...,\\ &q_{\times d_m}, q_{\phi 1}, q_{\phi 2}, ..., q_{\phi k-1}, q_{\phi k}) = \mathbf{p'''} \times \mathbf{q'''}^T\end{aligned} \tag{35}$$

The result of (35) also is a $d \times d$ matrix denoted by $\mathbf{R}$. Then, User computes the multiplication of m_p, m_q as (36). Only is one-time multiplication permissable in this scheme in the state of cipher-text.

$$\prod_{i=d_a+1}^{d_a+d_m} \mathbf{R}[i][i] = m_p \times m_q \tag{36}$$

F. Division Operation

Let us recall the referred case about 6-dimension vector firstly. Examine the third column of $\mathbf{R}, \mathbf{R_{*3}}$,and sum its elements No. 1, No. 2 and No. 6 as (37).

$$\begin{aligned}&p_{+1}q_{\times 1} + p_1 q_{\times 1} + p_{+2}q_{\times 1} + p_2 q_{\times 1} + p_{\phi 2} q_1 =\\ &p_{+1}q_{\times 1} + p_1 q_{\times 1} + p_{+2}q_{\times 1} + p_2 q_{\times 1} - (p_1 + p_2)\\ &\times q_{\times 1} = (p_{+1} + p_{+2}) \times q_{\times 1} = m_p \times q_{\times 1}\end{aligned} \tag{37}$$

Similarly, as to the fourth column of $\mathbf{R}, \mathbf{R_{*4}}$, and sum its elements No. 1, No. 2 and No. 6 as (38).

$$\begin{aligned}&p_{+1}q_{\times 1} + p_1 q_{\times 2} + p_{+2}q_{\times 1} + p_2 q_{\times 2} + p_{\phi 2} q_2 =\\ &p_{+1}q_{\times 2} + p_1 q_{\times 2} + p_{+2}q_{\times 2} + p_2 q_{\times 2} - (p_1 + p_2)\\ &\times q_{\times 2} = (p_{+1} + p_{+2}) \times q_{\times 2} = m_p \times q_{\times 2}\end{aligned} \tag{38}$$

Extract the product of (37) and (38), rewrite and reduce its mathematic process and (39) may be returned.

$$\begin{aligned}&\prod_{i=3}^{4}(\sum_{j=1,2,6} \mathbf{R}[j][i]) = m_p \times q_{\times 1} \times m_p \times q_{\times 2}\\ &= m_p^2 \times m_q\end{aligned} \tag{39}$$

Pay attention to the third row of $\mathbf{R}$, and sum its elements No. 1, No. 2 and No. 6 as (40), another approximate relation is to be found.

$$\begin{aligned}&p_{\times 1}q_{+1} + p_{\times 1}q_1 + p_{\times 1}q_{+2} + p_{\times 1}q_2 + p_{\times 1}q_{\phi 2} =\\ &p_{\times 1}q_{+1} + p_{\times 1}q_1 + p_{\times 1}q_{+2} + p_{\times 1}q_2\\ &-p_{\times 1}(q_1 + q_2) = p_{\times 1} \times (q_{+1} + q_{+2}) = p_{\times 1} \times m_q\end{aligned} \tag{40}$$

As to the fourth row of $\mathbf{R}$,and sum its elements No. 1, No. 2 and No. 6 as (41).

$$\begin{aligned}&p_{\times 2}q_{+1} + p_{\times 2}q_1 + p_{\times 2}q_{+2} + p_{\times 2}q_2 + p_{\times 2}q_{\phi 2} =\\ &p_{\times 2}q_{+1} + p_{\times 2}q_1 + p_{\times 2}q_{+2} + p_{\times 2}q_2\\ &-p_{\times 2}(q_1 + q_2) = p_{\times 2} \times (q_{+1} + q_{+2}) = p_{\times 2} \times m_q\end{aligned} \tag{41}$$

Extract the product of (40) and (41), rewrite and reduce its mathematic process and (42) may be returned.

$$\begin{aligned}&\prod_{i=3}^{4}(\sum_{j=1,2,6} \mathbf{R}[i][j]) = m_q \times p_{\times 1} \times m_q \times p_{\times 2}\\ &= m_q^2 \times m_p\end{aligned} \tag{42}$$

Divide the right of (39) by that of (42) and the quotient of $m_p \div m_q$ is to be output as (43).

$$\frac{\prod_{i=3}^{4}(\sum_{j=1,2,6} \mathbf{R}[j][i])}{\prod_{i=3}^{4}(\sum_{j=1,2,6} \mathbf{R}[i][j])} = m_p \div m_q \tag{43}$$

By the analysis of the case, it is easy to give an algorithm of dividing-operation of encipher-text. At first, SP operates the cipher-text-pair $\hat{\mathbf{p}}, \hat{\mathbf{q}}$ as (34) and the result of (34) is a $d \times d$ matrix which is to be returned to User by SP, User can decrypt it as (35) and the preprocessing course is the same with multiplication operation. In order to get dividing result, User must execute the further operation as (44),(45) and (46).

$$\prod_{i=d_a+1}^{d_a+d_m}(\sum_{j=1,2,...,d_a,d} \mathbf{R}[j][i]) = m_p^{d_m} \times m_q \tag{44}$$

$$\prod_{i=d_a+1}^{d_a+d_m}(\sum_{j=1,2,...,d_a,d} \mathbf{R}[i][j]) = m_q^{d_m} \times m_p \tag{45}$$

$$\sqrt[d_m-1]{\frac{\prod_{i=d_a+1}^{d_a+d_m}(\sum_{j=1,2,...,d_a,d} \mathbf{R}[j][i])}{\prod_{i=d_a+1}^{d_a+d_m}(\sum_{j=1,2,...,d_a,d} \mathbf{R}[i][j])}} = m_p \div m_q \tag{46}$$

it is self-evident that the right of " = " in (46) is just the answer, i.e. the quotient of dividing m_p by m_q. What is notable is that only one-time division operation is permitted in this scheme in the event of encryption.

IV. Proof of Correctness

As a cipher-text operable encryption scheme, correctness of OCEVMO should be demonstrated in two respects: exactness of encrypting-decrypting and its homomorphic compatibility [19]. So, its proof question is to be broken into two sub-questions as follows.

1.$\forall m \in \mathbf{X}$,proof $\mathcal{D}[\mathcal{E}(m, \mathbf{K}), \mathbf{K}] = m$.

2.For $\forall\{\hat{\mathbf{p_1}}, \hat{\mathbf{p_2}}, ..., \hat{\mathbf{p_t}}\}$,and subjected to $\hat{\mathbf{p_i}} \in \mathbf{Y}$, proof that (47) should come into existence.

$$\begin{aligned}&\mathcal{O}(\hat{\mathbf{p_1}}, \hat{\mathbf{p_2}}, ..., \hat{\mathbf{p_t}}, opsign) = \mathcal{E}\{\mathcal{O}[\mathcal{D}(\hat{\mathbf{p_1}}, \mathbf{K}),\\ &\mathcal{D}(\hat{\mathbf{p_2}}, \mathbf{K}), ..., \mathcal{D}(\hat{\mathbf{p_t}}, \mathbf{K}), opsign], \mathbf{K}\}\end{aligned} \tag{47}$$

Proof 1. OCEVMO is based on Matrix operation. $\mathbf{K}$ is a $d \times d$ reversible matrix, so the matrix multiplication is reversible. In addition,the course of transforming plain-text m into vector $\hat{\mathbf{m}}_\mathbf{p}$ is recoverable, which is denoted by $\mathcal{T}(m) = \mathbf{m_p}$. In sum, the process of transformation is to be expressed by (48) and its reversibility and correctness is self-evident.

It is the end of proof 1.

$$\begin{aligned}&\mathcal{D}\{\mathcal{E}(m, \mathbf{K}), \mathbf{K}\} = \mathcal{T}^{-1}\{\mathcal{D}[\mathcal{E}(\mathcal{T}(m), \mathbf{K}), \mathbf{K}]\\ &= \mathcal{T}^{-1}\{\mathcal{D}[\mathcal{E}(\mathbf{m_p}, \mathbf{K}), \mathbf{K}]\} = \mathcal{T}^{-1}\{\mathbf{m_p}\} = m\end{aligned} \tag{48}$$

Proof 2. Where $opsign = \text{“}+\text{”}$ and $t = 2$, the proof object may be adapted into (49).

$$\begin{aligned}&\mathcal{O}(\hat{\mathbf{p_1}}, \hat{\mathbf{p_2}}, +) = \\ &\mathcal{E}\{\mathcal{O}[\mathcal{D}(\hat{\mathbf{p_1}}, \mathbf{K}), \mathcal{D}(\hat{\mathbf{p_2}}, \mathbf{K}), +], \mathbf{K}\}\end{aligned} \tag{49}$$

(49) can be rewritten into (50) further.

$$\begin{aligned}&\hat{\mathbf{p_1}} + \hat{\mathbf{p_2}} = \mathcal{E}\{\mathcal{O}[\mathbf{p_1}''', \mathbf{p_2}''', +], \mathbf{K}\} \\ &= \mathcal{E}\{\mathbf{p_1}''' + \mathbf{p_2}''', \mathbf{K}\} = \mathbf{K} \times (\mathbf{p_1}''' + \mathbf{p_2}''')\end{aligned} \tag{50}$$

It is obvious that the left and the right of (50) just may be formed into by substituting variables of (19). In the same way, alter $opsign = \text{“}+\text{”}, \times, \div$ in turn and make reference to (22), (34) and (46), satisfiability of other case can be build up easily. In one word, predication 2 is true.

It is the end of proof 2.

V. Analysis of Security

Theorem 1. OCEVMO **is distance-unrecoverable.**

Proof. Suppose OCEVMO is distance-unrecoverable, there must exist a function denoted by f subject to (51).

$$\begin{aligned}&f[\mathcal{E}(m_p, \mathbf{K}), \mathcal{E}(m_q, \mathbf{K})] = d(m_p, m_q) \\ &\forall\{m_p, m_q\} \in \mathbf{X}\end{aligned} \tag{51}$$

Choose 2 different keys $\mathbf{K_1}, \mathbf{K_2}$ and 2 different message $\{m_x, m_y\} \in \mathbf{X}$,and OCEVMO satisfies (52).

$$\begin{aligned}&(i).\ \alpha_1 = \mathcal{E}(m_p, \mathbf{K_1}) = \mathcal{E}(m_x, \mathbf{K_2}) \\ &(ii).\ \alpha_1 = \mathcal{E}(m_q, \mathbf{K_1}) = \mathcal{E}(m_y, \mathbf{K_2}) \\ &(iii).\ d(m_p, m_q) \neq d(m_x, m_y)\end{aligned} \tag{52}$$

Because of (51),then:

$$\begin{aligned}&f(\alpha_1, \alpha_2) = f(\mathcal{E}(m_p, \mathbf{K_1}), \mathcal{E}(m_q, \mathbf{K_1})) \\ &= d(m_p, m_q); f(\alpha_1, \alpha_2) = f(\mathcal{E}(m_x, \mathbf{K_2}), \\ &\mathcal{E}(m_y, \mathbf{K_2}) = d(m_x, m_y) = d(m_p, m_q)\end{aligned} \tag{53}$$

Obviously, the last item of (53) is a contradiction to the last item of (52). So,there must not exist the function f, and OCEVMO cannot but distance-unrecoverable.

Definition 6 Unsolvable Equation. Let $\widehat{\mathbf{P}}$ be the set of d dimension vector, $\widehat{\mathbf{K}}$ be the set of $d \times d$, as to $\forall \hat{p}_i \in \widehat{\mathbf{P}}, \forall \mathbf{K}_j \in \widehat{\mathbf{K}}$ there exists the equation denoted by $f(\hat{p}_i, \mathbf{K}_j) = \hat{p}_k, \hat{p}_k \in \widehat{\mathbf{P}}, i, j, k \in N$, subject to $s_L > s_R$ and s_L, s_R denote the number of the unknowns in both sides of “ = ” respectively, so that the equation $f(\hat{p}_i, \mathbf{K}_j) = \hat{p}_k$ is defined an **Unsolvable Equation** [20].

Theorem 2. As to encryption-decryption and the mathematic operation of numeric plain-text, OCEVMO is of security under IND-CCA if the number of adding factor $d_a > 3$.

Proof. Case 1. An adaptive chosen cipher-text attacker $\widetilde{H}$ oracles to have gotten t pair of plain-cipher text by means of encrypting-decrypting trust data generated by **OCEVMO**. In **OCEVMO**, let the dimension of vector be $d = n+k$ and the size of matrix be $d \times d$ where n is the number of computational elements and k is the number of random elements. To $\widetilde{H}$, the number of the unknown in $\mathbf{K}$ is $d \times d$, and the number of the unknown in the known part of each cipher-plain text is $d_a + (n-2) + (k-1)$, that of another part is d [21]. In addition, according to the section III, the unknown number in the both sides of the equation of **OCEVMO** and their relationship can be expressed by (54). So, due to d^2, t be positive, if $d_a > 3$ is satisfied, (54) is sure to be true, and the equation group derived from the matrix **OCEVMO** is unsolvable.

$$\begin{aligned}&d \times d + t \times (d_a + (n-2) + (k-1)) > \\ &t \times d \Longrightarrow d^2 + (d_a - 3) \times t > 0\end{aligned} \tag{54}$$

Case 2. Hacker $\widetilde{H}$ kicks off attack against **OCEVMO** following steps as follows. 1. $\widetilde{H}$ picks up two items of data m_1, m_2 and sends them to Owner, who encrypts either of them at random denoted by $m_r, r \in 0, 1$ and returns the cipher-text $\hat{\mathbf{m}}_r$ to $\widetilde{H}$. 2. $\widetilde{H}$ selects some plain-text (or cipher-text) and query Owner for **OCEVMO** encryption (or decryption), some corresponding result is returned back. 3. $\widetilde{H}$ repeats the step 2 until there are t pairs plain-cipher text couples denoted by $(m_1, \hat{\mathbf{m}}_1)$,$(m_2, \hat{\mathbf{m}}_2)$,...$(m_t, \hat{\mathbf{m}}_t)$ in $\widetilde{H}$'s hand. 4. $\widetilde{H}$ tries his best to compute and output m' as his oracle of m_b [22].

According to the transformation procedure of numeric data, the cipher-text of m_p is $\hat{\mathbf{p}}$ extracted by (55).

$$\begin{aligned}&\hat{\mathbf{p}} = \mathbf{K} \times \mathbf{p}''' \\ &= \mathbf{K} \times (p_{+1} + p_1, p_{+2} + p_2, ..., p_{+d_a} + p_{d_a}, \\ &p_{\times 1}, p_{\times 2}, ..., p_{\times d_m}, p_{\phi 1}, p_{\phi 2}, ..., p_{\phi k-1}, p_{\phi k})^T\end{aligned} \tag{55}$$

In (55), beyond $p_{+d_a}, p_{\times d_m}, p_{\phi k}$, the left elements are random real numeric, which are sampled at random with respect to m_p. On principle of Vector-Matrix operation, each element of the vector is determined by including all the elements of matrix and vector that plays the role of the operand, in the meantime, is affected by random numeric too [23]. Thus, it is assured that if the same numeric plain-text m_p is encrypted by the same key $\mathbf{K}$ time after time, the output cipher-text of each time are different. Because the range of **OCEVMO** is $\mathcal{R}$, and let $\parallel \mathcal{R} \parallel$ denote the element number of $\mathcal{R}$, the advantage probability of $m' = m_b$ in $\widetilde{H}$'s hand may be measured by (56).

$$\begin{aligned}&Adv(\widetilde{H}) = |Prob[m' = m_b] - \tfrac{1}{2}| \\ &= |(\tfrac{1}{2} - \tfrac{1}{\parallel \mathcal{R} \parallel}) - \tfrac{1}{2}| = |\tfrac{1}{\parallel \mathcal{R} \parallel}|\end{aligned} \tag{56}$$

Hence, where $d_a > 3$, the advantage probability of $m' = m_b$ in $\widetilde{H}$'s hand is a negligible quantity.

Case 3. While math operation is performed on cipher-text, it is stated in the section III that the indeterminacy of cipher-text is not influenced upon by a bit during the course of operation, and the advantage probability of giving a success oracle in $\widetilde{H}$'s hand is the same with Case 2 in that $\widetilde{H}$ is not in the know about key.

Sum up Case 1, 2, and 3, it is drawn that when the number of adding factor $d_a > 3$, OCEVMO is of security under IND-CCA [24].

It is the end of Proof.

VI. Performance Testing Analysis

In this Section, the performance of OCEVMO is estimated by drawing a parallel between the algorithm unpadded_RSA which supports multiple homomorphic, and the algorithm Piller which is compatible with additional homomorphic in terms of running performance. The indexes of performance include encrypting-decrypting speed, arithmetic operation performance and loads of storing and communication. All of the experiment is deployed on the platform named by **ArgSoSo** [25],which is the Agriculture Information Intelligent Searching Platform developed by the project crew of Chinese National Engineering Research Center for Information Technology in Agriculture based on Web technology and Cloud Computing, the hardware of which is a cluster consisted of 10 servers named DeepCom made by Lenovo [26].

TABLE I.
Performance of OCEVMO & concerned schemes

Algos	U_RSA	Piller	OCEVMO			
Para	50-bits- key		d			
			10	30	80	100
E	0.024	0.067	0.022	0.051	2.945	5.487
D	0.033	0.049	0.026	0.077	2.738	5.794
SP+	\	0.028	0.033	0.002	0.002	0.001
SP-	\	0.029	0.002	0.002	0.002	0.001
U+	\	0.050	0.002	0.019	0.045	0.096
U-	\	0.050	0.018	0.021	0.043	0.098
SP×	0.002	\	0.004	0.015	0.128	0.209
SP÷	0.002	\	0.004	0.015	0.107	0.274
U×	0.021	\	0.055	0.497	8.679	9.345
U÷	0.021	\	0.047	0.495	8.677	9.428
cLen	11	21	44	130	347	427

A. Experimental Statistics

In the experiment, 50-bits-key is used as secret key in unpadded_RSA and Piller. Statistics is listed in Table I in detail. What is a supplementary explanation is that SP_+ represents the addition operation is carried by SP; U denotes User and U_+ marks the addition operation is operated by User. Other symbols not referred here is to be explained analogically.“ E ”,“ D ” and “ cLen ” indicate original Encryption and Decryption operation, cipher-text Length respectively.

B. Analysis of the Statistics

From Table I, the results are discovered as follows. (1). In the case of $d < 10$, the encryption-operation time of OCEVMO is longer than unpadded_RSA [27], [28] and shorter than Piller [29], [30]; as to storing-communication loads, OCEVMO is the biggest among 3 schemes; the theoretic complexity of running and storing-communication are $O(d^2)$ and $O(d)$ respectively. (2). Addition time of OCEVMO and subtraction OCEVMO are equal nearly, while on condition of $d < 100$, the addition-substraction time of OCEVMO is shorter than that of Piller; because the theoretic complexity of running is $O(d)$, the things is to be reversed on condition that d increases to some critical point. (3). Add-subtract output decryption time of OCEVMO is pretty much the same thing, which with the theoretic complexity $O(d^2)$ is shorter than Piller in case of $d < 80$. (4). multiplication-time of OCEVMO and dividing-time OCEVMO are equal nearly, which is far more than that of unpadded_RSA and can be expressed by $O(d^2)$. (5). Multiple-divide output decryption time of OCEVMO is pretty much the same thing too, which is with the theoretic complexity $O(d^3)$ longer than unpadded_RSA .

Taking one with another, OCEVMO is characterized as follows: a favorable encryption performance, a moderate cost time of addition-subtraction while a relatively long cost time of multiplication-division, a burdensome load of storing-communicating, and that the magnitude of each index swells up with the increasing dimension of vector.

VII. Conclusion

Addressed to the question of privacy-securing in cloud computing system, this literature pioneers a cloud computing model supporting privacy-securing and designs An Innovative Encryption Method for Agriculture Intelligent Information System based on Cloud Computing Platform OCEVMO, which realizes 4 operations of numeric data, i.e. addition, subtraction, multiplication and division. Theoretic analysis demonstrates that 4 operations of numeric data OCEVMO is of IND-CCA security in case of the adding factor bigger than 3. Experimental statistics and its estimation proves that OCEVMO is characterized by a better encryption performance, an effective implementation of cipher addition-subtraction, a favorable versatile performance and it is a promising scheme to secure privacy in the course of storing and computing and other Agriculture Intelligent Applications based cloud platform.

On the next research practice, We will focus on how to better the multiplication-division performance of this scheme, and strive to implement multi-time multiple-divide operation, in the meantime to reduce the storing-communication load and further to optimize its versatile performance.

Acknowledgement

This work is funded by Chinese National Natural Science Foundation (61271257, 61102126); Chinese National Science and Technology Support Program (2013BAJ04B04, 2011BAD21B02, 2012BAD52G01); Beijing Natural Science Foundation (4122034); Hunan Provincial Natural Science Foundation of China (12JJ9020); Hunan Provincial Science and Technology Plan(2013GK3135, 2012GK3125); Project of the Education Department of Hunan Province No. 11C0900 and Project of Hunan University of Arts and Science, No. JGYB1223.

The authors also gratefully acknowledge the helpful comments and suggestions from the reviewers, which contribute to a refined paper presentation.

REFERENCES

[1] Wand W C,Li Z W,Owens R; Secure and Efficient Access to outsourced Data,*Proceedings of 2009 ACM Workshop on Cloud Computing Security*, Chichgo, Inninois, USA, pp. 55-55, 2009.

[2] Li, Daoliang; Yang, Simon X; INTELLIGENT AUTOMATION AND CONTROL SYSTEMS FOR AGRICULTURE, *INTELLIGENT AUTOMATION AND SOFT COMPUTING*, Vol. 18, No. 5, pp. 439-441, 2012.

[3] Lukose, Dickson; World Wide Semantic Web of Agriculture Knowledge, *JOURNAL OF INTEGRATIVE AGRICULTURE*,Vol. 11, No. 5, pp. 769-774, 2012.

[4] Peres, Emanuel; Fernandes, Miguel A. ; Morais, Raul; An autonomous intelligent gateway infrastructure for in-field processing in precision viticulture, *COMPUTERS AND ELECTRONICS IN AGRICULTURE*, Vol. 78, No. 2, pp. 176-187, 2011.

[5] Aquino-Santos, Raul; Gonzalez-Potes, Apolinar; Edwards-Block, Arthur;Developing a New Wireless Sensor Network Platform and Its Application in Precision Agriculture, *SENSORS*, Vol. 11, No. 1, pp. 1192-1211, 2011.

[6] Liu Q,Wang G J,Wu J; An effiecent privacy preserving keyword search scheme in cloud computing,*Proceeding of the 12th IEEE International Conference on Computational Scinece and Engineering* , Vancouver, Canada, pp. 715-720, 2009.

[7] Satake, Yuichi; Yamazaki, Tomihiro; Using Food and Agriculture Cloud to Improve Value of Food Chain , *FUJITSU SCIENTIFIC & TECHNICAL JOURNAL*,Vol. 47, No. 4, pp. 378-386, 2011.

[8] LOU Xiao-ping,DAI Jun. Research and implement of a voice encryption method in the trunking communication, *Journal of Hunan University of Arts and Science:Natural Science Edition*, Vol. 20, No. 4, pp. 75-78, 2008.

[9] Bonech D,Crescenzo G D,Ostrovsky R,Public Key Encryption with keyword search ,*Proceedings of the Eurocrypt 2004*, Interlaken, Swizerland, pp. 506-522, 2004.

[10] Muhammad Asif, Nitin Tripathi. Evaluation of OpenID-Based Double-Factor Authentication for Preventing Session Hijacking in Web Applications ,*Journal of Computers*,vol. 7, No. 11. pp. 2623-2628, 2012.

[11] Pang Liao-Jun, Li Hui-Xian, Jiao Li-Cheng, et.al. Design and Analysis of a Provable Secure Multi-Recipient Public Key Encryption Scheme, *Journal of Software*, vol. 20, No.10, pp. 2907-2914, 2009.

[12] ZHANG Xiao-dan;XIAO Xiao-qiang. A Fast Algorithm on Pairs for Elliptic Curve Cryptosystems, *Journal of Hunan University of Arts and Science:Natural Science Edition*, Vol. 21, No. 4, pp. 83-85, 2007.

[13] Yue, Jun; Li, Zhenbo; Liu, Lu; An Improved Ant Colony Algorithm for Agricultural Knowledge Storage Scheduling Under Grid Environment , *SENSOR LETTERS*,Vol. 10, No. 1-2, pp. 562-569, 2012.

[14] Douglas Stebila and Nicolas Theriault. Unified Point Addition Formula and Side-Channel Attacks,*M. CHES, Springer-Verlag*, Berlin,pp.354-368, 2006.

[15] Tan WenXue,Wang XiPing; A novel practical Certificate-Less digital signing system based on super-elliptic bilinear map parings,*Journal of Software*,Vol. 6,No. 8, pp. 1403-1408, August 2011.

[16] PAN Bao-guo; XIAO Xiao-qiang. Parameters estimation of a bilinear model, *Journal of Hunan University of Arts and Science:Natural Science Edition*, Vol. 21, No. 4, pp. 9-12, 2009.

[17] Wang xue-liPei ding-yi; Theory and Implementation On Elliptic and super-Elliptic Curve Cryptography,*Bei Jing-Science Press*,pp. 448-475, 2006.

[18] WenXue Tan , YiYan Fan , XiPing Wang; An Innovative Scalar Multiplication Method Based on Improved m-ary,*Journal of Software*,Vol. 7,No. 11, pp. 2470-2477, 2012.

[19] MENG Yang, FU Guang-sheng. Grover Quantum Algorithm and Security Analysis of DES, *Journal of Hunan University of Arts and Science:Natural Science Edition*, Vol. 18, No. 3, pp. 78-79, 2006.

[20] Marc Joye. Highly Regular Right-to-Left Algorithms for Scalar Multiplication ,*CHES, LNCS 4727,Springer-Verlag,Berlin*, pp. 135-147, 2007.

[21] WenXue Tan,YiYan Fan and XiaoPing Lou; Research on a Novel Point Multiplication Method Based on Addition-Chain of Flexible-Window-Width,*ICIC Express Letters, Part B: Applications*, Vol. 3, No. 2, pp. 297-304, 2012.

[22] Xiangguo Cheng, Shaojie Zhou, Jia Yu, Xin Li, Huiran Ma. A Practical ID-Based Group Signature Scheme,*Journal of Computers*,Vol. 7, No. 11, pp. 2650-2654, 2012.

[23] Liu Duo, Dai Yi-Qi. A New Algorithm of Elliptic Curve Multi-Scalar Multiplication, *Chinese Journal of Computers*, Vol. 31, No. 7, pp. 1113-1137, 2008.

[24] Tan WenXue,Pan MeiSen,Wang XiPing,Shu XiaoHe; A method of security gradation against RSA IEA,*2010 1st ACIS International Symposium on Cryptography, and Network Security, Data Mining and Knowledge Discovery, E-Commerce and Its Applications, and Embedded Systems, CDEE 2010*, Vol. 1, pp. 170-174, 2010.

[25] Zhao Chunjiang, Wu H R, Gao R H. Realistic and Detail Rendering of Village Virtual Scene Based on Pixel Offset,*Applied Mathematics & Information Sciences*, Vol. 6, No. 3, pp.769-775, 2012.

[26] Yvo Desmed, Rosario Gennaroy Kaoru. A new and improved paradigm for hybrid encryption secure against chosen cipher text attack,*Journal of cryptology*, Vol. 23, No. 1,pp. 91-120, 2010.

[27] Gerald R Morris, Khalid H Abed; Mapping Floating-Point Kernels onto High Performance Reconfigurable Computers,*Journal of Computers*,Vol. 8, No. 4, pp. 1340-1344, 2013.

[28] Tan WenXue,Xi JinJu,Wang XiPing; A RSA key security gradating algorithm based on threshold attack time,*Journal of Software*, Vol. 6,No. 9, pp. 1873-1880, 2011.

[29] Huang Ru-Wei,Gui Xiao-Lin,Yu Si,Zhuang Wei;Privacy Preserving Computable Encryption Scheme of Cloud Computing,*Chinese Journal of Computers*,Vol. 34, No. 12, pp. 2391-2402, 2011.

[30] Tang-cenglin, Li-shirong. CI-Section or Maximal Completion of Maximal Subgrops and Solvable Fintte Groups, *Journal of Hunan University of Arts and Science:Natural Science Edition*, Vol. 19, No. 3, pp. 1-4, 2007.

Tan, Wen Xue (1973-). He is a PhD candidate of College of Computer Science, Beijing University of Technology. He graduated with Master's of Science in Information technology and Earth Exploring from East China Institute of technology, Jiang-xi, Mainland of P. R. China,2003. In 2004, he joined Hunan university of Art and Science as a lecturer,being approved and authorized as computer software System Analyst by Chinese Ministry China in 2005, and being promoted to Associate professor and Senior Engineer in 2008. His

current research interests include Agriculture Information Technology and Artificial Intelligence,Cloud Information Security.

Zhao, Chun Jiang (1968-). He is a PhD candidate supervisor of College of Computer Science, Beijing University of Technology, and is a professor of China National Engineering Research Center for Information Technology in Agriculture. He received the Ph.D. degree in agronomy from China Agricultural University, Beijing, China, in 1991. He is currently a Senior Scientist and the Director of the National Engineering Research Center for Information Technology in Agriculture. He is also a Member of the Science and Technology Commission, Ministry of Agriculture, China. He received the Excellent Scientist Award by Ministry of Science and Technology of China in 2001. His research interests include precision farming, intelligent information technology in agriculture, and crop decision support system.

Wu, Hua Rui (1975-). He is a professor of China National Engineering Research Center for Information Technology in Agriculture. He received the Ph.D. degree in Computer Science and Technology from Beijing University of Technology,Beijing, China, in 2010. He is interested in studying Artificial Intelligence. In recent years, he has participated in 18 national and provincial key scientific research projects, and published over 20 academic papers. He got the first prize of Beijing Science and Technology in 2005, and third prize of agricultural technology promotion in 2003. His research interests include Intelligent Information Technology for agriculture.

Wang, Xi Ping (1980-). She is a Graduate of Changsha University of Science and Technology and an Instructor of Hunan University of Arts and Science. She graduated with Bachelors of Marketing from East China Institute of Technology, Jiangxi, China, 2004. Her current research interests include Electronic Commerce and Information Security, Logistic Engineering.