Secure Remote Data Processing in Cloud Computing

Mohd Rizuan Baharon, Qi Shi, David Llewellyn-Jones, and Madjid Merabti

***Abstract*—Cloud computing provides solutions as a service to meet customers' needs such as massive data storage and a lot of computing resources to process customer data efficiently. To fully utilize such services, data need to be outsourced to Cloud Service Providers (CSPs). However, outsourcing precious data to the CSPs could lead to a disaster. Thus, the data need to be protected by means of encryption techniques. Primitive encryption techniques are ineffective to be used as such techniques required decryption process. To overcome such a problem, a fully homomorphic encryption (FHE) scheme is needed as the scheme enables encrypted data to be processed in an encrypted form. There are a number of existing FHE schemes have been proposed and improved upon, but efficiency is still a big obstacle for their implementation. Thus, in this paper, a new fully homomorphic encryption scheme based on finite fields that supports an *n*-multilinear map is proposed. The scheme should support the *n*-multilinear map so as to allow for arbitrary multiplications on encrypted data. Moreover, a new protocol that enables three or more parties to communicate with one another to process data in an encrypted form is proposed in this paper.**

***Index Terms*—Cloud computing, elliptic curve groups, homomorphic encryption, n-multilinear map.**

I. Introduction

Processing data remotely is becoming a hot trend for people to deal with their data recently. This is due to the benefits offered by the advent technology of cloud computing. Cloud Services Providers (CSPs) provide solutions as a service to meet customers' needs such as massive storage spaces and powerful computing resources to store and process their data efficiently. An example of services that provided by the CSPs like HP, is a rendering service. DreamWorks for instance has leveraged services from HP to access a big amount of computing resources to generate 3D frame. HP Media Cloud Solutions have been used to help them to produce animated films like Shrek and Toy Story. Such films require a lot of computing resources for its creation. Thus, the leverage services provided by CSPs enable animated film studios to reduce their upfront costs for servers and manpower as their services are charged on a utility basis [1].

To fully utilize services provided by the CSPs, data need to be outsourced into the CSPs. However, outsourcing precious data to an untrusted third party like a CSP could lead to data disclosure or data misuse by the CSP [2]. Thus, such data need to be protected by means of encryption techniques. Primitive encryption technique like AES is ideal to be used for storage purposes as this encryption technique provides a strong protection to the data in the cloud storage [3]. However, to enable the CSP to process the data, the associated decryption technique needs to be applied first to decrypt the encrypted data. The decryption in the cloud environment by the CSP is not a wise option as it may disclose some sensitive content of the data to the CSP. Furthermore, decrypting in such a way probably could disclose the data to other cloud customers as vulnerabilities exist in the environment [4]. Thus, to enable data to be processed securely in such an environment, a fully homomorphic encryption scheme is believed to be one of the potential solutions as such a scheme allows data to be processed in an encrypted form [5].

Recently, a number of existing fully homomorphic encryption schemes based on Lattices have been proposed and improved upon. Nevertheless, all of them are far from practical as efficiency is still a big obstacle for their implementation. This is due to the amount of noise used at encryption level for security reasons [6]. Managing noise on encrypted data is not an easy task mainly because the process involves many operations such as those in a rendering equation. Typically, the noise is doubled during addition, while increasing exponentially during multiplication [7]. Using a 2D/3D frame as an example, a rendering equation is used to create the frame based on a scene or model. The equation involves additions and multiplications on an input data. To enable some encrypted data to be processed using such an equation efficiently, an encryption technique, which enables arbitrary additions and multiplications with less noise to be performed on the encrypted data, is needed. Such an encryption technique is highly required to allow the data to be rendered by cloud-based applications to produce the 2D/3D frame in the cloud environment.

Additionally, a scheme proposed by Boneh *et al.* [8], which supports a bilinear map, has a limitation as the scheme allows arbitrary additions but just one multiplication on encrypted data. Such a scheme needs to be improved as the scheme is unable to run a process that involves more than one multiplication on encrypted data. Due to such a limitation, a new fully homomorphic encryption scheme based on a finite field that supports an *n*-multilinear map is proposed in this paper. The scheme supports the *n*-multilinear map so as to allow for arbitrary multiplications on encrypted data. Furthermore, a suitable protocol is required to allow a process to be executed by a designated CSP. Thus, a new secure protocol is also proposed in this paper. The protocol enables three or more parties to communicate with one another to get a result of processed data in an encrypted form.

This paper is structured as follows. Section II describes the

Manuscript received February 20, 2013; revised April 27, 2013. This work was supported in part by Liverpool John Moores University, United Kingdom, the Ministry of Higher Education, Malaysia, and University Technical Malaysia Malacca, Malaysia.

B. M. Rizuan, S. Qi, L. J. David, and M. Madjid are with the School of Computing and Mathematical Sciences, Liverpool John Moores University, Liverpool, L3 3AF, United Kingdom (e-mail: M.R.Baharon@2011.ljmu.ac.uk, Q.Shi@ljmu.ac.uk, D.Llewellyn-Jones@ljmu.ac.uk, M.Merabti@ljmu.ac.uk).

DOI: 10.7763/IJCTE.2013.V5.823

contributions of the paper. Some essential concepts used in this paper are summarised in Section III. In Section IV, explanations of some analysis, discussion and preliminaries results will be given. Finally, a conclusion of this paper is provided in Section V.

II. Paper Contribution

The expected key contributions of this paper are summarised in the following points:

1) A new FHE scheme. A new FHE scheme based on a finite field that supports an n-multilinear map is proposed. An elliptic curve EC group is implemented as the underlying group as EC promises high efficiency and strong security. Previous work that supports a bilinear map allows arbitrary additions but only one multiplication. Thus, to achieve arbitrary multiplications on encrypted data, an n-multilinear map will be implemented to the scheme subject to the existence of the generator in the map.
2) A secure data processing protocol. The protocol uses the above proposed FHE scheme to enable a huge amount of sensitive data to be processed securely and efficiently.

III. Background

This section describes several fundamental concepts and definitions that have been used in the proposed scheme.

A. An n-Multilinear Map

Definition of n-Multilinear Map: [9]

Let $G_1, G_2, \dots, G_n$ and G_t be cyclic groups of the same prime order q and $\mathbb{Z}_q^*$ be a finite field that is closed under multiplication operation. n-multilinear groups $G = G_1 = G_2 = \cdots = G_n$ are all isomorphic to one another as they have the same order and are cyclic. An n-multilinear map is a function $e: G_1 \times G_2 \times \dots \times G_n \rightarrow G_t$ such that the following properties are satisfied:

1) For all $a_1, a_2, \dots, a_n \in \mathbb{Z}_q^*$ and $g_1, g_2, \dots, g_n \in G$, $e\left(g_1^{a_1}, g_2^{a_2}, \dots, g_n^{a_n}\right) = e(g_1, g_2, \dots, g_n)^{a_1 a_2 \dots a_n} \in G_t$.
2) The map is non-degenerate: If $g \in G$ generates G then $e(g, g, \dots, g) \in G_t$ generates G_t.

An example of the construction of n-multilinear groups of order n using the Elliptic Curve group is given as below.

An n-multilinear group $G = G_1 = G_2 = \cdots = G_n$ of order n can be constructed as follows:

1) Let $l = 2,$ and $n = 10$ such that n is a square-free integer that is not divisible by 3. A square-free integer is one divisible by no square number, except 1. Then, $q = ln - 1 = 2(10) - 1 = 19$.
2) Let $E_{(1,0)}(F_{19})$: $y^2 = x^3 + x$ defined over a finite field F_{19} be the group of points. The curve has $q + 1 = ln = 20$ points inF_{19}. Thus, there exists a subgroup G in $E_{(1,0)}(F_{19})$ of order 10 since $n = 10$.
3) Let G_t be the subgroup of a finite field that is closed under multiplication, $F_{19^2}^* = F_{361}^*$ of order n. Our aim is to have an n-multilinear map $e: G_1 \times G_2 \times \dots \times G_n \rightarrow G_t$ which includes the admissible n-multilinear map generator.

B. Elliptic Curve over Finite Field F_q

Let $q > 3$ be an odd prime. An EC E over a prime field F_q is defined by an equation of the form:

$$y^2 = x^3 + ax + b$$

where $a, b \in F_q$, and $4a^3 + 27b^2 \not\equiv 0 \bmod q$.

The set $E(F_q)$ consists of all points$(x, y), x \in F_q$, which satisfy the above equation, together with the point at infinity O. The addition of distinct points and doubling a point on the curve can be done through the following algebraic formula. Let P, Q, O, and R be points on a curve $E(F_q)$. Then,

1) $P + O = O + P = P$ For all $P \in E(F_q)$.
2) If $P = (x, y) \in E(F_q)$, then $(x, y) + (x, -y) = O$. (The point $(x, -y)$ is denoted by$-P$, and is called the negative of P).
3) (Point addition) Let $P = (x_1, y_1) \in E\left(F_q\right)$ and $Q = (x_2, y_2) \in E\left(F_q\right)$ where $P \neq \pm Q$. Then $P + Q = R = (x_3, y_3)$, where $x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$ and$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$.
4) (Point doubling) Let$P = (x_1, y_1) \in E(F_q)$, where $P \neq -P$. Then$2P = (x_3, y_3)$, where $x_3 = \left(\frac{3{x_1}^2 + a}{2y_1}\right)^2 - 2x_1$ and $y_3 = \left(\frac{3{x_1}^2 + a}{2y_1}\right)(x_1 - x_3) - y_1$.

C. Working Example:

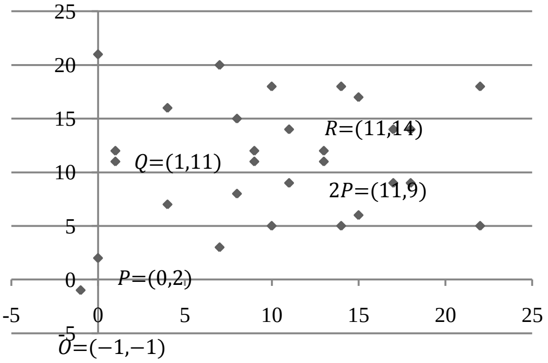


Fig. 1. Elliptic curve group over F_{23}, $E(F_{23})$.

Point addition and doubling can be computed as below, where the results of computation are as illustrated in Fig. 1.

1) Point Addition

Let $P = (0,2)$ and $Q = (1,11) \in E_{(1,4)}(F_{23})$ where $P \neq \pm Q$. Then $P + Q = R = (x_3, y_3)$, where

$$x_3 = \left(\frac{11-2}{1-0}\right)^2 - 0 - 1 = 11,$$

$$y_3 = \left(\frac{11-2}{1-0}\right)(0 - 11) - 2 = 14.$$

Thus, $R = (11,14) \in E_{(1,4)}(F_{23})$.

2) Point Doubling

Let $P = (0,2) \in E_{(1,4)}(F_{23})$, where $P \neq -P$. Then $2P = (x_3, y_3)$, where

$$x_3 = \left(\frac{3(0)^2+1}{2(2)}\right)^2 - 2(0) = 11,$$

$$y_3 = \left(\frac{3(0)^2+1}{2(2)}\right)(0 - 11) - 2 = 9.$$

Thus, $2P = (11,9) \in E_{(1,4)}(F_{23})$.

IV. The Proposed Scheme and Protocol

This section describes the proposed scheme and its related processes. This section also provides the proposed protocol together with its descriptions.

A. *The Proposed Scheme*

Let $m \in \{0,1\}$ be a plaintext, c be a ciphertext, $g \in G$ be a generator of $G, r \in \mathbb{Z}$, and $h = g^{\alpha q_2}$ such that α, and $q_2 \in \mathbb{Z}$. Then

1) Encryption: $c(m) = g^m h^r$.

2) Decryption: $m = c^{-1}(c(m)) = log_{g^{q_1}} c^{q_1}(m) = log_{g^{q_1}}(g^m h^r)^{q_1} = log_{g^{q_1}}(g^{q_1})^m$.

B. *Scheme Requirements*

The scheme should hold such properties:

1. Homomorphic under $*$ operations.

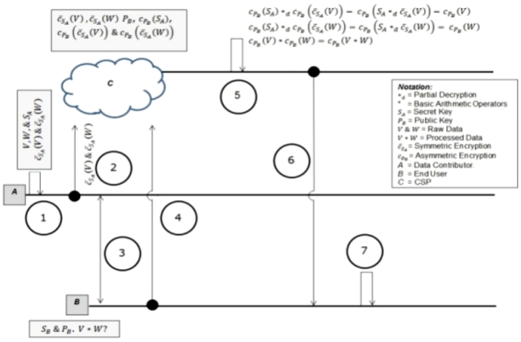
- $C = \sum_{i=1}^{n} c_i = \prod_{i=1}^{n} c_i \, h^r$ is homomorphic under addition.
- $C = \prod_{i=1}^{n} c_i$ is homomorphic under multiplication.

2. Double layer encryption.

To ensure the privacy of the outsource data is preserved.

C. *Basic Description Protocol*

The protocol is illustrated in Fig. 2, and its steps are explained below.



$\bar{c}_{S_A}(V), \bar{c}_{S_A}(W)\ P_B, c_{P_B}(S_A),$
$c_{P_B}(\bar{c}_{S_A}(V))\ \&\ c_{P_B}(\bar{c}_{S_A}(W))$
$c_{P_B}(S_A) *_d c_{P_B}(\bar{c}_{S_A}(V)) - c_{P_B}(S_A *_d \bar{c}_{S_A}(V)) - c_{P_B}(V)$
$c_{P_B}(S_A) *_d c_{P_B}(\bar{c}_{S_A}(W)) - c_{P_B}(S_A *_d \bar{c}_{S_A}(W)) - c_{P_B}(W)$
$c_{P_B}(V) * c_{P_B}(W) = c_{P_B}(V * W)$
C
$V, W, \& S_A$
$\bar{c}_{S_A}(V) \& \bar{c}_{S_A}(W)$
$\bar{c}_{S_A}(V) \& \bar{c}_{S_A}(W)$
Notation:
$*_d$ = Partial Decryption
$*$ = Basic Arithmetic Operators
S_A = Secret Key
P_B = Public Key
V & W = Raw Data
$V * W$ = Processed Data
$\bar{c}_{S_A}$ = Symmetric Encryption
c_{P_B} = Asymmetric Encryption
A = Data Contributor
B = End User
C = CSP
A
B
1
2
3
4
5
6
7
$S_B \& P_B. V * W?$

Fig. 2. The protocol.

1) A creates raw data $V = v_i \in \{0,1\}$, $W = w_i \in \{0,1\}$ for $i = 1, 2, .., n$ and secret key S_A . Then, A encrypts V and W usingS_A.
2) A sends $\bar{c}_{S_A}(V)$ and $\bar{c}_{S_A}(W)$ to C.
3) A encrypts S_A using P_B. A sends $c_{P_B}(S_A)$ to B to enable B to decrypt the processed result.
4) B requests C to re-encrypt $\bar{c}_{S_A}(V)$ and $\bar{c}_{S_A}(W)$ using P_B. Then, B sends $c_{P_B}(S_A)$ and instructions to C for processing on $c_{P_B}\left(\bar{c}_{S_A}(V)\right)$ and$c_{P_B}\left(\bar{c}_{S_A}(W)\right)$.
5) C re-encrypts $\bar{c}_{S_A}(V)$ and $\bar{c}_{S_A}(W)$ using P_B and run processes called partial decryption process:

$$c_{P_B}(S_A) *_d c_{P_B}\left(\bar{c}_{S_A}(V)\right) = c_{P_B}\left(S_A *_d \bar{c}_{S_A}(V)\right) = c_{P_B}(V).$$

$$c_{P_B}(S_A) *_d c_{P_B}\left(\bar{c}_{S_A}(W)\right) = c_{P_B}\left(S_A *_d \bar{c}_{S_A}(W)\right) = c_{P_B}(W).$$

Definition of $*_d$:

Let a and b be integers such that a is a secret key to encrypt x and $b = c_a(x)$ is a ciphertext. Then, $a *_d b = c_a^{-1}(b) = x$.

Then, the process on $c_{P_B}(V)$ and $c_{P_B}(W)$ is executed to produce $c_{P_B}(V * W)$.

1) C sends the result $c_{P_B}(V * W)$ to B.
2) B decrypts the result using S_B to recover $V * W$.

V. The Preliminary Results

The preliminary results based on performance of the encryption/decryption process proposed in the previous section have been summarised in Table I.

TABLE I: Performance Analysis of Encryption/Decryption Process

Performer	Tasks	Method	Perfor mance	Descriptions/R esults
A	Encrypts raw data (V and W) using S_A	Symmetric encryption scheme	Fast	$\bar{c}_{S_A}(V)$, and $\bar{c}_{S_A}(W)$
	Encrypts $S_A$using P_B	The proposed scheme /asymmetric	Fast	The key size is short. $c_{P_B}(S_A)$.
B	Decrypts $c_{P_B}(S_A)$ using S_B.	The proposed scheme /asymmetric	Fast	The key size is short. $d_{S_B}(c_{P_B}(S_A)) = S_A$.
	Decrypts $c_{P_B}(V * W)$ using S_B		Fast/ Slow	It is depends on the size of the output. $V * W$.
C	Re-encrypts $\bar{c}_{S_A}(V)$, and $\bar{c}_{S_A}(W)$ using P_B	The proposed scheme /asymmetric	Fast	$c_{P_B}(\bar{c}_{S_A}(V))$, and $c_{P_B}(\bar{c}_{S_A}(W))$
	Run a partial decryption process		Fast	$c_{P_B}(S_A) *_d c_{P_B}\left(\bar{c}_{S_A}(V)\right) = c_{P_B}\left(S_A *_d \bar{c}_{S_A}(V\right.$ $= c_{P_B}(V)$. $c_{P_B}(S_A) *_d c_{P_B}\left(\bar{c}_{S_A}(W)\right) = c_{P_B}\left(S_A *_d \bar{c}_{S_A}(W\right.$ $= c_{P_B}(W)$.

VI. Conclusion

A new FHE scheme for processing remote data in an encrypted form has been proposed in this paper. The EC group is implemented as the underlying group due to EC's promising efficiency, and also an *n*-multilinear map should be supported by the scheme to achieve the fully homomorphic properties. The proposed scheme is implemented in a process that requires arbitrary additions and multiplications such as a rendering process to check the ability of the proposed scheme to compute arbitrary additions and multiplications on encrypted data. The security of data encrypted and processed using the proposed protocol is guaranteed in cloud environments due to no information disclosed at any stage. Further works of this paper will be looking at the generator of an *n*-multilinear map. Furthermore, various ways will be investigated to prove that the generator exists in the map and can be computed efficiently.

REFERENCES

[1] H. P. Enterprise and C. Services, "Moving media and entertainment to the cloud," *HP Enterprise Cloud Services*, pp. 1–8, 2011.

[2] Y. Shen, W. Cui, Q. Li, and Y. Shi, "Hybrid fragmentation to preserve data privacy for saas," presented at 2011 Eighth Web Information Systems and Applications Conference, pp. 3–6, Oct. 2011.

[3] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, Jan. 2011.

[4] S. Sengupta, V. Kaulgud, and V. S. Sharma, "Cloud computing security-trends and research directions," *2011 IEEE World Congress on Services*, pp. 524–531, Jul. 2011.

[5] M. Van Dijk and C. Gentry, *Fully Homomorphic Encryption over the Integers*, 2010, pp. 1–28.

[6] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) fully homomorphic encryption without bootstrapping," in *Proc. of the 3rd Innovations in Theoretical Computer Science Conf. on - ITCS '12*, 2012, pp. 309–325.

[7] J. Fan and F. Vercauteren, "Somewhat Practical Fully Homomorphic Encryption," in *IACR Cryptology ePrint Archive*, 2012.

[8] D. Boneh, "Evaluating 2-DNF formulas on ciphertexts," in *Cambridge Proc. Second Theory of Cryptography Conf.*, 2005, pp. 325–341.

[9] C. Papamanthou, R. Tamassia, and N. Triandopoulos, "Optimal authenticated data structures with multilinear forms," in *Proc. of the 4th international conf. on Pairing-based Cryptography*, 2010, pp. 246–264.

Mohd Rizuan Baharon was born in Malacca, Malaysia in April 3, 1981. He received his bachelor degree in Mathemtics i.e. BSc. in Mathematics (Industrial Mathematics) from University Technology Malaysia, Malaysia in 2004. In 2006, he completed his master degree i.e. MSc. in Mathematics from the same university. Currently, he is a second year Ph.D. student at Liverpool John Moores University, United Kindom. He is doing research on computer network security and cryptography.

He has been employed by University Technical Malaysia Malacca as a lecturer from 2006 until recent. He is in the Faculty of Information and Communication Technology. He teached Mathematical subjects such as Linear Algebra, Calculus and Differential Equations. He also teached Computer Science subjects like Data Communication and Introduction to IT. He has published a couple of research papers either at national and international conferences. The conferences include the 13th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting, Liverpool, UK in 2012, the Second International Cryptology Conference (Cryptology2010), and The 3rd IMT-GT conference in 2007.

Mr. Baharon is a member of Mathematical and Sciences Society Malaysia, PERSAMA since 2004.

Qi Shi is a professor in Computer Security at Liverpool John Moores University in the School of Computing and Mathematical Sciences. Currently, he is the head of Research of the School. His research is centred on the increasingly important theme of ubiquitous/distributed computing security and privacy with the long-term goal of developing general frameworks for the intelligent provision of security and privacy protection to various applications in ubiquitous computing environments. Specifically, his main research interests include the areas of cryptographic protocol design, system-of-systems security, formal security models, intrusion and denial-of-service detection, sensor network security, identity management and computer. He has published over 130 papers in journals and conference proceedings in these areas.

He has supervised a number of funded research projects. The most recent project is a large EU project ANIKETOS with a total funding of €10 million and a duration of 3.5 years from August 2010, involving 17 project partners from 10 EU countries, to develop secure and trustworthy composite Internet services.

Qi Shi is a member of the PROTECT Research Centre for Critical Infrastructure Protection.

David Llewellyn-Jone originally studied Mathematics and Philosophy at St. Peter's College, part of the University of Oxford. Having completed his degree in 1998, he then went on to do a Ph.D. in Mathematical Logic and Model theory at the University of Birmingham under the supervision of Richard. His Ph.D. thesis involved a particular area of mathematics called model theory. He has over 10 years' experience in teaching and conducting research in computer and network security. Currently, he is Reader in Computer Security in the School of Computing and Mathematical Sciences at Liverpool John Moores University. His research interests include network security, secure component composition, networks and ubiquitous computing, networked appliances, code analysis and digital rights management. He has over 80 publications in these areas.

He was Research Fellow at Liverpool John Moores University from February 2006 to August 2010. From February 2003 to February 2006, he was a research assistant at Liverpool John Moores University. He was working on the EPSRC funded project "Secure Component Composition for Personal Ubiquitous Computing". From October 2001 to February 2003, he was a programmer at Codemasters. He was working on Pro Race Driver/TOCA Race Driver/DTM Race Driver computer game.

Madjid Merabti is a graduate of Lancaster University, UK. He has over 20 years' experience in conducting research and teaching in Distributed Multimedia Systems (Networks, Operating Systems, and Computer Security). Currently, he is the director of the School of Computing & Mathematical Sciences, a professor of Networked Systems at Liverpool John Moores University, and the director of the PROTECT Research Centre.

He has over 160 publications in these areas and a number of government and industry supported research projects in the areas: Multimedia Networking, Human Digital Life Memories Systems, Games Technology, Mobile and Wireless Networks, Networked Appliances, Sensor Networks, Intrusion Detection, Computer Forensic, and Network Security Architectures.

Merabti has been elected as an IEEE Distinguished lecturer 2011–2013 in networking and security, presenting a series of lectures in the UK, Brazil and the Middle East. He was invited to assist with the IEEE's worldwide Public Visibility efforts in security and mobile devices. Merabti actively participates in the research community in the UK and abroad, including being an EPSRC Peer Review College member, an EPSRC Funding Panel member for UK Communications Research, and an international reviewer for a number of research councils in countries such as France, the Netherlands, Qatar State, Switzerland and Canada. He was awarded a Peru-Honorary Professorship in 2005.