International Journal of Academic Studies International Journal of Academic Studies On theory and applications of mathematics to security in cloud computing: a case of addition-com...

Article · April 2016

CITATION
1

READS
12

2 authors, including:

Richard Omollo
Jaramogi Oginga Odinga University of Science and Technology
8 PUBLICATIONS **7** CITATIONS

SEE PROFILE

Inter. J. Acad. Stud. 2(4): (2016) 207-217
Journal home page: www.ijacademicstudies.com

International Journal of Academic Studies

On theory and applications of mathematics to security in cloud computing: a case of addition-composition fully homomorphic encryption scheme

Richard O. Omollo[a,*], **N. B. Okelo**[b]

[a]School of mathematics and Innovative Systems, Jaramogi Oginga Odinga University of Science and Technology, Box 210-40601, Bondo-Kenya

[b]School of mathematics and Actuarial science, Jaramogi Oginga Odinga University of Science and Technology, Box 210-40601, Bondo-Kenya.

[*]*Corresponding author*: James O. Yambo; *e-mail:* bnyaare@yahoo.com;

ARTICLE INFO

Article history:

Received 20th Mars 2016

Received in revised form 10th April 2016

Accepted 12th April 2016

Key words:

Homomorphism
Encryption
Addition
Composition
Cloud computing

ABSTRACT

Addition-Composition Fully Homomorphic Encryption is given in this paper to solve data security equation in cloud computation. An earlier attempt to solve security problem has been proposed by Craig Gentry, who combined additive and multiplicative operations, using lattice-based cryptography. Its construction started as a somewhat homomorphic encryption scheme that evaluates low-degree polynomials over encrypted data. He then modified it to make it bootstrappable and showed that any bootstrappable fully homomorphic encryption scheme can be converted into a fully homomorphic encryption. Subsequent efforts to improve on Craig's work still favor his approach, i.e. bootstrapping homomorphic cryptosystems with noisy ciphertexts into fully homomorphic cryptosystems. The approach in the design of the scheme in this paper is based on combining additive and composition properties making it complex to compromise. Finally, the scheme enables secure computation of cloud data without exposing it to deliberate risk.

1. Introduction

According to TechSoup Global Network (2012) survey results on cloud computing, over 90% were using cloud computing while 79% of the remaining intended to migrate to cloud services. Ateyaro & Feyisetan (2011), Rachana & Guruprasad (2014) and Gnanavelu & Gunasekaran (2014) in their respective researches showed that data security is one major security concern for cloud computing. In analyzing cloud security issues, it has been concluded that the success of its adoption depends on the

benefits to risk and threat ratio. Researchers have focused on access controls as a measure to boost cloud computing adoptability by consumers. They proposed use of digital ID's for consumers to minimize unauthorized access and address non-repudiation issues in cloud computing services. In addressing unauthorized access and tampering, Sasidharan *et al.*, (2011) proposed data-centric encryption security approach. Tiwari & Mishra (2012) in their research recommended that developers should develop applications that provide encrypted data for security in cloud computing. Gonzalez *et al.*, (2012) in their work carried a quantitative analysis of current security concerns in cloud computing and found out that there is still need to address those related to secure virtualization. Naruchitparames & Gunes (2013) addressed security of data on transit through blind processing whereas Gupta *et al.*, (2011) used block cipher method to propose hyper modern cryptography algorithm for confidentiality and integrity of data through data encryption but noted that encryption methods are easy to break especially when a key is used several times in encryption. Kaur (2012), Tebaa *et al.*, (2013) and Gomathisankaran (2012) proposed the use of Fully Homomorphic Encryption scheme as an effective solution to cloud computing security. In all these research attempts, cryptography is appreciated as better solutions to cloud architecture security challenges. Ravindran & Kaplana (2011) analyzed and recommended improvement on Fully Homomorphic Encryption for applications on cloud computing. However, the application of Fully Homomorphic Encryption experiences implementation defect due to its computational strain onto network and storage resources.

2. Preliminaries

In order to understand the derivation in this paper, we need the following fundamental concepts.

Definition 2. 1 If (G,*) and (H,$\circ$) are groups, then a function f:G$\rightarrow$H is a homomorphism if

$$f(x,y) = f(x)f(y) \qquad \forall x, y \in G$$

Definition 2.2 Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Remark 2.3 This study describes a new technique of addition-Composition Homomorphic Encryption which has never been done in literature. There are Three Address Codes which are description of a series of strings for example $\alpha_1 = aopb$ where $\alpha 1, a, b$ names of parameters are while *op* is a random operator. Normally we have two operations.

We can express them as follows:

$$\delta_1 = a \bullet b$$

$$\delta_2 = a + \delta_1$$

Where δ_1 and δ_2 are temporary variables formed by the compiler.

Definition 2.4 (Mixed-Multiplicative Homomorphic Encryption)

We consider a large number *n* such that n = $l \bullet$ k where *l* and *k* are large prime numbers. We adopt the following notations:

$Z_l = \{a: a \leq l\}$ the set of original plain text messages

$Z_n = \{a: a < n\}$ the set of cipher text message

$Q_l = \{b: b$ is not an element of $Z_l\}$ set of encryption dues

Here the simple encryption is as follows (Updhaye & Khot, 2013);

If y is encrypted as $y = E_l(a) \equiv b \bmod n$ then we can achieve it by picking a random number r and creating b = a + rl. So if the encryption y is a number of Z_n then we use the key *l* to recover a $D_p(y) \equiv y \bmod l$.

Example 2.5 Let l = 17, k=13, n=221=l $\bullet$ k and a_1=8 and E(8)=59, a_2=2 where E(2)=36. Now (59x36) mod 221 = 135. Decrypting 135 yields l = 135 mod 17. This is similar to $a_1 \bullet a_2 = 2 \bullet 8 = 16$.

Definition 2.6 Let V be a vector space a non-negative real-valued function $\| \ \|: V \to \Re$ is called a norm if the following conditions are satisfied:

(1) $\|x\| \geq 0$ and $\|x\| = 0$ if and only if x=0 $\forall$ x$\in$ V

(2) $\|x\| = |\lambda| \, \|x\| \ \forall x \in V$ and $\lambda \in K$

(3) $\|x + y\| \leq \|x\| + \|y\| \ \forall$ x,y$\in$ V

Remark: 2.7 We treated the members of V in a probabilistic sense that is without loss of generality.

Definition 2.8 A family H of hash functions h: $X \to Y$ is ε-pairwise independent if

$$\sum_{x \neq x'} (\Pr_{h \leftarrow H}[h(x) = h(x') - \frac{1}{|Y|}) \leq |X^2| \bullet \frac{\varepsilon}{|Y|}$$

Remark 2.9 A necessary and sufficient condition here is that the collision probability $\Pr_{h\leftarrow H}[h(x)=h(x')]$ should be at most $\frac{(1+\varepsilon)}{|Y|}$ on average with an infinitesimally small ε since $\frac{2}{|Y|}$ is not good enough.

Definition 2. 10 Let f(x) and g(x) be two polynomials such that $f(x):A\rightarrow B$ and $g(x):B\rightarrow C$ where A, B, C are arbitrary rings. Then the composition of f(x) and g(x) is well defined and given by $g(x)\circ f(x) = (g\circ f)(x) = g(f(x)) \quad \forall\ x \in A$.

Example 2.11 Let f(x) = 3x+1 and g(x) =x-2. Clearly, $(g\circ f)(x) = 3x-1$.

Definition 2.12 Consider two ciphers ψ and φ. We define addition-composition homomorphic encryption by $\eta(\psi\oplus\varphi)=\eta(\psi)\circ\eta(\varphi)$ where $\circ$ is a composite function and $\oplus$ is an additive function.

Definition 2.13 Given two groups G_1 and G_2, we say G_1 is orthogonal to G_2 if $<G_1,G_2>=0$. We note that taking $G_1^s = \hat{G}(C)\lambda c$ where $\lambda c = \Theta_{i\in C}x_i$ we can consider the orthogonality aspect. First we consider Parsevals equality. $\sum_{c\leq[l]}\hat{G}(c)^2 = E_x[G(x)^2]$.

3. Results and Discussions

First we give some preliminaries before we move to the main results.

Lemma 3.1 For all $a\in Z_l$, $D_l(E_l(a)) = a$ is true.

Proof: Let $y = E_l(a)$ and b be the random number used for the message encryption. It is clear that b mod n = y ……..……..(1)

Now, since l divides n equation (1) implies that y mod l = (b mod n) mod p =a, for all prime numbers p.

Example 3.2: Let l = 11, k = 7, n = 77 = l•k and a_1 = 5 where E(5) = 38 and a_2 = 2 where E(2) = 13 clearly (38x13) mod 77 = 32. When we decrypt 32 we obtain 10 = 32 mod 11.

Lemma 3.2 For all $s, t \in Z_l$, D(E(s)t) = D(E(st))…..……..……..(2)

Proof : We first give E(s)t and E(st) a critical look since multiplication is defined pointwise. E(s)t: To do the encryption of S we first choose a_1 such that $s \equiv a_1 \bmod l$ i.e. $a_1 = \beta_1 l+s$. Encrypting, we obtain $y_1 \equiv a_1 \bmod n$ and hence $a_1 = \beta_2 n + y_1$. Therefore $\beta_1 l + s = \beta_2 n + y_1$ and solving for y_1 we obtain $y_1 = \beta_1 l - \beta_2 n + s = (\beta_1 - \beta_2 k)l + s$ ……..……(3)

Now since E(s) = y_1 and E(s)t = y_1t we have $y_1t = (t\beta_1 - t\beta_2 k)l + ts$ which when you decrypt you obtain $D(E(s)t) = D(y_1t) = y_1t \bmod l = st$ ..……..……(4)

E(st): To encrypt st we choose a_2 such that $st = a_2 \bmod l$ where $a_2 = \beta_2 l + st$. We then encrypt st as $y_2 = a_2 \bmod n \Rightarrow a_2 = \beta_4 n + y_2$. Solving for y_2 we obtain $y_2 = (\beta_3 - \beta_4 k)l + st$ which when decrypted yields $D(E(st)) = D(y_2)y_2 \bmod l = st$ ……...…….……(5)

Now D(E(st)) = D(E(s)t) from Eqn. 4 and Eqn. 5. Hence $y_1t \bmod l = st = y_2 \bmod p \Rightarrow$ D(E(s)t) = D(E(s)t) with modulus l. This completes the proof.

For computation of the main result we need the following concepts.

Lemma 3.3

Take a real number x from the set y(k_1, ……..,k_m) then any ciphertext C from C(k_1,……..,k_m) can be correctly decrypted by the algorithm C - $[cx/l]$. For proof see (Craig, 2009).

At this point we need to discuss the Gentry Scheme and its implementation (Coron et al, 2011). For understanding $\lceil x \rceil$ means rounding up of x, $\lfloor x \rfloor$ means rounding down x and $[x]$ rounding x to the nearest integer.

Lemma 3.4 A family H of hash functions $h: X \to Y$ is pairwise independent if for all $x \neq x'$, it holds that $Pr_h[h(x) = h(x')] = 1/|Y|$. Now it is obvious that h' is not exactly pairwise independent therefore a general definition is necessary. For proof see (Coron, 2011), Lemma 6.

Theorem 3.5 Let H be a family of $\varepsilon -$ pairwise independent hash functions. Suppose that $h \leftarrow H$ and $x \leftarrow X$ are chosen uniformly and independently. Then (h, h(x)) is ($\frac{1}{2}\sqrt{|Y|/|X| + \varepsilon) -}$ uniform over H x Y.

Proof : Let $p \in \Re^{HxY}$ denote the probability vector corresponding to a random choice of $x \in X$ and $h \in H$. We must show that: $|p - 1|_1 \leq \sqrt{|H| \bullet |Y|} \cdot \|p - 1\|_2 = \sqrt{|H|.|Y|} \sqrt{\|p\|\frac{2}{2} - \|1\|\frac{2}{2}}$

We have $\|1\|\frac{2}{2} = 1/(|H|.|Y|)$ and by Parseval's equality

$$\|p\|\frac{2}{2} = \sum_{(h',y)\in HxY} \Pr_{(h,x)\leftarrow HxX}[h = h'; h(x) = y]^2 = \frac{1}{|H|^2} \sum_{(h,y)\in HxY} \Pr_{x\leftarrow X}[h(x) = y]^2$$

$$= \frac{1}{|H|^2} \sum_{(h,y)\in HxX} (\frac{1}{|X|^2} \sum_{(x,x')\in X^2} 1_{h(x)=y})^2 = \frac{1}{|H|^2.|X|^2} \sum_{(x,x')\in X^2} \sum_{h\in H} 1_{h(x)=h(x')}$$

$$= \frac{1}{|H|.|X|^2} \sum_{(x,x')\in X^2} \Pr_{h\leftarrow H}[h(x) = h(x')] = \frac{1}{|H|.|X|} + \frac{1}{|H|.|X|^2} \sum_{x\neq x'} \Pr_{h\leftarrow H}[h(x) = h(x')] \leq \frac{1}{|H|.|X|} + \frac{1+\varepsilon}{|H|.|Y|}$$

Hence, the statistical distance is bounded as:

$$|p-1|_1 \leq \sqrt{|H|.|Y|}\sqrt{\frac{1}{|H|.|X|} + \frac{1+\varepsilon}{|H|.|Y|} - \frac{1}{|H|.|Y|}} = \sqrt{\frac{|Y|}{|X|} + \varepsilon}$$ as desired.

Theorem 3.6 For an odd prime integer q, the hash function family H is ε-pairwise independent, with: $\varepsilon = \frac{1}{q} + \frac{\beta^2}{2^{\alpha\beta^2 - 2(\alpha+1)\beta}}$.

Proof: For each choice of $b \neq b'$, the probability $\Pr_{h\leftarrow H}[h(b) = h(b')]$ can be expressed in terms of the number of zeros of a certain hyperbolic quadratic form in $Z_q^{2\beta}$. More precisely let A=(a_{ij}) be the $\beta x\beta$ matrix in $M_\beta(Z_q)$ given by $a_{ij} = b_{ij} - b'_{ij}$. We have:

$$\Pr_h[h(b) = h(b')] = \frac{1}{q^{2\beta}} \#\{(u_1,....., u_\beta, v_1,....., v_\beta) \in Z_q^{2\beta} : \sum_{1\leq i,j\leq\beta} a_{ij}u_i v_j = 0\}$$

Now the quadratic form Q = $\sum_{1\leq i,j\leq\beta} a_{ij}u_i v_j$ has the matrix $\frac{1}{2}\begin{pmatrix} 0 & A \\ A^T & 0 \end{pmatrix}$, which is clearly conjugate to $\frac{1}{2}\begin{pmatrix} 0 & J \\ J & 0 \end{pmatrix}$ where J is the canonical row echelon form of A. It follows that Q is the orthogonal sum of *r* hyperbolic planes, with *r* the rank of A. Hence, its number of zeros is well-known:

$$\#\{(u_1,....., u_\beta, v_1,....., v_\beta) \in Z_q^{2\beta} : \sum_{1\leq i,j\leq\beta} a_{ij}u_i v_j = 0\} = q^{2\beta-1} + q^{2\beta-r} - q^{2\beta-r-1}$$

In particular, we get: $\Pr_h[h(b) = h(b')] - \frac{1}{q} \leq \frac{1}{q^r}$

This estimate is quite sufficient for our purposes, except in the case where r = 1. Therefore, we need to bound the number of pairs (b, b') such that the corresponding matrix A is of rank 1. Noting that A has all its entries in $-2^{\alpha}+1,.....,2^{\alpha}-1,$ it is enough to bound the cardinality of the set U_{α} of matrices of rank 1 in $M_{\beta}(Z_q)$ with entries in that interval. To do so, note that a matrix of rank 1 with a nonzero upper-left entry is entirely determined by its first line and its first column. If the entries are in $\{-2^{\alpha}+1,.....,2^{\alpha}-1\}$, this leaves $2^{\alpha+1}-2$ choices for the upper-left entries and $(2^{\alpha+1}-1)^{2\beta-2}$ choices for the remainder of the first line and the first column. Hence, there are less than $2^{2(\alpha+1)(\beta-1)}$ matrices in U_{α} with a nonzero upper-left entry (and usually much fewer, since not all first lines and first columns need to give rise to matrices with all their entries in the proper interval). The same argument can be applied to any other nonzero entry (i,j), leading to the coarse bound: $|U_x| < \beta^2.2^{2(\alpha+1)\beta}$. Now, the number of pairs (b,b') such that the corresponding matrix A is of rank 1 is at most $|X|.|U_x|$, since for any choice of b, there are at most $|U_x|$ possible values of b' such that A is in U_{α}. We can thus bound the value δ defined by:

$$\delta = \frac{|Y|}{|X|^2}\sum_{b\neq b'}(\Pr_h[h(b)=h(b')]-\frac{1}{|Y|})$$

as required. Indeed:

$$\delta = \frac{q}{|X|^2}\sum_{b\neq b'}(\Pr_h[h(b)=h(b')]-\frac{1}{q}) \leq \frac{q}{|X|^2}(\sum_{\substack{b\neq b'\\ A\notin U_\alpha}}\frac{1}{q^2}+\sum_{\substack{b\neq b'\\ A\in U_\alpha}}\frac{1}{q})$$

$$\leq \frac{q}{|X|^2}(\frac{|X|^2}{q^2}+\frac{|X|.|U_\alpha|}{q}) \leq \frac{1}{q}+\frac{|U_\alpha|}{|X|} \leq \frac{1}{q}+\frac{\beta^2}{2^{\alpha\beta^2-2(\alpha+1)\beta}}$$

Theorem 3.7 Let K be a field and π the principal ideal. Consider p, $\alpha \in \pi$. Then w(x) = $\delta(x) \circ$ v(x) over K such that $\|\delta(x)\|_{\infty} \leq \sqrt{j_k(4/3)^{(3k-1)/4}\beta_k}^{n/2k-1}$, for all xin K and w, v and δ in π.

Proof: Since α is a root of $f_n(x) = x^n + 1$ modulo p so $x^n + 1 = (x-\alpha) \circ g(x) \bmod p$. Without loss of generality we assume that $g(x) = x^{n-1} + g_{n-2}x^{n-2} + \ldots\ldots + g_0$. Hence, we obtain the following lattice $\begin{bmatrix} g_0 & g_1 & . & 1 \\ -1 & g_0 & . & g_{n-2} \\ . & . & . & . \\ 0 & 0 & . & p \end{bmatrix}$

We need to reduce this lattice. To do this we invoke the lattice reduction algorithm and we obtain w(x) = $\delta(x) \circ v(x)$ such that equality (5) holds. Moreover $w(x) \in \Re$ since $u(x) \circ v(x) = p \bmod f_n(x)$.

Example 3.8 Let n=4, u(x)=159+8x+4x^2+2x^3=[159 8 4 2], p=641407153, v(x)=4027071-204800x-91520x^2-40898x^3. u(x) and $f_4(x)=1+x^4$ are factored as follows:

[159 8 4 2] = 2*[[[26912186 1]1][[91823081 1]1]]mod641407153

[1 0 0 0 1] = [[[26912186 1]1][[91823081 1]1]]mod641407153

So, $\alpha = p - 26912186 = 614494967$ and the public key is $pk = (p, \alpha)$. According to pk, one computes g(x) = [382839894 343459750 614494967 1]. To obtain w(x), one constructs lattice M and calls the LLL algorithm for M. In fact, one finds the exact solution v(x) for this small example. Without loss of generality, assume $w(x) = \delta(x)v(x) = [4896893\ 3824893\ 4303943\ 15954106]$. To be simplicity, we compute $a^2 \bmod p = 343459750$ and $a^3 \bmod p = 382839894$.

To find $[\delta(x)]_2$, one first computes a ciphertext

$$\begin{aligned} c &= a(x)(\alpha) = (2r(x) + m(x)(\alpha) \bmod (p) \\ &= (3*382839894 + 4*343459750 + 5*614494967 + 9) \bmod (p) \\ &= 463576302 \\ d &= \lfloor 463576302/\ px[4896893382\ 4893430394\ 15954106] + [0.5\ 0.5\ 0.5\ 0.5] \rfloor \\ &= [3539224 - 2764437311\ 0670115308\ 12] \end{aligned}$$

Since $d \bmod 2 = [\delta(x)]_2\, x[a(x)]_2 \bmod 2, [\delta(x)]_2 = d \bmod 2x([a(x)]_2)^{-1} \bmod 2 = [1\ 1\ 1\ 0]$

Thus, one decrypts a ciphertext by using equivalent secret key w(x),[δ (x)] $_2$.

Let R = Z[x]/$\phi(x)$ where $\phi(x)$ is irreducible over Q[x] but factor modulo t. If ϕ splits exactly into r distinct irreducible factors of degree g = n/r = $\varphi(d)/r$ i.e. $\phi(x) = \prod_{j=1}^{r} j_j(x)$. Then by Chinese Remainder Theorem, the following $R_t \cong Z_t[x]/ (f_1(x) \otimes \ldots\ldots \otimes Z_t[x]/f_r(x))$ is a natural isomorphism which is obtained. In particular this helps to add and multiply in parallel. In our new technique we obtain the addition-composition via tensor products as shown in the main results below.

Lemma 3. 9 Generally, $\eta(\sum_{i=1}^{m} \chi_i) := \Theta\eta(\chi_i) \quad \forall m \in N = Z^+$

Proof: Definition is well posed and defined. To see this consider θ and τ and $z \in Z^+$ where z=Z.

So $\theta = \lambda^x \circ \alpha_1^y \bmod n^2$

$\tau = \lambda^k \circ \alpha_2^y \bmod n^2$

$\theta \circ \tau = \lambda^x \alpha_1^y \circ \lambda^k \alpha_2 \bmod n$

$= \lambda^{x+k} \circ (\alpha_1 \alpha_2)^y \bmod n^2$

So $\theta_1 \circ \theta_2 \circ \ldots\ldots\ldots\ldots \circ \theta_m = \lambda^{(x_1+x_2+\ldots\ldots+x_m)} \circ ((\lambda_1\lambda_2\ldots\ldots\ldots\lambda_m)^y \bmod n^m$ and this completes proof.

Theorem 3.10 Let $(G_1,\ldots\ldots,G_m)$ be a homomorphic private key encryption scheme with respect to addition-composition homomorphism and a set of families of polynomial sized spaces (are private key encryption scheme, H_i is a probabilistic polynomial-time algorithm and exists a polynomial m($\circ$) such that for every space $\{C_i\}$ $i \in N \in C$, $m \in N$ polynomial (($\circ$)), keys (e_i, d_i) and l = l(m) single but messages b_i - $b_l \in \{0,1\}$ the following holds:

(i) Correct decryption of addition-composition homomorphically generates encryptions

$D_i(H_i(C_l, E_e(b_1), \ldots\ldots..E_e(b_l) = C_l(b_1 \ldots.b_l)$ (i=1,……..,m)

(ii) The length of addition-composition homomorphically generated encryption is independent of l and is shorter i.e.

$|H_i(|C_l E_e(b_1,\ldots\ldots E_e(b_l) \leq m(n) \quad \forall n \in V$

Proof: By Lemma 3.9, addition-composition homomorphic encryption is well defined. So by Definition 2.10 it is easy to see that $D(H_i)$ depends in $f_i(x)$ and invoking Theorem 3.7, and Lemma 3.9, exactness is obtained. Linearity is trivial and the proof is complete.

Theorem 3.11: Let $G_1,\ldots\ldots G_m$ be as a base in the theorem X then for all $m\in N$, $b\in\{0,1\}$ and $C(G_1\circ G_2), k)\leftarrow G'(l^m)$ then $D_k^l(E^l_{G_1\circ G_2}(b)) = b$.

Proof: First consider the generation key $G^l(l^m)$ and encryption $E^l(G_1\circ G_2)$ and decryption $D_k^l(c)$: output $D_k(c)$.

Next consider the first property of addition-composition encryption. If we consider Theorem 3.10, then analogously, $D_k^l(E^l_{G_1\circ G_2}(b)) = D_k(H\oplus(G_1\circ G_2) = \overset{l}{\underset{i=1}{\oplus}} D_k(C_i)$ where $\oplus$ denotes the addition modulo i $C_i = G_i$ $i\in C$ and $C_i = G_i$ otherwise. Since D_i decrypts correctly $D_k(G_i)=0$ otherwise $D_k(G_i) = 1$, therefore, $D_k^l(E^l_{G_1\circ G_2}(b)) = \oplus_{i\in C} 1 = |C| \bmod i = b$. The next step is to ensure that the scheme is semantically secure.

Theorem 3.12 If $(G_1,\ldots..,G_m)$ is a semantically secure multiple message private key scheme then $(G_i^{'}, E_i^{'}, D_i^{'})$ is semantically secure public key scheme.

Proof: Assume without loss of generality that $(G_i^{'}, E_i^{'}, D_i^{'})$ is not semantically secure. Then it implies there exists a probabilistic polynomial time adversary A' of a polynomial $\phi(\circ)$ such that for infinitely many $n\in N$. $\Pr_{(G_1\circ G_2),k\leftarrow G_i^{'}(l^m)}[A'(G_1, G_2 E^{'}_{G_1\circ G_2}(b))=b] < \frac{1}{i} + \frac{1}{p(m)}$ $\qquad b\in R\{0,1\}$

The rest follows from Craig, (2009) analogously and this completes the proof.

4. Conclusions

The addition-multiplication homomorphic encryption is to the advantage of being usable in real time. The composite function element comes in handy since the result of the composite function f(x) is encrypted and malicious hosts cannot know the results of the function. For instance in the mobile phone technology, the owner of the function gets the encrypted result through the function g(x). For instance Richard Omollo is the owner of function h(x) he wants to calculate the input c of Bernard

Okelo but he doesn't want to expose himself as the owner of the function. So he chooses g(x) and creates f(x) then sends it to Bernard Okelo. Bernard Okelo hence calculates the result through f(x) using his input x and sends the result to Richard Omollo. Bernard Okelo cannot calculate h(x) because what he can see is just f(x). Only Richard Omollo can get the real result of h(x) through adding f(x) into inverse function i.e. $h(x) = g^{-1}(f(x))$. For this particular reason, we have developed some theoretic results based on the addition-composition homomorphic encryption.

References

Atayero, A. A. & Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption. Journal of Emerging Trends in Computing and Information Sciences. 2(10):546 – 552.

Craig, G. (2009). A Fully Homomorphic Encryption Scheme. PhD Thesis in Computer Science, Stanford University, California, USA.

Gnanavelu, D. & Gunasekaran, G. (2014). Survey on Security Issues and Solutions in Cloud Computing. International Journal of Computer Trends and Technology. 8(3):126–130.

Gomathisankaran, M., Tyagi A. & Namuduri, K. (2012). HORNS: A Homomorphic Encryption Scheme for Cloud Computing using Residue Number System. Proceedings of 2011 45th Annual Conference on Information Sciences and Systems, pp. 1 – 5, Baltimore, MD, IEEE.

Gomathisankaran, M., Tyagi A. & Namuduri, K. (2013). HORNS: A Semi-perfectly Secret Homomorphic Encryption System. American Journal of Science and Engineering. 2(1):17–21.

Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvallo, T., Naslund, M. & Pourzandi, M. (2012). A Quantitative Analysis of Current Security Concerns and Solutions in Cloud Computing. Journal of Cloud Computing: Advances, Systems and Applications. Springer.

Gupta, V., Singh, G., & Gupta, R. (2011). A Hyper Modern Cryptography Algorithm to Improved Data Security: HMCA. International Journal of Computer Science & Communication Networks.1(3):258 – 263.

Kaur, Simarjeet. (2012). Cryptography and Encryption in Cloud Computing. VSRD International Journal of Computer Science & Information Technology. 2(3):242–249.

Naruchitparames, J. & Gunes, M. H. (2013). Enhancing Data Privacy and Integrity in the cloud. IEEE Journal. 427 – 434.

Rachana, S. C. & Guruprasad, H. S. (2014). Emerging Security Issues and Challenges in Cloud Computing. International Journal of Engineering Science and Innovative Technology. 3(2):485–490.

Ravindra, S. & Kalpana, P. (2011). Data Storage Security Using Partially Homomorphic Encryption in a Cloud. International Journal of Advanced Research in Computer Science and Software Engineering. 3(4):603–606

Sasidharan, L, Neeth, P.R. & Reddy, L. (2011). Security Issues and Solutions in Cloud Computing. International Conference on Computational Techniques and Artificial Intelligence. Pp 61 – 64.

Tebaa, M. & Hajii S-E. (2013). Secure Cloud Computing through Homomorphic Encryption. International Journal of Advancements in Computing Technology. 5(16):29–38

Tiwari, P. K. & Mishra, B. (2012). Cloud Computing Security Issues, Challenges and Solution. International Journal of Emerging Technology and Advanced Engineering. 2(8).