On the Okamoto-Uchiyama cryptosystem: (A brief essay on basic mathematics applied in cryptography)

by Lawi Armin

Submission date: 19-Feb-2020 11:51AM (UTC+0700)
Submission ID: 1259987089
File name: Haryanto_2019_J._Phys.__Conf._Ser._1341_042013.pdf (692.73K)
Word count: 3697
Character count: 18458

On the Okamoto-Uchiyama cryptosystem: (A brief essay on basic mathematics applied in cryptography)

On the Okamoto-Uchiyama cryptosystem

(A brief essay on basic mathematics applied in cryptography)

Loeky Haryanto[1], Armin Lawi[2], Suhastina Suhastina[3], Putri Qarynah[4]

[1] Corresponding author
[2]Lecturer at Computer Science Study Program
[3,4]Students at Computer Science Study Program,
Mathematics Department, Hasanuddin University, Makassar, Indonesia

E-mail: l.haryanto@unhas.ac.id

Abstract.

The Okamoto-Uchiyama cryptosystem applies many consepts of basic abstract algebra, discrete mathematics and number theory. Many of these concepts are elementary and used in other branches of cryptography. However, those elementary concepts are not enough provided in the mathematics curriculla in under developed and developing countries despite the fact that in early stages teaching of those basic mathematics concepts, there is no need to provide sophiticated nor rigorous treatments beyond computations of integers.

By exploring the basic mathematics applied in Okamoto-Uchiyama's algorithm and its related concepts, this exploration should make mathematics teachers, educators and instructors to be aware of the important teaching the basic abstract algebra, discrete mathematics and number theory as early as high school senior level or at the first year in colleges and universities.

1 Introduction

The development of technology and information has changed many things, including the mathematics concepts studied and applied in applications. The current applications applied to information technology are much less related to the 'applied mathematics', a branch of mathematics referred to mathematics on differential equations, numerical analysis and similar topics in mathematics.

Today, hundreds or thousands of clouds servers exist and billions of electronic devices such as smartphones, DVD players and laptops are produced every day. Most of these cloud servers and devices need some

features to guarantee security and data integrity in communcations, or to protect identity and copyrights of the products or their users, or for other purposes. Many of the features need a new kind of mathematics applications that are very different from the applications of what is called 'applied mathematics'. One of these new applications led to a branch of mathematics called crytography.

The OU (Okamoto-Uchiyama) cryptosystem proposed in [7] is a part of cryptography that aims to conceal information from a third party when the information is sent from one party to another over a public channel. By the sender, this information is encrypted and by the receiver, the encrypted information (called ciphertexts) is decrypted to obtain the original information (messages or plaintexts).

In OU cryptosystem, the security of information sent through public channel is strengthen by the semantic security through the used of a probalistic random variable that makes a third party cannot determined which encrypted data was produced from a particular plaintext.

With hindsight, Sony's PlayStation network in 2011 would not be hacked if the company had used homomorphic encryption. As its users accessed their information or accounts for their needs, they had to decrypt their encrypted information and to do some computations. Without homomorphic encryption, the company should provide the secret decryption keys of all the users somewhere between its cloud server and the users (Ogburn et al. [6]). In this way, a third party had an opportunity to hack the secret keys and in turn, that third party was able to access thousands of users' information items.

With homomorphic encryption used by a cloud server, computations can be performed by the users on encrypted information without firstly decrypting the information. Therefore, the server does not need to provide secret keys beyond the server.

In the next Section 2, probabilistic and homomorphic encryption is briefly introduced informally. The next Section 3 describes how OU cryptosistem works and is completed with an example. Before the last Section 5 (Conclusion), a section on the importance of introducing somw basic and elementary mathematics related to cryptogrphy teaching is discussed as Section 4.

2 Probabilistic and Homomorphic Encrytion

Homomorphic encryption from plaintext (or message) space to cipher space is analogous to group homomorphism E: $(G_1, \oplus) \longrightarrow (G_2, \otimes)$ that satisfies $E(x \oplus y) = E(x) \otimes E(y)$ but the two spaces do not neccerarily posses algebraic structures. Not only is OU cryptosystem a homomorphic encryption, it also a probabilistic cyptosystem as a random constant r is added for every encryption of a plaintext m. This typical cryptosystem can be described by the following figure.

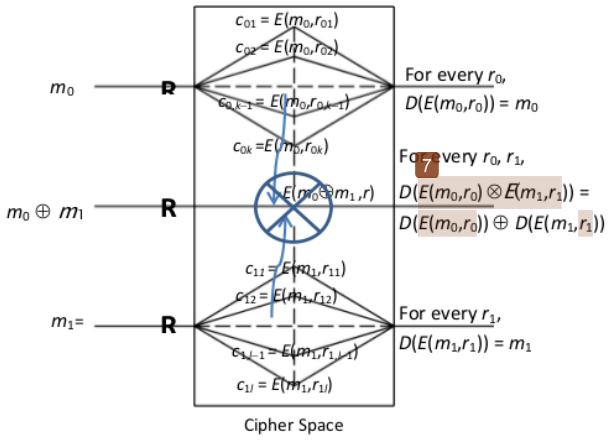

Figure . A typical probabilistic homomorphic cryptosystem with encryption function $E : (m, r) \mapsto c$ where r is a random constant generated by R

Details of the OU cryptosystem will be explained in Section 3. In a homomorphic encryption, the binary operation $\otimes$ between any two ciphertexts in the cipher space as shown in the figure above can be performed without revealing their respective plaintexts. In some respects, this operation mimics the operation $\oplus$ between their plaintexts disguised by the random integer r.

In practice, the operator $\otimes$ usually is the modular multiplication. In OU cryptosystem, the operator $\oplus$ is the modular addition and thefore the system is called an additive homomorphic encryption.

At first, only multiplicative or additive homomorphic encryption had been constructed until Gentry [3] in his dissertation was able to construct a full homomorphic encryption, which is an enrryption that is both additive and multiplicative homomorphic. This full homomorphic encryption allows

more computations among more functions over encrypted information without using a decryption key.

Homomorphic encryption opens many applications in which the ecrypted information is computed and can be used by a third party without disclosed its contents. A common proposed applications of hommorphic encryptions is on voting system, e.g. those proposed by Guarjardo et al. [5] and Anggreannie et al. [1]. These two applications make use an additive homomorphic cryptosystem introduced by Paillier [8].

3 The OU Cryptosystem

Every character or a group of charaters is represented internally by numbers. So is every piece of information sent and received in a digital or electronic communication. Therefore all the information in a cryptosystem are assumed to be integers.

The OU cryptosystem closely related to the multiplicative p-subgrup

$$\Gamma = \{\mathbf{x} \in \mathbf{Z}/p^2\mathbf{Z} | \mathbf{x} \equiv \mathbf{1} \mod p\} \tag{1}$$

of the group $\mathbf{Z}/p^2\mathbf{Z}$. Γ is the domain of the discrete, finite logarithmic function $L : \Gamma \longrightarrow \mathbf{Z}/p\mathbf{Z}$ with $L(x) = \frac{x-1}{p}$. The cryptosystem consists of the following steps elaborated with its related (algebraic) structures.

3.1 Key Generation

In a communication secured by OU cryptosystem, the secret keys p, q and the public key $n = p^2q$ are generated and provided by the system according to the following steps.

- Select secret keys: two large prime numbers p and q of the same length k-bits, and then set the public key $n = p^2q$.
- Randomly choose a generator $g \in (\mathbf{Z}/p^2\mathbf{Z})^*]$ such that $g_p = g^{p-1} mod p^2 \neq 1$ and $g^{p(p-1)} \mod p^2 = 1$ then set another public key $h = g^n \in \mathbf{Z}/n\mathbf{Z}$.

Note that $\mathbf{Z}/p^2\mathbf{Z}$ is a cyclic group, so it has a generator. The order of a generator g is $\phi(p^2) = p(p-1)$ and to ensure this happens, it is enough to impose the condition $g^{\phi(p^2)} = g^{p(p-1)} \mod p^2 = 1$, provided $g > 1$.

3.2 Encryption

In the encryption steps, information contained in a message (plaintext) is concealed through encryption with the public keys g, h and n. The information hidden in the resulted encrypted information is further disguised by introducing random constant r. This leads to a probabilistic cryptosystem, a typical cryptosystem that was firstly constructed by Goldwasser and Mikali [4], but the latter is inefficient since its encryption was done bit by bit.

The OU encryption steps are:

- Choose a plaintext $m \in \mathbf{Z}/p\mathbf{Z}$; i.e. $0 < m < 2^k$.
- Randomly select $r \in \mathbf{Z}/n\mathbf{Z}$
- Compute $c = E(m, r) = g^m \cdot h^r \bmod n$. and send $c_p = c^{p-1} \bmod p^2$.

Note that an integer of k-bits means that in 10-base, it is at most $2^k - 1$. Therefore, any positive integer m satisfying $0 < m < 2^k$ can be sufficiently represented by k bits.

3.3 Decryption

Both $g_p = g^{p-1}$ and $\gamma = (g^m)^{p-1} = (g_p)^m \bmod n$ are in Γ. The condition $g_p \bmod n \neq 1$ is equi.valent to the condition $L(g_p) \neq 0$ which implies the inverse of $L(g_p) \in \mathbf{Z}/p\mathbf{Z}$ exists.

The decryption steps are

- Find $\mu = L(g_p)^{-1}$.
- Decrypt the ciphertext $c = E(m, r)$ as follows, to obtain

$$M = D(c) = D(E(m, r)) = \frac{L(c_p)}{L(g_p)} = \mu \cdot L(c_p). \tag{2}$$

Note that the received cipher $c_p = c^{p-1} = (g^m \cdot h^r)^{p-1} = (g^m)^{p-1} \cdot (h^r)^{p-1} = \gamma \cdot (h^r)^{p-1} \bmod p^2 \in (h^r)^{p-1}\Gamma$ belongs to a coset of Γ

3.4 OU Homomorphic Encryption

In their paper, Okamoto and Uchiyama [7] states that OU cryptosystem satisfies the following homomorphic encryption: for any two plaintexts m_0, m_1 with $m_0 + m_1 < p$,

$$E(m_0, r_0) \cdot E(m_1, r_1) = E(m_0 + m_1, r_2). \tag{3}$$

As the constants r_0, r_1 and r_2 are randomly generated imdependently to each other, this equation cannot be true. However, if the third constant is made dependent on the first and second constant, i.e. $r_2 = r_0 + r_1$, the equation holds.

Theorem 3.1 *Let $m_0, m_1 \in \mathbf{Z}/p\mathbf{Z}$ be two plaintexts encrypted as $E(m_0, r_0)$ and $E(m_1, r_1)$, respectively. If $m_0 + m_1 < p$, then*

$$E(m_0, r_0) \cdot E(m_1, r_1) = E(m_0 + m_1, r_0 + r_1). \tag{4}$$

holds.

Proof.

$$\begin{aligned} E(m_0, r_0) \cdot E(m_1, r_1) &= (g^{m_0} h^{r_0}) \cdot (g^{m_1} h^{r_1}) = (g^{m_0} g^{m_1}) \cdot (h^{r_0} h^{r_1}) \\ &= g^{m_0+m_1} \cdot h^{r_0+r_1} = E(m_0 + m_1, r_0 + r_1). \blacksquare \end{aligned}$$

Although the random integers r_0 and r_1 keep changing, and so is the integer r_2 in $E(m_0 + m_1, r_2)$, the encryption step preserves each of the plaintexts m_0, m_1 and their sum $m_0 + m_1$ as the following theorem holds.

Theorem 3.2 *For every $m_0, m_1 \in \mathbf{Z}/p\mathbf{Z}$ and every $r_0, r_1, r_2 \in \mathbf{Z}/n\mathbf{Z}$, the following equation holds*

$$m_0 + m_1 = D(E(m_0 + m_1, r_2)) = D(E(m_0, r_0) \cdot E(m_1, r_1)). \tag{5}$$

Proof. Claim: for every $m \in \mathbf{Z}/p\mathbf{Z}$ and $r \in \mathbf{Z}/n\mathbf{Z}$

$$D(E(m, r)) = m. \tag{6}$$

First, it can be shown that

$$\begin{aligned} c_p = c^{p-1} &= (g^m \cdot h^r)^{p-1} = (g^m \cdot (g^n)^r)^{p-1} = (g^m)^{p-1} \cdot (g^{nr})^{p-1} \\ &= (g^m)^{p-1} \cdot (g^{p-1})^{nr} = (g^m)^{p-1} \cdot (g^{p-1})^{p^2qr} = (g^m)^{p-1} \cdot (g^{p(p-1)})^{pqr} \\ &= (g^m)^{p-1} \cdot (g^{\phi(p^2)})^{pqr} = (g^m)^{p-1} \cdot (1)^{pqr} = (g^m)^{p-1} \\ &= (g^{p-1})^m. \end{aligned}$$

where ϕ is the totient function. By (2) and the properties of a logarithm, the lefthand side (6) becomes

$$D(E(m, r)) = \frac{L(c_p)}{L(g_p)} = \frac{L((g^{p-1})^m)}{L(g_p)} = \frac{L(g_p^m)}{L(g_p)} = m,$$

which is the right hand side of (6). From the claim (6), the first equality in (5) is clearly true.

The claim (6) also states that the result of decrypting a ciphertext $c = E(m, r)$ is independent from the choice of random integer r. Therefore by choosing and subtituting $r_2 = r_0 + r_1$, the second equality in (5) is directly derived from the decryption of (4). ■

3.5 An Example

Suppose two secret keys $p = 23, q = 41$ are provided for a communication between Alice and Bob secured by the OU cryptosystem where two messages $m_0 = 5$ and $m_1 = 11$ are sent by Alice to Bob. Suppose also the cryptosystem generates public keys $g = 191, n = 21689$ and $h = g^n \bmod n = 724$.

For decrypting a ciphertext, a public key $g_p = g^{p-1} \bmod p^2 = 24$ is also announced, so $g_p \bmod p = 24 \bmod 23 = 1$, i.e. $g_p \in \Gamma$. Define denom $= L(g_p) = \frac{24-1}{23} = 1 \neq 0$ so $\mu = (denom)^{-1} = 1^{-1}$ in $\mathbf{Z}/p\mathbf{Z}$ exists. Clearly, $\mu = 1$. Notice that g satisfies the conditions $gcd(g, p^2) = 1, g_p = g^{p-1} \bmod p^2 = 191^{22} \bmod 23^2 = 24 \neq 1$ and $g^{p(p-1)} \bmod p^2 = g^{\phi(p^2)} \bmod p^2 = 1$.

Encrypting the message $m_0 = 5$ triggers a random constant $r_0 = 5049$ to produce a ciphertext

$c_0 = (g^{m_0})(h^{r_0}) \bmod n = (191^5) * (724^{5049}) \bmod 21689 = 17762$.

Next, compute $c_{p0} = c_0^{p-1} \bmod p^2 = 116$. Note that $c_{p0} \bmod p = 116 \bmod 23 = 1$ with implies that c_{p0} belongs to the p-subgroup Γ, the domain of the discrete, finite logarithm L.

In $\mathbf{Z}/p^2\mathbf{Z}$, the logarithm of c_0 is

$$\text{enum0} = L(c_{p0}) = L(116) = \frac{116-1}{23} = 5.$$

The ciphertext c_0 is decrypted using the last equality in (2) resulting

$$M_0 = \frac{L(c_{p0})}{L(g_p)} = \frac{enum0}{denom} = \mu \cdot enum0 = 1 \cdot 5 = 5 = m_0.$$

Encrypting the message $m_1 = 11$ triggers a random constant $r_1 = 12077$ to produce a ciphertext

$c_1 = (g^{m_1})(h^{r_1}) \bmod n = (191^{11}) * (724^{12077}) \bmod 21689 = 9800$.

Let $m_2 = m_0 + m_1 = 16 < p = 23$ which means the condition for equation (3) is satisfied. Encrypting the message $m_2 = 16$ triggers a random constant $r_2 = 7796$ to produce a ciphertext

$c_2 = (g^{m_2})(h^{r_2}) \bmod n = (191^{16}) * (724^{7796}) \bmod 21689 = 1106$
$\neq 13375 = (17762) \cdot (9800) \bmod 21689 = c_1 \dot{c}_2 \bmod n.$
This shows that equation (3) is not an equality between two numbers.

Now, instead of using the random $r_2 = 7796$, suppose the same message $m_2 = m_0 + m_1 = 16$ were encrypted with chosen constant $r_3 = r_0 + r_1 \bmod n = 5049 + 12077 \bmod 21689 = 17126$. With this chosen constant, the encryption would produce a ciphertext

$c_3 = (g^{m_2})(h^{r_3}) \bmod n = (191^{16}) * (724^{17126}) \bmod 21689 = 13375 = c_0 c_1.$
This ultimately confirms the equation (4) in Theorem 3.1

Similar to encyption that yiels $c_{p0} \in \Gamma$,

$c_{p1} = c_1^{p-1} \bmod p^2 = 254$, $c_{p2} = c_2^{p-1} \bmod p^2 = 369 = c_{p3} = c_3^{p-1} \bmod p^2$ are obtained and they all belong to Γ. Taking their logarithm yields
enum1 $= L(c_{p1}) = L(254) = 11$,
enum2 $= L(c_{p2}) = L(369) = 16$, and
enum3 $= L(c_{p2}) = L(369) = 16$.

Finally, decrypting the last three ciphertexts c_1, c_2 and c_3 results in
$M_1 = D(c_1) = \mu \cdot$ enum1 $= 1 \cdot 5 = 11 = m_1$,
$M_2 = D(c_2) = \mu \cdot$ enum2 $= 1 \cdot 16 = 16 = m_0 + m_1$, and
$M_3 = D(c_3) = \mu \cdot$ enum3 $= 1 \cdot 16 = 16 = m_0 + m_1$,
which are the original plaintexts $m_1, m_2 = m_3 = m_0 + m_1$.

4 The Basic Mathematics

Cryptography is one of new directions in mathematics that has been born and developed in order to solve new kind of problems in computer science and information technology.

The preceding sections only cover few mathematical concepts applied in OU cryptosystem, but many of the concepts are very common being used in other branches of crytopgrahpy and beyond, e.g. in the theory of error-correcting codes.

One common characteristic of computations in elementary cryptography, or generally in computer science, it mainly computes integers of finite values although within a computer, the word 'finite' may mean very large, more than $(2^{1024})^{2048}$ for example.

From group theory and modular computation prespectives, a unique mathematics concept explored in OU cryptosystem is the application of discrete and finite logarithm L expressed by (1). The logarithm is a group

isomorphism from the multiplicative group Γ onto the additive group $\mathbf{Z}/p\mathbf{Z}$ and both groups are of size p.

In expression (2), the logarithm L is applied in decrypting the ciphertext c to obtain $M = \frac{L(c^{p-1})}{L(g_p)}$. The construction of OU cryptosystem guarantees that both $c^{p-1} = (g^{p-1})^m$ and $g_p = g^{p-1}$ belong to Γ. Moreover, the construction also prevents $g_p = 1$, or equivalently prevents $L(g_p) = 0$. Therefore, $\mu = L(g_p)^{-1} \in \mathbf{Z}/p\mathbf{Z}$ exists.

Modular computation usually is introduced in elementary number theory including totient function, the Fermat's Little Theorem and its generalizaiton: Euler's Theorem, along with many topics like the Extended Euclidean Geometry, Chinesse Remainder Theorem, and many others.

Totient function explicitly applies in proving $c^{p-1} = (g^{p-1})^m$ appeared after (6). Fermat's Liitle Theorem and its generalization applied implicitly for many times in the construction of OU and many other cryptosystems. For example, the conditions $g^p \neq 1, g^{\phi(p)} = g^{p-1} \neq 1$ and $g^{\phi(p^2)} = g^{(p-1)p}$ mod $p^2 = g^{\phi(p^2)}$ mod $p^2 = 1$ ensure that g is a generator of $\mathbf{Z}/p^2\mathbf{Z}$.

Number theory is closely related to algebra. However, teachers and instructors should be aware the different laguages used in the two disciplines. For example, in the group $\mathbf{Z_7}$, the solutions of $x^2 = 4$ are 2 and 5 whereas in number theory, the solutions of $x^2 \equiv 4$ mod 7 are in the infinite set $\{\cdots, -12, -9, -5, 2, 5, 9, 12, \cdots\}$.

In a classroom, inverse of group elements can be computed using Extended Euclidean algorithm. However, there were no efficient algorithm to find a generator of a cylic group of small prime order p that can be executed manually in the classroom except by exhausted search. Therefore, a little prosedur or a small computer program for computations is still needed.

In number theory, the generator is called a primitive root modulo p. Unfortunately, algorithms for finding generator of a group of composite order are more complicated. However, by giving examples with small numbers, e.g. less than 10^8; an exhausted search such a generator using computer only takes few seconds.

From mathematics education prespective, high school and college mathematics in Indonesia and other developing countries or under developed countries still do not change very much from their traditional computations over real numbers based on 'applied mathematics'. For

example, most students in high school and university freshmen do not know modular arithmetic, a mathematical tool that limits and gives a bound for computations of integers.

Moreover, most university students in science have never been taught group theory, including the easier-learned groups of integers like the additive group $\mathbf{Z}/n\mathbf{Z}$ or the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^*$. The only mathematics applied in OU cryptosystem, which apparently is difficult to be learned by university fresmen, is the notion of p-(sub)group. How ever, by givin small size p-subgroup, in this case is $\mathbf{Z}/p^2\mathbf{Z} \subset \mathbf{Z}/n\mathbf{Z}$, it would be easy to be grasped by most students.

5 Conclusion

The OU cryptosystem applies some basic mathematics concepts that are commonly encountered in the study of cryptography. Therefore, there is no need to go through rigorous algebraic or number theory treatments or introducing advanced mathematical tool when teaching elementary cryptography.

By restricting only examples with computations over small integers, only few of these basic concepts need sophisticated softwares or hardwares. This short essay gives examples of basic concepts in mathematics in elementary cryptography and in similar mathematics disciplines. The concepts should be introduced in high school and in the first year of university terms and they should be given earlier than they used to be.

This is an effort through mathematics education and teaching to catch up and speed up the economy development related to advanced technology and information theory in underdeveloped or developing countries.

6 References

[1] Anggrianne S M, Nasution S M, Azmi F 2016 *Advanced e-voting system using Paillier homomorphic encryption algorithm* Proc 2016 International Conference on Informatic and Computing
[2] Fuchsbauer G J 2006 *An Introduction to Probabilistic Encryption* OSJEČKI MATEMATIČKI LIST vol 6 pp 37-44
[3] Gentry C 2009 *A Fully Homomorphic Scheme* Doctoral Dissertation (Symposium on the Theory of Computing, NY, New York, USA).
[4] Goldwasser S and Micali S 1984 *Probabilistic encryption.* (Journal of Computer and System Sciences) vol 28(2) pp 270-299.
[5] Guajardo J, Mennink B, Schoenmakers B 2010 *Modulo Reduction for Paillier Encryption and Application to Secure Statistical Analysis* Proc 14-Internaational Conference on Financial Cryptography and information Security, Tenerife, Canary Island
[6] Ogburn M, Turner C, Dahal P 2013 *Homomorphic Encryption* Procedia Computer Science, Dagli C H (Eds), Baltimore, MD, USA.

[7] Okamoto T and Uchiyama 1998 *A New Public-Key Cryptosystem As Secure as Factoring, Proc. of Advances in cryptology-EUROCRYPT'98*, Lecture Notes in Computer Science 1403, Springer-Verlag, pp. 308–318.
[8] Paillier P 1999 *Public-Key Cryptosystems based on Composite Degree Residue Classes* Proc of EuroCrypt 99 Springer Verlag LNCS series 1592 pp 223-238.

On the Okamoto-Uchiyama cryptosystem: (A brief essay on basic mathematics applied in cryptography)

ORIGINALITY REPORT

11%	8%	6%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.er-c.org Internet Source	4%
2	Submitted to School of Business and Management ITB Student Paper	1%
3	Minoru Kuribayashi. "A New Anonymous Fingerprinting Scheme with High Enciphering Rate", Lecture Notes in Computer Science, 2001 Publication	1%
4	Firdaus, N H Soekamto, Seniwati, M F Islam, Sultan. "Phenethyl ester and amide of Ferulic Acids: Synthesis and bioactivity against P388 Leukemia Murine Cells", Journal of Physics: Conference Series, 2018 Publication	1%
5	Submitted to Hellenic Open University Student Paper	<1%

Choi Dug-Hwan, Seungbok Choi, Dongho Won.

6	"Chapter 7 Improvement of Probabilistic Public Key Cryptosystems Using Discrete Logarithm", Springer Nature, 2002 Publication	<1%
7	static.usenix.org Internet Source	<1%
8	Cheng-Kang Chu. "Conditional Oblivious Cast", Lecture Notes in Computer Science, 2006 Publication	<1%
9	Rajat Saxena, Somnath Dey. "Cloud Audit: A Data Integrity Verification Approach for Cloud Computing", Procedia Computer Science, 2016 Publication	<1%
10	Ling Dong, Kefei Chen. "Cryptographic Protocol", Springer Nature, 2012 Publication	<1%
11	issuu.com Internet Source	<1%
12	oar.princeton.edu Internet Source	<1%
13	Lecture Notes in Computer Science, 2001. Publication	<1%
14	link.springer.com Internet Source	<1%
15	Open Problems in Mathematics, 2016. Publication	

<1%

16 Damith C. Herath, S. Kodagoda, Gamini Dissanayake. "New framework for Simultaneous Localization and Mapping: Multi map SLAM", 2008 IEEE International Conference on Robotics and Automation, 2008 <1%
Publication

17 Tatsuaki Okamoto. "A new public-key cryptosystem as secure as factoring", Lecture Notes in Computer Science, 1998 <1%
Publication

18 D. Vinodha, E. A. Mary Anita. "Secure Data Aggregation Techniques for Wireless Sensor Networks: A Review", Archives of Computational Methods in Engineering, 2018 <1%
Publication

19 Submitted to Universiti Putra Malaysia <1%
Student Paper

Exclude quotes	On	Exclude matches	< 5 words
Exclude bibliography	On		