Design of Public Key Cryptosystem Based on Isomorphism abelain group (IAG)  
Kian Rhim Qasem, Fras Hashem

1-1 Abstract:
After the 1973 there are several Public Key cryptosystem are development, all system based on hard mathematical problems such as discrete logarithm, Integer Factorization, subnet, or elliptic curve Discrete Logarithm problem. Which problems are defined over finite a blain Group. In this paper we proposes new concept in the public key system that is depend on isomorphism a blain group (IAG), mainly Algorithm. Along this paper new functions were revealed that have difference in complexity to find its inverse due to the isomorphism group.

Keywords: isomorphism a blain group (LAG), Discrete Logarithm problem (DLP), public Key cryptosystems

1-2 INTRODUCTION:
Computer is now found in every Layer Society, and information is being communicated and processed automatically on a large scale. Such as medical and financial files, automatic banking, video – phones, pay-tv, facsimiles, tele-shopping, and global computer networks in all these cases there is growing need for the protection of information to a guard economic interest, prevent fraud and to ensure privacy. Glyptography is the science and study of methods of protect detain computer and communication systems from unauthorized disclosclerse and modification [1] the cryptographic system are classified into two cryptosystems, private key cryptosystem, and public key cryptosystems, Both are based on complex mathematical algorithms and are controlled by keys. Many public key cryptographic systems are based on the finite mathematical groups. The most commonly fields are prime field F (the integer module a prime P) and binary field F@M (characteristic &finite fields). The cryptographic strength of these systems is derived from the computational intractability of computing logarithms in these groups. This can be called by discrete logarithm problem (DLP). The security of the cryptosystems using isomorphism group hinges on the intractability of the DLP in the algebraic system [2]. In the other word had introduced the notation of 'trapdoor' one –way-function (TOF) which is easy to evaluate bust computation the inverse without a secret "trap door" is
Design of Public Key Cryptosystem Based on Isomorphism abelian group (IAG) ..................................................... Kian Rhim Qasem, Fras Hashem

an intractable problem [3]. Since the beginning of key cryptography (elgamal public key system). That seem to defeat all attacks.

2-Algebraic preliminaries

2-1 groups: A group is a structure consisting of a set G and a binary operation * on G (ie for any a, b Є G, a*b Є G is defined) such that [4,5]
1- Closure: A*b Є G, for all a<b<c Є G
2- Associative: A*(b*c)=(a*b)*c for all a,b,c Є G
3- Existing of identity: there are unique element e Є G such that e*a=*e=a for every a Є G this unique element e is called the neutral element of G or identity.
4- Existing of inverse: for each at here is an element b Є G such that b*a=a*b=e and b is uniquely determined and is called the inverse of a.
5 - Commutativity: a*b=b*a for any a, b Є G if the group is commutative group also is called a blain group.

The notation (G,*) is and to represent a group with group operation*.(G,+)and(G,.) Are called an additive group and a multiplicative group, respectively. In an additive, the neutral element by the symbol 0 and the inverse of a is denoted as-. In a multiplicative group, the neutral element is represent by the symbol 1 and the inverse of a is denoted as$a^{-1}$. Let (G,*) be an a group and let H be a subnet of G. The structure (H,Θ) is said to be a subgroup of (G,*). if Θ is the restriction of * to H*H and (H,Θ) is a group [6]. If G is a finite group, then number of elements of g is called the order of G and it is denoted as IGI. Given a finite multiplicative group G, the order of an element a Є G is the smallest positive integer m such that $a^m=1$. Such as m for every element in a finite multiplicative group [5, 4, 7].

2-2 cyclic group: if the group G has an element a of order n= IGI then $G=\{a^k \mid k Є \mathbb{Z}\}$

G is called cyclic and a is called a generator of G

The set $\mathbb{Z}_n=\{0,1,2,..,n-1\}$ is a cyclic group of order n under addition module n, i.e. a+b=r mod n where r<n (r is the remainder where a+b is divided by n).[6,5,4]

2-3 finite fields: A finite fields consists of a finite set of element F. Twobinary operation, addition and multiplication , and the and the additive and multiplicative inverses of each element . The binary operations satisfy certain arithmetic properties. The number of element in the finite filed is called the order of the field. There exists a finite filed of order p if and only if q is a prime power Essentially there is only one finite filed of order P denoted by $F_p$ if $q=p^m$ where q is a prime and m is appositive integer. Then q is called the characteristic of $F_p$ and m is called extension of $F_p$
2-4 Group Isomorphism (Definition): The groups \((g, .)\) and \((G, .)\) exist function \(f: G \rightarrow G^*\) such that \(F(a \cdot b) = F(b)\) for all \(a, b \in G\). 
2-f is one to one 
f is on to 

Then \(G \cong G^*\).

3-Discrete logarithm problem (DLP): one of the most interesting open problems in cryptography is the realization of a trapdoor in the discrete logarithm. In which to solve the DLP is hard only if published parameter are used, while it is, easy by using a secret key trap door key) [3]. The DLP can be defined on various finite group as well as multiplicative group over a finite filed \(F_P[1]\). This idea can be extend to arbitrary group and, in particular, to group \(\mathbb{Z}/n\mathbb{Z}\). Or the finite filed \(F_P\), let \(a, b \in F_P\), recall that in that in the DLP to finite an integer \(k \in \mathbb{Z}\) is such that \(\alpha^k = b\).

4-analog of the Elgamal cryptosystem: In this system the finite filed \(F_P\) and the "base number" \(\alpha \in F_P^*\) and public information .Bob randomly choosen and secret integer \(a (\text{Ka}^≠F_P^*)\) and publishes the number \(\alpha^a\). If Alice auts to send the massage M (ie plain text. We equivalent to number denoted by m )to Bob, she will choose a secret random integer \(K (KK^≠F_P^*)\)and send \((M, \alpha^{ka}, \alpha^K)\)to Bob, Bob will then exponential the second number in the pair by a to get \((\alpha^K)^{-1}\) and multiply by the first number in the pair \((M, \alpha^{ka})\) key \(\alpha^{ka}\), to get \((\alpha^k)^{-1}\) and multiply by the first number in the pair \((M, \alpha^{ka})\) to find M. In the mean time, Charlie has only seen \(\alpha^a\). solving the DLP (finding a knowing \(\alpha^a\) and \(\alpha^{ka}\) there is no way for him to find M. The following algorithm illustrates this manner [8]. Algorithm (EL Gmail cryptosystem with DLP):

1-Initialization
- Alice an Bob Publicly choose a finite filed \(F_P^*(\text{P a large prime } )\)
- \(M=F_P^*\) (particular space)
- \(C=F_P^* X F_P^*\) (cipher text space)

They publicly choose a random "base number" \(\alpha \in F_P\) such that \(\alpha\) generates a large subgroup of \(F_P^*\).
Design of Public Key Cryptosystem Based on Isomorphism abelian group (IAG) ................................. Kian Rhim Qasem, Fras Hashem

2- Key Generation
• Bob choose a secret random integer a in interval $[2, ≠ F_P^*]$  
• Then compute $β=α^2$

• Make $m, β$, are public and $a$ is secret.

3- Encryption function $E_{α, β}$
Alice sent the Massage $M$ to Bob as following:
• Select random integer $K$ in interval $[2≠ F_P^*]$  
• Compute $E_{α, β} (m, K)=(K^α mod_P = (c_1 ,c_2)$ transmit the part (C1,C2)

4- Decryption Function $d_{α}$: Bob retrieves the message as following:
• Compute $d_{α} (c_1,c_2)= c_2, c_1 - α mod_P$
• Compute $d_{α}(E_{α,β}(M,K))= M$

5- El –Jamal algorithm with group isomorphism:
Let $G$ a abelian group, and $g ∈ g$ fixed element, $H=<g>$ cyclic group and let $n$ be the order of $H$, we have the canonical isomorphism $F: z/n zn→H$
Which is define $F$
$F(a)= ag= g+g+g+……+g$ (a times)
Let $t ∈ z/nz$ (secret key)
Then $v=f(t) ∈ H$ (public key)

Encryption
$M ∈ H$ plaintext and $r ∈ z/ nz$ reflow element
$C_2=rv+m$

Decryption
$M=c_2-tc_1$

6- Security of group isomorphism associated with CIS (group isomorphism cryptosystem) comes from the wide variety of possible group structures of the element is the $F (F_1g)$
And from the fact that modular multiplication is same what more complicated then classical modular multiplication
The security of IGCS depends on how difficult is to determine the integer \( d \), given the number \( b \) and the number \( a^d \).

8- Example:
1- Key generation
\( P = 3i \)
\( F_{3i} = \{0, 1, 2, \ldots, 30\} \)
\( G = 2 \)
\( H = \langle 2 \rangle = \{0, 1, 2, \ldots, 30\} \)
\( n = 31 \)
\( Z/31n = \{0, 1, 2, \ldots, 30\} \)
\( F: Z/3iz \rightarrow H \)
\( t = 12 \) secret key
\( v = f(12) = 2 + 2 + \ldots + 2 = 24 \) public key
12 times

2- Encryption:

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>O</td>
<td>P</td>
<td>Q</td>
<td>R</td>
<td>S</td>
<td>T</td>
<td>U</td>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Y</td>
<td>Z</td>
</tr>
<tr>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>250</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Design of Public Key Cryptosystem Based on Isomorphism abelain group (IAG) ............................... Kian Rhim Qasem, Fras Hashem

Plaintext: M=KIAN
K  I  A  N
10  8  0  13
M1 m2 m3 m4
M1=10
R1=20→random
C11=f(r1)=f(20)=(2+2+…….+2)mod 31
(c11,c21)=(9,25)
M1=c21-tc11=(25-12*9)mod31
    =25mod31-12*9mod31
    =25mod31-15mod31
    =(25-15)mod31=8
M1=10→ K
(C12, C22)=(10, 4)
M2=8→I
(c13, c23)=(26, 2)
M3=c23-tC12=(2-12*26)mod31
    =(2-2)=0
M3=0→A
(C14, C24)=(3,18)
M4=C42-tC14=(18-12*3)mod31
    =(18-5)mod31=13
M4=13→ N
Plain text+KIAN
Ciphertext= JZKEΘCDS

Conclusion:
1- The project defined isomorphism a belain group (IAG) toused in the proposed cryptosystem. The discover that (IAG)has a one way function similar to DLP. The construction of cipher system is based on the difficulty of solution of the (IAG) that is a change in the cryptography and opens new windows for treatment with special group and new operation.
2- It is hand for the attacks to regenerate cycle group in order to pick (t) that necessary to decrypt the cipher.
3- In EL Gmal the group is no processing to generate a group.
Design of Public Key Cryptosystem Based on Isomorphism abelian group (IAG) 

Kian Rhim Qasem, Fras Hashem

4- The IGDLP over $F_q$ is more intractable than the DLP in $F_q$ it is this feature that makes cryptographic system based on the IGDLP even more secure than that based on the DLP, because the $F(F_q)$ gives a large group over small field size. Same the group $F(F_q)$ of the order $q^2 - 1$ or the factors, therefore, some of the strongest algorithms for solving DLP cannot be adaptive to the IGDLP.

References:

Design of Public Key Cryptosystem Based on Isomorphism abelian group (IAG) .................................................. Kian Rhim Qasem , Fras Hashem

المستخلص:

م.م. كيان رحيم قاسم
م.م. فراس هاشم
جامعة ديالى/كلية التربية الرازي/قسم الحاسوب
جامعة المستنصرية/كلية العلوم/قسم الحاسوب

بعد عام 1973 طورت العديد من أنظمة التشفير ذات المفتاح العام، وهذه المنظمة جمعتها تعتمد على مشاكل رياضية صعبة مثل مشكلة اللوغاريتمية المتقطعة وتحليل الأرقام إلى عواملها الأولية، ومسألة اللوغاريتمية المتقطعة للمنحنى البيضوي. في هذا البحث حاولنا فهم تنوع أنظمة التشفير ذات المفتاح العام؛ فضلاً عن هذا المفهوم على التشاكل الزمر المهيمنة الإبداعية، ووجدنا مسألة رياضية صعبة في الزمر التي تعتمد على التشاكل الزمري حيث عرفنا زمرة جزئية دائري وقمنا بتصميم خوارزمية تعتمد على هذه المفاهيم.