Design of Public Key Cryptosystem Based on Isomorphism abelain group (IAG)

Kian Rhim Qasem
Fras Hashem
Mustansiriyah university

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 INTROUDUCTION:

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 afguard economic interest, prevent fraud and to ensure privacy. Glyptography is the science and study of methods of protecting detain computer and communication systems from unauthorized disclosclosure 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 " tarap door" is

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

2-Algebric 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 ЄG, a*b Єg is defined) such that [4,5]

1- Closure: A*bЄG, for all a<b<c ЄG

2-Associative:A*(b*c)=(a*b)*c for all a,b,c ЄG

3- Existing of identity: there are unique element e ЄG such that e*a=*e=a for every a ЄG 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-Commutatively: a*b=b*a for any a, BЄ 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 asa^{-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 ©is thΘe 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={$\overline{1e}^{a^k}$ Є7}

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

The set z_n={0,1,1,…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=q^m where q is a prime and m is appositive integer.Then q is called the characteristic ofF_P and m is called extension of F_P

2-4 Group Isomorphism (Definition): The groups (g,.) and (1-There exist function f: G→G^- such that F(a.b)=F(b)for all a,b € G
2-f is one to one
f is on to
Then GυG*
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 extendnd to arbitrary group and, in particular, to group z/n^Z.Or the finite filedF_P, let a,b € F_P,recall that in that in the DLP to finite an integer k € Z is such that a^k=b.
4-analog of the Elgamal cryptosystem: In this system the finite filed F_P and the "base number" α Є F_P* and public information .Bob randomly choosen and secret integer a (Ka‹≠F_P*) and publishes the number α^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, α^{kz}, α^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, α^{Ka}) keyα^{ka}, to get $(\alpha^k)^{-1}$ and multiply by the first number in the pair (M , α^{Ka}) to find M. In the mean time, Charlie has only seen $\alpha''.solving$ the DLP (finding a

knowing and $[\alpha] \uparrow k)$ 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*(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" α Є F_P such that α generates a large subgroup of F_P*

2- Key Generation

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

- Make m, β, are public and a is secret.

3- Encryption function $E_{\alpha,\beta}$

Alice sent the Massage M to Bob as following:

- Select random integer K in interval [2≠F_P *]
- Compute $E_{\alpha,\beta}$ (m, K)=($K^{\alpha}\ mod_P$ =(c1 ,c2)transmit the part (C1,C2)

4- Decryption Functiond_a : Bob retrieves the message as following:

- Compute d_a (c1,c2)= $c2_{c1}{}^{-a}\ mod_P$
- Compute d_a ($E_{\alpha,\beta}(M,K) = M$

5- El –Jamal algorithm with group isomorphism:

Let G a blain group, and g Є 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 Є z/nz (secret key)

Then v=f(t) ЄH (public key)

Encryption

M Є H plaintext and r Є z/ nz reflow element

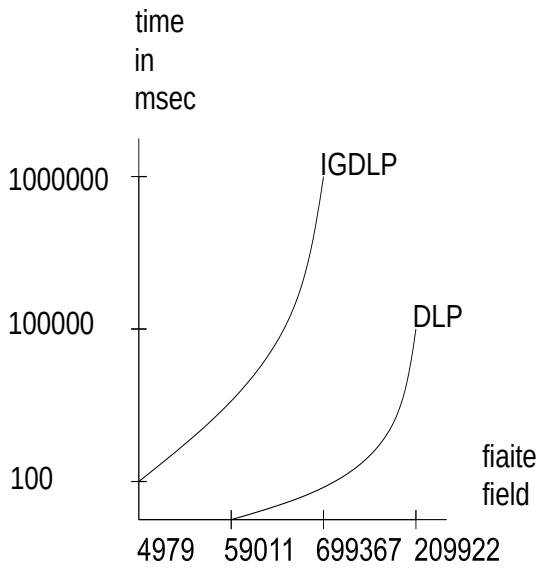
C2=rv+m

Decryption

M=c2-tc1

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_1q)

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_{31}={0,1,2,……., 30}

G=2

H=<2>={0,1,2,…….,30}

n=31

Z/31n={0,1,2,……..,30}

F:Z/3iz→H

t=12 secret key

v=f(12)=2+2+….+2=24 public key

12 times

2-Encrption:

A	B	C	D	E	F	G	H	I	J	K	L	M
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
13	14	15	16	17	18	19	20	21	22	23	24	250
1	3	4	5									
↓	↓	↓	↓	↓								

26 27 29 30 31

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.

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

References:

[1] H.Boker& F.Piper" Cipher System" The protection of communication, "Northwood books, London 1999

[2] IEEE P1363, "Standard Specifications for public key cryptography " ,draft 1997

[3] I.F.blake, R<m.Roth & G.Seroussi, "Efficient Arithmetic in GF (2n) Through plaind romid Visual computing Department, HPL-98- 13u.ang.1998.

[4] J.B.FFraleigh,"A First course in A bstract Algebra ", Addition Wesley pub, 1982

[5] M.B.Nathanson, "Elementray methods in number theory", Graduate Text in Mathematics 1951 , spring-verlage ,2000

[6] S,Y.Yan. "number Theory for Computing Springer- Verlay,2000.

[7] M.Sacki. :Elliptic Curve Cryptosystem M.SE thesis university of Megill Montreal.1999

[8] M.Stamp, Information Securty Principle and practice , John Wiley&sons, Ins2000 , J.M.Kizza .commuter network security ,springer inc. 2005

[9] G.berkho_,Saunder mac lane, A survey of modern Algeders, ISBN:978-1-56881-454-4,AKP classics, 2008.

[10]Ali M.sagheer, Design of public –Key cryptosystems Based on Matrices Discrete legayithm problem, masaum journal of computing,volume 1 issue 2, september2009 €

المستخلص:

م.م كيان رحيم قاسم **م.م فراس هاشم**

جامعة ديالى/كلية التربية الرازي/قسم الحاسبات الجامعة المستنصرية/كلية العلوم/قسم الحاسبات

بعد عام 1973 طورت العديد من انظمه التشفير ذات المفتاح العام وهذه الانظمه جميعها تعتمد على مشاكل رياضيه صعبه مثل مشكله اللوغارتميه المتقطع وتحليل الارقام الى عواملها الاوليه ومسأله اللوغارتميه المتقطع للمنحنيات البيضويه . في هذا البحثاقترحنامفهوم جديد لقيم انظمه تشفير ذات المفتاح العام يعتمد هذا المفهوم على التشاكل الزمر المهنيه الابداليه واوجدنا مسأله رياضيه صعبه في الزمره التي تعتمد على التشاكل الزمري حيث عرفنا زمره جزئيه دائريه وقمنا بتصميم خوارزميه تعتمد على هذه المفاهيم