Public key cryptosystem and a key exchange protocol using tools of non-abelian group

H. K. Pathak
S.o.S in Computer Science & IT
Pt. Ravishanker Shukla University
Raipur - 492010 (C.G.) India

Manju Sanghi
Department of Applied Mathematics
Rungta College of Engineering &Technology
Bhilai- 490024 (C.G.) India

Abstract. Public Key Cryptosystems assure privacy as well as integrity of the transactions between two parties. The sizes of the keys play an important role. The larger the key the harder is to crack a block of encrypted data. We propose a new public key cryptosystem and a Key Exchange Protocol based on the generalization of discrete logarithm problem using Non-abelian group of block upper triangular matrices of higher order. The proposed cryptosystem is efficient in producing keys of large sizes without the need of large primes. The security of both the systems relies on the difficulty of discrete logarithms over finite fields.

Keywords. Block matrices, Companion matrices, Diffie Hellman Key Exchange, Digital Signature, Discrete logarithm problem, Public key cryptography.

1. Introduction

Cryptography is a key technology in electronic key systems. It is used to keep data secret, digitally sign documents, access control and so forth. The two basic infrastructures used in cryptographic systems are public and private keys. Private (secret) key uses a single key for both encryption and decryption. Hence biggest difficulty with this approach is the distribution of keys which was solved by public key cryptography [1] the concept of which was introduced by Whitfield Diffie and Martin Hellman in 1975.

A lot of popular public key encryption systems are based on number theoretic problems whose algebraic structures are often abelian groups [2] which is especially true in the case of Diffie Hellman and Elgamal encryption system. In 1984 Odoni, Vardharajan and Sanders [3] introduced the use of matrices over finite fields which were non abelian groups. In crypto 2000 Ko et al. proposed a new cryptosystem based on Braid groups. In 2006 another matrix based key exchange protocol was proposed by Climent et al. [4] and recently Alvarez et al. [5], [6], [7] proposed a DH key exchange based on block upper triangular matrices of order 2x2.

In this paper we propose a public key cryptosystem and a key exchange protocol using block upper triangular matrices of higher order which form a non abelian group. These matrices when defined over Z_p can generate sets of a large and known order.

The rest of the paper is organized as follows. Section 2 and 3 gives the description of the system along with the proof of simple theorems. Section 4 explains DH key exchange protocol by the proposed method. In Section 5 the concept of Digital signature is given and the paper is concluded in section 6.

2. Description of the system

The following is the description of underlying group structure. Some basic definitions and theorems required for the proposed cryptosystem are explained. For a given prime p and r, s, t Є $\mathbb{N}$ let $Gl_r(\mathbb{Z}_p)$, $Gl_s(\mathbb{Z}_p)$ and $Gl_t(\mathbb{Z}_p)$ represent invertible matrices of order rxr, sxs and txt respectively , $\mathbb{Z}_p$ being the set of integers modulo p. Further let $mat_{rxs}(\mathbb{Z}_p)$, $mat_{rxt}(\mathbb{Z}_p)$ and $mat_{sxt}(\mathbb{Z}_p)$ denote matrices of size rxs, rxt and sxt respectively also with elements in $\mathbb{Z}_p$. We define a set of block upper triangular matrices Ɵ = (M_1, M_2 ...M_m) with

$$M = \begin{bmatrix} A & X & Y \\ 0 & B & Z \\ 0 & 0 & C \end{bmatrix}$$

where A Є $Gl_r(\mathbb{Z}_p)$, B Є $Gl_s(\mathbb{Z}_p)$, C Є $Gl_t(\mathbb{Z}_p)$,

$X \in \mathrm{mat}_{rxs}(\mathbb{Z}_p)$, $Y \in \mathrm{mat}_{rxt}(\mathbb{Z}_p)$, $Z \in \mathrm{mat}_{sxt}(\mathbb{Z}_p)$.

Theorem 1. The set Θ forms a non-abelian group with respect to multiplication of matrices.

Proof:

Closure & Associative: Obvious by the definition.

Identity: The identity element is

$$\begin{bmatrix} I_r & 0 & 0 \\ 0 & I_s & 0 \\ 0 & 0 & I_t \end{bmatrix}$$

I_r, I_s and I_t being identity matrices of order rxr, sxs and txt respectively.

Inverse: For every element M = $\begin{bmatrix} A & X & Y \\ 0 & B & Z \\ 0 & 0 & C \end{bmatrix} \in \Theta$

there exists an element M^{-1} =

$$\begin{bmatrix} A^{-1} & -A^{-1}XB^{-1} & A^{-1}XB^{-1}ZC^{-1} - A^{-1}YC^{-1} \\ 0 & B^{-1} & B^{-1}ZC^{-1} \\ 0 & 0 & C^{-1} \end{bmatrix}.$$

Also for $M_1, M_2 \in \Theta$, $M_1M_2 \neq M_2M_1$.

Theorem 2. Let M = $\begin{bmatrix} A & X & Y \\ 0 & B & Z \\ 0 & 0 & C \end{bmatrix} \in \Theta$. For any non negative integer h, we have

$$M^h = \begin{bmatrix} A^h & X^{(h)} & Y^{(h)} \\ 0 & B^h & Z^{(h)} \\ 0 & 0 & C^h \end{bmatrix} \qquad (2.1)$$

where

$$X^{(h)} = \sum_{i=1}^{h} A^{h-i} X B^{i-1} \qquad (2.2)$$

$$Z^{(h)} = \sum_{i=1}^{h} B^{h-i} Z C^{i-1} \qquad (2.3)$$

$$Y^{(h)} = \sum_{i=1}^{h} A^{h-i} Y C^{i-1} + \sum_{\substack{i=0 \\ i+j \le h-2}}^{h-2} A^i X B^j Z C^{h-i-j-2} \qquad (2.4)$$

Proof: We apply induction method on h.

For h = 2, we have

$$M^2 = \begin{bmatrix} A & X & Y \\ 0 & B & Z \\ 0 & 0 & C \end{bmatrix} \begin{bmatrix} A & X & Y \\ 0 & B & Z \\ 0 & 0 & C \end{bmatrix}$$

$$= \begin{bmatrix} A^2 & AX+XB & AY+YC+XZ \\ 0 & B^2 & BZ+ZC \\ 0 & 0 & C^2 \end{bmatrix}$$

$$= \begin{bmatrix} A^2 & X^{(2)} & Y^{(2)} \\ 0 & B^2 & Z^{(2)} \\ 0 & 0 & C^2 \end{bmatrix},$$

where $X^{(2)} = AX + XB$

$Y^{(2)} = AY + YC + XZ$

$Z^{(2)} = BZ + ZC$ which is true.

Assuming that (2.1) is true for h-1, we prove it for h.

Suppose M^{h-1} = $\begin{bmatrix} A^{h-1} & X^{(h-1)} & Y^{(h-1)} \\ 0 & B^{h-1} & Z^{(h-1)} \\ 0 & 0 & C^{h-1} \end{bmatrix}$

Then

$M^h = M.M^{h-1}$

$$= \begin{bmatrix} A & X & Y \\ 0 & B & Z \\ 0 & 0 & C \end{bmatrix} \begin{bmatrix} A^{h-1} & X^{(h-1)} & Y^{(h-1)} \\ 0 & B^{h-1} & Z^{(h-1)} \\ 0 & 0 & C^{h-1} \end{bmatrix}$$

$$= \begin{bmatrix} A^h & AX^{(h-1)} + XB^{h-1} & AY^{(h-1)} + XZ^{(h-1)} + YC^{h-1} \\ 0 & B^h & BZ^{(h-1)} + ZC^{h-1} \\ 0 & 0 & C^h \end{bmatrix}$$

Considering the term $AY^{(h-1)} + XZ^{(h-1)} + YC^{h-1}$

using equations (2.2), (2.3) and (2.4) we have

$$AY^{(h-1)} + XZ^{(h-1)} + YC^{h-1}$$

$$= A\left(\sum_{i=1}^{h-1} A^{h-1-i} Y C^{i-1} + \sum_{\substack{i=0 \\ i+j \le h-3}}^{h-3} A^i X B^j Z C^{h-i-j-3} \right)$$

$$+ X\left(\sum_{i=1}^{h-1} B^{h-1-i} Z C^{i-1} \right) + YC^{h-1}$$

$$= \left(\sum_{i=1}^{h-1} A^{h-i} Y C^{i-1} + \sum_{\substack{i=0 \\ i+j \le h-3}}^{h-3} A^{i+1} X B^{j} Z C^{h-i-j-3} \right)$$

$$+ \left(\sum_{i=1}^{h-1} X B^{h-1-i} Z C^{i-1} \right) + Y C^{h-1}$$

$$= \left(\sum_{i=1}^{h-1} A^{h-i} Y C^{i-1} + Y C^{h-1} \right)$$

$$+ \left(\sum_{\substack{i=0 \\ i+j \le h-3}}^{h-3} A^{i+1} X B^{j} Z C^{h-i-j-3} \sum_{i=1}^{h-1} X B^{h-1-i} Z C^{i-1} \right)$$

$$= \sum_{i=1}^{h} A^{h-i} Y C^{i-1} + \sum_{\substack{i=0 \\ i+j \le h-2}}^{h-2} A^{i} X B^{j} Z C^{h-i-j-2}$$

$= Y^{(h)}$.

which is similar to equation (2.4).

Equations (2.2) and (2.3) can be proved in the same way.

3. Order of the elements

Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots\ldots\ldots\ldots\ldots + a_{r-1}x^{r-1} + x^r$

$g(x) = b_0 + b_1x + b_2x^2 + \ldots\ldots\ldots\ldots\ldots + b_{s-1}x^{s-1} + x^s$

$h(x) = c_0 + c_1x + c_2x^2 + \ldots\ldots\ldots\ldots\ldots + c_{t-1}x^{t-1} + x^t$

be primitive polynomials in $\mathbb{Z}_p[x]$ and $\overline{A}, \overline{B}, \overline{C}$ be the corresponding companion matrices given by

$$\overline{A} = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \ldots & -a_{n-2} & -a_{n-1} \end{bmatrix}$$

Let P, Q, R be invertible matrices, we construct

$$A = P\overline{A}P^{-1}, B = Q\overline{B}Q^{-1}, C = R\overline{C}R^{-1}$$

so that the order of matrix M Є Θ as given by Odoni Vardhrajan and Sanderson [3] is

$$o(M) = \operatorname{lcm}(p^r - 1, p^s - 1, p^t - 1)$$

order of matrix M obtained for different values of r, s and t are given below.

Table1. Order of M for small values of p.

For p = 3

r	s	t	o(M) bits
31	32	29	2^{145}
60	61	59	2^{279}
30	131	127	2^{605}
216	217	207	2^{1004}

For p = 7

r	s	t	o(M) bits
31	32	29	2^{230}
60	61	59	2^{445}
130	131	127	2^{963}
216	217	207	2^{1599}

Table2. Order of M for large values of p.

For p = 2^{50} bits

r	s	t	o(M) bits
2	3	5	2^{400}
3	5	8	2^{700}
4	5	9	2^{800}
5	6	11	2^{1000}

For p = 2^{80} bits

r	s	t	o(M) bits
2	3	5	2^{640}
3	5	8	2^{1120}
4	5	9	2^{1280}
5	6	11	2^{1600}

Table3. Comparison of o(M) by Alvarez et al. and proposed method

P	r	s	t	o(M_A)bits	o(Mp)bits
5	30	33	29	39	62
11	64	63	62	67	185
31	16	15	14	40	63
257	32	31	30	93	217

Table 3 above gives the values of order of M obtained by Alvarez et al. o($M_{A)}$ and the values obtained by our proposed method o($M_{p)}$. It can be seen that the order of M by our proposed method is very large as compared to that obtained by Alvarez et al. Thus by using block matrices of order 3x3 in comparison to 2x2 we can generate matrices (keys) of very large orders and hence the proposed cryptosystem is secure against the Brute force attacks. Also, from table 1 it can be seen that the values of prime p need not be very large thereby avoiding primality tests.

4. Diffie Hellman Key Exchange

Public key cryptosystem can be used to provide a secure method for exchanging secret keys. The most common key exchange algorithm is the DH key exchange algorithm [8]. The original protocol uses the multiplicative group of integers modulo p. Here we apply our proposed cryptosystem using matrices.

Shared secret key generation

Two persons Alice and Bob wish to exchange a secret message. They first develop a common key for which they perform the following steps.

1. First Alice and Bob agree on $p \in \mathbb{Z}$ and matrices $M_1, M_2 \in \Theta$ of orders m_1 and m_2 respectively.

2. Alice randomly generates two private (secret) keys r, s with $1 \le r \le m_1$ and $1 \le s \le m_2$ and computes $C = M_1^r M_2^s$.

3. She sends C to Bob as her public key.

4. Bob also generates two private (secret) keys u, v with $1 \le u \le m_1$, $1 \le v \le m_2$ and computes $F = M_1^u M_2^v$

5. Bob calculates $D = M_1^u C\ M_2^v$

$$= M_1^u (M_1^r M_2^s) M_2^v$$

$$= M_1^{u+r}\ M_2^{s+v}$$

$$= M_1^{r+u}\ M_2^{v+s}$$

$= M_1^r\ M_1^u\ M_2^v\ M_2^s$ and sends this value to Alice as his public key.

6. Alice calculates $M_1^{-r} D\ M_2^{-s}$

$$= M_1^{-r} (M_1^r\ M_1^u M_2^v\ M_2^s)\ M_2^{-s}$$

$$= M_1^u M_2^v$$

$$= F$$

Thus Alice and Bob reach at the same value F. This F becomes their shared secret key. Now Alice and Bob can send and receive secret messages. An attacker could know the values of M_1 and M_2 but the difficulty of computing the shared key F is similar to the difficulty of solving the discrete logarithm problem.

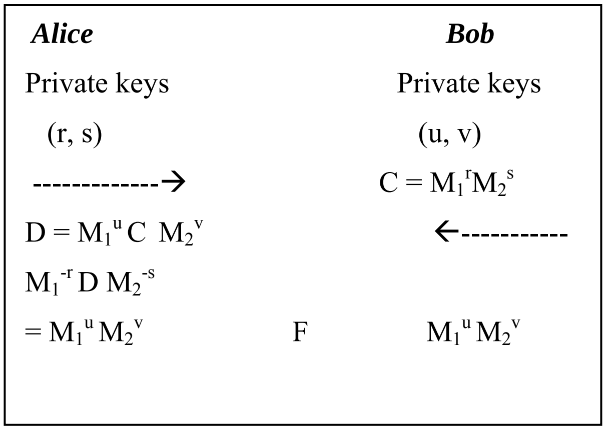

Fig 1. Key Exchange Protocol

Encryption Procedure:

1. Alice encrypts the message in the form of a matrix Δ of order r x t
2. Alice computes the matrix

$$T_1 = \begin{bmatrix} A_1 & X_1 & \Delta \\ 0 & B_1 & Z_1 \\ 0 & 0 & C_1 \end{bmatrix} \text{ and } F$$

3. Alice calculates the cipher text $C = T_1 F$ and sends this to Bob.

Decryption Procedure:

1. As F is the shared key of both, Bob calculates $T_1 = CF^{-1}$

2. Bob recovers the message Δ selecting the respective block of T_1.

5. Digital Signature Scheme

A digital signature [9], [10] is basically a way to ensure that an electronic document is authentic. In the process of Digital signature the sender uses a signing algorithm to sign the message and sends, the message and the signature to the receiver. The receiver receives the message and the signature and applies the verifying algorithm to the combination. If the result is true, the message is accepted, otherwise it is rejected.

Let us assume that Alice has sent the message Δ to Bob in the form of matrix T_1 and they both have generated the shared secret key F. Now Alice wants to sign her message to prove her authenticity. For this she follows the following procedure.

1. Alice generates a random number r

2. Computes F^r

3. Calculates $Q = T_1 + F^r$
4. Sends the message T_1 along with the digital Signature $S = (r, Q)$.

Now Bob wants to verify the signature for which he uses verifying algorithm.

1. Bob also gets the shared key F and computes F^r
2. Calculates $T_1 = Q - F^r$
3. Gets the value of Y from T_1
4. Compares Y with Δ
5. If $Y = \Delta$ the signature is accepted otherwise it is rejected.

Clearly Bob needs the original message for verifying the signature.

6. Conclusion

By defining a non-abelian group of block upper triangular matrices of order 3x3 or analogously higher order we propose a public key cryptosystem and a key exchange protocol based on the generalization of the discrete logarithm problem (DLP). The proposed cryptosystem can generate keys of very large sizes with small prime numbers. Further it is efficient in providing security against common attacks. Brute force attacks are infeasible if sufficiently large sizes of matrices M_1 and M_2 are chosen. Similarly by choosing big values for the private keys r, s, v and w man in the middle attack can be avoided.

References

[1] Stallings, W. Cryptography and Network Security, Principles and Practice, Third Edition Prentice Hall, New Jersey (2003).
[2] Koblitz, N.A Course in Number Theory and Cryptography. Springer-Verlag (1987).
[3] Odoni, R.W.K.,Varadharajan,V.,Sanders, P.W. Public Key Distribution in Matrix Rings. Electronic Letters. 20: (1984) 386-387.
[4] J. Climent, E. Gorla and J. Rosenthal, Cryptanalysis of the cfvz cryptosystem, Advances in Mathematics of Computations, 1 (2007), pp. 1-11.
[5] Alvarez,R., Tortosa,L., Vicent J-F.,Zamora, A public Key Cryptosystem based on Block upper Triangular Matrices. WSEAS Information security and Privacy(2005) 163-168.
[6] Alvarez, R.,Martinez,F-m., Vicent,J.F., Zamora A. A New public key cryptosys tem based on Matrices. WSEAS TransacTions on computers, vol.5-1 (2006) 165-170.
[7] Alvarez,R., Tortosa,L.,Vicent J- F.,Zamora, A. Analysis and design of a secure key exchange scheme. Information sciences 179 (2009) 2014-2021.
[8] Diffie,W.,Hellman, New directions in Cryptography. IEEE Trans.Information Theory.22, (1976) 644-654.
[9] Elgamal,T.A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Trans.Inform.Theory.31: (1985) 469-472.
[10] Rivest, R.Shamir, A.Adleman,L. A method for obtaining Digital Signatures and Public Key Cryptosystems. ACM Communications. 21: (1978) 120-126.

Authors Profile

1. Dr. H. k. Pathak received Post Graduate degree in Mathematics from Pt. Ravishanker Shukla University, Raipur. He was awarded Ph.D in 1988 by the same University. He has published more than 185 research papers in various international journals in the field of non linear analysis-Approximation and expansion, Calculus of variations and optimal controls Optimization, Field theory and polynomials, Fourier analysis, General topology, Integral equations, Number theory, Operations research, Mathematical programming, Operator theory, Sequences, series, summability. At present he is Professor and Head in S.o.S in Computer science & IT in Pt. Ravishanker Shukla University.

2. Mrs. Manju Sanghi received the post graduate degree in Mathematics from Ravishanker University Raipur in 1996. Since 2001 she has been working as lecturer in Rungta college of Engineering & Technology Bhilai. Currently she is pursuing PhD from School of studies in Mathematics Pt. Ravishanker Shukla University Raipur. Her research interests include cryptography.