IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 4, Issue 2, April - May, 2016
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

KEY EXCHANGE PROTOCOL WITH GAUSSIAN INTEGER MATRICES

B.P.Tripathi [1], Shruti Nathani[2]
Department of Mathematics
Govt. N.P.G.College of Science
Raipur(C.G.), India.

Abstract

Many security algorithms currently in use rely heavily on integer arithmetic modulo prime numbers. Gaussian integers can be used with most security algorithms that are formulated for real integers. By taking the advantage of matrix multiplication of two Gaussian integer matrices , we introduce a Diffe-Hellman key exchange protocol with Gaussian integer matrices to establish a common shared secret key between two communicating parties.

Keywords : Cryptography, Private Key, Public Key, Gaussian integer matrices,Key exchange protocol

(AMS) Mathematics Subject Classification No : **94A60**

1 INTRODUCTION

Cryptography is a key technology in electronic security system. Modern cryptographic techniques have many uses, such as to digitally sign documents , for access control, to implement electronic money and for copyright protection. The history of cryptography dates back thousands of years over most of this time,it has been a history of symmetric cryptography. It appeared obvious that the only way for several parties to communicate securely is to share a secret method or key.Key exchange is the weakest link of symmetric cryptography.The challenge of exchanging secret keys securely is magnified when there are many parties that need to communicate.

The revolution in cryptography happened in 1970s when public key or asymmetric cryptography was introduced. In 1976,Diffe and Hellman published a revolutionary paper titled "New directions in cryptography "[11], where they introduced the concept of public key or asymmetric cryptography . In addition they introduced the method of exchanging keys known as Diffe-Hellman(D-H) key exchange protocol. The D-H key exchange protocol relies on the difficulty of the discrete logarithm problem.

Modern cryptography is fundamentally concerned with the problem of secure private communication. Suppose two parties , Alice and BOb ,wish to communicate privately over a public channel(for instance , a telephone line with an evesdropper).If Alice and Bob are able to meet , privately , beforehand , and agree on some common secret key, then it becomes easy for them to achieve such private communication. But Alice and Bob might not be able to first meet in private and agree on a key.In this case, we ask under what assumptions they can steel agree on a common secret key , where their conversation is conducted entirely in public.[8]

A secret key exchange is a protocol where Alice and Bob having no secret information in common to start , are able to agree on a common secret key, conversing over a public channel.

The first attempt to using matrices over a finite field in a key exchange scheme was made by Odoni , Varadharajan and Sanders in 1984[10]. They use an invertible matrix as a group generator and then proceed as in the usual Diffie-Hellman key exchange protocol. In 2005, E. Stickel[2] gives a new method for exchanging secret keys. Another matrix based key exchange protocol was proposed by Climent et. al[7] in 2006. In 2012[6] , Climent et al. proposed a first key exchange protocol over noncommutative rings.

2 Introduction to Gaussian Integers and Matrices over Gaussian Integers :

Carl Friedrich Gauss introduced the ring of Gaussian integers in 1829-1831. Gaussian integers are complex numbers with integers as both real and imaginary parts. He formulated many properties of Gaussian integers like properties of factorization and the concept of Gaussian primes. Gauss used them as a tool to prove some theoretical results.The properties of Gaussian integers and Gaussian primes are well known and formulated so they are going to be used as facts.[3],[4]

2.1 Definition :

The Gaussian integers ,

$$Z[i] = \{a + ib | a, b \in Z\}$$

where a & b are integers and $i^2 = -1$. clearly the sum ,difference and product of two Gaussian integers are Gaussian integers , but the division of two Gaussian integers is $(a + ib)|(c + id)$ only if there is an $(e + if)$such that

$$(a + ib)(e + if) = (ae - bf) + i(af + be) = (c + id).$$

2.2 Gaussian Integer Matrix

A matrix whose elements may contain Gaussian integers, is called Gaussian integer matrix. Let A be an $n \times n$ Gaussian integer matrix defined as $a_{ij} + ib_{ij}$

$$A = \begin{bmatrix} a_{11} \pm ib_{11} & \cdots & a_{1n} \pm ib_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} \pm ib_{n1} & \cdots & a_{nn} \pm ib_{nn} \end{bmatrix}$$

All the definition of the integer matrices still hold in case of Gaussian integer matrices.

3 The Key Exchange Protocol of Climent et al.

Climent et al.[6] introduces a key exchange protocol over a noncommutative ring R.
Protocol: The element $M, N \in R$ are public.

1. Alice and Bob chooses their private keys $(r, s), (u, v) \in \mathbb{N}^2$ respectively.
2. Alice computes her public key $P_A = M^r N M^s$ and send it to Bob and Bob computes his public key $P_B = M^u N M^v$ and send it to Alice.
3. Alice and Bob compute $S_A$and S_B respectively as $S_A = M^r P_B M^s$ and $S_B = M^u P_A M^v$.
   The shared secret is $S_A = S_B$.

Note that if $MN = NM$ then
$P_A = M^r N M^s = N M^r M^s$ and $P_B = M^u N M^v = N M^u M^v$,
Therefore,

$$NS_A = NM^r M^u N M^v M^s = M^r N M^s M^u N M^v = P_A P_B,$$
$$NS_B = NM^u M^r N M^s M^v = M^u N M^v M^r N M^s = P_B P_A,$$

That is ,$NS_A = NS_B$, because $P_A P_B = P_B P_A$. So , the shared secret $S_A = S_B$ may be easily obtained by an unauthorized part , since N, P_A and P_B are public. Thus we need that ,$MN \neq NM$.

To avoid this weakness ,Climent et. al use polynomials over a non commutative ring instead of this we propose a new key exchange protocol using Gaussian integer matrices, that means in our protocol we take both M and N are the two Gaussian integer matrices over Z[i].

Because of taking M and N as the Gaussian integer matrices , in our protocol ,$MN = NM$, is not possible , because multiplication of two matrices is not commutative. Also in the proposed protocol we get P_A and P_B both are the Gaussian integer matrices ,so $P_A P_B = P_B P_A$ is also not possible.So the shared secret $S_A = S_B$ may not be easily obtained in our proposed protocol.

4 Proposed Protocol

In this section we propose a Diffe-Hellman key exchange protocol using two Gaussian integer matrices over Z[i].The element M and N are two Gaussian integer matrices of any order m. These two matrices M and N are publicly known.

1. Alice and Bob chooses their private keys $(r, s), (u, v) \in \mathbb{N}^2$ respectively.
2. Alice computes her public key $P_A = M^r N M^s$ and send it to Bob and Bob computes his public key $P_B = M^u N M^v$ and send it to Alice.
3. Alice and Bob compute $S_A$and S_B respectively as $S_A = M^r P_B M^s$ and $S_B = M^u P_A M^v$.

   The shared secret is$S_A = S_B$, As we can see in the following theorem.

4.1 Correctness of Algorithm

Theorem 4.1 *The equation $S_A = S_B$ is correct .*

Proof: We have,

$$S_A = M^r P_B M^s$$
$$S_A = M^r M^u N M^v M^s$$
$$S_A = M^{r+u} N M^{v+s}$$
$$S_A = M^{u+r} N M^{s+v}$$
$$S_A = M^u M^r N M^s M^v$$
$$S_A = M^u P_A M^v = S_B$$

$Thus, S_A = S_B$.

4.2 Example:

Choose two Gaussian integer matrices $M = \begin{bmatrix} i & 1+i \\ 2i & 3i \end{bmatrix}$ and $N = \begin{bmatrix} 4i & 3i \\ 2+i & i \end{bmatrix}$.

1. Alice and Bob chooses their private keys $(r, s) = (1, 2) \in N^2$and $(u, v) = (3, 4) \in N^2$.
2. Alice compute her public key $P_A = M^r N M^s = \begin{bmatrix} i & 1+i \\ 2i & 3i \end{bmatrix}^1 \begin{bmatrix} 4i & 3i \\ 2+i & i \end{bmatrix} \begin{bmatrix} i & 1+i \\ 2i & 3i \end{bmatrix}^2$

$$= \begin{bmatrix} -3+3i & -4+i \\ -11+6i & 9 \end{bmatrix} \begin{bmatrix} -3+2i & -4+4i \\ -8 & -11+2i \end{bmatrix}$$

Thus ,$P_A = \begin{bmatrix} 35-23i & 42-43i \\ 93-40i & 119-86i \end{bmatrix}$

Now , Bob computes his public key $P_B = M^u N M^v = \begin{bmatrix} i & 1+i \\ 2i & 3i \end{bmatrix}^3 \begin{bmatrix} 4i & 3i \\ 2+i & i \end{bmatrix} \begin{bmatrix} i & 1+i \\ 2i & 3i \end{bmatrix}$

$$= \begin{bmatrix} -10-11i & -17-13i \\ -4-30i & -14-41i \end{bmatrix} \begin{bmatrix} 4i & 3i \\ 2+i & i \end{bmatrix} \begin{bmatrix} 37-44i & 40-72i \\ 112-32i & 149-76i \end{bmatrix}$$

$$P_B = \begin{bmatrix} 23-83i & 46-47i \\ 133-112i & 131-26i \end{bmatrix} \begin{bmatrix} 37-44i & 40-72i \\ 112-32i & 149-76i \end{bmatrix}$$

Thus ,$P_B = \begin{bmatrix} 847-10819i & -1774-15475i \\ 13833-17100i & 14799-27886i \end{bmatrix}$

Now Alice sends her public key P_A to Bob and Bob sends his public key P_B to Alice.

3. Now Alice computes her shared secret key S_A ,

$$S_A = M^r P_B M^s = \begin{bmatrix} i & 1+i \\ 2i & 3i \end{bmatrix}^1 \begin{bmatrix} 847-10819i & -1774-15475i \\ 13833-17100i & 14799-27886i \end{bmatrix} \begin{bmatrix} i & 1+i \\ 2i & 3i \end{bmatrix}^2$$

$$= \begin{bmatrix} 41752-2420i & 58160-14861i \\ 72938+43193i & 114608+40849i \end{bmatrix} \begin{bmatrix} -3+2i & -4+4i \\ -8 & -11+2i \end{bmatrix}$$

Thus ,$S_A = \begin{bmatrix} -585696+209652i & -767366+456479i \\ -1222064-310495i & -1806910-101143i \end{bmatrix}$

Bob computes his shared secret key S_B ,

$$S_B = M^u P_A M^v = \begin{bmatrix} i & 1+i \\ 2i & 3i \end{bmatrix}^3 \begin{bmatrix} 35-23i & 42-43i \\ 93-40i & 119-86i \end{bmatrix} \begin{bmatrix} i & 1+i \\ 2i & 3i \end{bmatrix}^4$$

$$= -\begin{bmatrix} 10+11i & 17+13i \\ 4+30i & 14+41i \end{bmatrix} \begin{bmatrix} 35-23i & 42-43i \\ 93-40i & 119-86i \end{bmatrix} \begin{bmatrix} 37-44i & 40-72i \\ 112-32i & 149-76i \end{bmatrix}$$

$$= -\begin{bmatrix} 2704+684i & 4034+117i \\ 3772+4211i & 6650+4763i \end{bmatrix} \begin{bmatrix} 37-44i & 40-72i \\ 112-32i & 149-76i \end{bmatrix}$$

$$S_B = -\begin{bmatrix} 585696-209652i & 767366-456479i \\ 1222064+310495i & 1806910+101143i \end{bmatrix}$$

$$S_B = \begin{bmatrix} -585696+209652i & -767366+456479i \\ -1222064-310495i & -1806910-101143i \end{bmatrix}$$

Thus $S_A = S_B$.

5 Conclusion:

The D-H key exchange is not new by any means and over the year numerous mathematicians have proposed many ideas for the key exchange to take place in.

In this paper we show how Gaussian integer matrices can be used in order to provide protocols that allow a key exchange in a secure manner .

We have improved upon the central idea by suggesting the use of Gaussian integer matrices ,that is , matrix multiplication of two Gaussian integer matrices is time consuming process. This idea therefore makes it harder for an attacker ,Oscar to find secret key .

References

1. D.R. Stinson , Cryptography. Theory and practice, CRC Press, Boca Raton FL 1995.
2. E. Stickel ,A new method for exchanging secret keys. In Proceeding of the Third International Conference on Information Technology and Application (ICITA'05) pages 426-430.Sidney , Australia 2005.
3. Gaussian Integer -Wikipedia the free encyclopedia,http://en.wikipedia.org/wiki/Gaussianintege
4. Gaussian Integer-from wolfarm mathworld.mathworld.wolfarm.com/Gaussianinteger.html
5. J. Buchmann , Introduction to Cryptography ,October (2003).
6. J.J.Climent , P.R.Navarro and L.Tortosa ,"Key exchange protocols over non-commutative rings ,The case of END($\mathbb{Z}_P \times \mathbb{Z}_p{}^2$)" may 17, 2012 , AMS.
7. J. Climent , E. Gorla and J. Rosenthal , Cryptanalysis of the CFVZ cryptosystem Advances i mathematics of computations. (2007) pp-1-11.
8. M. Bellare , L. Cowen , S. Goldwasser "On the structure of secret key exchange protocols" CRYPTO ' 89 LNCS 435 ; pp. 604-605,Springer-Verlag Berlin Heidelberg 1990.
9. N. Koblitz, A course in number theory and cryptography, Springer Verlag 1987.
10. R.W.K. Odoni and V. Vardharajan and P.W. Sanders . Public key distribution in matrix rings. Electronic letters,20:386-387(1984).
11. W.Diffie , M .Hellman ,New Directions In Cryptography ,IEEE Transactions on information theory 22(1976) 644-654.