Dynamic Blind Group Digital Signature Scheme in E-Banking

Malik Sikandar Hayat Khiyal, Aihab Khan, Saba Bashir, Farhan Hassan Khan, and Shaista Aman

Abstract---**This paper describes the signature scheme in which an individual can sign a document or messages on behalf of entire group. Here, a dynamic group blind signature scheme has been proposed, which is an extension of [L n R] and [B] Group Blind signature scheme. Proposed blind signature scheme has two separate authorities; an issuer, for issuing the membership certificate to group members and an opener, who can open the identity of a signature's originator in the case of a dispute. This scheme is based on the concept of PKI (public key infrastructure) environment and three key requirements i.e., Traceability, Anonymity and Non-Frameability. The problem of revocation of identity in group signatures has also solved in this paper. Before that many constructions have been proposed, however, a recurrent problem concerning with the revocation of group members, remained the same. Therefore, an efficient revocation algorithm is used to revoke the members and prevent frauds at the time of signing a document in future. Also the security of group keys is the major concern of this research.**

Index Terms---**Blind Digital Signature, Cryptography, Digital Signature, Dynamic Group, Group Digital Signature.**

I. Introduction

Digital Signature Schemes enable people to electronically "sign" their documents in a secure and efficient manner. It is difficult to forge the signatures, yet verifying the validity of the digital signature is easy. It works on the principal of PKI. The first construction of digital signature based on a number-theoretic assumption was given by Rivest [1]. However, the formal definition of security for digital signatures was first outlined by Goldwasser [2]. They discussed the concept of an existential adaptive chosen-message attack which is the strongest form of possible attack, one could imagine on a digital signature. An interesting variant on the basic Digital Signature is the Blind Digital Signature. Chaun [3] introduced the concept of a Blind Digital Signature. It describes the spender anonymity in Electronic Cash Systems. The theme of this concept is that, there are some signatures which require that a signer be able to sign a document without knowing its contents. Moreover, when the signer ever sees the document/signature pair, he should not be able to determine when or for whom he signed it [4]. In Dynamic Group Blind Digital Signature, the number of group member is not fixed and can be increased as a result of join algorithm. This dynamic property creates a problem that the members who don't want to use the authority of signing, the document will have the membership of group and can misuse this authority in future. Therefore, a mechanism is required which should be able to resolve the discrepancies in existing techniques.

Hence, a new scheme based on cryptographic construct known as Dynamic Group Blind Digital Signature is proposed. It combines the existing notion of a Group Digital Signature [r] and a Blind Digital Signature. In this scheme, dynamic property is modified and the number of members can be increased or decreased as a result of join and revoke algorithms. This additional feature makes the scheme flexible and secure. A digital signature can be verified by confirming that a verifier must obtain a public key and have assurance that public key corresponds to the signer's private key. The trusted third party, which distributes the keys, is termed as a "Certification Authority". If the subscriber loses control of the private key, the certificate becomes unreliable. While misusing anonymity, a cheating member must be revoked by the authority, making him unable to sign in the future, but without scarifying the security of group signatures[5]. The main feature is member revocation. It revokes the membership when one leaves the group. To prevent fraud, revocation algorithm cancels the membership when a member leaves the group or when the signer time duration of membership finishes. With increasing awareness about security, it is being hoped that the implemented technique earn real-world acceptance in the years to come.

The paper is organized as follows. Section 2 describes the related work done in the problem domain. Framework overview is given in section 3. The proposed Dynamic Blind Group Digital Signature Scheme is discussed in section 4. Testing, results and analysis are discussed in section 5 and section 6 describes the conclusion.

II. Related Work

Bellare Shiy, Zhangz in [6] presents a novel idea of introducing a new case in group signature scheme where groups are dynamic in nature. It describes the basics for dynamic group signatures in the form of model, strong formal definitions of security, and a construction proven secure under general assumptions. This is an important and useful step as it helps in bridging the gaps between the previous practical works and delivers a basis on which existing practical schemes may be evaluated in future or proven secure. An extension of the existing treatment of static group to the dynamic case has been provided. Dynamic groups are more complex, bringing in new elements, security requirements and issues. The important features of the proposed technique are PKI, two authorities, trust levels and three key requirements. The major drawback of the proposed technique is that it is polynomial-time but does not possess efficiency.

M.Bellare, D.Micciancio and B. Warinschi in [7] defines

Manuscript received March 23, 2011 ;revised July 11, 2011

the multiple definitions the main requirements for ambiguity and how to trace it. Their experiments were based on assumptions that trapdoor permutations are required to meet the formal definitions. They also assume that the noval attack capabilities and success measures to make strong versions of the core requirements e.g., full anonymity and full traceability to check only two security properties make it easier to give formal proofs of security when new group signature schemes are invented. The disadvantages of this scheme are, for the setting in which the group is static, the number and identities of numbers is decided at the time the group is setup and numbers cannot be added later. Their paper provided the formal definitions of security and provably-secure construction for dynamic group signatures as the subject of ongoing work. In this scheme member can join and leave the group overtime. Their construction can be easily adopted to satisfy either definition of security for fully dynamic groups e.g. by re-keying the entire group at the end of each time period.

J.Camensich and M.Michels in [8] proposed an idea of group signature scheme. It is different from existing schemes in this way that it does not depend on size of the group and is suitable for large group having long public key. It is based on a variation of RSA (Rivest, Shamir and Adleman) problem called strong RSA assumption. Signatures can be verified by single public key without revealing the identity of signer. The membership manager is responsible for the system setup and for adding group members while manager has the ability to revoke the anonymity of signatures. This scheme has overcome the problems of length of public key and of the signature, as were in previous schemes, as well as the computational effort for signing and verifying, and independent of the number of the group members. Furthermore, the public key remains unchanged if new members are added to the group. It also conceals the size of the group.

A-Lysyanskaya, Z. Ramzan in [9] constructs a practical Group Blind Signature Scheme. This scheme is an extension of Group Signature Scheme, proposed in [10] with the addition of blindness property. This construct shows electronic cash system in which multiple banks can securely distributes anonymous and untraceable e-cash. Group size does not relate to space, time and computational complexities. Blindness, unforgeibility, undeniable signer identity, Signer anonymity, unlinkibilty and security against framing attacks are the major properties of this approach. But the main drawback is not being fully dynamic in nature i.e. a member once joined the group remain there throughout the life of group. It means it does not provide the concept of revocation. Other limitations are that a trusted entity chooses the signing key for group member in addition with public key and opening key. The reason is that identities of group members are fixed. It also does not allow one to add members to the group with time; hence, they also require an uncomfortably high degree of trust in the party performing setup [11].

Another scheme proposed in [12] is as competent to the scheme proposed by Camensich and Stadler [10], where all the operations, except open, take constant time. The open protocol time is directly proportional to the size of the group. All signatures are based on constatnt space and the communication complexity per signature is constant. Approach proposed in [13] does not concern about the size of the document to be signed because of the hash of the message. A change of security parameter affects both signing and verifying operations. Partially blind signatures gave us the idea of linkage between the common information, which is not blinded. As the increase in security parameter, the time and memory required to sign or verify signatures shoots up substantially. This gives the trade off between the strength of security and resource overhead.

Compared to the most efficient scheme given in [12], this scheme [8] is about three times more efficient and signatures are about three times shorter. However, the registration protocol is less efficient in this scheme. Signatures made shorter without compromising the security of the scheme.

III. Framework Overview

The framework overview of the proposed technique is shown in Fig 1.

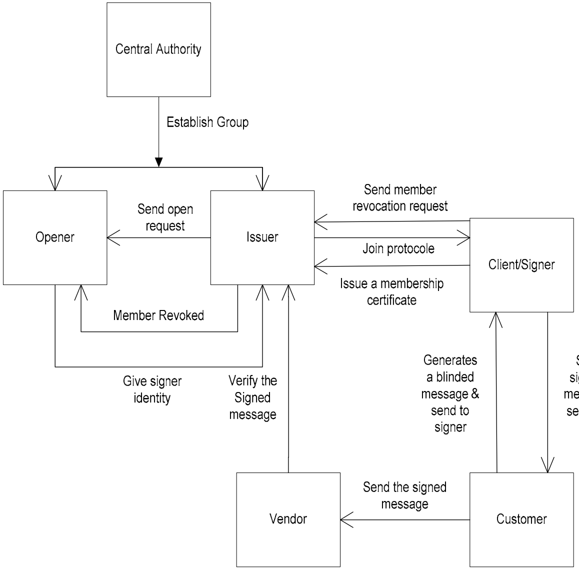
Central Authority
Establish Group
Opener
Send open request
Issuer
Send member revocation request
Join protocole
Client/Signer
Issue a membership certificate
Member Revoked
Give signer identity
Verify the Signed message
Generates a blinded message & send to signer
Signer signs the message & send back
Vendor
Send the signed message
Customer

Fig 1: Dynamic Blind Group Digital Signature Scheme

The entities involve in the scheme are as b :

Central Authority: This authority will establish the group.

Issuer: Appoints new members of the group.

Opener: Opens the signature to revoke the anonymity of the signer.

User: User is any person who wants to join the group.

Signer: Those members who have already joined the group and are allowed to create sign on the behalf of group.

Clients: Clients are those who send the request to signer to create a new sign.

Vendor: Vendor does not belong to the group but has the access to the group's public key.

The assumptions of this scheme are as follows:

1) There is some authority called Central Authority (CA), and it is treated as trusted entity. It can be called as an owner of the group.
2) CA appoints the group authorities, i.e. issuer and opener.
3) CA creates group keys.

4) CA establishes all the rules for group.
5) Issuer adds new members to the group, handles the group database, and has the right to delete public keys.
6) Opener has read-only access to the group database.
7) Each user has personal secret key associated with a personal certified public key.
8) The group manager has also the certified pair of keys.
9) All public keys are published and are accessible to any one over a secure way.

Proposed Dynamic Blind Group Digital Signature Scheme has two separate authorities; an issuer and an opener. Issuer issues the membership certificate to group members for joining and revoking, whereas opener opens the identity of a signature's originator in the case of a dispute. These authorities have the power of establishing a group as well as revoking the particular member of the group if he leaves the group or if his time limit meets the specified criteria. These authorities are assigned to some specified tasks among each other so to share the load of work performed by central authority like verification of sign and opening the identity of the signer by opener. Issuer has both read/write accesses to the database whereas opener has just read access to the database. The revocation algorithm revokes the membership of the registered signer so that he becomes ineligible for signing documents in future. Client sends request for revocation and issuer revokes his membership in response, and when a member is revoked, it is necessary to inform the opener as well in order to make the verification and opening of the sign easier.

The notations used throughout the paper are elaborated in Table 1.

TABLE 1: NOTATIONS

Symbols	Description
DgbSk	Group Signature Secret Key
DgbPk	Group Signature Public Key used for verification
DgbEnc	Group Encryption Key
DgbDec	Group Decryption Key
DgbCrtCr	Group Certificate Creation Key used to verify member certificates
DgbCrtVf	Group Certificate Verification Key used to verify member certificates
Set-up ()	Set up Algorithm
Join ()	Join-Issue Algorithm
Revoke ()	Revoke Algorithm
Sign ()	Sign Algorithm
Verify ()	Verify Algorithm
Open()	Open Algorithm
IK	Issuer key
OK	Opener key
GS	Group Secret Key of the Member
GP	Group Public Key of the Member
PS	Personal Secret Key of the User
PP	Personal Public Key of the User
m	*m* is text file that is to be signed
m_{DS}	signed file

IV. Proposed Technique

The procedure of the proposed technique is given under. RSA key generation algorithm is used for encryption/decryption and for signature creation/verification.

A. Set-Up Algorithm

Set up algorithm is required to generate the secret keys GS (Group Secret Key of the Member) and GP (Group Public Key of the Member) that are used in further algorithms as secret parameters.

```
Algorithm: set-up()
Input: key size
Output: GS, GP (keys)
Determine key size of 1024 bits
// for GS and GP
Create group encryption and decryption keys i.e., DgbEnc and DgbDec    // through RSA
Create certificate for creation and verification i.e., DgbCrtCr and DgbCrtVf
Create group signature creation key DgbSk and group public key DgbPk
Assign DgbCrtCr to issuer as his IK.
Assign DgbCrtVf to opener as his OK
```

Fig 2: Set-Up Algorithm for DgbSS

Fig 2 shows set-up algorithm for Dynamic Blind Group Digital Signature Scheme. It is run by CA. In this algorithm, key size is the required input whereas GS and GP becomes the output of set-up algorithm. According to line 1, key size is decided; and it should be within the range of 1024 bits. From line 2, group encryption and decryption keys are created i.e., *DgbEnc* (Group Encryption Key) and *DgbDec* (Group Decryption Key). From line 3, certificate for creation and verification are created i.e., *DgbCrtCr* (Group Certificate Creation Key used to verify member certificates) and *DgbCrtVf* (Group Certificate Verification Key used to verify member certificates). At line 4, keys for group signature creation are generated where *DgbSk* is the Group Signature secret Key and *DgbPk* is the group signature public key that is further used for group verification. According to line 5-6, created *DgbCrtCr* and *DgbCrtVf* from line 3 are then assigned to issuer and opener as IK and OK respectively. *DgbEnc*, *DgbDec*, *DgbCrtCr*, *DgbCrtVf*, *DgbSk*, *DgbPk* are the inbuilt functions in C#, java.

B. Join Algorithm

Join algorithm is required to check the validity of client. If client is the member, then he can get/receive digital signature else not. Received digital signatures are then updated in the database.

```
Algorithm: Join ()
Inputs: user_id, type
Secret Parameter: GS
Output: Digital Signature
1. Enter user_id and type
   // if user wants to join type specifies either to join on permanent basis or temporary
2. if (user is valid) then
   // issuer checks the validity of user
3 hash_id =compute hash (user_id)
                         // through hash algorithm
4. Send (hash_id, type)
                         //send to server
5.    Put user_id and type in database
6.    Digital Signature =concatenate (hash_id, hash_secret)
      // hash_id = hashed value of user_id,
      // hash_secret = hashed value of GS
7.    Get (Digital Signature)
                         //from server side to client side
8.    Update database
9. else
10.   exit
11. endif
```

Fig 3: Join Algorithm for DgbSS

Fig 3 shows join algorithm for Dynamic Blind Group Digital Signature Scheme. Here, GS is the secret parameter whereas user_id and type are the required inputs for this algorithm, and digital signature gives the output. According to line 1, user who wants to join the group will send a join-request by providing his user_id and type i.e. wants to join on permanent or temporary basis. At line 2, issuer checks the validity of user, if he is valid then allows him to join and continue else from line 10, exit. For valid user (member), hash_id is calculated by applying hashing through hash function MD5 algorithm on user_id at line 3. From line 4-5 computed hash_id and type selected by user are sent to server, and then user_id and type are inserted in the database. According to line 6, digital signature is computed by concatenating hash_id and hash_secret on server side, where hash_secret is the hashed value of GS (hash value of GS is computed in order to make it a group digital signature). From line 7-8, the created digital signature is then sent from server side to client side and database is updated.

C. *Revoke Algorithm*

The revocation algorithm revokes the membership of the registered signer so that he becomes ineligible for signing documents in future. Client sends request for revocation and issuer revokes his membership in response, and when a member is revoked, it is necessary to inform the opener as well in order to make the verification and opening of the sign easier.

```
Algorithm: revoke ()
Input:  user_id
                    //name of user who wants to revoke
Secret Parameter: PS
Output: revocation performed
1.  if (user_id is matched) then
2.      delete record of user_id     //issuer's response
3.  endif
4. if (current date == expiry date)
  //automatically checked by server for temporary members
5.  delete record                    //issuer's response
6.  endif
```

Fig 4: Revoke Algorithm for DgbSS

Fig 4 shows the revoke algorithm for Dynamic Blind Group Digital Signature Scheme. According to line 1-2, if entered user_id is matched with the user_id in database, then from line 2, in response issuer will revoke that user's membership by deleting member's name, signature keys, type of membership and all other information of that member from database. Otherwise from line 4-5, for temporary members, server automatically checks if the current date matches any user's account's expiry date, then i

D. *Sign Algorithm*

Sign algorithm is used to insert the digital signature within the desired file. Signer will create a digital sign using his GS on message.

```
Algorithm: Sign()
Input: user_id, m                    // m is text file that is to be
signed
Secret Parameter: GS
Output: $m_{DS}$                     //signed file
1. if (user_id = true) then
// verified member
2. Text File with Digital Signature = append_signature (m)
//signature inserted in desired file
3.  endif
4.  exit
```

Fig 5: Sign Algorithm for DgbSS

Fig 5 shows the sign algorithm for Dynamic Blind Group Digital Signature Scheme. Let m be the message on which sign has to be produced. After creating the signature, signer encrypts his identity; he makes a cipher text C. then the signer again creates simple RSA traditional signature called group signature and the name of group with group signature key. Signer will send created signature on blinded message, cipher text and group signature back to person in question.

E. *Verify Algorithm*

Group signature will be verified by the RSA verification method using MD5 hash function.

```
Algorithm: verify ()
Input: $m_{DS}$
Secret Parameter: GP, PP
Output: verify                              //variable to
determine verification
1.  check_signature = get_signature ($m_{DS}$)
2.  Hash1 = compute hash (check_signature)
      // through hash algorithm   [ ] with GP
3.  Hash* = compute hash (check_signature)
// through hash algorithm   [ ] with PP
4.  if  (Hash* = Hash1) then
5.          signature has been verified
6.          return 1
7.  else
8.          signature has not been verified
9.          return 0
10.  endif
```

Fig 6: Verify Algorithm for DgbSS

Fig 6 shows the verify algorithm for DgbSS. According to algorithm verifier gets the public key of both the signer and message, and then from line 1 verifier gets the signature from the signed file. In line 2 he computes his own hash value (call this hash*) for the received message and in line 3 he decrypts the signed message with signer's public key decrypts then compares hash* to the hashed value of *check_signature*. Verification algorithm returns a bit. According to line 4 - 5, if bit is one, it means, signature of m is valid and returns bit 1.Otherwise from line 9, returns 0.

F. *Open Algorithm*

Open algorithm returns the name of the signer who signs the corresponding message.

```
Algorithm: Open()
Input: $m_{DS}$
Output: user_id
1.  check_signature = get_signature ($m_{DS}$)
2.  ID = compute hash (check_signature)
// through hash algorithm with GP
3.  if (ID = user_id) then
 // check hash in group database
4.      Name has been found
5.      return user_id
6.  else
7.      Name has not been found
8.      return 0
9.  endif
```

Fig 7: Open Algorithm for DgbSS

Fig 7 shows the open algorithm for Dynamic Blind Group Digital Signature Scheme. In line 1 opener takes signature, from the signed file and from line 2, opener decrypts the cipher text and gets the identity of the signer. From line 3, check the group database for the identity. According to line 3-4, if the specific entry is found, then returns the name of the signer; otherwise from line 8, returns 0.

V. Experimental Analysis

This scheme provides the security level with quite practical features: two authorities, PKI environment and Blind Signature. Proposed signature scheme, named DgbSS provides anonymity in two levels, by encrypting signature with group encryption key which provides anonymity of the signer and by blinding the message. Furthermore, it is more secure and reliable than all those schemes of group signatures in which there is only a single authority for both issuing and opening.

Here, public keys infrastructure has been used in order to achieve the anonymity and joining of group member, his authentication and group signature verification is there which makes this scheme as for dynamic groups. This technique is a combination of producing the blind signature with two separated authorities for join and open algorithm and such a public key infrastructure. This scheme holds following properties.

TABLE 2: Test Case for Joining

Test Case Name : *Join*			
ID	**Description**	**Expected Output**	**Actual Output**
1	Enter data in all fields	Register User	Register User
2	Data missing in any field	Missing field message	Missing field message
3	Data missing in all fields	Missing field message	Missing field message

TABLE 3: Test Case for Computing Hash

Test Case Name : *Compute Hash*			
ID	**Description**	**Expected Output**	**Actual Output**
1	Compute hash on NIC of user	Compute hash successfully	Compute hash successfully
2	Compute hash on group private key	Compute hash successfully	Compute hash successfully
3	Compute hash without NIC of user	Error raised	Error raised
	Compute hash without private key	Error raised	Error raised

TABLE 4: Test Case for Revoking

Test Case Name : *Revoke*			
ID	**Description**	**Expected Output**	**Actual Output**
1	Enter valid user name	Revoke User	Revoke User
2	Enter invalid user name	Invalid user message	Invalid user message
3	Data missing in any field	Missing field message	Missing field message

TABLE 5: Test Case for Login

Test Case Name : *Login*			
ID	**Description**	**Expected Output**	**Actual Output**
1	Enter valid User name	Login User	Login User
2	Enter invalid User name	Authorization message	Authorization message

TABLE 6: Test Case for Sign

Test Case Name : *Sign*			
ID	**Description**	**Expected Output**	**Actual Output**
1	Enter user name	User entered for signing	User entered for signing
2	Data missing in any field	Missing field message	Missing field message

TABLE 7: Test Case for Locating File

Test Case Name : *Locate File*			
ID	**Description**	**Expected Output**	**Actual Output**
1	Enter valid file name	Load file	Load file
2	Enter invalid file name	File not loaded	File not loaded
3	Data missing in any field	Missing field message	Missing field message

TABLE 8: Test Case for Verification

Test Case Name : *Verify*			
ID	**Description**	**Expected Output**	**Actual Output**
1	Enter valid file name	Verify file	Verify file
2	Enter invalid file name	File not verified	File not verified
3	Data missing in any field	Missing field message	Missing field message

TABLE 9: Test Case for Opening

Test Case Name : *Open*			
ID	**Description**	**Expected Output**	**Actual Output**
1	Enter valid file name	Open Signer's identity	Open Signer's identity
2	Enter invalid file name	Identity not opened	Identity not opened
3	Data missing in any field	Missing field message	Missing field message

TABLE 10: Test Case for Database Connectivity

Test Case Name : *Database Connectivity*			
ID	**Description**	**Expected Output**	**Actual Output**
1	Database does not exist	Exception raised	Exception raised
2	Incorrect database name	Error message	Error message
3	Correct database entry	Connection established	Connection established

After testing, the found results are analyzed and are given in the following table 11.

TABLE 11: EXPERIMENTAL RESULTS

Parameters	**Dynamic Blind Group Digital Signature Scheme**	**A. Lysyanskaya's and Z. Ramzan's Scheme**
Blindness	Yes	Yes
Two Authorities	Yes	No
Trust Level	Yes	No
Three key Requirement	Yes	Yes
Transferability	Yes	No
PKI	Yes	No
Divisibility	Yes	No
Member Revocation (on client request)	Yes	No
Member Revocation [on temporary basis (time)]	Yes	No
Non-Fraudulent	Yes	No

This scheme provides the anonymity of signature as well as the anonymity of the person who sends request to sign the message.

VI. CONCLUSION

Previously no group digital signature scheme used the blind signature protocol to achieve the anonymity of content of the message with two separate authorities for opening the signature at the time of dispute and for issuing. Membership to new members and than for implementing it in the E-Banking which is the emerging technology all over the world. This scheme results the decrease of high level of trust in one and only one authority for all the managing task of the group. In this scheme, neither the number nor the identities of group members are fixed at the setup phase. Our proposed technique not only reduces the uncomfortable high degree of trust but also reduces the work load of single entity of the group which is an achievement, with special reference to group blind signature schemes. This scheme also results in the efficient join-issue protocol without need of certificate from third party for checking the authenticity of issuer and client as well. Hence for E-Banking, we create the rules for its entities and other rules for E-transactions.

In the technique proposed, group signatures allow members of a group to sign messages anonymously on behalf of the group. These signatures are anonymous and non fraudulent, but a group authority is able to open them in case of dispute. In revocation algorithm a cheating member is revoked by the authority, so he can not sign in the future, but without scarifying the security of group signatures. Results shows that keys are secured none of group member and the group authority can threat any other.

REFERENCES

[1] R. RIVBST, "The MD5 message-digest algorithm," IETF Network Working Group, RFC 1321, April 1992.

[2] S. GOLDWASSER, S. MICALI AND R. RIVEST, "A digital signature scheme secure against adaptive chosenmessage attacks," *SIAM* Journal of Computing,17(2):281-308, April 1988.

[3] D. Chaum. "Blind signatures for untraceable payments". In *Advances in Cryptology { CRYPTO82*, pp. 199{203, Plenum, 1983.

[4] www. eprint.iacr.org

[5] www.di.ens.fr

[6] Bellare Shiy, Zhangz "Foundations of Group Signatures: The Case of Dynamic Groups" Topics in Cryptology CT-RSA '05,Lecture Notes in computer Science ,A.Menezes ed, Springer-Verlag,20.

[7] M.Bellare, D.Micciancio and B. Warinschi. "Foundation of group signatures: Formal definitions, Simplified requirements and a construction based on general assumptions". Advances in cryptology, EUROCRYPT 03, Lecture Notes in Computer Science vol. 2656, E.Biham ed.,Spriger-Verlag, 2003.

[8] J.Camensich and M.Michels," A group signature based on an RSA-variant." Technical Report RS-98-27, BRICS, University of Aarhus, November 1998.

[9] A-Lysyanskaya, Z. Ramzan, "Group Blind Signature: A Scalable Solution to Electronic cash". Financial Cryptography (FC'98), Lecture Notes in Computer Science, vol 1465,Springer-verlag.ppl184-197,1998.

[10] J.Camensich and M.Stadler "Efficient Group Signature schemes for large groups" In B.Kaliski, editor, Advances in cryptology-CRYPTO '97,volume 1296 of Lecture Notes in Computer Science, Pages 410-424. Springer Verlag 1997.

[11] www. cseclassic.ucsd.edu

[12] Zulfikar Amin Ramazan "Group Blind Digital Signature: theory and Application" at Massachusetts Institute of technology, May 1999.

[13] Vijay Gabale, Ashutosh, Dhekne, Sagar Bijwe and Nishant Burte"Blind Digital Signatures, Group Digital Signatures And Revocable Anonymity", Department of Computer Science and Engineering, IIT Bombay, 1999

M.Sikandar Hayat Khiyal, born at Khushab, Pakistan. He is Chairman Dept. Computer Sciences and Software Engineering in Fatima Jinnah Women University Pakistan. He Served in Pakistan Atomic Energy Commission for 25 years and involved in different research and development program of the PAEC. He developed software of underground flow and advanced fluid dynamic techniques. He was also involved at teaching in Computer Training Centre, PAEC and International Islamic University. His area of interest is Numerical Analysis of Algorithm, Theory of Automata and Theory of Computation. He has more than hundred research publications published in National and International Journals and Conference proceedings. He has supervised three PhD and more than one hundred and thirty research projects at graduate and postgraduate level. He is member of SIAM, ACM, Informing Science Institute, IACSIT. He is associate editor of IJCTE and Co editor of the journals JATIT and International Journal of Reviews in Computing. He is reviewer of the journals, IJCSIT, JIISIT, IJCEE and CEE of Elsevier.

Aihab Khan, works in Dept. of Computer Sciences Fatima Jinnah Women University Pakistan. His research interests are in the field of Data Mining, Data Warehousing as well as Information security.

Saba Bashir, is doing PhD in computer software Engineering from National University of Science and technology. Ms from National University of Science and technology. BS from Fatima Jinnah Women University, Rawalpindi. Pakistan. Currently doing job as Assistant Professor in Federal Urdu University of Arts, Science and Technology, Islamabad.

Farhan Hassan Khan, is doing PhD in Computer Software Engineering from National University of Science and Technology. Ms from National University of Science and Technology. BS from University of Engineering and Technology, Taxila. Currently serving as Project Manager in Software firm.

Saista Iman, is a graduate from Dept. of Software Engineering, Fatima Jinnah Women University, Pakistan.