ISSN:0975-9646

Privacy Protecting Group Signature Scheme Supporting Controllable Linkability

Anu Treesa George[#1,] **Prof.Kavitha N**[#2]

[#1] *M.Tech , Dept. CSE , Rajiv Gandhi Institute of Technology , Kerala , India* ,anutreesa10@gmail.com

[#2] *Associate Professor, Rajiv Gandhi Institute of Technology, Kerala, India* , kavitha@rit.ac.in

***Abstract*— Many real time applications like Sybil attack detection in a vehicular ad hoc network and privacy preserving data mining, there is a need to support linkability. while keeping the anonymity .For this group signature scheme are commonly used.Group Signature schemes , allows a group member to sign messages on behalf of the group, without revealing the identity of the signer using the signature. The controllable linkability of group signatures allows an entity with a linking key to find whether two group signatures were generated by the same signer or not , while preserving the anonymity. This paper introduces a new signature scheme that supports controllable linkability.This system allows a valid to generate signatures which hide his or her identity as normal group signatures, at the same time can be anonymously linked regardless of changes to the membership status of the signer and without revealing the history of the joining and revocation. By using this controllable linkability property of a group signature, anonymity may be flexibly or elaborately controlled according to a desired level**

***Keywords*—**controllable linkability, group signature, anonymity, privacy

I.INTRODUCTION

Because of the advancements in modern technologies, personal information is more and more publicly accessible and accordingly privacy is became an important security issue. Privacy is ,mainly characterized by two fundamental properties, anonymity and unlinkability [2]. Anonymity stand for concealing user's identity or identifiable information is in authentication messages. Unlinkability indicate that given two authentication messages, an unauthorized entity cannot tell whether they are generated by the same user or not. Intrinsically, identifiable information have higher priority than the linkable information with respect to exposure, because identifiable information can always be used as linkable information, but not the reverse. Generally speaking, while accessing a service, user always prefer to preserve their privacy, but the service provider is more relax to their privacy to gain sufficient user information. Various personalized services combined with data mining make crucial use of customer behaviors. That is, linkability is the key feature required in data mining. However, anonymity is necessary for privacy. It is possible to hide an identity or identifiable information from transactions while revealing still linkable information.

Extending digital signature schemes into groups, a new signature scheme i.e. group signature scheme is introduced, which gives permission for a group member to sign messages anonymously on behalf of the group. A client can verify the authenticity of the signature by using only the group's public key parameters. It must be computationally hard to identity of the group member so that he cannot be linked from a signed message or his signature. However, in the case of a legal dispute, the identity of a signer or member can be revealed by a designated entity i.e. the group manager. The major feature of group signature is the security of the information or the data that makes it more important as well as attractive for many real time applications, such as e-commerce, e-auction and e-voting, where the priority is privacy and anonymity of signer which is very much high and important for any organization.

For an application environment, privacy needs to be adjusted according to the desired policy or reasonable expectation of profit. If the requirements of privacy for both the users and service providers are properly balanced, privacy will be attractive for both of them. Linkability is the key feature required in data mining. However, anonymity is necessary for privacy. It is possible to hide an identity or identifiable information from transactions while revealing still linkable information. For example recommendation system such as the one at Amazon.com[3]. Customers might be happy to participate in the system only if their anonymity is kept and the linkability is given only to their service provider. Customers will feel assured if their buying pattern is revealed only to the service provider and their identities have not been revealed to anyone.

To provide both linkability and anonymity many privacy-protecting signature scheme are introduced. Conceptually, this signature schemes resides between pseudonym systems and normal GS schemes[4],which means that neither signers identity nor linking information is revealed explicitly from these signatures but, at the same time, these can be controlled by keys. That is, the corresponding signer identity and linkage information can be revealed by an opening key and a linking key,respectively[5].So, these signatures commonly known as PS-OL scheme. To be more descriptive, this **P**rivacy-protecting **S**ignature scheme with both **O**pening and **L**inking capabilities in a controllable manner is referred to as a PS-OL

scheme for short. The PS-OL schemes are introduced to supports two seemingly-incompatible properties, that is, privacy and data mining versatility by selectively providing linkability and anonymity. Here, a new method for PS-OL scheme is introduced. The proposed PS-OL scheme supports a dynamic group membership where a user can join or leave a group. Leaving a group is also considered as revoked. However, the linking capability can be consistently preserved regardless of changes to the membership status of the signer. In addition, the controllable linkability property does not expose the history of the joining and revocation. Above all , our scheme has a compact structure to yield a very short signature that is one group element shorter than the best-known GS [6] in the literature .So, the computation overhead of generating the signature can be effectively reduced.

II. RELATED WORKS

There are mainly two cryptographic solutions have been widely used to preserve privacy, a pseudonym system and group signatures (GS) [7]. Since the pseudonym system supports anonymity, it has the disadvantage that a signer cannot avoid being linked by anyone who obtains their signatures. A group signature (GS) scheme is considered as one of the most versatile primitives for anonymity. GS schemes provide controllable anonymity such that a signer can be identified from a signature by a trusted group manager. It also provides unlinkability on signatures against all users except the group manager. After the introduction of first GS in in 1991 [8], a number of GS schemes have been presented to address various features.

Chaum and Heyst proposed a new GS scheme which provides authority to any group member to sign messages anonymously on behalf of the group.In this work a client have given the permission to verify the authenticity of the signature by using only the group's public key parameters.

Novel conic-based group signature scheme with revocation proposed by Haiyong [9]introduced the first group signature scheme with group member revocation function from conic. Due to the properties of conic, the proposed scheme is of great efficiency .Before these method a number for other group signature schemes which support revocation were introduced. But that have some drawbacks of security flaws.. In this method , based on the practical and provably secure coalition resistant group signature construct an efficient and secure group signature scheme with revocation

Shivendu Mishra [10],proposed an ID based signature scheme from bilinear pairing based on k-plus problem. An ID-based cryptosystem enables the user to use public keys without exchanging public key certificates. In this work, they proposed an ID-based signature scheme from bilinear pairing based on k-plus problem. And this scheme was computationally more efficient than other existing schemes at that time and also unforgeable due to hardness of the k-plus problem.

Gene Yong[11] introduced a multi-signature scheme based on bilinear pairs. In this scheme a multi-signature scheme based on signers' identity is proposed by using CL - PKC technology. The scheme uses signers' identity information, such as E-mail address, IP address, phone number, etc as signers' public key, which reduces the overhead of establishment and management of public key infrastructure and avoids certificate storage and transmission of such issues. At the same time, the scheme eliminates PKG 's forgery signature defects that it is common in digital signature based on bilinear pairings.

Practical group signatures from hyper elliptic curves cryptography by Biao Liu [12] proposed a new and practical approach to group signature schemes. A trusted on-line third party is introduced in this scheme to help to make this scheme much more simple and practical than the previous schemes of this kind. This scheme also makes full use of the superiority of HCC, such as high efficiency, short key length and etc, and the scheme greatly improves the efficiency of hardware and software application.

Design of an efficient ID-based short designated verifier proxy signature scheme proposed by Hafizul Islam[13] introduced an efficient and secure ID-based short designated verifier signature (ID-SDVPS) scheme based on ECC. This scheme combines idea of Hu-Huang's scheme and suggestion from Park scheme. The proposed scheme captures the advantages of both the IBC and ECC. And this scheme is more secure and computation efficient than others. So, the proposed scheme is more practical and suitable for the environments with limited bandwidth, computing power and storage space.

Liqun Chen introduced a ring group signature scheme [14]. In many applications of group signatures, not only a signer's identity but also which group the signer belongs to sensitive information regarding signer privacy. This method combine a group signature with a ring signature to create a ring group signature, which specifies a set of possible groups without revealing which member of which group produced the signature.. The ring group signature solution will benefit any applications based on group signatures, in which group identities are sensitive.

A server-aided aggregate verification signature scheme from bilinear pairing introduced by Huai [15]design a secure and efficient sever aided verification signature scheme combined with aggregate verification for low-power devices, which is defined as Server-Aided Aggregate Verification Signature Scheme (SAAV).They define a security model of this scheme. Then, design a concrete server-aided aggregate verification signature scheme based BGLS signature scheme and prove that scheme is secure.

Lu Zhang et al proposed a robust certificate less short signature scheme[16]. Certificate less cryptography is introduced to eliminate certificate management in traditional public key cryptography and key escrow problem in identity-based cryptography. Here they propose a new certificateless short signature, of which the length is just 160 bits as short as BLS short signature scheme. And This scheme not only enjoys a high security level, but is also very efficient. There is no pairing operation in signing process and only two pairing operations in verification process. Moreover, when compared with all other CLS schemes with short signature sizes, the this scheme is the only one with provable security against key replacement attacks in which the attackers can obtain valid signatures under false public keys, and the scheme binds user's public key with private key, so attackers are unable to forge the public key without the knowledge of user's private key.

In Democratic GS scheme, the authority and responsibility are given to all group members equally, i.e, the group membership is controlled jointly and equally by all group members. So, here the owner of a particular message can be identified by every group member.

Hwang [1] introduced another short dynamic group signature scheme supporting controllable linkability, which provides a signature scheme which is the shortest ever known. This enables an entity who has a linking key to find whether or not two group signatures were generated by the same signer, while preserving the anonymity. This functionality is very useful in many applications that require the linkability but still need the anonymity, such as Sybil attack detection in a vehicular ad hoc network and privacy preserving data mining .In this method, they construct a PS-OL scheme for a dynamic membership, where group signatures can be anonymously linked, but the corresponding linkage information can only be revealed with a linking key .But the major disadvantage of this system is that this method is based on complex mathematical computations so the underlying structure is quiet complex.

III.Problem Statement

From the literature, it is clear that, pseudonym system and group signatures (GS) [7] are the most widely used cryptographic solutions to preserve privacy. Even though pseudonym system supports anonymity, it cannot be avoided that, anyone who obtain the signature can link the signer. Unlike pseudonym systems , a group signature (GS) scheme is considered as one of the most versatile primitives for anonymity. But in traditional GS (or referred to as a normal GS), special group manager act as the opener with the linking property . So, this increases the working overhead of the opener. Along with this, previous papers focuses on static membership , which means the number and identities of members is decided at set up phase and new members cannot join the group later[17].

So, from the literature, it concluded that there is a need to develop a signature scheme, which satisfies the basic requirements

- Group signature scheme must satisfy all basic security requirements like anonymity, traceability, and unlinkability.
- An unauthorized entity cannot able to sign the messages even though he previously signed keys.
- Group signature scheme should be unaffected by joining or leaving of any member.
- Group signature scheme which support controllable linkability with minimum computational overheads
- Group signature scheme based upon hard computational assumptions, like elliptic curve cryptography (ECC)

EC cryptography is a public-key mechanisms which provides the same facilities as that of other cryptography mechanisms like RSA or Elgamal. The main advantage of the EC systems is that, it provides better security with minimal key length than that of the rest.

IV.System design

For providing controllable linkability in group signature scheme PS-OL scheme is used over time. PS-OL scheme stands for Privacy-protecting Signature scheme with both Opening and Linking capabilities in a controllable manner.PS-OL scheme is mainly introduced for supporting two seemingly-incompatible properties, that is, privacy and data mining versatility by selectively providing linkability and anonymity. The main advantage of PS-OL over other group signature schemes is that a linker can be built up separately from an opener. This helps to remove the bottleneck (strong trusted relationship and on-line processing) present in an anonymous system. Since the PS-OL scheme supports controllable linkability, the underlying structure is quite complex because the system requires heavy operations and it is constructed from a linear combination encryption with many parameters. So signature length is also relatively long. To solve all these problems, in this paper, we construct a PS-OL scheme for a dynamic membership, with the property that the linkage information can only be revealed with a linking key. The linking key is secretly managed by a privileged party called a linker who is delegated the link capability by the opener. Note that the linking capability of this dynamic group signature introduced in this paper is differs from the tracing capability of a traceable signature scheme, because traceable signature scheme deals with tracing only a specific user's signatures. But in our scheme, using a linking key, the linker can deal with every user's linkage information. Early works of GSSs considered only a static setting [18], where the group is fixed at the time of the setup, whereas more recent constructions consider dynamic groups [19], i.e., new members may be added and possibly deleted to and from the group over time. Even though the proposed scheme supports a dynamic group membership where a user can join or leave a group, the linking capability can be consistently preserved regardless of changes to the membership status of the signer. In addition to this , he controllable linkability property does not expose the history of the joining and revocation. Above all ,our scheme has a compact structure to yield signature that is one group element shorter than the best-known GS.

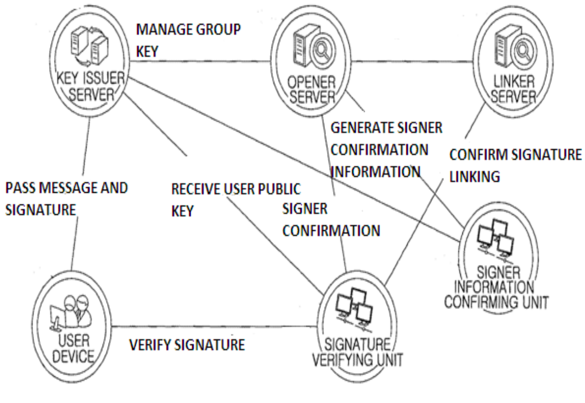

Fig. 1 Overall working of the system

V.IMPLEMENTATION

The PS-OL scheme has mainly three authorities:

- Issuer
- Opener and
- Linker

Each of them have their own independent privileges and authorities. An issuer is the module responsible for accepting the users, update user key and group key, message verification etc. Opener is responsible for opening the message to verify the validity of the messages. A linker can able to find the users identity using the signatures. For the updation of keys , the model explicitly considers a revocation algorithm .For the revocation, it makes use of a revocation list, denoted by **RL**. An entry of **RL** consists of an index and private information for a user who has been revoked and the entries are arranged to the latest revocation index. It is managed by the Issuer and initially set to be empty [20]. The list is used to update a user signature key and a group public key. In this model, whenever a particular user is became revoked, **RL** is immediately updated to include them . One can publicly access the list. The PS-OL scheme uses a registration list **REG** = *(*REG[1], . . . ,REG[*n*]*)*. REG[*i*] contains private information for the *i*-th registered user. The registered users are all different. **REG** is managed by Issuer and can be accessed by Opener to identify a signature.

- Setup phase: group manager computes the public group key and the secret key of individual users in this phase by implementing the algorithm for group key generation. The secret key is kept with him and the group public key is circulated among the members. The user signature key is of the form *gpk*0 = *(g, h*1, h_θ, g_1, g_2 , *u*, *w*, *d), where* g_1, g_2, *u*, *w*, *d* were updated per revocation. The user key is of the form **usk**[*i*] = *(*x_i, y_i , z_i , A_i) were, the value A_i is updated per revocation .The group join is also associated with this phase, where user can register a new group, for his various purposes. Group key is used for identifying a particular group among a list of groups and user key is mainly for user identification and revocation purposes.
- Sign phase: This is the signing phase in which an protocol is established between the group member and the issuer and a signature is generated. This signature is used to authenticate the user. The sign phase allows, the users to send the messages to the group using the group key and the user key.

  To make the transmission more secure , it is more better encrypt the messages before transmission . For this ,ECDSA algorithms used. It is a public key algorithm based on ECC.

  ECC is considered as the best encryption method with the minimum number of keys than the other public key encryption methods like RSA or DES.
- Verify phase: This phase implements a deterministic algorithm using given users public key and the signed message to verify the validity of the group signature. Signer sends the messages using the ECDSA algorithm to the verifier. And in the verification phase, the encrypted message is verified to make sure that no manipulations takes place during the transmission. The message is accepted if true value is returned by the verification phase else the message is rejected if false value is returned by the verification phase. For improving the performance the bulk message verification in introduced in the system. So this helps to reduce the processing time for verification.
- Open phase: This phase implements a deterministic algorithm to reveal the identity of the signer, by taking input a signed message and the secret key of group manager. The signature is taken as input by the group manager and using the private parameters of the opener , outputs the identity of the signer as return value. This open algorithm is implemented when an incident of a legal dispute arises.
- Link phase:This phase deals with the linkage information of every user with a linking key. Usin linking key, we can check whether two messages are generated from the same user or not, without revealing the user details or message details. In this way linkability can be proved.

VI.SECURITY NOTATION

- Anonymity: Using this proposed method, if a valid signature is given , it must be very difficult to discover the identity of the signer computationally only using that signature. This is because , the constant used for generating user key differs every time and the same user uses different signature for every new signed message. Only the group manager have the authority to determine the identity of the signing member using his secret key. For a non member, it is almost impossible to determine the secret parameters of the signing group member because without the secret key of the manager, it is almost impossible to determine the secret parameters of the signer. They agreed on a key exchange protocol and hence an outsider cannot able to discover the identity of the signer. In this property we conclude that if neither group manager's secret key nor group member's secret key is exposed then it is infeasible to reveal the signer of a authorized valid signature.
- Unforgeability: The property concluded that only a valid authorized group member can produce a valid signature i.e. a valid member only can produce a signature on behalf of his group because the keys used for generating the signature issued only by the group manager.
- Unlinkability: This property states that it is impossible for an outsider to decide whether two valid signatures were generated by the same group member or not . According to this property it is practically impossible to conclude that both signatures are from the same member or not if anybody provided with two signatures.

VII.RESULTS

The processing speed comparison of the system is carried out based on single verification and bulk verification. And from the analysis is it is clear that ,by including bulk verification the processing speed can be improved

TABLE I
EXPERIMENTAL RESULT II (single verification)

user	Message	Single verification
U1	M1	921.32 ms
U1	M2	895.20 ms
U2	M1	933.30 ms
U2	M2	892.45 ms

TABLE II
EXPERIMENTAL RESULT II (bulk verification)

user	Message	Bulk verification
U1	M1+M2	1.23
U2	M1+M2	1.29

VIII.CONCLUSION

In this work, a dynamic PS-OL scheme is constructed with minimum short signature length. The constructed scheme achieves anonymity, traceability, non-frameability, and also other security requirements for controllable linkability. Also this scheme outperforms the best-known anonymous signature schemes. This scheme will be very versatile and can be effectively used in many privacy-preserving applications with limited resources.

REFERENCES

[1] Jung Yeon Hwang, Liqun Chen, Hyun Sook Cho, and DaeHun Nyang, “short dynamic group signature scheme supporting controllable linkability”, ieee transactions on information forensics and security, vol. 10, no. 6, june 2015

[2] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, “A practical and provably secure coalition-resistant group signature scheme,” in Advancesin Cryptology (Lecture Notes in Computer Science), vol. 1880. Berlin, Germany: Springer-Verlag, 2000, pp. 255–270.

[3] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 3152. Berlin, Germany: Springer Verlag, 2004, pp. 41–55

[4] J.-M. Bohli and A. Pashalidis, “Relations among privacy notions,” ACM Trans. Inf. Syst.Security, vol. 14, no. 1, 2011, Art. ID 4.

[5] D. Boneh and X. Boyen, “Short signatures without random oracles and the SDH assumption in bilinear groups,” J. Cryptol., vol. 21, no. 2, pp. 149–177, 2008.

[6] C. Delerablée and D. Pointcheval, “Dynamic Fully Anonymous Short Signature Scheme,” J vol. 4341. Berlin, Germany, Springer-Verlag, pp. 193–210, 2006

[7] M. Bellare, H. Shi, and C. Zang, “Foundations of group sigatures: The case of dynamic groups,” in Topics in Cryptology (Lecture Notes in Computer Science), vol. 3376. Berlin, Germany: Springer- Verlag, 2004, pp. 136–153

[8] D. Chaum and E. van Heyst, “Group Signatures,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 547. Berlin, Germany: Springer-Verlag, 1991, pp. 257–26

[9] HaiyongBao, HaiyongBao, and Zhenfu Cao, “Novel conic-based group signature scheme withrevocation”, 2011 Eighth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)

[10] Shivendu Mishra, Rajeev AnandSahu, SahadeoPadhyeand Rama Shankar Yadav ,”An ID-Based Signature Scheme From Bilinear Pairing Based on k-plus problem”, 978-1-4244-8679-3/11/$26.00 ©2011 IEEE

[11] GENG Yong-jun and ZHANG Jun-feng , “A New Multi-Signature Scheme Basedon Bilinear Pairs” , 978-1-4244-8694-6/11/$26.00 ©2011 IEEE

[12] Biao Liu, Jian-HuaGe, Jian He and Fei Jiang ,” Practical Group Signatures from Hyper-ellipticCurves Cryptography”, 978-1-4244-8039-5/11/$26.00 ©2011 IEEE

[13] SK Hafizul Islam , G. P. Biswas, “Design of an Efficient ID-based Short DesignatedVerifier Proxy Signature Scheme” , 1st Int’l Conf. on Recent Advances in Information Technology RAIT-2012

[14] Liqun Chen and HP Labs ,” Ring Group Signatures “,2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications

[15] Huai WU and Chunxiang XU “ ,A Server-aided Aggregate Verification Signature Scheme from Bilinear Pairing” , 2013 5th International Conference on Intelligent Networking and Collaborative Systems

[16] Lu Zhang , Jingwei Liu , Huichao Wu and Rong Sun , “An Efficient And Robust Certificateless Short Signature Scheme”,

[17] P. Bichsel, J. Camenisch, T. Groß, and V. Shoup, “Anonymous credentials on a standard java card,” in Proc. ACM CCS, 2009, pp. 600–610.

[18] E. Brickell, L. Chen, and J. Li, “Simplified security notions of direct anonymous attestation and a concrete scheme from pairings,” Int. J. Inf.Security, vol. 8, no. 5, pp. 315–330, 2009.

[19] P. Bichsel, J. Camenisch, G. Neven, B. Warinschi, and N. P. Smart, “Get short via group signatures without encryption,” in Security andCryptography for Networks. Berlin, Germany: Springer-Verlag, 2010, pp. 381–398

[20] X. Boyen and B. Waters, “Compact group signatures without random oracles,” in Advances in Cryptology, vol. 4004. Berlin, Germany: Springer-Verlag, 2006, pp. 427–444.