International Journal on Cybernetics & Informatics (IJCI) Vol. 5, No. 2, April 2016

DYNAMIC PRIVACY PROTECTING SHORT GROUP SIGNATURE SCHEME

Ashy Eldhose[1] and Thushara Sukumar[2]

[1] Student, Department of Computer Science and Engineering, MBITS Nellimattom
[2]Assistant Professor, Department of Computer Science and Engineering, MBITS Nellimattom

ABSTRACT

Group Signature, extension of digital signature, allows members of a group to sign messages on behalf of the group, such that the resulting signature does not reveal the identity of the signer. The controllable linkability of group signatures 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. This paper presents a new signature scheme supporting controllable linkability.The major advantage of this scheme is that the signature length is very short, even shorter than this in the best-known group signature scheme without supporting the linkability. A valid signer is able to create signatures that hide his or her identity as normal group signatures but can be anonymously linked regardless of changes to the membership status of the signer and without exposure of the history of the joining and revocation. From signatures, only linkage information can be disclosed, with a special linking key. Using this controllable linkability and the controllable anonymity of a group signature, anonymity may be flexibly or elaborately controlled according to a desired level.

KEYWORDS

Anonymity, Privacy, Group Signature, Opening, Linkability

1. INTRODUCTION

Personal information is more and more publicly accessible due to modern technologies and accordingly privacy is increasingly becoming an important security property. Privacy is characterized by two fundamental notions, anonymity and unlink ability [1]. Anonymity means that a user's identity or identifiable information is concealed in authentication messages. Unlink ability means that given two authentication messages, an unauthorized entity cannot tell whether they are generated by the same user or not..Generally speaking, for accessing a service, users prefer to preserve their privacy, but the service provider may want to relax their privacy to gain sufficient user information.

Extending the idea of digital signature schemes into groups, a new signature scheme i.e. group signature scheme, provides authority to any 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-

DOI: 10.5121/ijci.2016.5216

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.

A privacy-protecting signature scheme was recently introduced to provide elaborate privacy controls. Conceptually, it resides between pseudonym systems and normal GS schemes[11]. Neither information identifying a signer nor information linking signatures is revealed explicitly from signatures. However, the anonymity and unlinkability 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[2]. Using a trapdoor-based approach on these two privacy notions, one can establish a two-level access hierarchy on signer privacy. 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. A PS-OL scheme supports two seemingly-incompatible properties, that is, privacy and data mining versatility by selectively providing linkability and anonymity.

2. RELATED WORKS

As we know of digital signature and facilities it has provided regarding information security, so extending the idea of digital signature to group where we can parallely authorize multiple information or documents and save time. Group Signatures have vital role in day to day corporate organizations' ecommerce applications. Extending the idea of digital signature schemes into groups, a new signature scheme i.e. group signature scheme, first introduced by Chaum and Heyst in 1991, provides authority to any group member to sign messages anonymously on behalf of the group [19]. 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. GS schemes provide controllable anonymity such that a signer can be identified from a signature by a trusted group manager. It provides unlinkability on signatures against all users except the group manager. A number of GS schemes have been presented to address various features [7].

Direct Anonymous Attestation (DAA) has been proposed for the remote anonymous authentication of a trusted platform module. While DAA guarantees complete anonymity, i.e., no party can reveal a signer's identity from a signature, it provides signer-controllable linkability, i.e., a signer can generate an anonymous signature with a tag, which is linkable to another signature from the same signer. There are variants of a GS scheme to alleviate the centralized group manager's rights that can reveal a signer's identity[4].

In the Democratic GS scheme, the group membership is controlled jointly and equally by all group members. A signer of a signature can be identified by a member, in other words, the

signer's anonymity can be provided only against non members. In the tracing-by-linking GS scheme, no signer can be identified by any authority if he or she signs only once per event.

Some schemes with controllable or revocable anonymity provide linkability by adding a tag to a signature [9]. Using the tag associated with a signature, one can check the linkability on signatures easily and explicitly. For example, a linkable democratic GS scheme is a variant of a democratic GS scheme to support the tag-based linkability. A message-linkable GS scheme was suggested to resist Sybil attacks in VANET[10].

The message-linkable property means that given two anonymous signatures on the same message, one can easily decide whether they are generated by the same signer or not. To provide this property, the scheme uses a static tag generated with a message and a secret key[11].

3. PROBLEM DEFINITION

The secret signing key of a group member includes a key-pair for a standard digital signature scheme that is certified by the group manager. The group member's signature is an encryption, under a public encryption key held by the group manager, of a standard signature of the message together with certificate and identity information, and accompanied by a non-interactive zero-knowledge proof that encryption contains what it should. Previous works did not try to achieve security notions as strong as this paper target, nor to pin down what properties of the building blocks suffice to actually prove security. It is well-known in the literature that two cryptographic solutions have been widely used to preserve privacy, a pseudonym system and group signatures (GS) [12]. The pseudonym system supports anonymity, but 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. However, following the concept of a traditional GS (or referred to as a normal GS), the linkability is given only to an opener, who is not usually a service provider but a special group manager. The definitions and results of previous paper are for the setting in which the group is static, meaning the number and identities of members is decided at the time the group is set up and new members cannot be added later[5]. An also proper definition for security has not been provided even for the basic static-group case.

The objective of this paper is to implement a group signature scheme based on following assumptions:

- Group signature scheme based upon hard computational assumptions, such as, elliptic curve cryptography (ECC) and a honest verifier ZKPK Protocol.
- Group signature scheme should be unaffected by joining or leaving of any member.
- Group signature scheme must satisfy all basic security requirements like anonymity, traceability, and unlinkability.

EC cryptography schemes are public-key mechanisms which are able to give the same facilities as the schemes of RSA or Elgamal. But the security of ECC is based on a hardness of another problem, known as the elliptic curve discrete logarithm problem (ECDLP). The best algorithms to solve ECDLP have full exponential-time (unlike RSA's algorithms which have the sub exponential-time)[17]. Thus, required security level can by achieved with significantly smaller keys in elliptic curve system than in its rival- RSA system. Zero-knowledge is defined by means of a distinguisher Dwhich essentially tries to distinguish between proofs produced by a prover (with respect to a real common random string), or a simulator (with respect to a simulated common random string)[8].

4. PRIVACY PROTECTING SIGNATURE SCHEME WITH BOTH OPENING AND LINKING CAPABILITY

Privacy-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. A PS-OL scheme supports two seemingly-incompatible properties, that is, privacy and data mining versatility by selectively providing linkability and anonymity. A PS-OL scheme has benefits in flexibly organizing participants over a normal GS, considering that a linker can be built up separately from an opener. This separation enables a bottleneck (strong trusted relationship and on-line processing) to be removed in an anonymous system. A PS-OL scheme is constructed from a linear combination encryption with many parameters. Since the underlying structure is quite complex, the system requires heavy operations, and its signature length is also relatively long. In this paper, we 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. 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 capability of linking signatures is placed below the capability of opening the signer identity of the signatures. We can achieve a stepwise access control on anonymity by adding this Controllable Linkability (CL) to the controllable anonymity that can identify a signer from signatures using an opening key. The linking capability of this dynamic group signature differs from the tracing capability of a traceable signature scheme. The traceable signature scheme enables a tracer to trace only a specific user's signatures, not other users. In contrast, a linker of our scheme can deal with every user's linkage information with a key. Though a traceable signature scheme can be used for our linkability, it involves complex computation. For example, for n signatures and m tracing keys, $n \times m$ computation is required for a traceable signature scheme while n computation is required for this scheme.

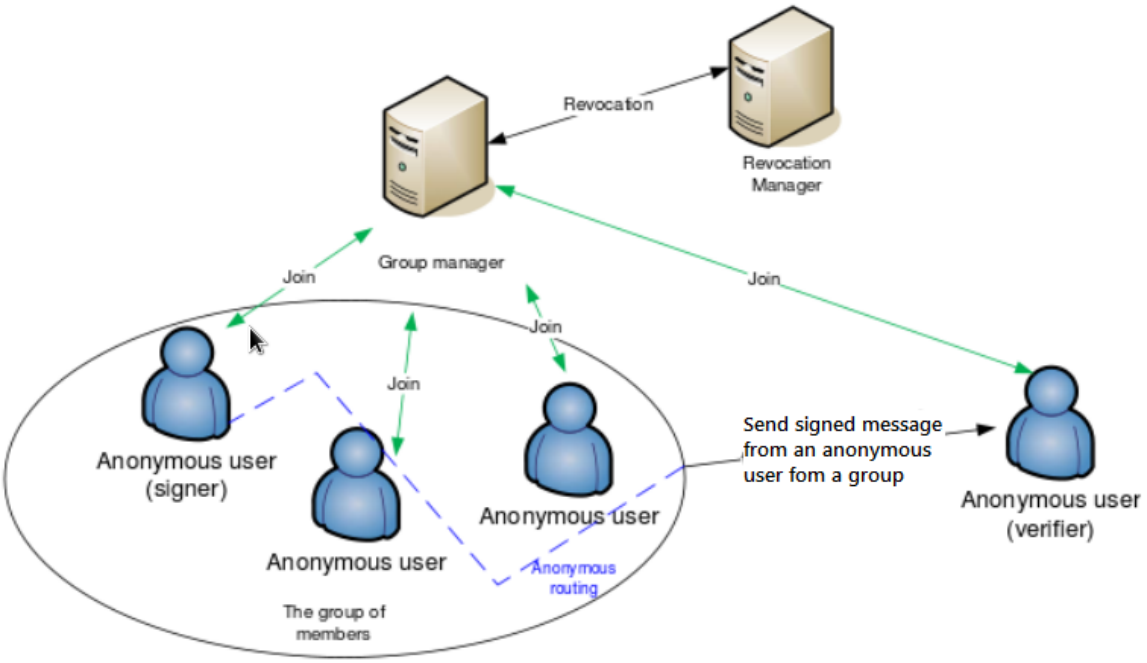

Figure 1 Principles of Group Signature Scheme

The proposed PS-OL scheme supports a dynamic group membership where a user can join or leave a group. Leaving a group is also referred as to be revoked. However, the linking capability can be consistently preserved regardless of changes to the membership status of the signer. In addition, the CL property does not expose the history of the joining and revocation. Despite the

additional functionality of CL, our scheme has a compact structure to yield a very short signature that is one group element shorter than the best-known GS.Early works of GSSs considered only a static setting [6], where the group is fixed at the time of the setup, whereas more recent constructions consider dynamic groups [7], i.e., new members may be added and possibly deleted to and from the group over time. Moreover, in some cases it is also desirable to have distributed authorities, i.e., one party only receives the opening key and a distinct party receives the issuing key required to add new members or to revoke existing members.

4.1 Model

This section presents a security model for a PS-OL scheme. This model assumes three authorities

- Issuer
- Opener and
- Linker

who have their independent privileges and a certain level of trust. A linker is assumed to behave honestly but curiously, and so it can try to find passively user's identity only with signatures collected.

This model explicitly considers a revocation algorithm that performs the update of keys. 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. It is managed by the Issuer and initially set to be empty [14]. The list is used to update a user signature key and a group public key. In this model, whenever the information of keys to be revoked are given according to a pre-defined policy, **RL** is immediately updated to include them and entries are arranged to the latest revocation index. One can publicly access the list. A user signature key includes a non-negative integer λ, called a revocation index, to indicate that the key has been updated up to the λ^{th} entry of **RL**. Let $\lambda\hat{} > \lambda$ be the most up-to-date number of revoked keys in **RL**. For generation of a signature, the user signature key is updated up to the $\lambda\hat{}^{th}$ entry of **RL**. The generated signature includes $\lambda\hat{}$ to indicate that the signature was generated by the key which has been updated up to the $\lambda\hat{}^{th}$ entry of **RL**. It can be verified with the group public key that has been updated up to the $\lambda\hat{}^{th}$ entry of **RL**.

The PS-OL scheme uses a registration list **REG** = *(*REG[1], . . . ,REG[*n*]*)*. REG[*i*] contains private informationforthe *i*-th registered user. The registered usersareall different. **REG** is managed by Issuer and can be accessedby Opener to identify a signer.
A PS-OL scheme consists of the following algorithms.

- Setup phase: group manager computes the public key and the secret key in this phase by implementing the algorithm for group key generation. He inputs a security parameter to the algorithm and it returns the group public key and also the secret key of group manager. The secret key is kept with him and the group public key is circulated among the members.

- Issue phase: an interactive protocol is established in this phase between the group manager and the to-be-member after which the user becomes a valid group member. A secret key is chosen by the Group member using which another parameter is generated by the member. This generated parameter is sent to the group manager. Then using his own secret key the group manager generates the group member's signing key and returns it to newly joined group member.

- Sign phase: This is the signing phase in which an protocol is established between the group member and the verifier where he has to verify a group signature whether it is generated by a valid group member or not. Group member uses the signing key pairs to sign the message. The generated group member signature of knowledge is sent by the member to the verifier for verification.

- Verify phase: This phase implements a deterministic algorithm using given group public key and the signed message to verify the validity of the group signature. Signer sends his signature to the verifier, i.e. the signature generated by the signature of knowledge. 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.

- 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 outputs the identity of the signer as return value. This open algorithm is implemented when a incident of a legal dispute arises.

- Judge phase: This phase implements a judge algorithm to check the user produced the signature on the message using the secret key.

- Link phase:This phase deals with the linkage information of every user with a key. The linkage information can only be revealed with a linking key [17].

4.2 Security Notions

- Anonymity: Given a sign which is valid must be difficult for anyone to discover the identity of the signer computationally. As the constant differs every time, the same member generates different signature for every new message to be signed. The group manager only can determine the identity of the signing member using his secret key. For a nonmember it is almost not possible to discover the secret parameters of the signing group member as the knowledge of the secret key of the group manager is required and so without the secret key of the group manager it is almost impossible to determine the secret parameters of the signer and hence an outsider cannot cannot determined 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: Only a valid authorized member belonging to the group can produce a valid signature i.e. a valid member only can produce a signature on behalf of his group.

- Unlinkability: This property states that deciding if two valid signatures were generated by the same group member is difficult. According to this property one cannot conclude that both signatures are from the same member or not if he's provided with two signatures.

- Traceability: Using only open algorithm and the group manager's secret key, the group manager can track the identity of the signing member if given any valid signature. Like in case of any legal dispute or emergencies, any signer's identity can be traced by the group manager only. It is not possible for an outsider to track the signer because open algorithm, which used to trace a signing group member, requires the knowledge of the secret key of the group manager.

- Exculpability: The group members even along with the group manager are not able to sign a document on behalf of any other group member. The knowledge of the secret parameters of the group member is required to generate a valid signature. And every member has his own unique secret key that are used to generate the signature. Even a group manager cannot sign on behalf of any group member because the group manager does not have the members' secret keys[18].

5. CONCLUSION

A dynamic PS-OL scheme is constructed which yields a short signature. The constructed scheme achieves anonymity, traceability, non-frameability, and also three security requirements for (controllable) linkability. Also this scheme outperforms the best-known anonymous signature schemes. This scheme will be very versatile and useful in many privacy-enhancing applications with limited resources.

REFERENCES

[1] 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.

[2] 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.

[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] E.Brickell, J. Camenisch, and L. Chen, "Direct anonymous attestation," in Proc. ACM CCS, 2004,pp.132–145.

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

[6] 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.

[7] 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.

[8] X. Boyen and C. Delerablee, "Expressive subgroup signatures," in Security and Cryptography for Networks (Lecture Notes in Computer Science), vol. 5229. Berlin, Germany: Springer-Verlag, 2008, pp. 185–200.

[9] E. Brickell and J. Li, "A pairing-based DAA scheme further reducing TPM resources," in Proc. 3rd TRUST, 2010, pp. 181–195.

[10] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 2656. Berlin, Germany: Springer-Verlag, 2003, pp. 614–629.

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

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

[13] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in Proc. ACM CCS, 2004, pp. 168–177.

[14] 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.

[15] X. Boyen and B. Waters, "Full-domain subgroup hiding and constant size group signatures," in Public Key Cryptography, vol. 4450. Berlin, Germany: Springer-Verlag, 2007, pp. 1–15.

[16] J. Camenisch and T. Groß, "Efficient attributes for anonymous credentials," in Proc. ACM CCS, 2004, pp. 345–356.
[17] J. Camenisch, S. Hohenberger, and A. Lysyanskaya, "Compact E-cash," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 3494. Berlin, Germany: Springer-Verlag, 2005, pp. 302–321.
[18] J. Camenisch and A. Lysyanskaya, "Dynamic accumulators and application to efficient revocation of anonymous credentials," in Advancesin Cryptology (Lecture Notes in Computer Science), vol. 2442. Berlin, Germany: Springer-Verlag, 2002, pp. 61–76.

Authors

Ashy Eldhose is currently pursuing M.Tech in Cyber Security in MBITS, Nellimattom. She completed her B.Tech from MBITS, Nellimattom, Kerala, India. Her areas of research are Network Security and Information Forensics.

ThusharaSukumar is currently working as the Assistant Professor in Department of Computer Science and Engineering at MBITS, Nellimattom, Kerala, India. She received her B-Tech Degree in Computer Science and Engineering from College of Engineering, Kidangoor and ME in Computer Science and Engineering from PSNACET, Dindigul. Her research interest include Image Mining.