Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 6, June 2016, pg.274 – 278

A Survey of Digital and Group Signature

Falgun Shah[1], Hitul Patel[2]
[1]M.E in C.E, Swaminarayan College of Engineering &Technology (S.C.E.T., Kalol), India
[2]Asst. Prof. in Swaminarayan College of Engineering & Technology (S.C.E.T., Kalol), India
falgunshah1990@gmail.com; hitulce@gmail.com

ABSTRACT--- An extension to Digital signature is a Group Signature scheme which allows the members of the group to sign messages containing information on behalf of the group, having the feature of hiding the identity of the signer. A single group public key is used to verify the Signatures. In case of any dispute, only a designated group manager, holding their special property, is able to open signatures, and thus reveal the signer's identity. Its applications are used widespread, especially in e-commerce such as e-cash, e-voting and e-auction. This paper incorporate the detailed study of group signature definition, concept and the main contributions in this field such as applications of group signature that tells where we can use this technique. It starts with overview, concept, properties, keys used, application, challenges, and attack of group signature and a comparative analysis of some group signature techniques.

I. INTRODUCTION

A digital signature is a mathematical scheme for providing the authenticity of a digital information or document.
A valid digital signature provides a proper reason to the recipient to believe that the information was provided by a known sender, so the sender cannot deny having seen the message, moreover it also checks that the message was not altered in transit.
Digital signatures are computed based on the documents (message/ information) that need to be signed and it is done on some private information held only by the sender. In practice, instead of using the whole message, a hash function is applied to the message to obtain the message digest. A hash function, in this context, takes an arbitrary-sized message as input and produces a fixed-size message digest as output. Among the commonly used hash functions in practice are MD-5 (message digest 5) and SHA (secure hash algorithm).
Digital signatures are basically applied for software distribution, financial transactions, and in cases of disputes where detect forgery or tampering of digital information are very important.

II. INTRODUCTION TO DIGITAL SIGNATURE TECHNOLOGY

Authentication of messages or we say information, protects the party involved in the communication or the process of information exchange from some exterior interference or say the third party. However, it does not protect the two parties against each other. Several forms of dispute between the two are possible. In situations where there is not complete trust between sender and receiver, something more than authentication is needed. The most attractive solution to this problem is the digital signature. It combines a hash with a digital signature algorithm. The digital signature is analogous to the handwritten signature.
A digital signature is said to be valid if it satisfy the following properties.

- It must verify the author and the date and time of the signature.
- It must to authenticate the contents at the time of the signature.
- It must be verifiable by third parties, to resolve disputes

Thus a digital signature must be a bit pattern that depends on the message being signed. It must also have some information that should be unique to the sender to prevent both forgery and denial. It must be easy to produce, recognize and verify a digital signature. It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message. Lastly it must be practical to retain a copy of the digital signature in storage.

A digital signature is a piece of data which is attached to a message and which can be used to find out if the message was tampered with during the conversation. The digital signature for a message is generated in two steps:
1. A *message digest* is generated. A message digest is a 'summary' of the message we are going to transmit, and has two important properties: (a) it is always smaller than the message itself and (b) Even the slightest change in the message produces a different digest. The message digest is generated using a set of hashing algorithms.
2. The message digest is encrypted using the sender's *private* key. The resulting encrypted message digest is the *digital signature*.
The digital signature is attached to the message, and sent to the receiver. The receiver then does the following:
1. Using the sender's public key decrypts the digital signature to obtain the message digest generated by the sender.
2. Uses the same message digest algorithm used by the sender to generate a message digest of the received message.
3. Compares both message digests (the one sent by the sender as a digital signature, and the one generated by the receiver).
If they are not *exactly the same*, the message has been tampered with by a third party. We can be sure that the digital signature was sent by the sender (and not by a malicious user) because *only* the sender's public key can decrypt the digital signature (which was encrypted by the sender's private key; remember that what one key encrypts, the other one decrypts, and vice versa). If decrypting using the public key renders a faulty message digest, this means that either the message or the message digest are not exactly what the sender sent.

The following are the techniques based on Digital signature.
Group Signature: The concept of group signatures allows a group member to sign messages anonymously on behalf of the group. However, in the case of a dispute, the identity of a signature's originator can be revealed by a designated entity.
Ring Signature: A similar system that excludes the requirement of a group manager and provides true anonymity for signers.
Threshold Signature: A threshold signature involves a fixed-size quorum (threshold) of signers. Each signer must be a genuine group member with a share of a group secret signing key. A (t,n) threshold signature scheme supports n potential signers, any t of which can on behalf of the group. Threshold signatures reveal nothing about the t signers; no one can trace the identity of the signers (not even a trusted center who have set up the system).
Multi signature: A multi signature represents a certain number of signers signing a given message. Number of signers is not fixed and signers' identities are evident from a given multi-signature. A multisignature is much shorter (sometimes constant) than the simple collection of individual signatures.
Proxy Signature: A proxy signature allows a delegator to give partial signing rights to other parties called proxy signers. Proxy signatures do not offer Anonymity.
Blind Signature: A signer can sign messages for users. The signer does not know the message he is signing. The signer should not be able to recognize the message nor the signature he has produced. The user is anonymous w.r.t all other users. Blind Signature implemented based on Schnorr Signature. It is lot faster than group signature.

III. DETAIL INTRODUCTION TO GROUP SIGNATURE

A technique of signing the documents or any relevant information anonymously on behalf of group is known as Group Signature scheme, where group consist of manager and various designated members. The designated verifier verifies the integrity of sign, and where the verifier is aware of the correctness of the sign not the identity of member who signed the documents.

There are three participants in this scheme which are as follows:

Group Manager: The manager of group for managing the memberships and generating the membership keys of group members (Signers). Group Manager enabling signers to sign on behalf of the group, and revealing the identity of the signature's originator when dispute.

Group Member: The group member, he/she have his/her membership key, and he/she can using the membership key to sign message on behalf of the group.

Verifier: Receiver of group signature or anyone can check the validity of the group signature by the public key of group.

A group signature scheme consists of the following four procedures:

Setup: a probabilistic interactive protocol between a designated group manager and the members of the group. Its result consists of the group's public key Y, the individual secret keys x of the group members, and a secret administration key for the group manager.

Sign: a probabilistic algorithm which, on input a message m and a group member's secret key x, returns a signature s on m.

Verify: an algorithm which, on input a message m, a signature s, and the group's public key Y, returns whether the signature is correct.

Open: on input a signature s and the group manager's secret administration key this algorithm returns the identity of the group member who issued the signature s together with a proof of this fact.

It is assumed that all communications between the group members and the group manager are secure.

For a group Signature to be valid needs to satisfy the following properties:

- Only group members are able to correctly sign messages **(unforgeability)**.
- It is neither possible to find out which group member signed a message **(anonymity)** nor to decide whether two signatures have been issued by the same group member **(unlinkability)**.
- Group members can neither circumvent the opening of a signature nor sign on behalf of other group members; even the group manager cannot do so **(security against framing attacks)**.

A consequence of the last property is that the group manager must not know the secret keys of the group members.

There are three types of key are used in this scheme as:

- **Master Public Key:** anyone who knows this key can verify that some group member has signed the message..
- **Master Secret Key:** given to all group members for signing of messages.
- **Administrative Key:** only known to manager to identify that which group member has signed the message.

IV. APPLICATIONS AND ATTACKS

Applications:

The following are the applications of Group Signature.

Electronic Voting Mechanism

E-voting also known as electronic voting collectively means to cast vote and count the votes electronically.

E-voting is physically supervised by representatives of governmental or independent electoral authorities where group signature would be beneficial. Voting is also performed within the voter's sole influence, and is not physically supervised by representatives of governmental authorities where the authorization plays a vital role as trusted party is needed to govern the voting scheme, in such case group signature can be best applicable.

Electronic Sales and Bidding System
Electronic commerce, commonly known as e-commerce, is a type of industry where buying and selling of product or service is conducted over electronic systems such as the Internet and other computer networks. It consists of the exchange of data to facilitate the financing and payment aspects of business transactions. Group signature is effective and efficient way of providing security in communicating within an organization.

Corporate Organization:
Any organization well developed consist of many roles working for the particular objective to be achieved which comprises of vital information to be shared between them, thus group signature proves to be efficient way to authorize the information among everyone and saving the valuable time with a reliable approach.

Attacks
There are various attacks imposed on different group signature schemes which will be described here as follows:
Meet-in-the-middle attack: This type of attack can be used for forging signatures on mixed-type digital signatures schemes, and takes less time than an exhaustive attack. This has been analyzed that an optimal strategy for forgers to apply this attack, pointing out that
an intermediate value of 64 bit length is not secure for any mixed-type digital signatures scheme.
Forgery attack: Shi's group signature scheme is not secure; Fangguo Zhang and Kwangjo Kim propose a universal forgery attack of this group signature scheme against the known-message attack [18].
Unforgeability attack: This is another attack which should be possible on group signature scheme. It has been proved that the scheme is universally unforgeable; namely, anyone can forge a valid group signature on another message by a valid signature. Unforgeability is the basic property of group signature. This property is a primitive condition of group signature which be used in electronic commerce.
Unlinkability attack: Unlinkability is an important property of group signature which is distinguished from other signature types. Unlinkability means that, given two group signatures, it is hard to distinguish whether the two group signatures were produced by the same signer.
Conspiracy attack: Conspiracy attack against group signature, put forward by Taiwan scholar Li C.M, means that malicious members can recover the secret polynomials to obtain group private key under their conspiring in order to impersonate others signature irresponsibility. Many scholars have done a lot of works to resist conspiracy attack, but the conspiracy attack has always been difficult to solve in group signature system.

V. CONCLUSION

Here in this paper we have represented an overview of Digital Signature. This further includes their use in the practical world. Apart from this a detail study on Group Signature is included, along with their applications and the attacks that can occur. In this paper we tried to give the complete information about the group signature which will help the new researchers to get the maximum knowledge in this domain.

References

[1] J. J. . Chen and Y. Liu. A traceable group signature scheme. Mathematical and Computer Modelling, 31(2-3):147–160, 2000.
[2] T. Isshiki, K. Mori, K. Sako, I. Teranishi, and S. Yonezawa. Using group signatures for identity management and its implementation. In Proceedings of the Second ACM Workshop on Digital Identity Management, DIM 2006. Co-located with the 13th ACM Conference on Computer and Communications Security, CCS'06, pages 73–78, 2006.
[3] Y. Geng, G. Shao, M. Zheng, and G. Cui. An improved efficient group signature scheme for large groups. HuazhongKejiDaxueXuebao (ZiranKexue Ban)/Journal of Huazhong Uni- versity of Science and Technology (Natural Science Edition), 37(7):66–69, 2009.
[4] L. Chen and T. P. Pedersen. New group signature schemes. In A. De Santis, editor, Advances in Cryptology- EUROCRYPT'94, pages 171–181. Springer, Berlin,, 1994.
[5] Mihir Bellare and Sara K. Miner. A forward-secure digital signature scheme. pages 431–448. Springer-Verlag, 1999.
[6] W.B. Lee and C.C. Chang. Efficient group signature scheme based on the discrete logarithm. volume 145, pages 15–18. IEE, 1998.

[7] Dan Boneh and Hovav Shacham. Group signatures with verifier-local revocation. In ACM Conference on Computer and Communications Security, pages 168–177, 2004.
[8] Fengyin Li, Jiguo Yu, and Hongwei Ju. A new threshold group signature scheme based on discrete logarithm problem. In Proceedings of the Eighth ACIS International Confer- ence on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing - Volume 03, SNPD '07, pages 1176–1182, Washington, DC, USA, 2007. IEEE Computer Society.
[9] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of group signatures: formal definitions, simplified requirements, and a construction based on general assump- tions. In Proceedings of the 22nd international conference on Theory and applications of cryptographic techniques, EUROCRYPT'03, pages 614–629. Springer-Verlag, 2003.
[10] Steven D. Galbraith and Mark Holmes. A non-uniform birthday problem with applications to discrete logarithms. Discrete Applied Mathematics, 160(10-11):1547–1560, 2012.
[11] Jeffrey Hoffstein, Jill Pipher, and J.H. Silverman. An Introduction to Mathematical Cryp- tography. Springer Publishing Company, Incorporated, 1 edition, 2008.
[12] Henk C. A. van Tilborg and Sushil Jajodia, editors. Encyclopedia of Cryptography and Security, 2nd Ed. Springer, 2011.
[13] Behrouz A. Forouzan. Cryptography & Network Security. McGraw-Hill, Inc., 1 edition,2008.
[14] G. Tsudik and G. Ateniese, "Quasi-efficient revocation of group signatures", in To Appear in Financial Cryptography, 2002.
[15] M. Harkavy, H. Kikuch and J.D. Tygar, "Electronic auction with private commerce", in Proceedings of the 3rd USENLX Workshop on Electronic Commerce, August 1998.
[16] L. Harn and Y.Xu, "Design of generalized ElGamal type digital signature schemes based on discrete logarithm", Electronics Letters, 1994.
[17] W.H. He, "Digital signature scheme based on factoring and discrete logarithms", Electronics Letters, 2001.
[18] Fangguo Zhang and Kwangjo Kim, "Security of A New Group Signature Scheme", IEEE TENCON'02

