A survey of Identity Based Multireceiver Signcryption scheme

Shweta Khullar, Vivek Richhariya, Vineet Richhariya

Abstract— These Identity based signcryption is the technique of signcrypting the message on the basis of identity of the receiver. Although the signature-then-encryption increases the computational cost, hence signature-then-encryption is performed in a single logical step. Here we are implementing the concept of signcryption using the identity of multi receiver so that the security of these receivers and the message authentication is maintained. Identity based encryption is the technique of encrypting the message using the concept of generating a flag string of the receiver and on the basis of identity of the receiver the sender is authenticated. In this paper we use an efficient implementation of the combination of the identity based multireceiver and then signcryption scheme using elliptic curve cryptography.

Index Terms— Signcryption, Digital Signatures, multireceiver, random oracle, broadcast, unforgeability, confidentiability.

1 INTRODUCTION

The term Signcryption is referred as a technique of encrypting the data with the use of signatures in area of public key cryptography. This technique concurrently fulfils both the functional advantages of digital signature and public key encryption in a single step. In this way computational cost is significantly lower than that required by the traditional 'signature and encryption' technique.

Let consider a general condition when a sender wants to send a confidential letter in such way that it cannot be counterfeit. For this it has been a common practice for the sender of the letter to first sign or authenticates the message and put it in an envelope and then seals it before handing it over to be delivered. If sender wants to communicate with unknown or first time met receiver then it should discover Public key cryptography. Public key cryptography has made communication between people who have never met before over an open and the network which is insecure. There are many ways to send and authenticate the message. Before sending a message, some common activities performed by sender are:

- Prepare a message and sign or authenticate it.
- Encrypt the message with signature using private key cryptography or algorithm by choosing key.
- Again encrypt the message with receiver public key.
- Now send the message to receiver.

Today the concept of securing the message and the authenticity of the sender's private data is important to achieve. Although there are many techniques implemented for the security of sender's private data. A new way of securing the data is using the process of signing the data and then encrypts it, but the technique increases the computational costs and communication overhead [1]. So to reduce these computational cost and communication overhead the next step is to combine the signature-then-encryption within a single logical step which was first performed by Yuliang Zheng in 1997 [2].

A signcryption technique is a combination of digital signature which is used for authentication and public key cryptography which is used for securing the message. Digital signature is a brand of authentication. It is widely used to judge or authenticate the valid source of data or identifying the original nodes that generate the message. While public key cryptography is message security mechanism that helps to provide confidentiality and secure delivery of message. Both are work independently, first message was digitally signed (or authenticated by sender) and then encrypted before sending. This is traditionally known as sign then encryption. But later on they are combined together and can be named as signcryption.

A signcryption scheme typically consists of three algorithms: Key Generation (Gen), Signcryption (SC), and Unsigncryption (USC). Key Generation (Gen) generates a couple of keys for user, signcryption (SC) is normally a probabilistic algorithm, and Unsigncryption (USC) is almost certainly to be deterministic. Any signcryption scheme should have correctness, Efficiency and Security as main properties [3].

Bellare et al. [4] has proposed a multireceiver signcryption scheme in which there are n receivers where each of the receivers contains a pair (ski, pki) i.e private and public key pair. The pki can be used by the sender to encrypt a message Mi to obtain a ciphertext Ci for i=1,2….n and then sends (C1,C2……Cn) as ciphertext. The receiver i then extracts Ci and decrypt the ciphertext using ski.

1. RELATED WORK

Although there are many signcryption scheme has implemented for the security of data from sender to receiver, but here a way of securing the data is by using multireceiver identity based signcryption.

Jianhong Zhang, Zhipeng Chen and Min Xu proposed a new signcryption scheme based on ID-based Multireceiver Threshold Signcryption scheme [1]. The scheme given here is based on random oracle model where the prevention from various types of attacks is made possible using ID-based multireceiver signcryption. The technique used here best prevents from unforgeability and confidentiability.

The signcryption scheme given here provides public verifiability and prevents from attacks in the network [5]. The scheme also provides third party authentication where the technique implemented here is based on random oracle model and removes the disadvantages of work done in [6] and [7].

An efficient and certificate less Signcryption Scheme has been proposed in [8]. The technique provides comparison from various techniques and provides best signcryption scheme for CLSC scheme.

An efficient identity-based broadcast signcryption scheme has been proposed which is based on short ciphertext size and public ciphertext authenticity of the data [9]. The security issues and different attacks are on the basis of random oracle model and it has reduced computational cost and time.

An identity-based anonymous signcryption scheme for multiple receivers has been proposed which implements the concept of novel cryptographic primitive [10]. The scheme used here is used for the standard model and provides prevention from various security attacks such as unforgeability and mutual authentication. The technique also gives security proof regarding Deffie-Hellman problem.

The identity based multireceiver scheme is also implemented for the MANET where the main security and privacy concern is on the prevention from various attacks [11]. The ID-based multireceiver signcyption scheme when implemented for the multireceiver in an Ad-hoc Network can be used in a wide variety of applications.

A secure signcryption scheme for random oracle model is proposed based on the concept of aggregation [12]. The scheme used here provides various security issues and prevention from various attacks. The technique used here for the aggregation is by taking the aggregate of n number of receivers by taking n users.

Signcryption is a technique of using signature and encryption within a single logical step. Here the proposed work is based without random oracle model [13]. The scheme provides non-repudiation with respect to plaintext. The scheme also provides and verify using third party authentication.

A probably-secure improved scheme to correct the vulnerable and also give the unforgeability & confidentiality of improved scheme under the existing security assumption. Multireceiver Identity Based Signcryption [14]. The scheme provides an efficient way of signcryption the message having an extra authentication and prevention from various security attacks.

A revocable ID-based signcryption scheme is proposed which provides an authentication and prevention from attacks [15]. The scheme proposed here provides prevention from various possible threat and attacks. The scheme implemented here proves security issues regarding BDH and CDH schemes.

3. MULTI-RECEIVER IDENTITY BASED SIGNCRYPTION TECHNIQUE

Syntax: In the context of multi-receiver identity based signcryption, either a single message or multiple messages can be signcrypted. In this context, it is assumed that a single message is signcrypted to multiple receivers [16].

Definition: A generic multi-receiver identity based signcryption (MIBSC) scheme consists of the following algorithms.

Setup: Given a security parameter, the private key generator (PKG) generates a master key *mkPKG* and a common parameter *cpPKG*. *cpPKG* is given to all interested parties while *mkPKG* is kept secret.

Extract (private key extraction): Providing an identity ID received from a user and its master key *mkPKG* as input, the PKG runs this algorithm to generate a private key associated with ID, denoted by *SID*.

Signcrypt: To send a message *m* to multiple receivers whose identities are *ID*1, ..., *IDn* respectively, the sender runs this algorithm to generates a signcrypted ciphertext *C* = *Signcrypt*(*M,SIDS, ID*1*, ..., IDn*).

De-signcrypt: Upon receiving a ciphertext *C*, the receiver *IDi* computes *Desigcrypt* (*C, SIDi, IDS*) and obtains $m \in M \cup \{\perp\}$, where $\perp$ indicates that the message was not encrypted or signed properly.

In this approach, a multi-receiver signcrypted ciphertext is a combination of two parts. The first part is same to all the receivers and the second part can be viewed as an *n*-tuple where the *i*-th component is specific to receiver *IDi*. When decrypting a ciphertext, receiver *IDi* extracts the first part and the i-th component from the second part and then runs the De-signcryption algorithm. [16] Refer to the former as receiver information part and the latter as text part. They adopt this approach because it simplifies the security model and allows for a clear explanation of the security notions.

4. CONCLUSION

In this paper the survey of the signcryption techniques is presented along with the technique of using identity based multireceiver signcryption technique. Although there are many technique already implemented for the signcrypting the data using id-based multireceiver but there might be the chances of different types of attacks in the network. So in the future when implementing using id-based multireceiver then to reduce the number of attacks in the network we use elliptic curve cryptography an asymmetric approach for the security of the data.

REFERENCES

[1] Jianhong Zhang, Zhipeng Chen, Min Xu "On the Security of ID-based Multi-receiver Threshold Signcryption Scheme", In proceedings of 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), pp. 1944 – 1948, 2012.

[2] Y.Zheng. "Digital signcryption or how to achieve cost (signature & encryption) cost (signature)+cost (encryption)", Crypto'97, LNCS 1294, pp. 165-179, Springer-Verlag, 1997.

[3] M. Toorani, "Cryptanalysis of an Elliptic Curve-based Signcryption Scheme", International Journal of Network Security, Vol.10, No.1, pp.51–56, Jan. 2010.

[4] M. Bellare, A. Boldyreva and S. Micali: Public key encryption in a multi-user setting: Security proofs and improvements, EUROCRYPT" 2000, LNCS # 1807, pp. 259-274, Springler-Verlag, 2000.

[5] S. Sharmila Deva Selvi, S. Sree Vivek, C. Pandu Rangan, "Identity Based Public Verifiable Signcryption Scheme", Proceedings of the 4th international conference on Provable security (ProvSec'10), Lecture Notes in Computer Science Volume 6402, pp 244-260, 2010.

[6] Feng Bao and Robert H. Deng. "A signcryption scheme with signature directly verifiable by public key". In Public Key Cryptography, volume 1431 of Lecture Notes in Computer Science, pages 55–59. Springer, 1998.

[7] Raylin Tso, Takeshi Okamoto, and Eiji Okamoto. Ecdsa-verifiable signcryption scheme with signature verification on the signcrypted message. In Information Security and Cryptology(Inscrypt 07), volume 4990 of Lecture Notes in Computer Science, pages 11–24. Springer, 2008.

[8] Gang Yu, Hongzhi Yang, Shuqin Fan, YongShen, Wenbao Han, "Efficient Certificate less Signcryption Scheme", Proceedings of the Third International Symposium on Electronic Commerce and Security Workshops(ISECS '10), pp. 55-59, 2010.

[9] Hien D.T., Tien T.N., Thu Hien T.T, "An efficient identity-based broadcast signcryption scheme", Proceedings of the 2010 Second International Conference on Knowledge and Systems Engineering (KSE '10), pp. 209-216, 2010.

[10] Bo Zhang, Qiuliang Xu, "An ID-based Anonymous Signcryption Scheme for Multiple Receivers", Proceedings of the 2010 international conference on Advances in computer science and information technology, pp. 15-27, 2010.

[11] Lei Wu, "An id-based multi-receiver signcryption scheme in MANET", Journal of Theoretical and Applied Information Technology, Vol. 46 No.1, pp. 120-124, dec-2012.

[12] Jayaprakash Kar, "Provably Secure Identity-Based Aggregate Signcryption Scheme in Random Oracles", Cryptology ePrint Archive: Report 2013/037, Jan 2013. Available at: http://eprint.iacr.org/2013/037.pdf

[13] Prashant Kushwah and Sunder Lal, "Provable secure identity based signcryption schemes without random oracles", International Journal of Network Security & Its Applications (IJNSA), ISSN: 0974 – 9330, Vol.4, No.3, pp. 97-110, May 2012.

[14] Wei Yuan, Liang Hu*, Hongtu Li, Jianfeng Chu, Yuyu Sun* "Cryptanalysis and Improvement of Selvi et al.'s Identity-Based Threshold Signcryption Scheme", Journal of Networks, *ISSN 1796-2056,* Vol 6, No 11, pp. 1557-1564, Nov 2011.

[15] Tsu-Yang Wu, Tung-Tso Tsai and Yuh-Min Tseng "A Revocable ID-based Signcryption Scheme", Journal of Information Hiding and Multimedia Signal Processing, ISSN 2073-4212, Volume 3, Number 3, pp. 240-251, July 2012.

[16] Shanshan Duan and Zhenfu Cao "Efficient and provably secure multi-receiver identity-based signcryption", In Proceedings of the 11th Australasian conference on Information Security and Privacy (ACISP-06), pp. 195–206, 2006.