International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-2, Issue-11, November 2014

Identity based Signcryption and security attacks and prevention- A Survey

Abhishek Tripathi, Dr. Kavita Burse

***Abstract*— Secret and secure delivery of message is most important concern in field of security hence signcryption were used. The term signcryption is a new paradigm in public key cryptography that simultaneously fulfils both the functions of digital signature and public key encryption in a logically single step, and with a cost significantly lower than that required by the traditional "signature and encryption" approach. Identity based signcryption is used to encrypt the message using receiver identity. In this paper we are presenting some signcryption based methods.**

***Index Terms*— Authentication, signcryption, Security, ID-based signcryption.**

I. INTRODUCTION

Signcryption is a useful cryptographic primitive that achieves confidentiality and authentication in an efficient manner. As far as message security is concern along with authentication of sender's identity for communication over non secured channel is essentially required. In Internet scenario it is most important for keeping message private and unforgeable. In this respect the sender can use a digital signature algorithm with his private key to sign the message followed by encrypts the message and its signature by a symmetric encryption algorithm with secret key. The message encrypted by senders secrete key with the combination of receivers public key. This is a sign-then-encrypt scheme used to authentication and encryption. This method leads larger computational const and communication overhead [1].

Signcryption is referred as a technique of encrypting the data with the use of signatures in area of public key cryptography. Let consider a general condition when a sender needs to send a confidential letter in such way that it cannot be forged. In old days a sender generally writes a letter put authentication as signature then put it on envelop and finally seal it before tender to recipients. If sender wants to commune 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 conduct to send and authenticate the message. To attain it prepare a message first then authenticate it with sign. After authentication encrypt the message with private key cryptography or another cryptographic algorithm. Again encrypt the message with receiver's public key and lastly send the message to receiver.
[2].

Manuscript received November 14, 2014.
Abhishek Tripathi, Oriental College of Technology, Bhopal, India
Dr. Kavita Burse, Oriental College of Technology, Bhopal, India

Multi-receiver signcryption used to swiftly present authenticity and confidentiality to numerous receivers through single signcryption operation. This procedure makes it perform well in efficiency. Only the allied receivers can un-signcrypt cipher text to obtain the equivalent message using its own private key. No one can get anything from the cipher text [3]. Threshold cryptography is generally used to reduce key leakage problem by including a secret share system. And threshold decryption is used to decentralize the control of decryption right by secret share decrypting key.

Digital signatures rely on certain types of encryption to ensure authentication. Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode. Authentication is the process of verifying that information is coming from a trusted source. These two processes work hand in hand for digital signatures. It is an electronic authentication identity used for validate the user. Such types of validation or authentication are essential for secure message delivery over Internet or unsecure channels. Digital signatures are certified by Certificate Authorities (CAs) which are used in communication over electronic super highway. For securing digital signature various schemes were proposed like ID-based signature, ID Based scheme with key-insulation mechanism, ID-based signcryption etc. Most of these schemes are based on hash function to map ID- based information via elliptic curve cryptography [4].

Identity based cryptography (IBC) is the user's public key based cryptography. It has two parts first is user entity and second is private key generator (PKG). Private Key Generator provides secure communication among sender and recipient and digital signature is used to authenticate legitimate sender. The PKG initializes and generates parameters and master key before starting service process which processes parameter requests and private key requests. With respect to sender, he gets system parameters first before initializing them. IBE based signature is generated and sent to receiver. Then he will start monitoring process. He has provisions for receiving encrypted files and also signature information [4].

The Multi-receiver based signcryption scheme uses conception of multiple receiver against single sender. The key problem with several receivers is correct authentication and security of message. In this scheme multiple pairing of sender's private key and receiver's public key were essential at sender end. The message was encrypted using receiver's public key after digital signature provided by sender for authentication. Then message is transfer or delivered to respective receiver. If it is receive by unauthorized recipient. Then it is not able to decrypt message without private key of actual sender. For decrypting message private key of actual receiver is essential. This was secure message until private

key of that receiver is safe or not leak. [5]

In year 2002, Bellare et al. [6] has offered a multi-receiver based signcryption scheme. In this scheme, there are n receivers where each of the receivers contains a pair (ski, pki) i.e pair of private and public key of receiver. 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 private key .

A multi-receiver signcryption is a technique of transferring the message to the recipient through the identity of the receiver. The signcryption using ID based multi-receiver provides security from a variety of attacks such as unforgeability, identity disclosure attack and various attacks. The rest of paper is organized as follows. In Section II describes about background information of signcryption. Section III describes related work in fields of multi-receiver based signcryption followed by a conclusion in Section IV.

II. BACKGROUND

In modern cryptography two main concerns are Data confidentiality and data integrity. Where Confidentiality can be obtain via encryption algorithms or cipher texts, while integrity can be achieved by the use of authentication techniques. There are various Encryption algorithms fall into one of two broad groups: private key encryption and public key encryption. Likewise, authentication techniques can be categorized by private key authentication algorithms and public key digital signatures. Private Key encryption and public key digital signature performs fast computation with less message expansion. Both are required bulky computation like exponential equations based large integers or composite integer with larger finite fields. Presently the consequence of signcryption in real-world applications has gained recognition by experts in data security.

III. RELATED WORK

In this section we presenting review about signcryption based techniques.

In year 2012, Zhang et al [1] offered on the security of ID-based multi-receiver threshold signcryption scheme. They try to analyze the concept of multi-receiver threshold signcryption scheme proposed in Qin et al [7]. They showed that the signcryption scheme was insecure via random oracle model. This scheme fails to provide confidentiality and unforgeability. They also analyze attack behaviour of offered method in [7]. On behalf of their study they offer corresponding attack that was capable to solve above mention problems.

The signcryption scheme with multiple receivers has been offered by Kullare et al [2] using elliptic curve cryptography. They are able to include confidentiality and authenticity in their offered methods. During the process of signcryption; the data confidentiality is maintained among user and receiver so that the chances of attack have been reduced. Signature verifiability with non-repudiation also achieved in this method. Signature Verifiability is a way of signcryption where the sender needs to encrypt message with his signatures and then at the receiver need to verify these signatures. During the transmission of data from user to the receiver third party can't access the data even with the help of his private key. Attackers are unable to read the data even having private key of user. 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 [2].

In year 2013, a multi-message and multi-receiver ID based method for signcryption was proposed by Jing et al [3]. In this method sender can signcrypt multiple numbers of messages simultaneously for numbers of receivers. The receivers can decrypt message using their own private key. This method holds authenticity along with confidentiality. This scheme holds former multi-receiver signcryption can only deal with one message. They are trying to develop an efficient and provable cryptographic technique that can capable to gain confidentiality and authenticity in multi-receiver circumstance. A new multi-message and multi-receiver ID-based signcryption scheme (MM-IDSC) can simultaneously signcrypt multiple messages for multiple receivers. Computation and communication overhead of this scheme is quite less and it more secure against Bilinear Diffie-Hellman (BDH) problem. As compared to current multi-receiver ID-based signcryption scheme offered MM-IDSC is much more efficient in computational costs and communication overheads also. In this scheme, signcryption operation requires n pairing pre-computations and one multiplication, and unsigncryption operation requires only one pairing pre-computation and two multiplications. Especially, pre-computation can be computed ahead to be stored in memory, and the results can be invoked by a user when needed [3]

A review on Multi Level Identity Based Cryptography using digital signature authentication was presented in [4]. Many ID based signature schemes are best used to improve security with authentication, confidentiality, integrity and non-repudiation. According to their survey there are many identity based schemes with various features were offered by various researchers. However, there lacks research in the literature that focuses on multi-level identity based cryptography. The usage of digital signatures has become ubiquitous and the new emerging technologies like data mining, and cloud computing. Identity based cryptography can secure digital signature authentication but somehow lacking of ensuring integrity, confidentiality and non-repudiation [4].

Multi-receiver identity based signcryption scheme for single pairing computation for multiple receivers was proposed in [5]. To signcrypt the message single pair of computation is used while message was delivered to various receivers. This scheme also supports confidentiality and authenticity simultaneously in the multi-receiver setting. They also try to compare their scheme with existing multi-receiver based schemes according to efficiency and security. They also observed that this scheme performs better among them. They try to send message to multiple nodes while sender is same and efficiency of this method is not compromised. To design a

multi-receiver identity-based signcryption (MIBSC) scheme with a high-level of computational efficiency with authenticity and confidentiality simultaneously. They offered efficient multi-receiver IBSC scheme able to signcrypt multiple messages with one key pairing computation for numerous recipients. Selective multi-identity attack model was also specified in [5]. This model adversary commits ahead of time to multiple identities. It intends to attack and formalize two security notions for MIBSC schemes. They also presented MIBSC constructions and compare their scheme with existing on the basis of security and efficiency [5]. Lei Wu proposed Multi-Receiver ID-Based Signcryption Scheme in Mobile Ad-hoc Network. To avoid high computational costs and communication overheads multi-receiver signcryption was proposed. It also supports confidentiality and authenticity for multiple receivers in a single logical step. It is also capable to gain higher efficiency than signcrypting a message for each receiver. According toresult obtained this scheme is probable efficient with low computation cost and secure under random oracle model [8].

Lal and kuswaha presented a multi receiver identity based anonymous signcryption scheme. This scheme is enriched with message confidentiality along with unforgeability and anonymity with public authenticity [9]. Laura Savu presented schnorr digital signature based signcryption. A Schnorr signature is a digital signature produced by the Schnorr signature algorithm. Its security is based on the intractability of certain discrete logarithm problems. There are two definitions for security of signcryption depending on whether the adversary is an “outsider” or “insider”. The security goal is to provide both authenticity and privacy of communicated data. In the symmetric key scenario, the sender and the receiver share the same secret key, the only security model that makes sense is one in which the adversary is modeled as a third party or an outsider who does not know the shared secret key [10].

SIGNCRYPTION SCHEME	CONFIDENTIALITY	INTEGRITY	UNFORGEABILITY	NON-REPUDIATION	TIME TAKEN
R.J. HWANG ET AL.	NO	NO	NO	Directly	More
H.Y. JUNG ET AL.	YES	YES	YES	Additional Protocol	More
C. GAMAGE ET AL.	YES	YES	YES	Directly	More
F. BAO & R. H. DENG	YES	YES	YES	Directly	More
Y. ZHENG AND H. IMAI	YES	YES	YES	Additional Protocol	More
Y. ZHENG	YES	YES	YES	Additional Protocol	More

IV. CONCLUSION

Here in this paper various signcryption techniques are discussed and present their various advantages and disadvantage. These signcryption techniques prevent data from various attacks. Hence by analyzing these signcryption techniques and their various performance parameters a new and efficient technique for signcryption can be implemented in the future.

REFERENCES

[1] Zhang, Jianhong, Zhipeng Chen, and Min Xu. "On the security of ID-based multi-receiver threshold signcryption scheme." In 2012 2nd International IEEE Conference on Consumer Electronics, Communications and Networks (CECNet), pp. 1944-1948, 2012.

[2] Khullar, Shweta, Vivek Richhariya, and Vineet Richhariya. "An Efficient identity based Multi-receiver Signcryption Scheme using ECC." International Journal of Advancements in Research & Technology, ISSN 2278-7763, vol. 2, issue 4, pp. 189 – 193, 2013.

[3] Jing, Q. I. U., B. A. I. Jun, S. O. N. G. Xin-chuan, and H. O. U. Su-mei. "Secure and efficient multi-message and multi-receiver ID-based signcryption for rekeying in ad hoc networks,” Journal of Chongqing University, ISSN 1671-8224, vol.12, no. 2, pp. 91 -96, 2013.

[4] Sumalatha, P., and B. Sathyanarayana. "A Review On Multi Level Identity Based Cryptography For Secure Digital Signature Authentication", International Journal of Computer Engineering and Applications, Vol. 5, Issue 1, Jan-2014.

[5] Duan, Shanshan, and Zhenfu Cao. "Efficient and provably secure multi-receiver identity-based signcryption." In Information Security and Privacy, pp. 195-206, Springer Berlin Heidelberg, 2006.

[6] Bellare, Mihir, Alexandra Boldyreva, and Silvio Micali. "Public-key encryption in a multi-user setting: Security proofs and improvements." In *Advances in Cryptology—EUROCRYPT 2000*, pp. 259-274, Springer Berlin Heidelberg, 2000.

[7] Qin, Huawang, Yuewei Dai, and Zhiquan Wang. "Identity-based multi-receiver threshold signcryption scheme" Security and Communication Networks, vol. 4, no. 11, pp. 1331-1337, 2011.

[8] Wu, Lei. "An ID-Based Multi-Receiver Signcryption Scheme In MANET." Journal of Theoretical & Applied Information Technology, vol. 46, no. 1, 2012.

Lal, Sunder, and Prashant Kushwah. "Anonymous ID Based Signcryption Scheme for Multiple Receivers." IACR Cryptology ePrint Archive 2009, artile no 345, 2009