Cryptanalysis of Signcryption Protocols Based On Elliptic Curve

Sumanjit Das[1], Prasant Kumar Sahoo[2]
1(Department of Computer Science and Engineering, Centurion University of Technology & Management, India)
2 (Department of Computer Science and Engineering, Subas Institute of Technology, India)

ABSTRACT: *The security of data become a major issue in the present days, there are different dimensions of security in this paper we will discuss one of the major properties of security. The signcryption is one of the techniques to secure your data by encrypting it. It was first introduced by Zheng in 1997 based on DLP. The signcryption combines the techniques of digital signature and encryption which reduces computational cost and communication overhead. The Signcryption scheme verifies the integrity of message before decryption of cipher text it also provides how the message can be verify by third party without reading the content of message. Many researchers have given their signcryption scheme to achieve security goals like confidentiality, unforgeability, integrity, forward secrecy and public verification every scheme is having their own limitations. This paper represents the cryptanalysis of popular signcryption scheme in terms of major security goals alpng with the communication overhead and computational cost.*

Keywords*: ecc, forward secrecy, public verification, signcryption.*

I. INTRODUCTION

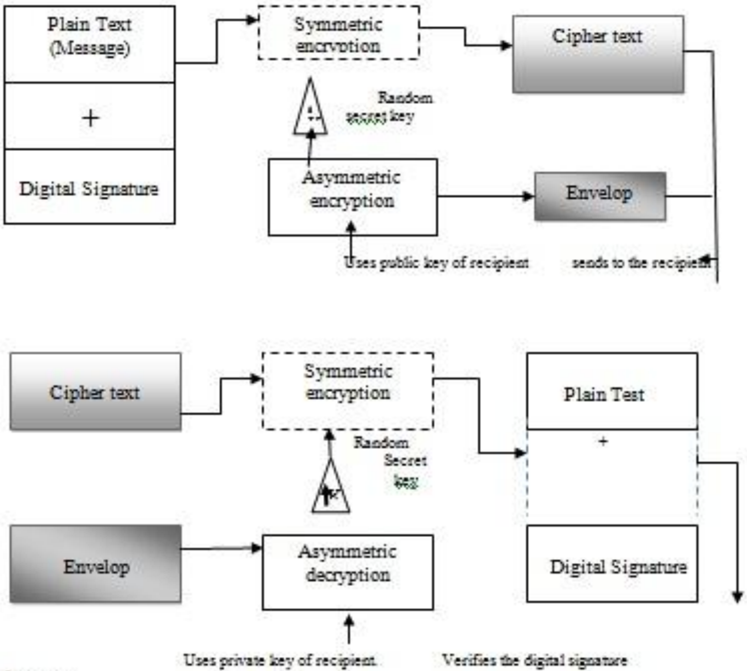
The encryption of data and digital signature are two primary cryptographic tools that can guarantee the unforgeability, integrity, and confidentiality of communications. In public key schemes, a traditional method is to digitally sign a message then followed by an encryption algorithm (signature-then-encryption) that can have two problems: Low efficiency and high cost of such summation, and the case that any arbitrary scheme cannot guarantee the security. The signcryption is a relatively new cryptographic technique that is supposed to fulfill the functionalities of digital signature and encryption in a single logical step and can effectively decrease the computational costs and communication overheads in comparison with the traditional signature-then-encryption schemes [1, 2, and 7].

At the time of sending a message to a person over an anxious channel such as internet we must provide confidentiality, integrity, authenticity and non-repudiation [1]. These are the four major security aspects [2] or goals. Before the modern era, cryptography was concerned solely with message confidentiality (i.e., encryption) conversion of messages from a comprehensible form into an incomprehensible one and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge (namely the key needed for decryption of that message). Encryption was used to (attempt to) ensure secrecy in communications, such as those of spies, military leaders, and diplomats. In recent decades, the field has expanded beyond confidentiality concerns to include techniques for message integrity checking, sender/receiver identity authentication, digital signatures, and interactive proofs and secure computation, among others. In ancient times, the use of cryptography was restricted to a small community essentially forms by the military and secret services. The keys were distributed secretly by a courier and the same key is used to encipher and decipher the message. We have a number of encryption algorithms those can be broadly classified into two categories: Symmetric/Private key encipherment and Asymmetric/Public key encipherment [3, 4].

In order to send a confidential letter in a way that it can't be forged, it has been a common practice for the sender of the letter to be sign it, put it in an envelope and then seal it before handing it over to be delivered. Discovering public key cryptography has made communication between people who have never met before over an open and insecure network such as Internet [10], in a secure and authenticated way possible. Before sending a message the sender has to do the following:

1. Sign it using a digital signature scheme (DSS)
2. Encrypt the message and the signature using a private key encryption algorithm under randomly chosen encryption key
3. Encrypt the random message encryption key using receiver's public key
4. Send the message following steps 1 to 3

This approach is known as “Signature-Then-Encryption ". It can be shown in the following Fig-1



(Figure-1)

II. SIGNCRYPTION

In the case of public-key cryptography, confidentiality is provided by encryption schemes, while authenticity is provided by signature schemes. In many applications, both confidentiality and authenticity are needed together. Such applications include secure email (S/MIME), secure shell (SSH), and secure web browsing (HTTPS). Until recently, the de facto solution was to use both an encryption scheme and a signature scheme, typically by sequentially composing the encryption and signature operations. This state of affairs changed in 1997, when Zheng [15] proposed using a single cryptographic primitive to achieve both confidentiality and authenticity. He called this primitive signcryption. At first glance, it is not clear why there should be any advantage to combining both goals into a single primitive. However, Zheng and others have demonstrated, through concrete examples, that signcryption schemes can provide clear benefits over the traditional sequential composition of encryption and signature schemes.

Public Parameter:
C: an elliptic curve of GF (ph), either with p≥2 150 and h=1 or p=2 and & h≥150.
Q: a large prime number whose size is approximately |ph|.
G: a point with order q, chosen randomly from the points on C.
Hash: a one-way hash function output of 128 bits at least.
KH: a keyed one-way hash function.
ED: the encryption and decryption algorithm of a private key cipher.

Alice's key:
Va: Alice's private key, chosen uniformly at random from [1….q-1].
Pa: Alice's public key (Pa=VaG, a point on C).

Bob's Key:
Vb: Bob's private key, chosen uniformly at random from [1….q-1].
Pb: Bob's public key (Pb=VbG, a point on C).

III. SECURITY GOAL

Confidentiality:

Confidentiality is achieved by encryption. To decrypt the cipher text(c), an adversary needs to have Bob's private key. Which is the secret key of Bob and he will never disclose it. Therefore it is unknown to third party.

Unforgeability:

It is computationally infeasible to forge a valid signcrypted text (*c*, *R*, *s*) and claim that it is coming from Alice without having Alice's private key. The private key of Alice is unknown to third party. The computation process of R and s is very difficult and infeasible to guess the solution of signcryption text.

Non-repudiation:

If the sender Alice denies that she sent the signcrypted text (*c*, *R*, *s*), any third party can run the verification procedure above to check that the message came from Alice.

Public verifiability:

Verification requires knowing only Alice's public key. All public keys are assumed to be available to all system users through a certification authority or published directly. The receiver of the message does not need to engage in a zero-knowledge proof communication with a judge or to provide a proof.

Forward secrecy:

An adversary that obtains Private Key of receiver will not be able to decrypt past messages. Previously recorded values of (*c*, *R*, *s*) that were obtained before the compromise cannot be decrypted because the adversary that has Private Key will need to calculate *r* to decrypt. Calculating *r* requires solving the ECDLP on *R*, which is a computationally difficult.

Encrypted message authentication:

The proposed scheme enables a third party to check the authenticity of the signcrypted text (*c*, *R*, *s*) without having to reveal the plaintext *m* to the third party. This property enables firewalls on computer networks to filter traffic and forward encrypted messages coming from certain senders without decrypting the message. This provides speed to the filtering process as the firewalls do not need to do full unsigncryption to authenticate senders. It also provides additional confidentiality in settling disputes by allowing any trusted/untrusted judge to verify messages without revealing the sent message *m* to the judge by running verification process as follows[15,17].

As the signcrypted text computed by the help of Alice's public key P_a and the ID_A can be verify by certificate Authority (CA). Therefore we can say the message is coming from Alice without decrypting the original message and which is authentic sender.

IV. ANALYSIS OF SIGNCRYPTION SCHEME

Comparisons based on securities properties: Table-1 [13, 17]

	Confidentiality	**Integrity**	**Unforgeability**	**Forward Security**	**Public verification**
Zheng and Imai	Yes	Yes	Yes	No	No
Bao & Deng	**Yes**	**Yes**	**Yes**	**No**	**Yes**
Gamage et al	**Yes**	**Yes**	**Yes**	**No**	**Yes**
Jung et al.	**Yes**	**Yes**	**Yes**	**Yes**	**No**

Computational Complexity:

Elliptic curve point operations are time consuming process. The propose signcryption scheme is having three point multiplication for signcryption, two point multiplication for unsigncryption and one point addition, for verification it requires one point multiplication and one point addition. The table 2 gives the details of comparison with the existing schemes and proposed scheme. [13]

Table 2: comparison of schemes on basis of computational complexity

Schemes	**Participant**	**ECPM**	**ECPA**	**Mod. Mul**	**Mod. Add**	**Hash**
Zheng & Imai	Alice	1	-	1	1	2
	Bob	2	1	2	-	2
Han et al	Alice	2	-	2	1	2
	Bob	3	1	2	-	2
Hwang et al	Alice	2	-	1	1	1
	Bob	3	1	-	-	1

Table 3: comparison based on average computational time of major operation in same secure level the elliptic curve multiplication only needs 83ms & the modular exponential operation takes 220 ms for average computational time in infineon's SLE66CU* 640P security controller.[15]

Schemes	**Sender average. computational time in ms**	**Recipient average computational time in ms**
Zheng & Imai	1* 83=83	2*83=166
Bao & Deng	2*220=440	3*220=660
Gamage et al	2*220=440	3*220=660

Jung et al	2*220=440	3*220=660

V. CONCLUSION

The security of zheng & Imai, Bao & Deng, Gamage et al, Jung et al and Han et al.'s signcryption scheme [11, 8, 5] are analyzed on basics of security goal, communication overhead and computational cost. All the schemes are satisfying all the properties of security. The signcryption schemes by Bao & Deng and Gamage et al are having public verification but no forward secrecy. Similarly the Zheng & Imai not supports the forward secrecy and public verification [8] where as the Jung et al scheme supports forward secrecy but can't verifiable by public[9, 11, 13]. In terms of computational cost the Zheng & Imai scheme take less time in comparison with Bao & Deng, Gamage et al and Jung et al signcryption schemes [13]. A signcrypton scheme can be developed which will provide all the properties of security.

Reference

[1] Yuliang Zheng. Digital signcryption or how to achieve cost (signature encryption) Cost (signature), Cost (encryption). In CRYPTO '97: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, pages 165-179, London, UK, 1997. Springer-Verlag.

[2] William Stallings. Cryptography and Network security: Principles and Practices. Prentice Hall Inc., second edition, 1999.

[3] Paul C. van Oorschot Alfred J. Menezes and Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press,1996.

[4] Behrouz A. Forouzan. Cryptography and Network Security. Tata McGraw-Hill, 2007.

[5] F. Bao, R.H. Deng, "A signcryption scheme with signature directly verifiable by public key", Proceedings of PKC'98, LNCS 1431, Springer-Verlag, 1998, pp. 55–59.

[6] LEI Feiyu, CHEN Wen, CHEN Kefei, "A generic solution to realize public verifiability of signcryption", Wuhan University Journal of Natural Sciences, Vol. 11, No. 6, 2006, 1589-1592.

[7] Mohsen Toorani and Ali Asghar Beheshti Shirazi. Cryptanalysis of an efficient signcryption scheme with forward secrecy based on elliptic curve. Computer and Electrical Engineering, International Conference on, 428-432, 2008.

[8] Yuliang Zheng and Hideki Imai. How to construct efficient signcryption schemes on elliptic curves. Inf. Process. Lett., 68(5):227-233, 1998.

[9] Jung.H.Y,K.S Chang, D.H Lee and J.I. Lim, Signcryption scheme with forward secrecy. Proceeding of Information Security Application-WISA, Korea, 403-475, 2001.

[10] Gamage, C., J.Leiwo, Encrypted message authentication by firewalls. Proceedings of International Workshop on Practice of Theory in Public Key Cryptography, Berlin, 69-81, 1999.

[11] X. Yang Y. Han and Y. Hu. Signcryption based on elliptic curve and its multi-party schemes. Proceedings of the 3rd ACM International Conference on Information Security (InfoSecu 04), pages 216-217, 2004.

[12] Henri Cohen and Gerhard Frey, editors. Handbook of elliptic and hyperelliptic curve cryptography. CRC Press, 2005.

[13] Mohsen Toorani and Ali Asghar Beheshti Shirazi. An elliptic curve-based signcryption scheme with forward secrecy. Journal of Applied Sciences, 9(6):1025 -1035, 2009.

[14] G. Seroussi. Elliptic curve cryptography. page 41, 1999.

[15] Hwang Lai Su. An efficient signcryption scheme with forward secrecy based on elliptic curve. Journal of applied mathematics and computation, pages 870-881, 2005.

[16] Mohsen Toorani and Ali Asghar Beheshti Shirazi. Cryptanalysis of an elliptic curve-based signcryption scheme. International journal of network security vol.10, pp 51-56, 2010.

[17] Wang Yang and Zhang. Provable secure generalized signcryption. Journal of computers, vol.5, pp 807-814, 2010.