RESEARCH REVIEW JOURNALS
Volume-03
Issue-06
June-2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Mechanism of Signcryption – A Review

*Anuj Kumar Singh

Assistant Professor, Amity University, Haryana, Gurgaon (India)

ARTICLE DETAILS

Article History
Published Online: 16 June 2018

Keywords
Signcryption, Mechanism, Review

***Corresponding Author**
Email: anujbtechcs[at]gmail.com

ABSTRACT

Signcryption is a relatively new way to achieve confidentiality and authentication simultaneously. Before the advent of signcryption the approach was to first encrypt and then to sign the message, but this scheme had more computational cost and communication overhead. Many signcryption schemes have been developed and implemented so far, but differ in security attributes they provide and computational cost they incur. This paper explains the mechanism of signcryption and analyzes the different cryptographic approaches which can be used along with signcryption. It also provides a glimpse of different signcryption schemes proposed.

1. Introduction

The technique of Signcryption was introduced by Yuliang Zheng [1] in 1997. Signcryption is relatively a new cryptographic system which combines encryption and authentication in only one logical step. Zheng claimed that signcryption incurs 58% less computational cost and 85% less overhead in comparison to the conventional signature-then-encryption approach. Since the inception of signcryption many signcryption schemes have been given by the authors throughout the years offering different security attributes while having certain advantages and limitations. Also these signcryption schemes are based on DLP (Discrete Logarithmic Problem), ECDLP (Elliptic Curve Discrete Logarithmic Problem) or BDHP (Bilinear Diffie Hellman Problem). The mechanism of signcryption has been explained in the upcoming section of the paper.

2. Mechanism of Signcryption

Signcryption mechanism has three phases namely Initialization Phase, Signcryption Phase and Un-signcryption phase [1].

a) *Initialization Phase* is intended to select global public parameters used by Alice (Sender) and the Bob (Receiver). The key pair for Alice and Bob is also chosen in this phase. The steps carried out are shown in Figure 1.

b) *Signcryption Phase* enables sender Alice to send the signcrypted message to the recipient Bob. Alice selects a random integer x in the range [1, q-1]. The key k is generated and divided into two subkeys k1 and k2 of equal length, used in subsequent operations. The computations performed are shown in Figure 2. Alice sends signcrypted message (c,r,s) to Bob.

c) *Un-signcryption Phase* - After receiving the signcrypted message (c,r,s) Bob computes the key k and divides it into two subkeys k1 and k2 of equal length. The computations are shown in Figure 3.

In this way using signcryption encryption and authentication are performed in only one logical step.

Selection of Public Parameters

1. p and q – two large prime numbers, where q is a large prime factor of $p-1$
2. g – a random integer in the range $[1, p-1]$ with order q modulo p.
3. KH – a one-way keyed hash function
4. H – a one-way hash function
5. (E, D) – Encryption, Decryption

Selection of Key Pairs

1. x_a – a random number in the range $[1, q-1]$. (Private key of Alice)
2. y_a – computed as $y_a = g^{xa} \bmod p$. (Public key of Alice)
3. x_b – a random number in the range $[1, q-1]$. (Private key of Bob)
4. y_b – computed as $y_b = g^{xb} \bmod p$. (Public key of Bob)

Figure 1: Steps in Initialization Phase

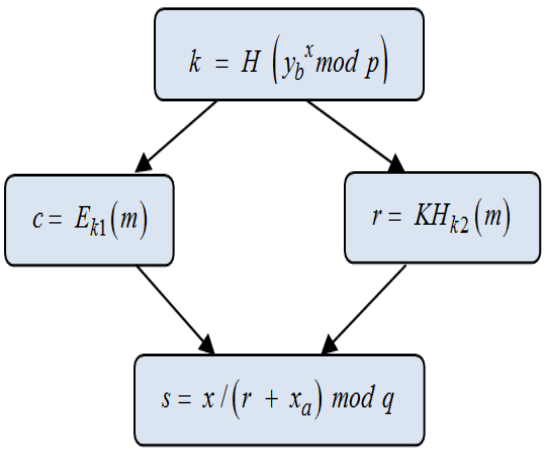

Figure 2: Computations Performed in Signcryption Phase

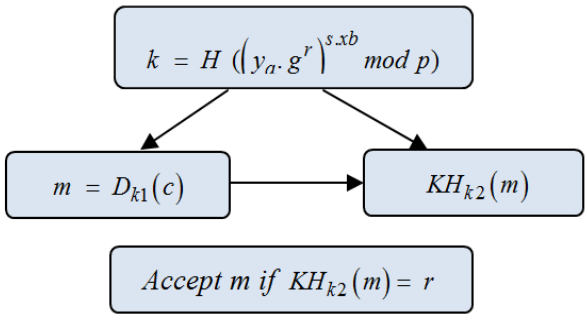

Figure 3: Computations in Un-Signcryption Phase

Furthermore, signcryption scheme should possess correctness, efficiency and security properties which are critical to resource constrained applications.

1) *Correctness:* A signcryption scheme is correct if it correctly verifies the signature and recovers the original plaintext from ciphertext successfully.

2) *Efficiency:* If signcryption scheme incurs less computational time and less communication overhead in comparison to the conventional signature followed by encryption approach then it is said to be efficient.

3) *Security:* A signcryption scheme enables secure communication if the same satisfies the following security attributes - confidentiality, unforgeability, integrity, non-repudiation, forward secrecy, encrypted message authentication and public verification.

3. Different Signcryption Schemes

With the use of heterogeneous devices in today's computing environment many types of signcryption schemes have been proposed which are being analyzed in this section.

The very first signcryption scheme was given by by Yuliang Zheng [1] saving 50% of computational time and 85% communication overhead in comparison to to the conventional method of signature-then-encryption at the same time providing confidentiality, unforgeability and non-repudiation. This approach was designed on the basis of discrete logarithmic problem (DLP) and involved modular exponentiation .

Zheng's signcryption scheme was improved by Bao and Deng [2] enabling a judge or a third party to authenticate signature without knowing the receiver's private key, in the case a dispute occurs. But it requires the use of exterior key exchange algoritthn for the process of verification.

First ECC (Elliptic Curve Cryptography) based signcryption scheme was given by Zheng and Imai [3] with all the basic security features. The scheme took 58% reduced computational cost and 40% reduced communication cost than the old signature-then-encryption method. As the scheme uses ECC it was suitable for applications involving resource constrained devices. This scheme provides all the basic security features but misses forward secrecy.

C.Gamage et al. [4] proposed a new signcryption system providing encrypted message authentication i.e the scheme can verify signature at application layer and plain text is not needed in the process of verification.

Jung et al.5 proposed a new signcryption method based in which even if an attacker obtains the private key of the sender he cannot deduce the original message. This scheme was based on DLP and also provides forward secrecy but in this scheme when a dispute occurs the judge can not verify the message directly.

Hwang [5] gave a method to design efficient signcryption schemes based on elliptic curve arithmetic taking lower computational cost, communication overhead, and less key size while at the same time providing all the security attributes including confidentiality, unforgeability, message authentication, integrity of the message, non-repudiation, forward secrecy and public verification by trusted third party. But this scheme was analyzed by Mohsen Toorani and Ali Asghar [6] who proved that the scheme fails to provide necessary security attributes. They also showed that the scheme has weak session key establishment and fails to provide validity verification of public keys and the certificates.

Han et.al [7] designed an elliptic curve based generalized signcryption method providing confidentiality and authentication differently with the condition of specific inputs. In the proposed scheme a third party using ECDSA (Elliptic Curve Digital Signature Algorithm) can verify the signcrypted text publicly.

E.Mohamed et.al [8] suggested a new signcryption approach based on elliptic curves providing forward secrecy along with encrypted message authentication for firewalls. In this scheme without sender's private key a judge can directly verify the sender's signature on the signcrypted messages. This scheme combines the all the basic security properties with less computational complexity and communication overhead.

Xiu-Xia et.al. [9] proposed an ID-based proxy signcryption scheme which posses strong security attributes such as verifiability, strong non-repudiation, strong unforgeability, confidentiality, prevention of misuse and forward secrecy. This scheme was based on bilinear pairings.

Toorani and Asghar [10] designed a new signcryption scheme offering all the necessary security attributes including basic security features in combination with forward secrecy and public verification. The scheme was based on ECC but takes more computational cost in terms of number of computations (Table II), as compared to existing schemes.

F.Amounas [11] designed an improved signcryption scheme based on elliptic curve cryptography providing all the required security properties with less cost. The scheme was found suitable for resource constrained devices.

Fagen, Hui and Tsuyoshi [12] proposed two efficient signcryption schemes for heterogeneous environment providing confidentiality, integrity, authentication and non repudiation. The

first scheme allows an entity in PKI (Public Key Infrastructure) to send a message to an entity in an IBC (Identity based Cryptosystem). The second scheme enables an entity in IBC to send a message to an entity in PKI. The proposed schemes takes less key size and the ciphertext size is relatively small.

Huiyan, Yong and Jinpin [13] constructed a new identity based signcryption scheme which can process arbitrary length plaintexts. The scheme produced shorter ciphertexts.

S.Lal and P.Khushwah [14] designed a new generalized signcryption scheme that can work as an encryption scheme as well as a signature scheme. The scheme was based on bilinear pairings.

S.Mohanty and M.Prasad [15] proposed a blind signcryption scheme which provides universal verification, traceability, non-repudiation and unforgeability of parameters. The scheme was proved to be more secure in maintaining user's anonymity.

L.Cheng and Q. Wen [16] enhanced the signcryption scheme given by Liu et.al. [17]. The scheme proposed by Chen and Wen was impossible to tell apart against chosen plaintext attack and was unforgeable against chosen ciphertext attacks. This scheme has smaller public parameter size than the previous schemes but incurs more computational cost.

4. Analysis of Cryptographic approaches

With the advancement in cryptographic techniques to make communication more secure primarily the focus has been on three types of systems namely private key cryptography, public key cryptography and elliptic curve cryptography. With the inception of public key cryptography it has been widely used because it solves the problem of key distribution, a well known drawback of secret key cryptography. In 1985 when V. Miller [19] and N. Koblitz [20] introduced elliptic curve cryptography the paradigm began to shift due to the efficiency of ECC.

Table 1 shows the key size required by each of the three cryptographic systems to achieve same level of security [21]. We can deduce that ECC outperforms public key methods and attain same security level with relatively a very small key size.

Table 1. Key size required for equal level of security

S. No	Private Key Cryptography	Public Key Cryptography	Elliptic Curve Cryptography
1	80	1024	160
2	112	2048	224
3	128	3072	256
4	192	7680	384
5	256	15360	512

Furthermore L.Batina et al. [22] mentioned in their work that SLE 66CUX640P processor of maximum clock frequency 15 MHz, takes 220 ms to execute a modular exponentiation operation (modulus size 1024 bits) and it takes 83 ms in computing an ECPM (elliptic curve point multiplication) operation (modulus size 160 bits). We may conclude that the signcryption schemes based on elliptic curves are more efficient in terms of computational cost than modular exponentiation based schemes. And due to this reason the schemes based on elliptic curves are better suited to resource constrained environments involving low computing devices.

5. Conclusion

In the new computing era, today security has become a very important and essential aspect of any system. Signcryption has revolutionized the implementation of security features due to its low cost and less overhead. This article has explained the process and properties of signcryption in detail. Furthermore different cryptographic approaches has been analyzed to see their potential applicability in signcryption schemes. The work presented in this paper is useful for students and researchers working in the field of security.

References

1. Y. 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*, 1997, p. 165-179.
2. H. Deng and F. Bao, "A signcryption scheme with signature directly verifiable by public key", *Lecture Notes in Computer Science- Springer-Verlag,* vol. 1431, pp. 55-59, 2006.
3. Y. Zheng and H. Imai, "How to construct efficient signcryption schemes on elliptic curves", *Inormation Processing Leters - Elsevier,* vol. 68(5), pp. 227-233, 1998.
4. C. Gamage, J. Leiwo and Y. Zheng, "Encrypted message authentication by firewalls*", Lecture Notes in Computer Science- Springer-Verlag*, vol. 1450, pp. 69-81, 1999.
5. R. Hwang, C.H. Lai and F.F. Su, "An effcient signcryption scheme with forward secrecy based on elliptic curve", *Journal of Applied Mathematics and Computation*, vol. 167(2), pp. 870- 881, 2005.
6. M. Toorani and A.A.B. Shirazi, "Cryptanalysis of an elliptic curve-based signcryption scheme", Inernational *Journal of Network Security*, vol. 10(1), pp. 51–56, 2010.
7. Y. Han, X. Yang and Y. Hu, "Signcryption based on elliptic curve and its multi-party schemes", in *Proceedings of the 3rd ACM International Conference on Information Security (InfoSecu 04),* 2004, p. 216- 21.
8. E. Mohamed and H. Elkamchouchi, "Elliptic Curve Signcryption with Encrypted Message Authentication and Forward Secrecy", *International Journal of Computer Science and Network Security*, vol. 9(1), pp. 395-398, 2009.
9. X. Tian, J.P. Xu, H.J. Li, Y. Peng and Q. Zhang, "Secure ID-Based Proxy Signcryption Scheme with Designated Proxy Signcrypter", in *International Conference on Multimedia Information Networking and Security,* Hubei, 2009, p. 351-355.
10. M. Toorani and A.A.B. Shirazi, "An elliptic curve-based signcryption scheme with forward secrecy", *Journal of Applied Sciences,* vol. 9 (6), pp. 1025-1035, 2010.
11. F. Amounas, H. Sadki and E.H.E. Kinani, "An Efficient Signcryption Scheme based on The Elliptic Curve Discrete Logarithm Problem", *International Journal of Information & Network Security,* vol. 2(3), pp. 253-259, 2013.

12. F. Li, H. Zhang and T. Takagi, "Efficient Signcryption for Heterogeneous Systems", *IEEE Systems Journal*, vol. 7(3), pp. 420-429, 2013.
13. H. Chen, Y. Li and J. Ren, "A Practical Identity-based Signcryption Scheme", *International Journal of Network Security*, vol. 15(6), pp. 484–489, 2013.
14. S Lal and P. Kushwah, "ID based generalized signcryption", Cryptology ePrint Archive, Report, 2008/84, http://eprint.iacr.org/2008/84.pdf.
15. S. Mohanty and M. Prasad, "A universally verifiable blind signcryption scheme with message recovery", in *2nd International Conference on Signal Processing and Integrated Networks (SPIN),* 2015, p. 630-632.
16. L. Cheng and Q. Wen, "An improved certificateless signcryption in the standard model", *International Journal of Network Security*, vol. 17(3), pp. 229- 237, 2015.
17. Z. Liu, Y. Hu, X. Zhang and H. Ma, "Certificateless sgncryption scheme in the standard model", *Information Sciences*, vol. 180(3), pp. 452-464, 2010.
18. M. Toorani and A.A.B. Shirazi, "Cryptanalysis of an efficient signcryption scheme with forward secrecy based on elliptic curve", in *Proceedings of 2008 International Conference on Computer and Electrical Engineering (ICCEE'08),* 2008, p. 428–432.
19. V. Miller, "Use of elliptic curves in cryptography", in *Advances in Cryptology - CRYPTO '85 Proceedings*, 1985, p. 417–426.
20. N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation,* vol. 48 (177), pp. 203–209, 1987.
21. S.A. Vanstone, "Elliptic curve cryptosystem the answer to strong fast public-key cryptography for securing constrained environments", Information Security Technical Report 2(2), 1997, pp. 78-87.
22. L. Batina, S. Berna, B. Parneel and J. Vandewalle, "Hardware architectures for public key cryptography", *Integration- The VLSI Journal,* vol. 34 (1-2), pp. 1-64, 2003.

