Signcryption Approaches for Network Security

S.K.B.Sangeetha,
S.L.Jayalakshmi

Abstract— Signcryption is a new public key cryptography approach to combine digital signature and encryption functionalities as a consequence of the growing consumer demand for information security. The necessity to achieve confidentiality, integrity, authenticity and non-repudiation properties in data communication that motivates new demands for signcryption schemes. The framework of signcryption involves key generation, signcryption and unsigncryption. Current signcryption schemes development is still limited by the certain constraints given by real-time applications. For example, broadcasting signcrypted message increases bandwidth consumption and computational resource usage remains largely an unsolved problem. In order to address these problems, ElGamal's signature scheme, Schnorr's signature scheme or Digital signature schemes , Diffie Hellman method, Elliptic Curve method and RSA algorithm are widely used for signcryption. This paper provides a tutorial and overview of strategies in implementing these algorithms and provides a focus on asymmetric techniques in research.

Index Terms— Key generation, Signcryption, Unsigncryption,DES,AES,Elliptic curve,Asymmetric algorithms.

1 Introduction

Cryptography is a technique to share message in secured manner. Applications of cryptography is surveyed in (7).Private key cryptography uses private key which is shared between sender and receiver where keys may be compromised due to disclosed communication. This method is also called as symmetric key cryptography. Several symmetric key algorithms include Data Encryption Standard(DES), 3DES, Advanced Encryption Standard(AES) , Rivest Cipher or Ron's Code etc. Comparative analysis of symmetric key cryptography algorithms is described in [9][10]. Pair of keys shared between parties in public key cryptography. Message is encrypted using public key and private key is used for decryption. Signcryption is a public key cryptography approach to ensure authentication, confidentiality, integrity and nonrepudiation[1]. Traditional signature then encryption increases computational cost and communication overhead. In 1997 Yuliang Zheng introduced Signcryption scheme that overcomes the existing problem and provides an efficiency in terms of better computation time.

Signcryption has wide variety of applications such as ecommerce, groupware (such as video conferencing, multicasting a message to specific members, electronic filing cabinets) and ATM networks etc. There exists a web portal that provides all information about signcryption standards[2].Data communication includes the following:1) Sender, which is a source to transmit data, source usually a computer.; 2)Medium through which data is transferred, it may be wired or wireless.;3)Receiver, which is a device to receive the Data[3]. In this paper, we focus on signcryption based data communication and a survey on signcryption methods.

There are various surveys related to signcryption approach that are listed in following table 1.

Table 1. Surveys on Signcryption

Year	Author	Topic
1996	Y.Zheng et al.	Efficient Signcryption Schemes on Elliptic Curves
2005	LI Xiang-xue et al.	Cryptanalysis and Improvement of Signcryption Schemes on Elliptic Curves
2005	Yevgeniy Dodis	Signcryption (Short Survey)
2009	Sharmila Deva Selvi et al.	A note on Certificateless Multireceiver Signcryption Scheme
2011	FagenLi et al.	A Survey of Identity-Based Signcryption
2012	LI Fa-gen et al.	A Survey of Digital Signcryption
2013	Shweta Khullar et al.	A Survey of Identity Based Multireciever Signcryption scheme
2013	Hassan M.Elkamchouchi et al.	An Efficient ID based Proxy Signcryption Scheme without Bilinear Pairings
2013	Wei Zhang	Improvements and Generalisations of Signcryption Schemes

Fagen Li at al. (4) give formal model of Identity based signcryption and its special properties along with identity based hybrid signcryption. Identity based approach is a better alternate for traditional certificate based approach. Paper (8) discusses a survey of applications of Identity based approach. LI Xiang xue et al.(5) analyses elliptic curve based signcryption schemes. In (6) provides the research work that has been carried out in signcryption during the year 1997 to 2011. Historical development of signcryption is described in (11).

Traditional signature-then- encryption method signs the message using digital signature and it is encrypted using sender's private key followed by receiver's public key. Fig 1

- *S.K.B.Sangeetha is currently working as an assistant professor in computer science and engineering department in Velammal Engineering College, Chennai. E-mail: skbsangeetha@gmail.com*
- *S.L.Jayalakshmi is currently working as an assistant professor in computer science and engineering department in Velammal Engineering College, Chennai.E-mail: sathishjayalakshmi02@gmail.com*

gives the framework of signature then encryption method. This method consumes more machine cycles and increases cost for digital signature and encryption. Signcryption fulfills the requirement of digital signature then encryption. It combines both the functionalities which reduces the cost and average computation time.

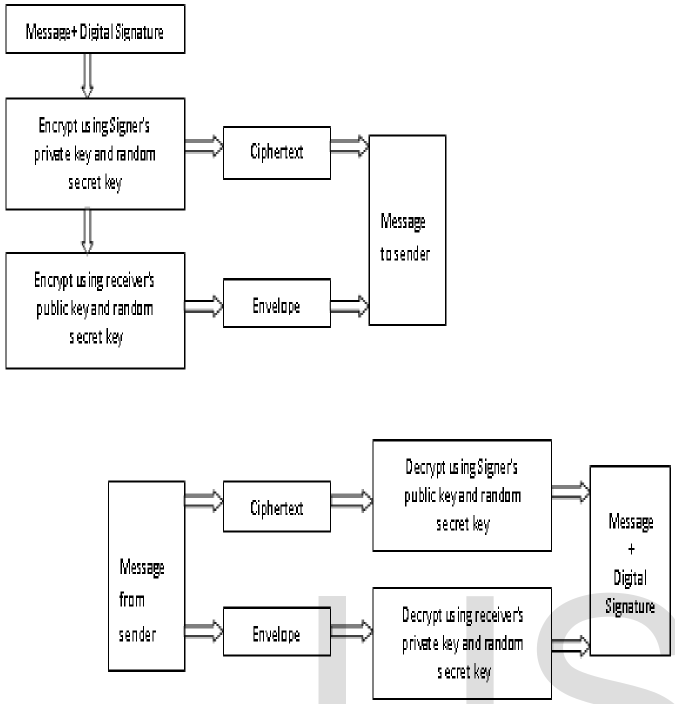
Message+ Digital Signature
Encrypt using Signer's private key and random secret key
Ciphertext
Message to sender
Encrypt using receiver's public key and random secret key
Envelope
Message from sender
Ciphertext
Decrypt using Signer's public key and random secret key
Message + Digital Signature
Envelope
Decrypt using receiver's private key and random secret key

Fig 1. Signature –then- Encryption Scheme

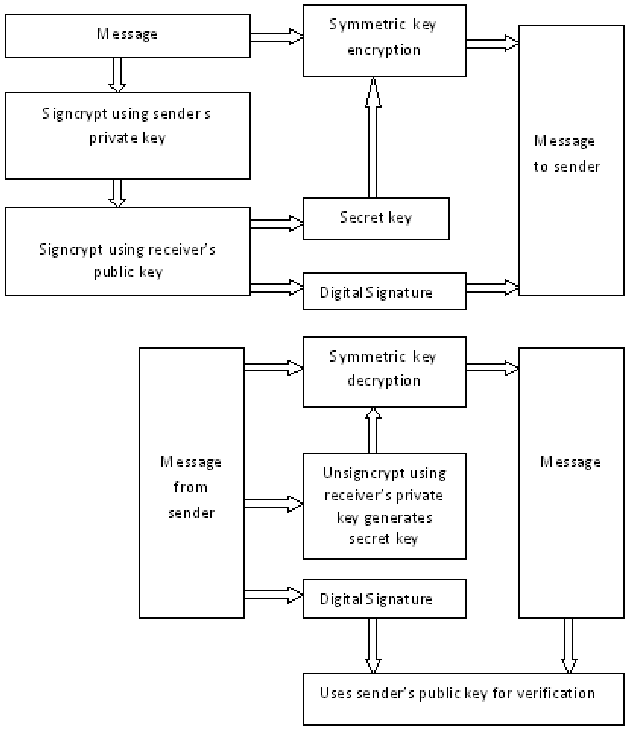
Message
Symmetric key encryption
Signcrypt using sender s private key
Message to sender
Secret key
Signcrypt using receiver's public key
Digital Signature
Message from sender
Symmetric key decryption
Message
Unsigncrypt using receiver's private key generates secret key
Digital Signature
Uses sender's public key for verification

Fig 2. Signcryption scheme

Signcryption concerns four facets of data transfer.

1.Confidentiality

The message transmitted from sender to receiver cannot be read by anyone else.

2. Authenticity

The message received by receiver ensures that the message could be sent only by sender.

3. Integrity

Receiver knows that the message transmitted from sender has not been altered.

4. Non –Repudiation

The sender cannot claim that message transferred without his / her knowledge.

We give more detailed overview about the overall process of signcryption which is outlined in figure 2. The framework includes the following: 1) Key generation : generates primary key and public key; 2) Signcryption: includes digital signature and encryption to produce ciphertext from message;3) Unsigncryption: decrypts ciphertext to get the message. In this paper, the methods used for signcryption and future developments in signcryption are reviewed. The main contribution of this paper is

1) Signcryption components and its relationships are described clearly.
2) Various approaches for signcrypting meassge are discussed with its merits and demerits.

The above said points clearly distinguish this survey from other surveys. It gives the detail as broad as earlier works. The paper is organized as follows: Section II reviews the work related to key generation. Section III discusses signcryption techniques. Section IV summarizes the current work.

II.KEY GENERATION

Key plays an important role in transformation of plaintext to ciphertext and vice versa. Protection of key is easy and it can be changed easily, if it is compromised. In private key cryptography same key is used for both encryption and decryption but in public key cryptography pair of keys used.

1. Key Size

Key size is an important factor that must be considered for secrecy. It is simplest to use brute force attack which tries all possible numbers up to the length of the key. Key size must as long as the message size otherwise the attacker can predict all possible combinations. Key size (in bits) is a number in power of two which is preferred. If key length is n bits, it can produce exponential number of keys. 128 bit key size is used wide spread. To achieve the high level security, different algorithms use different key sizes. The security of algorithm is distinct and cannot exceed than key length. Symmetric key algorithm 3DES has key length 168 bits but provides security of atmost 112 bits. Symmetric key algorithms are designed to have key size equivalent to security. But asymmetric algorithms like elliptic curve cryptography algorithm uses security equivalent to half its key length. Table 2 and Table 3 list the recommended key sizes for symmetric and asymmetric algorithms. [16] describes key length recommendations from well known organizations.

a. Symmetric algorithm key length

No	Algorithm	Key size
1	DES	56
2	3DES	168 / 112 / 56
3	AES	128 / 192 / 256
4	RC	128

b. Asymmetric algorithm key length

No	Algorithm	Key size
1	Elliptic Curve	2048 / 3072
2	DiffieHellman	2048 / 3072
3	DSA	2048 / 3072
4	RSA	1024 / 2048 / 3072
5	ElGamal	1024 / 2048

2. Key Management

Key management used to protect secrecy of data. Because, if key is obtained by the attacker, then data can be easily decrypted.

Key management scheme involves following phases

i) Preoperational phase

Key is not available. It involves Key generation, Key distribution, Key agreement and Key registration.

ii) Operational phase

Key is available and it is in normal use. It performs Key storage, Key recovery, Key exchange and Key derivation

iii) Post operational phase

Key can be accessed but not in normal use. It has Key deregistration, Key destruction and Key revocation.

In [12] Key management phases and functions are described in detail.

3. Classification of Keys

There are different types of keys used for cryptography. Key types can also be used in combinations to increase security level. Key types are classified based on

i)Authentication which provides assurance for the integrity of data communication,
ii)Authorization which is used for verifying the privileges,
iii)Agreement and transport which are used for establishing keys and other keying material,
iv)Signature which is used for verifying signatures,
v)Wrapping keys which can be used to protect keys,
vi)Random number generation .

Key types can be either private or public. All these key types can be used both for symmetric and asymmetric algorithms[1].

a. Private Key

Private key also known as secret key which is shared between the parties before communication. Traditionally, One Time Pad method is used which generates private key randomly and it can be used only once. Private keys are used in symmetric key algorithms. It must be as long as the message to be encrypted.

Private key encryption is simple and faster than public key encryption. It uses less computation resources. But this algorithm needs a secure channel for exchanging keys which is difficult in practical. For the group communication, individual private keys equal to N*(N-1)/2 has to distributed where N is number of peoples in group. Authentication is not guaranteed because sender and receiver uses same key.

b.Public key

Public key cryptosystem requires public key for encryption and private key for decryption. Private key is authorized but public key is published. It is difficult to compromise the properly generated private key from its corresponding public key. Public keys are used in asymmetric key algorithms. Public key encryption is convenient because private keys are kept secret and also provides authenticity of message. This algorithm does not need a secure channel for exchanging secret keys. The algorithm needs to authenticate the public keys and loss of private key may occur.

III.SIGNCRYPTION TECHNIQUES

1.ENCRYPTION

Cipher is an algorithm which converts the plaintext into ciphertext by using key which is called an encryption. Traditionally substitution techniques and transposition techniques were used[13].

A.Substitution Methods

The unit of plaintext is replaced by the unit of ciphertext.

1. Caesar Cipher

Replaces each alphabet with the letter positioned three places from the alphabet. Only 25 keys for brute-force analysis, so it is insecure.

2. Monoalphabetic Cipher

Cipher text can be permutation of alphabets. But relative frequency reflects the original data.

3. Playfair Cipher

5*5 matrix is constructed using keyword.26*26=676 individual matrices. Identification of matrice and guessing frequency of data occurrence is impractical.

4. Hill Cipher

M successive plaintext characters are substituted by M ciphertext letters based on linear algebra. No possibility of guessing single letter frequencies as in playfair algorithm. But it can be easily broken with known plaintext attack.

5. Poly alphabetic Cipher

Original message is replaced through different monoalphabetic substitution. In paper [15], polyalphabetic cipher techniques were discussed in detail.

Two forms of polyalphabetic cipher

a. Vigenere Cipher

Multiple ciphertext letters are distributed to each plaintext letter based on letters of keyword.But frequency of data occurrence remains.

b. Vernam Cipher

Plaintext combined with random generated key to produce ciphertext by performing XOR function.

c. One-Time pad

The algorithm uses randomly generated key but the key can be used one time.

B. Transposition Methods

The unit of plaintext is rearranged to form ciphertext. It can be considered more secure because of more than one stage of transposition. The simplest method is rail fence cipher which writes the plaintext in diagonal and reads the sequence horizontally.

C. Rotor Machines

It consists set of rotors to have an array of electrical contacts to implement fixed letter substitution which is complex than polyalphabetic substitution cipher[1].

D. Stegnography

The method hides the existence of plaintext which makes concealed writing. Traditionally character marking, invisible ink, pin punctures, typewrite correction ribbon etc..were used. Stefan katzenbeisser et al.[14] introduced the field of information hiding followed by detailed description of stegnographic techniques and its applications.

E.Digital Signature

Digital signature ensures the authenticity , integrity and non-repudiation of the transmitted message and sender's or signer's identity. It can be used with any kind of message whether it may be encrypted or not.

It consist two algorithms

1. Generation of digital signature

   The algorithm encrypts the message and sender's private key to produce digital signature.

2. Verification of digital signature

   The algorithm verifies the digital signature using receiver's public key.

2.ASYMMETRIC ALGORITHMS

A.Elliptic curve Algorithm

Elliptic curve cryptography is an asymmetric algorithm which is based on finite field on algebraic system. The points on elliptic curve forms an abelian group under a well defined group operation. The algorithm significantly requires smaller key size for providing faster computation and availing less storage space. Paper [19] discusses elliptic curve cryptography algorithm and its application in detail.

B.RSA Algorithm

The algorithm implements public key cryptosystem where public key is used for encryption and private key is used for decryption. In [18] Hong Biao Zeng introduced new method to carry out the calculations of RSA algorithms using spreadsheet. The algorithm uses large numbers, therefore it is secure due to the cost of factoring large numbers. But chosen ciphertext attack is possible. Factoring problem is an open challenge in RSA encryption. In [17], author demonstrated an efficient method for the factoring problem in this algorithm.

C.DSA Algorithm

The algorithm selects the parameters which is shared to different users. Based on the set of parameters , private key and public key is computed for single user. Security of algorithm depends on the security of computing discrete logarithms. The algorithms is faster than RSA but more complex than ElGamal scheme.

D.DiffieHellman Algorithm

The algorithm uses exponential key agreement protocol and allows the users to exchange secret key which is based on discrete logs. DiffieHellman algorithm plays a vital role in creation of secure protocols such as Secure Socket Layer(SSL), Secure Shell(SSH), Internet Protocol Security(IpSec), Public Key Infrastructure (PKI) etc[20].

E.Elgamal Encryption

The algorithm is based on DiffieHellman method and used in hybrid cryptosystem where message is encrypted using symmetric method and elgamal encrypts the key used for symmetric method. The security of algorithm depends on difficulty of computing discrete logarithms in a large prime modules.The method is quite slow and used for key authentication protocols [21].

IV.CONCLUSION

Signcryption is a new public key cryptography approach to address the problem of bandwidth consumption and computational resource which also ensures four facets of data transfer. ElGamal's signature scheme, Schnorr's signature scheme or Digital signature schemes , Diffie Hellman method, Elliptic Curve method and RSA algorithm are widely used for signcryption. The importance of signcryption and key generation with the overview of strategies in implementing these algorithms are discussed.

V.REFERENCES

[1] En.wikipedia.org/wiki

[2] www.signcryption.org/standards

[3] Behrouz Forouzan, “ Data communications and Networking”, Tata McGrew Hill, Fifth Edition, 2012.

[4] Fagen Li and Muhammad khurram khan, “ A Survey of Identity-based Signcryption”, IETE Technical review, Vol 28, Issue 3, June 2011.

[5] LI Xiang-xue, CHEN ke-fei and LI Shi-qun, “ Cryptanalysis and Improvement of Signcryption Schemes on Elliptic Curves”, Wuhan University Journal of Natural Sciences, Vol.10 , No 1,2005.

[6] LI Fa-gen and ZHONG Di, “ A Survey of Digital Signcryption”, CNKI Journal, China, 2012.

[7] Shivangi Goyal, “ A Survey on the Applications of Cryptography”, International Journal of Engineering and Technology, Volume 2 No.3, March 2012.

[8] Shushan Zhao, Akshai Aggarwal, Richard Frost and Xiaole Bai, “ A Survey of Applications of Identity- Based Cryptography in Mobile Ad-Hoc Networks”, IEEE Communications Surveys & Tutorials, 2011.

[9] Anjali Patil and Rajeshwari Goudar, “ A Comparative Survey of Symmetric Encryption Techniques For Wireless Devices, International Journal of Scientific and Technology Research, Volume 2, Issue 8, August 2013.

[10] Monika Agarwal and Pradeep Mishra, “ A Comparative Survey on Symmetric Key Encryption Techniques”, International Journal on Computer Science and Engineering, Vol 4, 2012.

[11] Alexander W.Dent, Yuliang Zheng, “ Practical Signcryption”, Springer, 2010.

[12] Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid, “ Recommendation for Key Management”, National Institute of Standards and Technology , Special Publication, 2007.

[13] William Stallings,” Cryptography and Network Security Principles and Practice”, 5th edition,Pearson education,2011.

[14] Stefan katzenbeisser and Fabien A.P.Petitcolas, “ Information Hiding Techniques for Stegnography and Digital Watermarking”, Artech House, INC , London,2000, ISBN 1-58053-035-4.

[15] Sonia Dhull, Sonal Beniwal, Preeti Kalra, “ Plyalphabetic Cipher Techniques used for Encryption purpose”, International Journal of Advanced Research in Computer science and Software Engineering”, Volume 3, Issue 2, Febraury 2013.

[16] www.keylength.com

[17] Ambedkar, Gupta, Gautam, Bedi, “ An Efficient Method to Factorize the RSA Public Key Encryption”, IEEE International Conference on Communication Systems and Network Technologies, June,2011.

[18] Hong Biao Zeng, “ Teaching the RSA algorithm using spreadsheets”, Journal of Computing Sciences, Oct 2012.

[19] Amara, Siad, “Elliptic Curve Cryptography And Its Applications Systems, Signal Processing And Their Applications (WOSSPA), 2011 7th International Workshop On May 2011.

[20] Ik Rae Jeong, ETRI,Daejeon, Jeong Ok Kwon and Dong Hoon Lee, “ Strong Diffie-Hellman-DSA Key Exchange”, Communications Letters, IEEE, Volume 11, Issue 5, May 2007.

[21] Flonta.S, Miclea.L, “ An Extension of the ElGamal Encryption Algorithm”,IEEE International Conference on Automation, Quality and Testing, Robotics, 2008.