New Hybrid Signcryption Approach: Efficient Digital Envelope Signcryption

The` Seint Aye, Than Naing Soe
University of Computer Studies Mandalay
tseintaye@gmail.com, konaing2006@gmail.com

Abstract

In the study of Cryptography, the most important and widely studied are confidentiality and integrity. Confidentiality is supported by encryption schemes, while integrity is provided by digital signature schemes. Drawback of symmetric encryption is key distribution problem. Although asymmetric encryption can solve this problem, all of these ciphers are hundreds or thousands of times slower than symmetric ciphers. Digital envelope combines the advantages of asymmetric and symmetric key ciphers. It eliminates time complexity problem of asymmetric encryption and key exchange problem of symmetric encryption. But it cannot provide data integrity. So it cannot be avoidable to use digital signature scheme to guarantee the source and integrity. New hybrid signcryption approach named "Efficient Digital Envelope Signcryption" is proposed. This new approach operates digital signature process and asymmetric encryption process in a single step. It takes advantages of digital envelope scheme and signcryption scheme with appropriate algorithms.

1. Introduction

Signcryption was introduced by Zheng in 1997. It is a new paradigm in public key cryptography. In two-step approach, signature-then-encryption, the sender would sign the message and encrypt the message [8]. Signcryption simultaneously fulfils both the functions of section 3 and in section 4. The proposed digital envelope signcryption scheme is presented in section 5. Design for the proposed scheme is shown in section 6. Finally, concluding remark will follow in Section 7.

2. Related Works

Wenbo Mao and John Malone-Lee [7] presented a signature scheme based on RSA. It provides proofs of security in the random oracle model for its privacy and unforgeability. Their scheme has two very appealing aspects to it. First, it does not use any symmetric encryption. Secondly it offers non-repudiation in a very straightforward manner. The resulting scheme is very digital signature and public key encryption in a logically single step [11].

A digital envelope (encryption) is the electronic equivalent of putting your message into a sealed envelope to provide privacy and resistance to tampering. A digital signature is the electronic equivalent of a signet ring and sealing wax: the sender seals the message so that the receiver has a high degree of confidence that the message really came from the purported sender and that no one has altered it [5]. Digital envelope scheme uses the symmetric key ciphers and the asymmetric key ciphers. It provides confidentially service. Moreover, digital signature cannot be imitated by someone else, and can be automatically time-stamped. The benefits of digital signatures are data authentication and data integrity. Therefore, it can support confidentiality, integrity, authentication, unforgeability and non-repudiation.

The proposed scheme will decrease time complexity and will be preliminary step for future research trend of lightweight cryptography and mobile devices computing. For that reason, the proposed scheme costs are significantly smaller than required by the best currently known signature-then-encryption scheme.

This paper is organized as follows: In section 2, some paper related with signcryption is described. Encryption, digital signature, digital envelope and digital signcryption are discussed as theoretical study in

efficient in terms of bandwidth: a signcryption is half the size of a message signed and encrypted using standard techniques for RSA. Therefore, they give it the name Two Birds One Stone.

Alexander W. Dent and Royal Holloway [1] described a paradigm for constructing signcryption schemes with insider security based on the ideas of hybrid cryptography. The asymmetric and symmetric parts of the cryptosystem are formally separated into an asymmetric key encapsulation mechanism (KEM) and a symmetric data encapsulation mechanism (DEM). It guarantees that the overall encryption scheme was secure.

Anirvan Chkraborty, Vishnu Vardhan, Sulaiman Binmalik and Sam Renji [2] showed the advantages and disadvantages of signcryption. Signcryption is an efficient scheme as it does two steps at once during singncryption and unsigncryption. There is low computational cost as well as savings in bandwidth are major factors. And they combined two security schemes which by themselves are complex enough to withstand attacks. The last one is message recovery. But it needs to signcrypt the message with each of its intended recipient's public keys and send them separately to each one of them. This approach is redundant in terms of bandwidth consumption and computational resource usage.

3. Theory Background

Encryption is the process of transforming information (plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. Encryption of the data always ensures that the data is not in an accessible format for the unauthorized users. Two forms of encryption re in common use: conventional or symmetric encryption and public key or asymmetric encryption [12].

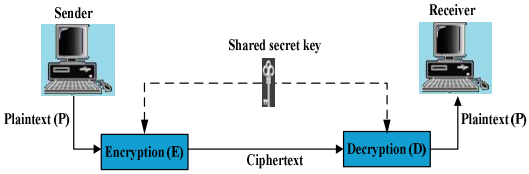

Figure1. Schematic Diagram of Symmetric Cryptosystem

Use the same key, or the secret key, to encrypt or scramble and decrypt or unscramble message. It needs to share session key as Figure 1.

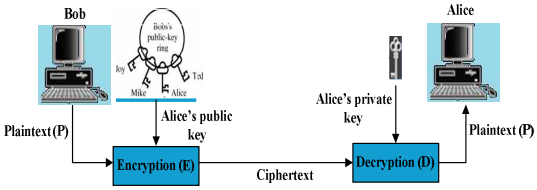

Figure2. Schematic Diagram of Asymmetric Cryptosystem

Use one key to encrypt a message and a different key to decrypt it. It is also called public key cryptosystems. It relies on technology in which two keys, the public key and the private key are use to encrypt or decrypt data as figure 2.

3.1. Digital Signature

A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message [3].

Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature in proving to a third party that the signature was in fact generated by the signatory. This is known as non-repudiation since the signatory cannot, at a later time, repudiate the signature.

The digital signature is proof to the recipient that the document comes from the correct entity. When a customer signs a check, the bank need to be sure that the check is issued by that customer and nobody else. A signature on a document, when verified, is a sign of authentication-the document is authentic.

Several digital signature schemes have evolved during the last few decades such as RSA digital signature scheme, ElGalMal digital signature scheme, Schnorr digital signature scheme and Elliptic Curve digital signature scheme.

Three algorithms are suitable for digital signature (DS) generation and verification. These are DSA, the RSA algorithm and the ECDSA algorithm. Suitable applications for public key cryptosystems are shown in table1.

Table1. Applications for Public-Key Cryptosystems

Algorithm	Encryption/ Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS/DSA	No	Yes	No

When a message is received, the recipient may desire to verify that the message has not been altered in transit. Furthermore, the recipient may wish to be certain of the originator's identity. Both of these services can be provided by a DS algorithm. A digital signature is an electronic analogue of a written signature in that the digital signature can be used in proving to the recipient or a third party that the message was, in fact, signed by the originator. Digital signatures may also be generated for stored data and programs so that the integrity of the data and programs may be verified at any later time [6].

The process begins with the hashing of the message, *M*, to produce a message digest, *H*. The digest is then encrypted using the sender's private key {*n*, *d*} to produce the signature, S in equation (1).

$$S = Hd \bmod n \quad (1)$$

To verify the message, the receiver will hash the message in equation (2), M by using the same digest function. At the same time, the signature, S is decrypted using the receiver's public key.

$$H = Se \bmod n \quad (2)$$

The results of the two processes are then compared. If they are equal then the message is authenticated and the integrity of the message is maintained.

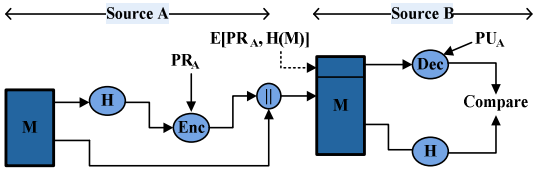

Figure3. Digital Signature

3.1. Digital Envelope

The main problem in using secret key cryptography is the distribution of the secret key among the communicating parties. To overcome this key management problem the idea of public key cryptography emerged. In public key cryptography a key consists of two parts: A public part and a private part. The public part of the key is known to all. However, the private part is only known to the owner. Furthermore, if a message is encrypted using a public or private key then it can only be decrypted using the respective private or public key. This idea has immensely simplified the key management problem. Now the participants don't have to exchange any secret key. However all they have to know is the public key of the party to whom he/she wants to send a secret message. And as this public key is known to all the sender can just grab it and start the communication. Digital Envelope is a framework, which tries to combine the advantages of the above mentioned cryptographic service [4].

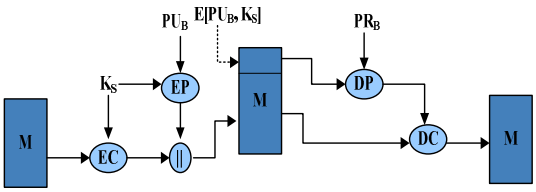

Figure4.Conceptual Model of Digital Envelope Scheme

The digital envelope process as the following equations:

$$\boldsymbol{C} = \boldsymbol{E_k(M)} \quad (3)$$

$$\boldsymbol{\beta} = AsymE\ (PU_B, \boldsymbol{k}) \quad (4)$$

Send $\boldsymbol{C}||\boldsymbol{\beta}$ *to receiver B* (5)

$$\boldsymbol{K} = AsymD\ (PR_B \boldsymbol{\beta}) \quad (6)$$

$$\boldsymbol{M} = \boldsymbol{D}_k(\boldsymbol{C}) \quad (7)$$

C = cipher text
E = symmetric encryption
K = one time section key
M = origin message
AsymE = asymmetric encryption
PU_B = public key of recipient
AsymD = asymmetric decryption
PR_B = private key of recipient
D = symmetric decryption

4. Digital Signcryption Approach

Zheng [10] effectively launched the study of signcryption by giving a pair of signcryption schemes which are significantly more efficient than sign-then-encryption both in terms of computation and message expansion. Signcryption has two schemes: Digital Signature and Public Key Encryption. There are many schemes base on signcryption.

Currently the standard approach to achieving both message confidentiality and authenticity is signature followed by encryption, namely before a message is sent out, the sender of the message would sign it using a digital signature scheme, and then encrypt the message (and the signature) using a private key encryption algorithm under randomly chosen message encryption key. The random message encryption key would then be encrypted using the recipient's public key. It is called two-step approach "signature-then-encryption" [8].

The computational cost, which includes the computational time involved both in signcryption and unsigncryption, and the communication overhead or added redundant bits, of the scheme is smaller than that required by the best currently known signature- then-encryption scheme [8].

There are many schemes based on signcryption. The figure 5, basic signcryption scheme as following [7]:

Signcryption (m):

For Alice to signcrypt a message

m€{0, 1}n for Bob:

R←r{0, 1}k0

ω←H(m||r)

s←G(ω)+(m||r)

c←f(s|| ω)

Send c to Bob

Unsigncryption:

For Bob to unsigncrypt a cryptogram c from Alice:

$s||\omega \leftarrow f^{-1}(c)$

$m||r \leftarrow G(\omega)+s$

If $H(m||r)= \omega$ accept m

Else reject

Figure5. Basic Signcrption Scheme

A shortened version of Digital Signature Standard is the first of Zheng's signcryption schemes. Signcryption based on SDSS (Shortened Digital Signature Scheme) is expressed in figure 6 as below [9]:

Signcryption

random x(1,…,q-1)

$K=hash\ (y_b x \bmod p)$

generate k1 and k2

$c=Ek1\ (m)$

$r= KH_{K2}(m)$

$s=x/\ (r+x_a) \bmod q$

Send c, r, s to receiver

Unsigncryption

$K=hash\ ((y_a * g^r)^{s.xb} \bmod p$

Split k1 and k2

$m= D_{K1}(c)$

$KH_{K2}\ (m)=r?$

Figure6. Signcryption based on SDSS

5. Digital Envelope Signcryption Scheme

The proposed scheme consists of three portions. The first portion is key generation portion: A probabilistic common parameter generation algorithm. It takes as input a security parameter, and returns all the global information I needed by users of the scheme, such as choice of groups or hash functions. For a probabilistic sender key generation algorithm, $KeyGen_A$ is generated. It takes as input the global information I, and outputs a private/public keypair for sender A (PR_A, PU_A) that is used to send signcrypted messages.

In a probabilistic receiver key generation algorithm, KeyGenB is produced. It takes as input the global information I, and outputs a private/public keypair for recipient B (PR_B, PU_B) that is used to receive signcrypted messages.

The second portion contains signcryption portion: A probabilistic signcryption algorithm. It takes as input the private key of the sender PR_A, the public key of the receiver PU_B, and a message m. It outputs a signcrypttext.

The third portion holds unsigncryption portion: A deterministic unsigncryption algorithm. It takes as input the public key of the sender PU_A, the private key of the receiver PR_B , and a signcrypttext It outputs either a message m or the unique error symbol.

The proposed scheme, figure 7 is described as:

Sender:

K← Key Gen( )

C1←SymE(K,M)

W←Sign (H(C1||K))

$S \leftarrow G(w) \oplus (C1||K)$

$C2 \leftarrow ASymE\ (PU_B,w)$

Send C2||S to recipient B

Receiver:

$W \leftarrow ASymD(PR_B,C2)$

$C1||K \leftarrow G(w)\ S$

If (H(C1||K))==Verify (w))

Accept—>

M←SymD (K,C1)

Figure7. Proposed Digital Envelope Signcryption Scheme

K = key

M=origin message

C = cipher text

PU_B = B's public key

PR_B = B's private key

SymE = symmetric encryption

ASymE = asymmetric encryption

SymD = symmetric decryption

AsymD = asymmetric decryption

H, G = message digest

There are many research and publications separately in digital envelope and signcryption. Today research-trends are not limited in security concern but in time efficiency, low-cost and lightweight computing, embedded and mobile computing. The current innovation is combination of digital envelope and signcryption which can significantly provide speed efficiency and security in lightweight cryptography and mobile devices. Then theoretically analyze security strength and time efficiency of the proposed scheme.

6. Design of Proposed Scheme

The process diagram of proposed signcryption scheme is shown as figure 8. Firstly, it takes session key to encrypt the input message. When getting cipher text C_1, concatenate with previous session key. This concatenation is processed by hash function as message digest. And use digital signature method by using sender's private key to produce W as signed message. The signed message is encrypted through receiver's public key to erect second cipher text C_2. That W is

treated as message digest G again. After that, G is XOR with earlier concatenation. It constructs as S and joins C_2. Finally, sends to recipient.

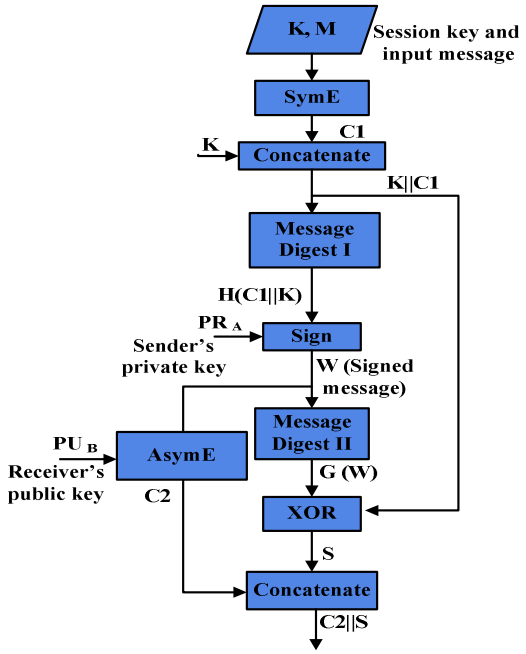

Figure8. The process diagram of proposed signcryption scheme

The process diagram of proposed unsigncryption scheme is demonstrated as figure9. The recipient splits C2 and S, then decrypts with his private key to get W. By hashing, W is manufactured as message digest and XOR amid S. After XOR, getting C1 and K. cipher text and session convert as message digest and compare with W. It can accept or reject depends on verifying. In another part, C1 and K are decrypted to obtain original message again.

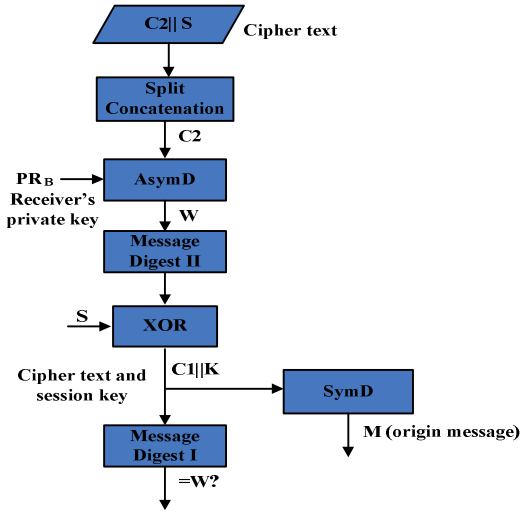

Figure9. The process diagram of proposed unsigncryption scheme

7. Conclusion

The proposed scheme can take advantages of digital envelope scheme and signcryption approach. Digital Envelope Signcryption can provide data confidentiality, data integrity, data authentication, non-repudiation and unforgeability. This approach can be an innovation in lightweight cryptography and mobile devices security area. Experimental result will prove the time efficiency and security strength of proposed scheme comparatively with sign-then-encryption scheme and traditional signcryption scheme.

References

[1] Alexander W. Dent and Royal Holloway, "Hybrid Signcryption Schemes with Insider Security (Extended Abstract)", University of London.

[2] Anirvan Chkraborty, Vishnu Vardhan, Sulaiman Binmalik and Sam Renji, "Introduction to Signcryption", The University of BIRMINGHAM.

[3] D.Sosnoski, "Java Web Services:Axis2 WS-Security Signing and Encryption",2009. [1] Wenbo Mao and John Malone-Lee, "Two Birds One Stone: Signcryption using RSA", HP Laboratories Bristol, 2002.

[4] Faisal Abdul Kadir," RewritingHealer: An approach for securing web service communication", Stockholm, Sweden, 2007.

[5] Lawrence E. Hughes,"Digital Envelopes and Signatures", Windows IT pro, 1996.

[6] R.G.Kammer, "Federal Information Processing Standard Publication", National Institute of Standards and Technology, 2000.

[7] Wenbo Mao and John Malone-Lee, "Two Birds One Stone: Signcryption using RSA", HP Laboratories Bristol, 2002.

[8] Yuliang Zheng, Hideki Imai, "How to construct efficient signcryption schemes on elliptic curves", Monash University, 1998.

[9] Yuliang Zheng, "Signcryption or How to achieve Cost (Signature and Encryption)<< Cost(Signature)+Cost(Encryption)" , Monash, 1999.

[10] Yuliang Zheng, "Signcryption in the Discrete Logarithm Setting", Chapter4, 1998.

[11] Yuliang Zheng,"Signcryption and Its Applications in Efficient Public Key Solutions", Monash University, 1998.

[12] http://en.m.wikipedia.org/wiki/Encryption