An efficient multi recipient signcryption scheme offering non repudiation

Fahad Ahmed
Information Security Dept
College of Telecommunication
Engineering (MCS)
Rawalpindi, Pakistan
fahad.ahmad@mcs.edu.pk

Dr Asif Masood
Computer Science Dept
College of Telecommunication
Engineering (MCS)
Rawalpindi, Pakistan
amasood@mcs.edu.pk

Firdous Kausar
Computer Science Dept
FAST-National University of
Computer and Emerging Sciences
Islamabad, Pakistan
firdous.kausar@nu.edu.pk

Abstract—**Signcryption was first proposed by Zheng and there after several signcryption schemes have been formulated. The broadcast scheme for Zheng does not offer non repudiation using public verification. A latest research by Elkamchouchi et. al proposed a new signcryption scheme for the broadcast environment. The scheme is known as Signcryption Multiple-Recipients Variant (SMRV). From the detail analysis of the scheme, it is observed that confidentiality of the information is lost when the parameters are sent to the third party for verification. Thus the scheme violates the basic property of security. Upon further analysis it is seen that the computational cost of the scheme can be reduced by eliminating few unnecessary steps which do not strengthen the security of the scheme but introduces an extra computational cost. In this paper an efficient and improved signcryption scheme for the broadcast environment is presented. The presented scheme is more efficient than Zheng's and Elkamchouchi et. al scheme in terms of computational cost. The scheme offers non repudiation through public verification and confidentiality of the information is also ensured.**

Keywords; Diffie-Hellman Problem, Discrete Logarithm Problem, Non-repudiation, Public verifiability, Signcryption

I. INTRODUCTION

A traditional approach to guarantee confidentiality, integrity and unforgibility of communications is to digitally sign a message followed by public key encryption. This two step process is referred to as sign-then-encrypt scheme. The cost involved in this approach is the sum of the cost involved in signing the message added with the cost of encrypting it. The sender would sign the message using an already chosen digital signature scheme and then using a private key encryption mechanism the message is encrypted. Using this approach "expanded" bit are added to the message, signature generation and encryption consume machine cycles thus increasing the cost of computation. Likewise at the receiving end, there is almost an equal amount of computation required to decrypt the messages and verify the signatures. A new cryptographic primitive termed as signcryption was first introduced by Zheng [1]. This scheme possessed both the functionalities of the digital signature and that of the encryption schemes. The process of digitally signing a message and then encrypting it is performed in one logical step thus reducing the cost of computation. A comparison of performance and cost involved using Zheng's signcryption scheme compared to well known sign-then-encrypt schemes such as RSA, DSS + Elgamal encryption, Schnorr signature + Elgamal encryption is mentioned in [2]. Generally a typical signcryption scheme having a signcryption algorithm S and an unsigncryption algorithm U should possess the following properties.

Efficiency: The computational and communicational overhead offered by any signcryption scheme should be less than the traditional sign-then-encrypt scheme.

Unique unsigncryptability: A ciphertext "C" obtained after signcrypting a message "m" using the algorithm "S" should be able to unsigncrypt accurately using the algorithm "U".

Security: The signcryption (S) and unsigncryption (U) algorithm both at the same time should meet the security requirements of the digital signatures as well as of encryption. The signcrypted messages designated for the intended receiver should only be read by him/her. An attacker without the knowledge of the receiver`s private key should not be able to decrypt the message. The signcryption scheme should also hold the properties of unforgeability and non repudiation.

Considering a typical wired or a wireless LAN the need for the broadcast information is of vital importance. The security updates, patches or antivirus signatures are pushed mostly from a central server and broadcasted to all the connected users. In case of an organization where different people are working in one group, the need to broadcast information is quite frequent. One property of the broadcast is that all the users receiving the broadcast message from the source should be able recover the correct and consistent information. It should also be ensured that all the users are able to receive the broadcast message and no user is deliberately left off. If this property is not ensured than a compromised server or user can deliberately leave out a user to receive the updates and use the victim for its malicious activities.

Another important aspect is that a user sending a broadcast message can deny its signatures, to cater this issue an efficient mechanism is required that can ensure that the signatures are verified publicly and non repudiation is guaranteed.

To address the issues highlighted above, an Efficient Signcryption Broadcast Scheme (ESBS) is proposed in this paper. The proposed scheme guarantees confidentiality of information with an added feature of ensuring message uniformity.

978-0-7695-4108-2/10 $26.00 © 2010 IEEE
DOI 10.1109/CIT.2010.280

II. RELATED WORK

The signcryption scheme first proposed by Zheng [1] lacked non repudiation using public verification. The later schemes offer this feature but with an additional cost as mentioned in [2][4]. In the scenario where a legitimate user A turns out to behave maliciously and denies its signature, there should be a mechanism to justify the claim. To cater this issue different schemes have been proposed that make use of a third party to publicly verify the claim. A signcryption scheme in [2] offers non repudiation but introduces a cost of two exponential modulo. The drawback of this scheme is that the facility of public verification comes at an increased cost. The cost of signcryption and unsigncryption is greater than the original Zheng's scheme thus reducing the efficiency. It has also been established that this scheme is proven to be insecure when marked on the scale of privacy based on indistinguishability of signcryption [4]. Another scheme proposed in [3] offers non repudiation but the sender's privacy is lost when the third party is involved in case of a dispute. This makes the scheme unsuitable for the implementation. A new scheme has been proposed recently by Elkamchouchi et. al [5] which offers non repudiation using public verification keeping the cost of signcryption and unsigncryption similar to the original Zheng's scheme but introduces a cost of two modular exponentiation for public verification. This scheme is thus better than Zheng's scheme as it offers additional feature of non repudiation and also outperforms than Bao Deng scheme interms of computation required in signcryption and unsigncryption. The broadcast variant of Elkamchouchi et. al scheme loses confidentiality of information when the message m and key K_i is send to the third party for public verification. These two parameters are send in plaintext thus an adversary eavesdropping on the communication path between the trusted third party and the user sending these parameters can capture the key and the message. The computation cost of the scheme can also be reduced by eliminating extra hash functions which only add additional computation and does not add security to the scheme. Also the unsigncryption process and public verification part also requires two modular exponentiations. This cost can also be reduced to increase efficiency.

In this paper the proposed scheme ESBS offers the same feature of public verification using a third party but at a reduced cost. The cost of unsigncryption and public verification is one exponential modulo as compared to two exponential modulo of Elkamchouchi et. al scheme. Instead of taking hash four times in the former scheme, the proposed scheme uses hash function three times thus reducing the cost of computation. The parameters m and K_i are not send in plaintext which ensures the confidentiality of information.

III. PRELIMINARIES

A. Diffie-Hellman Problem (DHP):

Let G be a cyclic group of prime order p and g be a generator of G, the DHP states that given (g, g^a, g^b) for randomly picked $a, b \in \{1, ... , q - 1\}$, there exists no polynomial time algorithm which can find an element $C \in G$ such that $C = g^{ab}$ mod p with non-negligible probability.

B. Discrete Logarithm (DL) Problem:

Let G be a cyclic group of prime order p and g be a generator of G. The DL problem to the base g means the following problem:

Given g, $h \in G$, find an integer x such that $g^{x} = h$.

IV. PROPOSED SCHEME

The proposed scheme assumes that there are N number of recipients $r_1, r_2, r_3, \ldots\ldots r_N$.

The scheme is partitioned into five phases: Pre-requisites setup, key generation phase, signcryption phase, unsigncryption phase, non-repudiation and public verifiability phase. The variables mentioned in the scheme are kept the same as in [5] for better understanding.

A. Pre-requisites setup

The variables, hash functions, encryption/decryption algorithms are all setup in this phase.

TABLE I. VARIABLES/FUNCTIONS DESCRIPTION

Variables/Functions	Description
p	A large prime with length at least 512 bit
q	A large prime factor of p-l
g	An integer in the interval [1,...., p-l] with order q modulo p
Hash(.)	A one-way hash function such as Secure Hash Algorithm-2 (SHA-2) [6] is considered
E(.) and D(.)	A symmetric key encryption/decryption algorithm such as Advanced Encryption Standard (AES) is used[7,8].
X_A & X_i	Private key of user A and i respectively
Y_A & Y_i	Public key of user A and i respectively
Y_{Ai}	Shared key between user A and i_{th} recipient
T	Third party user required for verification

B. Key Generation Phase

The private key for the recipient r_n is a number x_i that is selected at random from the interval [1,……, q-1].
To calculate the public key of the recipient the following calculation will be performed.

$$Y_i \equiv g^{x_i} \bmod p \qquad \text{when } 1 \leq i \leq n \tag{1}$$

At user A: The shared key (y_{Ai}) between the user A and the recipient r_i is computed as:

$$\begin{aligned} y_{Ai} &\equiv y_i^{\,X_A} \bmod p \\ &\equiv (g^{x_i})^{X_A} \bmod p \\ &\equiv g^{x_i\,X_A} \bmod p \end{aligned} \tag{2}$$

At the recipient r_i: The shared key (y_{Ai}) is calculated as follows:

$$\begin{aligned} y_{Ai} &\equiv y_A^{x_i} \bmod p \\ &\equiv (g^{x_A})^{x_i} \bmod p \\ &\equiv g^{x_i x_A} \bmod p \qquad (3) \end{aligned}$$

C. *Signcryption*

Let's suppose a message m is to be transmitted securely and uniformly by user A to n recipients.

(a) A random key k is selected for message encryption.

(b) Calculate: α = Hash (m, k) (4)

(c) Calculate: C = E_k (m, α) (5)

(d) The message encryption key k has to be signcrypted so that the recipients can unsigncrypt and use it to decrypt the messages. The signcrypted ciphertext for k is calculated for n recipients in the following manner.

(a) A random integer x is calculated between the interval [1,……,q-1].

(b) $\gamma \equiv g^x \bmod p$ (6)

(c) $\beta_i \equiv (\gamma \, . \, Y_{Ai}) \bmod p$ (7)

(d) $K_i \equiv$ hash (β_i) (8)

(e) $Z_i = E_{Ki}(k)$ (9)

(f) Hash is calculated using:

$$H_i = \text{hash } (m \,||\, \alpha \,||K_i) \qquad (10)$$

(g) The signature for A is calculated as follows:

$$S = (x - X_A) / \sum_{i=1}^{n} H_i \mod q \qquad (11)$$

The broadcast message to n recipients will contain the following parameters (C, S, $\sum_{i=1}^{n} Z_i$, $\sum_{i=1}^{n} H_i$).

D. *Unsigncryption*

After receiving the broadcast message each recipient will perform the following calculations in order to obtain and verify the message m.

(a) Each recipient will obtain its respective (C, S, Z_i, H_i) from the broadcast message (C, S, $\sum_{i=1}^{n} Z_i$, $\sum_{i=1}^{n} H_i$).

Recipient r_1:	(C, S, Z_1, H_1)
Recipient r_2:	(C, S, Z_2, H_2)
Recipient r_3:	(C, S, Z_3, H_3)
.	.
.	.
.	.
Recipient r_N:	(C, S, Z_N, H_N)

(b) Calculate: $\gamma`$ using the parameters H, S

$$\gamma` \equiv (Y_A \, . \, g^{S. \sum Hi}) \bmod p \qquad (12)$$

Substituting the values of Y_A and S in above equation we get

$$\gamma` \equiv (g^{X_A} \, . \, g^{(x - X_{A)} / Hi \, . \, Hi)}) \bmod p \qquad (13)$$

$$\gamma` \equiv (g^{(X_A + x - X_A)}) \bmod p \qquad (14)$$

$$\gamma` \equiv g^x \bmod p \qquad (15)$$

As from equation 24 we know: $\gamma \equiv g^x \bmod p$
Therefore $\gamma` \equiv \gamma$

(a) $\beta_i` \equiv (\gamma` \, . \, Y_{Ai}) \bmod p$ (16)

(b) $K_i` =$ Hash ($\beta_i`$) (17)

(c) $k` = D_{Ki}` (Z_i)$ (18)

(d) The signcrypted ciphertext C is decrypted using the above calculated key as follows.

$$w = D_{k`}(C) \qquad (19)$$

(e) Split w to obtain message m and hash α

(f) α can be calculated by taking the hash of (m , k`)

(g) H can be computed as Hash(m || α ||K_i`)

(h) The recipient r_i will accept the message m if and only if both:

α = Hash (m, k`)
H = Hash (m || α ||K_i)

V. NON REPUDIATION AND PUBLIC VERIFICATION PHASE FOR ESBS

let's suppose a malicious user A denies the signature of the message m after transmitting. After the decryption and verification is performed by the recipient the false claim of the user A can be publicly verified. Just like the single recipient scheme public verification can be considered in two scenarios. The details of which have been explained earlier in section V.

1) Scenario:

The parameters (C, S, Hi , α , $E_{YZ}(Y_{Ai})$, Z_i , $\sum Hi$) can be send to any trusted third party T to verify that the message really came from user A.
User T will calculate:

$$\gamma` \equiv (Y_A \, . \, g^{S \cdot \sum Hi}) \bmod p$$

Substituting the values of Y_A and S in above equation we get

$$\gamma` \equiv (g^{X_A} \, . \, g^{(x - X_{A)} / Hi \, . \, Hi}) \bmod p$$

$$\gamma` \equiv (g^{(X_A + x - X_A)}) \bmod p$$

$$\gamma` \equiv g^x \bmod p$$

As from eq. 6 we know: $\gamma \equiv g^x \bmod p$
$\gamma` \equiv \gamma$

User T will use its private key to obtain Y_{Ai}

(a) $\beta` \equiv (\gamma` . Y_{Ai}) \bmod p$ (20)

(b) $K_i` = \text{hash}(\beta`)$ (21)

(c) $k` = D_{Ki`}(Z_i)$ (22)

(d) $w` = D_{k`}(C)$ (23)

Now T will split w` to obtain m and α.

(e) Calculate: $\alpha' = \text{Hash}(m, k`)$

(f) Verify if $\alpha' = \alpha$ and $H` = \text{Hash}(m \| \alpha \| K_i)$

The above scheme allows any trusted third party to verify the source of the message. It also helps to ensure that when a message is broadcasted no recipient is deliberately dropped out by an adversary for its malicious activities. A dishonest message originator may deliberately cause the recipient to recover a message different as compared to other recipients. The proposed scheme takes care of this issue in the following ways.

From eq. 4 $\alpha = \text{Hash}(m, k)$
From eq. 5 $C = E_k(m, \alpha)$
This shows that the message m and hash value α both are encrypted together. Since m and k both participate in the development of H_i and S as can be seen from eq. 10 thus the proposed scheme effectively forbids an adversary to deliberately prevent a recipient from being excluded from the group broadcast.

VI. SECURITY ANALYSIS

The key parameter to be considered in the implementation of any scheme is to ensure how secure the scheme is under the different attacks. An adversary will try to obtain the private parameters using the public information. The parameters are classified as:

Public parameters:	(C, H, S, Y_A, Y_N)
Private parameters:	(x, X_A, X_i, Y_{Ai})

A. Attack Scenario 1

Diffie Hellman problem (DHP)

The secret key Y_{Ai} cannot be derived by a malicious user eavesdropping on the communication link between the user A and ith recipient because of Diffie Hellman problem (DHP). The public information H and S cannot help the adversary to infer or calculate any useful information that can reveal the shared key between the communicating party.

B. Attack Scenario 2

Discrete Logarithmic Problem (DLP)

Using the public information an adversary can try different possible combinations of the parameters to obtain secret information but will fail to do so due to well known mathematical problems.

(a) The secret parameter x cannot be derived from the parameters (m, H, S) due to DLP.

(b) The secret key Y_{Ai} cannot be calculated using Y_A, Y_i due to DHP.

C. Attack scenario 3

One way Hash property

(c) From eq. 7 & 8 it can be seen that the secret key Y_{Ai} between the user A and ith user cannot be recovered because of the one way property of hash function.

D. Attack scenario 4

Two Unknown Variables in one Equation

(d) From eq. 11 it can be seen that there are two unknown variables in one equation therefore the secret parameters x and X_A cannot be derived from signature S.

E. Attack scenario 5

From the public parameters transmitted (C, H, S) an adversary may try to forge the signature of the sender. The security of the scheme against such an attack can be compared with Schnorr scheme [11] where the same parameters H and S are considered. The scheme in [11] has been proven to be unforgeable against chosen plaintext attacks so the scheme proposed in this paper is also unforgeable against chosen plaintext attacks.

VII. EFFICIENCY

To mark the efficiency of ESBS the computational and communication cost will be compared with the Zheng's multi recipient scheme [12] and SMRV scheme proposed by Elkamchouchi et. al [5].

A. Computational Cost

The comparison of different schemes can be seen below in the table. The proposed scheme ESBS gives no cost in terms of modular exponentiation as compared to scheme [5] when the message m is transmitted in plaintext and the key is also send for verification. The proposed scheme however takes a cost of one exponential modulo which is less than that of [5] and adds confidentiality to the public verification part which the former scheme does not offer.

TABLE II COST INTERMS OF MODULAR EXPONENTIATION

Scheme	Signcryption Cost	Unsigncryption Cost	Public Verification
Zheng's original scheme	1	2	No
Elkamchouchi et. al scheme	1	2	2
Proposed Scheme	1	1	1

B. Communication Cost

The communication cost is calculated using the parameters that are send as signcrypted bits. For t recipients the communication cost projected by Zheng's scheme is as follows: $[t \, . \, ((|r| + |Z|) + |s|) + |C|]$. The analysis of the

Elkamchouchi et. al scheme shows that the communication cost is [t . (|H| + |Z|) + |S| + |C|].

In this paper, the communication cost for the presented scheme is [t . (|H| + |Z|) + |S| + |C|]. The communication cost appears to be the same as compared to scheme in [5] but in actual, less computations will be performed as only three parameters are required to calculate the hash value H which can be seen from eq. 10.

Thus the presented scheme uses the same parameters (C, S, H, Z) for communication as compared to scheme in [5] but will do so by utilizing less machine cycles. The presented scheme is also more efficient than scheme in [12] which makes it suitable for the broadcast environment.

VIII. CONCLUSION

The research paper projected an efficient signcryption scheme for broadcast offering public verification at a low cost. The security of the proposed scheme is based upon some of the well known mathematical problems such as DLP, DHP and one way hash function. The proposed idea offers additional feature of public verification as compared to Zheng's scheme. The computational cost of one modular exponentiation is required for signcryption step. For unsigncryption and public verification one modular exponentiation is required as compared to two modular exponentiation as in Elkamchouchi et. al scheme. The computational cost is further reduced by using hash function three times instead of four. For calculating hash, three parameters are used in the proposed scheme as compared to five parameters in [5] while keeping the security of the scheme intact. The parameters m and key K_i are not sent in plaintext to ensure the confidentiality of information.

REFERENCES

[1] Yuliang Zheng "Digital Signcryption or How to Acheive Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption)" Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology

[2] F. Bao and R. H. Deng, "A Signcryption Scheme with Signature Directly Verifiable by Public Key", Proceedings ofPublic Key Cryptography 1998, LNCS 1431, pages 55-59, 1998.

[3] J. Baek, R. Steinfeld , and Y. Zheng. "Formal Proofs for the Security of Signcryption", In Public Key Cryptography, volume 2274 of Lecture Notes in Computer Science, pages 80-98. Springer-Verlag, 2002.

[4] J. Malone-Lee, "Signcryption with Non-interactive Non-repudiation", Technical Report CSTR-02-004, Department of Computer Science, University of Bristol, May 2004.

[5] H. M. Elkamchouchi, M. E. Nasr, Roayat Ismail "A New Efficient Publicly Verifiable Signcryption Scheme and Its Multiple Recipients Variant for Firewalls Implementation" 26th NATIONAL RADIO SCIENCE CONFERENCE (NRSC2009) sponsored by IEEE.

[6] National Institute of Science and Technology, "Secure Hash Standard", USA, Federal Information Processing Standard (FIPS) 180-2, Aug. 2002.

[7] J. Daemen and R. Rijmen, "Rijndael: The Advanced Encryption Standard", Dr. Dobb`s Journal, pages 137139, Mar. 2001.

[8] R. Rivest, R. Sidney, "The RC6 Block Cipher", Dr. Dobb`s Journal, pages 160-171, Jan. 1998.

[9] Goh, E.-J. and Jarecki, S., A signature scheme as secure as the Diffie-Hellman problem. In: LNCS, vol. 2656. Springer-Verlag, Berlin. pp. 401-415.

[10] Yuliang Zheng, Hideki Imai "How to construct efficient signcryption schemes on elliptic curves", December 1998 Information Processing Letters, Volume 68 Issue 5.

[11] C. P. Schnorr, "Efficient Signature Generation by Smart Cards", Journal of Cryptology

[12] Yuliang Zheng, "Signcryption and Its applications in Efficient Public Key Solutions ", An invited lecture at the 1997 Information Security Workshop (ISW`97), Lecture Notes in Computer Science, volume 1397, pages 291-312, Springer-Verlag, 1998.