

Cryptanalysis and Improvement of Multi Recipient Signcryption Scheme

Abdul Waheed¹, Arif Iqbal Umar¹, Nizamuddin², Noor Ul Amin¹,
Jawaid Iqbal¹

¹Department of Information Technology Hazara University Mansehra, Pakistan

²Iqra National University Peshawar, Pakistan

Received: January 7, 2016

Accepted: March 22, 2016

ABSTRACT

Due to its cost efficiency signcryption attract cryptographic research community interest. To fulfill the need of secure multicast environment many multicast signcryption scheme has been proposed. Till date, Ahmad et al proposed multi recipient signcryption scheme, is the most cost effective multi receiver scheme. This paper present cryptanalysis of Ahmad et al.'s scheme, analysis shows this scheme do not provide "Confidentiality" the basic property of signcryption. An improved multi receiver signcryption scheme has also been presented.

KEYWORDS—Discrete logarithm Problem; Signcryption; Multi Receiver

I. INTRODUCTION

Signcryption is a cryptographic primitive first proposed by Zheng [2] provide the functionality of digital signature and encryption in a single logical step with low computational cost and communication overhead. Many secure signcryption schemes are proposed to improve the performance and efficiency in public key cryptosystem [3], [4].

In multicast environment a sender communicate with t recipient. Such communication is useful for environment where several people work on combined task and share information amongst. The sender send signcrypted message to multi receiver and the entire receiver should be able to recover relevant information.

The concept of multi receiver signcryption was formalized by Bellare et al [5]. But to improve the efficiency and minimize the cost, many techniques [6], [7] proposed to improve the performance of the multi receiver signcryption.

In this paper we present cryptanalysis of Ahmad et al proposed scheme "An efficient multi recipient signcryption scheme offering non repudiation". Our analysis shows that the scheme does not provide confidentiality. We also proposed an improved multi recipient signcryption scheme, and its analysis has been presented.

The rest of the paper organized as: Section 2: presents formal model of multi recipient signcryption scheme. Section 3: presents review of the Ahmad et al scheme Section 4: presents cryptanalysis of Ahmad et al scheme. Section 5: presents improved version of Ahmad et al scheme. Section 6: presents security analysis of improved scheme. Section 7: presents computational cost and communication overhead of improved scheme and Section 8: comprises the conclusion of the paper.

II. FORMAL MODEL

A generic multi receiver signcryption scheme consists of the following three algorithms: Setup, Signcrypt and Unsigncrypt

Setup: Given a security parameters k , the algorithm generates public/ private key pairs. The public and private key pairs for the sender are X_A, Y_A and for the multicast receivers are X_i, Y_i such that $i \in \{1, \dots, t\}$.

Signcrypt: To send a message m to t receivers whose public keys are Y_i . Signcrypt (m, X_A, Y_A, Y_i, h, E) , to obtain signcrypted text c .

Unsigncrypt: when receiving c each receiver unencrypt (c, X_i, Y_i, h, D) and obtain the plaintext m or the symbol \perp if c is an invalid ciphertext between the sender and t receiver.

III. AHMAD et al.'s SCHEME

This section describe Ahmad et al scheme [1].The propose scheme presume that there is t number of receivers $r_1, r_2, r_3, \dots, r_t$.

Notation guide, used in this paper are provided here for the ease of understanding.

Table 1. Variables Description

Variables	Description
P	A large prime with length at least 512 bit
q	A large prime number
g	An integer in the interval $[1, \dots, p-1]$
h	A one-way hash function
E(.) / D(.)	A symmetric key encryption/decryption
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	Number of Recipient
m	Plaintext
c	Ciphertext
⊥	Rejection
M_{exp}	Modular Exponentiation
M_{Inv}	Modular Inversion

Signcryption

Multi recipient signcryption (m, X_A, Y_A and $\{Y_i \dots Y_i\}, h, E(.)$)

1. Generates $k \in_R \{0, 1, 2, \dots, p\}$
2. Computes $\alpha = \text{hash}(m, k)$
3. Computes $c = E_k(m, \alpha)$
4. Calculates $\gamma = g^{X_A} \bmod p$ and $\beta_i = \gamma \cdot Y_{Ai} \bmod p$
5. Computes $K_i \equiv \text{hash}(\beta_i)$, $z_i = E_{K_i}(k)$ and $h_i = \text{hash}(m || \alpha || K_i)$
6. Calculates $s = (x - X_A) / \sum_{i=1}^t h_i \bmod P$

Multicast ($c, s, \sum_{i=1}^t z_i, \sum_{i=1}^t h_i$) to t recipient

Unsigncryption

Receiving the signcrypted data each user's unsigncrypt to obtain message m and verify it. Each receiver goes through the following steps.

Multi recipient unsigncryption ($c, s, \sum_{i=1}^t z_i, \sum_{i=1}^t h_i, X_i, Y_i, Y_A, h, D(.)$)

1. Computes $\hat{\gamma} = (Y_A \cdot g^{s \cdot \sum_{i=1}^t h_i}) \bmod p$
2. Computes $\hat{\beta}_i = \hat{\gamma} \cdot Y_{Ai} \bmod p$, $\hat{K}_i = \text{hash}(\hat{\beta}_i)$, $\hat{k} = D_{\hat{K}_i}(z_i)$, $\hat{k} = D_{\hat{K}_i}(z_i)$ and $\hat{k} = D_{\hat{K}_i}(z_i)$
3. Computes $m, \alpha = w = D_{\hat{k}_i}(c)$
4. Computes $\alpha = \text{hash}(m, \hat{k})$ and $h = \text{hash}(m || \alpha || K_i)$

Accepted the message if $\alpha = h$ else reject

IV. CRYPTANALYSIS Of AHMAD et al.'s SCHEME

Scheme does not provide confidentiality as: decryption keys K_i and \hat{k} can be computed from public parameters $Y_A, c, s, \sum_{i=1}^t z_i, \sum_{i=1}^t h_i$ as:

1. Computes $\hat{\gamma} = (Y_A \cdot g^{s \cdot \sum_{i=1}^t h_i}) \bmod p$
2. Computes $\hat{\beta}_i = \hat{\gamma} \cdot Y_{Ai} \bmod p$
3. Computes $\hat{K}_i = \text{hash}(\hat{\beta}_i)$
4. Computes $\hat{k} = D_{\hat{K}_i}(z_i)$
5. Computes $w = D_{\hat{k}_i}(c)$

We can get message m from w as:

$$m, \alpha = w$$

This implies that secret parameters keys K_1 and k can be computed from public parameters and message m can be computed from signcrypt text c using keys K_1 and k , so the scheme does not provide confidentiality.

V. IMPROVED MULTI RECIPIENT SIGNCRYPTION SCHEME

Signcryption

User A sends the message m to n recipient uniformly, key (k) is randomly chosen for encryption the message.

In order to signcrypt a message to multi receivers, sender has to accomplish the following

Operations:

1. Generates $K \in_R \{0, 1, 2, \dots, n-1\}$
2. Computes $k_i = (Y_i)^K \bmod p$
3. Computes $\bar{x}_i = (g^{k_1 \oplus k_{i-1} \oplus k_{i+1} \oplus k_t}) \bmod p$
4. Computes $\Omega = (\bar{x}_1, \dots, \bar{x}_t)$
5. Computes $(K_{enc}, K_{hash}) = \text{hash}((\bar{x}_i^{k_i}) \bmod p)$
6. Computes $r = \text{hash}(m || K_{hash})$
7. Computes $s = \frac{K}{(1+rX_A)} \bmod p$
8. Computes $c = K_{enc}(m)$
9. Returns $\omega = (c, r, s, \Omega)$

Sender sends to each recipient the values (c, r, s, Ω) .

Unsigncryption

In order to unsigncrypt a message m from sender, each receiver has to accomplish the following operations.

Multi recipient unsigncryption (ω, d_{Bi}, Y_A)

1. Calculates $k_i = (Y_A * g^r)^{s * X_i}$
2. $(K_{enc}, K_{hash}) = \text{hash}(((\bar{x}_i)^{k_i}) \bmod p)$
3. $c = K_{enc}(m)$
4. $r = \text{hash}(m || K_{hash})$
5. $r' = r$
6. if $r \neq r'$ return \perp , else return m

VI. SECURITY ANALYSIS

This section provides security of the improved scheme.

A. Confidentiality

Our proposed scheme provides confidentiality. If an attacker wants to compute secret parameter $a = (\bar{x}_i^{k_i}) \bmod p$, he/she has to solve an equivalent problem to discrete logarithm problem called strong linear problem given $(g, g^x, g^z \in F_p)$ to find $c_1, c_2 \in F_p$ such $g^{x \cdot c_1} = g^{z \cdot c_2}$. This computation infeasibility claim insures the confidentiality property of proposed scheme.

B. Integrity

Integrity means that the received message is not altered. Our improved scheme provides integrity. One way hash function is used to insure integrity of the message. Receiver compute $r' = \text{hash}(m || K_{hash})$ and check the equality $r' = r$ if holds accept the message otherwise reject.

C. Authentication

Our improved scheme fulfills the property of authenticity. The recipient can authenticate message using the public key of sender Y_A .

D. Unforgeability

Our enhanced scheme provides unforgeability property. For generation of (c, r, s, Ω) private key is required and only legitimate user has that private key.

Table 2. Security comparison of proposed and Ahmed et al scheme

Schemes	Confidentiality	Integrity	Authentication	Unforgeability	Message Verifiability
Ahmed et al [1]	No	Yes	Yes	Yes	No
Proposed	Yes	Yes	Yes	Yes	Yes

VII. COST OF THE IMPROVED SCHEME

A. Computational cost

Our improved multi recipient signcryption scheme may require: 1 modular exponentiation, 1 inverse addition operation, 2 hash function and 1 symmetric encryption operation at the sender's side.

And 1 modular exponentiation, 2 hashing, 1 symmetric decryption at each receiver side.

Time complexity of the different operation are as: M-Exp (modular exponentiation), M-Inv (Modular Inversion), XOR (Bit wise XOR operation), and hash (one way hash function).

To get the cost of different operations simulated under a specific environment (Windows CE, 5.6 OS over 64-bit, Intel(R) Core (TM) i3 CPU M330@ 2.13 GHz processor and 4GB memory). According to simulation results modular exponentiation 63.51 ms, and one way hash operation processing time 14.62 ms for the same security level of 1024 bit RSA algorithm. Furthermore some operations evaluation time is negligible like XOR operation, point addition and string concatenation operation [8].

Table 3. Computational and communication cost comparison

Schemes	Computational Cost							Communication Overhead
	Sender Side				Each Receiver Side			
	M_{exp}	M_{Inv}	h	$E(.)$	M_{exp}	h	$D(.)$	
Proposed	1	1	2	1	1	2	1	$ c_i + h + q $
Ahmed et al[1]	1	1	$2t + 1$	1	1	3	1	$t(c_i + t h) + q $

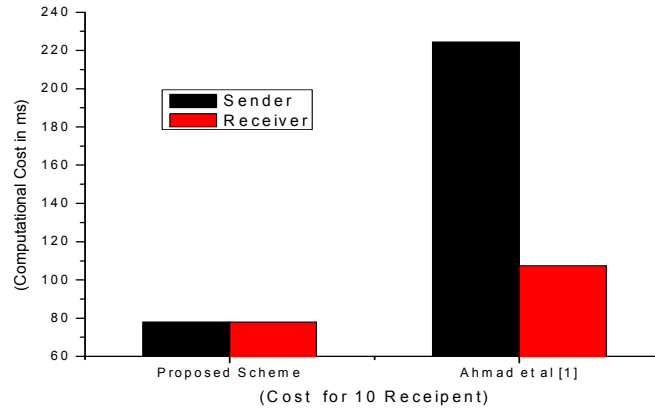


Figure 1. Computational cost comparison for 10 recipients

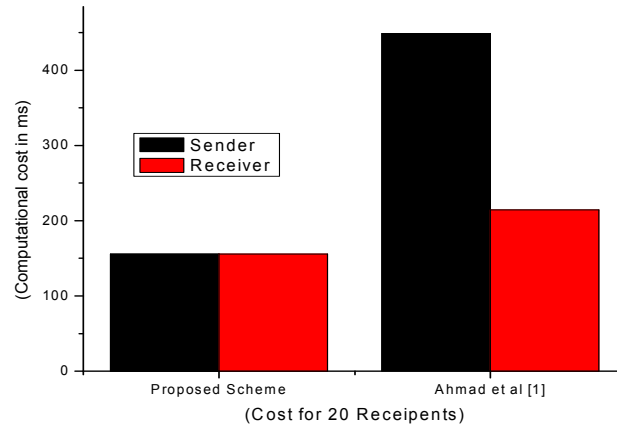


Figure 2. Computational cost comparison for 20 recipients

B. Communication overhead

Communications overhead of the improved multi recipient signcryption scheme are based on these assumptions $|C|+|r|+|s|+|\Omega|$. Communication overhead comparison on the basis of 1, 5 and 10 recipient are shown in figure 3 which shows that our scheme is suitable for resource constraint environment.

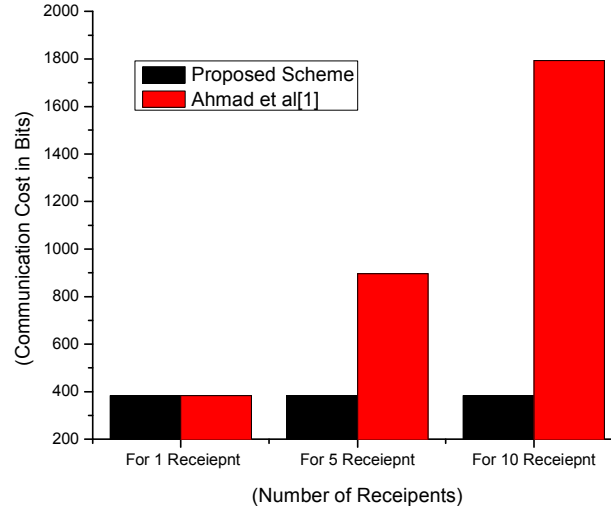


Figure 3. Communication overhead comparison on the basis of 1, 5 and 10 recipient

VIII. CONCLUSION

This paper shows the cryptanalysis of the Ahmad et al scheme that does not provide confidentiality. A polynomial time algorithm is present to compute secure parameter from public parameter.

We also proposed an improved scheme and give the new security model for confidentiality as well as prove the security goals such that confidentiality, integrity, authentication, unforgeability, of the message against possible attacks. Thus our scheme turns out to be the provably secure multi recipient signcryption scheme.

REFERENCES

- [1] F. Ahmed, A. Masood and F. Kausar. "An efficient multi recipient signcryption scheme offering non repudiation," *In 10th IEEE International Conference on Computer and Information Technology*, pp. 1577–1581, 2010.
- [2] Y. Zheng. "Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)," *In Proc. Advances in Cryptology-CRYPTO'97*, LNCS 1294, pp. 165-79, 1997.
- [3] Y. Zheng, H. Imai. "How to construct efficient signcryption schemes on elliptic curves", *Information Processing Letters*, pp. 227-233, 1998.
- [4] J. H. An, Y. Dodis, T. Rabin, "On the security of joint signature and encryption", *Advances in Cryptology-EUROCRYPT 2002*, Springer, pp. 83-107, 2002.
- [5] M. Bellare, A. Boldyreva, S. Micali, "Public-key Encryption in a Multi-User Setting: *Security Proofs and Improvements*", in *Advances in Cryptology-Eurocrypt 2000*, LNCS Vol. 1807, Springer-Verlag, pp. 259-274, 2000.
- [6] K. Kurosawa, "Multi-recipient public-key encryption with shortened ciphertext", *PKC 2002*, LNCS Vol. 2274, pp. 48-63, 2002.
- [7] M. Bellare, A. Boldyreva, J. Staddon, "Randomness reuse in multi-recipient encryption scheme", *PKC 2003*, LNCS Vol. 2567, pp. 85-99, 2003.
- [8] S. A. Ch, Nizamuddin, M. Sher, A. Ghani, H. Naqvi, A. Irshad "An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography," *Multimedia Tools and Applications*, Volume 74, Issue 5, pp 1711-1723, March 2015