Comments on " Multi Recipient Aggregate Signcryption Scheme Based on Elliptic Curve"

Nizamud Din . Abdul Waheed . Nasir Saeed

Abstract Aggregate signcryption combines the functionalities of aggregate signature and encryption. Very recently, Zia & Ali [1] (*Wireless Personal Communications, https://doi.org/10.1007/s11277-020-07637-z*) proposed an elliptic curve cryptography (ECC) based multi-recipient aggregate signcryption scheme. The authors claimed that their scheme is correct, efficient, and secure against known attacks. However, by this comment, we show that their scheme is incorrect and the receiver(s) is unable to unsigncrypt the message.

Keywords: Aggregate signature . Signcryption . ECC . Multicasting . Data authentication

1 Introduction

The concept of the aggregate signature coined by Boneh [2] combines the multiple signatures used for multi-recipient and generates an aggregate signature. Fan et al. [3] first constructed identity-based multi-recipient encryption using Lagrange's interpolating polynomial mechanism to anonymize the receiver's identity. Signcryption [4] combined the two functionalities such as signature and encryption using

Nizamud Din
Department of Computer Science, University of Chitral, Chitral 17200, Pakistan
e-mail: nizam@uoch.edu.pk

Abdul Waheed
Department of Information Technology, Hazara University, Mansehra 21120, Pakistan
e-mail: abdul@netlab.snu.ac.kr

Nasir Saeed
Postdoctoral Fellow, CEMSE Division Building 1, Level 3, Office #3130, King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Saudi Arabia
e-mail: mr.nasir.saeed@ieee.org

a single logical step to attract scarce resource environments. Recently, Zia & Ali proposed elliptic curve-based aggregate signcryption schemes for one-to-one and one-to-many communication environments and claimed that the scheme is correct, efficient, and secure against known attacks. In this comment paper, we evaluated the Zia & Ali scheme. Unfortunately, we found the said scheme is technically incorrect and each of the receivers is unable to unsigncrypt the signcrypted text.

2 Review of Zia & Ali Scheme

For the reader's convenience, we have taken basic terminologies from [1].

2.1 Single-recipient Aggregate Signcryption Scheme

2.1.1 Key Generation

Alice (sender) chooses private key $d_A < n$ randomly, and computes U_A the public key as $U_A = d_A\mathbb{G}$.
Bob (receiver) also chooses private key $d_B < n$ randomly and computes U_B the public key as $U_B = d_B\mathbb{G}$.

2.1.2 Single-recipient Signcryption Phase

Let the sender "*Alice*" would like to transmit a message $\mathcal{M}$ to receiver "*Bob*". The Alice first maps the original message $\mathcal{M}$ into elliptic curve points [5] and then signcrypts the message as following:

1. Verify Bob public key U_B
2. Select a random number $r < n$
3. Computes $\mathcal{R} = r\mathbb{G} = (r_1, r_2)$
4. Computes $A = rU_B = (k, l)$
5. Computes $C = [(d_A\mathcal{R}), (\mathcal{M} + d_A A)]$
6. Computes $C' = [(d_A\mathcal{R}), l(\mathcal{M} + d_A A)] = [(P'_1, P'_2), (P'_3, P'_4)]$
7. Computes $C'' = [((P'_1+k)l, (P'_2+k)l), (P'_3+k)l, (P'_4+k)l)] = [(P_1, P_2), (P_3, P_4)]$
8. Computes $d = \sum_{j=1}^{4} P_j = P_1 + P_2 + P_3 + P_4$
9. Computes $s = \mathbb{H}(d||k)$
10. Forward $(C, \mathcal{R}, s)$ to Bob.

2.1.3 Single-recipient Unsigncryption Phase

Bob receives $(\mathcal{C}, \mathcal{R}, s)$ and verifies the sender (Alice) and collected message authenticity and then unsigncrypt to obtain the message $\mathcal{M}$. Bob use the following steps to perform unsigncryption operation.

1. Verify Alice public key U_A
2. Computes $A = d_B\mathcal{R} = (k, l)$
3. Computes $C = [(d_A\mathcal{R}), l(\mathcal{M} + d_A A)] = [(P'_1, P'_2), (P'_3, P'_4)]$
4. Computes $y = \sum_{j=1}^{4} p'_j = P'_1 + P'_2 + P'_3 + P'_4$
5. Computes $d' = (y + 4k)l$
6. Computes $s' = \mathbb{H}(d'||k)$
7. Compare $s' = s$
8. Computes $C_1 = [(d_B \cdot d_A\mathcal{R}), (\mathcal{M} + d_A A)] = [(d_A A), (\mathcal{M} + d_A A)]$
9. Computes $\mathcal{M} = [\mathcal{M} + d_A A - d_A A)]$

2.1.4 Technical Problem in Single-recipient Scheme

In unsigncryption phase, each of the receivers wants to unsigncrypt the signcrypted message must computes C as $C = [(d_A\mathcal{R}), l(\mathcal{M} + d_A A)]$ using Alice private key d_A and computes C_1as $C_1 = [(d_B \cdot d_A\mathcal{R}), (\mathcal{M} + d_A A)]$ again using Alice private key. As Bob has no access to Alice private key and cannot unsigncrypt the message $\mathcal{M}$. Therefore, Bob fails to unsigncrypt the the signcrypted text $(\mathcal{C}, \mathcal{R}, s)$ and the scheme causes a technical issue.

2.2 Multi recipient Aggregate Signcryption Scheme

2.2.1 Key Generation

Alice (sender) chooses private key $d_A < n$ randomly and computes U_A the public key as $U_A = d_A\mathbb{G}$.
Each receiver also chooses private key $d_i < n$ randomly and computes U_i the public key as $U_i = d_i\mathbb{G}$.

2.2.2 Multi-recipient Signcryption Phase

Let the sender "*Alice*" would like to transmit a message $\mathcal{M}$ to multi-recipient $[r_1, r_2, r_3, \cdots r_N]$. The Alice first maps the original message $\mathcal{M}$ into elliptic curve points [5] and then signcrypts the message as following:

1. Verify each receiver (r_i) public key U_i
2. Select a random number $r < n$

3. Computes $X = rU_A = (k, l)$
4. Computes $A_i = d_A U_i = (k_i, l_i)$
5. Computes the ciphertext $C = [(d_A\mathbb{G}), (\mathcal{M} + kU_A)]$
6. Computes $C' = [(d_A\mathbb{G}), l(\mathcal{M} + kU_A)] = [(P'_1, P'_2), (P'_3, P'_4)]$
7. Computes $C'' = [((P'_1{+}k)l, (P'_2{+}k)l), (P'_3{+}k)l, (P'_4{+}k)l)] = [(P_1, P_2), (P_3, P_4)]$
8. Computes $d = \sum_{j=1}^{t} P_j$
9. Computes $s = \mathbb{H}(d||k)$
10. Computes $z_i = (k_i - r)/l_i \bmod n\mathbb{H}(d||k)$
11. Forward $(C, \mathcal{R}, s)$ to receiver r_i.

2.2.3 Multi-recipient Unsigncryption Phase

Each receiver of a multi-recipient group collects $(C, \mathcal{R}, s)$ and verifies the authenticity of Alice and message (received) and then unsigncrypt to obtain the message $\mathcal{M}$. The unsigncryption operation steps are as the following:

1. Verify first the Alice's public key U_A
2. Computes $A_i = d_i U_A = (k_i, l_i)$
3. Computes $X = (k_i - z_i l_i)U_A = (k, l)$
4. Computes $C' = [(d_A\mathbb{G}), l(\mathcal{M} + kU_A)] = [(P'_1, P'_2), (P'_3, P'_4)]$
5. Computes $y = \sum_{j=1}^{t} p'_j$
6. Computes $d' = (y + kt)l$
7. Computes $s' = \mathbb{H}(d'||k)$
8. Compare $s' = s$
9. Computes $C = [(kU_A)(M + kU_A)]$
10. Computes $\mathcal{M} = (\mathcal{M} + kU_A) - (kU_A)]$

2.2.4 Technical Problem in Multi recipient Scheme

In unsigncryption phase, each of the receivers wants to unsigncrypt the signcrypted message must computes C' as $C' = [(d_A\mathbb{G}), l(\mathcal{M} + kU_A)]$ using Alice's private key d_A. Bob has no access to Alice's private key and cannot unsigncrypt the message $\mathcal{M}$. Therefore, Bob fails to unsigncrypt the signcrypted text $(C, \mathcal{R}, s)$ and the scheme causes a technical issue.

3 Conclusion

This comment paper has analyzed the elliptic curve-based aggregate signcryption scheme presented recently by Zia & Ali. It is found and proved that the said schemes technically incorrect and its required the sender's private key during unsigncrypion phase of both the scheme(s) which is secret and only known to the sender instead of the receiver.

References

1. Zia, M., & Ali, R. (2020). A Multi Recipient Aggregate Signcryption Scheme Based on Elliptic Curve. Wireless Personal Communications, 1-16.
2. Boneh, D., Gentry, C., Lynn, B., & Shacham, H. (2003, May). Aggregate and verifiably encrypted signatures from bilinear maps. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 416-432). Springer, Berlin, Heidelberg.
3. Fan, C. I., Huang, L. Y., & Ho, P. H. (2010). Anonymous multireceiver identity-based encryption. IEEE Transactions on Computers, 59(9), 1239-1249.
4. Zheng, Y. (1997, August). Digital signcryption or how to achieve cost (signature & encryption) $\ll$ cost (signature)+ cost (encryption). In Annual international cryptology conference (pp. 165-179). Springer, Berlin, Heidelberg.
5. Rao, O. S., & Setty, S. P. (2010). Efficient mapping methods for elliptic curve cryptosystems. International Journal of Engineering Science and Technology, 2(8), 3651-3656.