Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/070416

Cryptanalysis of a certificateless aggregate signature scheme for mobile computation

Muhammad Khurram Khan[1,*] *and Debiao He*[2]

[1]Center of Excellence in Information Assurance, King Saud University, Saudi Arabia
[2]School of Mathematics and Statistics, Wuhan University, Wuhan, China

Received: 22 Nov. 2012, Revised: 13 Jan. 2013, Accepted: 10 Feb. 2013
Published online: 1 Jul. 2013

Abstract: Recently, Xiong et al. proposed an efficient certificateless aggregate signature (CLAS) scheme for mobile computation. They demonstrated that their scheme is provably secure in the random oracle model. Unfortunately, by giving a concrete attack, in this paper, we point out that Xiong et al.'s scheme is not secure at all and an adversary without the partial private key and the secret value could forge a legal message. Hence, Xiong et al.'s scheme is not feasible for practical applications.

Keywords: Certificateless cryptography; Aggregate signature; Bilinear pairing

1 Introduction

The aggregate signature (AS) scheme, which was first introduced by Boneh et al. [1], is a variation of the signature scheme. The AS scheme could aggregate n signatures on n distinct messages from n distinct users into a single signature. The AS scheme has been wide used in practical applications since it could reduce bandwidth and storage.

To solve the key escrow problem in the ID-based public key cryptography, Al-Riyami et al. [2] proposed the concept of the certificateless public key cryptography. Since then, many certificateless signature schemes [3,4,5], certificateless key agreement schemes [6,7,8] and certificateless signcryption schemes [9,10] have been proposed. To satisfy applications in certificateless environment, several certificateless aggregate signature (CLAS) schemes [11,12,13,14] also were proposed. Recently, Xiong et al. [15] proposed a new CLAS scheme using bilinear pairings. Compared with previous CLAS schemes [11,12,13,14], Xiong et al.'s scheme is very efficient in terms of computation. They also demonstrated that their scheme is provably secure in the random oracle model. Unfortunately, we find that a general adversary, who knows nothing about the partial private key and the secret value, could forge a legal signature of any message. The analysis shows Xiong et al.'s schemes are not secure for practical applications.

The organization of the paper is sketched as follows. Section 2 gives a brief review of Xiong et al.'s scheme. The security flaw of Xiong et al.'s scheme is shown in Section 3. Finally, we give some conclusions in Section 4.

2 Review of Xiong et al.'s schemes

In this section, we will briefly review Xiong et al.'s CLAS scheme. Their CLAS scheme consists of six algorithms: *MasterKeyGen*, *PartialKeyGen*, *UserKeyGen*, *Sign*, *Aggregate* and *AggregateVerify*. The detail of these algorithms is described as follows:

MasteKeyGen : Given a security parameter , the key generation centre(KGC) runs the algorithm as follows:

–1 Generate a cyclic additive group G_1 and a cyclic multiplicative group G_2 with prime order q.

–2 Generate two generators P, Q of G_1 and an admissible pairing $e : G_1 \times G_1 \rightarrow G_2$.

–3 Generate a random number $s \in Z_q^*$ and compute $P_{pub} = sP$.

–4 Choose cryptographic hash functions $H_0, H_0^{'} : \{0,1\}^* \rightarrow G_1$ and $H_1, H_2, H_2^{'} \{0,1\}^* \rightarrow Z_q$.

[*] Corresponding author e-mail: mkhurram@ksu.edu.sa

–5 KGC publishes the system parameters, which are $\left\{q, G_1, G_2, e, P, Q, P_{pub}, H_0, H_0^{'}, H_1, H_2, H_2^{'}\right\}$ and key the master key s secretly.

PartialKeyGen: Given a user's identity ID_i, KGC computes the user's partial private key $psk_{ID_i} = \left(sQ_{ID_i}, sQ_{ID_i}^{'}\right)$ and transmits it to the user secretly, where $Q_{ID_i} = H_0\left(ID_i\right)$ and $Q_{ID_i} = H_0^{'}\left(ID_i\right)$.

UserKeyGen: The user with identity ID_i selects a random number $x_{ID_i} \in Z_q^*$ as his secret key usk_{ID_i}, and computes his public key as $upk_{ID_i} = usk_{ID_i}$.

Sign: Given a message m_i, the partial private key psk_{ID_i}, the secret key usk_{ID_i}, the user with identity ID_i and the corresponding public key upk_{ID_i} performs the following steps to generate a signature.

1) Compute
$h_{i1} = H_1\left(m_i, ID_i, upk_{ID_i}\right)$,
$h_{i2} = H_2\left(m_i, ID_i, upk_{ID_i}\right)$ and
$h_{i2}^{'} = H_2^{'}\left(m_i, ID_i, upk_{ID_i}\right)$.

2) Compute
$\sigma_i = h_{i1} \cdot uskr_{ID_i} \cdot Q + h_{i2} \cdot sQ_{ID_i} + h_{i2}^{'} \cdot sQ_{ID_i}^{'}$.

3) Output σ_i as the signature on m_i.

Aggregate: For an aggregating set of n users $\{u_1, \ldots, u_n\}$ with identities $\{ID_1, \ldots, ID_n\}$ and the corresponding public keys $\{upk_1, \ldots, upk_n\}$, and message-signature pairs $\{(m_1, \sigma_1), \ldots, (m_n, \sigma_n)\}$ from $\{u_1, \ldots, u_n\}$ respectively, the aggregate signature generator computes $\sigma = \sum_{i=1}^{n} \sigma_i$ and outputs σ as an aggregate signature.

AggregateVerify: To verify an aggregate signature σ signed by n users $\{u_1, \ldots, u_n\}$ with identities $\{ID_1, \ldots, ID_n\}$ and the corresponding public keys $\{upk_1, \ldots, upk_n\}$ on messages $\{m_1, \ldots, m_n\}$, the verifier performs the following steps:

1) Compute
$Q_{ID_i} = H_0\left(ID_i\right)$,
$Q_{ID_i}^{'} = H_0^{'}\left(ID_i\right)$,
$h_{i1} = H_1\left(m_i, ID_i, upk_{ID_i}\right)$,
$h_{i2} = H_2\left(m_i, ID_i, upk_{ID_i}\right)$ and
$h_{i2}^{'} = H_2^{'}\left(m_i, ID_i, upk_{ID_i}\right)$ for $i = 1, \ldots, n$.

2) Verify

$$e\left(\sigma, P\right) = e\left(\sum_{i=1}^{n} h_{i1} \cdot upk_{ID_i}, Q\right) \times e\left(\sum_{i=1}^{n} \left(h_{i2} \cdot Q_{ID_i} + h_{i2}^{'} \cdot Q_{ID_i}^{'}\right), P_{pub}\right)$$

holds or not. If it holds, accept the signature.

3 Cryptanalysis of Xiong et al.'s scheme

Xiong et al. [15] claimed their CLAS scheme is provably secure under the assumption of computational Diffie-Hellman problem [16, 17]. Unfortunately, it is not true, since an adversary A could extract the partial private key and the secret value from the intercepted signatures. Therefore, A could forge a signature of any message using the two private keys. The detail of the attack is described as follows:

Step 1:

For $i = 1, 2, \ldots, n$, A gets $uskr_{ID_i} \cdot Q$, sQ_{ID_i} and $sQ_{ID_i}^{'}$ through the following steps:

A submits ID_i and three messages $m_i, \overline{m}_i$ and $\overline{\overline{m}}_i$ to the *Sign* oracle and gets three legal signatures $\sigma_i, \overline{\sigma}_i$*and* $, \overline{\overline{\sigma}}_i$ of message $m_i, \overline{m}_i$ and $\overline{\overline{m}}_i$ respectively, where

$\sigma_i = h_{i1} \cdot uskr_{ID_i} \cdot Q + h_{i2} \cdot sQ_{ID_i} + h_{i2}^{'} \cdot sQ_{ID_i}^{'}$,

$\overline{\sigma}_i = \overline{h}_{i1} \cdot usk_{ID_i} \cdot Q + \overline{h}_{i2} \cdot sQ_{ID_i} + \overline{h}_{i2}^{'} \cdot sQ_{ID_i}^{'}$,

$\overline{\overline{\sigma}}_i = \overline{\overline{h}}_{i1} \cdot uskr_{ID_i} \cdot Q + \overline{\overline{h}}_{i2} \cdot sQ_{ID_i} + \overline{\overline{h}}_{i2}^{'} \cdot sQ_{ID_i}^{'}$,

$h_{i1} = H_1\left(m_i, ID_i, upk_{ID_i}\right)$,
$h_{i2} = H_2\left(m_i, ID_i, upk_{ID_i}\right)$,
$h_{i2}^{'} = H_2^{'}\left(m_i, ID_i, upk_{ID_i}\right)$,
$\overline{h}_{i1} = H_1\left(\overline{m}_i, ID_i, upk_{ID_i}\right)$,
$\overline{h}_{i2} = H_2\left(\overline{m}_i, ID_i, upk_{ID_i}\right)$,
$\overline{h}_{i2} = H_2^{'}\left(\overline{m}_i, ID_i, upk_{ID_i}\right)$,
$\overline{\overline{h}}_{i1} = H_1\left(\overline{\overline{m}}_i, ID_i, upk_{ID_i}\right)$,
$\overline{\overline{h}}_{i2} = H_2\left(\overline{\overline{m}}_i, ID_i, upk_{ID_i}\right)$
and
$\overline{\overline{h}}_{i2} = H_2^{'}\left(\overline{\overline{m}}_i, ID_i, upk_{ID_i}\right)$.

Then, we could get the following three equations.

$$\sigma_i = h_{i1} \cdot uskr_{ID_i} \cdot Q + h_{i2} \cdot sQ_{ID_i} + h_{i2}^{'} \cdot sQ_{ID_i}^{'} \tag{1}$$

$$\overline{\sigma}_i = \overline{h}_{i1} \cdot usk_{ID_i} \cdot Q + \overline{h}_{i2} \cdot sQ_{ID_i} + \overline{h}_{i2}^{'} \cdot sQ_{ID_i}^{'} \tag{2}$$

and

$$\overline{\overline{\sigma}}_i = \overline{\overline{h}}_{i1} \cdot uskr_{ID_i} \cdot Q + \overline{\overline{h}}_{i2} \cdot sQ_{ID_i} + \overline{\overline{h}}_{i2}^{'} \cdot sQ_{ID_i}^{'} \tag{3}$$

The probability of $\begin{vmatrix} h_{i1} & h_{i2} & h_{i2}^{'} \\ \overline{h}_{i1} & \overline{h}_{i2} & \overline{h}_{i2}^{'} \\ \overline{\overline{h}}_{i1} & \overline{\overline{h}}_{i2} & \overline{\overline{h}}_{i2}^{'} \end{vmatrix} = 0$ is negligible since all the elements of the determinant are random number. So we could get the values of $uskr_{ID_i} \cdot Q, sQ_{ID_i}$ and $sQ_{ID_i}^{'}$ as follows.

$$sQ_{ID_i} = \begin{vmatrix} h_{i1} & \sigma_i & h_{i2}^{'} \\ \overline{h}_{i1} & \overline{\sigma}_i & \overline{h}_{i2}^{'} \\ \overline{\overline{h}}_{i1} & \overline{\overline{\sigma}}_i & \overline{\overline{h}}_{i2}^{'} \end{vmatrix} \Big/ \begin{vmatrix} h_{i1} & h_{i2} & h_{i2}^{'} \\ \overline{h}_{i1} & \overline{h}_{i2} & \overline{h}_{i2}^{'} \\ \overline{\overline{h}}_{i1} & \overline{\overline{h}}_{i2} & \overline{\overline{h}}_{i2}^{'} \end{vmatrix} \tag{4}$$

$$uskr_{ID_i}\cdot Q=\begin{vmatrix}\sigma_i & h_{i2} & h_{i2}^{'}\\ \bar{\sigma}_i & \bar{h}_{i2} & \bar{h}_{i2}^{'}\\ \bar{\bar{\sigma}}_i & \bar{\bar{h}}_{i2} & \bar{\bar{h}}_{i2}^{'}\end{vmatrix}\Big/\begin{vmatrix}h_{i1} & h_{i2} & h_{i2}^{'}\\ \bar{h}_{i1} & \bar{h}_{i2} & \bar{h}_{i2}^{'}\\ \bar{\bar{h}}_{i1} & \bar{\bar{h}}_{i2} & \bar{\bar{h}}_{i2}^{'}\end{vmatrix} \tag{5}$$

$$=\frac{\bar{h}_{i2}\bar{\bar{h}}_{i2}^{'}\cdot\sigma_i+\bar{\bar{h}}_{i2}h_{i2}^{'}\cdot\bar{\sigma}_i+h_{i2}^{'}\bar{h}_{i2}^{'}\cdot\sigma_i-h_{i2}^{'}\bar{\bar{h}}_{i1}\cdot\bar{\bar{\sigma}}_i-h_{i2}^{'}\bar{h}_{i2}\cdot\bar{\bar{\sigma}}_i-h_{i2}\bar{\bar{h}}_{i2}^{'}\cdot\bar{\sigma}_i}{h_{i1}\bar{h}_{i2}\bar{\bar{h}}_{i2}^{'}+\bar{h}_{i1}\bar{\bar{h}}_{i2}h_{i2}^{'}+h_{i2}\bar{h}_{i2}^{'}\bar{\bar{h}}_{i1}-h_{i2}^{'}\bar{h}_{i2}\bar{\bar{h}}_{i1}-\bar{h}_{i2}^{'}\bar{\bar{h}}_{i2}h_{i1}-h_{i2}\bar{h}_{i1}\bar{\bar{h}}_{i2}^{'}}$$

$$=\frac{h_{i1}\bar{\bar{h}}_{i2}^{'}\cdot\bar{\sigma}_i+\bar{h}_{i1}h_{i2}^{'}\cdot\bar{\bar{\sigma}}_i+\bar{h}_{i2}^{'}\bar{\bar{h}}_{i1}\cdot\sigma_i-h_{i2}^{'}\bar{\bar{h}}_{i1}\cdot\bar{\sigma}_i-\bar{h}_{i2}h_{i1}\cdot\bar{\bar{\sigma}}_i-\bar{h}_{i1}\bar{\bar{h}}_{i2}^{'}\cdot\sigma_i}{h_{i1}\bar{h}_{i2}\bar{\bar{h}}_{i2}^{'}+\bar{h}_{i1}\bar{\bar{h}}_{i2}h_{i2}^{'}+h_{i2}\bar{h}_{i2}^{'}\bar{\bar{h}}_{i1}-h_{i2}^{'}\bar{h}_{i2}\bar{\bar{h}}_{i1}-\bar{h}_{i2}^{'}\bar{\bar{h}}_{i2}h_{i1}-h_{i2}\bar{h}_{i1}\bar{\bar{h}}_{i2}^{'}}$$

and

$$sQ_{ID_i}^{'}=\begin{vmatrix}h_{i1} & h_{i2} & \sigma_i\\ \bar{h}_{i1} & \bar{h}_{i2} & \bar{\sigma}_i\\ \bar{\bar{h}}_{i1} & \bar{\bar{h}}_{i2} & \bar{\bar{\sigma}}_i\end{vmatrix}\Big/\begin{vmatrix}h_{i1} & h_{i2} & h_{i2}^{'}\\ \bar{h}_{i1} & \bar{h}_{i2} & \bar{h}_{i2}^{'}\\ \bar{\bar{h}}_{i1} & \bar{\bar{h}}_{i2} & \bar{\bar{h}}_{i2}^{'}\end{vmatrix} \tag{6}$$

$$=\frac{h_{i1}\bar{h}_{i2}\cdot\bar{\bar{\sigma}}_i+\bar{h}_{i1}\bar{\bar{h}}_{i2}\cdot\sigma_i+h_{i2}\bar{\bar{h}}_{i1}\cdot\bar{\sigma}_i-\bar{h}_{i2}\bar{\bar{h}}_{i1}\cdot\sigma_i-\bar{\bar{h}}_{i2}h_{i1}\cdot\bar{\sigma}_i-h_{i2}\bar{h}_{i1}\cdot\bar{\bar{\sigma}}_i}{h_{i1}\bar{h}_{i2}\bar{\bar{h}}_{i2}^{'}+\bar{h}_{i1}\bar{\bar{h}}_{i2}h_{i2}^{'}+h_{i2}\bar{h}_{i2}^{'}\bar{\bar{h}}_{i1}-h_{i2}^{'}\bar{h}_{i2}\bar{\bar{h}}_{i1}-\bar{h}_{i2}^{'}\bar{\bar{h}}_{i2}h_{i1}-h_{i2}\bar{h}_{i1}\bar{\bar{h}}_{i2}^{'}}$$

Step 2 :
For $i=1,2,...,n$ and a given message m_i, A computes
$\widetilde{h}_{i1}=H_1(m_i,ID_i,upk_{ID_i})$,
$\widetilde{h}_{i2}=H_2(m_i,ID_i,upk_{ID_i})$,
$\widetilde{h}_{i2}^{'}=H_2^{'}(m_i,ID_i,upk_{ID_i})$, and
$\sigma_i=\widetilde{h}_{i1}\cdot uskr_{ID_i}\cdot Q+\widetilde{h}_{i2}\cdot sQ_{ID_i}+\widetilde{h}_{i2}^{'}\cdot sQ_{ID_i}^{'}$,
where $uskr_{ID_i}\cdot Q, sQ_{ID_i}$ and $sQ_{ID_i}^{'}$ are the values computed in the above step.

Step 3 : A computes
$\sigma=\sum\limits_{i=1}^{n}\sigma_i$ and outputs σ as the aggregate signature.

Since
$\widetilde{h}_{i1}=H_1(m_i,ID_i,upk_{ID_i})$,
$\widetilde{h}_{i2}=H_2(m_i,ID_i,upk_{ID_i})$,
$\widetilde{h}_{i2}^{'}=H_2^{'}(m_i,ID_i,upk_{ID_i})$
and
$\sigma_i=\widetilde{h}_{i1}\cdot uskr_{ID_i}\cdot Q+$
$\widetilde{h}_{i2}\cdot sQ_{ID_i}+\widetilde{h}_{i2}^{'}\cdot sQ_{ID_i}^{'}$, we could have that

$$\begin{aligned}&e(\widetilde{\sigma},P)=e\left(\sum_{i=1}^{n}\sigma_i,P\right)\\&=e\left(\textstyle\sum_{i=1}^{n}\left(\widetilde{h}_{i1}\cdot usk_{ID_i}\cdot Q+\widetilde{h}_{i2}\cdot sQ_{ID_i}+\widetilde{h}'_{i2}\cdot sQ'_{ID_i}\right),P\right)\\&=e\left(\sum_{i=1}^{n}\widetilde{h}_{i1}\cdot usk_{ID_i}\cdot Q,P\right)e\left(\sum_{i=1}^{n}\left(\widetilde{h}_{i2}\cdot sQ_{ID_i}+\widetilde{h}'_{i2}\cdot sQ'_{ID_i}\right),P\right)\\&=e\left(\sum_{i=1}^{n}\widetilde{h}_{i1}.upk_{ID_i}.Q\right)e\left(\sum_{i=1}^{n}\left(\widetilde{h}_{i2}.Q_{ID_i}+\widetilde{h}'_{i2}\cdot Q'_{ID_i}\right),P_{pub}\right)\end{aligned}\tag{7}$$

Therefore, σ is a legal aggregate signature and Xiong et al.'s CLAS scheme is not secure.

4 Conclusion

In this paper, we show a very efficient CLAS scheme is not secure by proposing a concrete attack. The analysis shows that the scheme is insecure and infeasible for practical applications. We will propose an improved scheme to overcome the security weakness.

References

[1] D. Boneh, C. Gentry, B. Lynn, H. Shacham, Aggregate and verifiably encrypted signatures from bilinear maps, in: EUROCRYPT03, LNCS 3027 pp. 416432 (2003).
[2] S.S. Al-Riyami, K. Paterson, Certificateless Public Key Cryptography. in AsiaCrypt 2003, LNCS 2894, pp. 452-473, (2003).
[3] He D, Chen J, Zhang R. An efficient and provably-secure certificateless signature scheme without bilinear pairings. International Journal of Communication Systems 2011. DOI: 10.1002/dac.1330.
[4] Tian M, Huang L, Cryptanalysis of a certificateless signature scheme without pairings, International Journal of Communication Systems 2012. DOI: 10.1002/dac.2310.
[5] Tsai J, Lo N, Wu T, Weaknesses and improvements of an efficient certificateless signature scheme without using bilinear pairings, International Journal of Communication Systems 2012. DOI: 10.1002/dac.2388.

[6] He D, Chen Y, Chen J, Zhang R, A new two-round certificateless authenticated key agreement protocol without bilinear pairings, Mathematical and Computer Modelling **54** (11-12) pp. 31433152 (2011).

[7] He D, Chen J, Hu J, A pairing-free certificateless authenticated key agreement protocol, International Journal of Communication Systems, **25**(2) pp. 221-230 (2012).

[8] He D, Padhye S, Chen J, An efficient certificateless authenticated key agreement protocol, Computers & Mathematics with Applications 2012; DOI: 10.1016/j.camwa.2012.03.044.

[9] Zhu H, Li H, Wang Y, Certificateless Signcryption Scheme Without Pairing, Journal of Computer Research and Development **47**(9) pp. 1587-1594 (2010).

[10] Liu W, Xu C, Certificateless Signcryption Scheme Without Bilinear Pairing, Journal of Software **22**(8) pp. 1918-1926 (2011).

[11] R. Castro, R. Dahab, Efficient Certificateless Signatures Suitable for Aggregation, Cryptology ePrint Archive, Available online: http://eprint.iacr.org/2007/454.

[12] Z. Gong, Y. Long, X. Hong, K. Chen, Two certificateless aggregate signatures from bilinear maps, in: IEEE SNPD 2007, vol. **3**, pp. 188-193, (2007).

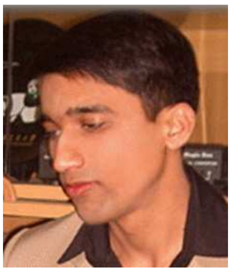
[13] L. Zhang, B. Qin, Q. Wu, F. Zhang, Efficient many-to-one authentication with certificateless aggregate signatures, Computer Networks, **54**(14), pp. 2482-2491, (2010).

[14] L. Zhang, F. Zhang, A new certificateless aggregate signature scheme, Computer Communications, **32**(6), pp. 1079-1085, (2009).

[15] H. Xiong, Q. Wu, Z. Chen. Strong Security Enabled Certificateless Aggregate Signatures Applicable to Mobile Computation. 2011 Third International Conference on Intelligent Networking and Collaborative Systems, IEEE Computer Society, Washington, pp. 92-99, (2011).

[16] M. Khurram Khan, D. He, “A New Dynamic Identity based Authentication Protocol for Multi-server Environment using Elliptic Curve Cryptography”, Security and Communication Networks, vol. **5**, Issue 11, pp. 1260-1266 (2012).

[17] M. Khurram Khan, Jiashu Zhang, “Improving the Security of ’A Flexible Biometrics Remote User Authentication Scheme”, Computer Standards and Interfaces, vol. **29**, issue 1, pp. 84-87 (2007).



Muhammad Khurram Khan is currently an Associate Professor with the Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia. He has edited seven books and proceedings published by Springer-Verlag and IEEE. He has published more than 150 papers in international journals and conferences and he is an inventor of 7 U.S./PCT patents in the information security field. Dr. Khurram is a Founding Editor of the Bahria University Journal of Information and Communication Technology. He is on the editorial boards of several International SCI journals, including the Journal of Network and Computer Applications (Elsevier), the Journal of Security and Communication Networks (Wiley), Telecommunication Systems (Springer), Computers and Electrical Engineering (Elsevier), Electronic Commerce Research (Springer), journal of Computing & Informatics, the Journal of Information Hiding and Multimedia Signal Processing (JIHMSP), and the International Journal of Biometrics (Inderscience). Dr. Khurram is one of the organizing chairs of several top-class international conferences and he is also on the program committee of dozens of conferences. He is a recipient of several national and international awards for his research contributions. In addition, he has been granted several national and international funding projects in the field of information security. His current research interests include biometrics, multimedia security, and digital authentication.

Debiao He received his Ph.D. degree in applied mathematics from School of Mathematics and Statistics, Wuhan University in 2009. He is currently a lecturer of Wuhan University. His main research interests include cryptography and information security, in particular, cryptographic protocols.