IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 19 December 2023, accepted 4 January 2024, date of publication 12 January 2024, date of current version 26 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3353609

COMMENTS AND CORRECTIONS

Comments on "A Conditional Privacy-Preserving Certificateless Aggregate Signature Scheme in the Standard Model for VANETs"

JE HONG PARK AND BONWOOK KOO
The Affiliated Institute of ETRI, Daejeon 34044, Republic of Korea

Corresponding author: Je Hong Park (jhpark@nsr.re.kr)

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) Grant funded by the Korean Government [Ministry of Science and ICT (MSIT)] (Development of next-generation cryptosystem to improve security and usability of national information system) under Grant 2021-0-00046.

ABSTRACT In the above paper "A Conditional Privacy-Preserving Certificateless Aggregate Signature Scheme in the Standard Model for VANETs," a pairing-based certificateless aggregate signature (CLAS) scheme was proposed. However, a malicious-but-passive KGC attack on this scheme was subsequently presented by Shim. In this paper, we show that even if the CLAS scheme is modified to prevent malicious-but-passive KGC attacks by incorporating Shim's countermeasure, there are still weaknesses that allow an adversary to forge aggregate or individual signatures.

INDEX TERMS Aggregate signature scheme, signature, certificateless public key cryptography, cryptanalysis.

I. INTRODUCTION

As a way to resolve key management problems while effectively authenticating multiple vehicles in VANETs, the use of certificateless aggregate signature (CLAS) schemes is being explored. In CLAS schemes, a user private key is composed of values generated independently by the third-party key generation center (KGC) and the owner, and the corresponding public key is determined by these user private key components. A signature aggregation function allows n individual signatures on n different messages from n different users to combine all of these signatures into a single signature. The validity of an aggregate signature will convince any verifier that the n users signed the n original messages. Such signature aggregation is useful for reducing bandwidth and storage and is particularly attractive for mobile devices in VANETs.

Recently, Wang et al. proposed a pairing-based CLAS scheme [1]. However, Shim subsequently presented a malicious-but-passive KGC attack on this CLAS scheme [3]. This attack allows a malicious KGC to create individual signatures of a user by modifying a system parameter at will. Shim also provided a countermeasure to prevent her attack.

In this paper, we show that two attacks are possible against Wang et al.'s CLAS scheme applying Shim's countermeasure. These attacks allow anyone to create aggregate signatures without the participation of other users, or to create individual signatures by impersonating other users. It is easy to see that these weaknesses are inherent in the original CLAS scheme, regardless of Shim's countermeasure.

II. REVIEW OF WANG et al.'s CLAS SCHEME

A. MATHEMATICAL NOTATIONS AND DEFINITIONS

Let λ denote the security parameter. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of some large prime order q. And let $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$ denote the quotient ring of integers modulo q and let $\mathbb{Z}_q^*$ denote the multiplicative group of $\mathbb{Z}_q$. We write $\mathbb{G}_1$ additively and $\mathbb{G}_2$ multiplicatively. Then $[k]P$ denotes $(k-1)$ times addition of $P \in \mathbb{G}_1$ and g^k denotes $(k-1)$ times multiplication of $g \in \mathbb{G}_2$, respectively.

A pairing is a map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ with the following properties.

- Bilinearity: $\hat{e}([a]P, [b]Q) = \hat{e}(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_q$.
- Non-degeneracy: There exist $P, Q \in \mathbb{G}_1$ such that $\hat{e}(P, Q) \neq 1_{\mathbb{G}_2}$, where Let $1_{\mathbb{G}_2}$ is the identity of $\mathbb{G}_2$.
- Computability: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for all $P, Q \in \mathbb{G}_1$.

Note that $\hat{e}$ is symmetric ($\hat{e}(P, Q) = \hat{e}(Q, P)$ for all $P, Q \in \mathbb{G}_1$) since $\hat{e}$ is bilinear and $\mathbb{G}_1$ is a cyclic group.

Let $\{0, 1\}^*$ denote the set of all finite-length binary strings (including the empty string ϵ), let $[1..m]$ denote the set $\{i \in \mathbb{Z} \mid 1 \leq i \leq m\}$, and let $\{a_i\}_{i=1}^n$ denote a tuple $(a_1, \ldots, a_n)$.

B. SCHEME DESCRIPTION

Here we describe the CLAS scheme of Wang et al. [1]. This scheme is used as a building block for a conditional privacy-preserving authentication protocol for VANETs. Therefore, the pseudonym generation algorithm is incorporated into the plain CLAS scheme and time parameters are used to thwart replay attacks. However, since we are interested in the security of the plain CLAS scheme itself, we omit the pseudonym generation algorithm and the time parameters and assume that each user has a real identity ID.

- Setup: The KGC generates parameters as follows:
  - generates groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order $q > 2^\lambda$ with a pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$.
  - chooses cryptographic hash functions $H_0 : \mathbb{G}_1 \to \mathbb{G}_1$ and $H_1, H_2 : \{0, 1\}^* \to \mathbb{Z}_q^*$.
  - randomly selects $P, P' \in \mathbb{G}_1$ and $s \in \mathbb{Z}_q^*$, and sets $P_{\text{pub}} \leftarrow [s]P$ and $Q \leftarrow H_0(P')$.
  - broadcasts the public parameters $params = \{\mathbb{G}_1, \mathbb{G}_2, q, \hat{e}, P, Q, P_{\text{pub}}, H_0, H_1, H_2\}$, and keeps the master private key $msk = s$ secret.

  We assume $params$ to be an input to all subsequent algorithms.
- Partial Private Key Generation: For a user with $ID \in \{0, 1\}^*$, KGC randomly selects $r \in \mathbb{Z}_q^*$, computes $R \leftarrow [r]P$, $h_1 \leftarrow H_1(ID, R)$ and $d \leftarrow r + h_1 \cdot msk$, then sends d to the user via a secure channel.
- Public/Private Key Generation: The user with ID randomly selects $x \in \mathbb{Z}_n^*$ and computes $X \leftarrow [x]P$. Then sets $pk = (R, X)$ as a public key and $sk = (d, x)$ as a private key.
- Individual Signature Generation: For a message $m \in \{0, 1\}^*$, the signer with ID performs the following steps:
  - randomly selects $u \in \mathbb{Z}_q^*$, and computes
  $$U \leftarrow [u]P \quad \text{and} \quad V \leftarrow [u]Q.$$
  - computes $h_2 \leftarrow H_2(m, ID, U, V, pk)$ and
  $$W \leftarrow [d + h_2 \cdot x]Q + V.$$
  - outputs $\sigma = (U, V, W)$ as a signature on m.
- Individual Signature Verification: For a given signature $\sigma (= (U, V, W))$ on a message m under $(ID, pk(= (R, X))$, a verifier performs as following:
  - computes $h_1 \leftarrow H_1(ID, R)$ and $h_2 \leftarrow H_2(m, ID, U, V, pk)$.
  - checks
  $$\hat{e}(W, P) \stackrel{?}{=} \hat{e}\big(R + [h_1]P_{\text{pub}} + [h_2]X + U, Q\big). \quad (1)$$
  Then accepts σ if Eq. (1) holds, otherwise rejects it.
- Aggregate: Given a tuple of individual signatures $\{\sigma_i\}_{i=1}^n$ on messages $\{m_i\}_{i=1}^n$ under $\{(ID_i, pk_i)\}_{i=1}^n$, anyone computes $W \leftarrow \sum_{i=1}^n W_i$, and outputs an aggregate signature
  $$\sigma = (\{U_i\}_{i=1}^n, \{V_i\}_{i=1}^n, W).$$
- Aggregate Signature Verification: Given an aggregate signature $\sigma = (\{U_i\}_{i=1}^n, \{V_i\}_{i=1}^n, W)$ on messages $\{m_i\}_{i=1}^n$ under $\{(ID_i, pk_i(= (R_i, X_i))\}_{i=1}^n$, a verifier performs as follows:
  - for each $i \in [1..n]$, computes $h_{1i} \leftarrow H_1(ID_i, R_i)$ and $h_{2i} \leftarrow H_2(m_i, ID_i, U_i, V_i, pk_i)$.
  - checks
  $$\hat{e}(W, P) \stackrel{?}{=} \hat{e}\Big(\sum_{i=1}^n R_i + \sum_{i=1}^n [h_{1i}]P_{\text{pub}} + \sum_{i=1}^n [h_{2i}]X_i + \sum_{i=1}^n U_i, Q\Big). \quad (2)$$
  Then accepts σ if Eq. (2) holds, otherwise rejects it.

Apart from the simplified description, this CLAS scheme has been modified from the original version by adapting Shim's countermeasure [3] against malicious-but-passive KGC attacks. The attack in [3] allows a malicious KGC to forge individual signatures by generating Q as $[\alpha]P$ for some $\alpha \in \mathbb{Z}_q^*$ instead of generating it randomly. To prevent this attack, Shim suggested using a hash function to break the algebraic relation between P and Q, and we have included this (see the Setup algorithm).

We also fix a technical error in the original Individual Signature Generation and Aggregate algorithms. Note that each component of an individual signature is generated as follows in the original Individual Signature Generation algorithm.

$$U \leftarrow [u]P, \ V \leftarrow [u]Q, \ h_2 \leftarrow H_2(m, ID, U, V, W, pk),$$
$$W \leftarrow [d + h_2 \cdot x]Q + V.$$

Here we see that the input to H_2 contains W, and the result, h_2, is used to compute W again. To resolve this contradiction, we omit W from the input to H_2. To obtain h_{2i} in the aggregate signature verification phase, it is necessary to include the components U_i and V_i of all individual signatures σ_i in the aggregate signature σ, as already pointed out in [3]. On the other hand, unlike [3], it is sufficient to include only $\sum_{i=1}^n W_i$ in σ, which is a return to the original version.

III. CRYPTANALYSIS

Although the CLAS scheme described in Section II is secure against malicious-but-passive KGC attacks, we show in this section that it still has weaknesses. In particular, we show that it is possible to forge aggregate signatures and even individual signatures.

A. AGGREGATE SIGNATURE FORGERY ATTACK

Let $\mathcal{A}$ be an adversary trying to forge an aggregate signature on a tuple of messages $\{m_i\}_{i=1}^n$. Without loss of generality,

assume that $\mathcal{A}$ has the identity ID_n, $pk_n = (X_n, R_n)$, and $sk_n = (x_n, d_n)$. As a preparatory step, $\mathcal{A}$ collects public information of other $(n-1)$ users $\{(ID_i, pk_i)\}_{i=1}^{n-1}$. Here, each public key $pk_i = (R_i, X_i)$ is assumed to be valid. Then $\mathcal{A}$ performs the following procedure:

1) randomly selects $u_i \in \mathbb{Z}_q^*$ and $V_i \in \mathbb{G}_1 \backslash \{\mathcal{O}\}$, and computes $U_i \leftarrow [u_i]P$ and $h_{2i} \leftarrow H_2(m_i, ID_i, U_i, V_i, pk_i)$ for each $i \in [1..(n-1)]$.
2) computes $h_{1i} \leftarrow H_1(ID_i, R_i)$ for each $i \in [1..n]$.
3) randomly selects $u_n \in \mathbb{Z}_q^*$, and computes

$$U_n \leftarrow [u_n]P - \sum_{i=1}^{n-1}\Big(U_i + \big(R_i + [h_{1i}]P_{\text{pub}}\big) + [h_{2i}]X_i\Big).$$

4) randomly selects $V_n \in \mathbb{G}_1 \backslash \{\mathcal{O}\}$, and computes $h_{2n} \leftarrow H_2(m_n, ID_n, U_n, V_n, pk_n)$ and

$$W \leftarrow [u_n + d_n + h_{2n} \cdot x_n]Q.$$

5) outputs $\sigma \leftarrow \big(\{U_i\}_{i=1}^n, \{V_i\}_{i=1}^n, W\big)$ as a signature on $\{m_i\}_{i=1}^n$ under $\{(ID_i, pk_i)\}_{i=1}^n$.

Since

$$\begin{aligned}[u_n]P &= U_n + \sum_{i=1}^{n-1}\Big(U_i + \big(R_i + [h_{1i}]P_{\text{pub}}\big) + [h_{2i}]X_i\Big)\\ &= \sum_{i=1}^{n} U_i + \sum_{i=1}^{n-1}\Big(\big(R_i + [h_{1i}]P_{\text{pub}}\big) + [h_{2i}]X_i\Big)\end{aligned}$$

and

$$[d_n + h_{2n} \cdot x_n]P = R_n + [h_{1n}]P_{\text{pub}} + [h_{2n}]X_n,$$

any verifier confirms that

$$\begin{aligned}\hat{e}(W, P) &= \hat{e}\big([u_n + d_n + h_{2n} \cdot x_n]Q, P\big)\\ &= \hat{e}\big(Q, [u_n + d_n + h_{2n} \cdot x_n]P\big)\\ &= \hat{e}\big(Q, [u_n]P + [d_n + h_{2n} \cdot x_n]P\big)\\ &= \hat{e}\Big(Q, \sum_{i=1}^{n}\Big(U_i + \big(R_i + [h_{1i}]P_{\text{pub}}\big) + [h_{2i}]X_i\Big)\Big).\end{aligned}$$

As a result, we show that anyone can create valid aggregate signatures without the contribution of other users.

In the above attack procedure, $\mathcal{A}$ randomly selects components $V_1, \ldots, V_n$ of all individual signatures. This shows that component V has no role in the individual signature. Looking at the Individual Signature Generation algorithm, although both U and V are generated as the commitments of $u \in \mathbb{Z}_n^*$, only U is used in the verification phase because

$$W = [d + h_2 \cdot x]Q + V = [u + d + h_2 \cdot x]Q, \quad \text{and}$$
$$\hat{e}(W, P) = \hat{e}(Q, [u + d + h_2 \cdot x]P).$$

The reason this attack is possible is that the hash value h_2 combining the message and the random commitment U in an individual signature does not depend on the random commitment of other signatures. Therefore, a signer can manipulate its random commitment to remove the verification equation terms of other individual signatures from Eq. (2).

B. INDIVIDUAL SIGNATURE FORGERY ATTACK

Let $\mathcal{A}$ be an adversary trying to forge an individual signature on a message m by impersonating a user with ID. Then $\mathcal{A}$ performs the following procedure:

1) randomly selects $u, x \in \mathbb{Z}_q^*$ and $R \in \mathbb{G}_1 \backslash \{\mathcal{O}\}$, and sets $U \leftarrow [u]P - (R + [h_1]P_{\text{pub}})$ where $h_1 = H_1(ID, R)$.
2) randomly selects $V \in \mathbb{G}_1 \backslash \{\mathcal{O}\}$, and computes $h_2 \leftarrow H_2(m, ID, U, V, pk)$ and $W \leftarrow [u + h_2 \cdot x]Q$.
3) outputs $\sigma \leftarrow (U, V, W)$ as a signature on m under (ID, pk) where $pk = (R, X(= [x]P))$.

Since

$$\begin{aligned}\hat{e}(W, P) &= \hat{e}\big([u + h_2 \cdot x]Q, P\big)\\ &= \hat{e}\big(Q, [u + h_2 \cdot x]P\big)\\ &= \hat{e}\big(Q, [u]P + [h_2]X\big)\\ &= \hat{e}\big(Q, U + (R + [h_1]P_{\text{pub}}) + [h_2]X\big),\end{aligned}$$

any verifier accepts σ as a valid signature on m under $(ID, (R, X))$.

This attack implies that anyone can create valid individual signatures without the partial private key d.

The reason this attack is possible is that the random secret value u and the partial private key d are linearly combined. Therefore, a signer can manipulate its random commitment to remove the term related to the partial private key from Eq. (1).

IV. CONCLUSION

In this paper, we show that Wang et al.'s CLAS scheme and its revised scheme applying Shim's countermeasure are weak against forgery attacks. Since Wang et al.'s scheme can be seen as a simple conversion of a pairing-free CLAS scheme [2], we believe that other secure pairing-free CLAS schemes can be used to improve this scheme.

REFERENCES

[1] H. Wang, L. Wang, K. Zhang, J. Li, and Y. Luo, "A conditional privacy-preserving certificateless aggregate signature scheme in the standard model for VANETs," *IEEE Access*, vol. 10, pp. 15605–15618, 2022, doi: 10.1109/ACCESS.2022.3147595.
[2] S. Liu, Y. Liu, W. Liu, and Y. Zhang, "A certificateless multi-dimensional data aggregation scheme for smart grid," *J. Syst. Archit.*, vol. 140, Jul. 2023, Art. no. 102890, doi: 10.1016/J.SYSARC.2023.102890.
[3] K.-A. Shim, "Security analysis of conditional privacy-preserving authentication schemes for VANETs," *IEEE Access*, vol. 11, pp. 33956–33963, 2023, doi: 10.1109/ACCESS.2023.3263738.