Hindawi
Security and Communication Networks
Volume 2020, Article ID 6183861, 8 pages
https://doi.org/10.1155/2020/6183861

Research Article

Cryptanalysis and Improvement of a Group Authentication Scheme with Multiple Trials and Multiple Authentications

Zhe Xia,[1,2] **Yining Liu**,[3] **Ching-Fang Hsu**,[4] **and Chin-Chen Chang**[5,6]

[1]*School of Computer Science, Wuhan University of Technology, Wuhan 430071, China*
[2]*Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China*
[3]*School of Computer and Information Security, Guilin University of Electronic Technology, Guilin 541004, China*
[4]*Computer School, Central China Normal University, Wuhan 430079, China*
[5]*Department of Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan*
[6]*School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou 310018, China*

Correspondence should be addressed to Zhe Xia; xiazhe@whut.edu.cn

Received 27 November 2019; Revised 1 April 2020; Accepted 11 June 2020; Published 13 July 2020

Academic Editor: Leandros Maglaras

Authentication is one of the most fundamental services in cryptography and information security. Compared with the traditional authentication methods, group authentication allows a group of users to be authenticated at once rather than authenticating each of these users individually. Therefore, it is more desirable in the group oriented environment, such as multicast/conference communications. In this paper, we first demonstrate that a recent group authentication scheme by Chien (Security and Communication Networks, 2017) suffers some security flaws, i.e. an adversary in the asynchronous communication model can pretend to be a legitimate group member without being detected. We then use the Anonymous Veto Networks (AV-net) to patch Chien's scheme, so that its security can be rigorously proved in a well-defined security model.

1. Introduction

Authentication confirms whether some entity is who or what it claims to be. It is an important security service in cryptography and information security. Traditionally, the authentication process is carried out between two parties. The prover proves its identity to the verifier using a single or some combination of the following methods: something it has, something it knows, or something it is. The verifier will accept the proof if the prover, indeed, possesses the credential. However, this one-to-one authentication approach is inefficient in the group oriented environment, e.g., multicast/conference communications and broadroom elections [1, 2]. If each user needs to authenticate every user's identity, a large number of authentication operations (quadratic to the number of users) need to be performed across the entire group. To address this problem, group authentication [3] has been proposed recently, so that instead of authenticating each user individually, all users in the group can be authenticated at once. If all users are legitimate group members, the group authentication is sufficient to prove that they all belong to the same group. Even if there exist some nonmembers, the group authentication still can be used as a preprocessing step before applying some traditional authentication techniques to identify those nonmembers.

In general, a group authentication scheme consists of two phases. In the *initialization phase*, the group manager (GM) generates a credential for each group member, and these credentials are sent through some secure networks. In the *authentication phase,* each player uses her credential to compute a token and broadcasts it. As follows, every user can use the revealed information to verify whether all these users are belonging to the same group. Two security requirements are fundamental for group authentication schemes. One is that if all users are legitimate group members, the authentication will always be successful. The other is that any nonmember with no valid credential cannot pretend to be a

group member without being detected. Moreover, two other requirements are also highly desirable for group authentication schemes: (1) reuse of the credentials in multiple authentication sessions; (2) allowance of players to broadcast their tokens through asynchronous networks. Note that the first requirement helps to avoid the cumbersome processes of distributing credentials for every authentication session, and the asynchronous networks are easier to be established than the synchronous ones, especially in the distributed environment.

1.1. Our Contributions. In his work [4], Chien has proposed a group authentication scheme, claiming to satisfy the abovementioned requirements. In this paper, we first demonstrate that Chien's scheme fails to achieve its claimed security in the asynchronous networks. In particular, an adversary in the asynchronous communication model can always wait until the other legitimate users having revealed their tokens and then fabricate a valid token using the revealed ones. We then use a novel technique, called *Anonymous Veto Networks* (AV-net), to patch Chien's scheme. To avoid the "design-break-patch loop," our proposed scheme is rigorously analyzed in a well-defined security model [5].

1.2. Organization of the Paper. The rest of the paper is organized as follows. In Section 2, we briefly review some related works in the literature. Chien's scheme is described and analyzed in Section 3. In Section 4, we outline some preliminaries, including notations, building blocks, and security models. In Section 5, we introduce our improvement of Chien's scheme and analyze it with respect to security and efficiency. Finally, we conclude in Section 6.

2. Related Works

After the concept being initially introduced by Harn [3], group authentication has been widely accepted as a useful tool in cryptography to simultaneously prove that a group of users are all legitimate members [6]. Recently, a number of group authentication schemes have been proposed in the literature. For example, Chien [4] used a different mathematical structure to renovate Harn's scheme, with the purpose of allowing the credentials to be used in multiple trials in asynchronous networks. Liu et al. [7] considered the resource restrained environment and proposed a lightweight group authentication scheme in which the authentication is executed by checking whether the interpolation of the credentials returns a polynomial with the expected degree. Mahalle et al. [8] used the threshold Paillier cipher to design a group authentication scheme for the Internet of Things. Li et al. [9] extended the functionalities of group authentication so that not only the group members can be authenticated at once but also pairwise keys can be established among the group members. Guo et al. [10] and Elmouaatamid et al. [11] independently explored how to further trace the nonmembers if the group authentication fails.

However, a common drawback of these existing works is that their security is only justified using heuristic arguments rather than formal security proofs, and several of these schemes have already been found to contain security flaws. For example, Ahmadian and Jamshidpour [12] showed that Harn's scheme is insecure because an adversary in the asynchronous networks can impersonate a group member without being detected. In paper [3], Harn simply conjectured that the adversary needs to reconstruct all the polynomials to fabricate a valid token. But, this adversary may use a very novel method, called the linear subspace attack, to fabricate a valid token without recovering any of the polynomials. In their work [5], Xia et al. proposed a formal security model for group authentication that captures the main security requirements. This work has also improved Harn's scheme so that the modified scheme can be rigorously proved to achieve the desirable security properties.

In this paper, we first demonstrate that Chien's scheme is also insecure in the asynchronous networks. We then propose an improvement of Chien's scheme and prove its security using the security model in paper [5].

3. Analysis of Chien's Scheme

3.1. Description. Note that our description here is slightly different from Chien's original scheme [4]. We use a symmetric bilinear map in order to simplify the description, while Chien uses an asymmetric bilinear map. It is well known that compared with the symmetric bilinear map, the asymmetric one has advantages in security and bandwidth, but our attack against Chien's scheme also works when an asymmetric bilinear map is used instead.

We denote G_1 and G_2 as two finite cyclic groups of order q for some large prime q. A bilinear map $\hat{e}$: $G_1 \times G_1 \longrightarrow G_2$ is defined between these two groups, satisfying the following properties:

(i) Bilinear: the map $\hat{e}$: $G_1 \times G_1 \longrightarrow G_2$ is said to be bilinear if $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $P, Q \in G_1$ and all $a, b \in \mathbb{Z}_q$

(ii) Nondegenerate: the map $\hat{e}$ does not send all pairs in $G_1 \times G_1$ to the identity in G_2

(iii) Computable: there exists an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in G_1$

Chien's multiple group authentication scheme works as follows:

(i) Init: GM first selects two finite cyclic groups G_1 and G_2 with prime order q and a bilinear map $\hat{e}$: $G_1 \times G_1 \longrightarrow G_2$. Denote P as a generator of G_1. GM then selects a secret $R_i \leftarrow_R \mathbb{Z}_q$ and sets $Q = sP$. GM selects l values $R_i \leftarrow_R G_1$ for $i \in \mathbb{Z}_l$. GM associates the pairwise different integers $\{w_1, w_2, \ldots, w_n\}$ with the group members. Finally, GM outputs the system parameters $params = (G_1, G_2, \hat{e}, q, P, Q, \{R_i\}_{i \in \mathbb{Z}_l}, \{w_i\}_{i \in \mathbb{Z}_n})$.

(ii) Dist: GM selects a random polynomial $f(x) = a_0 + a_1 x + \cdots + a_{t-1}x^{t-1}$ over $\mathbb{Z}_q$ with degree $t-1$, such that $a_0 = s$. GM, then computes the credentials $s_i = f(w_i)$, and sends them to the group members through the secure channel.

(iii) Comp: in the σ-th session ($\sigma\epsilon\{1, 2, \ldots, l\}$), every participating user in $\Omega(|\Omega| \geq t)$ computes her token $c_i = (s_i\mathscr{L}_i)R_\sigma$ and broadcasts it, where $\mathscr{L}_i = \prod_{j\varepsilon\Omega, j\neq i} w_j/(w_j - w_i)$ is the Lagrange coefficient.

(iv) Auth: in the σ-th session, every user can verify whether all the users are legitimate group members by checking:

$$\widehat{e}\left(\sum_{t\in\Omega} c_i, P\right) = \widehat{e}(R_\sigma, Q). \tag{1}$$

Note that if all players are legitimate group members, we have $\sum_{t\in\Omega} c_i = sR_\sigma$. Also, thanks to the bilinear property, this further implies that the abovementioned equation holds. But, if there exist some nonmembers, the relation $\sum_{t\in\Omega} c_i = sR_\sigma$ can only satisfy with negligible probability. Therefore, the abovementioned equation can be used to check whether a group authentication is successful.

3.2. Analysis. Now, we demonstrate that, in the asynchronous communication model, an adversary $\mathscr{A}$ who has no valid credential can pretend to be a legitimate group member without being detected. Without loss of generality, suppose that $\mathscr{A}$ attends the σ-th group authentication session together with t legitimate group members $\{U_1, U_2, \ldots, U_t\}$ and $\mathscr{A}$ would like to impersonate the group member U_{t+1}. The attack works as follows:

(i) Each legitimate group member U_i computes and broadcasts her token $c_i = (s_i\mathscr{L}_i)R_\sigma$, where $\mathscr{L}_i = \prod_{j=1, j\neq t+1}^{t+1} w_j/(w_j - w_i)$ is the Lagrange coefficient.

(ii) After receiving these tokens, $\mathscr{A}$ modifies them as $c_i' = c_i \cdot (\mathscr{L}_i)^{-1} = s_i R_\sigma$ for $i\varepsilon\{1, 2, \ldots, t\}$ and interpolates $s_{t+1}R_\sigma = \sum_{i=1}^{t} c_i'\mathscr{L}_i'(w_{t+1})$, where

$$\mathscr{L}_i'(w_{t+1}) = \prod_{j=1, j\neq i}^{t} \frac{w_{t+1} - w_j}{w_i - w_j}. \tag{2}$$

(i) Finally, $\mathscr{A}$ computes the token $c_{t+1} = (s_{t+1}\mathscr{L}_{t+1})R_\sigma$, where $\mathscr{L}_{t+1} = \prod_{j=1, j\neq t+1}^{t+1} w_j/(w_j - w_{t+1})$, and broadcasts c_{t+1}.

At this time, the group authentication will be successful because $\sum_{i=1}^{t+1} c_i = sR_\sigma$. The consequence is that the adversary $\mathscr{A}$ has impersonated the group member U_{t+1} without being detected. The main reason for this attack is that since the Lagrange coefficients can be publicly computed, $\mathscr{A}$ can remove them from the revealed tokens and then uses the modified tokens to interpolate a new valid token. To solve this problem, we need to disable $\mathscr{A}$'s ability of removing the Lagrange coefficients from the revealed tokens.

4. Preliminaries

4.1. Notations. We assume that all players are probabilistic polynomial time (PPT) algorithms with respect to the security parameter λ. Standard notations are used for probabilistic algorithms and experiments. For example, if A is a probabilistic algorithm, then $A(x_1, x_2, \ldots)$ denotes the result of running A on inputs x_1, x_2, and so on. We denote $y \leftarrow A(x_1, x_2, \ldots)$ as the experiment of assigning y as $A(x_1, x_2, \ldots)$. If S is a finite set, then we denote $x \leftarrow_R S$ as the operation of picking an element uniformly from S. Moreover, $\Pr[x \leftarrow S; y \leftarrow T; \cdots : p(x, y, \ldots)]$ denotes the probability that the predicate $p(x, y, \ldots)$ will be true after the ordered execution of the algorithms $x \leftarrow S$; $y \leftarrow T$, and so on. A function $\varepsilon(k)$: $\mathbb{N} \longrightarrow \mathbb{R}^+$ is called negligible if for all $c > 0$, there exists a k_0 such that $\varepsilon(k) < (1/k^c)$ for all $k > k_0$.

4.2. Building Blocks. Shamir secret sharing [13]: it shares the secret value $s\varepsilon\mathbb{Z}_q$ among n users, so that any t or more users can work together to recover the secret, but less than t users cannot get any information of the secret. In the sharing phase, the dealer first selects a random polynomial $f(x) = a_0 + a_1 x + \cdots + a_{t-1}x^{t-1}$ over $\mathbb{Z}_q$ with degree $t-1$, where $a_0 = s$. Then, the dealer computes the shares $s_i = f(w_i)$ and sends them to each user through the secure channel. Here, $\{w_1, w_2, \ldots, w_n\}$ are public parameters associated with the users that are pairwise different. In the reconstruction phase, any subset Ω (where $|\Omega| \geq t$) of these users can reconstruct the secret s by Lagrange interpolation: $s = \sum_{i\in\Omega} s_i\mathscr{L}_i$, where $\mathscr{L}_i = \prod_{j\varepsilon\Omega, j\neq i} w_j/(w_j - w_i)$ is called the Lagrange coefficient.

Anonymous veto networks (AV-nets) [14]: they assume that there exist broadcast channels, and all the messages are exchanged through these channels. Suppose n users are involved, and then the protocol works as follows:

(i) Round 1: each user U_i selects a value $x_i \leftarrow_R \mathbb{Z}_q$ and broadcasts g^{x_i}. U_i also proves that she has the knowledge of x_i without revealing it, e.g., using the Schnorr identification technique [15]. When this round finishes, every user computes $g^{y_i} = \prod_{j=1}^{i-1} g^{x_j} / \prod_{j=i+1}^{n} g^{x_j}$.

(ii) Round 2: every user broadcasts a value $g^{x_i y_i}$ and proves the knowledge of x_i within $g^{x_i y_i}$ without revealing it. Now, we have

$$\prod_{i=1}^{n} g^{x_i y_i} = 1. \tag{3}$$

To see that the abovementioned property always holds, by definition, $y_i = \sum_{j<i} x_j - \sum_{j>i} x_j$; hence, we have

$$\begin{aligned}\sum_i x_i y_i &= \sum_i \sum_{j<i} x_i y_j - \sum_i \sum_{j>i} x_i y_j, \\ &= \sum \sum_{j<i} x_i y_j - \sum \sum_{i<j} x_i y_j, \\ &= \sum \sum_{j<i} x_i y_j - \sum \sum_{j<i} x_j y_i, \\ &= 0.\end{aligned} \tag{4}$$

4.3. Security model. We adapt the models and definitions in paper [5] and prove our proposed scheme using this security model.

The participants: there are four types of participants in group authentication schemes:

(i) Group manager (GM): the GM initializes the protocol and generates credentials for the users. In any authentication protocol, the user needs to possess some secret that is unknown to the others.

(ii) Users: each of the n users will receive a credential from the GM, and they will use their credentials to participate in the group authentication.

(iii) Inside adversary: the inside adversary $\mathscr{A}_I$ controls at most $t-1$ users, where t is the threshold such that $t > n/2$. $\mathscr{A}_I$ can obtain these users' internal states. $\mathscr{A}_I$'s purpose is to learn some secret information or to pass the group authentication by herself.

(iv) Outside adversary: the outside adversary $\mathscr{A}_O$ does not own any valid credential generated by the GM, but her purpose is to impersonate a group member in the group authentication without being detected.

Communication model: we assume that there exists a secure channel between the GM and every user, so that the credentials can be distributed securely. Moreover, we assume that every participant is connected to a broadcast channel, where any message sent through this channel can be heard by the other participants within some specified time bound. Note that the broadcast channel is only assumed to be asynchronous, such that messages sent from the uncorrupted users to the corrupted ones can be delivered relatively fast, the case in which the adversary can wait for the messages of the uncorrupted users to arrive, then decide on her computation and communication, and still get her messages delivered to the honest users on time. In comparison, all the users need to send their messages simultaneously in the synchronous networks. Therefore, adversaries in an asynchronous network are more powerful as they could obtain more information to assist their attacks.

System model: the group authentication scheme is specified by the following four randomized algorithms: *Init*, *Dist*, *Comp*, and *Auth*.

(i) The initialization algorithm *Init* is run by the GM. *Init* takes as inputs the security parameter λ; it outputs the system parameters *params*.

(ii) The distribution algorithm *Dist* is run by the GM. *Dist* takes as inputs the system parameters *params* and the number of users n; it outputs a set of credentials $\{s_1, s_2, \ldots, s_n\}$. These credentials are sent to U through the secure channel, where U denotes the set of all legitimate group members.

(iii) The computation algorithm *Comp* is run by every user. *Comp* takes as inputs the system parameters *params*, the session index σ, the set of participated users Ω, and a credential s_i; it outputs a token c_i through the broadcast channel.

(iv) The group authentication algorithm *Auth* is run by the participated users. *Auth* takes as inputs the system parameters *params*, the session index σ and a set of tokens $\{c_i\}_{i\varepsilon\Omega}$; it outputs 1 if $|\Omega| \geq t$ and Ω only contains legitimate group members, and it outputs 0 otherwise.

Security Model: the following security properties are considered in the security model.

Definition 1 (correctness). If a set Ω ($|\Omega| \geq t$) of users are participating in the group authentication and they are all legitimate group members, then the group authentication will be successful. Formally, a group authentication scheme is said to have the correctness property if we have

$$\begin{aligned}&\Pr[params \longleftarrow Init(\lambda); \{s_i\}_{i\varepsilon\Omega} \longleftarrow "Dist("params, n"); " \\ &c_i \longleftarrow Comp(params, \sigma, \Omega, s_i)|_{i\varepsilon\Omega}; \\ &"Auth("params, \sigma, \{c_i\}_{i\varepsilon\Omega}") = 1"] = 1.\end{aligned} \tag{5}$$

In the abovementioned expression, $\Omega \subseteq U$ and $|\Omega| \geq t$.

Definition 2 (secrecy). The inside adversary $\mathscr{A}_I$ cannot learn any secret information in the group authentication process. Formally, a group authentication scheme is said to have the secrecy property if we have

$$View_{\mathscr{A}_I}\left(\text{Real}_{\prod}(\lambda, params)\right) \cong_c View_{\mathscr{A}_I}(SIM_S(\lambda, params)). \tag{6}$$

In the abovementioned expression, $View_{\mathscr{A}_I}(\text{Real}_{\prod}(\lambda, params))$ is denoted as $\mathscr{A}_I$'s view in the real run of the protocol $\prod$, $\cong_c$ means computationally indistinguishable, and $View_{\mathscr{A}_I}(SIM_S(\lambda, params))$ is denoted as $\mathscr{A}_I$'s view of the transcripts simulated by a PPT simulator S with only public information as inputs.

Definition 3 (no forgery). The inside adversary $\mathscr{A}_I$ cannot pass the group authentication by herself. Formally, a group authentication scheme is said to have the no forgery property if we have

$$\Pr\Big[params \longleftarrow Init(\lambda); \{s_i\}_{i\in U} \longleftarrow "Dist("params, n"); "$$
$$T \longleftarrow \mathscr{A}_I^O\big(params, \sigma, \Omega, \{s_i\}_{i\in U_{\mathscr{A}}}\big);$$
$$"\sigma \notin " \sum \wedge "Auth("params, \sigma, T") = 1"\Big] < \varepsilon(\lambda). \tag{7}$$

In the abovementioned expression, $U_{\mathscr{A}}$ denotes the users that are controlled by $\mathscr{A}_I$, such that $U_{\mathscr{A}} \subset U$ and $|U_{\mathscr{A}}| \le t-1$. Ω denotes an oracle that is used to query the group authentication service, and Σ records all the session indexes which have been queried.

Definition 4 (no impersonation). The outside adversary $\mathscr{A}_O$ cannot impersonate a group member without being detected. Formally, a group authentication scheme is said to have the no impersonation property if we have

$$\Pr\Big[params \longleftarrow Init(\lambda); \{s_i\}_{i\in U} \longleftarrow "Dist("params, n"); "$$
$$c_i \longleftarrow Comp(params, \sigma, \Omega \cup \{\mu\}, s_i)\big|_{i\in\Omega};$$
$$c_\mu \longleftarrow \mathscr{A}_O(params, \sigma, \Omega \cup \{\mu\}, [\![\{c_i\}]\!]_{i\in\Omega};$$
$$"Auth\Big("params, \sigma, [\![\{c_i\}]\!]_{i\in\Omega\cup\{\mu\}}"\Big) = 1"\Big] < \varepsilon(\lambda). \tag{8}$$

In the abovementioned expression, $\mathscr{A}_O$ is assumed to impersonate the user U_μ, where $\mu \notin \Omega$.

Computational assumptions: we assume that the following assumptions hold against any PPT algorithm.

Definition 5 (discrete logarithm (DL) assumption). The description of the finite cyclic group G is given, where $|G| \ge q$ and g is a generator of G. The discrete logarithm assumption implies that there exists a negligible function $\varepsilon(\cdot)$ such that for all PPT adversaries $\mathscr{A}_{DL}$, we have

$$\Pr\big[x \leftarrow_R \mathbb{Z}_q; x^* \leftarrow \mathscr{A}_{DL}(G, q, g, g^x): x^* = x\big] < \varepsilon(\lambda). \tag{9}$$

Definition 6 (computational Diffie–Hellman (CDH) assumption). The description of the finite cyclic group G given, where $|G| \ge q$ and g is a generator of G. The computational Diffie–Hellman assumption implies that there exists a negligible function $\varepsilon(\cdot)$ such that for all PPT adversaries $\mathscr{A}_{CDH}$, we have $\Pr[x \leftarrow_R \mathbb{Z}_q; y \leftarrow_R \mathbb{Z}_q; R \leftarrow \mathscr{A}_{CDH}(G, q, g, g^x, g^y): R = g^{xy}] < \varepsilon(\lambda)$.

5. An Improvement of Chien's Scheme

5.1. The Proposed Scheme. The improved multiple group authentication scheme in the asynchronous communication model works as follows:

(i) Init: GM first selects two finite cyclic groups G_1 and G_2 with prime order q, and a bilinear map $\hat{e}: G_1 \times G_1 \longrightarrow G_2$. P is denoted as a generator of G_1. GM then selects a secret $s \leftarrow_R \mathbb{Z}_q$ and sets $Q = sP$. GM selects l values $R_i \leftarrow_R G_1$ for $i \in \mathbb{Z}_l$. GM associates the pairwise different integers $\{w_1, w_2, \ldots, w_n\}$ with the group members. Finally, GM outputs the system parameters $params = (G_1, G_2, \hat{e}, q, P, Q, \{R_i\}_{i\in\mathbb{Z}_l}, \{w_i\}_{i\in\mathbb{Z}_n})$.

(ii) Dist.: GM selects a random polynomial $f(x) = a_0 + a_1 x + \cdots + a_{t-1}x^{t-1}$ over $\mathbb{Z}_q$ with degree $t-1$, such that $a_0 = s$. GM, then computes the credentials $s_i = f(w_i)$, and sends them to the group members through the secure channel.

(iii) Comp: in the σ-th session, every participating user in Ω first selects $u_i \leftarrow_R \mathbb{Z}_q$ and broadcasts $u_i R_\sigma$. Then, each user computes $v_i R_\sigma = \sum_{j\in\Omega, j<i} u_j R_\sigma - \sum_{j\in\Omega, j>i} u_j R_\sigma$. As follows, every user computes and broadcasts her token as

$$c_i = (s_i \mathscr{L}_i) R_\sigma + u_i v_i R_\sigma, \tag{10}$$

where $\mathscr{L}_i = \prod_{j\in\Omega, j\ne i} w_j/(w_j - w_i)$ is the Lagrange coefficient.

(iv) Auth: In the σ-th session, every user can verify whether all the users are legitimate group members by checking:

$$\hat{e}\left(\sum_{i\in\Omega} c_i, P\right) = \hat{e}(R_\sigma, Q). \tag{11}$$

5.2. Security Analysis

Theorem 1. *Our modified group authentication scheme satisfies the correctness property.*

Proof. If $\Omega \subseteq U$ and $|\Omega| \ge t$, the Lagrange interpolation implies that $s = \sum_{i\in\Omega} s_i \mathscr{L}_i$, where $\mathscr{L}_i = \prod_{j\in\Omega, j\ne i} w_j/(w_j - w_i)$ is the Lagrange coefficient. Moreover, because the AV-nets have the property that $\sum_{i\in\Omega} u_i v_i R_\sigma = 0$, we have

$$\begin{aligned}\sum_{i\in\Omega} c_i &= \sum_{i\in\Omega} (s_i \mathscr{L}_i) R_\sigma + \sum_{i\in\Omega} (u_i v_i) R_\sigma, \\ &= \left(\sum_{i\in\Omega} s_i \mathscr{L}_i\right) R_\sigma, \\ &= sR_\sigma.\end{aligned} \tag{12}$$

Therefore, the equation $\hat{e}(\sum_{t\in\Omega} c_i, P) = \hat{e}(R_\sigma, Q)$ will hold, and the authentication will be successful. □

Theorem 2. *Our modified group authentication scheme satisfies the secrecy property, assuming that the DL problem holds in* G_1.

Proof. We denote $Real_{\prod}(\lambda, params)$ as the real run of the protocol $\prod$ and $SIM_S(\lambda, params)$ as the protocol simulated by a PPT simulator S with only public information as inputs.

$Real_{\prod}(\lambda, params)$:

(i) Init: GM generates and outputs the system parameters $params = (G_1, G_2, \hat{e}, q, P, Q, \{R_i\}_{i\in\mathbb{Z}_l}, \{w_i\}_{i\in\mathbb{Z}_n})$.

(ii) Dist: GM computes the credentials $s_i = f(w_i)$ and sends them to the group members through the secret channel. Without loss of generality, we assume that the credentials $\{s_1, s_2, \ldots, s_{t-1}\}$ are learnt by the inside adversary $\mathscr{A}_I$.

(iii) Comp: in the σ-th session, every participating user in Ω selects $u_i \leftarrow_R \mathbb{Z}_q$ and broadcasts $u_i R_\sigma$. Then, each user computes $v_i R_\sigma = \sum_{j\in\Omega, j<i} u_j R_\sigma - \sum_{j\in\Omega, j>i} u_j R_\sigma$ and broadcasts her token as $c_i = (s_i \mathscr{L}_i) R_\sigma + u_i v_i R_\sigma$. In this step, $\mathscr{A}_I$ learns $\{u_1, u_2, \ldots, u_{t-1}\}$ which are possessed by the corrupted users and all the broadcast values.

(iv) Auth: in the σ-th session, everyone verifies whether $\hat{e}(\sum_{i\in\Omega} c_i, P) = \hat{e}(R_\sigma, Q)$.

$SIM_S(\lambda, params)$:

(i) Init: the simulator S outputs the system parameters $params = (G_1, G_2, \hat{e}, q, P, Q, \{R_i\}_{i\in\mathbb{Z}_l}, \{w_i\}_{i\in\mathbb{Z}_n})$.

(ii) Dist: S sends the credentials $\{s_1, s_2, \ldots, s_{t-1}\}$ to the inside adversary $\mathscr{A}_I$.

(iii) Comp: We denote $k = |\Omega|$. In the σ-th session, S randomly selects k values $\{u_1', u_2', \ldots, u_k'\}$ from $\mathbb{Z}_q$ and broadcasts $u_i' R_\sigma$ for $i \in \{1, 2, \ldots, k\}$. S sends $\{u_1', u_2', \ldots, u_{t-1}'\}$ to $\mathscr{A}_I$. S, then, randomly selects $k-1$ values $\{c_1', c_2', \ldots, c_{k-1}'\}$ from G_1 and computes $c_k' = \sum_{i\in\Omega} c_i - \sum_{i=1}^{k-1} c_i'$. Then, S broadcasts the tokens $\{c_1', c_2', \ldots, c_k'\}$.

(iv) Auth: in the σ-th session, everyone verifies whether $\hat{e}(\sum_{i\in\Omega} c_i', P) = \hat{e}(R_\sigma, Q)$.

We now prove that it is infeasible for the inside adversary $\mathscr{A}_I$ to distinguish these two protocols. In the *Init* algorithm, the same public parameters *params* are published in both protocols. In the *Dist* algorithm, the same credentials $\{s_1, s_2, \ldots, s_{t-1}\}$ are learnt by $\mathscr{A}_I$ in both protocols. In the *Comp* algorithm, both sets $\{u_1, u_2, \ldots, u_{t-1}\}$ and $\{u_1', u_2', \ldots, u_{t-1}'\}$ are randomly distributed in $\mathbb{Z}_q$, and all the broadcast values are randomly distributed in G_1. In *Auth*, the algorithm will be successful in both protocols. Therefore, $\mathscr{A}_I$ cannot distinguish between $Real_{\prod}(\lambda, params)$ and $SIM_S(\lambda, params)$ because all these algorithms in $\mathscr{A}_I$'s view are indistinguishable. In other words, we have

$$View_{\mathscr{A}_I}\left(Real_{\prod}(\lambda, params)\right) \cong_c View_{\mathscr{A}_I}\left(SIM_S(\lambda, params)\right). \tag{13}$$

Moreover, based on the DL assumption, $\mathscr{A}_I$ cannot learn any secret information of s from the public information $Q = sP$ or $\sum_{i\in\Omega} c_i = sR_\sigma$. Hence, our modified scheme satisfies the secrecy property. □

Theorem 3. *Our modified group authentication scheme satisfies the no forgery property, assuming that the CDH problem holds in* G_1.

Proof. We denote X as the event that $\mathscr{A}_I$ can predict the value sR_σ from the public parameters *params* and Y as the event that $\mathscr{A}_I$ has learnt some secret information through querying the oracle Ω. We denote F as the event that $\mathscr{A}_I$ outputs a successful forgery. Then, we have

$$\begin{aligned}\Pr[F] &= \Pr[F|X\vee Y]\cdot\Pr[X\vee Y] + \Pr[F|\overline{X}\wedge\overline{Y}]\cdot\Pr[\overline{X}\wedge\overline{Y}] \\ &\le \Pr[X\vee Y] + \Pr[F\mid\overline{X}\wedge\overline{Y}] \le \Pr[X] + \Pr[Y] \\ &\quad + \Pr[F\mid\overline{X}\wedge\overline{Y}].\end{aligned} \tag{14}$$

In the abovementioned expression, $\overline{X}$ and $\overline{Y}$ denote the complements of X and Y, respectively.

Firstly, we prove that $\Pr[X]$ is negligible. Assume that the inside adversary $\mathscr{A}_O$ can predict the value sR_σ from the public parameters *params* with nonnegligible probability, e.g., $\mathscr{A}_I$ derives sR_σ from the equation $\hat{e}(sR_\sigma, P) = \hat{e}(R_\sigma, Q)$. Then, we show that there exists another adversary $\mathscr{B}$ who can use $\mathscr{A}_I$ as a subroutine to break the CDH problem in G_1 with nonnegligible probability. The reduction works as follows: suppose $\mathscr{B}$ is given the description of G_1 with prime order q and P is a generator of G_1. Moreover, $\mathscr{B}$ is given two random values $Q = sP$ and $R_\sigma = xP$ in G_1, and $\mathscr{B}$'s task is to compute $sR_\sigma = sxP$. In the *Init* algorithm, B simulates the public parameters *params* by selecting another cyclic group G_2 with order q, a bilinear map $\hat{e}$: $G_1 \times G_1 \longrightarrow G_2$, as well as $l-1$ random values $\{R_i\}_{i\in\{1,2,\ldots,l\}\setminus\{\delta\}}$ in G_1. B, then, sends *params* to $\mathscr{A}_I$. In the *Dist* algorithm, B selects $t-1$ random values $\{s_1, s_2, \ldots, s_{t-1}\}$ in $\mathbb{Z}_q$ and sends them to $\mathscr{A}_I$. In the *Comp* algorithm, B selects $t-1$ random values $\{u_1, u_2, \ldots, u_{t-1}\}$ in $\mathbb{Z}_q$ and sends them to $\mathscr{A}_I$. B also broadcasts the required number of random values in G_1. Note that the abovementioned steps generate a simulated environment for $\mathscr{A}_I$ that is indistinguishable from a real run of our modified scheme Π. If $\mathscr{A}_I$ outputs her predict of sR_σ, B uses it to solve the *CDH* problem. Because it is assumed that the CDH assumption holds in G_1, our hypothesis that $\mathscr{A}_I$ can predicate the value sR_σ from *params* with nonnegligible probability must be false. Hence, we have $\Pr[X] < \varepsilon_1(\lambda)$ for some negligible function $\varepsilon_1(\cdot)$.

Secondly, Theorem 2 implies that the real run of our modified scheme Π does not leak any secret information to $\mathscr{A}_I$, based on the DL assumption in G_1. Also, the hybrid argument [16] further implies that $\mathscr{A}_I$ does not learn any secret information even if she has queried the oracle O polynomial number of times. Hence, we have $\Pr[Y] < \varepsilon_2(\lambda)$ for some negligible function $\varepsilon_2(\cdot)$.

Finally, we analyze the probability $\Pr[F\mid\overline{X}\wedge\overline{Y}]$. In this case, $\mathscr{A}_I$ needs to guess the value sR_σ. Because s is randomly distributed in $\mathbb{Z}_q$ and $\mathscr{A}_I$ only controls at most $t-1$ group members, the probability of guessing sR_σ correct in each trial is exactly $1/q$. Recall that $\mathscr{A}_I$ can try polynomial number of times, and we have $\Pr[F\mid\overline{X}\wedge\overline{Y}] = Q/q$, where Q denotes the number of trials $\mathscr{A}_I$ has made.

Table 1: Comparison between our scheme and Chien's scheme.

	Init	*Dist*	*Comp*	*Auth*
Chien's scheme	$1 \times G_1$	$(t-1) \times \mathbb{Z}_q$, $t + \mathbb{Z}_q$	$1 \times G_1$	$n + G_1, 1 \longrightarrow$
Our scheme	$1 \times G_1$	$(t-1) \times \mathbb{Z}_q$, $t + \mathbb{Z}_q$	$(n+2) \times G_1, n + G_1$	$n + G_1, 1 \longrightarrow$

Putting the abovementioned analyses together, assuming that the CDH assumption holds in G_1, we have

$$\begin{aligned} \Pr[F] &\leq \Pr[X] + \Pr[Y] + \Pr[F \mid \overline{X} \wedge \overline{Y}] \\ &< \varepsilon_1(\lambda) + \varepsilon_2(\lambda) + \frac{Q}{q} \\ &\leq \varepsilon(\lambda), \end{aligned} \tag{15}$$

for some negligible function $\varepsilon(\cdot)$. Therefore, our modified scheme satisfies the no forgery property. □

Theorem 4. *Our modified group authentication scheme satisfies the no impersonation property, assuming that the CDH problem holds in* G_1.

Proof. Denote X as the event that $\mathcal{A}_O$ can predict the value sR_σ from the public parameters *params* and F as the event that $\mathcal{A}_O$ can impersonate a group member without being detected. Then, we have

$$\begin{aligned} \Pr[F] &= \Pr[F \mid X]\Pr[X] + \Pr[F \mid \overline{X}]\Pr[\overline{X}] \\ &\leq \Pr[X] + \Pr[F \mid \overline{X}]. \end{aligned} \tag{16}$$

Firstly, we prove that $\Pr[X]$ is negligible. Assume that the outside adversary $\mathcal{A}_O$ can predict the value sR_σ from *params* with nonnegligible probability. Then, one can prove that there exists another adversary B who can use $\mathcal{A}_O$ as a subroutine to break the CDH problem in G_1 with nonnegligible probability. The reduction is very similar as in Theorem 3. The main difference is that B does not need to send any user's internal states to $\mathcal{A}_O$. Hence, we have $\Pr[X] < \varepsilon(\lambda)$ for some negligible function $\varepsilon(\cdot)$.

Next, we analyze the probability $\Pr[F \mid \overline{X}]$. In this case, $\mathcal{A}_O$ needs to output a token c_{t+1}, such that the equation $\sum_{i=1}^{t+1} c_i = sR_\sigma$ holds, where the set $\{c_1, c_2, \ldots, c_t\}$ denotes the other users' tokens that $\mathcal{A}_O$ has already learnt. Because s is randomly selected in $\mathbb{Z}_q$, the value sR_σ is randomly distributed in G_1. Moreover, because the value sR_σ is unpredictable, the probability that $\mathcal{A}_O$ outputs a valid token is exactly $1/q$. Recall that $\mathcal{A}_O$ can try polynomial number of times, and we have $\Pr[F \mid \overline{X}] = Q/q$, where Q denotes the number of trials $\mathcal{A}_O$ has made.

Putting the abovementioned analysis together, we conclude that $\Pr[F] < \varepsilon(\lambda) + Q/q$, which is negligible. Therefore, our modified scheme satisfies the no impersonation property assuming that the CDH assumption holds in G_1. □

5.3. Efficiency Analysis. We now give a brief efficiency analysis of our modified scheme. In the *Init* algorithm, GM selects the system parameters, including two finite cyclic group G_1 and G_2, a bilinear map $\hat{e}$ between these two groups, and some random values in G_1. The computation of $Q = sP$ takes 1 multiplication in G_1. In the *Dist* algorithm, GM selects a random polynomial $f(x)$ over $\mathbb{Z}_q$ with degree $t-1$ and evaluates this polynomial at n different points. When using Horner's rule, each evaluation of $f(x)$ takes $t-1$ multiplications and t additions in $\mathbb{Z}_q$, and each credential is a value in $\mathbb{Z}_q$. In the *Comp* algorithm, each user broadcasts 2 values in G_1 in two individual rounds. The total computations for each user require at most $n+2$ multiplications and n additions in G_1. Note that, in this step, the Lagrange coefficients can be precomputed beforehand. In the *Auth* algorithm, each user performs at most n additions in G_1 and 2 bilinear maps.

An efficiency comparison between our proposed scheme and Chien's scheme [4] is given in Table 1. Denote the symbols $+G_1$, $\times G_1$, $+\mathbb{Z}_q$, $\times \mathbb{Z}_q$ and $\longrightarrow$ as the computations of addition in G_1, multiplication in G_1, addition in $\mathbb{Z}_q$, multiplication in $\mathbb{Z}_q$, and bilinear pairing $G_1 \times G_1 \longrightarrow G_2$, respectively. Also, we ignore the other calculations, i.e., select a random element from a group, since their costs are negligible compared with the abovementioned computations.

6. Conclusions

In this paper, we have pointed out a security flaw in an existing group authentication scheme by Chien [4]. If this scheme was used in the asynchronous communication model, the adversary can pretend to be a legitimate group member without being detected. The major reason for this attack is that the adversary is able to remove the Lagrange coefficients from the revealed tokens. We have employed the AV-net to solve this problem, and we have rigorously proved that our improvement satisfies the desirable security properties in a well-defined security model. Therefore, our proposed protocol can be safely used as a drop-in replacement for Chien's scheme in asynchronous networks.

Data Availability

The authors confirm that no data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant nos. 61662016 and 61772224), Key Projects of Guangxi Natural Science Foundation (Grant

no. 2018JJD170004), and Guangxi Key Laboratory of Trusted Software (Grant no. KX201908).

References

[1] Y. Liu and Q. Zhao, "E-voting scheme using secret sharing and k-anonymity," *World Wide Web*, vol. 22, no. 4, pp. 1–11, 2019.

[2] Y. Zhou, Y. Liu, C. Jiang, and S. Wang, "An improved FOO voting scheme using blockchain," *International Journal of Information Security*, vol. 19, no. 3, pp. 303–310, 2019.

[3] L. Harn, "Group authentication," *IEEE Transactions on Computers*, vol. 62, no. 9, pp. 1893–1898, 2013.

[4] H.-Y. Chien, "Group authentication with multipletrials and multiple authentications," *Security and Communication Networks*, vol. 2017, Article ID 3109624, 7 pages, 2017.

[5] Z. Xia, L. Harn, B. Yang et al., "Provably secure group authentication in the asynchronous communication model," in *Proceedings of the 21st International Conference on Information and Communications Secuirty (ICICS)*, Springer, Beijing, China, pp. 1–16, 2019.

[6] W.-T. Su, W.-M. Wong, and W.-C. Chen, "A survey of performance improvement by group-based authentication in IoT," in *Proceedings of the 2016 International Conference on Applied System Innovation (ICASI)*, IEEE, Okinawa, Japan, pp. 1–4, 2016.

[7] Y. Liu, Q. Sun, Y. Wang, L. Zhu, and W. Ji, "Efficient group authentication in rfid using secret sharing scheme," *Cluster Computing*, vol. 22, no. S4, pp. 8605–8611, 2018.

[8] P. N. Mahalle, N. R. Prasad, and R. Prasad, "Threshold cryptography-based group authentication (TCGA) scheme for the internet of things (IoT)," in *Proceedings of the 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE)*, Aalborg, Denmark, 2014.

[9] J. Li, M. Wen, and T. Zhang, "Group-based authentication and key agreement with dynamic policy updating for mtc in lte-a networks," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 408–417, 2016.

[10] C. Guo, R. Zhuang, L. Yuan, and B. Feng, "A group authentication scheme supporting cheating detection and identification," in *Proceedings of the 2015 Ninth International Conference on Frontier of Computer Science and Technology (FCST)*, IEEE, Dalian, China, pp. 110–114, 2015.

[11] O. Elmouaatamid, M. Lahmer, and M. Belkasmi, "Group authentication with fault tolerance for internet of things," in *Ubiquitous Networking*, pp. 299–307, Springer, Berlin, Germany, 2017.

[12] Z. Ahmadian and S. Jamshidpour, "Linear subspace cryptanalysis of Harn's secret sharing-based group Authentication scheme," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 502–510, 2018.

[13] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[14] H. Feng and P. Zielinski, "A 2-round anonymous veto protocol," in *International Workshop on Security Protocols*, pp. 202–211, Springer, Berlin, Germany, 2006.

[15] C.-P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161–174, 1991.

[16] S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of Computer and System Sciences*, vol. 28, no. 2, pp. 270–299, 1984.