Chinese Journal of Electronics
Vol.24, No.1, Jan. 2015

# Asynchronous Group Authentication*

MIAO Fuyou, JIANG Huiwen,JI Yangyang and XIONG Yan

(*School of Computer Science and Technology, University of Science and Technology of China, Hefei 230027,China* )

**Abstract — Group Authentication usually checks whether an individual user belongs to a pre-defined group each time but cannot authenticate all users at once without public key system. The paper proposes a Randomized Component-based Asynchronous (t,m,n) Group Authentication ((t,m,n)-RCAGA) scheme. In the scheme, each user uses the share of (t,n)-threshold secret sharing as the token, constructs a Randomized Component with the share and verifies whether all users belong to a pre-defined group at once without requiring all users to release randomized components simultaneously. Moreover, each group member just uses a single share as the token and the scheme does not depend on any public key system. Therefore, the proposed scheme is simple and flexible. Analyses show the proposed scheme can resist up to t-1 group members conspiring to forge a token, and an adversary is unable to forge a valid token or derive a token from a Randomized Component.**

**Key words — Randomized component, Group authentication, Chinese remainder theorem, Asynchronous.**

## I. Introduction

Nowadays, group oriented applications such as online conference get more and more popular. In these applications, group members interact with one another and security is one of the main concerns. Take online conferences for example, members are limited within a small scope if the topic of the conference is confidential. In this case, each member would rather give up the conference than leak confidential information to a spy. Therefore, each member should be assured that all members are legal before the conference.

It is actually an issue of group authentication, which guarantees all participants of the conference should be legal group members. There are many group authentication schemes that verify whether a user belongs to a group, i.e., they authenticate a user each time. For example, Aboudagga et al.[1] proposed an authentication protocol named *mGAP*, which predicts nodes' behavior and manages the authentication of mobile groups and individual nodes during roaming across administrative domains. The protocol considers the limited resource of mobile node in authentication. Chen et al.[2] presented a similar group authentication protocol for roaming, in which, authenticating the first mobile node requires the Server Node to perform full authentication but the following authentication of the other nodes can be simplified without decreasing the security. Sprague[3] published a group authentication method in which pseudorandom number is used to authorize an anonymous individual or a member of a group to access some content.

There are also some group authentication schemes which can authenticate all users at once, but most of them are based on public key system. For example, In 2014, Yang et.al.[4] proposed a general framework for group authentication, which works in a one-to-multiple mode, where a party can authenticate several parties mutually, and allows member-to-member authentication and server-to-client authentication. As a general framework, the scheme allows using different public cryptographic primitives such as Diffie-Hellman key exchange system, Discrete Logarithm Problem (DLP) or elliptic curve discrete logarithm problem (ECDLP). In 2015, Wang et.al.[5] proposed an group authentication for Ad Hoc networks without a group manager, which is an identity-based scheme based on bilinear pairings. In the scheme, all group members can be authenticated by using Gentry and Ramzan's Identity-based Multi-signature Scheme. However, bilinear pairings need more computing effort when compared with symmetric cryptographic system, which makes it unsuitable for platforms with low computing power. There are many other similar group authentication schemes, e.g.,Ref.[6].

There are also some group authentication scheme not based on public key system, for example, Martucci et al.[7] proposed a lightweight group authentication mechanism for ad hoc network by using a pre-shared secret. The scheme is used to check whether nodes of an ad hoc network belong to a group but needs loose synchronization among the devices' real time clocks to thwart replay attacks. However, the synchronization of clocks is complicated especially in distributed networks.

$(t, n)$ threshold secret sharing (or $(t, n)$-SS)[8,9] is a fundamental cryptographic primitive which divides a secret into $n$ shares such that $t$ or more than $t$ shares can recover the secret while less than $t$ shares cannot. Unlike public key cryptogra-

*Manuscript Received Apr. 2015; Accepted June 2015. This work is supported in part by the National Natural Science Foundation of China ( No.61572454,No.61232018,No.61272472,No.61202404), and Open Project of Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University.

phy, $(t,n)$-SS schemes seldom depend on some hard problem, and thus are efficient in computation.

In order to improve the efficiency of group authentication, Harn[10] introduced the notion of $t$-threshold, $m$-user and $n$-group authentication (or $(t,m,n)$ group authentication), and proposed 3 schemes based on Shamir's $(t,n)$-threshold secret sharing[8]. In the asynchronous $(t,m,n)$ group authentication scheme, $k$ polynomials are used to generate $k$ shares for each group member as the token and users are allowed to release their authentication components asynchronously. An $(t,m,n)$ group authentication scheme guarantees that $m(m \geq t)$ users are of the same group if they all can recover the same secret successfully, and up to $t-1$ colluded group members cannot forge any valid token. Although the scheme is not based on public key, it requires as many as $k$ polynomials and $k$ is restricted by $t$ as well as $n$. Therefore, it is not efficient and flexible enough. Based on the notion of $(t,m,n)$ group authentication, Parikshit N. Mahalle, et.al.[11] developed a group authentication (TCGA) scheme for the Internet of Things, which uses Paillier Threshold Cryptography as the underlying secret sharing scheme. Paillier Threshold Cryptography is a public key variant of the $(t,n)$ threshold scheme. However, it is doubtful whether or not the TCGA scheme is appropriate for Internet of Things because most nodes in Internet of Things are low in computing power. Moreover, the scheme does not mention how to use Paillier Threshold Cryptography to construct the $(t,m,n)$ group authentication. In fact, the way to construct a $(t,m,n)$ group authentication highly depends on the underlying $(t,n)$ threshold secret sharing scheme.

Actually, we can utilize Randomized Components (RC)[12,13] in $(t,n)$ secret sharing schemes to make the above $(t,m,n)$ group authentication scheme more efficient and flexible. A RC binds the share of a participant with the identities of all the other participants during the secret reconstruction. RCs serve as 2 functions, protecting the contained share and recovering the secret. Therefore, the paper focuses on how to construct a more efficient and flexible asynchronous $(t,m,n)$ group authentication scheme with the same functionalities as Harn's scheme and put forwards a RC based Asynchronous $(t,m,n)$ Group Authentication scheme, which uses a Chinese Remainder Theorem based $(t,n)$-SS.

The rest of paper is organized as follows, section II presents some preliminaries, section III describes the system model of our scheme; the scheme is proposed in section IV and security analyses are given in section V. Section VI summarizes the properties and compares the proposed scheme with Harn's. Section VII concludes the paper.

## II. Preliminaries

This section gives some preliminaries including Chinese Remainder Theorem, Asmuth-Bloom's $(t,n)$-SS scheme, Randomized Component and Harn's $(t,m,n)$ Asynchronous Group Authentication Scheme.

**1. Chinese Remainder Theorem (CRT)**

For the following system of equations,

$$\begin{cases} x = s_1 \bmod p_1; \\ x = s_2 \bmod p_2; \\ \quad\quad . \\ \quad\quad . \\ \quad\quad . \\ x = s_t \bmod p_t; \end{cases} \tag{1}$$

one unique solution can be determined as $x = \sum_{i=1}^{t} y_i s_i N/p_i \bmod N$,where all moduli are pairwise coprime, i.e., $\gcd(p_i,p_j)=1$, for $i \neq j$, $y_i N/p_i \bmod p_i = 1$ and $N = p_1 \cdot p \cdot ... \cdot p_t$.

CRT was used in constructing $(t,n)$ secret sharing schemes[9,14].

**2. Asumth-Bloom's $(t,n)$ Secret Sharing**[9]

Our proposed scheme is built on the variant of Asumth-Bloom's $(t,n)$ Secret Sharing, the original scheme consists of the following 2 steps.

1) Share generation. Assume that $\mathcal{U} = \{U_i | i = 1,2,...,n\}$ are $n$ shareholders. The dealer first picks an integer $p_0$ and a sequence of pairwise coprime positive integers, $p_0 < p_1 < ... < p_n$, such that $p_0 \cdot p_{n-t+2} \cdot ... \cdot p_n < p_1 \cdot p_2 \cdot ... \cdot p_t$ and $\gcd(p_0,p_i)=1$, $i = 1,2,...,n$, where each $p_i$ is the public modulus associated with $U_i$, $t$ is the threshold. Then it randomly selects the secret $s$ within $Z_{p_0}$ and an integer,$\alpha$, such that $s + \alpha p_0 \in Z_{p_1 \cdot p_2 \cdot ... \cdot p_t}$. Finally, it computes $s_i = (s + \alpha p_0) \bmod p_i$ and sends it to $U_i$ as the share for $i = 1,2,...,n$.

2) Secret reconstruction. Suppose a group of $m(m \geq t)$ participants, $\mathcal{U}_{I_m} = \{U_{i_1}, U_{i_2}, ..., U_{i_m}\} \subseteq \mathcal{U}$, with the corresponding shares $\{s_{i_1}, s_{i_2}, ..., s_{i_m}\}$ and public modulus set $\mathcal{P}_{I_m} = \{p_{i_1}, p_{i_2}, ..., p_{i_m}\}$ accordingly, wants to recover the secret $s$, each participant $U_{i_j}(U_{i_j} \in \mathcal{U}_{I_m})$ releases the share $s_{i_j}$ to the others. On obtaining all shares in $\{s_{i_1}, s_{i_2}, ..., s_{i_m}\}$ ,$U_{i_j}$ recovers $s$ as $s = \sum_{j=1}^{m} y_{i_j} s_{i_j} N/p_{i_j} \bmod N$, where $N = \prod_{j=1}^{m} p_{i_j}$, $y_{i_j}$ is the multiplicative inverse of $N/p_{i_j}$ modulo $p_{i_j}$.

**3. Randomized Component**

In 2015, we proposed the notion of Randomized Component (or RC)[12,13] for secret sharing, which adds new fine features to traditional $(t,n)$ secret sharing schemes and is suitable for constructing asynchronous $(t,m,n)$-group authentication schemes.

During the secret reconstruction of a $(t,n)$-SS, a RC binds the share and all participants together by a random number, and can be used to recover the secret. In other words, all participants form a tightly coupled group by each producing a RC with the share, and thus recovering the secret requires each participant to have a valid share and actually join the secret reconstruction. Therefore, RCs improve the security of secret sharing and are more suitable for group oriented applications based on $(t,n)$-SS.

Formally, assume that $\mathcal{S}_i$ and $\mathcal{S}$ are the share space and secret space respectively in a $(t,n)$-SS, $\mathcal{U}_m$ is the participant set consisting of $m(m \geq t)$ shareholders, each participant $U_i(U_i \in \mathcal{U}_m)$, with the share $s_i$, constructs its RC $c_i$ as $c_i = f(s_i, INF_m, r_i)$, where $f : \mathcal{S}_i \times \mathcal{S}_i^{(m)} \times \mathcal{S} \to \mathcal{S}_i$ is a function over $\mathcal{S}_i$, $INF_m$ is the public information of all $m$ participants

and $r_i$ is a random integer uniformly selected over $\mathcal{S}$. In this case, the secret $s$ can only be reconstructed from all $m$ RCs.

A RC has 2 properties, 1) Share Protection: each RC, e.g. $c_i$ can protect the share $s_i$ from exposure; 2) Secret Recoverability: the secret can be recovered from all RCs. As a concrete type, CRT- based RCs will be constructed in the proposed asynchronous $(t, m, n)$ group authentication scheme.

**4. Harn's Asynchronous Group Authentication**

In 2013, Harn proposed an asynchronous $(t, m, n)$ group authentication scheme[10] based on Shamir's $(t, n)$-SS, which can check whether $m$ users belong to a pre-defined group. It consists of the following 2 steps.

1) Token generation. Assume there are totally $n$ group members,$\{U_i|i = 1, 2, ..., n\}$, in the scheme, each member $U_i$ with the public information $x_i$. The Group Manager (GM), coordinator of the scheme, selects $k$ random polynomials, $f_l(x), l = 1, 2, ..., k$, with degree $t-1$ each, and produces tokens $f_l(x_i), l = 1, 2, ..., k$, for each group member $U_i$,(i.e.,$kt > n - 1$ ). For the secret $s$, GM finds integers,$w_j, d_j, j = 1, 2, ..., k$, in $GF(p)$, such that $s = \sum_{j=1}^{k} d_j f_j(w_j)$, where $w_i \neq w_j$, for every pair of $i$ and $j$.GM publishes integers $w_j, d_j, j = 1, 2, ..., k$, and $H(s)$, where $H(.)$ is a one way hash function.

2) Group authentication. Assume that $m$ out of $n$ users, e.g., $\{U_i|i = 1, 2, ..., m\}, (t \leq m \leq n)$ for simplicity, need to be authenticated, each user $U_i$ uses its tokens $f_l(x_i), l = 1, 2, ..., k$, to compute and release $c_i = \sum_{j=1}^{k} d_j f_j(x_i) \prod_{r=1, r\neq i}^{m} (w_j - x_r)/(x_i - x_r) \bmod p$ to the others. Knowing $\{c_i|i = 1, 2, ..., m\}$, each user computes s'=$\sum_{i=1}^{m} c_i \bmod p$, If H(s')=H(s) all users are authenticated successfully, otherwise, there is at least one non-member in $\{U_i|i = 1, 2, ..., m\}$.

**Remark:** the scheme can authenticate $m$ users all at once on the condition $kt > n-1$ , which means that each user needs to have $k$ tokens, and $k$ is restricted by the threshold $t$ and the total number of group members $n$ . Therefore, the scheme is not efficient and flexible enough.

## III.System Model

**1. Entities**

Assume that there are 3 types of entities in the proposed asynchronous $(t, m, n)$ group authentication scheme, the Group Manager (GM), group members and some adversaries.

*a)* Group Manager (GM): he Group Manager is the coordinator of the scheme, which is trusted by all group members and responsible for the setup and distributing a token (share) to each member. It is assumed that a secure channel exits between GM and each group member, that is, GM can dispatch a token securely to each member.

*b)* Group Members: all Group members belong to a predefined group. Before authentication, each group member obtains a token (i.e., shares of a secret sharing) from GM securely. All entities, including Group members and adversaries, are called users when they participate in group authentication. We assume that every 2 users share a private channel to exchange RCs during authentication, the same group of users is never authenticated twice and the token of a group member cannot be obtained from inside the group member.

*c)* Adversaries: There are 2 types of adversaries, Insiders and Outsiders.

**2. Adversary Model**

In the scheme, each group member has a token generated by GM. Besides, there are 2 types of adversaries.

*a)* Outsiders: An Outsider does not belong to the above group and thus has no valid token. However, during the group authentication, an outsider may crack some private channels, intercept RCs, try to derive a valid token and impersonate the owner of the token; it may also directly forge a token for itself.

*b)* Insiders: An Insider is a legal group member, which possesses a valid token. However, $t - 1$ Insiders may conspire to forge a valid token for some Outsiders. We assume that there are at most $t - 1$ Insiders in the proposed scheme. Besides, an Insider never leak its share to Outsiders.

The scheme is supposed to prevent any Outsider from obtaining a valid token or thwart $t-1$ Insider conspiring to forge a token.

## IV.Proposed RC based Asynchronous $(t, m, n)$ Group Authentication

**1. Overview**

The proposed RC based Asynchronous $(t, m, n)$ Group Authentication ($(t, m, n)$-RCAGA) scheme aims to verify whether all users are of a pre-defined group at once rather than authenticate each individual user. It doesn't require users to release their tokens simultaneously. To attain this goal, the scheme employs shares of a $(t, n)$-secret sharing as tokens of group members and publishes H(s), the one way hash value of the secret as the proof.

In $(t, m, n)$-RCAGA, each user releases a RC which is constructed with the token, this process need not occur simultaneously. Upon collecting all RCs from the others, the user recover a value s' and check whether H(s') and H(s) are equal. If both values are equal, all users are group members; otherwise, at least one user is not group member (non-member).

However, if each user is allowed to release the token (i.e., share) instead of RC asynchronously and there are more than $t$ users, including a non-member, to be authenticated, the non-member may collect at least $t$ shares to generate a valid share as the token temporarily and thus passes the group authentication.

Therefore, the proposed scheme utilizes RCs instead of tokens during group authentication; i.e., all users release RCs to reconstruct a value s' for authentication. From the properties of RCs, we know that the secret can be recovered, i.e., s'=s only from all valid RCs. Therefore, the RC-based scheme can guarantee all users belong to the same group only if they all have a valid RC each, i.e., they all have valid tokens (shares).

**2. Proposed scheme**

The proposed $(t, m, n)$-RCAGA consists of 3 steps, 1) Token Generation, 2) Randomized Component Construction based on CRT and 3) Group Authentication.

1) Token Generation. Assume that $\mathcal{U} = \{U_i|i = 1, 2, ..., n\}$, are $n$ group members. The Group Manager (GM) first picks an large integer $p_0$ and a sequence of pairwise coprime positive integers,$p_0 < p_1 < ... < p_n$, such that $p_0^2 \cdot p_{n-t+2} \cdot ... \cdot p_n < p_1 \cdot p_2 \cdot ... \cdot p_t$, $np_0^3/(p_0 - 1) < p_1$ and $\gcd(p_0, p_i) = 1$,

$i = 1, 2, ..., n$, where each $p_i$ is the public modulus associated with $U_i$, $t(t \leq n)$ is the threshold. Next it randomly selects a value $s \in Z_{p_0}$ and a private integer,$\alpha$, such that $s + \alpha p_0 \in Z_{\lceil (p_1 \cdot p_2 \cdot \ldots \cdot p_t)/p_0 \rceil}$. Then, GM computes $s_i = (s + \alpha p_0) \bmod p_i$ and securely sends it to $U_i$ as the token for $i = 1, 2, ..., n$. Finally, it makes $p_0, p_1, ..., p_n$,$n$,$t$ and $H(s)$ publicly known while keeps $\alpha$ in secret, where $H(.)$ is a public one-way hash function.

2) Randomized Component Construction based on CRT. If $m(n \geq m \geq t)$ users, $\mathcal{U}_{I_m} = \{U_{i_1}, U_{i_2}, ..., U_{i_m}\} \subseteq \mathcal{U}$ with the corresponding shares $\mathcal{S}_{I_m} = \{s_{i_1}, s_{i_2}, ..., s_{i_m}\}$ and public moduli $\mathcal{P}_{I_m} = \{p_{i_1}, p_{i_2}, ..., p_{i_m}\}$, need to be authenticated, each user $U_{i_j} (U_{i_j} \in \mathcal{U}_{I_m})$ constructs a Randomized Component (RC) as

$$c_{i_j} = (s_{i_j} y_{i_j} N/p_{i_j} + r_{i_j} p_0 N/p_{i_j}) \bmod N \tag{2}$$

where $y_{i_j} (N/p_{i_j}) \bmod p_{i_j} = 1$,$N = \prod_{j=1}^{m} p_{i_j}$ and $r_{i_j}$ is uniformly selected within $Z_{p_0}$ by $U_{i_j}$.

3) Group Authentication. To decide whether all users are from the same group, each user,$U_{i_j} (U_{i_j} \in \mathcal{U}_{I_m})$, releases the RC $c_{i_j}$ within $\mathcal{U}_{I_m}$. After obtaining all RCs, $\{c_{i_j} | j = 1, 2, ..., m\}$, $U_{i_j}$ computes s'=$\sum_{j=1}^{m} c_{i_j} \bmod N \bmod p_0$. If $H(s') = H(s)$, all users in $\mathcal{U}_{I_m}$ belong to the same group; otherwise, $\mathcal{U}_{I_m}$ includes at least one non-member.

**3. Correctness**

The following fact guarantees that all users are authenticated successfully in the case of $s' = s$ due to

$$\begin{aligned} s' &= \sum_{j=1}^{m} c_{i_j} \bmod N \bmod p_0 \\ &= \sum_{j=1}^{m} (s_{i_j} y_{i_j} N/p_{i_j} \bmod N + r_{i_j} p_0 N/p_{i_j} \bmod N) \\ &\quad \bmod N \bmod p_0 \\ &= (s + \alpha p_0 + \sum_{j=1}^{m} (r_{i_j} p_0 N/p_{i_j}) \bmod N) \bmod N \bmod p_0 \\ &= (s + \alpha p_0 + \sum_{j=1}^{m} r_{i_j} p_0 N/p_{i_j}) \bmod N \bmod p_0 \\ &= (s + \alpha p_0 + \sum_{j=1}^{m} r_{i_j} p_0 N/p_{i_j}) \bmod p_0 = s. \end{aligned}$$

Recall $p_0^2 \cdot p_{n-t+2} \cdot ... \cdot p_n < p_1 \cdot p_2 \cdot ... \cdot p_t$,$np_0^3/(p_0 - 1) < p_1$ and $(s + \alpha p_0) \in Z_{\lceil (p_1 \cdot p_2 \cdot \ldots \cdot p_t)/p_0 \rceil} < N/p_0$, we have $\sum_{j=1}^{m} r_{i_j} p_0 N/p_{i_j} < m p_0^2 N/p_{i_j} < (1 - \frac{1}{p_0})N$ and thus $(s + ap_0 + \sum_{j=1}^{m} r_{i_j} p_0 N/p_{i_j}) \bmod N = (s + ap_0 + \sum_{j=1}^{m} r_{i_j} p_0 N/p_{i_j})$.

## V. Security Analyses

As mentioned previously,$p_0$ is a large integer in a cryptographic sense, i.e., $1/p_0$ is negligible. In our scheme, an Outsider may intercept a RC released by a user if it cracks the private channel successfully. However, due to Theorem 1, it is impossible for an Outsider to derive the token from a RC with the probability more than $1/p_0$ and thus the scheme is secure even if a RC is accidentally exposed to an Outsider

**Theorem 1** In the proposed scheme, an Outsider cannot derive the token from a released Randomized Component, i.e., given the RC $c_{i_j} = (s_{i_j} y_{i_j} N/p_{i_j} + r_{i_j} p_0 N/p_{i_j}) \bmod N$, the Outsider cannot derive the token $s_{i_j}$ with the probability more than $1/p_0$.

**Proof** Given

$$c_{i_j} = (s_{i_j} y_{i_j} N/p_{i_j} + r_{i_j} p_0 N/p_{i_j}) \bmod N \tag{3}$$

the Outsider has $c_{i_j} p_{i_j}/N = (s_{i_j} y_{i_j} + r_{i_j} p_0) \bmod p_{i_j}$, i.e.,

$$s_{i_j} = (c_{i_j} p_{i_j}/N - r_{i_j} p_0) y_{i_j}^{-1} \bmod p_{i_j} \tag{4}$$

where $y_{i_j}^{-1}$ is the multiplicative inverse of $y_{i_j} \bmod p_{i_j}$ i.e.,$N/p_{i_j} \bmod p_{i_j}$, note that $c_{i_j}$ is the multiple of $N/p_{i_j}$ because of Eq.(3). Apparently, given $c_{i_j}, p_0, p_{i_j}$ and $N$ in Eq.(4), there must exist a distinct value of $s_{i_j}$ for each different $r_{i_j} \in Z_{p_0}$ since both $N/p_{i_j}$ and $p_0$ are relatively prime to $p_{i_j}$. Since $r_{i_j}$ is uniformly distributed over $Z_{p_0}$, there are $p_0$ possible values of $s_{i_j}$ satisfying Eq.(3), each with the identical probability. Therefore, an Outsider derives the token $s_{i_j}$ from $c_{i_j}$ exactly with the probability $1/p_0$.

**Lemma 1** In $c_{i_j} = (s_{i_j} y_{i_j} N/p_{i_j} + r_{i_j} p_0 N/p_{i_j}) \bmod N$, if $s_{i_j}$ and $r_{i_j}$ are random variables uniformly distributed over $Z_{p_{i_j}}$ and $Z_{p_0}$ respectively, then $c_{i_j} p_{i_j}/N \bmod p_{i_j}$ has the uniform distribution over $[0, p_{i_j})$, for given $p_{i_j}, p_0$ and $N$, where $y_{i_j}$ is the multiplicative inverse of $N/p_{i_j} \bmod p_{i_j}$.

**Proof** $c_{i_j} = (s_{i_j} y_{i_j} N/p_{i_j} + r_{i_j} p_0 N/p_{i_j}) \bmod N$ is followed by $c_{i_j} p_{i_j}/N = (s_{i_j} y_{i_j} + r_{i_j} p_0) \bmod p_{i_j}$, let $a_{i_j} = c_{i_j} p_{i_j}/N \bmod p_{i_j}$ , we have

$$a_{i_j} = (s_{i_j} y_{i_j} + r_{i_j} p_0) \bmod p_{i_j} \tag{5}$$

in which each value of $s_{i_j} \in Z_{p_{i_j}}$ produces a distinct $a_{i_j}$ for fixed $r_{i_j}$ because of $\gcd(y_{i_j}, p_{i_j}) = 1$. Similarly, each value of $r_{i_j} \in Z_{p_0}$ also corresponds a distinct $a_{i_j} \in Z_{p_{i_j}}$ for fixed $s_{i_j}$ due to $\gcd(p_0, p_{i_j}) = 1$. Consequently, there are totally $p_{i_j} p_0$ values of $a_{i_j}$ when $s_{i_j}$ and $r_{i_j}$ uniformly vary within $Z_{p_{i_j}}$ and $Z_{p_0}$ respectively, each distinct value appears $p_0$ times. Therefore, each distinct value of $a_{i_j} \in Z_{p_{i_j}}$ has the possibility of $p_0/p_{i_j} p_0 = 1/p_{i_j}$.That is,$c_{i_j} p_{i_j}/N \bmod p_{i_j}$ has the uniform distribution over [0,$p_{i_j}$) for given $p_{i_j}, p_0$ and $N$. In other words, $c_{i_j}$ is uniformly distributed over all multiples of $N/p_{i_j}$ within [0,$N$).

**Theorem 2** In the proposed scheme, an Outsider cannot manage to impersonate a group member by replaying a previously released Randomized Component of the group member in a new group authentication.

**Proof** From the adversary model, it is known that a group never be authenticated twice. Thus, we assume without losing generality that a user $U_{i_m}$ released a RC $c'_{i_m} = (s_{i_m} y'_{i_m} N'/p_{i_m} + r_{i_m} p_0 N'/p_{i_m}) \bmod N'$ during the authentication of the group $\mathcal{U}'_{I_m} = \{U'_{i_1}, U_{i_2}, ..., U_{i_m}\} \subseteq \mathcal{U}$ in the past, which is obtained later by the Outsider $U_O$ ,where $N' = p'_{i_1} p_{i_2} ... p_{i_m}$, $p_{i_j}$ is the public modulus of $U_{i_j}, j = 1, 2, ..., m$. Now $U_O$ impersonates $U_{i_m}$ and replays $c'_{i_m}$ in the authentication of the new group $\mathcal{U}_{I_m} = \{U_{i_1}, U_{i_2}, ..., U_{i_m}\} \subseteq \mathcal{U}$. In this case, the other users don't notice the impersonation of $U_O$ and still consider $U_O$ as $U_{i_m}$. Each of them, e.g.,$U_{i_j} (1 \leq j \leq m - 1)$, constructs and releases a RC $c_{i_j} = (s_{i_j} y_{i_j} N/p_{i_j} + r_{i_j} p_0 N/p_{i_j}) \bmod N$, and finally computes $s' = (\sum_{j=1}^{m-1} c_{i_j} + c'_{i_m}) \bmod N$, where $N = p_{i_1} p_{i_2} ... p_{i_m}$. However, successful

group authentication requires $s' = (\sum_{j=1}^{m-1} c_{i_j} + c'_{i_m}) \bmod N = \sum_{j=1}^{m} c_{i_j} \bmod N = s$ . That is, $c'_{i_m} = c_{i_m} \bmod N$, note that $c'_{i_m}$ is known for $U_O$ while $c_{i_m} \bmod N$ is uniformly distributed over $\{iN/p_{i_m} | i = 0, 1, ..., p_{i_m} - 1\}$ from Lemma l, which means that even if $c'_{i_m}$ is a multiple of $N/p_{i_m}$ , the probability of $c'_{i_m} = c_{i_m} \bmod N$ is at most $1/p_{i_m}$, which is negligible. Therefore,$U_O$ cannot impersonate a group member by replaying an old RC.

**Theorem 3** an Outsider cannot pass the group authentication by forging a RC.

**Proof(Omitted)** the proof is similar to that of Theorem 2.

In some case, some Insiders may conspire to try to jointly produce a valid token for an Outsider, Theorem 4 demonstrates the security of our scheme in this aspect.

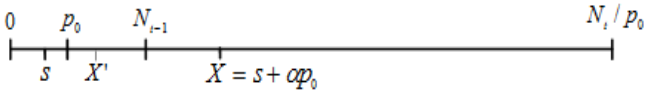
**Theorem 4** $t-1$ Insiders cannot figure out a valid token for an Outsider.

**Proof** In the proof, all parameters are the same as in Section IV.2, so we would not repeat their explanation here if unnecessary.

We consider the extreme case that $t-1$ out of $n$ group members $\mathcal{U}_{t-1} = \{U_i | i = n-t+2, ..., n\}$, try to derive a valid token, each group member $U_i$ has the public modulus $p_i$ and token $s_i$ , where $s_i = s + \alpha p_0 \bmod p_i$,$s \in Z_{p_0}$ and $s + \alpha p_0 \in Z_{\lceil (p_1 \cdot p_2 \cdot \cdots \cdot p_t)/p_0 \rceil}$. To derive a valid token, they have to first figure out $X = s + \alpha p_0 \in Z_{\lceil (p_1 \cdot p_2 \cdot \cdots \cdot p_t)/p_0 \rceil}$, and then compute a token, e.g., $s_j = X \bmod p_j$, $p_j$ is designated as the new public modulus of an Outsider.

Knowing $\{p_{(n-t+2)}, p_{(n-t+4)}, ..., p_n\}$, $\mathcal{U}_{t-1}$ can solve the following system of equations to obtain $X' \in Z_{p_{(n-t+2)} p_{(n-t+3)} \cdots p_n}$ by Chinese Remainder Theorem with $X' = X \bmod p_{(n-t+2)} p_{(n-t+3)} \cdots p_n$. i.e.,$X = X' + \lambda p_{(n-t+2)} p_{(n-t+3)} \cdots p_n$, for integer some $\lambda$ .

$$\begin{cases} X' = s_{(n-t+2)} \bmod p_{(n-t+2)} \\ X' = s_{(n-t+3)} \bmod p_{(n-t+3)} \\ X' = s_{(n-t+4)} \bmod p_{(n-t+4)} \\ \quad\quad . \\ \quad\quad . \\ \quad\quad . \\ X' = s_n \bmod p_n \end{cases} \tag{6}$$




$N_t = p_1 p_2 ... p_t$; $N_{t-1} = p_{(n-t+2)} p_{(n-t+3)} \cdots p_n$;

Fig. 1. Relationship among parameters in Theorem 4

However, we know from Fig.1 that there are at least $(N_t/p_0)/N_{t-1} = p_1 p_2 ... p_t / p_0 p_{(n-t+2)} p_{(n-t+3)} \cdots p_n > p_0$ possible values of $\lambda$ satisfying $X = X' + \lambda p_0 p_{(n-t+3)} \cdots p_n$ due to $p_0^2 \cdot p_{(n-t+2)} \cdot ... \cdot p_n < p_1 \cdot p_2 \cdot ... \cdot p_t$. Note that when $\mathcal{U}_{t-1}$ conspire,$N_{t-1}$,the product of $t-1$ public moduli has the largest value and thus there are the least possible values of $\lambda$ satisfying $X = X' + \lambda p_{(n-t+2)} p_{(n-t+3)} \cdots p_n$.

Therefore, the probability for $t-1$ Insiders to conspire to derive a valid token is $1/p_0$, which is negligible.

# VI. Properties and Comparisons

In this section, we will summarize the properties of our scheme and make comparisons with Harn's Asynchronous $(t, m, n)$ group authentication scheme.

**1. Properties**

1) Efficiency. Traditional group authentications authenticate one user each time. However, in our proposed group authentication scheme, each user authenticates all users at once just by recovering the secret s. Moreover, the proposed scheme is not based on public key systems and thus is more efficient in computation. That is, our scheme can efficiently decide whether all users are legal group members.

2) Simplicity and Flexibility. Our scheme allows each group member to have only one token, and one can flexibly choose parameters in the underlying secret sharing scheme, such as the threshold and the total number of group members.

3) Security. Due to the underlying $(t, n)$ secret sharing scheme, our scheme guarantees that even up to $t-1$ Insiders cannot to derive a valid token. In addition, the token of a group member is protected by the RC as shown in Theorem 1, and thus the group member doesn't need to worry about the exposure of its token during group authentication. Moreover, our scheme does not utilize any public key cryptographic primitives (i.e., it does not depend on any hard problem) and thus it is more desirable than those based on public key systems.

**2. Comparisons**

Because of the similarity to Harn's $(t, m, n)$ Asynchronous Group Authentication, we will compare our scheme with it in the following 2 aspects.

1) Flexibility. Harn's scheme uses $k (k > 2)$ polynomials of degree $t-1$ to generate $t-1$ shares for each of $n$ group members as the token. It requires $kt > n-1$ to guarantee the security, which implies that the threshold $t$ is restricted by the number of polynomials $k$ and the total number of group members $n$. Therefore, the scheme is not flexible especially when $n$ is large.

For example, if there are 1000 group members in all and Harn's scheme uses polynomials of degree 2 to generate tokens, then at least 500 polynomials are required, which means each group member has to hold 500 shares as the token and thus the scheme is too inefficient. If the scheme uses 2 polynomials, then more than half group members need to participate in the group authentication, which is usually impractical to have such high threshold in applications with a large number of group members.

In contrast, each group member in our scheme just need one share as the token, and the threshold $t$ is basically independent of the total number of group members $n$. our scheme allows GM to choose $t$ flexibly even for a large $n$ as long as $n \geq t$ holds. Therefore our scheme is more flexible than Harn's.

2) The ratio of token size/secret size. The ratio of token size/secret size is an important metrics to measure the efficiency of group authentication. Apparently, the less the ratio is, the better a group authentication scheme is.

In Harn's scheme, each group member has $k$ $(k \geq 2)$ shares as token which is $k$ times of the secret $s$ in size, because each share and the secret $s$ are from the same finite field in the underlying Shamir's SS. Compared with Harn's scheme,

group member $U_n$ in our scheme has the token $s_n \in Z_{p_n}$ with the largest size $\log_2 p_n$, while the secret $s$ has the size $\log_2 p_0$, since $np_0^3/(p_0-1) < p_1 < p_n$,we can control $p_n$ such that $np_0^3/(p_0-1) < p_n < p_0^3$ holds, i.e., the size of a token is no more than 3 times of the secret (note that $p_0$ is much larger than $n$ ). Therefore, our scheme is more efficient than Harn's in the ratio of token size/secret size.

## VII. Conclusion and Future Work

The paper proposed an asynchronous $(t, m, n)$ group authentication scheme based on Randomized Components in a $(t, n)$ secret sharing, which verifies whether all users belong to the same group at once. In the scheme, each user has a single share of a $(t, n)$ secret sharing scheme as the token, constructs a RC and recovers the secret to authenticate all users at once. The scheme does not depend on any public key system. Compared with Harn's scheme, the proposed scheme is simpler and more flexible. Analyses show that our scheme can resist up to $t-1$ group members conspiring to forge a token, and an adversary is unable to derive the token from a RC, or forge a token or replay a previously released RC to pass the authentication.

In Ref.[10], Harn's also presents a multiple group authentication scheme, which allows a group member to reuse the tokens for multiple authentications. A similar multiple authentication scheme based on RC can be constructed accordingly.

The proposed scheme actually presents a general method to construct an Asynchronous $(t, m, n)$ Group Authentication scheme based on Randomized Components. In the future, we are about to construct polynomial or linear code based RCs, instead of CRT based RC, and employ them to design new asynchronous $(t, m, n)$ Group Authentication schemes. These schemes share the similar properties in security with the proposed scheme.

# References


[1] N. Aboudagga, J.J. Quisquater and M. Eltoweissy, "Group authentication protocol for mobile networks", *Wireless and Mobile Computing, Networking and Communications,Third IEEE International Conference on. IEEE* , New York, USA, pp.28-28, 2007.

[2] Y.W. Chen, J.T. Wang and K.H. Chi, "Group-based authentication and key agreement", *Wireless Personal Communications* ,Vol.62, No.4, pp.965–979, 2012.

[3] S. Sprague, "Method and system for user and group authentication with pseudo-anonymity over a public network", *U.S. Patent Application*, 09/906,375, 2001-7-16.

[4] H. Yang, L. Jiao and V.A. Oleshchuk , "A General Framework for Group Authentication and Key Exchange Protocols", *Foundations and Practice of Security. Springer International Publishing*, pp.31–45, 2014.

[5] F. Wang, C.C. Chang and Y.C. Chou, "Group Authentication and Group Key Distribution for Ad Hoc Networks", *International Journal of Network Security*, Vol.17, No.2, pp.199–207, 2015.

[6] S.B. Guthery, "Group Authentication Using the Naccache-Stern Public-Key Cryptosystem ", *arXiv.org>cs>arXiv:cs/0307059*, 2003.

[7] L.A. Martucci, T. Carvalho and W.V. Ruggiero ,"A lightweight distributed group authentication mechanism " *INC2004-Fourth International Network Conference*, pp.393–400, 2004.

[8] A. Shamir, "How to share a secret", *Communications of the ACM* ,Vol.22, No.11, pp.612–613, 1979.

[9] C. Asmuth and J. Bloom, "A modular approach to key safeguarding", *IEEE Transactions on Information Theory*,Vol.30, No.2, pp.208–210, 1983.

[10] L. Harn, "Group authentication", *Computers, IEEE Transactions on*,Vol.62, No.9, pp.1893–1898, 2013.

[11] P.N. Mahalle, N.R. Prasad and R. Prasad, "Threshold Cryptography-based Group Authentication (TCGA) scheme for the Internet of Things (IoT)", *Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE),* 2014 4*th International Conference on. IEEE*, pp.1–5, 2014.

[12] F.Y. Miao, Y. Xiong and X.F. Wang, "Randomized Component and Its Application to (t, m, n)-Group Oriented Secret Sharing", *IEEE Transactions on Information Forensics and Security*, Vol.10, No.5, pp.889–899, 2015.

[13] F.Y. Miao and Y.Y. Fan," A (t,m,n)-Group Oriented Secret Sharing Scheme", *Chinese Journal of Electronics(to appear)*, 2015.

[14] M. Mignotte, "How to share a secret", *Cryptography-EUROCRYPTO'82*,LNCS 149,pp.371–375, 1983.



**Miao Fuyou** received his Master degree in Computer Science and Technology from the China University of Mining Technology (Beijing) in 1999. In 2005, he received his Ph.D. degree in Computer Science from the University of Science and Technology of China. Currently, he is an associate professor with the School of Computer Science and Technology, University of Science and Technology of China. His research interests are applied cryptography, network security and mobile computing. (Email: mfy@ustc.edu.cn)