IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 23, 2019, accepted January 4, 2020, date of publication January 10, 2020, date of current version February 4, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2965732

Multi-Receiver Authentication Scheme for General Access Structure

QIUXIA XU[1], CHUNMING TANG[1,2], AND JINGTONG WANG[3]
[1]School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China
[2]Key Laboratory of Information Security Technology in Guangdong Province, Guangzhu 510006, China
[3]School of Mathematics and Statistics, Hunan University of Technology and Business, Changsha 410205, China

Corresponding author: Chunming Tang (ctang@gzhu.edu.cn)

This work was supported in part by the Foundation of National Natural Science of China under Grant 61772147, in part by the Guangdong Province Natural Science Foundation of Major Basic Research and Cultivation project under Grant 2015A030308016, in part by the Collaborative Innovation Major Projects of Bureau of Education of Guangzhou City under Grant 1201610005, in part by the National Cryptography Development Fund under Grant MMJJ20170117, in part by the Open Subject Project of State Key Laboratory of Cryptography Science and Technology under Grant MMKFKT201913.

ABSTRACT Authentication is an important primitive of cryptography. With the rapid progress of network communication, the urgent data needs to ensure it integrity and privacy, therefore, the authentication of multi-receiver has a significant impact on the development of network interaction. R. Safavi-Nalni and H. Wang showed that authentication scheme based on Reed-Solomon code is unconditionally secure and allows multiple messages to be authenticated, but the number of receiver to verify is less than q, where the messages are in $\mathbb{F}_q$. In 2014, the secure multi-receiver authentication scheme base on linear code was proposed, however, this scheme can not realize any a given access structure. In this paper, we present a multi-receiver authentication scheme to realize any a given ideal access structure, and demonstrate that our scheme is unconditionally secure and allows r messages to be authenticated with each receiver own private key.

INDEX TERMS Multi-receiver authentication scheme, access structure, adversary structure, linear code.

I. INTRODUCTION

Authentication [9], [10] is an important primitive of cryptography. The difference between authentication scheme and encryption scheme is that encryption scheme pays more attention to data privacy [11], [12], while authentication scheme [13], [14] is more attention to the integrity of data. The traditional model of authentication scheme is that a single sender sends a message with the tag to a receiver by a public channel. With the rapid progress of network communication, the urgent data needs to ensure it integrity and privacy, therefore, the authentication of multiple receivers has a significant impact on the development of network interaction.

In the multi-receiver authentication [15], a sender broadcasts an authenticated message with the tag such that all the receivers can independently verify the message with their own private keys. In this authentication scheme, it needs to prevent multiple malicious receivers to make a substitution attack, fake a message or impersonate the transmitter.

The associate editor coordinating the review of this manuscript and approving it for publication was Kuo-Hui Yeh.

Secret sharing scheme [16]–[18] is to divide the secret into several pieces and then distribute them to different participants. Only qualified sets can recover the secret and no information of this secret is available to any unqualified sets. In principle, every linear code can be used to construct secret sharing schemes [19], [20], [24]. But determining the access structure [21]–[23] is very hard as characterizing the minimal codewords of the underlying linear code is a hard problem. Massey [4] used linear codes to construct secret sharing schemes and indicated that the main problem is to characterize what types of access structure can be realized by linear codes. McEliece *et al.* [5] made a pioneering work in 1981 for secret sharing based on linear codes, they constructed a threshold scheme with Reed-Solomon code and pointed out the equivalence between Shamir's secret share and Reed-Solomon codes.

The subject of study in this paper is multi-receiver authentication scheme for general access structure. Namely, three parties, a trusted authority, a sender and receivers, want to transmit messages to receivers by a public channel that the malicious groups cannot make a substitute or fake

the messages. The authentication scheme has been extensively studied for two reasons, firstly authentication is a foundational primitive for cryptography and secondly it has many practical applications. For example, authentication scheme has been proposed in Internet of things, an efficient authentication mechanism for providing secure communication between the users [10], [29], road condition monitoring [30], biometrics template privacy [31], smart grid [32] and so on.

A. OUR CONSTRUCTION

Tang *et al.* [7] provided a method to achieve a linear code for any given access structure, it is equivalent to solving a system of quadratic equations constructed by the given access structure and the corresponding adversary structure. We use Tang's method to present a multi-receiver authentication scheme based on J. Zhang and F. Fu (2014) [8] that perform a given access structure, which can realize an ideal linear code C with minimum distance more than or equal to 2 (a linear code is ideal [25] if the length of code is $n + 1$, where n is the number of participants). There are less number of malicious groups in our scheme than J. Zhang and F. Fu (2014) that can corrupt receiver. The scheme is unconditionally secure and allows r messages to be authenticated with each receiver own private key.

B. RELATED WORK

Desmedt *et al.* [2] first gave an authentication scheme of single message for multi-receivers. In this scheme, there is only one message and multi-receivers can verify it. The sender broadcasts the message with tag by a public channel and each receiver can verify it using his/her own private key. Safavi-Naini and Wang [6] extended the DFY scheme [2] to be an authentication scheme of multiple messages for multi-receivers based on the idea of Shamir's secret sharing. Wang [14] constructed a multi-sender authentication codes. Zhang *et al.* [8] constructed multi-receiver authentication scheme based on generalization linear code, it allows arbitrarily many receivers to check the integrity of messages, and the minimal group of receivers that can successfully make a substitution attack is determined by the minimal codeword of the dual code.

Massey [4] gave the definite of the minimum codeword and pointed out that there is one-to-one relationship between minimum qualified set of secret sharing scheme and minimum codeword of the dual code. Ding *et al.* [23] constructed some linear codes whose covering structure can be determined, and used them to construct secret sharing schemes with interesting access structures. Cramer [1] constructed a linear secret sharing scheme based on algebraic geometric codes. Tang *et al.* [7] provided a method to judge whether there exist an ideal linear code to realize a given access structure, it is equivalent to solving a system of quadratic equations constructed by the given access structure and the corresponding adversary structure.

TABLE 1. Meaning of some symbols.

Symbol	Meaning	Symbol	Meaning
$\mathbb{F}_q$	finite field	$\mathcal{R}$	an adversary structure
q	prime	Γ	an access structure
$\mathbb{F}_q^{n+1}$	vector space	f_i	the ith qualified set
s	secret	R_i	the ith unqualified set
s_i	the share of p_i	$\mathbb{P}$	private key of sender
P	the set of participants	K	the private keys of receivers
p_i	the ith participant	K_i	the private key of receiver p_i
C	linear code	$T(m)$	the tag of message m
$\mathbf{u}$	a vector	$T_i(m)$	the ith element of $T(m)$
$C^{\perp}$	dual code	M_r	a matrix
$\mathbf{c}$	codeword	E	identity matrix
supp($\mathbf{c}$)	support of $\mathbf{c}$	V	the coalition of malicious receivers
Wt($\mathbf{c}$)	Hamming weight of $\mathbf{c}$	m_i	the ith message
$d(C)$	minimum distance	$dim(U)$	the dimension of U
$\mathbb{H}$	check matrix	S'	unqualified set
$\mathbb{G}$	generator matrix	S	qualified set
$\mathbf{g}_i$	the ith column of $\mathbb{G}$		

The remainder of this paper is organized as follows. Section 2 introduces definitions and the relationships between secret sharing schemes and linear codes; section 3 adopts the method of Tang et al. to obtain the ideal linear code and constructs an authentication scheme for a given access structure; section 4 is the security analysis of the scheme. Section 5 is conclusion.

II. PRELIMINARIES

In this section, some notations is listed, we recall Shamir's secret sharing scheme and introduce the definition of linear code and general secret sharing, and the connection of them. Finally, we modify the definition of the minimal codeword slightly.

A. SHAMIR'S SECRET SHARING SCHEME

The threshold secret sharing schemes was presented independently by Shamir [26] and Blakley *et al.* [27] in 1979. Shamir's scheme uses polynomial interpolation, while Blakley's scheme is based on finite geometries. We demonstrate the Shamir threshold scheme here.

Secret sharing is a cryptosystem consisting of a distribution algorithm and a reconstruction algorithm. The Shamir's scheme of the distribution algorithm and the reconstruction algorithm are following,

Distribution Algorithm: let $\mathbb{F}_q$ be a field finite, q be a prime and $q > n$. $s, s \in \mathbb{F}_q$, is the secret to be shared in n participants $\{p_1, p_2, \ldots, p_n\}$,

1. A dealer D secretly choose (randomly and independently) $t-1$ elements of $\mathbb{F}_q$, $a_1, a_2, \ldots, a_{t-1}$;
2. For $1 \leq i \leq n$, D computes $y_i = f(x_i)$, where $f(x) = s + \sum_{j=1}^{t-1} a_j x^j$;
3. For $1 \leq i \leq n$, D chooses n distinct nonzero elements $x_1, x_2, \ldots, x_n, x_i \in \mathbb{F}_q$, and secretly distributes (x_i, y_i) to the participant p_i.

Reconstruction Algorithm: Without loss of generality, suppose that participants $p_1, p_2, \ldots, p_t$ want to determine the secret s. The Lagrange interpolation formula is an explicit formula for the polynomial $f(x)$ of degree at most $t-1$. The formula is as follows:

$$f(x) = \sum_{j=1}^{t} y_j \prod_{1 \le k \le t, k \ne j} \frac{x - x_k}{x_j - x_k}$$

The t participants know the shares $y_i = f(x_i)$, $1 \le i \le t$, and they can compute $s = f(0)$, that is,

$$s = \sum_{j=1}^{t} y_j \prod_{1 \le k \le t, k \ne j} \frac{x_k}{x_j - x_k}.$$

Therefore, any t or more than t participants altogether can reconstruct the secret s, while any less than t participants collusion can obtain no information about the s.

There is an alternative method, based on linear equation. The t participants can obtain t linear equations according $f(x) = s + \sum_{j=1}^{t-1} a_j x^j$. This can be written in matrix form as follows,

$$\begin{pmatrix} 1 & x_1 & \ldots & x_1^{t-1} \\ 1 & x_2 & \ldots & x_2^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_t & \ldots & x_t^{t-1} \end{pmatrix} \cdot \begin{pmatrix} s \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{pmatrix}.$$

The coefficient matrix A is a Vandermonde matrix and $rank(A) = t$, $s, a_1, \ldots, a_t$ is the unique solution. Hence, the t participants can obtain the secret s. In fact, the coefficient matrix of Shamir's secret sharing scheme is also the generator matrix of the Reed-Solomon code, and the multi-receiver authentication scheme of Safavi-Naini and Wang [6] is based on the Reed-Solomon code.

The (t, n) threshold secret sharing is far too simple for many applications because it assumes that every participant has equal privilege to the secret. Therefore, more research works considered the general secret sharing schemes. In this paper, we main consider multi-receiver authentication scheme for general access structure based on ideal linear code. The next section is the definition of linear code and the corresponding general secret sharing.

B. LINEAR CODE AND GENERAL SECRET SHARING

Definition 1 (Linear Code): Let $\mathbb{F}_q^{n+1}$ be the vector space over finite field $\mathbb{F}_q$. A linear subspace C of $\mathbb{F}_q^{n+1}$ is known as q-array linear code.

Let $\mathbf{c} = (c_0, c_1, \ldots, c_n) \in \mathbb{F}_q^{n+1}$ be a codeword of C. $\text{supp}(\mathbf{c}) = \{ i \mid i \in [0, n], c_i \ne 0\}$ is known as **support** of $\mathbf{c}$.

The **Hamming weight** $\text{Wt}(\mathbf{c})$ of $\mathbf{c}$ is defined as the number of non-zero coordinates, i.e.,

$$Wt(c) = \#\{c_i |\ c_i \ne 0, 0 \le i \le n\}.$$

The **minimum distance** $d(C)$ of C is the minimum **Hamming weight** of all non-zero vectors in C, that is,

$$d(C) = min\{Wt(c) |\ c \in C/\{0\}\}.$$

A $[n+1, k, d]$ linear code C is a linear subspace of $\mathbb{F}_q^{n+1}$ with dimension k and minimum distance d. Let $\mathbb{G} = (\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_n)$ be the generator matrix of C, that is, the row vector of $\mathbb{G}$ generate the linear code C.

The **dual code** $C^\perp$ of C is defined as

$$C^\perp = \{x \in \mathbb{F}_q^{n+1} |\ (x, c) = 0 \, for \, all \, c \in C\}.$$

Lemma 1: Suppose that C is a linear code, $\mathbb{H} = (h_0, h_1, \ldots, h_n)$ is the check matrix of C, the minimum distance of C is d if and only if any $d-1$ columns of $\mathbb{H}$ are linearly independent and there exist d linearly dependence.

Definition 2: A codeword $\mathbf{c} = (c_0, c_1, \ldots, c_n) \in \mathbb{F}_q^{n+1}$ is minimal if

i) $\mathbf{c}$ is a non-zero codeword whose leftmost nonzero component is 1;
ii) $\mathbf{c}$ covers no other codeword $\mathbf{c}'$ in C whose leftmost nonzero component is 1.

Definition 3 (General Secret Sharing): A general secret sharing scheme is a policy of breaking the secret, s, divided into n pieces $s_1, s_2, \ldots, s_n$ to be shared among the participants $P = \{p_1, p_2, \ldots, p_n\}$, with s_i secretly distributed to p_i such that

i) $S \subseteq P$ is a qualified subset of participants if the secret s can be reconstructed by the shares $\{s_i \mid p_i \in S\}$;
ii) $S' \subseteq P$ is an unqualified subset of participants if the secret s cannot be reconstructed by the shares $\{s_i \mid p_i \in S'\}$.

Suppose that a secret sharing scheme is constructed from C, the secret $s \in \mathbb{F}_q$ is to share among n participants, denoted by $p_1, p_2, \ldots, p_n$. To compute the shares of s, a dealer chooses randomly a vector $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1}) \in \mathbb{F}_q^k$ such that $\mathbf{u}\mathbf{g}_0 = s$, there are q^{k-1} such vector $\mathbf{u} \in \mathbb{F}_q^k$ and the dealer computes the codeword $\mathbf{s} = (s, s_1, \ldots, s_n) = \mathbf{u} \cdot \mathbb{G}$ in C. Then securely send s_i to participant p_i as share for $i = 1, 2, \ldots, n$.

In principle, every linear code can determine a secret sharing policy [3]. Noted that $\mathbf{u}\mathbf{g}_0 = s$, and it is easy to determine the secret s by the shares of S iff $\mathbf{g}_0 = \sum_{p_i \in S} x_i \, \mathbf{g}_i$.

Proposition 1: Let $\mathbb{G}$ be a generator matrix of linear code C. In the secret sharing scheme based on C, a set of shares $\{s_{i_1}, s_{i_2}, \ldots, s_{i_m}\}$ determine the secret s if and only if there is a codeword

$$(1, 0, \ldots, 0, c_{i_1}, 0, \ldots, 0, c_{i_m}, 0, \ldots, 0) \tag{1}$$

in the dual code $C^\perp$, where $c_{i_j} \ne 0$ for at least one j, $1 \le i_1 \le \cdots \le i_m \le n$ and $1 \le m \le n$.

If there exist a codeword as (1) in $C^\perp$, then $\mathbf{g}_0$ is a linear combination of $\mathbf{g}_{i_1}, \mathbf{g}_{i_2}, \ldots, \mathbf{g}_{i_m}$. That is,

$$\mathbf{g}_0 = -\sum_{j=1}^{m} c_{i_j} \cdot \mathbf{g}_{i_j}.$$

Then the participants $p_{i_1}, p_{i_2}, \ldots, p_{i_m}$ together can recover the secret s by

$$s = \mathbf{u} \cdot \mathbf{g}_0 = -\mathbf{u} \sum_{j=1}^{m} c_{i_j} \cdot \mathbf{g}_{i_j}$$
$$= -\sum_{j=1}^{m} c_{i_j} \cdot (\mathbf{u} \cdot \mathbf{g}_{i_j}) = -\sum_{j=1}^{m} c_{i_j} \cdot s_{i_j}.$$

A group of participants $A \subseteq [1, n]$ is known as qualified set if they can recover the secret by combining their shares, then any group of participants containing this group can also recover the secret. A group of participants is called a minimal access set if they can recover the secret with their shares, any of its proper subgroups cannot do so. $A \subseteq [1, n]$ is known as qualified set of linear code C if there is $\mathbf{c} \in C^{\perp}$ such that $\mathbf{c}_0 = 1$ and supp($\mathbf{c}$)$\subseteq A \cup \{0\}$, where supp($\mathbf{c}$) $= \{i \mid i \in [0, n], c_i \neq 0\}$.

All collection of qualified sets is known as **access structure**. Suppose $\Gamma = \{f_1, f_2, \ldots, f_z\}$ is an access structure, without loss of generality, we assume that no subset in Γ contains another subset of Γ. Then Γ is known as a **minimal access structure**.

A subset R of $[1, n]$ is known as an unqualified set if it can't recover the secret s. The collection of the unqualified sets is known as **adversary structure**. Let $\mathcal{R}$ denote the collection of all maximal unqualified set of Γ.

As [8], we consider which a coalition of malicious receivers can successfully make a substitution attack to a fixed receiver p_i and produce a fake authenticated message to be accepted by receiver p_i, thus we modify the definition of the minimal codeword slightly [4].

Definition 4: Let $C \in \mathbb{F}_q^{n+1}$ be a linear code and $j \in [1, n+1]$. A codeword c is called j-minimal if c is a non-zero codeword whose jth component is 1 and it covers no other codeword c' in C whose jth component is 1.

III. AUTHENTICATION SCHEME

In this section we develop multi-receiver authentication scheme for general access structure based on linear code. Firstly, we recall the general definition of multi-receiver authentication scheme. Most notably, in order to realize any access structure on multi-receiver authentication scheme, we introduce the algorithm to obtain the adversary structure $\mathcal{R}$ for the given access structure Γ, and then determine the generator matrix of the linear code.

A. GENERAL DEFINITION OF AUTHENTICATION SCHEME

In a multi-receiver authentication scheme, there is a trusted authority to generate and distribute the required keys. The scheme has three phases as following,

i) **Key Generation and Distribution.** The trusted authority center privately sends the private keys to the sender and the receivers, respectively.

ii) **Broadcast.** For a message m, the sender generates an authenticated message using his/her key and broadcasts the authenticated message.

iii) **Verification.** Each receiver verifies the received message.

Tang et al. demonstrate that finding linear codes for an access structure Γ is equivalent to solving a system of quadratic polynomial equations which is constructed from Γ and $\mathcal{R}$. Next we first introduce an algorithm for determining $\mathcal{R}$ from Γ [28].

B. ALGORITHM OF OBTAINING $\mathcal{R}$

For a more convenient description, the collection of participants $P = \{p_1, p_2, \ldots, p_n\}$ is denoted by $\{x_1, x_2, \ldots, x_n\}$ in the algorithm below. $Q = \{x_1^{b_1} \cdot x_2^{b_2} \cdot \cdots \cdot x_n^{b_n} \mid b_i \in \{0, 1\}\}$, $\Gamma = \{f_1, f_2, \ldots, f_m\}$ is a subset of Q. $F(\mathbf{x}) = \prod_{j=1}^{n} x_j$ and $R[l]$ is the lth polynomial of $\mathcal{R}$.

Example 1: Suppose $\Gamma = \{x_1x_2x_3, x_3x_4x_5, x_3x_5x_6\}$ is an access structure of a secret sharing scheme with participants $\{x_1, x_2, x_3, x_4, x_5, x_6\}$.

The maximal adversary structure is

$$\mathcal{R} = \{x_1x_2x_4x_5x_6, x_1x_3x_4x_6, x_2x_3x_4x_6, x_1x_3x_5, x_2x_3x_5\}.$$

C. DETERMINE LINEAR CODE FOR GIVEN ACCESS STRUCTURE

Suppose that given an access structure

$$\Gamma = \{f_1, f_2, \ldots, f_z\},$$

where $f_i \subseteq \{p_1, p_2 \ldots, p_n\}$ for $i = 1, \ldots, z$. We denote Γ by a matrix as following:

$$\Gamma = \begin{pmatrix} h_{11} & h_{12} & \ldots & h_{1n} \\ h_{21} & h_{22} & \ldots & h_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ h_{z1} & h_{z2} & \ldots & h_{zn} \end{pmatrix}.$$

where $h_{ij} \in \mathbb{F}_q^*$ if $p_j \in f_i$, else $h_{ij} = 0$ for $i \in [1, z], j \in [1, n]$. And define a matrix $\mathbb{H}_{z\times(n+1)}$ with form:

$$\mathbb{H} = (1 \ \ \Gamma) = \begin{pmatrix} 1 & h_{11} & h_{12} & \ldots & h_{1n} \\ 1 & h_{21} & h_{22} & \ldots & h_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & h_{z1} & h_{z2} & \ldots & h_{zn} \end{pmatrix}.$$

where all elements in the first column of $\mathbb{H}$ are 1.

We shall assume that the access structure mentioned in the rest of the paper is a minimal access structure, the adversary structure mentioned as following is a maximal adversary structure and each participant p_i is in some subset of Γ, therefore $\mathbb{H}$ has no columns with all 0.

Lemma 2 [24]: Suppose that $C \subseteq \mathbb{F}_q^{n+1}$ is any linear code. Then a subset $R \subseteq [1, n]$ is an unqualified set of C iff there is a codeword $\mathbf{c} = (c_0, c_1, \ldots, c_n) \in C$ such that $c_0 = 1$ and $c_i = 0$ for all $i \in R$.

According to [7], in fact, Lemma 2 gives a method for finding a linear code to realize a given access structure. Let $\mathbb{H}$ be defined as above where all $h_{ij} \in \mathbb{F}_q^*$ were unknown

Algorithm 1 Determining $\mathcal{R}$ From Γ

Input: $\Gamma = \{f_1, f_2, \ldots, f_m\}$ with participants $\{x_1, x_2, \ldots, x_n\}$
Output: $\mathcal{R}$

```
Initially R := {F(x)};
for i from 1 to m do
    R_temp := ∅;
    for l from 1 to |R| do
        if f_i | R[l] then
            R_temp := R_temp ∪ {R[l]/x_j | x_j divides f_i};
        else
            R_temp := R_temp ∪ {R[l]};
        end if
    end for
    R := Max(R_temp);
end for
```

for $p_j \in f_i$. Suppose that we have found the corresponding adversary structure of Γ by algorithm 1:

$$\mathcal{R} = \{R_1, R_2, \ldots, R_t\}.$$

We define matrix

$$\mathbb{G} = \begin{pmatrix} 1 & g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ 1 & g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & g_{t,1} & g_{t,2} & \cdots & g_{t,n} \end{pmatrix}.$$

where $g_{ij} = 0$ if $p_j \in R_i$ and $g_{ij} \in \mathbb{F}_q^*$ for $p_j \notin R_i$.

A linear code is ideal if the length of code is $n + 1$, where n is the number of participants. The following theorem demonstrates whether there exist an ideal linear code for a given access structure.

Theorem 1: There is a linear code for a given access structure Γ iff the following system of quadratic equation

$$\mathbb{G}\mathbb{H}^T = 0,$$

has a solution for $g_{ij} \in \mathbb{F}_q^*, p_j \in A_i$ and $h_{ij} \in \mathbb{F}_q^*, p_j \notin R_i$.

The theorem illustrates if the equation has a solution, then there exist an ideal linear code $C \in \mathbb{F}_q^{n+1}$ to realize the given access structure and the linear code C is the row span of matrix $\mathbb{G}$. In the ideal linear code, each participant in Γ owns only one component of the code, hence he owns only the corresponding a column of matrix $\mathbb{G}$ and matrix $\mathbb{H}$.

Our scheme is slightly different from the general definition of authentication scheme. In order to realize authentication scheme for general access structure based on ideal linear code, it first needs to call adversary structure generating algorithm to obtain $\mathcal{R}$ for the given general access structure Γ, and achieve the generator matrix of the linear code which is corresponding to the Γ.

D. AUTHENTICATED SCHEME

Suppose that given an access structure Γ, call algorithm 1 to obtain the corresponding adversary structure $\mathcal{R}$. According to the above, the ideal linear code C is determined by the matrix $\mathbb{G}$. Without loss of generality, suppose that the row of the matrix $\mathbb{G}$ are linearly independent, C is with minimum distance $d(C) \geqslant 2$, and the minimum distance of the dual code $C^\perp$ is $d(C^\perp) \geqslant 2$. The authenticated scheme is following,

i) **Generate Matrix.** Given an access structure $\Gamma = \{f1, \ldots, f_z\}$, and call algorithm 1 to generate $\mathcal{R} = \{R_1, R_2, \cdots, R_t\}$, according to the above definition to obtain the generator matrix

$$\mathbb{G} = \begin{pmatrix} 1 & g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ 1 & g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & g_{t,1} & g_{t,2} & \cdots & g_{t,n} \end{pmatrix}.$$

Make the matrix $\mathbb{G}$ public.

ii) **Key Generation and Distribution.** The trusted authority randomly chooses a matrix $\mathbb{P} \in \mathbb{F}_q^{(r+1)\times t}$

$$\mathbb{P} = \begin{pmatrix} p_{0,1} & p_{0,2} & \cdots & p_{0,t} \\ p_{1,1} & p_{1,2} & \cdots & p_{1,t} \\ \vdots & \vdots & \ddots & \vdots \\ p_{r,1} & p_{r,2} & \cdots & p_{r,t} \end{pmatrix},$$

and distributes $\mathbb{P}$ to sender.
Compute

$$K = \mathbb{P} \cdot \mathbb{G} = \begin{pmatrix} K_{00} & K_{01} & \ldots & K_{0,n} \\ K_{10} & K_{11} & \ldots & K_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ K_{r0} & K_{r1} & \ldots & K_{r,n} \end{pmatrix},$$

then distributes 1th to nth columns of K to receiver $p_1, p_2, \ldots, p_n$, respectively.

iii) **Broadcast.** For message $m \in \mathbb{F}_q$, the sender computes

$$T_j(m) = \sum_{v=0}^{r} p_{v,j} \cdot m^v$$

as the tag of m, where $j = 1, 2, \ldots, t$ and let $T(m) = (T_1(m), T_2(m), \ldots, T_t(m))$. Broadcast $M = (m, T(m))$.

iv) **Verification.** The receiver p_i, $i = 1, \ldots, n$, accepts the message $M = (m, T(m))$ if

$$\sum_{v=0}^{r} K_{v,i} \cdot m^v = \sum_{j=1}^{t} g_{j,i} \cdot T_j(m).$$

Correctness. The receiver p_i, $i = 1, \ldots, n$ receives the the message $M = (m, T(m))$ and computes by his/her private key $K_i = (K_{0i}, K_{1i}, \ldots, K_{ri})$.

They verify that

$$\begin{aligned} \sum_{v=0}^{r} K_{v,i} \cdot m^v &= \sum_{v=0}^{r} (p_{v,1} \cdot g_{1,i} + \cdots + p_{v,t} \cdot g_{t,i}) \cdot m^v \\ &= \sum_{v=0}^{r} (\sum_{j=1}^{t} p_{v,j} \cdot g_{j,i}) \cdot m^v \\ &= \sum_{j=1}^{t} (\sum_{v=0}^{r} p_{v,j} \cdot m^v) \cdot g_{j,i} \\ &= \sum_{j=1}^{t} T_j(m) \cdot g_{j,i}. \end{aligned}$$

In the authentication scheme we construct, a generator matrix $\mathbb{G}$ is determined for any given access structure and published, the trusted authority chooses randomly a matrix as the secret key and generates the private key using matrix $\mathbb{G}$, then he transmits the shares of private key to each receiver, and distributes secret key to the sender. The sender computes the tag of the message m with the secret key, and broadcast m and the tag. In the verification phase, each receiver can verify the integrity of m with his/her private key.

IV. SECURITY

In a traditional model of authenticated scheme, there are three parties involved: sender, receivers, and malicious group. When sender sends the messages to receivers by a public channel, the malicious group may fake or substitute the messages transmitted by the public channel. In this section, we analyze the security of the above schemes. Notice that a tagged message $(m', T'_1, \ldots, T'_t)$ is accepted by receiver p_i iff $\sum_{v=0}^{r} K_{v,i} \cdot (m')^v = \sum_{j=1}^{t} g_{j,i} \cdot T'_j(m)$. Therefore, if the malicious group makes a substitution attack to receiver p_i, they must know the label $\sum_{v=0}^{r} K_{v,i} \cdot (m')^v$ for $m' \in \mathbb{F}_q$. So the security of the scheme is similar with [9] that depends on the hardness of finding the secret key $\mathbb{P}$. However, the first column of the generate matrix of our scheme is all $'1'$, the number of malicious groups of our scheme is less than [8] that can corrupt receiver. Suppose that a group of k malicious receivers collaborate to recover $\mathbb{P}$ and make a substitution attack.

Without loss of generality, we assume that the malicious receivers are $p_1, p_2, \ldots, p_k$, $m_1, \ldots, m_r$ are the messages that are sent to each malicious receiver. Each malicious receiver p_i has some informations as following, $i = 1, 2, \ldots, k$,

$$\begin{pmatrix} K_{0i} \\ K_{1i} \\ \vdots \\ K_{ri} \end{pmatrix} = \mathbb{P} \begin{pmatrix} g_{1i} \\ g_{2i} \\ \vdots \\ g_{ti} \end{pmatrix},$$

and

$$\mathbb{P}^T \cdot \begin{pmatrix} 1 & 1 & \ldots & 1 \\ m_1 & m_2 & \ldots & m_r \\ \vdots & \vdots & \ddots & \vdots \\ m_1^r & m_2^r & \ldots & m_r^r \end{pmatrix} = \begin{pmatrix} T_1(m_1) & T_1(m_2) & \ldots & T_1(m_r) \\ T_2(m_1) & T_2(m_2) & \ldots & T_2(m_r) \\ \vdots & \vdots & \ddots & \vdots \\ T_t(m_1) & T_t(m_2) & \ldots & T_t(m_r) \end{pmatrix}$$

The group of malicious receivers, $p_1, p_2, \ldots, p_k$, combines their informations, and they have s system of linear equations that

$$\begin{cases} \mathbb{P}^T \cdot \begin{pmatrix} 1 & 1 & \ldots & 1 \\ m_1 & m_2 & \ldots & m_r \\ \vdots & \vdots & \ddots & \vdots \\ m_1^r & m_2^r & \ldots & m_r^r \end{pmatrix} = \begin{pmatrix} T_1(m_1) & \ldots & T_1(m_r) \\ T_2(m_1) & \ldots & T_2(m_r) \\ \vdots & \ddots & \vdots \\ T_t(m_1) & \ldots & T_t(m_r) \end{pmatrix} \\ \mathbb{P} \cdot \begin{pmatrix} g_{11} & g_{12} & \ldots & g_{1k} \\ g_{21} & g_{22} & \ldots & g_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ g_{t1} & g_{t2} & \ldots & g_{tk} \end{pmatrix} = \begin{pmatrix} K_{01} & K_{02} & \ldots & K_{0k} \\ K_{11} & K_{12} & \ldots & K_{1k} \\ \vdots & \vdots & \ddots & \vdots \\ K_{r1} & K_{r2} & \ldots & K_{rk} \end{pmatrix} \end{cases}$$

Lemma 3: Suppose that U is the subspace of $\mathbb{F}_q^t$ generated by $\{g_j | \ j = 1, 2, \ldots, k\}$, where g_j is the jth column of the generator matrix $\mathbb{G}$. If $\dim U \leq t - 1$, there exists q^{t-dimU} matrices $\mathbb{P}$ such that the above system of equations hold.

Proof: We would like to demonstrate that the malicious receivers combining their informations cannot determine the matrix $\mathbb{P}$. In the other words, the matrix satisfying the above equations is not unique.

The elements in matrix $\mathbb{P}$ can be treat as $t \times (r + 1)$ variables,

$$(p_{0,1}, \ldots, p_{r,1}, p_{0,2}, \ldots, p_{r,t})$$

and the above equations can be written in the following form,

$$\begin{cases} p_{0,1} + m_1 \cdot p_{1,1} + \cdots + m_1^r \cdot p_{r,1} + 0 \cdots + 0 = T_1(m_1) \\ \qquad \ldots \\ p_{0,1} + m_r \cdot p_{1,1} + \cdots + m_r^r \cdot p_{r,1} + 0 \cdots + 0 = T_1(m_r) \\ \qquad \vdots \\ p_{0,t} + m_r \cdot p_{1,t} + \cdots + m_r^r \cdot p_{r,t} + 0 \cdots + 0 = T_t(m_r) \\ g_{1,1} \cdot p_{0,1} + 0 + \cdots + 0 + g_{2,1} \cdot p_{0,2} + 0 + \cdots + 0 \\ \qquad + \cdots + g_{t,1} \cdot p_{0,t} + 0 \cdots + 0 = K_{01} \\ \qquad \ldots \\ g_{1,k} \cdot p_{0,1} + 0 + \cdots + 0 + g_{2,k} \cdot p_{0,2} + 0 + \cdots + 0 \\ \qquad + \cdots + g_{t,k} \cdot p_{0,t} + 0 \cdots + 0 = K_{0k} \\ \qquad \vdots \\ g_{1,k} \cdot p_{r,1} + 0 + \cdots + 0 + g_{2,k} \cdot p_{r,2} + 0 + \cdots + 0 \\ \qquad + \cdots + g_{t,k} \cdot p_{r,t} + 0 \cdots + 0 = K_{rk} \end{cases}$$

Suppose that

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ m_1 & m_2 & \ldots & m_r \\ \vdots & \vdots & \ddots & \vdots \\ m_1^r & m_2^r & \ldots & m_r^r \end{pmatrix} = M_r,$$

The coefficient matrix can be written as,

$$\begin{pmatrix} M_r^T & & & \\ & M_r^T & & \\ & & \ddots & \\ & & & M_r^T \\ g_{1,1}\cdot E & g_{2,1}E & \dots & g_{t,1}\cdot E \\ \vdots & \ddots & \vdots & \\ g_{1,k}\cdot E & g_{2,k}\cdot E & \dots & g_{t,k}\cdot E \\ \vdots & \vdots & \vdots & \\ \vdots & \vdots & \vdots & \\ g_{1,k}\cdot E & g_{2,k}\cdot E & \dots & g_{t,k}\cdot E \end{pmatrix},$$

where E is the identity matrix with $rank(E) = r+1$. Notice that the generated space by rows of M_r is contained in the space $\mathbb{F}_q^{r+1}$ generated by $g_{i,j}\cdot E$ if $g_{i,j}\neq 0$ for $i\in[1,t], j\in[1,k]$. Therefore, the rank of the coefficient matrix is $t\cdot r + dimU$. However, $dimU \leq t-1$, the system of equations above has $q^{t\cdot(r+1)-t\cdot r-dimU} = q^{t-dimU}$ solutions.

From the lemma 3, the security of the scheme is as following.

Theorem 2: The above scheme is an unconditionally secure multi-receiver authentication scheme for general access structure against a coalition of up to $d(C^{\perp})-2$ malicious receivers in which each key can be used to authenticate up to r messages.

Proof: We main consider the substitution attack. Suppose that the group of malicious receivers are $p_1,\dots,p_k$, the sender has transmitted $m_1,\dots,m_r$ to every receiver. The malicious receivers want to generate a valid tag $b_1g_{1,k+1}+\cdots+b_tg_{t,k+1}$ for m_{r+1} such that it is accepted by receiver p_{k+1}. They try to guess the value of $K_{0,k+1}+K_{1,k+1}\cdot m_{r+1}+\cdots+K_{1,k+1}\cdot m_{r+1}^r$ and construct $b_1g_{1,k+1}+\cdots+b_tg_{t,k+1}$ such that

$$b_1g_{1,k+1}+\cdots+b_tg_{t,k+1} = K_{0,k+1}+\cdots+K_{1,k+1}\cdot m_{r+1}^r.$$

Suppose that $d(C^{\perp})$ is the minimum distance of $C^{\perp}$. According to Lemma 1, any $d(C^{\perp})-1$ column of the generator matrix $\mathbb{G}$ are linearly independent, and there exist $d(C^{\perp})$ column of $\mathbb{G}$ linearly dependent.

$$\mathbb{G} = \begin{pmatrix} 1 & g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ 1 & g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & g_{t,1} & g_{t,2} & \cdots & g_{t,n} \end{pmatrix} = (g_0, g_1, \dots, g_n),$$

$$K = \mathbb{P}\cdot\mathbb{G} = \begin{pmatrix} K_{00} & K_{01} & \dots & K_{0,n} \\ K_{10} & K_{11} & \dots & K_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ K_{r0} & K_{r1} & \dots & K_{r,n} \end{pmatrix} = (K_0, K_1, \dots, K_n),$$

We assume that $g_1, g_2\dots, g_k$ are linearly independent. If g_{k+1} is not contained in the subspace of $\mathbb{F}_q^t$ generated by $1th, 2th, \dots, k+1th$ column of $\mathbb{G}$,

Suppose that $k = d(C^{\perp})-1$, we assume that $g_1, g_2\dots, g_k$ are linearly independent and add g_{k+1}, $g_1, g_2\dots, g_{k+1}$ are still linearly independent, the malicious receivers $p_1,\dots,p_k$ cannot obtain any information about K_{k+1}. If $g_1, g_2\dots, g_k$ are linearly independent and only $g_0, g_1\dots, g_k$ are linearly dependent, the malicious receivers $p_1,\dots,p_k$ cannot make a substitution attack to any another receiver.

If g_{k+1} is contained in the subspace of $\mathbb{F}_q^t$ generated by $g_1, g_2\dots, g_k$ of $\mathbb{G}$, the $k+1th$ column g_{k+1} can be linear representation by

$$a_1g_1+\cdots+a_kg_k.$$

The malicious receivers $p_1,\dots,p_k$ can make a substitution attack to p_{k+1} by combining their k private key,

$$\begin{aligned} K_{k+1} &= P\cdot g_{k+1} = P\cdot(a_1g_1+\cdots+a_kg_k) \\ &= a_1P\cdot g_1+\cdots+a_kP\cdot g_k \\ &= a_1\cdot K_1+\cdots+a_k\cdot K_k \end{aligned}$$

Therefore, k is most up to $d(C^{\perp})-2$. According to Lemma 3, there exists $q^{k-d(\perp)+2}$ matrices $\mathbb{P}$ satisfying the equations above.

The information held by the group of the malicious receivers allows them to calculate q equally likely different tags for m_{r+1} and hence their probability of success is $1/q$. Our scheme is main to realize multi-receiver authentication scheme for general access structure based on ideal linear code. The first column of the generator matrix of the ideal linear code is all '1', there are less malicious groups than F. Fu (2014) that can corrupt any a receiver in our scheme.

Theorem 3: The group that is minimal substitution receivers to receiver p_j is determined completely by j-minimal codeword whose the first component is 0 in $C^{\perp}$.

Proof: The coalition of malicious receivers V can successfully make a substitution attack to receiver p_j, by Proposition 1 and Theorem 3, if and only if g_j is contained in the subspace of $\mathbb{F}_q^t$ generated by $\{g_i|\ p_i\in V\}$, where g_i represents the i-th column of the generator matrix $\mathbb{G}$. Their private key of receiver p_j is a linear combination of the V receivers private keys, and any a participant cannot obtain the information of the first column of $\mathbb{P}$. Therefore, receiver p_j can accept the faked message determined completely by j-minimal codeword whose the first component is 0 in $C^{\perp}$.

Corollary 1: The group that can fake an authenticated message being accepted by receiver p_j contains any support of j-minimal codeword excluding $\{j\}$ in $C^{\perp}$.

In fact, it is NP-hard to determine all substitution groups, which is corresponding to j-minimal codeword, to receiver p_j. Further, by theorem 3, the minimal substitution group to p_j is determined by j-minimal codeword whose the first component must be 0. Therefore, the number of minimal substitution groups to any receiver p_j in our scheme are less than J. Zhang and F.Fu.

Example 2: Given an access structure Γ={(1, 2, 4, 5), (1, 2, 3, 6), (3, 4, 5, 6)}.

Then $\mathcal{R}$ ={(2, 4, 5, 6), (2, 3, 5, 6), (2, 3, 4, 6), (2, 3, 4, 5), (1, 4, 5, 6), (1, 3, 5, 6), (1, 3, 4, 6), (1, 3, 4, 5), (1, 2, 5, 6), (1, 2, 3, 5), (1, 2, 4, 6), (1, 2, 3, 4)}

Let

$$\mathbb{H} = (1 \ \ \Gamma) = \begin{pmatrix} 1 & h_{11} & h_{12} & 0 & h_{14} & h_{15} & 0 \\ 1 & h_{21} & h_{22} & h_{23} & 0 & 0 & h_{26} \\ 1 & 0 & 0 & h_{33} & h_{34} & h_{35} & h_{36} \end{pmatrix}.$$

$$\mathbb{G} = \begin{pmatrix} 1 & g_{11} & 0 & g_{13} & 0 & 0 & 0 \\ 1 & g_{21} & 0 & 0 & g_{24} & 0 & 0 \\ 1 & g_{31} & 0 & 0 & 0 & g_{35} & 0 \\ 1 & g_{41} & 0 & 0 & 0 & 0 & g_{46} \\ 1 & 0 & g_{52} & g_{53} & 0 & 0 & 0 \\ 1 & 0 & g_{62} & 0 & g_{64} & 0 & 0 \\ 1 & 0 & g_{72} & 0 & 0 & g_{75} & 0 \\ 1 & 0 & g_{82} & 0 & 0 & 0 & g_{86} \\ 1 & 0 & 0 & g_{93} & g_{94} & 0 & 0 \\ 1 & 0 & 0 & 0 & g_{10,4} & 0 & g_{10,6} \\ 1 & 0 & 0 & g_{11,3} & 0 & g_{11,5} & 0 \\ 1 & 0 & 0 & 0 & 0 & g_{12,5} & g_{12,6} \end{pmatrix}.$$

There exists the solution for the equation $\mathbb{G}\mathbb{H}^T = 0$ in $\mathbb{F}_q^7$. That is, $g_{64} = g_{82}^{-1}(-g_{72}g_{94} + g_{82}g_{94})$, $g_{62} = g_{72}$, $g_{53} = g_{72}^{-1}(g_{72} - g_{82})g_{93}$, $g_{52} = g_{82}$, $g_{46} = g_{86}$, $g_{35} = g_{75}$, $g_{31} = g_{82}^{-1}g_{41}g_{72}$, $g_{24} = g_{64}$, $g_{21} = g_{31}$, $g_{13} = g_{53}$, $g_{12,6} = g_{31}g_{86}(g_{31} - g_{41})^{-1}$, $g_{12,5} = g_{41}g_{75}(-g_{31} + g_{41})^{-1}$, $g_{11,5} = g_{12,5}$, $g_{11,3} = g_{93}$, $g_{11} = g_{41}$, $g_{10,6} = g_{12,6}$, $g_{10,4} = g_{94}$, $h_{11} = -g_{41}^{-1}$, $h_{12} = g_{31}h_{11}g_{72}^{-1}$, $h_{14} = (-1-g_{31}h_{11})g_{64}^{-1}$, $h_{15} = -g_{12,5}^{-1}$, $h_{21} = (g_{12,6}-g_{86})h_{11}g_{12,6}^{-1}$, $h_{22} = -g_{41}h_{12}h_{21}$, $h_{23} = (-1 - g_{41}h_{21})g_{53}^{-1}$, $h_{26} = -g_{12,6}^{-1}$, $h_{33} = g_{31}h_{23}(g_{31} - g_{41})^{-1}$, $h_{34} = h_{14} + g_{93}h_{14}h_{33}$, $h_{35} = h_{15} + g_{93}h_{15}h_{33}$, $h_{36} = -g_{93}h_{26}h_{33}$

Let $\mathbb{F}_q = \mathbb{F}_5$. The $r = 3$ messages are $m_1 = 1$, $m_2 = 2$, $m_3 = 3$. Suppose that the matrix $\mathbb{G}$ of the ideal linear code for given access structure is

$$\mathbb{G} = \begin{pmatrix} 1 & 2 & 0 & 3 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 4 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 3 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 2 \\ 1 & 0 & 4 & 3 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 4 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 & 3 & 0 \\ 1 & 0 & 4 & 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & 2 & 3 & 0 & 0 \\ 1 & 0 & 0 & 0 & 3 & 0 & 3 \\ 1 & 0 & 0 & 2 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 3 \end{pmatrix}.$$

the generator matrix is

$$\mathbb{G}' = \begin{pmatrix} 1 & 2 & 0 & 3 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 2 \\ 1 & 0 & 4 & 3 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 & 3 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 1 & 0 \end{pmatrix}.$$

and the dual code $C^\perp$ has minimum distance $d(C^\perp) = 5$. The corrupted receivers are at most 3.

TABLE 2. Minimal substitution groups to receiver p_3 in example 2.

	Participants' number	the Number of Malicious Group	Support
J.Zhang et al.' scheme	7	3 (2 0 0 1 2 1 4) (3 2 1 1 0 0 4) (0 1 3 1 1 3 4)	3 {2,3,5,6,7} {1,5,6,7} {1,2,3,7}
Our scheme	6	1 (0 1 3 1 1 3 4)	1 {2,3,5,6,7}

The trusted authority randomly chooses $P \in \mathbb{F}_q^{4\times 5}$, for instance,

$$\mathbb{P} = \begin{pmatrix} 3 & 2 & 2 & 0 & 2 \\ 0 & 4 & 3 & 0 & 2 \\ 0 & 1 & 2 & 3 & 1 \\ 3 & 3 & 0 & 1 & 3 \end{pmatrix}.$$

The trusted authority computes

$$K = \mathbb{P} \cdot \mathbb{G}' = \begin{pmatrix} 4 & 0 & 3 & 4 & 0 & 2 & 4 \\ 4 & 3 & 2 & 3 & 0 & 2 & 3 \\ 2 & 2 & 3 & 4 & 4 & 1 & 2 \\ 0 & 2 & 0 & 2 & 3 & 3 & 1 \end{pmatrix}.$$

and distributes the i-th column of K to the receiver p_i as his/her private key.

Suppose p_1, p_2, p_3 are corrupted and they have the authenticated messages. They have information about the key matrix $\mathbb{P}$:

$$\begin{cases} \mathbb{P}^T \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 4 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 \\ 0 & 3 & 4 \\ 2 & 1 & 4 \\ 4 & 0 & 4 \\ 3 & 4 & 3 \end{pmatrix} \\ \mathbb{P} \begin{pmatrix} 2 & 0 & 3 \\ 2 & 0 & 0 \\ 0 & 4 & 3 \\ 0 & 0 & 2 \\ 0 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 3 & 4 \\ 3 & 2 & 3 \\ 2 & 3 & 4 \\ 2 & 0 & 2 \end{pmatrix} \end{cases}$$

This system of linear equations has 25 solutions.

Suppose that the corrupted receiver would like to make a substitution attack to receiver p_3. The 4-minimal codewords in $C^\perp$ is following:

(2001214), (3211004), (0131134),

4-minimal codeword with the first component of 0 is the only one: (0 1 3 1 1 3 4).

The support of 4-minimal codeword with the first component of 0 is {2, 3, 5, 6, 7}.

So minimal substitution group to receiver p_3 must contain the support {2, 3, 5, 6, 7}, in fact, just all receivers together except receiver p_3 could make a substitution attack.

As it sees the example above, it is 3 groups that can make a minimal substitution attack to receiver 3 based on J. Zhang and F.Fu, however, it is just 1 group that can make a minimal substitution attack based on our scheme.

V. CONCLUSION

In this paper, we present a multi-receiver authentication scheme for any a given access structure that is corresponding an ideal linear code. The scheme is unconditionally secure and allows r messages to be authenticated with each receiver own private key. There are less number of malicious groups than F. Fu (2014) that can corrupt any a receiver, because the malicious group to any a receiver is corresponding to the minimal codeword in $C^{\perp}$ whose the first component is 0. In the future, we will investigate the consistent characteristics of the access structure that can realize an ideal linear code, which is inspired by the designed example above.

REFERENCES

[1] H. Chen and R. Cramer, "Algebraic geometric secret sharing schemes and secure multi-party computations over small fields," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 2006, pp. 521–536.
[2] Y. Desmedt, Y. Frankel, and M. Yung, "Multi-receiver/multi-sender network security: Efficient authenticated multicast/feedback," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, 1992.
[3] C. Ding and J. Yuan, "Covering and secret sharing with linear codes," in *Proc. 4th Int. Conf. Discrete Math. Theor. Comput. Sci. (DMTCS)*, Dijon, France, in Lecture Notes in Computer Science, vol. 2731. Springer, Jul. 2003, pp. 11–25.
[4] J. L. Massey, "Minimal codewords and secret sharing," in *Proc. 6th Joint Swedish-Russian Workshop Inf. Theory*, 1993, pp. 276–279.
[5] R. J. Mceliece and D. V. Sarwate, "On sharing secrets and reed-solomon codes," *Commun. ACM*, vol. 24, no. 9, pp. 583–584, Sep. 1981.
[6] R. Safavi-Naini and H. Wang, "New results on multi-receiver authentication codes," in *Proc. EUROCRYPT*, vol. 1403, 1998, pp. 527–541.
[7] C. Tang, S. Gao, and C. Zhang, "The optimal linear secret sharing scheme for any given access structure," *J. Syst. Sci. Complex.*, vol. 26, no. 4, pp. 634–649, Aug. 2013.
[8] J. Zhang, X. Li, and F.-W. Fu, "Multi-receiver authentication scheme for multiple messages based on linear codes," in *Proc. ISPEC*, vol. 8434, 2014, pp. 287–301.
[9] A. G. Reddy, A. K. Das, E.-J. Yoon, and K.-Y. Yoo, "A secure anonymous authentication protocol for mobile services on elliptic curve cryptography," *IEEE Access*, vol. 4, pp. 4394–4407, 2016.
[10] M. Karthigaiveni and B. Indrani, "An efficient two-factor authentication scheme with key agreement for IoT based E-health care application using smart card," *J. Ambient Intell. Humanized Comput.*, pp. 1–12, Oct. 2019, doi: 10.1007/s12652-019-01513-w.
[11] G. Wang, C. Liu, Y. Dong, P. Han, H. Pan, and B. Fang, "IDCrypt: A multi-user searchable symmetric encryption scheme for cloud applications," *IEEE Access*, vol. 6, pp. 2908–2921, 2018.
[12] A. Alrawais, A. Alhothaily, C. Hu, X. Xing, and X. Cheng, "An attribute-based encryption scheme to secure fog communications," *IEEE Access*, vol. 5, pp. 9131–9138, 2017.
[13] I.-C. Lin, M.-S. Hwang, and L.-H. Li, "A new remote user authentication scheme for multi-server architecture," *Future Gener. Comput. Syst.*, vol. 19, no. 1, pp. 13–22, Jan. 2003.
[14] X. Wang and F.-W. Fu, "Multi-receiver authentication scheme with hierarchical structure," *IET Inf. Secur.*, vol. 11, no. 5, pp. 223–229, Sep. 2017.
[15] Y. Qiang and D. Yi, "Information-theoretic lower bounds for multi-receiver authentication codes and their combinatorial characterization," *Acta Mathematicae Applicatae Sinica*, vol. 22, no. 1, pp. 545–554, 1999.
[16] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," *Electron. Commun. Jpn.*, vol. 72, no. 9, pp. 56–64, 1989.
[17] M. Stadler, "Publicly verifiable secret sharing," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, 1996, pp. 190–199.
[18] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions," in *Proc. Conf. Theory Appl. Cryptogr.*, Santa Barbara, CA, USA. Springer, 1990, pp. 27–35.
[19] C. Carlet, C. Ding, and J. Yuan, "Linear codes from perfect nonlinear mappings and their secret sharing schemes," *IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 2089–2102, Jun. 2005.
[20] J. Yuan and C. Ding, "Secret sharing schemes from three classes of linear codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 206–212, Jan. 2006.
[21] Y. Song, Z. Li, Y. Li, and J. Li, "A new multi-use multi-secret sharing scheme based on the duals of minimal linear codes," *Secur. Commun. Netw.*, vol. 8, no. 2, pp. 202–211, Jan. 2015.
[22] X. Wang, C. Xiang, and F.-W. Fu, "Secret sharing schemes for compartmented access structures," *Cryptogr. Commun.*, vol. 9, no. 5, pp. 625–635, Sep. 2017.
[23] C. Ding and A. Salomaa, "Secret sharing schemes with nice access structures," *Fundamenta Informaticae*, vol. 73, no. 12, pp. 51–63, 2006.
[24] J. Pieprzyk and X.-M. Zhang, "Ideal threshold schemes from MDS codes," in *Proc. Int. Conf. Inf. Secur. Cryptol.*, 2002, pp. 253–263.
[25] J. Martífarré and C. Padró, "Ideal secret sharing schemes whose minimal qualified subsets have at most three participants," *Des. Codes Cryptogr.*, vol. 52, pp. 1–14, Jul. 2009.
[26] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 1, pp. 612–613, 1979.
[27] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Int. Workshop Manag. Requirements Knowl. (MARK)*, Jun. 1979.
[28] C. Tang, Q. Xu, and G. Hu, "Finding the maximal adversary structure from any given access structure," *Inf. Sci.*, vol. 508, pp. 329–342, Jan. 2020.
[29] Y. Harbi, Z. Aliouat, A. Refoufi, S. Harous, and A. Bentaleb, "Enhanced authentication and key management scheme for securing data transmission in the Internet of Things," *Ad Hoc Netw.*, vol. 94, Nov. 2019, Art. no. 101948.
[30] M. Cui, D. Han, and J. Wang, "An efficient and safe road condition monitoring authentication scheme based on fog computing," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9076–9084, Oct. 2019.
[31] M. Qi and J. Chen, "Anonymous biometrics-based authentication with key agreement scheme for multi-server environment using ECC," *Multimed Tools Appl*, vol. 78, no. 19, pp. 27553–27568, Oct. 2019.
[32] X. Li, F. Wu, S. Kumari, L. Xu, A. K. Sangaiah, and K.-K.-R. Choo, "A provably secure and anonymous message authentication scheme for smart grids," *J. Parallel Distrib. Comput.*, vol. 132, pp. 242–249, Oct. 2019, doi: 10.1016/j.jpdc.2017.11.008.

QIUXIA XU received the B.Sc. degree from the Hunan Institute of Science and Technology and the M.Sc. degree from Guangzhou University, where she is currently pursuing the Ph.D. degree. Her research interests include coding, secret sharing, and secure multiparty computation.

CHUNMING TANG received the Ph.D. degree in applied mathematics from the Academy of Mathematics and Systems Science, Chinese Academy of Sciences, China, in 2004. He is currently a Professor with the College of Mathematics and Information Science, Guangzhou University, China. His research interests include cryptography, secure multiparty computing, and outsourced computing. He is a member of the Chinese Association for Cryptologic Research.

JINGTONG WANG received the M.Sc. degree from the School of Mathematics, Xiangtan University, in 2001. He is currently pursuing the Ph.D. degree in mathematics with the Prof. Yanming Wang's group, Sun Yat-sen University. He is an internal Associate Professor with the School of Mathematics and Statistics, Hunan University of Technology and Business, Changsha, China. His current research interests include algebra and information security, and the Internet financial risk.