CONCURRENCY AND COMPUTATION: PRACTICE AND EXPERIENCE
Concurrency Computat.: Pract. Exper. 0000; **00**:1–22
Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/cpe

Homomorphic Authentication Codes for Network Coding

Zhaohui Tang*

Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore

SUMMARY

Authentication codes (A-codes) are a well studied technique to provide unconditionally secure authentication. An A-code is defined by a map that associates a pair formed by a message and a key to a tag. A-codes linear in the keys have been studied for application to distributed authentication schemes. In this paper, we address the dual question, namely the study of A-codes that are linear in the messages. This is usually an undesired property, except in the context of network coding. Regarding these A-codes, we derive some lower bounds on security parameters when key space is known. We also show a lower bound on key size when security parameter values are given (with some special properties) and construct some codes meeting the bound. We finally present a variant of these codes that authenticate multiple messages with a same key while preserving unconditional security. Copyright © 0000 John Wiley & Sons, Ltd.

Received . . .

KEY WORDS: Authentication codes; unconditional security; network coding; pollution attack.

1. INTRODUCTION

We consider the following network coding scenario: a source is transmitting data over a network that implements linear network coding, that is, each node transmits on its outgoing edges linear combinations of the packets it received on its incoming edges.

In order to perform authentication, a tag, or signature, should be appended to messages sent over the network. As mentioned in [2] (and references therein), classical authentication schemes are not possible: since network coding is used, the received packets are most likely different than those sent, and thus one cannot check a tag or signature without accessing the original packets. An alternative would be to first decode the message, however, the receiver does not know a priori which of the packets it receives are corrupted, thus it will have to try to decode subsets of received messages until it can first decode, then only check the authentication, and start all over if authentication fails. Yet, authentication mechanisms are indeed necessary, especially in the context of pollution attacks, to prevent rogue packets to be combined to legitimate data, thus propagating bogus vectors.

When a node performs coding on its input vectors, the newly generated vector will have as tag a linear combination of the received tags. It is desirable to use a homomorphic authentication mechanism, such as [3, 4] or [5] particularly for wireless sensor networks, where the linear combination of the received tags is indeed the proper tag corresponding to the newly created vector. A receiver can then perform authentication directly on the received packets.

This is a property which is usually undesirable, since it permits an adversary to forge illegitimate data with a valid tag, by exactly computing a linear combination of observed

*Correspondence to: E-mail: TANG0209@e.ntu.edu.sg packets. However in this setting, any linear combination of the sent messages and their corresponding tag might be considered as a legitimate vector, in that they will serve the right purpose: provide linear equations to decode the original message. This means that the authentication is then not really performed on the messages themselves, but rather on the subspace spanned by the data vectors, an idea which is now well understood in the context of network coding authentication.

The idea of considering the vector space spanned by the data vectors is also present in the context of network coding error correction (e.g. [6]), an alternative way to deal with insertion of errors in the network.

In this paper, we are interested in the study of authentication codes (see Section 2 for more details), which fall in the category of unconditional security. Most works in the literature related to network coding authentication focus on either computational security, or error-correction, see [7] for one example of unconditional scheme that deals with multiple receivers.

1.1. Organization and contributions

In Section 2, we recall authentication codes, particular those linear in the keys. We call an A-code *homomorphic* if it is linear in messages. We present a definition of *homomorphic A-codes* with parameters introduction in Section 3.

The contributions of this paper mainly exist in Sections 4, 5 and 6. In Section 4 we show some bounds on security parameters for a general homomorphic A-code (see Theorem 1) and a lower key size bound for a homomorphic A-code (with some special properties) (see Theorem 2). Afterwards, in Section 5, we construct some codes meeting the key size bound (see Theorem 3 and Corollary 1). In Section 6 we propose a variant of homomorphic A-code that authenticates multiple messages with a same key while preserving unconditional security.

We review the related work in Section 7. Oggier and Fathi [7] proposed a multi-receiver A-code for a network coding setting. We firstly recall their proposed A-code and point out that it is not homomorphic. We then twist it a little bit to make it homomorphic (see Lemma 6) and finally evaluate the key size and security parameters for the resulting homomorphic A-code (see Lemma 8).

We conclude and propose future work in Section 8.

2. LINEAR A-CODES

A-codes (standing for authentication codes) were first proposed in [8], while the framework for unconditionally secure authentication was established in the seminal work by Simmons [9].

A *systematic* A-code (or A-code *without secrecy*) consists of a quadruple $(\mathcal{S}, \mathcal{K}, \mathcal{A}, f)$ where $\mathcal{S}, \mathcal{K}, \mathcal{A}$ denote the source space, key space and tag space respectively and f is a function from $\mathcal{S} \times \mathcal{K} \to \mathcal{A}$. An A-code is used to perform authentication as follows: the sender and the receiver secretly share a common key $\mathbf{k} \in \mathcal{K}$. To send a message $\mathbf{s} \in \mathcal{S}$, the sender firstly generates a tag $\mathbf{t} = f(\mathbf{s}, \mathbf{k}) \in \mathcal{A}$ and transmits the message-tag pair $(\mathbf{s}, \mathbf{t})$ to the receiver. The receiver checks the authenticity of the received message $\mathbf{s}$ by verifying whether the received message-tag pair $(\mathbf{s}, \mathbf{t})$ satisfies $\mathbf{t} = f(\mathbf{s}, \mathbf{k})$. If the equality holds, $\mathbf{s}$ is accepted; otherwise it is rejected.

Let $(\mathcal{S}, \mathcal{K}, \mathcal{A}, f)$ define an A-code. For each key $\mathbf{k} \in \mathcal{K}$, the authentication map $f : \mathcal{S} \times \mathcal{K} \to \mathcal{A}$ induces a mapping $\psi_{\mathbf{k}} : \mathcal{S} \to \mathcal{A}$, given by

$$\psi_{\mathbf{k}}(\mathbf{s}) = f(\mathbf{s}, \mathbf{k}),\ \forall\ \mathbf{s} \in \mathcal{S}$$

and similarly, for each $\mathbf{s} \in \mathcal{S}$, the same map f induces another mapping $\phi_{\mathbf{s}} : \mathcal{K} \to \mathcal{A}$, defined by

$$\phi_{\mathbf{s}}(\mathbf{k}) = f(\mathbf{s}, \mathbf{k}),\ \forall\ \mathbf{k} \in \mathcal{K}.$$

In both cases, the A-code is characterized by the families $\{\psi_{\mathbf{k}}, \mathbf{k} \in \mathcal{K}\}$ and $\{\phi_{\mathbf{s}}, \mathbf{s} \in \mathcal{S}\}$ respectively.

In [10], linear A-codes were studied, where $\{\phi_{\mathbf{s}}, \mathbf{s} \in \mathcal{S}\}$ forms a family of $\mathbb{F}_q$-linear mappings from $\mathcal{K}$ to $\mathcal{A}$, and $\mathcal{K}$ and $\mathcal{A}$ are thus assumed to be vector spaces over the finite field $\mathbb{F}_q$. This means that by fixing a basis of $\mathcal{K}$ and one of $\mathcal{A}$, every $\phi_{\mathbf{s}}$ can be represented by a matrix S with coefficients in $\mathbb{F}_q$ such that

$$\phi_{\mathbf{s}}(\mathbf{k}) = \mathbf{k}S,\ \forall\ \mathbf{k} \in \mathcal{K}.$$

Advantages of A-codes which are linear in keys were discussed [10] in the context of distributed authentication schemes.

One could consider the reverse scenario, where linearity in messages is asked instead of linearity in keys. This in turn means that $\{\psi_{\mathbf{k}}, \mathbf{k} \in \mathcal{K}\}$ becomes a family of $\mathbb{F}_q$-linear mappings from $\mathcal{S}$ to $\mathcal{A}$, that $\mathcal{S}$ and $\mathcal{A}$ are vector spaces over $\mathbb{F}_q$, and that every $\psi_{\mathbf{k}}$ can be written as a matrix K such that

$$\psi_{\mathbf{k}}(\mathbf{s}) = \mathbf{s}K,\ \forall\ \mathbf{s} \in \mathcal{S}.$$

The security of A-codes is usually evaluated via two security parameters: (1) the probability P_I of impersonation, which represents the probability of an adversary successfully inserting a new message tag pair without prior observation, and (2) the probability P_S of substitution, where an adversary first observes a valid message tag pair $(\mathbf{s}, \mathbf{t})$ and then succeeds in inserting $(\mathbf{s}', \mathbf{t}')$ with $\mathbf{s} \neq \mathbf{s}'$. Formally [10]

$$P_I = \max_{\mathbf{s}\in\mathcal{S}, \mathbf{t}\in\mathcal{A}} P((\mathbf{s}, \mathbf{t}) \text{ valid}) \tag{1}$$

where a message tag pair $(\mathbf{s}, \mathbf{t})$ is *valid* if there exists a key $\mathbf{k} \in \mathcal{K}$ such that

$$\mathbf{t} = f(\mathbf{s}, \mathbf{k}),$$

while

$$P_S = \max_{\mathbf{s}\in\mathcal{S}, \mathbf{t}\in\mathcal{A}} \max_{\mathbf{s}\neq\mathbf{s}', \mathbf{t}'} P((\mathbf{s}', \mathbf{t}') \text{ valid} \mid (\mathbf{s}, \mathbf{t}) \text{ observed}). \tag{2}$$

One easily observes that there is a problem with P_S: suppose that $(\mathbf{s}, \mathbf{t})$ is observed, then the adversary can pick $\mathbf{s}' = \alpha\mathbf{s}$ where $\alpha \in \mathbb{F}_q$, $\alpha \neq 1$. Now using the $\mathbb{F}_q$-linearity of the A-code in $\mathbf{s}$, we have that

$$f(\mathbf{s}', \mathbf{k}) = \psi_{\mathbf{k}}(\alpha\mathbf{s}) = \alpha\mathbf{s}K = \alpha\psi_{\mathbf{k}}(\mathbf{s}),$$

and the adversary can forge the tag $\mathbf{t}' = \alpha\mathbf{t}$. The message-tag pair $(\mathbf{s}', \mathbf{t}') = (\alpha\mathbf{s}, \alpha\mathbf{t})$ will be accepted and $P_S = 1$. This explains why the literature on classical A-codes has avoided this scenario so far. We will show below that this apparent disadvantage becomes useful in the context of network coding, where A-codes linear in messages make sense, with however a proper reformulation of P_S.

3. HOMOMORPHIC NETWORK CODING A-CODES

Suppose now that transmissions occur over a network. Given a file $\mathbf{s}$ to be sent to a receiver, the source (or sender) cuts the file into m packets $\mathbf{s}_1, \dots, \mathbf{s}_m$ of length say n, which can be represented as vectors with coefficients in $\mathbb{F}_q$, that is, $\mathbf{s}_i \in \mathbb{F}_q^n$, $i = 1, \dots, m$. We assume that a linear network code over $\mathbb{F}_q$ is used, where every node in the network computes an $\mathbb{F}_q$-linear combination of the received vectors on its incoming edges, before forwarding the resulting linear combination on its outgoing edges. Decoding at the receiver is performed, to recover the file $\mathbf{s}$.

Since each received message is a linear combination of the input, it is possible to give the receiver a so-called transfer matrix, which describes how the output linearly depends on the input message. Alternatively, before transmission, each vector $\mathbf{s}_i$ can be appended a vector $\mathbf{e}_i$, where $\mathbf{e}_i$ denotes a whole zero vector of length m, with a 1 at the ith position. The vectors $(\mathbf{s}_i, \mathbf{e}_i) \in \mathbb{F}_q^{n+m}$, $i = 1, \dots, m$ are then sent over the network, and the receiver can use the m

DOI: 10.1002/cpe

last symbols to recover the linear transformations the vector went through. In both cases, the receiver needs to obtain m non-corrupted linearly independent vectors encoding $\mathbf{s}$ to be able to decode.

Let V denote the vector space spanned by the $\mathbf{v}_i$, where $\mathbf{v}_i$ denotes a transmitted packet, which is either $\mathbf{s}_i$ or $(\mathbf{s}_i, \mathbf{e}_i)$. Note that when V is the span of the vectors $(\mathbf{s}_1, \mathbf{e}_1), \ldots, (\mathbf{s}_m, \mathbf{e}_m)$, it forms a vector space of dimension m since by construction, the addition of the $\mathbf{e}_i$ vectors ensure that the $(\mathbf{s}_i, \mathbf{e}_i)$ are linearly independent. When $V = \text{span}(\mathbf{s}_1, \ldots, \mathbf{s}_m)$, it is a vector space of dimension at most m.

We use an A-code $\{\psi_{\mathbf{k}},\ \mathbf{k} \in \mathcal{K}\}$ which is linear in messages, as described in the previous section, for authentication purposes. By authenticating every $\mathbf{v}_i$, we consequently provide an authentication for the subspace V. More precisely, we define a (q, n, m) *homomorphic A-code* as an A-code which can be used to authenticate any m-dimensional subspace $V \subseteq \mathcal{S}$ when $\mathcal{S}$ is an n-dimensional vector space over $\mathbb{F}_q$.

Definition 1
An A-code $(\mathcal{S}, \mathcal{K}, \mathcal{A}, f)$ is a (q, n, m)-homomorphic A-code if

i) $\mathcal{S}$ and $\mathcal{A}$ are finite-dimensional vector spaces over $\mathbb{F}_q$, with $\dim(\mathcal{S}) = n$,
ii) for every m-dimensional subspace $V \subseteq \mathcal{S}$, and every $\mathbf{v} = \sum_{i=1}^{m} \alpha_i \mathbf{v}_i \in V$, $f(\mathbf{v}, \mathbf{k}) = \psi_{\mathbf{k}}(\mathbf{v})$ satisfies
$$f(\sum_{i=1}^{m} \alpha_i \mathbf{v}_i, \mathbf{k}) = \sum_{i=1}^{m} \alpha_i f(\mathbf{v}_i, \mathbf{k}).$$

The second property is a rephrasing of the fact that $\psi_{\mathbf{k}}$ is linear in messages. In what follows, we will assume that $\mathcal{S} = \mathbb{F}_q^n$, $\mathcal{A} = \mathbb{F}_q^t$ and $\mathcal{K} \subseteq \mathbb{F}_q^{n \times t}$. It might be convenient to think of $\{\psi_{\mathbf{k}}\}$ as a set of $|\mathcal{K}|$ matrices of size $n \times t$ parameterized by $|\mathcal{K}|$ keys.

Given a homomorphic A-code $(\mathcal{S}, \mathcal{K}, \mathcal{A}, f)$, the tag generation and verification are similar to that of classic A-codes. Assume that the recipient shares a private key $\mathbf{k} \in \mathcal{K}$ with the source, message authentication is then carried out as shown in Figure 1. The security of homomorphic A-codes can be evaluated via three security parameters P_I, $P_{I_{sub}}$ and P_S.

- **Tag Generation:** The sender generates a tag $\mathbf{t}_i = f(\mathbf{v}_i, \mathbf{k}) \in \mathcal{A}$ for each of $\mathbf{v}_i$ for $i = 1, \ldots, m$.
- **Combination:** Assume that each intermediate node receives some message-tag pair $(\mathbf{x}_j, \mathbf{t}_{\mathbf{x}_j})$ for some index j, where each $\mathbf{x}_j$ is already a linear combination of $\mathbf{v}_i$. The intermediate node computes $\sum_j \alpha_j \mathbf{t}_{\mathbf{x}_j}$ as the tag $\mathbf{t}_{\mathbf{y}}$ corresponding to an output vector $\mathbf{y} = \sum_j \alpha_j \mathbf{x}_j$, where the sum is over some subset of the received tags.
- **Verification:** The recipient takes as input a received message-tag pair $(\mathbf{v}, \mathbf{t})$ and the shared key $\mathbf{k}$, and checks if $\mathbf{t} = f(\mathbf{v}, \mathbf{k})$. If the equation holds, the recipient accepts $(\mathbf{v}, \mathbf{t})$; otherwise it rejects. Note that indeed, any output $\mathbf{v}$ can be written as $\sum_{i=1}^{m} g_{\mathbf{v}i} \mathbf{v}_i$. We call $(g_{\mathbf{v}1}, \ldots, g_{\mathbf{v}m})$ as a *global encoding vector* of $\mathbf{v}$.

Figure 1. Definition of homomorphic A-code scheme.

1) P_I represents the success probability of *message impersonation attack* where an adversary forges a valid tag for a message $\mathbf{0} \neq \mathbf{v} \in \mathcal{S}$ without prior observation.
A message impersonation attack is similar to the impersonation attack of a classical authentication code. The adversary blindly sends to the receiver a message $\mathbf{v} \in \mathcal{S}$ to which it appends a random tag $\mathbf{t}$ picked in $\mathcal{A}$. The source is in fact sending some subspace V from $\mathcal{S}$, but the adversary does not know which one. In all cases, the adversary has to generate a valid tag. Even if the attack is successful in that a valid tag is generated, it does not mean that the attack actually hurts the receiver, since there is still a chance that the message randomly chosen by the adversary was in fact inside V. We will thus from now on focus on the probability of guessing a valid tag. Note that if $(\mathbf{v}, \mathbf{t})$ is accepted,

DOI: 10.1002/cpe

then a linear combination involving $(\mathbf{v}, \mathbf{t})$ would be accepted as well, since

$$f(\mathbf{x} + \alpha\mathbf{v}, \mathbf{k}) = f(\mathbf{x}, \mathbf{k}) + \alpha f(\mathbf{v}, \mathbf{k}) = \mathbf{t_x} + \alpha\mathbf{t}$$

where $\mathbf{t_x}$ is a valid tag corresponding to a legitimate packet $\mathbf{x}$. Conversely, and for the same reason, if $(\mathbf{v}, \mathbf{t})$ is not accepted, then neither would a linear combination of $(\mathbf{v}, \mathbf{t})$ mixed with other packets. Thus (1) holds, and assuming that $\mathbf{k}$ and $\mathbf{v}$ are uniformly distributed, becomes [10]:

$$P_I = \max_{\mathbf{v}\in\mathcal{S},\mathbf{t}\in\mathcal{A}} \frac{|\mathbf{k} \in \mathcal{K} \mid f(\mathbf{v}, \mathbf{k}) = \mathbf{t}|}{|\mathcal{K}|} = \max_{\mathbf{v}\in\mathcal{S},\mathbf{t}\in\mathcal{A}} \frac{|\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}|}{|\mathcal{K}|}.$$

2) $P_{I_{sub}}$ represents the success probability of *subspace impersonation attack* where an adversary creates a valid tag for a previously unseen m-dimensional subspace $V = \text{span}(\mathbf{v}_1, \cdots, \mathbf{v}_m)$. A subspace-tag $(V, (\mathbf{t}_1, \cdots, \mathbf{t}_m))$ is *valid* if there exists a key $\mathbf{k} \in \mathcal{K}$ such that

$$\mathbf{t}_i = f(\mathbf{v}_i, \mathbf{k}), 1 \leq i \leq m.$$

Formally, we have:

$$P_{I_{sub}} = \max_{V\subseteq\mathcal{S},\mathbf{t}_i\in\mathcal{A}} P((V, (\mathbf{t}_1, \cdots, \mathbf{t}_m)) \text{ valid}). \tag{3}$$

Moreover, assuming that $\mathbf{k}$ and V are uniformly distributed, we have:

$$P_{I_{sub}} = \max_{V,\mathbf{t}_i} \frac{|\{\mathbf{k} \in \mathcal{K} \mid f(\mathbf{v}_i, \mathbf{k}) = \mathbf{t}_i\}|}{|\mathcal{K}|} = \max_{V,\mathbf{t}_i} \frac{|\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}_i) = \mathbf{t}_i\}|}{|\mathcal{K}|}.$$

To our best knowledge, it is a first time to introduce $P_{I_{sub}}$ as a security parameter in A-codes arena. Indeed, usually it is not an important criterion unless applications can be found as in our network coding scenario where an adversary possibly intends to forge entire files (mathematically formalized as subspaces) that will be accepted as authentic. We here use $P_{I_{sub}}$ to measure the probability of an adversary successfully forging an entire file to be accepted in a network coding transmission.

3) P_S denotes the success probability of *subspace substitution attack* where an adversary forges a valid tag for message $\mathbf{v}$ when he/she observes a tag for an m-dimensional subspace $V = \text{span}(\mathbf{v}_1, \cdots, \mathbf{v}_m)$ with $\mathbf{v} \notin V$.

A subspace substitution attack in a homomorphic A-code is different from a substitution attack in a classical authentication code. To see why, for the former one we need to consider subspaces instead of messages in the latter one: the adversary sees a subspace V and its tags, and it has to fake a vector $\mathbf{v} \notin V$, since replacing a linear combination of the $\mathbf{v}_i$ by another is possible and is not a problem. Furthermore, the maximization has to be done over all possible observed subspaces instead of observed messages.

A subspace substitution attack is certainly different from a message impersonation attack. In a message impersonation attack, the adversary performs an attack blindly, and in the context of network coding does not know which subspace $V \subset \mathcal{S}$ is being sent. Thus the best strategy consists of guessing a valid tag. If then the message randomly picked is in V, then even though the tag was guessed successfully, the attack will not hurt. In the case of subspace substitution instead, the adversary mounts an attack after observing some transmissions. Since we assume the adversary observes all the m messages sent from the source, that is $V = \text{span}(\mathbf{v}_1, \ldots, \mathbf{v}_m)$, we have

$$P_S = \max_{V,\mathbf{t}_i} \max_{\mathbf{v}\notin V,\mathbf{t}} P((\mathbf{v}, \mathbf{t}) \text{ valid } |(\mathbf{v}_1, \mathbf{t}_1), \ldots, (\mathbf{v}_m, \mathbf{t}_m) \text{ observed}).$$

Note that since the adversary knows the network code, knowing any linearly independent vectors is the same as knowing $\mathbf{v}_1, \ldots, \mathbf{v}_m$, and vice-versa.

Apart knowing which subspace is sent, another difference with a message impersonation attack is that a single key $\mathbf{k}$ is used to sign V, that is $\mathbf{t}_i = f(\mathbf{v}_i, \mathbf{k})$ for all i, thus the

adversary might guess some information about $\mathbf{k}$, and consequently be able to fake a message tag pair with $\mathbf{t} = f(\mathbf{v}, \mathbf{k})$, $\mathbf{v} \notin V$, that will be validated with $\mathbf{k}$.
Assuming again that the keys and messages are uniformly distributed, we get, for $i = 1, \ldots, m$

$$P_S = \max_{V, \mathbf{t}_i} \max_{\mathbf{v} \notin V, \mathbf{t}} \frac{|\{\mathbf{k} \in \mathcal{K} \mid f(\mathbf{v}_i, \mathbf{k}) = \mathbf{t}_i, f(\mathbf{v}, \mathbf{k}) = \mathbf{t}\}|}{|\{\mathbf{k} \in \mathcal{K} \mid f(\mathbf{v}_i, \mathbf{k}) = \mathbf{t}_i\}|} = \max_{\mathbf{v} \notin V, V} \max_{\mathbf{t}, \mathbf{t}_i} \frac{|\{\mathbf{k} \mid \psi_{\mathbf{k}}(\mathbf{v}_i) = \mathbf{t}_i\} \cap \{\mathbf{k} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}\}|}{|\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}_i) = \mathbf{t}_i\}|}$$

where

$$\{\mathbf{k} \mid \psi_{\mathbf{k}}(\mathbf{v}_i) = \mathbf{t}_i,\ i = 1, \ldots, m\} = \bigcap_{i=1}^{m} \{\mathbf{k} \mid \psi_{\mathbf{k}}(\mathbf{v}_i) = \mathbf{t}_i\}.$$

When adopting homomorphic A-code into linear network coding for authentication, it is always assumed that the source space, tag space, and the subspace to authenticate are all given as a priori, in other words, the parameters q, n, m, t are fixed. The performance of a (q, n, m)-homomorphic A-code is thus determined by the efficiency (in terms of storage cost) parameter $|\mathcal{K}|$, and three security parameters $P_I, P_{I_{sub}}, P_S$. We certainly expect high security (that is, small $P_I, P_{I_{sub}}, P_S$) and small storage cost (namely, small $|\mathcal{K}|$), however, in fact high security always requires big storage cost. Therefore, it would be interesting to study a trade-off between efficiency and security. In the next section, we show some lower bounds on the three security parameters when key space is given and a lower bound on key size when security parameter values are provided.

4. BOUNDS

4.1. Definitions and notations

We represent a random variable $\widetilde{\mathcal{W}}$ as the collection of all message-tag pairs in a homomorphic A-code $\{\psi_{\mathbf{k}}, \mathbf{k} \in \mathcal{K}\}$, that is, $\widetilde{\mathcal{W}} = \{w = (\mathbf{v}, \mathbf{t}) : \mathbf{v} \in \mathcal{S}, \mathbf{t} \in \mathcal{A}\}$.[†] With this notation, we call w is *valid* and/or $\mathbf{k}$ *incident* with w if there exists a $\mathbf{k} \in \mathcal{K}$ such that $\mathbf{t} = \psi_{\mathbf{k}}(\mathbf{v})$. Particularly, we represent $\mathcal{W}$ as the collection of all the *valid* message-tag pairs in $\{\psi_{\mathbf{k}}, \mathbf{k} \in \mathcal{K}\}$.
In order to study $P_{I_{sub}}$ and P_S, we introduce a sequence $\overline{w} = (\overline{w_1}, \cdots, \overline{w_m})$ where each $\overline{w_i} \in \mathcal{W}$. We call a sequence $\overline{w}$ *valid* if $\overline{w_i}$'s are linearly independent from each other in $\mathbb{F}_q$ and there exists a $\mathbf{k} \in \mathcal{K}$ incident with $\overline{w_i}$ for all i; in this situation, we call $\mathbf{k}$ *incident* with the sequence $\overline{w}$. We use $\overline{\mathcal{W}}^m = \overline{\mathcal{W}_1} \times \cdots \times \overline{\mathcal{W}_m}$ to denote the collection of all such *valid* sequences $\overline{w} = (\overline{w_1}, \cdots, \overline{w_m})$ with $\overline{w_i} \in \overline{\mathcal{W}_i}(1 \leq i \leq m)$. For any valid sequence $(\overline{w_1}, \cdots, \overline{w_m}) = \overline{w} \in \overline{\mathcal{W}}^m$, we introduce another element $w' \in \mathcal{W}$; we call w' is *valid when* $\overline{w}$ *observed* if it satisfies that $w' \notin \mathrm{span}(\overline{w_1}, \cdots, \overline{w_m})$ and there exists a $\mathbf{k} \in \mathcal{K}$ incident with $w', \overline{w_i}(1 \leq i \leq m)$. We use a random variable $\mathcal{W}'$ to denote the collection of all such w''s for $\overline{\mathcal{W}}^m$.

We follow some notations from [11] and [12] in the whole article. For any random variable X, Y, Z, we use following notations for probability distributions induced by a current system. We use $P(x)$ to denote the probability distribution when $X = x$; $P(x, y)$ to denote the probability distribution when $X = x$ and $Y = y$; $P(y|x)$ the conditional probability of $Y = y$ when provided $X = x$; $H(X)$ the entropy of X; $H(Y|X)$ the conditional entropy of Y given X; $I(Y; X)$ the mutual information between Y and X; and $I(Z; Y|X)$ the conditional mutual information of Z and Y given X.

4.2. Bounds on $P_I, P_{I_{sub}}$ and P_S

In this section, we show some bounds on security parameters for a general homomorphic A-code when $\mathcal{K}$ is given.

[†] Here, certainly we can directly use $(\mathcal{S}, \mathcal{A})$ instead of $\widetilde{W}$, however, we adopt the shorter notation $\widetilde{\mathcal{W}}$ for expression convenience.

Theorem 1
Let $P_I, P_{I_{sub}}, P_S$ be defined as above in Section 3, we have:

$$(i)\ \ P_I \geq 2^{-I(\mathcal{K};\mathcal{W})};\ \ (ii)\ \ P_{I_{sub}} \geq 2^{-I(\mathcal{K};\overline{\mathcal{W}}^m)};\ \ (iii)\ \ P_S \geq 2^{-I(\mathcal{W}';\mathcal{K}|\overline{\mathcal{W}}^m)}.$$

Proof

(i) We define a characteristic function $\mathcal{X}_I(w, \mathbf{k})$ on $\widetilde{\mathcal{W}} \times \mathcal{K}$ by:

$$\mathcal{X}_I(w, \mathbf{k}) = \begin{cases} 1 & \text{if } \mathbf{k} \text{ is incident with } w; \\ 0 & \text{otherwise.} \end{cases}$$

From the definition of P_I, we have:

$$P_I = \max_{w \in \widetilde{\mathcal{W}}} \{P(w \text{ valid})\} \geq \sum_{w \in \widetilde{\mathcal{W}}} P(w)P(w \text{ valid}). \tag{4}$$

On the other hand, we have:

$$\begin{aligned} I(\mathcal{K}; \widetilde{\mathcal{W}}) &= \sum_{w \in \widetilde{\mathcal{W}}, \mathbf{k} \in \mathcal{K}} P(w, \mathbf{k}) \log \frac{P(w, \mathbf{k})}{P(w)P(\mathbf{k})} = \sum_{w \in \widetilde{\mathcal{W}}, \mathbf{k} \in \mathcal{K}} P(w)P(\mathbf{k}|w) \log \frac{P(w, \mathbf{k})}{P(w)P(\mathbf{k})} \\ &= \sum_{\substack{w \in \widetilde{\mathcal{W}} \\ P(w) \neq 0}} P(w) \sum_{\mathbf{k} \in \mathcal{K}} P(\mathbf{k}|w) \log \frac{P(w, \mathbf{k})}{P(w)p(\mathbf{k})} = \sum_{\substack{w \in \widetilde{\mathcal{W}} \\ P(w) \neq 0}} P(w) \sum_{\mathbf{k} \in \mathcal{K}} P(\mathbf{k}|w) \log \frac{P(w)P(\mathbf{k}|w)}{P(w)P(\mathbf{k})} \\ &= \sum_{w \in \widetilde{\mathcal{W}}, P(w) \neq 0} P(w) \sum_{\mathbf{k} \in \mathcal{K}} P(\mathbf{k}|w) \log \frac{P(\mathbf{k}|w)}{P(\mathbf{k})} \end{aligned}$$

We note here that, when $P(w) \neq 0$, if $\mathcal{X}_I(w, \mathbf{k}) = 0$, then $P(\mathbf{k}|w) = 0$. So, the summation taken over $\mathcal{K}$ above is restricted to all $\mathbf{k}$ for which $\mathcal{X}_I(w, \mathbf{k}) = 1$. Henceforth, we have:

$$I(\mathcal{K}; \widetilde{\mathcal{W}}) = \sum_{w \in \widetilde{\mathcal{W}}, P(w) \neq 0} P(w)\ (\sum_{\mathbf{k} \in \mathcal{K}} P(\mathbf{k}|w)\mathcal{X}_I(w, \mathbf{k}) \log \frac{P(\mathbf{k}|w)\mathcal{X}_I(w, \mathbf{k})}{P(\mathbf{k})\mathcal{X}_I(w, \mathbf{k})}\ ).$$

By log-sum inequality, we furthermore have:

$$I(\mathcal{K}; \widetilde{\mathcal{W}}) \geq \sum_{w \in \widetilde{\mathcal{W}}, P(w) \neq 0} P(w)\ (\sum_{\mathbf{k} \in \mathcal{K}} P(\mathbf{k}|w)\mathcal{X}_I(w, \mathbf{k})) \log \frac{\sum_{\mathbf{k} \in \mathcal{K}} P(\mathbf{k}|w)\mathcal{X}_I(w, \mathbf{k})}{\sum_{\mathbf{k} \in \mathcal{K}} P(\mathbf{k})\mathcal{X}_I(w, \mathbf{k})}. \tag{5}$$

Again, as we have observed, for each w, if $P(w) \neq 0$ and $\mathcal{X}_I(w, \mathbf{k}) = 0$, then $P(\mathbf{k}|w) = 0$. This implies

$$\sum_{\mathbf{k} \in \mathcal{K}} P(\mathbf{k}|w)\mathcal{X}_I(w, \mathbf{k}) = 1 \tag{6}$$

and

$$\sum_{\mathbf{k} \in \mathcal{K}} P(\mathbf{k})\mathcal{X}_I(w, \mathbf{k}) = P(w \ \text{ valid}). \tag{7}$$

Based on (6) and (7) above, we continue (5) and have:

$$I(\mathcal{K}; \widetilde{\mathcal{W}}) \geq \ \ -\sum_{w \in \widetilde{\mathcal{W}}} P(w) \log_{\mathbf{k} \in \mathcal{K}} P(\mathbf{k})\mathcal{X}_I(w, \mathbf{k}) = -\sum_{w \in \widetilde{\mathcal{W}}} P(w) \log P(w \ \text{ valid}). \tag{8}$$

We now return to investigate P_I shown in (4). By Jensen's inequality, it follows that

$$\log P_I \geq \sum_{w \in \widetilde{\mathcal{W}}} P(w) \log P(w \text{ valid}) \tag{9}$$

Considering (8) together with (9), we have:

$$P_I \geq 2^{-I(\mathcal{K};\widetilde{\mathcal{W}})}.$$

Furthermore, it is obvious to see that $I(\mathcal{K};\widetilde{\mathcal{W}}) = I(\mathcal{K};\mathcal{W})$. Indeed, if we write $I(\mathcal{K};\widetilde{\mathcal{W}})$ as $I(\mathcal{K};\widetilde{\mathcal{W}}) = I(\mathcal{K};\mathcal{W}) + I(\mathcal{K};\widehat{\mathcal{W}'})$ where $\widehat{\mathcal{W}'} = \widetilde{\mathcal{W}} \backslash \mathcal{W}$, then it holds trivially that $I(\mathcal{K};\widetilde{\mathcal{W}'}) = 0$.
Finally, we have $P_I \geq 2^{-I(\mathcal{K};\widetilde{\mathcal{W}})} = 2^{-I(\mathcal{K};\mathcal{W})}$ and thus complete the proof of (i) in the theorem.

(ii) We denote $\mathcal{W}^m = \mathcal{W} \times \cdots \times \mathcal{W}$ as the collection of all m-tuple elements, each of which is from $\mathcal{W}$; formally, $\mathcal{W}^m = \{(w_1, \ldots, w_m) : w_i \in \mathcal{W}, 1 \leq i \leq m\}$. We can prove the inequality (10) below, in a quite similar way as the proof above for (i) (we don't repeat the proof details here due to space constraints.):

$$P_{I_{sub}} \geq 2^{-I(\mathcal{K};\mathcal{W}^m)}. \tag{10}$$

Furthermore, we claim that

$$I(\mathcal{K};\mathcal{W}^m) = I(\mathcal{K};\overline{\mathcal{W}}^m). \tag{11}$$

Indeed, if we write $\underline{\mathcal{W}^m} = \mathcal{W}^m \backslash \overline{\mathcal{W}}^m$, we can prove that all the mutual information between $\mathcal{K}$ and $\underline{\mathcal{W}^m}$ is included in the mutual information between $\mathcal{K}$ and $\overline{\mathcal{W}}^m$, which proves our claim (11). We demonstrate the claim by investigating a random sequence $(y_1, \cdots, y_m) = y \in \underline{\mathcal{W}^m}$. There are two cases:

> Case 1: if there is any key $\mathbf{k}$ incident with all the m elements $y_1, \ldots, y_m$ (in this case, y_i's are not all linearly independent, which leads to $y \notin \overline{\mathcal{W}}^m$); then in this case there always exists a sequence $(x_1, \cdots, x_m) = x \in \overline{\mathcal{W}}^m$ such that $\mathbf{k}$ is incident with x and $y_i \in \text{span}(x_1, \cdots, x_m), 1 \leq i \leq m$; therefore the the information contained in y which is useful for the adversary to disclose the key $\mathbf{k}$, can be considered as a proper subset of and thus included in the useful information contained in x; in other words, with holding this additional y, the adversary cannot have more information helpful for disclosing $\mathbf{k}$ than holding only x.
> Case 2: if there is any key $\mathbf{k}$ incident with $j < m$ of the m elements, say, they are $y_{i_1}, \cdots, y_{i_j}$; then similar to Case 1 above, we can always find a sequence $(x_1, \cdots, x_m) = x \in \overline{\mathcal{W}}^m$ such that $\mathbf{k}$ is incident with x and $y_{i_h} \in \text{span}(x_1, \cdots, x_m), 1 \leq h \leq j$; therefore the information contained in y which can help the adversary reveal the key $\mathbf{k}$, can be regarded as a proper subset of and thus included in the helpful information contained in x; in other words, with holding this additional y, the adversary cannot have more information helpful for disclosing $\mathbf{k}$ than holding only x.

Since the above analysis can be generalized into all sequences $y \in \underline{\mathcal{W}^m}$, we henceforth demonstrate that all the mutual information between $\mathcal{K}$ and $\underline{\mathcal{W}^m}$ is included in the mutual information between $\mathcal{K}$ and $\overline{\mathcal{W}}^m$.
Combining (10) and (11), we finally have $P_{I_{sub}} \geq 2^{-I(\mathcal{K};\overline{\mathcal{W}}^m)}$ and thus complete the proof of (ii) in the theorem.

(iii) We define a characteristic function $\mathcal{X}_S(w', \overline{w}, \mathbf{k})$ on $\mathcal{W}' \times \overline{\mathcal{W}}^m \times \mathcal{K}$ by :

$$\mathcal{X}_S(w', \overline{w}, \mathbf{k}) = \begin{cases} 1 & \text{if } \mathbf{k} \text{ is incident with } w' \text{ and } \overline{w}; \\ 0 & \text{otherwise.} \end{cases}$$

For convenience of expression, we later employ "Δ" as a condition identical to: "$w' \notin \mathrm{span}(\overline{w_1}, \cdots, \overline{w_m})$". According to the definition of P_S, we have:

$$P_S = \max_{\substack{\overline{w}\in\overline{\mathcal{W}}^m \\ w'\in\mathcal{W}',\Delta}} \{P(w' \text{ valid } |\overline{w} \text{ observed}\} \geq \sum_{\overline{w}\in\overline{\mathcal{W}}^m} P(\overline{w}) \sum_{\substack{\Delta, \\ w'\in\mathcal{W}'}} P(w'|\overline{w})P(w' \text{ valid}|\overline{w} \text{ observed}). \tag{12}$$

On the other hand, we compute $I(\mathcal{W}';\mathcal{K}|\overline{\mathcal{W}}^m)$ as below:

$$I(\mathcal{W}';\mathcal{K}|\overline{\mathcal{W}}^m) = \sum_{\mathbf{k}\in\mathcal{K}, w'\in\mathcal{W}', \overline{w}\in\overline{\mathcal{W}}^m,\Delta} P(w', \mathbf{k}, \overline{w}) \log \frac{P(w', \mathbf{k}|\overline{w})}{P(w'|\overline{w})P(\mathbf{k}|\overline{w})}$$

$$= \sum_{\mathbf{k}\in\mathcal{K}, w'\in\mathcal{W}', \overline{w}\in\overline{\mathcal{W}}^m,\Delta} P(w', \overline{w})P(\mathbf{k}|w', \overline{w}) \log \frac{P(w'|\overline{w})P(\mathbf{k}|w', \overline{w})}{P(w'|\overline{w})P(\mathbf{k}|\overline{w})}$$

$$= \sum_{w'\in\mathcal{W}', \overline{w}\in\overline{\mathcal{W}}^m,\Delta, P(w',\overline{w})\neq 0} P(w', \overline{w}) \sum_{\mathbf{k}\in\mathcal{K}} P(\mathbf{k}|w', \overline{w}) \log \frac{P(\mathbf{k}|w', \overline{w})}{P(\mathbf{k}|\overline{w})}.$$

We note here that, when $P(w', \overline{w}) \neq 0$, if $\mathcal{X}_I(w', \overline{w}, \mathbf{k}) = 0$, then $P(\mathbf{k}|w', \overline{w}) = 0$. So, the summation taken over $\mathcal{K}$ above is restricted to all $\mathbf{k}$ for which $\mathcal{X}_I(w', \overline{w}, \mathbf{k}) = 1$. Henceforth, we have:

$$I(\mathcal{W}';\mathcal{K}|\overline{\mathcal{W}}^m) = \sum_{\substack{w'\in\mathcal{W}', \overline{w}\in\mathcal{W}^m \\ \Delta, P(w',\overline{w})\neq 0}} P(w', \overline{w}) \sum_{\mathbf{k}\in\mathcal{K}} P(\mathbf{k}|w', \overline{w})\mathcal{X}_S(w', \overline{w}, \mathbf{k}) \log \frac{P(\mathbf{k}|w', \overline{w})\mathcal{X}_S(w', \overline{w}, \mathbf{k})}{P(\mathbf{k}|\overline{w})\mathcal{X}_S(w', \overline{w}, \mathbf{k})}).$$

By log-sum inequality, we furthermore have:

$$I(\mathcal{W}';\mathcal{K}|\overline{\mathcal{W}}^m) \geq \sum_{\substack{w'\in\mathcal{W}', \overline{w}\in\mathcal{W}^m \\ \Delta, P(w',\overline{w})\neq 0}} P(w', \overline{w}) \sum_{\mathbf{k}\in\mathcal{K}} P(\mathbf{k}|w', \overline{w})\mathcal{X}_S(w', \overline{w}, \mathbf{k})(\log \frac{\sum_{\mathbf{k}\in\mathcal{K}} P(\mathbf{k}|w', \overline{w})\mathcal{X}_S(w', \overline{w}, \mathbf{k})}{\sum_{\mathbf{k}\in\mathcal{K}} P(\mathbf{k}|\overline{w})\mathcal{X}_S(w', \overline{w}, \mathbf{k})}). \tag{13}$$

Again, as we have observed, for each $(w', \overline{w})$ pair, if $P(w', \overline{w}) \neq 0$ and $\mathcal{X}_S(w', \overline{w}, \mathbf{k}) = 0$, then $P(\mathbf{k}|w', \overline{w}) = 0$. This implies

$$\sum_{\mathbf{k}\in\mathcal{K}} P(\mathbf{k}|w', \overline{w})\mathcal{X}_S(w', \overline{w}, \mathbf{k}) = 1, \tag{14}$$

and

$$\sum_{\mathbf{k}\in\mathcal{K}} P(\mathbf{k}|\overline{w})\mathcal{X}_S(w', \overline{w}, \mathbf{k}) = P(w' \text{ valid}|\overline{w} \text{ observed}). \tag{15}$$

Based on (14) and (15), we continue (13) and have:

$$I(\mathcal{W}';\mathcal{K}|\overline{\mathcal{W}}^m) \geq \sum_{w'\in\mathcal{W}', \overline{w}\in\overline{\mathcal{W}}^m,\Delta} P(w', \overline{w}) \log P(w' \text{ valid}|\overline{w} \text{ observed})$$

$$= -\sum_{\overline{w}\in\overline{\mathcal{W}}^m} P(\overline{w}) \sum_{w'\in\mathcal{W}',\Delta} P(w'|\overline{w}) \log P(w' \text{ valid}|\overline{w} \text{ observed}) \tag{16}$$

We now return to the computation of P_S shown in (12). By Jensen's inequality, we have:

$$\log P_S \geq -\sum_{\overline{w}\in\overline{\mathcal{W}}^m} P(\overline{w}) \sum_{w'\in\mathcal{W}',\Delta} P(w'|\overline{w}) \log P(w' \ \text{valid}|\overline{w} \ \text{observed}) \tag{17}$$

Combining (16) and (17), we have

$$P_S \geq 2^{-I(\mathcal{W}';\mathcal{K}|\overline{\mathcal{W}}^m)}.$$

We therefore finish the proof of (iii) in the theorem.

□

4.3. Bounds on $|\mathcal{K}|$

In this part, we derive a bound on $|\mathcal{K}|$ for a special class of homomorphic A-codes, that is, we require $P_{I_{sub}} \leq (P_I)^m$ in $\{\psi_{\mathbf{k}}, \mathbf{k}\in\mathcal{K}\}$.
If we denote $P_D = \max\{P_I, P_S\}$ and γ as a pre-determined value (for security consideration in application), then we have the following theorem for $|\mathcal{K}|$.

Theorem 2
Given a (q, n, m)-homomorphic A-code $\{\psi_{\mathbf{k}}, \mathbf{k}\in\mathcal{K}\}$ where $P_{I_{sub}} \leq (P_I)^m$ and $P_D \leq \frac{1}{\gamma}$, we have $|\mathcal{K}| \geq \gamma^n$ in $\{\psi_{\mathbf{k}}, \mathbf{k}\in\mathcal{K}\}$.

Proof
We consider an adversary *Adv* who is conducting a subspace impersonation attack on a given subspace $V = \text{span}(\mathbf{v}_1, \cdots, \mathbf{v}_m)$, and $n-m$ times of *independent* subspace substitution attacks when he/she observes a valid tag for V. We explain the meaning of "$n-m$ times of *independent* subspace substitution attacks". Assume *Adv* is able to conduct $n-m$ times of subspace substitution attacks after seeing a valid tag for V, where he/she chooses the message-tag pair [‡] $(v_i, t_i) = u_i \in \mathcal{W}'_i$ for the i-th attack; here $\mathcal{W}'_i = \text{span}(u_i)$ with $v_i \notin \text{span}(\mathbf{v}_1, \cdots, \mathbf{v}_m)$ (this is defined in subspace substitution attack). We say such $n-m$ times of subspace substitution attacks are *independent* if it holds that $\mathcal{W}'_1 \neq \mathcal{W}'_2 \cdots \neq \mathcal{W}'_{n-m-1} \neq \ \mathcal{W}'_{n-m}$. Since V is an m-dimensional subspace of the source space $\mathcal{S}$ which is an $n-$dimensional vector space (over $\mathbb{F}_q$), it is reasonable to assume that *Adv* conducts such $n-m$ times of independent subspace substitution attacks after observing a tag for V.

Since $P_{I_{sub}} \leq (P_I)^m$ and $P_D \leq \frac{1}{\gamma}$ in $\{\psi_{\mathbf{k}}, \mathbf{k}\in\mathcal{K}\}$. Exploiting results from Theorem 1, we have:

$$(\frac{1}{\gamma})^n \geq (P_I)^m \ (P_S)^{n-m} \geq P_{I_{sub}} \ (P_S)^{n-m} \geq 2^{-I(\mathcal{K};\overline{\mathcal{W}}^m)} 2^{-(I(\mathcal{W}'_1;\mathcal{K}|\overline{\mathcal{W}}^m)+\cdots+I(\mathcal{W}'_{n-m};\mathcal{K}|\overline{\mathcal{W}}^m))} \tag{18}$$

Now it is sufficient to prove the inequality below:

$$I(\mathcal{W}'_1;\mathcal{K}|\overline{\mathcal{W}}^m) + \cdots + I(\mathcal{W}'_{n-m};\mathcal{K}|\overline{\mathcal{W}}^m) \leq H(\mathcal{K}|\overline{\mathcal{W}}^m). \tag{19}$$

Since if (19) is proved, we continue (18) and then have:

$$\begin{aligned}(\frac{1}{\gamma})^n \quad &\geq \quad 2^{-(I(\mathcal{K};\overline{\mathcal{W}}^m)+I(\mathcal{W}'_1;\mathcal{K}|\overline{\mathcal{W}}^m)+\cdots+I(\mathcal{W}'_{n-m};\mathcal{K}|\overline{\mathcal{W}}^m))} \geq 2^{-(I(\mathcal{K};\overline{\mathcal{W}}^m)+H(\mathcal{K}|\overline{\mathcal{W}}^m))} \\ &= 2^{-H(\mathcal{K})} \geq 2^{-\log|\mathcal{K}|} = \frac{1}{|\mathcal{K}|},\end{aligned}$$

[‡] Here, the adversary forges a tag t_i for the message v_i.

which implies that $|\mathcal{K}| \geq \gamma^n$ and our theorem is proved.
Indeed, we can prove (19) as follows:

$$H(\mathcal{K}) = I(\mathcal{K}; \mathcal{W}'_1, \cdots, \mathcal{W}'_{n-m}, \overline{\mathcal{W}}^m) + H(\mathcal{K}|\mathcal{W}'_1, \cdots, \mathcal{W}'_{n-m}, \overline{\mathcal{W}}^m), \;\; H(\mathcal{K}|\mathcal{W}'_1, \cdots, \mathcal{W}'_{n-m}, \overline{\mathcal{W}}^m) \geq 0 \Rightarrow$$

$$H(\mathcal{K}) \geq I(\mathcal{K}; \mathcal{W}'_1, \cdots, \mathcal{W}'_{n-m}, \overline{\mathcal{W}}^m) \Rightarrow$$

$$H(\mathcal{K}) \geq \sum_{i=1}^{n-m} I(\mathcal{K}; \mathcal{W}'_i, \overline{\mathcal{W}}^m | \mathcal{W}'_{i-1}, \mathcal{W}'_{i-2}, \cdots, \mathcal{W}'_1, \overline{\mathcal{W}}^m) \Rightarrow$$

$$H(\mathcal{K}) \geq I(\mathcal{K}; \mathcal{W}'_1, \overline{\mathcal{W}}^m) + \cdots + I(\mathcal{K}; \mathcal{W}'_{n-m}, \overline{\mathcal{W}}^m) \Rightarrow$$

$$(n-m-1)H(\mathcal{K}) \leq (n-m)H(\mathcal{K}) - (I(\mathcal{K}; \mathcal{W}'_1, \overline{\mathcal{W}}^m) + \cdots + I(\mathcal{K}; \mathcal{W}'_{n-m}, \overline{\mathcal{W}}^m)) \Rightarrow$$

$$(n-m-1)H(\mathcal{K}) \leq (H(\mathcal{K}) - I(\mathcal{K}; \mathcal{W}'_1, \overline{\mathcal{W}}^m)) + \cdots + (H(\mathcal{K}) - I(\mathcal{K}; \mathcal{W}'_{n-m}, \overline{\mathcal{W}}^m)) \Rightarrow$$

$$(n-m-1)H(\mathcal{K}) \leq H(\mathcal{K}|\mathcal{W}'_1, \overline{\mathcal{W}}^m) + \cdots + H(\mathcal{K}|\mathcal{W}'_{n-m}, \overline{\mathcal{W}}^m) \Rightarrow \tag{20}$$

$$(n-m-1)H(\mathcal{K}|\overline{\mathcal{W}}^m) \leq H(\mathcal{K}|\mathcal{W}'_1, \overline{\mathcal{W}}^m) + \cdots + H(\mathcal{K}|\mathcal{W}'_{n-m}, \overline{\mathcal{W}}^m) \Rightarrow$$

$$H(\mathcal{K}|\overline{\mathcal{W}}^m) - H(\mathcal{K}|\mathcal{W}'_1, \overline{\mathcal{W}}^m) + \cdots + H(\mathcal{K}|\overline{\mathcal{W}}^m) - H(\mathcal{K}|\mathcal{W}'_{n-m}, \overline{\mathcal{W}}^m) \leq H(\mathcal{K}|\overline{\mathcal{W}}^m) \Rightarrow$$

$$I(\mathcal{W}'_1; \mathcal{K}|\overline{\mathcal{W}}^m) + \cdots + I(\mathcal{W}'_{n-m}; \mathcal{K}|\overline{\mathcal{W}}^m) \leq H(\mathcal{K}|\overline{\mathcal{W}}^m).$$

As above, the transition (20) is due to $n > m$ and $H(\mathcal{K}) \geq H(\mathcal{K}|\overline{\mathcal{W}}^m) \geq 0$. □

The lower bound shown in Theorem 2 is tight, as in the next section we have a construction which meets this bound.

5. CONSTRUCTIONS

In this section, we construct a class of (q, n, m)-homomorphic A-codes. These codes will show that, the lower bound derived in Theorem 2 can be achieved when $P_{I_{sub}} = (P_I)^m$, and $P_I = P_S$.

Definition 2
A (q, n, m)-homomorphic A-code $\{\psi_{\mathbf{k}}, \mathbf{k} \in \mathcal{K}\}$ is called an $[M, d_1, d_2, d_3]$ (q, n, m)-homomorphic A-code, if $|\mathcal{K}| = M, P_I = d_1, P_{I_{sub}} = d_2$ and $P_S = d_3$.

We use a natural (in terms of homomorphism) mapping for our A-code $\{\psi_{\mathbf{k}}, \mathbf{k} \in \mathcal{K}\}$, that is, $\psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{vk}$ for $\forall \mathbf{v} \in \mathcal{S}$ and $\mathbf{k} \in \mathcal{K}$. It is easy to see that an A-code with this mapping is always homomorphic in the source space $\mathcal{S}$. After the mapping is given, the construction of a $[M, d_1, d_2, d_3]$ (q, n, m)-homomorphic A-code is essentially a construction of $\mathcal{K} \subseteq \mathbb{F}_q^{n \times t}$ satisfying $|\mathcal{K}| = M, P_I = d_1, P_{I_{sub}} = d_2, P_S = d_3$.
Before constructing such a $\mathcal{K}$, we need some prerequisites.

DOI: 10.1002/cpe

5.1. Key Linearity

The A-code $\{\psi_{\mathbf{k}}, \mathbf{k} \in \mathcal{K}\}$ we are constructing is $\mathbb{F}_q$-linear in $\mathcal{K}$ as well as in $\mathcal{S}$. When focusing on an A-code with a property of key linearity, we are able to evaluate the security parameters as below:

Lemma 1
If the homomorphic A-code $\{\psi_{\mathbf{k}}\}$ is $\mathbb{F}_q$-linear in $\mathcal{K}$, we have

$$P_I = \max_{\mathbf{v} \in \mathcal{S}, \mathbf{v} \neq \mathbf{0}} \frac{|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v} \in \ker \psi_{\mathbf{k}}\}|}{|\mathcal{K}|},$$

$$P_{I_{sub}} = \max_{V} \frac{|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}_i \in \ker \psi_{\mathbf{k}}\}|}{|\mathcal{K}|},$$

$$P_S = \max_{\mathbf{v} \notin V} \frac{|\{\mathbf{k} \mid \mathbf{v}_i \in \ker \psi_{\mathbf{k}}\} \cap \{\mathbf{k} \mid \mathbf{v} \in \ker \psi_{\mathbf{k}}\}|}{|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}_i \in \ker \psi_{\mathbf{k}}\}|}.$$

Here $\mathbf{v} \in \mathcal{S}$ and $V = \mathrm{span}(\mathbf{v}_1, \cdots, \mathbf{v}_m)$ is an m-dimensional subspace.

The proof of this lemma can be found in Appendix A.

5.2. Invariant Property

In an A-code which is $\mathbb{F}_q$-linear in the keys, the key space $\mathcal{K}$ is always a subspace over $\mathbb{F}_q$. *From now on in this section, unless otherwise mentioned, we always assume the key space $\mathcal{K}$ is a subspace of $\mathbb{F}_q^{n\times t}$ over $\mathbb{F}_q$.*

In addition to requiring $\mathcal{K}$ be a subspace over $\mathbb{F}_q$, we impose another property on $\mathcal{K}$, with which we can have a convenient way to compute $P_I, P_{I_{sub}}$ and P_S. We say it is "convenient" since, as will be seen, if we follow Lemma 1 to compute the security parameter values, the computation will be independent from message and/or the subspace choices. In other words, the computation will be the same for different choices on $\mathbf{v}$ and V.

We say $\mathcal{K}$ **satisfies invariant property** if it holds that $AB \in \mathcal{K}$ for any $B \in \mathcal{K}$ and any non-singular matrix $A \in \mathbb{F}_q^{n\times n}$.

Lemma 2
We evaluate security parameters based on Lemma 1. If $\mathcal{K}$ satisfies invariant property, we have: P_I obtains the same value for different choices of $\mathbf{v}$; $P_{I_{sub}}$ obtains the same value for different choices of V (with a fixed dimension); P_S obtains the same values for different choices of $\mathbf{v}$ and V (with a fixed dimension). Moreover, if we denote $\mathcal{K}^i \subseteq \mathcal{K}$ as the set of matrices where entries in the first i rows are all zeros, we have $P_I = \frac{|\mathcal{K}^1|}{|\mathcal{K}|}, P_{I_{sub}} = \frac{|\mathcal{K}^m|}{|\mathcal{K}|}$ and $P_S = \frac{|\mathcal{K}^{m+1}|}{|\mathcal{K}^m|}$.

We defer Appendix B to the proof of this lemma.

5.3. A necessary and sufficient condition to satisfy invariant property

We now give a necessary and sufficient condition for a key space $\mathcal{K}$ to satisfy invariant property. We firstly give some notations. For any matrix $A \in \mathbb{F}_q^{h\times l}$, we use $\langle A\rangle_R$ to denote the row space of A, namely, the set of all possible $\mathbb{F}_q$-linear combinations of its row vectors. Formally, if we write A as $A = \begin{bmatrix} A_1 \\ \cdot \\ \cdot \\ \cdot \\ A_h \end{bmatrix}$ with $A_i \in \mathbb{F}_q^l$ its i-th row, we have $\langle A\rangle_R = \{\sum_{i=1}^h c_i A_i, c_i \in \mathbb{F}_q\}$.

Lemma 3
$\mathcal{K}$ is a subspace over $\mathbb{F}_q$ and satisfies invariant property if and only if : $A \in \mathcal{K}$ and $\langle B\rangle_R \subseteq \langle A\rangle_R$ implies that $B \in \mathcal{K}$.

Reader can find the proof of this lemma in Appendix C.

DOI: 10.1002/cpe

5.4. Constructions

Example 1
Letting $A \in \mathbb{F}_q^{n\times t}$ be a matrix with $\mathsf{rank}(A) = d$, we denote $\mathcal{K}_A$ as the set of all matrices B_A where $B_A \in \mathbb{F}_q^{n\times t}$ and each row of B_A belongs to $\langle A\rangle_R$. Formally,

$$\mathcal{K}_A = \{B = \begin{bmatrix} B_1 \\ \cdot \\ \cdot \\ \cdot \\ B_n \end{bmatrix} : B_i \in \langle A\rangle_R\}.$$

Theorem 3
Given a matrix $A \in \mathbb{F}_q^{n\times t}$ where $\mathsf{rank}(A) = d$, if we let $\mathcal{K} = \mathcal{K}_A$ (defined in Example 1 above), then the A-code $\{\psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{vk} \mid \mathbf{k} \in \mathcal{K}\}$ is a $[q^{nd}, q^{-d}, q^{-md}, q^{-d}]$ (q, n, m)-homomorphic A-code for all q, m, n, t, d with $m < n$ and $1 \le d \le t$.

Proof
It is equivalent to show that, if we let $\mathcal{K} = \mathcal{K}_A$ in the (q, n, m)-homomorphic A-code $\{\psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{vk} \mid \mathbf{k} \in \mathcal{K}\}$, we have:

$$|\mathcal{K}| = q^{dn}, P_I = q^{-d}, P_{I_{sub}} = q^{-md}, P_S = q^{-d}. \tag{21}$$

Firstly, according to the definition of $\mathcal{K} = \mathcal{K}_A$, it is easy to see that $|\mathcal{K}| = q^{dn}$ since each row has q^d choices and there are totally n rows. We next prove $P_I = q^{-d}, P_{I_{sub}} = q^{-md}$ and $P_S = q^{-d}$ in this setting.
We firstly claim that $\mathcal{K}_A$ is a subspace over $\mathbb{F}_q$ and satisfies invariant property. After that, we will compute $P_I, P_{I_{sub}}$ and P_S based on Lemma 2. Indeed, from the definition of $\mathcal{K}_A$, we know that $\mathbf{0} \in \mathcal{K}_A$; for any $X \in \mathcal{K}_A, Y \in \mathcal{K}_A$, we have $(X + Y) \in \mathcal{K}_A$; for any $X \in \mathcal{K}_A$ and $c \in \mathbb{F}_q$, $cX \in \mathcal{K}_A$. This shows that $\mathcal{K}_A$ is a subspace over $\mathbb{F}_q$. In addition, it is easy to check that $\mathcal{K}_A$ satisfies the condition exhibited in Lemma 3, which implies that $\mathcal{K}_A$ satisfies invariant property.
We then exploit Lemma 2 to compute our security parameter values. We have $|\mathcal{K}^1| = q^{d(n-1)}$ because we have q^d choices for each of the last $n-1$ rows. Similarly, we have $|\mathcal{K}^m| = q^{d(n-m)}$ and $|\mathcal{K}^{m+1}| = q^{d(n-m-1)}$. With these, we compute as below:

$$P_I = \frac{|\mathcal{K}^1|}{|\mathcal{K}|} = \frac{q^{d(n-1)}}{q^{dn}} = q^{-d}, P_{I_{sub}} = \frac{|\mathcal{K}^m|}{|\mathcal{K}|} = \frac{q^{d(n-m)}}{q^{dn}} = q^{-dm}, P_S = \frac{|\mathcal{K}^{m+1}|}{|\mathcal{K}^m|} = \frac{q^{d(n-m-1)}}{q^{d(n-m)}} = q^{-d}.$$

Finally, we prove (21). It is easy to check that the proof above is true for all q, m, n, t, d with $m < n$ and $1 \le d \le t$. We therefore complete the proof in the theorem. □

Comparing Theorem 3 with the bound from Theorem 2, it is trivial to have a following corollary:

Corollary 1
The parameters in Theorem 3 meets the bounds in Theorem 2.

As a further step, we next show a lemma that $\mathcal{K} = \mathcal{K}_A$ is simultaneously a minimal subspace $\mathcal{K}$ for a given A to satisfy invariant property. In other words, given a matrix $A \in \mathbb{F}_q^{n\times t}$, the smallest size of all the key spaces being a subspace and satisfying invariant property, is $|\mathcal{K}| = |\mathcal{K}_A| = q^{dn}$. Recall that this bound exactly matches the lower key size bound derived in Theorem 2.

Lemma 4
Let $A \in \mathbb{F}_q^{n\times t}$, then the minimal key space $\mathcal{K}$, where $A \in \mathcal{K}$ and $\mathcal{K}$ satisfies invariant property as well as being a subspace over $\mathbb{F}_q$, is $\mathcal{K} = \mathcal{K}_A$.

DOI: 10.1002/cpe

We defer the proof of this lemma to Appendix D.

Example 2
We would like to give a toy example to conclude our construction in this section. More precisely, assuming $q = 2, n = 3, t = 2, m = 2$ and a matrix $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 1 & 0 \end{bmatrix}$, we show that the key space $\mathcal{K}_A = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \right\}$ is the minimal subspace (over $\mathbb{F}_q$) which makes $P_{I_{sub}} = (P_I)^m = (P_S)^m = 2^{-2} = q^{m \times \mathsf{rank}(A)}$. This demonstrates that our construction meets the bound shown in Theorem 2 (since $|\mathcal{K}| = 8 = q^{n \times \mathsf{rank}(A)}$) and the bound is tight (due to minimality). Indeed, readers can check one fact that, for any homomorphic A-code $\{\psi_{\mathbf{k}} | \mathbf{k} \in \mathcal{K}\}$ with $\mathcal{K} = \mathcal{K}' \subsetneq \mathcal{K}_A$ and $\mathcal{K}'$ being a subspace over $\mathbb{F}_q$, we have: $P_I = 1, P_S = 1, P_{I_{sub}} = \frac{1}{2}$. This fact implies that the bound in Theorem 2 cannot be satisfied unless we make $\mathcal{K} = \mathcal{K}_A$.

Following construction, one interesting problem might be how to convert a given key space $\mathcal{K} \subseteq \mathbb{F}_q^{n \times t}$ into a new key space $\mathcal{K}' \supseteq \mathcal{K}$ such that $\mathcal{K}'$ satisfies invariant property and $\mathcal{K}'$ is minimal. Our lemma below shows that we can always find such a minimal key space $\mathcal{K}'$. We use the same notation $\mathcal{K}_A$ as in Example 1.

Lemma 5
For any given key space $\mathcal{K} \subseteq \mathbb{F}_q^{n \times t}$ written as $\mathcal{K} = \{A \mid A \in \mathcal{K}\}$, the new key space $\mathcal{K}' = \{\mathcal{K}_A \mid A \in \mathcal{K}\}$ is the minimal space where $\mathcal{K}' \supseteq \mathcal{K}$ and $\mathcal{K}'$ satisfies invariant property.

Proof
It is easily to check from Lemma 3 that $\mathcal{K}' = \{\mathcal{K}_A \mid A \in \mathcal{K}\}$ satisfies invariant property and from Lemma 4 that it is the minimal one. □

6. HOMOMORPHIC A-CODES FOR MULTIPLE FILE AUTHENTICATION

One main concern regarding practical use of our scheme might be that keys cannot be reused for multiple files authentication due to information theoretic security. However, as we will show in this section, we can use *one* key to authenticate multiple files.

Let us assume that we have to authenticate a sequence of η files. Clearly, a trivial, straightforward way to do that is to use one key per file, implying that we require η independent keys. However, inspired by the work of Atici and Stinson [1], we show that we can do better than that. We present a variant of our scheme that requires only one key for all the η files, while achieving unconditional security. Particularly, we use one key comprising $\mathbf{k} \in \mathcal{K}$ and an $(\eta - 1)$-tuple $(a_1, \ldots, a_{\eta-1}) \in \mathcal{A}^{\eta-1}$ to authenticate η consecutive files. We show that for each additional file, the sender and the verifier needs a key of size $\log |\mathcal{A}|$ bits. By contrast with the aforementioned trivial approach, which requires a $\log |\mathcal{K}|$-bit key at the sender and the verifier for each additional file, our scheme is more efficient since $|\mathcal{A}| \leq |\mathcal{K}|$. To illustrate with a more concrete example using the homomorphic A-code shown in Theorem 3, we have $q^t = |\mathcal{A}| \leq |\mathcal{K}| = q^{nd}$ where $t \leq n, 1 \leq d$.

Recall from Figure 1 that we use $(g_{\mathbf{v}1}, \ldots, g_{\mathbf{v}m})$ as a global encoding vector for the message $\mathbf{v} = \sum_{i=1}^{m} g_{\mathbf{v}i} \mathbf{v}_i$. In the following scheme, each message $\mathbf{v}$ is required to carry one additional bit to keep track of the value $\sum_{i=1}^{m} g_{\mathbf{v}i}$. With this, given a (q, n, m)-homomorphic A-code $(\mathcal{S}, \mathcal{K}, \mathcal{A}, f)$ complying with Definition 1 and assuming that the verifier and the source share a secret key $(\mathbf{k}, a_1, \ldots, a_{\eta-1})$ where $\mathbf{k} \in \mathcal{K}$ and $(a_1, \ldots, a_{\eta-1}) \in \mathcal{A}^{\eta-1}$, we are ready to specify our homomorphic A-code for the l-th $(1 \leq l \leq \eta)$ file transmission, as illustrated in Figure 2.

- **Tag generation:** If $l = 1$, then it follows **Tag generation** in Figure 1. Otherwise, For each message $\mathbf{v}_i \in \mathcal{S}$ $(1 \leq i \leq m)$, the source computes $f(\mathbf{v}_i, \mathbf{k}) + a_{l-1}$ as the corresponding tag $\mathbf{t}_i$ and sends out the packet $(1, \mathbf{v}_i, \mathbf{t}_i)$.
- **Combination:** If $l = 1$, then it follows **Combination** in Figure 1. Otherwise, Assume that each intermediate node receives some packet $(\sum_{i=1}^{m} g_{\mathbf{x}_h i}, \mathbf{x}_h, \mathbf{t}_{\mathbf{x}_h})$ for some index h, where each $\mathbf{x}_h$ is already a linear combination of some messages $\mathbf{v}_i$. The intermediate node computes $g_y = \sum_h \alpha_h \sum_{i=1}^{m} g_{\mathbf{x}_h i}$ and $\mathbf{t}_\mathbf{y} = \sum_h \alpha_h \mathbf{t}_{\mathbf{x}_h}$ corresponding to an output vector $\mathbf{y} = \sum_h \alpha_h \mathbf{x}_h$, where the sum is taken over some subset of the received tags. The intermediate node sends out the packet (g_y, y, t_y) when there is any transmitting opportunity regarding y.
- **Verification:** If $l = 1$, then it follows **Verification** in Figure 1. Otherwise, assume that the verifier possesses a private key $(\mathbf{k}, a_1, \ldots, a_{\eta-1})$ and it receives a message $\mathbf{v}$ and the corresponding tag $\mathbf{t}_\mathbf{v}$. The verifier checks if $f(\mathbf{v}, \mathbf{k}) + g_\mathbf{v} a_{l-1} = \mathbf{t}_\mathbf{v}$; it accepts $(\mathbf{v}, \mathbf{t}_\mathbf{v})$ if the equation holds; otherwise it rejects.

Figure 2. Definition of homomorphic A-code scheme for multiple file transmission $(1 \leq l \leq \eta)$.

We first show the correctness of the scheme in Figure 2. For $\mathbf{v} = \sum_{j=1}^{m} g_{\mathbf{v}j} \mathbf{v}_j$ we have:

$$\mathbf{t}_\mathbf{v} = \sum_{j=1}^{m} g_{\mathbf{v}j}(f(\mathbf{v}_j, \mathbf{k}) + a_{l-1}) = \sum_{j=1}^{m} g_{\mathbf{v}j} f(\mathbf{v}_j, \mathbf{k}) + (\sum_{j=1}^{m} g_{\mathbf{v}j}) a_{l-1}.$$

Since our homomorphic A-code $(\mathcal{S}, \mathcal{K}, \mathcal{A}, f)$ is a (q, n, m)-homomorphic A-code, we furthermore have:

$$\sum_{j=1}^{m} g_{\mathbf{v}j} f(\mathbf{v}_j, \mathbf{k}) + (\sum_{j=1}^{m} g_{\mathbf{v}j}) a_{l-1} = f(\sum_{j=1}^{m} g_{\mathbf{v}j} \mathbf{v}_j, \mathbf{k}) + (\sum_{j=1}^{m} g_{\mathbf{v}j}) a_{l-1} = f(\mathbf{v}, \mathbf{k}) + g_\mathbf{v} a_{l-1}.$$

and thus the verification is correct.

We claim that the security for the l-th $(2 \leq l \leq \eta)$ file transmission is the same as the 1-st file transmission. To see this, we have:

$$\max_{\mathbf{v} \in \mathcal{S}, \mathbf{t} \in \mathcal{A}, a_{l-1} \in \mathcal{A}} |\mathbf{k} \in \mathcal{K} \mid f(\mathbf{v}, \mathbf{k}) + a_{l-1} = \mathbf{t}| = \max_{\mathbf{v} \in \mathcal{S}, \mathbf{t} \in \mathcal{A}} |\mathbf{k} \in \mathcal{K} \mid \ f(\mathbf{v}, \mathbf{k}) = \mathbf{t}|,$$

which implies that from the view of the attacker, guessing a key $(\mathbf{k}, a_{l-1})$ associated with the l-th file transmission is equivalent to guessing a key $\mathbf{k}$ associated with the 1-st file transmission. Therefore, the attacker has the same success probability at the l-th file transmission as with that of the 1-st file transmission. With that, we infer that our scheme for multiple file transmission based on homomorphic A-code $(\mathcal{S}, \mathcal{K}, \mathcal{A}, f)$ achieves the same security level as with the A-code $(\mathcal{S}, \mathcal{K}, \mathcal{A}, f)$ for one single file.

7. RELATED WORK

An example of multireceiver authentication codes for network coding has been proposed in [7], which can be adapted to suit the single receiver case. The source has m messages $\mathbf{s}_1, \ldots, \mathbf{s}_m \in \mathbb{F}_q^n$ to be sent. Before transmission, one symbol in $\mathbb{F}_q$ is appended to the message, that is $(\mathbf{s}_i, 1)$ is actually transmitted for every i, however, since this one symbol is not authenticated, we have $\mathbf{v}_i = \mathbf{s}_i$. A tag for $\mathbf{s}_i$ is computed by

$$\psi_\mathbf{k}(\mathbf{s}_i) = A_{\mathbf{s}_i}(X) = P_0(X) + \mathbf{s}_i P_1(X) + \mathbf{s}_i^q P_2(X) + \ldots + \mathbf{s}_i^{q^{l-1}} P_l(X) \in \mathbb{F}_{q^n}[X],$$

where $P_0(X), \ldots, P_l(X)$ are private polynomials of degree d with coefficients in $\mathbb{F}_{q^n}$ owned by the source, namely

$$\mathbf{k} = (P_{00}, \ldots, P_{0,d-1}, P_{10}, \ldots, P_{1,d-1}, \ldots, P_{l0}, \ldots, P_{l,d-1}).$$

The parameter l refers to the number of usage of the key, which should be at least m, thus we can assume that $l = m$ for one round of transmissions, while d is 1 here, since $d-1$ refers to the number of internal adversaries, that is the number of dishonest receivers which can collude against others. Thus $P_i(X)$ are constant polynomials, which we write $P_i(X) = P_i$. The tag $\mathbf{t}_i$ contains the coefficients of the polynomial $A_{\mathbf{s}_i}(X)$, which in the one receiver case is simply a constant element in $\mathbb{F}_{q^n}$. We then have that $\mathcal{S} = \mathbb{F}_{q^n}$, $\mathcal{K} = \mathbb{F}_{q^n}^{m+1}$, $\mathcal{A} = \mathbb{F}_{q^n}$. This is essentially a particular case where $t = n$ in our A-code definition.

The vector space $V = \text{span}(\mathbf{s}_1, \ldots, \mathbf{s}_m)$ associated to the source message obtains the tag $(\mathbf{t}_1, ..., \mathbf{t}_m)$. It could be that this tag is redundant, in the case where V is of dimension less than m.

The homomorphic property does not hold immediately [§], but instead does for a similar construction.

Lemma 6
Set $\mathbf{k} = (P_0, \ldots, P_m) \in \mathcal{K}$ and $\mathbf{v} = \sum_{i=1}^{m} \alpha_i \mathbf{v}_i$. The map

$$\psi_{\mathbf{k}}(\mathbf{v}) = P_0\mathbf{v} + P_1\mathbf{v}^q + P_2\mathbf{v}^{q^2} + \ldots + P_m\mathbf{v}^{q^m} \in \mathbb{F}_q^n \tag{22}$$

satisfies that

$$\psi_{\mathbf{k}}(\mathbf{v}) = \sum_{i=1}^{m} \alpha_i \psi_{\mathbf{k}}(\mathbf{v}_i).$$

Proof
We have by definition that

$$\begin{aligned}
\psi_{\mathbf{k}}(\mathbf{v}) &= \left(\sum_{i=1}^{m} \alpha_i \mathbf{v}_i\right) P_0 + \left(\sum_{i=1}^{m} \alpha_i \mathbf{v}_i\right)^q P_1 + \ldots + \left(\sum_{i=1}^{m} \alpha_i \mathbf{v}_i\right)^{q^m} P_m \\
&= \left(\sum_{i=1}^{m} \alpha_i \mathbf{v}_i\right) P_0 + \left(\sum_{i=1}^{m} \alpha_i \mathbf{v}_i^q\right) P_1 + \ldots + \left(\sum_{i=1}^{m} \alpha_i \mathbf{v}_i^{q^m}\right) P_m \\
&= \sum_{i=1}^{m} \alpha_i \left(\mathbf{v}_i P_0 + \mathbf{v}_i^q P_1 + \ldots + \mathbf{v}_i^{q^m} P_m\right) = \sum_{i=1}^{m} \alpha_i \psi_{\mathbf{k}}(\mathbf{v}_i),
\end{aligned}$$

which concludes the proof. □

The above lemma means that $\{\psi_{\mathbf{k}}, \mathbf{k} \in \mathcal{K}\}$ as defined is in fact a $\mathbb{F}_q$-linear mapping from $\mathbb{F}_{q^n}$ to itself, thus, by fixing an $\mathbb{F}_q$-basis $\nu = \{\nu_1, \ldots, \nu_n\}$ of $\mathbb{F}_{q^n}$, it can be written in matrix form as $\psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{v}A_{\mathbf{k}}$ where $A_{\mathbf{k}}$ is an $n \times n$ matrix over $\mathbb{F}_q$. Indeed, let M_{P_i} be the matrix of multiplication by P_i and $\mathbf{v} = (v_1, \ldots, v_n)$ both in the chosen basis. We have that

$$\mathbf{v}P_i = \sum_{j=1}^{n} v_j (P_i \nu_j) = (v_1, \ldots, v_n) M_{P_i} \begin{pmatrix} \nu_1 \\ \vdots \\ \nu_n \end{pmatrix}$$

and similarly, for any $1 \leq x \leq m$, writing $\nu_j^{q^x}$ as $\sum_{h=1}^{n} b_{x_{jh}} \nu_h$, with $B_x = (b_{x_{ij}})$, we have:

$$\mathbf{v}^{q^x} P_i \quad = \quad \sum_{j=1}^{n} v_j \nu_j^{q^x} P_i = \sum_{j=1}^{n} v_j (b_{x_{j1}}, \ldots, b_{x_{jn}}) \begin{pmatrix} \nu_1 \\ \vdots \\ \nu_n \end{pmatrix} P_i = (v_1, \ldots, v_n) B_x M_{P_i} \begin{pmatrix} \nu_1 \\ \vdots \\ \nu_n \end{pmatrix}$$

[§] Though this A-code is lack of homomorphism, the paper [7] still implemented a successful authentication. They required a knowledge about network coding coefficients, which are traced by the last “1’ bit in $(\mathbf{s}_i, 1)$.

so that

$$A_{\mathbf{k}} = M_{P_0} + B_1 M_{P_1} + \cdots + B_m M_{P_m}. \tag{23}$$

From now on, we fix an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$, say ν mentioned above. Then, we use M_u to denote the multiplication matrix for an $u \in \mathbb{F}_q^n$. Furthermore, we represent $\mathcal{M}$ as the set of all multiplication matrices for elements from $\mathbb{F}_{q^n}$, formally, $\mathcal{M} = \{M_u \mid u \in \mathbb{F}_{q^n}\}$.
It is known that, $\mathcal{M}$ is a subspace over $\mathbb{F}_q$, and thus we can continue (23) and rewrite $A_{\mathbf{k}}$ as:

$$A_{\mathbf{k}} = M_{P_0} + B_1 M_{P_1} + \cdots + B_m M_{P_m} = \sum_{i=0}^{m} M_{u_i}. \tag{24}$$

BY the second equation of (24), we particularly mean that we let $M_{u_0} = M_{P_0}$ and $M_{u_i} = B_i M_{P_i}$ for $1 \leq i \leq m$. Since $P_i \in \mathbb{F}_{q^n} (0 \leq i \leq m)$ while $B_i (1 \leq i \leq m)$ is a fixed nonzero multiplication matrix, we are easy to see that M_{u_i} can be any multiplication matrix from $\mathcal{M}$. We therefore can redefine the homomorphic A-code as below:

Lemma 7
In the (q, n, m)-homomorphic A-code $\{\psi_{\mathbf{k}}, \mathbf{k} \in \mathcal{K}\}$ as defined in Lemma 6, we have: $\mathcal{K} = \{\mathbf{k} = (\mathbf{k}_0, \ldots, \mathbf{k}_m) : \mathbf{k}_i \in \mathcal{M}\}$ and $\psi_{\mathbf{k}}(\mathbf{v}) = A_{\mathbf{k}} = \sum_{i=0}^{m} \mathbf{v}\mathbf{k}_i$.

We next evaluate security parameters and key size for this homomorphic A-code.

Lemma 8
In the (q, n, m)-homomorphic A-code $\{\psi_{\mathbf{k}}, \mathbf{k} \in \mathcal{K}\}$ as defined in Lemma 6, we have:

$$|\mathcal{K}| = q^{(m+1)n}, P_I = \frac{1}{q^n}, P_{I_{sub}} = \frac{1}{q^n}, P_S = 1. \tag{25}$$

Proof
The key size $|\mathcal{K}| = q^{(m+1)n}$ can been seen immediately from the expression of $\mathcal{K}$ in Lemma 7. We now evaluate the security parameters.
Firstly, again $\mathcal{K}$ is a subspace over $\mathbb{F}_q$, so we can compute based on on Lemma 1. That is:

$$P_I = \max_{\mathbf{v} \in \mathcal{S}, \mathbf{v} \neq \mathbf{0}} \frac{\{|\mathbf{k} \in \mathcal{K} \mid \sum_{j=0}^{m} \mathbf{v}\mathbf{k}_j = 0\}|}{q^{(m+1)n}}, \tag{26}$$

$$P_{I_{sub}} = \max_{V} \frac{|\{\mathbf{k} \in \mathcal{K} \mid \sum_{j=0}^{m} \mathbf{v}_i \mathbf{k}_j = 0\}|}{q^{(m+1)n}}, \tag{27}$$

and

$$P_S = \max_{\mathbf{v} \notin V} \frac{|\{\mathbf{k} \in \mathcal{K} \mid \sum_{j=0}^{m} \mathbf{v}_i \mathbf{k}_j = 0\} \cap \{\mathbf{k} \mid \sum_{j=0}^{m} \mathbf{v}\mathbf{k}_j = 0\}|}{|\{\mathbf{k} \in \mathcal{K} \mid \sum_{j=0}^{m} \mathbf{v}_i \mathbf{k}_j = 0\}|}. \tag{28}$$

Here $\mathbf{k} = (\mathbf{k}_0, \ldots, \mathbf{k}_m)$ with each $\mathbf{k}_i \in \mathcal{M}$, $\mathbf{v} \in \mathcal{K}$ and $V = \text{span}(\mathbf{v}_1, \cdots, \mathbf{v}_m)$ is an m-dimensional subspace to authenticate.
Secondly, it is known that all non-zero multiplication matrices are non-singular matrices and their sums are non-singular matrices as well, which implies that, for any $\mathbf{k} = (\mathbf{k}_0, \ldots, \mathbf{k}_m)$:

$$\text{For } \forall \mathbf{v} \neq \mathbf{0}, \sum_{j=0}^{m} \mathbf{v}\mathbf{k}_j = 0 \iff \sum_{j=0}^{m} \mathbf{k}_j = 0;$$

$$\text{For } \forall\, V, \sum_{j=0}^{m} \mathbf{v}_i \mathbf{k}_j = 0 \iff \sum_{j=0}^{m} \mathbf{k}_j = 0;$$

DOI: 10.1002/cpe

$$\text{For } \forall\, \mathbf{v} \notin V,\ \sum_{j=0}^{m} \mathbf{v}_i \mathbf{k}_j = 0, \sum_{j=0}^{m} \mathbf{v}\mathbf{k}_j = 0 \iff \sum_{j=0}^{m} \mathbf{k}_j = 0.$$

Now, since $|\{\mathbf{k} \mid \sum_{j=0}^{m} \mathbf{k}_j = 0\}| > 0$ (due to $\mathbf{0} \in \{\mathbf{k} \mid \sum_{j=0}^{m} \mathbf{k}_j = 0\}$), we can immediately continue (28) and compute P_S as:

$$P_S = \frac{|\{\mathbf{k} \mid \sum_{j=0}^{m} \mathbf{k}_j = 0\}|}{|\{\mathbf{k} \mid \sum_{j=0}^{m} \mathbf{k}_j = 0\}|} = 1.$$

We still have to calculate the number $|\{\mathbf{k} \mid \sum_{j=0}^{m} \mathbf{k}_j = 0\}|$, in order to compute P_I and $P_{I_{sub}}$. In fact, we can find all such keys $\mathbf{k}$ satisfying $\sum_{j=0}^{m} \mathbf{k}_j = 0$ in a following way. We let each of the first m elements, that is, $\mathbf{k}_i (0 \leq i \leq m-1)$, randomly chosen from $\mathcal{M}$; in other words, there are $|\mathcal{M}| = |q^n|$ random choices for each of them. We then declare that there is one and only one $\mathbf{k}_m \in \mathcal{M}$ that leads to $\sum_{j=0}^{m} \mathbf{k}_j = 0$. Indeed, if we denote $\mathbf{k}_i = M_{u_i}$ for $0 \leq i \leq m-1$, then the candidate $\mathbf{k}_m = M_{(q^n - \sum_{i=0}^{m-1} u_i)}$ always exists and is the only one to make $\sum_{j=0}^{m} \mathbf{k}_j = 0$ happen. As a result, the number is:

$$|\{\mathbf{k} \mid \sum_{j=0}^{m} \mathbf{k}_j = 0\}| = q^{nm}. \tag{29}$$

Finally, together with (26) and (29), we have: $P_I = \frac{q^{mn}}{q^{(m+1)n}} = \frac{1}{q^n}$. Computing (27) with (29), we have: $P_{I_{sub}} = \frac{q^{mn}}{q^{(m+1)n}} = \frac{1}{q^n}$. We therefore finish the proof in the lemma. □

8. CONCLUSION AND FUTURE WORK

We studied a class of A-codes that are linear in messages, which are useful in network coding scenario for authentication. We derive some lower bounds on security parameters when key space is known for a general homomorphic A-code. We also obtain a lower bound on key size when security parameter values are given with some special properties, and constructed some codes meeting this bound. It would be interesting to show a bound on key size for general security parameter values and find constructions meeting the corresponding bounds. Another future work is to show an efficient scheme for a network with multiple verifiers, moreover, a network with dynamic sender(s) which would be particularly beneficial for network coding-based wireless sensor network applications.

REFERENCES

1. M. Atici and D.R. Stinson. “Universal hashing and multiple authentication”. *CRYPTO 96*, pp. 16 – 30, Springer-Verlag, 1996.
2. D. Boneh, D. Freeman, J. Katz, B. Water, “Signing a Linear Subspace: Signature Schemes for Network Coding”, *Public Key Cryptography, PKC*2009, pp. 68 – 87, LNCS 5443, Springer Verlag, 2009.
3. D. Charles, K. Jain, K. Lauter, “Signatures for Network Coding”,*40th Annual Conference on Information Sciences and Systems*, 2006. Available at http://eprint.iacr.org.
4. S. Agrawal and D. Boneh, “Homomorphic MACs: MAC-Based Integrity for Network Coding”, *ACNS* 2009 : 292 – 305, Springer Verlag.
5. K. Izawa, A. Miyaji and K. Omote,“Lightweight Integrity for XOR Network Coding in Wireless Sensor Networks”,*Information Security Practice and Experience*, Lecture Notes in Computer Science, Springer, 2012.
6. R. Koetter and F. Kschischang, “Coding for Errors and Erasures in Random Network Coding”, *IEEE Trans. Information Theory*, vol. 54, no.8, pp. 3579C3591, Aug. 2008.
7. F. Oggier and H. Fathi, “An Authentication Code against Pollution Attacks in Network Coding”, *IEEE/ACM Transactions on Networking*, Issue 99, March 2011. CoRR abs/0909.3146 (2009)
8. E. N. Gilbert, F. J MacWilliams, N. J. A. Sloane, “Codes which detect deception,” *Bell Syst. Techn. Journal*, vol. 33, 1974.
9. G. J. Simmons, “Authentication theory/coding,” *Advances in Cryptology - Crypto 84*, Lecture Notes in Computer Science, Springer, 1984.

10. H. Wang, C. Xing and R. Safavi-Naini, "Linear Authentication Codes: Bounds and Constructions," *IEEE Trans. on Information Theory*, vol. 49, no. 4, 2003.
11. Reihaneh Safavi-Naini, Huaxiong Wang: Multireceiver Authentication Codes: Models, Bounds, Constructions, and Extensions. Inf. Comput. (IANDC) 151(1-2):148-172 (1999)
12. M.Walker, Information-Theoretic Bounds for Authentication Schemes, *J. of Cryptology*, Vol 2, No. 3, 1990, pp 131-143.

A. PROOF OF LEMMA 1

Proof
We firstly prove it for P_I. It suffices to prove the statement below for $\forall\ 0 \neq \mathbf{v} \in \mathcal{S}$ and $\forall\ 0 \neq \mathbf{t} \in \mathcal{A}$:

$$|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v} \in \ker\psi_{\mathbf{k}}\}| \geq |\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}\}|.$$

We claim as below:
Claim:
$|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v} \in \ker\psi_{\mathbf{k}}\}| > |\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}\}|$ if $\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}\} = \varnothing$. $(*)$
$|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v} \in \ker\psi_{\mathbf{k}}\}| = |\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}\}|$ if $\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}\} \neq \varnothing$. $(**)$

Indeed, since $\mathcal{K}$ is a subspace over $\mathbb{F}_q$, we always have $\mathbf{0} \in \mathcal{K}$, which implies that $|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v} \in \ker\psi_{\mathbf{k}}\}| \geq 1$ for $\forall\ \mathbf{v} \in \mathcal{S}$. This way, if $\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}\} = \varnothing$, we have $|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v} \in \ker\psi_{\mathbf{k}}\}| > |\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}\}|$, henceforth the (*) part is proved. We can prove the (**) part by exploiting the trick from [10]. That is, if $\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}\} \neq \varnothing$, then there always exists an $k_0 \in \{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}\}$. We define a function ϕ from $\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}\}$ to $\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v} \in \ker\psi_{\mathbf{k}}\}$ by $\phi(\mathbf{k}) = \mathbf{k} - k_0$. We can easily see that ϕ is one-to-one, which implies that

$$|\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}\}| \leq |\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v} \in \ker\psi_{\mathbf{k}}\}|. \qquad (A.1)$$

On other hand, we can define another function φ from $\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v} \in \ker\psi_{\mathbf{k}}\}$ to $\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}\}$ via $\varphi(\mathbf{k}) = \mathbf{k} + k_0$. We can also check that φ is one-to-one, which implies that

$$|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v} \in \ker\psi_{\mathbf{k}}\}| \leq |\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}\}| \qquad (A.2)$$

A combination of (A.1) and (A.2) demonstrates that $|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v} \in \ker\psi_{\mathbf{k}}\}| = |\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}\}|$.
With the claim, it is easy to see that the theorem holds for P_I.

We now prove the theorem for $P_{I_{sub}}$, P_S. In an analogous way of demonstrating the aforementioned claim, we can prove that for $\forall\ V, \mathbf{t}_i (1 \leq i \leq m)$ we have $|\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}_i) = \mathbf{t}_i\}| = 0$ or $|\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}_i) = \mathbf{t}_i\}| = |\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}_i \in \ker\psi_{\mathbf{k}}\}|$. It then follows that we can compute $P_{I_{sub}}$ as:

$$P_{I_{sub}} = \max_{V} \frac{|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}_i \in \ker\psi_{\mathbf{k}}\}|}{|\mathcal{K}|}.$$

To compute P_S, we only consider the situation where $|\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}_i) = \mathbf{t}_i, 1 \leq i \leq m\}| \neq 0$, that is, where $|\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}_i) = \mathbf{t}_i, 1 \leq i \leq m\}| = |\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}_i \in \ker\psi_{\mathbf{k}}, 1 \leq i \leq m\}|$. We now compute P_S for this case. We now have:

$$P_S = \max_{\mathbf{v} \notin V, V} \max_{\mathbf{t}, \mathbf{t}_i} \frac{|\{\mathbf{k} \mid \psi_{\mathbf{k}}(\mathbf{v}_i) = \mathbf{t}_i\} \cap \{\mathbf{k} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}\}|}{|\{\mathbf{k} \in \mathcal{K} \mid \psi_{\mathbf{k}}(\mathbf{v}_i) = \mathbf{t}_i\}|} = \max_{\mathbf{v} \notin V, V} \max_{\mathbf{t}, \mathbf{t}_i} \frac{|\{\mathbf{k} \mid \psi_{\mathbf{k}}(\mathbf{v}_i) = \mathbf{t}_i\} \cap \{\mathbf{k} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}\}|}{|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}_i \in \ker\psi_{\mathbf{k}}\}|}$$

Again, using the same way of proving the claim above, we can easily see that:

$$|\{\mathbf{k} \mid \mathbf{v}_i \in \ker\psi_{\mathbf{k}}, 1 \leq i \leq m\} \cap \{\mathbf{k} \mid \mathbf{v} \in \ker\psi_{\mathbf{k}}\}| \geq |\{\mathbf{k} \mid \psi_{\mathbf{k}}(\mathbf{v}_i) = \mathbf{t}_i, 1 \leq i \leq m\} \cap \{\mathbf{k} \mid \psi_{\mathbf{k}}(\mathbf{v}) = \mathbf{t}\}|.$$

Henceforth, we compute P_S as:

$$P_S = \max_{\mathbf{v}\notin V, V} \frac{|\{\mathbf{k} \mid \mathbf{v}_i \in \ker \psi_{\mathbf{k}}\} \cap \{\mathbf{k} \mid \mathbf{v} \in \ker \psi_{\mathbf{k}}\}|}{|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}_i \in \ker \psi_{\mathbf{k}}\}|}$$

Finally, we complete the proof of the theorem. □

B. PROOF OF LEMMA 2

Proof
We firstly prove it for P_I. From Lemma 1, we have:

$$P_I = \max_{\mathbf{v}\in\mathcal{S}, \mathbf{v}\neq\mathbf{0}} \frac{|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v} \in \ker \psi_{\mathbf{k}}\}|}{|\mathcal{K}|}.$$

It therefore suffices to prove that for any $0 \neq \mathbf{v}_1 \in \mathcal{S}$ and $0 \neq \mathbf{v}_2 \in \mathcal{S}$, we have:

$$\frac{|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}_1 \in \ker \psi_{\mathbf{k}}\}|}{|\mathcal{K}|} = \frac{|\mathcal{K}^1|}{|\mathcal{K}|} = \frac{|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}_2 \in \ker \psi_{\mathbf{k}}\}|}{|\mathcal{K}|}.$$

We define $\mathcal{K}(\mathbf{v}) = \{\mathbf{k} \in \mathcal{K} \mid \mathbf{v} \in \ker \psi_{\mathbf{k}}\}$ for any $0 \neq \mathbf{v} \in \mathcal{S}$. This way, it is sufficient to prove the statement as below:

$$|\mathcal{K}(\mathbf{v}_1)| = |\mathcal{K}^1| = |\mathcal{K}(\mathbf{v}_2)|. \qquad (B.1)$$

We now prove the first equation for statement (B.1). For any $0 \neq \mathbf{v}_1 \in \mathcal{S}$, in terms of basic linear algebra, we can always choose a non-singular $n \times n$ matrix P so that $\mathbf{v}_1 P = (|\mathbf{v}_1|, 0, \cdots, 0)$ where $|\mathbf{v}_1|$ represents the Euclidean norm of $\mathbf{v}_1$. According to the definition of $\mathcal{K}(\mathbf{v})$, we have $|\mathcal{K}(\mathbf{v}_1)| = |\{A \in \mathcal{K} \mid \mathbf{v}_1 A = 0\}|$ and $|\mathcal{K}(\mathbf{v}_1 P)| = |\{B \in \mathcal{K} \mid \mathbf{v}_1 P B = 0\}|$. Since $\mathcal{K}$ satisfies invariant property, we have the equation below:

$$|\mathcal{K}(\mathbf{v}_1)| = |P\mathcal{K}(\mathbf{v}_1 P)| \qquad (B.2)$$

By definition again, we have:

$$\mathcal{K}(\mathbf{v}_1 P) = \{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}_1 P \in \ker \psi_{\mathbf{k}}\}.$$

Note that $\mathbf{v}_1 P = (|\mathbf{v}_1|, 0, \cdots, 0)$, according to the definition of $\mathcal{K}^1$, it is easy to see that:

$$\mathcal{K}(\mathbf{v}_1 P) = \mathcal{K}^1. \qquad (B.3)$$

On the other hand, since $\mathcal{K}$ satisfies invariant property which ensures that $Pk \in \mathcal{K}$ for all $k \in \mathcal{K}$, it always holds that $P\mathcal{K}(\mathbf{v}_1 P) \subseteq \mathcal{K}$. We therefore have

$$|P\mathcal{K}(\mathbf{v}_1 P)| = |\mathcal{K}(\mathbf{v}_1 P)|. \qquad (B.4)$$

Combining (B.2), (B.3) and (B.4), we have:

$$|\mathcal{K}(\mathbf{v}_1)| = |P\mathcal{K}(\mathbf{v}_1 P)| = |\mathcal{K}(\mathbf{v}_1 P)| = |\mathcal{K}^1|.$$

which immediately shows that:

$$|\mathcal{K}(\mathbf{v}_1)| = |\mathcal{K}^1|.$$

And thus the proof for $\mathbf{v}_1$ is completed. Since $\mathbf{v}_1$ is randomly chosen from $\mathcal{S}\backslash\{0\}$, then the equation for $\mathbf{v}_2$, namely, the second equation of (B.1), is proved as well. This implies that the whole statement of (B.1) is proved and thus we finish the proof for P_I.
We can prove the theorem for $P_{I_{sub}}$ and P_S in a similar way. Indeed, according to Lemma 1, we have:

$$P_{I_{sub}} = \max_{V} \frac{|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}_i \in \ker \psi_{\mathbf{k}}\}|}{|\mathcal{K}|}.$$

DOI: 10.1002/cpe

and

$$P_S = \max_{\mathbf{v} \notin V} \frac{|\{\mathbf{k} \mid \mathbf{v}_i \in \ker \psi_{\mathbf{k}}\} \cap \{\mathbf{k} \mid \mathbf{v} \in \ker \psi_{\mathbf{k}}\}|}{|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}_i \in \ker \psi_{\mathbf{k}}\}|}.$$

It then suffices to prove:

$$|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}_i \in \ker \psi_{\mathbf{k}}\}| = |\mathcal{K}^m| \tag{B.5}$$

and

$$|\{\mathbf{k} \mid \mathbf{v}_i \in \ker \psi_{\mathbf{k}}\} \cap \{\mathbf{k} \mid \mathbf{v} \in \ker \psi_{\mathbf{k}}\}| = |\mathcal{K}^{m+1}|. \tag{B.6}$$

We prove (B.5) firstly. Given m, we consider a special m-dimensional subspace $V = \mathrm{span}(\mathbf{v}_1, \cdots, \mathbf{v}_m)$ with $\mathbf{v}_i$ a vector where all entries are zeros but the i-th position. It is easy to see that for this specific V, it holds that $|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}_i \in \ker \psi_{\mathbf{k}}\}| = |\mathcal{K}^m|$. Then it suffices to prove that for any other m-dimensional subspace $V' = \mathrm{span}(\mathbf{v}'_1, \cdots, \mathbf{v}'_m)$, it also holds that $|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}'_i \in \ker \psi_{\mathbf{k}}\}| = |\mathcal{K}^m|$.
Indeed, firstly, we claim that we can always find a non-singular matrix $W \in \mathbb{F}_q^{n \times n}$ such that $\mathbf{v}'_i W = \mathbf{v}_i$ for all $1 \leq i \leq m$. To see why, if we denote Z as the collection of the row vectors $\mathbf{v}_1, \cdots, \mathbf{v}_m$, and consider all the column vectors in Z, we will find that the column vectors of Z span to the vector space $\mathbb{F}_q^m$. Then, since $\mathcal{K}$ satisfies invariant property, with this W we can have $|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}'_i \in \ker \psi_{\mathbf{k}}\}| = |W\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}_i \in \ker \psi_{\mathbf{k}}\}|$ and $|W\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}_i \in \ker \psi_{\mathbf{k}}\}| = |\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}_i \in \ker \psi_{\mathbf{k}}\}| = |\mathcal{K}^m|$, which implies that $|\{\mathbf{k} \in \mathcal{K} \mid \mathbf{v}'_i \in \ker \psi_{\mathbf{k}}\}| = |\mathcal{K}^m|$ and (A.5) is proved.
We can prove (B.6) in a similar way but choosing a special $\mathbf{v}$ as a vector where all entries are zeros but the $(m+1)$-th position. Details are omitted due to space limitations.
We thus finish the proof for $P_{I_{sub}}$ and P_S, and thus the whole lemma. □

C. PROOF OF LEMMA 3

Proof
It can be seen from the definition of invariant property and the knowledge that left multiplying by the non-singular $n \times n$ matrix P is equivalent to doing row operations described by P.
More precisely, we consider all the row operations on A. Since every row operation described by P results in a matrix $B = PA$ where $\langle B \rangle_R \subseteq \langle A \rangle_R$, the "only if" part is proved. On the other hand, for each B satisfying $\langle B \rangle_R \subseteq \langle A \rangle_R$, there always exists an $n \times n$ non-singular matrix P such that $B = PA$, the "if" part is proved. □

D. PROOF OF LEMMA 4

Proof
As it has been proved in Theorem 3 that $\mathcal{K}_A$ is a subspace and satisfies invariant property, we only need to prove that $\mathcal{K}_A$ is the minimal one. Assume $\mathrm{rank}(A) = d$ $(1 \leq d \leq t)$ and denote B_{A_r} as all the set of $B \in \mathbb{F}_q^{n \times t}$ with each row of B belongs to $\langle A \rangle$ and $\mathrm{rank}(B) = r$. It is easy to see that $\mathcal{K}_A = \{B_{A_r}, 1 \leq r \leq d\}$. Let $\mathcal{K}_S$ represent the minimal subspace $\mathcal{K}$ where $A \in \mathcal{K}$ and $\mathcal{K}$ satisfies invariant property. This way, to prove $\mathcal{K}_A$ is the minimal one is equal to prove that $\mathcal{K}_S \supseteq \{B_{A_r}, 1 \leq r \leq d\}$. We next prove this point. Note that as below we use M^T to denote the transpose of matrix M.

Firstly, it is obvious that $\mathcal{K}_S \supseteq B_{A_d}$, so we thus only need to prove $\mathcal{K}_S \supseteq \{B_{A_r}, 1 \leq r < d\}$.
(1): When $r = 1$. We prove $\mathcal{K}_S \supseteq B_{A_1}$.
If $d = 1$, then we are done. So it is sufficient to prove that $\mathcal{K}_S \supseteq B_{A_1}$ when $d > 1$.
[**Case 1:** $q = 2$] We will prove that, in this situation, we have

$$\begin{bmatrix} v & v & \mathbf{0} & \cdots & \mathbf{0} \end{bmatrix}^T = C^v \in \mathcal{K}_S, \quad \text{for } \forall\, \mathbf{0} \neq v \in \langle A \rangle. \tag{D.1}$$

DOI: 10.1002/cpe

Once (D.1) is proved, we have $\mathcal{K}_S \supseteq \{B_{C^v}\}$ where $B_{C^v} \in \mathbb{F}_q^{n\times t}$ with each row of B_{C^v} belonging to $\langle C^v \rangle$. Since v is randomly chosen from $\langle A \rangle$, we then have $\mathcal{K}_S \supseteq B_{A_1}$. We now prove (D.1) as below:
Since $d > 1$, we have for any $\mathbf{0} \neq v \in \langle A \rangle$, there exists $v_1 \in \langle A \rangle, v_2 \in \langle A \rangle, v_1 \neq v_2$ such that $v = v_1 + v_2$. Moreover, there always exists two matrices $C_1 \in B_{A_d}, C_2 \in B_{A_d}$ such that the first two rows of them are exchanged but the other rows of them are equal to each other. Formally, we can write them as: $C_1 = \begin{bmatrix} v_1 & v_2 & C_{1_3} & C_{1_4} & \cdots & C_{1_n} \end{bmatrix}^T$, and $C_2 = \begin{bmatrix} v_2 & v_1 & C_{2_3} = C_{1_3} & C_{2_4} = C_{1_4} & \cdots & C_{2_n} = C_{1_n} \end{bmatrix}^T$. It is easy to see $C^v = C_1 + C_2 = \begin{bmatrix} v & v & \mathbf{0} & \cdots & \mathbf{0} \end{bmatrix}^T$. Now, since $\mathcal{K}_S$ is a subspace, then $C_1 + C_2 \in \mathcal{K}_S$, which implies that $C^v \in \mathcal{K}_S$.
[Case 2: $q > 2$] We will prove that, in this situation, we have

$$\begin{bmatrix} v & \mathbf{0} & \cdots & \mathbf{0} \end{bmatrix}^T = C^v \in \mathcal{K}_S, \quad \text{for } \forall\, \mathbf{0} \neq v \in \langle A \rangle. \tag{D.2}$$

Once (D.2) is proved, then similar to Case 1 above, we have $\mathcal{K}_S \supseteq B_{A_1}$.
Indeed, we always have such a $v_1 \in \langle A \rangle$ that $2v_1 = v$, and we also have two matrices $C_1 \in B_{A_d}, C_2 \in B_{A_d}$ described as below: $C_1 = \begin{bmatrix} v_1 & C_{1_2} & C_{1_3} & \cdots & C_{1_n} \end{bmatrix}^T$, and $C_2 = \begin{bmatrix} v_1 & C_{2_2} = (q-1)C_{1_2} & C_{2_3} = (q-1)C_{1_3} & \cdots & C_{2_n} = (q-1)C_{1_n} \end{bmatrix}^T$. Again, it is easy to see $C^v = C_1 + C_2 = \begin{bmatrix} v & \mathbf{0} & \cdots & \mathbf{0} \end{bmatrix}^T$. Since $\mathcal{K}_S$ is a subspace, then $C_1 + C_2 \in \mathcal{K}_S$, which implies that $C^v \in \mathcal{K}$.

(2): When $1 < r < d$**.** We prove $\mathcal{K}_S \supseteq B_{A_r}$. It is sufficient to take $D_1, D_2, \cdots, D_{r-1}, D_r$ as below, and claim $(D_1 + D_2 + \cdots + D_{r-1} + D_r) \in \mathcal{K}_S$:

$$D_1 = \begin{bmatrix} v_1 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \cdots & \mathbf{0} \end{bmatrix}^T, \qquad D_2 = \begin{bmatrix} \mathbf{0} & v_2 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \cdots & \mathbf{0} \end{bmatrix}_T, \cdots,$$

$$D_{r-1} = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & v_{r-1} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \end{bmatrix}^T, \; D_r = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & v_r & \mathbf{0} & \cdots & \mathbf{0} \end{bmatrix}^T$$

where randomly chosen $v_1, v_2, \cdots, v_{r-1}, v_r \in \langle A \rangle$ are linearly independent from each other.
Indeed, We have proved in **(1)** above that $D_1, D_2, \cdots, D_{r-1}, D_r \in \mathcal{K}_S$, since $\mathcal{K}_S$ is a subspace, then $(D_1 + D_2 + \cdots + D_{r-1} + D_r) \in \mathcal{K}_S$.
When we consider all such $v_1, v_2, \cdots, v_{r-1}, v_r$, we get $\mathcal{K}_S \supseteq B_{A_r}$.

Combing **(1)** and **(2)** above, we complete the proof in the lemma.

□