Leakage-Resilient Secret Sharing With Constant Share Size

Ivan Tjuawinata, Member, IEEE, and Chaoping Xing, Senior Member, IEEE

Abstract—In this work, we consider the leakage-resilience of algebraic-geometric (AG for short) codes based ramp secret sharing schemes extending the analysis on the leakage-resilience of linear threshold secret sharing schemes over prime fields that is done by Benhamouda et al. in the effort to construct linear leakage-resilient secret sharing schemes with constant share size. Since there does not exist any explicit efficient construction of AG codes over prime fields with constant field size, we consider constructions of AG codes over extension fields. Extending the Fourier analysis done by Benhamouda et al., one can show that concatenated AG codes over prime fields do produce some nice leakage-resilient secret sharing schemes. One natural and curious question is whether AG codes over extension fields produce better leakage-resilient secret sharing schemes than the construction based on concatenated AG codes. Such construction provides several advantages compared to the construction over prime fields using concatenation method. It is clear that AG codes over extension fields give secret sharing schemes with a smaller reconstruction threshold for a fixed privacy parameter $t$. In this work, it is also confirmed that indeed AG codes over extension fields have stronger leakage-resilience under some reasonable assumptions. Furthermore, we also show that AG codes over extension fields may provide strong multiplicative property which may be used in its application to the study of multiparty computation. In contrast, the same cannot be said for constructions based on concatenated AG codes, even when we are considering multiplication friendly embeddings. These advantages strongly motivate the study of secret sharing schemes from AG codes over extension fields. The current paper has two main contributions: (i) we obtain leakage-resilient secret sharing schemes with constant share sizes and unbounded numbers of players. Some of the schemes constructed without the use of concatenation also possesses strong multiplicative property (ii) via Fourier Analysis, we analyze the leakage-resilience of secret sharing schemes from codes over extension fields. This is of its own theoretical interest independent of its application to secret sharing schemes from algebraic geometric codes over extension fields.

Index Terms—Secret sharing scheme, algebraic geometric code, leakage-resilience.

I. INTRODUCTION

A secret sharing scheme, which enables a secret to be distributed among a group of players where each player receives a share, is a very important building block in the study of modern cryptography. Intuitively, it allows for any authorized set of players to use their share to recover the original secret while the shares of any forbidden set of players contain no information of the original secret. It has found many applications in fields such as secure multiparty computation [4], [9], [14], distributed authorities [6], [38], fair exchange [3], electronic voting [38], [44] and threshold cryptography [15], [16], [29], [46], [47]. There are also different variants of secret sharing schemes that provide different functionalities such as proactive secret sharing scheme [28], [52], [53], verifiable secret sharing [20], [41], [42], [50] and computationally secure secret sharing scheme [11], [34], [43].

All the variants we discussed so far have the same basic assumption, namely, any share is either fully corrupted or completely hidden from the adversary. However, such assumption may not be reasonable for all cases. Side-channel attacks may enable the adversary to get some partial information about all the shares. In this case, the previous investigations do not provide any privacy threshold. Such leak can also be shown to have large risk towards the privacy of the secret. A simple example can be found from additive secret sharing scheme over the field $\mathbb{F}_{2^w}$ for some positive integer $w$. In this scenario, it can be shown that leakage of just one bit from each share may leak a bit of the secret which can be used as a distinguisher between shares generated using the additive secret sharing scheme from uniformly random strings. Guruswami and Wootters [27] showed that when Shamir’s secret sharing scheme is used in some settings, a full recovery of the whole secret is even possible from just one-bit leakage from each share. Due to the high usage of secret sharing schemes over $\mathbb{F}_{2^w}$ [2], [13], such vulnerability is important to be considered. To address this, recently, there has been a new research direction which considers the security of secret sharing scheme under such leakage [1], [5], [7], [19], [24], [25], [40], [49].

The existence of leakage-resilient secret sharing schemes have been shown to be related to other fields. A leakage-resilient secret sharing scheme can be used to build...
an MPC scheme that is secure against semi-honest adversary enjoying some local leakage of shares of uncorrupted players [5]. In another direction, having such leakage-resilient secret sharing scheme shows that we cannot have the same secret sharing scheme or the related code to have the regenerating property with the same bandwidth since it is shown that any leak of such magnitude should not be sufficient to recover much information about the original secret.

In 2019, Benhamouda et al. [5] established the leakage resilience of linear Maximum Distance Separable codes over prime fields. More specifically, they provided leakage resilience of explicitly constructed Reed-Solomon-codes based secret sharing scheme better known as Shamir’s secret sharing scheme over prime field. Despite the wide use of Shamir’s secret sharing scheme, one of its main drawbacks is the need of the field size to be larger than the number of players. This implies that the share size increases as the number of players increases. It is then interesting to consider non-trivial explicit family of leakage resilient ramp secret sharing schemes with share size being a constant with respect to the number of players. Due to the relation between secret sharing scheme with the field of multiparty computation, it is then also interesting to consider (strong) multiplicative property and linearity of the resulting secret sharing scheme.

A. Existing Results

Leakage-resilient cryptography is a research topic that has attracted many attentions (see for example [17], [18], [23], [30], [32], [33]). We refer interested readers to the survey [31] for detailed overview of the progress on such direction. In particular, there have also been quite extensive studies on secret sharing schemes providing resilience against local leakage. Such research direction was first considered by Dziembowski and Pietrzak [19] and it can be mainly divided to two directions. The first direction is the study of non-linear secret sharing schemes specially constructed for their leakage-resilience properties (see for example [24], [35]). Such construction provides non-malleability property, which, intuitively provides a guarantee that with high probability, an adversary cannot generate a valid share. By definition, such secret sharing scheme cannot be linear or multiplicative. For this work, we are following another direction, which is to study a more general family of linear secret sharing schemes for their leakage-resilience properties. We will discuss in more detail the works in this direction.

In 2019, Benhamouda et al. [5] investigated the effect of leakage of partial information of all shares when threshold secret sharing schemes that are based on linear Maximum Distance Separable (MDS for short) codes over prime fields are considered. More specifically, given a secret element $s$ of a finite field $F_q$, the share for each party can be generated from linear combination(s) of $s$ along with some random field elements. Local leakage from each player can then be extracted as a function of his share. Such study was inspired by a result on regenerating codes by Guruswami and Wootters [27]. In their work, they discovered that in some settings, a secret that is being shared using Shamir’s secret sharing schemes over any finite field of characteristic 2 may be completely recovered just by using 1 bit of leakage from each share. More specifically, the result shown in [27, Corollary 2] states that when Reed-Solomon codes defined over a field $F$ of characteristic 2 of length $|F|$ and rate $\frac{1}{2}$ has a linear exact repair scheme where the total message required to recover one entry is $|F| - 1$ bits. This implies that the Shamir’s secret sharing scheme that corresponds to it has $|F| - 1$ players and the secret $s$ with its corresponding polynomial $f(x)$ such that $f(0) = s$ can be recovered by leaking in total $|F| - 1$ bits from the other players. In order to investigate the extent of such attack, Benhamouda et al. [5] considered the leakage-resilience of general linear threshold secret sharing schemes over prime fields. The resilience of a scheme to the leakage can be measured by finding the statistical distance between the leakage from different possible secrets. Intuitively, a secret sharing scheme is local leakage-resilient against $\theta$ corruption and $\mu$-bit of independent leakage if given the full shares of any $\theta$ players along with any $\mu$-bit information independently from each of the remaining shares, the adversary cannot learn much information regarding the original secret being secretly shared. We call such scheme to be $(\theta, \mu, \epsilon)$-LL resilient if the amount of information the adversary may learn, which is measured by the statistical distance of his view given different possible secrets, can be bounded by $\epsilon$. A formal definition of such term can be found in Definition 2. By analyzing the leakage-resilience of linear MDS codes over prime fields and using the close relation between linear threshold secret sharing schemes and linear MDS codes, Benhamouda et al. [5] provided some leakage-resilience measure for linear threshold secret sharing schemes over prime fields. Through this analysis, they discovered some families of additive secret sharing schemes that provide leakage-resilience even when less than 1 bit of randomness remains from each share. They also identified some Shamir’s secret sharing schemes that provide leakage-resilience when a constant fraction of each share is leaked.

Such study on the leakage-resilience of threshold secret sharing scheme over prime fields is then extended by Maji et al. [36]. In their work, they provide an improvement on the leakage-resilience of threshold secret sharing schemes over prime fields. They then proved that with overwhelming probability, a secret sharing scheme based on a random linear MDS codes over prime fields is leakage-resilient.

Concurrently, Nielsen and Simkin [40] have also considered the leakage-resilience of information theoretic threshold secret sharing schemes. Instead of considering the existence of threshold secret sharing schemes with strong leakage-resilience capability, they provided a lower bound for the share length to ensure leakage-resilience against unconditional adversary. Combined with the results in [5] and [36], these works identify the range of parameters of a Shamir’s secret sharing scheme that can provide some leakage-resilience capability.

B. Our Contribution

In order to achieve the objective that we have mentioned above, we consider the use of algebraic-geometric codes (AG codes for short). It is a well-known fact that codes over prime
fields provide better leakage-resilient secret sharing schemes than codes over extension fields. However, AG codes over prime fields cannot be explicitly constructed in polynomial time. So far, only AG codes over extension fields can be constructed in polynomial time [21]. In order to overcome this challenge, we have two approaches: (i) directly study the resilience of secret sharing schemes from AG codes over extension fields; (ii) consider leakage-resilience secret sharing schemes from concatenated AG codes over prime fields (i.e., concatenate AG codes over extension fields with some other codes over prime fields to get concatenated AG codes over prime fields);

First, we state the main result on the ramp secret sharing schemes we obtain from AG codes over extension fields. We note that for secret sharing schemes over extension fields of characteristic $p$, to obtain a leakage-resilient secret sharing scheme, the leakage rate from each share must be less than $\log p$ bits. This is due to the existence of a distinguishing attack utilizing $\log p$ bits leakage from each share. A more detailed discussion on this attack can be found in Section II-B.

We note that we only state our main results in the scenario when the extension degree is 2. This does not mean that our result is only applicable for this specific case. In general, all our constructions can also be done for any extension degree.

**Theorem 1:** Let $q = p^2$ for some prime $p$ and $\mathbb{F}_q$ be a finite field of $q$ elements. Then there exists an infinite family of ramp secret sharing schemes that can be explicitly constructed over $\mathbb{F}_q$ in polynomial time with share size $O(1)$ bits for $N$ players providing $T \leq N - \frac{2N}{\sqrt{q-1}}$ privacy and reconstruction level $R = T + \frac{N}{q-1} + 1$ such that any of such secret sharing schemes is $(\theta, \mu, \epsilon)$-LL resilient for any $\theta < T$ and $\mu < \log q$ where

$$
\epsilon = \min \left\{ \frac{q(N - T - \frac{2N}{\sqrt{q-1}}) \cdot c_{\mu} \cdot \theta + 1}{(N - T - \frac{2N}{\sqrt{q-1}}) \cdot c_{\mu} \cdot \theta + 1}, \frac{q(N - T - \frac{2N}{\sqrt{q-1}}) \cdot c_{\mu} \cdot \theta + 1}{(N - T - \frac{2N}{\sqrt{q-1}}) \cdot c_{\mu} \cdot \theta + 1} \right\},
$$

with $c_{\mu} = \frac{2\mu \sin \left( \frac{\mu}{q} \right)}{p \sin \left( \frac{\mu}{q} \right)}$ and $c_{\mu}' = \frac{2\mu \sin \left( \frac{\mu}{q} + \frac{\mu}{q-1} \right)}{p \sin \left( \frac{\mu}{q} \right)}$.

**Remark 1:** We would like to remark that the infinite family mentioned above refers to the existence of an infinite sequence of increasing positive integers $\{N_1, N_2, \cdots\}$ such that for any $i \in \{1, 2, \cdots\}$, there is a ramp secret sharing schemes that can be explicitly constructed over $\mathbb{F}_{q_i}$ in polynomial time which belongs to our family and it is defined for $N_i$ players. Here the share size is $O(1)$ with respect to the number of players, $N_i$. The share is an element of $\mathbb{F}_{q_i}$. Hence, its share size is $2 \log p$ bits. This remark also applies to the statement of Theorems 2 and 3 where their share size becomes $\log q$ bits.

Furthermore, a similar result as Theorem 1 can also be obtained for $q = p^w$ with any integer $w$. This can be found in Corollary VI.2.

Apart from considering an extension field, an alternative way to reduce the share size requirement with respect to the number of players is by concatenating a secret sharing scheme over an extension field with the trivial code over a base field. Such method results in a secret sharing scheme with a larger number of players each holding a share of smaller size. Applying this method, we have the following main result.

**Theorem 2:** Let $q$ be a prime and $\mathbb{F}_q$ be a finite field of $q$ elements. Then there exists an infinite family of ramp secret sharing schemes that can be explicitly constructed over $\mathbb{F}_q$ in polynomial time with share size $O(1)$ bits for $N$ players providing $T < \frac{N}{2} - \frac{2N}{3(q-1)}$ privacy and reconstruction level $R = \frac{N}{2} + T + \frac{N}{3(q-1)} + 1$ such that any of such secret sharing schemes is $(\theta, \mu, \epsilon)$-LL resilient for any $\theta < T$ and $\mu < \log q$ where

$$
\epsilon = q(N - 2T - \frac{N}{2} \cdot \frac{2N}{3(q-1)}) \cdot c_{\mu} \cdot \theta + 1
$$

where $c_{\mu} = \frac{2\mu \sin \left( \frac{\mu}{q} \right)}{q \sin \left( \frac{\mu}{q} \right)}$.

**Remark 2:** The reconstruction parameter $R$ in Theorem 2 is at least $N \left( \frac{1}{q} + \frac{1}{q-1} + \frac{2N}{3(q-1)} \right)$ larger than that given in Theorem 1. Furthermore, under some reasonable assumptions, the secret sharing schemes from algebraic geometry codes over extension fields given in Theorem 1 have stronger leakage-resilience property than those given in Theorem 2 (The comparison is given in Lemma VI.7). This shows a strong motivation to study secret sharing schemes over extension fields.

Similar to Theorem 1, the result in Theorem 1 also applies for a more general case where $q = p^w$ for some positive integer $w$ and the construction is based on AG-code defined over $p^{nw}$. Such result can be found in Corollary VI.4.

One of the properties provided by the AG code used in Theorem 1 is that with some careful choice of the parameters, it can be used to construct a secret sharing scheme that is strongly multiplicative, which is discussed in more detail in Section VI. This is a useful property of the secret sharing scheme when we want to multiply two secrets being secretly shared, which is essential in its application in constructing an MPC scheme. However, when concatenating the AG code with the trivial code to obtain an AG code over prime field as done in Theorem 1, the resulting secret sharing scheme no longer has the strong multiplicative property. So we consider the use of multiplication friendly embeddings or MFE for short [8]. Using MFE instead of the trivial code to transform the AG code to a code over prime field, although it results in a longer code, we may preserve the strong multiplicative property. Having such code, the resulting secret sharing scheme will possess the strong multiplicative property. Such construction, as well as the analysis of its leakage-resilience, is summarized in Theorem 3.

**Theorem 3:** Let $q$ be a prime and $\mathbb{F}_q$ be a finite field of $q$ elements. Then there exists an infinite family of ramp secret sharing schemes that can be explicitly constructed over $\mathbb{F}_q$ in polynomial time with share size $O(1)$ bits for $N$ players providing $T < \frac{N}{2} - \frac{2N}{3(q-1)}$ privacy and reconstruction level $R = \frac{N}{2} + T + \frac{2N}{3(q-1)} + 1$ such that any of such secret sharing schemes is $(\theta, \mu, \epsilon)$-LL resilient for any $\theta < T$ and $\mu < \log q$ where

$$
\epsilon = q(N - 2T - \frac{2N}{3(q-1)}) \cdot c_{\mu} \cdot \theta + 1
$$

where $c_{\mu} = \frac{2\mu \sin \left( \frac{\mu}{q} \right)}{q \sin \left( \frac{\mu}{q} \right)}$. 


Remark 3: It is easy to see that when the privacy threshold is fixed and \( q \) is sufficiently large (while still being a constant with respect to \( N \)), the scheme presented in Theorem 3 has a much larger reconstruction threshold than either Theorems 1 or 2. However, it can also be verified that its leakage-resilience is always stronger compared to that of the scheme described in Theorem 2. Similar to Theorem 2, the result in Theorem 3 is also true for a more general case where \( q = p^u \) for some prime \( p \) and positive integer \( u \) where the construction is based on AG-code defined over \( p^{uv} \) for some positive integer \( v \). Such result can be found in Corollary VI.6.

Remark 4: Note that although the constructions in both Theorem 3 and Corollary VI.6 have strong multiplicative property, it is not actually useful due to the fact that since \( v \geq 1 \), we must have \( R > \frac{1}{2} \). Hence it is impossible to recover the product of the two secrets from the product of the corresponding shares due to the lack of available players. This shows that even when we are using the multiplication friendly embedding in our concatenation, the resulting secret sharing scheme is still not strongly multiplicative. This provides an advantage of considering the AG-code-based secret sharing scheme over extension field.

Note that although the construction of leakage-resilient secret sharing schemes with constant share size and unbounded number of players through the use of concatenation may be achieved more easily, in general, the parameter of the ramp secret sharing schemes constructed using the concatenation method can be less flexible. More specifically, ramp secret sharing schemes constructed using the concatenation method generally have larger reconstruction threshold when the privacy threshold is fixed, an observation that is discussed in more detail in Proposition II.2. Such restriction is not present when we consider a ramp secret sharing scheme arising from AG codes over an extension field. However, the study of its leakage resilience can no longer directly use the result presented in [5].

It is then natural to consider whether the ramp secret sharing scheme defined over an extension field comes with advantages compared to the one obtained using concatenation method over a prime field. In order to investigate this, we are considering two main factors. The first factor we are considering is regarding their leakage-resilience. When comparing the leakage-resilience of two different secret sharing schemes, we consider the parameters such that the two schemes have similar number of players, number of corrupted players, privacy threshold and leakage rate. Given such requirements, we then compare their upper bounds for statistical distance between the distribution of information obtained by the adversary given various secrets. Such information comes from both the parties he corrupts as well as the information obtained from the leakage from other players. If a scheme comes with a smaller upper bound in such comparison, we say that such scheme has a stronger leakage-resilience. Using such technique to compare the AG-code based ramp secret sharing scheme over extension field and Concatenated AG code-based ramp secret sharing scheme over prime field, we show that with some reasonable assumptions, the ramp secret sharing scheme over extension field can provide a stronger leakage-resilience. Such result can be found in Lemma VI.7.

This shows that under some reasonable assumptions, in addition of having smaller reconstruction threshold, an AG code based ramp secret sharing scheme defined over an extension field also provides a better leakage-resilience compared to one obtained by trivial concatenation method.

The second factor that we are interested in is related to its application to secure multiparty computation, which is the (strong) multiplicative property. As has been discussed before, under some assumption on the parameters values, construction without the use of concatenation comes with a strong multiplicative property. On the other hand, even when we are using multiplication friendly embeddings, construction through the use of concatenation do not have any multiplicative property. This provides a further advantage of directly using AG-code-based-secret sharing scheme over extension field.

This shows that consideration of secret sharing schemes defined over an extension field may provide us with an interesting family of leakage-resilient secret sharing schemes over extension fields that may further be set to be (strongly) multiplicative. A summary of such comparison can be found in Table I and a more detailed discussion of it can also be found in Section VI-D. In the comparison below, let \( \Sigma_1, \Sigma_2 \) and \( \Sigma_3 \) be the secret sharing schemes constructed in Theorems 1, 2 and 3 respectively where we assume that they are defined over sufficiently large finite fields with approximately the same size \( q \), approximately the same number of players \( N \), approximately the same privacy level \( T \) as well as the same level of corruption \( \theta \) and leakage \( \mu \). Furthermore, we assume that for \( i = 1, 2, 3 \), \( \Sigma_i \) has reconstruction level \( R_i \) and leakage resilience level \( \epsilon_i \).

C. Our Techniques

The calculation of leakage-resilience depends on the statistical distance between the outputs of leakage functions given that the inputs are either a secret sharing using a specific scheme or a set of uniformly and independently sampled strings of the same length. In order to facilitate such calculation, we closely follow the proof idea of [5]. More specifically, we utilize Fourier Analysis to transform the statistical distance formula to a sum of some Fourier coefficients. When the underlying field is a prime field \( \mathbb{F}_p \), such Fourier coefficients are always pairwise distinct \( p \)-th roots of unity. Because of this, bounding such sum can then be reduced to the problem of bounding the sum of some pairwise distinct \( p \)-th roots of unity. When we generalize the underlying field to an arbitrary finite field \( \mathbb{F}_q \) for some prime power \( q = p^w \) where \( p \) is a prime and \( w \) is a positive integer that is larger than 1, the Fourier coefficients are now defined with respect to \( \omega_p^{Tr(i)} \) where \( Tr(\cdot) \) is the field trace of \( \mathbb{F}_{p^w} \) over \( \mathbb{F}_p \). Since the field trace function is not injective, although the Fourier coefficients are still \( p \)-th roots of unity, they are no longer guaranteed to be pairwise distinct. So, instead of bounding the sum of \( s \) pairwise distinct \( p \)-th roots of unity, we need to derive a bound of integer combinations of \( p \)-th roots of unity with the sum of the coefficients being fixed to \( s \). Such upper bound can be found in Lemma III.2.

Here we provide some intuition on how to establish such upper bound. Note that each \( \omega_p^{Tr(i)} \) has the same magnitude
while having different phases. Sum of two of such vectors are maximized when they have the same phase while it decreases as the phase difference between the two vectors increases. Hence the strategy to maximize the sum is to have as many vectors with the same phase as possible to be summed up. Once such vector is chosen, we can again maximize the sum by adding vectors with the same phase as the one we just chose until such vectors are exhausted. We can keep doing this until we have summed up $s$ of such vectors. Lemma III.2 confirmed that such strategy indeed leads to a tight upper bound of the sum.

Having such upper bound, we cannot apply it directly to the ramp secret sharing schemes we are interested in. This is because the adversary learns not only the leak from the shares, but he also learns the full share of some of the players he corrupted. Having such information, the remaining shares no longer follow the distribution of the original secret sharing scheme. Hence, instead of analysing the leakage-resilience of the secret sharing scheme itself, we need to consider the leakage-resilience for a more general linear or affine codes that we obtain after the corrupted shares are already considered.

In the following, we present the leakage-resilience results that applies to any linear codes with leakage defined over its coordinates.

**Table I**

| Factor | $\Sigma_1$ | $\Sigma_2$ | $\Sigma_3$ |
|--------|------------|------------|------------|
| Constructibility and Reconstruction Level | $\frac{N}{2} - \frac{N}{q-1} \leq T \leq N - \frac{2N}{q-1}$ | Possible | Impossible | Impossible |
| | $\frac{N}{3} - \frac{2N}{3(q-1)} \leq T < \frac{N}{2} - \frac{N}{q-1}$ | Possible | Possible | Impossible |
| | $T < \frac{N}{3} - \frac{2N}{3(q-1)}$ | Possible | Possible | Possible |
| Multiplicativity | $\frac{N}{2} - \frac{N}{q-1} \leq T \leq N - \frac{2N}{q-1}$ | Not Multiplicative | Not Multiplicative | Not Multiplicative |
| | $\frac{N}{3} - \frac{2N}{3(q-1)} \leq T < \frac{N}{2} - \frac{N}{q-1}$ | Multiplicative | | |
| | $T < \frac{N}{3} - \frac{2N}{3(q-1)}$ | Strongly Multiplicative | | |

**Leakage Resilience**

$\epsilon \leq \epsilon_1 \leq \epsilon_2$

**D. Application of Results**

As has been discussed, secret sharing schemes are widely used in many applications such as multiparty computation. Having the leakage-resilience analysis on secret sharing schemes, either additive, Shamir or Algebraic Geometric code based secret sharing schemes, provides us with a wider choice of secret sharing schemes to be used in such applications. Such analysis can also be used to investigate if a linear secret sharing scheme used in an application provides any leakage-resilience which can be a useful factor in the consideration of which linear secret sharing schemes to be used in different applications. Here we briefly discuss the application of leakage-resilient secret sharing scheme in the construction of secure multiparty computation scheme as has been analysed in [5]. First, we provide a short intuition on the leakage-resilience of MPC schemes. A complete discussion on the definition of leakage-resilient MPC protocol can be found in [5]. Intuitively, given an MPC protocol $\Pi$ conducted by $n$ parties to compute a function $f$ with each party $U_i$ having transcript $\text{View}_i$ for $i = 1, \ldots, n$, a semi-honest adversary can corrupt a subset of parties $\Theta \subseteq \{U_1, \ldots, U_n\}$ of size $|\Theta| = \theta < n$. In addition to the $\theta$ corrupted parties, for any $i = 1, \ldots, n$, the adversary also defines a leakage function $\tau_i : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n$ with $\mu$ bits output that the adversary learns $\tau_i(\text{View}_i)$, which is the $\mu$ bits leaked information from the transcript of $U_i$. Hence the adversary may learn the transcript of the corrupted parties and the $\mu$ bits of information from all other parties. The protocol $\Pi$ is said to provide leakage-resilience if the distribution of the information obtained by the server can be simulated by a simulator with access only to the ideal simulator of $\Pi$. It was shown in [5] that a leakage-resilient GMW-type MPC protocol using Beaver triples with preprocessing can be constructed from any linear leakage-resilient secret sharing scheme [5, Theorems 5.5 and 5.6]. Due to the generality of these results, they are also applicable for the linear leakage-resilient secret sharing schemes provided in Theorems 1, 2 and 3.

**E. Organization**

This paper is organized as follows. In Section II, we define some notations that will be used throughout the paper and briefly discuss some basic concepts that are useful in our discussion. Section III provides some review on Fourier Analysis and discussion on some results that are essential in our
investigation of leakage-resilience for secret sharing schemes defined over finite fields. Section IV discusses and proves the leakage-resilience results for general linear codes defined over arbitrary finite fields. This result is then used to provide some leakage-resilience property of additive and Shamir’s secret sharing schemes that are defined over arbitrary finite fields. Lastly, such result is then used to investigate the local leakage-resilience of ramp secret sharing schemes that are defined based on algebraic geometric codes, which can be found in Section VI.

II. Notation and Preliminaries

A. Notation

Throughout the paper, we use \( \mathbb{Z} \) and \( \mathbb{C} \) to denote the ring of integers and field of complex numbers respectively, \( 1 = \sqrt{-1} \in \mathbb{C} \) the imaginary number and \( U_1 = \{ x \in \mathbb{C} : |x| = 1 \} \). For a prime \( p \), let \( q \) be a power of \( p \), i.e. \( q = p^w \) for some positive integer \( w \). For any positive integers \( a \) and \( b \), we denote by \( \mathbb{F}_a \) and \( \mathbb{F}_a^{x \times b} \) the set of vectors over \( \mathbb{F}_a \) of length \( a \) and the set of matrices over \( \mathbb{F}_a \) with \( a \) rows and \( b \) columns respectively. Lastly, for any positive integer \( n \), we denote by \([n]\) the set \( \{ 1, 2, \ldots, n \} \).

Let \( S \) be any finite set. We use \( x \sim S \) to denote that \( x \) is sampled uniformly at random from the finite set \( S \). In other words, \( \mathbb{E}_{x \sim S}[f(x)] = \frac{1}{|S|} \sum_{x \in S} f(x) \).

For any polynomials \( p(x) \) and \( f(x) \), we define \( p(x)^{\alpha}(f(x)) \) if \( p(x)^{\alpha}f(x) \) but \( p(x)^{\alpha+1}f(x) \). That is, \( \alpha \) is the multiplicity of \( p(x) \) in \( f(x) \).

Given a set \( T \) of size \( n \) where its elements are indexed by integers from \( 1 \) to \( n \), \( T = \{ t_1, \ldots, t_n \} \) and \( S_T \subseteq T \), we denote by \( v(S_T) \) the vector of length \( |S_T| \) containing \( v_i \) for any \( t_i \in S_T \). In particular, this also applies when \( T = [n] \) and \( t_i = i \).

B. Linear Secret Sharing Scheme

Let \( U = \{ U_1, \ldots, U_n \} \) be a finite set of players. A forbidden set \( \mathcal{F} \) is a family of subsets of \( U \) such that for any \( A \subseteq \mathcal{F} \) and \( A' \subseteq A \), we must have \( A' \notin \mathcal{F} \). For any \( t < n \), we define \( \mathcal{F}_{t,n} \) to be the forbidden set containing all subsets of \( U \) of size at most \( t \). On the other hand, a qualified set \( \Gamma \) is a family of subsets of \( U \) such that for any \( B \in \Gamma \) and \( B' \subseteq B \), we must have \( B' \in \Gamma \). For any \( r \leq n \), we define \( \Gamma_{r,n} \) to be the qualified set containing all subsets of \( U \) of size at least \( r \). For any forbidden set \( \mathcal{F} \) and a qualified set \( \Gamma \) over \( U \) such that \( \mathcal{F} \cap \Gamma = \emptyset \), the pair \((\mathcal{F}, \Gamma)\) is called an access structure.

A secret sharing scheme with access structure \((\mathcal{F}, \Gamma)\) over \( \mathbb{F}_q \) on \( U \) is a pair of functions \((\text{Share}, \text{Rec})\) where \text{Share} is a probabilistic function that calculates the random shares for the \( n \) players given the secret. For any secret \( s \in \mathbb{F}_q \), if \( (s_1, \ldots, s_n) = \text{Share}(s) \), for any \( A \subseteq U \), we denote by \( s^A = (s_i)_{U_i \in A} \), the vector containing the shares of all players \( U_i \in A \). On the other hand, \text{Rec} accepts shares from a set of players in \( U \) and attempt to recover the original secret that satisfies the following requirements:

1. For any \( B \in \Gamma \), given the shares of \( U_i \in B \), \text{Rec} returns the original secret.
2. For any \( A \in \mathcal{F} \), the shares of \( U_i \in A \) does not give any information regarding the secret. That is, the joint distribution of the shares received by \( U_i \in A \) is independent of the secret.

A secret sharing scheme with access structure \((\mathcal{F}, \Gamma)\) over \( \mathbb{F}_q \) on \( U \) is defined as follows. Fix a positive integer \( m \) and \( V_1, \ldots, V_n \) subspaces of \( \mathbb{F}_q^m \). We also fix \( u \in \mathbb{F}_q^m \setminus \{0\} \). For any \( A \subseteq [n] \), define \( V_A = \sum_{i \in A} V_i \), which is the smallest subspace containing \( V_i \) for all \( i \in A \). We further fix \( \phi \) a basis of \( V_i \). An LSSS \((\text{Share}, \text{Rec})\) is defined as follows. Let \( s \in \mathbb{F}_q \) be the secret. Then the \text{Share} function starts by choosing a random linear map \( \phi : \mathbb{F}_q^m \to \mathbb{F}_q \) such that \( \phi(u) = s \). The share for player \( U_i \) is then defined as \( s_i = \phi(V_i^*) = \{ \phi(x) : x \in V_i^* \} \).

Now we define the function \text{Rec}. Let \( B \subseteq U \) be such that \( u \in V_B \). Due to the linearity of \( \phi \) and the fact that \( u \in V_B \), there exists a vector \( w = \sum_{t \in \Gamma \cap \mathcal{F}} V_i^* \) such that \( s = \phi(u) = w(s_i)_{U_i \in B} \). This further proves that the qualified set \( \Gamma \) of this LSSS is \( \Gamma = \{ B \subseteq U : u \in V_B \} \). A simple algebraic manipulation tells us that \( \mathcal{F} = \{ A \subseteq U : \exists \kappa : \mathbb{F}_q^n \to \mathbb{F}_q, \kappa(x) = 0 \forall x \in V_A \text{ and } \kappa(u) = 1 \} \). For the remainder of the paper, we only consider linear secret sharing schemes.

A linear secret sharing scheme \( \Sigma \) is said to be multiplicative if there is a vector \( \lambda \in \mathbb{F}_q^n \) such that for any two secrets \( s, s' \in \mathbb{F}_q \) with their respective shares \( \text{Share}(s) = \{ s_1, \ldots, s_n \} \) and \( \text{Share}(s') = \{ s'_1, \ldots, s'_n \} \), \( \lambda \cdot \text{Share}(s) = \{ \lambda s_1, \ldots, \lambda s_n \} \) for any \( i = 1, \ldots, n \), \( \lambda \cdot \text{Share}(s') = s \cdot \text{Share}(s') \) where \( \cdot \) represents the standard inner product. Furthermore, a linear secret sharing \( \Sigma \) is said to be \( t \)-strongly multiplicative if it has \( t \)-privacy and for any two secrets \( s, s' \in \mathbb{F}_q \) and \( (s_1, \ldots, s_n) = \text{Share}(s), (s'_1, \ldots, s'_n) = \text{Share}(s') \), \( ss' \) can be recovered from any \( n - t \) entries of \( (s_1, \ldots, s_n) \).

To model leakage-resilient secret sharing, first we discuss the local leakage model as proposed in \[24\] and \[5\]. In short, the adversary can provide an arbitrary independent leakage functions for each party with a fixed output length that will provide the leakage of information from each of the share to the adversary. We note that this information is provided in addition to the capability of the adversary to corrupt some number of players. The following definitions formalize the concept of leakage function and leakage-resilience.

Definition 1 (Leakage Function): Let \( \tau = (\tau_1, \ldots, \tau_n) \) be a vector of functions where for each \( i = 1, \ldots, n \), \( \tau_i : \{0, 1\}^{\Gamma_{|T|}} \to \{0, 1\}^{\mathbb{F}_q^2} \). Then for a secret sharing \( (s_1, \ldots, s_n) = \text{Share}(s) \) of a secret \( s \in \mathbb{F}_q \), define \( (b_1, \ldots, b_n) = \tau(s_1, \ldots, s_n) = (\tau_1(s_1), \ldots, \tau_n(s_n)) \). Given a set of players
$\Theta \subseteq U$ and $\mu$ bits output leakage function $\tau$. We define the information learned by the adversary on a secret sharing $s = (s_1, \ldots, s_n) = \text{Share}(s)$ as

$$\text{Leak}_{\Theta, \tau}(s) \triangleq \left(s^{(0)}, (\tau_1(s_i))_{i \in \Theta} \right).$$

Next, we define the concept of local leakage-resilient or LL resilience for short.

**Definition 2 (Local Leakage-Resilience):** Let $\Theta \subseteq U$ be a set of players. A secret sharing scheme $(\text{Share}, \text{Rec})$ is said to be $(\Theta, \mu, \epsilon)$-local leakage-resilient (or $(\Theta, \mu, \epsilon)$-LL resilient) if for any leakage function family $\tau = (\tau_1, \ldots, \tau_n)$ where each $\tau_i$ has a $\mu$-bit output and for every pair of secrets $s_0, s_1 \in \mathbb{F}_q$, we have

$$SD \left( \{\text{Leak}_{\Theta, \tau}(s) : s = \text{Share}(s_0)\}, \{\text{Leak}_{\Theta, \tau}(s) : s = \text{Share}(s_1)\} \right) \leq \epsilon. $$

For a positive integer $\theta \leq n$, we say a secret sharing scheme $(\text{Share}, \text{Rec})$ is $(\theta, \mu, \epsilon)$-LL resilient if for any $\Theta \subseteq U, |\Theta| \leq \theta$, it is $(\Theta, \mu, \epsilon)$-LL resilient.

We conclude this subsection by providing an attack that shows that any linear secret sharing scheme over $\mathbb{F}_{p^m}$ does not provide any leakage-resilience if the leak is beyond $\log p$ bits even when no party is fully corrupted. The attack provided below is a generalization of the attacks on additive and Shamir’s secret sharing scheme over fields of characteristic two. Recall that for any $\alpha \in \mathbb{F}_q$, by fixing an $\mathbb{F}_p$-basis of $\mathbb{F}_q$, $\{\lambda_1, \ldots, \lambda_w\}$, we can see $\alpha$ as a vector of length $w$ over $\mathbb{F}_p$. If $\alpha = \sum_{i=1}^{w} \alpha_i \lambda_i$, for some $\alpha_i \in \mathbb{F}_p$, we define $\varphi_p(\alpha) = \alpha_1 \in \mathbb{F}_p$. We will first describe the attack on additive secret sharing schemes over $\mathbb{F}_p$ of characteristic $p$.

Let $s \in \mathbb{F}_q$ be the secret and suppose that $s = \sum_{i=1}^{w} s^{(1)}_i \lambda_i$ for some $s_1, \ldots, s_n \in \mathbb{F}_p$. In order to share such secret using additive secret sharing scheme, $n$ random elements $s_1, \ldots, s_n$, of $\mathbb{F}_q$ is uniformly sampled with the condition that $s_1 + \cdots + s_n = s$. We further assume that for any $i = 1, \cdots, n$, there exists $s^{(1)}_i \cdots, s^{(w)}_i \in \mathbb{F}_p$ such that $s_i = \sum_{j=1}^{w} s^{(j)}_i \lambda_j$. It is then easy to see that $s^{(1)} = \sum_{i=1}^{n} s^{(1)}_i$. This implies that the leakage of $\varphi_p(s_i)$ for $i = 1, \cdots, n$ completely leaks the value of $s^{(1)}$ even when no party is fully corrupted. Now we extend such attack to any linear secret sharing scheme.

Consider a linear secret sharing scheme with access structure $(\mathcal{F}, \Gamma)$ over $\mathbb{F}_q$ on $U$ such that $\Gamma \neq \emptyset$. Then it is easy to see that $U \in \Gamma$. Set $m, V_1, \cdots, V_n$ subspaces of $\mathbb{F}_q^n$ with their corresponding bases $V^*_1, \cdots, V^*_n$ and $u = (1, 0, \cdots, 0) \in \mathbb{F}_q^n \setminus \{0\}$ as defined above. For $i = 1, \cdots, n$, let $V^*_i = \{v_1, 1, \cdots, v_i, 1\}$. Recall that by the analysis above, since $U \in \Gamma$, there exists $w^* = (w_{11}, \cdots, w_{n,m}) \in \mathbb{F}_q^{m \times n}$ such that $u \in w^* \cdot (V_1, \cdots, V_i, \cdots, V_n)$. For $i = 1, \cdots, n$, we define $u_i = (w_{i1}, \cdots, w_{i,m}) \cdot (v_1, \cdots, v_i, \cdots, v_n)^T$. Furthermore, we define $s_i = (v_1, \cdots, v_i, \cdots, v_n)^T$. It is easy to see that $s_i$ can be locally computed by player $U_i$ and $s = \sum_{i=1}^{n} s_i$. Hence, we can see such $(s_1, \ldots, s_n)$ to be a valid additive secret shares of $s$. Hence we may launch the same attack discussed above to obtain a complete information leakage of $s^{(2)}$ with $[\log p]$-bits of independent leakage from each parties even when no party is fully corrupted.

### C. Linear Codes

In this section, we briefly discuss the concept of linear codes and in particular, a family of linear codes called Algebraic Geometric code or AG code for short.

**Definition 3 (Linear Codes):** Let $n, k, d$ be non-negative integers such that $d$ and $k$ are at most $n$. A linear code $C$ over $\mathbb{F}_q$ with parameter $[n, k, d]$ is a subspace $C \subseteq \mathbb{F}_q^n$ of dimension $k$ such that for any non-zero $c \in C \setminus \{0\}$, $wt_H(c) \geq d$ where for any vector $x = (x_1, \cdots, x_n)$, $wt_H(x)$ is defined to be the Hamming weight of $x$, i.e., $wt_H(x) = \{i : x_i \neq 0\}$. By the Singleton bound, we have the relation $d \leq n - k + 1$; a code that satisfies this bound with an equality is called a Maximum Distance Separable code or MDS code for short.

A linear $[n, k, d]$ code $C$ can be represented by its generator matrix $G \in \mathbb{F}_{q}^{k \times n}$. So given $G$, we have $C = \{x \cdot G : x \in \mathbb{F}_{q}^{k}\}$. Given a linear code $C$, its dual code $C^\perp$ is defined to be the dual subspace of $C$ over $\mathbb{F}_q$. That is, $C^\perp = \{x \in \mathbb{F}_{q}^{n} : \langle c, x \rangle = 0 \forall c \in C\}$ where $\langle \cdot, \cdot \rangle$ denotes the inner product operation. Then, $C^\perp$ is an $[n, n-k, d']\leq k-1$ code. A parity check matrix $H \in \mathbb{F}_{q}^{(n-k)\times n}$ of $C$ is a generator matrix of $C^\perp$. In the following, we provide the characterization of a linear code based on its generator matrix and its parity check matrix.

**Proposition II.1:** An $[n, k, d]$ linear code $C$ has minimum distance $d$ if and only if every set of $d-1$ columns of its parity check matrix $H \in \mathbb{F}_{q}^{(n-k)\times n}$ are linearly independent and there exists a set of $d$ columns of $H$ that is linearly dependent. Furthermore, for its generator matrix $G \in \mathbb{F}_{q}^{k\times n}$, the minimum distance of $C$ is $d$ if and only if any submatrix $G' \in \mathbb{F}_{q}^{k\times (n-d+1)}$ has full rank while there exists a submatrix $G' \in \mathbb{F}_{q}^{k\times (n-d)}$ that does not have full rank.

Next, we briefly discuss how we can construct a linear secret sharing scheme given a linear code $C$ of length $n+1$ over $\mathbb{F}_q$ with a generator matrix $G \in \mathbb{F}_{q}^{k\times (n+1)}$. Such construction directly follows the Massey secret-sharing scheme proposed in [37]. Suppose that the coordinates of any codeword of $C$ is indexed by $\{0, \cdots, n\}$. Without loss of generality, we assume that the 0-th coordinate of $C$ is not identically zero. Due to the linearity of $C$, the codewords of $C$ can be partitioned to $q$ equal size subcodes depending on the value of its 0-th coordinate. For $i = 0, \cdots, n$, denote by $V_i$, the $i$-th column of $G$ and for $i = 1, \cdots, n$, denote by $V_i = \text{span}_{\mathbb{F}_q}(V_i)$. Here we can define the linear secret sharing scheme using $(V_0, V_1, \cdots, V_n)$. Suppose that we want to secret share $s \in \mathbb{F}_q$. Since $C$ is not identically zero in the 0-th coordinate, there exists $c = (c_0, \cdots, c_n) \in C$ such that its 0-th coordinate equals 0. Let $u \in \mathbb{F}_q^n$ such that $u \cdot G = c$. We can then define $\phi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q$ such that for any $x \in \mathbb{F}_q^n$, we define $\phi(x) = u \cdot x$. Then for $i = 0, \cdots, n$, $\phi(V_i) = c_i$. Here we denote such transformation by $\Sigma(C)$.

Lastly, we consider a concatenation of a code over $\mathbb{F}_q$ where $q = p^w$ with an $\mathbb{F}_p$-isomorphism to obtain a code over $\mathbb{F}_p$ and investigate the result to its corresponding secret-sharing scheme.

**Proposition II.2:** Let $C \subseteq \mathbb{F}_{q}^{n}$ be a $q$-ary $[n, k, d]$ linear code where $q = p^w$ for some prime $p$ and positive integer $w$. We also assume that its dual $C^\perp$ is a $q$-ary $[n, n-k, d']$ linear code over $\mathbb{F}_q$. Let $w' \geq w$ and let $\Pi : \mathbb{F}_q \rightarrow \mathbb{F}_{q'}$ be an
injective $\mathbb{F}_p$ homomorphism between $\mathbb{F}_q$ and $\mathbb{F}_p^{|w|}$. Let

$$\tilde{C} \triangleq \Pi(C) = \left\{ (\Pi(c_1)||\cdots||\Pi(c_n)) : (c_1, \ldots, c_n) \in C \right\} \subseteq \mathbb{F}_p^{|w|}.$$ 

Then $\tilde{C}$ is a $p$-ary linear code with parameter $|n' = w'n, k' = \log d \cdot |d|$, and its dual $\tilde{C}^*$ is a $p$-ary linear code with parameter $|n' = w'n, n' - k', (d')^2 \geq d^2|$. Furthermore, if the secret sharing scheme constructed from $C$ using Massey's method provides $t$ privacy and $r$ reconstruction thresholds, the corresponding secret sharing scheme constructed from $\tilde{C}$ provides $t$ privacy and $(w' - 1)n + r$ reconstruction.

Proof: It is easy to see that $\Pi$ defines an injective $\mathbb{F}_p$-vector space homomorphism between $\mathbb{F}_q$ and $\mathbb{F}_p^{|w|}$ and it is a code over $\mathbb{F}_p$ of length $n' = w'n$. By linearity of $\Pi$, it is also clear that it has dimension $k' = |w|n$. Now note that for any non-zero $c \in \Pi(C)$, it has at least $d$ non-zero entries. Due to the injectivity and linearity of $\Pi$, it is easy to see that $\Pi$ maps each of such non-zero entry to a non-zero vector in $\mathbb{F}_p^{|w|}$. Hence $\Pi(c)$ contains at least $d$ non-zero entries. Hence $d' \geq d$. Using the same argument, we obtain the parameter for $\tilde{C}^{\perp}$. Lastly, we consider the secret sharing scheme $\Sigma(C)$ constructed from $\tilde{C}$.

Note that we can see that the shares of $\Sigma(\tilde{C})$ is obtained by first secretly sharing a secret $s \in \mathbb{F}_p$, seen as an element of $\mathbb{F}_q$ using the secret sharing scheme obtained from $C$ to $n$ intermediate players $u'_1, \ldots, u'_n$, and we apply $\Pi$ to each $u'_i$ to obtain $w$ shares in $\mathbb{F}_p$ to the corresponding $w'$ players. Then, it is easy to see that having $t$ out of the $nw'$ shares, it may contain information of at most $t$ of the intermediate shares $u'_i$.

Since this secret sharing scheme over $\mathbb{F}_q$ is assumed to have $t$ privacy, having $t$ out of the $nw'$ shares does not provide any information about the original secret $s$. Hence it has $t$ privacy. On the other hand, by Pigeonhole principle, it is easy to see that having $(w' - 1)n + r$ out of the $nw'$ shares guarantees the existence of at least $r$ values of $i \in \{1, \ldots, n\}$ such that we obtain all $w'$ entries of $\Pi(u'_i)$. Since $\Pi$ is injective, this means that we can recover $r$ out of the $nw'$ intermediate shares $u'_1, \ldots, u'_r$. Since this intermediate secret sharing scheme is assumed to have $r$ reconstruction, we can use such information to recover the secret $s$. This shows that the secret sharing scheme obtained from $\tilde{C}$ has $(w' - 1)n + r$ reconstruction, concluding the proof.

\[\square\]

D. Algebraic Geometric Code

In this section, we briefly discuss algebraic-geometric codes (AG codes for short) and their properties. Before we discuss the construction of AG codes, first we provide a brief discussion on algebraic function field. For a complete discussion on algebraic function field and the construction of AG code, see [51].

Let $K$ be a field. We say $F$ is an algebraic function field over $K$ in one variable if $F$ is a finite algebraic extension of $K(x)$ for some element $x \in F$ that is transcendental over $K$. The algebraic closure $\overline{K}$ of $K$ in $F$ contains all the elements in $F$ that is algebraic over $K$. The field $K$ is called the full constant field of $F$ if $\overline{K} = K$.

We define a map $\varphi: F \to \mathbb{Z} \cup \{\infty\}$ as a discrete valuation of $F/K$ if: (i) $\varphi(0) = \infty$ and $\varphi(x) = 0$ for any $x \in K \setminus \{0\}$, (ii) For any $x, y \in F$, $\varphi(xy) = \varphi(x) + \varphi(y)$ and $\varphi(x + y) \geq \min\{\varphi(x), \varphi(y)\}$, and (iii) $\varphi^{-1}(1) \neq \emptyset$.

Any discrete valuation $\varphi$ defines a valuation ring $O \triangleq \{x \in F : \varphi(x) \geq 0\}$ which is a local ring with its maximal ideal $P \triangleq \{x \in F : \varphi(x) > 0\}$, which is called a place. The collection of all places in $F$ is denoted by $P_F$. The discrete valuation and the valuation ring corresponding to a place $P$ are denoted by $\varphi_P$ and $O_P$ respectively. By definition, $F_P \triangleq O_P/P$ is a finite field extension of $K$. The degree of $P$, denoted by $\deg(P)$ is defined to be the extension degree $|F_P : K|$. We say $P$ is a rational place if $\deg(P) = 1$. For any $x \in O_P$, we define $x(P) \in F_P$, the residue class of $x$ modulo $P$. So if $P$ is a rational place, $x(P) \in K$.

For a non-zero $x \in F$, we denote its principal divisor by $\text{div}(x)$ which is defined as $\text{div}(x) = \sum_{P \in P_F} \varphi_P(x)P$. We also define $\text{div}(x)_0 = \sum_{P \in P_F \setminus \{P_0\}} \varphi_P(x)P$ and $\text{div}(x)_{\infty} = -\sum_{P \in P_F \setminus \{P_0\} \cup \{\infty\}} \varphi_P(x)P$ the zero and pole divisors of $x$ respectively. The divisor group, $\text{Div}(F)$ is the free Abelian group generated by all elements of $P_F$. An element $D \in \text{Div}(F)$ is called a divisor of $F$ and it can be written as $D = \sum_{P \in P_F} n_P(P)P$ where $n_P(D) \in \mathbb{Z}$ and $n_P(D) = 0$ for all but finitely many $P \in P_F$. The finite set of all places $P \in P_F$ where $n_P(D) \neq 0$ is called its support, denoted by $\text{Supp}(D)$.

We denote by $0$ a divisor of $F/K$ with $n_P(0) = 0$ for all $P \in P_F$. For any two divisors $D$ and $D'$, we say $D \geq D'$ if for any $P \in P_F$, we have $n_P(D) \geq n_P(D')$. Lastly, for any divisors $D = \sum_{P \in \text{Supp}(D)} v_P(D)P$, we define its degree by $\deg(D) \triangleq \sum_{P \in \text{Supp}(D)} v_P(D) \cdot \deg(P)$.

Next we define the Riemann-Roch space associated to a divisor. For any divisor $D$ of $F/K$, the Riemann-Roch space $L(D)$ associated with $D$ is defined as $L(D) \triangleq \{f \in F \setminus \{0\} : \text{div}(f) + D \geq 0\}$ union $\{0\}$. It can be shown that $L(D)$ is a finite dimensional $K$-vector space with dimension $\dim_K(L(D)) \geq \deg(D) + 1 - g$ where $g$ is the genus of $F$ and equality holds if $\deg(D) \geq 2g - 1$ [51].

Consider the case when $K = F_q$ and $F = F_q(x)$. Then every discrete valuation of $F_q/F_q$ is either $\varphi(x)$ for some irreducible polynomial $p(x)$ or $\varphi_\infty$ where for any $f \neq 0 \in F_q[x], \varphi_\infty(f/g) = a - b$ where $p(x)^a||f$ and $p(x)^b||g$ and $\varphi_\infty(f/g) = \deg(g) - \deg(f)$.

Now we are ready to construct algebraic geometric codes. Let $q = p^w$ for some prime $p$ and a positive integer $w$. Assume that $F_q/F_q$ is a function field of genus $g$ and at least $n + 1$ pairwise distinct rational places. We label the $n + 1$ points as $P_1, \ldots, P_n, P_\infty$ and $P = (P_1, \ldots, P_n)$. Set $m \geq 2g - 1$ and $D = mQ$. We define the AG code $C(D, P)$ as $C(D, P) = \{(x(P_1), \ldots, x(P_n)) : x \in \text{L}(D)\}$. Note that for any $i = 1, \ldots, n$, we have $n_P(x) = 0$, which implies that $x \in O_P$ and making $x(P_i)$ to be a well defined element of $F_q$. Hence $C(D, P) \subseteq F_q^n$. Furthermore, $C(D, P)$ is an $[n, k = m - g + 1, d \geq n - m] - $ linear code while its dual code $C^\perp$ is an $[n, n - m + g - 1, d' \geq m - 2g + 2] - $ linear code [51, Section 2.2].

We can construct a ramp secret sharing scheme based on algebraic-geometric code [10]. The construction is done in the
following manner. First, let $F/F_q$ be a function field of genus $g$. Let $n$ be a positive integer such that $F$ has at least $n + 2$ pairwise distinct rational places, denoted by $P_1, \ldots, P_n$. Define $F$ and $Q$ for some $q = p^m$. Fix an $F_q$-basis of $F/F_q$ and define an $F/F_q$-isomorphism between $F$ and $F_q$. It is easy to see that $\Pi$ is an $F/F_q$-isomorphism between $F$ and $F_q$. In particular, it is also an injective $F/F_q$-vector space homomorphism.

Let $C = C(D, P) \subseteq F_q^\alpha$ for some $q = p^m$. Fix an $F/F_q$-basis of $F/F_q$ and $F/F_q$ such that $F/F_q$ and $F/F_q$ are $F/F_q$-isomorphic. We denote $\Pi : F_q \to F_q^\alpha$ where for any $\alpha = \sum_{s=1}^{\infty} \alpha_s P_s$ in $F_q$, define $\Pi(\alpha) = (\alpha_1, \ldots, \alpha_n)$.

Let us consider the linear map $F/F_q \to F/F_q$. Obviously, $\Pi$ is a linear map with parameter $[m, k = w^m - w^g + w, d \geq m - n - 2g + 2]$. Furthermore, the corresponding secret sharing scheme provides $t = m - 2g - 1$ reconstruction.

E. Multiplication Friendly Embeddings

Lastly, we discuss about the concept of multiplication friendly embeddings. It was first studied in the context of asymptotic arithmetic complexity [12, 48] and was first proposed as a tool in the study of coding theory in [8].

Definition 4: Let $F_q$ be a finite field and consider $F_q^m$ an extension field of $F_q$ of extension degree $m$ for some positive integer $m$. A multiplication friendly embedding (MFE for short) of $F_q^m$ over $F_q$ is a triple $(\gamma, \sigma, \psi)$ where $\gamma$ is a positive integer which is the called the expansion of the embedding while $\sigma : F_q^m \to F_q$ and $\psi : F_q \to F_q^m$ are $F_q$-linear maps such that for any $x, y \in F_q^m$, we have $xy = \psi(\sigma(x) \cdot\sigma(y))$ where given two vectors $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_m)$ of the same length, $u \cdot v = (u_1v_1, \ldots, u_nv_n)$ is the Schur product of $u$ and $v$.

The existence of MFE enables us to transform a linear code $C \subseteq F_q^n$ such that $\Sigma(C)$ is a strongly multiplicative secret sharing scheme in an extension field $F_q^m$ to a linear code $C'$ over $F_q$ such that $\Sigma(C')$ is also a strongly multiplicative secret sharing scheme in the base field $F_q$ with some multiplicative constant increase of number of players. Such result can be found in the following theorem, which is a restatement of Theorems 2 and 7 in [8].

Theorem 4: [8, Restatement of Theorems 2 and 7] Let $C \subseteq F_q^{n+1}$ such that its 0th coordinate is not identically zero and $\Sigma(C)$ is $t_1 \geq t$-strongly multiplicative for some positive integer $t$. Suppose that there exists an MFE $(\gamma, \sigma, \psi)$ of $F_q^m$ over $F_q$. Define $C = \{c = (c_0, \ldots, c_m) \in C : c_0 \in F_q\}$. Let $\chi : F_q^m \times (F_q^m)^n \to (F_q^m)^{1+n+\gamma}$ and $\chi(c_0|c_1) \in (c_0|c_1) \ldots |(c_0|c_n)$ where $n = m - m - \ell - 1$. Then $C^* = \chi(C) = \{c(c) : c \in C\} \subseteq F_q^m$. Then $C^*$ is an $F_q^m$-linear code and $\Sigma(C^*)$ is a $t$-strongly multiplicative linear secret sharing scheme with $\gamma n$ players for some positive integer $t \geq t$.

Lastly, we recall the construction of MFE in various values of $F_q^m$.

Theorem 5: [8, Restatement of Theorems 8 and 9] Let $q$ be a prime power and $v \geq 2$ be a positive integer.

1. There exists an explicit MFE of $F_q^v$ over $F_q$ with expansion 3.
2. There exists an explicit MFE of $F_q^v$ over $F_q$ of expansion $(v+1)^2 = \frac{v(v+1)}{2}$. 
3) If \( q \geq 2v - 2 \), there exists an explicit MFE of \( \mathbb{F}_q \) over \( \mathbb{F}_q \) of expansion \( 2v - 1 \).

### III. Fourier Analysis

In this section, we provide a brief discussion on Fourier coefficients of a function along with some of the properties that are useful in the discussion later. For a more complete discussion, see [26].

Let \( G \) be any finite Abelian group. A character \( \chi : G \rightarrow \mathbb{C} \) is a group homomorphism between the group \( G \) and the multiplicative group \( \mathbb{U}_1 \). That is, for any \( a, b \in G \), \( \chi(a + b) = \chi(a) \cdot \chi(b) \). Let \( G \) be the set of characters of \( G \). Then equipped with point-wise product operation, \( G \) is a group that is isomorphic to \( G \). So we can write any element of \( G \) by \( \chi_g \) for some \( g \in G \) where the correspondence is done using a fixed isomorphism between \( G \) and \( G \).

Note that we are interested in the case when \( G = \mathbb{F}_q \) where \( q = p^w \) where \( p \) is a prime number and \( w \) is a positive integer. We denote by \( \omega_p = e^{2\pi i/p} \in \mathbb{C} \) the \( p \)-th root of unity. Let \( \alpha \in \mathbb{F}_q \). It can be shown that \( \chi_\alpha \in \mathbb{F}_q \) is defined to be \( \chi_\alpha(x) = \omega_p^{\text{Tr}_{\mathbb{F}_q/p}(\alpha x)} \) where \( \text{Tr}_{\mathbb{F}_q/p} \) is the field trace of \( \mathbb{F}_q \) over \( \mathbb{F}_p \). That is, \( \text{Tr}_{\mathbb{F}_q/p}(y) = \sum_{i=0}^{p-1} y^p^i \). For simplicity of notation, when \( \mathbb{F}_q \) and \( \mathbb{F}_p \) are clear, we use the notation \( \text{Tr} \) to represent \( \text{Tr}_{\mathbb{F}_q/p} \).

**Definition 5 (Fourier Coefficients):** For functions \( f : G \rightarrow \mathbb{C} \), the Fourier basis is composed of the group of characters \( \chi_g \in G \). Then the Fourier coefficient \( \hat{f}(\chi) \) corresponding to the characters \( \chi \in G \) is defined to be

\[
\hat{f}(\chi) = \mathbb{E}_{x \rightarrow G}[f(x) \cdot \chi(x)] \in \mathbb{C}.
\]

Recall that \( \mathbb{G} \) is isomorphic to \( G \). So we can identify an element \( \alpha \) of \( G \) with the character \( \chi_\alpha \in \mathbb{G} \). To simplify the notation, for any function \( f : G \rightarrow \mathbb{C} \) and \( \alpha \in G \), instead of writing \( f(\chi_\alpha) \), we write \( f(\alpha) \). Next we provide some existing properties of Fourier Transform.

**Lemma III.1:** Let \( G \) be a finite Abelian group and \( \mathbb{G} \) be its group of characters. We further let \( f, g : G \rightarrow \mathbb{C} \) be two functions. Then

1) (Parseval’s Identity) We have

\[
\mathbb{E}_{x \rightarrow G}[f(x) \cdot g(x)] = \sum_{\chi \in \mathbb{G}} \hat{f}(\chi) \cdot \hat{g}(\chi)
\]

where \( \hat{f}(\chi) \) is the Fourier coefficient of \( f \) corresponding to a character \( \chi \). In particular, \( \|f\|^2 = \|\hat{f}\|^2 \) where \( \|f\|^2 = \mathbb{E}_{x \rightarrow G}[|f(x)|^2] \) and \( \|\hat{f}\|^2 = \sum_{\chi \in \mathbb{G}} |\hat{f}(\chi)|^2 \).

2) (Fourier Inversion Formula) For any \( x \in G, f(x) = \sum_{\chi \in \mathbb{G}} \hat{f}(\chi) \cdot \chi(x) \).

We proceed by providing some analysis on some sums of roots of unity when \( G = \mathbb{F}_p \) for a prime \( p \). We note that the general proof structure and the flow follow the same direction as that of [5]. However, as can be seen in Lemma III.2, there are some differences. Suppose that \( \omega_p = e^{2\pi i/p} \in \mathbb{C} \) is a \( p \)-th root of unity. For any \( S \subseteq \mathbb{F}_p \), we define \( \omega_p^S = \sum_{x \in S} \omega_p^{\text{Tr}(x)} \). Note that in contrast to the prime field case, the summands of such sum can no longer be guaranteed to be pairwise distinct. Repetition can even be guaranteed if \( |S| \geq p \) since \( |\text{Tr}(\mathbb{F}_p)| = p \). Hence, the bound for \( |\omega_p^S| \) which is established for prime fields no longer holds in this more general case. Lemma III.2 provides an upper bound of such sums which only depends on the size of \( S \).

**Lemma III.2:** Let \( S \subseteq \mathbb{F}_p \) of size \( s \leq p^w - 1 \) and set \( s = s_1(1/p^{w-1} + s_2) \) for some \( 0 \leq s_1 \leq p-1 \) and \( 0 \leq s_2 \leq p^w - 1 - s_1 \). For any \( i = 0, \ldots, p-1 \), we set \( T_{is} = \{ x \in \mathbb{F}_p : \text{Tr}(x) = i \} \). Recall that \( |T_i| = p^{w-1} \) for any \( i \). We set \( T_{s} \) to be any subset of \( T_{s_1} \) of size \( s_2 \) and \( S^* = \bigcup_{i=0}^{s_1} T_i \cup T_{s_1} \). Then

\[
|\omega_p^S| \leq |\omega_p^{S^*}| = s_1 \sum_{i=0}^{s_1} \omega_p^i + (p^{w-1} - s_2) \sum_{i=0}^{s_1-1} \omega_p^i \leq p^{w-1} \frac{\sin(\pi s/p^w)}{\sin(\pi/p)}.
\]

**Proof:** Note that the equality can be easily verified by the definition of \( S^* \). Using triangle inequality and further algebraic manipulation, we get

\[
\begin{align*}
&= s_2 \sum_{i=0}^{s_1} \omega_p^i + (p^{w-1} - s_2) \sum_{i=0}^{s_1-1} \omega_p^i \\
&= s_2 \frac{|\omega_p^{s_1} - 1|}{|\omega_p - 1|} + (p^{w-1} - s_2) \frac{|\omega_p^{s_1} - 1|}{|\omega_p - 1|} \\
&= s_2 \frac{\sin(\pi s_1/p)}{\sin(\pi/p)} + (p^{w-1} - s_2) \frac{\sin(\pi s_1/p)}{\sin(\pi/p)} \\
&= \frac{p^{w-1}}{\sin(\pi/p)} \frac{s_2}{p^{w-1}} \cdot \sin \left( \frac{\pi}{p} \cdot (s_1 + 1) \right) + \frac{p^{w-1} - s_2}{p^{w-1}} \cdot \sin \left( \frac{\pi}{p} \cdot s_1 \right)
\end{align*}
\]

Note that \( 0 \leq p s_1/p < p (s_1 + 1)/p \leq \pi \). By the concavity of \( \sin(x) \) for \( x \in [0, \pi] \), we have that for any \( 0 \leq y < \pi \) and \( \alpha \in [0, 1] \), \( \sin(\alpha x + (1 - \alpha) y) \geq \alpha \sin(x) + (1 - \alpha) \sin(y) \). Setting \( \alpha = p s_1/p < p (s_1 + 1)/p \), noting that \( \alpha s_1 + (1 - \alpha)(s_1 + 1) = p^{w-1} s_1 s_1 = p^{w-1} \), we can have the term in the last equation \( \frac{p^{w-1}}{\sin(\pi/p)} \frac{s_2}{p^{w-1}} \cdot \sin \left( \frac{\pi}{p} \cdot (s_1 + 1) \right) + \frac{p^{w-1} - s_2}{p^{w-1}} \cdot \sin \left( \frac{\pi}{p} \cdot s_1 \right) \) to be at most

\[
\frac{p^{w-1}}{\sin(\pi/p)} \cdot \sin \left( \frac{\pi}{p} \cdot s_1 \right) = \frac{p^{w-1} \sin(\pi s/p^w)}{\sin(\pi/p)}.
\]

It remains to prove the first inequality of the claim. Suppose that \( S \subseteq \mathbb{F}_p \) of size \( s = s_1(1/p^{w-1} + s_2) \leq p^w - 1 \) for some \( 0 \leq s_1 \leq p-1 \) and \( 0 \leq s_2 \leq p^{w-1} - 1 \) has the largest value for \( |\omega_p^S| \) and set \( \xi = |\omega_p^S| \). That is, \( \xi = |\omega_p^S| \geq |\omega_p^S| \). For any \( i = 0, \ldots, p-1 \), define \( S_i = S \cap T_i \) and \( |S_i| = \theta(s) \geq 0 \) for each \( i \) and \( \sum_{i=0}^{s_1} \theta(s) = s \). Then \( \omega_p^S = \sum_{i=0}^{s_1} \theta(s) \omega_p^i \). First we consider the case when \( s \leq p^{w-1} \). For any \( x, y \in \mathbb{C} \) of magnitude 1, assuming that \( \theta \in [0, \pi] \) is the angle between \( x \) and \( y \), without loss of generality, we can write \( y = x \cdot e^{i\theta} \).
Then \(|x + y| = |1 + e^{i\theta}| = \sqrt{(1 + \cos(\theta))^2 + (\sin(\theta))^2}\). It is easy to see that \(|x + y|\) is a decreasing function as \(\theta\) grows from 0 to \(\pi\) where the value reaches its maximum \(|x + y| = 2\) when \(\theta = 0\) and its minimum \(|x + y| = 0\) when \(\theta = \pi\). This shows that if \(s \leq p^{w-1}, |\omega_p^S| \leq s\) and equality is achieved by setting \(S \subseteq T_i\) for some \(i \in \{0, \ldots, p-1\}\), proving the first inequality for this special case of \(s \leq p^{w-1}\). Now we suppose that \(s > p^{w-1}\) or equivalently, \(s_1 \geq 1\).

Note that the actual elements from each \(S_i\) do not affect \(\omega_p^S\) since any element from the same \(S_i\) contributes \(\omega_p^S\) to the sum. So we are only interested in the vector \(s = (s(0), \ldots, s(p-1))\). We further note that performing cyclic shift operation to \(s\) does not change \(|\omega_p^S|\). For any non-negative integer \(z\), we denote by \(g(z)\) to be the vector we obtained by cyclic shifting \(s\) to the right by \(z\) position and \(a_i^{(z)}\) be its \(i\)-th entry for \(i = 0, \ldots, p - 1\). So we can find a non-negative integer \(z\) such that

\[
\arg\min_{z \in \{0, \ldots, p-1\}} \left\{ y_z : g(z) \neq 0, \forall i > y_z, g(z) = 0 \right\}
\]

Without loss of generality, we can assume that \(y_0 = y \geq s_1 \geq 1\). Then \(\omega_p^S = \sum_{i=0}^y s(i)\omega_p^i\). Note that by the minimality of \(y, s(0)\) must be non-zero.

**Claim III.3:** There exists \(S' = \bigcup_{i=0}^y S'_{i} \subseteq \mathbb{F}_{p^w}\) and an integer \(a'\) where \(S_{i}' = T_i\) for any \(i = (a' + 1) \mod p\), \(S_{i}' = T_{i'}\) and \(S_{i'}' \subseteq T_{i'}\) such that \(|\omega_p^S'| \geq \xi\).

**Proof:** Note that if \(y = 1\), the claim is already true by setting \(S' = S\). So assume that \(y > 1\). Then there exists \(j^* \in \{0, \ldots, y - 1\}\) such that \(\omega_p^S\) lies between \(\omega_p^{j^*}\) and \(\omega_p^{j^*+1}\). Then for any \(i = 0, \ldots, j^*-1\), \(\omega_p^{i}\omega_p^{S} \leq \omega_p^{i}\omega_p^{j^*}\omega_p^{S}\) and for any \(i = j^* + 2, \ldots, y, \omega_p^{i}\omega_p^{S} \leq \omega_p^{j^*+1}\omega_p^{S}\). Here \(\alpha\) represents the inner product between the two complex numbers. More specifically, for any \(z, z' \in \mathbb{C}, \alpha \circ z' = [z][z']^\top \cos \theta \) where \(\theta\) is the angle between \(z\) and \(z'\).

Now suppose that there exists \(x \in \{1, \ldots, y - 1\}\) such that \(s(x) < p^{w-1}\). Then \(1 \leq x \leq j^*\) or \(j^* + 1 \leq x \leq y - 1\). We consider the case when \(1 \leq x \leq j^*\) while the proof for \(j^* + 1 \leq x \leq y - 1\) can be done in a similar way. As discussed before, \(s(0) > 0\). Hence there exists an element \(\alpha\) of \(S_0\). On the other hand, since \(s(x) < p^{w-1}\), the set \(T_x \setminus S_x\) is non-empty, suppose that \(\beta \in T_x \setminus S_x\). By the assumption above, we get that \(\omega_p^\beta \circ \beta = \omega_p^\alpha \circ \alpha\). Note that for the case of \(j^*+1 \leq x \leq y - 1\), we choose \(\alpha\) from \(S_y\) and \(\beta \in T_x \setminus S_x\).

Now consider \(\tilde{S} = S \cup \{\beta\} \setminus \{\alpha\}\). Then \(\omega_p^S = \omega_p^{S} + \beta - \alpha\). Note that \(|\omega_p^S| = |\omega_p^{S+2}\circ\beta - \alpha| + 2|\omega_p^{S}|\cdot|\beta - \alpha| \cdot \cos(\theta)|\) when \(\theta\) is the angle between \(\omega_p^{S}\) and \(\beta - \alpha\). Recall that \(\omega_p^\beta \circ (\beta - \alpha) \geq 0\). Hence \(\theta \in [-\frac{\pi}{2}, \frac{\pi}{2}]\). So it is easy to see that \(|\omega_p^{S+2}| \geq |\omega_p^{S}|^2\).

The claim is proved since we can keep repeating this process until the desired form is achieved.

Due to the invariance of the sum with respect to cyclic shift operation on \(s\), we can assume \(a' = 0\). So we can assume that \(S = S_0 \cup T_1 \cup \cdots \cup T_{S_1-1} \cup S_{S_1}\), where \(S_0 \subseteq T_0\) and \(S_{S_1} \subseteq T_{S_1}\). Note that since \(\omega_p^S\) is also invariant with respect to complex conjugation, without loss of generality, we can assume that \(\omega_p^S \circ 1 = \omega_p^S \circ \omega_p^{S_1}\). So if \(|S_0| < p^{w-1}\), a similar proof as the one used above can be used to prove that replacing an element \(\alpha\) of \(S_0\) from \(S\) with an element \(\beta \in T_0 \setminus S_0\) does not reduce the sum. So by repeating this step until \(S_0 = T_0\), we complete the proof.

**Remark 5:** We define a function \(\text{sinc} : \mathbb{R} \rightarrow \mathbb{R}\) where

\[
\text{sinc}(x) = \begin{cases} 1, & \text{if } x = 0, \\ \frac{\sin(x)}{x}, & \text{otherwise}. \end{cases}
\]

The upper bound for \(\|\omega_p^S\|\) established in Lemma III.2 can then be rewritten as

\[
|\omega_p^S| \leq s \frac{\text{sinc}(\pi s/p^w)}{\text{sinc}(\pi/p)}.
\]

Next we provide a relation between product of functions over a linear code over \(\mathbb{F}_{p^w}\) with the sum of products of their Fourier coefficients via the Poisson Summation formula.

**Lemma III.4 (Poisson Summation Formula over \(\mathbb{F}_{p^w}\):** Let \(p > 2\) be a prime and \(w\) be a positive integer. Let \(C \subseteq \mathbb{F}_{p^w}\) be a linear code with dual code \(C^\perp\). Let \(f_1, \ldots, f_n : \mathbb{F}_{p^w} \rightarrow \mathbb{C}\) be functions. Let \(\Lambda\) be defined as follows:

\[
\Lambda(f_1, \ldots, f_n) = E_{x \in \mathbb{C}} \prod_{i=1}^n f_i(x_i)
\]

where \(x = (x_1, \ldots, x_n)\). Then

\[
\Lambda(f_1, \ldots, f_n) = \sum_{\alpha \in C^\perp} \prod_{i=1}^n \tilde{f}_i(\alpha_i).
\]

The lemma can be shown using a similar proof idea as Lemma 4.16 of [5]. For completeness, proof can be found in Appendix A.

IV. LEAKAGE-RESILIENCE OF LINEAR CODES

Now we are ready to proceed to the discussions of our results. In this section, we investigate the statistical distance between leakage from codewords of a fixed linear code and the leakage from a random string. We note that the analysis mainly follows the analysis in [5] with some modifications to allow for results to be applicable for a larger family of codes, i.e., linear codes over any finite fields. The objective of this section is to prove the following two theorems. Firstly, we provide a bound on the statistical distance, which can be found in Theorem 6.

**Theorem 6:** Let \(C \subseteq \mathbb{F}_{p^w}\) be an \([n, k, d \leq n - k + 1]\) code with the dual code \(C^\perp\) which is an \([n, n - k, d^\perp \leq k + 1]\) code. Furthermore, let \(\tau = (\tau(1), \ldots, \tau(n))\) be any family of leakage functions where \(\tau(1) : \mathbb{F}_{p^w} \rightarrow \mathbb{F}_p^w\). For simplicity of notation, for any set \(S \subseteq \mathbb{F}_{p^w}\), we denote by \(\tau(S)\) the random variable \((y_1, \ldots, y_n)\) where \(y_i = \tau(x_i)\) and \(x = (x_1, \ldots, x_n)\) is uniformly sampled from \(S\).

Let \(c_\mu = 2^\mu \text{sinc}(\pi/2^\mu)\) which is less than 1 when \(2^\mu < p\). Then

\[
SD(\tau(C), \tau(U_n)) \leq \frac{1}{2} \cdot p^{w(n-k)} \cdot c_\mu^d.
\]

**Remark 6:** Following the definition in Remark 5, we note that here \(c_\mu = \frac{\text{sinc}(\pi/2^\mu)}{\text{sinc}(\pi/p)}\).
A. Proof of Theorem 6

Before we prove Theorem 6, we first discuss some supporting lemmas that will help in our proof.

**Lemma IV.1 (A Generalization of Lemma 4.15 in [5]):** Let $C \subseteq \mathbb{F}_{p^n}$ be any $[n, k, d \leq n - k + 1]$ linear code with dual distance $d^\perp$. Suppose that $d^\perp > \frac{2k}{n}$. Let $\{\tau^{(1)}, \tau^{(2)}, \ldots, \tau^{(n)}\}$ be any family of leakage functions where $\tau^{(j)} : \mathbb{F}_{p^n} \to \mathbb{F}_2$. For any $j = 1, \ldots, n$, $\ell_j \in \mathbb{F}_p^n$, and $x \in \mathbb{F}_{p^n}$, define $\mathbb{I}_{\ell_j} : \mathbb{F}_{p^n} \to \{0, 1\}$ where $\mathbb{I}_{\ell_j}(x) = 1$ if and only if $\tau^{(j)}(x) = \ell_j$. Then

$$SD(\tau(C), \tau(U_n)) = \frac{1}{2} \sum_{C \subseteq \mathbb{F}_2^{\mu \times n}} \left| \sum_{\mathbb{I}_{\ell_j} \in \tau^{(j)}} \prod_{\alpha \in C \setminus \{0\}} \mathbb{I}_{\ell_j}(\alpha_j) \right|.$$  

**Proof:** Recall that for any $S \subseteq \mathbb{F}_p^n$ and $\ell \in \mathbb{F}_2^{\mu \times n}$,

$$Pr_{x \in S}(\tau(x) = \ell) = \mathbb{E}_{x \in S} \left[ \prod_{j} \mathbb{I}_{\ell_j}(x_j) \right].$$

Hence,

$$SD(\tau(C), \tau(U_n)) = \frac{1}{2} \sum_{\ell} \left| Pr_{x \in C}(\tau(x) = \ell) - Pr_{x \in U_n}(\tau(x) = \ell) \right| = \frac{1}{2} \sum_{\ell} \left| Pr_{x \in C}(\prod_{j} \mathbb{I}_{\ell_j}(x_j)) - Pr_{x \in U_n}(\tau(x) = \ell) \right| = \frac{1}{2} \sum_{\ell} \sum_{\alpha \in C \setminus \{0\}} \prod_{j} \mathbb{I}_{\ell_j}(\alpha_j).
$$

where the last equality is based on Lemma III.4. Now note that when $x \in U_n$, for each $j = 1, \ldots, n$, $x_j$ is identically and uniformly distributed over $\mathbb{F}_p$. Hence, denoting $p = Pr_{x \in U_n}(\tau(x) = \ell)$, we have

$$p = \prod_{j=1}^{n} Pr_{x_j \in \mathbb{F}_p}(\tau^{(j)}(x_j) = \ell_j) = \prod_{j=1}^{n} \left( \frac{1}{p} \right)^{\ell_j} = \prod_{j=1}^{n} \mathbb{I}_{\ell_j}(0).$$

Since $0 \in C^{\perp}$,

$$SD(\tau(C), \tau(U_n)) = \frac{1}{2} \sum_{\ell} \left| \sum_{\alpha \in C \setminus \{0\}} \prod_{j=1}^{n} \mathbb{I}_{\ell_j}(\alpha_j) \right|. \phantom{\Bigg]}
$$

**Lemma IV.2 (A Generalization of Lemma 4.17 in [5]):** Let $\mu$ be a positive real number such that $2^\mu$ is an integer. Let $c_\mu = \frac{2^{\mu} \sin(\pi/2^\mu)}{p \sin(\pi/\mu)}$. For any sets $A_1, \cdots, A_{2^n} \subseteq \mathbb{F}_{p^n}$ such that $\sum_{i=1}^{2^n} |A_i| = p^w$, we have

$$\sum_{i=1}^{2^n} |\mathbb{I}_{A_i}(\alpha)| \leq c_\mu, \quad \text{if } \alpha \neq 0,$$

$$\sum_{i=1}^{2^n} |\mathbb{I}_{A_i}(\alpha)| = 1, \quad \text{if } \alpha = 0$$

where for any $A \subseteq \mathbb{F}_{p^n}$, $\mathbb{I}_A : \mathbb{F}_{p^n} \to \{0, 1\}$ is the characteristic function of the set $A \subseteq \mathbb{F}_{p^n}$.

**Proof:** First, note that $\mathbb{I}_A(0) = \mathbb{E}_x [\mathbb{I}_A(x) \cdot \omega_0^{x \tau(\alpha)x}] = \frac{|A|}{p}$, where $\omega_A$ has the same size as $A$. So by Lemma III.2,

$$\sum_{i=1}^{2^n} |\mathbb{I}_{A_i}(\alpha)| \leq \frac{1}{p^{w/\mu}} \sum_{i=1}^{2^n} |\omega_0^{\alpha A_i}| = \frac{1}{p^{w/\mu}} \sum_{i=1}^{2^n} \frac{\sin(\pi t_i/p^w)}{\sin(\pi/\mu)} \leq \frac{1}{p^{w/\mu}} \sum_{i=1}^{2^n} \frac{\sin(\pi t_i/p^w)}{\sin(\pi/\mu)}.$$

Note that since $\sin$ is a concave function between $[0, \pi]$, the sum is maximized if all $t_i = \frac{\pi}{2^\mu}$. Hence

$$\sum_{i=1}^{2^n} |\mathbb{I}_{A_i}(\alpha)| \leq \frac{1}{p^{w/\mu}} \sum_{i=1}^{2^n} \sin(\pi t_i/p^w) \leq \frac{2^\mu \sin(\pi/2^\mu)}{p^{w/\mu}}.$$

We are now ready to prove Theorem 6. First we restate the theorem.

**Theorem 6:** Let $C \subseteq \mathbb{F}_{p^n}$ be an $[n, k, d \leq n - k + 1]$ code with the dual code $C^{\perp}$ which is an $[n, n - k, d^{\perp} \leq k + 1]$ code. Furthermore, let $\tau = (\tau^{(1)}, \cdots, \tau^{(n)})$ be any family of leakage functions where $\tau^{(j)} : \mathbb{F}_{p^n} \to \mathbb{F}_2$. For simplicity of notation, for any set $S \subseteq \mathbb{F}_{p^n}$, we denote by $\tau(S)$ the random variable $(y_1, \cdots, y_n)$ where $y_i = \tau(x_i)$ and $x = (x_1, \cdots, x_n)$ is uniformly sampled from $S$. Let $c_{\mu} = \frac{2^{\mu} \sin(\pi/2^\mu)}{p^{\mu}}$ (which is less than 1 when $2^\mu < p$). Then

$$SD(\tau(C), \tau(U_n)) \leq \frac{1}{2} \cdot 2^{w(n-k)} \cdot c_{\mu}d^{\perp}.$$  

**Proof:** By Lemma IV.1 and triangle inequality, we have

$$SD(\tau(C), \tau(U_n)) = \frac{1}{2} \sum_{\ell} \left| \sum_{\alpha \in C^{\perp} \setminus \{0\}} \prod_{j=1}^{n} \mathbb{I}_{\ell_j}(\alpha_j) \right| \leq \frac{1}{2} \sum_{\ell} \sum_{\alpha \in C^{\perp} \setminus \{0\}} \prod_{j=1}^{n} \mathbb{I}_{\ell_j}(\alpha_j) \leq \frac{1}{2} \sum_{\alpha \in C^{\perp} \setminus \{0\}} \sum_{j=1}^{n} \mathbb{I}_{\ell_j}(\alpha_j).$$
Note that for any \( j, (\tau^{(j)})^{-1}(\ell_j) \) partitions \( \mathbb{F}_p \) to \( 2^\mu \) sets. So by Lemma IV.2,

\[
\sum_{\ell_j} \sum_{\alpha \in C_{\downarrow} \setminus \{0\}} |\widehat{I}_{\ell_j}(\alpha_j)| \leq c_\mu, \quad \text{if } \alpha_j \neq 0,
\]

\[
\sum_{\ell_j} \sum_{\alpha \in C_{\downarrow} \setminus \{0\}} |\widehat{I}_{\ell_j}(\alpha_j)| = 1, \quad \text{if } \alpha_j = 0
\]

Note that for any \( \alpha \in C_{\downarrow} \setminus \{0\} \), \( |\{ j : \alpha_j \neq 0 \}| \geq d^\perp \). Hence, since \( c_\mu \leq 1, \)

\[
SD(\tau(C), \tau(U_n)) \leq \frac{1}{2} \sum_{\alpha \in C_{\downarrow} \setminus \{0\}} \prod_{\ell_j} |\widehat{I}_{\ell_j}(\alpha_j)|
\]

\[
= \frac{1}{2} \sum_{\alpha \in C_{\downarrow} \setminus \{0\}} c_{\mu}(\alpha)
\]

\[
\leq \frac{1}{2} \cdot \left| C_{\downarrow} \right| \cdot d^\perp = \frac{1}{2} p^{\mu(n-k)} d^\perp.
\]

\[\square\]

### B. Proof of Theorem 7

In this subsection, we aim to prove Theorem 7 which provides an alternative direction of bounding the statistical distance from the result in Theorem 6. Before we prove Theorem 7, first we provide some supporting lemmas that are useful in the proof of Theorem 7.

Firstly, instead of finding a bound for the sum of the Fourier coefficients of \( I_{A_i} \) in each character separately as has been done in Lemma IV.2, we consider the bound where for each \( A_i \), we consider the character that maximizes each Fourier coefficients separately.

**Lemma IV.3:** Let \( \mu \) be some positive real such that \( 2^\mu \) is an integer. Let \( c_\mu = \frac{2^\mu \sin(\pi/2^\mu)}{\sin(\pi/2)} \). For any sets \( A_1, \ldots, A_{2^\mu} \subseteq \mathbb{F}_p^\mu \) such that \( \sum_{i=1}^{2^\mu} |A_i| = p^\mu \), we have

\[
\sum_{\alpha \in C_{\downarrow} \setminus \{0\}} \left| I_{A_i}(\alpha) \right| \leq c_\mu.
\]

Proof: For simplicity of notation, let \( SD = SD(\tau(C), \tau(U_n)) \). Recall that \( \alpha \in C_{\downarrow} \setminus \{0\} \) if and only if there exists \( \beta \in \mathbb{F}_p^{n-k} \setminus \{0\} \) such that \( \alpha = \beta H \)

where for each \( j, \alpha_j = \langle \beta, h_j \rangle \). By Lemma IV.1 and Cauchy-Schwarz inequality, we have

\[
SD = \frac{1}{2} \sum_{\alpha \in C_{\downarrow} \setminus \{0\}} \left| I_{A_i}(\alpha) \right|
\]

\[
= \frac{1}{2} \sum_{\alpha \in C_{\downarrow} \setminus \{0\}} \prod_{j=1}^{n} \left| \widehat{I}_{\ell_j}(\langle \beta, h_j \rangle) \right|
\]

\[
= \frac{1}{2} \sum_{\beta \in \mathbb{F}_p^{n-k} \setminus \{0\}} \prod_{j=1}^{n} \left| \widehat{I}_{\ell_j}(\langle \beta, h_j \rangle) \right|
\]

Recall that since \( C_{\downarrow} \) has minimum distance \( d^\perp \leq k+1 \), any \( n - d^\perp + 1 \) columns of \( H \) has full rank. So in particular, since \( |I_1| = |I_2| = n - d^\perp + 1 \), for any \( i = 1, 2 \), the function \( \beta \in \mathbb{F}_p^{n-k} \rightarrow \{ \langle \beta, h_j \rangle \}_{j=1}^{n} \in \mathbb{F}_p^{n-d^\perp+1} \) is injective. So for any \( i = 1, 2 \),

\[
\sum_{\beta \in \mathbb{F}_p^{n-k} \setminus \{0\}} \prod_{j \in I_{\ell_j}} \left| \widehat{I}_{\ell_j}(\langle \beta, h_j \rangle) \right|^2
\]

\[
\leq \sum_{\beta \in \mathbb{F}_p^{n-k} \setminus \{0\}} \prod_{j \in I_{\ell_j}} \left| \widehat{I}_{\ell_j}(\langle \beta, h_j \rangle) \right|^2
\]

Applying this to the previous inequality, we have

\[
SD \leq \frac{1}{2} \sum_{\ell_j} \left\| \prod_{j \in I_{\ell_j}} \widehat{I}_{\ell_j} \right\|^2 \cdot \left\| \prod_{j \in I_{\ell_j}} \widehat{I}_{\ell_j} \right\|^2
\]

\[
= \frac{1}{2} \left( \prod_{j \in I_{\ell_j}, \ell_j} \sum_{\beta \in \mathbb{F}_p^{n-k} \setminus \{0\}} \left| \widehat{I}_{\ell_j}(\langle \beta, h_j \rangle) \right|^2 \right)
\]

\[
\cdot \sum_{\beta \in \mathbb{F}_p^{n-k} \setminus \{0\}} \left| \widehat{I}_{\ell_j}(\langle \beta, h_j \rangle) \right|^2
\]
We conclude the proof by proving that
\[ \prod_{j\in I_{\ell_1} \cup I_{\ell_2}} \sum_{\ell_j} \| \vec{E}_{\ell_j} \|_2 \leq 2^{\mu(n-d+1)}. \]
Note that to prove this, it is sufficient to prove the following proposition.

**Proposition IV.5:** For any \( j \in [n] \) and \( \mu \), we have
\[ \sum_{\ell_j \in F^\mu_2} \| \vec{E}_{\ell_j} \|_2 \leq 2^{\mu/2}. \]

**Proof:** Recall that by Parseval's Identity in Lemma III.1, we have
\[ \| \vec{E}_{\ell_j} \|_2 = \sqrt{\Pr_{x\in F_{p^w}}[\hat{1}]^2 - \Pr_{x\in F_{p^w}}[\hat{1}]^2} = \sqrt{\Pr_{x\in F_{p^w}}[\hat{1}]^2}. \]
For any \( \ell \in F^\mu_2 \), denote by \( S_{\ell} = \{x \in F_{p^w} : \hat{1}_\ell(x) = 1\} \). It is easy to see that \( F_{p^w} = \bigcup_{\ell \in F^\mu_2} S_{\ell} \).

Hence we have
\[ \| \vec{E}_{\ell_j} \|_2 = \sqrt{\sum_{\ell \in F^\mu_2} |S_{\ell}| / p^w} = \sqrt{\sum_{\ell \in F^\mu_2} |S_{\ell}| / p^w}. \]

Recall that for any non-negative real numbers \( a_1, \ldots, a_n \), the arithmetic between their geometric and quadratic mean
tell us that \( \sum_{i=1}^n a_i \) is upper bounded by \( \sqrt{n} \sqrt{\sum_{i=1}^n a_i^2} \).
So by setting the non-negative real numbers to be \( \| \vec{E}_{\ell_j} \|_2 \), we have
\[ \sum_{\ell_j \in F^\mu_2} \| \vec{E}_{\ell_j} \|_2 = \sqrt{\sum_{\ell_j \in F^\mu_2} |S_{\ell_j}| / p^w} \leq 2^{\mu/2}. \]

This completes the proof of Proposition IV.5. \( \square \)

Applying Proposition IV.5, we have the desired bound for \( SD(\tau(C), \tau(U_n)) \). \( \square \)

Lemma IV.4 bounds the statistical distance of a linear code using some functions that are related to a submatrix of its parity check matrix. Note that such submatrix defines a linear code with length \( |L_3| \). Lastly, we provide a bound for such code in Lemma IV.6.

**Lemma IV.6:** Let \( D \subseteq \mathbb{F}_{p^w}^n \) be any code of distance at least \( d \). Consider an arbitrary family of leakage functions \( \tau = (\tau^{(1)}, \ldots, \tau^{(n)}) \) where \( \tau^{(j)} : \mathbb{F}_{p^w} \rightarrow \mathbb{F}^\mu_2 \). Recall that we defined \( \vec{E}_{\ell_j}(x) = 1 \) if \( \tau^{(j)}(x) = \ell_j \) and 0 otherwise. Let \( c'_\mu = 2^\mu \frac{\sin(\pi/2^\mu + \pi/2^{\mu+1})}{\sin(\pi/\mu)} \). Then
\[ \sum_{\ell \in \mathbb{F}_p^{\mu \times \infty}} \max_{\alpha \in D \setminus \{0\}} \prod_{j=1}^n |\vec{E}_{\ell_j}(\alpha_j)| \leq 2^{(4\mu+1) \cdot (\kappa - d)} \cdot (c'_\mu)^\kappa. \]

**Proof:** Denote by
\[ \eta = \sum_{\ell \in \mathbb{F}_p^{\mu \times \infty}} \max_{\alpha \in D \setminus \{0\}} \prod_{j=1}^n |\vec{E}_{\ell_j}(\alpha_j)|. \]

Here we prove a bound for \( \sum_{\ell \in \mathbb{F}_p^{\mu \times \infty}} |\vec{E}_A(\alpha)| \) that we will use instead of the bounds from Lemma IV.2.

**Lemma IV.7:** Let \( \xi_{p^w} : \{0, \ldots, p^w - 1\} \rightarrow \mathbb{R}_{\geq 0} \) such that \( \xi_{p^w}(x) = \frac{p^{2\mu} \sin(\pi/2^\mu + \pi/2^{\mu+1})}{\sin(\pi/\mu)} \). We further let \( \xi_{p^w} : \{0, \ldots, p^w - 1\} \rightarrow \mathbb{R}_{\geq 0} \) be defined such that for \( \xi_{p^w}(x) = \max(\xi_{p^w}(x)/p^w, 2^{-(4\mu+1)}) \). Then the function \( \xi_{p^w} \) has the following properties:
1) For every set \( A \) of size \( t \),
\[ |\vec{E}_A(\alpha)| \leq \begin{cases} \xi_{p^w}(t), & \text{if } \alpha \neq 0, \\ 2^{4\mu+1} \cdot \xi_{p^w}(t), & \text{if } \alpha = 0. \end{cases} \]
2) Let \( A_1, \ldots, A_{2^\mu} \) be any partition of \( \mathbb{F}_{p^w}^\mu \). Then,
\[ \sum_{i=1}^{2^\mu} \xi_{p^w}(|A_i|) \leq c'_\mu. \]

First we prove Lemma IV.7 before using it to complete the proof of Lemma IV.6.

**Proof of Lemma IV.7:**
1) Note that since \( \xi_{p^w}(t) \geq \zeta_{p^w}(t) \), the inequality when \( \alpha \neq 0 \) follows from Lemma III.2. Noting that \( |\vec{L}_3(0)| = \frac{|A_1|}{|p^w-1|} \) and \( 2^{4\mu+1} \).
\( \xi_{p^w}(x) \geq 2^{4\mu+1}, 2^{-(4\mu+1)} = 1, \) the inequality for the case \( \alpha = 0 \) directly follows.

2) First we note that \( \xi_{p^w}(p^{2\mu}/2^{\mu+1})/p^w = \frac{\sin(\pi/2^\mu)}{\sin(\pi/\mu)} \).

Note that \( x - \sin(x) \) is a non-decreasing function and it is zero only if \( x = 0 \). So \( p \sin(\pi/\mu) \leq p \cdot \frac{\sin x}{x} = \pi \leq 4 \).
We further note that \( \frac{\sin x}{x} \) is a decreasing function for \( x \in (0, \pi/2) \) by the same reason as above. This means that for any \( x < y, \frac{\sin x}{x} \geq \frac{\sin y}{y} \).
Equivalently, \( \frac{\sin x}{x} \geq \frac{\sin y}{y} \).

Now suppose that \( |A_i| = t_i \) where \( \sum_{i=1}^{2^\mu} t_i = p^w \), we have
\[ \sum_{i=1}^{2^\mu} \xi_{p^w}(t_i) \leq \frac{1}{p^w} \sum_{i=1}^{2^\mu} \frac{p^w}{\sin(\pi/\mu)} \left( \frac{\sigma_i}{\sin(\pi/\mu)} \max \left( \frac{t_i}{2^{4\mu}}, \frac{p^{2\mu}}{2^{\mu+1}} \right) \right) \]
\[ = \frac{1}{p^w} \sum_{i=1}^{2^\mu} \frac{\pi}{\sin(\pi/\mu)} \max \left( \frac{t_i}{2^{4\mu}}, \frac{p^{2\mu}}{2^{\mu+1}} \right) \]
We note that due to the concavity of the sine function in the range \( [0, \pi/2] \) for any \( a_1, \ldots, a_{2^\mu} \in [0, \pi/2], \sum \sin(a_i) \leq 2^\mu \sin \left( \frac{\pi a_i}{2^\mu} \right) \). So we have
\[ \sum_{i=1}^{2^\mu} \xi_{p^w}(t_i) \leq \frac{2^\mu}{p^w} \sin \left( \frac{\pi}{2^\mu} \sum_{i=1}^{2^\mu} \frac{t_i}{2^{4\mu}} \right) \]
\[ = \frac{2^\mu}{p^w} \sin \left( \frac{\pi}{2^\mu} \sum_{i=1}^{2^\mu} t_i \right) \]
\[ = \frac{2^\mu}{p^w} \sin \left( \frac{\pi}{2^\mu} \left( \frac{p^w}{2^{4\mu}} \right) \right) \]
\[ = \frac{2^\mu \sin(\pi/2^\mu + \pi/2^{\mu+1})}{\sin(\pi/\mu)} = c'_\mu. \]

This completes the proof of Lemma IV.7. \( \square \)

Now we continue the proof of Lemma IV.6. For any \( j \) and \( \ell_j \in F^\mu_2 \), denote \( t_{\ell_j,j} = |\tau_j^{-1}(\ell_j)| \). By the first claim in
Lemma IV.7, noting that \(\text{wt}_H(\alpha) \geq d\) for any \(\alpha \in D \setminus \{0\}\),
\[
\eta \leq \sum_{t \in \mathbb{F}_p^k} \max_{\alpha \in D \setminus \{0\}} \prod_{j=1}^\kappa \xi_{p^\mu}(t_{j},j) \cdot (2^{4\mu+1})^{1_0(\alpha_j)}
\]
\[
= \sum_{t \in \mathbb{F}_p^k} \prod_{j=1}^\kappa \xi_{p^\mu}(t_{j},j) \cdot \max_{\alpha \in D \setminus \{0\}} \prod_{j=1}^\kappa 2^{(4\mu+1)(1_0(\alpha_j))}
\]
\[
= \sum_{t \in \mathbb{F}_p^k} \prod_{j=1}^\kappa \xi_{p^\mu}(t_{j},j) \cdot \max_{\alpha \in D \setminus \{0\}} 2^{(4\mu+1)(\kappa-\text{wt}_H(\alpha))}
\]
\[
\leq \sum_{t \in \mathbb{F}_p^k} \prod_{j=1}^\kappa \xi_{p^\mu}(t_{j},j) \cdot \max_{\alpha \in D \setminus \{0\}} 2^{(4\mu+1)(\kappa-d)}
\]
\[
= 2^{(4\mu+1)(\kappa-d)} \cdot \prod_{j=1}^\kappa \sum_{t_j \in \mathbb{F}_p^\mu} \xi_{p^\mu}(t_{j},j).
\]

Note that for any \(j, \sum_j t_j \in \mathbb{F}_p\) as a partion of \(\mathbb{F}_p^w\), by the second claim of Lemma IV.7, we have
\[
\prod_{j=1}^\kappa \sum_{t_j \in \mathbb{F}_p^\mu} \xi_{p^\mu}(t_{j},j) \leq \prod_{j=1}^\kappa c_{\mu} = (c_{\mu})^\kappa.
\]

Combining this inequality with the upper bound of \(\eta\) above, we have the desired inequality. \(\square\)

Now we are ready to prove Theorem 7. First, we restate the theorem.

**Theorem 7:** Let \(C \subseteq \mathbb{F}_p^{n,w}\) be any \([n,k,d \leq n-k+1]\) linear code with dual distance \(d^\perp\). Suppose that \(d^\perp \geq 2^{4\mu+1}\). Let \(\tau = (\tau^{(1)}, \ldots, \tau^{(n)})\) be any family of leakage functions where \(\tau^{(j)} : \mathbb{F}_p^{w} \to \mathbb{F}_2^d\). Let \(c_{\mu} = 2^{\delta_s \sin(\pi/2^{\mu+\mu/2^{\mu}})}\).

1. \(SD(\tau(C),\tau(U_n)) \leq \frac{1}{2} \cdot 2^{(5\mu+1)(n-d^\perp)+\mu} \cdot (c_{\mu})^{2^d-n-2}\)
2. \(SD(\tau(C),\tau(U_n)) \leq \frac{1}{2} \cdot 2^{(5\mu+1)(n-d^\perp)+\mu} \cdot (c_{\mu})^{2^d-n-2}\)

**Proof:** By Lemma IV.4, we have
\[
SD(\tau(C),\tau(U_n)) \leq \frac{1}{2} \cdot 2^{(5\mu+1)(n-d^\perp)+\mu} \cdot (c_{\mu})^{2^d-n-2}
\]

where \(I_3 \subseteq [n]\) of size \(\kappa \leq n-2(n-d^\perp+1) = 2^{d^\perp} - n - 2\). Let \(D = \{(x,j) \in I_3 : x \in C^\perp\}\). Since \(C^\perp\) is an \([n,k,d \leq k+1]\) code, \(D\) is a \([k,\kappa',d']\) code where \(\kappa' \leq n-k\) and \(d' \geq d^\perp - (n-\kappa)\). This implies that \(\kappa - d' \leq n - d^\perp\). Then by Lemma IV.6,
\[
\sum_{\{t_j\}_{j \in I_3}} \max_{\beta \in \mathbb{F}_p^{n-w-k}} \prod_{j \in I_3} \left|E_t((\beta, h_j))\right|
\]
\[
= \sum_{\{t_j\}_{j \in I_3}} \max_{\alpha \in D \setminus \{0\}} \prod_{j \in I_3} \left|E_t(\alpha_j)\right|
\]
\[
\leq 2^{(4\mu+1)(\kappa-d')} \cdot (c_{\mu})^{\kappa}
\]
\[
\leq 2^{(4\mu+1)(n-d^\perp)} \cdot (c_{\mu})^{2^d-n-2}.
\]

So we have
\[
SD(\tau(C),\tau(U_n)) \leq \frac{1}{2} \cdot 2^{(5\mu+1)(n-d^\perp)+\mu} \cdot (c_{\mu})^{2^d-n-2}
\]

which completes the proof. \(\square\)

**V. LOCAL LEAKAGE-RESILIENCE OF ADDITIVE SECRET SHARING SCHEMES AND SHAMIR’S SECRET SHARING SCHEMES OVER ARBITRARY FINITE FIELDS**

In this section, we apply our analysis in Section IV to the family of MDS codes. This generalizes the result of [5] to threshold secret sharing schemes defined over field extensions. In order to achieve this, we state the results in Theorems 6 and 7 when applied to MDS codes.

**Corollary VI.1:** Let \(C \subseteq \mathbb{F}_p^{n,w}\) be an MDS \([n,k,n-k+1]\) code with the dual code \(C^\perp\) which is an \([n,k,n-k+1]\) code. Furthermore, let \(\tau = (\tau^{(1)}, \ldots, \tau^{(n)})\) be any family of leakage functions where \(\tau^{(j)} : \mathbb{F}_p^{w} \to \mathbb{F}_2^d\) for some integer \(\mu < \log p\). Let \(c_{\mu} = 2^{\delta_s \sin(\pi/2^{\mu+\mu/2^{\mu}})}\). Then
\[
SD(\tau(C),\tau(U_n)) \leq \frac{1}{2} \cdot 2^{\delta_s \sin(\pi/2^{\mu+\mu/2^{\mu}})} \cdot 2^{(5\mu+1)(n-d^\perp)+\mu} \cdot (c_{\mu})^{2^d-n-2}.
\]

Using the same approach in [5, Theorem 4.7], we have the following result on additive secret sharing over \(\mathbb{F}_p^{w}\).

**Corollary VI.2:** Let \(C \subseteq \mathbb{F}_p^{n,w}\) be the code generated with codewords having entries being valid additive shares of 0. Letting \(\tau = (\tau^{(1)}, \ldots, \tau^{(n)})\) be any family of leakage functions where each \(\tau^{(j)}\) has \(\mu\) bit output for some \(\mu < \log p\). Letting \(c_{\mu} = 2^{\delta_s \sin(\pi/2^{\mu+\mu/2^{\mu}})}\). Then
\[
SD(\tau(C),\tau(U_n)) \leq \frac{1}{2} \cdot 2^{\delta_s \sin(\pi/2^{\mu+\mu/2^{\mu}})} \cdot 2^{(5\mu+1)(n-d^\perp)+\mu} \cdot (c_{\mu})^{2^d-n-2}.
\]

Using Corollaries VI.1 and VI.2, we can obtain similar results on leakage-resilience of both additive secret sharing schemes and Shamir’s secret sharing schemes as discussed in [5, Section 4.2.2 and Section 4.2.3].

**VI. LOCAL LEAKAGE-RESILIENCE OF ALGEBRAIC GEOMETRIC CODES BASED RAMP SECRET SHARING SCHEME**

Let \(q = p^w\) and \(F/\mathbb{Q}_q\) be a function field of genus \(\mu\) and at least \(n+2\) distinct \(\mathbb{F}_q\)-rational places \(P_{\infty}, P_0, \ldots, P_n\). Set \(\mathcal{P} = \{P_1, \ldots, P_n\}\) and \(\mathcal{P}_0 = \{P_0\} \cup \mathcal{P}\). Consider a ramp secret sharing scheme \(AGSh_{m,P_0,\mathcal{P}}\) over \(\mathbb{F}_q\) based on \(C(mP_\infty, \mathcal{P})\) constructed using the technique discussed in Section II-D. In this section, we utilize Theorems 6 and 7 to establish the local leakage-resilience of \(AGSh_{m,P_0,\mathcal{P}}\).
A. Local Leakage-Resilience of $AGSh_{m,P_{\infty},\mathcal{P}}$

First we recall the the local leakage scenario we are considering. We use the algebraic-geometric code based ramp secret sharing scheme $AGSh_{m,P_{\infty},\mathcal{P}}$ with $t = m - 2g$ privacy and $r = 2g + t + 1$ reconstruction to secret share a secret to a set of players $\mathcal{U} = \{U_1, \ldots, U_n\}$. A passive adversary then chooses $\Theta \subseteq \mathcal{U}$ of size $|\Theta| = \theta < t$ to control as well as the leakage function $\tau = (\tau(1), \ldots, \tau(n))$ with each leakage function outputting $\mu < \log p$ bits each. This defines the view of the adversary as $Leak_{\Theta,\tau}$. Note that in the view of the adversary, due to the $\theta$ shares that he has learned in full, the remaining required information is less than what is originally needed. In fact, we can no longer apply Theorems 6 and 7 directly using $C(m,P_{\infty},\mathcal{P})$ as the linear code. The following lemma provides a linear code $C$ that is equivalent to the view of the adversary after learning the shares of the players in $\Theta$.

**Lemma VI.1:** Consider the secret sharing scheme $AGSh_{n,r,t} = AGSh_{m,P_{\infty},\mathcal{P}}$ which is used to secret share $s \in \mathbb{F}_p$ to each user $U_i$ gets a share $s_i \in \mathbb{F}_p$. Let $\Theta \subseteq \mathcal{U}$ be a set of $\theta \leq t = m - 2g$ players that is corrupted by the adversary and set $\Theta = \mathcal{U} \setminus \Theta$. Consider the following experiment. Let the values of the shares held by the corrupted parties be $x(\Theta)$. Let $AGSh_{n,r,t}(s)|_{x(\Theta):x(\Theta)}$ be the distribution on the shares conditioned on the revealed values $s(\Theta)$ being $x(\Theta)$. Then there exists an $[n - \theta, n - m - g, d' \geq n - m + 1]$ code $C' \subseteq \mathbb{F}_p^{n-\theta}$ with dual code $C''$ with parameter $[n - \theta, n - m + g, (d')^\perp \geq m - \theta - 2g + 1]$ and a shift vector $b \in \mathbb{F}_p^\theta$ such that

$$AGSh_{n,r,t}(s)|_{x(\Theta):x(\Theta)} \equiv \left\{ (y(\Theta)|0(\Theta)) + b : y(\Theta) \leftrightarrow C' \right\}.$$  

**Proof:** Without loss of generality, assume that $\Theta = \{U_1, \ldots, U_{\theta}\}$. Then by Lemma II.3, there exists $p \in \mathcal{L}(m,P_{\infty})$ such that $p(P_i) = x_i$ for all $i \in \Theta$. So $AGSh_{n,r,t}(s)|_{x(\Theta):x(\Theta)} \equiv AGSh_{n,r,t}(0)|_{x(\Theta):0}$. Then $AGSh_{n,r,t}(s)|_{x(\Theta):0}$ is equivalent to $C'$, which is an $[n - \theta, n - m - g, d' \geq n - m + 1]$ code with dual code $(C')^\perp$ an $[n - \theta, n - m + g, (d')^\perp \geq m - \theta - 2g + 1]$ code.

Using this observation, we can then provide the leakage-resilience of the ramp secret sharing scheme $AGSh_{n,r,t}(s)$ which is defined over $\mathbb{F}_{p^w}$.

**Corollary VI.2:** The ramp secret sharing scheme $AGSh_{n,r,t}(s)$ defined over $\mathbb{F}_{p^w}$ is $(\theta, \mu, \epsilon)$-LL resilient where

$$s = \begin{cases} \min \left\{ w(n-\theta) \varepsilon_{\mu}^0 \frac{\mu}{2}, w(n-\theta) \varepsilon_{\mu}^0 \frac{\mu}{2}, \right\} & \text{if } t \geq n + \theta \frac{w}{2}, \\ \min \left\{ w(n-\theta-1) \varepsilon_{\mu}^0 \frac{\mu}{2}, w(n-\theta-1) \varepsilon_{\mu}^0 \frac{\mu}{2}, \right\} & \text{otherwise}, \end{cases}$$

where $w = (n + 1)(2g + t + 1) - \sum_{i \in \Theta} P_i$.

**Proof:** Let $s, s' \in \mathbb{F}_{p^w}$. For simplicity of notation, we denote by $SD$ the statistical distance between the outputs of $\tau$ with inputs being the shares generated by $s$ and $s'$ respectively under the assumption that $s(\Theta) = x(\Theta)$. By Lemma VI.1, having the adversary seeing the values of $s(\Theta) = x(\Theta)$, the adversary specifies any family of $\mu$-bit output leakage functions $\tau(\Theta) = (\tau(i))_{i \in \Theta}$. Since the distribution of $AGSh_{n,r,t}(s)$ after the leak of $s(\Theta)$ is equivalent to an $[n - \theta, n - m - g, d' \geq n - m + 1]$ code, by Theorem 6, $SD \leq \frac{1}{2} p_{w \mu}^{w(n-m-g)}(\varepsilon_{\mu}^0)^{\tau(\Theta)} \leq \frac{1}{2} p_{w \mu}^{w(n-m-g)} \cdot \frac{\mu}{2} \cdot (\varepsilon_{\mu}^0)^{\tau(\Theta)\theta+1}$. Using triangle inequality, we have that for any $s \neq s' \in \mathbb{F}_{p^w}$, we have

$$SD \leq p_{w \mu}^{w(n-t-\theta-1)} \cdot \varepsilon_{\mu}^0 \cdot \theta + 1.$$  

Using the same argument based on Theorem 7, when $t \geq n \frac{\theta}{2} - 1$, we have $t - \theta + 1 \geq n \frac{\theta}{2}$, and hence

$$SD \leq 2^{n(\theta-t-1)(\mu\theta+1) + \mu} \cdot (\varepsilon_{\mu}^0)^{2t-n \cdot \theta}.$$  

This completes the proof.

In order to obtain a ramp secret sharing scheme that can be constructed in polynomial time, we construct the code by applying the Garcia-Stichtenoth tower [21] to construct the AG code. However, for such method to be applicable, we need to be working over $\mathbb{F}_q$ where $q$ is a square of a prime. In other words, our resulting ramp secret sharing scheme is defined over $\mathbb{F}_q$ where $q = p^2$. Hence, applying this result when $w = 2$, we have our first main result.

**Theorem 1:** Let $q = p^2$ for some prime $p$ and $\mathbb{F}_q$ be a finite field of $q$ elements. Then there exists an infinite family of ramp secret sharing schemes that can be explicitly constructed over $\mathbb{F}_q$ in polynomial time with share size $O(1)$ bits for $N$ players providing $T \leq N - \frac{2N}{\sqrt{q}}$-privacy and reconstruction level $R = T + \frac{N}{\sqrt{q}} + 1$ such that any of such secret sharing schemes is $(\theta, \mu, \epsilon)$-LL resilient for any $\theta < T$ and $\mu < \log p$ where

$$\epsilon = \frac{\min \left\{ w(N-T) \varepsilon_{\mu}^0 \frac{\mu}{2}, w(N-T) \varepsilon_{\mu}^0 \frac{\mu}{2}, \right\}}{w(N-T) \varepsilon_{\mu}^0 \frac{\mu}{2}} \cdot \frac{\mu}{2} \cdot \frac{\mu}{2} \cdot (\varepsilon_{\mu}^0)^{T-\theta+1},$$

with $c_{\mu} = \frac{2^{\mu \sin \left( \frac{\pi}{2} \right)}}{p \sin \left( \frac{\pi}{2} \right)}$ and $c'_{\mu} = \frac{2^{\mu \sin \left( \frac{\pi}{2} + \frac{\pi}{2} \right)}}{p \sin \left( \frac{\pi}{2} + \frac{\pi}{2} \right)}$.

B. Construction of Algebraic-Geometric Codes-Based Ramp Secret Sharing Scheme by Concatenation Scheme

Recall that for any element in $\mathbb{F}_{p^w}$ where $w$ is a positive integer that can be factorized to $w = uv$ for some positive integers $u$ and $v$, there is a vector space isomorphism between $\mathbb{F}_{p^w}$ with $\mathbb{F}_{p^u}$ and $\mathbb{F}_{p^v}$. Fix one of such isomorphisms and denote it by $\Pi_{u,v}$.

Consider an AG-codes based ramp secret sharing scheme defined over $\mathbb{F}_{p^w}$. Then using $\Pi_{u,v}$, we can map the $n$ shares $s_1, \ldots, s_n \in \mathbb{F}_{p^w}$ to $v$ shares $s'_1, \ldots, s'_v \in \mathbb{F}_{p^u}$ where for any $i = 1, \ldots, n$, $s'_i = \Pi_{u,v}(s_i)$. Then the resulting ramp secret sharing schemes has $N = vn$ players providing $T = m - 2g$ privacy and $R = (v-1)n + m + 1 = \frac{w}{2}N + m + 1$ reconstruction. Note that this can be easily verified by noting that learning any $T$ shares provides at most $T$ shares of the original AG-code based ramp secret sharing scheme that is defined over $\mathbb{F}_{p^u}$. Hence by definition, the
adversary learns no information about the original secret from any of such \( T \) shares. On the other hand, by Pigeon Hole principle, having \( R \) shares, there are at least \( m + 1 \) of \( i \) such that we learned \( (s_{\mu}(i-1), \ldots, s_{\mu}^1) \). Hence, using the isomorphism \( \Pi_{u,v} \), we can learn at least \( m + 1 \) of the original shares \( s_i \in \mathbb{F}_{p^N} \). By definition, such information is sufficient to reconstruct the original secret. Denote the resulting ramp secret sharing scheme by \( EAGSh_{N,R,T}(s) \) that secretly shares a secret \( s \in \mathbb{F}_{p^N} \) to \( N = m \) players over \( \mathbb{F}_{p^N} \). Here we denote the set of \( N \) players by \( \mathcal{U} = \{U_1, \ldots, U_N\} \).

We consider the extension of Lemma VI.1.

**Lemma VI.3:** Let \( \Theta \subseteq \mathcal{U} \) be a set of \( \theta \leq T \) players. Consider the following experiment where for a given secret \( s \in \mathbb{F}_{p^N} \), the \( N \) shares \( s = (s_1, \ldots, s_N) = EAGSh_{N,R,T}(s) \) are generated while the shares \( s_i \) of \( U_i \) for all \( U_i \in \Theta \) are leaked. Let these values be \( x(s) \). Let \( EAGSh_{N,R,T}(s) \left|_{x(s)=x(s)} \right. \) be the distribution of the shares conditioned on the revealed values \( s(s) \) being \( x(s) \). Then there exists an \( [N - \theta, \theta, (m - \theta - g), D' \geq m - \theta + 1] \) code \( C' \subseteq \mathbb{F}_{p^{N-R}} \) with dual code \( C^\perp \) with parameter \( \left|\{N - \mu, \theta, -vm + v\gamma, (D')^\perp \geq m - \theta - 2g + 1\right| \) and a shift vector \( \hat{b} \in \mathbb{F}_{p^N} \) such that

\[
EAGSh_{N,R,T}(s) \left|_{x(s)=x(s)} \right. \subseteq \{ \left( \begin{array}{c} \hat{x}(s') \nonumber \\ \hat{b} \end{array} \right) \mid \hat{y}(s') = c' \}.
\]

Then, using the isomorphism \( \Pi_{u,v} \), setting \( C' = \Pi_{u,v}^1(C) \subseteq \mathbb{F}_{p^{N-R}} \) with parameter \( \left|\{N - \theta, \theta, (m - \theta - g), D' \geq m - \theta + 1\right| \) and dual \( (C')^\perp = \Pi_{u,v}^1(C^\perp) \subseteq \mathbb{F}_{p^{N-R}} \) with parameter \( \left|\{N - \theta, \theta, -vm + v\gamma, (D')^\perp \geq m - \theta - 2g + 1\right| \) along with a shift vector \( \hat{b} = \Pi_{u,v}(\hat{b}) \in \mathbb{F}_{p^N} \), we have the desired result.

**Proof:** Suppose that \( \Theta \subseteq \mathcal{U} \) with \( |\Theta| = \theta \leq t \). Then in the worst case, the leaks reveal the \( \theta \) values in the corresponding ramp secret sharing scheme over \( \mathbb{F}_{p^N} \). Suppose that the \( \theta \) values leaked in the corresponding ramp secret sharing scheme over \( \mathbb{F}_{p^N} \) is \( s_1, \ldots, s_\theta \). Then by Lemma VI.1, there exists an \( [n - \theta, \theta, \theta, g, d \geq n - m + 1] \) code \( C \subseteq \mathbb{F}_{p^{N-R}} \) with dual code \( C^\perp \) with parameter \( \left|\{N - \theta, \theta, -vm + v\gamma, (D')^\perp \geq m - \theta - 2g + 1\right| \) and a shift vector \( \hat{b} \in \mathbb{F}_{p^N} \) such that the distribution on the corresponding \( n \) shares over \( \mathbb{F}_{p^N} \) conditioned on the revealed values is equivalent to \( \{ \left( \begin{array}{c} \hat{x}(s') \nonumber \\ \hat{b} \end{array} \right) \mid \hat{y}(s') = c' \} \).

Similarly, when \( T \geq \frac{N-(v-2)N}{2} \), Theorem 7 implies

\[
S \leq \frac{1}{N-N-R-T+1} \cdot \mu, \quad \mu = \theta+N-T+1.
\]

As before, we aim to obtain a ramp secret sharing scheme that can be explicitly constructed over \( \mathbb{F}_q \) in polynomial time with share size \( O(1) \) bits for \( N \) players providing \( T < \frac{N}{2} - \frac{N}{2} - \frac{N}{2} - \frac{N}{2} - \frac{N}{2} + \frac{N}{2} + 1 \) such that any of such secret sharing schemes is \((\theta, \mu, \epsilon)\) LR resilient for any \( \theta < T \) and \( \mu < \log q \) where

\[
\epsilon = q^{N-2T-N} \cdot \epsilon_{\mu+1}^{T+1}.
\]

**C. Construction of Strongly Multiplicative Algebraic-Geometric Codes-Based Ramp Secret Sharing Scheme Through Multiplication Friendly Embeddings**

Note that although the embedding used in Section VI-B is optimal in the sense that it is impossible to have an embedding of \( \mathbb{F}_{p^N} \) to a space over \( \mathbb{F}_{p^N} \) with smaller length, such embedding causes the resulting code to no longer have multiplicative or strong multiplicative property possessed by the initial AG codes.

We again start from an AG code \( C \) defined over \( \mathbb{F}_{p^N} \). Let \( F \) be an algebraic function field over \( \mathbb{F}_{p^N} \) with genus \( g \) and more than \( 4(g+1) \) pairwise distinct rational places. Choose \( n \) to be a positive integer such that there are at least \( n + 1 \) rational places and \( m \) and \( t \) be positive integer such that \( t = m - 2g \) and \( 3t < n - 4g \). As discussed in Section II-D, we can then define an AG code \( C \subseteq \mathbb{F}_{p^N}^{n+1} \) of dimension \( k = m - g + 1 \) and minimum distance \( d \geq n - m \) such that \( \Sigma(C) \) is \( t = m - 2g \)-strongly multiplicative. Furthermore, we also have that \( \Sigma(C) \) has reconstruction level of at most \( r = m + 1 \).

In order to have an explicit family of ramp secret sharing schemes over \( \mathbb{F}_{p^N} \) from those over \( \mathbb{F}_{p^N} \) that possess multiplicative or strong multiplicative property, we make use of MFE, which is discussed in Section II-E. More specifically, following the existence of the MFE described in Theorem 5, there exists an explicit MFE \((\gamma(p^N,v), \sigma(p^N,v), \psi(p^N,v))\) of \( \mathbb{F}_{p^N} \) over \( \mathbb{F}_{p^N} \) where

\[
\gamma(p^N,v) = \left\{ \begin{array}{ll} 2v-1, & \text{if } p^N \geq 2v-2 \\
\frac{v(v+1)}{2}, & \text{if } p^N < 2v-2 \end{array} \right.
\]

Having \( C \), we utilize the MFE \((\gamma(p^N,v), \sigma(p^N,v), \psi(p^N,v))\) of \( \mathbb{F}_{p^N} \) over \( \mathbb{F}_{p^N} \) and the mapping \( \chi(p^N,v) : \mathbb{F}_{p^N} \times (\mathbb{F}_{p^N})^n \rightarrow (\mathbb{F}_{p^N})^{1+\gamma(p^N,v)n} \) described in Theorem 4 to obtain \( C^* = \mathbb{F}_{p^N}^{1+\gamma(p^N,v)n} \). By Theorem 4, such code \( C^* \) is an \( \mathbb{F}_{p^N} \)-linear
code and $\Sigma(C^*)$ is an LSSS with $N = \gamma(p^u,v)n$ players and it is $T = m - 2g$-strongly multiplicative. On the other hand, using similar argument as that given in Section VI-B, it has reconstruction level of at most $R = (\gamma(p^u,v) - 1)n + m + 1 = \gamma(p^u,v)\frac{1}{2}N + m + 1$.

Remark 7: Note that although the resulting ramp secret sharing scheme is shown to have $T$-strong multiplicative property, it is easy to see that since $v > 1$, $\frac{\gamma(p^u,v) - 1}{2} > \frac{1}{2}$. Hence, there will not be enough number of players to recover the product of two secrets from the products of their corresponding shares. This shows that even when MFEs are used, the property of strong multiplicativity on the resulting ramp-secret sharing scheme cannot be used.

Denote the resulting ramp secret sharing scheme by $MFEGAGSh_{N,R,T}$ with secret $s \in \mathbb{F}_{p^u}$ being shared to $N = \gamma(p^u,v)n$ players, each having shares belonging to $\mathbb{F}_{p^u}$. Denote the set of $N$ players by $\hat{U} = \{U_1, \ldots, U_N\}$.

Hence, using the same argument as Lemma VI.3, we obtain the following result.

**Lemma VI.5.** Let $\Theta \subseteq \hat{U}$ be a set of $\theta \leq T$ players. Consider the following experiment where for a given secret $s \in \mathbb{F}_{p^u}$, the $N$ shares $s = (s_1, \ldots, s_N) = MFEGAGSh_{N,R,T}(s)$ are generated while the shares $s_i$ of $U_i$ for all $U_i \in \Theta$ are leaked. Let these values be $x(\Theta)$. Let $MFEGAGSh_{N,R,T}(s)|_{x(\Theta)}$ be the distribution on the shares conditioned on the revealed values $x(\Theta)$ being $x(\Theta)$. Then there exists an $[N - \gamma(p^u,v)\theta, N - \gamma(p^u,v)(m - \theta - g), D'] \supseteq [N - \gamma(p^u,v)m, m - \theta - 2g + 1]$ and a shift vector $b \in \mathbb{F}_{p^u}$ such that $MFEGAGSh_{N,R,T}(\cdot)|_{x(\Theta)=\Theta} = \left\{y(\Theta) + b : y(\Theta) - c'\right\}$.

**Proof:** Suppose that $\Theta \subseteq [N]$ with $|\Theta| = \theta < t$. Then in the worst case, the leaks reveal the $\theta$ values in the corresponding ramp secret sharing scheme over $\mathbb{F}_{p^u}$. Suppose that the $\theta$ values leaked in the corresponding ramp secret sharing scheme over $\mathbb{F}_{p^u}$ is $s_1, \ldots, s_\theta$. Then by Lemma VI.1, there exists an $[n - \theta, m - \theta - g, \hat{d} \geq n - m + 1]$ code $\hat{C} \subseteq \mathbb{F}_{p^u}^{n - \theta}$ with dual code $\hat{C}^\perp$ with parameter $[n - \theta, n - m + g, \hat{d} \geq m - \theta - 2g + 1]$ and a shift vector $\hat{b} \in \mathbb{F}_{p^u}$ such that the distribution on the corresponding $n$ shares over $\mathbb{F}_{p^u}$ conditioned on the revealed values is equivalent to $\left\{\hat{y}(\Theta) + \hat{b} : \hat{y}(\Theta) - c'\right\}$.

Then, using the mapping $\chi(p^u,v)$ described in Theorem 4, setting $C' = \left\{(\sigma(c_1)) \cdots (\sigma(c_n - \theta)) : (c_1, \ldots, c_n) \in \hat{C}\right\} \subseteq \mathbb{F}_{p^u}^{n - \theta}$, we obtain a code with parameter $[N - \gamma(p^u,v)\theta, N - \gamma(p^u,v)(m - \theta - g), D'] \supseteq \left[\frac{\gamma(p^u,v)}{2}, m - \theta - 2g + 1\right]$ and dual $C'^\perp = \Pi_{u,v}(\hat{C}^\perp) \subseteq \mathbb{F}_{p^u}^{n - \theta}$ with parameter $[N - \gamma(p^u,v)\theta, N - \gamma(p^u,v)(m - g), (D')^\perp \geq m - \theta - 2g + 1]$ along with a shift vector $\hat{b} = (\sigma(p^u,v)(\hat{b}_1) \cdots (\sigma(p^u,v)(\hat{b}_n)) \in \mathbb{F}_{p^u}^n$ where $\hat{b} = (\hat{b}_1, \ldots, \hat{b}_n)$. Hence we have the desired result. □

Using the same argument as Corollary VI.4, we have the following leakage-resilience of $MFEGAGSh_{N,R,T}$.

**Corollary VI.6.** For simplicity of notation, write $\gamma(p^u,v)$ as $\gamma$. The ramp secret sharing scheme $MFEGAGSh_{N,R,T}(\cdot)$ defined over $\mathbb{F}_{p^u}$ is $(\theta, \mu, \epsilon)$-LL resilient where $\epsilon$ satisfies the following inequalities. Firstly, we have

$$\epsilon \leq p^\frac{1}{2} \left(\frac{N - T - R + 1}{\gamma(p^u,v)}\right)^{T-\theta+1}.$$ 

Furthermore, if $T \geq \frac{N - (\gamma - 1)T}{2}$,

$$\epsilon = q^{(N - (\gamma - 1)T - T - 1)(5\mu + 1) + \mu} \cdot (c_\mu)^{2T + (\gamma - 2)T - N}.$$ 

We conclude this section by providing a concrete instantiation that can be constructed in polynomial time by using Garcia-Stichtenoth tower to obtain an explicit AG code defined over $\mathbb{F}_{p^u}$, which is then transformed to a code over $\mathbb{F}_q$, using an MFE with expansion 3. Similar to Theorem 2, we have $T < \frac{N - 2N}{3(q - 1)}$, which is always less than $\frac{N - \theta}{2}$.

**Theorem 3:** Let $q$ be a prime and $\mathbb{F}_q$ be a finite field of $q$ elements. Then there exists an infinite family of ramp secret sharing schemes that can be explicitly constructed over $\mathbb{F}_q$ in polynomial time with share size $O(1)$ bits for $N$ players providing $T < \frac{N - 2N}{3(q - 1)}$-privacy and reconstruction level $R = \frac{2N}{3} + T + \frac{2N}{3(q - 1)} + 1$ such that any of such secret sharing schemes is $(\theta, \mu, \epsilon)$-LL resilient for any $\theta < T$ and $\mu < \log q$

where $\epsilon = \frac{2N}{3(q - 1)} - T$, and $c_\mu = \frac{2^p \sin\left(\frac{\pi}{q}\right)}{q \sin\left(\frac{\pi}{q}\right)}$.

### D. Comparison of Three Construction Techniques

Note that in Section VI, we have considered three main constructions of leakage-resilient AG-based ramp secret sharing scheme. Firstly, we have the direct construction from AG-codes defined in an extension field. Such result is discussed in Corollary VI.2 and Theorem 1. The two other constructions we considered use AG code over a field $\mathbb{F}_{p^u}$, which is a field extension of a basic finite field $\mathbb{F}_{p^u}$. In the first construction concatenates an AG code over $\mathbb{F}_{p^u}$ with an $\mathbb{F}_{p^u}$-isomorphism between $\mathbb{F}_{p^u}$ and $\mathbb{F}_p$ to obtain a code over $\mathbb{F}_p$. Such code is then used as a base to construct the leakage-resilient ramp secret sharing scheme which is discussed in Corollary VI.4 and Theorem 2. Lastly, we also consider the concatenation of an AG code over $\mathbb{F}_{p^u}$ with an MFE over $\mathbb{F}_{p^u}$ of extension degree $\gamma(p^u,v)$ to obtain a code over $\mathbb{F}_{p^u}$. This is then used to construct a leakage-resilient ramp secret sharing scheme which is discussed in Corollary VI.6 and Theorem 3.

In this section, we aim to provide some comparison between the three constructions. In particular, when we set $u = 1$, this provides a way to see if the first construction, which produces a leakage-resilient ramp secret sharing scheme over extension field, has enough advantage to justify the need of investigation on the leakage-resilience property for secret sharing schemes over an extension field.

For simplicity, we focus the comparison on the constructions discussed in Theorems 1, 2 and 3. It is easy to see that when strong multiplicative property is not required, the construction in Theorem 1 can be done for any $T \leq N - \frac{2N}{q - 1}$. Hence, in particular, for $q \geq 17$, it allows for construction of leakage-resilient ramp secret sharing scheme where $\frac{N - \theta}{2} < T \leq N - \frac{2N}{q - 1}$, a range of $T$ that is not achievable by
either Theorem 2 or Theorem 3. This shows that in order to have a construction with privacy threshold beyond $\frac{N}{2} - \frac{N}{q^{1/3}}$, we cannot rely on any construction that is based on the concatenation technique to obtain a leakage-resilient secret sharing scheme over prime field with constant share size. Instead, we need to rely on constructions of leakage-resilient secret sharing schemes over extension field with constant share size.

Next, suppose that we consider the case when $T < \frac{N}{3} - \frac{2N}{\sqrt{q-1}}$. In such case, although such range of $T$ is achievable for all three constructions, only the construction in Theorem 1 possesses strong multiplicative property. In order for such property to be useful, we also require $R_1 < \frac{N}{2}$. So we require $T < \frac{N}{3} - \frac{2N}{\sqrt{q-1}}$. Furthermore, when we assume all three constructions have the same privacy threshold $T$, we have the reconstruction thresholds for the constructions based on Theorem 1, 2 and 3 to be $R_1 \equiv T + \frac{2N}{\sqrt{q-1}} + 1$, $R_2 \equiv \frac{N}{3} + T + \frac{N}{4} - 1$ and $R_3 \equiv \frac{N}{3} + T + \frac{N}{8} + 1$ respectively. In order for the strong multiplicative property to be useful, we also require $R_1 < \frac{N}{3}$. So we restrict $T$ further and require $T < \frac{N}{3} - \frac{2N}{\sqrt{q-1}}$. It is easy to see that when $q \geq 8$, $R_1 \leq R_2 \leq R_3$. Hence, for the same level of $T$, Theorem 1 provides a scheme with the least restricted lower bound on the reconstruction threshold. This shows that without considering the leakage-resilience property, the construction based on Theorem 1 has exhibited advantages in terms of (strong) multiplicative property and the flexibility of reconstruction threshold with respect to the privacy threshold.

We proceed by performing comparison analysis on the leakage-resilience of schemes presented in Theorems 1, 2 and 3 to determine whether it is possible to have a ramp secret sharing scheme defined over a field extension that has a better leakage-resilience property compared to a ramp secret sharing scheme defined over a prime field with comparable parameters. In other words, we assume that they are defined in fields with approximately the same size $q$, approximately the same length $N$ and privacy $T$. Then, assuming that $\mu < \log \sqrt{q}$ and $0 \leq \theta < T$, we aim to compare the leakage-resilience parameter $\epsilon$ for the constructions in the three main results. Note that since we are using the same values of $q, N$ and $T$ for the three constructions, by the assumption discussed above, we require $T < \frac{N}{3} - \frac{2N}{\sqrt{q-1}}$. Note that in such case, we must have $T < \frac{N - \theta}{\sqrt{q}}$ for any $0 \leq \theta < T$. Hence the leakage-resilience parameter for Theorems 1, 2 and 3 is $\epsilon_1 \equiv q^{N - T - \frac{2N}{\sqrt{q-1}}} \cdot c_1^{T-\theta+1}$, $\epsilon_2 \equiv q^{N - 2T - \frac{2N}{\sqrt{q-1}}} \cdot c_2^{T-\theta+1}$ and $\epsilon_3 \equiv q^{N - 2T - \frac{2N}{\sqrt{q-1}}} \cdot c_3^{T-\theta+1}$ respectively where $c_1 = \frac{2^\mu \sin \left(\frac{\pi}{q}\right)}{\sqrt{q} \sin \left(\frac{\pi}{q}\right)}$ and $c_2 = \frac{2^\mu \sin \left(\frac{\pi}{q}\right)}{\eta \sin \left(\frac{\pi}{q}\right)}$. We also observe that in order for $T < \frac{N}{3} - \frac{2N}{\sqrt{q-1}}$ to make sense, we require $q > 49$.

We claim that in such setting, $\epsilon_3 < \epsilon_1 < \epsilon_2$. In other words, construction in Theorem 1 provides better leakage-resilience compared to the one in Theorem 2 but worse compared to the one in Theorem 3. Although the construction in Theorem 1 provides worse leakage resilience compared to Theorem 3, it is reasonable to justify such disadvantage by its sufficiently strong advantages in other properties such as (strong) multiplicative property or the flexibility of its reconstruction threshold.

Note that $\epsilon_2 = q^{-\frac{N}{q-1}}$ which has negative exponent. Hence we must have $\epsilon_3 < \epsilon_2$. This implies that when we fix $q, N, T, \mu$ and $\theta$, the construction in Theorem 3 provides a better leakage-resilience property than the construction in Theorem 2. Next, we compare $\epsilon_1$ and $\epsilon_3$. It is easy to see that

$$\epsilon_1 \equiv q^{N - T - \frac{2N}{\sqrt{q-1}}} \cdot c_1^{T-\theta+1}$$

and

$$\epsilon_3 \equiv q^{N - T - \frac{2N}{\sqrt{q-1}}} \cdot c_2^{T-\theta+1}$$

where

$$c_1 = \frac{2^\mu \sin \left(\frac{\pi}{q}\right)}{\sqrt{q} \sin \left(\frac{\pi}{q}\right)} \quad \text{and} \quad c_2 = \frac{2^\mu \sin \left(\frac{\pi}{q}\right)}{\eta \sin \left(\frac{\pi}{q}\right)}.$$

Let $\Sigma_1 \triangleq AGSh_{N,T+\frac{2N}{\sqrt{q-1}}+O(1)}$, $T$ be a ramp secret sharing scheme defined over $\mathbb{F}_q$ with $N$ players and $T$ privacy by Theorem 1 such that $q_1$ is a square of a prime such that $q_1 \approx q$ which is $(\theta, \mu, \epsilon_1)$-local leakage-resilient. Furthermore, let $\Sigma_2 \triangleq EAGSh_{N,T+\frac{2N}{\sqrt{q-1}}+O(1), T}$ be a ramp secret sharing scheme defined over $\mathbb{F}_{q_2}$ with $N$ players and $T$ privacy by Theorem 2 such that $q_2$ is a prime such that $q_2 \approx q$. Then when $N \geq \frac{\frac{1}{\sqrt{q}} + \frac{1}{\sqrt{q}}}{\epsilon_1 + \epsilon_2} - 3T$, $\epsilon_1 < \epsilon_2$. In other words, when $N \geq \frac{1}{\epsilon_1 + \epsilon_2 + 3T}$, $\Sigma_1$ provides a stronger leakage-resilience against $A$ compared to $\Sigma_2$.

**Proof:** Here, it is sufficient to show that $\Delta \triangleq \frac{\epsilon_2}{\epsilon_1} < 1$ for the choices of $N, T$ and $\theta$. Letting $\rho = \frac{T}{N}$ and $\tilde{\rho} = \frac{\theta}{N}$, we have

$$\Delta \equiv q^{N \left(\frac{\rho}{\sqrt{q}} - \frac{1}{\sqrt{q}}\right)} \frac{\sqrt{q} \sin \left(\frac{\pi}{q}\right)}{\sin \left(\frac{\pi}{q}\right)}.$$
specific settings of the parameters, we have the possibility of having the statistical distance upper bound $T$ such that $\rho < \hat{\rho}$. Hence for the choice of $N$, the exponent of $q$ is non-positive, which implies that $\Delta < 1$ concluding the proof. 

E. Example Parameter Settings

In this section, we consider some specific parameter settings for constructions in Theorems 1, 2 and 3 to demonstrate the possibility of having the statistical distance upper bound $\epsilon$ to be small. In particular, we will show that for some specific settings of the parameters, we have $\epsilon = \epsilon^{-\Omega(N)}$. Note that this means that it can be set arbitrarily small as $N$ grows. Moreover, to provide some more concrete illustration, we will also provide some specific values of the parameters such that $\epsilon = 2^{-40}$.

1) AGSh$_{N,T}$: In this section, we provide parameter settings for constructions in Theorem 1.

Lemma VI.8: Let $q > 300$ be a square of a prime. Let $N$ be the number of players and let $0 < \hat{\rho} < \rho < 1 - \frac{2}{\sqrt{q} - 1}$ be two positive real numbers and let $T = \rho N$ and $\theta = \hat{\rho} N$. Lastly, let $\mu < \log \sqrt{q}$. Then if the parameters satisfy the following three conditions:

$$\frac{6}{\pi^2} \frac{\ln q}{\sqrt{q} - 3} + 1 > \frac{1}{\sqrt{q} - 1} \quad (1)$$

$$\rho > \frac{\ln q}{\sqrt{q} - 1} \quad (2)$$

and

$$\hat{\rho} < \rho - \frac{\ln q}{\sqrt{q} - 1} \left(1 - \frac{1}{\sqrt{q} - 1} \right), \quad (3)$$

the secret sharing scheme AGSh$_{N,T}$ proposed in Theorem 1 is $(\mu, \rho)$-LL resilient where $\epsilon = \epsilon^{-\Omega(N)}$.

Proof: We first note that since $q > 300$, there exists $\mu \geq 1$ a positive integer such that $\mu$ satisfies Condition (1). By having such $\mu$, we can verify that there exists $\rho < 1 - \frac{2}{\sqrt{q} - 1}$ such that $\rho$ satisfies Condition (2). In turn, this implies that there exists $\hat{\rho} > 0$ such that $\hat{\rho}$ satisfies Condition (3). Let $(\mu, \rho, \hat{\rho})$ be a triple that satisfies all such conditions.

Recall that by Theorem 1, for a code of length $N$ with $\theta < T$ and $\mu < \log \sqrt{q}$, we have $g = \frac{N}{\sqrt{q} - 1}$ and $\epsilon \leq q^{N - T} \frac{2^\mu \sin \left(\frac{\pi}{q}\right)}{\sqrt{q} \sin \left(\frac{\pi}{\sqrt{q}}\right)}$ for any $T \leq N \left(1 - \frac{2}{\sqrt{q} - 1}\right)$. By using Taylor expansion, we can estimate

$$\frac{2^\mu \sin \left(\frac{\pi}{q}\right)}{\sqrt{q} \sin \left(\frac{\pi}{\sqrt{q}}\right)} \approx q - \frac{\mu^2}{6} \frac{q}{2^{2\mu}} + O \left(\frac{q}{\mu^3}\right).$$

Then we have the estimation

$$\log_q (\epsilon) \leq N \left(1 - \frac{1}{\sqrt{q} - 1} \right) - \frac{1}{\ln q} \left(\rho - \hat{\rho} + \frac{1}{N}\right) \frac{\pi^2}{6} \left(\frac{1}{2^{2\mu}} - \frac{1}{q}\right) + O \left(\frac{1}{q^2 \ln q}\right).$$

Hence, to have $\epsilon$ being negligible with respect to $N$, it is sufficient to require that

$$1 - \frac{1}{\sqrt{q} - 1} - \rho < \frac{1}{\ln q} \left(\rho - \hat{\rho} + \frac{1}{N}\right) \frac{\pi^2}{6} \left(\frac{1}{2^{2\mu}} - \frac{1}{q}\right)$$

or equivalently

$$\hat{\rho} < \rho - \frac{\ln q}{\sqrt{q} - 1} \left(1 - \frac{1}{\sqrt{q} - 1} \right).$$

However, this is guaranteed by Condition (3), which is satisfied by our choice of $\rho$ and $\hat{\rho}$, completing the proof.

In the following we provide an example of the concrete values of the parameters to obtain a concrete upper bound for $\epsilon$. More specifically, we provide a concrete set of parameters such that $\epsilon \leq 2^{-40}$.

Example 1: Let $q = 31^2 = 961$, $\mu = 1$, $\rho = 0.9265$ and $\hat{\rho} = 0.25$. Then the triple $(\mu, \rho, \hat{\rho})$ satisfies Conditions (1), (2) and (3). Furthermore, it can be verified that for any $N \geq 1000$, we have $\epsilon < 2^{-40}$.

2) EAGSh$_{N,T}$: In this section, we provide similar results for constructions in Theorem 2. Since the proof will be the same as that of Lemma VI.8, we state the result without proof.

Lemma VI.9: Let $q \geq 17$ be a prime. Let $N$ be the number of players and let $0 < \hat{\rho} < \rho < 1 - \frac{2}{\sqrt{q} - 1} - \frac{1}{\sqrt{q}}$ be two positive real numbers, $T = \rho N$ and $\theta = \hat{\rho} N$. Lastly, let $\mu < \log q$. Then if the parameters satisfy the following three conditions:

$$\frac{12}{\pi^2} \frac{\ln q}{q - 3} + \frac{1}{q^2} < \frac{1}{2^{2\mu}} \quad (4)$$

$$\rho > \frac{\ln q}{\sqrt{q} - 1} \quad (5)$$

and

$$\hat{\rho} < \rho - \frac{\ln q}{\sqrt{q} - 1} \left(1 - \frac{1}{\sqrt{q} - 1} \right) \quad (6)$$

the secret sharing scheme EAGSh$_{N,T}$ proposed in Theorem 2 is $(\mu, \rho, \hat{\rho})$-LL resilient where $\epsilon = \epsilon^{-\Omega(N)}$.

Next, we provide an example of the concrete values of the parameters to obtain a concrete upper bound of $2^{-40}$ for $\epsilon$.

Example 2: Let $q = 97$, $\mu = 1$, $\rho = 0.485$ and $\hat{\rho} = 0.25$. Then the triple $(\mu, \rho, \hat{\rho})$ satisfies Conditions (4), (5) and (6). Furthermore, it can be verified that for any $N \geq 1600$, we have $\epsilon < 2^{-40}$.

3) MFEAGSh$_{N,T}$: In this section, we provide similar results for constructions in Theorem 3. Since the proof will be the same as that of Lemma VI.8, we state the result without proof.

Lemma VI.10: Let $q \geq 17$ be a prime. Let $N$ be the number of players and let $0 < \hat{\rho} < \rho < 1 - \frac{2}{\sqrt{q} - 1} - \frac{1}{\sqrt{q}}$ be two positive
real numbers, $T = \rho N$ and $\theta = \rho \tilde{N}$. Lastly, let $\mu < \log q$. Then if the parameters satisfy the following three conditions:
\begin{align}
\frac{12 \ln q}{\pi^2 q - 3} + \frac{1}{q^2} &< \frac{1}{24 \mu}, \\
\rho &> \frac{\ln q - \frac{2}{q^2}}{\ln q - \frac{2}{q^2}} + 2 \ln q
\end{align}
and
\begin{align}
\hat{\rho} &< \rho - \frac{\ln q}{\frac{1}{2q^2} - \frac{1}{q^2}} \left( \frac{2}{3} - \frac{2}{3(q-1)} - 2\rho \right),
\end{align}
the secret sharing scheme $MFEAGSH_{N, \alpha} = \mathbb{F}_q^N + T + \frac{2N}{3(q-1)} + 1, T$ proposed in Theorem 3 is $(\theta, \mu, \epsilon)$-LL resilient where $\epsilon = \frac{q}{\Omega(N)}$.

Next, we provide an example of the concrete values of the parameters to obtain a concrete upper bound of $2^{40}$ for $\epsilon$.

**Example 3:** Let $q = 211$, $\mu = 1$, $\rho = 0.33$ and $\hat{\rho} = 0.25$. Then the triple $(\mu, \rho, \hat{\rho})$ satisfies Conditions (7), (8) and (9). Furthermore, it can be verified that for any $N \geq 1600$, we have $\epsilon < 2^{-40}$.

**APPENDIX**

**A. Proof of Lemma III.4**

By Fourier Inversion Formula, the linearity of expectation and additivity of trace function, we have
\begin{align*}
\mathbb{E}_{x \in \mathbb{C}} \left[ \prod_{i=1}^{n} f_i(x_i) \right] &= \mathbb{E}_{x \in \mathbb{C}} \left[ \prod_{i=1}^{n} \sum_{\alpha_i \in \mathbb{F}_{p^w}} \hat{f}_i(\alpha_i) \cdot \chi_{\alpha_i}(x_i) \right] \\
&= \mathbb{E}_{x \in \mathbb{C}} \sum_{\alpha \in \mathbb{G}_{p^w}} \prod_{i=1}^{n} \hat{f}_i(\alpha_i) \cdot \chi_{\alpha}(x_i) \\
&= \mathbb{E}_{x \in \mathbb{C}} \left[ \sum_{\alpha \in \mathbb{G}_{p^w}} \prod_{i=1}^{n} \frac{1}{p^w} \omega_{p}^{-Tr(\alpha_i, x_i)} \right] \\
&= \sum_{\alpha \in \mathbb{G}_{p^w}} \mathbb{E}_{x \in \mathbb{C}} \left[ \frac{1}{p^w} \omega_{p}^{-Tr(\alpha, x)} \right].
\end{align*}

Next we consider $\mathbb{E}_{x \in \mathbb{C}} \left[ \frac{1}{p^w} \omega_{p}^{-Tr(\alpha, x)} \right]$ for various values of $\alpha$. Note that if $\alpha \in \mathbb{C}^\perp$, we have $\langle \alpha, x \rangle = 0$ for any $x \in C$. Hence $\mathbb{E}_{x \in \mathbb{C}} \left[ \frac{1}{p^w} \omega_{p}^{-Tr(\alpha, x)} \right] = 1$ for any $\alpha \in \mathbb{C}^\perp$.

So we focus the remainder of the proof for the case when $\alpha \notin \mathbb{C}^\perp$. Consider $\varphi_\alpha : C \to \mathbb{F}_p$ such that for any $x \in C, \varphi_\alpha(x) = Tr(\alpha, x)$. It is easy to see that $\varphi_\alpha$ is $\mathbb{F}_p$-linear, that is, for any $x, y \in C$ and $\lambda, \mu \in \mathbb{F}_p$, $\varphi_\alpha(\lambda x + \mu y) = \lambda \varphi_\alpha(x) + \mu \varphi_\alpha(y)$. This shows that for any $z \neq z' \in \mathbb{F}_p$ such that $(\varphi_\alpha)^{-1}(z)$ and $(\varphi_\alpha)^{-1}(z')$ are both non-empty, we have $|((\varphi_\alpha)^{-1}(z))| = |((\varphi_\alpha)^{-1}(z'))|$. Next we prove that $\varphi_\alpha$ is surjective. Since $\alpha \notin \mathbb{C}^\perp$, there exists $x' \in C$ such that $\langle \alpha, x' \rangle \neq 0 \in \mathbb{F}_{p^w}$. Due to the linearity of inner product and $C$ along with the fact that $\mathbb{F}_{p^w}$ is a field, for any $y \in \mathbb{F}_{p^w}$, we can find an appropriate multiplier $\lambda \in \mathbb{F}_{p^w}$ such that $\lambda x' \in C$ and $\langle \alpha, \lambda x' \rangle = y$. In particular, since the trace function is a surjective function from $\mathbb{F}_{p^w}$ to $\mathbb{F}_p$, there exists $x \in C$ such that $\varphi_\alpha(x) = 1$. Then for any $z \in \mathbb{F}_p$, it is easy to see that $z x \in (\varphi_\alpha)^{-1}(z)$. This shows that for any $z \in \mathbb{F}_p$, $(\varphi_\alpha)^{-1}(z)$ is non-empty and they have the same size for all choices of $z$, which is $p^{k-1}$. Hence, if $\alpha \notin \mathbb{C}^\perp$,
\begin{align*}
\mathbb{E}_{x \in \mathbb{C}} \left[ \frac{1}{p^w} \omega_{p}^{-Tr(\alpha, x)} \right] &= \frac{1}{|C|} \sum_{x \in C} \frac{1}{p^w} \omega_{p}^{-Tr(\alpha, x)} \\
&= \frac{1}{p^w} \cdot \sum_{i=0}^{p^w-1} \omega_{p}^{-i} = 0
\end{align*}
where the last equality is based on the fact that $\omega_{p}$ is a root of the polynomial $1 + x + \cdots + x^{p^w-1}$.

So we have
\begin{align*}
\mathbb{E}_{x \in \mathbb{C}} \left[ \frac{1}{p^w} \omega_{p}^{-Tr(\alpha, x)} \right] &= \begin{cases} 1, & \text{if } \alpha \in \mathbb{C}^\perp, \\ 0, & \text{otherwise} \end{cases}
\end{align*}
which completes our proof.

**B. Proof of Lemma IV.3**

Note that for $\alpha \neq 0$, we have $\mathbb{E}_{A_i(\alpha) \in \mathbb{C}} = p^{-w_{p}^{A_i}A_i}$ which is well defined. Let $\alpha_i \in \mathbb{F}_{p^w}$ be an element that maximizes $\mathbb{E}_{A_i(\alpha) \in \mathbb{C}}$. Then $\mathbb{E}_{A_i(\alpha) \in \mathbb{C}} = p^{-w_{p}^{A_i}A_i} = |\mathbb{E}_{A_i(\alpha) \in \mathbb{C}}|$. For $i = 1, \cdots, 2^N$, let $B_i = \alpha_i A_i$. Then we have $B_1, \cdots, B_{2^N} \subseteq \mathbb{F}_{p^w}$ such that $\sum_{i=1}^{2^N} |B_i| = p^{w_{p}}$. So applying Lemma IV.2, we have
\begin{align*}
\sum_{i=1}^{2^N} \max_{\alpha \neq 0} \left| \mathbb{E}_{A_i(\alpha) \in \mathbb{C}} \right| &\leq c_p.
\end{align*}

**REFERENCES**

[1] D. Aggarwal et al., “Stronger leakage-resilient and non-malleable secret sharing schemes for general access structures,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 11693, A. Boldyreva and D. Micciancio, Eds., Cham, Switzerland: Springer, 2019, doi: 10.1007/978-3-030-26951-7-18.

[2] T. Araki, J. Furukawa, Y. Lindell, A. Nof, and K. Ohara, “High-throughput semi-honest secure three-party computation with an honest majority,” in Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS). New York, NY, USA: Association for Computing Machinery, 2016, pp. 805–817, doi: 10.1145/2976749.2978331.

[3] G. Avoine and S. Vaudenay, “Optimistic fair exchange based on publicly verifiable secret sharing in Information Security and Privacy (Lecture Notes in Computer Science), vol. 3108, H. Wang, J. Pieprzyk, and V. Varadharajan, Eds. Berlin, Germany: Springer, 2004, doi: 10.1007/3-540-27800-9-7.

[4] M. Ben-Or, S. Goldwasser, and A. Wigderson, “Completeness theorems for non-cryptographic fault-tolerant distributed computation,” in Proc. 20th Ann. ACM Symp. Theory Comput. (STOC). New York, NY, USA: Association for Computing Machinery, 1988, pp. 1–10, doi: 10.1145/62212.62213.1998.

[5] F. Benhamouda, A. Degwekar, Y. Ishai, and T. Rabin, “On the local leakage resilience of linear secret sharing schemes,” J. Cryptol., vol. 34, no. 2, pp. 1–65, 2021. [Online]. Available: https://eprint.iacr.org/2019/653

[6] D. Boneh and M. K. Franklin, “Identity-based encryption from the Weil pairing,” in Proc. 21st Ann. Int. Cryptol. Conf. Adv. Cryptol. (CRYPTO). Berlin, Germany: Springer-Verlag, 2001, pp. 213–229.
[47] V. Shoup and R. Gennaro, “Securing threshold cryptosystems against chosen ciphertext attack,” J. Cryptol., vol. 15, no. 2, pp. 75–96, Jan. 2002.

[48] I. E. Shparlinski, M. A. Tsfasman, and S. G. Vladut, “Curves with many points and multiplication in finite fields,” in Coding Theory and Algebraic Geometry. New York, NY, USA: Springer-Verlag, 1992, pp. 145–169.

[49] A. Srinivasan and P. N. Vasudevan, “Leakage resilient secret sharing and applications,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 11693, A. Boldyreva and D. Micciancio, Ed. Cham, Switzerland: Springer, 2019, doi: 10.1007/978-3-030-26951-7-17.

[50] M. Stadler, “Publicly verifiable secret sharing,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 1070, U. Maurer, Ed. Berlin, Germany: Springer, 1996, doi: 10.1007/3-540-68339-9_17.

[51] H. Stichtenoth, Algebraic Function Fields and Codes, 2nd ed. Cham, Switzerland: Springer, 2008.

[52] D. R. Stinson and R. Wei, “Unconditionally secure proactive secret sharing scheme with combinatorial structures,” in Selected Areas in Cryptography (Lecture Notes in Computer Science), vol. 1758, H. Heys and C. Adams, Eds. Berlin, Germany: Springer, 2000, doi: 10.1007/3-540-46513-8-15.

[53] L. Zhou, F. B. Schneider, and R. Van Renesse, “APSS: Proactive secret sharing in asynchronous systems,” ACM Trans. Inf. Syst. Secur., vol. 8, no. 3, pp. 259–286, Aug. 2005.

Ivan Tjuawinata (Member, IEEE) received the Ph.D. degree from Nanyang Technological University, Singapore, in 2017. He is currently a Research Fellow with the Strategic Centre for Research in Privacy-Preserving Technologies and Systems (SCRiPTS), Nanyang Technological University. His research interests include secure multiparty computation, cryptanalysis, and coding theory.

Chaoping Xing (Senior Member, IEEE) received the Ph.D. degree from the University of Science and Technology of China in 1990. From 1990 to 1993, he was a Lecturer and an Associate Professor with the University of Science and Technology of China. From 1993 to 1995, he joined the University of Duisburg–Essen, Germany, as an Alexander von Humboldt Fellow. After this, he spent most time at the Institute of Information Processing, Austrian Academy of Sciences, in 1998. From March 1998 to November 2007, he was working with the National University of Singapore, as an Assistant Professor, an Associate Professor, and a Full Professor. From December 2007 to August 2019, he was working with Nanyang Technological University, as a Full Professor. Since September 2019, he has been with Shanghai Jiao Tong University, as a Chair Professor. He has been working on the areas of coding theory, cryptography, algebraic curves over finite fields, and quasi-Monte Carlo methods.