Improved Bounds on the Threshold Gap in Ramp Secret Sharing*

Ignacio Cascudo†, Jaron Skovsted Gundersen‡ and Diego Ruano§

Department of Mathematics, Aalborg University

15th January 2018

Abstract

In this paper we consider linear secret sharing schemes over a finite field $\mathbb{F}_q$, where the secret is a vector in $\mathbb{F}_q^\ell$ and each of the n shares is a single element of $\mathbb{F}_q$. We obtain lower bounds on the so-called threshold gap g of such schemes, defined as the quantity $r - t$ where r is the smallest number such that any subset of r shares uniquely determines the secret and t is the largest number such that any subset of t shares provides no information about the secret. Our main result establishes a family of bounds which are tighter than previously known bounds for $\ell \geq 2$. Furthermore, we also provide bounds, in terms of n and q, on the partial reconstruction and privacy thresholds, a more fine-grained notion that considers the amount of information about the secret that can be contained in a set of shares of a given size. Finally, we compare our lower bounds with known upper bounds in the asymptotic setting.

1 Introduction

Secret sharing, introduced independently by Blakley and Shamir, is among the most useful primitives in cryptography. A secret sharing scheme allows to distribute the knowledge of a secret among n participants by sending each of them a piece of information (a *share*), in such a way that only certain prescribed subsets of these participants can reconstruct the secret from the joint information they have received. Secret sharing schemes are not only useful as a stand-alone primitive that can be used for secure distributed storage of information, but also play an important role as an element in more complex cryptographic tools, in areas such as threshold cryptography or secure multiparty computation.

In the study of secret sharing schemes and its applications it is often interesting to determine the amount of information about the shared secret that can be derived from

*Supported by the Danish Council for Independent Research, grant DFF-4002-00367, and the Spanish Ministry of Economy/FEDER: grants MTM2015-65764-C3-2-P and MTM2015-69138-REDT.

†ignacio@math.aau.dk

‡jaron@math.aau.dk

§diego@math.aau.dk

pooling together a certain fixed number of shares. We say that a secret sharing scheme has t-privacy if any set of t shares provides no additional information about the secret to what was known a priori. On the other hand, the secret sharing scheme has r-reconstruction if the knowledge of any set of r shares uniquely determines the secret. By abuse of notation, fix t to be the largest integer for which there is t-privacy and fix r to be the smallest integer for which there is r-reconstruction. Then obviously $0 \leq t < r \leq n$, and we define the *threshold gap* as $g = r - t$, which is thus a strictly positive integer. It is usually desirable for applications of secret sharing that the privacy and reconstruction thresholds are as close as possible and hence, that the threshold gap is small. Since this allows to optimize the compromise between security against an adversary who attempts to learn enough shares to gain information about the secret (for which we want to set t large), and resilience against losing a number of shares by corruption or other reasons (for which we want to set r small).

Secret sharing schemes with threshold gap $g = 1$ are called *threshold secret sharing schemes*. Shamir's secret sharing scheme (see Section 2 for its definition) is the most well-known example of a threshold secret sharing scheme: for any integers t and n with $1 \leq t < n$, one can construct a Shamir secret sharing scheme for n participants with t privacy and $t + 1$ reconstruction. However, Shamir's scheme presents some restrictions regarding the size of the secret and shares in terms of n: in first place, both the secret and each of the shares are elements of the same finite field, which means that each of the shares is as large as the secret; in second place, the finite field must have at least $n + 1$ elements (remember n is the number of participants) and therefore each share must be at least $\log(n + 1)$ bits long.

Typically, in applications of secret sharing we would like the secret to be as large as possible while the shares are small, but it turns out that the two restrictions above are unavoidable for threshold secret sharing schemes, and more in general in secret sharing schemes with small threshold gap.

Indeed, consider first the relation between the size of the shares and the size of the secret. It is well-known that in any threshold secret sharing scheme, each share must be at least the same size as the secret (this holds more generally for any perfect secret sharing scheme, i.e., any secret sharing scheme where every set of shares either has full information about the secret or no information about it). And, more generally, if every share is an element of a certain alphabet of size q and the secret is a-priori uniformly distributed in an alphabet of size M, then it necessarily holds that

$$g \geq \log_q M, \tag{1}$$

see [3]. This bound is tight: it can be attained by a generalization of Shamir's scheme frequently known as packed Shamir's scheme, first proposed by Blakley and Meadows [2] (also defined in Section 2) where each share is in a finite field $\mathbb{F}_q$, the secret is in $\mathbb{F}_q^\ell$ for some $\ell \geq 1$ and we have $g = \ell$. We point out that this secret sharing scheme requires that $q \geq n + \ell$

Second, the size of the shares in a threshold scheme is also restricted by the number of participants, as a series of results have shown. Indeed, in first place, it is known that threshold secret sharing schemes where the secret and each share is in the same alphabet are equivalent to MDS codes. The length of these codes is upper bounded by the size of the alphabet over which they are defined. Exploiting this connection, one can already show that if $1 \leq t < n-1$ (and $g = 1$, since we are considering threshold schemes), then $n < 2q - 2$ (see [11], Theorem 11.113).

But even in the more general case where we do not assume that the secret is in the same alphabet as the shares (for example even if the secret is just one bit), it was first noticed in the unpublished work [17] (see [6] for the statement and proof) that in any threshold scheme the average bitlength λ^* of the shares is $\Omega(\log(n-t))$. The result was later generalized in [6], where it was shown that for any secret sharing scheme where $t \geq 1$ (no individual participant obtains information about the secret) it necessarily holds that

$$g \geq \frac{n-t+1}{2^{\lambda^*}}.$$

If all shares belong to some alphabet of cardinality q, the bound can be rewritten as

$$g \geq \frac{n-t+1}{q}. \tag{2}$$

This bound hence establishes that, for certain values of t and n, there exist limitations on how small the threshold gap can be that depend solely on the size of the shares (and not on the secret). The bound was shown to be tight for $t = 1$ and $t = 2$ (the latter only in the case $q = 2$) in [21].

Later, [5] showed that if $r \leq n-1$, the bound

$$g \geq \frac{r+1}{q}$$

holds, which together with the bound in [6] implies

$$g \geq \frac{n+2}{2q-1} \tag{3}$$

as long as $1 \leq t < r \leq n-1$. This last bound had been shown earlier by [6] only in the case where the secret sharing scheme is $\mathbb{F}_q$-linear.

The two kinds of limitations that we have mentioned, represented by Equations (1) and (3) above are incomparable: the former depends on the relation between the sizes of the secret and shares, while the latter sets limitations on the relation between the size of the shares and the number of participants. Note that, even though the bound given in Equation (1) can be attained by the Blakley-Meadows construction, this requires that $n < q$, and therefore the bound is not necessarily tight when n grows in relation to q (and in fact in general it cannot be attained, by virtue of Equation (3)). It is then natural to investigate what bounds one can get which depend on all these parameters simultaneously. In this regard, for $\mathbb{F}_q$-linear schemes where the secret is in $\mathbb{F}_q^\ell$ with $\ell \geq 2$ and each share is in $\mathbb{F}_q$, [6] showed the bound

$$g \geq \frac{n+2}{2q+1} + \frac{2q}{2q+1}(\ell - 1) \tag{4}$$

which is tighter than the straightforward combination $g \geq \max\{\ell, \frac{n+2}{2q-1}\}$ of Equations (1) and (3), when ℓ is large enough.

1.1 Contributions

In this paper we focus on $\mathbb{F}_q$-linear secret sharing schemes where secrets are in $\mathbb{F}_q^\ell$ and every share is in $\mathbb{F}_q$. In Section 3, we improve the bound (4) given in [6]. More precisely our main result (Theorem 3.2) is a family of bounds given by

$$g \geq \frac{q^m - 1}{q^{m+1} - 1}(n+2) + \frac{q^{m+1} - q^m}{q^{m+1} - 1}(\ell - 2m), \tag{5}$$

for $m = 0, 1, \ldots, \ell - 1$, and we show that for any $\ell \geq 2$, there is some m for which the new bound is tighter than (4).

Furthermore, in Section 4 we consider a more fine-grained notion of information-access thresholds. Let r_i, for $i = 1, \ldots, \ell$, be the smallest number such that every set of shares of that size gives at least i q-bits of information about the secret and let t_i, also for $i = 1, \ldots, \ell$, be the largest integer such that every set of shares of that size learns less than i q-bits about the secret. Note that $r_\ell = r$ and $t_1 = t$. There are several potential uses of partial reconstruction and privacy thresholds in cryptography. For example, the notion of functional secret sharing introduced in [1] considers a scenario where large enough sets of participants can recover certain functions of the secrets and hence the threshold r_i gives us some information about functional secret sharing schemes where the output of the functions of interest consist of i q-bits. On the other hand, considering a relaxed notion of privacy (the threshold t_i) may be interesting in applications where secret sharing is combined with some other privacy amplification technique. For example with the goal of constructing a linear-time encodable secret sharing scheme [10] combines an error correcting code (which can be seen as a secret sharing scheme where small sets of participants can obtain partial information about the secret) with a hash function that destroys this partial information, so that perfect privacy is obtained in the final construction. This combination of "imperfect" secret sharing and privacy amplification may be of interest in secure computation, too.

Partial reconstruction and privacy thresholds were studied in [15, 18], by using the representation of a linear secret sharing scheme in terms of nested codes, introduced in [9]. It is then shown that the Relative generalized Hamming weights of the pair of nested codes used to define the secret sharing scheme determine the thresholds [19].

We extend some of the aforementioned previous results on limitations on r and t in both this paper and [6] to the partial reconstruction and privacy thresholds. We derive that as long as $t \geq 1$, we necessarily have

$$r_i \geq \frac{n}{q^{\ell-i+1}} + 1$$

for all $i \in \{1, \ldots, \ell\}$. Note that for $i = \ell$ we obtain $r \geq \frac{n}{q} + 1$. This is a bound that was also shown in [6] and was used to prove the more general inequality (2).

Moreover, we can also prove this bound under milder conditions, namely if $t_j \geq j$ for some $j \in \{1, \ldots, \ell\}$, then the same bound

$$r_i \geq \frac{n}{q^{\ell-i+1}} + 1$$

holds, but now for every $i \in \{j, j+1, \ldots, \ell\}$.

Moreover, we show that

$$g \geq \frac{n+2}{2q-1} + \frac{q-1}{2q-1}(a_i + b_i),$$

where $a_i = t_i - t - i + 1 \geq 0$ and $b_i = r - r_{\ell-i+1} - i + 1 \geq 0$ are two quantities that capture how much the scheme deviates from the situation where $t_1 = t, t_2 = t+1, \ldots, t_\ell = t+\ell-1$ and $r_\ell = r$, $r_{\ell-1} = r-1, \ldots, r_1 = r-\ell+1$, which occurs in the scheme of Blakley-Meadows (also known as packed Shamir), and which would correspond to $a_i = 0$, $b_i = 0$ for all i. Furthermore, we consider an example attaining this bound.

Finally, we consider asymptotic secret sharing schemes in Section 5. We adopt the setting considered in [14], define an asymptotic threshold gap (in Equation (23)) and provide the asymptotic version of the previous bounds. Finally, we compare our bound with the asymptotic version of the bounds in [6] and investigate how sharp is our bound by comparing it with threshold gaps of secret sharing schemes constructed from algebraic geometric codes (in the case of large fields) and from random linear codes (for small fields).

2 Secret Sharing

In this section, we recall some notions regarding secret sharing schemes and their relationship with linear codes.

Let $S_0, S_1, \ldots, S_n$ be random variables taking values in the finite alphabets $\mathcal{S}_0, \mathcal{S}_1, \ldots, \mathcal{S}_n$. Then we call $\mathbf{S} = (S_0, S_1, \ldots, S_n)$ a vector of random variables. In this paper, we let $\mathcal{I} = \{0, 1, \ldots, n\}$ and $\mathcal{I}^* = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$ and for a subset $A \subseteq \mathcal{I}$ we denote by $\mathbf{S}_A$ the vector $(S_i)_{i \in A}$. Notice that $\mathbf{S} = \mathbf{S}_{\mathcal{I}}$. With this notation we define a secret sharing scheme.

Definition 2.1 (Secret Sharing Scheme): *A secret sharing scheme Σ is a vector of random variables*

$$\mathbf{S} = (S_0, S_1, \ldots, S_n) \in \mathcal{S}_0 \times \mathcal{S}_1 \times \cdots \times \mathcal{S}_n,$$

such that

$$H_q(S_0) = \log_q |\mathcal{S}_0|,$$

where H_q is the Shannon entropy with base q.[1] *Further, we require that*

$$H_q(S_0 | \mathbf{S}_{\mathcal{I}^*}) = 0.$$

We call S_0 the *secret* and, for $i \in \mathcal{I}^*$, we call S_i the i'th *share*. The scheme has n *participants*, which we identify with the set $\mathcal{I}^*$, and the i'th participant holds S_i, for $i = 1, 2, \ldots, n$.

The requirement that $H_q(S_0) = \log_q |\mathcal{S}_0|$ implies that the random variable S_0 is uniformly distributed in $\mathcal{S}_0$; while it is of course possible to consider secret sharing schemes

[1] Note that H_q is the Shannon entropy of base q and not the Rényi entropy of order q.

with a different distribution on the secret space, it was shown in [4] that such scheme could be transformed into one where the distribution of secrets is uniform and with the same reconstruction and privacy thresholds (introduced below). Therefore, this assumption is without loss of generality for our purposes.

The other requirement, that $H_q(S_0|\mathbf{S}_{\mathcal{I}^*}) = 0$, means that the secret is uniquely determined by the set of all the shares with probability 1.

A secret sharing scheme is called *linear* if $\mathbf{S}$ is uniformly distributed on some subspace $V \subseteq \mathcal{S}_0 \times \mathcal{S}_1 \times \cdots \times \mathcal{S}_n$ and if $\mathcal{S}_i$ is a $\mathbb{F}_q$-vector space for all $i \in \mathcal{I}$ where $\mathbb{F}_q$ is the finite field with q element. In this paper, we will focus on the schemes, where $\mathcal{S}_i$ is one-dimensional for $i \in \mathcal{I}^*$ and $\mathcal{S}_0$ is ℓ-dimensional. Without loss of generality we can assume that $\mathcal{S}_0 = \mathbb{F}_q^\ell$ and $\mathcal{S}_i = \mathbb{F}_q$ for the $i \in \mathcal{I}^*$.

Linear secret sharing schemes are also characterized by the following property; consider two secrets $\mathbf{s}, \mathbf{t} \in \mathcal{S}_0 = \mathbb{F}_q^\ell$. Let $\mathbf{x} \in \mathbb{F}_q^n$ be a possible share vector for the secret $\mathbf{s}$, i.e. $P((S_0, \mathbf{S}_{\mathcal{I}^*}) = (\mathbf{s}, \mathbf{x})) > 0$, and $\mathbf{y} \in \mathbb{F}_q^n$ a possible share vector for $\mathbf{t}$. Thus, $(\mathbf{s}, \mathbf{x}) \in V$ and $(\mathbf{t}, \mathbf{y}) \in V$. For $a, b \in \mathbb{F}_q$, we have $(a\mathbf{s} + b\mathbf{t}, a\mathbf{x} + b\mathbf{y}) \in V$, proving that

$$P((S_0, \mathbf{S}_{\mathcal{I}^*}) = (a\mathbf{s} + b\mathbf{t}, a\mathbf{x} + b\mathbf{y})) > 0.$$

Therefore, a linear combination of share vectors results in a share vector for the same linear combination of the corresponding secrets. This property makes linear secret sharing schemes very useful for secure multiparty computation and threshold cryptography.

Well known examples of linear secret sharing schemes are Shamir's secret sharing scheme and its generalization by Blakley and Meadows, described below. Assume that $n + \ell \leq q$. Let $\alpha_{0,1}, \alpha_{0,2}, \ldots, \alpha_{0,\ell}, \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_q$ be pairwise-distinct. Fix an integer $\ell - 1 \leq k \leq n - 1$ and define the vector of random variables $\mathbf{S}$ given by selecting a polynomial uniformly at random among the set of polynomials in $\mathbb{F}_q[X]$ of degree less than k and defining S_0 as the variable taking the value $(f(\alpha_{0,1}), f(\alpha_{0,2}), \ldots, f(\alpha_{0,\ell})) \in \mathbb{F}_q^\ell$ and each of the S_i's as the variables taking values $f(\alpha_i) \in \mathbb{F}_q$. Note that the condition $n + \ell \leq q$ can be weakened to $n \leq q$ by using an element of an extension field as a single evaluation point for the secret, rather than the elements $\alpha_{0,1}, \alpha_{0,2}, \ldots, \alpha_{0,\ell}$, as was done in for example [8].

Shamir's scheme as defined in [22] is the version with $\ell = 1$ and $\alpha_{0,1} = 0$. Blakley and Meadows' scheme is sometimes referred to as packed Shamir's scheme. It is easy to verify that this scheme is linear.

The following alternative definition of linear secret sharing schemes was given in [9]. For completion we show that the definitions are equivalent in Appendix A.

Let C_1, C_2, and L be linear codes in $\mathbb{F}_q^n$, such that $C_1 = L \oplus C_2$. Further, let $\dim L = \ell$, $\dim C_2 = k_2$, $\dim C_1 = k_1 = k_2 + \ell$, and let $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_\ell\}$ be a basis of L and $\{\mathbf{b}_{\ell+1}, \mathbf{b}_{\ell+2}, \ldots, \mathbf{b}_{k_1}\}$ be a basis of C_2. We define a linear secret sharing scheme from the nested linear codes $C_2 \subsetneq C_1$ in the following manner. Given the secret $\mathbf{s} \in \mathbb{F}_q^\ell$, choose k_2 uniformly random elements in $\mathbb{F}_q$, say $a_1, a_2, \ldots, a_{k_2}$. Then the vector

$$\mathbf{c} = s_1\mathbf{b}_1 + s_2\mathbf{b}_2 + \cdots + s_\ell\mathbf{b}_\ell + a_1\mathbf{b}_{\ell+1} + a_2\mathbf{b}_{\ell+2} + \cdots + a_{k_2}\mathbf{b}_{k_1} \in C_1$$

is called a share vector and the i'th share is defined to be the i'th entry of this vector $\mathbf{c}$. One should notice that, setting the distribution of the secret to be uniform in $\mathbb{F}_q^\ell$, this is indeed a secret sharing scheme according to our definition, since the set of all shares corresponds to a vector in $C_1 = C_2 \oplus L$ which can be projected into a unique element in L.

In secret sharing, we are interested in determining which subsets of participants are able to reconstruct the secret from their shares and which subsets are not. This leads to the definition of privacy and reconstructing sets.

Definition 2.2 (Privacy and Reconstructing set): *Let Σ be a secret sharing scheme given by the vector of random variables $\mathbf{S}$ and let $A \subseteq \mathcal{I}^*$. Then A is a privacy set if*

$$H_q(S_0|\mathbf{S}_A) = H_q(S_0),$$

and A is a reconstructing set if

$$H_q(S_0|\mathbf{S}_A) = 0.$$

As in Definition 2.1, $H_q(S_0|\mathbf{S}_A) = 0$ implies that the secret is uniquely determined by the shares held by the participants in A. On the other hand, $H_q(S_0|\mathbf{S}_A) = H_q(S_0)$ is equivalent to S_0 and $\mathbf{S}_A$ being independent. Therefore, the participants in A have no information about the secret from their shares. Additionally, we can define the information held by the participants in A using the *mutual information*

$$I_q(S_0, \mathbf{S}_A) = H_q(S_0) - H_q(S_0|\mathbf{S}_A). \tag{6}$$

This quantity is measured in q-bits and lies between $0 \leq I_q(S_0, \mathbf{S}_A) \leq H_q(S_0)$. It equals 0 exactly when A is a privacy set and it equals $H_q(S_0)$ exactly when A is a reconstructing set. One should notice that for linear secret sharing schemes with $\mathcal{S}_0 = \mathbb{F}_q^\ell$ we have $H_q(S_0) = \ell$. Furthermore, it is shown in [18] that for such schemes the mutual information is given by

$$I_q(S_0, \mathbf{S}_A) = \dim \pi_A(C_1) - \dim \pi_A(C_2), \tag{7}$$

where π_A is the *projection* $\pi_A \colon \mathbb{F}_q^n \to \mathbb{F}_q^{|A|}$ given by $\pi_A(\mathbf{c}) = \mathbf{c}_A$. Hence, we conclude that, in linear secret sharing, the information about the secret held by some set of participants, when expressed in q-bits, is always an integer between 0 and ℓ. Furthermore, we have for a subset $A \subseteq \mathcal{I}^*$ and an element $i \in \mathcal{I}^* \setminus A$ that

$$I_q(S_0, \mathbf{S}_A) \leq I_q(S_0, \mathbf{S}_{A\cup\{i\}}) \leq I_q(S_0, \mathbf{S}_A) + 1.$$

The set of all privacy sets is called the *adversary structure* of the scheme and is denoted by $\mathcal{A}(\Sigma)$. Similarly, the set of all reconstructing sets is called the *access structure* and is denoted by $\Gamma(\Sigma)$. From these definitions we introduce some thresholds for the secret sharing schemes.

Definition 2.3 (Privacy and Reconstruction Threshold): *Let Σ be a secret sharing scheme with adversary structure $\mathcal{A}(\Sigma)$ and access structure $\Gamma(\Sigma)$. The privacy threshold t for the scheme Σ is given by the maximal s such that*

$$\{A \subseteq \mathcal{I}^* : |A| = s\} \subseteq \mathcal{A}(\Sigma).$$

Similarly, the reconstruction threshold r is given by the minimal s such that

$$\{A \subseteq \mathcal{I}^* : |A| = s\} \subseteq \Gamma(\Sigma).$$

Definition 2.4 (Threshold gap): *Let Σ be a secret sharing scheme, and let t and r be the privacy and reconstruction threshold, respectively. Then*

$$g = r - t$$

is the threshold gap.

By (6) it can be deduced that $0 \leq t < r \leq n$, and therefore the threshold gap g is always a positive integer. Secret sharing schemes with $r = t + 1$, and therefore $g = 1$, are called threshold secret sharing schemes. As mentioned in the introduction it is often desirable to have a small g, but this will have the disadvantage that the shares are large compared to the secret, which means one has to consider this trade-off.

In a secret sharing scheme with secrets larger than the shares, some subsets of participants will obtain partial information about the secret. This gives rise to defining the partial privacy and reconstruction thresholds in a similar manner that we defined t and r.

Definition 2.5 (Partial Privacy and Reconstruction Thresholds): *The i'th partial privacy threshold of a secret sharing scheme, t_i, is given by*

$$t_i = \max\{s \mid \forall A \subseteq \mathcal{I}^*, |A| = s, I_q(S_0, \mathbf{S}_A) < i\}.$$

Similarly, the i'th partial reconstruction threshold, r_i, is given by

$$r_i = \min\{s \mid \forall A \subseteq \mathcal{I}^*, |A| = s, I_q(S_0, \mathbf{S}_A) \geq i\}.$$

This means that t_i is the maximal number such that all sets of t_i participants do not obtain i q-bits of information. On the other hand, r_i is the minimal number such that all subsets of r_i participants can reconstruct i q-bits of information.

Since the information in q-bits is always a nonnegative integer and the maximum information is ℓ we have that $t = t_1$ and $r = r_\ell$.

We will denote the *dual* of a linear code C by $C^\perp$, the *minimum distance* by $d_{\min}(C)$, the *support* by

$$\operatorname{supp}(C) = \{i : \exists (c_1, c_2, \ldots, c_n) \in C, c_i \neq 0\},$$

and the *support weight* by $w_S(C) = |\operatorname{supp}(C)|$. With these definitions, the i'th *relative generalized Hamming weight* (RGHW) is defined as

$$M_i(C_1, C_2) = \min\{w_S(D) : D \subseteq C_1, D \cap C_2 = \{0\}, \dim(D) = i\}.$$

We notice that the first RGHW is simply the minimum Hamming weight of $C_1 \setminus C_2$, which implies that $d_{\min}(C_1) \leq M_1(C_1, C_2)$. For $C_2 = \{0\}$ we have $d_{\min}(C_1) = M_1(C_1, C_2)$.

In [15, 18] it is shown that the RGHWs characterize the partial privacy and reconstruction thresholds. They showed that

$$\begin{aligned} t_i &= M_i(C_2^\perp, C_1^\perp) - 1 \\ r_i &= n - M_{\ell-i+1}(C_1, C_2) + 1. \end{aligned} \tag{8}$$

Further, it is shown in [19] that $M_i(C_1, C_2)$ is strictly increasing with i, which implies that $t_i < t_{i+1}$ and $r_i < r_{i+1}$, for all $i = 1, 2 \ldots \ell - 1$.

In particular, (8) yields

$$\begin{aligned} t &= M_1(C_2^\perp, C_1^\perp) - 1 \\ r &= n - M_1(C_1, C_2) + 1 \\ g &= n - \big(M_1(C_1, C_2) + M_1(C_2^\perp, C_1^\perp)\big) + 2, \end{aligned} \tag{9}$$

which implies that

$$\begin{aligned} t &\geq d_{\min}(C_2^\perp) - 1 \\ r &\leq n - d_{\min}(C_1) + 1 \\ g &\leq n + 2 - \big(d_{\min}(C_1) + d_{\min}(C_2^\perp)\big)\,. \end{aligned} \tag{10}$$

3 Bounds from the Generalized Griesmer Bound

In applications, we often want secret sharing schemes where the privacy and reconstruction thresholds are close to each other, which means that we want the threshold gap to be small. From this point of view, we could refer to the bounds in (10) as positive bounds.

However, as it was mentioned in the introduction, there are known restrictions for how small the shares of such schemes can be when one requires a small threshold gap. These restrictions come from two sources: the relative size of the secret with respect to the shares and the relation between the size of the shares and the total number of participants.

In this section we obtain new bounds for the threshold gap of linear secret sharing schemes that depend on the two aforementioned factors simultaneously and show how they improve previous bounds in all cases.

First we recall known bounds. As in the previous section, let $\mathbb{F}_q^\ell$ be the space of secrets and let each of the shares be an element of $\mathbb{F}_q$. Then, it is well-known that $g \geq \ell$. This is a consequence of the more general result, also valid for non-linear secret sharing schemes, that $g \geq H(S_0)/H(S_i)$ for every share S_i, as proved in [3]. Coming back to the linear case, it is interesting to see this bound in the light of partial privacy and reconstruction thresholds too: in the context of Wiretap channel type II, the results in [19] imply the following bounds on t_i and r_i:

$$\begin{aligned} t_i &\leq k_2 + i - 1 \\ r_i &\geq k_2 + i, \end{aligned} \tag{11}$$

which combined also yield $g \geq \ell$. This bound is of the first type mentioned above: it only depends on the relation between the size of the secret and the size of the shares, but does not take into account the number of participants. The bound is attainable by the Blakley-Meadows' secret sharing scheme, but this scheme requires $n \leq q$.

In [6] lower bounds on the threshold gap depending on the number of participants and its relation to the size of the shares were derived. If we denote by

$$\begin{aligned} \mathrm{B}_{\mathrm{CCX}(1)}(n, q) &= \frac{n+2}{2q-1}, \\ \mathrm{B}_{\mathrm{CCX}(2)}(n, q, \ell) &= \frac{n+2}{2q+1} + \frac{2q}{2q+1}(\ell - 1), \end{aligned}$$

then the bounds in [6] state that

$$\begin{aligned} &g \geq \mathrm{B}_{\mathrm{CCX}(1)}(n, q), && \text{if } 1 \leq t < r \leq n-1 \\ &g \geq \mathrm{B}_{\mathrm{CCX}(2)}(n, q, \ell), && \text{if } \ell \geq 2. \end{aligned} \tag{12}$$

Both bounds were proved in [6] for linear secret sharing schemes. However, the first one is also valid for non-linear secret sharing schemes, as shown in [5].

Note that both bounds exclude the case $\ell = 1$ and $t = 0$, and the case $\ell = 1$ and $r = n$. This is unavoidable, since in both cases there exist secret sharing schemes where n and q are unrestricted. Indeed in the first case the scheme consisting on simply distributing the secret to all participants fulfils $r = 1$, and hence $g = 1$. On the other hand, for the second case consider additive secret sharing schemes, where the secret is the sum of all the shares, implying that $t = n - 1$. Note that the second bound implies that the bound $g \geq \ell$ we mentioned above cannot be attained with equality for all n and q as long $\ell \geq 2$.

In the following, by considering RGHWs, we construct a new lower bound on the threshold gap for linear secret sharing schemes which, as in the case of $g \geq \mathrm{B}_{\mathrm{CCX}(2)}(n, q, \ell)$, also takes both the secret and the share size into account. Additionally, we will derive limitation bounds on t_i and r_i using the same approach. We will compare the bound on the threshold gap with the bounds in (12), showing improvement in most cases.

We first present the following bounds on the RGHWs from [25].

Proposition 3.1 (The generalized Griesmer bound on RGHW): *Let $C_2 \subsetneq C_1$ be linear codes. For $0 \leq i \leq k_1 - k_2 = \ell$, the i'th RGHW satisfies*

$$n \geq k_2 + M_i(C_1, C_2) + \sum_{j=1}^{\ell - i} \left\lceil \frac{q-1}{q^j(q^i - 1)} M_i(C_1, C_2) \right\rceil .$$

By using that $\lceil a \rceil \geq a$, for the first m terms in the sum, and $\lceil a \rceil \geq 1$, for the remaining terms, we write

$$\begin{aligned} &n \geq k_2 + M_i(C_1, C_2) + \frac{q-1}{q^i - 1} M_i(C_1, C_2) \sum_{j=1}^{m} \frac{1}{q^j} + \ell - i - m \Leftrightarrow \\ &n \geq k_1 - i - m + M_i(C_1, C_2) + \frac{q^m - 1}{q^{m+i} - q^m} M_i(C_1, C_2), \end{aligned}$$

which is equivalent to

$$M_i(C_1, C_2) \leq \frac{q^{m+i} - q^m}{q^{m+i} - 1} \left(n - k_1 + i + m \right). \tag{13}$$

Similar arguments show that

$$M_i(C_2^{\perp}, C_1^{\perp}) \leq \frac{q^{m+i} - q^m}{q^{m+i} - 1} \left(k_2 + i + m \right). \tag{14}$$

One should notice that different choices of m lead to different bounds on the RGHWs. It is not necessarily the highest possible m which gives the best bound, and hence we need to choose the parameter m carefully in order to make the bound as good as possible.

The expressions in (13) and (14) lead to the following bounds on the partial privacy and reconstruction thresholds together with the threshold gap as well.

Theorem 3.2: *Let $C_2 \subsetneq C_1$ define a linear secret sharing scheme. Then for $i \in \{1, 2, \ldots, \ell\}$,*

$$t_i \leq \frac{q^{m+i} - q^m}{q^{m+i} - 1}(k_2 + m + i) - 1,$$
$$r_{\ell-i+1} \geq \frac{q^m - 1}{q^{m+i} - 1} n + \frac{q^{m+i} - q^m}{q^{m+i} - 1}(k_1 - m - i) + 1,$$

for all $m \in \{0, 1, \ldots, \ell - i\}$. Now, let

$$\mathrm{B_{Gr}}^{(m)}(n, q, \ell) = \frac{q^m - 1}{q^{m+1} - 1}(n + 2) + \frac{q^{m+1} - q^m}{q^{m+1} - 1}(\ell - 2m).$$

Then the threshold gap satisfies

$$g \geq \mathrm{B_{Gr}}^{(m)}(n, q, \ell),$$

for all $m \in \{0, 1, \ldots, \ell - 1\}$.

Proof:
For $r_{\ell-i+1}$ we combine (8) and (13) and obtain

$$r_{\ell-i+1} \geq n - \frac{q^{m+i} - q^m}{q^{m+i} - 1}(n - k_1 + i + m) + 1 \Leftrightarrow$$
$$r_{\ell-i+1} \geq \frac{q^m - 1}{q^{m+i} - 1} n + \frac{q^{m+i} - q^m}{q^{m+i} - 1}(k_1 - m - i) + 1.$$

Similarly the bound on t_i follows by combining (8) with (14).

In order to show the bound on g, we recall from (9) that

$$g = n + 2 - \left(M_1(C_1, C_2) + M_1(C_2^\perp, C_1^\perp)\right),$$

which by (13) and (14) yield

$$g \geq \frac{q^m - 1}{q^{m+1} - 1}(n + 2) + \frac{q^{m+1} - q^m}{q^{m+1} - 1}(\ell - 2m)$$

for all $m \in \{0, 1, \ldots, \ell - 1\}$. ■

One should notice that $g \geq \mathrm{B_{Gr}}^{(0)}(n, q, \ell)$ leads to the well-known bound $g \geq \ell$. Hence, for secret sharing schemes having $\ell = 1$, this bound on the threshold gap do not improve the existing bounds. However, when $\ell \geq 2$ we will show that there exist choices of m such that $\mathrm{B_{Gr}}^{(m)}(n, q, \ell)$ is at least as good, and in almost all cases, better than the bounds $\mathrm{B_{CCX(1)}}(n, q)$ and $\mathrm{B_{CCX(2)}}(n, q, \ell)$ in (12). We only consider $m = 0$, which imply $g \geq \ell$ as explained above, and $m = 1$, which imply the bound

$$g \geq \mathrm{B_{Gr}}^{(1)}(n, q, \ell) = \frac{q - 1}{q^2 - 1}(n + 2) + \frac{q^2 - q}{q^2 - 1}(\ell - 2)$$
$$= \frac{n + 2}{q + 1} + \frac{q}{q + 1}(\ell - 2).$$

One should notice that other choices of m could improve $\mathrm{B_{Gr}}^{(m)}(n, q, \ell)$, but in the following theorem we show that either $m = 0$ or $m = 1$ imply a bound which is at least as good as the known bounds.

Theorem 3.3: *Let $\ell \geq 2$, then*

$$\mathrm{B_{Gr}}^{(1)}(n,q,\ell) \geq \mathrm{B_{CCX(1)}}(n,q), \tag{15}$$

and

$$\begin{aligned} \mathrm{B_{Gr}}^{(0)}(n,q,\ell) &\geq \mathrm{B_{CCX(2)}}(n,q,\ell), \;\; \textit{when } \ell \geq n-2(q-1), \\ \mathrm{B_{Gr}}^{(1)}(n,q,\ell) &\geq \mathrm{B_{CCX(2)}}(n,q,\ell), \;\; \textit{when } \ell \leq n-2(q-1). \end{aligned} \tag{16}$$

Proof:
In order to prove (15) we consider the difference

$$\begin{aligned} \mathrm{B_{Gr}}^{(1)}(n,q,\ell) - \mathrm{B_{CCX(1)}}(n,q) &= \frac{n+2}{q+1} + \frac{q}{q+1}(\ell-2) - \frac{n+2}{2q-1} \\ &= \frac{q-2}{(q+1)(2q-1)}(n+2) + \frac{q}{q+1}(\ell-2) \\ &\geq 0, \end{aligned} \tag{17}$$

where the inequality holds for all n and q, since $\ell \geq 2$ and $q \geq 2$.

To prove (16) we start by considering the difference

$$\begin{aligned} \mathrm{B_{Gr}}^{(0)}(n,q,\ell) - \mathrm{B_{CCX(2)}}(n,q,\ell) &= \ell - \left(\frac{n+2}{2q+1} + \frac{2q}{2q+1}(\ell-1)\right) \\ &= \frac{\ell-n+2(q-1)}{2q+1}. \end{aligned}$$

This is greater than or equal to zero if

$$\ell \geq n-2(q-1).$$

Similarly, the difference $\mathrm{B_{Gr}}^{(1)}(n,q,\ell) - \mathrm{B_{CCX(2)}}(n,q,\ell)$ is greater than or equal to zero if

$$\begin{aligned} &0 \leq \frac{n+2}{q+1} + \frac{q}{q+1}(\ell-2) - \left(\frac{n+2}{2q+1} + \frac{2q}{2q+1}(\ell-1)\right) \Leftrightarrow \\ &0 \leq \frac{q}{(q+1)(2q+1)}(n-\ell+2) - \frac{2q^2}{(q+1)(2q+1)} \Leftrightarrow \\ &\ell \leq n-2(q-1), \end{aligned}$$

which proves (16). ■

Remark:
One should notice that the inequality in (17) is strict if $\ell > 2$ or if $\ell \geq 2$ and $q > 2$ showing that the bound $\mathrm{B_{Gr}}^{(1)}(n,q,\ell)$ is sharper in these cases. Similarly, if $\ell \neq n-2(q-1)$ and $\ell \geq 2$ there exists a choice of m such that $\mathrm{B_{Gr}}^{(m)}(n,q,\ell) > \mathrm{B_{CCX(2)}}(n,q,\ell)$.

In order to illustrate how much this new bound on the threshold gap improves the existing bounds we consider an example.

Example 3.5: Let $q = 2$, $n = 100$, and $\ell = 10$. Then the well-known bound $g \geq \ell$ yields $g \geq 10$. The bound $\mathrm{B}_{\mathrm{CCX}(1)}(100, 2)$ implies $g \geq 34$. Similarly, the bound $\mathrm{B}_{\mathrm{CCX}(2)}(n, q, \ell)$ implies $g \geq 28$, since we can round up because the threshold gap is an integer. However, for $m = 4$, which is the optimal value for m in this example, we have $\left\lceil {\mathrm{B}_{\mathrm{Gr}}}^{(4)}(100, 2, 10) \right\rceil = 51$. Hence, we conclude that a linear secret sharing scheme over $\mathbb{F}_2$ with 100 participants for sharing 10-bit long secrets has a threshold gap greater than or equal to 51. ◀

We return to the bounds in Theorem 3.2 in Section 5, where the bounds are considered asymptotic. Before that, we will focus on the bound $\mathrm{B}_{\mathrm{CCX}(1)}(n, q)$.

4 Further Bounds on the Partial Reconstruction thresholds

Now, we will consider the bound $g \geq \mathrm{B}_{\mathrm{CCX}(1)}(n, q)$ from [6] more in depth. This bound is obtained first by proving that $r \geq \frac{n}{q} + 1$ under the assumption that $t \geq 1$, later using shortening of secret sharing schemes to show $g \geq \frac{n-t+1}{q}$ (still assuming $t \geq 1$) and finally applying this bound to the scheme and its dual, which yields $g \geq \mathrm{B}_{\mathrm{CCX}(1)}(n, q)$ under the conditions $t \geq 1, r \leq n - 1$.

In this section we consider the first step of that argument (the one showing $r \geq \frac{n}{q} + 1$ if $t \geq 1$) and explore its generalization to the partial reconstruction and privacy thresholds when $\ell > 1$. First, we show that we can obtain the same bound on r but under a weaker assumption, $t_j \geq j$. Note that $t \geq 1$ implies $t_j \geq j$ for all j, since $t_j < t_{j+1}$ as mentioned in Section 2, but the converse is not necessarily true. Furthermore, we may extend the results to obtain bounds for the partial reconstruction thresholds as well. We will derive that

$$r_i \geq \frac{n}{q^{\ell-i+1}} + 1,$$

for $i \in \{j, j+1, \ldots, \ell\}$, if $t_j \geq j$. Notice that under the assumption $t \geq 1$ we obtain that $r_i \geq \frac{n}{q^{\ell-i+1}} + 1$, for all $1 \leq i \leq \ell$. Similarly, the result $r \geq \frac{n}{q} + 1$ holds even if we only assume that $t_\ell \geq \ell$. From these results on r_i we will also generalize the bound $g \geq \mathrm{B}_{\mathrm{CCX}(1)}(n, q)$ by using shortening of codes.

Before proving the new bound for partial reconstruction thresholds we shall consider Lemma 4.1 and introduce the following notation. For a subset $V \subseteq \mathbb{F}_q^n$, an element $a \in \mathbb{F}_q$, and an index $i \in \{1, \ldots, n\}$ define

$$(V)_{a,i} = \{\mathbf{v} \in V : \pi_i(\mathbf{v}) = a\}.$$

Note that if V is a linear code, where $(V)_{a,i} \neq \emptyset$ for some $a \neq 0$, then

$$|(V)_{a,i}| = |(V)_{b,i}| \tag{18}$$

for all $a, b \in \mathbb{F}_q$ by the linearity of V.

Lemma 4.1: *Let $C_2 \subsetneq C_1$ define a secret sharing scheme and assume that $t_j \geq j$ for some $j \in \{1, 2, \ldots, \ell\}$. Then there exists a set $W = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{\ell-j+1}\} \subseteq L$, such* *that the elements in W are linearly independent, and for all $m \in \{1, 2, \ldots, n\}$ and $k \in \{1, 2, \ldots, \ell - j + 1\}$, we either have that*

$$\pi_m(C_2) = \{0\} \text{ and } \pi_m(\mathbf{v}_k + C_2) = \{0\}$$

or

$$|(C_2)_{a,m}| = |(\mathbf{v}_k + C_2)_{a,m}| = q^{k_2 - 1}, \text{ for all } a \in \mathbb{F}_q.$$

Proof:
Let $B = \{m : \pi_m(C_2) = \{0\}\}$ and notice that $\pi_B(C_1) = \pi_B(L \oplus C_2) = \pi_B(L)$. For any $A \subseteq B$ we have that $I_q(S_0, \mathbf{S}_A) = \dim \pi_A(C_1) = \dim \pi_A(L) \leq \ell$. Now consider the homomorphism $\pi_B \colon L \to \mathbb{F}_q^{|B|}$, and assume that $\dim \pi_B(L) \geq j$. Then one can puncture the code $\pi_B(L)$ at a set A with cardinality j, such that $\dim \pi_A(L) = j$. This contradicts the assumption that $t_j \geq j$. Hence, $\dim \pi_B(L) < j$, which means that the kernel of π_B has dimension at least $\ell - j + 1$. Let W consists of $\ell - j + 1$ linearly independent vectors in this kernel.

let $m \in \{0, 1, \ldots, \ell - 1\} \setminus B$ and a $\mathbf{v}_k \in W$. By (18), $|(C_2)_{a - \pi_m(\mathbf{v}_k), m}| = q^{k_2 - 1}$, for all $a \in \mathbb{F}_q$. This shows that $|(\mathbf{v}_k + C_2)_{a,m}| \geq q^{k_2 - 1}$, for all $a \in \mathbb{F}_q$. However, since C_2 and $\mathbf{v}_k + C_2$ can be considered as quotient classes in C_1/C_2, we have that $|C_2| = |\mathbf{v}_k + C_2| = q^{k_2}$, implying that $|(\mathbf{v}_k + C_2)_{a,m}| = q^{k_2 - 1}$ for all $a \in \mathbb{F}_q$. ∎

We can now prove the aforementioned generalizations on r_i.

Theorem 4.2: *Let $C_2 \subsetneq C_1$ define a secret sharing scheme. If $t_j \geq j$ the thresholds r_i satisfy*

$$r_i \geq \frac{n}{q^{\ell - i + 1}} + 1,$$

for $i \in \{j, j + 1, \ldots, \ell\}$.

Proof:
By assumption $i \geq j$, implying that $\ell - i + 1 \leq \ell - j + 1$. Therefore, by Lemma 4.1 there exists $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{\ell - i + 1} \in L$ linearly independent vectors satisfying for all $m \in \{1, 2, \ldots, n\}$ and $k \in \{1, 2 \ldots, \ell - i + 1\}$, that $\pi_m(C_2) = \{0\}$ and $\pi_m(\mathbf{v}_k + C_2) = \{0\}$ or

$$|(C_2)_{a,m}| = |(\mathbf{v}_k + C_2)_{a,m}| = q^{k_2 - 1},$$

for all $a \in \mathbb{F}_q$. We define the vector space

$$V(\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_{\ell - i + 1}) = \langle \mathbf{v}_1 + \mathbf{r}_1, \mathbf{v}_2 + \mathbf{r}_2, \ldots, \mathbf{v}_{\ell - i + 1} + \mathbf{r}_{\ell - i + 1} \rangle,$$

for some vectors $\mathbf{r}_k$, and consider the sum

$$\sum_{\mathbf{r}_1 \in C_2} \sum_{\mathbf{r}_2 \in C_2} \cdots \sum_{\mathbf{r}_{\ell - i + 1} \in C_2} w_S(V(\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_{\ell - i + 1})).$$

Since $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{\ell - i + 1}$ are linearly independent, $\mathbf{r}_k \in C_2$, and $\mathbf{v}_k \in L$, for all k, the set $V(\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_{\ell - i + 1})$ is an $\ell - i + 1$ dimensional vector space in C_1 having only $\mathbf{0}$ in common with C_2. Therefore, we conclude that $w_S(V(\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_{\ell-i+1})) \geq M_{\ell-i+1}(C_1, C_2)$ and hence

$$\begin{aligned}&\sum_{\mathbf{r}_1\in C_2}\sum_{\mathbf{r}_2\in C_2}\cdots\sum_{\mathbf{r}_{\ell-i+1}\in C_2} w_S(V(\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_{\ell-i+1}))\\ &\geq q^{(\ell-i+1)k_2} M_{\ell-i+1}(C_1, C_2)\\ &= q^{(\ell-i+1)k_2}(n - r_i + 1),\end{aligned} \tag{19}$$

where the last equality follows from (8). Now notice that

$$w_S(V(\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_{\ell-i+1})) = \sum_{m=1}^{n} \dim \pi_m(V(\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_{\ell-i+1})),$$

which implies that

$$\begin{aligned}&\sum_{\mathbf{r}_1\in C_2}\sum_{\mathbf{r}_2\in C_2}\cdots\sum_{\mathbf{r}_{\ell-i+1}\in C_2} w_S(V(\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_{\ell-i+1})) =\\ &\sum_{\mathbf{r}_1\in C_2}\sum_{\mathbf{r}_2\in C_2}\cdots\sum_{\mathbf{r}_{\ell-i+1}\in C_2}\sum_{m=1}^{n} \dim \pi_m(V(\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_{\ell-i+1})) =\\ &\sum_{m=1}^{n}\sum_{\mathbf{r}_1\in C_2}\sum_{\mathbf{r}_2\in C_2}\cdots\sum_{\mathbf{r}_{\ell-i+1}\in C_2} \dim \pi_m(V(\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_{\ell-i+1})).\end{aligned}$$

In each term the dimension can either be zero or one. It is zero exactly when

$$\pi_m(\mathbf{r}_k) = -\pi_m(\mathbf{v}_k)$$

for all $k = 1, 2, \ldots, \ell - i + 1$. By the assumptions on $\mathbf{v}_k$, we have that $\pi_m(\mathbf{r}_k) = -\pi_m(\mathbf{v}_k)$ for at least q^{k_2-1} of the elements $\mathbf{r}_k \in C_2$ for a specific m. Since this holds for all $k = 1, 2, \ldots, \ell - i + 1$, we have that $\pi_m(\mathbf{r}_k) = -\pi_m(\mathbf{v}_k)$, for all k, at least $q^{(\ell-i+1)(k_2-1)}$ times. Hence,

$$\begin{aligned}&\sum_{m=1}^{n}\sum_{\mathbf{r}_1\in C_2}\sum_{\mathbf{r}_2\in C_2}\cdots\sum_{\mathbf{r}_{\ell-i+1}\in C_2} \dim \pi_m(V(\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_{\ell-i+1}))\\ &\leq \sum_{m=1}^{n} q^{(\ell-i+1)k_2} - q^{(\ell-i+1)(k_2-1)}\\ &= nq^{(\ell-i+1)k_2}\left(1 - q^{-(\ell-i+1)}\right)\end{aligned}$$

Combining this inequality with (19) we obtain that

$$\begin{aligned}q^{(\ell-i+1)k_2}(n - r_i + 1) \leq nq^{(\ell-i+1)k_2}\left(1 - q^{-(\ell-i+1)}\right) \Leftrightarrow\\ r_i \geq \frac{n}{q^{\ell-i+1}} + 1.\end{aligned}$$ ■

We first define the notion of shortening a secret sharing scheme and prove some results on the shortened schemes parameters before we prove the bounds on the threshold gap. Let $C_2 \subseteq C_1$ define a secret sharing scheme and let $A \subseteq \mathcal{I}^*$. Now define $\bar{A} = \mathcal{I}^* \setminus A$. Then the shortened secret sharing scheme is given by the code pair $C_2^A \subsetneq C_1^A$, where

$$C_i^A = \pi_{\bar{A}}(\ker \pi_A(C_i)).$$

Lemma 4.3: *Let $A \subseteq \mathcal{I}^*$ be a set of participants in the secret sharing scheme defined by $C_2 \subsetneq C_1$ such that $I_q(S_0, \mathbf{S}_A) = m$. Denote by ℓ^A the dimension of L^A, where L^A is a code such that $C_1^A = L^A \oplus C_2^A$. Additionally, denote by t_i^A and r_i^A the partial privacy and reconstruction thresholds of the shortened scheme $C_2^A \subsetneq C_1^A$, and let n^A be the length of the shortened codes. Then*

$$\begin{aligned} n^A &= n - |A|, \\ \ell^A &= \ell - m \\ t_i^A &\geq t_{i+m} - |A|, \\ r_i^A &\leq r_{i+m} - |A|, \end{aligned}$$

for all $i \in \{1, 2, \dots, \ell^A\}$.

Proof:
The result on n^A follows from the definition of $\pi_{\bar{A}}$. For ℓ^A we use Forney's first duality lemma [12], stating that for a code C,

$$\dim C = \dim \pi_A(C) + \dim C^A.$$

This leads to

$$\begin{aligned} \ell^A &= \dim C_1^A - \dim C_2^A \\ &= k_1 - \dim \pi_A(C_1) - k_2 + \dim \pi_A(C_2) \\ &= \ell - m. \end{aligned}$$

Now let $B \subseteq \bar{A}$ and notice, that knowing $|B|$ shares in the scheme $C_2^A \subsetneq C_1^A$ corresponds to knowing $|B \cup A| = |B| + |A|$ shares in the scheme $C_2 \subsetneq C_1$. However, for $B = \emptyset$, we have $I_q(S_0, \mathbf{S}_\emptyset) = 0$ in the shortened scheme, while it gives $I_q(S_0, \mathbf{S}_A) = m$ in the original scheme. So the information held by B in the shortened scheme equals $I_q(S_0, \mathbf{S}_{A \cup B}) - m$ in the original scheme.

If $|B| + |A| \leq t_{i+m}$, the participants will know at most $i + m - 1$ q-bits in the scheme $C_2 \subsetneq C_1$. This corresponds to knowing at most $i - 1$ q-bits in the shortened scheme, and hence $t_i^A \geq t_{i+m} - |A|$, for $i \in \{1, 2, \dots, \ell^A\}$.

Similarly for r_i^A, if $|B| + |A| \geq r_{i+m}$, the participants in B will know at least i q-bits in the shortened scheme, showing that $r_i^A \leq r_{i+m} - |A|$. ■

We will use the notation a_i and b_i to describe the gaps between t_i and t, and r and $r_{\ell-i+1}$, respectively. Therefore, denote by

$$\begin{aligned} a_i &= t_i - t - i + 1 \\ b_i &= r - r_{\ell-i+1} - i + 1. \end{aligned} \tag{20}$$

Since $t = t_1$, $r = r_\ell$, we have that $a_1 = b_1 = 0$. Using that t_i and r_i are strictly increasing with i we have that $a_i \geq 0$ and $b_i \geq 0$.

Another way to interpret a_i and b_i is to consider the t_i's and r_i's as a staircase. Two consecutive t_i's differ by at least one unit. The values a_i measure how different the sequence of t_i behaves from the case where all these steps $t_i' := t_i - t_{i-1}$ are exactly 1 (this happens in the Blakley-Meadows' scheme). Indeed $a_i - a_{i-1} = t_i - t_{i-1} - 1$. So if all steps t'_i are 1, then all a_i's are 0, and in general $a_i = \sum_{j=2}^{i}(t'_i - 1)$, the sum of "all deviations from 1" up to step i. An analogous relation holds with with r_i and b_i.

This also implies that a_i and b_i are non-decreasing with i, which is useful in the following theorem.

Theorem 4.4: *Let $C_2 \subsetneq C_1$ define a secret sharing scheme. Fix some $i \in \{1, 2, \ldots, \ell\}$ and let a_i and b_i be as in (20). If $t_i \geq i$, then the threshold gap g satisfies*

$$g \geq \frac{n-t+1}{q} + \frac{q-1}{q} a_i. \tag{21}$$

If $r_{\ell-i+1} \leq n-i$, then the threshold gap g satisfies

$$g \geq \frac{r+1}{q} + \frac{q-1}{q} b_i. \tag{22}$$

If both $t_i \geq i$ and $r_{\ell-i+1} \leq n-i$, then the threshold gap g satisfies

$$g \geq \frac{n+2}{2q-1} + \frac{q-1}{2q-1}(a_i + b_i).$$

Proof:
Choose A such that $|A| = t - 1 + a_i$. Hence, the shortened scheme given by $C_2^A \subsetneq \mathcal{C}_1^A$ has parameters $n^A = n - t + 1 - a_i$, $r^A \leq r - t + 1 - a_i$, and $t_i^A \geq i$ by Lemma 4.3. By Theorem 4.2 and Lemma 4.3, the threshold gap now satisfies

$$\begin{aligned} g = r - t &\geq r^A + a_i - 1 \\ &\geq \frac{n^A}{q} + a_i \\ &= \frac{n-t+1-a_i}{q} + a_i \\ &= \frac{n-t+1}{q} + \frac{q-1}{q} a_i. \end{aligned}$$

By (8) and (9) one has that the dual scheme has thresholds $t_i^\perp = n - r_{\ell-i+1}$ and $r_{\ell-i+1}^\perp = n - t_i$. Therefore, the threshold gap of the dual scheme is the same as for the original and a_i of the dual equals b_i. We can use the bound in (21) on the dual scheme if it holds that $t_i^\perp \geq i$, but this is equivalent to the assumption $r_{\ell-i+1} \leq n-i$. Therefore, we obtain

$$g \geq \frac{n-t^\perp+1}{q} + \frac{q-1}{q} b_i = \frac{r+1}{q} + \frac{q-1}{q} b_i.$$

The last bound is obtained by summing the bounds in (21) and (22).

$$\begin{aligned} 2g &\geq \frac{n-t+1+r+1}{q} + \frac{q-1}{q}(a_i+b_i) = \frac{n+g+2}{q} + \frac{q-1}{q}(a_i+b_i) \Leftrightarrow \\ g &\geq \frac{n+2}{2q-1} + \frac{q-1}{2q-1}(a_i+b_i). \end{aligned}$$

■

The bounds in [6], stating that

$$g \geq \frac{n-t+1}{q}, \quad g \geq \frac{r+1}{q}, \quad g \geq \mathrm{B}_{\mathrm{CCX}(1)}(n,q),$$

if $t \geq 1$ and $r \leq n-1$, are a particular case of this theorem.

In the following example we will consider a scheme attaining the bounds in Theorem 4.2. We will also note in which cases, for this particular example, the bounds from Theorem 4.4 are sharp. Similar examples of codes attaining the bound $g \geq \frac{n-t+1}{q}$ can be found in [21].

Example 4.5: Let $\mathbf{v}_1^T, \mathbf{v}_2^T, \ldots, \mathbf{v}_{q^\ell}^T$ be all possible vectors in $\mathbb{F}_q^\ell$, and define the code C_1 from the $(\ell+1) \times q^\ell$ generator matrix

$$G = \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_{q^\ell} \\ 1 & 1 & \cdots & 1 \end{bmatrix}$$

where C_2 is generated by the last all-one row. Then clearly $I_q(S_0, S_j) = 1 - 1 = 0$ by (7) for all $1 \leq j \leq n$, meaning that $t \geq 1$. In fact $t_i = i$ for all i in this example. This comes from the fact that the canonical basis vectors and the all zero vector lie in $\mathbb{F}_q^\ell$. The set of participants corresponding to these vectors is a set with cardinality $\ell + 1$, which can reconstruct all ℓ q-bits. Therefore, $t_\ell \leq \ell$, and from this we conclude $t_i = i$. Hence, we will show that the bounds in Theorem 4.2 are sharp for this secret sharing scheme, that is

$$r_i = \frac{n}{q^{\ell-i+1}} + 1 = \frac{q^\ell}{q^{\ell-i+1}} + 1 = q^{i-1} + 1.$$

We consider a set of participants A knowing $i-1$ q-bits, and derive that $|A| \leq q^{i-1}$, which means that $q^{i-1}+1$ participants will know at least i q-bits, and hence $r_i \leq q^{i-1}+1$. Combining this with Theorem 4.2 yields $r_i = q^{i-1}+1$.

Thus, assume that A knows $i-1$ q-bits and assume for contradiction that $|A| > q^{i-1}$. First notice that by (7), we have

$$\dim \pi_A(C_1) = i - 1 + \dim \pi_A(C_2) = i$$

On the other hand, we can determine the dimension of $\pi_A(C_1)$ in another way by considering the generator matrix. Let $A = \{j_1, j_2, \ldots, j_k\}$, where $k > q^{i-1}$. Denote by

$$G_A = \begin{bmatrix} \mathbf{v}_{j_1} & \mathbf{v}_{j_2} & \cdots & \mathbf{v}_{j_k} \\ 1 & 1 & \cdots & 1 \end{bmatrix}$$

and

$$G'_A = \begin{bmatrix} \mathbf{v}_{j_1} & \mathbf{v}_{j_2} & \cdots & \mathbf{v}_{j_k} \end{bmatrix}.$$

The rank of G_A equals $\dim \pi_A(C_1)$. Clearly, $\mathrm{rank}(G'_A) \leq \mathrm{rank}(G_A)$, but since $|A| > q^{i-1}$, we obtain $\mathrm{rank}(G'_A) = i$. This means that we have i linearly independent columns, and without loss of generality we denote these by $\mathbf{v}_{j_1}, \mathbf{v}_{j_2}, \ldots, \mathbf{v}_{j_i}$. Hence, all the columns in G'_A must be of the form

$$a_1 \mathbf{v}_{j_1} + a_2 \mathbf{v}_{j_2} + \cdots + a_i \mathbf{v}_{j_i},$$

for some $a_k \in \mathbb{F}_q$. However, since $\mathrm{rank}(G'_A) = \mathrm{rank}(G_A)$ one has that $\sum_{k=1}^{i} a_k = 1$. Therefore, $|A| \leq q^{i-1}$, contradicting the assumption on A.

From this we conclude that $r_i = q^{i-1} + 1$, showing that the bound in Theorem 4.2 is sharp for this example. The threshold gap in this example can also be determined; $g = r - t = q^{\ell-1} + 1 - 1 = q^{\ell-1}$. Now considering the bounds in Theorem 4.4 we show that some of these bounds are attained in this case as well. Since $t_i = i$, we have that $a_i = 0$ for all i in Theorem 4.4. Thus,

$$\frac{n-t+1}{q} = \frac{q^\ell - 1 + 1}{q} = q^{\ell-1} = g,$$

which shows that the inequality in (21) is sharp. We consider the inequality in (22) as well, and since b_i is non-decreasing we determine b_ℓ in order to make the bound as good as possible.

$$b_\ell = r - r_1 - \ell + 1 = q^{\ell-1} + 1 - 2 - \ell + 1 = q^{\ell-1} - \ell.$$

Hence, the bound states

$$\begin{aligned} g \geq \frac{r+1}{q} + \frac{q-1}{q} b_\ell &= \frac{q^{\ell-1}+2}{q} + \frac{q-1}{q}\left(q^{\ell-1} - \ell\right) \\ &= q^{\ell-1} - \ell + \frac{2+\ell}{q}. \end{aligned}$$

Note that there is no contradiction with $g = q^{\ell-1}$, since the bound does not hold for $\ell = 1$ and $q = 2$. When $\ell = 1$ we require, in order to use the bound, that $r \leq n - 1$, but $n = 2^1 = 2$ and $r = 2^{1-1} + 1 = 2$ in this case.

For this bound to be sharp $\ell = \frac{2+\ell}{q}$, which implies $\ell(q-1) = 2$. Therefore, this bound is attained in the case where $\ell = 2$ and $q = 2$. The same would then hold for the last bound in Theorem 4.4, since this bound is obtained by summing the two previous bounds. ◀

5 Asymptotic Comparisons

In this section we analyse the asymptotic behaviour of the bounds presented in Theorem 3.2 when the number of players n grows, and the size of the secret ℓ grows as a linear function of n.

We assume the setting considered in [14]; let $\{\Sigma_j\}_{j=1}^{\infty}$ denote an infinite family of $\mathbb{F}_q$-linear secret sharing schemes with increasing number of participants n_j and where Σ_j has secrets in $\mathbb{F}_q^{\ell_j}$, so that $\{\ell_j\}_{j=1}^{\infty}$ is a monotonely increasing sequence such that

$$\lim_{j\to\infty} \frac{\ell_j}{n_j} = L \text{ , for some } L \in \mathbb{R} \text{ with } 0 < L < 1.$$

To simplify, we assume that if we denote $k_1(j), k_2(j)$ the dimensions of the codes C_1 and C_2 in any nested code pair representation of $\{\Sigma_j\}$, then $\frac{k_1(j)}{n_j}$ converges to some $R_1 \in \mathbb{R}$ and $\frac{k_2(j)}{n_j}$ converges to some $R_2 \in \mathbb{R}$. Clearly, $L = R_1 - R_2$ since $\ell_j = k_1(j) - k_2(j)$.

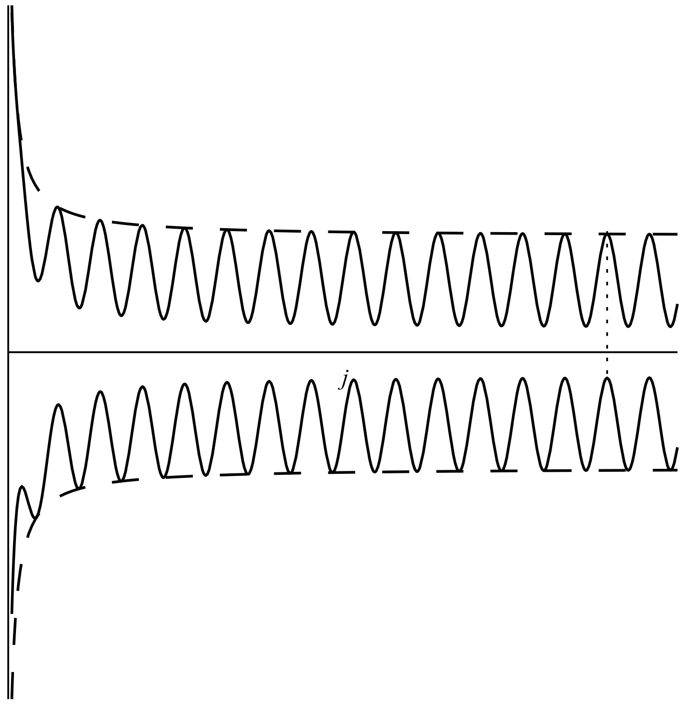

Figure 1: Illustration of $\Omega^{(3)}$. The solid lines illustrate $\frac{t(\Sigma_j)}{n_j}$ and $\frac{r(\Sigma_j)}{n_j}$, both as a function of j, and the black vertical dashed line illustrates $\frac{g(\Sigma_j)}{n_j}$ for a specific j.

Denote the privacy threshold and reconstruction threshold of Σ_j by $t(\Sigma_j)$ and $r(\Sigma_j)$ respectively. Furthermore, we define

$$\Omega^{(1)} = \liminf_{j\to\infty} \frac{t(\Sigma_j)}{n_j} \text{ and } \Omega^{(2)} = \limsup_{j\to\infty} \frac{r(\Sigma_j)}{n_j}.$$

Additionally, we denote the threshold gap of Σ_j by $g(\Sigma_j)$ and define

$$\Omega^{(3)} = \limsup_{j\to\infty} \frac{g(\Sigma_j)}{n_j}. \tag{23}$$

Note that $\Omega^{(3)}$ does not necessarily equal $\Omega^{(2)} - \Omega^{(1)}$. Indeed, in general we have

$$\Omega^{(3)} = \limsup_{j\to\infty} \left(\frac{r(\Sigma_j)}{n_j} - \frac{t(\Sigma_j)}{n_j} \right) \leq \limsup_{j\to\infty} \frac{r(\Sigma_j)}{n_j} - \liminf_{j\to\infty} \frac{t(\Sigma_j)}{n_j} = \Omega^{(2)} - \Omega^{(1)}. \tag{24}$$

but equality may not hold as the example illustrated in Figure 1 shows. The lower dashed line illustrates $\Omega^{(1)}$ and the top dashed line $\Omega^{(2)}$. As we can see in the figure, the difference between $\Omega^{(2)}$ and $\Omega^{(1)}$ is larger than the actual threshold gap, which is the black vertical dashed line.

We now present the asymptotic version of the bound $g \geq \mathrm{B_{Gr}}^{(m)}(n, q, \ell)$ together with bounds on $\Omega^{(1)}$ and $\Omega^{(2)}$.

Theorem 5.1: *Let $\{\Sigma_j\}$ be a family of secret sharing schemes over $\mathbb{F}_q$ as above. We have*

$$\begin{aligned}\Omega^{(1)} &\leq \frac{q-1}{q}R_2,\\ \Omega^{(2)} &\geq \frac{1}{q}+\frac{q-1}{q}R_1,\\ \Omega^{(3)} &\geq \frac{1}{q}+\frac{q-1}{q}L.\end{aligned} \tag{25}$$

Proof:
We have by Theorem 3.2 that

$$\begin{aligned}\frac{t(\Sigma_j)}{n_j} &\leq \frac{q^{m_j+1}-q^{m_j}}{q^{m_j+1}-1}\left(\frac{k_2(j)}{n_j}+\frac{m_j}{n_j}+\frac{1}{n_j}\right)-\frac{1}{n_j},\\ \frac{r(\Sigma_j)}{n_j} &\geq \frac{q^{m_j}-1}{q^{m_j+1}-1}+\frac{q^{m_j+1}-q^{m_j}}{q^{m_j+1}-1}\left(\frac{k_1(j)}{n_j}-\frac{m_j}{n_j}-\frac{1}{n_j}\right)+\frac{1}{n_j},\\ \frac{g(\Sigma_j)}{n_j} &\geq \frac{q^{m_j}-1}{q^{m_j+1}-1}\left(1+\frac{2}{n_j}\right)+\frac{q^{m_j+1}-q^{m_j}}{q^{m_j+1}-1}\left(\frac{\ell_j}{n_j}-2\frac{m_j}{n_j}\right)\end{aligned} \tag{26}$$

where m_j is any choice of m for Σ_j in Theorem 3.2, i.e. $m_j \in \{0,\ldots,\ell_j-1\}$. In particular we can choose m_j as a function of n_j such that $m_j = o(n_j)$ but still $\lim_{j\to\infty} m_j = \infty$, for example $m_j = \min\{\ell_j - 1, \lfloor \log n_j \rfloor\}$ (where $L > 0$ implies that for large enough j, we simply have $m_j = \lfloor \log n_j \rfloor$).

Letting j tend to infinity in (26) with such selection of m_j, we obtain the claimed result. ∎

It is not difficult to see that the bound

$$\Omega^{(3)} \geq \frac{1}{q}+\frac{q-1}{q}L$$

that we just derived is strictly tighter than the asymptotic versions of the bounds $g \geq \ell$, $\mathrm{B}_{\mathrm{CCX(1)}}(n,q)$, and $\mathrm{B}_{\mathrm{CCX(2)}}(n,q,\ell)$, which are respectively

$$\Omega^{(3)} \geq L,\ \Omega^{(3)} \geq \frac{1}{2q-1},\ \Omega^{(3)} \geq \frac{1}{2q+1}+\frac{2q}{2q+1}L,$$

for any q and any $0 < L < 1$. We show these four bounds on $\Omega^{(3)}$ in Figure 2 for the case $q = 2$.

In the rest of this section, we collect known results on upper bounds for $\Omega^{(3)}$, and compare them with the lower bounds we have obtained.

We will consider algebraic geometric codes and random codes. As far as the authors know, secret sharing schemes from algebraic geometric codes yield the smallest values of $\Omega^{(3)}$ when the finite field $\mathbb{F}_q$ is sufficiently large, while random codes give smaller $\Omega^{(3)}$ for small q.

An algebraic geometric evaluation code is defined from an algebraic function field F, a divisor G of F (which determines a space of functions to be evaluated) and a set of

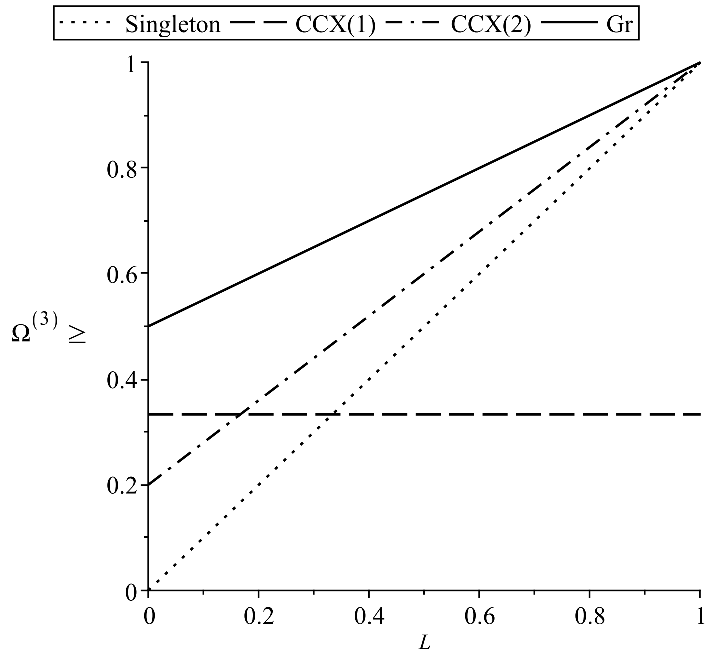

Figure 2: Comparison of asymptotic bounds on the threshold gap for $q = 2$.

rational places in F (as evaluation points), the latter usually represented by a divisor D. We remit the reader to [23] for details. Secret sharing schemes defined from algebraic geometric codes where first considered in [7]. We here use the construction from [9], defined by a nested code pair where both codes are algebraic geometric codes defined using the same function field F and the set of all rational places as evaluation points, but different divisors G_1, G_2. Such secret sharing schemes then satisfy $t \geq k_2 - \mathcal{G}$ and $r \leq k_1 + \mathcal{G}$, where $\mathcal{G}$ is the genus of the function field, and k_1, k_2 are as always the dimensions of the two linear codes. Moreover, the length of these codes (and hence the number of shares n) is the number of rational places of the function field.

Consider now an optimal tower of function fields $\{F_j\}_{j=1}^{\infty}$, i.e. $\lim_{j\to\infty} \frac{N_j}{\mathcal{G}_j} = A(q)$ where $N_j, \mathcal{G}_j$ are respectively the number of rational places and genus in F_j and $A(q)$ is the so-called Ihara's constant and $\mathcal{G}_j$ is the genus. Applying the construction described above gives a family of secret sharing schemes such that

$$\Omega^{(1)} \geq R_2 - \frac{1}{A(q)},$$
$$\Omega^{(2)} \leq R_1 + \frac{1}{A(q)},$$

see [14]. By (24) this implies

$$\Omega^{(3)} \leq L + \frac{2}{A(q)}. \tag{27}$$

While Ihara's constant $A(q)$ has not been determined for every q, we sum up some known facts next. First $A(q) > 0$ for all q, and in fact $A(q) \geq c\log(q)$ for some constant c, see for instance [20]. On the other hand, $A(q) \leq \sqrt{q} - 1$, see [24]. If q is a perfect square, it was shown in [16] that $A(q) = \sqrt{q} - 1$. Furthermore, Garcia and Stichtenoth gave a explicit construction [13] of an optimal tower of function fields in this case.

Consequently, for small values of q, the bound in (27) is trivial since $A(q) \leq 2$. For large enough q, however, we have $A(q) > 2$ (for example for q square with $q \geq 16$).

We observe the following, in relation with the lower bounds: the difference between the upper bound (27) and the lower bound from Theorem 5.1 is

$$\frac{2}{A(q)} - \frac{1}{q}(1 - L).$$

Note that the term $\frac{1}{q}(1 - L)$ is precisely what the bound in Theorem 5.1 has gained with respect to the lower bound $\Omega^{(3)} \geq L$. However this factor is overshadowed by the considerably larger factor $2/A(q)$. It is an interesting open question to bring these bounds together, by either proving stronger lower bounds or improving the known constructions.

For small finite fields, the bounds in (27) are trivial and the best upper bounds are achieved by inifinite families of secret sharing schemes based on random codes. We follow the results from [9]. The following result is a consequence of the fact that random codes are on the Gilbert-Varshamov bound.

Proposition 5.2: *Let* C *be a random variable with the uniform distribution taking values in the set of all* $[n, k]$ *linear codes over* $\mathbb{F}_q$*, and let* $0 < d, d^{\perp} < (1 - \frac{1}{q})n$ *be integers. For a realization of* $\mathrm{C} = C$ *we then have*

$$P(d_{\min}(C) < d) \leq q^{k+n(H_q(\frac{d}{n})-1)}$$
$$P(d_{\min}(C^{\perp}) < d^{\perp}) \leq q^{nH_q(\frac{d^{\perp}}{n})-k},$$

where $H_q(x) = x\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x)$ *is the* q*-ary entropy function.*

The q-ary entropy function H_q is strictly increasing and therefore injective in the interval $[0, 1 - \frac{1}{q}]$ (we define $H_q(0) = 0$ as usual) and there its image is the interval $[0, 1]$. We can therefore define the inverse $H_q^{-1} : [0, 1] \to [0, 1 - \frac{1}{q}]$. With this definition in mind, we can choose $\frac{d}{n} = H_q^{-1}(1 - \frac{k}{n} - \varepsilon')$ and $\frac{d^{\perp}}{n} = H_q^{-1}(\frac{k}{n} - \varepsilon')$ for some $\varepsilon' > 0$ and both probabilities above become lower than or equal to $q^{-\varepsilon' n}$.

A linear code C_1 can be chosen uniformly at random from all $[n, k_1]$ linear codes by rejection sampling of the elements $\mathbf{b}_i$ in its basis. The subcode $C_2 \subsetneq C_1$ generated by the last k_2 basis elements is then also uniformly random among all $[n, k_2]$ linear codes. Combining Proposition 5.2 and the comment below with the inequalities in (10), we obtain

$$\begin{aligned} P\left(\frac{r}{n} < 1 - H_q^{-1}\left(1 - \frac{k_1}{n} - \varepsilon'\right) + \frac{1}{n}\right) &\geq 1 - q^{-\varepsilon' n} \\ P\left(\frac{t}{n} > H_q^{-1}\left(\frac{k_2}{n} - \varepsilon'\right) - \frac{1}{n}\right) &\geq 1 - q^{-\varepsilon' n}, \end{aligned} \tag{28}$$

For any fixed $\varepsilon' > 0$ the probabilities in (28) are larger than 0, and hence by the probabilistic method we conclude that there exists an infinite family of secret sharing schemes with

$$\Omega^{(3)} \leq 1 - H_q^{-1}(1 - R_1 - \varepsilon') - H_q^{-1}(R_2 - \varepsilon').$$

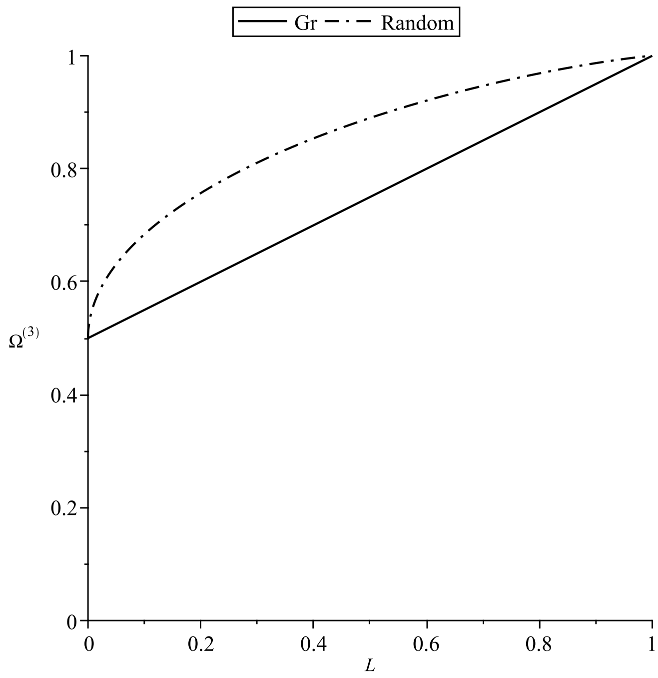

Figure 3: Comparison of asymptotic lower and upper bounds (when $R_1 = 1$) on the threshold gap for $q = 2$.

For a fixed $L = R_1 - R_2$, the smallest value of the right-hand side is attained by setting R_1 close to 1 (and hence R_2 close to $1 - L$) or, symmetrically, setting R_2 close to 0 (and $R_1 = L$). In that case, the inequality becomes

$$\Omega^{(3)} \leq 1 - H_q^{-1}(1 - L) + \varepsilon,$$

for any $\varepsilon > 0$.

In Figure 3, we compare this upper bound, in the case $q = 2$, with our lower bound from equation (25).

At last, we make the following remark on the asymptotic behaviors of the partial privacy and reconstruction thresholds, which is one of the main focus in the work [14]. There the authors define

$$\begin{aligned}\Lambda^{(1)}(\delta_1) = \sup \Bigg\{ \liminf_{j\to\infty} \frac{t_{m_1(j)}}{n_j} \Bigg| & \\ & \{m_1(j)\}_{j=1}^{\infty}, 1 \leq m_1(j) \leq \ell_j, \lim_{j\to\infty} \frac{m_1(j)}{n_j} = \delta_1 L \Bigg\},\\ \Lambda^{(2)}(\delta_2) = \inf \Bigg\{ \limsup_{j\to\infty} \frac{r_{\ell_j - m_2(j)+1}}{n_j} \Bigg| & \\ & \{m_2(j)\}_{j=1}^{\infty}, 1 \leq m_2(j) \leq \ell_j, \lim_{j\to\infty} \frac{m_2(j)}{n_j} = \delta_2 L \Bigg\}.\end{aligned}$$

That is, asymptotically, no fraction less than $\Lambda^{(1)}(\delta_1)$ of the participants holds more than a fraction of δ_1 of the secret. Similarly, $\Lambda^{(2)}(\delta_2)$ ensures that asymptotically a fraction of $\Lambda^{(2)}(\delta_2)$ of the participants will be able to reconstruct a fraction of $1 - \delta_2$ of the secret.

In [14] the gap between the limitations on $\Lambda^{(1)}(\delta_1)$ and $\Lambda^{(2)}(\delta_2)$ and what is possible to achieve is almost closed. The limitations considered there are derived from (11), i.e.,

$$\begin{aligned} \Lambda^{(1)}(\delta_1) &\leq R_2 + \delta_1 L, \\ \Lambda^{(2)}(\delta_2) &\geq R_1 - \delta_2 L. \end{aligned} \tag{29}$$

We can obtain the same bounds from Theorem 3.2 by setting $m = 0$. However, contrary to what happens in the proof of Theorem 5.1, choosing m as a small fraction of ℓ will not improve this bound in this case.

A Linear Secret Sharing

Proposition A.1: *A secret sharing scheme based on a nested code pair $C_2 \subseteq C_1$ is a linear secret sharing scheme.*

Proof:
Clearly, $\mathcal{S}_i$ is a $\mathbb{F}_q$-linear subspace. So we need to show that $\mathbf{S}$ is uniformly distributed on some subspace $V \subseteq \mathcal{S}_0 \times \mathcal{S}_1 \times \cdots \times \mathcal{S}_n$. Indeed, this is the case for

$$V = \{(\mathbf{s}, \mathbf{c}) : \mathbf{s} \in \mathbb{F}_q^\ell \quad \text{and} \quad \mathbf{c} \in (s_1\mathbf{b}_1 + s_2\mathbf{b}_2 + \cdots + s_\ell \mathbf{b}_\ell) + C_2\}.$$

First of all it is a subspace, so we show that $\mathbf{S}$ is uniformly distributed on V.

$$\begin{aligned} P(\mathbf{S} = (\mathbf{s}, c_1, c_2, \ldots, c_n)) &= P(\mathbf{S}_{\mathcal{I}^*} = (c_1, c_2, \ldots, c_n) | S_0 = \mathbf{s}) P(S_0 = \mathbf{s}) \\ &= \frac{1}{q^{k_2}} \frac{1}{q^\ell} \end{aligned}$$

for $\mathbf{S}$ in V, showing that this construction resulting in a linear secret sharing scheme. ■

Proposition A.2: *All linear secret sharing schemes can be represented by a nested code pair $C_2 \subsetneq C_1$.*

Proof:
Let a linear secret sharing scheme be given by $\mathbf{S}$. Let V be the subspace such that $\mathbf{S}$ is uniformly distributed on V, and define

$$\begin{aligned} C_2 &= \{\mathbf{c} : (\mathbf{0}, \mathbf{c}) \in V \text{ where } \mathbf{0} \in \mathcal{S}_0 \text{ and } \mathbf{c} \in \mathcal{S}_1 \times \mathcal{S}_2 \times \cdots \mathcal{S}_n\} \\ C_1 &= \{\mathbf{c} : (\mathbf{s}, \mathbf{c}) \in V \text{ where } \mathbf{s} \in \mathcal{S}_0 \text{ and } \mathbf{c} \in \mathcal{S}_1 \times \mathcal{S}_2 \times \cdots \mathcal{S}_n\} \end{aligned}$$

Clearly, $C_2 \subseteq C_1$ and both are linear subspaces and therefore linear codes. Denote by k_2 the dimension of C_2 and k_1 the dimension of C_1. Since both $\mathbf{S}$ and S_0 are uniformly distributed we also obtain that $\mathbf{S}|S_0 = \mathbf{0}$ is uniformly distributed on C_2 with probability function

$$p_{\mathbf{S}}(\mathbf{S}|S_0) = \frac{p_{\mathbf{S}}(\mathbf{S})}{p_{S_0}(S_0)} = \frac{\frac{1}{q^{k_1}}}{\frac{1}{q^\ell}} = \frac{1}{q^{k_1 - \ell}}.$$

Hence, $k_2 = k_1 - \ell$. Because all the shares uniquely determine the secret in a secret sharing scheme, there is a one-to-one correspondence between C_1 and V, showing that for any possible outcome of $\mathbf{S}$ there is a corresponding element in C_1. Therefore, we can represent the scheme using the nested codes $C_2 \subsetneq C_1$. ■

References

[1] Amos Beimel, Mike Burmester, Yvo Desmedt, and Eyal Kushilevitz. Computing functions of a shared secret. *SIAM J. Discrete Math.*, 13(3):324–345, 2000.

[2] G. R. Blakley and Catherine Meadows. Security of ramp schemes. *Advances in Cryptology: Proceedings of CRYPTO 84*, pages 242–268, 1985.

[3] Carlo Blundo, Alfredo De Santis, and Ugo Vaccaro. Efficient sharing of many secrets. *Proceedings of the 10th Annual Symposium on Theoretical Aspects of Computer Science*, pages 692–703, 1993.

[4] Carlo Blundo, Alfredo De Santis, and Ugo Vaccaro. On secret sharing schemes. *Inf. Process. Lett.*, 65(1):25–32, 1998.

[5] Andrej Bogdanov, Siyao Guo, and Ilan Komargodski. Threshold secret sharing requires a linear size alphabet. *Theory of Cryptography*, pages 471–484, 2016.

[6] Ignacio Cascudo, Ronald Cramer, and Chaoping Xing. Bounds on the threshold gap in secret sharing and its applications. *IEEE Transactions on Information Theory*, 59(9):5600–5612, September 2013.

[7] Hao Chen and Ronald Cramer. Algebraic geometric secret sharing schemes and secure multi-party computations over small fields. *Advances in Cryptology - CRYPTO 2006*, pages 521–536, August 2006.

[8] Hao Chen, Ronald Cramer, Robbert de Haan, and Ignacio Cascudo Pueyo. Strongly multiplicative ramp schemes from high degree rational points on curves. *Advances in Cryptology – EUROCRYPT 2008*, pages 451–470, 2008.

[9] Hao Chen, Ronald Cramer, Shafi Goldwasser, Robert de Haan, and Vinod Vaikuntanathan. Secure computation from random error correcting codes. *Advances in Cryptology - EUROCRYPT 2007*, pages 291–310, 2007.

[10] Ronald Cramer, Ivan Bjerre Damgård, Nico Döttling, Serge Fehr, and Gabriele Spini. Linear secret sharing schemes from error correcting codes and universal hash functions. *Advances in cryptology—EUROCRYPT 2015. Part II*, 9057:313–336, 2015.

[11] Ronald Cramer, Ivan Bjerre Damgård, and Jesper Buus Nielsen. *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press, 2015.

[12] George David Forney. Dimension/length profiles and trellis complexity of linear block codes. *IEEE International Symposium on Information Theory*, 40, November 1994.

[13] Arnaldo Garcia and Henning Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *Journal of Number Theory*, 61(2):248–273, 1996.

[14] Olav Geil, Stefano Martin, Umberto Martínez-Peñas, Ryutaroh Matsumoto, and Diego Ruano. On asymptotically good ramp secret sharing schemes. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E100.A(12):2699–2708, 2017.

[15] Olav Geil, Stefano Martin, Ryutaroh Matsumoto, Diego Ruano, and Yuan Luo. Relative generalized hamming weights of one-point algebraic geometric codes. *IEEE Transactions on Information Theory*, 60(10):5938–5949, October 2014.

[16] Yasutaka Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3):721–724 (1982), 1981.

[17] Joe Kilian and Noam Nisan. Unpublished result, 1991.

[18] Jun Kurihara, Tomohiko Uyematsu, and Ryutaroh Matsumoto. Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized hamming weight. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 95(11):2067–2075, 2012.

[19] Yuan Luo, Chaichana Mitrpant, A. J. Han Vinck, and Kefei Chen. Some new characters on the wire-tap channel of type ii. *IEEE Transactions on Information Theory*, 51(3):1222–1229, March 2005.

[20] Harald Niederreiter and Chaoping Xing. *Rational Points on Curves over Finite Fields: Theory and Applications.* Cambridge University Press, New York, NY, USA, 2001.

[21] Maura B. Paterson and Douglas R. Stinson. A simple combinatorial treatment of constructions and threshold gaps of ramp schemes. *Cryptography Commun.*, 5(4):229–240, December 2013.

[22] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, November 1979.

[23] Henning Stichtenoth. *Algebraic Function Fields and Codes.* Graduate Texts in Mathematics. Springer, 2 edition, 2009.

[24] S. G. Vlèduts and V. G. Drinfeld. The number of points of an algebraic curve. *Funktsional. Anal. i Prilozhen.*, 17(1):68–69, 1983.

[25] Zhuojun Zhuang, Yuan Luo, A. J. Han Vinck, and Bin Dai. Some new bounds on relative generalized hamming weight. *2011 IEEE 13th International Conference on Communication Technology*, pages 971–974, September 2011.