On asymptotically good ramp secret sharing schemes *

Olav Geil[†1], Stefano Martin[‡1], Umberto Martínez-Peñas[§1], Ryutaroh Matsumoto[¶1,2], and Diego Ruano[‖1]

[1]Department of Mathematical Sciences, Aalborg University
[2]Department of Information and Communications Engineering, Tokyo Institute of Technology

Abstract

Asymptotically good sequences of linear ramp secret sharing schemes have been intensively studied by Cramer et al. in terms of sequences of pairs of nested algebraic geometric codes [4, 5, 6, 7, 8, 10]. In those works the focus is on full privacy and full reconstruction. In this paper we analyze additional parameters describing the asymptotic behavior of partial information leakage and possibly also partial reconstruction giving a more complete picture of the access structure for sequences of linear ramp secret sharing schemes. Our study involves a detailed treatment of the (relative) generalized Hamming weights of the considered codes.

Keywords: Algebraic geometric codes, generalized Hamming weights, relative generalized Hamming weights, secret sharing.

1 Introduction

A secret sharing scheme [22, 2, 3, 27] is a cryptographic method to encode a secret $\mathbf{s}$ into multiple shares $c_1, \ldots, c_n$ so that only from specified subsets of the shares one can recover $\mathbf{s}$. Often it is assumed that n participants each receive a share,

no two different participants receiving the same. The secret and the share vector $\mathbf{c} = (c_1, \ldots, c_n)$ corresponding to it are assumed to be taken at random with some given distributions (usually uniform), and the recovery capability of a set of shares is measured from an information-theoretical point of view [27]. The term ramp secret sharing scheme [27, 3, 7] is used for those schemes where some sets of shares partially determine the secret, but not completely. This allows the shares to be of smaller size than the secret.

In this paper, we concentrate on linear ramp secret sharing schemes with uniform distribution on the secret and uniform distribution on the share vector conditioned to the secret, which is widely considered in the literature (see, for instance, [6, 7, 12, 17]). Here, the secret is a vector $\mathbf{s} \in \mathbb{F}_q^\ell$ (for some finite field $\mathbb{F}_q$), and we assume that the shares are elements $c_1, \ldots, c_n \in \mathbb{F}_q$. The term linear means that a linear combination of share vectors is a share vector of the corresponding linear combination of secrets. In [7, Sec. 4.2] it was shown that such schemes are equivalent to the following construction based on two nested linear codes $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ with $\dim C_1 - \dim C_2 = \ell$. Writing $k_2 = \dim C_2$ and $k_1 = \dim C_1$ (and consequently $\ell = k_1 - k_2$) let $\{\mathbf{b}_1, \ldots, \mathbf{b}_{k_2}\}$ be a basis for C_2 and extend it to a basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_{k_1}\}$ for C_1. A secret $\mathbf{s} = (s_1, \ldots, s_\ell)$ is encoded by first choosing at random coefficients $a_1, \ldots, a_{k_2} \in \mathbb{F}_q$ and then letting the share vector be

$$\mathbf{c} = a_1 \mathbf{b}_1 + \cdots + a_{k_2} \mathbf{b}_{k_2} + s_1 \mathbf{b}_{k_2+1} + \cdots + s_\ell \mathbf{b}_{k_1}. \tag{1}$$

Define a q-bit of information to be $\log_2(q)$ bits of information. Then, for the schemes that we consider, the mutual information between the secret and a set of shares is an integer between 0 and ℓ if measured in q-bits [17, Proof of Th. 4]. Therefore, for each $m = 1, \ldots, \ell$, we may define the following threshold values [12, Def. 2]:

- The m-th privacy threshold of the scheme is the maximum integer t_m such that from no set of t_m shares one can recover m q-bits of information about the secret. That is, $t_m = \max\{\#J \mid J \subseteq \{1, \ldots, n\}, I(J) < m\}$, where $I(J) = I\big(s_1, \ldots, s_\ell ; (c_i \mid i \in J)\big)$. Here, c_i is the i-th component of $\mathbf{c}$ in (1), and $I(;)$ is the mutual information taking logarithms in base q.

- The m-th reconstruction threshold of the scheme is the minimum integer r_m such that from any set of r_m shares one can obtain m q-bits of information about $\mathbf{s}$. That is, $r_m = \min\{\#J \mid J \subseteq \{1, \ldots, n\}, I(J) \geq m\}$.

The numbers $t = t_1$ and $r = r_\ell$ have been intensively studied in the literature, e.g. [3, 7, 27], where they are called privacy and reconstruction threshold, respectively. Clearly t is the greatest number such that no set of t shares holds any information on the secret and r is the smallest number such that from any set of r shares one can reconstruct the information in full. In a series of papers the asymptotic behavior of such parameters has been investigated [4, 5, 6, 7, 8, 10] in terms of corresponding infinite sequences of nested code pairs of increasing length. In the present paper we take a particular interest in sequences of nested code pairs $(C_2(i) \subsetneq C_1(i) \subset \mathbb{F}_q^{n_i})_{i=1}^\infty$

with n_i and with $\ell_i = \dim C_1(i) - \dim C_2(i)$ satisfying

$$\lim_{i \to \infty} n_i = \infty, \quad \text{and} \quad \liminf_{i \to \infty}(\ell_i/n_i) = L \qquad (2)$$

for some fixed $0 < L < 1$, see [4, 5, 6, 7, 8, 10]. The reason for us to require (2) is to obtain a constant information rate. For instance if the schemes are to be used in connection with distributed storage as mentioned in [27] then a memory of size $1/L$ times the information size is enough. As in the above listed papers the focus in on full privacy and full reconstruction, what is studied there is

$$\liminf_{i \to \infty} \frac{t}{n_i} = \Omega^{(1)} \quad \text{and} \quad \limsup_{i \to \infty} \frac{r}{n_i} = \Omega^{(2)}. \qquad (3)$$

Here, t and r are the privacy and reconstruction thresholds for the schemes based on $C_2(i) \subsetneq C_1(i) \subset \mathbb{F}_q^{n_i}$, and thereby are functions in i. For any chosen value of L and corresponding feasible $\Omega^{(1)}$ it is desirable to have the threshold gap $\Omega^{(2)} - \Omega^{(1)}$ as small as possible. One way of achieving this [4, 5, 6, 7, 8, 10] is to base the secret sharing schemes on sequences of nested code pairs related to an optimal tower of function fields and to require $\lim_{i\to\infty}(\dim C_1(i)/n_i) = R_1$ and $\lim_{i\to\infty}(\dim C_2(i)/n_i) = R_2$ for some fixed rates $R_1 > R_2$. Using the Goppa bound [15] one then obtains good parameters $L = R_1 - R_2$, $\Omega^{(2)}$ and $\Omega^{(1)}$. For future reference we formalize the concept of asymptotic goodness in a definition, where for completeness we also include the case $L = 0$, although we do not study this case in the present paper.

Definition 1. Let $0 < R_2 \leq R_1 < 1$ and consider a sequence of nested codes $(C_2(i) \subsetneq C_1(i) \subset \mathbb{F}_q^{n_i})_{i=1}^{\infty}$ with $n_i \to \infty$, $\dim C_2(i)/n_i \to R_2$ and $\dim C_1(i)/n_i \to R_1$ for $i \to \infty$. The corresponding sequence of linear ramp secret sharing schemes is said to be asymptotically good if the parameters from (3) satisfy $0 < \Omega^{(1)}$ and $\Omega^{(2)} < 1$.

The purpose of the present paper is to provide additional information on the access structure of sequences of linear ramp secret sharing schemes by studying partial information leakage and partial reconstruction parameters. More precisely, given a sequence of linear ramp secret sharing schemes and any fixed numbers $0 \leq \varepsilon_1, \varepsilon_2 \leq 1$ we study the asymptotic parameters

$$
\begin{aligned}
\Lambda^{(1)}(\varepsilon_1) &= \sup \Big\{ \liminf_{i \to \infty} \frac{t_{m_1(i)}}{n_i} \mid (m_1(i))_{i=1}^{\infty} \text{ satisfies} \\
&\qquad 1 \leq m_1(i) \leq \ell_i, \lim_{i \to \infty}(m_1(i)/n_i) = \varepsilon_1 L \Big\}, \\
\Lambda^{(2)}(\varepsilon_2) &= \inf \Big\{ \limsup_{i \to \infty} \frac{r_{\ell_i - m_2(i)+1}}{n_i} \mid (m_2(i))_{i=1}^{\infty} \text{ satisfies} \\
&\qquad 1 \leq m_2(i) \leq \ell_i, \lim_{i \to \infty}(m_2(i)/n_i) = \varepsilon_2 L \Big\}.
\end{aligned}
$$

Such parameters tell us that asymptotically no fraction less than $\Lambda^{(1)}(\varepsilon_1)$ of the shares holds more information on the secret than a fraction ε_1. Similarly, from any fraction greater than $\Lambda^{(2)}(\varepsilon_2)$ of the shares one can gain information on the secret

corresponding to a fraction $1 - \varepsilon_2$ or more. Of particular interest is $\Lambda^{(1)}(0)$ which ensures almost full privacy. It is a surprising fact that for secret sharing schemes based on algebraic geometric codes this number can be significantly larger than $\Omega^{(1)}$, meaning that such schemes are more secure than anticipated (see Section 3 and Theorem 21). The situation is similar with regards to reconstruction. In another direction, for fixed values of L and corresponding feasible $\Lambda^{(1)}(\varepsilon_1)$ we determine for the general class of ramp secret sharing schemes the smallest value $\Lambda^{(2)}(\varepsilon_2)$ such that a sequence of codes with these parameters exists. This bound – which can be seen as an asymptotic Singleton bound for linear ramp secret sharing schemes – is then by a non-constructive proof shown to be achievable, but unfortunately, we obtain no information regarding $\Omega^{(1)}$ and $\Omega^{(2)}$ for those sequences.

Sequences of linear ramp secret sharing schemes based on algebraic geometric codes defined from optimal towers of function fields are interesting for the following three reasons. Firstly, for such sequences the parameters L, $\Omega^{(1)}$ and $\Omega^{(2)}$ are simultaneously good. Also $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$ are good, although they do not always reach the Singleton bound. Secondly, such sequences are constructible if q is a perfect square and are semi-constructible if not. Finally, as demonstrated in [4, 5, 6, 7, 8, 10] examples of such sequences are important in connection with secure multiparty computation due to nice properties on the componentwise product of share vectors.

Our analysis of the asymptotic secret sharing parameters is based on the material in [12, 17] which translates information-theoretical properties of a ramp secret sharing scheme based on nested linear codes $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ into coding-theoretical properties of the nested codes. In particular, bounding generalized Hamming weights [26] of C_1 and $C_2^\perp$ and relative generalized Hamming weights [18] of the pairs $C_2 \subsetneq C_1$ and $C_1^\perp \subsetneq C_2^\perp$ implies bounds on the privacy and reconstruction numbers t_i and r_i.

The paper is organized as follows. In Section 2 we give the Singleton bound for linear ramp secret sharing schemes. Using the material from A we then show that for arbitrary L, sequences of schemes exist such that for arbitrary $\varepsilon_1, \varepsilon_2$ one gets arbitrarily close to the Singleton bound for $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$. In Section 3 we then discuss how to obtain sequences of ramp secret sharing schemes with good values of L, $\Omega^{(1)}$ and $\Omega^{(2)}$ from optimal towers of function fields. As a preparation step to treat later in the paper $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$ for these sequences of schemes we next study relative generalized Hamming weights of algebraic geometric codes in Section 4 and derive asymptotic consequences in Section 5. Then finally in Section 6 we collect our findings into information on $\Omega^{(1)}$, $\Omega^{(2)}$, $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$ for sequences of ramp secret sharing schemes based on algebraic geometric codes coming from optimal towers of function fields.

2 The Singleton bound

The code parameters governing the privacy and reconstruction numbers t_m and r_m of linear ramp secret sharing schemes are the relative generalized Hamming weights [18] which we now define together with the generalized Hamming weights [26].

Definition 2. Consider $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ and let $\ell = k_1 - k_2$ where $k_1 = \dim C_1$ and $k_2 = \dim C_2$. For $m = 1, \ldots, \ell$ the m-th relative generalized Hamming weight (RGHW) is:

$$
\begin{aligned}
M_m(C_1, C_2) \;=\; \min\{ &\#\mathrm{Supp}(D) \mid D \subset C_1 \text{ is a linear space} \\
&\text{with } \dim(D) = m \text{ and } D \cap C_2 = \{\mathbf{0}\}\},
\end{aligned}
$$

where $\mathrm{Supp}(D) = \{i \in \{1, 2, \ldots, n\} \mid \exists \mathbf{d} \in D, d_i \neq 0\}$. For $m = 1, 2, \ldots, k_1$, the m-th generalized Hamming weight (GHW) of C_1 is defined as $d_m(C_1) = M_m(C_1, \{\mathbf{0}\})$.

Clearly, the RGHWs can be lower bounded by the GHWs of the same index, and as the latter are often easier to estimate we shall also take an interest in them. The following theorem, which is [12, Th. 3], gives a characterization of the threshold numbers t_m and r_m in terms of the RGHWs of the pairs $C_2 \subsetneq C_1$ and $C_1^\perp \subsetneq C_2^\perp$, where $C^\perp$ denotes the dual of the linear code C.

Theorem 3. *Consider a linear ramp secret sharing scheme based on codes $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$. Then for $m = 1, 2, \ldots, \ell$,*

$$
\begin{aligned}
t_m &= M_m(C_2^\perp, C_1^\perp) - 1, \ and \\
r_m &= n - M_{\ell-m+1}(C_1, C_2) + 1.
\end{aligned}
$$

Observe, that as a consequence we obtain $t_m \geq d(C_2^\perp) - 1$ and $r_m \leq n - d_{\ell-m+1}(C_1) + 1$. Given a sequence of linear ramp secret sharing schemes satisfying (2), numbers $0 \leq \varepsilon_1, \varepsilon_2 \leq 1$ and any two sequences $(m_1(i))_{i=1}^\infty$ and $(m_2(i))_{i=1}^\infty$ with $\lim_{i \to \infty}(m_1(i)/n_i) \to \varepsilon_1 L$ and $\lim_{i \to \infty}(m_2(i)/n_i) \to \varepsilon_2 L$ we then obtain

$$
\Omega^{(1)} \;=\; \liminf_{i \to \infty} \frac{M_1(C_2^\perp, C_1^\perp)}{n_i} \geq \liminf_{i \to \infty} \frac{d(C_2^\perp)}{n_i} \tag{4}
$$

$$
\Omega^{(2)} \;=\; 1 - \liminf_{i \to \infty} \frac{M_1(C_1, C_2)}{n_i}
$$

$$
\leq \; 1 - \liminf_{i \to \infty} \frac{d(C_1)}{n_i} \tag{5}
$$

$$
\Lambda^{(1)}(\varepsilon_1) \;\geq\; \liminf_{i \to \infty} \frac{M_{m_1(i)}(C_2^\perp, C_1^\perp)}{n_i} \tag{6}
$$

$$
\geq \; \liminf_{i \to \infty} \frac{d_{m_1(i)}(C_2^\perp)}{n_i} \tag{7}
$$

$$
\Lambda^{(2)}(\varepsilon_2) \;\leq\; 1 - \liminf_{i \to \infty} \frac{M_{m_2(i)}(C_1, C_2)}{n_i} \tag{8}
$$

$$
\leq \; 1 - \liminf_{i \to \infty} \frac{d_{m_2(i)}(C_1)}{n_i} \tag{9}
$$

To study the optimality of linear ramp secret sharing schemes we recall the Singleton bound [18, Section IV] for a linear code pair $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ and its dual pair $C_1^\perp \subsetneq C_2^\perp \subset \mathbb{F}_q^n$: for each $m = 1, 2, \ldots, \ell$,

$$
M_m(C_1, C_2) \leq n - k_1 + m, \quad \text{and} \quad M_m(C_2^\perp, C_1^\perp) \leq k_2 + m. \tag{10}
$$

From these bounds and Theorem 3, it follows that $r_m \geq k_2 + m$ and $t_m \leq k_2 + m - 1$, and as a consequence

$$\Omega^{(2)} - \Omega^{(1)} \geq L \tag{11}$$

and

$$\Lambda^{(2)}(\varepsilon_2) - \Lambda^{(1)}(\varepsilon_1) \geq L(1 - \varepsilon_1 - \varepsilon_2). \tag{12}$$

There exist choices of $\Omega^{(1)} < \Omega^{(2)}$ such that (11) is not nearly tight, meaning that L cannot be close to $\Omega^{(2)} - \Omega^{(1)}$ [4, Th. 3.26, Th. 4.6]. It is therefore surprising that for any fixed value of $\Lambda^{(1)}(0) < \Lambda^{(2)}(0)$ there exist sequences of linear ramp secret sharing schemes with L arbitrarily close to $\Lambda^{(2)}(0) - \Lambda^{(1)}(0)$. Even more, by the strict monotonicity of RGHWs [18, Pro. 2], for such schemes $L(1 - \varepsilon_1 - \varepsilon_2)$ becomes arbitrarily close to $\Lambda^{(2)}(\varepsilon_2) - \Lambda^{(1)}(\varepsilon_1)$ for all $0 \leq \epsilon_1, \epsilon_2 \leq 1$. Our proof is non-constructive, as might be expected, and it unfortunately does not reveal any non-trivial information on the corresponding values of $\Omega^{(1)}$ and $\Omega^{(2)}$. We leave it for further research to determine simultaneous information on these parameters, and in particular to decide if the sequences fulfill the requirements in Definition 1 for being asymptotically good. In A we prove the following result:

Theorem 4. *For $0 \leq R_2 < R_1 \leq 1$, $0 \leq \delta \leq 1$, $0 \leq \delta^\perp \leq 1$, $0 < \tau \leq \min\{\delta, R_1 - R_2\}$ and $0 < \tau^\perp \leq \min\{\delta^\perp, R_1 - R_2\}$, if*

$$R_1 + \delta < 1 + \tau \quad and \quad (1 - R_2) + \delta^\perp < 1 + \tau^\perp, \tag{13}$$

then for any prime power q there exists an infinite sequence of nested linear code pairs $C_2(i) \subsetneq C_1(i) \subset \mathbb{F}_q^{n_i}$, where $n_i \to \infty$ for $i \to \infty$, and where

$$\lim_{i \to \infty} \frac{\dim(C_1(i))}{n_i} = R_1,$$

$$\lim_{i \to \infty} \frac{\dim(C_2(i))}{n_i} = R_2,$$

$$\liminf_{i \to \infty} \frac{M_{\lceil n_i \tau \rceil}(C_1(i), C_2(i))}{n_i} \geq \delta, \quad and$$

$$\liminf_{i \to \infty} \frac{M_{\lceil n_i \tau^\perp \rceil}(C_2(i)^\perp, C_1(i)^\perp)}{n_i} \geq \delta^\perp.$$

As a corollary we see that the difference in (12) can become arbitrarily close to zero.

Corollary 5. *For any $0 < R_2 < R_1 < 1$ there exists a sequence of linear ramp secret sharing schemes satisfying (2) with $L = R_1 - R_2$ and having simultaneous $\Lambda^{(1)}(\varepsilon_1)$ arbitrarily close to $R_2 + \varepsilon_1 L$ and $\Lambda^{(2)}$ arbitrarily close to $R_1 - \varepsilon_2 L$ for all $0 \leq \varepsilon_1, \varepsilon_2 \leq 1$.*

Proof. As noted prior to Theorem 4 by the strict monotonicity of the RGHWs it is enough to prove $L = R_1 - R_2$ and that $\Lambda^{(1)}(0)$ can be arbitrarily close to R_2 simultaneously with $\Lambda^{(2)}(0)$ being arbitrarily close to R_1. We start by proving a result which at a first glance seems weaker – but from which the above will follow. Let $0 < \varepsilon \leq \min\{R_1/L, (1-R_2)/L\}$ and choose arbitrarily small $\mu > 0$. In Theorem 4 choose $\tau = \tau^\perp = \varepsilon L$, $\delta = 1 - R_1 + \varepsilon L - \mu$ and $\delta^\perp = R_2 + \varepsilon L - \mu$. By inspection all the conditions of the theorem are satisfied and therefore by (6) and (8) for any ε in the considered interval there exists a sequence of linear ramp secret sharing schemes satisfying (2) such that $\Lambda^{(1)}(\varepsilon)$ is arbitrarily close to $R_2 + \varepsilon L$ simultaneously with $\Lambda^{(2)}(\varepsilon)$ being arbitrarily close to $R_1 - \varepsilon L$. The theorem finally follows by considering a sequence of numbers $(\varepsilon(i))_{i=1}^\infty$ between 0 and $\min\{R_1/L, (1-R_2)/L\}$ and with $\lim_{i\to\infty} \varepsilon(i) = 0$. For each $\varepsilon(i)$ we have a sequence $\mathcal{S}(i)$ of secret sharing schemes as described above. Now build a new sequence of schemes in which the i-th scheme is the i-th scheme from the sequence $\mathcal{S}(i)$. The resulting scheme satisfies the requirement mentioned at the beginning of the proof. $\qquad\square$

3 Asymptotically good sequences of schemes from algebraic geometric codes

In the remaining part of the paper we concentrate on ramp secret sharing schemes defined from pairs of nested algebraic geometric codes. In the present section we collect known information to describe what is possible concerning the parameters L, $\Omega^{(1)}$ and $\Omega^{(2)}$. In subsequent sections we then derive information on $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$.

Let $\mathcal{F}$ be an algebraic function field over $\mathbb{F}_q$ of transcendence degree one. In the rest of the paper we consider divisors $D = P_1 + \cdots + P_n$ and G with disjoint supports, where the places P_i are rational and pairwise distinct. For any divisor E, we define the Riemann-Roch space $\mathcal{L}(E)$ of functions $f \in \mathcal{F}$ such that the divisor $(f) + E$ is effective (see also [15, Def. 2.36]). We denote by $C_\mathcal{L}(D, G)$ the evaluation code of length n obtained by evaluating functions $f \in \mathcal{L}(G)$ in the places P_i. An algebraic geometric code is a code of the form $C_\mathcal{L}(D, G)$ or $C_\mathcal{L}(D, G)^\perp$. We call the first primary algebraic geometric codes and the latter dual. The well-known Goppa bound [15, Th. 2.65] gives information on the relation between dimension and minimum distance for primary or dual codes.

Theorem 6. *Let C be an algebraic geometric code of dimension k defined from a function field of genus g. Then the minimum distance satisfies $d(C) \geq n - k + 1 - g$.*

Given a function field $\mathcal{F}$, we shall write $N(\mathcal{F})$ for its number of rational places and $g(\mathcal{F})$ for its genus. For asymptotic purposes, we will make use of Ihara's constant [16]

$$A(q) = \limsup_{g(\mathcal{F})\to\infty} \frac{N(\mathcal{F})}{g(\mathcal{F})},$$

where the limit is taken over all function fields over $\mathbb{F}_q$ of genus $g(\mathcal{F}) > 0$. The Drinfeld-Vlăduţ bound [25] states that

$$A(q) \leq \sqrt{q} - 1. \tag{14}$$

As is well-known $A(q)$ is always strictly positive and equality in (14) holds if q is a perfect square [16]. See [1] for the status on what is known about $A(q)$ for q being a non-square. For convenience, we give the following definition:

Definition 7. A tower of function fields $(\mathcal{F}_i)_{i=1}^{\infty}$ over $\mathbb{F}_q$ is optimal if $N(\mathcal{F}_i) \to \infty$ and $N(\mathcal{F}_i)/g(\mathcal{F}_i) \to A(q)$ for $i \to \infty$. On the other hand, $(C_i)_{i=1}^{\infty}$ is an optimal sequence of one-point algebraic geometric codes defined from $\mathcal{F}_i$ if $n_i/N(\mathcal{F}_i) \to 1$ for $i \to \infty$, where n_i is the length of C_i.

The above together with (4) and (5) immediately combine into the following result concerning the existence of asymptotically good sequences of ramp secret sharing schemes.

Theorem 8. Let $(C_2(i) \subsetneq C_1(i) \subset \mathbb{F}_q^{n_i})_{i=1}^{\infty}$ be a sequence of nested algebraic geometric codes defined from an optimal tower of function fields and satisfying $n_i = N(\mathcal{F}_i) - 1$, $\dim C_1(i)/n_i \to R_1$ and $\dim C_2(i)/n_i \to R_2$ for some $0 < R_2 \leq R_1 < 1$. Then the corresponding sequence of linear ramp secret sharing schemes (see Section 1) satisfies $\Omega^{(1)} \geq R_2 - \frac{1}{A(q)}$ and $\Omega^{(2)} \leq R_1 + \frac{1}{A(q)}$.

In particular we obtain asymptotically good ramp secret sharing schemes (Definition 1) if $\frac{1}{A(q)} < R_2 \leq R_1 < 1 - \frac{1}{A(q)}$. If moreover $R_2 < R_1$ then also the crucial requirement (2) is satisfied. Observe that due to the assumption $n_i = N(\mathcal{F}_i) - 1$ we may choose the codes in Theorem 8 as one-point codes, meaning that without loss of generality we may consider codes of the form $C_2(i) = C_{\mathcal{L}}(D, \mu_2(i)Q)$ and $C_1(i) = C_{\mathcal{L}}(D, \mu_1(i)Q)$, where D is the sum of n_i distinct rational places in $\mathcal{F}_i$ and Q is another rational place in the same function field.

4 RGHWs and GHWs of algebraic geometric codes

In this section, we give non-asymptotic analysis that are necessary in Sections 5 and 6 to treat the parameters $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$ of the sequences of algebraic geometric schemes discussed in the previous section. The next theorem combines [15, Th. 2.65], [24, Th. 4.3, Cor. 4.2] and [26, Th. 1]. The first part which is a generalization of Theorem 6 is known as the Goppa bound for GHWs.

Theorem 9. Let C be an algebraic geometric code of dimension k defined from a function field of genus g. Then $d_m(C) \geq n - k + m - g$, for $1 \leq m \leq g$, and $d_m(C) = n - k + m$, for $g + 1 \leq m \leq k$.

For algebraic geometric codes $C_2 \subsetneq C_1$, the above theorem exactly gives $d_m(C_1)$ and $M_m(C_1, C_2)$ when $g < m$. In Proposition 12 and Proposition 13 below, we will improve it in the case $m \leq g$ for one-point codes. From now on we will concentrate on one-point algebraic geometric codes. That is, codes $C_{\mathcal{L}}(D, G)$ or $C_{\mathcal{L}}(D, G)^{\perp}$, where $G = \mu Q$, Q is a rational place and $\mu \geq -1$. Writing ν_Q for the valuation at Q, the Weierstrass semigroup corresponding to Q is

$$H(Q) = -\nu_Q \left(\bigcup_{\mu=0}^{\infty} \mathcal{L}(\mu Q) \right) = \{\mu \in \mathbb{N}_0 \mid \mathcal{L}(\mu Q) \neq \mathcal{L}((\mu - 1)Q)\}.$$

As is well-known, the number of missing positive numbers in $H(Q)$ equals the genus g of the function field. The conductor c is by definition the smallest element in $H(Q)$ such that all integers greater than or equal to that number belong to the set. The following lemma is well-known [15, Th. 2.65]:

Lemma 10. *For $\mu \geq -1$, $k = \dim C_{\mathcal{L}}(D, \mu Q)$ satisfies:*

- $k \geq \mu + 1 - g$ *if $\mu \leq 2g - 2$,*

- $k = \mu + 1 - g$ *if $2g - 2 < \mu < n$, and*

- $k \leq \mu + 1 - g$ *if $n \leq \mu$.*

If $\mu = n + 2g - 1$, then $C_{\mathcal{L}}(D, \mu Q) = \mathbb{F}_q^n$.

From [12, Th. 19, 20] we have the following result.

Theorem 11. *Let $C_1 = C_{\mathcal{L}}(D, \mu_1 Q)$ and $C_2 = C_{\mathcal{L}}(D, \mu_2 Q)$, with $-1 \leq \mu_2 < \mu_1$. Write $k_1 = \dim C_1$, $k_2 = \dim C_2$ and $\ell = k_1 - k_2$. If $1 \leq m \leq \ell$, then*

1. *$M_m(C_1, C_2) \geq n - \mu_1 + \min\{\#\{\alpha \in \cup_{s=1}^{m-1}(i_s + H(Q)) \mid \alpha \notin H(Q)\} \mid -(\mu_1 - \mu_2) + 1 \leq i_1 < \ldots < i_{m-1} \leq -1\}.$*

2. *$M_m(C_2^{\perp}, C_1^{\perp}) \geq \min\{\#\{\alpha \in \cup_{s=1}^{m}(i_s + (\mu_1 - H(Q))) \mid \alpha \in H(Q)\} \mid -(\mu_1 - \mu_2) + 1 \leq i_1 < \ldots < i_m \leq 0\}.$*

Choosing $C_2 = \{\mathbf{0}\}$ in item 1, we obtain a bound on the GHWs of C_1. Similarly, choosing $C_1 = \mathbb{F}_q^n$ in item 2, we get a bound on the GHWs of $C_2^{\perp}$.

Proposition 12. *For $0 \leq \gamma \leq c$, let $h_\gamma = \#(H(Q) \cap (0, \gamma])$ and let $\mu \geq -1$ and $k = \dim C_{\mathcal{L}}(D, \mu Q)$. If $\mu < n$ and $1 \leq m \leq \min\{k, g\}$, then*

$$d_m(C_{\mathcal{L}}(D, \mu Q)) \geq n - k + 2m - c + h_{c-m} \geq n - k + 2m - c.$$

Proof. We will apply item 1 in Theorem 11 for $\mu_1 = \mu$ and $\mu_2 = -1$. Consider numbers $-\mu \leq i_1 < \cdots < i_{m-1} \leq -1$. We have $[c - m + 1, c] \setminus H(Q) \subset [\max\{0, c + i_1\}, c] \setminus H(Q) \subset \{\alpha \in \cup_{s=1}^{m-1}(i_s + H(Q)) \mid \alpha \notin H(Q)\} \cap [0, \infty)$, where the first inclusion comes from $i_1 \leq -m+1$. Now the number of elements in $[c-m+1, c] \cap H(Q)$ is at most

$(c - g) - h_{c-m}$, and we have that $\# \left(\{ \alpha \in \cup_{s=1}^{m-1}(i_s + H(Q)) \mid \alpha \notin H(Q) \} \cap [0, \infty) \right) \geq m - (c - g) + h_{c-m}$. On the other hand, we have that $\{ i_1, \ldots, i_{m-1} \} \subset \{ \alpha \in \cup_{s=1}^{m-1}(i_s + H(Q)) \mid \alpha \notin H(Q) \} \cap (-\infty, 0)$. Thus, from Theorem 11, we obtain $d_m(C_{\mathcal{L}}(D, \mu Q)) \geq (n - \mu) + (m - 1) + (m - c + g + h_{c-m})$. Since $k \geq \mu - g + 1$ by Lemma 10, the result follows. □

Proposition 13. *For $\gamma \geq 1$, let $h'_\gamma = \#([\gamma, \infty) \setminus H(Q))$ and let $\mu > 2g - 2$ and $k = \dim C_{\mathcal{L}}(D, \mu Q)^\perp$. If $1 \leq m \leq \min\{k, g\}$, then*

$$d_m(C_{\mathcal{L}}(D, \mu Q)^\perp) \geq n - k + 2m - c + h'_{\mu-c+m} \geq n - k + 2m - c.$$

Proof. We will apply item 2 in Theorem 11 for $\mu_1 = n + 2g - 1$ and $\mu_2 = \mu$ to prove that $M_m(C_2^\perp, C_1^\perp) \geq k_2 + 2m - c + h'_{\mu_2-c+m}$, where $k_2 = \dim C_2$. Consider numbers $-(\mu_1 - \mu_2) + 1 \leq i_1 < \cdots < i_m \leq 0$. First, $(i_m + \mu_1 - H(Q)) \cap [0, \mu_2]$ contains the set $[0, \mu_1 - c - (\mu_1 - \mu_2) + m] = [0, \mu_2 - c + m]$, since $i_m \geq -(\mu_1 - \mu_2) + m$ and $\mu_1 - c - (\mu_1 - \mu_2) + m \leq \mu_2$. Here, we used the assumption $m \leq g$ and the fact that $g \leq c$. Thus, $\# ((i_m + \mu_1 - H(Q)) \cap H(Q) \cap [0, \mu_2])$ is greater than or equal to $(\mu_2 - c + m + 1) - (g - h'_{\mu_2-c+m})$. On the other hand, $\{\mu_1 + i_1, \ldots, \mu_1 + i_m\}$ is contained in $\{\alpha \in \cup_{s=1}^m (i_s + (\mu_1 - H(Q))) \mid \alpha \in H(Q)\}$, which are m elements in the range $(\mu_2, \mu_1]$. Thus, from the previous theorem we obtain $M_m(C_2^\perp, C_1^\perp) \geq (\mu_2 - c + m + 1 - g + h'_{\mu_2-c+m}) + m$. Since $k_2 \leq \mu_2 - g + 1$ and $C_1 = \mathbb{F}_q^n$ by Lemma 10, the result follows. □

5 Asymptotic analysis for algebraic geometric codes

As a preparation step to treat the parameters $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$ of sequences of schemes based on algebraic geometric codes, in this section we derive asymptotic consequences of the non-asymptotic results derived in the previous section. We start our investigations by commenting on [24, Th. 5.9], which if true would imply that the codes in Theorem 8 would attain the Singleton bound (12) in all cases $\frac{1}{q} < R_2 < R_1 < 1 - \frac{1}{q}$ and for all $0 \leq \varepsilon_1, \varepsilon_2 \leq 1$. Below we reformulate [24, Th. 5.9] with the needed modification which ensures that the Singleton bound is reached when $1/A(q) < \rho$, in contrast to $0 \leq \rho$, as it appears in [24]. We also adapt the formulation to better fit our purposes of constructing asymptotically good sequences of secret sharing schemes. We include the proof from [24] to explain why this modification is needed.

Theorem 14. *Let $(\mathcal{F}_i)_{i=1}^\infty$ be an optimal tower of function fields over $\mathbb{F}_q$. Consider R, ρ with $0 \leq \rho \leq R \leq 1$. Let $(C_i)_{i=1}^\infty$ be an optimal sequence of one-point algebraic geometric codes defined from $(\mathcal{F}_i)_{i=1}^\infty$ such that $\dim C_i / n_i \to R$. For all sequences of positive integers $(m_i)_{i=1}^\infty$ with $m_i / n_i \to \rho$, it holds that $\delta = \liminf_{i \to \infty} d_{m_i}(C_i)/n_i \geq 1 - R + \rho - \frac{1}{A(q)}$ and, if $1/A(q) < \rho$, then $\delta = 1 - R + \rho$.*

Proof. The first bound on δ is an easy consequence of the Goppa bound (the first part of Theorem 9). Now assume $1/A(q) < \rho$. By assumption, for i large enough we have $m_i > g(\mathcal{F}_i)$, which by the last part of Theorem 9 implies that $d_{m_i}(C_i) = n_i - \dim C_i + m_i$. Dividing by n_i and taking the limit, we obtain the result. □

The theorem states that the Singleton bound (10) can be asymptotically reached when $1/A(q) < \rho$, which implies $1/(\sqrt{q} - 1) < \rho$ by (14). However, this leaves the cases $1/A(q) \geq \rho$ undecided. In the following, we shall concentrate on finding asymptotic results for the cases $1/A(q) \geq \rho$. We will need [24, Cor. 3.6] and Wei's duality theorem [26, Th. 3], which we now recall in this order:

Lemma 15. *For every linear code $C \subset \mathbb{F}_q^n$ we have that*

$$d_m(C) \geq d_1(C)\frac{q^m - 1}{q^m - q^{m-1}}, \quad m = 1, \ldots, \dim C.$$

Lemma 16. *Let $C \subset \mathbb{F}_q^n$ be a linear code, $\dim C = k$. Write $d_r = d_r(C)$, $d_s^{\perp} = d_s(C^{\perp})$ for $1 \leq r \leq k$, $1 \leq s \leq n - k$. Then,*

$$\{1, \ldots, n\} = \{d_1, \ldots, d_k\} \cup \{n + 1 - d_{n-k}^{\perp}, \ldots, n + 1 - d_1^{\perp}\}.$$

Our first result is a strict improvement to Theorem 14.

Theorem 17. *Let $(\mathcal{F}_i)_{i=1}^{\infty}$ be an optimal tower of function fields over $\mathbb{F}_q$. Consider R, ρ with $1/A(q) \leq R \leq 1$ and $\frac{q}{q-1}\frac{1}{A(q)} - \frac{1}{q-1}R \leq \rho \leq R$. Let $(C_i)_{i=1}^{\infty}$ be an optimal sequence of one-point algebraic geometric codes defined from $(\mathcal{F}_i)_{i=1}^{\infty}$ such that $\dim C_i/n_i \to R$. There exists a sequence of positive integers $(m_i)_{i=1}^{\infty}$ such that $m_i/n_i \to \rho$ and $d_{m_i}(C_i)/n_i \to \delta = 1 - R + \rho$.*

Proof. In this proof we use the notation $k_i = \dim C_i$. Let $f : \mathbb{N} \to \mathbb{N}$ be a function such that $f(i) \to \infty$ and $f(i)/n_i \to 0$, as $i \to \infty$. Now fix i. The Goppa bound (Theorem 9) together with Lemma 15 tell us that

$$d_{f(i)}(C_i^{\perp}) \geq \frac{q^{f(i)} - 1}{q^{f(i)} - q^{f(i)-1}}(k_i - g(\mathcal{F}_i)).$$

Write $h(i)$ for the right-hand side, that is, $d_{f(i)}(C_i^{\perp}) \geq \lceil h(i) \rceil$. Observe that $h(i) > 0$, since asymptotically $k_i > g(\mathcal{F}_i)$. If we write $d_s^{\perp} = d_s(C_i^{\perp})$ for $1 \leq s \leq n_i - k_i$, we have that $n_i + 1 - \lceil h(i) \rceil \geq n_i + 1 - d_{f(i)}^{\perp}$. From this inequality and the monotonicity of GHWs, it follows that the sets

$$\{n_i + 1 - \lceil h(i) \rceil, n_i + 2 - \lceil h(i) \rceil, \ldots, n_i\} \text{ and}$$

$$\{n_i + 1 - d_{n_i-k_i}^{\perp}, n_i + 1 - d_{n_i-k_i-1}^{\perp}, \ldots, n_i + 1 - d_{f(i)+1}^{\perp}\}$$

are disjoint. Therefore, from Lemma 16 it follows that

$$d_{k_i - \lceil h(i) \rceil + f(i)}(C_i) \geq n_i + 1 - \lceil h(i) \rceil. \tag{15}$$

Now take a sequence of positive integers $(m_i)_{i=1}^{\infty}$ such that

$$k_i - \lceil h(i) \rceil + f(i) \leq m_i \leq k_i \tag{16}$$

11

(observe that the left-hand side is smaller than k_i for large i). From (15), (16) and the monotonicity of GHWs we get

$$
\begin{aligned}
d_{m_i}(C_i) &\geq d_{k_i - \lceil h(i) \rceil + f(i)}(C_i) + m_i - k_i + \lceil h(i) \rceil - f(i) \\
&\geq n_i - k_i + m_i - f(i) + 1.
\end{aligned}
\tag{17}
$$

Dividing by n_i and letting $i \to \infty$, (16) and (17) become

$$
\frac{q}{q-1} \frac{1}{A(q)} - \frac{1}{q-1} R \leq \rho \leq R,
$$

$$
\delta = \lim_{i \to \infty} \frac{d_{m_i}(C_i)}{n_i} = 1 - R + \rho.
$$

$\square$

We have the following result for lower values of ρ.

Theorem 18. *Let $(\mathcal{F}_i)_{i=1}^{\infty}$ be an optimal tower of function fields over $\mathbb{F}_q$. Consider R, ρ with $0 \leq \rho \leq R \leq 1$. Let $(C_i)_{i=1}^{\infty}$ be an optimal sequence of one-point algebraic geometric codes defined from $(\mathcal{F}_i)_{i=1}^{\infty}$ such that $\dim C_i / n_i \to R$. For all sequences of positive integers $(m_i)_{i=1}^{\infty}$ with $m_i / n_i \to \rho$, the number $\delta = \liminf_{i \to \infty} d_{m_i}(C_i)/n_i$ satisfies*

$$
\delta \geq \frac{q}{q-1} \left(1 - R - \frac{1}{A(q)} \right) + \rho.
$$

Proof. Let $0 < \varepsilon < 1$ be an arbitrary fixed number. From the Goppa bound (Theorem 9) and Lemma 15 we obtain that

$$
\frac{d_{\lceil \varepsilon m_i \rceil}(C_i)}{n_i} \geq \frac{q^{\varepsilon m_i} - 1}{q^{\varepsilon m_i} - q^{\varepsilon m_i - 1}} \left(1 - \frac{\dim C_i}{n_i} - \frac{g_i}{n_i} \right).
$$

Using again the monotonicity of GHWs we obtain that

$$
\frac{d_{m_i}(C_i)}{n_i} \geq \frac{q^{\varepsilon m_i} - 1}{q^{\varepsilon m_i} - q^{\varepsilon m_i - 1}} \left(1 - \frac{\dim C_i}{n_i} - \frac{g_i}{n_i} \right) + \frac{m_i(1 - \varepsilon)}{n_i}.
$$

Now, letting $i \to \infty$ first and then $\varepsilon \to 0$, we obtain

$$
\delta = \liminf_{i \to \infty} \frac{d_{m_i}(C_i)}{n_i} \geq \frac{q}{q-1} \left(1 - R - \frac{1}{A(q)} \right) + \rho.
$$

$\square$

In the following, we concentrate on Garcia and Stichtenoth's second tower [11] of function fields $(\mathcal{F}_i)_{i=1}^{\infty}$ over $\mathbb{F}_q$ where q is an arbitrary perfect square. From [21] we have a complete description of the corresponding Weierstrass semigroups and [23] gives an efficient method for constructing the corresponding optimal sequences of one-point algebraic geometric codes. We will apply the two new bounds on GHWs

given in Proposition 12 and Proposition 13 to this tower. In the rest of this section, q is always a perfect square and by $(\mathcal{F}_i)_{i=1}^\infty$ we mean Garcia and Stichtenoth's second tower [11]. We will need the following properties of each $\mathcal{F}_i$ ([11, 21]): its number of rational places satisfies $N(\mathcal{F}_i) > q^{\frac{i-1}{2}}(q - \sqrt{q})$, its genus is given by

$$g(\mathcal{F}_i) = \begin{cases} (q^{\frac{i}{4}} - 1)^2 & \text{if } i \text{ is even,} \\ (q^{\frac{i+1}{4}} - 1)(q^{\frac{i-1}{4}} - 1) & \text{if } i \text{ is odd,} \end{cases}$$

and it has a rational place Q_i such that the conductor of $H(Q_i)$ is given by

$$c_i = \begin{cases} q^{i/2} - q^{i/4} & \text{if } i \text{ is even,} \\ q^{i/2} - q^{(i+1)/4} & \text{if } i \text{ is odd.} \end{cases}$$

In the rest of the section, $(C_i)_{i=1}^\infty$ is an optimal sequence of one-point algebraic geometric codes defined from $(\mathcal{F}_i)_{i=1}^\infty$, and where C_i is of the form $C_\mathcal{L}(D_i, \mu_i Q_i)$ or $C_\mathcal{L}(D_i, \mu_i Q_i)^\perp$. Recall from [23] that we may assume without loss of generality that D_i is chosen in such a way that C_i can be constructed using $\mathcal{O}(n_i^3 \log_q^3(n_i))$ operations in $\mathbb{F}_q$.

Theorem 19. *Let $(\mathcal{F}_i)_{i=1}^\infty$ be Garcia-Stichtenoth's second tower of function fields over $\mathbb{F}_q$, where q is a perfect square. Let $(C_i)_{i=1}^\infty$ be a corresponding optimal sequence of one-point algebraic geometric codes as described above. Consider R, ρ with $0 \leq R \leq 1 - \frac{1}{\sqrt{q}-1}$ and $0 \leq \rho \leq \min\{R, \frac{1}{\sqrt{q}-1}\}$, and assume that $\dim C_i/n_i \to R$. For all sequences of positive integers $(m_i)_{i=1}^\infty$ with $m_i/n_i \to \rho$, it holds that $\delta = \liminf_{i\to\infty} d_{m_i}(C_i)/n_i$ satisfies*

$$\delta \geq 1 - R + 2\rho - \frac{1}{\sqrt{q}-1}.$$

Proof. We may assume that C_i is of the form $C_\mathcal{L}(D_i, \mu_i Q_i)$ or $C_\mathcal{L}(D_i, \mu_i Q_i)^\perp$, with $2g(\mathcal{F}_i) - 2 < \mu_i < n_i$ and $(\mu_i - g(\mathcal{F}_i))/n_i \to R$. As $\lim_{i\to\infty} c_i/n_i = \lim_{i\to\infty} g(\mathcal{F}_i)/n_i = 1/(\sqrt{q}-1)$, the result follows from Proposition 12 or Proposition 13. $\square$

6 The parameters $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$ for algebraic geometric code based schemes

In Section 3 we estimated $\Omega^{(1)}$ and $\Omega^{(2)}$ for asymptotically good sequences of schemes based on algebraic geometric codes coming from optimal towers of function fields, the sequences being called asymptotically good if $\Omega^{(1)} > 0$ and $\Omega^{(2)} < 1$. Employing the analysis in Section 5 together with (7) and (9) we are now able to give a more complete picture of the information leakage and reconstruction by providing also estimates on $\Lambda^{(1)}(\varepsilon_1)$ and $\Lambda^{(2)}(\varepsilon_2)$. We emphasize that the below theorems apply also in the cases where one or both of the conditions $\Omega^{(1)} > 0$ and $\Omega^{(2)} < 1$ fails to hold. Throughout the section recall that by definition the numbers ε_1 and ε_2 always satisfy $0 \leq \varepsilon_1, \varepsilon_2 \leq 1$.

Theorem 20. *For the sequence of linear ramp secret sharing schemes described in Theorem 8 we have the following estimates: If $1/A(q) \leq 1 - R_2$ and $\varepsilon_1 \geq \left(\frac{q}{q-1}\frac{1}{A(q)} - \frac{1}{q-1}(1 - R_2)\right)/L$ then $\Lambda^{(1)}(\varepsilon_1) \geq R_2 + \varepsilon_1 L$. If $1/A(q) \leq R_1$ and $\varepsilon_2 \geq \left(\frac{q}{q-1}\frac{1}{A(q)} - \frac{1}{q-1}R_1\right)/L$ then $\Lambda^{(2)}(\varepsilon_2) \leq R_1 - \varepsilon_2 L$.*

Proof. Apply Theorem 17 with $\rho = \varepsilon_1 L$ and $\rho = \varepsilon_2 L$, respectively, in combination with (7) and (9), respectively. ∎

Theorem 21. *For the sequence of linear ramp secret sharing schemes described in Theorem 8 we have the following estimates: $\Lambda^{(1)}(\varepsilon_1) \geq \frac{q}{q-1}(R_2 - \frac{1}{A(q)}) + \varepsilon_1 L$ and $\Lambda^{(2)}(\varepsilon_2) \leq \frac{q}{q-1}(R_1 + \frac{1}{A(q)}) - \frac{1}{q-1} - \varepsilon_2 L$.*

Proof. Apply Theorem 18 in combination with (7) and (9). ∎

Observe that from Theorem 21 we get an estimate on $\Lambda^{(1)}(0)$ wich is $q/(q-1)$ times as large as the estimate on $\Omega^{(1)}$ in Section 3. Hence, the studied sequences of secret sharing schemes are more secure than previously anticipated. A similar remark holds regarding reconstruction.

Theorem 22. *Let q be a perfect square. For the sequence of linear ramp secret sharing schemes described in Theorem 8 we have the following estimates: If $R_2 \geq 1/(\sqrt{q} - 1)$ and $\varepsilon_1 \leq \frac{1}{\sqrt{q}-1}\frac{1}{L}$ then $\Lambda^{(1)}(\varepsilon_1) \geq R_2 + 2\varepsilon_1 L - \frac{1}{\sqrt{q}-1}$. If $R_1 \leq 1 - \frac{1}{\sqrt{q}-1}$ and $\varepsilon_2 \leq \frac{1}{\sqrt{q}-1}\frac{1}{L}$ then $\Lambda^{(2)}(\varepsilon_2) \leq R_1 - 2\varepsilon_2 L + \frac{1}{\sqrt{q}-1}$. The i-th scheme in the sequence can be constructed using $\mathcal{O}(n_i^3 \log(n_i)^3)$ operations in $\mathbb{F}_q$.*

Proof. Apply Theorem 19 in combination with (7) and (9). ∎

We finally remark that when q is a perfect square, then similarly to Theorem 22, one can assume in Theorem 20 and Theorem 21 that the i-th scheme in the sequence can be constructed using $\mathcal{O}(n_i^3 \log(n_i)^3)$ operations in $\mathbb{F}_q$.

Acknowledgments

A   Proof of Theorem 4

In this appendix we give a proof of Theorem 4. The theorem is an improvement of [20, Th. 9], the improvement stating that the RGHWs of primary and dual nested linear code pairs can get *simultaneously* asymptotically as close to the Singleton bound (10) as wanted. We use the notation and results in [13, 18, 19, 20]. In particular, we use the concept of relative dimension length profile (RDLP) as appears in [18, Sec. III]. For $1 \le d \le n$, and linear codes $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ define

$$
\begin{aligned}
K_d(C_1, C_2) \quad = \quad &\max\{\dim(C_1 \cap V_I) - \dim(C_2 \cap V_I) \mid \\
&I \subset \{1, \ldots, n\}, \#I = d\},
\end{aligned}
$$

where $V_I = \{\mathbf{x} \in \mathbb{F}_q^n \mid x_i = 0 \text{ if } i \notin I\}$. The sequence $(K_d(C_1, C_2))_{d=1}^n$ is then the RDLP of the pair $C_2 \subsetneq C_1$ and is known to be non-decreasing [18, Prop. 1]. Our interest in the RDLP comes from the following result corresponding to the first part of [18, Th. 3]:

$$
M_m(C_1, C_2) = \min\{d \mid K_d(C_1, C_2) \ge m\}. \tag{18}
$$

As in [13, 19], we define for integers a, u, v, w the numbers:

$$
N_1(w, u) = \frac{\prod_{i=0}^{u-1}(q^w - q^i)}{\prod_{i=0}^{u-1}(q^u - q^i)}, \quad N_2(w, u, v) = \frac{\prod_{i=0}^{v-1}(q^w - q^{u+i})}{\prod_{i=0}^{v-1}(q^v - q^i)},
$$

and $N_3(w, u, v, a) = N_1(u, a)N_2(w - a, u - a, v - a)$. The meaning of N_1 is [13], [19, Lem. 5 and 6]:

Lemma 23. *Let W be an $\mathbb{F}_q$-linear vector space and let u, v, $w = \dim W$ be non-negative integers. If $u \le w$, then $N_1(w, u)$ is the number of subspaces $U \subset W$ of dimension u. Furthermore, if U is fixed and $u \le v \le w$, then $N_1(w - u, v - u)$ is the number of $\mathbb{F}_q$-linear vector spaces V such that $U \subset V \subset W$ and $\dim V = v$.*

From [19, Lem. 9] we have:

Lemma 24. *Consider fixed integers $1 \le k_2 < k_1 < n$ and a fixed set $I \subset \{1, \ldots, n\}$ with $\#I = d$. Let s be an integer with $s \le \min\{d, k_1 - k_2\}$. The number of linear code pairs $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ such that $\dim C_1 = k_1$, $\dim C_2 = k_2$, and $\dim(C_1 \cap V_I) - \dim(C_2 \cap V_I) = s$, equals*

$$
\begin{aligned}
N_4(n, k_1, k_2, d, s) = \sum_{a=0}^{\min\{d-s, k_1-s, k_2\}} \bigg(&N_1(d, a) \\
N_2(n - a, d - a, k_2 - a)&N_3(n - k_2, d - a, k_1 - k_2, s)\bigg).
\end{aligned}
$$

We next extend [19, Cor. 3].

Theorem 25. *Consider fixed integers* $1 \leq k_2 < k_1 < n$, $1 \leq d \leq n$, $1 \leq d^\perp \leq n$, $1 \leq s \leq \min\{d, k_1 - k_2\}$, *and* $1 \leq s^\perp \leq \min\{d^\perp, k_1 - k_2\}$. *There exists a nested linear code pair* $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ *such that* $\dim C_1 = k_1$, $\dim C_2 = k_2$, $M_s(C_1, C_2) > d$ *and* $M_{s^\perp}(C_2^\perp, C_1^\perp) > d^\perp$, *if*

$$N_1(n, k_2)N_1(n - k_2, k_1 - k_2) > \binom{n}{d} \sum_{\sigma = s}^{k_1 - k_2} N_4(n, k_1, k_2, d, \sigma)$$

$$+ \binom{n}{d^\perp} \sum_{\sigma^\perp = s^\perp}^{k_1 - k_2} N_4(n, n - k_2, n - k_1, d^\perp, \sigma^\perp).$$

Proof. By Lemma 23, the term $N_1(n, k_2)N_1(n - k_2, k_1 - k_2)$ is the total number of pairs $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ such that $\dim C_1 = k_1$ and $\dim C_2 = k_2$. On the other hand, by Lemma 24, the number of pairs $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ such that $\dim C_1 = k_1$, $\dim C_2 = k_2$ and $K_d(C_1, C_2) \geq s$ is at most $\binom{n}{d} \sum_{\sigma = s}^{k_1 - k_2} N_4(n, k_1, k_2, d, \sigma)$. Similarly, the number of pairs $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ such that $\dim C_1 = k_1$, $\dim C_2 = k_2$ and $K_{d^\perp}(C_2^\perp, C_1^\perp) \geq s^\perp$ is at most $\binom{n}{d^\perp} \sum_{\sigma^\perp = s^\perp}^{k_1 - k_2} N_4(n, n - k_2, n - k_1, d^\perp, \sigma^\perp)$. The inequality therefore ensures the existence of a code pair $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$ with $\dim C_1 = k_1$, $\dim C_2 = k_2$, $K_d(C_1, C_2) < s$ and $K_{d^\perp}(C_2^\perp, C_1^\perp) < s^\perp$. But the RDLP is non-decreasing and $K_n(C_1, C_2) = K_n(C_2^\perp, C_1^\perp) = k_1 - k_2$ which is larger than or equal to s and s'. Therefore there exists a smallest index j such that $K_j(C_1, C_2) \geq s$ and a smallest index $j^\perp$ such that $K_{j^\perp}(C_2^\perp, C_1^\perp) \geq s^\perp$ and $j > d$ as well as $j^\perp > d^\perp$ hold. The theorem now follows from (18). $\qquad\square$

To apply Theorem 25 in an asymptotic setting we will need a couple of lemmas.

Lemma 26. *Define* $\pi(q) = \prod_{i=1}^\infty (1 - q^{-i})$. *Then*

$$\pi(q)q^{u(w-u)} \leq N_1(w, u) \leq \pi(q)^{-1}q^{u(w-u)}, \tag{19}$$
$$N_2(w, u, v) \leq \pi(q)^{-1}q^{v(w-v)},$$
$$N_3(w, u, v, a) \leq \pi(q)^{-2}q^{a(u-a)}q^{(v-a)(w-v)}. \tag{20}$$

Proof. The inequality (19) is [14, Cor. 2] and the last two inequalities correspond to [20, Lem. 3] except that $\pi(q)^{-2}$ in (20) by a mistake was there written $\pi(q)^{-1}$ and similarly $q^{a(u-a)}$ was written $q^{u(u-a)}$. $\qquad\square$

The next lemma corresponds to [9, Ex. 11.1.3].

Lemma 27. *Let* $H_q(x) = -x \log_q(x) - (1 - x) \log_q(1 - x)$, *then*

$$\frac{1}{n+1}q^{nH_q(m/n)} \leq \binom{n}{m} \leq q^{nH_q(m/n)}.$$

With the above machinery we can now give the promised proof.

Proof of Theorem 4. Let R_1, R_2, δ, $\delta^\perp$, τ and $\tau^\perp$ be as in the theorem (in particular assume (13) to hold). Let $(n_i)_{i=1}^\infty$ be a strictly increasing sequence of positive integers and define $k_1(i) = \lfloor n_i R_1 \rfloor$, $k_2(i) = \lceil n_i R_2 \rceil$, $s(i) = \lceil n_i \tau \rceil$, $s^\perp(i) = \lceil n_i \tau^\perp \rceil$, $d(i) = \lfloor n_i \delta \rfloor$ and $d^\perp(i) = \lfloor n_i \delta^\perp \rfloor$. Using Theorem 25, we will show that for i large enough there exist nested linear codes $C_2(i) \subsetneq C_1(i) \subset \mathbb{F}_q^{n_i}$ of dimensions $k_2(i)$ and $k_1(i)$, respectively, with

$$M_{s(i)} \geq d(i), \quad \text{and} \quad M_{s^\perp(i)} \geq d^\perp(i). \tag{21}$$

Observe that (13) implies that

$$k_1(i) + d(i) - n_i - s(i) < 0, \tag{22}$$

$$(n_i - k_2(i)) + d^\perp(i) - n_i - s^\perp(i) < 0, \tag{23}$$

which we will need later in the proof. For brevity, we will write k_1, k_2, d, $d^\perp$, s, $s^\perp$, and n rather than $k_1(i)$, $k_2(i)$, $d(i)$, $d^\perp(i)$, $s(i)$, $s^\perp(i)$, and n_i. Applying Lemma 26, Lemma 27, and Theorem 25 we see that a sufficient condition for the existence of a linear code pair satisfying (21) is

$$
\pi(q)^2 q^{k_2(n-k_2)} q^{(k_1-k_2)(n-k_1)}
$$
$$
> \quad q^{nH_q(d/n)} \sum_{\sigma=s}^{k_1-k_2} \sum_{a=0}^{\min\{d-\sigma,k_1-\sigma,k_2\}} \left[\pi(q)^{-1} q^{a(d-a)} \right.
$$
$$
\left. \pi(q)^{-1} q^{(k_2-a)(n-a-k_2+a)} \pi(q)^{-2} q^{\sigma(d-a-\sigma)} q^{(k_1-k_2-\sigma)(n-k_2-k_1+k_2)} \right]
$$
$$
+ q^{nH_q(d^\perp/n)} \sum_{\sigma^\perp=s^\perp}^{k_1-k_2} \sum_{a=0}^{\min\{d^\perp-\sigma^\perp,n-k_2-\sigma^\perp,n-k_1\}} \left[\pi(q)^{-1} q^{a(d^\perp-a)} \right.
$$
$$
\left. \pi(q)^{-1} q^{(n-k_1-a)(n-a-n+k_1+a)} \pi(q)^{-2} q^{\sigma^\perp(d^\perp-a-\sigma^\perp)} q^{(k_1-k_2-\sigma^\perp)k_2} \right].
$$

But then another sufficient condition (named Condition A) for the existence of a nested code pair satisfying (21) is

$$
q^{k_2(n-k_2)+(k_1-k_2)(n-k_1)} >
$$
$$
f(q,n) \max \left\{ q^{a(d-a)+(k_2-a)(n-k_2)+\sigma(d-a-\sigma)+(k_1-k_2-\sigma)(n-k_1)} \; \right|
$$
$$
\left. s \leq \sigma \leq k_1 - k_2, 0 \leq a \leq \min\{d-\sigma, k_1-\sigma, k_2\} \right\} +
$$
$$
f^\perp(q,n) \max \left\{ q^{a(d^\perp-a)+(n-k_1-a)k_1+\sigma^\perp(d^\perp-a-\sigma^\perp)+(k_1-k_2-\sigma^\perp)k_2} \; \right|
$$
$$
s^\perp \leq \sigma^\perp \leq k_1 - k_2, \text{ and}
$$
$$
0 \leq a \leq \min\{d^\perp-\sigma^\perp, n-k_2-\sigma^\perp, n-k_1\} \right\},
$$

where $f(q,n) = \pi(q)^{-6}q^{nH_q(d/n)}n^2$, and where $f^\perp(q,n) = \pi(q)^{-6}q^{nH_q(d^\perp/n)}n^2$. Consider now the expression $\sigma(k_1 + d - n - \sigma - a)$, which contains the terms in the first exponent on the right-hand side of Condition A related to σ. As a function in σ, this is a downward parabola intersecting the first axis in $\sigma = 0$. For $s \leq \sigma$, it follows from (22) and $0 \leq a$ that $k_1 + d - n - \sigma - a < 0$. Hence, the maximal value of $\sigma(k_1 + d - n - \sigma - a)$ for $s \leq \sigma$ is attained when $\sigma = s$, and we therefore substitute σ with s in Condition A. In a similar fashion, we see from (23) that $\sigma^\perp$ can be replaced with $s^\perp$. After these substitutions, the terms related to a in the first exponent on the right-hand side of Condition A become $-a^2 + a(k_2 + d - n - s)$, which is equal to 0 for $a = 0$ and negative for $a > 0$, as a consequence of (22). Similarly, the terms related to a in the last exponent on the right-hand side become $-a^2 + a(d^\perp - k_1 - s^\perp)$ which again is equal to 0 for $a = 0$ and negative for $a > 0$ as a consequence of (23). Hence, we can substitute a with 0 in Condition A. After the above substitutions, Condition A simplifies to

$$q^{k_2(n-k_2)+(k_1-k_2)(n-k_1)} \quad > f(q,n)q^{k_2(n-k_2)+s(d-s)+(k_1-k_2-s)(n-k_1)}$$
$$+ f^\perp(q,n)q^{(n-k_1)k_1+s^\perp(d^\perp-s^\perp)+(k_1-k_2-s^\perp)k_2}.$$

In this formula, we now replace the two expressions on the right-hand side with the largest one multiplied by 2. We then take the logarithm over q and finally divide by n^2. Assume that the first term on the right-hand side of Condition A is greater than or equal to the last term. After simplifying equal terms on both sides and using the definition of k_1, d and s, we see that Condition A holds if

$$0 > g(i) + \tau(\delta - \tau) - \tau(1 - R_1), \tag{24}$$

where $g(i) = \log_q(2f(q,n_i))/n_i^2$, which goes to 0 as i goes to infinity. Similarly, if the last term on the right-hand side is greater than or equal to the first term, we see that Condition A holds if

$$0 > g^\perp(i) + \tau^\perp(\delta^\perp - \tau^\perp) - \tau^\perp R_2, \tag{25}$$

where $g^\perp(i) = \log_q(2f^\perp(q,n_i))/n_i^2$, which again goes to 0 as i goes to infinity. Finally, for i large enough, (24) follows from the first part of (13), since $\tau > 0$, and (25) follows from the last part of (13), since $\tau^\perp > 0$. Therefore, Condition A holds for i large enough and we are done. $\square$

References

[1] A. Bassa, P. Beelen, A. Garcia, H. Stichtenoth, Towers of function fields over non-prime finite fields, *Moscow Mathematical Journal*, 15:1–29, 2015.

[2] G.R. Blakley, Safeguarding cryptographic keys, *Proc. of the National Computer Conference 1979*, 48:313–317, 1979

[3] G.R. Blakley, C. Meadows, Security of ramp schemes, Advances in cryptology—CRYPTO 1984, *Lecture Notes in Comput. Sci.*, 196:242–268, 1995.

[4] I. Cascudo, R. Cramer, C. Xing, Bounds on the threshold gap in secret sharing and its applications, *IEEE Trans. Inform. Theory*, 59:5600–5612, 2013.

[5] I. Cascudo, R. Cramer, C. Xing, Torsion limits and Riemann-Roch systems for function fields and applications, *IEEE Trans. Inform. Theory*, 60:3871–3888, 2014.

[6] H. Chen, R. Cramer, Algebraic geometric secret sharing schemes and secure multi-party computations over small fields, in: Advances in cryptology—CRYPTO 2006, *Lecture Notes in Comput. Sci.*, 4117:521–536, 2006.

[7] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, V. Vaikuntanathan, Secure computation from random error correcting codes, in: Advances in cryptology—EUROCRYPT 2007, *Lecture Notes in Comput. Sci.*, 4515:291–310, 2007.

[8] H. Chen, R. Cramer, R. de Haan, I. Cascudo, Strongly multiplicative ramp schemes from high degree rational points on curves, in: Advances in cryptology—EUROCRYPT 2008, *Lecture Notes in Comput. Sci.*, 4965:451–470, 2008.

[9] T. M. Cover, J. A. Thomas, *Elements of Information Theory*, 2nd edition, Wiley Interscience, 2006.

[10] R. Cramer, I.B. Damgård, N. Döttling, S. Fehr, G. Spini, Linear secret sharing schemes from error correcting codes and universal hash functions, in: Advances in cryptology—EUROCRYPT 2015, *Lecture Notes in Comput. Sci.*, 9057:313–336, 2015.

[11] A. Garcia, H. Stichtenoth, On the asymptotic behaviour of some towers of function fields over finite fields, *Journal of Number Theory*, 61:248–273, 1996.

[12] O. Geil, S. Martin, R. Matsumoto, D. Ruano, Y. Luo, Relative generalized Hamming weights of one-point algebraic geometric codes, *IEEE Trans. Inform. Theory*, 60:5938–5949, 2014.

[13] J. Goldman, G.-C. Rota, On the foundations of combinatorial theory IV: Finite vector spaces and Eulerian generating functions, *Studies in Applied Mathematics*, 49:239–258, 1970.

[14] T. Helleseth, T. Klöve, V. I. Leveshtein, Ø. Ytrehus, Bounds on the minimum support weights, *IEEE Trans. Inform. Theory*, 41:432–440, 1995.

[15] T. Høholdt, J.H. van Lint, R. Pellikaan, Algebraic geometry codes, in: V.S. Pless, W.C. Huffman (Eds.), *Handbook of Coding Theory*, 1:871–961, Elsevier, Amsterdam, 1998.

[16] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Tokyo*, 28:721-–724, 1981.

[17] J. Kurihara, T. Uyematsu, R. Matsumoto, Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight, *IEICE Trans. Fundamentals*, E95-A:2067–2075, 2012.

[18] Y. Luo, C. Mitrpant, A.J. Han Vinck, K. Chen, Some new characters on the wire-tap channel of type II, *IEEE Trans. Inform. Theory*, 51:1222–1229, 2005.

[19] R. Matsumoto, Gilbert-Varshamov-type bound for relative dimension length profile, *IEICE Comm. Express*, 2 (8):343–346, 2013.

[20] R. Matsumoto, New asymptotic metrics for relative generalized Hamming weight, *Proceedings of IEEE International Symposium on Information Theory*, 3142–3144, 2014.

[21] R. Pellikaan, H. Stichtenoth, F. Torres, Weierstrass semigroups in an asymptotically good tower of function fields, *Finite Fields Appl.*, 4: 381–392, 1998.

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

[23] K.W. Shum, I. Aleshnikov, P.V. Kumar, H. Stichtenoth, V. Deolaikar, A low-complexity algorithm for the construction of algebraic-geometric codes better than the Gilbert-Varshamov bound, *IEEE Trans. Inform. Theory*, 47:2225–2241, 2001.

[24] M.A. Tsfasman, S.G. Vlăduţ, Geometric approach to higher weights, *IEEE Trans. Inform. Theory*, 41:1564–1588, 1995.

[25] S.G. Vlăduţ, V.G. Drinfeld, The number of points of an algebraic curve, *Funktsional. Anal. i Prilozhen.*, 17:68–69, 1983.

[26] V.K. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inform. Theory*, 37:1412–1418, 1991.

[27] H. Yamamoto, Secret sharing system using (k,L,n) threshold scheme, *Electronics and Communications in Japan (Part I: Communication)*, 69:46–54, 1986