Blackbox Secret Sharing Revisited: A Coding-Theoretic Approach with Application to Expansionless Near-Threshold Schemes

Ronald Cramer* and Chaoping Xing †

Abstract

A *blackbox* secret sharing (BBSS) scheme works in exactly the same way for all finite Abelian groups G; it can be instantiated for any such group G and *only* black-box access to its group operations and to random group elements is required. A secret is a single group element and each of the n players' shares is a vector of such elements. Share-computation and secret-reconstruction is by integer linear combinations. These do not depend on G, and neither do the privacy and reconstruction parameters t, r. This classical, fundamental primitive was introduced by Desmedt and Frankel (CRYPTO 1989) in their context of "threshold cryptography." The expansion factor is the total number of group elements in a full sharing divided by n. For threshold BBSS with t-privacy ($1 \leq t \leq n-1$), $t+1$-reconstruction and arbitrary n, constructions with minimal expansion $O(\log n)$ exist (CRYPTO 2002, 2005).

These results are firmly rooted in number theory; each makes (different) judicious choices of orders in number fields admitting a vector of elements of very large length (in the number field degree) whose corresponding Vandermonde-determinant is sufficiently controlled so as to enable BBSS by a suitable adaptation of Shamir's scheme. Alternative approaches generally lead to very large expansion. The state of the art of BBSS has not changed for the last 15 years.

Our contributions are two-fold. (1) We introduce a novel, nontrivial, effective construction of BBSS based on *coding theory* instead of number theory. For threshold-BBSS we also achieve minimal expansion factor $O(\log n)$. (2) Our method is more versatile. Namely, we show, for the first time, BBSS that is *near-threshold*, i.e., $r-t$ is an arbitrarily small constant fraction of n, *and* that has expansion factor $O(1)$, i.e., individual share-vectors of *constant* length ("asymptotically expansionless"). Threshold can be concentrated essentially freely across full range. We also show expansion is minimal for near-threshold and that such BBSS cannot be attained by previous methods.

Our general construction is based on a well-known mathematical principle, the local-global principle. More precisely, we first construct BBSS over local rings through either Reed-Solomon or algebraic geometry codes. We then "glue" these schemes together in a dedicated manner to obtain a global secret sharing scheme, i.e., defined over the integers, which, as we finally prove using novel insights, has the desired BBSS properties. Though our main purpose here is advancing BBSS for its own sake, we also briefly address possible protocol applications.

1 Introduction

This paper advances the state of the art in *blackbox* secret sharing (BBSS), a classical, fundamental primitive first studied by Desmedt and Frankel [15, 16] in the late 1980s, motivated by their context of "threshold cryptography." A BBSS scheme works in exactly the same way for all finite Abelian

*CWI Amsterdam, Amsterdam, the Netherlands, email: cramer@cwi.nl and Leiden University, Leiden, the Netherlands, email: cramer@math.leidenuniv.nl

†Nanyang Technological University, Singapore, : email: xingcp@ntu.edu.sg

groups G. I.e., it can be instantiated for any such group G and *only* black-box access to its group operations and to random group elements is required. The secret-space equals G (so the secret is a *single* group element) and the share-space for each of n players is a fixed finite product over G (so each share is a vector). Viewing G additively and using the basic fact that G may be viewed as a $\mathbb{Z}$-module, [1] each share is obtained by applying $\mathbb{Z}$*-linear forms* [2] on a vector consisting of secret and random group elements; likewise for secret-reconstruction from appropriate shares. Whether a given player set is reconstructing or gives privacy does not depend on structural information on G (e.g. access to its order), other than it being finite Abelian. This also holds for the integer coefficients of the forms in share computation and secret reconstruction. In this section, we first discuss the technical background of BBSS and its history. Then we overview our results and method. We also argue why our main claim cannot be achieved by previous methods. Finally, we briefly discuss possible protocol applications.

1.1 Background on BBSS

BBSS is conveniently formalized and elucidated mathematically by *Integer Span Programs* (ISP). The latter notion, introduced in [12], is not only sufficient for BBSS but also necessary; it captures exactly the principles laid out above. In a nutshell, an ISP is characterized by a positive integer e and $\mathbb{Z}$-submodules $V_1, \ldots, V_n \subset \mathbb{Z}^e$. Note that, by standard theory, any such submodule is free, i.e., has a basis. Let V_0 denote the $\mathbb{Z}$-module spanned by the "target vector" $\boldsymbol{\mu}_e = (1, 0, \ldots, 0) \in \mathbb{Z}^e$, i.e., V_0 consists of all its integer multiples. [3] For a nonempty subset $A \subset \{1, \ldots, n\}$ we write $V_A = \sum_{i \in A} V_i$, the $\mathbb{Z}$-span of the V_i's with $i \in A$.. A set A is a *reconstructing set* if $V_0 \subset V_A$. It is a *privacy set* if there is a $\mathbb{Z}$-linear form $\phi_A : \mathbb{Z}^e \to \mathbb{Z}$ such that $\phi_A(V_A) \equiv 0$, whereas $\phi_A(V_0) = \mathbb{Z}$. The latter is equivalent to the condition $V_A \cap V_0 = \{0\}$. [4]

One may easily rephrase this definition in terms of matrices; this way one readily observes that a matrix whose rows are partitioned into n blocks each constituting a basis of a different space V_i can be used to define computation of shares by having the matrix act on a vector whose first coordinate is the secret and whose remaining ones are random group elements. Reconstruction is derived from the integer coefficients according to a span of the target vector. Privacy can be verified using the linear form in question, in a way familiar from schemes over finite fields.

Note that there is similarity with *Monotone Span Programs* or MSP [26], a notion due to Karchmer and Wigderson known to be intimately connected with linear secret sharing over finite fields, as first shown by Beimel [2]. In MSPs, the dividing line between the two types sets of sets is "to span or not to span the target vector." This is not the case for ISPs. The reconstruction condition is still equivalent to "the target vector being in the span." However, the privacy condition is *not* simply its negation; since we work over $\mathbb{Z}$ and not over a field it could be so that some nonzero multiple of the target vector is spanned but not the target vector itself. Indeed, write $V_A \cap V_0 = (a)\boldsymbol{\mu}_e$ for some principal ideal (a) of the ring $\mathbb{Z}$ with $a \neq 0, \pm 1$. Then choose, for instance, a prime number p dividing a and a prime number p' not dividing it. Now, if we take G as the cyclic group of order p, the set A is a privacy set, whereas, if we take G as the cyclic group of order p', it is a reconstructing

[1] Briefly, "vectorspace axioms are satisfied except that scalars are defined over $\mathbb{Z}$ instead of a field."

[2] Owing to $\mathbb{Z}$-module structure, a form maps $(g_1, \ldots, g_m) \in G^m$ to $\sum_i \lambda_i g_i \in G$ for a fixed vector $(\lambda_1, \ldots, \lambda_m) \in \mathbb{Z}^m$.

[3] In fact, any vector whose coordinates do not have a nontrivial common divisor may be taken as the target vector.

[4] The implication starting from the form-based definition is trivial. In the other direction, it follows e.g. using basic structural theory of finitely-generated modules over principal ideal domains, such as $\mathbb{Z}$.

set. In particular, the ISP definition is not just a verbatim translation of the MSP definition from finite fields to the integers. For more discussion, see [12, 10].

The expansion factor in BBSS is the length of a full vector of n shares (i.e., the total number of group elements) divided by n. For threshold BBSS with t-privacy ($1 \leq t \leq n-1$), $t+1$-reconstruction and arbitrary positive n, Cramer and Fehr [12] show a construction that achieves expansion $O(\log n)$, which is minimal. This improved the $O(n)$ expansion from the earlier construction due to Desmedt and Frankel [15, 16]. In [14], Cramer, Fehr and Stam prove that absolutely minimal expansion (up to an additive constant) can be achieved. For the lower bounds, please refer to [12, 14]. [5]

These results are firmly rooted in number theory. More precisely, each makes a judicious choice of orders in algebraic number fields [6] admitting a finite, large dedicated set of points that is sufficiently controlled so as to enable BBSS by a suitable adaptation of Shamir's secret sharing over finite fields. The choice of order, the control, and the exact way BBSS is realized all vary across these known results. In a nutshell, these methods all use "polynomials" whose coefficients are chosen in the tensor-product $R \otimes_{\mathbb{Z}} G$, where R is the order in question. The latter object is an R-module in a natural way. Thus, such a "polynomial" can be evaluated in a set of points in R. Getting a theshold BBSS in this way, mimicking Shamir's scheme to a certain degree, is down to a Vandermonde-determinant determined by these points satisfying one out of several possible convenient number-theoretical properties. The central issue in construction is then to find an infinite family of orders R such that $\mathbb{Z}$-rank of R tends to infinity and such that R admits a dedicated evaluation-point set constrained as indicated above that is very large compared to the $\mathbb{Z}$-rank of R, since the number of players n equals the cardinality of this set and the expansion factor equals the $\mathbb{Z}$-rank of R divided by n. In addition, care must be taken such that each positive number n of players can be accommodated.

In [15, 16], this determinant attached to the evaluation-point set is required to be a *multiplicative unit* of R, so that the Lagrange Interpolation Theorem holds over R. This is best forced by using cyclotomic number fields. But the resulting expansion is $O(n)$. In [12], *two* evaluation sets are required whose attached determinants are *co-prime* in R. It is shown how to construct orders R admitting two such sets of cardinality 2^k where k is the $\mathbb{Z}$-rank of R. One of these sets can be taken simply as $\{1, \ldots, n\}$, the other being more intricate and depending on R. This gives minimal expansion $O(\log n)$. In [14], the two sets are reduced to a single one by requiring the attached determinant to be *primitive*, i.e., its only rational integers divisors are ± 1. It is shown that orders R of rank k exist that admit evaluation-point sets of cardinality 2^k. So expansion is minimal here too, in fact, better by an additive constant. The latter result, though, is not explicit and is significantly more intricate, mathematically. For a full treatment of threshold BBSS, please refer to [10]. There are alternative, more generic approaches. E.g., one can combine Benaloh-Leichter secret sharing [20] with Valiant's result on polynomial-size monotone Boolean formulas for threshold functions [38]. But this leads to very large expansion (but still polynomial in n). The state of the art of BBSS has not changed for the last 15 years.

[5] Note that the case $t = 0$ is trivial and that the case $t = n - 1$ is expansionless via "additive n-out-of-n secret sharing." Hence the restriction on t above. For those "interesting" t, the first step to lower bounds is the observation that threshold BBSS gives binary linear secret sharing for threshold access structures.

[6] An order $\mathcal{O}$ in an algebraic number field K of degree k is a subring $\mathcal{O}$ of its ring of integers $\mathcal{O}_K$ such that $\mathcal{O}$ has finite index in $\mathcal{O}_K$ as a $\mathbb{Z}$-submodule, i.e., $|\mathcal{O}_K/\mathcal{O}|$ is finite. In particular, $\mathcal{O}$ has rank k as $\mathbb{Z}$-module, just as $\mathcal{O}_K$.

1.2 Our contributions

Our contributions here are two-fold.

1. We introduce a completely different, nontrivial effective construction of BBSS based on *coding theory* instead of number theory. For the threshold case we also achieve minimal expansion factor $O(\log n)$ as before. The threshold can be chosen freely.

2. Our general method is more *versatile* than previous methods. As an application *not* attainable by any previous method (as argued below), we demonstrate, for the first time, BBSS that is *near-threshold*, i.e., t-privacy and r-reconstruction are such that $r - t$ is an arbitrarily small constant fraction of n, *and* that achieves *expansion factor* $O(1)$, i.e., a constant number of group elements per share. Moreover, it is supported for arbitrary n and thresholds can be chosen essentially freely, for instance, concentrated around $n/2$. This result is asymptotically expansionless and minimal for near-threshold, as we also prove (see Main Theorem 1).

We now give a straightforward argument why the latter claim on expansionless, near-theshold BBSS cannot be fulfilled by previous methods. We restrict to the general approach from [12, 14] based on "polynomial interpolation" involving number fields (since this approach gives exponentially smaller expansion anyway). Towards a contradiction, suppose, first, that BBSS as claimed above is achieved by evaluations of a *single* polynomial with coefficients in $R \otimes_{\mathbb{Z}} G$ (for some given R). Then the $\mathbb{Z}$-rank of R must be a constant c (equivalently, the number field in question has constant degree), since otherwise the $O(1)$ expansion claim is not met. We may assume there are at least n evaluation points in R used and each share corresponds to one or more (but at most a constant number of them) evaluations of a given polynomial.

Now fix a prime number p and note that $|R/(p)| = p^c$, also a constant. Suppose $n \gg p^c$. If we restrict the assumed BBSS work over $G = \mathbb{Z}/p\mathbb{Z}$ and consider that, *when taken modulo* p, the set of evaluation points used "collapses" to at most p^c distinct ones, this set can be partitioned into at most p^c "blocks" such that, within each block, polynomial evaluation gives the same result across the entire block. In other words, there is just "a constant number of evaluations that matter"; the others are always duplicates. Combining this with the fact that the assumed BBS ensures, in particular, that a full vector of shares determines the secret, there is in fact a *constant-sized* set of players that can reconstruct the secret jointly in case $G = \mathbb{Z}/p\mathbb{Z}$: a contradiction with the assumed parameters. Second, this argument extends to the case where various polynomials are used instead of just one [7] and where R may differ per polynomial. Also note that the argument does not depend on R being an order in a number field; it extends to any commutative ring R that has finite rank as a $\mathbb{Z}$-module, which exactly represents the minimal requirement on R for the BBSS paradigm from [12, 14] to make sense anyway.

1.3 Our method

Our general construction is based on a well-known mathematical principle, the local-global principle. More precisely, we first construct BBSS over local rings through either Reed-Solomon or algebraic geometry codes. We then "glue" these schemes together in a dedicated manner to obtain a global

[7] In [12], *two* polynomials are used, whereas in [15, 16, 14] there is a single one.

secret sharing scheme, i.e., defined over the integers, which, as we finally prove, has the desired BBSS properties.

In some more detail, we start from an observation exploited in [12] and earlier in [34]. Namely, a *weak* form of threshold BBSS is achievable simply by taking "polynomials" with coefficients in G and then evaluating in the integer points $0, 1, \ldots, n$. Defining $\Delta = \prod_{0 \leq i < j \leq n}(j - i)$, the free coefficient is taken as $\Delta \cdot s$, with $s \in G$ equal to the secret. The other coefficients are random in G. It is now straightforward to show that, using polynomials of degree $\leq t$ (with $1 \leq t < n$), there is t-privacy, and, in addition, there is $(t+1)$-reconstruction not of the secret s itself but of a multiple $\Delta^2 \cdot s$, In [12], an order of rank $\log n$ is then hand-crafted that admits evaluation points $0, \alpha_1, \ldots, \alpha_n \in R$ such that, also by weak-BBSS with t-privacy, there is $(t+1)$-reconstruction of the value $(\Delta')^2 \cdot s$, where Δ' is a Vandermonde determinant defined by the α_i's *and* such that Δ, Δ' are *coprime* in R. This leads to a "double-sharing" approach: by secret sharing a given secret independently according to each of these two weak-BBSS schemes, the secret can be reconstructed by a known linear combination over R (translated into linear combinations over $\mathbb{Z}$). This gives the desired BBSS. On a high level, we also follow this double-sharing approach, starting with weak-BBSS from polynomial-evaluation at integer points. However, our approach towards creating the second weak-BBSS, which, together with the first, shouild enforce the co-primality property, is completely different.

Let $P(n)$ denote the set of prime numbers p with $2 \leq p \leq n$. For the moment, fix n arbitrarily. For each $p \in P(n)$, we select an $\mathbb{F}_p$-linear secret sharing scheme with secret-space dimension 1 and "small" share-space dimension. We construct these schemes from linear codes as in [11], i.e., via codes with large distance as well as large dual distance (but, in the present case, without consideration of multiplicative properties). We also fix generator matrices for each, or, more precisely, monotone span programs. The privacy and reconstruction parameters are designed such that they match (sufficiently well) with the desired values t, r in each case. Note that this influences the constant in share-space dimension; e.g., if this constant was just 1, then this upperbounds the achievable r, t just on account of (dual-) distance bounds on binary linear codes.

Now, we glue these $|P(n)|$ schemes together in two steps: First, we apply *Chinese Remaindering* to the monotone span programs at hand, and second, we *arbitrarily lift* the result to the integers. Somewhat surprisingly, as a result, we obtain a weak-BBSS with t-privacy and r-reconstruction of a λ-multiple of the secret, where λ is an integer *coprime* with Δ. Indeed, this is by no means obvious since, at face value, this procedure does not even seem to account for behavior over groups whose order is (divisible by) a *power* of a prime in $P(n)$, a class of groups that is obviously infinite for each n. But still we get around this issue thanks to novel, nontrivial ideas on lifting of linear secret sharing over finite fields to rings while preserving the relevant parameters. In the particular case of ours here, that means lifting schemes over $\mathbb{F}_p$ to schemes over $\mathbb{Z}/p^k\mathbb{Z}$; this is a key ingredient for making our local-global approach work, i.e., this allows to reduce the "global" problem to addressing, for each n, just a *finite* number of "local" problems.

As for recovering $\log n$ expansion for *threshold* BBSS, we may work with Shamir's scheme defined over a large enough extension of a prime field $\mathbb{F}_p$ with $p \in L(n)$ and turn it into a linear scheme over $\mathbb{F}_p$ in a standard way; simply "expand" extension field elements into coordinate-vectors over the base field, after selection of a basis; this turns out to work for our purposes. Since, in this case, we need threshold secret sharing over e.g. $\mathbb{F}_2$ in particular, it is clear that share-space dimension (over $\mathbb{F}_2$) will be $\log n$ in the worst case (as we go through $L(n)$). Note that the expansion achieved here matches exactly that of the number-theoretic approach from [12]. We do not necessarily say that the approach for threshold-BBSS in the present paper is conceptually/technically simpler than that of [12]: each feels "mathematically right" albeit seen from different standpoints. However, the result in [14], also number-theoretic and more intricate than [12], is still better by an *additive* constant.

Finally, we get to our claim on *expansionless, flexible near-threshold* BBSS, which is *not* attainable by previous methods as we have argued. We choose, for each prime p, linear secret sharing schemes over $\mathbb{F}_p$ with appropriate asymptotic properties. Here, asymptotic theory of linear codes comes into play here; asymptotic results from [11] show at once that all the necessary connections can be made. Indeed, by choosing a large enough *fixed* extension of a base field $\mathbb{F}_p$, one gets, asymptotically, that distance and dual distance can be concentrated around an arbitrary constant fraction of n, with the difference between distance and dual distance being an arbitrarily small constant fraction of n. This translates into similar properties for t-privacy and r-reconstruction in corresponding linear secret sharing schemes with share-space of constant dimension over the base field. As in the threshold case, schemes over extension fields are turned into schemes over the base field in a standard way.

It is for these reasons that we can achieve expansionless, flexible near-threshold BBSS. The gluing procedure is then by a form of diagonalization. I.e., index rows by the positive integers n and index the columns by the prime numbers. In location (n, p), we have a linear secret sharing scheme over $\mathbb{F}_p$ supporting n players and achieving the desired privacy and reconstruction. Then, for each n, we glue along the n-th row "up to the diagonal," i.e., up to location (n, p) where p is the largest prime $p \leq n$. Finally, for the compound BBSS to be explicit (poly-time) the underlying codes are required to be explicit. This means we need to resort to algebraic-geometric codes (AG). However, the latter cannot be taken off-the-shelf since we need to ensure that the compound BBSS works for each and every n and achieves the desired parameters. This leads us to handcraft the required AG-codes. In addition, we encounter several technical issues of parameter fine-tuning that have been suppressed in our overview for sake of brevity but that are still necessary for our approach.

1.4 Brief remarks on possible protocol applications

Though our primary purpose here is to advance the theoretical state of the art in BBSS, we briefly address some potential applications. Threshold-RSA [15] was eventually realized very effiently without recourse to BBSS, exploiting specifics of RSA not generally present in cryptosystems over groups with secret of hard to compute order. Very briefly, "Shamir-sharing over the integers" can be used here for the purpose of practical threshold-RSA signatures [34]. Even though only reconstruction of a *multiple* of the secret can be guaranteed when doing so, this works for RSA if the constant scalar in this multiple is co-prime both to the public exponent and to the order of the (sub-group) of the "RSA-group" in question. The latter is by forcing existence of an easily accessible constant-index subgroup of the "RSA-group" whose order only has very large prime factors (implied by requiring prime factors of RSA-modulus to be Sophie Germain) and the former by requiring that the public exponent is a prime exceeding the number of players.

By applying our techniques for expansionless near-threshold BBSS to practical ranges of n (making some practical substitutions for the codes), one may, in principle remove the lower bound condition on the public exponent, with the benefit of rendering faster signature verification, while maintaining "practicality" and active security. In case of passive security only, the Sophie Germain requirement may also be removed. Note that, in the active case, the Sophie German condition facilitates the efficient zero knowledge proofs of correct "partial verification" in the style of Schnorr-proofs with exponentially large challenge space for exponentially small error probability in a single run. Without that condition one would have to resort to repetition of proofs supporting a 1-bit challenge space only (so error 1/2 per run), leading to efficiency loss. However, using amortization techniques for zero knowledge [8], this effect can be neutralized if many statement are proven simultaneously. Thus, if many signatures are verified simultaneously, we may also remove the Sophie-Germain condition in the active case. Alternatively, we may thus also consider deploying these ideas towards improved threshold-RSA *decryption*. We suggest that this all merits further study.

Moreover, in [18], ISPs are shown to imply "integer linear secret sharing" with statistical privacy, by selecting secret and randomness from an appropriately large bounded range of integers instead of blackbox groups. Clearly, ISPs allow for full secret-reconstruction, not just a multiple. Known applications are to threshold cryptosystems based on class groups. [8] Also results also apply directly here. We believe there are other useful applications, for instance in MPC over the integers. [9] This may offer advantages for certain functions, compared to methods which emulate integer operations by first working over e.g. finite fields. But more research is needed still for this to be conclusive,

1.5 Organization of the paper

In Section 2, we introduce monotone span programs and near-threshold black-box secret sharing schemes. We also show how to lift a monotone span programs modulo prime powers to a monotone span program over $\mathbb{Z}$. In Section 3, we show a lower bound on expansion factor on near-threshold black-box secret sharing schemes. This generalizes the lower bound on threshold black-box secret sharing schemes. Section 4 presents our glue technique that glues a Vandermonde matrix with a generator matrix modulo an integer. Section 5 shows how to construct a generator matrix over $\mathbb{Z}$ that gives a linear code with both good minimum distance and dual minimum distance modulo every small prime p. The last section collects the results prepared in the previous sections to form our main result of this paper.

2 Monotone span programs and near-threshold black-box secret sharing schemes

Throughout the paper, we denote by $[n]$ the set $\{1, 2, 3, \cdots, n\}$. We denote by $2^{[n]}$ the set of all subsets of $[n]$. Then $2^{[n]}$ has size 2^n.

2.1 Monotone span program

Monotone span programs (MSP for short) over finite fields were introduced by Karchmer and Wigderson [24]. Monotone span program is an efficient tool to construct linear secret sharing

[8] Whereas these seemed out of fashion for some time, they appear to be making a comeback in the blockchain context presently.

[9] a topic which, surprisingly, has not seen much attention lately, especially given the surge in MPC research

scheme (LSSS for short) for a given access structure. It is well known that there is a one-to-one correspondence between monotone span programs over finite fields with linear secret sharing schemes over finite fields (see e.g. [2, 19]). Monotone span programs over rings (in particular over integers $\mathbb{Z}$) were introduced in [12, 14] and it turns out that they have a similar correspondence with black-box secret sharing schemes. In addition, monotone span programs over rings are the basis for multi-party computation over black-box rings, as studied in [13]. In particular, the techniques of [9] for secure multiplication and VSS apply to this flavor of monotone span program as well.

Definition 1. The pair (Γ, Δ) with $\Gamma, \Delta \subseteq 2^{[n]}$ is called an access structure on $[n]$ if $\emptyset \in \Delta$, $[n] \in \Gamma$ and $\Gamma \cap \Delta = \emptyset$. Furthermore, it is called a monotone access structure if Γ is monotonously increasing and Δ is monotonously decreasing, i.e.,

(i) if $T_1 \in \Gamma$ and $T_1 \subseteq T_2$, then $T_2 \in \Gamma$;

(ii) if $S_1 \in \Delta$ and $S_2 \subseteq S_1$, then $S_2 \in \Delta$.

A monotone increasing set Γ can be efficiently described by the set Γ^- consisting of the minimal elements (sets) in Γ, i.e., the elements in Γ for which no proper subset is also in Γ. Similarly, the set Δ^+ consists of the maximal elements (sets) in Δ, i.e., the elements in Δ for which no proper superset is also in Δ. It is obvious that (Γ^-, Δ^+) generates a monotone access structure (Γ, Δ), i.e., Γ consists of subsets of $[n]$ containing an element of Γ^- and Δ consists of subsets of $[n]$ that are contained in an element of Δ^+.

Definition 2. A monotone access structure (Γ, Δ) is said to be complete if $\Gamma \cup \Delta = 2^{[n]}$. Let $t, r, n \in \mathbb{Z}$ with $0 < t < r < n$. Then $\mathfrak{R}_{t,r,n} = (\Delta_{t,n}, \Gamma_{r,n})$ is defined to be the access structure satisfying

(i) $\Delta_{t,n} = \{S \subseteq [n] : \ |S| \leq t\}$, and

(ii) $\Gamma_{r,n} = \{T \subseteq [n] : \ |T| \geq r\}$.

Thus, if $r = t+1$, then $\mathfrak{R}_{t,r,n}$ is complete. In this case, we say that it is a threshold access structure and denote $\mathfrak{R}_{t,t+1,n}$ by $\mathfrak{R}_{t,n}$.

We provide necessary and sufficient conditions under which a (Γ, Δ)-scheme is a black-box secret sharing scheme for (Γ, Δ) . This is a generalization of threshold monotone span programs over rings introduced in [12], where the latter was a generalization of monotone span program over finite fields introduced by Karchmer and Wigderson [24]. We will show that monotone span programs in this paper have a similar correspondence with black-box secret sharing schemes.

Let R be a ring and let (Γ, Δ) be a monotone access structure on $[n]$ and $M \in R^{h \times e}$ with $h \geq n$. We define a surjective function $\Psi : \ [h] \rightarrow [n]$ to group the rows of M. We say that "the j-th row is labelled by $\Psi(j)$" or "$\Psi(j)$ owns the j-th row." For any $S \subseteq [n]$, we write M_S to denote the sub-matrix of M obtained from the rows owned by $i \in S$. Denote by h_S the number of rows of M_S. For any vectors $\mathbf{x}$ of length n, we define $\mathbf{x}_S$ analogously. Furthermore, for each $S \in \Gamma$, there exists a vector $\boldsymbol{\lambda}(S) \in R^{h_S}$ which is called a reconstruction vector. Denote by $\mathcal{R}$ the collection of reconstruction vectors. We denote by $\mathcal{B}$ the quadruple $(R, M, \Psi, \mathcal{R})$. Throughout this paper, all vectors are row vectors and we denote by $\mathbf{u}'$ the transpose of a vector $\mathbf{u}$.

Definition 3. A Monotone Span Program (MSP) $\mathcal{M}$ over a ring R is a quadruple $(R, M, \Psi, \boldsymbol{\mu}_e)$, where M is a matrix over R (with h rows and $n \le h$ columns), $\Psi : [h] \to [n]$ is a surjective function and $\boldsymbol{\mu}_e = (1, 0, 0, \ldots, 0) \in R^e$ is a vector that is called the target vector. The size of $\mathcal{M}$ is the number h of rows of M and is denoted as size$(\mathcal{M})$. If $R = \mathbb{Z}$, we call it an integer monotone span program. The expansion factor of $\mathcal{M}$ is defined to be the ratio h/n, where h is the number of rows of M.

Definition 4. Let R be a ring and let (Γ, Δ) be a monotone access structure on $[n]$. We say that a monotone span program $\mathcal{M} = (R, M, \Psi, \boldsymbol{\mu}_e)$ computes (Γ, Δ) if

(P1) for any $S \in \Gamma$, $\boldsymbol{\mu}_e \in \mathrm{im}(M'_S)$, where M'_S is the transpose of M_S and $\mathrm{im}(M'_S)$ stands for the row space of M_S; and

(P2) for any $T \in \Delta$, there exists a vector $\boldsymbol{\lambda} \in R^e$ with the first coordinate $\lambda_1 = 1$ such that $M_T \boldsymbol{\lambda}' = \mathbf{0}'$.

As noted in [12], if R is a field, then $\boldsymbol{\mu}_e \notin \mathrm{im}(M'_S)$ implies that there exists a vector $\boldsymbol{\lambda} \in R^e$ with the first coordinate $\lambda_1 = 1$ such that $M_S \boldsymbol{\lambda}' = \mathbf{0}'$. If R is not a field this does not necessarily hold.

Using representations of monotone access structures as monotone Boolean formulas and using induction in a similar style as in [20], it is straightforward to verify that for every monotone access structure (Γ, Δ), there is an integer monotone span program that computes (Γ, Δ).

Lemma 1. *A monotone span program $\mathcal{M} = (R, M, \Psi, \boldsymbol{\mu}_e)$ computes (Γ, Δ) if and only if*

(R1) for any $S \in \Gamma$, the equation $\mathbf{x} M_S = \boldsymbol{\mu}_e$ is solvable in R;

(R2) for any $T \in \Delta$, the equation $\binom{\boldsymbol{\mu}_e}{M_T} \mathbf{x} = \boldsymbol{\mu}'_{h_T+1}$ is solvable in R.

Proof. It is clear that (P1) and (R1) are equivalent. To see the equivalence of (P2) and (R2), we note that $\boldsymbol{\mu}_e \cdot \mathbf{x} = 1$ implies that the first coordinate of $\mathbf{x}$ is 1. □

The above result converts a monotone span program $\mathcal{M} = (R, M, \Psi, \boldsymbol{\mu}_e)$ computing (Γ, Δ) to solvability of linear equations in R. If R is the integer ring, then we can reduce solvability of linear equations in $\mathbb{Z}$ to solvability of linear equations in $\mathbb{Z}_{p^\ell}$ for every prime p and integer $\ell \ge 1$.

Lemma 2. *Let $N \in \mathbb{Z}^{m \times n}$ and $\mathbf{b} \in \mathbb{Z}^m$. Then $N\mathbf{x}' = \mathbf{b}'$ is solvable over $\mathbb{Z}$ if and only if it is solvable over $\mathbb{Z}_{p^\ell}$ for all prime p and integer $\ell \ge 1$.*

Proof. The "only if" part is clear.

Now we prove the "if" part. By [12, Lemma 1], it is sufficient to show that $N\mathbf{x}' = \mathbf{b}'$ is solvable modulo k for every integer $k \ge 2$. Let k have the canonical factorization $k = \prod_{i=1}^{r} p_i^{e_i}$. Assume that $\mathbf{u}_i$ is a solution of $N\mathbf{x}' \equiv \mathbf{b}' \pmod{p_i^{e_i}}$. By the Chinese Remainder Theorem, we can find a vector $\mathbf{u} \in \mathbb{Z}_k$ such that $\mathbf{u} \equiv \mathbf{u}_i \pmod{p_i^{e_i}}$. This implies that $\mathbf{u}$ is a solution of $N\mathbf{x}' \equiv \mathbf{b}' \pmod{k}$. □

Theorem 1. *Let (Γ, Δ) be a monotone access structure on $[n]$. Then $\mathcal{M} = (\mathbb{Z}, M, \Psi, \boldsymbol{\mu}_e)$ is a monotone span program computing (Γ, Δ) if and only if $\mathcal{M}_{p^\ell} = (\mathbb{Z}_{p^\ell}, M, \Psi, \boldsymbol{\mu}_e)$ is a monotone span program computing (Γ, Δ) for every prime p and integer $\ell \ge 1$, where M and $\boldsymbol{\mu}_e$ in $\mathcal{M}_p$ are viewed as a vector and a matrix modulo p^ℓ, respectively.*

Proof. Assume that $\mathcal{M} = (\mathbb{Z}, M, \Psi, \boldsymbol{\mu}_e)$ is a monotone span program computing (Γ, Δ). By taking modulo p^ℓ, we can easily show that $\mathcal{M}_p = (\mathbb{Z}_{p^\ell}, M, \Psi, \boldsymbol{\mu}_e)$ is a monotone span program computing (Γ, Δ) for every prime p and integer $\ell \geq 1$.

Now we prove the other direction. By Lemma 1, the conditions (R1) and (R2) are satisfied for $R = \mathbb{Z}_{p^\ell}$ for every prime p and integer $\ell \geq 1$. By Lemma 2, the conditions (R1) and (R2) are satisfied for $R = \mathbb{Z}$. By Lemma 1 again, $\mathcal{M} = (\mathbb{Z}, M, \Psi, \boldsymbol{\mu}_e)$ is a monotone span program computing (Γ, Δ). □

This is an interesting mathematical result that obeys the local-global principle, also known as the Hasse principle. In mathematics (in particular number theory), the local-global principle says that a phenomenon is true globally if and only if it is true locally. A well-known example obeying this the local-global principle is the Hasse-Minkowski theorem which states that the local-global principle holds for the problem of representing 0 by quadratic forms over the rational numbers. Of course, there are also some examples that do not obey the local-global principal. A counterexample by Ernst S. Selmer shows that the Hasse-Minkowski theorem cannot be extended to forms of degree 3 (see [29, pp.250-258]).

Theorem 1 is a bridge to connect integer monotone span programs with monotone span programs over p^ℓ. This in turns allows us to construct integer monotone span programs via monotone span programs over finite fields.

Theorem 2. *Let (Γ, Δ) be a monotone access structure on $[n]$. Let p be a prime and let $(\mathbb{Z}_p, M, \Psi)$ be a triple defined in Subsection 2.1. If $M \in \mathbb{Z}_p^{h\times e}$ and*

(O1) for any $S \in \Gamma$, the $\mathbb{F}_p$-rank of M_S is e; and

(O2) for any $T \in \Delta$, the $\mathbb{F}_p$-rank of N_T is h_T, where N is the $n \times (e-1)$ matrix obtained from M by removing the first column,

Then for any integer $\ell \geq 1$, $(\mathbb{Z}_{p^\ell}, M^{(\ell)}, \Psi, \boldsymbol{\mu}_e)$ a monotone span program computing (Γ, Δ), where $M^{(\ell)}$ is viewed as a lifting of M modulo p^ℓ.

Proof. By Lemma 1, it is sufficient to show that the conditions (R1) and (R2) hold for the quadruple $(\mathbb{Z}_{p^\ell}, M^{(\ell)}, \Psi, \boldsymbol{\mu}_e)$. Let $S \in \Gamma$, then by (O1) the $\mathbb{F}_p$-rank of M_S is e, there is an $e \times e$ submatrix A of M_S such that $\det(A) \not\equiv 0 \mod p$. This implies that $A \pmod{p^\ell}$ is invertible. Thus, there exists a vector $\mathbf{u} \in \mathbb{Z}_{p^\ell}^e$ such that $\mathbf{u}A \equiv \boldsymbol{\mu}_e \pmod{p^\ell}$. Without loss of generality, we may assume that $M^{(\ell)} = \binom{A}{C}$ for some $(h-e) \times e$ matrix C over $\mathbb{F}_q$. Then $(\mathbf{u}, \mathbf{0})M^{(\ell)} = (\mathbf{u}, \mathbf{0})\binom{A}{C} = \mathbf{u}A \equiv \boldsymbol{\mu}_e \pmod{p^\ell}$. This proves $(R1)$ for the quadruple $(\mathbb{Z}_{p^\ell}, M^{(\ell)}, \Psi, \boldsymbol{\mu}_e)$.

Let $M = (\mathbf{b}'|N)$. By (O2), for any $T \in \Delta$, the $\mathbb{F}_p$-rank of N_T is h_T. Hence, there is an $h_T \times h_T$ submatrix E of N_T such that $\det(E) \not\equiv 0 \mod p$. This implies that $E \pmod{p^\ell}$ is invertible. Thus, there exists a vector $\mathbf{v} \in \mathbb{Z}_{p^\ell}^{h_T}$ such that $E\mathbf{v}' \equiv -\mathbf{b}' \pmod{p^\ell}$. Without loss of generality, we may assume that $M_T^{(\ell)} = (\mathbf{b}'|E, F)$. Then $M_T^{(\ell)}(1, \mathbf{v}, \mathbf{0})' = (\mathbf{b}'|E, F)(1, \mathbf{v}, \mathbf{0})' = \mathbf{b} + E\mathbf{v}' = \mathbf{0} \pmod{p^\ell}$. This proves $(R2)$ for the quadruple $(\mathbb{Z}_{p^\ell}, M^{(\ell)}, \Psi, \boldsymbol{\mu}_e)$. □

We are interested in the smallest size of a monotone span program $\mathcal{M}$ computing (Γ, Δ). This is because this number determines the secret size (see Theorem).

Definition 5. For a given (Γ, Δ), denote by $\mathrm{msp}_R(\Gamma, \Delta)$ the smallest size of a monotone span program $\mathcal{M}$ over R computing (Γ, Δ). We also denote $\mathrm{msp}_{\mathbb{Z}}(\Gamma, \Delta)$ by $\mathrm{msp}(\Gamma, \Delta)$.

The main purposes of this papers are (i) to derive a lower bound on $\mathrm{msp}(\Gamma, \Delta)$; and more importantly (ii) to explicitly construct an MSP over $\mathbb{Z}$ with expansion factor achieving this lower bound up to a constant multiplicative factor.

2.2 Black-box secret sharing scheme

In this subsection, we will prove a one-to-one correspondence between black-box secret sharing schemes and integer monotone span programs. Now we introduce black-box secret sharing schemes.

Definition 6. Let (Γ, Δ) be a monotone access structure on $[n]$. A black-box secret sharing scheme (BBSSS for short) for (Γ, Δ) is a quadruple $\mathcal{B} = (\mathbb{Z}, M, \Psi, \mathcal{R})$ defined in Subsection 2.1 satisfying the following requirement. Let G be an arbitrary finite Abelian group and $S \subseteq [n]$ be a non-empty set. For a uniformly distributed $s \in G, \mathbf{g} = (g_1, \cdots, g_e) \in G^e$ given that $g_1 = s$, define $\mathbf{s} = \mathbf{g}M' \in \mathbb{Z}^h$. Then:

(Q1) (Completeness) If $S \in \Gamma$, then $\boldsymbol{\lambda}(S) \cdot \mathbf{s}'_S = s$ with probability 1.

(Q2) (Privacy) If $T \in \Delta$, then $\mathbf{s}_T$ contains no Shannon information on s.

If $(\Gamma, \Delta) = \mathfrak{R}_{t,r,n}$, we say $\mathcal{B}$ is a near-threshold black-box secret sharing scheme with privacy t and reconstruction r. Furthermore, if $(\Gamma, \Delta) = \mathfrak{R}_{t,n}$, we say $\mathcal{B}$ is a threshold black-box secret sharing scheme.

In [12], it was proved that there is a one-to-one correspondence between threshold black-box secret sharing schemes and integer monotone span programs. We also note that [12] gives a characterization on threshold black-box secret sharing schemes.

Theorem 3. *Let (Γ, Δ) be a monotone access structure on $[n]$. Then there is a black-box secret sharing scheme $\mathcal{B} = (\mathbb{Z}, M, \Psi, \mathcal{R})$ for (Γ, Δ) if and only if there exists an integer monotone span program $\mathcal{M} = (\mathbb{Z}, M, \Psi, \boldsymbol{\mu}_e)$ computing (Γ, Δ).*

Proof. Assume that $\mathcal{M} = (\mathbb{Z}, M, \Psi, \boldsymbol{\mu}_e)$ is an integer monotone span program computing (Γ, Δ), i.e., the conditions (P1) and (P2) are given. Now we want to show that the conditions (Q1) and (Q2) are satisfied.

Let us fix a finite Abelian group G. Sample $s \in G$ uniformly at random and sample $\mathbf{g} = (s, g_2, \cdots, g_e)$ uniformly at random from $\{s\} \times G^{e-1}$. Lastly, let $\mathbf{s} = \mathbf{g}M'$. Let $S \in \Gamma$, by (P1), there exists a vector $\mathbf{u} \in \mathbb{Z}^{h_S}$ such that $\mathbf{u}M_S = \boldsymbol{\mu}_e$. This gives $s = \boldsymbol{\mu}_e \cdot \mathbf{g}' = (\mathbf{u}M_S) \cdot \mathbf{g}' = \mathbf{u} \cdot \mathbf{s}'_S$. To prove (Q2), we have to show that for any $T \in \Delta$ and any $s_1, s_2 \in G$, given a vector $\mathbf{g}_1 \in \mathbb{Z}^e$ with the first coordinate of $\mathbf{g}_1$ equal to s_1, there exists $\mathbf{g}_2$ such that s_2 is the first coordinate of $\mathbf{g}_2$ and $M_T\mathbf{g}'_1 = M_T\mathbf{g}'_2$. Let $\mathbf{v} \in \mathbb{Z}^e$ with the first coordinate equal to 1 such that $M_T\mathbf{v}' = \mathbf{0}'$. Put $\mathbf{g}_2 = \mathbf{g}_1 + (s_2 - s_1)\mathbf{v}$. Then the first coordinate of $\mathbf{g}_2$ is s_2. Furthermore, we have $M_T\mathbf{g}'_2 = M_T(\mathbf{g}_1 + (s_2 - s_1)\mathbf{v})' = M_T\mathbf{g}'_1 + (s_2 - s_1)M_T\mathbf{v}' = M_T\mathbf{g}'_1$.

Now we prove the other direction. We prove one by one. For any $S \in \Gamma$, let $\boldsymbol{\lambda}(S) \in \mathcal{R}$. Choose a prime p such that p is bigger than all entries of $\boldsymbol{\lambda}(S)M_S$. Set $G = \mathbb{Z}_p$ and let $\mathbf{g}_i \in G^e$ be the vector such that the ith position of $\mathbf{g}_i$ is 1 and the rest are 0. Then for $j \in [e]$, we have

$$\delta_{1,j} \equiv \boldsymbol{\lambda}(S)M_S\mathbf{g}_i' \pmod{p},$$

where $\delta_{1,j}$ is the Kronecker-delta function. Combining these e equations together, we obtain $\boldsymbol{\mu}_e \equiv \boldsymbol{\lambda}(S)M_S \pmod{p}$. As p is bigger than all entries of $\boldsymbol{\lambda}(S)M_S$, we get $\boldsymbol{\mu}_e = \boldsymbol{\lambda}(S)M_S \in \mathrm{im}(\mathrm{M})$.

Suppose that $T \in \Delta$. Recall that we want to show the existence of $\mathbf{v} = (1, v_2, \cdots, v_e) \in \mathbb{Z}^e$ such that $M_T\mathbf{v}' = \mathbf{0}'$. Let $M_T = (\mathbf{b}'|N_T)$, where $\mathbf{b}' \in \mathbb{Z}^{h_T}$ is the first column of M_T and $N_T \in \mathbb{Z}^{h_T \times (e-1)}$. Then the existence of such $\mathbf{v}$ is equivalent to the solvability of $-\mathbf{b}' = N_T\mathbf{x}$ in $\mathbb{Z}$. So by Lemma 2, to show that $-\mathbf{b}' = N_T\mathbf{x}$ is solvable over $\mathbb{Z}$, it is equivalent to showing that it is solvable modulo k for any integer $k \geq 2$.

Fix $k \geq 2$ and set $G = \mathbb{Z}_k$. Now for $T \in \Delta$, it follows from the privacy condition (Q2) that there exists $\mathbf{g}_1 \in \mathbb{Z}^e$ such that the first coordinate of $\mathbf{g}_1$ is $s - 1$ and $\mathbf{g}_1(M_T)' = \mathbf{g}(M_T)'$. Setting $\mathbf{v} = \mathbf{g} - \mathbf{g}_1$, Then the first coordinate of $\mathbf{v}$ is 1 and $M_T\mathbf{v}' = \mathbf{0}'$, i.e., $-\mathbf{b}' = N_T\mathbf{x}$ is solvable over $\mathbb{Z}_k$. □

Definition 7. Let (Γ, Δ) be a monotone access structure on $[n]$. The expansion factor ϱ of a black-box secret sharing scheme $\mathcal{B} = (\mathbb{Z}, M, \Psi, \mathcal{R})$ for (Γ, Δ) is defined to be the ratio $\frac{h}{n}$, where h is the number of rows of M.

3 A lower bound on expansion factors

In this section, we are going to derive a lower bound on the expansion factor so that we know how far our construction of BBSSS is away from optimality. The idea is to obtain a lower bound on monotone span programs over finite fields $\mathbb{F}_p$ for primes p. As an integer monotone span program gives rise to a monotone span program modulo a prime with the same expansion factor, any lower bound on expansion factors of monotone span programs modulo primes is also a lower bound on integer monotone span programs. As one can expect, the worst lower bound on expansion factors of monotone span programs are from modulo 2. Thus, by deriving a lower bound on monotone span programs modulo 2 for the access structure $\mathfrak{R}_{t,r,n}$, we obtain a lower bound on the expansion factor of BBSSS.

Let write $\mathrm{msp}_2(\Gamma, \Delta)$ for $\mathrm{msp}_{\mathbb{F}_2}(\Gamma, \Delta)$. We first provide a lower bound on $\mathrm{msp}_2(\mathfrak{R}_{1,r,n})$.

Proposition 3. *One has* $\mathrm{msp}_2(\mathfrak{R}_{1,r,n}) \geq n \log \frac{n}{r-1}$.

Proof. Let $\mathcal{M} = (\mathbb{Z}_2, M, \Psi, \boldsymbol{\mu}_e)$ be a monotone span program computing $\mathfrak{R}_{1,r,n}$. For $M \in \mathbb{Z}_2^{h \times e}$, we write $M_i \in \mathbb{Z}_2^{h_i \times e}$ and h_i to represent $M_{\{i\}}$ and $h_{\{i\}}$, respectively. Since we are going to find a lower bound on h, we want to bound them when h_i is minimized. So we assume that all rows of M_i are $\mathbb{Z}_2$-linearly independent for any $1 \leq i \leq n$.

Define $H_0 = \{(0, v_2, \cdots, v_e) \in \mathbb{Z}_2^e\}$ and $H_1 = \{(1, v_2, \cdots, v_e) \in \mathbb{Z}_2^e\}$. Since $\{i\} \in \Delta(\mathfrak{R}_{1,r,n})$, there exists $\mathbf{c} \in \ker(M_i)$ with the first coordinate equal to 1, where $\ker(M_i)$ denotes the solution space of $M_i\mathbf{x}' = \mathbf{0}'$. Hence, $\ker(M_i) \cap H_1 \neq \emptyset$. We claim that $|\ker(M_i) \cap H_0| = |\ker(M_i) \cap H_1| = 2^{e-1-h_i}$. Note that $\ker(M_i) \subseteq H_0 \cup H_1 = \mathbb{Z}_2^e$ and $|\ker(M_i)| = 2^{h_i}$. To prove our claim, it is sufficient to show that $|\ker(M_i) \cap H_0| = |\ker(M_i) \cap H_1|$. This is true as one can easily verify that $\mathbf{c} + \ker(M_i) \cap H_0 = |\ker(M_i) \cap H_1$.

Let S be a subset of $[n]$ of size r, we have $S \in \Gamma(\mathfrak{R}_{1,r,n})$. Thus, $\boldsymbol{\mu}_e$ belongs to $\mathrm{im}(M'_S)$. In other words, the first column of M_S is not a linear combination of the others. This implies that $\ker(M_S) \cap H_1 = \emptyset$. This means that for any $\mathbf{v} \in H_1$, it can appears in $\ker(M_i) \cap H_1$ for at most $(r-1)$ of $i \in S$. This gives the following inequality

$$(r-1)2^{e-1} = (r-1)|H_1| \geq \sum_{i=1}^{n} |\ker(M_i) \cap H_1| = \sum_{i=1}^{n} 2^{e-1-h_i},$$

i.e., $\sum_{i=1}^{n} 2^{-h_i} \leq r-1$.

Recall that by the Log Sum Inequality, for any non-negative $a_1, \cdots, a_n, b_1, \cdots, b_n$, we have

$$\sum_{i=1}^{n} a_i \log \frac{a_i}{b_i} \geq a \log \frac{a}{b},$$

where $a = \sum_{i=1}^{n} a_i$ and $b = \sum_{i=1}^{n} b_i$. Let $a_i = 1$ and $b_i = 2^{-h_i}$. Then $a = n$ and $b = \sum_{i=1}^{n} 2^{-h_i} \leq r-1$. Then

$$h = \sum_{i=1}^{n} h_i = \sum_{i=1}^{n} 1 \cdot \log \frac{1}{2^{-h_i}} \geq n \log \frac{n}{\sum_{i=1}^{n} 2^{-d_i}} \geq n \log \frac{n}{r-1}.$$

□

To find lower bounds on the expansion factor of the access structure $\mathfrak{R}_{t,r,n}$, let us consider the dual of $\mathfrak{R}_{t,r,n}$.

Definition 8. The dual (Γ^*, Δ^*) of a monotone access structure (Γ, Δ) on $[n]$ is defined by

(i) $\Delta^* = \{T \subseteq [1,n] : \bar{T} \in \Gamma\}$, where $\bar{T}$ is the complement of T, i.e., $(\bar{T}) = [n] \setminus T$.

(ii) $\Gamma^* = \{S \subseteq [1,n] : \bar{S} \in \Delta\}$.

It is easy to verify that (Γ^*, Δ^*) is a monotone access structure $[n]$ as long as (Γ, Δ) is.

Remark 1. One has $\mathfrak{R}^*_{t,r,n} = \mathfrak{R}_{n-r-1,n-t-1,n}$.

Lemma 4 (See [24])**.** *For any finite field* $\mathbb{F}$ *and monotone access structure* (Γ, Δ), *we have the equality* $\mathrm{msp}_{\mathbb{F}}(\Gamma, \Delta) = \mathrm{msp}_{\mathbb{F}}(\Gamma^*, \Delta^*)$.

Remark 2. It follows from Lemma 4 that $\mathrm{msp}_{\mathbb{F}}(\mathfrak{R}_{t,r,n}) = \mathrm{msp}_{\mathbb{F}}(\mathfrak{R}_{n-t-1,n-r-1,n})$. Thus, to find $\mathrm{msp}_{\mathbb{F}}(T_{t,r,n})$, we can always assume that $r \geq \frac{n-1}{2}$.

Theorem 4. $\mathrm{msp}_2(\mathfrak{R}_{t,r,n}) \geq n \log \frac{n+1}{2(r-t)}$.

Proof. By Remark 2, we may assume that $r \geq \frac{n-1}{2}$. Consider any MSP $\mathcal{M} = (\mathbb{F}_2, M, \Psi, \epsilon)$ computing $\mathfrak{R}_{t,r,n}$. Without loss of generality, we may assume that $h_1 \leq h_2 \leq \cdots \leq h_n$. It is clear that $(M'_1|M'_2|\cdots|M'_{r+1})'$ is an MSP computing $\mathfrak{R}_{t,r,r+1}$. So we have $\sum_{i=1}^{r+1} h_i \geq \mathrm{msp}_2(\mathfrak{R}_{t,r,r+1})$. Note that for any $j > r+1, h_j \geq h_{r+1} \geq \frac{\mathrm{msp}_2(\mathfrak{R}_{t,r,r+1})}{r+1}$. Hence,

$$\begin{aligned} h &= \sum_{i=1}^{r+1} h_i + \sum_{j=r+2}^{n} h_i \geq \mathrm{msp}_2(\mathfrak{R}_{t,r,r+1}) + \frac{n-(r+1)}{r+1}\mathrm{msp}_2(\mathfrak{R}_{t,r,r+1}) \\ &= \frac{n}{r+1}\mathrm{msp}_2(\mathfrak{R}_{t,r,r+1}). \end{aligned}$$

This gives

$$\begin{aligned}\mathrm{msp}_2(\mathfrak{R}_{t,r,n}) &\geq \frac{n}{r+1}\mathrm{msp}_2(\mathfrak{R}_{t,r,r+1}) = \frac{n}{r+1}\mathrm{msp}_2(\mathfrak{R}_{1,r-t,r+1}) \\ &\geq n\log\frac{r+1}{r-t} \geq n\log\frac{n+1}{2(r-t)}\end{aligned}$$

and the proof is completed. □

By considering modulo 2, we obtain the following lower bound.

Theorem 5. *For all integers r, t, n with $0 < t < r < n, \mathrm{msp}(\mathfrak{R}_{t,r,n}) \geq n \cdot \log \frac{n+1}{2(r-t)}$.*

4 Gluing method

In Subsection 2.1, we witnessed that an integer monotone span program obeys the local-global principle. Thus, given an access structure $\mathfrak{R}_{t,r,n}$, construction of an integer monotone span program computing $\mathfrak{R}_{t,r,n}$ is equivalent to construction of a monotone span program computing $\mathfrak{R}_{t,r,n}$ modulo every prime power. However, it is usually not easy to directly construct an integer monotone span program computing $\mathfrak{R}_{t,r,n}$ that is also a monotone span program computing $\mathfrak{R}_{t,r,n}$ modulo every prime power. On the other hand, it is much easier to develop a monotone span program computing $\mathfrak{R}_{t,r,n}$ modulo one given prime power. Thus, by the Chinese Remainder Theorem, for any given finite number n, we can lift monotone span programs computing $\mathfrak{R}_{t,r,n}$ modulo all prime $p \leq n$ to an integer monotone span program. The question is how to make it into an integer monotone span program modulo all prime $p > n$.

Our idea is to glue two integer monotone span programs, one is a monotone span program modulo primes $p \leq n$ and other one modulo primes $p > n$. The first one can be obtained by lifting monotone span programs modulo every prime power $p \leq n$. The other one can be constructed via an integer Vandermonde matrix. As a result, the integrated matrix gives an integer monotone span program that is also a monotone span program modulo every prime power. Hence, by the local-global principal, we obtain an integer monotone span program.

For positive integers $x_1, x_2, \ldots, x_n$, let us define the Vandermonde matrix

$$\Delta_i(x_1, x_2, \ldots, x_n) = \begin{pmatrix} x_1^i & x_1^{1+i} & x_1^{2+i} & \ldots & x_1^{n-1+i} \\ x_2^i & x_2^{1+i} & x_2^{2+i} & \ldots & x_2^{n-1+i} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_n^i & x_n^{1+i} & x_n^{2+i} & \ldots & x_n^{n-1+i} \end{pmatrix}.$$

We further denote by $\delta(x_1, x_2, \ldots, x_n)$ the determinant of $\Delta_1(x_1, x_2, \ldots, x_n)$, i.e., $\delta(x_1, x_2, \ldots, x_n) = \left(\prod_{i=1}^n x_i\right)\left(\prod_{1\leq i<j\leq n}(x_j - x_i)\right)$. It is clear that every prime divisor of $\delta(x_1, x_2, \ldots, x_n)$ is at most $\max\{x_1, x_2, \ldots, x_n\}$. The matrix defined in the following lemma gives a threshold black-box secret sharing scheme modulo large primes.

Lemma 5. *Define the matrix*

$$L = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 2 & 2^2 & 2^3 & \ldots & 2^t \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ n & n^2 & n^3 & \ldots & n^t \end{pmatrix} \in \mathbb{Z}^{n\times t}. \tag{1}$$

Then we have

(i) *For every subset T of $[n]$ of size t, the equation $\begin{pmatrix} 1 & \mathbf{0} \\ \delta\mathbf{1}' & L_T \end{pmatrix}\mathbf{x}' = \boldsymbol{\mu}'_{t+1}$ is solvable modulo p^ℓ for any prime $p > n$ and integer $\ell \geq 1$, where $\delta = \delta(1, 2, \ldots, n)$.*

(ii) *For every subset S of $[n]$ of size r with $r \geq t+1$, the equation $\mathbf{x}(\delta\mathbf{1}', L_S) = \boldsymbol{\mu}_{t+1}$ is solvable modulo p^ℓ for all primes $p > n$ and integers $\ell \geq 1$.*

Proof. To prove part (i), we let $|T| = t$ with $T = \{i_1, i_2, \ldots, i_t\}$. Then the matrix L_T is in fact the matrix $\Delta_1(i_1, i_2, \ldots, i_t)$. As $\det(\Delta_1(i_1, i_2, \ldots, i_t)) = \delta(i_1, i_2, \ldots, i_t)$ is co-prime to p^ℓ for every prime $p > n$ and $\ell \geq 1$, we can find a matrix $A \in \mathbb{Z}^{t\times t}$ such that $\Delta_1(i_1, i_2, \ldots, i_s)A$ is the identity matrix I_t modulo p^ℓ, thus we have $\delta\mathbf{1}' \equiv \delta L_T A \mathbf{1}' \pmod{p^\ell}$, i.e, $(1, -\delta\mathbf{1}A') \in \mathbb{Z}_{p^\ell}^{t+1} \pmod{p^\ell}$ is a solution of $(\delta\mathbf{1}', \Delta_1(i_1, i_2, \ldots, i_t))\mathbf{x}' \equiv \mathbf{0}'$ modulo p^ℓ. Thus, it is also a solution of $\begin{pmatrix} 1 & \mathbf{0} \\ \delta\mathbf{1}' & L_T \end{pmatrix}\mathbf{x}' = \boldsymbol{\mu}'_{t+1}$ modulo p^ℓ.

Now let $|S| = r \geq t+1$ and denote $S = \{i_1, i_2, \ldots, i_r\}$. Then

$$(\delta\mathbf{1}', L_S) = \begin{pmatrix} \Delta^{(\delta)}(i_1, \ldots, i_{t+1}) \\ B \end{pmatrix}, \tag{2}$$

for a matrix B in $\mathbb{Z}^{(r-t-1)\times(t+1)}$, where $\Delta^{(\delta)}(i_1, \ldots, i_{t+1})$ is the matrix obtained from $\Delta_0(i_1, \ldots, i_{t+1})$ by multiplying δ to the first column. As $\Delta_0(i_1, \ldots, i_{t+1})$ is invertible modulo p^ℓ, $\Delta^{(\delta)}(i_1, \ldots, i_{t+1})$ is also invertible modulo p^ℓ. Hence, there is a solution $\mathbf{c} \in \mathbb{Z}_{p^\ell}^{t+1}$ of the equation $\mathbf{x}\Delta^{(\delta)}(i_1, i_2, \ldots, i_{t+1}) = \boldsymbol{\mu}_{t+1}$ modulo p^ℓ. Thus, $(\mathbf{c}, \mathbf{0}) \in \mathbb{Z}^r$ is a solution of the equation $\mathbf{x}(\delta\mathbf{1}', L_S) \equiv \boldsymbol{\mu}_{t+1}$ modulo p^ℓ. □

We now present our gluing method.

Proposition 6. *Let $N_i \in \mathbb{Z}^{m\times(l-1)}$ with $mt < l \leq mr$ be a matrix for $1 \leq i \leq n$. Let $\mathbf{c}_i \in \mathbb{Z}^m$. Put*

$$G = \begin{pmatrix} \mathbf{c}'_1 & N_1 \\ \mathbf{c}'_2 & N_2 \\ \vdots & \vdots \\ \mathbf{c}'_n & N_n \end{pmatrix}, \qquad N = \begin{pmatrix} N_1 \\ N_2 \\ \vdots \\ N_n \end{pmatrix}.$$

Suppose that for every prime $p \leq n$, every subset T of $[n]$ of size t and every subset S of $[n]$ of size r, the $\mathbb{Z}_p$-ranks of N_T and G_S are mt and l, respectively. Then there exists a monotone span program $\mathcal{M} = (\mathbb{Z}, M, \Psi, \boldsymbol{\mu}_{t+l})$ computing $\mathfrak{R}_{t,r,n}$ with $M \in \mathbb{Z}^{(m+1)n\times(t+l)}$. As a result, $\mathrm{msp}(\mathfrak{R}_{t,r,n}) \leq (m+1)n$.

Proof. Define the product

$$\rho_N = \prod_{S\subset[n],|S|=t} \left(\prod_{A\in\mathcal{M}_t(N_S),\det(A)\neq 0} \det(A) \right),$$

where $\mathcal{M}_t(N_S)$ stands for the set of $mt \times mt$ submatrices of N_S. By the given condition, we know that ρ_N is well defined and it is a nonzero integer. We write the above ρ_N into the product

$\rho_N = \zeta_N \times \eta_N$ such that $\gcd(\zeta_N, \prod_{p \leq n} p) = 1$, and all prime divisors of η_N are less than or equal to n.

Define

$$M = \left(\begin{array}{ccc} \delta & \mathbf{0} & \mathbf{e}_1 \\ \zeta_N \mathbf{c}_1' & N_1 & \mathbf{0} \\ \hline \delta & \mathbf{0} & \mathbf{e}_2 \\ \zeta_N \mathbf{c}_2' & N_2 & \mathbf{0} \\ \hline \vdots & \vdots & \vdots \\ \hline \delta & \mathbf{0} & \mathbf{e}_n \\ \zeta_N \mathbf{c}_n' & N_n & \mathbf{0} \end{array}\right), \tag{3}$$

where $\delta = \delta(1, 2, \ldots, n)$ and $\mathbf{e}_i = (i, i^2, \ldots, i^t)$ for $1 \leq i \leq n$. Let Ψ be the map splitting M into the blocks of (3). We claim that $\mathcal{M} = (\mathbb{Z}, M, \Psi, \boldsymbol{\mu}_{t+l})$ is an integer monotone span program computing $\mathfrak{R}_{t,r,n}$.

To prove privacy, by Lemma 1, it is sufficient to show that for every subset $T = \{i_1, i_2, \ldots, i_t\}$ of $[n]$ of size t and every prime power p^ℓ, the equation

$$\begin{pmatrix} \boldsymbol{\mu}_{t+l} \\ M_T \end{pmatrix} \mathbf{x}' \equiv \boldsymbol{\mu}'_{(m+1)t+1} \pmod{p^\ell} \tag{4}$$

has solutions in $\mathbb{Z}_{p^\ell}^{t+l}$. For $p \leq n$, we let L be the matrix defined in (1). Then $L_T = \Delta_1(i_1, i_2, \ldots, i_t)$. As $\det(L_T)$ is a divisor of δ, one can find $D \in \mathbb{Z}^{t \times t}$ such that $L_T D \equiv \det(L_T) I_t \pmod{p^\ell}$. Thus, $(1, -\frac{\delta}{\det(L_T)} \mathbf{1} D')$ is a solution of the equation $\begin{pmatrix} 1 & \mathbf{0} \\ \delta \mathbf{1}' & L_T \end{pmatrix} \mathbf{x}' \equiv \boldsymbol{\mu}_t \pmod{p^\ell}$. On the other hand, it follows from the given condition that there exists an $mt \times mt$ submatrix A of N_T such that $\gcd(\det(A), p^\ell) = 1$. Then there exists an integer g such that $g \det(A) \equiv 1 \pmod{p^\ell}$. Without loss of generality, we may assume that $N_T = (A, B)$ with $B \in \mathbb{Z}^{mt \times (l - mt)}$. Let $H \in \mathbb{Z}_{p^\ell}^{mt \times mt}$ such that $AH = \det(A) I_{mt}$. Then $(1, -g\mathbf{c}H', \mathbf{0})$ is a solution of the equation $\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{c}' & N_T \end{pmatrix} \mathbf{x}' = \begin{pmatrix} 1 & \mathbf{0} & \mathbf{0} \\ \mathbf{c}' & A & B \end{pmatrix} \mathbf{x}' = \boldsymbol{\mu}_l$ modulo p^ℓ, where $\mathbf{c} = \zeta_N(\mathbf{c}_{i_1}, \mathbf{c}_{i_2}, \ldots, \mathbf{c}_{i_t})$. In conclusion, the vector $(1, -g\mathbf{c}H', \mathbf{0}, -\frac{\delta}{\det(L_T)} 1$ is a solution of (4).

If $p > n$, by Lemma 5 the equation $\begin{pmatrix} 1 & \mathbf{0} \\ \delta \mathbf{1}' & L_T \end{pmatrix} \mathbf{x}' \equiv \boldsymbol{\mu}'_{t+1} \pmod{p^\ell}$ has a solution $(1, \mathbf{u}) \in \mathbb{Z}^{t+1}$. On the other hand, by the given condition, there exists an $mt \times mt$ submatrix E of N_T such that $\det(E) \neq 0$. Without loss of generality, we may assume that $N_T = (E, F)$ with $F \in \mathbb{Z}^{mt \times (l - mt)}$. Assume that $e \geq 0$ is an integer such that $p^e | \det(E)$ and $p^{e+1} \nmid \det(E)$. Then by the definition of ζ_N, we have $p^e | \zeta_N$. Let $\zeta = p^e a$ and let $\det(E) = p^e b$ with $\gcd(b, p) = 1$. Then there exists an integer d such that $bd \equiv 1 \pmod{p^\ell}$. Let $C \in \mathbb{Z}_{p^\ell}^{mt \times mt}$ such that $AC = \det(E) I_{mt} = p^e b I_{mt}$. Hence, $(1, -ad\mathbf{v}C', \mathbf{0})$ is a solution of the equation $\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{c}' & N_S \end{pmatrix} \mathbf{x}' = \begin{pmatrix} 1 & \mathbf{0} & \mathbf{0} \\ \mathbf{c}' & E & F \end{pmatrix} \mathbf{x}' \equiv \boldsymbol{\mu}_{mt+1} \pmod{p^\ell}$, where $\mathbf{c} = \zeta_N(\mathbf{c}_{i_1}, \mathbf{c}_{i_2}, \ldots, \mathbf{c}_{i_t})$ and $\mathbf{v} = (\mathbf{c}_{i_1}, \mathbf{c}_{i_2}, \ldots, \mathbf{c}_{i_t})$. Thus, the vector $(1, -ae\mathbf{v}C', \mathbf{0}, \mathbf{u})$ is a solution of (4).

To prove reconstruction, by Lemma 1, it is sufficient to show that for every subset $S =$

$\{i_1, i_2, \ldots, i_r\}$ of $[n]$ of size r and every prime power p^ℓ, the equation

$$\mathbf{x}M_S \equiv \boldsymbol{\mu}_{l+e} \pmod{p^\ell} \tag{5}$$

is solvable. If $p \leq n$, then $\mathbb{Z}_p$-rank of G_S is l. Without loss of generality, we may write $G_S = \binom{\mathbf{b}' \ E}{\mathbf{c}' \ F}$ such that $(\mathbf{b}', E)$ is ann $l \times l$ invertible matrix modulo p^ℓ. As ζ_N is co-prime with p, $(\zeta_N \mathbf{b}^T, E)$ is also an $l \times l$ invertible matrix modulo p^ℓ. Thus, there exists a vector $\mathbf{v} \in \mathbb{Z}^l$ such that $\mathbf{v}E \equiv \boldsymbol{\mu}_l \pmod{p^\ell}$. Hence, $(\mathbf{v}, \mathbf{0})$ is a solution of (5).

If $p > n$, let $S_1 = \{i_1, i_2, \ldots, i_{t+1}\} \subseteq S$. By Lemma 5, there is a vector $\mathbf{a} \in \mathbb{Z}_{p^\ell}^{t+1}$ such that $\mathbf{a}(\delta \mathbf{1}, L_{S_1}) \equiv \boldsymbol{\mu}_{t+1} \pmod{p^\ell}$. This implies that (5) is solvable modulo p^ℓ. □

5 Lifting codes over prime fields

As we have seen in the previous section, to construct a monotone span program, it is sufficient to construct a matrix G satisfying the conditions in Proposition 6. Our idea is to construct generator matrices over $\mathbb{Z}_p$ of the same size for every prime p such that each of generator matrices over $\mathbb{Z}_p$ satisfies the conditions in Proposition 6. Then we lift these matrices using the Chinese Remainder Theorem to obtain the desired matrix G in Proposition 6.

It has been known that linear secret sharing schemes with same secret and share spaces are equivalent to linear codes (see e.g. [7, 27]).

Let us first review some notions from coding theory (see e.g. [31, 30]) that are relevant to this work. Let $\mathbb{F}_q$ be a finite field of q elements. A q-ary linear code $\mathcal{C}$ of length n is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$. Then dimension of this code is defined to be the dimension of $\mathcal{C}$ as an $\mathbb{F}_q$-linear space. We denote by $[n, k]_q$ a q-ary linear code of length n and dimension k. In case there is no confusion, we just denote $[n, k]_q$ by $[n, k]$ or q-ary $[n, k]$-linear code. The (Euclidean) dual code of $\mathcal{C}$, denote by $\mathcal{C}^\perp$, is defined to be the set $\{\mathbf{x} \in \mathbb{F}_q : \langle \mathbf{c}, \mathbf{x} \rangle = 0 \text{ for all } \mathbf{c} \in \mathcal{C}\}$, where $\langle \cdot, \cdot \rangle$ is the Euclidean inner product. Then it is well known from linear algebra that $\mathcal{C}^\perp$ is a q-ary $[n, n-k]$-linear code. Apart from length and dimension, there is a third parameter d, called minimum distance which plays an important role in coding theory. We denote by $[n, k, d]_q$ a q-ary linear code of length n, dimension k and minimum distance d. We use $d^\perp$ to denote the minimum distance of the dual code. We also call $d^\perp$ the dual distance of $\mathcal{C}$. The distance d and dual distance $d^\perp$ are closely related to privacy and reconstruction of the linear secret sharing scheme arising from this code (see e.g. [7, 27]).

For an $[n, k]_q$-linear code $\mathcal{C}$, a matrix G is called a generator matrix of $\mathcal{C}$ if the columns of G form an $\mathbb{F}_q$-basis of $\mathcal{C}$ (note that this is different from the usual definition in which rows of G form an $\mathbb{F}_q$-basis of $\mathcal{C}$). Thus, G has the size $n \times k$. A generator matrix of $\mathcal{C}^\perp$ is called a parity-check matrix of $\mathcal{C}$. Hence, H has size $n \times (n-k)$. It is clear that a linear code $\mathcal{C}$ is uniquely determined by either a generator matrix or a parity-check matrix. Therefore, all three parameters of a linear code $\mathcal{C}$ are completely determined by a generator matrix G or a parity-check matrix H. The length and dimension of $\mathcal{C}$ are determined by size of G or H in an obvious way. The following result shows how the minimum distance is determined by G or H.

Lemma 7 (see [30, 39])**.** *Let $\mathcal{C}$ be a q-ary $[n, k]$-linear code with a generator matrix G or a parity-check matrix H. Then*

(i) *$\mathcal{C}$ has minimum distance d if and only if every $(n-d+1) \times k$ submatrix of G has rank k; and there is a $(n-d) \times k$ submatrix of G with rank less than k.*

(ii) *$\mathcal{C}$ has minimum distance d if and only if every $(d-1)\times(n-k)$ submatrix of H has rank $d-1$; and there is a $d\times(n-k)$ submatrix of H with rank less than d.*

In coding theory, there is a well-known propagation rule to construct new codes from given codes, called concatenation rule. Let $\mathcal{C}_1$ be a p^{k_0}-ary $[n_1, k_1, d_1]$-linear code and let $\mathcal{C}_0$ be a p-ary $[n_0, k_0, d_0]$-linear code. We fix an $\mathbb{F}_p$-isomorphism τ between $\mathbb{F}_{p^{k_0}}$ and $\mathcal{C}_0$. Then the concatenated code $\mathcal{C}$ is defined by $\{(\tau(c_1), \tau(c_2), \ldots, \tau(c_n)) : (c_1, c_2, \ldots, c_n) \in \mathcal{C}_1\}$. Furthermore, $\mathcal{C}$ is an $[n_0n_1, k_0k_1, \geq d_0d_1]_p$-linear code (see e.g. [30]). However, usually $\mathcal{C}$ has small dual distance. In fact, the dual distance of $\mathcal{C}$ is at most the dual distance of $\mathcal{C}_0$. On the other hand, if $\mathcal{C}_0$ is the trivial code $\mathbb{F}_q^{k_0}$, then the dual distance of $\mathcal{C}$ is the least the dual distance of $\mathcal{C}_1$

Fix an $\mathbb{F}_p$-basis $\gamma_1, \gamma_2, \ldots, \gamma_m$ of $\mathbb{F}_{p^m}$. Let $\beta_1, \beta_2, \ldots, \beta_m$ be an orthogonal balsas of $\gamma_1, \gamma_2, \ldots, \gamma_m$, i.e, $\mathrm{Tr}(\alpha_i\beta_j) = \delta_{ij}$, where Tr is the trace map from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ and where $\delta_{i,j}$ is the Kronecker-delta function. We define maps φ and ψ from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p^m$ by setting $\varphi(\alpha) = (a_1, a_2, \ldots, a_m)$ if $\alpha = \sum_{i=1}^m a_i\gamma_i$ and $\psi(\alpha) = (b_1, b_2, \ldots, b_m)$ if $\alpha = \sum_{i=1}^m b_i\beta_i$, respectively. Then both maps are $\mathbb{F}_p$-isomorphisms from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p^m$. Furthermore, we have $\langle\varphi(\alpha), \psi(\beta)\rangle = \mathrm{Tr}(\alpha\beta)$. We can extend these two $\mathbb{F}_p$-isomorphisms: $\mathbb{F}_{p^m}^n \to \mathbb{F}_p^{mn}$ by defining $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\varphi(\alpha_1), \varphi(\alpha_2), \ldots, \varphi(\alpha_n))$ and $\psi(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\psi(\alpha_1), \psi(\alpha_2), \ldots, \psi(\alpha_n))$, respectively. Then they become $\mathbb{F}_p$-isomorphisms from $\mathbb{F}_{p^{mn}}$ to $\mathbb{F}_p^{mn}$.

Lemma 8. *If $\mathcal{C}$ is a p^m-ary $[n, k, d]$-linear code with dual distance $d^\perp$. Then $\varphi(\mathcal{C})$ is a p-ary $[nm, km]$-linear code with distance at least d and dual distance at least $d^\perp$. Furthermore, the dual code of $\varphi(\mathcal{C})$ is $\psi(\mathcal{C}^\perp)$.*

Proof. $\varphi(\mathcal{C})$ (and $\psi(\mathcal{C}^\perp)$, respectively) is the concatenated code with the outer code $\mathcal{C}$ (and $\mathcal{C}^\perp$, respectively) and trivial inner code $\mathbb{F}_p^m$. Thus, $\varphi(\mathcal{C})$ is a p-ary linear code with the desired parameters. It remains to prove that $\varphi(\mathcal{C})^\perp$ is $\psi(\mathcal{C}^\perp)$.

Since the $\mathbb{F}_p$-dimension of $\varphi(\mathcal{C})^\perp$ is $nm - \dim_{\mathbb{F}_p}\varphi(\mathcal{C}) = nm - \dim_{\mathbb{F}_p}\mathcal{C} = nm - mk = \dim_{\mathbb{F}_p}\psi(\mathcal{C}^\perp)$, it is sufficient to show that codewords of $\varphi(\mathcal{C})$ and those of $\psi(\mathcal{C}^\perp)$ are orthogonal. Let $\mathbf{u} = (\varphi(\alpha_1), \varphi(\alpha_2), \ldots, \varphi(\alpha_n)) \in \varphi(\mathcal{C})$ with $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathcal{C}$. Let $\mathbf{v} = (\psi(\lambda_1), \psi(\lambda_2), \ldots, \psi(\lambda_n)) \in \psi(\mathcal{C}^\perp)$ with $(\lambda_1, \lambda_2, \ldots, \lambda_n) \in \mathcal{C}^\perp$. Then the inner product of these vectors are

$$\langle\mathbf{u}, \mathbf{v}\rangle = \sum_{i=1}^n \langle\varphi(\alpha_i), \psi(\lambda_i)\rangle = \sum_{i=1}^n \mathrm{Tr}(\alpha_i\lambda_i) = \mathrm{Tr}\left(\sum_{i=1}^n \alpha_i\lambda_i\right) = 0.$$

This completes the proof. □

Corollary 9. *Let $\mathcal{C}$ be a p^m-ary $[n, k, d]$-linear code with dual distance $d^\perp$. Let $(a_{ij})_{1\leq i\leq n, 1\leq j\leq k}$ be a generator matrix of $\mathcal{C}$. Then the matrix in $\mathbb{F}_p^{mn\times km}$ given below*

$$G = \begin{pmatrix} \varphi(\gamma_1a_{11}) & \varphi(\gamma_2a_{11}) & \cdots & \varphi(\gamma_ma_{11}) & \cdots & \cdots & \varphi(\gamma_1a_{1k}) & \varphi(\gamma_2a_{1k}) & \cdots & \varphi(\gamma_ma_{1k}) \\ \varphi(\gamma_1a_{21}) & \varphi(\gamma_2a_{21}) & \cdots & \varphi(\gamma_ma_{21}) & \cdots & \cdots & \varphi(\gamma_1a_{2k}) & \varphi(\gamma_2a_{2k}) & \cdots & \varphi(\gamma_ma_{2k}) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \varphi(\gamma_1a_{n1}) & \varphi(\gamma_2a_{n1}) & \cdots & \varphi(\gamma_ma_{n1}) & \cdots & \cdots & \varphi(\gamma_1a_{nk}) & \varphi(\gamma_2a_{nk}) & \cdots & \varphi(\gamma_ma_{nk}) \end{pmatrix} \tag{6}$$

is a generator matrix of $\varphi(\mathcal{C})$, where each $\varphi(\gamma_ia_{jl})$ is viewed as a column vector of length m. Furthermore, define Ψ to be the map from $[mn]$ to $[n]$ such that the first m numbers of $[mn]$ are mapped to 1 and the second m numbers of $[mn]$ are mapped to 2 and so on. Then

(i) *for any* $S \subseteq [n]$ *with* $|S| \geq n-d+1$*,* $\varphi(G_S)$ *has* $\mathbb{F}_p$*-rank equal to* mk*;*

(ii) *for any* $T \subseteq [n]$ *with* $|T| \leq d^{\perp}-1$*,* $\varphi(G_T)$ *has* $\mathbb{F}_p$*-rank equal to* mt*.*

Proof. It is clear that every column of G is a codeword of $\varphi(\mathcal{C})$. By Lemma 8, $\varphi(G)$ has dimension mk. Thus, to show that $\varphi(G)$ is a generator matrix of $\varphi(\mathcal{C})$, it is sufficient to show that all columns of $\varphi(\mathcal{C})$ are linearly independent. Let $\mathbf{g}_1', \mathbf{g}_2', \dots, \mathbf{g}_k'$ be column vectors of G. We want to show that $\{\varphi(\gamma_i \mathbf{g}_j)\}_{1\leq i\leq m, 1\leq j\leq k}$ are $\mathbb{F}_p$-linearly independent. Suppose that $\sum_{i=1}^m \sum_{j=1}^k \lambda_{ij}$ $\varphi(\gamma_i\mathbf{g}_j) = \mathbf{0}$ for some $\lambda_{ij} \in \mathbb{F}_p$, i.e., $\varphi\left(\sum_{i=1}^m \sum_{j=1}^k \lambda_{ij}\gamma_i\mathbf{g}_j\right) = \mathbf{0}$. As φ is an isomorphism, we get $\sum_{i=1}^m \left(\sum_{j=1}^k \lambda_{ij}\gamma_i\right) \mathbf{g}_j = \mathbf{0}$. Since $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_k$ are $\mathbb{F}_{p^m}$-linearly independent, this forces that $\sum_{j=1}^k \lambda_{ij}\gamma_i = 0$ for $i = 1, 2, \dots, k$. This gives $\gamma_{ij} = 0$ for all $1 \leq i \leq m$ and $1 \leq j \leq k$.

Now let $S \subseteq [n]$ with $|S| \geq n-d+1$. Consider the new code $\mathcal{C}_1$ that is obtained from $\mathcal{C}$ by deleting $n-|S|$ positions at $i \in [n] \setminus S$. Then $\mathcal{C}_1$ is p^m-ary $[n-|S|, k, \geq d-n+|S|]$-linear code. By the first part of this lemma, we know that of $\varphi(G_S)$ is a generator matrix of $\varphi(\mathcal{C}_1)$. Hence, it has rank mk.

Let $T \subseteq [n]$ with $|T| \leq d^{\perp}-1$. If $\mathbf{u}_T \in \mathbb{F}_p^{mt}$ is a solution of $\mathbf{x}\varphi(G_T) = \mathbf{0}$. Then $(\mathbf{u}_T, \mathbf{0}_{[n]\setminus T})$ is a solution of $\mathbf{x}\varphi(G) = \mathbf{0}$. By Lemma 8, $(\mathbf{u}_T, \mathbf{0}_{[n]\setminus T})$ is a codeword in $\psi(\mathcal{C}^{\perp})$. Hence $\psi^{-1}(\mathbf{u}_T, \mathbf{0}_{[n]\setminus T})$ is a codeword of $\mathcal{C}^{\perp}$. As the Hamming weight of $\psi^{-1}(\mathbf{u}, \mathbf{0}_{[n]\setminus T})$ is at most $|T| \leq d^{\perp}-1$, we conclude that $\mathbf{u} = \mathbf{0}$. This implies that the $\mathbb{Z}_p$-rank of $\varphi(G_T')$ is mt. The proof is completed. □

Given a matrix $A = (a_{ij})_{1\leq i\leq n, 1\leq j\leq k} \in \mathbb{F}_{p^m}^{n\times k}$, we denote by $\varphi(A)$ the matrix given in (6).

5.1 Reed-Solomon codes

In this subsection, we are going to make use of Reed-Solomon codes to construct a matrix G satisfying the conditions of Proposition 6.

Let $m = \lceil \log n \rceil$. Then for any prime p, we have $n \leq 2^m \leq p^m$. Choose n distinct elements $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}_{p^m}$. We denote by $\mathbb{F}_{p^m}[x]_{<t}$ the set of polynomials in $\mathbb{F}_{p^m}[x]$ of degree less than t. Then $\mathbb{F}_{p^m}[x]_{<t}$ is an $\mathbb{F}_{p^m}$-space of dimension t with a canonical basis $\{1, x, , x^2, \dots, x^{t-1}\}$. A Reed-Solomon code is defined below

$$\mathcal{RS}[n,t] := \{(f(\alpha_i), f(\alpha_2), \dots, f(\alpha_n)) : \ f \in \mathbb{F}_{p^m}[x]_{<t}\}.$$

The code $\mathcal{RS}[n,t]$ is a p^m-ary $[n,t]$-linear code with distance $d = n-t+1$ and dual distance $d^{\perp} = t+1$, respectively.

Fix an $\mathbb{F}_{p^m}$-basis $f_2, f_3, \dots, f_{t+1}$ of $\mathbb{F}_{p^m}[x]_{<t}$. Extend this basis to an $\mathbb{F}_{p^m}$-basis $\{f_i\}_{i=1}^{t+1}$ of $\mathbb{F}_{p^m}[x]_{\leq t}$. Define the matrix

$$A^{(p)} = \begin{pmatrix} f_1(\alpha_1) & f_2(\alpha_1) & f_3(\alpha_1) & \cdots & f_{t+1}(\alpha_1) \\ f_1(\alpha_2) & f_2(\alpha_2) & f_3(\alpha_2) & \cdots & f_{t+1}(\alpha_2) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ f_1(\alpha_n) & f_2(\alpha_n) & f_3(\alpha_n) & \cdots & f_{t+1}(\alpha_n) \end{pmatrix} \tag{7}$$

Then $A^{(p)}$ is a generator matrix of $\mathcal{RS}[n, t+1] = [n, n-t-1]_{p^m}$.

Lemma 10. *Put $G^{(p)} = \varphi(A^{(p)})$. Then*

(i) *for any subset S of $[n]$ of size $t+1$, $G_S^{(p)}$ has $\mathbb{F}_p$-rank equal to $(t+1)m$; and*

(ii) *for any subset T of $[n]$ of size t, N_T has $\mathbb{F}_p$-rank mt, where N is obtained from $G^{(p)}$ by removing the first column from the left.*

Proof. As $A^{(p)}$ is a generator matrix of $\mathcal{RS}[n, t+1]$ whose distance is $n-t$, Part (i) directly follows from Corollary 9 (i). To prove Part (ii), we consider $B^{(p)}$ that is obtained from $A^{(p)}$ by removing the first column. Then $B^{(p)}$ is a generator matrix of $\mathcal{RS}[n, t]$ whose dual distance is $t+1$. By Corollary 9 (ii), $\varphi(B_T^{(p)})$ has $\mathbb{F}_p$-rank mt. Furthermore, $\varphi(B^{(p)})$ is in fact obtained from N_T by removing the first $m-1$ columns. As a result, N_T has $\mathbb{F}_p$-rank mt as well. □

Corollary 11. *For any integer $n \geq 2$ and any integer t with $0 < t < n$, there exists a triple $(\mathbb{Z}, G, \Psi)$ defined in Subsection 2.1 such that $G \in \mathbb{Z}^{nm \times (t+1)m}$ with $m \geq \lceil \log n \rceil$ and $|\Psi^{-1}(j)| = m$ for all $1 \leq j \leq n$ such that, for every prime $p \leq n$, if G is viewed a matrix modulo p, then*

(i) *for any subset S of $[n]$ of $t+1$, G_S has $\mathbb{F}_p$-rank equal to $(t+1)m$; and*

(ii) *for any subset T of $[n]$ of t, N_T has $\mathbb{F}_p$-rank mt, where N is obtained from G by removing the first column from the left.*

Proof. By Lemma 10, for every prime $p \leq n$, we can construct a matrix $G^{(p)} \in M \in \mathbb{Z}^{nm \times (t+1)m}$ satisfying the two conditions in Lemma 10. By the Chinese Remainder Theorem, we can lift all $G^{(p)}$'s to one matrix $G \in \mathbb{Z}^{nm \times (t+1)m}$ such that $G \equiv G^{(p)} \pmod{p}$. Then G is the desired matrix. □

5.2 Algebraic geometry codes

In the previous section, we made use of Reed-Solomon codes to construct a matrix G satisfying the conditions in Proposition 6. This would give a threshold BBSSS (see Theorem 6). However, the expansion factor $h = nm = n\lceil \log n \rceil$, i.e., the ratio is $\frac{h}{n} = \lceil \log n \rceil$ is unbounded. If we want to get a bounded ratio $\frac{h}{n}$, then the lower bound in Theorem 5 indicates that we have to use a near-threshold BBSSS. As in the case of linear secret sharing schemes, we can use algebraic geometry codes to get a bounded ratio $\frac{h}{n}$.

Let us first introduce an algebraic geometry codes very briefly. The reader may refer to the books [35, 37] for the details on this topic. For convenience of the reader, we start with some background on global function fields over finite fields. The reader may refer to [35, 32] for detailed background on function fields and algebraic-geometric codes.

For a prime power q, let $\mathbb{F}_q$ be the finite field of q elements. An algebraic function field over $\mathbb{F}_q$ in one variable is a field extension $F \supset \mathbb{F}_q$ such that F is a finite algebraic extension of $\mathbb{F}_q(x)$ for some $x \in F$ that is transcendental over $\mathbb{F}_q$. The field $\mathbb{F}_q$ is called the full constant field of F if the algebraic closure of $\mathbb{F}_q$ in F is $\mathbb{F}_q$ itself. Such a function field is also called a global function field. From now on, we always denote by $F/\mathbb{F}_q$ a function field F with the full constant field $\mathbb{F}_q$.

A discrete valuation of $F/\mathbb{F}_q$ is a map from F to $\mathbb{Z} \cup \{+\infty\}$ satisfying certain properties (see [35, Definition 1.19]). Then each discrete valuation ν from $F/\mathbb{F}_q$ to $\mathbb{Z} \cup \{+\infty\}$ defines a valuation ring $O = \{f \in F : \nu(f) \geq 0\}$ that is a local ring [35, Theorem 1.1.13]. The maximal ideal P of O is given by $P = \{f \in F : \nu(f) > 0\}$ and it is called a *place.* We denote the valuation ν and the local ring O corresponding to P by ν_P and O_P, respectively. The residue class field O_P/P, denoted by F_P, is a finite extension of $\mathbb{F}_q$. The extension degree $[F_P : \mathbb{F}_q]$ is called *degree* of P, denoted by $\deg(P)$. A place of degree one is called a *rational* place. For a nonzero function $z \in F$, the principal divisor of z is defined to be $\text{div}(z) = \sum_{P\in\mathbb{P}_F} \nu_P(z)P$. The zero and pole divisors of z are defined to be $\text{div}(z)_0 = \sum_{\nu_P(z)>0} \nu_P(z)P$ and $\text{div}(z)_\infty = -\sum_{\nu_P(z)<0} \nu_P(z)P$, respectively. Then we have $\deg(\text{div}(z)) = 0$, i.e, $\deg(\text{div}(z)_0) = \deg(\text{div}(z)_\infty)$. For two functions $f, g \in F$ and a place P, we have $\nu_P(f + g) \geq \min\{\nu_P(f), \nu_P(g)\}$ and the equality holds if $\nu_p(f) \neq \nu_P(g)$ (note that $\nu_P(0) = +\infty$). This implies that $f + g \neq 0$ if $\nu_P(f) \neq \nu_P(g)$.

If F is the rational function field $\mathbb{F}_q(x)$, then every discrete valuation of $F/\mathbb{F}_q$ is given by either ν_∞ or $\nu_{p(x)}$ for an irreducible polynomial $p(x)$, where ν_∞ is defined by $\nu_\infty(f/g) = \deg(g) - \deg(f)$ and $\nu_{p(x)}(f/g) = a - b$ with $p(x)^a||f$ and $p(x)^b||g$ for two nonzero polynomials $f, g \in \mathbb{F}_q[x]$. It is straightforward to verify that the degrees of places corresponding to ν_∞ and $\nu_{p(x)}$ are 1 and $\deg(p(x))$, respectively.

Let $\mathbb{P}_F$ denote the set of places of F. The divisor group, denoted by $\text{Div}(F)$, is the free abelian group generated by all places in $\mathbb{P}_F$. An element $D = \sum_{P\in\mathbb{P}_F} n_P P$ of $\text{Div}(F)$ is called a divisor of F, where $n_P = 0$ for almost all $P \in \mathbb{P}_F$. We denote n_p by $\nu_P(D)$. The support, denoted by Supp(D), of D is the set $\{P \in \mathbb{P}_F : n_P \neq 0\}$. Thus, Supp(D) of a divisor D is always a finite subset of $\mathbb{P}_F$. For a divisor D of $F/\mathbb{F}_q$, we define the Riemann-Roch space associated with D by

$$\mathcal{L}(D) := \{f \in F^* : \text{div}(f) + D \geq 0\} \cup \{0\},$$

where F^* denotes the set of nonzero elements of F. Then $\mathcal{L}(D)$ is a finite dimensional space over $\mathbb{F}_q$ and its dimension $\dim_{\mathbb{F}_q} \mathcal{L}(D)$ is determined by the Riemann-Roch theorem which gives

$$\dim_{\mathbb{F}_q} \mathcal{L}(D) = \deg(D) + 1 - \mathfrak{g} + \dim_{\mathbb{F}_q} \mathcal{L}(W - D),$$

where $\mathfrak{g}$ is the genus of F and W is a canonical divisor of degree $2\mathfrak{g} - 2$. Therefore, we always have that $\dim_{\mathbb{F}_q} \mathcal{L}(D) \geq \deg(D) + 1 - \mathfrak{g}$ and the equality holds if $\deg(D) \geq 2\mathfrak{g} - 1$ [35, Theorems 1.5.15 and 1.5.17].

Let p be a prime and let $n > l \geq 2$ be two integers. Let $F/\mathbb{F}_{p^m}$ be a function field with genus $\mathfrak{g}$ and $n + 1$ distinct $\mathbb{F}_{p^m}$-rational places $P_\infty, P_1, P_2, \ldots, P_n$. Put $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$. Denote by $\mathcal{C}(lP_\infty, \mathcal{P})$ the algebraic geometric code defined by

$$\mathcal{C}(lP_\infty, \mathcal{P}) = \{(f(P_1), f(P_2), \ldots, f(P_n)) : f \in \mathcal{L}(lP_\infty)\}. \tag{8}$$

Lemma 12. (see [35, Theorem 2.2.4]) *Let $\mathfrak{g} < k < n - \mathfrak{g}$. Then $\mathcal{C}((k + \mathfrak{g} - 1)P_\infty, \mathcal{P})$ is a p^m-ary $[n, k, \geq n - k - \mathfrak{g} + 1]$-linear code and $\mathcal{C}^\perp((t + 2\mathfrak{g} - 1)P_\infty, \mathcal{P})$ is a p^m-ary $[n, n - k, \geq k - \mathfrak{g} + 1]$-linear code. Furthermore, the matrix*

$$A = \begin{pmatrix} f_1(P_1) & f_2(P_1) & f_3(P_1) & \cdots & f_k(P_1) \\ f_1(P_2) & f_2(P_2) & f_3(P_2) & \cdots & f_k(P_2) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ f_1(P_n) & f_2(P_n) & f_3(P_n) & \cdots & f_k(P_n) \end{pmatrix} \tag{9}$$

is a generator matrix of $\mathcal{C}((k+\mathfrak{g}-1)P_\infty, \mathcal{P})$ whenever $f_1, f_2, \ldots, f_k$ are a basis of $\mathcal{L}((k+\mathfrak{g}-1)P_\infty)$.

Similar to Corollary 11, we have the following result.

Lemma 13. *Let $\mathfrak{g} < k < n - \mathfrak{g}$. Let $f_2, f_3, \dots, f_{k-1}$ be a $\mathbb{F}_{p^m}$-basis of $\mathcal{L}((k + \mathfrak{g} - 2)P_\infty)$ and let $f_1, f_2, f_3, \dots, f_{t+\mathfrak{g}+1}$ be an $\mathbb{F}_{p^m}$-basis of $\mathcal{L}((k+\mathfrak{g}-1)P_\infty)$. Let A be the matrix defined in (9) and put $G^{(p)} = \varphi(A)$. Furthermore, define Ψ to be the map from $[mn]$ to $[n]$ such that the first m numbers of $[mn]$ are mapped to 1 and the second m numbers of $[mn]$ are mapped to 2 and so on. Then*

- (i) *for any subset S of $[n]$ of size at least $k + \mathfrak{g}$, $G_S^{(p)}$ has $\mathbb{F}_p$-rank equal to $(t + \mathfrak{g} + 1)m$; and*
- (ii) *for any subset T of $[n]$ of size at most $k - \mathfrak{g} - 1$, N_T has $\mathbb{F}_p$-rank mt, where N is obtained from $G^{(p)}$ by removing the first column from the left.*

Proof. Note that A is a generator matrix of $\mathcal{L}((t + 2\mathfrak{g})P_\infty)$ with minimum distance at least $n - 2\mathfrak{g}$. Part (i) follows from Corollary 9.

Let B be the matrix of A obtained from A by removing the first column of A. Then B is a generator matrix of $\mathcal{C}((k + \mathfrak{g} - 2)P_\infty, \mathcal{P})$. By mimicking proof of Corollary 11(ii), we can Part (ii). □

Corollary 14. *Let $m \geq 2$ be an even integer. Then for any integer $n \geq 2$ and any integer k with $\frac{2(n+1)}{2^{m/2}-1} < k < n - \frac{2(n+1)}{2^{m/2}-1}$, there exists a triple $(\mathbb{Z}, G, \Psi)$ defined in Subsection 2.1 such that $G \in \mathbb{Z}^{nm \times km}$ and $|\Psi^{-1}(j)| = m$ for all $1 \leq j \leq n$ such that, for every prime $p \leq n$, if G is viewed as a matrix modulo p, then*

- (i) *for any subset S of $[n]$ of size r with $r \geq k + \frac{2(n+1)}{2^{m/2}-1}$, G_S has $\mathbb{F}_p$-rank equal to km; and*
- (ii) *for any subset T of $[n]$ of size t with $t \leq k - \frac{2(n+1)}{2^{m/2}-1} - 1$, N_T has $\mathbb{F}_p$-rank mt, where N is obtained from G by removing the first column from the left.*

Proof. If $p^m \geq n$, then the desired result follows from Corollary 11. Now we assume that $p^m < n$.

Define

$$i(p, m, n) = \left\lceil \log_p \left(\frac{n}{p^m - 1} \right) \right\rceil. \tag{10}$$

We claim that

$$p^{i(p,m,n)-1}(p^m - 1) < n \leq p^{i(p,m,n)}(p^m - 1). \tag{11}$$

To prove (11), it is sufficient to verify that $p^{i(p,m,n)-1} < \frac{n}{p^m-1} \leq p^{i(p,m,n)}$, i.e, $i(p, m, n) - 1 < \log_p \left(\frac{n}{p^m-1} \right) \leq i(p, m, n)$ for all primes p.

Define

$$i(m, n) = \max_{p^m \leq n} p^{i(p,m,n)}(p^{m/2} + 1). \tag{12}$$

For $p^m \leq n$, we have

$$\begin{aligned} p^{i(p,m,n)}(p^{m/2} + 1) &\leq p^{1+\log_p\left(\frac{n+1}{p^m-1}\right)}(p^{m/2} + 1) \leq p \left(\frac{n + 1}{p^m - 1} \right) (p^{m/2} + 1) \\ &= \frac{p(n + 1)}{p^{m/2} - 1} \leq \frac{2(n + 1)}{2^{m/2} - 1}. \end{aligned}$$

For every p with $p^m \leq n$, by Lemma 15, there exists an algebraic function field $F/\mathbb{F}_{p^m}$ of genus $\mathfrak{g} \leq i(m,n)$ such that it has at least $n+1$ distinct $\mathbb{F}_{p^m}$-rational points. We label these $n+1$ pairwise distinct $\mathbb{F}_{p^m}$-rational points $P_\infty, P_1, P_2, \ldots, P_n$. Let $f_2, f_3, \ldots, f_{t+\mathfrak{g}+1}$ be a $\mathbb{F}_{p^m}$-basis of $\mathcal{L}((t+2\mathfrak{g}-1)P_\infty)$ and extend to a $\mathbb{F}_{p^m}$-basis $f_1, f_2, f_3, \ldots, f_{t+\mathfrak{g}+1}$ of $\mathcal{L}((t+2\mathfrak{g})P_\infty)$. Let A be the matrix defined in (9) and put $G^{(p)} = \varphi(A)$.

By Corollary 14, for any subset S of $[n]$ or size r with $r \geq k + \frac{2(n+1)}{2^{m/2}-1} \geq k + \mathfrak{g}$, $G_S^{(p)}$ has $\mathbb{F}_p$-rank equal to km; and for any subset T of $[n]$ of size t with $t \leq k - \frac{2(n+1)}{2^{m/2}-1} - 1 \leq k - \mathfrak{g} - 1$, N_T has $\mathbb{F}_p$-rank mt. Now by the Chinese Remainder Theorem, we can lift all $G^{(p)}$ to a matrix $G \in \mathbb{Z}^{nm \times km}$ such that $G \equiv G^{(p)} \pmod{p}$. The desired result follows. □

6 The main results

We are ready to state our final results by collecting some previous results.

Theorem 6. *For any $0 < t < n$, there is a threshold BBSSS over the access structure $\mathfrak{R}_{t,n}$ whose expansion factor ϱ satisfies $\log \frac{n+1}{2} \leq \varrho \leq 1 + \lceil \log n \rceil$.*

Proof. The lower bound follows Theorem 5 directly. By applying the matrix G obtained in Corollary 11 to Proposition 6, we obtain the desired upper bound.

□

The above upper bound is better than the one given in [12] by an additive constant and worse than the one given in [14] by an additive constant.

Theorem 7. *Let $m \geq 2$ be an even integer. Then for any integer $n \geq 2$ and any integer k with*

$$\frac{2(n+1)}{2^{m/2}-1} < k < n - \frac{2(n+1)}{2^{m/2}-1}, \quad r \geq k + \frac{2(n+1)}{2^{m/2}-1}, \quad t \leq k - \frac{2(n+1)}{2^{m/2}-1} - 1,$$

one has $\mathrm{msp}(\mathfrak{R}_{t,r,n}) \leq n(1+m)$. As a result, for any $0 < t < n - 2\left\lceil \frac{2(n+1)}{2^{m/2}-1} \right\rceil$ and r with $r = t + 2\left\lceil \frac{2(n+1)}{2^{m/2}-1} \right\rceil + 1$, there is a near-threshold BBSSS over the access structure $\mathfrak{R}_{t,r,n}$ whose expansion factor ϱ satisfies

$$\frac{m}{2} - 3 \approx \log \frac{n+1}{2(r-t)} \leq \varrho \leq m+1.$$

Proof. The lower bound on $\mathrm{msp}(\mathfrak{R}_{t,r,n})$ follows Theorem 5 directly. By applying the matrix G obtained in Corollary 14 to Proposition 6, we obtain the desired upper bound $\mathrm{msp}(\mathfrak{R}_{t,r,n})$. □

An immediate consequence of Theorem 7 is the following result showing that our near-threshold black-box secret sharing schemes are expansionless.

MAIN THEOREM 1. *For any odd integer $\varrho \geq 3$, there exists a near-threshold BBSSS over the access structure $\mathfrak{R}_{t,r,n}$ with expansion factor ϱ and $r - t = \exp(-O(\varrho))n$. Furthermore, this is expansionless, i.e., every near-threshold BBSSS over the access structure $\mathfrak{R}_{t,r,n}$ with expansion factor ϱ must obey $r - t = \exp(-\Omega(\varrho))n$.*

Proof. The first part follows from Theorem 7, while the second part follows from Theorem 5.

□

References

[1] G. R. Blakley, *Safeguarding cryptographic keys,* In Proc. National Computer Conference'79, volume 48 of AFIPS Proceedings, pages 313-317, 1979.

[2] A. Beimel, *Secure schemes for secret sharing and key distribution,* Ph.D.-thesis, Technion, Haifa, June 1996.

[3] J. Benaloh and J. Leichter, *Generalized secret sharing and monotone functions,* In: Proc. CRYPTO'88, Springer LNCS, vol. 765, pp. 274-285, 1988.

[4] M. Bertilsson, I. Ingemarsson,*A construction of practical secret sharing schemes using linear block codes,* In Proc. AUSCRYPT'92, Springer LNCS, vol. 718, pp. 67-79, 1993.

[5] S. Blackburn, M. Burmester, Y. Desmedt, and P. Wild, *Efficient multiplicative sharing scheme,* In: Proc. EUROCRYPT'96, Springer LNCS, vol. 1070, pp. 107-118, 1996.

[6] R. Coulangeon, M. I. Icaza and M. ORyan, *Lenstras Constant and Extreme Forms in Number Fields,* https://projecteuclid.org.

[7] I. Cascudo, H. Chen, R. Cramer, and C. Xing, *Asymptotically Good Ideal Linear Secret Sharing with Strong Multiplication over Any Fixed Finite Field,* Advances in CryptographyCrypto 09, LNCS 5677, pp. 466C486, 2009.

[8] R. Cramer and Ivan Damgård, *On the Amortized Complexity of Zero-Knowledge Protocols,* CRYPTO 2009: 177-191

[9] R. Cramer, I. Damgård, and U. Maurer, *Efficient general secure multi-party computation from any linear secret-sharing scheme,* Advances in Cryptography, Springer LNCS, vol. 1807, pp. 316C334, 2000.

[10] R. Cramer, I. Damgård and J. Buus Nielsen, "Secure Multiparty Computation and Secret Sharing," Cambridge University Press 2015, ISBN 9781107043053

[11] H. Chen, R. Cramer, S. Goldwasser, R. de Haan and V. Vaikuntanathan, *Secure Computation from Random Error Correcting Codes,* EUROCRYPT 2007: 291-310

[12] R. Cramer and S. Fehr, *Optimal black-box secret sharing over arbitrary Abelian groups,* Advances in Cryptography-Crypto 02, LNCS 2442, pp. 272C287, Springer-Verlag, 2002.

[13] R. Cramer, S. Fehr, Y. Ishai, and E. Kushilevitz, *Efficient multi-party computation over rings,* Advances in Cryptography-2003 LNCS 2656, pp. 596C613, 2003.

[14] R. Cramer, S. Fehr, and M. Stam, *Black-Box Secret Sharing from Primitive Sets in Algebraic Number Fields,* Advances in Cryptography-Crypto 02, LNCS 2442, pp. 344-360, Springer-Verlag, 2002.

[15] Y. Desmedt and Y. Frankel, *Threshold cryptosystem,* Advances in Cryptography-Crypto89, volume 435 of Lecture Notes in Computer Science, pages 307-315. Springer-Verlag, 1989.

[16] Y. Desmedt and Y. Frankel, *Perfect Homomorphic Zero-Knowledge Threshold Schemes over any Finite Abelian Group,* SIAM J. Discrete Math. 7(4): 667-679 (1994)

[17] Y. Desmedt, B. King, W. Kishimoto, and K. Kurosawa, *A comment on the efficiency of secret sharing scheme over any finite abelian group,* ACISP97, volume 1438 of Lecture Notes in Computer Science, pages 391-402. Springer-Verlag, 1998.

[18] I. Damgård nad R. Thorbek, *Linear Integer Secret Sharing and Distributed Exponentiation,* Public Key Cryptography 2006: 75-90

[19] A. Gál, *Combinatorial methods in boolean function complexity,* Ph.D.-thesis, University of Chicago, 1995.

[20] J. Benaloh and J. Leichter, *Generalized secret sharing and monotone functions,* Advances in CryptographyCrypto 1988, Springer LNCS, vol. 765, pp. 274C285, 1988.

[21] A. Garcia and H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Invent. Math. **121**(1995), 211–222.

[22] A. Garcia and H. Stichtenoth, *On the asymptotic behavior of some towers of function fields over finite fields*, J. Number Theory **61**(1996), 248–273.

[23] Y. Desmedt and Y. Frankel, *Threshold cryptosystem,* Crypto'89, volume 435 of Lecture Notes in Computer Science, pages 307-315. Springer-Verlag, 1990.

[24] M. Karchmer and A. Wigderson, *On span programs,* In: Proc. Structures in Complexity Theory'93, IEEE Computer Society Press, pp. 102-111, 1993.

[25] B. S. King, *Some Results in Linear Secret Sharing,* PhD thesis, University of Wisconsin-Milwaukee, 2000.

[26] M. Karchmer and A. Wigderson, *On Span Programs,* Structure in Complexity Theory Conference 1993: 102-111

[27] J. L. Massey, *Minimal codewords and secret sharing,* In: Proceedings of the 6th Joint Swedish-Russian Workshop on Information Theory, (1993)269C279

[28] L. Massey, P. G. Farrell, *Some applications of coding theory in cryptography, Codes and Ciphers Cryptography and Coding IV,* Formara Lt, Esses, England, pp. 33-47, 1995.

[29] S. Lang, "Survey of Diophantine geometry," Springer-Verlag, 1997.

[30] S. Ling and Chaoping Xing, "Coding Theorya first course," Cambridge University Press, 2004.

[31] van Lint, J.H.: Introduction to Coding Theory. Graduate Texts in Mathematics. Springer, Heidelberg, 1999.

[32] H. Niederreiter and C.P. Xing, Rational Points on Curves over Finite Fields: Theory and Applications, LMS **285**, Cambridge, 2001.

[33] A. Shamir, *How to share a secret,* Communications of the ACM, 22(11):612-613, 1979.

[34] V. Shoup, *Practical Threshold Signatures,* EUROCRYPT 2000: 207-220.

[35] H. Stichtenoth, *Algebraic Function Fields and Codes*, Graduate Texts in Mathematics **254**, Springer Verlag, 2009.

[36] D. Stinson and R. Wei, *Bibliography on Secret Sharing Schemes,* http://www.cacr.math.uwaterloo.ca/∼dstinson/ssbib.html, 2003.

[37] M. A. Tsfasman and S.G.Vlăduţ, “Algebraic-Geometric Codes,” Amsterdam, The Netherlands: Kluwer, 1991.

[38] L. Valiant, *Short Monotone Formulae for the Majority Function,* Journal of Algorithms , Vol. 5 (3), pages 363–366, 1984.

[39] C. Xing and S. L. Yeo, *Construction of Global Function Fields from Linear Codes and Vice Versa,* Trans. Amer. Math. Soc. 361 (2009), 1333-1349.

A The subfields of the Garcia-Stichtenoth tower

In the original Garcia-Stichtenoth tower $\{E_i/\mathbb{F}_{p^m}\}_{i=1}^{\infty}$ (see [21, 22], the extension degree $[E_{i+1}:E_i]=p^m$ for all $i\geq 1$. However, in order to have a tower of slowly growing genus, we split each extension E_{i+1}/E_i into m extensions of degree p.

Lemma 15. *Let m be an even number and let p be a prime. Then there exists a function field family $\{F_i/\mathbb{F}_{p^m}\}_{i=1}^{\infty}$ such that, for every $i\geq 1$, the genus $\mathfrak{g}(F_i)$ is upper bounded by $p^i(p^{m/2}+1)$ and the number $N(F_i)$ is lower bounded by $p^i(p^m-1)$.*

Proof. Put $r=p^{m/2}$. Let $E_1\subseteq E_2\subseteq\dots$ be the tower of global function fields over $\mathbb{F}_{p^m}$ constructed by Garcia and Stichtenoth [21], that is, $E_1=\mathbb{F}_{p^m}(x_1)$ is a rational function field and $E_{n+1}=E_n(z_{n+1})$ for $n=1,2,\dots$ with

$$z_{n+1}^r+z_{n+1}=x_n^{r+1}\qquad\text{and}\qquad x_{n+1}=\frac{z_{n+1}}{x_n}.$$

Then E_{n+1}/E_n is a Galois extension of degree r and $\mathrm{Gal}(E_{n+1}/E_n)\simeq\mathbb{Z}_p^{m/2}$ for each $n\geq 1$. Hence there exists a chain of fields

$$E_n=K_{n,0}\subset K_{n,1}\subset\dots\subset K_{n,m/2}=E_{n+1}$$

such that $[K_{n,i+1}:K_{n,i}]=p$ for $0\leq i\leq m/2-1$. From results in [21] we know that for all $n\geq 1$ we have

$$\mathfrak{g}(E_n)\leq r^n+r^{n-1},\qquad N(E_n)\geq(p^m-1)r^{n-1}+1.$$

The last inequality implies

$$N(K_{n,i})\geq\frac{N(E_{n+1})}{[E_{n+1}:K_{n,i}]}\geq p^i(p^m-1)r^{n-1}+1\qquad\text{for } 0\leq i\leq m/2.$$

Next we establish an upper bound for $\mathfrak{g}(K_{n,i})$. From [21] we know that for each place P of E_n that is ramified in the extension E_{n+1}/E_n we have $\nu_P(x_n)=-1$, and therefore we obtain

$\nu_P(x_n^{r+1}) = -r-1$. It follows that P is totally ramified in E_{n+1}/E_n. According to [21], the sum of the degrees of these places P is equal to $r^{\lfloor n/2 \rfloor}$, and so the same holds for the sum of the degrees of the places P' of $K_{n,i}$ that are ramified in $E_{n+1}/K_{n,i}$, where $0 \leq i \leq m/2-1$. For any such P' and the unique place P'' of E_{n+1} lying over it we have

$$d(P''|P') = (p^{m/2-i}-1)(r+2).$$

By combining these facts with the Hurwitz genus formula, we obtain

$$2\mathfrak{g}(E_{n+1}) - 2 = p^{m/2-i}(2\mathfrak{g}(K_{n,i}) - 2) + r^{\lfloor n/2 \rfloor}(r+2)(p^{m/2-i}-1)$$

for $0 \leq i \leq m/2$, and so

$$\mathfrak{g}(K_{n,i}) \leq \frac{p^i}{r}\left(\mathfrak{g}(E_{n+1}) - 1\right) - \frac{1}{2} r^{\lfloor n/2 \rfloor - 1}(r+2)(r-p^i) + 1 \leq p^i \left(r^n + r^{n-1}\right).$$

Taking $\{F_i\}$ be the family $\{K_{0,0}, K_{0,1}, \ldots, K_{0,m/2}, K_{1,0}, K_{1,1}, \ldots, K_{1,m/2}, \ldots\}$ gives the desired result. □