Optimal Black-Box Secret Sharing over Arbitrary Abelian Groups

Ronald Cramer and Serge Fehr

BRICS*, Department of Computer Science, Aarhus University, Denmark
{cramer,fehr}@brics.dk

Abstract. A *black-box* secret sharing scheme for the threshold access structure $T_{t,n}$ is one which works over any finite Abelian group G. Briefly, such a scheme differs from an ordinary linear secret sharing scheme (over, say, a given finite field) in that distribution matrix and reconstruction vectors are defined over $\mathbb{Z}$ and are designed *independently* of the group G from which the secret and the shares are sampled. This means that perfect completeness and perfect privacy are guaranteed *regardless* of which group G is chosen. We define the black-box secret sharing problem as the problem of devising, for an arbitrary given $T_{t,n}$, a scheme with minimal expansion factor, i.e., where the length of the full vector of shares divided by the number of players n is minimal.
Such schemes are relevant for instance in the context of distributed cryptosystems based on groups with secret or hard to compute group order. A recent example is secure general multi-party computation over black-box rings.
In 1994 Desmedt and Frankel have proposed an elegant approach to the black-box secret sharing problem based in part on polynomial interpolation over cyclotomic number fields. For arbitrary given $T_{t,n}$ with $0 < t < n - 1$, the expansion factor of their scheme is $O(n)$. This is the best previous general approach to the problem.
Using certain low degree integral extensions of $\mathbb{Z}$ over which there exist pairs of sufficiently large Vandermonde matrices with co-prime determinants, we construct, for arbitrary given $T_{t,n}$ with $0 < t < n - 1$, a black-box secret sharing scheme with expansion factor $O(\log n)$, which we show is minimal.

1 Introduction

A *black-box* secret sharing scheme for the threshold access structure $T_{t,n}$ is one which works over any finite Abelian group G. Briefly, such a scheme differs from an ordinary linear secret sharing scheme (over, say, a given finite field; see e.g. [5, 24, 6, 3, 2, 20, 19, 1, 16, 8]) in that distribution matrix and reconstruction vectors are defined over $\mathbb{Z}$ and are designed *independently* of the group G from which the secret and the shares may be sampled. In other words, the dealer computes

* Basic Research in Computer Science (www.brics.dk), funded by the Danish National Research Foundation.

the shares for the n players as $\mathbb{Z}$-linear combinations of the secret group element of his interest and secret randomizing group elements, and reconstruction of the secret from the shares held by a large enough set of players is by taking $\mathbb{Z}$-linear combinations over those shares. Note that each player may receive one or more group elements as his share in the secret. Perfect completeness and perfect privacy are guaranteed *regardless* of which group G is chosen. Here, perfect completeness means that the secret is uniquely determined by the joint shares of at least $t+1$ players, and perfect privacy means that the joint shares of at most t players contain no Shannon information at all about the secret of interest. Note that these schemes are homomorphic in the sense that the sum of share vectors is a share vector for the sum of the corresponding secrets.

We define the black-box secret sharing problem as the problem of devising, for an arbitrary given $T_{t,n}$, a scheme with minimal expansion factor, i.e., where the length of the full vector of shares divided by the number of players n is minimized. [1] Note the case $t = n - 1$ is easily solved by "additive n-out-of-n sharing," which has expansion factor 1. The cases $t = 0, n$ have no meaning for secret sharing. For the rest of this discussion we assume $0 < t < n - 1$.

The idea of black-box secret sharing was first considered by Desmedt and Frankel [11] in the context of distributed cryptosystems based on groups with secret order. Shamir's polynomial based secret sharing scheme over finite fields [24] cannot immediately be adapted to the setting of black-box secret sharing. Later, Desmedt and Frankel [12] showed a black-box secret sharing scheme that elegantly circumvents problems with polynomial interpolation over the integers by passing to an integral extension ring of $\mathbb{Z}$ over which a sufficiently large *invertible* Vandermonde matrix exists. Their scheme is then constructed using the fact that (sufficiently many copies of) an arbitrary Abelian group can be viewed as a module over such an extension ring.

For a given commutative ring R with 1, the largest integer l such that there exists an invertible $l \times l$ Vandermonde matrix with entries in R is called the *Lenstra constant* $l(R)$ of the ring R. Equivalently, $l(R)$ is the maximal size of a subset E of R that is "exceptional" in that for all $\alpha, \alpha' \in E$, $\alpha \neq \alpha'$, it holds that $\alpha - \alpha'$ is a unit of R.

Given an integral extension ring R of degree m over $\mathbb{Z}$, they construct a black-box secret sharing scheme with expansion factor m for a threshold access structure on *at most* $l(R) - 1$ players. For any prime p, Lenstra's constant for the ring of integers of the pth cyclotomic number field is p. [2] Given an arbitrary $T_{t,n}$ and choosing R as the ring of integers of the pth cyclotomic number field,

[1] That minimal expansion is at most polynomial in n, even when appropriately generalizing the concept to encompass non-Abelian groups as well, is verified by combination of the technique of Benaloh-Leichter [2] with the classical result of complexity theory that all monotone threshold functions are representable by poly-size monotone Boolean formulas. See also [10].

[2] It is not hard to find an exceptional set of size p in this ring. To see that the maximal size of such a set is p, let K be a number field of degree m, and let $\mathbb{Z}_K$ denote its ring of algebraic integers. For an arbitrary non-trivial ideal I of $\mathbb{Z}_K$, it is easy to see that $l(\mathbb{Z}_K) \leq |\mathbb{Z}_K/I|$ ($\leq 2^m$). In the case where K is the pth cyclotomic number

where p is the smallest prime greater than n, they construct a black-box secret sharing scheme for $T_{t,n}$ with expansion factor between n and $2n$. This is the best previous general approach to the problem. Further progress on the black-box secret sharing problem via the approach of [12] depends on the problem of finding for each n an extension whose degree is *substantially* smaller than n and whose Lenstra constant is greater than n. To the best of our knowledge, this is an open problem of algebraic number theory (see also [12] and the references therein).

Except for some quite special cases, namely when t is constant or when t (resp. $n-t$) is small compared to n [14, 4] or the constant factor gain from [15], no substantial improvement on the general black-box secret sharing problem has been reported since.

The crucial difference with our approach to the black-box secret sharing problem is that we avoid dependence on Lenstra's constant altogether. Namely, first, we observe that a sufficient condition for black-box secret sharing is the existence (over an extension of $\mathbb{Z}$) of *a pair* of sufficiently large Vandermonde matrices with *co-prime determinants*. And, second, we show how to construct *low degree* integral extensions of $\mathbb{Z}$ satisfying this condition. For arbitrary given $T_{t,n}$, this leads to a black-box secret sharing scheme with expansion factor $O(\log n)$. Using a result of Karchmer and Wigderson [20], we show that this is minimal.

There are several applications of black-box secret sharing. For instance, the result of [12] is exploited in [13] to obtain an efficient and secure solution for sharing any function out of a certain abstract class of functions, including RSA. The interest in application of the result of [12] to practical distributed RSA-based protocols seems to have decreased somewhat due to recent developments, see for instance [25] and the references therein. However, apart from the fact that optimal black-box secret sharing is perhaps interesting in its own right, we note that in [9] our black-box secret sharing scheme is applied in protocols for secure general multi-party computation over black-box rings. Also, optimal black-box secret sharing may very well be relevant to new distributed cryptographic schemes for instance based on class groups.

This paper is organized as follows. In Section 2 we give a formalization of the notion of black-box secret sharing, and show a natural correspondence between such schemes and our notion of *integer span programs* (ISPs). This generalizes the well-known correspondence between monotone span programs over finite fields [20] and linear secret sharing schemes over finite fields. In Section 3 we show lower bounds on the size of ISPs computing threshold access structures. Our main result is presented in Section 4, where we construct an ISP with minimal size for an arbitrary given threshold access structure. This leads to an optimal black-box secret sharing scheme for an arbitrary given threshold access structure. At the end, we point out further combinatorial properties of our scheme that are useful when exhibiting *efficient simulators* as required in the security proofs of threshold crypto-systems such as threshold RSA.

---

field, the integer prime p totally ramifies. Hence $l(\mathbb{Z}_K) \leq |\mathbb{Z}_K/P| = p$, where P is the unique prime ideal of $\mathbb{Z}_K$ lying above p.

2 Black-Box Secret Sharing

2.1 Definitions

Definition 1. *A* monotone access structure *on* $\{1, \ldots, n\}$ *is a non-empty collection* Γ *of sets* $A \subset \{1, \ldots, n\}$ *such that* $\emptyset \notin \Gamma$ *and such that for all* $A \in \Gamma$ *and for all sets* B *with* $A \subset B \subset \{1, \ldots, n\}$ *it holds that* $B \in \Gamma$.

Definition 2. *Let* t *and* n *be integers with* $0 < t < n$. *The* threshold access structure $T_{t,n}$ *is the collection of sets* $A \subset \{1, \ldots, n\}$ *with* $|A| > t$. [3]

Let Γ be a monotone access structure on $\{1, \ldots, n\}$. Let $M \in \mathbb{Z}^{d,e}$ be an integer matrix, and let $\psi : \{1, \ldots, d\} \rightarrow \{1, \ldots, n\}$ be a surjective function. We say that the jth row ($j = 1 \ldots d$) of M is *labelled* by $\psi(j)$ or that "$\psi(j)$ owns the jth row." For $A \subset \{1, \ldots, n\}$, M_A denotes the restriction of M to the rows jointly owned by A. Write d_A for the number of rows in M_A. Similarly, for $\mathbf{x} \in \mathbb{Z}^d$, $\mathbf{x}_A \in \mathbb{Z}^{d_A}$ denotes the restriction of $\mathbf{x}$ to the coordinates jointly owned by A. For each $A \in \Gamma$, let $\boldsymbol{\lambda}(A) \in \mathbb{Z}^{d_A}$ be an integer (column-) vector. We call this the *reconstruction vector for* A. Collect all these vectors in a set $\mathcal{R}$.

Definition 3. *Let* Γ *be a monotone access structure on* $\{1, \ldots, n\}$*, and let* $\mathcal{B} = (M, \psi, \mathcal{R})$ *be as defined above.* $\mathcal{B}$ *is called an* integer Γ-scheme. *Its* expansion rate *is defined as* d/n*, where* d *is the number of rows of* M.

Let G be a finite Abelian group. We use additive notation for its group operation, and use 0_G to denote its neutral element. The group G is of course a $\mathbb{Z}$-module (see e.g. [23]), by defining the map $\mathbb{Z} \times G \rightarrow G,\ (\mu, g) \mapsto \mu \cdot g$, where $0 \cdot g = 0_G$, $\mu \cdot g = g + \ldots + g$ (μ times) for $\mu > 0$ and $\mu \cdot g = -((-\mu) \cdot g)$ for $\mu < 0$. [4] We also write μg or $g\mu$ instead of $\mu \cdot g$. Note that it is well-defined how an integer matrix acts on a vector of group elements.

Definition 4. *Let* Γ *be a monotone access structure on* $\{1, \ldots, n\}$ *and let* $\mathcal{B} = (M, \psi, \mathcal{R})$ *be an integer* Γ*-scheme. Then* $\mathcal{B}$ *is a* black-box secret sharing scheme *for* Γ *if the following holds. Let* G *be an arbitrary finite Abelian group* G*, and let* $A \subset \{1, \ldots, n\}$ *be an arbitrary non-empty set. For arbitrarily distributed* $s \in G$*, let* $\mathbf{g} = (g_1, \ldots, g_e)^T \in G^e$ *be drawn uniformly at random, subject to* $g_1 = s$. *Define* $\mathbf{s} = M\mathbf{g}$. *Then:*

- (Completeness) *If* $A \in \Gamma$*, then* $\mathbf{s}_A^T \cdot \boldsymbol{\lambda}(A) = s$ *with probability 1, where* $\boldsymbol{\lambda}(A) \in \mathcal{R}$ *is the reconstruction vector for* A.
- (Privacy) *If* $A \notin \Gamma$*, then* $\mathbf{s}_A$ *contains no Shannon information on* s.

[3] Note that some authors define $T_{t,n}$ as consisting of all sets of size *at least* t. Our definition is consistent with a convention in the multi-party computation literature.

[4] If the group operation in G is efficient, multiplication by an integer can also be efficiently implemented using standard "double-and-add."

Note that these schemes [5] are homomorphic in the sense that the sum $\mathbf{s}+\mathbf{s}'$ of two share vectors $\mathbf{s}$ and $\mathbf{s}'$, is a share vector for the sum $s+s'$ of their corresponding secrets s and s'.

2.2 Monotone Span Programs over Rings

In this section we provide quite natural necessary and sufficient conditions under which an integer Γ-scheme is a black-box secret sharing scheme for Γ. To this end, we introduce the notion of *monotone span programs over rings*. This is a certain variation of monotone span programs over finite fields, introduced by Karchmer and Wigderson [20]. These are well-known to have a natural one-to-one correspondence with linear secret sharing schemes over *finite fields* (see e.g. [19, 1]). Monotone span programs over $\mathbb{Z}$ (*ISPs*) will turn out to have a similar correspondence with black-box secret sharing schemes. We also show an efficient conversion of a monotone span program over an integral extension ring of $\mathbb{Z}$ to an ISP.

As an aside, monotone span programs over rings are the basis for multi-party computation over black-box rings, as studied in [9]. In particular, the techniques of [8] for secure multiplication and VSS apply to this flavor of monotone span program as well.

Throughout this paper, R denotes a (not necessarily finite) commutative ring with 1. Let Γ be a monotone access structure on $\{1,\ldots,n\}$, and let $M \in R^{d,e}$ be a matrix whose d rows are labelled by a surjective function $\psi : \{1,\ldots,d\} \to \{1,\ldots,n\}$.

Definition 5. *$\boldsymbol{\varepsilon} = (1,0,\ldots,0)^T \in R^e$ is called the* target vector. *Furthermore, $\mathcal{M} = (R, M, \psi, \boldsymbol{\varepsilon})$ is called a* monotone span program (over the ring R). *If $R=\mathbb{Z}$, it is called an integer span program, or ISP, for short. We define* size$(\mathcal{M}) = d$, *where d is the number of rows of M.*

For $N \in R^{a,b}$, $\mathrm{im}N$ denotes its column space, i.e., the space of all vectors $N\mathbf{x} \in R^a$, where $\mathbf{x}$ ranges over R^b, and $\ker N$ denotes its null-space, i.e., the space of all vectors $\mathbf{x} \in R^b$ with $N\mathbf{x} = \mathbf{0} \in R^a$.

Definition 6. *As above, let Γ be a monotone access structure and let $\mathcal{M} = (R, M, \psi, \boldsymbol{\varepsilon})$ be a monotone span program over R. Then $\mathcal{M}$ is a monotone span program* for Γ, *if for all $A \subset \{1,\ldots,n\}$ the following holds.*

- *If $A \in \Gamma$, then $\boldsymbol{\varepsilon} \in \mathrm{im}M_A^T$.*
- *If $A \notin \Gamma$, then there exists $\boldsymbol{\kappa} = (\kappa_1,\ldots,\kappa_e)^T \in \ker M_A$ with $\kappa_1 = 1$.*

We also say that $\mathcal{M}$ computes *Γ.*

[5] See [21] for an equivalent definition. We also note that only requiring reconstruction to be linear, as some authors do, results in an equivalent definition of black-box secret sharing. This is an easily proved consequence of Lemma 2, but we omit the details here.

If R is a *field*, our definition is equivalent to the computational model of monotone span programs over fields [20]. Indeed, this model is characterized by the condition that $A \in \Gamma$ if and only if $\boldsymbol{\varepsilon} \in \mathrm{im} M_A^T$. The equivalence follows from the remark below.

Remark 1. By basic linear algebra, if R is a *field*, then $\boldsymbol{\varepsilon} \notin \mathrm{im} M_A^T$ implies that there exists $\boldsymbol{\kappa} \in \ker M_A$ with $\kappa_1 = 1$. If R is *not a field* this does not necessarily hold. [6] The implication in the other direction trivially holds regardless of R.

Using (generally inefficient) representations of monotone access structures as monotone Boolean formulas and using induction in a similar style as in e.g. [2], it is straightforward to verify that for all Γ and for all R, there is a monotone span program over R that computes Γ.

Definition 7. *For any Γ and for any R, $\mathrm{msp}_R(\Gamma)$ denotes the minimal size of a monotone span program over R computing Γ. If $R = \mathbb{Z}$, we write $\mathrm{isp}(\Gamma)$.*

Define a *non-degenerate monotone span program* as one for which the rows of M span the target-vector. As opposed to the case of fields, a non-degenerate monotone span program over a ring need not compute any monotone access structure. This is of no concern here, though.

The following proposition characterizes black-box secret sharing schemes in terms of ISPs.

Proposition 1. *Let Γ be a monotone access structure on $\{1, \ldots, n\}$, and let $\mathcal{B} = (M, \psi, \mathcal{R})$ be an integer Γ-scheme. Then $\mathcal{B}$ is a black-box secret sharing scheme for Γ if and only if $\mathcal{M} = (\mathbb{Z}, M, \psi, \boldsymbol{\varepsilon})$ is an ISP for Γ and for all $A \in \Gamma$, its reconstruction vector $\boldsymbol{\lambda}(A) \in \mathcal{R}$ satisfies $M_A^T \boldsymbol{\lambda}(A) = \boldsymbol{\varepsilon}$.*

Proof. The argument that the stated ISP is sufficient for black-box secret sharing is quite similar to the well-known case of linear secret sharing over finite fields. The other direction of the implication follows in essence from Lemma 1 below. We include full details for convenience.

Consider the ISP from the statement of the proposition, together with the assumption on the reconstruction vectors. Consider an arbitrary set $A \subset \{1, \ldots, n\}$ and an arbitrary finite Abelian group G. Define $\mathbf{s} = M\mathbf{g}$ for arbitrary $\mathbf{g} = (s, g_2, \ldots, g_e)^T \in G^e$. Suppose $A \in \Gamma$, and let $\boldsymbol{\lambda}(A) \in \mathcal{R}$ be its reconstruction vector. It follows that $\mathbf{s}_A^T \boldsymbol{\lambda}(A) = (M_A \mathbf{g})^T \boldsymbol{\lambda}(A) = \mathbf{g}^T (M_A^T \boldsymbol{\lambda}(A)) = \mathbf{g}^T \boldsymbol{\varepsilon} = s$. Thus the completeness condition from Definition 4 is satisfied. If $A \notin \Gamma$, then there exists $\boldsymbol{\kappa} \in \mathbb{Z}^e$ with $M_A \boldsymbol{\kappa} = \mathbf{0} \in \mathbb{Z}^{d_A}$ and $\kappa_1 = 1$, by Definition 6. For arbitrary $s' \in G$, define $\mathbf{s}' = M(\mathbf{g} + (s' - s)\boldsymbol{\kappa}) \in G^{d_A}$. The secret defined by $\mathbf{s}'$ equals s', while on the other hand $\mathbf{s}'_A = \mathbf{s}_A$. This implies perfect privacy: the assignment $\mathbf{g}' = \mathbf{g} + (s' - s)\boldsymbol{\kappa}$ provides a bijection between the set of possible vectors of "random coins" consistent with $\mathbf{s}_A$ and s, and the set of those consistent with $\mathbf{s}_A$ and s'. Therefore, the privacy condition from Definition 4 is also satisfied.

[6] Consider for example the integer matrix $M = (2\ 0)$.

In the other direction of the proposition, we start with a black-box secret sharing scheme for Γ according to Definition 4. Consider an arbitrary set $A \subset \{1, \ldots, n\}$. Suppose $A \in \Gamma$, and let $\boldsymbol{\lambda}(A) \in \mathcal{R}$ be its reconstruction vector. For an arbitrary prime p, set $G = \mathbb{Z}_p$. By the completeness condition from Definition 4, it follows that $(1, 0, \ldots, 0)^T \equiv (M_A I_e)^T \boldsymbol{\lambda}(A) \equiv M_A^T \boldsymbol{\lambda}(A) \bmod p$, where $I_e \in \mathbb{Z}_p^{e,e}$ is the identity matrix. This holds for all primes p. Hence, $M_A^T \boldsymbol{\lambda}(A) = (1, 0, \ldots, 0)^T = \boldsymbol{\varepsilon}$. Therefore, the condition on the sets $A \in \Gamma$ in Definition 6 and the condition on the reconstruction vectors $\mathcal{R}$ from the statement of the proposition are satisfied.

To conclude the proof we show that the privacy condition from Definition 4 implies the condition on the sets $A \notin \Gamma$ from Definition 6. The following formulation is equivalent. Let $\mathbf{y} \in \mathbb{Z}^{d_A}$ denote the left-most column of M_A, and let $N_A \in \mathbb{Z}^{d_A, e-1}$ denote the remaining $e-1$ columns. Then it is to be shown that the linear system of equations $N_A \mathbf{x} = \mathbf{y}$ is solvable over $\mathbb{Z}$.

By Lemma 1 below, it is sufficient to show that this holds modulo m, for all $m \in \mathbb{Z}$, $m \neq 0$. With notation as in Definition 4 and considering $G = \mathbb{Z}_m$, it follows from the privacy condition that there exists $\mathbf{g}' \in \mathbb{Z}_m^e$ such that $g_1' \equiv s - 1$ and $\mathbf{s}_A \equiv M_A \mathbf{g}'$. Setting $\boldsymbol{\kappa} \equiv \mathbf{g} - \mathbf{g}' \in \mathbb{Z}_m^e$, we have $M_A \boldsymbol{\kappa} \equiv \mathbf{0}$ with $\kappa_1 \equiv 1$. In other words, $N_A \mathbf{x} = \mathbf{y}$ is solvable over $\mathbb{Z}_m$ for all integers $m \neq 0$. □

We note that [21] also gives a characterization. Although there are some similarities in the technical analysis, the conditions stated there are still in terms of the black-box secret sharing scheme, rather than by providing simple algebraic conditions on the matrix M as we do. Therefore, we feel that our approach based on integer span programs is perhaps more useful and insightful, especially since monotone span programs over finite fields have since long been known to be equivalent to linear secret sharing schemes over finite fields.

Lemma 1. *Let $N \in \mathbb{Z}^{a,b}$ and $\mathbf{y} \in \mathbb{Z}^a$. Then the linear system of equations $N\mathbf{x} = \mathbf{y}$ is solvable over $\mathbb{Z}$ if and only if it is solvable over $\mathbb{Z}_m$ for all integers $m \neq 0$.*

Proof. The forward direction of the proposition is trivial. In the other direction, consider the $\mathbb{Z}$-module H generated by the columns of N. By basic theory of $\mathbb{Z}$-modules (see e.g. [23]), there exists a $\mathbb{Z}$-basis $\mathcal{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_a)$ of $\mathbb{Z}^a$, and non-zero integers $a_1, \ldots, a_l$ such that $\mathcal{B}_H = (a_1 \mathbf{b}_1, \ldots, a_l \mathbf{b}_l)$ is a $\mathbb{Z}$-basis of H. Let L denote the $\mathbb{Z}$-module with basis $\mathcal{B}_L = (\mathbf{b}_1, \ldots, \mathbf{b}_l)$. Note that $H \subset L$. Let p be an arbitrary prime, and let $\overline{(\cdot)}$ denote reduction modulo p. Since the determinant of $\mathcal{B}$ is ± 1, $\overline{\mathcal{B}}$ (resp. $\overline{\mathcal{B}}_L$) provides a basis for the vector-space $\mathbb{F}_p^a$ (resp. the vector-space $\overline{L}$). Note that $\overline{\mathcal{B}}_L \subset \overline{\mathcal{B}}$.

It follows from the assumptions that $\overline{\mathbf{y}} \in \overline{H} \subset \overline{L}$. Let $(y_1, \ldots, y_a) \in \mathbb{Z}^a$ denote the coordinates of $\mathbf{y}$ wrt. $\mathcal{B}$. Since the latter observation holds for all primes p, it follows that $y_{l+1} = \ldots = y_a = 0$. Hence, $\mathbf{y} \in L$. Now set $\hat{m} = \prod_{i=1}^{l} a_i$. By the assumptions, there exists $\mathbf{c}_{\hat{m}} \in \mathbb{Z}^a$ such that $\mathbf{y} + \hat{m} \cdot \mathbf{c}_{\hat{m}} \in H$. Therefore, $\hat{m} \cdot \mathbf{c}_{\hat{m}} \in L$, and by the definition of L, $\mathbf{c}_{\hat{m}} \in L$. By the choice of $\hat{m}$, it follows that $\hat{m} \cdot \mathbf{c}_{\hat{m}} \in H$. We conclude that $\mathbf{y} \in H$, as desired. □

Remark 2. Let $\mathcal{M} = (R, M, \psi, \boldsymbol{\varepsilon})$ compute Γ. If R is a field or a principal ideal domain (such as $\mathbb{Z}$), then we may assume without loss of generality that $e \le d$, i.e., there are at most as many columns in M as there are rows.

This is easily shown using elementary linear algebra, and using the basic properties of modules over principal ideal domains (see e.g. [23] and the proof of Lemma 1). Briefly, since $\mathcal{M}$ is non-degenerate, the last statement in Remark 1 implies that the space generated by the 2nd up to the eth column of M does not contain even a non-zero multiple of the first column. Without changing the access structure that is computed, we can always replace the 2nd up to the eth column of M by any set of vectors that generates the same space. If R is a field or a principal ideal domain, this space has a basis of cardinality at most $d - 1$.

Remark 3. We may now identify a black-box secret sharing scheme for Γ with an ISP $\mathcal{M} = (\mathbb{Z}, M, \psi, \boldsymbol{\varepsilon})$ for Γ. A reconstruction vector for $A \in \Gamma$ is simply any vector $\boldsymbol{\lambda}(A) \in \mathbb{Z}^{d_A}$ such that $M_A^T \boldsymbol{\lambda}(A) = \boldsymbol{\varepsilon}$. Note that the expansion rate of the corresponding black-box secret sharing scheme is equal to $\text{size}(\mathcal{M})/n$. By Remark 2 it uses at most $\text{size}(\mathcal{M})$ random group elements.

We now state some lemmas that are useful in the sequel.

Definition 8. *The dual Γ^* of a monotone access structure Γ on $\{1, \ldots, n\}$ is the collection of sets $A \subset \{1, \ldots, n\}$ such that $A^c \notin \Gamma$.*

Note that Γ^* is a monotone access structure on $\{1, \ldots, n\}$, that $(\Gamma^*)^* = \Gamma$, and that $(T_{t,n})^* = T_{n-t-1,n}$. The lemma below generalizes a similar property shown in [20] for the case of fields.

Lemma 2. $\text{msp}_R(\Gamma) = \text{msp}_R(\Gamma^*)$*, for all R and Γ.*

Proof. Let $\mathcal{M} = (R, M, \psi, \boldsymbol{\varepsilon})$ be a monotone span program for Γ. Select an arbitrary generating set of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_l$ for $\ker M^T$, and choose $\boldsymbol{\lambda}$ with $M^T \boldsymbol{\lambda} = \boldsymbol{\varepsilon}$. Let M^* be the matrix defined by the $l+1$ columns $(\boldsymbol{\lambda}, \mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_l)$, and use ψ to label M^* as well. Define $\mathcal{M}^* = (R, M^*, \psi, \boldsymbol{\varepsilon}^*)$, where $\boldsymbol{\varepsilon}^* = (1, 0, \ldots, 0)^T \in R^{l+1}$. Note that $\text{size}(\mathcal{M}^*) = \text{size}(\mathcal{M})$. We claim that $\mathcal{M}^*$ computes Γ^*. This is easy to verify.

If $A^c \notin \Gamma$, then by Definition 6, there exists $\boldsymbol{\kappa} \in R^{l+1}$ such that $M_{A^c} \boldsymbol{\kappa} = \mathbf{0}$ and $\kappa_1 = 1$. Define $\boldsymbol{\lambda}^* = M_A \boldsymbol{\kappa}$. Then $(M^*)_A^T \boldsymbol{\lambda}^* = ((M^*)^T \cdot M)\boldsymbol{\kappa} = \boldsymbol{\varepsilon}^*$. On the other hand, if $A^c \in \Gamma$, then there exists $\hat{\boldsymbol{\lambda}} \in R^d$ such that $M^T \hat{\boldsymbol{\lambda}} = \boldsymbol{\varepsilon}$ and $\hat{\boldsymbol{\lambda}}_A = \mathbf{0}$. By definition of M^*, there exists $\boldsymbol{\kappa} \in R^{l+1}$ such that $M^* \boldsymbol{\kappa} = \hat{\boldsymbol{\lambda}}$ and $\kappa_1 = 1$. Hence, $M_A^* \boldsymbol{\kappa} = \hat{\boldsymbol{\lambda}}_A = \mathbf{0}$ and $\kappa_1 = 1$. This concludes the proof. □

The lemma below holds in a more general setting, but we tailor it to ours.

Lemma 3. *Let $f(X) \in \mathbb{Z}[X]$ be a monic, irreducible polynomial. Write $m = \deg(f)$. Consider the ring $R = \mathbb{Z}[X]/(f(X))$. Suppose $\mathcal{M} = (R, M, \psi, \boldsymbol{\varepsilon})$ is a monotone span program over R for a monotone access structure Γ. Then there exists an ISP $\hat{\mathcal{M}} = (\mathbb{Z}, \hat{M}, \hat{\psi}, \hat{\boldsymbol{\varepsilon}})$ for Γ with $\text{size}(\hat{\mathcal{M}}) = m \cdot \text{size}(\mathcal{M})$.*

Proof. The proof is based on a standard algebraic technique for representing a linear map defined over an extension ring in terms of a linear map defined over the ground ring. This technique is also used in [20] for monotone span programs over extension fields. Since our definition of monotone span programs over rings differs slightly from the definitions in [20], we explain it in detail.

Note that R is a commutative ring with 1 and that it has no zero divisors, but that it is not a field. Fix $w \in R$ such that $f(w) = 0$ (such as $w = \overline{X}$, the class of X modulo $f(X)$). Then for each $x \in R$, there exists a unique coordinate-vector $\overrightarrow{x} = (x_0, \ldots, x_{m-1})^T \in \mathbb{Z}^m$ such that $x = x_0 \cdot 1 + x_1 \cdot w + \cdots + x_{m-1} \cdot w^{m-1}$. In other words, $\mathcal{W} = \{1, w, \ldots, w^{m-1}\}$ is a basis for R when viewed as a $\mathbb{Z}$-module.

For each $x \in R$ there exists a matrix in $\mathbb{Z}^{m,m}$, denoted as $[x]$, such that, for all $y \in R$, $[x]\overrightarrow{y} = \overrightarrow{xy}$ (the coordinate vector of $xy \in R$). The columns of $[x]$ are simply the coordinate vectors of $x, x \cdot w, \ldots, x \cdot w^{m-1}$. If $x \in \mathbb{Z}$, then $[x]$ is a diagonal matrix with x's on its main diagonal. Furthermore, for all $x, y \in R$, we have the identities $[x + y] = [x] + [y]$ and $[xy] = [x][y]$.

Consider the monotone span program $\mathcal{M} = (R, M, \psi, \boldsymbol{\varepsilon})$ from the statement of the lemma. As before, write d (resp. e) for the number of rows (resp. columns) of M. We define the ISP $\hat{\mathcal{M}} = (\mathbb{Z}, \hat{M}, \hat{\psi}, \hat{\boldsymbol{\varepsilon}})$ as follows. Construct $\hat{M} \in \mathbb{Z}^{md,me}$ from M by replacing each entry $x \in R$ in M by the matrix $[x]$. The labeling ψ is extended to $\hat{\psi}$ in the obvious way, i.e., if a player owns a certain row in M, then that same player owns the m rows that it is substituted with in $\hat{M}$. The target vector $\hat{\boldsymbol{\varepsilon}}$ is defined by $\hat{\boldsymbol{\varepsilon}} = (1, 0 \ldots, 0)^T \in \mathbb{Z}^{me}$.

We verify that $\hat{\mathcal{M}}$ is an ISP for Γ. First, consider a set $A \in \Gamma$. By definition, there exists a vector $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_{d_A})^T \in R^{d_A}$ such that $M_A^T \boldsymbol{\lambda} = \boldsymbol{\varepsilon}$. Using the identities stated above and carrying out matrix multiplication "block-wise," it follows that $\hat{M}_A^T([\lambda_1], \ldots, [\lambda_{d_A}])^T = ([1], [0], \ldots, [0])^T$. Define $\hat{\boldsymbol{\lambda}} \in \mathbb{Z}^{md_A}$ as the first column of the matrix $([\lambda_1], \ldots, [\lambda_{d_A}])^T$. Then $\hat{M}_A^T \hat{\boldsymbol{\lambda}} = \hat{\boldsymbol{\varepsilon}}$. Now consider a set $A \notin \Gamma$. By definition, there exists $\boldsymbol{\kappa} = (\kappa_1, \kappa_2, \ldots, \kappa_e)^T \in R^e$ such that $\kappa_1 = 1$ and $M_A \boldsymbol{\kappa} = \mathbf{0} \in R^{d_A}$. Using similar reasoning as above, it follows that $\hat{M}_A([\kappa_1]^T, \ldots, [\kappa_e]^T)^T = ([0]^T, \ldots, [0]^T)^T$. Define $\hat{\boldsymbol{\kappa}} \in \mathbb{Z}^{me}$ as the first column of the matrix derived from $\boldsymbol{\kappa}$ in the above equation. Then, the first m entries of $\hat{\boldsymbol{\kappa}}$ are $1, 0, \ldots, 0$ (since $\kappa_1 = 1$) and $\hat{M}_A \hat{\boldsymbol{\kappa}} = \mathbf{0} \in \mathbb{Z}^{d_A}$.

This proves the lemma. As an aside, it follows directly from the analysis above that we may delete the 2nd up to mth leftmost colums of $\hat{M}$ and the corresponding coordinates of $\hat{\boldsymbol{\varepsilon}}$ without changing the access structure computed. Hence, $1 + m(e - 1)$ columns suffice, rather than me. □

3 Lower Bounds for the Threshold Case

Proposition 2. *For all integers t, n with $0 < t < n-1$, $\mathrm{isp}(T_{t,n}) = \Omega(n \cdot \log n)$. Hence, the expansion factor of a black-box secret sharing scheme for $T_{t,n}$ with $0 < t < n - 1$ is $\Omega(\log n)$.*

Proposition 2 follows quite directly from the bound shown in Theorem 1 for binary monotone span programs, as proved in [20]. [7] Before we give the details of the proof of Proposition 2, we include a proof of their bound for convenience. Note that we have made constants for their asymptotic bound explicit.

Throughout this section, K denotes a field. Let $\mathcal{M} = (K, M, \psi, \boldsymbol{\varepsilon})$ be a non-degenerate monotone span program. The access structure of $\mathcal{M}$, denoted $\Gamma(\mathcal{M})$, is the collection of sets A such that $\boldsymbol{\varepsilon} \in \mathrm{im} M_A^T$. Note that by Remark 1 this is consistent with our Definition 6. We write $\mathrm{msp}_2(\Gamma)$ instead of $\mathrm{msp}_{\mathbb{F}_2}(\Gamma)$.

Proposition 3. *[20]* $\mathrm{msp}_2(T_{1,n}) \geq n \cdot \log n$.

Proof. Consider a monotone span program $\mathcal{M} = (\mathbb{F}_2, M, \psi, \boldsymbol{\varepsilon})$ such that $\Gamma(\mathcal{M}) = T_{1,n}$. Define e as the number of columns of M, d as its number of rows, and d_i as the number of rows of M_i for $i = 1 \dots n$, where we write M_i instead of $M_{\{i\}}$ and d_i instead of $d_{\{i\}}$. Without loss of generality, assume that the rows of each M_i are linearly independent over $\mathbb{F}_2$. Let H_1 collect the vectors in $\mathbb{F}_2^e$ with first coordinate equal to 1. Since $\{i\} \notin T_{1,n}$, Remark 1 implies that $|\mathrm{ker} M_i \cap H_1| \neq \emptyset$. By assumption on M_i, $|\mathrm{ker} M_i \cap H_1| = 2^{e-1-d_i}$ for $i = 1 \dots n$. On the other hand, $\{i, j\} \in T_{1,n}$. Hence, by Remark 1, we have $\mathrm{ker} M_i \cap \mathrm{ker} M_j \cap H_1 = \emptyset$, for all i, j with $1 \leq i < j \leq n$. By counting and normalizing, $2^{-d_1} + \cdots + 2^{-d_n} \leq 1$. By the Log Sum Inequality (see e.g. [7]), $d = d_1 + \cdots + d_n \geq n \log n$. □

Theorem 1. *[20]* $n \cdot (\lfloor \log n \rfloor + 1) \geq \mathrm{msp}_2(T_{t,n}) \geq n \cdot \log \frac{n+3}{2}$*, for all* t, n *with* $0 < t < n - 1$.

Proof. The upper bound, which is not needed for our purposes, follows by considering an appropriate Vandermonde matrix over the field $\mathbb{F}_{2^u}$, where $u = (\lfloor \log n \rfloor + 1)$. This is turned into a binary monotone span program for $T_{t,n}$ using a similar conversion technique as in Lemma 3.

For the lower bound, note that we may assume that $t \geq (n-1)/2$, since $\mathrm{msp}_2(T_{t,n}) = \mathrm{msp}_2(T_{n-t-1,n})$ by Lemma 2. We have the following estimates.

$$\begin{aligned} \mathrm{msp}_2(T_{t,n}) &\geq \frac{n}{t+2} \cdot \mathrm{msp}_2(T_{t,t+2}) = \frac{n}{t+2} \cdot \mathrm{msp}_2(T_{1,t+2}) \\ &\geq \frac{n}{t+2} \cdot (t+2) \cdot \log(t+2) \geq n \cdot \log \frac{n+3}{2}. \end{aligned}$$

The first inequality is argued as follows. Consider an arbitrary monotone span program $\mathcal{M} = (\mathbb{F}_2, M, \psi, \boldsymbol{\varepsilon})$ for $T_{t,n}$. Assume without loss of generality that the number of rows in M_i is at most the number of rows in M_{i+1}, $i = 1, \dots, n-1$. The first $t+2$ blocks $M_1, \dots, M_{t+2}$ clearly form a monotone span program for $T_{t,t+2}$. Hence, the total number of rows in these blocks is at least $\mathrm{msp}_2(T_{t,t+2})$. Each other block M_j with $j > t+2$ has at least as many rows as any of the first $t+2$ blocks. Therefore, M_j has at least $\mathrm{msp}_2(T_{t,t+2})/(t+2)$ rows. Summing up over all i according to the observations above gives the first inequality.

The equality is implied by Lemma 2, the second to last inequality follows from Proposition 3, and the last one from $t \geq (n-1)/2$. □

[7] Note that $\mathrm{isp}(T_{n-1,n}) = n$: the case $t = n-1$ is solved by simple additive "n-out-of-n secret sharing."

For the proof of Proposition 2, let an ISP for $T_{t,n}$ be given, and consider the ISP matrix, but with all entries reduced modulo 2. By our ISP definition and by arguing the cases $A \notin T_{t,n}$ using Remark 1, it follows that a binary monotone span program for $T_{t,n}$ is obtained in this way. The argument is concluded by applying Theorem 1. [8] The statement about black-box secret sharing follows from Proposition 1.

Note that our lower bound on black-box secret sharing can also be appreciated without reference to Proposition 1, by essentially the same argument as above. Namely, setting $G = \mathbb{Z}_2$ in Definition 4, we clearly obtain a (binary) linear secret sharing scheme. This is well-known to be equivalent to a binary monotone span program, as mentioned before. Hence, we can directly apply the bound from Theorem 1.

4 Optimal Black-Box Threshold Secret Sharing

Theorem 2. *For all integers t, n with $0 < t < n-1$, $\mathrm{isp}(T_{t,n}) = \Theta(n \cdot \log n)$. Hence, there exists a black-box secret sharing scheme for $T_{t,n}$ with expansion factor $O(\log n)$, which is minimal.*

Proof. By Proposition 1 it is sufficient to focus on the claim about the ISPs. The lower bound follows from Proposition 2. For the upper bound, we consider rings of the form $R = \mathbb{Z}[X]/(f(X))$, where $f(X) \in \mathbb{Z}[X]$ is a monic, irreducible polynomial. Write $m = \deg(f)$, the degree of R over $\mathbb{Z}$.

On account of Lemma 3, it is sufficient to exhibit a ring R together with a monotone span program $\mathcal{M}$ over R for $T_{t,n}$ such that $m = O(\log n)$ and $\mathrm{size}(\mathcal{M}) = O(n)$.

The proof is organized as follows. We first identify a certain technical property of a ring R that facilitates the construction of a monotone span program over R for $T_{t,n}$, with size $O(n)$. We finalize the proof by constructing a ring R that enjoys this technical property, and that has degree $O(\log n)$ over $\mathbb{Z}$.

For $x_1, \ldots, x_n \in R$, define

$$\Delta(x_1, \ldots, x_n) = \prod_{i=1}^{n} x_i \cdot \prod_{1 \leq j < i \leq n} (x_i - x_j).$$

Assume, for the moment, that there exist $\alpha_1, \ldots, \alpha_n \in R$ and $r_0, r_1 \in R$ such that

$$r_0 \cdot \Delta(1, \ldots, n)^2 + r_1 \cdot \Delta(\alpha_1, \ldots, \alpha_n)^2 = 1.$$

This assumption implies the existence of a monotone span program over R for $T_{t,n}$ with size $2n$, as we now show. Define

$$\Delta_0 = \Delta(1, \ldots, n) \in \mathbb{Z}, \quad \text{and} \quad \Delta_1 = \Delta(\alpha_1, \ldots, \alpha_n) \in R.$$

[8] See [21, 22] for lower bounds on the randomness required in black-box secret sharing schemes.

Let $N_0 \in R^{n,t+1}$ (resp. $N_1 \in R^{n,t+1}$) be the matrix in which the i-th row is equal to $(\Delta_0, i, i^2, \ldots, i^t)$ (resp. $(\Delta_1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^t)$), $i = 1 \ldots n$. In both cases, the ith row is labelled by i. When studied as possible monotone span programs over R for $T_{t,n}$, N_0 (resp. N_1) satisfies Definition 6 for the sets $A \notin T_{t,n}$. On the other hand, in both cases, the rows owned by a set $A \in T_{t,n}$ do not necessarily span the target vector $(1, 0, \ldots, 0) \in R^{t+1}$. However, these rows do span [9] the vector $(\Delta_0^2, 0, \ldots, 0) \in R^{t+1}$ (resp. $(\Delta_1^2, 0, \ldots, 0) \in R^{t+1}$). Both properties stated can be verified immediately, for instance using the well-known expression for a Vandermonde determinant in combination with Cramér's rule (see e.g. [23]); passing to the fraction field K of R (note that R has no zero-divisors), this rule implies that a $c \times c$ linear system of equations $N\mathbf{x} = \mathbf{y}$ over the ring R, has a solution at least in case where $\mathbf{y} \in \det(N) \cdot R^c$. Another way is by using Lagrange Interpolation over K, and clearing denominators.

Define a new monotone span program matrix $M \in R^{2n,2t+1}$ consisting of all pairs of rows

$$(\Delta_0, i, i^2, \ldots, i^t, 0, \ldots, 0), \quad \text{and} \quad (\Delta_1, 0, \ldots, 0, \alpha_i, \alpha_i^2, \ldots, \alpha_i^t),$$

for $i = 1 \ldots n$. The shown padding consists of t zeroes in both cases, and each of the rows in a pair is labelled by i. Define $\boldsymbol{\varepsilon} = (1, 0, \ldots, 0)^T \in R^{2t+1}$. The sets $A \notin T_{t,n}$ clearly satisfy Definition 6, and this time the rows owned by sets $A \in T_{t,n}$ span the target vector: they span in particular all vectors of the form $(r \cdot \Delta_0^2 + s \cdot \Delta_1^2, 0, \ldots, 0)$, with $r, s \in R$. By setting $r = r_0$ and $s = r_1$, these include the target vector $\boldsymbol{\varepsilon}$.

To conclude, we exhibit a ring R with degree $O(\log n)$ over the integers and $\alpha_1, \ldots, \alpha_n, r_0, r_1 \in R$ with $r_0 \cdot \Delta_0^2 + r_1 \cdot \Delta_1^2 = 1$, where $\Delta_0 = \Delta(1, \ldots, n)$ and $\Delta_1 = \Delta(\alpha_1, \ldots, \alpha_n)$.

These conditions are reformulated as follows. Let Π_n denote the set of integer primes p with $2 \leq p \leq n$ and define

$$Q_n = \prod_{p \in \Pi_n} p \in \mathbb{Z}.$$

Then we are looking for a ring R with degree $O(\log n)$ over the integers and $\alpha_1, \ldots, \alpha_n \in R$ such that

$$\overline{\Delta_1} \in (R/(Q_n))^*,$$

i.e., the residue-class of Δ_1 in the ring $R/(Q_n)$ is a unit.

Indeed, if $\overline{\Delta_1} \in (R/(Q_n))^*$, then $\overline{\Delta_1} \in (R/(Q_n^k))^*$ as well, for any positive integer k. To verify this by induction, suppose that $\Delta_1 \cdot v = 1 + w \cdot Q_n^i$ for some $v, w \in R$ and $i \geq 1$: then $\Delta_1 \cdot (v - vw \cdot Q_n^i) = 1 - w^2 \cdot Q_n^{2i}$ and $2i \geq i + 1$. As a consequence, $\overline{\Delta_1} \in (R/(\Delta_0^2))^*$. Namely, as an integer, Δ_0^2 factors completely over the primes $p \in \Pi_n$. Then choose k_* large enough such that Δ_0^2 divides $Q_n^{k_*}$, and apply the previous observation. It follows that $\overline{\Delta_1}^2 \in (R/(\Delta_0^2))^*$ as well, or equivalently, there exist $r_0, r_1 \in R$ such that $r_0 \cdot \Delta_0^2 + r_1 \cdot \Delta_1^2 = 1$.

[9] A similar property was first noticed and exploited in [17, 18] and later in [25].

Set $m = \lfloor \log n \rfloor + 1$. Let $\hat{f}(X) \in \mathbb{Z}[X]$ be any monic, irreducible polynomial of degree m such that for all $p \in \Pi_n$, $\hat{f}_p(X)$ (the polynomial $\hat{f}(X)$ with its coefficients reduced modulo p) is irreducible in $\mathbb{F}_p[X]$.

One way of constructing such a polynomial is as follows. For all $p \in \Pi_n$, select a monic, irreducible polynomial $\hat{f}_p(X) \in \mathbb{F}_p[X]$ of degree m. By the theory of finite fields, this is always possible. Applying the Chinese Remainder Theorem to each of the coefficients separately, select an arbitrary lift to a monic polynomial $\hat{f}(X) \in \mathbb{Z}[X]$ of degree m such that $\hat{f}(X) \equiv \hat{f}_p(X) \bmod p$. Note that the monic polynomial $\hat{f}(X)$ is irreducible in $\mathbb{Z}[X]$: if not, reduction modulo p with $p \in \Pi_n$, gives a non-trivial factorization of $\hat{f}_p(X)$ in $\mathbb{F}_p[X]$.

Set $R = \mathbb{Z}[X]/(\hat{f}(X))$. By definition of $\hat{f}(X)$, it follows that $R/(p)$ is a finite field, for all $p \in \Pi_n$. Indeed, for all $p \in \Pi_n$,

$$R/(p) \simeq \mathbb{Z}[X]/(p, \hat{f}(X)) \simeq \mathbb{F}_p[X]/(\hat{f}_p(X)) \simeq \mathbb{F}_{p^m}.$$

Note that all ideals (p) of R with $p \in \Pi_n$ are distinct and maximal. It follows, using the Chinese Remainder Theorem for general rings, that

$$R/(Q_n) \simeq \prod_{p \in \Pi_n} \mathbb{F}_{p^m}.$$

For all $p \in \Pi_n$ we have $|\mathbb{F}^*_{p^m}| = p^m - 1 \geq 2^m - 1 \geq n$. Therefore, for each $p \in \Pi_n$, distinct non-zero

$$\beta_1^{(p)}, \ldots, \beta_n^{(p)} \in \mathbb{F}_{p^m}$$

can be selected. Finally, select arbitrary $\alpha_1, \ldots, \alpha_n \in R$ such that, for $i = 1 \ldots n$,

$$R/(Q_n) \ni \overline{\alpha}_i \longleftrightarrow (\beta_i^{(p)})_{p \in \Pi_n} \in \prod_{p \in \Pi_n} \mathbb{F}_{p^m},$$

where the correspondence is via the (implicit) isomorphism. By construction, for all i, j with $1 \leq i, j \leq n$ and $i \neq j$, it holds that $\overline{\alpha}_i \in (R/(Q_n))^*$ and $\overline{\alpha}_i - \overline{\alpha}_j \in (R/(Q_n))^*$. Hence, $\overline{\Delta}_1 \in (R/(Q_n))^*$, as desired. □

Corollary 1. *For all integers t, n with $0 < t < n-1$, there exists an ISP of size $n \cdot (\lfloor \log n \rfloor + 2)$ for $T_{t,n}$.*

Proof. Let $R, \alpha_1, \ldots, \alpha_n, r_0, r_1, N_0, N_1$ be as constructed in the proof of Theorem 2. Apply the construction from the proof of Lemma 3 to N_1, and take into account the final remark of that proof. This gives an ISP matrix $\hat{N}_1$ with $n \cdot (\lfloor \log n \rfloor + 1)$ rows and $1 + t(\lfloor \log n \rfloor + 1)$ columns. Clearly, the sets $A \notin T_{t,n}$ satisfy Definition 6. For the sets $A \in T_{t,n}$, the rows owned by A span $\delta_1 \cdot \hat{\varepsilon}$, where $\delta_1 \in \mathbb{Z}$ is the first coordinate of $r_1 \cdot \Delta_1^2$.

The ISP matrix N_0 has the properties stated in the proof of Theorem 2 also over $\mathbb{Z}$. Hence, the sets $A \notin T_{t,n}$ satisfy Definition 6 over $\mathbb{Z}$. For the sets $A \in T_{t,n}$, the rows owned by them clearly span $(\delta_0, 0, \ldots, 0) \in \mathbb{Z}^{t+1}$, where $\delta_0 \in \mathbb{Z}$ is the first coordinate of $r_0 \cdot \Delta_0^2$. Since $\delta_0 + \delta_1 = 1$, this leads directly to an ISP for $T_{t,n}$, where the ISP matrix has $n \cdot (\lfloor \log n \rfloor + 2)$ rows and $t(\lfloor \log n \rfloor + 2) + 1$ columns. □

5 Concluding Remarks

5.1 A Note on Simulateability

The ISPs $\hat{\mathcal{M}} = (\mathbb{Z}, \hat{M}, \hat{\psi}, \hat{\boldsymbol{\varepsilon}})$ constructed in the proofs of Theorem 2 and Corollary 1 satisfy the following additional properties, which are helpful when proving the security of certain threshold cryptosystems.

Let the share vector $\mathbf{s} = \hat{M}\mathbf{g}$ be computed according to the corresponding black-box secret sharing scheme, then the following holds.

1. The entries of $\mathbf{s}_A$ are *independent* random group elements for any subset A of $\{1, \ldots, n\}$ with $|A| \leq t$.
2. Every player i can compute a *reconstruction share* $\mathbf{s}'_i$ by taking $\mathbb{Z}$-linear combinations (of course independent of the group) of the entries of his original share $\mathbf{s}_i$, such that any t reconstruction shares $\mathbf{s}'_i$ still allow to reconstruct the secret s, and such that any t original shares $\mathbf{s}_i$ together with s allow to compute the complete reconstruction share vector $\mathbf{s}'$ (by taking $\mathbb{Z}$-linear combinations).

The former property is inherited from the two Vandermonde matrices upon which the construction of $\hat{\mathcal{M}}$ is based on, and the latter holds for $\mathbf{s}'$ defined as $\mathbf{s}' = \hat{M}'\mathbf{g}$, where the ISP $\hat{\mathcal{M}}' = (\mathbb{Z}, \hat{M}', \hat{\psi}, \hat{\boldsymbol{\varepsilon}})$ is constructed from the matrices $\Delta_0 N_0$ and $\Delta_1 N_1$ in a way similar to which $\hat{\mathcal{M}}$ is constructed from N_0 and N_1 in the proof of Theorem 2.

Assuming that the group operation is efficiently computatble and that (almost) random group elements can be sampled efficiently, these properties allow the players of a set A with $|A| \leq t$ to *efficiently* simulate their joint view $\mathbf{s}_A$ of the distribution phase, by sampling (almost) random elements from the group and to *efficiently* simulate their view of the corresponding reconstruction phase by computing $\mathbf{s}'$ from $\mathbf{s}_A$ and the secret s.

When proving the security of a direct application of our black-box secret sharing scheme to distributed RSA for instance, these properties enable an efficient simulator for the adversary's view of the distributed decryption or signing process (see also [12, 25]).

5.2 Implementation

We stress that in this paper we are primarily interested in the asymptotically optimal result from Theorem 2. Several choices in its proof have been made to simplify the mathematical exposition, while suppressing computational aspects.

There are a number of possible practical implementations of black-box secret sharing based on our result. We do not optimize its performance here, but merely indicate below that straightforward implementations run in time polynomial in n.

Note that the scheme consumes $O(n \log n)$ random coins (group elements) and that the expansion factor is $O(\log n)$ in any case, i.e., each player receives

$O(\log n)$ groups elements as his share in a secret group element. For an implementation, it is important to limit the necessary *computational resources* for dealer and players.

One implementation is based on the well-known fact that for any finite Abelian group G, G^m can be viewed as a module over the ring R (see also [12]). The multiplication of an element of R by an element of G^m can be performed having only black-box access to the group operation of G. This way, the monotone span program over R acts directly on vectors of elements of G^m. This leads in a straightforward fashion to an attractive implementation of black-box secret sharing where the actual ISP it is based upon can be left implicit. See for instance [12] for the computational details of this general procedure, taking into account the remarks below.

By the constructive method from the proof of Theorem 2, we may assume without loss of generality that the coefficients of the polynomial $f(X)$ have bit length smaller than $\log Q_n \leq \log(n!) = O(n \log n)$ bits. Recall that its degree m is $\lfloor \log n \rfloor + 1$. For given threshold parameters t, n, it can be fixed once and for all. One simple possible choice for the α_i's is to identify them with distinct, non-zero integer polynomials of degree at most $\lfloor \log n \rfloor$, such that each of the coefficients is either 0 or 1. For instance, α_i can point to i by basing it on the bit representation of i. Δ_0^2 is simply represented by an integer with bit length $O(n^2 \cdot \log n)$. The value Δ_1^2 is the product of $O(n^2)$ elements of R, each of which has integer coordinates -1, 0 or 1. The values r_0 and r_1 can be obtained by computing the inverse $\overline{u}$ of $\overline{\Delta}_1^2 \in R/(\Delta_0^2)$, for instance by solving a linear system of equations over $\mathbb{Z}_{\Delta_0^2}$, and by computing $u \cdot \Delta_1^2 \in R$. The reconstruction vectors are computed from r_0, r_1 and obvious "interpolation coefficients" obtained from the α_i's.

6 Acknowledgments

We thank Ivan Damgaard for many helpful suggestions and discussions. Also thanks to Yvo Desmedt, Yair Frankel, Anna Gál, Yuval Ishai, Brian King and the anonymous referees of CRYPTO '02 for comments.

References

1. A. Beimel. Secure schemes for secret sharing and key distribution. Ph.D.-thesis, Technion, Haifa, June 1996.
2. J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In: Proc. CRYPTO '88, Springer LNCS, vol. 765, pp. 274–285, 1988.
3. 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.
4. 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.

5. G. R. Blakley. Safeguarding cryptographic keys. In: Proc. National Computer Conference '79, AFIPS Proceedings, vol. 48, pp. 313-317, 1979.
6. E. F. Brickell. Some ideal secret sharing schemes. In: J. Combin. Maths. & Combin. Comp. vol. 9, pp. 105–113, 1989.
7. T. Cover and J. Thomas. Elements of information theory. Wiley Series in Telecommunications, 1991.
8. R. Cramer, I. Damgaard, and U. Maurer. Efficient general secure multi-party computation from any linear secret-sharing scheme. In: Proc. EUROCRYPT '00, Springer LNCS, vol. 1807, pp. 316–334, 2000.
9. R. Cramer, S. Fehr, Y. Ishai, and E. Kushilevitz. Efficient multi-party computation over rings. Manuscript, February 2002.
10. Y. Di Crescenzo, and Y. Frankel. Existence of Multiplicative Secret Sharing Schemes with Polynomial Share Expansion. In: Proc. SODA '99, ACM Press, pp. 895–896, 1999.
11. Y. Desmedt and Y. Frankel. Theshold cryptosystem. In: Proc. CRYPTO '89, Springer LNCS, vol. 435, pp. 307–315, 1990.
12. Y. Desmedt and Y. Frankel. Homomorphic zero-knowledge threshold schemes over any finite Abelian group. In: SIAM Journal on Discrete Mathematics, 7(4), pp. 667–679, 1994.
13. Y. Desmedt, A. De Santis, Y. Frankel, and M. Yung. How to share a function securely. In: Proc. STOC '94, ACM Press, pp. 22–33, 1994.
14. Y. Desmedt, G. Di Crescenzo, and M. Burmester. Multiplicative non-abelian sharing schemes and their application to threshold cryptography. In: Proc. ASIACRYPT '94, Springer LNCS, vol. 917, pp. 21–31, 1995.
15. Y. Desmedt, B. King, W. Kishimoto, and K. Kurosawa. A comment on the efficiency of secret sharing scheme over any finite Abelian group. In: Proc. ACISP '98, Springer LNCS, vol. 1438, pp. 391–402, 1998.
16. M. van Dijk. Secret key sharing and secret key generation. Ph. D. Thesis, Eindhoven University of Technology, 1997.
17. Y. Frankel, P. Gemmell, P. MacKenzie, and M. Yung. Optimal resilience proactive public-key cryptosystems. In: Proc. FOCS '97, IEEE Press, pp. 384–393, 1997.
18. Y. Frankel, P. Gemmell, P. MacKenzie, and M. Yung. Proactive RSA. In: Proc. CRYPTO '97, Springer LNCS, vol. 1294, pp. 440–454, 1997.
19. A. Gál. Combinatorial methods in boolean function complexity. Ph.D.-thesis, University of Chicago, 1995.
20. M. Karchmer and A. Wigderson. On span programs. In: Proc. Structures in Complexity Theory '93, IEEE Computer Society Press, pp. 102–111, 1993.
21. B. King. Some results in linear secret sharing. Ph.D.-thesis, University of Wisconsin-Milwaukee, 2001.
22. B. King. Randomness required for linear threshold sharing schemes defined over any finite abelian group. In: Proc. ACISP '01, Springer LNCS, vol. 2119, pp. 376–391, 2001.
23. S. Lang. Algebra. Addison-Wesley Publishing Co., 2nd edition, 1984.
24. A. Shamir. How to share a secret. In: Communications of the ACM, (22) pp. 612–613, 1979.
25. V. Shoup. Practical threshold signatures. In: Proc. EUROCRYPT '00, Springer LNCS, vol. 1807, pp. 207–220, 2000.