Black-Box Secret Sharing from Primitive Sets in Algebraic Number Fields

Ronald Cramer[1,2], Serge Fehr[1], and Martijn Stam[3,⋆]

[1] CWI, Amsterdam, The Netherlands
{cramer,fehr}@cwi.nl
[2] Mathematical Institute, Leiden University, The Netherlands
[3] Department of Computer Science, University of Bristol, United Kingdom
stam@cs.bris.ac.uk

Abstract. A *black-box* secret sharing scheme (BBSSS) for a given access structure works in exactly the same way over any finite Abelian group, as it only requires black-box access to group operations and to random group elements. In particular, there is no dependence on e.g. the structure of the group or its order. The expansion factor of a BBSSS is the length of a vector of shares (the number of group elements in it) divided by the number of players n.

At CRYPTS 2002 Cramer and Fehr proposed a threshold BBSSS with an asymptotically minimal expansion factor $\Theta(\log n)$.

In this paper we propose a BBSSS that is based on a new paradigm, namely, *primitive sets in algebraic number fields*. This leads to a new BBSSS with an expansion factor that is absolutely minimal up to an additive term of at most 2, which is an improvement by a constant additive factor.

We provide good evidence that our scheme is considerably more efficient in terms of the computational resources it requires. Indeed, the number of group operations to be performed is $\tilde{O}(n^2)$ instead of $\tilde{O}(n^3)$ for sharing and $\tilde{O}(n^{1.6})$ instead of $\tilde{O}(n^{2.6})$ for reconstruction.

Finally, we show that our scheme, as well as that of Cramer and Fehr, has asymptotically optimal randomness efficiency.

1 Introduction

The concept of *secret sharing* was introduced independently by Shamir [12] and by Blakley [1] as a means to protect a secret simultaneously from exposure and from being lost. It allows to share the secret among a set of n participants, in such a way that any coalitions of at least $t+1$ participants can reconstruct the secret (completeness) while any t or fewer participants have no information about it (privacy). The work of Shamir and Blakley spawned a tremendous amount of research [15].

⋆ This author is partially supported by the EPSRC and by the Commission of European Communities through the IST program under contract IST-2002-507932 ECRYPT.

Of particular interest to us is *black-box* secret sharing, introduced by Desmedt and Frankel [4]. A black-box secret sharing scheme is distinguished in that it works over any finite Abelian group and requires only black-box access to the group operations and to random group elements. The distribution matrix and the reconstruction vectors are defined independently of the group from which the secret is sampled, and completeness and privacy are guaranteed to hold regardless of which group is chosen. Simple cases are $t = 0$ where each participant is given a copy of the secret, and $t = n - 1$ where a straightforward additive sharing suffices. We will henceforth assume that $0 < t < n - 1$ to exclude these trivial cases.

The original motivation for looking at black-box secret sharing was their applicability to threshold RSA. Although threshold RSA can nowadays be much more conveniently dealt with using Shoup's threshold RSA technique [13] (or in the proactive case using the techniques of Frankel et al. [7]), black-box secret sharing still remains a useful primitive with several applications such as black-box ring multiparty computation [3] or threshold RSA with small public exponent (in which case Shoup's technique fails), and it may very well be relevant to new distributed cryptographic schemes, for instance based on class groups. Furthermore, this problem has turned into an interesting cryptographic problem in its own right.

The average number of group elements handed out to a participant in order to share a single group element is known as the *expansion factor*. The expansion factor expresses the bandwidth taken up by the scheme and is therefore an important property of the scheme. Desmedt and Frankel [4] proposed a scheme with expansion factor linear in the number n of participants. Their scheme is based on finding an invertible Vandermonde determinant over a cyclotomic number field. In subsequent works some improvements to the expansion factor were made, but all within a constant factor [5, 10].

At Crypto 2002, Cramer and Fehr [2] used a new approach based on finding pairs of co-prime Vandermonde determinants over low degree integral extensions of $\mathbb{Z}$. This results in black-box secret sharing schemes with logarithmic expansion factor. They also show that this is asymptotically optimal by proving a tight lower bound. In fact, they prove that the expansion factor of their scheme is minimal up to an additive term of at most three.[1]

We improve these results on black-box secret sharing in several ways. We describe a novel technique for constructing black-box secret sharing schemes, by in a way combining the advantages of both approaches. Briefly, our approach requires to find *one* primitive Vandermonde determinant over a *low degree* integral extension of $\mathbb{Z}$. A Vandermonde determinant is primitive in an integral extension if its only rational integer divisors are $-1, +1$. This allows us to further reduce the gap between the expansion factor and the lower bound by one. By using a

[1] Note that Fehr [6, Corollary 4.1] incorrectly claims an additive term of at most two.

slight tweak which applies very generally to Shamir-like schemes, the expansion factor drops one more in case the number of participants is a power of two.[2]

We also give evidence that the new approach not only leads to a scheme with (slightly) improved bandwidth, but also with significantly improved computational complexity. Indeed, it appears, and we can confirm this for all practical values of n, that sharing a group element with our scheme requires $\tilde{O}(n^2)$ and reconstructing the secret from the shares $\tilde{O}(n^{1.6})$ group operations, in contrast to $\tilde{O}(n^3)$ respectively $\tilde{O}(n^{2.6})$ or more for previous schemes. At present there is no such proof for general n.

Finally, we address the *randomness complexity* of black-box secret sharing, i.e., the number of random group elements that need to be sampled to share a group element. We prove the lower bound $\Omega(t \cdot \lg n)$, which meets the randomness complexity of our (as well as the scheme from [2]) black-box secret sharing scheme and hence shows that these schemes are also optimal with respect to their randomness complexity. We would like to point out that recently a similar lower bound has been proven in [9]. However, the proof given seems a bit vague as it makes use of a better lower bound result on the expansion factor of black-box secret sharing schemes than what can be proven.

The paper is organized as follows. In the following Section 2, we give some definitions and known results regarding black-box secret sharing, and in Section 3 we describe a framework on which previous as well as our new black-box secret sharing scheme are based. In Section 4, we then briefly describe the schemes from [4] and [2], before we discuss our new approach in Section 5. Section 6 is dedicated to the lower bound on the randomness complexity before we conclude in Section 7.

2 Definitions and Known Results

Throughout this section let n and $t < n$ be non-negative integers. Informally, in a black-box secret sharing scheme the shares are computed from the secret and from random group elements by solely using the group operations addition and subtraction (considering the group to be additive), i.e., by taking $\mathbb{Z}$-linear combinations of the secret and random group elements. Similarly, the secret is reconstructed by taking an appropriate $\mathbb{Z}$-linear combination of the shares. Additionally, the coefficients for these linear combinations are designed independently of and correctness and privacy hold regardless of the group to which the scheme is applied. This leads to the following formal definition due to [2].

We first introduce the notion of a labeled matrix. A *labeled matrix* consists of a matrix $M \in R^{d \times e}$ over some given ring R, together with a surjective function $\psi : \{1, \ldots, d\} \to \{1, \ldots, n\}$. We say that the j-th row of M is *labeled* by $\psi(j)$. For $\emptyset \neq A \subseteq \{1, \ldots, n\}$, $M_A \in R^{d_A \times e}$ denotes the restriction of M to those rows that

[2] This tweak is interesting in its own right: it allows one to do a Shamir-like secret sharing over a field F of size $|F| \geq n$, rather than $|F| > n$. Yet—although we are not aware of it being mentioned elsewhere in the literature—we dare not claim its novelty.

are labeled by an $i \in A$. Similarly, for an arbitrary d-vector $\mathbf{x} = (x_1, \ldots, x_d)$ (over a possibly different domain), $\mathbf{x}_A$ denotes the restriction of $\mathbf{x}$ to those coordinates x_j with $\psi(j) \in A$. In order to simplify notation, we write M_i and $\mathbf{x}_i$ instead of M_A and $\mathbf{x}_A$ in case $A = \{i\}$, and we typically do not make ψ explicit.

Definition 1 (Black-Box Secret Sharing). *A labeled matrix $M \in \mathbb{Z}^{d \times e}$ over the integers is a* black-box secret sharing scheme *for n and t if the following holds. For an arbitrary finite Abelian group G and an arbitrarily distributed $s \in \mathsf{G}$ let $\mathbf{g} = (g_1, \ldots, g_e)^T \in \mathsf{G}^e$ be drawn uniformly at random subject to $g_1 = s$ only. Define the share vector as $\mathbf{s} = M\mathbf{g}$ (where $\mathbf{s}_i$ is given to the i-th participant). Then, for any nonempty subset $A \subseteq \{1, \ldots, n\}$:*

i. (Completeness) If $|A| > t$ then there exists $\boldsymbol{\lambda}(A) \in \mathbb{Z}^{d_A}$, only depending on M and A, such that $\mathbf{s}_A^T \cdot \boldsymbol{\lambda}(A) = s$ with probability 1.
ii. (Privacy) If $|A| \leq t$ then $\mathbf{s}_A$ contains no Shannon information on s.

Note that a black-box secret sharing scheme is linear by definition (essentially because a black-box group allows only linear operations).

Definition 2 (Expansion Factor and Randomness Complexity). *The* expansion factor η *of a black-box secret sharing scheme $M \in \mathbb{Z}^{d \times e}$ for n and t is defined by $\eta = d/n$, and the* randomness complexity ρ *by $\rho = e - 1$.*

The expansion factor of a black-box secret sharing scheme measures the average number of group elements each participant receives (and need not be integral). For the trivial cases $t = 0$ and $t = n - 1$ the expansion factor 1 can be achieved. The randomness complexity determines the number of random group elements that need to be sampled to share a secret. The number of group operations during dealing and reconstructing depends both on d and e and on the size of the elements in the matrix M (optimizing the number of group operations given M is essentially an addition chain problem).

Theorem 1 ([2]). *Let $M \in \mathbb{Z}^{d \times e}$ be a labeled matrix. Define $\boldsymbol{\varepsilon} = (1, 0, \ldots, 0) \in \mathbb{Z}^e$. Then M is a black-box secret sharing scheme for n and t if and only if for every nonempty $A \subseteq \{1, \ldots, n\}$ the following holds.*

i. (Completeness) If $|A| > t$ then $\boldsymbol{\varepsilon} \in \mathrm{im}(M_A^T)$.
ii. (Privacy) If $|A| \leq t$ then there exists $\boldsymbol{\kappa} = (\kappa_1, \ldots, \kappa_e)^T \in \ker(M_A)$ with $\kappa_1 = 1$.

Note the difference between this definition and that of monotone span programs (which is equivalent with linear secret sharing over finite fields). Whereas in the latter case the completeness condition and the privacy condition are characterized by "to span or not to span", over $\mathbb{Z}$ and in the context of blackbox secret sharing this is slightly more subtle. See [2].

In [2] the above theorem is used to prove a lower bound on the expansion factor by looking at an instantiation of any given black-box secret sharing scheme over the group $\mathbb{F}_2$ and borrowing arguments from Karchmer and Wigderson [8]. The upper bound in the theorem below follows from the explicit construction of a black-box secret sharing scheme in [2].

Theorem 2 **([2]).** *The minimal expansion factor η of a black-box secret sharing scheme for n and t with $0 < t < n-1$ satisfies*

$$\lfloor \lg n \rfloor - 1 < \lg \frac{n+3}{2} \leq \eta \leq \lceil \lg(n+1) \rceil + 1 = \lfloor \lg n \rfloor + 2 \ .$$

If $t = 1$ then it even holds that $\eta \geq \lg n$.

3 Integral Extensions and *Weak* Black-Box Secret Sharing

Let R be a ring of the form $R = \mathbb{Z}[X]/(f)$ where f is a monic irreducible polynomial in $\mathbb{Z}[X]$ of degree m. We call such a ring an *integral extension* (of degree m).[3] Note that R is a free $\mathbb{Z}$-module[4] with basis $\bar{1}, \bar{X}, \ldots, \bar{X}^{m-1}$ (the residue classes of $1, X, \ldots, X^{m-1}$ modulo $f(X)$). Furthermore, let G be a finite Abelian (additive) group. Such a group is naturally a $\mathbb{Z}$-module. The fact is that the m-fold direct sum $\mathsf{G}^m = \mathsf{G} \oplus \cdots \oplus \mathsf{G}$ can be regarded as an R-module. Indeed, as a group, respectively as $\mathbb{Z}$-module, G^m is isomorphic to the tensor product $R \otimes_{\mathbb{Z}} \mathsf{G}$ (with isomorphism $(g_1, g_2, \ldots, g_m) \mapsto \bar{1} \otimes g_1 + \bar{X} \otimes g_2 + \cdots + \bar{X}^{m-1} \otimes g_m$); the latter though, sometimes referred to as the *extension of* G *over* R [11], is an R-module by "multiplication into the R-component".

Now, since G^m is an R-module, polynomials with coefficients in G^m can be evaluated over R. This allows us to perform a version of Shamir secret sharing [12]: Given the parameters n and t as well as the secret $s \in \mathsf{G}$, the dealer picks uniformly at random a *sharing polynomial*

$$g(x) = r_0 + \cdots + r_{t-1}x^{t-1} + \hat{s}x^t \in \mathsf{G}^m[x]$$

of degree t with coefficients in G^m such that its *leading* coefficient equals $\hat{s} = (s, 0, \ldots, 0) \in \mathsf{G}^m$ (we need to embed the secret s into G^m). Given n pairwise different evaluation points $\alpha_i \in R$, known to everyone, the dealer hands out share $s_i = g(\alpha_i) \in \mathsf{G}^m$ to participant i for $i = 1, \ldots, n$.

We would like to point out that by fixing the basis $\bar{1}, \bar{X}, \ldots, \bar{X}^{m-1}$ for R over $\mathbb{Z}$ and using standard techniques this candidate black-box secret sharing scheme can be described by a labeled integer matrix M and thus fits into the framework of our formal Definition 1; although, as discussed below, correctness holds only in a weak sense. The expansion factor is obviously $\eta = m$: each share is an element in G^m, and the randomness complexity is $\rho = t \cdot m$: the randomness is enclosed by the t non-leading coefficients of $g \in \mathsf{G}^m[x]$.

Jointly, any $t+1$ participants know $t+1$ points on a polynomial of degree t. Normally, when working over a field, this would allow them to reconstruct the entire polynomial using Lagrange interpolation. In our setting, where divisions cannot necessarily be done (in R), we will have to settle with a multiple $\Delta \cdot \hat{s} \in \mathsf{G}^m$

[3] Using standard terminology from algebraic number theory, R is an example of an *order*.

[4] Loosely speaking, a *module* is a vector space over a ring rather than over a field, and it is called *free* if it allows for a basis (which is not granted for general modules).

of the secret, where $\Delta \in R$ is some common multiple of the denominators of the Lagrange coefficients. A possible generic choice for Δ is the Vandermonde determinant

$$\Delta(\alpha_1, \ldots, \alpha_n) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j) .$$

Reconstruction by a set A of $t+1$ participants can be expressed in the following formula:

$$\Delta \cdot \hat{s} = \sum_{i \in A} \left(\Delta \cdot \prod_{\substack{j \in A \\ j \neq i}} \frac{1}{\alpha_i - \alpha_j} \right) s_i \ .$$

Putting the secret into the leading coefficient as we do (rather than into the constant coefficient) of the sharing polynomial immediately leads to privacy. Essentially, for any $A \subset \{1, \ldots, n\}$ with $|A| \leq t$, privacy follows from the existence of the polynomial $\kappa = \prod_{i \in A}(x - \alpha_i) \in R[x]$ of degree at most t with leading coefficient 1 and with $\kappa(\alpha_i) = 0$ for all $i \in A$. Indeed, for any secrets $s, s' \in \mathsf{G}$ and any sharing polynomial $g \in \mathsf{G}^m[x]$ for s, the participants in A cannot distinguish between a sharing of s with sharing polynomial g and a sharing of s' with sharing polynomial $g' = g + (s' - s)\kappa$.

Introducing the notion of a δ-*weak* black-box secret sharing scheme for $\delta \in R$, to be understood in that the correctness condition of a black-box secret sharing scheme (Definition 1) only holds in that $\delta \cdot \hat{s}$ (rather than s) can be reconstructed while the privacy condition holds fully, we can summarize the observations of this section as follows.

Theorem 3. *Let R be an integral extension of degree m, and let $\alpha_1, \ldots, \alpha_n \in R$ be pairwise different. Then there exists a $\Delta(\alpha_1, \ldots, \alpha_n)$-weak black-box secret sharing scheme for n and t with expansion factor $\eta = m$ and randomness complexity $\rho = t \cdot m$.*

Note that an additional advantage of putting the secret into the leading coefficient of the sharing polynomial (rather than into the constant coefficient) is that 0 may be used as evaluation point. This extra evaluation point is relevant for the expansion factor if the number of participants is a power of 2. This "swapping" trick, putting the secret in the leading coefficient instead of in the constant term, is not exploited in [4] nor in [2], but it applies to their schemes as well.

4 Previous Schemes

Based on the common framework just described, we can summarize previous research. It all boils down to reconstructing s given $\Delta \cdot \hat{s}$ and the restriction the scheme poses on Δ for the reconstruction to be possible.

4.1 Using an Invertible Δ

Desmedt and Frankel [4] provide a solution for black-box secret sharing with expansion factor $O(n)$. They achieve this by selecting the polynomial f in such a way that Δ can be chosen to be a unit in $R = \mathbb{Z}[X]/(f)$. A necessary and sufficient condition for this is that there exist n evaluation points in the ring whose differences are all units in the ring.[5] In this case, all divisions required for Lagrange interpolation can in fact take place in the ring R, so Δ can be forgotten altogether.

The maximal cardinality of a subset of R such that all differences are units is called the Lenstra constant of the ring R. If we set $R = \mathbb{Z}[X]/(f(X))$, where $f(X) \in \mathbb{Z}[X]$ is the p-th cyclotomic polynomial, we have a ring of degree $p-1$ and with Lenstra constant p. So if we take p as the smallest prime greater than n, we have black-box secret sharing scheme with expansion factor $O(n)$ for n players. Finding integral extensions for which the Lenstra constant is exponential (or super-linear) in the degree of the ring is part of an open problem in number theory, as far as we know

4.2 Using Two Relatively Co-Prime Δ's

Cramer and Fehr [2] propose scheme which has expansion factor $\lfloor \lg n \rfloor + 2$. In a nutshell, it shares the secret *twice* using weak secret sharing schemes with two different sets, say $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$, of evaluation points. This allows to reconstruct two different multiples of the secret: $\Delta(\boldsymbol{\alpha}) \cdot \hat{s}$ and $\Delta(\boldsymbol{\beta}) \cdot \hat{s}$. By ensuring that $\Delta(\boldsymbol{\alpha})$ and $\Delta(\boldsymbol{\beta})$ are co-prime, standard Euclidean techniques can be used to recover $\hat{s}$ and the real secret s: let a and b be such that $a \cdot \Delta(\boldsymbol{\alpha}) + b \cdot \Delta(\boldsymbol{\beta}) = 1$, then $a \cdot \Delta(\boldsymbol{\alpha})\hat{s} + b \cdot \Delta(\boldsymbol{\beta})\hat{s} = \hat{s} = (s, 0, \ldots, 0)$.

A small expansion factor can then be obtained by picking the α_i's in the integers and the β_i's in a suitable integral extension $R = \mathbb{Z}[X]/(f)$. A necessary and sufficient condition for the existence of $\boldsymbol{\beta}$ such that $\Delta(\boldsymbol{\alpha})$ and $\Delta(\boldsymbol{\beta})$ are co-prime is that for all primes p the *lowest* irreducible polynomial dividing f modulo p has degree $\underline{d}_p$ such that $n \leq p^{\underline{d}_p}$. This can be satisfied by certain polynomials f of degree $m = \lceil \lg(n+1) \rceil = \lfloor \lg n \rfloor + 1$, and thus results in a total expansion factor $\lfloor \lg n \rfloor + 2$.

In [2] polynomials f of degree $\lfloor \lg n \rfloor + 1$ are considered that are irreducible modulo all the primes $p \leq n$. It is then possible to set $\alpha_i = i$ and β_i to the (residue class modulo f of the) unique polynomial of degree less than m with coefficients in $\{0, 1\}$ that evaluates to i in the point 2, in other words, whose coefficient vector is the binary representation of i. (Note that the "swapping" trick allows us to use a polynomial of degree $m = \lceil \lg n \rceil$ instead of $\lfloor \lg n \rfloor + 1$, although there is only a difference if n is a power of two.)

[5] If the secret is embedded in the constant term, the evaluation points need to be units themselves as well and evaluation in zero is prohibited.

5 The New Black-Box Secret Sharing Scheme

5.1 The New Scheme: Using a Primitive Δ

As an example, consider the case $t = 1$, where only two participants are needed to reconstruct the secret (for any number of participants n). If we use $R = \mathbb{Z}[X]/(f)$ with *any* (monic and irreducible) f of degree at least $\lceil \lg n \rceil$, and the same $\{0,1\}$-polynomial evaluation points β_i as described in Section 4.2, then any pair $(i,j), i \neq j$ can reconstruct $(\beta_i - \beta_j)\hat{s}$. For concreteness, suppose $\deg f = 4$ and that $\beta_i - \beta_j$ equals $\bar{1} - \bar{X} + \bar{X}^3$. In this case we know that $(\beta_i - \beta_j)\hat{s} = (s, -s, 0, s)$. Indeed, as discussed in Section 3, $(\beta_i - \beta_j)\hat{s}$ is computed by associating $\hat{s} = (s, 0, \ldots, 0)$ with $\bar{1} \otimes s$, computing $(\beta_i - \beta_j) \cdot (\bar{1} \otimes s) = (\beta_i - \beta_j) \otimes s = \bar{1} \otimes s + \bar{X} \otimes (-s) + \bar{X}^3 \otimes s$, and reading out the "coefficients". So, $(\beta_i - \beta_j)\hat{s}$ already contains s as a coordinate! There is no need for a second sharing or $\beta_i - \beta_j$ being a unit in R. Our choice of $\beta_i - \beta_j$ is inconsequential in this argument. If the β_i's are defined as they are as non-zero polynomials of degree smaller than m with coefficients in $\{0,1\}$ (regardless of f), then $(\beta_i - \beta_j)\hat{s}$ contains at least one copy of the secret or its negative.

In general, using the weak black-box secret sharing scheme the participants can reconstruct $\Delta \cdot \hat{s}$. Since $\hat{s} = (s, 0, \ldots, 0)$, this module scalar-multiplication equals $\Delta \cdot \hat{s} = (\Delta_0 \cdot s, \ldots, \Delta_{m-1} \cdot s)$ with integer Δ_i's such that $\Delta = \sum_{i=0}^{m-1} \Delta_i \cdot \bar{X}^i$. The secret s can be reconstructed from the Δ_i's if and only if the Δ_i's are co-prime, by using the extended Euclidean algorithm. In essence, the ideas of [4] (using a single weak black-box secret sharing scheme) and of [2] (recovering s from co-prime multiples) are combined. Contrary to the scheme from [2], we do not need a second sharing. This is where our improvement and lower expansion factor stem from.

A prime $p \in \mathbb{Z}$ is a divisor of all Δ_i's if and only if $\Delta \equiv 0 \bmod pR$. A sufficient and necessary condition on the set of interpolation points is that it is a primitive set in the integral extension R, as defined below.

Definition 3 (Primitive Elements and Sets). *Let R be an integral extension. Then $\delta \in R$ is* primitive *if its only rational integer divisors are* 1 *and* -1*, i.e., if $\delta \not\equiv 0 \bmod pR$ for all primes $p \in \mathbb{Z}$. A set $\{\alpha_1, \ldots, \alpha_n\}$ in R is called* primitive *if its Vandermonde determinant $\Delta(\alpha_1, \ldots, \alpha_n)$ is primitive.*

For an arbitrary $\mathbb{Z}$-basis of R, $p \in \mathbb{Z}$ dividing $\delta \in R$ is equivalent to p dividing all the rational integer coordinates of δ with respect to that basis. Therefore, $\delta \in R$ is primitive if and only if its coordinates have no non-trivial common factor in $\mathbb{Z}$. Note also that the required property is stronger than requiring the α_i's to be pairwise different modulo every prime p, since not every prime $p \in \mathbb{Z}$ is necessarily also prime in R.

For $f(X) \in \mathbb{Z}[X]$ and for a prime $p \in \mathbb{Z}$, define $f_p(X) \in \mathbb{F}_p[X]$ as f taken mod$p$, and write $f_p = f_{p,1}^{\epsilon_{p,1}} \cdots f_{p,\ell_p}^{\epsilon_{p,\ell_p}}$ for its factorization into powers of distinct irreducible polynomials in $\mathbb{F}_p[X]$. The degree of such $f_{p,i}$ is denoted $d_{p,i}$. Also define $\bar{d}_p = \max_{1 \le i \le \ell_p} d_{p,i}$.

Theorem 4. *Let $R = \mathbb{Z}[X]/(f)$ be an integral extension of degree $m > 1$. If $n \leq p^{\bar{d}_p}$ for every prime $p \in \mathbb{Z}$, then there exists a primitive set in R with cardinality n.*

This implies the existence of an integral extension of degree $\lceil \lg(n) \rceil$ with a primitive set of size n, by taking f such that f_p is irreducible for all primes p with $2 \leq p \leq n$. Such f can for instance be constructed using the Chinese Remainder Theorem, see also [2].

Corollary 1. *For any $t, n \in \mathbb{Z}$ with $0 < t < n-1$ there exists a black-box secret sharing scheme M with expansion factor $\eta = \lceil \lg(n) \rceil$ and randomness complexity $\rho = t \cdot \lceil \lg(n) \rceil$.*

The *computational* efficiency of the scheme is discussed in Section 5.4.

5.2 Proof of Theorem 4

Let $p \in \mathbb{Z}$ be a prime. Then we have

$$R/pR \simeq \mathbb{F}_p[X]/(f_{p,1}^{\epsilon_{p,1}} \cdots f_{p,\ell_p}^{\epsilon_{p,\ell_p}}) \simeq \mathbb{F}_p[X]/(f_{p,1}^{\epsilon_{p,1}}) \times \cdots \times \mathbb{F}_p[X]/(f_{p,\ell_p}^{\epsilon_{p,\ell_p}})$$

and thus we have the canonical projection

$$R/pR \to \mathbb{F}_p[X]/(f_{p,1}) \times \cdots \times \mathbb{F}_p[X]/(f_{p,\ell_p}) \simeq \mathbb{F}_{p^{d_{p,1}}} \times \cdots \times \mathbb{F}_{p^{d_{p,\ell_p}}}$$

where (for any prime power q) $\mathbb{F}_q$ denotes the field with q elements. Hence, if $n \leq p^{\bar{d}_p}$, then there clearly exist $\alpha_1, \ldots, \alpha_n \in R$ such that $\Delta(\alpha_1, \ldots, \alpha_n) \not\equiv 0 \bmod pR$: choose n distinct elements from $\mathbb{F}_{p^{\bar{d}_p}}$ and lift them arbitrarily to elements in R. Furthermore, different solutions modulo a *finite* set of different primes p can be combined to a solution modulo all primes from that set by the Chinese Remainder Theorem. However, we are after a solution that holds modulo *all* primes simultaneously.

Instead, we construct a primitive set of size n by induction: as long as the upperbound on n as stated in the theorem is satisfied, then, given a primitive set $\{\alpha_1, \ldots, \alpha_{n-1}\} \subset R$, we can construct $\alpha_n \in R$ such that $\{\alpha_1, \ldots, \alpha_{n-1}, \alpha_n\} \subset R$ is a primitive set as well. For technical reasons to become clear later on, the actual induction hypothesis corresponds to a slightly stronger claim, but we suppress this at this point in the exposition.

Assume we are given a primitive set $\{\alpha_1, \ldots, \alpha_{n-1}\} \subset R$. Consider the polynomial

$$\Delta(\alpha_1, \ldots, \alpha_{n-1}, X) = \Delta(\alpha_1, \ldots, \alpha_{n-1}) \cdot \prod_{i<n} (\alpha_i - X) \in R[X] \,.$$

Let $e_1 \ldots, e_m$ be some fixed $\mathbb{Z}$-basis of R, where m is the degree of $f(X)$. Clearly, there exist polynomials $F_1, \ldots, F_m \in \mathbb{Z}[X_1, \ldots, X_m]$ such that

$$\mathbf{d} = (F_1(x_1, \ldots, x_m), \ldots, F_m(x_1, \ldots, x_m)) \in \mathbb{Z}^m$$

represents the coordinate-vector (w.r.t. the chosen basis) of $\Delta(\alpha_1, \ldots, \alpha_{n-1}, x) \in R$ for an arbitrary $x = x_1 e_1 + \cdots + x_m e_m \in R$ $(x_1, \ldots, x_m \in \mathbb{Z})$.

Now suppose that the intersection between the ideal $\hat{I} = (F_1, \ldots, F_m) \cdot \mathbb{Z}[X_1, \ldots, X_m]$ and $\mathbb{Z}[X_1]$ contains a non-zero polynomial $g(X_1)$. In other words, there exist polynomials $\mu_1, \ldots, \mu_m \in \mathbb{Z}[X_1, \ldots, X_m]$ such that

$$g(X_1) = \sum_{i=1}^{m} \mu_i(X_1, \ldots, X_m) \cdot F_i(X_1, \ldots, X_m).$$

Therefore, if we choose $x_1 \in \mathbb{Z}$ such that $g(x_1) \neq 0$, then, *no matter how* $x_2, \ldots, x_m \in \mathbb{Z}$ *are chosen*, it will be the case that a given prime $p \in \mathbb{Z}$ does not divide all $F_i(x_1, \ldots, x_m) \in \mathbb{Z}$, or equivalently, $\Delta(\alpha_1, \ldots, \alpha_{n-1}, x) \not\equiv 0 \bmod pR$, unless perhaps when p divides $g(x_1)$.

Based on these observations the proof of the theorem essentially consists of two main steps. First, we show the existence of $g(X_1)$. Second, with a proper choice of $x_1 \in \mathbb{Z}$ such that $g(x_1) \neq 0$, we select for each prime $p \in \mathbb{Z}$ that divides $g(x_1)$ an element $a_{n,p} \in R$ such that its first coordinate is equal to $x_1 \bmod p$ and such that $\Delta(\alpha_1, \ldots, \alpha_{n-1}, a_{n,p}) \not\equiv 0 \bmod pR$.

The proof is then easily completed by constructing the desired $\alpha_n \in R$ such that its first coordinate is x_1 and such that $\alpha_n \equiv \alpha_{n,p} \bmod pR$ for each of those finitely many primes p. This is by simple coordinate-wise application of the CRT. More precisely, let $\alpha_n = x_1 e_1 + x_2 e_2 + \cdots + x_m e_m$, where x_1 is as above, and for each $i \geq 2$, $x_i \in \mathbb{Z}$ is such that x_i is equivalent to the i-coordinate of $a_{n,p}$ modulo each those primes p.

We now start with the existence of $g(X_1)$. The argument utilizes the following well-known theorem from algebraic geometry (see e.g. [11]), which we state for convenience below.

Theorem 5 (Hilbert's Nullstellensatz). *Let K be an algebraically closed field, let $I \subset K[X_1, \ldots, X_r]$ be an ideal, and let $\mathcal{Z}(I) \subset K^r$ denote the algebraic variety $\{(z_1, \ldots, z_r) \in K^r \mid g(z_1, \ldots, z_r) = 0 \ \forall g \in I\}$. If $h \in K[X_1, \ldots, X_r]$ satisfies $h(z_1, \ldots, z_r) = 0$ for every $(z_1, \ldots, z_r) \in \mathcal{Z}(I)$, i.e., it vanishes on the variety, then there exists a positive integer k such that $h^k \in I$.*

Let $\bar{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$, i.e., the field of all algebraic numbers, and let I denote the ideal $(F_1, \ldots, F_m) \cdot \bar{\mathbb{Q}}[X_1, \ldots, X_m]$. We claim that the algebraic variety $\mathcal{Z}(I)$ is finite. This is argued in two steps. Consider the tensor-product $\bar{\mathbb{Q}} \otimes_{\mathbb{Z}} R$, which has a natural ring structure. First, $\mathcal{Z}(I)$ is in one-to-one correspondence with the solutions to the univariate polynomial equation $\Delta(\alpha_1, \ldots, \alpha_{n-1}, x) = 0$ with $x \in \bar{\mathbb{Q}} \otimes_{\mathbb{Z}} R$, which we show below. Second, as a ring, $\bar{\mathbb{Q}} \otimes_{\mathbb{Z}} R$ is isomorphic to a finite product of fields.[6] Therefore, the univariate polynomial equation has at most a finite number of solutions, and the claim follows. One-to-one correspondence is argued as follows. The elements of $\bar{\mathbb{Q}} \otimes_{\mathbb{Z}} R$ uniquely

[6] Indeed, $\bar{\mathbb{Q}} \otimes_{\mathbb{Z}} R \simeq \bar{\mathbb{Q}}[X]/(f) \simeq \prod_{i=1}^{m} \bar{\mathbb{Q}}$. The first isomorphism is by a standard fact that can be found e.g. in [11], and the second follows since f factors into distinct linear polynomials.

correspond to the expressions of the form $\sum_{i=1}^{m} q_i \otimes e_i$ with the $q_i \in \bar{\mathbb{Q}}$. Using simple rewriting properties of tensor-product, it follows that $\Delta(\alpha_1, \ldots, \alpha_{n-1}, x) = 0$ for $x \in \bar{\mathbb{Q}} \otimes_{\mathbb{Z}} R$ if and only if $\sum_{i=1}^{m} F_i(q_1, \ldots, q_m) \otimes e_i = 0$. This happens if and only if all $F_i(q_1, \ldots, q_m)$ are 0, or equivalently, $(q_1, \ldots, q_m) \in \mathcal{Z}(I)$. Note that some of the properties of tensor product we have used above rely on the fact that R has a $\mathbb{Z}$-basis.

Finiteness of $\mathcal{Z}(I)$ implies the existence of a non-zero polynomial $\tilde{g}(X_1)$ in the intersection of I and $\bar{\mathbb{Q}}[X_1]$. Indeed, the polynomial $\prod_{z \in \mathcal{Z}(I)}(X_1 - z_1) \in \bar{\mathbb{Q}}[X_1]$ (where z_1 denotes the first coordinate of z) clearly vanishes on $\mathcal{Z}(I)$, and by the Nullstellensatz some power of this polynomial is in I. In turn this implies the existence of a non-zero polynomial $g(X_1)$ in the intersection of $\hat{I}$ and $\mathbb{Z}[X_1]$, as desired. This is an immediate consequence of basic field theory.[7]

With the existence of $g(X_1)$ settled, we proceed with the remainder of the proof. As a matter of terminology, for $\beta, \gamma \in R$, we will say that $\beta = \gamma$ *within* $\mathbb{F}_p^{d_{p,i}}$ if the canonical projections of β and γ coincide in that component. Similar for $\mathbb{F}_p[X]/(f_{p,i}^{\epsilon_{p,i}})$.

First we make the actual induction hypothesis precise. We assume there exists a primitive set $\alpha_1, \ldots, \alpha_{n-1} \in R$ such that *additionally* for every prime $p \in \mathbb{Z}$ with $1 < p < n$ it holds that $\Delta(\alpha_1, \ldots, \alpha_{n-1})$ is non-zero within the *largest* field $\mathbb{F}_{p^{\bar{d}_p}}$. The induction hypothesis is clearly satisfied in case of a single element set. If $n \leq p^{\bar{d}_p}$ for every prime $p \in \mathbb{Z}$, then we construct $\alpha_n \in R$ such that $\{\alpha_1, \ldots, \alpha_{n-1}, \alpha_n\}$ is a primitive set *and* such that the additional requirement is satisfied.

Instead of selecting $x_1 \in \mathbb{Z}$ arbitrarily such that $g(x_1) \neq 0$, we have to give a special treatment to the primes $p \in \mathbb{Z}$ with $1 < p < n$ first, for reasons to become clear later on. We start by choosing for every such prime p an $a_{n,p} \in R$ such that $\Delta(\alpha_1, \ldots, \alpha_{n-1}, a_{n,p})$ is non-zero within (the largest field) $\mathbb{F}_{p^{\bar{d}_p}}$. This can be done by virtue of the induction hypothesis and using arguments as in the beginning of the section. Then we choose $x_1 \in \mathbb{Z}$ such that modulo every prime $p \in \mathbb{Z}$ with $1 < p < n$, x_1 is congruent to the first coordinate of $a_{n,p}$, and such that $g(x_1)$ is non-zero. Such x_1 exists as g has only a finite number of zeroes.

Now fix any prime $p \in \mathbb{Z}$ with $p \geq n$ and p divides $g(x_1)$. We now select $a_{n,p}$ as required. We have $\Delta(\alpha_1, \ldots, \alpha_{n-1}) \neq 0$ within at least one of the $\mathbb{F}_p[X]/(f_{p,i}^{\epsilon_{p,i}})$ into which R/pR splits, by the induction hypothesis. Fix an index k for which this is the case.

We first treat the case when $f_p(X) \in \mathbb{F}_p[X]$ is irreducible (so $\ell_p = k = 1$). In this case $R/pR \simeq \mathbb{F}_p[X]/(f_p) \simeq \mathbb{F}_{p^m}$. Since $p \geq n$, there are $p^{m-1} \geq n$ elements

[7] It is given that $\tilde{g} = \sum_{i=1}^{m} \lambda_i F_i$ for some $\lambda_i \in \bar{\mathbb{Q}}[X_1, \ldots, X_m]$. There exists $\theta \in \bar{\mathbb{Q}}$ such that each of the coefficients of each of the λ_i's is in $\mathbb{Q}(\theta)$. Note that $\mathbb{Q}(\theta)$ is a $\mathbb{Q}$-vectorspace with basis $1, \theta, \ldots, \theta^{e-1}$ for some e. Consider the fraction field $L = \mathbb{Q}(X_1, \ldots, X_m)$. Similarly, $L(\theta)$ is an L-vectorspace with the same basis. Now consider an arbitrary non-zero coordinate of $\tilde{g}$ w.r.t. that basis. Then we have $g = \sum_{i=1}^{m} \mu_i F_i$ where $g \in \mathbb{Q}[X_1]$, respectively, $\mu_i \in \mathbb{Q}[X_1, \ldots, X_m]$, is this coordinate of $\tilde{g}$, respectively, of λ_i. Clearing denominators gives the desired result.

in $\mathbb{F}_{p^m}$ with first coordinate x_1, and it is clearly possible to select $a_{n,p} \in R$ as required, i.e., its first coordinate is x_1 and $\Delta(\alpha_1, \ldots, \alpha_{n-1}, a_{n,p}) \not\equiv 0 \bmod pR$.

Second, suppose that the polynomial $f_p(X) \in \mathbb{F}_p[X]$ is reducible. Since $p \geq n$, $\mathbb{F}_{p^{d_{p,k}}}$ ($\simeq \mathbb{F}_p[X]/(f_{p,k})$) has at least n elements. So it is possible to select $a_{n,p} \in R$ such that within $\mathbb{F}_{p^{d_{p,k}}}$ it differs from $\alpha_1, \ldots, \alpha_{n-1}$. As a consequence all $a_{n,p} - \alpha_j$ are invertible within $\mathbb{F}_p[X]/(f_{p,k})$, and hence also within $\mathbb{F}_p[X]/(f_{p,k}^{\epsilon_{p,k}})$. Thus, $\Delta(\alpha_1, \ldots, \alpha_{n-1}, a_{n,p})$ is *non-zero* within $\mathbb{F}_p[X]/(f_{p,k}^{\epsilon_{p,k}})$, and therefore also non-zero modulo pR.

It remains to argue that $a_{n,p}$ may be chosen such that its first coordinate equals x_1. This is by adding a suitable rational integer multiple of a special element $\delta_p \in R$ which has first coordinate 1 but that is 0 within $\mathbb{F}_{p^{d_{p,k}}}$. We construct it below, and this finishes the proof.

For convenience, take $\bar{1}, \bar{X}, \ldots, \bar{X}^{m-1} \in \mathbb{Z}[X]/(f)$ as the $\mathbb{Z}$-basis $e_1, \ldots, e_m$ for R introduced earlier on. Let $c \in \mathbb{F}_p \setminus \{0\}$ be the constant coefficient of the irreducible polynomial $f_{p,k} \in \mathbb{F}_p[X]$ and $c^{-1} \in \mathbb{F}_p$ its inverse. Let $h(X) = h_0 + h_1 X + \cdots + h_{d_{p,k}} X^{d_{p,k}} \in \mathbb{Z}[X]$ have coefficients in $\{0, \ldots, p-1\}$ such that modulo p it equals $c^{-1} f_{p,k}(X)$. Since f_p is reducible, h has degree smaller than m. Moreover it has constant coefficient $h_0 = 1$. Then define δ_p as $\overline{h(X)} \in R$. Indeed, its first coordinate is 1 and δ_p is clearly 0 within $\mathbb{F}_{p^{d_{p,k}}}$. $\square$

5.3 A Generalization of Theorem 4

It is possible to give a generalization of Theorem 4 that applies to arbitrary orders (of non-zero discriminant), rather than only to integral extensions and which shows that the lower bound on n is tight if we require that not only Δ but all powers of Δ must have no non-trivial integral divisors. Consider for instance $f = X^2 + 1$ so that $R \simeq \mathbb{Z}[i]$ (the Gaussian integers). Then Theorem 4 promises a primitive set of size 2, while if fact there is a primitive set of size 3. Indeed, $\Delta(0, 1, i) = 1 + i$ has no non-trivial divisors; $\Delta(0, 1, i)^2 = (1 + i)^2 = 2i$ however has.

Definition 4 (*Radically* Primitive Elements and Sets). *A element δ in an order R is called* radically *primitive if the only rational integer divisors of* any power of δ *are 1 and -1, i.e., if $\delta^k \not\equiv 0$ modulo any prime $p \in \mathbb{Z}$, for all $k > 0$. And a set $\{\alpha_1, \ldots, \alpha_n\}$ in R is called* radically primitive *if its Vandermonde determinant $\Delta(\alpha_1, \ldots, \alpha_n)$ is radically primitive.*

Using similar but more general arguments as in the proof of Theorem 4, the following can be proved.

Theorem 6. *Let R be an order with discriminant $\Delta_{R/\mathbb{Z}} \neq 0$. For any prime $p \in \mathbb{Z}$ let $n(p) = \max_{\mathfrak{p}} |R/\mathfrak{p}|$, where $\mathfrak{p}$ ranges over all prime ideals $\mathfrak{p} \subseteq pR$ over p. Then the maximal cardinality for a radically primitive set in R is* $\min_{p\ prime} n(p)$.

5.4 Computational Complexity

Apart from having a small expansion factor, we would also like to exhibit that the number of black-box group operations is polynomial in the number of participants. This requires that the entries of the sharing matrix M are small (if we assume that d and e are sufficiently small as is the case for the constructions above). For an integral extension $R = \mathbb{Z}[X]/(f)$ this requires small coefficients of f and small coefficients of the evaluation points α_i when expressed as polynomials of minimal degree.

As mentioned in Section 4.2, for the scheme from [2] one method always works, namely picking an irreducible polynomial modulo p for every prime $p < n$ and using the Chinese Remainder Theorem to get a polynomial f over the integers. The coefficients of this polynomial are all smaller than $\prod_{p<n} p$, which corresponds to a bitlength linear in n. We cannot hope to find polynomials with coefficients that are much smaller than random CRT based polynomials and that are still irreducible modulo p for all $p < n$. The evaluation points that are used have minimal coefficients (either 0 or 1).

For our new construction, the set of suitable polynomials f is a proper superset of those employed by [2]. This means that we could take f as constructed above with coefficients whose sizes are linear in n. Unfortunately, the proof of existence of a primitive set $\alpha_1, \ldots, \alpha_n$ for a suitable f does not guarantee any reasonable bound on the size of the coefficients: the main problem in the proof occurs around the place where Hilbert's Nullstellensatz is invoked.

However, practical experiments indicate that f and the α_i's can in fact be chosen in such a way that their coefficients are within $\{-1, 0, 1\}$, which makes our scheme computationally more efficient by a factor n then the scheme from [2] (and any other scheme). Indeed, Fig. 1 shows polynomials f of degree m up to 12, and thus suitable for n up to 2^{12}, that allow the following primitive sets: choose $\alpha_1, \ldots, \alpha_n$ as (residue classes modulo f of) polynomials with coefficients in $\{0, 1\}$ and degree less than m such that α_i evaluates to $i-1$ at point 2 (similar as described in Section 4.2 for the β_i's in the scheme from [2]).

m	sample f	m	sample f
2	$X^2 - X - 1$	8	$X^8 + X^4 - X^3 + X - 1$
3	$X^3 - X - 1$	9	$X^9 + X^4 - 1$
4	$X^4 - X - 1$	10	$X^{10} - X^3 + X^2 + X - 1$
5	$X^5 - X^3 - X^2 + X + 1$	11	$X^{11} - X^5 + X^3 + X^2 - 1$
6	$X^6 - X - 1$	12	$X^{12} + X^6 - X^5 - X^4 - X^3 - X + 1$
7	$X^7 - X^3 + X^2 + X - 1$		

Fig. 1. Polynomials f that allow binary α_i's

We have been searching for suitable polynomials f with *minimal* residual degree $\deg(f - X^m)$, and that the polynomials found have rather small residual degree. This suggests that there is no shortage of suitable polynomials at all. As an aside, if we assume the existence of a suitable $\{-1,0,1\}$-polynomial for every n, then it can always be found in polynomial time.[8]

The best implementation of the scheme from [2] is given by Stam [14] using multi-exponentiation techniques. The achieved sharing complexity is $\tilde{O}(n^3)$ and the reconstruction complexity $\tilde{O}(n^{1+\lg 3})$ group operations. It appears to be hard to further improve the complexity of the scheme from [2], as the scheme seems to be bound to an f with n-bit coefficients, and thus the module scalar-multiplication of a "small" number in $R = \mathbb{Z}[X]/(f)$ (meaning represented by a $\{-1,0,1\}$-polynomial of degree $< m$) with an element in G^m requires $\Theta(mn)$ group operations. That is where our complexity improvement stems from: since we can choose f with constant coefficients, a module scalar-multiplication with a small number requires only $O(m^2)$ group operations, and we achieve a sharing complexity of $\tilde{O}(n^2)$ and a reconstruction complexity of $\tilde{O}(n^{\lg 3})$ group operations.[9] (The $\lg(n)$-factors hidden by the $\tilde{O}$-notation have exponent at most 2).

The conclusion is that for reasonable values of n (namely for n up to 4096) our scheme is considerably more efficient than the scheme from [2] (and any other black-box secret sharing scheme). Furthermore, the evidence indicates that this is true for *any* n.

6 A Tight Lower Bound for the Randomness

In this final section we prove that our new black-box secret sharing scheme is not only optimal with regard to the expansion factor but also with regard to the randomness complexity. Specifically, we prove a lower bound of $t \cdot \lg(n) - O(t)$ for the randomness complexity of *binary linear* secret sharing schemes, which immediately implies the same bound for black-box secret sharing schemes. Recall that the randomness complexity of our scheme is $t \cdot \lceil \lg(n) \rceil$.

Recently, King proved the lower bound $\lg\big(n \cdot (n-1) \cdots (n-t+2)\big)$ [9, Theorem 12], which, using similar techniques as we do, can also be shown to be $t \cdot \lg(n) - O(t)$. However, the proposed proof assumes that the number of rows in any black-box secret sharing scheme $M \in \mathbb{Z}^{d \times e}$ is lower bounded by $d \geq n\lg(n)$, while in fact the best known lower bound is $d \geq n\lg(n+3) - n$ (see Theorem 2). Note that the bound $d \geq n\lg(n)$ used by King is widely conjectured to hold and sharpening the known lower bound to this conjectured lower bound is an interesting open problem.

---

[8] In time $\tilde{O}(n^{3\lg 3})$: there are $O(n^{\lg 3})$ candidate polynomials f. Each candidate can be checked by computing the product of all non-zero $\{-1,0,1\}$-polynomials modulo f. There are $O(n^{\lg 3})$ factors in this product and the size of the coefficients in any step is also bounded by $\tilde{O}(n^{\lg 3})$. Note that for $n = 2^{12}$ this polynomial upper bound is already close to practically infeasible.

[9] The exponent $\lg 3$ results from the fact that Δ (respectively $\Delta(\boldsymbol{\beta})$ in the scheme from [2]) can be replaced by its square-free part, which is the product of distinct polynomials of degree less than $m \approx \lg n$ with coefficients in $\{-1,0,1\}$, of which there exist $3^m \approx n^{\lg 3}$.

Recall that a linear secret sharing scheme over a finite field F is defined along the lines of Definition 1 and 2, except that $\mathbb{Z}$ is replaced by F and G is restricted to $\mathsf{G} = F$. In the following, e denotes the Euler number $\mathrm{e} \approx 2.718$.

Theorem 7. *For arbitrary $t, n \in \mathbb{Z}$ with $0 < t < n-1$, the randomness complexity ρ of any binary linear secret sharing scheme $M \in \mathbb{F}_2^{d\times e}$, and thus in particular of any black-box secret sharing scheme $M \in \mathbb{Z}^{d\times e}$, for n and t satisfies $\rho > t \cdot \lg n - (1 + \lg \mathrm{e})t$.*

Proof. First of all, the bound for black-box secret sharing immediately follows from the bound on binary linear secret sharing, as any black-box secret sharing scheme $M \in \mathbb{Z}^{d\times e}$ reduced modulo 2 results in a binary linear secret sharing scheme.

Consider a binary linear secret sharing scheme $M \in \mathbb{F}_2^{d\times e}$ for t and n as in the claim. Without loss of generality we may assume that the rows of M_i are linearly independent for any i. Also, by the lower bound on the expansion factor from Theorem 2, which also applies to binary linear schemes, we may assume that, say, M_n consists of $d_n \geq \lceil \lg(n+3) \rceil - 1$ rows (respectively $d_n \geq \lceil \lg(n) \rceil$ in case $t = 1$). Furthermore, as $t > 0$, $\varepsilon = (1, 0, \ldots, 0)$ is not in the space spanned by the rows in M_n. Altogether this implies that, essentially by a basis change, M can be brought into a form where M_n consists of the $(d_n \times d_n)$-identity-matrix padded with zeroes to its left, while still being a binary linear secret sharing scheme for n and t. Consider now the labeled matrix $M' \in \mathbb{F}_2^{(d-d_n)\times(e-d_n)}$ by removing M_n as well as the last d_n columns of M (i.e. the columns that overlap with the identity matrix embedded in M_n). The labeling (of the remaining rows) is left unchanged. It is not hard to see that M' is a binary linear secret sharing scheme for $n' = n - 1$ and $t' = t - 1$. This procedure can be applied iteratively t times, resulting in a secret sharing scheme for $n - t$ participants and threshold 0 (which may have randomness complexity 0). The total number of rows removed during this process, and thus the randomness complexity of the original secret sharing scheme M is $\rho \geq \sum_{i=0}^{t-2} \bigl(\lceil \lg(n+3-i) \rceil - 1\bigr) + \lceil (\lg(n-t+1) \rceil$. Using Stirling's bounds

$$\sqrt{2\pi}\, n^{n+1/2}\, \mathrm{e}^{-n+1/(12n)} < n! < \sqrt{2\pi}\, n^{n+1/2}\, \mathrm{e}^{-n+1/(12n+1)}$$

for factorials, we get

$$
\begin{aligned}
\rho &\geq \sum_{i=0}^{t-2} \big(\lceil \lg(n+3-i) \rceil - 1\big) + \lceil (\lg(n-t+1) \rceil \\
&\geq \sum_{i=0}^{t-1} \lg(n-i) - t + 1 \; = \; \lg \prod_{i=0}^{t-1} (n-i) - t + 1 \; = \; \lg \frac{n!}{(n-t)!} - t + 1 \\
&> \lg \frac{n^{n+1/2}\, \mathrm{e}^{-n+1/(12n)}}{(n-t)^{(n-t)+1/2}\, \mathrm{e}^{-(n-t)+1/(12(n-t)+1)}} - t + 1 \\
&> \lg \frac{n^{n+1/2}\, \mathrm{e}^{-n+1/(12n)}}{n^{(n-t)+1/2}\, \mathrm{e}^{-(n-t)+1/(12(n-t)+1)}} - t + 1 \\
&= t \lg n - \Big(t + \frac{1}{12(n-t)+1} - \frac{1}{12n}\Big) \lg \mathrm{e} - t + 1 \\
&> t \lg n - (1 + \lg \mathrm{e}) t
\end{aligned}
$$

□

7 Concluding Remarks

From a practical point of view, the proposed black-box secret sharing scheme is essentially optimal with respect to its expansion factor (and its randomness complexity) and it is reasonably efficient for practical values of n: there seems to be little room for improvement (besides maybe squeezing the constant in the computational complexity). From a theoretical point of view, there are still a few open ends: First of all, we only have evidence but no proof that the proposed black-box secret sharing scheme is computationally efficient for large n. Furthermore, the question about the minimal achievable expansion factor is still not entirely solved, there is still a gap of (at most) 2 between the expansion factor achieved by the proposed scheme and the known lower bound; and we know that for certain parameters our construction is not optimal: it is for instance an easy exercise to construct a black-box secret sharing scheme for $t = 1$ and $n = 3$ with expansion factor 5/3 (in contrast to 2, achieved by the proposed generic construction). Finally, all (reasonably good) black-box secret sharing schemes (for arbitrary t and n) are based on the framework discussed in Section 3. It would be interesting to discover completely new approaches.

Acknowledgements

The authors owe many thanks to H.W. Lenstra, jr. for contributing Theorem 6 and its proof to this work, and for his kind permission to include it in this paper; Theorem 4 (as well as its proof) is an adaptation to a special case of this more general theorem. Part of this work was done while Cramer was employed at Aarhus University and while Stam was a visitor under the Marie-Curie Program there. Part of this work was also done while Cramer was visiting the Centre de Recerca Matemàtica (CRM) in Bellaterra, Spain.

References

1. G. R. Blakley. Safeguarding cryptographic keys. In *Proc. National Computer Conference '79*, volume 48 of *AFIPS Proceedings*, pages 313–317, 1979.
2. R. Cramer and S. Fehr. Optimal black-box secret sharing over arbitrary Abelian groups. In M. Yung, editor, *Advances in Cryptography—Crypto'02*, volume 2442 of *Lecture Notes in Computer Science*, pages 272–287. Springer-Verlag, 2002.
3. R. Cramer, S. Fehr, Y. Ishai, and E. Kushilevitz. Efficient multi-party computation over rings. In E. Biham, editor, *Advances in Cryptography—Eurocrypt'03*, volume 2656 of *Lecture Notes in Computer Science*, pages 596–613. Springer-Verlag, 2003.
4. Y. Desmedt and Y. Frankel. Threshold cryptosystem. In G. Brassard, editor, *Advances in Cryptography—Crypto'89*, volume 435 of *Lecture Notes in Computer Science*, pages 307–315. Springer-Verlag, 1990.
5. Y. Desmedt, B. King, W. Kishimoto, and K. Kurosawa. A comment on the efficiency of secret sharing scheme over any finite abelian group. In C. Boyd and E. Dawson, editors, *ACISP'97*, volume 1438 of *Lecture Notes in Computer Science*, pages 391–402. Springer-Verlag, 1998.
6. S. Fehr. *Secure Multi-Player Protocols: Fundamentals, Generality, and Efficiency.* PhD thesis, University of Århus, 2003.
7. Y. Frankel, P. Gemmell, P. MacKenzie, and M. Yung. *Optimal resilience proactive public-key cryptosystems.* In: *Proceedings of FOCS '97*, IEEE Press, pp. 384–393, 1997.
8. M. Karchmer and A. Wigderson. On span programs. In *Proceedings of the Eigth Annual Structure in Complexity Theory Conference*, pages 102–111. IEEE Computer Society Press, 1993.
9. B. King. A Comment on Group Independent Threshold Sharing. In K. Chae and M. Yung, editors, *WISA'03*, volume 2908 of *Lecture Notes in Computer Science*, pages 425–441. Springer-Verlag, 2004.
10. B. S. King. *Some Results in Linear Secret Sharing.* PhD thesis, University of Wisconsin-Milwaukee, 2000.
11. S. Lang. *Algebra, 3rd ed.* Addison-Wesley Publishing Company, 1997.
12. A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.
13. V. Shoup. Practical threshold signatures. In B. Preneel, editor, *Advances in Cryptography—Eurocrypt'00*, volume 1807 of *Lecture Notes in Computer Science*, pages 207–220. Springer-Verlag, 2000.
14. M. Stam. *Speeding up Subgroup Cryptosystems.* PhD thesis, Technische Universiteit Eindhoven, 2003.
15. D. Stinson and R. Wei. *Bibliography on Secret Sharing Schemes.* http://www.cacr.math.uwaterloo.ca/~dstinson/ssbib.html, 2003.