On Polynomial Secret Sharing Schemes

Radune Artiom[1,2] and Anat Paskin-Cherniavsky[2]

[1] The Open University, Israel
[2] Ariel University, Ariél, Israel

Abstract. Nearly all secret sharing schemes studied so far are linear or multi-linear schemes. Although these schemes allow to implement any monotone access structure, the share complexity may be suboptimal – the gap between the best known lower bounds and best known upper bounds is exponential for some access structures.
There is growing evidence in the literature, that non-linear schemes can improve share complexity for some access structures - with the work of Beimel and Ishai (CCC 01') being among the first to demonstrate it. This motivates further study of non linear schemes.
We initiate a systematic study of polynomial secret sharing schemes (PSSS), where shares are (multi-variate polynomials) of secret and randomness vectors over some finite field. Our main hope is that the nice algebraic structure of polynomials would help obtain better lower bounds than those known for the general setting, extending over the class of multi-linear schemes.
Some of the concrete new results we prove in this work are as follows.
On share complexity of polynomial schemes.
First we studied degree 1 in randomness (where the degree of secret is unlimited). We have shown that a large subclass of these schemes are equivalent to multi-linear schemes, in the sense that for any such scheme, there exists an equivalent multi-linear scheme with very similar share complexity. Also, we have shown that the class of schemes of polynomials of degree exactly 2 in r, without degree 1 in r monomials, is very weak, and can implement only trivial access structures where the minterms consist of single parties.
Another observation we make refers to the share complexity (per bit) of multi linear schemes (polynomial schemes of total degree 1). We observe that the scheme by Liu et. al obtaining share complexity $O(2^{0.994n})$ can be transformed into a multi-linear scheme with similar share complexity per bit, for sufficiently long secrets.
On the randomness complexity of polynomial schemes.
We prove that for every degree 2 polynomial secret sharing scheme, there exists an equivalent degree-2 scheme with identical share complexity with randomness complexity bounded by $O(2^{2^n})$. For general PSSS, randomness complexity can be bounded by $SC^{O(SC)^2}$, where SC is the share complexity of the original scheme. So far, bounds on randomness complexity were known only for multi linear schemes, demonstrating that $RC \leq SC$ is always achievable. Our bounds are not nearly as practical, and may be viewed as a proof of concept. If a much better bound for some $d = O(1)$ is obtained, it would lead directly to counting-based

lower bounds for degree-d PSSS which are better than the best known lower bounds for general schemes.
One nice application of low (say polynomial) randomness complexity is transforming polynomial schemes with polynomial (in n) algebraic formulas $C(s, r)$, into a degree-3 scheme with only polynomial blowup in share complexity, using standard randomizing polynomials constructions.

1 Introduction

Secret sharing is a primitive allowing a dealer to share a secret s among n players. The secret sharing scheme implements a (monotone) access structure $\mathcal{A} \subseteq 2^{[n]}$ if any $A \in \mathcal{A}$ can learn the secret from their joint share vector (A is called qualified set), and any set $B \notin \mathcal{A}$ learns nothing about the secret (B is called unqualified set). Secret sharing was introduced in 79' by Shamir [1] and Blakley [2] for threshold access structures, and was followed by thousands of works exploring the primitive itself, and its many applications found since. As a notable application, secret sharing is used as a key building block in various MPC (secure Multi-Party Computation) constructions [3]. As to secret sharing itself, quite early on [4] put forward a first construction realizing any monotone access structure.

Arguably, the most important complexity measures of a secret sharing scheme are its share complexity (share complexity). Share complexity is the maximum, over the parties' share length, received from the dealer by any of the parties. A somewhat relaxed measure is its information ratio, which is the share complexity *per shared bit*. It can be viewed as 'amortized' share complexity, which is a useful measure if secrets are allowed to be long.

Unfortunately, there is a huge gap in our understanding of this measure. Namely, the best known lower bound on share complexity for a general scheme is $\Omega(n/\log(n))$ [5], while the best known constructions for certain access structures have exponential complexity $O(2^{0.892n})$ [6]. In [5], techniques from information theory are used, characterizing the existence of a secret sharing scheme in terms of requirements on the entropy of various distributions. The lower bound in [5] is on information ratio (making it stronger) and states an explicit access structure for which it holds. It is important to note that counting arguments do not work for general secret sharing schemes.[3]

In spite of extensive research attempting to extend [5]'s result, using information theoretic techniques, the best known lower bound for general schemes has not improved since (even for implicit access structures).

See [7] and references therein, for example, for a more thorough discussion of the many positive and negative results on share complexity of secret sharing schemes, as well as their numerous applications.

[3] In a nutshell, even if randomness domain is polynomially bounded in the share complexity, we still get a double-exponential number of secret sharing schemes of share complexity $O(n/\log(n))$, which is about the number of monotone access structures.

On the other hand, much more is known about the share complexity of a well studied family of secret sharing family of linear, and more generally multi linear secret schemes. In a nutshell, a linear scheme is a scheme where each share is a linear combination of elements from a finite field $\mathbb{F}$, each of which is either the secret or a random variable, while a multi-linear scheme is a scheme where the secret can be vector of elements from $\mathbb{F}$ and the shares are a linear combination of these elements and the random variables. Linear schemes are relatively easy to design, often exploiting the insights and intuition we have into linear algebra. Perhaps a more important reason for their popularity is their "homomorphic" property. In MPC, for example, linear schemes are a useful building block, as they allow computing a sharing of the sum of shared secrets by locally adding the corresponding shares. Even more importantly, for (multi) linear schemes better lower bounds on share complexity are also known. In particular, counting arguments yield exponential lower bounds for non-explicit schemes, and recently, an exponential lower bound has been obtained on the share complexityof linear schemes for an explicit access structure. See next section for more details. For now, the observation important for discussion is that as well as upper bounds, lower bounds for (multi) linear secret sharing schemes heavily exploit the (linear-)algebraic structure of the sharing scheme.

Motivated by the hope to narrow the gap between upper and lower bounds for share complexityand information ratio in secret sharing schemes, in this work, we continue the work of [8], which initiates a study of the power of non-linear secret sharing schemes. The main motivation in [8] for studying non-(multi) linear schemes is that most constructions of secret sharing schemes so far were either linear or multi linear, so new insights both on upper and lower bounds may be gained. Indeed [8] put forward several innovative secret sharing schemes for access structures for which linear schemes of comparable complexity are not known, or even do not exist under reasonable assumptions. In [8] the authors explore both arbitrary non-linear schemes, and a specific generalization of linear schemes, they refer to as *quasi-linear* schemes.

We have the additional motivation of obtaining new lower bounds for a broader class of schemes than linear and multi linear ones, making a step back from general schemes, lower bounds for which proved notoriously hard so far. More specifically, we chose to explore the arguably natural extension of multi linear schemes, we call *polynomial schemes*, or PSSS. A PSSS is defined as multi linear scheme over a finite field $\mathbb{F}$, where each share is some polynomial over $\mathbb{F}$ in the secret and randomness elements, rather than necessarily a degree-1 polynomial (corresponding to a multi linear scheme). We hope that the rich algebraic structure of polynomials - especially of polynomials of low degree, say 2, would help develop techniques for lower bounds of more *algebraic* nature, as they proved useful for linear and multi linear schemes. A slightly more general notion of polynomial schemes is one where $S \subseteq \mathbb{F}^k$, rather than the entire set $\mathbb{F}^k$. We refer to such schemes as *generalized* polynomial schemes. Such a notion could as well suffice. The reason we do not make it our default notion is to obtain a 'smooth' extension of multi linear schemes, which do require this property.

Quite surprisingly, it turns out that this property of our schemes (that the secret domain equals the entire $\mathbb{F}^k$) turns out to be useful in one of the lower bounds we prove on the power of a certain subclass of PSSS.

Besides the potential for useful analytic techniques, we believe PSSS is a useful set of schemes to study as it is very broad. In particular, as any function $f : \mathbb{F}^n \to \mathbb{F}$ can be represented by an n-variate polynomial over $\mathbb{F}$, it takes a moment to think why not every secret sharing scheme can be represented by a PSSS with the same share complexity. The reason for that is that a secret sharing scheme is a randomized mapping $Sh : S \times R \to S_1 \times ... \times S_n$, rather a deterministic function. Sh where the randomness is uniformly sampled from a finite set R. Note that for a finite $\mathbb{F}_p$, the probability of Sh outputting a sharing $\mathbf{s}^* = (s_1^*, ..., s_n^*)$ on input 0 has a finite representation in base p. So, for instance, if $Pr[Sh(s) = (s_1, ..., s_n)]$, we can not implement it by polynomials over any finite field in the straightforward way of partitioning R into sets $R_{s,(s_1,...,s_n)}$ such that $Sh(s, r) = (s_1, ..., s_n)$ iff. $r \in R_{s,(s_1,...,s_n)}$, as there is no suitable subset $R_{0,\mathbf{s}^*}$, for 1/6 is not of the form $\frac{a}{p^l}$ $(a, l \in \mathbb{N})$ for any prime p. It is true that if one settles for statistical secret sharing, allowing for small correctness and/or privacy errors, the above approach indeed works. In this work we focus on the standard notion of perfect secret sharing schemes, though.

This leaves the following fundamental question on the power of PSSS - are general schemes more powerful than PSSS. More precisely

Question 1 (Informal). Do there exist access structures, that have non-polynomial schemes much more efficient than any PSSS?

See a discussion on this question in Section 1.2.3, with certain evidence in the positive direction.

Other interesting questions are understanding the effect of various parameters of PSSS on their power, in terms of achievable share complexityand information ratio. There are various interesting parameters. One useful parameter is k - the length of the vector space $\mathbb{F}^k$ constituting the secret domain S. The distinction between $k = 1$ and arbitrary k is the difference between linear and multi-linear schemes, when considering PSSS of total degree $d = 1$. Generally, as we discuss below, the distinction between small secrets - $k = 1$ (or small k) appears meaningful in terms of achievable information ratio - see discussion in Section 1.2. An Additional question to study is the effect of the particular field $\mathbb{F}_p$ on the power of the induced PSSS class.

A concrete natural question is obtaining lower bounds for low degree PSSS, say of degree $d = O(1)$. A simple approach for $k = 1$ would be to bound $|R|$ as a function of share complexity, and then rely on the fact that there are few different degree-d polynomials in $R + 1$ variables (exponentially many in share complexity) for a constant $\mathbb{F}_p$. The number of monotone access structures is double-exponential in n. For linear schemes, it is well known that wlog. $|R| \leq$ share complexity, leading to a $2^{\Omega n}$ lower bound on share complexity of linear schemes over any fixed $\mathbb{F}_p$. However, for any $d > 1$, there are no known explicit bounds on $|R|$ in terms of |share complexity|, so this approach does not currently work. In this work we make a first step in the direction of filling in

the missing component, obtaining certain upper bounds on $|R|$ (as a function of share complexity). This leaves the following interesting question open.

Question 2 (informal). Fix some finite field $\mathbb{F}_q$, and $d = O(1)$. Does there exist a polynomial bound $h(\cdot)$ on $|R|$ as a function of share complexity, such that any PSSS over $\mathbb{F}_q$ of degree d has an equivalent PSSS over $\mathbb{F}_q$ and degree q with the same share complexity, and $|R| \leq h(\text{share complexity})$.[4]

1.1 Our results

For more long-term goals and motivation for the introduced framework see Section B.

Feasibility and share complexity lens. On the negative side, we show that a large subclass of PSSS with r-degree 1 is equivalent to multi-linear schemes in the sense that for each such scheme, a multi-linear scheme for the same access structure with (almost) the same share complexity and over the same field exists. We conjecture that all schemes with r-degree 1 are as weak as multi-linear schemes, and leave it as an interesting open problem. See Theorem 3 and Theorem 4 for a precise statement of the class involved of schemes in question.

In addition we have shown that there are sub classes with r-degree 2 that are very weak. Namely, it is the class of

That is to say, if the scheme is from that sub class it can implement only trivial access structures. Namely every party can reconstruct the secret alone or on the contrary does not have any information about the secret.

On the positive side, we observe that a surprising recent result indicating all monotone access structures have a scheme construction share complexity $O(2^{0.994n})$ [9] can be replaced with a multi-linear construction (instead of a non-polynomial scheme).

We show that there exists (multi) linear secret sharing schemes based on the multi-linear CDS [10] with information ratio O(1) for a certain class (not all) of access structures for a sufficiently large share domain.[5]

Theorem 1. *Let $n > 0$ be an integer. Then all monotone access structures on n parties admit a multi-linear scheme over $S = \mathbb{F}_2^{O(2^n)}$ with information ratio $O(2^{0.994n})$ per party. (in our language, degree-1 polynomial scheme over $\mathbb{F}_2$).*

[4] A sufficiently small super-polynomial bound on $|R|$ would still imply non-trivial bounds on share complexity, say better than the best known bound of $\Omega(n/\log n)$ for general schemes.

[5] The following pair of results are simple observations, which may be described and understood within the limits of the introduction, and we think they hope gain intuition on. The full proof of the first observation relies on particular details of [10]'s construction, and are deferred to Section A. The proof of the second is included below.

We sketch the proof of this simple observation in Appendix A. This observation demonstrates the power of amortization (increasing k) all else kept equal. Additionally, we can obtain a polynomial scheme of (possibly) high degree with the same share complexity.

Theorem 2. *Let $n > 0$ be an integer. Then all monotone access structures on n parties assume a polynomial scheme over $S = \mathbb{F}_{2^{O(2^n)}}$ with information ratio of $O(2^{0.994n})$ per party.*

This is a direct corollary of Theorem 1. This holds due to the simple observation that any polynomial scheme over $\mathbb{F}_q^{k'}$, where q is a prime power (of any degree) can be replaced by a scheme where $S = \mathbb{F}_{q^{k'}}$, (that is, a scheme with $k = 1$) and the sharing polynomials are of possibly higher degree than the original ones. This is done by thinking of the vector of field elements in parties' shares and the vector of random field elements as vectors of elements over $\mathbb{F}_q^{k'}$, and the secret as an element of $\mathbb{F}^{q^{k'}}$. Then, the fact that any finite field $\mathbb{F}$ and function $\mathbb{F}^{1+r'} \to \mathbb{F}$ can be represented as a multi-variate polynomial over $\mathbb{F}$ implies that the original scheme can be implemented as a polynomial scheme with $k = 1$ over $\mathbb{F}_{q^{k'}}$.

The overall share complexity overhead of this transformation is at most n, as the overall share complexity is at least $\log_2(|S|)$ to maintain perfect correctness.

This general observation implies that there is certain redundancy regarding the usefulness of various parameters ($k, |F|$ and total degree) of polynomial schemes towards reducing share complexity. Namely, if we are free to adjust $\mathbb{F}$ and the degree arbitrarily, then without loss of generality k can be fixed to 1 without loss of generality.

Randomness complexity lens. An additional aspect that we have studied is the randomness complexity of PSSS. Here we study what is the best upper bound on the randomness complexity, as a function of the share complexity of a scheme – $\mathbb{rc}(SC)$. That is, for every scheme in the (sub) class of polynomial schemes with share complexity SC, there exists an equivalent scheme in the class with the same share complexity and randomness complexity at most $\mathbb{rc}(SC)$. For linear and multi-linear schemes it is known that their randomness complexity is (without loss of generality) upper bounded by SC (the equivalent scheme is also over the same field). To the best of our knowledge, no such bounds appear in the literature for other broad classes of schemes. In particular, we have not found a bound for general (perfect) secret sharing schemes (we believe it was likely previously known).

In this work we put forward an upper bound for randomness complexity for general PSSS (see Theorem 10), as well as on degree-2 PSSS (see Theorem 8). A bound for general (not necessarily PSSS schemes) in included for completeness in Theorem 12.

Roadmap. In Section 2 we provide the precise (standard) definition of secret sharing that we use, and introduce some new definitions and notations for PSSS.

It also contains required primitives we use in this work. In Section 3, we present our results on feasibility and share complexity. In Section 4 we provide our results on randomness complexity.

1.2 Previous work

In the following, we provide an overview of research on the effect of various parameters of the PSSS framework mentioned above appearing in previous work.

1.2.1 Linear Secret Sharing Schemes The most studied and most commonly used class of secret sharing schemes is the linear secret sharing schemes class. In a linear scheme, the secret is viewed as an element of a finite field (in our terminology $k = 1$), the randomness is comprised of vectors over the finite field, and the shares are obtained by applying a linear mapping to the secret and several independent random field elements.

A particularly useful access structure is the (t, n)-threshold access structure, where qualified sets are those including t or more participants. For this particular access structure, tight bounds on share complexity are known. In particular, Shamir's secret sharing scheme [1] is an *ideal* secret sharing schemes - having information ratio 1 (which is optimal) for sufficiently large secret domain. It also provides the best known upper bound for 1-bit secrets on the share complexity of threshold schemes [11]. This scheme is linear over $\mathbb{F}_{p^k}$ if portrayed over a secret domain $S = \mathbb{F}_{p^k}$ for any $p^k > n$.

Share complexity of general linear secret sharing. Unlike the useful special case of threshold access structures, as we mentioned before, the share complexity of schemes for general access structures is far from resolved. This is the case even for linear schemes, although quite some progress has been made in this realm. In our view, linear schemes correspond to polynomials of degree 1 in the random elements r_i and in secret elements s_i.

In a seminal work, among other things, initiating the systematic study of linear secret sharing schemes, Karchmer and Wigderson introduced in [12] a linear algebraic computational complexity model of computation, the span program (SP) and monotone span program (MSP). They proved that MSP is equivalent to linear secret sharing schemes. That is, an access structure has an MSP of size m over a field $\mathbb{F}$ for a monotone access structure $f : \{0,1\}^n \to \{0,1\}$ iff it has a secret sharing scheme giving m field elements to the parties implementing the access structure defined by f.

Known lower bounds on the size of monotone span programs. As mentioned above, unlike for general schemes, a simple counting approach is useful for proving almost tight lower bounds on the share complexity of linear schemes. More precisely, for any constant-sized field $\mathbb{F}_p$, it is easy to obtain a lower bound of $\tilde{\Omega}(2^{n/2})$ on the share complexity of most access structures for linear schemes over $\mathbb{F}_p$. This result has recently been extended to obtain a bound of $\tilde{\Omega}(2^{n/3})$ on the

share complexityfor all linear schemes (over any field), exploiting the connection between representable matroids and linear secret sharing schemes [13]. In a nutshell, it relies on an upper bound on the number of representable matroids over a given finite set.

The state of affairs for explicit access structures is also much better for linear secret sharing schemes. The techniques used there deviate from [5]'s information-theoretic approach for general schemes, instead heavily exploiting the (linear) algebraic properties of the sharing scheme.

The first lower bounds for monotone span programs, due to Karchmer and Wigderson [12], showed that all threshold functions over $GF(2)$ require monotone span programs of size $\Omega(n\log(n))$. The first super-polynomial lower bounds, on the order of $n^{\Omega(\log n/\log\log n)}$, were obtained by Babai [14] against a function in NP. These bounds were simplified and improved by Gál [15] to $n^{\Omega(\log(n))}$. Beimel and Weinreb [16] later gave $n^{\Omega(\sqrt{\log n})}$ lower bounds for a function in uniform NC^2 (and therefore in P), proving that monotone span programs can be weaker than polynomial time.

The technique of [15] is notable, as it generalizes many of the previous results in a very useful way. This technique is based by observing a connection between lower bounds on MSP size, and a combinatorial-algebraic measure of covers which has been used to prove (superpolynomial) lower bounds on other models such as monotone formula size by Razborov [17].[6]

Very recently, in a break-through result, [18] demonstrated exponential lower bounds on MSP size for the function GEN_n - namely, they obtained a lower bound on share complexity of 2^{n^ϵ} for some constant $\epsilon > 0$. This work relies on clever analysis of Razborov's Rank method, which so far only yielded quasi-polynomial lower bounds on MSP size.

1.2.2 Multi-linear Secret Sharing Schemes Another class of secret sharing schemes that was also heavily studied is multi-linear secret sharing schemes. In such schemes the secret is a vector of some field elements, and the sharing is done by applying some linear mapping on this elements and some other random field elements. This class is an extension of the linear class. Linear secret sharing schemes are multi-linear schemes with only one secret field element. In our terminology, these schemes are polynomial schemes of total degree 1 (and no apriori bound on the number of secret field elements).

Lower bounds on multi-linear schemes. Above, we have seen superpolynomial lower bounds on MSP size over any field for explicit access structures. Next, we review a more recent result, extending the lower bound to the multi-linear setting. In fact, the result holds for certain access structures for which the MSP lower bounds above hold. This is non-trivial, because increasing the number of field elements in the secret could potentially save on information ratio (although clearly not on absolute share complexity). On the flip side, in this section we will survey evidence to the usefulness of increasing k for degree-1 sharing.

[6] In particular, note that formula size is a lower bound on MSP size, as follows from [4]

Beimel, Ben-Efraim, Padró and Tyomkin proved in [19] that ideal multi-linear secret-sharing schemes in which the secret is composed of p field elements are more powerful than schemes in which the secret is composed of less than p field elements (for every prime p). Similarly to linear schemes, In addition, they prove a super-polynomial lower bound on the share size $n^{\Omega(\log n)}$ in multi-linear secret sharing schemes for an explicit access structure.

The authors in [19] proved that multi-linear schemes are equivalent to a complexity theoretic model generalizing MSP, they dubbed Multi-Target Monotone Span Program - MTMSP (again, the equivalence is in terms of share complexity vs. MTMSP size, and over the same field). They generalize a rank method-based approach for MSP's to the MTMSP setting, and prove an $n^{\log(n)}$ lower bound on share complexity of multi-linear schemes (this improves over the lower bound for linear schemes, as this prove that amortization by increasing k does not help avoid the lower bound proved for $k = 1$).

On the benefit of increasing k for degree-1 polynomial schemes. (multi-linear vs. linear schemes) In [19] a (constant) gap between linear and multi-linear information ratio for certain access structures is demonstrated for certain $\mathbb{F}$. According to recent evidence, (very) large values of $k(n)$ allow for optimal - $O(1)$ information ratio per party for a large set of access structures, where the sharing algorithm has degree 1 (multi-linear) [10]. Namely, this holds for the so-called d-uniform access structures for constant d, to be defined below, a scheme with information ratio of $O(1)$ over $\mathbb{F}_2$ exists. On the flip side, the same family of access structures only admits linear ($k = 1$) scheme with share complexity $\Omega(n^{(d-1)/2})$. This yields an arbitrarily large provable gap of $\Omega(n^{(d-1)/2})$ between the lowest possible and large enough value of k for degree 1 for certain access structures.[7]

Quite surprisingly, a very recent work of [9] demonstrated a degree-1 polynomial construction with share complexity $O(2^{0.999n})$ can be obtained for $k = 1$ over $\mathbb{F}_2$, and share complexity of $O(2^{0.994n})$ can be obtained for non linear (in fact, non-polynomial) schemes. This result was improved in [6] to a share complexity $O(2^{0.942n})$ for linear schemes and to $O(2^{0.892n})$ for general schemes. This result is not a provable separation, but a gap between the best known schemes. It is however particularly exciting, as it contradicts a long held conjecture that optimal share complexity corresponds to the complexity of implementing the access structure f in some complexity model, likely (even non-monotone) circuits, while worst case complexity circuit complexity is $2^{(1-o(1))n}$.

In this work, we observe that a multi-linear scheme over $\mathbb{F}_2$ can do as well as the non-polynomial scheme from [9] for sufficiently large (exponential) $k(n)$.

1.2.3 Beyond Degree-1 PSSS

[7] In fact, their work implies a slightly super-polynomial gap for d-uniform access structures for slightly super-constant d.

General low-degree polynomials. An interesting setting generalizing the most studied setting of degree is that of polynomials with relatively low degree. Low degree polynomials have found many uses in cryptography and complexity theory. One notable use is encoding functions by a vector of (randomized) low degree polynomials [20] [21]. Quite surprisingly, it turns out that all functions can be encoded via a vector of degree-3 polynomials. In a nutshell, a randomized encoding of a function $f(x)$ is a function $g(x;r)$ taking an auxiliary input r. The output of g is a distribution resulting from sampling r uniformly at random from its domain R. The encoding should preserve correctness and privacy of the function in the sense that $g(x;r)$ reveals $f(x)$, and only it. Such encodings are useful in MPC as the degree of a function f typically corresponds to the round complexity of most protocols from the literature.

Due to the privacy of randomized encodings, securely evaluating the encoding indeed results in secure evaluation of the original function. Thus, evaluating low degree randomized encodings of a function via standard protocols [3] is a simple approach to obtaining general constant round MPC protocols in various settings.

In [16] super-polynomial lower bounds are obtained on *quasi-linear* schemes for certain access structures. Obtaining strong lower bounds for other broader-than-linear classes of schemes is definitely an important goal. Our hope is that future research will obtain such bounds for the broader (than multi-linear) class of polynomial schemes of degree $1 > d = O(1)$ for some fixed $\mathbb{F}_q$ and $k = 1$. These bounds would hopefully be better than the best known bounds for general schemes [5] based on lower bounds on the normalized entropy function describing a valid secret sharing scheme - using Shannon inequalities. This bound can prove at most $O(n)$ bounds on the share complexity of a single party.

The Case of $k = 1$ - increasing degree helps. Quite recently, a flurry of work on conditional disclosure of secrets (CDS) has led to exciting progress on upper bounds for share complexity in secret sharing schemes using non-linear schemes.

Non-linear schemes were studied by [22] from the perspective of CDS. CDS is a "non-monotone" variant of secret sharing. In CDS for a predicate P, the parties hold x, y respectively, and are given shares s_x, s_y respectively of the secret s.[8] The secret is disclosed given $x, y \in \{0,1\}^{n/2}$ and s_x, s_y if x, y satisfy a (not necessarily monotone) predicate $P(x, y)$. Otherwise, s_x, s_y reveal nothing about the secret. The "share complexity" measure of CDS is the same as for secret sharing. Every 2-party CDS problem is naturally equivalent to an access structure specified by a bipartite graph $G(V_1, V_2, E)$ of $m = 2^{n/2+1}$ vertices, where $(x, y) \in V_1 \times V_2$ iff $P(x, y) = 1$ [23]. The corresponding access structure has minterms (minimal qualified sets) that are either pairs $\{x, y\} \in E$ or sets of 3 vertices (one can move back and forth with essentially the same share complexity). This class of access structures is referred as bipartite *forbidden graph* access structures. Transforming CDS schemes into secret sharing for the corresponding access structure and vice versa incur only linear blowup in share complexity. It

[8] In the literature, CDS is usually viewed as an MPC protocol among 2 senders and a receiver, and the shares referred as messages.

can be further demonstrated that 2-party CDS for all predicates with maximum (over all predicates P) share complexity sh implies secret sharing with share complexity $O(sh \cdot m)$ (where m is the number of parties) for a generalized set of forbidden graph access structures on $m = 2^{n/2+1}$ vertices specified by any, not necessarily bi-partite graphs [24] (edges in the graph or sets of size 3 are the minterms here). Forbidden graph access structures are also called 2-uniform access structures. d-uniform schemes studied in [10] to which we referred in Section 1.2.2 are a generalization of 2-uniform access structures to ones specified by hypergraphs where edges contain exactly d vertices, and the minterms are either all vertices in an edge, or sets of size $d+1$ vertices.

Via a CDS construction of [22], a secret sharing scheme of total share complexity $\tilde{O}(m^{1/3})$ is obtained for 2-uniform access structures. More precisely, for all prime q, a polynomial scheme over $\mathbb{F}_q$ of degree 2 (with $k = 1$) with share complexity as above exists. These properties are directly "inherited" from the original CDS construction.

In comparison, there exist 2-party CDS schemes [22,25] translating into linear secret sharing schemes (with $k = 1$) with share complexity $\tilde{O}(m^{1/2})$ for 2-uniform access structures. In [24], this is shown to be optimal for this type of access structures and $k = 1$, thereby demonstrating a separation between attainable share complexity between degree-2 polynomial schemes and degree-1 polynomial schemes over $S = \mathbb{F}_2$. See discussion below on $k > 1$, where the situation is quite different. It is an interesting open problem to separate between degree-2 and higher degree polynomial schemes (starting with $k = 1$ and same field)

Even more recently [22] introduced a framework for transforming 2-party CDS into k-party CDS for other values of k with similar complexity to the corresponding 2 party CDS. In these schemes the input (x, y) is distributed among k parties.

One instantiation of their framework generalizes the construction from [25] over $\mathbb{F}_2$ to work for any number $k > 2$ parties with similar complexity to the original 2-party schemes. Similarly to the 2-party case, there exists a transformation from schemes for h-party CDS predicates $P : \{0,1\}^n \to \{0,1\}$ into a corresponding secret sharing scheme on graphs with vertex set $V = \{v_{1,1}, v_{1,2^{n/h}}, \ldots, v_{n,1}, v_{k,2^{n/h}}\}$ with minterms of the form $\{v_{1,g_1}, \ldots, v_{n,g_h}\}$ such that $P(g_1, \ldots, g_h) = 1$, and sets of size $h+1$, overall this is a $m = k2^{n/k}$ party access structure. In particular, for $h = n$ we get $m = 2n$. In this case, the family $\mathcal{A}_m$ consists of $2^{2^{m/2}}$ (out of the $2^{2^{m-O(\log(m))}}$ possible) access structures.

In particular, the linear CDS from [25] translates into a linear scheme with share complexity $O(2^{m/2})$ for the family $\mathcal{A}_m$.

The MV-based scheme from [22] translates into a scheme with $2^{\tilde{O}((\log(m))^{0.5})}$ for the same set of schemes. This scheme is also not polynomial.

The technique used in [22] reducing CDS for large k to CDS with $k = 2$ employs the beautiful and simple idea of emulating each of the parties in the 2-party CDS by PSM [26] among several parties that each holds a part of the input bits of x or y (there are $O(\log(m))$ such parties, each holding a single bit

in the variant that yields secret sharing schemes for $\mathcal{A}_m$). The PSM outputs are the pair of original CDS shares.

The goal is to devise a PSM with particularly good communication complexity that incurs small overhead over its output size, which is the share complexity of the original CDS.

It is an interesting open question whether a similar general technique applies to the degree-2 construction from [22] which also results in a polynomial CDS scheme. This would, at best, yield improved polynomial schemes for a large family of access structures with share complexity $O(2^{m/3})$.

1.3 Beyond PSSS

[22] puts forward a CDS scheme implying non-polynomial secret sharing scheme over $\mathbb{F}_2$ with share complexity $m^{o(1)}$ based on so called matching vector (MV) families for $m/2$-uniform access structures.[9] By the simple observation above, this scheme implies a generalized polynomial statistical scheme with $poly(k)$ multiplicative overhead over the $m^{o(1)}$. The above perfect secret sharing scheme suggests the intriguing possibility that non-polynomial secret sharing schemes may be more efficient than polynomial schemes (over any field) for certain access structures.[10] Making progress in either positive of negative direction would shed light on Question 3.

The line of work on secret sharing schemes from CDS culminates with a surprising recent result [9], demonstrating that there exists a secret sharing scheme with share complexity $O(2^{0.994m})$ for all (monotone) access structures. This breaks the widely held "representation model" conjecture that secret sharing for an access structure f is $\Omega(S)$, where S is the size of $f : \{0,1\}^m \to \{0,1\}$ in some representation model, such as formulas or monotone span programs or circuits. The first two models are consistent with the best (until [9]'s work) known general constructions [12] for general access structures, and the latter is consistent with the best known construction for computationally secure secret sharing. Previously, no better general schemes were known even for the computational setting. By a counting argument, this led to the conjecture that the "right" share complexity for general access structures $2^{m-O(\log(m))}$, which quite surprisingly turned out to be incorrect. The above construction uses CDS for predicates $P : \{0,1\}^g$ for g related to m as a building block. Plugging in the best known MV-based CDS construction outlined above, results in $O(2^{0.994n})$ share complexity. The resulting scheme is also non-polynomial.

The best linear construction, obtained by plugging in the best known linear CDS (for arbitrary k) from [22] results in general linear secret sharing with share complexity $O(2^{0.999n})$.

[9] It is "polynomial" over the ring $\mathbb{Z}_6$, though.

[10] This is true in several other settings, notably for MV codes - MV codes over $\mathbb{Z}_h$ for composite h turn out to be more efficient than over any $\mathbb{Z}_p$ where p is a polynomial.

2 Preliminaries

We will introduce several basic definitions from [7] regarding secret sharing.

Definition 1. *[7] Access Structure: For a set of parties $\{p_1, ..p_n\}$ a subset $\mathcal{A} \subseteq 2^{\{p_1,..,p_n\}}$ is called monotone if $B \in \mathcal{A}$ and $B \subseteq C$ implies $C \in \mathcal{A}$. Sets in $\mathcal{A}$ are called authorized and sets not in $\mathcal{A}$ are called unauthorized.*

Definition 2. *[7] Distribution Scheme: Distribution scheme with domain of secrets K, is a tuple $\Sigma =< \Pi, \mu >$ where μ is a probability distribution on some finite set R (called the set of random strings) and Π is a mapping from $K \times R$ to a set of n-tuples $K_1 \times K_2 \times ... \times K_n$, where K_j is called the domain of shares of p_j. A dealer distributes a secret $k \in K$ according to Σ by first sampling a random string $r \in R$ according to μ, computing a vector of shares $\Pi(k, r) = (s_1, ..., s_n)$, and privately communicating each share s_j to party p_j. For a set $A \subseteq \{p_1, ..., p_n\}$, we denote $\Pi(s, r)_A$ as the restriction of $\Pi(s, r)$ to its A-entries.*

We are now ready to define secret sharing.

Definition 3. *[7] Secret Sharing: Let K be a finite set of secrets, where $|K| \geq 2$. A distribution scheme $< \Pi, \mu >$ with domain of secrets K is a secret-sharing scheme realizing an access structure $\mathcal{A}$ if the following two requirements hold:*

***Correctness**. The secret k can be reconstructed by any authorized set of parties. That is, for any set $B \in \mathcal{A}$ (where $B = \{p_{i_1}, ..., p_{i_{|B|}}\}$), there exists a reconstruction function $Recon_B : K_{i_1} \times ... \times K_{i_{|B|}} \to K$ such that for every $k \in K$,*

$$Pr[Recon_B(\Pi(k, r)_B) = k] = 1 \tag{1}$$

***Perfect Privacy**. Every unauthorized set cannot learn anything about the secret (in the information theoretic sense) from their shares. Formally, for any set $T \notin \mathcal{A}$, for every two secrets $a, b \in K$, and for every possible vector of shares $< s_j >_{p_j \in T}$:*

$$Pr[\Pi(a, r)_T =< s_j >_{p_j \in T}] = Pr[\Pi(b, r)_T =< s_j >_{p_j \in T}] \tag{2}$$

(Multi)Linear secret sharing schemes The most studied and most commonly used class of secret sharing schemes is the linear secret sharing schemes class. This class is subclass of multi-linear secret sharing schemes.

A secret sharing scheme is said to be multi-linear, if $S = \mathbb{F}^k, R = \mathbb{F}^m$ for some finite field $\mathbb{F}$, and each share s_i consists of g linear combinations $l_{i,1}(s_1, \ldots, s_k, r_1, \ldots, r_m) \ldots, l_{i,g}(s_1, \ldots, s_k, r_1, \ldots, r_m)$ over $\mathbb{F}$. The scheme is called linear if additionally $t = 1$.

Complexity measures of secret sharing schemes. The information ratio of a secret sharing scheme, $\mathcal{M}$, is the ratio between the maximum length of the shares and the length of the secret. Formally, $IR(\mathcal{M}) = (\max_{i \in [n]} \log(|S_i|))/|\log S|$, where the maximum is taken over all dealer's random strings r.

The share complexity of secret sharing scheme, $\mathcal{M}$, is $SC(\mathcal{M}) = \max_{i\in[n]} |S_i|$.

We define randomness complexity of a secret sharing scheme $\mathcal{M}$ as $rc(\mathcal{M}) = \log_2(|R|)$ - unlike share complexity, it will be convenient to look at $\log_2(|R|)$ and not at $|R|$.This is the number of bits required to store an element of the set R.

2.1 Polynomial Secret Sharing Schemes (PSSS)

We introduce a natural generalization of (multi)-linear secret sharing schemes - where shares are allowed to be general polynomials of $\overline{s}, \overline{r}$, rather than just linear combinations. Namely:

Definition 4 (PSSS:). *A polynomial sharing scheme (PSSS) is specified by* $(\mathbb{F}, t, k, Sh)$ *where* $\mathbb{F}$ *is a finite field, a secret domain* $\mathbb{F}^t$*, randomness domain* $\mathbb{F}^k$*, and* $t, k \in \mathbb{N}^+$*. The sharing function* $Sh(i, \vec{s}; \vec{r})$ *returns* $(p_{i,1}(\vec{s}, \vec{r}), ..., p_{i,l_i}(\vec{s}, \vec{r}))$ *as the i'th party's share, where each* $p_{i,j}(\vec{s}, \vec{r})$ *is a multivariate polynomial over* $\mathbb{F}$*.*

We will denote the corresponding classes of polynomial schemes over $\mathbb{F}$ via $PSSS_{regexp[s,r],\mathbb{F}}$, where *regexp* is a (variant of) a regular expression in $r, s, 1$. The syntax and semantics of the expression set is defined recursively as follows: r encodes the set of polynomials $\{\sum_{j\in[k]} a_j r_j | a_j \in \mathbb{F}\}$, and s encodes $\{\sum_{j\in[t]} a_j s_j | a_j \in \mathbb{F}\}$, 1 encodes $\{a | a \in \mathbb{F}\}$. For a pair of regular expressions g_1, g_2; g_1^* encodes the set $\{p_1 \cdot ... \cdot p_h | h \in \mathbb{N}, \forall i \in [h], p_i \in g_1\}$; $g_1 + g_2$ encodes $\{p_1 + p_2 | p_1 \in g_1, p_2 \in g_2\}$, and $g_1 \cdot g_2$ encodes the set $\{\sum_{j\in[h]} p_{1,j} \cdot p_{2,j} | h \in \mathbb{N}, \forall j p_{1,j} \in g_1, p_{2,j} \in g_2\}$. g_1^i is a shorthand for $g_1 \cdot ... \cdot g_1$ with i appearances of g_1. We also say that a scheme M has degree at most (exactly) d in r (s), if each monomial contains at most (exactly) d r_i's (s_i's).

For polynomial schemes $\mathcal{M}$, we measure share complexity in field elements, rather than in bits. Formally, these measures will be denoted by $sc_q(\mathcal{M}), SC_q(\mathcal{M}), rc_q(\mathcal{M})$ respectively (it always the case $sc_q(\mathcal{M}) = sc(\mathcal{M})$, as this measure is normalized by secret size).

Our definition is a generalization of the notion of multi linear secret sharing in a natural direction, which potentially adds power over multi-linear schemes. We try to keep it as close as possible to the definition of multi-linear schemes, and insist that the domain where secrets, randomness and computation are performed is a finite field.[11]

A slightly more general notion of polynomial schemes is one where $S \subseteq \mathbb{F}^k$, rather than the entire set $\mathbb{F}^k$.[12]. We refer to such schemes as *generalized* polynomial schemes.

[11] Note that some of the schemes appearing in [8] are quite close to "polynomial" schemes, but the domains employed there are rings R which are (crucially) not fields, and the secrets and randomness do not necessarily come from domains of the form R^t, R^m.

[12] If no restriction on the degree are made, we may replace the subset S with any other subset of the same size, without affecting the other parameters.

3 On Feasibility and Share Complexity of PSSS

In the next two sections, we present some negative result. Our positive result on the power of multilinear schemes is a rather simple observation based on existing work, and is delayed to Appendix A

3.1 Degree 1 in r

We show that a large sub-class of polynomial schemes of degree at most 1 in r ($PSSS_{s^*r+s^*}$) are not more powerful than multi-linear schemes, in the sense that they can not reduce share complexity super-polynomially over multi-linear schemes.

Our first result is that a certain (strict) extension of the class of multi-linear secret sharing schemes as in Definition 4 is equivalent to multi-linear secret sharing. The equivalence is in the sense that for any such scheme, there exists a multilinear scheme over the same field and $poly(n)$ overhead in share complexity. We start with a theorem, that may be interesting on its own right.

Theorem 3. *For all finite fields $\mathbb{F}$, if there exists a scheme $PSSS_{s^*\cdot r+s,\mathbb{F}}$ for an access structure $\mathcal{A}$, then there exists a scheme for $\mathcal{A}$ in $PSSS_{s+r,\mathbb{F}}$ with the same share complexity.*

The idea of proof: The idea of the proof is to show an algorithm that for every scheme in $PSSS_{s+r,\mathbb{F}}$ builds an equivalent multi-linear scheme. We are doing it by substituting the coefficient of r's in the given scheme by some specific secret s. Then we prove that the received scheme is equivalent to the origin one. We are doing it by showing that every qualified set and unqualified set in the received scheme are also qualified or unqualified sets respectively in the origin scheme.

First, observe that we may assume without loss of generality that each polynomial representing a share has free coefficient 0. This is so, because sharing scheme where some polynomials has free coefficients $a_i \neq 0$ is equivalent to an sharing scheme where all the polynomials has free coefficient 0. One can transform shares from the first scheme to the second by just adding a constant vector to the sharing vector and vice versa. So the first scheme realizes the same access structure as the second one. From now on, we assume the polynomials all have 0 free coefficients.

To prove this theorem, let us restate $PSSS_{s^*r+s,\mathbb{F}}$ more conveniently. For such a scheme, a sharing of a secret (vector) s can be represented as $Vs + M_s r$, where r is the randomness vector. Here each entry of M_s is some polynomial $p_{i,j}(s)$, and V is constant. $V \in \mathbb{F}^{a\times k}, M_s \in \mathbb{F}[s]^{a\times t}$. In other words the share vector is $S = (V|M_s) \cdot (s_1, ..., s_k, r_1, ..., r_t)$. A function $\rho : \{1, ..., a\} \longrightarrow \{p_1, ..., p_n\}$ labels each secret entry by a party, so that party P_i receives $\{V_j\}_{j|\rho(j)=i}$. For a set A of parties, we let $M_{s,A}, V_A$ denote the submatrices involved in generating A's shares.

Claim. Let $\mathcal{M} = \{\mathbb{F}, V, M_s, \rho\}$, in $PSSS_{s^*r+s,\mathbb{F}}$, be a secret sharing scheme for an access structure $\mathcal{A}$. The scheme $\mathcal{M}'$ where M_s is substituted by a constant matrix $M_{\vec{s_1}}$ for some fixed s_1 is a (multi-linear) secret sharing scheme for the same access structure.

Proof. Fix some secret vector s_1 as in the statement of the claim. We will divide the proof into two parts: correctness, and privacy.

Correctness: Consider any $\vec{s_0} \in \mathbb{F}^t$. Now we will look at authorized set A. For notation convenience let V_A denote the sub-matrix obtained by restricting V to the rows labeled by parties in A, and A_s denote the sub-matrix obtained by restricting M_s to the rows labeled by parties in A. Let us look at the two share distributions $(V_A|A_{\vec{s_1}}) \cdot (\vec{s_1}|r_1)^t$ and $(V_A|A_{\vec{s_0}}) \cdot (\vec{s_0}|r_0)^t$ of secrets $\vec{s_1}$ and $\vec{s_0}$, where $\vec{r_1}, \vec{r_0} \in \mathbb{F}^k$ are independent random vectors. The correctness of $\mathcal{M}$ is equivalent to stating that for all pairs r_0, r_1, we have:

$$\begin{gathered}(V_A|A_{\vec{s_1}}) \cdot (\vec{s_1}|r_1)^t \neq (V_A|A_{\vec{s_0}}) \cdot (\vec{s_0}|r_0)^t \\ \Downarrow \\ V_A \cdot (\vec{s_0} - \vec{s_1})^t \neq A_{\vec{s_1}} \cdot r_1^t - A_{\vec{s_0}} \cdot r_0^t.\end{gathered} \tag{3}$$

It is correct in particular for $r_0 = \bar{0}$. Which means that:

$$V_A \cdot (\vec{s_0} - \vec{s_1})^t \neq A_{\vec{s_1}} \cdot r_1^t \tag{4}$$

Due to the fact that Equation 4 is correct for any $\vec{s_0} \in \mathbb{F}^k$ and by the structure of the secret domain, for any two secret vectors $\vec{s_2}, \vec{s_3} \in \mathbb{F}^k$ there exists $\vec{s_0}$ for which $\vec{s_2} - \vec{s_3} = \vec{s_0} - \vec{s_1}$. From equation 4:

$$V_A \cdot (\vec{s_2} - \vec{s_3})^t \neq A_{\vec{s_1}} \cdot r_1^t \tag{5}$$

For all $r_1 \in \mathbb{F}^t$. So for any $r_2, r_3 \in \mathbb{F}^t$ we can denote $r_1 = r_3 - r_2$. We conclude that:

$$\begin{gathered}V_A \cdot (\vec{s_2} - \vec{s_3})^t \neq A_{\vec{s_1}} \cdot r_1^t \\ \Downarrow \\ (V_A|A_{\vec{s_1}}) \cdot (\vec{s_2}|r_2)^t \neq (V_A|A_{\vec{s_1}}) \cdot (\vec{s_3}|r_3)^t\end{gathered} \tag{6}$$

Which is precisely the definition of correctness: as r_1 is arbitrary, the pair $r_2, r_3 = r_1 - r_2$ is any pair of vectors on $\mathcal{F}^t$.

Privacy: Let us choose a secret $\vec{s_1} \neq \vec{s_0} \in \mathbb{F}^k$. It follows directly from privacy that for each unauthorized set A, for any $\vec{r_0} \in \mathbb{F}^t$ there exists $\vec{r_1} \in \mathbb{F}^t$ for which:

$$\begin{gathered}(V_A|A_{\vec{s_1}}) \cdot (\vec{s_1}|r_1)^t = (V_A|A_{\vec{s_0}}) \cdot (\vec{s_0}|r_0)^t \\ \Downarrow \\ V_A \cdot (\vec{s_0} - \vec{s_1})^t = A_{\vec{s_1}} \cdot r_1^t - A_{\vec{s_0}} \cdot r_0^t\end{gathered} \tag{7}$$

In particular this is true for $r_0 = \bar{0}$. Then for any $\vec{s_0}$ there exists $r_1 \in \mathbb{F}^t$ for which:

$$V_A \cdot (\vec{s_0} - \vec{s_1})^t = A_{\vec{s_1}} \cdot r_1^t \tag{8}$$

Let us look now at multi-linear sharing scheme which is obtained by substituting $\vec{s}$ in $M_{\vec{s}}$ by $\vec{s_1}$ and on two secrets $\vec{s_2}$ and $\vec{s_3}$. Consider $\vec{s_0}$ for which $\vec{s_2}-\vec{s_3} = \vec{s_0}-\vec{s_1}$. From 8 we know that there exist r_1 for which:

$$\begin{aligned} V_A \cdot (\vec{s_0} - \vec{s_1})^t &= A_{\vec{s_1}} \cdot r_1^t \\ &\Downarrow \\ V_A \cdot (\vec{s_2} - \vec{s_3})^t &= A_{\vec{s_1}} \cdot r_1^t \end{aligned} \tag{9}$$

So for any vector $r_3 \in \mathbb{F}^t$ we get:

$$\begin{aligned} V_A \cdot (\vec{s_2} - \vec{s_3})^t &= A_{\vec{s_1}} \cdot r_1^t \\ &\Downarrow \\ V_A \cdot (\vec{s_2} - \vec{s_3})^t &= A_{\vec{s_1}} \cdot (r_3 - (r_3 - r_1))^t \\ &\Downarrow \\ (V_A | A_{\vec{s_1}}) \cdot (\vec{s_2} | r_3 - r_1)^t &= (V_A | A_{\vec{s_1}}) \cdot (\vec{s_3} | r_3)^t \end{aligned} \tag{10}$$

We prove that this implies privacy. Picking r_3 at random, the vector $r_3 - r_1$ is a random vector as well (correlated with r_3, but it does not matter). Thus, the left hand size, where r_3 is picked at random is distributed precisely as the shares seen by A when sharing $\vec{s_2}$ in $\mathcal{M}'$. This value is uniform over the affine subspace $V_A\vec{s_2} + \text{colSpan}(A_{\vec{s_1}})$. Now, the right hand side is also a random element of an affine subspace of the form $V_A\vec{s_3} + \text{colSpan}(A_{\vec{s_1}})$, and is distributed precisely as a share of s_3 seen by A at M'. As these affine subspaces intersect, they must be the same subspace, since both are cosets of $\text{colSpan}(A_{\vec{s_1}})$. This concludes the proof.

Next, we complement the above result with a lower bound on the power of another interesting class of schemes where monomials of degree 0 in r can have unbounded degree in r, but monomials of degree 1 in r have degree 0 in s. Namely, $PSSS_{s^*+r}$. We show any such scheme can be emulated by a multi-linear one upto an increase of a factor n in share complexity.

Theorem 4. *For every scheme $\mathcal{M} = (V^s, M, \mathbb{F}, \rho)$ in $PSSS_{s^*+r}$ with parameters t, k there exists a multilinear scheme $\mathcal{M}'$ for the same access structure with share complexity $sc(\mathcal{M}') \leq n \cdot sc(\mathcal{M})$.*[13]

Proof. We say that a set of t vectors V satisfies the correctness (privacy) condition relatively to M, if a scheme with a sharing algorithm $Sh(\overline{s}, r) = \sigma_{v_i \in V} s_i v_i + Mr$ is correct (private).

We are now ready to construct our basis. First, observe that given a set of vectors $T = \{V^{s_1}, \ldots, V^{s_y}\}$ that satisfies the privacy condition relatively to M, then so does $span(T)$ (as $V_A^{s_j}$ belongs to the 0-coset of A).

As the set we construct will be a subset of $span(\{V^s\}_{s \in S})$, it remains to prove the constructed set satisfies correctness. The construction is as follows.

[13] Here V^s is a set of vectors corresponding to the various secrets in S, and M is the common matrix multiplying the r-portion.

1. Iteration 0: Initialize $B = \phi$ (recall $span(B)$ is $\{\vec{0}\}$).
2. Iteration $i > 0$: Find some $s \in S$, so that for all minterms $A \subseteq [n]$, V^s belongs to a coset of $\mathbb{F}^{\#_{rows}(M_A)}/colSpan(M_A)$ that differs from coset(v) for all $v \in span(B)$. Halt if no such s exists. If it does, add one such V^s to B.

We show that at least $t - n$ iterations are made by the above procedure, and that the resulting B indeed satisfies correctness relatively to M. That is, we prove that we successfully complete iteration i for all $i \leq t - n$, and that B at the end of iteration i is a vector space of dimension i by induction on i.

The base case trivially holds, as B is initially empty. Assume $span(B)$ is correct relatively to M at the end of iteration $i < ..$, and $Image_{f_A}(B)$ has dimension i. Consider some minterm A. Then, by correctness $Image_{f_A}(S)_A$ mapping S to distributions over $\mathbb{F}^{\#_{rows}(M_A)}$, is of size $\mathbb{F}^t$ (where all resulting distributions have pairwise disjoint support). Consider a linear mapping . Then by construction $f_A(S)$ maps each s to a uniform distribution over a coset $f'_A(g(s))$ of $colSpan(M_A)$, where f'_A is a linear mapping from $\mathbb{F}^{\#_{rows}(M_A)}$ to $\mathbb{F}^{\#_{rows}(M_A)}$, the kernel of which is exactly $colSpan(M_A)$, and g is some (injective) mapping from S to $\mathbb{F}^t$. This holds as the coset of v in $\mathbb{F}^r$ relatively to a linear subspace $C \subseteq \mathbb{F}^t$ is the image of v under a (unique) linear mapping f_A from C to $\mathbb{F}^{\#_{rows}(M_A)}$ whose kernel is precisely $colSpan(M_A)$.

By correctness of the sharing scheme, all the cosets are pairwise distinct. By correctness of B relatively to M, $f'_A(span(B)_A)$ is a linear subspace of dimension i of $\mathbb{F}^{\#_{rows}(M_A)}$. This is the case by choice of B. For each minterm A, the set of cosets $f'_A(g(s))$ are pairwise distinct. Thus at most $|\mathbb{F}|^i$ of the vectors V^s are already in $span(B)_A$, while the rest are not. There are at most 2^n minterms (a gross estimation) in AS, thus, going over all minterms, rules out at most $2^n|\mathbb{F}|^i \leq |\mathbb{F}|^{i+n}$ vectors in V_s that satisfy the condition in item 2. Thus, up until iteration $i = t - n$, we always have a remaining vector V^s to add to B.

3.2 $PSSS_{s^*+s^*r^2+1}$ is very weak

In this section we will show that if the shares are from the class $PSSS_{s^*+s^*r^2+1}$ captures only the access structures consisting of a set of singletons as its minterms. Formally:

Theorem 5. *Let $\mathbb{F}$ be a finite field of odd characteristic. Then the class $PSSS_{s*+s*r^2+1,\mathbb{F}}$ can only implement a simple set of access structures where its minterms are all singletons.*

Our proof will rely heavily on [27] where the number of solutions of quadratic form equations are studied. They have proved that there are only 3 types of quadratic form equations, and each type has a determined number of solutions. Using these facts we have shown that, in a perfect secret sharing scheme, if a party receives a share which was calculated by quadratic form formula has to receive the hole secret or to receive share that does not depend on the secret at all (just some constant or a random number).

We first present some required background from [27].

Theorem 6 ([27]). *If f is a quadratic form in n variables defined over F_q, then f is equivalent to a nondegenerate quadratic form having order m, for some $0 \leq m \leq n$, of exactly one of the following types:*

1. $x_1x_2 + x_3x_4 + ... + x_{m-1}x_m$
2. $x_1x_2 + x_3x_4 + ... + x_{m-3}x_{m-2} + (\alpha_1 x_{m-1}^2 + \alpha_2 x_{m-1}x_m + \alpha_3 x_m^2), \alpha_i \in \mathbb{F}$
3. $x_1x_2 + x_3x_4 + ... + x_{m-2}x_{m-1} + ax_m^2, a \in \mathbb{F}^*$

Another result is even more important for us:

Definition 5. *Let q be odd and let η be the real-valued function of $\mathbb{F}^*$ with $\eta(c) = 1$ if c is the square of an element of F^* and $\eta(c) = -1$ otherwise. Then η is called the quadratic character of F.*

Theorem 7 ([27]). *Let $f(x_1, ..., x_n)$ be a quadratic form defined over F having order m, $1 \leq m \leq n$, and let $b \in \mathbb{F}^*$. Then, the number of solutions:*

$$N(f(x_1, ..., x_n) = b) = \begin{cases} q^{n-m}(q^{m-1} - q^{\frac{m-2}{2}}) & \text{if } f \text{ is of Type 1.} \\ q^{n-m}(q^{m-1} + q^{\frac{m-2}{2}}) & \text{if } f \text{ is of Type 2.} \\ q^{n-m}(q^{m-1} + \eta(ab)q^{\frac{m-2}{2}}) & \text{if } f \text{ is of Type 3, } q \text{ odd.} \\ q^{n-m}(q^{m-1}) & \text{if } f \text{ is of Type 3, } q \text{ even.} \end{cases}$$

Proof of Theorem 5. We are looking only at the cases where q (the size of the field) is odd. So the last line in Theorem 7 is irrelevant for us. The number of solutions that is given in Theorem 7 is only for $b \in \mathbb{F}^*$, but the number of solutions for $b = 0$ can be easily calculated by subtracting all the solutions for all $b \in \mathbb{F}^*$ from all the possible solutions which is q^n.

$$N(f(x_1, ..., x_n) = 0) = \begin{cases} q^{n-m}(q^{m-1} + (q-1)q^{\frac{m-2}{2}}) & \text{if f is of Type 1.} \\ q^{n-m}(q^{m-1} - (q-1)q^{\frac{m-2}{2}}) & \text{if f is of Type 2.} \\ q^{n-m}(q^{m-1} - \sum\limits_{b \in \mathbb{F}^*} \eta(ab)q^{\frac{m-2}{2}}) & \text{if f is of Type 3, q odd.} \\ q^{n-m}(q^{m-1}) & \text{if f is of Type 3, q even.} \end{cases}$$

In the first two types it is obvious that $N(f(x_1, ..., x_n) = 0) \neq N(f(x_1, ..., x_n) = b)$ fro all $b \neq 0$. For the third type, where q is odd, $N(f(x_1, ..., x_n) = 0) \neq N(f(x_1, ..., x_n) = b)$ for all $b \neq 0$ too. Because $\eta(ab) = \pm 1$ and since q is odd $\sum\limits_{b \in \mathbb{F}^*} \eta(ab)$ is even. So $\eta(ab) \neq \sum\limits_{b \in \mathbb{F}^*} \eta(ab)$ for all $b \in \mathbb{F}^*$.

From these results we can conclude that if the size of $\mathbb{F}$ is odd and a party receives share of the form $f(\vec{s}, \vec{r}) = q(\vec{s}) + \sum\limits_{\substack{i,j \in \{1,..,n\} \\ i \leq j}} q_{i,j}(\vec{s}) r_i r_j + a$, where $q(\vec{s})$ is not constant, then there are $\vec{s_1}, \vec{s_2} \in S$ for which the distribution of $f(\vec{s_1}, \vec{r})$ differ from the distribution of $f(\vec{s_2}, \vec{r})$. So this party has to be alone in a minterm.

For now we have observed a shares of the class $PSSS_{s^*+s^*r^2+1}$ where $q(\vec{s})$ is not constant. Let us look at the case where $q(\vec{s})$ is constant.

So the shares that each party p receive is of the form

$$\mathrm{f}_p(\vec{s},\vec{r}) = \sum_{\substack{i,j\in\{1,..,n\}\\ i\le j}} q_{i,j}(\vec{s})r_i r_j + a_p$$

. For any $\vec{s} \in S$ we have $f_p(\vec{s},\vec{0}) = a_p$. It is a contradiction to the correctness of a secret sharing scheme, because if even all the parties receive a share $(a_1, a_2,$ $..., a_n)$ (for simple notation we assume that every party receive one share. Our claim can be easily modified for a scheme where every party receive a vector of shares), they will not be able to calculate the secret. □

4 On the randomness complexity of polynomial schemes

In this section we will focus on bounding the randomness complexity needed for secret sharing.

4.1 Bounding the Number of Random Variables in Quadratic Secret Sharing Schemes

Theorem 8. *For any quadratic scheme $\mathcal{M} \in PSSS_{s+r^2+r+1}$ there exist quadratic scheme $\mathcal{M}' \in PSSS_{s+r^2+r+1}$ for which the number of random variables is bounded by $O(2^{2^n})$.*

We are looking now on schemes in $PSSS_{s*+r^2+r+1}$. Each polynomial in these schemes is of the form: $f(\vec{s},\vec{r}) = q(\vec{s}) + \sum_{\substack{i,j\in\{1,..,n\}\\ i\le j}} a_{ij}r_i r_j + \sum_{i\in\{1,..,n\}} b_i r_i + a$. So each polynomial can be separated into two parts, a linear part and a quadratic form part.

Lemma 1. *For any degree 2 polynomial $p(\vec{r})$ where $\vec{r} \in \mathbb{F}^n$. If p is linear type than there exist a linear transformation $T : \mathbb{F}^n -> \mathbb{F}^n$ for which $p(r'_1, ..r'_n) = q(r'_1...r'_m) + l(r'_{m+1}..r'_n)$ where q is quadratic form and l is linear. That is to say, p consists of 2 disjoint parts, a quadratic form and a linear part.*

Proof of lemma 1: Polynomial $p(\vec{r})$ consists of 2 polynomials, a quadratic form polynomial $q(\vec{r})$ and a linear polynomial $l(\vec{r})$. In this proof we will iteratively transform $\vec{r} = (r_1, ..., r_n)$ to $\vec{r}' = (r'_1, ..., r'_n)$. In each step we will choose coordinate r_i in $\vec{r}$ that exists in $q(\vec{r})$ and in $l(\vec{r})$ and find a linear transformation T for which $q(T(\vec{r}))$ and $l(T(\vec{r}))$ has one common significant variable less than in $q(\vec{r})$ and $l(\vec{r})$. From theorem 6 there are 3 types of quadratic form polynomials. So there is a linear transformation T_0 which transforms q to one of the types:

1. $r_1r_2 + r_3r_4 + ... + r_{m-1}r_m$
2. $r_1r_2 + r_3r_4 + ... + r_{m-3}r_{m-2} + (\alpha_1 r^2_{m-1} + \alpha_2 r_{m-1}r_m + \alpha_3 r^2_m), \alpha_i \in \mathbb{F}$
3. $r_1r_2 + r_3r_4 + ... + r_{m-2}r_{m-1} + ar^2_m, a \in \mathbb{F}^*$

Now, after this transformation, we will move to the iterative choosing of transformation. We will choose a coordinate r_i that is significant (exists) in q and in l after the transformation T_0 is applied on them.

case 1: if $1 \leq i \leq m-2$.

Regardless of the quadratic form type of q, $q(\vec{r}) = r_1 r_2 + ... + r_i r_{i+1} + ...$ and $l(\vec{r}) = ... + a r_i + ...$ Let us look at transformation $T : \mathbb{F}^n \to \mathbb{F}^n$ which transforms r'_j to r_j for $j \neq i+1$ r'_{i+1} to $r_{i+1} + a$. After this transformation is applied on p, $q(T(\vec{r}))$ and $l(T(\vec{r}))$ has one common significant variable less than in $q(\vec{r})$ and $l(\vec{r})$.

case 2: if $i = m-1$ or $i = m$ for type 1.

The same transformation from the previous case will work here too.

case 3: if $i = m-1$ or $i = m$ for type 2.

With out loss of generality let us choose $i = m$. For type 3 $q(\vec{r}) = r_1 r_2 + ... + r_{m-3} r_{m-2} + (a_1 r_{m-1}^2 + a_2 r_{m-1} r_m + a_3 r_m^2)$ and $l(\vec{r}) = ... + a r_m + ...$ Let us look at transformation $T : \mathbb{F}^n \to \mathbb{F}^n$ which transforms r'_j to r_j for $j \neq m, m-1$, r'_m to $r_m + \frac{2aa_1}{a_2^2 - 4a_1a_3}$ and r'_{m-1} to $r_{m-1} - \frac{aa_2}{a_2^2 - 4a_1a_3}$ ($a_2^2 \neq 4a_1a_3$ because otherwise q would be type 3 and not type 2). So

$$p(\vec{r}) = ... + (a_1 r_{m-1}^2 + a_2 r_{m-1} r_m + a_3 r_m^2) + a r_m + ... =$$
$$... + a_1 (r'_{m-1} + \frac{aa_2}{a_2^2 - 4a_1a_3})^2 + a_2 (r'_{m-1} + \frac{aa_2}{a_2^2 - 4a_1a_3})(r'_m - \frac{2aa_1}{a_2^2 - 4a_1a_3}) +$$
$$+ a_3 (r'_m - \frac{2aa_1}{a_2^2 - 4a_1a_3})^2 + ... = ... + a_1 r'^2_{m-1} + c r'_{m-1} r'_m + a_3 r'^2_m + d + ... \quad (11)$$

Where c and d are constants. So after this transformation is applied on p, $q(T(\vec{r}))$ and $l(T(\vec{r}))$ has one common significant variable less than in $q(\vec{r})$ and $l(\vec{r})$.

case 4: if $i = m$ for type 3.

For type 3 $q(\vec{r}) = r_1 r_2 + ... + r_{m-2} r_{m-1} + b r_m^2$ and $l(\vec{r}) = ... + a r_m + ...$ Let us look at transformation $T : \mathbb{F}^n \to \mathbb{F}^n$ which transforms r'_j to r_j for $j \neq m$ r'_m to $r_m + \frac{a}{2b}$ ($b \neq 0$ because otherwise q would be type 1 and not type 3). So

$$p(\vec{r}) = ... + b r_m^2 + a r_m + ... = ... + b(r'_m - \frac{a}{2b})^2 + a(r'_m - \frac{a}{2b}) + ... = ... + b r'^2_m - \frac{a^2}{4b} \quad (12)$$

So after this transformation is applied on p, $q(T(\vec{r}))$ and $l(T(\vec{r}))$ has one common significant variable less than in $q(\vec{r})$ and $l(\vec{r})$.

Using this cases iteratively for all coordinates in $\vec{r}$ which exist in q and in l we will receive a transformation that transforms $p(\vec{r})$ to $p(T(\vec{r}))$ which consists of 2 disjoint parts, a quadratic form and a linear part which do not have any significant r_i in common.

Proof of Theorem 8: **The idea of the proof**: The random variables in $\mathcal{M}$ is a vector that is sampled uniformly from $\mathbb{F}^t$. We will try to choose a subspace $A \subseteq \mathbb{F}^t$ in such way that if we will sample our random variables from this space, the privacy and correctness will be preserved. We will build such a subspace by adding iteratively vectors to a basis.

Proof:

privacy: In our proof we will use Vazirani's xor lemma from [28]. This lemma implies that polynomials $(p_1(\vec{r})...p_1(\vec{r}))$ for $\vec{r} \in \mathcal{A}$ are distributed uniformly over $\mathcal{A}^n$ iff all the linear combinations $\sum_{i=1}^{n} a_i p_i(\vec{r})$ distributes uniformly over $\mathcal{A}$. Let us consider a max unqualified set M. Let us look at the polynomials resulting from Vazirani's xor lemma. From corollary **??**, for an unqualified set M, all the linear combinations of polynomials are linear type. For every such polynomial (resulted from Vazirani's xor lemma) $p(\vec{r}) = q(\vec{r}) + l(\vec{r})$ using lemma 1 we will choose vector $\vec{r}$ that will zero $q(\vec{r})$ and will not zero $l(\vec{r})$. If this vector is not already in A we will add it to the basis of A.

Let us see why every polynomial resulted from Vazirani's xor lemma distribute uniformly over subspace $A \in \mathbb{F}^t$. For polynomial $p(\vec{r}) = q(\vec{r}) + l(\vec{r})$ let us look at a basis $\vec{b_1}, ..., \vec{b_m}$ of A that contains the vector that zeros q and does not zero l. Let this vector be b_1. Every vector $\vec{r} \in A$ can be presented as $\vec{r} = \sum_{i=1}^{m} c_i b_i$. $p(c_1 b_1)$ for $c_1 \in \mathbb{F}$ is distributed uniformly over $\mathbb{F}$. So if we set c_i for $i \in 2, .., m$ to a specific values, than $p(\sum_{i=1}^{m} c_i b_i)$ is distributed uniformly over $\mathbb{F}$. Thus, without presetting c_i for $i \in 2, .., m$, $p(\sum_{i=1}^{m} c_i b_i)$ also distributes uniformly over $\mathbb{F}$.

In conclusion, all the polynomial resulted from Vazirani's xor lemma are distributed uniformly over subspace $A \in \mathbb{F}^t$. So from Vazirani's xor lemma follows that the polynomials which computes the shares for M are also distributed uniformly over $\mathbb{F}^{|M|}$. That is to say, M will preserve privacy if the random variables will be sampled from A.

We will do this process for all the max unqualified sets, and we will receive a subspace A that satisfies the privacy of all the unqualified set.

correctness: The correctness is preserved automatically if the space of the random variables is subspace of $\mathbb{F}^t$. Because if the random variables is sampled from A, the set of shares that a qualified set will receive is included in the set of shares that could be received if the randomness were sampled from $\mathbb{F}^t$.

There are at most $O(2^n)$ max unqualified sets. In each such set there are at most $O(2^n)$ polynomials that generate the shares. so for each such set there are at most $O(2^{2^n})$ polynomials resulted from Vazirani's xor lemma. So there are $O(2^n * 2^{2^n})$ vectors in the basis of A.

Now, that we bounded the number of random variables for the family $PSSS_{s+r^2+r+1}$, we will extend our proof to the general quadratic polynomials family $PSSS_{s*+r^2+rs+r+1}$.

Theorem 9. *For any quadratic scheme $\mathcal{M} \in PSSS_{s*+r^2+rs+r+1}$ there exists quadratic scheme $\mathcal{M}' \in PSSS_{s*+r^2+rs+r+1}$, with the same sharing rate, for which the number of random variables is bounded by $O(|S|2^n 2^{2^n})$. Where n is the number of parties in the access structure and $|S|$ is the number of secrets.*

Here we will use more general version of Vazirani's xor lemma, that states:

Lemma 2. *2 vectors of random variables $(X_1, ..., X_n)$ and $(X'_1, ..., X'_n)$ has the same distribution iff for any linear combination, $\sum_{i=1}^{n} a_i X_i$ and $\sum_{i=1}^{n} a_i X'_i$ has the same distribution.*

Here we will again construct a linear subspace, A, of $\mathbb{F}^t$. The difference here that for an unqualified set M, the polynomials resulted from Vazirani's xor lemma are not have to be of a linear type. Let us look at one such polynomial $p(\vec{s}, \vec{r})$. Notice, that if p has the same distribution over $\mathbb{F}$ for any 2 secrets $\vec{s_1}$ and $\vec{s_2}$ when $\vec{r} \in \mathbb{F}^t$. So from theorem 6, the polynomial $p(\vec{s_1}, \vec{r})$ and $p(\vec{s_2}, \vec{r})$ are from the same type.

If by setting any $\vec{s_i}$ in $p(\vec{s}, \vec{r})$ we receive a linear polynomial, for all $\vec{s_i} \in S$ we will add a vector that zeros the quadratic form part of $p(\vec{s_i}, \vec{r})$ and will not zero the linear part to the basis of A (like we have done in the previous proof). In this case, for any two shares $\vec{s_1}$ and $\vec{s_2}$ the polynomials $p(\vec{s_1}, \vec{r})$ and $p(\vec{s_2}, \vec{r})$ will have a uniform, and accordingly also same, distribution over A.

In other cases, not linear type, let us look at polynomials $p(\vec{s_1}, \vec{r}) = q(\vec{r}) + l(\vec{s_1}, \vec{r})$ and $p(\vec{s_2}, \vec{r}) = q(\vec{r}) + l(\vec{s_2}, \vec{r})$ that are obtained from $p(\vec{s}, \vec{r})$ by substituting some $\vec{s_1}, \vec{s_2} \in S$. The polynomials are one of the 3 types from theorem 6. From the proof of lemma 1 we can see that q has the same type as p. So $p(\vec{s_1}, \vec{r})$ and $p(\vec{s_2}, \vec{r})$ has the same type. From theorem 6 there is a linear transformation $T : \mathbb{F}^t -> \mathbb{F}^t$ that normalizes q (the quadratic part of p). That is to say,

$$p(T(\vec{r}), \vec{s}) = q(T(\vec{r})) + l(\vec{s}, T(\vec{r})) = q'(\vec{r}) + l'(\vec{s}, \vec{r}) = p'(\vec{r}, \vec{s})$$

where q' is one of the 3 types of quadratic form from theorem 6. Let us denote subspace $B = T(A)$. From the proof of lemma 1 we can see that for any secret $\vec{s_i}$ there is transformation $T_i(\vec{r}) = \vec{r} + \vec{d_i}$ that satisfies

$$p'(T_i(\vec{r}), \vec{s_i}) = p'(\vec{r} + \vec{d_i}, \vec{s_i}) = q'(\vec{r})$$

. Let us add all the d_i to the basis of B. So now we received new subspace $B \subseteq B'$ that contains all d_is. for any $\vec{r} \in B'$ and any two secrets s_1 and s_2

$$p'(\vec{r} + \vec{d_1}, \vec{s_1}) = q'(\vec{r}) = p'(\vec{r} + \vec{d_2}, \vec{s_2})$$

So it is easily seen that $p'(\vec{r}, \vec{s_1})$ and $p'(\vec{r}, \vec{s_2})$ has the same distribution over B'. Note that if we add the vectors $T^{-1}(d_i)$ to the basis of A we will receive subspace A' that satisfies $A' = T^{-1}(B')$. We have already proved that $p'(\vec{r}, \vec{s_i})$ has the same distribution over B' for every secret s_i. Due to the definition of p' $p(\vec{r}, \vec{s_i})$ has the same distribution over A' for every secret s_i.

In conclusion, for every polynomial p resulted from Vazirani's xor lemma 2 we have found at most $|S|$ vectors that should be added to the basis of A, so that p will have the same distribution over A for any secret $s \in S$. There are $O(2^n)$ unqualified sets. Each set has $O(2^{2^n})$ polynomials resulted from Vazirani's xor lemma and each polynomial contributes $O(|S|)$ vectors to the basis of A. So $dim(A) = O(|S|2^n 2^{2^n})$. So we have found a secret sharing scheme $\mathcal{M}'$ that has the same properties like $\mathcal{M}$ (access structure, sharing rate...) and the number of random variables is bounded by $O(|S|2^n 2^{2^n})$.

4.2 Bounding the Number of Random Variables in (general) PSSS

In this section we will present a bound on the number of random variables in generalized PSSS.

Theorem 10. *Let $\mathcal{M}$ denote a (possibly generalized) secret sharing scheme over the finite field $\mathbb{F}_{q^d}$ of characteristic q ($S = \mathbb{F}_{q^d}^k$ for some integer k), implementing an access structure $\mathcal{A}$. Let us denote its share complexity counting the number of field elements in its share vector by $SC = SC_{q^d}(\mathcal{M})$. Then, there exists an equivalent (generalized iff M is) polynomial scheme $\mathcal{M}'$ with the same $\mathcal{S}$, $\mathcal{S}_1 \times ... \times \mathcal{S}_n$ satisfying $rc_{q^d}(\mathcal{M}') = \mathcal{SC}^{\tilde{\mathcal{O}}(\mathcal{SC})^3}$*[14].

Notation and some facts on LP's: Before proving the theorem we will need some facts on linear programming. Here we will only care about the feasible region of a linear program (LP), and will not have a target function to optimize. Without loss of generality we consider LP's comprised of systems of inequalities of the form $Ax = b, x \geq 0$, where A, b are over $\mathbb{R}$, all b's components are non-negative. We denote such LP's by (A, b). We may also assume without loss of generality that $A \in \mathbb{R}^{m \times n}$, where $m \leq n$, and A has full rank (m). We say that a solution to the system is a basic feasible solution (BFS) if x only has non zero coordinates corresponding to an invertible submatrix of A (taking a subset of columns). For a finite set $B \subseteq \mathbb{R}^m$ of vectors, a convex combination of B is a linear combination $\sum_{b \in B} \alpha_b b$, so that $\sum_{b \in B} \alpha_b = 1$, and $\forall b \in B, \alpha_b \geq 0$. The convex hall of a set $A \subseteq \mathbb{R}^m$ is the set of all linear combinations of finite subsets $B \subseteq A$. We denote it as $CH(A)$. We say a set $A \subseteq \mathbb{R}^m$ is convex if $CH(A) = A$. An extreme point of a convex set A is a point $y \in A$ such that if y is a convex combination of $\{x, z\} \subseteq A$, then either $x = y$ or $z = y$. It is well known that the set of solutions of an LP is convex. We say an LP has a *bounded* solution set X, if there exists an integer N, such that $\ell_\infty(x) \leq N$ for all $x \in X$.

For a set $A = \{a_1, ..., a_t\} \subseteq \mathcal{R}^m$, the affine dimension of A, aff(A), is the dimension of $\{a_2 - a_1, ..., a_t - a_1\}$. We say that a set A has *full affine dimension* if aff$(A) = |A| - 1$.

Theorem 11. *[[29], chapter 2] The set of extreme points $\mathcal{B}$ of a bounded non-empty solution set X of an LP $(A, b) \in \mathbb{R}^{m \times n} \times \mathbb{R}^{m \times 1}$ is non empty, and $X = CH(\mathcal{B})$. Furthermore, the set $\mathcal{B}$ is precisely the set of BFS's of (A, b).*

Lemma 3. *[Cramer's rule] Let $A \in \mathcal{R}^{m \times m}$ denote an invertible matrix. Then, $A^{-1}_{i,j} = |A_{i,j}|/|A|$. Here $A_{i,j}$ is the (i, j)'th cofactor of A, obtained from removing the i'th column and j'th row from A.*

Lemma 4. *Let $A \in \mathbb{R}^{m \times m}$ denote a matrix whose entries $a_{i,j}$ all satisfy $|a_{i,j}| \in \{0\} \cup [\delta, 1]$ for $0 > \delta$. Then every entry $a'_{i,j}$ in A^{-1} satisfies*

$$|a'_{i,j}| \text{ or } |a'_{i,j}| \geq \delta^m / m^m.$$

Additionally, if the $a_{i,j}$'s are rational, then so are the $a'_{i,j}$'s.

The proof of the above lemma follows directly from Lemma 3.

[14] Additionally, if the original scheme is (fully) polynomial, $\mathcal{M}'$ is fully polynomial as well.

Proof of Theorem 10 The proof consists of several steps:
step 1:

Proof. Let us consider the given (generalized) polynomial scheme $\mathcal{M}$ as in the theorem statement. Let us also denote $sc = \log_Q(SC)$, and $Q = q^d$.

We denote the share vector output by Sh for any $\vec{s} \in S$ by $\vec{sh} = (sh_1, ..., sh_n) \in \mathbb{F}_Q^{sc})$. For every secret $\vec{s}_i \in S$, and for every possible $\vec{sh}_j \in \mathbb{F}_Q^{sc}$ let us denote by p_{ij} the probability to receive $\vec{sh}_j$ as the share vector on input $\vec{s}_i$. (For each $\vec{s}_i$, there are Q^{sc} such probabilities.)

Now we will build a matrix that will hold all the constraints on the probabilities $p_{i,j}$ for a scheme $\mathcal{M}'$ with $S, S_1 \times ... \times S_n$ for $\mathcal{A}$. Let $p_{\mathcal{M}}$ denote the probabilities vector induced by $\mathcal{M}$. Our set of requirements will be stronger than stating that $\mathcal{M}'$ is a secret sharing scheme for $\mathcal{A}$, as it will additionally require that $\mathcal{M}'$ is "similar" to $\mathcal{M}$ in a certain way. A solution will be guaranteed to exist, as $p_{\mathcal{M}}$ is such a solution ($\mathcal{M}$ is "similar" to itself).

The constraints are divided into 3 sets:
privacy: For any max unqualified set A, for every two secrets $s_i, s_j \in S$ the probability of getting the same shares (for this specific set) should be equal. That is to say, for any two secrets $s_i, s_j \in S$ and projection of shares on A, $\vec{sh}'$ (some specific share that parties in A receive).

$$\sum_{\substack{all\ k\ for\ which\ the\ projection \\ of\ \vec{sh}_k\ on\ A\ is\ \vec{sh}'}} p_{ik} = \sum_{\substack{all\ k\ for\ which\ the\ projection \\ of\ \vec{sh}_k\ on\ A\ is\ \vec{sh}'}} p_{jk}$$

Reorganizing, we get.

$$\sum_{\substack{all\ k\ for\ which\ the\ projection \\ of\ \vec{sh}_k\ on\ A\ is\ \vec{sh}'}} p_{ik} - \sum_{\substack{all\ k\ for\ which\ the\ projection \\ of\ \vec{sh}_k\ on\ A\ is\ \vec{sh}'}} p_{jk} = 0 \qquad (13)$$

correctness: For any minimal qualified set A, for every two secrets $s_i, s_j \in S$ there are no share $\vec{sh}_k$ for which both p_{ik} and p_{jk} are not zero. That is to say, for every two secret $s_i \in S$ and projection of shares on A $\vec{sh}'$ (some specific share that parties in A receive), for each s_j so that $Pr(Sh(s_j, r)_A = \vec{sh}') = 0$

$$\sum_{\substack{all\ k\ for\ which\ the\ projection \\ of\ \vec{sh}_k\ on\ A\ is\ \vec{sh}' \\ and\ j \neq i}} p_{jk} = 0 \qquad (14)$$

By correctness, for each $\vec{sh}'$, there are at least $|S| - 1$ such j's.

probability restrictions: For any secret $\vec{s}_i \in S$

$$\sum_j p_{ij} = 1 \qquad (15)$$

That is to say, that for every secret the sum of all the probabilities to get any share is 1.Another constraint is for every i and j.

$$0 \leq p_{ij} \tag{16}$$

We stress that the privacy and probability restrictions follow from the requirements on any secret sharing scheme implementing $\mathcal{A}$. The correctness restrictions are constructed based on the concrete scheme $\mathcal{M}$.

The matrix M_1 defining our LP will be built from these three sets of equations 13, 14, 15, where the variables are the the p_{ij}-s. In addition we will remove all the rows that depend on other rows, so our matrix M_1 will have a full rank. Let us denote:

$$r = |S|SC \leq SC^2 \tag{17}$$

There are at most r columns in M_1 thus and at most r rows.[15]

This LP is solvable since $p_{\mathcal{M}}$ is a solution for it. The right hand side b is the vector obtained from Equations 13, 14, 15 $(0, 0, \ldots, 0, 1, \ldots, 1)$ (with $|S|$ 1's at the end).

Observation 1. *In the LP (M_1, b) above, all the entries in M_1 and in b are 1, -1 or 0.*

step 2: As mentioned above, any solution $\vec{p}'$ to the LP specified by (M_1, b) defines a secret sharing scheme for the desired access structure. The problem is that if the elements in $\vec{p}'$ will be not multiples of $Q^{-t'}$ for some t' it will be impossible to present this secret sharing scheme with polynomials over $\mathbb{F}_Q$. We know one solution $p_{\mathcal{M}}$ that has probabilities which are multiples of Q^{-t} for some, possibly very large, t (the one induced by $\mathcal{M}$). Now we want to show that there is $t' = SC^{\tilde{O}(SC^3)}$, for which there is solution p' to (M_1, b) where all probability $p_{i,j}$ are multiples of $Q^{-t'}$, which will prove the theorem. By theorem 11, there is a set of BFS's $G = \{p_1, ..., p_\ell\}$ for the system, so that there exists a solution (the one induced by $\mathcal{M}$) $p_{\mathcal{M}} \in CH(G)$.[16]. Next, we prove that the entries of all $p_i \in G$ are of "low" resolution, which implies Theorem 10 for $|G| = 1$, as p is already a multiple of Q^{-t}. More precisely, the following corollary of Lemma 4 holds.

Claim. For all $g \in G$, all entries of g satisfy $0 \leq g_i \leq 1/r^{2r}$.

Proof of Claim.

Proof. This follows from the fact that the BFS in G is of the form $M_{1,H}^{-1}b$, where $M_{1,H}$ is a subset of M_1's columns corresponding to an invertible (square) matrix so that the entries in b corresponding to the other columns are all 0's. As M_1, b have entries in $\{0, 1, -1\}$ by Observation 1, the claim follows from Lemma 4.

[15] The second inequality follows from correctness of the scheme.

[16] Note that (M_1, b)'s solution set is indeed bounded, as all coordinates of a solution p are in the range $[0, 1]$.

In fact, in the case of $|G| = 1$ we obtain a much better bound.

Thus, we assume from now on that $|G| \geq 2$. In particular, we may also assume that $|G| \leq r$, by the bound on the number of rows in M_1.

Let $G = [p_1| \ldots |p_\ell]$. The LP $([G, \mathbf{1}], (p_{\mathcal{M}}, 1))$ is solvable.[17]. Next, we observe that the system remains solvable if the right hand size is modified into any $b'_2 = (b', 1)$ so that b' remains within $CH(G)$. Any such b' is a feasible solution for the original LP (M_1, b).

The additional requirement we introduce is that all b''s components are multiples of $Q^{-t'}$ for a t' which is not too large.

In fact, we will drop the last equation and enforce it "manually", by only considering b''s in $CH(G)$. As a second step, we will make sure that among those, we pick one that also satisfies the second requirement. Let $(M'_2 = G, b')$ denote the LP induced by some $b' = p'$. In the next step we find the subset of $CH(G)$ that we will focus on.

step 3:

We rewrite (any) LP $(M'_2, b_2 = p)$ defined above to obtain an equivalent LP: A solution to the LP satisfies: $\sum_{i=1}^{\ell} \alpha_i = 1$.

So:

$$\begin{array}{l} \alpha_1 = 1 - \sum_{i=2}^{\ell} \alpha_i \\ \Updownarrow \\ p_1(1 - \sum_{i=2}^{\ell} \alpha_i) + \sum_{i=2}^{\ell} \alpha_i p_i = \vec{p} \\ \Updownarrow \\ \sum_{i=2}^{\ell} \alpha_i (p_i - p_1) = \vec{p} - p_1 \end{array}$$

Let us denote $\beta_i = \alpha_{i+1}$ for $1 \leq i \leq \ell - 1$. And we will receive a system of equations:

$$\begin{aligned} \sum_{i=1}^{\ell-1} \beta_i (p_{i+1} - p_1) &= \vec{p} - p_1 \\ 0 &\leq \beta_i \\ \sum_i \beta_i &\leq 1 \end{aligned} \tag{18}$$

step 4: The above system defines an LP with $M_2 = [p_2 - p_1| \, p_3 - p_1| \ldots| \, p_n - p_1]$ and $b_2 = p - p_1$. This LP, together with the constraint that $\sum_{i=1}^{\ell-1} \beta_i \leq 1$ and that $\beta_i \geq 0$ for all i is equivalent to the original one. Let us consider the LP (M_2, b_2), again deliberately leaving out the requirement of the coordinate sum being at most 1. As before we will take care of this requirement "manually". Also, there is no guarantee that $b_2 \geq 0$, but this can be taken care of by multiplying the rows corresponding to negative

[17] The additional row is to require the combination is a convex one.

b_2-coordinates by -1. Thus, we assume without loss of generality that (M_2, b_2) satisfies $b_2 \geq 0$. We will move back and forth between the two equivalent representations of the LP, dubbed β-representation $(M_2, b_2 - p_1)$ for the latter and the α-representation (M_2', b_2). They are equivalent in the sense that there exists a (simple) bijection between the solution sets of the two LP's (with the convexity requirement).

To find b' as we seek, let us consider the first $rank(M_2)$ rows of M_2 that are linearly independent. We denote the submatrix of M_2 restricted to these rows by M_3, and let b_3 denote the entries of b' corresponding to the selected rows in M_3. Similarly, we denote by G_3 the projeciton of G onto this set of coordinates. From Lemma 4 we know that all the denominators of all the entries in M_3 and b_3, $|b_{3,i}|$ are (reduced) fractions h/w with $w \leq r^{2r}$.

we show there exists a (not very small) $\epsilon > 0$, and point $p_3' \in CH(G_3)$ such that the $ball_\epsilon^\infty(p_3') \subseteq CH(G_3)$. In particular, all points p' corresponding to points in that ball are solutions to the original LP (M_1, b) (p_3' uniquely determines p'). Next, we provide a lower bound on the possible value of ϵ. This will require the following technical Lemma.

Claim. Let $A \in \mathbb{R}^{m \times m+1}$ denote a matrix whose set of columns has full affine dimension. Assume also that there exists an integer $M \in \mathbb{N}^+$ such that all coordinates in A satisfy $|A_{i,j}| = w/h \in [0,1]$ where w/h is a reduced fraction where $h \leq M$. Then there exists $\epsilon \geq 1/2m^m M^2$ and a point $p \in CH(cols(A))$ such that $ball_\epsilon^\infty(p) \subseteq CH(cols(A))$.

Proof. Denote $G = \{g_1, \ldots, g_{m+1}\}$ the set of points in G. Consider the point $p = g_1 + 0.5 \sum_{2 \leq i \leq m+1} (g_i - g_1)$. It is not hard to see that $CH(A)$ equals $\{g_1 + \sum_{i \in [m]} \alpha_i (g_{i+1} - g_1)\}_{\alpha \geq 0, \sum_{i \in [m]} \alpha_i \leq 1}$. Equivalently, $CH(A) = p + \{g_1 + \sum_{i \in [2,m+1]} \alpha_i (g_{i+1} - g_1)\}_{\alpha \geq 0, \sum_{i \in [m]} \alpha_i \leq 0.5}$. Next, by definition of affine dimension of the set $\{\Delta_i | \Delta_i = g_{i+1} - g_1 | i \in [m]\}$ is m. By the upper bound on the coordinates of the g_i's we have that each coordinate $\Delta_{i,j}$ satisfies $|\Delta_{i,j}| = w/h|$, where w/h is a reduced fraction where $h \leq M^2$. In particular, all entries are either 0 or at least $1/M^2$. Also, as the g_i's are all in $[0,1]$. Thus, for all $i, j \in [m]$ $|\Delta_{i,j}| \leq 1$. Let $B = [\Delta_1, \ldots, \Delta_m]$. We ask for which h, the unique solution x to the equation $Bx = h$ satisfies $\ell_\infty(x) \leq 0.5$. From the bound on the $|\Delta_{i,j}|$'s and Lemma 4, we have that $x = B^{-1}h \leq \ell_\infty(h) m^m \cdot M^2$. Thus, setting $\epsilon = \ell_\infty(h) = \frac{1}{2m^m M^2}$.

Moving from (M_3, b_3) back to the α-representation results in (M_3', b_3') of full affine degree (as M_3 is of full rank). Thus, from Claim 4.2 and Claim 4.2 we obtain a point p_3' and a hypercube with edge size $\epsilon = \frac{1}{2r^{3r}}$ around it so that for any $p_3'' \in ball_\epsilon(p_3')$ (M_3', p_3'') has a solution α satisfying $< 1, \alpha >= 1$. Moving back to the β-representation, the vector α translates into a solution β for the corresponding beta-representation $(M_3, b_3 = p_3'' - p_{1,3})$.[18] In particular, the set of vectors corresponding to the set of p'''s above is precisely $p' - p_1 + ball_\epsilon$. As $M_3 \in \mathbb{R}^{h \times h}$ (for some h) has degree h, it spans M_2. Thus, b_3 can be uniquely completed into a vector of full length $b' \in \mathbb{R}^r$ that falls into $CH(G)$.

[18] This notation means $p'' - p_1$, both restricted to the rows of M_3.

This is the case since $b_3 = M_3\beta$, but the other rows M_4 of M_2 (besides the last one) are spanned by the rows of M_3, as follows:

$$\forall(h < j \leq r)M_{2,j} = \sum_{i=1}^{h} k_{i,j}M_{3,1} \tag{19}$$

We denote this set of p'''s by

$$Good_1 = \{p''|p''_3 \in ball_\epsilon(p'_3)\}$$

Next, we show how to choose $p'' \in Good_1$ so that every coordinate of p'' is a multiple of $Q^{-t'}$ where t' is not very large.

step 5: In this step we characterize requirement (2) in a way that will help us find p'' satisfying the requirement.

As a recap on notation, $M_2 = (M_3, M_4)$, with corresponding $b_2 = (b_3, b_4)$.

A vector p so that the system $(M_2, b_2 = p - p_1)$ has a solution, iff p itself satisfies the following system of equations in the $p_{3,i}$'s (the β's have been eliminated). We find $p_3 \in CH(cols(M_3))$, so that the resulting p is a multiple of $Q^{-t'}$ for a relatively small t'.

$$p_j = p_{1,j} + \sum_{i=1}^{h} k_{i,j}(p_i - p_{1,i}) \qquad h < j \leq r \tag{20}$$

By similar reasoning to some previous arguments, we conclude that the denomenators of all coefficients involved in the above equation are not very large.

Observation 2. *In Equation 20, all coefficients $k_{i,j}, p_{1,i}, p_{1,j}$ are reduced fractions of the form w/h, where $h \geq r^{r^2+r}$.*

Proof. The observation for the $p_{1,i}, p_{i,j}$'s follows from Claim 4.2. For the $k_{i,j}$'s it follows from the fact that for each $j > h$, $k^j = (k_{1,j}, \ldots, k_{h,j})$ satisfies

$$k^j M_3 = M_{3,j}$$

Since all entires in M_3 are of the form $w/h \in [0, 1]$ with $h \leq r^r$. Thus, from Lemma 4, we conclude that the entries of k^j are reduced fractions with $h \leq r^{2r^2+r}$.

From the fact that we started from a given secret sharing scheme we know that system of equations 18 has solution $p_{\mathcal{M}}$ which all entries are multiplies of $Q^{t'}$ for some t that can be very big.

Let $M = Q^{\tilde{t}}R$ denote the common denominator of all coefficients of Equation 20, together with all denomenators of $p_{\mathcal{M}}$. Here R is coprime to Q.

Let us spell out the denominator and numerator of all coefficients in equation 20. We assume without loss of generality that each entry p_i of p is a multiple

of $Q^{-\tilde{t}}$, and its representation w/h as a fraction needs not be reduced. The denomenator of every other coefficient of the equation is a reduced w/h, where the highest divider of the form $Q^{t'}$ of such h satisfies $t' \leq \tilde{t}$. The assumption on the p_i's is indeed without loss of generality as we are looking for $Q^{\tilde{t}}$ which is up to $2^{poly(r)}$, so there is no problem going slightly beyond the existing coefficients, and expand the fraction by number $Q^{t'}$ (or even more if necessary).

Let $k_i^j = \tilde{k_i^j}/M$ a reduced fraction. Introducing similar notation for this and all other elements of the equation system we get.

$$\begin{aligned} \forall i \leq h \forall j > h \quad \tilde{k_i^j} = k_i^j M = \forall i \geq 1, \frac{b_i^j}{D_{i,j}^k} M \\ \forall i \geq 1 \quad \tilde{p_{1,i}} = p_{1,i} M = \frac{c_{1,i}}{D_{1,i}} M \\ \forall i \leq h \quad \tilde{p_i} = p_i M = \frac{l_i}{Q^{\tilde{t}}} M = l_i R \end{aligned} \tag{21}$$

Again, the fractions on the right in the first and second line are reduced.
When multiplying both sides of all the equations in 20 by M^2 we get:

$$l_j R M = \tilde{p_j} M = \tilde{p_{1,j}} M + \sum_{i=1}^{h} \tilde{k_i^j} (\tilde{p_i} - \tilde{p_{1,i}}) \tag{22}$$

And we already incorporated the requirements that p_i's for $i \leq h$ are multiples of $Q^{-\tilde{t}}$ into Equation 21 (third line). It remains to make sure that the $\tilde{p}_i$'s are such that $\tilde{p}_j$ for $j > h$ are as well multiples of $Q^{-\tilde{t}}$. This requirement is equivalent to the following modular system of equations modulo MR

$$\forall j > h, \tilde{p_{1,j}} M + \sum_{i=1}^{h} \tilde{k_i^j} (\tilde{p_i} - \tilde{p_{1,i}}) \equiv 0 \ (mod \ MR) \tag{23}$$

We already know that it has a solution (p).
If we denote $D' = lcm(\{D_{i,j}\} \cup \{D_{i,j}^k\})$ and $D = D'^2$ we can factor out $\frac{MR}{D}$:

$$\forall j > h, \frac{MR}{D} (c_{1,j} \frac{D}{D_{1,j}} Q^{\tilde{t}} + \sum_{i=1}^{h} (b_i^j \frac{D}{D_{i,j}^k} l_i - b_i^j c_{1,i} \frac{D}{D_{i,j}^k D_{1,i}} Q^{\tilde{t}})) \equiv 0 \ (mod \ MR) \tag{24}$$

The main observation that will be crucial in the sequel, is that the above system of equations is equivalent to the following system of equations modulo D.

$$\forall j > h \quad c_{1,j} \frac{D}{D_{1,j}} Q^{\tilde{t}} + \sum_{i=1}^{h} (b_i^j \frac{D}{D_{i,j}^k} l_i - b_i^j c_{1,i} \frac{D}{D_{i,j}^k D_{1,i}} Q^{\tilde{t}}) \equiv 0 \ (mod \ D) \tag{25}$$

Note that due to the choice of D all coefficients in this equations above are indeed integers [19]

step 6: So far, we have formulated the two requirements on p'' we are searching for.

1. p'' is in $Good_1$. This implies that the resulting p'' is a feasible solution to the original LP (M_1, b).
2. p'''s coordinates are all multiples of $Q^{-\tilde{t}}$.

Requirement (2) is taken care of by picking some $\tilde{t}$, and formulating a system of modular equations modulo M^2, where $M = Q^{\tilde{t}}R$. The crucial observation is that most of the components of this equation system are independent of the particular choice of $\tilde{t}$ (and thus M). First, indeed R depends on the vectors in G, and does not depend on the choice of M. In particular, the equivalent system of equations 25 modulo D, including the value of D and "almost" all coefficients of that equations are independent of D does not depend on $\tilde{t}$. [20]. The "almost" here is because $Q^{\tilde{t}}$ does depend on $\tilde{t}$ (while all other components like $c_{1,j}$, the $Dk_{i,j}$'s etc. do not).

Now, we know the system has a solution l (modulo D) for $M = Q^{\tilde{t}}R$. If we let $M = Q^{t'}R$ such that

$$Q^{t'} \equiv Q^{\tilde{t}}(\mod D)$$

This system would be solvable, since we know of a particular value $\tilde{t}$ leads to a solvable system. Thus, there exists a value v modulo D, so that system of Equations 25 is solvable if $Q^{\tilde{t}}$ is replaced with v. Now, clearly, there exists at least one value $t' = \tilde{t}$ such that $Q^{t'} \equiv v \mod D$. Now, there are two possible cases. There could be only one such value $t' = \tilde{t}$, which occurs only if $1 \notin \{Q^t \mod D | t \in \mathbb{N}\}$. In this case, we must have $\tilde{t} \leq D$ (by pegion hole principle). Otherwise, there are more than one suitable t'. In this case, there are in fact infinitely many such values t'

$$Good = \{a + iz \in \mathbb{N} | a \in [D], i \in \mathbb{N}, Q^z \equiv 1 \mod D\}.$$

satisfying this requirement. Similarly to the first case, $k \leq D$.

Let us obtain a gross upper bound on D.

$$D = lcm(\{D_{i,j}\} \cup \{D^k_{i,j}\}) \leq (r^{2r})^{r^2+r} = r^{O(r^3)}. \tag{26}$$

In the first case, we just learn that

$$\tilde{t} \leq D.$$

[19] E.g $\frac{D}{Dk_{i,j}D_{1,i}}$ is an integer - this "worst" case led us to choosing $D = D'^2$, rather than just $D = D'$.

[20] As mentioned before, we only assume that $Q^{\tilde{t}}$ is divisible by all Q-powers in all coefficients in Equation 25

So this bounds the randomness complexity of the scheme by $r^{O(r^3)} = SC^{O(SC^3)}$ elements over $\mathbb{F}_q$. This is (at least) double exponential in the share complexity $sc = \log_q(SC)$ in case the secret domain equals $\mathbb{F}_q$ (that is, $k = 1$).

In the second case, we pick some t' in *Good* that satisfies $t' = r^{O(r^3)}$. Consider a solution l to the set of modular equations 25. That is, any l such that all l_i's have the "right" values $(v_1, \ldots, v_h)$ modulo D. To satisfy the first requirement we want that $p''_3 = (l_1/Q^{t'}R, \ldots, l_h/Q^{t'}R) \in ball_\epsilon(p'_3)$. This can be done by adding multiples of D/M to any coordinate of to p'' (that is Dk/M for $k \in \mathbb{Z}$). In parituclar, we are allowed to move at most ϵ in each coordinate (in both directions) from p'_3 to stay inside $ball_\epsilon(p'_3)$. On the other hand, we would need to move from p'_3 by at most Q^D/M in each coordinate, to satisfy the constraint system 25.

We therefor require

$$Q^D/M \leq \epsilon \Leftrightarrow Q^{t'} \geq \frac{Q^D}{\epsilon R} \Leftrightarrow t' \geq \log_q(r^{O(r^3)}) = D + \tilde{O}(r^2) \tag{27}$$

Observation 2, also implies $Q^{t'} \geq r^{O(r^2)} \Rightarrow t' \geq \tilde{O}(r^2)$ suffices.

Overall, both the above restrictions allow to set $t' = r^{O(r^3)}$ for sufficiently large r.

Substituting back $r = O(|SC|^2)$, we get a bound of $SC^{\tilde{O}(SC^3)}$ on the (absolute) randomness complexity of a scheme equivalent to our original one.

As a simple corollary of the proof of Theorem 10, we obtain the following bound on the randomness complexity for general schemes.

Theorem 12. *Let $\mathcal{M} = (S, S_1 \times \ldots \times S_n, R, Sh, Dec)$ denote a (general) secret sharing scheme. Then, there exists an equivalent scheme $\mathcal{M}'$ over $\mathbb{F}_{Q^t}$ with the same share complexity SC, for which the (absolute) randomness complexity is at most $\tilde{O}(SC^2)$.*[21]

Proof sketch. Let $\mathcal{M}$ denote a scheme with parameters $S, S_1 \times \ldots \times S_n$ implementing an access structure $\mathcal{A}$. In a nutshell, we obtain the bound as we are only looking for a feasible solution for the LP (M_1, b), formulated based on S, $S_1 \times \ldots \times S_n$ (requirement (1)). But requirement (2), introducing restrictions on the form of the probabilities in D is not present - this allows to improve the randomness from exponential to polynomial in the share domain. Now, taking a BFS p of (M_1, b) we obtain a solution p with entries $p_i = w/h$ with $h \leq r^{2r}$. Thus, we may set $|R| \leq 1/h$, proving there exists a scheme $\mathcal{M}'$ induced by p with $rc(\mathcal{M}') = \log_2(2^{2r}) = \tilde{O}(SC^2)$.

[21] This holds even if we start from a general scheme where the randomness source of Sh is not necessarily uniform, and the resulting scheme samples randomness from a distribution U_R.

References

1. A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979. [Online]. Available: http://doi.acm.org/10.1145/359168.359176
2. G. R. Blakley, "One time pads are key safeguarding schemes, not cryptosystems fast key safeguarding schemes (threshold schemes) exist," in *Proceedings of the 1980 IEEE Symposium on Security and Privacy, Oakland, California, USA, April 14-16, 1980*. IEEE Computer Society, 1980, pp. 108–113. [Online]. Available: https://doi.org/10.1109/SP.1980.10016
3. M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract)," in *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, J. Simon, Ed. ACM, 1988, pp. 1–10. [Online]. Available: http://doi.acm.org/10.1145/62212.62213
4. J. C. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions," in *Advances in Cryptology - CRYPTO '88, 8th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1988, Proceedings*, ser. Lecture Notes in Computer Science, S. Goldwasser, Ed., vol. 403. Springer, 1988, pp. 27–35. [Online]. Available: https://doi.org/10.1007/0-387-34799-2_3
5. L. Csirmaz, "The size of a share must be large," in *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, ser. Lecture Notes in Computer Science, A. D. Santis, Ed., vol. 950. Springer, 1994, pp. 13–22. [Online]. Available: https://doi.org/10.1007/BFb0053420
6. B. Applebaum, A. Beimel, O. Farràs, O. Nir, and N. Peter, "Secret-sharing schemes for general and uniform access structures," Cryptology ePrint Archive, Report 2019/231, 2019, https://eprint.iacr.org/2019/231.
7. A. Beimel, "Secret-sharing schemes: A survey," in *Coding and Cryptology*, Y. M. Chee, Z. Guo, S. Ling, F. Shao, Y. Tang, H. Wang, and C. Xing, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 11–46.
8. A. Beimel and Y. Ishai, "On the power of nonlinear secret-sharing," *IACR Cryptology ePrint Archive*, vol. 2001, p. 30, 2001. [Online]. Available: http://eprint.iacr.org/2001/030
9. T. Liu, V. Vaikuntanathan, and H. Wee, "Towards breaking the exponential barrier for general secret sharing," in *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I*, ser. Lecture Notes in Computer Science, J. B. Nielsen and V. Rijmen, Eds., vol. 10820. Springer, 2018, pp. 567–596. [Online]. Available: https://doi.org/10.1007/978-3-319-78381-9_21
10. B. Applebaum and B. Arkis, "Conditional disclosure of secrets and d-uniform secret sharing with constant information rate," *IACR Cryptology ePrint Archive*, vol. 2018, p. 1, 2018. [Online]. Available: http://eprint.iacr.org/2018/001
11. A. Bogdanov, S. Guo, and I. Komargodski, "Threshold secret sharing requires a linear size alphabet," in *Theory of Cryptography - 14th International Conference, TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part II*, ser. Lecture Notes in Computer Science, M. Hirt and A. D. Smith, Eds., vol. 9986, 2016, pp. 471–484. [Online]. Available: https://doi.org/10.1007/978-3-662-53644-5_18

12. M. Karchmer and A. Wigderson, "On span programs," in *Proceedings of the Eigth Annual Structure in Complexity Theory Conference, San Diego, CA, USA, May 18-21, 1993*. IEEE Computer Society, 1993, pp. 102–111. [Online]. Available: https://doi.org/10.1109/SCT.1993.336536
13. A. Beimel, "Old Lower Bounds and New Upper Bounds for Secret Sharing Schemes," https://www.youtube.com/watch?v=tGGkDrWoq20&list=PLTIpfWOd7pE47DbiFs6nTRJAAINxm4gLo&index=4, 2019.
14. L. Babai, A. Gál, and A. Wigderson, "Superpolynomial lower bounds for monotone span programs," *Combinatorica*, vol. 19, no. 3, pp. 301–319, Mar 1999. [Online]. Available: https://doi.org/10.1007/s004930050058
15. A. Gàl, "A characterization of span program size and improved lower bounds for monotone span programs," *computational complexity*, vol. 10, no. 4, pp. 277–296, Dec 2001. [Online]. Available: https://doi.org/10.1007/s000370100001
16. A. Beimel and E. Weinreb, "Separating the power of monotone span programs over different fields," in *44th Symposium on Foundations of Computer Science (FOCS 2003), 11-14 October 2003, Cambridge, MA, USA, Proceedings*. IEEE Computer Society, 2003, pp. 428–437. [Online]. Available: https://doi.org/10.1109/SFCS.2003.1238216
17. A. A. Razborov, "Applications of matrix methods to the theory of lower bounds in computational complexity," *Combinatorica*, vol. 10, no. 1, pp. 81–93, 1990. [Online]. Available: https://doi.org/10.1007/BF02122698
18. T. Pitassi and R. Robere, "Lifting nullstellensatz to monotone span programs over any field," in *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, I. Diakonikolas, D. Kempe, and M. Henzinger, Eds. ACM, 2018, pp. 1207–1219. [Online]. Available: http://doi.acm.org/10.1145/3188745.3188914
19. A. Beimel, A. Ben-Efraim, C. Padró, and I. Tyomkin, "Multi-linear secret-sharing schemes," in *Theory of Cryptography*, Y. Lindell, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 394–418.
20. Y. Ishai and E. Kushilevitz, "Randomizing polynomials: A new representation with applications to round-efficient secure computation," in *41st Annual Symposium on Foundations of Computer Science, FOCS 2000, 12-14 November 2000, Redondo Beach, California, USA*. IEEE Computer Society, 2000, pp. 294–304. [Online]. Available: https://doi.org/10.1109/SFCS.2000.892118
21. ——, "Perfect constant-round secure computation via perfect randomizing polynomials," in *Automata, Languages and Programming, 29th International Colloquium, ICALP 2002, Malaga, Spain, July 8-13, 2002, Proceedings*, ser. Lecture Notes in Computer Science, P. Widmayer, F. T. Ruiz, R. M. Bueno, M. Hennessy, S. Eidenbenz, and R. Conejo, Eds., vol. 2380. Springer, 2002, pp. 244–256. [Online]. Available: https://doi.org/10.1007/3-540-45465-9_22
22. T. Liu, V. Vaikuntanathan, and H. Wee, "Conditional disclosure of secrets via non-linear reconstruction," in *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, 2017, pp. 758–790. [Online]. Available: https://doi.org/10.1007/978-3-319-63688-7_25
23. A. Beimel, Y. Ishai, R. Kumaresan, and E. Kushilevitz, "On the cryptographic complexity of the worst functions," in *Theory of Cryptography*, Y. Lindell, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 317–342.
24. A. Beimel, O. Farràs, Y. Mintz, and N. Peter, "Linear secret-sharing schemes for forbidden graph access structures," in *Theory of Cryptography - 15th*

International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part II, ser. Lecture Notes in Computer Science, Y. Kalai and L. Reyzin, Eds., vol. 10678. Springer, 2017, pp. 394–423. [Online]. Available: https://doi.org/10.1007/978-3-319-70503-3_13
25. R. Gay, I. Kerenidis, and H. Wee, "Communication complexity of conditional disclosure of secrets and attribute-based encryption," in *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*, 2015, pp. 485–502. [Online]. Available: https://doi.org/10.1007/978-3-662-48000-7_24
26. Y. Ishai and E. Kushilevitz, "Private simultaneous messages protocols with applications," in *Fifth Israel Symposium on Theory of Computing and Systems, ISTCS 1997, Ramat-Gan, Israel, June 17-19, 1997, Proceedings*. IEEE Computer Society, 1997, pp. 174–184. [Online]. Available: https://doi.org/10.1109/ISTCS.1997.595170
27. M. Hubenthal, "Maximal subspaces of zeros of quadratic forms over finite fields," 2006.
28. Y. Ishai and E. Kushilevitz, "Randomizing polynomials: A new representation with applications to round-efficient secure computation," in *41st Annual Symposium on Foundations of Computer Science, FOCS 2000, 12-14 November 2000, Redondo Beach, California, USA*. IEEE Computer Society, 2000, pp. 294–304. [Online]. Available: https://doi.org/10.1109/SFCS.2000.892118
29. R. K. Gupta, *Linear Programming*. Krishna Prakashan. [Online]. Available: https://books.google.co.il/books?id=Ur2vi5kB5IoC
30. M. Ito, A. Saito Nonmember, T. Nishizeki Member, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," vol. 72, pp. 56 – 64, 09 1989.
31. A. Healy, "Randomness-efficient sampling within nc^1," *Computational Complexity*, vol. 17, no. 1, pp. 3–37, 2008. [Online]. Available: https://doi.org/10.1007/s00037-007-0238-5
32. C. Blundo, A. G. Gaggia, and D. R. Stinson, "On the dealer's randomness required in secret sharing schemes," *Designs, Codes and Cryptography*, vol. 11, no. 3, pp. 235–259, Jul 1997. [Online]. Available: https://doi.org/10.1023/A:1008242111272
33. L. Csirmaz, "The dealer's random bits in perfect secret sharing schemes," 1994.
34. *41st Annual Symposium on Foundations of Computer Science, FOCS 2000, 12-14 November 2000, Redondo Beach, California, USA*. IEEE Computer Society, 2000. [Online]. Available: http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=7164

A Evidence of the Power of Multi-Linear Schemes

In this section we sketch the proof of Theorem 1.

Proof of Theorem 1. Here our starting point is the construction of [9] for a general access structure on n parties for $k = 1$. On a high level, their construction is a monotone formula with unbounded AND, OR gates, and additionally more complex gates for access structures that have secret sharing scheme based on a (h, n)-CDS with $h = \sqrt{n}$ and $n = O(\log(m))$. Their scheme now proceeds as in [30] to perform the sharing.

– The formula is evaluated recursively top-down. The secret is assigned to the top gate. Now, for an AND gate g' with an assigned label $s_{g'}$, each of its child gates g but the first one are assigned a fresh random bit r_g, and the last child gate is assigned $r_i \oplus \sum_{g>1} r_g$. That is, $s_{g'}$ is shared via (n,n)-threshold secret sharing. Similarly, an OR gate labeled by $s_{g'}$ passes this label to each of its children.
– In the CDS-based nodes always have a copy of all input wires entering it. Every such gate implements an access function $f' : \{0,1\}^m \to \{0,1\}$ implies by a $(n = O(\log m), h = O(\sqrt{n}))$-CDS for a certain predicate depending on f'. Here the best known scheme has complexity $2^{\tilde{O}(\sqrt{n})} = 2^{\tilde{O}((\log m)^{0.5})}$ per party. The scheme is implied by [22]'s MV-based general CDS. The construction of the secret sharing scheme from the CDS scheme for that particular type of f is a clever specialized transformation, and is not quite the straightforward generic construction of $m = O(n^{1/h}h)$ secret sharing from (n,h)-CDS, that in particular does not yield the types of schemes f that we need. In particular, several calls to the CDS are made by the sharing scheme, and the overhead over the share complexity of the CDS is therefor large relatively to the share complexity of CDS $n = O(\log m)$. Each CDS call yields CDS-shares for an input secret which is some linear combination over $\mathbb{F}_2$ of the original secret bit and random bits. Each of these shares is shared via a multi-linear scheme $\mathcal{A}$ among the parties (the CDS-shares are strings). The scheme has share complexity $O(n|s|)$, where s is the size of CDS shares, and such a scheme exists for all $|s| \in \mathbb{N}$. Also, the secret s itself is shared among certain subsets via Shamir secret sharing.
– Each party P_i is given the shares implied by the CDS scheme, and labels assigned to input wires b_i entering an AND or an OR gate.
– To reconstruct the secret, a set of parties evaluates it from the bottom up using the shares it holds, and learns the secret bit s iff the formula evaluates to 1.

This scheme results in information ratio $O(2^{0.994m})$ and $O(2^{0.999m})$ for general and linear secret sharing schemes respectively. This difference stems only from the differences in the best information ratio of known CDS protocols. This complexity is $2^{\tilde{O}(\sqrt{\log(m)})}$ for the best known general CDS and higher for linear secret sharing. Now, our main observation is that if the secret bit is replaced by a vector of elements of $\mathbb{F}_2$, the entire construction goes through, as AND gates can now be extended to use strings for masking, and OR gates just copy the share vector k. In leaf gates that can be implemented by reduction to CDS as above, we can replace the best known CDS implementation by an implementation with information ratio $O(1)$ for secrets of length $k = O(2^{2^n}) = 2^{m^{O(1)}}$. Now, that the CDS shares themselves are (multi) linear functions of the share elements (in $\mathbb{F}_2$) and random field elements, the shares resulting from this resulting are a composition of multi-linear schemes, resulting in a multi-linear scheme. Furthermore, the Shamir secret sharing, which is linear over $\mathbb{F}_{2^g}$ for a sufficiently large g (with $k = 1$!), can be viewed as a multi=linear scheme over $\mathbb{F}_2^g$. This can be seen by examining multiplication and even more easily addition over the field $\mathbb{F}^{2^g}$ - as

operations modulo n irreducible polynomial in $\mathbb{F}_2[x]$ of degree g. Analyzing the resulting sharing scheme, and the information ratio of the entire formula-based resulting construction, information ratio of at most $O(2^{0.994m})$ is obtained.[22]

B Motivation for the Framework and Future Work

Our long term goal is to put forward a useful and general framework for studying secret sharing schemes and their share complexity. We chose the setting of PSSS for reasons to be outlined below.

We believe this framework will prove useful due to the nice algebraic properties of (multi-variate) polynomials. First, any function $f : \mathbb{F}^t \to \mathbb{F}$ can be encoded as a multivariate polynomial $p(x_1, \ldots, x_t)$ over $\mathbb{F}$ (of degree at most $|\mathbb{F} - 1|(t-1)$, as a linear combination of Lagrange polynomials). Polynomials have additional nice mathematical properties, such as the Schwartz-Zippel theorem stating that polynomial's outputs don't have outputs with "too many" preimages, which could possibly come in handy, hopefully even in developing new methods for lower bounds on share complexity.

A statistical PSSS is a PSSS that allows some error ϵ in privacy and correctness. A moments' thought shows that such schemes are very general indeed. Any secret sharing scheme for sharing a single bit can be replaced by a statistical polynomial scheme over $\mathbb{F}_2$ with the same share complexity and only a small increase in randomness complexity[23].

This is done by sampling the randomness of the original scheme via a circuit (simple, $NC1$ [31] circuit) accepting a uniform vector $\mathbb{F}_2^m$ for some sufficiently large $m = O(\log(|R|) + k)$, treating it as an integer and reducing it modulo $|R|$ (where R is the original randomness domain sampled uniformly).

Then, to generalize to any share domain S, we can embed S in $\mathbb{F}_2^t$ for a sufficiently large t, and represent each share separately.

Although this leaves the question of perfect (the default) secret sharing open, the above observation implies this model is quite general indeed.

Two general questions are of interest:

Question 3. What is the largest gap between the best share complexity of a (perfect) polynomial scheme over some field $\mathbb{F}_q^k$ and the best share complexity for some access structure?

[22] We did not perform the full analysis, but the bound increases monotonously with the CDS complexity. Improved CDS complexity would imply a better bound on the share complexity of the resulting scheme.

[23] If the original scheme was perfect, its security degrades to statistical, though. Keep in mind that our primary goal is to obtain a framework that does not increase the best attainable share complexity beyond that of the "most general" framework as described below. In terms of feasibility for all monotone access structures, there exists a linear scheme over any finite field $\mathbb{F}$. The construction here is a straightforward generalization of [4]. That is, a polynomial scheme of degree 1 and $k = 1$ always exists. In fact, this particular scheme generalizes to any cyclic group $\mathbb{Z}_m$.

Question 4. Among polynomial schemes, how influential are various parameters on the achievable share complexity. In particular, all other parameters kept the same ($\mathbb{F}_q, k$), how much does increasing the degree of the polynomial, for starters, from the traditional value of 1 *to* $O(1)$ *affect share complexity. In particular, what can be said for degree* 2*?*

To the best of our knowledge, question 3, hasn't been looked at. And the trade-offs between different parameters of polynomial schemes have been (implicitly) studied (partially addressing question 4), as we discussed it in literature review. In this paper, we make some progress on the second question. We obtain results in two directions. One type of results refers to the share complexity of natural subclasses of polynomial schemes. Certain subclasses are shown to be too weak to implement most access structures (even regardless of share complexity). The second type of results deals with share complexity.

The most fundamental open question in our view, is whether there is a gap (say, for 1-bit secrets) in best share complexity between (generalized) polynomial schemes and non-polynomial schemes. We have suggested a candidate access structure, for which we conjecture a gap may exist.

Another fundamental question that remains open is whether there exists a degree > 2 PSSS of constant degree that has better sharing complexity than any multi-linear secret sharing scheme for some access structure and some fields.

As to schemes with $k = 1$ and constant field size, it is interesting to develop techniques for lower bounding share complexity of polynomial schemes of degree higher than 1.

Finally, for degree-1, it would be nice to generalize [18]'s lower bounds from the linear to the multi-linear setting. This goal seems quite achievable, and we conjecture that these lower bounds can indeed be transferred.

C Additional Previous Work - on Randomness Complexity of Secret Sharing

Another aspect of secret sharing that was studied is finding an upper and lower bounds on the randomness complexity that is needed to be used by the dealer for specific secret sharing scheme. It is easy to see that linear and multi-linear secret sharing schemes' randomness complexity is upper bounded by the share complexity. The gap in our knowledge about randomness complexity is regarding non-linear secret sharing schemes. [32] presents an upper bound for the randomness complexity for several classes of access structures. In addition they presented a lower bound when the graph is cycle C_n; when n is odd their bound is tight. The bounds are $O(\frac{n}{2}\log|S|)$ when n is odd and $O(\frac{n-1}{2}\log|S|)$ when n is even. Also, access structures on at most five participants are researched in [32], obtaining exact values for the dealer's randomness complexity for all access structures on at most four participants, and for all connected graphs on five vertices. Lower bound on randomness complexity for general access structures was presented in [33]. They have found an access structure for n participants

which obligates the dealer to use at least $n^2/\log(n)$ random bits for each secret bit. Pushing the lower bound of random complexity from, previously known, $O(n/\log(n))$ to $O(n^2/\log(n))$.