On Polynomial Secret Sharing Schemes

Anat Paskin-Cherniavsky[*] Radune Artiom[†]

June 2020

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, SC, may be suboptimal – there are access structures for which the gap between the best known lower bounds and best known multi-linear schemes is exponential.

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 $\vec{s}, \vec{r}$ respectively over some finite field $\mathbb{F}_q$. Our main hope is that the algebraic structure of polynomials would help obtain better lower bounds than those known for the general secret sharing. Some of the initial results we prove in this work are as follows.

On share complexity of polynomial schemes.
First we study degree (at most) 1 in randomness variables $\vec{r}$ (where the degree of secret variables is unlimited). We have shown that for a large subclass of these schemes, there exist equivalent multi-linear schemes with $O(n)$ share complexity overhead. Namely, PSSS where every polynomial misses monomials of exact degree $c \geq 2$ in $\vec{s}$ and 0 in $\vec{r}$, and PSSS where all polynomials miss monomials of exact degree ≥ 1 in $\vec{s}$ and 1 in $\vec{r}$. This translates the known lower bound of $\Omega(n^{\log(n)})$ for multi linear schemes onto a class of schemes strictly larger than multi linear schemes, to contrast with the best $\Omega(n^2/\log(n))$ bound known for general schemes, with no progress since 94'. An observation in the positive direction 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. For the next natural degree to consider, 2 in $\vec{r}$, we have shown that PSSS where all share polynomials are of exact degree 2 in $\vec{r}$ (without exact degree 1 in $\vec{r}$ monomials) where $\mathbb{F}_q$ has odd characteristic, can implement only trivial access structures where the minterms consist of single parties.

[*] Ariel University, Ariél, Israel. anatpc@ariel.ac.il. This work was supported by The Ariel Cyber Innovation Center in conjunction with the Israel National Cyber directorate in the Prime Minister's Office.

[†] Ariel University, Ariél, Israel and The Open University, Raanana, Israel. tom.radune@gmail.com

Obtaining improved lower bounds for degree-2 in $\vec{r}$ PSSS, and even arbitrary degree-1 in $\vec{r}$ PSSS is left as an interesting open question.

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, RC, bounded by $2^{poly(SC)}$. For general PSSS, we obtain a similar bound on RC (preserving SC and $\mathbb{F}_q$ but not degree). 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 as those for multi-linear schemes, and should be viewed as a proof of concept. If a much better bound for some degree bound $d = O(1)$ is obtained, it would lead directly to super-polynomial counting-based lower bounds for degree-d PSSS over constant-sized fields . Another application of low (say, polynomial) randomness complexity is transforming polynomial schemes with polynomial-sized (in n) algebraic formulas $C(\vec{s}, \vec{r})$ for each share , 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 [39] and Blakley [17] for threshold access structures, and was followed by thousands of works exploring the primitive itself, and its many applications found since. Quite early on [15,32] put forward a first construction realizing any monotone access structure. As a notable application, secret sharing is used as a key building block in various secure Multi-Party Computation (MPC) constructions [14, 23].

Arguably, the most important complexity measure of a secret sharing scheme is its share complexity (SC). 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 rate, 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 $\Omega(n/\log(n))$ [19], while the best known constructions for certain access structures have exponential complexity $O(2^{0.637n})$ [4]. In [19], 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 [19] is on information rate (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.[1]

In spite of extensive research attempting to improve [19]'s lower bound, the

[1] 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.

best known lower bound for general schemes has not improved since (even for implicit access structures). A major motivation for this work is the hope that departing from previous approaches relying mostly on information theoretic techniques, making use of algebraic techniques could potentially yield improved lower bounds for large classes of schemes, and hopefully eventually for general schemes. 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.

(Multi-)linear schemes. On the other hand, much more is known about the share complexity of the well studied family of linear secret sharing schemes, and more generally multi linear secret sharing 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 access structures, and recently, an exponential lower bound has been obtained on the share complexity of 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 complexity and information rate in secret sharing schemes, in this work, we continue the work of [11], which initiates a study of the power of non-linear secret sharing schemes. The main motivation in [11] 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 [11] 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 [11] 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 forward towards improved lower bounds for general schemes, 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 where the secret domain S is a subset of $\mathbb{F}^k$, rather than the entire set $\mathbb{F}^k$. We refer to such schemes as *generalized* polynomial schemes.

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 is that a secret sharing scheme is a randomized mapping $Sh : S \times R \to S_1 \times \ldots \times S_n$, rather than a deterministic function. In Sh, the randomness is uniformly sampled from a finite set R. Now observe that in any PSSS scheme $Sh' : \mathbb{F}_p^s \times \mathbb{F}_p^r$ over a finite field $\mathbb{F}_p$, the probability of outputting any share vector is a multiple of p^{-r}. The straightforward way to convert from Sh into an equivalent scheme Sh' as above is to embed S and R into $\mathbb{F}_p^s, \mathbb{F}_p^r$ for some s, r respectively, and evaluate the shares as polynomials corresponding to every share $Sh_i(s, r)$ (which are guaranteed to exist). More precisely, arbitrarily partition $\mathbb{F}_p^r$ into $|R|$ equal parts $R'_1, \ldots, R'_{|R|}$, the embedding labels every element of R'_j by r_j and sets Sh' accordingly. The problem with this approach in perfect secret sharing is that p^r may not be divisible by $|R|$ for any prime p and any r. For instance, for $|R| = 6$ in Sh there is no such embedding, as $1/6$ can not be written as $\frac{a}{p^r}$ for any prime p and $a \in \mathbb{N}$. We note that the above approach of transformation into PSSS (over any field $\mathbb{F}_p$) does work for statistical secret sharing, by choosing a sufficiently large r and R_j's of almost equal size, making the privacy 'leakage' arbitrarily small, and keeping correctness perfect. In this work we focus on the standard notion of perfect secret sharing schemes, though.

1.1 Our Results

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 per secret bit and over the same field exists.

Theorem 1.1. *(Informal) Let $\mathcal{M}$ be a PSSS of degree 1 in $\vec{r}$, where all share polynomials are either missing monomials of (exact) degree $c \geq 2$ in $\vec{s}$ and 0 in $\vec{r}$, or all share polynomials miss monomials of exact degree ≥ 1 in $\vec{s}$ and 1 in $\vec{r}$. Then there exists an equivalent multi linear scheme $\mathcal{M}'$ with share complexity at most n times that of $\mathcal{M}$.*

We conjecture that all schemes with $\vec{r}$-degree 1 are as weak as multi-linear schemes, and leave it as an interesting open problem. See Theorem 3.1 and Theorem 3.3 for a formal statement and a proof of the above theorem. The proofs of both theorems are constructive, transforming the r-degree 1 schemes into multi linear schemes. The validity of the constructions is proved by rather simple linear algebraic techniques, but the constructions themselves, especially that of Theorem 3.1 are somewhat surprising, in our opinion.

Moving to the next natural class of $\vec{r}$-degree 2, we show that a certain natural subclass of such PSSS only allows to implement a small subset of access structures (regradless of share complexity).

Theorem 1.2. *(Informal) PSSS of degree exactly 2 in $\vec{r}$ over fields of odd characteristic capture only access structures where all minterms are singletons.*

That is, somewhat intuitively, linear terms are required in degree-2 schemes for implementing useful access structures. The proof here relies on facts regarding the number of solutions of equations of the form $p(x_1, \ldots, x_n) = b$, where b is a quadratic form.

To contrast with the bounds in [31] on functions representable by polynomial-sized randomizing polynomials with r-degree 2 and any constant degree in s (over small fields), indicating the corresponding functions are relatively simple, falling in NC_3. The reason why their bound does not directly imply that PSSS of r-degree 2 and polynomial share complexity works for relatively simple schemes, is that their bound holds for representations polynomial in input size . In particular, they assume the randomness vector's size is polynomially bounded in the input vector's size. For PSSS with $poly(n)$ randomness and share complexity we could indeed obtain a similar bound on the type of access structures for which such PSSS exists. However, lacking bounds on the randomness complexity (see the following section), assuming only polynomial share complexity does not seem to suffice. [2]

On the positive side, we observe that a surprising recent result indicating all monotone access structures have a scheme construction share complexity $O(2^{0.994n})$ [36] 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 [2] with information rate O(1) for a certain class (not all) of access structures for a sufficiently large share domain.[3]

Observation 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 rate $O(2^{0.994n})$ per party. (in our language, degree-1 polynomial scheme over $\mathbb{F}_2$).*

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.

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

[2] Still, if we had polynomial in share complexity upper bounds on randomness complexity, a modification of [31]'s result would yield bounds on this type of limited constant degree PSSS which are stronger than just counting-based bounds for constant-degree PSSS given suitable bounds on randomness complexity. Namely, not only do access structures that cannot be implemented efficiently exist, but there are candidates in relatively low complexity classes (under standard assumptions).

[3] 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 [2]'s construction. The proof of the second is simple and appears below.

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 – $\mathrm{RC}(SC)$. 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 $\mathrm{RC}(SC)$. 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 secret sharing schemes as well as various types of PSSS.

Theorem 1.3. *(Informal) Let $\mathcal{M}$ be a secret sharing scheme. Then, there exists an equivalent scheme $\mathcal{M}'$ with the same share complexity SC and randomness $RC = 2^{poly(SC)}$ such that if $\mathcal{M}'$ is a PSSS of degree 2, then so is $\mathcal{M}'$, and if $\mathcal{M}$ is a PSSS then so is $\mathcal{M}$. Also, in the two latter cases, $\mathcal{M}$ and $\mathcal{M}'$ are defined over the same field.*

To prove the bound for degree-2 PSSS, we restate the privacy requirements into sets of equality of distributions restrictions for single polynomials obtained using a variant of Vazirani's XOR lemma (already satisfied by $\mathcal{M}$). In particular, we prove there exists a linear mapping from the vector space $span(r_1, \ldots, r_t)$ to a (much) smaller $span(r_1, \ldots, r_{t'})$ and every share polynomial $p(\vec{s}, \vec{r})$ is replaced by $p(\vec{s}, L(r_1), \ldots, L(r_n))$ so that privacy is still satisfied. The proof is based on a somewhat involved case analysis based on the theory on output distributions of quadratic forms. The bound for general secret sharing is proved using the following approach: given a PSSS scheme, we state the correctness and privacy requirements for any secret sharing scheme for the same access structure as an LP . Curiously, the LP formulation makes use of the scheme we already have at hand (with potentially high RC), rather than just a formulation of correctness and privacy. A solution to the LP determines the probabilities of mapping each secret s to each share vector $(\vec{\mathrm{sh}}_1,\ldots,\vec{\mathrm{sh}}_n)$, which easily extends into a PSSS over the same field and same share complexity. Briefly, the LP variables are probabilities $p_{i,k}$ where $\vec{s_i}$ is a secret and $\vec{sh_k}$ is a share vector. Privacy implies that for all maxterms A, and share vectors $\vec{\mathrm{sh}}_A$ it must hold that

$$\sum_{\substack{all\ k\ for\ which\ the\ projection\\ of\ \vec{sh}_k\ on\ A\ is\ \vec{sh}_A}} p_{i,k} - \sum_{\substack{all\ k\ for\ which\ the\ projection\\ of\ \vec{sh}_k\ on\ A\ is\ \vec{sh}_A}} p_{j,k} = 0.$$

From correctness, it follows that for every minterm A, for every value $\vec{\mathrm{sh}}_A$ all but at most $\vec{s}$, the projection value $\vec{\mathrm{sh}}_A$ is seen with probability 0. This constraint would result in a degree-2 inequality in the $p_{\vec{s},\vec{\mathrm{sh}}}$'s. To make it linear, the trick is to require that the 0 probabilities are exactly as in the scheme $\mathcal{M}$. That is, of every $(A,\vec{\mathrm{sh}}_A)$ we require: $\sum_{\substack{all\ k\ for\ which\ the\ projection\\ of\ \vec{sh}_k\ on\ A\ is\ \vec{sh}_A\\ and\ j\notin I}} p_{j,k} = 0$, where I is either $\{i\}$ for some i, or empty, and is fixed according to $\mathcal{M}$. Finally, the requirement that $(p_{i,1},\ldots,p_{i,l})$ is a probability vector is also expressed by linear inequalities. We look for solutions with small randomness vector length - as the LP has small integer entries, it easily follows that the probabilities are a multiple of some $1/L$, where L is not very large (exponential in LP dimensions). In particular, this implies a scheme with R of size L and same share complexity. This alone, already yields a bound on the randomness complexity $(\log(|R|))$ of general (perfect) secret sharing schemes. Given $\mathcal{M}$ is a PSSS, to obtain a PSSS with the required parameters it is necessary and sufficient that additionally the probabilities in the solution are powers of $q = |\mathbb{F}|$. We formally state both facts in Theorem A.8 and prove the theorem in Section A.

All of the bounds above are exponential in SC and may serve as a proof of concept. A strong motivation here is that good upper bounds on randomness complexity $\mathrm{RC}(SC)$ for constant-degree PSSS would lead to good existential bounds on the share complexity of such PSSS which we do not currently have (over small enough $\mathbb{F}$). More concretely, for constant $\mathbb{F}$ and $poly(SC)$ randomness complexity there exist access structures with share complexity $2^{\Omega(n)}$ of PSSS over $\mathbb{F}$.

We stress that all our upper bounds on randomness complexity are for *perfect* secret sharing schemes, and are therefore require new techniques even in the general secret sharing and unbounded degree PSSS settings. For general non-PSSS (or PSSS) statistically secure schemes, partial derandomization techniques from the literature can be applied. In more detail, for ϵ-statistical secret sharing, bounds of $\ell(h) = O(SC+\log\epsilon)$ on randomness complexity can be easily obtained by replacing the randomness with the output of a non-boolean PRG (nb-PRG) [20] against the sharing algorithm, mapping from $\ell(h)$ random bits to h random bits as used by the sharing algorithm. By standard analysis similar to that in the proof of Claim 2 in [5]'s full version, a random function from ℓ to h bits is a suitable nb-PRG. Such results however are not useful for lower bounds, however. It is unclear whether nb-PRGs can be applied to constant-degree PSSS to yield even statistical secret sharing schemes, as the resulting sharing scheme does not necessarily remain low-degree (as the nb-PRG itself may be of high degree). Thus, good lower bounds for low-degree PSSS even in the statistical setting are left as an interesting open problem.

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. In Section 3, we present our results on feasibility and share complexity. In Section A we prove out upper bounds on randomness complexity. The bound for degree-2 PSSS appears in Section A.1, and the result on general secret sharing schemes and general PSSS in Section A.2. Section D contains a broader survey of previous work from the perspective of PSSS implicit in it. Suggestions for future work appear in Section C.

1.2 Open questions

In this work we have obtained some preliminary results on PSSS but many fundamental questions remain open.

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

There exists certain evidence in the positive direction. In a nutshell, it considers secret sharing constructions based on large matching vectors families such as [35], which are known to exist over rings $\mathbb{Z}_m$ of composite size but provably do not exist when m is a prime.

Other interesting questions concern understanding the effect of various parameters of PSSS on their power, in terms of achievable share complexity and information rate. 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 rate. 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 the share complexity, and then rely on the fact that there are few different degree-d polynomials in $R + 1$ variables (exponentially many in the 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. $\log(|R|) \leq$ 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 $|\text{share complexity}|$, 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 $|R| \leq h(SC)$.*[4]

2 Preliminaries

General notation. In this work we consider finite fields $\mathbb{F}$. We write $\mathbb{F}_q$ to denote a field of size q (some prime power). For matrices M_1, M_2 (of the proper sizes) over some field $\mathbb{F}$, we denote by $(M_1|M_2)$ the matrix resulting from concatenating M_2 to the right of M_1, and $(M_1; M_2)$ results from concatenating M_2 below M_1. Vectors are denoted by $\vec{v}$ or just v when there is no risk of confusion (with scalars), and are by default column vectors. We let M_i denote the i'th row of M, and M^i its i'th column. We let M_I (M^I) denote a submatrix with rows (columns) restricted to I. For a matrix $M \in \mathbb{F}^{n \times n}$, we denote by $N \in \mathbb{F}^{m \times m}$ the matrix resulting from removing all row-column pairs such that $M^i = (M_i^T) = \vec{0}$.

Secret sharing. We use standard definitions of secret sharing schemes, following [7].

Definition 2.1. *[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 2.2. *[7] Distribution Scheme: Let S,$|S| \geq 2$ be a finite set of secrets. A secret sharing scheme with secrets domain S, is a tuple $\mathcal{M} =< Sh, \mu >$ where μ is a probability distribution over some finite set R (called the set of random strings) and Sh is a mapping from $S \times R$ to a set of n-tuples $S_1 \times S_2 \times \ldots \times S_n$, where S_j is called the domain of shares of p_j. For a set $A \subseteq \{p_1, \ldots, p_n\}$, we denote $Sh(s,r)_A$ as the restriction of $Sh(s,r)$ to its A-entries. Sh satisfies the following properties:*

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

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

We refer to sets in $\mathcal{A}$ as qualified, and to minimal qualified B in the sense that B is qualified and no $B' \subsetneq B$ is qualified as minterms of $\mathcal{A}$. We refer to maximal unqualified sets, in the sense that B is unqualified but for all $P_i \notin B$, $\{P_i\} \cup B$ is qualified as maxterms of $\mathcal{A}$.

***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 $a, b \in S$, and for every possible vector of shares $< \vec{sh}_j >_{p_j \in T}$:*

$$Pr[Sh(a,r)_T =< \vec{sh}_j >_{p_j \in T}] = Pr[Sh(b,r)_T =< \vec{sh}_j >_{p_j \in T}] \tag{2}$$

[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.

Observe that wlog., each share polynomial $q_{i,j}$ has free coefficient 0 (as any constant may be locally added by *Recon*). We will assume this implicitly throughout the paper.

Sometimes, we will be interested in ϵ statistical secret sharing, where ϵ error in correctness is allowed, and the distributions $Sh(a,r)_T$ and $Sh(b,r)_T$ are for unqualified T may be at statistical distance up to ϵ. Our default notion throughout the paper is that of perfect secret sharing as in Definition 2.2.

(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 $\vec{\mathrm{sh}}_i$ consists of g linear combinations $l_{i,1}(\mathrm{s}_1, \ldots, \mathrm{s}_k, r_1, \ldots, r_m) \ldots, l_{i,g}(\mathrm{s}_1, \ldots, \mathrm{s}_k, r_1, \ldots, r_m)$ over $\mathbb{F}$. The scheme is called linear if additionally $k = 1$.

Complexity measures of secret sharing schemes. The information rate, IR 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 $SC(\mathcal{M}) = \max_{i\in[n]} \log(|S_i|)$.

We denote the randomness complexity of a secret sharing scheme $\mathcal{M}$ by $\mathrm{RC}(\mathcal{M})) = \lceil \log_2(|R|) \rceil$ - the number of bits required to represent an element of R.

2.1 Polynomials over finite fields

In this work we focus on the set $\mathbb{F}_q[y_1, \ldots, y_n]$ of multivariate polynomials over finite fields. We say a polynomial $p(y_1, \ldots, y_n)$ is of degree i if all monomials in the polynomials have a cumulative degree of at most i. We say p has degree exactly i if all monomials in p are of cumulative degree exactly i. Similarly, for a subset $I \subseteq [n]$, we say p is of degree i in $x_I = \{x_j | j \in I\}$ if every monomial of p has cumulative degree at most i in the variables from x_I (similarly, for exact degree in x_I). In a finite field $\mathbb{F} = \mathbb{F}_{p^\ell}$, where p is prime, let $Tr_{\mathbb{F}}(\alpha) = \sum_{i=0}^{\ell-1} \alpha^{p^i}$ is the *trace* mapping from $\mathbb{F}$ to itself.[5]

2.1.1 Output distributions of degree-2 polynomials

Some of our results require some theory on degree-2 polynomials over finite fields. In particular, we will reduce understanding the output distributions of (various subclasses of) degree-2 PSSS to understanding the output distribution of a *single* degree-2 multivariate polynomial. For (any) polynomial in $p(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$, we let $N_{f,b}$ denote the number of solutions in $\mathbb{F}_q^n$ for the equation $f(x_1, \ldots, x_n) = b$. Polynomials in $\mathbb{F}[x_1, \ldots, x_n]_q$ where all monomials are of exactly degree 2, called *quadratic forms.* It is convenient to represent quadratic forms $f(x)$, by a matrix $A \in \mathbb{F}_q^{n\times n}$, where $f(x) = x^T Ax$. That is, $A_{i,j}$ is the coefficient of $x_i x_j$. We will need the following existing theory

[5] In fact, the image of $Tr_{\mathbb{F}}$ is always contained in $\mathbb{F}_p$.

characterizing $N_{f,b}$ for f which are quadratic forms over a finite fields, and general degree-2 polynomials over fields of characteristic 2. All required theory and discussions appears in chapter 6 in [34], and is included here for self containment. Also, some of the theorems we state here are straightforward corollaries of [34], but were not explicitly stated there.

Fields of odd characteristic. Fix some finite field $\mathbb{F}$ of odd charactersitic. We let η denote the quadratic character on $\mathbb{F}^*$. That is, $\eta(x) = 1$ if x is a quadratic residue modulo q, and -1 otherwise. We extend its definition to 0 via $\eta(0) = 0$.

We also let $\nu : \mathbb{F} \to \mathbb{Z}$ be $\nu(b) = -1$ for $b \in \mathbb{F}^*$, and $\nu(0) = q - 1$. Recall a quadratic form f over a characteristic field $\mathbb{F}$ in variables $x_1, \ldots, x_n$ is a polynomial where all monomials are of degree exactly 2. It is known that a quadratic form $f(x)$ in variables $x = (x_1, \ldots, x_n)$ has a representation of the form $f(x) = x^T C \cdot M_f \cdot C^T x$, where C is an invertible matrix in $\mathbb{F}^{n \times n}$, and $M_f \in \mathbb{F}_q^{n \times n}$ is diagonal, and all $rank(M_f)$ non-zero elements in the diagonal are at entries $M[i,i]$ for $i \leq rank(M_f)$. Such a representation M_f is called canonical. Here, M_f represents a quadratic form $p'(v) = v^T M_f v$ in a new vector $\vec{v} = (v_1, \ldots, v_n)$ of variables, obtained from $\vec{x}$ via $\vec{v} = C^T x$. The number $m \leq n$ of non-zero elements on M_f's diagonal is an invariant for all canonical representations of f. The function $\eta(det(M_f^-))$ is another invariant, independent of the concrete canonical representation M_f. (see Theorem 6.21 in [34] and discussion beforehand for more intuition). We denote the type of a quardatric form $f(x_1, \ldots, x_n)$ over $\mathbb{F}_q$ of odd characteristic as (n, m, η), where (m, η) are the corresponding values of the above invariants of equivalent canonical forms.

To understand the expression for $N_{f,b}$ for a quadratic form f, it suffices to understand $N_{g,b}$ for the quadratic form $g(v_1, \ldots, v_n)$ in a new vector of variables $v = (v_1, \ldots, v_n)$, where $g(v) = v^T M_f v$ where M_f is a canonical representation of a quadratic form, as $N_{f,b} = N_{g,b}$ for all $b \in \mathbb{F}_q$. We refer to such g as canonical forms. This holds as $v(x) = C^T x$ is a bijection between the domain of $f(x)$ and the domain of $g(v)$ satisfying $f(x) = g(v(x))$ for all $x \in \mathbb{F}_q^n$. We say that f is equivalent to a canonical form g as above. We define the *type* of a quadratic form $f(x_1, \ldots, x_n)$ of odd characteristic via the triple $(n, m, \eta(\text{det}))$ (with $m, \eta(det)$ invariants of canonical forms equivalent to f).

By the above discussion, we may assume wlog. that $n = m$, and calculate the number of roots in that case. In the general case of f of type (n, m, η), compute the number of roots for an equivalent canonical g of type $(n = m, m, \eta)$, and multiply by q^{n-m}.

The following theorem now follows directly by combining theorems 6.26, 6.27 from [34]. For a quadratic form $f(x)$ we denote the number of solutions to the equation $f(x) = b$ by $N_{f,b}$,

Theorem 2.1. *Let $p(x_1, \ldots, x_n)$ denote a quadratic form over a finite field $\mathbb{F}_q$ of odd characteristic of type (n, m, d). Consider a representation $f(x) = v^T M_f v$ as above, $x = (x_1, \ldots, x_n)$,and the v_i's are (independent, by choice of C) linear combinations of the x_j's. Then*

1. *If m is even, then for every $b \in \mathbb{F}$*

$$N_{f,b} = q^{n-m}(q^{m-1} + q^{(m-2)/2}\nu(b)\eta((-1)^{m/2})d).$$

2. If m is odd, for every $b \in \mathbb{F}$

$$N_{f,b} = q^{n-m}(q^{m-1} + q^{(m-1)/2}\eta(b(-1)^{m/2})d).$$

Following Theorem 2.1, we define the *type* of a quadratic form $f(x_1, \ldots, x_n)$ of odd characteristic via $(m, \det)$. Evidently, the type of f determines the distribution of $f(x)$ when x is picked uniformly from $\mathbb{F}^n$. Here we no longer assume $m = n$.

Fields of characteristic 2. Let $\mathbb{F}$ be a field of characteristic 2. Here we also have a canonical representation of quadratic forms, albeit somewhat less simple. Namely, for every quadratic form $f(x_1, \ldots, x_n)$, there exists a number $m \leq n$, and a non-signular matrix $C \in \mathbb{F}^{n \times n}$ such that $f(x) = x^T C M_f C^T x$, where M_f has one of the following forms:

1. (Type $T = 1$) m is even. M_f has 0's everywhere except for entries $M[2i-1, 2i]$ for $1 \leq i \leq m/2$ for some integer $m \leq n$, which are all 1.

2. (Type $T = 2$) m is even. M_f has 0's everywhere except for entries $M[2i-1, 2i]$ for all $1 \leq i \leq m/2$ for some integer $m \leq n$ which are 1, $M[m-1, m-1] = 1$, and $M[m, m] = a$, where $Tr_{\mathbb{F}}(a) = 1$.

3. (Type $T = 3$) m is odd. M_f has 0's everywhere except for entries $M[2i-1, 2i]$ for $1 \leq i \leq (m-1)/2$ which are all 1, and also $M[m, m] = 1$.

Similarly to the odd characteristic case, we refer to M_f as a canonical representation. By Theorem 6.30 in [34], the number m and T of the canonical M_f is and invariant depending only on f, and not on the particular representation f. Thus, we denote the type of a quadratic form $f(x_1, \ldots, x_n)$ as (n, m, T), according to n and the above invariants. For each type, and $b \in \mathbb{F}$, a characterization of $N_{f,b}$ for quadratic forms is known, as follows from Theorem 6.32 in [34].[6]

Theorem 2.2. *Let $p(x_1, \ldots, x_n)$ denote a quadratic form of type (n, m, T) over a finite field $\mathbb{F}_q$ of characteristic 2. Then*

1. If $T = 1$, for every $b \in \mathbb{F}_q$, $N_{f,b} = q^{n-m}(q^{m-1} + q^{(m-2)/2}\nu(b))$.

2. If $T = 2$, for every $b \in \mathbb{F}_q$, $N_{f,b} = q^{n-m}(q^{m-1} - q^{(m-1)/2}\nu(b))$.

3. If $T = 3$, for all $b \in \mathbb{F}_q$, $N_{f,b} = q^{n-1}$.

2.2 Polynomial Secret Sharing Schemes (PSSS)

In this work, we put forward a natural generalization of (multi)-linear secret sharing schemes - where shares are allowed to be general polynomials of $\vec{s}, \vec{r}$, rather than just linear combinations. Namely:

Definition 2.3 (PSSS:). *A polynomial secret sharing scheme (PSSS) $\mathcal{M} = (Sh, \mu)$ is a secret sharing scheme specified by $(\mathbb{F}, t, k, Sh)$ where $\mathbb{F}$ is a finite field, $S = \mathbb{F}^k$ is the domain of secrets, μ is uniform over $R = \mathbb{F}^t$, and $t, k \in \mathbb{N}^+$. The sharing function $Sh(\vec{s}; \vec{r})_i$ returns $(p_{i,1}(\vec{s}, \vec{r}), \ldots, p_{i,l_i}(\vec{s}, \vec{r}))$ as the i'th party's share, where each $p_{i,j}(\vec{s}, \vec{r})$ is a (multivariate) polynomial over $\mathbb{F}$.*

[6] The theorem applies to $m = n$, but reasoning similar to the odd characteristic case implies $N_{f,b}$ for general m, n as a simple corollary.

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 $\{\sum_{j\in[k]} a_j \mathrm{s}_j | a_j \in \mathbb{F}\}$, 1 encodes $\{a | a \in \mathbb{F}\}$. For a pair of regular expressions g_1, g_2; g_1^* encodes the set $\{p_1 \cdot \ldots \cdot p_h | h \in \mathbb{N}, \forall i \in [h], p_i \in g_1\}$; $g_1 + g_2$ 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 $g_1 \cdot \ldots \cdot g_1$ 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 $SC_{\mathbb{F}}(\mathcal{M}$ etc. (it always the case $IR_{\mathbb{F}}(\mathcal{M}) = IR(\mathcal{M})$, 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.[7]

A slightly more general notion of polynomial schemes is one where $S \subseteq \mathbb{F}^k$, rather than the entire set $\mathbb{F}^k$.[8] We refer to such schemes as *generalized* polynomial schemes.

3 On Feasibility and Share Complexity of PSSS

In the next two sections, we present our negative results. Our positive result on the power of multilinear schemes is a rather simple observation based on existing work, and is deferred to the full version.

3.1 Bounds on efficiency of degree 1 in r PSSS

We show that a large sub-class of polynomial schemes of degree at most 1 in r ($PSSS_{s^*\cdot r+s^*}$) 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 proves that $PSSS_{s^*\cdot r+s}$ can be replaced by a multi-linear scheme without any loss in parametres.

Theorem 3.1. *For every scheme $\mathcal{M} = (\mathbb{F}, t, k, Sh)$ in $PSSS_{s^*\cdot r+s}$, there exists a $PSSS_{s+r}$ scheme $\mathcal{M}' = (\mathbb{F}, t, k, Sh')$ for the same access structure and $\mathcal{A}$ with $SC(\mathcal{M}') = SC(\mathcal{M})$.*

Proof idea: Somewhat surprisingly, for any scheme $PSSS_{s+r,\mathbb{F}}$ we build an equivalent multi-linear scheme by replacing the coefficient polynomials of

[7] Note that some of the schemes appearing in [11] 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^k.

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

the r_i's in the shares (which have the form $p(s)$) by constants resulting from substituting an arbitrary fixed vector $s' \in S$ into the coefficients.

To prove this theorem, let us restate the sharing algorithm Sh more conveniently. For such a scheme, $Sh(s, r)$ can be represented as $Vs + Mr$, where $V \in \mathbb{F}^{a \times k}, M \in \mathbb{F}[\mathrm{s}_1, \ldots, \mathrm{s}_n]^{a \times t}$. Here each entry of M is a formal polynomial $p_{i,j}$ in s, a the total number of polynomials in the share vector, and V a constant. M_s is a shorthand for $M(s)$ - substituting a concrete value s as the secret vector, into the matrix of polynomials.

A function $\rho : \{1, ..., a\} \longrightarrow \{p_1, ..., p_n\}$ labels each row by a party, so that party P_i receives the shares corresponding to rows $H_i = j|\rho(j) = i$. For a set A of parties, we abbreviate the submatrix pf M involved in generating A's shares on secret vector s (aka $\cup_{i \in A} H_i$) as $A_s = (V_A | M_{s,A})$.

Claim 3.2. *Let $\mathcal{M} = \{\mathbb{F}, t, k, (V|M)\}$, in $PSSS_{s^* r + s, \mathbb{F}}$, be a secret sharing scheme for an access structure $\mathcal{A}$. The scheme $\mathcal{M}'$ where M is substituted by a constant matrix $M_{\vec{s_1}}$ for some fixed secret $\vec{s_1}$ is a (multi-linear) secret sharing scheme for the same access structure.*

Proof. Fix some secret vector $\vec{\mathrm{s}_1}$ as in the statement of the claim. We prove the scheme remains valid.

Correctness: Consider any $\vec{\mathrm{s}_0} \in \mathbb{F}^k$. Now we will look at authorized set A. Let us look at the two share distributions $(V_A | A_{\vec{\mathrm{s}_1}}) \cdot (\vec{\mathrm{s}_1} | \vec{r_1})$ and $(V_A | A_{\vec{\mathrm{s}_0}}) \cdot (\vec{\mathrm{s}_0} | \vec{r_0})$ of secrets $\vec{\mathrm{s}_1}$ and $\vec{\mathrm{s}_0}$, where $\vec{r_1}, \vec{r_0} \in \mathbb{F}^t$ are independent random vectors. The correctness of $\mathcal{M}$ is equivalent to stating that for all pairs $\vec{r_0}, \vec{r_1}$, we have:

$$\begin{gathered}(V_A | A_{\vec{\mathrm{s}_1}}) \cdot (\vec{\mathrm{s}_1} | \vec{r_1}) \neq (V_A | A_{\vec{\mathrm{s}_0}}) \cdot (\vec{\mathrm{s}_0} | \vec{r_0}) \\ \Downarrow \\ V_A \cdot (\vec{\mathrm{s}_0} - \vec{\mathrm{s}_1}) \neq A_{\vec{\mathrm{s}_1}} \cdot \vec{r_1} - A_{\vec{\mathrm{s}_0}} \cdot \vec{r_0}.\end{gathered} \tag{3}$$

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

$$V_A \cdot (\vec{\mathrm{s}_0} - \vec{\mathrm{s}_1}) \neq A_{\vec{\mathrm{s}_1}} \cdot \vec{r_1} \tag{4}$$

for all $\vec{r_1}$. Due to the fact that Equation 4 is correct for any $\vec{\mathrm{s}_0} \in \mathbb{F}^k$ and by the structure of the secret domain, for any two distinct secret vectors $\vec{\mathrm{s}_2}, \vec{\mathrm{s}_3} \in \mathbb{F}^k$ there exists $\vec{\mathrm{s}_0}$ for which $\vec{\mathrm{s}_2} - \vec{\mathrm{s}_3} = \vec{\mathrm{s}_0} - \vec{\mathrm{s}_1}$. From equation 4:

$$V_A \cdot (\vec{\mathrm{s}_2} - \vec{\mathrm{s}_3}) \neq A_{\vec{\mathrm{s}_1}} \cdot r_1 \tag{5}$$

For all $\vec{r_1} \in \mathbb{F}^t$. Let $\vec{r_2}, \vec{r_3} \in \mathbb{F}^t$. Writing $\vec{r_1} = \vec{r_3} - \vec{r_2}$ we conclude that (as r_1 in Equation 5 is arbitrary),

$$\begin{gathered}V_A \cdot (\vec{\mathrm{s}_2} - \vec{\mathrm{s}_3}) \neq A_{\vec{\mathrm{s}_1}} \cdot \vec{r_1} \\ \Downarrow \\ (V_A | A_{\vec{\mathrm{s}_1}}) \cdot (\vec{\mathrm{s}_2} | \vec{r_2}) \neq (V_A | A_{\vec{\mathrm{s}_1}}) \cdot (\vec{\mathrm{s}_3} | \vec{r_3})\end{gathered} \tag{6}$$

Which is precisely the definition of correctness for the new scheme (as $\vec{r_2}, \vec{r_3}, \vec{\mathrm{s}_2} \neq \vec{\mathrm{s}_3}$ are otherwise arbitrary).

Privacy: Consider some secret $\vec{\mathrm{s}_0} \neq \vec{\mathrm{s}_1} \in \mathbb{F}^k$. 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:

$$\begin{gathered}(V_A | A_{\vec{\mathrm{s}_1}}) \cdot (\vec{\mathrm{s}_1} | \vec{r_1}) = (V_A | A_{\vec{\mathrm{s}_0}}) \cdot (\vec{\mathrm{s}_0} | \vec{r_0}) \\ \Downarrow \\ V_A \cdot (\vec{\mathrm{s}_0} - \vec{\mathrm{s}_1}) = A_{\vec{\mathrm{s}_1}} \cdot \vec{r_1} - A_{\vec{\mathrm{s}_0}} \cdot \vec{r_0}\end{gathered} \tag{7}$$

In particular this is true for $\vec{r_0} = \vec{0}$. Then for any $\vec{\mathrm{s}_0}$ there exists $\vec{r_1} \in \mathbb{F}^t$ for which:

$$V_A \cdot (\vec{\mathrm{s}_0} - \vec{\mathrm{s}_1}) = A_{\vec{\mathrm{s}_1}} \cdot \vec{r_1} \tag{8}$$

Let $\vec{\mathrm{s}_2}, \vec{\mathrm{s}_3}$ denote a pair of secrets. Fix $\vec{\mathrm{s}_0}$ for which $\vec{\mathrm{s}_2} - \vec{\mathrm{s}_3} = \vec{\mathrm{s}_0} - \vec{\mathrm{s}_1}$. From 8 it follows there exists $\vec{r_1}$ for which:

$$V_A \cdot (\vec{\mathrm{s}_2} - \vec{\mathrm{s}_3}) = A_{\vec{\mathrm{s}_1}} \cdot \vec{r_1} \tag{9}$$

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

$$\begin{gathered}V_A \cdot (\vec{\mathrm{s}_2} - \vec{\mathrm{s}_3}) = A_{\vec{\mathrm{s}_1}} \cdot r_1 \\ \Downarrow \\ V_A \cdot (\vec{\mathrm{s}_2} - \vec{\mathrm{s}_3}) = A_{\vec{\mathrm{s}_1}} \cdot (\vec{r_3} - (\vec{r_3} - \vec{r_1})) \\ \Downarrow \\ (V_A | A_{\vec{\mathrm{s}_1}}) \cdot (\vec{\mathrm{s}_2} | \vec{r_3} - \vec{r_1}) = (V_A | A_{\vec{\mathrm{s}_1}}) \cdot (\vec{\mathrm{s}_3} | \vec{r_3})\end{gathered} \tag{10}$$

We prove that this implies privacy. Picking $\vec{r_3}$ at random, the vector $\vec{r_3} - \vec{r_1}$ is a random vector as well. Thus, the left hand size, where $\vec{r_3}$ is picked at random is distributed precisely as the shares seen by A when sharing $\vec{\mathrm{s}_2}$ in $\mathcal{M}'$. This value is uniform over the affine subspace $V_A\vec{\mathrm{s}_2} + \mathrm{colSpan}(A_{\vec{\mathrm{s}_1}})$. Similarly, the right hand side is also a random element of an affine subspace of the form $V_A\vec{\mathrm{s}_3} + \mathrm{colSpan}(A_{\vec{\mathrm{s}_1}})$, and is distributed precisely as a share of $\vec{\mathrm{s}_3}$ seen by A at M'. By Equation 10, these affine subspaces intersect, so they must be the same subspace, since both are cosets of $\mathrm{colSpan}(A_{\vec{\mathrm{s}_1}})$. This concludes the proof. □

Next, we prove that a $PSSS_{s^*+r}$ scheme can be replaced by a multi-linear scheme up to a small loss in rate due to a small reduction in the dimension k of the secret space. Here, it will be convenient to specify $Sh(s,r)$ by a pair $(v(s), M)$, where $v(s) = (v_1(\mathrm{s}), \ldots, v_\ell(\mathrm{s}))$ is a vector of (multivariate) polynomials in s, and M is a constant matrix, and

$$Sh(s,r) = Mr + \sum_{i \in [k]} \mathrm{s}_i \frac{v^{(i)}}{\mathrm{s}_i}(s) = Mr + v(s) \tag{11}$$

Such an expression exists as we assume all share polynomials have a non-zero free coefficient. Here every $v^{(i)}(s)$ is a vector of formal polynomials, comprised of sums of all monomials in v in which s_i's degree is at least 1, and that were not included in $v^{(j)}$ for $j < i$ (we construct the $v^{(i)}$'s iteratively, starting from $i = 1$).[9] In this representation, s_i appears only in $v^{(j)}$ with $j \leq i$. We will sometimes denote Sh in $PSSS_{s^*+r}$ schemes as a pair (v, M) as above.

Theorem 3.3. *For every scheme $\mathcal{M} = (\mathbb{F}, t, k, (v, M))$ in $PSSS_{s^*+r}$ there exists a multilinear scheme $\mathcal{M}' = (\mathbb{F}, t, k - n, Sh)$ for the same access structure $\mathcal{A}$ with share complexity $SC(\mathcal{M}') \leq n \cdot SC(\mathcal{M})$.*

[9] Unlike in the previous section, it is more convenient to denote the formal polynomial vector by v, rather than v_s, in analog to M_s in the previous section, to simplify notation. We let $v(s)$ denote the evaluation of v on a specific vector s.

Proof. We construct a multi-linear scheme $\mathcal{M}' = (\mathbb{F}, t, k', (V'|M))$, by constructing a basis B for V''s column space, where $Sh(s,r) = (V'|M)(s,r)$ is the sharing algorithm of the multi-linear scheme (note V' here is constant). By Equation 11, for $s' = \vec{0}$, the distribution of $Sh(s',r)$ is therefor uniform over the zero coset of $Mr = \mathit{colSpan}(M)$. We conclude the following:

Claim 3.4. *For all $s' \in \mathbb{F}^k$ and every unqualified A, the vector $v_A(s')$ is in $\mathit{colSpan}(M_A)$.*

Proof of claim. To see this, consider a representation of Sh as in Equation 11 of the form $Sh(\mathrm{s}', r) = Mr + v(\mathrm{s}')$ as above. Let v_A denote v restricted to entries held by A. We have $v_A(0, \mathrm{s}'_2, \ldots, \mathrm{s}'_k) = v_A(\mathrm{s}') - v_A^{(1)}(\mathrm{s}')$ (since only $v_A^{(1)}$ depends on s_1). Since by privacy of $\mathcal{M}$ both $v_A(s')$ and $v_A(0, s'_2, \ldots, s'_k)$ must belong to $\mathit{colSpan}(M_A)$ (as this holds for $s' = \vec{0}$), so does $v_A^{(1)}(s')$. Since s' is arbitrary, we conclude that $s''_1 v_A^{(1)}(s'')$ is in $\mathit{colSpan}(M_A)$ for all $s' = s''$. Now, comparing $Sh(s',r)$ and $s'' = (s'_1, 0, s'_3, \ldots, s'_k)$, by similar reasoning to the above, we conclude that $v_A^{(2)}(\mathrm{s}')$ is also $\vec{0}$ in $\mathbb{F}^{\#_{rows}(M_A)}/\mathit{colSpan}(M_A)$. This follows from the fact that $v_A^{(j)}$'s for $j > 2$ are independent of s_2, and the fact that $v_A^{(1)}(\mathrm{s}')$ and $v_A^{(1)}(\mathrm{s}'')$ are 0 in $\mathbb{F}^{\#_{rows}(M_A)}/\mathit{colSpan}(M_A)$ as we proved before, so it does not effect the coset. Similarly to the case of $j = 2$, by induction on j we can prove that $v_A^{(j)}(s')$ equals $\vec{0}$ in $\mathbb{F}^{\#_{rows}(M_A)}/\mathit{colSpan}(M_A)$. Now, as $v_A(s') = \sum_i v_A^{(i)}(s')$, it also equals $\vec{0}$, as required. □

From Claim 3.4, it follows that taking any V' with columns in $\mathit{span}(\{v(s')|s' \in \mathbb{F}^k\}$, $(V'|M)$ immediately satisfies privacy. We will indeed pick our basis B out of $\mathit{span}(\{v(s')|s' \in \mathbb{F}^k\}$, so we will only need to worry that the resulting scheme satisfies correctness. The construction is as follows.

1. Initialization: Initialize $B = \phi$ (recall $\mathit{span}(B)$ 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 $\mathbb{F}^{\#_{rows}(M_A)}/\mathit{colSpan}(M_A)$ that differs from coset(v) for all $v \in \mathit{span}(B)$. Halt if no such s exists. If it does, add one such V^s to B.

We prove by induction that at the end of every iteration $i \leq max(1, k-n)$, we B is a size-i independent set in $\mathbb{F}^{\#_{rows}(M)}$ such that $(B|M)(s,r)$ is correct for $\mathcal{A}$ with secret domain $S = \mathbb{F}^i$ (and private, which we observed before).

First, observe that the above procedure will yield at least a single vector. For every $s' \neq \vec{0}$, and every minterm A, $v_A(s')$ is non zero in $\mathbb{F}^{\#_{rows}(M_A)}/\mathit{colSpan}(M_A)$ by correctness of $\mathcal{M}$. Now, any product $\alpha\vec{s'}$ for $\alpha \in \mathbb{F}$ will yield a different coset in $\mathbb{F}^{\#_{rows}(M_A)}/\mathit{colSpan}(M_A)$, as v_A is non-zero. Thus, we can add $v_s(s')$ to our set. By the inductive hypothesis, at the end of iteration i, we have $|\mathbb{F}|^i$ vectors already in $\mathit{span}(B)$ - for clarity, denote B at the end of iteration i by $B^{(i)}$. We observe that for every minterm A all projections $v_A(s')$ are distinct for different values s' - which follows from correctness of $\mathcal{M}$. Therefor, going over all A's, at most

$$(\text{number of minterms})|\mathbb{F}|^i \leq 2^n|\mathbb{F}|^i \leq |\mathbb{F}|^{i+n}$$

vectors are excluded as candidates for the next $v_s(s')$ to join B. Finally, by the condition imposed on the new vector to join B, it follows that $B^{(i+1)}$ is a size-$i+1$ independent set, as satisfies that $(B|M)$ is correct for secret domain $S = \mathbb{F}^{i+1}$ (the formal argument is similar to the base case, observing that $v_A(s')$ is non-zero as a coset of $(M_A|B_A^{(i)})$). As there are $|\mathbb{F}|^k$ vectors in $\mathcal{M}$'s domain to begin with, we conclude (from the proof of the inductive step above) that at least $k-n$ iterations can be made before running out of vectors to add, which concludes the proof. □

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

In this section we will show that if the shares are from the class $PSSS_{s^*+s^*r^2}$ (no r-degree 1 part) captures only the access structures consisting of a set of singletons as its minterms.[10]

Theorem 3.5. *Let $\mathbb{F}$ be a finite field of odd characteristic. Then the class $PSSS_{s*+s*r^2,\mathbb{F}}$ can only implement a simple set of access structures where its minterms are all singletons.*

Indeed, observe that we can not expect a similar result for all fields, as for $\mathbb{F}_2$, for instance, we have $r_i^2 = r_i$, so one can represent any multi linear scheme over $\mathbb{F}_2$ as a $PSSS_{s*+s*r^2,\mathbb{F}}$ scheme, by replacing every variable r_i by r_i^2, which are equal over $\mathbb{F}_2$. However, linear schemes over $\mathbb{F}_2$ do capture all monotone access structures (e.g, via the formula-based construction of [16]). See 2 for required background and notation on quadratic forms.

Furthermore, we have

Observation 3. *Let $f_1(x_1,\ldots,x_n), f_2(x_1,\ldots,x_n)$ be two quadratic forms over a field $\mathbb{F}_q$ of odd characteristic of (possibly same) types $(n_1,m_1,d_1),(n_2,m_2,d_2)$ respectively. Then for all $b \in \mathbb{F}-\{0\}$, $Pr_{x\leftarrow\mathbb{F}^n}(f_1(x)=0) \neq Pr_{x\leftarrow\mathbb{F}^n}(f_2(x)=b)$.*

The observation follows by simple case analysis. In some more detail, by Theorem 2.1, $N(f_1(x=0))$ is either a single q^x or of the form $q^{x_1} \pm q^{x_2} \pm q^{x_3}$ for $x_1 > x_2 > x_3$, while for $b \neq 0$, $N(f_2(x=b))$ is of the form $q^{x_1} \pm q^{x_2}$ for $x_1 > x_2$. So, the probabilities (after dividing both numbers by q^n) must differ. This is regardless of the values of m_1, m_2.

Now, consider a party P_h that receives a share of the form

$$f(\vec{s},\vec{r}) = p(\vec{s}) + \sum_{\substack{i,j\in\{1,..,n\}\\ i\leq j}} p_{i,j}(\vec{s})r_ir_j = p(\vec{s}) + q_{\vec{s}}(\vec{r}).$$

where each $q_{\vec{s}}(\vec{r})$ is a polynomial in $\vec{r}$ with coefficients in the ring $\mathbb{F}_q[s_1,\ldots,s_n]$, and $p(\vec{s})$ is non constant over $\mathbb{F}_q^n$. First consider the case when $p(\vec{s})$ is non-constant over $\mathbb{F}_q^n$. We prove that there exists a pair of secrets $\vec{s_1},\vec{s_2}$ that P_h can distinguish by itself. To see this, fix two vectors $\vec{s_1},\vec{s_2}$ such that $p(\vec{s_1}) \neq p(\vec{s_2})$. By observation 3, it directly follows that the unique probability (over the choice of $\vec{r}$) of $f(\vec{s_1},\vec{r})$ hitting $p(\vec{s_1})$ equals the probability of $q_{\vec{s_1}}(r)$ hitting 0, while the probability of hitting values $b \neq p(\vec{s_1})$, equals the probability of $q_{\vec{s_1}}(r)$ hitting corresponding non-zero values (indeed, adding a constant permutes the distribution). A similar situation occurs with $f(\vec{s_2},\vec{r})$ and the 'spacial' point $p(\vec{s_2})$. Thus, the points with the 'special 0-probability for the $q_{\vec{s_i}}$-part' for $\vec{s_1}$

[10] Note that our results only rule out perfect schemes.

and $\vec{s_2}$ differ for $f(\vec{s_1}, \vec{r})$ and $f(\vec{s_2}, \vec{r})$. We conclude that the two distributions $f(\vec{s_1}, r), f(\vec{s_2}, r)$ are distinct. To see this, note that the contribution of $b = p(\vec{s_1})$ to the statistical distance between $f(\vec{s_1}, r)$ and $f(\vec{s_2}, r)$ is $1/2|Pr[q_{\vec{s_1}}(\vec{r}) = 0] - Pr[q_{\vec{s_2}}(\vec{r}) = p(\vec{s_1}) - p(\vec{s_2})]|$, which is non-zero by Observation 3.

Finally, let us look at all the remaining parties with only shares where $p(\vec{s})$ is constant (zero, wlog. since the free coefficient is 0). Such parties receive only shares of the form $f(\vec{s}, \vec{r}) = q_{\vec{s}}(\vec{r})$, where every $q_{\vec{s}}$ is a quadratic form. Therefore, for any $\vec{s} \in S$ we have $f_p(\vec{s}, \vec{0}) = 0$. Thus, all these parties together can not reconstruct the secret with probability 1, implying that the singletons above are the only minterms of the access structure. □

References

[1] *41st Annual Symposium on Foundations of Computer Science, FOCS 2000, 12-14 November 2000, Redondo Beach, California, USA*. IEEE Computer Society, 2000. URL: https://ieeexplore.ieee.org/xpl/conhome/7164/proceeding.

[2] Benny Applebaum and Barak Arkis. Conditional disclosure of secrets and d-uniform secret sharing with constant information rate. *IACR Cryptology ePrint Archive*, 2018:1, 2018. URL: http://eprint.iacr.org/2018/001.

[3] Benny Applebaum, Amos Beimel, Oriol Farràs, Oded Nir, and Naty Peter. Secret-sharing schemes for general and uniform access structures. Cryptology ePrint Archive, Report 2019/231, 2019. https://eprint.iacr.org/2019/231.

[4] Benny Applebaum, Amos Beimel, Oded Nir, and Naty Peter. Better secret-sharing via robust conditional disclosure of secrets. *Electronic Colloquium on Computational Complexity (ECCC)*, 27:8, 2020. URL: https://eccc.weizmann.ac.il/report/2020/008.

[5] Benny Applebaum and Prashant Nalini Vasudevan. Placing conditional disclosure of secrets in the communication complexity universe. In Avrim Blum, editor, *10th Innovations in Theoretical Computer Science Conference, ITCS 2019, January 10-12, 2019, San Diego, California, USA*, volume 124 of *LIPIcs*, pages 4:1–4:14. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2019. doi:10.4230/LIPIcs.ITCS.2019.4.

[6] László Babai, Anna Gál, and Avi Wigderson. Superpolynomial lower bounds for monotone span programs. *Combinatorica*, 19(3):301–319, Mar 1999. doi:10.1007/s004930050058.

[7] Amos Beimel. Secret-sharing schemes: A survey. In Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang, Huaxiong Wang, and Chaoping Xing, editors, *Coding and Cryptology*, pages 11–46, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[8] Amos Beimel. Old Lower Bounds and New Upper Bounds for Secret Sharing Schemes. https://www.youtube.com/watch?v=tGGkDrWoq20&list=PLTIpfWOd7pE47DbiFs6nTRJAAINxm4gLo&index=4, 2019.

[9] Amos Beimel, Aner Ben-Efraim, Carles Padró, and Ilya Tyomkin. Multi-linear secret-sharing schemes. In Yehuda Lindell, editor, *Theory of Cryptography*, pages 394–418, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

[10] Amos Beimel, Oriol Farràs, Yuval Mintz, and Naty Peter. Linear secret-sharing schemes for forbidden graph access structures. In Yael Kalai and Leonid Reyzin, editors, *Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part II*, volume 10678 of *Lecture Notes in Computer Science*, pages 394–423. Springer, 2017. `doi:10.1007/978-3-319-70503-3_13`.

[11] Amos Beimel and Yuval Ishai. On the power of nonlinear secret-sharing. *IACR Cryptology ePrint Archive*, 2001:30, 2001. URL: `http://eprint.iacr.org/2001/030`.

[12] Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions. In Yehuda Lindell, editor, *Theory of Cryptography*, pages 317–342, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

[13] Amos Beimel and Enav 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*, pages 428–437. IEEE Computer Society, 2003. `doi:10.1109/SFCS.2003.1238216`.

[14] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In Janos Simon, editor, *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 1–10. ACM, 1988. URL: `http://doi.acm.org/10.1145/62212.62213`, `doi:10.1145/62212.62213`.

[15] Josh Cohen Benaloh and Jerry Leichter. Generalized secret sharing and monotone functions. In Goldwasser [24], pages 27–35. `doi:10.1007/0-387-34799-2_3`.

[16] Josh Cohen Benaloh and Jerry Leichter. Generalized secret sharing and monotone functions. In Goldwasser [24], pages 27–35. `doi:10.1007/0-387-34799-2\_3`.

[17] 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*, pages 108–113. IEEE Computer Society, 1980. `doi:10.1109/SP.1980.10016`.

[18] Andrej Bogdanov, Siyao Guo, and Ilan Komargodski. Threshold secret sharing requires a linear size alphabet. In Martin Hirt and Adam D. Smith, editors, *Theory of Cryptography - 14th International Conference, TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part II*, volume 9986 of *Lecture Notes in Computer Science*, pages 471–484, 2016. `doi:10.1007/978-3-662-53644-5\_18`.

[19] László Csirmaz. The size of a share must be large. In Alfredo De Santis, editor, *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, volume 950 of *Lecture Notes in Computer Science*, pages 13–22. Springer, 1994. doi:10.1007/BFb0053420.

[20] Bella Dubrov and Yuval Ishai. On the randomness complexity of efficient sampling. In Jon M. Kleinberg, editor, *Proceedings of the 38th Annual ACM Symposium on Theory of Computing, Seattle, WA, USA, May 21-23, 2006*, pages 711–720. ACM, 2006. doi:10.1145/1132516.1132615.

[21] Ana Gàl. A characterization of span program size and improved lower bounds for monotone span programs. *computational complexity*, 10(4):277–296, Dec 2001. doi:10.1007/s000370100001.

[22] Romain Gay, Iordanis Kerenidis, and Hoeteck Wee. Communication complexity of conditional disclosure of secrets and attribute-based encryption. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 485–502. Springer, 2015. doi:10.1007/978-3-662-48000-7_24.

[23] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred V. Aho, editor, *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA*, pages 218–229. ACM, 1987. doi:10.1145/28395.28420.

[24] Shafi Goldwasser, editor. *Advances in Cryptology - CRYPTO '88, 8th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1988, Proceedings*, volume 403 of *Lecture Notes in Computer Science*. Springer, 1990. doi:10.1007/0-387-34799-2.

[25] R. K. Gupta. *Linear Programming*. Krishna Prakashan. URL: https://books.google.co.il/books?id=Ur2vi5kB5IoC.

[26] Alexander Healy. Randomness-efficient sampling within nc^1. *Computational Complexity*, 17(1):3–37, 2008. doi:10.1007/s00037-007-0238-5.

[27] Yuval Ishai and Eyal 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*, pages 174–184. IEEE Computer Society, 1997. doi:10.1109/ISTCS.1997.595170.

[28] Yuval Ishai and Eyal 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* [1], pages 294–304. doi:10.1109/SFCS.2000.892118.

[29] Yuval Ishai and Eyal 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* [1], pages 294–304. `doi:10.1109/SFCS.2000.892118`.

[30] Yuval Ishai and Eyal Kushilevitz. Perfect constant-round secure computation via perfect randomizing polynomials. In Peter Widmayer, Francisco Triguero Ruiz, Rafael Morales Bueno, Matthew Hennessy, Stephan Eidenbenz, and Ricardo Conejo, editors, *Automata, Languages and Programming, 29th International Colloquium, ICALP 2002, Malaga, Spain, July 8-13, 2002, Proceedings*, volume 2380 of *Lecture Notes in Computer Science*, pages 244–256. Springer, 2002. `doi:10.1007/3-540-45465-9_22`.

[31] Yuval Ishai, Eyal Kushilevitz, and Anat Paskin-Cherniavsky. From randomizing polynomials to parallel algorithms. In Shafi Goldwasser, editor, *Innovations in Theoretical Computer Science 2012, Cambridge, MA, USA, January 8-10, 2012*, pages 76–89. ACM, 2012. `doi:10.1145/2090236.2090244`.

[32] Mitsuru Ito, Akira Saito Nonmember, Takao Nishizeki Member, Akira Saito, and Takao Nishizeki. Secret sharing scheme realizing general access structure. 72:56 – 64, 09 1989.

[33] Mauricio Karchmer and Avi Wigderson. On span programs. In *Proceedings of the Eigth Annual Structure in Complexity Theory Conference, San Diego, CA, USA, May 18-21, 1993*, pages 102–111. IEEE Computer Society, 1993. `doi:10.1109/SCT.1993.336536`.

[34] Rudolf Lidl and Harald Neiderreiter. *Introduction to finite fields and their applications.* Cambridge University Press, 1997.

[35] Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Conditional disclosure of secrets via non-linear reconstruction. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, volume 10401 of *Lecture Notes in Computer Science*, pages 758–790. Springer, 2017. `doi:10.1007/978-3-319-63688-7\_25`.

[36] Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Towards breaking the exponential barrier for general secret sharing. In Jesper Buus Nielsen and Vincent Rijmen, editors, *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*, volume 10820 of *Lecture Notes in Computer Science*, pages 567–596. Springer, 2018. `doi:10.1007/978-3-319-78381-9_21`.

[37] Toniann Pitassi and Robert Robere. Lifting nullstellensatz to monotone span programs over any field. In Ilias Diakonikolas, David Kempe, and Monika Henzinger, editors, *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA,*

June 25-29, 2018, pages 1207–1219. ACM, 2018. URL: `http://doi.acm.org/10.1145/3188745.3188914`, `doi:10.1145/3188745.3188914`.

[38] Alexander A. Razborov. Applications of matrix methods to the theory of lower bounds in computational complexity. *Combinatorica*, 10(1):81–93, 1990. `doi:10.1007/BF02122698`.

[39] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979. URL: `http://doi.acm.org/10.1145/359168.359176`, `doi:10.1145/359168.359176`.

A On the randomness complexity of polynomial schemes

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

A.1 Bounding the Number of Random Variables in Quadratic Secret Sharing Schemes

Theorem A.1. *For any scheme $\mathcal{M} = (\mathbb{F}_q, t, k, Sh) \in PSSS_{s*+r^2+rs+r}$ for an access structure $\mathcal{A} \subseteq 2^{[n]}$ there exists a scheme $\mathcal{M}' = (\mathbb{F}_q, t', k, Sh') \in PSSS_{s*+r^2+rs+r}$, with the same share complexity, where $t' \leq 2^{\tilde{O}(SC(\mathcal{M}))}$.*

The proof idea is to replace the space $\mathbb{F}^t$ from which the random variables in $\mathcal{M}$ are sampled with a carefully chosen subspace $A \subseteq \mathbb{F}^t$ in such a way that if we sample our input $\vec{r}$ to the share polynomials of the original scheme from this smaller space, the privacy and correctness will be preserved. Preservation of correctness is immediate, since correctness was originally perfect. Thus A will be determined using only the privacy requirement. We will build such a subspace iteratively adding vectors to a basis. More precisely, we set a linear mapping L from the $\mathbb{F}_q$-vector space $V_{r,t} = span(1, r_1, \ldots, r_t)$, where the formal variables $1, r_1, \ldots, r_t$ are viewed as vectors, to the $\mathbb{F}_q$-vector space $V_{\tilde{r}} = span(1, \tilde{r}_1, \ldots, \tilde{r}_{t'})$ where $t' << t$ is to be fixed later. To obtain Sh', we replace every share polynomial $p_{i,j}(\vec{s}, r_1, \ldots, r_t)$ output by Sh by the polynomial $p_{i,j}((\vec{s}, L(r_1), \ldots, L(r_t)))$, resulting in a degree-2 polynomial in $\vec{s}, \vec{\tilde{r}}$, where $\vec{\tilde{r}}$ is of length only t'. We set $L(1) = 1$.[11] For a subset $A \subseteq V_{r,t}$, we denote $L(A) = \{L(a) | a \in A\}$. For a subset $I \subseteq [t']$, Define by $V_{\tilde{r},I} = span(\{\tilde{r}_i | i \in I\})$. For a linear subspace $\tilde{V} \subseteq V_{\tilde{r},t'}$ we let $\mathbf{proj}_{\tilde{V}}(x)$ return the projection of $x \in V_{\tilde{r},t'}$ onto $\tilde{V}$ (a similar notion will occasionally be used for any linear space and a subspace thereof).

Before we prove the above theorem, we start with some notation and more technical observations about degree-2 polynomials.

Observation 4. *Let $p(r) = r^2 + ar + c$ be a univariate degree-2 polynomial over $\mathbb{F}_q$ of characteristic 2. Denote $q = 2^l$. Then if $a = 0$, the output distribution of the random variable $p(r)$, where r is sampled uniformly from $\mathbb{F}_q$ is uniform over $\mathbb{F}_q$. Now consider $\mathbb{F}_q$ as a $\mathbb{F}_2$-vector space of dimension l. If $a \neq 0$ $p(r)$*

[11] We added 1 to the vector spaces to simplify the proof, $L(1)$ is not directly used by Sh' above.

is uniform over a coset of a linear subspace B of $\mathbb{F}_q$ of dimension $l-1$. B is determined only by a.

Proof. The observation is proved by noticing that $p'(r) = p(r) - c$ is a linearizing polynomial, satisfying $p'(x+y) = p'(x) + p'(y)$, and only $\{0, a\} = span(\{a\})$ are 0's of the polynomials, and thus equal the kernel of p as a linear mapping. Thus, $Image(p')$ is uniform over a subspace B of dimension $l-1$ if $a \neq 0$, otherwise the mapping p', and also p is a bijection. For $a \neq 0$, $Image(p)$ is uniform over $B + c$, which equals B iff. $c \in B$. Indeed, $B = Image(p')$ depends only on a, as $Kernel(p')$ depends only on k. □

Lemma A.2. *Consider a degree 2 polynomial $p(\vec{r}) = f_p(\vec{r}) + l_p(\vec{r})$ where $\vec{r} \in \mathbb{F}_q^n$. Then there exists an affine transformation $H : \mathbb{F}^n \to \mathbb{F}^n$, such that $H(\vec{r}) = C\vec{r'} + \vec{b}$ where C is non-singular such that the following holds (we thereby refer to this transformation as a non-singualr affine transfomration).*[12] *Let $p(H(r)) = p'(r'_1, \ldots, r'_n)$ where $p'(\vec{r'}) = f_{p'}(r'_1, \ldots, r'_m) + l_{p'}(r'_m, r'_{m+1}, \ldots, r'_n) + a_{p'}$ for some $m \leq n$, and $f_{p'}$ is a canonical quadratic form. Additionally, if r'_m has a non-zero coefficient in $l_{p'}$, then $\mathbb{F}_q$ has characteristic 2, and $f_{p'}(\vec{r'})$ is of type $(n, m, T = 3)$.Furthermore, C depends only on f_p. We refer to p' as above as a canonical degree-2 polynomials (generalizing the concept of a canonical quadratic form), and we say p is equivalent to p' when a transformation H as above exists.*

We extend the notion of a type of quadratic forms to general canonical p' as in Lemma A.2. For a canonical $p'(\vec{r'}) = \sum_{i<j} a'_{i,j} r'_i r'_j + \sum_i a'_i r'_i + a'_p$ as in Lemma A.2, let (n, m, d) or (n, m, T) (according to the parity of the characteristic of $\mathbb{F}_q$) denote the type of $f_{p'}$. Let $l_{p'} = \sum_{i=m}^t a'_i r'_i$ we denote $mask_{p'}(\vec{r'}) = \sum_{i=m+1}^t a'_i < \alpha'_i, \vec{r} >$ if $a'_i > 0$ for some $i > m$. In this case, we say p' is of lin0. Otherwise, if $f_{p'}$ is of type $(n, m, T = 3)$ we let $mask_{p'}(\vec{r'}) = a'_{m,m}(< \alpha'_m, \vec{r} >)^2 + a'_m < \alpha'_m, \vec{r} >$, in this case we say the polynomial is of type lin1 if $a'_m = 0$, and type lin2 otherwise. Otherwise, we let $mask_{p'}(\vec{r'}) = 0$ and refer to the polynomial as of non-linear type. For convenience, we unify the types of odd characteristic and characteristic 2 and denote the type by a 5-tuple $(\mathbb{F}_q, n, m, y, b)$, where $\mathbb{F}_q$ is the field over which p is defined, y is either d or T depending on whether $\mathbb{F}_q$ has characteristic 2. The part states linearly. If p' is lin0 or lin1, $b = 0$ or $b = 1$ respectively. Otherwise, for lin3 (happens only together with $T = 3$), apply Observation 4 to $r_m^2 + br_m + a_{p'}$. Then $b = (3, B, b')$, where B is the linear subspace in Observation 4 (specified by $l-1$ field elements which are a basis of B), $b' = 0$ if the coset supporting the output distribution of $r_m^2 + br_m + a_{p'}$ contains $\vec{0}$. Finally, for non-linear type polynomials, $b = 3$. Indeed, the type of any degree-2 p is well-defined as:

Observation 5. *For a degree-2 polynomial $p(r_1, \ldots, r_n)$, all canonical polynomials $p'(r'_1, \ldots, r'_n)$ equivalent to p are of the same type $(\mathbb{F}_q, n, m, y, b)$.*

The proof of Observation 5 is a direct corollary of the following observation and the fact that the transformation from $p(\vec{r})$ to a canonical polynomial $p'(\vec{r'})$ preserves the output distribution.

[12] More precisely, we view this transformation as mapping from $\mathbb{F}_q$-linear spaces spanned by the formal variable sets $\{r_1, \ldots, r_n\}$ and $\{r'_1, \ldots, r'_n\}$ respectively.

Observation 6. *Let $p_1(r'_1,\dots,r'_n), p_2(r'_1,\dots,r'_n)$ be a pair of canonical polynomials. Then their output distributions (for $\vec{r'}$ uniformly sampled from $\mathbb{F}_p^n$) are equal iff. they are of the same type.*

We will need the notion of an *almost canonical* polynomial. We say a degree-2 polynomial $p(\vec{r}) = f_p + l_p + a_p$ is *almost canonical* if $f_p(\vec{r})$ if it is obtained from a canonical polynomial $p'(\vec{r'})$ of type $(\mathbb{F}_q, n, m, y, b)$ by replacing each r'_i by an affine combination $\sum_{j\in[n]} \alpha_{i,j} r_j + b_i =< \alpha_i, \vec{r} > +b_i$, where all $< \alpha_i, \vec{r} >$'s are all linearly independent elements of $V_{r,t}$. (equivalently, by replacing $\vec{r'}$ by $\vec{r}$ obtained from $\vec{r'}$ by means of a non-singular affine mapping $\vec{r'} = H' \cdot \vec{r} + \vec{b'}$). If the $< \alpha_i, \vec{r} >$'s are not necessarily linearly independent, we say p is *somewhat canonical.* For a somewhat (almost) canonical p, we refer to $p(\vec{r'})$ as the associated canonical polynomial for p. For (any) quadratic form $p(\vec{r})$, we denote by *span*(p) the set $\{l_{f_p(r_1+\Delta_1,\dots,r_n+\Delta_n)} \in V_{r,n} | \Delta \in \mathbb{F}_q^n\}$.

We have the following characterization of the 'linearity status' b in the type of *almost canonical* polynomials.

Lemma A.3. *Let $p(r_1,\dots,r_n)$ be an* almost canonical *polynomial, with an associated canonical polynomial $p'(\vec{r'})$ of type $(\mathbb{F}_q, n, m, y, b)$. Then, the (partial) type of p as a polynomial in $\vec{r}$ satisfies:*

1. *p is of type lin0 iff. $l_p(\vec{r})$ is not spanned by $r'_1,\dots,r'_m$ (all as elements of $V_{r,n}$). Equivalently, $l_p(\vec{r})$ is not in span(p).*[13]
2. *p is lin1 iff. char$(\mathbb{F}_q) = 2, y = 3$ and l_p is spanned by $\{r'_1,\dots,r'_{m-1}\}$.*
3. *p is lin2 iff. char$(\mathbb{F}_q) = 2, y = 3$, and l_p is spanned by $r'_1,\dots,r'_{m-1},r'_m$, but not by $r'_1,\dots,r'_{m-1}$*
4. *p is non-linear type iff. it satisfies none of the conditions above.*

The proof of the lemma is not hard, and makes observations along the lines of the proof of Lemma A.2.

Proof of lemma A.2 First, let $\vec{r} = C\vec{r''}$ where C is non-singular, and $f_p(r) = \vec{r''}^T M_{f_{p''}} \vec{r''}$, where $f_{p''}$ is a canonical quadratic form of type (t, m, T). Now, substituting $\vec{r} = C^{-1}\vec{r''}$ into $l_p(\vec{r}) + a_p$ we obtain $l_{p''}(\vec{r''}) + a_{p''}$, we obtain $p(\vec{r}) = p''(\vec{r''})$ (as formal polynomials) where $f_{p''}$ is a canonical quadratic form. Next, we divide the analysis according to characteristic of $\mathbb{F}_q$. We start with charactersitic 2. We iteratively transform $\vec{r''}$ into $\vec{r'}$ via non-singular affine transformations as above starting from $p''(\vec{r'})$ resulting in $p'(\vec{r'})$ with the required properties. The composition of the trasnformation above from $\vec{r}$ to $\vec{r''}$ with these transformations will result in a non-singular affine transformation $\vec{r} \to \vec{r'}$. Each transformation will not change $f_{p''}$ (keeping it canonical), and remove one variable from the $l_{p''}$ part. Let i denote the highest index among $[m]$ where $a_i r''_i$ in $l_{p''}$ has a non-zero a_i. For simplicity of notation, we will refer to the polynomials after each transformation as p'', and to its variable vectors as $\vec{r''}$ (rather than a new set of variables as results after each transformation). If no such i exists, we are done. Otherwise, there are several cases.

case 1: Assume $1 \le i \le m-2$. (Regardless of T type of $f_{p''}$.) assume $f_{p''}(\vec{r''}) = r''_1 r''_2 + ... + r''_i r''_{i+1} + \dots$. Let $\vec{r''} = H(\vec{r'})$ ($\vec{r'}$ is the new vector of

[13] It is not necessarily equivalent for somewhat canonical polynomials p.

variables for the resulting polynomial) be $r''_{i+1} = r''_{i+1} + a$ and $r''_j = r'_j$ otherwise. Then in $p'(H(r'))$ the coefficient of r'_i is $ar'_i + ar'_i = 0$. By maximality of i, $a_{p'} = a_{p''}$. Also, $f_{p'} = f_{p''}$. Similarly, if $f_{p''} = r''_1 r''_2 + ... + r''_{i-1} r''_i + \ldots$, we set $r''_{i-1} = r'_{i-1} + a$ and $r''_j = r'_j$ otherwise. As before, the coefficient of r'_i becomes 0, $f_{p'}$ remains unchanged and the free coefficient possibly changes.

case 2: Assume $i = m - 1$ 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.

Similarly to the previous case, if $i = m-1$ we set H so that $\vec{r''}_{i+1} = \vec{r''}_{i+1} + 1$. This keeps $f_{p''}$ unchanged, cancels r'_i and does not add new linear terms. In particular, note that br''^2_m does not contribute to the linear part $l_{p'}$, as $2ab = 0$ in $\mathbb{F}_q$. The free coefficient changes by ba^2 due to br''^2_m's contribution. A similar transformation (letting $r''_{m-1} = r'_{m-1} + a$) works for $i = m$.

case 4: Assume $i = m$ for type 3. In this case do noting.

In all cases, proceed to eliminating the next largest ar'_i in p' (to which we now refer as p''), if exists. The process takes at most m steps until terminating. After the above procedure terminates, it is easy to see that there is either no intersection in the variables appearing in $f_{p'}$ and $l_{p'}$, or they only have only r'_m in common, in which case $f_{p''}$ is of type $(t, m, T = 3)$.

Next, we move to odd characteristic, where the situation is quite simple. Starting from $p''(\vec{r''})$ above, where $f_{p''} = a_{1,1} r''^2_1 + a_{2,2} r''^2_2 + \ldots + a_{m,m} r''^2_m$. Now, we make a single transformation $\vec{r''} = H(\vec{r''})$ where for every $i \leq m$, we let $r''_i = r'_i + a_i/2$, where a_i is the coefficient of r''_i in $l_{p''}$ (this is well-defined, since $2 \neq 0$ for fields of odd characteristic).

□

Proof of Theorem A.1:

In our proof we will use a variant of Vazirani's xor lemma from [28] over general finite fields.

Lemma A.4 (Vazirani's XOR lemma). *Let $\mathbb{F}_q$ be a finite field, and let $\vec{X} = (X_1, \ldots, X_n), \vec{Y} = (Y_1, \ldots, Y_n)$ denote random variables over $\mathbb{F}_q^n$. Then $\vec{X}, \vec{Y}$ are identically distributed iff. for all $\vec{\alpha} \in \mathbb{F}_q^n$, $\sum_i \alpha_i X_i$ and $\sum_i \alpha_i Y_i$ are identically distributed.*

As an immediate corollary, we obtain the following.

Claim A.5. *Consider a $PSSS_{s^*+sr+r+r^2}$ scheme $\mathcal{M}(\mathbb{F}_q, t, k, Sh)$ for an access structure $\mathcal{A}$. Recall the polynomials in the share of P_i are labeled by $p_{i,1}, \ldots, p_{i,l_i}$. Then $\mathcal{M}$ is private iff. for every maxterm $M = \{P_{i_1}, \ldots, P_{i_h}\}$ of $\mathcal{A}$ and every $\alpha \in \mathbb{F}_q^{\sum_{j \leq h} l_{i_j}}$ all polynomials in the set $G_{M,\alpha} = \{p_{M,\alpha,\vec{s}}(\vec{r}) = \sum_{j \leq h} \sum_{l \leq l_{i_j}} \alpha_{i_j,l} p_{i_j,l}(\vec{s}, \vec{r}) | \vec{s} \in \mathbb{F}_q^k\}$ have identically distributed outputs (for random inputs $\vec{r}$).*

By Claim A.5, for a given (M, α), all polynomials in $G_{M,\alpha}$'s have the same output distribution (over inputs in $\mathbb{F}_q^t$). We will go over all (M, α) pairs one by one, and update the mapping L, specified over a certain basis of $\mathbb{F}_q^t$ (this basis will also be determined adaptively, for a more convenient proof). The exact t' will also be determined in the process. Then, we will prove that indeed for each (M, α), all polynomials $p_{M,\alpha,\vec{s}}(L(r_1), \ldots, L(r_n)) = \tilde{p}_{M,\alpha,\vec{s}}(\vec{r})$ in $G_{M,\alpha}$ have the same output distribution.

For every $p_{M,\alpha,\vec{s}}(\vec{r})$, we rewrite it in canonical form $p'_{M,\alpha,\vec{s}}(\vec{r'})(\vec{r}')$, as guaranteed in Lemma A.2 but consider them as polynomials in new variables $\vec{r''}$, where for each $\vec{r'}_i =< \alpha'_1, \vec{r} > +b'_1$ we have $\vec{r''}_i =< \alpha'_1, \vec{r} >$. We denote the new representation by the polynomial $p''(\vec{r}'')$. To clarify what we mean, consider for example the $(\mathbb{F}_q, n, m, T = 1, 3)$-type polynomial $p'(\vec{r}')$. We get

$$\begin{aligned} &p''(\vec{r}) = (a'_{1,2}(r''_1 + b'_1)(r''_2 + b'_2) + \ldots + (a'_{m-1,m}(r''_{m-1} + b'_{m-1})(r''_m b'_m)) = \\ &a'_{1,2}r''_1 r''_2 + a'_{3,4}r''_3 r''_4 + \ldots + a'_{m-1,m}r''_{m-1}r''_m + \\ &a'_{1,2}b'_1 r''_2 + a''_{1,2}b'_2 r''_1 \ldots + a_{m-1,m}b'_{m-1}r''_m + a_{m-1,m}b'_m r''_{m-1} + \\ &a'_{1,2}b'_1 b'_2 + \ldots + a'_{m-1,m}b'_{m-1}b'_m = \\ &f_{p''}(\vec{r''}) + l_{p''}(\vec{r''}) + a_{p''} \end{aligned} \tag{12}$$

where each $\alpha_i \in \mathbb{F}_q^n, b'_i \in \mathbb{F}_q$. We will mostly think of the p'''s as polynomials in $\vec{r}$, which is common for all our polynomials, unlike the $\vec{r'}$ which may differ among the polynomials, as evident from Lemma A.2. What have we gained from this back-and-forth transformation? A more convenient restatement of the polynomials, from which the canonical form is evident. Finally, we note that among the polynomials p in some $G_{M,\alpha}$, however, only the l_p, a_p parts may differ among the resulting polynomials p''.

Observation 7. *For a fixed (M, α), all polynomials $p(\vec{r}) \in G_{M,\alpha}$ have the same f_p-part (and the r'''s are also the same as functions of $\vec{r}$).*

This stems from the fact that all share polynomials in a $PSSS_{s^*+(s+1)r+r^2}$ are of total degree 2, so all monomials in $p_{M,\alpha,\vec{s}}$ of r-degree 2 do have s-degree 0, and from the fact that the C-part in the transformation H in Lemma A.2 depends only on f_p (and therefor, also in the inverse transformation $H^{-1}(\vec{r'}) = C^{-1}\vec{r} - C^{-1}b$). In the following, we slightly abuse notation and identify between $p(\vec{r})$ and $p''(\vec{r})$ (as we only care about output distributions). Note that the p'''s are *almost canonical* (as the p''s are canonical). We proceed to constructing L. Roughly, for each (M, α), we require that certain properties satisfied by the original polynomials $p \in G_{M,\alpha}$ are satisfied by $L(p)$. This will ensure that the $L(p)$'s retain equal distributions.

1. (Collecting independence constraints): Here we fix a set of independence requirements that L needs to maintain. Go over all (M, α) pairs.
   (a) If all $p \in G_{M,\alpha}$ are of type lin0, for each $p \in G_{M,\alpha}$ add the constraint that $L(l_{p''})$ is not spanned by $A = L(\{r''_1, \ldots, r''_m\})$ to S_{ind} (note the concrete $r''_1, \ldots, r''_m$ may differ among the different polynomials in $G_{M,\alpha}$). We store the constraint in S_{ind} as a tuple $(l_{p''}, A)$, where A is a set spanning a subspace of $V_{r,t}$.[14]
   (b) If all $p \in G_{M,\alpha}$ are of type $(\mathbb{F}_q, n, m, y, b)$ of type lin1 or lin2, for each $p \in G_{M,\alpha}$ add the requirement that r''_m is not spanned by $\{r''_1, \ldots, r''_{m-1}\}$ to S_{ind}.
2. (Collecting dependence constraints). Here we fix a set of dependence requirements that L needs to maintain. Go over all (M, α) pairs.

[14] As L is linear, we can represent the constraint by the pair $l_{p''}, A$ before the transformation.

(a) If all $p \in \bigcup_{M,\alpha} G_{M,\alpha}$ are of non-linear type, for each $p \in G_{M,\alpha}$ add the requirement that l_p is spanned by $span(p'')$ to S_{dep}. Crucially, unlike in S_{ind}, here we store the constraint as a tuple $(l_p, f_{p''})$, rather than $span(p'')$, as $span(p'')$. The relevant subspace will be derived from $f_{p''}$ *and* the current value of L upon 'implementing' that particular constraint.[15]

(b) If all $p \in \bigcup_{M,\alpha} G_{M,\alpha}$ are of type lin1, for each $p \in G_{M,\alpha}$ add the requirement that $l_{p''}$ is spanned by $span(p'')$ to S_{dep}. Again, the requirement is represented by $(l_{p''}, f_{p''})$

(c) If all $p \in \bigcup_{M,\alpha} G_{M,\alpha}$ are of type lin2, for each $p \in G_{M,\alpha}$ add the requirement that $l_{p''}$ is spanned by $span(p'') \cup \{r''_m\}$ to S_{dep}. The requirement here is represented by $(l_{p''}, (f_{p''}, r''_m))$.

3. (implementing constraints).

(a) Go over the set of elements $\{v \in V_{r,t} | (v, A) \in S_{ind}\}$. Let $B_1 = \{b_1, \ldots, b_h\}$ denote a basis for these elements. Set $L(b_i) = \tilde{r}_i$ for each $b_i \in V_{r,t}$. Complement B_1 into a basis of $V_{r,t} \setminus \{1\}$ arbitrarily, and let $B_2 = \{b_{h+1}, \ldots, b_t\}$ denote the added basis vectors. Set $z = h$.

(b) Go over the constraints $(v, A) \in S_{ind}$. Extend the mapping L into L' as guaranteed by Claim A.6 applied to $L, B' = B_1, V = A, l = l_{p''}$. Update $z \leftarrow z + 1$. Set $L \leftarrow L''$.[16]

(c) Go over the constraints $(v, A) \in S_{dep}$.

- Extend the mapping L (to $V_{r,z}$) into a mapping L' to $V_{r,z+1}$ as obtained by applying Claim A.7 to $L, B' = B_1, V = f_{p''}, l = l_{p''}$. Update $z \leftarrow z + 1$, $L \leftarrow L''$.

Note that the mapping $L : V_{r,t} \to V_{\tilde{r},t'}$ resulting at the end of the proccess indeed satisfies all dependence and independence constraints. This easily follows by induction on the constraint number handled by the above construction in step 3. The base case holds since the inputs to the claims satisfy the claims' precondition by construction (the definition of L and B_1). In particular, in Claim A.6, indeed l always belongs to $span(B')$ ($B' = B_1$), and L is invertible over B'. The step holds roughly due to the 'moreover' part in Claim A.6 and Claim A.7. Also, t' is of size

$$t' \leq |S| \times |\{(M, \alpha)\}| \leq |S| 2^n q^{n \cdot SC/log(q)} \leq 2^{n + n \cdot SC(\mathcal{M}) + k}$$

As $k \leq SC(\mathcal{M})$, we have.

$$RC(\mathcal{M}) \leq t' \leq 2^{O(n \cdot SC(\mathcal{M})} \tag{13}$$

as stated in the theorem.

Claim A.6. *Let $B' = \{b_1, \ldots, b_{u'}\}$ denote a basis of a subspace $V' \subseteq V_{r,t}$. Let L denote a linear mapping from $V_{r,t}$ to $V_{\tilde{r},u}$ for some $u' \leq u \leq t$ which has kernel $\{0\}$ when restricted to V'. Let V denote a subspace of $V_{r,t}$, and $l \in span(B') \setminus V$.*

[15] This is the case as $span(p''(L(\vec{r})))$ may not equal $L(span(p''))$, but rather be a strict subset of the latter.

[16] Both Claim A.6 and Claim A.7 could return $L' = L$, so increasing the dimension of the image space by 1 could be avoided. For simplicity, we do not make this optimization.

Then there exists a linear mapping $L' : V_{r,t} \to V_{\tilde{r},u+1}$ 'extending' L' satisfying:[17] *(1) $L'(b_i) = L(b_i)$ for all $b_i \in B'$. (2) $\mathbf{proj}_{V_{\tilde{r},u}}(L'(v)) = \mathbf{proj}_{V_{\tilde{r},u}}(L'(v))$ for all $v \in V_{r,t}$. (3) $L'(l)$ is not spanned by $L'(V)$. (4) Moreover, every $L'' : V_{r,t} \to V_{\tilde{r},t}$ that agrees with L on B', and for every $x \in V_{r,t}$, $\mathbf{proj}_{V_{\tilde{r},u+1}}(L''(x)) = \mathbf{proj}_{V_{\tilde{r},u+1}}(L'(x))$ satisfies (3) (that is, $L''(l) \notin span(\{L''(r'_i)\}_{i\in[m]})$).*

Claim A.7. *Let $B' = \{b'_1, \dots, b'_{u'}\}$ denote a basis of a subspace $V' \subseteq V_{r,t}$. Let L denote a linear mapping from $V_{r,t}$ to $V_{\tilde{r},u}$ for some $u' \leq u \leq t$ which has kernel $\{0\}$ when restricted to V'. Additionally, let $p(r_1, \dots, r_t)$ denote an* almost canonical *polynomial with associated canonical polynomial $p'(r'_1, \dots, r'_t)$ of type $(\mathbb{F}_q, n, m, y, b)$ where $b \neq 0$, and $l \in span(L(\{r'_1, \dots, r'_m\}))$.*[18] *Then there exists a mapping 'extending' L in the following way: (1) $L'(b_i) = L(b_i)$ for all $b_i \in B'$. (2) $\mathbf{proj}_{V_{\tilde{r},u}}(L'(v)) = \mathbf{proj}_{V_{\tilde{r},u}}(L'(v))$ for all $v \in V_{r,t}$. (3) $L'(l)$ is spanned by $span(L'(span(p)))$ if p is not of type lin2. Otherwise, $L'(l)$ is spanned by $span(L'(f_p)) \cup \{L'(r'_m)\}$). (4) Moreover, every $L'' : V_{r,t} \to V_{\tilde{r},t}$ that agrees with L on B', and for every $x \in V_{r,t}$, $\mathbf{proj}_{V_{\tilde{r},u+1}}(L''(x)) = \mathbf{proj}_{V_{\tilde{r},u+1}}(L'(x))$ satisfies (3) as well.*

We will sketch the proofs of the above claims at the end of this proof. Next, we prove that if all constraints are satisfied, then the new scheme is private. That is, for all (M, α) all output distributions of polynomials $\tilde{p}(L(r_1), \dots, L(r_n))$ for $p \in (M, \alpha)$ are identical. We demonstrate the claim for the case of (all polynomials in) $G_{M,\alpha}$ are of type lin2, which is relatively involved. Other types are similar, by analyzing the particular output distribution of canonical polynomials of that type. Consider a pair $p''_1(\vec{r}), p''_2(\vec{r})$ of polynomials in $G_{M,\alpha}$ of type lin1. By Lemma A.3, $p''_1(\vec{r}'')$ $(p''_1(\vec{r}''))$ satisfies that $l_{p''_1}$ $(p''_1(\vec{r}''))$ is spanned by its corresponding $\{r''_1, \dots, r''_m\}$, but not by $\{r''_1, \dots, r''_{m-1}\}$. By construction, as we observed above, the polynomials $L(p''_1), L(p''_2)$ satisfy the same constraints. Let $\Delta^1 \in \mathbb{F}_q^{t'}$ be a vector such that $l_{f_{L(p''_1)}(\tilde{r}_1+\Delta_1,\dots,\tilde{r}_n+\Delta_n)} + cL(r''_m) = l_{p''_1}$ for some $c \neq 0$, as guaranteed by the dependence constraints. Therefor, $L(p''_1)(\tilde{r}-Delta^1)$ is a polynomial of the form $\tilde{p}_1(L(r''_1), \dots, L(r''_{m-1})) + L({r''}^2_m) + (L(r''_m))^2 + cL({r''}_m) + d$ for some $c \neq 0$ and quadratic form $\tilde{p}_1$ (not necessarily canonical), where $L(r''_m)$ is not spanned by $\{L(r''_1), \dots, L(r''_m)\}$, as guaranteed by the independence constraints. Thus, the output distribution of

$$L(p''_1(\vec{r} - \Delta^1)) = \tilde{p}_1(L(r''_1), \dots, L(r''_{m-1})) + \tilde{p}_{1,m}(L(r''_m))$$

is a sum of two independent random variables. Its output distribution is the same as $L(p''_1(\vec{r''}))$'s since adding a constant to each $\tilde{r}_i$ does not change the polynomials output distribution. Making a similar transformation for p''_2, we obtain

$$L(p''_2(\vec{r} - \Delta^2)) = \tilde{p}_2(L(r''_1), \dots, L(r''_{m-1})) + \tilde{p}_{2,m}(L(r''_m))$$

Since the quadratic part in p_1, p_2 was initially the same, $\tilde{p}_1 = \tilde{p}_2$. Also, as p''_1, p''_2 are almost canonical of the same type, before the transformation their ${r''}^2_m + cr''_m + d$-parts had the same output distribution (the r''_m in p''_1, p''_2 are possibly different elements of $V_{r,t}$). As we only replaced r''_m by $L(r''_m)$ mapping to a non-zero elements of $V_{\tilde{r},t'}$, these parts $(\tilde{p}_{2,m}, \tilde{p}_{1,m})$ keep their (equal) distributions (and

[17] Intuitively, we say it 'extends' L as it only defines a coefficient in $\tilde{r}_{u+1}$ - the 'new' vector in its output, and keeps to coefficients of 'old' variables $\tilde{r}_i$ for $i \leq u$ the same as in L.

[18] Again, viewing the r'_i's as elements of $V_{r,t}$.

are possibly no longer in canonical form). The $\tilde{p}_2(L(r''_1), \ldots, L(r''_{m-1})), \tilde{p}_1(L(r''_1), \ldots, L(r''_{m-1}))$ parts are equal, because the quadratic parts in the original polynomial are equal. Thus, in both we have a sum of two independently distributed random variables $A_{1,1} + A_{1,2}$ for $L(p''_1)$ and $A_{2,1} + A_{2,2}$ for $L(p''_2)$, where every pair $A_{1,1}, A_{2,1}$ has the same output distribution. [19]

It remains to prove the claims hold.

Claim A.6. Assume L' satisfies (1), (2), (3). We prove L' satisfies (4). By the assumption L' is a linear mapping $L' : V_{r,t} \rightarrow V_{\tilde{r},u+1}$ satisfying that $L(l)$ is not spanned by $L(V)$. By a duality argument, this holds iff. there exists $v \notin Ker(L(l))$, but $v \in Ker(V)$. Extending L' into L'' arbitrarily, there now exists v' as above, by simply letting v' to equal v on the first u coordinates (that is, $\mathbf{proj}_{V_{\tilde{r},u}}(v') = v$), and set the other $t - u$ coordinates to 0. Let us represent the required L' as a matrix M' of size $h \times (u+1)$, where h is the dimension of V, the rows are labeled by $g_0 = l, g_1, g \ldots, g_h$, where $B'' = \{g_1, \ldots, g_h\}$ is a basis of V. Entry $M_{i,j} = \mathbf{proj}_{V_{\tilde{r},\{j\}}}(L'(g_i))$. We define a similar matrix $M \in \mathbb{F}^{h \times u}$ for L. For convenience, assume wlog. that $\tilde{r}_1, \ldots, \tilde{r}_{u'}$ satisfy $\tilde{r}_i = L(b'_i)$, and that $B'' \cap span(B)\{g_1, \ldots, g_{h'}\}$ for some $h' \leq h$. Assume wlog. that $I = [h']$, and that all g_i for $i \in [h'']$ for some $h'' < h$ are in $span(B')$, and all g_j for $j \in [h'] \setminus [h'']$ are not in $span(B')$. Let $v = (v_1, \ldots, v_{u'}, 0, \ldots, 0) \in \mathbb{F}_q^u$ denote a vector for which $< L(g_i), v >= 0$ for all $i \in [h']$, and $< L(l), v >\neq 0$. It exists as $l \notin span(\{g_1, \ldots, g_{h'}\})$ (as it's not even in $span(\{g_1, \ldots, g_h\})$, $l \in span(B')$ and L is 1-1 on B'). Now, extend v into $v' = (v_1, \ldots, v_{u'}, 0, \ldots, 0, 1) \in \mathbb{F}_q^{u+1}$, and extend L on the (linearly independent set) $\{l, g_1, \ldots, g_{h'}\}$ according to (1) (setting $\mathbf{proj}_{V_{\tilde{r},[u+1]}}(\cdot)$ to 0). Finally, set $M'_{i,u+1}$ for all $i \in [h] \setminus [h']$ to $- <v, M_i>$ - note that if $[h] \setminus [h']$ is empty, there is nothing to set, and we could actually have $L' = L$ (and would not actually need the $u + 1$'th coordinate). In all cases, note that $< M_{[h]} \cdot v' = 0 >$, while $< M_0 \cdot v' >\neq 0$, implying $L'(l) \notin L'(span(V))$, as required. □

Next, we sketch the proof of Claim A.7.

Claim A.7. Let $l = \sum_i \Delta_i L(r'_i)$. Let us focus on the case of p with $(\mathbb{F}_q, n, m, y = 1, b = 3)$ with $char(q) = 2$. That is, the associated canonical $p'(r'_1, \ldots, r'_m)$ has $f_{p'} = r'_1 r'_2 + \ldots + r'_{m-1} r'_m$. Other cases rely on similar ideas. First observe that replacing each $L(r'_{2i})$ by $L(r'_{2i}) + \Delta_{2i-1}$ and $L(r'_{2i-1}) + \Delta_{2i}$ would yield $l_{f_{p'}(\vec{r'}+\Delta)} = l$, as required. The problem is that some $< \vec{r'}, \Delta >$'s may not be in $span(L(f_p))$, as the $L(r'_i)$'s are not necessarily linearly independent (note that for all $v \in span(L(f_p))$, $v \in span(\{L(r'_1), \ldots, L(r'_m)\})$). To achieve a given arbitrary Δ in $span(L'(f_p))$ let $\mathbf{proj}_{V_{\tilde{r},u+1}}(L'(r'_{2i}))$ $(2i-1)$ to be Δ_{2i-1} $(\Delta_2 i)$, except for those that are in $span(B')$. Then, it is easy to prove that the $+\vec{\Delta}$ can be emulated in by replacing $\tilde{r}_{u+1} = \tilde{r}_{u+1} + 1$, and the $\tilde{r}_i$'s for $i \leq u$ by $\tilde{r}_i + \delta_i$ in such a way that for $L(r'_{2i})$ $(2i-1)$, $L(r'_{2i})$'s $(2i-1)$ resulting added constant equals Δ_{2i-1} $(2i)$ for r. This can be achieved as L restricted to $span(B')$ has kernel $\{0\}$, and all r'_i's are linearly independent. □

[19] Intuitively, the only chance for the distributions to differ was that the linear part would no longer be canceled out in p_1 but not in p_2 after the transformation, as possibly Δ^1 used in the almost canonical polynomial would not be generated by the lower-dimension $\tilde{\vec{r}}$. The dependence constraints make sure it does not occur.

A.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 (perfectly correct and private) PSSS and general secret sharing schemes.

Theorem A.8. *Let $\mathcal{M}$ denote a secret sharing scheme implementing an access structure $\mathcal{A}$ (with perfect privacy and correctness). Then there exists an equivalent secret sharing scheme with $RC(\mathcal{M}) = 2^{\tilde{O}(SC(\mathcal{M}))}$. Furthermore, if $\mathcal{M} = (\mathbb{F}_{q^d}, t, k, Sh)$ is a PSSS, then there exists an equivalent PSSS scheme $\mathcal{M}' = (\mathbb{F}_{q^d}, t', k, Sh')$ with $SC(\mathcal{M}') = SC(\mathcal{M})$ and $RC(\mathcal{M}') = 2^{poly(SC(\mathcal{M}))}$.*

Notation and some facts on Linear programs. For a PSSS scheme $\mathcal{M} = (\mathbb{F}_{q^d}, t, k, Sh)$, let us denote by sc the number of polynomial evaluations (field elements) output by Sh. Thus, $sc \geq k$ (since the set of sharings must be at least as large as S). We will need some theory of linear programs (LP). 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 $A = \{a_1, \ldots, a_t\} \subseteq \mathcal{R}^m$, the affine dimension of A, $\mathrm{aff}(A)$, is the dimension of $\{a_2 - a_1, \ldots, a_t - a_1\}$. We say that a set A has *full affine dimension* if $\mathrm{aff}(A) = |A| - 1$.

Theorem A.9. *[[25], 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). Furthermore, Any solution p of (A, b) is a convex combination of a subset $\{p_1, \ldots, p_\ell\} \subseteq \mathcal{B}$ of full affine dimension, where $\ell \leq m + 1$.

Lemma A.10. *[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 A.11. *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 integers, then the $|a'_{i,j}|$'s are multiples of a constant $0 < L \leq m^m$.

The proof of the above lemma follows directly from Lemma A.10.

Proof. (Of Theorem A.8) The proof consists of several steps:

step 1: Let us consider the given polynomial scheme $\mathcal{M}$ as in the theorem statement. We denote $Q = q^d$, $SC = Q^{SC(\mathcal{M})}$, and $sc = \log_Q(SC)$.

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 $p_{i,j}$ 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 $S, S_1 \times \ldots \times S_n$ 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 $\mathrm{s}_i, \mathrm{s}_j \in S$ the probability of getting the same shares (for this specific set) should be equal. That is to say, for any two secrets $\mathrm{s}_i, \mathrm{s}_j \in S$ and projection of shares on A, $\vec{sh}'$ (some specific share that parties in A receive).

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

Reorganizing, we get.

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

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

$$\sum_{\substack{all\ k\ for\ which\ the\ projection\\ of\ \vec{sh}_k\ on\ A\ is\ \vec{sh}'\\ and\ j \neq i}} p_{j,k} = 0 \qquad (15)$$

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

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

$$\sum_j p_{i,j} = 1 \qquad (16)$$

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.

$$0 \leq p_{i,j} \tag{17}$$

We stress that the privacy and probability constraints follow from the requirements on any secret sharing scheme implementing $\mathcal{A}$. The correctness constraints 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 14, 15, 16, where the variables are the the $p_{i,j}$-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:

$$r = 2^n |\mathbb{F}_Q^k| SC \leq SC^3 \tag{18}$$

Here the inequality holds since $n, k \leq sc$. There are at most r columns in M_1 thus and at most r rows.[20]

This LP is solvable since $p_{\mathcal{M}}$ is a solution for it. The right hand side b is the vector obtained from Equations 14, 15, 16 $(0, 0, \ldots, 0, 1, \ldots, 1)$ (with $|S|$ 1's at the end).

Observation 8. *In the LP (M_1, b) above, all the entries in M_1 and in b are 1, -1 or 0.*

step 2: Now, any solution $\vec{p'}$ to the LP specified by (M_1, b) defines a secret sharing scheme for the desired access structure. Namely, assuming all entries in a solution $\vec{p}$ are multiples of some $1/L$ for some integer, we can set R to be of size L, and an arbitrary mapping Sh from $(\vec{s}, \vec{r})$'s to share vectors in $\mathbb{F}_Q^{sc}$ that agree with the probabilities in $\vec{p}$.

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 exists $t' = 2^{2^{poly(SC)}}$, 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 A.9, 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 $\mathcal{M}$) $p_{\mathcal{M}} \in CH(G)$.[21]. Next, we prove that the entries of all $p_i \in G$ are of "low" resolution.

Claim A.12. *For every $g \in G$, there exists an integer $0 < L \leq r^{2r}$, every entry g_i of g is a multiple of $1/L$.*

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 8, the claim follows from Lemma A.11. □ □

For any G, if the resulting scheme $\mathcal{M}'$ is not required to be a PSSS, then we are also done, as we can take (e.g.) $p_1 \in G$ as a basis for the scheme,

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

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

and set R of size $L \leq 2^{2r}$ as guaranteed by Lemma A.12. The randomness complexity of the resulting scheme is $\log_2(L) = 2^{\tilde{O}(SC(\mathcal{M}))}$. Additionally, for the case of $\mathcal{M}$ is a PSSS, $\mathcal{M}'$ is as in the theorem if $|G| = 1$, then p_1 must be a single solution, and its entries are already multiples of q^d, and we are done, as $M \leq r^{2r} \leq 2^{2^{\tilde{O}(SC(\mathcal{M}))}}$. Therefor, the solution vector p_1 induces a PSSS where $t = \log_Q(M) = 2^{\tilde{O}(SC(\mathcal{M}))}$. This is also the case if some BFS $p_i \in G$ happens to have entries which are all multiples of $Q^{-t'}$ for some t'. Otherwise, we prove below that $CH(G)$ contains some solution where all entries are multiples of $Q^{-t'}$ where $t' = 2^{poly(SC)}$.

From now on 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.[22]. 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:

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

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

$$\begin{aligned} \sum_{i=1}^{\ell-1} \beta_i (p_{i+1} - p_1) = \vec{p} - p_1 \\ 0 \leq \beta_i \\ \sum_i \beta_i \leq 1 \end{aligned} \tag{19}$$

step 4: The above system defines an LP with $M_2 = \begin{bmatrix} p_2 - p_1 | & p_3 - p_1 | & \ldots | & p_n - p_1 \end{bmatrix}$ 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

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

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 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 A.11 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 $w \leq r^{2r}$. For a point $v \in \mathbb{R}^n$, let us denote by $ball_\epsilon^\infty(v)$ the set of points $\mathbb{R}^n$ at ℓ_∞ distance $\leq \epsilon$ from v. 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 A.13. *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 A.11, 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 A.13 and Claim A.12 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 $(M_3, b_3 = p_3'' - p_{1,3})$.[23] In particular, the set of vectors corresponding to the set of p'''s above is precisely $p' - p_1 + ball_\epsilon$. As

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

$M_3 \in \mathbb{R}^{h\times h}$ (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 $CH(G)$.

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:

$$\forall (h < j \leq r) M_{2,j} = \sum_{i=1}^{h} k_{i,j} M_{3,1} \tag{20}$$

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'.

$$\begin{gathered} p_j = p_{1,j} + \sum_{i=1}^{h} k_{i,j}(p_i - p_{1,i}) \\ h < j \leq r \end{gathered} \tag{21}$$

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 9. *In Equation 21, all coefficients $k_{i,j}, p_{1,i}, p_{1,j}$ are reduced fractions of the form w/h, where $h \leq r^{r^2+r}$.*

Proof. The observation for the $p_{1,i}, p_{i,j}$'s follows from Claim A.12. 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 A.11, 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 19 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 21, 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 21. 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.

$$\begin{aligned} \forall i \leq h \forall j > h \quad \tilde{k_i^j} &= k_i^j M = \forall i \geq 1, \frac{b_i^j}{D_{i,j}^k} M \\ \forall i \geq 1 \quad \tilde{p_{1,i}} &= p_{1,i} M = \frac{c_{1,i}}{D_{1,i}} M \\ \forall i \leq h \quad \tilde{p_i} &= p_i M = \frac{l_i}{Q^{\tilde{t}}} M = l_i R \end{aligned} \tag{22}$$

Again, the fractions on the right in the first and second line are reduced.

When multiplying both sides of all the equations in 21 by M^2 we get:

$$l_j R M = \tilde{p_j} M = \tilde{p_{1,j}} M + \sum_{i=1}^{h} \tilde{k_i^j} (\tilde{p_i} - \tilde{p_{1,i}}) \tag{23}$$

And we already incorporated the requirements that p_i's for $i \leq h$ are multiples of $Q^{-\tilde{t}}$ into Equation 22 (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

$$\forall j > h, \tilde{p_{1,j}} M + \sum_{i=1}^{h} \tilde{k_i^j} (\tilde{p_i} - \tilde{p_{1,i}}) \equiv 0 \ (mod \ MR) \tag{24}$$

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 $\frac{MR}{D}$:

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

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.

$$\forall j > h \quad c_{1,j} \frac{D}{D_{1,j}} Q^{\tilde{t}} + \sum_{i=1}^{h} (b_i^j \frac{D}{D_{i,j}^k} l_i - b_i^j c_{1,i} \frac{D}{D_{i,j}^k D_{1,i}} Q^{\tilde{t}}) \equiv 0 \ (mod \ D) \tag{26}$$

Note that due to the choice of D all coefficients in this equations above are indeed integers [24]

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

[24] 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 $D = D'$.

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 26 modulo D, including the value of D and "almost" all coefficients of that equations are independent of D does not depend on $\tilde{t}$. [25]. 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

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

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 26 is solvable if $Q^{\tilde{t}}$ is replaced with v. Now, clearly, there exists at least one value $t' = \tilde{t}$ such that $Q^{t'} \equiv v \bmod D$. Now, there are two possible cases. There could be only one such value $t' = \tilde{t}$, which occurs only if $1 \notin \{Q^t \bmod D | t \in \mathbb{N}\}$. In this case, we must have $\tilde{t} \leq D$ (by pigeon hole principle). Otherwise, there are more than one suitable t'. In this case, there are in fact infinitely many such values t'

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

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

Let us obtain a gross upper bound on D.

$$D = lcm(\{D_{i,j}\} \cup \{D^k_{i,j}\}) \leq \left(r^{2r}\right)^{r^2+r} = r^{O(r^3)}. \tag{27}$$

In the first case, we just learn that

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

So this bounds the randomness complexity of the scheme by $r^{O(r^3)} = SC^{O(SC^9)}$ 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 26. 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 pariticular, 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

[25] As mentioned before, we only assume that $Q^{\tilde{t}}$ is divisible by all Q-powers in all coefficients in Equation 26

would need to move from p_3' by at most Q^D/M in each coordinate, to satisfy the constraint system 26.

We therefore require

$$Q^D/M \leq \epsilon \Leftrightarrow Q^{t'} \geq \frac{Q^D}{\epsilon R} \Leftrightarrow t' \geq \log_q(r^{O(r^3)}) = D + \tilde{O}(r^2) \tag{28}$$

Observation 9, 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 $r = O(SC^3)$, we get a bound of $2^{\tilde{O}(SC^9)}$ on $RC(\mathcal{M}')$.

□

B 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 [36] 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 [32] 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 $2^{\tilde{O}(\sqrt{n})} = 2^{\tilde{O}\left((\log m)^{0.5}\right)}$ per party. The scheme is implied by [35]'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 rate$O(2^{0.994m})$ and $O(2^{0.999m})$ for general and linear secret sharing schemes respectively. This difference stems only from the differences in the best information rate 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 rate $O(1)$ 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 rate of the entire formula-based resulting construction, information rate of at most $O(2^{0.994m})$ is obtained.[26]

C 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 as believe this framework will prove useful due to the rich algebraic structure of (multi-variate) polynomials. For example, 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. Moreover, 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).

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[27].

[26] 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.

[27] If the original scheme was perfect, its security degrades to statistical, though. In terms of feasibility for all monotone access structures, there exists a linear scheme over any finite field

This is done by sampling the randomness of the original scheme via a circuit (simple, $NC1$ [26] 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 - using the fact that any function can be represented as a multi-variate polynomial.

Although this leaves the question of perfect (the default) secret sharing open, the above observation implies that PSSS is a very general framewok.

Two general questions are of interest:

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

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.

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. This can be done by further improving the upper bounds on randomness complexity. For degree-2, we need a bound of $RC = 2^{O(SC)}$ for a sufficiently low constant in the exponent to beat the best known lower bound on SC for general secret sharing schemes (which is $n^2/log(n)$ for total share complexity). Another interesting question open for degree-2 polynomials is understanding the complexity of access structures admitting a $PSSS$ with $d = 2$ with $poly(n)$ share complexity over some field. For degree-1 this set is contained in NC.[28]

Finally, for degree-1, it would be nice to generalize [37]'s lower bounds from the linear to the multi-linear setting.

$\mathbb{F}$. The construction here is a straightforward generalization of [15]. That is, a polynomial scheme of degree 1 and $k = 1$ always exists. In fact, this particular scheme generalizes to any cyclic group $\mathbb{Z}_m$.

[28] In [31], the authors provide a bound along these lines for randomizing polynomials, but it does not directly apply here, as in secret sharing there are generally exponentially many minterms.

D Additional 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.

D.0.1 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 [39] is an *ideal* secret sharing schemes - having information rate 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 [18]. 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 [33] 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 [8]. 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 [19]'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 [33], 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 [6] against a function in NP. These bounds were simplified and improved by Gál [21] to $n^{\Omega(\log(n))}$. Beimel and Weinreb [13] later gave $n^{\Omega(\sqrt{\log n})}$ lower bounds for a function in uniform NC^2 (and therefore in P), proving that the languages captured by monotone span programs do not contain polynomial time.

The technique of [21] 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 [38].[29]

Very recently, in a break-through result, [37] 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.

D.0.2 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 rate (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.

Beimel, Ben-Efraim, Padró and Tyomkin proved in [9] 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 [9] 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

[29] In particular, note that formula size is a lower bound on MSP size, as follows from [15]

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 [9] a (constant) gap between linear and multi-linear information rate 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 rate per party for a large set of access structures, where the sharing algorithm has degree 1 (multi-linear) [2]. Namely, this holds for the so-called d-uniform access structures for constant d, to be defined below, a scheme with information rate 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.[30]

Quite surprisingly, a very recent work of [36] 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 [3] 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 also observe that a multi-linear scheme over $\mathbb{F}_2$ can do as well as the non-polynomial scheme from [36] for sufficiently large (exponential) $k(n)$.

D.0.3 Beyond Degree-1 PSSS

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 [29] [30]. 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

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

low degree randomized encodings of a function via standard protocols [14] is a simple approach to obtaining general constant round MPC protocols in various settings.

In [13] 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 [19] 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 [35] 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 $\vec{\mathrm{sh}}_x, \vec{\mathrm{sh}}_y$ respectively of the secret s.[31] The secret is disclosed given $x, y \in \{0,1\}^{n/2}$ and $\vec{\mathrm{sh}}_x, \vec{\mathrm{sh}}_y$ if x, y satisfy a (not necessarily monotone) predicate $P(x, y)$. Otherwise, $\vec{\mathrm{sh}}_x, \vec{\mathrm{sh}}_y$ 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 $P(x, y) = 1$ [12]. 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 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 [10] (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 [2] to which we referred in Section D.0.2 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 [35], 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.

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

In comparison, there exist 2-party CDS schemes [22, 35] translating into linear secret sharing schemes (with $k = 1$) with share complexity $\tilde{O}(m^{1/2})$ for 2-uniform access structures. In [10], 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 [35] 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 [22] 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 [22] translates into a linear scheme with share complexity $O(2^{m/2})$ for the family $\mathcal{A}_m$.

The matching vectors (MV) based scheme from [35] 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 [35] 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 [27] 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 [35] 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 $O(2^{m/3})$.