On the Power of Nonlinear Secret-Sharing*

(PRELIMINARY VERSION)

Amos Beimel
Dept. of Computer Science
Ben-Gurion University
Beer-Sheva 84105, Israel
beimel@cs.bgu.ac.il

Yuval Ishai
DIMACS and AT&T Labs – Research
96 Frelinghuysen Road
Piscataway, NJ 08854, USA
yuval@dimacs.rutgers.edu

Abstract

A secret-sharing scheme *enables a dealer to distribute a secret among n parties such that only some predefined authorized sets of parties will be able to reconstruct the secret from their shares. The (monotone) collection of authorized sets is called an* access structure*, and is freely identified with its characteristic monotone function $f : \{0,1\}^n \to \{0,1\}$. A family of secret-sharing schemes is called* efficient *if the total length of the n shares is polynomial in n. Most previously known secret-sharing schemes belonged to a class of* linear *schemes, whose complexity coincides with the* monotone span program *size of their access structure. Prior to this work there was no evidence that nonlinear schemes can be significantly more efficient than linear schemes, and in particular there were no candidates for schemes efficiently realizing access structures which do not lie in* NC.

The main contribution of this work is the construction of two efficient nonlinear schemes: (1) A scheme with perfect privacy whose access structure is conjectured not to lie in NC*; (2) A scheme with statistical privacy whose access structure is conjectured not to lie in* $\mathrm{P/poly}$*. Another contribution is the study of a class of nonlinear schemes, termed* quasi-linear *schemes, obtained by* composing *linear schemes over different fields. We show that while these schemes are possibly (super-polynomially) more powerful than linear schemes, they cannot efficiently realize access structures outside* NC.

1 Introduction

Secret-sharing schemes enable a dealer, holding a secret piece of information, to distribute this secret among n parties such that only some predefined authorized subsets of parties can reconstruct the secret from their shares and others learn nothing about it. The (monotone) collection of authorized sets that can reconstruct the secret is called an *access structure*, and is freely identified with its characteristic monotone function $f : \{0,1\}^n \to \{0,1\}$.

The first secret-sharing schemes were introduced by Blakley [14] and Shamir [48]. They constructed *threshold* schemes, in which the access structure is defined by a threshold function. General secret-sharing schemes, realizing non-threshold access structures, were introduced by Ito, Saito, and Nishizeki [41], where it was shown that every monotone access structure can be (inefficiently) realized by a secret-sharing scheme. More efficient schemes for specific types of access structures were presented, e.g., in [11, 50, 18, 42]. We refer the reader to [49, 52] for

*This paper was accepted for publication in the proceedings of the 16th Annu. IEEE Conf. on Computational Complexity, 2001.

extensive surveys on secret-sharing literature.[1]

Originally motivated by the problem of secure information storage, secret-sharing schemes have found numerous other applications in cryptography and distributed computing (cf. [46, 10, 23, 25, 28]). However, secret-sharing is independently interesting as a pure complexity question. The default complexity measure of secret-sharing schemes is their *share size*, i.e., the total length of all shares distributed by the dealer. This is a measure of the amount of communication (or storage) required for sharing a secret.[2] One of the most interesting open questions in this area is to characterize which access structures can be *efficiently* realized, i.e., with shares of polynomial size in the number of parties n. For most access structures, the best known upper bound on the share size is exponential. However, unlike other concrete complexity measures such as circuit complexity, one cannot apply simple counting arguments to show that this must indeed be the case. In fact, given the current knowledge, one cannot even rule out the possibility that *all* access structures can be efficiently realized.

Several lower bounds on the share size of secret-sharing were obtained [22, 15, 30, 27, 26]. The strongest current bound is $\Omega(n^2/\log n)$ [26]. This bound applies to an *explicit* access structure. However, as noted above, there is a huge gap between these lower bounds and the best known upper bounds.

1.1 Linear vs. Nonlinear Secret-Sharing

Most previously known secret-sharing schemes were *linear*. In a linear scheme, the secret is viewed as an element of a finite field F, and the shares are obtained by applying a linear mapping to the secret and several independent random field elements. Linear schemes may be equivalently defined by requiring that each authorized set reconstructs the secret by applying a linear function to its shares [8]. For example, the schemes of [48, 14, 41, 11, 50, 18, 42, 31] are all linear.

The share size in linear schemes over F realizing a monotone function f is proportional to the *monotone span program* size of f over F. (Span programs are a linear-algebraic model of computation introduced in [42].) In fact, there is a one-to-one correspondence between linear secret-sharing schemes and monotone span programs. The class of functions that have polynomial size monotone span programs, which coincides with those admitting efficient linear secret-sharing schemes, is fairly well understood: (1) it contains monotone NC^1 and even monotone symmetric logspace [11, 12, 42]; (2) it is contained in algebraic NC^2 (as follows from [13, 17, 45, 21]), implying that it is contained in NC^3 when $\log|F|$ is polynomially bounded; and (3) there are explicit monotone functions that are provably not in this class [9, 2, 35].

As opposed to linear secret-sharing schemes, nearly nothing is known for general (i.e., possibly nonlinear) schemes. Several constructions of nonlinear secret-sharing schemes have been suggested, both for the threshold case [55, 29, 47] and for general access structures [19, 33]. The question of basing verifiable secret-sharing and secure multi-party computation on nonlinear secret-sharing has been recently studied in [24]. However, none of these works provides evidence that nonlinear schemes are significantly more powerful than their linear counterparts.

The relation between linear and nonlinear complexity has been studied in other contexts, such as coding and randomness extraction (cf. [54]). While in some of these contexts the margins of possible improvement obtained by relaxing the linearity restriction are provably small, this is not the case for our problem. As discussed above, it is not even known if there exists an access structure that *cannot* be efficiently realized by a nonlinear scheme. On the other hand, prior to this work there was no evidence that nonlinear schemes are significantly more efficient than linear schemes. In particular, there were no explicit candidates for secret-sharing schemes realizing access structures which do not lie in NC.

[1] Similarly to almost all of the vast literature on secret-sharing, this work is concerned with the *information-theoretic* variant of the problem. A relaxed notion of *computationally*-secure secret-sharing has been considered in [43, 6].

[2] By default, we ignore the *computational* complexity of the scheme. However, most of our efficient constructions are also computationally efficient. We explicitly indicate when this is not the case.

1.2 Our Results

We attempt to remedy the above state of affairs. To this end, we take two different approaches.

Specific candidates. The main contribution of this work is the construction of specific efficient nonlinear schemes, whose access structures are conjectured to be hard. We present two main schemes, whose access structures are related to two variants of the quadratic residuosity problem.[3] A third scheme, which is a simplified version of the second, realizes an access structure related to the co-primality problem.[4]

The first scheme realizes an access structure whose computational complexity is equivalent to that of deciding quadratic residuosity modulo a *fixed* prime, where the prime modulus may depend only on the number of parties.[5] This problem is not known to be in NC. In particular, assuming that it is indeed not in NC, a separation of efficient nonlinear schemes from efficient linear schemes follows.

The second scheme realizes a presumably much harder access structure, whose computational complexity is equivalent to the general quadratic residuosity problem. The latter is widely conjectured to require exponential-size circuits, and its intractability is implied by the so-called *Quadratic Residuosity Assumption* [37], which is commonly relied on in cryptography. In contrast to the first construction, the second construction only meets a more liberal notion of secret-sharing (with a statistical relaxation of the perfect correctness and privacy requirements, see Section 2), and its reconstruction procedure is computationally inefficient. Yet, the second scheme demonstrates that the share size in a secret-sharing scheme may be super-polynomially smaller than the circuit size of its access structure.

As a variant of the second scheme described above, we obtain a scheme whose access structure is equivalent to the co-primality problem. Similarly to quadratic residuosity modulo a (fixed) prime, the co-primality problem is in P but is not known to be in NC. The third scheme meets only the more liberal notion of security. However, unlike the second scheme it is also computationally efficient. Compared to the first scheme, the co-primality problem is more standard than the problem of deciding quadratic residuosity modulo a *fixed* prime. The main properties of the three schemes described above are summarized in Table 1.

section	perfect/ statistical	access structure related to...	comput. efficient?
§3	perfect	quadratic residuosity modulo a fixed prime	yes
§4	statistical	quadratic residuosity	no
§4.2	statistical	co-primality	yes

Table 1. Summary of Our Main Schemes.

Our constructions were inspired by a non-interactive private protocol for the quadratic residuosity problem from [34]. In fact, every protocol in the model of [34, 40] can be transformed into a secret-sharing scheme for a related access structure. In the context of communication complexity lower bounds, the quadratic residuosity problem has been used in [4, 3].

Quasi-linear schemes. In addition to the above specific candidates, we study the class of nonlinear schemes obtained by *composing* linear schemes over (possibly) different fields, which we term *quasi-linear* schemes. Composition of secret-sharing schemes has been used in previous works (cf. [11, 20, 53, 44, 25]). However, to the best

[3] The quadratic residuosity problem is that of deciding, given a pair of integers w, u, whether w is a square modulo u.

[4] The co-primality problem is that of deciding, given w, u, whether $\gcd(w, u) = 1$.

[5] While a generalization to quadratic residuosity modulo a *fixed* composite is possible, this problem is essentially equivalent in a non-uniform setting to deciding quadratic residuosity modulo a fixed prime.

of our knowledge this is the first work to explicitly discuss compositions of linear schemes over different fields. We characterize the complexity of quasi-linear schemes in terms of Boolean formulas over the basis of monotone span programs. While quasi-linear schemes are likely to be strictly more powerful than linear schemes, we prove that they cannot realize any access structure outside NC. Specifically, we show that the class of structures which they can efficiently realize is contained in NC^4. Thus, quasi-linear schemes do not provide the strong (conjectured) results implied by the specific candidates described above. On a positive note, we show an application of quasi-linear schemes for the construction of secret-sharing schemes efficiently realizing monotone span programs over a ring $\mathcal{Z}_u$, where u is a square-free composite. A naive generalization of the construction for monotone span programs over *fields* [42] fails to achieve this goal.[6]

ORGANIZATION. In Section 2 we present some definitions and background. In Sections 3 and 4 we describe our two main constructions of efficient nonlinear schemes, and discuss the complexity of their access structures. In Section 5 we introduce and study the class of quasi-linear schemes. Finally, in Section 6 we mention some open problems.

2 Preliminaries

In this section we define secret-sharing schemes, linear schemes, and span programs, and briefly discuss the connections between these notions. We end this section with some definitions related to the quadratic residuosity problem.

Definition 2.1 (Access Structure) *Let $\{P_0,\ldots,P_{n-1}\}$ be a set of parties. A collection $\mathcal{A} \subseteq 2^{\{P_0,\ldots,P_{n-1}\}}$ is* monotone *if $B \in \mathcal{A}$ and $B \subseteq C$ imply $C \in \mathcal{A}$. An* access structure *is a monotone collection $\mathcal{A}$ of non-empty subsets of $\{P_0,\ldots,P_{n-1}\}$ (that is, $\mathcal{A} \subseteq 2^{\{P_0,\ldots,P_{n-1}\}} \setminus \{\emptyset\}$). The sets in $\mathcal{A}$ are called the* authorized sets. *A set B is called a* minimal set *of $\mathcal{A}$ if $B \in \mathcal{A}$, and for every $C \subsetneq B$ it holds that $C \notin \mathcal{A}$. The minimal sets of an access structure uniquely define it. Finally, we freely identify an access structure with its monotone characteristic function $f_{\mathcal{A}} : \{0,1\}^n \to \{0,1\}$, whose variables are denoted $x_0,\ldots,x_{n-1}$.*

Definition 2.2 (Secret-Sharing) *Let S be a finite set of secrets, where $|S| \geq 2$. An n-party* secret-sharing scheme *Π with* secret-domain *S is a randomized mapping from S to a set of n-tuples $S_0 \times S_1 \times \ldots \times S_{n-1}$, where S_i is called the* share-domain *of P_i. A dealer distributes a secret $s \in S$ according to Π by first sampling a vector of* shares *$(s_0,\ldots,s_{n-1})$ from $\Pi(s)$, and then privately communicating each share s_i to the party P_i. We say that Π* realizes *an access structure $\mathcal{A} \subseteq 2^{\{P_0,\ldots,P_{n-1}\}}$ (or the corresponding monotone function $f_{\mathcal{A}} : \{0,1\}^n \to \{0,1\}$) if the following two requirements hold:*

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

$$\Pr[\,\mathrm{Rec}_B(\Pi(s)_B) = s\,] = 1,$$

where $\Pi(s)_B$ denotes the restriction of $\Pi(s)$ to its B-entries.

Privacy. *Every unauthorized subset cannot learn anything about the secret (in the information theoretic sense) from their shares. Formally, for any subset $C \notin \mathcal{A}$, for every two secrets $a, b \in S$, and for every possible shares $\langle s_i \rangle_{P_i \in C}$:*

$$\Pr[\,\Pi(a)_C = \langle s_i \rangle_{P_i \in C}\,] \;=\; \Pr[\,\Pi(b)_C = \langle s_i \rangle_{P_i \in C}\,].$$

[6] This result does not follow from [33], who impose stronger requirements in their definition of span programs over rings.

The share complexity *of the scheme (or* complexity *for short) is defined as* $\sum_{i=0}^{n-1}\log|S_i|$.

The above correctness and privacy requirements capture the strict notion of *perfect* secret-sharing, which is the one most commonly referred to in the secret-sharing literature. We will also consider a relaxed but natural notion of *statistical* secret-sharing, in which Π accepts an additional argument k, called the *security parameter*, and the perfect correctness and privacy requirements are relaxed to *statistical correctness* and *statistical privacy*, defined as follows.

Statistical correctness. *Any authorized subset of parties can reconstruct the secret s except with* negligible *probability $\epsilon(k)$. That is, for every authorized $B \in \mathcal{A}$ there exists a reconstruction function* Rec_B *such that*

$$\Pr[\,\mathrm{Rec}_B(\Pi(s)_B) = s\,] \geq 1 - \epsilon(k) \tag{1}$$

for some $\epsilon(k) \in k^{-\omega(1)}$.

Statistical privacy. *Any unauthorized subset of parties learns only a negligible amount of information about the secret. That is, for any unauthorized $C \notin \mathcal{A}$ and two secrets $a, b \in S$,*

$$\mathrm{SD}(\Pi(a,k)_C, \Pi(b,k)_C) \leq \epsilon(k) \tag{2}$$

for some $\epsilon(k) \in k^{-\omega(1)}$, where $\mathrm{SD}(Y_0, Y_1)$ *denotes the* statistical distance *between distributions Y_0, Y_1 and is defined by* $\mathrm{SD}(Y_0,Y_1) = \frac{1}{2}\sum_y |\Pr[Y_0 = y] - \Pr[Y_1 = y]|$.[7]

We next define the class of *linear* secret-sharing schemes. There are several equivalent definition for these schemes, see [8].

Definition 2.3 (Linear Secret-Sharing) *Let F be a finite field. A secret-sharing scheme Π is said to be* linear *over F if:*

1. *The secret-domain S is a subset of F.*
2. *There exist $d_0, \ldots, d_{n-1}$ such that each share-domain S_i is a subset of the vector space F^{d_i}.*
3. *The randomized mapping Π can be computed as follows. First, the dealer chooses independent random variables, denoted $r_1, \ldots, r_\ell$, each uniformly distributed over F. Then, each coordinate of each of the n shares is obtained by taking a* linear combination *of $r_1, \ldots, r_\ell$ and the secret s.*

We remark that the notions of perfect secret-sharing and statistical secret-sharing coincide in the case of linear schemes: Any linear scheme that satisfies the weaker conditions of statistical correctness and privacy satisfies the stronger requirements of perfect correctness and privacy.

As for any other concrete complexity measure, we will often implicitly use the term "scheme" for referring to an infinite *family* of schemes $\{\Pi_n\}_{n\in\mathcal{N}}$, parameterized by the number of parties n. In the statistical case, we require the same negligible function $\epsilon(k)$ to apply in Equations (1) and (2) for all Π_n in the family. In the linear case, such a family can have a different underlying field for each n. A family $\{\Pi_n\}_{n\in\mathcal{N}}$ is *efficient* if the complexity of Π_n is polynomial in n (or the complexity of $\Pi_n(k)$ is polynomial in n and k in the statistical case). Note that the above definition does not make any requirement on the computational complexity of the scheme. We say that the scheme is *computationally efficient* if both sharing the secret and reconstructing it can be done in time poly(n,k,$\log|S|$). Finally, the family of access structures $\{\mathcal{A}_n\}$ realized by a scheme family $\{\Pi_n\}$ is naturally identified with a monotone Boolean function $f : \{0,1\}^* \to \{0,1\}$ or its characteristic language.

We next define span programs – a linear algebraic model of computation whose monotone version is equivalent to linear secret-sharing.

[7] Equivalently, the statistical distance between Y_0 and Y_1 may be defined as the maximum, over all functions A, of the *distinguishing advantage* $|\Pr[A(Y_0) = 1] - \Pr[A(Y_1) = 1]|$.

Definition 2.4 (Span Program [42]) *A* span program *over a field F is a triplet $\widehat{M} = \langle M, \rho, \vec{v} \rangle$, where M is an $r \times c$ matrix over F, the vector $\vec{v} \in F^c$ is a non-zero row vector called the* target vector*, and ρ is a labeling of the rows of M by literals from $\{x_0, \bar{x}_0, \ldots, x_{n-1}, \bar{x}_{n-1}\}$ (every row is labeled by one literal, and the same literal can label many rows). A span program $\widehat{M}$ is said to be* monotone *if all of its rows are labeled by positive literals.*

A span program accepts or rejects an input by the following criterion. For every input $y \in \{0,1\}^n$ let M_y denote the sub-matrix of M consisting of those rows whose labels are satisfied by the assignment y. The span program $\widehat{M}$ accepts *y if and only if $\vec{v}$ is in the row-span of M_y (where each row of M is viewed as a vector in F^c). A span program* computes *a Boolean function $f : \{0,1\}^n \to \{0,1\}$ if it accepts exactly those inputs y such that $f(y) = 1$. Note that monotone span programs compute monotone functions. Finally, the* size *of $\widehat{M}$ is the number of* rows *in M.*

The complexity of realizing a given access structure by a linear secret-sharing scheme over F is proportional to the minimal size of a monotone span program over F computing f. Specifically,

Lemma 2.5 ([42, 8]) *An access structure can be realized by a linear secret-sharing scheme over F in which the shares include a total of d field elements if and only if it can be computed by a monotone span program over F of size d.*

It follows from [13, 17, 45, 21] that all functions that have small span programs are in NC. Specifically,

Lemma 2.6 *If a function f has a span program over $F = \mathrm{GF}(q)$ of size ℓ, then f has an arithmetic circuit of size $\mathrm{poly}(\ell)$ and depth $O(\log^2 \ell)$ over F, implying that it has a Boolean circuit of size $\mathrm{poly}(\ell, \log q)$ and depth $O(\log^2 \ell \log\log q)$.*

Quadratic Residues. Let $\mathcal{Z}_u$ be the ring of integers modulo u, whose elements are identified with the integers $\{0, 1, \ldots, u-1\}$. Let $\mathcal{Z}_u^*$ denote the multiplicative group of the elements of $\mathcal{Z}_u$ that are relatively prime to u, that is, the elements of $\mathcal{Z}_u^*$ are $\{1 \leq w < u \ : \ \gcd(w, u) = 1\}$. The number of element in $\mathcal{Z}_u^*$ is denoted by $\varphi(u)$, and is referred to as the Euler function of u.

An integer w is said to be a *quadratic residue* modulo u if $\gcd(w, u) = 1$ and there exists an integer b such that $w \equiv b^2 \bmod u$. It is said to be a *quadratic non-residue* modulo u if $\gcd(w, u) = 1$ and there is no integer b such that $w \equiv b^2 \bmod u$. We will pay particular attention to the case where the modulus is an odd prime p; thus, w and b may be viewed as elements of the field $\mathcal{Z}_p$. In this case, $w \in \mathcal{Z}_p^* = \mathcal{Z}_p \setminus \{0\}$ is said to be a quadratic residue if it is a square of some field element, and a *quadratic non-residue* otherwise. (The element 0 is neither a quadratic residue nor a quadratic non-residue.) The number of quadratic residues modulo p is equal to the number of quadratic non-residues and is $(p-1)/2$. The quadratic residues form a subgroup of the multiplicative group $\mathcal{Z}_p^*$. The *quadratic residuosity problem* is that of deciding, given w and u, whether w is a quadratic residue modulo u. When u is restricted to be a prime (or given the factorization of u) this problem can be solved in polynomial time, but is not known to have an efficient *parallel* algorithm. When u is arbitrary, this problem is widely assumed to be intractable. See Section 3.1 for more details.

3 An Efficient Nonlinear Scheme: The Perfect Case

In this section we construct an efficient nonlinear secret-sharing scheme whose access structure is conjectured not to lie in NC. The scheme constructed in this section is *perfectly* private and correct. A *statistical* scheme realizing a computationally harder access structure will be given in the next section.

Definition 3.1 (The Access Structure $\mathbf{NQRP}_p$) *Let p be an odd prime and $m \stackrel{\text{def}}{=} \lfloor \log p \rfloor$. We define the n-party access structure $\mathbf{NQRP}_p$, where $n \stackrel{\text{def}}{=} 2m$, by specifying its collection of minimal sets. The parties of the access* *structure are denoted by P_i^b, where $0 \le i < m$ and $b \in \{0,1\}$. With each $w \in \{0,1\}^m$ (also viewed as an m-bit integer) we naturally associate a set B_w of size m defined by: $B_w \stackrel{def}{=} \{P_i^{w_i} : 0 \le i < m\}$. A set B is a minimal set of $\mathbf{NQRP}_p$ if:*

- *$B = \{P_i^0, P_i^1\}$ for some $0 \le i < m$, or:*
- *$B = B_w$ for some w such that w is* not *a quadratic residue modulo p. (That is, it is either 0 or a quadratic non-residue.)*

We let $\mathbf{NQRP}$ denote a family of access structures such that the n-th structure is $\mathbf{NQRP}_p$ for some p such that $\lfloor \log p \rfloor = \lfloor n/2 \rfloor$ (say, the least such p).[8]

We next construct a secret-sharing scheme for $\mathbf{NQRP}$.

Theorem 3.2 *For every odd prime p there exists a perfect secret-sharing scheme for $\mathbf{NQRP}_p$ in which the secret-domain is $\{0,1\}$ and the share-domain of each party is $\mathcal{Z}_p$.*

Proof: We prove this theorem by describing the secret-sharing scheme.

The dealer chooses at random $m-1$ random elements $z_0, z_1, \ldots, z_{m-2} \in \mathcal{Z}_p$ and an additional random element $r \in \mathcal{Z}_p^*$. Define $z_{m-1} \stackrel{\text{def}}{=} -\sum_{i=0}^{m-2} z_i$, where here and in the following all arithmetic operations involving ring elements are performed in $\mathcal{Z}_p$. The shares of the parties are specified in Table 2. We turn to prove that this secret-

	$s=0$	$s=1$
P_0^b	$r^2 + z_0$	$br^2 + z_0$
P_i^b $1 \le i < m$	z_i	$2^i br^2 + z_i$

Table 2. A secret-sharing scheme for $\mathbf{NQRP}_p$.

sharing scheme satisfies the correctness and privacy properties with respect to $\mathbf{NQRP}_p$. Let SUM_w denote the sum of the m shares held by parties in B_w. Both the correctness and the privacy proofs will rely on the following lemma.

Lemma 3.3 $\mathrm{SUM}_w = w^s r^2$.

Proof:

- If $s = 0$ then

$$\mathrm{SUM}_w = \sum_{i=0}^{m-1} z_i + r^2 = r^2.$$

- If $s = 1$ then

$$\begin{aligned} \mathrm{SUM}_w &= \sum_{i=0}^{m-1} (z_i + w_i 2^i r^2) \\ &= \sum_{i=0}^{m-1} z_i + r^2 \sum_{i=0}^{m-1} (w_i 2^i) \\ &= r^2 w. \end{aligned}$$

□

[8] To make the access structure ZPP-uniform, p can be chosen to be the least prime in the interval $[2^{\lceil n/2 \rceil}, 2^{\lceil n/2 \rceil} + n]$, or 3 if none exists. However, as for other number-theoretic functions, a random choice of p may be safer when assuming that $\mathbf{NQRP}$ is not in NC.

Correctness. We separately consider two types of minimal authorized sets B:

- $B = \{P_i^0, P_i^1\}$ for some $0 \le i < m$. In this case, $s = 0$ iff the shares of P_i^0 and P_i^1 are equal. This follows from the fact that $2^i r^2 \not\equiv 0 \bmod p$ for every i.

- $B = B_w$ for some w such that w is not a quadratic residue. In this case, it follows from Lemma 3.3 that $s = 0$ iff SUM_w is a quadratic residue (since the product of a quadratic residue and a non quadratic residue is a non quadratic residue).

Privacy. We need to prove that every unauthorized subset $C \notin \mathbf{NQRP}_p$ has no information on the secret. It suffices to prove this claim for every *maximal* C not in the access structure. There are two cases to consider.

- $C = B_w \setminus \left\{P_j^{w_j}\right\}$ for some $w \in \{0,1\}^m$ and $0 \le j < m$. That is, C is a set of size $m-1$ such that for exactly one j it contains neither P_j^0 nor P_j^1. We claim that in this case the share-vector of the parties in C is uniformly distributed in $\mathcal{Z}_p^{m-1}$, regardless of the secret. It suffices to show that for every secret $s \in \{0,1\}$, every possible value of the share-vector from $\mathcal{Z}_p^{m-1}$, and every fixed $r_0 \in \mathcal{Z}_p^*$, there exists a unique choice of $z_0, \ldots, z_{m-2}$ generating this value with $r = r_0$. This can be verified by inspection of the corresponding system of linear equations over $\mathcal{Z}_p$.

- $C = B_w$ for some $w \in \{0,1\}^m$ such that w is a quadratic residue. In this case we claim that, regardless of the value of the secret, the share-vector of the parties in C is uniformly distributed over the m-tuples of field elements whose sum is a quadratic residue. Indeed, by Lemma 3.3, if $s = 0$ then $\text{SUM}_w = r^2$, which is a uniformly random quadratic residue. Furthermore, fixing the choice of r, the choices of z_i induce a uniformly random share vector among all those which sum to r^2. Similarly, if $s = 1$ then $\text{SUM}_w = r^2 w$. Since w is a quadratic residue, SUM_w is again a uniformly random quadratic residue determined by r, and the same argument as above applies.

□

A generalization of our construction for $\mathbf{NQRP}$ is described in Appendix A.

3.1 Does $\mathbf{NQRP}$ Have an Efficient Linear Secret-Sharing Scheme?

The access structure $\mathbf{NQRP}$ we have realized above is related to the problem of deciding quadratic residuosity modulo a prime. We would like to argue that $\mathbf{NQRP}$ is likely not to be in NC, which would imply in particular that $\mathbf{NQRP}$ cannot be efficiently realized by linear schemes. We start by describing some known facts about the complexity of the quadratic residuosity problem.

Unlike quadratic residuosity modulo a composite, whose intractability is commonly assumed in cryptography (see [37]), quadratic residuosity modulo a prime can be decided in polynomial time. All known algorithms for this problem are sequential. It is not known if efficient parallel algorithms for this problem exist; that is, the situation is similar to the exponentiation function and the gcd function. There are two types of known algorithms. The first uses Euler's criterion, which states that w is a quadratic residue modulo an odd prime p iff $w^{(p-1)/2} \equiv 1 \bmod p$. Thus, this algorithm requires modular exponentiation. For a survey of algorithms for exponentiation see [38]. The second type of algorithm computes the Jacobi symbol in a way similar to Euclid's algorithm for computing the gcd. For more details see, e.g., [5, Chapter 5]. "Weak" parallel algorithms for checking quadratic residuosity follow from the algorithms of [32] for computing the Jacobi symbol and the algorithm of [1] for exponentiation. More precisely, there is (1) an algorithm that runs in $O(n/\log\log n)$ time using $O(n^{1+\epsilon})$ processors [32]; (2) an algorithm that runs in $O(\log^2 n \log\log n)$ time using $2^{O(n/\log n)}$ processors [32]; (3) an algorithm that runs in $O(\log^3 n)$ time using $2^{O(\sqrt{n \log n})}$ processors [1].

The best known polynomial-size circuit for the quadratic residuosity problem has depth $O(n/\log\log n)$ where $n = \log p$ [32]. Thus, given the current state of knowledge on this problem and the related modular exponentiation problem, it is reasonable to assume that they are not in NC. In fact, this assumption (for the exponentiation problem) has been explicitly relied on in [16].

It is easy to see that deciding quadratic residuosity modulo p can be very efficiently reduced to computing the monotone function defined by $\mathbf{NQRP}_p$. However, there is a major difference between the "standard" algorithmic setting for this problem and our setting. Our setting is highly non-uniform, in the sense that with each input length (or number of parties) we associate some *fixed* prime p. Hence, when computing this access structure one may use a non-uniform "advice" depending on p. In algorithmic terms, we allow unlimited preprocessing which depends on the prime p but not on the other input w. Nevertheless, we do not know how to use this type of preprocessing to obtain an efficient parallel algorithm for the quadratic residuosity problem.[9] (It is interesting to note, however, that deciding quadratic residuosity modulo a *composite* is no more difficult in our setting than deciding quadratic residuosity modulo a prime, since the factorization of the composite may be used as advice.) To conclude, the assumption that $\mathbf{NQRP} \notin \mathrm{NC}$ is stronger than the assumption that the standard quadratic residuosity problem (or modular exponentiation) is not in NC, although still seems very reasonable given the current state of knowledge.

In light of the uncertain situation described above, one could hope for an unconditional super-polynomial lower bound on a size of a *monotone span program* computing $\mathbf{NQRP}$. This would be sufficient for proving that $\mathbf{NQRP}$ cannot be efficiently realized by linear schemes and, as noted in the introduction, there are explicit monotone functions for which such bounds are known. However, as we argue next, such lower bounds are impossible to prove for the $\mathbf{NQRP}$ structure without proving that $\mathrm{NC}^1 \neq \mathrm{P}$. For a fixed $(m+1)$-bit prime p, the quadratic residuosity function (modulo p) is defined as: $f_p(x_0, \ldots, x_{m-1}) = 1$ iff $\sum_{i=0}^{m-1} x_i 2^i$ is a quadratic residue modulo p. This function is not monotone. To define the monotone access structure $\mathbf{NQRP}$ we replaced each literal by two parties, obtaining an access structure with $2m$ parties. (This is a standard transformation, e.g., when proving that monotone circuit evaluation is P-complete [36].) For technical reasons we also added m minterms of size two. It follows that the monotone formula size of $\mathbf{NQRP}_p$ is *equal*, up to an additive $O(n)$ difference, to the (non-monotone) formula size of the function f_p. Thus, one cannot expect to prove strong lower bounds on the size of a monotone span program (or even a monotone formula) for $\mathbf{NQRP}$, since they will imply, in particular, strong lower bounds on the (non-monotone) formula size of the quadratic residuosity function.[10]

4 An Efficient Nonlinear Scheme: The Statistical Case

In this section we construct an efficient nonlinear secret-sharing scheme whose access structure is as hard as the general quadratic residuosity function. Unlike the previous construction, the scheme we construct below is only statistically private and correct, and its reconstruction procedure is computationally inefficient. In Section 4.1 we show that perfect correctness (but not perfect privacy) can be achieved under a number-theoretic assumption. We end this section by discussing a generalization of our construction which applies to the so-called t-residuosity problem. As a special case, we obtain an efficient scheme whose access structure is computationally equivalent to the co-primality problem.

Definition 4.1 (The Access Structure $\mathbf{NQR}_m$) *Let m be a positive integer. We define the n-party access structure $\mathbf{NQR}_m$, where $n \stackrel{def}{=} 4m$, by specifying its collection of minimal sets. It will be convenient in the following to denote the first $2m$ parties by W_i^b, where $b \in \{0,1\}$ and $0 \leq i < m$, and the last $2m$ parties by U_i^b. With each pair (w,u), where $w, u \in \{0,1\}^m$, we naturally associate a subset of parties $B_{w,u}$ of size $2m$, defined by:*

$$B_{w,u} \stackrel{def}{=} \{W_i^{w_i} : 0 \leq i < m\} \cup \{U_i^{u_i} : 0 \leq i < m\}.$$

[9] Preprocessing can parallelize the algorithms for exponentiation when the field size and the exponentiation base are given in advance (see [38]). However, in our case we know in advance the field size and the exponentiation power.

[10] The best known lower bound on the formula size for an explicit function is $\Omega(n^{3-o(1)})$ [39].

We will freely identify strings w, u as above with integers in the interval $[0, 2^m - 1]$. A set B is a minimal set of $\mathbf{NQR}_m$ if:

1. *$B = \{W_i^0, W_i^1\}$ or $B = \{U_i^0, U_i^1\}$ for some $0 \le i < m$, or:*
2. *$B = B_{w,u}$ for some w, u such that w is* not *a quadratic residue modulo u. (For technical reasons, we assume here that this condition never holds when $u = 1$, and always holds when $u = 0$ except when $w = 1$.)*

We let $\mathbf{NQR}$ denote the family of access structures in which the n-th structure is $\mathbf{NQR}_{\lfloor n/4 \rfloor}$.

We start by observing that the computational complexity of the access structure $\mathbf{NQR}$ is essentially the same as that of the general quadratic residuosity problem.

Claim 4.2 *The circuit complexity of $\mathbf{NQR}$ is the same, up to an $O(n)$ difference, as that of the language $\{(w, u) : |w| = |u| \wedge a \text{ is w quadratic residue modulo } u\}$.*

It follows that under the Quadratic Residuosity Assumption [37], computing $\mathbf{NQR}$ requires circuits of super-polynomial size. The remainder of this section will be devoted to proving the existence of an efficient nonlinear secret-sharing scheme for $\mathbf{NQR}$. Specifically, we show:

Theorem 4.3 *There exists a statistical secret-sharing scheme for $\mathbf{NQR}_m$ in which:*

- *the secret-domain is $\{0, 1\}$;*
- *the share size of each party is $O(k^2 + km)$;*
- *the reconstruction error probability is 2^{-k};*
- *the privacy level is $\epsilon(k) = O(k/2^k)$.*

Our secret-sharing scheme for $\mathbf{NQR}_m$ proceeds as follows. Let $D \stackrel{\text{def}}{=} 2^{4m+3k+1}$. In the following, all arithmetic operations will be performed in $\mathcal{Z}_D$. The dealer chooses $z_0, z_1, \ldots, z_{2m-1} \in \mathcal{Z}_D$ at random subject to the restriction that they sum to 0. In addition, it chooses two random integers $1 \le r \le 2^{m+k}$ and $1 \le r' \le 2^{3(m+k)}$. Each party receives a single element of $\mathcal{Z}_D$, as specified in Table 3. For amplifying the correctness probability,

	$s = 0$	$s = 1$
W_0^b	$r^2 + z_0$	$br^2 + z_0$
W_i^b $1 \le i < m$	z_i	$2^i br^2 + z_i$
U_i^b $0 \le i < m$	$2^i br' + z_{i+m}$	$2^i br' + z_{i+m}$

Table 3. A secret-sharing scheme for $\mathbf{NQR}_m$.

the above distribution procedure should be independently repeated k times, so that each party receives k elements of $\mathcal{Z}_D$. In addition, the minimal authorized sets of size 2 should be taken care of separately, by independently sharing s among each such authorized pair (that is, for each such pair choose an independent random bit α, and give α to the first party and $\alpha \oplus s$ to the second).[11] This only adds a single bit to the size of each share. The following analysis will mostly focus on the core of the scheme, as described in Table 3.

[11]In fact, as in the previous construction this additional sharing is unnecessary for sets of the form $\{W_i^0, W_i^1\}$.

Let $\mathrm{SUM}_{w,u}$ be the sum of the $2m$ shares held by parties in $B_{w,u}$.
If $\gcd(w,u) = 1$ then (* w is a quadratic non-residue modulo u *)
    If $\mathrm{SUM}_{w,u}$ is quadratic residue modulo u then $s = 0$ else $s = 1$
If $\gcd(w,u) \neq 1$ then
    Let $c = \gcd(w,u)$
    If c divides $\mathrm{SUM}_{w,u}$ then $s = 1$ else $s = 0$

Figure 1. Reconstruction Procedure for $B_{w,u}$ in $\mathbf{NQR}_m$.

Statistical correctness. The minimal authorized sets of size 2 were explicitly taken care of in the above construction. It thus remains to prove the correctness for a subset $B_{w,u}$, where w is not a quadratic residue modulo u. If r were chosen such that $\gcd(r,u) = 1$ then the correctness would follow from similar arguments to those of the proof for $\mathbf{NQRP}$ (that is, the secret is reconstructed by checking if the sum of shares is a quadratic residue). However, since here u is not fixed, we cannot guarantee that the above condition always holds. Nevertheless, this already implies that the secret can be correctly reconstructed from the shares in Table 3 with a one-sided error probability of at most $1 - \varphi(u)/u$, which is bounded away from 1. The following tighter analysis shows that the one-sided error probability of reconstruction can be as low as $1/2$. Hence, with k independent repetitions the error probability is at most 2^{-k}. In Figure 1 we present the reconstruction procedure and then prove its correctness. The following lemma can be verified by inspection of Table 3.

Lemma 4.4 *For any $0 \leq w, u < 2^m$ and secret $s \in \{0,1\}$, it holds that $\mathrm{SUM}_{w,u} = r^2 w^s + r'u$ (where $\mathrm{SUM}_{w,u}$ is the sum of the $2m$ shares held by parties in $B_{w,u}$).*

Note that by our choice of parameters, the expression $r^2 w^s + r'u$ in Lemma 4.4 is always less than D. We will therefore treat this expression as being evaluated over the integers.

From now on, we assume that $u \geq 2$ (the case that $u = 0$ and $w \neq 1$ can be verified separately). Suppose first that $\gcd(w,u) = c > 1$. In this case, c always divides $r^2 w + r'u$, whereas c divides $r^2 + r'u$ if and only if c divides r. Thus, with probability at least $1 - 1/c \geq 1/2$ it does not divide $r^2 + r'u$. It follows that when $\gcd(w,u) > 1$ the case $s = 0$ can be distinguished from the case $s = 1$ with a one-sided error probability of at most $1/2$, as described above.

Now suppose that w is a quadratic non-residue modulo u. In this case, $r^2 + r'u \equiv r^2 \bmod u$ is always a square modulo u. This implies that $\mathrm{SUM}_{w,u}$ is a quadratic residue when $s = 0$. The following lemma shows that with probability at least $1/2$, this is not the case for $r^2 w + r'u$, i.e., when $s = 1$.

Lemma 4.5 *Suppose that w is a quadratic non-residue modulo u (in particular, $\gcd(w,u) = 1$). Then, the probability that $r^2 w$ is a quadratic residue modulo u is at most $1/2$.*

Proof: By the Chinese Remainder Theorem, a number is a quadratic-residue modulo u if and only if it is a quadratic-residue modulo each prime power dividing u. Thus, there exists a prime power p^α dividing u such that w is a quadratic non-residue modulo p^α. Now, if wr^2 is a square modulo u, then it is also a square modulo p^α, and so there exists d such that $d^2 \equiv wr^2 \bmod p^\alpha$. We argue that it must be the case that p divides r. Otherwise, r has an inverse modulo p^α and $w \equiv (d/r)^2 \bmod p^\alpha$ contradicting the fact that w is a quadratic non-residue modulo p^α. The lemma follows by noting that the probability that p divides r is at most $1/p \leq 1/2$, as required. $\square$

This concludes the analysis of the reconstruction procedure described above. Note that this reconstruction procedure is computationally inefficient if the factorization of u is unknown.

Statistical privacy. We now prove the privacy of our construction. As before, it suffices to consider maximal unauthorized sets of two types. The first type consists of sets C such that $|C| < 2m$ and C does not contain a pair W_i^0, W_i^1 or a pair U_i^0, U_i^1. For such a set C, it can be verified that the shares received by its parties are uniformly and independently distributed over $\mathcal{Z}_D$, regardless of the secret s.

We turn to the more interesting case of a set $C = B_{w,u}$ such that $u \geq 2$ and w is a quadratic residue modulo u. (The cases $u = 1$ and $u = 0, w = 1$ can be verified separately.) When $s = 0$ the shares are otherwise random numbers whose sum is $r^2 + r'u$, and when $s = 1$ the shares are otherwise random integers whose sum is $r^2 w + r'u$. Thus, it suffices to show that in this case $\text{SD}(r^2 + r'u, r^2 w + r'u) = O(2^{-k})$. We prove this using the following lemmas. In the lemmas we denote by r, r' the random variables used in the scheme (taking uniform integral values from the intervals $[1, 2^{m+k}]$ and $[1, 2^{3(m+k)}]$, respectively). For the proof we also use an additional random variable r_u which is a uniformly distributed integer in $[0, u-1]$.

Lemma 4.6 *If w is a quadratic residue modulo u, then the distribution of $(wr_u^2) \bmod u$ is identical to that of $r_u^2 \bmod u$.*

Proof: Since w is a quadratic residue modulo u, there exists b such that $\gcd(b, u) = 1$ and $b^2 \equiv w \bmod u$. Since $wr_u^2 \equiv (br_u)^2 \bmod u$, it suffices to show that $(br_u) \bmod u$ is identically distributed to $r_u \bmod u = r_u$. Finally, since $\gcd(b, u) = 1$, i.e., b has an inverse modulo u, then for every value β it holds that $\Pr[br_u \equiv \beta] = \Pr[r_u \equiv (\beta/b)] = 1/u$. $\square$

Lemma 4.7 $\text{SD}(r^2 \bmod u\, ,\, r_u^2 \bmod u) \leq 2^{-k}$.

Proof: Recall that r is chosen uniformly from the interval $[1, 2^{m+k}]$. If u divides 2^{m+k} then the above two distributions are identical. Otherwise, the contribution of each $y \in [0, u-1]$ to this distance is at most $1/2^{m+k}$, and since $u < 2^m$ the total contribution is at most $2^m/2^{m+k} = 2^{-k}$. $\square$

From the previous two lemmas, we may conclude that

$$\text{SD}(wr^2 \bmod u, r^2 \bmod u) = O(2^{-k}). \tag{3}$$

Now, define the multisets

$$V = \left\{ wr^2 \bmod u \,:\, 1 \leq r \leq 2^{m+k} \right\}$$

and

$$Z = \left\{ r^2 \,:\, 1 \leq r \leq 2^{m+k} \right\}.$$

Let Z' be a maximal multiset such that $Z' \subseteq Z$ and $Z' \bmod u \stackrel{\text{def}}{=} \{z \bmod u \,:\, z \in Z'\} \subseteq V$. It follows from Eq. (3) that $|Z'| = (1 - O(2^{-k}))|Z|$. Define $S = Z' \cup (V \setminus (Z' \bmod u))$. Note that $|S| = |V| = 2^{m+k}$. We will denote the elements of S by $y_1, \ldots, y_{2^{m+k}}$ and the uniform distribution over S by Y. It follows from the above that Y satisfies: (1) $\text{SD}(Y, r^2) = O(2^{-k})$; (2) the distribution of $Y \bmod u$ is *identical* to that of $ar^2 \bmod u$; and (3) $Y \leq 2^{2(m+k)}$.

We would like to conclude that $\text{SD}(wr^2 + r'u, r^2 + r'u) = O(2^{-k})$. To this end, we use the following lemma.

Lemma 4.8 *Let y, z be two integers in some interval $[0, M]$ such that $y \equiv z \bmod u$, and let R be uniformly distributed in the interval $[1, MK]$. Then,* $\text{SD}(y + Ru\, ,\, z + Ru) \leq 1/K$.

Proof: The statistical distance is bounded by $|y - z|/(uMK) \leq M/(uMK) < 1/K$. $\square$

We are now ready to complete the proof of privacy. From Property (1) of Y it follows that

$$\text{SD}(Y + r'u, r^2 + r'u) = O(2^{-k}). \tag{4}$$

From property (2) of Y, we may assume that $y_r \equiv wr^2 \bmod u$ for every $1 \leq r \leq 2^{m+k}$. Letting $M = 2^{3m+2k}$ and $K = 2^k$, both Y and wr^2 are no larger than M, and r' is uniform in $[1, MK]$. Since

$$\mathrm{SD}(Y + r'u, wr^2 + r'u) \leq E_r[\mathrm{SD}(y_r + r'u, wr^2 + r'u)]$$

it follows from Lemma 4.8 that

$$\mathrm{SD}(Y + r'u, wr^2 + r'u) \leq 2^{-k}. \tag{5}$$

Combining Eq. (4) and Eq. (5) we get that $\mathrm{SD}(wr^2 + r'u, r^2 + r'u) = O(2^{-k})$, as required.

As explained above, to reduce the error probability in the reconstruction from $1/2$ to 2^{-k} we share the secret independently k times. By standard arguments, this can only increase the statistical distance to $O(k/2^k)$, which is still negligible in k.

4.1 A Perfectly Correct Scheme

In this section we show that under the Extended Riemann Hypothesis (abbreviated ERH), one can obtain a variant of the above scheme which is *perfectly* correct, though still only statistically private. (It is open if there is a scheme with perfect correctness and privacy which efficiently realizes $\mathbf{NQR}$.) The only required modification is the choice of r: instead of choosing it uniformly from the interval $[1, 2^{m+k}]$, it is chosen as a random *prime* from the interval $[2^m, 2^{m+k}]$. Since $u < 2^m$, this guarantees that r is relatively prime to u, and this in turn is sufficient to guarantee perfect correctness. We next argue that under the ERH, the resulting scheme is statistically private.

We will need the following results on the distribution of primes. For more information on this subject the reader might consult, e.g., [5, Chapter 8]. For an integer x let $\pi(x)$ be the number of primes in the interval $[1, x]$, and for integers x, w and u let $\pi(x, u, w)$ be the number of primes in the interval $[1, x]$ that are congruent to $w \bmod u$. It is known that $\pi(x) \approx x/\log x$. If $\gcd(w, u) > 1$ then every number that is congruent to $w \bmod u$ is a composite. It turns out that the primes are nearly uniformly distributed among the other residue classes modulo u. That is, if $\gcd(w, u) = 1$ then $\pi(x, u, w) \approx \frac{1}{\varphi(u)} x/\log x$, where $\varphi(u)$ is the Euler function of u.

We will need good bounds on the error terms in the above approximations. The bounds that can be proved unconditionally are too crude for our purpose, and we will need bounds based on the the Extended Riemann Hypothesis. Proving this famous hypothesis is one of the most important open questions in mathematics. We will not formulate the statement of this hypothesis, and only state the following conclusion from the ERH. The estimations that are used to derive the next theorem are presented in Appendix B.

Theorem 4.9 *If the ERH holds and* $\gcd(w, u) = 1$ *then for every x and x', where $u \leq x' \leq \sqrt{x}$,*

$$\left| \frac{\pi(x, u, w) - \pi(x', u, w)}{\pi(x) - \pi(x')} - \frac{1}{\varphi(u)} \right| = O\left(\frac{\log^2 x}{\sqrt{x}} \right),$$

where the constant in the "O" notation is an absolute constant independent of w and u.

Notice that $\frac{\pi(x,u,w) - \pi(x',u,w)}{\pi(x) - \pi(x')}$ is the probability that a uniformly random prime in the interval $[x', x]$ is congruent to u modulo w. Thus, the above theorem states that this probability is close to the probability that a uniformly random element from $\mathcal{Z}_u^*$ is equal to w.

Corollary 4.10 *Let $u < 2^m$, U be a random variable distributed uniformly in $\mathcal{Z}_u^*$, and r be a uniformly chosen prime in the interval $[2^m, 2^{m+k}]$. If ERH holds then for every k, m such that $k \leq 2m$ it holds that* $\mathrm{SD}(U, r \bmod u) \leq 2^{-\Omega(k)}$*, and in particular* $\mathrm{SD}(U^2 \bmod u, r^2 \bmod u) \leq 2^{-\Omega(k)}$.

Proof:

$$
\begin{aligned}
&\mathrm{SD}(U, r \bmod u) \\
&= \frac{1}{2} \sum_{y \in \mathcal{Z}_u^*} |\Pr[U = y] - \Pr[r \bmod u = y]| \\
&\leq \varphi(u) \cdot O\left(\frac{(m+k)^2}{\sqrt{2^{m+k}}}\right) \\
&= O\left(\frac{2^m (m+k)^2}{2^{0.5(m+k)}}\right) = 2^{-\Omega(k)}.
\end{aligned}
$$

The last equality holds since $k \geq 2m$. □

To guarantee that the statistical distance decreases exponentially with the security parameter *independently of* m, we execute the scheme with $k' = \max(k, 2m)$. Closely following the privacy proof of the previous protocol (and replacing Lemma 4.7 with Corollary 4.10), one can show that the scheme is statistically private with $\epsilon(k) = 2^{\Omega(-k)}$. The next theorem summarizes the properties of this scheme.

Theorem 4.11 *If ERH holds, then there exists a statistical secret-sharing scheme for* $\mathbf{NQR}_m$ *with perfect correctness in which:*

- *the secret-domain is* $\{0, 1\}$*;*
- *the share size of each party is* $O(k + m)$*;*
- *the privacy level is* $\epsilon(k) = 2^{-\Omega(k)}$.

4.2 Schemes for t-residuosity

The quadratic residuosity problem naturally generalizes to the t-residuosity problem defined as follows. An integer w is a t-residue modulo u if $\gcd(w, u) = 1$ and there exists an integer b such that $w \equiv b^t \bmod u$. The access structure $\mathbf{N}t\mathbf{R}$ is defined as the access structure $\mathbf{NQR}$, with quadratic residuosity replaced by t-th residuosity.

A scheme for $\mathbf{N}t\mathbf{R}$ can be obtained by the following small modification to the scheme for $\mathbf{NQR}$: the ring size D is changed to $2^{(t+2)m+(t+1)k+1}$, the random string r' is chosen with uniform distribution from $[1, 2^{(t+1)(t+k)}]$, and in the dealer's distribution procedure we replace r^2 by r^t. The correctness and privacy of the modified scheme are argued similarly to the original scheme. These modification also work in the scheme based on the ERH.

An interesting special case of the general scheme is when $t = 1$. In the resultant scheme, $B_{w,u}$ can reconstruct the secret iff the integers w and u are not co-primes (i.e., $\gcd(w, u) > 1$). Hence, its access structure is computationally equivalent to the co-primality problem. Checking if two integers are co-prime is clearly in P, and it is not known to be in NC. An important feature of this instance of the general construction is that it is computationally efficient: indeed, reconstruction only requires checking if $\gcd(w, u)$ divides $\mathrm{SUM}_{w,u}$.

5 Quasi-Linear Secret-Sharing

In this section we study a natural extension of the class of linear secret-sharing schemes to what we call *quasi-linear* schemes. Quasi-linear schemes are obtained by *composing* a finite number of linear secret-sharing schemes, possibly over different fields.

Towards defining quasi-linear schemes, it will be convenient to use the following notation for extending the secret-domain of a given secret-sharing scheme to an arbitrarily large finite domain.

Definition 5.1 *Let Π be a secret-sharing scheme with secret-domain S and share-domains $S_0, \ldots, S_{n-1}$, let $T = \{0, 1, \ldots, |T| - 1\}$ be any finite secret-domain, and let $\ell = \lceil \log_{|S|} |T| \rceil$. Then, by $\tilde{\Pi}_T$ we denote the randomized mapping from T to $S_0^\ell \times \cdots \times S_{n-1}^\ell$ defined as follows. For a secret $t \in T$, let $(t_1, \ldots, t_\ell)$ denote its base-$|S|$ representation, where $t_i \in S$ for all i. The output of $\tilde{\Pi}_T(t)$ is obtained by independently applying Π to each t_i and letting the i-th entry of the output be the concatenation of the i-th entries from the ℓ outputs of Π.*

As can be easily seen, $\tilde{\Pi}_T$ defines a secret-sharing scheme realizing the same access structure as Π, whose secret-domain is T and whose share-complexity is $\ell = \lceil \log_{|S|} |T| \rceil$ times that of Π. We are now ready to formally define the notion of quasi-linear schemes.

Definition 5.2 *An n-party quasi-linear secret-sharing scheme is recursively defined as follows:*

1. *Any n-party linear secret-sharing scheme is an n-party quasi-linear scheme.*
2. *Suppose that Π is an n'-party linear scheme over a field F with share-domains $S_0, \ldots, S_{n'-1}$, and let $\Pi^0, \ldots, \Pi^{n'-1}$ be n-party quasi-linear schemes. Then, define an n-party quasi-linear scheme $\Pi(\Pi^0, \ldots, \Pi^{n'-1})$ with secret-domain F as follows. To share $s \in F$, first apply $\Pi(s)$ to obtain shares $s_0, \ldots, s_{n'-1}$. Then, identifying each share-domain S_i with the set $\{0, 1, \ldots, |S_i| - 1\}$, independently share each s_i among the n parties using $\tilde{\Pi}^i_{S_i}$.*

It is convenient to view an n-party quasi-linear scheme Π as a tree, in which every node contains a linear secret-sharing scheme. Associating each linear scheme with its corresponding monotone span program, we may view this tree as a Boolean formula φ_Π over the basis of all monotone span programs (over all finite fields);[12] that is, each gate in the formula computes the Boolean function computed by a monotone span program. For brevity we refer to such a formula as an *MSP-formula*.

The following proposition establishes the correspondence between a quasi-linear scheme and its associated MSP-formula. Its straightforward proof, generalizing the proof for the AND-OR-Threshold formula construction from [11], is omitted from this abstract.

Proposition 5.3 *Let Π be a quasi-linear secret-sharing scheme and φ_Π be the corresponding MSP-formula. Then, Π realizes the access structure computed by φ_Π.*

Are quasi-linear schemes strictly stronger than linear schemes, or can every quasi-linear scheme be simulated by a linear scheme with a polynomial complexity overhead? Given the current understanding of monotone span program complexity, no conclusive answer can be obtained. However, under the plausible assumption that the power of monotone span programs over fields of different characteristics is incomparable, quasi-linear schemes are indeed (super-polynomially) stronger. This unsurprising observation can be formally argued by embedding two or more monotone span programs over different fields as restrictions of one efficient MSP-formula. For instance, suppose that f (respectively, g) can be efficiently computed by a monotone span program over GF(2) (resp., GF(3)), but has $n^{\omega(1)}$ monotone span program size over any field whose characteristic is different from 2 (resp., 3). Then, the function $h = (y \wedge f) \vee (z \wedge g)$, where the variables y, z appear neither in f nor in g, can be efficiently realized by a quasi-linear scheme, but cannot be efficiently realized by any linear scheme.

However, as we show next, quasi-linear schemes cannot be too powerful. More specifically, if there is an efficient quasi-linear scheme for f then f can be computed by a shallow circuit. The idea of the proof is to consider the corresponding MSP-formula φ. We use a result of [7] showing that a formula φ over a general basis can be "balanced" to obtain an equivalent formula whose depth is small and its size is not too big (this is a generalization of the well-known result from [51] for bounded fan-in formulae over the standard basis). An instantiation of this result which is useful for our purposes is quoted in the following lemma.

[12] An input variable is viewed as a size-1 monotone span program in the variables $x_0, \ldots, x_{n-1}$ returning its value.

Lemma 5.4 (Beigel and Fu [7]) *Let φ be a MSP-formula. Then, there exists a MSP-formula $\hat{\varphi}$ such that: (1) $\hat{\varphi}$ computes the same function as φ; (2) the depth of $\hat{\varphi}$ is $O(\log(\mathrm{size}(\varphi)))$; (3) the size of $\hat{\varphi}$ is $\mathrm{size}(\varphi)^{O(1)}$; and (4) each node of $\hat{\varphi}$ is either labeled by some span program appearing in φ, or is labeled by an AND, OR, or NOT gate.*

Theorem 5.5 *Suppose that f is efficiently realized by quasi-linear schemes. Then, $f \in \mathrm{NC}^4$.*

Proof: Let Π be an efficient quasi-linear scheme realizing f, and let φ be the corresponding MSP-formula. We may assume without loss of generality that the span program labeling each *internal* node of φ depends on all of its inputs, and has at least two inputs; otherwise Π could be simplified into a quasi-linear scheme Π' whose MSP-formula φ' satisfies this property. As the number of leaves in such a φ is a lower bound on the complexity of Π (and the degree of each internal node of φ is at least 2), φ must be of size $\mathrm{poly}(n)$. It also follows that each node v of φ must be labeled by a *polynomial-size* monotone span program M_v over a field $\mathrm{GF}(q_v)$ such that $\log q_v = \mathrm{poly}(n)$.[13] By Lemma 2.6, the function f_v computed by M_v can be simulated by a Boolean circuit of size $\mathrm{poly}(n)$ and depth $O(\log^3 n)$. The theorem follows by applying Lemma 5.4 to φ and replacing each node in $\hat{\varphi}$ by a corresponding NC^3 circuit. □

We conclude this section by showing an application of quasi-linear schemes for the construction of secret-sharing schemes efficiently realizing monotone span programs over a ring $\mathcal{Z}_u$, where u is a square-free composite.[14]

Theorem 5.6 *Let M be a monotone span program over $\mathcal{Z}_u$, where u is the product of k distinct primes $p_1, \ldots, p_k$. Then, there exists a quasi-linear scheme Π_M realizing the access structure defined by M, whose share-complexity is $\mathrm{size}(M) \cdot \sum_{j=1}^{k} \log p_j$.*

Proof: Π_M is defined by the following depth-2 MSP-formula φ_M. The root contains an AND gate with fan-in k (represented by a size-k monotone span program over GF(2)). The j-th leave, $1 \le j \le k$, contains a monotone span program M_j over $\mathrm{GF}(p_j)$, obtained from M by reducing each of its entries modulo p_j. By Proposition 5.3, to prove that Π_M indeed realizes the access structure defined by M it suffices to show that φ_M computes the same function as M. Indeed, if $M(x) = 1$, then clearly $M_j(x) = 1$ for all j (as witnessed by the same linear combination, modulo p_j). The converse follows by applying the Chinese Remainder Theorem to the k linear combination vectors witnessing that $M_j(x) = 1$, $1 \le j \le k$. □

Example 5.7 Figure 2 shows an efficient span program over $\mathcal{Z}_u$ for testing whether the input x (viewed as an integer) is co-prime to u. Replacing each negative literal with a new variable, this example gives a very efficient quasi-linear scheme for a monotone access structure derived from the co-primality problem.[15]

6 Open Problems

The main open problem in this area remains that of characterizing the class of access structures admitting efficient secret-sharing. A more modest problem is to obtain an *unconditional* separation between the access structures which can be efficiently realized by linear schemes and those efficiently realized by general (nonlinear)

[13] The converse does not hold. It is easy to construct a polynomial-size MSP-formula (even a shallow one) which is efficient in this sense, but whose corresponding quasi-linear scheme is inefficient.

[14] Span programs over rings are defined in a completely analogous way to span programs over fields.

[15] Whether x is co-prime to u can be tested in NC^1 given an advice depending on u (namely, its factorization). Hence, there exist efficient linear secret-sharing schemes for this access structure. Still, the exact efficiency of the quasi-linear scheme is much better. See Example A.2 for an efficient nonlinear realization which does not rely on the factorization of u.

$$
\begin{array}{c|cccccc}
\bar{x}_0 & 0 & 1 & 0 & 0 & \cdots & 0 \\
x_0 & 1 & 1 & 0 & 0 & \cdots & 0 \\
\bar{x}_1 & 0 & -1 & 1 & 0 & \cdots & 0 \\
x_1 & 2 & -1 & 1 & 0 & \cdots & 0 \\
\vdots & \vdots & & & & & \vdots \\
\bar{x}_{n-2} & 0 & 0 & \cdots & 0 & -1 & 1 \\
x_{n-2} & 2^{n-2} & 0 & \cdots & 0 & -1 & 1 \\
\bar{x}_{n-1} & 0 & 0 & \cdots & 0 & 0 & -1 \\
x_{n-1} & 2^{n-1} & 0 & \cdots & 0 & 0 & -1 \\
\hline
\text{target} & 1 & 0 & \cdots & 0 & 0 & 0
\end{array}
$$

Figure 2. A span program over $\mathcal{Z}_u$ testing whether $\gcd(x, u) = 1$.

schemes. As indicated in Section 5, it suffices to prove strong separations between monotone span program complexity over fields of different characteristics.

We next suggest a candidate for a function that has a small monotone span program over $\mathrm{GF}(2)$ and does not have small monotone span program over fields of different characteristic. The candidate is the ODD-FACTOR function considered in [2]: The function has $n = v^2$ variables; the input is a bipartite graph with v vertices in each part represented by a $(0, 1)$-matrix of size $v \times v$. The graph is accepted if it has an odd factor, i.e., a spanning subgraph such that all vertices have odd degree in the subgraph. Babai, Gál, and Wigderson [2] prove that this function has a small monotone span program over $\mathrm{GF}(2)$, but has only exponential monotone formulae and quasi-polynomial monotone circuits. The open problem is whether the ODD-FACTOR function has small monotone span program over fields of a different characteristic.

Acknowledgments. The first author would like to thank Daniel Berend and Yuval Ginosar for helpful discussions. The second author would like to thank Eric Allender and Dieter van-Melkebeek for helpful discussions and pointers.

References

[1] L. M. Adleman and K. Kompella. Using smoothness to achieve parallelism. In *Proc. of the 20th Annu. ACM Symp. on the Theory of Computing*, pages 528–538, 1988.

[2] L. Babai, A. Gál, and A. Wigderson. Superpolynomial lower bounds for monotone span programs. *Combinatorica*, 19(3):301–319, 1999.

[3] L. Babai, P. G. Kimmel, and S. V. Lokam. Simultaneous messages vs. communication. In *12th Annual Symposium on Theoretical Aspects of Computer Science*, volume 900 of *Lecture Notes in Computer Science*, pages 361–372. Springer, 1995.

[4] L. Babai, N. Nisan, and M. Szegedy. Multiparty protocols and logspace-hard pseudorandom sequences. In *Proc. of the 21st Annu. ACM Symp. on the Theory of Computing*, pages 1–11, 1989.

[5] E. Bach and J. Shalit. *Algorithmic Number Theory*, volume 1: Efficient Algorithms. MIT press, 1996.

[6] P. Beguin and A. Cresti. General short computational secret sharing schemes. In L. C. Guillou and J. J. Quisquater, editors, *Advances in Cryptology – EUROCRYPT '95*, volume 921 of *Lecture Notes in Computer Science*, pages 194–208. Springer, 1995.

[7] R. Beigel and B. Fu. Circuits over PP and PL. *J. of Computer and System Sciences*, 60:422–441, 2000. Preliminary version in the proceedings of the 12th Annual IEEE Conference on Computational Complexity, pp. 24-35, 1997.

[8] A. Beimel. *Secure Schemes for Secret Sharing and Key Distribution*. PhD thesis, Technion – Israel Institute of Technology, 1996.

[9] A. Beimel, A. Gál, and M. Paterson. Lower bounds for monotone span programs. *Computational Complexity*, 6(1):29–45, 1997. Conference version: FOCS '95.

[10] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for noncryptographic fault-tolerant distributed computations. In *Proc. of the 20th Annu. ACM Symp. on the Theory of Computing*, pages 1–10, 1988.

[11] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In S. Goldwasser, editor, *Advances in Cryptology – CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 27–35. Springer-Verlag, 1990.

[12] J. Benaloh and S. Rudich. Private communication, 1989.

[13] S. J. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Inform. Process. Lett.*, 18:147–150, 1984.

[14] G. R. Blakley. Safeguarding cryptographic keys. In R. E. Merwin, J. T. Zanca, and M. Smith, editors, *Proc. of the 1979 AFIPS National Computer Conference*, volume 48 of *AFIPS Conference proceedings*, pages 313–317. AFIPS Press, 1979.

[15] C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro. On the information rate of secret sharing schemes. *Theoretical Computer Science*, 154(2):283–306, 1996.

[16] D. Boneh and M. Naor. Timed commitments. In *Advances in Cryptology – CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 236–254. Springer-Verlag, 2000.

[17] A. Borodin, J. v. z. Gathen, and J. Hopcroft. Fast parallel matrix and GCD computations. *Information and Control*, 52(3):241–256, 1982.

[18] E. F. Brickell. Some ideal secret sharing schemes. *Journal of Combin. Math. and Combin. Comput.*, 6:105–113, 1989.

[19] E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *J. of Cryptology*, 4(73):123–134, 1991.

[20] E. F. Brickell and D. R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *J. of Cryptology*, 5(3):153–166, 1992.

[21] G. Buntrock, C. Damm, U. Hertrampf, and C. Meinel. Structure and importance of the logspace-mod class. *Math. Systems Theory*, 25:223–237, 1992.

[22] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. *J. of Cryptology*, 6(3):157–168, 1993.

[23] D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols. In *Proc. of the 20th Annu. ACM Symp. on the Theory of Computing*, pages 11–19, 1988.

[24] R. Cramer, I. Damgård, and S. Dziembowski. On the complexity of verifiable secret sharing and multiparty computation. In *Proc. of the 32th Annu. ACM Symp. on the Theory of Computing*, pages 325–334, 2000.

[25] R. Cramer, I. Damgård, and U. Maurer. General secure multi-party computation from any linear secret-sharing scheme. In B. Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 316–334. Springer, 2000.

[26] L. Csirmaz. The dealer's random bits in perfect secret sharing schemes. *Studia Sci. Math. Hungar.*, 32(3–4):429–437, 1996.

[27] L. Csirmaz. The size of a share must be large. *J. of Cryptology*, 10(4):223–231, 1997.

[28] Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. In J. Feigenbaum, editor, *Advances in Cryptology – CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 457–469. Springer-Verlag, 1992.

[29] Y. Desmedt and Y. Frankel. Homomorphic zero-knowledge threshold schemes over any finite abelian group. *SIAM J. on Discrete Mathematics*, 7(4):667–679, 1994.

[30] M. v. Dijk. On the information rate of perfect secret sharing schemes. *Designs, Codes, and Cryptography*, 6:143–169, 1995.

[31] M. v. Dijk. A linear construction of secret sharing schemes. *Designs, Codes, and Cryptography*, 12(2):161–201, 1997.

[32] S. M. Eikenberry and J. P. Sorenson. Efficient algorithms for computing the Jacobi symbol. *Journal of Symbolic Computation*, 26(4):509–523, 1998.

[33] S. Fehr. Span programs over rings and how to share a secret from a module. Master's thesis, ETH Zurich, 1998.

[34] U. Feige, J. Kilian, and M. Naor. A minimal model for secure computation. In *Proc. of the 26th Annu. ACM Symp. on the Theory of Computing*, pages 554–563, 1994.

[35] A. Gál. A characterization of span program size and improved lower bounds for monotone span programs. In *Proc. of the 30th Annu. ACM Symp. on the Theory of Computing*, pages 429–437, 1998.

[36] L. Goldschlager. The monotone and planar circuit value problem is complete for P. *SIGACT News*, 9:25–27, 1977.

[37] S. Goldwasser and S. Micali. Probabilistic encryption. *J. of Computer and System Sciences*, 28(21):270–299, 1984.

[38] D. M. Gordon. A survey of fast exponentiation methods. *Journal of Algorithms*, 27(1):129–146, 1998.

[39] J. Håstad. The shrinkage exponent of de Morgan formulas is 2. *SIAM J. on Computing*, 27(1):48–64, 1998.

[40] Y. Ishai and E. Kushilevitz. Private simultaneous messages protocols with applications. In *5th Israel Symp. on Theory of Computing and Systems*, pages 174–183, 1997.
[41] M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structure. In *Proc. of the IEEE Global Telecommunication Conf., Globecom 87*, pages 99–102, 1987. Journal version: Multiple Assignment Scheme for Sharing Secret. *J. of Cryptology*, 6(1):15-20, 1993.
[42] M. Karchmer and A. Wigderson. On span programs. In *Proc. of the 8th Annu. IEEE Structure in Complexity Theory*, pages 102–111, 1993.
[43] H. Krawczyk. Secret sharing made short. In D. R. Stinson, editor, *Advances in Cryptology – CRYPTO '93*, volume 773 of *Lecture Notes in Computer Science*, pages 136–146. Springer-Verlag, 1994.
[44] K. M. Martin. New secret sharing schemes from old. *J. Combin. Math. Combin. Comput.*, 14:65–77, 1993.
[45] K. Mulmuley. A fast parallel algorithm to compute the rank of a matrix over an arbitrary field. *Combinatorica*, 7:101–104, 1987.
[46] M. O. Rabin. Randomized Byzantine generals. In *Proc. of the 24th Annu. IEEE Symp. on Foundations of Computer Science*, pages 403–409, 1983.
[47] A. Renvall and C. Ding. A nonlinear secret sharing scheme. In *ACISP: Information Security and Privacy: Australasian Conference*, volume 1172 of *Lecture Notes in Computer Science*, pages 56–66, 1996.
[48] A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.
[49] G. J. Simmons. An introduction to shared secret and/or shared control and their application. In G. J. Simmons, editor, *Contemporary Cryptology, The Science of Information Integrity*, pages 441–497. IEEE Press, 1992.
[50] G. J. Simmons, W. Jackson, and K. M. Martin. The geometry of shared secret schemes. *Bulletin of the ICA*, 1:71–88, 1991.
[51] P. M. Spira. On time hardware tradeoffs for Boolean functions. In *Proc. of 4th Hawaii International Symp. on System Sciences*, pages 525–527, 1971.
[52] D. R. Stinson. An explication of secret sharing schemes. *Designs, Codes, and Cryptography*, 2:357–390, 1992.
[53] D. R. Stinson. New general lower bounds on the information rate of secret sharing schemes. In E. F. Brickell, editor, *Advances in Cryptology – CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 168–182. Springer-Verlag, 1993.
[54] D. R. Stinson and J. L. Massey. An infinite class of counterexamples to a conjecture concerning non-linear resilient functions. *Journal of Cryptology*, 8:167–173, 1995.
[55] D. R. Stinson and S. A. Vanstone. A combinatorial approach to threshold schemes. *SIAM J. on Discrete Mathematics*, 1(2):230–236, 1988.

A A Generalization of the Scheme from Section 3

In this section we show how to generalize the scheme for $\mathbf{NQRP}$ to similar access structures. This generalization will uncover what algebraic properties we use in our construction, and will supply us with a few more examples.

Let $R = \langle A, +, * \rangle$ be a finite ring and $B \subseteq A \setminus \{0\}$ be such that $G = \langle B, * \rangle$ is a group.[16] In the sequence all arithmetic operations involving ring elements are performed in the ring. We assume that $2 * a \neq 0$ for every $a \in R \setminus \{0\}$. We Define the access structure $\mathcal{A}_{R,G}$ in a similar way to $\mathbf{NQRP}$.

Definition A.1 (The access structure $\mathcal{A}_{R,G}$) *Let $m \stackrel{def}{=} \lfloor \log |R| \rfloor$. We define the n-party access structure $\mathcal{A}_{R,G}$, where $n \stackrel{def}{=} 2m$, by specifying its collection of minimal sets. With an integer $w \in \{0,1\}^m$ we naturally associate a set B_w of size m defined by:*

$$B_w \stackrel{def}{=} \{B_i^{w_i} : 0 \leq i < m\}.$$

A set B is a minimal set of $\mathcal{A}_{R,G}$ if:

- *$B = \{P_i^0, P_i^1\}$ for some $0 \leq i < m$, or:*
- *$B = B_w$ for some $w \in \{0,1\}^m$ such that $w \notin G$.*

We next show haw to generalize the scheme for $\mathbf{NQRP}$ to a scheme for $\mathcal{A}_{R,G}$.

[16] We even do not need all the properties of these algebraic structures.

Distribution. The dealer chooses at random $m-1$ random elements $z_0, z_1, \ldots, z_{m-2} \in R$ and an additional random element $r \in G$. Define $z_{m-1} \stackrel{\text{def}}{=} -\sum_{i=0}^{m-2} z_i$. The shares of the parties are specified in Table 4.

	$s=0$	$s=1$
P_0^b	$r+z_i$	$br+z_i$
P_i^b $1 \le i < m$	z_i	$2^i br + z_i$

Table 4. A secret-sharing scheme for $\mathcal{A}_{R,G}$.

The reconstruction is similar to the scheme for $\mathbf{NQRP}$, where if $B = B_w$ for some $w \notin G$, then $s = 0$ iff $\mathrm{SUM}_w \in G$. The correctness of this rule follows from the fact that if $w \notin G$ and $b \in G$ then $w * b \notin G$.

For the security, we only consider the case where $C = B_w$ for some $w \in G$. (The first case is identical to the scheme for $\mathbf{NQRP}$.) In this case we claim that, regardless of the value of the secret, the vector-share of the parties in C is a random vector such that $\mathrm{SUM}_w \in G$. This is clearly true when $s = 0$. When $s = 1$, the sum SUM_w is $r \sum_{i=0}^{m-1} w_i 2^i = rw$, and since r is a random element of G and w has an inverse in G, the product is a random element of G.

We next show a few examples of access structures.

Example A.2 Let N be a positive integer, $R = \langle \mathcal{Z}_N, +, * \rangle$, and $G = \langle \mathcal{Z}_N^*, * \rangle$. In this case, an efficient linear scheme for $\mathcal{A}_{R,G}$ exists (see Footnote 15). A quasi-linear scheme for this access structure is described in Example 5.7. However, both the linear and the quasi-linear schemes require knowing the factorization of N. The nonlinear scheme does not require knowledge of the factorization, and all the computations involved are efficient.

Example A.3 Let p be a prime, $R = \langle \mathcal{Z}_{p^2}, +, * \rangle$, $B = \left\{ w \in \mathcal{Z}_{p^2} : w^{p-1} \equiv 1 \bmod p^2 \right\}$, and $G = \langle B, * \rangle$. In this case we do not know if there is a quasi-linear scheme for $\mathcal{A}_{R,G}$, or even if $\mathcal{A}_{R,G}$ is in NC.

B Explicit Estimates implied by ERH

The next theorem gives explicit bounds on the error term in the approximation of the distribution of the primes.

Theorem B.1 *Let* $\mathrm{li}(x) \stackrel{def}{=} \int_2^x \frac{dt}{\log t}$. *If the ERH holds then for* $x \ge 2657$*:*

$$\frac{x}{\log x + 2} \; < \; \pi(x) \; < \; \frac{x}{\log x - 4} \quad \text{[5, Theorem 8.8.1]}$$

$$|\pi(x) - \mathrm{li}(x)| \quad \le \quad \sqrt{x} \log x / 8\pi \quad \text{[5, Page 249]}$$

If ERH holds and $\gcd(w,u) = 1$ *then* [5, Theorem 8.8.18]

$$\left| \pi(x,u,w) - \frac{\mathrm{li}(x)}{\varphi(u)} \right| \quad \le \quad \sqrt{x}(\log x + 2 \log u).$$