Weakly-Private Secret Sharing Schemes*

Amos Beimel[1] and Matthew Franklin[2]

[1] Department of Computer Science, Ben-Gurion University.
[2] Department of Computer Science, University of California, Davis.

Abstract. Secret-sharing schemes are an important tool in cryptography that is used in the construction of many secure protocols. However, the shares' size in the best known secret-sharing schemes realizing general access structures is exponential in the number of parties in the access structure, making them impractical. On the other hand, the best lower bound known for sharing of an ℓ-bit secret with respect to an access structure with n parties is $\Omega(\ell n/\log n)$ (Csirmaz, EUROCRYPT 94). No major progress on closing this gap has been obtained in the last decade.

Faced by our lack of understanding of the share complexity of secret sharing schemes, we investigate a weaker notion of privacy in secrets sharing schemes where each unauthorized set can never rule out any secret (rather than not learn any "probabilistic" information on the secret). Such schemes were used previously to prove lower bounds on the shares' size of perfect secret-sharing schemes. Our main results is somewhat surprising upper-bounds on the shares' size in weakly-private schemes.

- For every access structure, we construct a scheme for sharing an ℓ-bit secret with $(\ell + c)$-bit shares, where c is a constant depending on the access structure (alas, c can be exponential in n). Thus, our schemes become more efficient as ℓ – the secret size – grows. For example, for the above mentioned access structure of Csirmaz, we construct a scheme with shares' size $\ell + n \log n$.
- We construct efficient weakly-private schemes for threshold access structures for sharing a one bit secret. Most impressively, for the 2-out-of-n threshold access structure, we construct a scheme with 2-bit shares (compared to $\Omega(\log n)$ in any perfect secret sharing scheme).

1 Introduction

Secret-sharing schemes are a tool used in many cryptographic protocols. A secret-sharing scheme involves a dealer who has a secret, a finite set of n participants, and a collection $\mathcal{A}$ of subsets of the set of participants called the access structure. A perfect secret-sharing scheme for $\mathcal{A}$ is a method by which the dealer distributes shares to the parties such that: (1) any subset in $\mathcal{A}$ can reconstruct the secret from its shares, and (2) any subset not in $\mathcal{A}$ can never reveal any partial information on the secret (in the information theoretic sense). Secret-sharing schemes were first introduced by Blakley [10] and Shamir [44] for the threshold case, that

* The work of the first author was done while on sabbatical at the University of California, Davis, partially supported by the Packard Foundation. The second author is partially supported by the NSF and the Packard Foundation.

is, for the case where the subsets that can reconstruct the secret are all the sets whose cardinality is at least a certain threshold. Secret-sharing schemes for general access structures were introduced by Ito, Saito, and Nishizeki [28]. More efficient schemes were presented in, e.g., [9,45,15,30,46,25]. Originally motivated by the problem of secure information storage, secret-sharing schemes have found numerous other applications in cryptography and distributed computing, e.g., Byzantine agreement [42], secure multiparty computations [8,18,19], threshold cryptography [23], access control [40], and attribute based encryption [26].

A major problem with secret-sharing schemes is that the shares' size in the best known secret-sharing schemes realizing general access structures is exponential in the number of parties in the access structure (e.g., in the schemes based on monotone span programs [30] presented in 1993). Thus, the known constructions for general access structures are impractical. This is true even for explicit access structures (e.g., access structures whose characteristic function can be computed by a small uniform circuit). On the other hand, the best known lower bounds on the shares' size for sharing a secret with respect to an access structure (e.g., in [31,9,17,12,24,20,21,11,41]) are far from the above upper bounds. The best lower bound was proved by Csirmaz [20] in 1994, proving that, for every n, there is an access structure with n parties such that sharing an ℓ-bit secrets requires shares of length $\Omega(\ell n/\log n)$. The question if there exist more efficient schemes, or if there exists an access structure that does not have (space) efficient schemes remains open. The following widely believed conjecture was made by the first author in 1996 [3]:

Conjecture 1. There exists an $\epsilon > 0$ such that for every positive integer n there is an access structure with n parties, for which every secret sharing scheme distributes shares of length exponential in the number of parties n, that is, $2^{\epsilon n}$.

Proving (or disproving) this conjecture is one of the most important open questions concerning secret sharing. No major progress on proving or disproving this conjecture has been obtained in the last decade.

Faced by our lack of understanding of the share complexity of secret sharing schemes, we investigate a weaker notion of privacy of secrets sharing schemes where each unauthorized set can never rule out any secret (rather than not learn any "probabilistic" information on the secret). Our belief is that studying these schemes will shed light on perfect secret-sharing schemes and the techniques needed to prove lower bounds and upper bounds for them. Our main results is somewhat surprising upper-bounds on the shares' size in weakly-private secret-sharing schemes.

Weakly-private scheme were studied implicitly and explicitly in previous papers. They were first studied in [16], where it is proved that ideal weakly-private secret-sharing schemes are perfect (a scheme is ideal if the domain of shares of each party is the same as the domain of shares). Thus, relaxing the privacy requirement does not help for ideal schemes. The relation between perfect secret sharing and weakly-private secret sharing was further discussed in [29]. Lower bounds for secret-sharing schemes were proved in [35] using combinatorial arguments; their results actually apply to weakly-private schemes. In particular, they show that the size of the share of each (non-redundant) party in a weakly-private scheme is at least the size of the secret (such result was proved for perfect schemes in [31]). Weakly-private secret-sharing schemes were used in [43,7] to prove lower bounds on the shares' size of perfect secret-sharing schemes of a certain (matroidial) access structure.

Our main motivation studying weakly-private secret-sharing schemes is to understand what makes them hard (if they are hard). The strongest lower bounds for secret-sharing schemes [17,12,24,20,21] consider the shares as random variables and use entropy arguments to prove the lower bounds. In particular, the proofs rely on the perfectness (or near perfectness) of the schemes. We raise the question if this requirement is essential for proving lower bounds for secret-sharing schemes. This can help in understanding what techniques can be used to prove such lower bounds. While more direct combinatorial methods used to prove lower bounds for weakly-private secret-sharing schemes (e.g., in [43,35,7]) are more intuitive, they might not be strong enough to prove super-polynomial lower-bounds.

To understand this question, let us consider two additional cryptographic protocols. Blundo et al. [13] proved a lower bound on the size of the shares in perfectly private key distribution schemes using entropy arguments. Beimel and Chor [5] showed that the same lower bound holds even for weakly-private key distribution schemes. A similar phenomenon is true for 2-party secure computation in the honest-but-curious model. Kushilevitz [36] characterizes the functions that can be computed privately in this model; in particular, a function can be computed in the honest-but-curious 2-party model with weak privacy if and only if it can be computed with perfect privacy.[3] As we have seen that weak privacy suffices for proving lower bounds and impossibility results for some cryptographic tasks, it is natural to ask if this is the case for secret-sharing schemes.

1.1 Our Results

Our main results in this paper are somewhat surprising upper-bounds on the shares' size in weakly-private secret-sharing schemes. In addition we prove some lowers bounds.

A generic construction of weakly-private schemes. For every access structure, we construct a scheme for sharing an ℓ-bit secret with $(\ell + c)$-bit shares, where c is a constant depending on the access structure (alas, c can be exponential in n – the number of the parties in the access structure). For comparison, in the best known constructions of perfect secret-sharing schemes realizing an arbitrary access structure, the size of the shares is $\ell c'$, where c' is a constant (which can also be exponential in n).

Let us consider a few examples. Capocelli et al. [17] proved that there is an access structures with 4 parties such that in every perfect secret-sharing scheme realizing it with ℓ-bit secrets, the shares of at least one party is at least 1.5ℓ-bit strings. In contrast, we show how to realize this access structures by a weakly-private scheme with $(\ell + 2)$-bit shares. Csirmaz [20] proved that for every $n \in \mathbb{N}$

[3] The notion of weak privacy in [36] is different than ours; however, the impossibility result for our definition of weak privacy follows from the proof in that paper. See treatment in [4].

there is an access structures $\mathcal{A}_n$ with n parties such that in every perfect secret-sharing scheme realizing $\mathcal{A}_n$ with ℓ-bit secrets, the shares of at least one party are $\Omega((n/\log n)\ell)$-bit strings. In contrast, we show how to realize this access structures by a weakly-private scheme in which the shares are $(\ell + n \log n)$-bit strings. In particular, if we take $\ell = n \log n$, then in any perfect scheme the shares are $\Omega(\ell^2/\log^2 \ell)$-bit strings, while in the weakly-private schemes we construct the shares are 2ℓ-bit strings.

As discussed above, one of the motivations for weakly-private secret-sharing schemes is for proving lower bounds on perfect schemes. For example, Kurosawa and Okada [35] have used combinatorial arguments to prove an inferior version of the above mentioned result of [17]. However, their proof applies to weakly-private schemes and our results show that using weakly-private schemes one cannot hope to prove a lower bound of $\ell+\omega(1)$. Beimel and Livne [7] (improving on Seymour [43]) proved lower bounds of the shares' size in a matroidial access structure $\mathcal{M}$ with 7 parties. On one hand, the shares in the best known perfect secret-sharing scheme realizing $\mathcal{M}$ with with ℓ-bit secrets are 1.5ℓ-bit strings [38]. On the other hand, by our result, there is secret-sharing scheme realizing $\mathcal{M}$ with with ℓ-bit secrets and $(\ell + 16)$-bit shares. Thus, if the lower bound for perfect scheme realizing $\mathcal{M}$ can be improved to $\ell + \omega(1)$, then such proof must use the fact that the scheme is perfect (e.g., generalize the combinatorial proof of [7] to use some additional ideas).

In addition, we present a construction, due to Yuval Ishai [27], giving efficient weakly-private secret-sharing schemes for a doubly exponential number of access structures. Specifically, for every $n \in \mathbb{N}$, there are 2^{2^n} access structures with $2n$ parties that have a weakly-private scheme for sharing a 1-bit secret using shares of length $O(n^3)$. This should be contrasted with perfect secret sharing schemes where efficient schemes for sharing a 1-bit secret are known only for exponentially many access structures.

Weakly-private threshold schemes for sharing one bit. The most important secret-sharing schemes are threshold secret-sharing schemes. Shamir [44] shows that there are very efficient perfect t-out-of-n secret-sharing schemes for sharing ℓ-bit secrets when $\ell \geq \log n$, namely the shares are ℓ-bit strings as well. However, the best known perfect t-out-of-n schemes for sharing a 1-bit secret (when $2 \leq t \leq n-1$) use $\log n$-bit shares (e.g., in Shamir's scheme).[4] Kilian and Nisan [32] proved that this is unavoidable when $t \leq \alpha n$ for some constant $\alpha < 1$; they prove that the shares are at least $\log(n - t + 2)$-bit strings.

In contrast, we construct efficient weakly-private schemes for threshold access structures for sharing a 1-bit secret. Our most efficient construction is a simple weakly-private 2-out-of-n secret-sharing scheme with 1-bit secrets and 2-bit shares. For larger values of t, we construct weakly-private t-out-of-n schemes for sharing 1-bit secrets with $O(t)$-bit shares. In particular, our scheme improves the share size when $t \leq \log n - 2 \log\log n$. These schemes have the additional nice property that they are anonymous, that is, the reconstruction of the secret does not depend on the identity of the authorized set. Anonymous secret-sharing schemes were introduced by [47], and were further studied in [14,33,39].

[4] For $t = 2$ and $t = n - 1$, we can use the formula-based scheme of [9].

We present an additional construction of weakly-private threshold scheme that is efficient for big thresholds. When n is a prime-power and $n > t/2$, we construct a weakly-private t-out-of-n scheme that is better than the *known* perfect schemes, that is, our scheme uses a domain of shares of size $n-1$ when $t \approx n/2$ and a domain of size $3n/4$ when $t = n-1$ (the size of the domain of shares in the best known perfect secret-sharing scheme is at least n). We remark that the size of the shares in the optimal perfect $(n-1)$-out-of-n schemes for sharing a 1-bit secret is unknown as the lower bound of [32] for this case on the size of the domain of shares is 3, and the upper bound is n.

Our last result is a lower bound on the size of shares in weakly-private t-out-of-n schemes for sharing a 1-bit secret. We prove that in this case the secrets are taken from a domain of size $\min\left\{t, \Omega(\frac{\log\log(n-t)}{\log\log\log(n-t)})\right\}$. For anonymous weakly-private t-out-of-n schemes for sharing a 1-bit secret we prove a much stronger lower bound of $\min\left\{2t, \sqrt{(n-t)/2}\right\}$. This should be compared to the lower bound of $n-t+2$ for perfect t-out-of-n schemes for sharing a 1-bit secret.

Are weakly-private schemes suitable for proving lower bounds? Our results suggest that weakly-private schemes are indeed weaker than perfect schemes. The ideas used in constructing our weakly-private schemes guarantee the weak privacy, but they are far from providing perfect privacy or statistical privacy. We conclude that weakly-private secret-sharing schemes are not useful for proving lower bounds for large domains of secrets (e.g., for proving that the information rate of an access structure is bounded from 1). The situation is less clear for secret sharing of a 1-bit secret. In this case the share complexity of weakly-private secret schemes is still open; weakly-private secret-sharing schemes might be useful for proving lower bounds for perfect scheme for sharing a 1-bit secret. The efficient weakly-private schemes for the doubly exponential family and the efficient weakly-private threshold schemes might discourage such belief.

Alternative notions of "weaker" secret sharing. In this work we discuss weakly-private secret-sharing schemes as a relaxation of perfect secret-sharing schemes. Below we mention a few other relaxations of perfect secret-sharing schemes; all these relaxations are incomparable to weakly-private secret-sharing schemes. A notion that is related is statistical secret-sharing schemes, considered in, e.g., [6,22]. In these schemes the privacy and possibly also the correctness are only statistical. Another related notion is computational secret-sharing schemes, considered in [49,34,2,48]. In these schemes, unauthorized sets of parties cannot distinguish in polynomial time between the different secrets.

Organization. In Section 2 we define perfect and weakly-private secret-sharing schemes. In Section 3 we present the construction of the generic weakly-private secret-sharing scheme for arbitrary access structures, and in Section 4 we describe efficient weakly-private secret-sharing schemes for doubly exponential number of access structures. In Section 5 we construct weakly-private threshold schemes for sharing 1-bit secrets, and in Section 6 we prove lower bounds for them.

2 Definitions and Notations

In this section we define perfect secret sharing and weakly-private secret sharing. We start by defining an access structure – the collection of sets that should be able to reconstruct the secret.

Definition 1 (Access Structure). *Let $U = \{P_1, \ldots, P_n\}$ be a set of parties. A collection $\mathcal{A} \subseteq 2^U$ is* monotone *if $B \in \mathcal{A}$ and $B \subseteq C$ imply that $C \in \mathcal{A}$. An* access structure *is a monotone collection $\mathcal{A} \subseteq 2^U$ of non-empty subsets of U. Sets in $\mathcal{A}$ are called* authorized*, and sets not in $\mathcal{A}$ are called* unauthorized*.*

Definition 2 (Perfect Secret-Sharing Schemes). *Let S be a finite set of secrets, where $|S| \geq 2$, and R be a set of random strings. An n-party* secret-sharing scheme *Π with* domain of secrets *S is a mapping from $S \times R$ to a set of n-tuples $S_1 \times \cdots \times S_n$, where S_i is called the* share-domain *of P_i. A dealer shares a secret $s \in S$ among the n parties according to Π by first sampling a random string $r \in R$ (according to some given distribution), computing the vector of* shares *$\Pi(s, r) = \langle s_1, \ldots, s_n \rangle$, and then privately communicating each share s_i to the party P_i. We say that Π* realizes *an access structure $\mathcal{A} \subseteq 2^U$ if the following two requirements hold:*

CORRECTNESS. *The secret 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 *$\textsc{Recon}_B : S_{i_1} \times \cdots \times S_{i_{|B|}} \to S$ such that $\textsc{Recon}_B(\Pi_B(s, r)) = s$ for every $s \in S$, every $r \in R$, and every possible value of $\Pi_B(s, r)$, the restriction of $\Pi(s, r)$ to its B-entries.*

PRIVACY. *Every unauthorized set can never learn anything about the secret (in the information theoretic sense) from their shares. Formally, for any set $C \notin \mathcal{A}$, for every two secrets $a, b \in S$, and for every possible $|C|$-tuple of shares $\langle s_i \rangle_{P_i \in C}$: $\Pr[\, \Pi_C(a, r) = \langle s_i \rangle_{P_i \in C} \,] = \Pr[\, \Pi_C(b, r) = \langle s_i \rangle_{P_i \in C} \,]$.*

In this work we concentrate on weakly-private secret-sharing schemes, where an unauthorized set can never rule out any secret.

Definition 3 (Weakly-Private Secret-Sharing Schemes). *We say that a secret-sharing scheme Π* weakly realizes *an access structure $\mathcal{A} \subseteq 2^U$ if it satisfies the correctness requirement of Definition 2 and it satisfies the following weak privacy requirement:*

WEAK PRIVACY. *Every unauthorized set can never rule out any secret from its shares. Formally, for any set $C \notin \mathcal{A}$, for every two secrets $a, b \in S$, and for every possible $|C|$-tuple of shares $\langle s_i \rangle_{P_i \in C}$: $\Pr[\, \Pi_C(a, r) = \langle s_i \rangle_{P_i \in C} \,] > 0$ if and only if $\Pr[\, \Pi_C(b, r) = \langle s_i \rangle_{P_i \in C} \,] > 0$.*

In this work we measure the share complexity of a scheme either as the length of the strings representing the shares or as the size of the domain of shares. The latter is used mainly when we discuss threshold schemes.

Definition 4 (Possible Vectors of Shares). *Let Π be a secret-sharing scheme and A be a set of parties. We say that a vector of shares $\langle s_i \rangle_{P_i \in A}$ is* possible with secret *a for A in Π if $\Pr[\, \Pi_A(a, r) = \langle s_i \rangle_{P_i \in A} \,] > 0$.*

The most important secret-sharing schemes are threshold schemes, where the authorized sets are all sets whose size is at least some given threshold.

Definition 5 (t-out-of-n Secret Sharing). *A secret-sharing scheme Π is a* t-out-of-n secret-sharing scheme *if it realizes the access structure* $\mathcal{A}_{t,n} \stackrel{def}{=} \{A \subseteq \{P_1, \ldots, P_n\} : |A| \geq t\}$. *We say that a secret-sharing scheme Π is a* weakly-private t-out-of-n secret-sharing scheme *if it weakly realizes $\mathcal{A}_{t,n}$.*

In the definition of secret-sharing schemes we say that for every set B there is a reconstruction function Recon_B that takes the shares of the parties of B and reconstructs the secret. That is, the reconstruction function can use the identities of the parties of B. For example, in Shamir's scheme the parties in every set B of size t reconstruct the secret by applying a linear function to their shares; the coefficients in this linear function depend on the set B. A scheme is anonymous if the reconstruction is done as a function of the shares without knowing the identities of the parties in B. The following definition, which is equivalent to the definition of [14], captures this intuition by requiring that if a vector of shares is possible given a secret s, then every possible permutation in the order of the coordinates in this vector is possible given s.

Definition 6 (Anonymous t-out-of-n Secret Sharing). *We say that a perfect or weakly-private t-out-of-n secret-sharing scheme is* anonymous *if for every $s \in S$, every vector of shares $\langle s_1, s_2, \ldots, s_n\rangle$, and every permutation $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$, the vector $\langle s_1, s_2, \ldots, s_n\rangle$ is possible with secret s for $\{P_1, \ldots, P_n\}$ iff the vector $\langle s_{\pi(1)}, s_{\pi(2)}, \ldots, s_{\pi(n)}\rangle$ is possible with secret s for $\{P_1, \ldots, P_n\}$.*

Notation. For a set Σ, let $\binom{\Sigma}{<t}$ be the collections of subsets of Σ of size less than t and let $\binom{\Sigma}{t}$ be the collections of subsets of Σ of size exactly t. For an integer $n \in \mathbb{N}$, let $[n] \stackrel{\text{def}}{=} \{1, \ldots, n\}$.

3 A Generic Construction of Weakly-Private Secret-Sharing Schemes

In this section we show that weakly-private schemes can be more efficient than perfect schemes. We construct for every access structure $\mathcal{A}$ a weakly-private secret-sharing scheme realizing $\mathcal{A}$ with shares whose size is linear in the size of the domain of secrets (but possibly exponential in the number of parties).

Theorem 1. *For every access structure $\mathcal{A}$ with n parties there is some constant c such that for every $\ell \in \mathbb{N}$ there exists a weakly-private secret-sharing scheme realizing $\mathcal{A}$ with ℓ-bit secrets and $(\ell + c)$-bit shares for each party (however, c may be exponential in n).*

The theorem is proven in Lemma 1. For comparison, the size of the shares in the best known constructions of perfect secret-sharing schemes realizing an arbitrary access structure, the size of the shares is $\ell \cdot c'$, where c' is a constant that can also be exponential in n.

Define the following sets of vectors of shares for a secret $s \in \{0,1\}^\ell$ are:

$\{P_1\}$-Vectors: $\langle\langle a, r\rangle, \langle\overline{a}, s\rangle\rangle$, for every $r \in \{0,1\}^\ell$ and every $a \in \{0,1\}$.
$\{P_2\}$-Vectors: $\langle\langle a, s\rangle, \langle a, r\rangle\rangle$ for every $r \in \{0,1\}^\ell$ and every $a \in \{0,1\}$.

To share a secret s, choose at random $i \in \{1,2\}$ and choose a random vector from the $\{P_i\}$-vectors.

Fig. 1. The weakly-private scheme realizing Γ.

A Warmup. Let Γ be the access structure with two participants P_1 and P_2 and one authorized set $\{P_1, P_2\}$. As a warm up, we describe a weakly-private scheme realizing Γ. The scheme we describe is inferior to the best perfect scheme realizing Γ. The main purpose of describing this scheme is to introduce the ideas of the general scheme.

In the scheme we construct, the secret is an ℓ-bit string and the shares are $(\ell+1)$-bit strings. The scheme is described in Fig. 1. In this scheme, in each vector of shares exactly one party holds the secret and the other party holds a random element. Only both parties together know which party holds the secret, thus they can reconstruct the secret and each individual party can never rule out any secret. The vectors of shares are divided to two sets, $\{P_1\}$-vectors and $\{P_2\}$-vectors. The $\{P_i\}$-vectors, where P_i holds a random element, disable $\{P_i\}$ from ruling out any secret (where $i \in \{0,1\}$).

We first explain how P_1 and P_2, holding shares $\langle a_1, b_2\rangle$ and $\langle a_2, b_2\rangle$ respectively (where a_i is a bit and b_i is either the secret or a random string), reconstruct the secret: If $a_1 = a_2$, then the secret is b_1, otherwise the secret is b_2. To argue that the scheme is weakly private, note that for every secret $s \in \{0,1\}^\ell$, Party P_i can get every share in $\{0,1\} \times \{0,1\}^\ell$ in the $\{P_i\}$-vectors.

The construction of the weakly-private schemes. Let $\mathcal{A}$ be an access structure with n parties and $\ell \in \mathbb{N}$. We first describe a very simple scheme with ℓ-bit secrets and ℓ-bit shares that has useful properties. To share a secret s, there is a set of vectors of shares for every maximal unauthorized set $C \notin \mathcal{A}$, called the C-vectors, which prevent C from ruling out any secret. In the C-vectors, the share of every $P_i \notin C$ is the secret s, while the share of each party in C ranges over all the possible shares in $\{0,1\}^\ell$. Thus, the number of C-vectors, for a given secret s, is $2^{\ell|C|}$.

Clearly, weak privacy holds in the above scheme (that is, every unauthorized set can never rule out any secret). We next argue that every authorized set B can reconstruct the secret with probability at least $1/|B| \geq 1/n$ (even when $\ell \gg n$). Let $B \in \mathcal{A}$ be any authorized set holding a vector of shares $\boldsymbol{v}$. This vector is a sub-vector of a C-vector for some $C \notin \mathcal{A}$. Since B is authorized and C is unauthorized, there must be some $P_i \in B \setminus C$, thus P_i holds s in $\boldsymbol{v}$. The parties in B, which do not know C, choose $P_i \in B$ at random and output its share as the secret.

Let $s \in \{0,1\}^{\ell}$ be the secret.

1. Choose at random a maximal unauthorized set $C \notin \mathcal{A}$.
2. Share the n-bit string representing C using a weakly-private scheme Π_{weak} realizing $\mathcal{A}$. Let $a_1, \ldots, a_n$ be the generated shares.
3. Choose a random $b_i \in \{0,1\}^{\ell}$ for every $P_i \in C$ and set $b_i = s$ for every $P_i \notin C$.
4. The share of P_i is (a_i, b_i).

Fig. 2. A generic weakly-private scheme Π_{generic} realizing an access structure $\mathcal{A}$.

In the previous scheme, the authorized set B could not know the set C. However, to reconstruct the secret with certainty, the set B needs to know C (or at least some $P_i \in B \setminus C$). Thus, we represent C as an n-bit string and share this string using a weakly-private scheme realizing $\mathcal{A}$. That is, we reduced the question of sharing a secret taken from a big domain to sharing a secret from a domain of size 2^n. Such (perfect) schemes, with $2^{O(n)}$-bit shares, exist for every access structure (e.g., [28,9,30]). The formal description of the scheme Π_{generic} appears in Fig. 2. The possible vectors of shares generated in Π_{generic} when the maximal unauthorized set chosen in Step (1) of the scheme is C are called the C-vectors.

Lemma 1. *The generic weakly-private scheme* Π_{generic}*, described in Fig. 2, weakly realizes the access structure* $\mathcal{A}$*. Furthermore, if* Π_{generic} *uses a weakly-private scheme* Π_{weak} *with* n*-bit secrets and* c*-bit shares, then, to share* ℓ*-bit secrets,* Π_{generic} *distributes* $(\ell + c)$*-bit shares.*

Proof. To prove that Π_{generic} weakly realizes $\mathcal{A}$, we prove the correctness and weak privacy of the scheme. To reconstruct the secret, an authorized set B, holding shares $\langle (a_i, b_i) \rangle_{P_i \in B}$, reconstructs the set C from the shares $\langle a_i \rangle_{P_i \in B}$, finds some $P_i \in B \setminus C$, and returns b_i.

To argue that the scheme is weakly private, consider a maximal unauthorized set C holding shares $\langle (a_i, b_i) \rangle_{P_i \in C}$ that are possible with some secret s_0. These shares are possible given any secret s: First, the shares $\langle a_i \rangle_{P_i \in B}$ are possible in Π_{weak} for the set C. Thus, by the definition of the C-vectors, the shares $\langle (a_i, b_i) \rangle_{P_i \in B}$ are a restriction of a C-vector that is possible for the secret s. □

Example 1. Csirmaz [20] proved that for every $n \in \mathbb{N}$ there is an access structures $\mathcal{A}_n$ with n parties such that in every perfect secret-sharing scheme realizing $\mathcal{A}_n$ with ℓ-bit secrets, the shares of at least one party are $\Omega((n/\log n)\ell)$-bit strings. The description of the access structure $\mathcal{A}_n$ is somewhat technical. The only property we need is that in $\mathcal{A}_n$ each party is contained in at most n minimal authorized sets. Thus, by [28], there is a perfect scheme realizing $\mathcal{A}_n$ for sharing n-bit secrets using $O(n^2)$ bit shares. By Lemma 1, there is a scheme weakly realizing $\mathcal{A}_n$ with ℓ-bit secrets and $(\ell + n^2)$-bit shares. If we use Lemma 2 and Lemma 3 (proved in section 3.1), we get a scheme weakly realizing $\mathcal{A}_n$ with ℓ-bit secrets and $(\ell + n \log n)$-bit shares. In particular, if we take $\ell = n \log n$, then in perfect scheme shares are $\Omega(\ell^2/\log^2 \ell)$-bit strings, while in the weakly-private schemes we construct the shares are 2ℓ-bit strings.

3.1 Improvements of the Generic Scheme

In the generic scheme Π_{generic}, presented in Fig. 2, the shares are $(\ell + c)$-bit strings, where c can be large, that is, it is the size of the shares in a scheme Π_{weak} realizing $\mathcal{A}$ with n-bit secrets. In this section we try to reduce the constant c. We observe that in the proof of Lemma 1, the properties required from the secret-sharing scheme Π_{weak} are the following:

- Every authorized set B can compute the identity of a party $P_i \in B \setminus C$, and
- Every unauthorized set C can never rule out that the shared set is C.

Next we formally define schemes satisfying these conditions.

Definition 7 (Weakly-Private Sharing of Unauthorized Sets). *Let S be the set of maximal unauthorized sets in $\mathcal{A}$. We say that a secret-sharing scheme Π with domain of secrets S* weakly shares the unauthorized sets *of an access structure $\mathcal{A}$ if it satisfies the following two requirements:*

- *For any set $B \in \mathcal{A}$ (where $B = \{P_{i_1}, \ldots, P_{i_{|B|}}\}$), there exists a* reconstruction function $\textsc{Recon}_B : S_{i_1} \times \cdots \times S_{i_{|B|}} \to S$ *such that for every maximal $C \in S$, for every $r \in R$, and for every possible value of $\Pi_B(C, r)$,*

$$\textsc{Recon}_B(\Pi_B(C, r)) = P_i \textit{ such that } P_i \in B \setminus C.$$

- *Every unauthorized set can never rule out itself from its shares. Formally, for any maximal unauthorized set $C \notin \mathcal{A}$, for every possible $|C|$-tuple of shares $\langle s_i \rangle_{P_i \in C}$: If there is some maximal unauthorized set $C_0 \notin \mathcal{A}$ such that* $\Pr[\, \Pi_C(C_0, r) = \langle s_i \rangle_{P_i \in C} \,] > 0$ *then* $\Pr[\, \Pi_C(C, r) = \langle s_i \rangle_{P_i \in C} \,] > 0$.

In Π_{generic}, if we use a scheme that weakly shares the unauthorized sets of $\mathcal{A}$, then the proof of Lemma 1 remains valid.

Lemma 2. *Assume that there is a scheme Π_{set} that weakly shares the unauthorized sets of $\mathcal{A}$ with c_{set}-bit shares. To share ℓ-bit secrets, the generic weakly-private scheme Π_{generic}, when using Π_{set} instead of Π_{weak}, weakly realizes the access structure $\mathcal{A}$ distributing $(\ell + c_{\text{set}})$-bit shares.*

We next give an example of weakly-private schemes for sharing unauthorized sets. We first use ideas similar to Ito, Saito, and Nishizeki [28]. They proved that if every party is contained in at most d minimal sets of an access structure $\mathcal{A}$, then there is a scheme perfectly realizing $\mathcal{A}$ with ℓ-bit secrets and ℓd-bit shares.

Lemma 3. *Assume $\mathcal{A}$ is an access structure such that every party is contained in at most d minimal authorized sets of $\mathcal{A}$. Then, there is a scheme for weakly sharing the unauthorized sets of $\mathcal{A}$ distributing $d \lceil \log n \rceil$-bit shares.*

Proof. To share a maximal unauthorized set C, for every minimal authorized set B, choose a random party $P_{j_B} \in B \setminus C$, choose $|B|$ random elements $\langle s_{i,B} \rangle_{P_i \in B}$ such that $s_{i,B} \in \{0, \ldots, n-1\}$ and $\sum_{\{i : P_i \in A\}} s_{i,B} \equiv j_B \pmod{n}$. The share of P_i is $\langle s_{i,B} : P_i \in B, B \in \mathcal{A}$ is a minimal authorized set$\rangle$. Clearly, this scheme is correct. Furthermore, each maximal unauthorized set can never rule out itself as the parties in C cannot rule out any j_B for a minimal authorized set B in $\mathcal{A}$. $\square$

4 Upper Bounds for Efficient Weakly-Private Sharing of Double Exponential Number of Access Structures

In this section we present a construction due to Yuval Ishai [27] giving an efficient weak secret-sharing schemes with a 1-bit secret for a family of access structures of a doubly exponential size. We first define this family.

Definition 8 (The Access Structure $\mathcal{A}_C$). *For every n and every $C \subseteq \{0,1\}^n$, we define an access structure $\mathcal{A}_C$ with $2n$ parties denoted $P_1^0, P_1^1, \ldots, P_n^0, P_n^1$. For every $c = \langle c_1, \ldots, c_n \rangle \in \{0,1\}^n$ define a set $Q_c \stackrel{def}{=} \{P_1^{c_1}, P_2^{c_2}, \ldots, P_n^{c_n}\}$. The minimal authorized sets in $\mathcal{A}_C$ are $\{Q_c : c \in C\} \cup \{\{P_j^0, P_j^1\} : j \in [n]\}$.*

Theorem 2. *For every $C \subseteq \{0,1\}^n$ there is a weakly-private secret-sharing scheme realizing $\mathcal{A}_C$ with domain of secrets $\{0,1\}$ and $O(n^3)$-bit shares.*

Proof. The idea, again, is that for every unauthorized set we construct a set of vectors that prevent the set from ruling out a secret. Towards this goal, we define the following function: For $a, b \in \{0,1\}$ and $x, y \in \{0,1\}^n$, let $f(a,b,x,y)$ be the function which outputs a if $x \neq y$ and outputs b otherwise. Informally, the input a of f is the secret we want to share, the input b is a random input, and if we set $x = y = z$, we will prevent the set Q_z from ruling out the secret b. To construct the scheme, we use the randomized encodings of Applebaum, Ishai, and Kushilevitz [1]. Specifically, the function f can be efficiently encoded by a function $f'((a,b,x,y),r)$ such that:

1. The output distribution of f' induced by a random choice of r reveals the output of f and no additional information about a, b, x, y, that is, there are two distributions D_0, D_1 such that
   (a) If $f(a,b,x,y) = 0$ then $f'((a,b,x,y),r)$ is distributed according to D_0 and if $f(a,b,x,y) = 1$ then $f'((a,b,x,y),r)$ is distributed according to D_1, and
   (b) The distributions D_0 and D_1 have a disjoint support.
2. The length of the output of f' is $O(n^3)$, and
3. Each output bit of f' depends on at most a single bit of (a,b,x,y).

In particular, if the ith bit of f' depends on x_j and we fix r, then we can compute the ith bit of f' from r and x_j without knowing the other bits of x (or knowing a, b, y).

For any subset $C \subseteq \{0,1\}^n$, we describe in Fig. 3 a weakly-private scheme realizing $\mathcal{A}_C$. First note that every pair $\{P_j^0, P_j^1\}$ can reconstruct the secret using the shares given in Step (1) of the scheme. Second, consider a set that contains at most one party from every pair $\{P_j^0, P_j^1\}$ and for some $j \in [n]$ does not contain neither P_j^0 nor P_j^1. Such set can never rule out any value of s_0, hence can never rule out any value of s. Thus, it remains to prove that a set Q_c can reconstruct the secret if and only if $c \in C$.

If $c \in C$, then in Step (4) of the scheme a $w \neq c$ is chosen. The parties of Q_c together hold the bits of $f'((s_1,b,c,w),r)$, which is an element of D_{s_1}, hence they can also compute $f(s_1,b,c,w) = s_1$ (since the support of D_0 and the support of D_1 are disjoint). Furthermore, they hold $q_1, \ldots, q_n$, hence, they can compute $s = s_0 \oplus \bigoplus_{j=1}^{n} q_j$.

To share a secret $s \in \{0,1\}$:

1. For every j choose $r_j \in \{0,1\}$ at random, and send to P_j^0 the bit r_j and to P_j^1 the bit $r_j \oplus s$,
2. Choose $s_0 \in \{0,1\}$ at random, define $s_1 \leftarrow s \oplus s_0$,
3. For every $j \in [n-1]$ choose $q_j \in \{0,1\}$ at random, set $q_n = s_0 \oplus \bigoplus_{j=1}^{n-1} q_j$, and send to P_j^0 and P_j^1 the bit q_j.
4. Choose $w \notin C$ at random, choose $b \in \{0,1\}$ at random, and choose a random r.
5. Send to player P_j^d, for $j \in [n]$ and $d \in \{0,1\}$, the value of output bits of $f'((s_1,b,x,w),r)$ that depend on x_j assuming that $x_j = d$.
6. All bits of $f'((s_1,b,x,w),r)$ that do not depend on bits of x are sent to all parties.

Fig. 3. A weakly-private scheme realizing $\mathcal{A}_C$.

For any $z \notin C$, the set of n players Q_z can never rule out any value of s_1: When $w = z$ and $b = 0$ are chosen in Step (4) of the scheme, the parties of Q_z can compute a random element of D_0 and when $w = z$ and $b = 1$ are chosen in Step (4) of the scheme they can compute a random element of D_1. Thus, the parties do not know if $w \neq z$ and they got an element of D_{s_1} or $w = z$ and $b = \overline{s_1}$ and they got an element of $D_{\overline{s_1}}$. $\square$

5 Upper Bounds for Weakly-Private Threshold Sharing of One Bit

In this section we construct weakly-private t-out-of-n secret-sharing schemes for sharing one bit. We first present a simple weakly-private 2-out-of-n scheme in which the size of the domain of shares of each party is 4. Generalizing the ideas of this scheme we present a 3-out-of-n scheme in which the size of the domain of shares of each party is 6, and a t-out-of-n scheme in which the size of the domain of shares of each party is $\tilde{O}(2^t)$. Finally, we present a different scheme, based on Shamir's scheme, in which the size of domain of shares is roughly $n - t/(2(n-t+1))$ (when n is a prime-power). The best known perfect t-out-of-n schemes use domain of shares of size n. By a lower bound of [32], the size of the domain of shares in every perfect t-out-of-n schemes is at least $n - t$. Thus, our weakly-private t-out-of-n secret-sharing schemes are more efficient than every perfect t-out-of-n secret-sharing schemes when $t < \log n - 2\log\log n$ and more efficient than known schemes when $t > n/2$.

5.1 The Weakly-Private Scheme for $t = 2$

Lemma 4. *There exists an anonymous weakly-private 2-out-of-n secret-sharing scheme with domain of secrets $\{0,1\}$ in which the size of the domain of shares of every party is 4.*

Proof. To prove the claim we describe a scheme with domain of shares $\{0,1,2,3\}$ for each party.

– To share the secret 0, choose a random index $i \in [n]$ and choose a random $\sigma \in \{2,3\}$. The share of P_i is σ. The share of P_j, for $j \neq i$, is 0 if $\sigma = 2$ and 1 if $\sigma = 3$.
– To share the secret 1, choose a random index $i \in [n]$ and choose a random $\sigma \in \{0,1\}$. The share of P_i is σ. The share of P_j, for $j \neq i$, is 3 if $\sigma = 0$ and 2 if $\sigma = 1$.

The 2-out-4 scheme is explicitly described in Example 2.

On one hand, the reconstruction of the secret by any two parties is simple: If the shares are $\{0,0\}$, $\{0,2\}$, $\{1,1\}$, or $\{1,3\}$, then the secret is 0. Otherwise the secret is 1. On the other hand, each value is possible for each coordinate for each secret, thus, the scheme is weakly private. □

Example 2. We explicitly describe the weakly-private 2-out-4 anonymous secret-sharing scheme. The shares for the secret 0 are randomly chosen from $\langle 0,0,0,2\rangle$, $\langle 0,0,2,0\rangle$, $\langle 0,2,0,0\rangle$, $\langle 2,0,0,0\rangle$ and $\langle 1,1,1,3\rangle$, $\langle 1,1,3,1\rangle$, $\langle 1,3,1,1\rangle$, $\langle 3,1,1,1\rangle$. The shares for the secret 1 are randomly chosen from $\langle 2,2,2,1\rangle$, $\langle 2,2,1,2\rangle$, $\langle 2,1,2,2\rangle$, $\langle 1,2,2,2\rangle$ and $\langle 3,3,3,0\rangle$, $\langle 3,3,0,3\rangle$, $\langle 3,0,3,3\rangle$, $\langle 0,3,3,3\rangle$.

5.2 Weakly-Private Schemes for $t < \log n$

We now describe a generalization of the above scheme for larger thresholds. Specifically, in the scheme we design: (1) the scheme is anonymous (as defined in Definition 6), (2) in each vector of shares all but at most $t-1$ coordinates are equal, and (3) every vector of values in Σ^{t-1} is possible for every $t-1$ parties for every secret (where Σ is the domain of shares of each party).

We will first describe a generic way to construct a weakly-private t-out-of-n scheme based on the existence of two functions f_0, f_1 with certain properties. Roughly speaking, these functions take an arbitrary vector of shares of length $t-1$ and stretch it to a vector of shares of length n. The exact properties we require from these functions are sufficient for proving the correctness of the scheme (however, weaker conditions may also be sufficient for proving correctness). We show a simple construction of f_0, f_1 satisfying these properties for $t = 3$ with domain of size 6. We then show that certain combinatorial structure can be used to construct such functions f_0 and f_1, and show that such structures exist implying a t-out-of-n scheme with domain of shares of size $O(t^2 2^t)$.

Lemma 5. *Let t be an integer, Σ be a finite domain, and Σ_0 and Σ_1 be a partition of Σ. Assume there are two functions f_0, f_1, where $f_s : \binom{\Sigma_{\bar{s}}}{<t} \to \Sigma_s$ for $s \in \{0,1\}$ satisfying*

$$\forall_{A_0 \subseteq \Sigma_0, A_1 \subseteq \Sigma_1 \text{such that } |A_0|+|A_1| \leq t} \; f_0(A_1) \notin A_0 \vee f_1(A_0) \notin A_1. \tag{1}$$

Then, for every $n \geq t$ there is an anonymous weakly-private t-out-of-n scheme with domain of secrets $\{0,1\}$ and domain of shares Σ for each party.

Proof. We describe the scheme using the given functions f_0 and f_1. To share the secret $s \in \{0,1\}$, do the following:

1. Choose $t-1$ random distinct indices $i_1, \ldots, i_{t-1} \in [n]$ and choose $t-1$ random values $\sigma_1, \ldots, \sigma_{t-1}$ for the parties $P_{i_1}, \ldots, P_{i_{t-1}}$ respectively.

2. Let $A_{\overline{s}}$ be the set of elements of $\Sigma_{\overline{s}}$ in $\sigma_1, \dots, \sigma_{t-1}$. For every $\ell \notin \{i_1, \dots, i_{t-1}\}$, the share of P_ℓ is $f_s(A_{\overline{s}})$.

The privacy is guaranteed since every $t-1$ parties can be chosen in Step 1. We next argue that Property (1) implies the correctness of the scheme. That is, every vector of t shares is possible for at most one secret. Assume towards contradiction that $\boldsymbol{b} = \langle b_1, \dots, b_t \rangle$ is possible both for the secret 0 and for the secret 1. For $s \in \{0,1\}$, let B_s be the set of elements of Σ_s in the vector $\boldsymbol{b}$ (without repetition). As $\boldsymbol{b}$ is possible for a secret $s \in \{0,1\}$, in Step 1 of the scheme some vector $\boldsymbol{\sigma} = \langle \sigma_1, \dots, \sigma_{t-1} \rangle$ could have been chosen, where $A_{\overline{s}}$ are the elements of $\Sigma_{\overline{s}}$ in this vector (without repetition). The vector $\boldsymbol{b}$ is obtained by taking a sub-vector of $\boldsymbol{\sigma}$ and completing it to a vector of length t with the value $f_s(A_{\overline{s}})$ (possibly with repetitions). Therefore, the following conditions must hold:

1. $B_{\overline{s}} \subseteq A_{\overline{s}}$,
2. Let n^s be the number of times that $f_s(A_{\overline{s}})$ appears in $\boldsymbol{b}$. Thus,

$$n^s \geq |A_{\overline{s}}| - |B_{\overline{s}}| + 1 \geq 1. \tag{2}$$

In particular, $f_s(A_{\overline{s}})$ appears at least once in $\boldsymbol{b}$.

Thus, $f_0(A_1) \in B_0 \subseteq A_0$ and $f_1(A_0) \in B_1 \subseteq A_1$. Furthermore, $|B_0| + |B_1| \leq t - n^0 - n^1 + 2$ (since $f_0(A_1)$ appears n^0 times in $\boldsymbol{b}$ and $f_1(A_0)$ appears n^1 times in $\boldsymbol{b}$), thus $|A_0| + |A_1| \leq t$ (by (2)). This contradicts Property (1), and thus the scheme is correct. □

We next reformulate Lemma 5 using only one function f_0.

Lemma 6. *Let t be an integer, Σ be a finite domain, and Σ_0 and Σ_1 be a partition of Σ. Assume there is a function $f_0 : \binom{\Sigma_1}{<t} \to \Sigma_0$ such that for every $A_0 \subseteq \Sigma_0$, where $|A_0| < t$,*

$$\bigcup \{A_1 \subseteq \Sigma_1 : |A_0| + |A_1| \leq t \text{ and } f_0(A_1) \in A_0\} \subsetneq \Sigma_1. \tag{3}$$

Then, for every $n \geq t$ there is an anonymous weakly-private t-out-of-n scheme with domain of secrets $\{0,1\}$ and domain of shares Σ for each party.

Proof. We show that there is a function f_1 such that f_0, f_1 satisfy Property (1) of Lemma 5. For every $A_0 \subseteq \Sigma_0$ define $f_1(A_0)$ as any element σ in

$$\Sigma_1 \setminus \left(\bigcup \{A_1 \subseteq \Sigma_1 : |A_0| + |A_1| \leq t \text{ and } f_0(A_1) \in A_0\} \right).$$

Now, if $f_0(A_1) \in A_0$, then $\sigma \notin A_1$, thus, f_0, f_1 satisfy Property (1). □

Specific implementation for $t = 3$

Lemma 7. *There exists an anonymous weakly-private 3-out-of-n secret-sharing scheme with domain of secrets $\{0,1\}$ in which the size of the domain of shares of every party is 6.*

Proof. We show how to implement the functions f_0, f_1 satisfying Property (1) of Lemma 5 with $\Sigma_0 = \{0,1,2\}$, $\Sigma_1 = \{3,4,5\}$, and $\Sigma = \Sigma_0 \cup \Sigma_1$. Define f_0 and f_1 as follows:

A_1	$f_0(A_1)$
$\emptyset$	0
$\{3\}$	0
$\{4\}$	1
$\{5\}$	2
$\{3,4\}$	1
$\{3,5\}$	0
$\{4,5\}$	2

A_0	A_1 s.t. $\lvert A_0\rvert + \lvert A_1\rvert \leq t$ and $f_0(A_1) \in A_0$	$f_1(A_0)$
$\emptyset$	–	3
$\{0\}$	$\emptyset, \{3\}, \{3,5\}$	4
$\{1\}$	$\{4\}, \{3,4\}$	5
$\{2\}$	$\{5\}, \{4,5\}$	3
$\{0,1\}$	$\emptyset, \{3\}, \{4\}$	5
$\{0,2\}$	$\{3\}, \{5\}$	4
$\{1,2\}$	$\{4\}, \{5\}$	3

As indicated by the table, Property (3) holds for f_0; the function f_1 is constructed using Lemma 6. □

Remark 1. We next explain why we need a share domain of size six in the above 3-out-of-n scheme. Assume, f_0, f_1 satisfy Property (1). Thus, for example, if $f_1(\{0,1\}) = \sigma$ we require $f_0(\{\sigma\}) \neq 0, 1$, and $|\Sigma_0| \geq 3$. Similarly, $|\Sigma_1| \geq 3$.

Generic implementation using set-systems

To construct the weakly-private t-out-of-n secret-sharing schemes for larger values of t we use a set-system with specific properties. The existence of such set-system is basically equivalent to the existence of a function f_0 satisfying Property (3) in Lemma 6. The definition of the set-system we use is similar to the definition used in [37] and the construction we present is the same as theirs.

Definition 9. *Let $\mathcal{C} = \{C_1, \ldots, C_m\}$ be a collection of m sets and $B = \bigcup_{i=1}^m C_i$. We say that $\mathcal{C}$ is an (ℓ, m, b) set-system if the following three requirements hold:*

1. *$|\mathcal{C}| = m$ and $|B| \leq b$,*
2. *The union of every ℓ sets in $\mathcal{C}$ is properly contained in B. That is, for every $A_0 \subset [m]$, where $|A_0| = \ell$,*
$$\bigcup_{i \in A_0} C_i \subsetneq B,$$
3. *Every subset of $A_1 \subseteq B$ of size ℓ is contained in at least one C_i, that is, $A_1 \subseteq C_i$.*

It is easy to satisfy one of the above Conditions 2 and 3. For example, to satisfy Conditions 2 we can partition B to $\ell + 1$ disjoint non-empty sets. To satisfy Conditions 3 we can take $\mathcal{C} = \{B\}$. The difficulty is to satisfy the two conditions simultaneously.

Example 3. Let $B = [\ell^2 + 1]$ and $\mathcal{C}$ be the collection of all subsets of size ℓ of B. Then, $\mathcal{C}$ is an $(\ell, m, \ell^2 + 1)$ set-system, where $m \stackrel{\text{def}}{=} \binom{\ell^2+1}{\ell} = 2^{O(\ell \log \ell)}$. Clearly, Items 1 and 3 of Definition 9 hold. To prove that Item 2 holds, notice that the size of B is $\ell^2 + 1$ and the size of each set in $\mathcal{C}$ is ℓ, thus the size of the union of ℓ subsets is at most ℓ^2, that is, there exists at least one element of B that is not in the union of the ℓ sets.

Lemma 8. *If there is a $(t-1, m, b)$ set-system, then there is an anonymous weakly-private t-out-of-n secret-sharing scheme with domain of secrets $\{0,1\}$ and domain of shares of size $m+b$.*

Proof. Let $C_1, \dots, C_m$ be a $(t-1, m, b)$ set-system and $B = \bigcup_{i=1}^{m} C_i$. Without loss of generality, assume that $B \cap [m] = \emptyset$. Let $\Sigma_0 = [m]$ and $\Sigma_1 = B$. We define $f_0 : \binom{[\Sigma_1]}{<t} \to \Sigma_0$ satisfying the condition of Lemma 6: For every $A_1 \subset B$ of size at most $t-1$, we define $f_0(A_1)$ as the smallest i such that $A_1 \subseteq C_i$. By Item 3 such i exists.

We prove that a stronger condition that Property (3) of Lemma 6 holds, namely, we prove that for every $A_0 \subseteq \Sigma_0$

$$\bigcup \{A_1 \subseteq \Sigma_1 : |A_1| \leq t-1 \text{ and } f_0(A_1) \in A_0\} \subsetneq \Sigma_1. \tag{4}$$

Notice that

$$\bigcup \{A_1 \subseteq \Sigma_1 : |A_1| \leq t-1 \text{ and } f_0(A_1) \in A_0\}$$
$$= \bigcup_{i \in A_0} \left(\bigcup \{A_1 \subseteq \Sigma_1 : |A_1| \leq t-1 \text{ and } f_0(A_1) = i\} \right).$$

However, $f_0(A_1) = i$ implies that $A_1 \subseteq C_i$. Thus,

$$\bigcup \{A_1 \subseteq \Sigma_1 : |A_1| \leq t-1 \text{ and } f_0(A_1) \in A_0\} \subseteq \bigcup_{i \in A_0} C_i \subsetneq \Sigma_1$$

(by Item 2 of Definition 9). By Lemma 6, there is a secret-sharing scheme with the parameters promised in the lemma. □

We show the existence of an (ℓ, m, m) set-system using a probabilistic proof provided that $\ell = O(\log m)$. The construction is simple; we choose m subsets independently with uniform distribution.

Lemma 9. *Let $m = 2^{\ell+1}\ell^2$. There exists an (ℓ, m, m) set-system.*

Proof. We show the existence using a probabilistic proof. Define $B = [m]$. Pick m sets $C_1, \dots, C_m \subset B$ where each set is chosen independently with uniform distribution (in particular, $\Pr[j \in C_i] = 1/2$ for every i and j).

We prove that with positive probability Conditions 2 and 3 hold, thus, there exists a "good" choice such that $\{C_1, \dots, C_m\}$ is an (ℓ, m, m) set-system.

We first prove that Condition 2 holds with probability greater than 0.5. First fix a set $A_0 \in [m]$ of size ℓ. For every index $j \in [m]$, the probability that for at least one $i \in A_0$ the index j is in C_i is $1 - 2^{-\ell}$. The probability that $\cup_{i \in A_0} C_i = B$ is the probability that for every $j \in [m]$ for at least one $i \in A_0$ the index j is in C_i. This probability is $(1 - 2^{-\ell})^m \leq e^{-m/2^{\ell}}$. Thus, by the union bound, the probability that there exists a set A_0 violating Condition 2 is at most $\binom{m}{\ell} e^{-m/2^{\ell}} < e^{\ell \ln m - m/2^{\ell}}$. By our choice of m, this probability is less than half.

The same calculations show that Condition 3 holds with probability greater than 0.5. First fix a set $A_1 \subset B$ of size ℓ. The probability that $A_1 \subseteq C_i$ for a fixed i is $2^{-\ell}$. Thus, the probability that $A_1 \not\subseteq C_i$ for every $i \in [m]$ is $(1 - 2^{-\ell})^m \leq e^{-m/2^{\ell}}$. By the union bound, the probability that there exists a set A_1 violating Condition 3 is at most $\binom{m}{\ell} e^{-m/2^{\ell}} < e^{\ell \ln m - m/2^{\ell}} < 1/2$. □

To share a secret $s \in \{0,1\}$ using a domain of shares $\Sigma \subseteq \mathrm{GF}(q)$ of size $\lfloor q-(q-1)(2(n-t+1)) \rfloor + 1$, where $q \geq n$ is a prime-power:

1. Pick random $s_1, \ldots, s_{t-1} \in \Sigma$, and let $a \leftarrow s$.
2. Compute the unique polynomial Q_a of degree at most $t-1$ such that
   - $Q_a(i) = s_i$ for every $1 \leq i \leq t-1$.
   - The coefficient of x^{t-1} in Q_a is a.
3. If $Q_a(i) \notin \Sigma$ for some $t \leq i \leq n$, then $a \leftarrow a+2$; Goto Step 2.
4. (* We found an a such $s \equiv a \pmod 2$ and $Q_a(i) \in \Sigma$ for $1 \leq i \leq n$ *) The share of P_i is $Q_a(i)$.

Fig. 4. A t-out-of-n secret-sharing scheme with domain of shares of size $\lfloor q-(q-1)(2(n-t+1)) \rfloor + 1$.

Theorem 3. *There is an anonymous weakly-private t-out-of-n secret-sharing scheme with domain of secrets $\{0,1\}$ in which the size of the domain of shares of each party is $2(t-1)^2 2^t$.*

In the full version of this paper, we discuss the restriction that we used in the construction of the above scheme. In particular, we prove that in every t-out-of-n scheme implementing Lemma 5 the size of the domain is $2^{\Omega(t)}$, thus our implementation in Theorem 3 is almost optimal.

5.3 Weakly-Private Schemes for $t \geq n/2$

We next present weakly-private t-out-of-n secret-sharing schemes for large values of t. For example, when n is a prime-power, we construct an $(n-1)$-out-of-n scheme with share domain of size roughly $0.75n$ for every party. For $t \approx n/2$, we construct a scheme with domain of shares of size $n-1$. In our scheme, we restrict the domain of shares in a variant of Shamir's scheme [44] to a subset of the field. In this variant of Shamir's scheme, the secret is the coefficient of x^{t-1} in the polynomial (compared to x^0 in Shamir's scheme). The advantage of this variant is that it reduces the size of the field by 1 (yielding the best known perfect t-out-of-n scheme for sharing 1-bit secrets). Unlike the previous schemes for $t < \log n$, the scheme we present in this section is not anonymous.

Theorem 4. *Let $n \in \mathbb{N}$ be integer and $q \geq n$ be a prime-power. For every $1 < t < n$ there is a weakly-private t-out-of-n secret-sharing scheme in which the size of the domain of shares of each party is* $\left\lfloor q - \frac{q-1}{2(n-t+1)} \right\rfloor + 1$.

Proof. We describe the scheme in Fig. 4. All arithmetic in the scheme is in $\mathrm{GF}(q)$. To simplify the notations, we assume that the elements of $\mathrm{GF}(q)$ are $\{0, \ldots, q-1\}$. In the proof below of the weak privacy, we prove that for every $s_1, \ldots, s_{t-1} \in \Sigma$ there exists at least one value a satisfying the conditions of Step 4, thus the scheme terminates. We say that a polynomial Q passes through a share s_i of P_i if $Q(i) = s_i$.

The reconstruction of the secret by t parties is done as in Shamir's scheme: the parties compute the unique polynomial Q of degree $t-1$ that passes through their shares, compute the coefficient a of x^{t-1} in Q, and output $a \bmod 2$. We next prove the weak privacy of the scheme, that is, every $t-1$ parties are unable to rule out either secret. Fix any set C of $t-1$ parties, fix any $t-1$ values $\langle s_i \rangle_{P_i \in C}$ in Σ as the shares of C, and fix a secret $s \in \{0,1\}$. There are at least $(q-1)/2$ values a such that $a \equiv s \bmod 2$. If for one such a the unique polynomial Q of degree $t-1$ with coefficient a of x^{t-1} that passes through the shares of C satisfies $Q(i) \in \Sigma$ for every $i \notin C$, then the shares $\langle s_i \rangle_{P_i \in C}$ are possible for C given s. We will show that every party $P_i \notin C$ eliminates at most $q - |\Sigma| < \frac{q-1}{2(n-t+1)}$ values of a and there are $n-t+1$ parties not in C. Thus, since $(n-t+1)\frac{q-1}{2(n-t+1)} \leq \frac{q-1}{2}$, there is at least one a that survives.

To complete the proof, we fix $P_i \notin C$, and prove that P_i eliminates at most $q - |\Sigma|$ values of a. For each value $s_i \in \{0,\ldots,q-1\} \setminus \Sigma$, there is a unique polynomial of degree $t-1$ that passes through the shares of $C \cup \{P_i\}$. Thus, such value s_i only eliminates the coefficient of x^{t-1} in this polynomial. $\square$

6 Lower Bounds for Weakly-Private Threshold Schemes

We state lower bounds on the size of domain of shares in weakly-private t-out-of-n schemes. The proofs of these results appear in the full version of this paper.

Lemma 10. *Let $n \geq 9$. In every weakly-private 2-out-of-n secret-sharing scheme with domain of secrets $\{0,1\}$, the size of the domain of shares of at least one party is at least 4.*

Theorem 5. *In every* anonymous *weakly-private t-out-of-n secret-sharing scheme with domain of secrets $\{0,1\}$, the size of the domain of shares of at least one party is at least* $\min\left\{2t, \sqrt{(n-t)/2}\right\}$.

Theorem 6. *In every weakly-private t-out-of-n secret-sharing scheme with domain of secrets $\{0,1\}$, the size of the domain of shares of at least one party is at least* $\min\left\{t, \frac{\log\log(n-t)}{2\log\log\log(n-t)}\right\}$. *Furthermore, if $n > t-1+(t-1)(2t-1)^{2\left((2t-1)^{t-1}\right)}$, in every weakly-private t-out-of-n secret-sharing scheme with domain of secrets $\{0,1\}$, the size of the domain of shares of at least one party is at least $2t$.*

Acknowledgments. We thank Benny Chor, Eyal Kushilevitz, Noam Livne, and Enav Weinreb for helpful discussions on this subject. We thank Yuval Ishai for allowing us to include the results described in Section 4.

References

1. B. Applebaum, Y. Ishai, and E. Kushilevitz. Cryptography in NC^0. In *Proc. of the 45th Symp. on Foundations of Computer Science*, pages 166–175, 2004.
2. P. Beguin and A. Cresti. General short computational secret sharing schemes. In *EUROCRYPT '95*, vol. 921 of *LNCS*, pages 194–208. 1995.
3. A. Beimel. *Secure Schemes for Secret Sharing and Key Distribution.* PhD thesis, Technion – Israel Institute of Technology, 1996.

4. A. Beimel. On private computation in incomplete networks. *Distributed Computing*, 2006.
5. A. Beimel and B. Chor. Communication in key distribution schemes. *IEEE Trans. on Information Theory*, 42(1):19–28, 1996.
6. A. Beimel and Y. Ishai. On the power of nonlinear secret-sharing. *SIAM J. on Discrete Mathematics*, 19(1):258–280, 2005.
7. A. Beimel and N. Livne. On matroids and non-ideal secret sharing. In *TCC 2006*, vol. 3876 of *LNCS*, pages 482–501, 2006.
8. M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computations. In *Proc. of the 20th STOC*, pages 1–10, 1988.
9. J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In *CRYPTO '88*, vol. 403 of *LNCS*, pages 27–35. 1990.
10. G. R. Blakley. Safeguarding cryptographic keys. In *Proc. of the 1979 AFIPS National Computer Conference*, pages 313–317. 1979.
11. C. Blundo, A. De Santis, R. de Simone, and U. Vaccaro. Tight bounds on the information rate of secret sharing schemes. *Designs, Codes and Cryptography*, 11(2):107–122, 1997.
12. C. Blundo, A. De Santis, A. Giorgio Gaggia, and U. Vaccaro. New bounds on the information rate of secret sharing schemes. *IEEE Trans. on Information Theory*, 41(2):549–553, 1995.
13. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly secure key distribution for dynamic conferences. *Info. and Comput.*, 146(1):1–23, 1998.
14. C. Blundo and D. R. Stinson. Anonymous secret sharing schemes. *Discrete Applied Math. and Combin. Operations Research and Comp. Sci.*, 77:13–28, 1997.
15. E. F. Brickell. Some ideal secret sharing schemes. *Journal of Combin. Math. and Combin. Comput.*, 6:105–113, 1989.
16. E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *J. of Cryptology*, 4(73):123–134, 1991.
17. 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.
18. D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols. In *Proc. of the 20th STOC*, pages 11–19, 1988.
19. R. Cramer, I. Damgård, and U. Maurer. General secure multi-party computation from any linear secret-sharing scheme. In *EUROCRYPT 2000*, vol. 1807 of *LNCS*, pages 316–334. 2000.
20. L. Csirmaz. The size of a share must be large. In *EUROCRYPT '94*, vol. 950 of *LNCS*, pages 13–22. 1995. Also in: *J. of Cryptology*, 10(4):223–231, 1997.
21. L. Csirmaz. The dealer's random bits in perfect secret sharing schemes. *Studia Sci. Math. Hungar.*, 32(3–4):429–437, 1996.
22. I. Damgård and R. Thorbek. Linear integer secret sharing and distributed exponentiation. In *PKC 2006*, vol. 3958 of *LNCS*, pages 75 – 90. 2006.
23. Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. In *CRYPTO '91*, vol. 576 of *LNCS*, pages 457–469. 1992.
24. M. van Dijk. On the information rate of perfect secret sharing schemes. *Designs, Codes and Cryptography*, 6:143–169, 1995.
25. M. van Dijk. A linear construction of secret sharing schemes. *Designs, Codes and Cryptography*, 12(2):161–201, 1997.
26. V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute based encryption for fine-grained access control of encrypted data. In *CCS 2006*, 2006.
27. Y. Ishai. Personal communication. 2006.
28. M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structure. In *Proc. of Globecom 87*, pages 99–102, 1987.

29. W.-A Jackson and K. M. Martin. Combinatorial models for perfect secret sharing schemes. *J. of Comb. Mathematics and Comb. Computing*, 28:249–265, 1998.
30. M. Karchmer and A. Wigderson. On span programs. In *Proc. of the 8th Structure in Complexity Theory*, pages 102–111, 1993.
31. E. D. Karnin, J. W. Greene, and M. E. Hellman. On secret sharing systems. *IEEE Trans. on Information Theory*, 29(1):35–41, 1983.
32. J. Kilian and N. Nisan. Private communication, 1990.
33. W. Kishimoto, K. Okada, K. Kurosawa, and W. Ogata. On the bound for anonymous secret sharing schemes. *Discrete Appl. Math.*, 121(1-3):193–202, 2002.
34. H. Krawczyk. Secret sharing made short. In *CRYPTO '93*, vol. 773 of *LNCS*, pages 136–146. 1994.
35. K. Kurosawa and K. Okada. Combinatorial lower bounds for secret sharing schemes. *Inform. Process. Lett.*, 60(6):301–304, 1996.
36. E. Kushilevitz. Privacy and communication complexity. *SIAM J. on Discrete Mathematics*, 5(2):273–284, 1992.
37. C. Lund and M. Yannakakis. On the hardness of approximating minimization problems. *J. of the ACM*, 41(5):960–981, 1994.
38. J. Martí-Farré and C. Padró. On secret sharing schemes, matroids and polymatroids. Technical Report 2006/077, Cryptology ePrint Archive, 2006.
39. Y. Miao. A combinatorial characterization of regular anonymous perfect threshold schemes. *Inform. Process. Lett.*, 85(3):131–135, 2003.
40. M. Naor and A. Wool. Access control and signatures via quorum secret sharing. *IEEE Transactions on Parallel and Distributed Systems*, 9(1):909–922, 1998.
41. C. Padró and G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Trans. on Information Theory*, 46:2596–2605, 2000.
42. M. O. Rabin. Randomized Byzantine generals. In *Proc. of the 24th IEEE Symp. on Foundations of Computer Science*, pages 403–409, 1983.
43. P. D. Seymour. On secret-sharing matroids. *J. of Combinatorial Theory, Series B*, 56:69–73, 1992.
44. A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.
45. G. J. Simmons, W. Jackson, and K. M. Martin. The geometry of shared secret schemes. *Bulletin of the ICA*, 1:71–88, 1991.
46. D. R. Stinson. Decomposition construction for secret sharing schemes. *IEEE Trans. on Information Theory*, 40(1):118–125, 1994.
47. D. R. Stinson and S. A. Vanstone. A combinatorial approach to threshold schemes. *SIAM J. on Discrete Mathematics*, 1(2):230–236, 1988.
48. V. Vinod, A. Narayanan, K. Srinathan, C. Pandu Rangan, and K. Kim. On the power of computational secret sharing. In *Indocrypt 2003*, vol. 2904 of *LNCS*, pages 162–176. 2003.
49. A. C. Yao. Unpublished manuscript, 1989. Presented at Oberwolfach and DIMACS workshops.