Linear Secret-Sharing Schemes for Forbidden Graph Access Structures*

Amos Beimel
Ben Gurion University of the Negev
Be'er Sheva, Israel

Oriol Farràs
Universitat Rovira i Virgili
Tarragona, Spain

Yuval Mintz
Ben Gurion University of the Negev
Be'er Sheva, Israel

Naty Peter
Ben Gurion University of the Negev
Be'er Sheva, Israel

July 11, 2020

Abstract

A secret-sharing scheme realizes the forbidden graph access structure determined by a graph $G = (V, E)$ if the parties are the vertices of the graph and the subsets that can reconstruct the secret are the pairs of vertices in E (i.e., the edges) and the subsets of at least three vertices. Secret-sharing schemes for forbidden graph access structures defined by bipartite graphs are equivalent to conditional disclosure of secrets protocols.

We study the complexity of realizing a forbidden graph access structure by linear secret-sharing schemes. A secret-sharing scheme is linear if the secret can be reconstructed from the shares by a linear mapping. We provide efficient constructions and lower bounds on the share size of linear secret-sharing schemes for sparse and dense graphs, closing the gap between upper and lower bounds. Given a sparse (resp. dense) graph with n vertices and at most $n^{1+\beta}$ edges (resp. at least $\binom{n}{2} - n^{1+\beta}$ edges), for some $0 \leq \beta < 1$, we construct a linear secret-sharing scheme realizing its forbidden graph access structure in which the total size of the shares is $\tilde{O}(n^{1+\beta/2})$. Furthermore, we construct linear secret-sharing schemes realizing these access structures in which the size of each share is $\tilde{O}(n^{1/4+\beta/4})$. We also provide constructions achieving different trade-offs between the size of each share and the total share size.

We prove that almost all forbidden graph access structures require linear secret-sharing schemes with total share size $\Omega(n^{3/2})$; this shows that the construction of Gay, Kerenidis, and Wee [CRYPTO 2015] is optimal. Furthermore, we show that for every $0 \leq \beta < 1$ there exist a graph with at most $n^{1+\beta}$ edges and a graph with at least $\binom{n}{2} - n^{1+\beta}$ edges such that the total share size in any linear secret-sharing scheme realizing the associated forbidden graph access structures is $\Omega(n^{1+\beta/2})$. Finally, we show that for every $0 \leq \beta < 1$ there exist a graph with at most $n^{1+\beta}$ edges and a graph with at least $\binom{n}{2} - n^{1+\beta}$ edges such that the size of the share of at least one party in any linear secret-sharing scheme realizing these forbidden graph access structures is $\Omega(n^{1/4+\beta/4})$. This shows that our constructions are optimal (up to poly-logarithmic factors).

*The first and the forth authors are supported by ISF grants 544/13 and 152/17 and by the Frankel center for computer science. The second author is supported by the grant 2017 SGR 705 from the Government of Catalonia and the grant RTI2018-095094-B-C21 "CONSENT" from the Spanish Government. A preliminary version of this paper appeared in *Theory of Cryptography – TCC 2017*, vol 10678 of *Lecture Notes in Computer Science*, Springer, 2017 [11].

1 Introduction

A secret-sharing scheme, introduced by [19, 50, 40], is a method in which a dealer, which holds a secret, can distribute shares to a set of parties, enabling only predefined subsets of parties to reconstruct the secret from their shares. These subsets are called authorized, and the family of authorized subsets is called the access structure of the scheme. The original motivation for defining secret-sharing was robust key management schemes for cryptographic systems. Nowadays, they are used in many secure protocols and applications, such as multiparty computation [16, 26, 28], threshold cryptography [32], access control [48], attribute-based encryption [39, 55], and oblivious transfer [51, 54].

In this paper we study secret-sharing schemes for forbidden graph access structures, first introduced by Sun and Shieh [53]. The forbidden graph access structure determined by a graph $G = (V, E)$ is the access structure whose parties are the vertices of the graph and its authorized sets are all pairs of vertices in E and all subsets of vertices of size greater than two. Secret-sharing schemes for forbidden graph access structure determined by bipartite graphs are equivalent to conditional disclosure of secrets protocols. Following [10, 12], we study the complexity of realizing a forbidden graph, and provide efficient constructions for sparse and dense graphs.

A secret-sharing scheme is linear if each share is a linear combination of the secret and random strings that are taken from some finite field. Equivalently, a scheme is linear if the reconstruction of the secret from the shares is a linear mapping. A linear secret-sharing can be constructed from a monotone span program, a computational model introduced by Karchmer and Wigderson [42], and every linear secret-sharing scheme defines a monotone span program. See [7] for discussion on equivalent definitions of linear secret-sharing schemes. In many of the applications of secret-sharing mentioned above, it is required that the scheme is linear. For example, Cramer, Damgård, and Maurer [28] constructed general secure multiparty computation protocols, i.e., protocols which are secure against an arbitrary adversarial structure, from any linear secret-sharing scheme in which a subset of parties is authorized if and only if it is not in the adversarial structure. Furthermore, it was shown by Attrapadung [6] and Wee [56] that linear secret-sharing schemes realizing forbidden graph access structures are a central ingredient for constructing public-key (multi-user) attribute-based encryption. These applications motivate the study of linear secret-sharing schemes for forbidden graph access structures in this paper.

1.1 Related Work

1.1.1 Secret-Sharing Schemes for Arbitrary Access Structures

Secret-sharing schemes were introduced by Shamir [50] and Blakley [19] for the threshold case, and by Ito, Saito, and Nishizeki [40] for the general case. Threshold access structures, in which the authorized sets are all the sets containing at least t parties (for some threshold t), can be realized by secret-sharing schemes in which the size of each share is the size of the secret [19, 50]. There are other access structures that admit secret-sharing schemes in which the size of the shares is small, i.e., polynomial (in the number of parties) share size [17, 18, 22, 42]. In particular, Benaloh and Leichter [17] proved that if an access structure can be described by a small monotone formula, then it admits an efficient secret-sharing scheme. Improving on this result, Karchmer and Wigderson [42] showed that if an access structure can be described by a small monotone span program, then it has an efficient secret-sharing scheme.

The best known secret-sharing schemes for general access structures are highly inefficient, i.e., their total share size is $2^{0.64n}$ (where n is the number of parties) [43, 4, 5]. The best known lower bound on the total share size of secret-sharing schemes realizing an access structure is $\Omega(n^2/\log n)$ [30, 29]; this lower

bound is very far from the upper bound.

1.1.2 Graph Access Structures

A secret-sharing scheme realizes the graph access structure determined by a given graph if every two vertices connected by an edge can reconstruct the secret and every independent set in the graph does not get any information on the secret. The trivial secret-sharing scheme for realizing a graph access structure consists in sharing the secret independently for each edge; this results in a scheme whose total share size is $O(n^2)$ (times the length of the secret, which will be ignored in the introduction). This can be improved – every graph access structure can be realized by a linear secret-sharing scheme in which the total size of the shares is $O(n^2/\log n)$ [34, 24]. Graph access structures have been studied in many works, such as [25, 23, 52, 21, 20, 13, 31, 10, 12]. In particular, Beimel, Farràs, and Mintz [10] showed that a graph with n vertices that contains $\binom{n}{2} - n^{1+\beta}$ edges for some constant $0 \leq \beta < 1$ can be realized by a scheme in which the total share size is $\tilde{O}(n^{5/4+3\beta/4})$.

1.1.3 Forbidden Graph Access Structures

Secret-sharing schemes for graph access structures and forbidden graph access structures have similar requirements. Indeed, given a secret-sharing scheme for a graph access structure, we can construct a secret-sharing scheme for the forbidden graph access structure associated to the same graph: We can independently share the secret using the secret-sharing scheme for the graph access structure and the 3-out-of-n secret-sharing scheme of Shamir [50]. The total share size of the new scheme is slightly greater than the former. Therefore, upper bounds on the share size for graph access structures imply the same upper bounds on the share size for forbidden graph access structures. It is not known how to efficiently construct schemes for graph access structures from schemes for forbidden graph access structures.

From now on, the secret-sharing schemes considered in this work realize forbidden graph access structures. In order to simplify the notation, we say that a secret-sharing schemes realizes G, in order to say that the scheme realizes the forbidden graph access structure determined by G.

Beimel, Ishai, Kumaresan, and Kushilevitz [14] proved that every forbidden graph access structure can be realized by a secret-sharing scheme in which the total size of the shares is $O(n^{3/2})$. Gay, Kerenidis, and Wee [37] proved that the same total share size of $O(n^{3/2})$ can be achieved by a linear secret-sharing scheme. Liu, Vaikuntanathan, and Wee [44] showed that every forbidden graph access structure can be realized by a non-linear secret-sharing scheme in which the total share size is $n^{1+o(1)}$.

Beimel, Farràs, and Peter [12] showed that any forbidden graph with n vertices and with at least $\binom{n}{2} - n^{1+\beta}$ edges (for some constant $0 \leq \beta < \frac{1}{2}$) can be realized by a linear secret-sharing scheme with total share size $O(n^{7/6+2\beta/3})$. They also showed that if a forbidden graph G can be realized by a secret-sharing scheme with total share size m, and at most $n^{1+\beta}$ edges are removed from G, then the resulting forbidden graph can be realized by a secret-sharing scheme whose total share size is $O(m + n^{7/6+2\beta/3})$. These results are improved in this paper.

1.1.4 Conditional Disclosure of Secrets

Gertner et al. [38] defined conditional disclosure of secrets (CDS) protocols. In 2-party CDS protocols, two parties Alice and Bob want to disclose a secret to a referee if and only if their inputs (strings of N bits) satisfy some predicate (e.g., if their inputs are equal). To achieve this goal, each party computes one message based on its input, the secret, and a common random string, and sends the message to the referee. If the predicate

holds, then the referee, which knows the two inputs, can reconstruct the secret from the messages it received. CDS protocols can be used to efficiently realize symmetrically-private information retrieval protocols [38], and to construct attribute-based encryption protocols [37], a cryptographic primitive that was introduced in [39, 49].

There is a correspondence between CDS protocols in which the size of the input of the parties is N and secret-sharing schemes for bipartite graphs with $n = 2^N$ vertices in each part as we next explain. Every predicate defines a bipartite graph, where every input of Alice is a vertex in the first part of the graph and every input of Bob is a vertex in the second part of the graph, and there is an edge between two vertices from different parts if and only if the two corresponding inputs satisfy the predicate. Given a CDS protocol for a predicate, we can construct a secret-sharing scheme realizing the bipartite graph defined by the predicate in which the share of a party z is the message sent in the CDS protocol to the referee by Alice or Bob (depending on z's part of the graph) when they hold the input z. Conversely, given a secret-sharing scheme for the bipartite graph we can construct a CDS protocol in which the messages are the corresponding shares.

Gertner et al. [38] proved that if a predicate f has a (possibly non-monotone) formula of size S, then there is a CDS protocol for f in which the length of the messages is S. A similar result holds if the predicate has a (possibly non-monotone) span program. This result provides a rich class of predicates for which there are efficient CDS protocols, and thus a rich class of forbidden graph access structures that can be realized by efficient secret-sharing schemes.

A CDS protocol is linear over a field $\mathbb{F}$ if the domain of secrets is $\mathbb{F}$, the randomness is a vector over $\mathbb{F}$, and when the predicate holds, the reconstruction function of the referee is linear. It was shown in [37] that for every predicate there exists a linear CDS protocol such that the size of each of the messages sent by the two parties to the referee is $2^{N/2}$. This implies that for every bipartite graph there exists a linear secret-sharing scheme realizing its forbidden graph access structure in which the size of each share is $O(n^{1/2})$ (where n is the number of the parties); in particular, the total share size of this scheme is $O(n^{3/2})$.

Liu et al. [44] have shown that every predicate has a non-linear CDS protocol in which the size of the messages the parties send to the referee is $2^{O(\sqrt{N \log N})}$. As a corollary, we get a non-linear secret-sharing scheme realizing the forbidden graph access structure for every bipartite graph with n vertices, in which the size of each share is $n^{O(\sqrt{\log \log n / \log n})} = n^{o(1)}$; in particular, the total share size of this scheme is $n^{1+O(\sqrt{\log \log n / \log n})} = n^{1+o(1)}$. By a transformation of [14, 12], the above two results hold for every graph (not necessarily bipartite).

Applebaum et al. [3] and Ambrona et al. [1] have shown that if there is a linear CDS protocol for some predicate f with message length c and shared random string length r, then there is a linear CDS protocol for the complement predicate $\overline{f}$ in which the message length and the shared random string length is linear in c and r. Translated to secret-sharing, it implied that if we have a linear secret-sharing scheme that uses r random field elements in the generation of the shares and realizes the forbidden graph access structure of a bipartite graph G, then we can realize its complement bipartite graph $\overline{G}$ with a linear scheme in which the size of each share is $O(r)$.

Applebaum and Arkis [2] (improving on [3]) have proved that for every predicate there exists a multilinear CDS protocol[1] for k-bit secrets, where k is double-exponential in N, such that the size of each of the messages sent by the two parties to the referee is $O(k)$. This gives us an amortized share size of $O(1)$ bits per each bit of the secret, much better than the message size of $2^{N/2}$ in the linear CDS protocol for one-bit secret [37] and even much better than the message size of $2^{\sqrt{N \log N}}$ in the CDS protocol for one-bit secret [44]. When considering forbidden graph access structures, we get that for every forbidden bipartite

[1] A multilinear CDS protocol is similar to linear CDS protocol, except that the secret is a vector over the field (and not one field element as in linear schemes).

graph access structure with n vertices there exists a multilinear secret-sharing scheme with secrets of length k and total share size of $O(kn)$, provided that k is exponential in n (more precisely, $k \geq 2^{n^2}$).

1.2 Our Results

The main result we show in this paper is the construction of linear secret-sharing schemes realizing forbidden graph access structures for sparse graphs and dense graphs. We also prove tight lower bounds on the share size of linear secret-sharing schemes realizing forbidden graph access structures.

1.2.1 Constructions

Our main constructions of linear secret-sharing schemes are the following ones:

- Given a sparse graph with n vertices and at most $n^{1+\beta}$ edges, for some $0 \leq \beta < 1$, we construct a linear secret-sharing scheme realizing it with total share size $\tilde{O}(n^{1+\beta/2})$. The best previously known linear secret-sharing scheme for such graphs is the trivial scheme that independently shares the secret for each edge; the total share size of this scheme is $O(n^{1+\beta})$.

- Given a dense graph with n vertices and at least $\binom{n}{2} - n^{1+\beta}$ edges, for some $0 \leq \beta < 1$, we construct a linear secret-sharing scheme realizing it with total share size $\tilde{O}(n^{1+\beta/2})$. The best previously known linear secret-sharing scheme for such graphs is the scheme of [12], which has total share size $O(n^{7/6+2\beta/3})$.

- Given a sparse graph with n vertices and at most $n^{1+\beta}$ edges, for some $0 \leq \beta < 1$, we construct a linear secret-sharing scheme realizing it where the size of the share of *each party* is $\tilde{O}(n^{1/4+\beta/4})$. The same results holds for graphs with at least $\binom{n}{2} - n^{1+\beta}$ edges. The best previously known linear secret-sharing scheme for such forbidden graphs is the scheme of [37], which has no restrictions on the number of edges; the share size of each party in this scheme is $O(n^{1/2} \log n)$.

  In the above scheme, the max share size is $\tilde{O}(n^{5/4+\beta/4})$. We construct a secret-sharing scheme which gives a trade-off between the max share size and total share size. Specifically, for every $0 \leq \gamma \leq 1/4 - \beta/4$, there is a linear secret-sharing scheme realizing G in which the share size of each vertex is $\tilde{O}(n^{1/4+\beta/4+\gamma})$ and the total share size of this scheme is $\tilde{O}(n^{5/4+\beta/4-\gamma})$.

- Let Σ be a secret-sharing scheme realizing a forbidden graph G where the size of each share is ℓ the total share size of Σ is m, and let G' be a graph that is obtained from G by changing (adding or removing) at most $n^{1+\beta}$ edges for some $0 \leq \beta < 1$. We construct two secret-sharing schemes realizing G': One with total share size $m + \tilde{O}(n^{1+\beta/2})$, and another one in which the size of each share is $\ell + \tilde{O}(n^{1/4+\beta/4})$. If Σ is linear, then the resulting schemes are also linear.

Taking into account the connection described above between CDS protocols and secret-sharing schemes for forbidden graph access structures, our constructions imply linear CDS protocols with message size $\tilde{O}(N^{1/4+\beta/4})$ for two families of predicates $f : [N] \times [N] \to \{0,1\}$: Predicates f with a few zero's, i.e., $|\{(x,y) : f(x,y) = 0\}| \leq N^{1+\beta}$ (for some $0 \leq \beta < 1$) and predicates f with a few one's, i.e., $|\{(x,y) : f(x,y) = 1\}| \leq N^{1+\beta}$.

1.2.2 Overview of Our Constructions

We construct secret-sharing schemes realizing sparse graphs in four stages. We start by realizing fairly simple bipartite graphs, and in each stage we realize a wider class of graphs using the schemes constructed in previous stages.

Our basic construction, described in Lemma 3.2, is a linear secret-sharing scheme realizing a bipartite graph $G = (A, B, E)$, where A is small and the degree of each vertex in B is at most d, for some $d < n$. To create this scheme, we construct a linear subspace V_a for each vertex $a \in A$, and a vector $\mathbf{z_b}$ for every vertex $b \in B$, such that $\mathbf{z_b} \in V_a$ if and only if $(a, b) \in E$. This construction implies a monotone span program for the access structure, hence a linear secret-sharing scheme realizing the access structure. The total share size of this scheme is $O(d|A| + |B|)$. A naive scheme for this graph, which shares the secret independently for each edge, has total share size $O(d|B|)$. Our scheme is much more efficient than the naive scheme when A is small and B is big. This is the scheme that enables us to construct efficient schemes for sparse forbidden graph access structures.

In the second stage, we construct, in Lemma 4.1, a secret-sharing scheme realizing a bipartite graph $G = (A, B, E)$, where the degree of every vertex in B is at most d (and there is no restriction on the size of A). Then, we construct, in Lemma 4.2, a secret-sharing scheme with total share size $O(n\sqrt{d}\log n)$ for bipartite graphs with $|A| = |B| = n$, where the vertices in B have degree at most d. The idea of this construction is to *randomly* partition the set A to $\ell = O(\sqrt{d}\ln n) = \tilde{O}(\sqrt{d})$ "small" subsets $A_1, \ldots, A_\ell$. We prove that with high probability, for every $1 \leq i \leq \ell$, the degree of every vertex $b \in B$ in the bipartite graph $G_i = (A_i, B, E \cap (A_i \times B))$ is at most $O(\sqrt{d})$ (which is smaller than its degree in G, which can be at most d). Then, we realize each sparse graph G_i using the basic scheme.

In the third stage, we construct, in Theorem 4.3, a secret-sharing scheme for a bipartite graph $G = (A, B, E)$, where $|E| \leq n^{1+\beta}$ for some $0 \leq \beta < 1$ (where $|A| = |B| = n$). That is, we realize forbidden graph access structures for bipartite graphs where the *average* degree of each vertex in B is at most n^β. To this purpose, we use an idea from [10] (also used in [12]). For some degree d, let B_{big} be the vertices in B whose degree is at least d and let $B_{\text{small}} = B \setminus B_{\text{big}}$. Since the number of edges in G is at most $n^{1+\beta}$, the size of B_{big} is at most $n^{1+\beta}/d$. Using the fact that B_{big} is small (however, the degree of each vertex in B_{big} can be n), the secret-sharing scheme of [37] (alternatively, the scheme of Lemma 4.1) realizes the graph $G_{\text{big}} = (A, B_{\text{big}}, E \cap (A \times B_{\text{big}}))$ with "quite small" shares. Using the fact that the degree of each vertex in B_{small} is small, the secret-sharing scheme of Lemma 4.1 realizes $G_{\text{small}} = (A, B_{\text{small}}, E \cap (A \times B_{\text{small}}))$ with total share size $O(n\sqrt{d}\log n)$. By taking the appropriate value for d, we get a secret-sharing scheme realizing G in which (for small enough values of β) the total share size is $o(n^{1+\beta})$, but still larger than the promised total share size. To get a secret-sharing scheme realizing G with total share size $\tilde{O}(n^{1+\beta/2})$, we group the vertices in B into $O(\log n)$ sets according to their degree, where the ith set B_i contains the vertices whose degree is between $n/2^{i+1}$ and $n/2^i$. We realize each graph $G_i = (A, B_i, E \cap (A \times B_i))$ independently using the secret-sharing scheme of Lemma 4.1.

In the last stage, we construct, in Theorem 4.4, a secret-sharing scheme for any forbidden graph access structure with the promised total share size. That is, if the number of edges in G is at most $n^{1+\beta}$ for some $0 \leq \beta < 1$ (where $|V| = n$), then the total share size is $\tilde{O}(n^{1+\beta/2})$. We use a generic transformation from [14, 12], which constructs a secret-sharing scheme for any graph from secret-sharing schemes for bipartite graphs.

To summarize, there are 4 stages in our construction for sparse graphs. The first two stages are the major new steps in our construction. The third stage uses ideas from [10], and the last stage uses a transformation of [14, 12] as a black-box. The construction for dense graphs is similar, but we construct a different scheme in the first stage.

In addition, we construct linear secret-sharing schemes that minimize the size of each share. We construct a linear secret-sharing scheme realizing bipartite graphs $G = (A, B, E)$, where $|A| = |B| = n$ and the number of edges in G is at most $n^{1+\beta}$, for some $0 \leq \beta < 1$, in which the share size of each vertex is $O(n^{1/4+\beta/4} \log n)$. This construction is similar to the one of presented in the third stage. Let $d = n^{1/2+\beta/2}$, let A_{big} (respectively, B_{big}) be the vertices in A (respectively, B) whose degree is at least d, and let $A_{\text{small}} = A \setminus A_{\text{big}}$ (respectively, $B_{\text{small}} = B \setminus B_{\text{big}}$). Since the number of edges in G is at most $n^{1+\beta}$, the size of A_{big} (respectively, B_{big}) is at most $n^{1+\beta}/d = n^{1/2+\beta/2}$. Thus, we can realize the graph $(A_{\text{big}}, B_{\text{big}}, E \cap (A_{\text{big}} \times B_{\text{big}}))$ using the scheme of [37] in which the share size of each vertex is $O((n^{1/2+\beta/2})^{1/2}) = O(n^{1/4+\beta/4})$. Next, since the degree of each vertex in A_{small} (respectively, B_{small}) is at most d, we can realize each of the graphs $(A, B_{\text{small}}, E \cap (A \times B_{\text{small}}))$ and $(A_{\text{small}}, B, E \cap (A_{\text{small}} \times B))$ by using our scheme of the second stage in which the share size of each vertex is $O(\sqrt{d} \log n) = O(n^{1/4+\beta/4} \log n)$, and get the desired share size.

Given a secret-sharing scheme Σ realizing G, we use ideas from [12] to construct a scheme realizing a graph G', obtained by changing a few edges from G. First, we share the secret s using the secret-sharing scheme realizing the sparse graph containing all edges added to G (we add at most $n^{1+\beta}$ edges to G). In addition, we share the secret s using a 2-out-of-2 secret-sharing scheme. That is, we choose two random elements s_1 and s_2 such that $s = s_1 \oplus s_2$. We share s_1 using Σ and share s_2 using the secret-sharing scheme realizing the dense graph containing all possible edges except for the edges removed from G (this graph is a dense graph with at least $\binom{n}{2} - n^{1+\beta}$ edges, since we remove at most $n^{1+\beta}$ edges from G).

1.2.3 Lower Bounds

We prove that for almost all forbidden graph access structures, the total share size required by any linear secret-sharing scheme with a one-bit secret realizing these access structures is $\Omega(n^{3/2})$, which shows that the construction of Gay et al. [37] is optimal. This also shows a separation between the total share size in non-linear secret-sharing schemes realizing forbidden graph access structures, which is $n^{1+o(1)}$ by [44], and the total share size required in linear secret-sharing schemes realizing forbidden graph access structures. This lower bound implies that, for almost all predicates $f : [N] \times [N] \to \{0, 1\}$, in every linear CDS protocol for f the length of the messages is $\Omega(\sqrt{N})$.

The technique we developed for proving lower bounds for almost all forbidden graph access structures is also applied to other families of access structures. In particular, we apply it to access structures of rank r, i.e., access structures whose minimal authorized sets are of size at most r. We show that almost all rank r access structures with n parties, the total share size in every linear secret-sharing scheme with a one-bit secret is $\Omega(n^{(r+1)/2})$.

Furthermore, we show that for every $0 \leq \beta < 1$ there exist a graph with at most $n^{1+\beta}$ edges and a graph with at least $\binom{n}{2} - n^{1+\beta}$ edges, such that the total share size in any linear secret-sharing scheme realizing their forbidden graph access structures is $\Omega(n^{1+\beta/2})$. Finally, we show that for every $0 \leq \beta < 1$ there exist a graph with at most $n^{1+\beta}$ edges and a graph with at least $\binom{n}{2} - n^{1+\beta}$ edges, such that the size of the share of at least one party in any linear secret-sharing scheme realizing it is $\Omega(n^{1/4+\beta/4})$. These lower bounds show that our constructions are optimal (up to poly-logarithmic factors). Our lower bounds are existential and use counting arguments. They previously appeared (in a somewhat less general form) in the master thesis of the third author of this paper [46].

1.3 Paper Organization

The rest of the paper is organized as follows. In Section 2, we review the definition of secret-sharing schemes and other primitives. In Section 3, we present a basic secret-sharing scheme realizing graphs of low degree; this scheme is used later in different constructions. In Section 4, we construct secret-sharing schemes realizing sparse graphs and dense graphs. In Section 5, we construct secret-sharing schemes providing trade-offs between the total share size and the max share size for sparse and dense graphs. In particular, we present secret-sharing schemes with small max share size. Finally, in Section 6, we present lower bounds on the total share size and the max share size for linear secret-sharing schemes.

2 Preliminaries

In this section we define secret-sharing schemes, monotone span programs, forbidden graph access structures, and conditional disclosure of secrets protocols.

Notation. We denote the logarithmic function with base 2 and base e by $\log$ and $\ln$, respectively. We denote vectors by bold letters, e.g., $\mathbf{v}$.

2.1 Secret-Sharing Schemes

We present the definition of secret-sharing scheme as given in [27, 9]. For more information about this definition and secret-sharing in general, see [8].

Definition 2.1 (Secret-Sharing Schemes)**.** *Let $P = \{p_1, \ldots, p_n\}$ be a set of parties. A collection $\Gamma \subseteq 2^P$ is* monotone *if $B \in \Gamma$ and $B \subseteq C$ imply that $C \in \Gamma$. An* access structure *is a monotone collection $\Gamma \subseteq 2^P$ of non-empty subsets of P. Sets in Γ are called* authorized*, and sets not in Γ are called* unauthorized*. The family of minimal authorized sets is denoted by $\min \Gamma$.*

A distribution scheme *$\Sigma = \langle \Pi, \mu \rangle$ with domain of secrets K is a pair, where μ is a probability distribution on some finite set R called the set of random strings and Π is a mapping from $K \times R$ to a set of n-tuples $K_1 \times K_2 \times \cdots \times K_n$, where K_j is called the* domain of shares *of p_j. A dealer distributes a secret $k \in K$ according to Σ by first sampling a random string $r \in R$ according to μ, computing a vector of* shares *$\Pi(k, r) = (s_1, \ldots, s_n)$, and privately communicating each share s_j to party p_j. For a set $A \subseteq P$, we denote $\Pi_A(k, r)$ as the restriction of $\Pi(k, r)$ to its A-entries (i.e., the shares of the parties in A).*

Given a distribution scheme, we define the size *of the secret as $\log |K|$, the (normalized)* share size *of party p_j as $\log |K_j| / \log |K|$, the (normalized)* max share size *as $\max_{1 \leq j \leq n} \log |K_j| / \log |K|$, and the (normalized)* total share size *of the distribution scheme as $\sum_{1 \leq j \leq n} \log |K_j| / \log |K|$.*

Let K be a finite set of secrets, where $|K| \geq 2$. A distribution scheme $\langle \Pi, \mu \rangle$ with domain of secrets K is a secret-sharing scheme *realizing an access structure Γ if the following two requirements hold:*

CORRECTNESS. *The secret k can be reconstructed by any authorized set of parties. That is, for any set $B = \{p_{i_1}, \ldots, p_{i_{|B|}}\} \in \Gamma$, there exists a* reconstruction function *$\mathrm{Recon}_B : K_{i_1} \times \ldots \times K_{i_{|B|}} \to K$ such that for every secret $k \in K$ and every random string $r \in R$,*

$$\mathrm{Recon}_B \left(\Pi_B(k, r) \right) = k.$$

PRIVACY. *Every unauthorized set cannot learn anything about the secret (in the information theoretic sense) from their shares. Formally, for any set $T \notin \Gamma$, every two secrets $a, b \in K$, and every possible vector of*

shares $\langle s_j \rangle_{p_j \in T}$,

$$\Pr[\, \Pi_T(a, r) = \langle s_j \rangle_{p_j \in T} \,] = \Pr[\, \Pi_T(b, r) = \langle s_j \rangle_{p_j \in T} \,],$$

when the probability is over the choice of r *from* R *at random according to* μ.

Definition 2.2 (Linear Secret-Sharing Scheme)**.** *Let* $\Sigma = \langle \Pi, \mu \rangle$ *be a secret-sharing scheme with domain of secrets* K*, where* μ *is a probability distribution on a set* R *and* Π *is a mapping from* $K \times R$ *to* $K_1 \times K_2 \times \cdots \times K_n$*. We say that* Σ *is a* linear secret-sharing scheme over a finite field $\mathbb{F}$ *if* $K = \mathbb{F}$*, the sets* $R, K_1, \ldots, K_n$ *are vector spaces over* $\mathbb{F}$*,* Π *is a* $\mathbb{F}$*-linear mapping, and* μ *is the uniform probability distribution over* R.

2.2 Monotone Span Programs

Monotone span programs (abbreviated MSPs) are a linear-algebraic model of computation introduced by Karchmer and Wigderson [42]. As explained below in Claim 2.4, MSPs over finite fields are equivalent to linear secret-sharing schemes.

Definition 2.3 (Monotone Span Programs [42])**.** *A* monotone span program *is a quadruple* $\widehat{M} = \langle \mathbb{F}, M, \delta, \mathbf{v} \rangle$*, where* $\mathbb{F}$ *is a field,* M *is an* $a \times b$ *matrix over* $\mathbb{F}$*,* $\delta : \{1, \ldots, a\} \to P$ *(where* P *is a set of parties) is a mapping labeling each row of* M *by a party,*[2] *and* $\mathbf{v}$ *is a non-zero vector in* $\mathbb{F}^b$*, called the target vector. The size of* $\widehat{M}$ *is the number of rows of* M *(i.e.,* a*). For any set* $A \subseteq P$*, let* M_A *denote the sub-matrix obtained by restricting* M *to the rows labeled by parties in* A*. We say that* $\widehat{M}$ *accepts a set* $B \subseteq P$ *if the rows of* M_B *span the vector* $\mathbf{v}$*. We say that* $\widehat{M}$ *accepts an access structure* Γ *if* $\widehat{M}$ *accepts a set* B *if and only if* $B \in \Gamma$.

By applying a linear transformation to the rows of M, the target vector can be changed to any non-zero vector without changing the size of the MSP. The default value for the target vector is $\mathbf{e_1} = (1, 0, \ldots, 0)$, but in this work we also use other vectors, e.g., $\mathbf{1}$ (the all one's vector).

Claim 2.4 ([42, 7])**.** *Let* $\mathbb{F}$ *be a finite field. There exists a linear secret-sharing scheme over* $\mathbb{F}$ *realizing* Γ *with total share size* a *if and only if there exists an MSP over* $\mathbb{F}$ *of size* a *accepting* Γ.

For the sake of completeness, we explain how to construct a linear secret-sharing scheme from an MSP. Given an MSP $\widehat{M} = \langle \mathbb{F}, M, \delta, \mathbf{e_1} \rangle$ accepting Γ, where M is an $a \times b$ matrix over $\mathbb{F}$, define a linear secret-sharing scheme as follows:

- **Input:** a secret $k \in \mathbb{F}$.
- Choose $b - 1$ random elements $r_2, \ldots, r_b$ independently with uniform distribution from $\mathbb{F}$ and define $\mathbf{r} = (k, r_2, \ldots, r_b)$.
- Evaluate $(s_1, \ldots, s_a) = M\mathbf{r}^T$, and distribute to each party $p \in P$ the entries corresponding to rows labeled by p.

In this linear secret-sharing scheme, every set in Γ can reconstruct the secret: Let $B \in \Gamma$ and $N = M_B$, thus, the rows of N span $\mathbf{e_1}$, and there exists some vector $\mathbf{v}$ such that $\mathbf{e_1} = \mathbf{v}N$. Notice that the shares of the parties in B are $N\mathbf{r}^T$. The parties in B can reconstruct the secret by computing $\mathbf{v}(N\mathbf{r}^T)$, since

$$\mathbf{v}(N\mathbf{r}^T) = (\mathbf{v}N)\mathbf{r}^T = \mathbf{e_1} \cdot \mathbf{r}^T = k.$$

The privacy proof of this scheme can be found in [42, 8].

[2] We label a row by a party rather than by a variable x_j as done in [42].

2.3 Forbidden Graph Access Structures

Recall that a *bipartite graph* $G = (A, B, E)$ is a graph where the vertices are $A \cup B$ (A and B are called the parts of G) and $E \subseteq A \times B$. A bipartite graph is *complete* if $E = A \times B$.

Definition 2.5 (The Bipartite Complement)**.** *Let $G = (A, B, E)$ be a bipartite graph. The* bipartite complement *of G is the bipartite graph $\overline{G} = (A, B, \overline{E})$, where every $a \in A$ and $b \in B$ satisfy $(a, b) \in \overline{E}$ if and only if $(a, b) \notin E$.*

Definition 2.6 (Forbidden Graph Access Structures)**.** *Let $G = (V, E)$ be a graph. The* forbidden graph access structure *defined by G is the collection of all pairs of vertices in E and all subsets of vertices of size greater than two.* [3]

Remark 2.7. As mentioned above, when we say that a secret-sharing scheme realizes a graph G, we mean that the scheme realizes the forbidden graph access structure of the graph G.

Next, we show how to realize the forbidden graph access structure of the union or the intersection of two graphs. This construction will be used later in the paper.

Claim 2.8. *Let Σ_1 and Σ_2 be two secret-sharing schemes with the same domain of secrets that realize $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$, respectively. Let ℓ_1 and ℓ_2 be the max share size of Σ_1 and Σ_2, respectively, and let m_1 and m_2 be the total share size of Σ_1 and Σ_2, respectively. Then, the graphs $G' = (V, E_1 \cup E_2)$ and $G'' = (V, E_1 \cap E_2)$ can be realized by secret-sharing schemes with max share size smaller than or equal to $\ell_1 + \ell_2$ and total share size $m_1 + m_2$.*

Proof. Let K be the domain of secrets of Σ_1 and Σ_2, and let $N = |K|$. We assume that $K = \{0, \ldots, N-1\}$. Let $s \in K$ be the secret to be shared.

First, observe that the intersection of the forbidden graph access structures of G_1 and G_2 is the forbidden graph access structure of G', and that the union of the forbidden graph access structures of G_1 and G_2 is the forbidden graph access structure of G''.

For G', we share s using Σ_1, and independently share s using Σ_2. The access structure of this new scheme is the union of the access structures of Σ_1 and Σ_2, which coincides with the forbidden graph access structure of G'.

For G'', we share the secret s using a 2-out-of-2 secret-sharing scheme. That is, we choose an element $s_1 \in K$ at random, and take $s_2 = (s - s_1) \mod N$. Then, we independently share s_1 using Σ_1 and share s_2 using Σ_2. The access structure of this new scheme is the intersection of the access structures of Σ_1 and Σ_2, which coincides with the forbidden graph access structure of G''.

In both cases, the max share size of the resulting scheme is at most $\ell_1 + \ell_2$, and the total share size is $m_1 + m_2$. □

2.4 Conditional Disclosure of Secrets

For the sake of completeness, we present the definition of conditional disclosure of secrets, originally defined in [38].

[3] In [53], the access structure is specified by the complement graph, i.e., by the edges that are forbidden from learning information on the secret.

Definition 2.9 (Conditional Disclosure of Secrets)**.** *Let $f : \{0,1\}^N \times \{0,1\}^N \to \{0,1\}$ be some function (also called predicate), and let $\text{ENC}_A : \{0,1\}^N \times S \times R \to M_A$, $\text{ENC}_B : \{0,1\}^N \times S \times R \to M_B$ be deterministic functions, where S is the domain of secrets and R is the domain of common random strings, and $\text{DEC} : \{0,1\}^N \times \{0,1\}^N \times M_A \times M_B \to S$ be a deterministic function. Then, $(\text{ENC}_A, \text{ENC}_B, \text{DEC})$ is a* conditional disclosure of secrets *(CDS) protocol for the function f if the following two requirements hold:*

CORRECTNESS. *For every $x, y \in \{0,1\}^N$ with $f(x,y) = 1$, every secret $s \in S$, and every common random string $r \in R$,*

$$\text{DEC}(x, y, \text{ENC}_A(x, s, r), \text{ENC}_B(y, s, r)) = s.$$

PRIVACY. *For every $x, y \in \{0,1\}^N$ with $f(x,y) = 0$, every two secrets $s_1, s_2 \in S$, and every messages $m_A \in M_A, m_B \in M_B$:*

$$\begin{aligned} &\Pr[\,\text{ENC}_A(x, s_1, r) = m_A \text{ and } \text{ENC}_B(y, s_1, r) = m_B\,] \\ &\quad = \Pr[\,\text{ENC}_A(x, s_2, r) = m_A \text{ and } \text{ENC}_B(y, s_2, r) = m_B\,], \end{aligned}$$

when the probability is over the choice of r from R at random with uniform distribution.

Remark 2.10. When using a secret-sharing scheme to construct a CDS protocol (as explained in Section 1.1.4), the only requirement is that pairs of vertices can reconstruct the secret if and only if they are connected by an edge. Hence, there may be subsets of vertices of size greater than two for which there are no requirements. In particular, it is enough to restrict the study to forbidden graph access structures, in which all sets of 3 or more vertices are authorized. This additional requirement increases only slightly the total share size required to realize forbidden graph access structures, since we can independently share the secret using the 3-out-of-n scheme of Shamir [50], in which the size of the share of every party is the size of the secret (when the size of the secret is at least $\log n$). To simplify the description of our schemes, in all our constructions we implicitly assume that we share the secret using Shamir's 3-out-of-n secret-sharing scheme.

3 The Basic Constructions for Graphs of Low Degree

Our basic construction for graphs of low degree is presented in Lemma 3.2. It requires the following construction of linear spaces, which will also be used for dense graphs.

Claim 3.1. *Let $G = (A, B, E)$ be a bipartite graph with $A = \{a_1, \ldots, a_m\}$, $B = \{b_1, \ldots, b_n\}$ such that the degree of every vertex in B is at most d and let $\mathbb{F}$ be a finite field with $|\mathbb{F}| \geq m$. Then, there are m linear subspaces $V_1, \ldots, V_m \subseteq \mathbb{F}^{d+1}$ of dimension d and $n+1$ vectors $\mathbf{z_1}, \ldots, \mathbf{z_n}, \mathbf{w} \in \mathbb{F}^{d+1}$ such that*

$$\mathbf{z_j} \in V_i \text{ if and only if } (a_i, b_j) \in E,$$

and $\mathbf{w} \notin V_i$ for every $1 \leq i \leq m$.

Proof. We identify vectors in $\mathbb{F}^{d+1}$ with polynomials of degree at most d in the indeterminate X. That is, for a vector $\mathbf{v} \in \mathbb{F}^{d+1}$ we consider a polynomial $v(X) \in \mathbb{F}[X]$ of degree d in which the coefficient of degree i is the $(i+1)$-th coordinate of $\mathbf{v}$.

For each vertex $a_i \in A$, we associate a distinct element $\alpha_i \in \mathbb{F}$. We define the subspace $V_i \subseteq \mathbb{F}^{d+1}$ of dimension d as the one associated to the space of polynomials $P(X)$ of degree at most d such that

$P(\alpha_i) = 0$, i.e., the space of polynomials spanned by $\left\{(X - \alpha_i), (X^2 - \alpha_i \cdot X), \ldots, (X^d - \alpha_i \cdot X^{d-1})\right\}$. Since these d polynomials are linearly independent, the dimension of each V_i is d. Furthermore, for a vertex $b_j \in B$, whose neighbors are $a_{i_1}, a_{i_2}, \ldots, a_{i_{d'}}$ (for some $d' \leq d$), we define

$$z_j(X) = (X - \alpha_{i_1}) \cdot (X - \alpha_{i_2}) \cdot \ldots \cdot (X - \alpha_{i_{d'}}).$$

Note that $\mathbf{z_j} \in V_i$ if and only if $z_j(\alpha_i) = 0$ if and only if $\alpha_i \in \left\{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{d'}}\right\}$ if and only if $(a_i, b_j) \in E$.

Finally, define $w(X) = 1$. For every $1 \leq i \leq m$, the vector $\mathbf{w}$ is not in V_i because $w(\alpha_i) \neq 0$. □

Lemma 3.2. *Let $G = (A, B, E)$ be a bipartite graph with $|A| = m$, $|B| = n$, such that the degree of every vertex in B is at most d. Then, there is a linear secret-sharing scheme realizing G with total share size $n + (d + 1)m$.*

Proof. Denote $A = \{a_1, \ldots, a_m\}$ and $B = \{b_1, \ldots, b_n\}$. We construct a monotone span program accepting G, where there are $d + 1$ rows labeled by a_i for every $1 \leq i \leq m$ and one row labeled by b_j for every $1 \leq j \leq n$. By Claim 2.4, this implies the desired linear secret-sharing scheme.

Let $V_1, \ldots, V_m$ and $\mathbf{z_1}, \ldots, \mathbf{z_n}$ be the linear subspaces and the vectors guaranteed by Claim 3.1. For every $1 \leq i \leq m$, let $\{\mathbf{v_{i,1}}, \ldots, \mathbf{v_{i,d}}\}$ be a basis of V_i. Define $\mathbf{v'_{i,\ell}} = (0, 0, \mathbf{v_{i,\ell}})$ for every $1 \leq i \leq m$ and $1 \leq \ell \leq d$ (that is, $\mathbf{v'_{i,\ell}}$ is the vector in $\mathbb{F}^{d+3}$ whose first two coordinates are 0 followed by the vector $\mathbf{v_{i,\ell}}$).

We consider the monotone span program with target vector is $(1, 1, 0, \ldots, 0)$ in which the rows labeled by a_i are $\mathbf{v'_{i,1}}, \ldots, \mathbf{v'_{i,d}}$ and $(0, 1, 0, \ldots, 0)$, and the row labeled by b_j is $\mathbf{z'_j} = (1, 0, \mathbf{z_j})$.

The monotone span program accepts $(a_i, b_j) \in A \times B$ if and only if

$$(1, 1, 0, \ldots, 0) \in \operatorname{span}\left\{\mathbf{z'_j}, \mathbf{v'_{i,1}}, \ldots, \mathbf{v'_{i,d}}, (0, 1, 0, \ldots, 0)\right\}.$$

This condition is satisfied if and only if $\mathbf{z_j} \in \operatorname{span}\{\mathbf{v_{i,1}}, \ldots, \mathbf{v_{i,d}}\}$, that is, if and only if $\mathbf{z_j} \in V_i$. Hence, by Claim 3.1, the monotone span program accepts (a_i, b_j) if and only if $(a_i, b_j) \in E$. Furthermore, two vertices from the same part do not span $(1, 1, 0, \ldots, 0)$: For two vertices in A, this follows since the first coordinate in all vectors they label is 0. For two vertices in B, this follows since the second coordinate in the vectors they label is 0. Therefore, the monotone span program accepts G. □

Remark 3.3. The construction of Lemma 3.2 can be slightly improved by replacing the rows labeled by every vertex $a_i \in A$ with degree less than d in G, which are $\mathbf{v'_{i,1}}, \ldots, \mathbf{v'_{i,d}}$ and $(0, 1, 0, \ldots, 0)$, with the rows $(0, 0, \mathbf{z_j})$ for every $b_j \in B$ such that $(a_i, b_j) \in E$ and $(0, 1, 0, \ldots, 0)$. It is easy to verify that for such $a_i \in A$ with degree less than d, the monotone span program accepts $(a_i, b_j) \in A \times B$ if and only if $(a_i, b_j) \in E$.

In this way, the total share size is $n + m + \sum_{i=1}^{m} \min\{\deg(a_i), d\}$, instead of $n + m + dm$ in the construction of Lemma 3.2. This improvement guarantees that the total share size of the scheme is at most $n + m + |E|$. However, this improvement cannot be used to improve the bounds on the share size of our constructions in Theorem 3.5 and in Section 4.

In Lemma 3.4 we prove an analogues result for dense graphs.

Lemma 3.4. *Let $G = (A, B, E)$ be a bipartite graph with $|A| = m$, $|B| = n$, such that the degree of every vertex in B is at least $m - d$. Then, there is a linear secret-sharing scheme realizing G with total share size $2n + (d + 1)m$.*

Proof. Denote $A = \{a_1, \ldots, a_m\}$, $B = \{b_1, \ldots, b_n\}$. Let $\overline{G} = (A, B, \overline{E})$ be the bipartite complement of G, and let $V_1, \ldots, V_m \subseteq \mathbb{F}^{d+1}$ be the linear subspaces of dimension d and $\mathbf{z_1}, \ldots, \mathbf{z_n}, \mathbf{w} \in \mathbb{F}^{d+1}$ be the

vectors guaranteed by Claim 3.1 for the graph $\overline{G}$. As proved in Claim 3.1, $\mathbf{z_j} \in V_i$ if and only if $(a_i, b_j) \notin E$ and $\mathbf{w} \notin V_i$ for every $1 \leq i \leq m$.

Next, we construct a monotone span program where there are $d+1$ rows labeled by a_i for every $1 \leq i \leq m$ and two rows labeled by b_j for every $1 \leq j \leq n$. Let $\{\mathbf{v_{i,1}}, \ldots, \mathbf{v_{i,d}}\}$ be a basis of V_i. The rows labeled by a_i are $(0, 0, \mathbf{v_{i,1}}), \ldots, (0, 0, \mathbf{v_{i,d}}), (0, 1, 0, \ldots, 0)$ and the rows labeled by b_j are $(0, 0, \mathbf{z_j})$ and $(1, 0, \ldots, 0)$. We take $(1, 1, \mathbf{w})$ as the target vector.

We first prove that the span program accepts an edge $(a_i, b_j) \in E$. Since $(a_i, b_j) \in E$, it holds that $\mathbf{z_j} \notin V_i$ and so the dimension of $\operatorname{span}\{\mathbf{z_j}, \mathbf{v_{i,1}}, \ldots, \mathbf{v_{i,d}}\}$ is 1 plus the dimension of V_i, i.e., $\operatorname{span}\{\mathbf{z_j}, \mathbf{v_{i,1}}, \ldots, \mathbf{v_{i,d}}\} = \mathbb{F}^{d+1}$, and in particular,

$$\mathbf{w} \in \operatorname{span}\{\mathbf{z_j}, \mathbf{v_{i,1}}, \ldots, \mathbf{v_{i,d}}\}.$$

Thus, $(1, 1, \mathbf{w})$ is in the span of the vectors labeled by a_i and b_j.

We next prove that this monotone span program does not accept any pair $(a_i, b_j) \notin E$ where $a_i \in A$ and $b_j \in B$. By Claim 3.1, $\mathbf{w} \notin V_i$. Since $(a_i, b_j) \notin E$, it holds that $\mathbf{z_j} \in V_i$ and so $\mathbf{w} \notin \operatorname{span}\{\mathbf{z_j}, \mathbf{v_{i,1}}, \ldots, \mathbf{v_{i,d}}\} = V_i$. Thus, $(1, 1, \mathbf{w})$ is not in the span of the vectors labeled by a_i and b_j.

Furthermore, two vertices from the same part do not span $(1, 1, \mathbf{w})$: For two vertices in A, this follows since the first coordinate in all vectors they label is 0. For two vertices in B, this follows since the second coordinate in the vectors they label is 0. Therefore, the monotone span program accepts G. □

Next, we show that Lemma 3.2 can be used to realize every bipartite graph by a linear secret-sharing scheme with total share size $O(n^{3/2})$. This scheme has the same total share size as the one in [37]. This construction is presented as a warm-up for our constructions for bipartite graphs with bounded degree.

Theorem 3.5. *Let $G = (A, B, E)$ be a bipartite graph such that $|A| = |B| = n$. Then, there is a linear secret-sharing scheme realizing G with total share size $O(n^{3/2})$.*

Proof. We arbitrarily partition A into $\sqrt{n}$ sets, $A_1, \ldots, A_{\sqrt{n}}$, each set of size at most $\sqrt{n}$. By Lemma 3.2, the bipartite graph $(A_i, B, E \cap (A_i \times B))$ can be realized by a linear secret-sharing scheme with total share size $O(n + (\sqrt{n}+1)\sqrt{n}) = O(n)$, because every vertex in B has at most $|A_i| \leq \sqrt{n}$ neighbors. We use this construction for each of the $\sqrt{n}$ sets $A_1, \ldots, A_{\sqrt{n}}$. Hence, the total share size of the resulting scheme is $O(n^{3/2})$. □

It can be verified that in the secret-sharing scheme of Theorem 3.5, the size of the share of each vertex is $O(n^{1/2})$.

4 Secret-Sharing Schemes for Sparse and Dense Graphs

In this section we present efficient secret-sharing schemes realizing sparse and dense graphs, that is, graphs with at most $n^{1+\beta}$ edges or at least $\binom{n}{2} - n^{1+\beta}$ edges, for some $0 \leq \beta < 1$. The main result is Theorem 4.4, where we show that these graphs admit secret-sharing schemes with total share size $O(n^{1+\beta/2} \log^3 n)$. Its proof is involved, and we use several intermediate results. First, we construct efficient secret-sharing schemes for sparse and dense bipartite graphs. In the construction for a sparse or a dense bipartite graph $G = (A, B, E)$ in Theorem 4.3, we partition the vertices in B into $O(\log n)$ sets according to their degree: The vertices in the ith set B_i are the vertices whose degrees are between $n/2^{i+1}$ and $n/2^i$. We realize each graph $G_i = (A, B_i, E \cap (A \times B_i))$ independently using the secret-sharing scheme of Lemma 4.1. This methodology is the same as in [10, 12]. The main new technical result in this section is Lemma 4.1, and it

is the basis of this construction. Finally, using a transformation that appeared in [14], we use the schemes for sparse and dense bipartite graphs to construct a scheme for general sparse and dense graphs.

Lemma 4.1. *Let $G = (A, B, E)$ be a bipartite graph with $|A| = n$, $|B| \leq n$, such that the degree of each vertex in B is at most d or the degree of every vertex in B is at least $n - d$, for some $d \leq n$. If $d|B| \geq n \log^2 n$, then there is a linear secret-sharing scheme realizing G in which the share size of each vertex is $O(\sqrt{nd/|B|} \log n)$. The total share size of this scheme is $O(\sqrt{n|B|d} \log n)$.*

Proof. We first prove the lemma for the case that the degree of every vertex in B is at most d. We define the parameters δ, γ, α, and ℓ as $\delta = \log_n d$ (that is, $d = n^\delta$), $\gamma = \log_n |B|$,

$$\alpha = \frac{1}{2} + \frac{\gamma}{2} - \frac{\delta}{2}, \tag{1}$$

and $\ell = 2n^{1-\alpha} \ln n$. We first prove that there are sets $A_1, \ldots, A_\ell \subset A$ of size n^α that satisfy the following properties:

(I) $\bigcup_{i=1}^{\ell} A_i = A$, and

(II) for every $1 \leq i \leq \ell$, the degree of the vertices in B in the graph $G_i = (A_i, B, E \cap (A_i \times B))$ is at most $12n^{\alpha+\delta-1}$.

For each $1 \leq i \leq \ell$, we independently choose A_i with uniform distribution among the subsets of A of size n^α. We show that, with positive probability, $A_1, \ldots, A_\ell$ satisfy properties (I) and (II).

First, we analyze the probability that (I) does not hold.

$$\begin{aligned} \Pr[A \neq \cup A_i] &\leq \sum_{a \in A} \Pr[a \notin \cup A_i] = \sum_{a \in A} \prod_{i=1}^{\ell} \Pr[a \notin A_i] = \sum_{a \in A} \left(1 - \frac{n^\alpha}{n}\right)^\ell \\ &\leq \sum_{a \in A} e^{-\ell/n^{1-\alpha}} = n\frac{1}{n^2} = \frac{1}{n}. \end{aligned}$$

Now we show that the probability that the sets $A_1, \ldots, A_\ell$ do not satisfy Property (II) is less than $1/4$. Fix an index $1 \leq i \leq \ell$ and a vertex $b \in B$. We analyze the probability that the degree of b in G_i is larger than $12n^{\alpha+\delta-1}$. We view the choice of the random set A_i as a process of n^α steps, where in the jth step we uniformly choose a vertex $a_j \in A$ amongst the vertices that have not been chosen in the first $j - 1$ steps. Using this view of choosing A_i, we define the following binary random variables $Z_1, \ldots, Z_{n^\alpha}$, where $Z_j = 1$ if (a_j, b) is an edge of G_i, and 0 otherwise. Then, we consider $Z = \sum_{j=1}^{n^\alpha} Z_j$, that is, Z is the degree of b in G_i.

We would like to apply a Chernoff bound to these variables, however, they are not independent. We use $Z_1, \ldots, Z_{n^\alpha}$ to define new random variables $Z'_1, \ldots, Z'_{n^\alpha}$ that are independent. For every $j \in [n^\alpha]$ and every binary vector $\mathbf{z} = (z_t)_{t \in [j-1]}$, let

$$p_{\mathbf{z}} = \Pr[\, Z_j = 1 | Z_t = z_t \text{ for all } t \in [j-1]\,].$$

By convention, if $\Pr[\, Z_t = z_t \text{ for all } t \in [j-1]\,] = 0$, then $p_{\mathbf{z}} = 0$. Note that

$$p_{\mathbf{z}} \leq \frac{n^\delta}{n - n^\alpha} \leq \frac{2}{n^{1-\delta}},$$

where $d = n^\delta$ is an upper bound on the number of vertices connected to b that can be chosen in the jth step, and $n - n^\alpha$ is a lower bound on the number of vertices that can be chosen in the jth step. Observe that the last inequality follows because $n^{1/2} \leq n^{\delta/2+\gamma/2}/\log n$, so

$$n^\alpha = n^{1/2+\gamma/2-\delta/2} \leq \frac{n^{(\delta/2+\gamma/2)+\gamma/2-\delta/2}}{\log n} = \frac{n^\gamma}{\log n} \leq \frac{n}{2},$$

obtaining that $n - n^\alpha \geq n/2$. The random variables $Z'_1, \ldots, Z'_{n^\alpha}$ are defined as follows. Let $z_1, \ldots, z_{n^\alpha}$ be the values given to $Z_1, \ldots, Z_{n^\alpha}$. If $z_j = 1$ then $Z'_j = 1$, and if $z_j = 0$ then $Z'_j = 1$ with probability $(2/n^{1-\delta} - p_{\mathbf{z}})/(1 - p_{\mathbf{z}})$ and $Z'_j = 0$ otherwise. Thus,

$$\Pr[\, Z'_j = 1 | Z_t = z_t \text{ for all } t \in [j-1]\,] = \frac{2}{n^{1-\delta}}.$$

Thus, Z'_j is independent of $(Z_t)_{t\in[j-1]}$, and, hence, independent of $(Z'_t)_{t\in[j-1]}$, for every $j \in [n^\alpha]$.

Let $Z' = \sum_{j=1}^{n^\alpha} Z'_j$. The expected value of Z' is $n^\alpha \cdot 2/n^{1-\delta} = 2n^{\alpha+\delta-1}$. Using a Chernoff bound [47, Theorem 4.4, (4.3)], we obtain

$$\Pr\left[Z > 12n^{\alpha+\delta-1}\right] \leq \Pr\left[Z' > 12n^{\alpha+\delta-1}\right] \leq 2^{-12n^{\alpha+\delta-1}}.$$

Since $n^{\gamma+\delta} \geq n \log^2 n$, by (1) we obtain $n^{\alpha+\delta-1} = n^{\gamma/2+\delta/2-1/2} \geq \log n$. Thus,

$$\Pr\left[Z > 12n^{\alpha+\delta-1}\right] \leq \frac{1}{n^{12}} \leq \frac{1}{4n\ell}.$$

Property (II) holds if for every $b \in B$ and every $1 \leq i \leq \ell$, the degree of b in G_i is at most $12n^{\alpha+\delta-1}$. By the union bound, the probability that (II) does not hold is at most $1/4$. Thus, again by the union bound, the probability that random sets $A_1, \ldots, A_\ell$ satisfy properties (I) and (II) is greater than $1/2$, and, in particular, such sets exist.

Given valid sets $A_1, \ldots, A_\ell$, we construct a secret-sharing scheme for each bipartite graph $G_i = (A_i, B, E \cap (A_i \times B))$ using Lemma 3.2. In each one of these subgraphs, the degree of each vertex in B is at most $12n^{\alpha+\delta-1}$. Hence, the total share size of the resulting scheme is

$$\begin{aligned}
\sum_{i=1}^{\ell} \left(|B| + |A_i| \cdot (12n^{\alpha+\delta-1} + 1)\right) &= O\left(\ell(n^\gamma + n^\alpha n^{\alpha+\delta-1})\right) \\
&= O\left(n^{1-\alpha} \ln n (n^\gamma + n^{2\alpha+\delta-1})\right) \\
&= O\left(\log n (n^{1+\gamma-\alpha} + n^{\alpha+\delta})\right).
\end{aligned}$$

This value is minimized when $1 + \gamma - \alpha = \alpha + \delta$, that is, when $\alpha = \frac{1}{2} + \frac{\gamma}{2} - \frac{\delta}{2}$ (this explains our choice of α). Using this value of α, we obtain total share size of $O(n^{1/2+\gamma/2+\delta/2} \log n) = O(\sqrt{n|B|d} \log n)$.

Additionally, every vertex in B participates in ℓ schemes, and gets a share of size one in each of these schemes. Hence, the share size of every vertex in B is

$$\ell = O(n^{1-\alpha} \log n) = O(n^{1/2+\delta/2-\gamma/2} \log n) = O(\sqrt{nd/|B|} \log n).$$

We can assume that each vertex in A is a member of exactly one set (by removing the vertex from every set except from one). Every vertex in A participates in one scheme, and gets a share of size

$$12n^{\alpha+\delta-1} + 1 = O(n^{\gamma/2+\delta/2-1/2}) = O(\sqrt{|B|d/n})$$

in this scheme. Overall, the share size of each vertex in the resulting scheme is $O(\sqrt{nd/|B|}\log n)$.

To prove the lemma for the case that the degree of every vertex in B is at least $n-d$, we take the bipartite complement $\overline{G} = (A, B, \overline{E})$, in which the degree of every vertex in B is at most d. We follow the same steps of the above proof with $\overline{G}$, except that we use the scheme of Lemma 3.4 to realize each bipartite graph G_i, instead of the scheme of Lemma 3.2. □

Lemma 4.2 is a special case of the Lemma 4.1 for $|A| = |B|$. In the proof of Lemma 4.2, we also take care of the case that d is small (in Lemma 4.1 we require that $d|B| > n\log^2 n$).

Lemma 4.2. *Let $G = (A, B, E)$ be a bipartite graph such that $|A| = |B| = n$ and the degree of every vertex in B is at most d or the degree of every vertex in B is at least $n - d$, for some $d \leq n$. Then, there is a linear secret-sharing scheme realizing G in which the share size of each vertex is $O(\sqrt{d}\log n)$ and the total share size of this scheme is $O(n\sqrt{d}\log n)$.*

Proof. If $d < \log^2 n$ and the degree of every vertex in B is at most d, we use the secret-sharing scheme of Lemma 3.2; in this scheme the share size of each vertex is $O(d) = O(\sqrt{d}\log n)$, and the total share size is $O(n\sqrt{d}\log n)$.

If $d < \log^2 n$ and the degree of every vertex in B is at least $n - d$, we use the construction presented in [12, Lemma 3.8]; in this scheme the share size of every vertex is $O(d) = O(\sqrt{d}\log n)$ and the total share size is $O(n\sqrt{d}\log n)$.

Otherwise, $d \geq \log^2 n$. In this case, $d|B| \geq n\log^2 n$ (since $|B| = n$), so we get the desired secret-sharing scheme from Lemma 4.1. □

Theorem 4.3. *Let $G = (A, B, E)$ be a bipartite graph with $|A| = |B| = n$ such that either $|E| \leq n^{1+\beta}$ or $|E| \geq n^2 - n^{1+\beta}$, for some constant $0 \leq \beta < 1$. Then, there is a linear secret-sharing scheme realizing G in which the share size of each vertex is $O(n^{1/3+\beta/6}\log^2 n)$, and the total share size of this scheme is $O(n^{1+\beta/2}\log^2 n)$.*

Proof. Suppose that $G = (A, B, E)$ is a bipartite graph with $|E| \leq n^{1+\beta}$. Define $A_{\text{small}} = \left\{a \in A : \deg(a) \leq n^{1/3+2\beta/3}\right\}$, $A_{\text{big}} = A \setminus A_{\text{small}}$, $B_{\text{small}} = \left\{b \in B : \deg(b) \leq n^{1/3+2\beta/3}\right\}$, and $B_{\text{big}} = B \setminus B_{\text{small}}$. Since the number of edges in G is at most $n^{1+\beta}$ and the degree of every vertex in A_{big} and B_{big} is at least $n^{1/3+2\beta/3}$, the number of vertices in A_{big} and the number of vertices in B_{big} is at most $\frac{n^{1+\beta}}{n^{1/3+2\beta/3}} = n^{2/3+\beta/3}$. By [37] (alternatively, by Theorem 3.5), there is a secret-sharing scheme realizing the forbidden graph access structure of the bipartite graph $(A_{\text{big}}, B_{\text{big}}, E \cap (A_{\text{big}} \times B_{\text{big}}))$ in which the share size of each vertex is $O((n^{2/3+\beta/3})^{1/2}) = O(n^{1/3+\beta/6})$, and the total share size is $O((n^{2/3+\beta/3})^{3/2}) = O(n^{1+\beta/2})$.

Next, we share the secret for the edges between B_{small} and A. We partition the vertices in B_{small} according to their degree, that is, for $i = 0, \ldots, (1/3 - \beta/3)\log n - 1$, define

$$B_i = \left\{ b \in B_{\text{small}} : \frac{n^{1/3+2\beta/3}}{2^{i+1}} < \deg(b) \leq \frac{n^{1/3+2\beta/3}}{2^i} \right\}$$

and $B_{\text{last}} = \left\{b \in B_{\text{small}} : \deg(b) \leq n^{\beta}\right\}$. Additionally, let $G_i = (A, B_i, E \cap (A \times B_i))$ and $G_{\text{last}} = (A, B_{\text{last}}, E \cap (A \times B_{\text{last}}))$.

For $i = 0, \ldots, (1/3 - \beta/3)\log n - 1$, we realize the graph G_i using Lemma 4.1. Since the number of edges in G is at most $n^{1+\beta}$ and the degree of every vertex in B_i is at least $n^{1/3+2\beta/3}/2^{i+1}$, the number of vertices in B_i is at most $\frac{n^{1+\beta}}{n^{1/3+2\beta/3}/2^{i+1}} = 2^{i+1}n^{2/3+\beta/3}$. By taking all the remaining vertices with the

highest degree to B_i, we can assume that $|B_i| = 2^{i+1}n^{2/3+\beta/3}$. By Lemma 4.1, there is a secret-sharing scheme realizing the forbidden graph access structure of G_i, in which the share size of each vertex is

$$O\left(\left(\frac{n \cdot n^{1/3+2\beta/3}/2^i}{2^{i+1}n^{2/3+\beta/3}}\right)^{1/2} \log n\right) = O(n^{1/3+\beta/6} \log n),$$

and the total share size is

$$O\left(\left(n \cdot n^{1/3+2\beta/3}/2^i \cdot 2^{i+1}n^{2/3+\beta/3}\right)^{1/2} \log n\right) = O(n^{1+\beta/2} \log n).$$

Finally, we realize G_{last} using the secret-sharing scheme of Lemma 4.2, in which the share size of each vertex is $O(n^{\beta/2} \log n) = O(n^{1/3+\beta/6} \log n)$, and the total share size is $O(n^{1+\beta/2} \log n)$. Notice that $n^{\beta/2} < n^{1/3+\beta/6}$ because $\beta < 1$.

Since we use $1 + (1/3 - \beta/3) \log n$ schemes, the share size of each vertex in the resulting scheme is $O(n^{1/3+\beta/6} \log^2 n)$, and the total share size is $O(n^{1+\beta/2} \log^2 n)$.

Finally, we share the secret for the edges between A_{small} and B (it would suffice to consider the edges between A_{small} and B_{big}, however, this optimization does not reduce the share size). We do the same for A_{small}, i.e., we partition the vertices in A_{small} according to their degree, that is, for $i = 0, \ldots, (1-\beta) \log n - 1$, define

$$A_i = \left\{ a \in A_{\text{small}} : \frac{n^{1/3+2\beta/3}}{2^{i+1}} < \deg(a) \leq \frac{n^{1/3+2\beta/3}}{2^i} \right\}$$

and $A_{\text{last}} = \left\{a \in A_{\text{small}} : \deg(a) \leq n^\beta\right\}$, and the graphs $(A_i, B, E \cap (A_i \times B))$ and $(A_{\text{last}}, B, E \cap (A_{\text{last}} \times B))$. As before, we get a scheme in which the share size of each vertex is $O(n^{1/3+\beta/6} \log^2 n)$, and the total share size is $O(n^{1+\beta/2} \log^2 n)$.

Now suppose that $G = (A, B, E)$ is a bipartite graph with $|E| \geq n^2 - n^{1+\beta}$. Observe that the bipartite complement $\overline{G} = (A, B, \overline{E})$ has at most $n^{1+\beta}$ edges. Hence, in this case, the proof is analogous. □

Theorem 4.4. *Let $G = (V, E)$ be a graph with n vertices such that either $|E| \leq n^{1+\beta}$ or $|E| \geq \binom{n}{2} - n^{1+\beta}$, for some constant $0 \leq \beta < 1$. Then, there is a linear secret-sharing scheme realizing G in which the share size of each vertex is $O(n^{1/3+\beta/6} \log^3 n)$, and the total share size of this scheme is $O(n^{1+\beta/2} \log^3 n)$.*

Proof. To simplify notation, assume that n is a power of 2. As in [14], we cover G by $\log n$ bipartite graphs, each graph having at most $n^{1+\beta}$ edges or at least $\binom{n}{2} - n^{1+\beta}$ edges. We assume that $V = \{v_1, \ldots, v_n\}$, and for a vertex v_i we consider i as a binary $\log n$ string $i = (i_1, \ldots, i_{\log n})$. For every $1 \leq t \leq \log n$, we define the bipartite graph $H_t = (A_t, B_t, F_t)$ as the subgraph of G in which A_t is the set of vertices whose t-th bit is 0, B_t is the set of vertices whose t-th bit is 1, and $F_t = E \cap (A_t \times B_t)$, i.e., F_t is the set of edges in E between the vertices of A_t and B_t.

To share a secret s, for every $1 \leq t \leq \log n$, we share s independently using the secret-sharing scheme of Theorem 4.3 realizing the bipartite graph H_t with total share size $O(n^{1+\beta/2} \log^2 n)$. Since we use $\log n$ schemes, the total share size in the scheme realizing G is $O(n^{1+\beta/2} \log^3 n)$.

For an edge $(v_i, v_j) \in E$, where $i = (i_1, \ldots, i_{\log n})$ and $j = (j_1, \ldots, j_{\log n})$, there is at least one $1 \leq t \leq \log n$ such that $i_t \neq j_t$, thus, $(v_i, v_j) \in F_t$ and $\{v_i, v_j\}$ can reconstruct the secret using the shares of the scheme realizing H_t. If $(v_i, v_j) \notin E$, then $(v_i, v_j) \notin F_t$ for every $1 \leq t \leq \log n$, and, hence, $\{v_i, v_j\}$ have no information on the secret. □

5 Trade-offs Between the Max Share Size and the Total Share Size

In Section 4, we presented secret-sharing schemes with optimal total share size (up to polylogarithmic factors) and small max share size, however, the max share size is not optimal. Now, we present secret-sharing schemes achieving a trade-off between the total share size and the max share size. As a special case, we construct secret-sharing schemes realizing sparse graphs with at most $n^{1+\beta}$ edges and dense graphs with at least $\binom{n}{2} - n^{1+\beta}$ edges, for some constant $0 \leq \beta < 1$, in which the share size of every vertex is $O(n^{1/4+\beta/4} \log^2 n)$. By Corollary 6.10, the constructions with max share $O(n^{1/4+\beta/4} \log^2 n)$ are optimal (up to a small polylogarithmic factor).

Lemma 5.1. *Let $G = (A, B, E)$ be a bipartite graph with $|A| = |B| = n$ such that either $|E| \leq n^{1+\beta}$ or $|E| \geq n^2 - n^{1+\beta}$, for some constant $0 \leq \beta < 1$. Then, for every $0 \leq \gamma \leq 1/4 - \beta/4$, there is a linear secret-sharing scheme realizing G in which the share size of each vertex is $O(n^{1/4+\beta/4+\gamma} \log^2 n)$, and the total share size of this scheme is $O(n^{5/4+\beta/4-\gamma} \log^2 n)$.*

Proof. Suppose that $G = (A, B, E)$ is a bipartite graph with $|E| \leq n^{1+\beta}$. First, define $A_{\text{big}} = \left\{a \in A : \deg(a) \geq n^{1/2+\beta/2}\right\}$ and $B_{\text{big}} = \left\{b \in B : \deg(b) \geq n^{1/2+\beta/2}\right\}$. Since the number of edges in G is at most $n^{1+\beta}$ and the degree of every vertex in A_{big} and B_{big} is at least $n^{1/2+\beta/2}$, the number of vertices in A_{big} and the number of vertices in B_{big} is at most $\frac{n^{1+\beta}}{n^{1/2+\beta/2}} = n^{1/2+\beta/2}$. By [37], there is a secret-sharing scheme realizing the bipartite graph $(A_{\text{big}}, B_{\text{big}}, E \cap (A_{\text{big}} \times B_{\text{big}}))$ in which the share size of each vertex is

$$O((n^{1/2+\beta/2})^{1/2}) = O(n^{1/4+\beta/4}) = O(n^{1/4+\beta/4+\gamma}),$$

and the total share size is

$$O((n^{1/2+\beta/2})^{3/2}) = O(n^{3/4+3\beta/4}) = O(n^{5/4+\beta/4-\gamma}),$$

where the last equality follows from the fact that $5/4 + \beta/4 - \gamma - (3/4 + 3\beta/4) = 1/2 - \beta/2 - \gamma > 1/4 - \beta/4 > 0$, since $\gamma \leq 1/4 - \beta/4$ and $\beta < 1$.

Second, define $B_{\text{med}} = \left\{b \in B : n^{\beta+2\gamma} < \deg(b) \leq n^{1/2+\beta/2}\right\}$. Since the number of edges in G is at most $n^{1+\beta}$ and the degree of every vertex in B_{med} is at least $n^{\beta+2\gamma}$, the number of vertices in B_{med} is at most $\frac{n^{1+\beta}}{n^{\beta+2\gamma}} = n^{1-2\gamma}$. By taking all the remaining vertices with the higher degree to B_{med}, we can assume that $|B_{\text{med}}| = n^{1-2\gamma}$. By Lemma 4.1, there is a secret-sharing scheme realizing the forbidden graph access structure of $G_{\text{med}} = (A, B_{\text{med}}, E \cap (A \times B_{\text{med}}))$, in which the share size of each vertex is

$$O\left(\left(\frac{n \cdot n^{1/2+\beta/2}}{n^{1-2\gamma}}\right)^{1/2} \log n\right) = O(n^{1/4+\beta/4+\gamma} \log n),$$

and the total share size is

$$O\left(\left(n \cdot n^{1/2+\beta/2} \cdot n^{1-2\gamma}\right)^{1/2} \log n\right) = O(n^{5/4+\beta/4-\gamma} \log n).$$

Next, define $B_{\text{small}} = \left\{b \in B : \deg(b) \leq n^{\beta+2\gamma}\right\}$. We partition the vertices in B_{small} according to their degree, that is, for $i = 0, \ldots, 2\gamma \log n - 1$, define

$$B_i = \left\{b \in B_{\text{small}} : \frac{n^{\beta+2\gamma}}{2^{i+1}} < \deg(b) \leq \frac{n^{\beta+2\gamma}}{2^i}\right\}$$

and $B_{\text{last}} = \left\{b \in B_{\text{small}} : \deg(b) \leq n^{\beta}\right\}$. Additionally, let $G_i = (A, B_i, E \cap (A \times B_i))$ and $G_{\text{last}} = (A, B_{\text{last}}, E \cap (A \times B_{\text{last}}))$.

We realize each graph G_i, for $i = 0, \ldots, 2\gamma \log n - 1$, using Lemma 4.1. Since the number of edges in G is at most $n^{1+\beta}$ and the degree of every vertex in B_i is at least $n^{\beta+2\gamma}/2^{i+1}$, the number of vertices in B_i is at most $\frac{n^{1+\beta}}{n^{\beta+2\gamma}/2^{i+1}} = 2^{i+1}n^{1-2\gamma}$. By taking all the remaining vertices with the higher degree to B_i, we can assume that $|B_i| = 2^{i+1}n^{1-2\gamma}$. By Lemma 4.1, there is a secret-sharing scheme realizing the forbidden graph access structure of G_i, in which the share size of each vertex is

$$O\left(\left(\frac{n \cdot n^{\beta+2\gamma}/2^i}{2^{i+1}n^{1-2\gamma}}\right)^{1/2} \log n\right) = O(n^{\beta/2+2\gamma} \log n) = O(n^{1/4+\beta/4+\gamma} \log n),$$

and the total share size is

$$O\left(\left(n\frac{n^{\beta+2\gamma}}{2^i}2^{i+1}n^{1-2\gamma}\right)^{1/2} \log n\right) = O(n^{1+\beta/2} \log n) = O(n^{5/4+\beta/4-\gamma} \log n).$$

In the computation of these upper bounds, we use the fact that $1/4+\beta/4+\gamma-(\beta/2+2\gamma) = 1/4-\beta/4-\gamma > 0$ and that $5/4 + \beta/4 - \gamma - (1 + \beta/2) = 1/4 - \beta/4 - \gamma > 0$.

Finally, we realize G_{last} using the secret-sharing scheme of Lemma 4.2, in which the share size of each vertex is $O(n^{\beta/2} \log n) = O(n^{1/4+\beta/4+\gamma} \log n)$, and the total share size is $O(n^{1+\beta/2} \log n) = O(n^{5/4+\beta/4-\gamma} \log n)$. Since we use $1 + 2\gamma \log n$ schemes, the share size of each vertex in the resulting scheme is $O(n^{1/4+\beta/4+\gamma} \log^2 n)$, and the total share size is $O(n^{5/4+\beta/4-\gamma} \log^2 n)$.

We do the same for A, and as before, we get a scheme in which the share size of each vertex is $O(n^{1/4+\beta/4+\gamma} \log^2 n)$, and the total share size is $O(n^{5/4+\beta/4-\gamma} \log^2 n)$. □

The proof of the following theorem is similar to the proof of Theorem 4.4, except that we use the secret-sharing scheme of Lemma 5.1 to realize each of the $\log n$ bipartite graphs, instead of the secret-sharing scheme of Theorem 4.3.

Theorem 5.2. *Let $G = (V, E)$ be a graph with n vertices such that either $|E| \leq n^{1+\beta}$ or $|E| \geq \binom{n}{2} - n^{1+\beta}$, for some constant $0 \leq \beta < 1$. Then, for every $0 \leq \gamma \leq 1/4 - \beta/4$, there is a linear secret-sharing scheme realizing G in which the share size of each vertex is $O(n^{1/4+\beta/4+\gamma} \log^3 n)$, and the total share size of this scheme is $O(n^{5/4+\beta/4-\gamma} \log^3 n)$.*

By taking the above construction with $\gamma = 0$, we obtain the following secret-sharing schemes for sparse and dense graphs, in which the max share size is optimal (up to a small polylogarithmic factor).

Corollary 5.3. *Let $G = (V, E)$ be a graph with n vertices such that either $|E| \leq n^{1+\beta}$ or $|E| \geq \binom{n}{2} - n^{1+\beta}$, for some constant $0 \leq \beta < 1$. Then, there is a linear secret-sharing scheme realizing G in which the share size of each vertex is $O(n^{1/4+\beta/4} \log^3 n)$.*

Remark 5.4. We can reduce the share size of the secret-sharing schemes of Corollary 5.3 by a factor of $\log n$ using a simpler constructions, in which A_{big} and B_{big} are defined as in Lemma 5.1, and let $A_{\text{small}} = A \setminus A_{\text{big}}$ and $B_{\text{small}} = B \setminus B_{\text{big}}$. We realize the bipartite graph with parts A_{big} and B_{big} as in Lemma 5.1 using Theorem 3.5, and realize the bipartite graphs with parts A and B_{small} and with parts B and A_{small}, which have bounded degree for one part, using Lemma 4.2.

5.1 Adding or Removing Few Edges from Forbidden Graph Access Structures

In the last construction in this paper, we analyze the size of the shares of secret-sharing schemes realizing graphs that differ in few edges.

Corollary 5.5. *Let $G = (V, E)$ be a graph with n vertices that can be realized by a secret-sharing scheme in which the max share size is ℓ, and the total share size is m, and let G' be a graph obtained from G by adding and removing at most $n^{1+\beta}$ edges, for some constant $0 \leq \beta < 1$. Then, there exist secret-sharing schemes realizing G' with the following properties:*

- *a scheme with total share size $m + O(n^{1+\beta/2} \log^3 n)$ and max share size $\ell + O(n^{1/3+\beta/6} \log^3 n)$, and*
- *a scheme with max share size $\ell + O(n^{1/4+\beta/4} \log^3 n)$.*

If the scheme that realizes G is linear, then these schemes are also linear.

Proof. First, we prove the existence of the first scheme. Let s be the secret, $E' \subset E$ be the set of edges removed from G, and E'' (where $E'' \cap E = \emptyset$) be the set of edges added to G. Note that $G' = (V, (E \setminus E') \cup E'') = (V, (E \cap \overline{E'}) \cup E'')$ and $|E'|, |E''| \leq n^{1+\beta}$. Since $|\overline{E'}| \geq \binom{n}{2} - n^{1+\beta}$, by Theorem 4.4 the graph $(V, \overline{E'})$ can be realized by a scheme with total share size $O(n^{1+\beta/2} \log^3 n)$ and max share size $O(n^{1/3+\beta/6} \log^3 n)$. Thus, by Claim 2.8, we can realize the graph $(V, E \cap \overline{E'})$ by a secret-sharing scheme in which the total share size is $m + O(n^{1+\beta/2} \log^3 n)$ and the max share size is $\ell + O(n^{1/3+\beta/6} \log^3 n)$.

By Theorem 4.4, the graph (V, E'') can be realized a secret-sharing scheme with total share size $O(n^{1+\beta/2} \log^3 n)$ and max share size $O(n^{1/3+\beta/6} \log^3 n)$. Thus, again by Claim 2.8, we can realize the graph $G' = (V, (E \cap \overline{E'}) \cup E'')$ by a secret-sharing scheme in which the total share size is $m + O(n^{1+\beta/2} \log^3 n)$ and the max share size is $\ell + O(n^{1/3+\beta/6} \log^3 n)$.

The existence of the second scheme is a consequence of Corollary 5.3. □

6 Lower Bounds for Linear Secret-Sharing Schemes

In this section, we prove that for almost all forbidden graph access structures with n parties, the total share size required by any linear secret-sharing scheme realizing these access structures, with a one-bit secret, is $\Omega(n^{3/2})$. We then use this result to prove that for almost all forbidden graph access structures with n parties and at most $n^{1+\beta}$ edges, the total share size required by any linear secret-sharing scheme realizing these access structures, with a one-bit secret, is $\Omega(n^{1+\beta/2})$. As we have shown in this paper, this bound is tight up to a poly-logarithmic factor. Furthermore, we bound the share size of families of access structures whose size of minimal authorized sets is small. Since linear secret-sharing schemes are equivalent to monotone span programs (see Claim 2.4), we prove the lower bounds using MSP terminology.

The section is organized as follows: We start with some definitions, then in Section 6.1 we discuss dual access structures and the dual of MSPs. In Section 6.2, we prove lower bounds for MSPs in which each party labels a bounded number of rows; this implies lower bounds for the max share size in linear secret-sharing schemes. In Section 6.3, we prove a stronger result – the same lower bounds hold for the size of MSPs; this implies lower bounds for the total share size in linear secret-sharing schemes (this result uses the results of Section 6.2).

Definition 6.1. *Let $\widehat{M} = \langle \mathbb{F}, M, \delta, \mathbf{1} \rangle$ be an MSP accepting an access structure Γ. Define $\rho_i(\widehat{M})$ as the number of rows labeled by i, and define $\rho(\widehat{M})$ as the maximal number of rows labeled by a single label:*

$\rho(\widehat{M}) \stackrel{def}{=} \max_{i \in P} \rho_i(\widehat{M})$. *Define* $\rho_q(\Gamma)$ *as the minimum* $\rho(\widehat{M})$ *over all MSPs accepting the access structure* Γ *over* $\mathbb{F}_q$.

Define $\mathrm{size}(\widehat{M})$ *as the number of rows in the matrix* M *and* $\mathrm{size}_q(\Gamma)$ *as the minimum* $\mathrm{size}(\widehat{M})$ *over all MSPs accepting the access structure* Γ *over* $\mathbb{F}_q$.

Notice that $\rho_q(\Gamma)$ is the minimal max share size of all linear secret-sharing schemes accepting Γ over $\mathbb{F}_q$, and $\mathrm{size}_q(\Gamma)$ is the minimal total share size of all linear secret-sharing schemes accepting Γ over $\mathbb{F}_q$.

Definition 6.2. *We say that an access structure* Γ *has rank* r *if the size of every minimal authorized set in* Γ *is at most* r.

By counting arguments it is possible to prove lower bounds on the monotone span program size for almost all access structures: Assume that every access structure can be accepted by an MSP of size S. The number of MSPs with n parties over $\mathbb{F}_q$ whose size is at most S is at most $n^S q^{S^2}$ (as proved in Proposition 6.6 below, we can consider MSPs in which the number of columns in the matrix of the MSP is at most S, thus, there are q^{S^2} possible matrices and n^S possible ways to label the rows, where n is the number of parties). Since the number of monotone access structures is at least $2^{2^n/\sqrt{n}}$ and every MSP accepts one monotone access structure, it must be that $n^S q^{S^2} \geq 2^{2^n/\sqrt{n}}$, i.e., $S \log n + S^2 \log q \geq 2^n/\sqrt{n}$, which implies that $S \log q > S\sqrt{\log q} = \Omega(2^{n/2}/n^{1/4})$ (where $S \log q$ is the non-normalized total share size of the scheme).

It is not clear how to use direct counting arguments to prove lower bounds on the size of MSPs accepting forbidden graph access structures: the number of graphs is $2^{O(n^2)}$, thus, we get that $n^S q^{S^2} \geq 2^{O(n^2)}$, which only implies the trivial lower bound $S \log q > S\sqrt{\log q} = \Omega(n)$.

6.1 Dual of Monotone Span Programs

We use the notion of *dual access structures* and *dual MSPs*, since their properties enable us to use a counting argument that will yield tight lower bounds on the size of MSPs accepting forbidden graph access structures. Such duals were studied in previous papers, e.g., [41, 36, 33, 35].

Definition 6.3 (Dual Access Structure)**.** *Given an access structure* $\Gamma \subseteq 2^P$*, its* dual access structure $\Gamma^\perp$ *is defined as*

$$\Gamma^\perp \stackrel{def}{=} \{B \subseteq P : P \setminus B \notin \Gamma\}.$$

For example, for the t-out-of-n access structure $\Gamma_t = \{B \subseteq P : |B| \geq t\}$ (where $|P| = n$),

$$\Gamma_t^\perp = \left\{B \subseteq P : \left|P \setminus B\right| < t\right\} = \{B \subseteq P : |B| > n - t\} = \Gamma_{n-t+1}.$$

Given an MSP, we can define its *dual MSP*. For this construction, recall that given an MSP $\langle \mathbb{F}, M, \delta, \mathbf{1} \rangle$ accepting Γ, for every authorized set $A \in \Gamma$ there exists a reconstruction vector $\mathbf{r_A}$ such that $\mathbf{r_A} M = \mathbf{1}$, and $(\mathbf{r_A})^T$ is non-zero only in rows labeled by A.

Construction 6.4 (Dual MSP)**.** Given an MSP $\widehat{M} = \langle \mathbb{F}, M, \delta, \mathbf{1} \rangle$ accepting Γ over $\mathbb{F}$, construct an MSP $\widehat{M^\perp} = \langle \mathbb{F}, M^\perp, \delta, \mathbf{1} \rangle$ in which for every minimal authorized set $A \in \min \Gamma$ there exists a column $(\mathbf{r_A})^T$ in $M^\perp$, where $\mathbf{r_A}$ is a reconstruction vector for A in M. The MSP $\widehat{M^\perp} = \langle \mathbb{F}, M^\perp, \delta, \mathbf{1} \rangle$ is called the *dual MSP*.

The following claim can be found in [36]. For completeness, we include its proof.

Claim 6.5. *Let $\widehat{M} = \langle \mathbb{F}, M, \delta, \mathbf{1} \rangle$ be an MSP accepting an access structure $\Gamma \subseteq 2^P$. The dual MSP $\widehat{M^\perp} = \langle \mathbb{F}, M^\perp, \delta, \mathbf{1} \rangle$, as defined in Construction 6.4, is an MSP accepting the dual access structure $\Gamma^\perp$. The sizes of $\widehat{M} = \langle \mathbb{F}, M, \delta, \mathbf{1} \rangle$ and $\widehat{M^\perp} = \langle \mathbb{F}, M^\perp, \delta, \mathbf{1} \rangle$ are the same.*

Proof. We begin by proving that for every authorized set $A \in \Gamma$, the set $B = P \setminus A$ is rejected by $\widehat{M^\perp}$. It suffices to consider only minimal authorized sets $A \in \min \Gamma$. The reconstruction vector $\mathbf{r_A}$ of A is a column of $M^\perp$, and has non-zero entries only in rows labeled by A. The rows labeled by $B = P \setminus A$ cannot span $\mathbf{1}$, since in the column $(\mathbf{r_A})^T$ all entries labeled by B are zero.

Now, assume that $A \notin \Gamma$. In this case, the rows of M labeled by elements from A do not linearly span $\mathbf{1}$. By orthogonality arguments, there is a column vector $\mathbf{v}$ such that $\mathbf{1} \cdot \mathbf{v} = 1$ and $M_A \mathbf{v} = \mathbf{0}$, where M_A are the rows of M labeled by elements from A. Denote $\mathbf{w} = (M\mathbf{v})^T$. We prove that $\mathbf{w} M^\perp = \mathbf{1}$, i.e., $\mathbf{w}$ is a reconstruction vector of $B = P \setminus A$ in $\widehat{M^\perp}$. For every column $\mathbf{r_C}$ of $M^\perp$ the following is true:

$$\mathbf{w} \cdot (\mathbf{r_C})^T = (M\mathbf{v})^T \cdot (\mathbf{r_C})^T = \mathbf{v}^T M^T (\mathbf{r_C})^T = \mathbf{v}^T (\mathbf{r_C} M)^T = \mathbf{v}^T \cdot \mathbf{1}^T = 1.$$

This implies that $\mathbf{w} \cdot M^\perp = \mathbf{1}$. Furthermore, the vector $\mathbf{w}^T$ is non-zero only in rows labeled by $B = P \setminus A$ (since $M_A \mathbf{v} = 0$). Thus, the set B has a reconstruction vector for the MSP $\widehat{M^\perp}$, and, therefore, is accepted by $\widehat{M^\perp}$.

Since the MSP and its dual MSP have the same labeling, the size of the MSP and the dual MSP are the same. □

Claim 6.5 implies that lower bounds on the size of the dual MSPs over $\mathbb{F}$ for forbidden graph access structures yield lower bounds on the total share size of linear secret-sharing schemes over $\mathbb{F}$ for forbidden graph access structures. The following simple proposition bounds the number of columns of an MSP.

Proposition 6.6. *For every non-empty access structure Γ and every prime-power q, there is an MSP $\widehat{M} = \langle \mathbb{F}_q, M, \delta, \mathbf{1} \rangle$ accepting Γ such that $\mathrm{size}(\widehat{M}) = \mathrm{size}_q(\Gamma)$ and the number of columns in M is at most $\mathrm{size}(\widehat{M})$.*

Proof. Let $\widehat{M'} = \langle \mathbb{F}_q, M', \delta, \mathbf{1} \rangle$ be an MSP accepting Γ such that $\mathrm{size}(\widehat{M'}) = \mathrm{size}_q(\Gamma)$. We remove all dependent columns from the MSP $\widehat{M'}$; this does not change the sets accepted by the MSP. We obtain an MSP $\widehat{M} = \langle \mathbb{F}_q, M, \delta, \mathbf{1} \rangle$ accepting Γ such that all columns of M are linearly independent. Since column rank equals row rank, the number of columns in M is at most the number of rows in M, which is the number of rows in M'.[4] □

Given an access structure Γ of rank r and an MSP $\widehat{M} = \langle \mathbb{F}, M, \delta, \mathbf{1} \rangle$ accepting Γ, we consider its dual $\widehat{M^\perp} = \langle \mathbb{F}, M^\perp, \delta, \mathbf{1} \rangle$, which accepts $\Gamma^\perp$. We can assume that $M^\perp$ has at most S independent columns that form a basis spanning all reconstruction vectors $\{\mathbf{r_A}\}_{A \in \min \Gamma}$ (where S is the size of the MSPs $\widehat{M}$ and $\widehat{M^\perp}$). In particular, for every column in $M^\perp$ there is a set of parties A of size at most r such that the non-zero elements in the column are only in rows labeled by A.

[4] Notice that the rows are not necessarily linearly independent (since rows labeled by different parties can be dependent). Therefore, the number of columns can actually be smaller than the number of rows.

6.2 Lower Bounds on the Max Share Size

Next, we compute the number of access structures of rank r that have an MSP such that each party labels at most s rows, and we show in Theorem 6.7 that there are at most $2^{O(rns^2 \log q)}$ such access structures. Using this result, we show in Corollary 6.9 that for almost all forbidden graph access structures, the max share size for sharing a one-bit secret in a linear secret-sharing scheme is $\Omega(\sqrt{n})$. As a corollary, we obtain in Corollary 6.13 a lower bound on the communication complexity of CDS protocols. Additionally, in Corollary 6.10 we show lower bounds on the max share size in sharing a one-bit secret by linear secret-sharing schemes for forbidden graph access structures of sparse and dense graphs.

Theorem 6.7. *Let q be a prime power and s, r, n be integers such that $s > \log n$. The number of access structures Γ with n parties, rank r, and $\rho_q(\Gamma) \leq s$ is at most $2^{2rns^2 \log q}$.*

Proof. If $\rho_q(\Gamma) \leq s$, then, as explained above, there is an MSP $\widehat{M^\perp} = \langle \mathbb{F}, M^\perp, \delta, \mathbf{1} \rangle$ accepting $\Gamma^\perp$ of the following form:

- $M^\perp$ is an $ns \times ns$ matrix (this can be achieved without changing the validity of the MSP by adding zero rows or duplicating columns).
- δ is fixed and $\delta(i) = \lceil \frac{i}{s} \rceil$, i.e., the first s rows are labeled by the first party, the next s rows are labeled by the second party, and so on.
- Every column of $M^\perp$ is a reconstruction vector of some minimal authorized set $A \in \min \Gamma$ (by Claim 6.5).

Every dual of a rank r access structure has an MSP of this form, and the number of these MSPs is bounded by the number of possible matrices. Every matrix has ns columns, each is a reconstruction vector of some $A \in \min \Gamma$. By the definition of reconstruction vectors, the columns can have non-zero values only in entries labeled by some $i \in A$, that is, at most rs entries can be non-zero. Therefore, the number of possible column vectors for a given minimal authorized set $A \in \min \Gamma$ is at most $|\mathbb{F}_q|^{rs} = q^{rs}$. Since we allow the entries in rows labeled by A to be zero, we can assume that the size of A is exactly r. The number of sets of size r that can label a column is $\binom{n}{r} < n^r < 2^{rs}$ (since $s > \log n$). Thus, since the number of columns is ns, the number of such matrices is at most

$$(2^{rs} q^{rs})^{ns} < 2^{2rns^2 \log q}. \qquad \square$$

Theorem 6.8. *Let L be a family of access structures with rank at most r. Then, for almost all access structures in L, the max share size for sharing a one-bit secret in a linear secret-sharing scheme is $\Omega(\sqrt{\log |L| / rn})$.*

Proof. Let $\ell = \log |L|$. If we share a one-bit secret using an MSP $\widehat{M}$ over $\mathbb{F}_q$ with $\rho(\widehat{M}) = s$, then the size of the share of at least one party is $s \log q$. For the max share size to be less than $\sqrt{\ell / rn}$, it must be that $s \log q \leq \sqrt{\ell / rn}$, and, in particular, $q \leq 2^{\sqrt{\ell / rn}}$.

We next bound the number of access structures in L that can be realized by a secret-sharing scheme with max share size at most θ. By Theorem 6.7, the number of access structures in L, each one of them has rank at most r, with n parties and $\rho_q(\Gamma) \leq \theta / \log q$, is at most $2^{2rn(\theta / \log q)^2 \log q} < 2^{2rn\theta^2}$. Since we are counting linear schemes, we need to sum the number of the MSPs for every possible finite field (there are

at most $2^{\sqrt{\ell/rn}}$ such fields, because $q \leq 2^{\sqrt{\ell/rn}}$). Consider the MSPs for which the max share size in the secret-sharing schemes defined by the MSPs is at most $\theta < \sqrt{\ell/rn}$. The number of such MSPs is at most

$$2^{\sqrt{\ell/rn}} \cdot 2^{2rn\theta^2} < 2^{\sqrt{\ell}+2rn\theta^2}.$$

Thus, if almost all access structures in L have a linear secret-sharing scheme with max share size θ, then

$$2^{\sqrt{\ell}+2rn\theta^2} > (1-o(1))2^{\ell},$$

i.e., $\theta^2 > (\ell - \sqrt{\ell})/2rn$, so $\theta = \Omega(\sqrt{\ell/rn})$. □

Corollary 6.9. *For almost all forbidden graph access structures, the max share size for sharing a one-bit secret in a linear secret-sharing scheme is* $\Omega(\sqrt{n})$.

Proof. Let L be the family of forbidden graph access structures. Then, the rank of each access structure in L at most $r = 3$, and the number of forbidden graph access structures over a set of n parties is the number of graphs with n vertices, which is $|L| = 2^{\ell}$, where $\ell = \binom{n}{2} \approx n^2/2$. Thus, by Theorem 6.8, we get that for almost all forbidden graph access structures, the max share size for sharing a one-bit secret in a linear secret-sharing scheme is $\Omega(\sqrt{\ell/rn}) = \Omega(\sqrt{n})$. □

The same lower bound holds for graph access structures. Furthermore, if we take sparse forbidden graphs with at most $n^{1+\beta}$ edges for some constant $0 \leq \beta < 1$, then the number of such graphs is at least

$$\binom{n^2/2}{n^{1+\beta}} \geq \left(\frac{n^2/2}{n^{1+\beta}}\right)^{n^{1+\beta}} = 2^{\Omega(n^{1+\beta}\log n)}.$$

Thus, the max share size of almost all sparse and dense forbidden graph access is $\Omega(\sqrt{n^{1+\beta}\log n/n}) = \Omega(n^{\beta/2}\sqrt{\log n})$. We next prove that there exist a sparse and a dense forbidden graph access structures whose total share size is $\Omega(n^{1/4+\beta/4})$.

Corollary 6.10. *Let* $0 \leq \beta < 1$ *be a constant. There exists a forbidden graph access structure with at most* $n^{1+\beta}$ *edges such that the max share size for sharing a one-bit secret in a linear secret-sharing scheme is* $\Omega(n^{1/4+\beta/4})$. *Furthermore, there exists a forbidden graph access structure with at least* $\binom{n}{2} - n^{1+\beta}$ *edges such that the max share size for sharing a one-bit secret in a linear secret-sharing scheme is* $\Omega(n^{1/4+\beta/4})$.

Proof. By Corollary 6.9, for every n there exists a graph G_n with n vertices such that the max share size in any linear secret-sharing scheme realizing its forbidden graph access structure is $\Omega(\sqrt{n})$. We use this graph (with fewer vertices) to construct a sparse graph $G = (V, E)$ with n vertices. We fix an arbitrary set of vertices $V' \subset V$ of size $n' = n^{1/2+\beta/2}$, and consider the graph $G_{n'} = (V', E')$ with the set of vertices V'. Let $G = (V, E')$, that is, the vertices in V' are connected according to E' and the vertices in $V \setminus V'$ are isolated.

Since all edges in G are between vertices in V', the number of edges is at most $\binom{n^{1/2+\beta/2}}{2} < n^{1+\beta}$. By Corollary 6.9, the max share size of any linear secret-sharing scheme realizing G is $\Omega(\sqrt{n'}) = \Omega((n^{1/2+\beta/2})^{1/2}) = \Omega(n^{1/4+\beta/4})$. Thus, the max share size of any linear secret-sharing scheme realizing G is $\Omega(n^{1/4+\beta/4})$.

To construct a dense graph with at least $\binom{n}{2} - n^{1+\beta}$ edges that requires large max share size in every linear scheme realizing its forbidden graph access structure, we use a similar construction, however, we add all edges incident to vertices in $V \setminus V'$. Similar analysis implies that the resulting graph has at least $\binom{n}{2} - n^{1+\beta}$ edges and the max share size of any linear secret-sharing scheme realizing the graph is $\Omega(n^{1/4+\beta/4})$. □

Implications to uniform access structures and CDS protocols. Using the above result we can prove a lower bound of $\Omega(k^{-3/4}n^{-1/2}2^{(h(k/n)/2)n})$ on the max share size for sharing a one-bit secret in every linear secret-sharing scheme that realizes k-uniform access structures. In k-uniform access structures, which are a generalization of forbidden graph access structures, all subsets of size more than k are authorized, all subsets of size less than k are unauthorized, and subsets of size exactly k can be either authorized or unauthorized. By the linear construction of [4] for k-uniform access structures with max share size $O(n2^{(h(k/n)/2)n})$, this bound is tight (up to a small polynomial factor).

Theorem 6.11. *For almost all k-uniform access structures, the max share size for sharing a one-bit secret in a linear secret-sharing scheme is $\Omega(k^{-3/4}n^{-1/2}2^{(h(k/n)/2)n})$.*

Proof. Let L be the family of k-uniform access structures. Then, the rank of each access structure in L at most $r = k + 1$, and the number of k-uniform access structures is $|L| = 2^{\ell}$, where $\ell = \binom{n}{k} = \Theta(k^{-1/2}2^{h(k/n)n})$. Thus, by Theorem 6.8, for almost all k-uniform access structures, the max share size for sharing a one-bit secret in a linear secret-sharing scheme is $\Omega(\sqrt{\ell/rn}) = \Omega(k^{-3/4}n^{-1/2}2^{(h(k/n)/2)n})$. □

Moreover, using the above result we can prove lower bounds on the max share size for sharing a one-bit secret in every linear secret-sharing scheme realizing k-partite k-uniform access structures. A k-uniform access structure is k-partite if the parties can be partitioned into k sets, such that every authorized set of size k contains exactly one party from each set of the partition.

Theorem 6.12. *For almost all k-partite k-uniform access structures, where the size of each part is N, the max share size for sharing a one-bit secret in a linear secret-sharing scheme is $\Omega(k^{-1}N^{(k-1)/2})$.*

Proof. Let L be the family of k-partite k-uniform access structures, where the size of each part is N. Then, the rank of each access structure in L at most $r = k+1$, the number of parties is $n = kN$, and the number of k-partite k-uniform access structures, where the size of each part is N, is $|L| = 2^{N^k}$. Thus, by Theorem 6.8, for almost all k-partite k-uniform access structures, the max share size for sharing a one-bit secret in a linear secret-sharing scheme is $\Omega(\sqrt{\log |L|/rn}) = \Omega(k^{-1}N^{(k-1)/2})$. □

Since CDS protocols are equivalent to secret-sharing schemes for multi-partite uniform access structures, we get the following corollary. By the linear construction of [15, 45] of k-server CDS protocol with message size $O(N^{(k-1)/2})$, this bound is tight (up to a factor of k).

Corollary 6.13. *For almost all k-input functions $f : [N]^k \to \{0,1\}$, the message size of every linear k-server CDS protocol for f with one-bit secret is $\Omega(k^{-1}N^{(k-1)/2})$.*

6.3 Lower Bounds on the Total Share Size

In this section we present lower bounds on the total share size for forbidden graph access structures and rank r access structures. In Theorem 6.14, we count the number of forbidden graph access structures with MSPs of size at most S. Using this result, we show in Corollary 6.15 that for almost all forbidden graph access structures, the total share size for sharing a one-bit secret in a linear secret-sharing scheme is $\Omega(n^{3/2})$. This result is stronger than Corollary 6.9. Then, we present in Corollary 6.16 lower bounds on the total share size for forbidden graph access structures of dense and sparse graphs. Finally, in Corollary 6.18 we count the number rank r access structures with MSPs of size at most S and prove that for almost all rank r access structures with n parties, the total size of the shares in every linear secret-sharing scheme with a one-bit secret realizing these access structures is $\Omega(n^{(r+1)/2})$.

Theorem 6.14. *Let q be a prime power and S, n be integers such that $S > n \log n$. The number of forbidden graph access structures Γ with n parties and $\mathrm{size}_q(\Gamma) \leq S$ is at most $2^{n^2/3+(72S^2 \log q)/n}$.*

Proof. Let $\widehat{M} = \langle \mathbb{F}, M, \delta, \mathbf{1} \rangle$ be a monotone span program accepting a forbidden graph access structure Γ of a graph $G = (V, E)$ with n parties $V = \{v_1, \ldots, v_n\}$ such that $\mathrm{size}(\widehat{M}) \leq S$. Let $B \subseteq V$ be the set of parties such that each one of the parties in B labels more than $4S/n$ rows in $\widehat{M}$. The size of B must be at most $n/4$. Let $\widehat{M'} = \langle \mathbb{F}, M', \delta', \mathbf{1} \rangle$ be the monotone span program obtained from $\widehat{M}$ by removing the rows of M labeled by parties in B. Notice that $\rho(\widehat{M'}) \leq 4S/n$. Furthermore, $\widehat{M'}$ accepts the forbidden graph access structure Γ' obtained from Γ by removing all the authorized sets containing parties from B. That is, Γ' is the forbidden graph access structure of the graph G' obtained by removing B from G, i.e., $G' = (V \setminus B, E \cap (V \setminus B) \times (V \setminus B))$.

We say that a forbidden graph access structure Γ is efficient if $\mathrm{size}_q(\Gamma) \leq S$. For every efficient forbidden graph access structure Γ of a graph G with n parties, arbitrarily choose an MSP $\widehat{M_G}$ accepting it whose size is exactly S,[5] choose a set B_G of size exactly $n/4$ such that each party in $V \setminus B_G$ labels at most $4S/n$ rows in $\widehat{M_G}$, and let H_G be the graph obtained by removing B_G from G. As explained above, if Γ is efficient then $\rho(\widehat{M'}) \leq 4S/n$.

Fix a set $B \subset V$ of size $n/4$ and a graph $H = (V_H, E_H)$ such that $V_H \subset \{v_1, \ldots, v_n\}$ and $|V_H| = 3n/4$. We next give an upper-bound on the number of efficient forbidden graph access structures Γ such that $B_G = B$ and $H_G = H$. The number of graphs $G = (V, E)$ such that H is obtained by removing B from G is at most

$$2^{\binom{n/4}{2}} \cdot 2^{\frac{n}{4} \cdot \frac{3n}{4}} \leq 2^{n^2/4},$$

where the first term corresponds to possible edges between vertices in B and the second term corresponds to possible edges between a vertex in B and a vertex in $V \setminus B$.

To conclude, the number of efficient forbidden graph access structures over $\mathbb{F}_q$ is at most

$$\binom{n}{n/4} \cdot 2^{n^2/4} \cdot 2^{6(3n/4)(4S/n)^2 \log q} \leq 2^{n^2/3+72(S^2/n) \log q},$$

where the first term is the number of possible choices of B, the second term is an upper bound on the number of graphs such that the graph obtained by removing B from these graph is the same, and the third term is an upper bound on the number of forbidden graph access structures Γ' whose set of parties is $V \setminus B$ and $\rho_q(\Gamma') \leq 4S/n$. □

Corollary 6.15. *For almost all forbidden graph access structures, the total share size for sharing a one-bit secret in a linear secret-sharing scheme is $\Omega(n^{3/2})$.*

Proof. If we share a one-bit secret using an MSP $\widehat{M}$ over $\mathbb{F}_q$ with $\mathrm{size}_q(\widehat{M}) = S$, then the total share size is $S \log q$. For the total share size to be less than $n^{3/2}$, it must be that $q \leq 2^{\sqrt{n}}$ (otherwise, each share contains more than $\sqrt{n}$ bits, and, in total, the share size is more than $n^{3/2}$), and, furthermore, $S \log q \leq n^{3/2}$.

On one hand, by Theorem 6.14, the number of forbidden graph access structures Γ with n parties and $\mathrm{size}_q(\Gamma) \leq \Theta/\log q$ is at most

$$2^{n^2/3+(72(\Theta/\log q)^2 \log q)/n} < 2^{n^2/3+72\Theta^2/n}.$$

[5] By adding all-zero rows we can assume that the size is exactly S.

Since we are counting linear schemes, we need to sum the number of the MSPs for every possible finite field (there are at most $2^{\sqrt{n}}$ such fields, because $q \leq 2^{\sqrt{n}}$). Consider the MSPs for which the total share size in the secret-sharing schemes defined by the MSPs is at most $\Theta < n^{3/2}$. The number of such MSPs is at most

$$2^{\sqrt{n}} \cdot 2^{n^2/3+72\Theta^2/n}.$$

On the other hand, the number of graphs is $2^{\binom{n}{2}} \approx 2^{n^2/2}$. Thus, if almost all the forbidden graph access structures have a linear secret-sharing scheme with total share size Θ, then $\sqrt{n}+n^2/3+72\Theta^2/n > n^2/2-1$, i.e., $\Theta = \Omega(n^{3/2})$. □

We cannot apply Theorem 6.14 directly to prove lower bounds on the total share size of linear schemes for sparse or dense forbidden graph access structures, since the term of $2^{n^2/3}$ in Theorem 6.14 dominates the number of sparse graphs. To prove lower bounds for sparse forbidden graph access structures, we use an idea from [10].

Corollary 6.16. *Let $0 \leq \beta < 1$ be a constant. There exists a forbidden graph access structure with at most $n^{1+\beta}$ edges such that the total share size for sharing a one-bit secret in a linear secret-sharing scheme is $\Omega(n^{1+\beta/2})$. Furthermore, there exists a forbidden graph access structure with at least $\binom{n}{2} - n^{1+\beta}$ edges such that the total share size for sharing a one-bit secret in a linear secret-sharing scheme is $\Omega(n^{1+\beta/2})$.*

Proof. By Corollary 6.15, for every n there exists a graph with n vertices such that the total share size in any linear secret-sharing scheme realizing its forbidden graph access structure is $\Omega(n^{3/2})$. We use such a graph (with fewer vertices) to construct a sparse graph $G = (V, E)$ with n vertices. We partition the vertices of G into $n^{1-\beta}$ disjoint sets of vertices $V_1, \ldots, V_{n^{1-\beta}}$, where $|V_i| = n^\beta$ for $1 \leq i \leq n^{1-\beta}$. We construct the edges as follows: For every i (where $1 \leq i \leq n^{1-\beta}$), we construct a copy of a graph from Corollary 6.15 with n^β vertices among the vertices of V_i. We denote this graph by G_i. There are no edges between vertices in different sets.

Since all edges in the above construction are between vertices in the same set, the number of edges is at most $\binom{n^\beta}{2} n^{1-\beta} < n^{1+\beta}$. The total share size of any linear secret-sharing scheme realizing G_i (for $1 \leq i \leq n^{1-\beta}$) is $\Omega((n^\beta)^{3/2}) = \Omega(n^{3\beta/2})$. Thus, the total share size of any linear secret-sharing scheme realizing G is $\Omega(n^{1-\beta} n^{3\beta/2}) = \Omega(n^{1+\beta/2})$.

To construct a dense graph with at least $\binom{n}{2} - n^{1+\beta}$ edges that requires large shares in every linear scheme realizing its forbidden graph access structure, we use a similar construction, however, we add all edges between different sets. Similar analysis implies that the resulting graph has at least $\binom{n}{2} - n^{1+\beta}$ edges and the total share size of any linear secret-sharing scheme realizing the graph is $\Omega(n^{1+\beta/2})$. □

Theorem 6.17. *Let q be a prime power and S, n, r be integers such that $S > n \log n$. The number of rank r access structures with n parties and $\text{size}_q(\Gamma) \leq S$ is at most*

$$\exp\left(O\left((1-(3/4)^r)\binom{n}{r} + \frac{rS^2 \log q}{n}\right)\right).$$

Proof. The proof is similar to the proof of Theorem 6.14 as we next explain. Given an MSP of size S, we find a set B of size $n/4$ containing all parties such that each party not in B labels at most $4S/n$ rows. Let Γ' be an access structure over $3n/4$ parties such that each one of them label at most $4S/n$ rows. To complete the proof, we need to upper bound the number of rank r access structures with n parties whose restriction

to $3n/4$ parties is Γ'. The number of sets of size r that intersect B is the number of sets of size r minus the number of sets of size r contained in $P \setminus B$ i.e.,

$$\binom{n}{r} - \binom{3n/4}{r} > (1-(3/4)^r)\binom{n}{r},$$

which holds since

$$\binom{3n/4}{r} = \frac{(\frac{3n}{4})(\frac{3n}{4}-1)\dots(\frac{3n}{4}-(r-1))}{r!} < \frac{(\frac{3}{4}n)(\frac{3}{4}n-\frac{3}{4})\dots(\frac{3}{4}n-\frac{3}{4}(r-1))}{r!} = \left(\frac{3}{4}\right)^r \binom{n}{r}.$$

Thus, the number of rank r access structures with an MSP over $\mathbb{F}_q$ of size at most S is at most

$$\binom{n}{n/4} \cdot 2^{(1-(3/4)^r)\binom{n}{r}} \cdot 2^{2r(3n/4)(4S/n)^2 \log q} = \exp\left(O\Big((1-(3/4)^r)\binom{n}{r} + \frac{rS^2 \log q}{n}\Big)\right).$$

□

The following result can be proved by using the bound in Theorem 6.17 and the counting argument used in the proof of Corollary 6.15.

Corollary 6.18. *For almost all rank r access structures with n parties, the total share size in every linear secret-sharing scheme with a one-bit secret realizing these access structures is $\Omega(n^{(r+1)/2})$.*

References

[1] Miguel Ambrona, Gilles Barthe, and Benedikt Schmidt. Generic transformations of predicate encodings: Constructions and applications. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017*, volume 10401 of *LNCS*, pages 36–66. Springer-Verlag, 2017.

[2] Benny Applebaum and Barak Arkis. On the power of amortization in secret sharing: d-uniform secret sharing and CDS with constant information rate. In Amos Beimel and Stefan Dziembowski, editors, *TCC 2018*, volume 11239 of *LNCS*, pages 317–344. Springer-Verlag, 2018.

[3] Benny Applebaum, Barak Arkis, Pavel Raykov, and Prashant Nalini Vasudevan. Conditional disclosure of secrets: Amplification, closure, amortization, lower-bounds, and separations. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017*, volume 10401 of *LNCS*, pages 727–757. Springer-Verlag, 2017.

[4] Benny Applebaum, Amos Beimel, Oriol Farràs, Oded Nir, and Naty Peter. Secret-sharing schemes for general and uniform access structures. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019*, volume 11478 of *LNCS*, pages 441–471. Springer-Verlag, 2019.

[5] Benny Applebaum, Amos Beimel, Oded Nir, and Naty Peter. Better secret sharing via robust conditional disclosure of secrets. In *52nd STOC*, pages 280–293. ACM, 2020.

[6] Nuttapong Attrapadung. Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 557–577. Springer-Verlag, 2014.

[7] Amos Beimel. *Secure Schemes for Secret Sharing and Key Distribution*. PhD thesis, Technion, 1996. www.cs.bgu.ac.il/~beimel/pub.html.

[8] Amos Beimel. Secret-sharing schemes: A survey. In Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang, Huaxiong Wang, and Chaoping Xing, editors, *Coding and Cryptology – Third International Workshop, IWCC 2011*, volume 6639 of *LNCS*, pages 11–46. Springer-Verlag, 2011.

[9] Amos Beimel and Benny Chor. Universally ideal secret sharing schemes. *IEEE Trans. on Information Theory*, 40(3):786–794, 1994.

[10] Amos Beimel, Oriol Farràs, and Yuval Mintz. Secret-sharing schemes for very dense graphs. *J. of Cryptology*, 29(2):336–362, 2016.

[11] Amos Beimel, Oriol Farràs, Yuval Mintz, and Naty Peter. Linear secret-sharing schemes for forbidden graph access structures. In Yael Kalai and Leonid Reyzin, editors, *TCC 2017*, volume 10678 of *LNCS*, pages 394–423. Springer-Verlag, 2017.

[12] Amos Beimel, Oriol Farràs, and Naty Peter. Secret sharing schemes for dense forbidden graphs. In Vassilis Zikas and Roberto De Prisco, editors, *SCN 2016*, volume 9841 of *LNCS*, pages 509–528, 2016.

[13] Amos Beimel, Anna Gál, and Mike Paterson. Lower bounds for monotone span programs. *Computational Complexity*, 6(1):29–45, 1997.

[14] Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions. In Yehuda Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 317–342. Springer-Verlag, 2014.

[15] Amos Beimel and Naty Peter. Optimal linear multiparty conditional disclosure of secrets protocols. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018*, volume 11274 of *LNCS*, pages 332–362. Springer-Verlag, 2018.

[16] Michael Ben-Or, Shaffi Goldwasser, and Avi Wigderson. Completeness theorems for noncryptographic fault-tolerant distributed computations. In *20th STOC*, pages 1–10, 1988.

[17] Josh Cohen Benaloh and Jerry Leichter. Generalized secret sharing and monotone functions. In Shaffi Goldwasser, editor, *CRYPTO '88*, volume 403 of *LNCS*, pages 27–35. Springer-Verlag, 1988.

[18] Michael Bertilsson and Ingemar Ingemarsson. A construction of practical secret sharing schemes using linear block codes. In Jennifer Seberry and Yuliang Zheng, editors, *AUSCRYPT '92*, volume 718 of *LNCS*, pages 67–79. Springer-Verlag, 1992.

[19] George Robert Blakley. Safeguarding cryptographic keys. In *Proc. of the 1979 AFIPS National Computer Conference*, volume 48 of *AFIPS Conference proceedings*, pages 313–317. AFIPS Press, 1979.

[20] Carlo Blundo, Alfredo De Santis, Roberto De Simone, and Ugo Vaccaro. Tight bounds on the information rate of secret sharing schemes. *Designs, Codes and Cryptography*, 11(2):107–122, 1997.

[21] Carlo Blundo, Alfredo De Santis, Douglas R. Stinson, and Ugo Vaccaro. Graph decomposition and secret sharing schemes. *J. of Cryptology*, 8(1):39–64, 1995.

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

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

[24] Siegfried Bublitz. Decomposition of graphs and monotone formula size of homogeneous functions. *Acta Inf.*, 23(6):689–696, 1986.

[25] Renato M. Capocelli, Alfredo De Santis, Luisa Gargano, and Ugo Vaccaro. On the size of shares for secret sharing schemes. *J. of Cryptology*, 6(3):157–168, 1993.

[26] David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols. In *20th STOC*, pages 11–19, 1988.

[27] Benny Chor and Eyal Kushilevitz. Secret sharing over infinite domains. *J. of Cryptology*, 6(2):87–96, 1993.

[28] Ronald Cramer, Ivan Damgård, and Ueli Maurer. General secure multi-party computation from any linear secret-sharing scheme. In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 316–334. Springer-Verlag, 2000.

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

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

[31] László Csirmaz. Secret sharing schemes on graphs. Technical Report 2005/059, Cryptology ePrint Archive, 2005. `eprint.iacr.org/`.

[32] Yvo Desmedt and Yair Frankel. Shared generation of authenticators and signatures. In Joan Feigenbaum, editor, *CRYPTO '91*, volume 576 of *LNCS*, pages 457–469. Springer-Verlag, 1992.

[33] Marten van Dijk, Wen-Ai Jackson, and Keith M. Martin. A note on duality in linear secret sharing schemes. *Bull. of the Institute of Combinatorics and its Applications*, 19:98–101, 1997.

[34] Paul Erdös and László Pyber. Covering a graph by complete bipartite graphs. *Discrete Mathematics*, 170(1–3):249–251, 1997.

[35] S. Fehr. Efficient construction of the dual span program. Manuscript, 1999.

[36] Anna Gál. *Combinatorial Methods in Boolean Function Complexity*. PhD thesis, U. of Chicago, 1995. Also: `www.eccc.uni-trier.de/\protect\unhbox\voidb@x\hbox{eccc-local/ECCC-Theses/gal.html}`.

[37] Romain Gay, Iordanis Kerenidis, and Hoeteck Wee. Communication complexity of conditional disclosure of secrets and attribute-based encryption. In Rosario Gennaro and Matthew Robshaw, editors, *CRYPTO 2015*, volume 9216 of *LNCS*, pages 485–502. Springer-Verlag, 2015.

[38] Yael Gertner, Yuval Ishai, Eyal Kushilevitz, and Tal Malkin. Protecting data privacy in private information retrieval schemes. *J. of Computer and System Sciences*, 60(3):592–629, 2000.

[39] Viput Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *13th CCS*, pages 89–98, 2006.

[40] Mitsuru Ito, Akira Saito, and Takao Nishizeki. Secret sharing schemes realizing general access structure. In *Globecom 87*, pages 99–102, 1987. Journal version: Multiple assignment scheme for sharing secret. *J. of Cryptology*, 6(1), 15-20, 1993.

[41] Wen-Ai Jackson and Keith M. Martin. Geometric secret sharing schemes and their duals. In *Designs, Codes and Cryptography*, volume 4, pages 83–95, 1994.

[42] Mauricio Karchmer and Avi Wigderson. On span programs. In *8th Structure in Complexity Theory*, pages 102–111, 1993.

[43] Tianren Liu and Vinod Vaikuntanathan. Breaking the circuit-size barrier in secret sharing. In *50th STOC*, pages 699–708, 2018.

[44] Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Conditional disclosure of secrets via non-linear reconstruction. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017*, volume 10401 of *LNCS*, pages 758–790. Springer-Verlag, 2017.

[45] Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Towards breaking the exponential barrier for general secret sharing. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018*, volume 10820 of *LNCS*, pages 567–596. Springer-Verlag, 2018.

[46] Yuval Mintz. Information ratios of graph secret-sharing schemes. Master's thesis, Dept. of Computer Science, Ben Gurion University, 2012.

[47] Michael Mitzenmacher and Eli Upfal. *Probability and Computing*. Cambridge University Press, 2005.

[48] Moni Naor and Avishai Wool. Access control and signatures via quorum secret sharing. In *3rd CCS*, pages 157–167, 1996.

[49] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In Ronald Cramer, editor, *EUROCRYPT 2005*, pages 457–473. Springer-Verlag, 2005.

[50] Adi Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.

[51] Bhavani Shankar, Kannan Srinathan, and C. Pandu Rangan. Alternative protocols for generalized oblivious transfer. In hrisha Rao, Mainak Chatterjee, Prasad Jayanti, C. Siva Ram Murthy, and Sanjoy Kumar Saha, editors, *9th ICDCN*, volume 4904 of *LNCS*, pages 304–309. Springer-Verlag, 2008.

[52] Douglas R. Stinson. Decomposition construction for secret sharing schemes. *IEEE Trans. on Information Theory*, 40(1):118–125, 1994.

[53] Hung-Min Sun and Shiuh-Pyng Shieh. Secret sharing in graph-based prohibited structures. In *INFOCOM '97*, pages 718–724, 1997.

[54] Tamir Tassa. Generalized oblivious transfer by secret sharing. *Designs, Codes and Cryptography*, 58(1):11–21, 2011.

[55] Brent Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *PKC 2011*, volume 6571 of *LNCS*, pages 53–70. Springer-Verlag, 2011.

[56] Hoeteck Wee. Dual system encryption via predicate encodings. In Yehuda Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 616–637. Springer-Verlag, 2014.