Secret Sharing Schemes for Dense Forbidden Graphs

Amos Beimel[1], Oriol Farràs[2], and Naty Peter[1(✉)]

[1] Ben Gurion University of the Negev, Be'er Sheva, Israel
amos.beimel@gmail.com, naty@post.bgu.ac.il
[2] Universitat Rovira i Virgili, Tarragona, Spain
oriol.farras@urv.cat

Abstract. A secret-sharing scheme *realizes 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 about the secret. A secret-sharing scheme *realizes a forbidden graph* if every two vertices connected by an edge can reconstruct the secret and every two vertices which are not connected by an edge do not get any information about the secret. Similar to secret-sharing schemes for general access structures, there are gaps between the known lower bounds and upper bounds on the total share size for graphs and for forbidden graphs. Following [Beimel et al. CRYPTO 2012], our goal in this paper is to understand how the total share size increases by removing few edges from a graph that can be realized by an efficient secret-sharing scheme.

We show that if a graph with n vertices contains at least $\binom{n}{2} - n^{1+\beta}$ edges for some $0 \leq \beta < \frac{1}{2}$, i.e., it is obtained by removing few edges from the complete graph, then there is a scheme realizing its forbidden graph in which the total share size is $O(n^{7/6+2\beta/3})$. This should be compared to $O(n^{3/2})$, the best known upper bound for the total share size in general forbidden graphs. Additionally, we show that a forbidden graph access structure obtained by removing few edges from an arbitrary graph G can be realized by a secret-sharing scheme with total share size of $O(m + n^{7/6+2\beta/3})$, where m is the total size of the shares in a secret-sharing scheme realizing G and $n^{1+\beta}$ is the number of the removed edges.

We also show that for a graph obtained by removing few edges from an arbitrary graph G with n vertices, if the chromatic number of the graph that contains the removed edges is small, then there is a fairly efficient scheme realizing the resulting graph; specifically, we construct a secret-sharing scheme with total share size of $\tilde{O}(m^{2/3}n^{2/3+2\beta/3}c^{1/3})$, where m is the total size of the shares in a secret-sharing scheme realizing G, the value $n^{1+\beta}$ is an upper bound on the number of the removed

Amos Beimel–Supported by ISF grant 544/13 and by the Frankel center for computer science.

Oriol Farràs–Supported by the Spanish Government through a Juan de la Cierva grant and TIN2014-57364-C2-1-R, by the European Union through H2020-ICT-2014-1-644024, and by the Government of Catalonia through Grant 2014 SGR 537.

V. Zikas and R. De Prisco (Eds.): SCN 2016, LNCS 9841, pp. 509–528, 2016.
DOI: 10.1007/978-3-319-44618-9_27

edges, and c is the chromatic number of the graph of the removed edges. This should be compared to $O(n^2/\log(n))$, the best known upper bound for the total share size for general graphs.

Keywords: Secret sharing · Covers by graphs · Avoiding covers

1 Introduction

A secret-sharing scheme, introduced by [11,32,41], is a method in which a dealer, which holds a secret (i.e., a string of bits), can distribute shares (which are strings) to a set of participants such that only predefined subsets of the participants can reconstruct the secret from their shares, while other subsets get no information about the secret. The collection of the subsets that can reconstruct the secret is called the access structure. Secret-sharing is an important primitive for storing sensitive information, being able to give access to just some subsets of parties. For example, secret-sharing schemes can be used in access control, giving access to the secret to some subsets of parties. Furthermore, secret-sharing schemes are used in many secure protocols and applications, such as multiparty computation [8,18], threshold cryptography [24], access control [38], attribute-based encryption [31,46], and oblivious transfer [42,45]. The question whether there is a secret-sharing scheme with small share size, i.e., polynomial in the number of participants, is the main open problem in secret-sharing schemes. Clearly, secret-sharing schemes with super-polynomial share size are not usable in the above-mentioned application of secret sharing.

In this paper we will mainly consider secret-sharing schemes in which the minimal authorized sets are of size 2, and we represent such access structures by graphs, where each vertex represents a participant and each edge represents a minimal authorized set. Following [5], we will study the problem of realizing graph access structures, in particular for graphs obtained by removing few edges from an arbitrary graph, and from the complete graph. Given a scheme realizing a graph, we want to understand how the size of the shares increases when removing few edges from the graph, compared to the size of the shares in the scheme of the original graph. We consider graphs with "good" schemes, i.e., graphs with schemes in which the size of the shares is small. We present efficient constructions both for graph access structures and for forbidden graph access structures.

1.1 Related Work

Works on Arbitrary Access Structures. Secret-sharing schemes were introduced by Shamir [41] and Blakley [11] for the threshold case, and by Ito et al. [32] for the general case. Threshold access structures, in which the authorized sets are all the sets containing at least t participants (for some threshold t), can be realized by secret-sharing schemes in which the size of each share is the size of the secret [11,41]. There are other access structures that have secret-sharing schemes in which the size of the shares is small, i.e., polynomial (in the number

of participants) share size [9,10,14,34]. In particular, Benaloh and Leichter [9] proved that if an access structure can be described by a small monotone formula, then it has an efficient secret-sharing scheme. Improving on this result, Karchmer and Wigderson [34] showed that if an access structure can be described by a small monotone span program, then it has an efficient secret-sharing scheme. However, the best known schemes for general access structures (e.g., [10,14,32,34]) are highly inefficient, i.e., they have share size of $2^{O(n)}$ (where n is the number of participants). The best lower bound known on the total share size of schemes realizing an access structure is $\Omega(n^2/\log(n))$ [21,22]. For linear secret-sharing schemes, which are secret-sharing schemes described by linear mappings, the best lower bound on the share size is $2^{\Omega(n^c)}$ for some constant $c < 1$ [20] (this very recent lower bound improves the results in [2,6,27,28]). Most known secret-sharing schemes are linear, and many applications require linear schemes. More information about secret sharing can be found in [3].

Graph Access Structures. A secret-sharing scheme realizes 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 is 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 size of the shares is $O(n^2/\log(n))$ [16,26].

Graph access structures have been studied in [5,6,12,13,15,17,23,43]. Capocelli et al. [17] proved that there exists a graph with 4 vertices such that the size of the share of at least one party is at least 3/2 times the size of the secret. Brickell and Davenport [15] showed that a graph access structure (with n vertices) can be realized by a secret-sharing scheme in which the total size of the shares is n if and only if the graph is a complete multipartite graph. Stinson [43] showed that for a graph with average degree d, there is a secret-sharing scheme realizing its graph access structure in which the average share size of a vertex is at most $(d+1)/2$. Blundo et al. [13] presented upper and lower bounds on the size of the shares of a scheme realizing graph access structures, for multipartite graphs, connected graphs, paths, cycles, and trees. In particular, it is proven in [13] that the smallest share size of a scheme which realizes a graph access structure is the size of the secret or at least 1.5 times greater than the size of the secret. Blundo et al. [12] showed that there exists a d-regular graph such that the share size of each vertex in any scheme that realizes its graph access structure is at least $(d+1)/2$. Beimel et al. [6] proved a lower bound of $\Omega(n^{3/2})$ on the total share size of a linear schemes realizing a certain graph access structure. Csirmaz [23], extending a result of van Dijk [25], showed that there exist graphs for which the total share size in every secret-sharing scheme realizing their graph access structures is $\Omega(n\log(n))$.

Beimel et al. [5] 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 $\tilde{O}(n^{5/4+3\beta/4})$. They also showed that if $n^{1+\beta}$ edges are removed

from an arbitrary graph that can be realized by a secret-sharing scheme with total share size m, then the resulting graph can be realized by a secret-sharing scheme with total share size $\tilde{O}(m^{1/2}n^{1+\beta/2})$.

Some of the results for graph access structures have been extended to general access structures, e.g., Martí-Farré and Padró [36], generalizing results of [13], showed that in every secret-sharing scheme realizing an access structure that is not a port matroid (and, hence, not ideal) the size of the shares is at least 1.5 times the size of the secret. Other results have been extended to homogenous access structures [35,39], which are access structures in which the minimal authorized sets are of the same size (in graph access structures, this size is 2), e.g., Padró and Sáez [39] showed upper bounds on the size of the shares of secret-sharing schemes realizing homogenous access structures. These results demonstrate that graph access structures can be used to understand problems about general access structures.

Forbidden Graph Access Structures. Another model we consider is the forbidden graph access structures, which was first described in [44]. A secret-sharing scheme realizes a forbidden graph access structure if every two vertices can reconstruct the secret if and only if they are connected by an edge. We do not care if sets of 3 or more vertices can reconstruct the secret (in [44], every set of 3 or more vertices can reconstruct the secret). The requirement that every set of 3 or more vertices can reconstruct the secret (as in [44]) increases slightly the total share size, since we can independently share the secret using the 3-out-of-n scheme of Shamir [41], in which the size of the share of every participant is the size of the secret (when the size of the secret is at least $\log(n)$).

The requirements for graph access structures are stronger than for forbidden graph access structures, since for graph access structures every independent set in the graph is an unauthorized subset, and in forbidden graph access structures we only require independent sets of size 2 to be unauthorized sets.

Every forbidden graph access structure can be realized by a secret-sharing scheme in which the size of the shares is $O(n^{3/2})$ [7]. Furthermore, this can be done by a linear scheme [29]. In contrast, the best *known* upper bound for graph access structures is $O(n^2/\log(n))$ [23].

Gertner et al. [30] presented conditional disclosure of secrets (CDS). In this problem, two parties 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). For that, each party sends one message to the referee (this message depends only on its input and the secret), and if the predicate holds the referee can reconstruct the secret from the messages it received. This problem is interesting, since in [30] CDS is used to efficiently realize a symmetrically-private information retrieval (SPIR) schemes. Additionally, in [29] it is shown that CDS can be used for attribute-based encryption [31,40].

We can represent the CDS problem as the problem of realizing a secret-sharing scheme for a forbidden graph access structure of a bipartite graph and vice-versa: Every possible input for the first party is a vertex in the first part of the graph and every possible input for the second party 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. The size of the share of each vertex is equivalent to the size of the message sent to the referee by the party, when it holds the input associated with the vertex. We get a bipartite graph with 2^N vertices in each part (where N is the size of the input of the parties).

It was shown in [29] that for every predicate there exists a linear CDS such that the size of each of the messages sent by the two parties to the referee is $2^{N/2}$.[1] It implies that there exists a linear secret-sharing scheme in which the total size of the shares is $O(n^{3/2})$ (where n is the number of the participants) for every forbidden graph access structure.

By a generalization of a result of [37], we get a lower bound of $\Omega(n^{3/2})$ on the size of the shares of a linear scheme realizing an implicit forbidden graph access structures.

1.2 Our Results

The first problem we deal with in this paper is the construction of secret-sharing schemes realizing forbidden graph access structures for dense graphs, i.e., for graphs in which its complement graph contains few edges. Given a dense graph with n vertices and with at least $\binom{n}{2} - n^{1+\beta}$ edges, for some $0 \leq \beta < \frac{1}{2}$, we construct a secret-sharing scheme that realizes its forbidden graph access structure, in which the total size of the shares is $O(n^{7/6+2\beta/3})$. Compared to [5], which shows that graph access structures of such graphs can be realized by a scheme with total share size $\tilde{O}(n^{5/4+3\beta/4})$, our scheme for forbidden graph access structures is more efficient.

As a corollary, we show that if a graph with n vertices contains $\binom{n}{2} - \ell$ edges for some $0 < \ell < n$, then it can be realized by a secret-sharing scheme in which the total share size is $O(n + \ell^{7/6})$. For example, if $\ell = O(n^{6/7})$, then the total share size of the scheme is $O(n)$.

In addition, we show that if an arbitrary forbidden graph access structure (with n vertices) can be realized by a secret-sharing scheme in which the total size of the shares is m, and we remove $n^{1+\beta}$ edges from it (for some $0 \leq \beta < \frac{1}{2}$), then the resulting forbidden graph access structure can be realized by a secret-sharing scheme in which the total size of the shares is $O(m + n^{7/6+2\beta/3})$.

The second problem we consider is constructing secret-sharing schemes that realize graph access structures for graphs obtained when removing few edges from an arbitrary graph that has a "good" scheme, i.e., the size of the shares in this scheme is relatively small. We solve this question when the graph of the removed edges has a small chromatic number.

Namely, we consider a graph with n vertices that can be realized by a secret-sharing scheme with total share size m, and we remove a set of at most $n^{1+\beta}$ edges from the graph, for some $0 \leq \beta < 1$. Then we show that if the chromatic number

[1] A linear CDS is a CDS in which if the predicate holds, then the reconstruction function of the referee is linear.

c of the graph with the removed edges satisfies $c < \frac{n^{1-\beta/2}}{m^{1/2}}$, then the obtained graph has a secret-sharing scheme with total share size $\tilde{O}(m^{2/3}n^{2/3+2\beta/3}c^{1/3})$.

It should be compared to the result of Beimel et al. [5], showing that such a graph can be realized by a scheme with total share size $\tilde{O}(m^{1/2}n^{1+\beta/2})$ without any restrictions on the chromatic number of the removed edges. Thus, our scheme is better when the chromatic number is relatively small and m is not too big (it is always more efficient when $c < \frac{n^{1-\beta/2}}{m^{1/2}}$).

Remark 1.1. In particular, our result is valid for graphs obtained by removing few edges from a graph with small chromatic number, denoted by c, since in this case the graph which contains the removed edges is a subgraph of the original graph, and thus, its chromatic number is at most c.

As a corollary, we show that if a graph with n vertices can be realized by a secret-sharing scheme with total share size m, and we remove ℓ edges from it, for some $0 < \ell < n$, such that the chromatic number of the graph containing the removed edges is c, where $c < \frac{\ell}{m^{1/2}}$, then we can realize the remaining graph by a secret-sharing scheme in which the total share size is $\tilde{O}(cm + m^{2/3}\ell^{2/3}c^{1/3})$. Thus, if $\ell = \Theta(cm^{1/2})$, then the total share size of the scheme is $\tilde{O}(cm)$.

Techniques. A cover of a graph G is a collection of subgraphs of G satisfying that every edge in G appears in at least one subgraph of the collection. Covers of graphs where used to construct secret-sharing schemes (e.g., in [5,43]). The idea of the construction is to share the secret independently for each subgraph in the cover. By choosing subgraphs that have efficient secret-sharing schemes (e.g., multipartite graphs, which have an ideal scheme), it is possible to find efficient schemes for other graphs.

When realizing the graph access structure of a graph obtained by removing few edges from a general graph G, we use a new technique of *avoiding covers*. We cover a bipartite graph, which is a subgraph of G, by bipartite graphs $G_1, \ldots, G_r$ in such a way that for every bipartite graph G_i of the cover, there are no removed edges between any two vertices (in the same part or in different parts) in the graph G_i. Then, for every graph G_i of the cover, we share the secret independently using the scheme of the graph G.

Following [5], we construct a scheme realizing graph access structures of graphs obtained by removing few edges with small chromatic number from a general graph in 3 main steps. We first realize all the edges incident to vertices with high degree in the graph of the removed edges by stars, and remove these vertices and their incident edges from the graph. After this step, the degree of every vertex in the graph of the removed edges is bounded. Next, we reduce the maximum degree of a vertex in the graph of the removed edges by using the chromatic number of the graph, and in the final step we use the avoiding cover to realize the remaining graph.

Similar to graph access structures, the main scheme realizing forbidden graph access structures of dense graphs contains 3 main steps. First, we realize all the

edges incident to vertices with high degree in the complement graph by two independent schemes, for the induced graph on these vertices, and for the bipartite graph between these vertices and the remaining vertices. We then remove these vertices and their incident edges from the graph. In this step, we use the scheme of [7,29] and get a more efficient scheme than the cover by stars used in [5] for graph access structures. We get a graph in which the degree of every vertex in its complement is bounded. Next, we decrease the maximum degree of a vertex in the complement graph $\log\log(n)$ times, and finally we realize the remaining graph using a *forest cover*.

2 Preliminaries

In this section we define secret-sharing schemes, secret-sharing schemes for graphs and for forbidden graphs, and some other useful definitions. Additionally, we present the graph terminology we use.

Notations. We denote the logarithmic function with base 2 and base e by log and ln, respectively. We use the $\tilde{O}$ notation, which ignores polylogarithmic factors, i.e., $O(n^{\delta}\log^{a}(n)) = \tilde{O}(n^{\delta})$ for a constant a. For any two strings of bits s_1, s_2, let $s_1 \oplus s_2$ denote the bitwise exclusive-or between the strings.

Secret Sharing. We start by defining access structures, distribution schemes, and secret-sharing schemes, as described in [4,19].

Definition 2.1 (Access Structures, Distribution Schemes, and Secret Sharing). *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 subsets 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 party 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 $\Pi_A(s, r)$ as the restriction of $\Pi(s, r)$ to its A-entries. Given a distribution scheme, the size of the secret is $\log(|K|)$, the (normalized) size of the share of party p_j is $\frac{\log(|K_j|)}{\log(|K|)}$, and the (normalized) total share size of the distribution scheme is $\sum_{j=1}^{n} \frac{\log(|K_j|)}{\log(|K|)}$.

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 requirement: *The secret k can be reconstructed by any authorized set of parties.*

Privacy requirement: *Every unauthorized set cannot learn anything about the secret from their shares.*

Graph Terminology. In this paper we consider graph access structures and forbidden graph access structures. In the sequence, $G = (V, E)$ is an undirected graph, where the vertices of V will also denote parties of an access structure as discussed below.

The degree of a graph is the maximum degree of a vertex in the graph. A graph $G' = (V', E')$ is a subgraph of the graph $G = (V, E)$ if $V' \subseteq V$ and $E' \subseteq E \cap (V' \times V')$. All through this paper, n is the number of the vertices in the graph $G = (V, E)$, i.e., $|V| = n$.

Definition 2.2 (The Complement Graph and Intersection of Graphs). *Given a graph $G = (V, E)$, the complement graph of G is the graph $\overline{G} = (V, \overline{E})$, where every two vertices $u, v \in V$ satisfy $(u, v) \in \overline{E}$ if and only if $(u, v) \notin E$. Given two graphs $G_1 = (V, E_1)$ and $G_2 = (V', E_2)$ such that $V' \subseteq V$, the intersection of G_1 and G_2 is $G_1 \cap G_2 = (V', E_1 \cap E_2)$.*

Next we define one of the techniques to construct a secret-sharing scheme realizing a graph that uses covers of graphs.

Definition 2.3 (λ-Covers). *Let $G = (V, E)$ be a graph. A λ-cover of G is a collection of graphs $G_1 = (V_1, E_1), \ldots, G_r = (V_r, E_r)$ such that each G_i is a subgraph of G, and each edge in E is in at least λ graphs of the collection. A cover of G is a 1-cover of G.*

Recall that a bipartite graph $G = (U, V, E)$ is a graph where the vertices are $U \cup V$ (U and V are called the parts of G) and $E \subseteq U \times V$. A bipartite graph is complete if $E = U \times V$. A complete bipartite λ-cover of G is a λ-cover of G by complete bipartite graphs. A complete bipartite cover of G is a complete bipartite 1-cover of G.

Definition 2.4 (Equivalence Graphs and Equivalence Covers [1]). *An equivalence graph is a vertex-disjoint union of cliques. An equivalence cover of the graph $G = (V, E)$ is a cover $G_1 = (V_1, E_1), \ldots, G_r = (V_r, E_r)$ of G such that each G_i is an equivalence graph.*

Definition 2.5 (The Graph G_F and the Graph G_F^*). *Given a graph $G = (V, E)$ and a set of vertices $F \subset V$, we define the bipartite graph $G_F = (F, V \setminus F, E \cap (F \times (V \setminus F)))$, which is the bipartite graph with parts F and $V \setminus F$, restricted to the edges of G.*

For a set of vertices $F \subset V$ and a set of edges $E^* \subset E$ (which is the set of the removed edges), we define $G_F^* = (F, V \setminus F, \overline{E^*} \cap (F \times (V \setminus F)))$, i.e., G_F^* is a bipartite graph with parts F and $V \setminus F$, which contains only the edges that are not removed from G.

Forbidden Graphs and Secret Sharing. We next present the definition of forbidden graph access structures, in which we only require that sets of size 2 that are edges can reconstruct the secret, while sets of size 2 that are not edges cannot learn any information about the secret.[2]

Definition 2.6 (Forbidden Graph Access Structures). *Given a graph $G = (V, E)$, its forbidden graph access structure Γ is the access structure on V composed of all the sets in E and all the sets of 3 or more vertices. For a graph $G = (V, E)$, a secret-sharing scheme realizes its forbidden graph if the scheme realizing its forbidden graph access structure, i.e., if every edge of E and every set of size at least 3 can reconstruct the secret, and every edge of $\overline{E}$ cannot get any information about the secret.*

In our constructions for forbidden graph access structures, edges are removed from the complete graph $G = (V, E)$, where $|E| = \binom{V}{2}$. The set $E^* \subset E$ is the set of edges we remove from the graph G, i.e., the excluded edges, such that $|E^*| \leq n^{1+\beta}$ for some constant $0 \leq \beta < \frac{1}{2}$, i.e., we remove at most $n^{1+\beta}$ edges from the complete graph. We want to realize the graph $G \cap G^* = G^*$, where $G^* = (V, \overline{E^*})$, i.e., we want to find a secret-sharing scheme in which each edge in $E \setminus E^* = \overline{E^*}$ can reconstruct the secret and each edge in E^* cannot learn any information about the secret. Note that since $|E^*| \leq n^{1+\beta}$, the number of edges in the graph G^* is $|\overline{E^*}| \geq \binom{n}{2} - n^{1+\beta}$, i.e., the graph G^* is a dense graph in which its complement contains few edges. Our constructions are only useful when $0 \leq \beta < \frac{1}{2}$, since for larger values of β, the total share size of the schemes we present is larger than $n^{3/2}$ and every forbidden graph access structure can be realized by a secret-sharing scheme whose total share size is $O(n^{3/2})$.

Graphs and Secret Sharing. Next, we formally define graph access structures.

Definition 2.7 (Graph Access Structures). *Given a graph $G = (V, E)$, its graph access structure is the access structure whose set of participants is V and whose minimal authorized sets are the edges in E, that is, a set is authorized if it contains an edge, and a set is not authorized if it is an independent set in G. We say that a secret-sharing scheme realizes a graph if the scheme realizes its graph access structure, i.e., if every edge can reconstruct the secret, and every independent set in G cannot get any information about the secret.*

Remark 2.8. When we say that a secret-sharing scheme realizes a graph, we mean that the scheme realizes its graph access structure or its forbidden graph access structure, according to the context, e.g., if we discuss forbidden graph access structures, we say that a secret-sharing scheme realizing a graph if the scheme realizing its forbidden graph access structure. In Sect. 3 we consider forbidden graph access structures and in Sect. 4 we consider graph access structures.

[2] In [44], the access structure is specified by the complement graph, i.e., by the edges that are forbidden from learning information on the secret.

We use the following notations: the graph $G = (V, E)$ is the original graph. The set $E^* \subset E$ is the set of edges we remove from the graph G, i.e., the excluded edges, such that $|E^*| \leq n^{1+\beta}$ for some constant $0 \leq \beta < 1$. Furthermore, m is the total share size of a secret-sharing scheme realizing the graph G.

We want to find a secret-sharing scheme in which each edge in $E \setminus E^*$ (equivalently, in $E \cap \overline{E^*}$) can reconstruct the secret, and such that every set of vertices with no edge in $E \setminus E^*$ cannot learn any information on the secret. Additionally, we use the notation G^*, where $G^* = (V, \overline{E^*})$, i.e., G^* is the graph of the edges that are not removed, and $\overline{G^*} = (V, E^*)$ is the graph which contains the removed edges from G. The value $\chi(\overline{G^*})$ is the chromatic number of $\overline{G^*}$, i.e., the minimal number of colors needed to color the vertices of V such that there are no edges of E^* between any two vertices with the same color. Our construction applies only when the graph of the removed edges has a small chromatic number.

In the definition of secret-sharing schemes realizing graph access structures we require that every independent set cannot learn any information about the secret. However, in our constructions in Sect. 4 we only claim that non-edges cannot learn information on the secret. The next claim shows that, due to the selection of special covers, in our constructions the latter requirement implies the former strong requirement (as discussed in Sect. 3, this is not true for general constructions).

Claim 2.9. *Let $G = (V, E)$ be a graph, and $G_1 = (V_1, E_1), \ldots, G_r = (V_r, E_r)$ be graphs such that each G_i is a subgraph of G. If we independently realize each graph G_i using a scheme that realizes the graph access structure of G_i (i.e., every independent set in G_i does not get any information on the secret), then every independent set in G cannot learn any information on the secret.*

Remark 2.10. In our construction, we use the scheme of the graph G to realize subgraphs of G with no removed edges (i.e., with no edges from E^*). We also use the trivial scheme for some edges from $E \setminus E^*$ (i.e., sharing the secret independently for each edge). These schemes also realize subgraphs of G with no edges from E^* (each such subgraph contains only one edge). Since we use schemes that realize the graph access structures of subgraphs of G, a set of vertices can reconstruct the secret if and only if it contains an edge from the graph G. So, by Claim 2.9, to argue that every independent set of $G \cap G^*$ cannot learn any information on the secret, it is sufficient to show that every edge in $\overline{E} \cup E^*$ cannot learn any information on the secret.

3 Schemes for Forbidden Graph Access Structures

In this section, we consider forbidden graph access structures, where every edge in the graph can reconstruct the secret, and every edge not in the graph cannot reconstruct the secret. In all the schemes in this section, except for the schemes presented in Lemma 3.1 and in Theorem 3.2, the size of the secret should be at least $\log(n)$, since in these schemes we use the t-out-of-n scheme of Shamir [41]. Some of the proofs in this section are deferred to the full version of this paper.

3.1 Constructions for Arbitrary Graphs

In the first scheme we realize bipartite graphs. The following schemes are based on the construction for CDS of [29].

Lemma 3.1. *Let $H = (U, V, E)$ be a bipartite graph such that $|U| = k$ and $|V| = n$. Then, there is a secret-sharing scheme such that: (1) each edge in H can reconstruct the secret, (2) each edge not in H cannot learn any information about the secret, and (3) if $k^2 \leq n$ then the total share size of the scheme is $O(n)$. Otherwise, the total share size of the scheme is $O(n^{1/2}k)$.*

The following theorem provides a scheme realizing an arbitrary graph G. We use the scheme of Lemma 3.1 for bipartite graphs $\log(n)$ times to get a scheme for an arbitrary graph.

Theorem 3.2 ([7,29]). *Let $G = (V, E)$ be a graph such that $|V| = n$. Then, there is a secret-sharing scheme such that: (1) each edge in G can reconstruct the secret, (2) each edge not in G cannot learn any information about the secret, and (3) if the size of the secret is 1, then the total share size of the scheme is $O(n^{3/2}\log(n)) = \tilde{O}(n^{3/2})$. If the size of the secret is $\Omega(\log^2(n))$, then the total share size of the scheme is $O(n^{3/2})$.*

3.2 Constructions for Bounded Degree Excluded Graphs

The next lemma shows that given a forest, i.e., a graph that does not contain any cycle, we can realize its complement graph with a scheme in which the total share size is $O(n)$. In the sequence, we use this scheme in the following construction, to realize the complement of a bounded degree graph.

Lemma 3.3. *Let $G = (V, E)$ be a graph such that its complement graph $\overline{G} = (V, \overline{E})$ is a forest. Then, there is a secret-sharing scheme such that: (1) each edge in G can reconstruct the secret, (2) each edge not in G cannot learn any information about the secret, and (3) the total share size of the scheme is at most $3n$.*

Proof Sketch. Denote $V = \{v_1, \ldots, v_n\}$. Since $\overline{G}$ is a forest, it is composed of trees. Let $T_1 = (V_1, E_1), \ldots, T_k = (V_k, E_k)$ be the trees in the graph $\overline{G}$ containing all the vertices in G (isolated vertices in $\overline{G}$ are trees with one vertex). First, we share the secret by generating $n + k$ shares $r_1, \ldots, r_{n+k}$ using the 4-out-of-$(n + k)$ scheme of Shamir [41]. For every $1 \leq i \leq k$, we give shares to the vertices in the tree T_i as follows: For the tree $T_i = (V_i, E_i)$, denote $|V_i| = t$ and $V_i = \{v_{i_1}, \ldots, v_{i_t}\}$. We consider the tree as a rooted tree, with a root v_{i_1}, and for every vertex v in T_i, we denote the parent of v by $\pi(v)$. The root vertex v_{i_1} gets the shares r_{n+i}, r_{i_1}, and for every $2 \leq j \leq t$, vertex $v_{i_j} \in V_i$ gets the shares r_p, r_{i_j}, where $\pi(v_{i_j}) = v_p$.

Additionally, we denote the maximum distance of a vertex from the root by D_i. For every $1 \leq \ell \leq D_i$, define $F_{i,\ell} = \{v \in V_i$: The distance of v

from the root in the tree T_i is $\ell\}$. For every $F_{i,\ell}$, we independently share the secret by generating $|F_{i,\ell}|$ shares $t_1, \ldots, t_{|F_{i,\ell}|}$ using the 2-out-of-$|F_{i,\ell}|$ scheme of Shamir, and giving the jth vertex in $F_{i,\ell}$ the share t_j. It can be verified that the above scheme is correct, private, and has shares of size $3n$. □

Definition 3.4 (Covers by Forests). *Let $H = (V, E)$ be a graph. A forest cover of H is a cover $G_1 = (V, E_1), \ldots, G_r = (V, E_r)$ of H such that each G_i is a forest.*

The next lemma shows that every graph with degree d can be covered by a forest cover of size d.

Lemma 3.5. *Let $H = (V, E)$ be a graph such that the degree of each vertex in H is bounded by d. Then, there is a cover of H by d forests $G_1 = (V, E_1), \ldots, G_d = (V, E_d)$ such that every edge $e \in E$ appears in exactly one graph of the cover.*

The forest cover is used below to construct a scheme for the complement of a bounded degree graph. The secret-sharing scheme we present saves a factor of $\Theta(\log(n))$ compared to the scheme of [5], which realizes graph access structures of bounded degree graphs (we only realize forbidden graph access structures).

Theorem 3.6. *Let $G = (V, E)$ be a graph such that the degree of every vertex in its complement graph $\overline{G} = (V, \overline{E})$ is bounded by d. Then, there is a secret-sharing scheme realizing the forbidden graph access structure of G such that the total share size of the scheme is at most $3dn$.*

Definition 3.7. (The Bipartite Complement). *Let $H = (U, V, E)$ be a bipartite graph. The bipartite complement of H is the bipartite graph $\overline{H} = (U, V, \overline{E})$, where every $u \in U$ and $v \in V$ satisfy $(u, v) \in \overline{E}$ if and only if $(u, v) \notin E$.*

First, we show how to construct a scheme realizing a bipartite graph such that the degree of every vertex in one part in its bipartite complement is bounded.

Lemma 3.8. *Let $H = (U, V, E)$ be a bipartite graph with $|V| = n$ and $|U| = k \leq n$ satisfying that the degree of every vertex in V in the bipartite complement graph $\overline{H} = (U, V, \overline{E})$ is at most d. Then, there is a secret-sharing scheme such that: (1) each edge in H can reconstruct the secret, (2) each edge not in H (including edges between vertices in the same part in the bipartite graph H) cannot learn any information about the secret, and (3) the total share size of the scheme is at most $8dn$.*

Proof. To share a secret s, we choose random strings s_1, s_2, s_3 such that $s = s_1 \oplus s_2 \oplus s_3$. We give s_1 to each vertex in U and give s_2 to each vertex in V. The total share size for these shares is at most $2n$. By Lemma 3.5, there is a cover of $\overline{H}$ by d forests such that every edge in $\overline{H}$ appears in exactly one graph of the cover. Next, consider the graph $G = (U \cup V, E \cup (U \times U) \cup (V \times V))$. Notice that G is the complement graph of the graph $\overline{H}$. We share s_3 to the graph G using the forest cover of $\overline{H}$ by the scheme from Theorem 3.6 such that each edge in G

can reconstruct the secret and each edge in $\overline{H}$ cannot learn any information on the secret, and the total share size of the scheme is at most $3d(|U|+|V|) \leq 6dn$. Thus, the total share of the resulting scheme is at most $8dn$.

For an edge $(u,v) \in E$ such that $u \in U$ and $v \in V$, the edge (u,v) is in G, and thus, the edge (u,v) can reconstruct s_3. Moreover, since $u \in U$, the vertex u holds s_1 and since $v \in V$, the vertex v holds s_2, and, hence, the edge (u,v) can reconstruct the secret s by performing bitwise exclusive-or between the strings s_1, s_2, s_3.

For an edge $(u,v) \notin E$ such that $u,v \in U$, vertices u,v do not hold the string s_2, and, hence, cannot learn any information on the secret. For an edge $(u,v) \notin E$ such that $u,v \in V$, the vertices u,v do not hold the string s_1, and, hence, cannot learn any information on the secret. For an edge $(u,v) \notin E$ such that $u \in U$ and $v \in V$, the edge (u,v) is in $\overline{H}$, and thus, the edge (u,v) cannot learn any information on s_3, and cannot learn any information about the secret. □

We use a different construction to realize a bipartite graph such that one part is much smaller than the other and the degree of every vertex in its bipartite complement is bounded.

Lemma 3.9. *Let $H = (U,V,E)$ be a bipartite graph with $|V| = n$ and $|U| = k \leq n$ satisfying that the degree of every vertex in $U \cup V$ in the bipartite complement graph $\overline{H} = (U,V,\overline{E})$ is at most d, where $d < k$. Then, there is a secret-sharing scheme realizing the forbidden graph access structure of H such that the total share size of the scheme is $O(n + d^{2/3}k^{4/3})$.*

Proof. Define $D_1 = \{v \in V :$ There exists $u \in U$ such that $(u,v) \in \overline{H}\}$. Since the degree of every vertex of U in $\overline{H}$ is at most d, the size of D_1 is at most dk. Furthermore, the complete bipartite graph $H_1 = (U, V \setminus D_1, U \times (V \setminus D_1))$ is a subgraph of H. We realize H_1 by an ideal scheme in which the total share size is at most $|U| + |V| = O(n)$ (see Fig. 1).

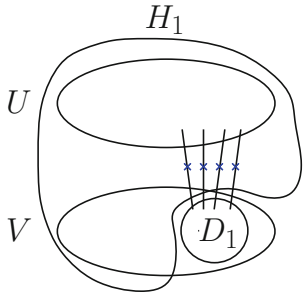

Fig. 1. The bipartite graph H_1. Edges in $\overline{E}$ are marked with blue crosses.

Next, define $D_2 = \{v \in D_1 :$ The degree of v in $\overline{H}$ is at least $(\frac{k}{d})^{\frac{1}{3}}\}$. Because the graph $\overline{H}$ contains at most dk edges, we get that $|D_2| \leq dk/(\frac{k}{d})^{\frac{1}{3}} = d^{4/3}k^{2/3}$.

Let $H_2 = (U, D_2, E \cap (U \times D_2))$. Since $d < k$, we get that $|U|^2 = k^2 = k^{4/3}k^{2/3} > d^{4/3}k^{2/3} \geq |D_2|$, and, hence, by Lemma 3.1, we can realize the graph H_2 such that each edge in H_2 can reconstruct the secret, each edge not in H_2 cannot learn any information about the secret, and the total share size of the scheme is $O(|D_2|^{\frac{1}{2}} \cdot |U|) = O((d^{4/3}k^{2/3})^{\frac{1}{2}}k) = O(d^{2/3}k^{4/3})$.

Finally, let $D_3 = D_1 \setminus D_2$ and $H_3 = (U, D_3, E \cap (U \times D_3))$. The degree of each vertex of D_3 in the graph $\overline{H_3}$ is at most $(\frac{k}{d})^{\frac{1}{3}}$. By Lemma 3.6, we can realize the graph H_3 by a scheme in which the total share size is $O((\frac{k}{d})^{\frac{1}{3}}dk) = O(d^{2/3}k^{4/3})$.

As H_1, H_2, and H_3 cover H, we constructed a scheme realizing H such that each edge in H can reconstruct the secret, each edge not in H cannot learn any information about the secret, and the total share size of the scheme is $O(n + d^{2/3}k^{4/3})$. □

3.3 Constructions for Excluded Graphs with Few Edges

Given a graph, the following construction shows how to realize the edges incident to vertices with high degree in its complement. Recall that $\overline{G^*}$ is the graph which contains the removed edges.

Lemma 3.10. *Let $G = (V, E)$ be the complete graph and $E^* \subset E$ such that $|E^*| \leq n^{1+\beta}$, where $0 \leq \beta < \frac{1}{2}$. Then, for every $d = n^{\beta+\varepsilon}$ for some constant $0 < \varepsilon \leq \frac{1}{2}$, we can remove a set of vertices and all their incident edges from the graph G^* and obtain the graph G^*_d such that the degree of every vertex in $\overline{G^*_d}$ is at most d, the graph $\overline{G^*_d}$ contains at most $n^{1+\beta}$ edges, and the total share size for the removed edges from G^* is $O(\frac{n^{3/2+\beta}}{d})$.*[3]

Proof Sketch. To prove the above lemma, note that there are at most $O(n^{1+\beta}/d)$ vertices whose degree in the graph of excluded edges is greater than d. We use Lemma 3.1 to realize the bipartite graph, where one part contains the vertices of degree greater than d and the other part are all other vertices. The share size in the above scheme is $O((n^{1+\beta}/d) \cdot n^{1/2}) = O(n^{3/2+\beta}/d)$. We also use the the scheme of Theorem 3.2 to realize the graph containing the edges between the vertices of degree at least d; the share size of this secret-sharing scheme is smaller than $O(n^{3/2+\beta}/d)$. □

For a graph such that the degree of every vertex in its complement is bounded, we show how to decrease the maximum degree of a vertex in its complement by removing few vertices from the graph and realize all the removed edges from it.

Lemma 3.11. *Let $0 < \alpha' < \alpha \leq 1$ such that $\alpha \geq \frac{1}{6}$ and let $G = (V, E)$ be the complete graph. Furthermore, let $E^* \subset E$ such that $|E^*| = \ell$, and assume that the degree of each vertex in $\overline{G^*}$ is at most n^α. Then, we can remove a set of vertices and all their incident edges from the graph G^* and obtain the graph*

[3] We intend to the total share size of the scheme realizing the graph of the edges we removed from G^* in Lemma 3.10 and are contained in $E \setminus E^*$. The same is also valid for Lemma 3.11.

$G^*_{\alpha'}$ such that the degree of every vertex in $\overline{G^*_{\alpha'}}$ is at most $n^{\alpha'}$, the graph $\overline{G^*_{\alpha'}}$ contains $\ell - \ell'$ edges for some $\ell' > 0$, and the total share size for the removed edges from G^* is $O(\ell' n^{1/4+\alpha/2-\alpha'})$.

Proof. Define $d = n^{\alpha}$ and $d' = n^{\alpha'}$ (notice that $d' < d$). Additionally, let

$$D = \{v \in V : \text{The degree of } v \text{ in } \overline{G^*} \text{ is at least } d'\}.$$

We remove the vertices of D in steps, where in each step we choose a set F of $k = \frac{n^{3/4}}{d^{1/2}} > 1$ (since $d \leq n$) vertices, and remove F and all the edges incident to the vertices of F (if the number of the remaining vertices with degree at least d' in $\overline{G^*}$ is smaller than k, then we take the remaining vertices with degree at least d' and put them in F).

First, consider all the edges between two vertices in F. By Theorem 3.2, we can realize the graph $G^*[F] = (F, \overline{E^*} \cap (F \times F))$ by a scheme such that every edge in $G^*[F]$ can reconstruct the secret and every edge not in $G^*[F]$ cannot learn any information about the secret, in which the total share size is $O(k^{\frac{3}{2}}) = O((\frac{n^{3/4}}{d^{1/2}})^{\frac{3}{2}}) = O(\frac{n^{9/8}}{d^{3/4}}) = O(n)$ (since $d \geq n^{1/6}$).

Next, consider the bipartite graph $G^*_F = (F, V \setminus F, \overline{E^*} \cap (F \times (V \setminus F)))$. Because the degree of every vertex in $\overline{G^*}$ is at most d, the degree of every vertex in the bipartite complement graph $\overline{G^*_F}$ is at most d. Hence, by Lemma 3.9, we can realize the graph G^*_F such that: (1) every edge in G^*_F can reconstruct the secret, (2) every edge not in G^*_F cannot learn any information about the secret, and (3) the total share size of the scheme is $O(n)$. Thus, we can remove the vertices of F and all the edges incident to them from the graph G^*, and the total share size of the scheme for this step is $O(n)$.

We continue in the same manner until the degree of all the vertices in the graph $\overline{G^*}$ is at most d' and obtain the graph $G^*_{\alpha'}$ after removing all the vertices with degree greater than d' in the graph $\overline{G^*}$ and the edges incident to them from G^*. Let ℓ' be the total number of edges we removed from $\overline{G^*}$ in these steps until the degree of every vertex in $\overline{G^*}$ is at most d'. The graph $\overline{G^*_{\alpha'}}$ contains $\ell - \ell'$ edges and the degree of every vertex in $\overline{G^*_{\alpha'}}$ is at most d'. Additionally, in every iteration, except for the last, we remove at least kd' edges. Thus, there are at most $1 + \frac{\ell'}{d'k} = O(\frac{\ell' d^{1/2}}{d' n^{3/4}})$ iterations in this process, and the total share size for the removed edges from G^* is $O(\frac{\ell' d^{1/2}}{d' n^{3/4}} \cdot n) = O(\ell' n^{1/4+\alpha/2-\alpha'})$. □

The next scheme realizes dense graphs using three main steps as described in the beginning of this section. We apply the degree reduction of the second step $\log\log(n)$ times, to get a scheme with smaller total share size.

Theorem 3.12. *Let $G = (V, E)$ be the complete graph and $E^* \subset E$ such that $|E^*| \leq n^{1+\beta}$, where $0 \leq \beta < \frac{1}{2}$. Then, there is a secret-sharing scheme such that: (1) each edge in $E \setminus E^*$ can reconstruct the secret, (2) each edge in E^* cannot learn any information about the secret, and (3) the total share size of the scheme is $O(n^{7/6+2\beta/3})$.*

3.4 Constructions for Arbitrary Graphs When Removing Few Edges

In the following theorem, we realize the graph obtained from an arbitrary graph G when removing few edges from it. We first share the secret using the 2-out-of-2 scheme. We share the first share using the scheme of the graph G and share the second share using the scheme of the graph G^*, which is the complement of the graph of the removed edges.

Theorem 3.13. *Let $G = (V, E)$ be a graph and $E^* \subset E$ such that $|E^*| \leq n^{1+\beta}$, where $0 \leq \beta < \frac{1}{2}$. Furthermore, assume that the forbidden graph access structure of G can be realized by a scheme in which the total share size is m. Then, there is a secret-sharing scheme such that: (1) each edge in $G \cap G^* = (V, E \setminus E^*)$ can reconstruct the secret, (2) each edge in $\overline{E} \cup E^*$ cannot learn any information about the secret, and (3) the total share size of the scheme is $O(m + n^{7/6+2\beta/3})$.*

Proof. Let s be the secret, and let s_1, s_2 be random strings such that $s = s_1 \oplus s_2$ (i.e., s_1 is chosen with uniform distribution and $s_2 = s_1 \oplus s$). We independently share s_1 using the scheme of the graph G with total share size m.

The graph $G^* = (V, \overline{E^*})$ is a dense graph, in which the number of edges in its complement is $|E^*| \leq n^{1+\beta}$, where $0 \leq \beta < \frac{1}{2}$. Hence, by Theorem 3.12, we can realize the graph G^* such that: (1) every edge not in E^* can reconstruct the secret, (2) every edge in E^* cannot learn any information about the secret, and (3) the total share size of the scheme is $O(n^{7/6+2\beta/3})$. We share s_2 using the scheme of the graph G^* with total share size $O(n^{7/6+2\beta/3})$. Combining, the total share size of the scheme is $O(m + n^{7/6+2\beta/3})$.

For an edge $e \in E \setminus E^* = E \cap \overline{E^*}$, since $e \in E$, the edge e can reconstruct s_1 from the scheme of G, and since $e \in \overline{E^*}$, the edge e can reconstruct s_2 from the scheme of G^*, and, hence, the edge e can reconstruct the secret s by performing bitwise-xor between the strings s_1 and s_2.

For an edge $e \in \overline{E} \cup E^*$, if $e \in \overline{E}$, the edge e cannot learn any information on s_1 from the scheme of G, and cannot reconstruct the secret s. Otherwise $e \in E^*$, and the edge e cannot learn any information on s_2 from the scheme of G^*. Hence, the edge e cannot learn any information on the secret s. □

Remark 3.14. The last scheme does not realize graph access structures. Indeed, every independent set in $G \cap G^*$ which contains an edge e_1 from E^* and an edge e_2 from $\overline{E}$ can reconstruct the secret, because the edge e_1 can reconstruct s_1 and the edge e_2 can reconstruct s_2, and together they can reconstruct the secret s.

Additionally, any improvement of the total share size of the scheme presented in Theorem 3.12 will lead to an improvement of the total share size of the scheme for a general graph G when removing few edges from it, for $m = o(n^{7/6+2\beta/3})$, where m is the total share size of a scheme in which each edge in G can reconstruct the secret, and each edge not in G cannot learn any information about the secret.

4 Using Avoiding Covers to Realize Graph Access Structures

In this section, we define avoiding covers and show how to use them to realize graphs obtained by removing few edges from an arbitrary graph, such that the degree of the graph which contains the removed edges is bounded. Avoiding covers are a special kind of covers by complete bipartite graphs that are used to reach the following goal. We want to realize a graph obtained by removing few edges from an arbitrary graph G. For that, we want to use a cover by complete bipartite graphs of the complete graph without the removed edges from the graph G (i.e., every edge between the parts in each graph in the cover is not a removed edge).

We would like to realize every graph in the cover by the scheme of the graph G restricted to the vertices of the graph. Notice that the graph G might contain edges between vertices in the same part; such edges would be able to reconstruct the secret. However, if one of the graphs in the cover contains removed edges between vertices in the same part, then they can reconstruct the secret although these edges are unauthorized sets and should not learn any information about the secret.

Thus, for a graph $G = (V, E)$ and a set $F \subset V$, we want to find a cover of the bipartite graph G_F (defined in Definition 2.5) by complete bipartite graphs such that there are no edges of $\overline{G}$ between any two vertices in the same part of each complete bipartite graph in the cover. We next define avoiding covers, which have this property.

Definition 4.1 (Avoiding λ-Covers by Complete Bipartite Graphs). *Let $G = (V, E)$ be a graph and $F \subset V$. A complete bipartite λ-cover $G_1 = (U_1, V_1, E_1), \ldots, G_r = (U_r, V_r, E_r)$ of G_F avoids $\overline{E}$ if $\overline{E} \cap ((U_i \times U_i) \cup (V_i \times V_i)) = \emptyset$ for every $1 \leq i \leq r$, that is, there are no edges of $\overline{G}$ between any two vertices in the same part of any G_i. A complete bipartite $\overline{E}$-avoiding cover of G_F is a complete bipartite $\overline{E}$-avoiding 1-cover of G_F.*

We show in the following claim the use of avoiding covers in our constructions.

Claim 4.2. *Let $G = (V, E)$ be a graph that can be realized by a scheme in which the total share size is m, and let $E^* \subset E$. Let $F \subset V$ be a set satisfying that there is an E^*-avoiding cover of G_F^* by complete bipartite graphs such that each vertex $v \in V$ is in at most μ graphs of the cover. Then, there is a secret-sharing scheme such that: (1) each edge in $G \cap G_F^*$ can reconstruct the secret, (2) every independent set in $G \cap G^*$ cannot learn any information on the secret (we do not care if the edges in $E \setminus E^*$ and not in G_F^* can learn information on the secret), and (3) the total share size is at most μm.*

For a graph G and a set of vertices F, the next lemma proves the existence of a small avoiding cover of the bipartite graph G_F when the degree of every vertex in its complement $\overline{G}$ is bounded by d. In this cover the number of graphs

is $O(d^2 \log(n))$, compared to $O(d \ln(n))$ graphs of the complete bipartite cover presented in [33]. However, each vertex in the cover we construct appears in $O(d \log(n))$ graphs of the cover. This makes this cover equivalent to the complete bipartite cover when comparing the total share size of the secret-sharing scheme in which we share the secret independently for each graph of the cover.

Lemma 4.3. *Let $G = (V, E)$ be a graph such that the degree of each vertex in $\overline{G}$ is bounded by $d > 1$ and $F \subset V$. Then, there is a $\log(n)$-cover of size $r = O(d^2 \log(n))$ of G_F by complete bipartite graphs that avoids $\overline{E}$ such that every vertex $v \in V$ appears in $O(d \log(n))$ graphs of the cover.*

Theorem 4.4. *Let $G = (V, E)$ be a graph that can be realized by a scheme with total share size m, and let $E^* \subset E$. If the degree of each vertex in $\overline{G^*}$ is bounded by d, then $G \cap G^*$ can be realized by a scheme in which the total share size is $\tilde{O}(dm)$.*

Remark 4.5. The degree in $\overline{G^*}$ is bounded by d, so by [5, Lemma 5.2] there exists an equivalence $\ln(n)$-cover, and in particular an equivalence cover of G^* with $O(d \ln(n))$ equivalence graphs. For every equivalence graph in the cover, and for every clique in it, we can share the secret among the vertices in the clique using the scheme of the graph G with total share size m. The edges that can reconstruct the secret are the edges of $E \setminus E^*$, and every independent set in $G \cap G^*$ cannot learn any information on the secret. The total share size of realizing each graph of the equivalence cover is m and the total share of the resulting scheme (realizing all the graphs of the cover) is $O(dm \ln(n)) = \tilde{O}(dm)$, slightly better than the above theorem. Using Stinson's technique [43], if the secret size is $\Omega(\log^2(n))$, then the total share size of the scheme realizing $G \cap G^*$ from Theorem 4.4 is $O(dm)$, which improves the total share size of the scheme from [5].

In the full version of this paper, we prove the following theorem, using avoiding covers and adapting techniques from [5].

Theorem 4.6. *Let $G = (V, E)$ be a graph that can be realized by a scheme with total share size m, let $E^* \subset E$ with $|E^*| \leq n^{1+\beta}$ and $0 \leq \beta < 1$, and let $c = \chi(\overline{G^*})$. If $c < \frac{n^{1-\beta/2}}{m^{1/2}}$, then $G \cap G^*$ can be realized by a scheme in which the total share size is $\tilde{O}(m^{2/3} n^{2/3+2\beta/3} c^{1/3})$.*

References

1. Alon, N.: Covering graphs by the minimum number of equivalence relations. Combinatorica **6**(3), 201–206 (1986)
2. Babai, L., Gál, A., Wigderson, A.: Superpolynomial lower bounds for monotone span programs. Combinatorica **19**(3), 301–319 (1999)
3. Beimel, A.: Secret-sharing schemes: a survey. In: Chee, Y.M., Guo, Z., Ling, S., Shao, F., Tang, Y., Wang, H., Xing, C. (eds.) IWCC 2011. LNCS, vol. 6639, pp. 11–46. Springer, Heidelberg (2011)

4. Beimel, A., Chor, B.: Universally ideal secret-sharing schemes. IEEE Trans. Inf. Theor. **40**(3), 786–794 (1994)
5. Beimel, A., Farràs, O., Mintz, Y.: Secret-sharing schemes for very dense graphs. J. Cryptol. **29**(2), 336–362 (2016)
6. Beimel, A., Gál, A., Paterson, M.: Lower bounds for monotone span programs. Comput. Complex. **6**(1), 29–45 (1997)
7. Beimel, A., Ishai, Y., Kumaresan, R., Kushilevitz, E.: On the cryptographic complexity of the worst functions. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 317–342. Springer, Heidelberg (2014)
8. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for noncryptographic fault-tolerant distributed computations. In: Proceedings of the 20th ACM Symposium on the Theory of Computing, pp. 1–10 (1988)
9. Benaloh, J.C., Leichter, J.: Generalized secret sharing and monotone functions. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 27–35. Springer, Heidelberg (1990)
10. Bertilsson, M., Ingemarsson, I.: A construction of practical secret sharing schemes using linear block codes. In: Zheng, Y., Seberry, J. (eds.) AUSCRYPT 1992. LNCS, vol. 718, pp. 67–79. Springer, Heidelberg (1993)
11. Blakley, G.R.: Safeguarding cryptographic keys. In: Proceedings of the 1979 AFIPS National Computer Conference, AFIPS Conference proceedings, vol. 48, pp. 313–317. AFIPS Press (1979)
12. Blundo, C., De Santis, A., de Simone, R., Vaccaro, U.: Tight bounds on the information rate of secret sharing schemes. Des. Codes Crypt. **11**(2), 107–122 (1997)
13. Blundo, C., De Santis, A., Stinson, D.R., Vaccaro, U.: Graph decomposition and secret sharing schemes. J. Cryptol. **8**(1), 39–64 (1995)
14. Brickell, E.F.: Some ideal secret sharing schemes. J. Combin. Math. Combin. Comput. **6**, 105–113 (1989)
15. Brickell, E.F., Davenport, D.M.: On the classification of ideal secret sharing schemes. J. Cryptol. **4**(73), 123–134 (1991)
16. Bublitz, S.: Decomposition of graphs and monotone formula size of homogeneous functions. Acta Inf. **23**(6), 689–696 (1986)
17. Capocelli, R.M., De Santis, A., Gargano, L., Vaccaro, U.: On the size of shares for secret sharing schemes. J. Cryptol. **6**(3), 157–168 (1993)
18. Chaum, D., Crépeau, C., Damgård, I.: Multiparty unconditionally secure protocols. In: Proceedings of the 20th ACM Symposium on the Theory of Computing, pp. 11–19 (1988)
19. Chor, B., Kushilevitz, E.: Secret sharing over infinite domains. J. Cryptol. **6**(2), 87–96 (1993)
20. Cook, S.A., Pitassi, T., Robere, R., Rossman, B.: Exponential lower bounds for monotone span programs. Electron. Colloq. Comput. Complex. **23**, 64 (2016). www.eccc.uni-trier.de/eccc/
21. Csirmaz, L.: The dealer's random bits in perfect secret sharing schemes. Studia Sci. Math. Hungar. **32**(3–4), 429–437 (1996)
22. Csirmaz, L.: The size of a share must be large. J. Cryptol. **10**(4), 223–231 (1997)
23. Csirmaz, L.: Secret sharing schemes on graphs. Technical report 2005/059, Cryptology ePrint Archive (2005). eprint.iacr.org/
24. Desmedt, Y.G., Frankel, Y.: Shared generation of authenticators and signatures. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 457–469. Springer, Heidelberg (1992)
25. van Dijk, M.: On the information rate of perfect secret sharing schemes. Des. Codes Crypt. **6**(2), 143–169 (1995)

26. Erdös, P., Pyber, L.: Covering a graph by complete bipartite graphs. Discrete Math. **170**(1–3), 249–251 (1997)
27. Gál, A.: A characterization of span program size and improved lower bounds for monotone span programs. In: Proceedings of the 30th ACM Symposium on the Theory of Computing, pp. 429–437 (1998)
28. Gál, A., Pudlák, P.: Monotone complexity and the rank of matrices. Inform. Process. Lett. **87**, 321–326 (2003)
29. Gay, R., Kerenidis, I., Wee, H.: Communication complexity of conditional disclosure of secrets and attribute-based encryption. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9216, pp. 485–502. Springer, Heidelberg (2015)
30. Gertner, Y., Ishai, Y., Kushilevitz, E., Malkin, T.: Protecting data privacy in private information retrieval schemes. J. Comput. Syst. Sci. **60**(3), 592–629 (2000)
31. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM conference on Computer and Communications Security, pp. 89–98 (2006)
32. Ito, M., Saito, A., Nishizeki, T.: Secret sharing schemes realizing general access structure. In: Proceedings of the IEEE Global Telecommunication Conference, Globecom, vol. 87, pp. 99–102 (1987). Journal version: Multiple assignment scheme for sharing secret. J. Cryptol. **6**(1), 15–20 (1993)
33. Jukna, S.: On set intersection representations of graphs. J. Graph Theor. **61**(1), 55–75 (2009)
34. Karchmer, M., Wigderson, A.: On span programs. In: Proceedings of the 8th IEEE Structure in Complexity Theory, pp. 102–111 (1993)
35. Martí-Farré, J., Padró, C.: Secret sharing schemes on sparse homogeneous access structures with rank three. Electr. J. Comb. **11**(1) (2004). http://www.combinatorics.org/ojs/index.php/eljc/article/view/v11i1r72/
36. Martí-Farré, J., Padró, C.: On secret sharing schemes, matroids and polymatroids. J. Math. Cryptol. **4**(2), 95–120 (2010)
37. Mintz, Y.: Information ratios of graph secret-sharing schemes. Master's thesis, Department of Computer Science, Ben Gurion University (2012)
38. Naor, M., Wool, A.: Access control and signatures via quorum secret sharing. In: 3rd ACM Conference on Computer and Communications Security, pp. 157–167 (1996)
39. Padró, C., Sáez, G.: Lower bounds on the information rate of secret sharing schemes with homogeneous access structure. Inform. Process. Lett. **83**(6), 345–351 (2002)
40. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)
41. Shamir, A.: How to share a secret. Commun. ACM **22**, 612–613 (1979)
42. Shankar, B., Srinathan, K., Rangan, C.P.: Alternative protocols for generalized oblivious transfer. In: Rao, S., Chatterjee, M., Jayanti, P., Murthy, C.S.R., Saha, S.K. (eds.) ICDCN 2008. LNCS, vol. 4904, pp. 304–309. Springer, Heidelberg (2008)
43. Stinson, D.R.: Decomposition construction for secret sharing schemes. IEEE Trans. Inf. Theor. **40**(1), 118–125 (1994)
44. Sun, H., Shieh, S.: Secret sharing in graph-based prohibited structures. In: Proceedings IEEE INFOCOM 1997, pp. 718–724 (1997)
45. Tassa, T.: Generalized oblivious transfer by secret sharing. Des. Codes Crypt. **58**(1), 11–21 (2011)
46. Waters, B.: Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 53–70. Springer, Heidelberg (2011)