Linear Secret-Sharing Schemes for Forbidden Graph Access Structures*

Amos Beimel[1], Oriol Farràs[2], Yuval Mintz[1], and Naty Peter[1]

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

Abstract. A secret-sharing scheme realizes the forbidden graph access structure determined by a graph $G = (V, E)$ if a pair of vertices can reconstruct the secret if and only if it is an edge in G. Secret-sharing schemes for forbidden graph access structures of bipartite graphs are equivalent to conditional disclosure of secrets protocols, a primitive that is used to construct attributed-based encryption schemes.

We study the complexity of realizing a forbidden graph access structure by linear secret-sharing schemes. A secret-sharing scheme is linear if the reconstruction of the secret from the shares is a linear mapping. In many applications of secret-sharing, it is required that the scheme will be linear. 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 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 its forbidden graph access structure in which the total size of the shares is $\tilde{O}(n^{1+\beta/2})$. We provide an additional construction showing that every dense graph with n vertices and at least $\binom{n}{2} - n^{1+\beta}$ edges can be realized by a linear secret-sharing scheme with the same total share size.

We provide lower bounds on the share size of linear secret-sharing schemes realizing forbidden graph access structures. We prove that for most forbidden graph access structures, the total share size of every linear secret-sharing scheme realizing these access structures is $\Omega(n^{3/2})$, which 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 of every linear secret-sharing scheme realizing these forbidden graph access structures is $\Omega(n^{1+\beta/2})$. This shows that our constructions are optimal (up to poly-logarithmic factors).

Key words. Secret-sharing, share size, monotone span program, conditional disclosure of secrets.

* 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 European Union through H2020-ICT-2014-1-644024 and H2020-DS-2015-1-700540, and by the Spanish Government through TIN2014-57364-C2-1-R.

1 Introduction

A secret-sharing scheme, introduced by [14, 43, 35], 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 [11, 21, 23], threshold cryptography [27], access control [41], attribute-based encryption [34, 48], and oblivious transfer [44, 47].

In this paper we study secret-sharing schemes for forbidden graph access structures, first introduced by Sun and Shieh [46]. The forbidden graph access structure determined by a graph $G = (V, E)$ is the collection of 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 [7, 8], 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 the shares are a linear function 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 which introduced by Karchmer and Wigderson [37], and every linear secret-sharing scheme implies a monotone span program. See [4], 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 will be linear. For example, Cramer, Damgård, and Maurer [23] construct general secure multiparty computation protocols, i.e., protocols which are secure against an arbitrary adversarial structure, from any linear secret-sharing scheme realizing the access structure in which a set is authorized if and only if it is not in the adversarial structure. Furthermore, it was shown by Attrapadung [3] and Wee [49] that linear secret-sharing schemes realizing forbidden graphs access structures are a central ingredient for constructing public-key (multi-user) attribute-based encryption. These applications motivate the study in this paper of linear secret-sharing schemes for forbidden graph access structures.

1.1 Related Work

Secret-Sharing Schemes for Arbitrary Access Structures. Secret-sharing schemes were introduced by Shamir [43] and Blakley [14] for the threshold case, and by Ito, Saito, and Nishizeki [35] 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 [14, 43]. 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 parties) share size [12, 13, 17, 37]. In particular, Benaloh and Leichter [12] 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 [37] 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 schemes for general access structures (e.g., [35, 13, 17, 37]) are highly inefficient, i.e., they have total share size of $2^{O(n)}$ (where n is the number of parties). The best known lower bound on the total share size of secret-sharing schemes realizing an access structure is $\Omega(n^2/\log n)$ [25, 24]; this lower bound is very far from the upper bound.

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 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 total size of the shares is $O(n^2/\log n)$ [29, 19]. Graph access structures have been studied in many works, such as [20, 18, 45, 16, 15, 9, 26, 7, 8]. In particular, Beimel, Farràs, and Mintz [7] 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 $\tilde{O}(n^{5/4+3\beta/4})$.

Forbidden Graph Access Structures. Gay, Kerenidis, and Wee [32] have proved that every forbidden graph access structure can be realized by a linear secret-sharing scheme in which the total size of the shares is $O(n^{3/2})$. Liu, Vaikuntanathan, and Wee [38] have recently shown that every forbidden graph access structure can be realized by a *non-linear* secret-sharing scheme in which the total size of the shares is $n^{1+o(1)}$.

Beimel, Farràs, and Peter [8] showed that any 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 in which the total share size is $O(n^{7/6+2\beta/3})$. They also showed that if less than $n^{1+\beta}$ 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 in which the total share size is $O(m + n^{7/6+2\beta/3})$. These results are improved in this paper.

Secret-sharing schemes for graph access structures and forbidden graph access structures have similar requirements, however, the requirements for graph access structures are stronger, since in graph access structures independent sets of vertices should not get any information on the secret. Given a secret-sharing scheme for a graph access structure, we can construct a secret-sharing scheme

for the forbidden graph access structure: We can independently share the secret using the scheme for the graph access structure and the 3-out-of-n scheme of Shamir [43]. 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.

Conditional Disclosure of Secrets. Gertner et al. [33] defined conditional disclosure of secrets (CDS). In this problem, 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. In [33], CDS is used to efficiently realize symmetrically-private information retrieval protocols. In [32], it is shown that CDS can be used to construct attribute-based encryption, a cryptographic primitive introduced in [34, 42].

We can represent the CDS for some predicate 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 Alice is a vertex in the first part of the graph and every possible input for 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 construct a secret-sharing scheme realizing the bipartite graph defined by the predicate in which the share of 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. Thus, given a predicate P, we get a bipartite graph with $n = 2^N$ vertices in each part (where N is the size of the input of the parties) such that the length of the messages required in a CDS for P is the length of the shares required by a secret-sharing realizing the forbidden graph access structure.

Gertner et al. [33] have proved that if a predicate P has a (possibly non-monotone) formula of size S, then there is a CDS protocol for P in which the length of the messages is S. A similar result holds if the predicate has a (possibly non-monotone) span program, or even a non-monotone secret-sharing scheme (this is a secret-sharing scheme realizing an access structure defined in [33] in which for every bit in the input there are two parties, one for every value of the bit). This result provides a rich class of predicates for which there are efficient CDS protocols. Thus, there is a rich class of forbidden graph access structures that can be realized by efficient secret-sharing schemes (by the equivalence between CDS and secret-sharing schemes for forbidden graph access structures).

It was shown in [32] 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

$2^{N/2}$.[3] This implies that for every bipartite graph there exists a linear secret-sharing scheme realizing the 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. [38] have recently shown that every predicate has a non-linear CDS scheme 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 [10, 8], the above two results hold for every graph (not necessarily bipartite).

Applebaum et al. [2] and Ambrona et al. [1] have shown that if we have a linear CDS for some predicate P with message length c and shared random string length r, then we can construct a linear CDS for the complement predicate $\overline{P}$ in which the message length and the shared random string length is linear in c and r. Translated to secret-sharing, we conclude 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 $O(r)$.

Another result shown in [2] is that for every predicate there exists a linear CDS for secrets of k bits, 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 $O(k \cdot N)$. This gives us an amortized size of $O(N)$ bits per each bit of the secret, much better than the size of $2^{N/2}$ for one-bit secret that was shown in [32]. When considering forbidden graph access structures, we get that for every forbidden bipartite graph access structure with n vertices there exists a linear secret-sharing scheme with secrets of length k and total share size of $O(kn \log n)$, provided that the size of the secret k is exponential in n.

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.

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 that realizes its forbidden graph access structure, in which the total size of the shares is

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

$\tilde{O}(n^{1+\beta/2})$. 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 that realizes its forbidden graph access structure 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 [8], which has total share size $O(n^{7/6+2\beta/3})$.
- As a corollary, we construct a secret-sharing scheme for forbidden graph access structures of graphs obtained by changing (adding or removing) few edges from an arbitrary graph G. If the forbidden graph access structure determined by a graph G can be realized by a secret-sharing scheme with total share size m and G' is obtained from G by changing at most $n^{1+\beta}$ edges, for some $0 \leq \beta < 1$, then we construct a secret-sharing scheme realizing the forbidden graph access structure of G' with total share size $m + \tilde{O}(n^{1+\beta/2})$. If the secret-sharing scheme realizing the forbidden graph access structure determined by G is linear, then the resulting scheme realizing the forbidden graph access structure determined by G' is also linear.

Overview of Our Constructions. We construct the secret-sharing scheme realizing forbidden graph access structures determined by sparse graphs in few stages, where in each stage we restrict the forbidden graph access structures that we can realize. 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 forbidden graph access structure for 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 construct 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 $(a, b) \in E$. The total size of the shares in the scheme we construct 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 for a forbidden graph access structure for a bipartite graph $G = (A, B, E)$, where the degree of every vertex in B is at most d (and there is no restriction that A is small). The total size of the shares in this scheme is $O(n\sqrt{d}\log n)$, where $|A| = |B| = n$. The idea of this construction is to *randomly* partition the set A to $\ell = O(\sqrt{d}\ln n) = \tilde{O}(\sqrt{d})$ "small" sets $A_1, \ldots, A_\ell$. 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 $O(\sqrt{d})$ (compared to its degree in

G, which can be at most d). We now 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 the number of edges in G is at most $n^{1+\beta}$ 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 [7] (also used in [8]). Fix some degree d, and let B_{big} be the vertices in B whose degree is at least d. Furthermore, 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 [32] (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 $\tilde{O}(n^{1+\beta/2})$. The last stage is done using a generic transformation of [10, 8], 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 [7], however, it requires designing appropriate secret-sharing schemes in the first two stages. In the last stage, we use a transformation of [10, 8] as a black-box. The construction for forbidden graph access structures determine by dense graphs is similar, however, we construct a different scheme for the first stage.

The construction of a scheme realizing a forbidden graph access structure determined by a graph G' obtained by adding or removing few edges from a graph G is done using ideas from [8] as follows: 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 $n^{1+\beta}$ 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 the scheme of the graph G 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 $n^{1+\beta}$ from G).

Lower Bounds. We prove that for most forbidden graph access structures, the total share size of every linear secret-sharing scheme realizing these access structures, with a one-bit secret, is $\Omega(n^{3/2})$, which shows that the construction of Gay et al. [32] 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 [38], and the total share size required in linear secret-sharing schemes realizing forbidden graph access structures. This lower bound implies that, for most predicates $P : \{0,1\}^N \times \{0,1\}^N \to \{0,1\}$, in every linear CDS protocol for P the length of the messages is $\Omega(2^{N/2})$.

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 of every linear secret-sharing scheme realizing their forbidden graph access structures is $\Omega(n^{1+\beta/2})$. This shows 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 [39].

2 Preliminaries

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

We present the definition of secret-sharing scheme as given in [22, 6]. For more information about this definition and secret-sharing in general, see [5].

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 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 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, 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.*

2.2 Monotone Span Programs

Monotone span programs (abbreviated MSPs) are a linear-algebraic model of computation introduced by Karchmer and Wigderson [37]. As explained below in Claim 2.4, MSPs over finite fields are equivalent to linear secret-sharing schemes.

Definition 2.3 (Monotone Span Programs [37]). *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,*[4] *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 where $\widehat{M}$ 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).

[4] We label a row by a party rather than by a variable x_j as done in [37].

Claim 2.4 ([37, 4]). *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 proof of the privacy of this scheme can be found in [37, 5].

2.3 Graphs and 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.* [5]

Remark 2.7. 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.

Remark 2.8. In applications of secret-sharing schemes for forbidden graph access structures (e.g., conditional disclosure of secrets), the only requirement is that pairs of vertices can reconstruct the secret if and only if they are connected by an edge. To fully specify the access structure of a forbidden graph, we also require

[5] In [46], the access structure is specified by the complement graph, i.e., by the edges that are forbidden from learning information on the secret.

that all sets of 3 or more vertices are authorized. This additional requirement only slightly increases 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 [43], 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 construction in Sections 3 to 5 we implicitly assume that we share the secret using Shamir's 3-out-of-n secret-sharing scheme.

2.4 Conditional Disclosure of Secrets

For completeness, we present the definition of conditional disclosure of secrets, originaly defined in [33].

Definition 2.9 (Conditional Disclosure of Secrets). *Let* $P : \{0,1\}^N \times \{0,1\}^N \to \{0,1\}$ *be some 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 the 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 predicate* P *if the following two requirements hold:*

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

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

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

3 The Basic Construction for Graphs of Low Degree

Our basic construction requires the following construction of linear spaces, which will be used both for sparse graphs and 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 $\{(X-\alpha_i), (X^2 - \alpha_i \cdot X), \ldots, (X^d - \alpha_i \cdot X^{d-1})\}$. Since these d polynomials are 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 $\alpha_i \in \{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{d'}}\}$ if and only if $(a_i, b_j) \in E$.

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

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 $A = \{a_1, \ldots, a_m\}$, $B = \{b_1, \ldots, b_n\}$, and let $V_1, \ldots, V_m$ and $\mathbf{z_1}, \ldots, \mathbf{z_n}$ be the linear subspaces and vectors guaranteed by Claim 3.1. 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 $\{\mathbf{v_{i,1}}, \ldots, \mathbf{v_{i,d}}\}$ be a basis of V_i, and for $1 \leq \ell \leq d$, define $\mathbf{v'_{i,\ell}} = (0, 0, \mathbf{v_{i,\ell}})$ (that is, $\mathbf{v'_{i,\ell}}$ is a vector in $\mathbb{F}^{d+3}$ whose first two coordinates are 0 followed by the vector $\mathbf{v_{i,\ell}}$). The rows labeled by a_i are $\mathbf{v'_{i,1}}, \ldots, \mathbf{v'_{i,d}}$ and $(0, 1, 0, \ldots, 0)$. The row labeled by b_j is $\mathbf{z'_j} = (1, 0, \mathbf{z_j})$. The target vector is $(1, 1, 0, \ldots, 0)$. The monotone span program accepts (a_i, b_j) if and only if $(1, 1, 0, \ldots, 0) \in \operatorname{span}\left\{\mathbf{z'_j}, \mathbf{v'_{i,1}}, \ldots, \mathbf{v'_{i,d}}, (0, 1, 0, \ldots, 0)\right\}$ if and only if $\mathbf{z_j} \in \operatorname{span}\{\mathbf{v_{i,1}}, \ldots, \mathbf{v_{i,d}}\}$ if and only if $\mathbf{z_j} \in V_i$ 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. □

We next 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 linear secret-sharing scheme of [32]. This construction is presented as a warmup for our construction for bipartite graphs with bounded degree.

Lemma 3.3. *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 $(A_i, B, E \cap (A_i \times B))$ (in which every vertex in B has at most $|A_i| = \sqrt{n}$ neighbors) can be realized by a linear secret-sharing scheme with total share size $O(n + (\sqrt{n}+1)\sqrt{n}) = O(n)$. 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 Lemma 3.3, the size of the share of each vertex is $O(n^{1/2})$.

4 Secret-Sharing Schemes for Sparse Graphs

In this section we present efficient secret-sharing schemes for forbidden graph access structures of sparse graphs, that is, graphs with at most $n^{1+\beta}$ 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 an efficient secret-sharing schemes for sparse bipartite graphs. In the construction for a sparse 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, that is, 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 [7, 8]. 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 [10], we use the schemes for sparse bipartite graphs to construct a scheme for general sparse 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 for some $d \leq n$. If $d|B| \geq n \log^2 n$, then there is a linear secret-sharing scheme realizing G with total share size $O\left(\sqrt{n|B|d} \log n\right)$.*

Proof. Let $\delta = \log_n d$ (that is, $d = n^\delta$), $\gamma = \log_n |B|$ (i.e., $|B| = n^\gamma$), and

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

and denote $\ell = 2n^{1-\alpha} \ln n$. 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.

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

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 vector $\mathbf{z} = (z_t)_{t\neq j}$, let

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

By convention, if $\Pr[Z_t = z_t \text{ for all } t \neq j] = 0$, 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 the upper bound on the degree of b given in the lemma. Observe that the last inequality follows because $n^{1/2} \leq n^{\delta/2+\gamma/2}/\log n$, and so

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

obtaining that $n - n^\alpha \geq n/2$.

The random variables $Z'_1, \ldots, Z'_{n^\alpha}$ are defined as follows: Let $z_1, \ldots, z_n$ be the values given to $Z_1, \ldots, Z_n$. 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, $\Pr[Z'_j = 1 | Z_t = z_t \text{ for all } t \neq j] = 2/n^{1-\delta}$. Therefore, Z'_j is independent of $(Z_t)_{t\neq j}$, and, hence, independent of $(Z'_t)_{t\neq j}$.

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 [40, Theorem 4.4, (4.3)], we obtain

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

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

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

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 will be

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

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 $O(n^{1/2+\gamma/2+\delta/2} \log n)$. □

The following theorem is a special case of the above lemma, when $|A| = |B|$. In the proof of Theorem 4.3 below, we also use Lemma 4.1.

Theorem 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 for some $d \leq n$. Then, there is a linear secret-sharing scheme realizing G in which the share size of each vertex is $O(\sqrt{d} \log n)$. The total share size of this scheme is $O(n\sqrt{d} \log n)$.*

Proof. If $d < \log^2 n$, we use the trivial secret-sharing scheme, where we share the secret independently for each edge; in this scheme the share size of each vertex is $O(d) = O(\sqrt{d} \log n)$, and the total share size is $O(n\sqrt{d} \log n)$.

Otherwise, $d \geq \log^2 n$, and let $\delta = \log_n d$, $\ell = 2n^{\delta/2} \ln n$, and $A_1, \ldots, A_\ell \subset A$ be the sets of size $n^{1-\delta/2}$ guarantied from Lemma 4.1 (taking $\gamma = 1$). 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). Note that the sets still satisfy the two desired properties.

Next, as in Lemma 4.1, we construct a secret-sharing scheme for each bipartite graph $G_i = (A_i, B, E \cap (A_i \times B))$ (for $1 \leq i \leq \ell$) using the scheme of Lemma 3.2. The degree of each vertex in B in the graph G_i is at most $12n^{\delta/2} = O(\sqrt{d})$. 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 $\ell = O(\sqrt{d} \log n)$. Every vertex in A participates in one scheme, and gets a share of size $12n^{\delta/2} + 1 = O(\sqrt{d})$ in this scheme. Overall, the share size of each vertex in the resulting scheme is $O(\sqrt{d} \log n)$, and the total share size is $O(n\sqrt{d} \log n)$. □

Theorem 4.3. *Let $G = (A, B, E)$ be a bipartite graph with $|A| = |B| = n$ and with at most $n^{1+\beta}$ edges, for some constant $0 \leq \beta < 1$. Then, there is a linear secret-sharing scheme realizing G with total share size $O(n^{1+\beta/2} \log^2 n)$.*

Proof. If $n^\beta \leq \log^2 n$, we use the trivial secret-sharing scheme, where we share the secret independently for each edge; in this scheme the total share size is $O(n^{1+\beta}) = O(n^{1+\beta/2} \log n)$.

We next deal with the interesting case where $n^\beta > \log^2 n$. In this case, we partition the vertices in B according to their degree, that is, for $i = 0, \ldots, (1 - \beta) \log n - 1$, define

$$B_i = \left\{ b \in B : \frac{n}{2^{i+1}} < \deg(b) \leq \frac{n}{2^i} \right\}$$

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

We realize each graph G_i, for $i = 0, \ldots, (1 - \beta) \log n - 1$, 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 $n/2^{i+1}$, the number of vertices in B_i is at most $\frac{n^{1+\beta}}{n/2^{i+1}} = 2^{i+1} n^\beta$. By adding dummy vertices to B_i with degree 0, we can assume that $|B_i| = 2^{i+1} n^\beta$. By Lemma 4.1, there is a secret-sharing scheme realizing the forbidden graph access structure of G_i with total share size $O(\sqrt{n \cdot 2^{i+1} n^\beta \cdot n/2^i} \cdot \log n) = O(n^{1+\beta/2} \log n)$. Note that, as required in Lemma 4.1, $d|B_i| = n/2^i \cdot 2^{i+1} n^\beta \geq n \log^2 n$.

Finally, we realize $(A, B_{\text{small}}, E \cap (A \times B_{\text{small}}))$ using the secret-sharing scheme of Theorem 4.2; the total share size of this scheme is $O(n^{1+\beta/2} \log n)$ as well. Since we use $1 + (1 - \beta) \log n$ schemes, the total share size of the resulting scheme is $O(n^{1+\beta/2} \log^2 n)$. □

Theorem 4.4. *Let $G = (V, E)$ be a graph with n vertices and with at most $n^{1+\beta}$ edges for some constant $0 \leq \beta < 1$. Then, there is a linear secret-sharing scheme realizing G with total share size $O(n^{1+\beta/2} \log^3 n)$.*

Proof. To simplify notation, assume that n is a power of 2. As in [10], we cover G by $\log n$ bipartite graphs, each graph having at most $n^{1+\beta}$ 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 Secret-Sharing Schemes for Dense Graphs

In this section we study forbidden graph access structures of dense graphs. The main result of this section is Theorem 5.5, where for every dense graph we present a linear secret-sharing scheme realizing its forbidden graph access structure. For sparse graphs, we designed a general construction starting from a basic secret-sharing scheme, described in Lemma 3.2. For dense graphs, we follow the same strategy, replacing the basic construction with a different scheme, given in Lemma 5.1.

Lemma 5.1. *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 span $\{\mathbf{z_j}, \mathbf{v_{i,1}}, \ldots, \mathbf{v_{i,d}}\}$ is 1 plus the dimension of V_i, i.e., span $\{\mathbf{z_j}, \mathbf{v_{i,1}}, \ldots, \mathbf{v_{i,d}}\} = \mathbb{F}^{d+1}$, and in particular,

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

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 $\mathbf{w} \notin \text{span}\left\{\mathbf{z_j}, \mathbf{v_{i,1}}, \ldots, \mathbf{v_{i,d}}\right\} = V_i$. 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. □

Lemma 5.2. *Let $G = (A, B, E)$ be a bipartite graph with $|A| = n$, $|B| \leq n$, and let $\overline{G} = (A, B, \overline{E})$ be the bipartite complement of G. If the degree of B in $\overline{G}$ is at most d, for some d satisfying $d \leq n$ and $d|B| \geq n \log^2 n$, then there is a linear secret-sharing scheme realizing G with total share size $O(\sqrt{n|B|d} \log n)$.*

Proof. We use the techniques presented in the proof of Lemma 4.1. We take $\delta = \log_n d$, $\gamma = \log_n |B|$, $\alpha = \frac{1}{2} + \frac{\gamma}{2} - \frac{\delta}{2}$, and $\ell = 2n^{1-\alpha} \ln n$. By the proof of Lemma 4.1, there exist sets $A_1, \ldots, A_\ell \subset A$ of size n^α that satisfy:

(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 $\overline{G}_i = (A_i, B, \overline{E} \cap (A_i \times B))$ is at most $12n^{\alpha+\delta-1}$.

Then, we construct a secret-sharing scheme for each bipartite graph $G_i = (A_i, B, E \cap (A_i \times B))$ using Lemma 5.1. The degree of each vertex in B in the graph G_i is at least $|A_i| - 12n^{\alpha+\delta-1}$, so the total share size will be

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

□

Theorem 5.3. *Let $G = (A, B, E)$ be a bipartite graph such that $|A| = |B| = n$ and 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 $O(\sqrt{d} \log n)$. The total share size of this scheme is $O(n\sqrt{d} \log n)$.*

Proof. If $d < \log^2 n$, we use the construction in [8, Lemma 3.8]; in this scheme the share size of each vertex is $O(d) = O(\sqrt{d} \log n)$, and the total share size is $O(n\sqrt{d} \log n)$.[6]

Otherwise, $d \geq \log^2 n$, and let $\delta = \log_n d$, $\ell = 2n^{\delta/2} \ln n$, and $A_1, \ldots, A_\ell \subset A$ be the sets of size $n^{1-\delta/2}$ guarantied from Lemma 5.2 (taking $\gamma = 1$). As in Theorem 4.2, we can assume that each vertex in A is a member of exactly one set, and the sets still satisfy the two desired properties.

Next, as in Lemma 5.2, we construct a secret-sharing scheme for each bipartite graph $G_i = (A_i, B, E \cap (A_i \times B))$ (for $1 \leq i \leq \ell$) using the scheme of Lemma 5.1. The degree of each vertex in B in the bipartite complement of G_i is at most $12n^{\delta/2} = O(\sqrt{d})$. Every vertex in B participates in ℓ schemes, and gets a share of size two in each of these schemes. Hence, the share size of every vertex in B is $2\ell = O(\sqrt{d} \log n)$. Every vertex in A participates in one scheme, and gets a share of size $12n^{\delta/2} + 1 = O(\sqrt{d})$ in this scheme. Overall, the share size of each vertex in the resulting scheme is $O(\sqrt{d} \log n)$, and the total share size is $O(n\sqrt{d} \log n)$. □

Theorem 5.4. *Let $G = (A, B, E)$ be a bipartite graph with $|A| = |B| = n$ such that its bipartite complement $\overline{G} = (A, B, \overline{E})$ has at most $n^{1+\beta}$ edges, for some constant $0 \leq \beta < 1$. Then, there is a linear secret-sharing scheme realizing G with total share size $O(n^{1+\beta/2} \log^2 n)$.*

Proof. As in the proof of Theorem 4.3, for $i = 0, \ldots, (1-\beta) \log n - 1$, define $B_i = \left\{b \in B : \frac{n}{2^{i+1}} < \deg_{\overline{G}}(b) \leq \frac{n}{2^i}\right\}$ and $B_{\text{small}} = \left\{b \in B : \deg_{\overline{G}}(b) \leq n^{\beta}\right\}$.

For every $0 \leq i \leq (1-\beta) \log n - 1$, we use Lemma 5.2 to construct a secret-sharing scheme realizing the graph $(A, B_i, E \cap (A \times B_i))$; the total share size of

[6] in [8, Lemma 3.8], it is only stated that the total share size in the scheme is $O(nd)$, however, in their scheme the size of the share of each vertex is $O(d)$.

this scheme is $O(\sqrt{n \cdot 2^{i+1} n^{\beta} \cdot n/2^i} \cdot \log n) = O(n^{1+\beta/2} \log n)$. Finally, we realize $(A, B_{\text{small}}, E \cap (A \times B_{\text{small}}))$ using the secret-sharing scheme of Theorem 5.3; the total share size of this scheme is $O(n^{1+\beta/2} \log n)$ as well. Since we use $1 + (1 - \beta) \log n$ schemes, the total share size of the resulting scheme is $O(n^{1+\beta/2} \log^2 n)$. □

Theorem 5.5. *Let $G = (V, E)$ be a graph with n vertices and with at least $\binom{n}{2} - n^{1+\beta}$ edges, for some constant $0 \leq \beta < 1$. Then, there is a secret-sharing scheme realizing G with total share size $O(n^{1+\beta/2} \log^3 n)$.*

Proof. For every $1 \leq t \leq \log n$, we define the bipartite graph $H_t = (A_t, B_t, F_t)$ as in Theorem 4.4. The bipartite complements of these bipartite graphs have at most $n^{1+\beta}$ edges. By Theorem 5.4, each such bipartite graph admits a secret-sharing scheme with total share size $O(n^{1+\beta/2} \log^2 n)$. The total share size of the resulting scheme is $O(n^{1+\beta/2} \log^3 n)$. □

We use Theorem 4.4 and Theorem 5.5 to show that the total share sizes required to realize two graphs that differ in a few edges is close.

Corollary 5.6. *Let $G = (V, E)$ be a graph with n vertices that can be realized by a secret-sharing scheme in which the total share size is m, and let G' be a graph obtained from G by adding and removing $n^{1+\beta}$ edges, for some constant $0 \leq \beta < 1$. Then, there is a secret-sharing scheme realizing G' with total share size $O(m + n^{1+\beta/2} \log^3 n)$.*

Proof. 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 $G' = (V, (E \setminus E') \cup E'')$ and $|E'|, |E''| \leq n^{1+\beta}$. First, we share the secret s using the secret-sharing scheme of Theorem 4.4 realizing the sparse graph (V, E'') with total share size $O(n^{1+\beta/2} \log^3 n)$. Next, we independently share the secret s using a 2-out-of-2 secret-sharing scheme. I.e., let s_1, s_2 be two random elements such that $s = s_1 \oplus s_2$ (i.e., s_1 is chosen at random and $s_2 = s_1 \oplus s$). We independently share s_1 using the scheme realizing G with total share size m, and share s_2 using the secret-sharing scheme of Theorem 5.5 realizing the dense graph $(V, \overline{E'})$ (note that $|\overline{E'}| \geq \binom{n}{2} - n^{1+\beta}$) with total share size $O(n^{1+\beta/2} \log^3 n)$. The total share size of the resulting scheme is $O(m + n^{1+\beta/2} \log^3 n)$.

For an edge e in the graph G', if $e \in E''$, then it can reconstruct the secret using the scheme of Theorem 4.4 realizing (V, E''), and if $e \in E \setminus E' = E \cap \overline{E'}$, then it can reconstruct s_1 using the scheme realizing G and can reconstruct s_2 using the scheme of Theorem 5.5 realizing $(V, \overline{E'})$, and, hence, can reconstruct the secret s.

For an edge e not in the graph G', if $e \in E'$, then it cannot get information on the secret s from the scheme realizing (V, E'') (since $E'' \cap E' = \emptyset$, which implies that $e \notin E''$), and it cannot learn information on s_2 from the scheme realizing $(V, \overline{E'})$, and, hence, it cannot get information on the secret s from the 2-out-of-2 scheme. Otherwise, if $e \in \overline{E \cup E''}$, then it cannot get information on the secret s from the scheme realizing (V, E'') (since $e \notin E''$), and it cannot

learn information on s_1 from the scheme realizing G (since $e \notin E$), and, hence, it cannot get information on the secret s from the 2-out-of-2 scheme. □

6 Lower Bounds for Linear Secret-Sharing Schemes

In this section, we prove that for most 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 most 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 show 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 most 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 would enable us to use a counting argument that will yield tight lower bounds on the size of MSPs accepting forbidden graph access structures. Such dual's were studied in many papers, e.g., [36, 31, 28, 30].

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 $|P| = n$),

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

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 [31]. 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'.[7] □

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.

[7] 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 Counting Monotone Span Programs with Small Max Share Size

We next compute the number of access structures of rank r that have an MSP such that each party labels at most s rows and prove that there are at most $2^{O(rns^2 \log q)}$ such access structures.

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

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

□

Theorem 6.7 bounds the number of MSPs over a given finite field. We use this result to give a lower bound on the share size in sharing a one-bit secret for forbidden graph access structures by a linear secret-sharing schemes over all finite fields.

Theorem 6.8. *For most 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. 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 $\sqrt{n}$, it must be that $q \leq 2^{\sqrt{n}}$ (otherwise, every share contains at least $\sqrt{n}$ bits), and, furthermore, $s \log q \leq \sqrt{n}$.

We next bound the number of forbidden graph access structures that can be realized by a secret-sharing scheme with max share size at most θ. Recall that

in forbidden graph access structures all sets of size 3 are authorized. On one hand, by Theorem 6.7, the number of forbidden graph access structures Γ, each one of them has rank at most 3, with n parties and $\rho_q(\Gamma) \leq \theta/\log q$, is at most $2^{6n(\theta/\log q)^2 \log q} < 2^{6n\theta^2}$. Since we are counting linear schemes, we need to sum the number of the MSPs for every possible finite field (there are at most $2^{\sqrt{n}}$ such fields, because $q \leq 2^{\sqrt{n}}$). Consider the MSPs for which the max share size in the secret-sharing schemes defined by the MSPs is at most $\theta < \sqrt{n}$. The number of such MSPs is at most $2^{\sqrt{n}} \cdot 2^{6n\theta^2} \ll 2^{7n\theta^2}$. On the other hand, the number of graphs is $2^{\binom{n}{2}} \approx 2^{n^2/2}$. Thus, if half of the forbidden graph access structures have a linear secret-sharing scheme with max share size θ, then $2^{7n\theta^2} > \frac{1}{2} \cdot 2^{n^2/2}$, i.e., $\theta = \Omega(\sqrt{n})$. □

Since CDS protocols are equivalent to secret-sharing schemes for forbidden graph access structures, we get the following corollary.

Corollary 6.9. *For most functions $f : \{0,1\}^N \times \{0,1\}^N \to \{0,1\}$, the communication complexity of every linear conditional disclosure of secrets protocol for f is $\Omega(2^{N/2})$.*

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 θ for such forbidden graph access structures has to satisfy $n\theta^2 > \Omega(n^{1+\beta}\log n)$, i.e., $\theta = \Omega(n^{\beta/2}\sqrt{\log n})$.

6.3 Counting Monotone Span Programs with Small Total Share Size

Theorem 6.7 counts the number of rank r access structures with $\rho_q(\Gamma) \leq s$. The total share size of access structures with max share size s can still be small, i.e., $n + s$. Next, we count the number of forbidden graph access structures with MSPs of size at most S.

Theorem 6.10. *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 $\text{size}_q(\Gamma) \leq S$ 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 $\text{size}(\widehat{M}) \leq S$. 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 $\text{size}_q(\Gamma) \leq S$. 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,[8] 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 6.11. *For most 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 $\text{size}_q(\widehat{M}) = S$, 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 6.10, the number of forbidden graph access structures Γ with n parties and $\text{size}_q(\Gamma) \leq \Theta/\log q$ is at most

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

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

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

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

On the other hand, the number of graphs is $2^{\binom{n}{2}} \approx 2^{n^2/2}$. Thus, if half of 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 6.10 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 6.10 dominates the number of sparse graphs. To prove lower bounds for sparse forbidden graph access structures, we use an idea from [7].

Corollary 6.12. *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 6.11, 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 6.11 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 part, 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 6.13. *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 $\mathrm{size}_q(\Gamma) \leq S$ is at most*

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

Proof. The proof is similar to the proof of Theorem 6.10, i.e., given an MSP of size S, we find a set B of size at most $n/4$ containing all parties such that each one of these parties labels more than $4S/n$ 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.,

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

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

$$\binom{n}{n/4} \cdot 2^{(1-(3/4)^r)\binom{n}{r}} \cdot 2^{2r(3n/4)(4S/n)^2 \log q} =$$

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

□

We conclude that for most rank r access structures with n parties, the size of the shares in every linear secret-sharing scheme realizing the access structure with a one-bit secret is $\Omega(n^{(r+1)/2})$.

References

1. Ambrona, M., Barthe, G., Schmidt, B.: Generic transformations of predicate encodings: Constructions and applications. In: Katz, J., Shacham, H. (eds.) Advances in Cryptology – CRYPTO 2017. LNCS, vol. 10401, pp. 36–66. Springer-Verlag (2017)
2. Applebaum, B., Arkis, B., Raykov, P., Vasudevan, P.N.: Conditional disclosure of secrets: Amplification, closure, amortization, lower-bounds, and separations. In: Katz, J., Shacham, H. (eds.) Advances in Cryptology – CRYPTO 2017. LNCS, vol. 10401, pp. 727–757. Springer-Verlag (2017)
3. Attrapadung, N.: Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In: Nguyen, P.Q., Oswald, E. (eds.) Advances in Cryptology – EUROCRYPT 2014. LNCS, vol. 8441, pp. 557–577. Springer-Verlag (2014)
4. Beimel, A.: Secure Schemes for Secret Sharing and Key Distribution. Ph.D. thesis, Technion (1996), www.cs.bgu.ac.il/ beimel/pub.html
5. Beimel, A.: Secret-sharing schemes: A survey. In: Chee, Y.M., Guo, Z., Ling, S., Shao, F., Tang, Y., Wang, H., Xing, C. (eds.) Coding and Cryptology – Third International Workshop, IWCC 2011. LNCS, vol. 6639, pp. 11–46. Springer-Verlag (2011)
6. Beimel, A., Chor, B.: Universally ideal secret sharing schemes. IEEE Trans. on Information Theory 40(3), 786–794 (1994)
7. Beimel, A., Farràs, O., Mintz, Y.: Secret-sharing schemes for very dense graphs. J. of Cryptology 29(2), 336–362 (2016)
8. Beimel, A., Farràs, O., Peter, N.: Secret sharing schemes for dense forbidden graphs. In: Security and Cryptography for Networks – 10th International Conference, SCN 2016. LNCS, vol. 9841, pp. 509–528. Springer-Verlag (2016)

9. Beimel, A., Gál, A., Paterson, M.: Lower bounds for monotone span programs. Computational Complexity 6(1), 29–45 (1997)
10. Beimel, A., Ishai, Y., Kumaresan, R., Kushilevitz, E.: On the cryptographic complexity of the worst functions. In: Proc. of the Eleventh Theory of Cryptography Conference – TCC 2014. LNCS, vol. 8349, pp. 317–342. Springer-Verlag (2014)
11. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for noncryptographic fault-tolerant distributed computations. In: Proc. of the 20th ACM Symp. on the Theory of Computing. pp. 1–10 (1988)
12. Benaloh, J., Leichter, J.: Generalized secret sharing and monotone functions. In: Advances in Cryptology – CRYPTO '88. LNCS, vol. 403, pp. 27–35. Springer-Verlag (1990)
13. Bertilsson, M., Ingemarsson, I.: A construction of practical secret sharing schemes using linear block codes. In: AUSCRYPT '92. LNCS, vol. 718, pp. 67–79. Springer-Verlag (1993)
14. Blakley, G.R.: Safeguarding cryptographic keys. In: Proc. of the 1979 AFIPS National Computer Conference. AFIPS Conference proceedings, vol. 48, pp. 313–317. AFIPS Press (1979)
15. Blundo, C., De Santis, A., de Simone, R., Vaccaro, U.: Tight bounds on the information rate of secret sharing schemes. Designs, Codes and Cryptography 11(2), 107–122 (1997)
16. Blundo, C., De Santis, A., Stinson, D.R., Vaccaro, U.: Graph decomposition and secret sharing schemes. J. of Cryptology 8(1), 39–64 (1995)
17. Brickell, E.F.: Some ideal secret sharing schemes. Journal of Combin. Math. and Combin. Comput. 6, 105–113 (1989)
18. Brickell, E.F., Davenport, D.M.: On the classification of ideal secret sharing schemes. J. of Cryptology 4(73), 123–134 (1991)
19. Bublitz, S.: Decomposition of graphs and monotone formula size of homogeneous functions. Acta Inf. 23(6), 689–696 (1986)
20. Capocelli, R.M., De Santis, A., Gargano, L., Vaccaro, U.: On the size of shares for secret sharing schemes. J. of Cryptology 6(3), 157–168 (1993)
21. Chaum, D., Crépeau, C., Damgård, I.: Multiparty unconditionally secure protocols. In: Proc. of the 20th ACM Symp. on the Theory of Computing. pp. 11–19 (1988)
22. Chor, B., Kushilevitz, E.: Secret sharing over infinite domains. J. of Cryptology 6(2), 87–96 (1993)
23. Cramer, R., Damgård, I., Maurer, U.: General secure multi-party computation from any linear secret-sharing scheme. In: Advances in Cryptology – EUROCRYPT 2000. LNCS, vol. 1807, pp. 316–334. Springer-Verlag (2000)
24. Csirmaz, L.: The dealer's random bits in perfect secret sharing schemes. Studia Sci. Math. Hungar. 32(3–4), 429–437 (1996)
25. Csirmaz, L.: The size of a share must be large. J. of Cryptology 10(4), 223–231 (1997)
26. Csirmaz, L.: Secret sharing schemes on graphs. Tech. Rep. 2005/059, Cryptology ePrint Archive (2005), eprint.iacr.org/
27. Desmedt, Y., Frankel, Y.: Shared generation of authenticators and signatures. In: Advances in Cryptology – CRYPTO '91. LNCS, vol. 576, pp. 457–469. Springer-Verlag (1992)
28. Dijk, M.v., Jackson, W., Martin, K.M.: A note on duality in linear secret sharing schemes. Bull. of the Institute of Combinatorics and its Applications 19, 98–101 (1997)
29. Erdös, P., Pyber, L.: Covering a graph by complete bipartite graphs. Discrete Mathematics 170(1–3), 249–251 (1997)

30. Fehr, S.: Efficient construction of the dual span program (1999), manuscript
31. Gál, A.: Combinatorial Methods in Boolean Function Complexity. Ph.D. thesis, U. of Chicago (1995), also: www.eccc.uni-trier.de/eccc-local/ECCC-Theses/gal.html
32. Gay, R., Kerenidis, I., Wee, H.: Communication complexity of conditional disclosure of secrets and attribute-based encryption. In: Advances in Cryptology – CRYPTO 2015. LNCS, vol. 9216, pp. 485–502. Springer-Verlag (2015)
33. Gertner, Y., Ishai, Y., Kushilevitz, E., Malkin, T.: Protecting data privacy in private information retrieval schemes. J. of Computer and System Sciences 60(3), 592–629 (2000)
34. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proc. of the 13th ACM conference on Computer and communications security. pp. 89–98 (2006)
35. Ito, M., Saito, A., Nishizeki, T.: Secret sharing schemes realizing general access structure. In: Proc. of the IEEE Global Telecommunication Conf., Globecom 87. pp. 99–102 (1987), Journal version: Multiple assignment scheme for sharing secret. J. of Cryptology 6(1), 15-20, (1993).
36. Jackson, W., Martin, K.M.: Geometric secret sharing schemes and their duals. In: Designs, Codes and Cryptography. vol. 4, pp. 83–95 (1994)
37. Karchmer, M., Wigderson, A.: On span programs. In: Proc. of the 8th IEEE Structure in Complexity Theory. pp. 102–111 (1993)
38. Liu, T., Vaikuntanathan, V., Wee, H.: Conditional disclosure of secrets via non-linear reconstruction. In: Katz, J., Shacham, H. (eds.) Advances in Cryptology – CRYPTO 2017. LNCS, vol. 10401, pp. 758–790. Springer-Verlag (2017)
39. Mintz, Y.: Information ratios of graph secret-sharing schemes. Master's thesis, Dept. of Computer Science, Ben Gurion University (2012)
40. Mitzenmacher, M., Upfal, E.: Probability and Computing. Cambridge University Press (2005)
41. Naor, M., Wool, A.: Access control and signatures via quorum secret sharing. In: 3rd ACM Conf. on Computer and Communications Security. pp. 157–167 (1996)
42. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Advances in Cryptology – EUROCRYPT 2005. pp. 457–473. Springer-Verlag (2005)
43. Shamir, A.: How to share a secret. Communications of the ACM 22, 612–613 (1979)
44. Shankar, B., Srinathan, K., Rangan, C.P.: Alternative protocols for generalized oblivious transfer. In: Proc. of ICDCN 2008. LNCS, vol. 4904, pp. 304–309. Springer-Verlag (2008)
45. Stinson, D.R.: Decomposition construction for secret sharing schemes. IEEE Trans. on Information Theory 40(1), 118–125 (1994)
46. Sun, H., Shieh, S.: Secret sharing in graph-based prohibited structures. In: Proceedings IEEE INFOCOM '97. pp. 718–724 (1997)
47. Tassa, T.: Generalized oblivious transfer by secret sharing. Designs, Codes and Cryptography 58(1), 11–21 (2011)
48. Waters, B.: Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) Public Key Cryptography – PKC 2011. LNCS, vol. 6571, pp. 53–70. Springer-Verlag (2011)
49. Wee, H.: Dual system encryption via predicate encodings. In: Lindell, Y. (ed.) Proc. of the Eleventh Theory of Cryptography Conference – TCC 2014. LNCS, vol. 8349, pp. 616–637. Springer-Verlag (2014)