SECRET SHARING SCHEMES FOR VERY DENSE GRAPHS

AMOS BEIMEL[1] **ORIOL FARRÀS**[2] YUVAL MINTZ[1]

[1]Ben-Gurion University of the Negev, Israel
[2]Universitat Rovira i Virgili, Spain

CRYPTO 2012

Program

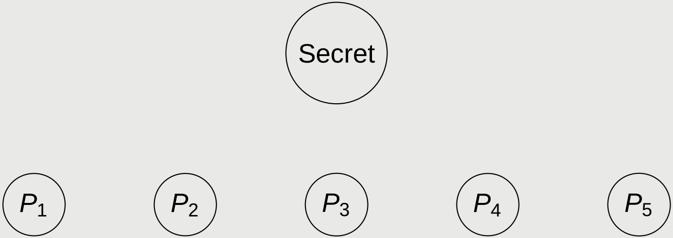
1. Introduction to Secret Sharing
2. Graph Secret Sharing
3. Our Results

1. Introduction to Secret Sharing
2. Graph Secret Sharing
3. Our Results

A method to protect a secret

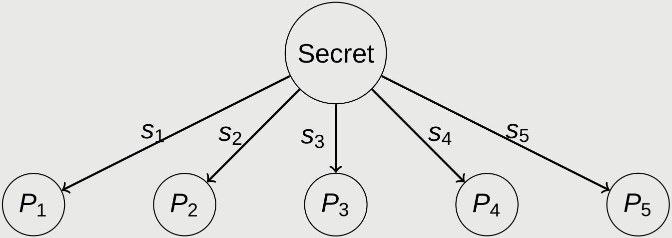
Secret Sharing Scheme

A method to protect a secret



Secret Sharing Scheme

A method to protect a secret

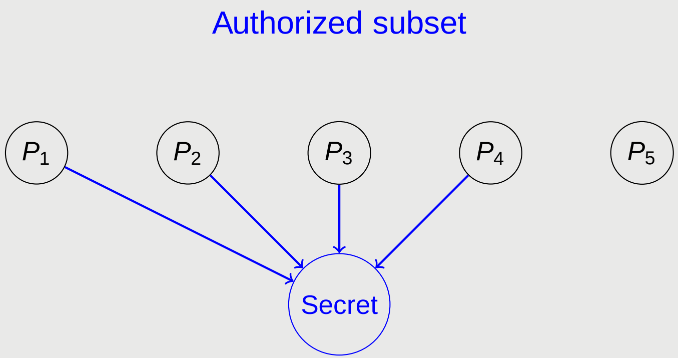


Secret Sharing Scheme

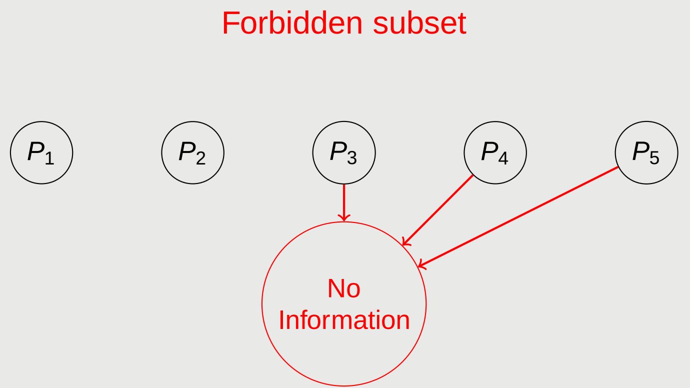
A method to protect a secret

Secret Sharing Scheme

A method to protect a secret



A method to protect a secret



Secret Sharing Scheme

A method to protect a secret

Access structure: Family of authorized subsets

P_1 P_2 P_3 P_4 P_5

Secret Sharing Schemes: Overview

- Shamir ('79), Blakley ('79), Ito, Saito, and Nishizeki ('87).

Secret Sharing Schemes: Overview

- Shamir ('79), Blakley ('79), Ito, Saito, and Nishizeki ('87).
- Unconditionally secure.

Secret Sharing Schemes: Overview

- Shamir ('79), Blakley ('79), Ito, Saito, and Nishizeki ('87).
- Unconditionally secure.
- Perfect schemes: subsets not in the access structure are forbidden.

Secret Sharing Schemes: Overview

- Shamir ('79), Blakley ('79), Ito, Saito, and Nishizeki ('87).
- Unconditionally secure.
- Perfect schemes: subsets not in the access structure are forbidden.

Cryptographic primitive with many applications

- Multiparty computation
- Threshold cryptography
- Access control
- Attribute-based encryption
- Oblivious transfer
- ...

Secret Sharing Schemes: Overview

- Shamir ('79), Blakley ('79), Ito, Saito, and Nishizeki ('87).
- Unconditionally secure.
- Perfect schemes: subsets not in the access structure are forbidden.

Cryptographic primitive with many applications

- Multiparty computation
- Threshold cryptography
- Access control
- Attribute-based encryption
- Oblivious transfer
- ...

Need of efficient schemes: Shares have to be small.

On the Share Size

As a measure of efficiency we use

$$\textcolor{red}{\text{total share size}}\text{:}\ \frac{\text{sum size of shares}}{\text{size of secret}} = \frac{\sum \log |S_i|}{\log |S|}$$

On the Share Size

As a measure of efficiency we use

$$\text{total share size: } \frac{\text{sum size of shares}}{\text{size of secret}} = \frac{\sum \log |S_i|}{\log |S|}$$

There exist efficient schemes for certain access structures.

On the Share Size

As a measure of efficiency we use

$$\text{total share size: } \frac{\text{sum size of shares}}{\text{size of secret}} = \frac{\sum \log |S_i|}{\log |S|}$$

There exist efficient schemes for certain access structures.

- e.g., threshold a.s. with n participants admits schemes with t.s.s. n (Shamir'79, Blakley'79).

On the Share Size

As a measure of efficiency we use

$$\text{total share size: } \frac{\text{sum size of shares}}{\text{size of secret}} = \frac{\sum \log |S_i|}{\log |S|}$$

There exist efficient schemes for certain access structures.

- e.g., threshold a.s. with n participants admits schemes with t.s.s. n (Shamir'79, Blakley'79).
- Schemes with total share size n are called ideal.

On the Share Size

As a measure of efficiency we use

$$\text{total share size: } \frac{\text{sum size of shares}}{\text{size of secret}} = \frac{\sum \log |S_i|}{\log |S|}$$

There exist efficient schemes for certain access structures.

- e.g., threshold a.s. with n participants admits schemes with t.s.s. n (Shamir'79, Blakley'79).
- Schemes with total share size n are called ideal.

... but which is the most efficient scheme for an access structure?

On the Share Size

As a measure of efficiency we use

$$\text{total share size: } \frac{\text{sum size of shares}}{\text{size of secret}} = \frac{\sum \log|S_i|}{\log|S|}$$

There exist efficient schemes for certain access structures.

- e.g., threshold a.s. with n participants admits schemes with t.s.s. n (Shamir'79, Blakley'79).
- Schemes with total share size n are called ideal.

... but which is the most efficient scheme for an access structure?

There are methods to construct schemes for every access structure...
(Benaloh and Leichter'88, Simmons et al'91, Brickell'89, Karchmer and Wigderson'93)

On the Share Size

As a measure of efficiency we use

$$\text{total share size: } \frac{\text{sum size of shares}}{\text{size of secret}} = \frac{\sum \log |S_i|}{\log |S|}$$

There exist efficient schemes for certain access structures.

- e.g., threshold a.s. with n participants admits schemes with t.s.s. n (Shamir'79, Blakley'79).
- Schemes with total share size n are called ideal.

... but which is the most efficient scheme for an access structure?

There are methods to construct schemes for every access structure...
(Benaloh and Leichter'88, Simmons et al'91, Brickell'89, Karchmer and Wigderson'93)
but in general are innefficient.

On the Share Size

As a measure of efficiency we use

$$\text{total share size: } \frac{\text{sum size of shares}}{\text{size of secret}} = \frac{\sum \log |S_i|}{\log |S|}$$

There exist efficient schemes for certain access structures.

- e.g., threshold a.s. with n participants admits schemes with t.s.s. n (Shamir'79, Blakley'79).
- Schemes with total share size n are called ideal.

... but which is the most efficient scheme for an access structure?

There are methods to construct schemes for every access structure...
(Benaloh and Leichter'88, Simmons et al'91, Brickell'89, Karchmer and Wigderson'93)
but in general are innefficient.

For most access structures, the t.s.s of these schemes is $2^{O(n)}$.

On the Share Size (II)

In general, the best upper bound on the t.s.s of the best scheme for an access structure is $2^{O(n)}$.

On the Share Size (II)

In general, the best upper bound on the t.s.s of the best scheme for an access structure is $2^{O(n)}$.

Lower Bounds:

There is a family of access structures for which the t.s.s. of any scheme is

$$\Omega(n^2/\log n)$$

(Csirmaz'97)

This is the best known lower bound for sharing a secret with respect to an access structure.

On the Share Size (II)

In general, the best upper bound on the t.s.s of the best scheme for an access structure is $2^{O(n)}$.

Lower Bounds:

There is a family of access structures for which the t.s.s. of any scheme is

$$\Omega(n^2 / \log n)$$

(Csirmaz'97)

This is the best known lower bound for sharing a secret with respect to an access structure.

Open Problem: BRIDGE THIS HUGE GAP

Our Results

Open Problem: BRIDGE THE GAP

Our Results

Open Problem: BRIDGE THE GAP

Open problem: Which access structures are HARD?
i.e. which access structures require large shares to be realized?

Our Results

Open Problem: BRIDGE THE GAP

Open problem: Which access structures are HARD?
i.e. which access structures require large shares to be realized?

We study these problems for GRAPH ACCESS STRUCTURES.

Our Results

Open Problem: BRIDGE THE GAP

Open problem: Which access structures are HARD?
i.e. which access structures require large shares to be realized?

We study these problems for GRAPH ACCESS STRUCTURES.

We find new UPPER AND LOWER BOUNDS for the t.s.s.

Our Results

Open Problem: BRIDGE THE GAP

Open problem: Which access structures are HARD?
i.e. which access structures require large shares to be realized?

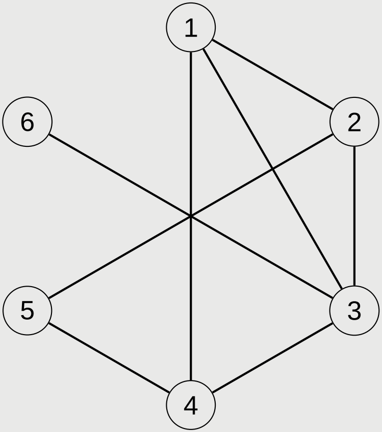
We study these problems for GRAPH ACCESS STRUCTURES.

We find new UPPER AND LOWER BOUNDS for the t.s.s.

We extend the techniques for finding upper bounds to

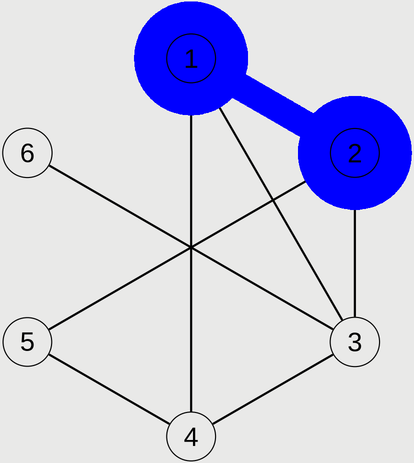
- homogeneous access structures
- the general case

Graph Secret Sharing



An access structure is a graph access structure if the minimal authorized subsets are of size two.
It defines a graph.

Graph Secret Sharing

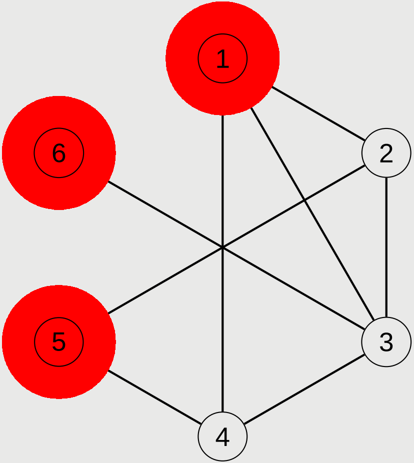


An access structure is a graph access structure if the minimal authorized subsets are of size two.
It defines a graph.

A set is authorized if contains an edge:

$$\{1, 2\}$$

Graph Secret Sharing

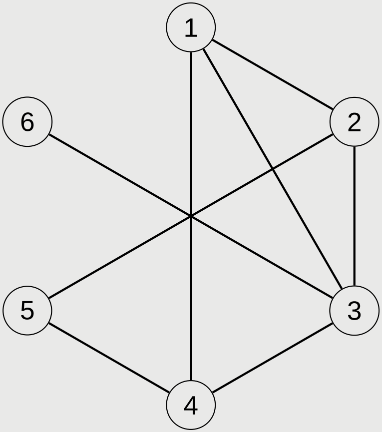


An access structure is a graph access structure if the minimal authorized subsets are of size two.
It defines a graph.

A set is forbidden if does not contain any edge:

$$\{1, 5, 6\}$$

Graph Secret Sharing



An access structure is a graph access structure if the minimal authorized subsets are of size two.
It defines a graph.

A graph secret sharing scheme is a scheme with graph access structure.

Graph Secret Sharing: Previous Results

Graph secret sharing schemes:

Graph Secret Sharing: Previous Results

Graph secret sharing schemes:

- All minimal authorized subsets are of size two.

Graph Secret Sharing: Previous Results

Graph secret sharing schemes:

- All minimal authorized subsets are of size two.
- Simple but interesting case.

Graph Secret Sharing: Previous Results

Graph secret sharing schemes:

- All minimal authorized subsets are of size two.
- Simple but interesting case.
- Studied in many previous works.

Graph Secret Sharing: Previous Results

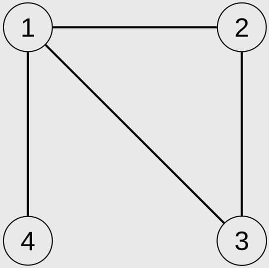
Graph secret sharing schemes:

- All minimal authorized subsets are of size two.
- Simple but interesting case.
- Studied in many previous works.
- First step for obtaining general results.

Graph Secret Sharing: Previous Results

Graph secret sharing schemes:

- All minimal authorized subsets are of size two.
- Simple but interesting case.
- Studied in many previous works.
- First step for obtaining general results.



Simple construction for any graph:

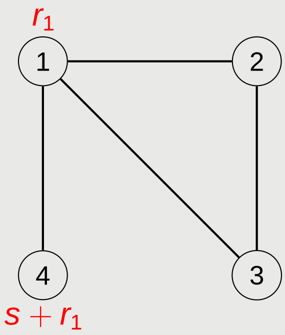
The secret s is shared independently for every edge.

The total share size is $2m$, where m is the number of edges.

Graph Secret Sharing: Previous Results

Graph secret sharing schemes:

- All minimal authorized subsets are of size two.
- Simple but interesting case.
- Studied in many previous works.
- First step for obtaining general results.



Simple construction for any graph:

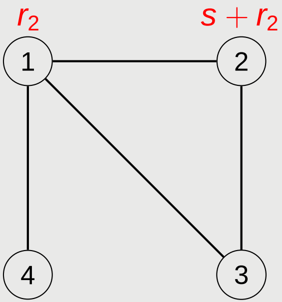
The secret s is shared independently for every edge.

The total share size is $2m$, where m is the number of edges.

Graph Secret Sharing: Previous Results

Graph secret sharing schemes:

- All minimal authorized subsets are of size two.
- Simple but interesting case.
- Studied in many previous works.
- First step for obtaining general results.



Simple construction for any graph:

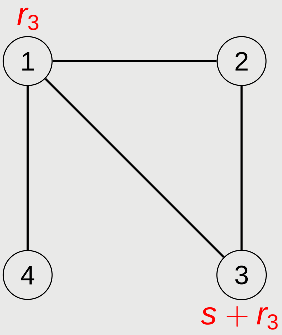
The secret s is shared independently for every edge.

The total share size is $2m$, where m is the number of edges.

Graph Secret Sharing: Previous Results

Graph secret sharing schemes:

- All minimal authorized subsets are of size two.
- Simple but interesting case.
- Studied in many previous works.
- First step for obtaining general results.



Simple construction for any graph:

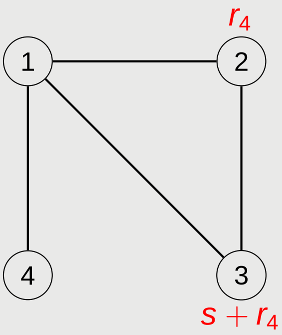
The secret s is shared independently for every edge.

The total share size is $2m$, where m is the number of edges.

Graph Secret Sharing: Previous Results

Graph secret sharing schemes:

- All minimal authorized subsets are of size two.
- Simple but interesting case.
- Studied in many previous works.
- First step for obtaining general results.

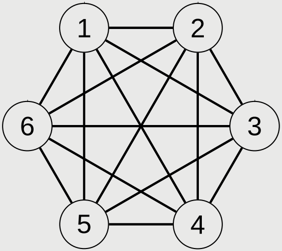


Simple construction for any graph:

The secret s is shared independently for every edge.

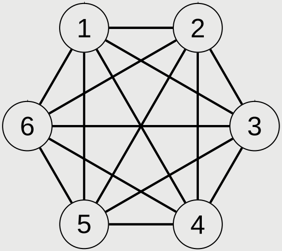
The total share size is $2m$, where m is the number of edges.

Graphs with Ideal Schemes



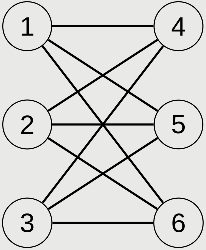
Clique:
It defines threshold access structure of threshold 2.

Graphs with Ideal Schemes

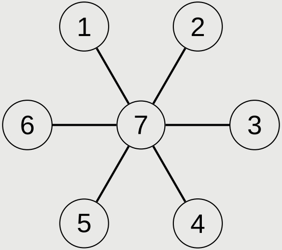


Clique:
It defines threshold access structure of threshold 2.

Complete Bipartite Graph



Star



Bounds on the Total Share Size

The total share size of the best scheme realizing a graph access structure is upper bounded by

Bounds on the Total Share Size

The total share size of the best scheme realizing a graph access structure is upper bounded by

- $O(m)$, where m is the number of edges

Bounds on the Total Share Size

The total share size of the best scheme realizing a graph access structure is upper bounded by

- $O(m)$, where m is the number of edges
- $O(n^2/\log n)$

Bounds on the Total Share Size

The total share size of the best scheme realizing a graph access structure is upper bounded by

- $O(m)$, where m is the number of edges
- $O(n^2/\log n)$
  (Bublitz'86, Blundo et al.'96, Erdös and Pyber'97)

Bounds on the Total Share Size

The total share size of the best scheme realizing a graph access structure is upper bounded by

- $O(m)$, where m is the number of edges
- $O(n^2/\log n)$
  (Bublitz'86, Blundo et al.'96, Erdös and Pyber'97)

Lower bounds:

Bounds on the Total Share Size

The total share size of the best scheme realizing a graph access structure is upper bounded by

- $O(m)$, where m is the number of edges
- $O(n^2 / \log n)$
  (Bublitz'86, Blundo et al.'96, Erdös and Pyber'97)

Lower bounds:

- There exists a family of access structures for which the total share size of the schemes realizing them is $\Omega(n \log n)$

Bounds on the Total Share Size

The total share size of the best scheme realizing a graph access structure is upper bounded by

- $O(m)$, where m is the number of edges
- $O(n^2/\log n)$
  (Bublitz'86, Blundo et al.'96, Erdös and Pyber'97)

Lower bounds:

- There exists a family of access structures for which the total share size of the schemes realizing them is $\Omega(n \log n)$
  (van Dijk'95, Blundo et al.'97, Csirmaz'05).

Bounds on the Total Share Size

The total share size of the best scheme realizing a graph access structure is upper bounded by

- $O(m)$, where m is the number of edges
- $O(n^2/\log n)$
  (Bublitz'86, Blundo et al.'96, Erdös and Pyber'97)

Lower bounds:

- There exists a family of access structures for which the total share size of the schemes realizing them is $\Omega(n \log n)$
  (van Dijk'95, Blundo et al.'97, Csirmaz'05).
- There exists a family of access structures for which the total share size of the linear schemes realizing them is $\Omega(n^{3/2})$

Bounds on the Total Share Size

The total share size of the best scheme realizing a graph access structure is upper bounded by

- $O(m)$, where m is the number of edges
- $O(n^2/\log n)$
  (Bublitz'86, Blundo et al.'96, Erdös and Pyber'97)

Lower bounds:

- There exists a family of access structures for which the total share size of the schemes realizing them is $\Omega(n \log n)$
  (van Dijk'95, Blundo et al.'97, Csirmaz'05).
- There exists a family of access structures for which the total share size of the linear schemes realizing them is $\Omega(n^{3/2})$
  (Beimel et al.'97).

Motivation of Our Work

To BRIDGE THE GAP between upper and lower bounds on the total share size for graph access structures.

Motivation of Our Work

To BRIDGE THE GAP between upper and lower bounds on the total share size for graph access structures.

We look for EFFICIENT constructions for graphs.

Motivation of Our Work

To BRIDGE THE GAP between upper and lower bounds on the total share size for graph access structures.

We look for EFFICIENT constructions for graphs.

We look for HARD GRAPHS

Motivation of Our Work

To BRIDGE THE GAP between upper and lower bounds on the total share size for graph access structures.

We look for EFFICIENT constructions for graphs.

We look for HARD GRAPHS
Since the total share size is upper bounded by $O(n^2/\log n)$, we try to solve the following question:

Motivation of Our Work

To BRIDGE THE GAP between upper and lower bounds on the total share size for graph access structures.

We look for EFFICIENT constructions for graphs.

We look for HARD GRAPHS
Since the total share size is upper bounded by $O(n^2/\log n)$, we try to solve the following question:

Is there any graph with total share size $\Omega(n^2/\text{polylog} n)$?

Motivation of Our Work

To BRIDGE THE GAP between upper and lower bounds on the total share size for graph access structures.

We look for EFFICIENT constructions for graphs.

We look for HARD GRAPHS
Since the total share size is upper bounded by $O(n^2/\log n)$, we try to solve the following question:

Is there any graph with total share size $\Omega(n^2/\mathrm{polylog} n)$?

Since every graph admits a scheme with total share size $2m$, in a hard graph m has to be big.

Motivation of Our Work

To BRIDGE THE GAP between upper and lower bounds on the total share size for graph access structures.

We look for EFFICIENT constructions for graphs.

We look for HARD GRAPHS
Since the total share size is upper bounded by $O(n^2/\log n)$, we try to solve the following question:

Is there any graph with total share size $\Omega(n^2/\mathrm{polylog} n)$?

Since every graph admits a scheme with total share size $2m$, in a hard graph m has to be big.

- We study VERY DENSE GRAPHS

Motivation of Our Work

To BRIDGE THE GAP between upper and lower bounds on the total share size for graph access structures.

We look for EFFICIENT constructions for graphs.

We look for HARD GRAPHS
Since the total share size is upper bounded by $O(n^2/\log n)$, we try to solve the following question:

Is there any graph with total share size $\Omega(n^2/\text{polylog}n)$?

Since every graph admits a scheme with total share size $2m$, in a hard graph m has to be big.

- We study VERY DENSE GRAPHS
- i.e. graphs with $\binom{n}{2} - \ell$ edges, with ℓ "small".

Our Main Result

Theorem

If a graph has $\binom{n}{2} - n^{1+\beta}$ edges for some $0 < \beta < 1$, then it admits a scheme with total share size

$$O(n^{5/4+3\beta/4} \log n).$$

Our Main Result

Theorem

If a graph has $\binom{n}{2} - n^{1+\beta}$ *edges for some* $0 < \beta < 1$*, then it admits a scheme with total share size*

$$O(n \cdot n^{1/4+3\beta/4} \log n).$$

Our Main Result

Theorem

If a graph has $\binom{n}{2} - n^{1+\beta}$ *edges for some* $0 < \beta < 1$*, then it admits a scheme with total share size*

$$\tilde{O}(n^{5/4+3\beta/4}).$$

Our Main Result

Theorem

If a graph has $\binom{n}{2} - n^{1+\beta}$ edges for some $0 < \beta < 1$, then it admits a scheme with total share size

$$\tilde{O}(n^{5/4+3\beta/4}).$$

Direct consequences:

Our Main Result

Theorem

If a graph has $\binom{n}{2} - n^{1+\beta}$ edges for some $0 < \beta < 1$, then it admits a scheme with total share size

$$\tilde{O}(n^{5/4+3\beta/4}).$$

Direct consequences:

- Is there any very dense graph with total share size $\Omega(n^2/\text{polylog} n)$?

Our Main Result

Theorem

If a graph has $\binom{n}{2} - n^{1+\beta}$ *edges for some* $0 < \beta < 1$*, then it admits a scheme with total share size*

$$\tilde{O}(n^{5/4+3\beta/4}).$$

Direct consequences:

- Is there any very dense graph with total share size $\Omega(n^2/\mathrm{polylog} n)$? the answer is NO.

Our Main Result

Theorem

If a graph has $\binom{n}{2} - n^{1+\beta}$ edges for some $0 < \beta < 1$, then it admits a scheme with total share size

$$\tilde{O}(n^{5/4+3\beta/4}).$$

Direct consequences:

- Is there any very dense graph with total share size $\Omega(n^2/\mathrm{polylog} n)$? the answer is NO.
- in a hard graph, both m and $\binom{n}{2} - m$ must be big.

Our Main Result

Theorem

If a graph has $\binom{n}{2} - n^{1+\beta}$ edges for some $0 < \beta < 1$, then it admits a scheme with total share size

$$\tilde{O}(n^{5/4+3\beta/4}).$$

Direct consequences:

- Is there any very dense graph with total share size $\Omega(n^2/\mathrm{polylog} n)$? the answer is NO.
- in a hard graph, both m and $\binom{n}{2} - m$ must be big.

Main techniques:

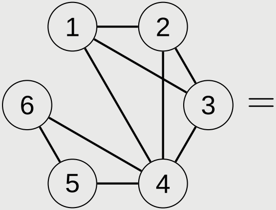
- Coverings by "easy" graphs: cliques, bipartite graphs and stars.
- The probabilistic method.
- Colorings of graphs. skip details

Our Main Result (II): Using Coverings

We cover the graph G by using easy graphs:
cliques, complete bipartite graphs, and stars.

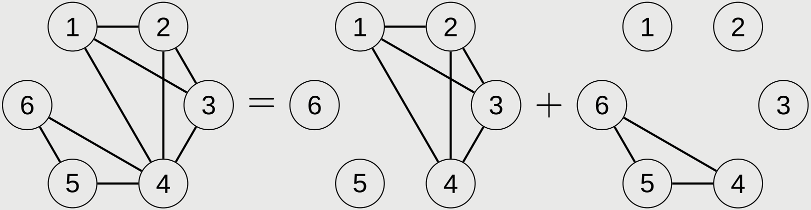
Our Main Result (II): Using Coverings

We cover the graph G by using easy graphs:
cliques, complete bipartite graphs, and stars.



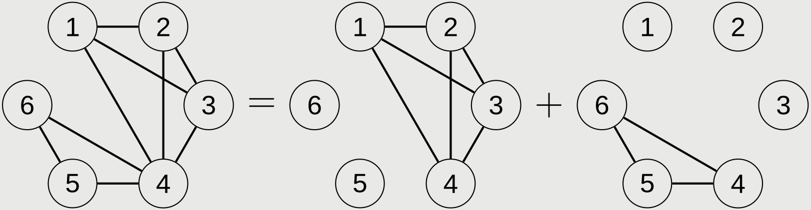
Our Main Result (II): Using Coverings

We cover the graph G by using easy graphs:
cliques, complete bipartite graphs, and stars.



Our Main Result (II): Using Coverings

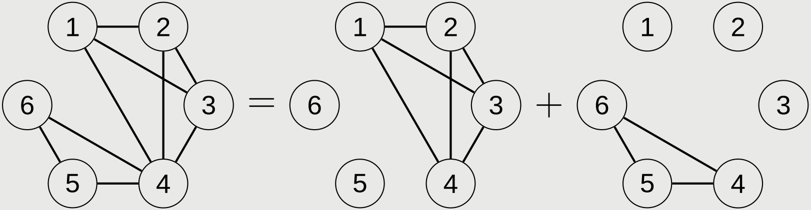
We cover the graph G by using easy graphs:
cliques, complete bipartite graphs, and stars.



The scheme for G consists on sharing the secret independently for every piece of the covering.

Our Main Result (II): Using Coverings

We cover the graph G by using easy graphs:
cliques, complete bipartite graphs, and stars.



The scheme for G consists on sharing the secret independently for every piece of the covering.

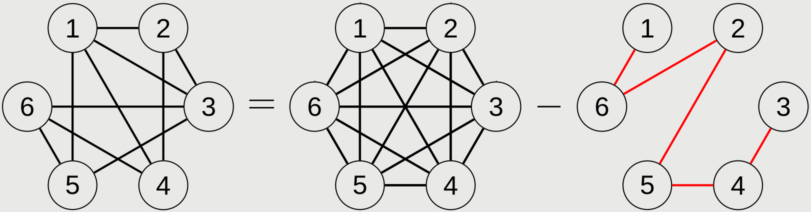
We look for small coverings in order to obtain efficient schemes.

Our Main Result (III): A New Technique

We describe the graph G as a clique minus the excluded graph G'

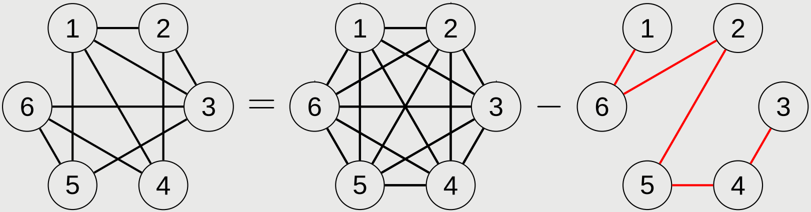
Our Main Result (III): A New Technique

We describe the graph G as a clique minus the excluded graph G'



Our Main Result (III): A New Technique

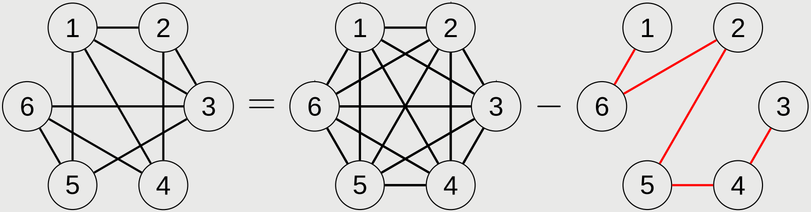
We describe the graph G as a clique minus the excluded graph G'



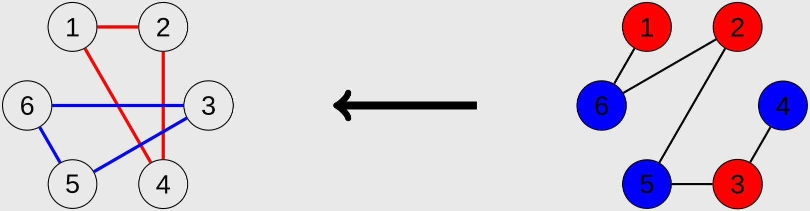
Each coloring of G' yields to a subgraph of G.

Our Main Result (III): A New Technique

We describe the graph G as a clique minus the excluded graph G'

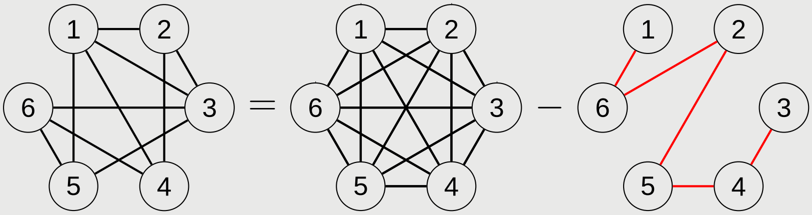


Each coloring of G' yields to a subgraph of G.

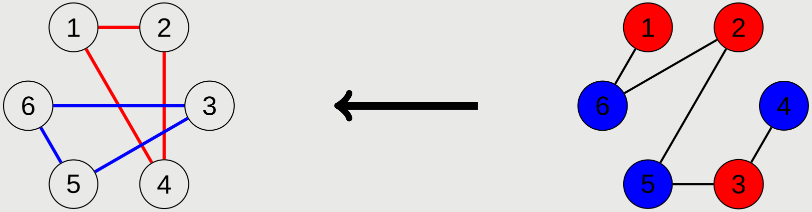


Our Main Result (III): A New Technique

We describe the graph G as a clique minus the excluded graph G'



Each coloring of G' yields to a subgraph of G.



Taking many random colorings of G' we end with a covering of G.

Our Main Result (IV): Corollaries

Theorem

If a graph has $\binom{n}{2} - n^{1+\beta}$ edges for some $0 < \beta < 1$, then it admits a scheme with total share size

$$\tilde{O}(n^{5/4+3\beta/4}).$$

Our Main Result (IV): Corollaries

Theorem

If a graph has $\binom{n}{2} - n^{1+\beta}$ edges for some $0 < \beta < 1$, then it admits a scheme with total share size

$$\tilde{O}(n^{5/4+3\beta/4}).$$

Corollary

If $\beta < 1/3$, then it admits a scheme with t.s.s. $o(n^{3/2})$.

Our Main Result (IV): Corollaries

Theorem

If a graph has $\binom{n}{2} - n^{1+\beta}$ *edges for some* $0 < \beta < 1$*, then it admits a scheme with total share size*

$$\tilde{O}(n^{5/4+3\beta/4}).$$

Corollary

If $\beta < 1/3$*, then it admits a scheme with t.s.s.* $o(n^{3/2})$.

Corollary

If a graph has $\binom{n}{2} - \ell$ *edges,*

Our Main Result (IV): Corollaries

Theorem

If a graph has $\binom{n}{2} - n^{1+\beta}$ *edges for some* $0 < \beta < 1$*, then it admits a scheme with total share size*

$$\tilde{O}(n^{5/4+3\beta/4}).$$

Corollary

If $\beta < 1/3$*, then it admits a scheme with t.s.s.* $o(n^{3/2})$*.*

Corollary

If a graph has $\binom{n}{2} - \ell$ *edges,*

- *and* $\ell < n/2$*, then it admits a scheme with t.s.s.* $n + O(\ell^{5/4})$*.*

Our Main Result (IV): Corollaries

Theorem

If a graph has $\binom{n}{2} - n^{1+\beta}$ edges for some $0 < \beta < 1$, then it admits a scheme with total share size

$$\tilde{O}(n^{5/4+3\beta/4}).$$

Corollary

If $\beta < 1/3$, then it admits a scheme with t.s.s. $o(n^{3/2})$.

Corollary

If a graph has $\binom{n}{2} - \ell$ edges,

- *and $\ell < n/2$, then it admits a scheme with t.s.s. $n + O(\ell^{5/4})$.*
- *and $\ell \ll n^{4/5}$, then it admits a scheme with t.s.s. $n + o(n)$.*

Deleting Minimal Authorized Subsets

Let G be a graph. Let Σ be a scheme of t.s.s. r realizing G.

Deleting Minimal Authorized Subsets

Let G be a graph. Let Σ be a scheme of t.s.s. r realizing G.

If we add ℓ edges to G, by using the trivial construction we can construct a scheme for the new graph with total share size $r + 2\ell$.

Deleting Minimal Authorized Subsets

Let G be a graph. Let Σ be a scheme of t.s.s. r realizing G.

If we add ℓ edges to G, by using the trivial construction we can construct a scheme for the new graph with total share size $r + 2\ell$.

But what happens if we delete edges from G? .

Deleting Minimal Authorized Subsets

Let G be a graph. Let Σ be a scheme of t.s.s. r realizing G.

If we add ℓ edges to G, by using the trivial construction we can construct a scheme for the new graph with total share size $r + 2\ell$.

But what happens if we delete edges from G? NOT KNOWN.

Deleting Minimal Authorized Subsets

Let G be a graph. Let Σ be a scheme of t.s.s. r realizing G.

If we add ℓ edges to G, by using the trivial construction we can construct a scheme for the new graph with total share size $r + 2\ell$.

But what happens if we delete edges from G? NOT KNOWN.

Theorem

If we delete ℓ edges from G, the new graph admits a scheme with total share size

- $\tilde{O}(\sqrt{\ell n r})$ if $\ell > r/n$
- $r + 2\ell n$ if $\ell \leq r/n$

Deleting Minimal Authorized Subsets

Let G be a graph. Let Σ be a scheme of t.s.s. r realizing G.

If we add ℓ edges to G, by using the trivial construction we can construct a scheme for the new graph with total share size $r + 2\ell$.

But what happens if we delete edges from G? NOT KNOWN.

Theorem

If we delete ℓ edges from G, the new graph admits a scheme with total share size

- $\tilde{O}(\sqrt{\ell n r})$ if $\ell > r/n$
- $r + 2\ell n$ if $\ell \leq r/n$

Direct consequence: If G admits an efficient scheme, the graphs that are close to G are not hard.

Deleting Minimal Authorized Subsets: Generalization

We extend the techniques for graph access structures to

- homogeneous access structures
- general access structures

go to details

Deleting Minimal Authorized Subsets: Generalization

We extend the techniques for graph access structures to

- homogeneous access structures
- general access structures

We provide new techniques and constructions, and we give answers to the following problems:

go to details

Deleting Minimal Authorized Subsets: Generalization

We extend the techniques for graph access structures to

- homogeneous access structures
- general access structures

We provide new techniques and constructions, and we give answers to the following problems:

- Deleting minimal authorized subsets in a threshold access structure.

go to details

Deleting Minimal Authorized Subsets: Generalization

We extend the techniques for graph access structures to

- homogeneous access structures
- general access structures

We provide new techniques and constructions, and we give answers to the following problems:

- Deleting minimal authorized subsets in a threshold access structure.
- Deleting minimal authorized subsets in any access structure.

go to details

Lower Bounds

Theorem

For every $2 < \ell < n$, there exists a family of graphs with $\binom{n}{2} - \ell$ edges whose schemes have t.s.s. at least $n + \ell$.

Lower Bounds

Theorem

For every $2 < \ell < n$*, there exists a family of graphs with* $\binom{n}{2} - \ell$ *edges whose schemes have t.s.s. at least* $n + \ell$.

There exists a scheme with t.s.s. $n + O(\ell^{5/4})$, when $1 < \ell < n/2$.

Lower Bounds

Theorem

For every $2 < \ell < n$*, there exists a family of graphs with* $\binom{n}{2} - \ell$ *edges whose schemes have t.s.s. at least* $n + \ell$.

There exists a scheme with t.s.s. $n + O(\ell^{5/4})$, when $1 < \ell < n/2$.

Theorem

For every $0 < \beta < 1$*, there exists a family of graphs with* $\binom{n}{2} - n^{1+\beta}$ *edges whose schemes have at least t.s.s.* $\Omega(\beta n \log n)$.

Lower Bounds

Theorem

For every $2 < \ell < n$, there exists a family of graphs with $\binom{n}{2} - \ell$ edges whose schemes have t.s.s. at least $n + \ell$.

There exists a scheme with t.s.s. $n + O(\ell^{5/4})$, when $1 < \ell < n/2$.

Theorem

For every $0 < \beta < 1$, there exists a family of graphs with $\binom{n}{2} - n^{1+\beta}$ edges whose schemes have at least t.s.s. $\Omega(\beta n \log n)$.

Theorem

For every $0 < \beta < 1$, there exists a family of graphs with $\binom{n}{2} - n^{1+\beta}$ edges whose linear schemes have at least t.s.s. $\Omega(n^{1+\beta/2})$.

Lower Bounds

Theorem

For every $2 < \ell < n$, there exists a family of graphs with $\binom{n}{2} - \ell$ edges whose schemes have t.s.s. at least $n + \ell$.

There exists a scheme with t.s.s. $n + O(\ell^{5/4})$, when $1 < \ell < n/2$.

Theorem

For every $0 < \beta < 1$, there exists a family of graphs with $\binom{n}{2} - n^{1+\beta}$ edges whose schemes have at least t.s.s. $\Omega(\beta n \log n)$.

Theorem

For every $0 < \beta < 1$, there exists a family of graphs with $\binom{n}{2} - n^{1+\beta}$ edges whose linear schemes have at least t.s.s. $\Omega(n^{1+\beta/2})$.

There exists a scheme with t.s.s. $\tilde{O}(n^{5/4+3\beta/4}) = \tilde{O}(n^{1+\beta/2} \cdot n^{1/4+\beta/4})$.

Summary and Open Directions

Summary:

- Secret sharing for very dense graphs.
- New upper and lower bounds for the total share size for the schemes realizing these graphs.
- Does exit any hard very dense graph?: No.
- New techniques for the construction of secret sharing schemes.
- Extension to homogeneous and general access structures.

Summary and Open Directions

Summary:

- Secret sharing for very dense graphs.
- New upper and lower bounds for the total share size for the schemes realizing these graphs.
- Does exit any hard very dense graph?: No.
- New techniques for the construction of secret sharing schemes.
- Extension to homogeneous and general access structures.

Open directions:

- To find hard graphs.
- New techniques for finding lower bounds on the total share size.
- To bridge the gap between upper and lower bounds on the total share size.

Thank you

Appendix: Deleting Minimal Authorized Subsets

Theorem

Let Γ be a t-threshold access structures for a constant t. If we delete ℓ minimal authorized subsets, then the resulting access structure admits a scheme with total share size

$$\tilde{O}(\ell n).$$

Let Γ be an access structure with a scheme of t.s.s. r such that

- if $A \in \min \Gamma$, then $|A| \leq k$ for some constant k.

Let Γ' be an access structure such that

- $\min \Gamma' = \min \Gamma \setminus \Delta$
- for every $p \in P$, there is at most d subsets in Δ containing p.

Theorem

The access structure Γ' admits a scheme with total share size

$$\tilde{O}(d^{k-1} r).$$