# Minimizing the total number of shadows in secret sharing schemes based on extended neighborhood coronas

**Raúl M. Falcón**[1], N. Mohanapriya[2] and V. Aparna[2]

[1] Department of Applied Maths I, Universidad de Sevilla, Spain. rafalgan@us.es
[2] PG and Research Dept. of Mathematics, Kongunadu Arts and Science College, India.

**Santander, October 19–21, 2022.**

# CONTENTS

# CONTENTS

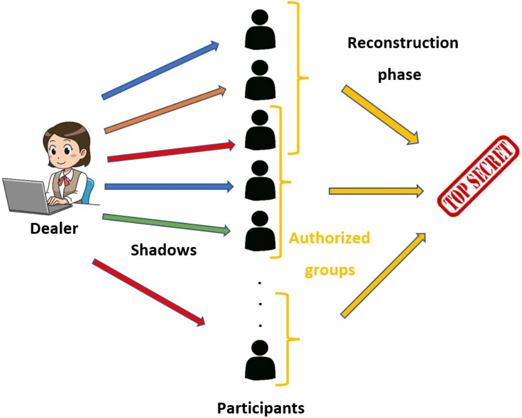
# $(n, t)$-threshold secret sharing scheme.

**[Blakley, 1979]** *Safeguarding cryptographic keys*. Int. Workshop Managing Requirements Knowledge, 313–317.

**[Shamir, 1979]** *How to share a secret*. Comm. ACM 22, 612–613.

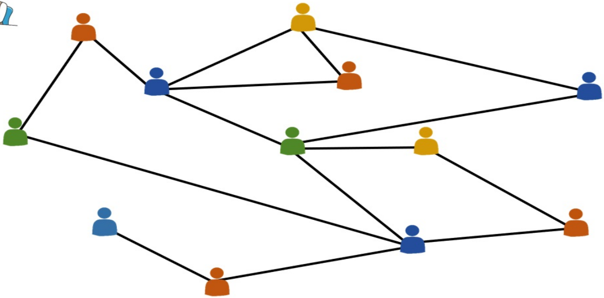
George R. **Blakley** Jr.

Adi **Shamir**



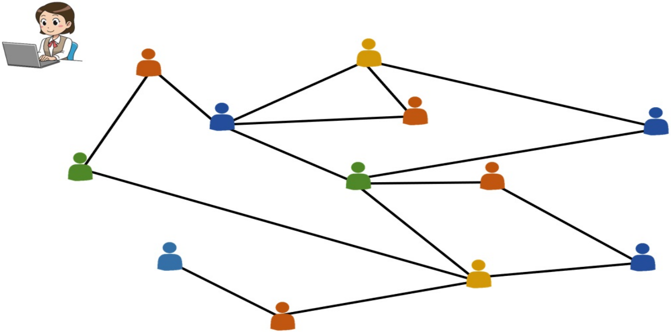

- $n$ shadows.
- Any authorized subgroup sharing at least $t$ distinct shadows can reconstruct the secret, but no subgroup sharing less than $t$ shadows can do it.

# $(n, t)$-threshold secret sharing scheme.



- Schemes based on *finite, simple and connected undirected graphs*.
- *Vertex* = Participant.
- *Edge* = Proximity relationship such that cooperation is possible.
- **One round of communication**: Each participant receives the shadows of her/his neighbors.
- *n*-**proper coloring**: One shadow (*color*) per participant so that no two neighbors have the same shadow.

# $t$-dynamic proper $n$-coloring.



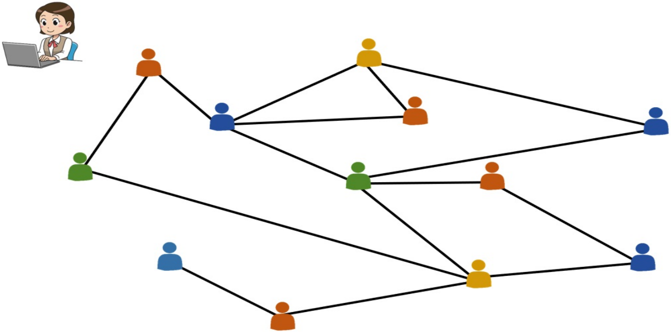
$(n, t) = (4, 3)$

- **[Kim and Ok, 2017]**: Every $t$-**dynamic proper** $n$-**coloring** describes a shadow allocation of an $(n, t+1)$-**threshold secret sharing scheme**.
- **[Montgomery, 2001]**: The number of different colors among the neighbors of a vertex is at least $t$, or all different if the vertex has less than $t$ neighbors.

$$|c(N_G(v))| \geq \min\{t, |N_G(v)|\}. \tag{1}$$

After just one round of communication, each participant can either reconstruct the secret, or obtain a different shadow from each one of his/her neighbors.

# $t$-dynamic proper $n$-coloring.

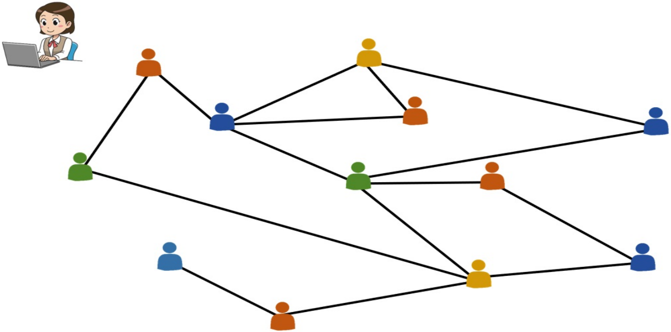


$(n, t) = (4, 3)$

- **Problem 1.** Which is the minimum number of rounds of communication that are necessary to ensure that the secret can be reconstructed by all the participants?

- **Problem 2.** Which is the minimum number of distinct shadows into which the secret has to split to ensure condition (1)?

# $t$-dynamic proper $n$-coloring.

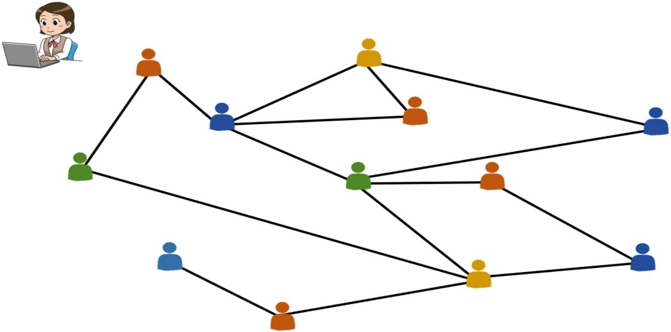


$(n, t) = (4, 3)$

**Problem 1**: *Minimum number of rounds of communication.*

- 1, if $t \leq \delta(G)$.
- Upper bounded by the diameter of the graph, otherwise.

# $t$-dynamic proper $n$-coloring.

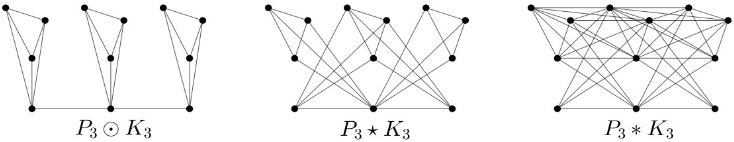


$(n, t) = (4, 3)$

**Problem 2**: *Minimum number of shadows.*

- $\chi_t(G)$: The $t$-**dynamic chromatic number** is the minimum number of shadows into which the secret has to split to ensure this coloring.
- Computing this number constitutes the *$t$-dynamic coloring problem* of the graph.
- If $t = 1$, then it coincides with the classical chromatic number $\chi(G)$.

# Extended neighborhood corona.




- *Corona product* **[Frucht and Harary, 1970]**: $G \odot H$.

  Every vertex $v_i$ in $G$ is joined to all the vertices in the $i^{\text{th}}$ copy of $H$.

- *Neighborhood corona product* **[Indulal, 2011]**: $G \star H$.

  Every neighbor of the vertex $v_i$ in $G$ is joined to every vertex in the $i^{\text{th}}$ copy of $H$.

- *Extended neighborhood corona product* **[Adiga et al., 2016]**: $G * H$.

  In $G \star H$, every vertex in the $i^{th}$ copy of $H$ is joined to every vertex in the $j^{\text{th}}$ copy of $H$, whenever $v_i$ and $v_j$ are connected.

# Extended neighborhood corona.

$G * H$ can model complex networks with **small average path length** ($\ell$) even if $G$ and/or $H$ grow asymptotically.

**Proposition (F. et al., 2022)**

*If $m = |V(G)|$ and $n = |V(H)|$, then*

1. $\lim_{m\to\infty} \ell_{G*H} = \frac{n+1}{n} \cdot \lim_{m\to\infty} \ell_G$.
2. $\frac{\ell_G \cdot (m-1)+1}{m} \leq \lim_{n\to\infty} \ell_{G*H} \leq \frac{\ell_G \cdot (m-1)+2}{m}$.
3. $\lim_{m,n\to\infty} \ell_{G*H} = \lim_{m\to\infty} \ell_G$.

If $\ell_G \to \infty$, then only $H$ can grow.

**Example**: $G = P_m$ (**center path**).

If $\ell_G$ is asymptotically bounded, then both $G$ and $H$ can grow.

**Example**: $G = S_m$ (**center star**).

# CONTENTS

# Solving the dynamic coloring problem.

$\omega(G)$ [**Clique number**]: Largest order of any complete subgraph in $G$.

## Lemma (F. et al., 2022)

$$\omega(G)\cdot\chi(H)\leq\chi_t(G*H)\leq\beta_t\cdot\chi_{\alpha_t}(G),$$

*where*

$$\alpha_t:=\min\left\{\lceil\frac{t}{n+1}\rceil,\,\Delta(G)\right\}$$

*and*

$$\beta_t:=\min\{n+1,\,\max\{t,\,\chi(H)\}\}.$$

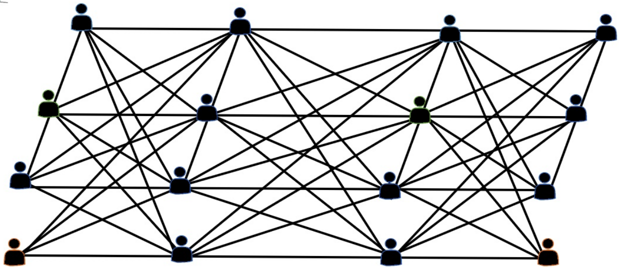
## Proposition (F. et al., 2022)

*If* $\omega(G)=\chi(G)$, *then*

$$\chi_t(G*H)=\chi(G)\cdot\chi(H),$$

*for every* $t\leq\chi(H)$.

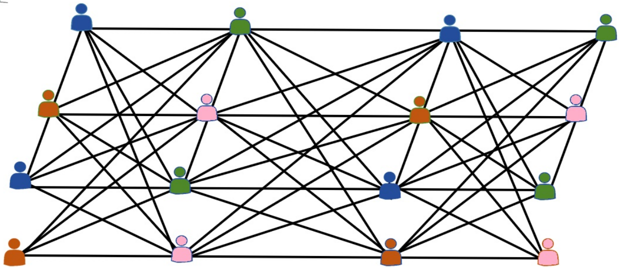
# Center path: $P_m * H$.



**Theorem (F. et al., 2022)**

$$\chi_t(P_m * H) = \begin{cases} 2 \cdot \max\{t, \chi(H)\}, & \textit{if } t \leq n+1, \\ n+t+1, & \textit{if } n+1 < t < 2n+2, \\ 3n+3, & \textit{otherwise.} \end{cases}$$

# Center path: $P_m * H$.

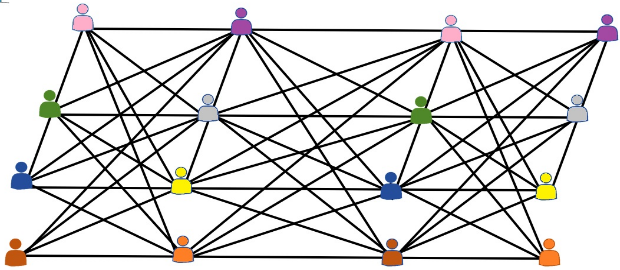


$\chi_2(P_4 * P_3) = 4.$

**Theorem (F. et al., 2022)**

$$\chi_t(P_m * H) = \begin{cases} 2 \cdot \max\{t, \chi(H)\}, & \text{if } t \leq n+1, \\ n+t+1, & \text{if } n+1 < t < 2n+2, \\ 3n+3, & \text{otherwise.} \end{cases}$$

# Center path: $P_m * H$.

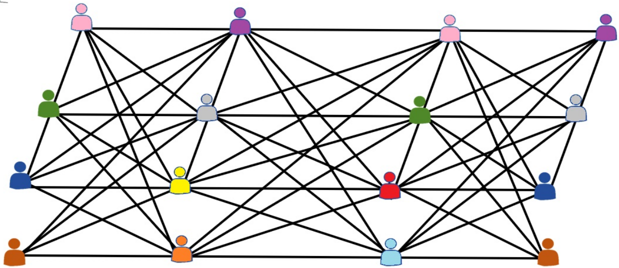


$\chi_4(P_4 * P_3) = 8.$

**Theorem (F. et al., 2022)**

$$\chi_t(P_m * H) = \begin{cases} 2 \cdot \max\{t, \chi(H)\}, & \text{if } t \leq n+1, \\ n+t+1, & \text{if } n+1 < t < 2n+2, \\ 3n+3, & \text{otherwise.} \end{cases}$$

# Center path: $P_m * H$.

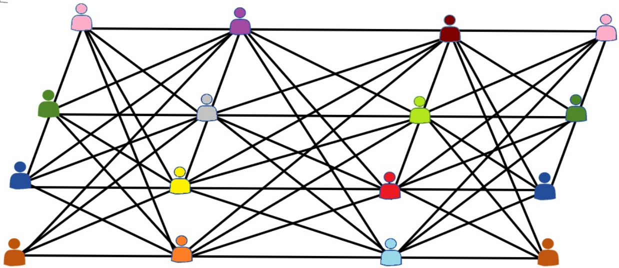


$\chi_6(P_4 * P_3) = 10.$

**Theorem (F. et al., 2022)**

$$\chi_t(P_m * H) = \begin{cases} 2 \cdot \max\{t, \chi(H)\}, & \textit{if } t \leq n+1, \\ n+t+1, & \textit{if } n+1 < t < 2n+2, \\ 3n+3, & \textit{otherwise.} \end{cases}$$

# Center path: $P_m * H$.



$\chi_t(P_4 * P_3) = 12$, whenever $t \geq 8$.

**Theorem (F. et al., 2022)**

$$\chi_t(P_m * H) = \begin{cases} 2 \cdot \max\{t,\, \chi(H)\}, & \text{if } t \leq n+1, \\ n+t+1, & \text{if } n+1 < t < 2n+2, \\ 3n+3, & \text{otherwise.} \end{cases}$$

# Center path: $P_m * H$.

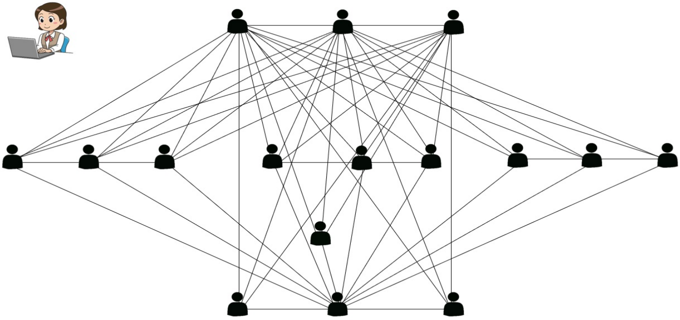
**Theorem (F. et al., 2022)**

$$\chi_t(P_m * H) = \begin{cases} 2 \cdot \max\{t,\, \chi(H)\}, & \text{if } t \leq n+1, \\ n+t+1, & \text{if } n+1 < t < 2n+2, \\ 3n+3, & \text{otherwise.} \end{cases}$$

- Two rounds of communication are enough to ensure that all the participants can reconstruct the secret, whenever everybody is honest.
- Minimum number of distinct shadows:

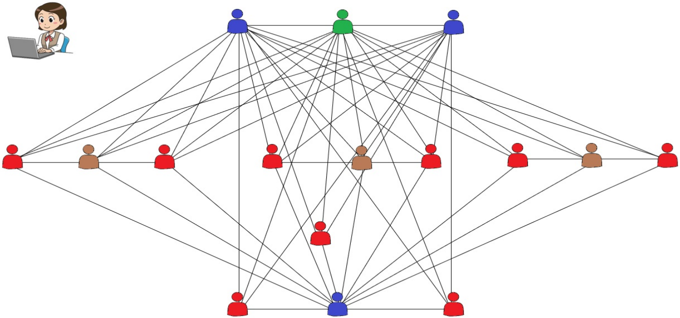
$$\lim_{n\to\infty} \chi_t(P_m * H) = 2 \cdot \max\{t, \chi(H)\}.$$

# Center star: $S_m * H$.



**Theorem (F. et al., 2022)**

$$\chi_t(S_m * H) = \begin{cases} 2 \cdot \max\{t, \chi(H)\}, & \text{if } t \leq n+1, \\ n+t+1, & \text{if } n+1 < t < mn+m, \\ (m+1)\cdot(n+1), & \text{otherwise.} \end{cases}$$

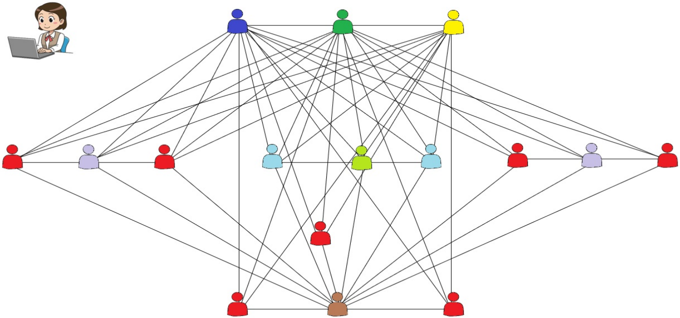


$\chi_2(S_3 * P_3) = 4.$

**Theorem (F. et al., 2022)**

$$\chi_t(S_m * H) = \begin{cases} 2 \cdot \max\{t, \chi(H)\}, & \text{if } t \leq n+1, \\ n+t+1, & \text{if } n+1 < t < mn+m, \\ (m+1)\cdot(n+1), & \text{otherwise.} \end{cases}$$

# Center star: $S_m * H$.

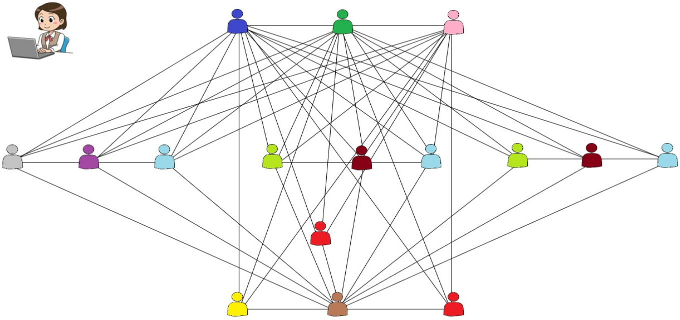


$\chi_4(S_3 * P_3) = 8.$

**Theorem (F. et al., 2022)**

$$\chi_t(S_m * H) = \begin{cases} 2 \cdot \max\{t, \chi(H)\}, & \text{if } t \leq n+1, \\ n+t+1, & \text{if } n+1 < t < mn+m, \\ (m+1) \cdot (n+1), & \text{otherwise.} \end{cases}$$

# Center star: $S_m * H$.

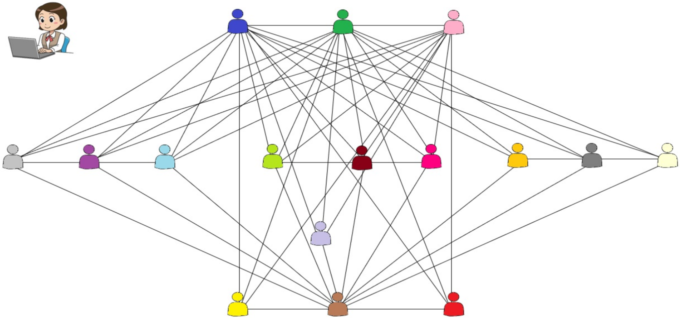


$\chi_7(S_3 * P_3) = 11.$

**Theorem (F. et al., 2022)**

$$\chi_t(S_m * H) = \begin{cases} 2 \cdot \max\{t,\, \chi(H)\}, & \textit{if } t \leq n+1, \\ n+t+1, & \textit{if } n+1 < t < mn+m, \\ (m+1)\cdot(n+1), & \textit{otherwise.} \end{cases}$$

# Center star: $S_m * H$.



$\chi_t(S_3 * P_3) = 16$, whenever $t \geq 12$.

**Theorem (F. et al., 2022)**

$$\chi_t(S_m * H) = \begin{cases} 2 \cdot \max\{t, \chi(H)\}, & \text{if } t \leq n+1, \\ n+t+1, & \text{if } n+1 < t < mn+m, \\ (m+1)\cdot(n+1), & \text{otherwise.} \end{cases}$$

# Center star: $S_m * H$.

**Theorem (F. et al., 2022)**

$$\chi_t(S_m * H) = \begin{cases} 2 \cdot \max\{t,\, \chi(H)\}, & \textit{if } t \leq n+1, \\ n+t+1, & \textit{if } n+1 < t < mn+m, \\ (m+1)\cdot(n+1), & \textit{otherwise}. \end{cases}$$

- Two rounds of communication are enough to ensure that all the participants can reconstruct the secret, whenever everybody is honest.
- Minimum number of distinct shadows:
  - If $S_m$ is large enough, then

$$\lim_{m\to\infty} \chi_t(S_m * H) = \begin{cases} 2 \cdot \max\{t,\, \chi(H)\}, & \text{if } t \leq n+1, \\ n+t+1, & \text{otherwise.} \end{cases}$$

  - If either $H$ or both $S_m$ and $H$ are large enough, then

$$\lim_{n\to\infty} \chi_t(S_m * H) = \lim_{m,n\to\infty} \chi_t(S_m * H) = 2 \cdot \max\{t, \chi(H)\}.$$

# CONTENTS

1. Preliminaries.
2. Minimizing the number of shadows.
3. Further work.

- **Problem A.** For any given graph, how many rounds of communications are, at least, necessary to ensure that the secret can be reconstructed by everybody? What if there are dishonest participants?

- **Problem B.** Which is the minimum number of distinct shadows into which the secret has to split to ensure that everybody recover it in, at most, $k$ rounds of communication?

$$|c(N_G^k(v))| \geq \min\{t, |N_G^k(v)|\},$$

where

$$N_G^k(v) := \{w \in V(G) \colon \; d_G(v, w) \leq k\}.$$

[$(t, k)$-**dynamic chromatic number** $\chi_{t,k}(G)$]

# REFERENCES


- **[Adiga et al., 2016]** *Spectra of extended neighborhood corona and extended corona of two graphs*. Electron. J. Graph Theory Appl. 4, 101–110.
- **[Blakley, 1979]** *Safeguarding cryptographic keys*. Int. Workshop Managing Requirements Knowledge, 313–317.
- **[F. et al., 2022]** *Optimal shadow allocations of secret sharing schemes arisen from the dynamic coloring of extended neighborhood coronas*. Mathematics 10, paper 2018, 13 pp.
- **[Frucht and Harary, 1970]** *On the corona of two graphs*. Aequationes Math. 4, 322–325.
- **[Indulal, 2011]** *The spectrum of neighborhood corona of graphs*. Kragujevac J. Math. 35, 493–500.
- **[Kim and Ok, 2017]** *Dynamic choosability of triangle-free graphs and sparse random graphs*. J. Graph Theory 87, 347–355.
- **[Montgomery, 2001]** *Dynamic coloring of graphs*. Ph.D Thesis, West Virginia University, ProQuest LLC, Ann Arbor, MI, United States, 2001.
- **[Shamir, 1979]** *How to share a secret*. Comm. ACM 22, 612–613.

# Many thanks!

## Minimizing the total number of shadows in secret sharing schemes based on extended neighborhood coronas

**Raúl M. Falcón**[1], N. Mohanapriya[2] and V. Aparna[2]

[1] Department of Applied Maths I, Universidad de Sevilla, Spain. rafalgan@us.es
[2] PG and Research Dept. of Mathematics, Kongunadu Arts and Science College, India.

**Santander, October 19–21, 2022.**