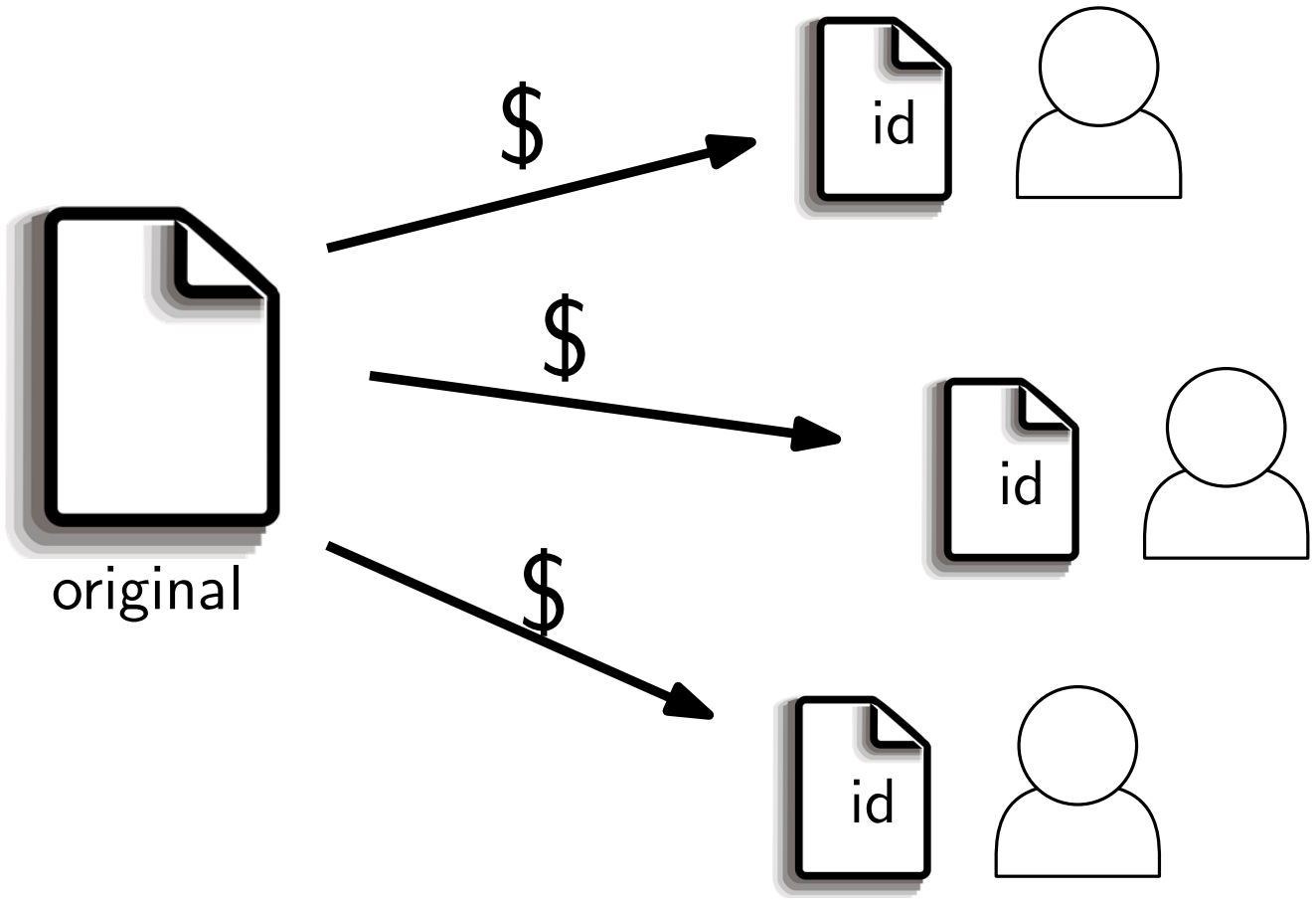
Foundations of Graph Watermarking

David Eppstein, Michael T. Goodrich,
Jenny Lam, Michael Mitzenmacher

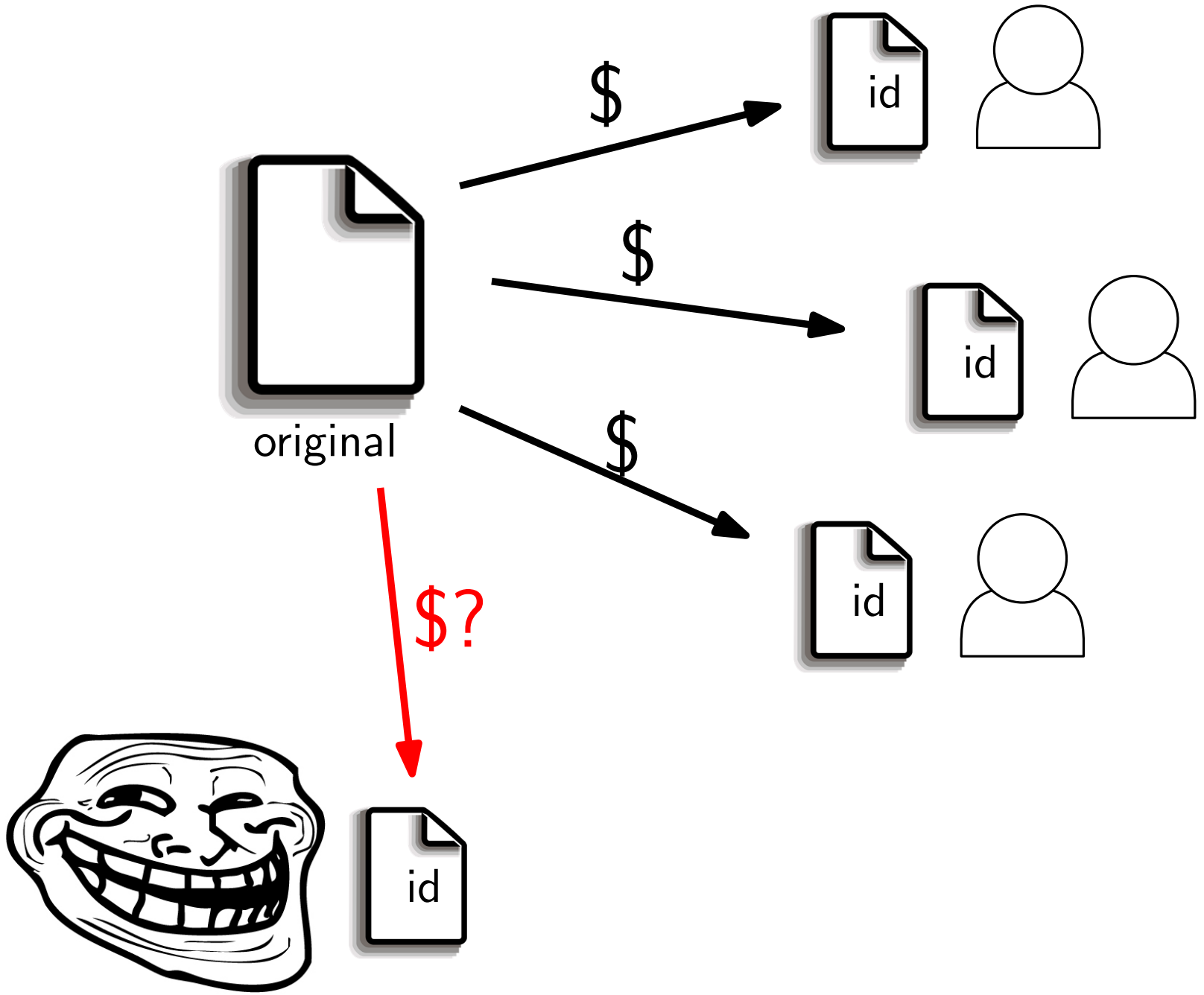
In submission at Financial Crypto 2016

problem

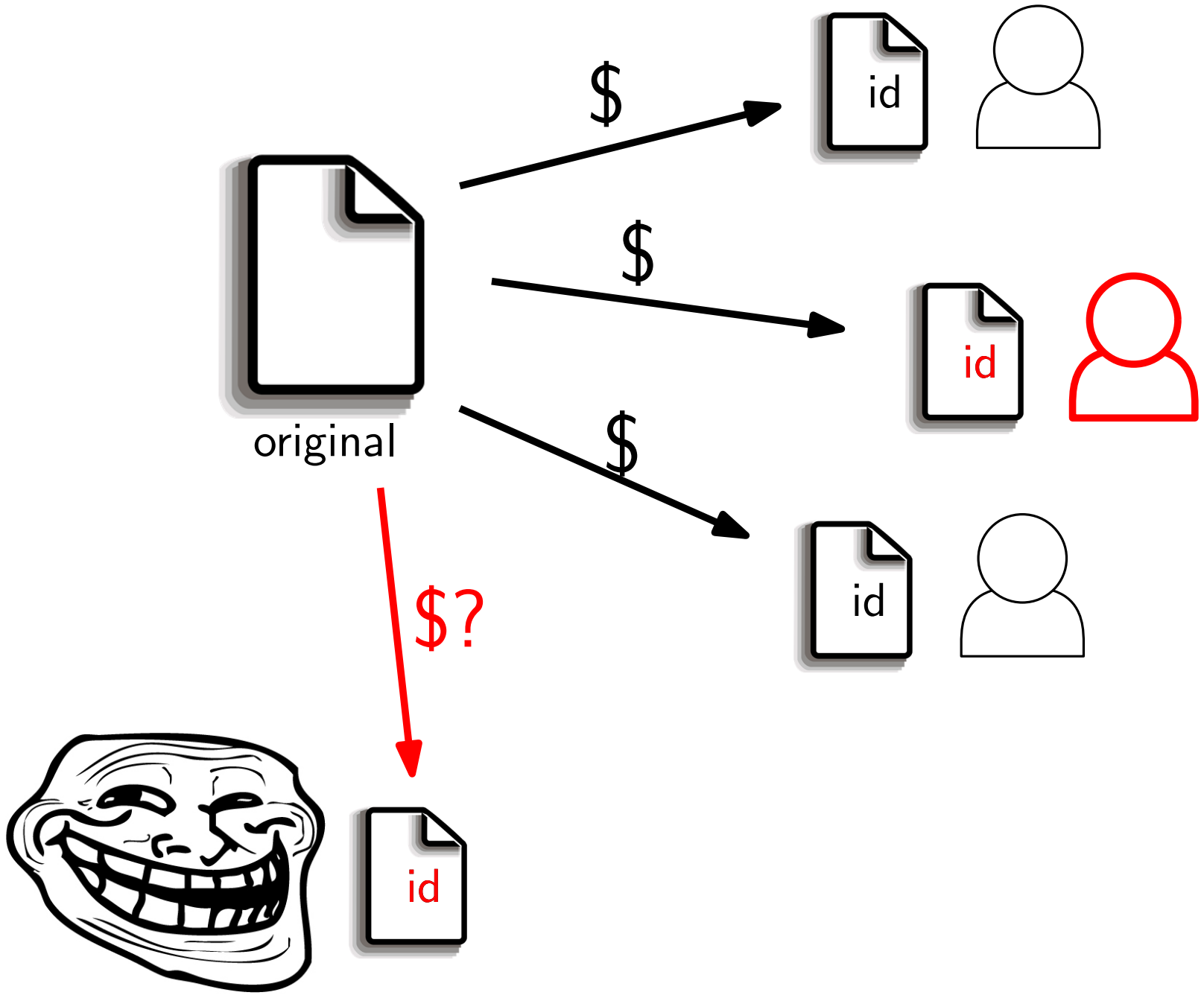
The digital watermarking problem



The digital watermarking problem



The digital watermarking problem



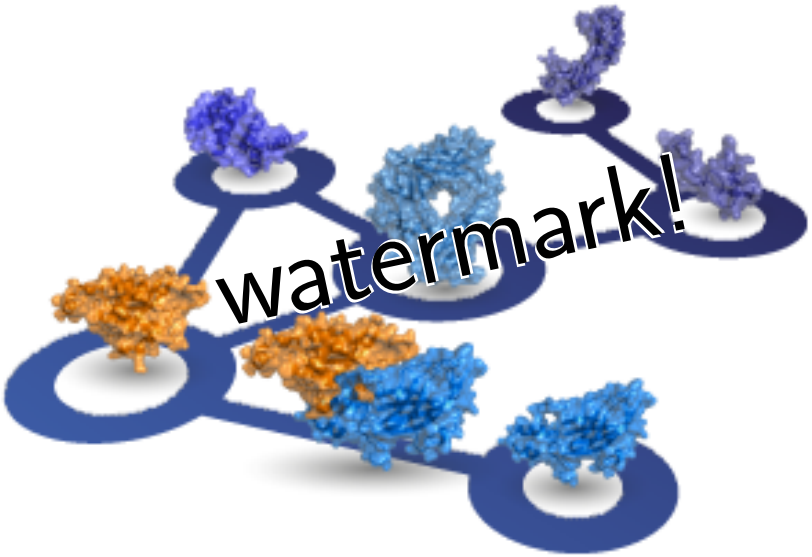

watermark!


watermark!


watermark!

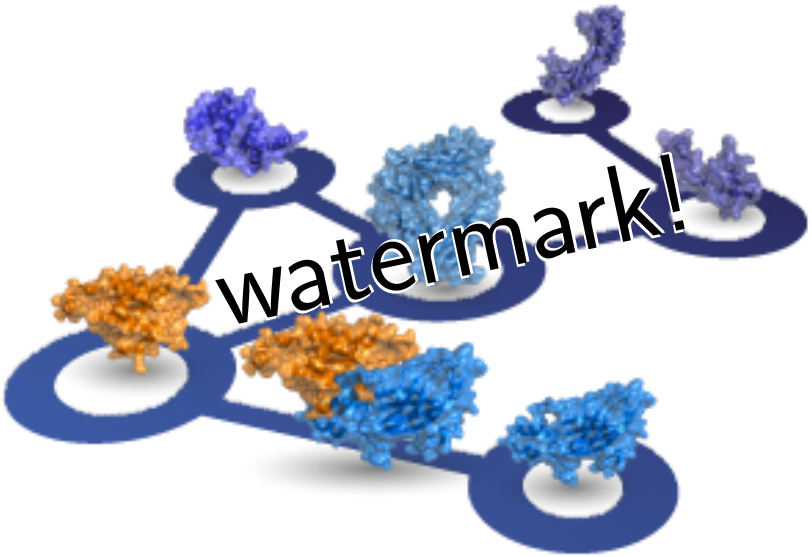

watermark!


watermark!


watermark!


watermark!

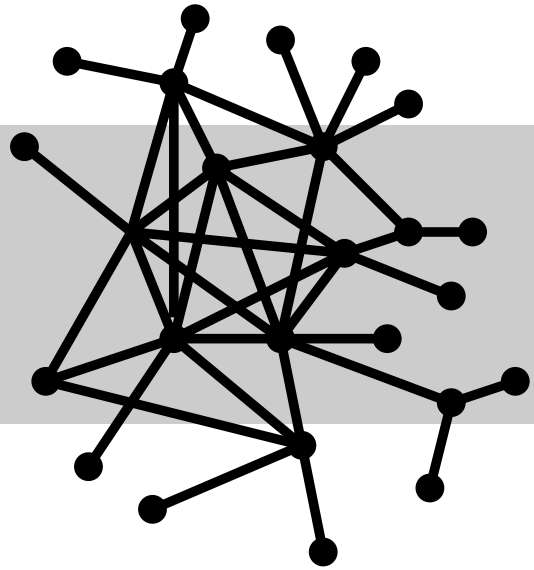

watermark!

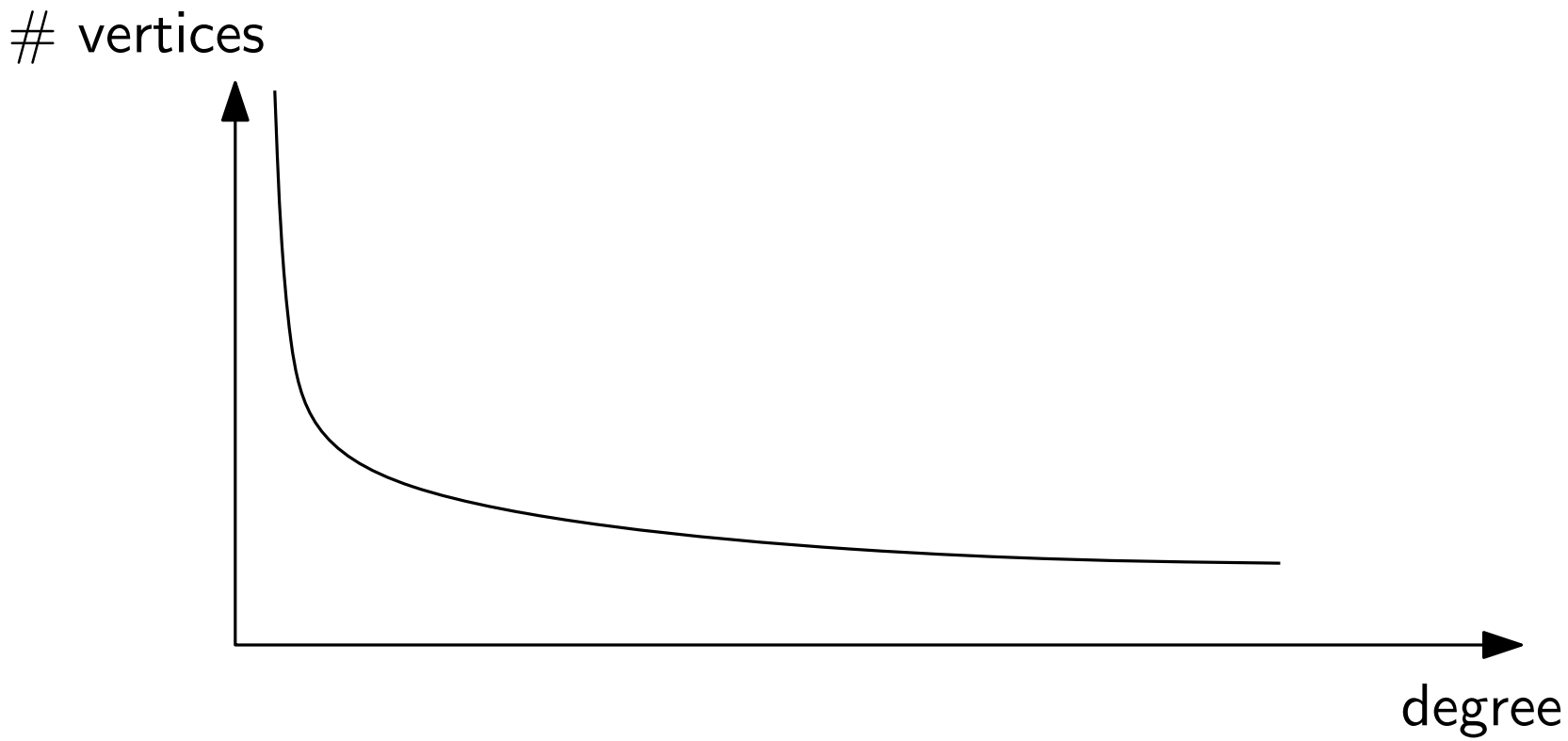

watermark!


watermark!

Scale-free networks

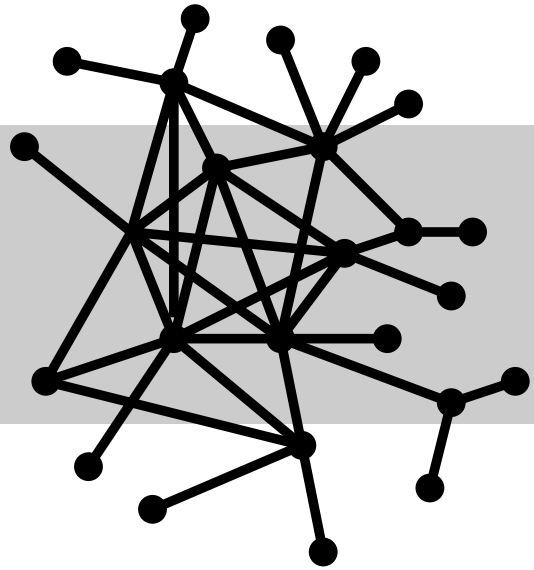
fraction of vertices with degree k $\propto$ $\frac{1}{k^\gamma}$ $2 < \gamma < 3$

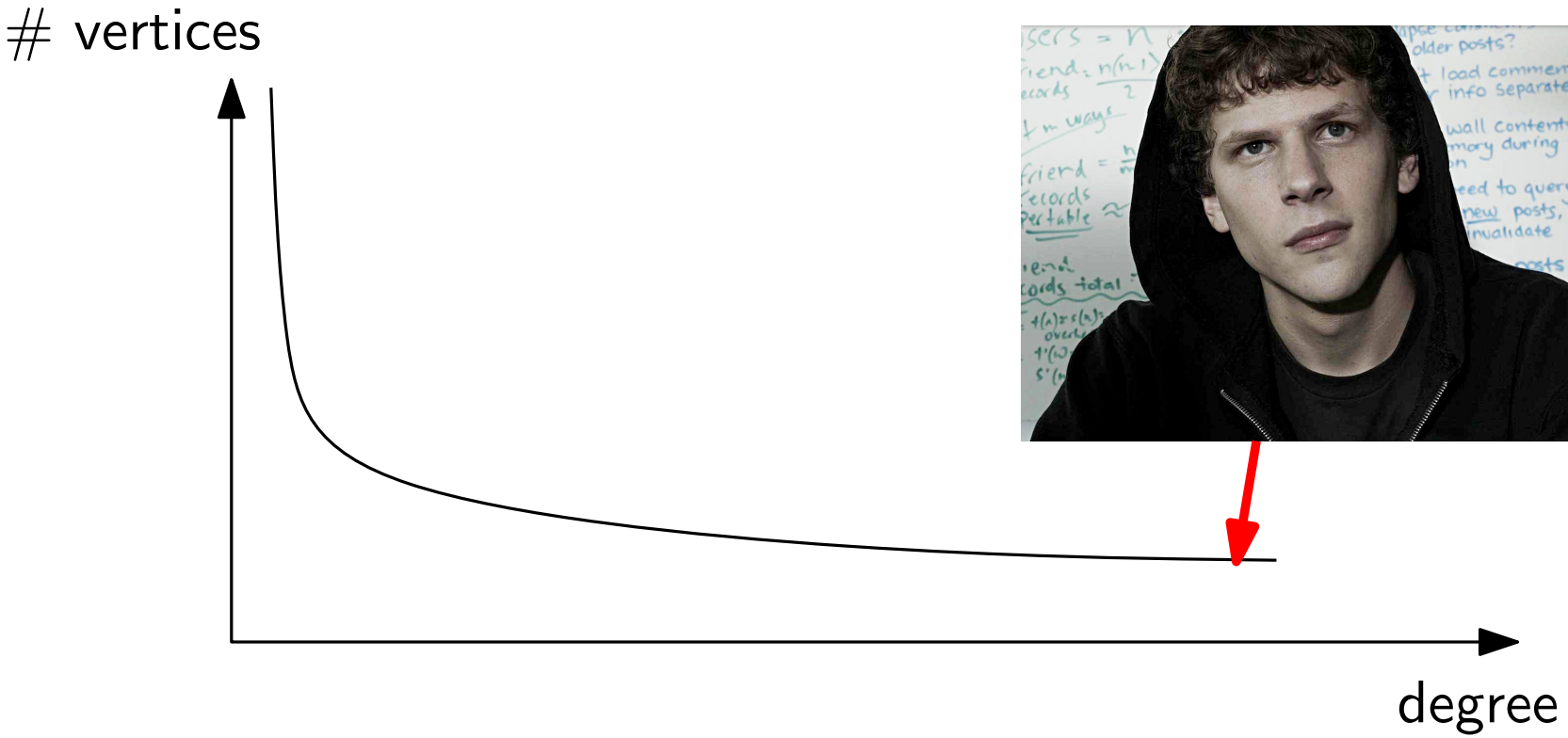




Scale-free networks

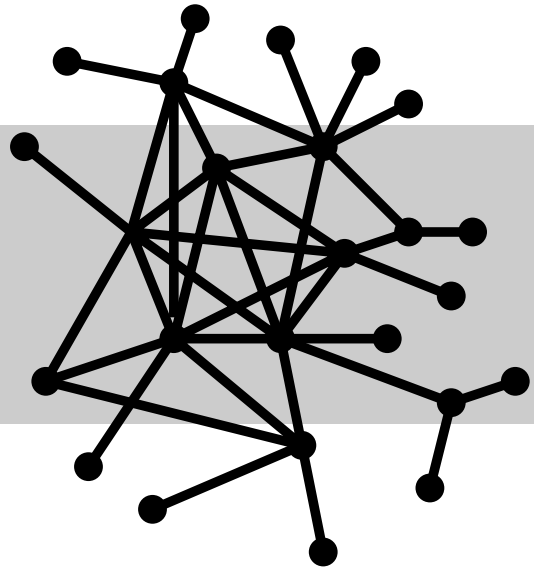
fraction of vertices with degree k $\propto$ $\frac{1}{k^\gamma}$ $2 < \gamma < 3$

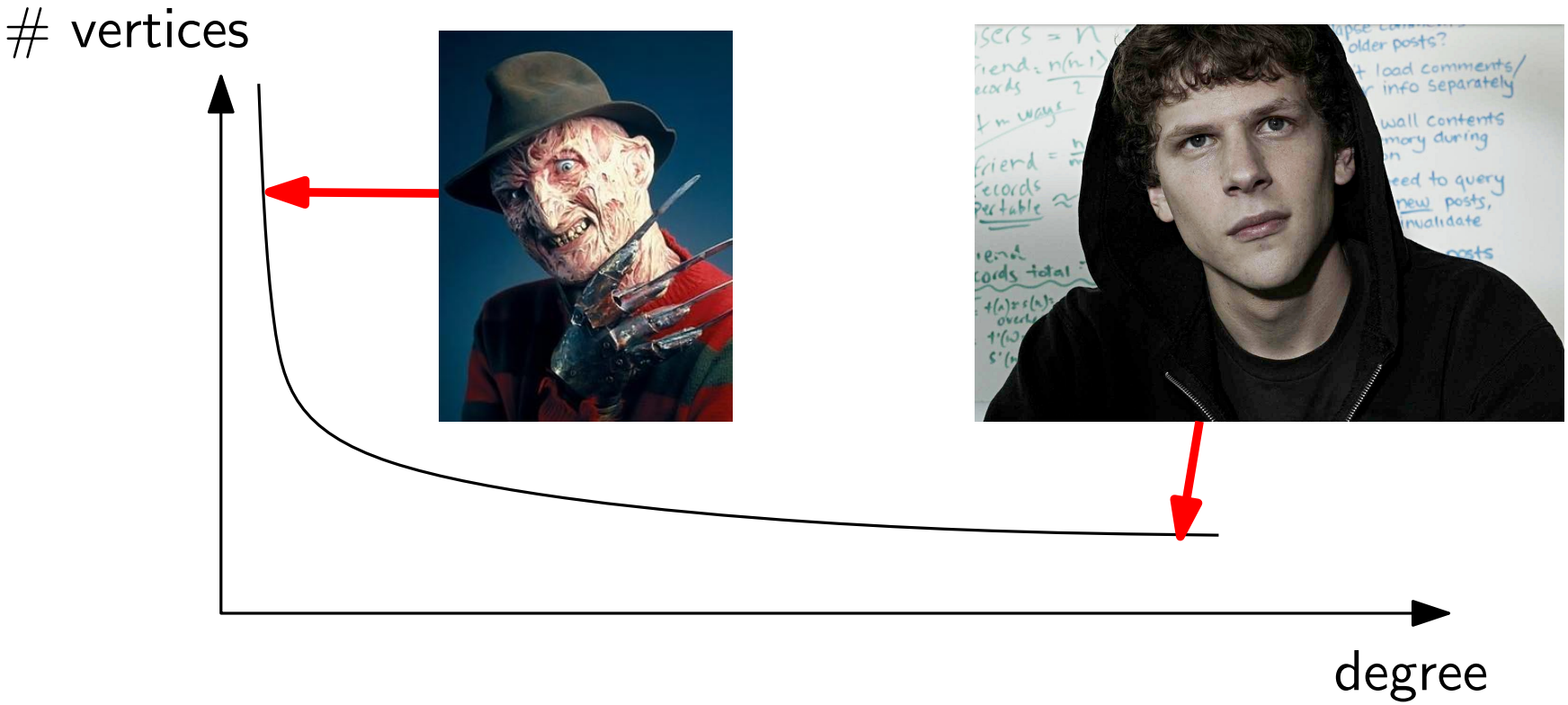




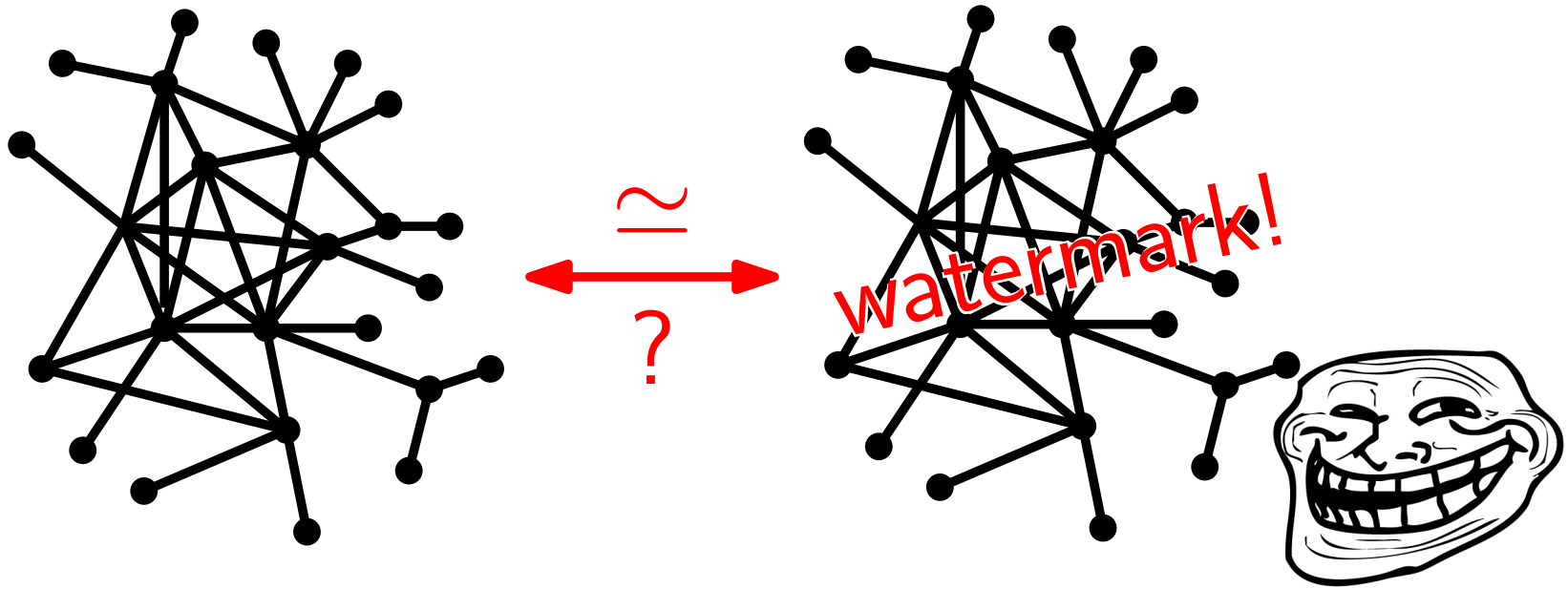
Scale-free networks

fraction of vertices with degree k $\propto$ $\frac{1}{k^\gamma}$ $2 < \gamma < 3$

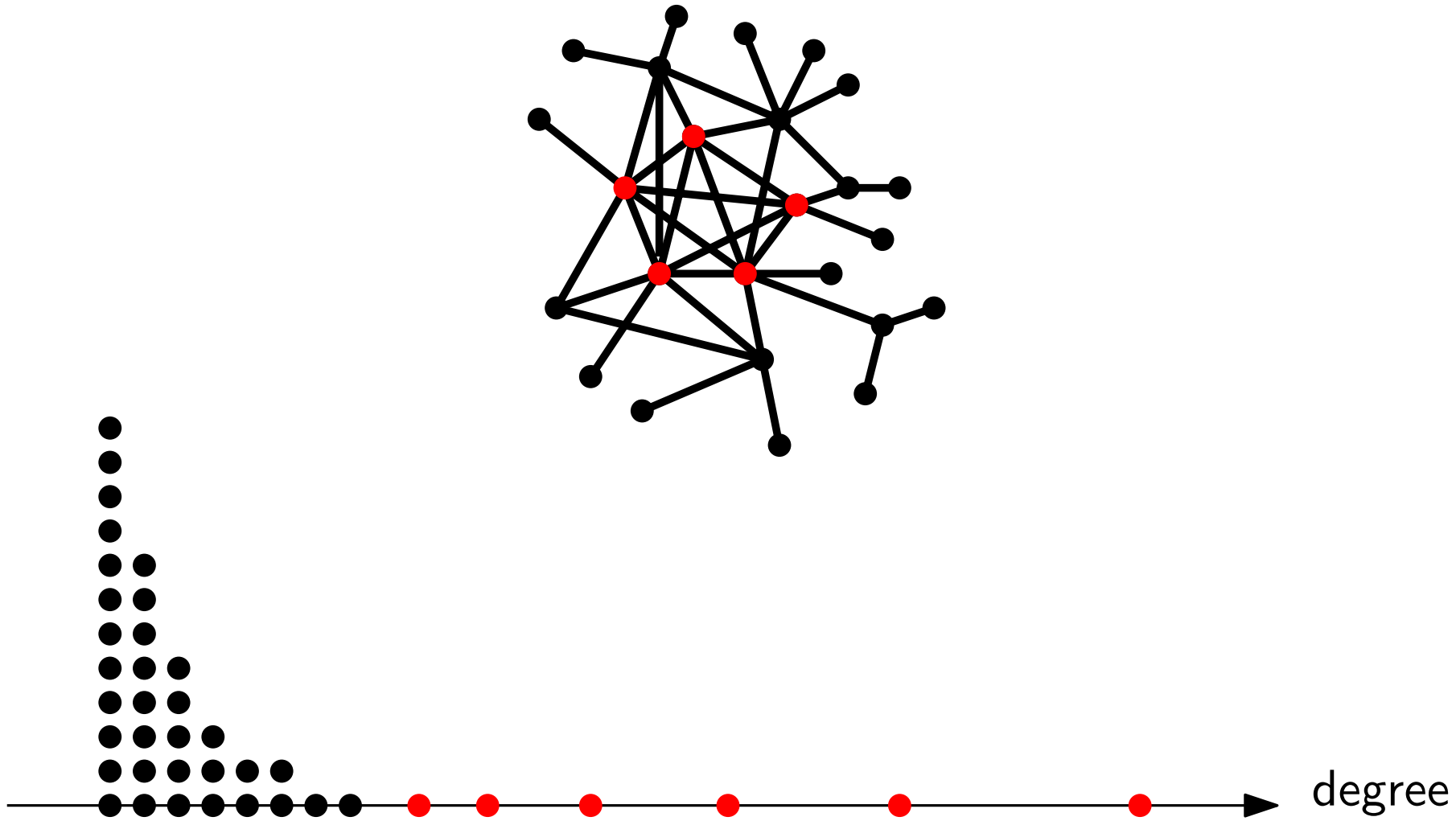


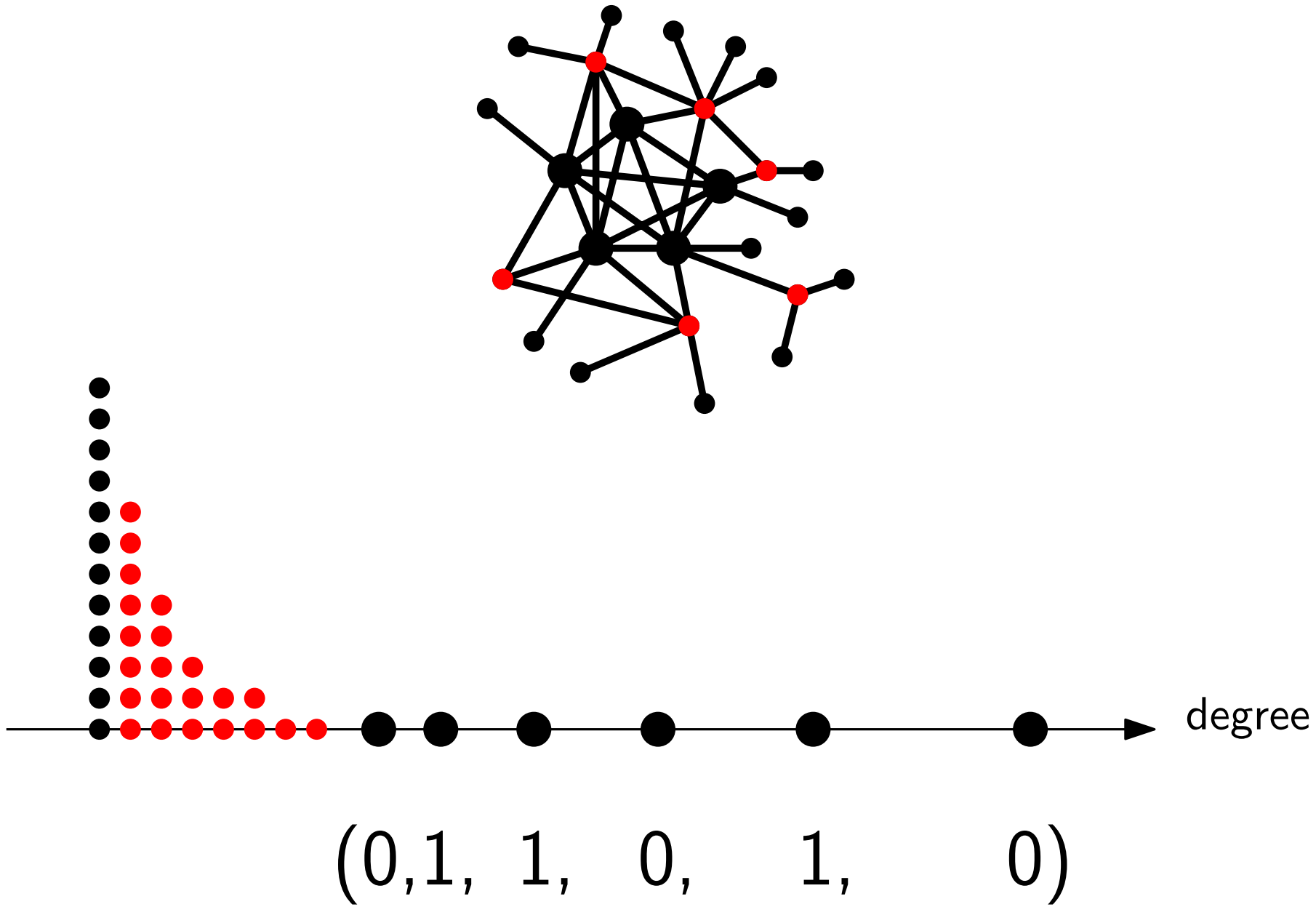


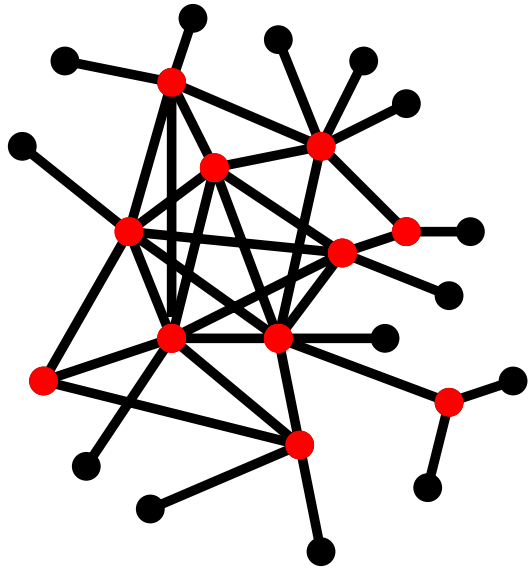

watermark!

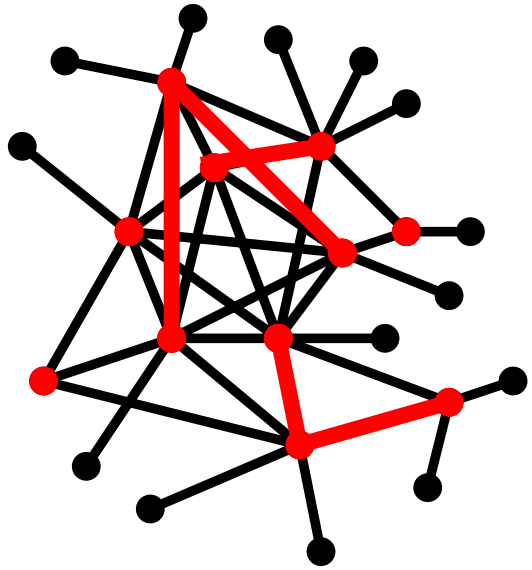

≃
?
watermark!

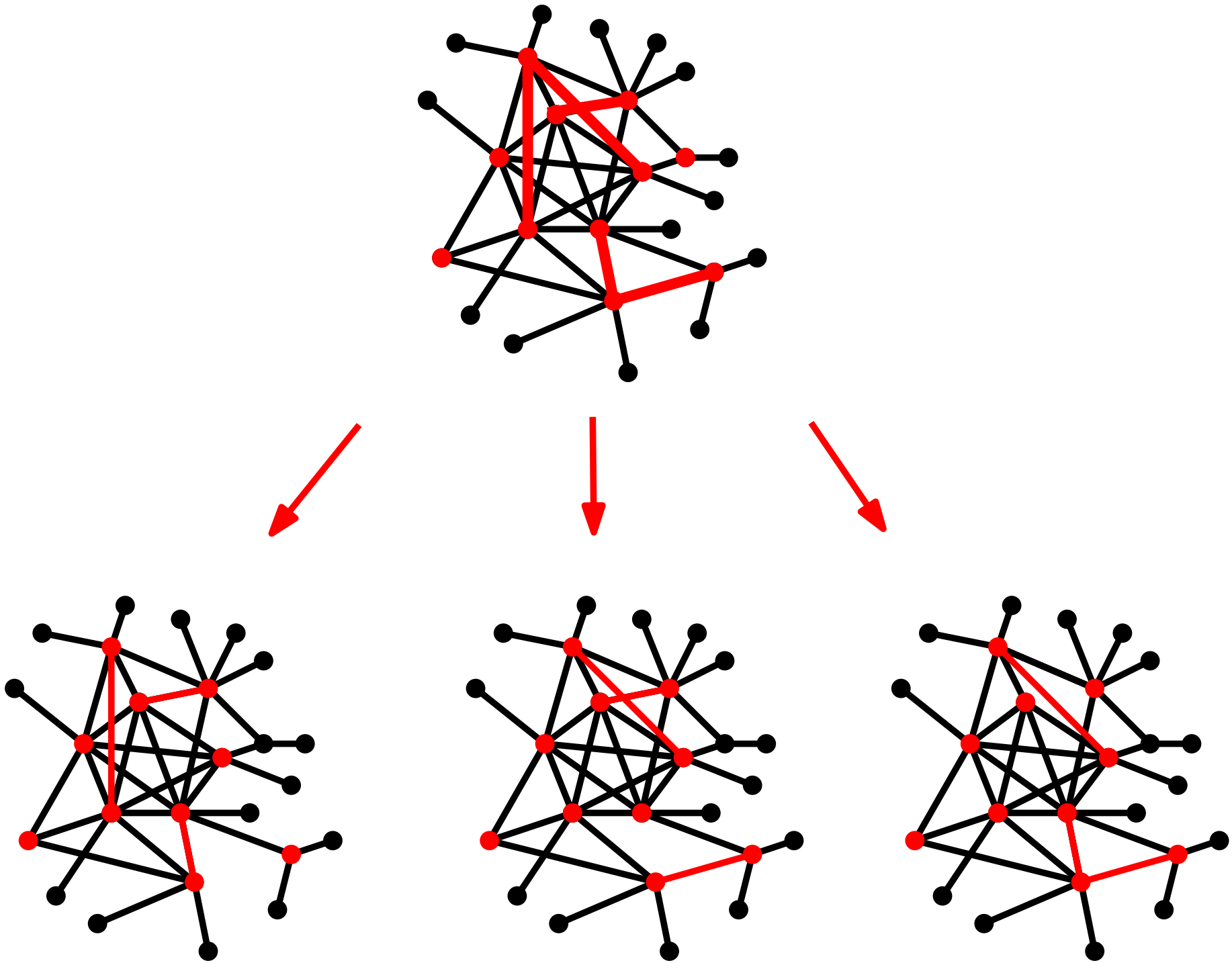
solution


degree


degree
(0,1, 1, 0, 1, 0)

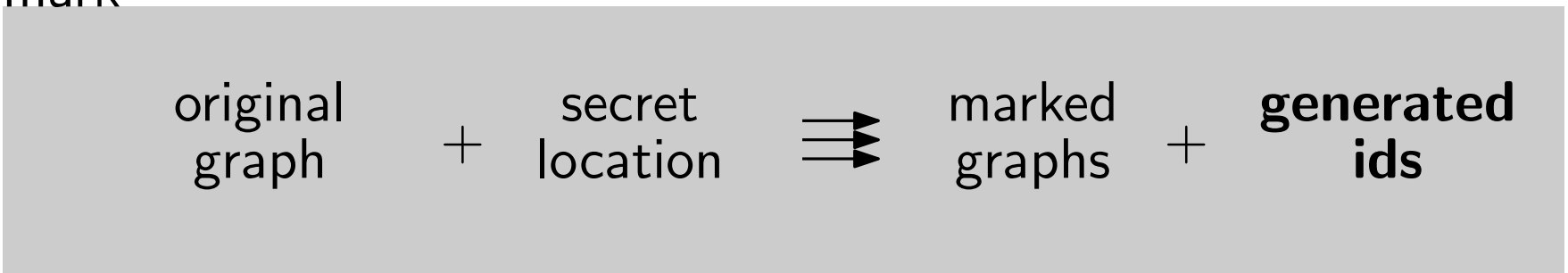




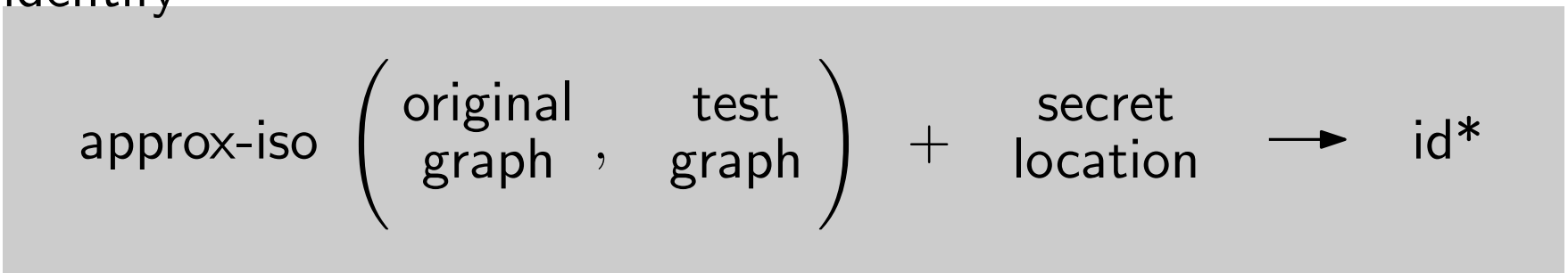


Watermarking scheme

mark

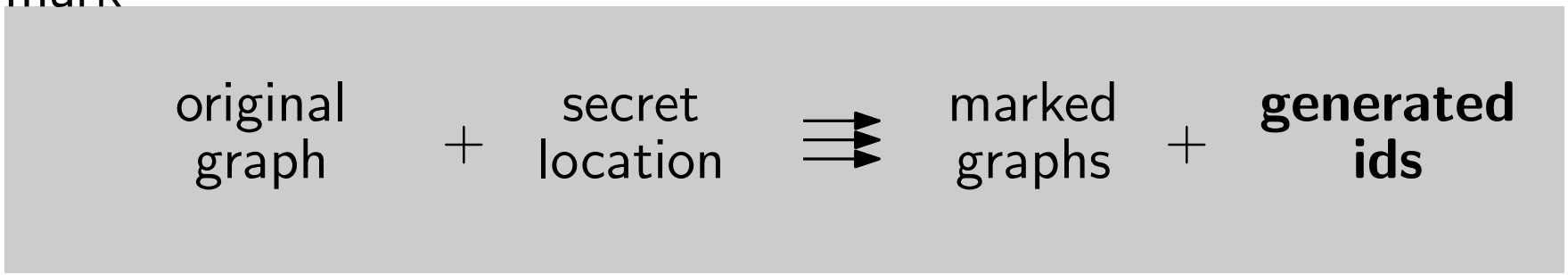


identify

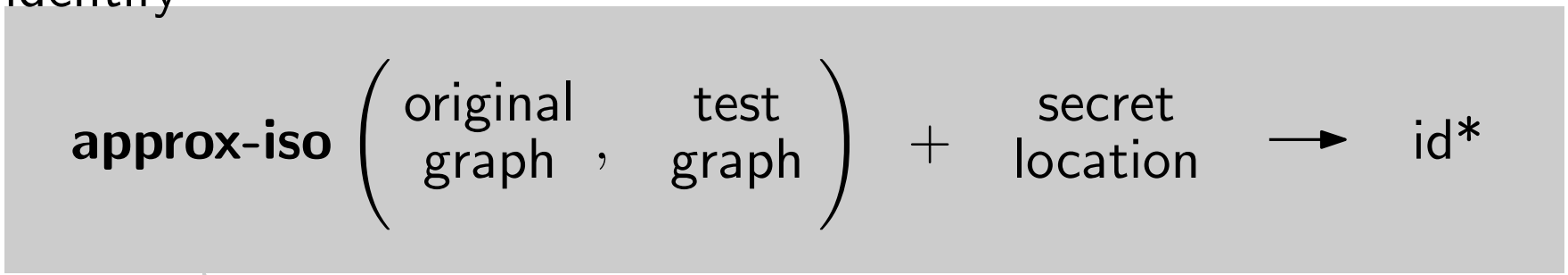


Watermarking scheme

mark



identify



high-degree

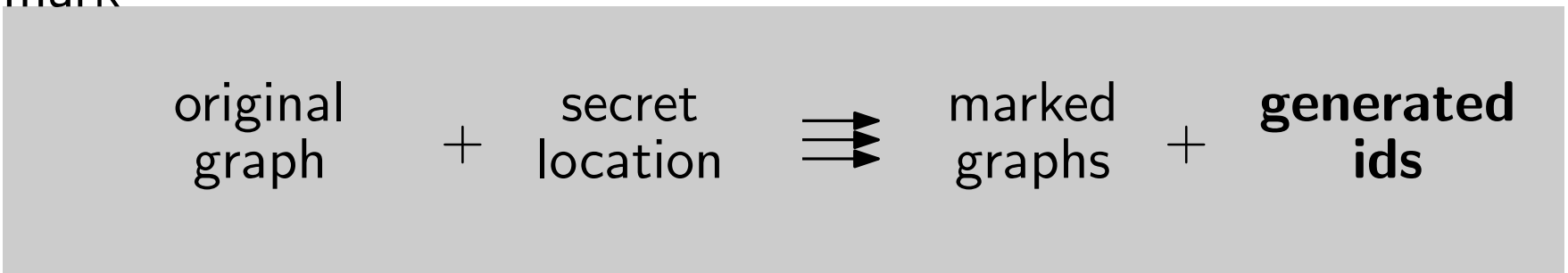
match by degree rank

medium-degree

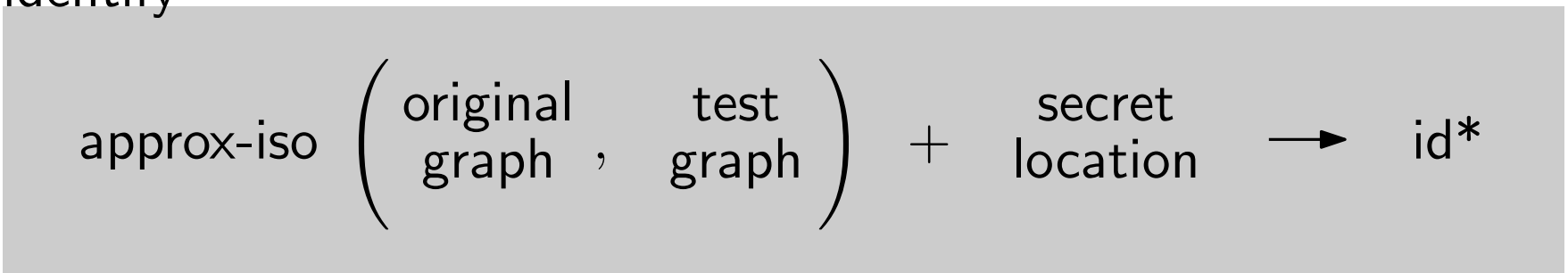
match closest pairs

Watermarking scheme

mark

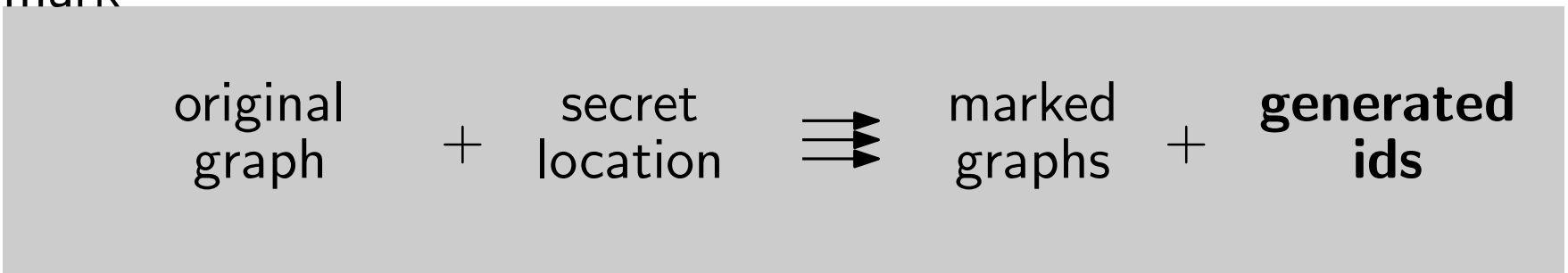


identify

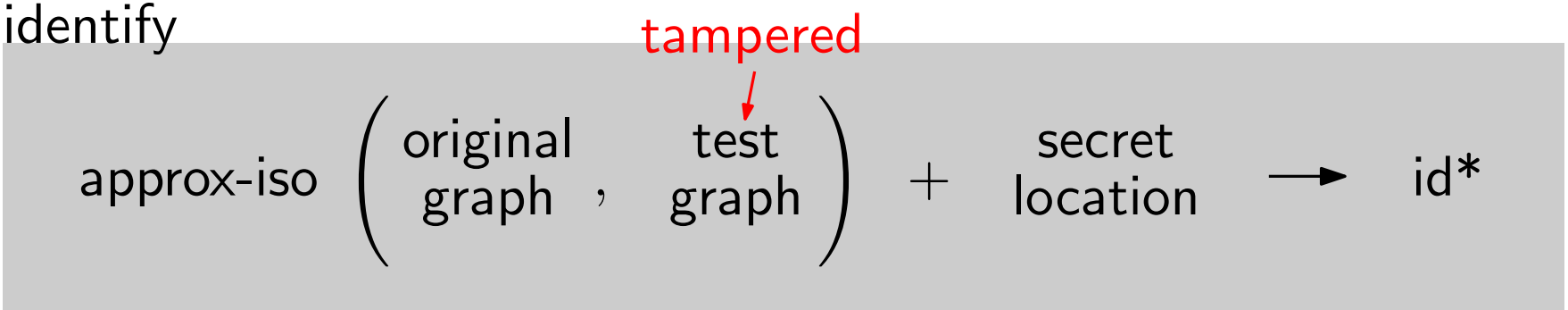


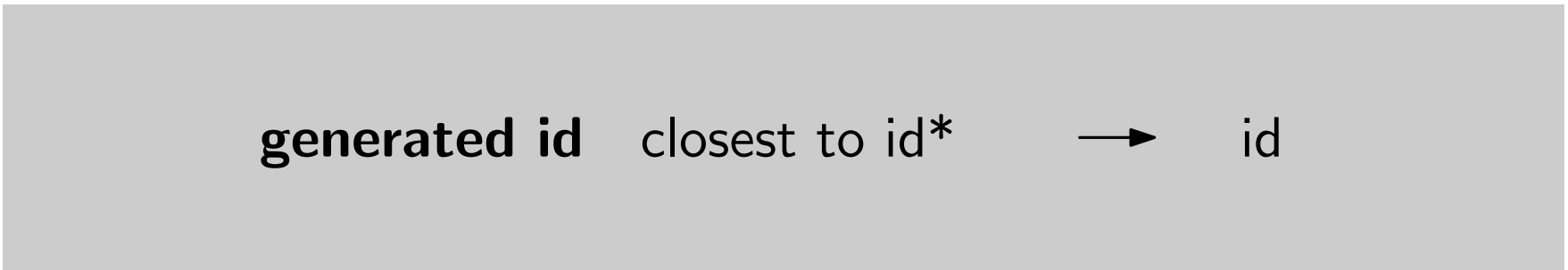
Watermarking scheme

mark



identify





evaluation

Security definition

experiment(adversary: $G \mapsto G'$)

random graph distribution $\longrightarrow G$

generate secret location

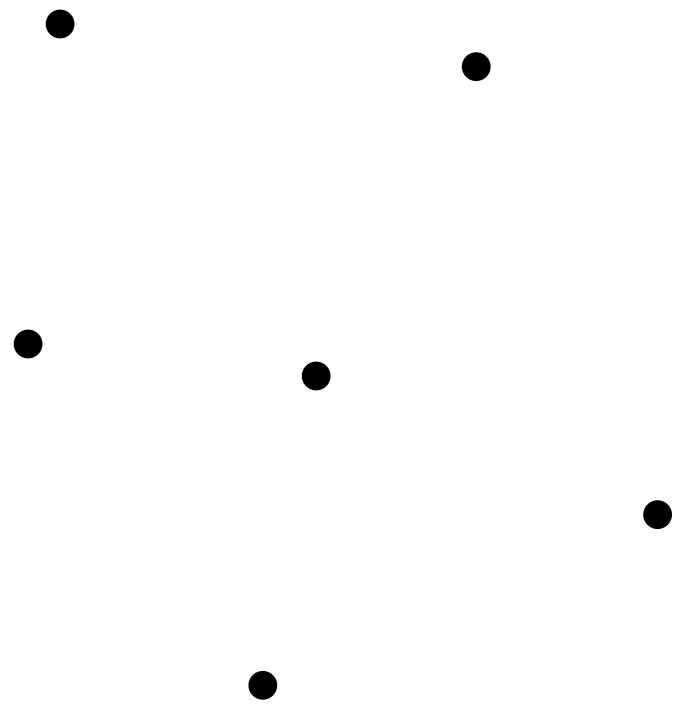
mark (G, secret location) $\longrightarrow (G_1, \mathrm{id}_1), \ldots (G_k, \mathrm{id}_k)$

$1, 2, \ldots k \longrightarrow j$

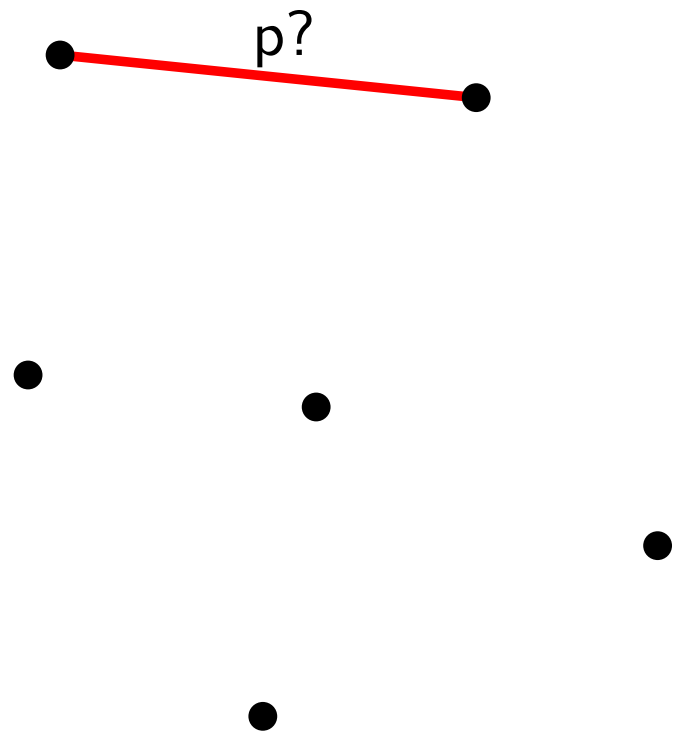
 (G_j) $\longrightarrow G'$

advantage of 

$$\Pr\left[\, \mathrm{dist}(G, G') \leq d, \quad \mathrm{identify}\left(G, G', \begin{matrix}\text{secret}\\ \text{location}'\end{matrix} \begin{matrix}\text{generated}\\ \text{ids}\end{matrix}\right)\right]$$

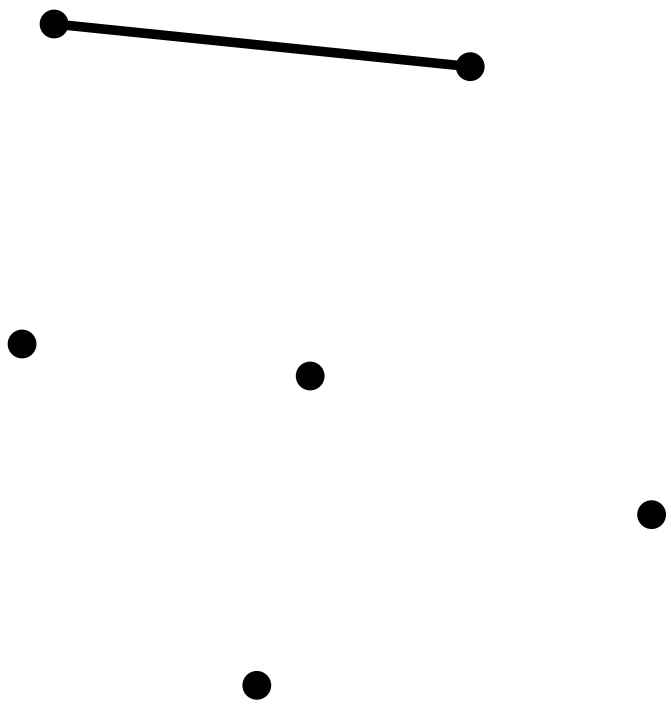


Erdös-Rényi
G(n, p)

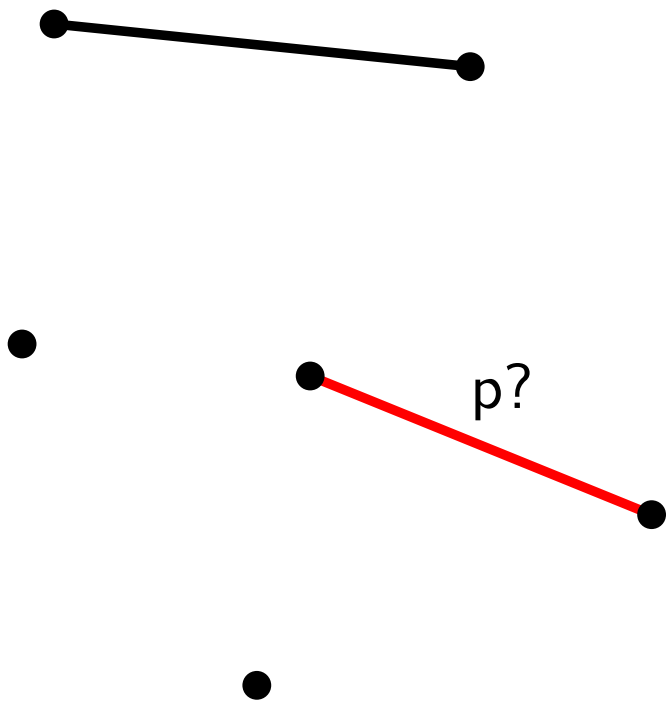


Erdös-Rényi

G(n, p)

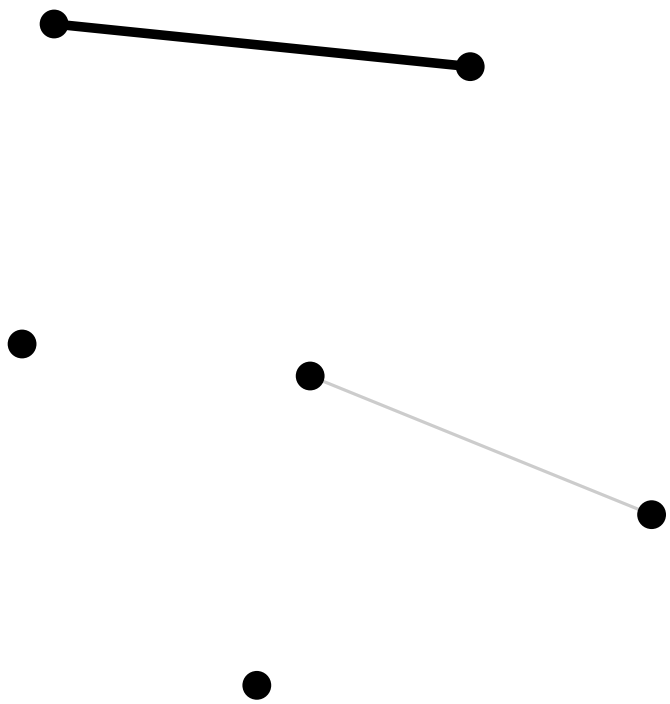


Erdös-Rényi
G(n, p)

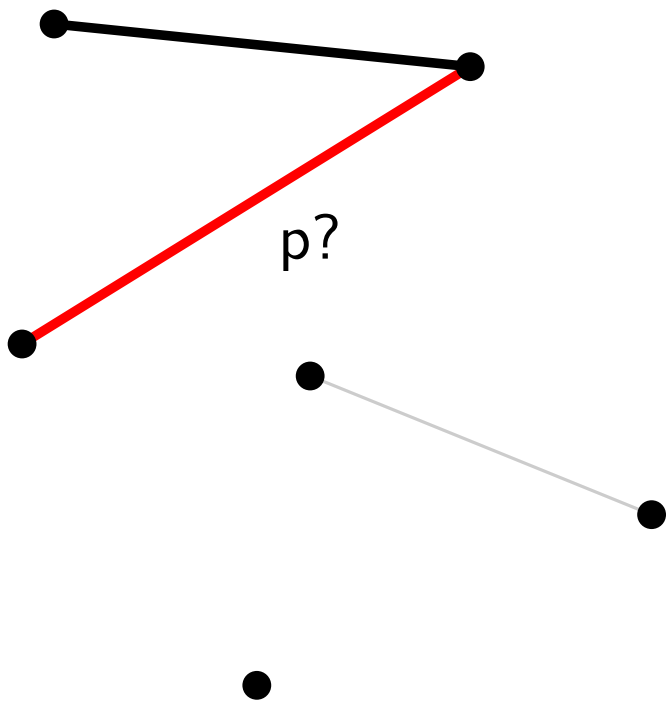


Erdös-Rényi

G(n, p)

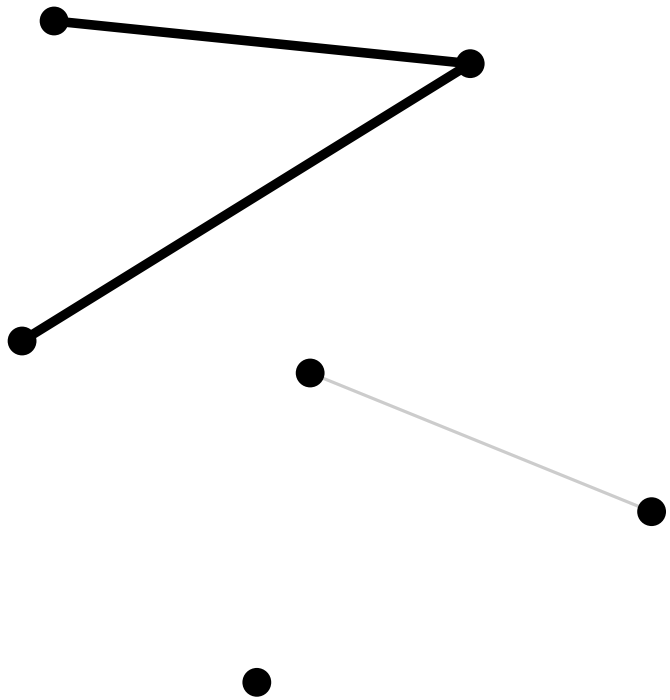


Erdös-Rényi
G(n, p)

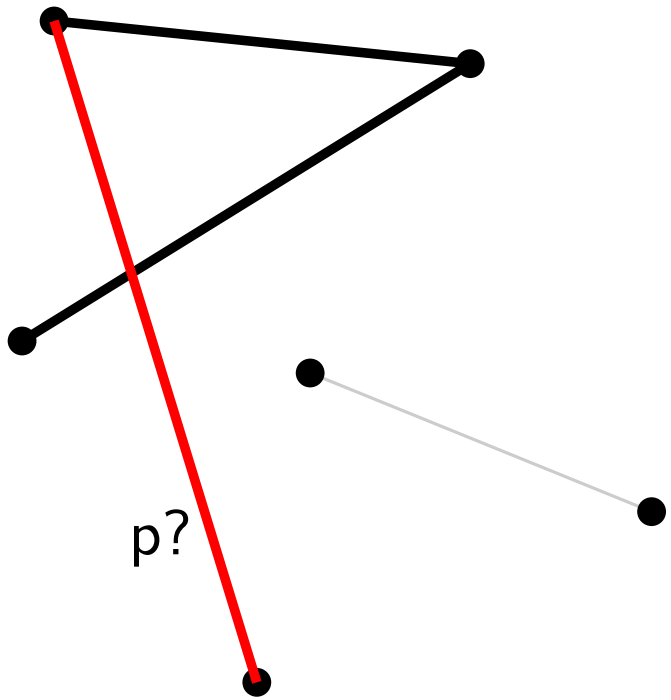


Erdös-Rényi

G(n, p)

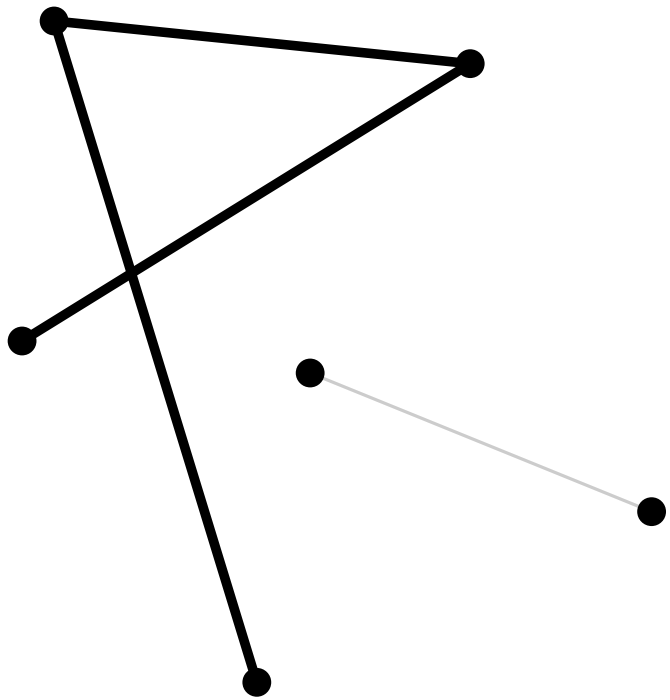


Erdös-Rényi
G(n, p)

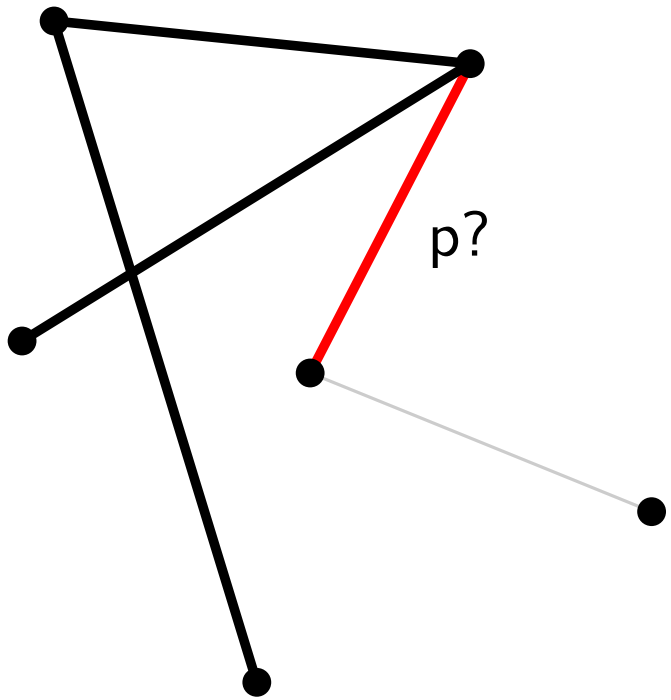


Erdös-Rényi

G(n, p)

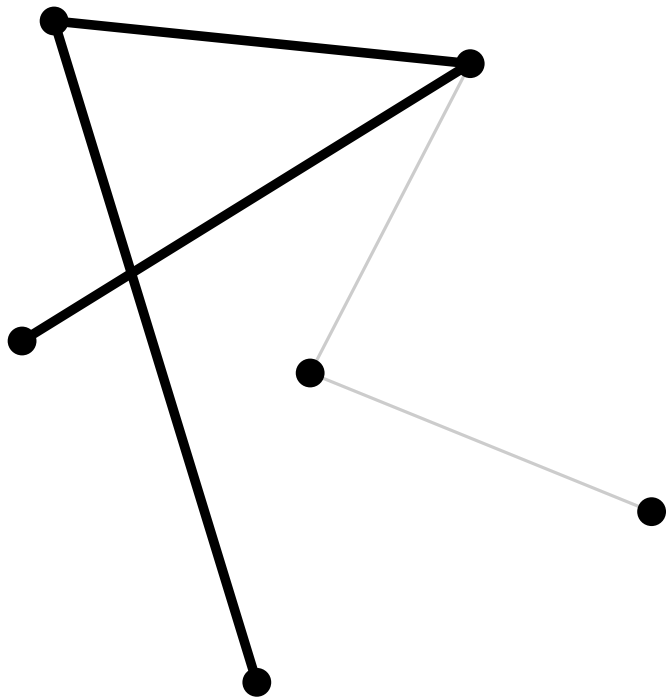


Erdös-Rényi
G(n, p)

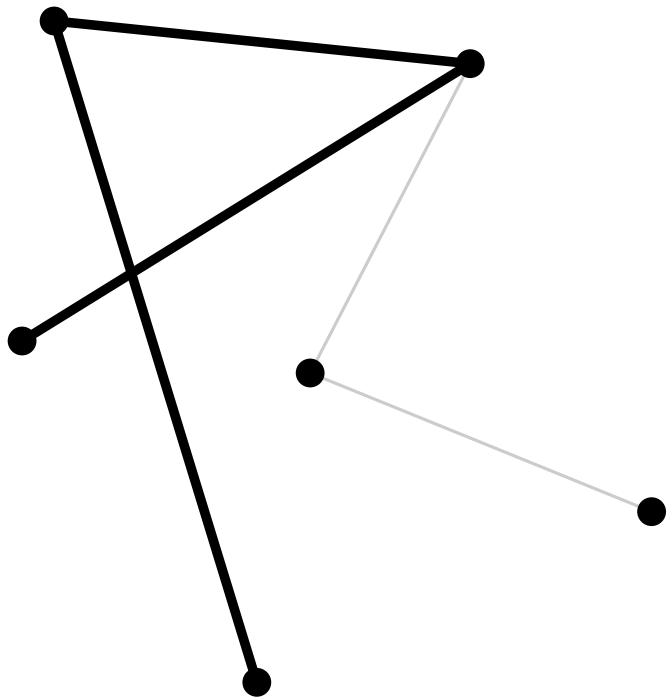


Erdös-Rényi

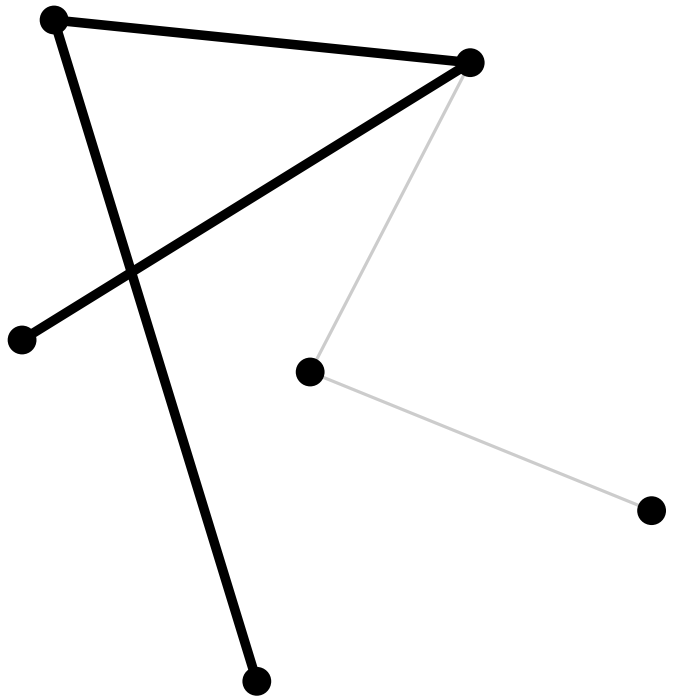
G(n, p)



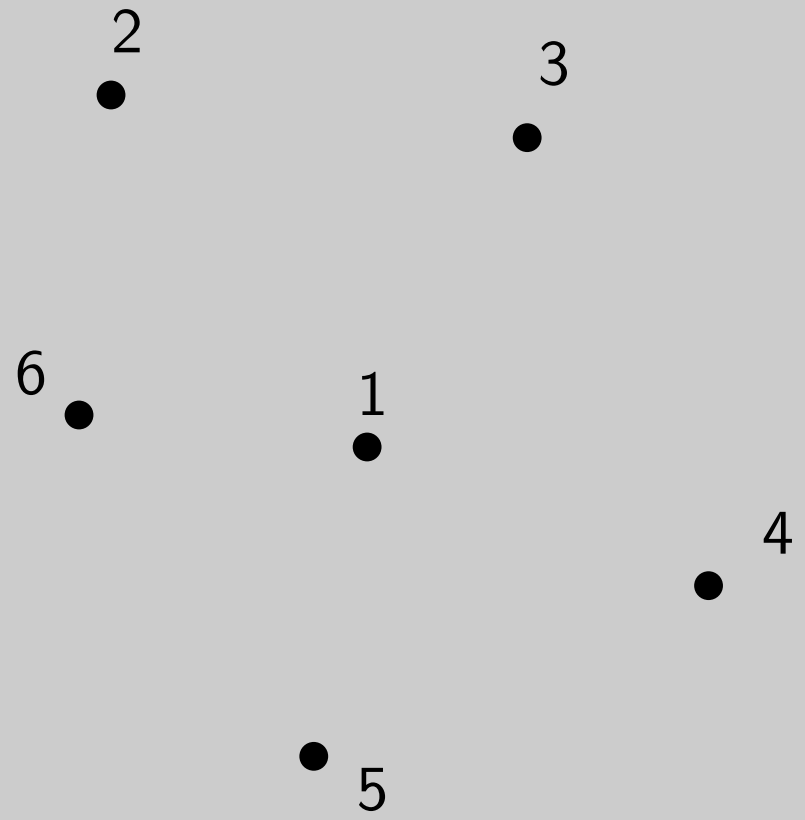
Erdös-Rényi
G(n, p)



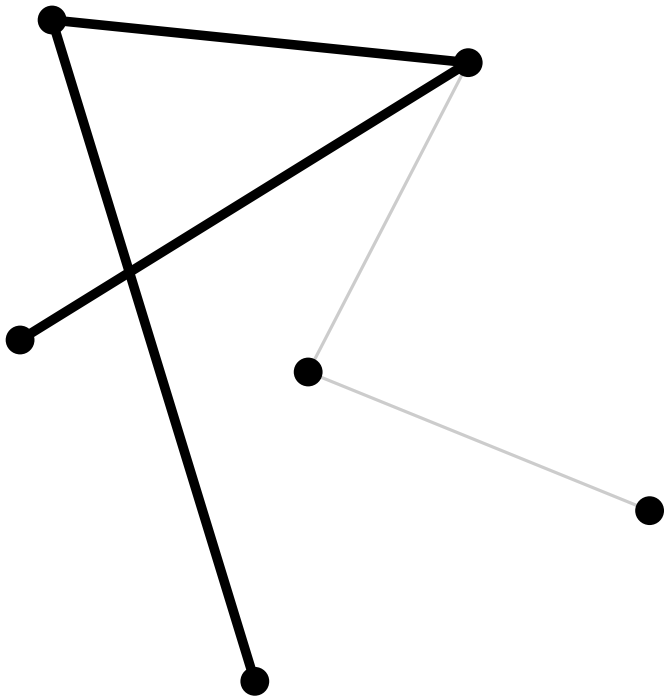
Erdös-Rényi
G(n, p)



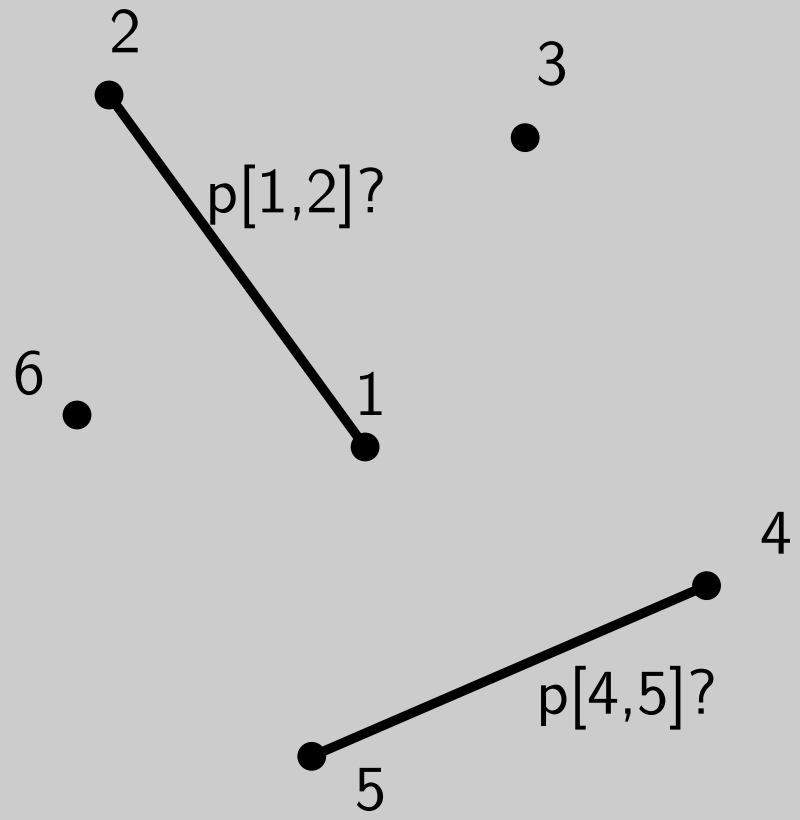
Erdös-Rényi
G(n, p)



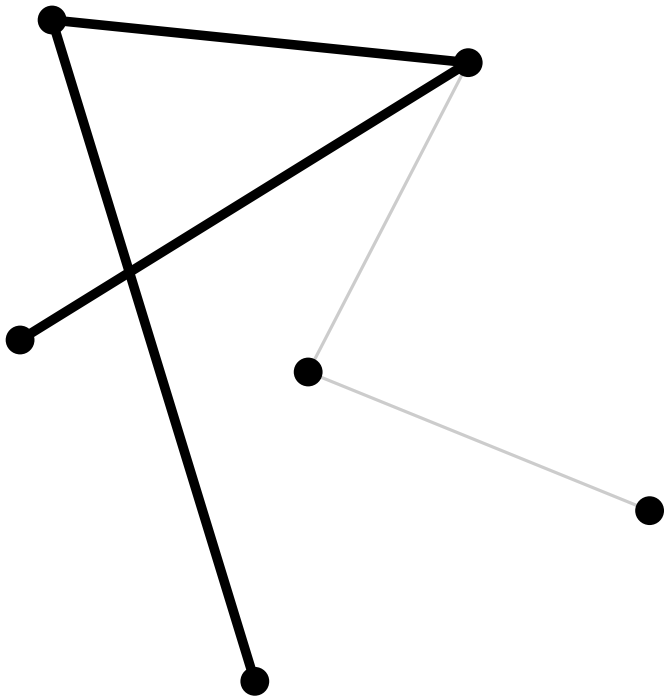
Rand power-law graph
G(w^{γ})



Erdös-Rényi
G(n, p)

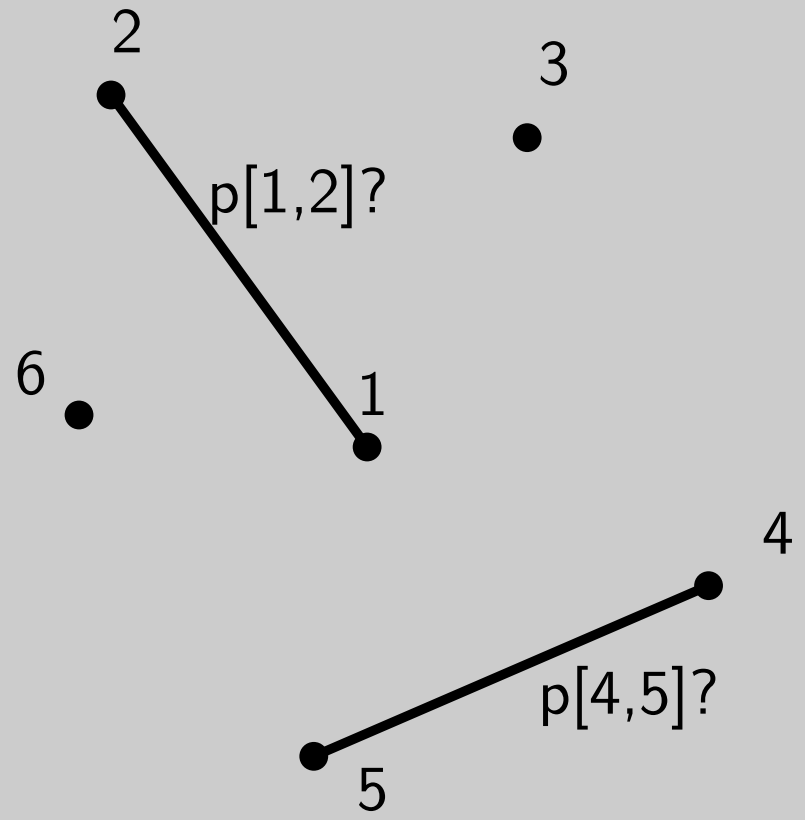


Rand power-law graph
G(w^{γ})



Erdös-Rényi
G(n, p)

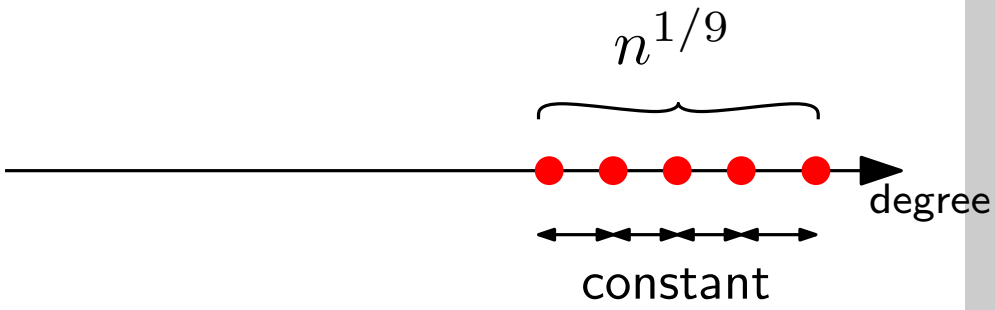
$$p[i,j] \sim \left(\frac{1}{n^{\gamma-3}ij}\right)^{\frac{1}{\gamma-1}}$$

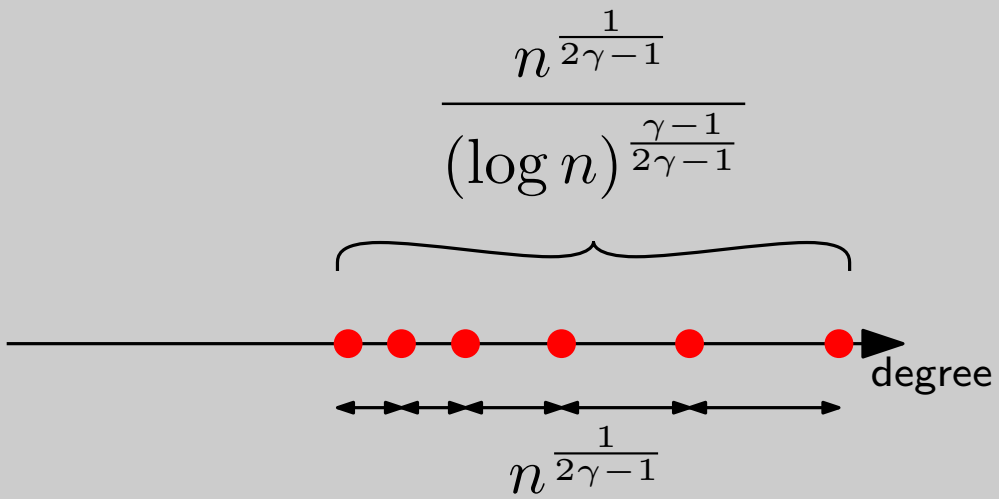


Rand power-law graph
G(w^{γ})

Separation of vertex labels

Separation of vertex labels

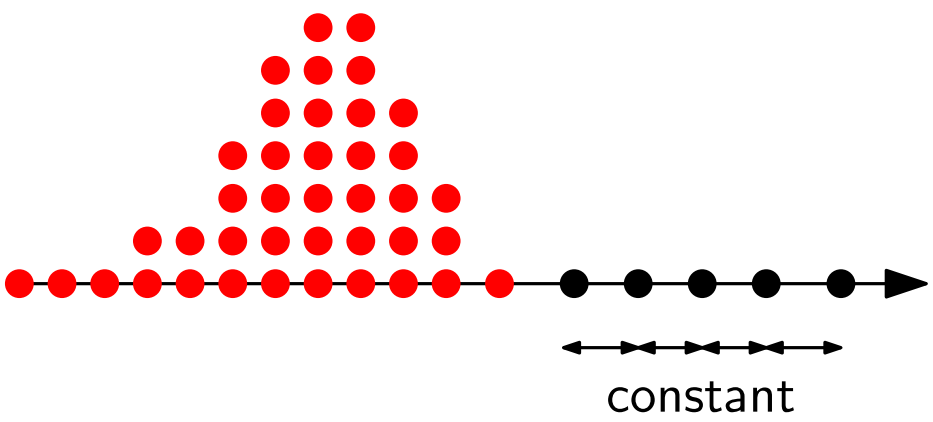


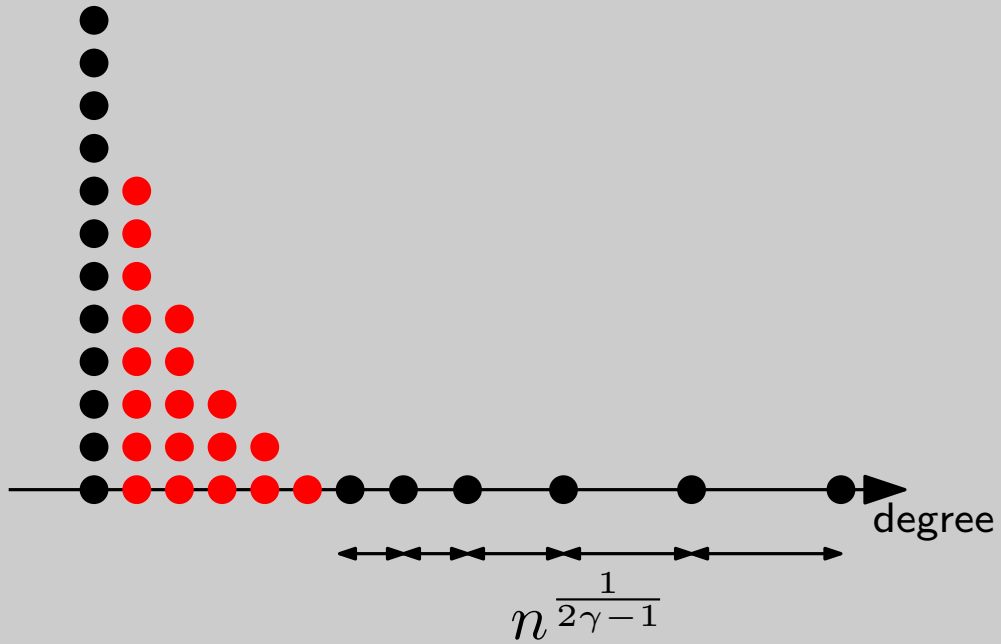


Erdos-Renyi
G(n, p)

Rand power-law graph
G(w$^{\gamma}$)

Separation of vertex labels

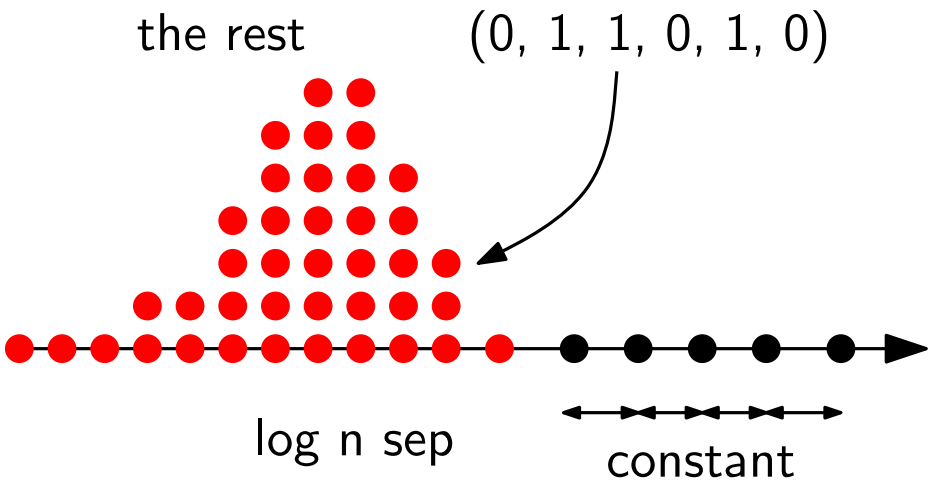




Erdos-Renyi G(n, p)

Rand power-law graph $G(w^{\gamma})$

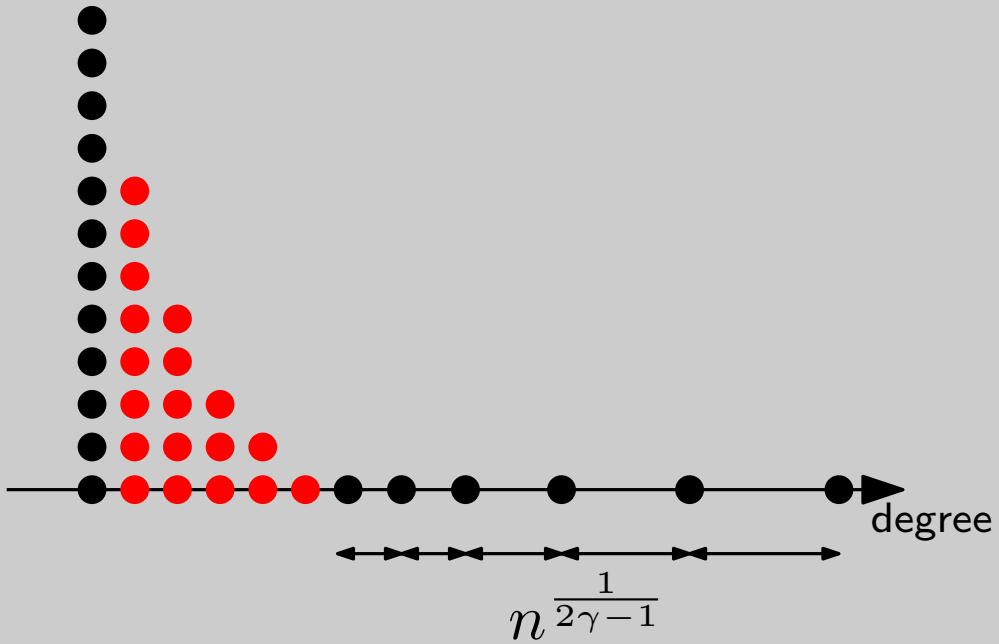
Separation



$$p = \omega(n^{-\epsilon} \log n)$$

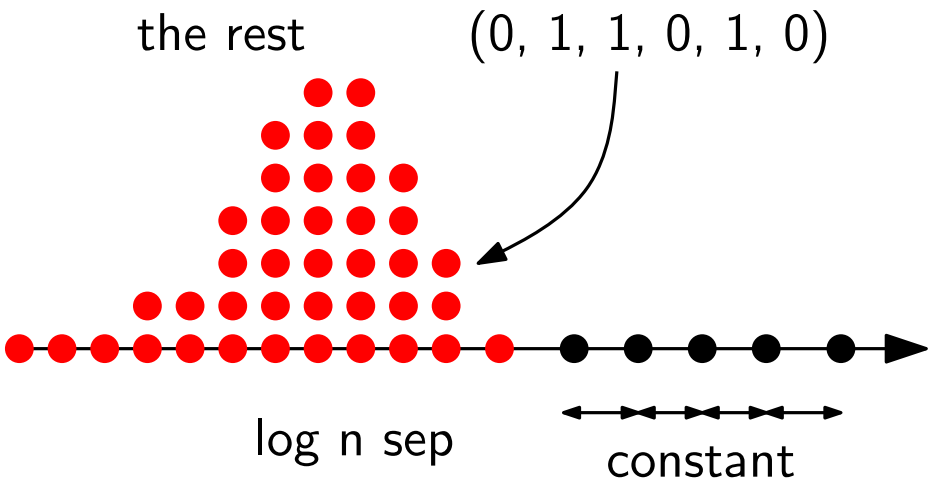
Erdos-Renyi
G(n, p)

of vertex labels



Rand power-law graph
G(w^{γ})

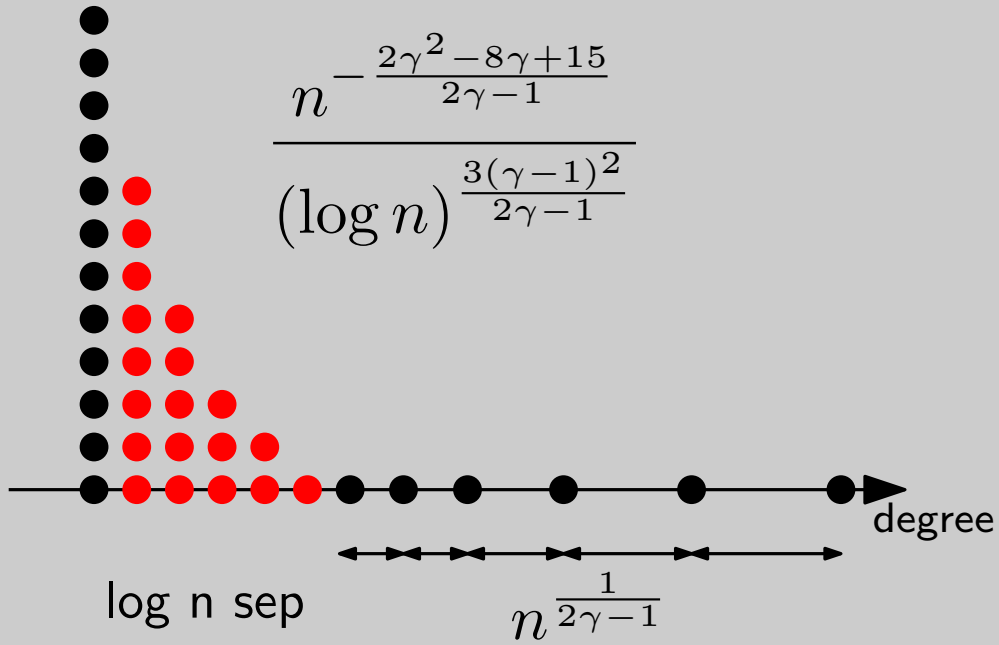
Separation



$$p = \omega(n^{-\epsilon} \log n)$$

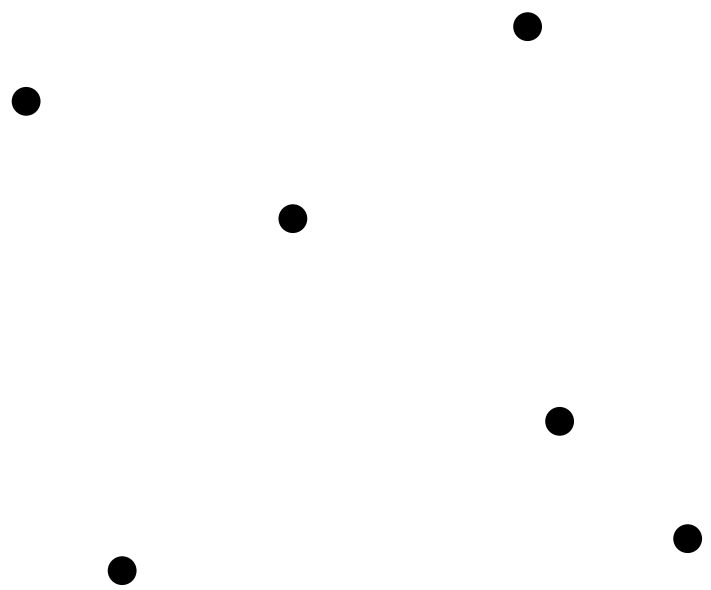
Erdos-Renyi
G(n, p)

of vertex labels

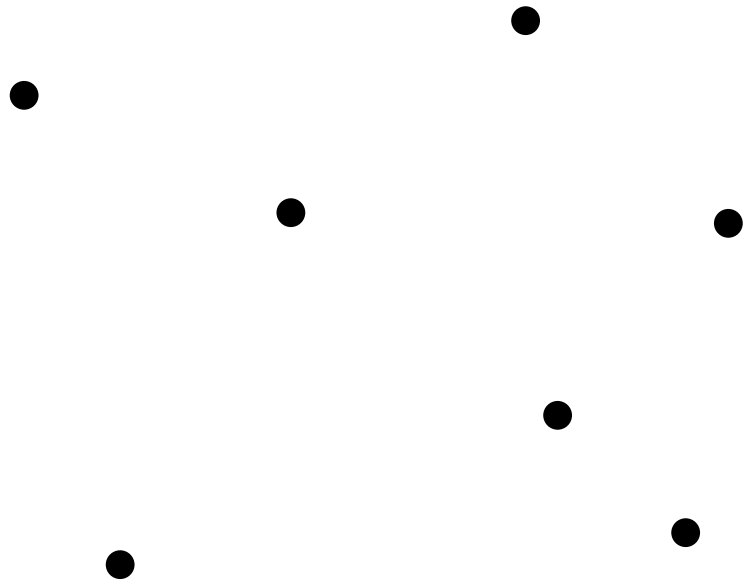


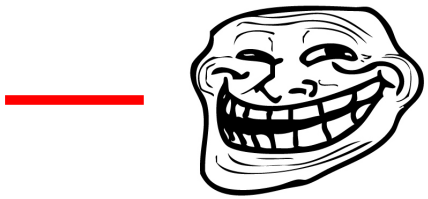
Rand power-law graph
G(w^{γ})

It's hard to guess the secret location



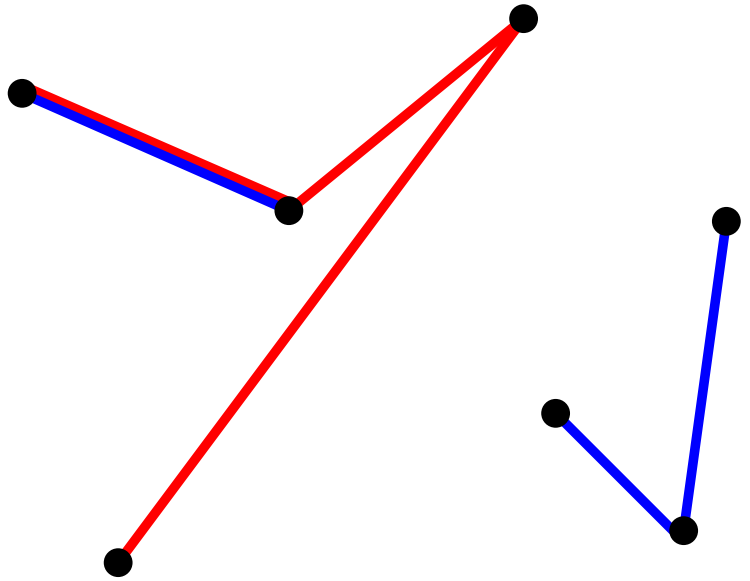
It's hard to guess the secret location

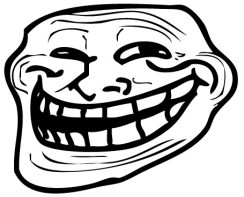




secret location

It's hard to guess the secret location



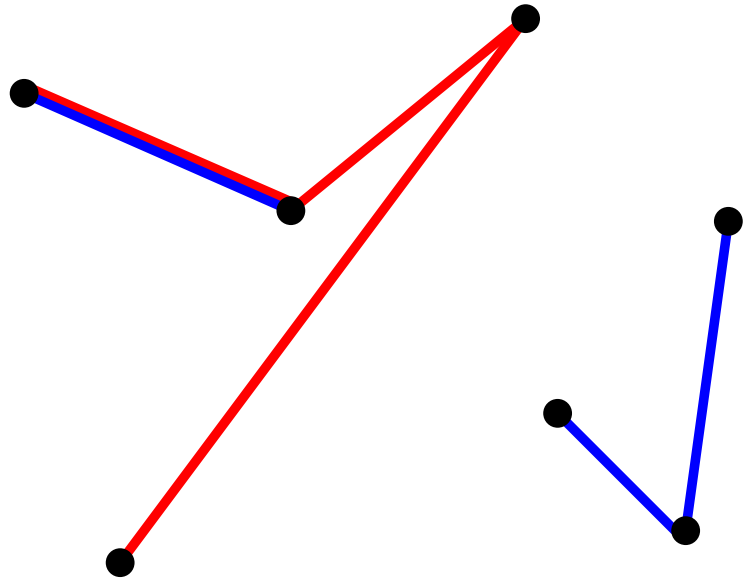


secret location

degree constraint

no more than t edges incident to any vertex

It's hard to guess the secret location



secret location

degree constraint

no more than t edges
incident to any vertex

$\ell \ll N$ Pr [secret location contains $8\ell r/N^2$ red edges] is small

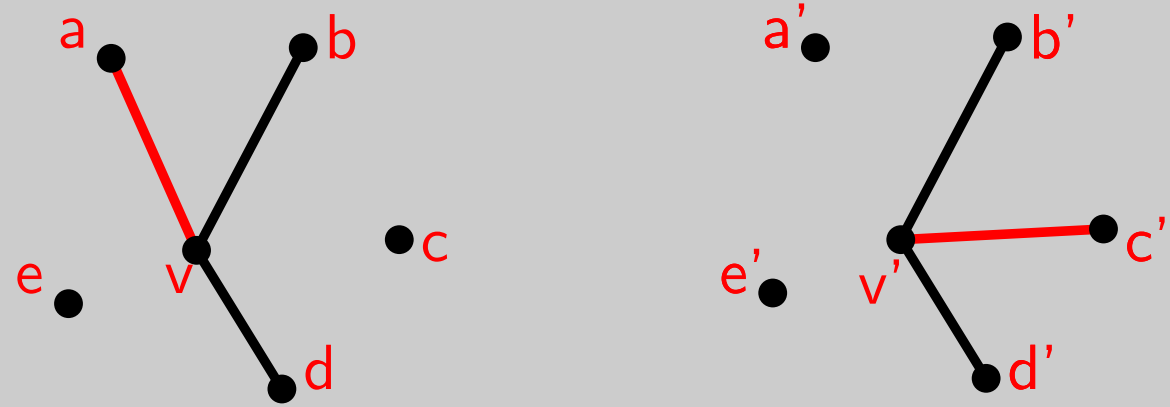
$\frac{\ell r}{N^2} \longrightarrow 0$ Pr [secret location contains 1 red edge] is small

Distance between graphs

graph edit distance

min number of edges to flip to go from G to H

vertex distance



min (over mappings) max(#edges/vertex to flip, G to H)

Security definition

experiment(adversary: $G \mapsto G'$)

random graph distribution $\longrightarrow G$

generate secret location

mark (G, secret location) $\longrightarrow (G_1, \mathrm{id}_1), \ldots (G_k, \mathrm{id}_k)$

$1, 2, \ldots k \longrightarrow j$

 (G_j) $\longrightarrow G'$

advantage of 

$$\Pr\left[\, \mathrm{dist}(G, G') \leq d, \quad \mathrm{identify}\left(G, G', \begin{matrix}\text{secret}\\ \text{location}'\end{matrix} \begin{matrix}\text{generated}\\ \text{ids}\end{matrix}\right)\right]$$

Security definition

edge flipper

experiment(adversary: $G \mapsto G'$)

random graph distribution $\longrightarrow G$

generate secret location

mark (G, secret location) $\longrightarrow (G_1, \mathrm{id}_1), \ldots (G_k, \mathrm{id}_k)$

$1, 2, \ldots k \longrightarrow j$

 (G_j) $\longrightarrow G'$

advantage of 

$$\Pr\left[\, \mathrm{dist}(G, G') \leq d, \quad \mathrm{identify}\left(G, G', \begin{matrix}\text{secret}\\ \text{location}'\end{matrix}, \begin{matrix}\text{generated}\\ \text{ids}\end{matrix}\right)\right]$$

Security definition

edge flipper

experiment(adversary: $G \mapsto G'$)

random graph distribution $\longrightarrow$ G G(n,p) or G(w^{γ})

generate secret location

mark (G, secret location) $\longrightarrow$ (G_1, id_1), . . . (G_k, id_k)

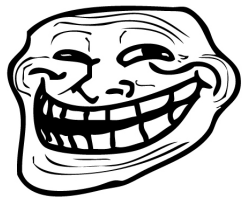
1, 2, . . . k $\longrightarrow$ j

(G_j) $\longrightarrow$ G'

advantage of 

$$\Pr\left[\text{dist}(G, G') \leq d, \quad \text{identify}\left(G, G', \begin{matrix}\text{secret} \\ \text{location'}\end{matrix} \quad \begin{matrix}\text{generated} \\ \text{ids}\end{matrix}\right)\right]$$

Security definition



edge flipper

experiment(adversary: $G \mapsto G'$)

random graph distribution $\longrightarrow$ G — G(n,p) or G(w^{γ})

generate secret location — small, degree constraint

mark (G, secret location) $\longrightarrow$ $(G_1, id_1), \ldots (G_k, id_k)$

$1, 2, \ldots k \longrightarrow j$

 (G_j) $\longrightarrow$ G'

advantage of 

$$\Pr\left[\text{dist}(G, G') \leq d, \quad \text{identify}\left(G, G', \begin{matrix}\text{secret} \\ \text{location}'\end{matrix} \quad \begin{matrix}\text{generated} \\ \text{ids}\end{matrix}\right)\right]$$

Security definition

edge flipper

experiment(adversary: $G \mapsto G'$)

random graph distribution $\longrightarrow$ G — G(n,p) or G(w^{γ})

generate secret location — small, degree constraint

mark (G, secret location) $\longrightarrow$ $(G_1, id_1), \ldots (G_k, id_k)$

1, 2, ... k $\longrightarrow$ j

 (G_j) $\longrightarrow$ G'

advantage of 

$$\Pr\left[\text{dist}(G, G') \leq d, \quad \text{identify}\left(G, G', \begin{matrix}\text{secret}\\ \text{location}'\end{matrix} \quad \begin{matrix}\text{generated}\\ \text{ids}\end{matrix}\right)\right]$$

graph edit distance

vertex distance

Erdos-Renyi G(n, p)

secret location	
edges	dn
edges/vertex	d
adversary	
edges	dn
edges/vertex	d
marked graphs	poly(n)

Rand power-law graph $G(w^{\gamma})$

secret location	
edges	log n / p
edges/vertex	log n
adversary	
edges	p (# identifiable vertices)^2
edges/vertex	log n
marked graphs	poly (n)

Erdos-Renyi G(n, p)

secret location

edges	dn
edges/vertex	d

adversary

edges	dn
edges/vertex	d

marked graphs poly(n)

Rand power-law graph $G(w^{\gamma})$

secret location

edges	log n / p
edges/vertex	log n

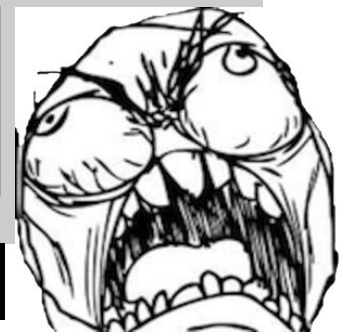
adversary

edges	p (# identifiable vertices)^2
edges/vertex	log n

marked graphs poly (n)

advantage of 

$$\Pr\left[\text{dist}(G, G') \leq d, \quad \text{identify}\left(G, G', \underset{\text{location}}{\text{secret}}, \underset{\text{ids}}{\text{generated}}\right)\right]$$



small

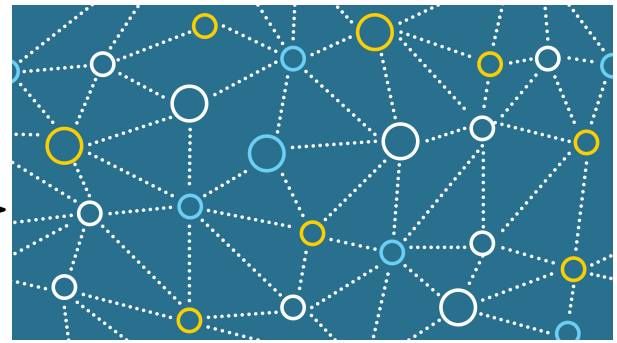
future work

Experiments

real-world network

Experiments

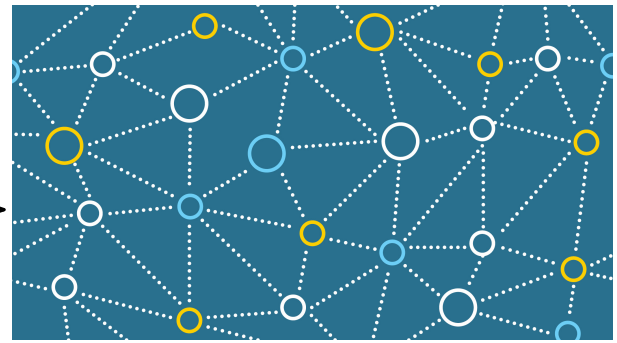
real-world network



random power-law model

Experiments

real-world network



random power-law model

experiments