CRYPTOGRAPHY FROM PLANTED GRAPHS:

SECURITY WITH LOG-SIZED MESSAGES

DAMIANO ABRAM

AMOS BEIMEL

YUVAL ISHAI

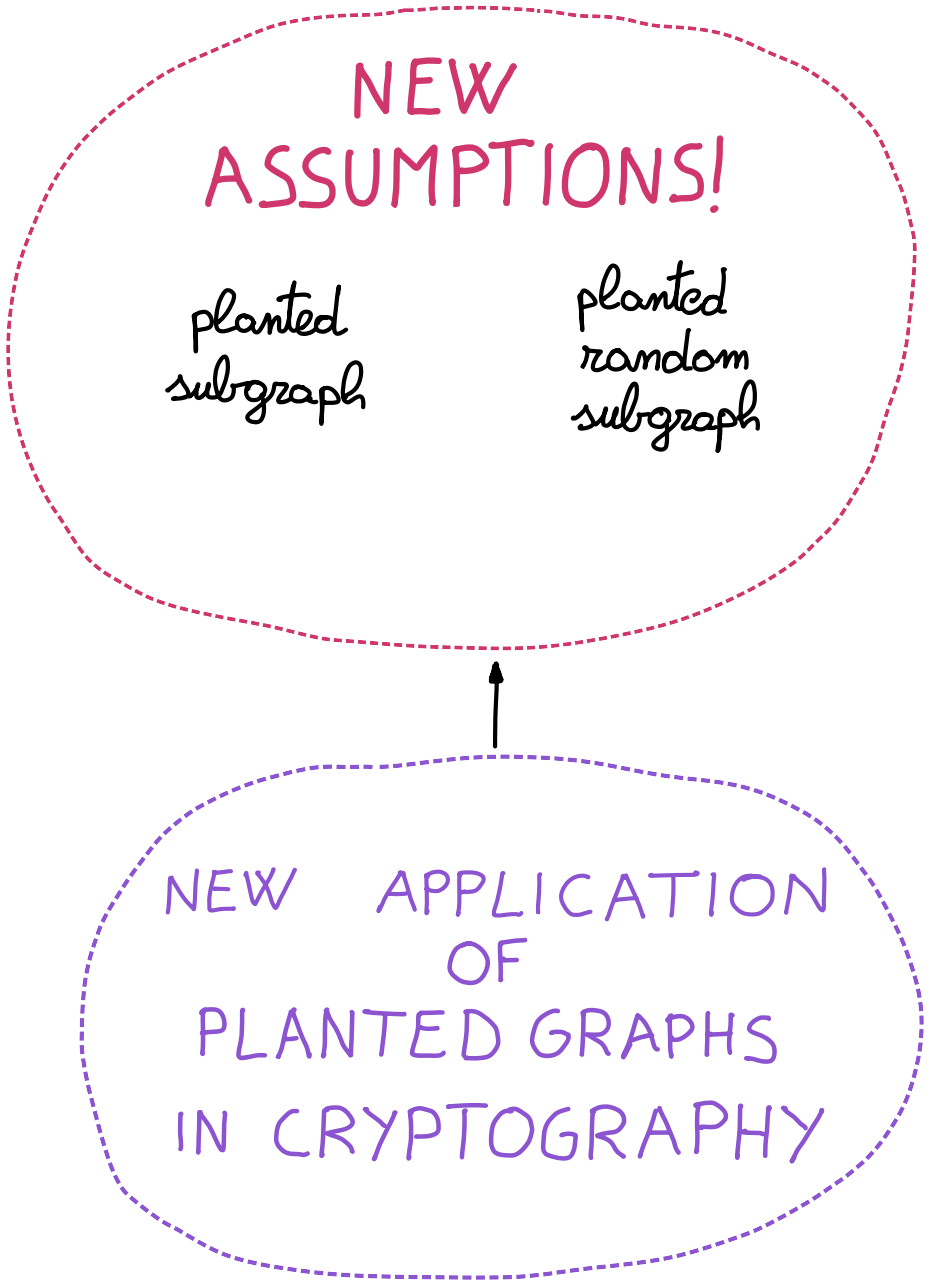
EYAL KUSHILEVITZ

VARUN NARAYANAN

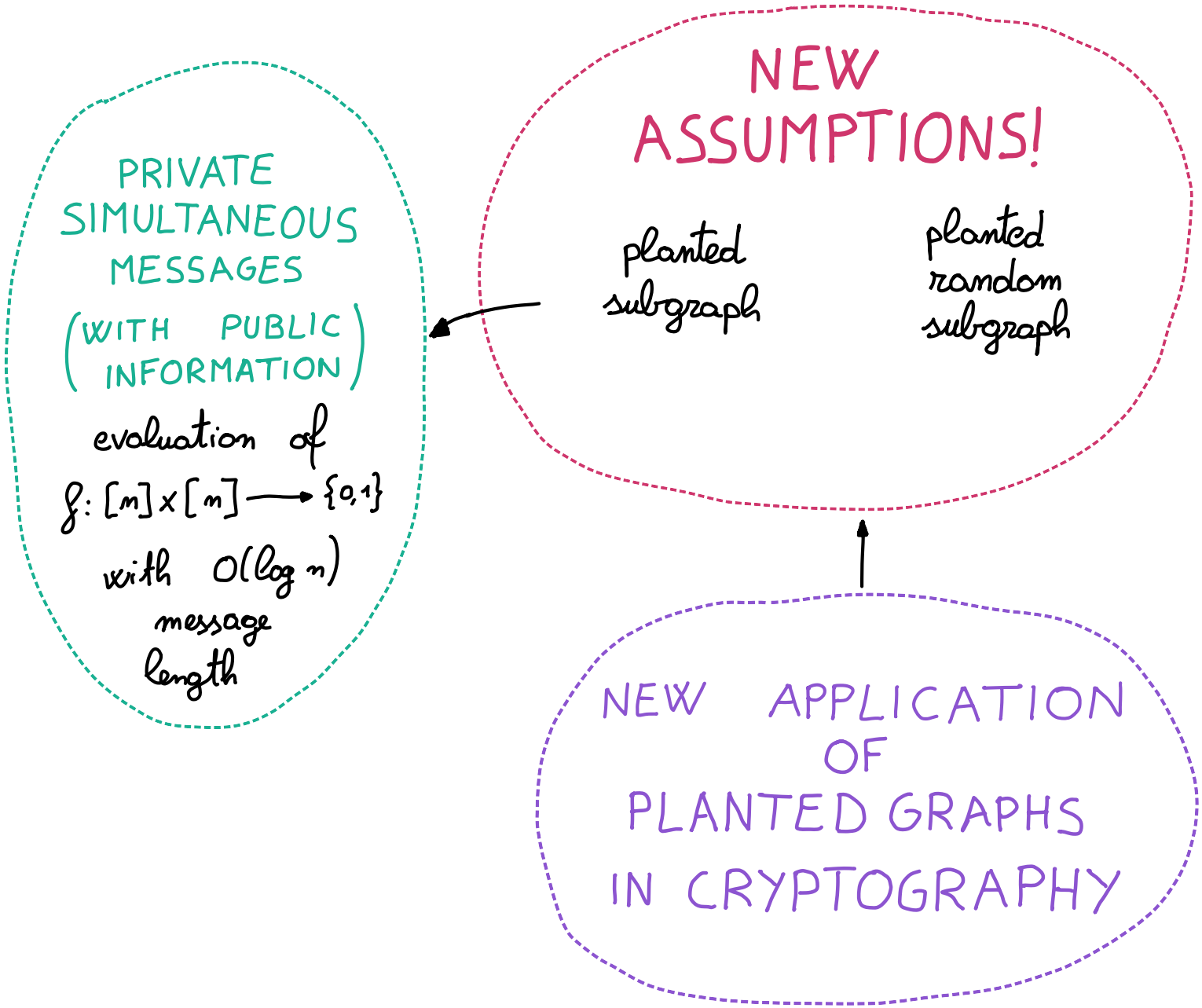
CONTRIBUTIONS

NEW APPLICATION
OF
PLANTED GRAPHS
IN CRYPTOGRAPHY

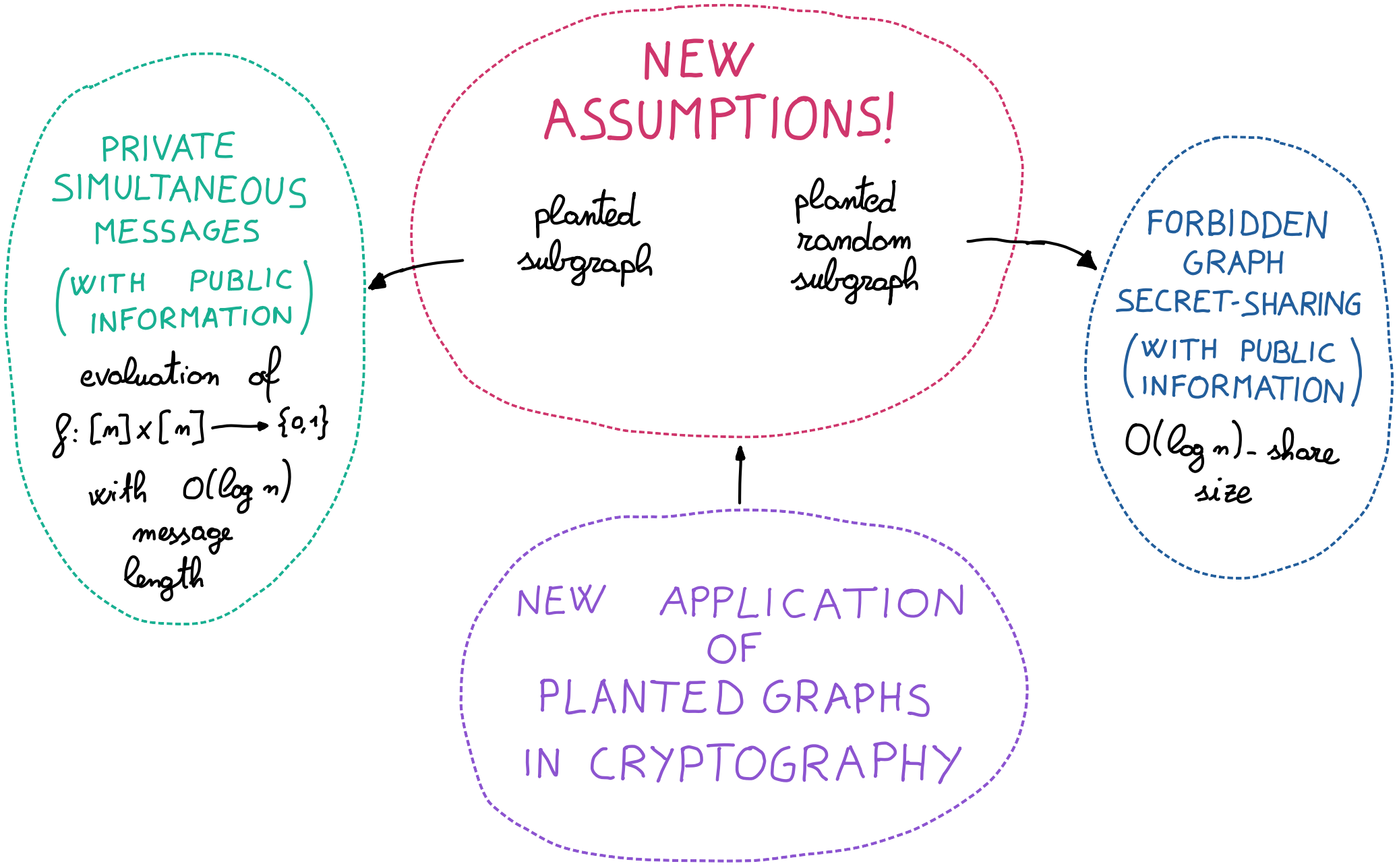
CONTRIBUTIONS



CONTRIBUTIONS



CONTRIBUTIONS



CONTRIBUTIONS

NEW ASSUMPTIONS!

planted subgraph

planted random subgraph

PRIVATE SIMULTANEOUS MESSAGES (WITH PUBLIC INFORMATION)

evaluation of $f: [n] \times [n] \longrightarrow \{0,1\}$ with $O(\log n)$ message length

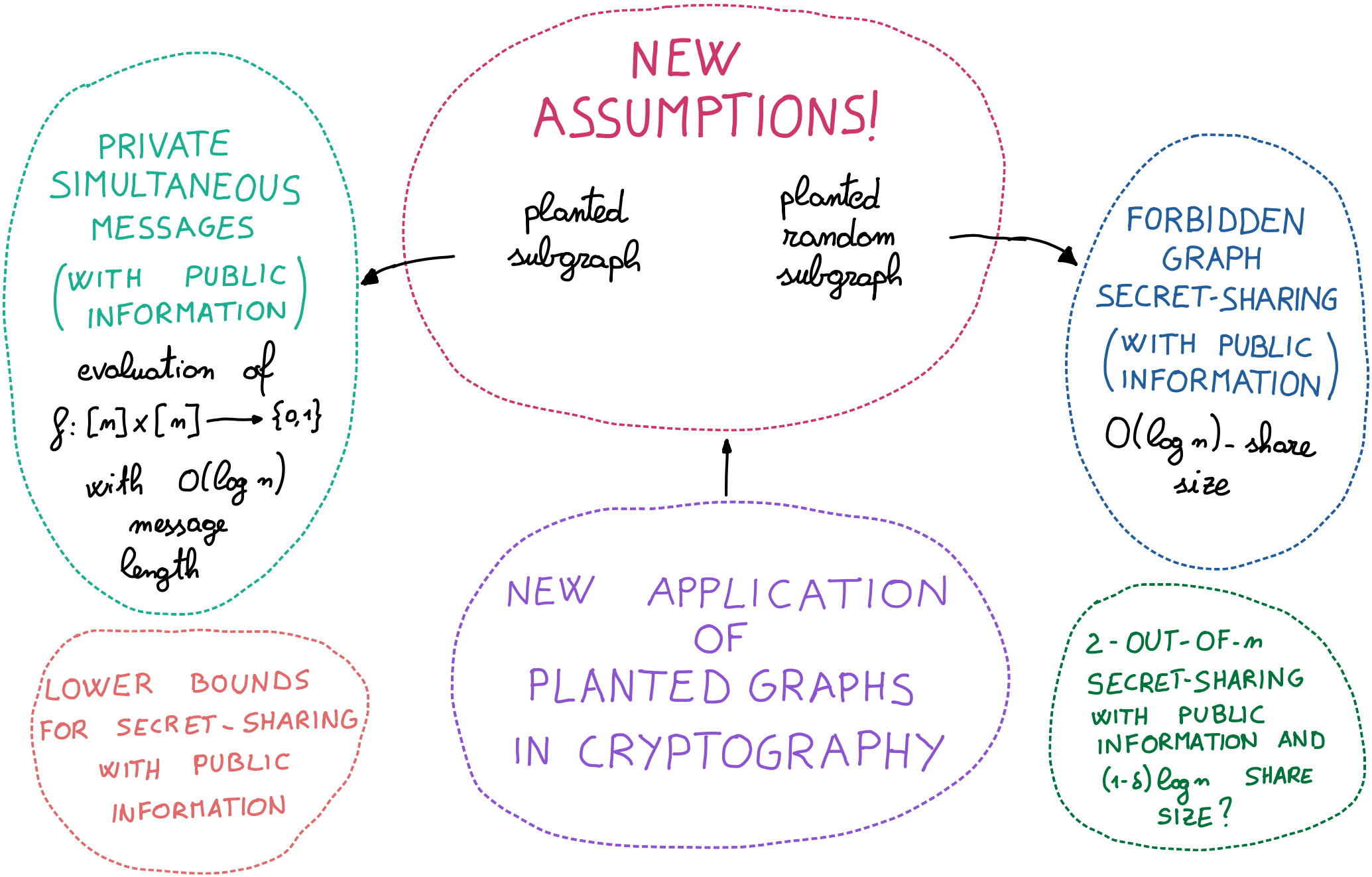
FORBIDDEN GRAPH SECRET-SHARING (WITH PUBLIC INFORMATION)

$O(\log n)$ - share size

NEW APPLICATION OF PLANTED GRAPHS IN CRYPTOGRAPHY

LOWER BOUNDS FOR SECRET-SHARING WITH PUBLIC INFORMATION

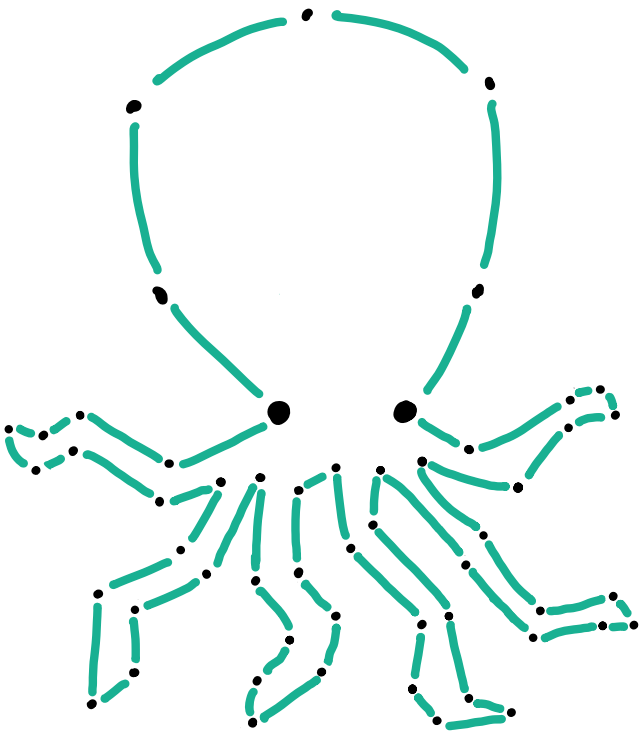
CONTRIBUTIONS



PLANTED GRAPH PROBLEMS

D_H

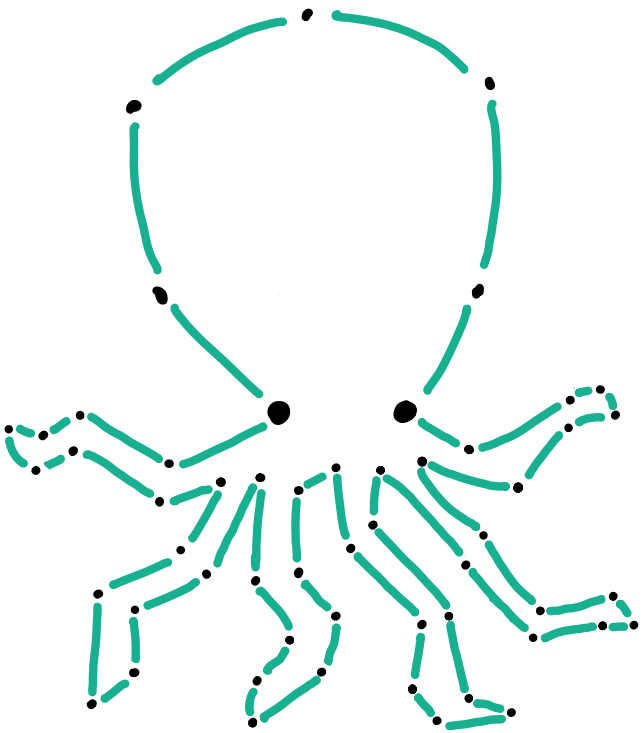
n nodes

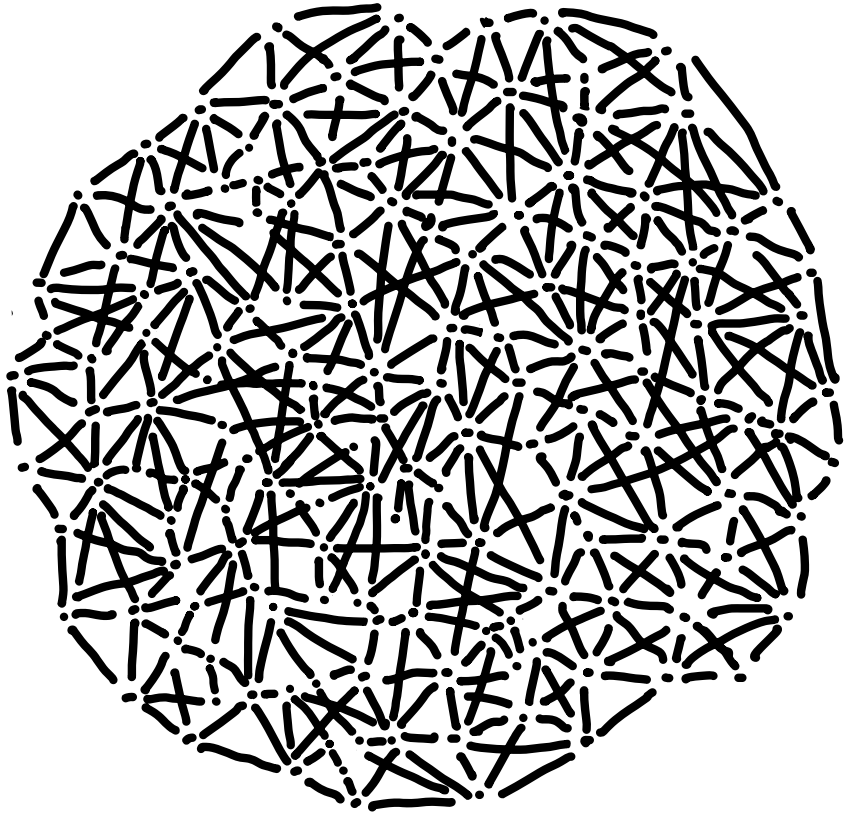


PLANTED GRAPH PROBLEMS

D_H D_A

n nodes $<$ N nodes

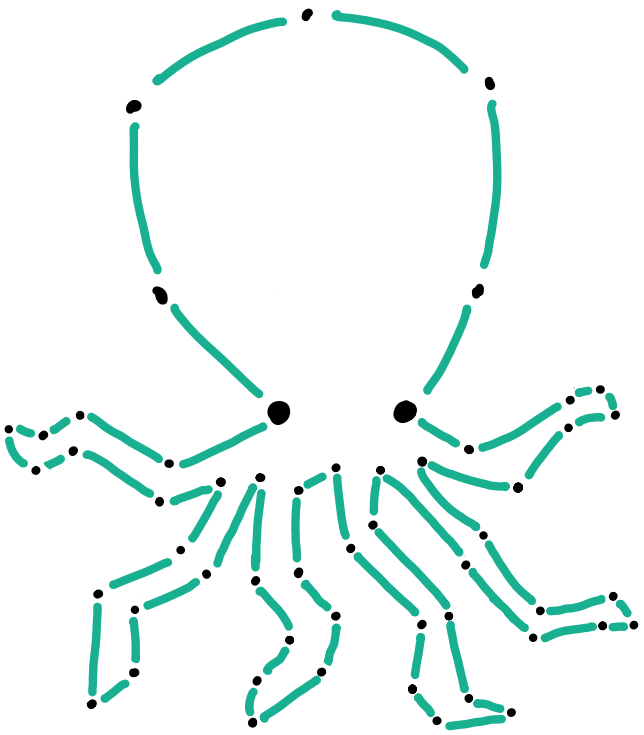


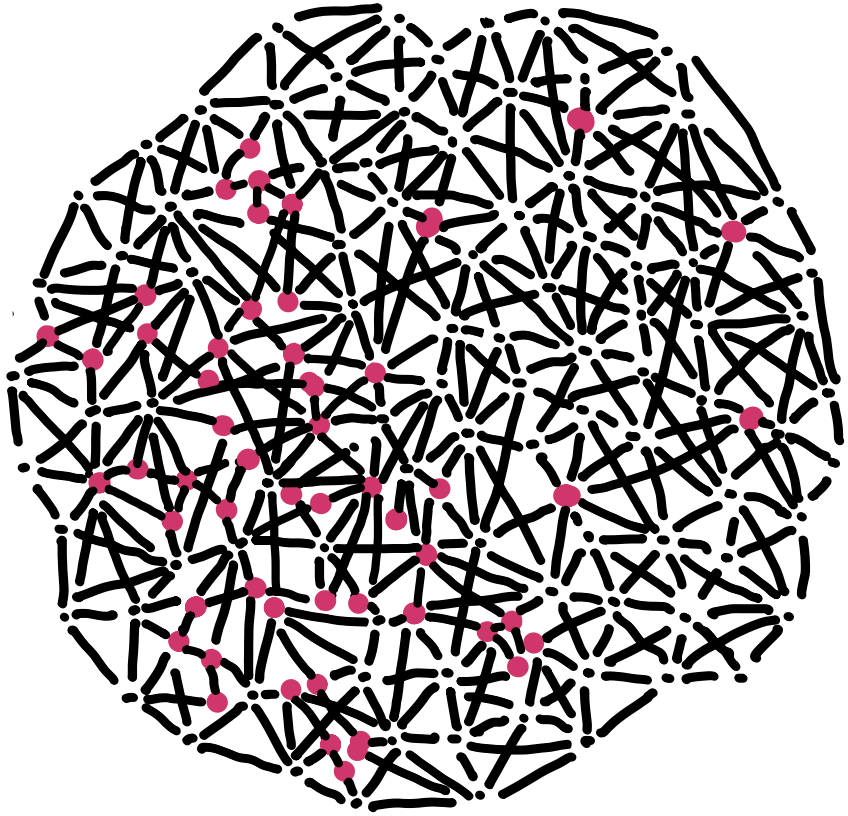


PLANTING OPERATION

D_H $<$ D_A

n nodes $<$ N nodes

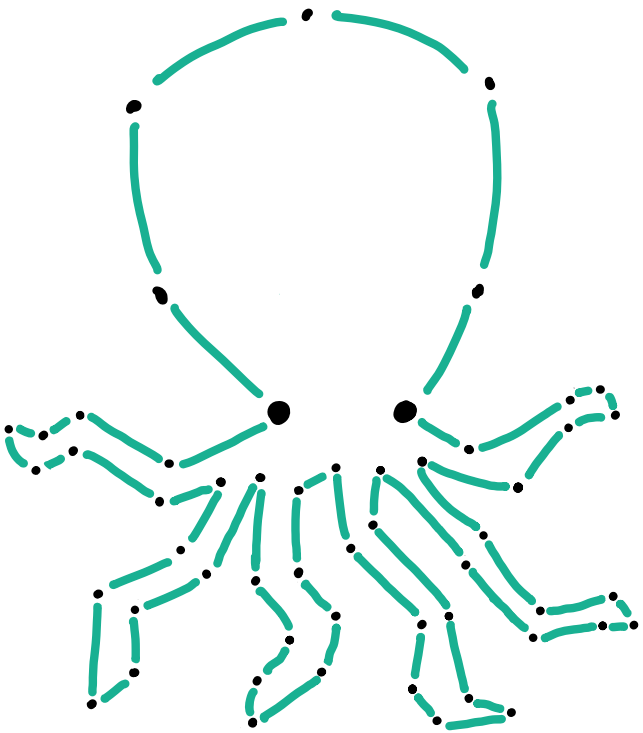


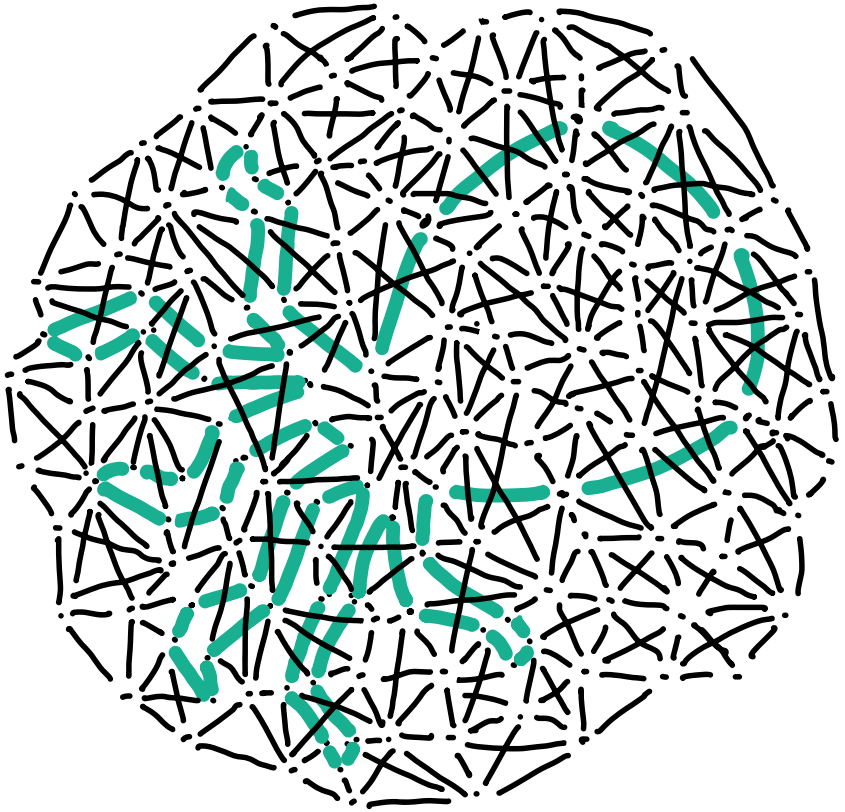


PLANTING OPERATION

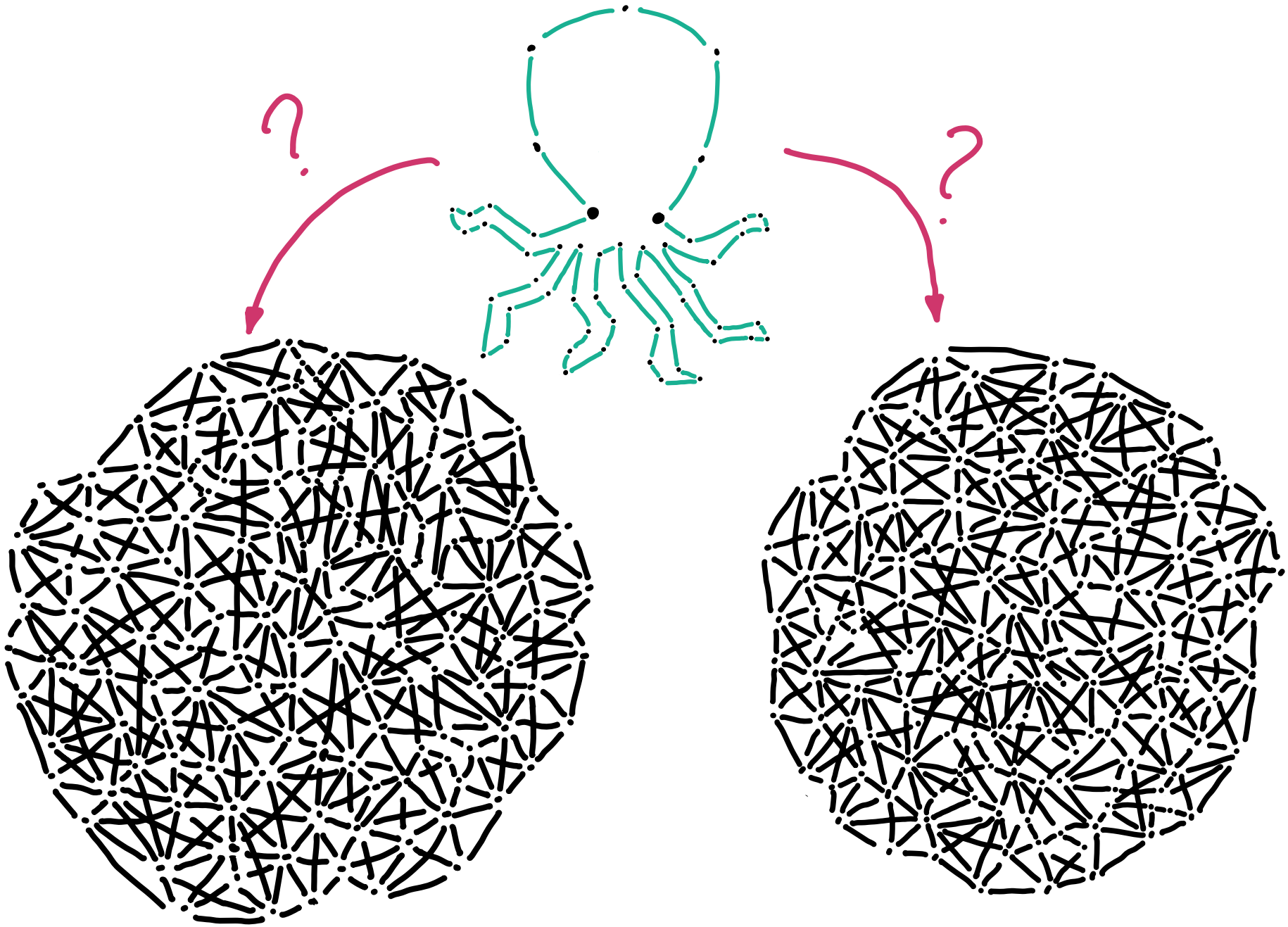
D_H $<$ D_A

n nodes $<$ N nodes

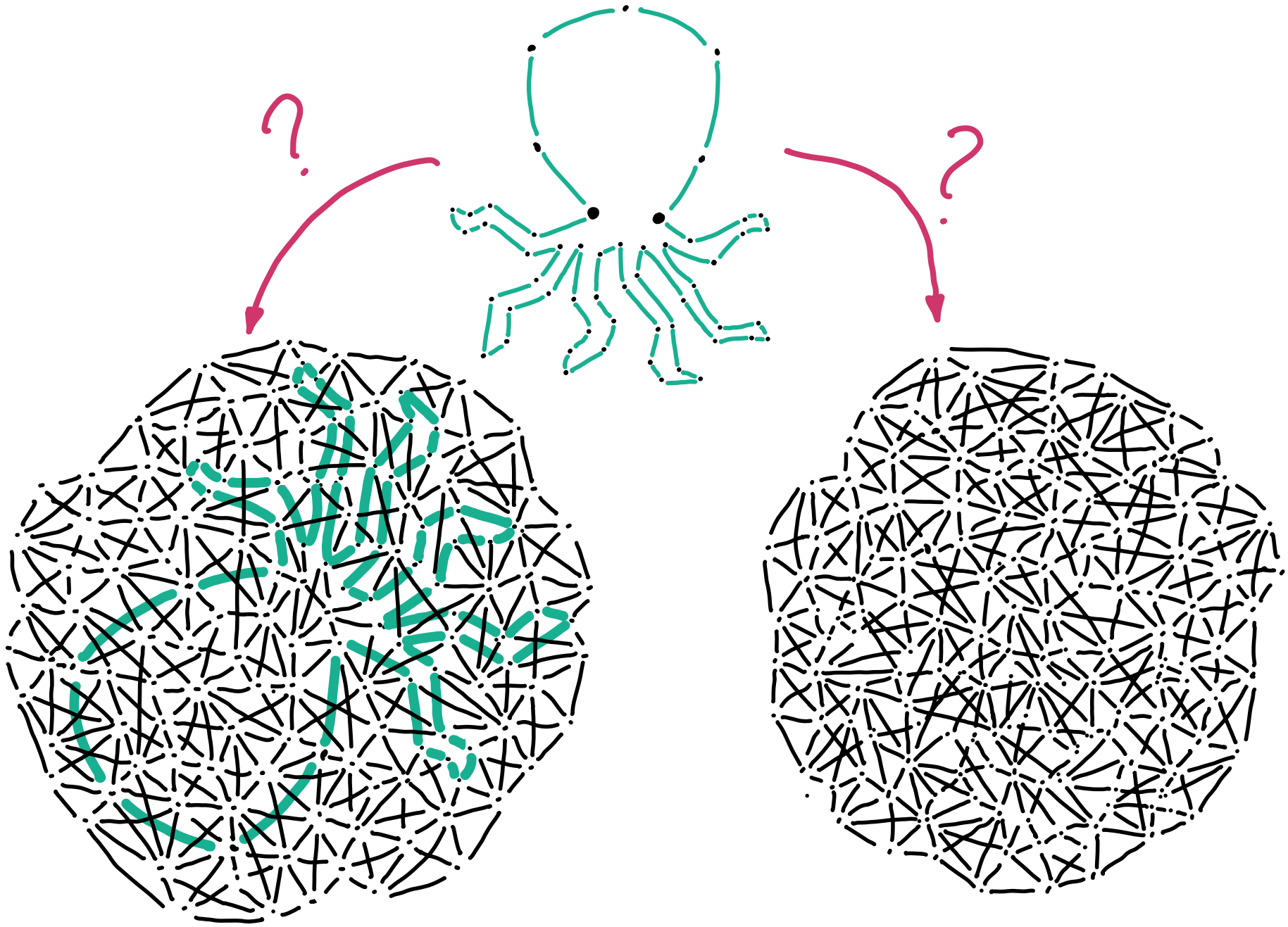




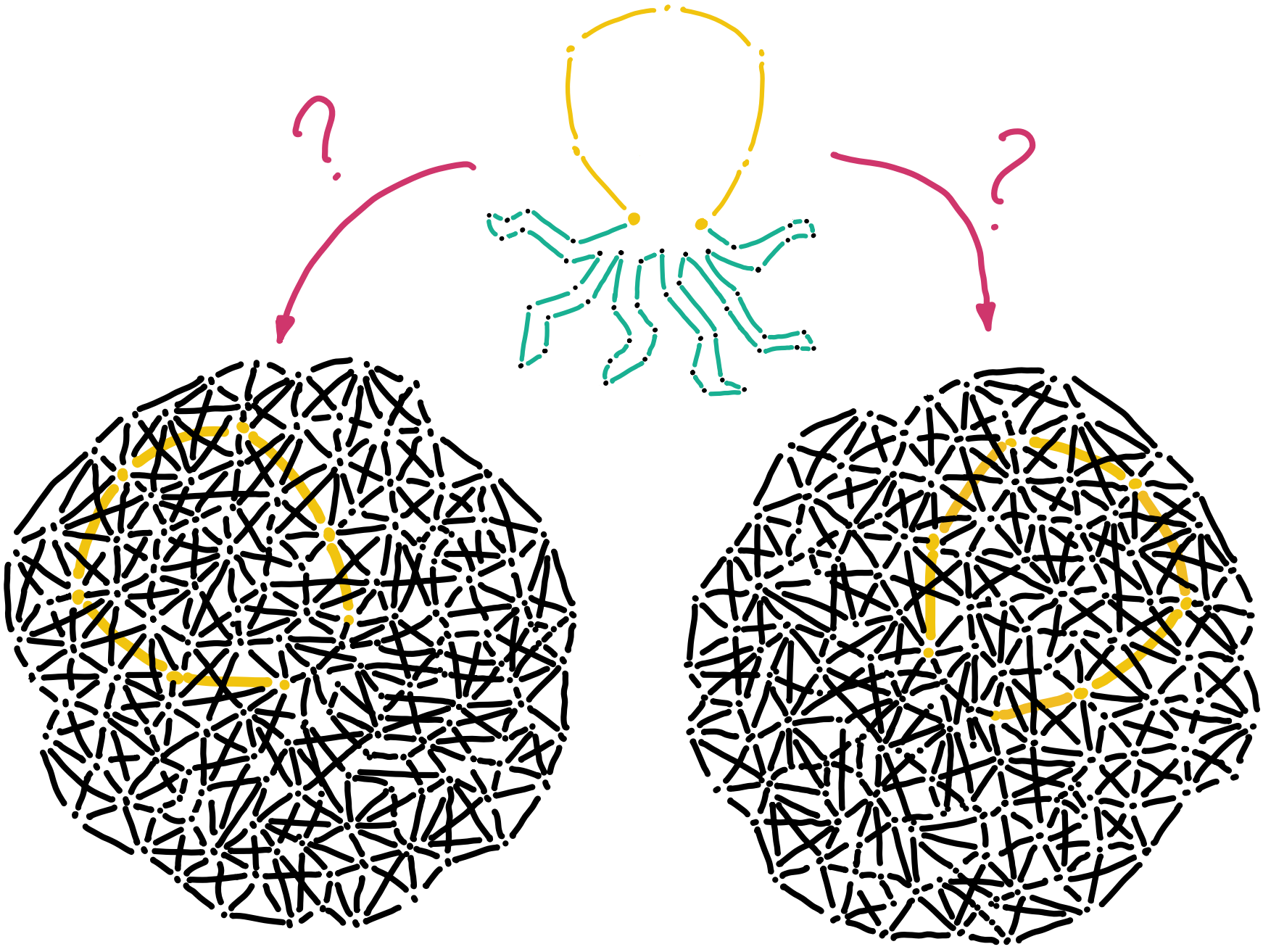
PLANTED GRAPH PROBLEMS



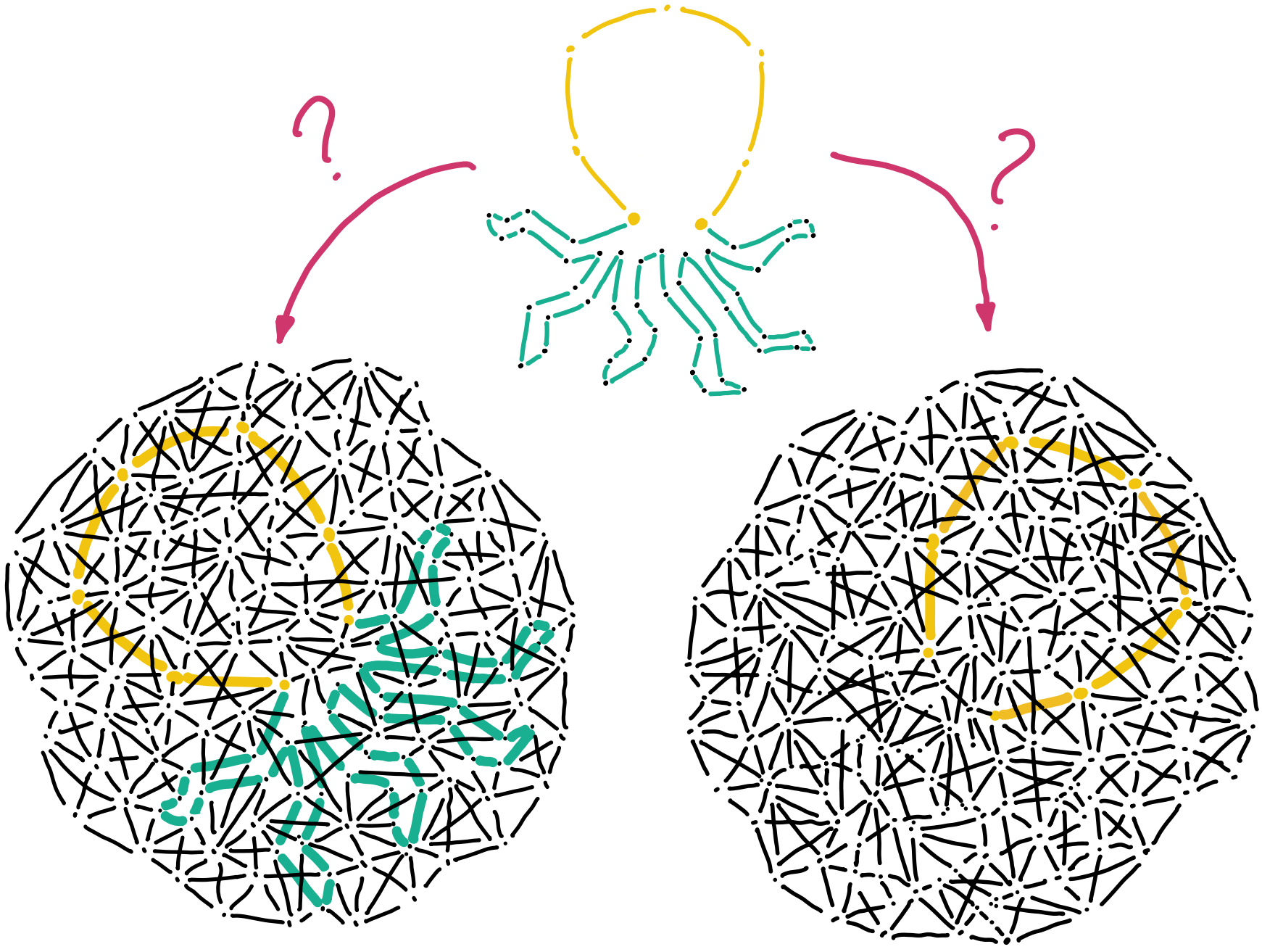
PLANTED GRAPH PROBLEMS



PLANTED GRAPHS WITH HINTS



PLANTED GRAPHS WITH HINTS



PLANTED GRAPH PROBLEMS

PLANTED
CLIQUE

PLANTED GRAPH PROBLEMS

PLANTED CLIQUE

← WELL STUDIED ASSUMPTION

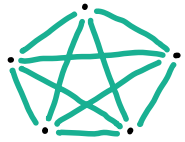
[JERRUM 92
KUČERA 95
BHK+16]

PLANTED GRAPH PROBLEMS

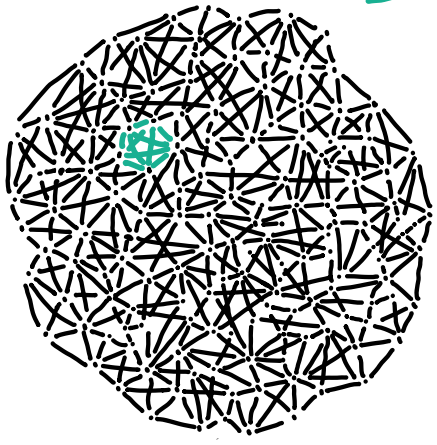
PLANTED CLIQUE

← WELL STUDIED ASSUMPTION

[JERRUM 92
KUČERA 95
BHK+16]

D_H 

RANDOM AMBIENT GRAPHS



PLANTED GRAPH PROBLEMS

PLANTED CLIQUE

← WELL STUDIED ASSUMPTION [JERRUM 92, KUČERA 95, BHK+16]

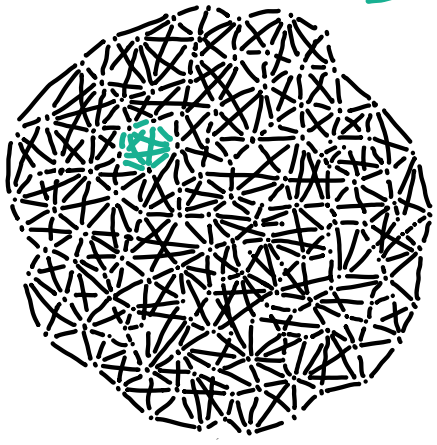
PLANTED SUBGRAPH

THIS WORK

PLANTED RANDOM SUBGRAPH

D_H

RANDOM AMBIENT GRAPHS



PLANTED GRAPH PROBLEMS

PLANTED CLIQUE

← WELL STUDIED ASSUMPTION

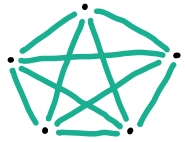
[JERRUM 92
KUČERA 95
BHK+16]

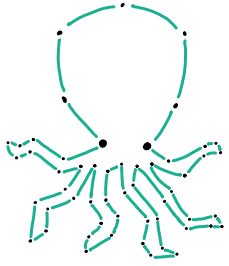
PLANTED SUBGRAPH

THIS WORK

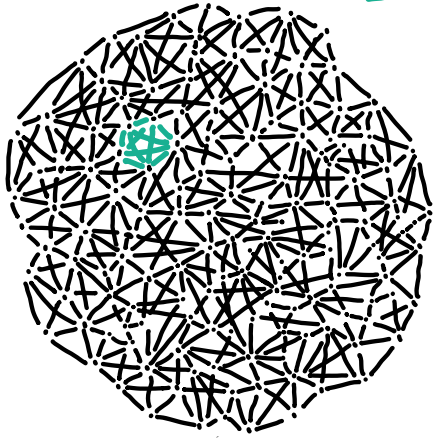
PLANTED RANDOM SUBGRAPH

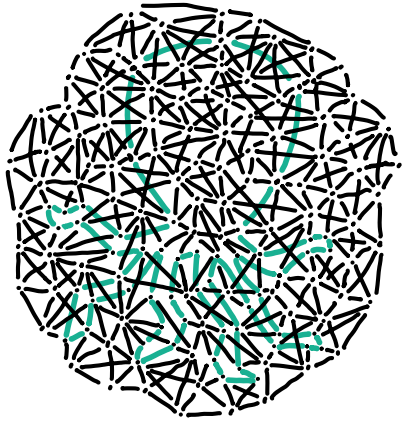
DETERMINISTIC

D_H 

D_H 

RANDOM AMBIENT GRAPHS





PLANTED GRAPH PROBLEMS

PLANTED CLIQUE

← WELL STUDIED ASSUMPTION

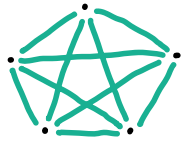
[JERRUM 92
KUČERA 95
BHK+16]

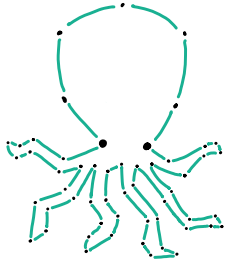
THIS WORK

PLANTED SUBGRAPH

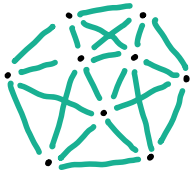
PLANTED RANDOM SUBGRAPH

DETERMINISTIC

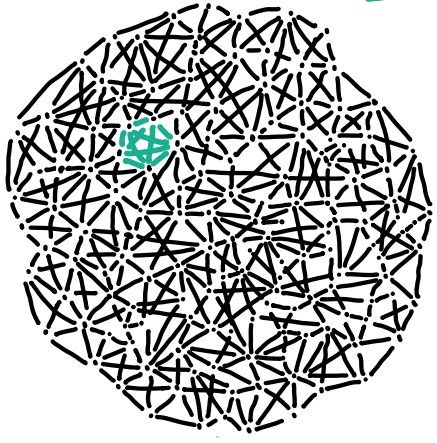
D_H 

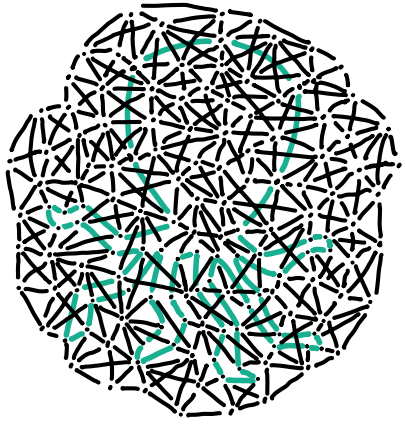
D_H 

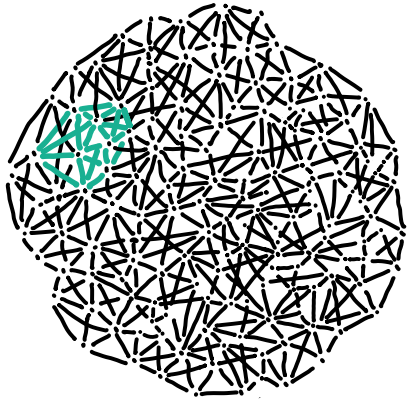
RANDOM

D_H 

RANDOM AMBIENT GRAPHS







PLANTED GRAPH PROBLEMS

PLANTED CLIQUE

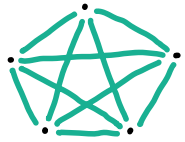
← WELL STUDIED ASSUMPTION [JERRUM 92, KUČERA 95, BHK+16]

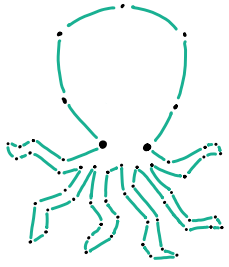
PLANTED SUBGRAPH

THIS WORK

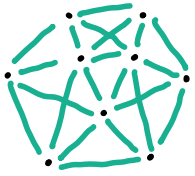
PLANTED RANDOM SUBGRAPH

DETERMINISTIC

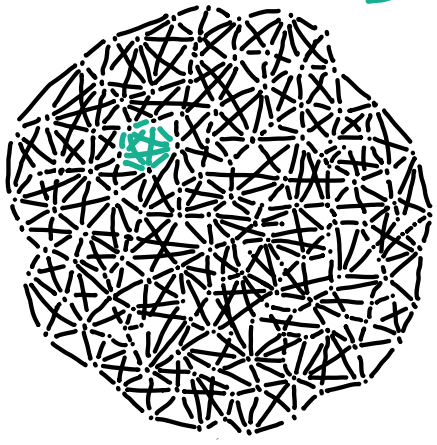
D_H 

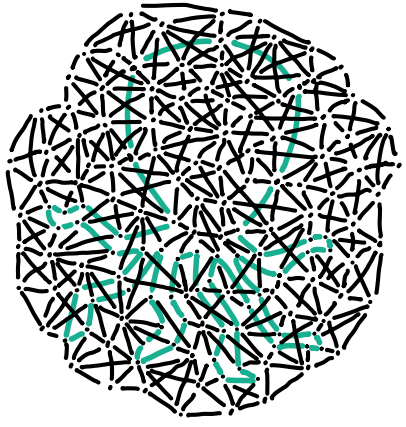
D_H 

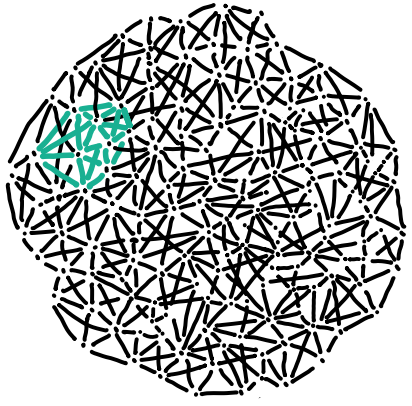
RANDOM

D_H 

RANDOM AMBIENT GRAPHS







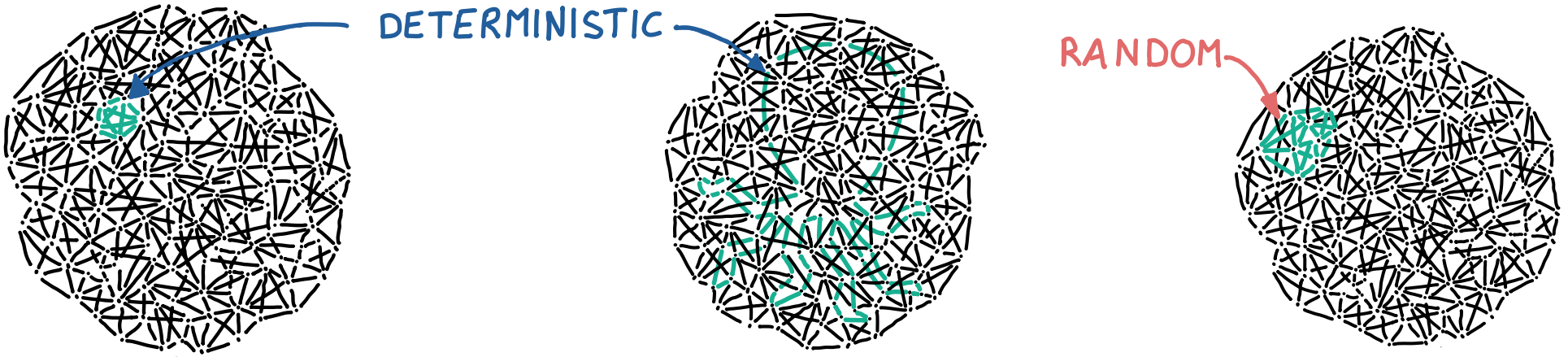
CONJECTURED HARDNESS (LOW-DEGREE ANALYSIS)

PLANTED GRAPH PROBLEMS PARAMETERS

PLANTED CLIQUE

PLANTED SUBGRAPH

PLANTED RANDOM SUBGRAPH

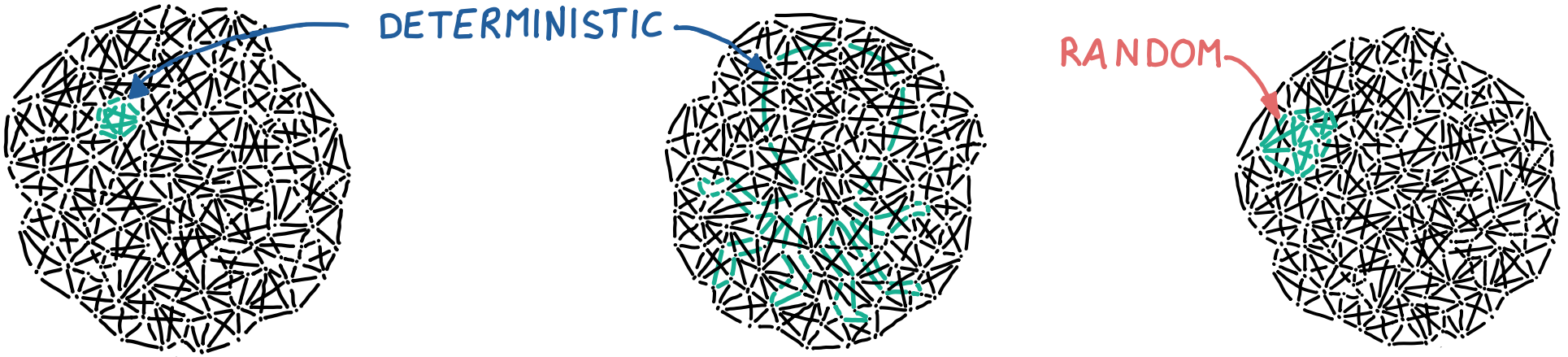


PLANTED GRAPH PROBLEMS PARAMETERS

PLANTED CLIQUE

PLANTED SUBGRAPH

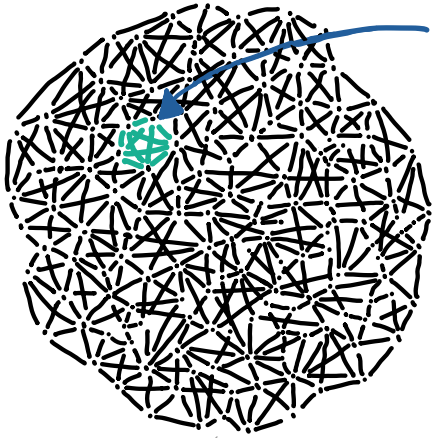
PLANTED RANDOM SUBGRAPH



$N = n^{2+\delta}$

PLANTED GRAPH PROBLEMS PARAMETERS

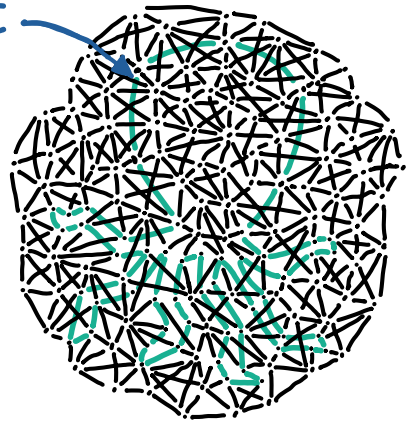
PLANTED CLIQUE



$N = n^{2+\delta}$

PLANTED SUBGRAPH

DETERMINISTIC

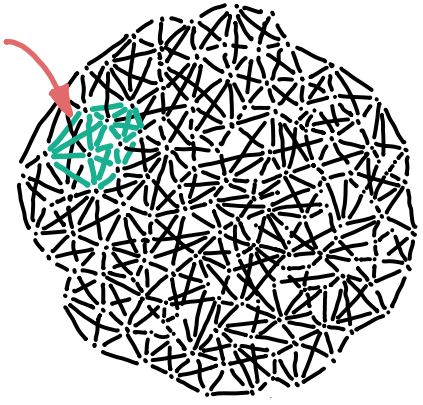


$N = n^{1+\delta}$

(for 1-negl(n) fraction of hidden graphs!)

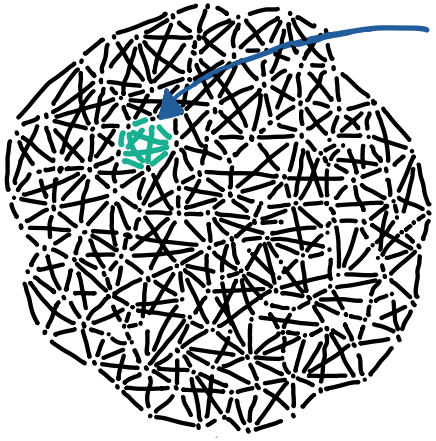
PLANTED RANDOM SUBGRAPH

RANDOM



PLANTED GRAPH PROBLEMS PARAMETERS

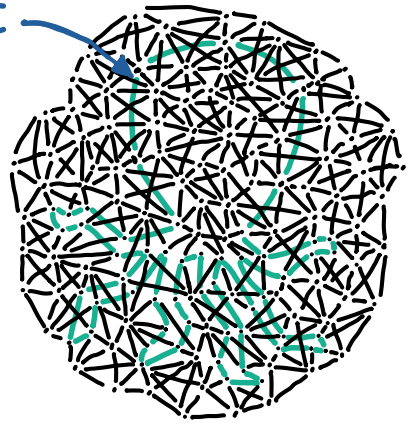
PLANTED CLIQUE



$N = n^{2+\delta}$

PLANTED SUBGRAPH

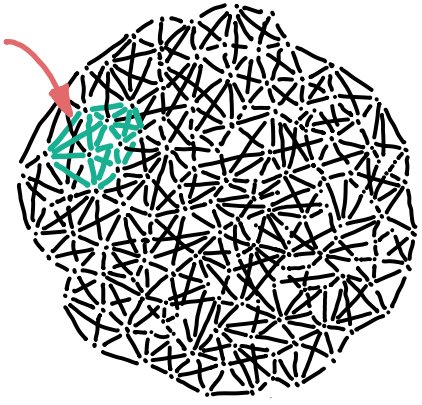
DETERMINISTIC



$N = n^{1+\delta}$

PLANTED RANDOM SUBGRAPH

RANDOM

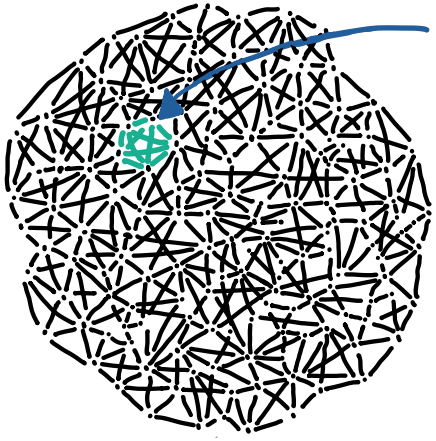


$N = n^{1+\delta}$

(for 1-negl(n) fraction of hidden graphs!)

PLANTED GRAPH PROBLEMS PARAMETERS

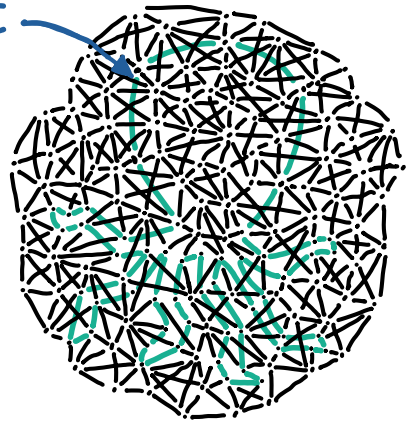
PLANTED CLIQUE



$N = n^{2+\delta}$

PLANTED SUBGRAPH

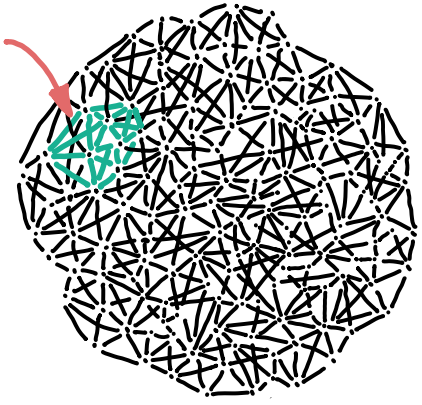
DETERMINISTIC



$N = n^{1+\delta}$

PLANTED RANDOM SUBGRAPH

RANDOM



$N = n^{1+\delta}$

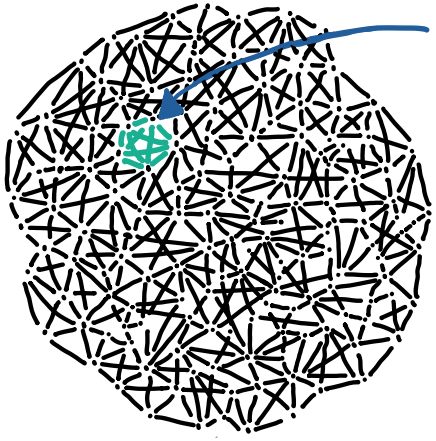
(for 1-negl(n) fraction of hidden graphs!)

CAVEAT

SECURITY AGAINST $n^{o(\log n)}$-TIME ADVERSARIES!

PLANTED GRAPH PROBLEMS PARAMETERS

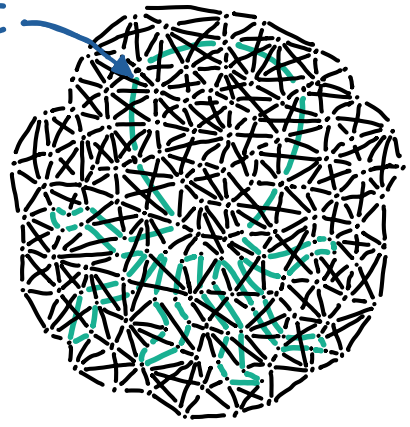
PLANTED CLIQUE



$N = n^{2+\delta}$

PLANTED SUBGRAPH

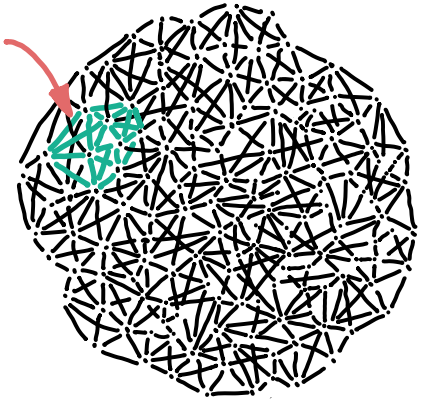
DETERMINISTIC



$N = n^{1+\delta}$

PLANTED RANDOM SUBGRAPH

RANDOM



$N = n^{1+\delta}$

(for 1-negl(n) fraction of hidden graphs!)

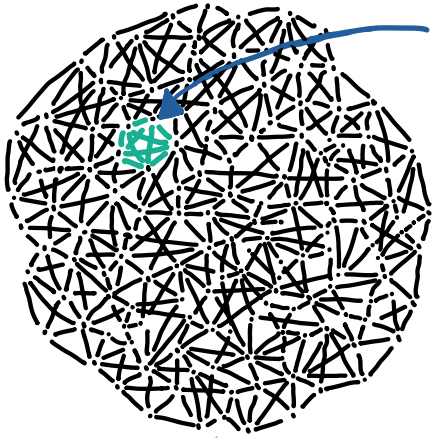
CAVEAT

SECURITY AGAINST $n^{o(\log n)}$-TIME ADVERSARIES!

INVERSE-POLYNOMIAL ADVANTAGE!

PLANTED GRAPH PROBLEMS PARAMETERS

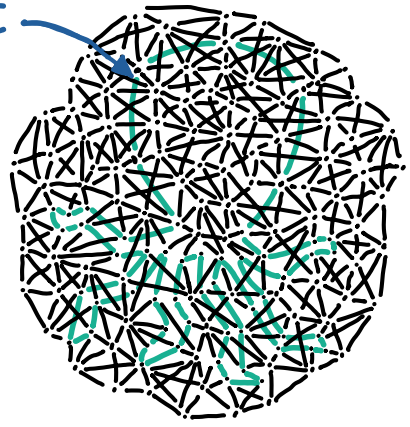
PLANTED CLIQUE



$N = n^{2+\delta}$

PLANTED SUBGRAPH

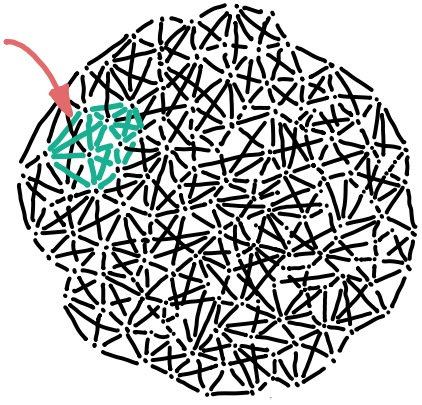
DETERMINISTIC



$N = n^{1+\delta}$

PLANTED RANDOM SUBGRAPH

RANDOM



$N = n^{1+\delta}$

(for $1 - \text{negl}(n)$ fraction of hidden graphs!)

CAVEAT

SECURITY AGAINST $n^{o(\log n)}$-TIME ADVERSARIES!

INVERSE-POLYNOMIAL ADVANTAGE!

EVEN WITH $t = O(1)$ HINTS!

PRIVATE SIMULTANEOUS MESSAGES [WITH PUBLIC INFORMATION]

$$f : [n] \times [n] \to \{0,1\}$$

PRIVATE SIMULTANEOUS MESSAGES [WITH PUBLIC INFORMATION]

$$f : [n] \times [n] \to \{0,1\}$$

ALICE

BOB

CAROL

PRIVATE SIMULTANEOUS MESSAGES [WITH PUBLIC INFORMATION]

$$f : [n] \times [n] \to \{0,1\}$$

ALICE

$x \in [n]$

BOB

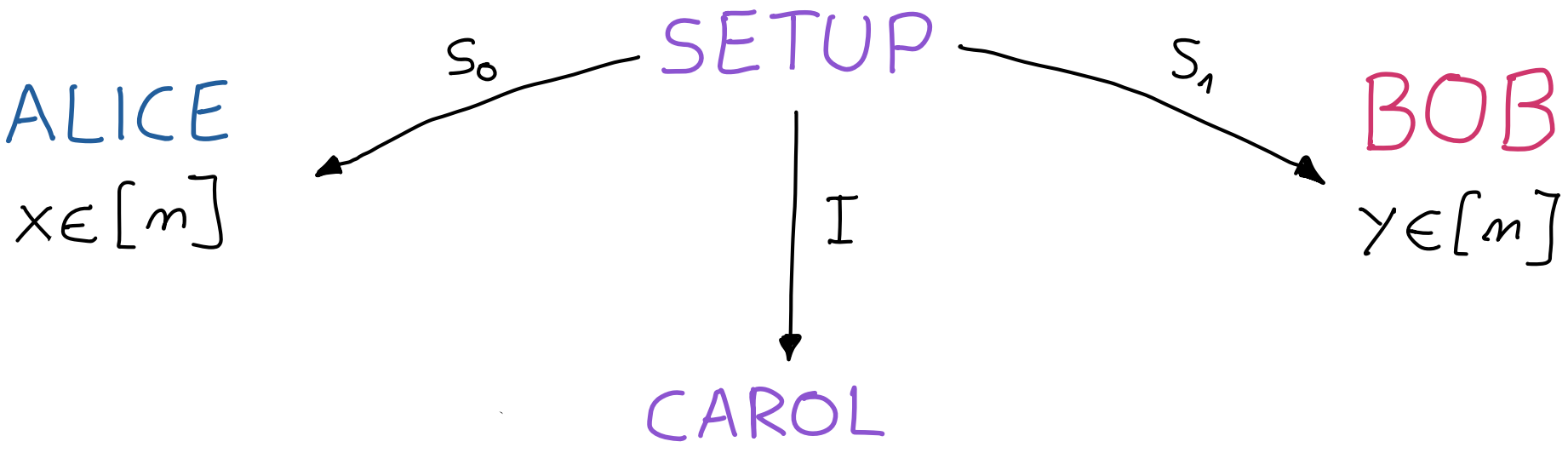
$y \in [n]$

CAROL

$f(x,y)$ ← NO ADDITIONAL LEAKAGE!

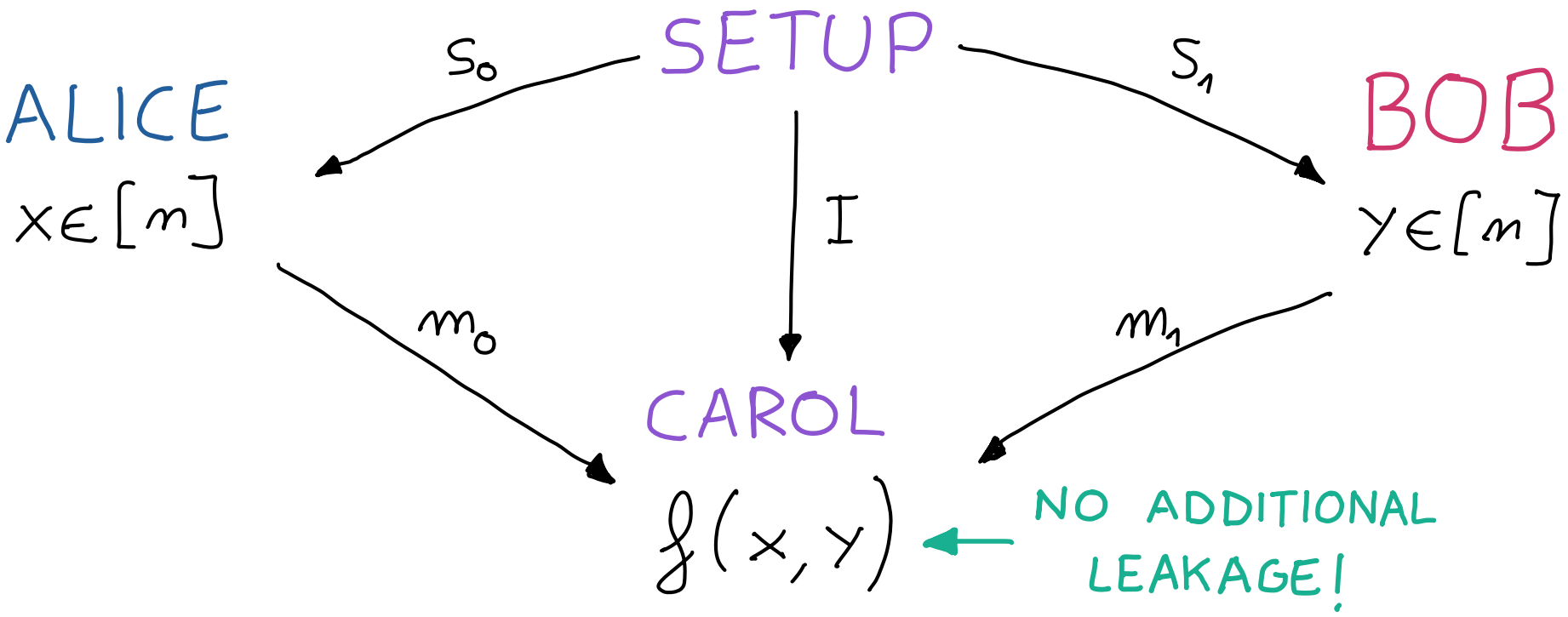
PRIVATE SIMULTANEOUS MESSAGES [WITH PUBLIC INFORMATION]

$$f : [n] \times [n] \to \{0,1\}$$



PRIVATE SIMULTANEOUS MESSAGES [WITH PUBLIC INFORMATION]

$$f : [n] \times [n] \to \{0,1\}$$



PRIVATE SIMULTANEOUS MESSAGES [WITH PUBLIC INFORMATION]

$f(x,y)$: is $y \in \{x, (x+1) \bmod n\}$?

ALICE

$x \in [n]$

BOB

$y \in [n]$

PRIVATE SIMULTANEOUS MESSAGES [WITH PUBLIC INFORMATION]

$f(x,y)$: is $y \in \{x, (x+1) \bmod n\}$?

ALICE

$x \in [n]$

0
1
2
⋮
$n-1$

BOB

$y \in [n]$

0
1
2
⋮
$n-1$

PRIVATE SIMULTANEOUS MESSAGES [WITH PUBLIC INFORMATION]

$f(x,y)$: is $y \in \{x, (x+1) \bmod n\}$?

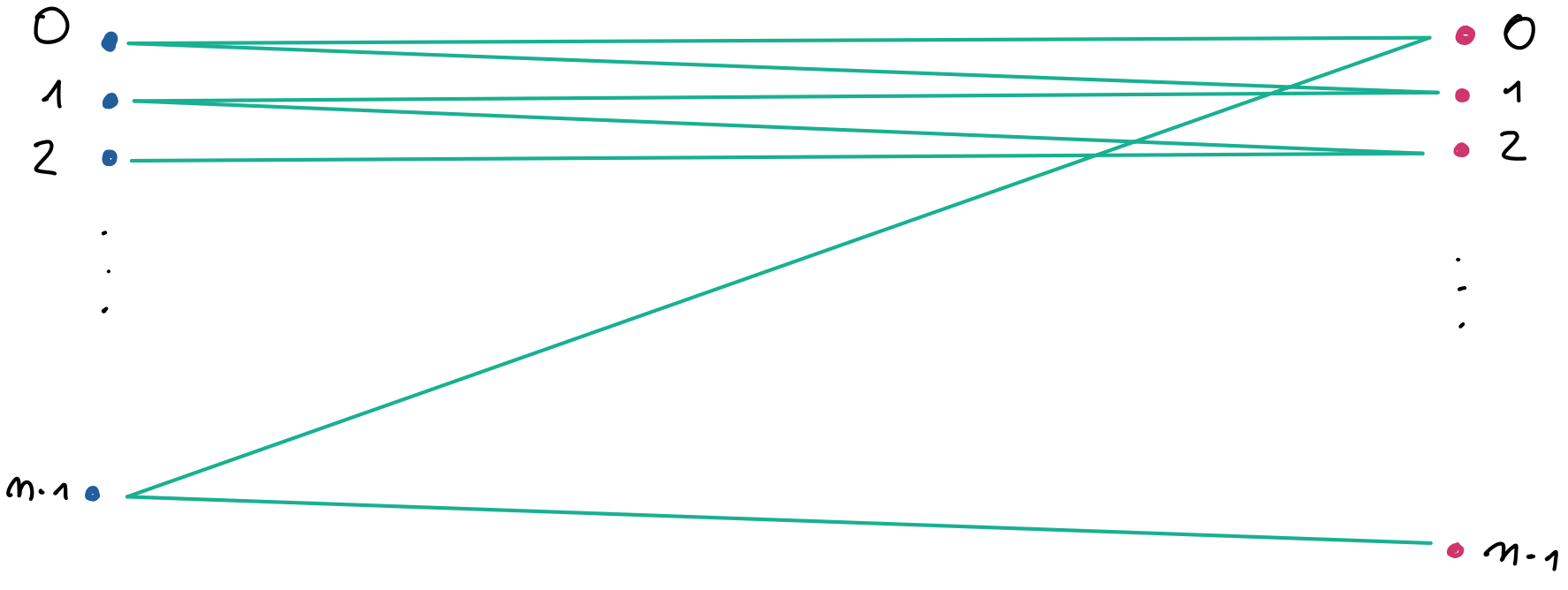
ALICE

$x \in [n]$

OCTOPUS GRAPH!

BOB

$y \in [n]$



PRIVATE SIMULTANEOUS MESSAGES [WITH PUBLIC INFORMATION]

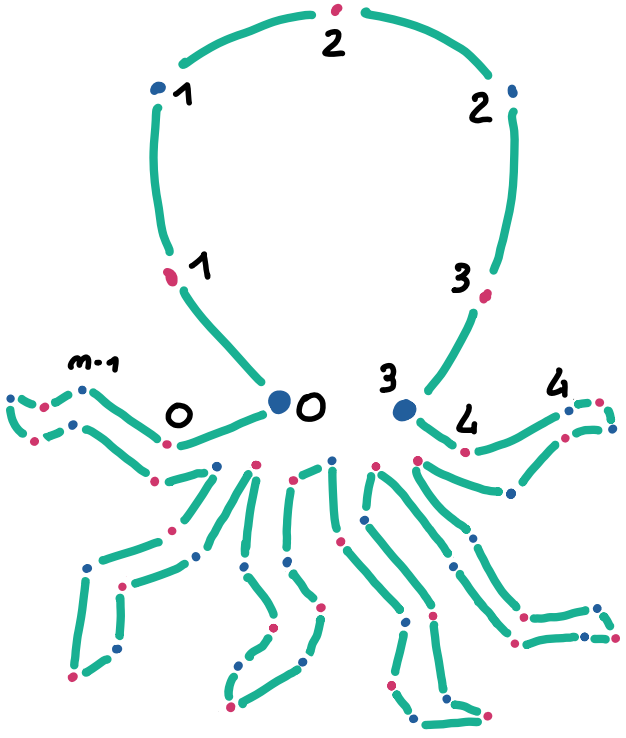
$f(x,y)$: is $y \in \{x, (x+1) \bmod n\}$?

ALICE

$x \in [n]$

BOB

$y \in [n]$



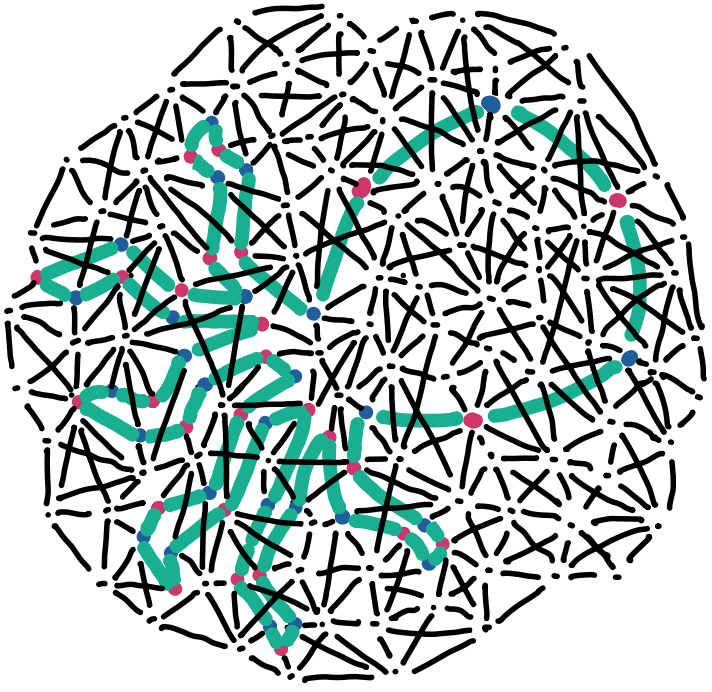
PRIVATE SIMULTANEOUS MESSAGES [WITH PUBLIC INFORMATION]

$f(x,y)$: is $y \in \{x, (x+1) \bmod n\}$?

SETUP

ALICE

$x \in [n]$



BOB

$y \in [n]$

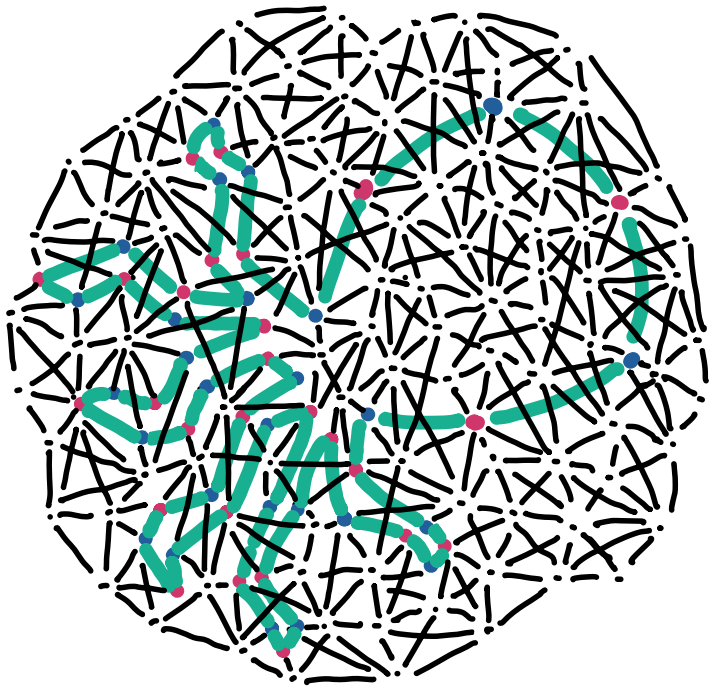
PRIVATE SIMULTANEOUS MESSAGES [WITH PUBLIC INFORMATION]

$f(x,y)$: is $y \in \{x, (x+1) \bmod n\}$?

SETUP

ALICE

$x \in [n]$



public information I

BOB

$y \in [n]$

PRIVATE SIMULTANEOUS MESSAGES [WITH PUBLIC INFORMATION]

$f(x,y)$: is $y \in \{x, (x+1) \bmod n\}$?

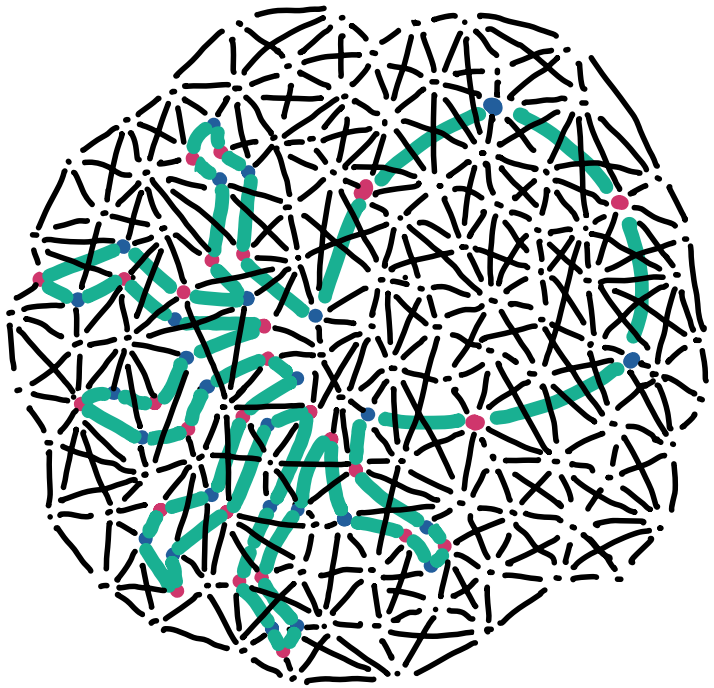
SETUP

ALICE

$x \in [n]$

s_0

position of blue nodes in I



public information I

s_1

position of red nodes in I

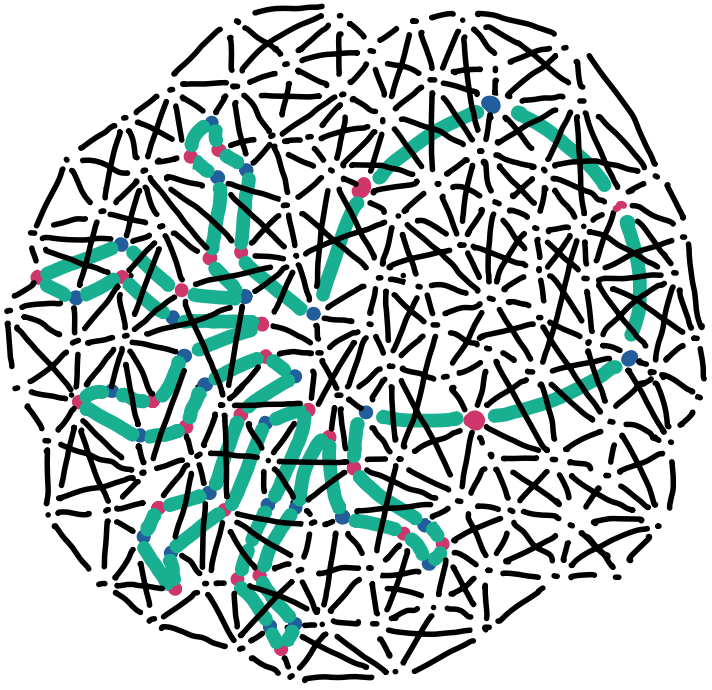
BOB

$y \in [n]$

PRIVATE SIMULTANEOUS MESSAGES [WITH PUBLIC INFORMATION]

$f(x,y)$: is $y \in \{x, (x+1) \bmod n\}$?

ALICE
$x = 3$



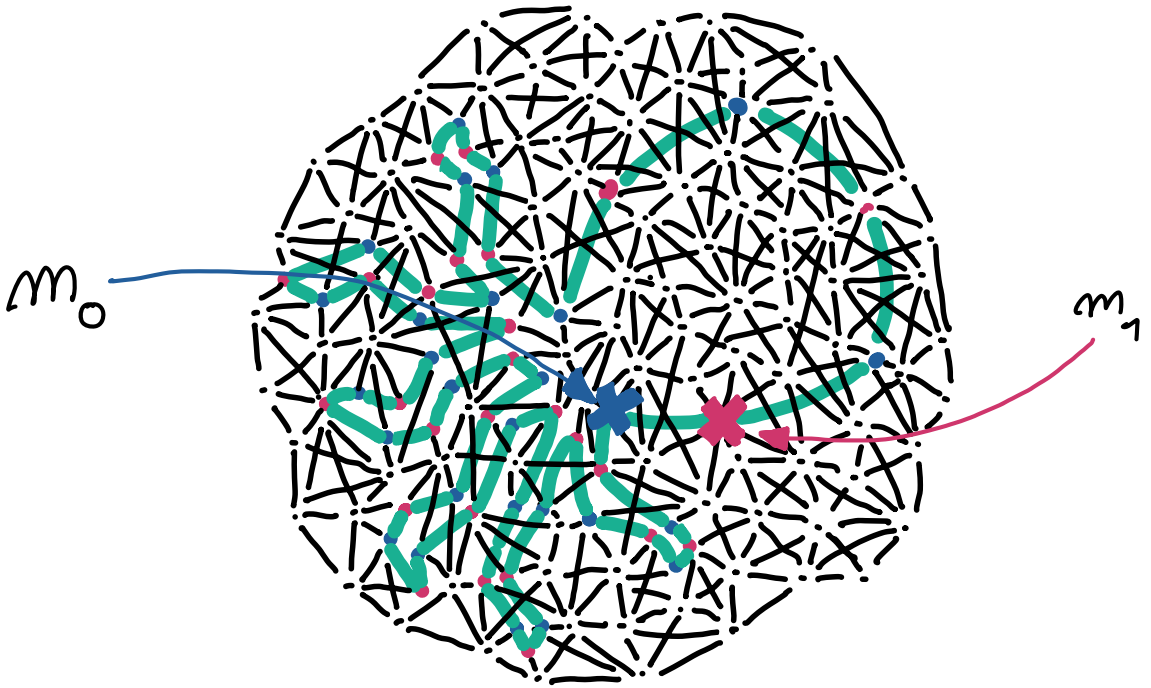
public information I

BOB
$y = 3$

PRIVATE SIMULTANEOUS MESSAGES [WITH PUBLIC INFORMATION]

$f(x, y)$: is $y \in \{x, (x+1) \bmod n\}$?

ALICE
$x = 3$



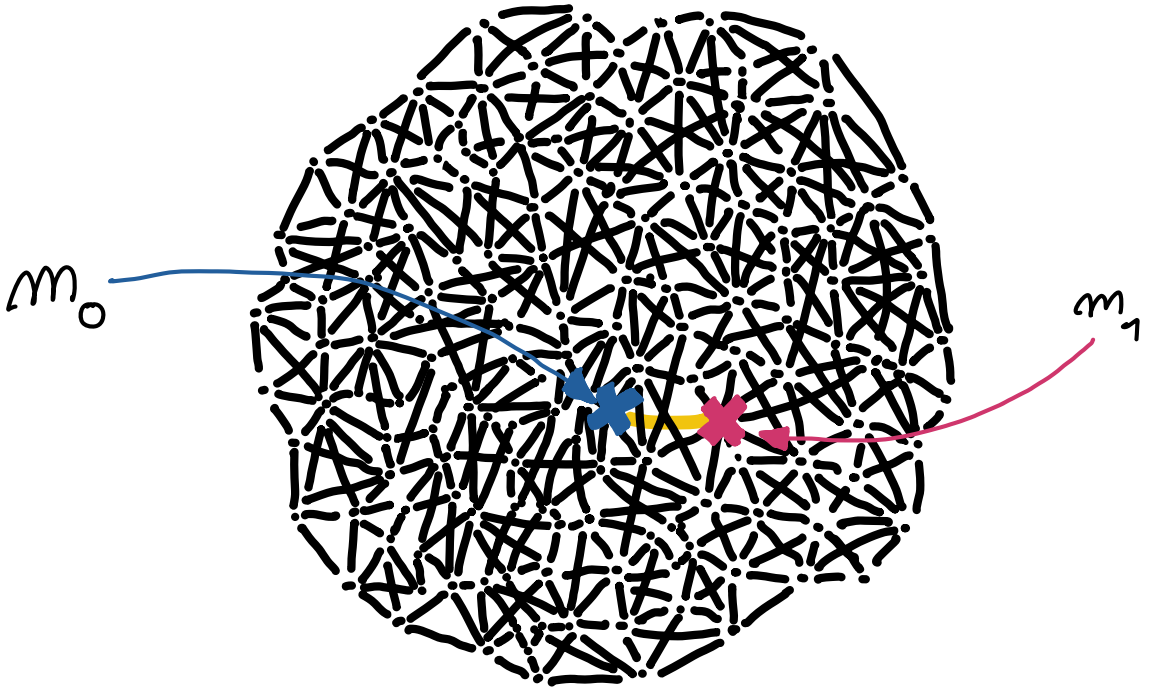
BOB
$y = 3$

PRIVATE SIMULTANEOUS MESSAGES [WITH PUBLIC INFORMATION]

$f(x,y)$: is $y \in \{x, (x+1) \bmod n\}$?

ALICE

$x = 3$



BOB

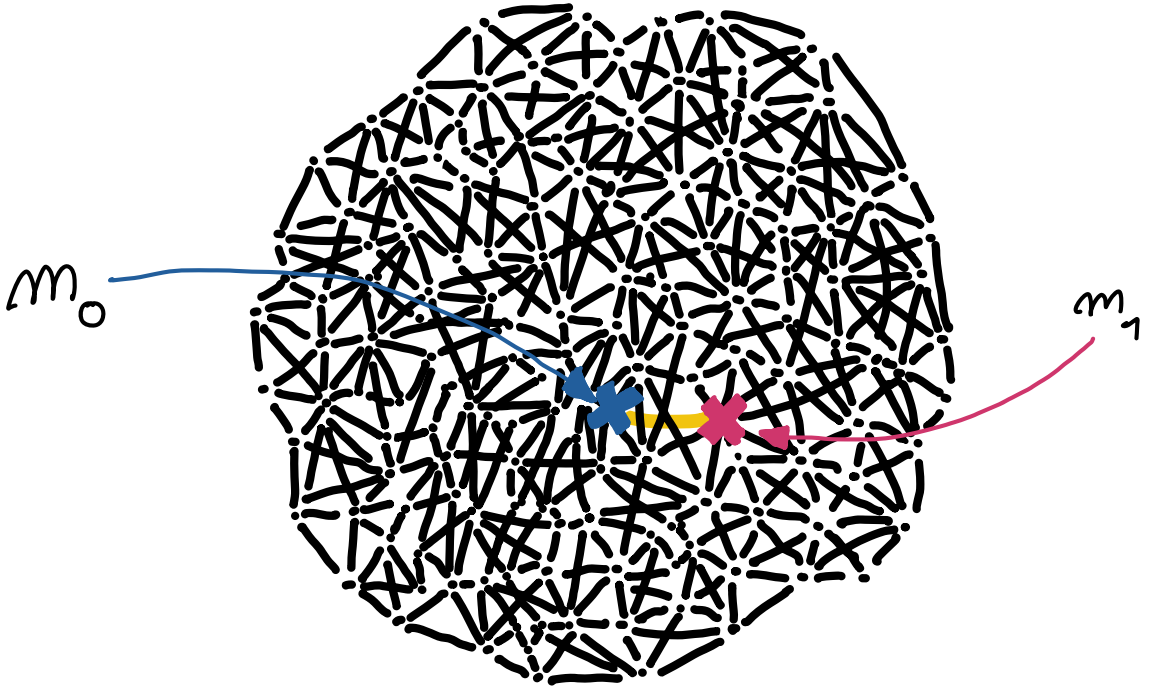
$y = 3$

CAROL

PRIVATE SIMULTANEOUS MESSAGES [WITH PUBLIC INFORMATION]

$f(x, y)$: is $y \in \{x, (x+1) \bmod n\}$?

ALICE
$x = 3$



BOB
$y = 3$

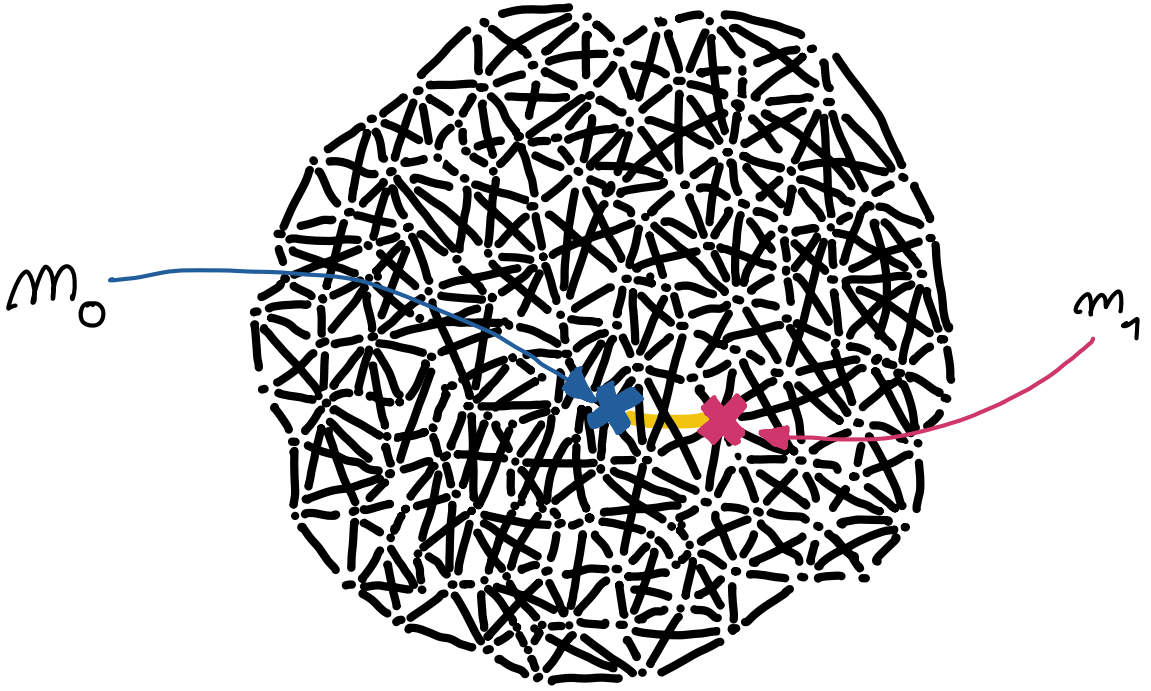
CAROL: what part of the octopus have I received?

PRIVATE SIMULTANEOUS MESSAGES [WITH PUBLIC INFORMATION]

$f(x,y)$: is $y \in \{x, (x+1) \bmod n\}$?

$$|m_0| = |m_1| = \log\binom{N}{2} = O(\log n)!$$

ALICE
$x = 3$



BOB
$y = 3$

CAROL: what part of the octopus have I received?

SUMMARY

NEW CRYPTOGRAPHIC ASSUMPTIONS BASED ON PLANTED GRAPHS:

planted subgraph (with hints) – PS(H)

planted random subgraph (with hints) – PRS(H)

OPEN QUESTION: are there better planting procedures? →

CAVEAT: SECURITY AGAINST $n^{o(\log n)}$-TIME ADVERSARIES! INVERSE-POLYNOMIAL ADVANTAGE!

POSSIBLE GAP! EQUIVALENT PLANTED GRAPH PROBLEM

APPLICATIONS

	INFORMATION THEORETIC		COMPUTATIONAL WITH PUBLIC INFORMATION	
PSM $f: [n]\times[n] \to \{0,1\}$	$\leq \sqrt{n}$	[BIKK14]	$\leq 1.01 \log n$	(under PSH)
	$\geq (1.5 - o(1)) \cdot \log n$	[AHMS18]	$\geq \log n$	
FORBIDDEN GRAPH SECRET-SHARING	$\leq 2^{\tilde{O}(\sqrt{\log n})}$	[LVW17]	$\leq 1.01 \log n$	(under PRSH)
	$\geq \log n$	[KN90]	$\Omega(\log\log n)$	
2-OUT-OF-n SECRET-SHARING	$\leq \log n$	[SHAMIR]	$\log n$	[SHAMIR]
	$\geq \log n$	[KN90]	$\Omega(\log\log n)$	
NON-IDEAL BINARY SECRET-SHARING	≥ 1		≥ 1	