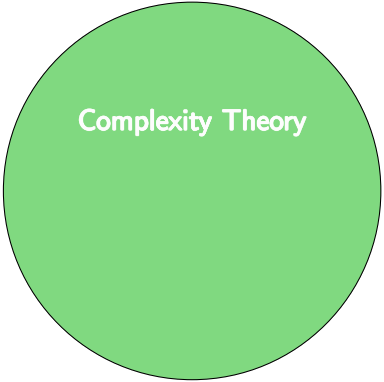
A Note on Low-Communication MPC via Circuit Depth-Reduction

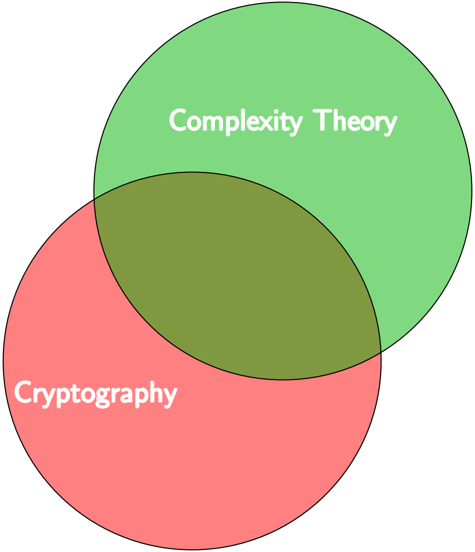
Pierre Charbit[1] Geoffroy Couteau[1] Pierre Meyer[2] Reza Naserasr[1]

[1]Université Paris Cité, IRIF, CNRS
[2]Aarhus University

TCC 2024

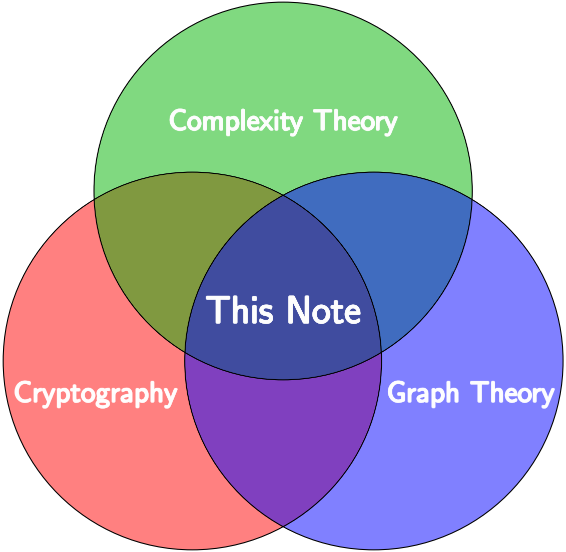


? Trade-off fan-in/size



? Trade-off fan-in/size

$\Rightarrow$ Low-communication MPC



? Trade-off fan-in/size

$\Rightarrow$ Low-communication MPC

! k-path hitting set

Size: Number of gates

Fan-in: Max number of inputs to a gate

Can **every** fan-in-2 circuit of size s be computed by a fan-in k circuit of size $\epsilon \cdot s$?

Size: Number of gates

Fan-in: Max number of inputs to a gate

Can **every** fan-in-2 circuit of size s be computed by a fan-in k circuit of size $\epsilon \cdot s$?

	Fractional regime
ϵ	$\in (0,1)$
k	$\leq \log\log s$

Size: Number of gates

Fan-in: Max number of inputs to a gate

Can **every** fan-in-2 circuit of size s be computed by a fan-in k circuit of size $\epsilon \cdot s$?

	Fractional regime	
ϵ	$\in (0,1)$	$2/3$
k	$\leq \log \log s$	4

Size: Number of gates

Fan-in: Max number of inputs to a gate

Can **every** fan-in-2 circuit of size s be computed by a fan-in k circuit of size $\epsilon \cdot s$?

	Fractional regime		
ϵ	$\in (0,1)$	$2/3$	$\to 2/5$
k	$\leq \log\log s$	4	$\omega(1)$

Size: Number of gates

Fan-in: Max number of inputs to a gate

Can **every** fan-in-2 circuit of size s be computed by a fan-in k circuit of size $\epsilon \cdot s$?

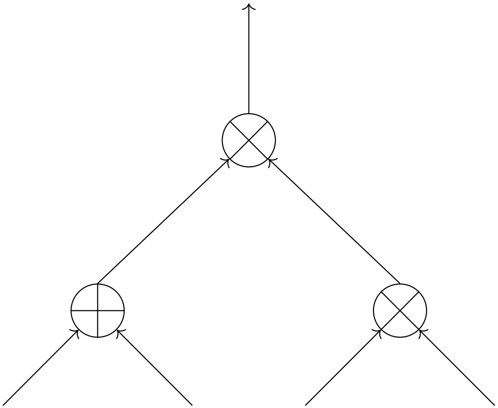
	Fractional regime			Sublinear regime
ϵ	$\in (0,1)$	$2/3$	$\to 2/5$	$o(1)$
k	$\leq \log\log s$	4	$\omega(1)$	$\leq \log\log s$

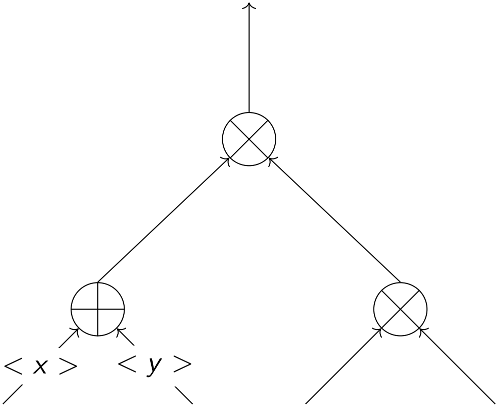
Size: Number of gates

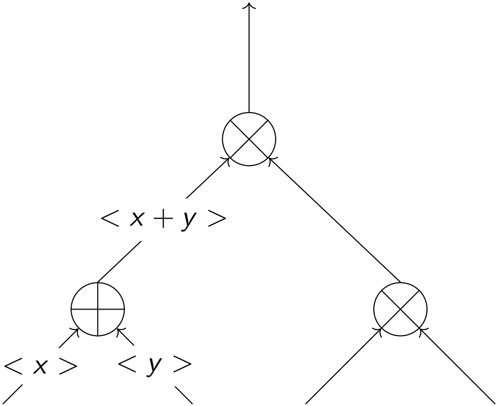
Fan-in: Max number of inputs to a gate

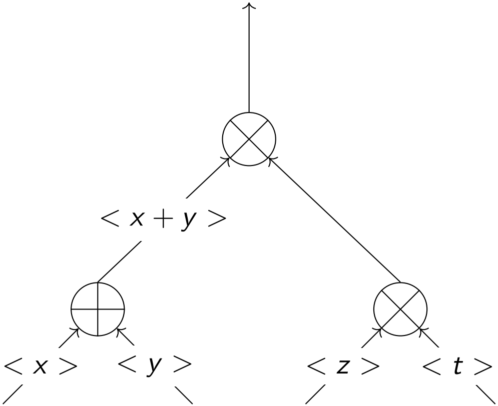
Can **every** fan-in-2 circuit of size s be computed by a fan-in k circuit of size $\epsilon \cdot s$?

	Fractional regime			Sublinear regime	
ϵ	$\in (0,1)$	$2/3$	$\rightarrow 2/5$	$o(1)$	$o(1)$
k	$\leq \log\log s$	4	$\omega(1)$	$\leq \log\log s$	$\text{depth}^{1-o(1)}$

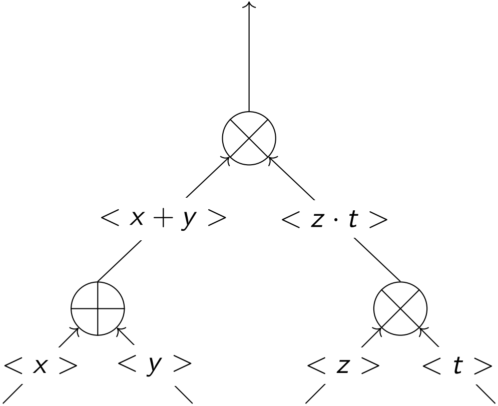


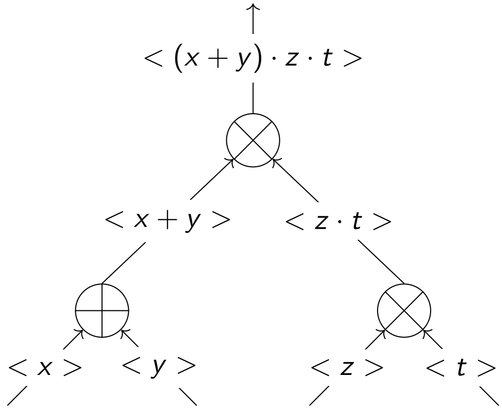

< x >
< y >

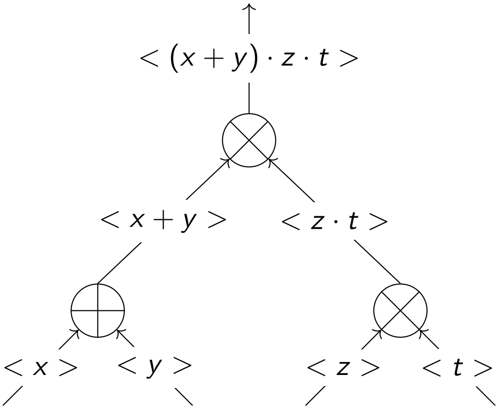

$< x + y >$
$< x >$
$< y >$



< x + y >
< x >
< y >
< z >
< t >


$< x + y >$
$< z \cdot t >$
$< x >$
$< y >$
$< z >$
$< t >$

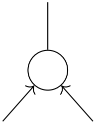

$< (x+y) \cdot z \cdot t >$
$< x+y >$
$< z \cdot t >$
$< x >$
$< y >$
$< z >$
$< t >$



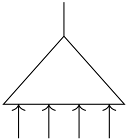
1 bit per gate per party

Gate-by-gate

Communication: s
Computation: s



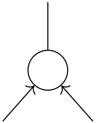
"truth-table-by-truth-table"



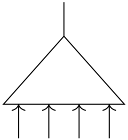
Communication: $s \cdot \epsilon$
Computation: $s \cdot 2^{2^k}$

Gate-by-gate

Communication: s
Computation: s



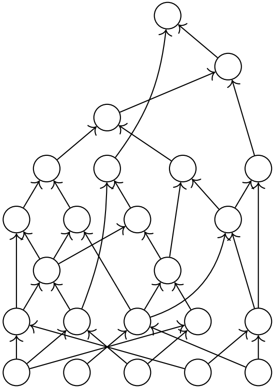
"truth-table-by-truth-table"



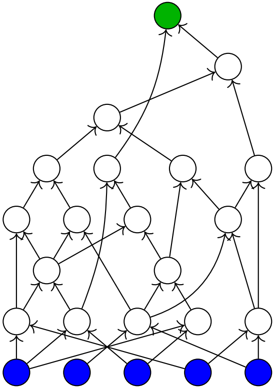
Communication: $s \cdot \epsilon$
Computation: $s \cdot 2^{2^k}$

fact©

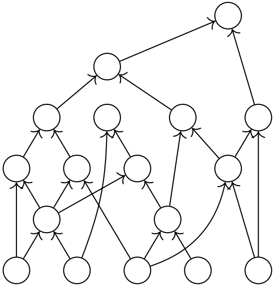
Works with correlated randomness, Homomorphic Secret Sharing, Somewhat Homomorphic Encryption, low-rate PIR...



- Take the underlying DAG G

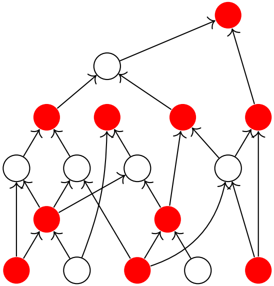


- Take the underlying DAG G
- Remove all input and output nodes



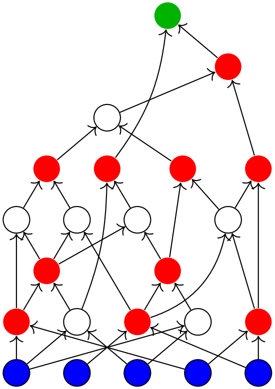
- Take the underlying DAG G
- Remove all input and output nodes

ℓ-path hitting set:
Vertex set intersecting every chain $u_1 \to \cdots \to u_\ell$



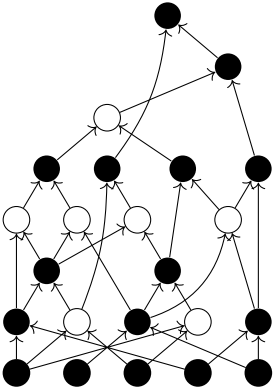
- Take the underlying DAG G
- Remove all input and output nodes
- Find a size-ϵ $(\log k)$-path hitting set

ℓ-path hitting set:
Vertex set intersecting every chain $u_1 \to \cdots \to u_\ell$

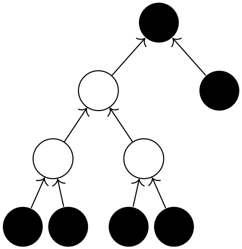


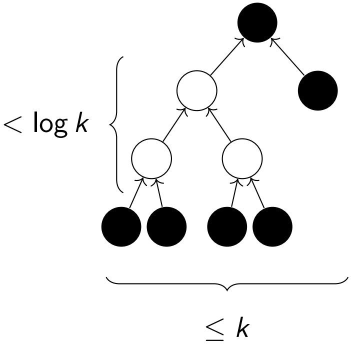
- Take the underlying DAG G
- Remove all input and output nodes
- Find a size-ϵ $(\log k)$-path hitting set
- Return the inputs and outputs

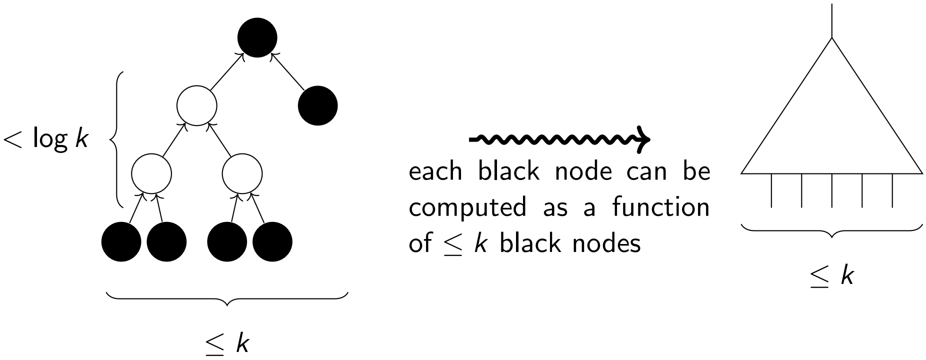
ℓ-path hitting set:
Vertex set intersecting every chain $u_1 \to \cdots \to u_\ell$



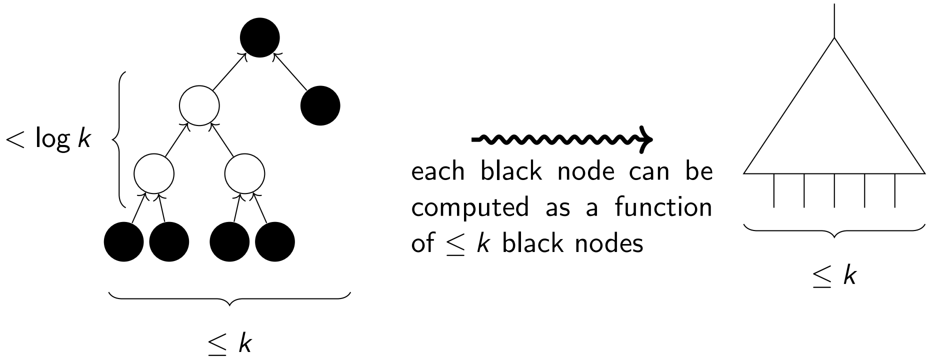
- Take the underlying DAG G
- Remove all input and output nodes
- Find a size-ϵ $(\log k)$-path hitting set
- Return the inputs and outputs




$< \log k$
$\leq k$



$< \log k$
$\leq k$
each black node can be computed as a function of $\leq k$ black nodes
$\leq k$



The size-s fan-in-2 circuit can be computed by a size-$(\epsilon \cdot s)$ fan-in-k circuit
IF there exists a size-ϵ $(\log k)$-path hitting set

1. $\forall \ell > 1$, ℓ-path hitting set is NP-hard in general graphs...
   ($\ell = 2$ is "Vertex Cover")

1. $\forall \ell > 1$, ℓ-path hitting set is NP-hard in general graphs. . .
   ($\ell = 2$ is "Vertex Cover")

2. . . . but **NOT** always hard in 2-degenerate graphs

2-degenerate $\approx$ fan-in 2

1. $\forall \ell > 1$, ℓ-path hitting set is NP-hard in general graphs…
   ($\ell = 2$ is "Vertex Cover")

2-degenerate $\approx$ fan-in 2

2. …but **NOT** always hard in 2-degenerate graphs
   - 3-colouring-based algorithm:

$$\epsilon = 2/3, \ k = 4$$

   - Feedback Vertex Set (FVS)-based algorithm:

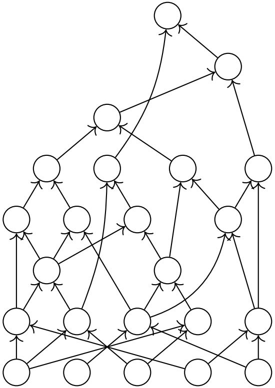
$$\epsilon = 2/5 \cdot (1 + \frac{3/5}{k}), \ \text{any } k \leq d$$

   - Valiant's edge-partitioning algorithm:

$$\epsilon = n \cdot (1 - \frac{\log k}{\log d}), \ \text{any } k \leq d$$

FVS:
Vertex set whose removal yields a forest

First algorithm, based on 3-colouring



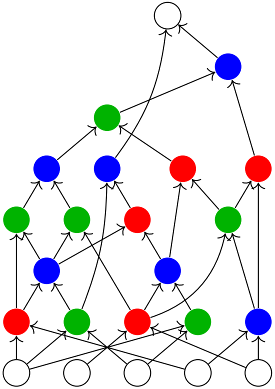
- Colour greedily in topological order

  (fan-in 2 implies there is always one of the three colours available)

- The union of the two smallest partitions is a vertex cover of size $\leq \lfloor 2s/3 \rfloor$

  (the complement—*i.e.* the largest colour—is an independent set of size at least $\lceil s/3 \rceil$)

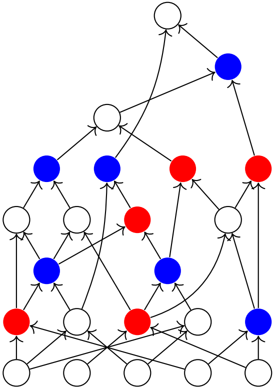
First algorithm, based on 3-colouring



- Colour greedily in topological order
  (fan-in 2 implies there is always one of the three colours available)

- The union of the two smallest partitions is a vertex cover of size $\leq \lfloor 2s/3 \rfloor$
  (the complement—*i.e.* the largest colour—is an independent set of size at least $\lceil s/3 \rceil$)

First algorithm, based on 3-colouring



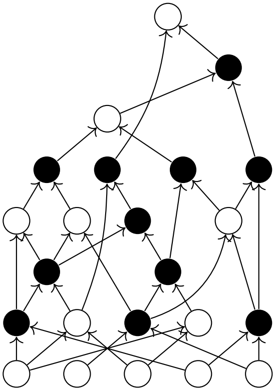
- Colour greedily in topological order

  (fan-in 2 implies there is always one of the three colours available)

- The union of the two smallest partitions is a vertex cover of size $\leq \lfloor 2s/3 \rfloor$

  (the complement—*i.e.* the largest colour—is an independent set of size at least $\lceil s/3 \rceil$)

First algorithm, based on 3-colouring



- Colour greedily in topological order

  (fan-in 2 implies there is always one of the three colours available)

- The union of the two smallest partitions is a vertex cover of size $\leq \lfloor 2s/3 \rfloor$

  (the complement—*i.e.* the largest colour—is an independent set of size at least $\lceil s/3 \rceil$)

Breaking the circuit-size barrier for information-theoretic MPC in the correlated randomness model

Selected Result: Fractionally linear-communication MPC for all circuits

Any size-s circuit can be securely computed in the correlated randomness model using $2s/5 + o(s)$ bits of communication per party and $\text{poly}(s)$ bits of computation.

1. Ring- and basis-agnostic (but no free-xor)
2. Not just asymptotic (explicit constants), and linear-time algorithms
3. **Also in the paper:** Applications to the "Bootstrapping Problem" for FHE

`https://ia.cr/2024/1473`

(more applications than presented here)