

Optimization of Bootstrapping in Circuits

Fabrice Benhamouda

Tancredi Lepoint

Claire Mathieu

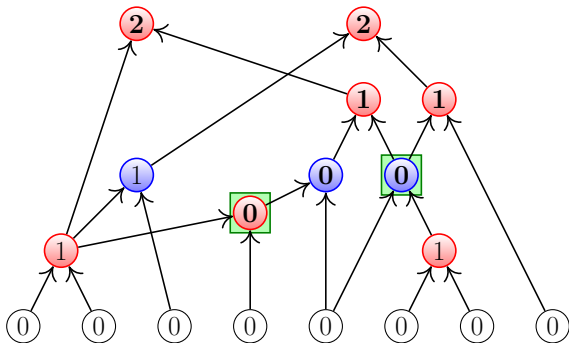
Hang Zhou

IBM Research, USA

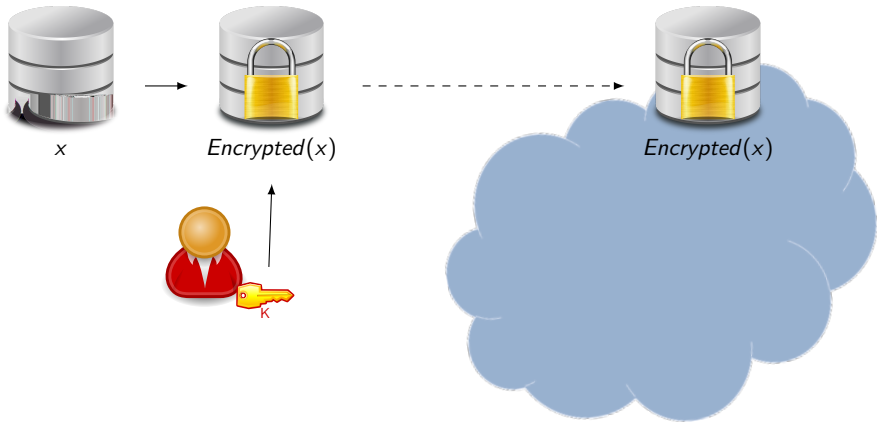
SRI International

École Normale Supérieure

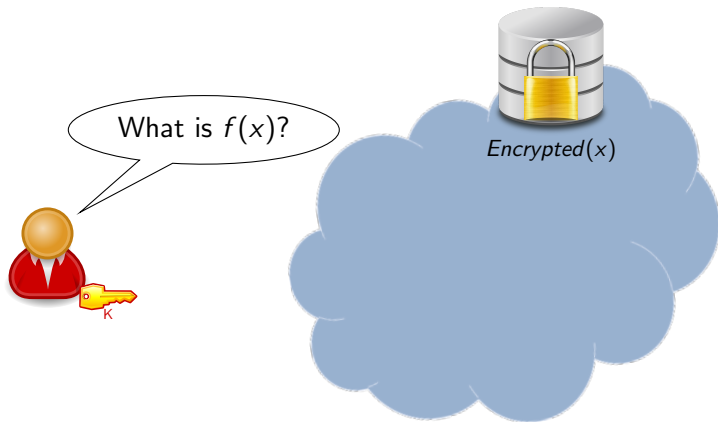
Max Planck Institute



Motivation: Classical Encryption

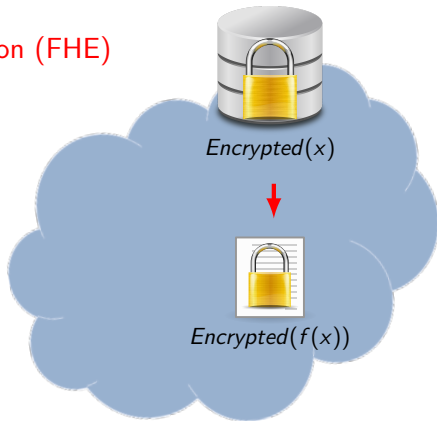


Motivation: Classical Encryption



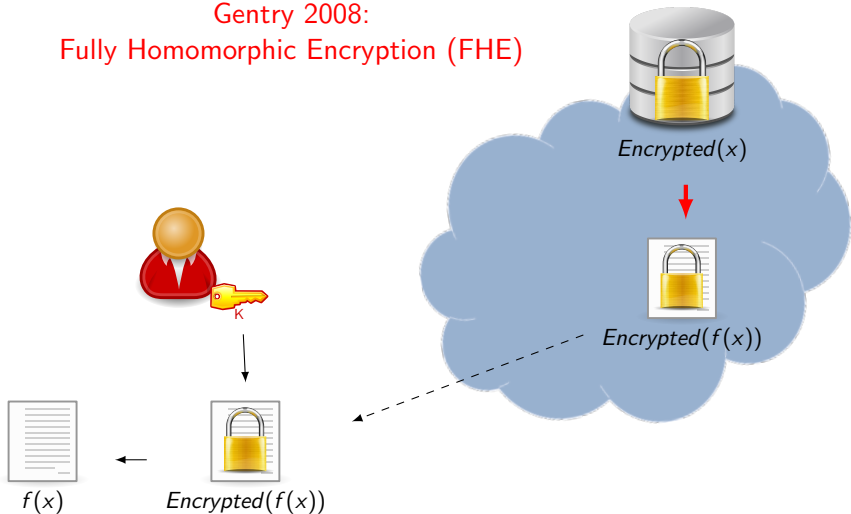
Motivation: Fully Homomorphic Encryption

Gentry 2008:
Fully Homomorphic Encryption (FHE)

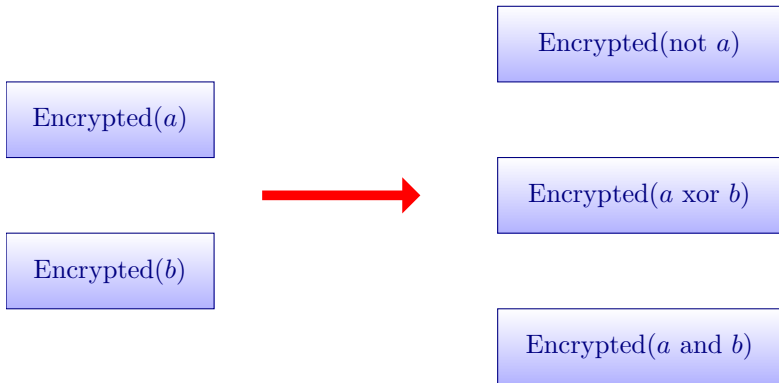


Motivation: Fully Homomorphic Encryption

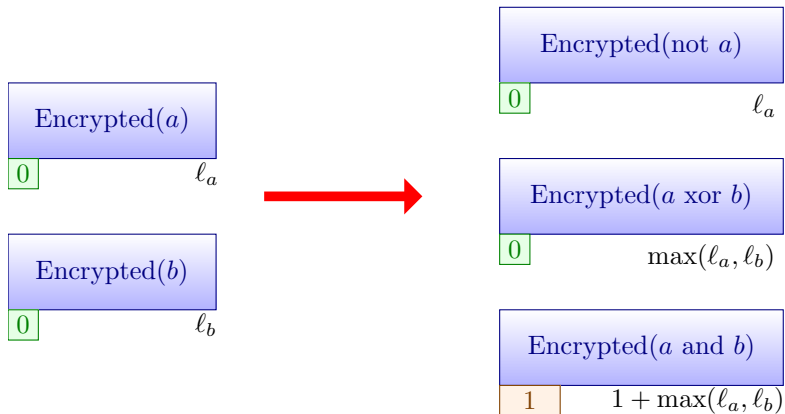
Gentry 2008:
Fully Homomorphic Encryption (FHE)



Motivation: Fully Homomorphic Encryption in Details



Motivation: Noise Level



Valid for decryption:

noise level within **some parameter L** ($L \approx 17$ in practice)



Motivation: Bootstrap Operations



Goal: Minimize the number of bootstrap operations

Bootstrap Problem

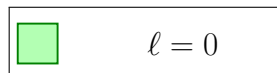
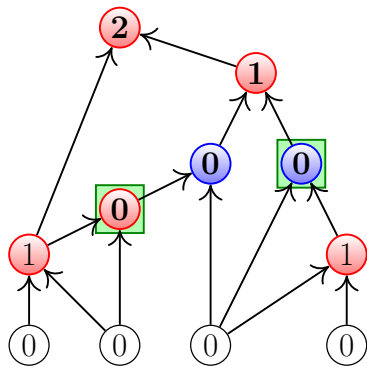
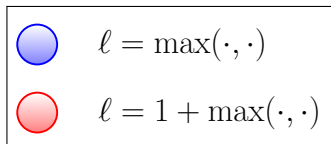
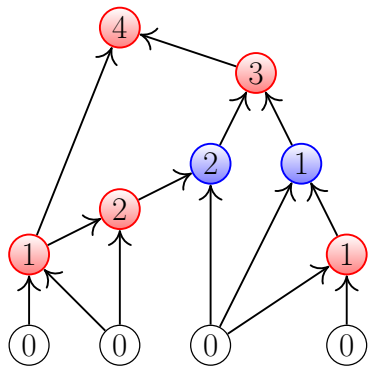
Input:

- a directed acyclic graph $G = (V, E)$ with two kinds of vertices:
 -  $\ell = \max(\cdot, \cdot)$
 -  $\ell = 1 + \max(\cdot, \cdot)$
- an integer parameter L

Output:

- a subset $S \subseteq V$ of minimum cardinality such that bootstrapping S ensures $\ell \leq L$ at every vertex

Example



$L = 2$

Previous Results

- Greedy approaches with approximation ratio $\Omega(|V|)$
[Gentry Halevi 2011; Gentry Halevi Smart 2012]
- Heuristic method
[Lepoint Paillier 2013]
- Polynomial time algorithm for $L = 1$ and NP-hardness for $L \geq 2$
[Paindavoine Vialla 2015]

Our Results

Approximation

Polynomial-time L -approximation algorithm ($L \geq 1$)

Idea: linear program and [new rounding scheme](#)

Inapproximability

NP-hard to compute an $(L - \epsilon)$ -approximation ($L \geq 2$), assuming the Unique Games Conjecture

Idea: reduction to the [DAG vertex deletion](#) problem [Svensson 2013]

Our Results

Approximation

Polynomial-time L -approximation algorithm ($L \geq 1$)

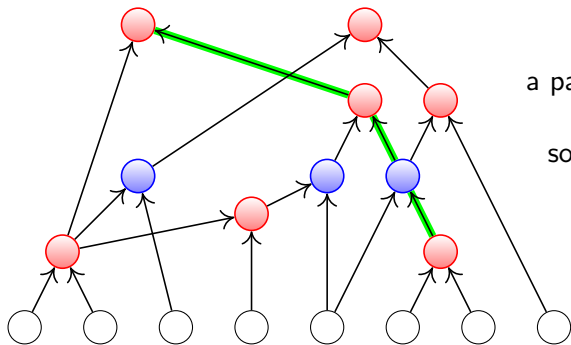
Idea: linear program and [new rounding scheme](#)

Inapproximability

NP-hard to compute an $(L - \epsilon)$ -approximation ($L \geq 2$), assuming the Unique Games Conjecture

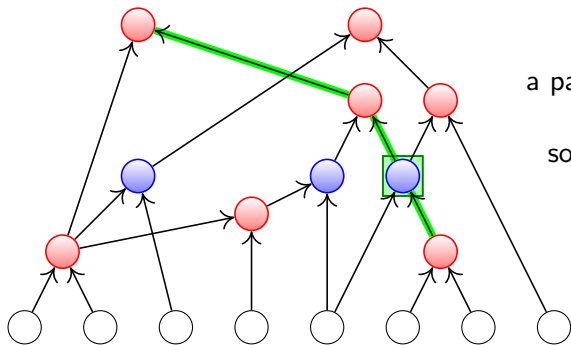
Idea: reduction to the [DAG vertex deletion](#) problem [Svensson 2013]

Preliminary Observation



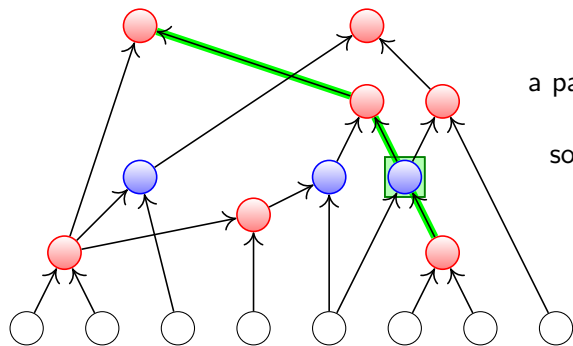
$L = 2$
a path containing 3 red vertices
↓
some vertex is bootstrapped

Preliminary Observation



$L = 2$
a path containing 3 red vertices
↓
some vertex is bootstrapped

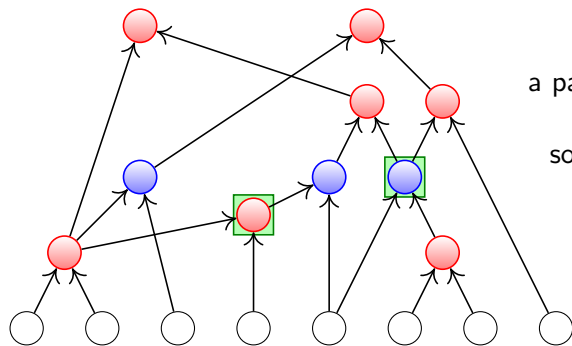
Preliminary Observation



$L = 2$
a path containing 3 red vertices
↓
some vertex is bootstrapped

Interesting path: containing $L + 1$ red vertices

Preliminary Observation



$L = 2$
a path containing 3 red vertices
 \Downarrow
some vertex is bootstrapped

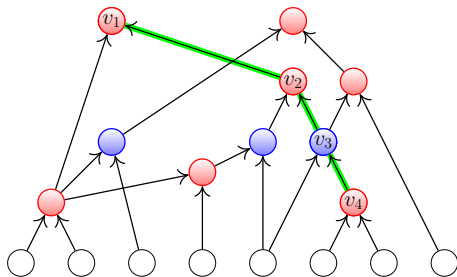
Interesting path: containing $L + 1$ red vertices

Observation

bootstrap solution \iff every **interesting path** has a bootstrapped vertex

Linear Program Relaxation

$$x_v = \begin{cases} 1 & \text{if } v \text{ is bootstrapped} \\ 0 & \text{otherwise} \end{cases}$$



constraint: $x_{v_1} + x_{v_2} + x_{v_3} + x_{v_4} \geq 1$

$$\min \sum_{v \in V} x_v$$

$$\text{s. t. } \sum_{v \in p} x_v \geq 1$$

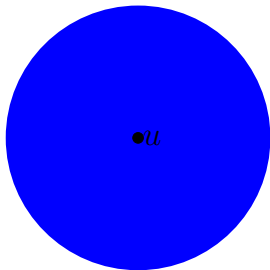
$$0 \leq x_v \leq 1$$

\forall interesting path p

$$\forall v \in V$$

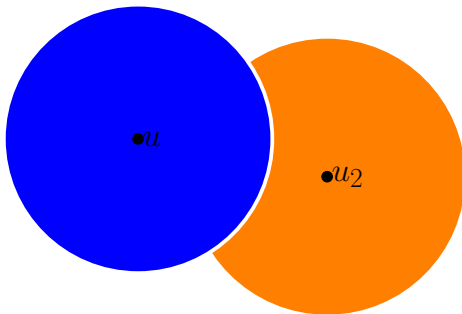
Standard Rounding: Sphere Growing Technique

- 1 choose a vertex u
- 2 compute distance from u in metric of $\{x_v\}$
- 3 bootstrap all vertices at distance ≈ 0.5
- 4 repeat



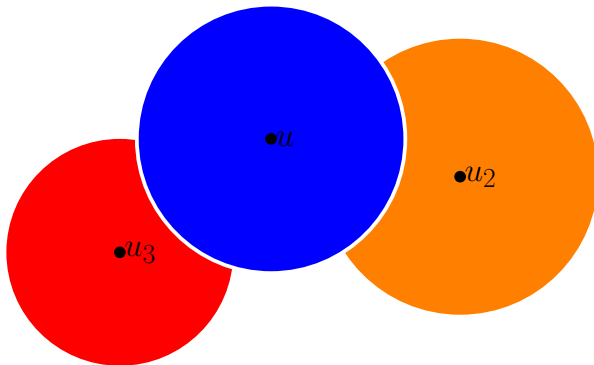
Standard Rounding: Sphere Growing Technique

- 1 choose a vertex u
- 2 compute distance from u in metric of $\{x_v\}$
- 3 bootstrap all vertices at distance ≈ 0.5
- 4 repeat

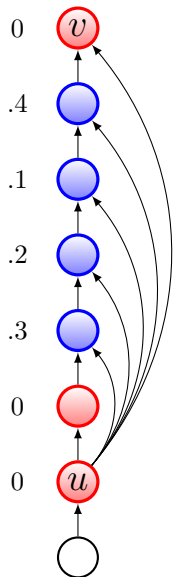


Standard Rounding: Sphere Growing Technique

- 1 choose a vertex u
- 2 compute distance from u in metric of $\{x_v\}$
- 3 bootstrap all vertices at distance ≈ 0.5
- 4 repeat



Standard Rounding: Counter Example



$$L = 2$$

u -to- v distance in the metric is 0.

New Rounding

Definition:

- length of a path: sum of x_v along the path
- For every $i \leq L$, define $f_{v,i}$:
minimum length of a path that ends at v and contains i red vertices.
- Interval $A_{v,i} := [f_{v,i}, f_{v,i} + x_v]$.

Randomized Rounding

- 1 Pick $t \in [0, 1]$ uniformly at random
- 2 For every vertex v , bootstrap v if $t \in A_{v,i}$ for some $i \in \{1, \dots, L\}$.

Every interesting path v_1, \dots, v_k contains a bootstrapped vertex.

Define $A_{v_j}^* := A_{v_j, i_j}$, where $i_j := \#$ red vertices among v_1, \dots, v_j .

Claim

The union of $A_{v_j}^*$ covers the $[0, 1]$ -interval.

Claim

The union of $A_{v_j}^*$ covers the $[0, 1]$ -interval.

Proof:

- 1 $A_{v_1}^*$ starts at 0;
- 2 every pair of consecutive intervals $A_{v_j}^*$ and $A_{v_{j+1}}^*$ intersect;
- 3 $A_{v_k}^*$ covers 1.



Claim

The union of $A_{v_j}^*$ covers the $[0, 1]$ -interval.

Proof:

- 1 $A_{v_1}^*$ starts at 0;
- 2 every pair of consecutive intervals $A_{v_j}^*$ and $A_{v_{j+1}}^*$ intersect;
- 3 $A_{v_k}^*$ covers 1.



Claim

The union of $A_{v_j}^*$ covers the $[0, 1]$ -interval.

Proof:

- 1 $A_{v_1}^*$ starts at 0;
- 2 every pair of consecutive intervals $A_{v_j}^*$ and $A_{v_{j+1}}^*$ intersect;
- 3 $A_{v_k}^*$ covers 1.



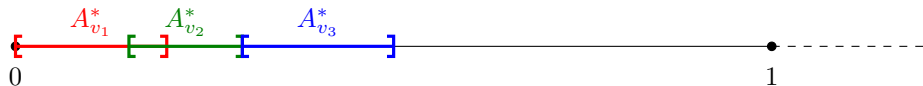
$$f_{v_{j+1}, i_{j+1}} \leq f_{v_j, i_j} + x_{v_j} \text{ by definition of } f$$

Claim

The union of $A_{v_j}^*$ covers the $[0, 1]$ -interval.

Proof:

- 1 $A_{v_1}^*$ starts at 0;
- 2 every pair of consecutive intervals $A_{v_j}^*$ and $A_{v_{j+1}}^*$ intersect;
- 3 $A_{v_k}^*$ covers 1.



$$f_{v_{j+1}, i_{j+1}} \leq f_{v_j, i_j} + x_{v_j} \text{ by definition of } f$$

Correctness

Claim

The union of $A_{v_j}^*$ covers the $[0, 1]$ -interval.

Proof:

- 1 $A_{v_1}^*$ starts at 0;
- 2 every pair of consecutive intervals $A_{v_j}^*$ and $A_{v_{j+1}}^*$ intersect;
- 3 $A_{v_k}^*$ covers 1.



$$f_{v_{j+1}, i_{j+1}} \leq f_{v_j, i_j} + x_{v_j} \text{ by definition of } f$$

Claim

The union of $A_{v_j}^*$ covers the $[0, 1]$ -interval.

Proof:

- 1 $A_{v_1}^*$ starts at 0;
- 2 every pair of consecutive intervals $A_{v_j}^*$ and $A_{v_{j+1}}^*$ intersect;
- 3 $A_{v_k}^*$ covers 1.



$$f_{v_{j+1}, i_{j+1}} \leq f_{v_j, i_j} + x_{v_j} \text{ by definition of } f$$

Claim

The union of $A_{v_j}^*$ covers the $[0, 1]$ -interval.

Proof:

- 1 $A_{v_1}^*$ starts at 0;
- 2 every pair of consecutive intervals $A_{v_j}^*$ and $A_{v_{j+1}}^*$ intersect;
- 3 $A_{v_k}^*$ covers 1.



$$i_k = L + 1 \quad \implies \quad f_{v_k, i_k} \geq 1 \text{ by definition of } f \text{ and LP constraints}$$

Approximation Ratio

A vertex v is bootstrapped if $t \in A_{v,i}$ for some $i \in \{1, \dots, L\}$.

$$\mathbb{P}[v \text{ is bootstapped}] \leq L \cdot x_v.$$

Expected number of bootstrapped vertices:

$$\sum_{v \in V} L \cdot x_v \leq L \cdot \text{OPT}.$$

Derandomization

$\{f_{v,i}\}_{v,i} \cup \{f_{v,i} + x_v\}_{v,i}$ contains $2|V| \cdot L$ values.

$[0, 1]$ interval is decomposed into $O(|V| \cdot L)$ sub-intervals.

Deterministic Rounding

- 1 For each sub-interval, pick any t and perform the previous rounding;
- 2 Return the best solution found.

Conclusion

Approximation

Polynomial-time L -approximation algorithm ($L \geq 1$)

Inapproximability

NP-hard to compute an $(L - \epsilon)$ -approximation ($L \geq 2$), assuming the Unique Games Conjecture

Thank you!