Rump Session 2016

FHE Circuit Privacy Almost For Free

Michele Minelli

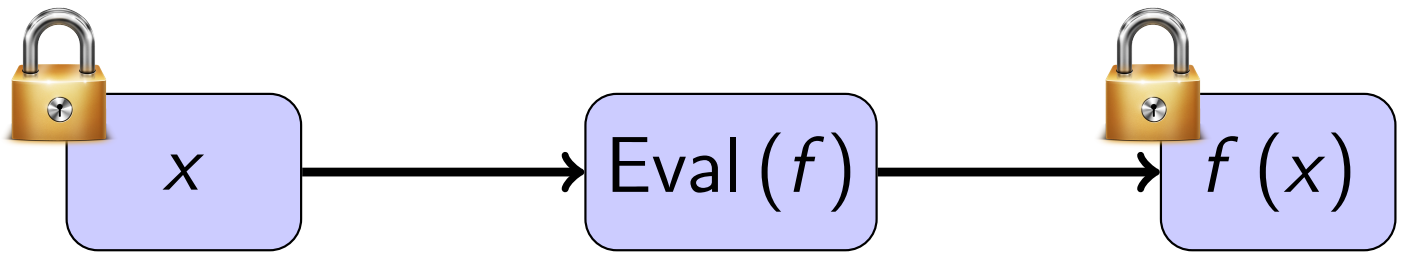
ENS

Florian Bourse Rafaël Del Pino **Michele Minelli** Hoeteck Wee

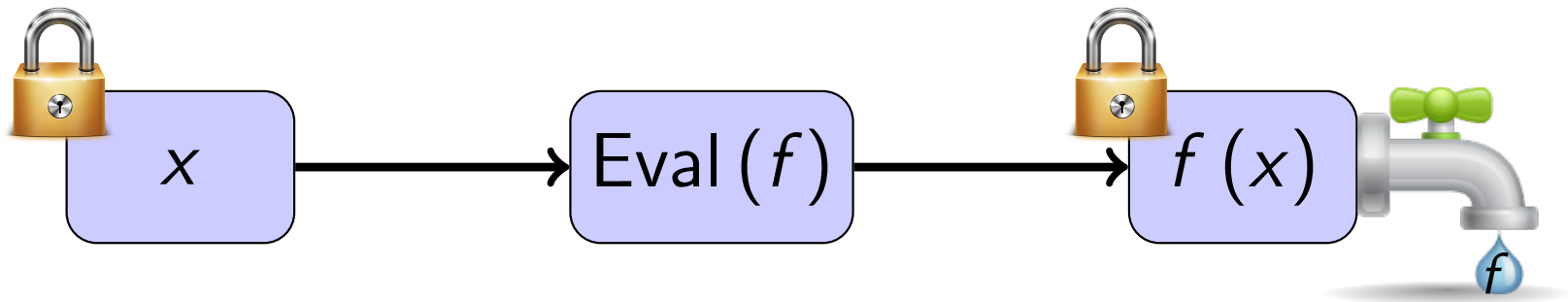
Ecole Normale Supérieure

FHE Circuit Privacy Almost For Free

FHE and circuit privacy

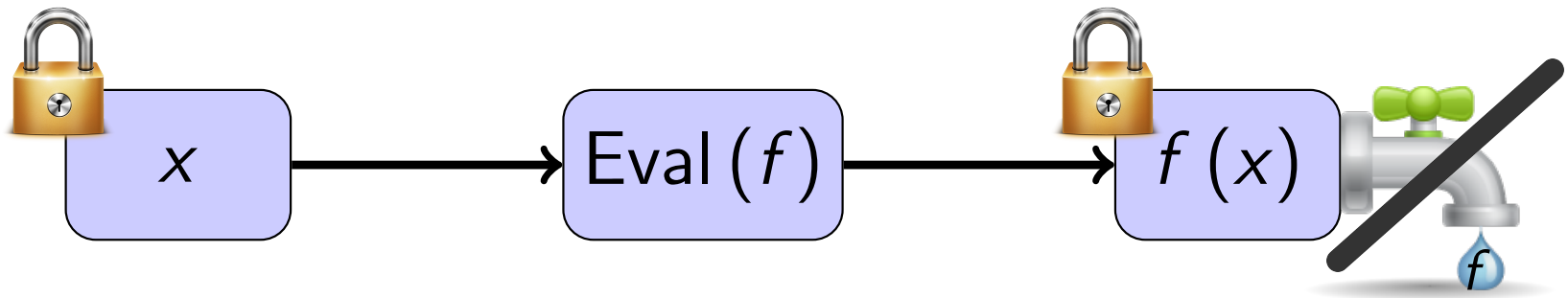


FHE and circuit privacy



The output ct. leaks information about f

FHE and circuit privacy



The output ct. leaks information about f

Goal: circuit privacy, i.e. hide f

Prior FHE for NC1

reference	standard LWE	poly hardness	multi hop	circuit-private
[BV14,AP14]	✓	✓	✓	
[Gen09]	✓		✓	✓
[GHV10, OPP14]	✓	✓		✓
[DS16]		✓	✓	✓
this work	✓	✓	✓	✓

Our scheme

[GSW13,BV14,AP14] + small noise

Analysis of the noise distribution
(instead of just giving a bound)

Our core lemma ([AR13,AGHS13])

$$\mathbf{e}^{\mathsf{T}} \cdot \mathbf{G}_{\mathsf{rand}}^{-1}(\mathbf{v})$$

error in output ciphertext

Our core lemma ([AR13,AGHS13])

$$\mathbf{e}^{\intercal} \cdot \mathbf{G}_{\text{rand}}^{-1}(\mathbf{v}) + y$$

y: poly noise

$\mathbf{e}^{\intercal} \cdot \mathbf{G}_{\text{rand}}^{-1}(\mathbf{v})$: error in output ciphertext

Our core lemma ([AR13,AGHS13])

$$\mathbf{e}^{\intercal} \cdot \mathbf{G}_{\text{rand}}^{-1}(\mathbf{v}) + y \approx_s e'$$

error in output ciphertext

poly noise

"fresh" Gaussian

Our core lemma ([AR13,AGHS13])

$$\mathbf{e}^{\intercal} \cdot \mathbf{G}_{\text{rand}}^{-1}(\mathbf{v}) + y \approx_s e'$$

error in output ciphertext

poly noise

"fresh" Gaussian

$$\mathbf{v} \text{ is hidden} \Rightarrow f \text{ is hidden}$$

Our core lemma ([AR13,AGHS13])

$$\mathbf{e}^{\intercal} \cdot \mathbf{G}_{\text{rand}}^{-1}(\mathbf{v}) + y \approx_s e'$$

error in output ciphertext

poly noise

"fresh" Gaussian

$\mathbf{v}$ is hidden $\Rightarrow$ f is hidden

ePrint 2016/381

Thank you!