On Treewidth, Separators and Yao's Garbling

Chethan Kamath Karen Klein Krzysztof Pietrzak

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

ETH zürich

IST AUSTRIA
Institute of Science and Technology

קרן עזריאלי
Azrieli Foundation
תוכנית עמיתי עזריאלי
Azrieli Fellows Program

erc

TCC 2021, Raleigh, US

Our Result

- **Theorem.** For Boolean circuits of size S and *treewidth* $w = w(S)$, Yao's garbling Γ is *adaptively-indistinguishable* with a loss in security $S^{O(w)}$.

- **Remarks:**
  1. Applebaum et al. [AIKW13] ruled out adaptive-*simulatability* of Γ
  2. Jafargholi-Wichs [JW16] proved adaptive-simulatability of Γ', a *variant* of Γ
  3. We can prove adaptive-simulatability of Γ' in terms of treewidth

Overview

Garbling

Security Models

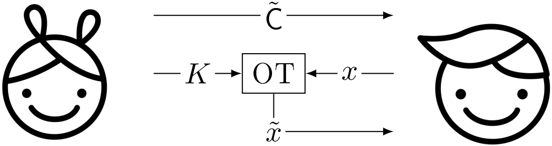
Yao's Garbling

Our Reduction

Garbling [Y86]

Circuit $\mathsf{C} : \{0,1\}^n \to \{0,1\}^\ell$

Input $x \in \{0,1\}^n$



$\tilde{\mathsf{C}}$

K

OT

x

$\tilde{x}$

$(\tilde{\mathsf{C}}, K) \leftarrow \mathsf{GCircuit}(\mathsf{C}, 1^\lambda)$

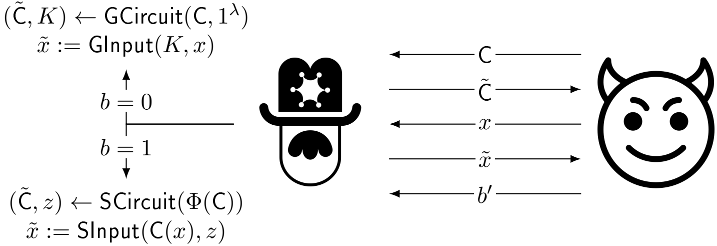
$\mathsf{C}(x) := \mathsf{GEval}(\tilde{\mathsf{C}}, \tilde{x})$

Garbling [BHR12]

- **Syntax**
  - $(\tilde{\mathsf{C}}, K) \leftarrow \mathsf{GCircuit}(\mathsf{C}, 1^\lambda)$
  - $\tilde{x} \leftarrow \mathsf{GInput}(x, K)$
  - $y := \mathsf{GEval}(\tilde{\mathsf{C}}, \tilde{x})$
- **Correctness** $\forall\lambda$, $\forall\mathsf{C}, \forall x$:

$$\Pr_{\substack{(\tilde{\mathsf{C}},K)\leftarrow\mathsf{GCircuit}(\mathsf{C},1^\lambda)\\ \tilde{x}\leftarrow\mathsf{GInput}(x,K)}}\left[\mathsf{GEval}(\tilde{\mathsf{C}}, \tilde{x}) = \mathsf{C}(x)\right] = 1$$

Security: Adaptive Simulatability



$(\tilde{\mathsf{C}}, K) \leftarrow \mathsf{GCircuit}(\mathsf{C}, 1^{\lambda})$

$\tilde{x} := \mathsf{GInput}(K, x)$

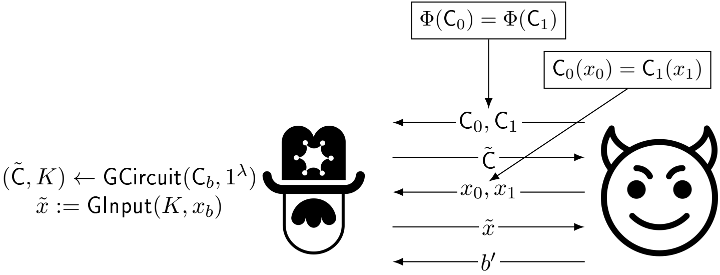
$b = 0$

$b = 1$

$(\tilde{\mathsf{C}}, z) \leftarrow \mathsf{SCircuit}(\Phi(\mathsf{C}))$

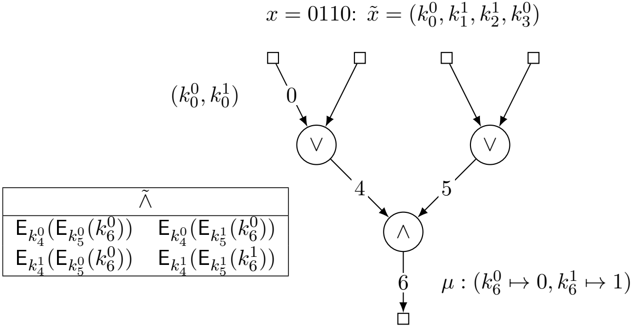
$\tilde{x} := \mathsf{SInput}(\mathsf{C}(x), z)$

Security: Adaptive Indistinguishability


$\Phi(\mathsf{C}_0) = \Phi(\mathsf{C}_1)$
$\mathsf{C}_0(x_0) = \mathsf{C}_1(x_1)$
$(\tilde{\mathsf{C}}, K) \leftarrow \mathsf{GCircuit}(\mathsf{C}_b, 1^\lambda)$
$\tilde{x} := \mathsf{GInput}(K, x_b)$
$\mathsf{C}_0, \mathsf{C}_1$
$\tilde{\mathsf{C}}$
x_0, x_1
$\tilde{x}$
b'

- Adaptive Simulatability $\implies$ Adaptive Indistinguishability
- Application: restricted symmetric-key FE [JSW17]

Yao's Garbling Γ



$x = 0110$: $\tilde{x} = (k_0^0, k_1^1, k_2^1, k_3^0)$

$\tilde{\wedge}$	
$\mathsf{E}_{k_4^0}(\mathsf{E}_{k_5^0}(k_6^0))$	$\mathsf{E}_{k_4^0}(\mathsf{E}_{k_5^1}(k_6^0))$
$\mathsf{E}_{k_4^1}(\mathsf{E}_{k_5^0}(k_6^0))$	$\mathsf{E}_{k_4^1}(\mathsf{E}_{k_5^1}(k_6^1))$

- Each wire in $w \in \mathsf{C}$ associated with secret keys (k_w^0, k_w^1)
- Garbled circuit, $\tilde{\mathsf{C}} := (\{\tilde{g}\}_{g \in \mathsf{C}}, \mu)$
    - Garbling table: $\tilde{g}$ for each gate $g \in \mathsf{C}$
    - Output map, μ: (k_w^0, k_w^1) of each o/p wire w mapped to bit
- Garbled i/p, $\tilde{x}$: keys of the i/p wires *selected* using x
- Evaluate: evaluate C "over the encryption"

YAO'S GARBLING Γ...

- Γ: *Online-complexity* depends only on $|x| = n$ (and security parameter)

- **Variant** Γ': o/p map μ sent in *online* phase
  - Garbled circuit: $\tilde{\mathsf{C}} := \{\tilde{g}\}_{g \in \mathsf{C}}$:
  - Garbled i/p: $(\tilde{x}, \mu)$

  - Online complexity depends also on the o/p length ℓ

- E.g.: garbling of a PRG $\mathsf{C} : \{0,1\}^n \to \{0,1\}^{n^c}$
  - Online complexity using Γ' is $\approx n^c$
  - Cannot be adaptively simulatable using Γ

Yao's Garbling: Security Landscape

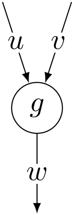
	Selective		Adaptive	
	Γ	Γ'	Γ	Γ'
Simulatability	[LP09]		[AIKW13]	[JW16]
Indistinguishability			This work	

Our Reduction

Garbling Modes

REAL	
$\mathsf{E}_{k_u^0}(\mathsf{E}_{k_v^0}(k_w^{g(0,0)}))$	$\mathsf{E}_{k_u^0}(\mathsf{E}_{k_v^1}(k_w^{g(0,1)}))$
$\mathsf{E}_{k_u^1}(\mathsf{E}_{k_v^0}(k_w^{g(1,0)}))$	$\mathsf{E}_{k_u^1}(\mathsf{E}_{k_v^1}(k_w^{g(1,1)}))$

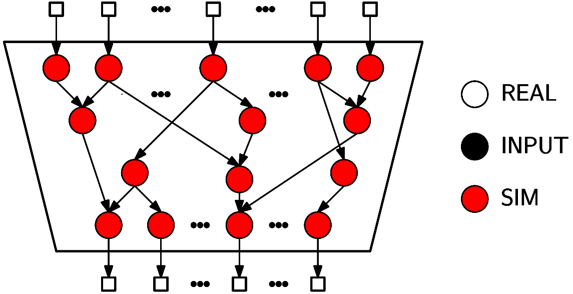
INPUT	
$\mathsf{E}_{k_u^0}(\mathsf{E}_{k_v^0}(k_w^{V(w)}))$	$\mathsf{E}_{k_u^0}(\mathsf{E}_{k_v^1}(k_w^{V(w)}))$
$\mathsf{E}_{k_u^1}(\mathsf{E}_{k_v^0}(k_w^{V(w)}))$	$\mathsf{E}_{k_u^1}(\mathsf{E}_{k_v^1}(k_w^{V(w)}))$



SIM	
$\mathsf{E}_{k_u^0}(\mathsf{E}_{k_v^0}(k_w^{0}))$	$\mathsf{E}_{k_u^0}(\mathsf{E}_{k_v^1}(k_w^{0}))$
$\mathsf{E}_{k_u^1}(\mathsf{E}_{k_v^0}(k_w^{0}))$	$\mathsf{E}_{k_u^1}(\mathsf{E}_{k_v^1}(k_w^{0}))$

- $V(w)$: value of the wire when evaluating $\mathsf{C}(x)$
- Indistinguishability game: $\mathsf{REAL}_0/\mathsf{REAL}_1$, $\mathsf{INPUT}_0/\mathsf{INPUT}_1$

Selective Simulatability [LP09]



- **Hybrid argument**
  1. Replace REAL with INPUT in *topological order*
     - Indistinguishable by ciphertext indistinguishability of SKE
  2. Replace INPUT with SIM in *reverse* topological order:
     - Indistinguishable information-theoretically
- **Programming**
  1. Program o/p map μ so that keys of output wires correctly map to $\mathsf{C}(x)$
- Implies adaptive simulatability with additional 2^n loss

Hurdles to Adaptive Indistinguishability

1. Problem: Input x only available in online phase

   1.1 Problem: Cannot program μ in the offline phase

   - [JW16] solution: Send μ in *online* phase (i.e., Γ'), *defer* programming
   - Our solution: Avoid SIM mode in the hybrids

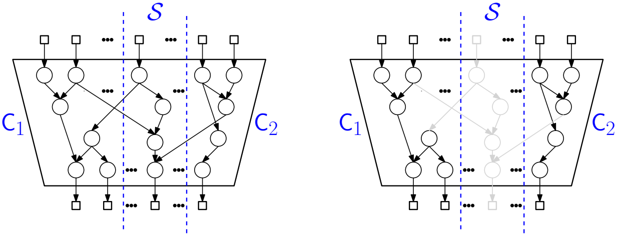
   1.2 Problem: How to simulate INPUT?

   - [JW16] solution: Minimise #INPUT gates and *guess* their values!

2. Problem: How to minimise #INPUT?
   - [JW16] solution: Restrict circuit classes, e.g., low-depth circuits
   - Our solution: *Divide and conquer* via treewidth/separator

Treewidth/Separator

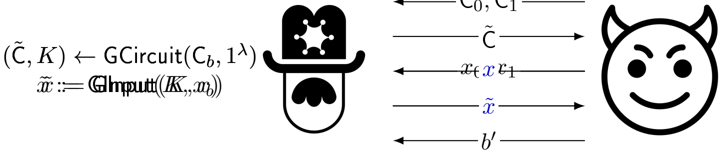
- **Treewidth.** Measure of how 'far' a circuit (DAG) is from a formula (tree)
    - E.g., Boolean formulae have treewidth 1
- **Separator.** A sub-set of gates $\mathcal{S}$ of a circuit C such that *removing* $\mathcal{S}$ (and its incident wires) from C results in *disconnected* sub-circuits of size at most $2/3|\mathsf{C}|$



- **Treewidth-Separator Theorem [RS86].** Any circuit of size S with treewidth $w = w(S)$ has a separator of size w.

Security: Adaptive Indistinguishability

- Simpler indistinguishability game with *single* i/p



$(\tilde{\mathsf{C}}, K) \leftarrow \mathsf{GCircuit}(\mathsf{C}_b, 1^\lambda)$

$\tilde{x} := \mathsf{GInput}(K, x_b)$

$\tilde{x} := \mathsf{GInput}(K, x)$

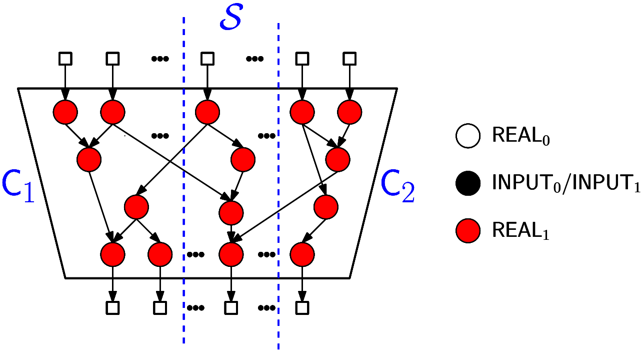
- Garbling modes: $\mathsf{REAL}_0/\mathsf{REAL}_1$, $\mathsf{INPUT}_0/\mathsf{INPUT}_1$

Our Reduction

- **Goal**: Switch all garbling tables from REAL_0 to REAL_1
- **Constraint**: Minimise $\#\mathsf{INPUT}_0/\mathsf{INPUT}_1$ garbling tables
- **Idea**: Maintain $\mathsf{INPUT}_0/\mathsf{INPUT}_1$ gates *only* "at" separator
  - Property of separator $\implies$ can *recurse* on components
  - *Small* separator $\implies$ few $\mathsf{INPUT}_0/\mathsf{INPUT}_1$ gates

Our Reduction...

- Recursive structure of hybrids:
  - Switch gates “on” separator $\mathcal{S}$ to $\mathsf{INPUT}_0/\mathsf{INPUT}_1$
  - *Recursively* switch C_1, C_2 from REAL_0 to REAL_1
  - Switch gates on separator to REAL_1



- $\#\mathsf{INPUT}_0/\mathsf{INPUT}_1 \approx |\mathcal{S}|\delta\log(S)$, δ is the degree

Our Reduction...

- Abstracted out, formalised using a pebble game

- **Lemma** 1. Hybrids corresponding to neighbouring pebble configurations are indistinguishable.
    - Based on ciphertext indistinguishability of SKE or information-theoretically
- **Lemma** 2. There exists a pebble strategy which uses $w\delta \log(S)$ black/gray pebbles.

- **Theorem.** For Boolean circuits of size S and *treewidth* $w = w(S)$, Yao's garbling Γ is *adaptively-indistinguishable* with a loss in security $S^{O(w)}$.
    - Using piecewise-guessing framework [JKK+17]

Thank you!

References

AIKW13 Applebaum, Ishai, Kushilevitz and Waters *Encoding Functions with Constant Online Rate, or How to Compress Garbling Keys*, Crypto 2013

BHR12 Bellare, Hoang and Rogaway, *Foundations of Garbled Circuits*, CCS 2012

JKK+17 Jafargholi, Kamath, Klein, Komargodski, Pietrzak and Wichs, *Be Adaptive, Avoid Overcommitting*, Crypto 2017

JSW17 Jafargholi, Scafuro and Wichs, *Adaptively Indistinguishable Garbled Circuits*, TCC 2017

JW16 Jafargholi and Wichs, *Adaptive Security of Yao's Garbled Circuits*, TCC 2016

LP09 Lindell and Pinkas, *A Proof of Security of Yao's Protocol for Two-Party Computation*, J. Cryptography 2009

RS86 Robertson and Seymour, *Graph Minors II*, J. Algorithms 1986

Acknowledgements

- Ipe Software
- OBS Project
- The Noun Project
  1. Sheriff by Oksana Latysheva
  2. Man, Girl by Zuzanna Nebes
  3. Devil by Alina Oleynik