A Full Characterization of Completeness for Two-party Randomized Function Evaluation

Daniel Kraschewski, Hemanta K. Maji, Manoj Prabhakaran, Amit Sahai

EUROCRYPT 2014

What this talk is about

What this talk is about

- which crypto-gates are all-powerful (such as OT)

What this talk is about

- which crypto-gates are all-powerful (such as OT)
  $\rightsquigarrow$ culminates line of research initiated by [Kilian-88]

What this talk is about

- which crypto-gates are all-powerful (such as OT)
  $\rightsquigarrow$ culminates line of research initiated by [Kilian-88]

What this talk is about

- which crypto-gates are all-powerful (such as OT)
  $\rightsquigarrow$ culminates line of research initiated by [Kilian-88]

- robust foundation of crypto-complexity

What this talk is about

- which crypto-gates are all-powerful (such as OT)
  $\rightsquigarrow$ culminates line of research initiated by [Kilian-88]

- robust foundation of crypto-complexity
  $\rightsquigarrow$ approach for lower complexity bounds?

What this talk is about

- which crypto-gates are all-powerful (such as OT)
  $\rightsquigarrow$ culminates line of research initiated by [Kilian-88]

- robust foundation of crypto-complexity
  $\rightsquigarrow$ approach for lower complexity bounds?

What this talk is about

- which crypto-gates are all-powerful (such as OT)
  $\rightsquigarrow$ culminates line of research initiated by [Kilian-88]

- robust foundation of crypto-complexity
  $\rightsquigarrow$ approach for lower complexity bounds?

- why this is not the end of the road

What this talk is about

- which crypto-gates are all-powerful (such as OT)
  $\rightsquigarrow$ culminates line of research initiated by [Kilian-88]

- robust foundation of crypto-complexity
  $\rightsquigarrow$ approach for lower complexity bounds?

- why this is not the end of the road

Setting

Setting

- information-theoretic security

Setting

- information-theoretic security
- only static corruption

Setting

- information-theoretic security
- only static corruption
- no fairness (i.e., adversarial party can abort after learning own output)

Setting

- information-theoretic security
- only static corruption
- no fairness (i.e., adversarial party can abort after learning own output)
- results hold with respect to UC as well as standalone security notions

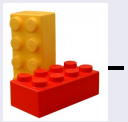
How the story started

How the story started

Yao's Millionaires' Problem [Yao-82]

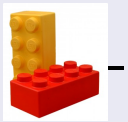
How the story started

Yao's Millionaires' Problem [Yao-82]

- Who has more  -bricks?  or  ?

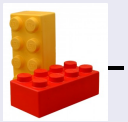
How the story started

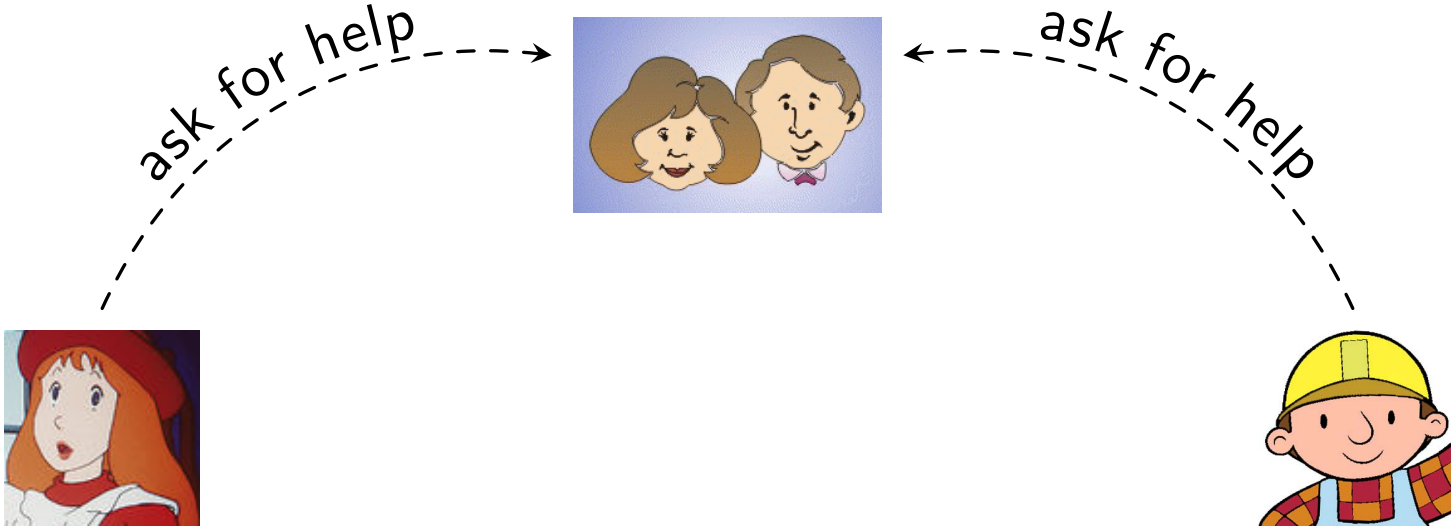
Yao's Millionaires' Problem [Yao-82]

- Who has more  -bricks?  or  ?
- children love secrets, won't reveal own wealth

How the story started

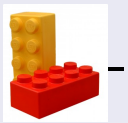
Yao's Millionaires' Problem [Yao-82]

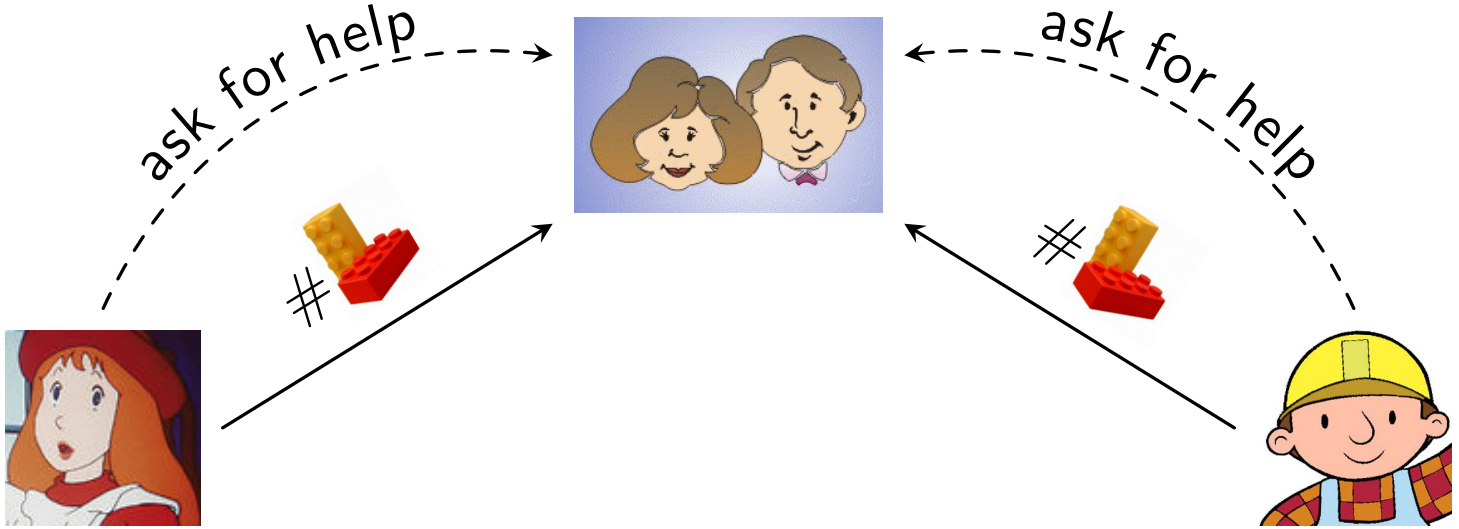
- Who has more  -bricks?  or  ?
- children love secrets, won't reveal own wealth



How the story started

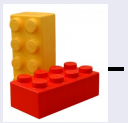
Yao's Millionaires' Problem [Yao-82]

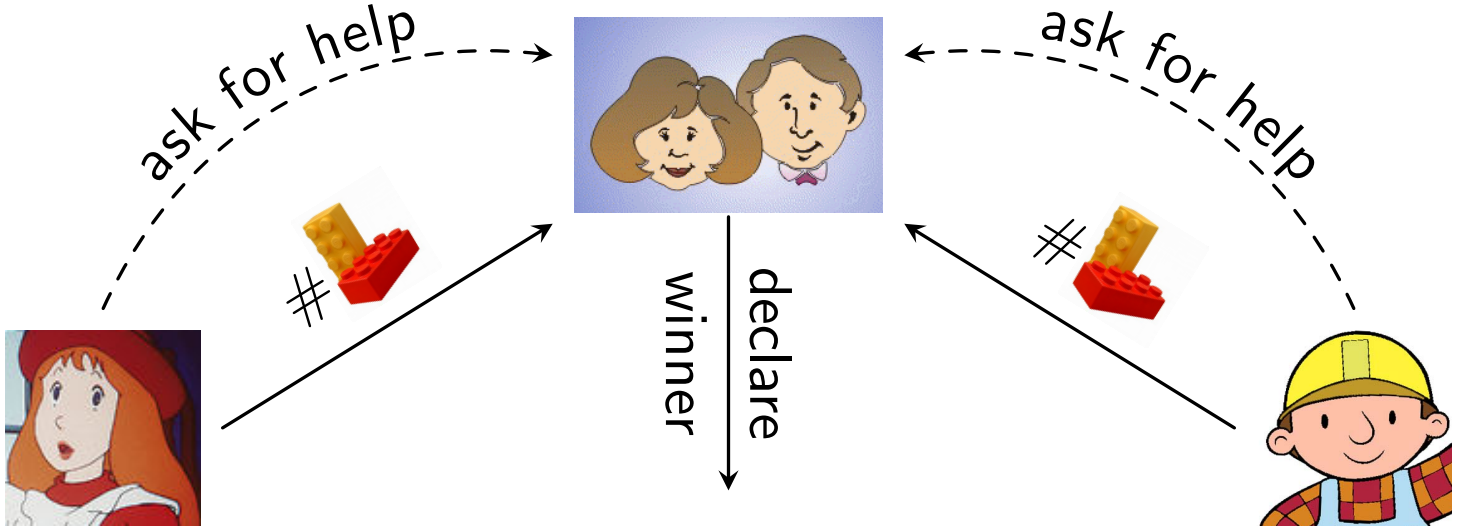
- Who has more  -bricks?  or  ?
- children love secrets, won't reveal own wealth



How the story started

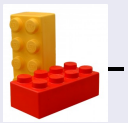
Yao's Millionaires' Problem [Yao-82]

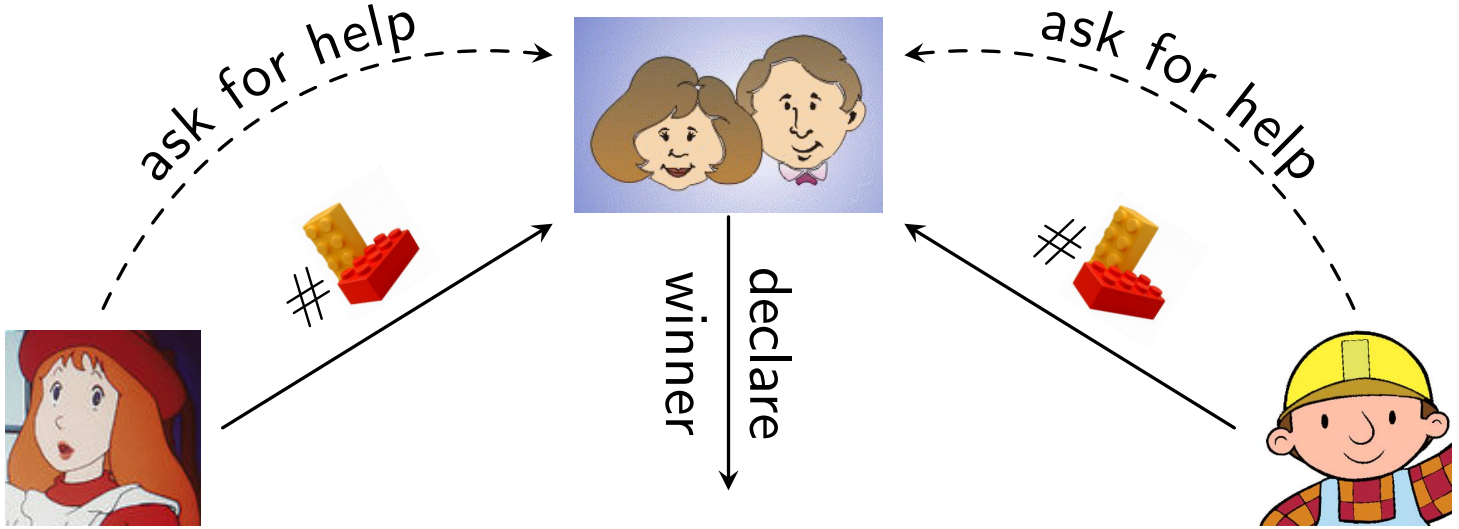
- Who has more  -bricks?  or  ?
- children love secrets, won't reveal own wealth



How the story started

Yao's Millionaires' Problem [Yao-82]

- Who has more  -bricks?  or  ?
- children love secrets, won't reveal own wealth

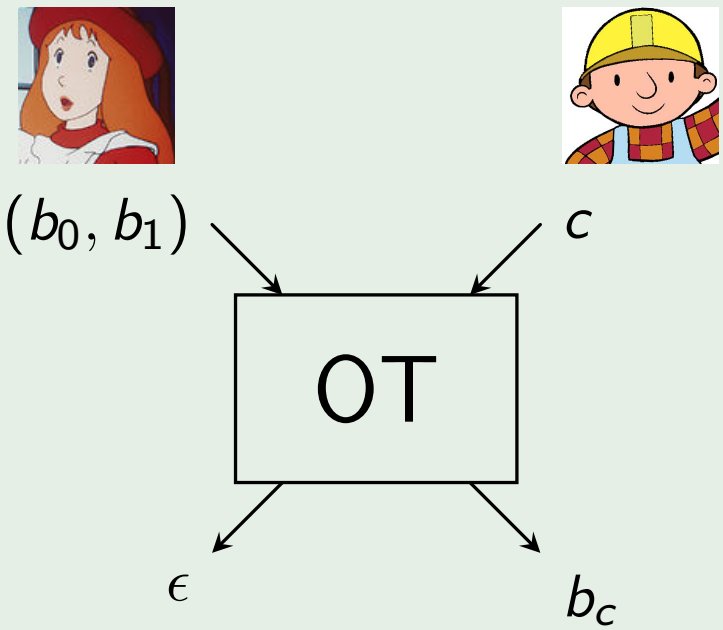


What about less general trusted 3rd parties?

Simple primitives can be very powerful

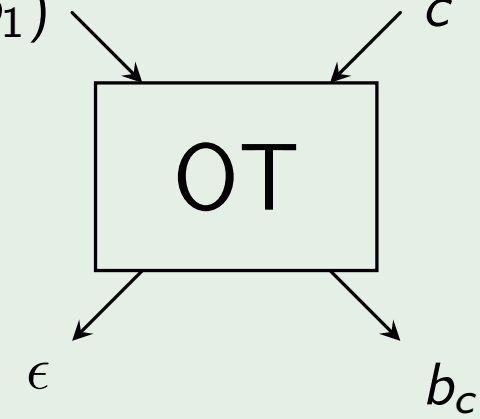
Simple primitives can be very powerful

Oblivious Transfer



Simple primitives can be very powerful

Oblivious Transfer

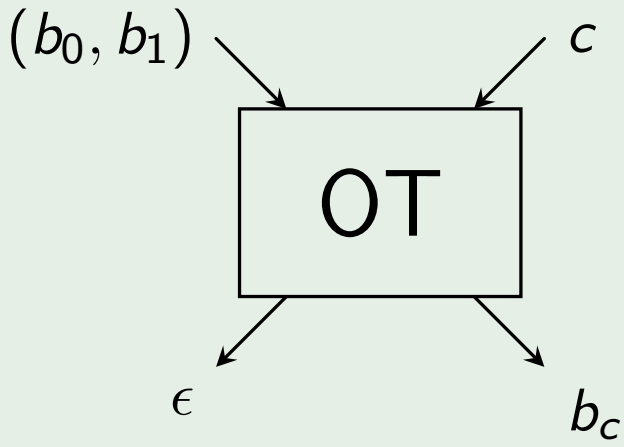



complete (= all-powerful)

[Kilian-88]
[Ishai-Prabhakaran-Sahai-08]

Simple primitives can be very powerful

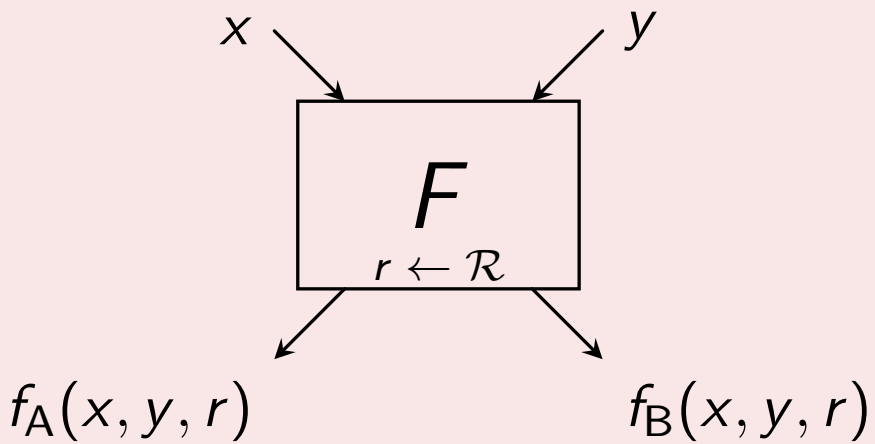
Oblivious Transfer

complete (= all-powerful)

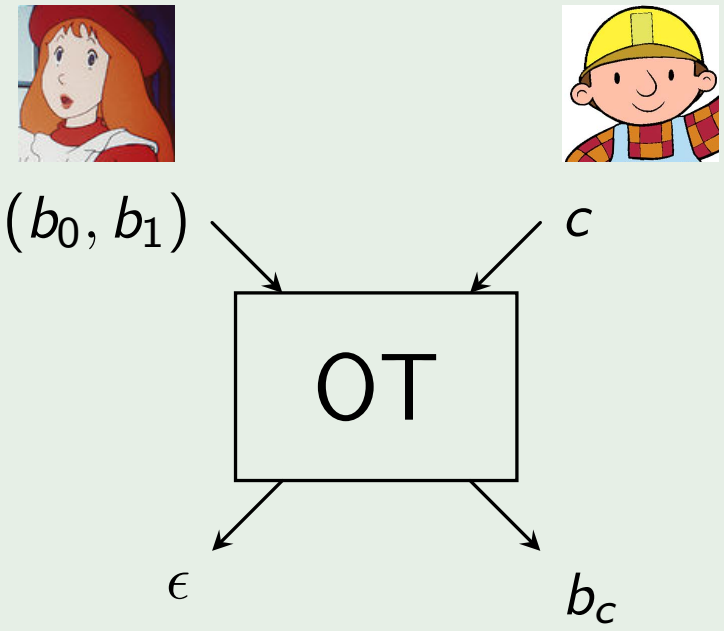
[Kilian-88]
[Ishai-Prabhakaran-Sahai-08]

General crypto-gate $F = (f_A, f_B)$

Simple primitives can be very powerful

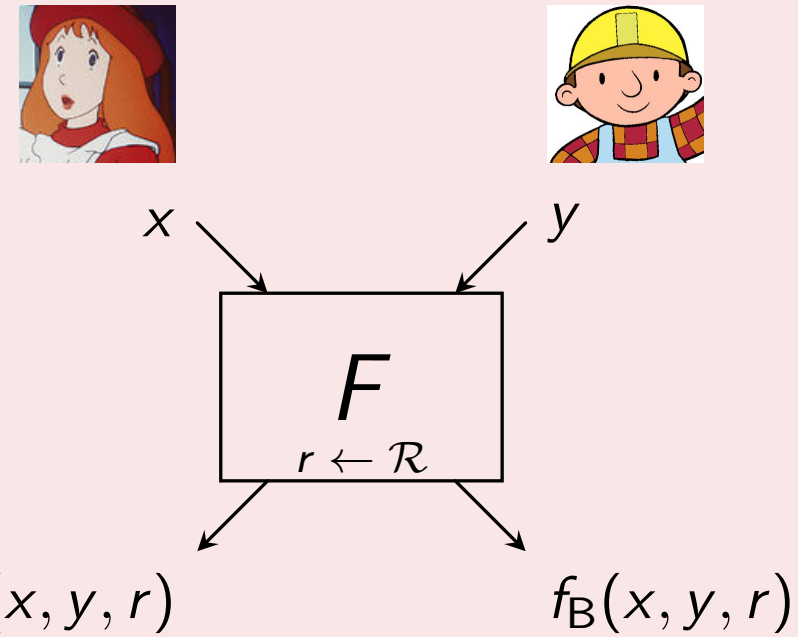
Oblivious Transfer



complete (= all-powerful)

[Kilian-88]
[Ishai-Prabhakaran-Sahai-08]

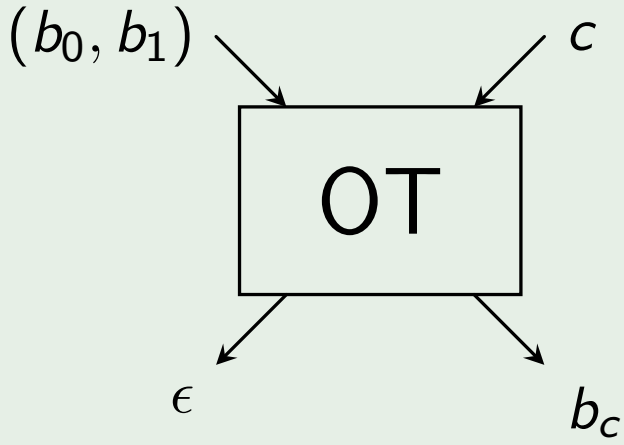
General crypto-gate $F = (f_A, f_B)$



Which ones are complete?

Simple primitives can be very powerful

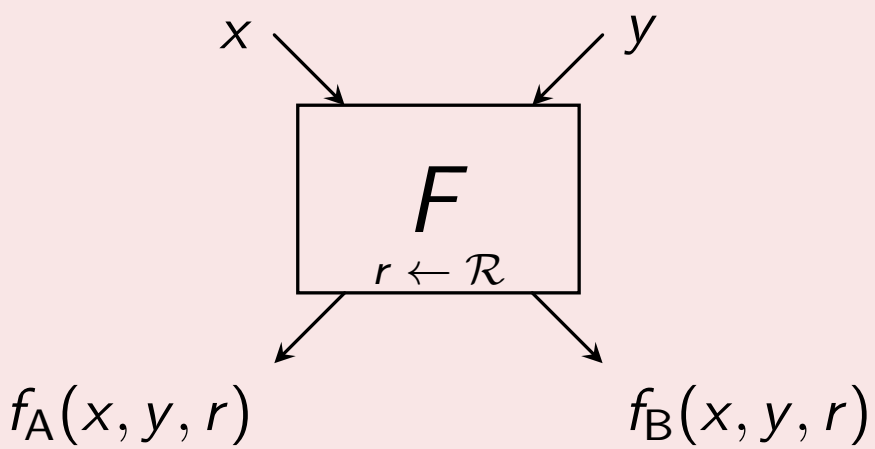
Oblivious Transfer

complete (= all-powerful)

[Kilian-88]
[Ishai-Prabhakaran-Sahai-08]

General crypto-gate $F = (f_A, f_B)$

Which ones are complete?

Special cases

symmetric: $f_A = f_B$

asymmetric: $f_A = \epsilon$

Known completeness criteria

		semi-honest	malicious
deterministic			
randomized			

Known completeness criteria

		semi-honest	malicious
deterministic	symmetric	**[Kilian-91]**	**[Kilian-91]**
randomized			

Known completeness criteria

		semi-honest	malicious
deterministic	symmetric	[Kilian-91]	[Kilian-91]
	asymmetric	**[Beimel-Malkin-Micali-99]**	
randomized			

Known completeness criteria

		semi-honest	malicious
deterministic	symmetric	[Kilian-91]	[Kilian-91]
	asymmetric	[Beimel-Malkin-Micali-99]	**[Kilian-00]**
randomized			

Known completeness criteria

		semi-honest	malicious
deterministic	symmetric	[Kilian-91]	[Kilian-91]
	asymmetric	[Beimel-Malkin-Micali-99]	[Kilian-00]
randomized	symmetric	**[Kilian-00]**	
	asymmetric	**[Kilian-00]**	

Known completeness criteria

		semi-honest	malicious
deterministic	symmetric	[Kilian-91]	[Kilian-91]
	asymmetric	[Beimel-Malkin-Micali-99]	[Kilian-00]
randomized	symmetric	[Kilian-00]	open
	asymmetric	[Kilian-00]	open

Known completeness criteria

		semi-honest	malicious
deterministic	symmetric	[Kilian-91]	[Kilian-91]
	asymmetric	[Beimel-Malkin-Micali-99]	[Kilian-00]
randomized	symmetric	[Kilian-00]	open
	asymmetric	[Kilian-00]	open*

* except for noisy channels [Crépeau-Kilian-88, Crépeau-Morozov-Wolf-04]

Known completeness criteria

		semi-honest	malicious
deterministic	symmetric	[Kilian-91]	[Kilian-91]
	asymmetric	[Beimel-Malkin-Micali-99]	[Kilian-00]
	general	**[K-MüllerQuade-11]**	**[K-MüllerQuade-11]**
randomized	symmetric	[Kilian-00]	open
	asymmetric	[Kilian-00]	open*

* except for noisy channels [Crépeau-Kilian-88, Crépeau-Morozov-Wolf-04]

Known completeness criteria

		semi-honest	malicious
deterministic	symmetric	[Kilian-91]	[Kilian-91]
	asymmetric	[Beimel-Malkin-Micali-99]	[Kilian-00]
	general	[K-MüllerQuade-11]	[K-MüllerQuade-11]
randomized	symmetric	[Kilian-00]	open
	asymmetric	[Kilian-00]	open*
	general	**[Maji-Prabhakaran-Rosulek-12]**	

* except for noisy channels [Crépeau-Kilian-88, Crépeau-Morozov-Wolf-04]

Known completeness criteria

		semi-honest	malicious
deterministic	symmetric	[Kilian-91]	[Kilian-91]
	asymmetric	[Beimel-Malkin-Micali-99]	[Kilian-00]
	general	[K-MüllerQuade-11]	[K-MüllerQuade-11]
randomized	symmetric	[Kilian-00]	open
	asymmetric	[Kilian-00]	open*
	general	[Maji-Prabhakaran-Rosulek-12]	open

* except for noisy channels [Crépeau-Kilian-88, Crépeau-Morozov-Wolf-04]

Known completeness criteria

		semi-honest	malicious
deterministic	symmetric	[Kilian-91]	[Kilian-91]
	asymmetric	[Beimel-Malkin-Micali-99]	[Kilian-00]
	general	[K-MüllerQuade-11]	[K-MüllerQuade-11]
randomized	symmetric	[Kilian-00]	**this work**
	asymmetric	[Kilian-00]	
	general	[Maji-Prabhakaran-Rosulek-12]	

* except for noisy channels [Crépeau-Kilian-88, Crépeau-Morozov-Wolf-04]

Our contribution

Main results

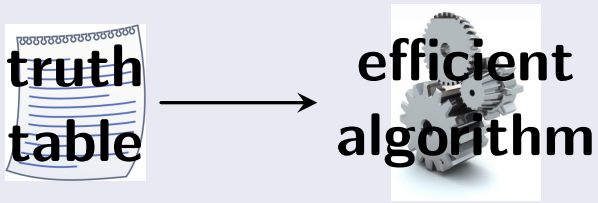
Our contribution

Main results

1. 

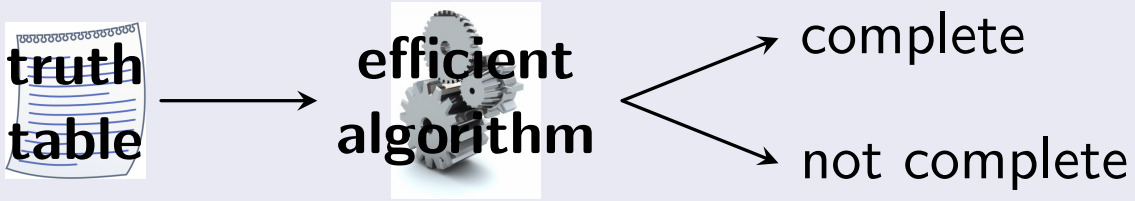
Our contribution

Main results

1. 

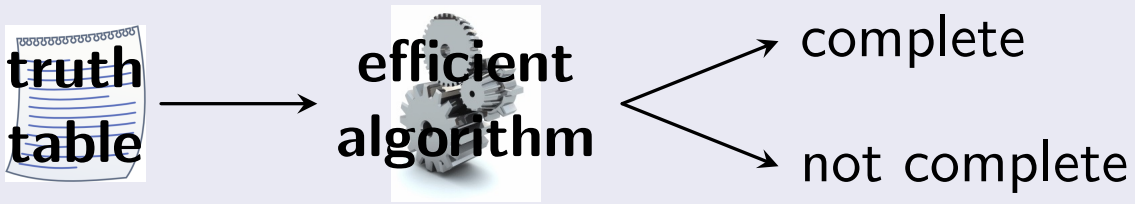
Our contribution

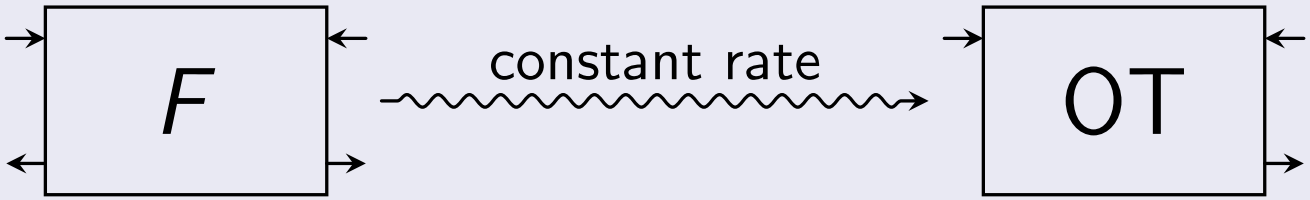
Main results

1. 

Our contribution

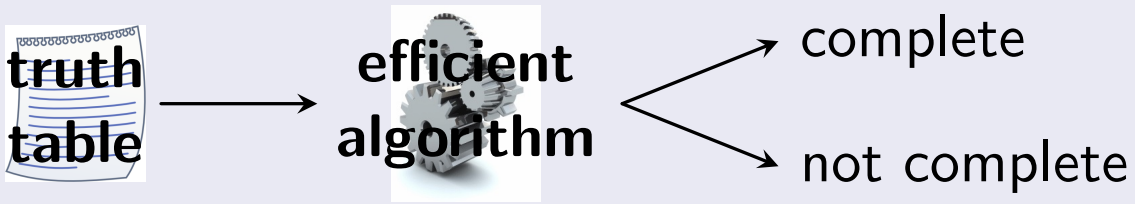
Main results

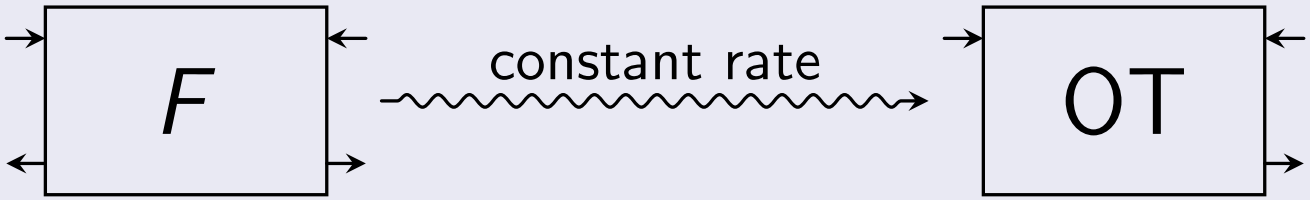
1. 

2. 

Our contribution

Main results

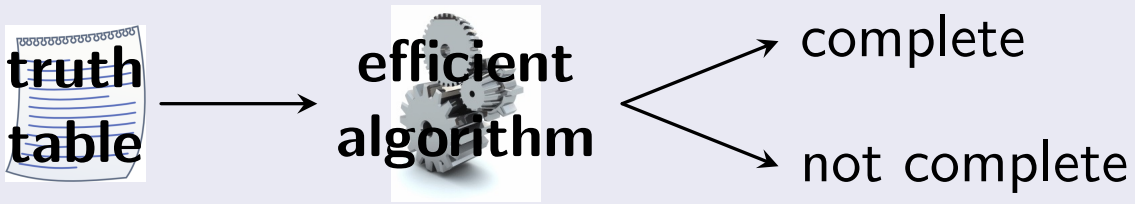
1. 

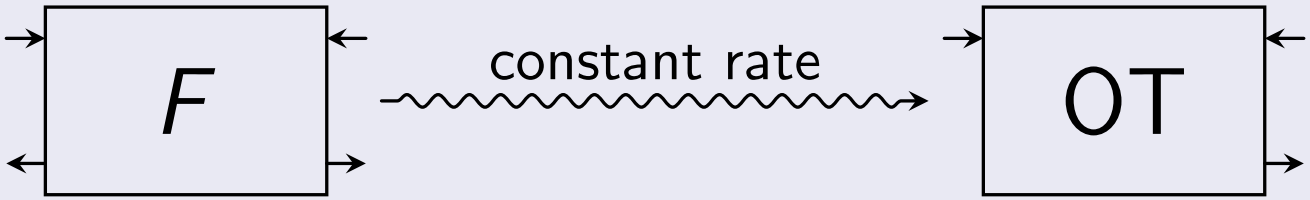
2. 

Implications

Our contribution

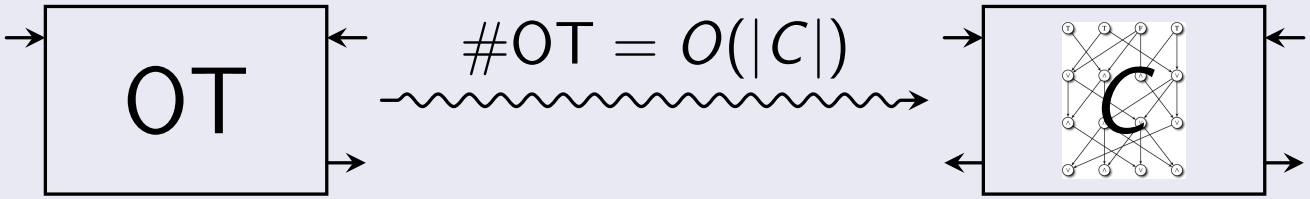
Main results

1. 

2. 

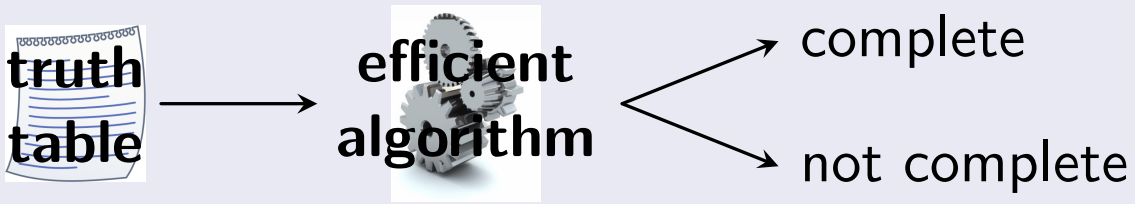
Implications

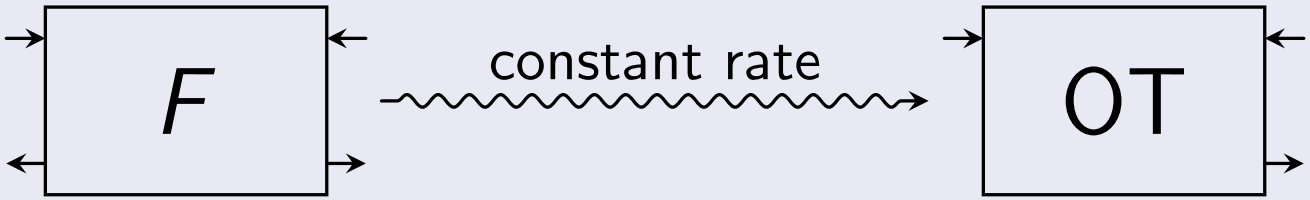
- [Ishai-Prabhakaran-Sahai-08]:



Our contribution

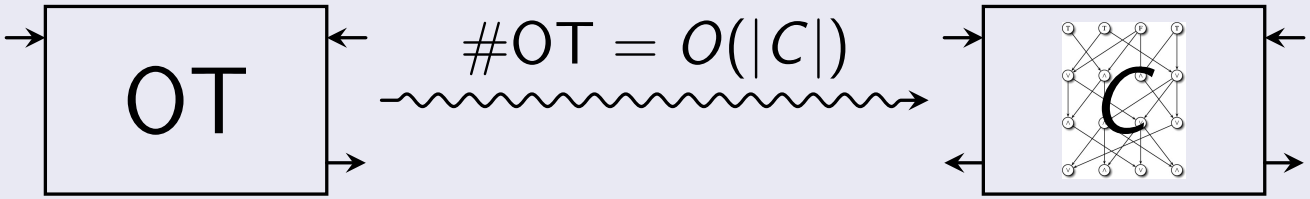
Main results

1. 

2. 

Implications

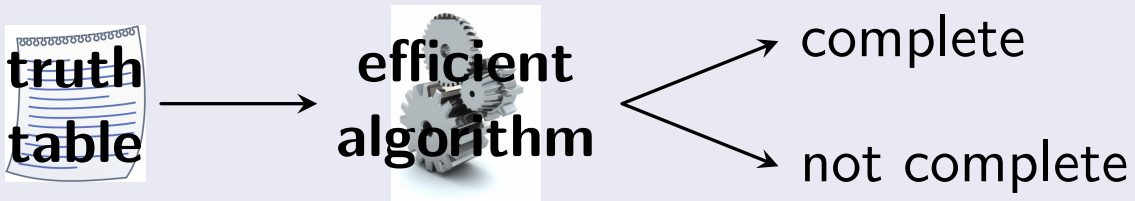
- [Ishai-Prabhakaran-Sahai-08]:

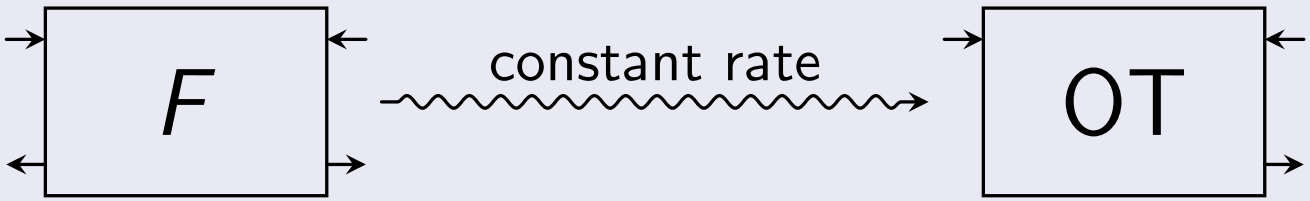


- constant-rate reduction between complete crypto-gates

Our contribution

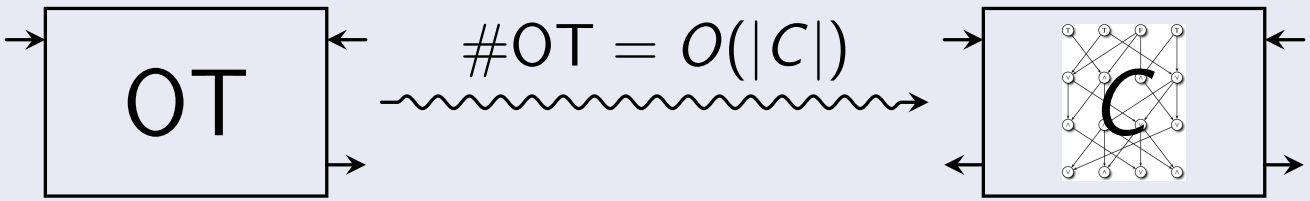
Main results

1. 

2. 

Implications

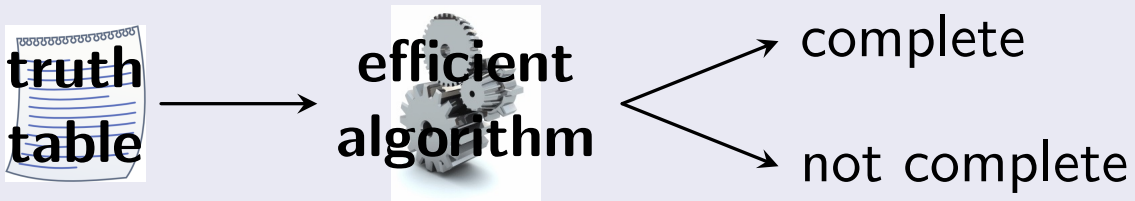
- [Ishai-Prabhakaran-Sahai-08]:

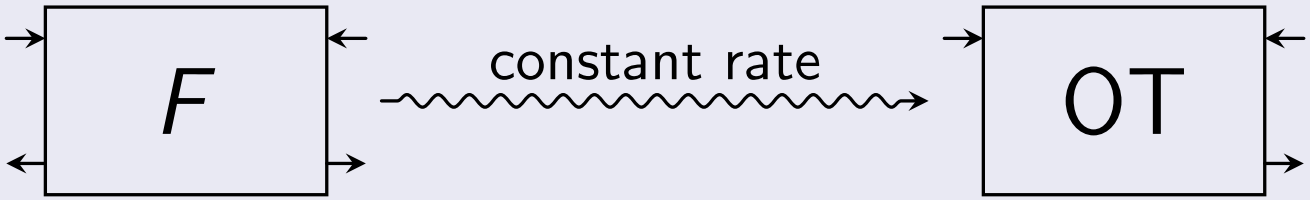


- constant-rate reduction between complete crypto-gates
- robust notion of "crypto-complexity" (independent of underlying gate)

Our contribution

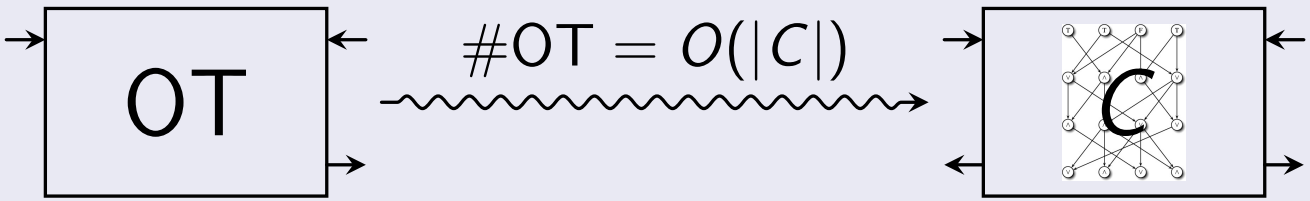
Main results

1. 

2. 

Implications

- [Ishai-Prabhakaran-Sahai-08]:



- constant-rate reduction between complete crypto-gates
- robust notion of "crypto-complexity" (independent of underlying gate)
- **new approach for lower bounds?**

Starting point: semi-honest completeness

Starting point: semi-honest completeness

Representation of crypto-gates

weighted bipartite graph

- left part: views (x, a) of 
- right part: views (y, b) of 
- edges: $\Pr[a, b \mid x, y]$

Starting point: semi-honest completeness

Representation of crypto-gates

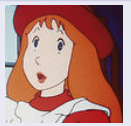
weighted bipartite graph
- left part: views (x, a) of 
- right part: views (y, b) of 
- edges: $\Pr[a, b \mid x, y]$

AND:

Starting point: semi-honest completeness

Representation of crypto-gates

weighted bipartite graph

- left part: views (x, a) of 
- right part: views (y, b) of 
- edges: $\Pr[a, b \mid x, y]$

AND:

Starting point: semi-honest completeness

Representation of crypto-gates

weighted bipartite graph {
- left part: views (x, a) of 
- right part: views (y, b) of 
- edges: $\Pr[a, b \mid x, y]$

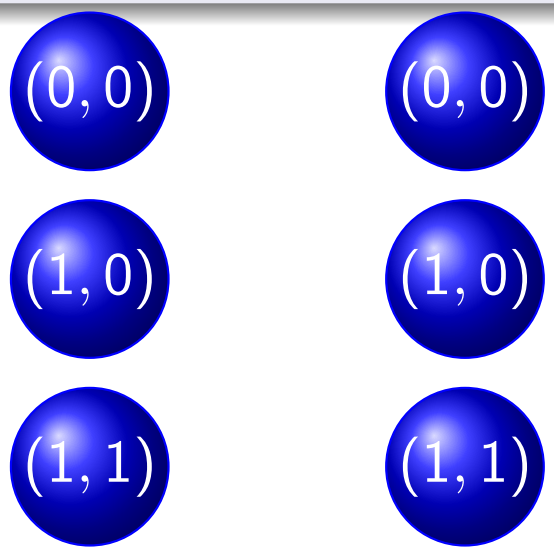
AND:

Starting point: semi-honest completeness

Representation of crypto-gates

weighted bipartite graph
- left part: views (x, a) of 
- right part: views (y, b) of 
- edges: $\Pr[a, b \mid x, y]$

AND:



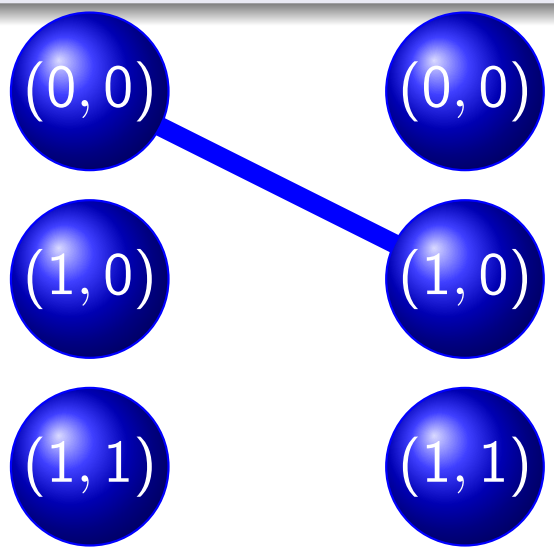
Starting point: semi-honest completeness

Representation of crypto-gates

weighted bipartite graph

- left part: views (x, a) of 
- right part: views (y, b) of 
- edges: $\Pr[a, b \mid x, y]$

AND:

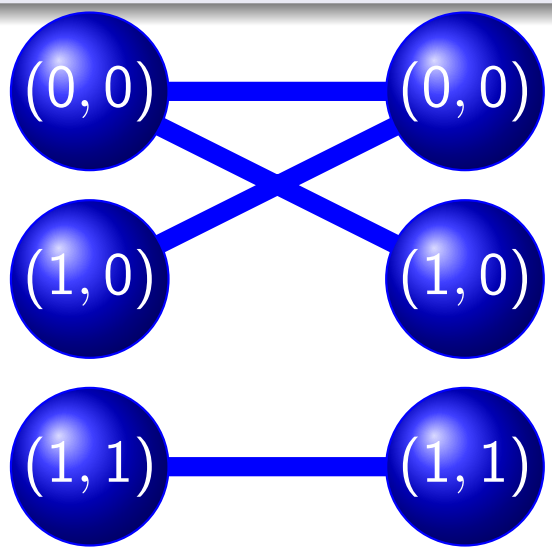


Starting point: semi-honest completeness

Representation of crypto-gates

weighted bipartite graph
- left part: views (x, a) of 
- right part: views (y, b) of 
- edges: $\Pr[a, b \mid x, y]$

AND:

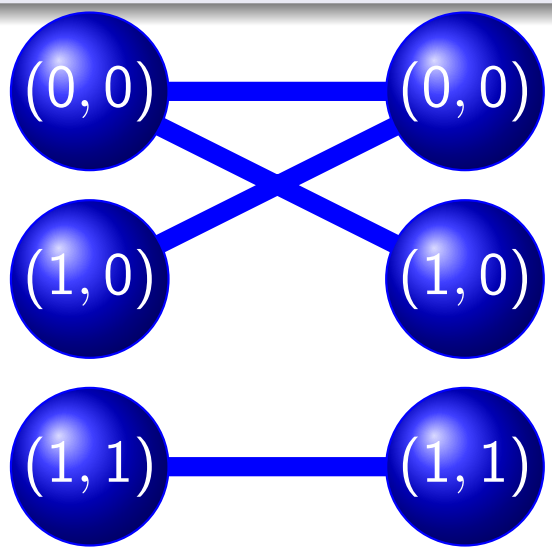


Starting point: semi-honest completeness

Representation of crypto-gates

weighted bipartite graph {
- left part: views (x, a) of 
- right part: views (y, b) of 
- edges: $\Pr[a, b \mid x, y]$

AND:



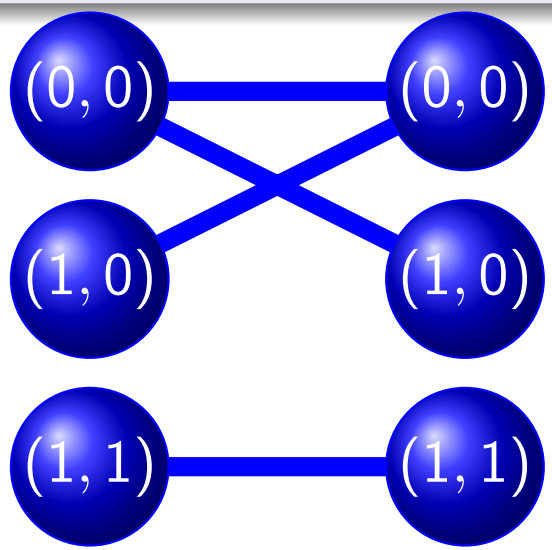
BSC:

Starting point: semi-honest completeness

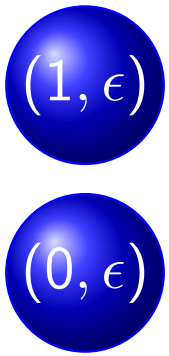
Representation of crypto-gates

weighted bipartite graph {
- left part: views (x, a) of 
- right part: views (y, b) of 
- edges: $\Pr[a, b \mid x, y]$

AND:



BSC:

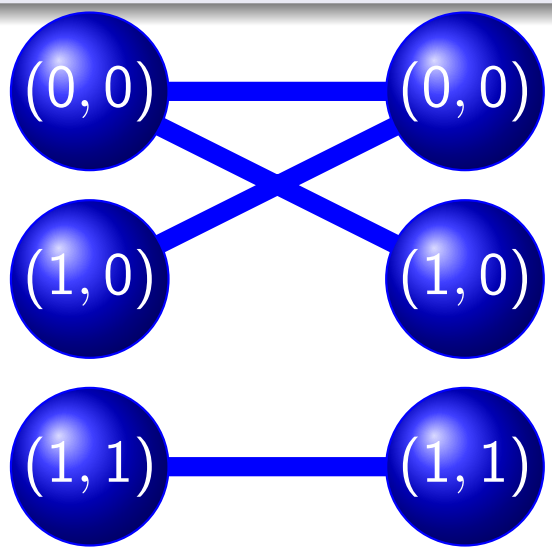


Starting point: semi-honest completeness

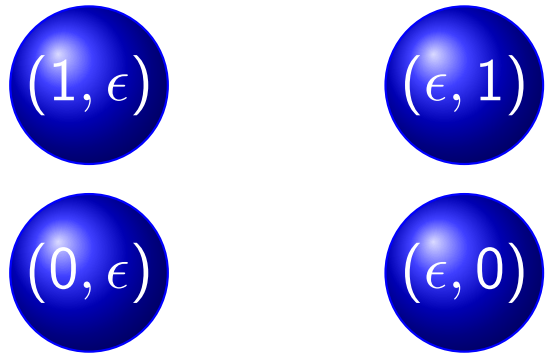
Representation of crypto-gates

weighted bipartite graph
- left part: views (x, a) of 
- right part: views (y, b) of 
- edges: $\Pr[a, b \mid x, y]$

AND:



BSC:

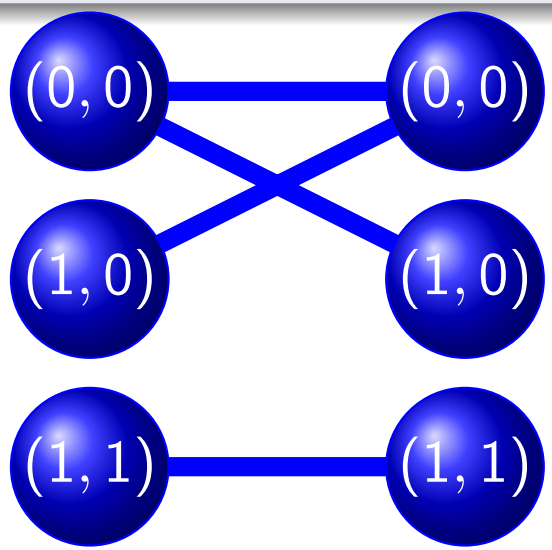


Starting point: semi-honest completeness

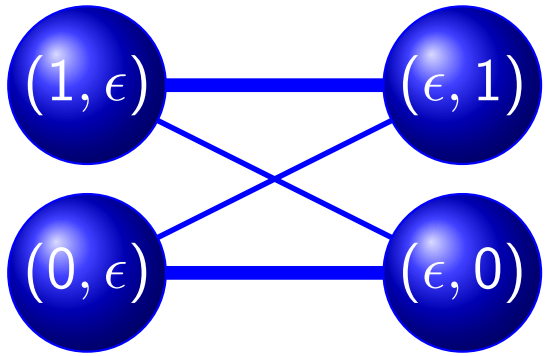
Representation of crypto-gates

weighted bipartite graph {
- left part: views (x, a) of 
- right part: views (y, b) of 
- edges: $\Pr[a, b \mid x, y]$

AND:



BSC:

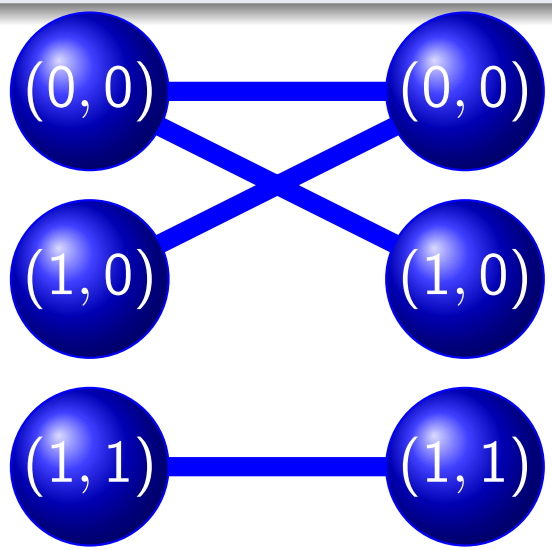


Starting point: semi-honest completeness

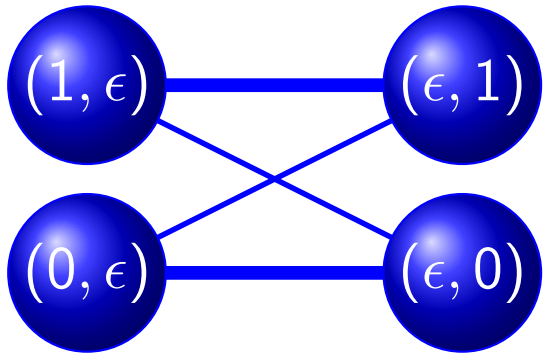
Representation of crypto-gates

weighted bipartite graph {
- left part: views (x, a) of 
- right part: views (y, b) of 
- edges: $\Pr[a, b \mid x, y]$

AND:



BSC:



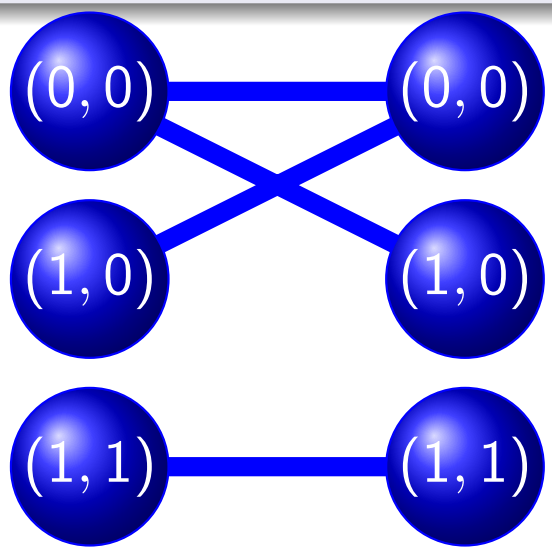
Semi-honest completeness [Maji-Prabhakaran-Rosulek-12]

Starting point: semi-honest completeness

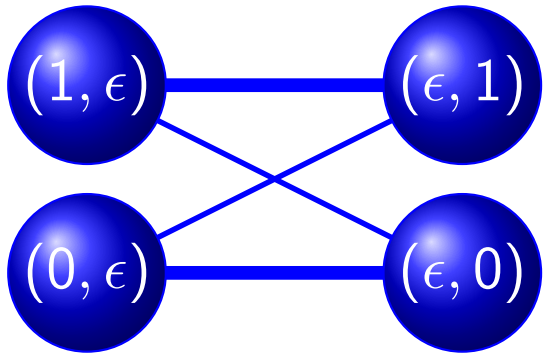
Representation of crypto-gates

weighted bipartite graph
- left part: views (x, a) of 
- right part: views (y, b) of 
- edges: $\Pr[a, b \mid x, y]$

AND:



BSC:



Semi-honest completeness [Maji-Prabhakaran-Rosulek-12]

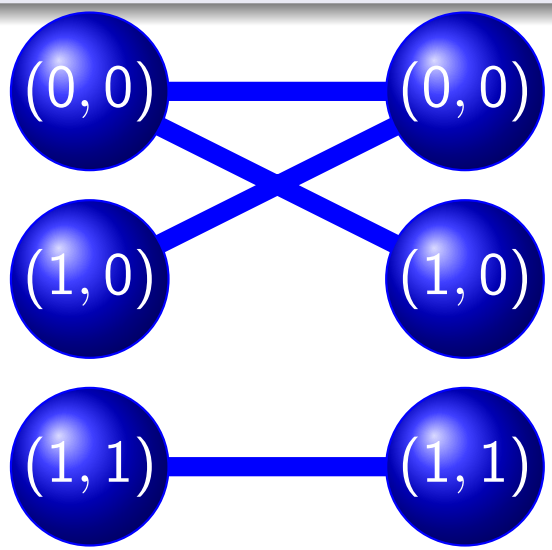
complete $\Leftrightarrow$ graph has connected component which is no product graph

Starting point: semi-honest completeness

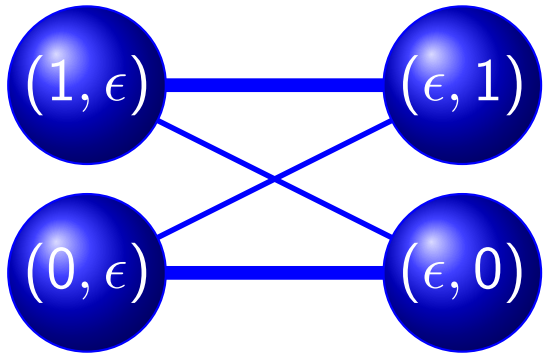
Representation of crypto-gates

weighted bipartite graph
- left part: views (x, a) of 
- right part: views (y, b) of 
- edges: $\Pr[a, b \mid x, y]$

AND:



BSC:



Semi-honest completeness [Maji-Prabhakaran-Rosulek-12]

complete $\Leftrightarrow$ graph has connected component which is no product graph
$\Leftrightarrow$ adjacency matrix has full-rank non-diagonal 2×2-submatrix

Malicious completeness

Malicious completeness

Redundancy

Malicious completeness

Redundancy

maliciously use only part of the crypto-gate, yet emulate honest behavior

Malicious completeness

Redundancy

maliciously use only part of the crypto-gate, yet emulate honest behavior

	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	1/4	1/4		1
(0,1)	1/4	1/4		
(1,0)			1/4	1/4
(1,1)	1		1/4	1/4

$$(a,b) = \begin{cases} \text{ind. rnd.} & \text{if } x = y \\ (x,y) & \text{if } x \neq y \end{cases}$$

Malicious completeness

Redundancy

maliciously use only part of the crypto-gate, yet emulate honest behavior

	(0,0)	(0,1)	(1,0)	(1,1)
(**0**,0)	1/4	1/4		1
(**0**,1)	1/4	1/4		
(1,0)			1/4	1/4
(1,1)	1		1/4	1/4

$$(a,b) = \begin{cases} \text{ind. rnd.} & \text{if } x = y \\ (x,y) & \text{if } x \neq y \end{cases}$$

Malicious completeness

Redundancy

maliciously use only part of the crypto-gate, yet emulate honest behavior

	$(\mathbf{0},0)$	$(\mathbf{0},1)$	$(1,0)$	$(1,1)$
$(\mathbf{0},0)$	$1/4$	$1/4$		1
$(\mathbf{0},1)$	$1/4$	$1/4$		
$(1,0)$			$1/4$	$1/4$
$(1,1)$	1		$1/4$	$1/4$

$$(a,b) = \begin{cases} \text{ind. rnd.} & \text{if } x = y \\ (x,y) & \text{if } x \neq y \end{cases}$$

Malicious completeness

Redundancy

maliciously use only part of the crypto-gate, yet emulate honest behavior

	$(\mathbf{0},0)$	$(\mathbf{0},1)$	$(1,0)$	$(1,1)$
$(\mathbf{0},0)$	$\mathbf{1/4}$	$\mathbf{1/4}$		1
$(\mathbf{0},1)$	$\mathbf{1/4}$	$\mathbf{1/4}$		
$(1,0)$			$1/4$	$1/4$
$(1,1)$	1		$1/4$	$1/4$

$$(a,b) = \begin{cases} \text{ind. rnd.} & \text{if } x = y \\ (x,y) & \text{if } x \neq y \end{cases}$$

Malicious completeness

Redundancy

maliciously use only part of the crypto-gate, yet emulate honest behavior

	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	1/4	1/4		1
(0,1)	1/4	1/4		
(**1**,0)			1/4	1/4
(**1**,1)	1		1/4	1/4

$$(a, b) = \begin{cases} \text{ind. rnd.} & \text{if } x = y \\ (x, y) & \text{if } x \neq y \end{cases}$$

Malicious completeness

Redundancy

maliciously use only part of the crypto-gate, yet emulate honest behavior

	$(\mathbf{0},0)$	$(\mathbf{0},1)$	$(1,0)$	$(1,1)$
$(0,0)$	$1/4$	$1/4$		1
$(0,1)$	$1/4$	$1/4$		
$(\mathbf{1},0)$			$1/4$	$1/4$
$(\mathbf{1},1)$	1		$1/4$	$1/4$

$$(a,b) = \begin{cases} \text{ind. rnd.} & \text{if } x = y \\ (x,y) & \text{if } x \neq y \end{cases}$$

Malicious completeness

Redundancy

maliciously use only part of the crypto-gate, yet emulate honest behavior

	$(\mathbf{0},0)$	$(\mathbf{0},1)$	$(1,0)$	$(1,1)$
$(0,0)$	$1/4$	$1/4$		1
$(0,1)$	$1/4$	$1/4$		
$(\mathbf{1},0)$			$1/4$	$1/4$
$(\mathbf{1},1)$	$\mathbf{1}$		$1/4$	$1/4$

$$(a,b) = \begin{cases} \text{ind. rnd.} & \text{if } x = y \\ (x,y) & \text{if } x \neq y \end{cases}$$

Malicious completeness

Redundancy

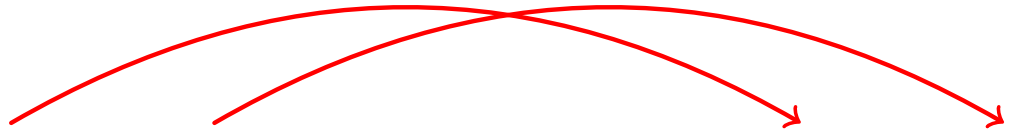
maliciously use only part of the crypto-gate, yet emulate honest behavior

	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)	(2,2)
(0,0)	1/4	1/4		1	1/8	1/8	1/2
(0,1)	1/4	1/4			1/8	1/8	
(1,0)			1/4	1/4		1/8	1/8
(1,1)	1		1/4	1/4	1/2	1/8	1/8

Malicious completeness

Redundancy

maliciously use only part of the crypto-gate, yet emulate honest behavior

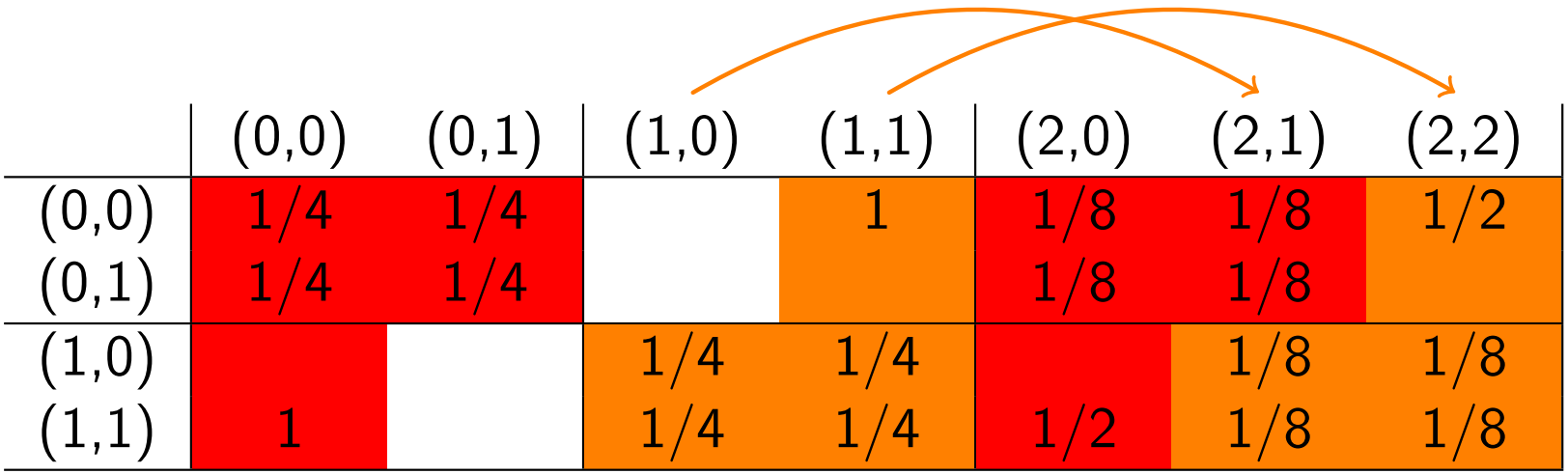


	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)	(2,2)
(0,0)	1/4	1/4		1	1/8	1/8	1/2
(0,1)	1/4	1/4			1/8	1/8	
(1,0)			1/4	1/4		1/8	1/8
(1,1)	1		1/4	1/4	1/2	1/8	1/8

Malicious completeness

Redundancy

maliciously use only part of the crypto-gate, yet emulate honest behavior



	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)	(2,2)
(0,0)	1/4	1/4		1	1/8	1/8	1/2
(0,1)	1/4	1/4			1/8	1/8	
(1,0)			1/4	1/4		1/8	1/8
(1,1)	1		1/4	1/4	1/2	1/8	1/8

Malicious completeness

Redundancy

maliciously use only part of the crypto-gate, yet emulate honest behavior

	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)	(2,2)
(0,0)	1/4	1/4		1	1/8	1/8	1/2
(0,1)	1/4	1/4			1/8	1/8	
(1,0)			1/4	1/4		1/8	1/8
(1,1)	1		1/4	1/4	1/2	1/8	1/8

Efficient characterization of malicious completeness

Malicious completeness

Redundancy

maliciously use only part of the crypto-gate, yet emulate honest behavior

	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)	(2,2)
(0,0)	1/4	1/4		1	1/8	1/8	1/2
(0,1)	1/4	1/4			1/8	1/8	
(1,0)			1/4	1/4		1/8	1/8
(1,1)	1		1/4	1/4	1/2	1/8	1/8

Efficient characterization of malicious completeness

1. detect redundancies (use linear programming)

Malicious completeness

Redundancy

maliciously use only part of the crypto-gate, yet emulate honest behavior

	(0,0)	(0,1)	(1,0)	(1,1)	
(0,0)	1/4	1/4		1	
(0,1)	1/4	1/4			
(1,0)			1/4	1/4	
(1,1)	1		1/4	1/4	

Efficient characterization of malicious completeness

1. detect redundancies (use linear programming)
2. keep removing redundancies, eventually obtain redundancy-free "core"

Malicious completeness

Redundancy

maliciously use only part of the crypto-gate, yet emulate honest behavior

	(0,0)	(0,1)	(1,0)	(1,1)	
(0,0)	1/4	1/4		1	
(0,1)	1/4	1/4			
(1,0)			1/4	1/4	
(1,1)	1		1/4	1/4	

Efficient characterization of malicious completeness

1. detect redundancies (use linear programming)
2. keep removing redundancies, eventually obtain redundancy-free "core"
3. malicious complete $\Leftrightarrow$ core is semi-honest complete

Malicious completeness

Redundancy

maliciously use only part of the crypto-gate, yet emulate honest behavior

	(0,0)	(0,1)	(1,0)	(1,1)	
(0,0)	1/4	1/4		1	
(0,1)	1/4	1/4			
(1,0)			1/4	1/4	
(1,1)	1		1/4	1/4	

Efficient characterization of malicious completeness

1. detect redundancies (use linear programming)
2. keep removing redundancies, eventually obtain redundancy-free "core"
3. malicious complete $\Leftrightarrow$ core is semi-honest complete

Complete construction

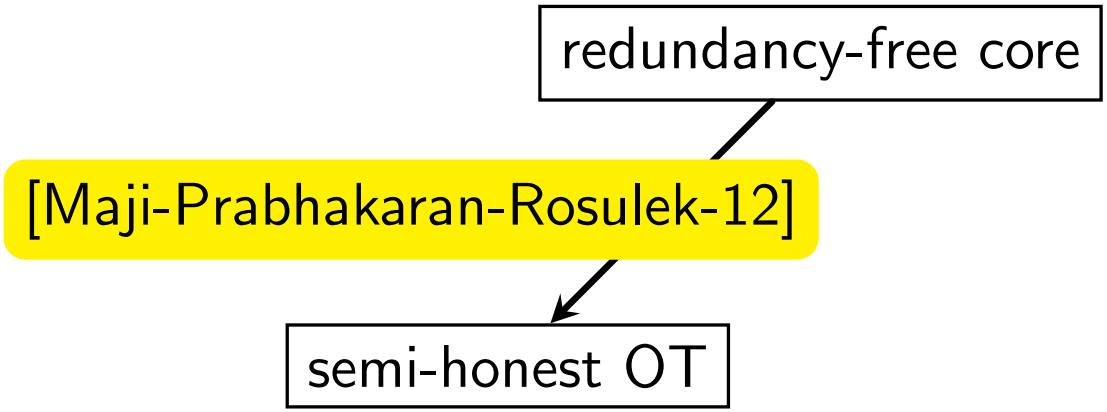
Complete construction

given crypto-gate

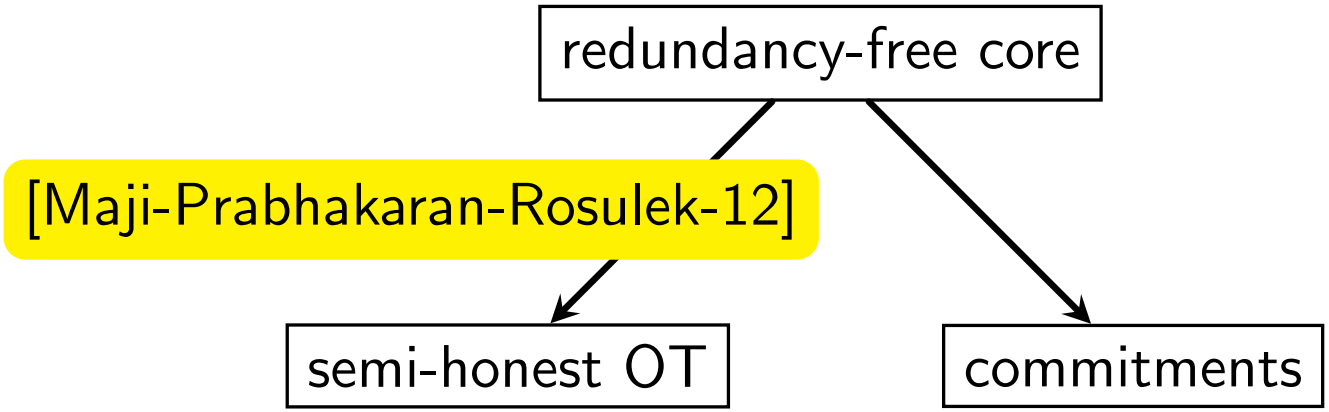
Complete construction

redundancy-free core

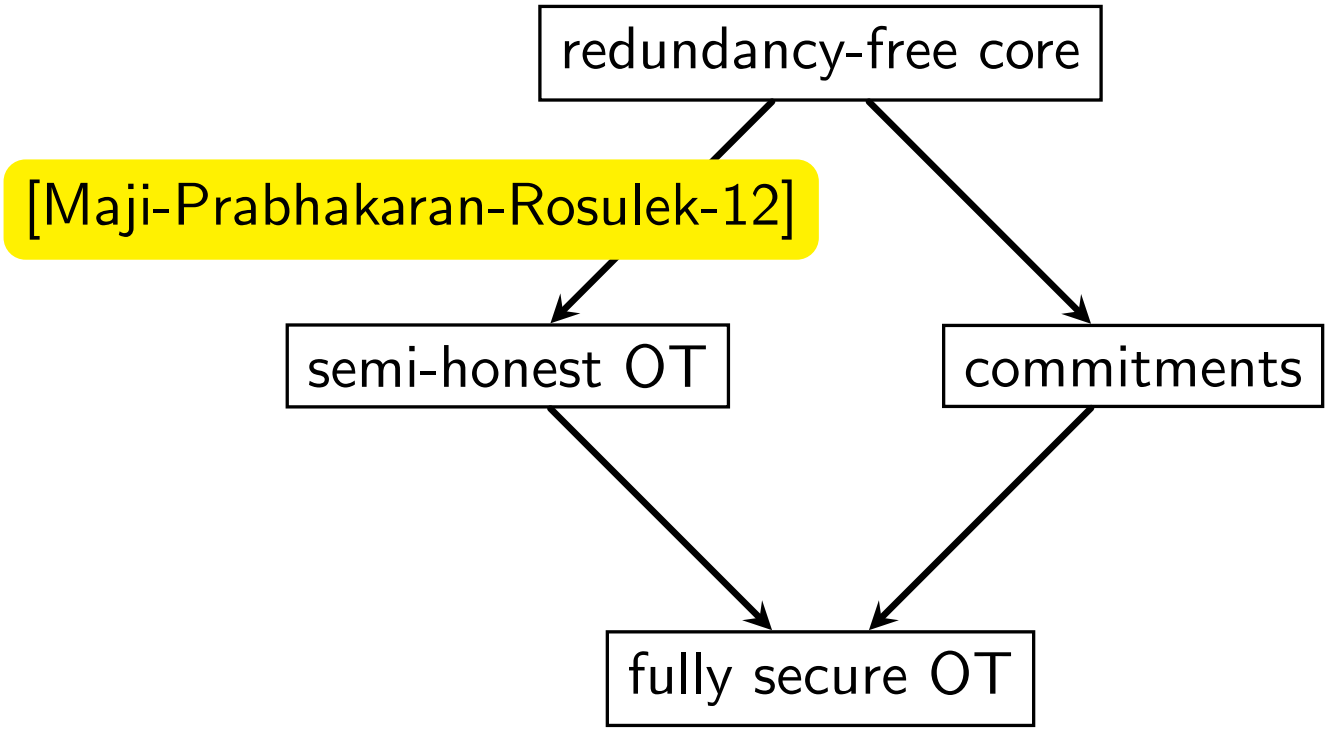
Complete construction



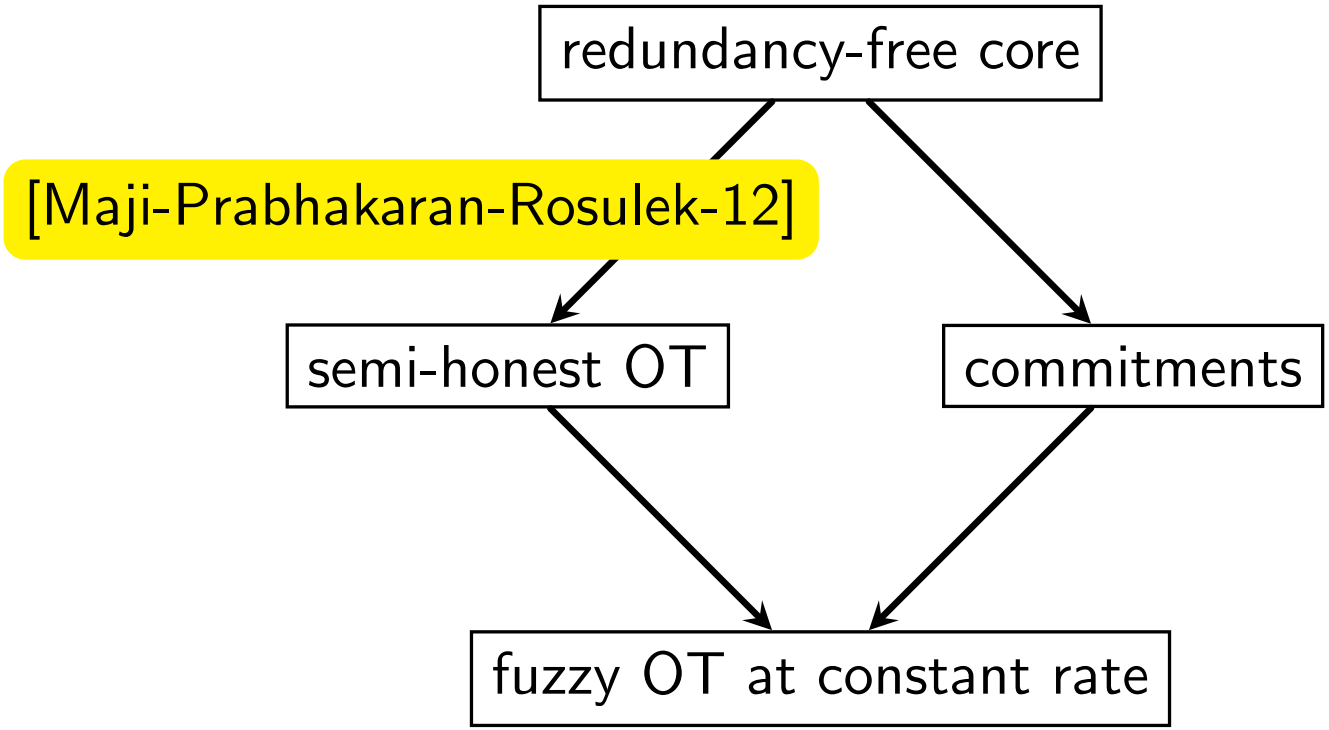
Complete construction



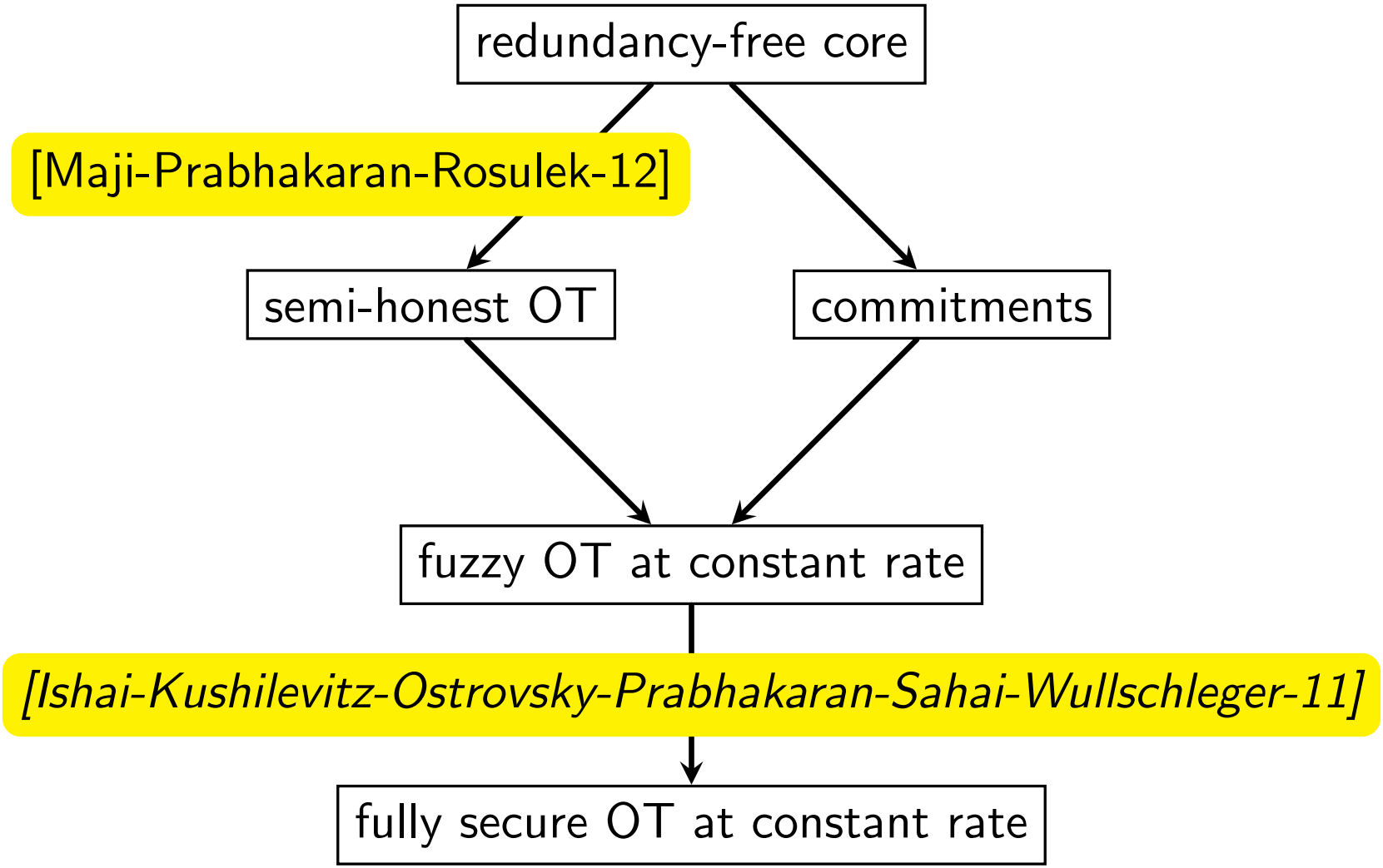
Complete construction



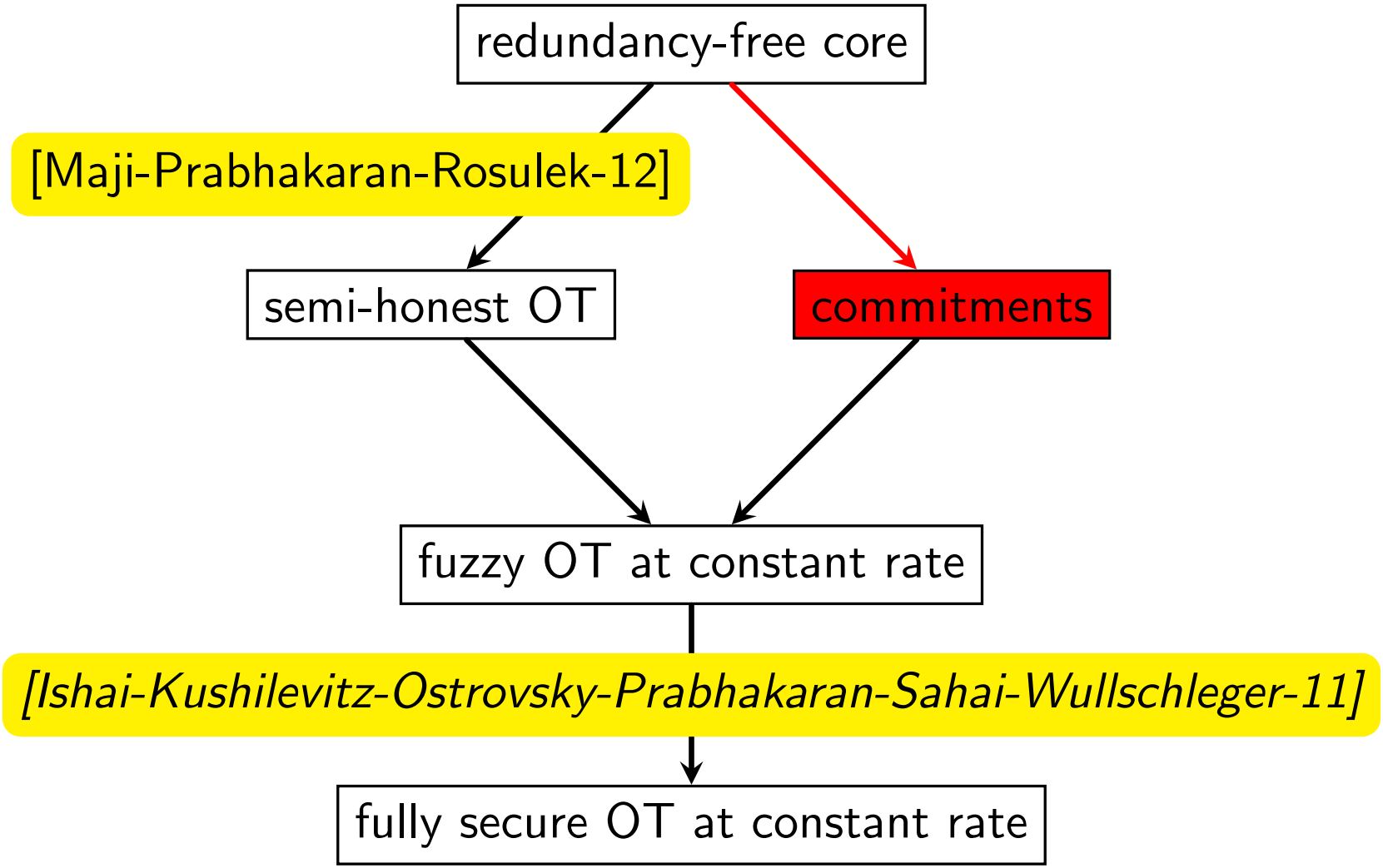
Complete construction



Complete construction



Complete construction



Commitment construction

Commitment construction

use crypto-gate as "channel"

 "sends" (x, a)

 "receives" (y, b)

Commitment construction

use crypto-gate as "channel"

 "sends" (x, a)

 "receives" (y, b)

hiding: push information through channel at larger rate than capacity

Commitment construction

use crypto-gate as "channel"

 "sends" (x, a)

 "receives" (y, b)

hiding: push information through channel at larger rate than capacity

binding: use good enough relative distance code

Commitment construction

use crypto-gate as "channel"

 "sends" (x, a)

 "receives" (y, b)

hiding: push information through channel at larger rate than capacity

binding: use good enough relative distance code

Caveats

Commitment construction

use crypto-gate as "channel"

 "sends" (x, a)  "receives" (y, b)

hiding: push information through channel at larger rate than capacity

binding: use good enough relative distance code

Caveats

- receiver influences channel

Commitment construction

use crypto-gate as "channel"

 "sends" (x, a)  "receives" (y, b)

hiding: push information through channel at larger rate than capacity

binding: use good enough relative distance code

Caveats

- receiver influences channel
- redundancy-free $\not\Rightarrow$ unfakeable input *distributions*

Technical contributions

Technical contributions

- linear algebraic definition of redundancy

Technical contributions

- linear algebraic definition of redundancy
  $\rightsquigarrow$ efficient completeness test by linear programming

Technical contributions

- linear algebraic definition of redundancy
  $\rightsquigarrow$ efficient completeness test by linear programming
- statistical tests: information-theoretic "proofs" for F-hybrid

Technical contributions

- linear algebraic definition of redundancy
  $\rightsquigarrow$ efficient completeness test by linear programming
- statistical tests: information-theoretic "proofs" for F-hybrid
  $\rightsquigarrow$ passive-to-active compiler

Technical contributions

- linear algebraic definition of redundancy
  $\rightsquigarrow$ efficient completeness test by linear programming
- statistical tests: information-theoretic "proofs" for F-hybrid
  $\rightsquigarrow$ passive-to-active compiler
- adaptive version of converse of Channel Coding Theorem

Technical contributions

- linear algebraic definition of redundancy
  $\rightsquigarrow$ efficient completeness test by linear programming
- statistical tests: information-theoretic "proofs" for F-hybrid
  $\rightsquigarrow$ passive-to-active compiler
- adaptive version of converse of Channel Coding Theorem
  $\rightsquigarrow$ commitments

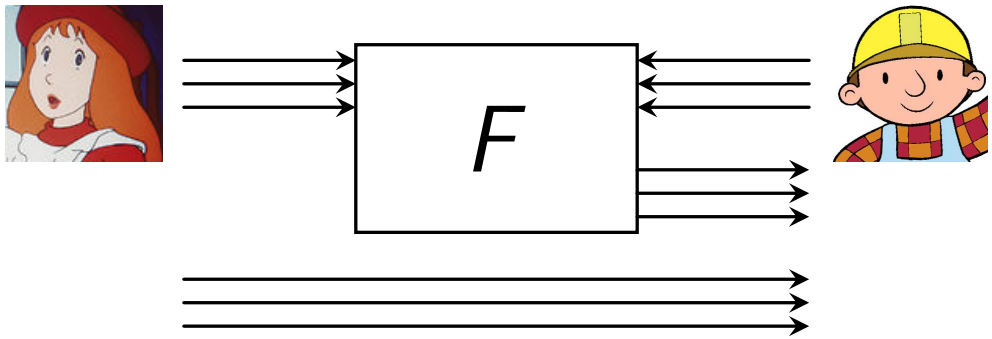
Open problems

Open problems

- non-interactive completeness

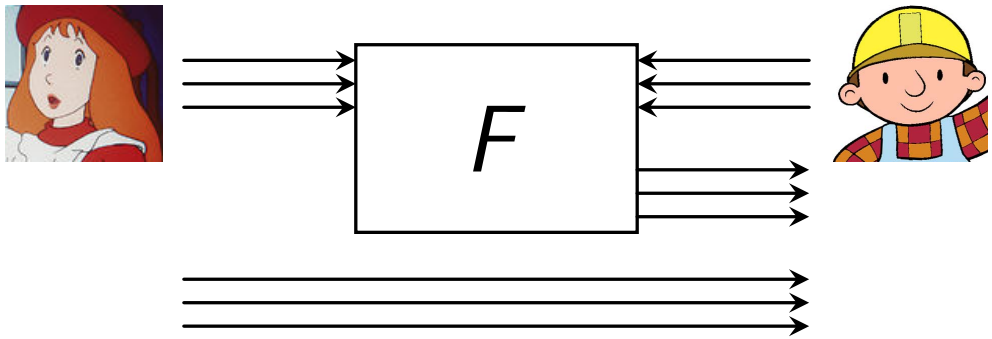
Open problems

- non-interactive completeness



Open problems

- non-interactive completeness $\sim$ Decomposable Randomized Encodings

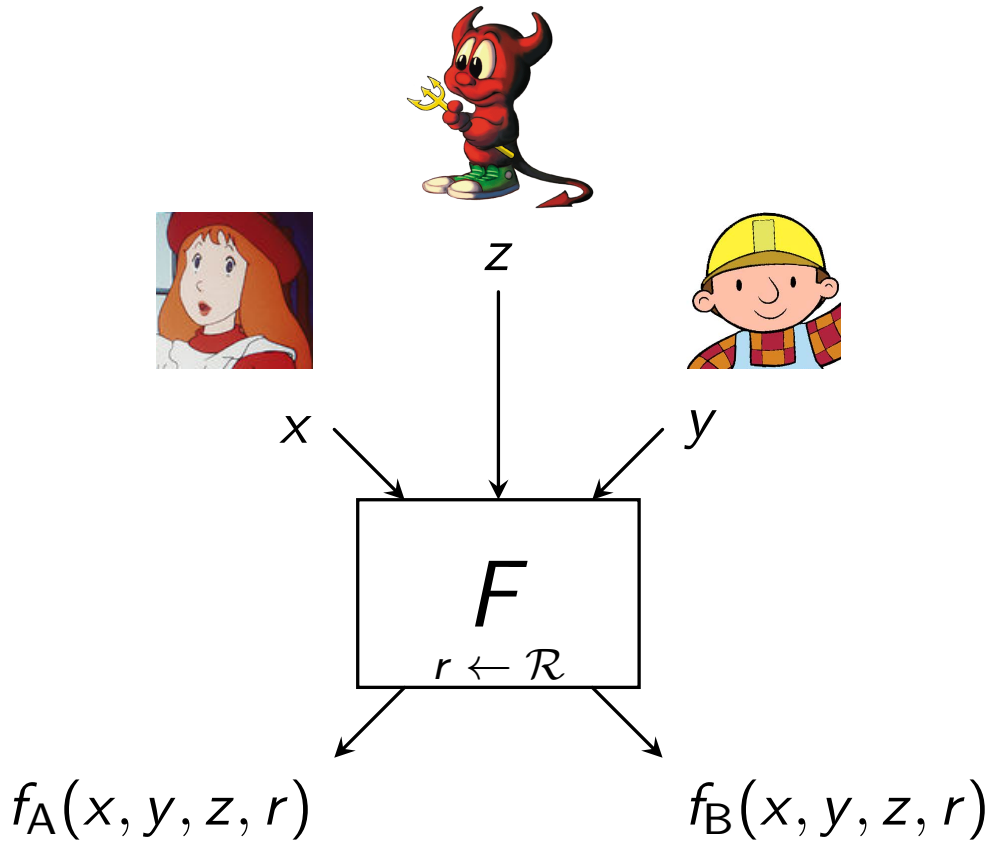


Open problems

- non-interactive completeness $\sim$ Decomposable Randomized Encodings
- leaky & unfair primitives

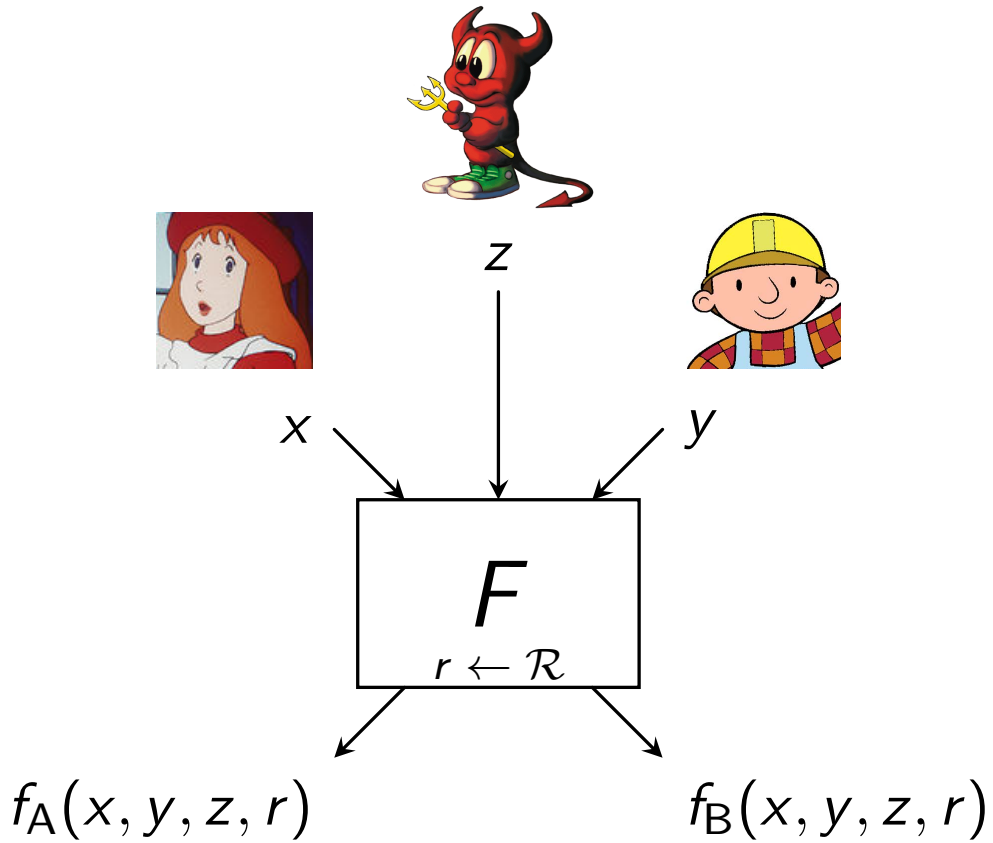
Open problems

- non-interactive completeness $\sim$ Decomposable Randomized Encodings
- leaky & unfair primitives



Open problems

- non-interactive completeness $\sim$ Decomposable Randomized Encodings
- leaky & unfair primitives $\sim$ Combiners and Extractors

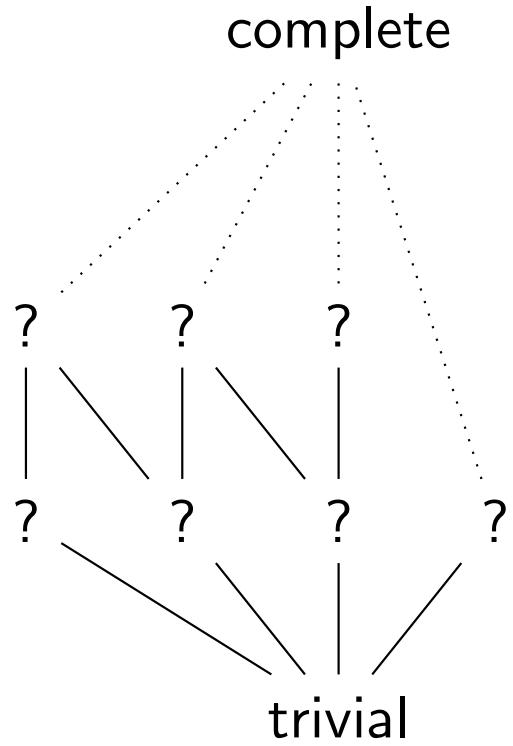


Open problems

- non-interactive completeness $\sim$ Decomposable Randomized Encodings
- leaky & unfair primitives $\sim$ Combiners and Extractors
- non-complete crypto-gates

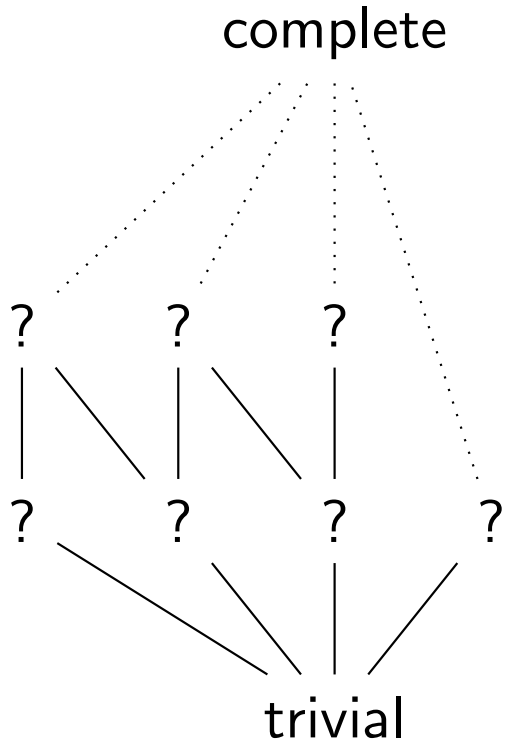
Open problems

- non-interactive completeness $\sim$ Decomposable Randomized Encodings
- leaky & unfair primitives $\sim$ Combiners and Extractors
- non-complete crypto-gates



Open problems

- non-interactive completeness $\sim$ Decomposable Randomized Encodings
- leaky & unfair primitives $\sim$ Combiners and Extractors
- non-complete crypto-gates $\sim$ Black-Box Separations

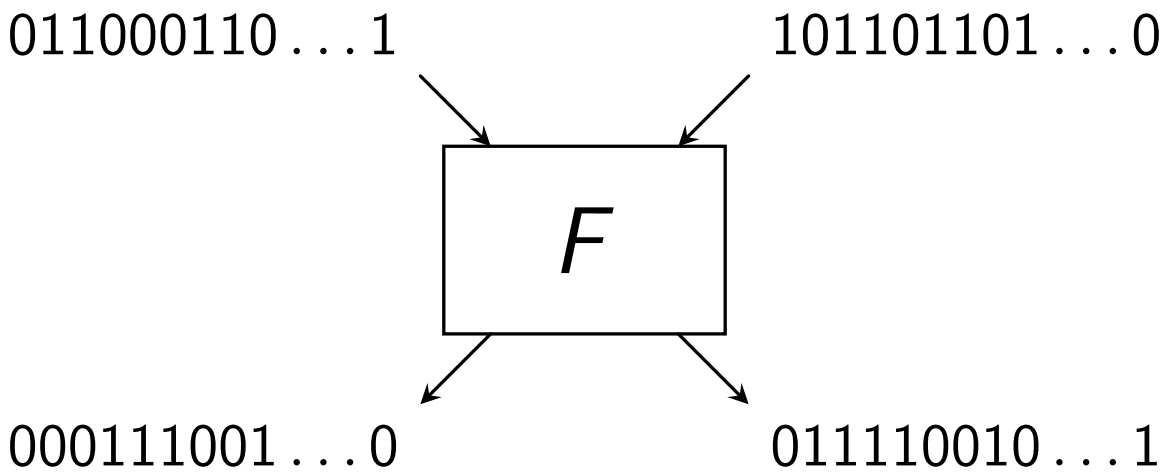


Open problems

- non-interactive completeness $\sim$ Decomposable Randomized Encodings
- leaky & unfair primitives $\sim$ Combiners and Extractors
- non-complete crypto-gates $\sim$ Black-Box Separations
- infinite number of possible inputs (and outputs)

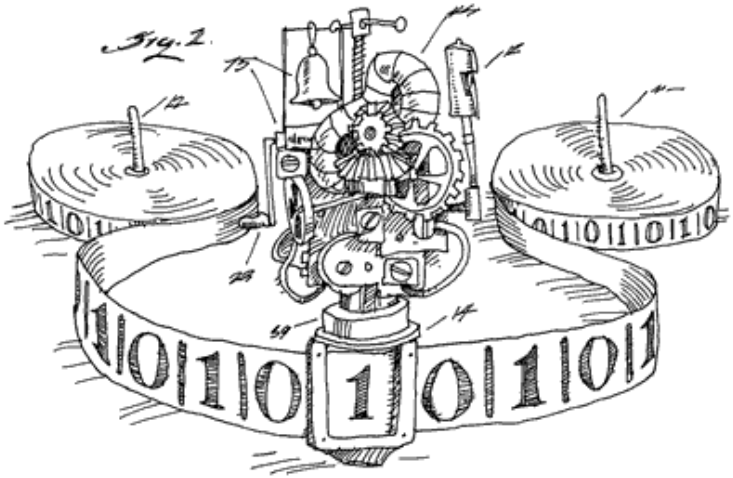
Open problems

- non-interactive completeness $\sim$ Decomposable Randomized Encodings
- leaky & unfair primitives $\sim$ Combiners and Extractors
- non-complete crypto-gates $\sim$ Black-Box Separations
- infinite number of possible inputs (and outputs)



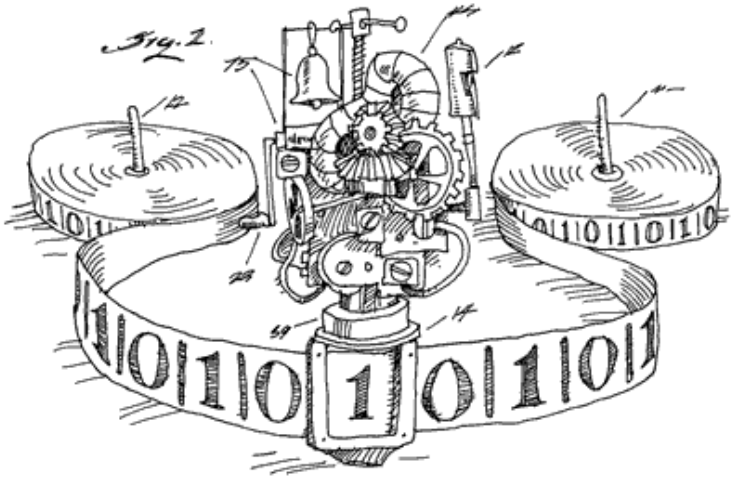
Open problems

- non-interactive completeness $\sim$ Decomposable Randomized Encodings
- leaky & unfair primitives $\sim$ Combiners and Extractors
- non-complete crypto-gates $\sim$ Black-Box Separations
- infinite number of possible inputs (and outputs)
- computationally bounded adversaries



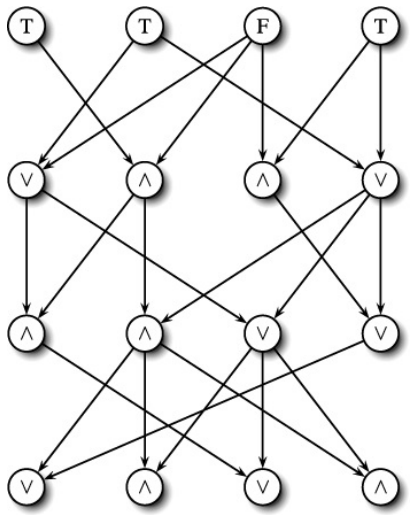
Open problems

- non-interactive completeness $\sim$ Decomposable Randomized Encodings
- leaky & unfair primitives $\sim$ Combiners and Extractors
- non-complete crypto-gates $\sim$ Black-Box Separations
- infinite number of possible inputs (and outputs)
- computationally bounded adversaries (non-black-box reductions)



Open problems

- non-interactive completeness $\sim$ Decomposable Randomized Encodings
- leaky & unfair primitives $\sim$ Combiners and Extractors
- non-complete crypto-gates $\sim$ Black-Box Separations
- infinite number of possible inputs (and outputs)
- computationally bounded adversaries (non-black-box reductions)
- lower (crypto-)complexity bounds



Thank you!

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 259426 - ERC - Cryptography and Complexity.

Work supported by NSF grants 07-47027 and 12-28856.

Research supported in part from a DARPA/ONR PROCEED award, NSF grants 1228984, 1136174, 1118096, and 1065276, a Xerox Faculty Research Award, a Google Faculty Research Award, an equipment grant from Intel, and an Okawa Foundation Research Grant.

References I

Paul Baecher, Christina Brzuska, and Arno Mittelbach.
Reset indifferentiability and its consequences.
In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology, Proceedings of ASIACRYPT 2013, Part I*, volume 8269 of *Lecture Notes in Computer Science*, pages 154–173. Springer, 2013.

Gilles Brassard, Claude Crépeau, and Miklos Santha.
Oblivious transfers and intersecting codes.
IEEE Transactions on Information Theory, 42(6):1769–1780, 1996.

Amos Beimel, Tal Malkin, and Silvio Micali.
The all-or-nothing nature of two-party secure computation.
In Michael J. Wiener, editor, *Advances in Cryptology, Proceedings of CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 80–97. Springer, 1999.

Claude Crépeau and Joe Kilian.
Achieving oblivious transfer using weakened security assumptions (extended abstract).
In *Proceedings of FOCS 1988*, pages 42–52. IEEE Computer Society, 1988.

Claude Crépeau, Kirill Morozov, and Stefan Wolf.
Efficient unconditional oblivious transfer from almost any noisy channel.
In Carlo Blundo and Stelvio Cimato, editors, *SCN 2004*, volume 3352 of *Lecture Notes in Computer Science*, pages 47–59. Springer, 2005.

References II

Jean-Sébastien Coron, Jacques Patarin, and Yannick Seurin.
The random oracle model and the ideal cipher model are equivalent.
In David Wagner, editor, *Advances in Cryptology, Proceedings of CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2008.

Ivan Damgård, Serge Fehr, Kirill Morozov, and Louis Salvail.
Unfair noisy channels and oblivious transfer.
In Moni Naor, editor, *Theory of Cryptography, Proceedings of TCC 2004*, volume 2951 of *Lecture Notes in Computer Science*, pages 355–373. Springer, 2004.

Ivan Damgård, Joe Kilian, and Louis Salvail.
On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions.
In *Advances in Cryptology, Proceedings of EUROCRYPT '99*, pages 56–73, 1999.

Yael Gertner, Sampath Kannan, Tal Malkin, Omer Reingold, and Mahesh Viswanathan.
The relationship between public key encryption and oblivious transfer.
In *Proceedings of FOCS 2000*, pages 325–335. IEEE Computer Society, 2000.

Yael Gertner, Tal Malkin, and Omer Reingold.
On the impossibility of basing trapdoor functions on trapdoor predicates.
In *Proceedings of FOCS 2001*, pages 126–135. IEEE Computer Society, 2001.

References III

Thomas Holenstein, Robin Künzler, and Stefano Tessaro.
The equivalence of the random oracle model and the ideal cipher model, revisited.
In Lance Fortnow and Salil P. Vadhan, editors, *Proceedings of STOC 2011*, pages 89–98. ACM, 2011.

Danny Harnik, Moni Naor, Omer Reingold, and Alon Rosen.
Completeness in two-party secure computation: a computational view.
In László Babai, editor, *Proceedings of STOC 2004*, pages 252–261. ACM, 2004.

Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, and Amit Sahai.
Efficient non-interactive secure computation.
In Kenneth G. Paterson, editor, *Advances in Cryptology, Proceedings of EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 406–425. Springer, 2011.

Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, Amit Sahai, and Jürg Wullschleger.
Constant-rate oblivious transfer from noisy channels.
In Phillip Rogaway, editor, *Advances in Cryptology, Proceedings of CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 667–684. Springer, 2011.

Yuval Ishai, Manoj Prabhakaran, and Amit Sahai.
Founding cryptography on oblivious transfer - efficiently.
In David Wagner, editor, *Advances in Cryptology, Proceedings of CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 572–591. Springer, 2008.

References IV


Russell Impagliazzo and Steven Rudich.
Limits on the provable consequences of one-way permutations.
In David S. Johnson, editor, *Proceedings of STOC 1989*, pages 44–61. ACM, 1989.


Joe Kilian.
Founding cryptography on oblivious transfer.
In *Proceedings of STOC 1988*, pages 20–31. ACM, 1988.


Joe Kilian.
A general completeness theorem for two-party games.
In *Proceedings of STOC 1991*, pages 553–560. ACM, 1991.


Joe Kilian.
More general completeness theorems for secure two-party computation.
In *Proceedings of STOC 2000*, pages 316–324. ACM, 2000.


Joe Kilian, Eyal Kushilevitz, Silvio Micali, and Rafail Ostrovsky.
Reducibility and completeness in private computations.
SIAM Journal on Computing, 29(4):1189–1208, 2000.


Daniel Kraschewski and Jörn Müller-Quade.
Completeness theorems with constructive proofs for finite deterministic 2-party functions.
In Yuval Ishai, editor, *Theory of Cryptography, Proceedings of TCC 2011*, volume 6597 of *Lecture Notes in Computer Science*, pages 364–381. Springer, 2011.

References V


Robin Künzler, Jörn Müller-Quade, and Dominik Raub.
Secure computability of functions in the IT setting with dishonest majority and applications to long-term security.
In Omer Reingold, editor, *Theory of Cryptography, Proceedings of TCC 2009*, volume 5444 of *Lecture Notes in Computer Science*, pages 238–255. Springer, 2009.


Eyal Kushilevitz.
Privacy and communication complexity.
SIAM Journal on Discrete Mathematics, 5(2):273–284, 1992.


Yehuda Lindell, Eran Omri, and Hila Zarosim.
Completeness for symmetric two-party functionalities - revisited.
In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology, Proceedings of ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 116–133. Springer, 2012.


Michael Luby and Charles Rackoff.
How to construct pseudorandom permutations from pseudorandom functions.
SIAM Journal on Computing, 17(2):373–386, 1988.


Mohammad Mahmoody, Hemanta K. Maji, and Manoj Prabhakaran.
Limits of random oracles in secure computation.
Electronic Colloquium on Computational Complexity (ECCC), 19:65, 2012.

References VI

Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek.
Complexity of multi-party computation problems: The case of 2-party symmetric secure function evaluation.
In Omer Reingold, editor, *Theory of Cryptography, Proceedings of TCC 2009*, volume 5444 of *Lecture Notes in Computer Science*, pages 256–273. Springer, 2009.

Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek.
A zero-one law for cryptographic complexity with respect to computational UC security.
In Tal Rabin, editor, *Advances in Cryptology, Proceedings of CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 595–612. Springer, 2010.

Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek.
A unified characterization of completeness and triviality for secure function evaluation.
In Steven D. Galbraith and Mridul Nandi, editors, *Progress in Cryptology, Proceedings of INDOCRYPT 2012*, volume 7668 of *Lecture Notes in Computer Science*, pages 40–59. Springer, 2012.

Mike Rosulek.
Universal composability from essentially any trusted setup.
In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology, Proceedings of CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 406–423. Springer, 2012.

References VII

Daniel R. Simon.
Finding collisions on a one-way street: Can secure hash functions be based on general assumptions?
In Kaisa Nyberg, editor, *Advances in Cryptology, Proceedings of EUROCRYPT '98*, volume 1403 of *Lecture Notes in Computer Science*, pages 334–345. Springer, 1998.

Jürg Wullschleger.
Oblivious transfer from weak noisy channels.
In Omer Reingold, editor, *Theory of Cryptography, Proceedings of TCC 2009*, volume 5444 of *Lecture Notes in Computer Science*, pages 332–349. Springer, 2009.

Andrew Chi-Chih Yao.
Protocols for secure computations (extended abstract).
In *Proceedings of FOCS 1982*, pages 160–164. IEEE Computer Society, 1982.

What's complicated about it?

What's complicated about it?

cannot use uniform distribution

What's complicated about it?

cannot use uniform distribution

$\frac{1}{3}$ $\frac{2}{3}$	$\frac{2}{3}$ $\frac{1}{3}$	$\frac{1}{2}$ $\frac{1}{2}$
1	1	$\frac{1}{2}$ $\frac{1}{2}$

What's complicated about it?

cannot use uniform distribution

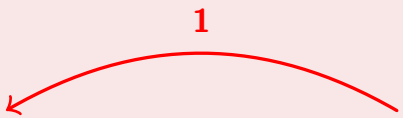
$\frac{1}{3}$ $\frac{2}{3}$	$\frac{2}{3}$ $\frac{1}{3}$	$\frac{1}{2}$ $\frac{1}{2}$
1	1	$\frac{1}{2}$ $\frac{1}{2}$

$\frac{1}{6}$ $\frac{1}{3}$	$\frac{1}{3}$ $\frac{1}{6}$	$\frac{1}{2}$ $\frac{1}{2}$
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$ $\frac{1}{2}$

What's complicated about it?

cannot use uniform distribution

$\frac{1}{3}$ $\frac{2}{3}$	$\frac{2}{3}$ $\frac{1}{3}$	$\frac{1}{2}$ $\frac{1}{2}$
1	1	$\frac{1}{2}$ $\frac{1}{2}$

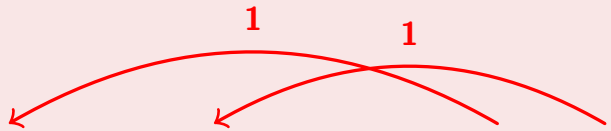


$\frac{1}{6}$ $\frac{1}{3}$	$\frac{1}{3}$ $\frac{1}{6}$	$\frac{1}{2}$ $\frac{1}{2}$
$\frac{1}{2}$	$\frac{1}{2}$ $\frac{1}{2}$	

What's complicated about it?

cannot use uniform distribution

$\frac{1}{3}$ $\frac{2}{3}$	$\frac{2}{3}$ $\frac{1}{3}$	$\frac{1}{2}$ $\frac{1}{2}$
1	1	$\frac{1}{2}$ $\frac{1}{2}$



$\frac{1}{6}$ $\frac{1}{3}$	$\frac{1}{3}$ $\frac{1}{6}$	$\frac{1}{2}$ $\frac{1}{2}$
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$ $\frac{1}{2}$

What's complicated about it?

cannot use uniform distribution

$\frac{1}{3}$ $\frac{2}{3}$	$\frac{2}{3}$ $\frac{1}{3}$	$\frac{1}{2}$ $\frac{1}{2}$
1	1	$\frac{1}{2}$ $\frac{1}{2}$

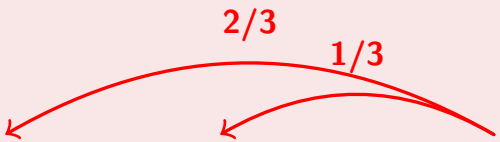
1/3

$\frac{1}{6}$ $\frac{1}{3}$	$\frac{1}{3}$ $\frac{1}{6}$	$\frac{1}{2}$ $\frac{1}{2}$
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$ $\frac{1}{2}$

What's complicated about it?

cannot use uniform distribution

$\frac{1}{3}$ $\frac{2}{3}$	$\frac{2}{3}$ $\frac{1}{3}$	$\frac{1}{2}$ $\frac{1}{2}$
1	1	$\frac{1}{2}$ $\frac{1}{2}$



$\frac{1}{6}$ $\mathbf{\frac{1}{3}}$	$\frac{1}{3}$ $\mathbf{\frac{1}{6}}$	$\frac{1}{2}$ $\frac{1}{2}$
$\mathbf{\frac{1}{2}}$	$\mathbf{\frac{1}{2}}$	$\frac{1}{2}$ $\frac{1}{2}$

What's complicated about it?

cannot use uniform distribution

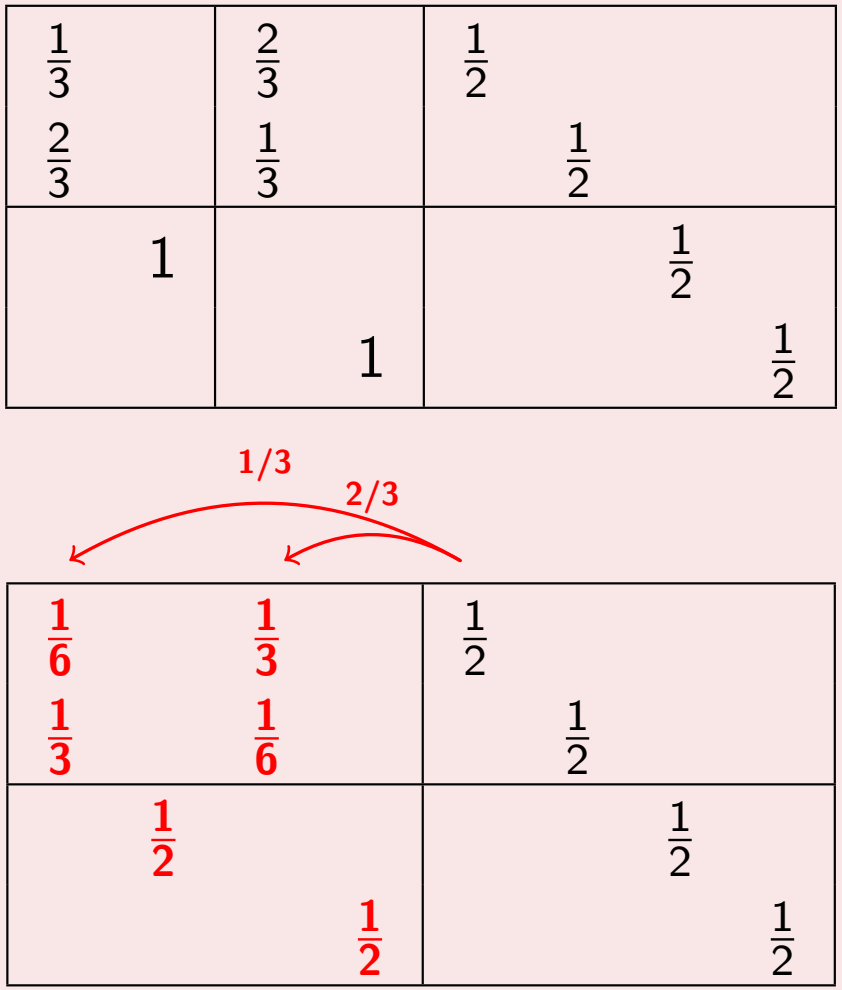
$\frac{1}{3}$ $\frac{2}{3}$	$\frac{2}{3}$ $\frac{1}{3}$	$\frac{1}{2}$ $\frac{1}{2}$
1	1	$\frac{1}{2}$ $\frac{1}{2}$

2/3

$\frac{1}{6}$ $\frac{1}{3}$	$\frac{1}{3}$ $\frac{1}{6}$	$\frac{1}{2}$ $\frac{1}{2}$
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$ $\frac{1}{2}$

What's complicated about it?

cannot use uniform distribution



$\frac{1}{3}$ $\frac{2}{3}$	$\frac{2}{3}$ $\frac{1}{3}$	$\frac{1}{2}$ $\frac{1}{2}$
1	1	$\frac{1}{2}$ $\frac{1}{2}$

$\mathbf{\frac{1}{6}}$ $\mathbf{\frac{1}{3}}$	$\mathbf{\frac{1}{3}}$ $\mathbf{\frac{1}{6}}$	$\frac{1}{2}$ $\frac{1}{2}$
$\mathbf{\frac{1}{2}}$	$\mathbf{\frac{1}{2}}$	$\frac{1}{2}$ $\frac{1}{2}$

What's complicated about it?

cannot use uniform distribution

$\frac{1}{3}$ $\frac{2}{3}$	$\frac{2}{3}$ $\frac{1}{3}$	$\frac{1}{2}$ $\frac{1}{2}$
1	1	$\frac{1}{2}$ $\frac{1}{2}$

$\frac{1}{6}$ $\frac{1}{3}$	$\frac{1}{3}$ $\frac{1}{6}$	$\frac{1}{2}$ $\frac{1}{2}$
$\frac{1}{2}$		$\frac{1}{2}$ $\frac{1}{2}$
	$\frac{1}{2}$	

cannot neglect inputs

What's complicated about it?

cannot use uniform distribution

$\frac{1}{3}$ $\frac{2}{3}$	$\frac{2}{3}$ $\frac{1}{3}$	$\frac{1}{2}$ $\frac{1}{2}$
1	1	$\frac{1}{2}$ $\frac{1}{2}$

$\frac{1}{6}$ $\frac{1}{3}$	$\frac{1}{3}$ $\frac{1}{6}$	$\frac{1}{2}$ $\frac{1}{2}$
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$ $\frac{1}{2}$

cannot neglect inputs

$\frac{1}{2}$ $\frac{1}{2}$	1	1
$\frac{1}{3}$ $\frac{2}{3}$	1	1

What's complicated about it?

cannot use uniform distribution

$\frac{1}{3}$ $\frac{2}{3}$	$\frac{2}{3}$ $\frac{1}{3}$	$\frac{1}{2}$ $\frac{1}{2}$
1	1	$\frac{1}{2}$ $\frac{1}{2}$

$\frac{1}{6}$ $\frac{1}{3}$	$\frac{1}{3}$ $\frac{1}{6}$	$\frac{1}{2}$ $\frac{1}{2}$
$\frac{1}{2}$		$\frac{1}{2}$ $\frac{1}{2}$
	$\frac{1}{2}$	

cannot neglect inputs

$\frac{1}{2}$ $\frac{1}{2}$	1	1

What's complicated about it?

cannot use uniform distribution

$\frac{1}{3}$ $\frac{2}{3}$	$\frac{2}{3}$ $\frac{1}{3}$	$\frac{1}{2}$ $\frac{1}{2}$
1	1	$\frac{1}{2}$ $\frac{1}{2}$

$\frac{1}{6}$ $\frac{1}{3}$	$\frac{1}{3}$ $\frac{1}{6}$	$\frac{1}{2}$ $\frac{1}{2}$
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$ $\frac{1}{2}$

cannot neglect inputs

$\frac{1}{2}$ $\frac{1}{2}$	1	1
$\frac{1}{3}$ $\frac{2}{3}$	1	1

What's complicated about it?

cannot use uniform distribution

$\frac{1}{3}$ $\frac{2}{3}$	$\frac{2}{3}$ $\frac{1}{3}$	$\frac{1}{2}$ $\frac{1}{2}$
1	1	$\frac{1}{2}$ $\frac{1}{2}$

$\frac{1}{6}$ $\frac{1}{3}$	$\frac{1}{3}$ $\frac{1}{6}$	$\frac{1}{2}$ $\frac{1}{2}$
$\frac{1}{2}$		$\frac{1}{2}$ $\frac{1}{2}$
	$\frac{1}{2}$	

cannot neglect inputs

$\frac{1}{3}$ $\frac{2}{3}$	1	1

What's complicated about it?

cannot use uniform distribution

$\frac{1}{3}$ $\frac{2}{3}$	$\frac{2}{3}$ $\frac{1}{3}$	$\frac{1}{2}$ $\frac{1}{2}$
1	1	$\frac{1}{2}$ $\frac{1}{2}$

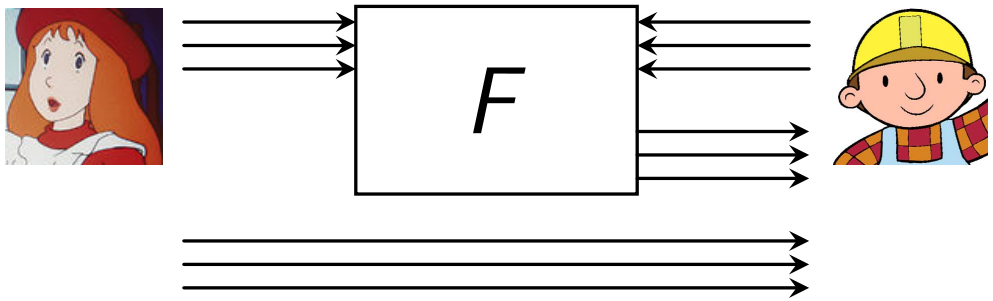
$\frac{1}{6}$ $\frac{1}{3}$	$\frac{1}{3}$ $\frac{1}{6}$	$\frac{1}{2}$ $\frac{1}{2}$
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$ $\frac{1}{2}$

cannot neglect inputs

$\frac{1}{2}$ $\frac{1}{2}$	1	1
$\frac{1}{3}$ $\frac{2}{3}$	1	1

Open Questions & Related Fields

Non-interactive completeness



related to Decomposable Randomized Encodings

what we know

- string-OT from bit-OT
  [Brassard-Crépeau-Santha-96]
- NC^1-NISC from OT, general NISC from OT+PRG
  [Ishai-Kushilevitz-Ostrovsky-Prabhakaran-Sahai-11]

open questions

- general information-theoretic NISC from OT?

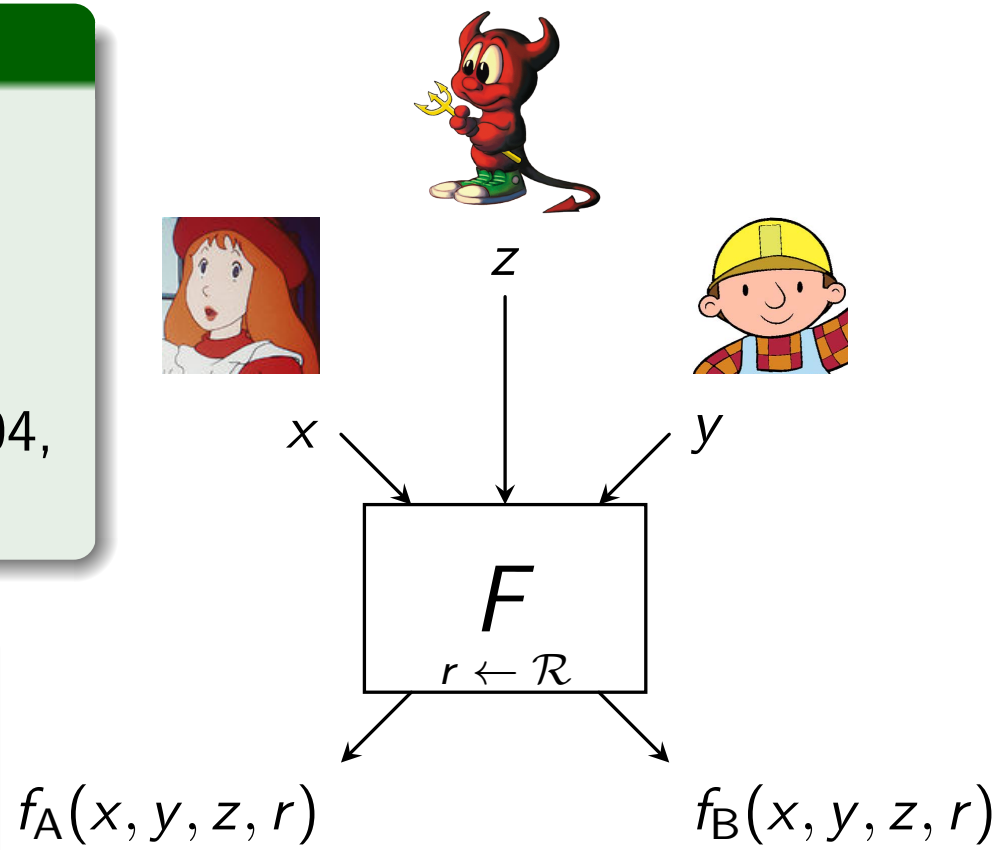
Leaky & unfair primitives

what we know

- completeness criteria for unfair noisy channels [Crépeau-Kilian-88, Damgård-Kilian-Salvail-99, Damgård-Fehr-Morozov-Salvail-04, Wullschleger-09]

open questions

- more complex crypto-gates?
- deterministic crypto-gates?



related to Combiners and Extractors

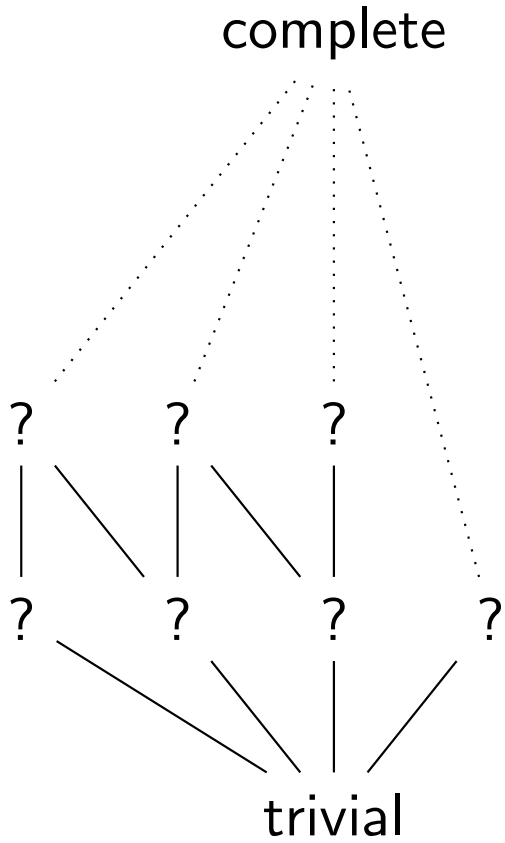
Non-complete crypto-gates

what we know

- classification of trivial crypto-gates [Kushilevitz-92, Beimel-Malkin-Micali-99, Künzler-MüllerQuade-Raub-09, Maji-Prabhakaran-Rosulek-09]
- examples for infinite hierarchy [Kilian-Kushilevitz-Micali-Ostrovsky-00, Maji-Prabhakaran-Rosulek-09]
- Non-complete crypto-gates are symmetric!

open questions

- concrete equivalence classes?
- constant-rate vs arbitrary (efficient) reduction?



related to Black-Box Separations

More than $O(1)$-size

this work

- $O(1)$-size $\rightsquigarrow$ efficient protocol for negligible error
- $O(2^k)$-size $\rightsquigarrow$ exponential complexity for negligible error?

what we know

- highly structured examples (e.g., string-OT, OPE)
- black-box reductions for oracle functionalities, e.g., IC and RO [Luby-Rackoff-88, Coron-Patarin-Seurin-08, Holenstein-Künzler-Tessaro-11, Baecher-Brzuska-Mittelbach-13]
- Random Oracle $\equiv$ Commitments [Mahmoody-Maji-Prabhakaran-12]

open questions

- completeness criteria for oracles?
- good definition for interesting crypto-gates with infinite number of possible inputs?

Computationally bounded adversaries

what we know

- An asymmetric F is complete, iff for some x_0, x_1 it is infeasible to reduce $f(x_1, \cdot)$ to $f(x_0, \cdot)$ [Harnik-Naor-Reingold-Rosen-04].
- Assuming a computational semi-honest OT protocol, (almost) every 2-party functionality is either trivial or complete [Maji-Prabhakaran-Rosulek-10, Rosulek-12].
- In the semi-honest model, any constant round protocol for a non-trivial $O(1)$-size function can be turned into an OT protocol [Lindell-Omri-Zarosim-12].
- black-box separations between OT, key-agreement, CRHF, OWF [Impagliazzo-Rudich-89, Simon-98, Gertner-Kannan-Malkin-Reingold-Viswanathan-00, Gertner-Malkin-Reingold-01]

open questions

- non-black-box reduction of OT to one-way functions?