



Revisiting Lower & Upper Bounds for Selective Decommitments

Rafail Ostrovsky

UCLA

Vanishree Rao

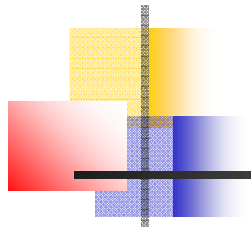
UCLA

Alessandra Scafuro

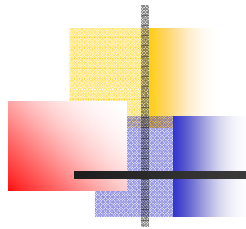
UCLA

Ivan Visconti

University of Salerno



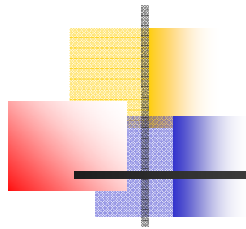
Commitment Schemes



Commitment Schemes

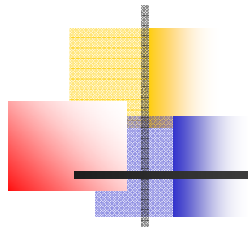
- . Binding

- . Hiding



Commitment Schemes

- Binding $\xrightarrow{\text{hybrid argument}}$ binding for multiple receivers
- Hiding



Binding against Multiple Receivers

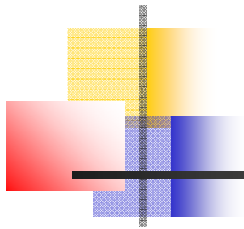
S^*

R_1

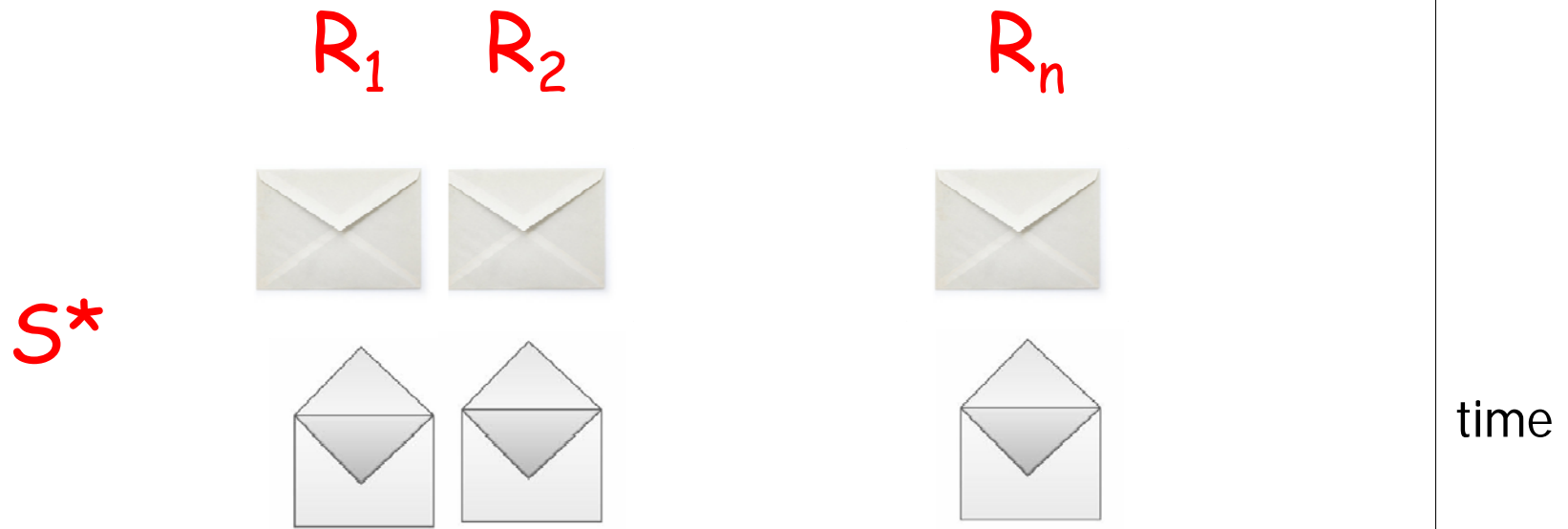
R_2

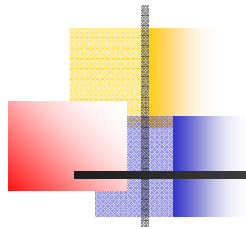
R_n

time

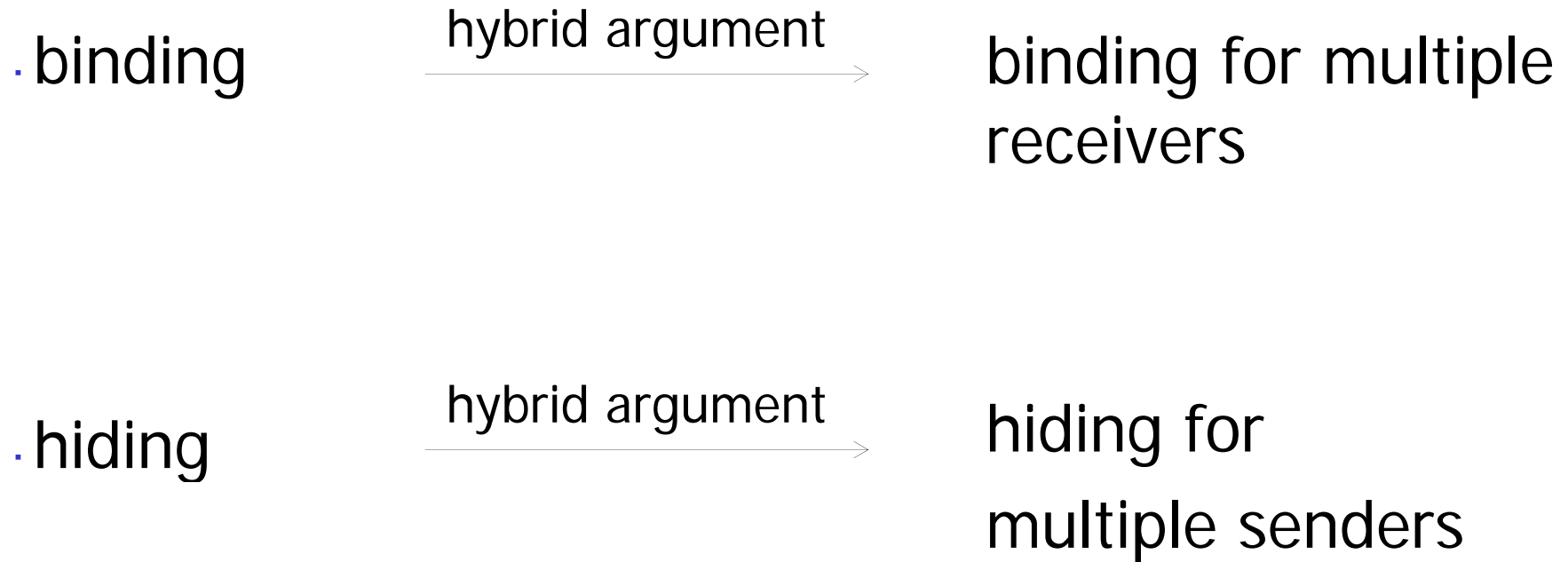


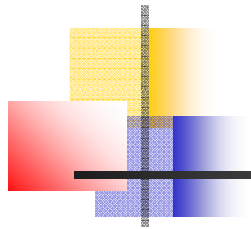
Binding against Multiple Receivers





Commitment Schemes



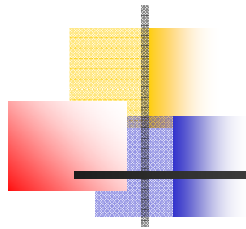


Hiding against Multiple Senders

S_1 S_2

S_n

R^*



Hiding against Multiple Senders

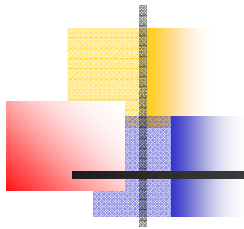
S_1

S_2

S_n



R^*



But if R^* continues...

S_1

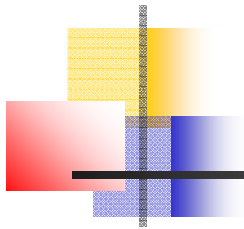
S_2

S_n



R^*





But if R^* continues...

S_1

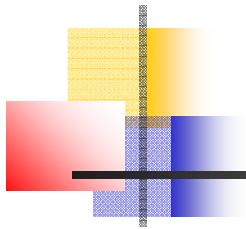
S_2

S_n



R^*

Hiding no longer follows
from hybrid argument



But if R^* continues...

[Dwork-Naor-Reingold-Stockmeyer-99]

S_1

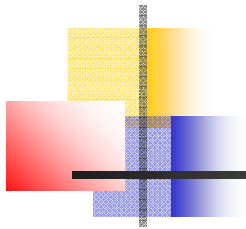
S_2

S_n



R^*

Hiding no longer follows
from hybrid argument



But if R^* continues...

[Dwork-Naor-Reingold-Stockmeyer-99]

S_1

S_2

S_n

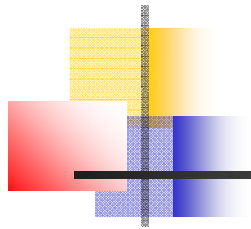


Selective Opening Attack (SOA)!

R^*



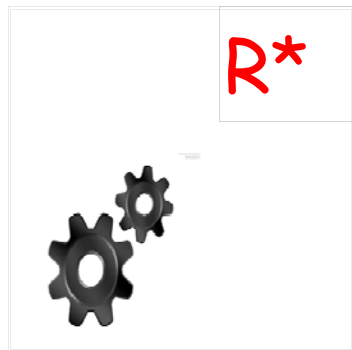
Hiding no longer follows from hybrid argument



Definition of SOA Security

Definition of SOA Security

Simulator



✓
0



✓
1



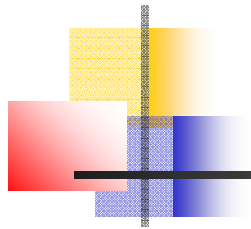
0



1



indistinguishable from real-world transcript

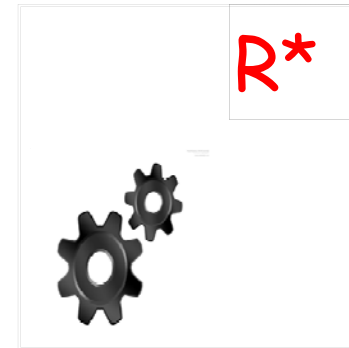


Security Definition - Fully BB



Security Definition - Fully BB

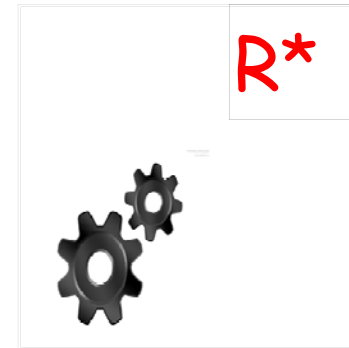
. simulator uses R^* in a BB manner;





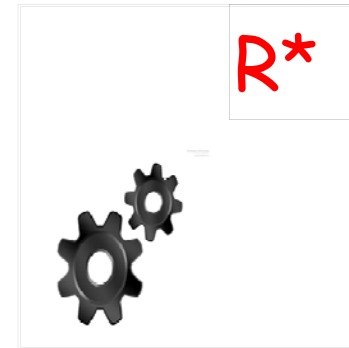
Security Definition - Fully BB

- . simulator uses R^* in a BB manner;
- . comm. scheme uses any underlying primitive (eg. OWP) in a BB manner.

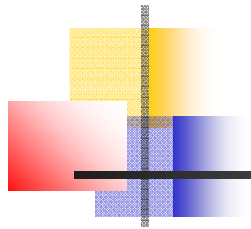




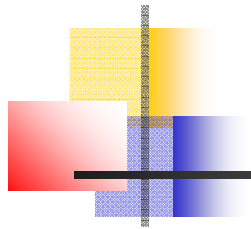
Security Definition - Fully BB



- . simulator uses R^* in a BB manner;
 - . comm. scheme uses any underlying primitive (eg. OWP) in a BB manner.
-
- . We focus on only this notion.



Parallel SOA Composition

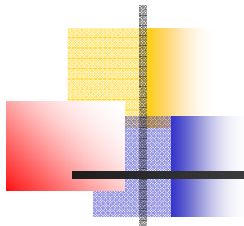


Parallel SOA Composition

S_1 S_2

S_n

R^*



Parallel SOA Composition

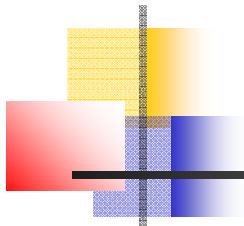
S_1

S_2

S_n



R^*



Parallel SOA Composition

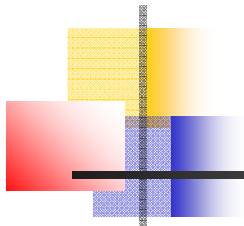
S_1

S_2

S_n



R^*



Parallel SOA Composition

S_1

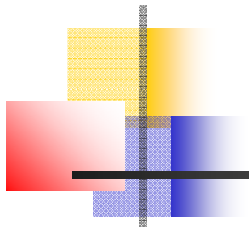
S_2

S_n



R^*





Parallel SOA Composition

[Dwork-Naor-Reingold-Stockmeyer-99]

S_1

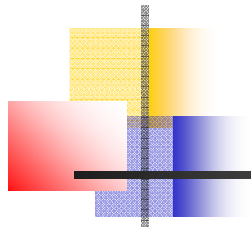
S_2

S_n



R^*





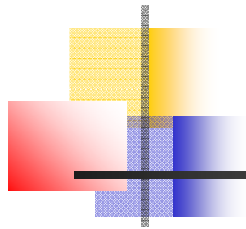
Fully-Concurrent SOA Composition

S_1

S_2

S_n

R^*



Fully-Concurrent SOA Composition

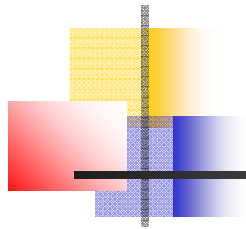
S_1

S_2

S_n



R^*



Fully-Concurrent SOA Composition

S_1

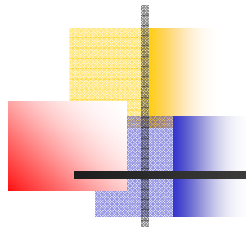


S_2

S_n



R^*



Fully-Concurrent SOA Composition

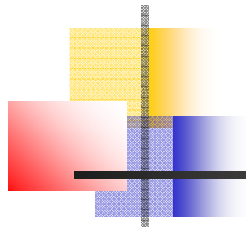
S_1

S_2

S_n



R^*



Fully-Concurrent SOA Composition

S_1

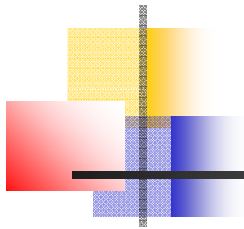
S_2

S_n



R^*





Fully-Concurrent SOA Composition

S_1



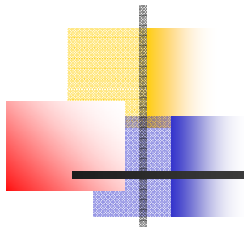
S_2



S_n



R^*



Fully-Concurrent SOA Composition

S_1



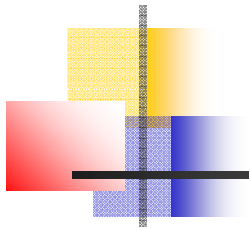
S_2



S_n



R^*



Fully-Concurrent SOA Composition

[Xiao-11]

S_1



S_2



S_n



R^*

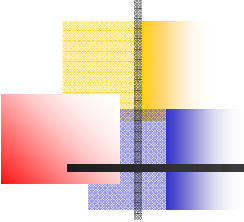


Concurrent-with-barrier SOA Composition

S_1 S_2

S_n

R^*



Concurrent-with-barrier SOA Composition

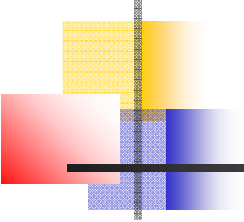
S_1

S_2

S_n



R^*



Concurrent-with-barrier SOA Composition

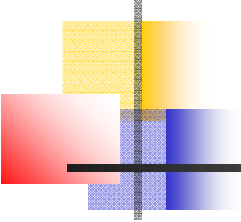
S_1

S_2

S_n



R^*



Concurrent-with-barrier SOA Composition

S_1



S_2



S_n



R^*



Concurrent-with-barrier SOA Composition

S_1



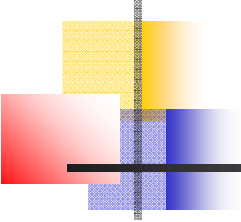
S_2



S_n



R^*



Concurrent-with-barrier SOA Composition

S_1



S_2

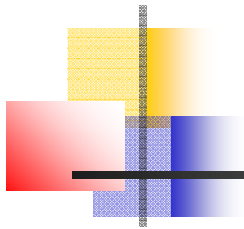


S_n



R^*





Concurrent-with-barrier SOA Composition

S_1



S_2

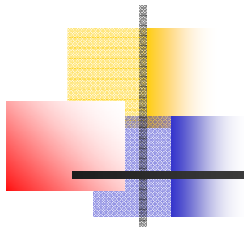


S_n



R^*





Concurrent-with-barrier SOA Composition

S_1



S_2

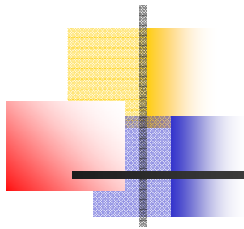


S_n



R^*





Concurrent-with-barrier SOA Composition

S_1

S_2

S_n



R^*



Concurrent-with-barrier SOA Composition

[Bellare-Hofheinz-Yilek-09, Hofheinz-11]

S_1

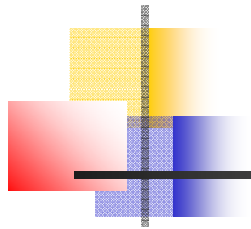
S_2

S_n

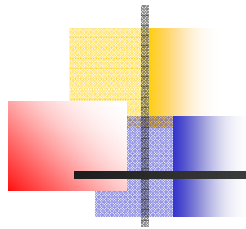


R^*



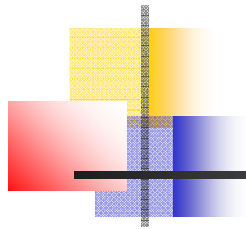


Nomenclature



Nomenclature

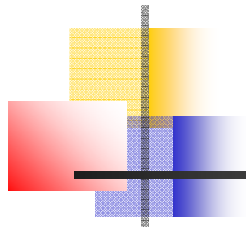
(x,y) - scheme



Nomenclature

(x,y) - scheme

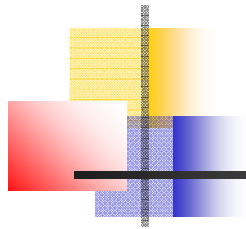
- Commitment Phase: x rounds



Nomenclature

(x,y) - scheme

- Commitment Phase: x rounds
- Decommitment Phase: y rounds



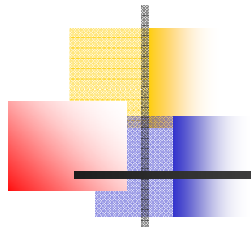
Nomenclature

(x,y) - scheme

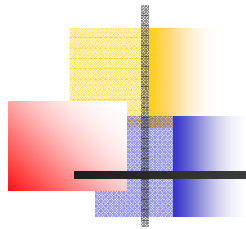
- Commitment Phase: x rounds
- Decommitment Phase: y rounds

One round



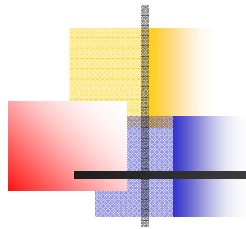


Significance of SOA-security



Significance of SOA-security

- . Commitment schemes are often used as sub-protocols in larger protocol, where only some commitments are opened;



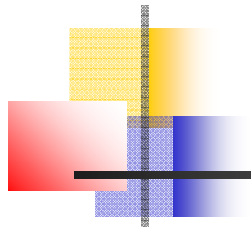
Significance of SOA-security

- . Commitment schemes are often used as sub-protocols in larger protocol, where only some commitments are opened;
- . Security of larger protocol relies on hiding of unopened commitments.



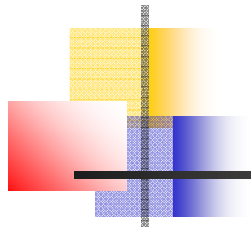
History - Rich Literature

- SOA-security for com. schemes (including indistinguishability based security):
 - [Dwork-Naor-Reingold-Stockmeyer-99, Gennaro-Micali-06, Bellare-Hofheinz-Yilek-09, Hemenway-Libert-Ostrovsky-Vergnaud-09, Hofheinz-11, Xiao-11, Bellare-Dowsley-Waters-Yilek-12, Goyal-Lee-Ostrovsky-Visconti-12, Xiao-12,...]
- SOA-security for public-key encryption schemes:
 - [Bellare-Hofheinz-Yilek-09, Fehr-Hofheinz-Kiltz-Wee-10, Bellare-Dowsley-Waters-Yilek-12, Böhl-Hofheinz-Kraschewski-12,...]
- SOA-security for identity-based encryption schemes:
 - [Bellare-Waters-Yilek-11,...]



Some Results of [BHY09, Hof11]

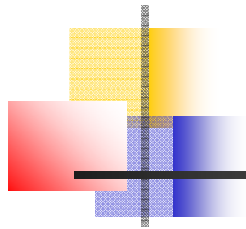
[Bellare-Hofheinz-Yilek-09, Hofheinz-11]



Some Results of [BHY09, Hof11]

[Bellare-Hofheinz-Yilek-09, Hofheinz-11]

- constructed **non-constant** round Conc.-with-barrier-SOA scheme, **NBB** use of OWP



Some Results of [BHY09, Hof11]

[Bellare-Hofheinz-Yilek-09, Hofheinz-11]

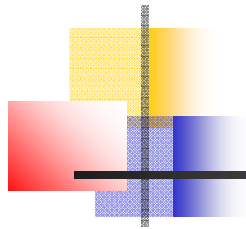
- constructed **non-constant** round Conc.-with-barrier-SOA scheme, **NBB** use of OWP
- also showed it is **impossible** to construct **non-interactive** SOA-scheme, **BB** use of any primitive, even for parallel composition, even if simulator uses adversary in a NBB manner



Some Results of [BHY09, Hof11]

[Bellare-Hofheinz-Yilek-09, Hofheinz-11]

- constructed **non-constant** round Conc.-with-barrier-SOA scheme, **NBB** use of OWP
- also showed it is **impossible** to construct **non-interactive** SOA-scheme, **BB** use of any primitive, even for parallel composition, even if simulator uses adversary in a NBB manner
- Immediate question: feasibility of **BB** SOA-schemes, their **round-optimality**?



Some Results of [BHY09, Hof11]

[Bellare-Hofheinz-Yilek-09, Hofheinz-11]

- constructed non-constant round Conc.-with-barrier-SOA scheme, NBB use of OWP
- also showed it is impossible to construct non-interactive SOA-scheme, BB use of any primitive, even for parallel composition, even if simulator uses adversary in a NBB manner
- Immediate question: feasibility of BB SOA-schemes, their round-optimality?



Some Results of [BHY09, Hof11]

[Bellare-Hofheinz-Yilek-09, Hofheinz-11]

- constructed non-constant round Conc.-with-barrier-SOA scheme, NBB use of OWP
- also showed it is impossible to construct non-interactive SOA-scheme, BB use of any primitive, even for parallel composition, even if simulator uses adversary in a NBB manner
- Immediate question: feasibility of BB SOA-schemes, their round-optimality?

Yes!



Some Results of [BHY09, Hof11]

[Bellare-Hofheinz-Yilek-09, Hofheinz-11]

- constructed non-constant round Conc.-with-barrier-SOA scheme, NBB use of OWP
- also showed it is impossible to construct non-interactive SOA-scheme, BB use of any primitive, even for parallel composition, even if simulator uses adversary in a NBB manner
- Immediate question: feasibility of BB SOA-schemes, their round-optimality?

Yes!

(3,1)



Some Results of [BHY09, Hof11]

[Bellare-Hofheinz-Yilek-09, Hofheinz-11]

- constructed non-constant round Conc.-with-barrier-SOA scheme, NBB use of OWP
- also showed it is impossible to construct non-interactive SOA-scheme, BB use of any primitive, even for parallel composition, even if simulator uses adversary in a NBB manner

Yes!

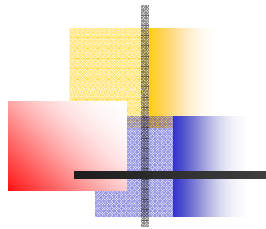
- Immediate question: feasibility of BB SOA-schemes, their round-optimality?

(3,1)

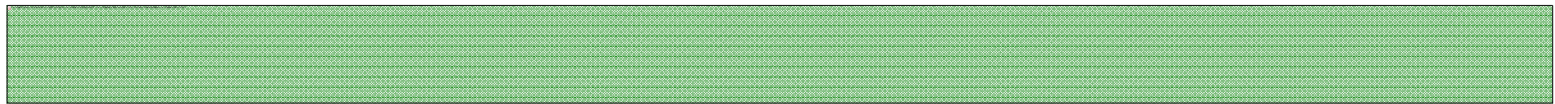
(2,1)-scheme is impossible [Xiao11]

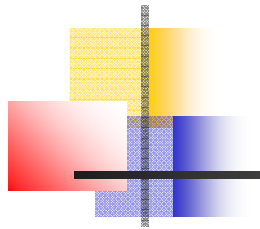


Our Results

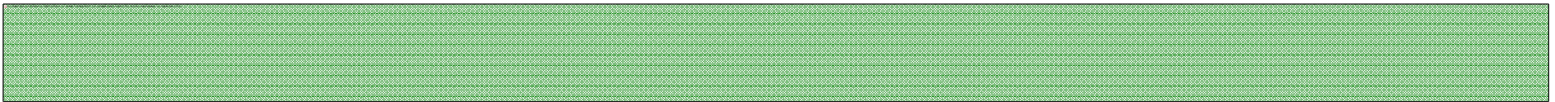
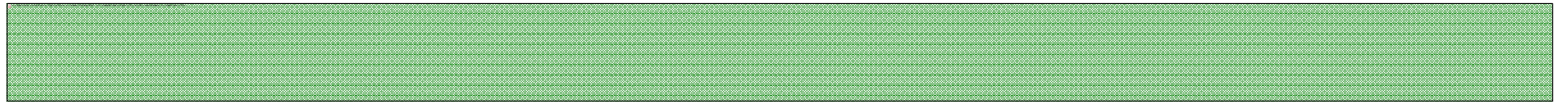


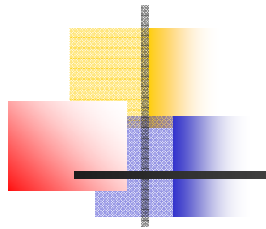
Our Results





Our Results





Our Results

[Redacted content]

[Redacted content]

[Redacted content]



Our Results

[Redacted]

[Redacted]

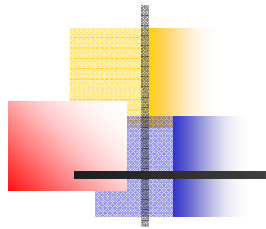
[Redacted]

[Lindell-03]

has to rewind;

more oracle queries for what bit values to open to.

Distinguishable!

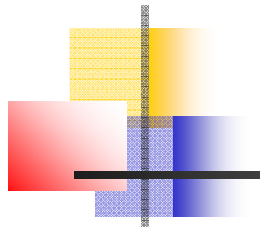


Our Results

[Green shaded area]

[Green shaded area]

[Green shaded area]

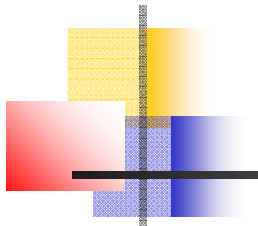


Our Results vs. [Xiao11]

[Redacted]

[Redacted]

[Redacted]



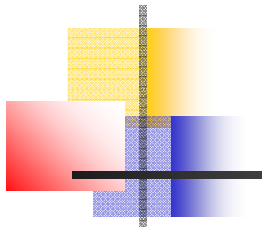
Our Results vs. [Xiao11]

[Redacted text block]

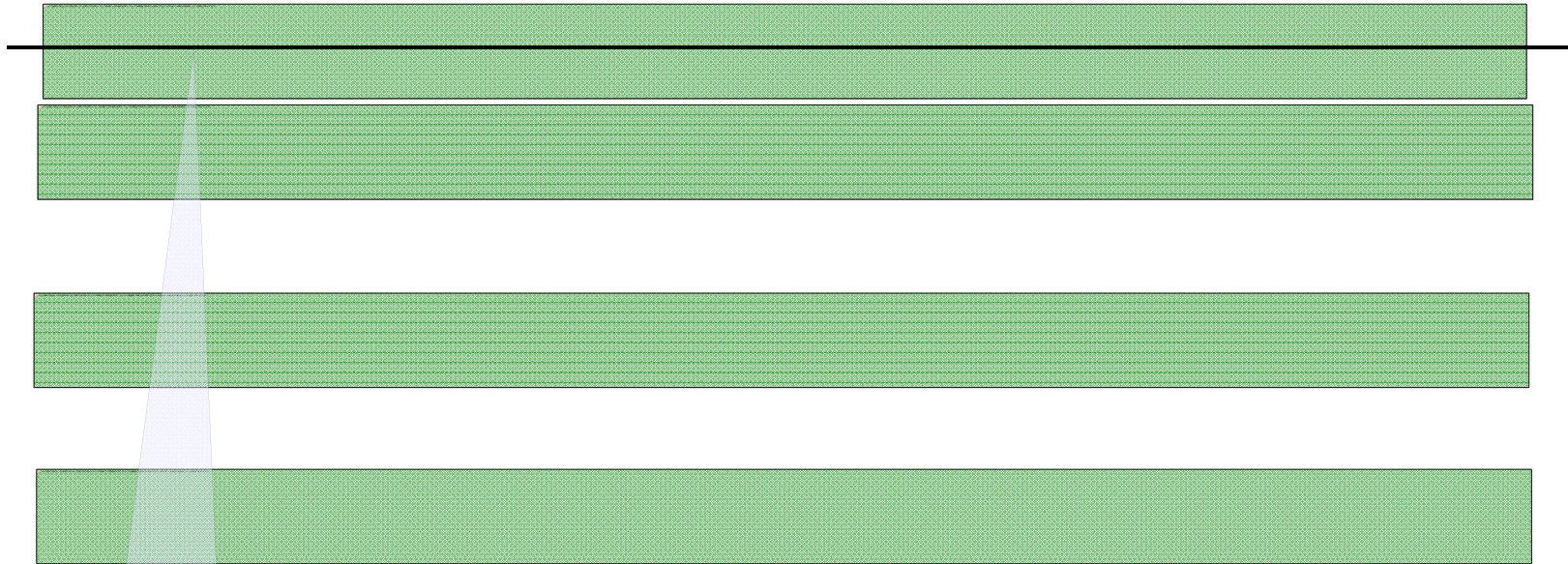
[Redacted text block]

[Redacted text block]

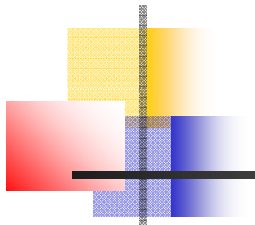
[Redacted text block]



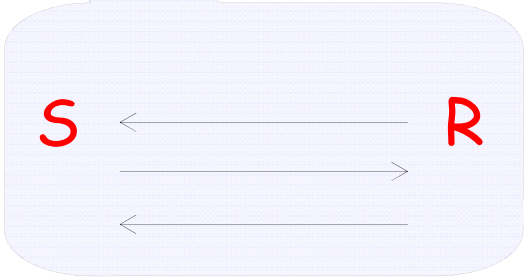
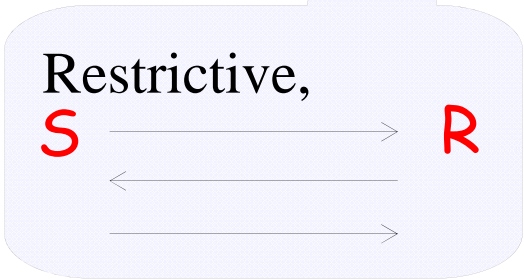
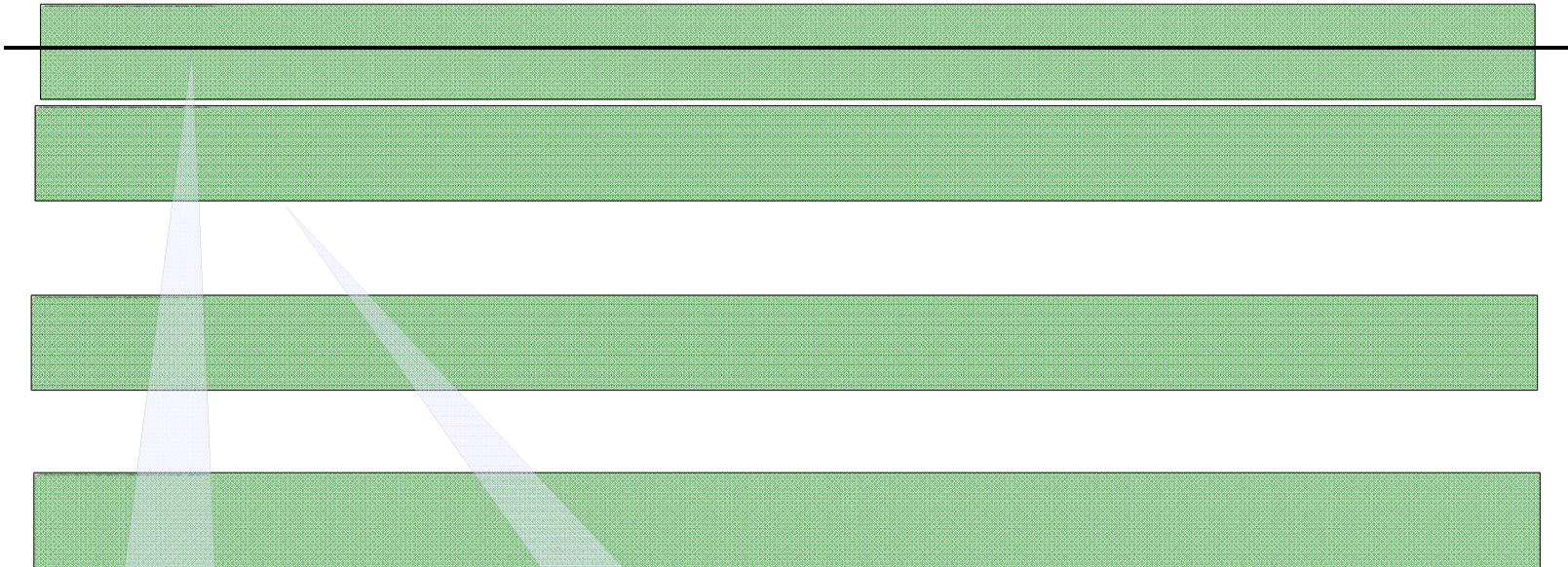
Our Results vs. [Xiao11]

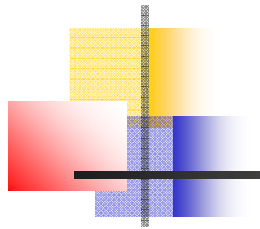


Restrictive,
S \longrightarrow **R**
 \longleftarrow
 \longrightarrow



Our Results vs. [Xiao11]





Our Results vs. [Xiao11]

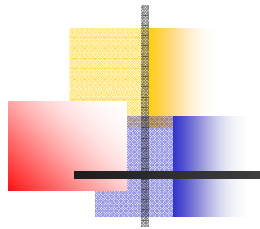
[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]



Our Results vs. [Xiao11]

[Redacted]

[Redacted]

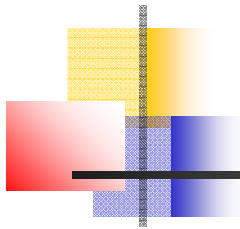
[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]



Our Results vs. [Xiao11]

[Redacted]

[Redacted]

[Redacted]

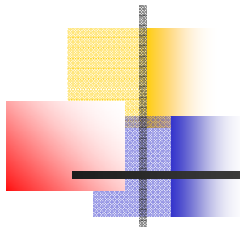
[Redacted]

[Redacted]

Proof of
hiding
against SOA

[Redacted]

[Redacted]



Our Results vs. [Xiao11]

[Redacted text block]

[Redacted text block]

[Redacted text block]

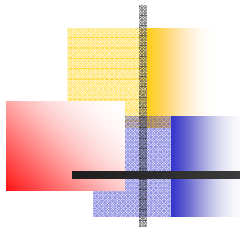
[Redacted text block]

[Redacted text block]

Proof of binding

[Redacted text block]

[Redacted text block]



Our Results vs. [Xiao11]

[Redacted]

[Redacted]

[Redacted]

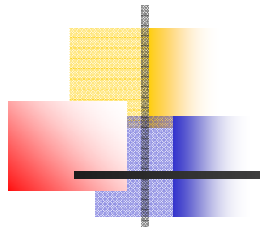
[Redacted]

[Redacted]

After our results were archived,
[Xiao12] showed different proof of hiding for $(t+3,1)$ -scheme

[Redacted]

[Redacted]



Our Results vs. [Xiao11]

[Redacted text block]

[Redacted text block]

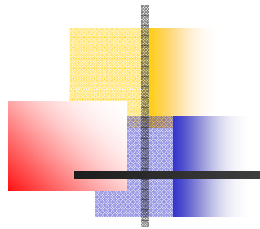
[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



Our Results vs. [Xiao11]

[Redacted]

[Redacted]

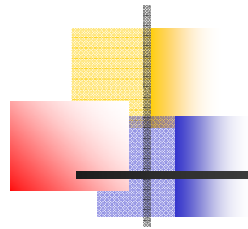
[Redacted]

[Redacted]

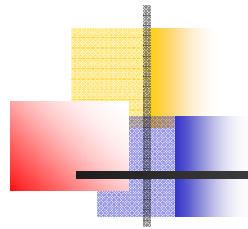
[Redacted]

[Redacted]

[Redacted]

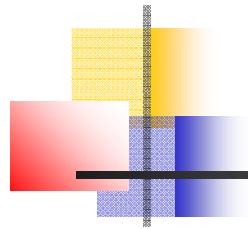


(5,1), BB OWP, Conc.-with-Barrier-SOA



$(5,1)$, BB OWP, Conc.-with-Barrier-SOA

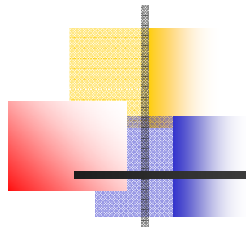
BB access to OWP



(5,1), BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

.Binding

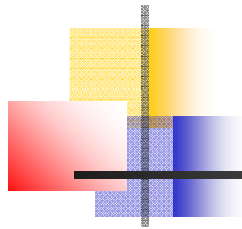


(5,1), BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

. Binding

. SOA-Hiding



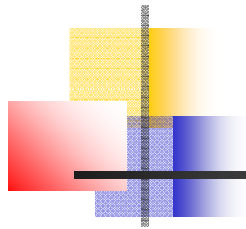
(5,1), BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

. Binding

. SOA-Hiding

implies non-interactive com. scheme



(5,1), BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

✓ binding

SOA-Hiding

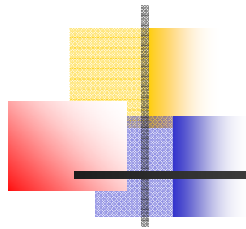
implies non-interactive com. scheme

$S(b)$

R

Com(b)

Open to b



(5,1), BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

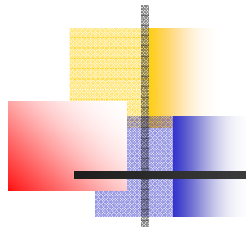
✓ binding

SOA-Hiding

$S(b)$

$Com_0(b)$
 $Com_1(b)$

R



$(5,1)$, BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

✓ Binding

SOA-Hiding

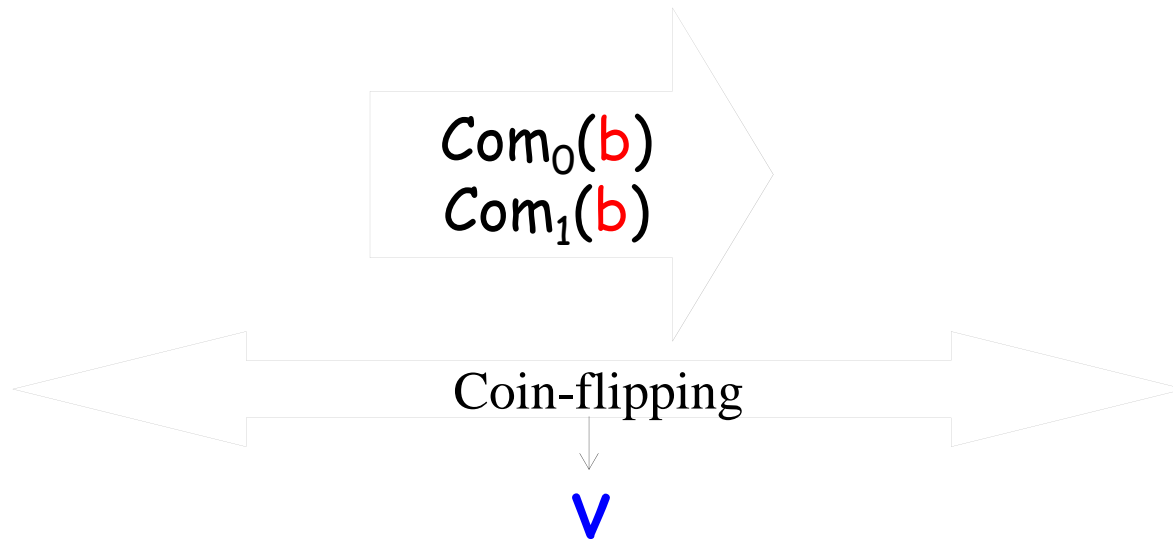
$S(b)$

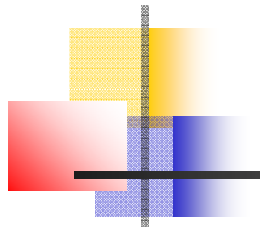
$Com_0(b)$
 $Com_1(b)$

R

Coin-flipping

v





$(5,1)$, BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

✓ binding

SOA-Hiding

$S(b)$

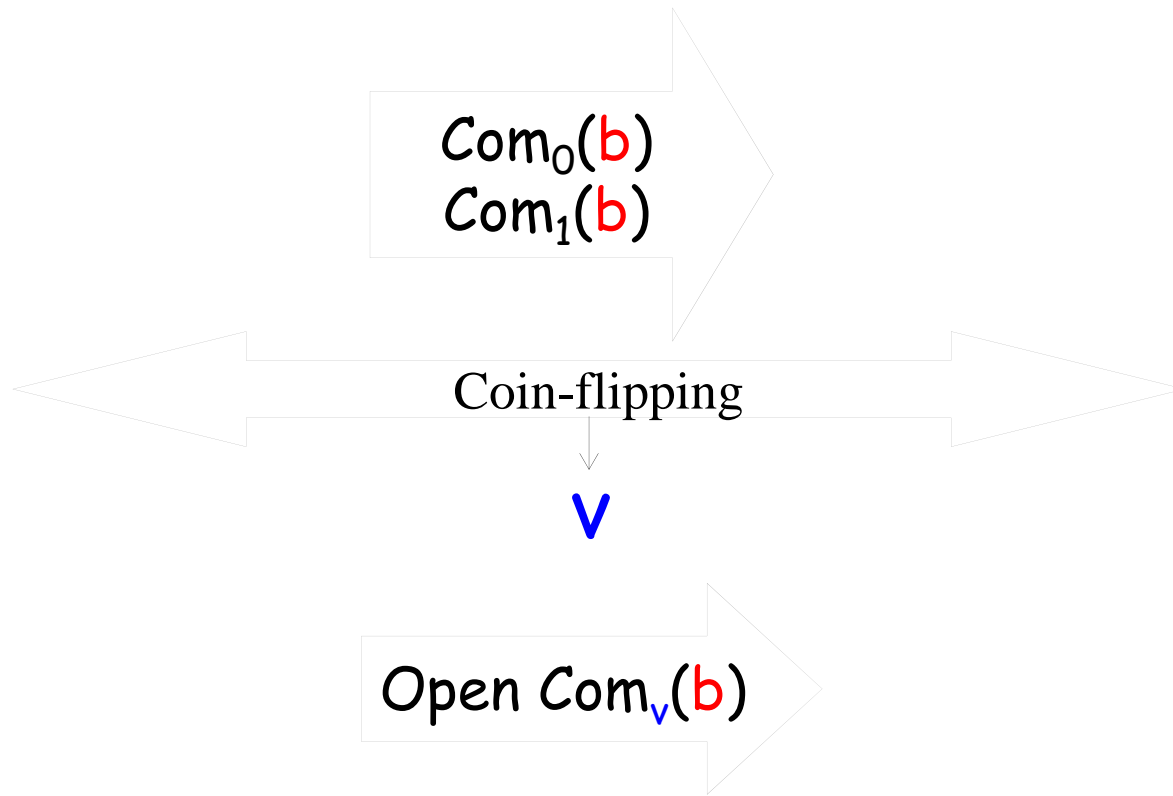
$Com_0(b)$
 $Com_1(b)$

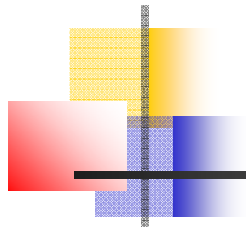
R

Coin-flipping

v

Open $Com_v(b)$



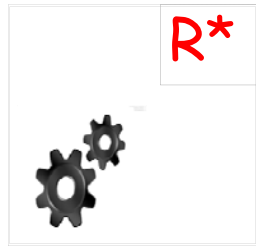


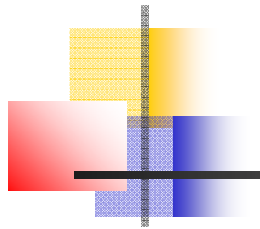
(5,1), BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

✓ binding

.SOA-Hiding



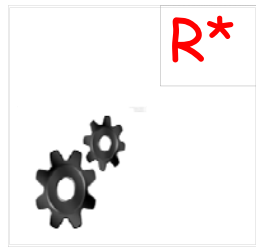


(5,1), BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

✓ binding

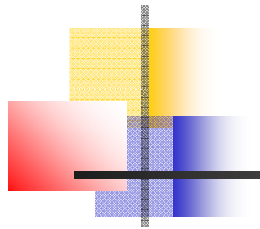
SOA-Hiding



0

Com₀(1)
Com₁(0)



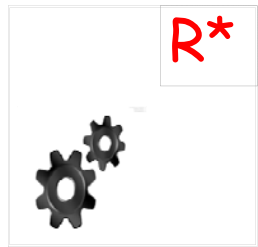


(5,1), BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

✓ Binding

SOA-Hiding

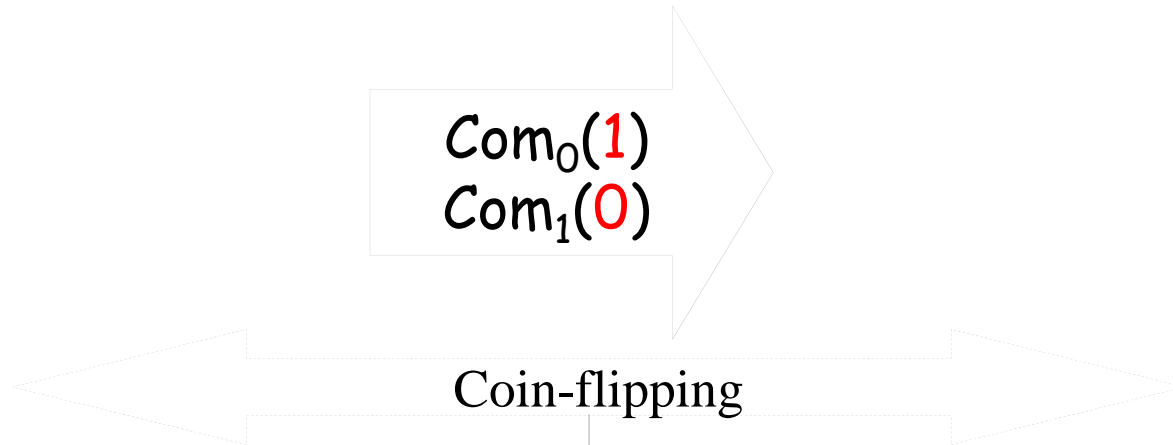


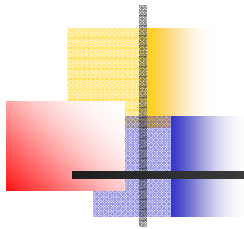
0

$Com_0(1)$
 $Com_1(0)$

Coin-flipping

1



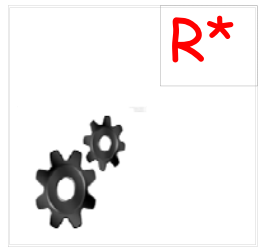


(5,1), BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

✓ Binding

SOA-Hiding



0

Com₀(1)
Com₁(0) ✓

Coin-flipping

1

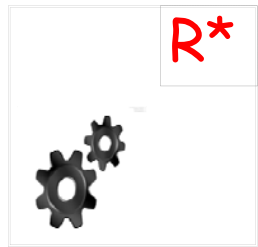
Open Com₁(0)

(5,1), BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

✓ Binding

SOA-Hiding



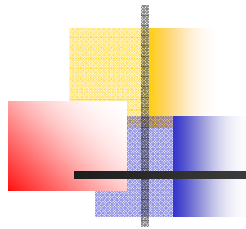
1

$Com_0(1)$ ✓
 $Com_1(0)$

Coin-flipping

0

Open $Com_0(1)$



$(5,1)$, BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

✓ Binding

✓ SOA-Hiding

$S(b)$

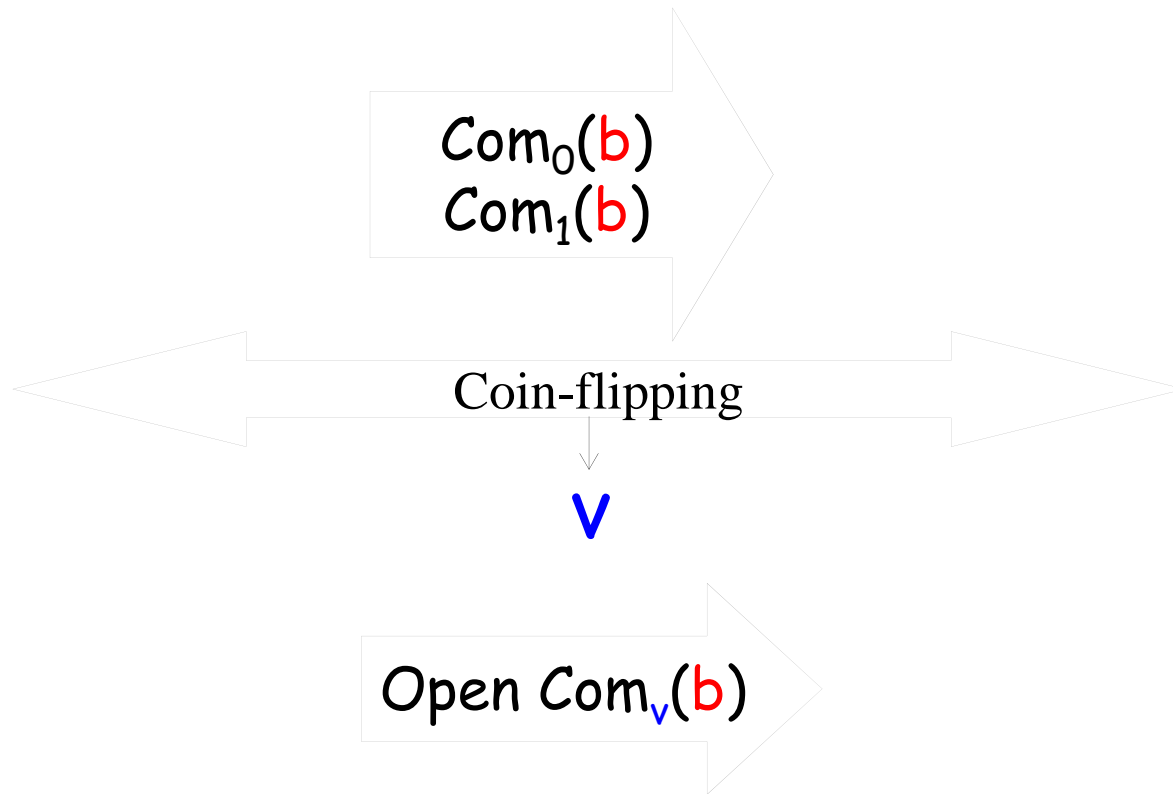
$Com_0(b)$
 $Com_1(b)$

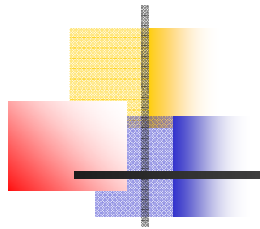
R

Coin-flipping

v

Open $Com_v(b)$





$(5,1)$, BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

X Binding

✓ SOA-Hiding

$S(b)$

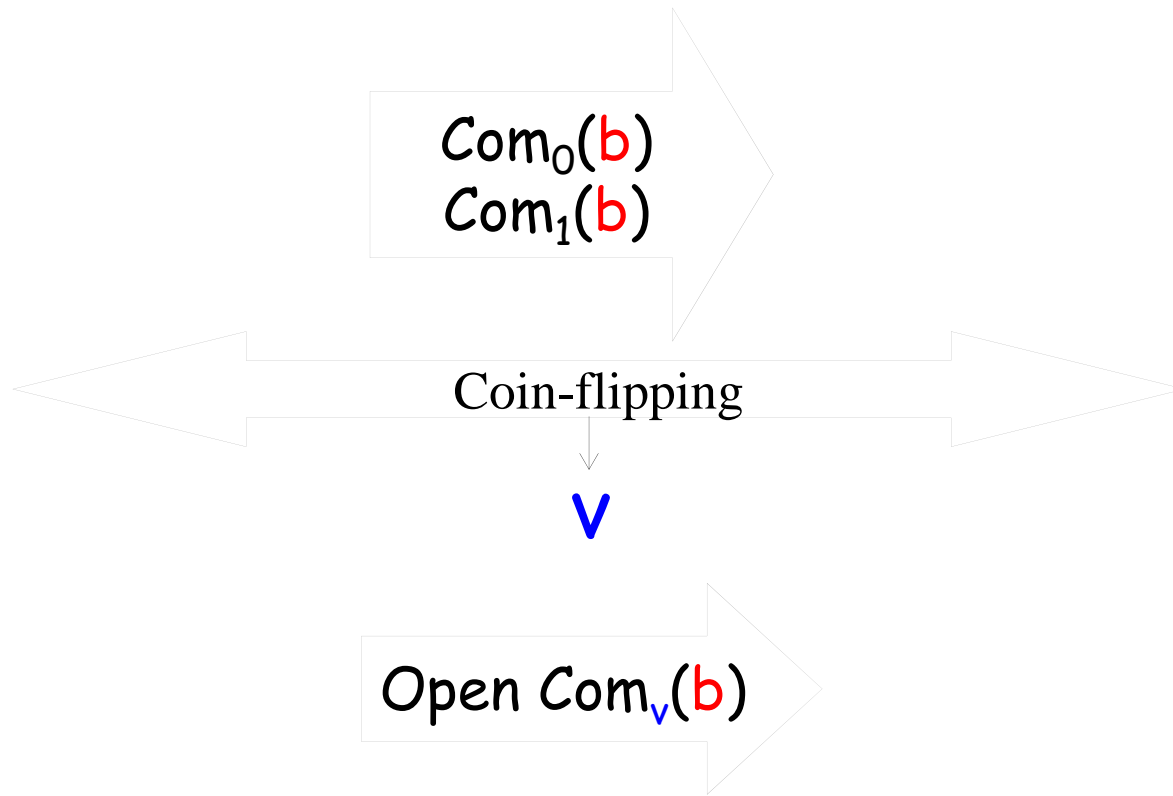
$Com_0(b)$
 $Com_1(b)$

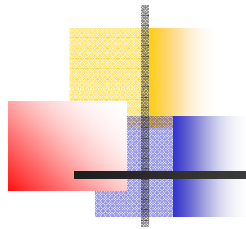
R

Coin-flipping

v

Open $Com_v(b)$





(5,1), BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

~~X~~ Binding

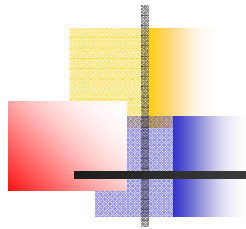
✓ SOA-Hiding

S^*

$Com_0(1)$
 $Com_1(0)$

R

Coin-flipping



(5,1), BB OWP, Conc.-with-Barrier-SOA

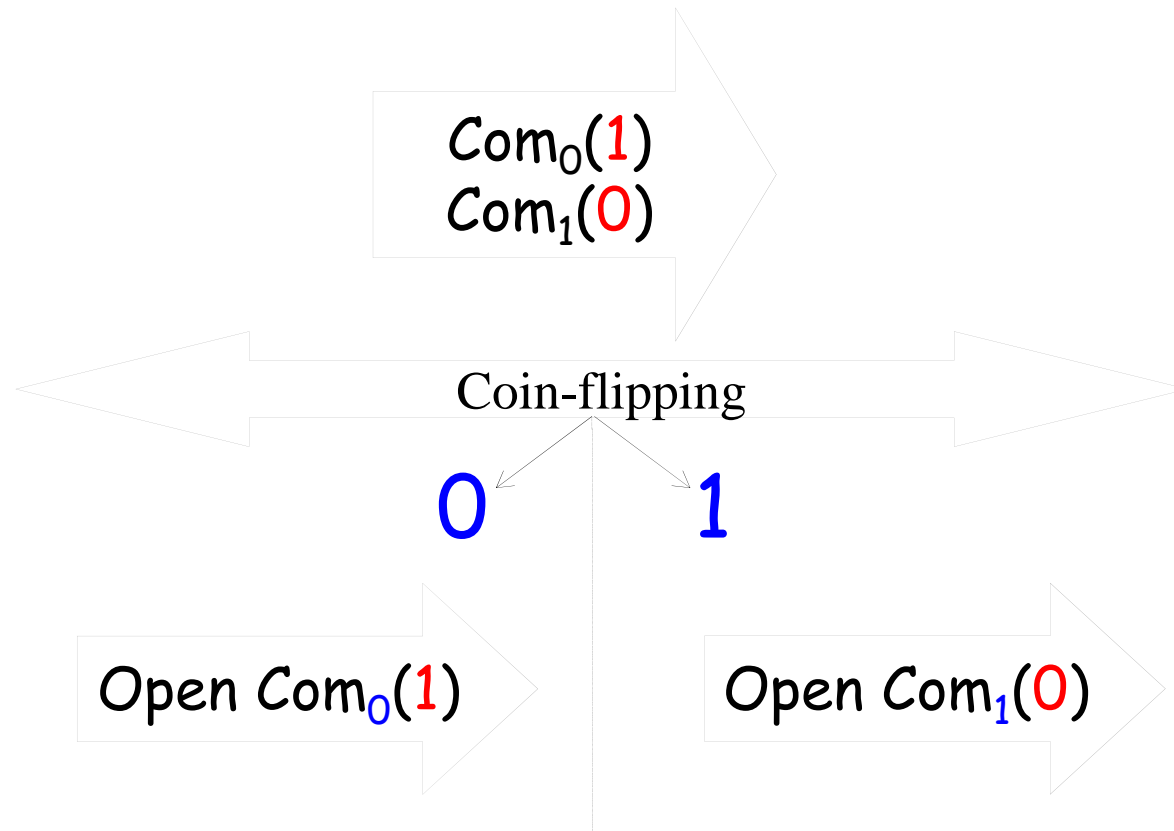
BB access to OWP

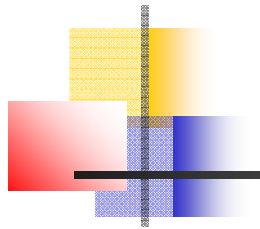
X Binding

✓ SOA-Hiding

S^*

R





(5,1), BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

X Binding

✓ SOA-Hiding

S(b)

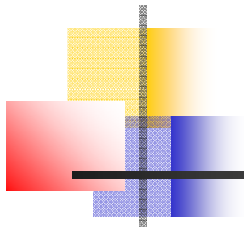
$Com_{10}(b), Com_{20}(b), \dots, Com_{n0}(b)$
 $Com_{11}(b), Com_{21}(b), \dots, Com_{n1}(b)$

R

Coin-flipping

v

Open $Com_v(b)$



(5,1), BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

X Binding

✓ SOA-Hiding

S(b)

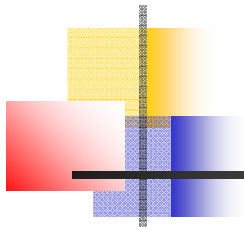
$Com_{10}(b), Com_{20}(b), \dots, Com_{n0}(b)$
 $Com_{11}(b), Com_{21}(b), \dots, Com_{n1}(b)$

R

Coin-flipping

10.....1

Open $Com_v(b)$



(5,1), BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

X Binding

✓ SOA-Hiding

S(b)

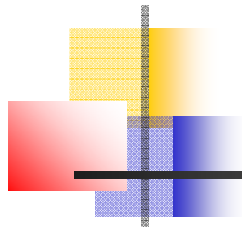
$Com_{10}(b), Com_{20}(b), \dots, Com_{n0}(b)$
 $Com_{11}(b), Com_{21}(b), \dots, Com_{n1}(b)$

R

Coin-flipping

10.....1

$Open_{10}(b), Open_{20}(b), \dots, Open_{n0}(b)$
 $Open_{11}(b), Open_{21}(b), \dots, Open_{n1}(b)$



$(5,1)$, BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

X Binding

✓ SOA-Hiding

$S(b)$

$Com_{10}(b), Com_{20}(b), \dots, Com_{n0}(b)$
 $Com_{11}(b), Com_{21}(b), \dots, Com_{n1}(b)$

6 rounds

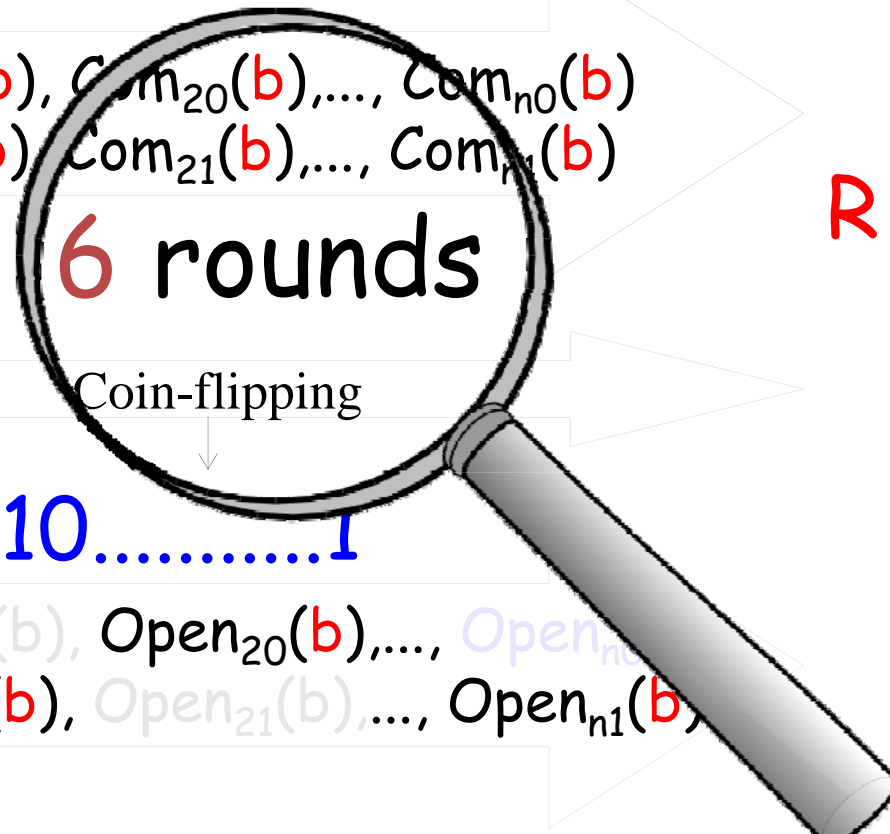
Coin-flipping

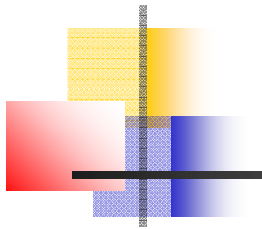
R

10.....1

$Open_{10}(b), Open_{20}(b), \dots, Open_{n0}(b)$
 $Open_{11}(b), Open_{21}(b), \dots, Open_{n1}(b)$

non-interactive
decommitment?!



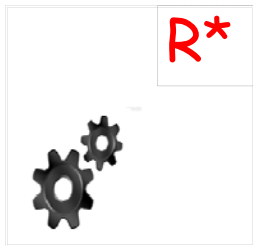


(5,1), BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

✓ Binding

✓ SOA-Hiding



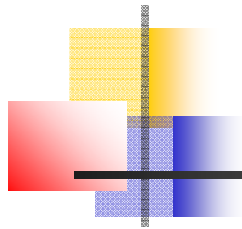
$Com_{10}(1), Com_{20}(0), \dots, Com_{n0}(1)$
 $Com_{11}(0), Com_{21}(1), \dots, Com_{n1}(0)$

?

Coin-flipping

??.....?

$Open_{10}(1), Open_{20}(0), \dots, Open_{n0}(1)$
 $Open_{11}(0), Open_{21}(1), \dots, Open_{n1}(0)$



(5,1), BB OWP, Conc.-with-Barrier-SOA

BB access to OWP
coin-flipping outcome

✓ Binding

✓ SOA-Hiding

$S(b)$

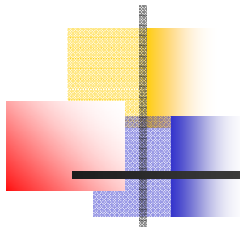
$Com_{10}(b), Com_{20}(b), \dots, Com_{n0}(b)$
 $Com_{11}(b), Com_{21}(b), \dots, Com_{n1}(b)$

R

Coin-flipping

10.....1

$Open_{10}(b), Open_{20}(b), \dots, Open_{n0}(b)$
 $Open_{11}(b), Open_{21}(b), \dots, Open_{n1}(b)$



(5,1), BB OWP, Conc.-with-Barrier-SOA

BB access to OWP

✓ Binding

✓ SOA-Hiding

coin-flipping outcome
or
its complement

$S(b)$

$Com_{10}(b), Com_{20}(b), \dots, Com_{n0}(b)$
 $Com_{11}(b), Com_{21}(b), \dots, Com_{n1}(b)$

R

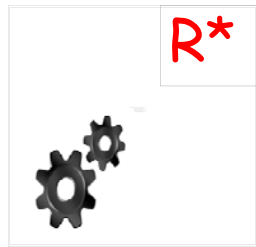
Coin-flipping

10.....1

$Open_{10}(b), Open_{20}(b), \dots, Open_{n0}(b)$
 $Open_{11}(b), Open_{21}(b), \dots, Open_{n1}(b)$

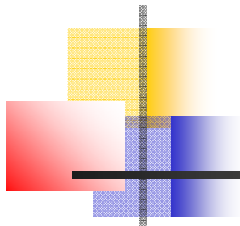


Conc.-With-Barrier Simulation Idea

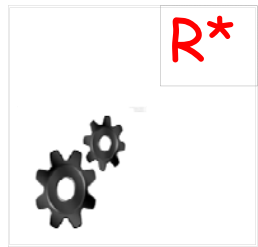


$Com_{10}(1), Com_{20}(0), \dots, Com_{n0}(1)$
 $Com_{11}(0), Com_{21}(1), \dots, Com_{n1}(0)$





Conc.-With-Barrier Simulation Idea



$Com_{10}(1), Com_{20}(0), \dots, Com_{n0}(1)$
 $Com_{11}(0), Com_{21}(1), \dots, Com_{n1}(0)$



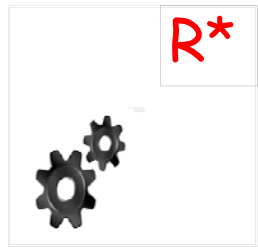
Coin-flipping

10.....1

0

$Open_{10}(1), Open_{20}(0), \dots, Open_{n0}(1)$
 $Open_{11}(0), Open_{21}(1), \dots, Open_{n1}(0)$

Conc.-With-Barrier Simulation Idea



$Com_{10}(1), Com_{20}(0), \dots, Com_{n0}(1)$
 $Com_{11}(0), Com_{21}(1), \dots, Com_{n1}(0)$



Coin-flipping

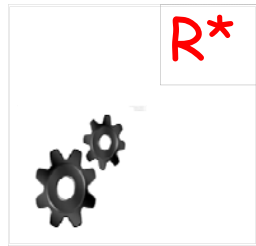
10.....1

1

$Open_{10}(1), Open_{20}(0), \dots, Open_{n0}(1)$
 $Open_{11}(0), Open_{21}(1), \dots, Open_{n1}(0)$

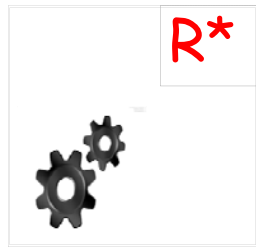


Conc.-With-Barrier Simulation Idea





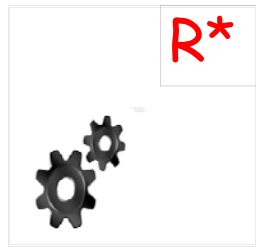
Conc.-With-Barrier Simulation Idea



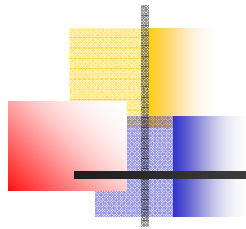
- . During simulation, for sessions newly started in rewind threads, no new oracle queries, due to **barrier!!**



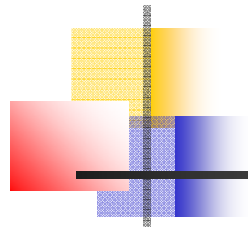
Conc.-With-Barrier Simulation Idea



- . During simulation, for sessions newly started in rewind threads, no new oracle queries, due to **barrier!!**
- . Fully conc. impossibility arguments do not apply.



Conclusions



Conclusions

- Round-optimal, fully BB SOA-secure schemes



Conclusions

- Round-optimal, fully BB SOA-secure schemes
- Point out issues in [Xiao11], significantly changed state-of-the-art



Thank You!