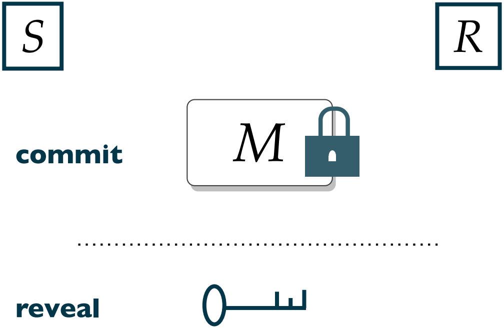
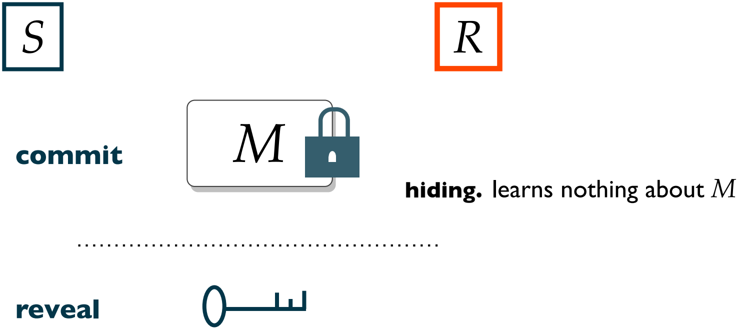
On the Complexity of UC Commitments

Juan A. Garay (**Yahoo Labs**)
Yuval Ishai (**Technion**)
Ranjit Kumaresan (**Technion**)
Hoeteck Wee (**ENS**)

commitments



commitments



commitments

S R

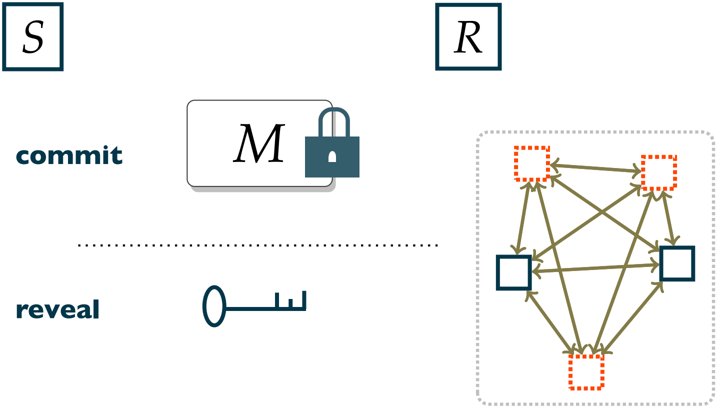
commit

hiding. learns nothing about M

reveal

binding. cannot change M

commitments



UC security [Canetti 01]

prior works

feasibility. [Canetti Fischlin 01, Canetti Lindell Ostrovsky Sahai 02]

– general assumptions, assuming a CRS

– impossible without set-up assumptions

prior works

feasibility. [Canetti Fischlin 01, Canetti Lindell Ostrovsky Sahai 02]

efficiency. [Damgård Nielsen 02, Damgård Groth 03, Lindell 11, Fischlin Libert Manulis 11, Abdalla Ben-Hamouda Blazy Chevalier Pointcheval 13, Julta Roy 13]

– $M \in \{0,1\}^L$, send $\geq 5L$ bits and $O(L/\kappa)$ exponentiations

prior works

feasibility. [Canetti Fischlin 01, Canetti Lindell Ostrovsky Sahai 02]

efficiency. [Damgård Nielsen 02, Damgård Groth 03, Lindell 11, Fischlin Libert Manulis 11, Abdalla Ben-Hamouda Blazy Chevalier Pointcheval 13, Julta Roy 13]

- $M \in \{0,1\}^L$, send $\geq 5L$ bits and $O(L/\kappa)$ exponentiations
- public-key operations are necessary [Damgård Groth 03]

stand-alone commitments.

- $L + 3\kappa$ bits and only PRG [Blum 81, Naor 89]

prior works

feasibility. [Canetti Fischlin 01, Canetti Lindell Ostrovsky Sahai 02]

efficiency. [Damgård Nielsen 02, Damgård Groth 03, Lindell 11, Fischlin Libert Manulis 11, Abdalla Ben-Hamouda Blazy Chevalier Pointcheval 13, Julta Roy 13]

- $M \in \{0,1\}^L$, send $\geq 5L$ bits and $O(L/\kappa)$ exponentiations
- public-key operations are necessary [Damgård Groth 03]

Q (1) rate 1 i.e. $(1+o(1))L$ bits ?

prior works

feasibility. [Canetti Fischlin 01, Canetti Lindell Ostrovsky Sahai 02]

efficiency. [Damgård Nielsen 02, Damgård Groth 03, Lindell 11, Fischlin Libert Manulis 11, Abdalla Ben-Hamouda Blazy Chevalier Pointcheval 13, Julta Roy 13]

– $M \in \{0,1\}^L$, send $\geq 5L$ bits and $O(L/\kappa)$ exponentiations

– public-key operations are necessary [Damgård Groth 03]

Q

(1) rate 1 i.e. $(1 + o(1))L$ bits ?

(2) poly(κ) public-key operations ?

bootstrapping?

bootstrapping?

commitment length extension

bootstrapping?

commit κ-bit s + $\mathsf{PRG}(s) \oplus M$

bootstrapping?

commit κ-bit s + PRG$(s) \oplus M$

communication. $L + O(\kappa)$ bits (rate 1)

computation. $O(1)$ exponentiations + 1 PRG

bootstrapping?

commit κ-bit s + $\mathsf{PRG}(s) \oplus M$

reveal $O(\kappa)$ bits

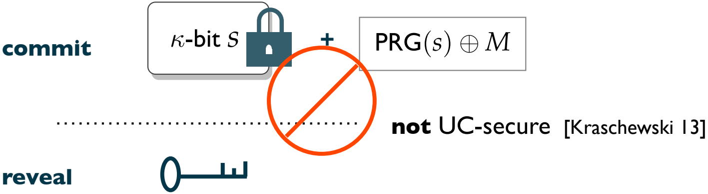
bootstrapping?

commit κ-bit s  **+** $\text{PRG}(s) \oplus M$

secure in stand-alone setting

reveal 

bootstrapping?



our results

1. **efficiency.** rate 1 UC commitments
   - ✓ $(1 + o(1))L$ bits in commit and reveal
   - ✓ $\tilde{O}(\kappa)$ OT calls, black-box use of a PRG

our results

1 **efficiency.** rate 1 UC commitments

- ✓ $(1 + o(1))L$ bits in commit and reveal
- ✓ $\tilde{O}(\kappa)$ OT calls, black-box use of a PRG

corollary #1. [Peikert Waters Vaikuntanathan 08, Choi Katz W Zhou 13]

- rate 1 UC commitments in CRS model
- $\tilde{O}(\kappa)$ exponentiations under DDH

our results

1 **efficiency.** rate 1 UC commitments

- ✓ $(1 + o(1))L$ bits in commit and reveal
- ✓ $\tilde{O}(\kappa)$ OT calls, black-box use of a PRG

corollary #2. [Choi Dachman-Soled Malkin W 09, Haitner Ishai Kushilevitz Lindell Petrank 11]

- rate 1 UC commitment length extension
- black-box use of semi-honest OT

our results

1. **efficiency.** rate 1 UC commitments
   - ✓ $(1 + o(1))L$ bits in commit and reveal
   - ✓ $\tilde{O}(\kappa)$ OT calls, black-box use of a PRG

corollary #2. [Choi Dachman-Soled Malkin W 09, Haitner Ishai Kushilevitz Lindell Petrank 11]

- rate 1 UC commitment length extension
- black-box use of semi-honest OT

2. **necessity.** UC commitment length extension implies OT

our results

1 **efficiency.** rate 1 UC commitments

✓ $(1+o(1))L$ bits in commit and reveal

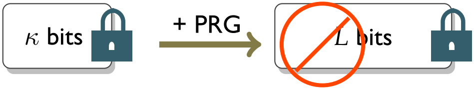
✓ $\tilde{O}(\kappa)$ OT calls, black-box use of a PRG

corollary #2. [Choi Dachman-Soled Malkin W 09, Haitner Ishai Kushilevitz Lindell Petrank 11]

– rate 1 UC commitment length extension

– black-box use of semi-honest OT

2 **necessity.** UC commitment length extension implies OT



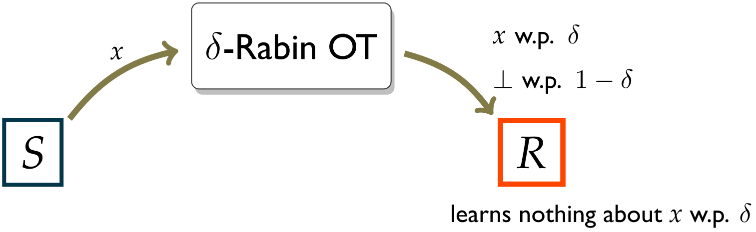
tool: oblivious transfer

tool: oblivious transfer

tool: oblivious transfer

doesn't know if R learns x

tool: oblivious transfer



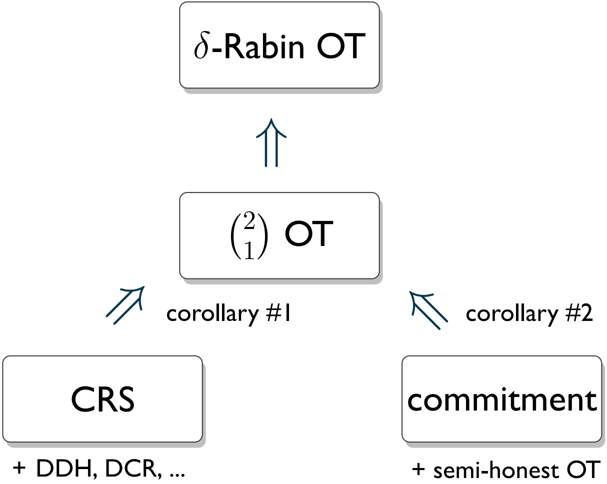
tool: oblivious transfer

δ-Rabin OT

$\Uparrow$ [Brassard Crépeau Robert 86, Ishai Prabhakaran Sahai 08]

$\binom{2}{1}$ OT $\times \log 1/\delta$

tool: oblivious transfer



1 rate one commitments

❶ rate one commitments

S R

commit $C \leftarrow \text{share}(M) \longrightarrow$ δ-Rabin OT

[Crépeau 87]

1 rate one commitments

S R

commit $C \leftarrow \mathsf{share}(M)$ → δ-Rabin OT

reveal C

1 rate one commitments

S R

commit $C \leftarrow \text{share}(M)$ → δ-Rabin OT

secret-sharing. rate $1+\delta$ over large field [Franklin Yung 92]

1 rate one commitments

S R

commit $C \leftarrow \text{share}(M) \longrightarrow$ δ-Rabin OT

secret-sharing. rate $1 + \delta$ over large field [Franklin Yung 92]

– any δ fraction are random $\Rightarrow$ hiding

1 rate one commitments

S R

commit $C \leftarrow \text{share}(M)$ → δ-Rabin OT

secret-sharing. rate $1 + \delta$ over large field [Franklin Yung 92]

– any δ fraction are random $\Rightarrow$ hiding

– distance δ $\Rightarrow$ binding

1 rate one commitments

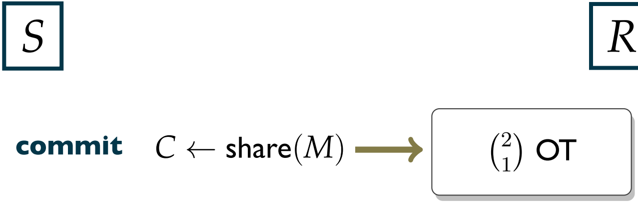
S R

commit $C \leftarrow \text{share}(M)$ ⟶ δ-Rabin OT

– communication: $(1+\delta)L$

– # OT calls: $\kappa \cdot 1/\delta$

1 rate one commitments



- communication: $(1+\delta)L + \kappa^2 \cdot 1/\delta \log 1/\delta$
- # OT calls: $\kappa \cdot 1/\delta \log 1/\delta$

2 necessity of oblivious transfer

2 necessity of key agreement

key agreement scheme.

- Alice commits to random M using Π and sends s

2 necessity of key agreement

key agreement scheme.

- Alice commits to random M using Π and sends s
- Bob gets M using commitment extractor

2 necessity of key agreement

key agreement scheme.

- Alice commits to random M using Π and sends s
- Bob gets M using commitment extractor

security against eavesdropper.

- equivocality implies $\mathsf{H}(M \mid \text{transcript}) = 2\kappa$

2 necessity of key agreement

key agreement scheme.

- Alice commits to random M using Π and sends s
- Bob gets M using commitment extractor

security against eavesdropper.

- equivocality implies $\mathsf{H}(M \mid \text{transcript}) = 2\kappa$
- $\mathsf{H}(M \mid \text{transcript}, s) \geq \kappa$

conclusion

this work. rate 1 UC commitments

- length extension for UC commitments qualitatively different from stand-alone commitments and UC OT.

conclusion

this work. rate 1 UC commitments

- length extension for UC commitments qualitatively different from stand-alone commitments and UC OT.

open problems.

- $L + \mathrm{poly}(\kappa, \log \mathrm{L})$ bits?

conclusion

this work. rate 1 UC commitments

- length extension for UC commitments qualitatively different from stand-alone commitments and UC OT.

open problems.

- $L + \mathrm{poly}(\kappa, \log \mathrm{L})$ bits?
- adaptive security?
  - non-commiting encryption extension implies OT strengthens [Lindell Zarosim 13]

conclusion

this work. rate 1 UC commitments

- length extension for UC commitments qualitatively different from stand-alone commitments and UC OT.

open problems.

- $L + \mathrm{poly}(\kappa, \log \mathrm{L})$ bits?
- adaptive security?
- rate 1 homomorphic UC commitments? (c.f. [Damgård David Giacomelli Nielsen 14])

the end