Karlsruhe Institute of Technology

Berkeley | EECS
Electrical Engineering and Computer Sciences

KASTEL

Concurrently Composable Security With Shielded Super-polynomial Simulators

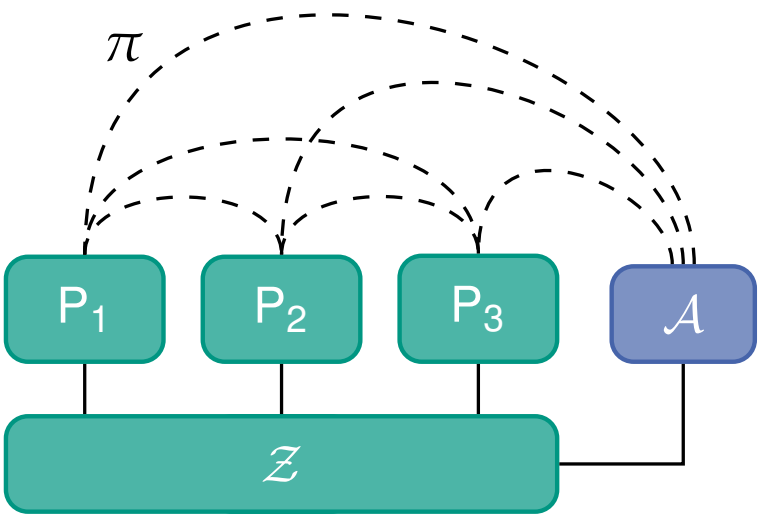
B. Broadnax, N. Döttling, G. Hartung, J. Müller-Quade, and M. Nagel

Faculty of Computer Science • Institute for Theoretical Informatics • Research Group for Cryptography and Security

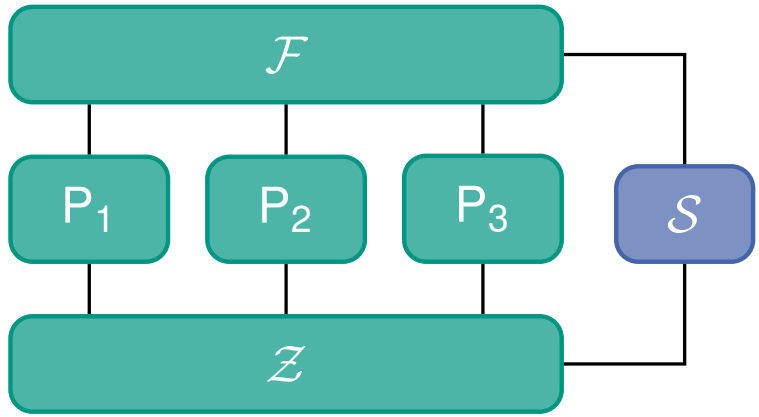
The UC Framework

A Short Introduction

- Security framework for cryptographic protocols (by [Can01])
- Follows the **simulation-based paradigm**
- Interactive distinguisher $\mathcal{Z}$ (“environment”)



Real



Ideal

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

The UC Framework

Pros and Cons

Benefits

UC is closed under general protocol **composition**:

- strong concurrent security guarantees
- modular analysis

Limitations

(e. g. [CF01; Can+02; Lin03; Kat07; LPV09; Dac+13])

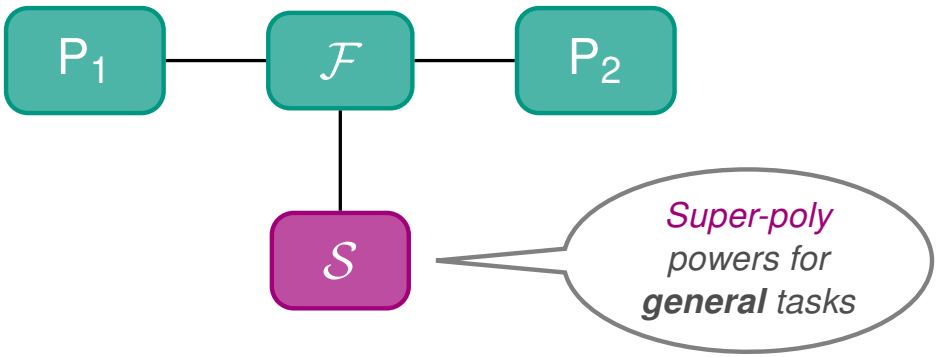
Very strong: UC **requires setup assumptions** for many cryptographic tasks

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

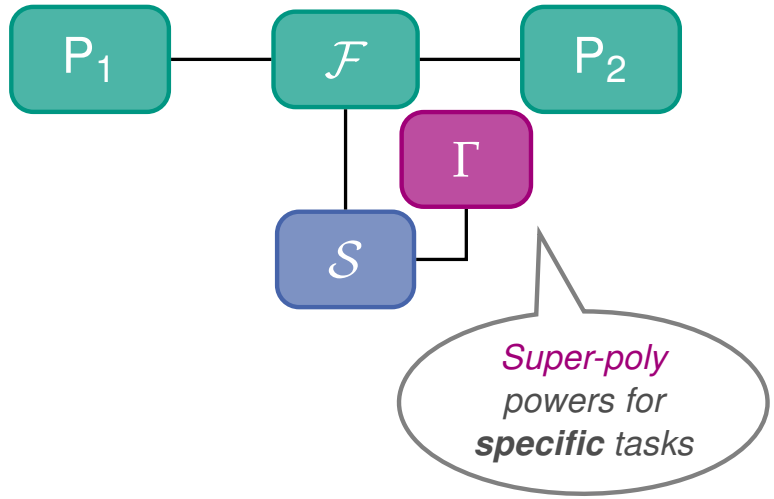
Relaxed Notions of UC Security

A Brief Overview

SPS [Pas03]



Angel-based [PS04; CLP10]

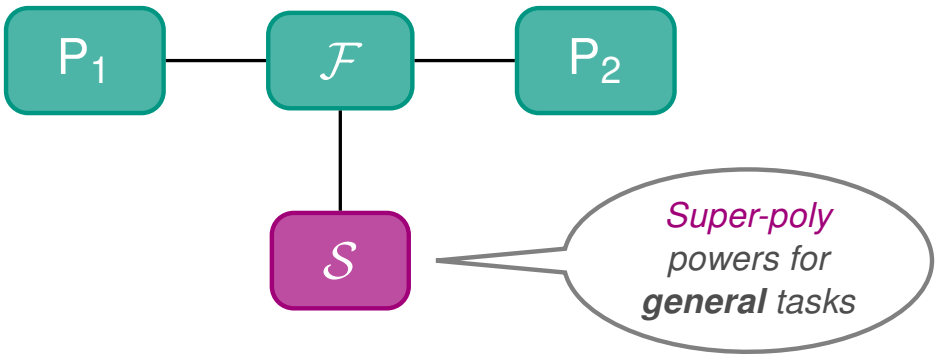


Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

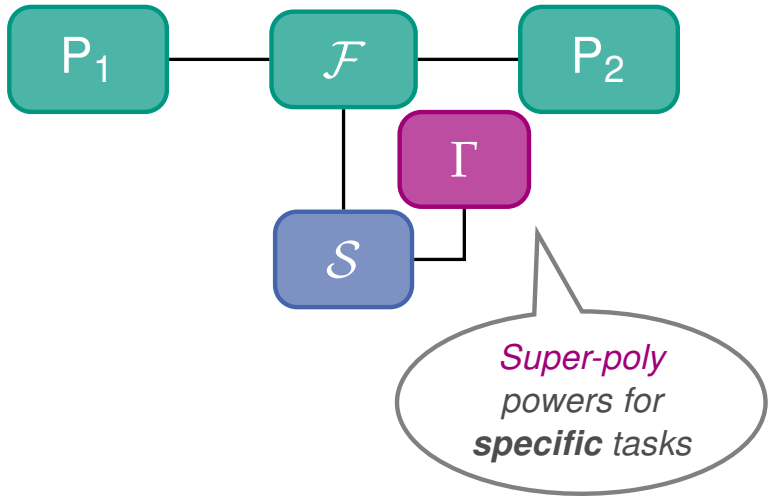
Relaxed Notions of UC Security

A Brief Overview

SPS [Pas03]



Angel-based [PS04; CLP10]



Multiple-Ideal Query Security and Input Indistinguishability

Not considered here.
See, e. g., [GJO10; Gar+12; GJ13; GGJ13; CGJ15].

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Relaxed Notions of UC Security

Pros and Cons

SPS

[Pas03; BS05; LPV09; LPV12; Gar+12]

+ Meaningful security notion for many cryptographic tasks
+ Constant-round general MPC in the plain model based on standard poly-time assumptions
– Not closed under general composition

Angel-based Security

[PS04; MMY06; CLP10; LP12; KMO14; Kiy14; Goy+15; HV16]

+ Closed under general composition (wrt. pre-chosen Angel)
+ Implies SPS security
+ General MPC in the plain model
– No known construction of general MPC protocol that is **both** constant-round and based on standard poly-time assumptions

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Our Contribution

Relaxed Security Notion

New Security Notion for Concurrently Composable Security

- Lies **strictly** between SPS and Angel-based Security
- Compatible with UC security
- Closed under general protocol composition
  - Implies concurrent security
  - Modular composition via protocols with “strong composition features”

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Our Contribution

Commitment Scheme with Strong Composition Features

Construction of a **commitment scheme** that is

- secure in our framework in the plain model
- provides strong composition features:
  1. Can be plugged into large class of UC-secure protocols
  2. Composite protocol is secure in our framework

Two **constant-round** instantiations:

- based on OWPs
- **black-box** based on homomorphic commitment schemes

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Our Contribution

Constant-round (Black-Box) General MPC in the Plain Model

Feasibility result: **General MPC** in the **plain model**

- in a **constant** number of rounds
- based on standard **poly-time** assumptions

Two constructions:

- non-black-box based on ETDPs

  → Conceptually very different alternative to [Gar+12; LPV12]

- **black-box** based on PKE with oblivious public-key generation and homomorphic commitment schemes

  → **First one**

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Our Contribution

Constant-round (Black-Box) General MPC in the Plain Model

Feasibility result

- in a **cor**
- based

Two constructi

- non-black-box base
  → Conceptually v erent alternative to [Gar+12; LPV12]
- **black-box** base PKE with oblivious public-key generation and homomorphic ommitment schemes
  → **First one**

First one that is

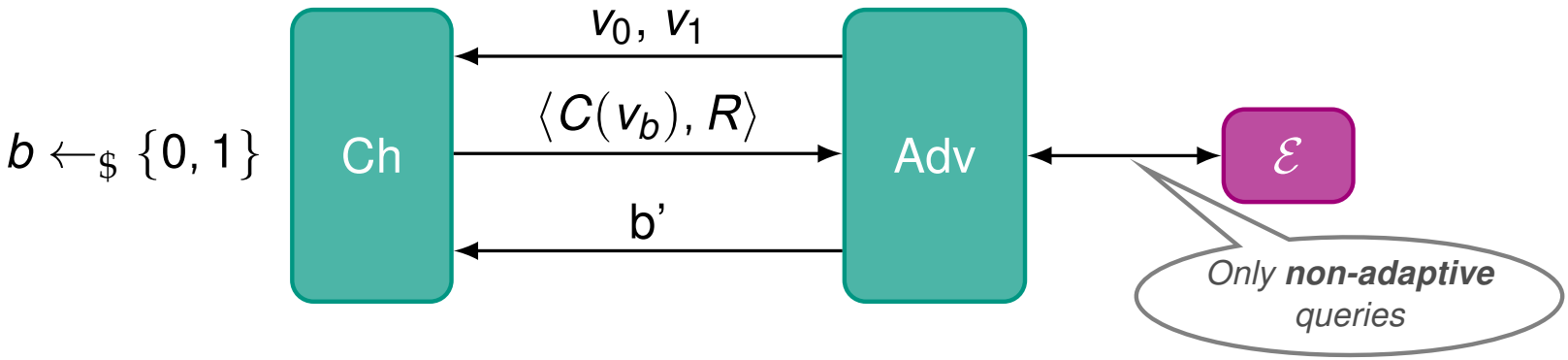
- concurrently secure in the plain model
- black-box
- constant-round
- based on standard poly-time assumptions

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Our Contribution

New Blueprint: Building on Weaker Primitives

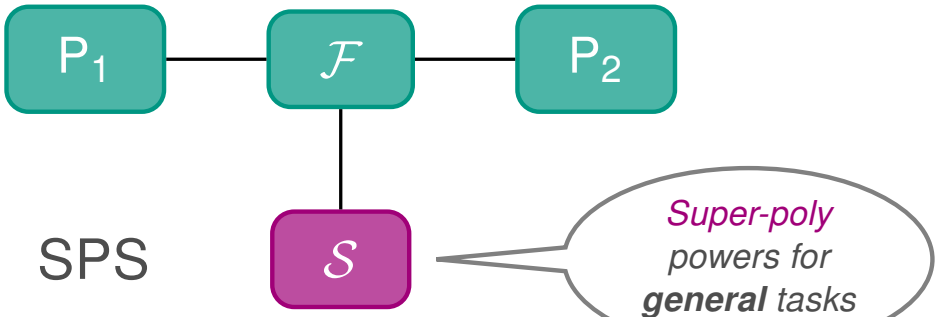
Constructions based only on **parallel CCA**-secure commitment schemes (instead of CCA-secure commitment schemes)



Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

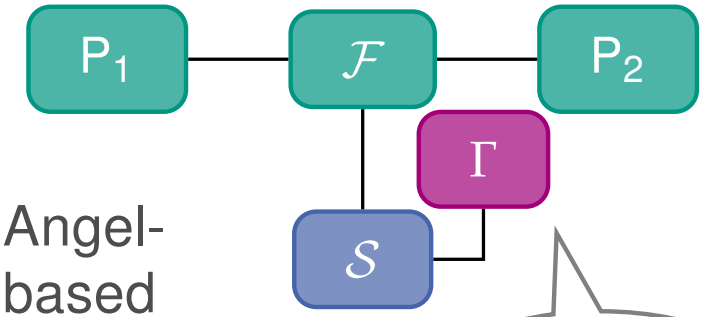
Our Approach

Shielding Away Super-Poly Resources



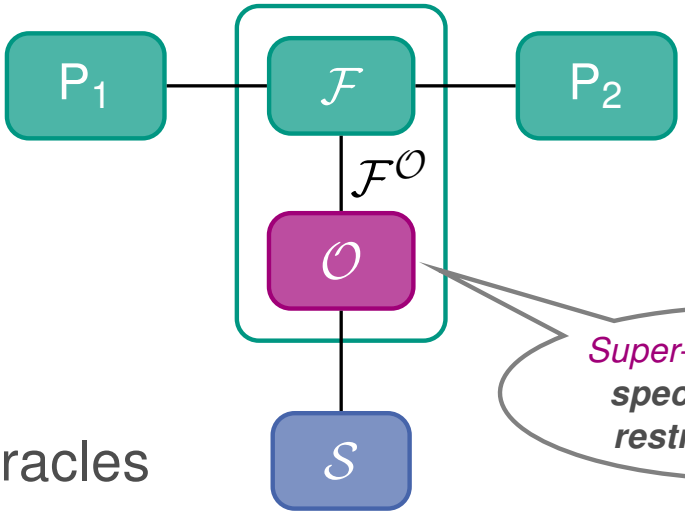
SPS

*Super-poly powers for **general** tasks*



Angel-based

*Super-poly powers for **specific** tasks*

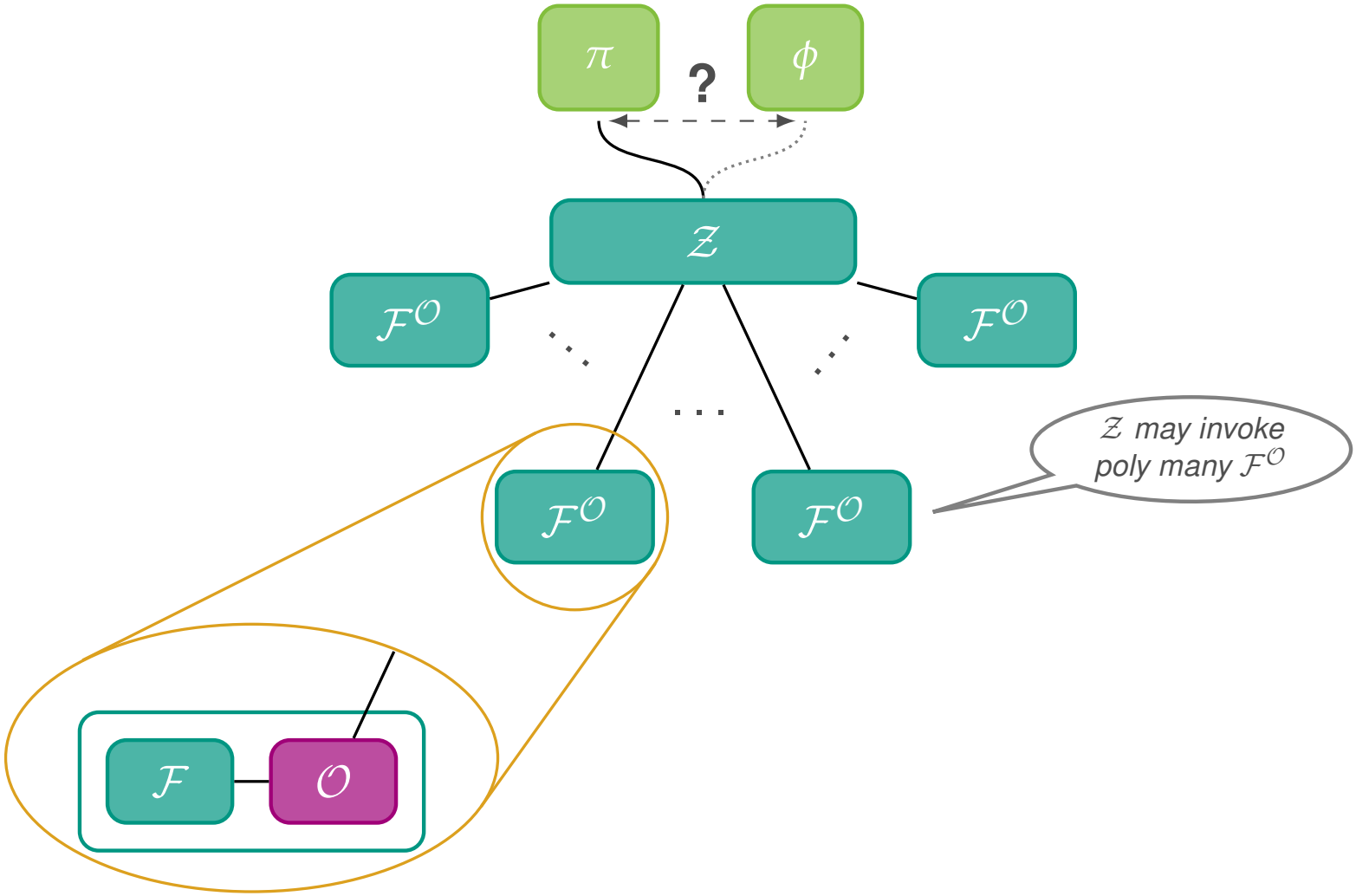


Shielded Oracles

*Super-poly powers for **specific** tasks with **restricted access***

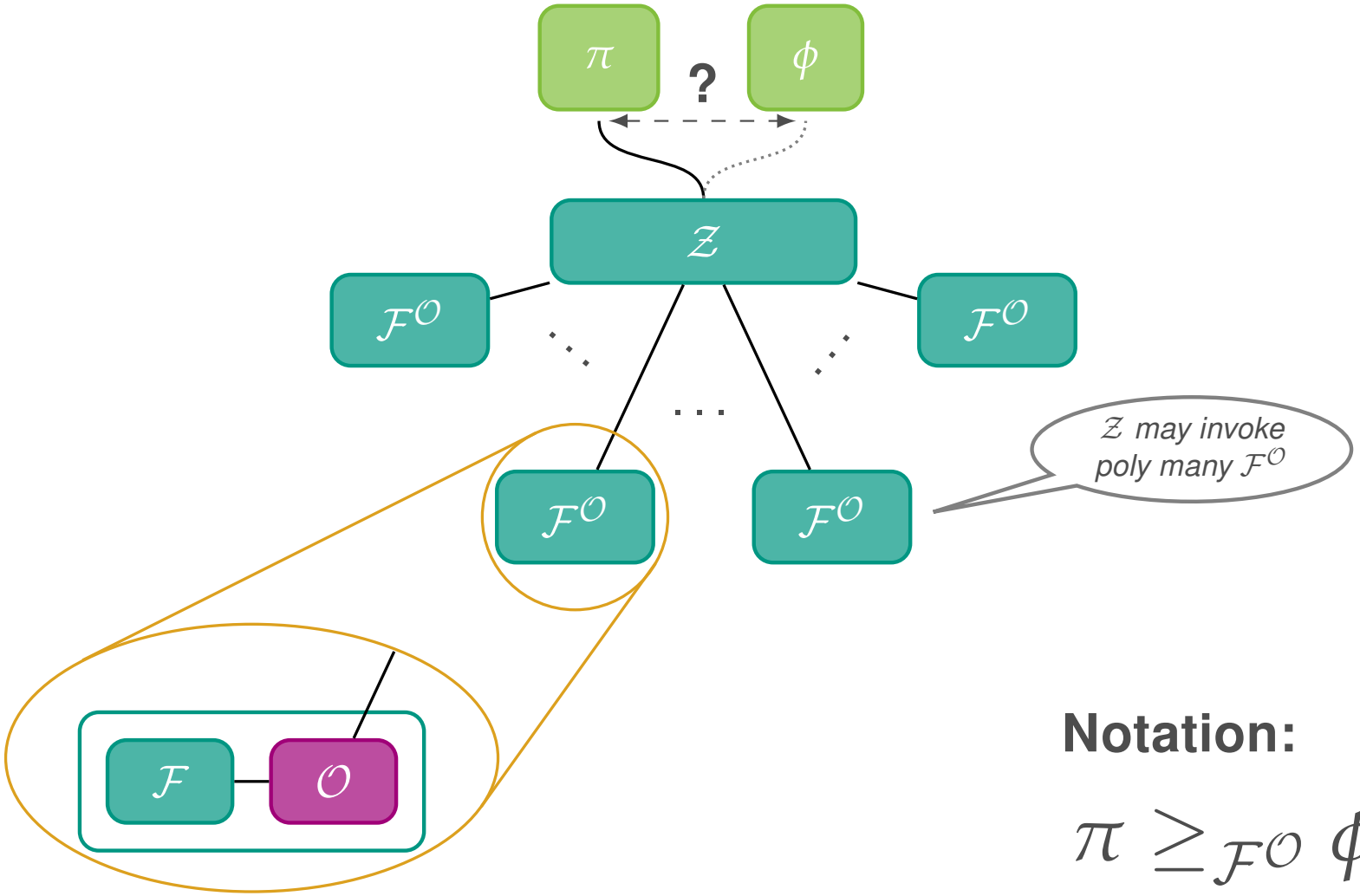
Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Augmented Environments



Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Augmented Environments



Notation:

$$\pi \geq_{\mathcal{F}^{\mathcal{O}}} \phi$$

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Composition Theorem

Augmented environments imply **composition** with protocols that may be in the $\mathcal{F}^{\mathcal{O}}$**-hybrid model**.

$$\pi \underset{\mathcal{F}^{\mathcal{O}}}{\geq} \mathcal{F}^{\mathcal{O}} \quad \Rightarrow \quad \rho^{\pi} \underset{\mathcal{F}^{\mathcal{O}}}{\geq} \rho^{\mathcal{F}^{\mathcal{O}}}$$

Composition with protocol ρ

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Polynomial Simulatability

Making $\mathcal{F}^{\mathcal{O}}$-augmented environments efficient

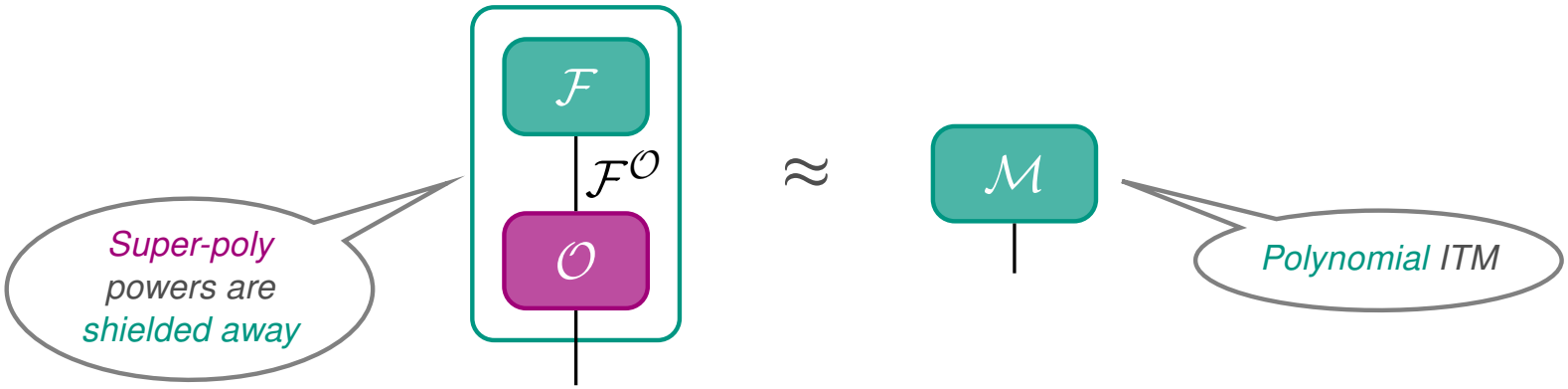
Main Technique

Replacing super-polynomial entities by polynomial ones

→ Making $\mathcal{F}^{\mathcal{O}}$-augmented environments efficient

Intuition

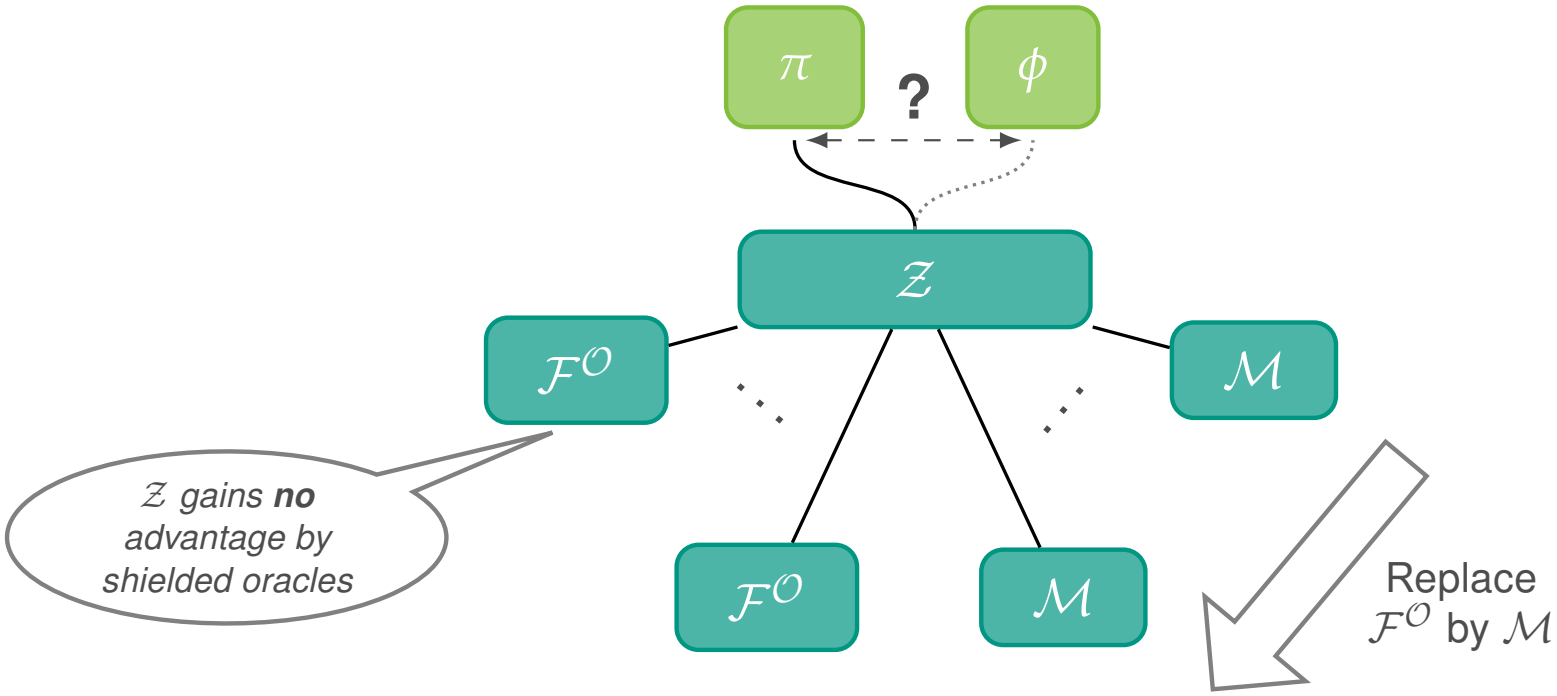
Shielded Oracles “look like poly” from the outside.



Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Polynomial Simulatability

Making $\mathcal{F}^{\mathcal{O}}$-augmented environments efficient

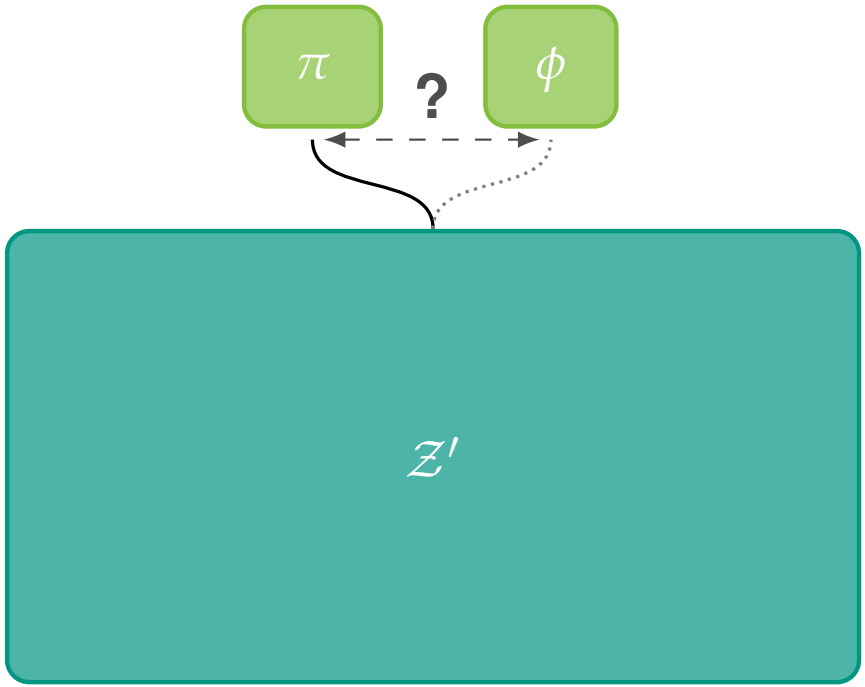


Augmented environment

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Polynomial Simulatability

Making $\mathcal{F}^{\mathcal{O}}$-augmented environments efficient



Standard poly-time UC environment

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Secure Commitment Scheme

Goal

Construct a protocol Π such that

$$\Pi \underset{\mathcal{F}_{\text{com}}^{\mathcal{O}}}{\geq} \mathcal{F}_{\text{com}}^{\mathcal{O}}$$

for a suitable $\mathcal{O}$.

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Secure Commitment Scheme

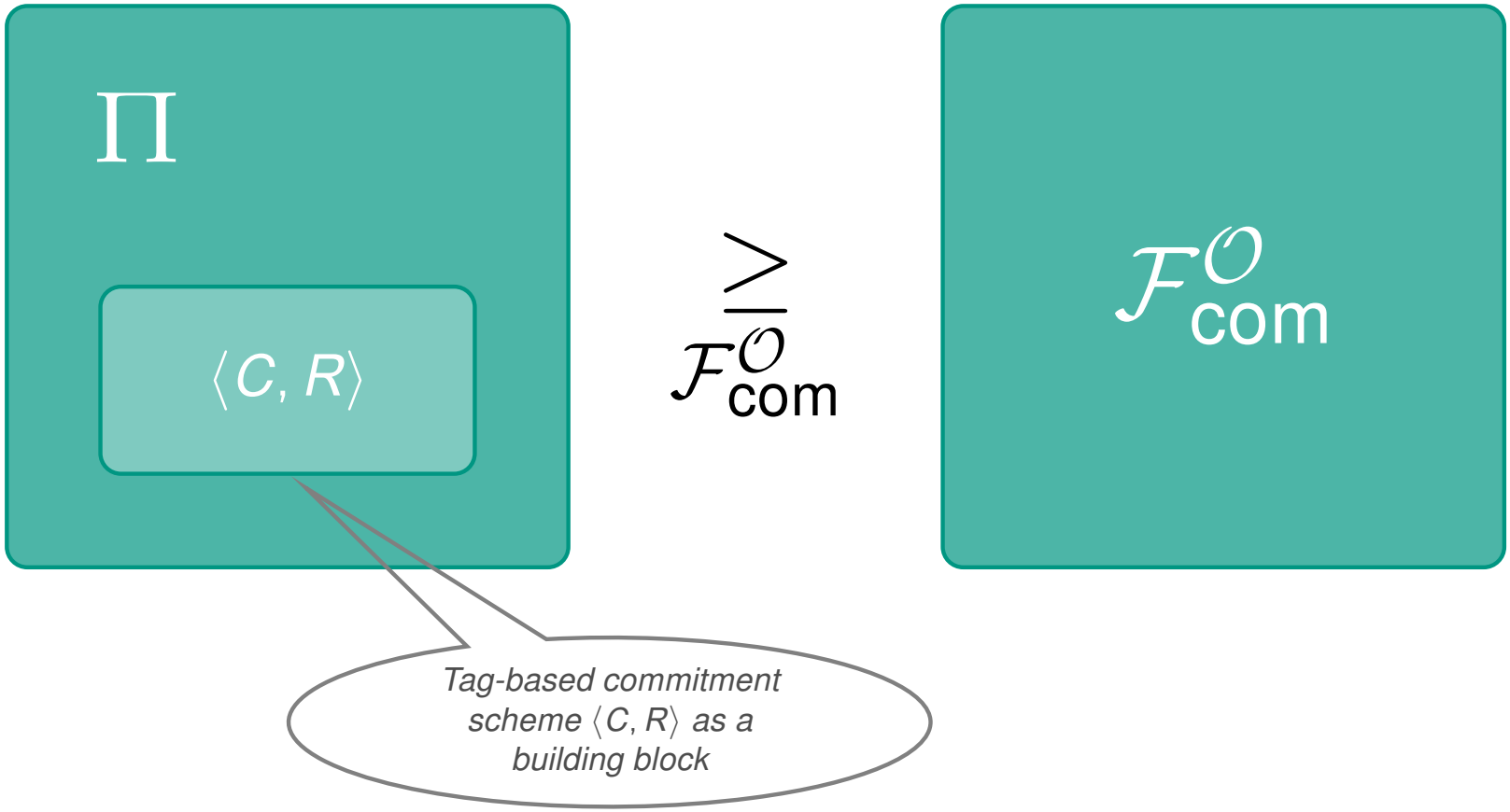
Necessary Prerequisites for Π

- Hiding can be broken with super-poly powers (extractability)
- Binding can be broken with super-poly powers (equivocality)

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Secure Commitment Scheme

The Big Picture

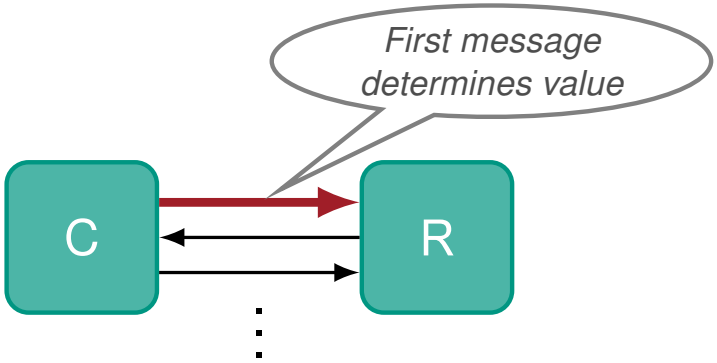


Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

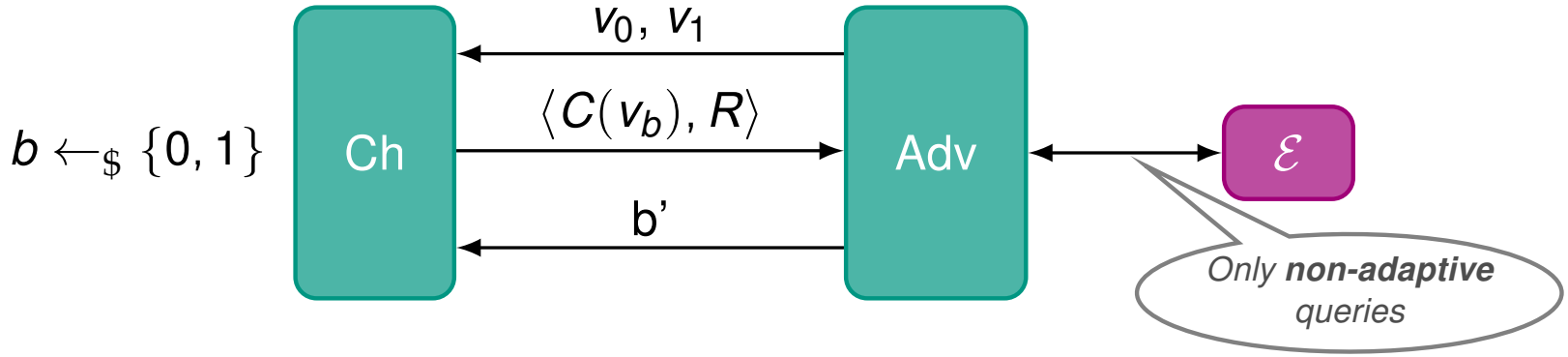
Secure Commitment Scheme

Building Block – Tag-based Commitment Scheme $\langle C, R \rangle$

- **Immediately Committing**
  → super-poly extractable



- **Parallel-CCA secure**



Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Secure Commitment Scheme

The Scheme Π

Extractability (in super-poly time)

. . . follows from the extractability of $\langle C, R \rangle$.

Equivocality (in super-poly time)

. . . using the transformation of [DS13]:

Receiver of Π commits to equivocation trapdoor at the beginning.

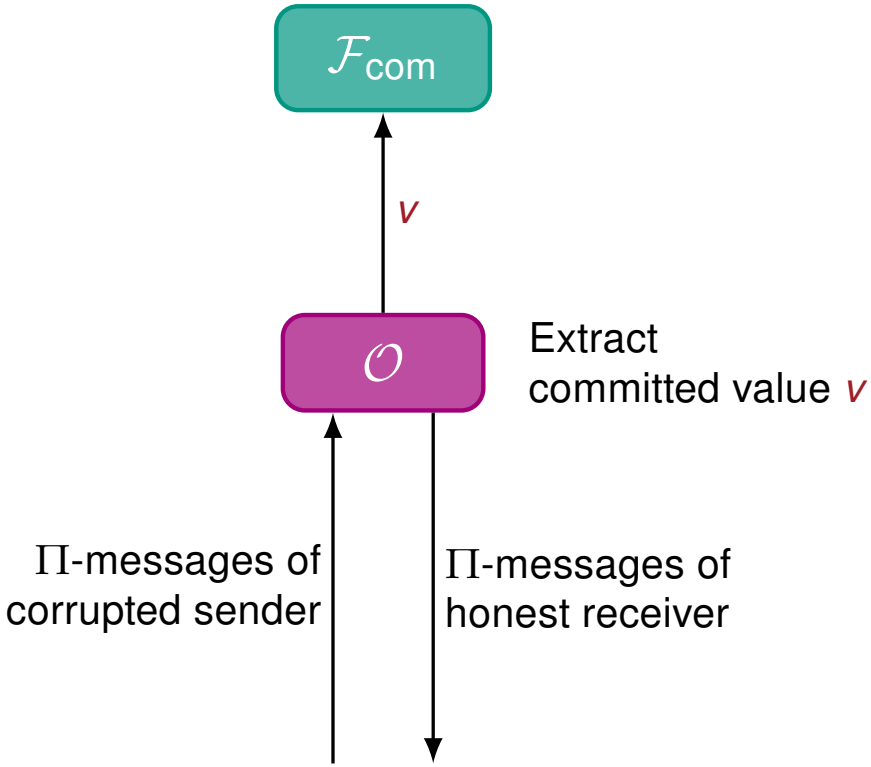
Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Secure Commitment Scheme

Definition of the Shielded Oracle $\mathcal{O}$

Corrupted Sender

$\mathcal{O}$ plays role of honest receiver



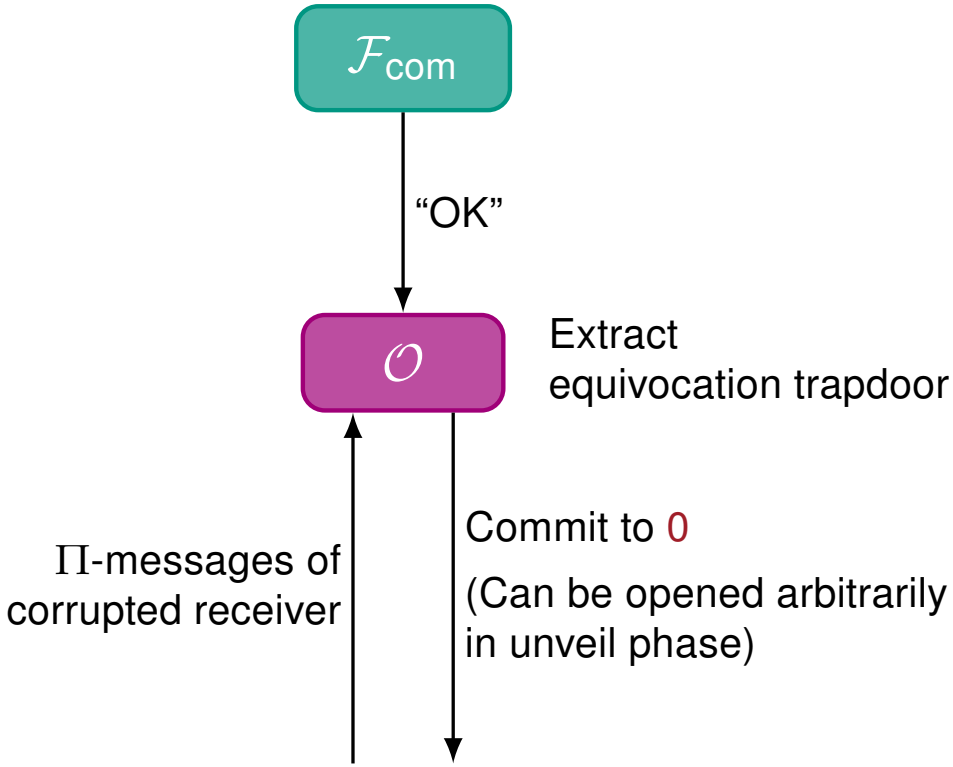
Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Secure Commitment Scheme

Definition of the Shielded Oracle $\mathcal{O}$

Corrupted Receiver

$\mathcal{O}$ plays role of sender



Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Secure Commitment Scheme

Security Statement

Theorem

If $\langle C, R \rangle$ is immediately committing and parallel-CCA-secure, then

$$\Pi \underset{\mathcal{F}_{\mathsf{com}}^{\mathcal{O}}}{\geq} \mathcal{F}_{\mathsf{com}}^{\mathcal{O}}$$

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

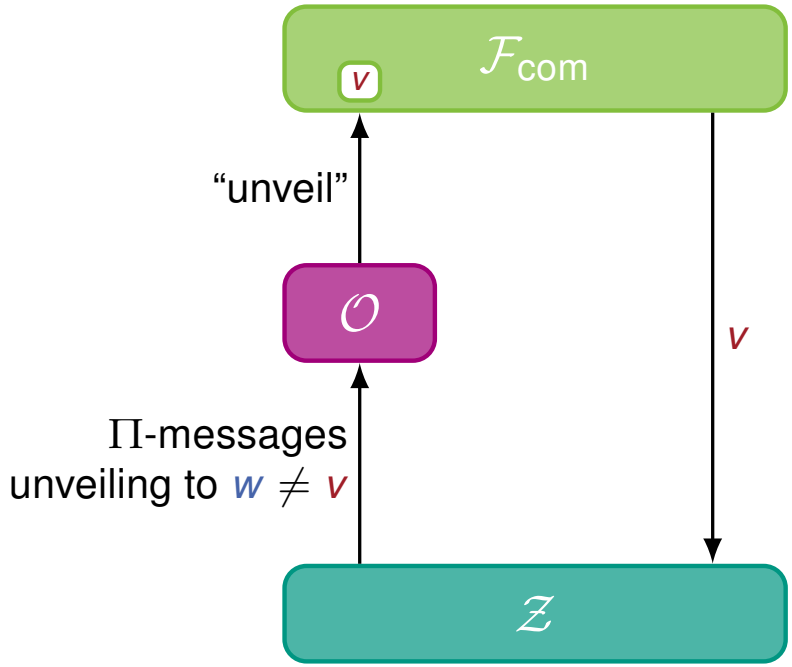
Secure Commitment Scheme

Proof Idea – Discrepancy

Let the **sender** be corrupted.

- Environment commits to value v but unveils different value w
- Output of receiver in real model: w
- Output of receiver in ideal model: v (value extracted by $\mathcal{O}$)

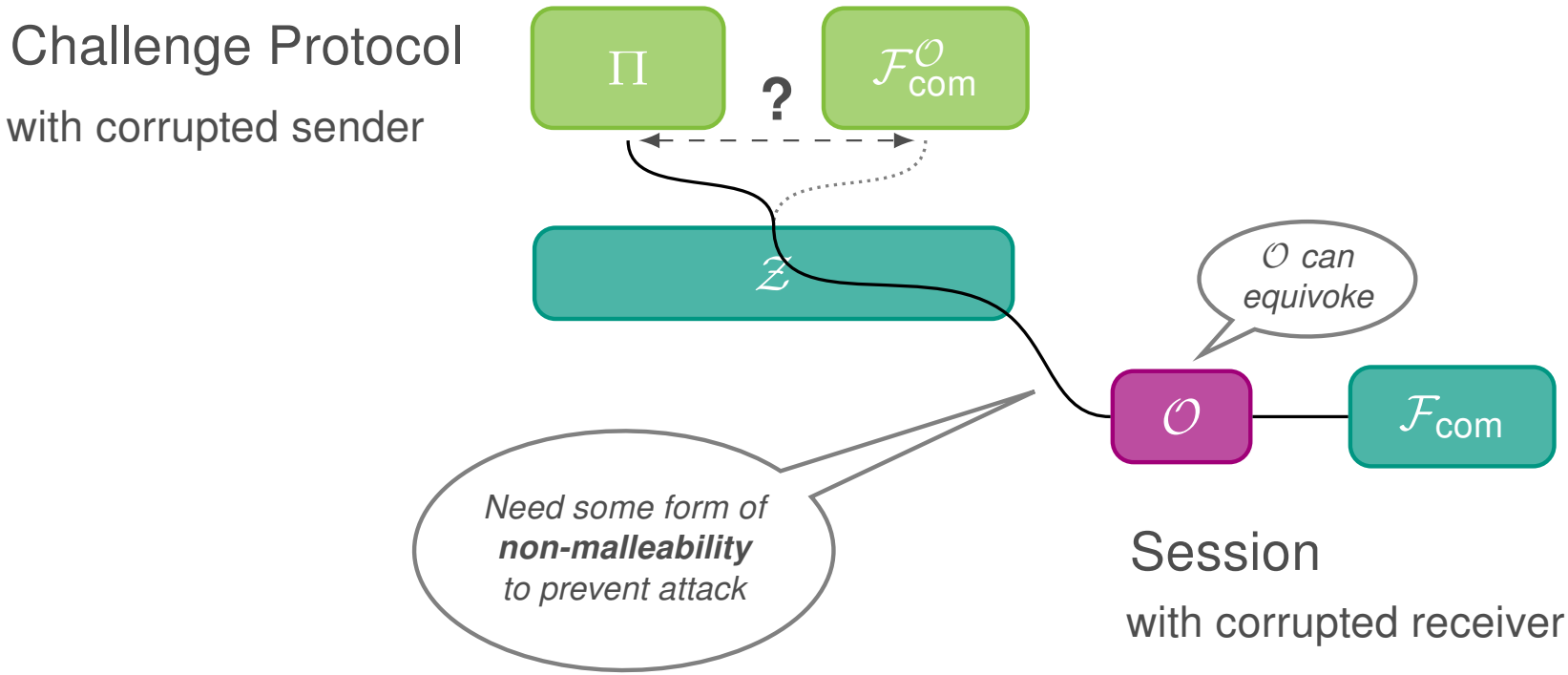
$\rightarrow$ Environment can distinguish



Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Secure Commitment Scheme

Proof Idea – A Possible Attack Strategy



Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Secure Commitment Scheme

Proof Idea

To show

$\mathcal{Z}$ cannot cause a discrepancy (except with negligible probability)

Proof by contradiction

Assume $\mathcal{F}_{\text{com}}^{\mathcal{O}}$-augmented environment can cause a discrepancy:

- Make environment efficient

  (interacting with only one $\mathcal{F}_{\text{com}}^{\mathcal{O}}$-session with a corrupted sender)
- Proof that no efficient environment can cause a discrepancy

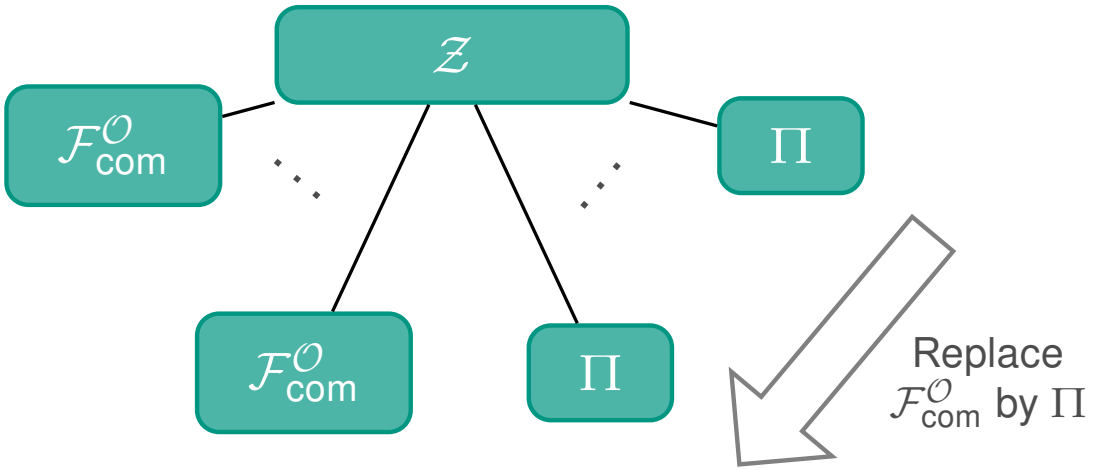
Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

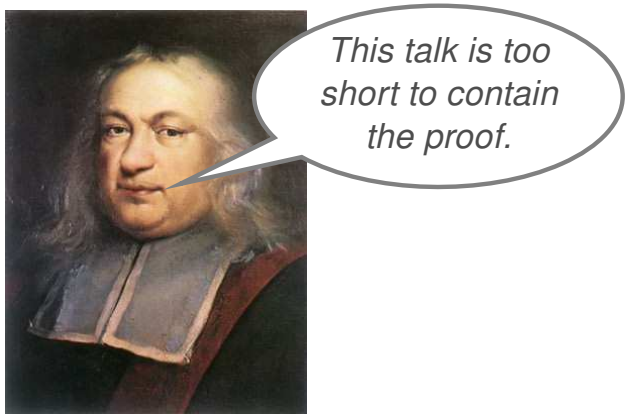
Secure Commitment Scheme

Making the Environment Efficient

"Carefully" replace $\mathcal{F}_{\text{com}}^{\mathcal{O}}$-sessions with the real protocol Π in a specific order

→ Non-uniform reduction to parallel-CCA-security of $\langle C, R \rangle$





Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

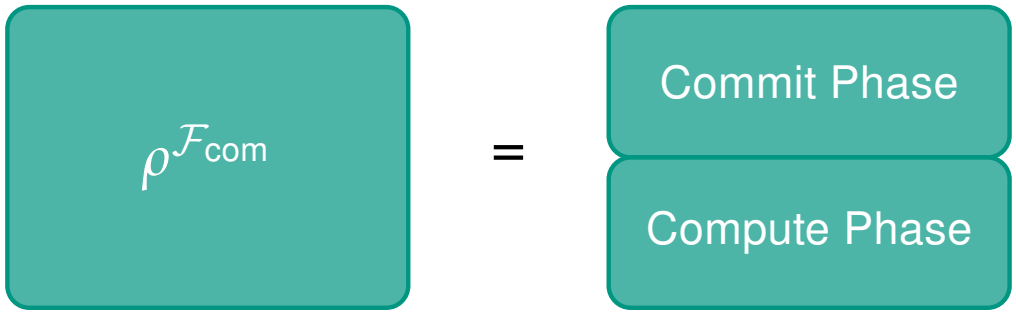
Modular Composition Theorem for Π

Composing with constant-round UC-secure protocols

If $\langle C, R \rangle$ has additional property ("*r*-non-adaptively robust")

as well as

$\rho^{\mathcal{F}_{\text{com}}}$ constant-round and



then

$$\rho^{\mathcal{F}_{\text{com}}} \underset{\text{UC}}{\geq} \mathcal{G} \quad \Rightarrow \quad \exists \text{ shielded oracle } \mathcal{O}' : \rho^{\Pi} \underset{\mathcal{G}^{\mathcal{O}'}}{\geq} \mathcal{G}^{\mathcal{O}'}$$

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Modular Composition Theorem for Π

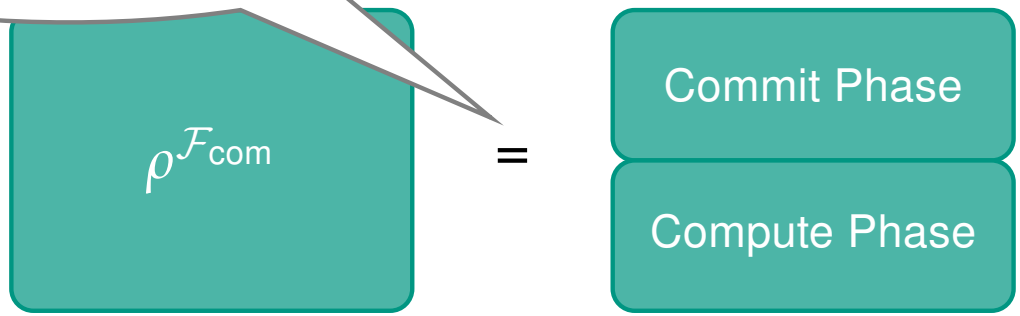
Composing with constant-round UC-secure protocols

If $\langle C, R \rangle$ has additi st")

as well as

$\rho^{\mathcal{F}_{\text{com}}}$ constant-round and

Any (poly-round) protocol can be **compiled** into one obeying this structure



then

$$\rho^{\mathcal{F}_{\text{com}}} \underset{\text{UC}}{\geq} \mathcal{G} \quad \Rightarrow \quad \exists \text{ shielded oracle } \mathcal{O}' : \rho^{\Pi} \underset{\mathcal{G}^{\mathcal{O}'}}{\geq} \mathcal{G}^{\mathcal{O}'}$$

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Secure Commitment Scheme

Constant-round Instantiations of Π

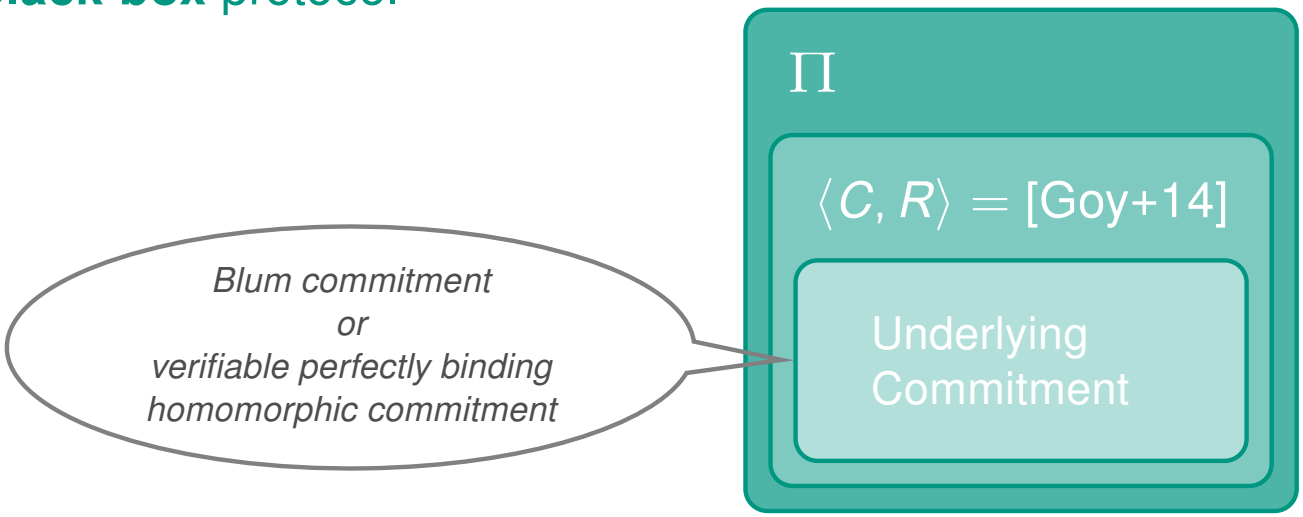
$\langle C, R \rangle$ can be instantiated with a modified version of the 8-round protocol in [Goy+14] . . .

- . . . using OWPs

  → Constant-round protocol based on OWPs.

- . . . using a verifiable perfectly binding homomorphic commitment scheme

  → Constant-round **black-box** protocol



Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Modular Composition Theorem for Π

Constant-round Instantiations of Π

Constant-round Instantiations of Π

- Π_r = instantiation of Π based on OWPs
- Π_r^{BB} = black-box instantiation of Π based on verifiable perfectly binding homomorphic commitment schemes

(Instantiated with a *r*-non-adaptively robust modified version of [Goy+14])

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Constant-round (Black-box) General MPC

UC-secure Protocol

Secure in Our Framework (in the Plain Model)

$$\rho^{\mathcal{F}_{\text{com}}} + \Pi_r \Longrightarrow \rho^{\Pi_r}$$

[Can+02; IPS08]

Constant-round, based on ETDPs

Constant-round, based on ETDPs

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Constant-round (Black-box) General MPC

UC-secure Protocol				Secure in Our Framework (in the Plain Model)
$\rho^{\mathcal{F}_{\text{com}}}$	$+$	Π_r	$\Rightarrow$	ρ^{Π_r}
[Can+02; IPS08]				
Constant-round, based on ETDPs				Constant-round, based on ETDPs
$\rho^{\mathcal{F}_{\text{com}}}$	$+$	Π_r^{BB}	$\Rightarrow$	$\rho^{\Pi_r^{\text{BB}}}$
[HV15]				
Constant-round, black-box, based on PKE with oblivious public-key generation				Constant-round, black-box, based on cryptographic primitives with polynomial hardness

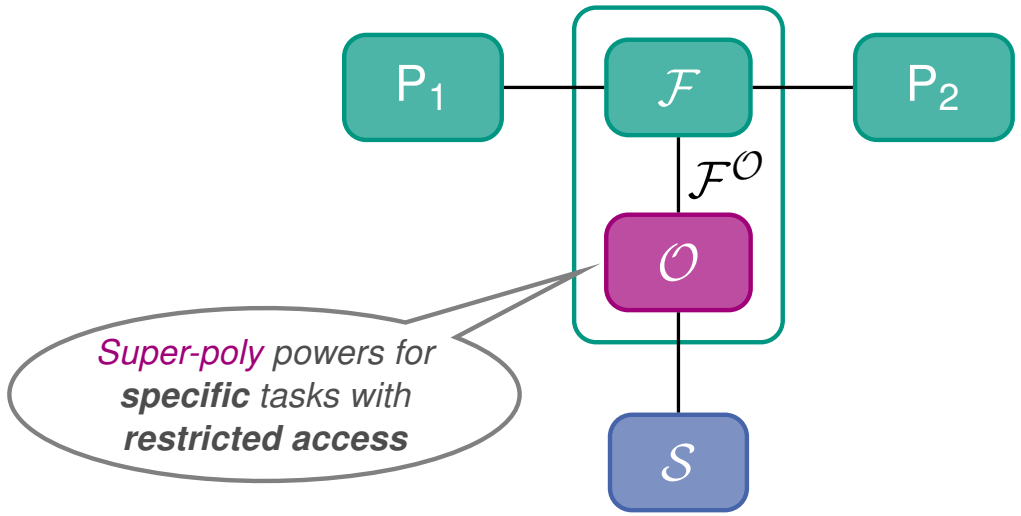
Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

The End

Take Away Messages

- New universally composable security framework
- Secure commitment scheme with modular composition property
- Constant-round black-box general MPC based on standard assumptions
- All results based only on parallel-CCA-secure commitments

Thank You



Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Bibliography

[BS05] Boaz Barak and Amit Sahai. “How to play almost any mental game over the net – concurrent composition via super-polynomial simulation.” In: *46st Annual IEEE Symposium on Foundations of Computer Science*. FOCS ’05. IEEE. 2005, pp. 543–552.

[Can+02] Ran Canetti et al. “Universally Composable Two-party and Multi-party Secure Computation.” In: *Proceedings of the 34th Annual ACM Symposium on Theory of Computing*. STOC ’02. ACM, 2002, pp. 494–503.

[Can01] Ran Canetti. “Universally Composable Security: A New Paradigm for Cryptographic Protocols.” In: *42th Annual IEEE Symposium on Foundations of Computer Science*. FOCS ’01. IEEE. 2001, pp. 136–145.

[CF01] Ran Canetti and Marc Fischlin. “Universally composable commitments.” In: *Advances in Cryptology – CRYPTO 2001: 21st Annual International Cryptology Conference, Proceedings*. Springer, 2001, pp. 19–40.

Bibliography (cont.)

[CGJ15] Ran Canetti, Vipul Goyal, and Abhishek Jain. "Concurrent Secure Computation with Optimal Query Complexity." In: *Advances in Cryptology – CRYPTO 2015: 35th Annual Cryptology Conference, Proceedings*. Springer, 2015, pp. 43–62.

[CLP10] Ran Canetti, Huijia Lin, and Rafael Pass. "Adaptive hardness and composable security in the plain model from standard assumptions." In: *51st Annual IEEE Symposium on Foundations of Computer Science*. FOCS '10. IEEE. 2010, pp. 541–550.

[Dac+13] Dana Dachman-Soled et al. "Adaptive and Concurrent Secure Computation from New Adaptive, Non-malleable Commitments." In: *Advances in Cryptology – ASIACRYPT 2013: 19th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings*. Springer, 2013, pp. 316–336.

Bibliography (cont.)

[DS13] Ivan Damgård and Alessandra Scafuro. "Unconditionally secure and universally composable commitments from physical assumptions." In: *Advances in Cryptology – ASIACRYPT 2013: 19th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings*. Springer, 2013, pp. 100–119.

[Gar+12] Sanjam Garg et al. "Concurrently Secure Computation in Constant Rounds." In: *Advances in Cryptology – EUROCRYPT 2012: 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings*. Springer, 2012, pp. 99–116.

[GGJ13] Vipul Goyal, Divya Gupta, and Abhishek Jain. "What Information Is Leaked under Concurrent Composition?" In: *Advances in Cryptology – CRYPTO 2013: 33rd Annual Cryptology Conference, Proceedings*. Springer, 2013, pp. 220–238.

Bibliography (cont.)

[GJ13] Vipul Goyal and Abhishek Jain. "On Concurrently Secure Computation in the Multiple Ideal Query Model." In: *Advances in Cryptology – EUROCRYPT 2013: 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings*. Springer, 2013, pp. 684–701.

[GJO10] Vipul Goyal, Abhishek Jain, and Rafail Ostrovsky. "Password-Authenticated Session-Key Generation on the Internet in the Plain Model." In: *Advances in Cryptology – CRYPTO 2010: 30th Annual Cryptology Conference, Proceedings*. Springer, 2010, pp. 277–294.

[Goy+14] Vipul Goyal et al. "An Algebraic Approach to Non-malleability." In: *55th Annual IEEE Symposium on Foundations of Computer Science*. FOCS '14. IEEE. 2014, pp. 41–50.

Bibliography (cont.)

[Goy+15] Vipul Goyal et al. “Round-Efficient Concurrently Composable Secure Computation via a Robust Extraction Lemma.” In: *Theory of Cryptography: 12th Theory of Cryptography Conference, TCC 2015, Proceedings*. Springer, 2015, pp. 260–289.

[HV15] Carmit Hazay and Muthuramakrishnan Venkitasubramaniam. “On Black-Box Complexity of Universally Composable Security in the CRS Model.” In: *Advances in Cryptology – ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Proceedings, Part II*. Springer, 2015, pp. 183–209.

[HV16] Carmit Hazay and Muthuramakrishnan Venkitasubramaniam. “Composable Adaptive Secure Protocols without Setup under Polytime Assumptions.” In: *Theory of Cryptography: 14th Theory of Cryptography Conference, TCC 2016-B, Proceedings*. Printed version not yet published. 2016.

Bibliography (cont.)

[IPS08] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. "Founding Cryptography on Oblivious Transfer – Efficiently." In: *Advances in Cryptology – CRYPTO 2008: 28th Annual International Cryptology Conference, Proceedings*. Springer, 2008, pp. 572–591.

[Kat07] Jonathan Katz. "Universally Composable Multi-party Computation Using Tamper-Proof Hardware." In: *Advances in Cryptology – EUROCRYPT 2007: 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings*. Springer, 2007, pp. 115–128.

[Kiy14] Susumu Kiyoshima. "Round-Efficient Black-Box Construction of Composable Multi-Party Computation." In: *Advances in Cryptology – CRYPTO 2014: 34th Annual Cryptology Conference, Proceedings*. Springer, 2014, pp. 351–368.

Bibliography (cont.)

[KMO14] Susumu Kiyoshima, Yoshifumi Manabe, and Tatsuaki Okamoto. "Constant-Round Black-Box Construction of Composable Multi-Party Computation Protocol." In: *Theory of Cryptography: 11th Theory of Cryptography Conference, TCC 2014, Proceedings*. Springer, 2014, pp. 343–367.

[Lin03] Yehuda Lindell. "General Composition and Universal Composability in Secure Multi-party Computation." In: *44th Annual IEEE Symposium on Foundations of Computer Science*. FOCS '03. IEEE. 2003, pp. 394–403.

[LP12] Huijia Lin and Rafael Pass. "Black-Box Constructions of Composable Protocols without Set-Up." In: *Advances in Cryptology – CRYPTO 2012: 32nd Annual Cryptology Conference, Proceedings*. Springer, 2012, pp. 461–478.

Bibliography (cont.)

[LPV09] Huijia Lin, Rafael Pass, and Muthuramakrishnan Venkitasubramaniam. "A Unified Framework for Concurrent Security: Universal Composability from Stand-alone Non-malleability." In: *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*. STOC '09. ACM, 2009, pp. 179–188.

[LPV12] Huijia Lin, Rafael Pass, and Muthuramakrishnan Venkitasubramaniam. "A Unified Framework for UC from Only OT." In: *Advances in Cryptology – ASIACRYPT 2012: 18th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings*. Springer, 2012, pp. 699–717.

[MMY06] Tal Malkin, Ryan Moriarty, and Nikolai Yakovenko. "Generalized Environmental Security from Number Theoretic Assumptions." In: *Theory of Cryptography: 3rd Theory of Cryptography Conference, TCC 2006, Proceedings*. Springer, 2006, pp. 343–359.

Bibliography (cont.)

[Pas03] Rafael Pass. “Simulation in Quasi-Polynomial Time, and Its Application to Protocol Composition.” In: *Advances in Cryptology – EUROCRYPT 2003: 22nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Proceedings*. Springer, 2003, pp. 160–176.

[PS04] Manoj Prabhakaran and Amit Sahai. “New Notions of Security: Achieving Universal Composability Without Trusted Setup.” In: *Proceedings of the 36th Annual ACM Symposium on Theory of Computing*. STOC ’04. ACM, 2004, pp. 242–251.

Karlsruhe Institute of Technology

Appendix

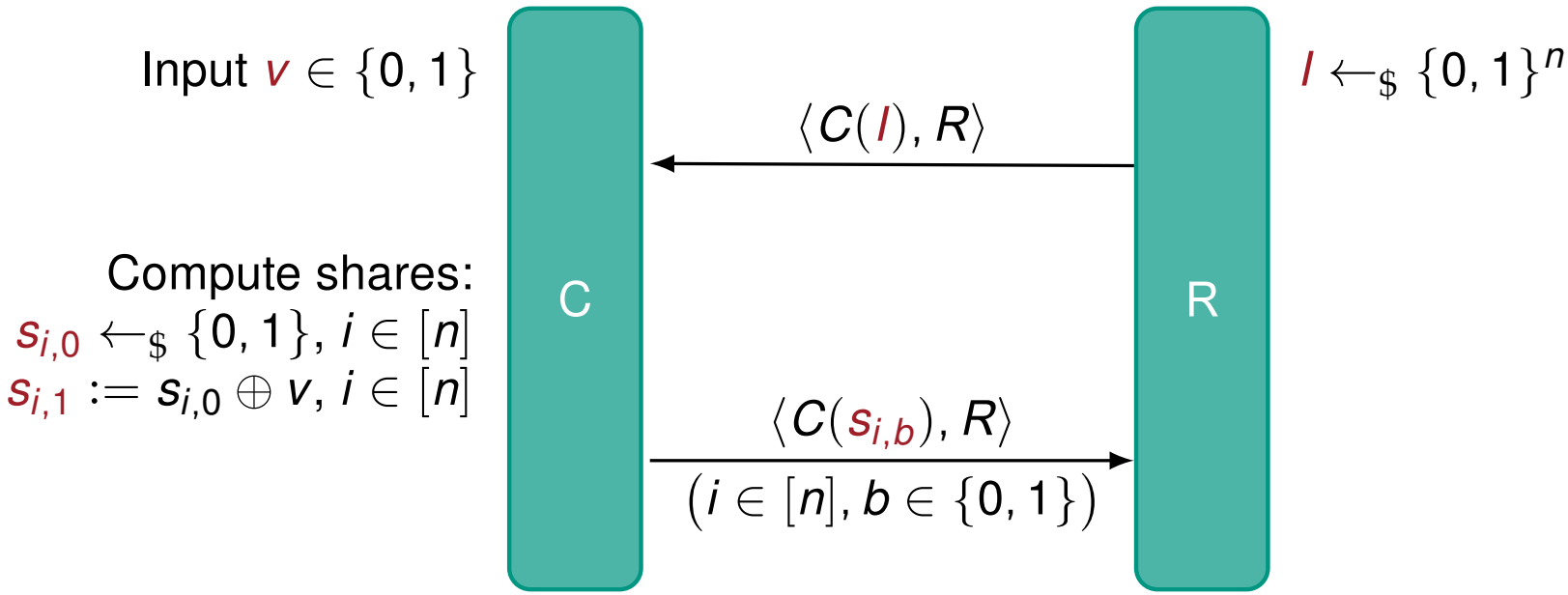
Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

KASTEL

Constant-round Commitment Scheme

The Scheme Π (Reminiscent of [DS13])

Commit Phase

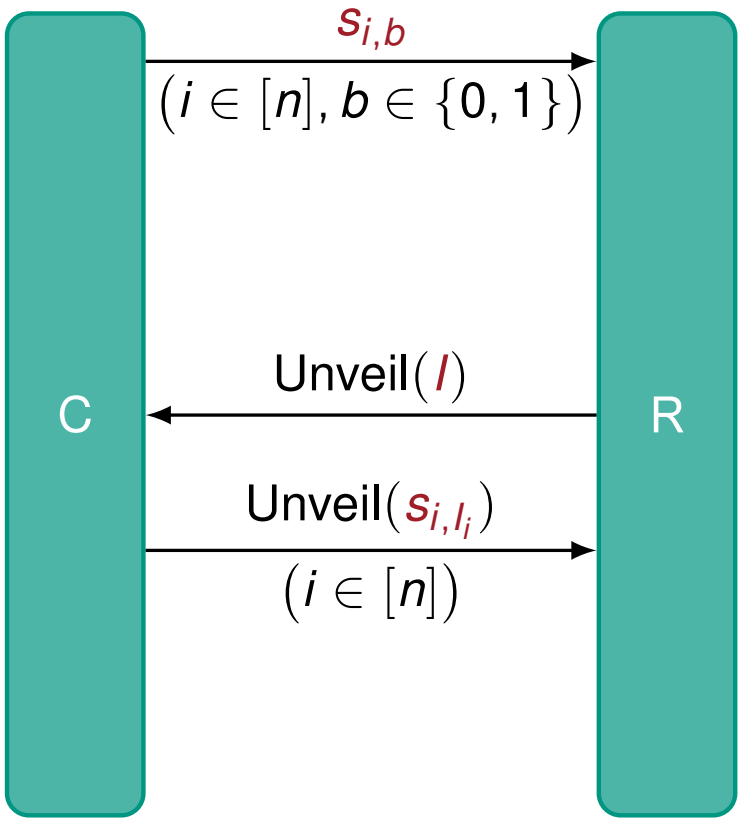


Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Constant-round Commitment Scheme

The Scheme Π

Unveil Phase



Check
$s_{1,0} \oplus s_{1,1} = \ldots = s_{n,0} \oplus s_{n,1}$,
else abort

If unveil valid, output
$w = s_{1,0} \oplus s_{1,1}$

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Constant-round Commitment Scheme

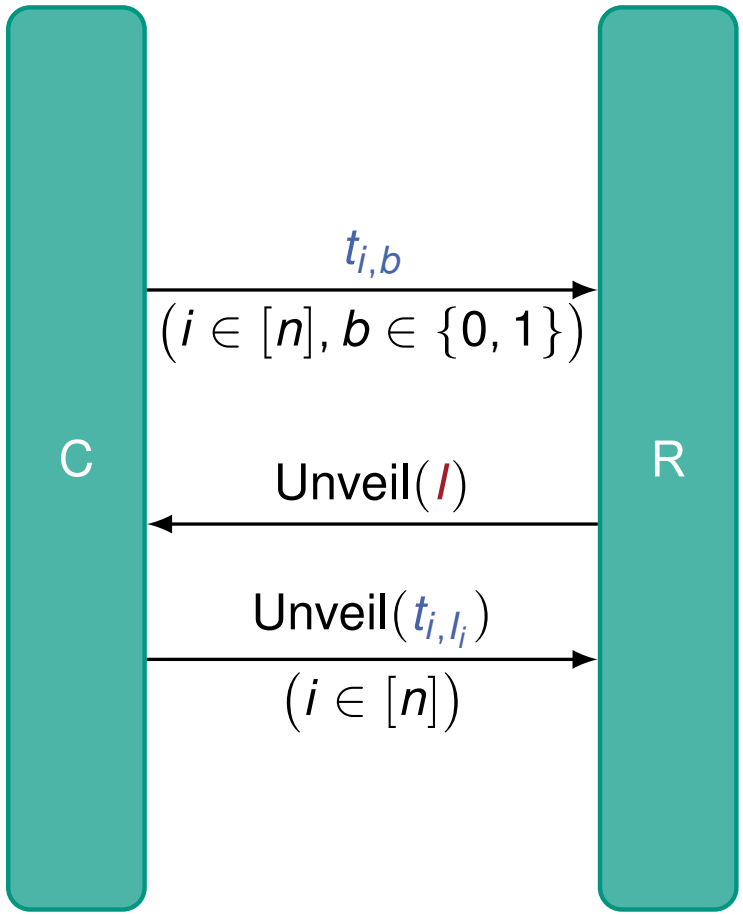
The Scheme Π

Equivocation Trapdoor Index set I serves as trapdoor

Compute "fake shares":

$t_{i,I_i} := s_{i,I_i}, i \in [n]$

$t_{i,\neg I_i} := s_{i,\neg I_i} \oplus 1, i \in [n]$



Check ...

If unveil valid, output

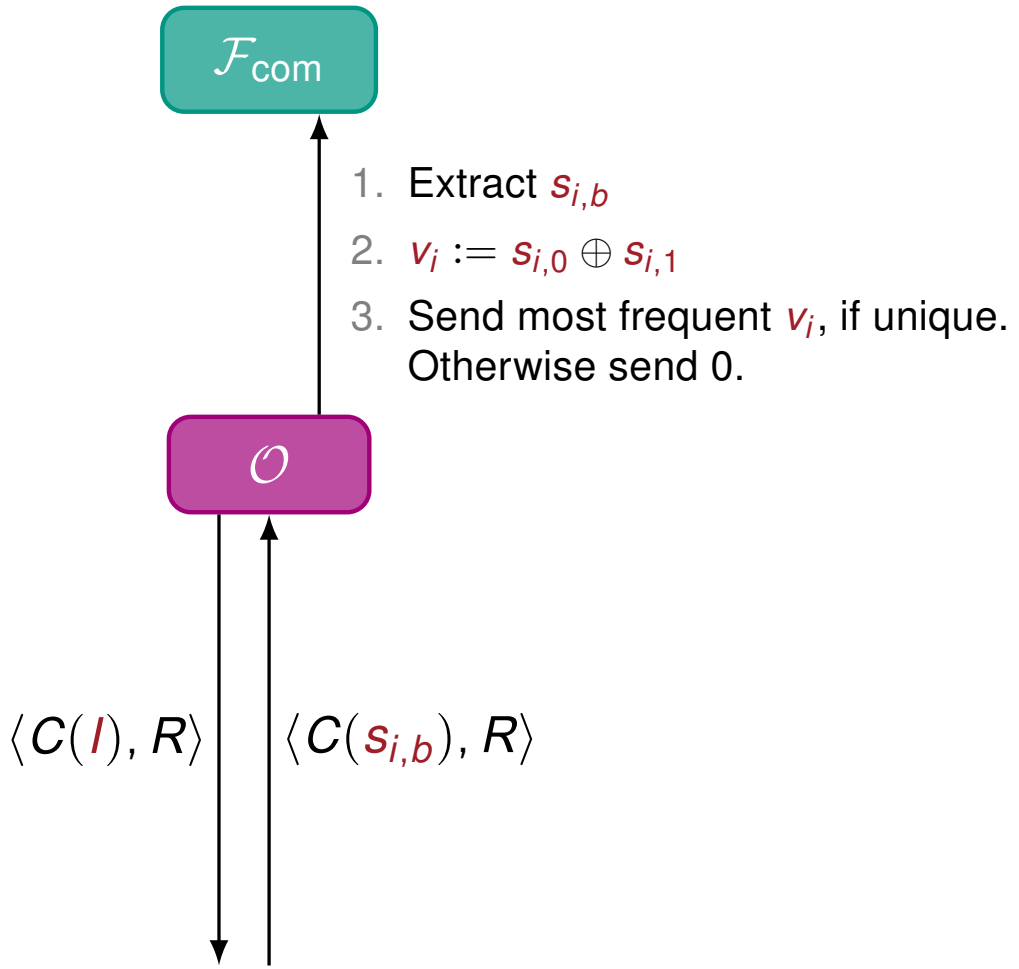
$w = t_{1,0} \oplus t_{1,1} = v \oplus 1$

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Constant-round Commitment Scheme

Definition of the Shielded Oracle $\mathcal{O}$

Corrupted Sender

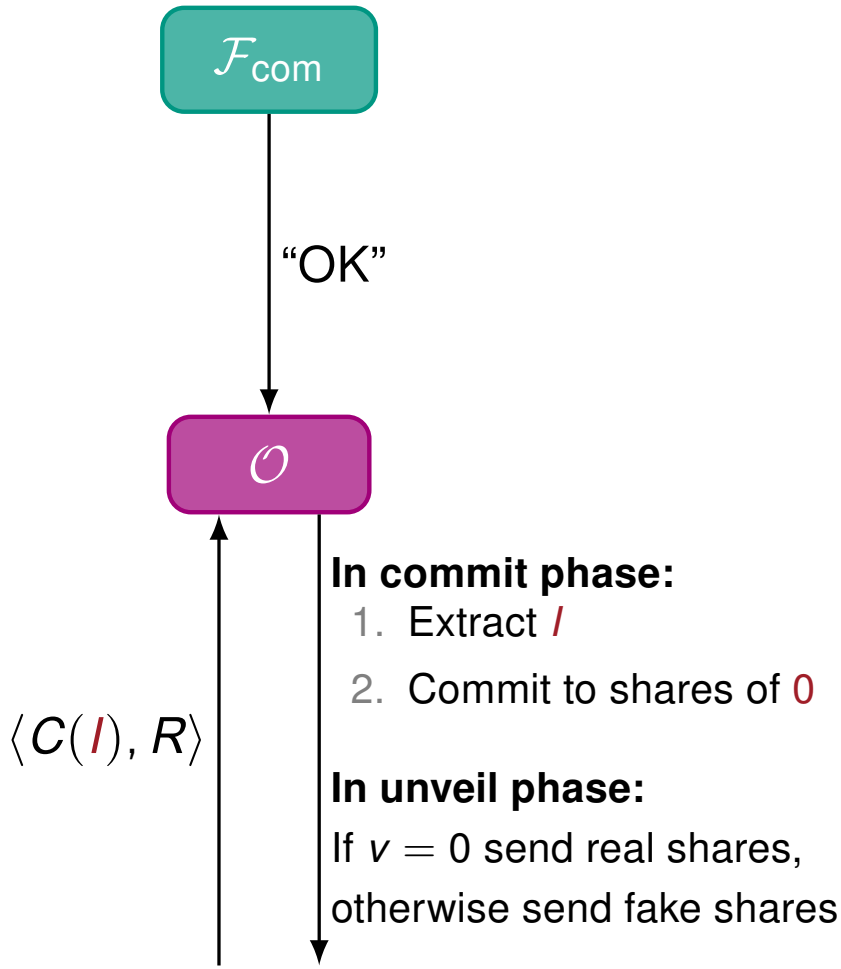


Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Constant-round Commitment Scheme

Definition of the Shielded Oracle $\mathcal{O}$

Corrupted Receiver

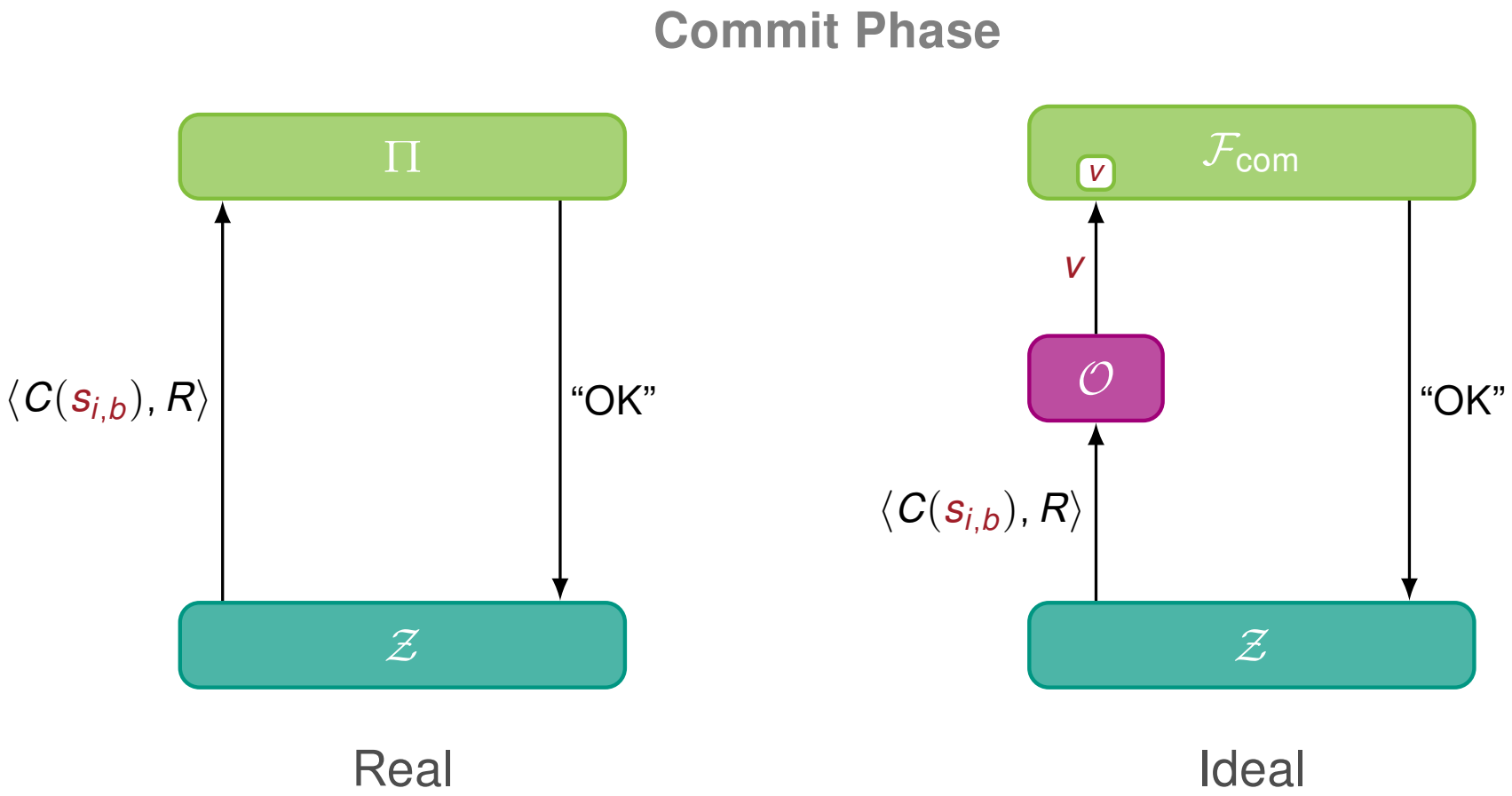


Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Constant-round Commitment Scheme

Proof Idea – Discrepancy

Let the sender be corrupted.

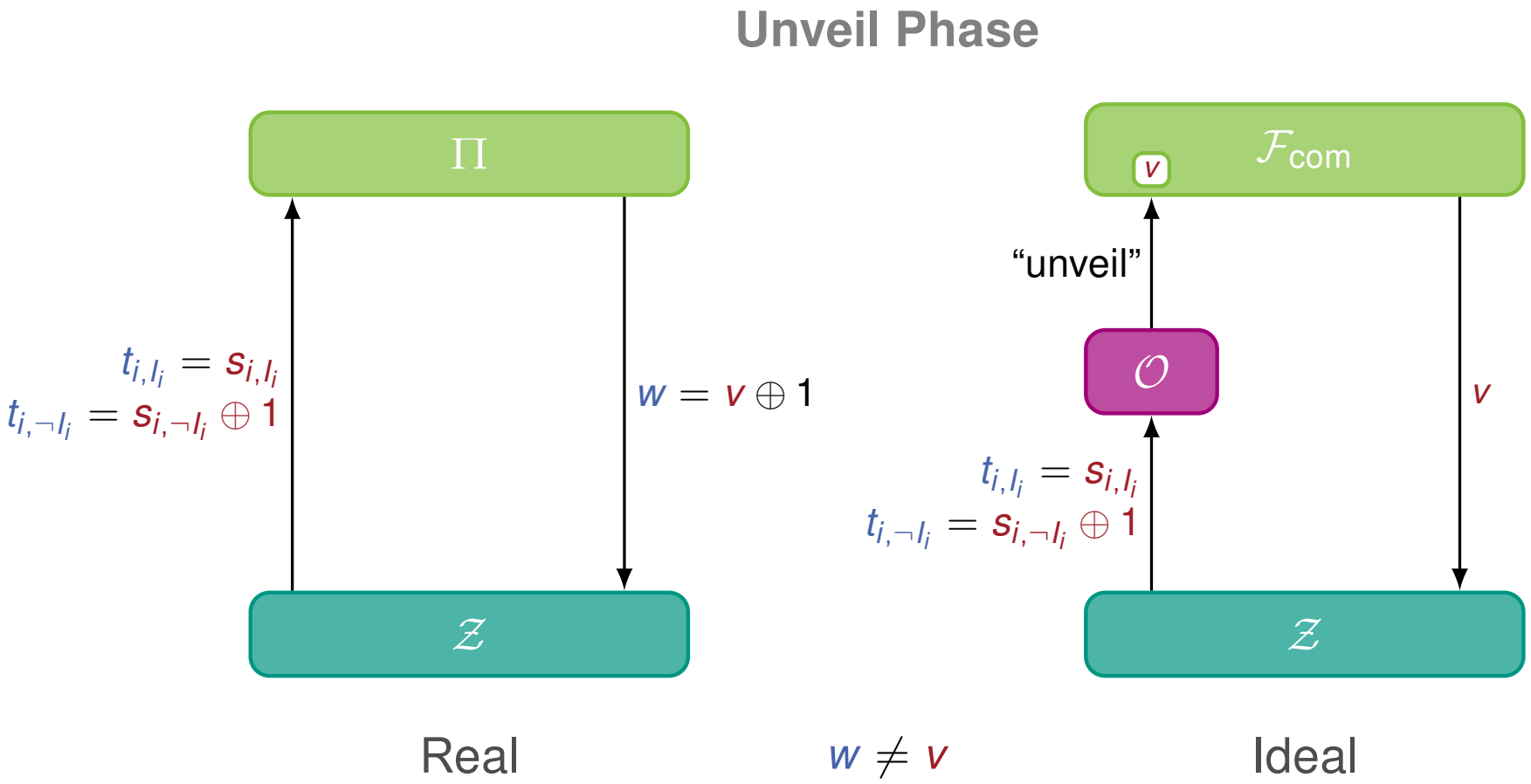


Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Constant-round Commitment Scheme

Proof Idea – Discrepancy

Let the sender be corrupted.

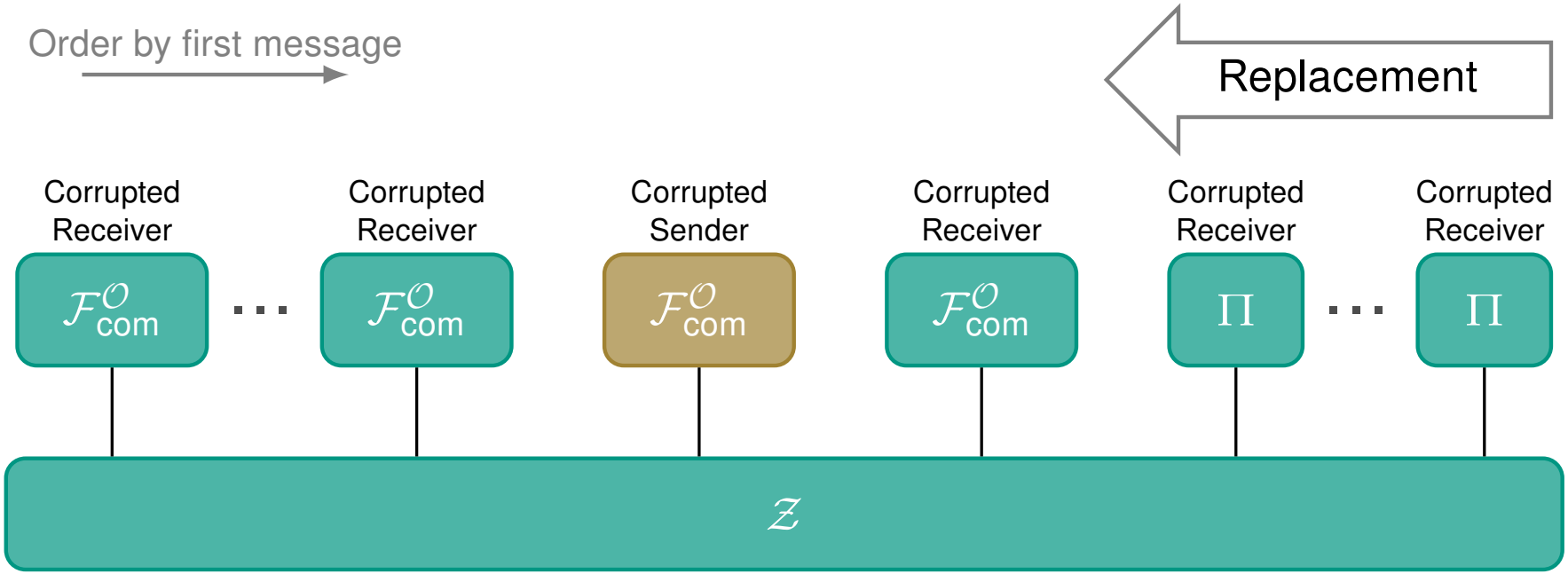


Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Constant-round Commitment Scheme

Proof Idea

- W. l. o. g.: Consider at most one $\mathcal{F}_{\text{com}}^{\mathcal{O}}$ with a corrupted sender
- Iteratively replace all $\mathcal{F}_{\text{com}}^{\mathcal{O}}$ with a corrupted receiver by Π, starting with the last session

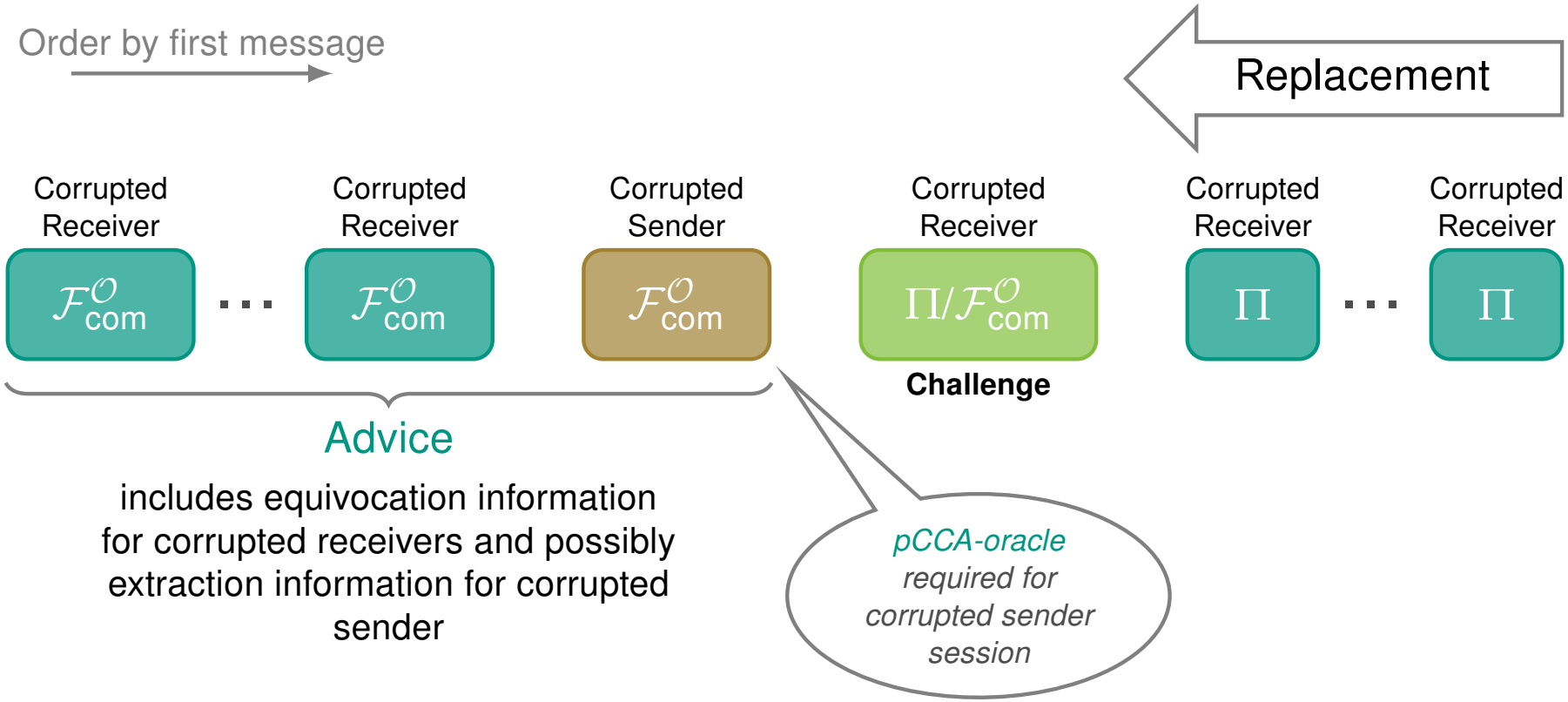


Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Constant-round Commitment Scheme

Proof Idea

Non-uniform reduction to parallel-CCA security of $\langle C, R \rangle$



Modular Composition Theorem for Π

Next Goal

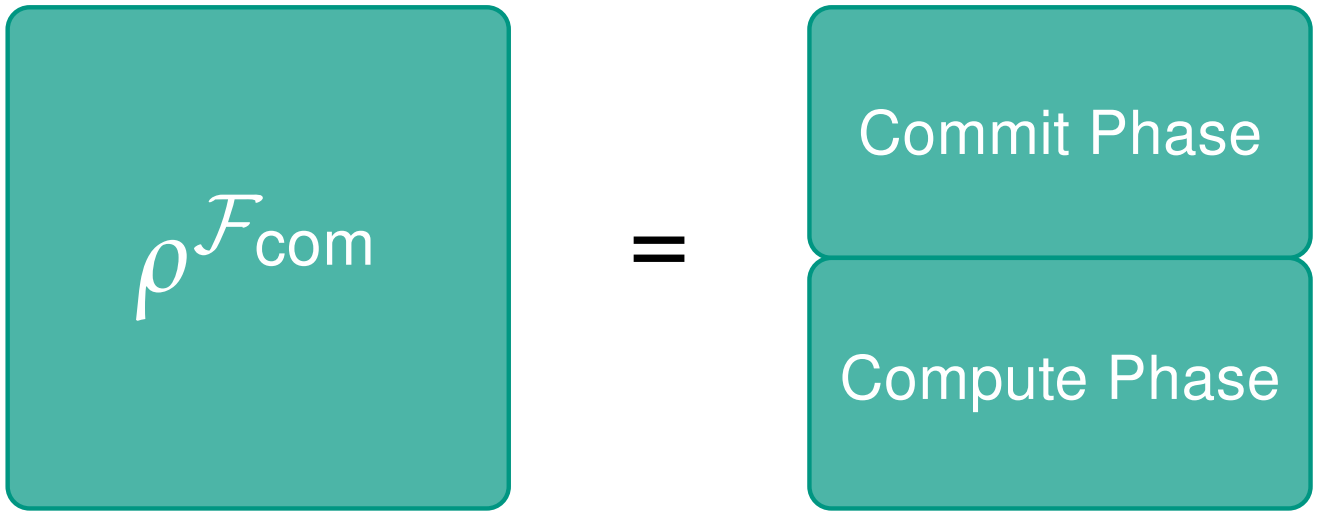
- Want to plug Π into UC-secure protocols
- Composite protocol secure in our framework

  → Allows to **re-use existing UC results**

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Modular Composition Theorem for Π

Commit-Compute Protocols



Any (poly-round) protocol can be **compiled** into one obeying this structure
(using randomized commitments)

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

Modular Composition Theorem for Π

The Theorem

Let $\rho^{\mathcal{F}_{\text{com}}}$ be a commit-compute protocol and Π as before.

$$\rho^{\mathcal{F}_{\text{com}}} \underset{\mathcal{E}\text{-pCCA}}{\geq} \mathcal{G} \quad \Rightarrow \quad \exists \text{ shielded oracle } \mathcal{O}' : \rho^{\Pi} \underset{\mathcal{G}^{\mathcal{O}'}}{\geq} \mathcal{G}^{\mathcal{O}'}$$

UC-environment has non-adaptive access to the decommitment oracle $\mathcal{E}$ of $\langle C, R \rangle$

This talk is too short to contain the proof.

Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security

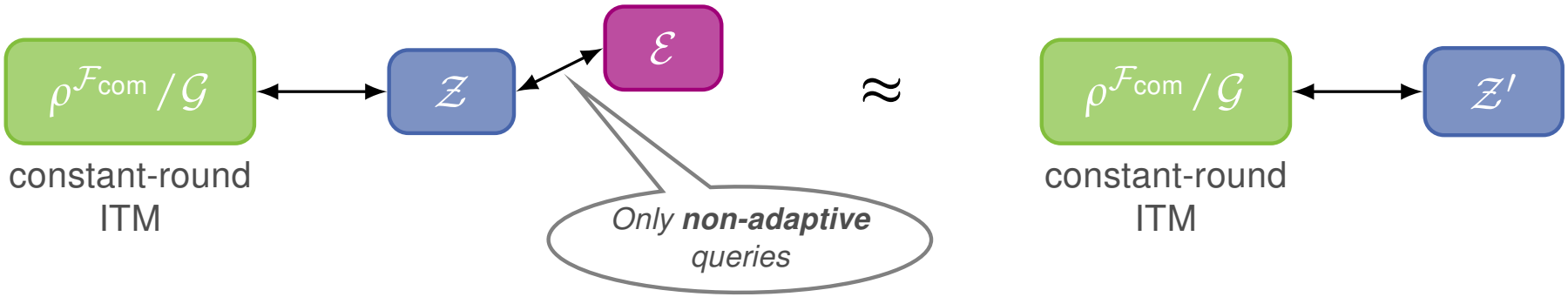
Modular Composition Theorem for Π

Composing with any constant-round UC-secure protocol

Given any constant-round $\rho^{\mathcal{F}_{\text{com}}} \geq_{\text{UC}} \mathcal{G}$.

- Compile $\rho^{\mathcal{F}_{\text{com}}}$
- Additionally require $\langle C, R \rangle$ to be *r*-non-adaptively robust

  (for sufficiently large *r*)



Faculty of Computer Science
Institute for Theoretical Informatics
Research Group for Cryptography and Security