Composable Long-Term Security with Rewinding

Robin Berger[1], Brandon Broadnax, Michael Klooß[1 → 2], Jeremias Mechler[1], Jörn Müller-Quade[1], Astrid Ottenhues[1], Markus Raiber[1]

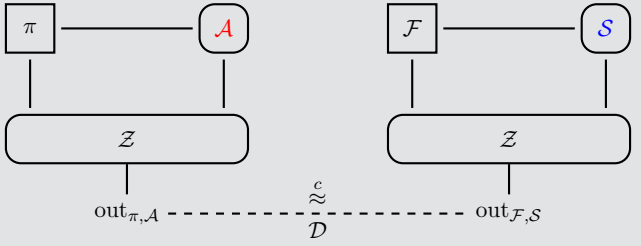
2023-12-02 @TCC

[1]KASTEL Security Research Labs, Karlsruhe Institute of Technology
[2]Aalto University

Computational UC in a nutshell [Can01; Can20]

Security experiment (Computional UC)

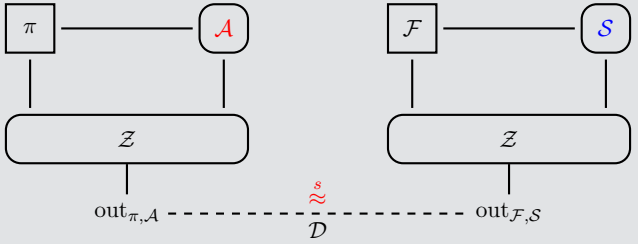
- **PPT** $\mathcal{A}$, $\mathcal{S}$, $\mathcal{Z}$ where $\mathcal{Z}$ outputs a **string** out.
- **PPT** distinguisher $\mathcal{D}$ gets out.



Statistical UC in a nutshell [Can01; Can20]

Security experiment (Statistical UC)

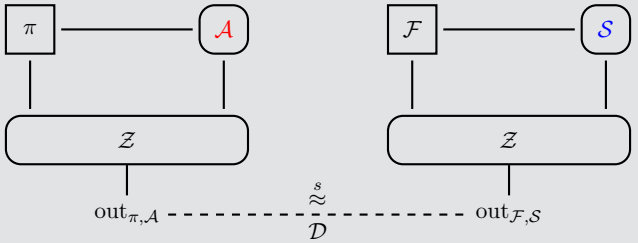
- **Unbounded** $\mathcal{A}$, $\mathcal{S}$, $\mathcal{Z}$ where $\mathcal{Z}$ outputs a **string** out.
- **Unbounded** distinguisher $\mathcal{D}$ gets out.



Long-Term UC in a nutshell [MU07]

Security experiment (Long-Term UC)

- PPT $\mathcal{A}$, $\mathcal{S}$, $\mathcal{Z}$ where $\mathcal{Z}$ outputs a **string** out.
- **Unbounded** distinguisher $\mathcal{D}$ gets out.



⇝ hardness assumptions hold *(only) during* protocol execution.

Long-Term UC commitments

Possibility results

$\mathcal{F}_{\text{Com}}$ from hardware assumptions (signature card [MU07], PUF+CRS [Mag+22]).

Impossibility result [MU07]

$\mathcal{F}_{\text{Com}}$ is impossible to realize in the CRS-hybrid model or any long-term revealing setup.

Long-Term UC commitments

Possibility results

$\mathcal{F}_{\text{Com}}$ from hardware assumptions (signature card [MU07], PUF+CRS [Mag+22]).

Impossibility result [MU07]

$\mathcal{F}_{\text{Com}}$ is impossible to realize in the CRS-hybrid model or any long-term revealing setup.

Core problem

- If CRS is not stat. hiding, $\mathcal{D}$ can extract.
- If CRS is stat. hiding, $\mathcal{S}$ cannot *straightline* extract...

Long-Term UC commitments

Possibility results

$\mathcal{F}_{\text{Com}}$ from hardware assumptions (signature card [MU07], PUF+CRS [Mag+22]).

Impossibility result [MU07]

$\mathcal{F}_{\text{Com}}$ is impossible to realize in the CRS-hybrid model or any long-term revealing setup.

Core problem

- If CRS is not stat. hiding, $\mathcal{D}$ can extract.
- If CRS is stat. hiding, $\mathcal{S}$ cannot *straightline* extract...
- ...but what about *rewinding*?

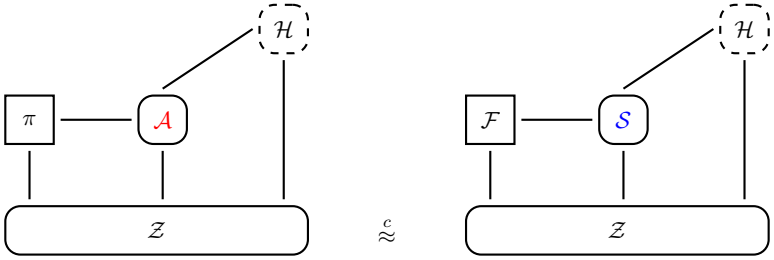
Our contribution

- New notion: **Long-term *rewinding* UC** (LTR-UC).
- New possibilities/protocols:
  - LTR-UC-secure $\mathcal{F}_{\mathsf{Com}}$ in the CRS-hybrid model (and commit-and-prove ZK).
  - One-sided LTR-UC-secure OT.
- New impossibilities: No full LTR-UC-secure OT from long-term revealing assumptions.
- New tools: **Pseudo-oracles** and their properties.

Angel-based UC security

Angel-based UC [PS04]

- Global entity, **helper** or **angel** $\mathcal{H}$ with "special power".
- E.g.: $\mathcal{H}$ brute-forces commitments under *judiciously chosen circumstances.*



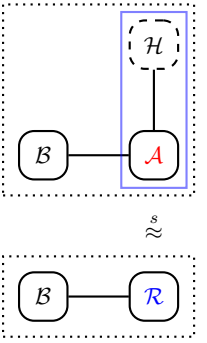
Rewinding-simulatable angels

[CLP10; Goy+15]

- $\mathcal{H}$ is a CCA commitment oracle:
  - $\mathcal{A}$ can run COM with $\mathcal{H}$.
  - $\mathcal{H}$ will brute-force extracts *accepting* commitments.
- $\mathcal{H}$ is **simulatable in PPT via rewinding** through $\mathcal{R}$.

Robust rewinding

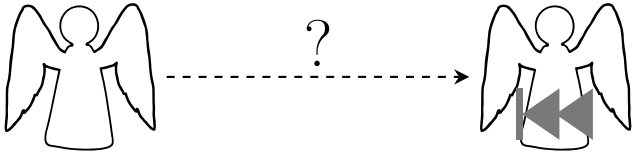
- UC simulation is straightline $\rightsquigarrow$ use $\mathcal{H}$
- Security reductions $\rightsquigarrow$ use $\mathcal{R}$.
- k-robust rewinding: Exempt k-round "left side" from being rewound.



$\langle \mathcal{B}, \mathcal{A}^{\mathcal{H}} \rangle \overset{s}{\approx} \langle \mathcal{B}, \mathcal{R} \rangle$

Rewinding-based angels/oracles?

- LTR-UC also based on a CCA commitment oracle $\mathcal{H}$.
- But what is an "angel/oracle that rewinds"?



Pseudo-Oracles

Oracle/ITM

Stateful $\mathcal{O}$ gets message from $\mathcal{A}$, returns output.

$\rightsquigarrow$ Inherently unable to rewind $\mathcal{A}$.

Pseudo-Oracles

Oracle/ITM

Stateful $\mathcal{O}$ gets message from $\mathcal{A}$, returns output.
$\rightsquigarrow$ Inherently unable to rewind $\mathcal{A}$.

Pseudo-Oracle

Stateful $\mathcal{O}$ gets message and **view of** $\mathcal{A}$, returns output.

Properties of pseudo-oracles

Black-box

$\mathcal{O}$ only uses $\mathcal{A}$ black-box (instead of view($\mathcal{A}$)).

Properties of pseudo-oracles

Black-box

$\mathcal{O}$ only uses $\mathcal{A}$ black-box (instead of view($\mathcal{A}$)).

k-robust pseudo-PPT ($\widehat{=}$ rewinding simulatable)

For any k-round $\mathcal{B}$:

$$\exists \text{PPT } \mathcal{R}: \quad \langle \mathcal{B}, \mathcal{A}^{\mathcal{O}} \rangle \overset{s}{\approx} \langle \mathcal{B}, \mathcal{R} \rangle$$

Properties of pseudo-oracles

Black-box

$\mathcal{O}$ only uses $\mathcal{A}$ black-box (instead of view($\mathcal{A}$)).

k-robust pseudo-PPT ($\widehat{=}$ rewinding simulatable)

For any k-round $\mathcal{B}$:

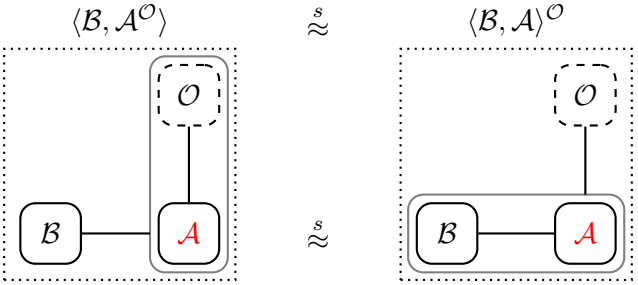
$$\exists \text{PPT } \mathcal{R}: \quad \langle \mathcal{B}, \mathcal{A}^{\mathcal{O}} \rangle \overset{s}{\approx} \langle \mathcal{B}, \mathcal{R} \rangle$$

k-robust composition-order invariant

For any k-round $\mathcal{B}$:

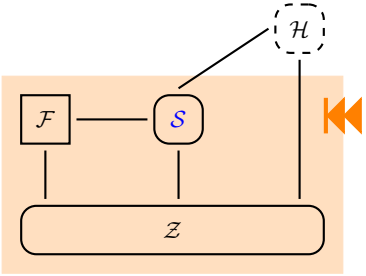
$$\langle \mathcal{B}, \mathcal{A}^{\mathcal{O}} \rangle \overset{s}{\approx} \langle \mathcal{B}, \mathcal{A} \rangle^{\mathcal{O}}$$

Composition-order invariance (COI)



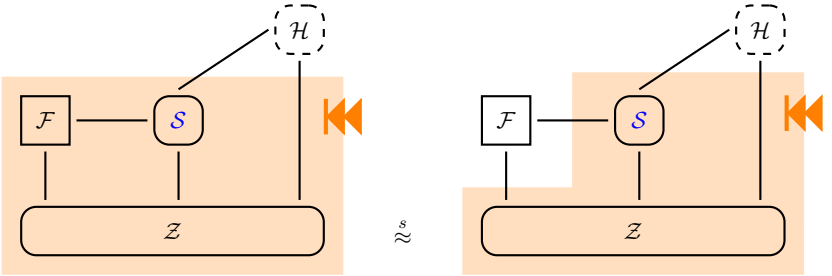
Why is LTR-UC meaningful at all?

- LTR-UC angel $\mathcal{H}$ **rewinds environment and ideal functionalities!**
- What remains of the ideal guarantees of $\mathcal{F}$?



Why is LTR-UC meaningful at all?

- LTR-UC angel $\mathcal{H}$ **rewinds environment and ideal functionalities!**
- What remains of the ideal guarantees of $\mathcal{F}$?
- **k-robust COI** $\implies$ meaningful for k-round functionalities.



Conclusion

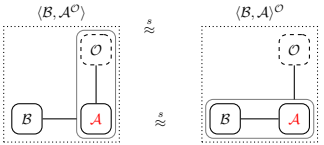
- LTR-UC brings rewinding-based simulation to UC.
  - New possibilities: Com, ZK, one-sided-secure OT *from CRS*
  - Old impossibilities: (fully secure) OT from long-term revealing assumptions.
- Pseudo-Oracles $\neq$ Oracles: Basic properties need non-trivial proofs.

Conclusion

Thank you!

- LTR-UC brings rewinding-based simulation to UC.
  - New possibilities: Com, ZK, one-sided-secure OT *from CRS*
  - Old impossibilities: (fully secure) OT from long-term revealing assumptions.
- Pseudo-Oracles $\neq$ Oracles: Basic properties need non-trivial proofs.

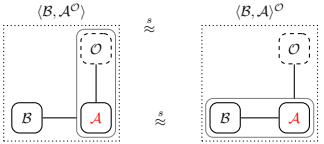
COI for our CCA-Com $\mathcal{O}$



Core difference to [CLP10; Goy+15]:

- [CLP10; Goy+15]: COI holds **unconditionally** due to bruteforce extraction.
- This work: COI via **reduction** to hardness assumption.

COI for our CCA-Com $\mathcal{O}$

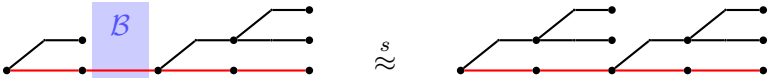


Core difference to [CLP10; Goy+15]:

- [CLP10; Goy+15]: COI holds **unconditionally** due to bruteforce extraction.
- This work: COI via **reduction** to hardness assumption.

Proof idea (based on [PRS02] rewinding schedule):

- Given same randomness, **main thread** execution is **identical, unless** different committed values extracted (during look-ahead).
- Reduce different extracted values to **binding break** of COM.



References I

[Can01] Ran Canetti. “Universally Composable Security: A New Paradigm for Cryptographic Protocols”. In: **42nd FOCS**. Oct. 2001.

[Can20] Ran Canetti. “Universally Composable Security”. In: **J. ACM** 67.5 (2020).

[CLP10] Ran Canetti, Huijia Lin, and Rafael Pass. “Adaptive Hardness and Composable Security in the Plain Model from Standard Assumptions”. In: **51st FOCS**. Oct. 2010.

[Goy+15] Vipul Goyal, Huijia Lin, Omkant Pandey, Rafael Pass, and Amit Sahai. “Round-Efficient Concurrently Composable Secure Computation via a Robust Extraction Lemma”. In: **TCC 2015, Part I**. Vol. 9014. LNCS. Mar. 2015.

[Mag+22] Bernardo Magri, Giulio Malavolta, Dominique Schröder, and Dominique Unruh. “Everlasting UC Commitments from Fully Malicious PUFs”. In: **Journal of Cryptology** 35.3 (July 2022).

[MU07] Jörn Müller-Quade and Dominique Unruh. “Long-Term Security and Universal Composability”. In: **TCC 2007**. Vol. 4392. LNCS. Feb. 2007.

References II

[PRS02] Manoj Prabhakaran, Alon Rosen, and Amit Sahai. "Concurrent Zero Knowledge with Logarithmic Round-Complexity". In: **43rd FOCS**. Nov. 2002.

[PS04] Manoj Prabhakaran and Amit Sahai. "New notions of security: Achieving universal composability without trusted setup". In: **36th ACM STOC**. June 2004.

Image sources

- Peter J. Yost, CC-BY-SA 4.0.