Games That Talk:
New Foundations for Composable Security

Lúcás Críostóir Meier
lucas@cronokirby.com

December 7, 2022

Abstract

We do things with UC security.

1 Introduction

[Mei22]

Definition 1.1 (Adversaries). An adversary is a cool thing.

Theorem 1.1 (Cool Beans). Woah mama

And that's what matters.

■

Lemma 1.2. Woah mama again!

Corollary 1.3. Woah mama again!

Γ^0

$x \leftarrow 3$
if $x + 2$:
  $y \xleftarrow{\$} \mathbb{F}_q$
$m \Rightarrow \langle \mathcal{P}_i, \mathcal{P}_j \rangle$ $y \leftarrow 4$
$m \Leftarrow \langle \mathsf{OT}, \mathcal{P}_i \rangle$ $x \leftarrow 3$

$\underline{\mathrm{Foo}(x, y)\text{:}}$
  $\mathrm{Bar}(x, y)$

(1)

Game 1.1: Some Game

1.1 Relevance of Time Travel

stuff

IND-CCA
$x \leftarrow 4$

Protocol 1.2: Some Protocol

IND-CCA
$x \leftarrow 4$

Protocol 1.3: Some Protocol

IND-CCA
$x \leftarrow 3$

Functionality 1.4: Encryption

2 State-Separable Proofs

3 Games That Talk

4 Protocols and Composition

5 Differences with UC Security

6 Examples

7 Further Work

8 Conclusion

References

[Mei22] Lúcás Críostóir Meier. MPC for group reconstruction circuits. Cryptology ePrint Archive, Report 2022/821, 2022. https://eprint.iacr.org/2022/821.