Abstract Modeling of System Communication in Constructive Cryptography using CryptHOL

David Basin
Dept. of Computer Science
ETH Zürich, Switzerland
basin@inf.ethz.ch

Andreas Lochbihler
Digital Asset
Zurich, Switzerland
mail@andreas-lochbihler.de

Ueli Maurer
Dept. of Computer Science
ETH Zürich, Switzerland
maurer@inf.ethz.ch

S. Reza Sefidgar
Dept. of Computer Science
ETH Zürich, Switzerland
reza.sefidgar@inf.ethz.ch

1-7607-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/CSF51468.2021.00047

***Abstract*—Proofs in simulation-based frameworks have the greatest rigor when they are machine checked. But the level of details in these proofs surpasses what the formal-methods community can handle with existing tools. Existing formal results consider streamlined versions of simulation-based frameworks to cope with this complexity. Hence, a central question is how to abstract details from composability results and enable their formal verification.**

In this paper, we focus on the modeling of system communication in composable security statements. Existing formal models consider fixed communication patterns to reduce the complexity of their proofs. However, as we will show, this can affect the reusability of security statements. We propose an abstract approach to modeling system communication in Constructive Cryptography that avoids this problem. Our approach is suitable for mechanized verification and we use CryptHOL, a framework for developing mechanized cryptography proofs, to implement it in the Isabelle/HOL theorem prover. As a case study, we formalize

complexity of ideal specifications and makes the security arguments intricate [6]. As such, existing formal results such as EasyUC [8] consider a simplified version of these frameworks with restricted communication capabilities between components. However, as we will show in Section III-A, such simplifications affect the reusability of security statements.

Constructive Cryptography (CC) [17], [18], [19] proposes a fundamental shift in how security statements are made and proved. It introduces an abstract approach to composable security arguments that allows one to focus on a particular aspect of security proofs without being distracted by other details. This makes composable security statements manageable for protocol designers. However, the existing CC results [12], [16] do not delve into the details of system communication.

B. Our Solution