YAZKC
Yet Another Zero-Knowledge Compiler

Endre Bangerter, Stephan Krenn, Ahmad-Reza Sadeghi, Thomas Schneider
1 Bern University of Applied Sciences, Biel-Bienne, Switzerland
2 University of Fribourg, Switzerland
3 Horst Görtz Institute for IT-Security, Ruhr-University Bochum, Germany

Introduction: ZK Proofs
- ... are basic crypto primitives
  - Used in Identification Schemes (e.g., Direct Anonymous Attestation and Anonymous Credentials), Group Signatures, e-Cash, Secure Multiparty Computation, ...
- ... are based on efficient \( \Sigma \)-protocols
- ... have to be implemented “by hand”
  - Time-Consuming, Error-Prone, Skill gap between Cryptographers & Programmers, ...
- Goal: Automatize design & implementation

CACE ZK Toolbox: FEATURES
- Support of (almost) all ZK proofs used in practice
  - Protocols: Sigma-Phi, Sigma-Exp, Damgård-Fujsaki
- Arbitrary Compositions: AND, OR, Threshold Structures
- Compilation to non-interactive ZK proofs (NIZK)
- Integrated optimization techniques
- Integrated, fully automatic, formal verification
  - First (and only) self-certifying zero-knowledge compiler
- Multiple output targets
  - Documentation: LaTeX
  - Code: C, Java (coming soon)
- Available online: http://zkc.cace-project.eu

CACE ZK Toolbox: ARCHITECTURE

CACE ZK Toolbox: PUBLICATIONS
A Certifying Compiler for Zero-Knowledge Proofs of Knowledge Based on Sigma-Protocols.

CACE ZK Toolbox: CONTRIBUTORS
José Bacelar Almeida, Endre Bangerter, Manuel Barbosa, Stefania Barzan, Thomas Briner, Andreas Grünert, Wilko Hennecka, Stephan Krenn, Ahmad-Reza Sadeghi, Thomas Schneider, Jose-Kai Tsyu