Yet Another Zero-Knowledge Compiler

Endre Bangerter¹, Stephan Krenn¹,², Ahmad-Reza Sadeghi³, Thomas Schneider³

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-Gash, secure multiparty computation, ...
- ... are based on efficient Σ-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-Π, Sigma-Exp, Damgård-Fujisaki
- 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

Protocol Specification Language
Multiple types of Σ-Protocols, groups, arbitrary compositions (AND, OR, ...), ...

Protocol Implementation Language
Algorithms, operations, messages, ...

Protocol Specification (PSL)
Automatic protocol composition and choice of parameters

Protocol Implementation (PIL)
Details of proof protocol, "pseudo-code"

What to prove?

What to prove?

CACE ZK Toolbox: FORMAL VERIFICATION

Formal Verification
- ... proves that compilation from the proof goal to pseudo-code was correct.
- ... is independent of the backend being used.
- ... works for a large subset of the proof goals our compiler can handle.
- ... does not require any human interaction.
- ... makes our toolbox the first certifying zero-knowledge compiler.

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

CACE ZK Toolbox: PUBLICATIONS
J.B. Almeida, E. Bangerter, M. Barbosa, S. Krenn, A.-R. Sadeghi, T. Schneider,
A Certifying Compiler for Zero-Knowledge Proofs of Knowledge Based on Sigma-Protocols.

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tusey,
In ECRYPT workshop on Software Performance Enhancements for Encryption and Decryption and Cryptographic Compilers (SPED-C'09), October 12-13, 2009.

E. Bangerter, T. Briner, W. Henckes, S. Krenn, A.-R. Sadeghi, T. Schneider,
Automatic Generation of Sigma-Protocols.
In 6th European Workshop on Public Key Services, Applications and Infrastructures (EUROPKS'09), September 10-11, 2009.

E. Bangerter, J. Camastrap, S. Krenn, A.-R. Sadeghi, T. Schneider,

E. Bangerter, S. Barzan, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tusey,
Bringing Zero-Knowledge Proofs of Knowledge to Practice.
In 7th International Workshop on Security Protocols (SP’09), April 1-3, 2009.