YAZKC
Yet Another Zero-Knowledge Compiler

Endre Bangerter[1], Stephan Krenn[1,2], Ahmad-Reza Sadeghi[3], Thomas Schneider[3]

[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 Σ-protocols**
- **… have to be implemented "by hand"**
  - Time-Consuming, Error-Prone, Skill gap between Cryptographers & Programmers, ...
- **Goal: Automatize design & implementation**

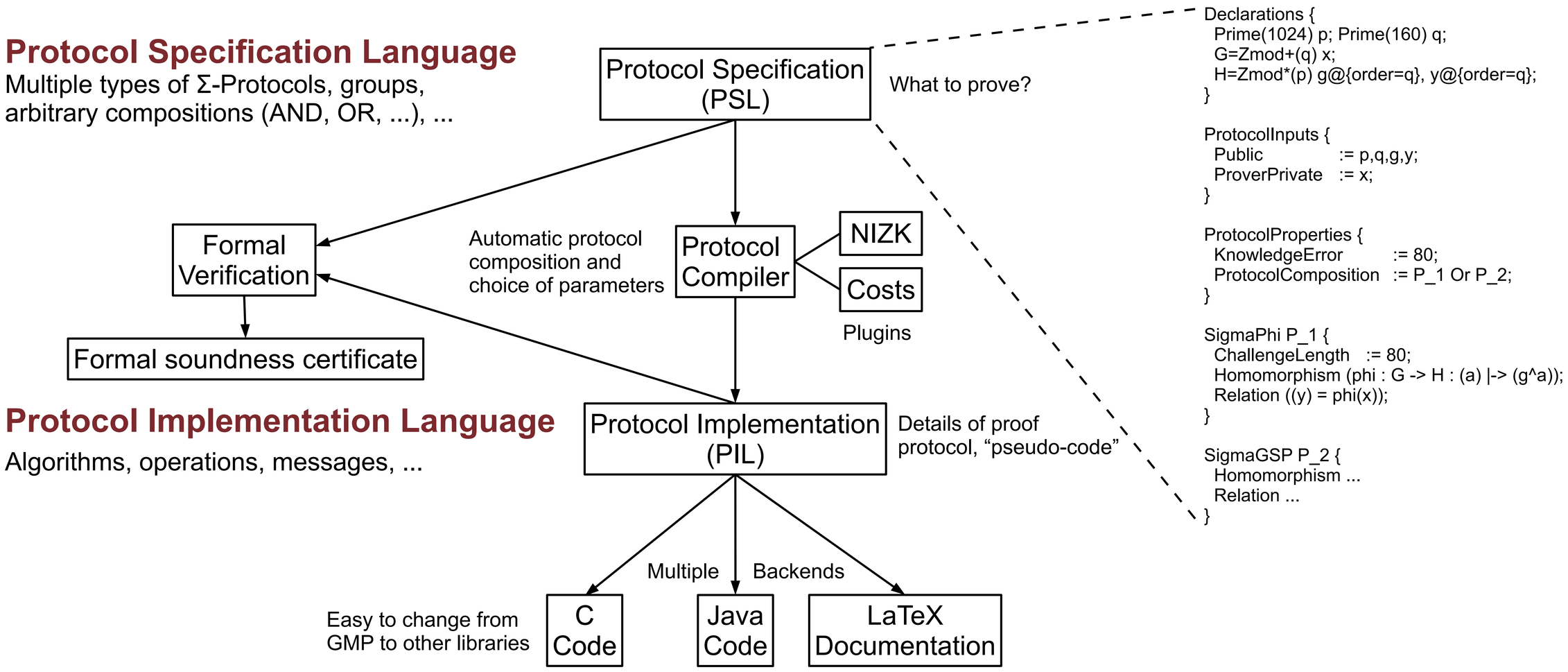
CACE ZK Toolbox: FEATURES

- **Support of (almost) all ZK proofs used in practice**
  - Protocols: Sigma-Phi, 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, ...), ...

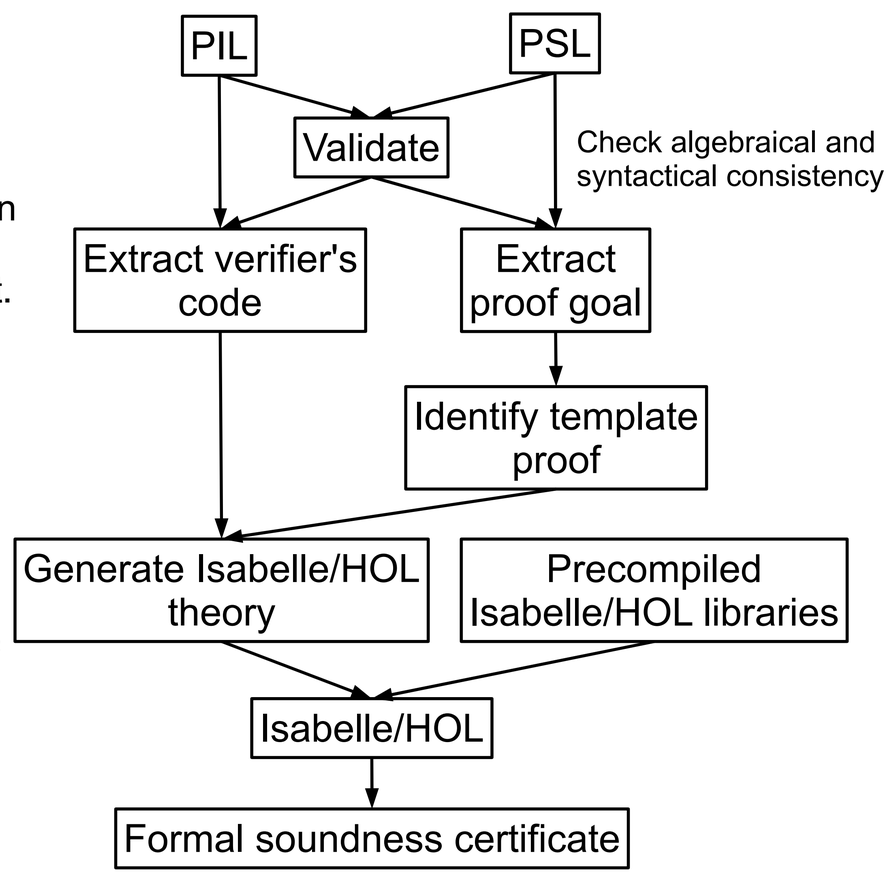
Protocol Implementation Language
Algorithms, operations, messages, ...



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 Grünert, Wilko Henecka, Stephan Krenn, Ahmad-Reza Sadeghi, Thomas Schneider, Joe-Kai Tsay

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. In *15th European Symposium on Research in Computer Security (ESORICS'10)*, September 20-22, 2010. Full version available at http://eprint.iacr.org/2010/339.

E. Bangerter, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay.
On the Design and Implementation of Efficient Zero-Knowledge Proofs of Knowledge.
In *ECRYPT workshop on Software Performance Enhancements for Encryption and Decryption and Cryptographic Compilers (SPEED-CC'09)*, October 12-13, 2009.
Implementation available at http://zkc.cace-project.eu.

E. Bangerter, T. Briner, W. Henecka, S. Krenn, A.-R. Sadeghi, T. Schneider.
Automatic Generation of Sigma-Protocols.
In *6th European Workshop on Public Key Services, Applications and Infrastructures (EUROPKI'09)*, September 10-11, 2009.
Implementation available at http://www.cace-project.eu/?Itemid=15.

E. Bangerter, J. Camenisch, S. Krenn, A.-R. Sadeghi, T. Schneider.
Automatic Generation of Sound Zero-Knowledge Protocols.
In *28th Advances in Cryptology - EUROCRYPT 2009 Poster Session*, April 26-30, 2009.
Full version available at http://eprint.iacr.org/2008/471.

E. Bangerter, S. Barzan, S. Krenn, A.-R. Sadeghi, T. Schneider, J.-K. Tsay.
Bringing Zero-Knowledge Proofs of Knowledge to Practice.
In *17th International Workshop on Security Protocols (SPW'09)*,
April 1-3, 2009. Full version available at http://eprint.iacr.org/2009/211.

EU FP7 Project Computer Aided Cryptography Engineering (CACE) - http://www.cace-project.eu

cace