

Automatic Generation of Sound Zero-Knowledge Protocols

Endre Bangerter¹, Jan Camenisch², Stephan Krenn^{1,3}, Ahmad-Reza Sadeghi⁴, Thomas Schneider⁴

¹Bern University of Applied Sciences, Biel-Bienne, Switzerland

²IBM Research, Zurich Research Labs, Rüschlikon, Switzerland

³University of Fribourg, Switzerland

⁴System Security Group, Ruhr-University Bochum, Germany

Introduction

- **ZK Proofs are Basic Crypto Primitives**
 - Used in Identification Schemes, Group Signatures, Secure Multiparty Computation, ...
- **First ZK Protocols Deployed in Practice**
 - Direct Anonymous Attestation (DAA) in TPM chips
 - Anonymous Credential Systems (IBM identity mixer)
- **Based on Efficient Sigma-Protocols**
 - Protocol Composition (AND, OR, ...)
 - Generic Transformations to Non-Interactive ZK (NIZK), ...
- **Design & Implementation “by Hand”**
 - Time-Consuming, Error-Prone, ...

Challenges

- **Protocol Design**
 - Choose Suitable Proof Techniques and Parameters
- **Implementation Efficiency**
 - From Semantic Proof Goal to Implementation
 - Skill Gap between Cryptographer & Programmers
- **Code Efficiency & Security**
 - Optimize Resources at Protocol & Code Level
 - Buffer Overflows, SW Side-Channels, ...

Automatic Generation of Sound ZK Protocols

High Level ZK-PoK Language

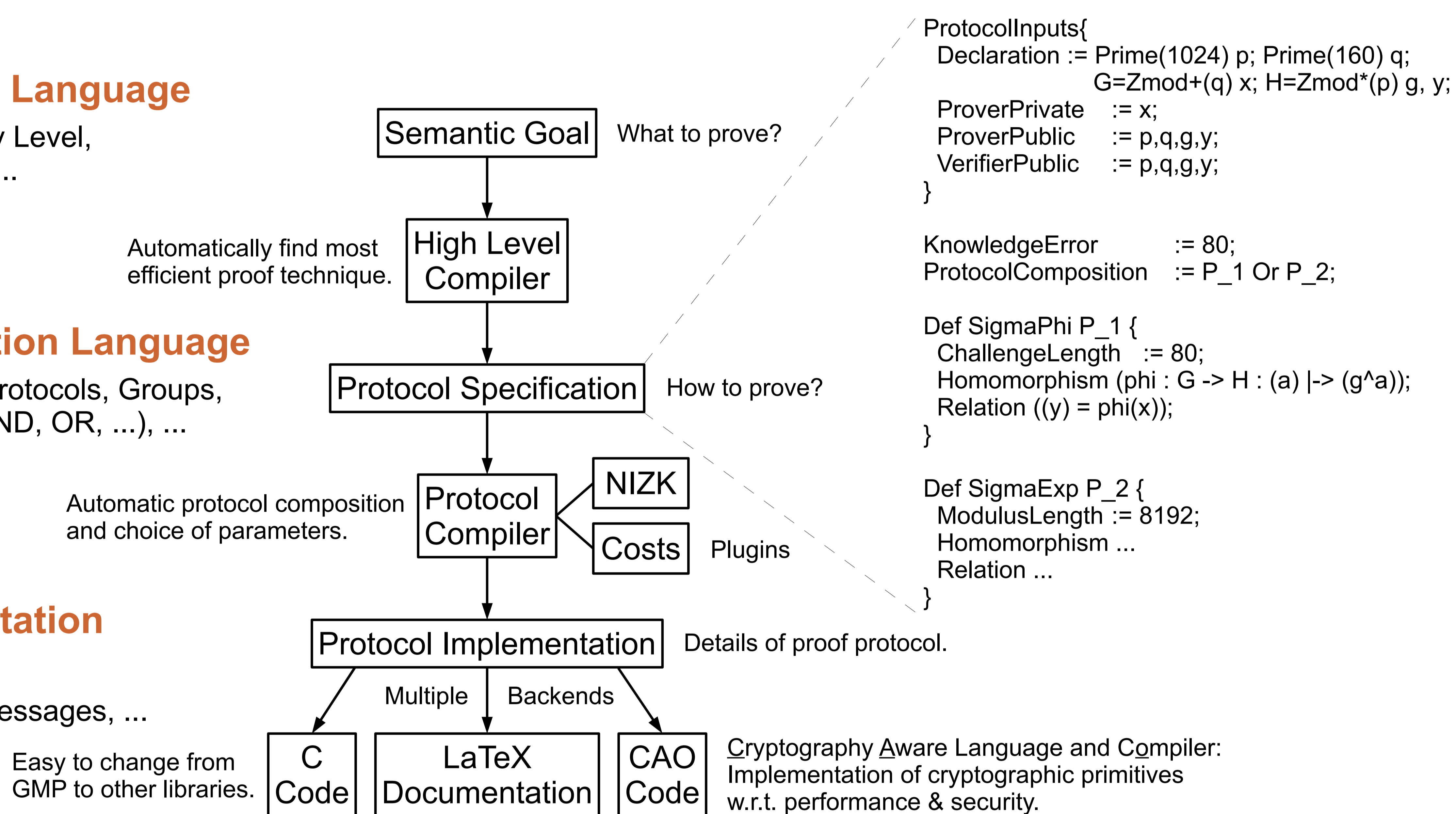
Relation to Prove, Security Level, Optimization Constraints, ...

Protocol Specification Language

Multiple Types of Sigma-Protocols, Groups, Arbitrary Compositions (AND, OR, ...), ...

Protocol Implementation Language

Algorithms, Operations, Messages, ...



Σ^{exp} – an Efficient Unconditionally Portable Protocol

Applications

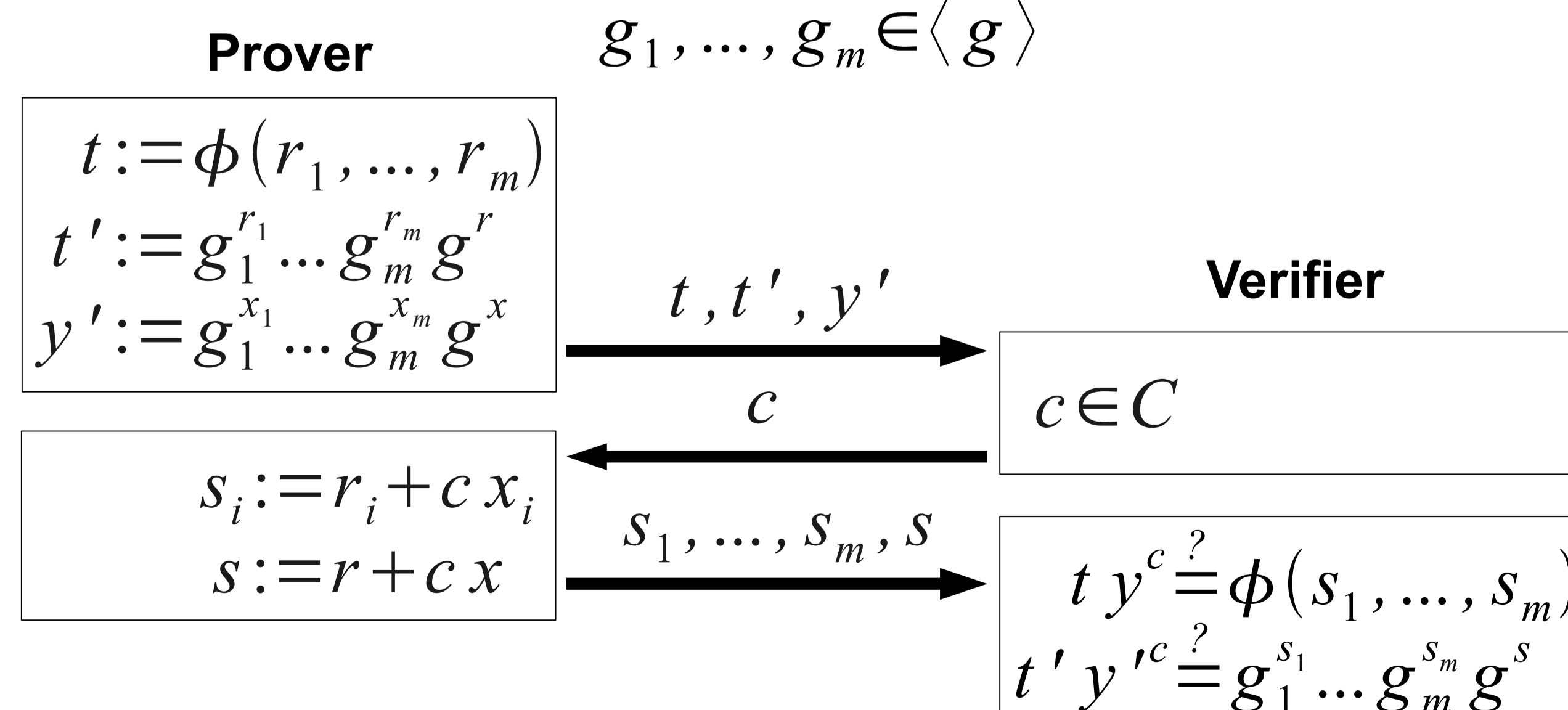
Proofs in hidden-order groups:

- Interval proofs
 - Boudot (Eurocrypt 00)
 - Lipmaa (ePrint 01)
- Anonymous Credential Systems
 - Camenisch, Lysyanskaya (SCN 02)
 - Camenisch, Van Herreweghen (ACM CCS 02)
- E-Cash
 - Camenisch, Hohenberger, Lysyanskaya (Eurocrypt 05)

High-Level Description of Σ^{exp}

$$ZPK [(x_1, \dots, x_m) : y = \phi(x_1, \dots, x_m)]$$

Auxiliary String
 n : RSA-Modulus
 $g \in \mathbb{Z}_n^*$
 $g_1, \dots, g_m \in \langle g \rangle$



Related Work

- Bangerter (PhD-Thesis 05)
- Bangerter, Camenisch, Maurer (PKC 05)
- Camenisch, Kiayias, Yung (Eurocrypt 09)

Advantage

Σ^{exp} has 3 instead of 6 moves:

- Higher Efficiency
- Efficient Transformations to
 - Non-Interactive ZK
 - Concurrent ZK
- Generic Protocol Composition