Formal Modeling of Cryptographic Games

Michael Backes, Matthias Berg
Dominique Unruh
Saarland University

Formal Proofs in Crypto

- **Crypto proofs: Extremely error prone**
- **Need: Computer verified proofs**
- **Sequences of Games**
  → Well-suited for mechanization

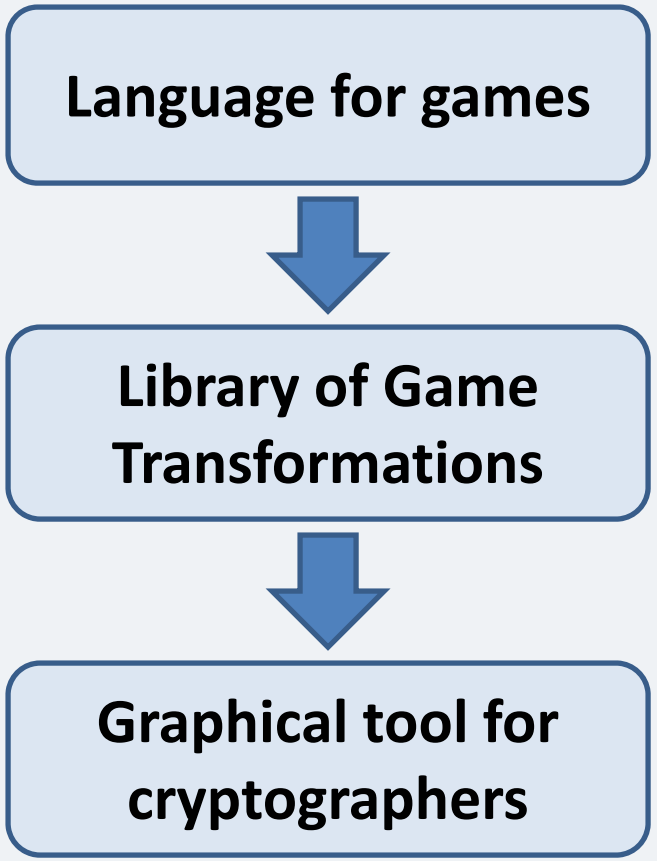
Our project

Mechanized verification

of cryptographic proofs

using Isabelle/HOL

Project Roadmap



Done (more or less)

In progress

Our vision

Language

Functional language

Formal semantics

Infinite objects (e.g., random tapes)

Oracles (with state)

Call for discussions

Contact me
if you're curious!

And thanks
for your attention