Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Ralf Sasse
January 2016

Verifying Security Protocols in Tamarin

Exercise Sheet 5

Assignment 5.1: Practical Tool Usage

Understand and verify/falsify protocols in order with regards to eCK model:

- NAXOS
- SignedDH

Assignment 5.2: Independent Tool Usage

Pick any protocol of your choice and try specifying it! Consider what security properties are desired, and which of those are reasonable to attempt to prove with Tamarin. Do not forget to add executability checks to ensure your specification is executable.