Automated Reverse Engineering using Lego®

Georg Chalupar and Stefan Peherstorfer
University of Applied Sciences Upper Austria

Erik Poll and **Joeri de Ruiter**
Radboud University Nijmegen

Introduction

- Used automated learning techniques to reverse engineer e.dentifier2
- Results in state machines
- Previously done for bank cards

e.dentifier2

- Developed by Todos (now Gemalto)
- EMV-CAP
- Can be used with or without USB
- With USB:
  - See-What-You-Sign
  - “the most secure sign-what-you-see end user device ever seen”
  - Good idea!

EMV-CAP

PIN

challenge

bitfilter(AC)

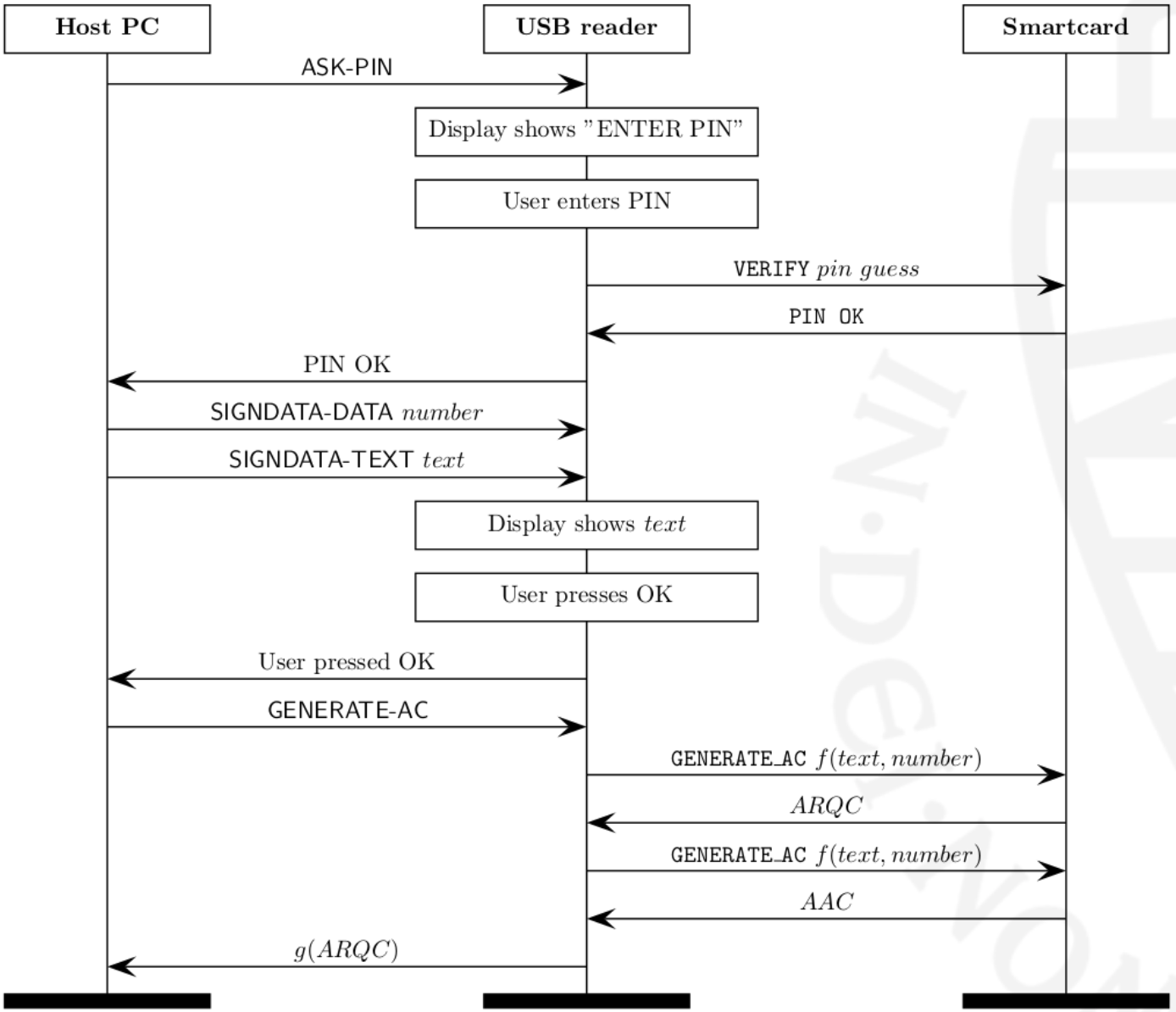
PIN

OK

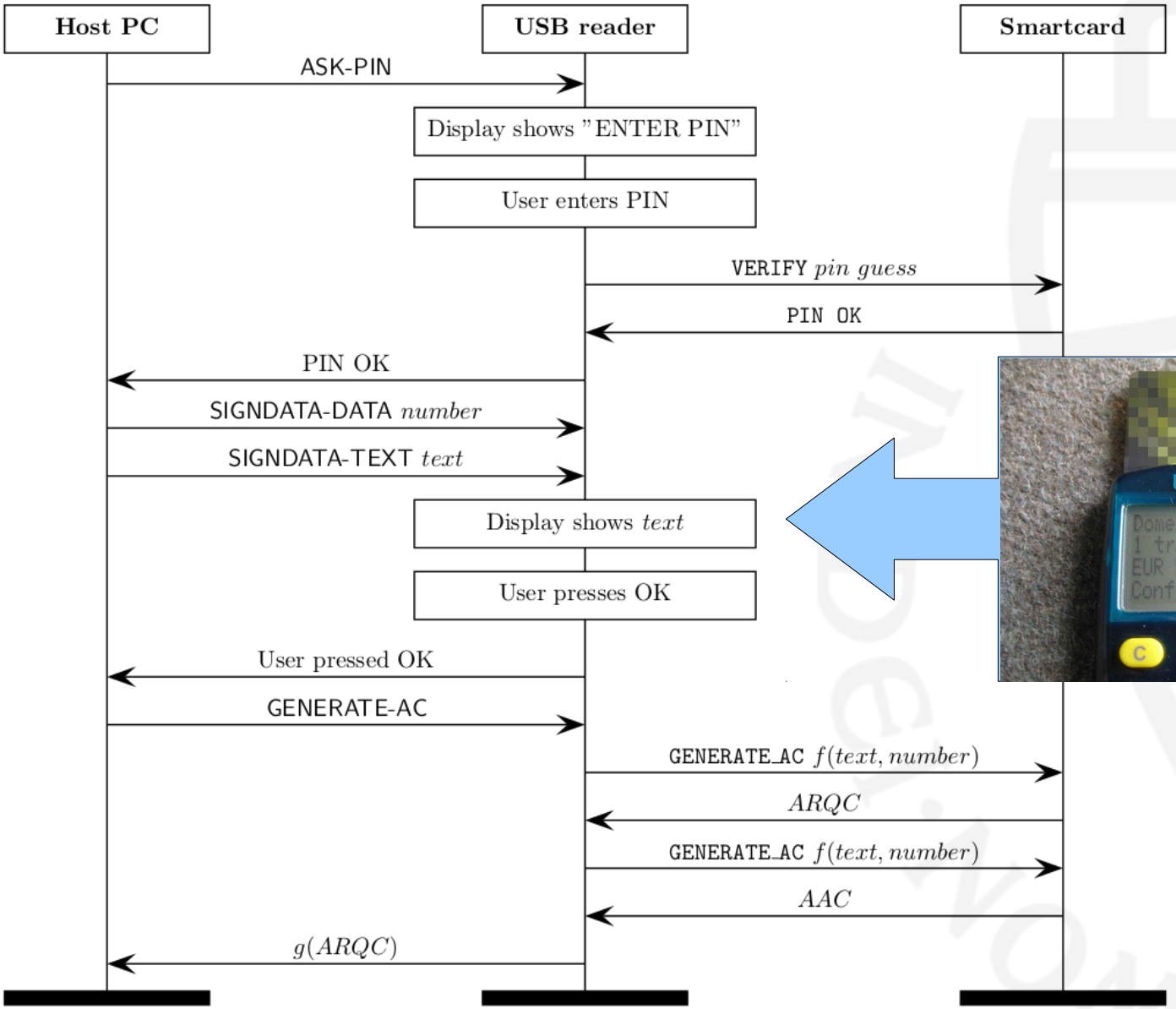
GENERATE AC (challenge,...)

AC

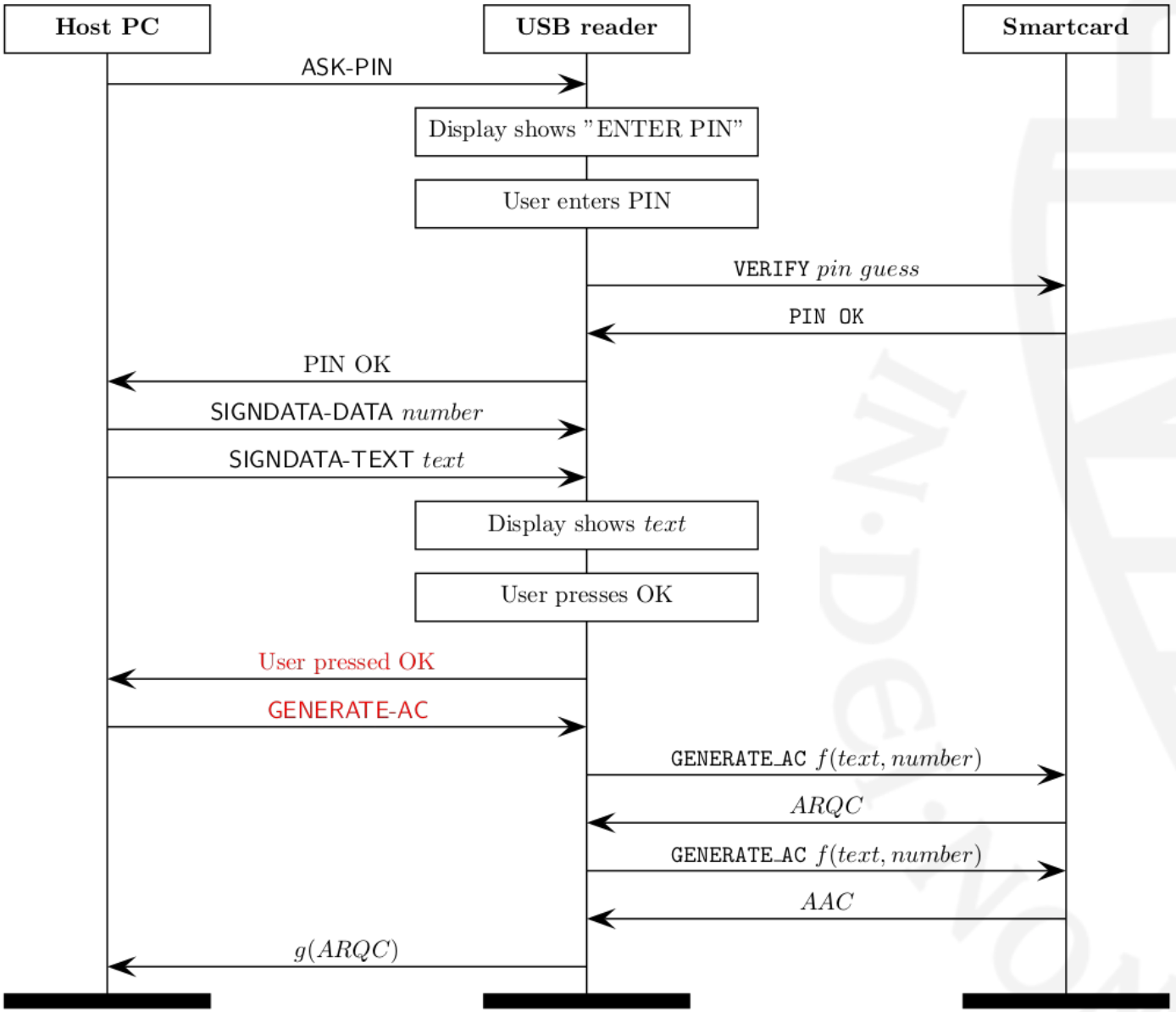
Protocol e.dentifier2



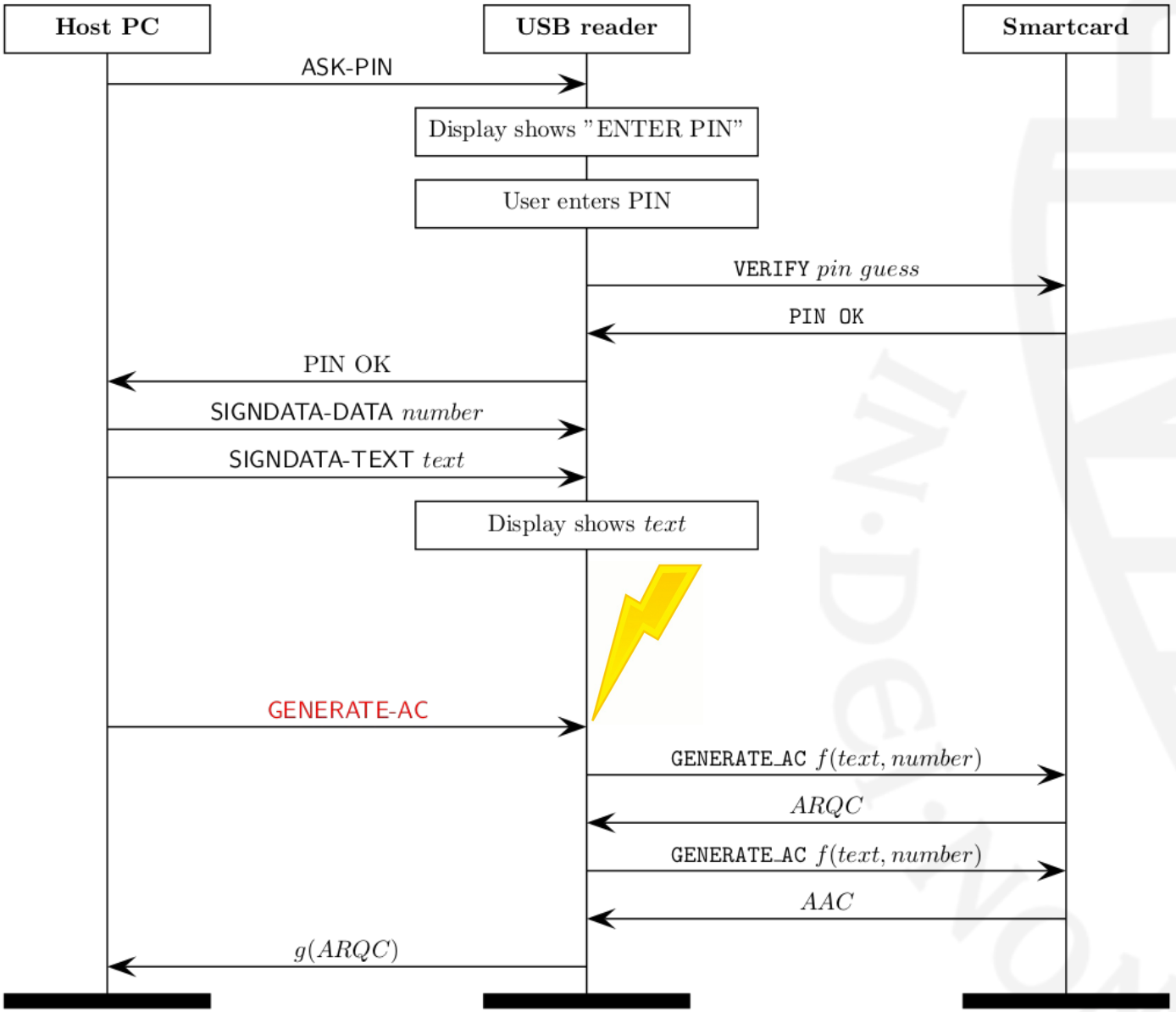
Protocol e.dentifier2



Protocol e.dentifier2

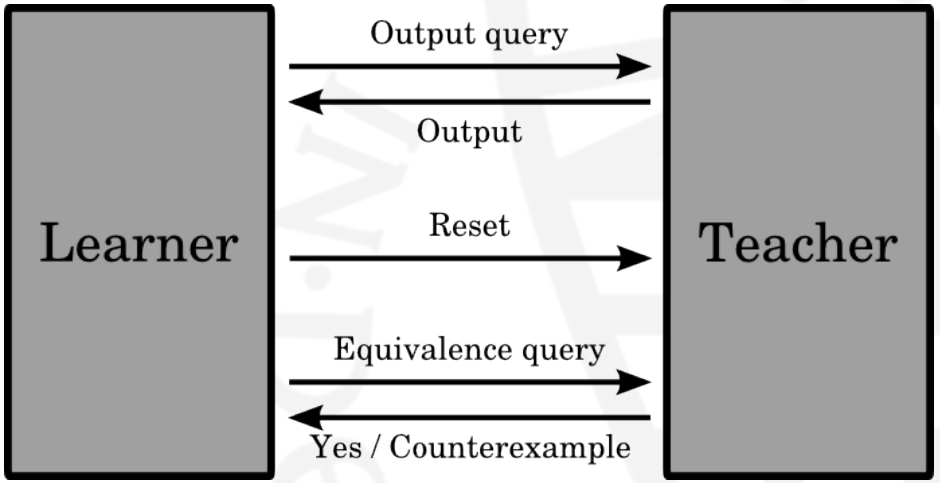


Protocol e.dentifier2



Automated learning

- Used LearnLib
  - Implementation of adapted L* algorithm
- Complete Mealy machine
- Equivalence queries approximated
  - Random traces
  - W-method



Using automated learning

- Reverse engineering
  - Manual inspection of correctness and security
- Fuzzing or model-based testing
  - Use as basis for automated fuzz testing
- Formal verification
  - Use as basis for model checking

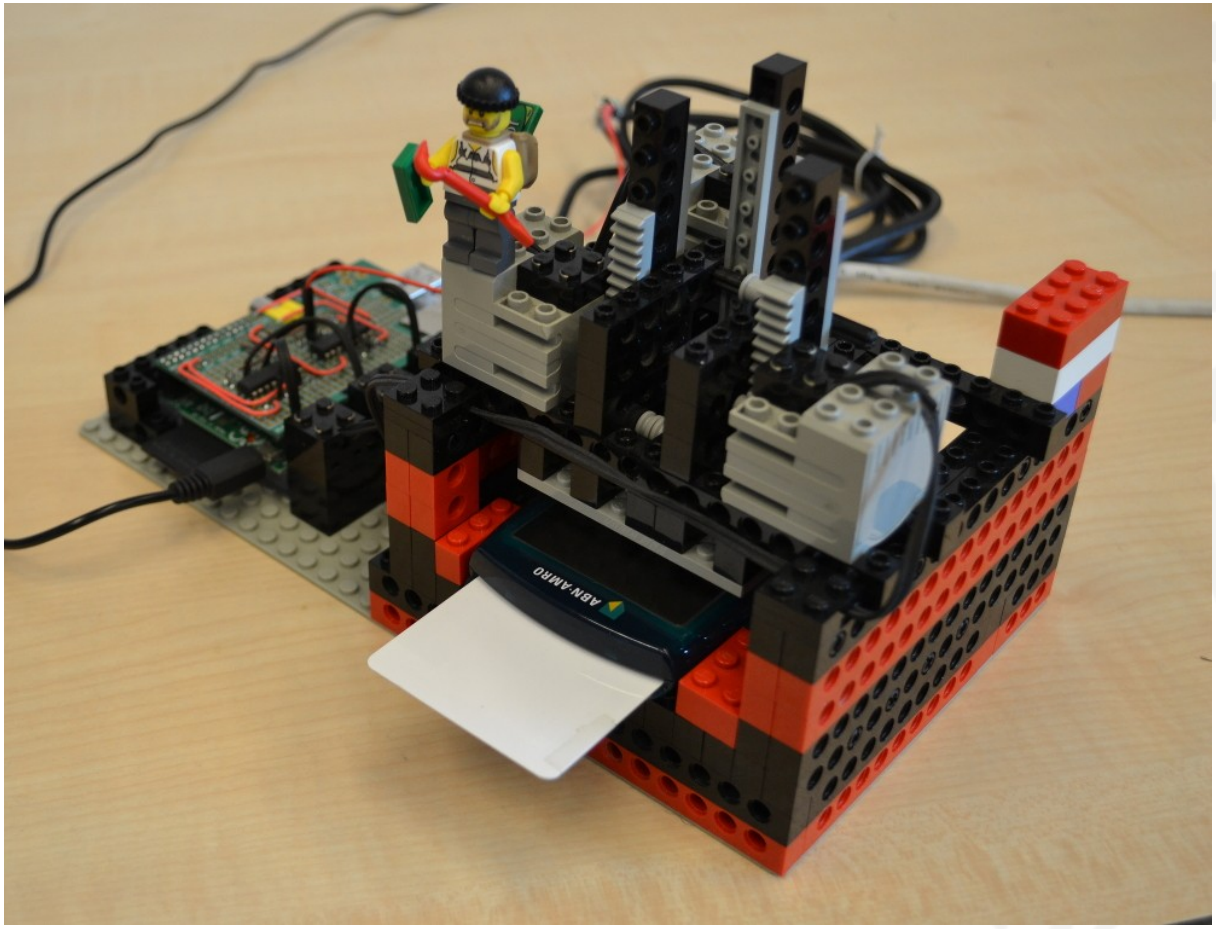
Automated reverse engineering

- Two different versions of the device
- Programmable smart card
  - All PIN codes accepted
  - Responses fixed
- Physical interaction needed

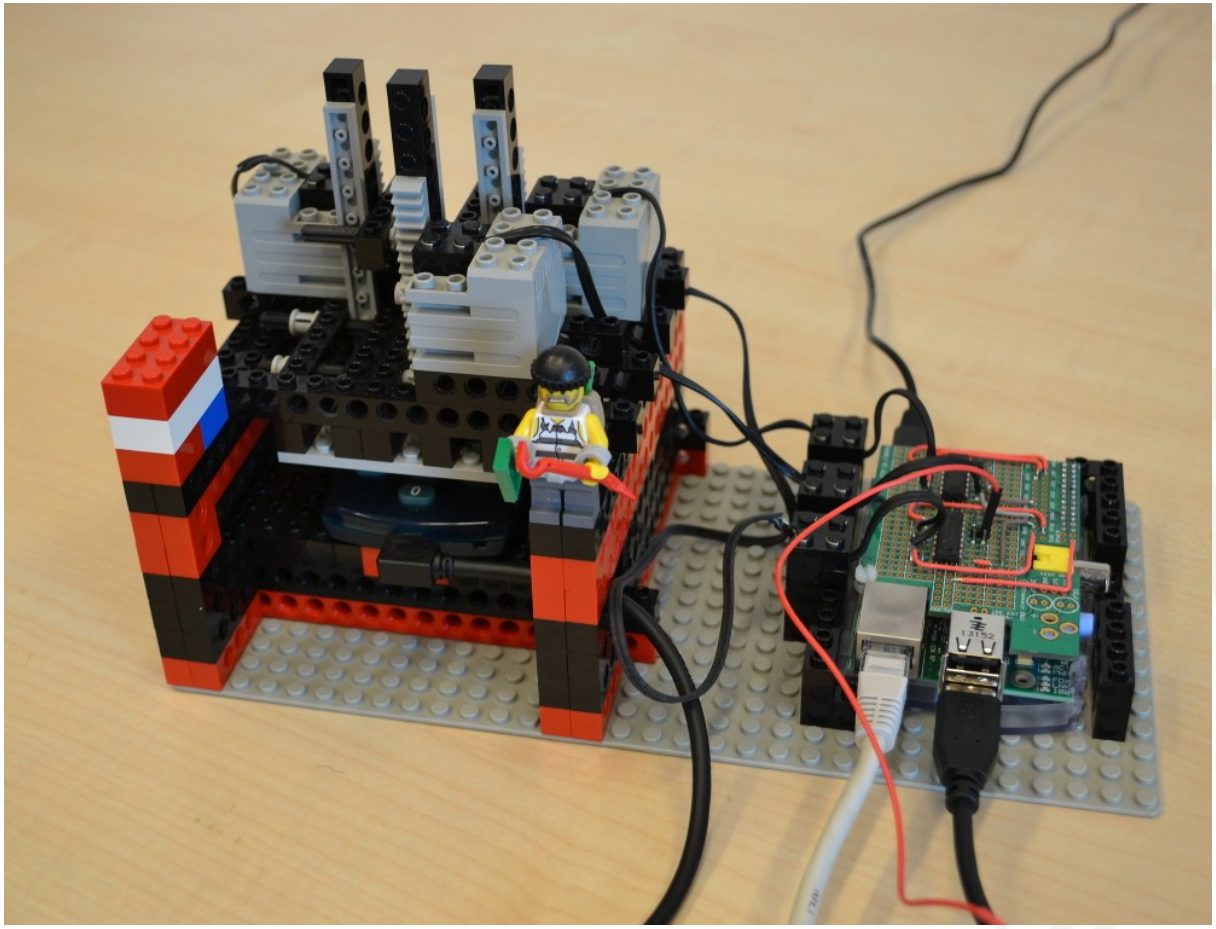
Robot

- Built using Lego
- Controlled by Raspberry Pi
  - 3 motors: OK, Cancel, digit
  - Power USB line
  - USB commands

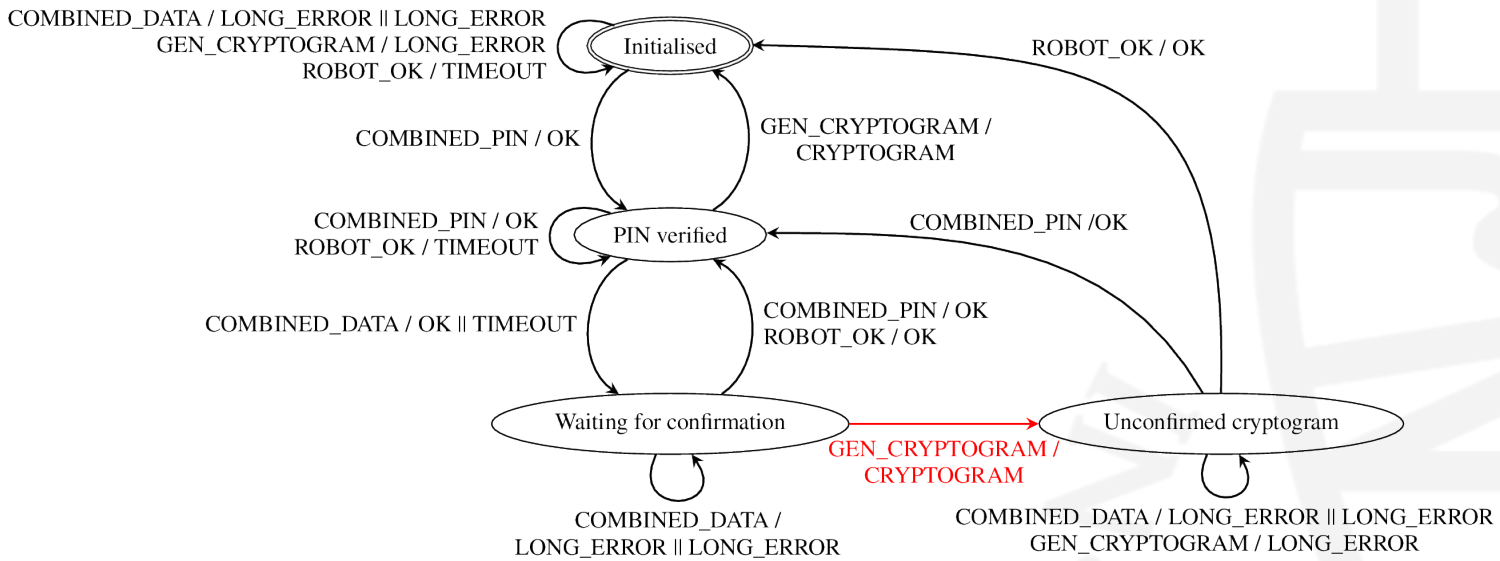
Robot

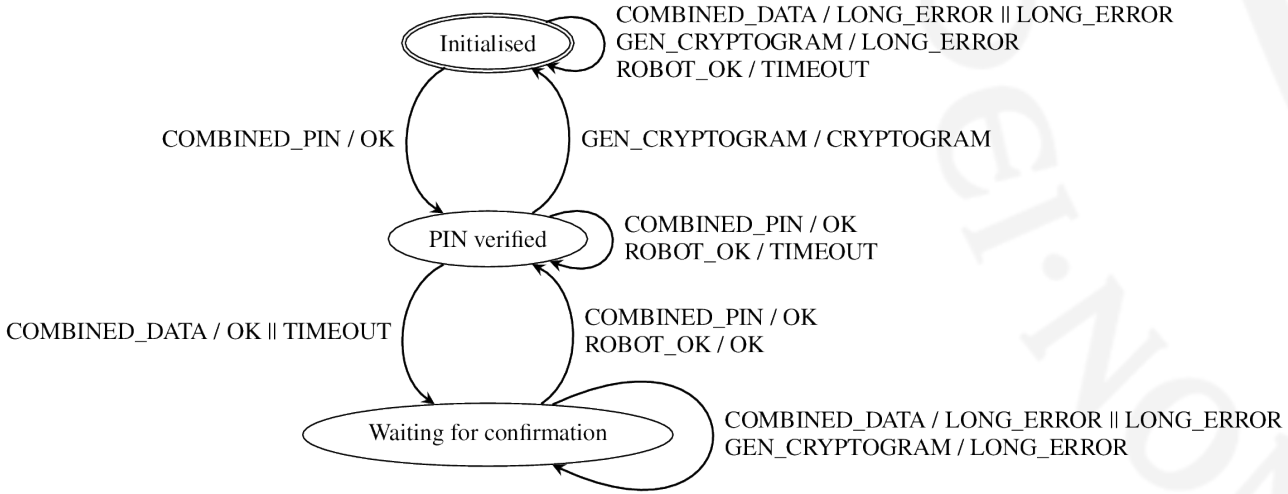


Robot

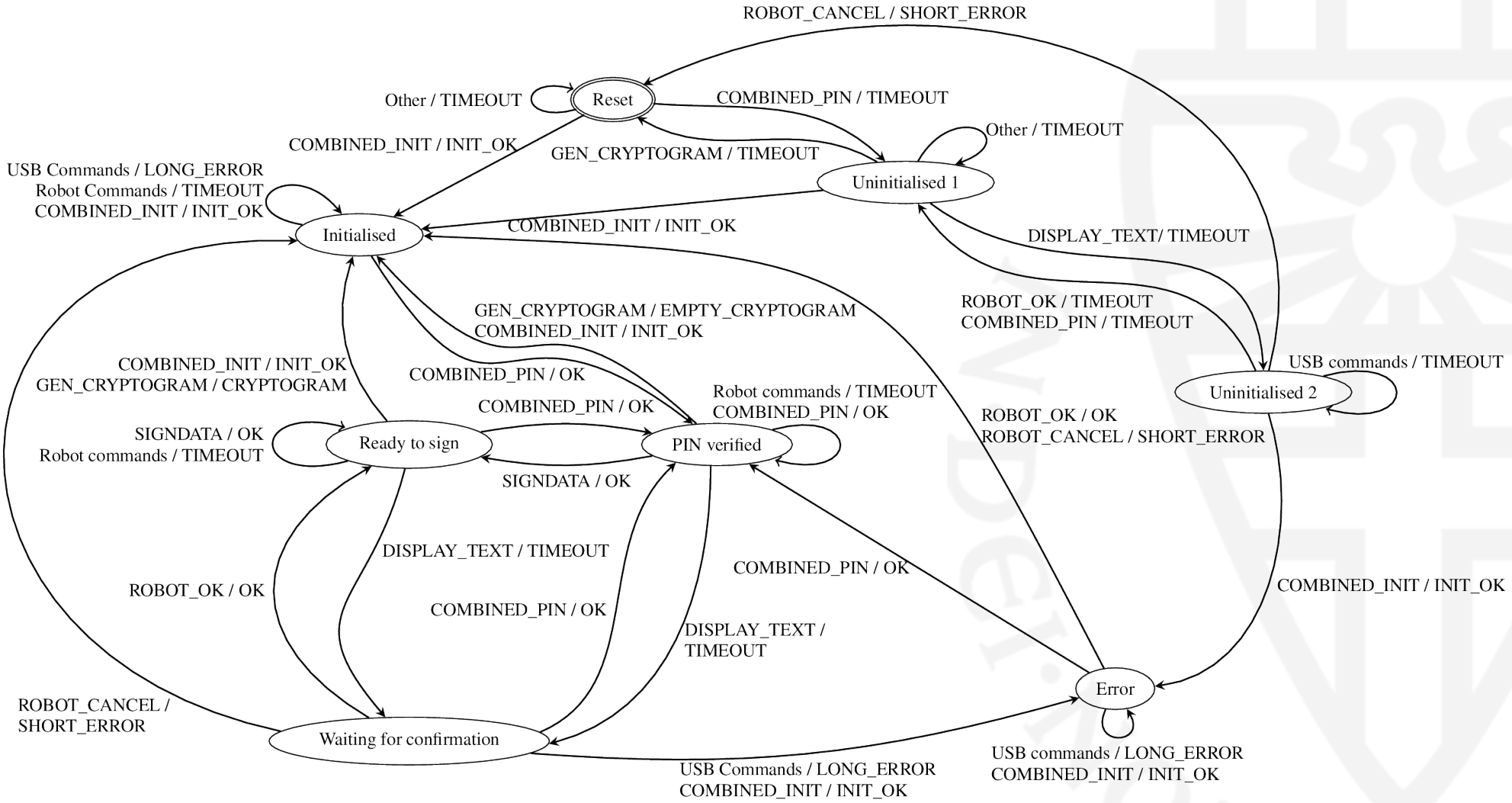


Results


COMBINED_DATA / LONG_ERROR || LONG_ERROR
GEN_CRYPTOGRAM / LONG_ERROR
ROBOT_OK / TIMEOUT
Initialised
ROBOT_OK / OK
COMBINED_PIN / OK
GEN_CRYPTOGRAM /
CRYPTOGRAM
COMBINED_PIN / OK
ROBOT_OK / TIMEOUT
PIN verified
COMBINED_PIN /OK
COMBINED_DATA / OK || TIMEOUT
COMBINED_PIN / OK
ROBOT_OK / OK
Waiting for confirmation
Unconfirmed cryptogram
GEN_CRYPTOGRAM /
CRYPTOGRAM
COMBINED_DATA /
LONG_ERROR || LONG_ERROR
COMBINED_DATA / LONG_ERROR || LONG_ERROR
GEN_CRYPTOGRAM / LONG_ERROR


Initialised
COMBINED_DATA / LONG_ERROR || LONG_ERROR
GEN_CRYPTOGRAM / LONG_ERROR
ROBOT_OK / TIMEOUT
COMBINED_PIN / OK
GEN_CRYPTOGRAM / CRYPTOGRAM
PIN verified
COMBINED_PIN / OK
ROBOT_OK / TIMEOUT
COMBINED_DATA / OK || TIMEOUT
COMBINED_PIN / OK
ROBOT_OK / OK
Waiting for confirmation
COMBINED_DATA / LONG_ERROR || LONG_ERROR
GEN_CRYPTOGRAM / LONG_ERROR

Results


ROBOT_CANCEL / SHORT_ERROR
Other / TIMEOUT
Reset
COMBINED_PIN / TIMEOUT
Other / TIMEOUT
COMBINED_INIT / INIT_OK
GEN_CRYPTOGRAM / TIMEOUT
USB Commands / LONG_ERROR
Robot Commands / TIMEOUT
COMBINED_INIT / INIT_OK
Uninitialised 1
Initialised
COMBINED_INIT / INIT_OK
DISPLAY_TEXT/ TIMEOUT
ROBOT_OK / TIMEOUT
COMBINED_PIN / TIMEOUT
GEN_CRYPTOGRAM / EMPTY_CRYPTOGRAM
COMBINED_INIT / INIT_OK
USB commands / TIMEOUT
COMBINED_INIT / INIT_OK
GEN_CRYPTOGRAM / CRYPTOGRAM
COMBINED_PIN / OK
Robot commands / TIMEOUT
COMBINED_PIN / OK
COMBINED_PIN / OK
Uninitialised 2
ROBOT_OK / OK
ROBOT_CANCEL / SHORT_ERROR
SIGNDATA / OK
Robot commands / TIMEOUT
Ready to sign
PIN verified
SIGNDATA / OK
DISPLAY_TEXT / TIMEOUT
COMBINED_PIN / OK
ROBOT_OK / OK
COMBINED_PIN / OK
COMBINED_INIT / INIT_OK
DISPLAY_TEXT / TIMEOUT
Error
ROBOT_CANCEL / SHORT_ERROR
Waiting for confirmation
USB commands / LONG_ERROR
COMBINED_INIT / INIT_OK
USB Commands / LONG_ERROR
COMBINED_INIT / INIT_OK

Model checking

- Converted output to labelled transition system
- Used model checker CADP
- Checked property in modal logic
  - Is valid cryptogram generated only after OK button is pushed?
- Resulted in an attack trace for the old device

Conclusions

- Automated learning techniques
  - Useful in security analysis for embedded devices
  - Can automatically find security vulnerabilities
  - Good excuse to play with Lego

Conclusions

- Automated learning techniques
  - Useful in security analysis for embedded devices
  - Can automatically find security vulnerabilities
  - Good excuse to play with Lego

Thanks for your attention!