Karlsruhe Institute of Technology

KASTEL

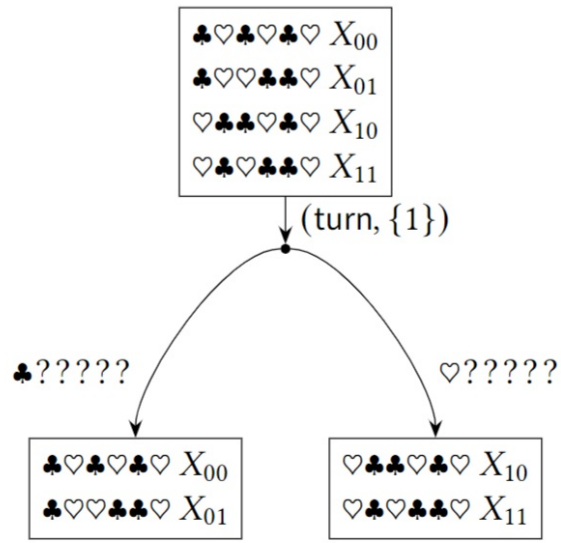
An Automated Approach to Generating Card-Based Cryptographic Protocols

Motivation and Tasks of Bachelor Thesis

Anne Hoff | November 10, 2022

Card-Based Cryptographic Protocols

- Secure multi-party computation
- Using two cards: ♣ and ♡
- 0 = ♣♡; 1 = ♡♣
- perform turns and shuffles



Motivation

Current state of research

- Card-based cryptography
  - Mostly focuses on (binary) boolean operators like AND, XOR, OR ...
  - Protocols mostly found "by hand"

Motivation

Current state of research

- Card-based cryptography
  - Mostly focuses on (binary) boolean operators like AND, XOR, OR ...
  - Protocols mostly found "by hand"
- Koch, Schrempp, and Kirsten 2021 (New Generation Computing 39(1))
  - Using bounded model checking to generate protocols
  - Still concerned with boolean operators

Motivation

Current state of research

- Card-based cryptography
  - Mostly focuses on (binary) boolean operators like AND, XOR, OR ...
  - Protocols mostly found "by hand"
- Koch, Schrempp, and Kirsten 2021 (New Generation Computing 39(1))
  - Using bounded model checking to generate protocols
  - Still concerned with boolean operators

Goal of this thesis

Finding protocols for practical problems e.g. a two-candidate election

Tasks

1. Create a modular formal verification method for finding protocols

Using a Protocol as a Module

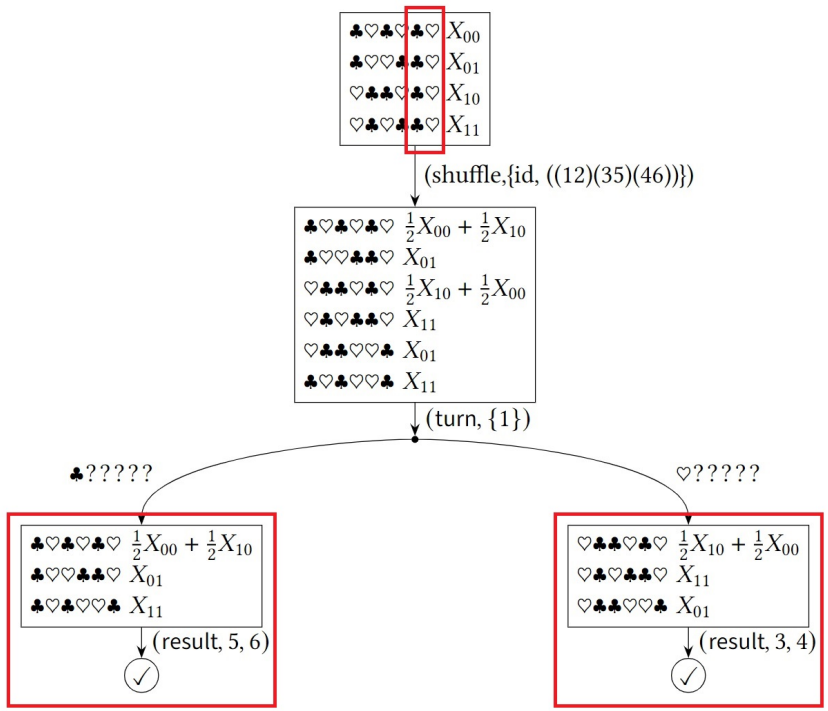


Figure: AND protocol by Mizuki and Sone 2009

Tasks

1. Create a modular formal verification method for finding protocols
2. Apply the approach to different problems

Tasks

1. Create a modular formal verification method for finding protocols
2. Apply the approach to different problems
3. Compare the approach to existing methods

Tasks

1. Create a modular formal verification method for finding protocols
2. Apply the approach to different problems
3. Compare the approach to existing methods

as well as

Optimize the existing CBMC program (Koch, Schrempp, and Kirsten 2021 New Generation Computing 39(1))
e.g different representation of the states (currently arrays) or
reducing the shuffle set size by removing redundant shuffles

Karlsruhe Institute of Technology

KASTEL

An Automated Approach to Generating Card-Based Cryptographic Protocols

Motivation and Tasks of Bachelor Thesis

Anne Hoff | November 10, 2022