Karlsruhe Institute of Technology

The Landscape of Optimal Card-Based Protocols

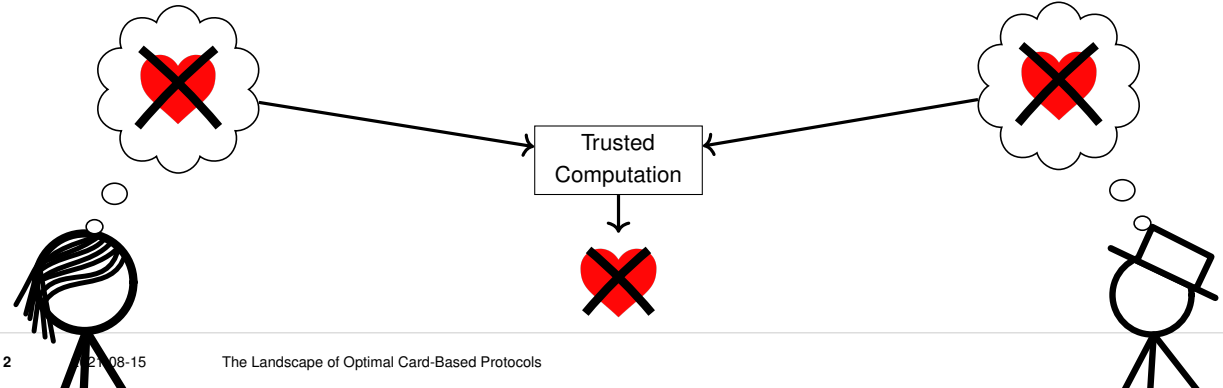
Talk at MathCrypt 2021

Alexander Koch | 15. August 2021

Motivating Scenario

- *Secrets:* Do I fancy him/her?
- *To compute:* Is there mutual interest?

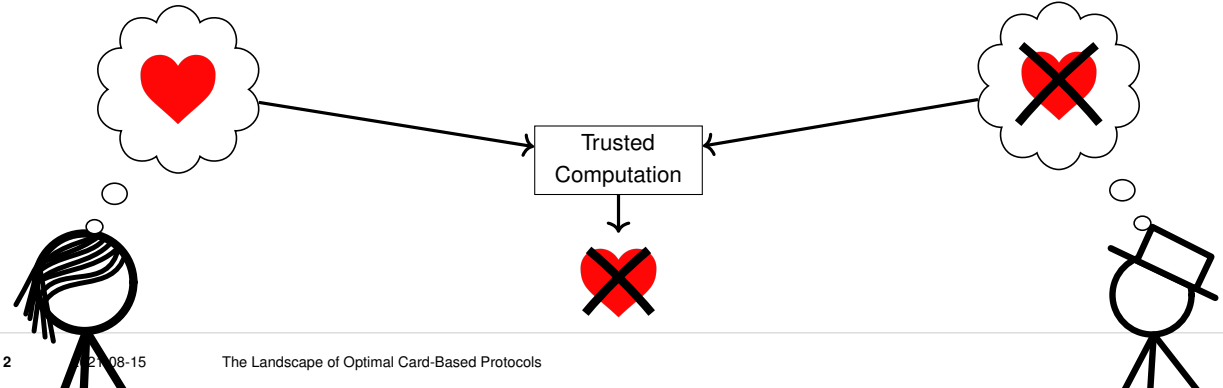
⇝ Secure 2-party AND without computers



Motivating Scenario

- *Secrets:* Do I fancy him/her?
- *To compute:* Is there mutual interest?

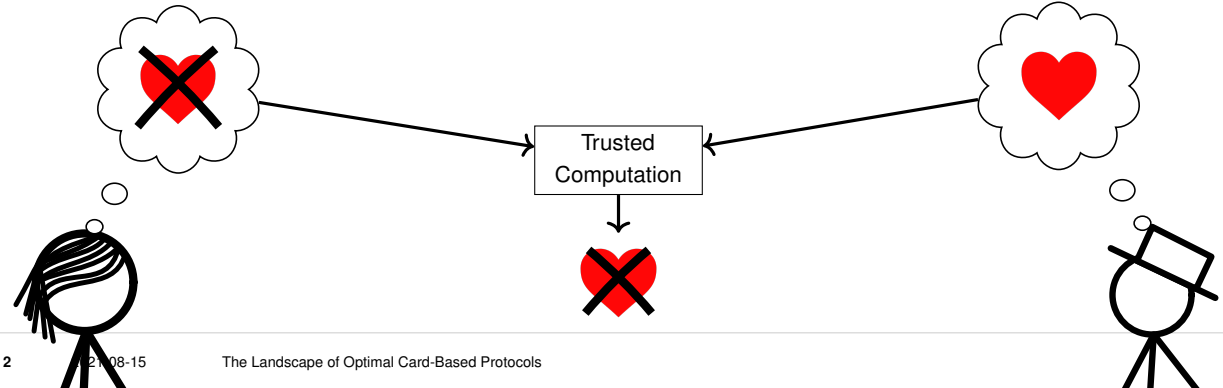
⇝ Secure 2-party AND without computers



Motivating Scenario

- *Secrets:* Do I fancy him/her?
- *To compute:* Is there mutual interest?

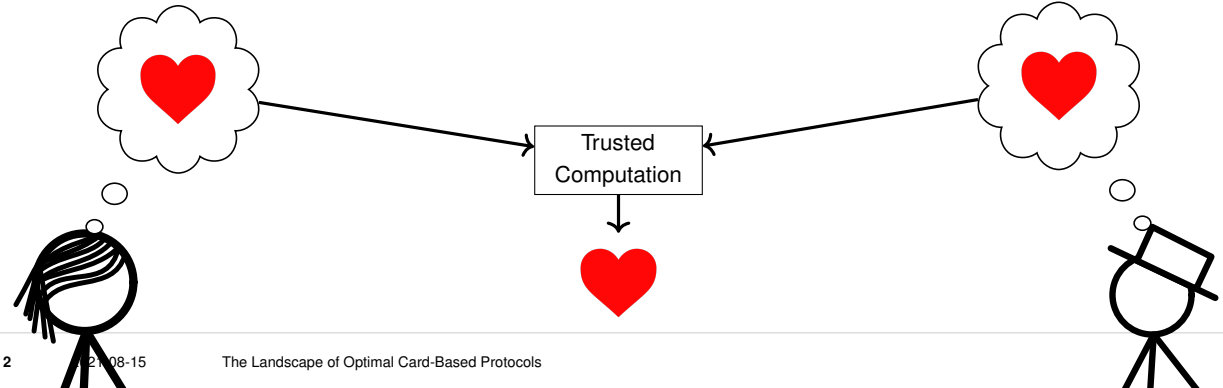
⇝ Secure 2-party AND without computers



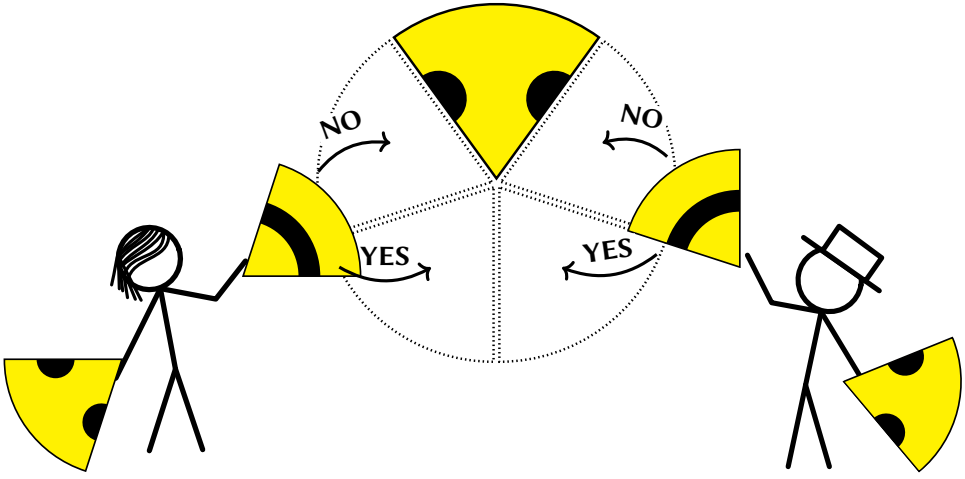
Motivating Scenario

- *Secrets:* Do I fancy him/her?
- *To compute:* Is there mutual interest?

⇝ Secure 2-party AND without computers

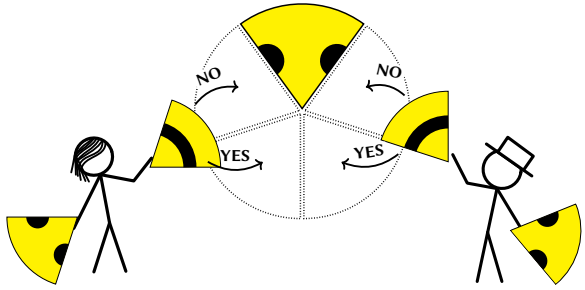


The Five-Card-Trick

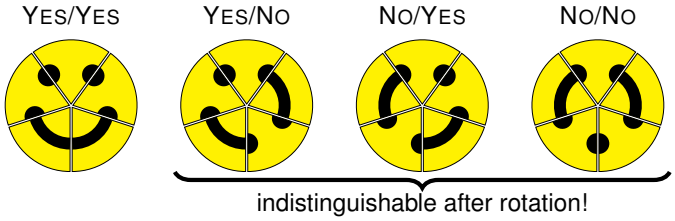


Protocol by Den Boer (1989), Version with tiles by Verhoeff (2014), Graphic by Stefan Walzer

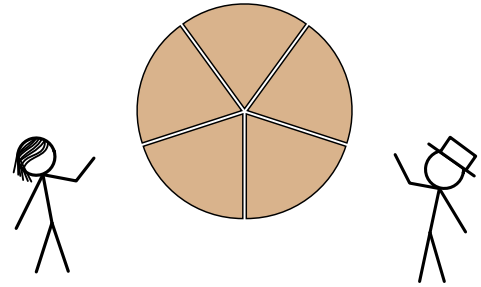
The Five-Card-Trick



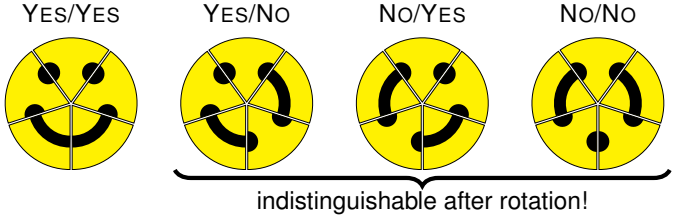
Configurations:



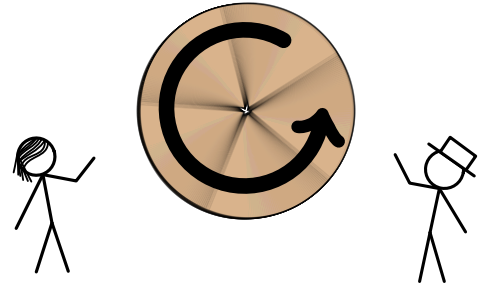
The Five-Card-Trick



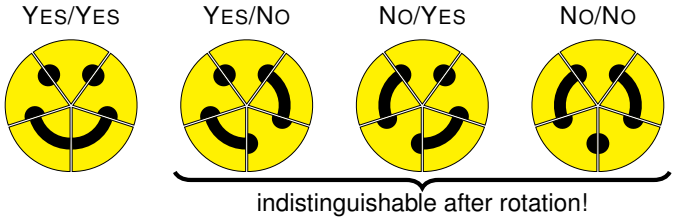
Configurations:



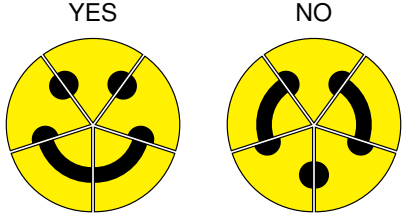
The Five-Card-Trick



Configurations:

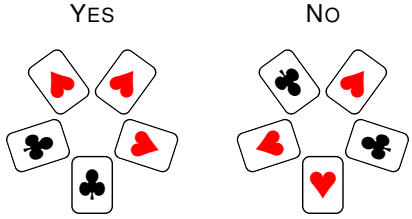


Revealing Tiles...



If you say **NO**, you do not learn anything about what the other said!

Revealing Cards... (equivalent)



If you say **NO**, you do not learn anything about what the other said!

Motivation: Explain Cryptography to Students

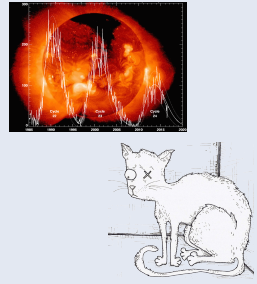
By brett jordan via flickr CC BY 2.0

Motivation II: Physical Assumptions in Cryptography

Idealized Hardware

Physical Objects

Physical Processes



Main advantages:

- Transparency and ease of understanding for the user
- Strong, otherwise unachievable, security guarantees

Research Question

We want to compute *arbitrary Boolean circuits*

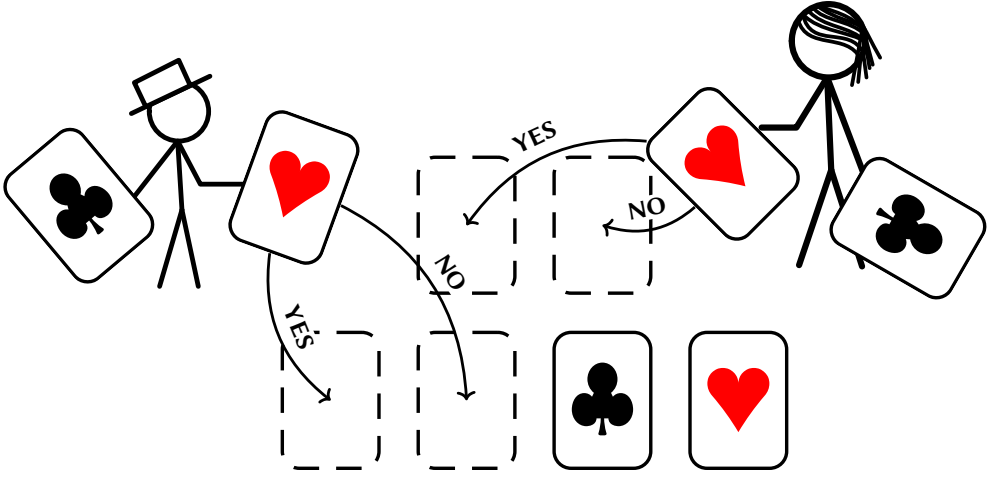
- For this, the output needs to stay *hidden*, in 2-card encoding
- We need protocols for *AND*, *NOT* and *Bit-Copy*

Question: What are the *best* protocol with hidden output?

Criteria:

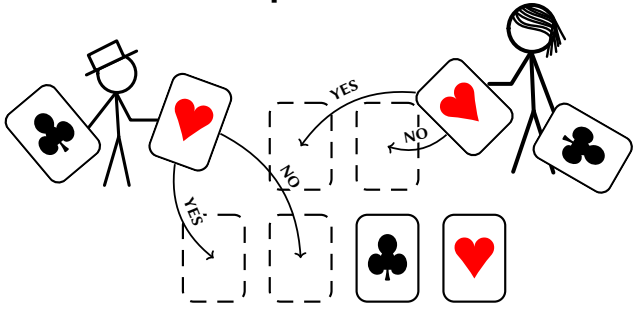
1. Number of cards used
2. Running time behavior (finite vs. Las Vegas; are restarts allowed?)
3. Number of steps
4. Practically of Shuffling steps

Computing AND with hidden output

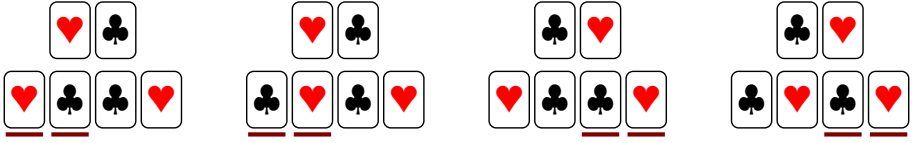


6-Card protocol by Mizuki and Sone (2009)

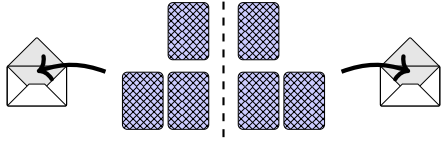
Computing AND with hidden output



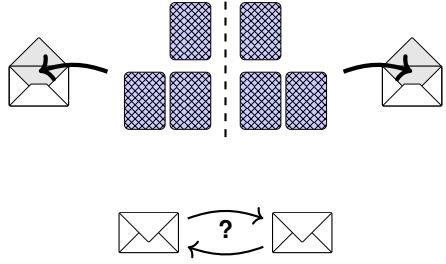
Configurations: YES/YES YES/NO NO/YES NO/NO



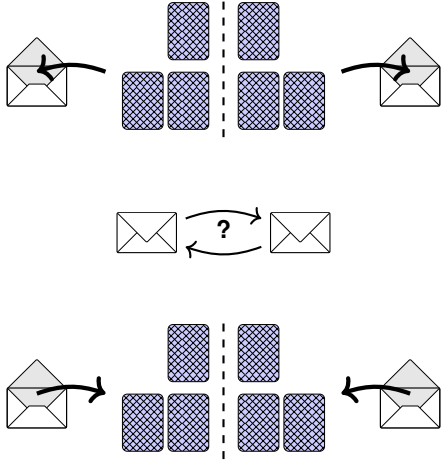
Computing AND with hidden output



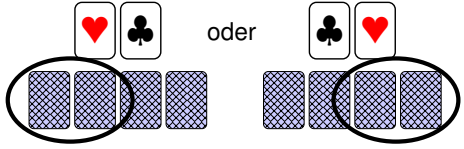
Computing AND with hidden output



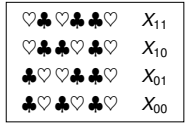
Computing AND with hidden output



Computing AND with hidden output

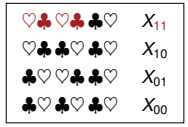


State Tree of the Protocol



Protocol State:
Currently possible sequences
with symbolic input probability
$X_{ij} = \Pr[\text{input} = (i, j)]$

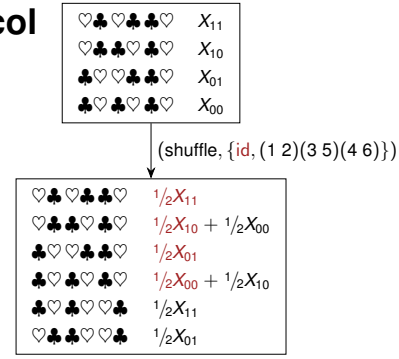
State Tree of the Protocol



Protocol State:
Currently possible sequences
with symbolic input probability
$X_{ij} = \Pr[\text{input} = (i, j)]$

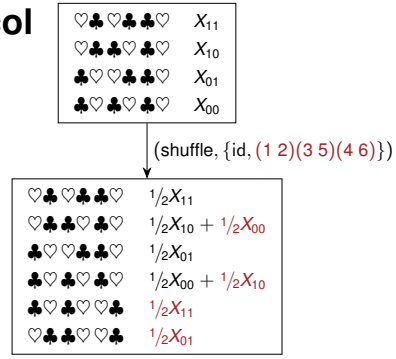
State Tree of the Protocol

Protocol State:
Currently possible sequences with symbolic input probability
$X_{ij} = \Pr[\text{input} = (i, j)]$



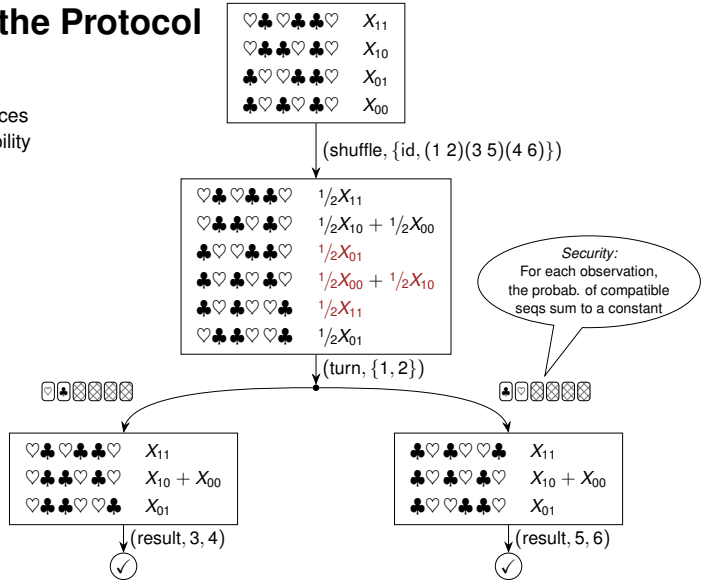
State Tree of the Protocol

Protocol State:
Currently possible sequences with symbolic input probability $X_{ij} = \Pr[\text{input} = (i, j)]$



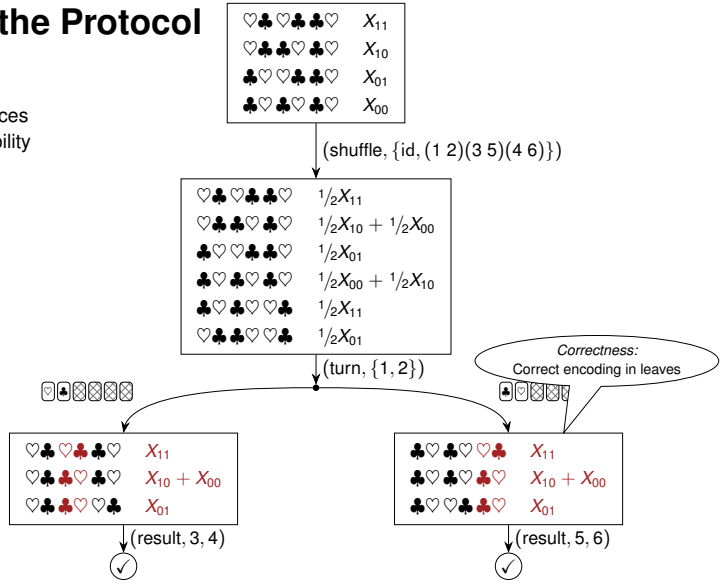
State Tree of the Protocol

Protocol State:
Currently possible sequences with symbolic input probability
$X_{ij} = \Pr[\text{input} = (i,j)]$

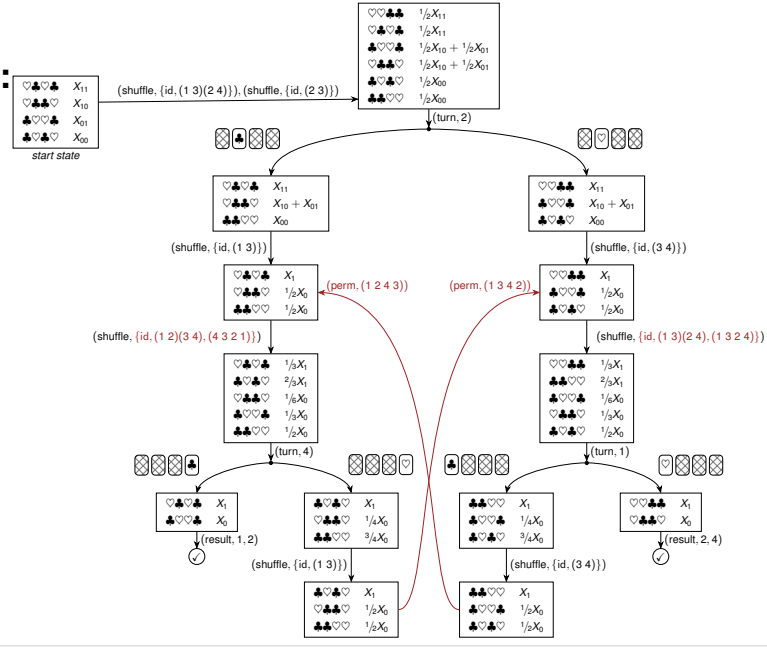


State Tree of the Protocol

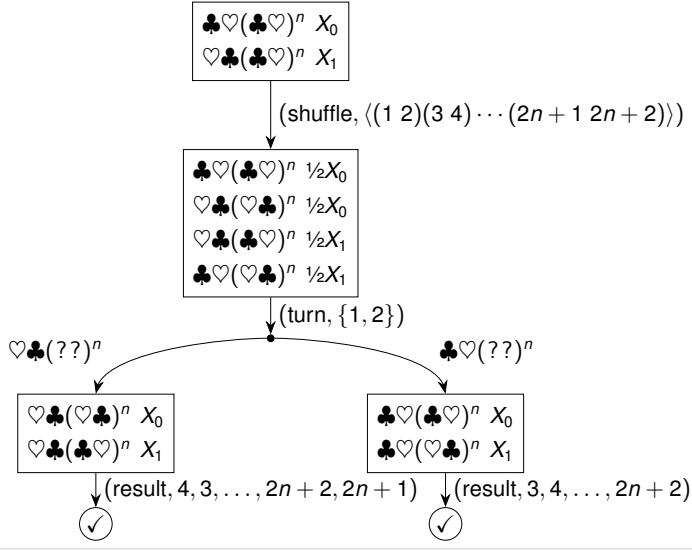
Protocol State:
Currently possible sequences with symbolic input probability $X_{ij} = \Pr[\text{input} = (i, j)]$



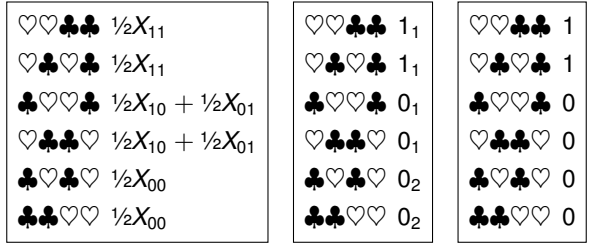
4-Card AND:


start state
(shuffle, {id, (1 3)(2 4)}), (shuffle, {id, (2 3)})
(turn, 2)
(shuffle, {id, (1 3)})
(shuffle, {id, (3 4)})
(perm, (1 2 4 3))
(perm, (1 3 4 2))
(shuffle, {id, (1 2)(3 4), (4 3 2 1)})
(shuffle, {id, (1 3)(2 4), (1 3 2 4)})
(turn, 4)
(turn, 1)
(result, 1, 2)
(result, 2, 4)
(shuffle, {id, (1 3)})
(shuffle, {id, (3 4)})

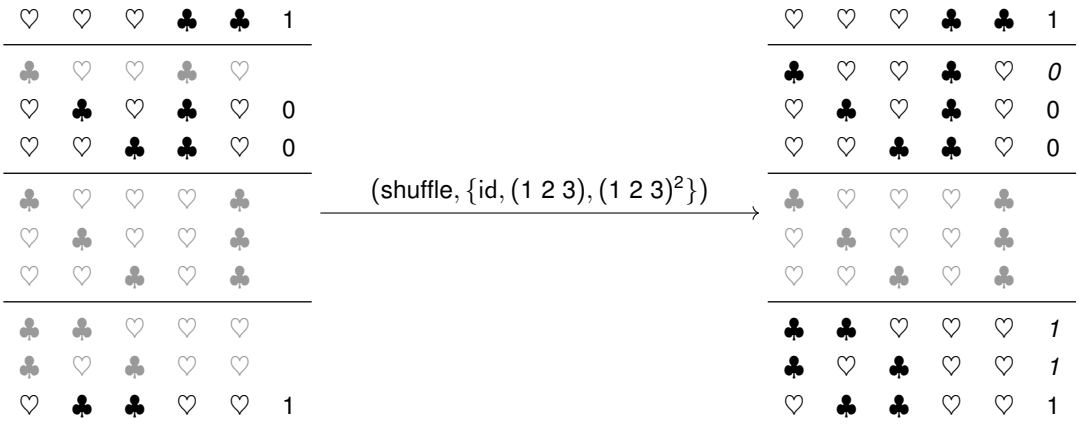
$2n + 2$-card Copy Protocol (Mizuki and Sone 2009)



Tool: “Reducing State Space”



Tool: “Closed Shuffling fills all inhabited orbits (same type)”

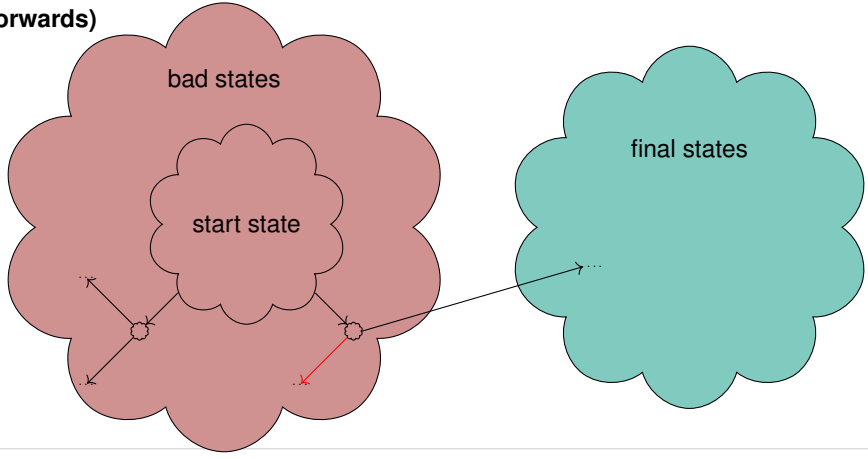


Lower Bounds Results

Theorem Type

“There is no secure AND protocol with a certain number of cards, and properties (e.g. finite runtime)”

Proof Idea (Forwards)



New Method: Going Backwards (systematically)

For

$o_1o_2\ o_3o_4$	0
$o_1o_2\ o_4o_3$	0
$o_2o_1\ o_3o_4$	1
$o_2o_1\ o_4o_3$	1

$\text{shuf}^{-1}(\cdot)$ contains:

$o_1o_2\ o_3o_4$	0
$o_1o_2\ o_4o_3$	0
$o_2o_1\ o_3o_4$	1
$o_2o_1\ o_4o_3$	1

,

$o_1o_2\ o_4o_3$	0
$o_2o_1\ o_3o_4$	1
$o_2o_1\ o_4o_3$	1

,

$o_1o_2\ o_3o_4$	0
$o_2o_1\ o_3o_4$	1
$o_2o_1\ o_4o_3$	1

,

$o_1o_2\ o_3o_4$	0
$o_1o_2\ o_4o_3$	0
$o_2o_1\ o_4o_3$	1

,

$o_1o_2\ o_3o_4$	0
$o_1o_2\ o_4o_3$	0
$o_2o_1\ o_3o_4$	1

,

$o_1o_2\ o_4o_3$	0
$o_2o_1\ o_4o_3$	1

,

$o_1o_2\ o_4o_3$	0
$o_2o_1\ o_3o_4$	1

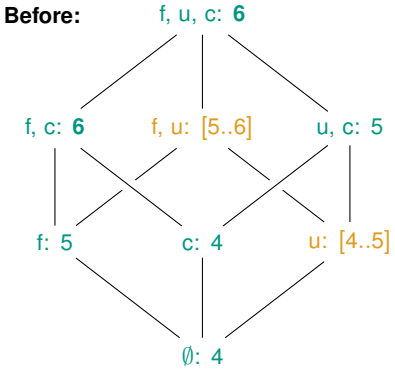
,

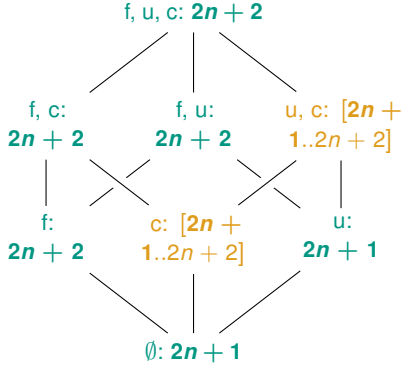
$o_1o_2\ o_3o_4$	0
$o_2o_1\ o_4o_3$	1

.

Summary

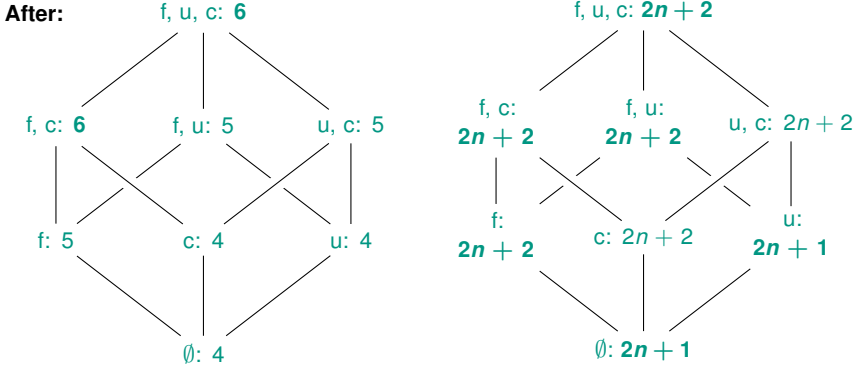
- 5 cards are (needed and) sufficient for finite-runtime **(f)** AND with uniform **(u)** shuffles
- 4 cards are (needed and) sufficient for AND with uniform shuffles
- $2n + 2$ cards are needed for COPY with closed **(c)** (and uniform closed) shuffles
- lower bounds for protocols even hold when allowing restarts





Summary

- 5 cards are (needed and) sufficient for finite-runtime **(f)** AND with uniform **(u)** shuffles
- 4 cards are (needed and) sufficient for AND with uniform shuffles
- $2n + 2$ cards are needed for COPY with closed **(c)** (and uniform closed) shuffles
- lower bounds for protocols even hold when allowing restarts



Literature


Bert den Boer. “More Efficient Match-Making and Satisfiability: The Five Card Trick”. In: *EUROCRYPT 1989*. Ed. by Jean-Jacques Quisquater and Joos Vandewalle. Vol. 434. LNCS. Springer, 1989, pp. 208–217. ISBN: 3-540-53433-4. DOI: 10.1007/3-540-46885-4_23.


Takaaki Mizuki and Hideaki Sone. “Six-Card Secure AND and Four-Card Secure XOR”. In: *FAW 2009*. LNCS 5598. Springer, 2009, pp. 358–369. DOI: 10.1007/978-3-642-02270-8_36.


Tom Verhoeff. *The Zero-Knowledge Match Maker*. June 18, 2014. URL: https://www.win.tue.nl/~wstomv/publications/liber-AMiCorum-arjeh-bijdrage-van-tom-verhoeff.pdf (visited on 08/23/2019).