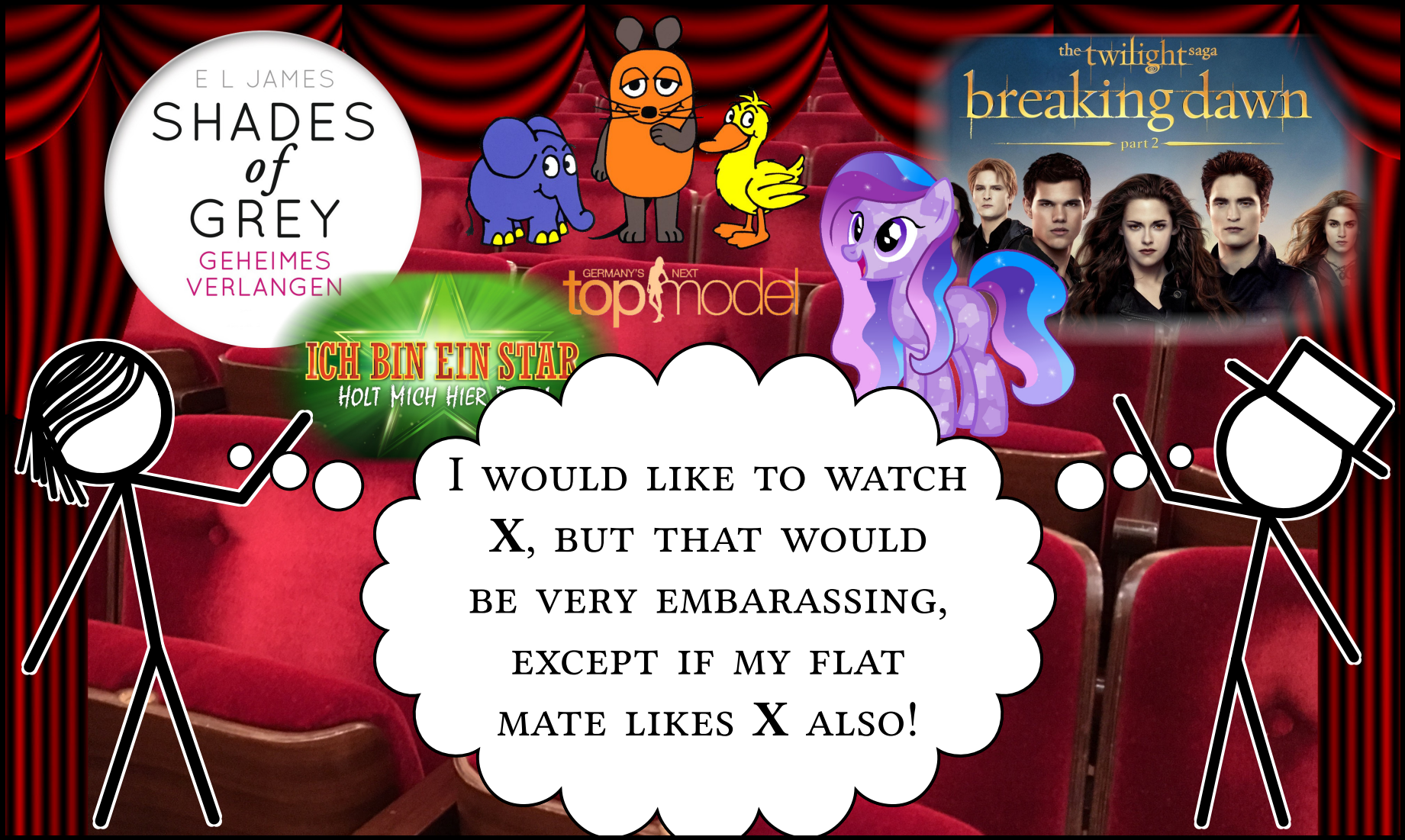
Karlsruhe Institute of Technology

The Minimum Number of Cards in Practical Card-based Protocols

ASIACRYPT 2017 | Julia Kastner, Alexander Koch, Stefan Walzer, Daiki Miyahara, Yu-ichi Hayashi, Takaaki Mizuki, Hideaki Sone

KARLSRUHE INSTITUTE OF TECHNOLOGY, TU ILMENAU, TŌHOKU UNIVERSITY, NARA INSTITUTE OF SCIENCE AND TECHNOLOGY

Problems at a Movie Evening...



Seats/curtains CC-0, Alice/Bob adapted from xkcd (by Randal Munroe) CC-BY-NC-2.5, logos copyrighted

First Try: Cryptographic Protocols in Software

(smartphone frame/devil CC-0, checkmark CC-BY-SA-3.0 Unported by S eschke, l gos copyrighted)

First Try: Cryptographic Protocols in Software

(smartphone frame/devil CC-0, checkmark CC-BY-SA-3.0 Unported by S eschke, l gos copyrighted)

First Try: Cryptographic Protocols in Software

(smartphone frame/devil CC-0, checkmark CC-BY-SA-3.0 Unported by S[illegible]eschke, logos copyrighted)

First Try: Cryptographic Protocols in Software

(smartphone frame/devil CC-0, checkmark CC-BY-SA-3.0 Unported by S eschke, l gos copyrighted)

First Try: Cryptographic Protocols in Software

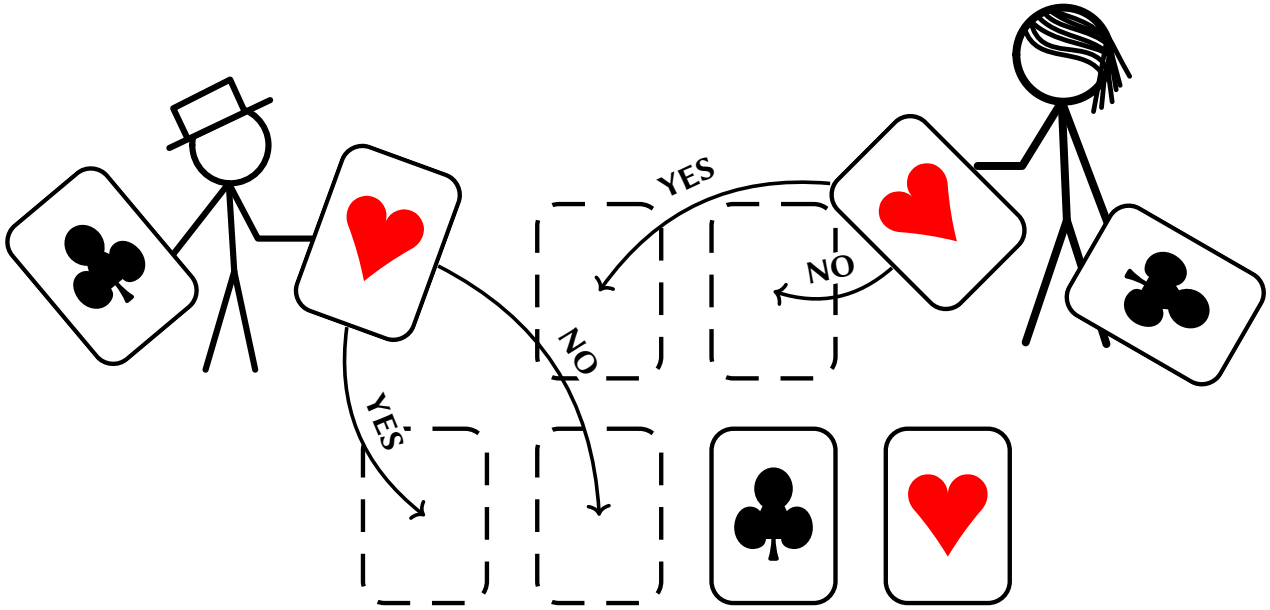
(smartphone frame/devil CC-0, checkmark CC-BY-SA-3.0 Unported by S eschke, l gos copyrighted)

Motivation II: Didactic Contexts

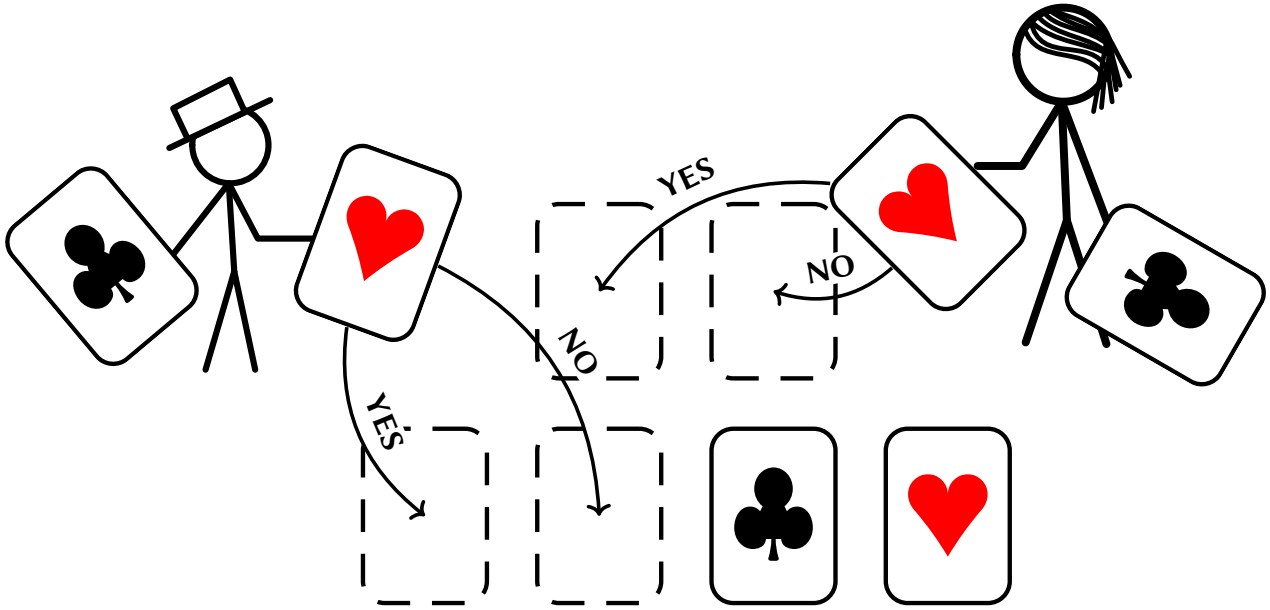
Introduce cryptography to young people and students

By brett jordan via flickr CC-BY-2.0

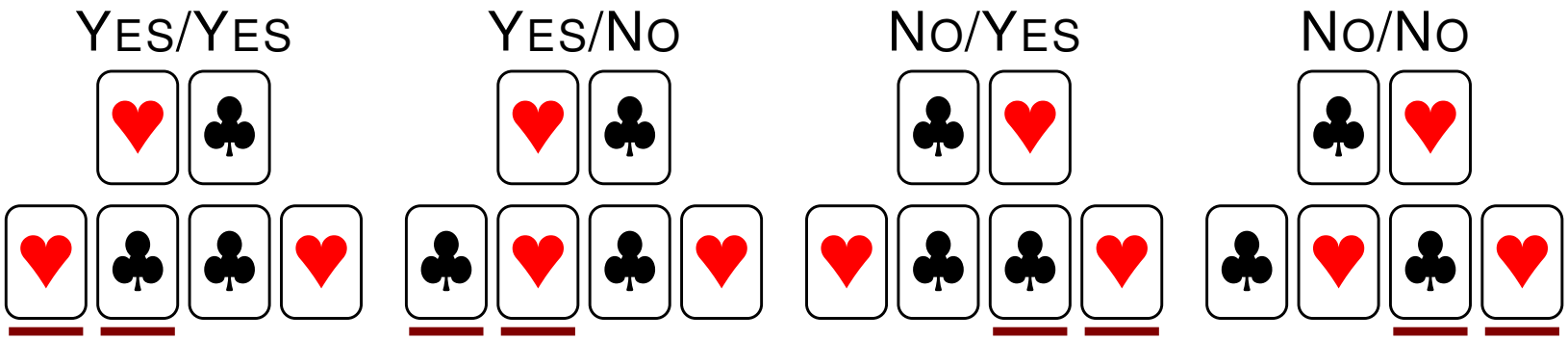
Computing AND with Six Cards [MS09]



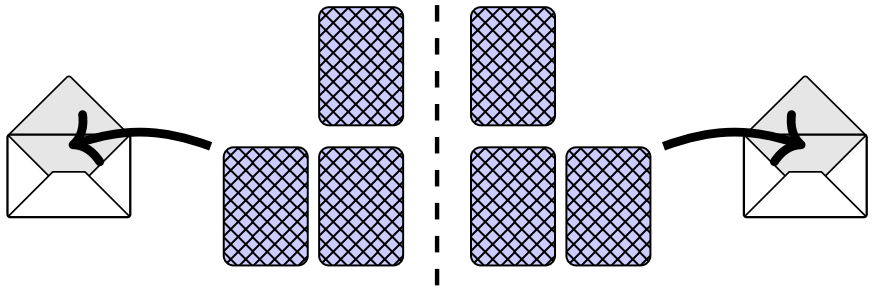
Computing AND with Six Cards [MS09]



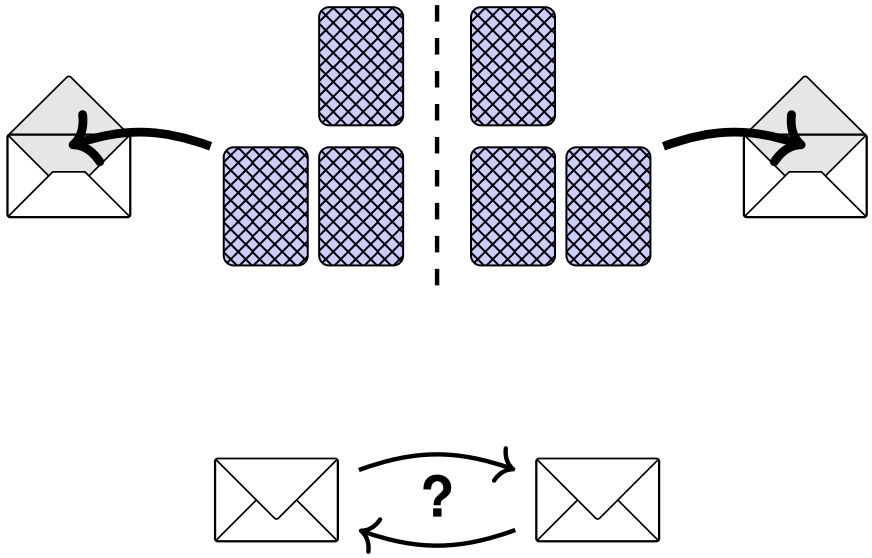
Configurations:



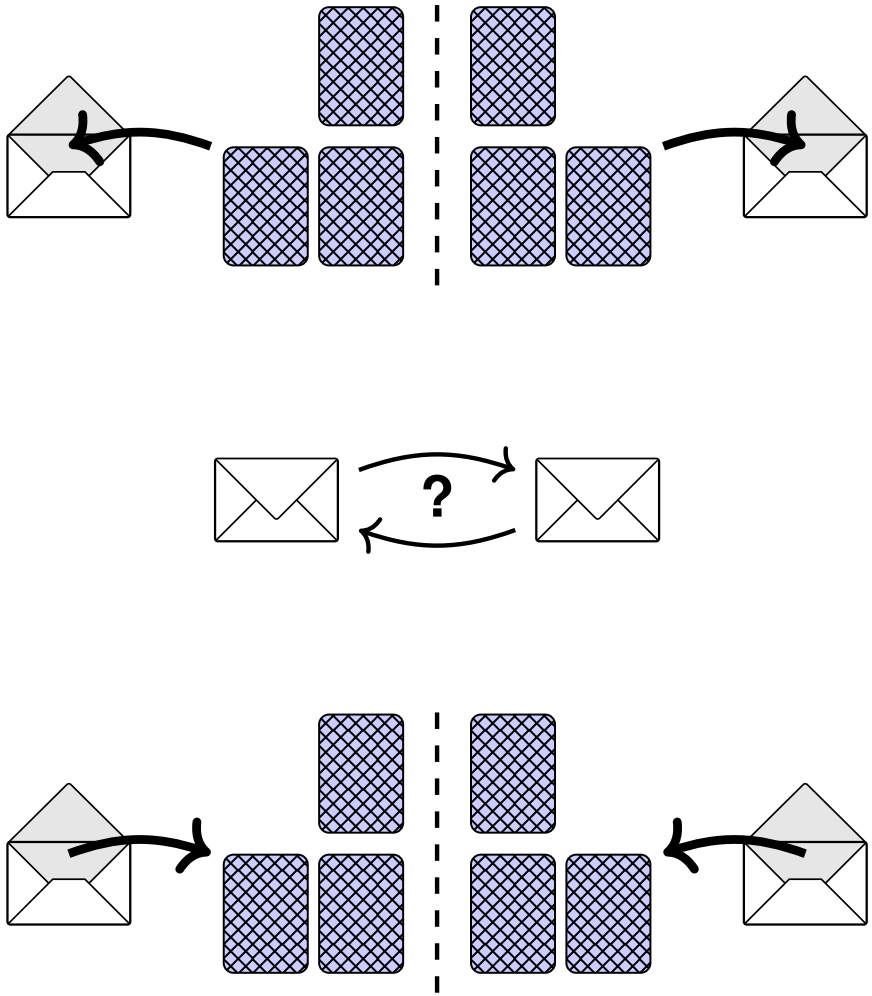
Computing AND with Six Cards [MS09]



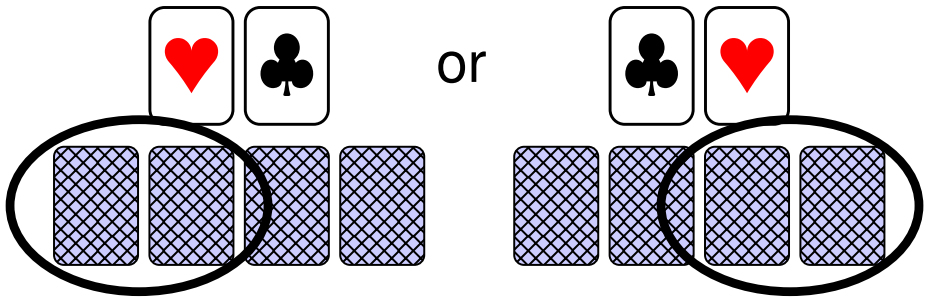
Computing AND with Six Cards [MS09]



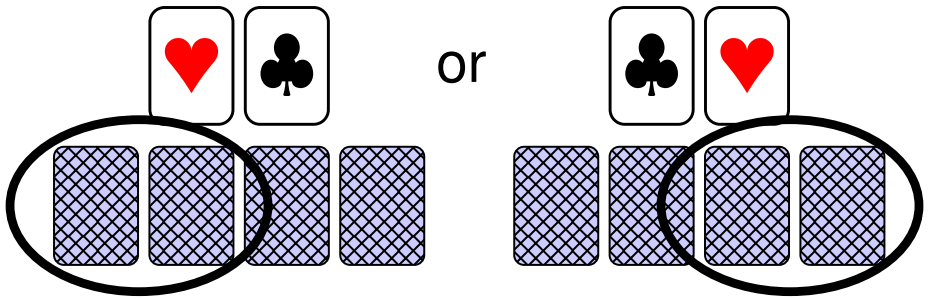
Computing AND with Six Cards [MS09]



Computing AND with Six Cards [MS09]

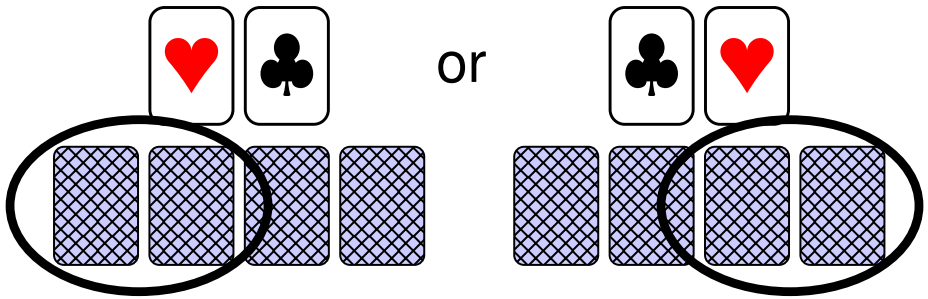


Computing AND with Six Cards [MS09]



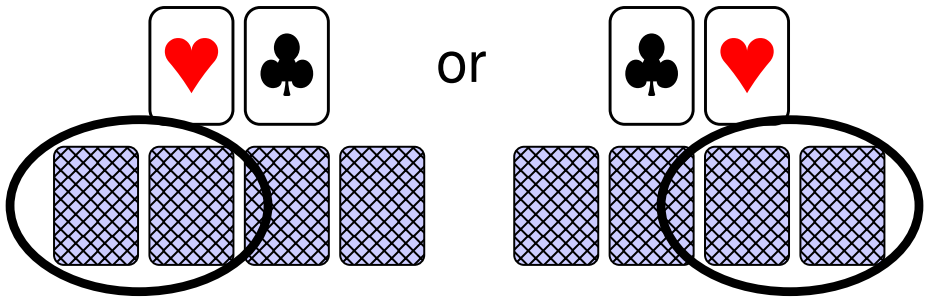
Main Question: 1. Can we do with less cards?

Computing AND with Six Cards [MS09]



Main Question: 1. Can we do with less cards? Yes [KWH15]

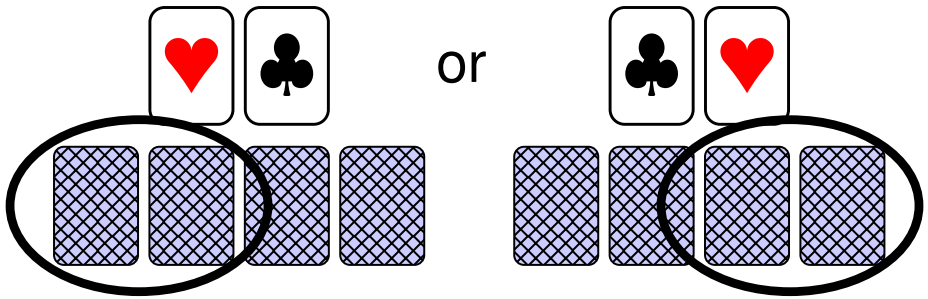
Computing AND with Six Cards [MS09]



Main Question: 1. Can we do with less cards? Yes [KWH15]

And still be very practical?

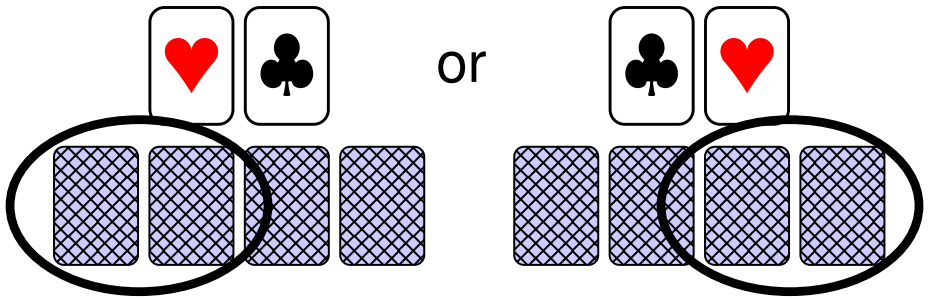
Computing AND with Six Cards [MS09]



Main Question: 1. Can we do with less cards? Yes [KWH15]

And still be very practical? (Partially:) No (this talk).

Computing AND with Six Cards [MS09]



Main Question: 1. Can we do with less cards? Yes [KWH15]

And still be very practical? (Partially:) No (this talk).

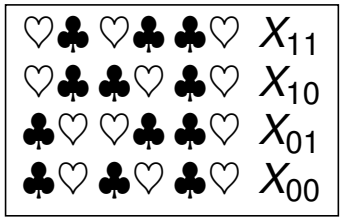
2. For arbitrary circuits, we additionally need COPY.
How many cards are necessary here?

State Tree of the Protocol

Karlsruher Institut für Technologie

Protocol State:

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

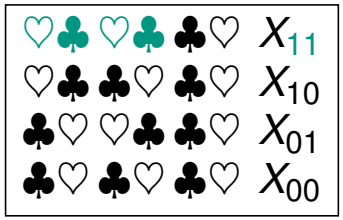


State Tree of the Protocol

Karlsruher Institut für Technologie

Protocol State:

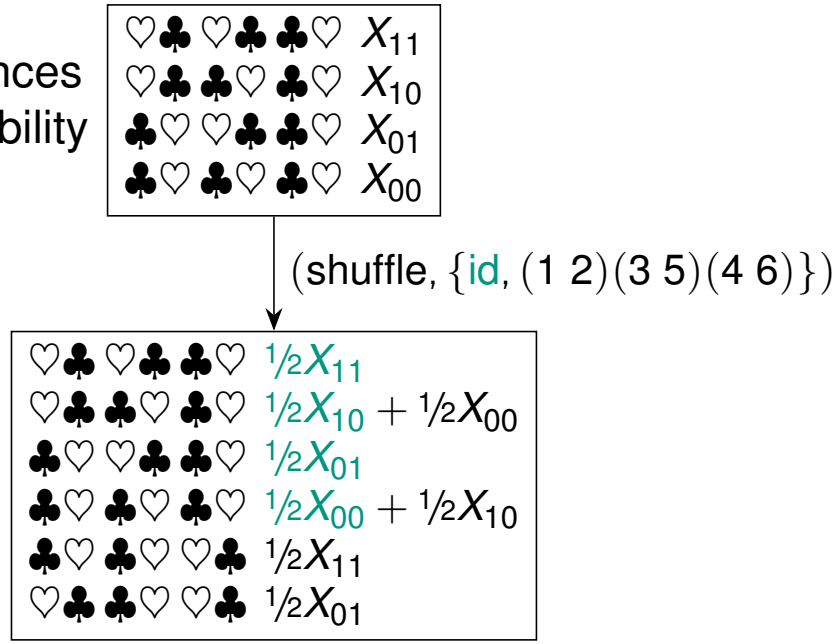
Currently possible sequences with symbolic input probability $X_{ij} = \Pr[\text{input} = (i, j)]$



State Tree of the Protocol

Protocol State:

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

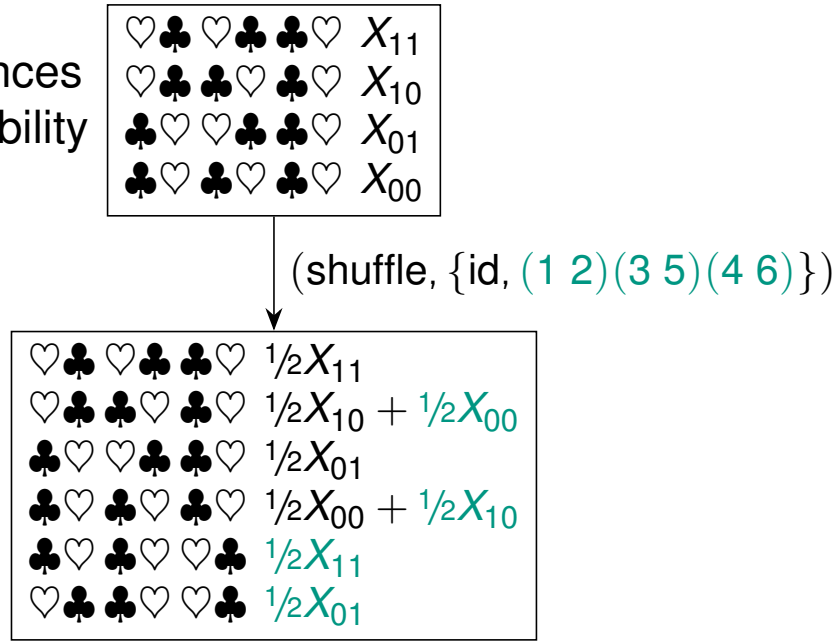


State Tree of the Protocol

Karlsruher Institut für Technologie

Protocol State:

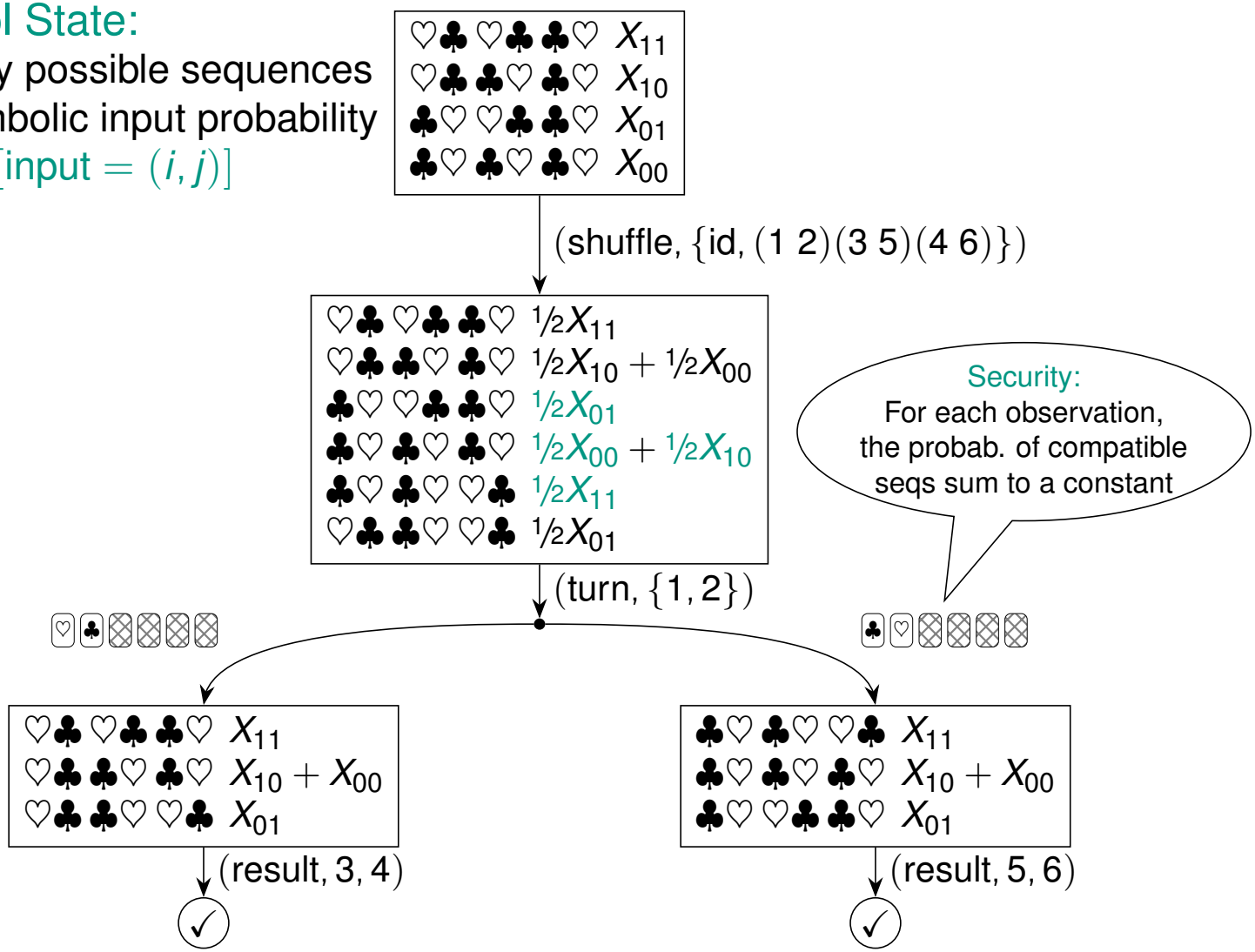
Currently possible sequences with symbolic input probability $X_{ij} = \Pr[\text{input} = (i, j)]$



State Tree of the Protocol

Protocol State:

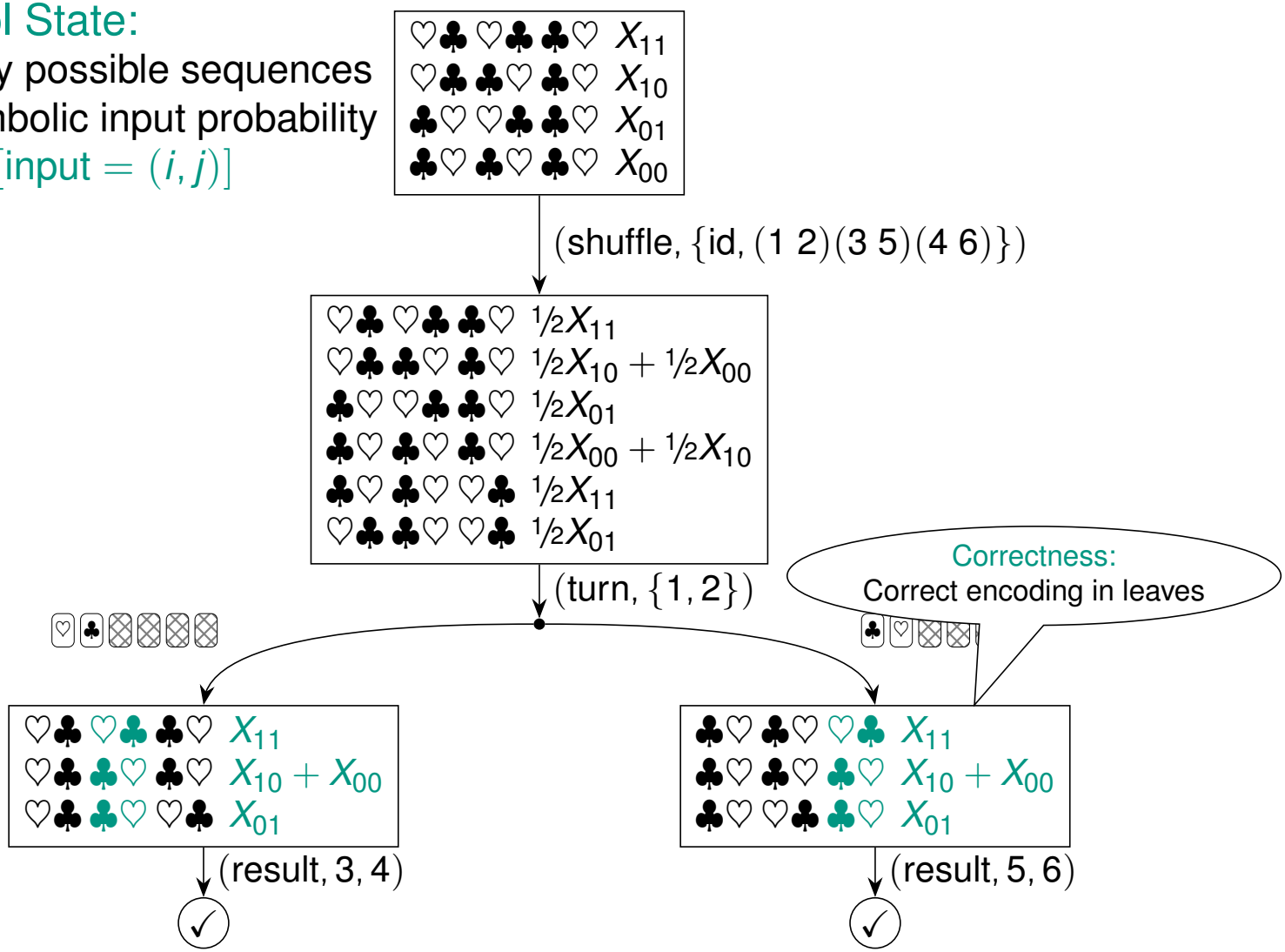
Currently possible sequences with symbolic input probability $X_{ij} = \Pr[\text{input} = (i, j)]$



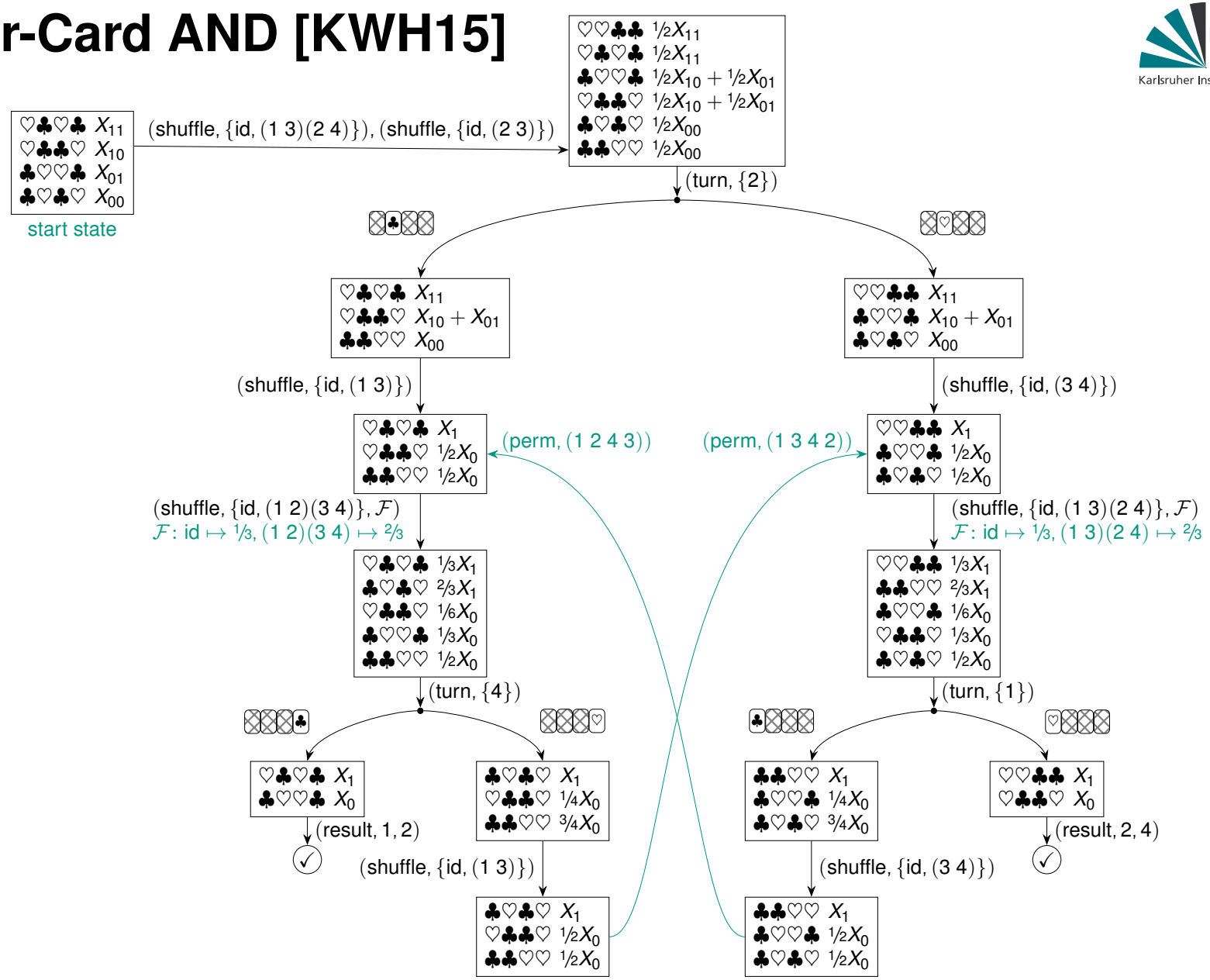
State Tree of the Protocol

Protocol State:

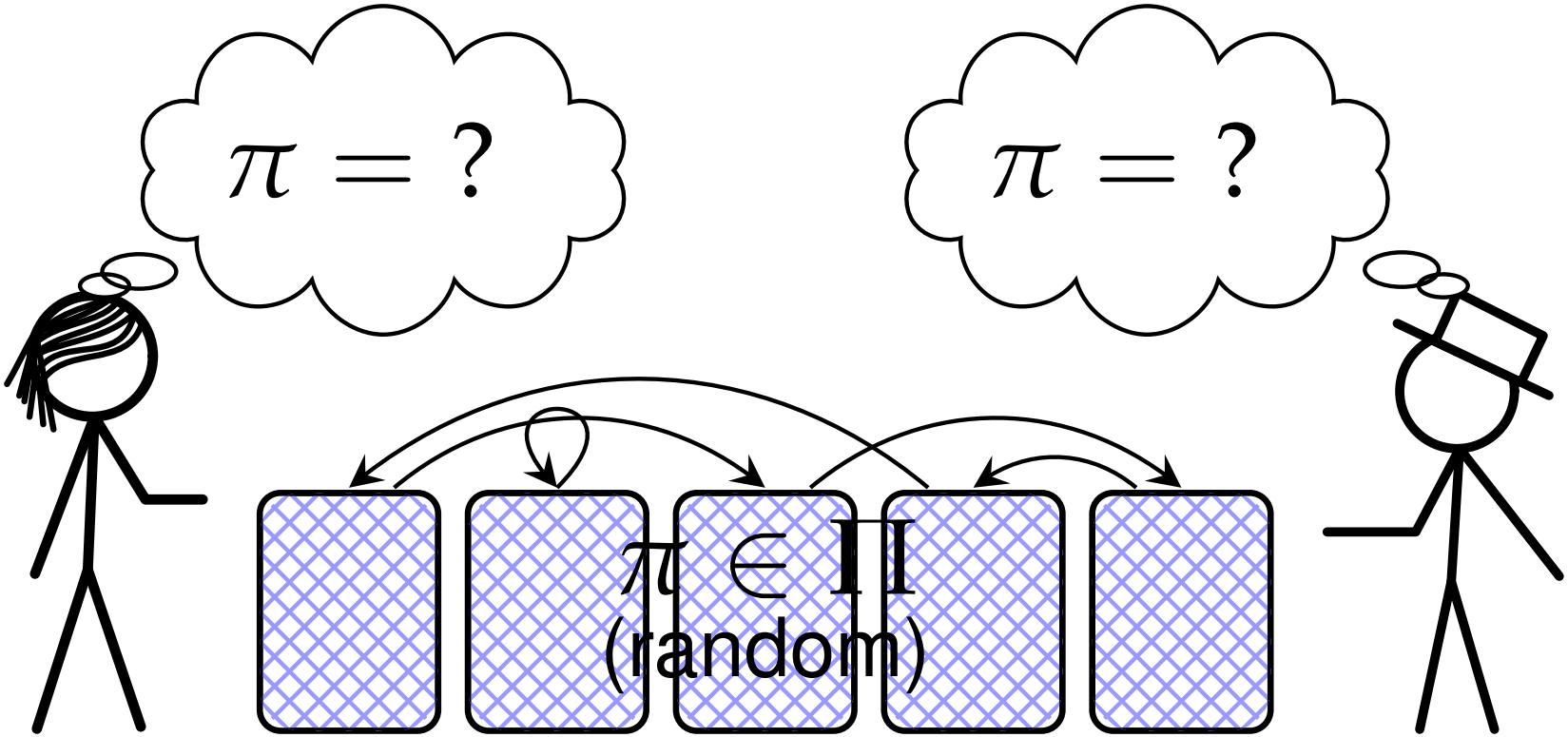
Currently possible sequences with symbolic input probability $X_{ij} = \Pr[\text{input} = (i, j)]$



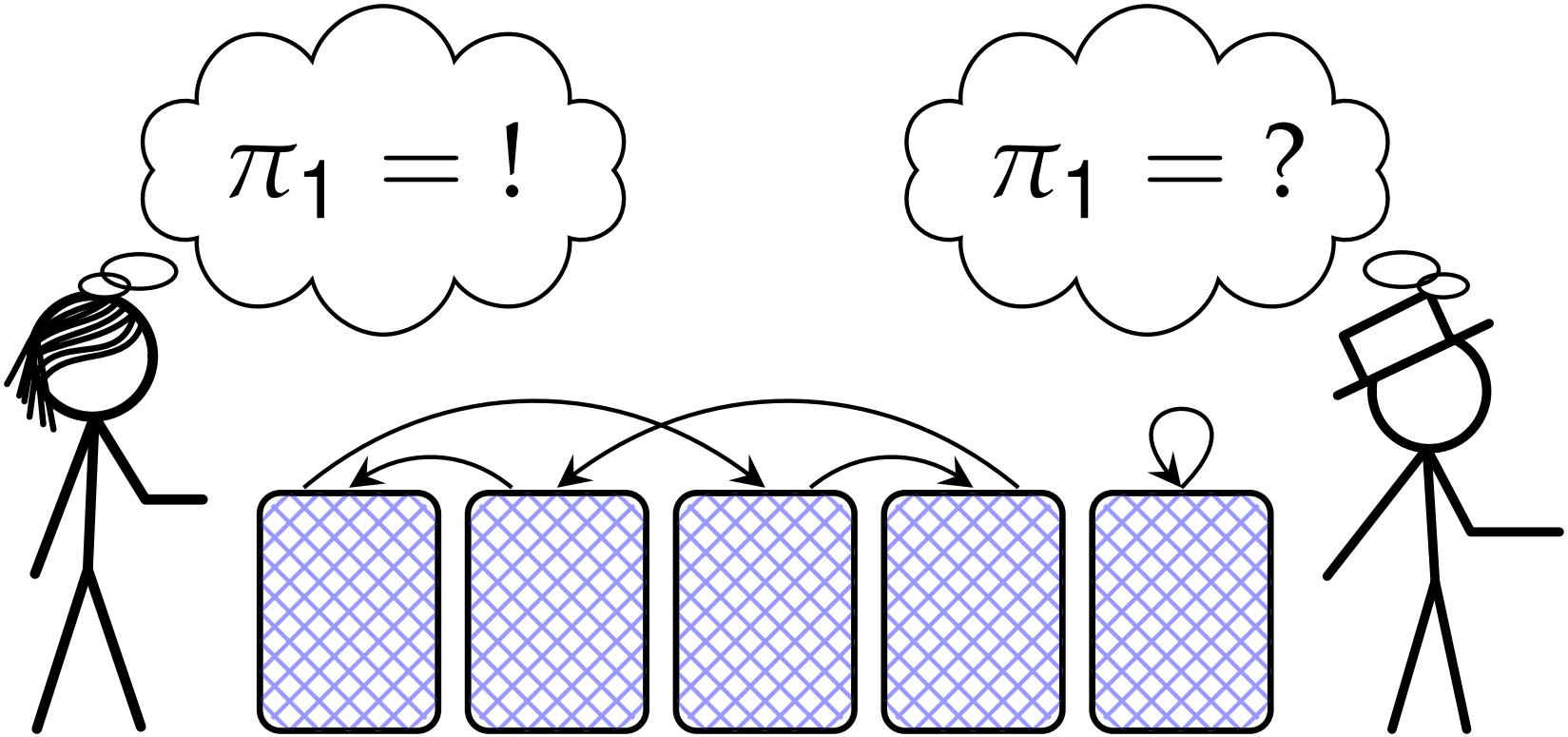
Four-Card AND [KWH15]



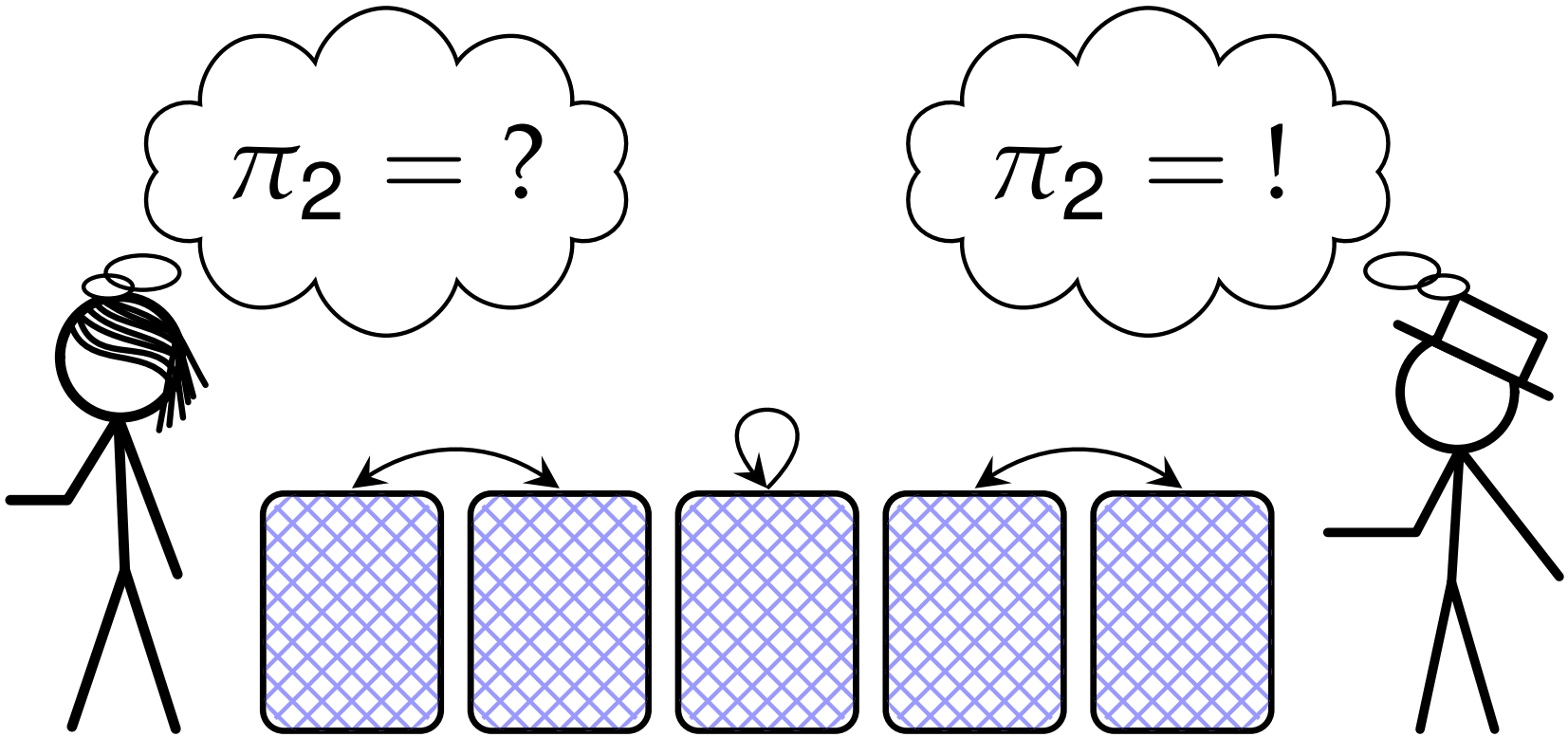
Why uniform closed shuffles are nice



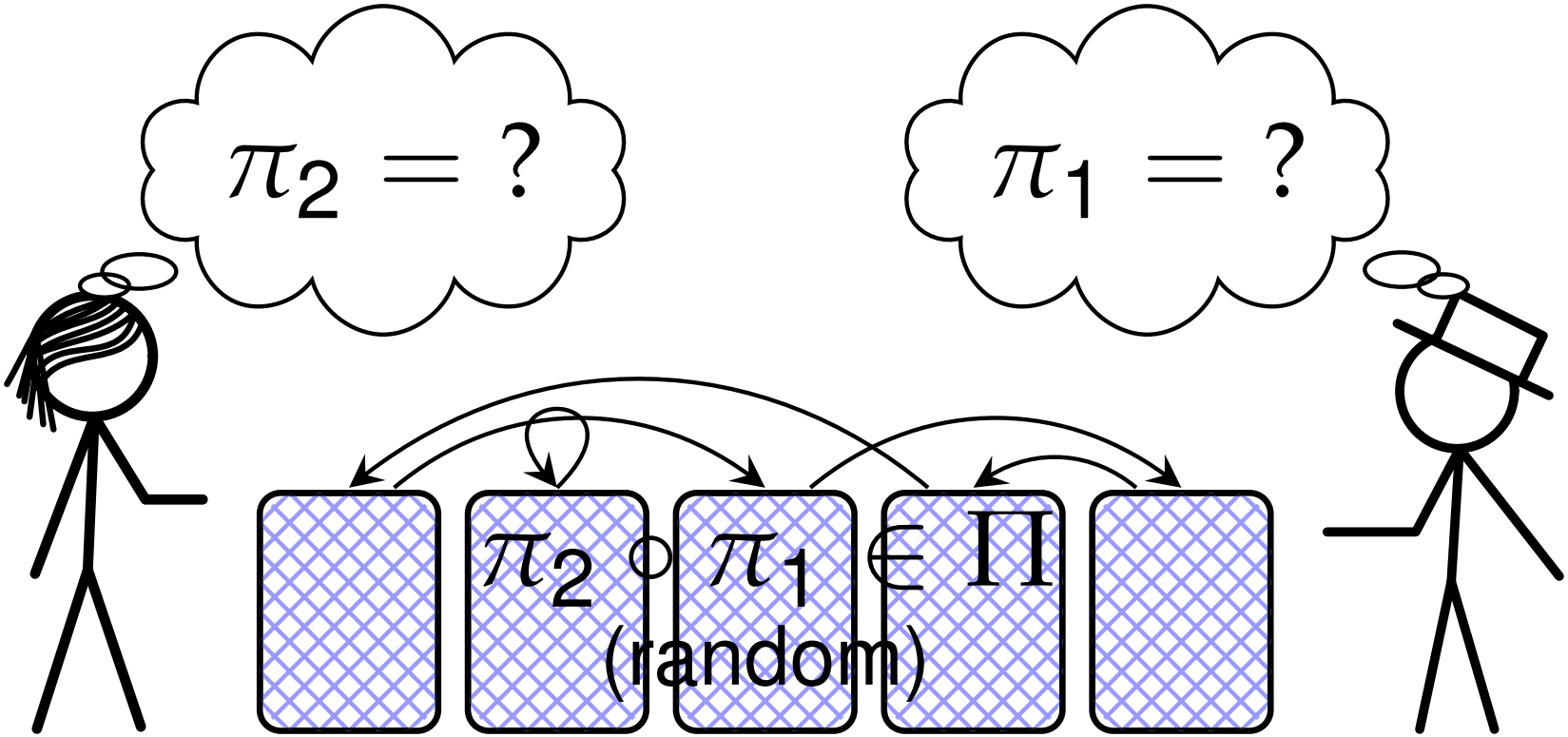
Why uniform closed shuffles are nice



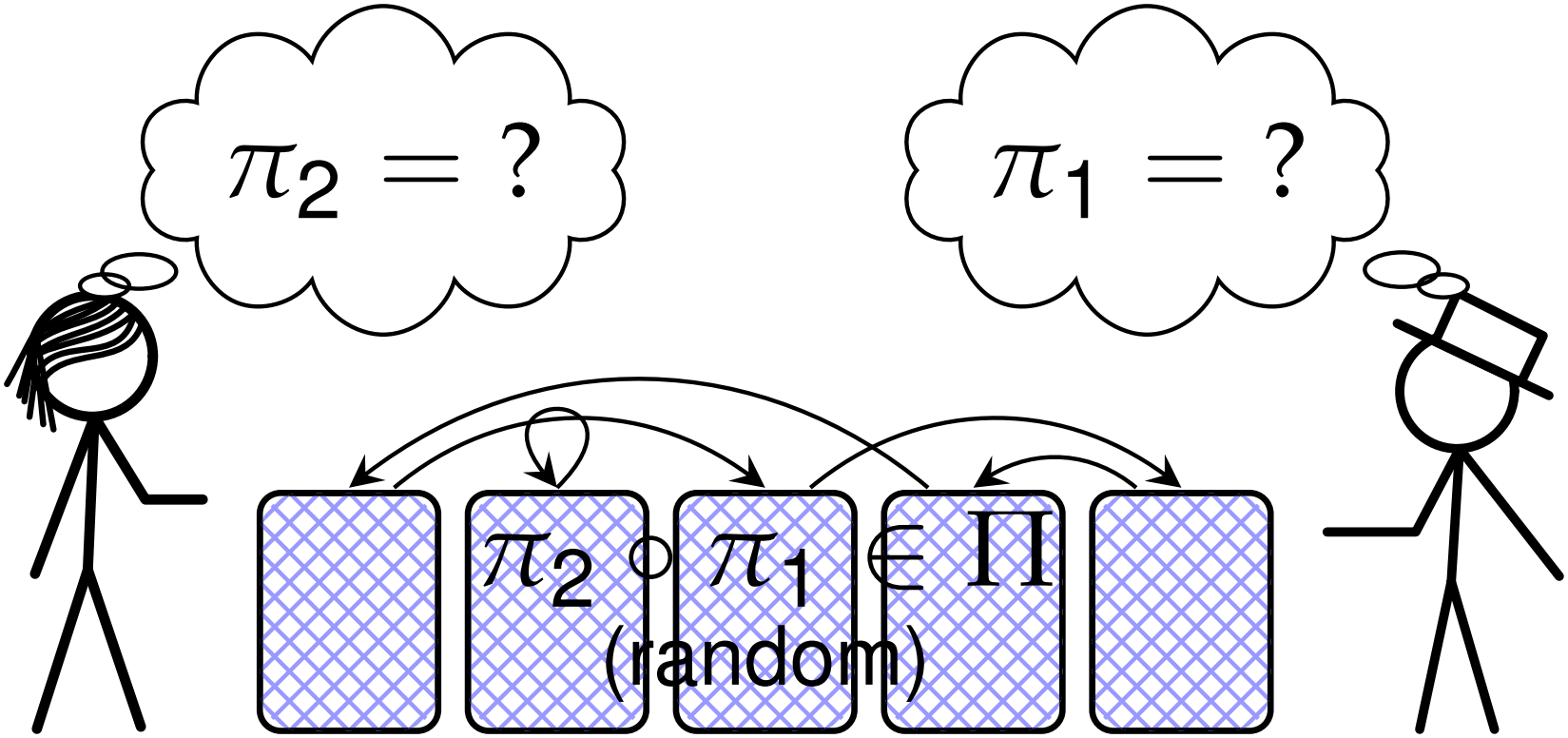
Why uniform closed shuffles are nice



Why uniform closed shuffles are nice



Why uniform closed shuffles are nice

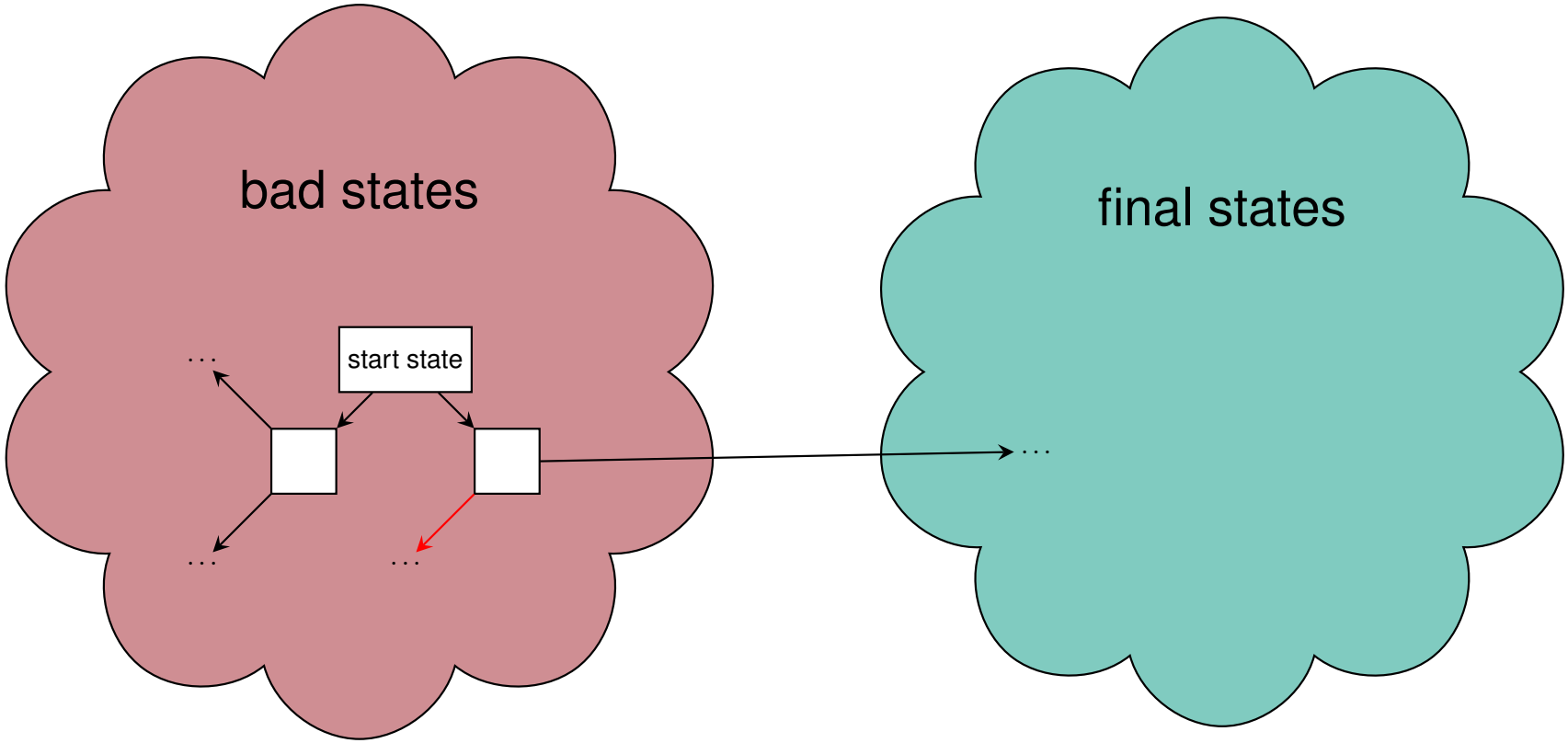


Note: there is an actively secure implementation using only uniform cuts and helping cards, where you do not look away [KW17].

Impossibility Result

Theorem
There is no secure finite-runtime closed-shuffle five-card AND protocol

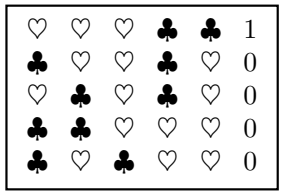
Proof Idea



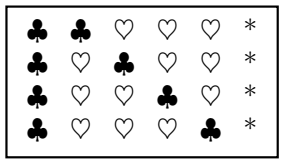
At least one outgoing edge (path) leads to a bad state again.

Proof Idea: Classification of States

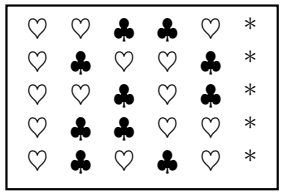
Bad States



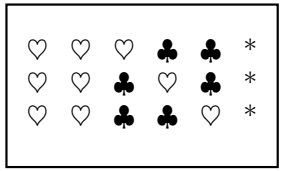
$\mathcal{B}_{4*}$
4 seqs of same type



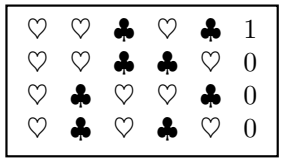
$\mathcal{B}_{3\clubsuit}$
♣-col, 3+ seqs



$\mathcal{B}_{5\heartsuit}$
♡-col, 5+ seqs

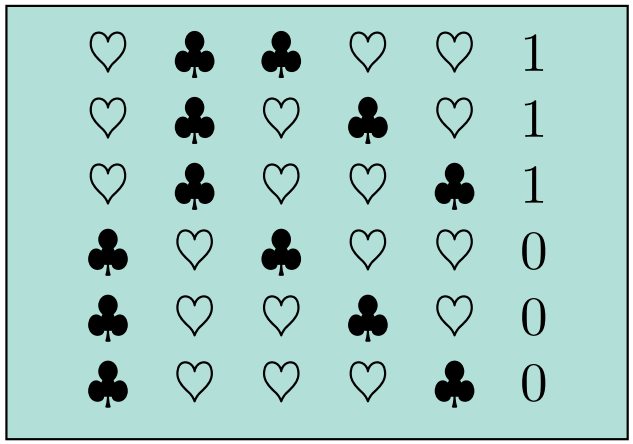


$\mathcal{B}_{3\heartsuit\heartsuit}$
2 ♡-cols, 3 seqs



$\mathcal{B}_{\heartsuit 3/1}$
♡-col, type 3/1 or 1/3

Final States

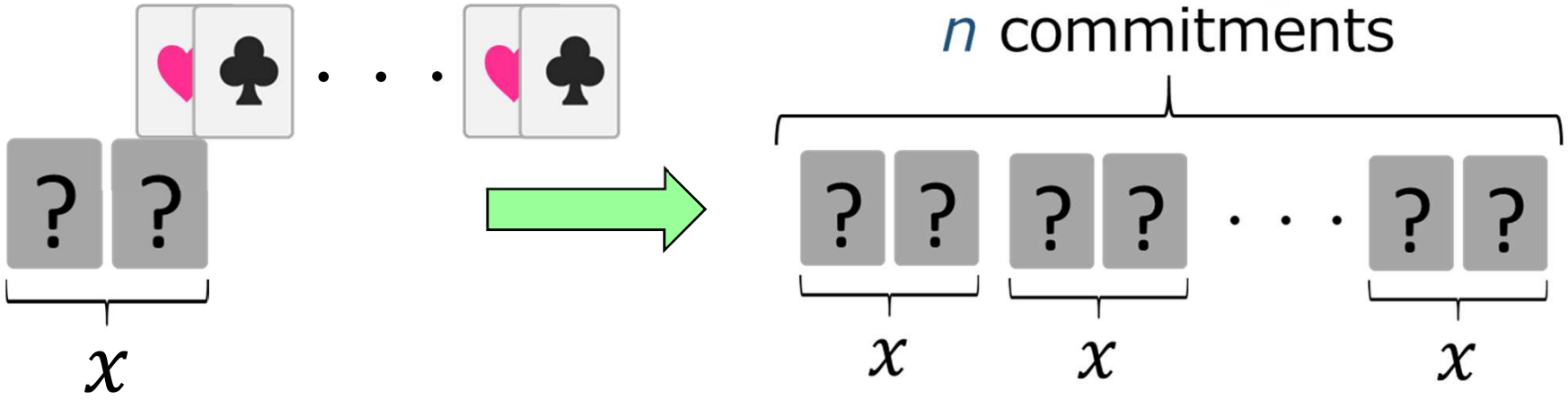


and any subset with at least a 1- and a 0-seq

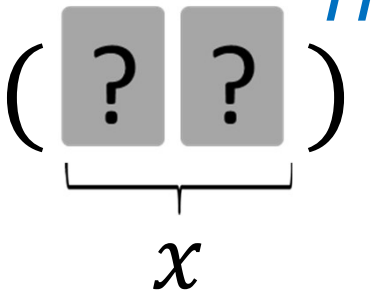
COPY protocols

✓Making n (≥ 2) copied commitments from an input commitment.

At least $2n$ cards are necessary.



✓We sometimes write $(??)^n$



The state-of-the-art COPY protocols

	# cards	Runtime
Mizuki-Sone [FAW09]	$2n+2$	Finite
Nishimura et al. [Soft Com.17]	$2n+1$	Las Vegas

Contribution

✓We show lower bounds on the numbers of cards:

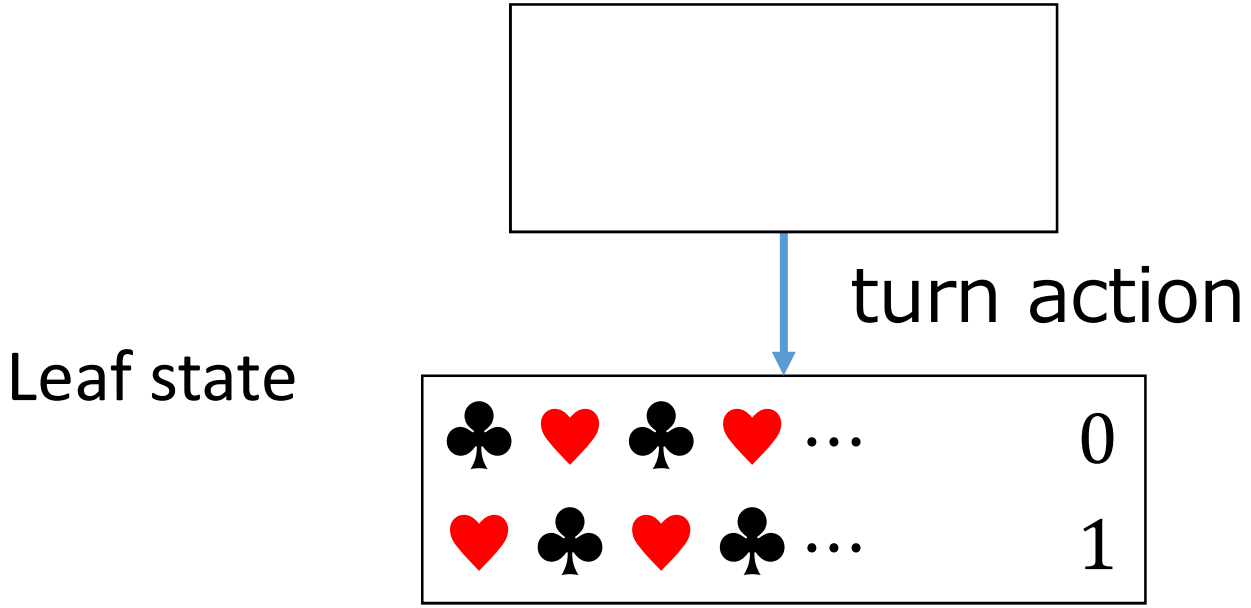
- ✓$2n+1$ cards are required for any COPY protocol;
- ✓$2n+2$ cards are necessary for finite-runtime.

These are optimal in terms of the number of required cards

	# cards	Runtime
Mizuki-Sone[FAW09]	$2n+2$	Finite
Nishimura et al.[Soft Com.17]	$2n+1$	Las Vegas

Impossibility with $2n$ cards

- ✓The proof outline:
  - ✓Assume the <u>existence</u> of COPY protocols with $2n$ cards,



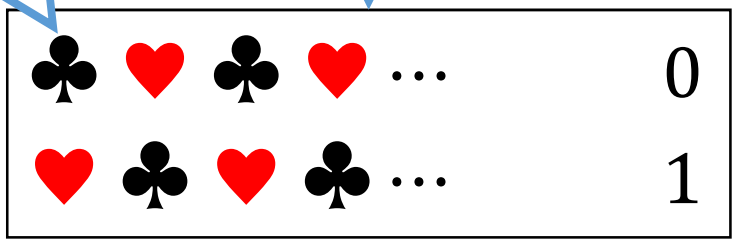
Impossibility with $2n$ cards

- ✓The proof outline:
  - ✓Assume the existence of COPY protocols with $2n$ cards,

Both the turned cards must be the same color, a contradiction.

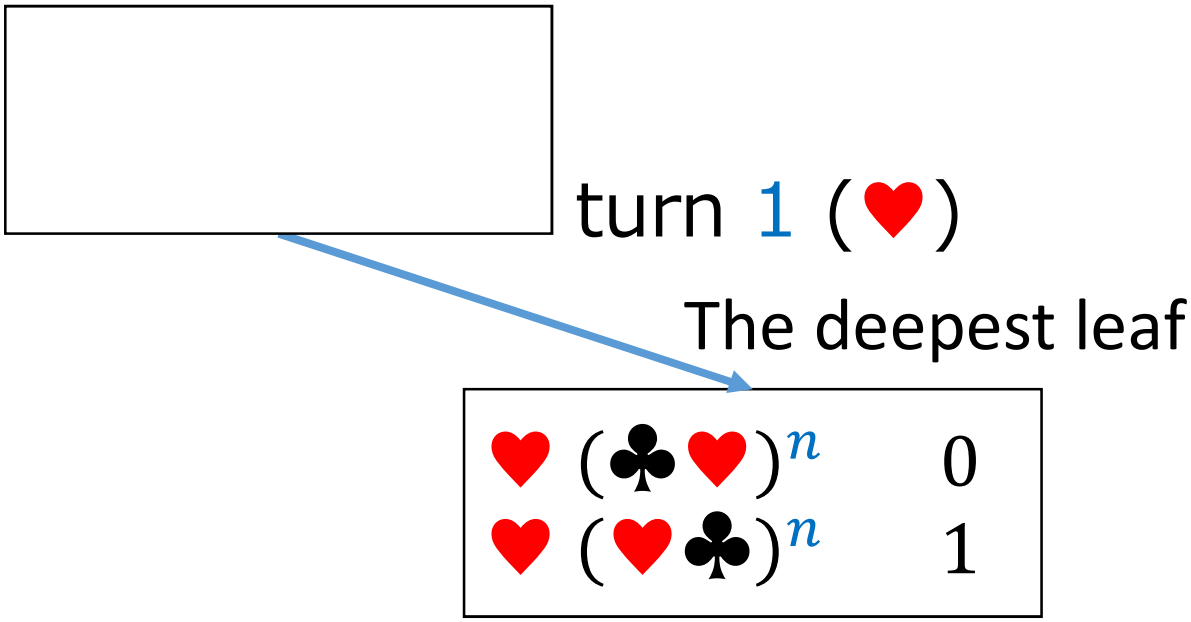
turn action

Leaf state



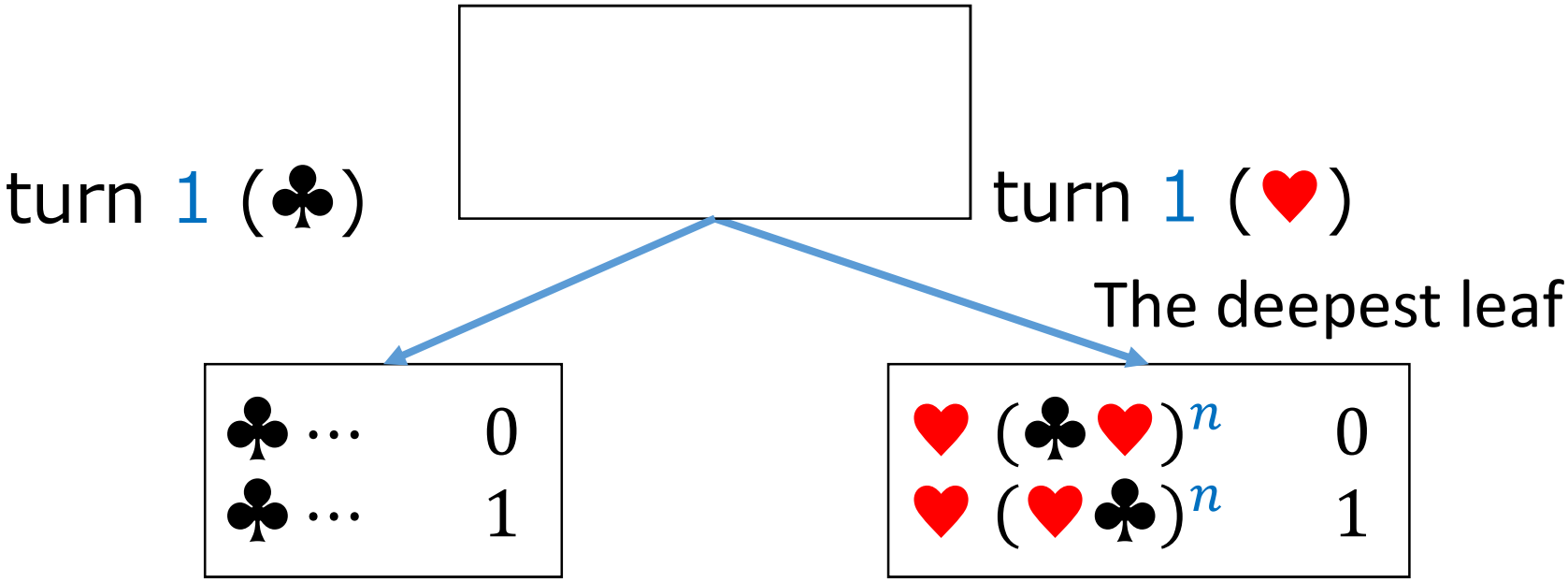
Impossibility with $2n+1$ cards for finite

- ✓The proof outline:
  - ✓Assume the existence of finite COPY with $\clubsuit^n, \heartsuit^{n+1}$.
  - ✓There must be the deepest leaf.



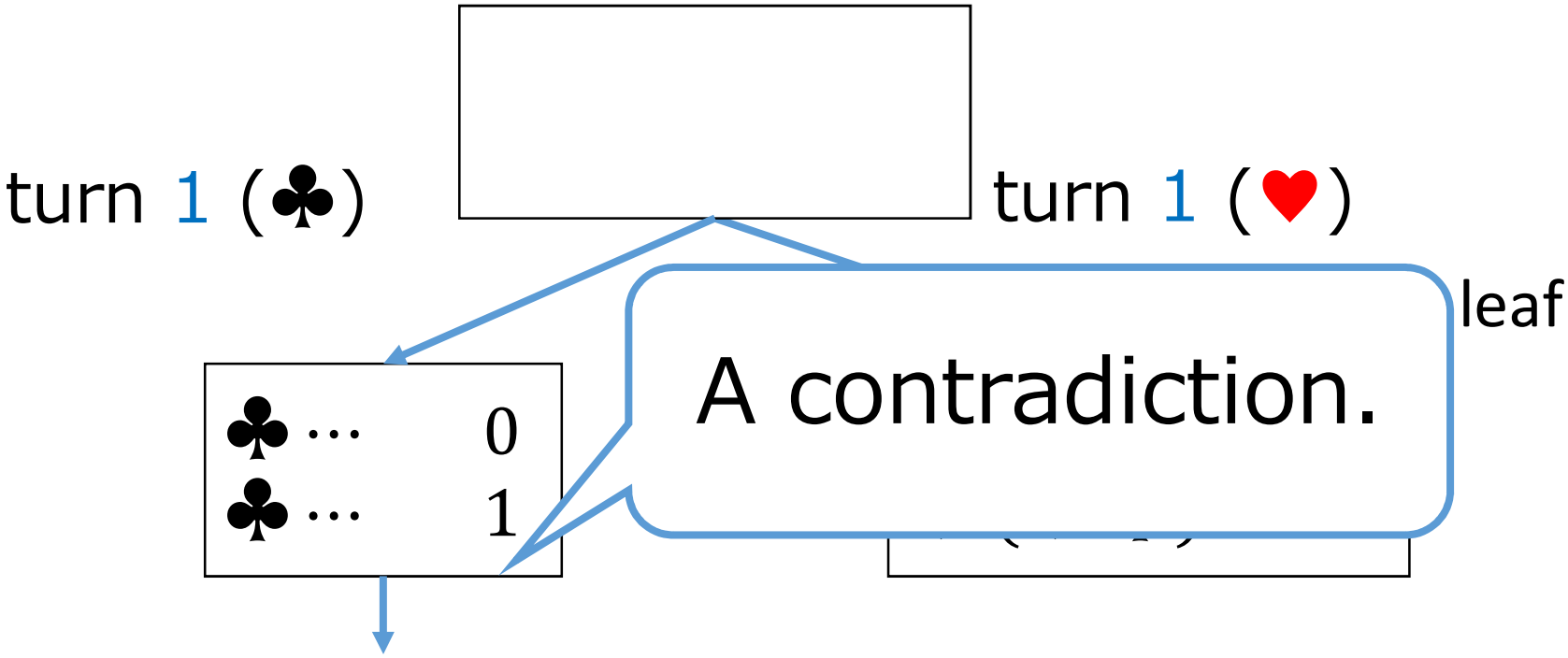
Impossibility with $2n+1$ cards for finite

- ✓The proof outline:
  - ✓Assume the existence of finite COPY with $\clubsuit^n, \heartsuit^{n+1}$.
  - ✓There must be the deepest leaf.



Impossibility with $2n+1$ cards for finite

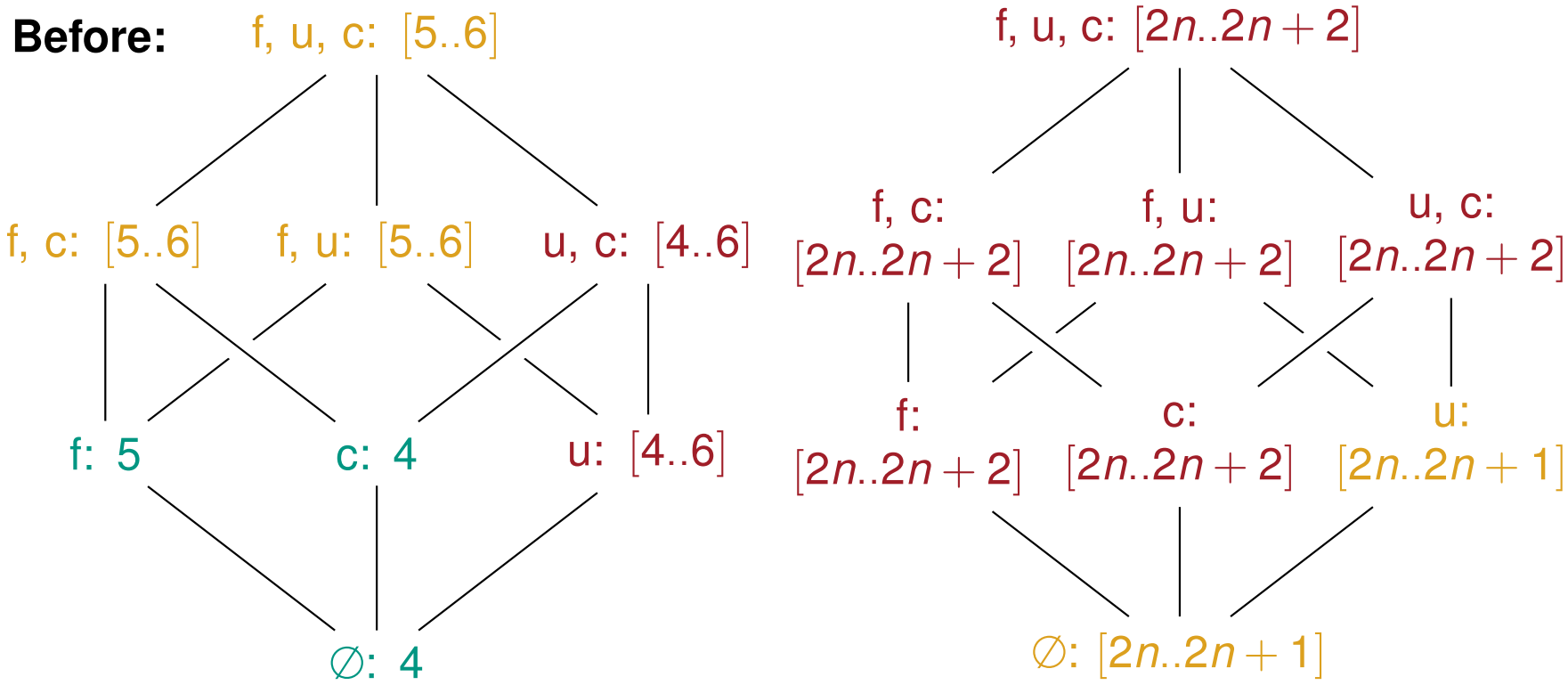
- ✓The proof outline:
  - ✓Assume the existence of finite COPY with $\clubsuit^n$, $\heartsuit^{n+1}$.
  - ✓There must be the deepest leaf.



- ✓Because we cannot construct n commitments with $\clubsuit^{n-1}$ and $\heartsuit^{n+1}$, there should be a deeper leaf.

Summary

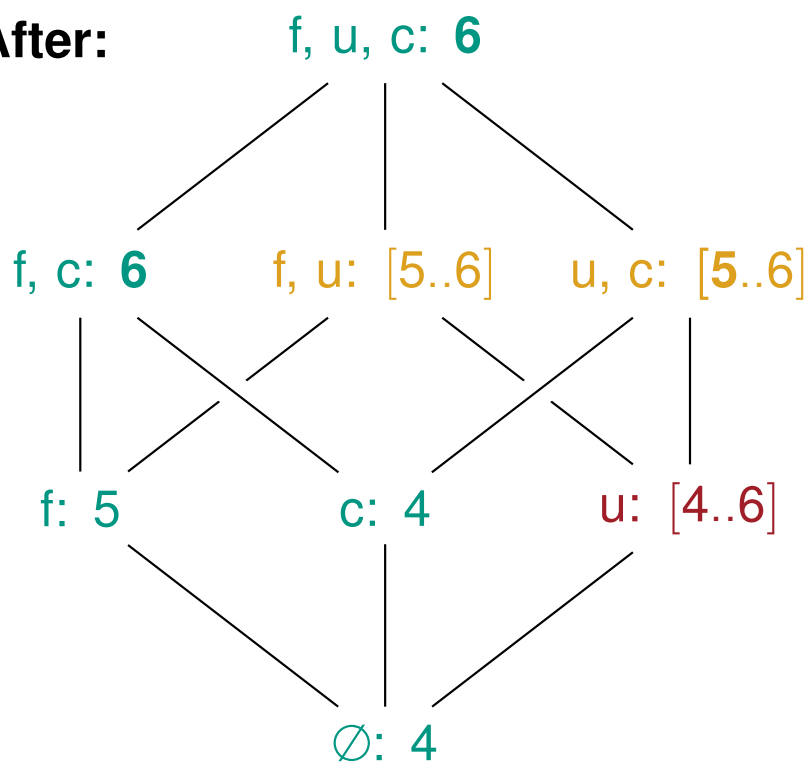
- 6 cards needed for finite-runtime **(f)** AND with closed **(c)** shuffles
- 5 cards needed for AND with uniform **(u)** closed shuffles
- $2n+1$ cards needed for COPY
- $2n+2$ cards needed for finite-runtime COPY

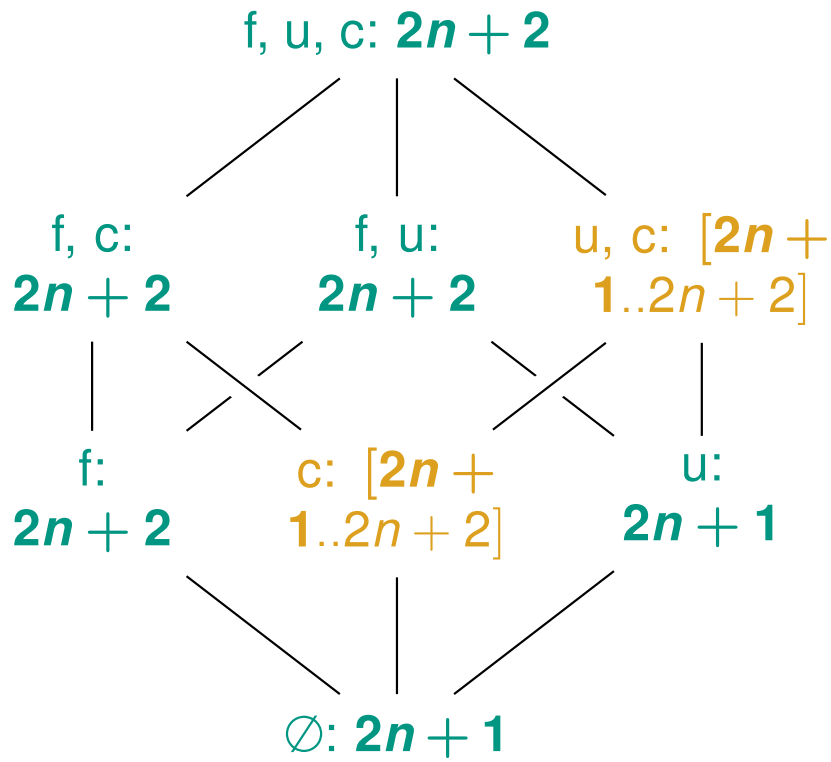


Summary

- 6 cards needed for finite-runtime **(f)** AND with closed **(c)** shuffles
- 5 cards needed for AND with uniform **(u)** closed shuffles
- $2n + 1$ cards needed for COPY
- $2n + 2$ cards needed for finite-runtime COPY

After:

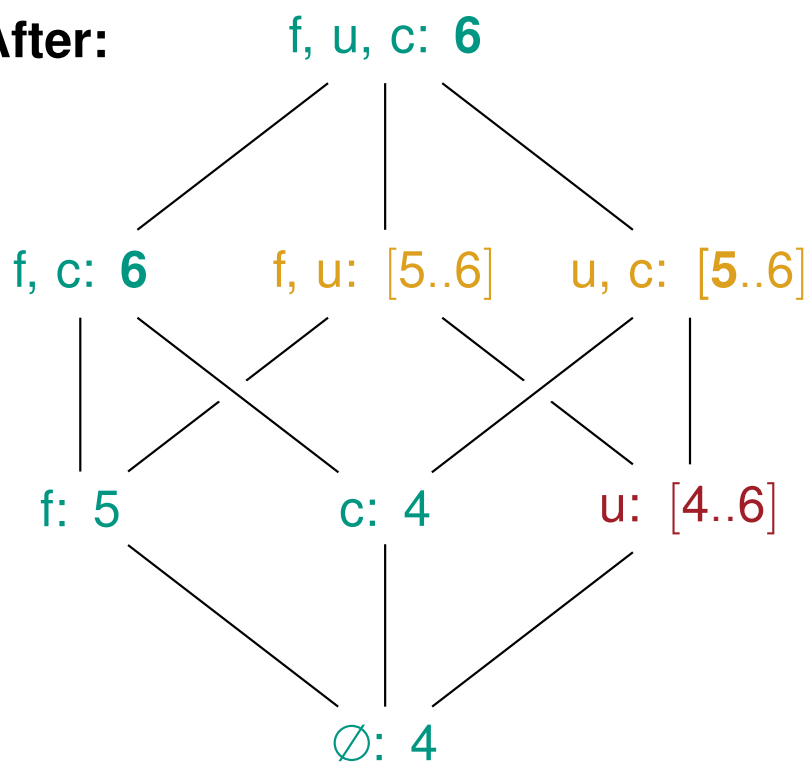


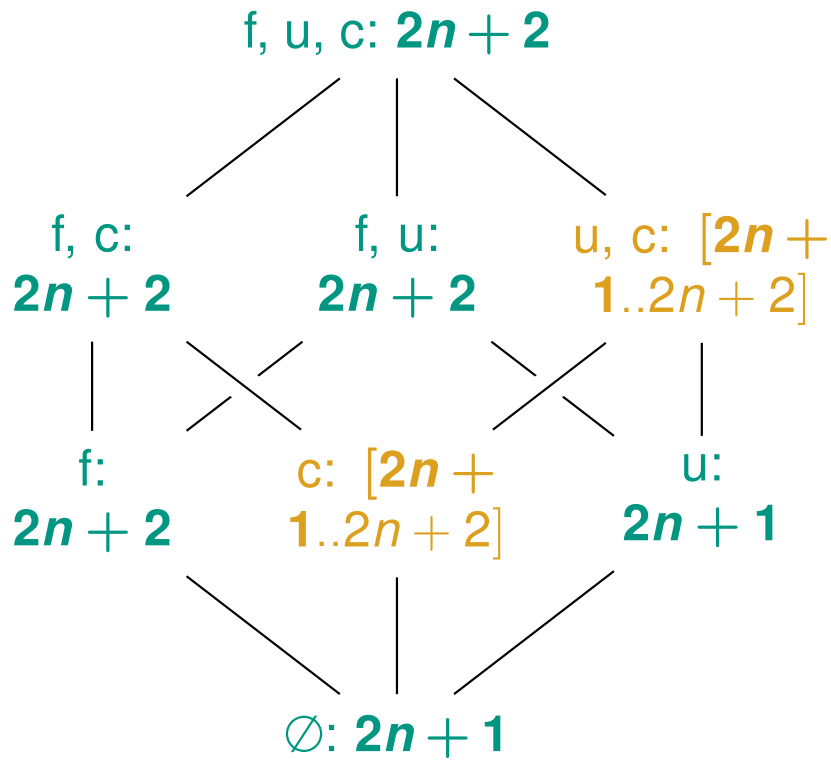


Summary

- 6 cards needed for finite-runtime **(f)** AND with closed **(c)** shuffles
- 5 cards needed for AND with uniform **(u)** closed shuffles
- $2n + 1$ cards needed for COPY
- $2n + 2$ cards needed for finite-runtime COPY

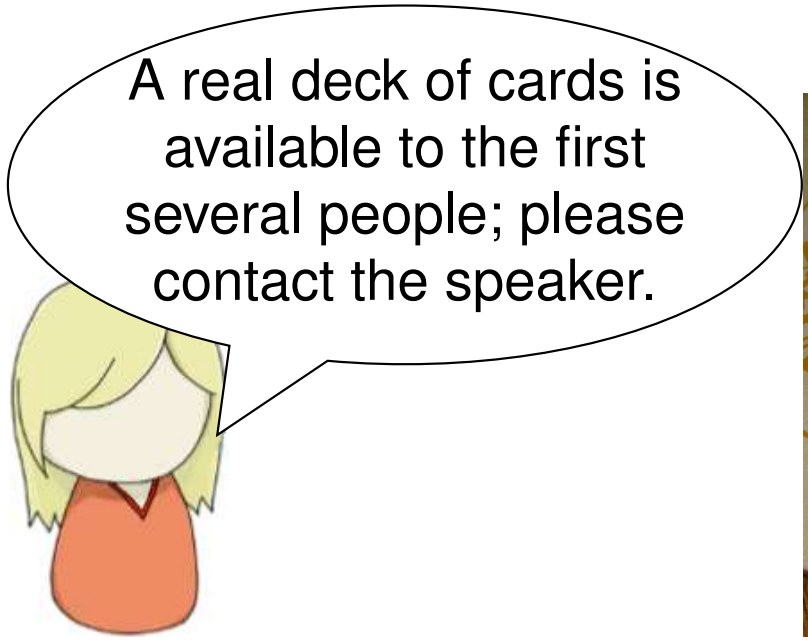
After:





Open: 5-card AND in “f, c” if helping card is ♠?

Thank you for your attention!



References: I

A. Koch and S. Walzer. Foundations for Actively Secure Card-based Cryptography. 2017. iacr: 2017/423.

A. Koch, S. Walzer, and K. Härtel. “Card-based Cryptographic Protocols Using a Minimal Number of Cards”. In: ASIACRYPT 2015. LNCS 9452. Springer, 2015, pp. 783–807.

T. Mizuki and H. Sone. “Six-Card Secure AND and Four-Card Secure XOR”. In: FAW 2009. LNCS 5598. Springer, 2009, pp. 358–369.

A. Nishimura, T. Nishida, Y. Hayashi, T. Mizuki, and H. Sone. “Card-Based Protocols Using Unequal Division Shuffle”. In: Soft Computing (2017).