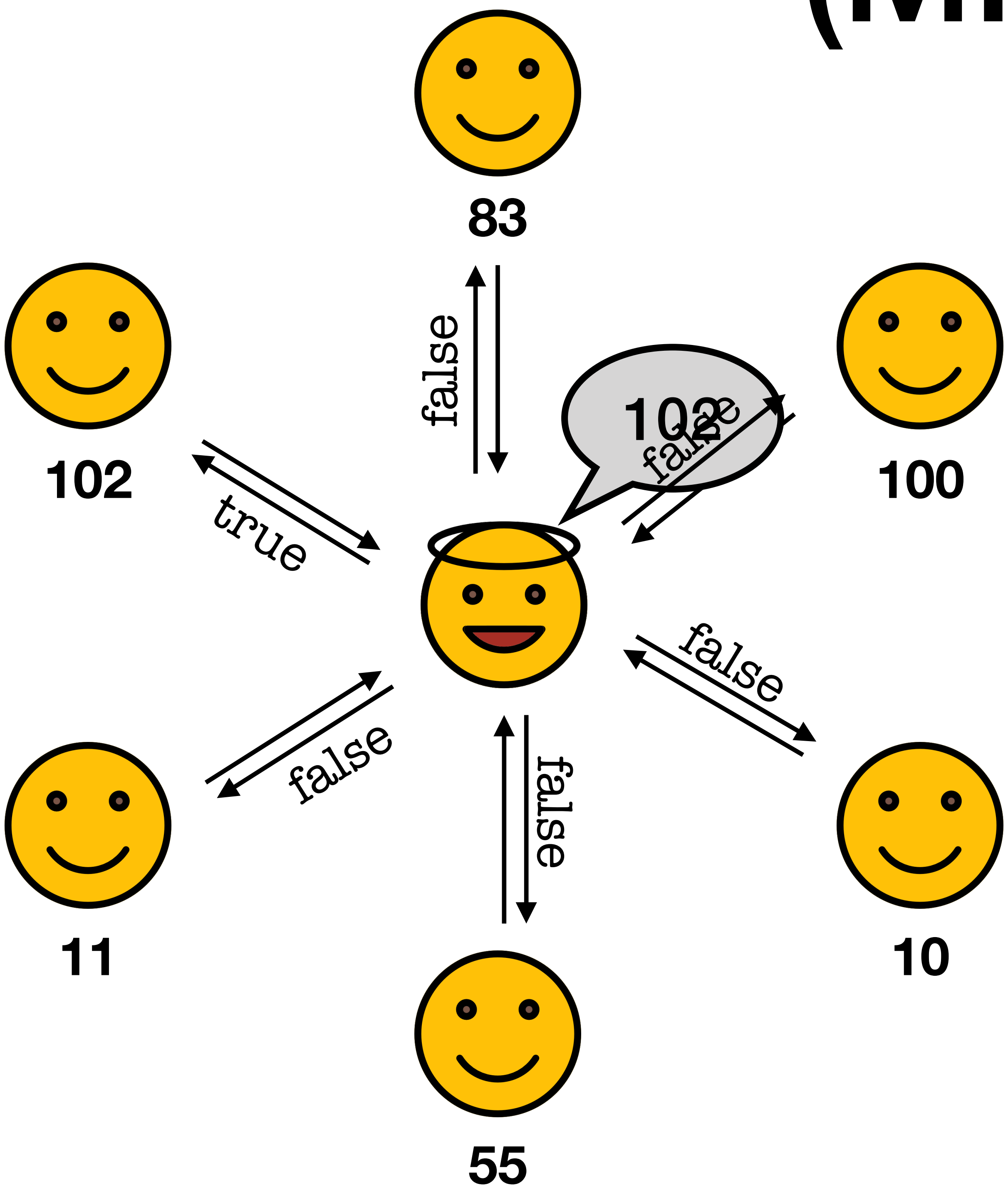
Secure Multi-party Quantum Computation with a Dishonest Majority

Yfke Dulek, Alex Grilo, Stacey Jeffery, Christian Majenz, Christian Schaffner

Introduction

Multi-party computation (MPC)



Input (player i): x_i

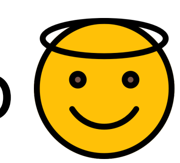
Output: $f(x_1, \ldots, x_k)$

e.g., what is the maximum input?

Output (player i): $f_i(x_1, \ldots, x_k)$

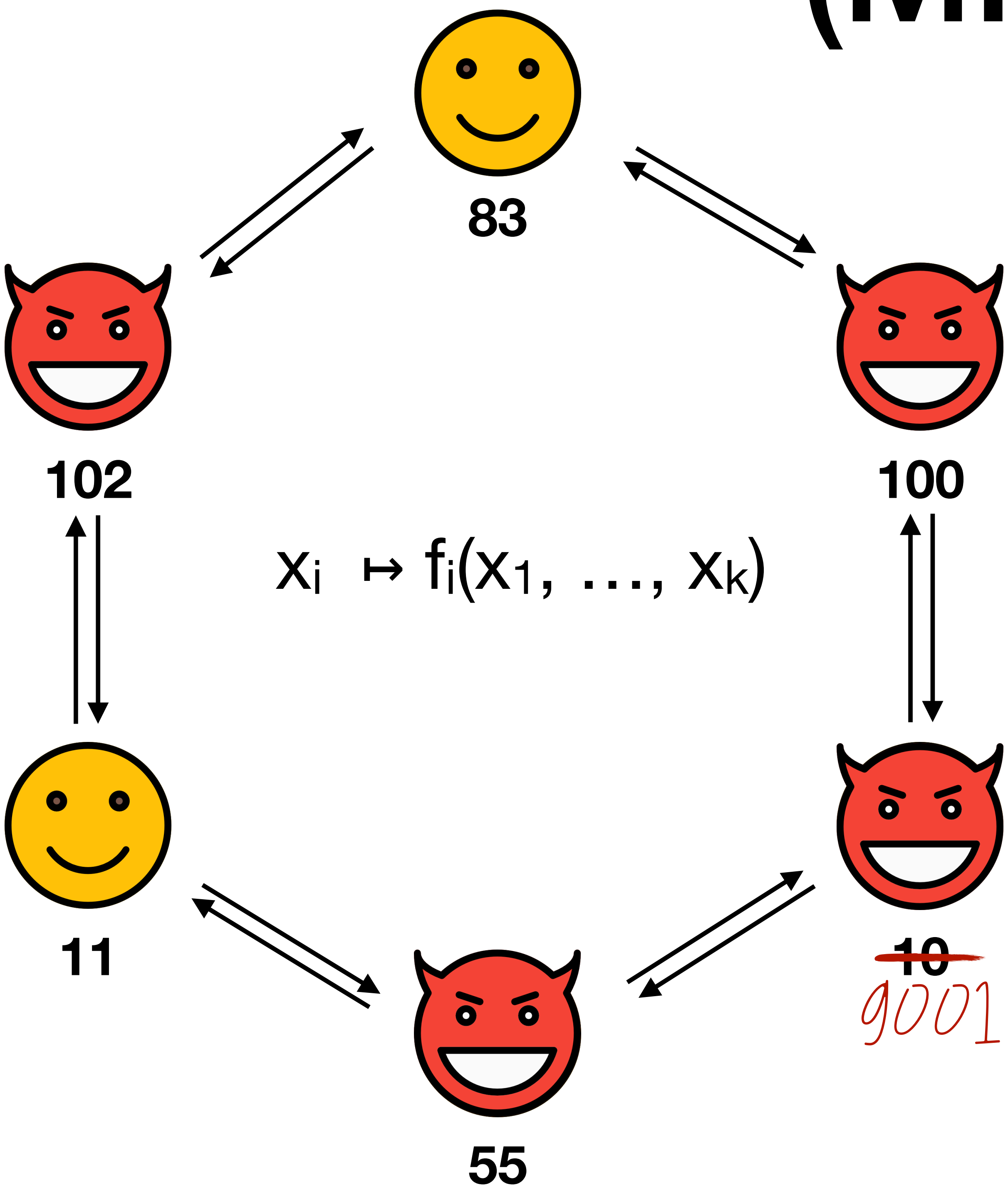
e.g., was my input the highest?

This is the **ideal** situation.

What if there is no  ?

Icons by Pixel perfect.

Multi-party computation (MPC)



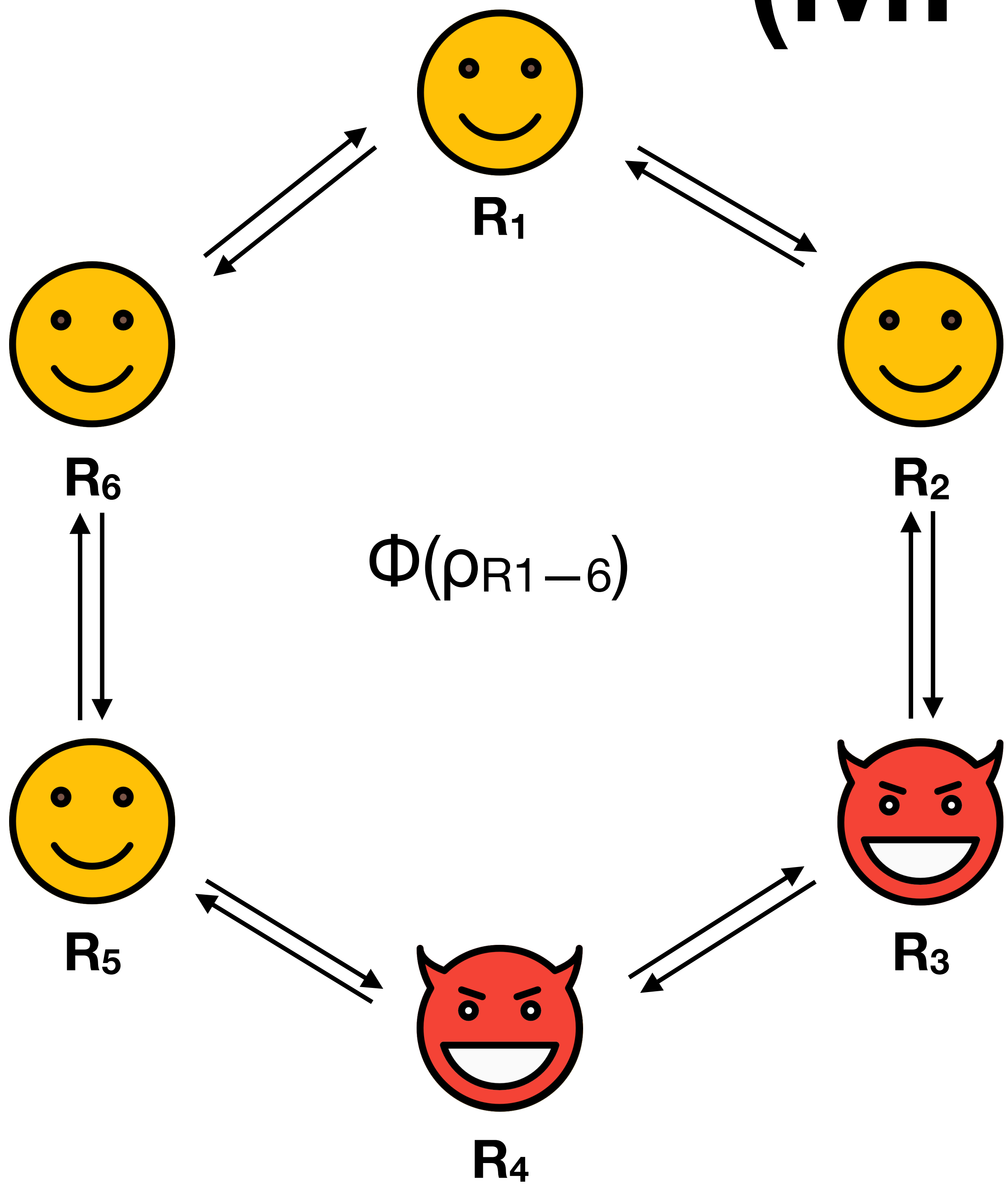
We want:

- privacy of inputs
- correctness of outputs

We cannot prevent:

- lying about inputs
- unfairness

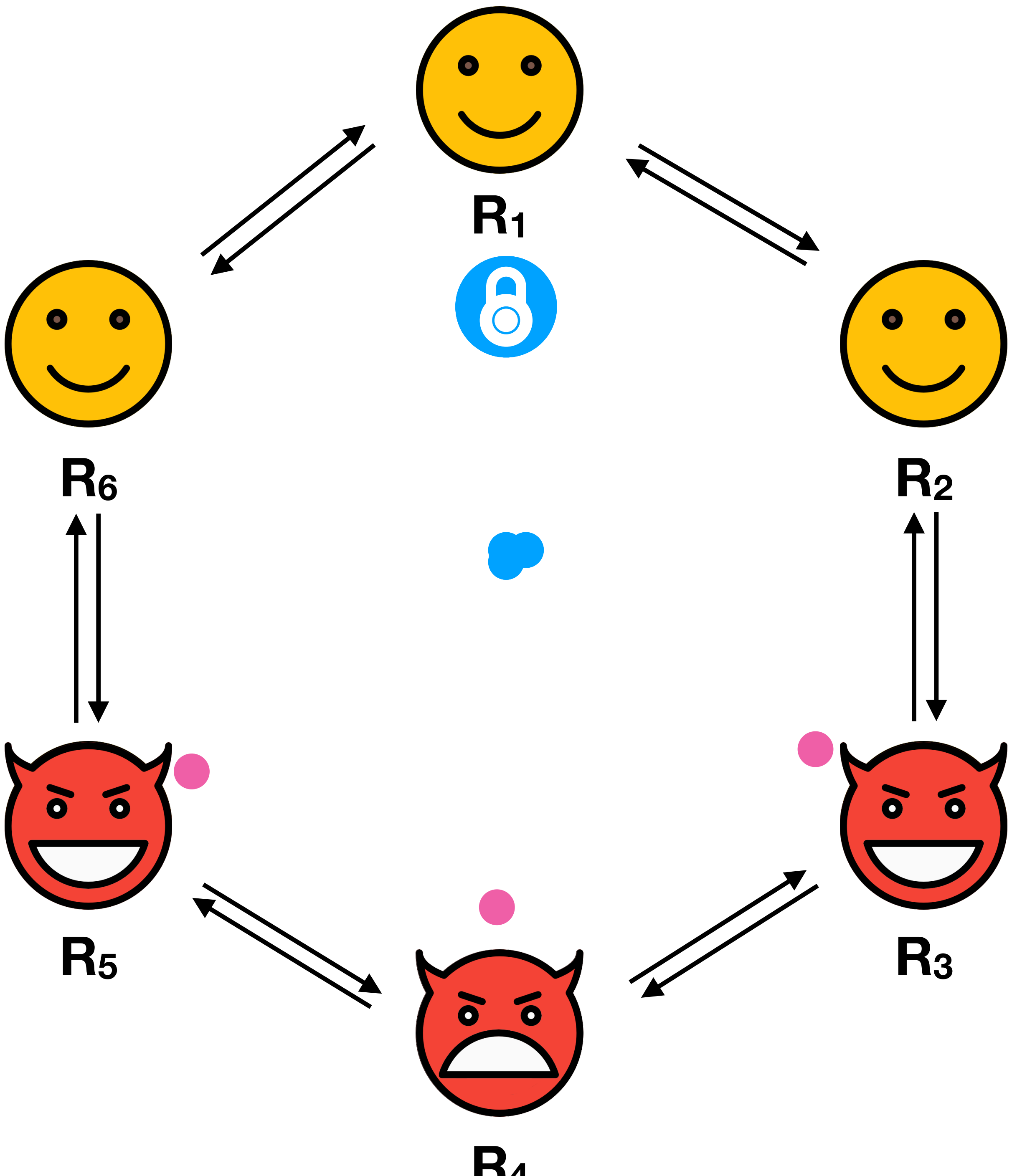
Goal: Quantum MPC (MPQC)



This talk: protocol for MPQC

- subroutine: classical MPC
- Up to k-1
- Computationally secure
- gate-by-gate, using $O\big(k(d+\log(n))\big)$ quantum rounds for d the {CNOT,T}-depth of the q computation

MPQC: two approaches



1. Secret sharing [CGS02]

- distribute inputs
- up to <k/2 dishonest

2. Authentication [DNS12]

- protect inputs
- hope: up to k-1 dishonest

[CGS02] Crépeau, Gottesman, and Smith. Secure multi-party quantum computation. (STOC 2002)

[DNS12] Dupuis, Nielsen, and Salvail. Actively secure two-party evaluation of any quantum operation. (CRYPTO 2012)

Introduction

Authentication

Computation

Magic-state generation

Summary

Clifford code

Key: $C \in_R \text{Clifford}_{n+1}$

SUBGROUP OF UNITARIES GENERATED BY H, $\sqrt{Z}$, CNOT
LOOKS "RANDOM"

Encoding: $|\psi\rangle \mapsto C\left(|\psi\rangle \otimes |0\rangle^{\otimes n}\right)$

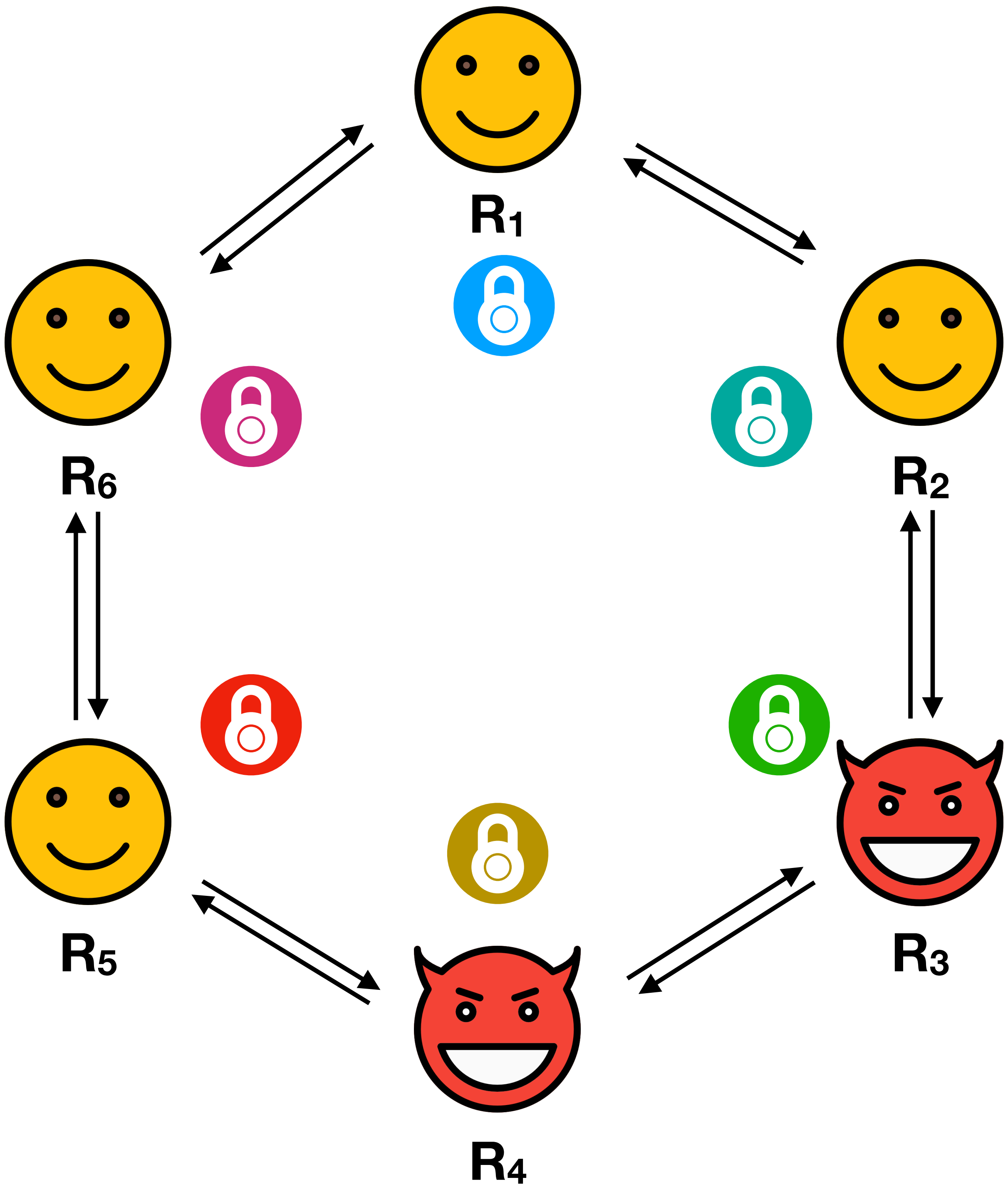
TRAPS

Decoding: apply $C^\dagger$, measure traps

Theorem (informal): for any A on $n+1$ qubits, the probability that A changes $|\psi\rangle$, but is not detected at decoding is very small (2^{-n}).

Bonus: the Clifford code also provides privacy.

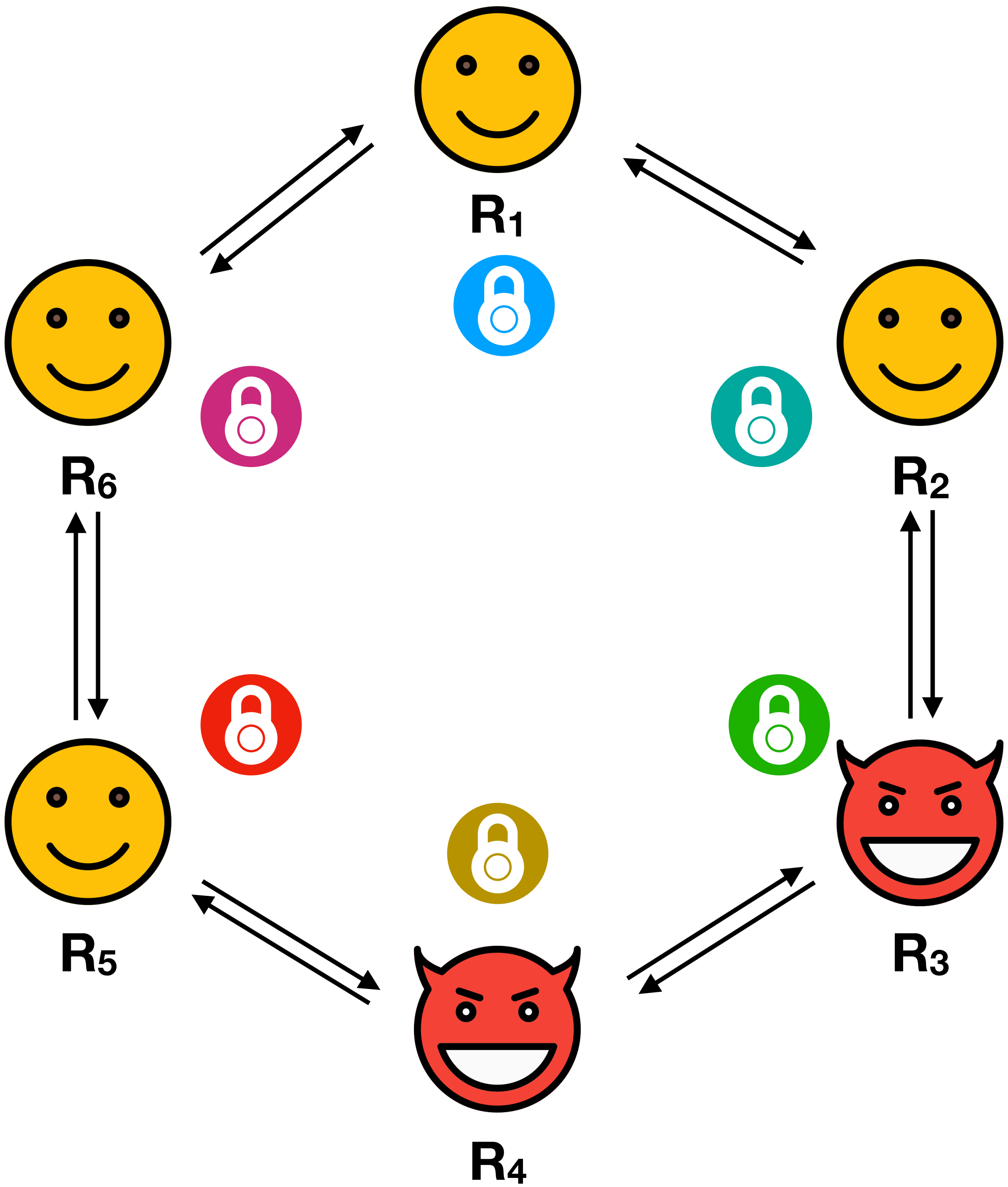
Clifford code in MPQC



- What if the encoding player is dishonest?
- How to do computation? Data is unalterable!

Answers: use classical multi-party computation! 😇

Public authentication test



$$C_6 C_5 C_4 C_3 C_2 C_1 (|\psi\rangle \otimes |0^{2n}\rangle)$$

Public authentication test

$$\underbrace{C_6C_5C_4C_3C_2C_1}_{C}(|\psi\rangle \otimes |0^{2n}\rangle)$$

UNKNOWN TO ALL

PLAYER I CREATED THESE

Using classical MPC:

- Select $g \in_R GL(2n, \mathbb{F}_2)$. Note: $g(y) = 0^{2n}$ iff $y = 0^{2n}$
  Lemma: apply random g and measure n traps
  $\approx$ measure $2n$ traps
- Let player 1 apply $(C' \otimes X^r)(I \otimes g)C^\dagger$ for random C', r
- Let player 1 measure last n qubits (check if outcome is r)

Result: authenticated state $C'(|\psi\rangle \otimes |0^n\rangle)$

Public authentication test

One player **performs** the test: applies Clifford, measures, …

All players **verify** the test through classical MPC

The test can be used:

- to test encodings (as in previous slide);
- to test whether a computation step was executed honestly

Introduction
Authentication
Computation
Magic-state generation
Summary

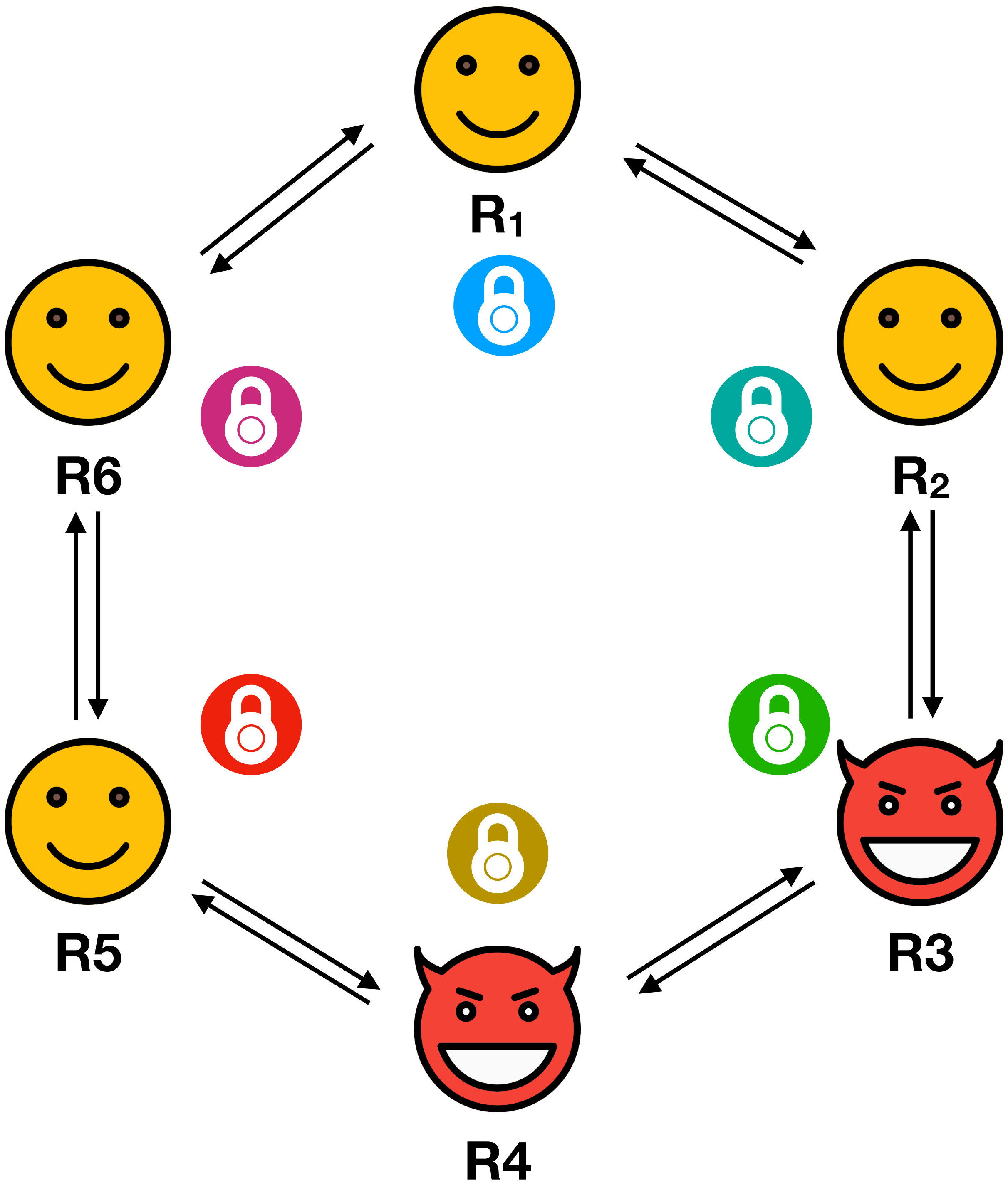
Computation

$|\psi\rangle$ $\quad\quad$ $G|\psi\rangle$

Protocols ($C(|\psi\rangle \otimes |0^n\rangle) \mapsto C'(G|\psi\rangle \otimes |0^n\rangle)$) for these G :

- 1-qubit Cliffords
- CNOT (2-qubit Clifford)
- T (non-Clifford)
- (Computational-basis measurement)

Single-qubit Cliffords



$$= C(|\psi\rangle \otimes |0\rangle^{\otimes n})$$

Using classical MPC: update classical key

$$C \;\mapsto\; C' := C(G^\dagger \otimes I^{\otimes n})$$

Then  will decode to

$$(C')^\dagger C(|\psi\rangle \otimes |0\rangle^{\otimes n})$$

$$= G|\psi\rangle \otimes |0\rangle^{\otimes n}$$

CNOT

 $\otimes$  $= (C_1 \otimes C_2)(|\psi_1\rangle \otimes |0^n\rangle \otimes |\psi_2\rangle \otimes |0^n\rangle)$

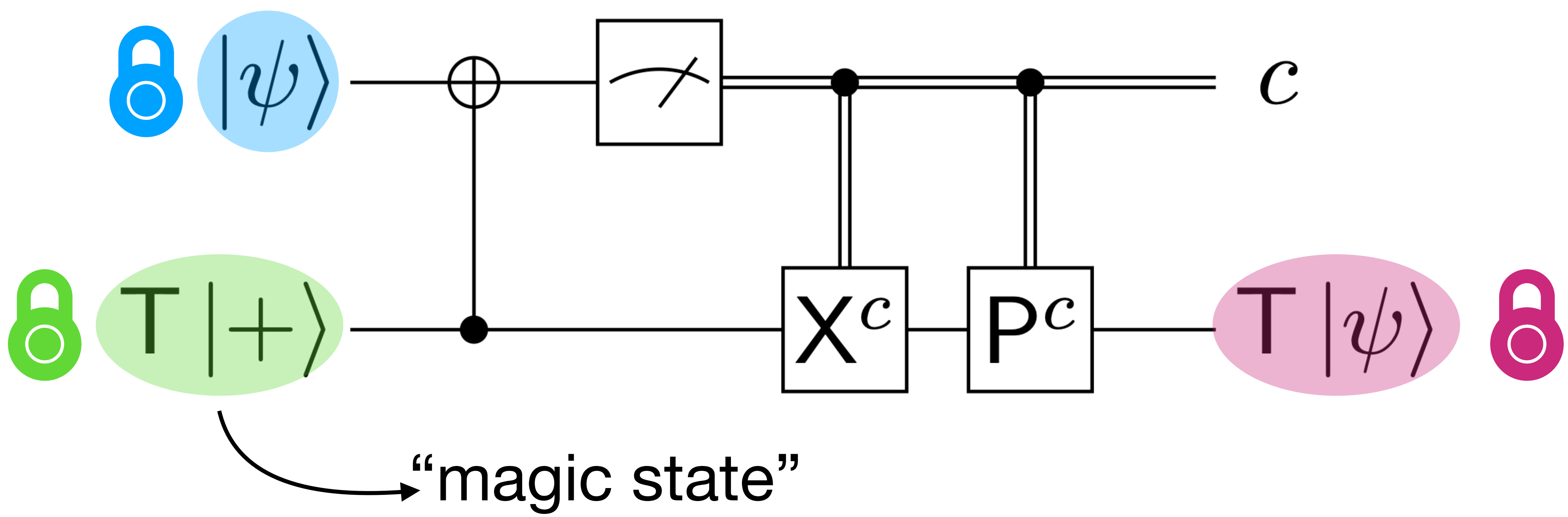
Same strategy does not work:
$(C_1 \otimes C_2)(CNOT^\dagger \otimes I^{\otimes 2n})$ is not in product form.

Instead:

- Player 1 applies $(C_1' \otimes C_2')CNOT(C_1^\dagger \otimes C_2^\dagger)$ for freshly random C_1', C_2' .
- Player 1 executes public authentication test.

Non-Clifford gate $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{\pi i/4} \end{bmatrix}$

Magic-state computation:



$$C_1(|\psi\rangle \otimes |0^n\rangle) \otimes C_2(T|+\rangle \otimes |0^n\rangle) \mapsto C_3(T|\psi\rangle \otimes |0^n\rangle)$$

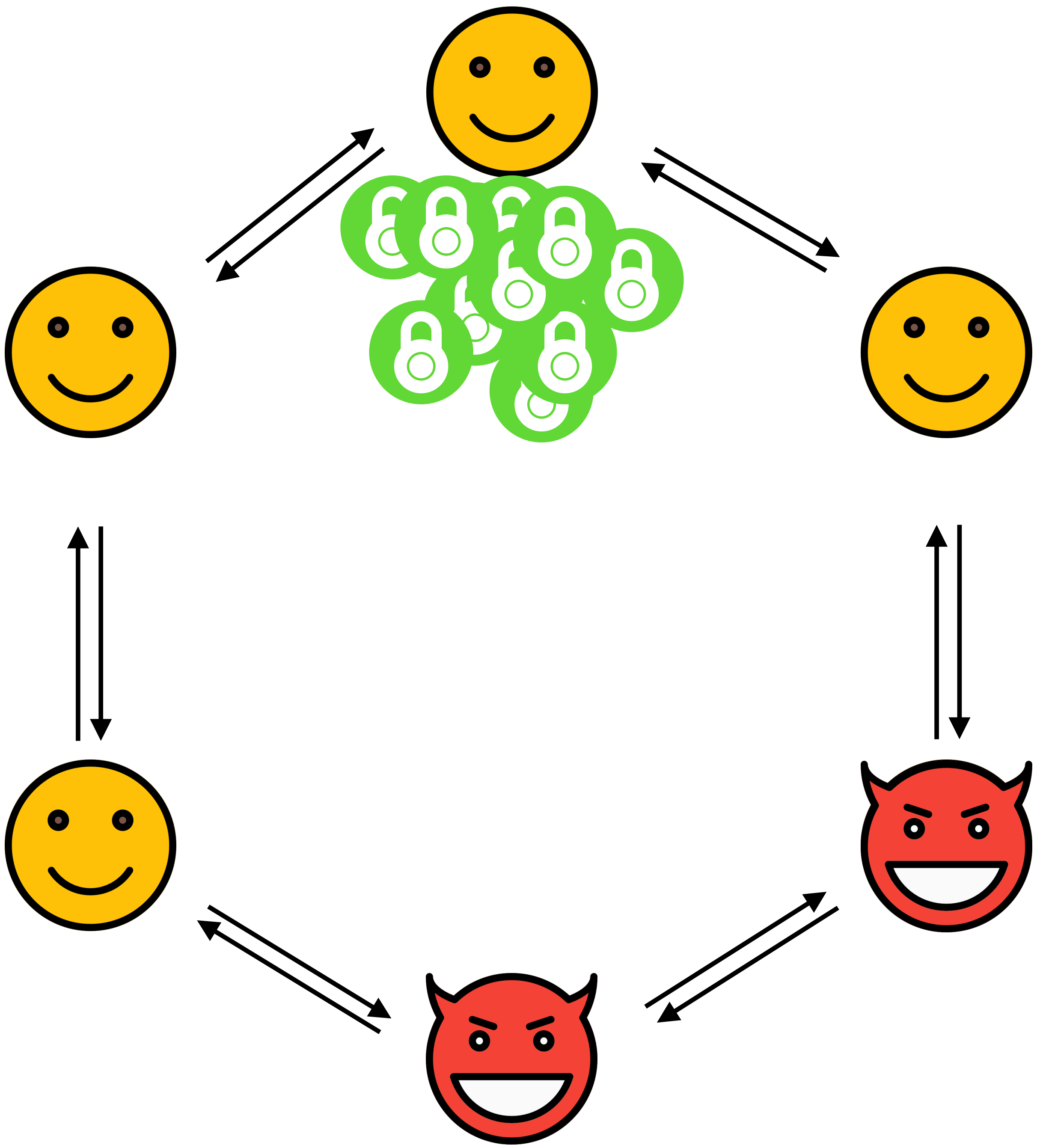
Nobody can be trusted to create encoded magic states!

Introduction
Authentication
Computation

Magic-state generation

Summary

Magic-state generation



$= C(T|+\rangle \otimes |0^n\rangle)$

1. "cut-and-choose":
   - every player tests n random states
   - remaining n copies are "pretty good"
2. magic-state distillation:
   - a Clifford circuit
   - remaining copy is "very good"

Summary

A protocol for multiparty computation of any quantum circuit:

- Computationally secure against $\leq k-1$ cheaters (out of k)
- Encoded states of size $2n+1$ (vs. $kn+1$ in [DNS12])
- Computation:
  - Cliffords are simple (CNOT requires quantum communication & public authentication test)
  - T gate: requires kn magic states (vs. n^k in [DNS12])

Thank you!