Beating Classical Impossibility of Position Verification

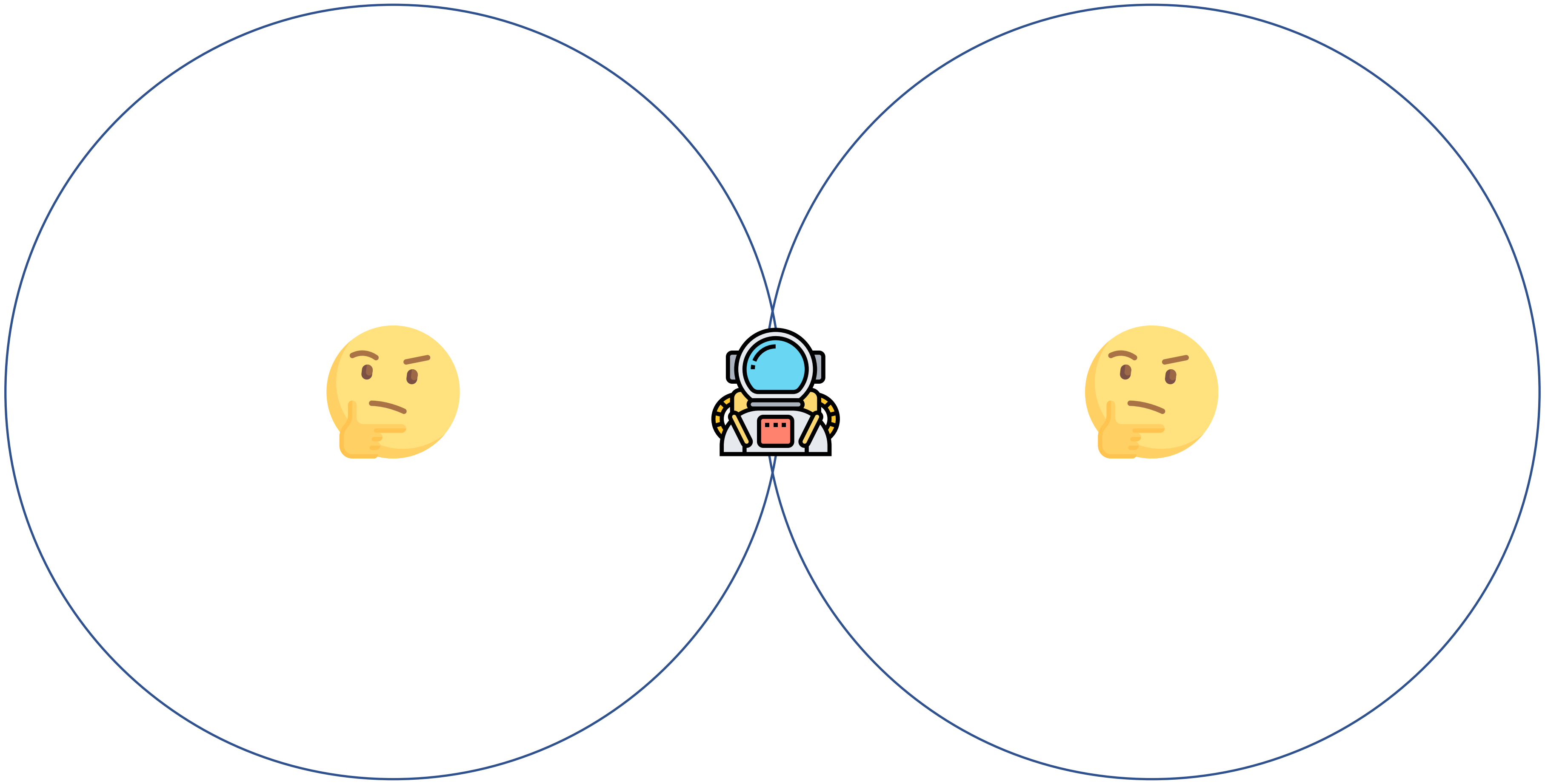
Jiahui Liu, UT Austin

Qipeng Liu, Simons Institute

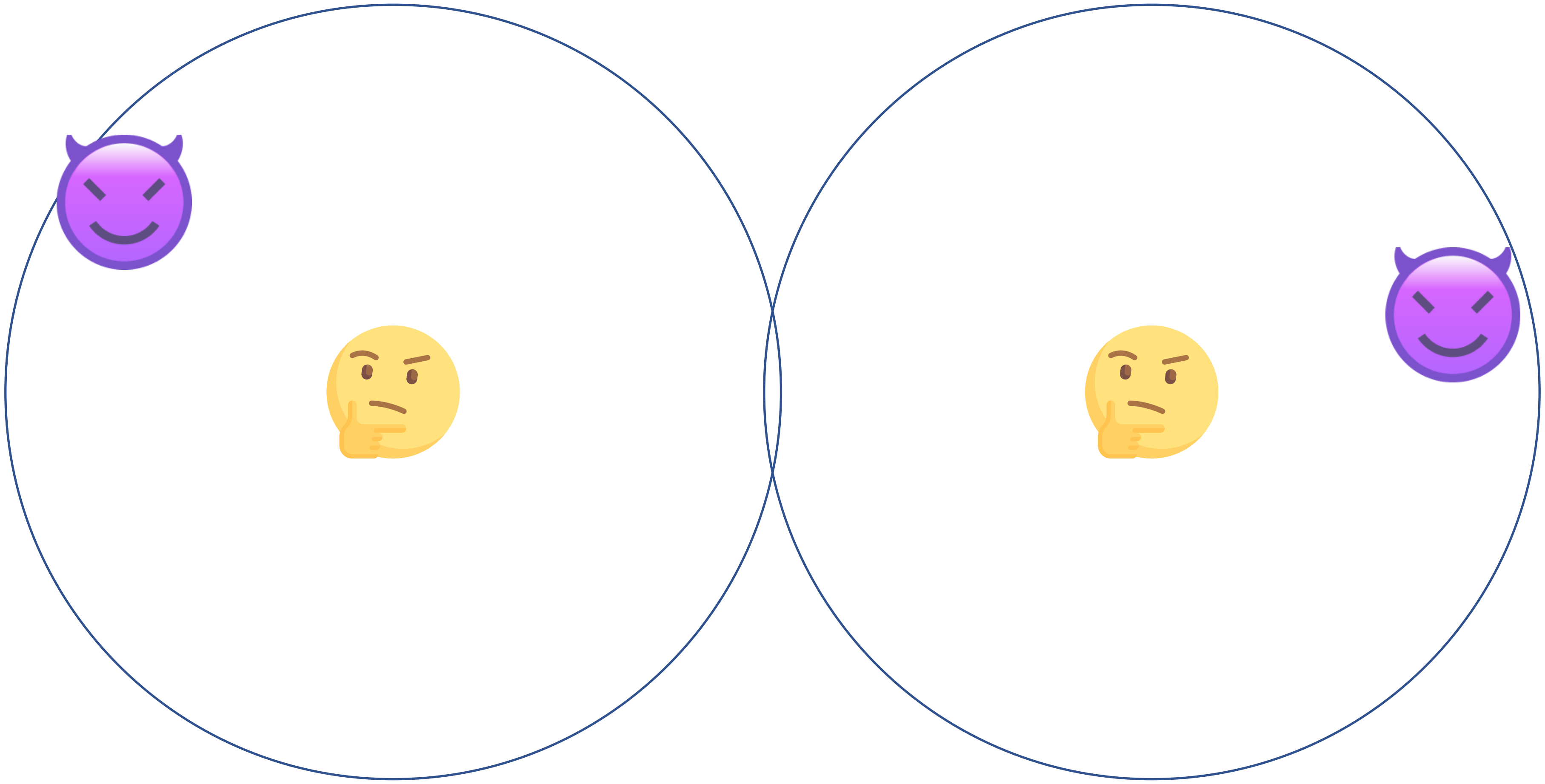
Luowen Qian, Boston University

arXiv/2109.07517

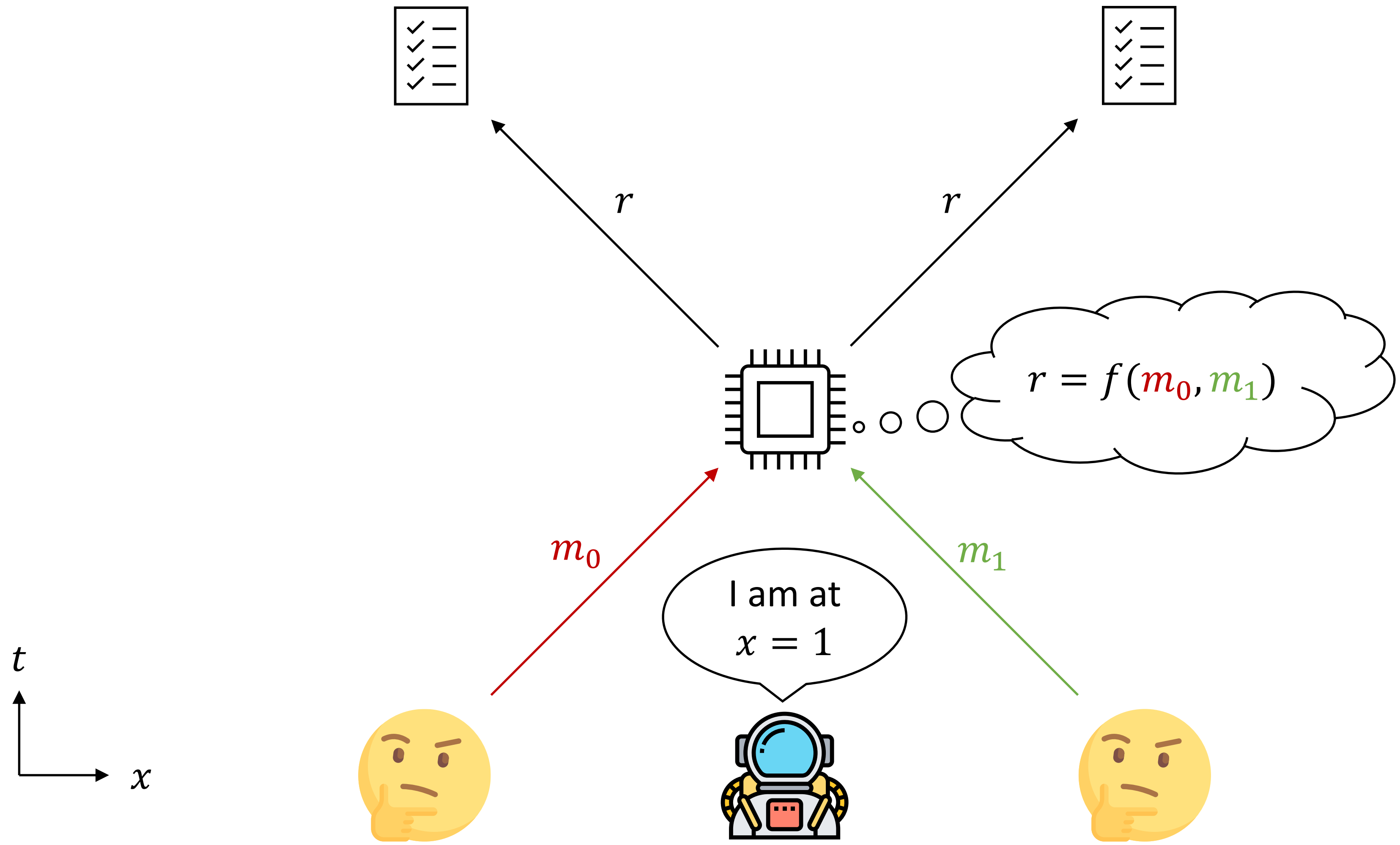
Position verification via distance bounding



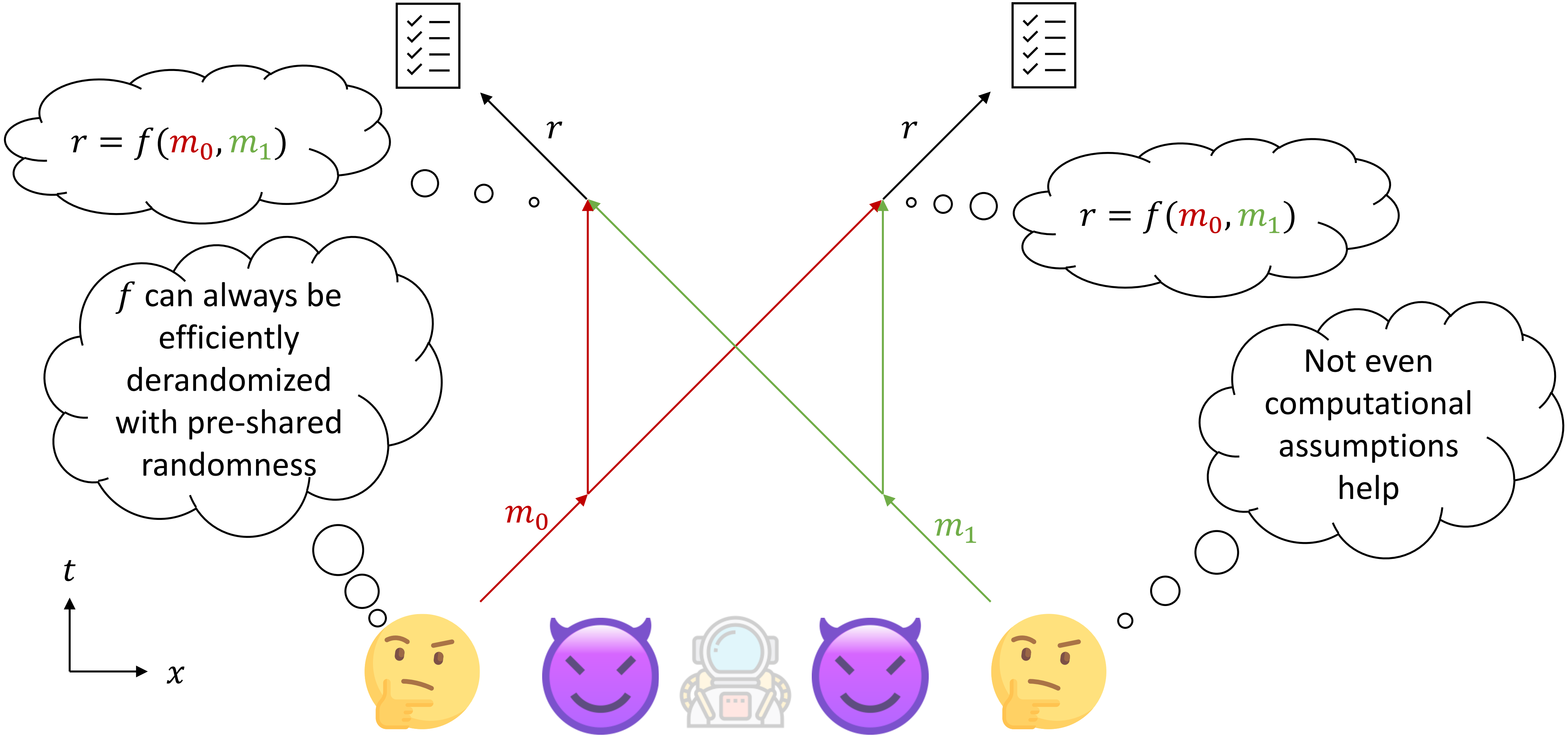
Attack with colluding adversaries



Position verification impossibility



Position verification impossibility



State of the art for position verification (PV)

- Chandran, Goyal, Moriarty, Ostrovsky (2009):
  - Impossibility
  - Protocol secure against bounded-storage adversaries
- Quantum protocols (quantum communication)
  - Kent (2002)
  - Burhman, Chandran, Fehr, Gelles, Goyal, Ostrovsky, Schaffner (2010)
  - Beigi, König (2011)
  - Kent, Munro, Spiller (2011)
  - Tomamichel, Fehr, Kaniewski, Wehner (2013)
  - Unruh (2014)
  - …

In this talk…

Quantum hardness of Learning with Errors (LWE) →
Classically verifiable position verification against quantum* adversaries

Classical verifiers
Classical communication

Can we do better?

- Quantum prover is necessary
- Computational assumptions are necessary
  (proofs of quantumness are necessary)

*security against entangled adversaries can be achieved with a stronger (standard) assumption/model

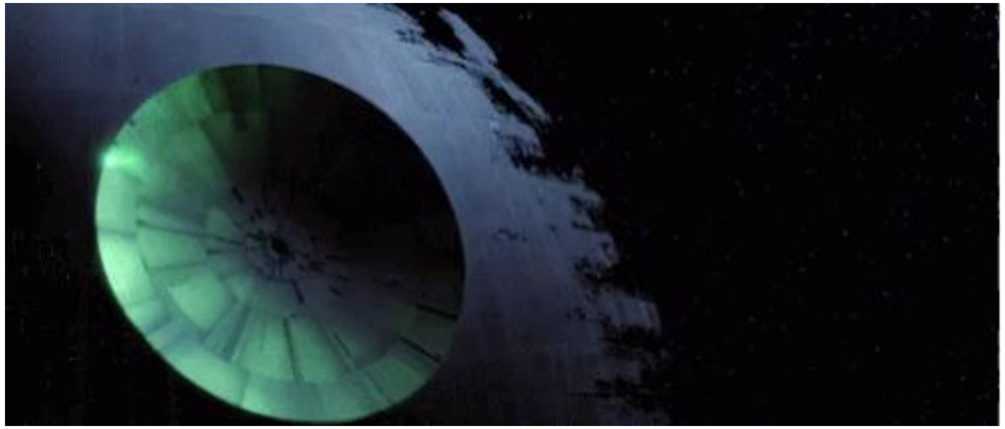
Practical advantages

Freespace communication has a high loss!

- Qi and Siopsis (2015): known quantum PVs break with high loss
- Loss-tolerant quantum PV:
  - Qi, Lo, Lim, Siopsis, Chitambar, Pooser, Evans, Grice (2015)
  - Chakraborty, Leverrier (2015)
  - Lim, Xu, Siopsis, Chitambar, Evans, Qi (2016)
  - Speelman (2016)
- LXSCEQ (2016) & Allerstorfer, Buhrman, Speelman, Lunel (2021): *fully* loss-tolerant quantum PV against *unentangled* adversaries
- Our work: full loss tolerance against entangled adversaries

Practical advantages, cont’d

Freespace quantum communication requires a tracking laser



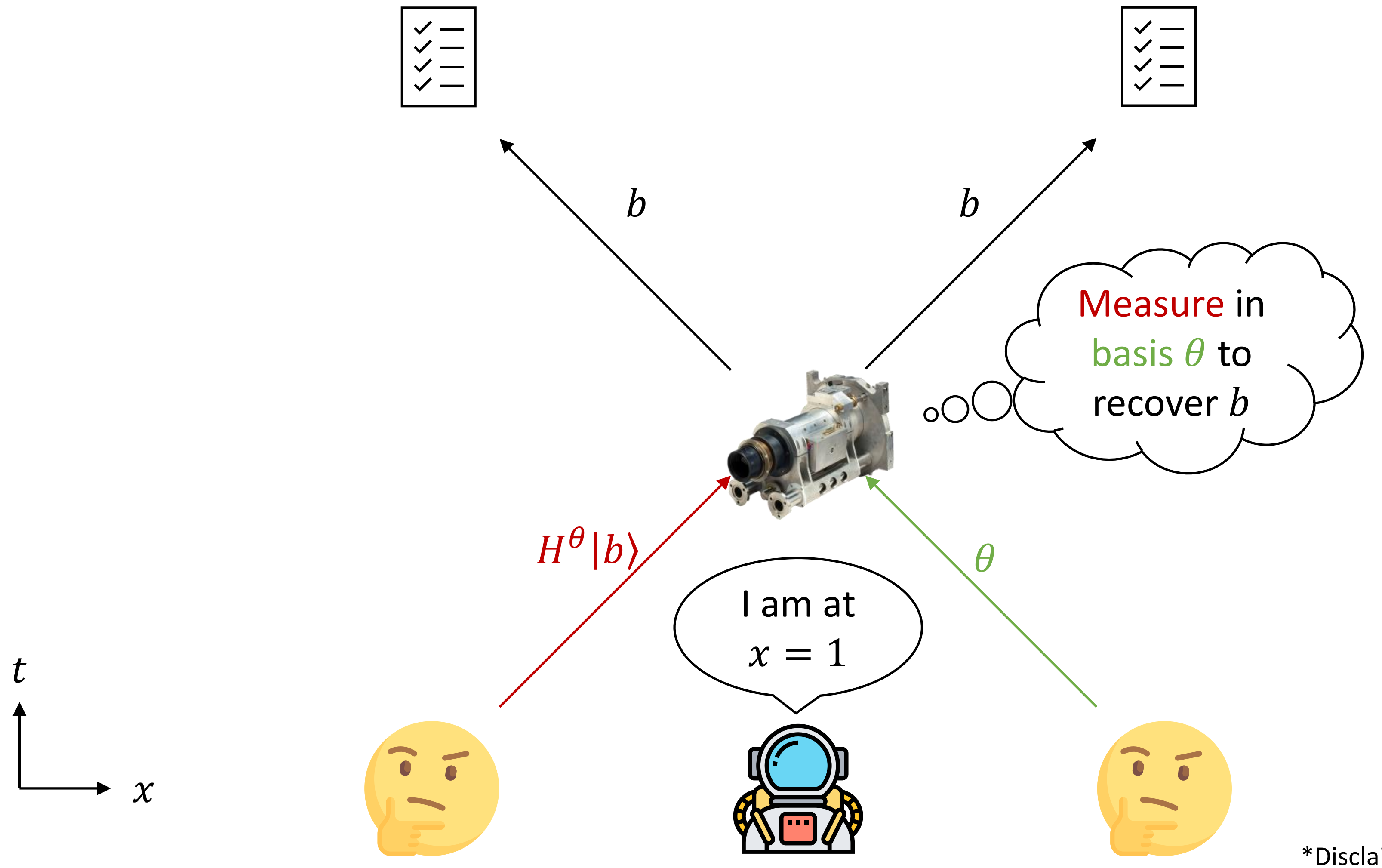
Quantum information is harder to compose for position-based cryptography, e.g., authentication

BB84 states [Wiesner ca. 1969]

- Computational basis: $|0\rangle, |1\rangle$
- Hadamard basis:
  - $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  - $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- Can recover the bit given the basis and the state
- Provably information theoretically unclonable w/o knowing basis

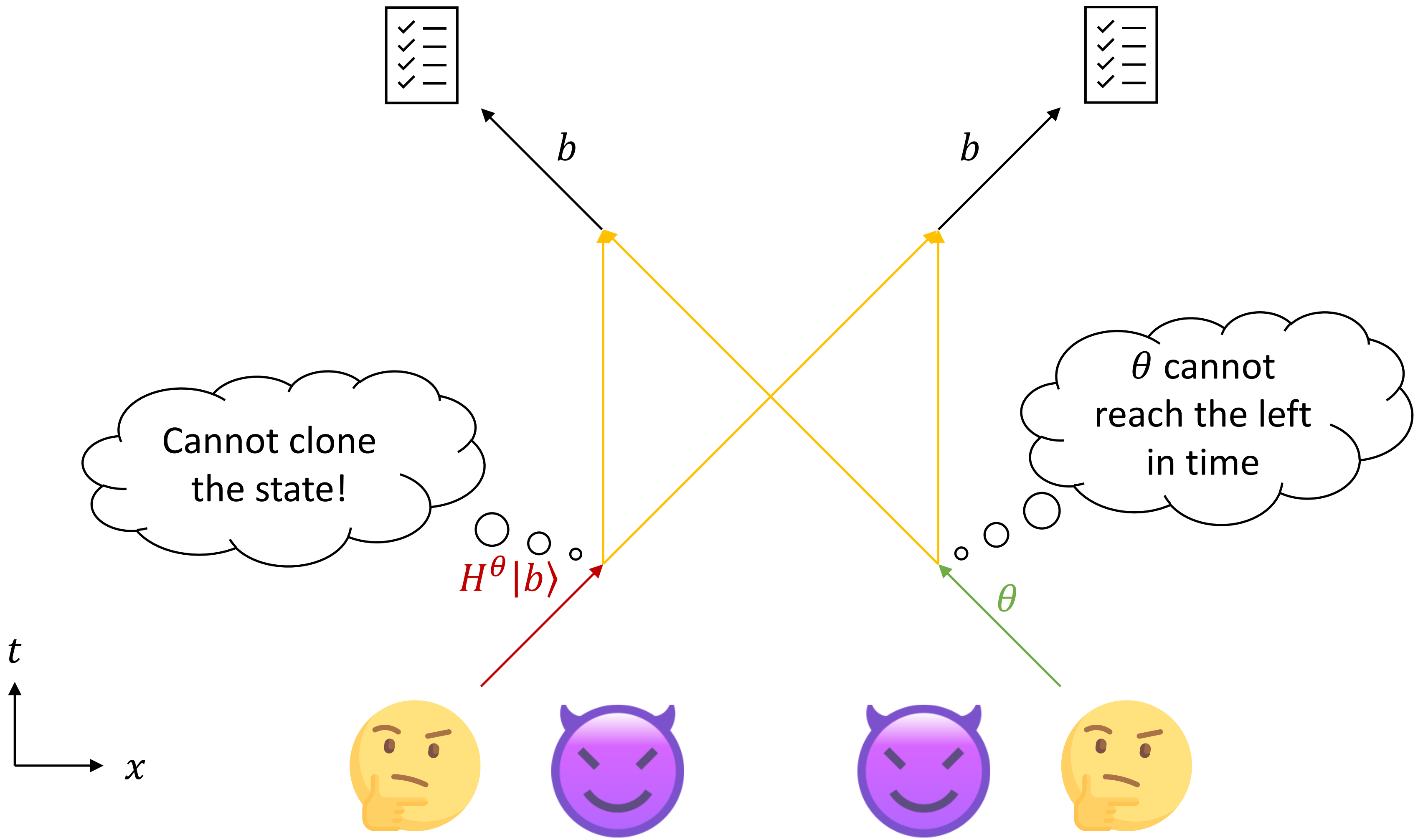
Quantum position verification with BB84

[BCFGGOS10, BK11, KMS11, TFKW13, …]

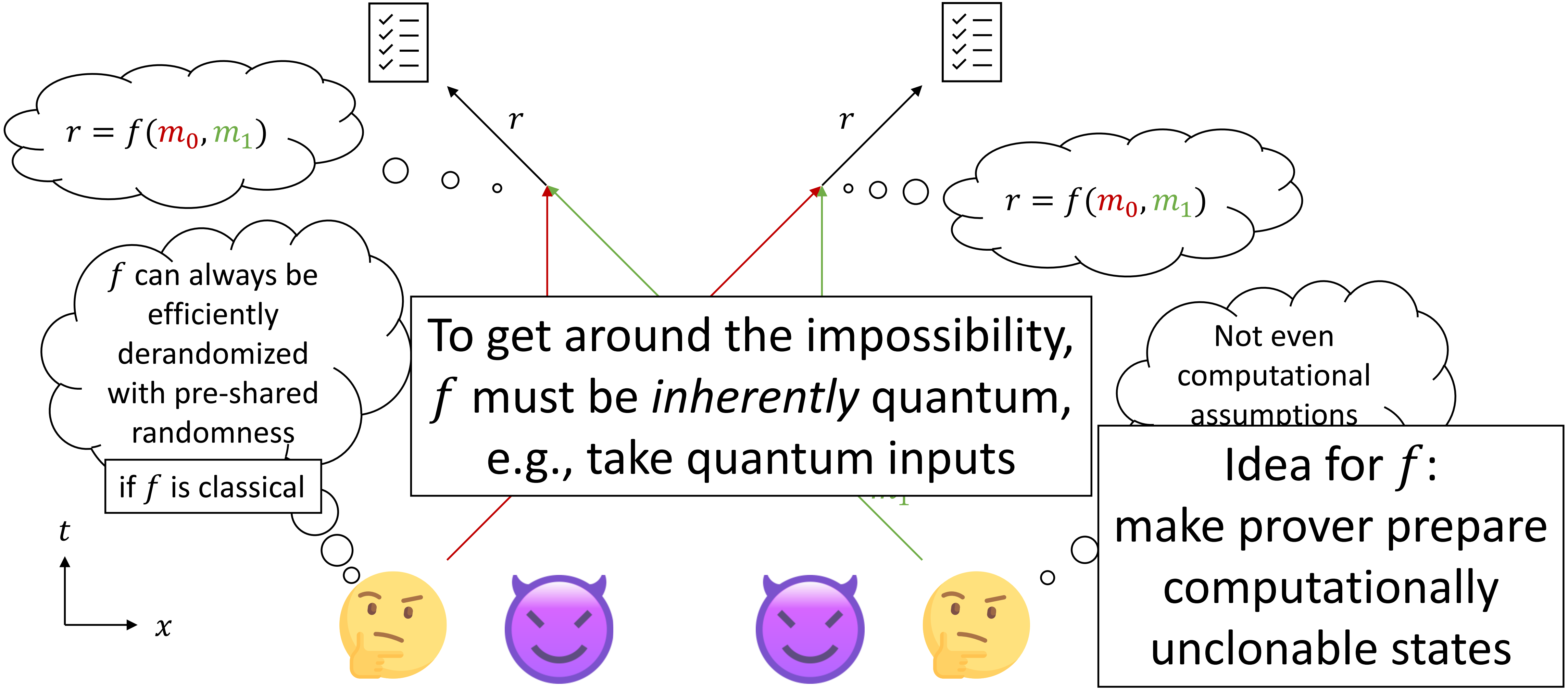


*Disclaimer: potentially inaccurate physical devices

BB84 position verification security [TFKW13]



Position verification impossibility



To get around the impossibility, f must be *inherently* quantum, e.g., take quantum inputs

Idea for f: make prover prepare computationally unclonable states

Trapdoor claw-free functions

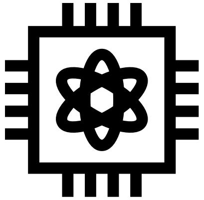
[Goldwasser, Micali, Rivest ’84]

$$f_{pk}\colon \{0,1\}^n \to \{0,1\}^m$$

- Claw-free: 2-to-1, hard to find collisions efficiently
- Trapdoor: $\exists td$ allows efficient inversion $y \to x_0, x_1$
- Adaptive hardcore bit: …

Proof of quantumness

[Brakerski, Christiano, Mahadev, Vazirani, Vidick; 2018]



$\frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle \boxed{|f_{pk}(x)\rangle}$ ← pk — td

$\frac{1}{\sqrt{2}}(|x_0\rangle + |x_1\rangle)$ → y → x_0, x_1

unclonable

← θ

→ ans

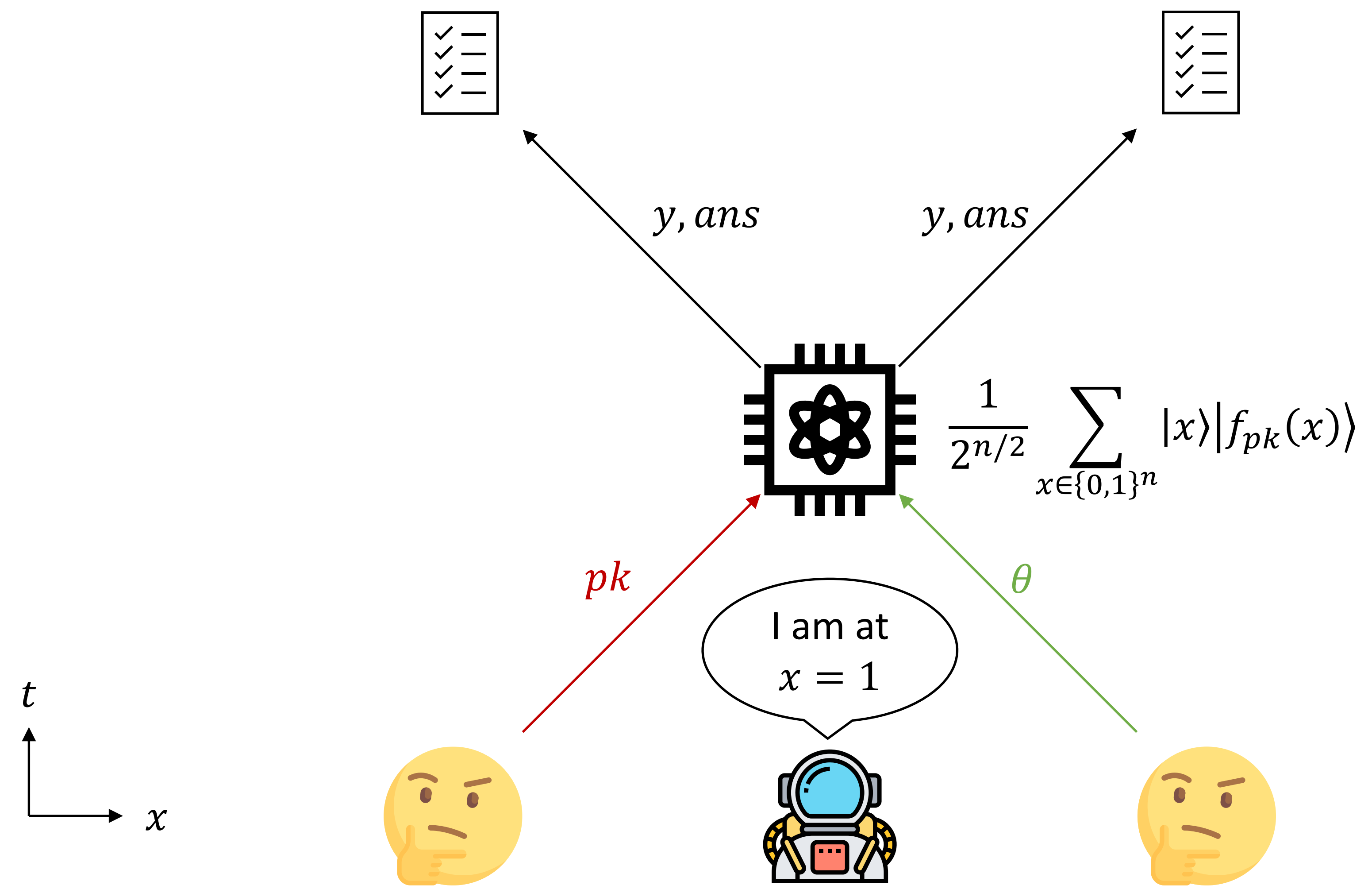
If $\theta = 0$, $ans = x_0$ or $ans = x_1$

If $\theta = 1$, $ans \cdot (x_0 \oplus x_1) = 0$ (and $ans \neq 0^n$)

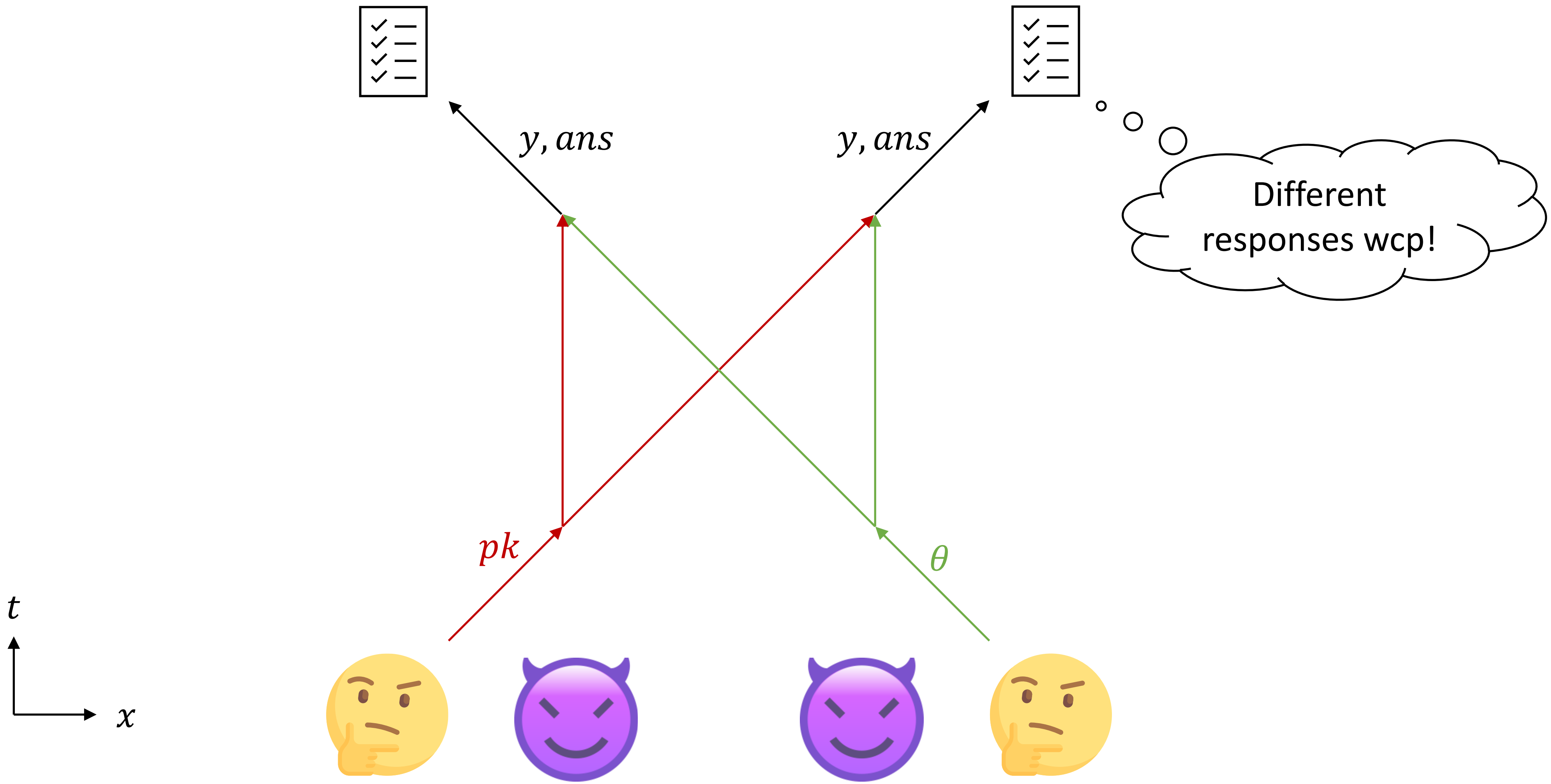
Noisy variant from LWE

Adaptive hardcore bit: cannot efficiently produce y, ans_0, ans_1 *simultaneously* with probability $\gg \frac{1}{2}$

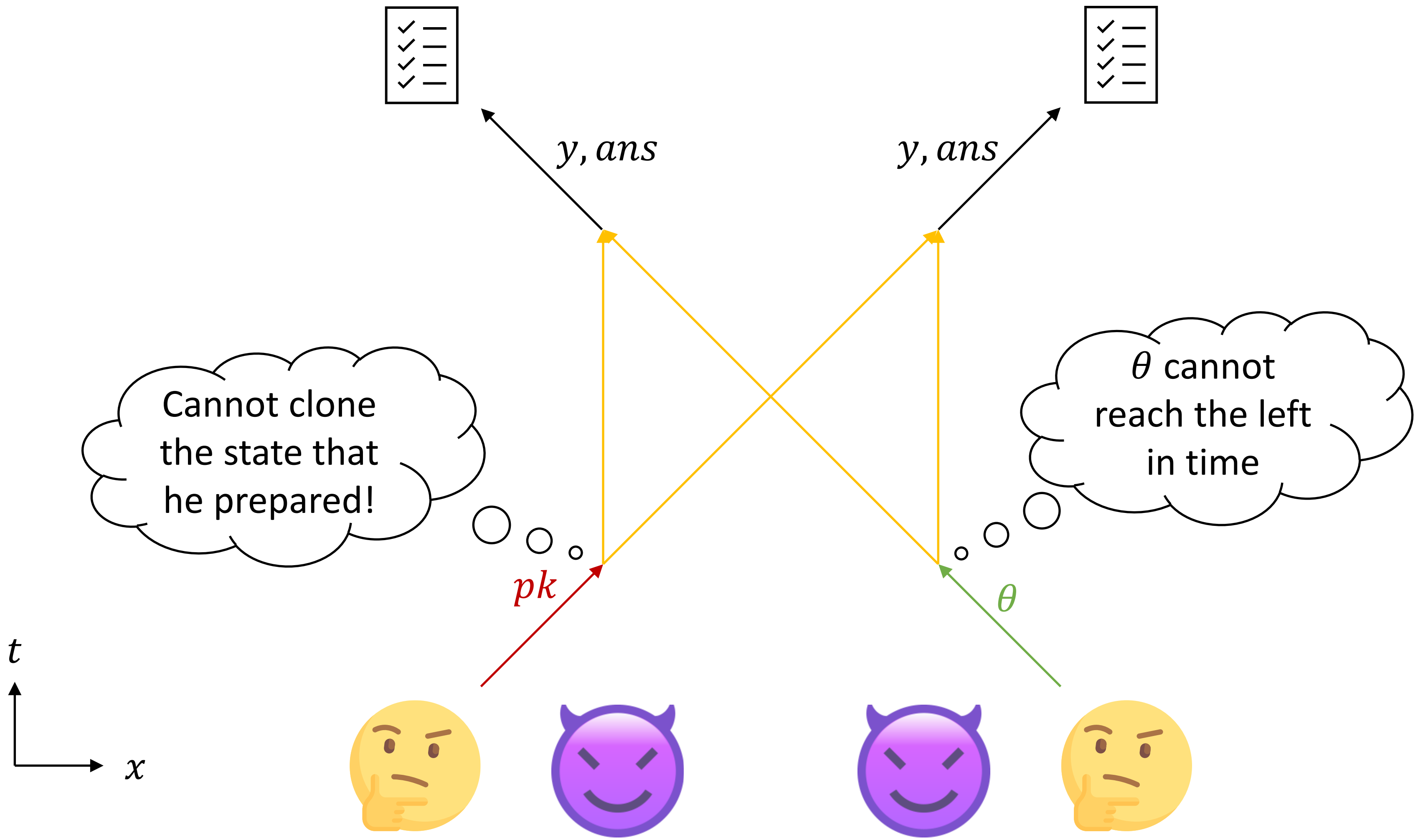
First attempt



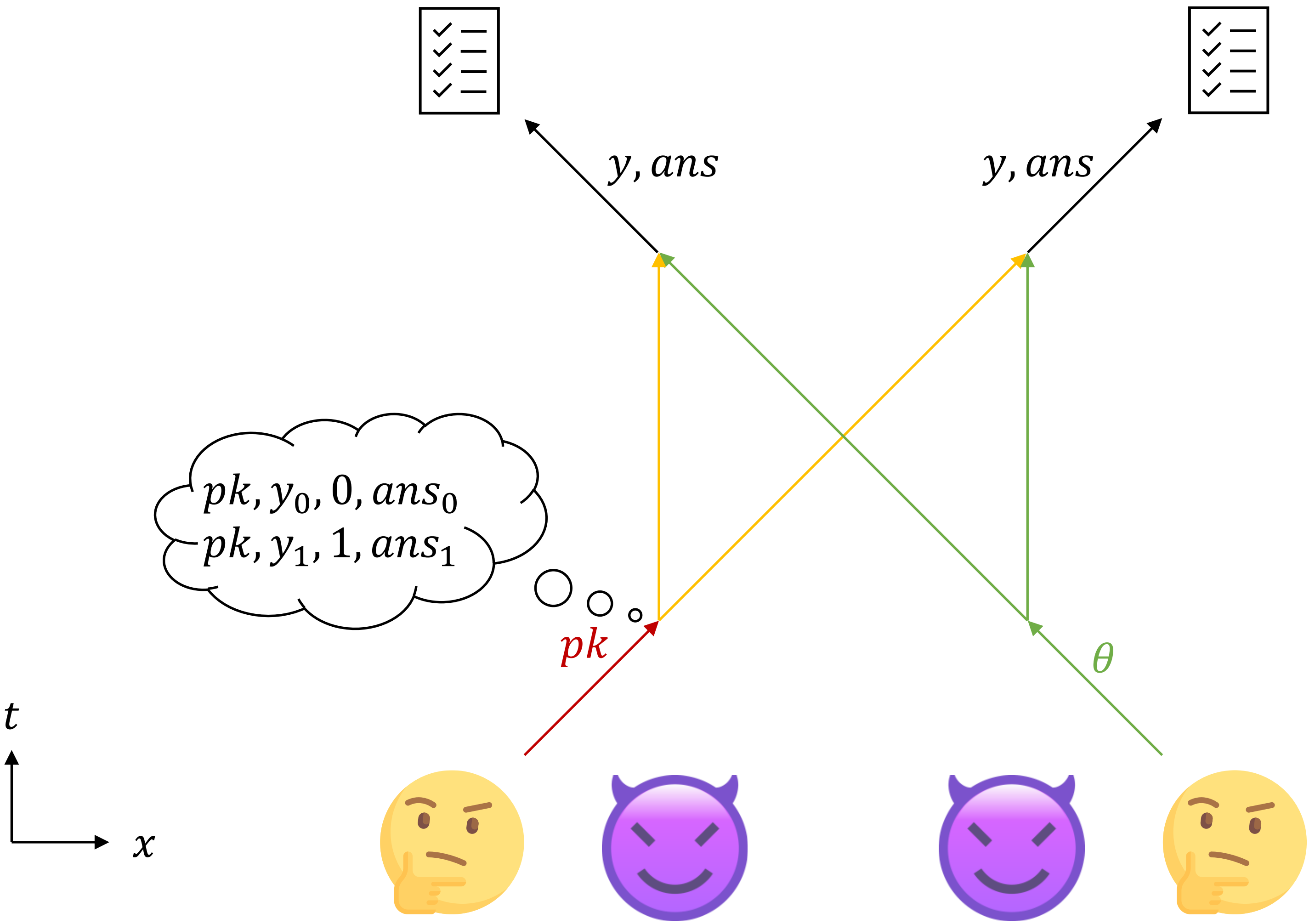
First attempt, cont'd



First attempt, cont'd

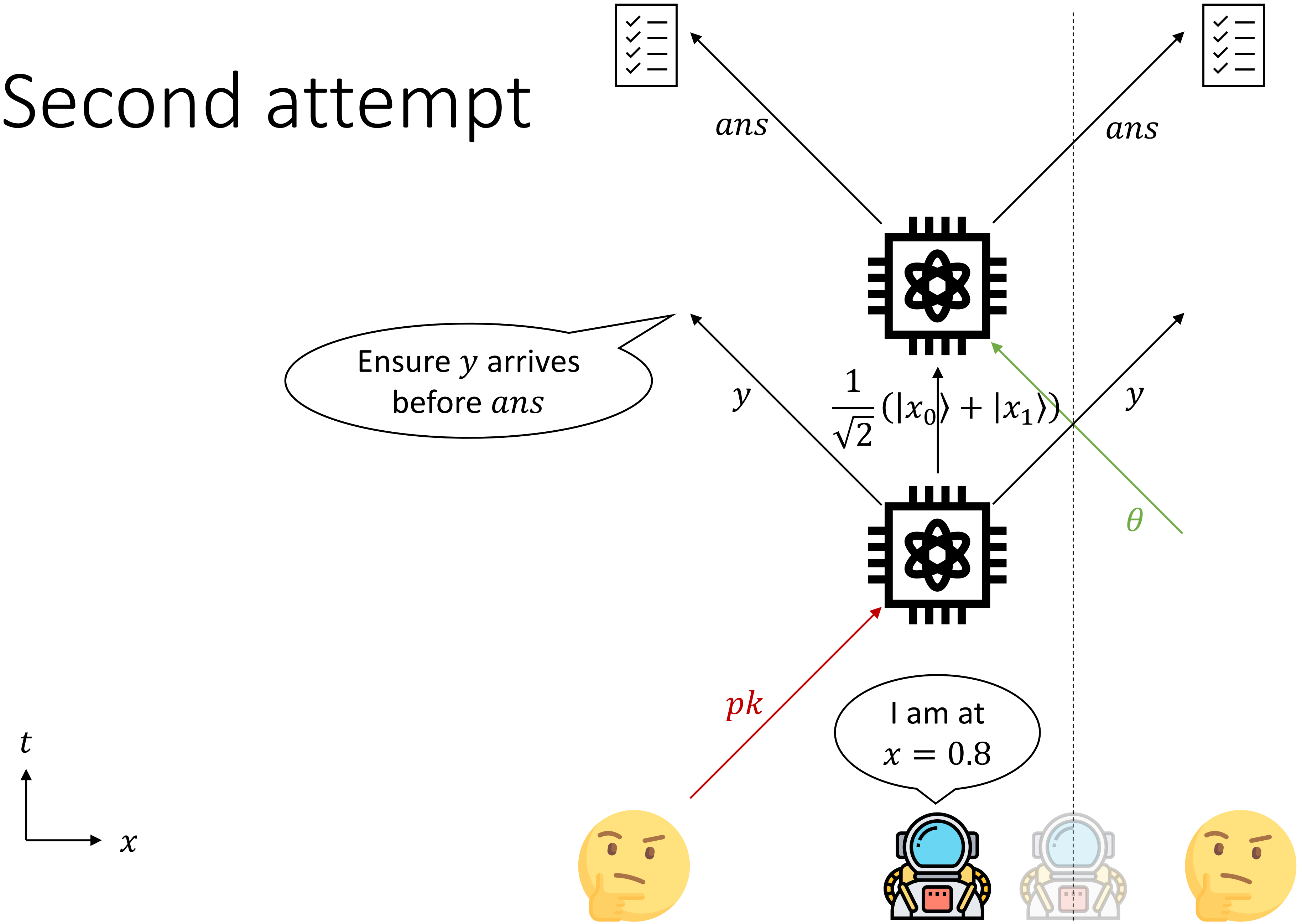


First attempt, attack

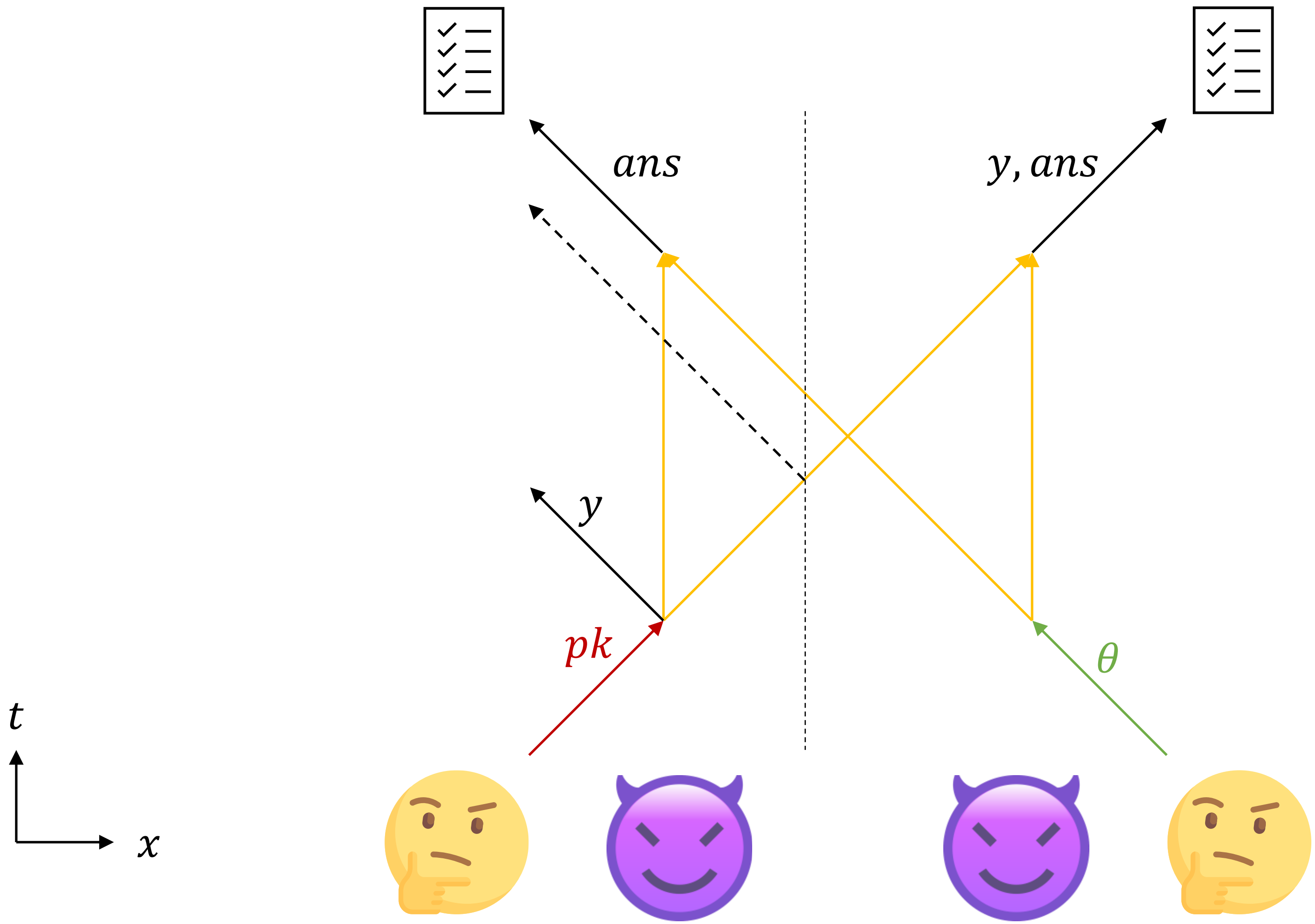


Idea: need to make prover commit to y

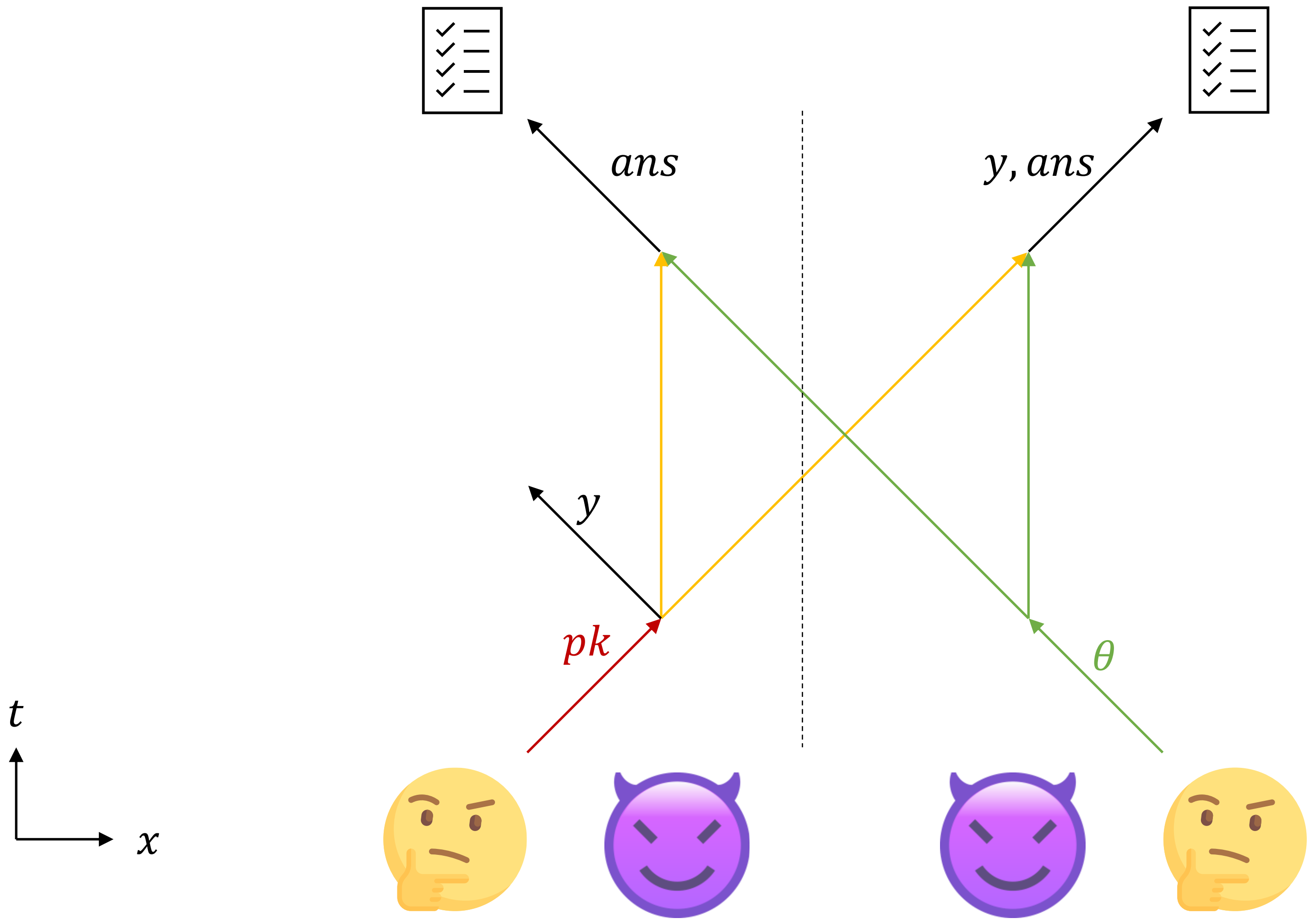
Second attempt



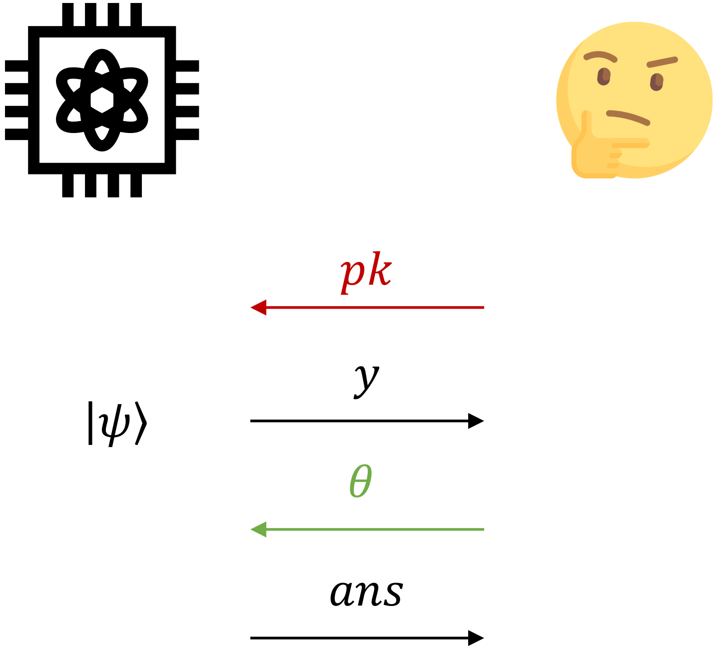
Second attempt, analysis



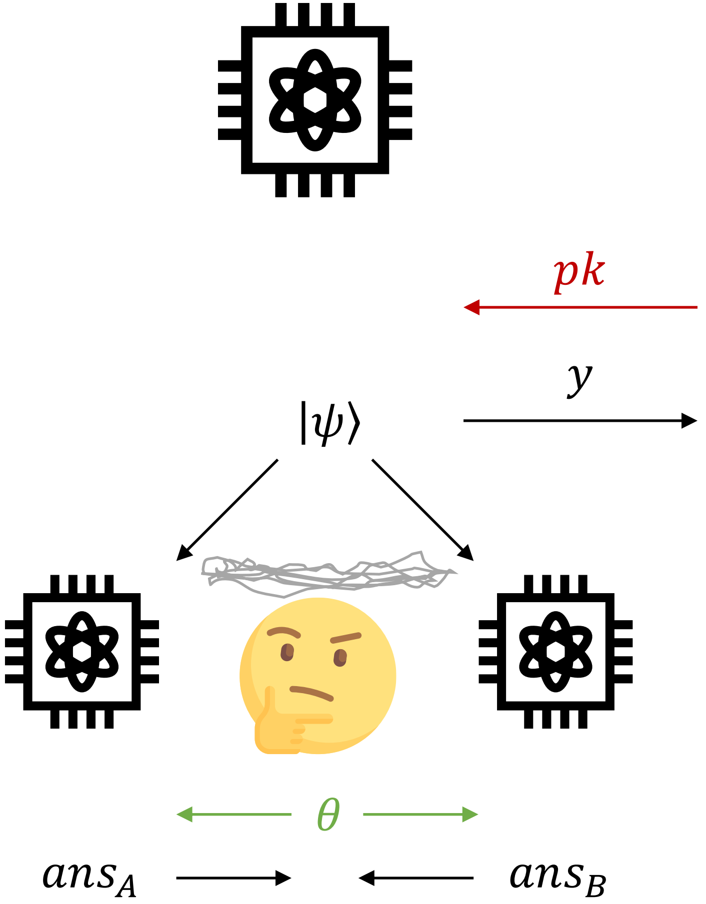
Security proof

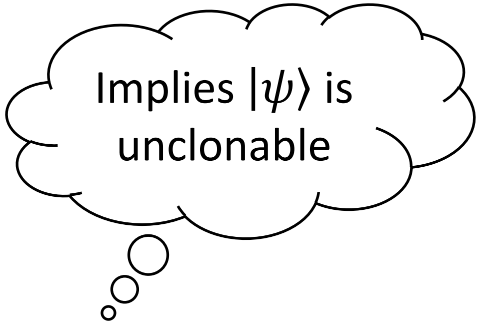


Computational non-local game of TCFs



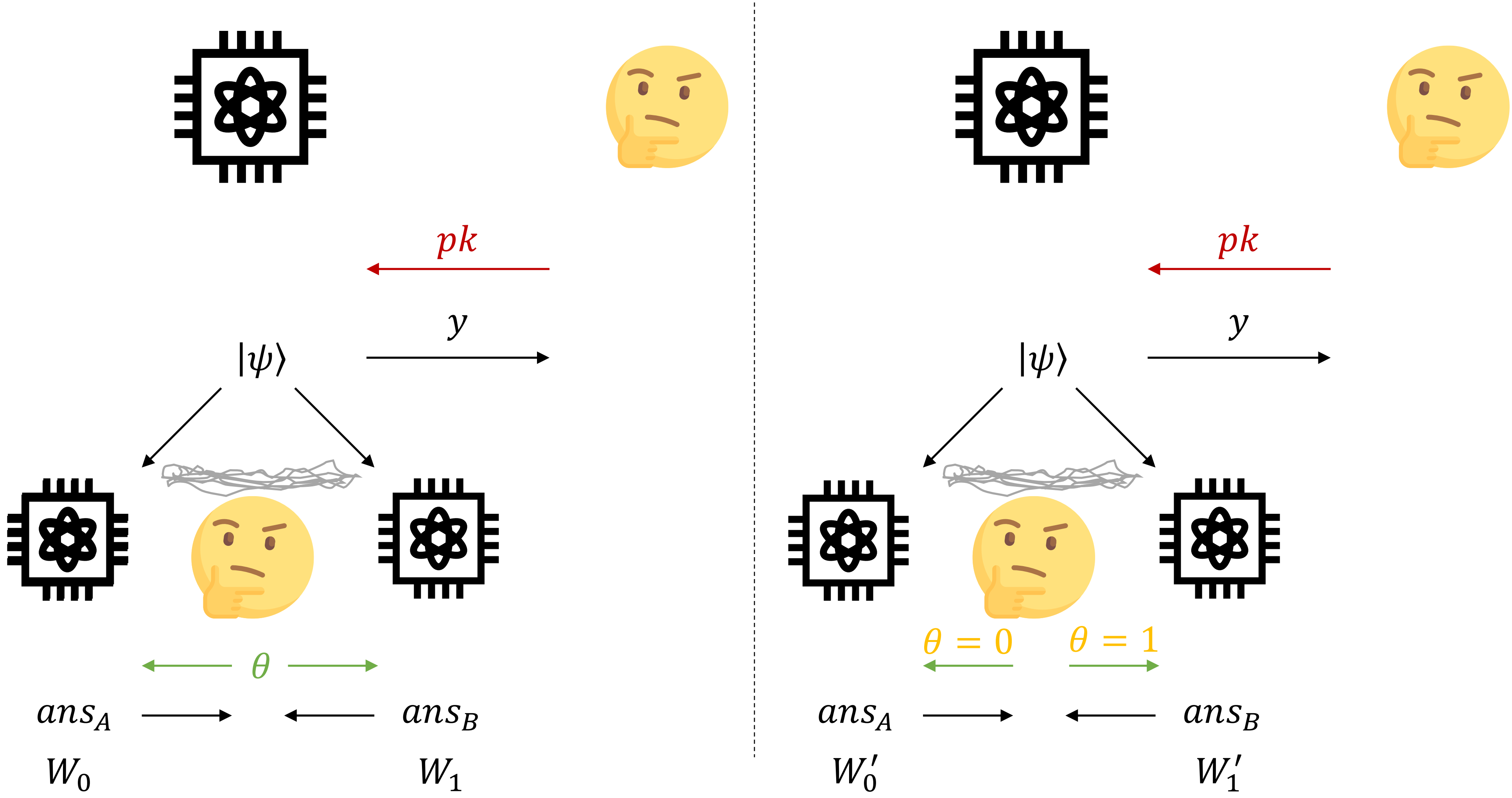
Computational non-local game of TCFs





Claim: success probability of passing both checks simultaneously is at most $\frac{3}{4}$

Computational non-local game of TCFs



Reduction to adaptive hardcore bit

Claim: By no-signaling, $\Pr[W_0'] = \Pr[W_0|\theta = 0]$
$\Pr[W_1'] = \Pr[W_1|\theta = 1]$

$$\Pr[W_0 \wedge W_1] = \frac{1}{2}(\Pr[W_0 \wedge W_1|\theta = 0] + \Pr[W_0 \wedge W_1|\theta = 1])$$
$$\leq \frac{1}{2}(\Pr[W_0|\theta = 0] + \Pr[W_1|\theta = 1])$$
$$= \frac{1}{2}(\Pr[W_0'] + \Pr[W_1']) \text{ (no signaling)}$$
$$\leq \frac{1}{2}(1 + \Pr[W_0' \wedge W_1']) \text{ (union bound)}$$
$$\leq \frac{3}{4} + \text{negl} \qquad \text{(adaptive hardcore bit)}$$

Other results

- Negligible soundness via parallel repetition
  [Radian, Sattath 2019; Alagic, Childs, Grilo, Hung 2020; Chia, Chung, Yamakawa 2020]
- Security against entangled adversaries
  - Bounded entanglement from subexponential hardness ($\exp(n^{\varepsilon})$-hardness)
    [Aaronson 2005; TFKW13]
  - Unbounded entanglement in the quantum random oracle model (QROM)
    [Unr14]
- Attack with entangled adversaries for standard model constructions

Future directions

- High dimensional classically verifiable position verification (CVPV)
- Time-entanglement trade-offs
- Is quantum memory/unclonability inherent for CVPV?
- Weakening the assumption/ideal model

Thank you!

Icons from flaticon.com
Picture of laser from wikipedia.org