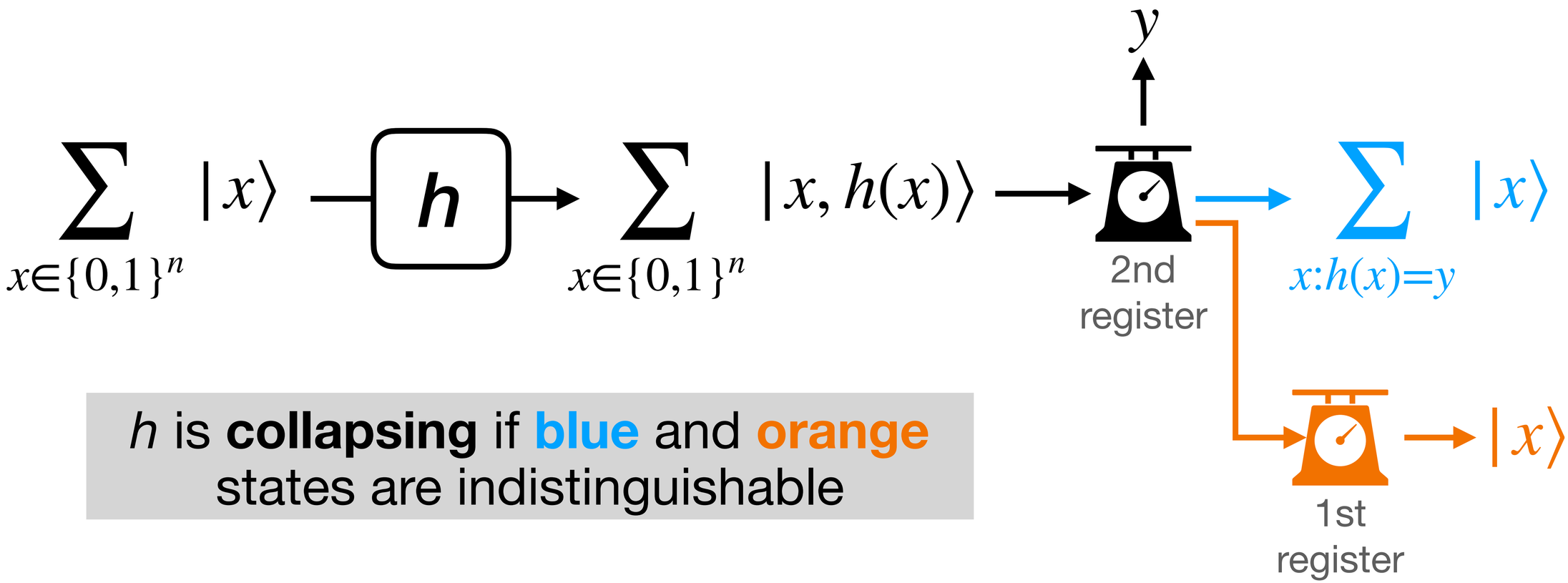
One-shot signatures from non-collapsing hash functions

Based on joint work with Marcel Dall'Agnol

Nick Spooner, 26th January 2024, University of Edinburgh

*simplified definition

Collapsing hash functions*



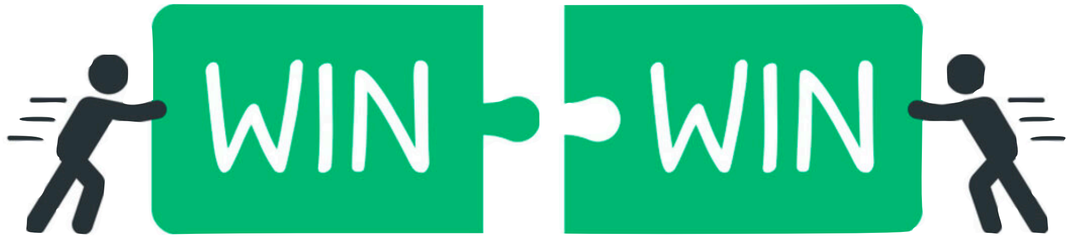
h is **collapsing** if **blue** and **orange** states are indistinguishable

Collapsing **implies** post-quantum collision resistance

Turns out to be the “correct” strengthening of CR for many applications

(ZKPs, succinct arguments, etc.)

Big open question: does PQ-CR imply collapsing?



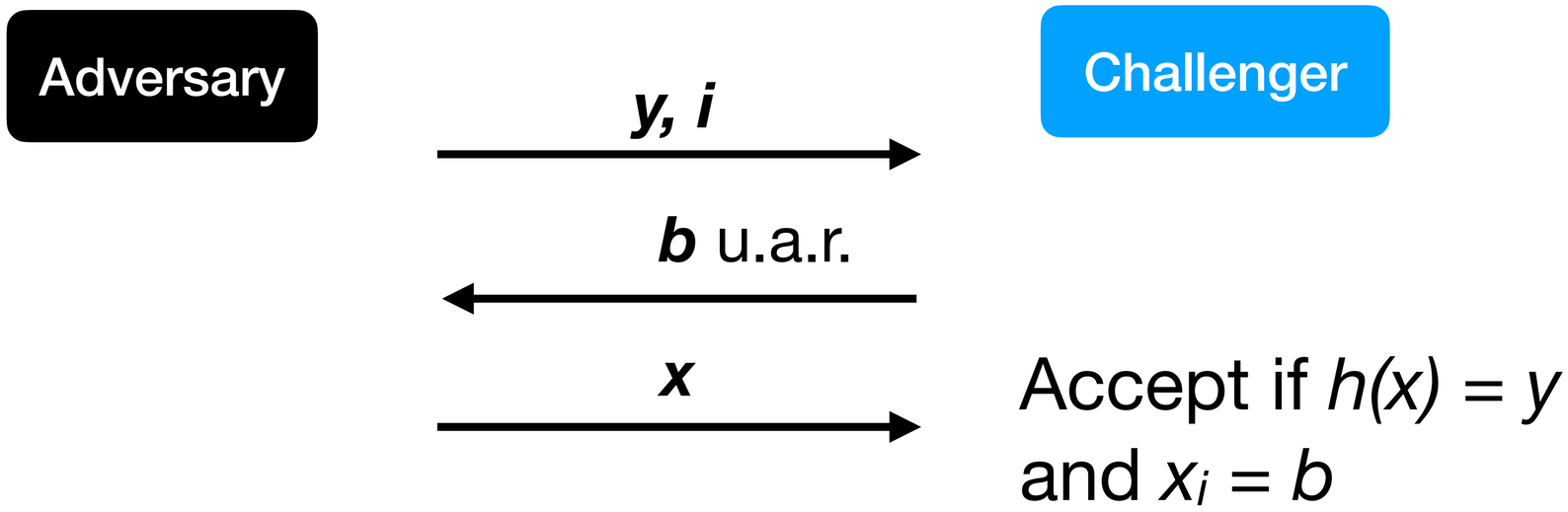
if **yes**, then collision resistance is **enough** for PQ security of protocols

(the answer is known to be **yes** for “regular” CRHFs [Zhandry22])

if **no**, then we get cool quantum crypto!

- quantum lightning (strengthening of quantum money) [Zhandry19]
- **one-shot signatures [DS23]**

Equivocation game



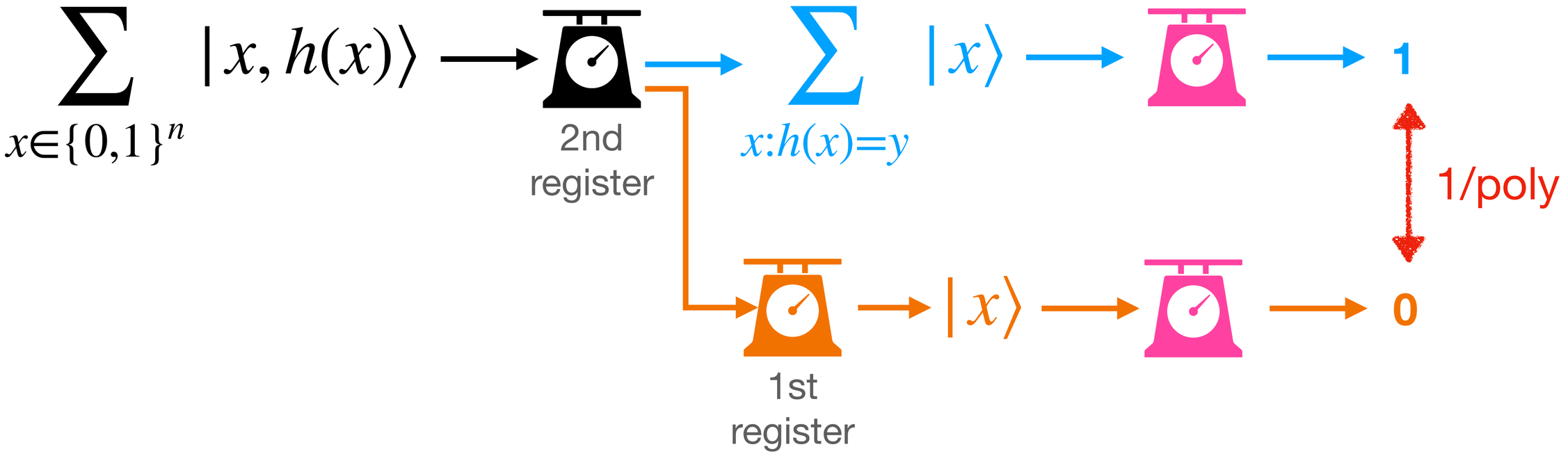
If ***h*** is collision-resistant, classical adversary wins w.p. <1/2+negl.

If ***h*** is **collapsing**, quantum adversary wins w.p. <1/2+negl. [Unruh16, CMSZ21]

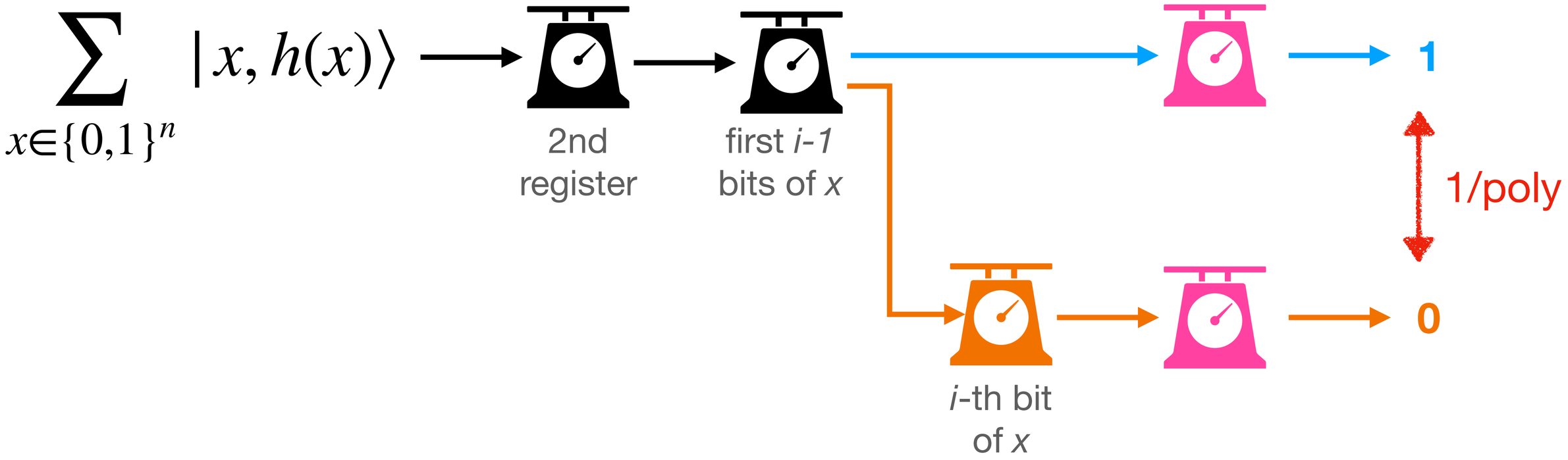
Can transform a quantum adversary winning w.p. **>1/2+1/poly** into OSS [DS23]

We show [DS23]: if *h* is **not** collapsing there **is** such an adversary

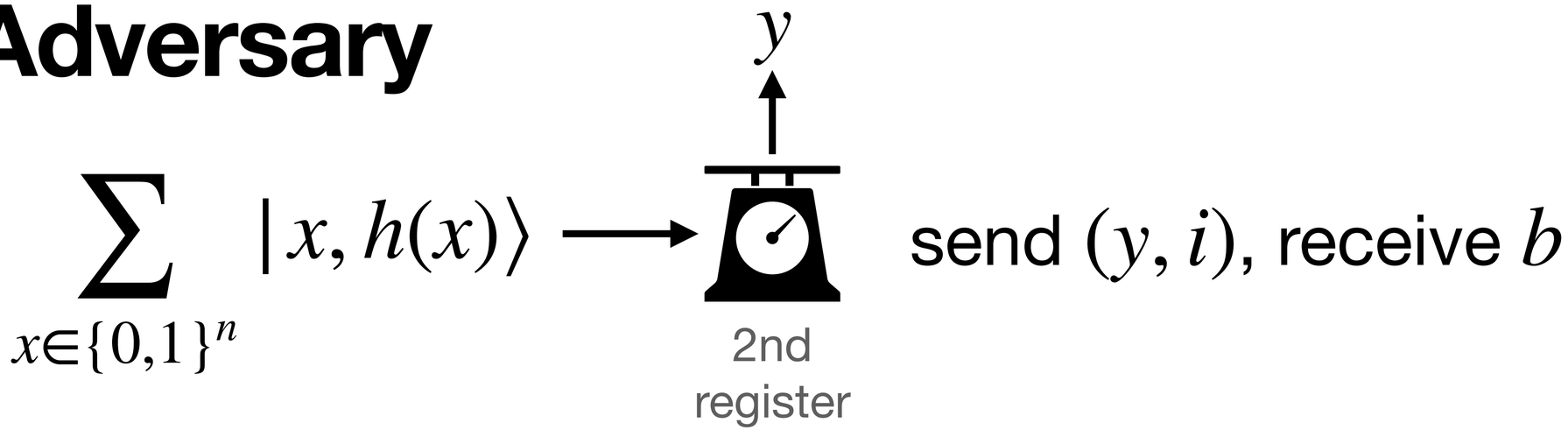
Suppose h is **not** collapsing:

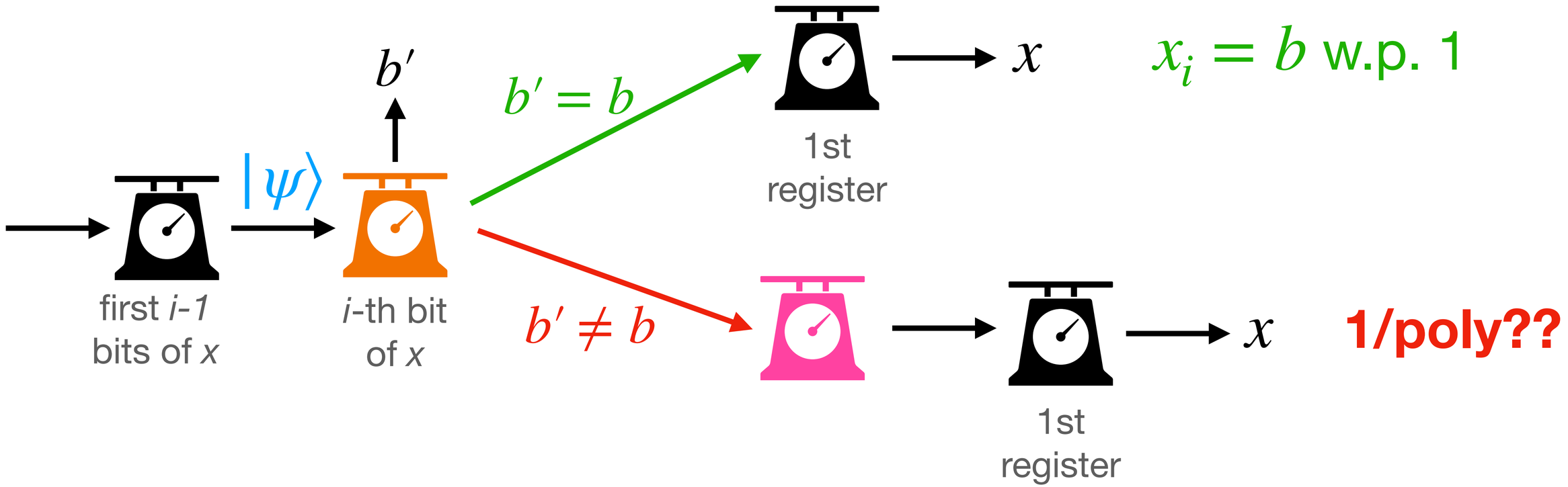


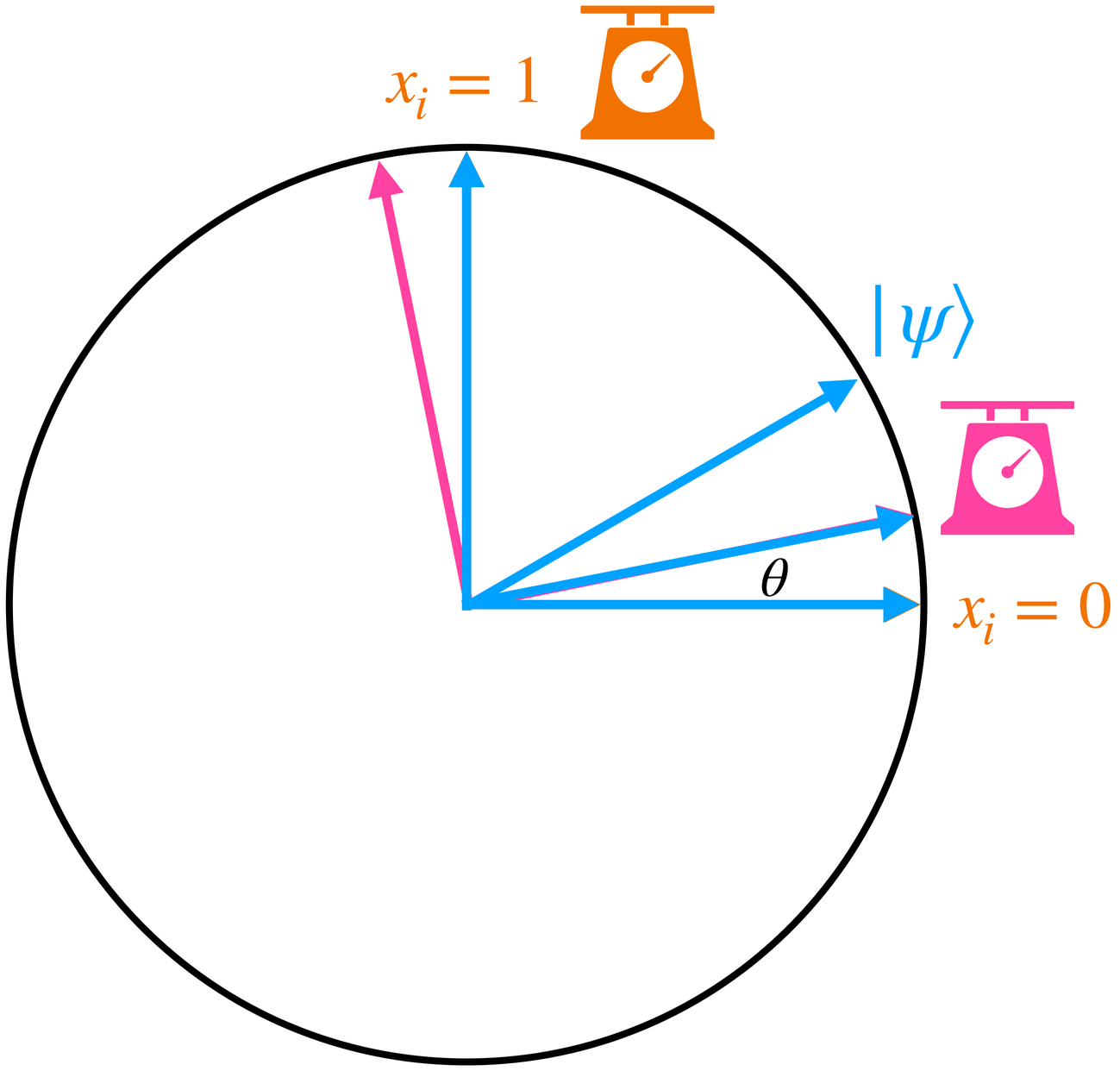
There is some index *i* such that:

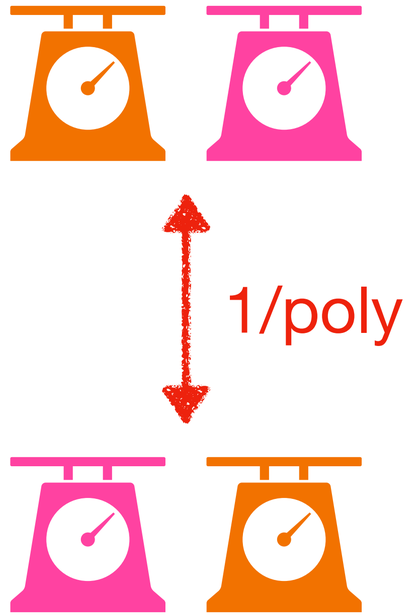


Adversary


$\sum_{x\in\{0,1\}^n} |x, h(x)\rangle$
y
2nd register
send (y, i), receive b


first i-1 bits of x
$|\psi\rangle$
b'
i-th bit of x
$b' = b$
1st register
x
$x_i = b$ w.p. 1
$b' \neq b$
1st register
x
1/poly??





$\Rightarrow \theta \geq 1/\text{poly}$

Applying orange measurement again gives **opposite** answer w.p. 1/poly!

Open question: are there non-collapsing PQCRHFs?

Potential route to constructing one-shot signatures (+ quantum money, etc.)

Many "natural" CRHFs *are* collapsing:

- Random functions [Unruh16]
- Ajtai hash function from LWE [LZ19, Poremba23]
- Polynomially-regular hash functions [Zhandry22]
- Optimally-secure CRHFs (PQ security $p(\lambda)/2^{\lambda}$) [Zhandry22]

Non-collapsing CRHFs must be *structured* and *sub-optimally secure.*