CHSH Game Reductions

CMSC858F Final Project Presentation

Rushil Dandamudi | December 8, 2022

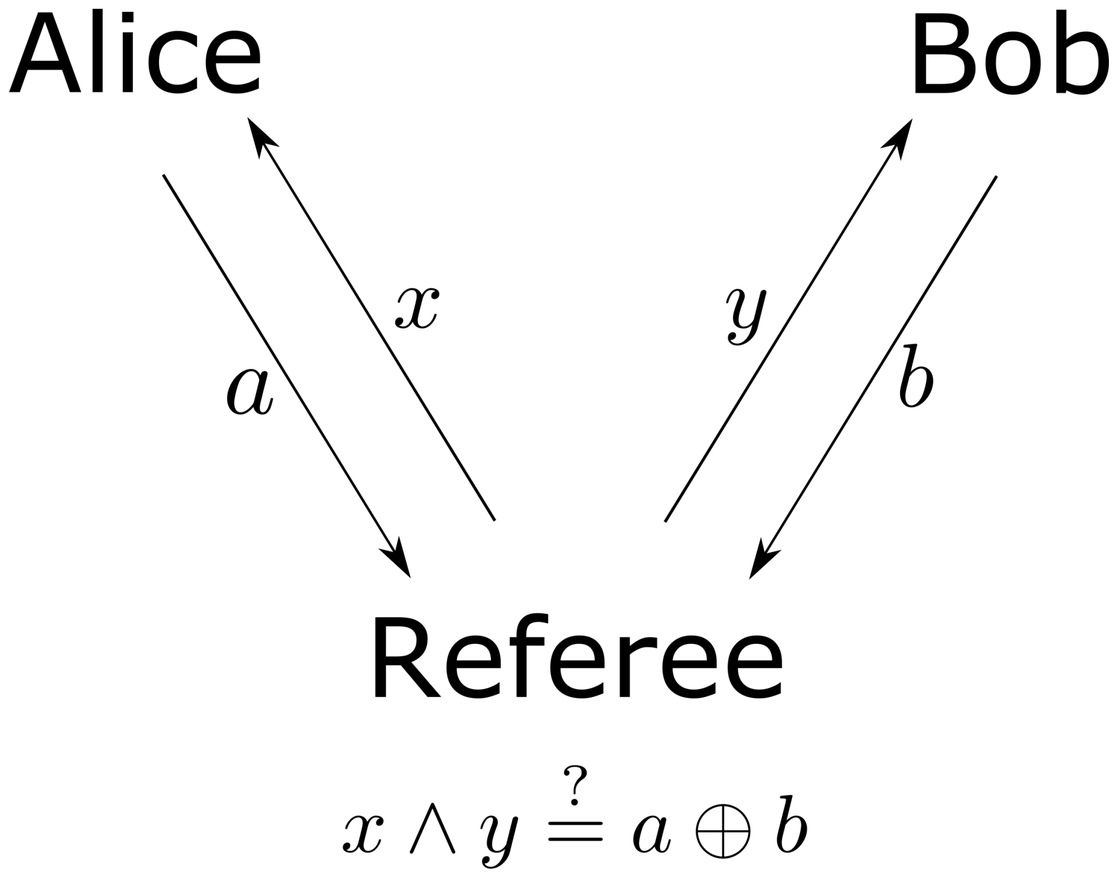
1

Background

2

The CHSH Game

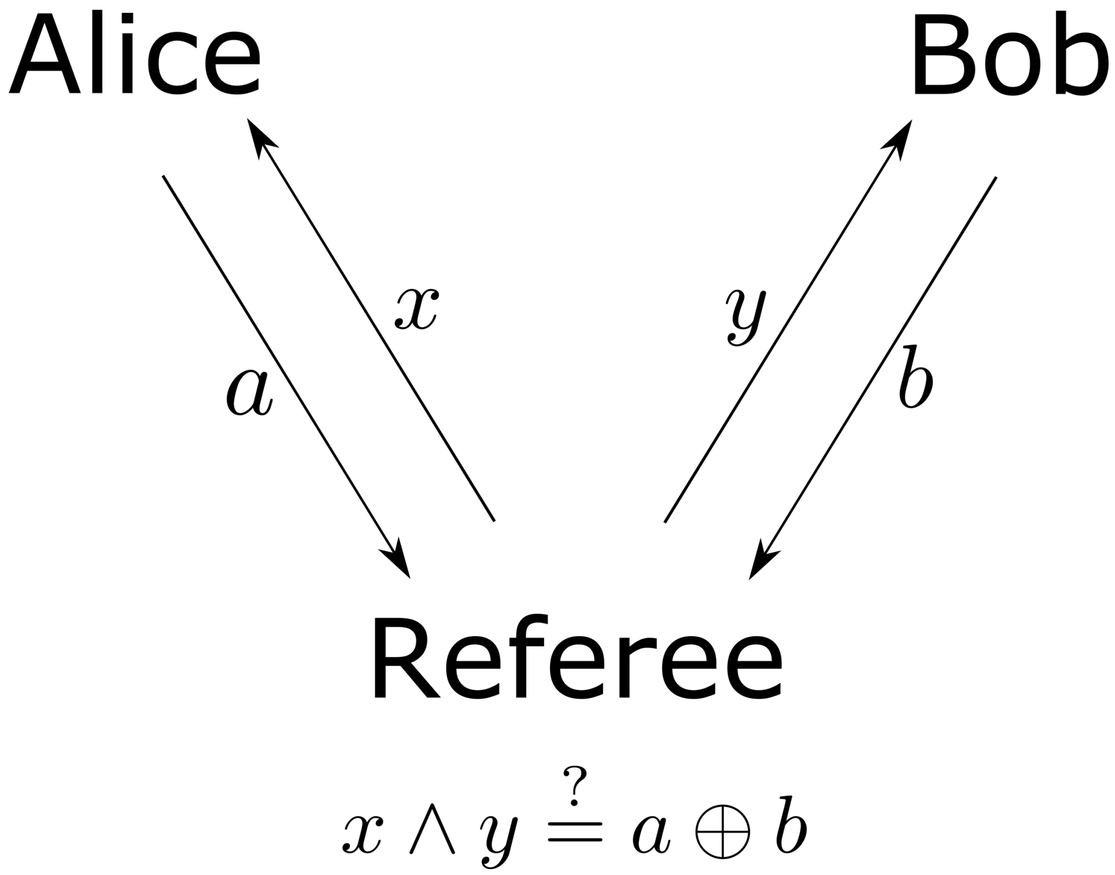
Clauser, Horne, Shimony, Holt: 1969 | APS



3

The CHSH Game

Clauser, Horne, Shimony, Holt: 1969 | PRA



Game Value

- Classical = .75
- Quantum = .85

Complexity Theory Ties

- Non-local games ← Graph coloring
- RG informing about BQP vs P

4

Tsirelson's Inequality

.85 is optimal for quantum players | Rigidity of CHSH

$$|S_q| = | < X_1 Y_1 > + < X_1 Y_2 > + < X_2 Y_1 > - < X_2 Y_2 > | \leq 2\sqrt{2}$$

5

Tsirelson's Inequality

.85 is optimal for quantum players | Rigidity of CHSH

$$|S_q| = | < X_1 Y_1 > + < X_1 Y_2 > + < X_2 Y_1 > - < X_2 Y_2 > | \leq 2\sqrt{2}$$

$$V(G_q) = \frac{1}{2}(1 + \frac{|S|}{4}) \rightarrow \frac{1}{2} + \frac{1}{2\sqrt{2}} = .85$$

Formula relates sum of expected measurement correlations to Referee's game challenge

Tsirelson 1980 | Letters in Mathematical Physics

Tsirelson's Inequality

.85 is optimal for quantum players | Rigidity of CHSH

$$|S_q| = | < X_1Y_1 > + < X_1Y_2 > + < X_2Y_1 > - < X_2Y_2 > | \leq 2\sqrt{2}$$

$$V(G_q) = \frac{1}{2}(1 + \frac{|S|}{4}) \rightarrow \frac{1}{2} + \frac{1}{2\sqrt{2}} = .85$$

CHSH Inequality shows $|S_c| \leq 2$
which results in .75

7

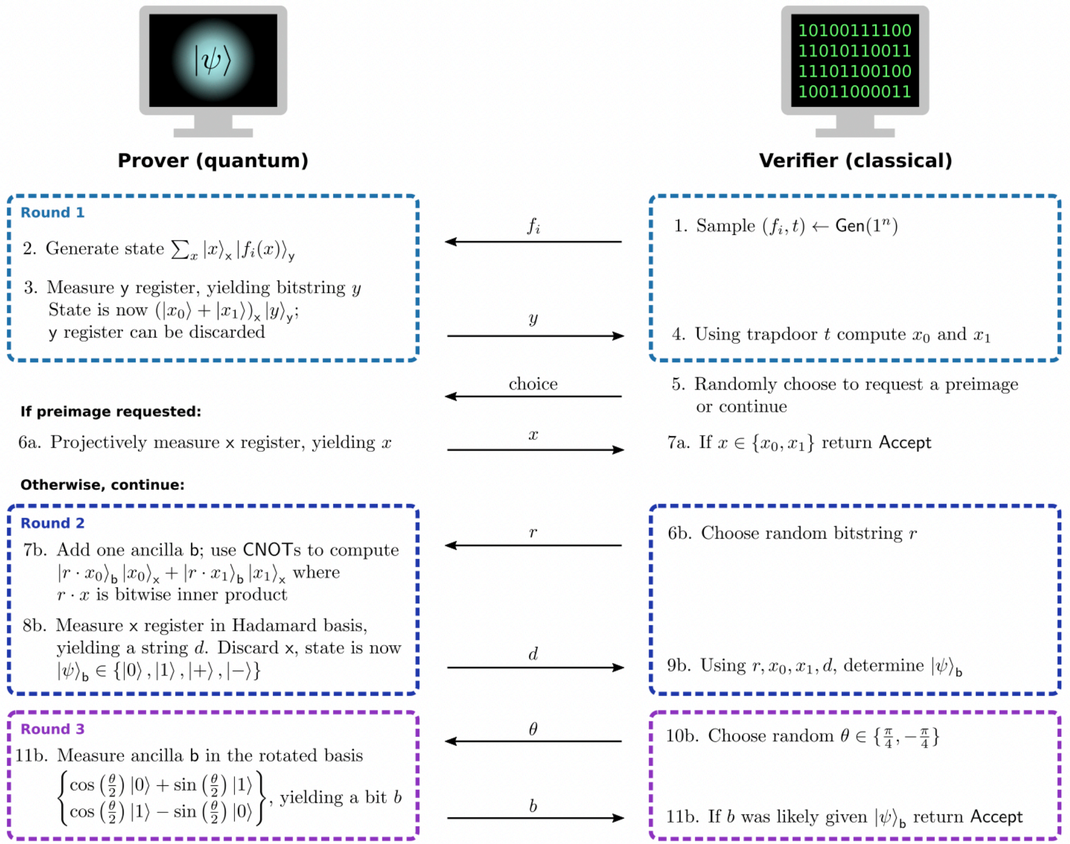
Interactive Proofs of Quantumness from CHSH

8

CHSH-based iPoQ (iPoQ-2)

Kahanamoku-Meyer et al.

- Constructs single-player game for a Proof of Quantumness
  - *“Computational Bell Test”*
  - Alice is replaced by a cryptographic construction (TCF)

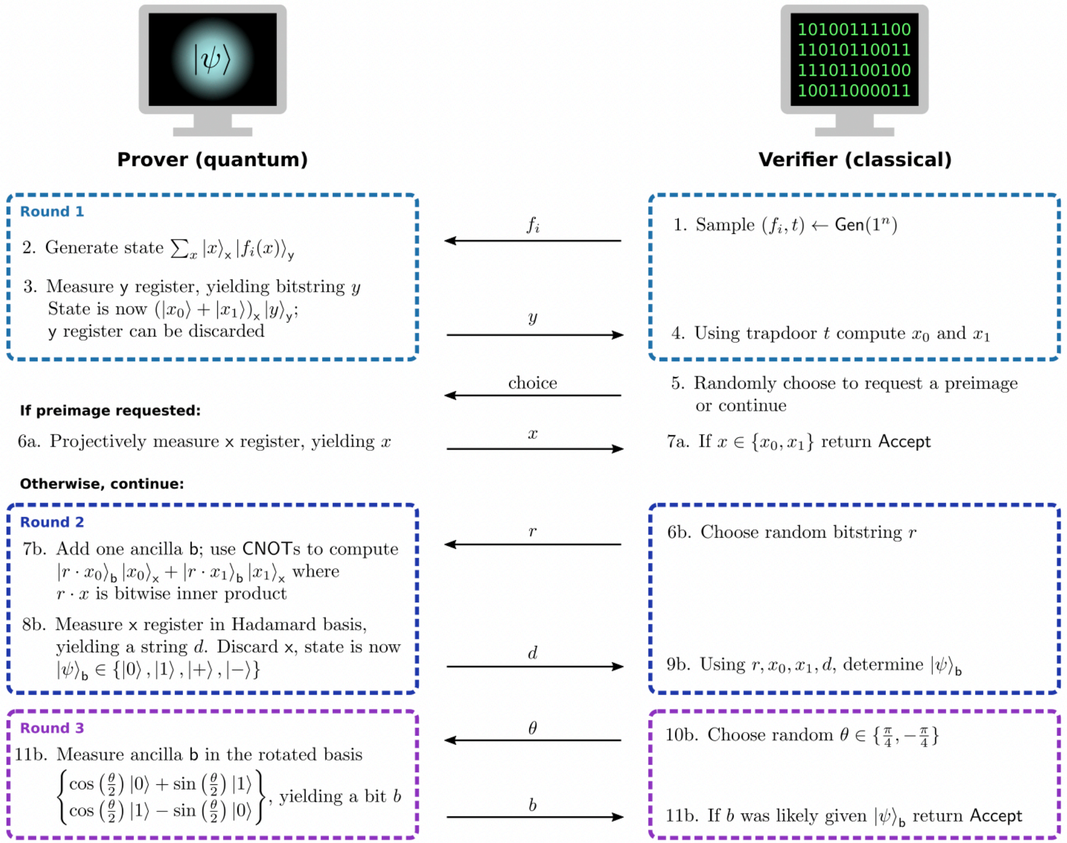


9

CHSH-based iPoQ (iPoQ-2)

Kahanamoku-Meyer, Choi, Vazirani, Yao 2021 | Nature Physics

- **Security:** hardness reduction from
  1. Claw-Free assumption:
     Winning Classical Adv →TCF Adv
  2. CHSH: *assumed, not proven*
     Gap of .10 is shown



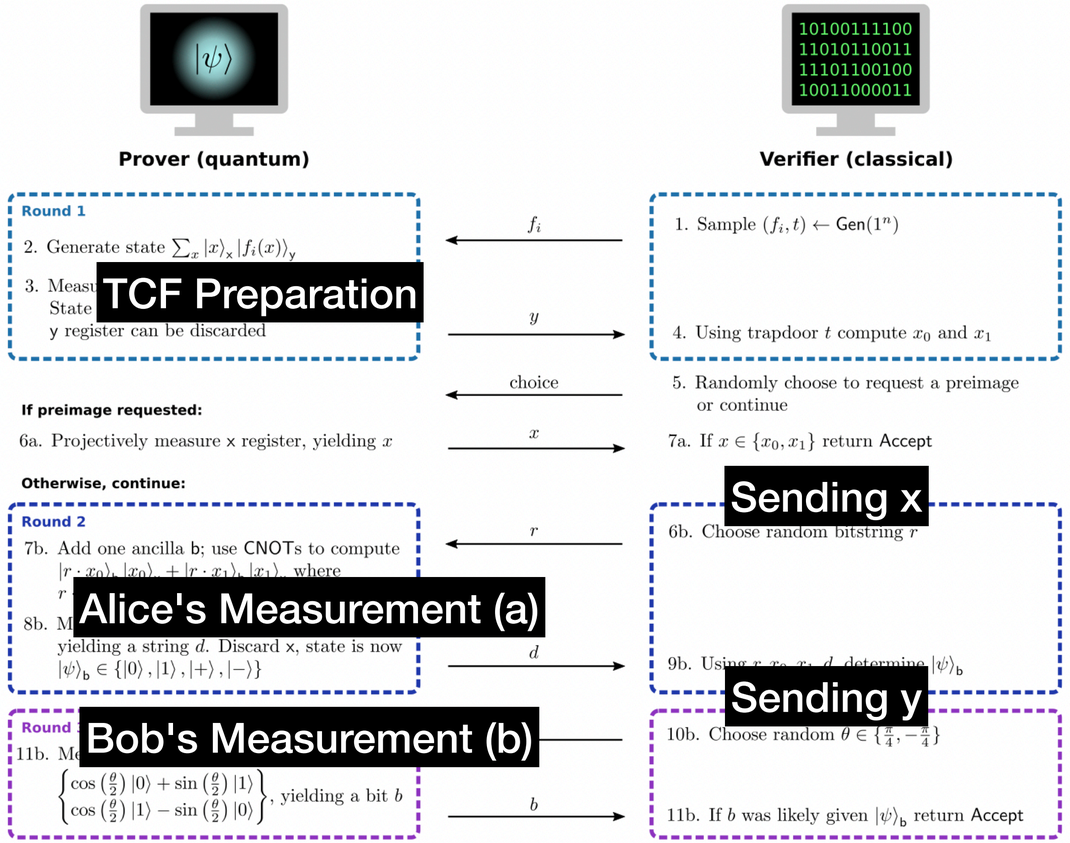
10

Reducing G-2222 to iPoQ-2

Completing security proof for iPoQ-2

- Winning Classical Adversary
  ↳ CHSH adversary

- Let (P-2,V-2) encapsulate an iPoQ-2 protocol
  - Both parties are classical
  - $P[pass] \approx .85$



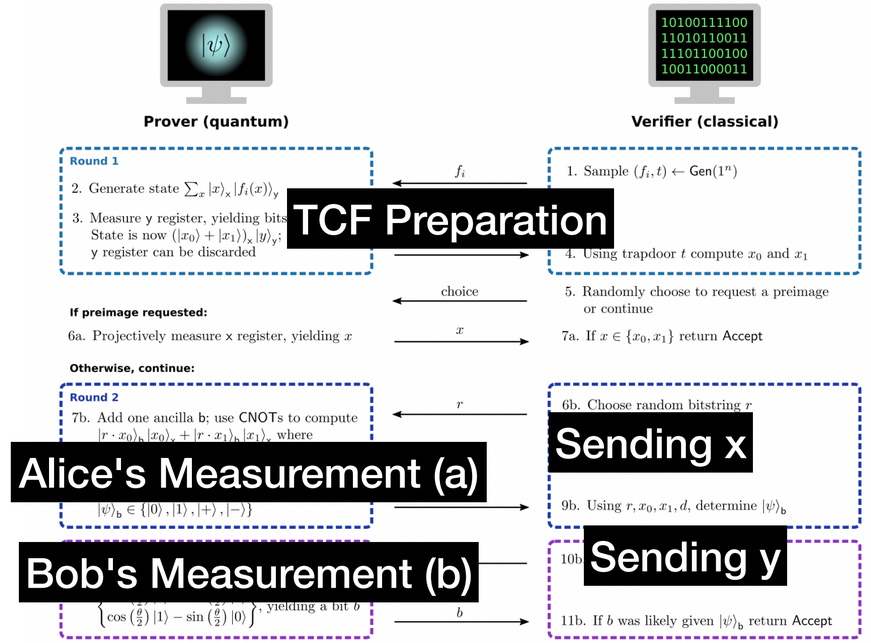
11

Reducing G-2222 to iPoQ-2

Completing security proof for iPoQ-2

- Referee R will construct Alice and Bob to play G-2222 nonlocally

  1. Alice and Bob decide strategy S
  2. Alice sends P-2 TCF f and receives f(x) from P-2
  3. Alice receives r from V-2 and sends to P-2
  4. Alice receives d from P-2
  5. $b :=$ P-2 final output
  6. $a := (r \cdot (x_0 \oplus x_1))(d \cdot (x_0 \oplus x_1) + (1 - r \cdot (x_0 \oplus x_1))(r \cdot x_0)$



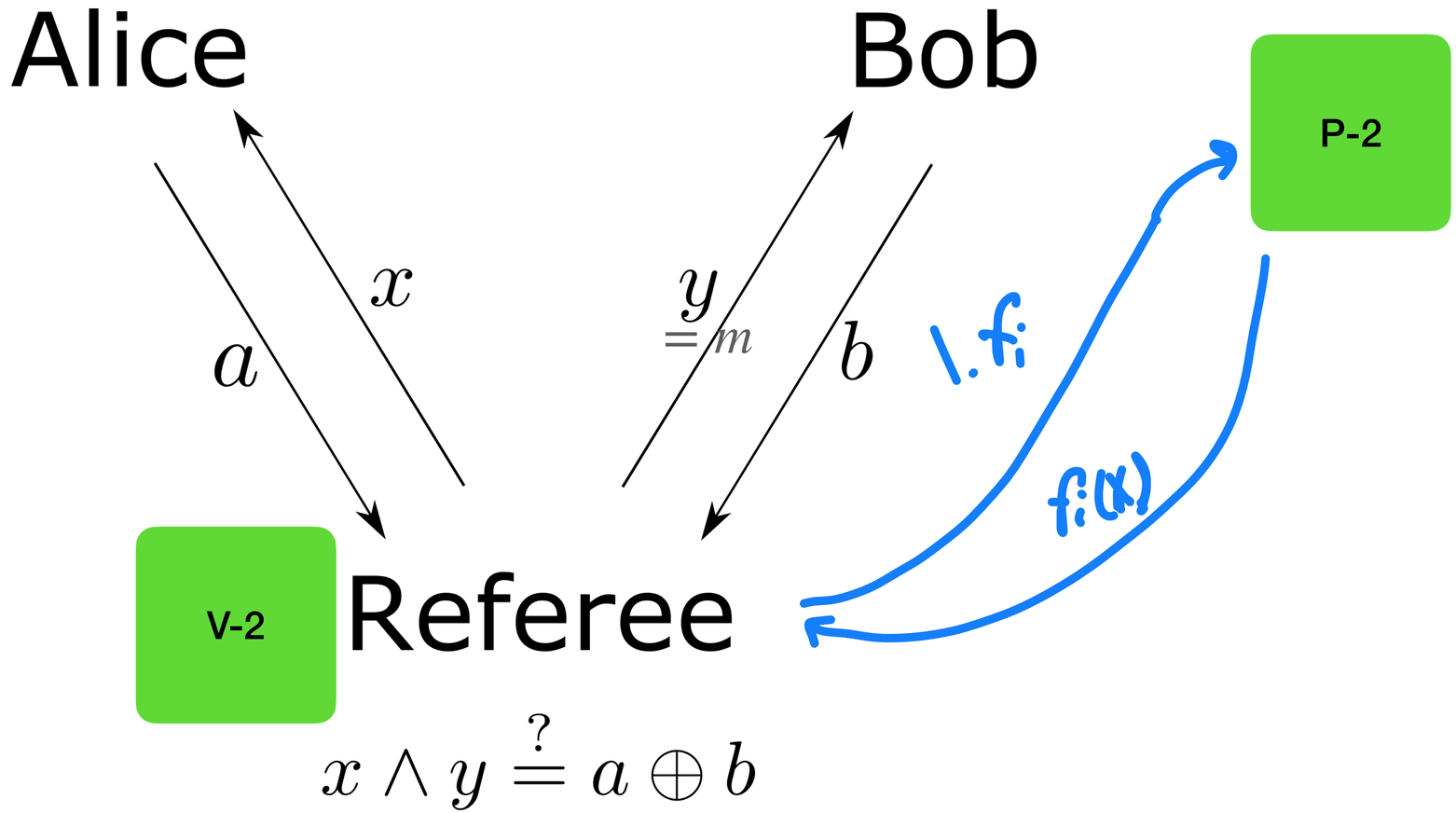
12

Reducing G-2222 to iPoQ-2

Completing security proof for iPoQ-2

Referee R will construct Alice and Bob to play G-2222 nonlocally

1. TLF Prep

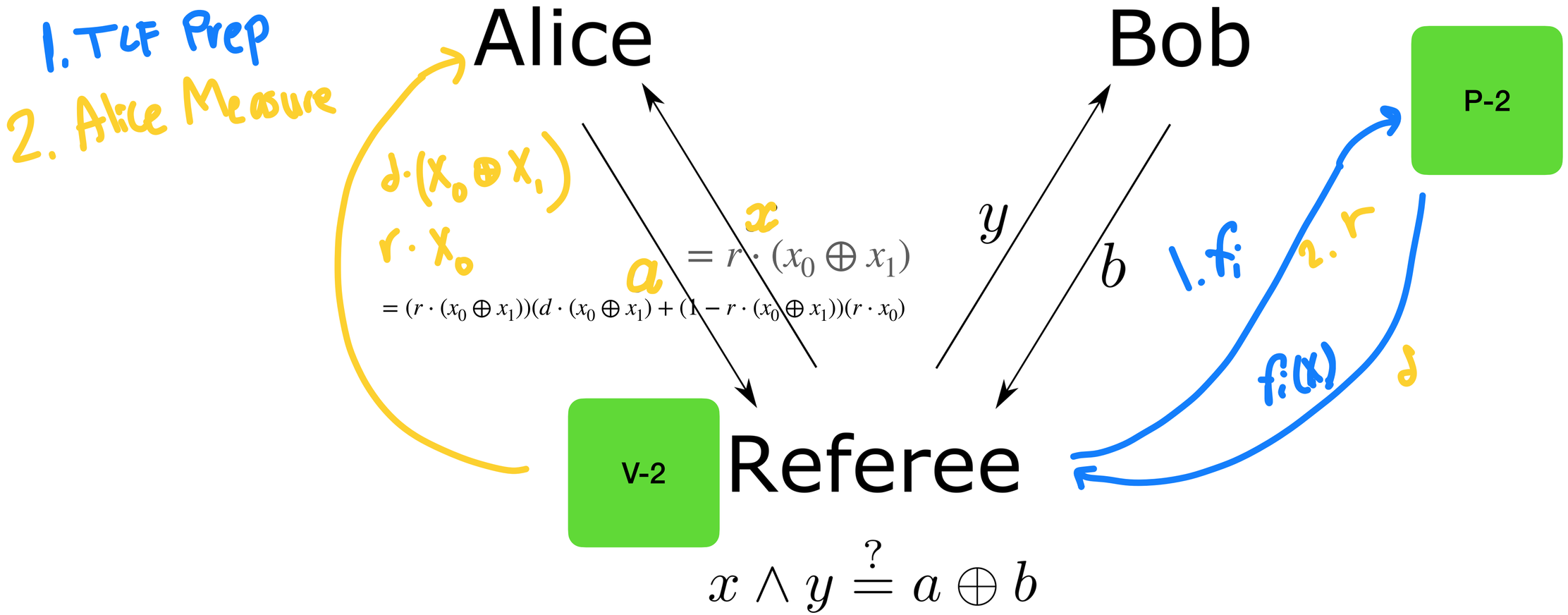


13

Reducing G-2222 to iPoQ-2

Completing security proof for iPoQ-2

Referee R will construct Alice and Bob to play G-2222 nonlocally

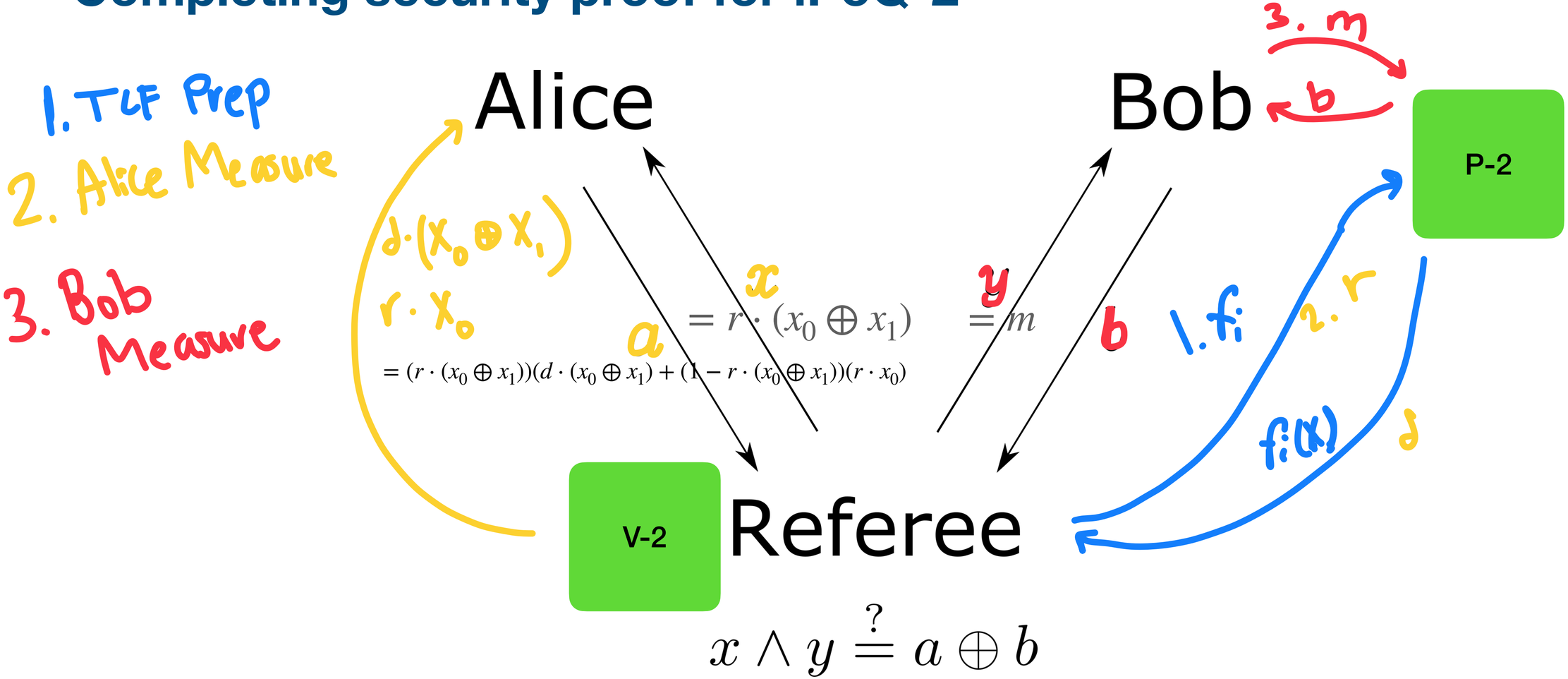


14

Reducing G-2222 to iPoQ-2

Completing security proof for iPoQ-2

Referee R will construct Alice and Bob to play G-2222 nonlocally

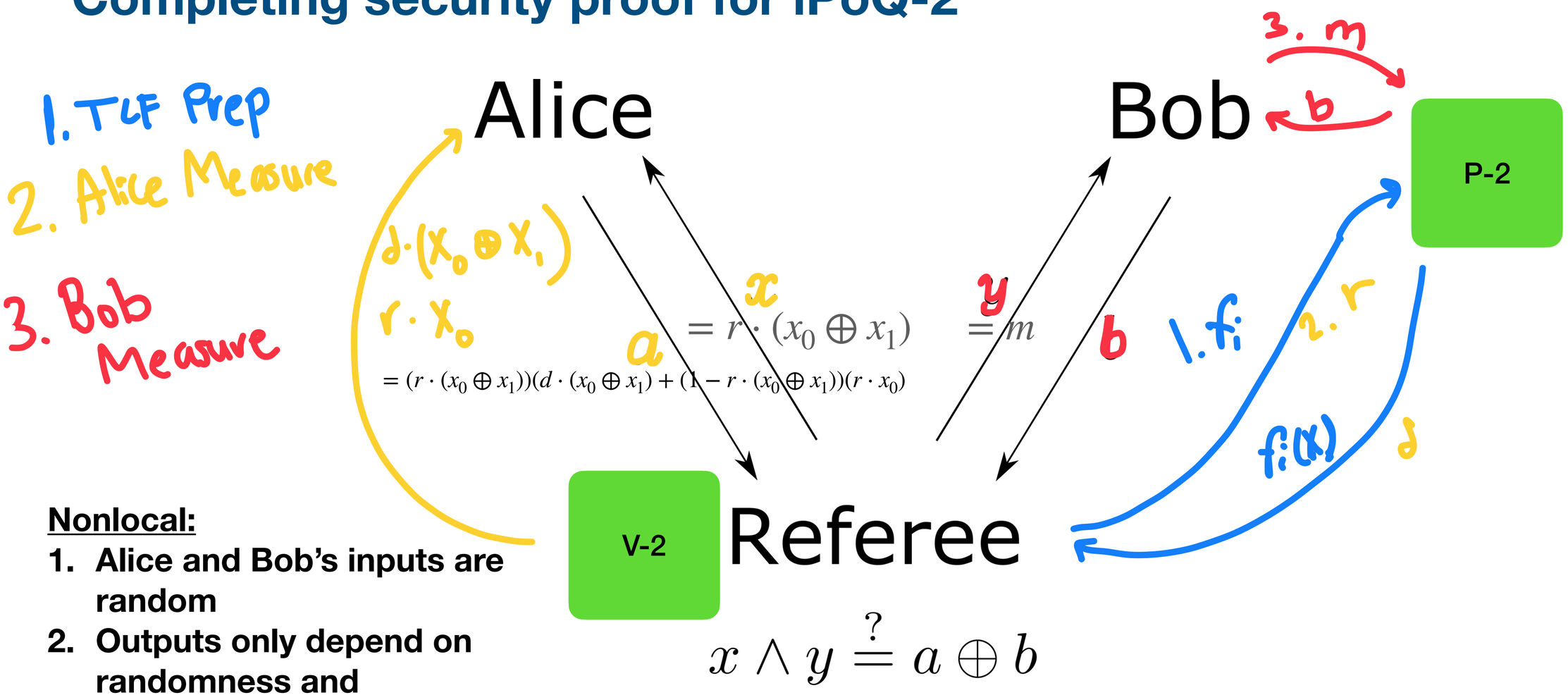


15

Reducing G-2222 to iPoQ-2

Completing security proof for iPoQ-2

Referee R will construct Alice and Bob to play G-2222 nonlocally



Nonlocal:

1. **Alice and Bob's inputs are random**
2. **Outputs only depend on randomness and computational secret**

16

Reducing G-2222 to iPoQ-2

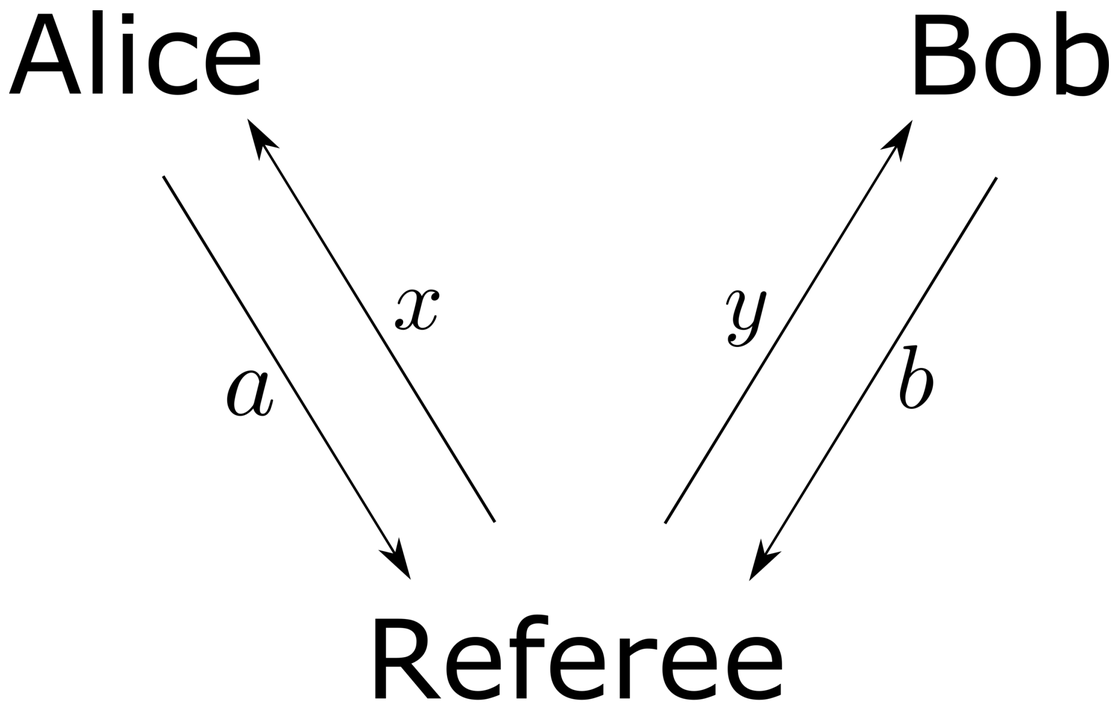
Extra whiteboard space

17

What about larger inputs?

18

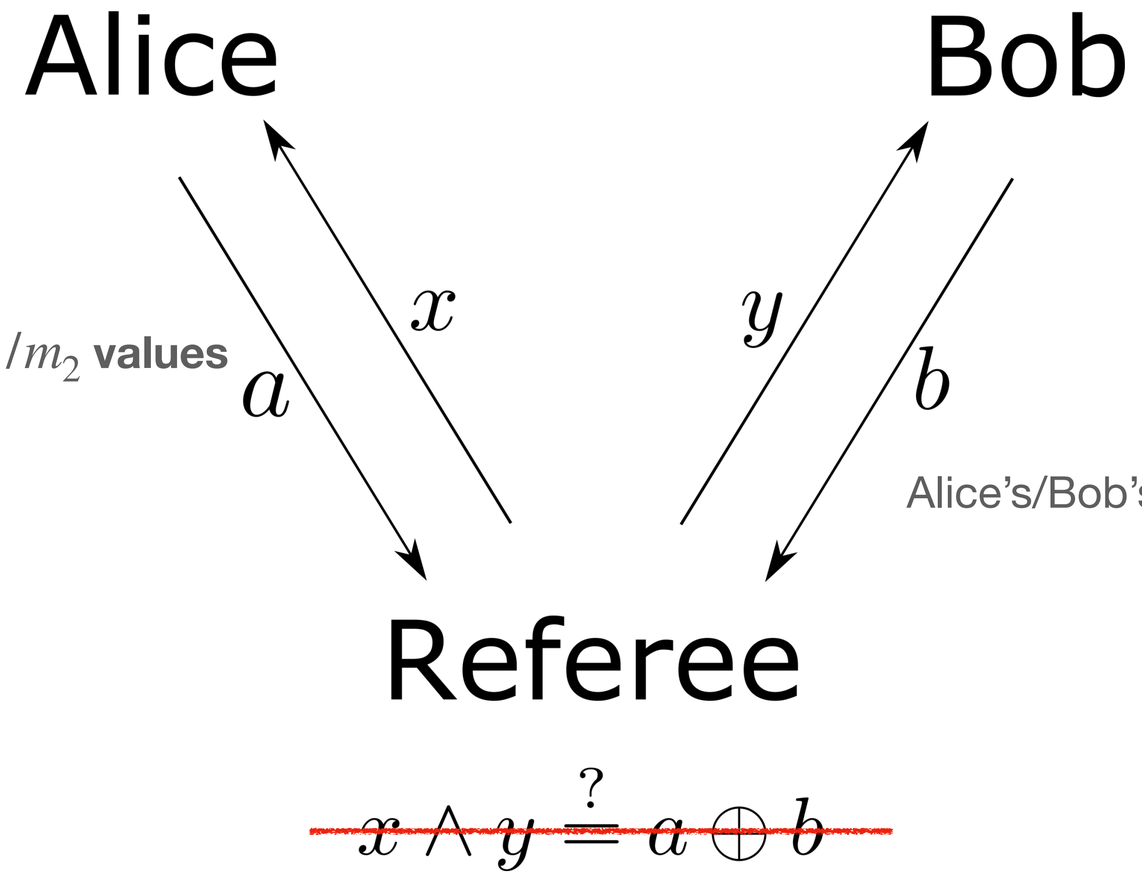
The CHSH Game (G_{2222})



$$x \wedge y \stackrel{?}{=} a \oplus b$$

19

The Generalized CHSH Game ($G_{m_1 m_2 n_1 n_2}$)



Alice's/Bob's input x/y is **1 of** m_1/m_2 **values**
(instead of 2)

Alice's/Bob's output a/b is **1 of** n_1/n_2 **values**
(instead of 2)

20

Generalized Inequalities

Wehner 2006. | PRA

- With 1 of n possible values, each player can choose 1 of n measurements

- General Sum $|S| = |\sum_{i=1}^{n} < X_i Y_i > + \sum_{i=1}^{n-1} < X_{i+1} Y_i > - < X_1 Y_n > |$

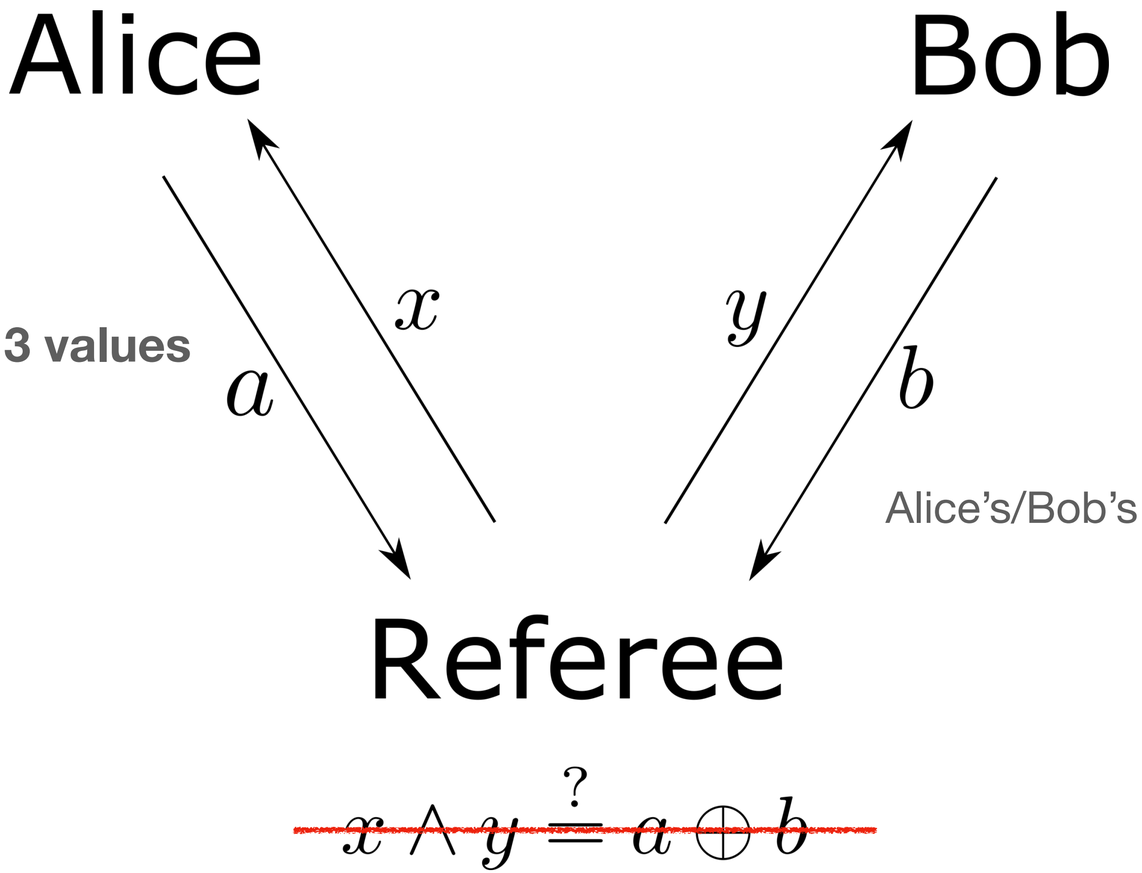
$$S_c \leq 2n - 2$$
$$S_q \leq 2n \cos(\frac{\pi}{2n})$$

21

G-3322

22

The 3-Input CHSH Game (G_{3322})



Alice's/Bob's input x/y is **1 of 3 values** (instead of 2)

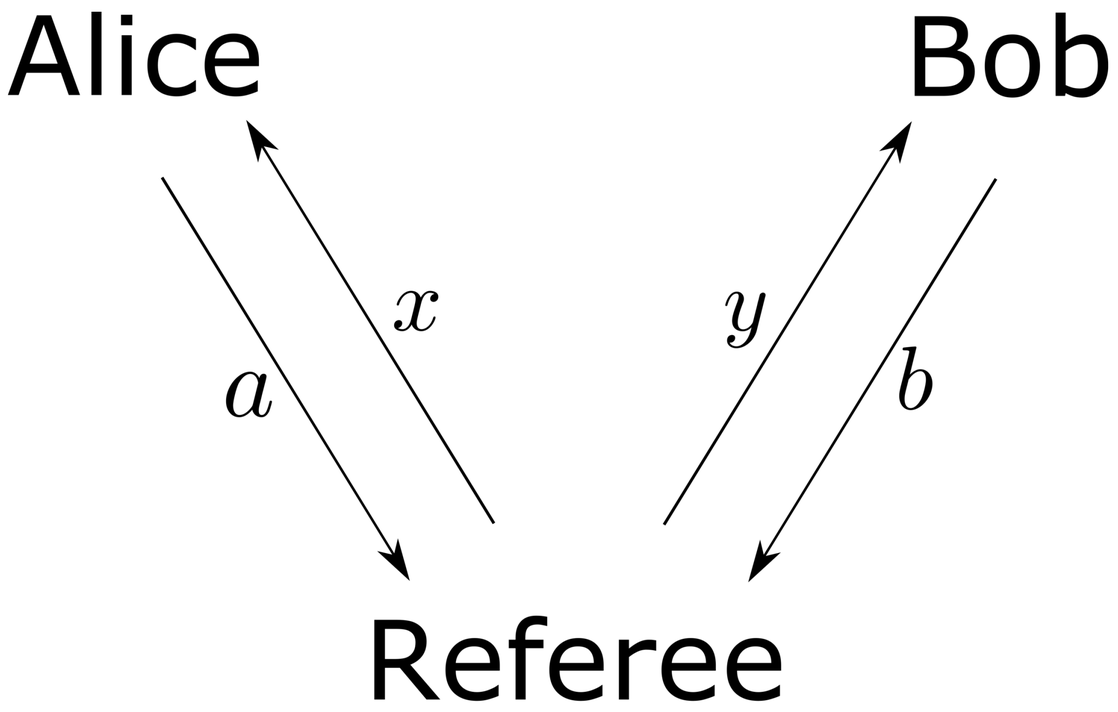
Alice's/Bob's output a/b is still **1 of 2 values**

23

The 3-Input CHSH Game (G_{3322})

Game Value

- Classical = .78
- Quantum = .93



$$x + y = 3 \leftrightarrow a \oplus b = 1$$

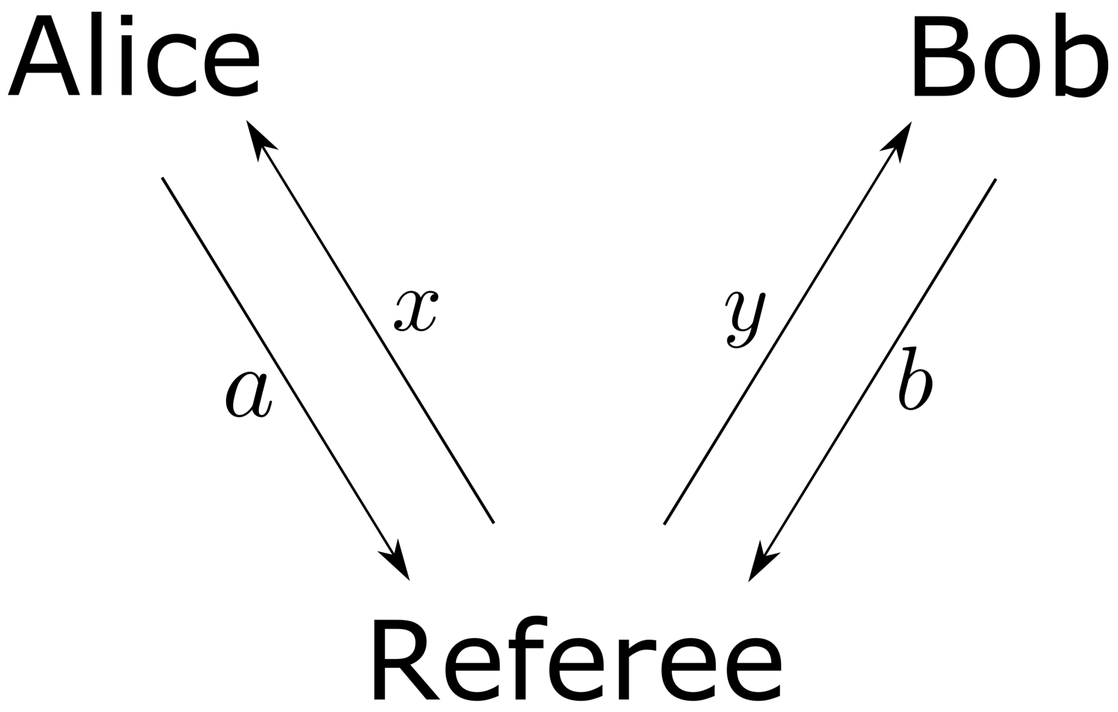
24

The Generalized CHSH Game (G_{3322})

Game Value**

- Classical $= .78 = \frac{1}{2}(1 + \frac{5}{9})$
- Quantum $= .93 = \frac{1}{2}(1 + \frac{9\cos(\pi/6)}{9})$

***Assuming all inputs are uniformly distributed and control over distribution of a and b*



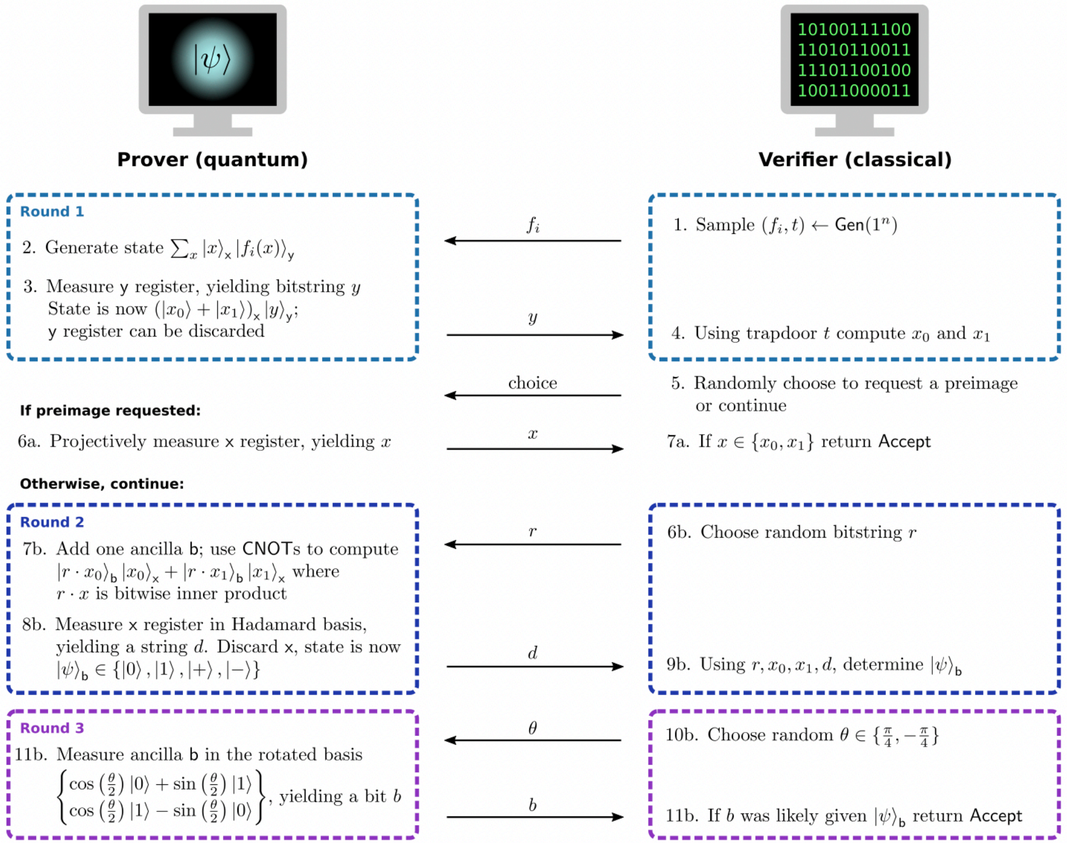
$$x + y = 3 \leftrightarrow a \oplus b = 1$$

25

CHSH-based iPoQ (iPoQ-3)

Using 3-to-1 TCFs

- **Possible States:** $\{0, \pm \frac{\pi}{7}\}$
  - *Not ideal (cannot reach .93)*
- **Best Measurements:** $\{0, \pm .16\pi\}$
  - *Computed using SDP*
- **Completeness: .84**
- **Soundness: .56**



26

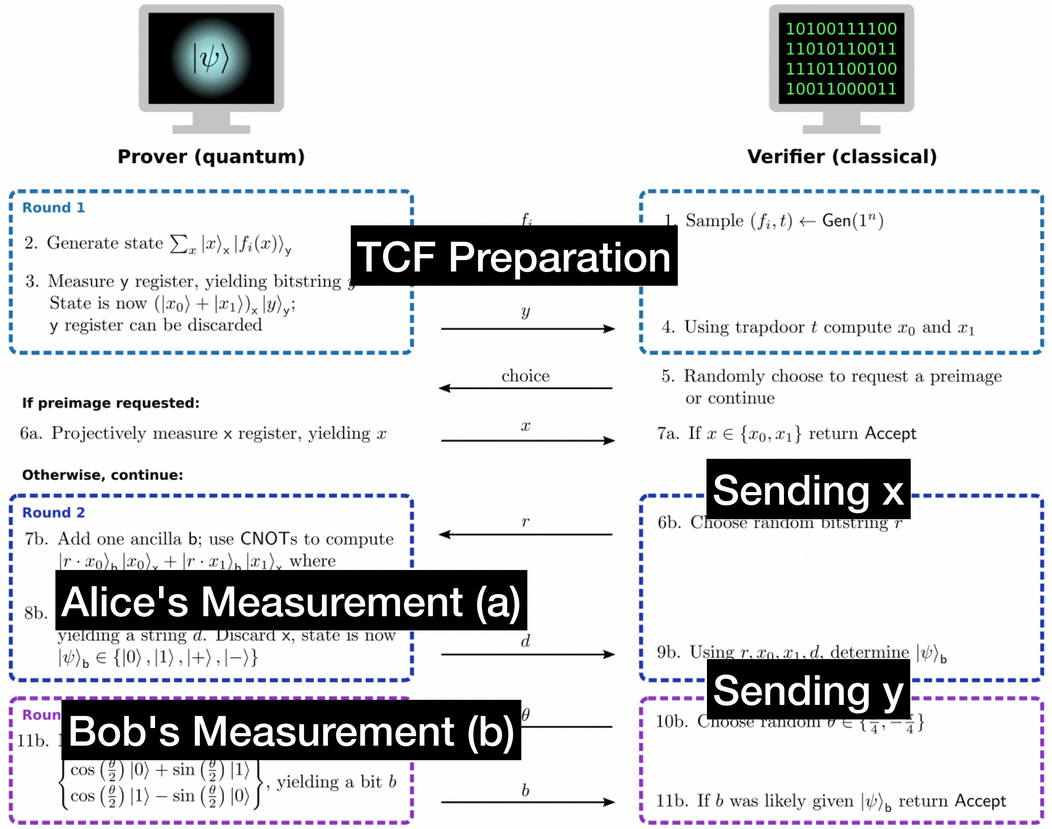
Reducing G-3322 to iPoQ-3

Security proof for iPoQ-3

- Winning Classical Adversary
  ↳ G-3322 Adversary

- Let (P-3,V-3) encapsulate an iPoQ-3 protocol

- Using the same structure of first reduction, proof follows WLOG
  - G-3322 states match candidate states from TCF
  - P-3 measurements match Bob's



27