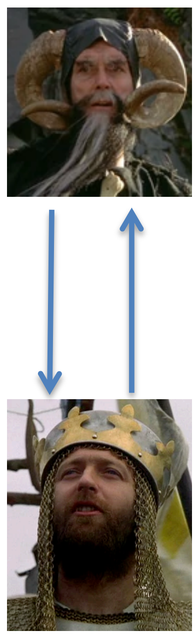
NEEXP $\subseteq$ MIP*

Anand Natarajan[1] and John Wright[2]
[1]Caltech, [2]MIT

Interactive proofs

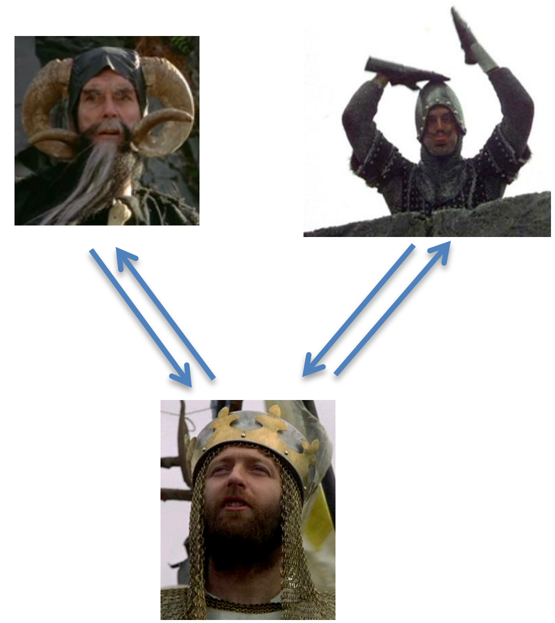
IP



= PSPACE

[Shamir '90]

MIP



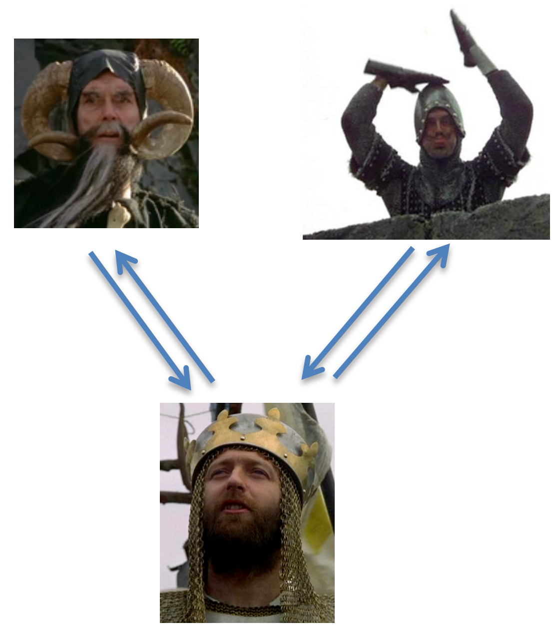
= NEXP

[BFL '91]

MIP

- Separately interrogate non-communicating provers
- Upper bound: NEXP
  - Witness is strategy
- Lower bound: NEXP [BFL'91]
  - Inspired probabilistically checkable proofs (PCPs)

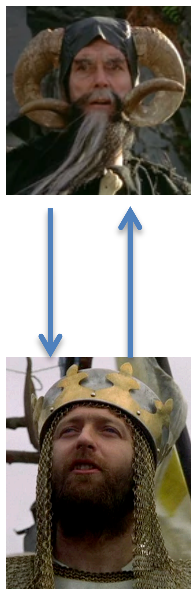
MIP



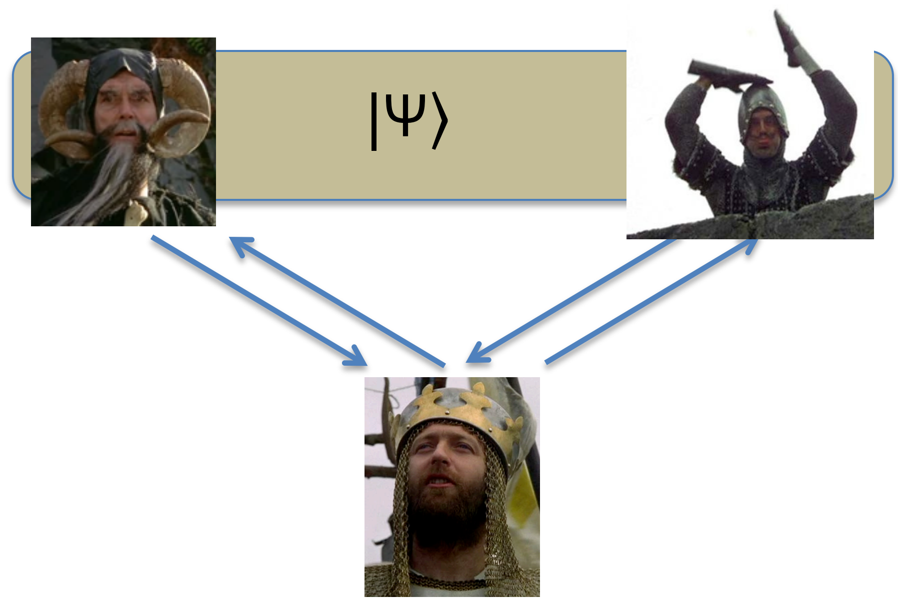
= NEXP
[BFL '91]

Quantum interactive proofs

QIP



MIP*



Still = PSPACE !

[JJUW'09]

- |Ψ⟩ is finite-dim but arbitrarily big
- Contained in RE (search over all |Ψ⟩)

Why MIP*?

- A computational lens on a physical question: what types of correlations can we get from local measurements on a bipartite system?
  - Can we distinguish different notions of locality (tensor product vs commuting)?
- Applications:
  - Delegated computation, certifiable randomness, hardness of approximation?

Entanglement can be used to cheat

- MIP* could be **weaker than MIP:**
  ⊕MIP = NEXP [Hastad'97]
  ⊕MIP* ⊆EXP [CHTW'04]
- But it isn't!
  - NEXP ⊆ MIP [IV'12]
  - Honest provers need no entanglement, and entanglement doesn't help dishonest provers cheat

Can entanglement help? Self-testing

- Entangled provers can prove they possess a particular quantum state: a uniquely quantum power!
- [Bell'64, CHSH'69]: a simple game where optimal quantum players need 1EPR pair
  - [Cir'80, SW'88]: near-optimal players
- Modern tests can certify many qubits
  - [NV'18]: n EPR pairs with log(n) communication

Can entanglement help? Some hints

- Idea: self-test a quantum state that's computationally difficult to produce
- [NV'18]: QMA in MIP* with log-sized messages
- [Ji'17, FJVY'19]: NEEXP and higher in MIP* with shrinking completeness-soundness gap
- All these results use history states
  - Need more than two provers
  - Technically challenging to get constant soundness

Our result

Thm: There is a two-prover, one-round MIP* protocol for NEEXP = NTIME[exp(exp(poly(n)))], with completeness 1 and soundness 1- Ω(1)

- NEXP ≠ NEEXP (unconditionally), so MIP ≠ MIP*
- No history states: honest provers only need EPR pairs

Proof outline

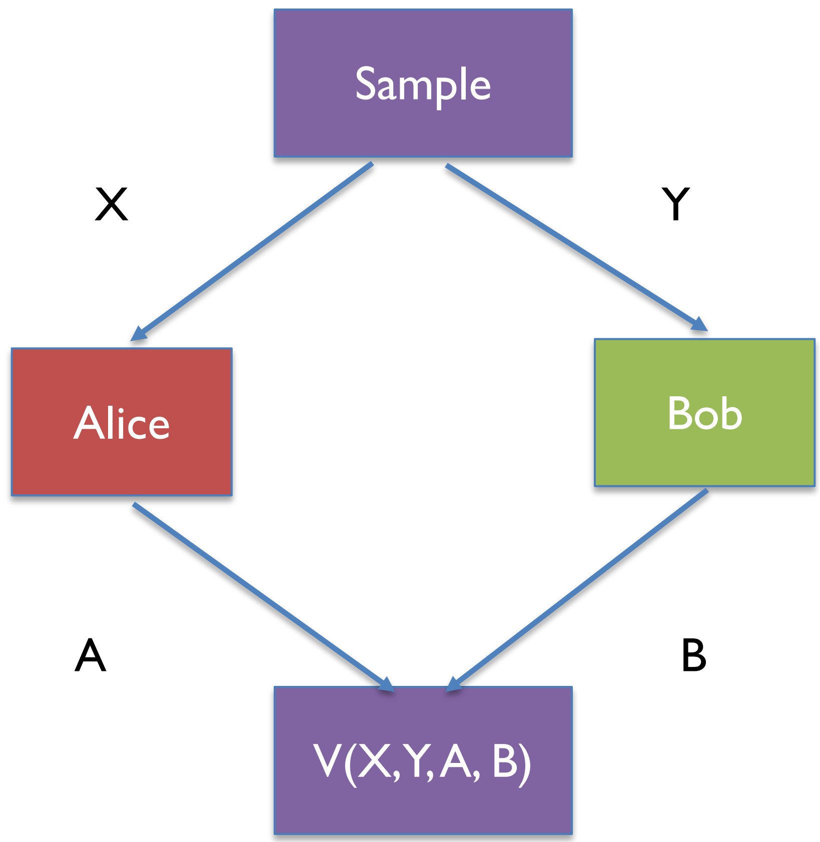
- Start with a classical protocol with an exponential verifier
  - Scale up NEXP $\subseteq$ MIP
- Question reduction
- Answer reduction

NEEXP

- NP = NTIME[poly(n)]. Complete problem is 3Sat
- NEXP = NTIME[exp(poly(n))]. Complete problem is Succinct-3Sat
  - Instance is a circuit C that generates exponentially large 3Sat formula
- NEEXP = NTIME[exp(exp(poly(n)))]. Complete problem is Succinct-Succinct-3Sat
  - Instance is a circuit C that generates a circuit C' that generates a doubly exponentially large 3Sat formula

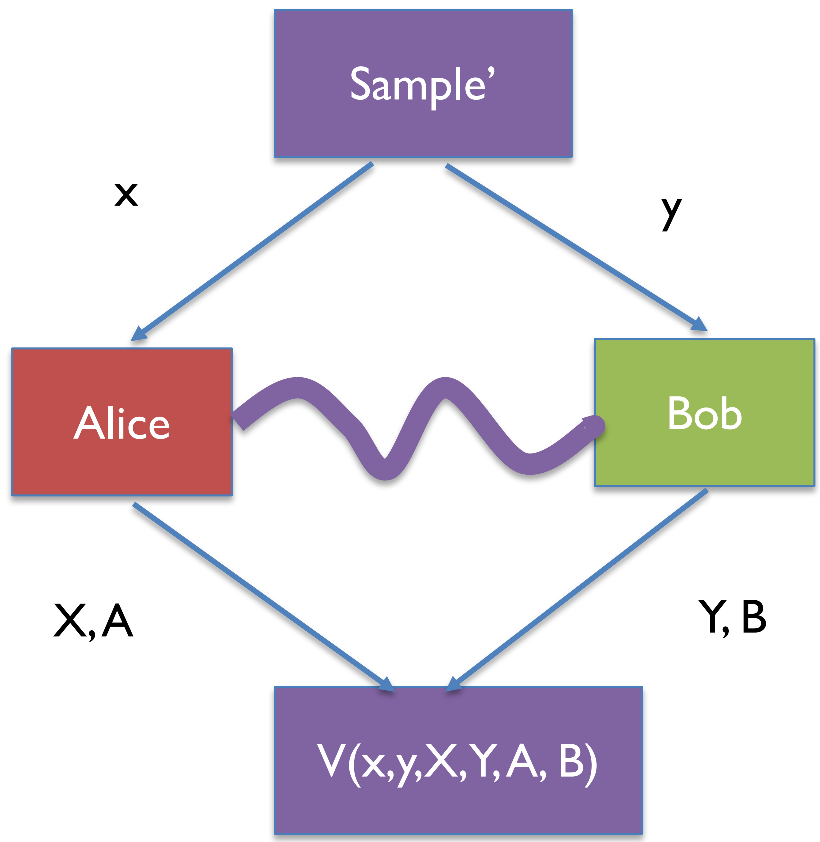
Starting point: a classical protocol

- NEEXP ⊆ MIP[exp(n), exp(n)]
  - Scaled-up MIP in NEXP
- Verifier needs exp(n) time to sample questions, and exp(n) time to check answers
  - Need to delegate these steps to provers!



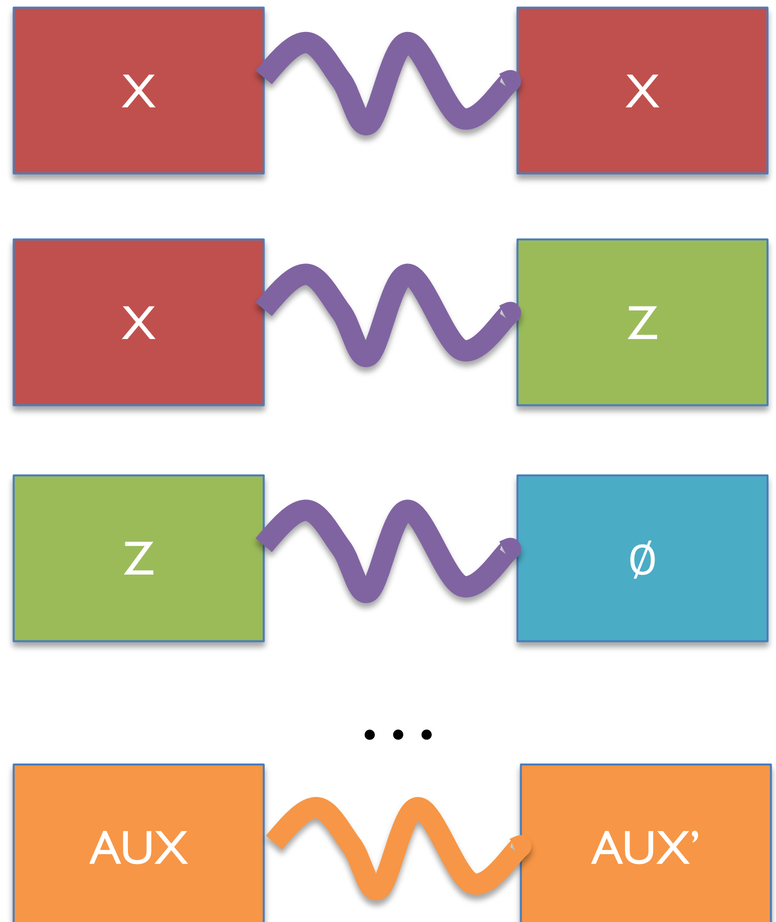
Question reduction

- NEEXP ⊆ MIP*[poly(n), exp(n)]
- **Introspection:** Ask Alice and Bob to generate X, Y by measuring shared state



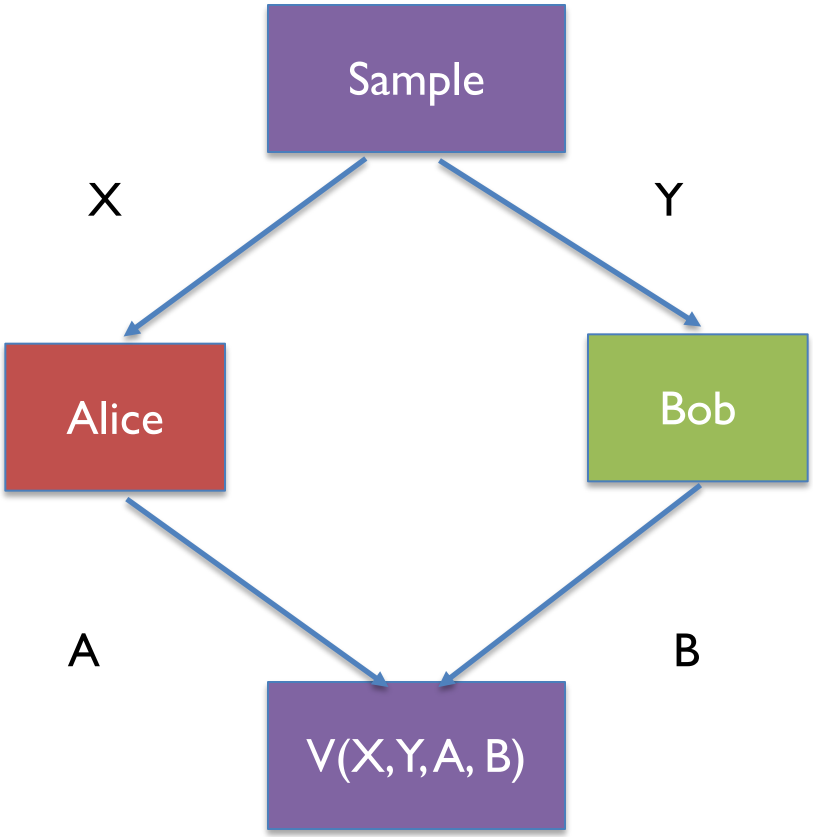
Interlude: testing Pauli measurements

- Using NV'18 self-test, can command provers to use **register strategy:**
  - O(1) registers of exp(n) EPR pairs each, with Pauli basis measurements



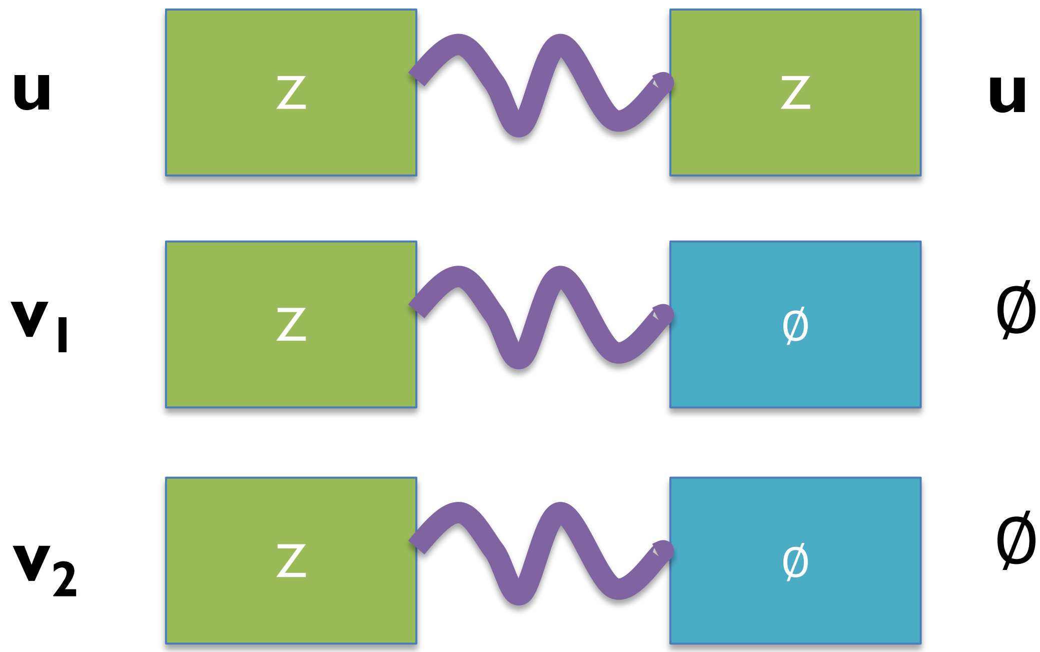
The point-plane distribution

- Pick X a random affine plane in $\mathbf{F}_q^m$
  $\{u + a\, v_1 + b\, v_2 : a, b \text{ in } \mathbf{F}_q\}$
  - Intercept u, slopes v_1, v_2
- Pick Y a random point on X



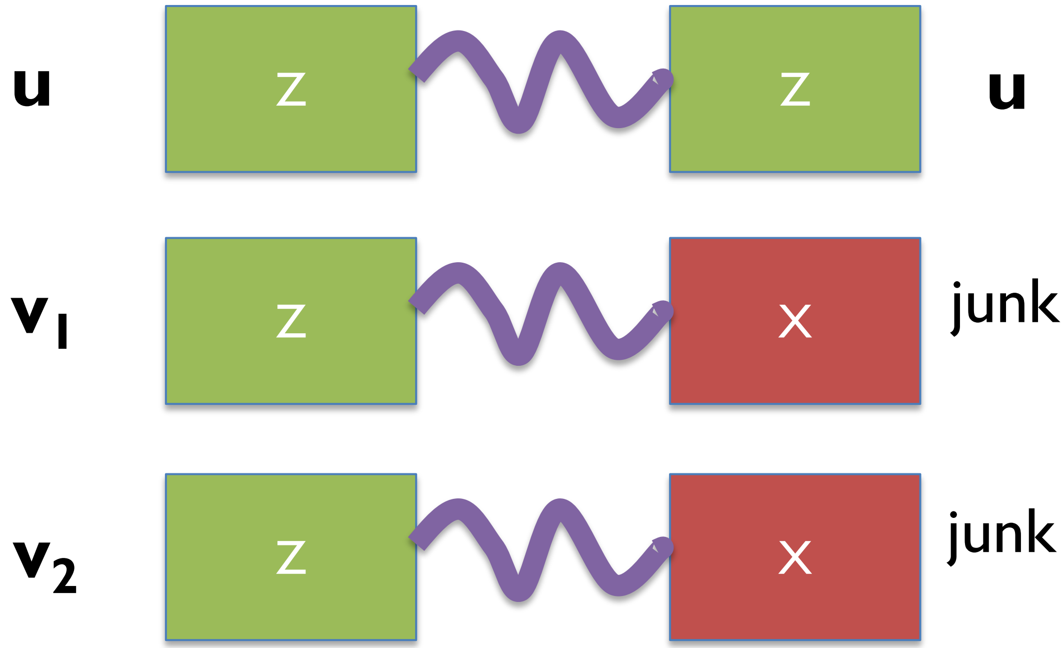
Sampling from EPR pairs: attempt 1

- Alice sets $X = \text{plane}(u, v_1, v_2)$
- Bob sets $Y = u$
- Not sound!
  - Alice learns Y
  - Bob can learn X



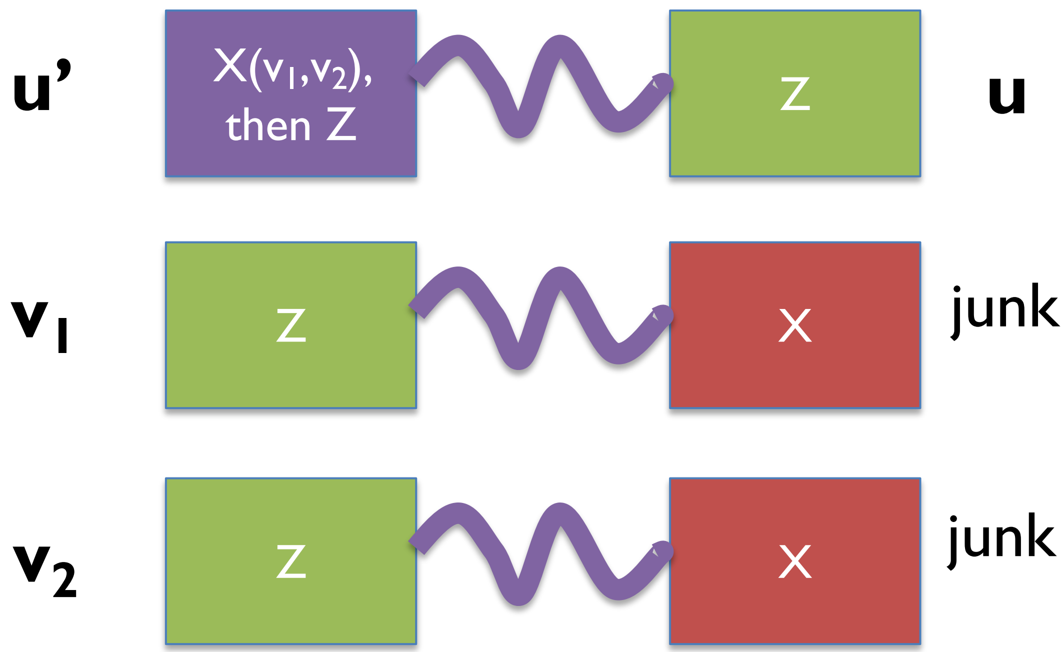
Data hiding

- Heisenberg: measuring momentum erases position!
- Hide v_1, v_2 from Bob by measuring in X basis
- What about u?



Partial data hiding

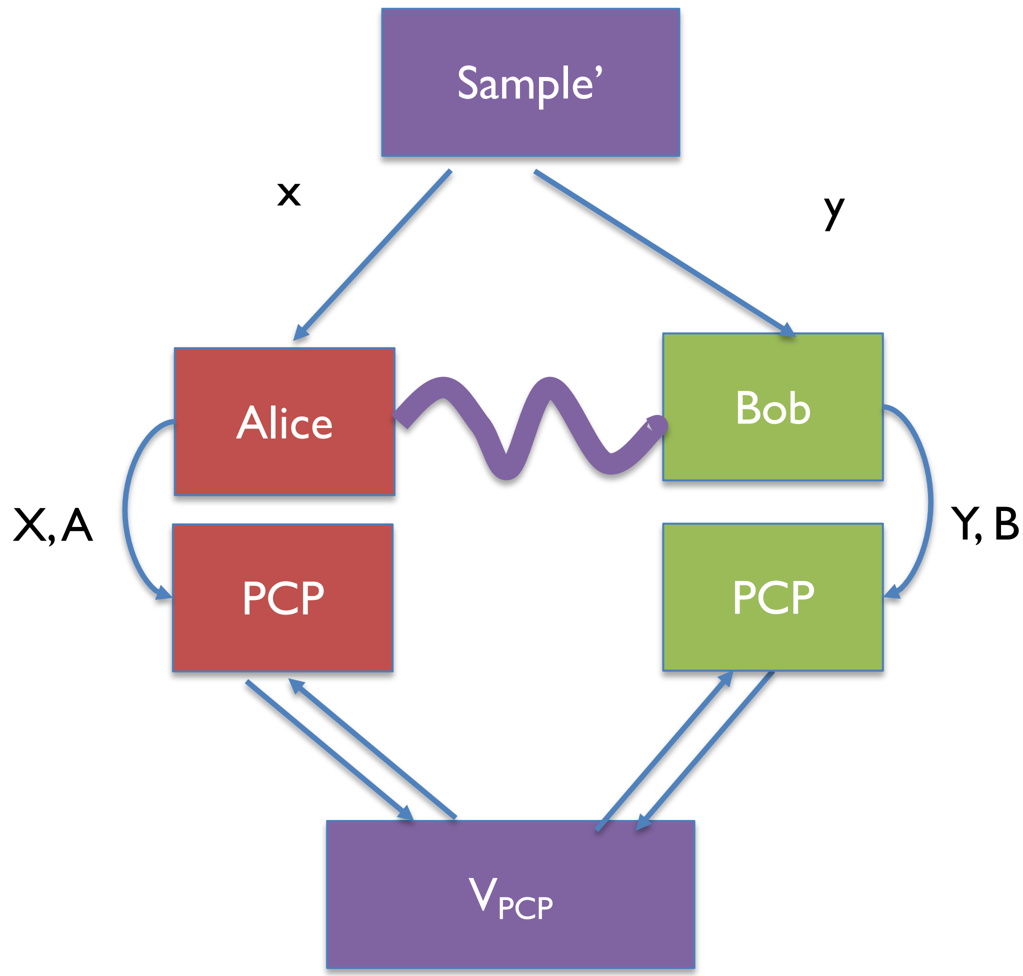
- Alice should learn plane (u, v_1, v_2), but not location of u on plane
- "Scramble" u by **partially** measuring in X basis



$$|u\rangle \xrightarrow{\text{measure } X(v_1)} \frac{1}{\sqrt{q}} \sum_{\lambda \in \mathbb{F}_q} \omega^{\alpha \cdot \lambda} |u + \lambda v_1\rangle$$

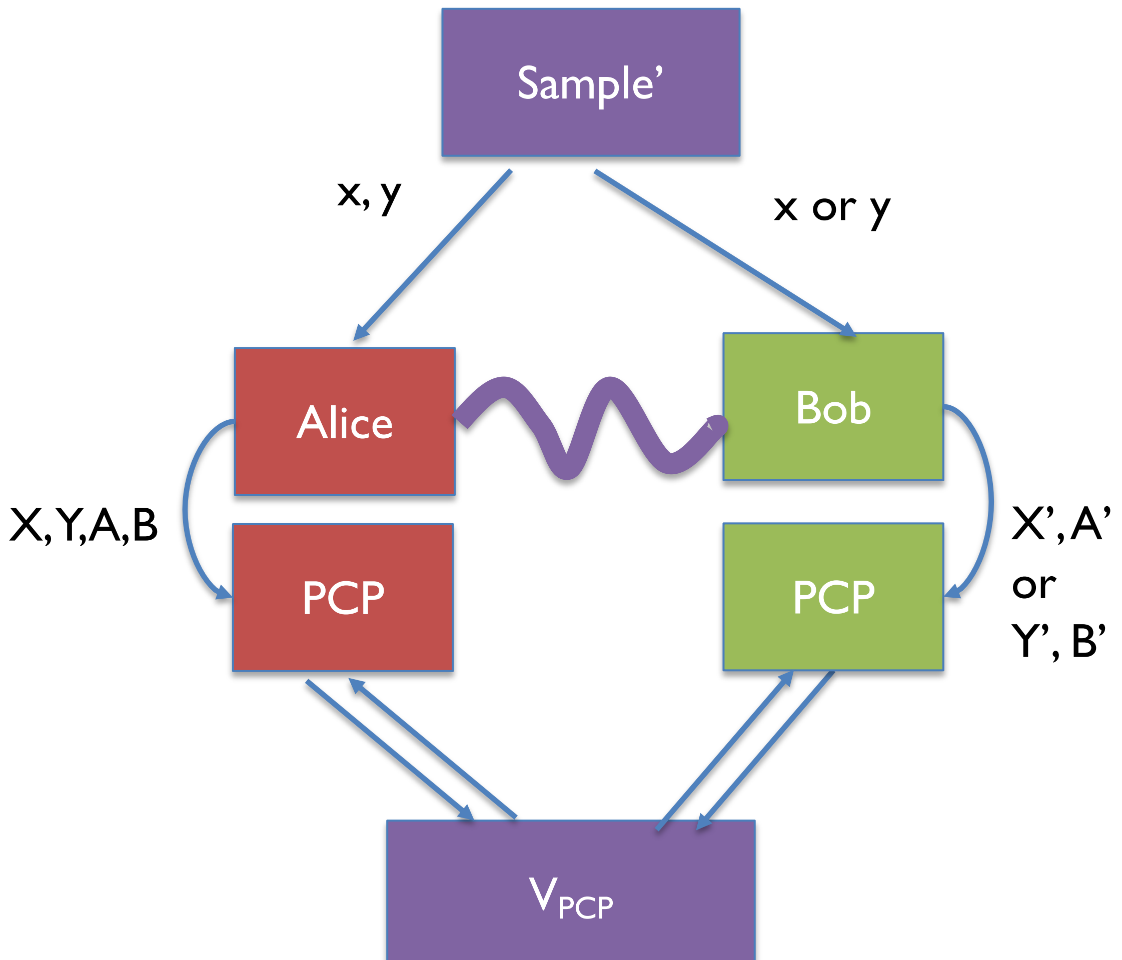
Answer reduction: PCPs

- NEEXP ⊆ MIP*[poly(n), poly(n)]
- Delegate checking exp(n)-long answers A, B to provers using PCP
  - "PCP composition"



Answer reduction: oracularization

- To use a PCP, one player must know X, Y, A, B
- Oracularization of MIP*
  - Always preserves soundness
  - Preserves completeness for EPR strategies



Future directions

- Better lower bounds?
  - NEEXP ⊆ ??? ⊆ MIP* ⊆ RE
- By iterating our protocol, can we get NEEEXP, NEEEEXP, …?
- [FJVY'19]: if a compression theorem for all MIP* exists, then MIP* contains undecidable promise problems
  - Would separate tensor-product and commuting-operator entanglement, solving Tsirelson's problem, Connes' embedding conjecture

THANKS!