Cryptography from NP-Hardness: can quantum computing help?

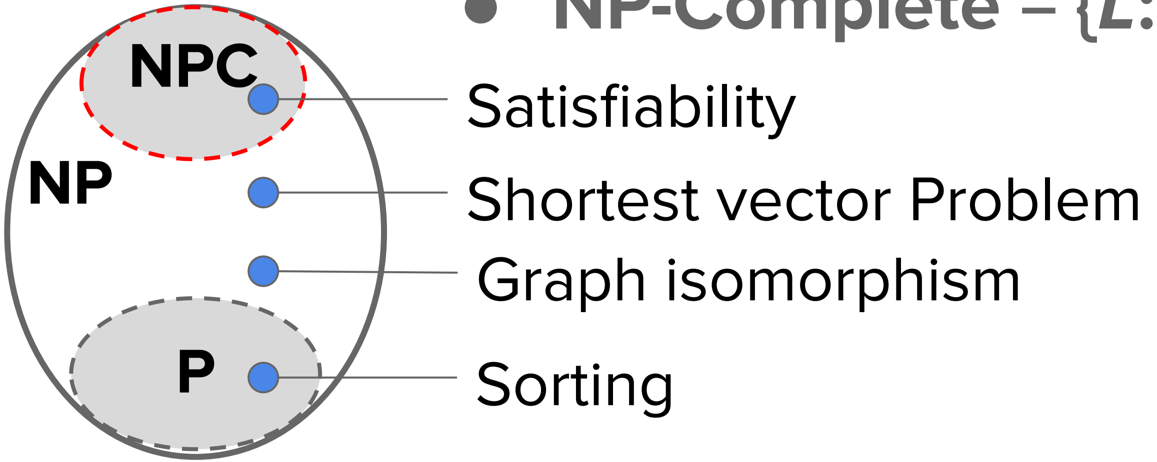
Fang Song
CSE @ TAMU

Joint work with
Nai-Hui Chia, UT Austin
Sean Hallgren, Penn State

arXiv:1804.10309

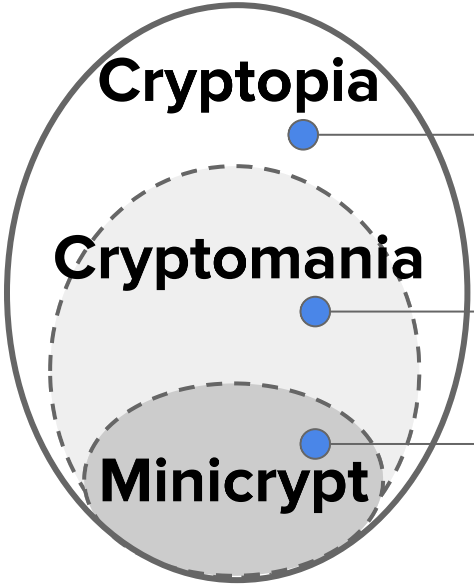
P = NP ?

- P = {L: poly-time computable}
- NP = {L: poly-time verifiable}
- NP-Complete = {L: "hardest" in NP}



(Unfortunate) reality: unlikely to solve NPC in P

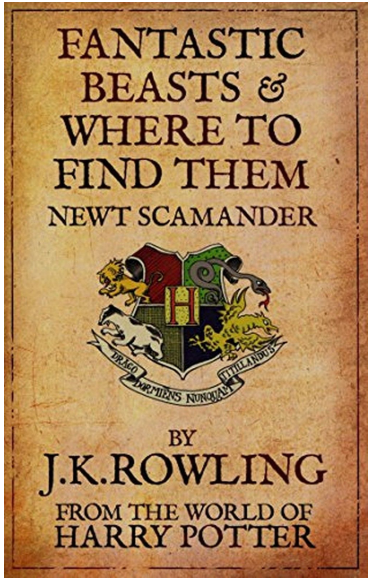
Cryptography: where to find?



Program obfuscation …

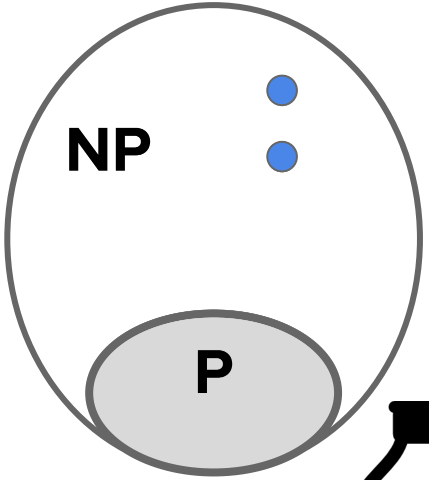
Public-key encryption …

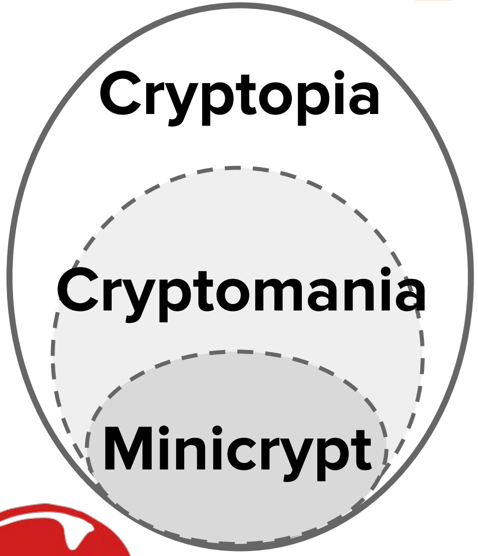
Symmetric-key encryption,
digital signature, …



(Unfortunate) reality: don't exist unconditionally

If P ≠ NP $\overset{?}{\Longrightarrow}$ Then Crypto





Basing crypto on NP-hardness

If P ≠ NP $\overset{?}{\Longrightarrow}$ **Then Crypto**

☹ **seems unlikely** [Bra79,FF93,BT06,AGGM06,BB15...]

... in the classical computing regime so far

Our work: quantum computing might not help

This Talk

1. Negative evidence in the classical world

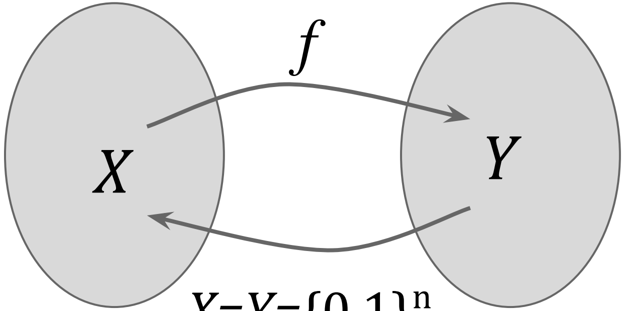
2. Our work: neg. evidence in the quantum world

Making the goal concrete

BPP={*L*: computable in probabilistic poly-time}

SAT $\notin$ **BPP** $\overset{?}{\Rightarrow}$ **OWF**  $\Leftrightarrow$ **Minicrypt**

One-Way Function



$X=Y=\{0,1\}^n$

- Easy to compute (poly-time)
- Hard to **invert** **on average**
  - Given: $y = f(x)$, $x \leftarrow X$ random
  - Find: x' s.t. $f(x')=y$.

Making sense of the goal

$\mathrm{SAT} \notin \mathrm{BPP} \; ?\!\!\Rightarrow \mathrm{OWF}$

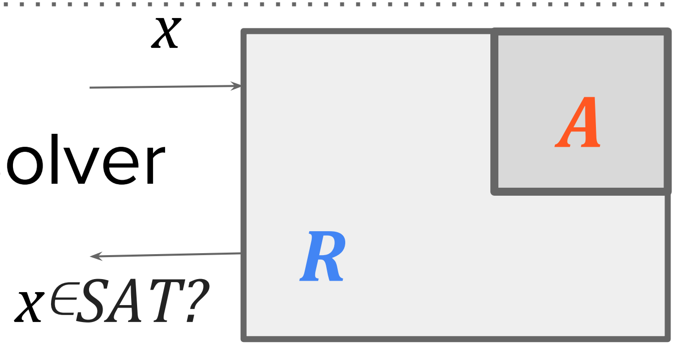
1. Construct a function f 2. Prove security of f

Inverting f is **as hard as** solving SAT

on average ⟵ worst-case

- **Given** A: inverter of f
- **Concoct** R: efficient SAT solver

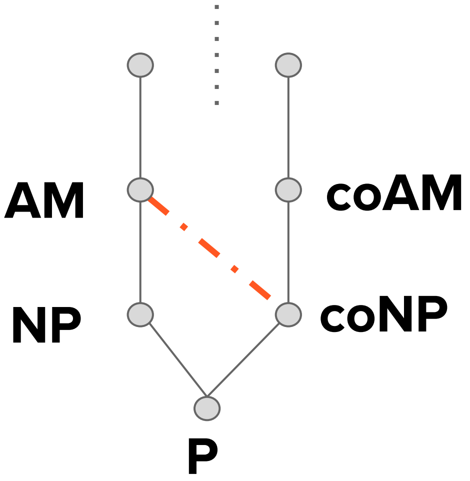
Reduction: $\mathrm{SAT} \leqslant \mathrm{OWF}$



Collapse of the wish

- If $\mathbf{SAT} \leqslant \mathbf{OWPermutation}$, then $\mathbf{coNP} \subseteq \mathbf{AM}$. [Bra79]
- If $\mathbf{SAT} \leqslant \mathbf{OWF}$, then $\mathbf{coNP} \subseteq \mathbf{AM}$.
  - Non-adaptive reductions R [AGGM05]
  - f preimage verifiable [BB15]

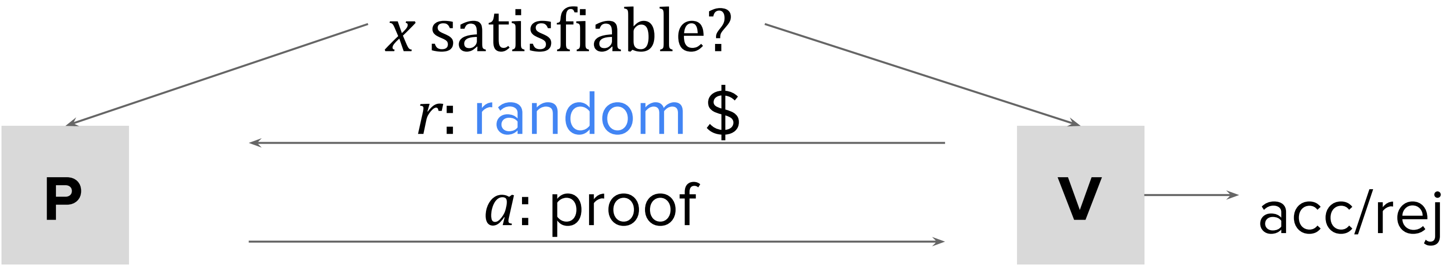
➔ PH collapses to 2nd level: widely believed unlikely



PH: polynomial hierarchy

Arthur-Merlin interactive proofs

- L∈**AM**, if ∃ <P,V>
  - (**Completeness**) if $x \in L$, V acc w.p. >⅔.
  - (**Soundness**) if $x \notin L$, ∀ (dishonest) **P***, V acc w.p < ⅓.



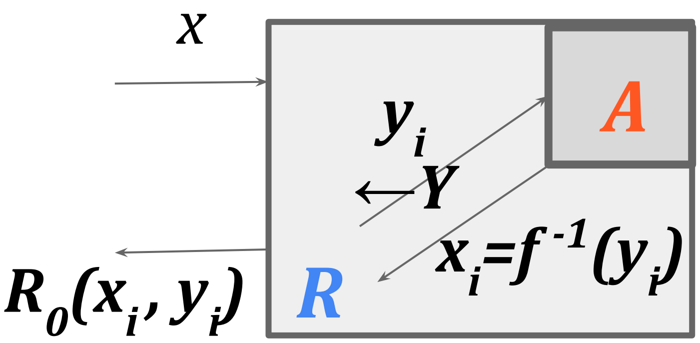
Prover: unbounded **Verifier: (randomized) poly-time**

- **NP⊆AM: prover ignores r and sends a witness**

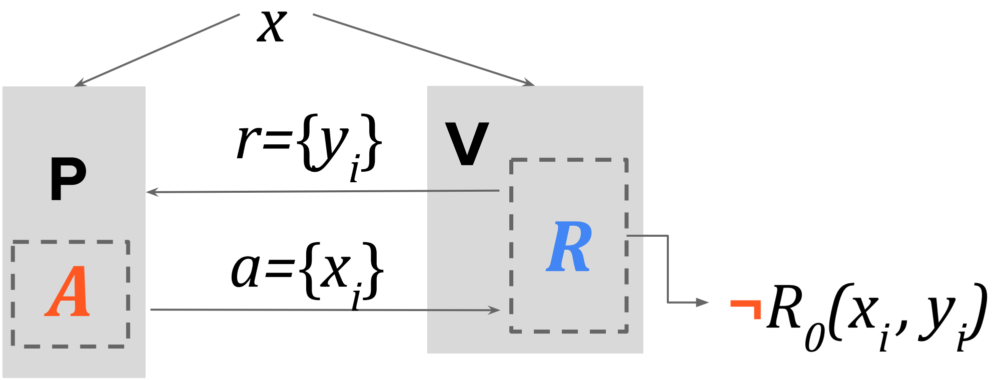
How come the negative evidence?

Theorem[Bra79] If $\mathbf{SAT} \leqslant \mathbf{OWP}$, then $\mathbf{coNP} \subseteq \mathbf{AM}$.

- Idea: prover can act as an inverter



AM protocol for co-SAT



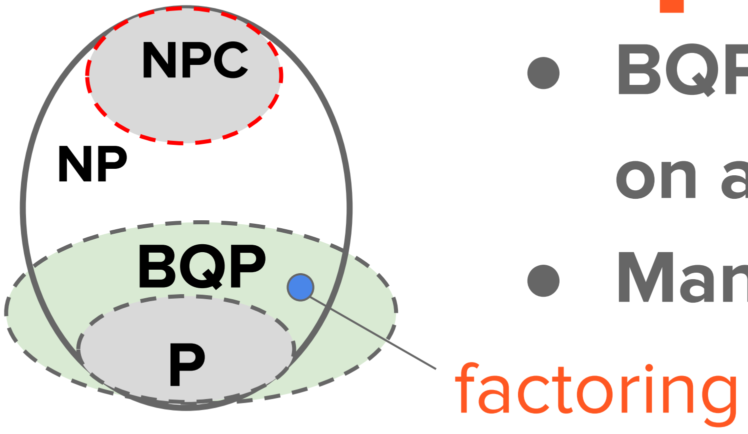
Enforce honest P: V checks $f(x_i)=y_i$

This Talk

1. Negative evidence in the classical world

2. Our work: neg. evidence in the quantum world

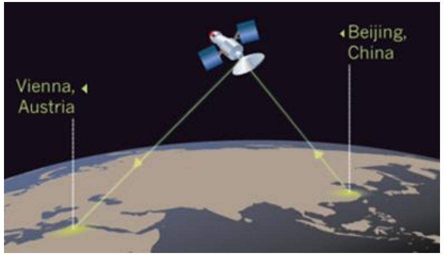
What quantum brings us



- BQP = {L: poly-time computable on a quantum computer}
- Many cryptosystems at risk …

😁 Quantum cryptography can be helpful

- Quantum Key Distribution (strong security)

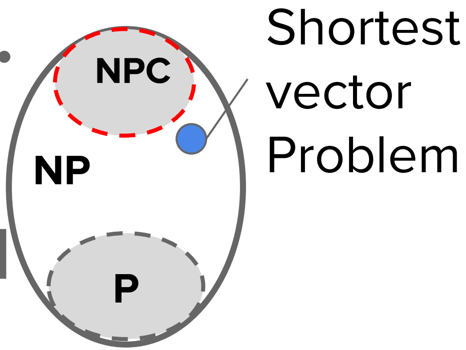


A highly hopeful message

😁😁 Quantum reduction from worst-case lattice problems to crypto [Regev05]

★ Enables cryptopia: FHE, FuncEnc, ...
★ Promising post-quantum candidate

- Later de-quantized, but not as good
  - Larger keys if via classical reduction

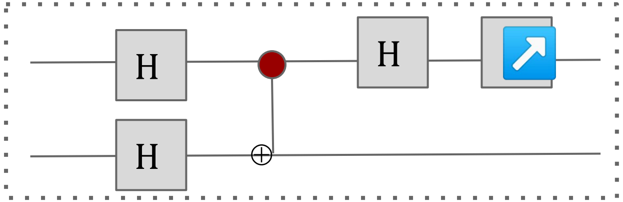


☹️ This lattice problem is unlikely NP-Complete

Revisiting our goal via a quantum lens

$\text{SAT} \notin \text{BPP} \overset{?}{\Longrightarrow} \text{OWF}$ $\text{SAT} \notin \text{BQP} \overset{?}{\Longrightarrow} \text{OWF}$

1. Construct a function f *by quantum algorithms*
    - Applications exist [DMS00]
    - Expensive for honest users



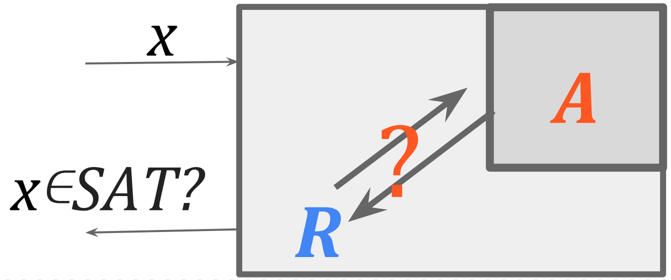
2. Prove security of f *by quantum algorithms*

OUR WORK

Quantum reductions

? Inverting f is as hard as quantumly solving SAT

- A: inverter of f (classical or quantum)
- R: **quantum** SAT solver



- **Options for the quantum reduction algorithm**
  - Quantum superposition queries vs. classical queries
  - Adaptive vs. Non-adaptive

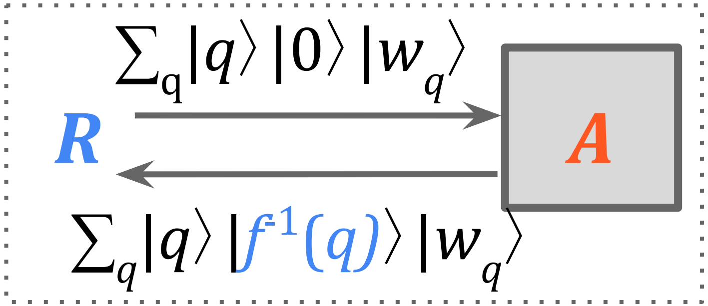
NB. Stronger Reductions ⇒ Stronger impossibility

We (kinda) rule out natural QRed's

Upon formally defining various Q Reductions ...

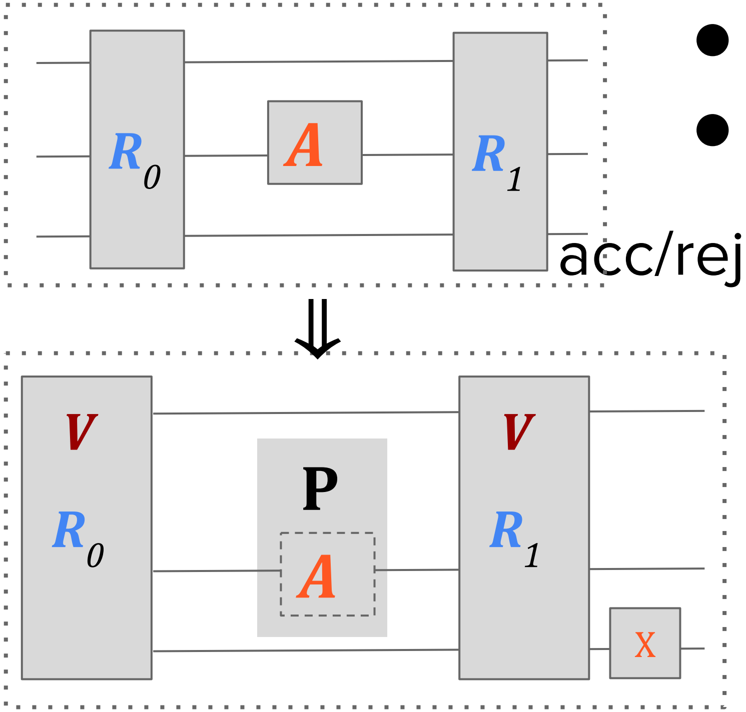
Our Main Theorem. If **SAT** $\leqslant_{\mathrm{UQ}}$ **OWP by *uniform quantum-query* reductions**, then **coNP** $\subseteq$ **QIP(2)**.

- 😁 Quantum queries allowed
- ☹️ Queries follow special format
- 😕 What about **QIP(2)**?



Progress on *approx* uniform and OW *functions* too

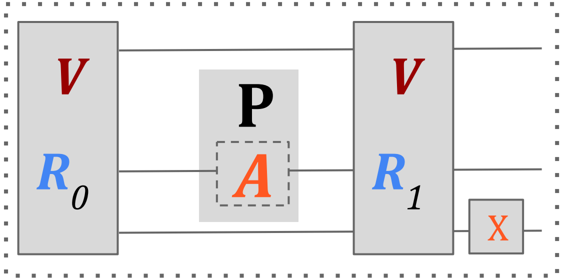
Reduction to protocol: same old trick?



- A: inverter of f
- R: **quantum** SAT solver w/ **uniform Q queries** to A

- **QIP(2) for co-SAT:**
  - 2 quantum msgs **P** ↔ **V**
- **Dishonest P*?**
  - Twist the uniform query
  - Seems undetectable

"Trap" query to enforce honest prover



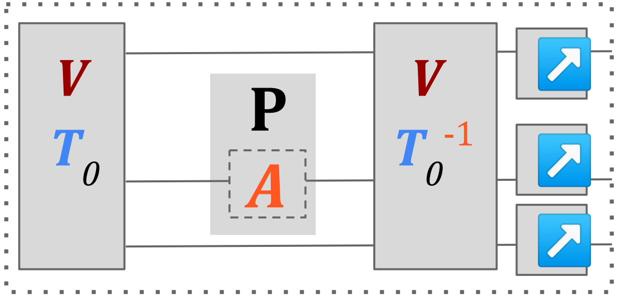
$$|0\rangle|0\rangle_M|0,0\rangle_W \overset{R_0}{\mapsto} |Q\rangle := \sum_q |q\rangle|0\rangle_M|w_q,q\rangle_W$$

$$\overset{A}{\mapsto} \sum_q |q\rangle|f^{-1}(q)\rangle_M|w_q,q\rangle_W \overset{R_1}{\mapsto} |0\rangle|\phi_0\rangle + |1,\phi_1\rangle$$

Computation path

$$Tr(|Q\rangle\langle Q|)_{\bar{M}} = Tr(|T\rangle\langle T|)_{\bar{M}}$$

Trap path



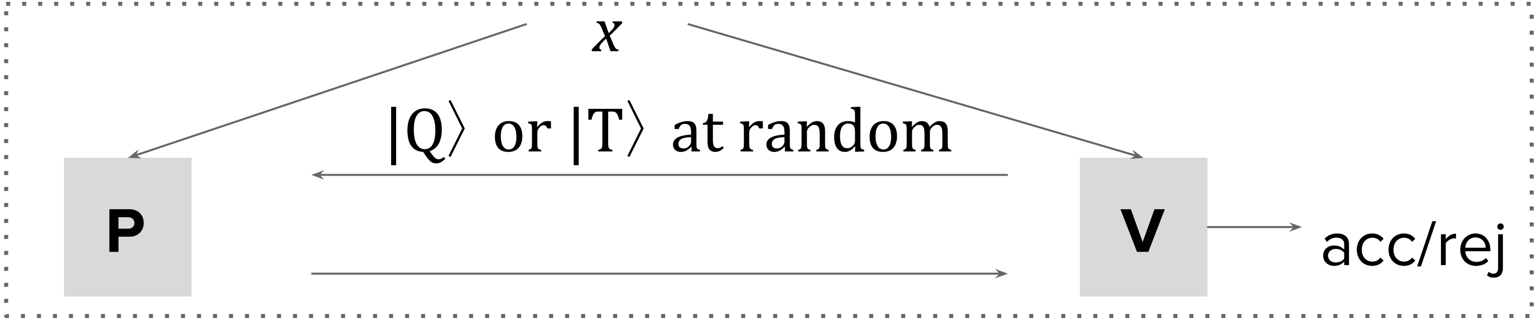
$$|0\rangle|0\rangle_M|0,0\rangle_W \overset{T_0}{\mapsto} |Q\rangle := \sum_q |q\rangle|0\rangle_M|0,q\rangle_W$$

$$\overset{A}{\mapsto} \sum_q |q\rangle|f^{-1}(q)\rangle_M|0,q\rangle_W \overset{T_0^*}{\mapsto} |0\rangle|0\rangle_M|0,0\rangle_W$$

Dishonest P ⇒ not all 0

A QIP(2) protocol for co-SAT

- V chooses to run Comp/Trap path at random

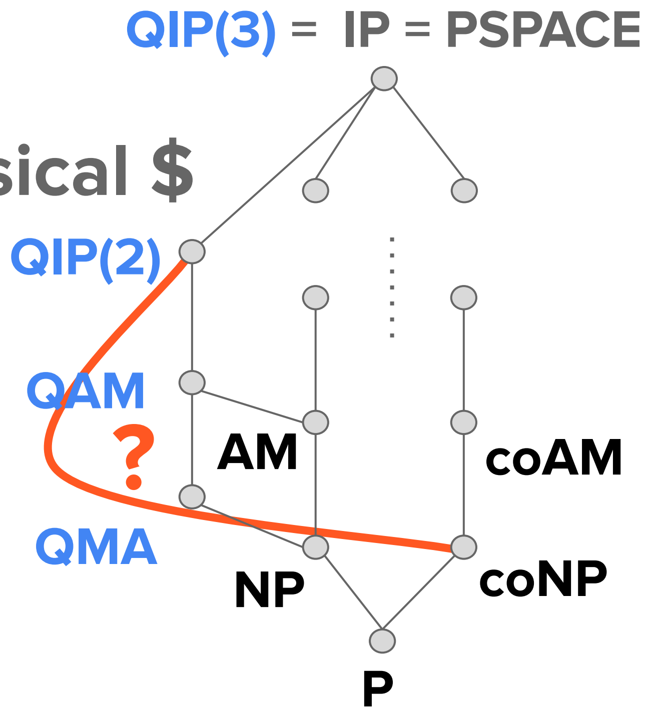


- **Completeness**: clear
- **Soundness**: P cannot tell and has to behave

The curious case of QIP(2)

- QIP(1) = QMA ⊇ NP
  - Common belief: **coNP ⊈ QMA**
- QAM = QIP(2) w/ 1st msg classical $
  - Common belief: **coNP ⊈ QAM**
- QIP(3) = PSPACE ⊇ coNP

★ Where does QIP(2) belong?



If P ≠ NP $\overset{?}{\Longrightarrow}$ Then Crypto

seems unlikely even with quantum reductions

- Strengthening the negative evidence
  - General reductions, QIP(2) → QAM?
- Revist crypto landscape via quantum reductions
  - Making [OWF $\Rightarrow$ Collision resistant hash] possible?

Thank you!