@Qcrypt'19, 08/2019, Montréal

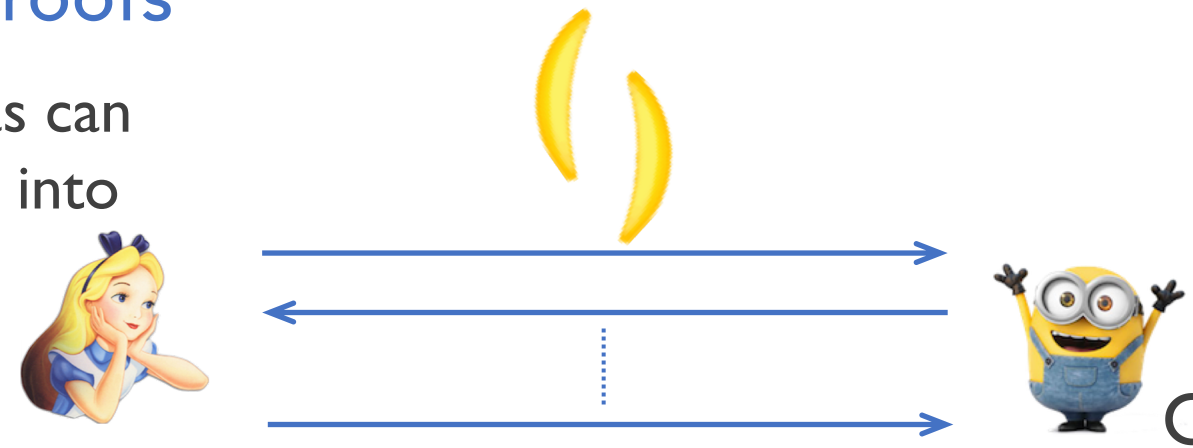
Zero-knowledge proofs in a quantum world

Fang Song
CSE, Texas A&M U

A tale of two parties

- Interactive Proofs

The two bananas can be transformed into each other



Okemar! (checked)

- Zero-Knowledge (ZK) Proofs

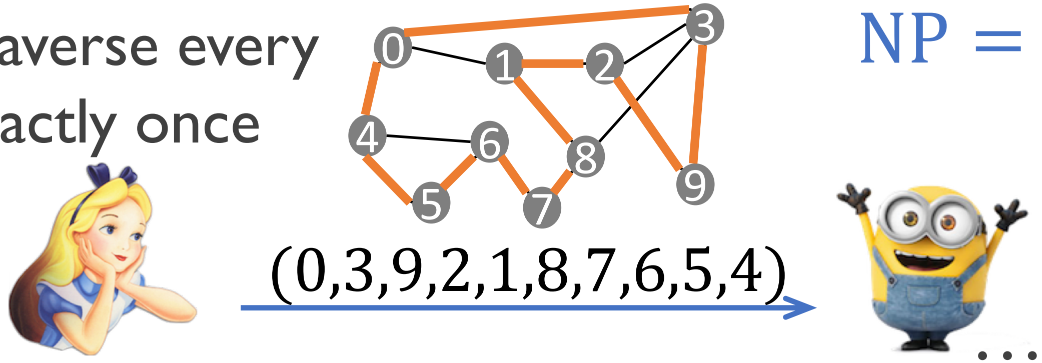
But I still don’t know how

Two examples that are NOT Zero-Knowledge

1

You can traverse every node exactly once

$\mathrm{NP} = \{A: \text{polytime verifiable}\}$



Okemar!

… but I learned the path!

2

Gru and Dru do not look the same

… but dishonest me can impersonate Alice

Why do we want Zero-Knowledge proofs?

- Cryptography: invaluable building block
  - Identification, digital signature, IND-CCA2 public-key encryption
  - Secure multi-party computation
  - Blockchain & bitcoin, cloud computing and delegation, …

- Complexity theory and philosophy

Our agenda

1. Which problems have ZK proof systems?

2. Do they remain ZK against quantum attacks?

3. How about making quantum interactive proofs ZK?

The triumph of zero-knowledge proofs

- Every problem in NP has* a ZK proof system [GMW'86]

  * under reasonable hardness assumptions

- Anything provable (i.e., IP) can* be proven in ZK [Ben-Or et al.'90]

Conditional

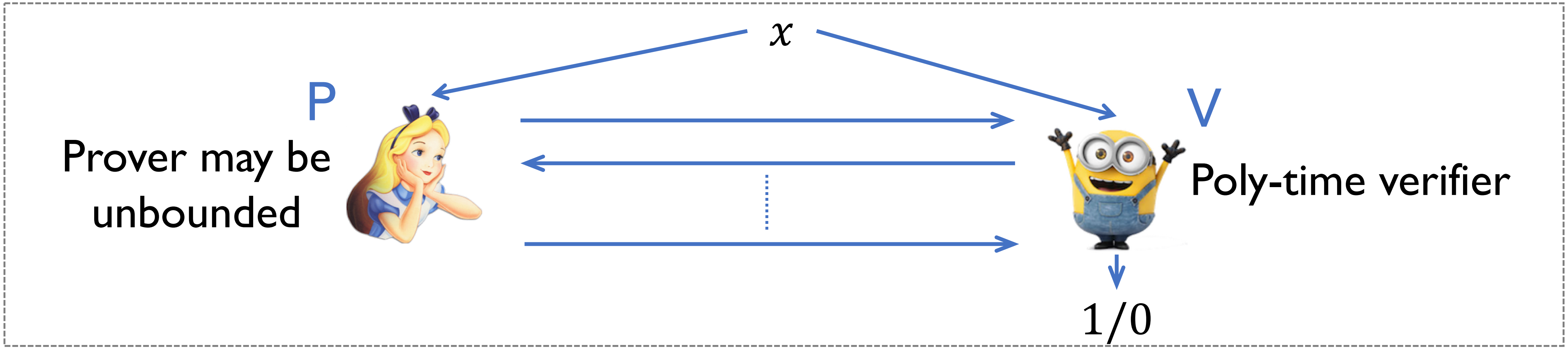
vs.

Unconditional

- General properties about ZK [GSV'96,Okamoto'96,Vadhan'06,…]

Interactive proofs: a little formality

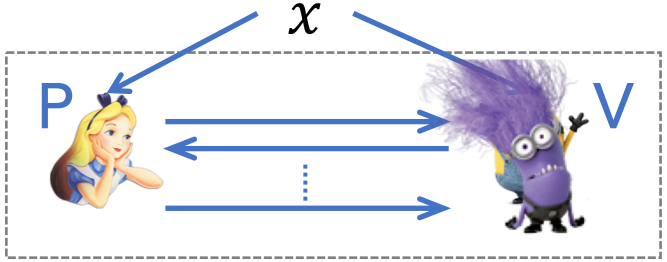
- $\langle P, V \rangle$: interactive proof system for problem A
  - **Completeness:** if $x \in A_Y$, V outputs 1 with probability $\geq 2/3$.
  - **Soundness:** if $x \in A_N$, $\forall$ (dishonest) P^*, V outputs 0 with probability $\geq 2/3$.



Promise problem: $A = (A_Y, A_N)$ where $A_Y, A_N \subseteq \{0,1\}^*$ & $A_Y \cap A_N = \emptyset$

Defining Zero-Knowledge: simulation paradigm

- $\langle P, V \rangle$: zero-knowledge proof system for problem A
  - Completeness & soundness
  - Zero-knowledge: whatever V gains could've been **simulated** by V on its own



"Indistinguishable"

$\approx$

$View(V, P, x)$

- output of V, protocol transcript
- local randomness, internal state …

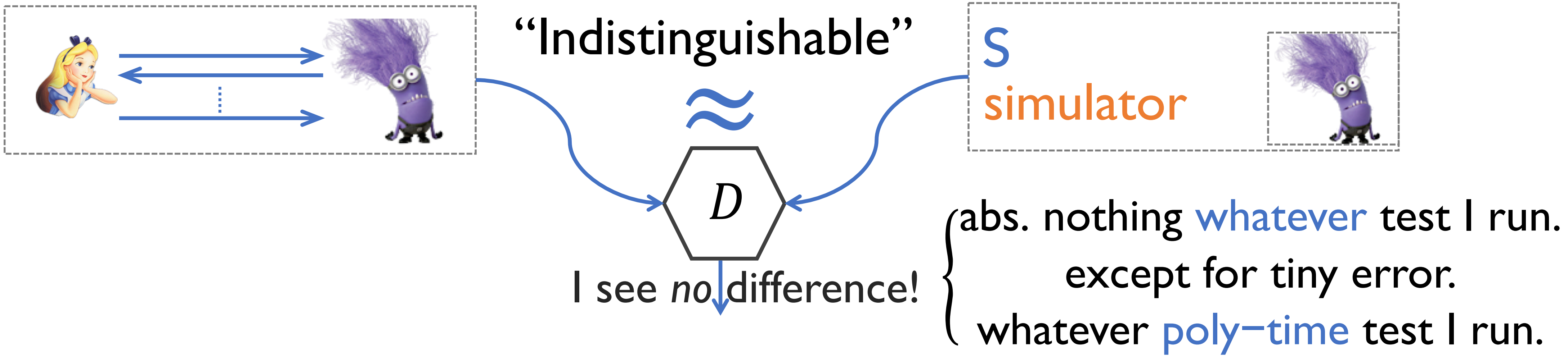
$S(V, x)$

$\exists$ poly−time S, s.t., $\forall x \in A_Y$, $View(V, P, x) \approx S(V, x)$.

Honest-Verifier ZK

$\forall$ poly−time V^*, $\exists$ poly−time S, s.t. $\forall x \in A_Y$, $View(V^*, P, x) \approx S(V^*, x)$.

Meanings of "indistinguishable"



- Perfect ZK: $View = Sim$, identical distributions.
- Statistical ZK: $View \approx_s Sim$, total variance distance negligible.
- (Computational) ZK: $View \approx_c Sim$, no efficient distinguisher.

A complexity-theoretic glossary: #1

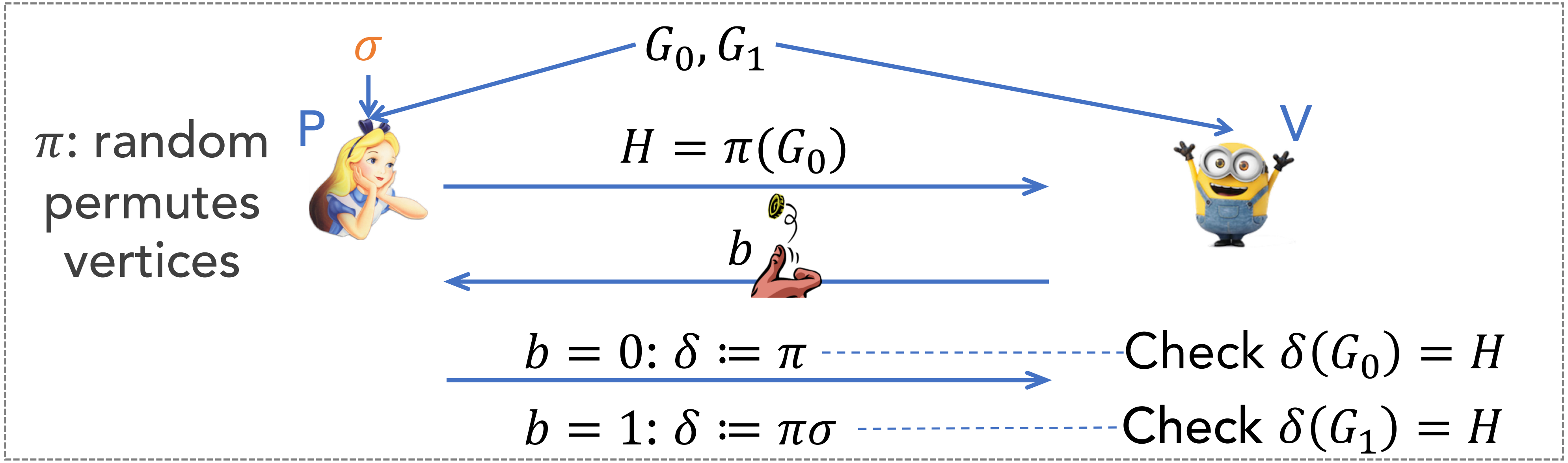
- IP $= \{A : A$ has an interactive proof system$\}$
- PZK $= \{A : A$ has a perfect ZK proof system$\}$
- SZK $= \{A : A$ has a statistical ZK proof system$\}$
- ZK $= \{A : A$ has a computational ZK proof system$\}$
- P $= \{A :$ polytime computable$\}$
- BPP $= \{A :$ probabilistic polytime computable$\}$
- NP $= \{A :$ polytime verifiable$\}$

Simple observation: $\mathrm{P} \subseteq \mathrm{BPP} \subseteq \mathrm{PZK} \subseteq \mathrm{SZK} \subseteq \mathrm{ZK}$

ZK for non-trivial (beyond BPP) problems?

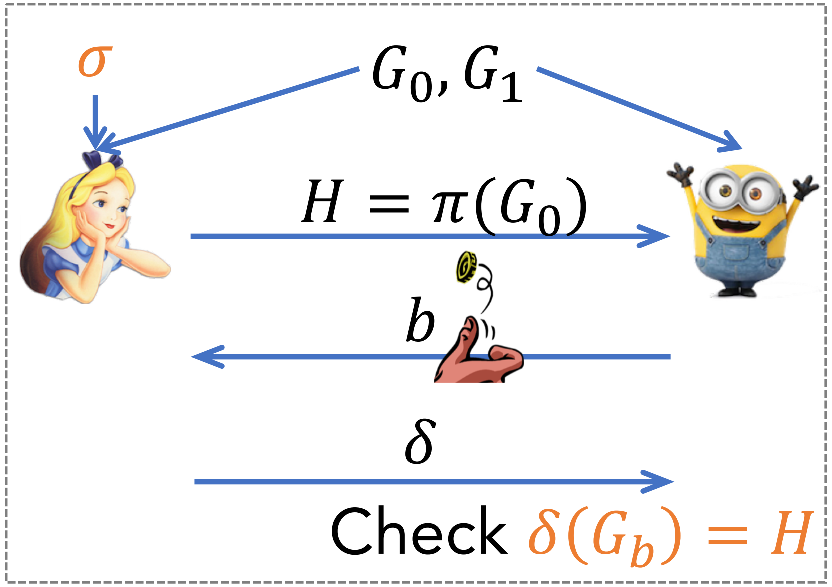
ZK for Graph Isomorphism

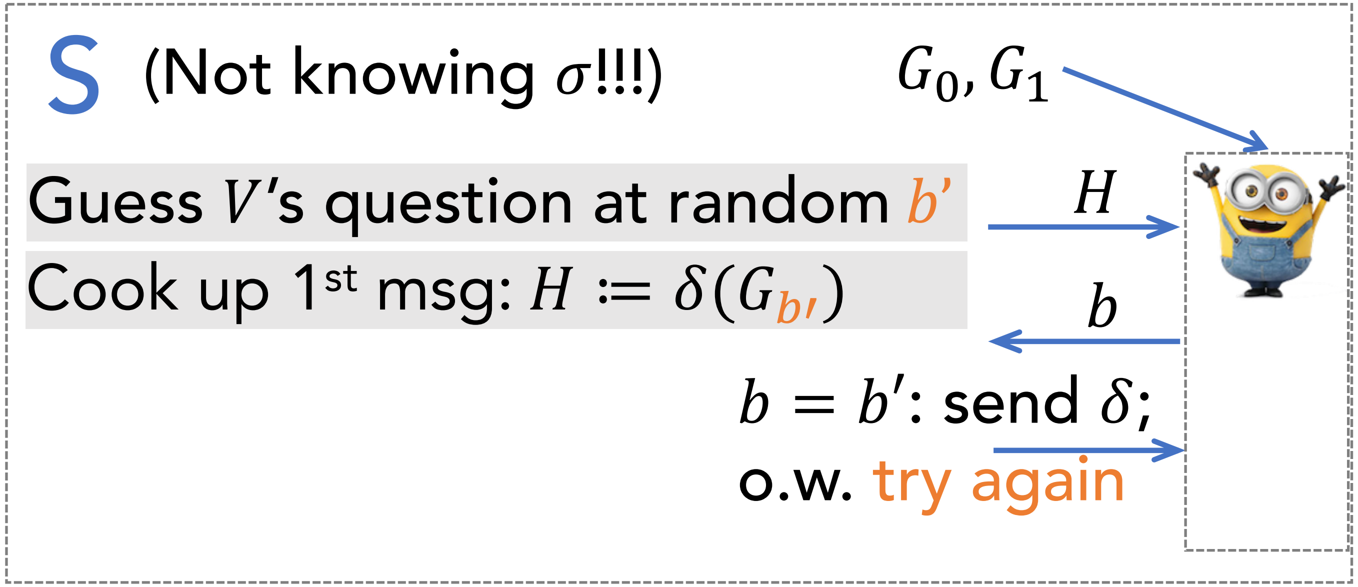
- Input: graph (G_0, G_1). Accept if they are isomorphic.
- P gets witness σ ($\sigma(G_1) = G_0$) if exists



- Completeness. OK
- Soundness. If (G_0, G_1) NOT isomorphic: P cannot answer both questions; caught by probability 1/2.

Simulation by rewinding

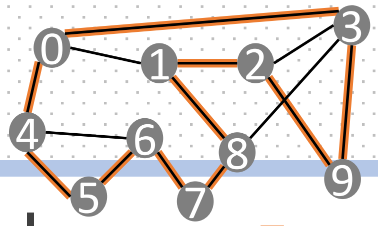




- Why rewinding works
  - b' independent of b: two iterations in expectation till $b' = b$
  - Also works for dishonest V^*
  - Trivia: S can run/reset V^* at any point

→ $\mathrm{GI} \in \mathrm{PZK}$ (GI not known in BPP) N.B. Graph Non-ISO also in SZK

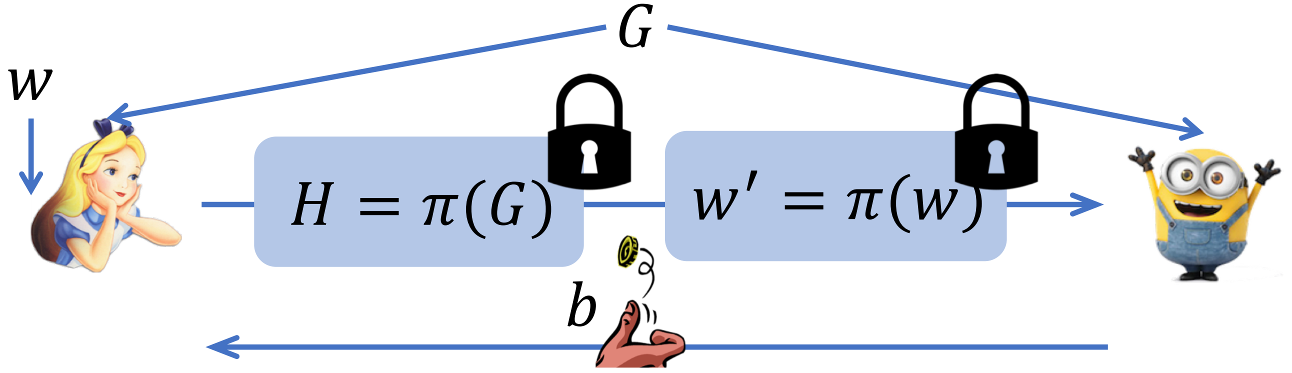
ZK for NP



- **Input**: graph G. Decide if there is a Hamiltonian cycle.
- P gets a witness w if exists.

Fact: HCycle is NP-complete

π: random permutes vertices



$b = 0$: open Box1 (H) and π ------ Check $\pi(G) = H$

$b = 1$: open Box1&2 (the part of H in w') and (w') --- Check $H_{w'}$ and w' match

$\therefore$ HCycle $\in^*$ ZK ➔ NP $\subseteq^*$ ZK

*assuming commitment scheme $\Leftrightarrow$ one-way functions

Our agenda

1. Which problems have ZK proof systems?

2. Do they remain ZK against malicious quantum verifiers?

3. How about making quantum interactive proofs ZK?

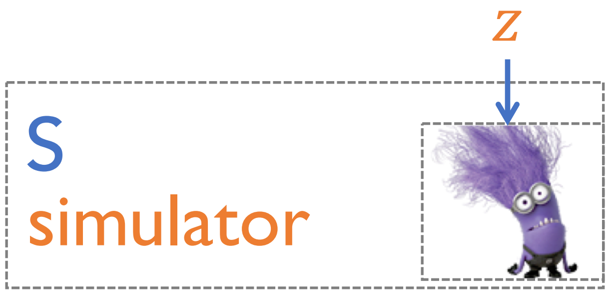
Is it as simple as switching to quantum-secure assumptions, e.g., using lattice-based rather than factoring?

Every problem in **NP** has* a ZK proof system secure against quantum malicious verifiers [Watrous'09]

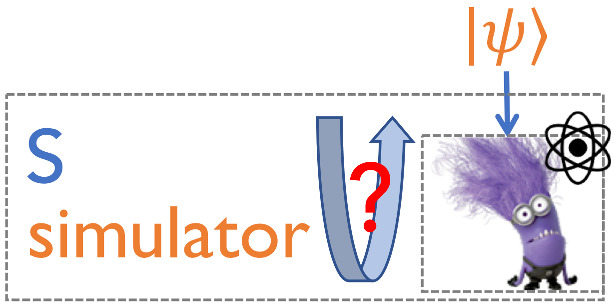
* under quantum-secure hardness assumptions

Every problem in **IP** has* a ZK proof system secure against quantum malicious verifiers [To be verified]

Difficulty of quantum rewinding



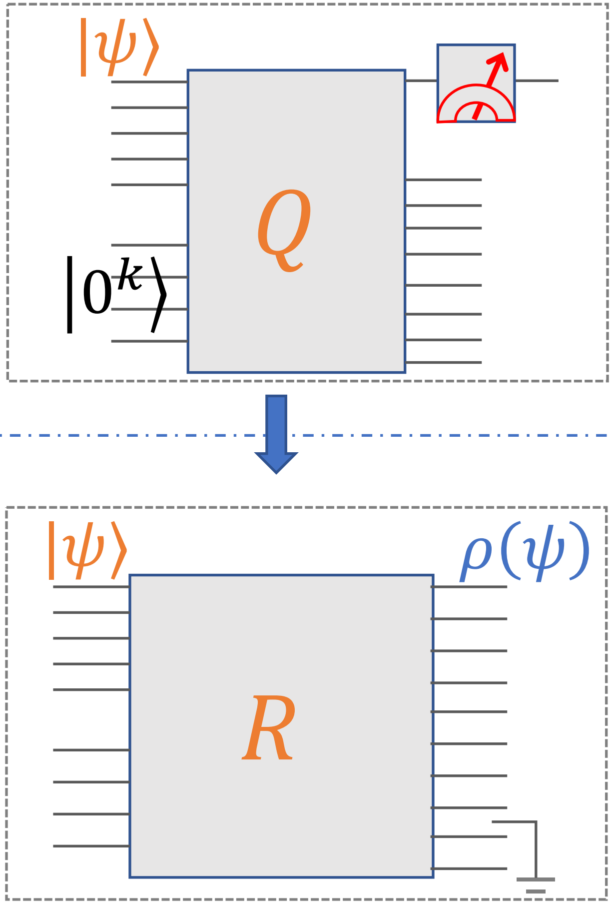
- Auxiliary input z to malicious V^*
  - Critical for composition: avoid "cross-ref" attacks



- Quantum V^* with auxiliary state $|\psi\rangle$
  - No cloning
  - Measurement may disturb the state
  - First observed in 1997 by van de Graaf, slow progress for a decade

- Breakthrough by Watrous [Watrous'09]
  - A quantum rewinding technique → Quantum-secure ZK for all NP

Watrous's rewinding technique



Q: attempt of simulation using k work qubits

- $|\psi\rangle$: V^*'s auxiliary state
- $p(\psi)$: probability of measuring 0
- $|\phi_0(\psi)\rangle$: desired state ≈ true view

$$Q|\psi\rangle|0^k\rangle = \sqrt{p(\psi)}|0\rangle|\phi_0(\psi)\rangle + \sqrt{1-p(\psi)}|1\rangle|\phi_1(\psi)\rangle$$

Wishful thinking: "no info. gain" → no disturbance?

Theorem. If $p(\psi) = p \in (0,1)$ constant over all $|\psi\rangle$, then one can construct R:

- Output $\rho(\psi) \approx_\epsilon |\phi_0(\psi)\rangle\langle\phi_0(\psi)|$
- $Size(R) = O(size(Q) \cdot \log 1/\epsilon)$

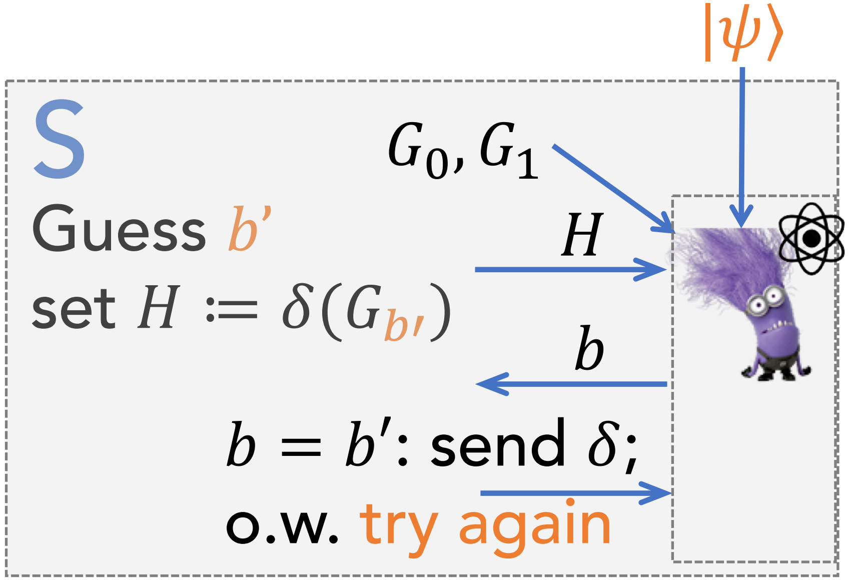
N.B. "True rewinding" (recover $|\psi\rangle$ from Q's output) possible by oblivious amplitude amplification [BCC+'14]

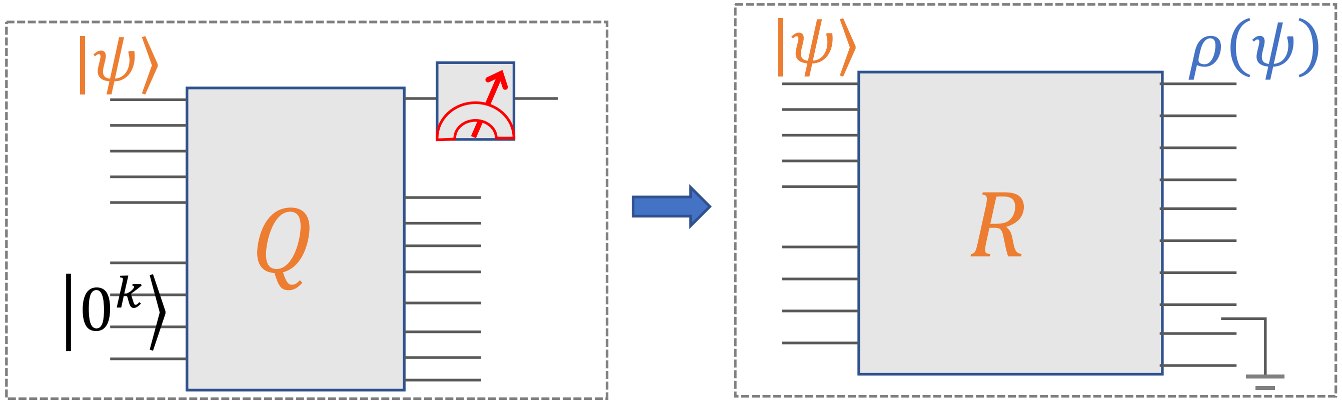
Constructing quantum simulators

Q: quantize classical simulator S

- Measure $b' = b$
- Obs. $p(|\psi\rangle) = \Pr[b' = b] = 1/2$

☺ Watrous's rewinding applicable!





R: quantum simulator ➔ Quantum-secure ZK for GI

➔Quantum-secure ZK for NP

- Watrous's "noisy" quantum rewinding works for Hcycle: $p(\psi) \approx$ constant

A complexity-theoretic glossary: #2

Quantum-secure ZK (qZK): $\forall$ quantum $\text{poly-time } V^*$, $\exists$ poly-time S, s.t. $\forall x \in A_Y$ & ρ, $\text{View}(P, V^*, x, \rho) \approx S(V^*, x, \rho)$.

i.e., the two channels $\langle P, V^* \rangle$ and S_{V^*} are indistinguishable.

- $\text{qPZK} = \{A: A \text{ has a quantum-secure perfect ZK proof system}\}$
- $\text{qSZK} = \{A: A \text{ has a quantum-secure statistical ZK proof system}\}$
- $\text{qZK} = \{A: A \text{ has a quantum-secure computational ZK proof system}\}$

Our agenda

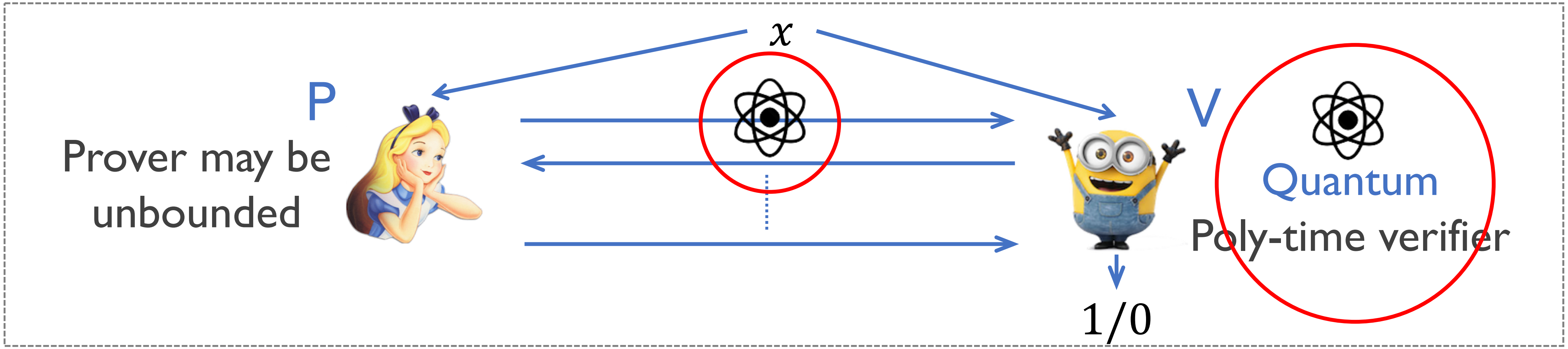
1. Which problems have ZK proof systems?

2. Do they remain ZK against malicious quantum verifiers?

3. How about making quantum interactive proofs ZK?

Equipping honest players with quantum

- $\langle P, V \rangle$: quantum interactive proof system for problem A
  - Completeness: if $x \in A_Y, V$ outputs 1 with probability $\geq 2/3$.
  - Soundness: if $x \in A_N$, $\forall$ (dishonest) P^*, V outputs 0 with probability $\geq 2/3$.



- QIP $= \{A: A$ has a quantum interactive proof system$\}$

Quantum zero-knowledge proofs

- $\langle P, V \rangle$: quantum zero-knowledge proof system for problem A
  - A quantum interactive proof system (completeness & soundness)
  - Quantum zero-knowledge: $\forall$ quantum poly$-$time V^*, $\exists$ poly$-$time S, s.t. $\forall x \in A_Y$ & ρ, two channels $\langle P, V^* \rangle$ and S_{V^*} are indistinguishable.

- $\mathrm{QPZK} = \{A: A$ has a perfect quantum ZK proof system$\}$
- $\mathrm{QSZK} = \{A: A$ has a statistical quantum ZK proof system$\}$
- $\mathrm{QZK} = \{A: A$ has a computational quantum ZK proof system$\}$
- $\mathrm{HVQZK} = \{A: A$ has a honest$-$verifer QZK proof system$\}$

Power of quantum interaction

- QIP = IP = PSPACE [JJUW'09]
  - No gain regarding solvable problems
  - Various niceties: (QIP) 3-messge = poly-message, …

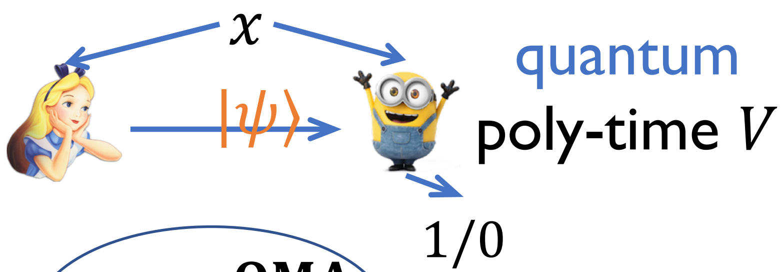
- Every problem in **QMA** has* a quantum ZK proof system [BJSW'06]

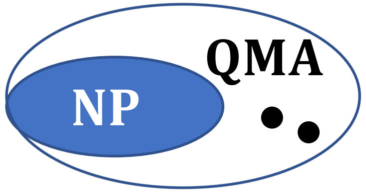
  * under same hardness assumptions as the quantum-secure (classical) ZK protocol for NP

  - De-quantized by Vidick and Zhang (check their talk later this morning), additionally assuming quantum hardness of the Learning-with-Errors problem

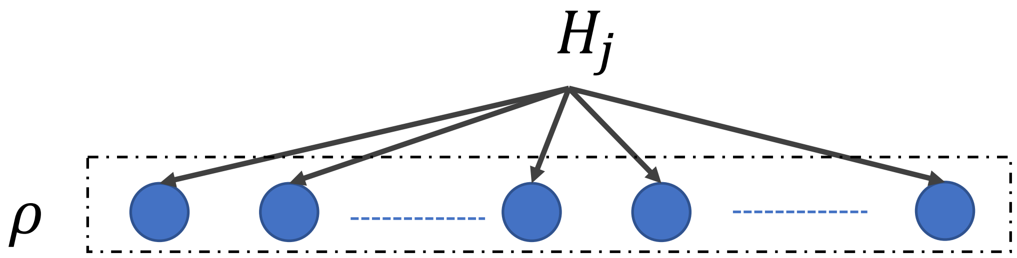
Quick tour of QMA

- Quantum analogue of NP (or MA)
  - Problems verifiable by efficient quantum circuit, i.e., admit $1-$message QIP system
  - $\exists\, L \in \mathrm{QMA}$, NOT believed in NP (ex. group non-membership)





- QMA-complete problem
  - Local Hamiltonian problem [KitaevSV]
  - Many variants identified



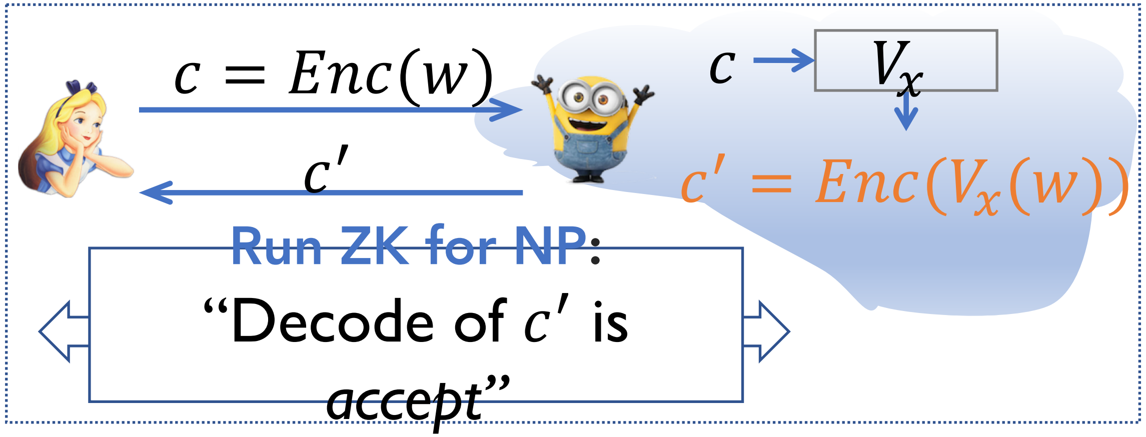
Input: Hamiltonian operators $H_1, \ldots H_m$, each H_j on 5 qubits

- YES: $\exists$ n-qubit state ρ, $\langle \rho, \sum H_j \rangle \leq 2^{-n}$ (no violation, low eigenvalue)
- NO: $\forall$ n-qubit state ρ, $\langle \rho, \sum H_j \rangle \geq 1/n$ (lots violation, large eigenvalue)

Towards quantum ZK proof for QMA

Wishful thinking: reduce (ZK for QMA) to (ZK for NP)

- Inspiration: ZK by homomorphic encryption



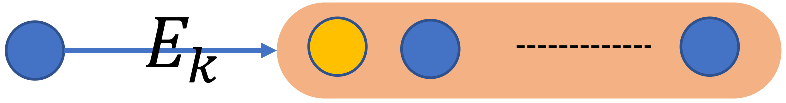
- Verifier homomorphically evaluates verification circuit
- Prover proves in ZK that the result encodes "*accept*"

- What we need
  - Right tools in the quantum setting: encoding, etc?
  - How to prevent dishonest verifier?

Evaluate another circuit compute 1^{st} bit of w!

Building the right tools [BJSW'16]

1. Augmented trap scheme*, supporting



* based on quantum error corr. & trap auth. scheme [BGS12]

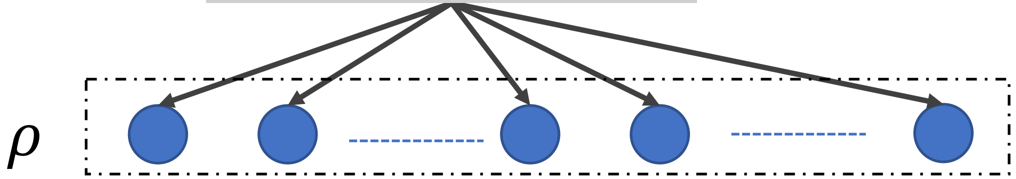
   i. Clifford circuits & measure, transversally ("somewhat homomorphic")
   ii. Perfect secrecy
   iii. Authentication: deviation from agreed operations can be detected

☹ Local Hamiltonian verification require more than Clifford ckts

2. Local Clifford-Hamiltonian (LCH) is QMA-complete

➔ we can run Verification on encoded witness (by AugTrap) transversally

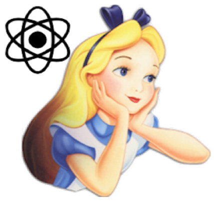
$H_j = C_j|0\rangle\langle 0|C_j^*$ C_j Clifford



QZK proof system for LCH

Input: $H_1, \ldots, H_m,\ H_j = C_j\ |0\rangle\langle 0| C_j^*$

Witness $|w\rangle$

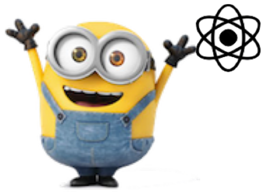


AugTrap E_k w. key k

$|w\rangle$

Committing k

k



1

2 Check $\hat{m}_j$ & H_j consistent

$j, \hat{m}_j$

Pick random j and measure H_j on encoded witness, outcome $\hat{m}_j$

3 (i.e. verifier was honest)

4 Open key bits k_j of term j

5 Invoke quantum-secure ZK proof for NP

a. open/commit consistent

b. decoding $\hat{m}_j$ according to key k_j not violate H_j

- Nice features
  - Simple structure 3-"move"
  - All but first message classical
  - Efficient prover
  - Only assuming: commitment (to classical msg) that is quantum-secure

A few remarks

- Quantum computation on authenticated data
  - Very useful technique, reducing quantum tasks to classical ones
  - E.x. quantum secure multi-party computation [BOCG+'06], …
- If conjecture true, why our effort?

IP has* a quantum-secure ZK proof system [To be verified]

☺ purely classical protocol

☹ Prover is not efficient

☹ poly-many rounds, and unlikely to be reduced

- Direct analogue of classical ZK for NP?
  - Local Consistency problem plausible, QMA-complete by Turing reduction [Liu'05]
  - Open question: prove QMA-Completeness via Karp reduction

The triumph of zero-knowledge proofs, again

- Every problem in **NP** & **QMA** has* a ZK proof system [GMW'86,BJSW'16]

  * under reasonable hardness assumptions

- Anything provable (i.e., IP) can be proven in ZK [Ben-Or et al.'90, quantum security TBV]

Conditional

vs.

Unconditional

- General properties about ZK [GSV'96,Okamoto'96,Vadhan'06,…]

What to say about ZK, unconditionally?

as a complexity theorist

- Honest-verifier ZK vs. general ZK
- Private-coin ZK vs. public-coin ZK (V just replies random coins)
- Perfect completeness ($1\ vs.\ 2/3$)
- ZK closed under union, complement, …?
- ZK with different flavors of simulators (e.x., black-box vs. non-black-box)
- …

- Relations among ZK classes, and with standard classes

A laundry list of ZK properties

SZK related [Vadhan'99]

- HVSZK = SZK
- Public-coin = private coin
- ∃ complete problems
- Closed under complement …

CZK related [Vadhan'06]

- HVZK = ZK
- Public-coin = private-coin
- Closed under union
- Perfect completeness

qZK related [HKSZ'08]

- SZK = qSZK
- ZK ⊇ ZK^+ = qZK (ZK^+: sim view quantum indist. from real)*

* verify quantum security of ZK for IP

QSZK related [Watrous'03,09]

- HVQSZK=QSZK
- ∃ complete problems
- Closed under complement
- 2-messages suffice (3 if public coin)

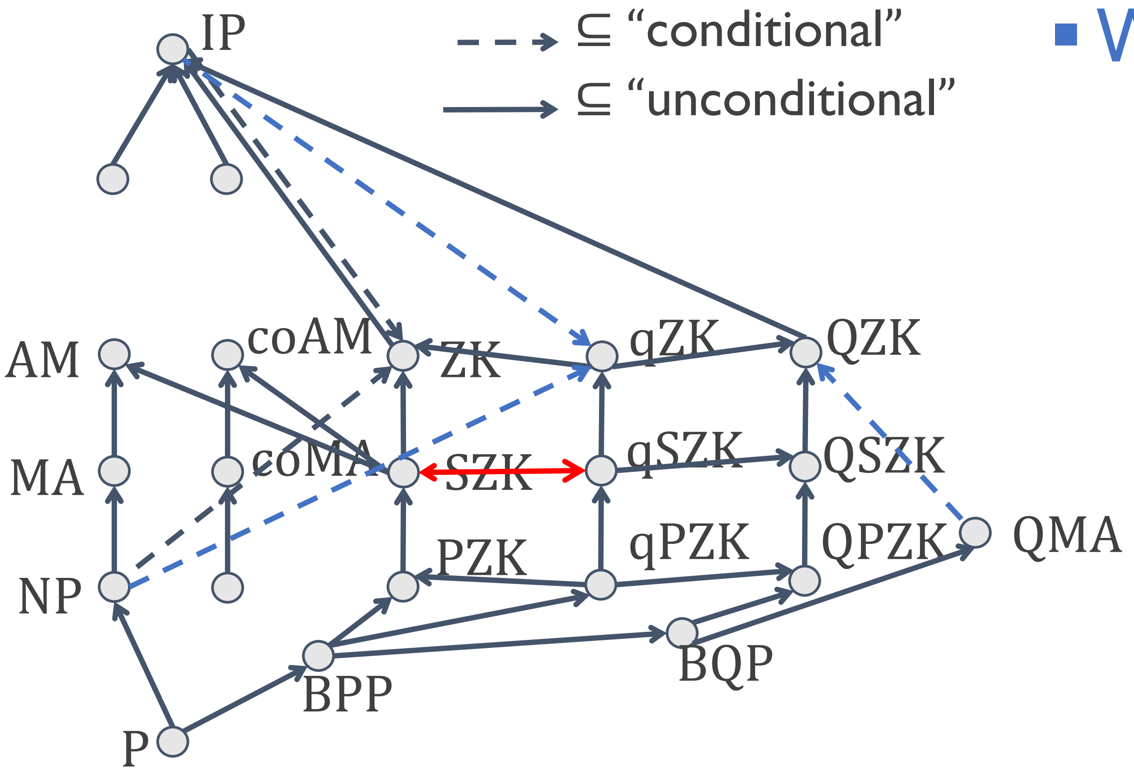
QZK related [Kobayashi'08]

- HVQZK=QZK
- Public-coin = private coin
- Perfect completeness

Complexity-theoretic landscape of ZK

- Something you wanted to ask
  - SZK ⊆ QSZK?

  → YES. Given SZK = qSZK ⊆ QSZK. Not clear *a prioi*!



- What is missing?
  - ZK ⊆ QZK? HVqZK = qZK?
  - QSZK better upper bound? (SZK ⊆ AM ∩ coAM)
  - Hybrid world: conditional meets unconditional. Possible scenario: if ∃quantum-secure one-way function, ZK = qZK = QZK = IP.
  - …

Our agenda

1. Which problems have ZK proof systems?

2. Do they remain ZK against malicious quantum verifiers?

3. How about making quantum interactive proofs ZK?

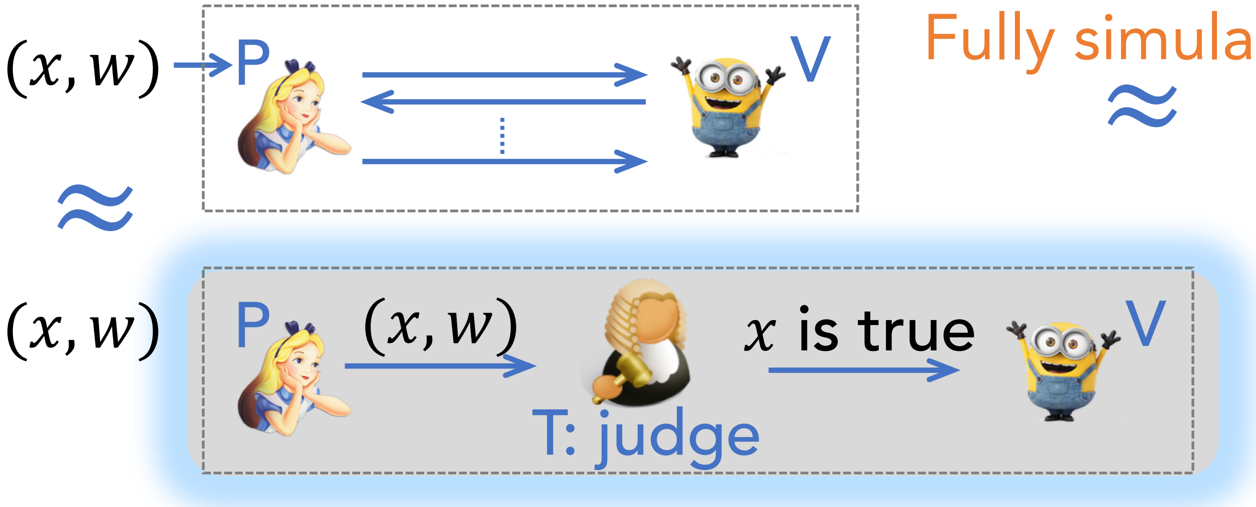
* Extensions

Ext. 1: Proofs of knowledge

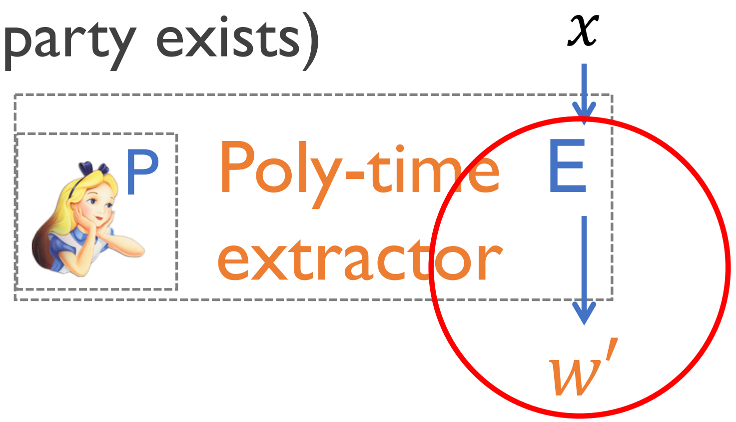
- $\langle P, V \rangle$: zero-knowledge proof of knowledge system for problem A
  - Completeness & soundness & zero-knowledge
  - Proof of knowledge: if P can prove it, P indeed "knows" a witness.

$\forall\ P^*$, $\exists$ extracotr E that outputs a witness, whenever P^* convinces V

- Fully-simulatable ZKPoK
  - In addition, E generates a "real-looking" view. Critical for composition
  - i.e. $\langle P, V \rangle$ realizes an ideal protocol (as if a trusted 3rd party exists)

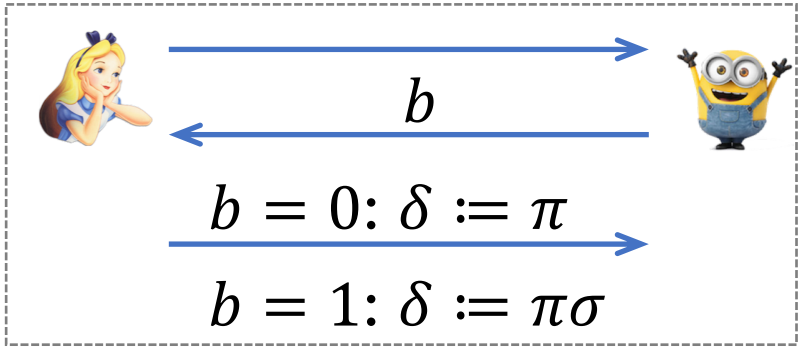


Fully simulatable: $\approx$



Results on ZKPoK

- Every **NP** problem has* a fully-simulatable ZKPoK proof system



Recall ZK for GI: $\sigma(G_1) = G_0$

- How I wish I can ask both questions!
- Extractor: will do! Ask one, *rewind*, ask again.
- Witness delivered: $\sigma := \delta_0^{-1} \circ \delta_1$

Are they quantum-secure?

☹ Watrous's rewinding is "oblivious": cannot extract

☺ Extraction against quantum provers [Unruh'12]
- but no simulation

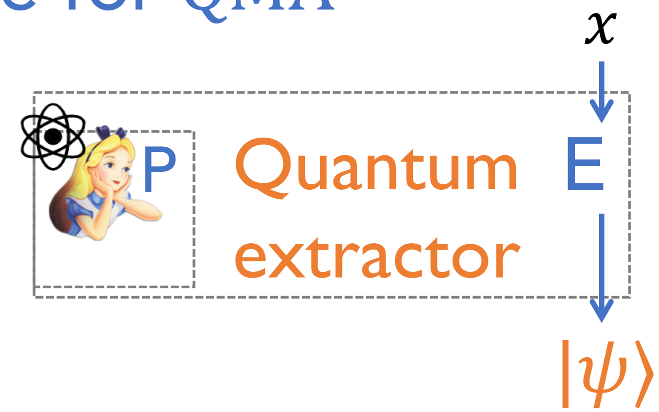
☺ Fully-simulatable ZKAoK [HSS'11]
- A more sophisticated protocol
- Argument not a proof: sound against poly-time provers only

Open questions on ZKPoK

- Quantum-secure fully-simulatble ZKPoK

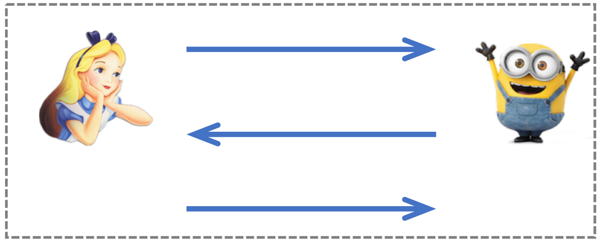
QUANTUM REWINDING

- Proofs of quantum knowledge for QMA



Ext. 2: constant-round ZK

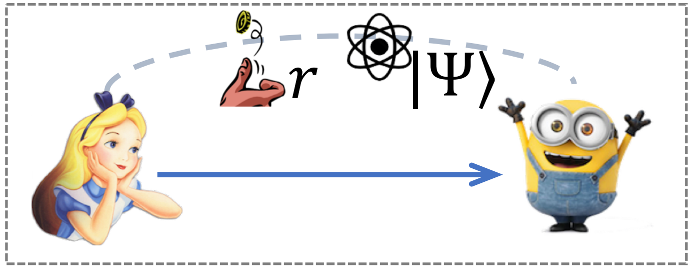
- Aren't the protocols we show already constant-round?
  - Want negligible soundness error (rather than constant)
  - Sequential composition preserves ZK, but parallel doesn't



- A fine classical picture*   * black-box simulator
  - $\leq$ 3-message ZK = BPP [GO'94], 4-message ZKP unlikely for NP [Katz'08]
  - ∃4-message ZKAoK for NP [FS'90]
  - ∃5-message ZKP for NP [GK'96], ∃constant-round ZKPoK for NP [Lin'13]
- An incomplete quantum picture
  - Quantum security of above unknown (lacking strong quantum rewinding)
  - (Quantum-secure) constant-round coin-flipping $\Leftrightarrow$ constant-round ZK for NP $\Leftrightarrow$ constant-round ZK for QMA [HSS'11,BJSW'16]
  - 3-message QZK = BQP [JKMR'06]

Ext. 3: non-interactive ZK

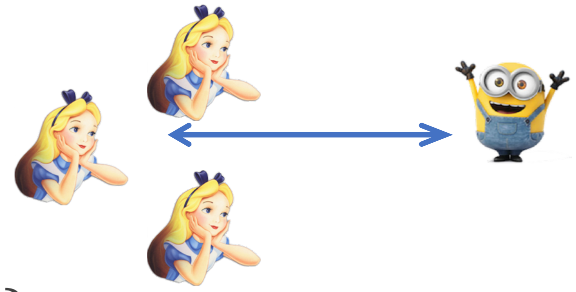
- NIZK: 1-message ZK with shared randomness
  - Recall: a single message alone is not useful
- QNIZK: 1-message QZK with entanglement



- What we know?
  - NIZK for NP assuming trapdoor permutations [BFM'88]
  - NIZK for NP assuming learning-with-errors [Peikert'19]
  - SNARKs: super-efficient delegation (Z-Cash) […]
  - Graph non-automorphism ∈ QNIZK [Kobayashi'03]
- Open Questions
  - Is [Peikert'19] quantum-secure? (NIZK = qNIZK?)
  - QNIZK with shared coins vs. shared entanglement

Ext. 4: multi-prover ZK

- Multi-prover interactive-proof system
  - Non-commuting provers once protocol begins
  - Can share randomness or entanglement
  - $\mathrm{MIP} = \{A\colon A \text{ has a multi}-\text{prover interactive proof system}\}$
  - $\mathrm{MIP}^* = \{A\colon A \text{ has a entangled multi}-\text{prover interactive proof system}\}$

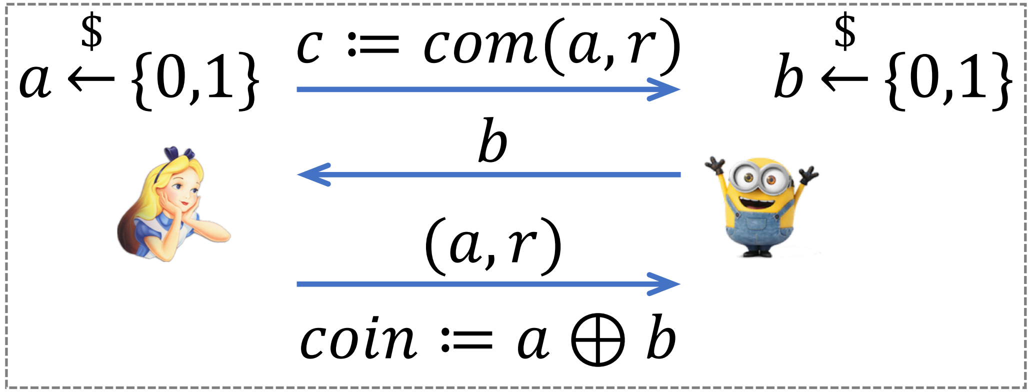


- What we know?
  - $\mathrm{MIP}=\mathrm{PZK}-\mathrm{MIP}$ [BGKW88]; can be made sound against entangled provers [CFGS18]
  - $\mathrm{MIP}^* = \mathrm{PZK}-\mathrm{MIP}^*$ [GSY19] (later this morning)

- Open Questions
  - ZK holds against quantum verifiers?

Reflecting on challenges of quantum ZK

- More general quantum rewinding, to get Q-secure protocols
  - Constant-round ZK
  - Fully-simulatable ZKPoK
  - Fully-simulatable coin tossing (embarrassing fact: even Blum's one-bit protocol on the right is unclear)

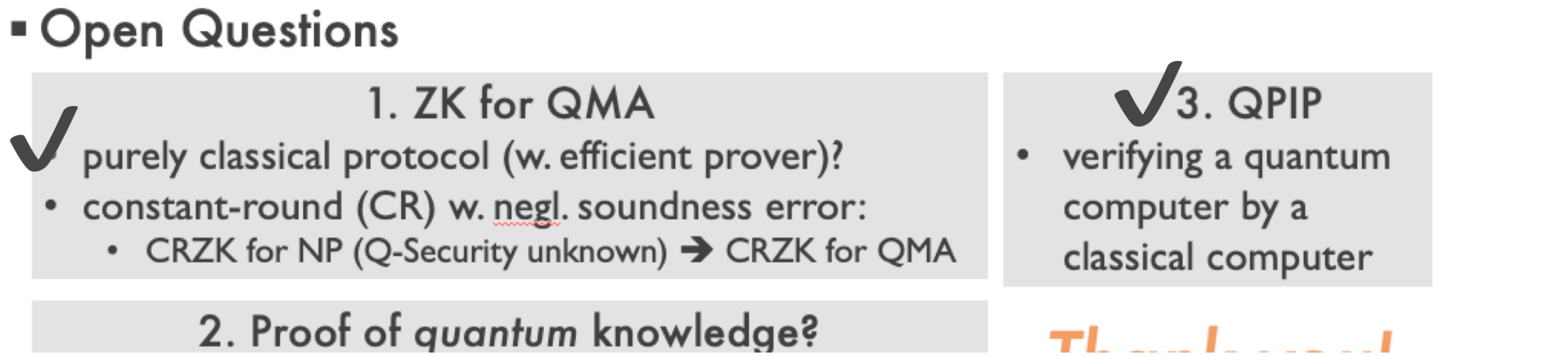


- Defining quantum ZK: a right one?
  - Classical relaxations: witness indistinguishable, witness hiding
  - Quantum witness: is leaking local density of the ground state so dreadful?

ZK in a quantum world: looking forward

- A lot of challenges
- A bright prospect

Screenshot of my talk at FOCS'16 (QZK for QMA)



Thank you!

References

- Bib file and (maybe) a companion survey paper will be posted soon at https://fangsong.info/research/#other-talks