QIP 2017

Zero-knowledge proof systems for QMA

Fang Song

Portland State University

Joint work with

Anne Broadbent
U of Ottawa

Zhengfeng Ji
U of Technology Sydney

John Watrous
U of Waterloo

How does cryptography **change** in a quantum world?

- Quantum attacks

Hard problems broken

- Factoring & DL [Shor'94],
- Some lattice problems [EHKS'14,BS'16,CDPR'16]

Security analyses fail

- Unique quantum attacks arise
- Difficult to reason about quantum adversaries!

- Quantum protocols

Outperform classical protocols

- Ex. Quantum key distribution

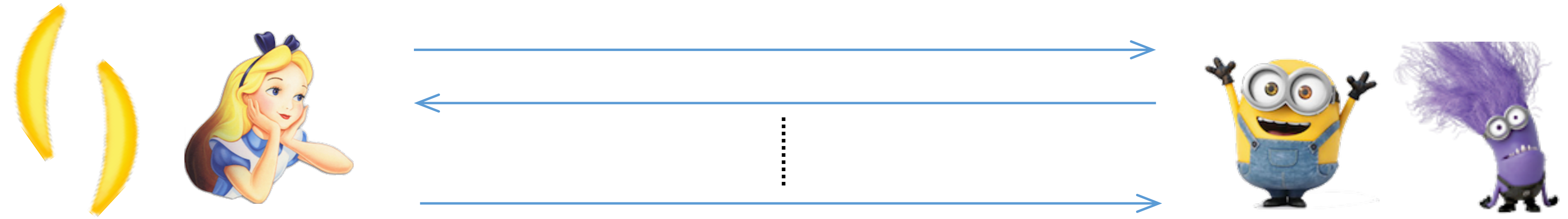
Crypto tools for quantum tasks

- Ex. Encrypt quantum data

Today's Topic

Zero-Knowledge proof systems

[GoldwasserMicaliRacoff STOC'84]



The two bananas can be transformed into each other

I'm convinced!
But I still don't know how

What problems can be proven in Zero-Knowledge?

Today in history: ZK for NP

What problems can be proven in Zero-Knowledge?

[GoldreichMicaliWidgerson FOCS'86]

Every problem in **NP** has a zero-knowledge proof system*

* Under suitable hardness assumptions

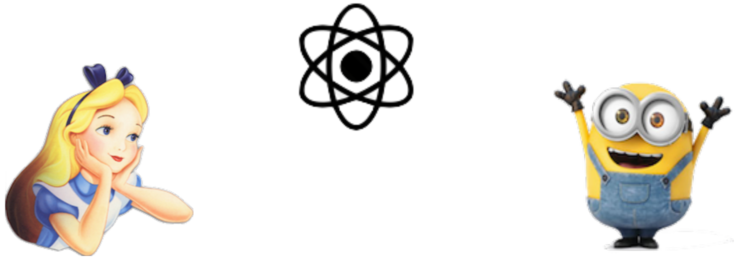
- Invaluable in modern cryptography

Today: ZK in a quantum world

What problems can be proven in Zero-Knowledge *quantumly*?

1. Do **classical** protocols remain Zero-Knowledge against quantum malicious verifiers?

2. Can **honest users** empower quantum capability and prove problems concerning quantum computation?



ZK in a quantum world: status

1. Classical ZK against quantum attacks: big challenge

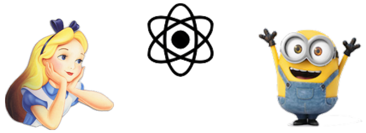
- **Rewinding**: difficult against quantum attackers [Graaf'97]

  Critical for showing ZK classically

- Special quantum rewinding [Watrous'06]
  - GMW protocol can be made quantum-secure
  - many other cases not applicable

Quantum-secure ✔ ZK for NP

2. ZK proofs for quantum problems: little known



- Quantum *statistical* zero-knowledge well understood
- We, as in GMW, consider computational zero-knowledge

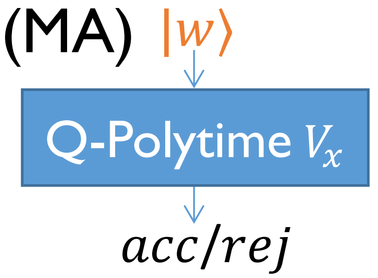
GMW analogue in Quantum?

Our main result

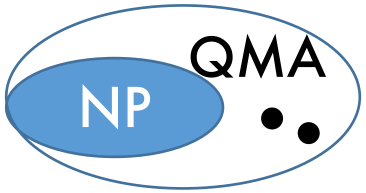
Every problem in QMA has a zero-knowledge proof system*

QMA: quantum analogue of NP (MA)

- Problems verifiable by efficient **quantum** alg.



- Power: $\exists\ L$ in QMA, NOT believed in NP (ex. group non-membership)



- Nice features of our **ZK** protocol for QMA:
  - Simple structure 3-"move": commit-challenge-respond
  - All communication classical except first message
  - *(Almost) minimal assumption: same as GMW with quantum resistance
  - Efficient prover: useful to build larger crypto constructions

Our additional contributions

New tools for quantum crypto and quantum complexity theory

- Identifying a new complete problem for QMA

  Corollary: QMA = QMA with very limited verifier

  - Simpler proof than some recent work [MorimaeNF'15'16]

Further implications?

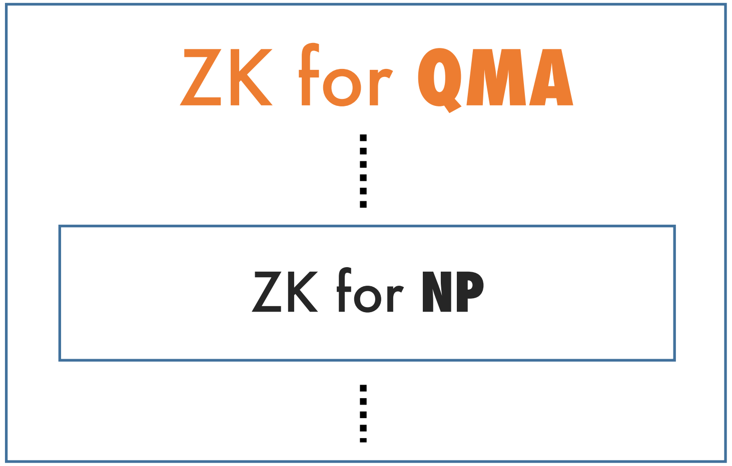
- A quantum encoding mechanism, supporting
  - "Somewhat homomorphic"
  - Perfect secrecy
  - Authentication

Other applications?

ZK for QMA
Our construction:

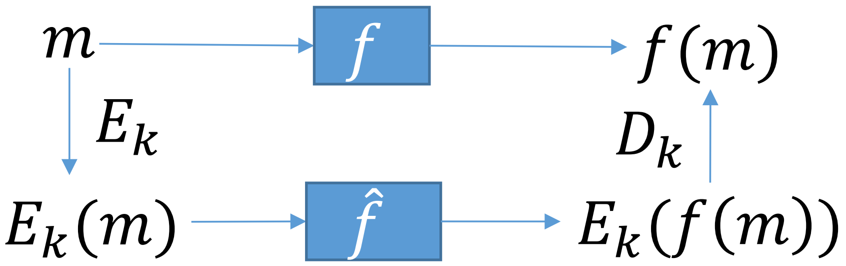
Inspiration: ZK by homomorphic encryption

Reductionist's wishful thinking:
reduce (ZK for QMA) to (ZK for NP)

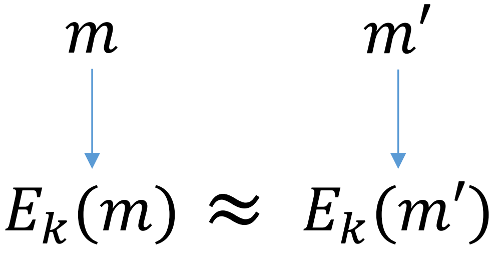


- **I seem to know how to:** reduce (ZK for NP) to (ZK for NP)

  using HOMOMORPHIC ENCRYPTION



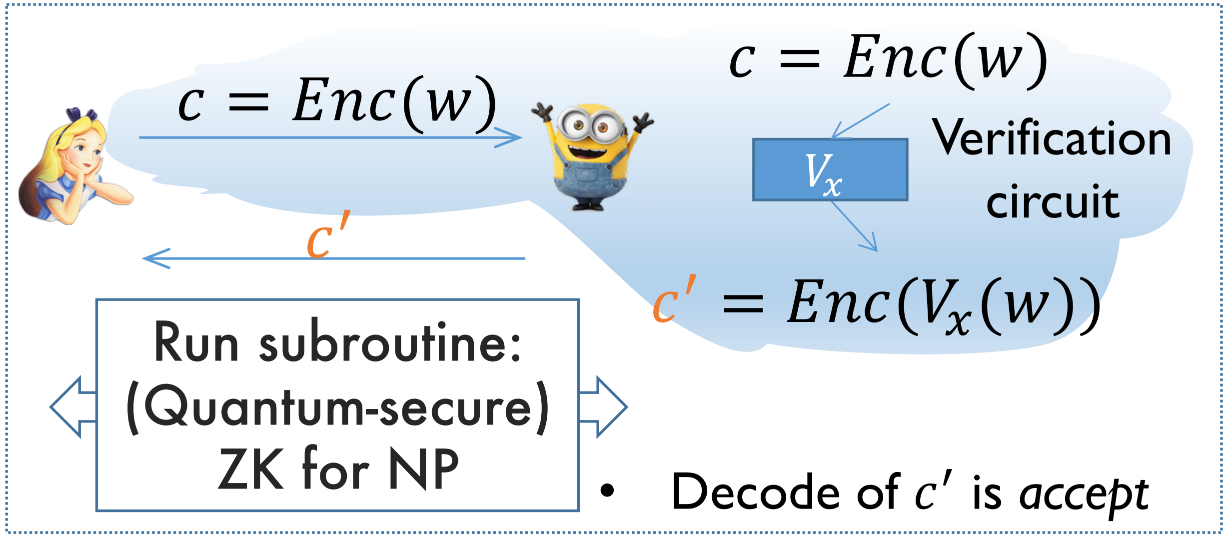
Homomorphic



Secrecy

Inspiration: ZK by homomorphic encryption

- Construct (ZK for NP) on (ZK for NP) using homomorphic Enc



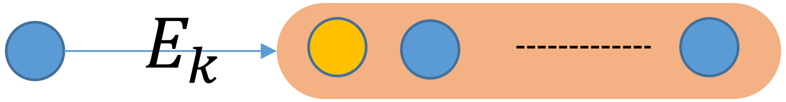
- Verifier homomorphically evaluates Verification ckt on encrypted witness
- Prover proves in ZK: the result encodes "*accept*"

- Challenges of adapting to QMA:
  - Right tools in the quantum setting: encoding, etc?
  - Need authentication: how to prevent dishonest verifier?

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

! We give an elegant quantum solution

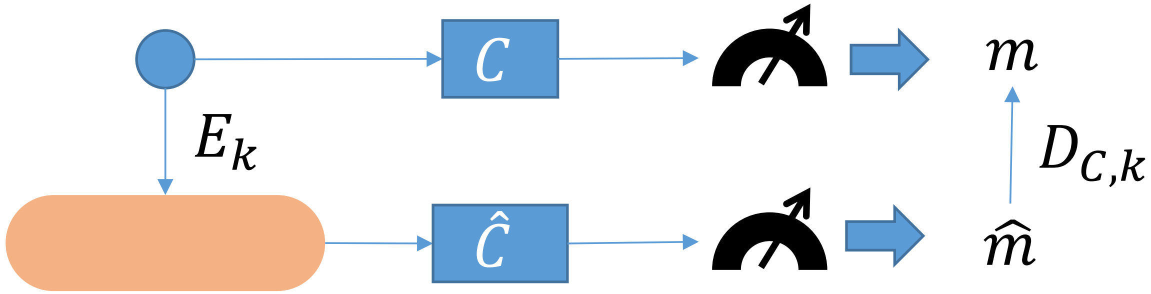
Build quantum tool I: a new encoding scheme



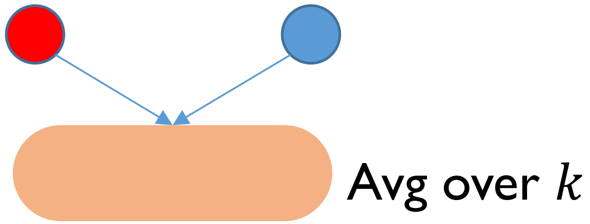
* Based on quantum error correcting & (trap) quantum auth. scheme [BGS12]

- Augmented trap scheme*, simultaneously supporting

i. Clifford circuits $\mathcal{C}$ & measure, transversally ("somewhat" homomorphic)



ii. Perfect* secrecy



* Need no computational assumptions

iii. **Authentication**

- Dishonest behavior can be detected

- But: verification of existing QMA-complete problems require more than $\mathcal{C}$(simple, non-universal)

Build quantum tool II: a new QMA-complete problem

- Local Clifford-Hamiltonian (**LCH**) Problem

Input: Hamiltonian $H_1, \ldots H_m,$ each H_j on 5 qubits & of form $C_j|0\rangle\langle 0|C_j^*$

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

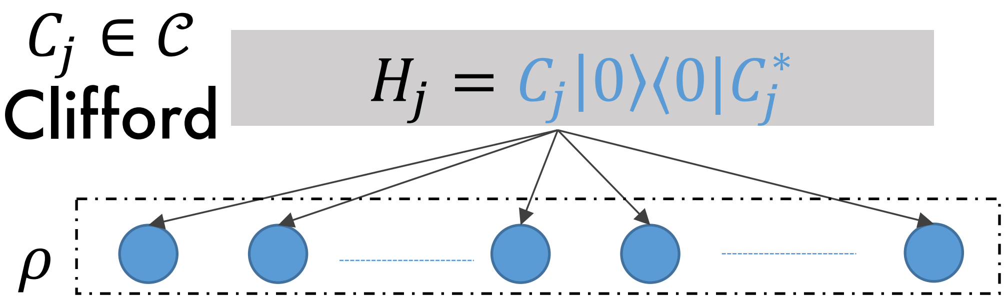
Theorem: LCH is QMA-Complete

→ QMA = QMA[Clifford verifier]
= QMA[single qubit measurement]

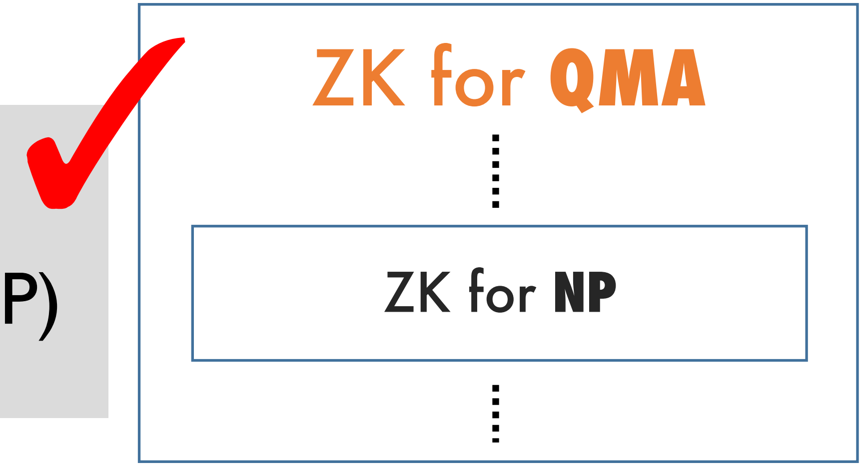
Verification circuit

- Pick small random part of witness
- Apply Clifford $C \in \mathcal{C}$ & measure:
  - non-zero string → accept

Can run **Verification** on *encoded* witness (by AugTrap) transversally



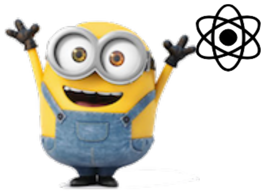
Reductionist's wishful thinking:
reduce (ZK for QMA) to (ZK for NP)



ZK proof system for LCH

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

Witness $|w\rangle$



1

AugTrap Enc w. key k — $|w\rangle$

Committing k — k

2

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

$j, \hat{m}_j$

3

Check $\hat{m}_j$ & H_j consistent (i.e. verifier seemed honest)

5

Invoke quantum-secure ZK proof for NP

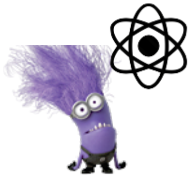
a. $\exists k$ consistent with commit

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

Our ZK protocol for LCH works

- Completeness: ✔
- Soundness: ✔
  - Full proof non-trivial, relying on error correcting code & binding of commit
- Zero-knowledge: for any malicious verifier

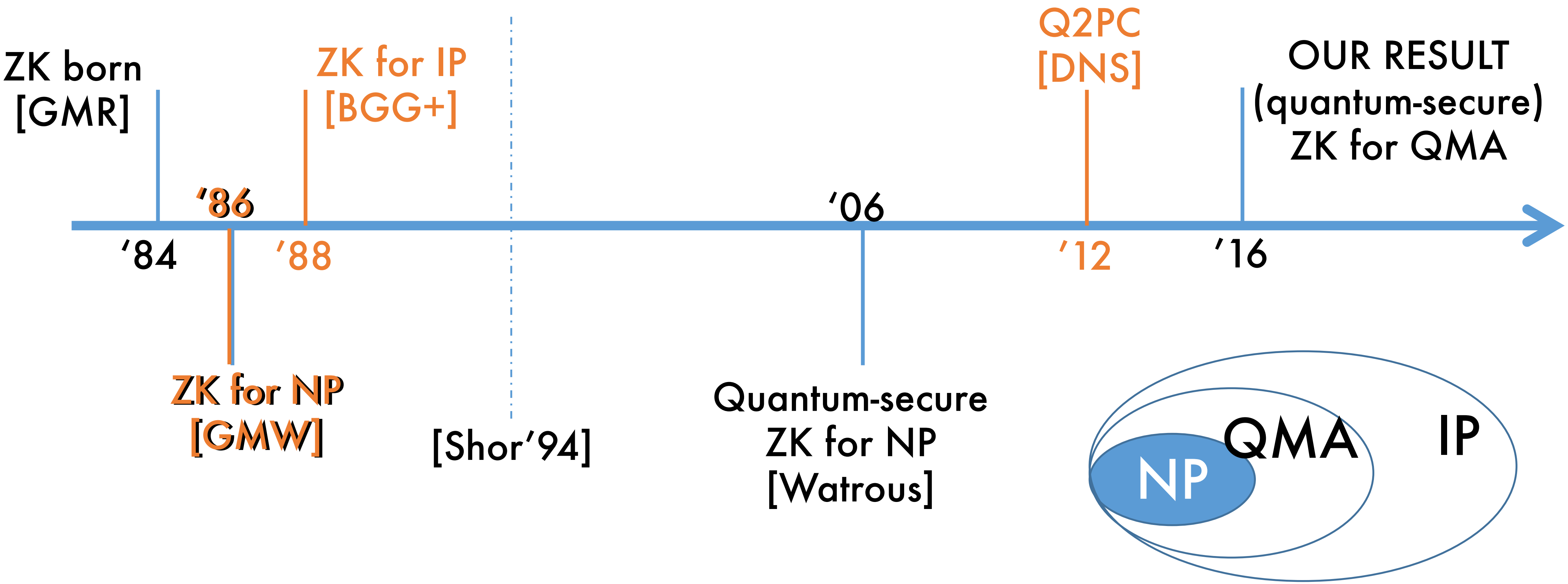


$E_k(|w\rangle)$ + k Can be viewed as hybrid encryption of $|w\rangle$

  - Verifier's measurement produces classical **encrypted** msg
  - "Leakage" **resilient**: acc/rej in step 3 may leak info. about k_j
    - k_j doesn't compromise secrecy on remaining qubits

Corollary: any problem in QMA has a ZK proof system

Timeline in retrospect: alternate approaches?



Comparison

	GMW analogue[1]	ZK for IP[1] w. Q-Security	Q2PC[1]	Our protocol
All QMA	✗	✔	✔	✔
Prover efficiency	✔	✗	✔	✔
Mild assumption[2]	✔	✔	✗	✔
Round #	✔	✗	✗[3]	✔
Availability	✔	✔✔[4]	✗	✔

1. plausible, but needs double-check; 2. commitment vs. dense PKE
3. depends on V's ckt; 4. purely classical

Concluding Remarks

Every QMA problem has a "nice" zero-knowledge proof system

New tools for quantum crypto & quantum complexity theory

- QMA complete: local Clifford Hamiltonian Problem
- Augmented Trap encoding scheme

- Future directions

1. ZK for QMA

- purely classical protocol (w. efficient prover)?
- constant-round (CR) w. negl. soundness error:
  - CRZK for NP (Q-Security unknown) ➔ CRZK for QMA

2. Proof of *quantum* knowledge?

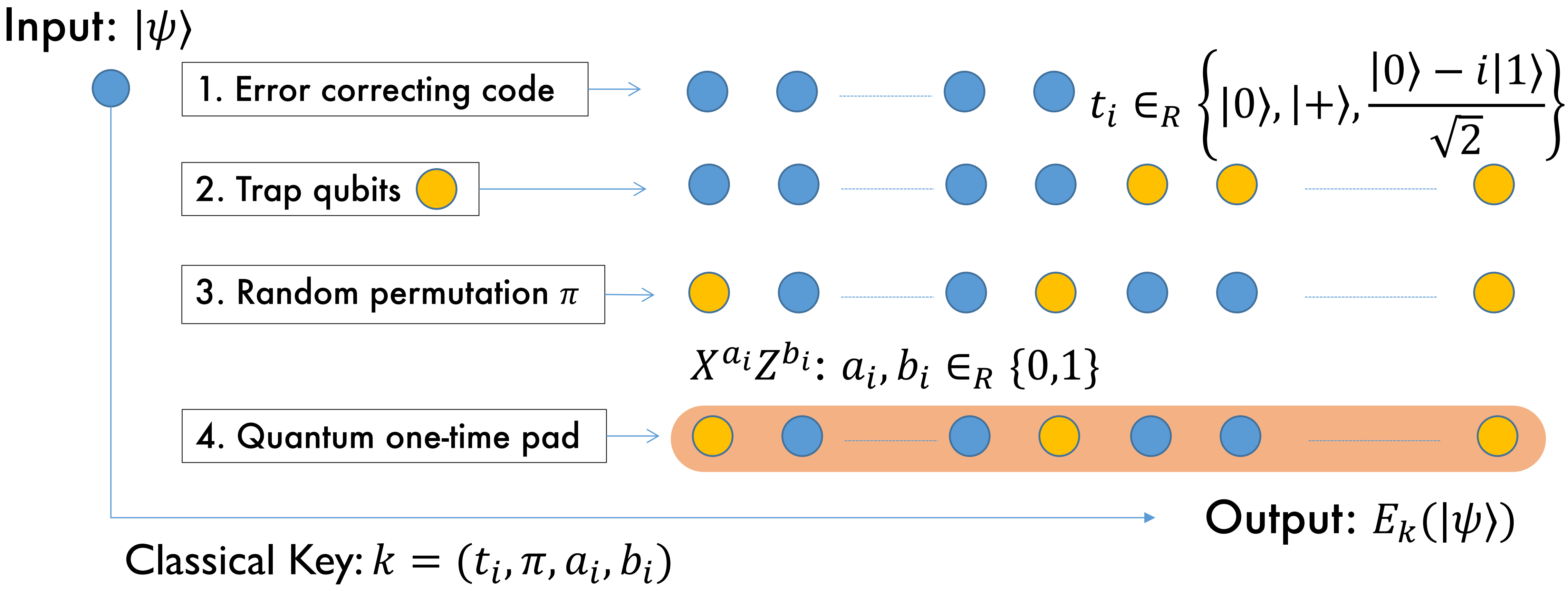
3. QPIP

- verifying a quantum computer by a classical computer?

Thank you!

Supplement materials

Augmented Trap Scheme



LCH: Proof sketch and implications

- It's (almost) there in Kitaev's proof:

$\boldsymbol{V}$ for an arb. QMA problem	→	$\boldsymbol{H} = H_{in} + H_{out} + H_{clock} + H_{prop}$

$$H_{prop,t} = \cdots = |10\rangle\langle 10|_{t-1,t+1} \otimes \frac{1}{2}[I_t \otimes I - |1\rangle\langle 0|_t \otimes U_t - |0\rangle\langle 1|_t \otimes U_t^*]$$

A universal gate set $\{\Lambda(P), H\}$: ☹

Instead, assume $U_t \in \{\Lambda(P), H \otimes H\}$

Ex. $\frac{1}{2}[I_t \otimes I - |1\rangle\langle 0|_t \otimes \boldsymbol{\Lambda(P)} - |0\rangle\langle 1|_t \otimes \boldsymbol{\Lambda(P)}^*]$

$= (ZH \otimes I \otimes I)|000\rangle + (ZH \otimes I \otimes X)|000\rangle$

$+ (ZH \otimes X \otimes I)|000\rangle + (P^*H \otimes X \otimes X)|000\rangle$

⇓

QMA = QMA with Clifford verifier

QMA = QMA with single qubit measurement

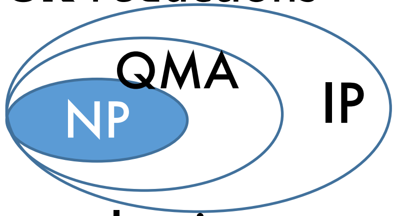
Simper proof than [MNS'16]

Alternate approaches?

- Mimicking GMW 3-Coloring protocol?
  - ☺ • A candidate: local-consistency problem [Liu05]
  - ☹ • But, does NOT give ZK for all QMA problem
    - Local-consistency was proven QMA-complete only under **Cook** reductions

Known QMA-complete problems **NOT** as fit …

- Making ZK for IP [BGG+88] quantum secure?
  - ☺ • Plausible w. comparable assumption
    - • Purely classical protocol
  - ☹ • Prover not poly-time
    - • Round complexity large



- Invoking secure quantum 2-party computation [DNS12]?
  - ☹ • Only sound against poly-time prover (i.e. argument system)
    - • Comm. inherently quantum, round # depends on Ver circuit
    - • Much stronger assumptions: quantum secure dense PKE