

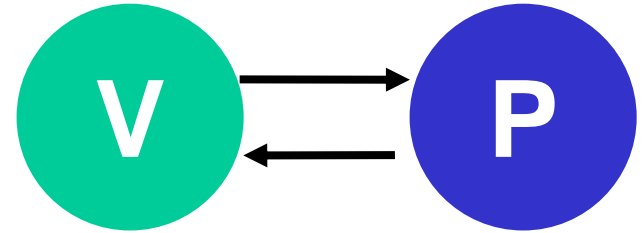
Some new results on quantum interactive proof systems

TQC 2006 February 22-23, 2006
NTT R&D Center, Atsugi, Kanagawa, Japan
Workshop on Theory of Quantum Computation, Communication, and Cryptography



K. G. Matsumoto
NII, JST

(Quantum) Interactive Proof System



- Want to solve {Yes No} question

- **Prover**

always asserts **Yes**, even if **No** is the case

can do **any unitary**

- **Verifier**

checks **P**'s assertion via interaction with high probability.

can do (quantum) **polynomial time** computation

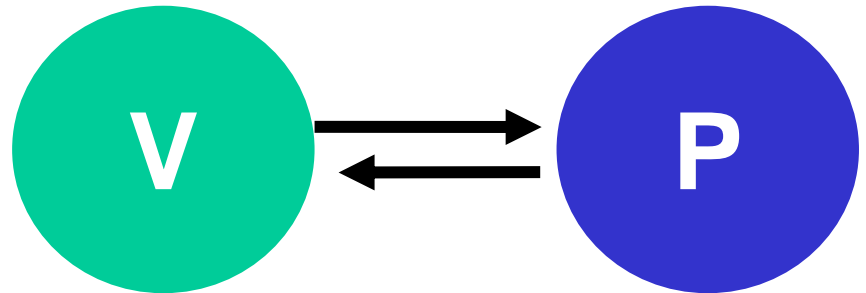
Easy question to solve is easy to verify, and hard question is hard to verify

Why important?

Many problems are related

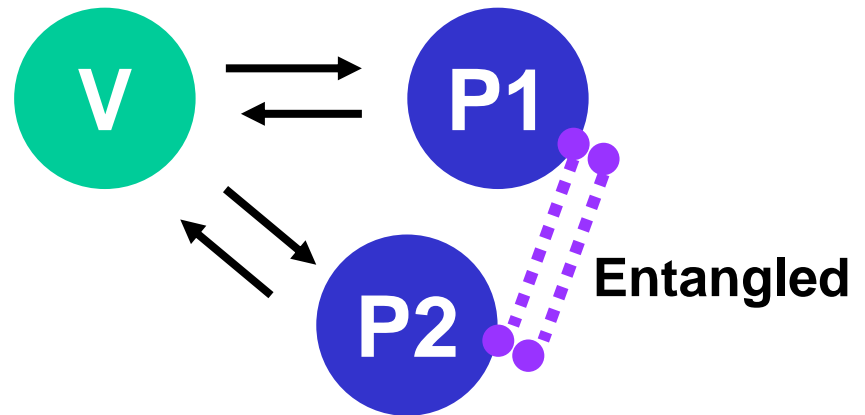
1. Cryptography
2. Inapproximability of certain optimization problems (e.g. max-3sat, creek, etc)
3. Locally decodable/testable code

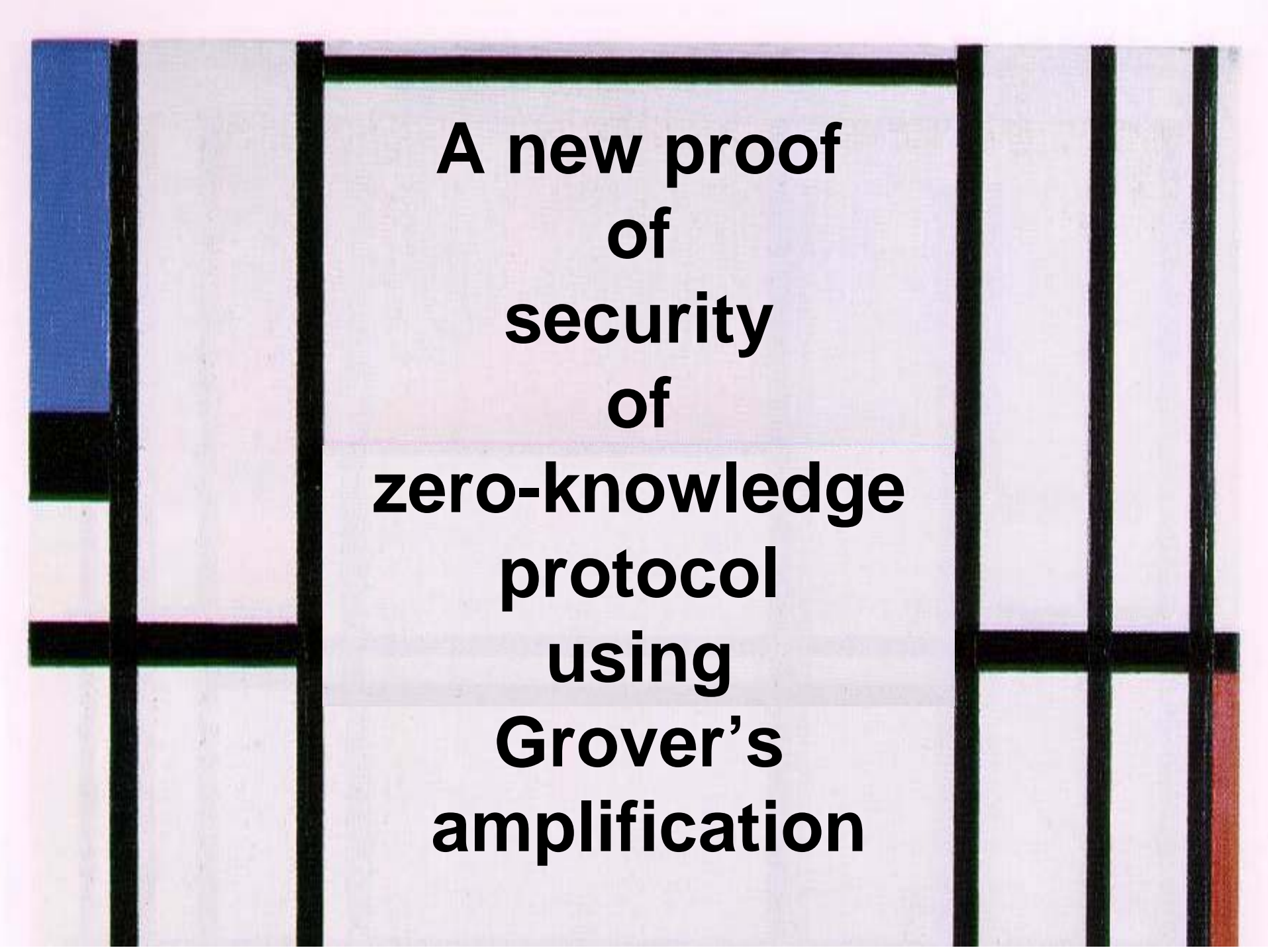
etc



The topics of this talk

- **Zero-knowledge property**
 - **V** learn nothing beyond verification
 - Can classical definition generalize to quantum honestly ? (no-cloning)
- **Multi-prover** proof systems and entanglement

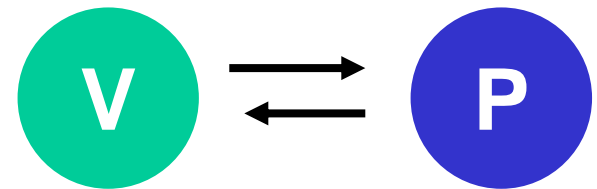




**A new proof
of
security
of
zero-knowledge
protocol
using
Grover's
amplification**

Zero-knowledge property

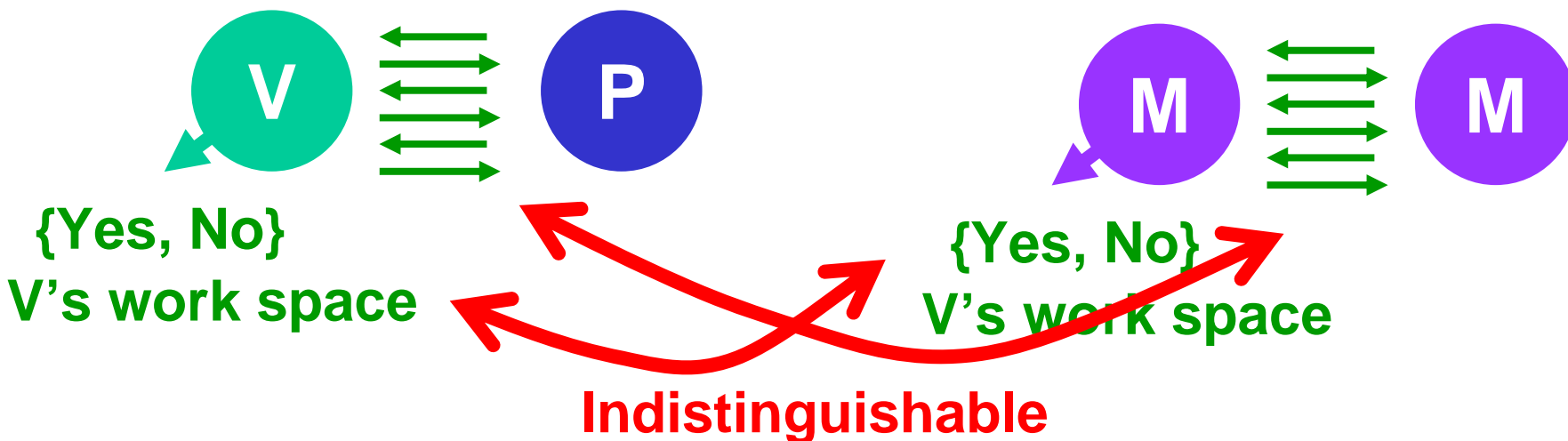
- Any **V** learns **nothing beyond verification** if **P** is honest
- **Applications**: An important **building block**
 1. Identification
 2. Enhancement of security of PKC
 3. Verifiable secret sharing
 4. Electric voting
etc



Definition of Zero-knowledge

If **P** is honest and the input is **Yes** instance,
 \exists **M**: poly time, without communication with
P which simulates

1. communications between **P** & **V**
2. **V**'s output



The Talk will be organized as follows

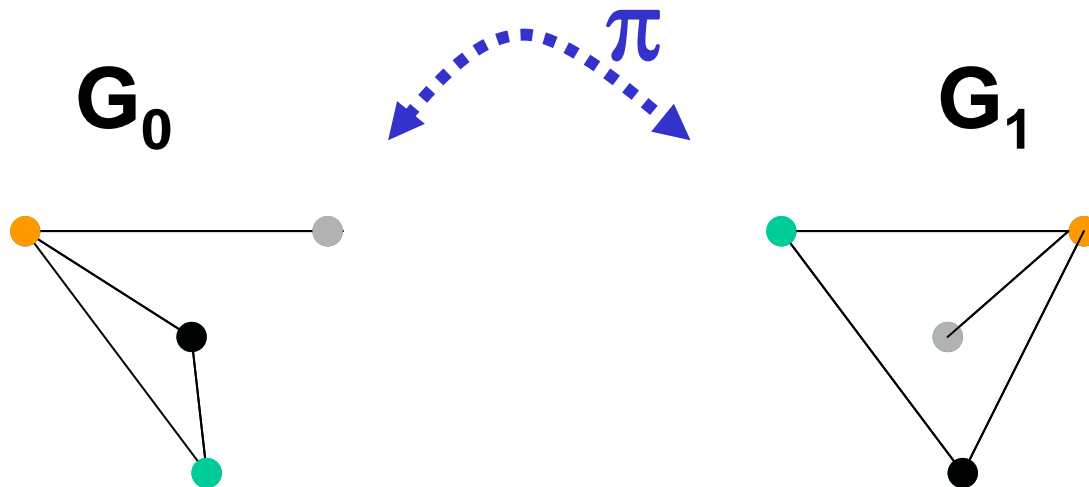
Concentrate on **Graph Isomorphism (GI)**.
The similar argument applies to other cases.

1. Classical protocol and simulator
2. Difficulty in quantum case
3. How to overcome

Graph Isomorphism (GI)

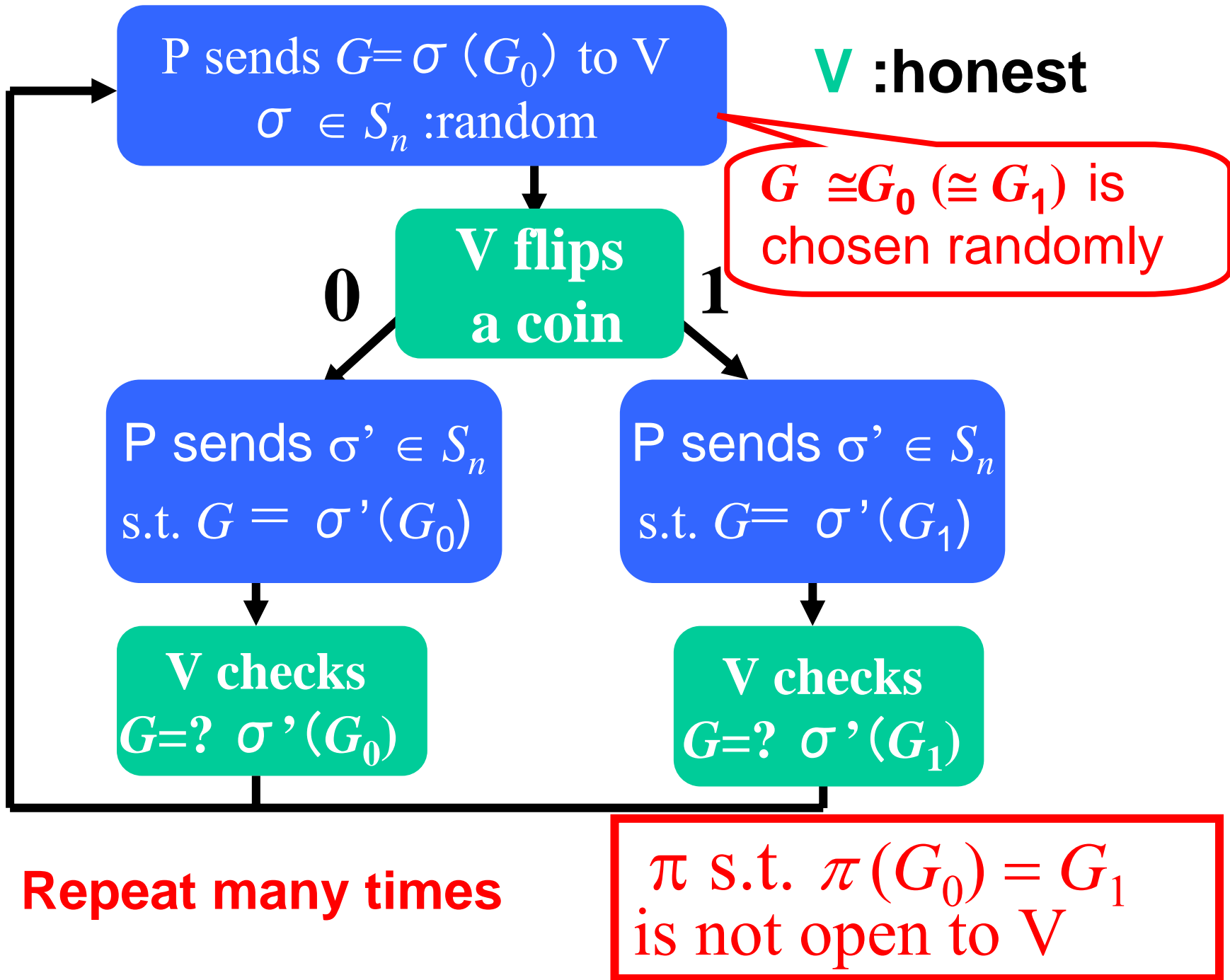
INPUT: A graph G_0 and G_1 with n vertices

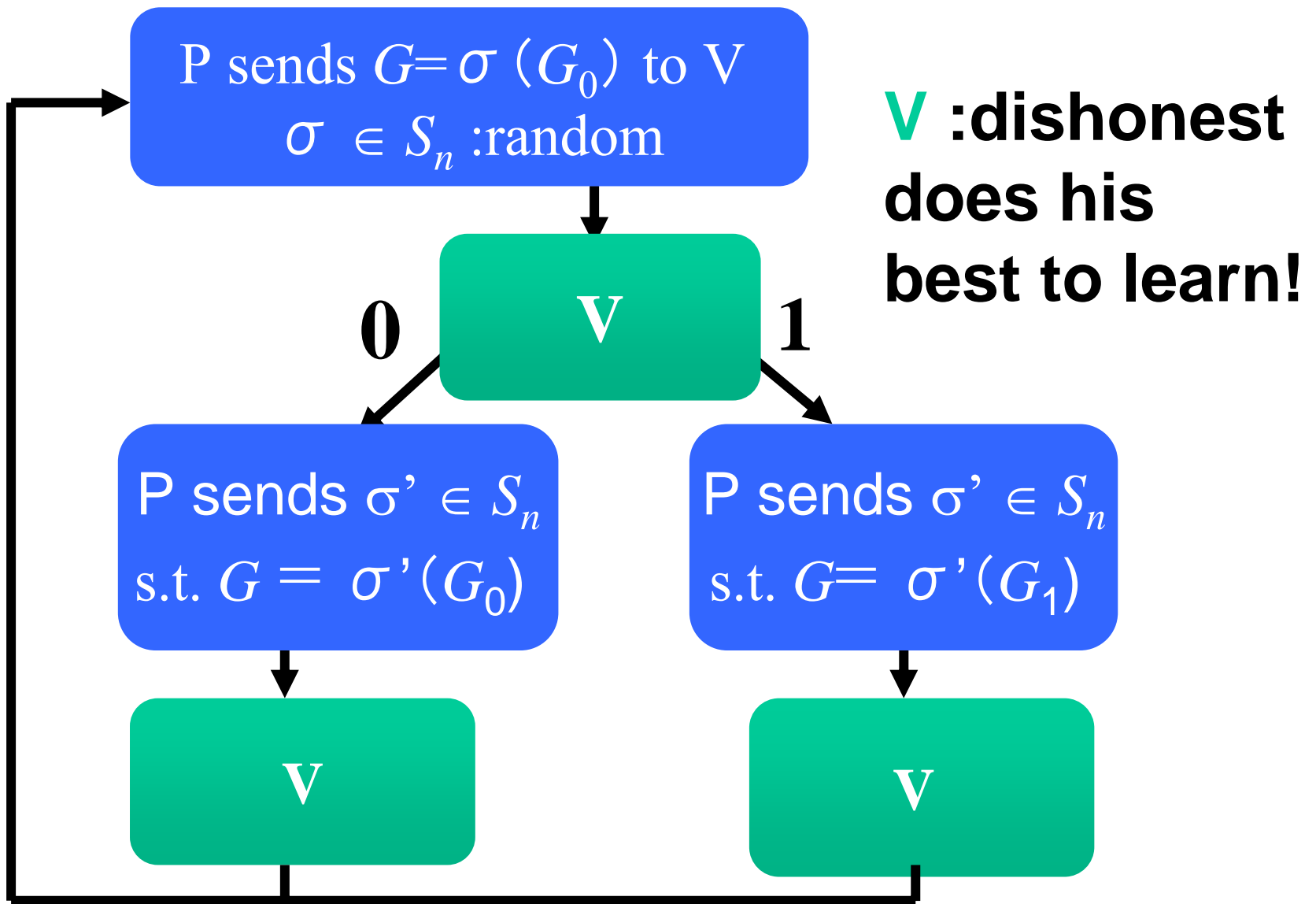
QUESTION: Is there any permutation $\pi \in S_n$ on vertices, s.t. $\pi(G_0) = G_1$?



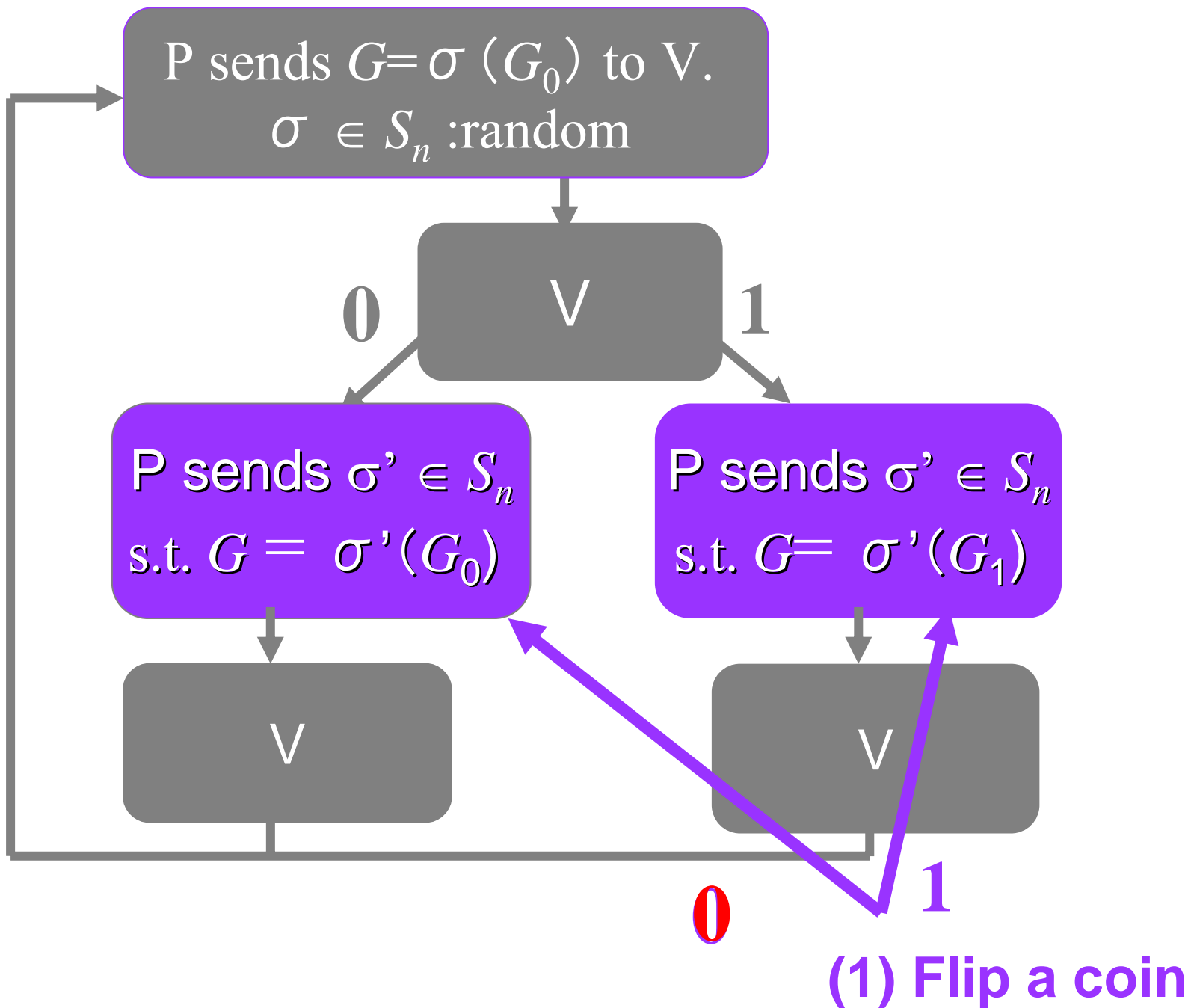
A protocol (GMW)

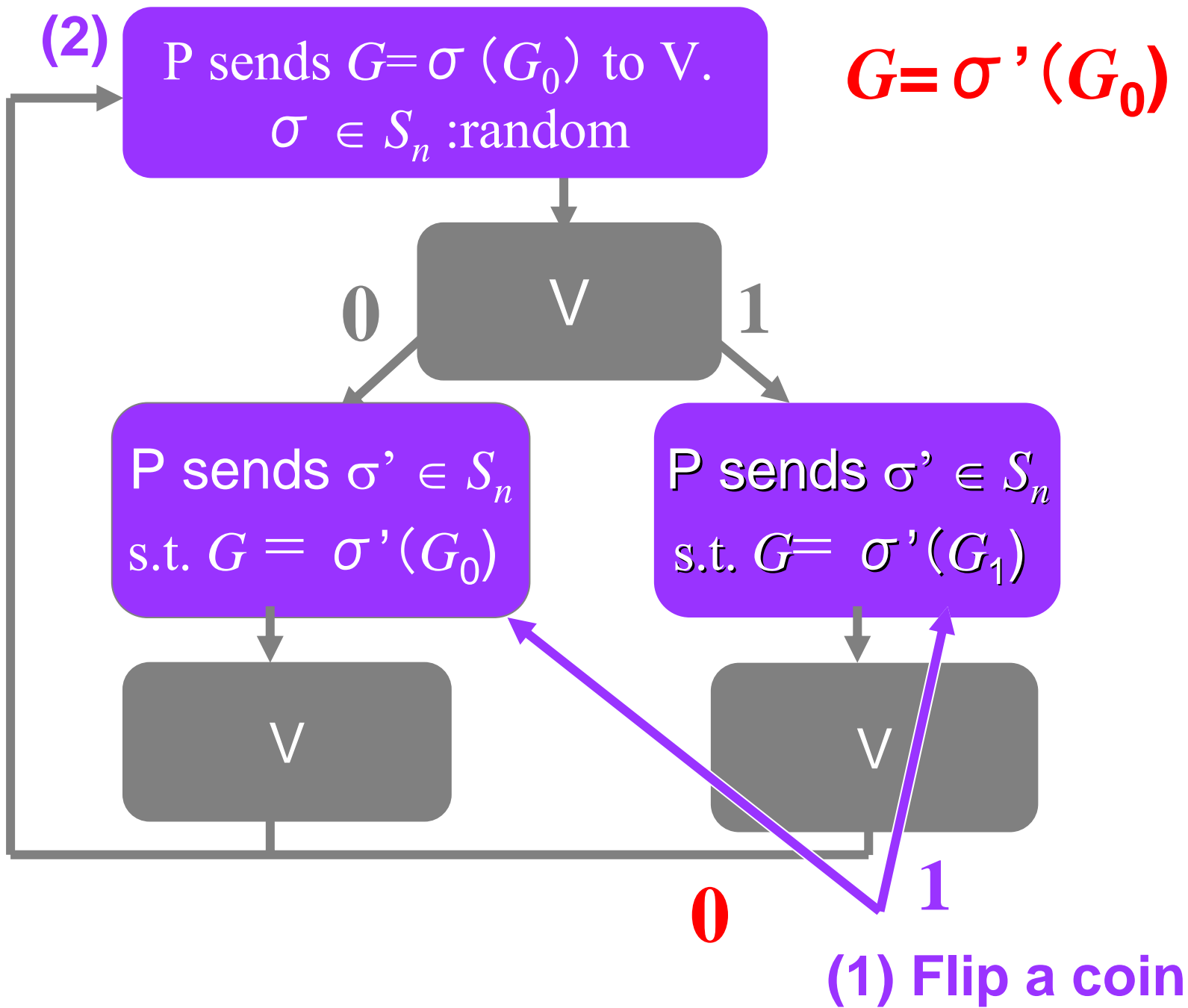
- Checks false statement with prob. $\frac{1}{2}$ for single iteration
- Many iterations for high prob. of check.
- Does not leak any extra information to **V**

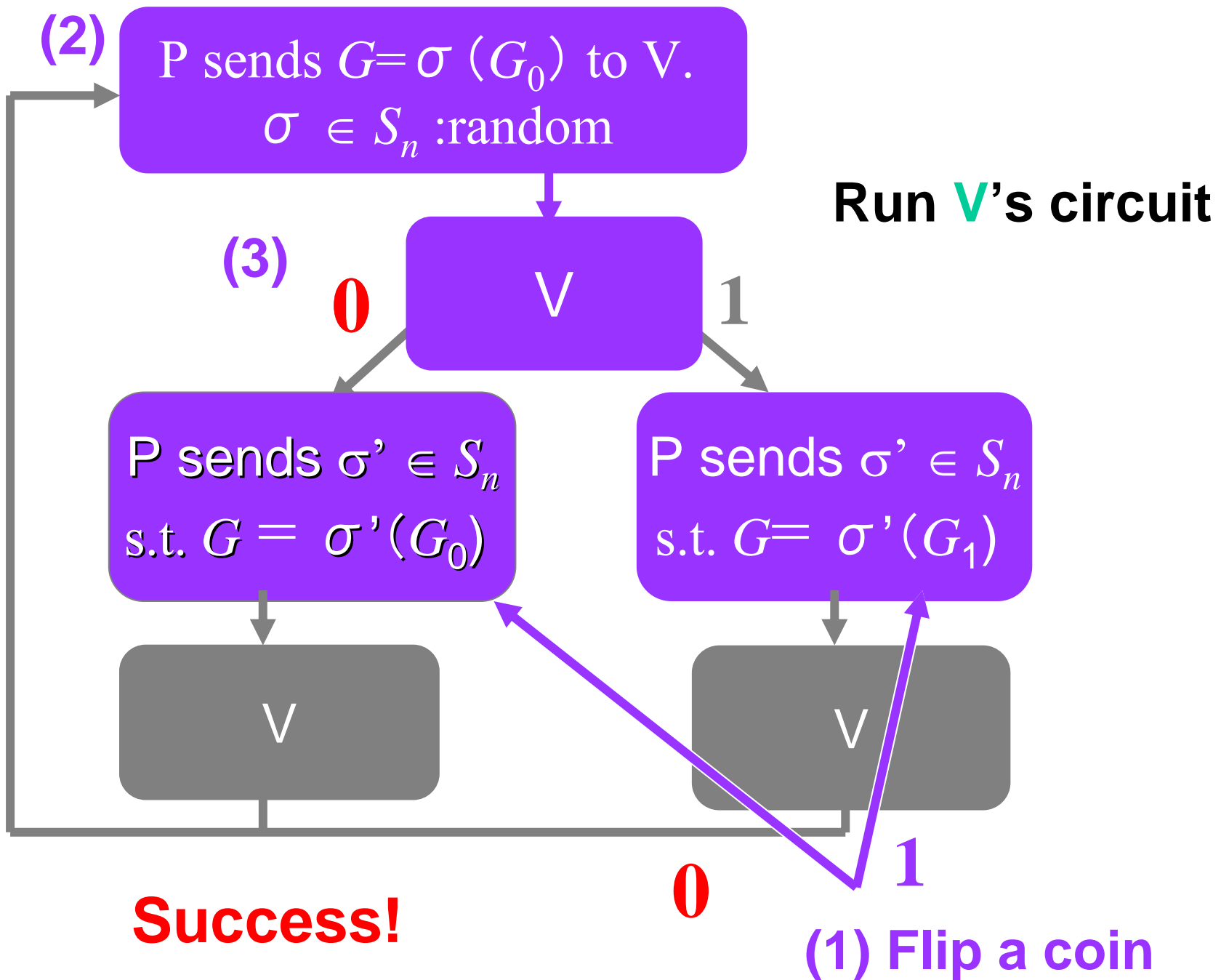


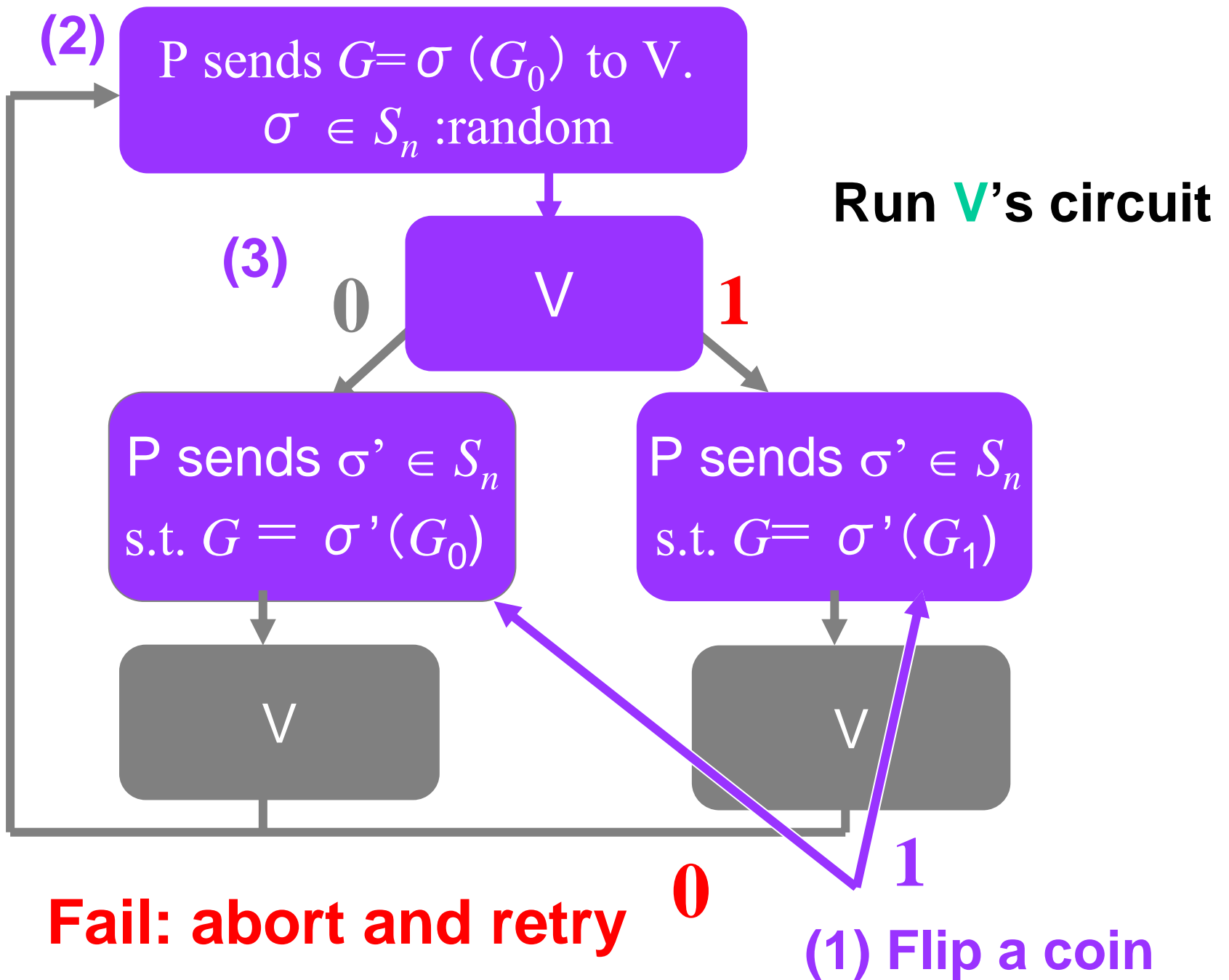


V cannot learn beyond verification, for the interaction can be simulated in polynomial time

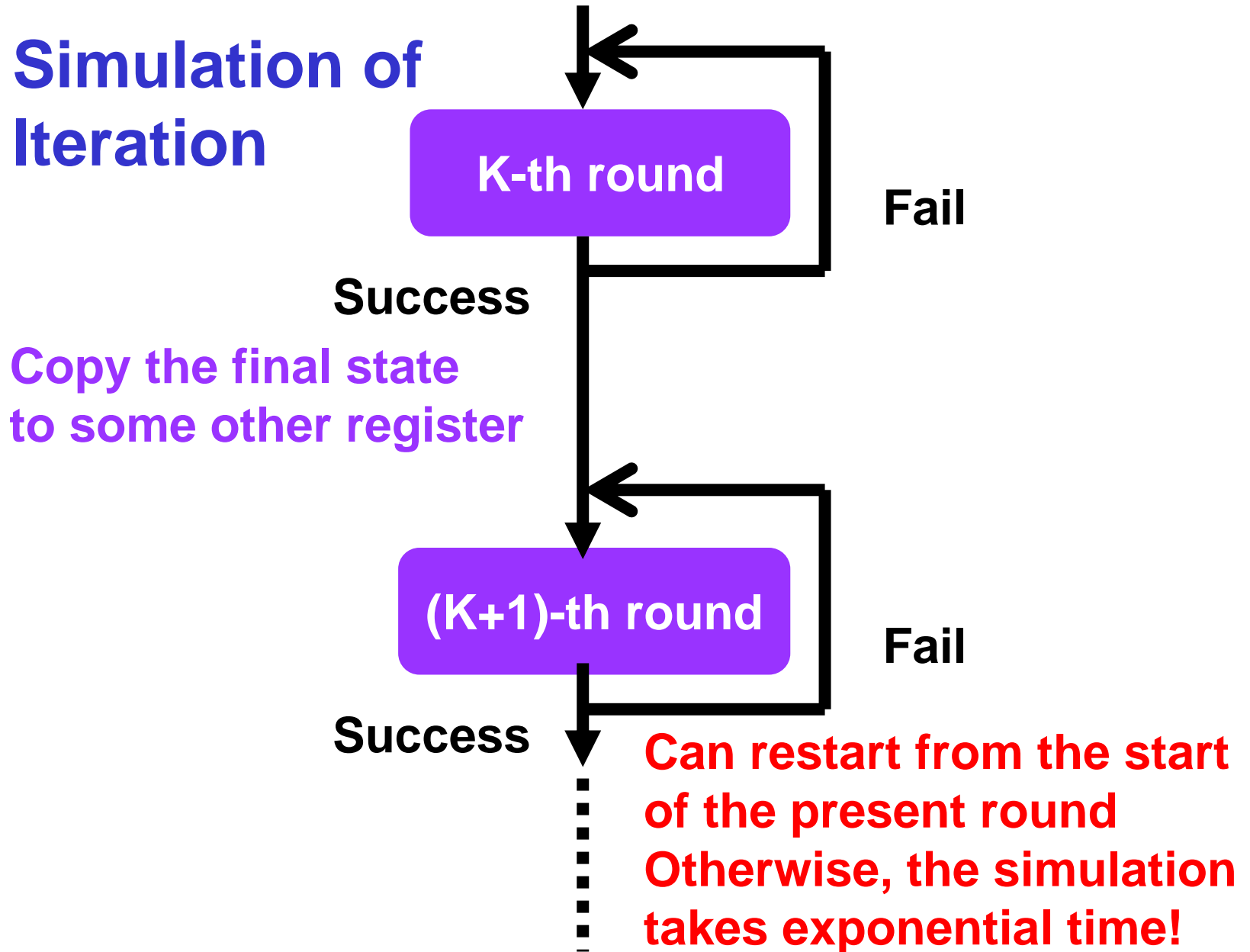






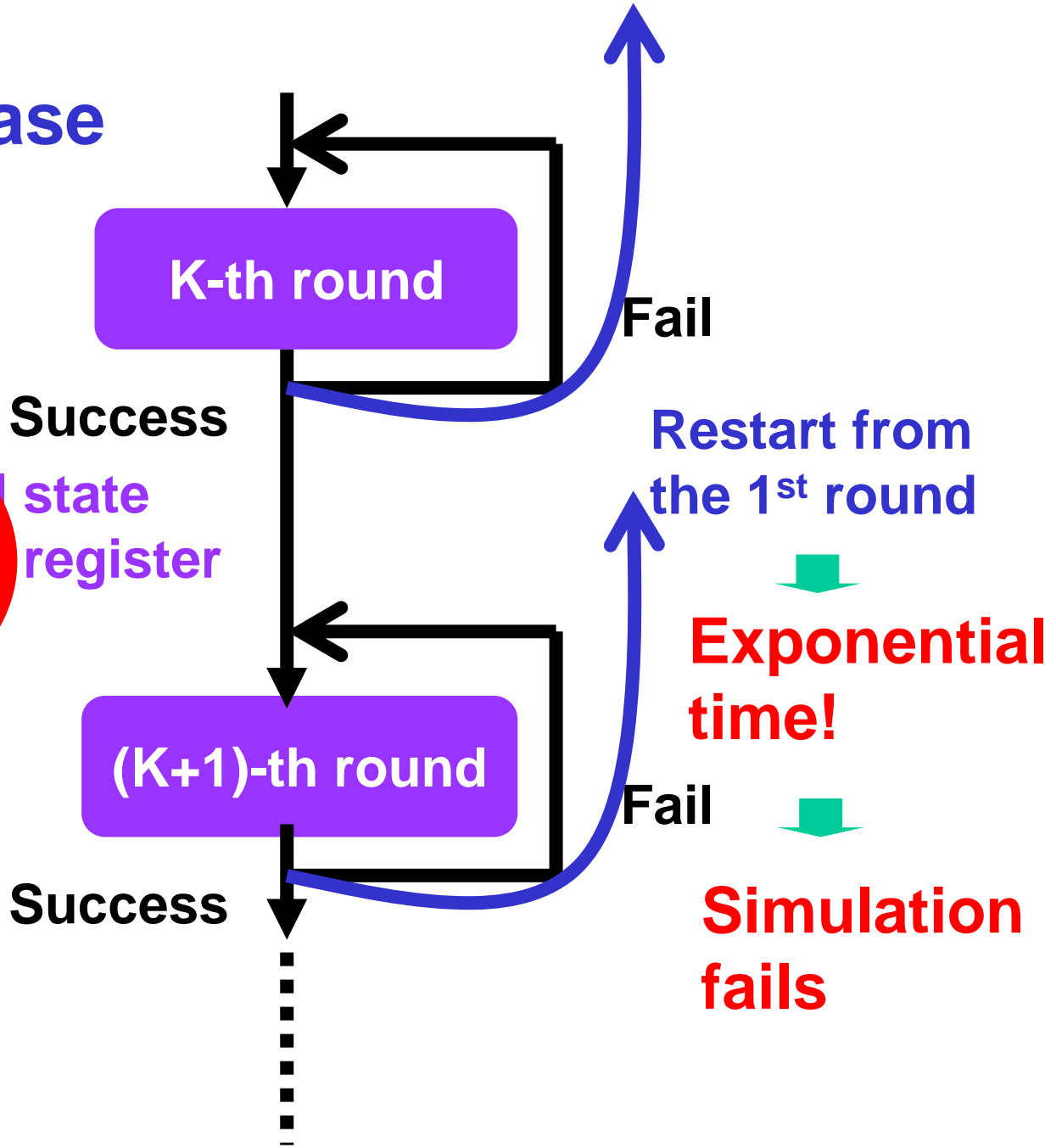


Simulation of Iteration



Quantum case

~~Copy the final state to some other register~~



This means ...

- **No easy proof** for the zero-knowledge against quantum **V**
- Some possibilities had been discussed.
 1. Security proof using **new technique**
 2. Security proof based on **new def.** of zero-knowledge
 3. The protocol is **insecure** against quantum attack

How to bypass the difficulty

- **[Watrous2005]**: Recover from failure. technique developed for QMA.

Use special tool. No intuitive picture

- **[This talk]**: Use Grover's amplification to make failure probability 0.

Use common tool. Intuitive picture

Grover's amplitude amplification

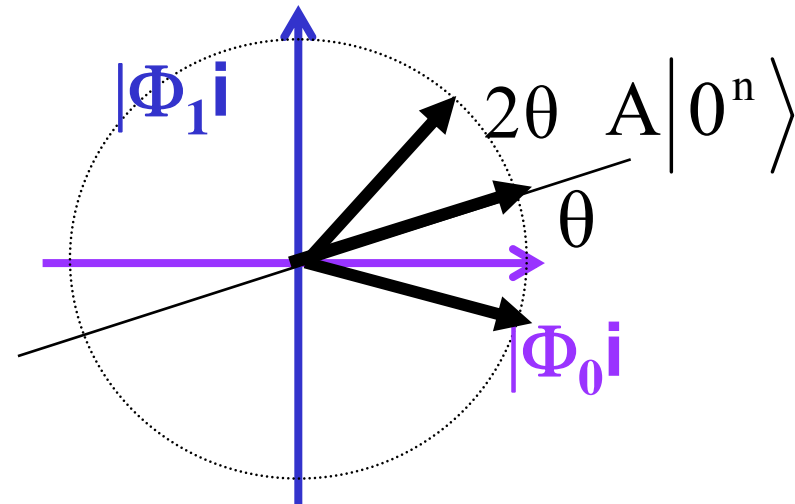
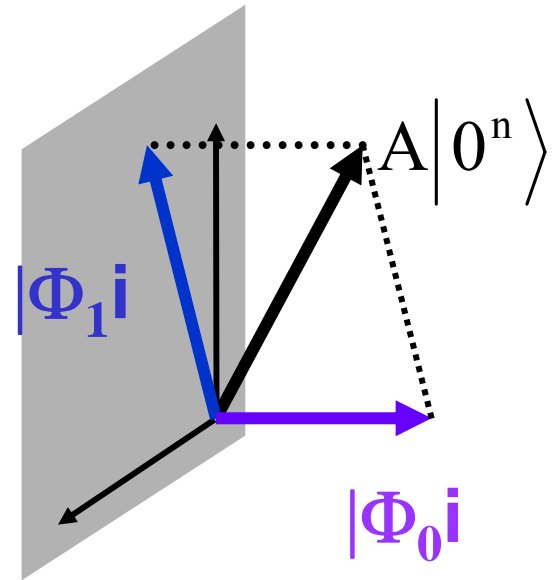
$$f|\phi\rangle; \Pi|\phi\rangle = |\phi\rangle$$

$$Q = -AS_0A^{-1}S_1$$

$$S_1 : |\phi\rangle \rightarrow \begin{cases} -|\phi\rangle & (\Pi|\phi\rangle = |\phi\rangle) \\ |\phi\rangle & \text{otherwise} \end{cases}$$

$$AS_0A^{-1} : A|0\rangle \rightarrow -A|0\rangle$$

$$A|x\rangle \rightarrow A|x\rangle, x \neq 0$$



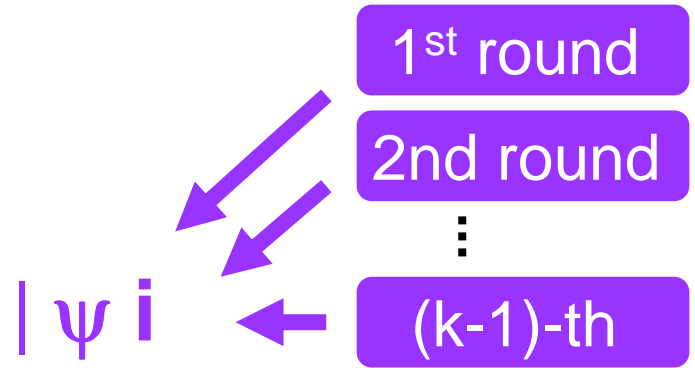
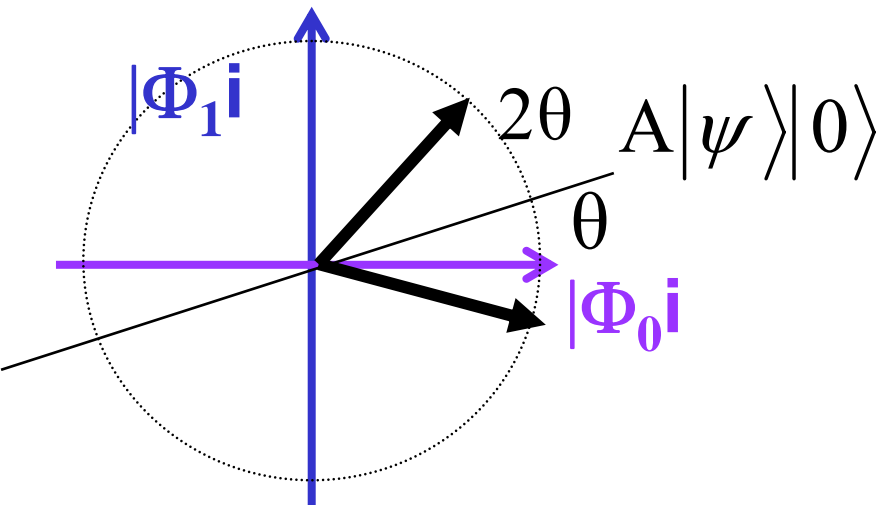
In our case ...

- **A** : the classical simulator
- **Π** : the projection to check whether the coin flip and the output of **V** matches. (Simulation succeeds or not)
- By Grover amplification, **$|\Phi_1\rangle$** is obtained, and this means 100 % success of simulation.
- However, 2 difficulties.

Difficulties and Solutions (1)

- The initial state: $|\psi\rangle|0\rangle$,
- How to construct the reflection about

$$A|\psi\rangle|0\rangle?$$



$$S_0 : |\psi\rangle|0\rangle \rightarrow -|\psi\rangle|0\rangle$$

$$|\psi\rangle|x\rangle \rightarrow |\psi\rangle|x\rangle, x \neq 0$$

$$\forall |\psi\rangle$$

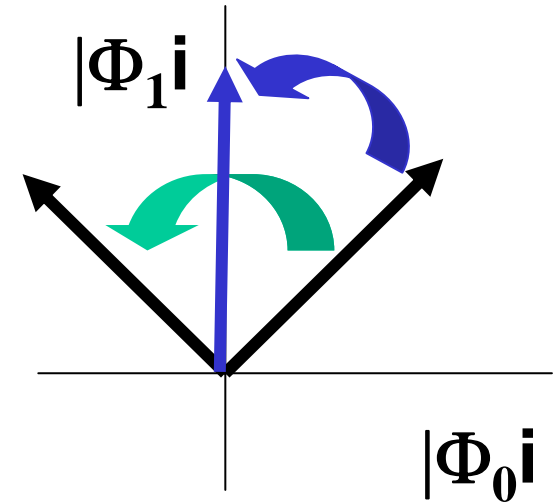
$-AS_0A^{-1}$ is the reflection

Key identity: $\langle 0|\Pi|0\rangle = I/2$

Success prob. is independent of $|\psi\rangle$

Difficulties and Solutions (2)

- Success prob. = 1/2. too big.
Rotate too much.



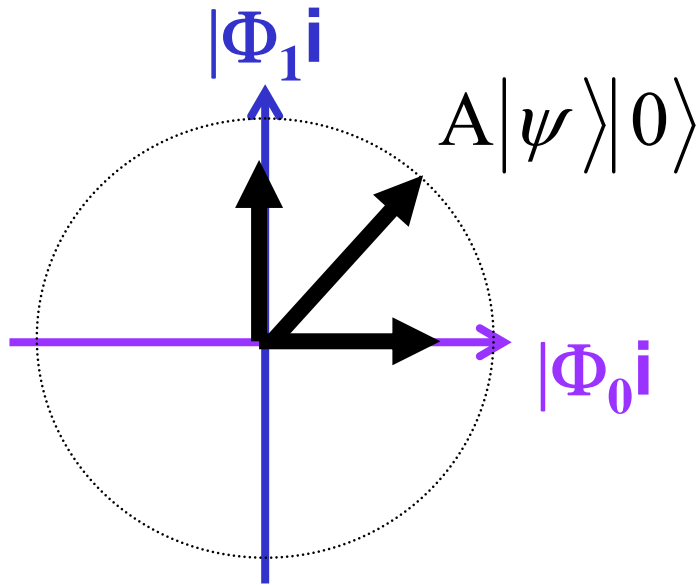
**Modify the phase factors
in S_0 , S_1 [BHT 98]**

$$S_0^i : |0\rangle \rightarrow i|0\rangle$$

$$|x\rangle \rightarrow |x\rangle, x \neq 0$$

$$S_1^i : |\phi\rangle \rightarrow \begin{cases} i|\phi\rangle \\ |\phi\rangle \end{cases} \quad (\Pi|\phi\rangle = |\phi\rangle) \\ \text{otherwise}$$

Another construction



1. A

2. Π

3. If succeed, done

4. If fail,

$$-AS_0A^{-1}$$

In fact, this is another expression
of the simulator in [Watrous2005]

Summary so far

- **A new proof** zero-knowledge against quantum verifiers. Uses a **common tool, Grover's amplification.**

([Watrous2005] uses a special amplification)

- **A new expression** of the simulator in [Watrous 2005]. in view of Grover's amplification

On amplification techniques

- **[Watrous2005]** If fail, recover
- **[this talk]** rotate to 100% success

c.f. Leader election problem:

- **[TKM2005:1]** If fail, recover
- **[TKM2005:2]** rotate to 100% success

In other problems ???

A decorative border surrounds the text, consisting of a thick black horizontal line at the top and bottom, and vertical black lines. Colored rectangular blocks are placed at the corners: a blue block at the top-left, a red block at the top-center, a red block at the top-right, and a yellow block at the bottom-right.

Multi-prover proof system and entanglement

Multi-prover proof systems

- **Provers**

all provers insists on a common proposition

can do any unitary

May share the entanglement and/or randomness

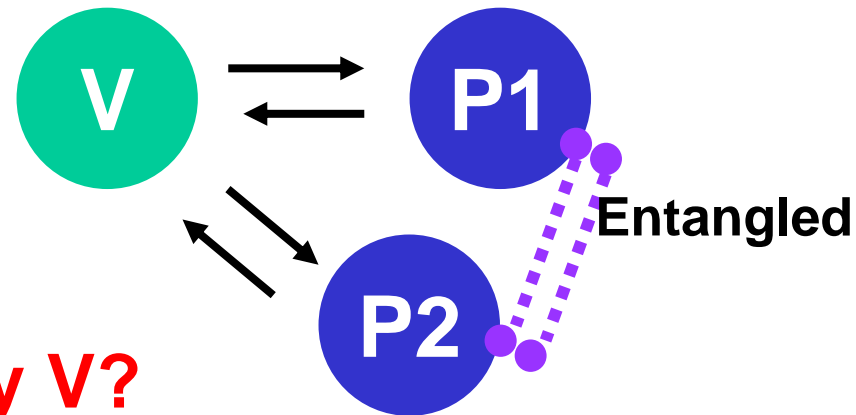
- **Verifier**

checks his assertion via interaction with high probability.

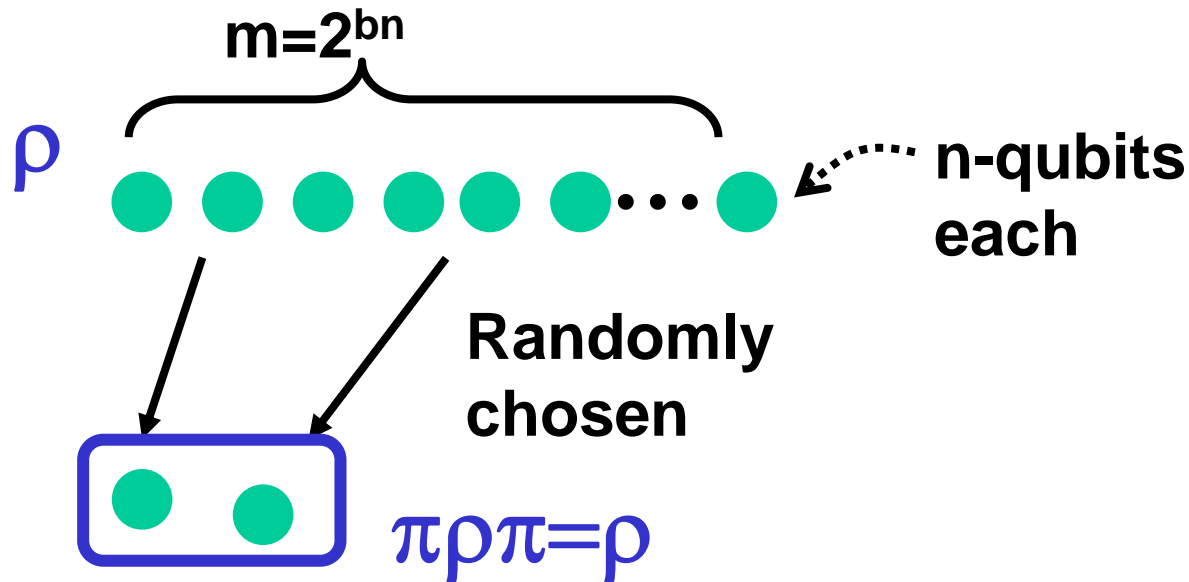
can do quantum polynomial time computation

[CHTW04] had shown that
Prior entanglement can cheat
the protocol which is secure
In classical case.

Any counter measure by V?



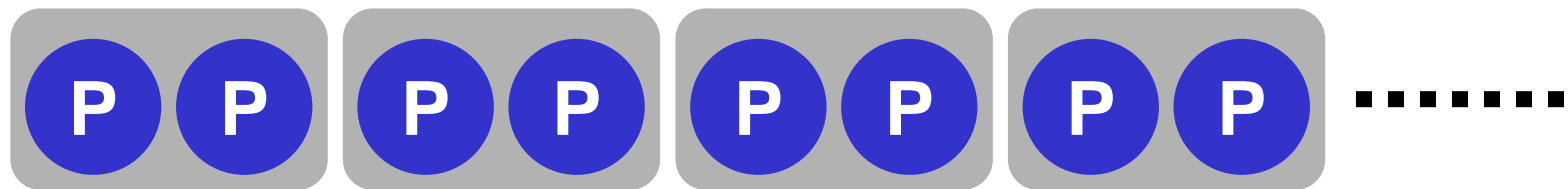
Quantum Definetti theorem: a symmetric state is almost separable [Rene 05][M 05]



Almost separable!

$$\min_{\{p_i, \sigma_i\}} \left\| \rho|_{\mathcal{H}_1 \otimes \mathcal{H}_2} - \sum_i p_i \sigma_i^{\otimes 2} \right\| = O\left(\sqrt{n} 2^{-\frac{b-1}{2}n}\right).$$

Symmetry can prohibit use of entanglement ??



Randomly
chosen

Almost separable
Due to Q-Defenetti

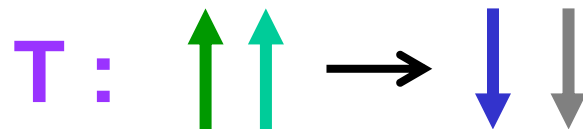
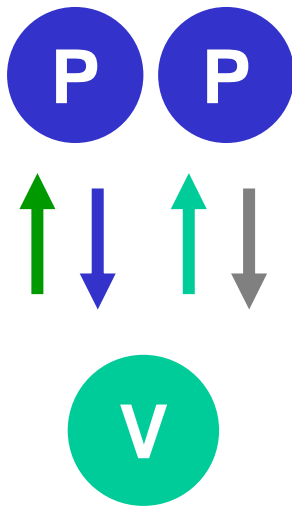
Implies no use of
entanglement?



No!

Why the argument does not apply?

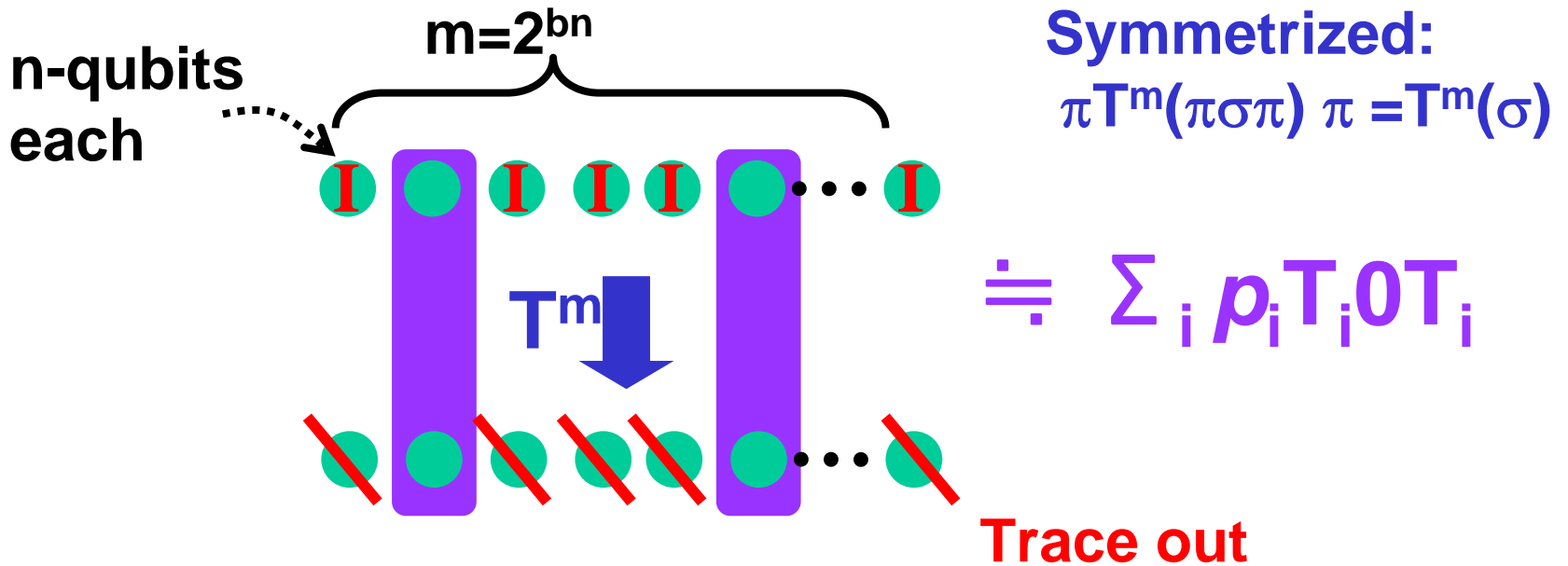
- In [CHTW04], messages are classical bits, (no entanglement between messages !) and still effect of prior entanglement.
- Have to see the mapping from $V \rightarrow P$ message to $P \rightarrow V$ message.



Is T separable ?

prob. mixture of T1 0T2 ?

Quantum Defenetti, channel version

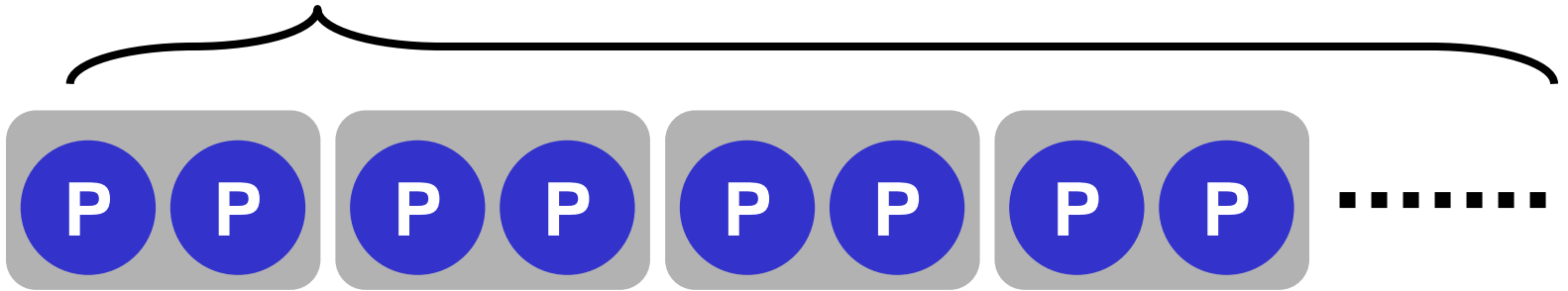


$$\min_{\{p_i, T_i\}} \max_{\sigma \in \mathcal{S}(\mathcal{H}_1 \otimes \mathcal{H}_2)} \left\| T^m \left(\sigma \otimes 2^{-n(m-2)} I \right) \Big|_{\mathcal{H}_1 \otimes \mathcal{H}_2} - \sum_i T_i^{\otimes 2}(\sigma) \right\| = O \left(n 2^{-(b-6)n} \right).$$

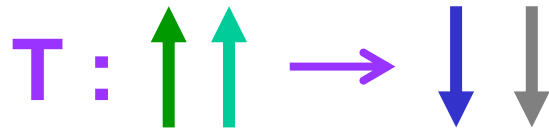
Proof: apply Q-Defenetti to Choi's representation $T^m \circ I$ (|max-ent.>)

Therefore...

$$m=2^{bn}$$



Randomly
chosen



is almost separable



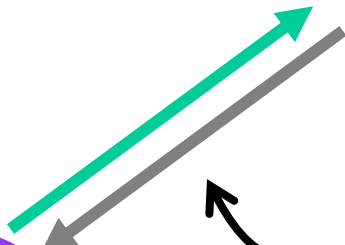
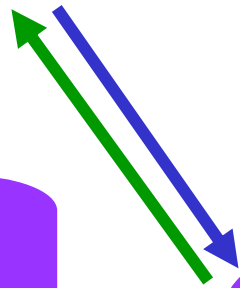
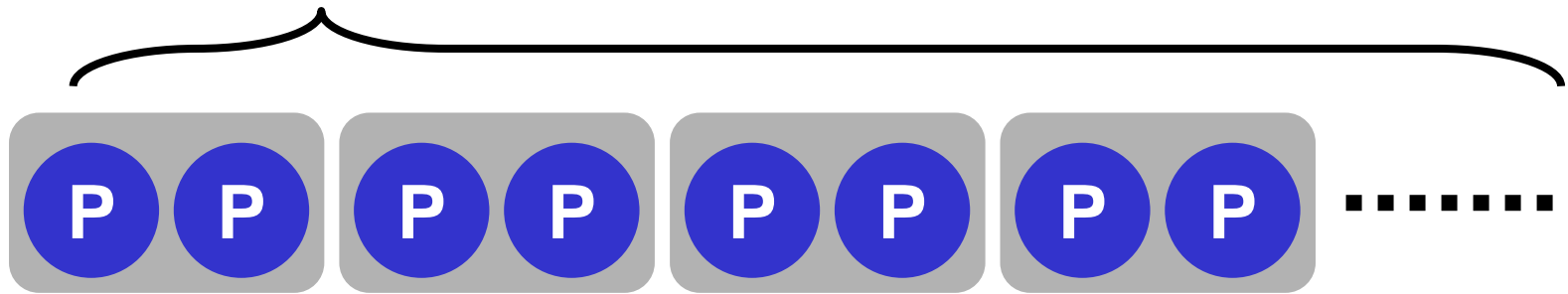
n-qubits

P cannot use entanglement !

**But V cannot keep communion channel
with 2^{bn} P's , for being poly-bounded.**

Hence, this doesn't work, but ...

$$m=2^{bn}$$

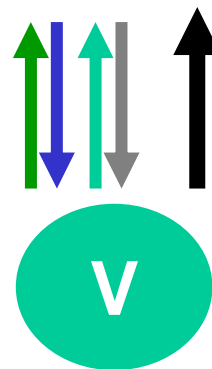


n-qubits

Oracle

mediate communication

This proof system can disable entanglement



bn bits to specify P's to communicate

Summary of the second part

- A **channel version** of quantum Defenetti
- Application to **QMIP**: prior entanglement is disabled with the help of **oracle**

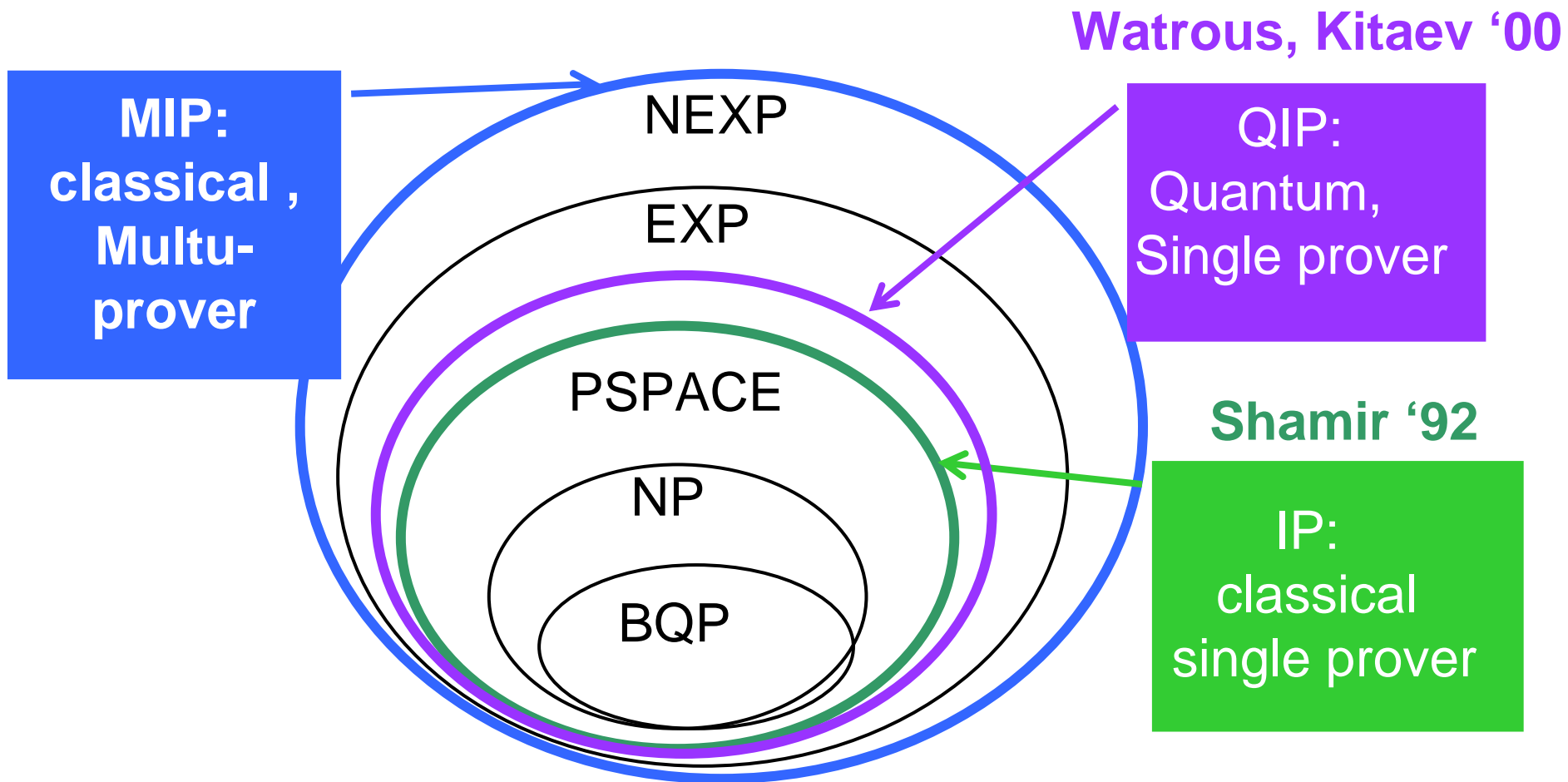
Open Problems

1. Any more applications of channel version of Q-Defenetti?
2. How to remove oracle?
3. Upper bound to the power of QMIP

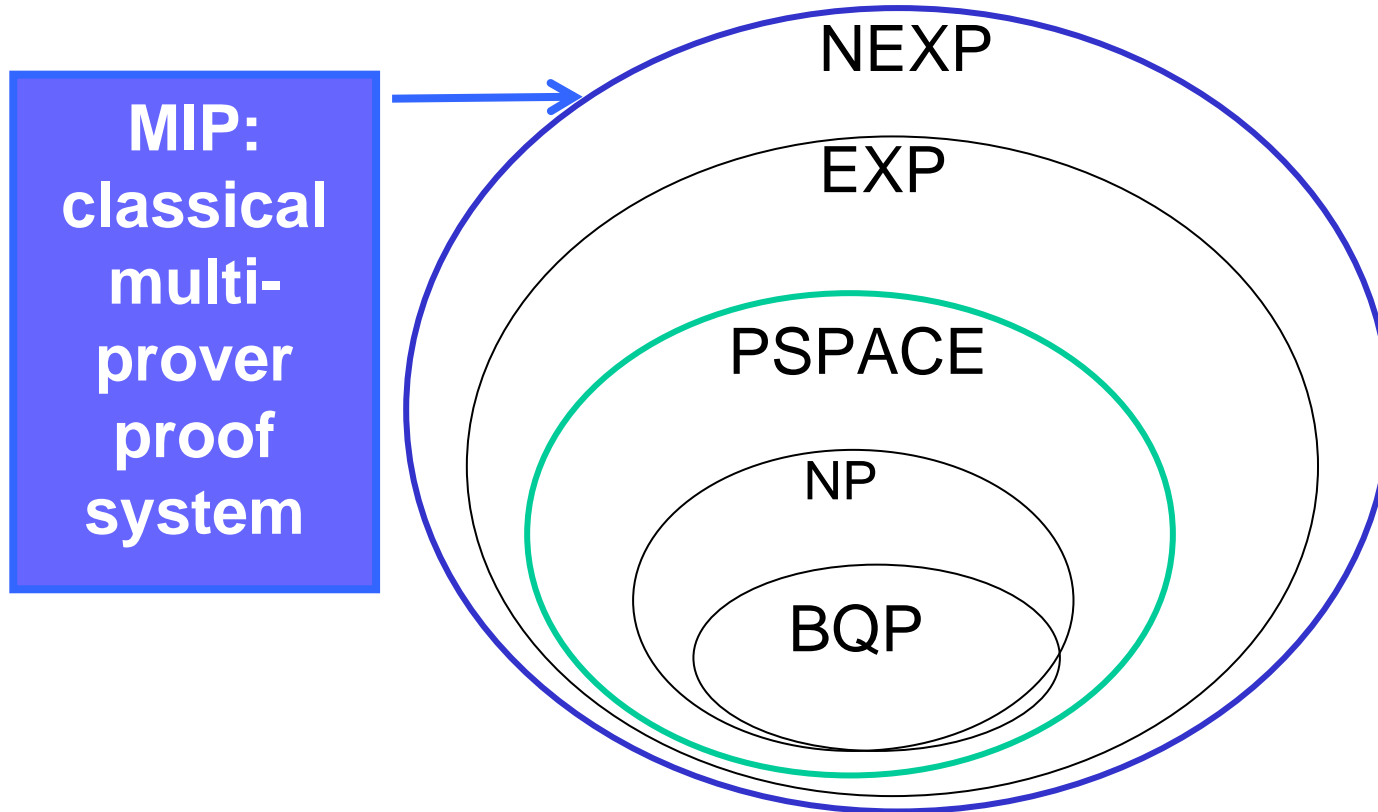
No signal

Power of proof systems

- Decision problem: the answer is {Yes, No}



Some key results



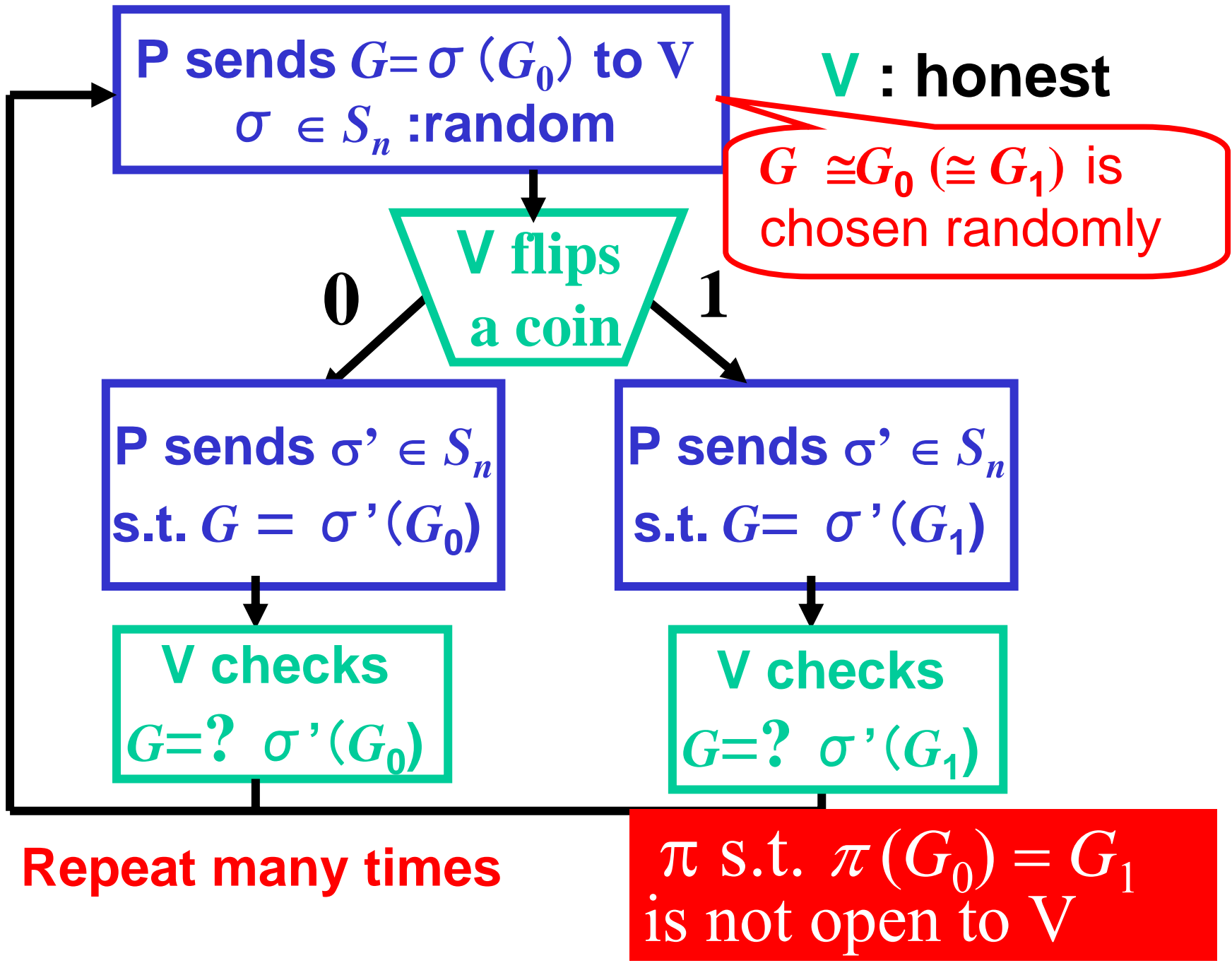
- Classical MIP with 2 **P**'s and 1-round communication ($\mathbf{V} \rightarrow \mathbf{P}, \mathbf{P} \rightarrow \mathbf{V}$) is enough to accept **NEXP**
- **Without** prior entanglement, **QMIP** system can accept **NEXP** [KM2003]

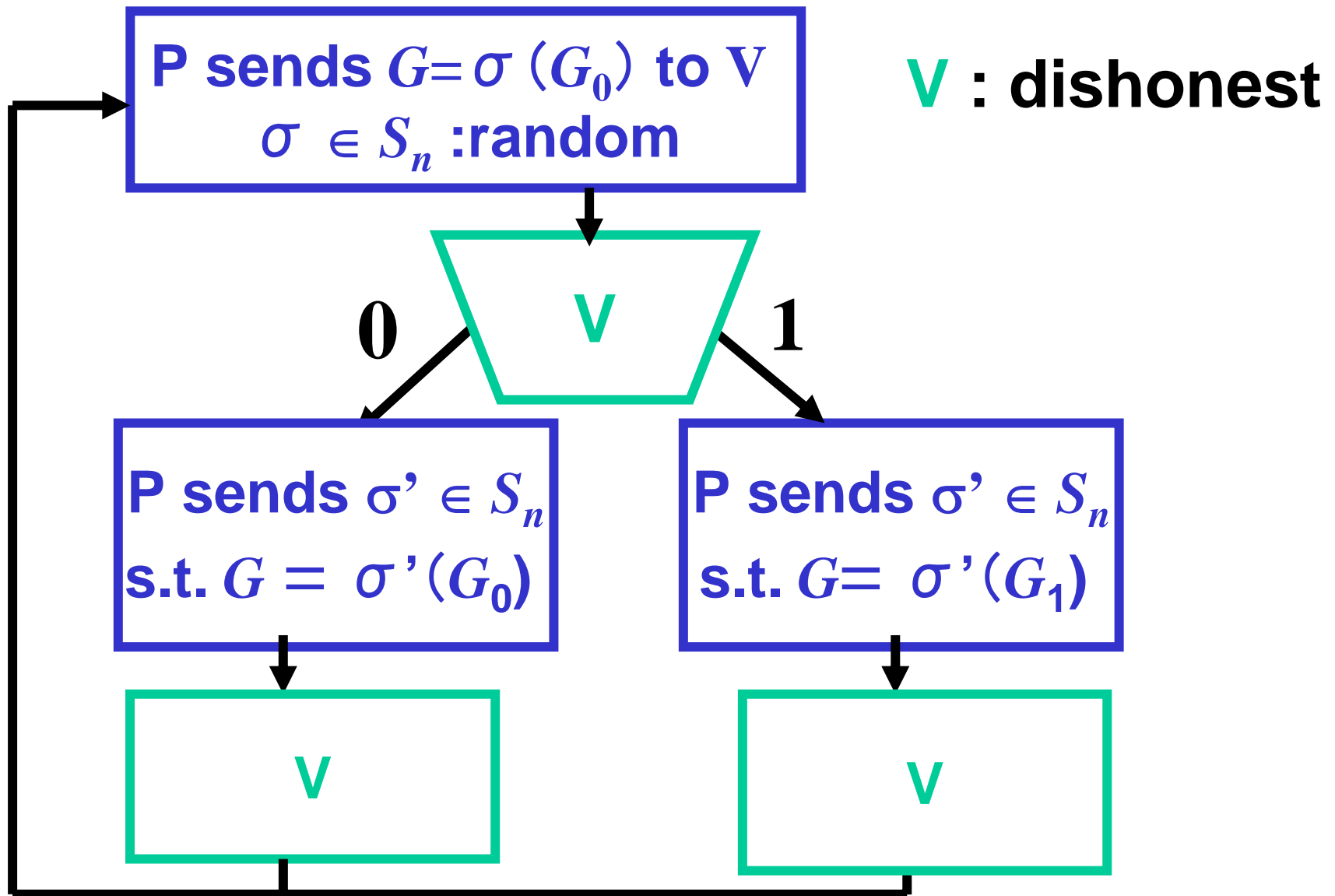
GMW protocol

1. **P** chooses a permutation σ randomly, and send $\sigma(G_0)$ to **V**.
A graph $G \cong G_0 (\cong G_1)$ is chosen randomly
 2. **V** randomly chooses G_0 or G_1 . Suppose G_b is chosen.
 3. **P** to sends $\tau \in S_n$ s. t. $\tau(G_b) = \sigma(G_0)$.
If **P** is honest, he can do this. Otherwise, he cannot.
V checks $\tau(G_b) = \sigma(G_0)$.
- Repeat 1-3 many times, to amplify the error prob.

A classical simulator \mathbf{M}

1. \mathbf{M} chooses G_0 or G_1 , randomly. Suppose G_b is chosen.
2. Choose σ randomly, and compute $\sigma(G_b)$. **A graph $G \cong G_0 (\cong G_1)$ is chosen randomly**
3. Let us run the same algorithm as \mathbf{V} , assuming $\sigma(G_b)$ is given to \mathbf{V} from \mathbf{P} .
4. If \mathbf{V} chooses G_b , the simulator can guess τ with $\tau(G_b) = \sigma(G_b)$. (**$\tau = \sigma$!**). This simulates last message from \mathbf{P} . **Record all the outputs and goes to next round.**
5. Otherwise, throw away the bits, and restart from Step 1.





**V does his best to learn from the interaction
(e.g. about π with $\pi(G_0) = G_1$)**

