# Classically Verifiable (Dual-Mode) NIZK for QMA with Preprocessing

Morimae and Yamakawa, arXiv:2102.09149


# QMA

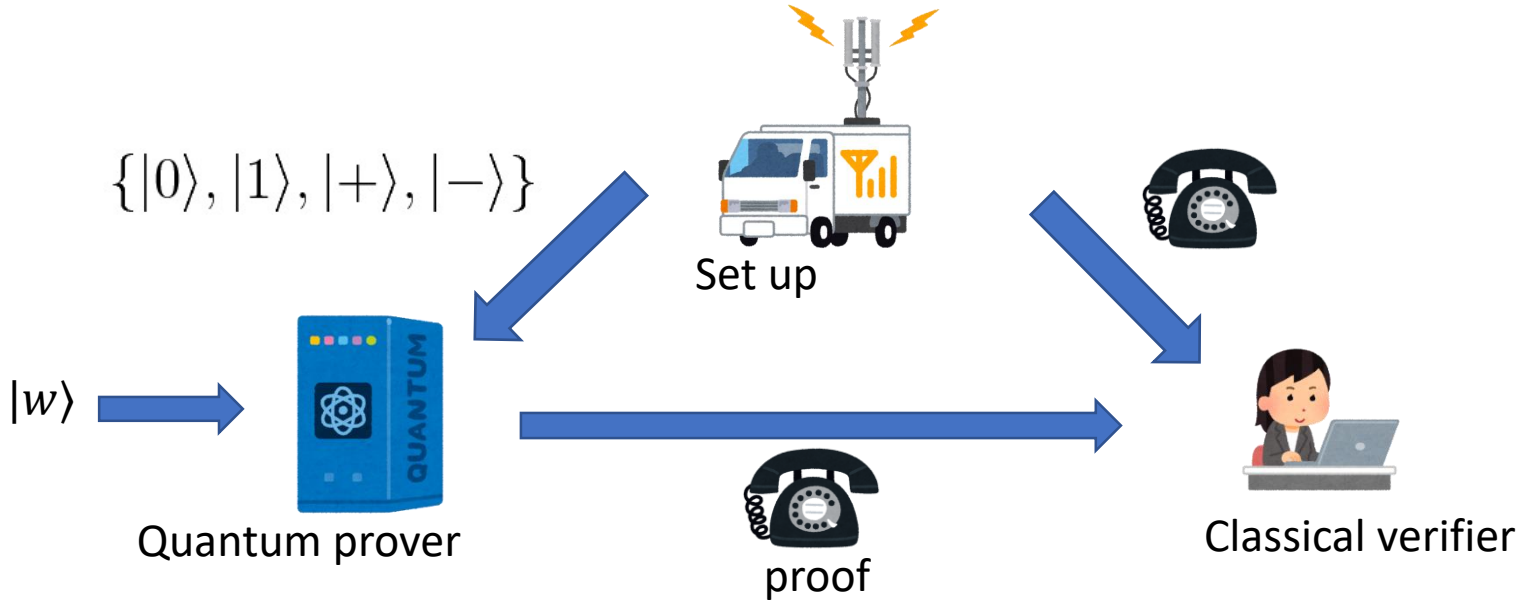
Quantum version of NP


Correctness: if $x \in L$ then there exits $|w\rangle$ s.t. Pr(V=1)>2/3

Soundness: if $x \notin L$ then for any $|w\rangle$, Pr(V=1)<1/3

# Result 1

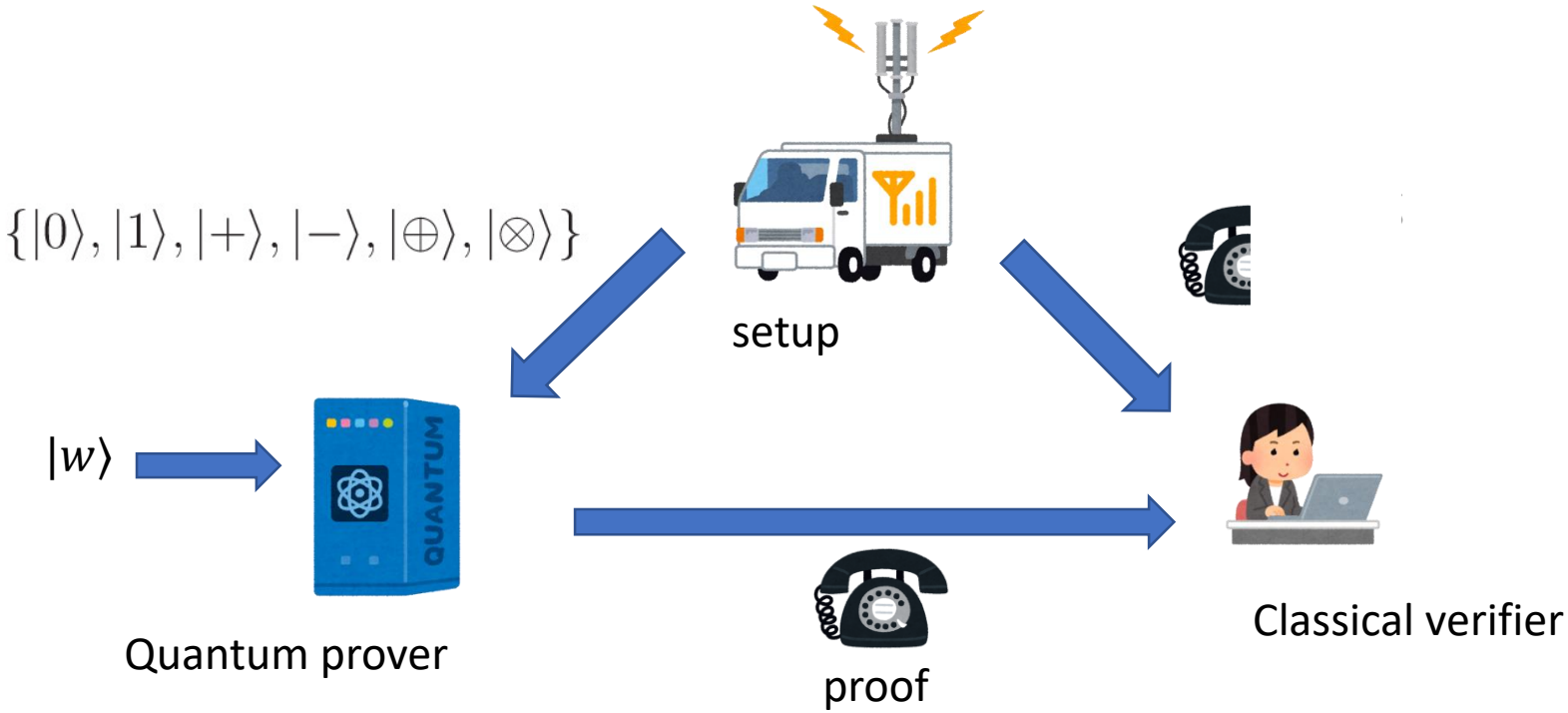
Classically-verifiable Non-interactive proof (CV-NIP) for QMA




| | verifier | rounds | soundness |
|---|---|---|---|
| Our result | Classical (Qsetup) | 1 | IT |
| Fitzsimons-Kashefi PRA 2017 | quantum | poly | IT |
| Morimae-Fitzsimons PRL2018 | quantum | 1 | IT |
| Mahadev [FOCS2018] | classical | Poly(4 or 2) | LWE |

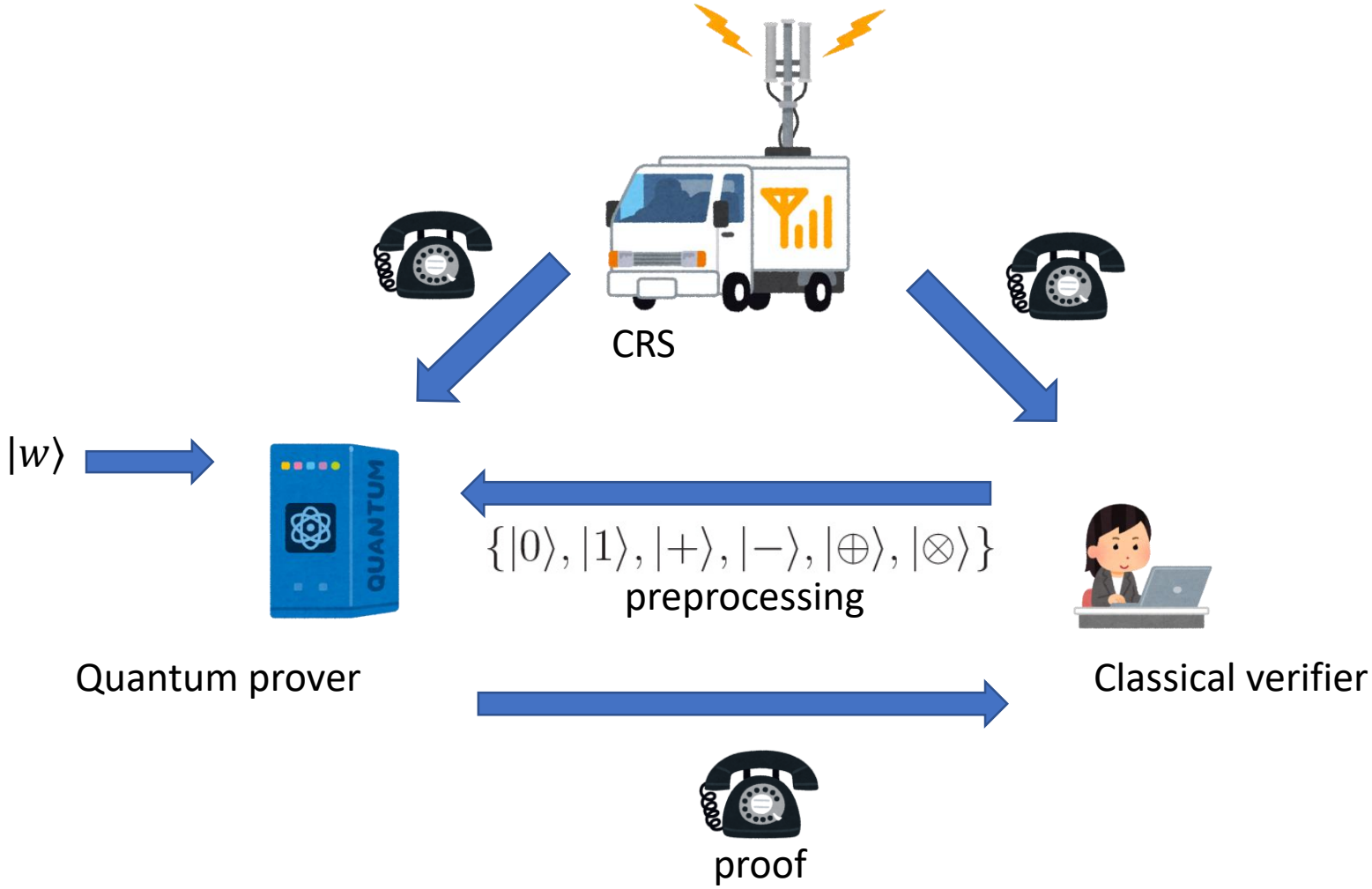
# Result 2

Classically-verifiable Non-interactive statistical zero-knowledge proof (NIZK) for QMA



# Result 3

Non-interactive statistical zero-knowledge proof (NIZK) for QMA with CRS+V→P



# NIZK comparison

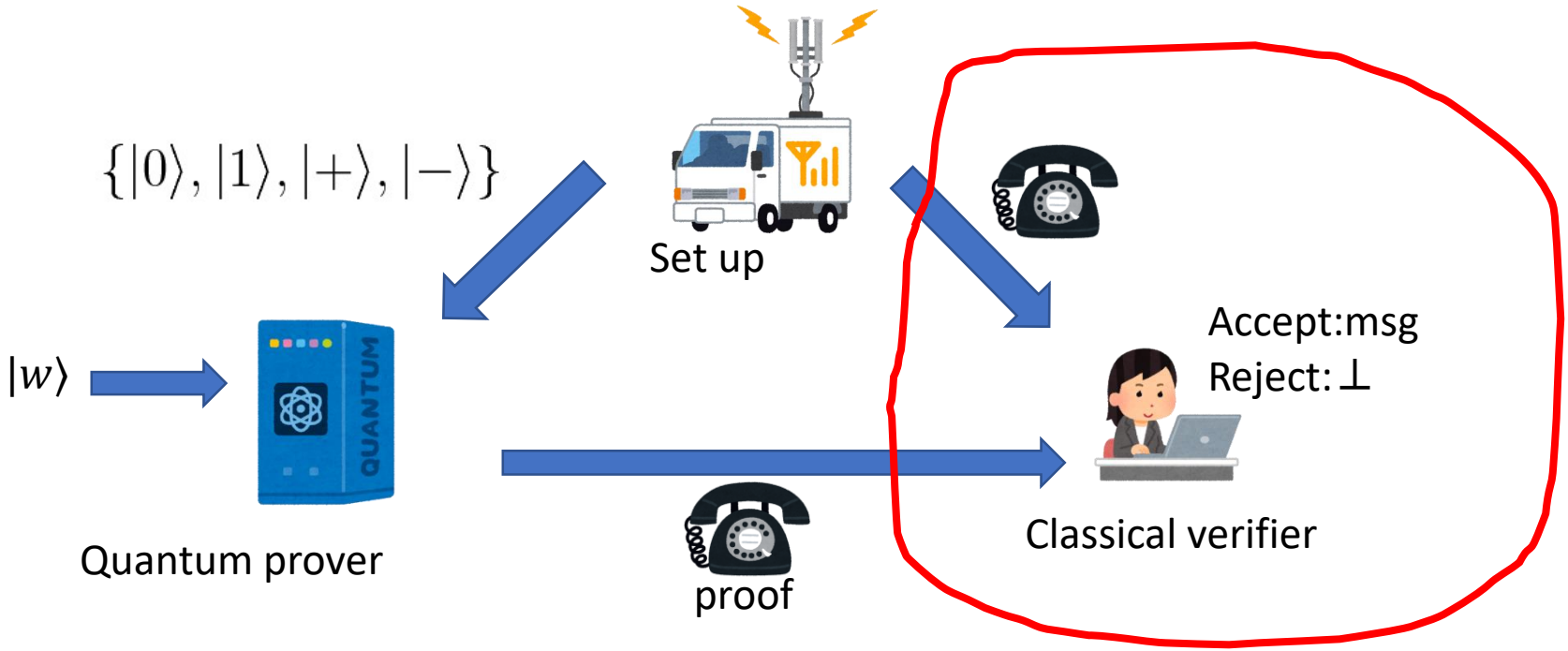
Table 1: Comparison of NIZKs for **QMA**.

| Reference | Soundness | ZK | Verification | Model | Assumption | Misc |
|---|---|---|---|---|---|---|
| [ACGH20] | comp. | comp. | classical | DV | LWE + RO | |
| [CVZ20] | comp. | comp. | quantum+classical | CRS + $(V \to P)$ | LWE | AoQK |
| [BG20] | stat. | stat. | quantum | SP | None | |
| [Shm20] | comp. | comp. | quantum | MDV | LWE | reusable |
| [BCKM20] | comp. | comp. | quantum | MDV | LWE | reusable and single-witness |
| Section 4 | stat. | stat. | classical | SP | None | |
| Section 5 | stat.<br>comp. | comp.<br>stat. | quantum+classical | CRS + $(V \to P)$ | LWE | dual-mode |

In column "Soundness" (resp. "ZK"), stat., and comp. mean statistical, and computational soundness (resp. zero-knowledge), respectively. In column "Verification", "quantum+classical" means that the verifier needs to send a quantum message in preprocessing but the online phase of verification is classical.

# Application: WE for QMA

Classically-verifiable Non-interactive proof (CV-NIP) for QMA




Bartusek-Malavolta[iacr eprint 2021/421]: using Mahadev and therefore LWE is necessary.
We do not need LWE.