

Sample-efficient device-independent verification and certification of quantum states

Aleksandra Goćanin (University of Belgrade)

Ivan Šupić (LIP6)

Borivoje Dakić (University of Vienna)

QUACC (2023)

Sample-Efficient Device-Independent Quantum State Verification and Certification

Aleksandra Gočanin^{1,*} , Ivan Šupić^{2,3} and Borivoje Dakić^{4,5}

¹

Sample-efficient

Sample-Efficient Device-Independent Quantum State Verification and Certification

Aleksandra Gočanin^{1,*} , Ivan Šupić^{2,3} and Borivoje Dakić^{4,5}

¹

Sample-efficient

device-independent

Sample-Efficient Device-Independent Quantum State Verification and Certification

Aleksandra Gočanin^{1,*} , Ivan Šupić^{2,3} and Borivoje Dakić^{4,5}

¹

Sample-efficient

device-independent

verification

Sample-Efficient Device-Independent Quantum State Verification and Certification

Aleksandra Gočanin^{1,*} , Ivan Šupić^{2,3} and Borivoje Dakić^{4,5}

¹

Sample-efficient

device-independent

verification

certification

Sample-Efficient Device-Independent Quantum State Verification and Certification

Aleksandra Gočanin^{1,*} , Ivan Šupić^{2,3} and Borivoje Dakić^{4,5}

¹

Sample-efficient

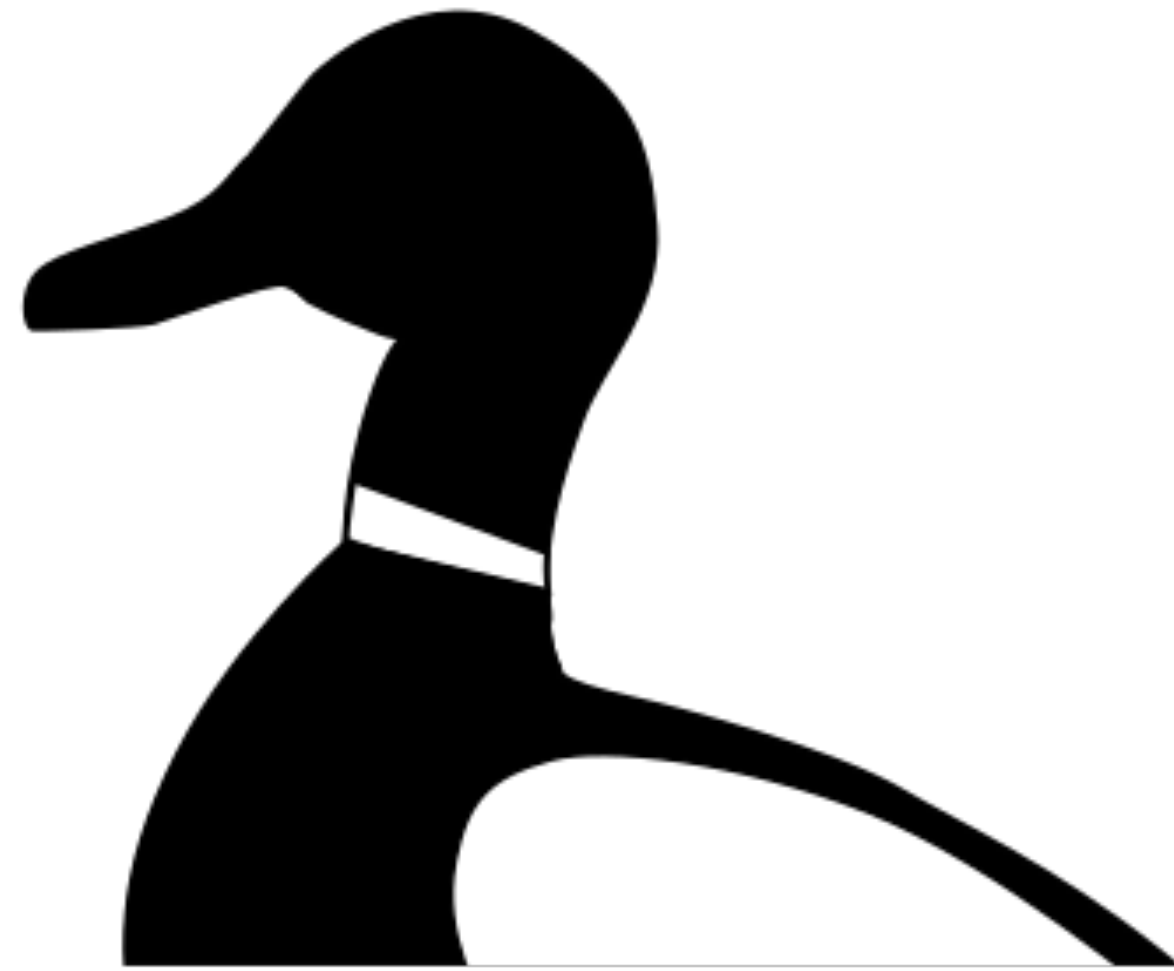
device-independent

verification

certification

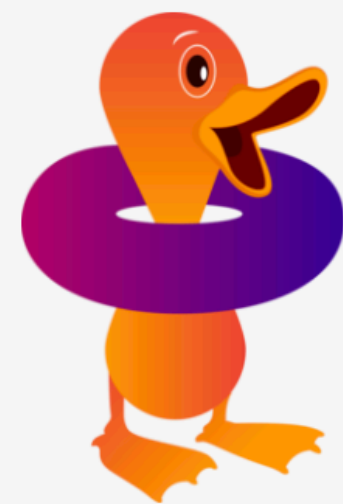
quantum states

Why is certification important?



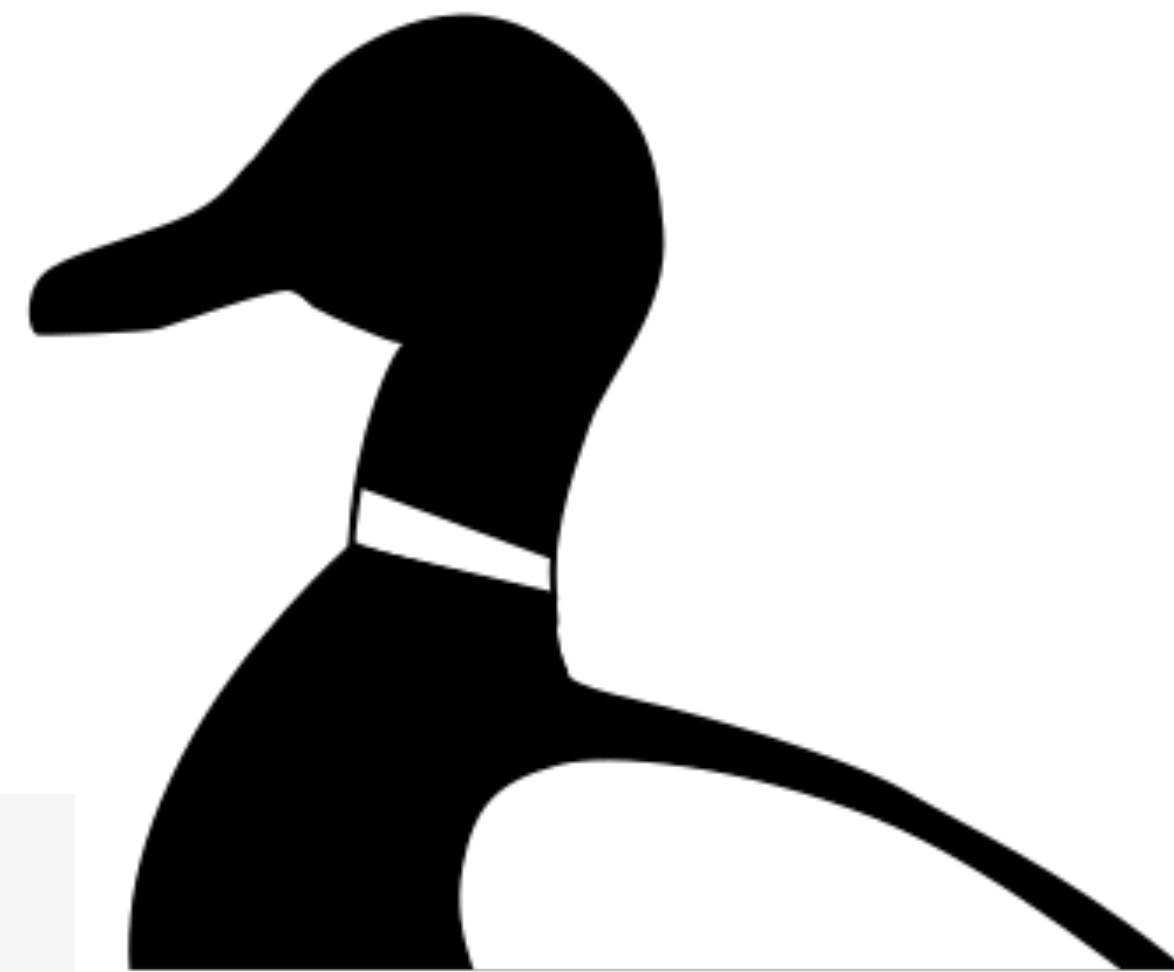
QUACC

Why is certification important?



QuAcc

[QuAcc](#) (the “Quantum Accelerator”) is a flexible and extensible platform for high-throughput computational materials science and quantum chemistry.



QUACC

Self-testing = device-independent quantum state certification

Is there anything to add?

The goal of self-testing is to characterise an a priori unknown quantum system based solely on measurement statistics, i.e. using an uncharacterised measurement device. Here we develop self-testing methods for quantum

Self-testing = device-independent quantum state certification

Is there anything to add?

The goal of self-testing is to characterise an a priori unknown quantum system based solely on measurement statistics, i.e. using an uncharacterised measurement device. Here we develop self-testing methods for quantum

Most previous research has focused on the problem of certifying the quantum state shared between the devices. Among others we can self-test the singlet [MYS12], graph states [McK14], high-dimensional maximally entangled states [Slo11, YN13] or non-maximally entangled states of two qubits [BP15]. The common fea-

Self-testing = device-independent quantum state certification

Is there anything to add?

The goal of self-testing is to characterise an a priori unknown quantum system based solely on measurement statistics, i.e. using an uncharacterised measurement device. Here we develop self-testing methods for quantum

Most previous research has focused on the problem of certifying the quantum state shared between the devices. Among others we can self-test the singlet [MYS12], graph states [McK14], high-dimensional maximally entangled states [Slo11, YN13] or non-maximally entangled states of two qubits [BP15]. The common fea-

Self-testing is a procedure for characterizing quantum resources with the minimal level of trust. Up to now it has been used as a device-independent certification tool for particular quantum measurements, channels, and pure entangled states. In this work we introduce the concept of self-testing more general

Self-testing = device-independent quantum state certification

Is there anything to add?

The goal of self-testing is to characterise an a priori unknown quantum system based solely on measurement statistics, i.e. using an uncharacterised measurement device. Here we develop self-testing methods for quantum

Most previous research has focused on the problem of certifying the quantum state shared between the devices. Among others we can self-test the singlet [MYS12], graph states [McK14], high-dimensional maximally entangled states [Slo11, YN13] or non-maximally entangled states of two qubits [BP15]. The common fea

Self-testing is a procedure for characterizing quantum resources with the minimal level of trust. Up to now it has been used as a device-independent certification tool for particular quantum measurements, channels, and pure entangled states. In this work we introduce the concept of self-testing more general

An alternative technique able to positively address these problems is *self-testing* [6]. Contrary to quantum state and process tomography, self-testing is a completely device-independent task. It aims to verify that a given quantum device operates on a certain quantum state, and performs certain measurements on it, solely from the correlations it generates. The building block for this, as well as for all other device-independent protocols is Bell's

Self-testing = device-independent quantum state certification

Is there anything to add?

The goal of self-testing is to characterise an a priori unknown quantum system based solely on measurement statistics, i.e. using an uncharacterised measurement device. Here we develop self-testing methods for quantum

Most previous research has focused on the problem of certifying the quantum state shared between the devices. Among others we can self-test the singlet [MYS12], graph states [McK14], high-dimensional maximally entangled states [Slo11, YN13] or non-maximally entangled states of two qubits [BP15]. The common fea

Self-testing is a procedure for characterizing quantum resources with the minimal level of trust. Up to now it has been used as a device-independent certification tool for particular quantum measurements, channels, and pure entangled states. In this work we introduce the concept of self-testing more general

An alternative technique able to positively address these problems is *self-testing* [6]. Contrary to quantum state and process tomography, self-testing is a completely device-independent task. It aims to verify that a given quantum device operates on a certain quantum state, and performs certain measurements on it, solely from the correlations it generates. The building block for this, as well as for all other device-independent protocols is Bell's

$$\{p(a, b | x, y)\}_{a,b,x,y}$$

←
Born rule

$$|\psi\rangle, \{M_{a|x}\}_{a,x}, \{M_{b|y}\}_{b,y}$$

Self-testing = device-independent quantum state certification

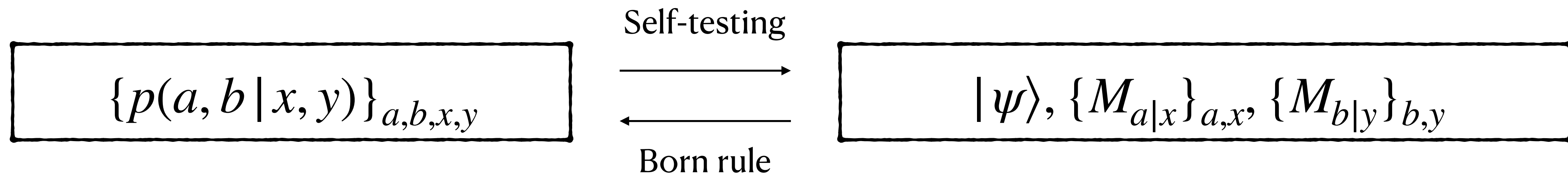
Is there anything to add?

The goal of self-testing is to characterise an a priori unknown quantum system based solely on measurement statistics, i.e. using an uncharacterised measurement device. Here we develop self-testing methods for quantum

Most previous research has focused on the problem of certifying the quantum state shared between the devices. Among others we can self-test the singlet [MYS12], graph states [McK14], high-dimensional maximally entangled states [Slo11, YN13] or non-maximally entangled states of two qubits [BP15]. The common fea

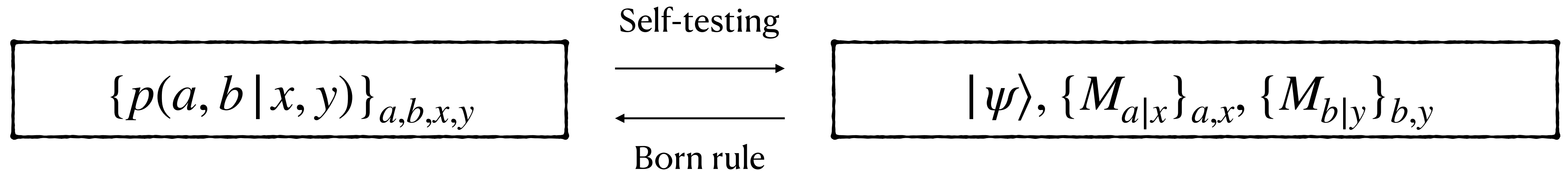
Self-testing is a procedure for characterizing quantum resources with the minimal level of trust. Up to now it has been used as a device-independent certification tool for particular quantum measurements, channels, and pure entangled states. In this work we introduce the concept of self-testing more general

An alternative technique able to positively address these problems is *self-testing* [6]. Contrary to quantum state and process tomography, self-testing is a completely device-independent task. It aims to verify that a given quantum device operates on a certain quantum state, and performs certain measurements on it, solely from the correlations it generates. The building block for this, as well as for all other device-independent protocols is Bell's



Self-testing = device-independent quantum state certification

Is there anything to add?



How $\{p(a, b | x, y)\}$ is obtained ?

Repeating experiment many times

Frequencies

not probabilities !



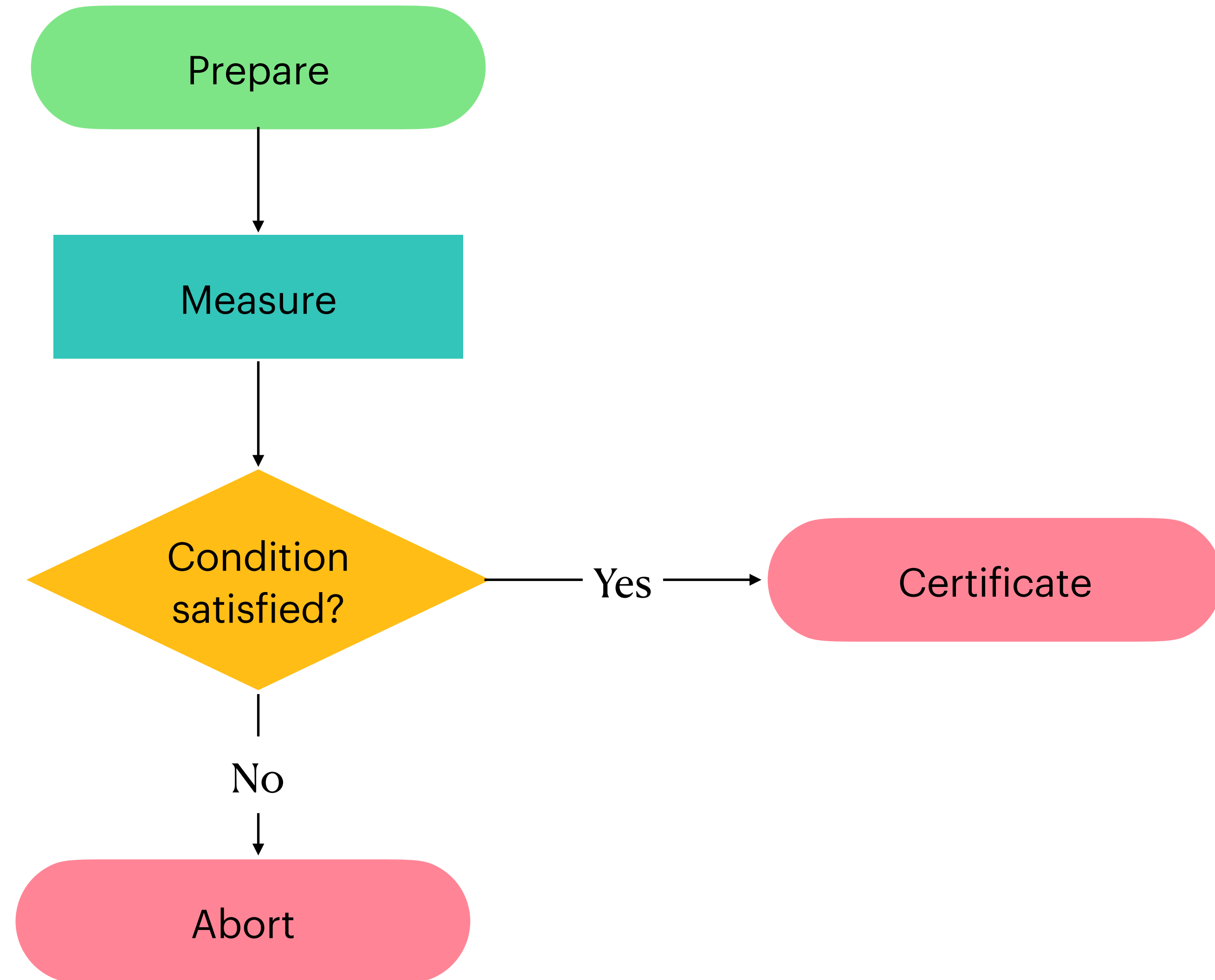
Robust self-testing

No assumptions on source : non IID



?

A need for a protocol



Complexity of a protocol

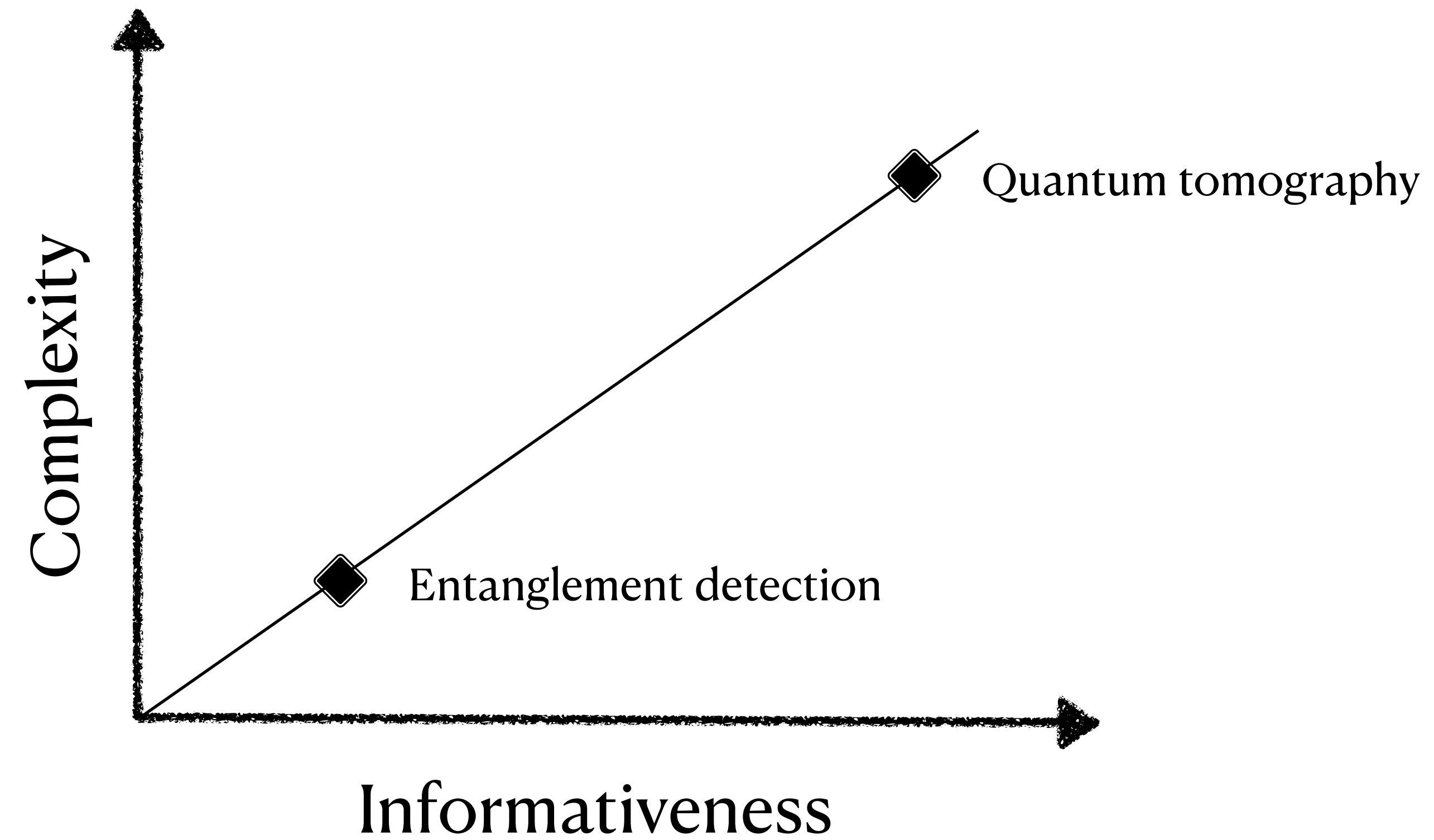
Sample complexity

Measurement complexity

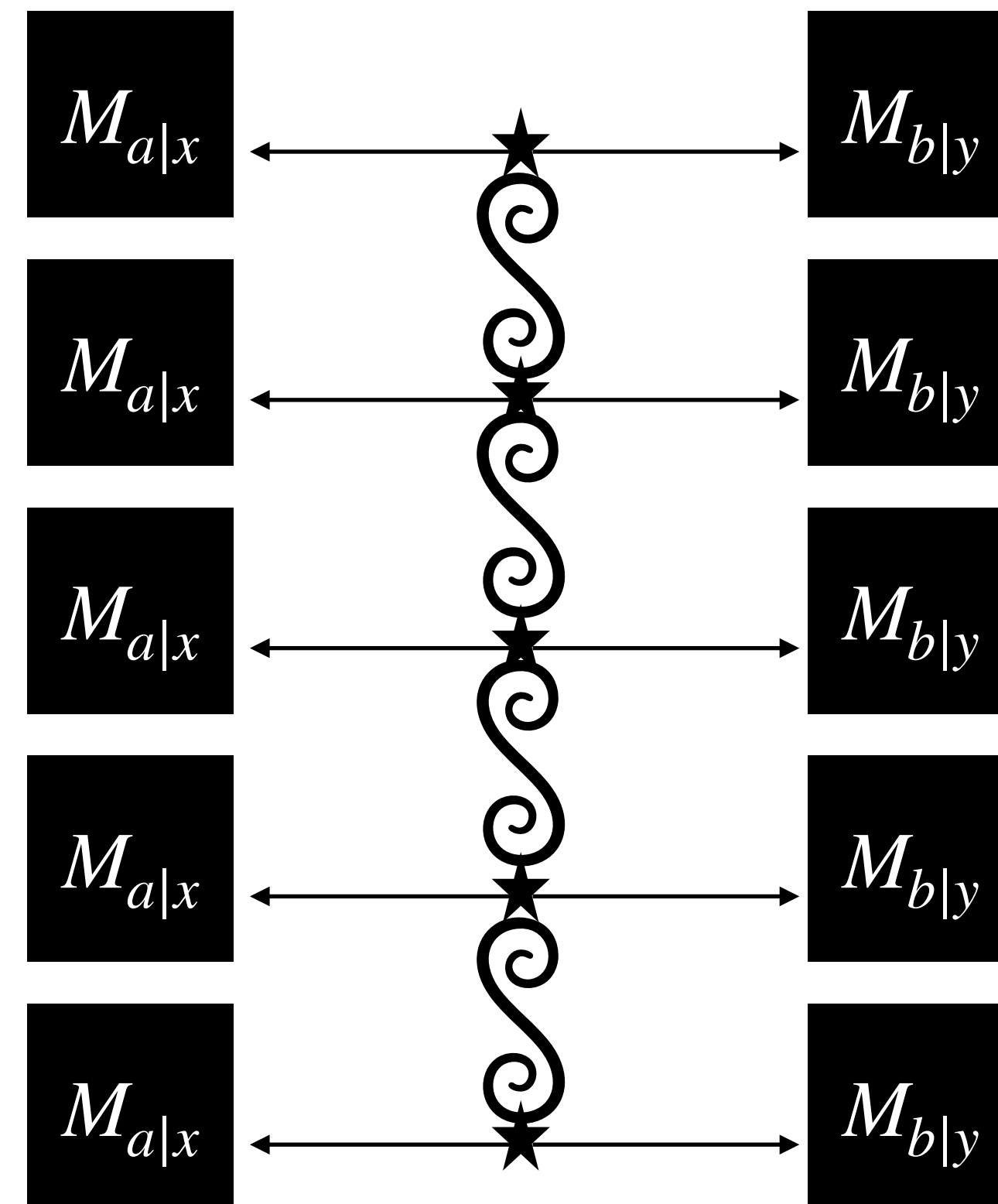
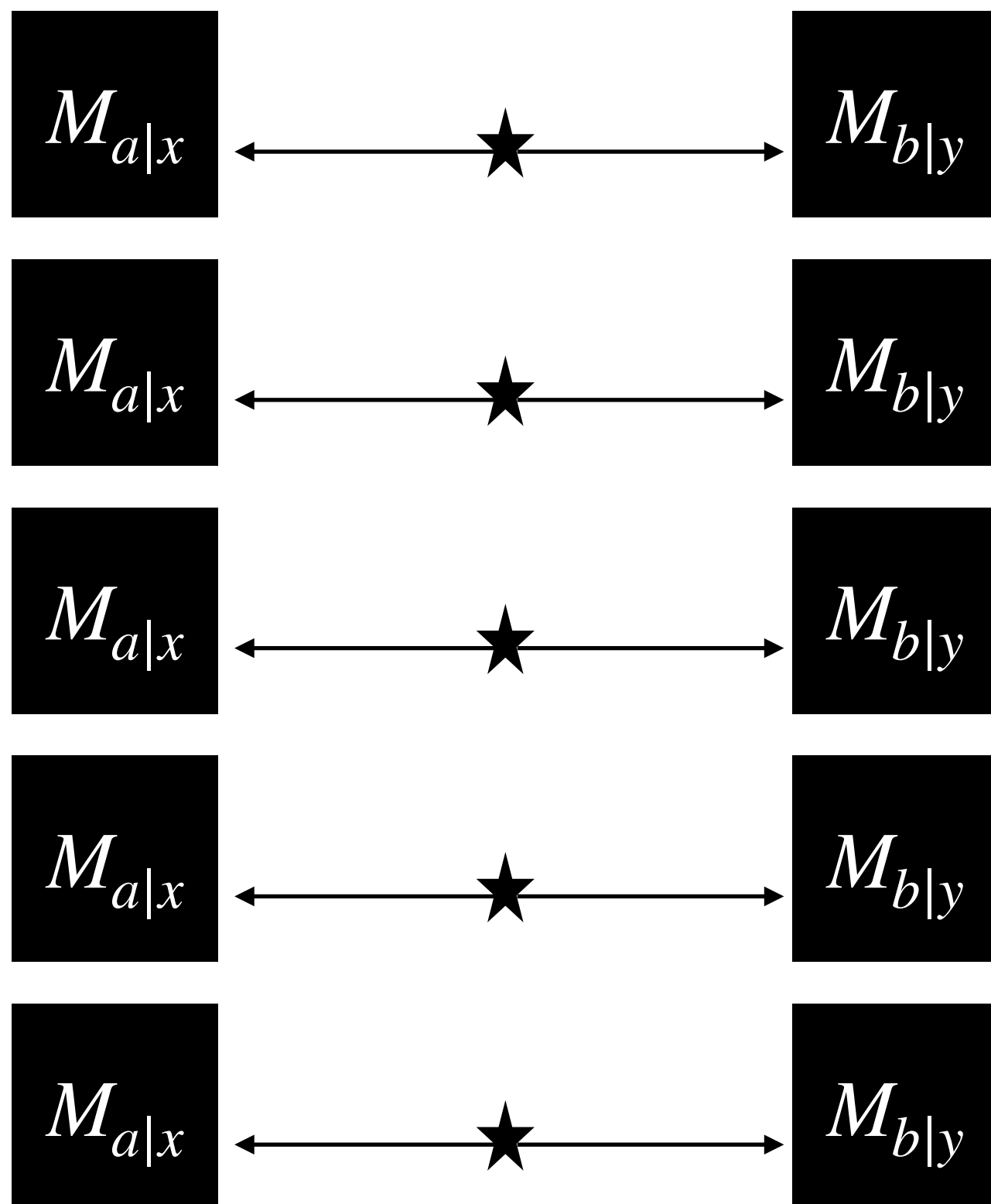
Quantum computational complexity

Post-processing complexity

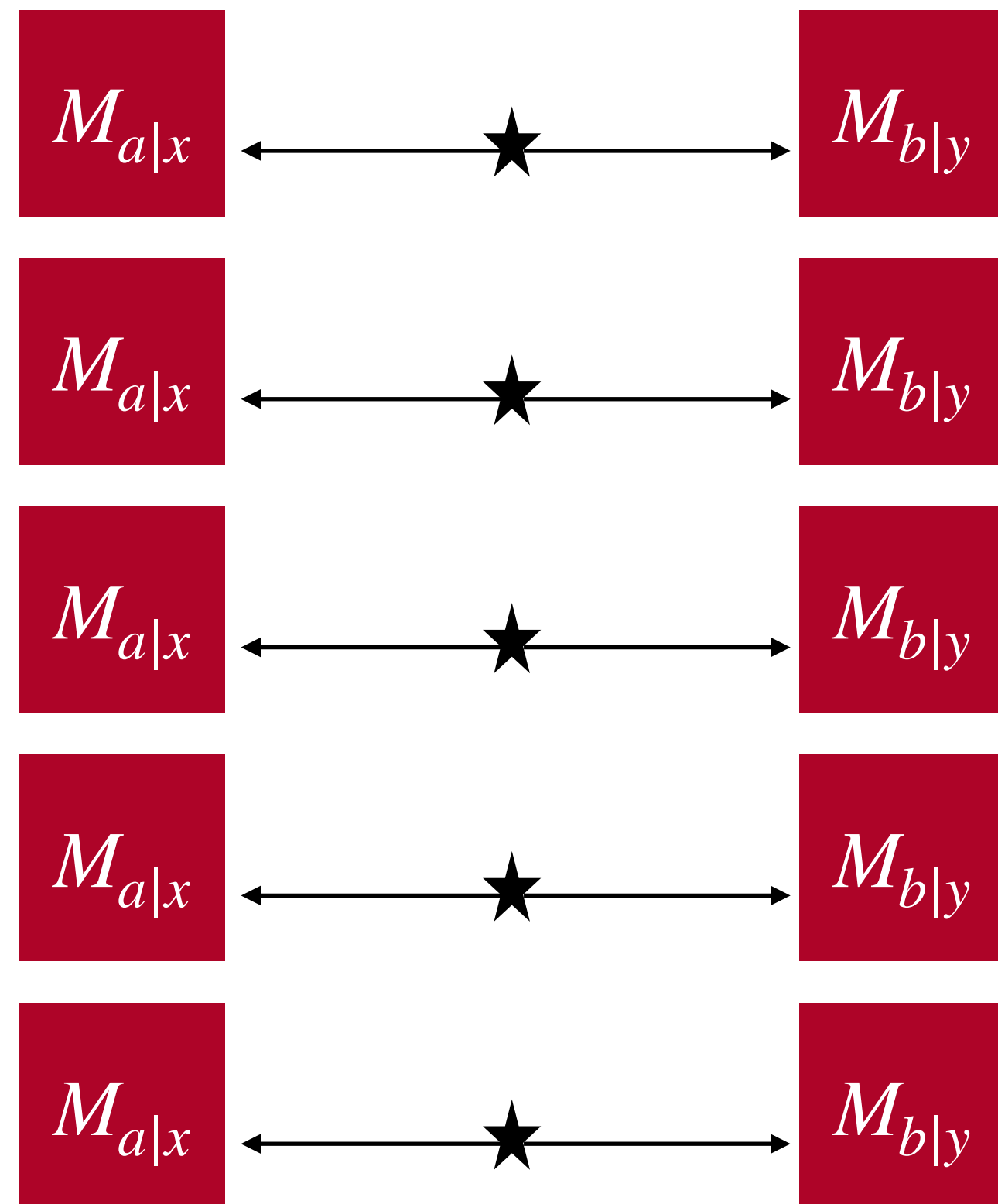
Complexity of a protocol



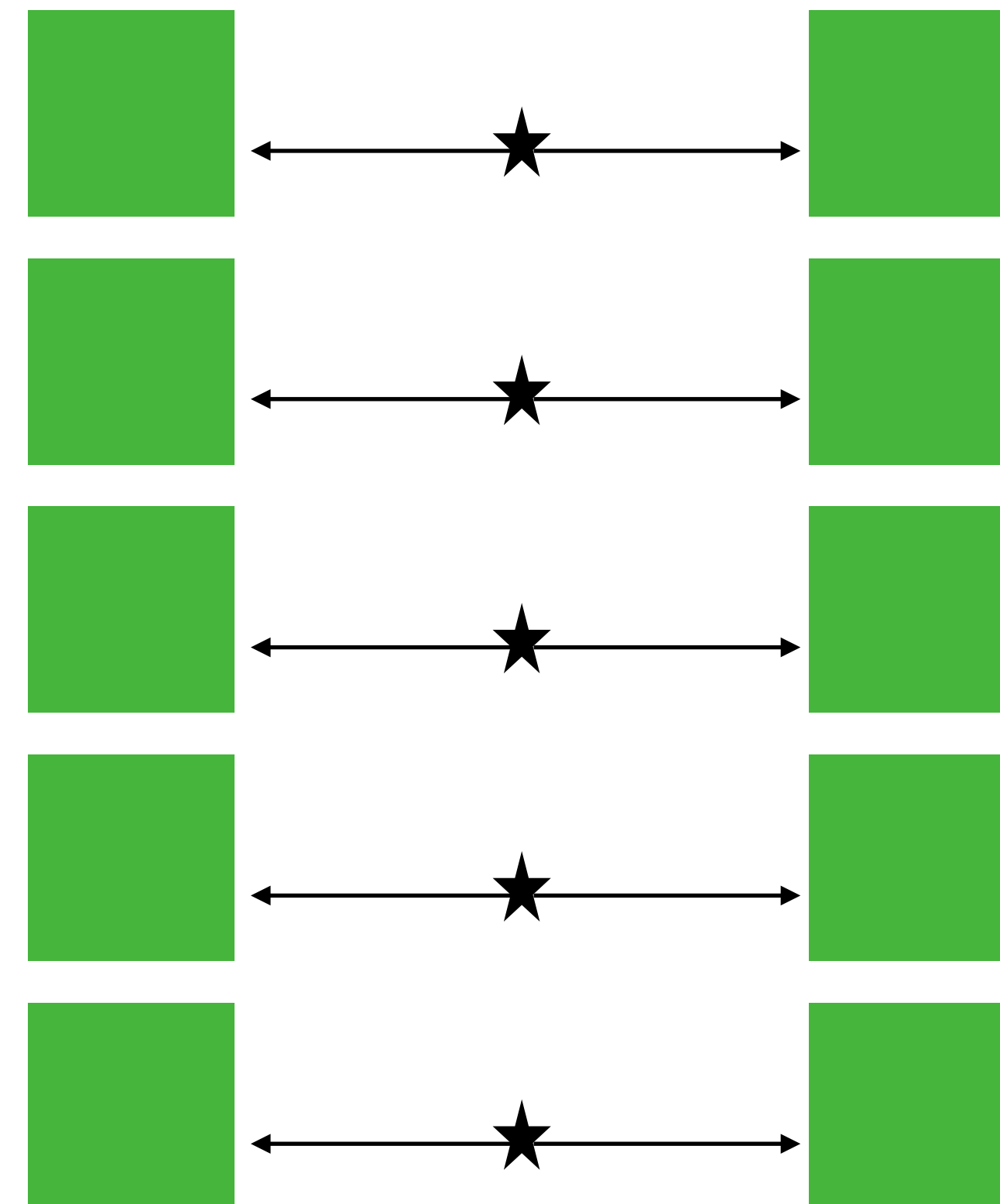
Device-independence



Zero - waste ?

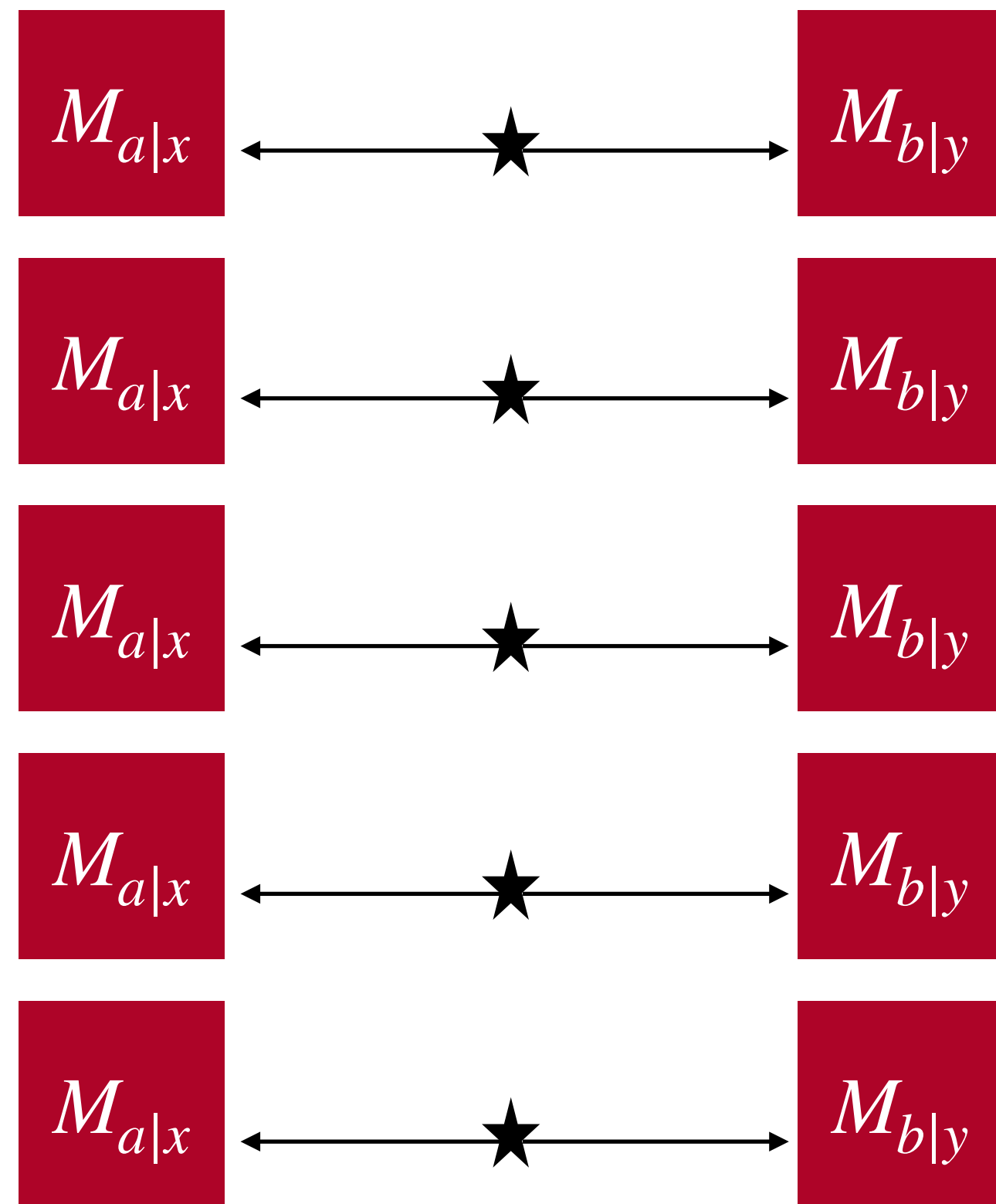


Measurements destroy entanglement

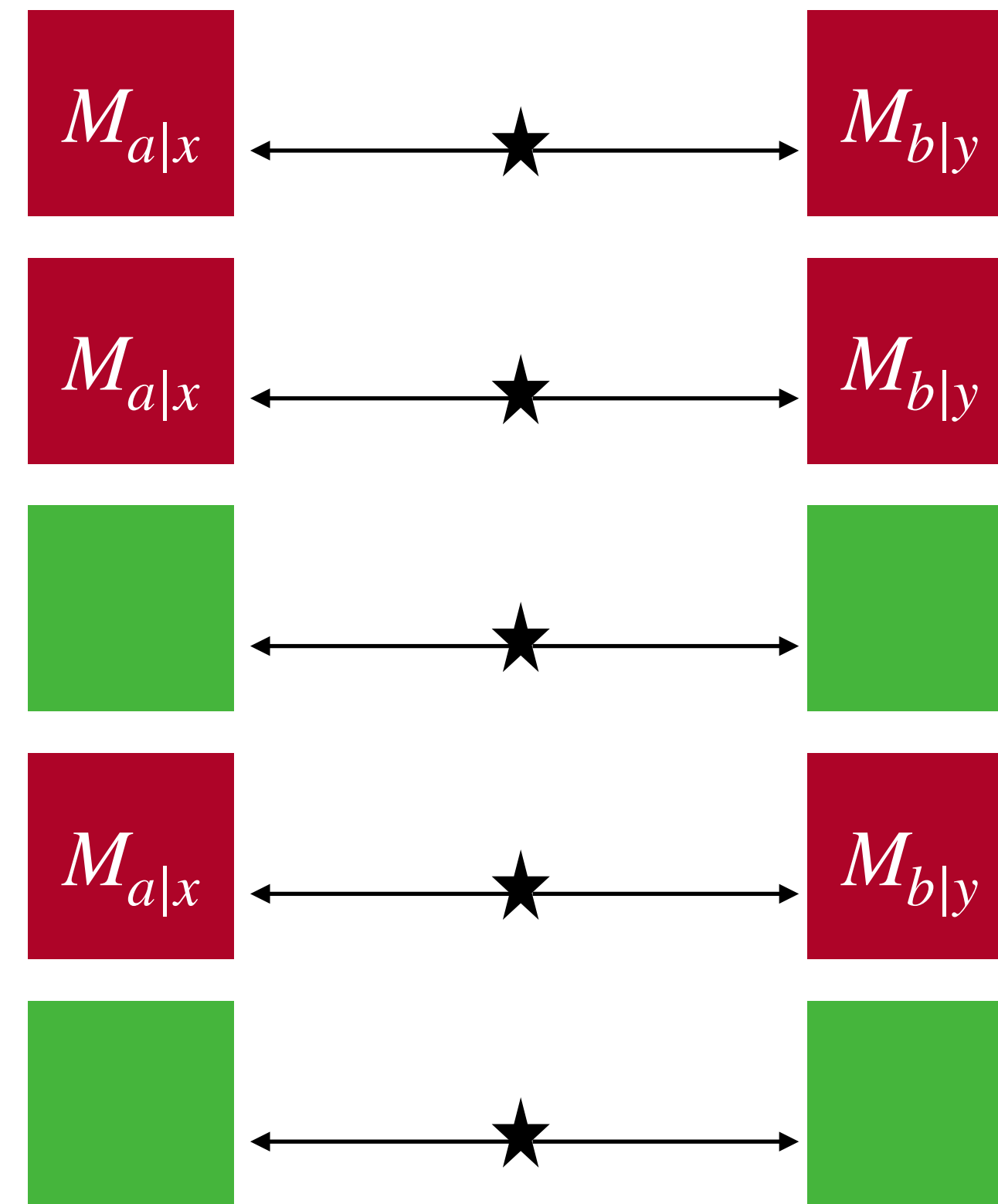


Zero-waste impossible

Verification and certification

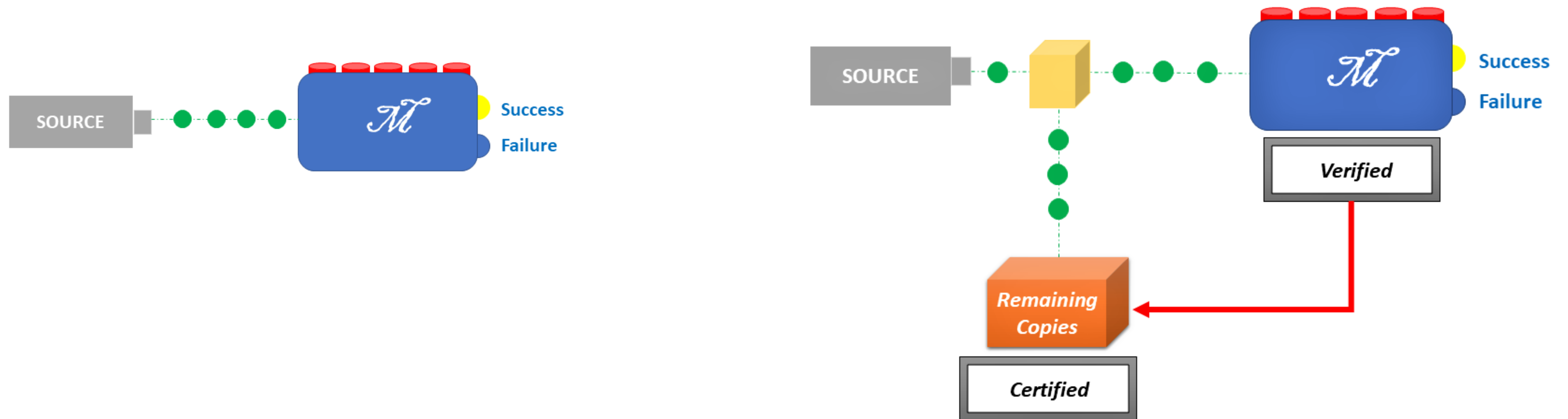


Verification



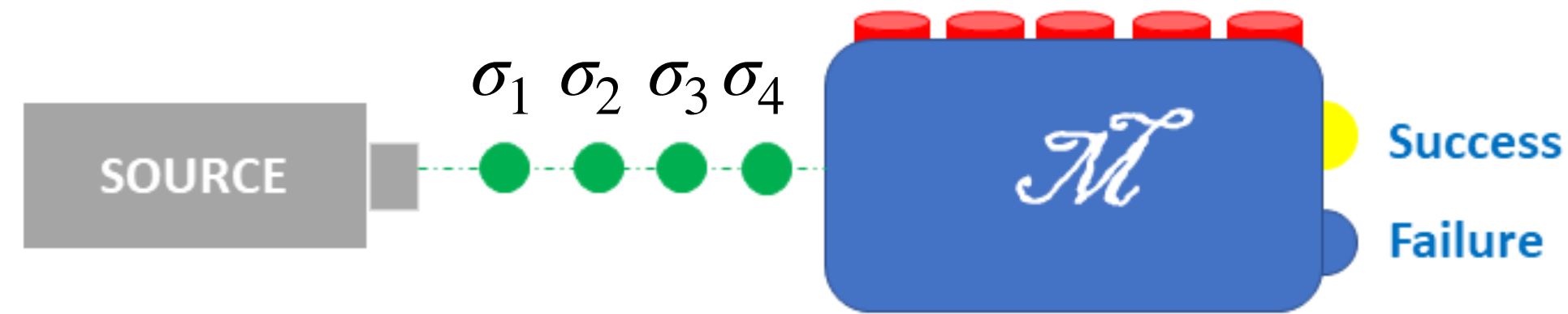
Certification

Verification and certification



Quantum state verification

Pallister, Linden, Montanaro (2018)



[the source is not IID, but it is ID]

Hypothesis testing:

Hypothesis 1: all states are equal to some target state ψ

Hypothesis 2: $F(\sigma_j, \psi) \leq 1 - \epsilon$, for all j

Measurement strategy operator $\Omega = \frac{1}{|l|} \sum_{i=1}^l M_{o|i}$,

output $o = 1$ means that the round is passed,

output $o = 0$ means that the round is failed

The target state ψ , thus should be the only state such that $\langle \psi | M_{1|i} | \psi \rangle = 1$ for all i .

Quantum state verification

Pallister, Linden, Montanaro (2018)

N states $\{\sigma_1, \dots, \sigma_N\}$
Strategy operator $\Omega = \frac{1}{|l|} \sum_{i=1}^l M_{o|i}$

Hypothesis 1: all states are equal to some target state ψ

Hypothesis 2: $F(\sigma_j, \psi) \leq 1 - \epsilon$, for all j

If all the rounds are successfully passed how sure are we that $\sigma_j = \psi$ for all j ?

Of all states σ such that $F(\sigma, \psi) \leq 1 - \epsilon$, the highest probability to pass all rounds has the state of the form $\sigma = (1 - \epsilon) |\psi\rangle\langle\psi| + \epsilon |\psi'\rangle\langle\psi'|$, where $|\psi'\rangle$ corresponds to the eigenvector of Ω associated to the second-largest eigenvalue $1 - \nu(\Omega)$ [$\nu(\Omega)$ is the spectral gap of Ω]

The highest probability that a wrong set of states passes all rounds is $(1 - \epsilon\nu(\Omega))^N$

Hence, our confidence that the source always produces the correct state is $\delta = 1 - (1 - \epsilon\nu(\Omega))^N$

$$N \approx \frac{1}{\epsilon\nu(\Omega)} \ln(\delta)^{-1}$$

Example

$$N \approx \frac{1}{\epsilon \nu(\Omega)} \ln(\delta)^{-1}$$

The best case when $\nu(\Omega) = 1$, but then Ω is entangled

- Target state $\psi = |\phi_+\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Strategy $\Omega = \frac{1}{3}(\sigma_z \otimes \sigma_z + \sigma_x \otimes \sigma_x - \sigma_y \otimes \sigma_y)$
- $\Omega = |\phi_+\rangle\langle\phi_+| + \frac{1}{3}\mathbf{1}$, $\nu(\Omega) = \frac{2}{3}$

Simple strategies for all stabiliser states!

Recipe for QSV

1. Build measurement strategy operator Ω ,

Recipe for QSV

1. Build measurement strategy operator Ω , such that
 - A. ψ is the only state such that $\langle \psi | \Omega | \psi \rangle = 1$

Recipe for QSV

1. Build measurement strategy operator Ω , such that
 - A. ψ is the only state such that $\langle \psi | \Omega | \psi \rangle = 1$
 - B. Ω consists of local measurements

Recipe for QSV

1. Build measurement strategy operator Ω , such that
 - A. ψ is the only state such that $\langle \psi | \Omega | \psi \rangle = 1$
 - B. Ω consists of local measurements
2. Find the spectral gap of the strategy operator $\nu(\Omega)$

Recipe for QSV

1. Build measurement strategy operator Ω , such that
 - A. ψ is the only state such that $\langle \psi | \Omega | \psi \rangle = 1$
 - B. Ω consists of local measurements
2. Find the spectral gap of the strategy operator $\nu(\Omega)$
3. The sample efficiency of the QSV protocol will be $N \approx \frac{1}{\epsilon \nu(\Omega)} \ln(\delta)^{-1}$

Variations

- Adapted to various classes of states (graph states, GHZ states, Dicke states)
- Abandoned promise that all states must be either the target state, or at least ϵ -far from it (Yu, Shang, Gühne 2019)
- Adapted to completely non-IID case (Zhu, Hayashi 2019)

Device-independent quantum state verification

Figure of merit (ID case)

- Device-independent verification is blind for exactly the same set of transformations as self-testing
- Aim to confirm with certain confidence level that the set of states has average fidelity with target state higher than some value $1 - \epsilon$
- Device-independent twin of fidelity is **extractability** (Kaniewski 2016):

$$\Xi(\sigma_j, \psi) = \max_{\Phi} F(\text{Tr}[\Phi(\sigma_j)], \psi)$$

- Average extractability: $\bar{\Xi} = \frac{1}{N} \Xi(\sigma_j, \psi)$

Device-independent quantum state verification

Figure of merit (non-IID case)

Example: $\sigma^N = \frac{1}{2} (\psi^{\otimes N} + \chi^{\otimes N})$

Device-independent quantum state verification

Figure of merit (non-IID case)

$$\text{Example: } \sigma^N = \frac{1}{2} (\psi^{\otimes N} + \chi^{\otimes N})$$

$$F(\sigma^N, \psi) = 2^{-N}$$

Device-independent quantum state verification

Figure of merit (non-IID case)

Example: $\sigma^N = \frac{1}{2} (\psi^{\otimes N} + \chi^{\otimes N})$

$F(\sigma^N, \psi) = 2^{-N}$

With probability 0.5 the source
sends us the correct state!

Device-independent quantum state verification

Figure of merit (non-IID case)

Example: $\sigma^N = \frac{1}{2} (\psi^{\otimes N} + \chi^{\otimes N})$

$$F(\sigma^N, \psi) = 2^{-N}$$

With probability 0.5 the source
sends us the correct state!

- Conditional state

$$\tilde{\sigma}_j \propto \text{Tr}_{1, \dots, j-1, j+1, \dots, N} \left[\bigotimes_{k=1}^{j-1} M_{o_k | i_k} \sigma^N \right]$$

Device-independent quantum state verification

Figure of merit (non-IID case)

Example: $\sigma^N = \frac{1}{2} (\psi^{\otimes N} + \chi^{\otimes N})$

$F(\sigma^N, \psi) = 2^{-N}$

With probability 0.5 the source
sends us the correct state!

- Conditional state

$$\tilde{\sigma}_j \propto \text{Tr}_{1,\dots,j-1,j+1,\dots,N} \left[\bigotimes_{k=1}^{j-1} M_{o_k|i_k} \sigma^N \right]$$

- Average conditional extractability

$$\bar{\Xi} = \frac{1}{N} \Xi(\tilde{\sigma}_j, \psi)$$

Anticipating DI verification

Nonlocal games

- In every round we measure a state with uncharacterised measurement: sending classical input and receiving classical output

Anticipating DI verification

Nonlocal games

- In every round we measure a state with uncharacterised measurement: sending classical input and receiving classical output
- Some sets of outputs for a given combination of inputs pass a round, while the other fail it

Anticipating DI verification

Nonlocal games

- In every round we measure a state with uncharacterised measurement: sending classical input and receiving classical output
- Some sets of outputs for a given combination of inputs pass a round, while the other fail it
- Nonlocal game!

Anticipating DI verification

Nonlocal games

- In every round we measure a state with uncharacterised measurement: sending classical input and receiving classical output
- Some sets of outputs for a given combination of inputs pass a round, while the other fail it
- Nonlocal game!
- Necessary condition: nonlocal game should be won optimally by the target state

Anticipating DI verification

Nonlocal games

- In every round we measure a state with uncharacterised measurement: sending classical input and receiving classical output
- Some sets of outputs for a given combination of inputs pass a round, while the other fail it
- Nonlocal game!
- Necessary condition: nonlocal game should be won optimally by the target state
- Nonlocal game has to be the self-test for the target state

Anticipating DI verification

Nonlocal games

- In every round we measure a state with uncharacterised measurement: sending classical input and receiving classical output
- Some sets of outputs for a given combination of inputs pass a round, while the other fail it
- Nonlocal game!
- Necessary condition: nonlocal game should be won optimally by the target state
- Nonlocal game has to be the self-test for the target state
- CHSH game, Mermin game

DI quantum state verification

1. Build measurement strategy operator Ω , such that
 - A. ψ is the only state such that $\langle \psi | \Omega | \psi \rangle = 1$
 - B. Ω consists of local measurements
2. Find the spectral gap of the strategy operator $\nu(\Omega)$
3. The sample efficiency of the QSV protocol will be $N \approx \frac{1}{\epsilon \nu(\Omega)} \ln(\delta)^{-1}$

DI quantum state verification

1. Build measurement strategy operator Ω , such that
 - A. ψ is the only state such that $\langle \psi | \Omega | \psi \rangle = 1$
 - B. Ω consists of local measurements
2. Find the spectral gap of the strategy operator $\nu(\Omega)$
3. The sample efficiency of the QSV protocol will be $N \approx \frac{1}{\epsilon \nu(\Omega)} \ln(\delta)^{-1}$

1. Build uncharacterised measurement strategy operator Ω (in this case a form of a Bell operator)

DI quantum state verification

1. Build measurement strategy operator Ω , such that
 - A. ψ is the only state such that $\langle \psi | \Omega | \psi \rangle = 1$
 - B. Ω consists of local measurements
2. Find the spectral gap of the strategy operator $\nu(\Omega)$
3. The sample efficiency of the QSV protocol will be $N \approx \frac{1}{\epsilon \nu(\Omega)} \ln(\delta)^{-1}$

1. Build uncharacterised measurement strategy operator Ω (in this case a form of a Bell operator)
 - A. ψ is the only state optimally winning the nonlocal game

DI quantum state verification

1. Build measurement strategy operator Ω , such that
 - A. ψ is the only state such that $\langle \psi | \Omega | \psi \rangle = 1$
 - B. Ω consists of local measurements
2. Find the spectral gap of the strategy operator $\nu(\Omega)$
3. The sample efficiency of the QSV protocol will be $N \approx \frac{1}{\epsilon \nu(\Omega)} \ln(\delta)^{-1}$

1. Build uncharacterised measurement strategy operator Ω (in this case a form of a Bell operator)
 - A. ψ is the only state optimally winning the nonlocal game
2. Find the spectral gap of the strategy operator $\nu(\Omega)$
- 3.

DI quantum state verification

1. Build measurement strategy operator Ω , such that
 - A. ψ is the only state such that $\langle \psi | \Omega | \psi \rangle = 1$
 - B. Ω consists of local measurements
2. Find the spectral gap of the strategy operator $\nu(\Omega)$
3. The sample efficiency of the QSV protocol will be $N \approx \frac{1}{\epsilon \nu(\Omega)} \ln(\delta)^{-1}$

1. Build uncharacterised measurement strategy operator Ω (in this case a form of a Bell operator)
 - A. ψ is the only state optimally winning the nonlocal game
2. Find the spectral gap of the strategy operator $\nu(\Omega)$
- 3.

DI quantum state verification

1. Build measurement strategy operator Ω , such that
 - A. ψ is the only state such that $\langle \psi | \Omega | \psi \rangle = 1$
 - B. Ω consists of local measurements
2. Find the spectral gap of the strategy operator $\nu(\Omega)$
3. The sample efficiency of the QSV protocol will be $N \approx \frac{1}{\epsilon \nu(\Omega)} \ln(\delta)^{-1}$

1. Build uncharacterised measurement strategy operator Ω (in this case a form of a Bell operator)
 - A. ψ is the only state optimally winning the nonlocal game
2. Find the spectral gap of the strategy operator $\nu(\Omega)$
3. ?

DI quantum state verification

- The best case is if state in every round has fidelity with the target state exactly equal to $1 - \epsilon$!

DI quantum state verification

- The best case is if state in every round has fidelity with the target state exactly equal to $1 - \epsilon$
- What is a probability of a state with such fidelity to win a random round of a nonlocal game?

DI quantum state verification

- The best case is if state in every round has fidelity with the target state exactly equal to $1 - \epsilon$
- What is a probability of a state with such fidelity to win a random round of a nonlocal game?
- Answer is given if the nonlocal game is a robust self-test

DI quantum state verification

- The best case is if state in every round has fidelity with the target state exactly equal to $1 - \epsilon$
- What is a probability of a state with such fidelity to win a random round of a nonlocal game?
- Answer is given if the nonlocal game is a robust self-test
- Robust self-test gives relation between the score $\omega^* - \eta$ in a nonlocal game and extractability of a state leading to such score: $\Xi(\sigma, \psi) = 1 - c\eta$

DI quantum state verification

- The best case is if state in every round has fidelity with the target state exactly equal to $1 - \epsilon$
- What is a probability of a state with such fidelity to win a random round of a nonlocal game?
- Answer is given if the nonlocal game is a robust self-test
- Robust self-test gives relation between the score $\omega^* - \eta$ in a nonlocal game and extractability of a state leading to such score: $\Xi(\sigma, \psi) = 1 - c\eta$
- This relation can be inverted and rescaled, which gives a probability of state characterised by given fidelity/extractability to win a randomly chosen round:

$$p_{succ} = \omega^* - c'\epsilon$$

DI quantum state verification

1. Build measurement strategy operator Ω , such that
 - A. ψ is the only state such that $\langle \psi | \Omega | \psi \rangle = 1$
 - B. Ω consists of local measurements
2. Find the spectral gap of the strategy operator $\nu(\Omega)$
3. The sample efficiency of the QSV protocol will be $N \approx \frac{1}{\epsilon \nu(\Omega)} \ln(\delta)^{-1}$

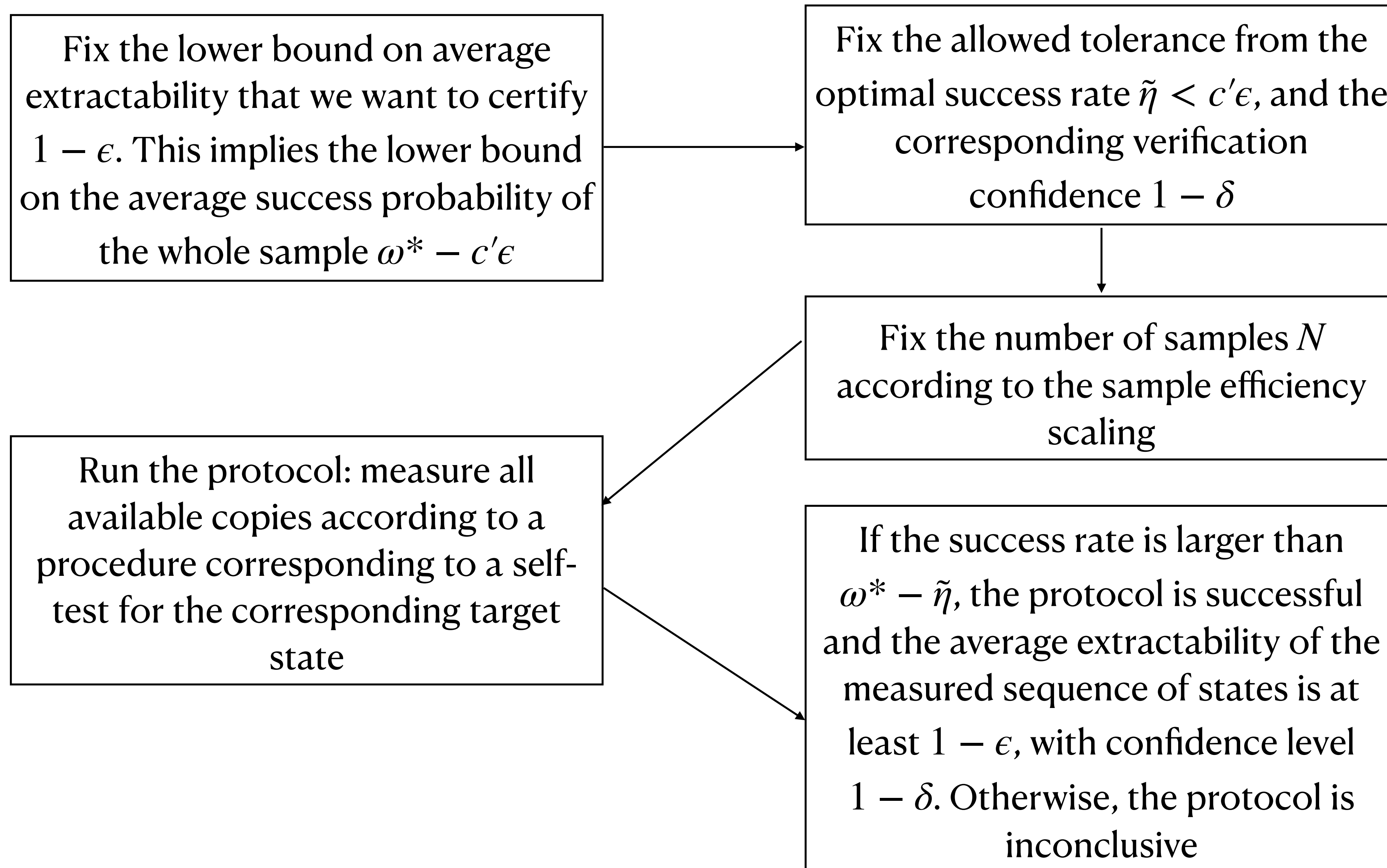
1. Build uncharacterised measurement strategy operator Ω (in this case a form of a Bell operator)
 - A. ψ is the only state optimally winning the nonlocal game
2. ~~Find the spectral gap of the strategy operator $\nu(\Omega)$~~ Calculate robustness of the self-test

DI quantum state verification

1. Build measurement strategy operator Ω , such that
 - A. ψ is the only state such that $\langle \psi | \Omega | \psi \rangle = 1$
 - B. Ω consists of local measurements
2. Find the spectral gap of the strategy operator $\nu(\Omega)$
3. The sample efficiency of the QSV protocol will be $N \approx \frac{1}{\epsilon \nu(\Omega)} \ln(\delta)^{-1}$

1. Build uncharacterised measurement strategy operator Ω (in this case a form of a Bell operator)
 - A. ψ is the only state optimally winning the nonlocal game
2. ~~Find the spectral gap of the strategy operator $\nu(\Omega)$~~
Calculate robustness of the self-test
3. The sample efficiency of the QSV protocol will be
$$N \approx \frac{1}{c\epsilon} \ln(\delta)^{-1}, \text{ if the nonlocal game is pseudo telepathy}$$
$$N \approx \frac{1}{(c\epsilon)^2} \ln(\delta)^{-1}, \text{ otherwise}$$

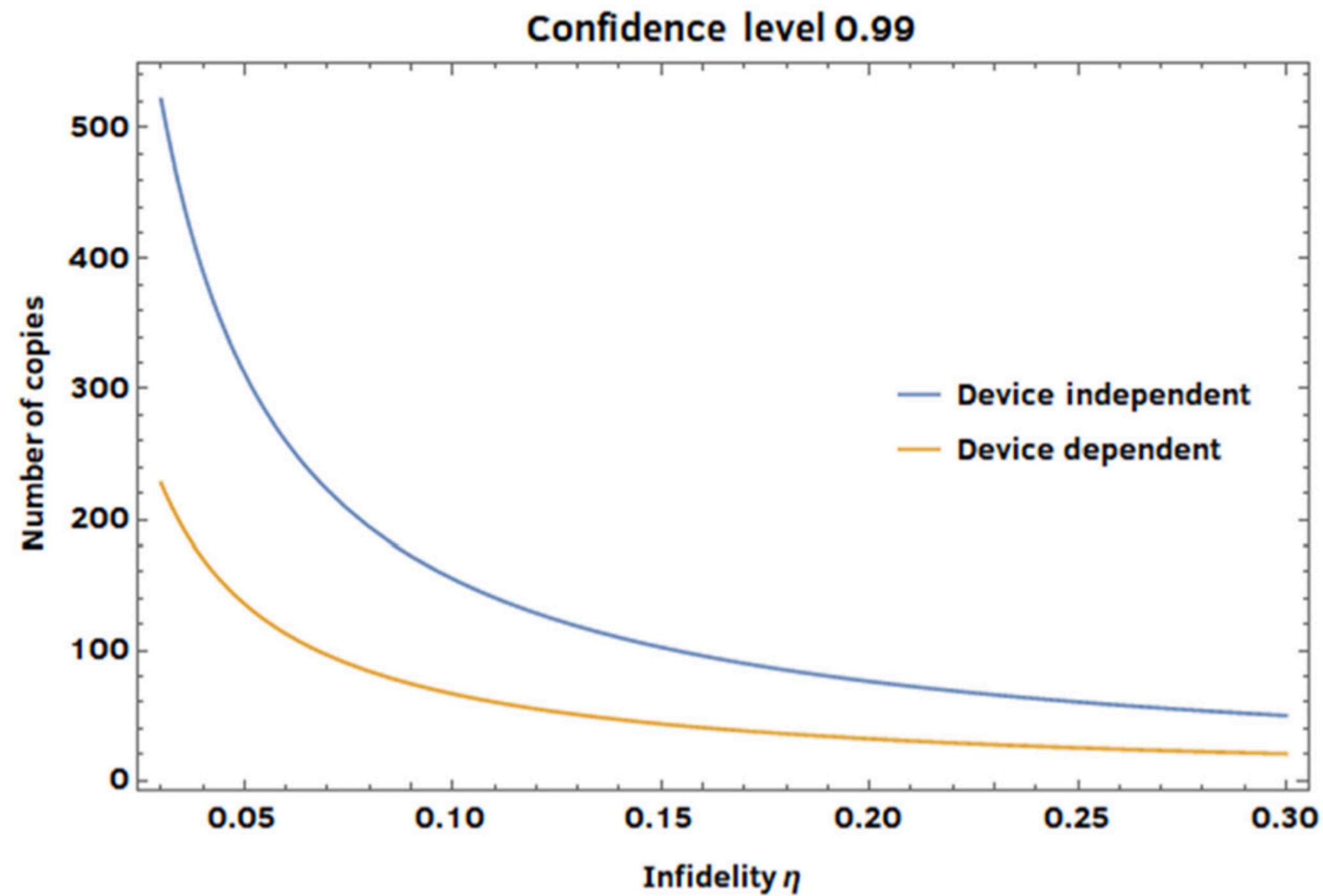
DIQSV protocol



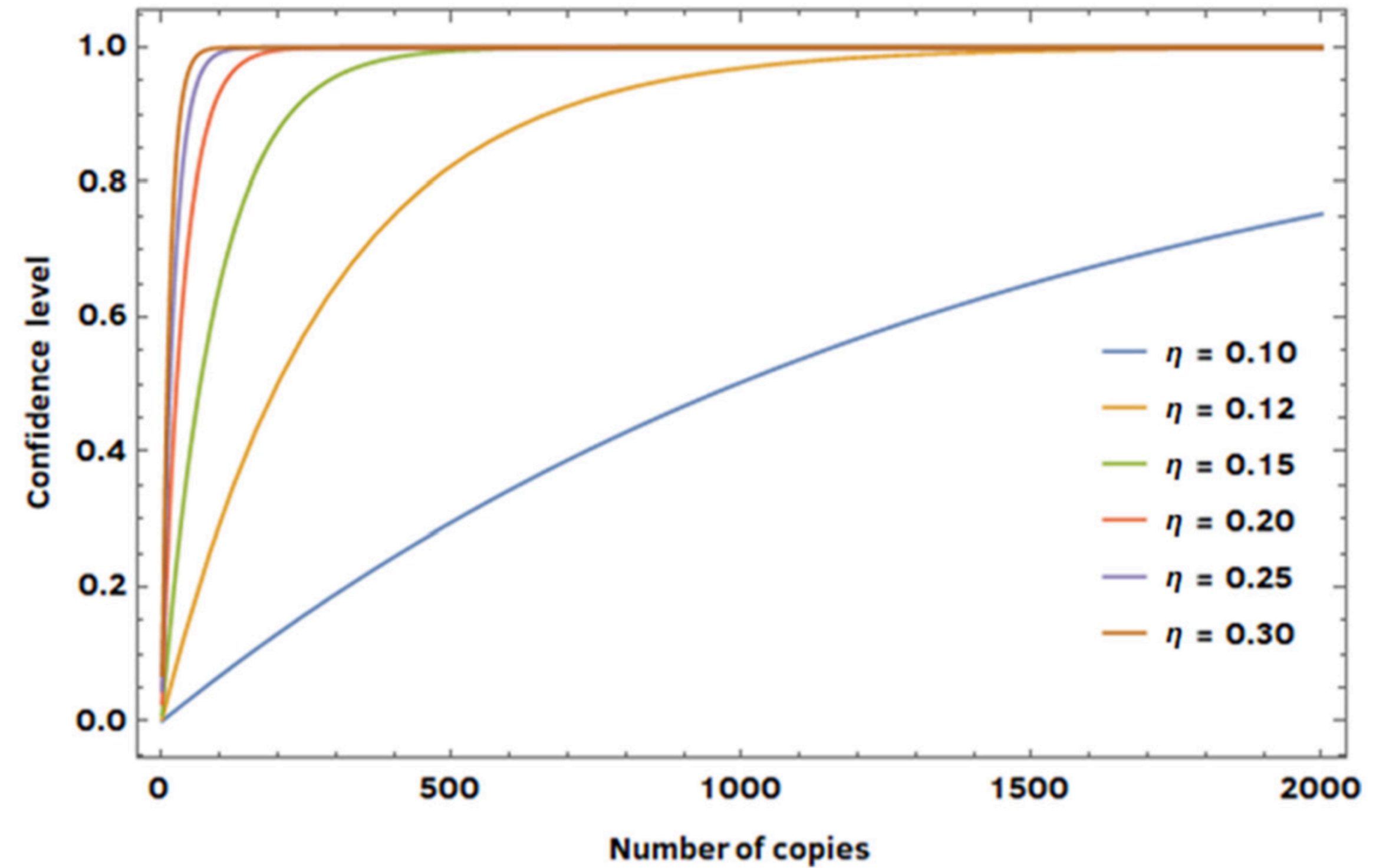
DIQSV main result

The entangled state ψ can be device-independently verified if there exists a robust self-test for it, which can be phrased as a nonlocal game. The verification test achieves optimal sample efficiency $O(\ln \delta^{-1}/c\epsilon)$ if the state saturates the algebraic bound of the corresponding nonlocal game. Otherwise, the state is verified with suboptimal sample efficiency $O(\ln \delta^{-1}/c^2\epsilon^2)$

Examples

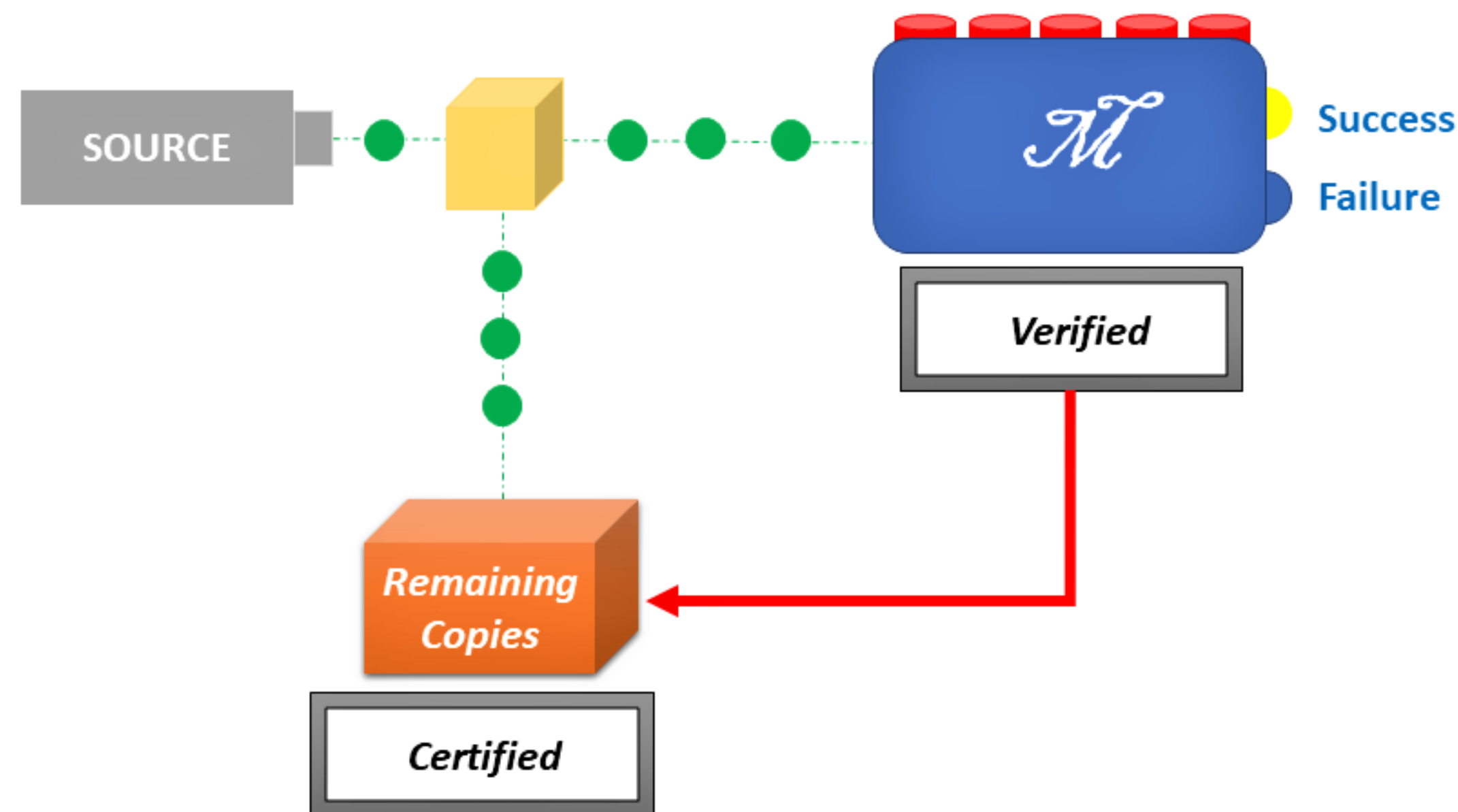


- GHZ verification



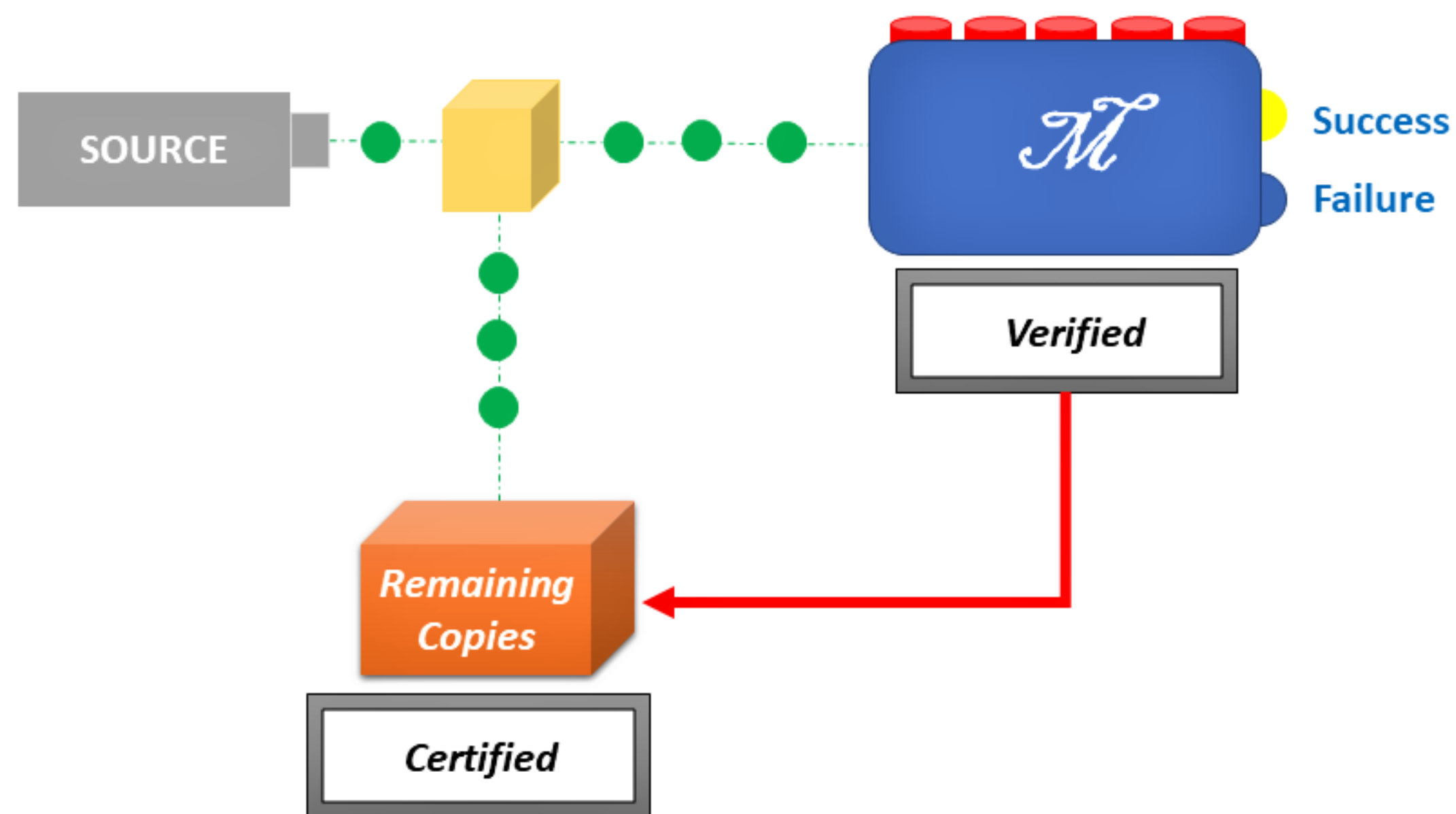
- DI GHZ verification when the success probability is 0.95

Framework for DI certification



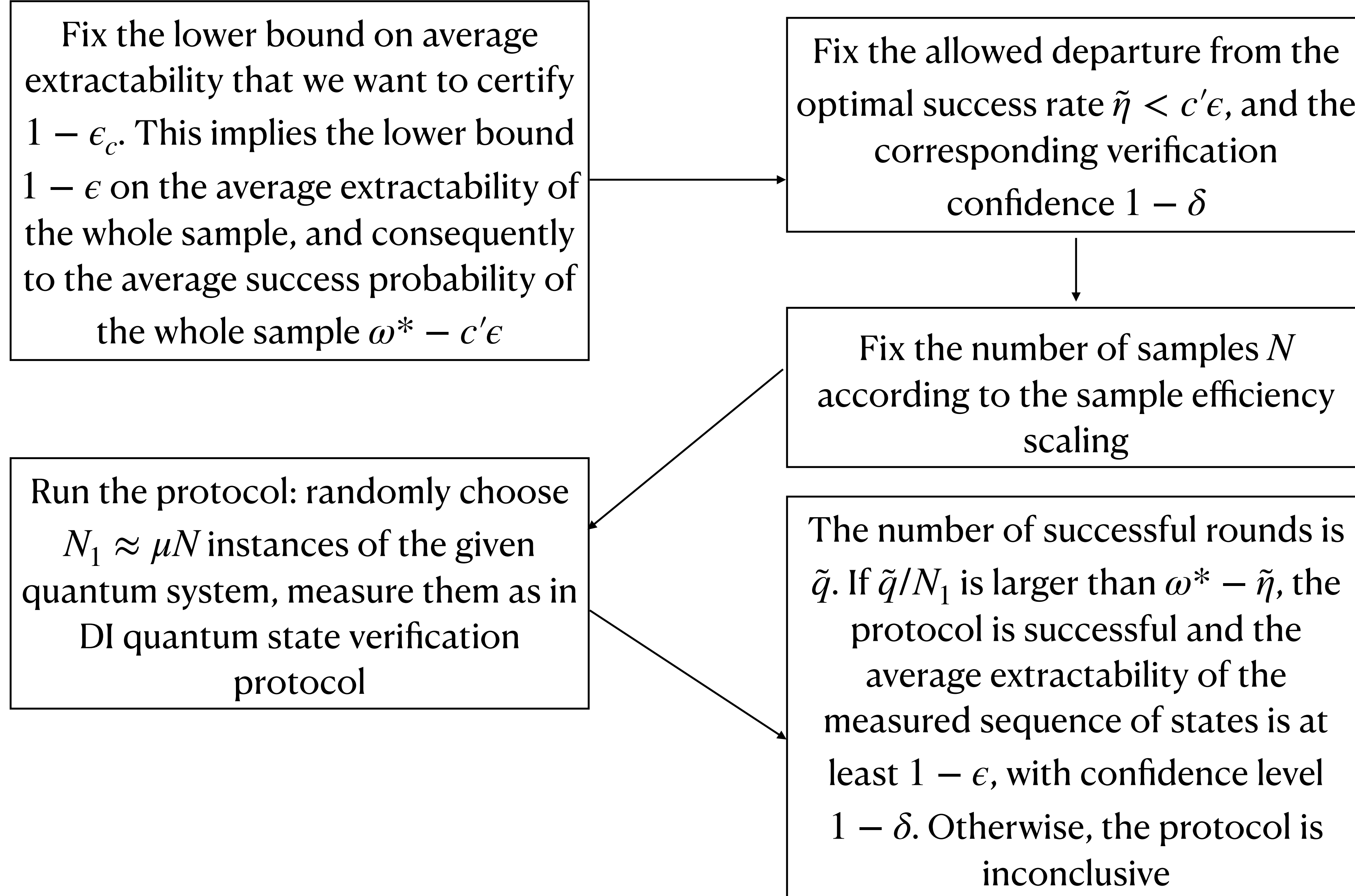
- Figure of merit: average conditional extractability
- $$\tilde{\sigma}_j \propto \text{Tr}_{1,\dots,j-1,j+1,\dots,N} \left[\bigotimes_{k=1}^{j-1} M_{o_k|i_k} \sigma^N \right]$$
- Difficult to define in this situation
 - Simplify the situation by assuming independence of samples (but not identity)
 - Figure of merit: **average extractability**

Framework for DI certification



- Randomly choose whether the copy will be measured or kept to be used in some protocol
- Perform DI QSV on the measured subset of copies
- The fact that copies to be measured are chosen **randomly**, imposes the permutational invariance of the whole state σ^N
- Using Markov's and Chernoff-Hoeffding inequalities

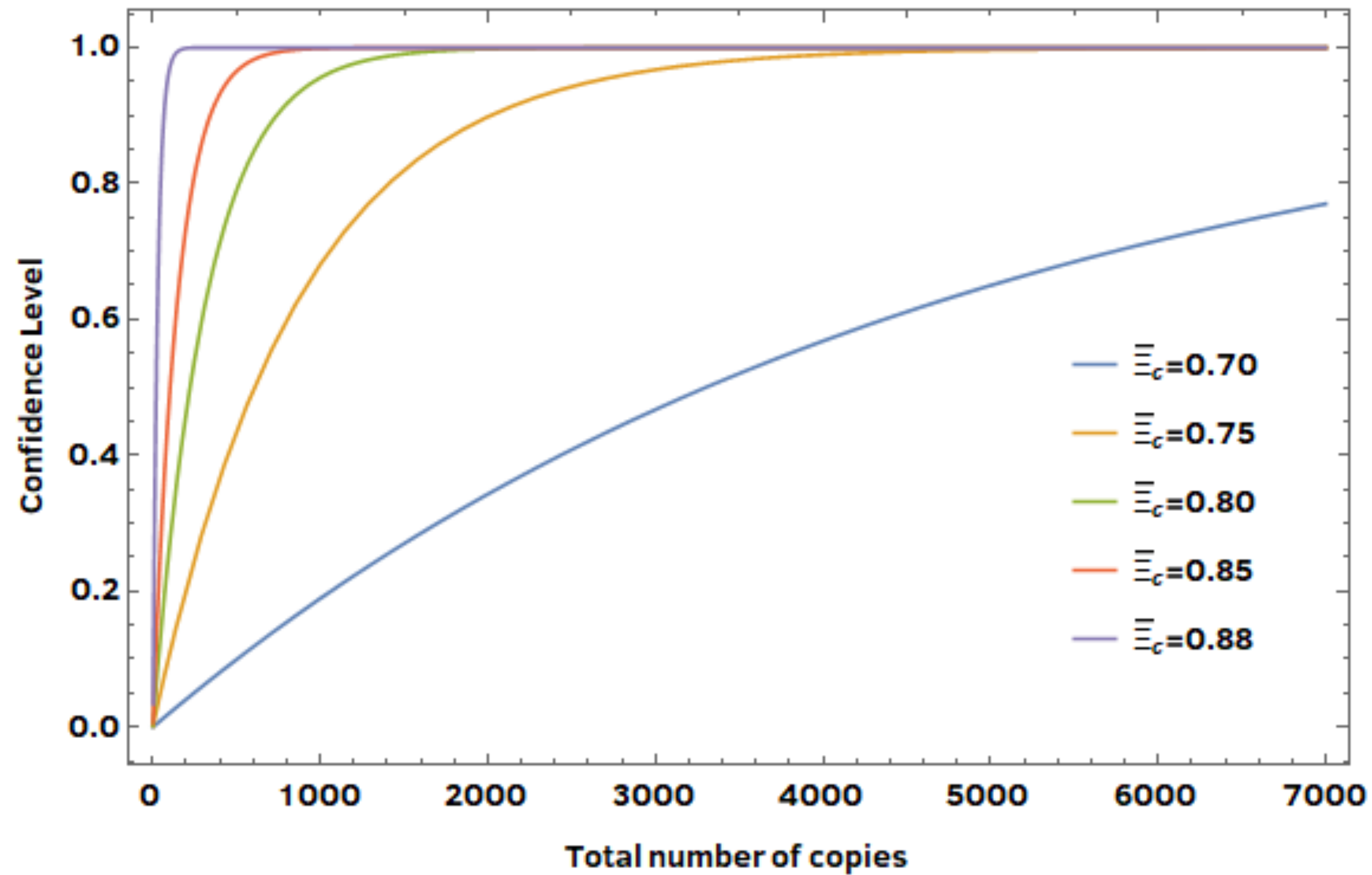
DIQSC protocol



DI QSC main result

The entangled state ψ can be device-independently certified if there exists a robust self-test for it, which can be phrased as a nonlocal game. The verification test achieves optimal sample efficiency $O(\ln \delta^{-1}/c\epsilon)$ if the state saturates the algebraic bound of the corresponding nonlocal game. Otherwise, the state is verified with suboptimal sample efficiency $O(\ln \delta^{-1}/c^2\epsilon^2)$

Examples



- GHZ certification with success rate 0.98 and $\mu = 0.5$

Final thoughts

- Device-independent quantum state verification, in general, has the same sample efficiency scaling as device-dependent one and constants are gentle
- Fully non-IID scenario
- In case of preserved copies, the scaling of the sample efficiency can still be optimal, but constants can get more nasty
- ID scenario
- Self-testing and robust self-testing play the key role!