Device-independent protocols from computational assumptions

Tony Metger (ETH Zürich)

Joint work with

Rotem Arnon-Friedman
(Weizmann Institute)

Andrea Coladangelo
(UC Berkeley)

Yfke Dulek
(CWI & QuSoft)

Thomas Vidick
(Caltech)

Self-testing of a single quantum device under computational assumptions, arXiv:2001.09161.

Device-independent quantum key distribution from computational assumptions, arXiv:2010.04175.

Outline

Outline

1. Setting for “standard” DIQKD

Outline

1. Setting for “standard” DIQKD

security based on Bell inequality violation

Outline

1. Setting for “standard” DIQKD

security based on Bell inequality violation

2. Setting for “computational” DIQKD

Outline

1. Setting for “standard” DIQKD ← security based on Bell inequality violation
2. Setting for “computational” DIQKD ← can’t base security on Bell inequality violation

Outline

1. Setting for “standard” DIQKD ← security based on Bell inequality violation
2. Setting for “computational” DIQKD ← can’t base security on Bell inequality violation
3. Main technical tool: computational self-testing

Outline

1. Setting for “standard” DIQKD ← security based on Bell inequality violation
2. Setting for “computational” DIQKD ← can’t base security on Bell inequality violation
3. Main technical tool: computational self-testing

replaces Bell inequality violation

Device-independent QKD

Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.

Device-independent QKD

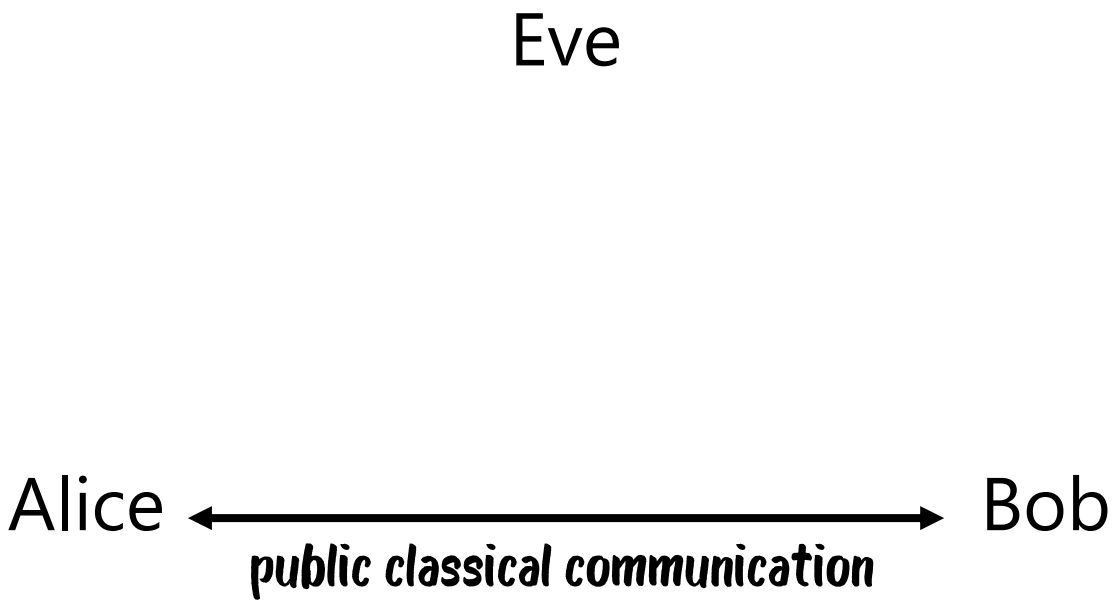
Eve

Alice

Bob

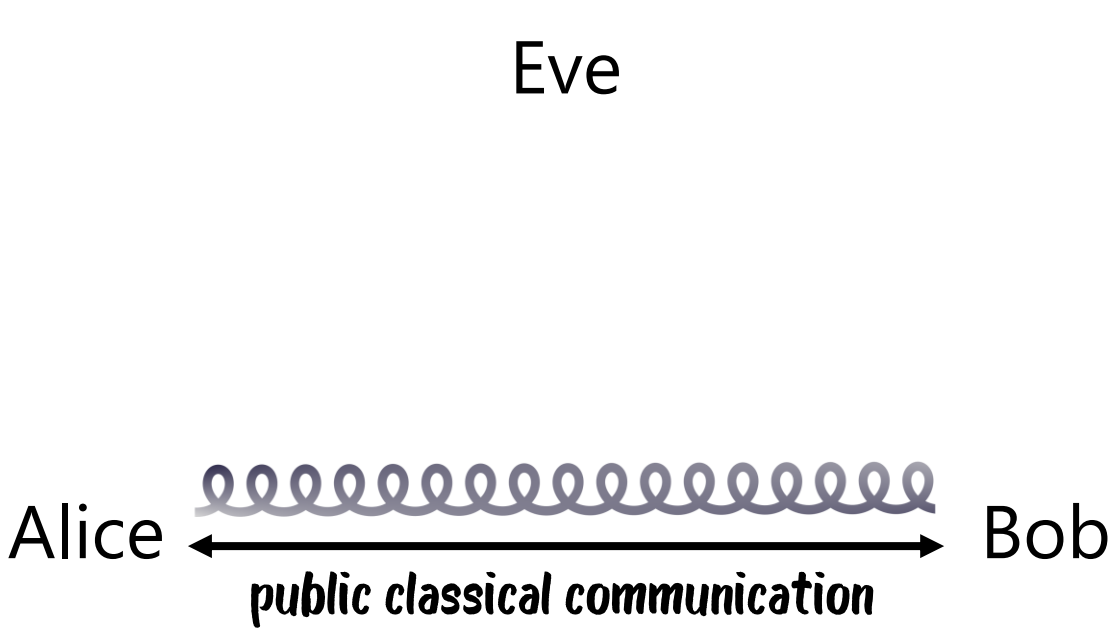
Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.

Device-independent QKD



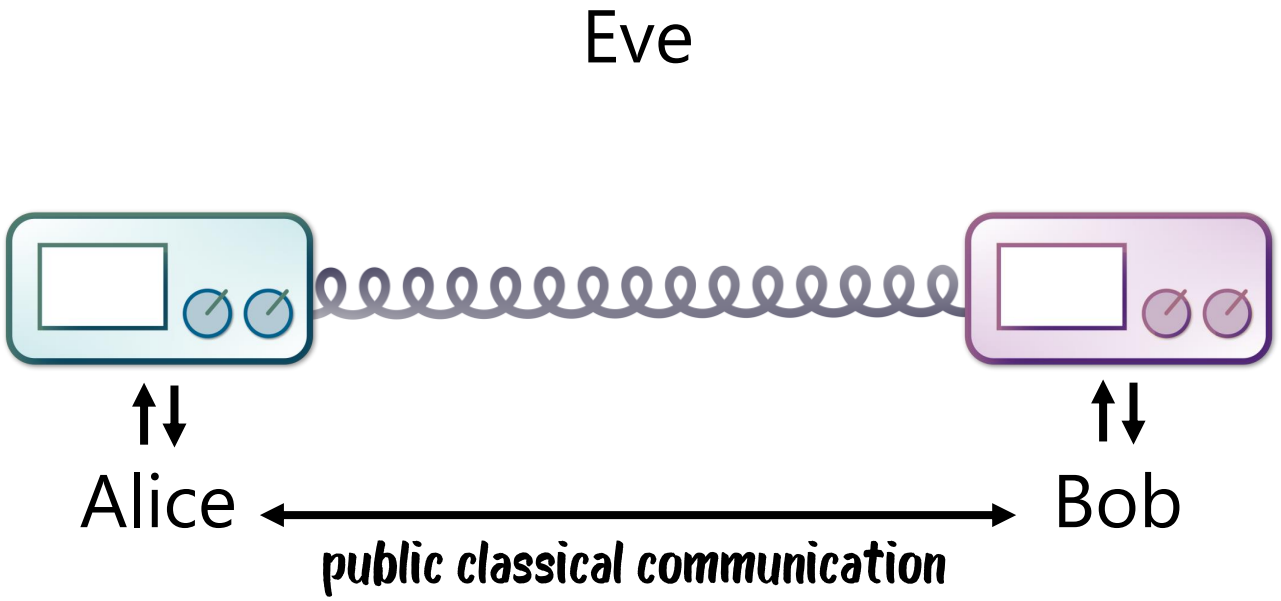
Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.

Device-independent QKD



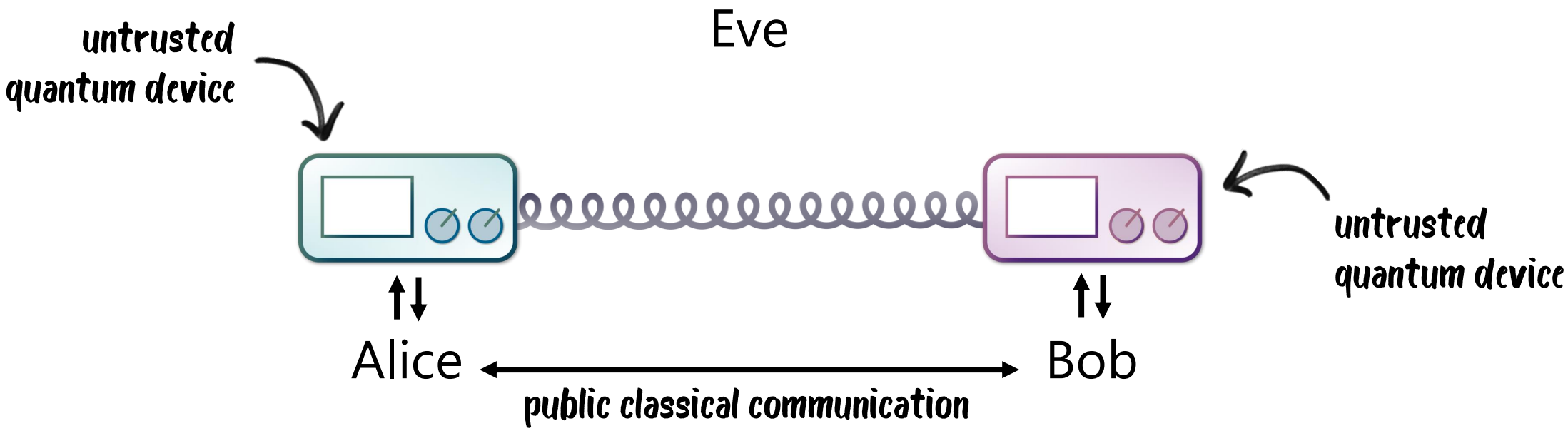
Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.

Device-independent QKD



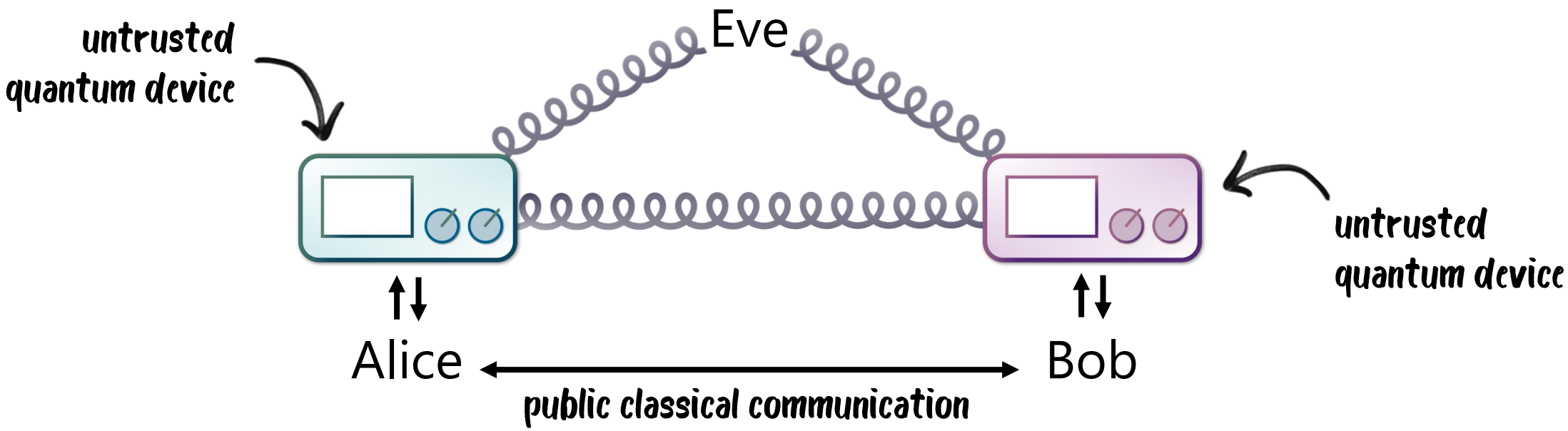
Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.

Device-independent QKD



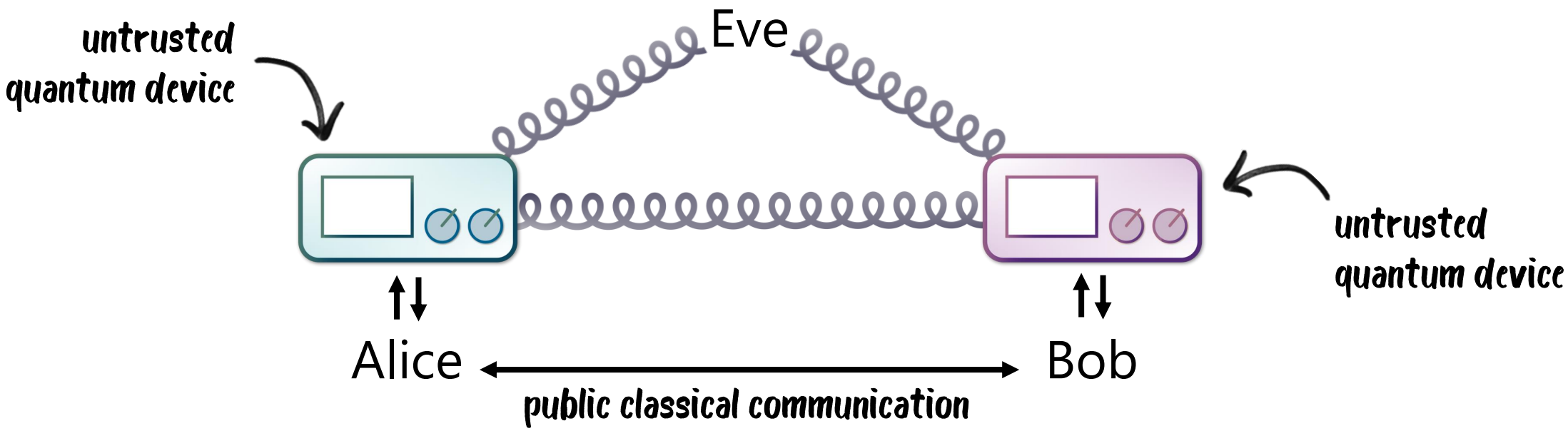
Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.

Device-independent QKD



Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.

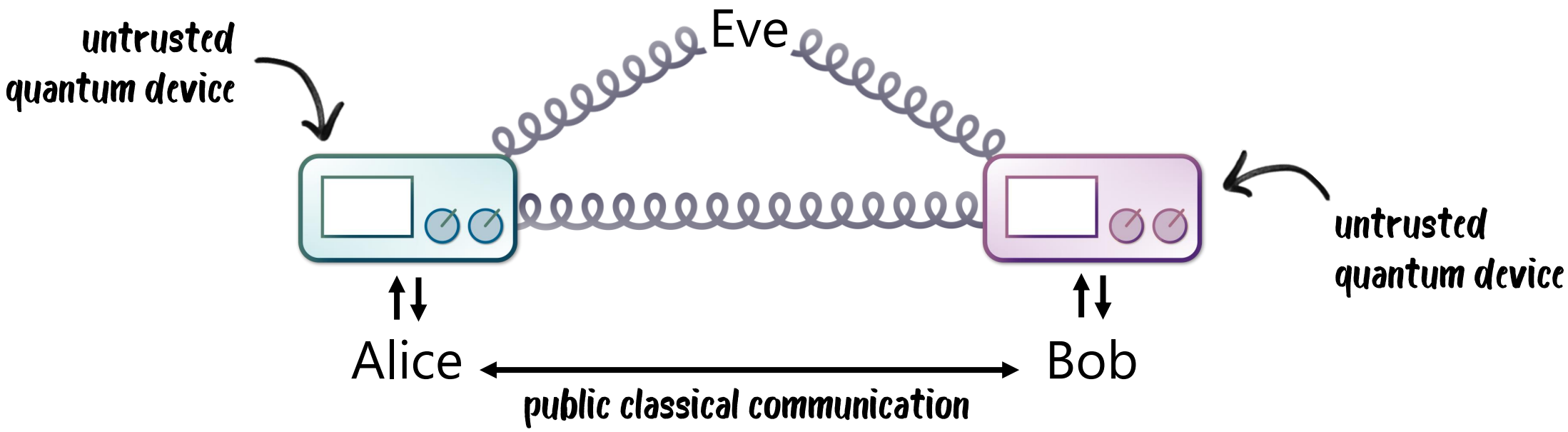
Device-independent QKD



Bell inequality
violation

Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.

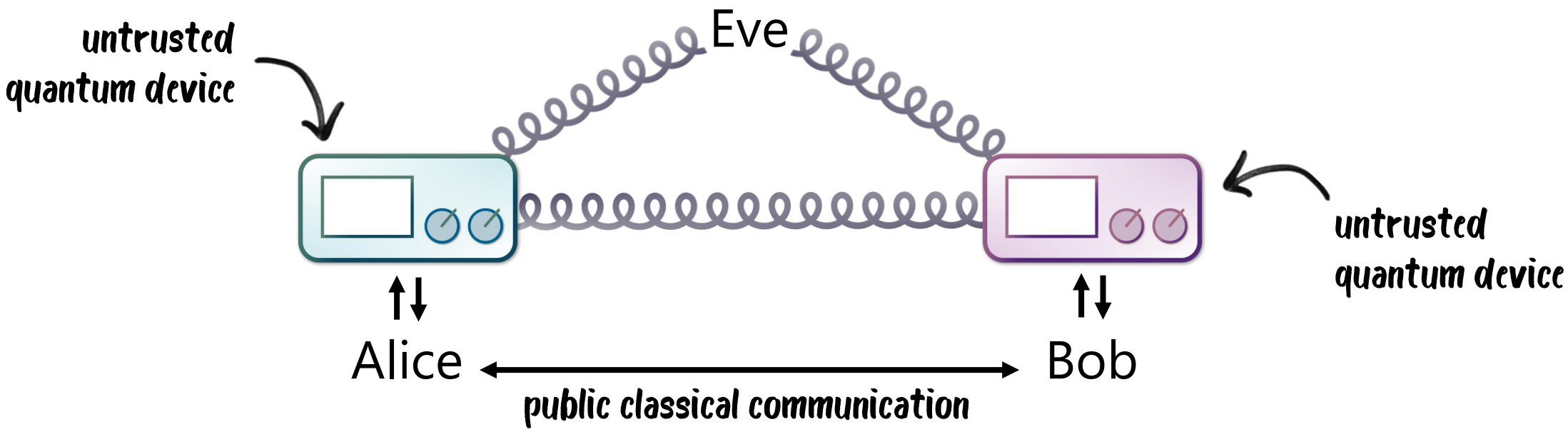
Device-independent QKD



Bell inequality violation → Statement about devices' states and measurements

Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.

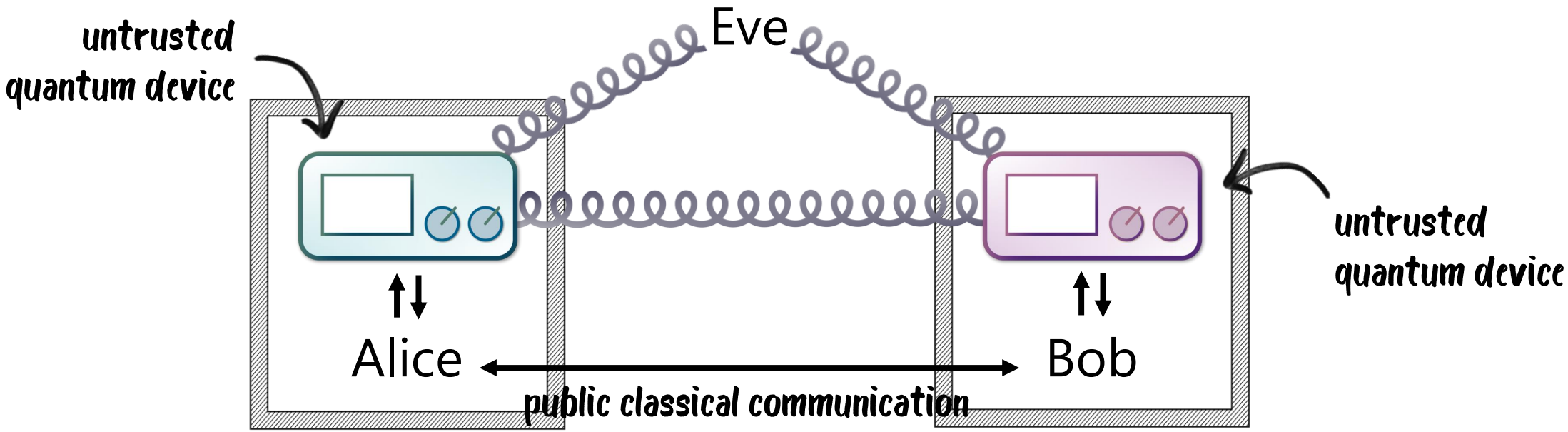
Device-independent QKD



Bell inequality violation → Statement about devices' states and measurements → **Information-theoretic security** of final key

Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.

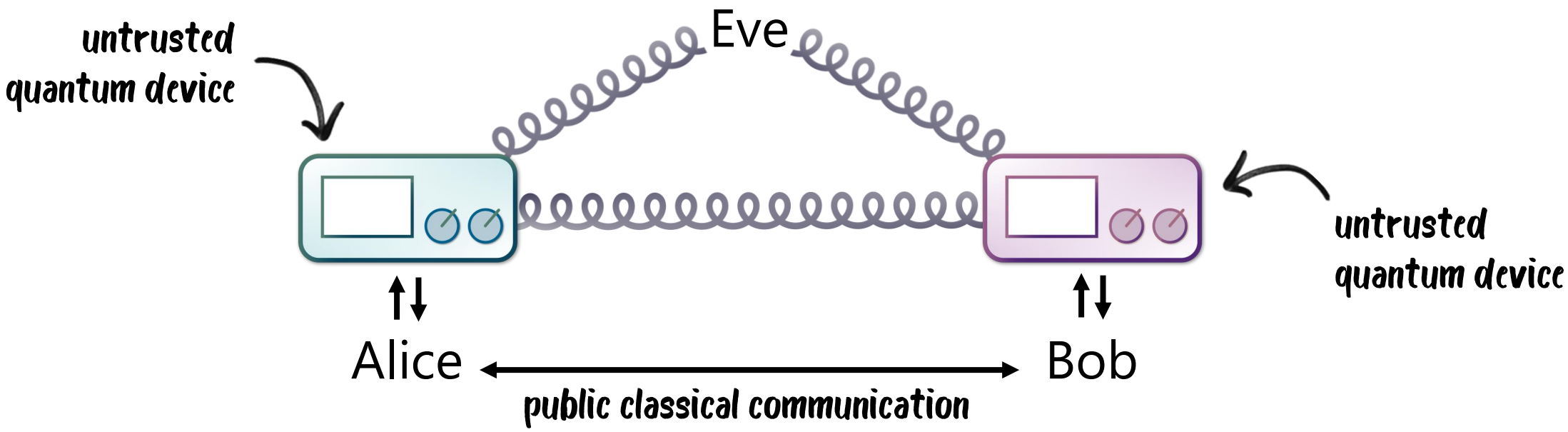
Device-independent QKD



Bell inequality violation → Statement about devices' states and measurements → **Information-theoretic security** of final key

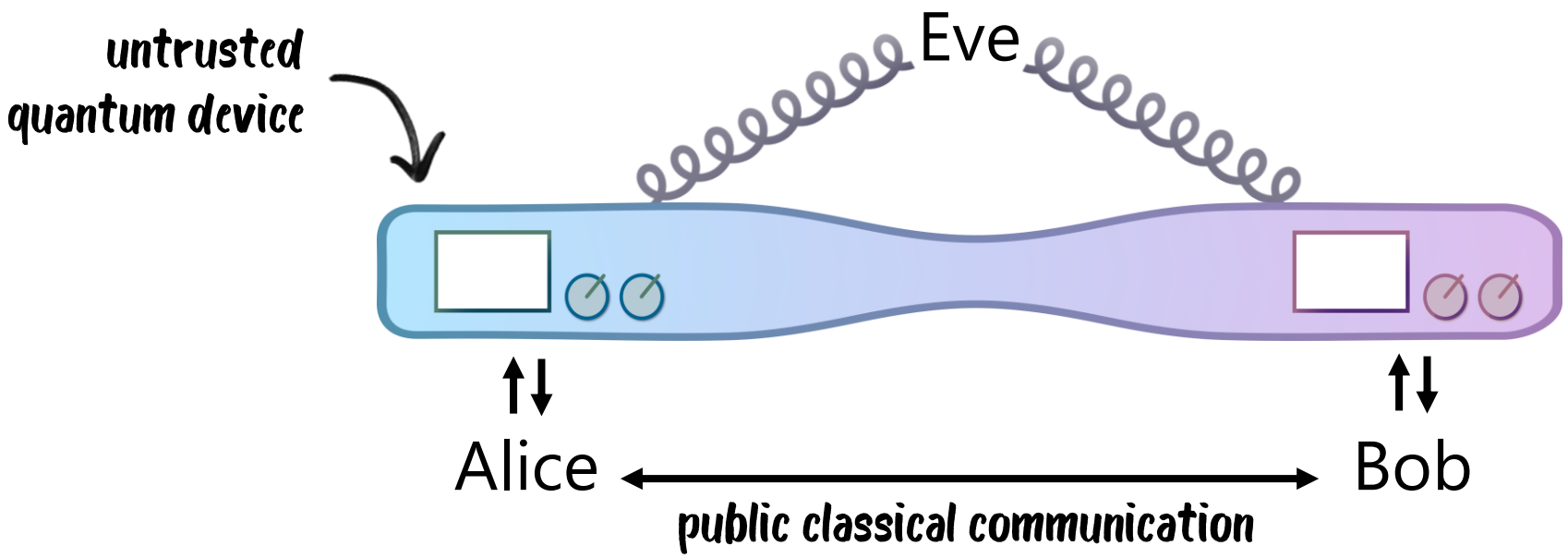
Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.

Device-independent QKD



Bell inequality violation → Statement about devices' states and measurements → **Information-theoretic security** of final key

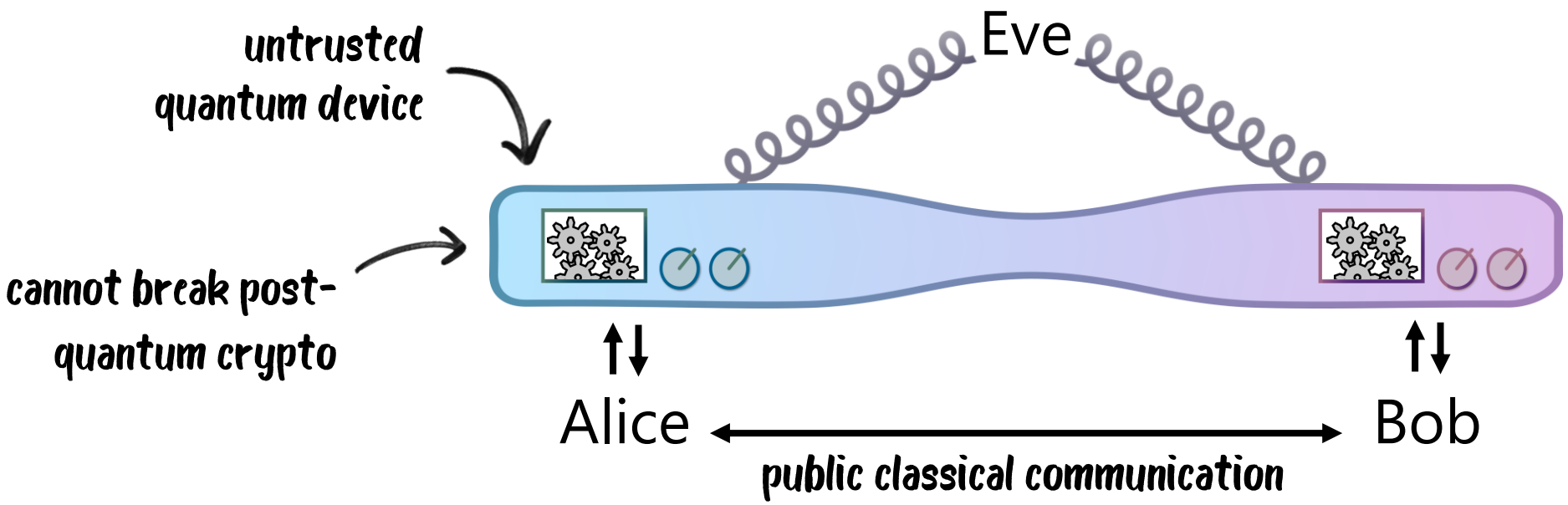
Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.



Bell inequality violation → Statement about devices' states and measurements → **Information-theoretic security** of final key

Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.

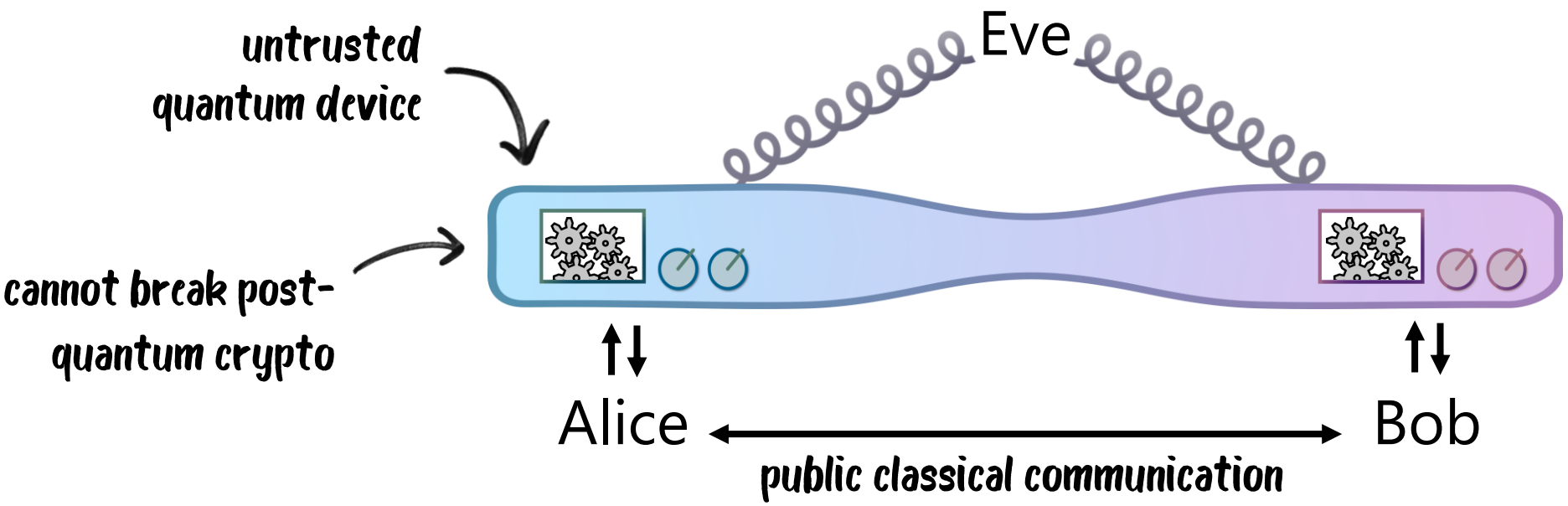
Computational DIQKD setting



Bell inequality violation → Statement about devices' states and measurements → **Information-theoretic security** of final key

Brakerski et al., A cryptographic test of quantumness and certifiable randomness from a single quantum device, FOCS 2018.
Mahadev, Classical Verification of Quantum Computations, FOCS 2018
Gheorghiu & Vidick, Computationally-secure and composable remote state preparation, FOCS 2019.

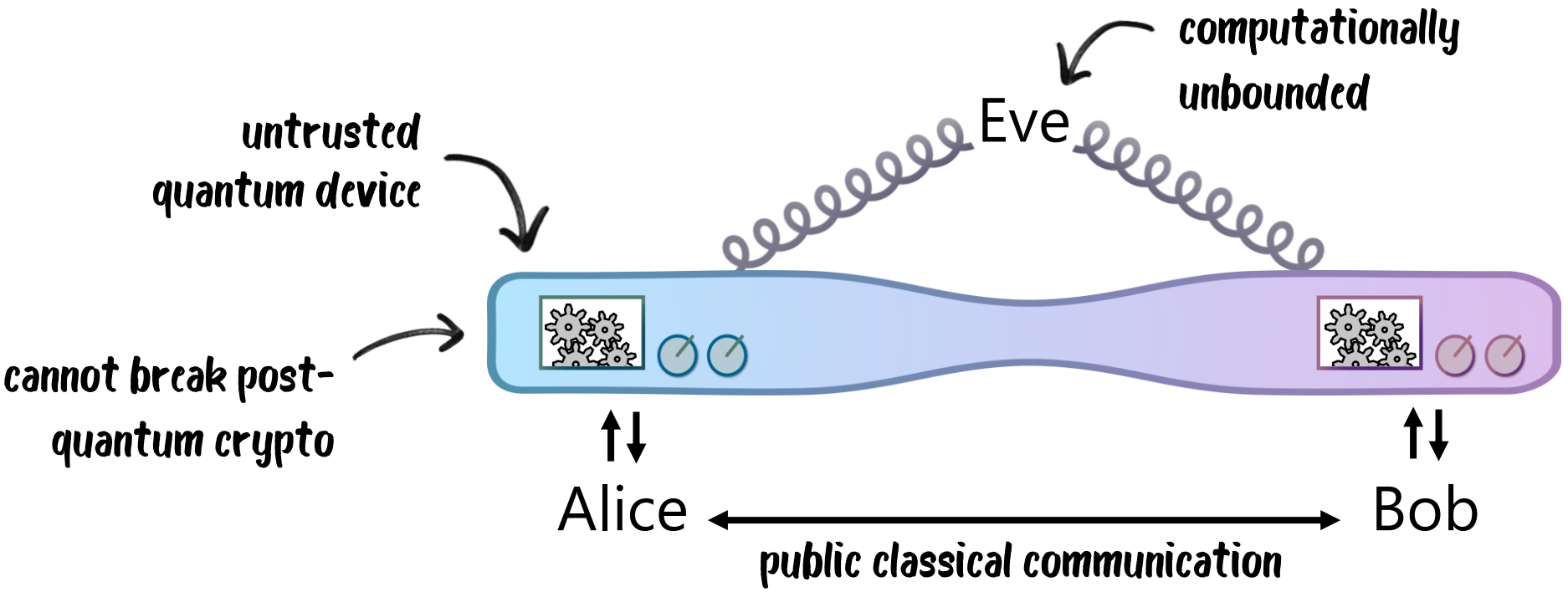
Computational DIQKD setting



Interactive protocol with **computational assumption** → Statement about devices' states and measurements → **Information-theoretic security** of final key

Brakerski et al., A cryptographic test of quantumness and certifiable randomness from a single quantum device, FOCS 2018.
Mahadev, Classical Verification of Quantum Computations, FOCS 2018
Gheorghiu & Vidick, Computationally-secure and composable remote state preparation, FOCS 2019.

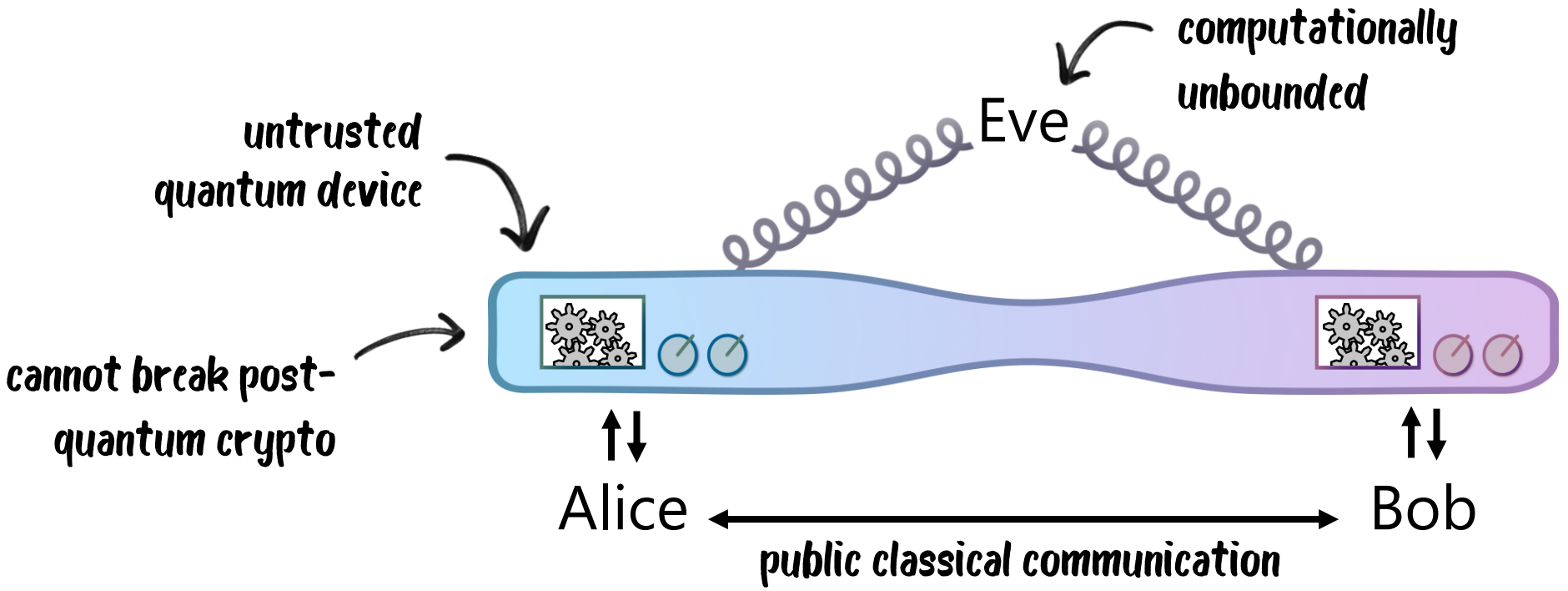
Computational DIQKD setting



Interactive protocol with **computational assumption** → Statement about devices' states and measurements → **Information-theoretic security** of final key

Brakerski et al., A cryptographic test of quantumness and certifiable randomness from a single quantum device, FOCS 2018.
Mahadev, Classical Verification of Quantum Computations, FOCS 2018
Gheorghiu & Vidick, Computationally-secure and composable remote state preparation, FOCS 2019.

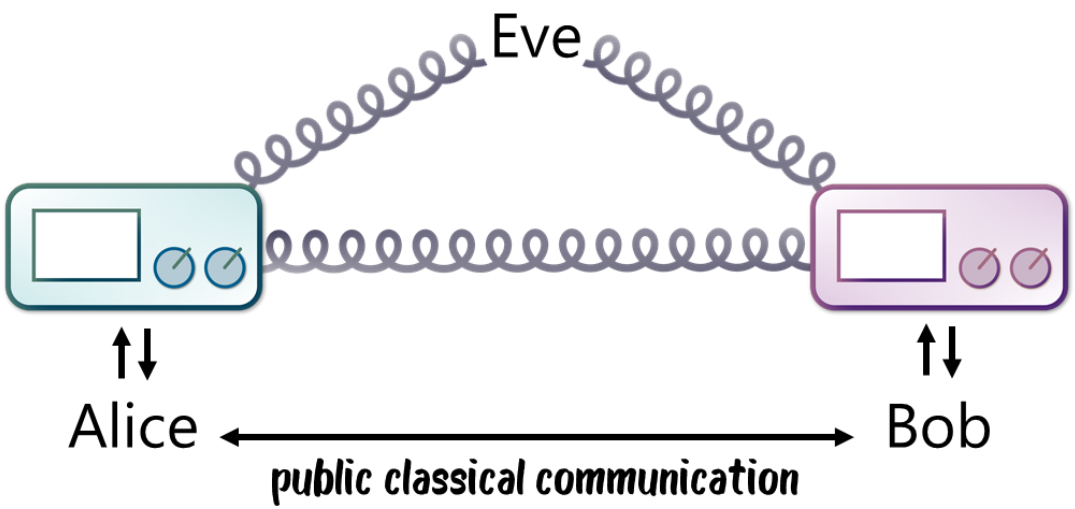
Computational DIQKD setting

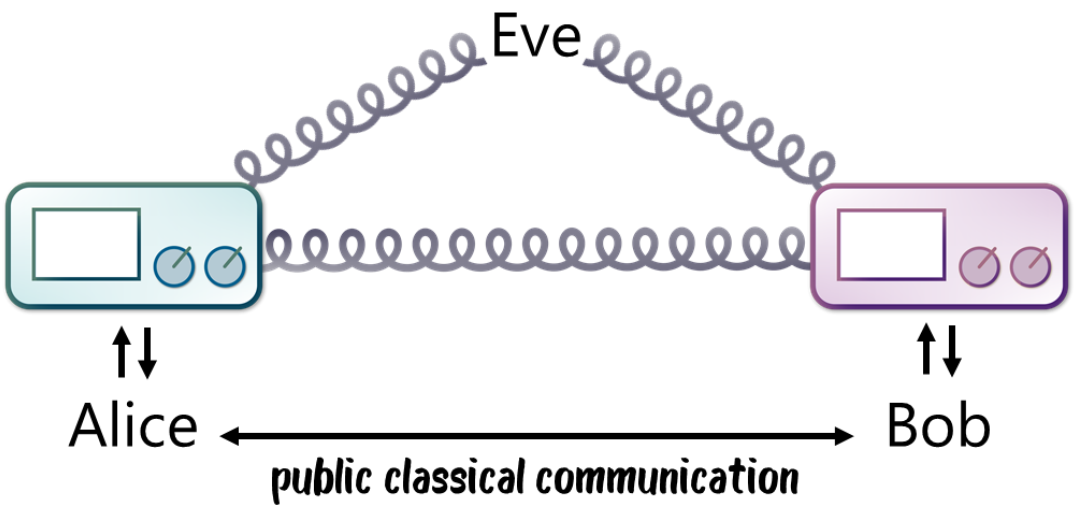


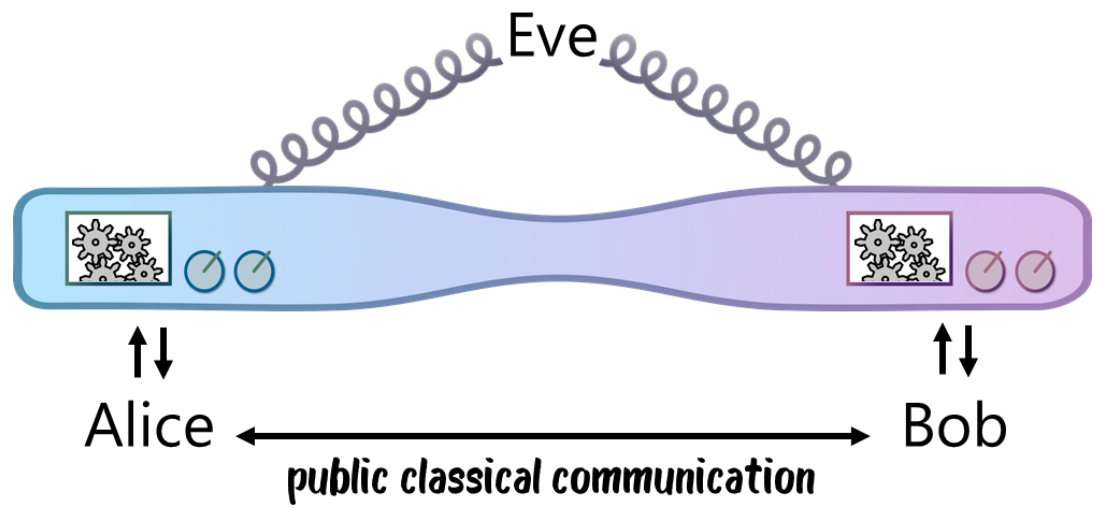
Interactive protocol with **computational assumption** → Statement about devices' states and measurements → **Information-theoretic security** of final key

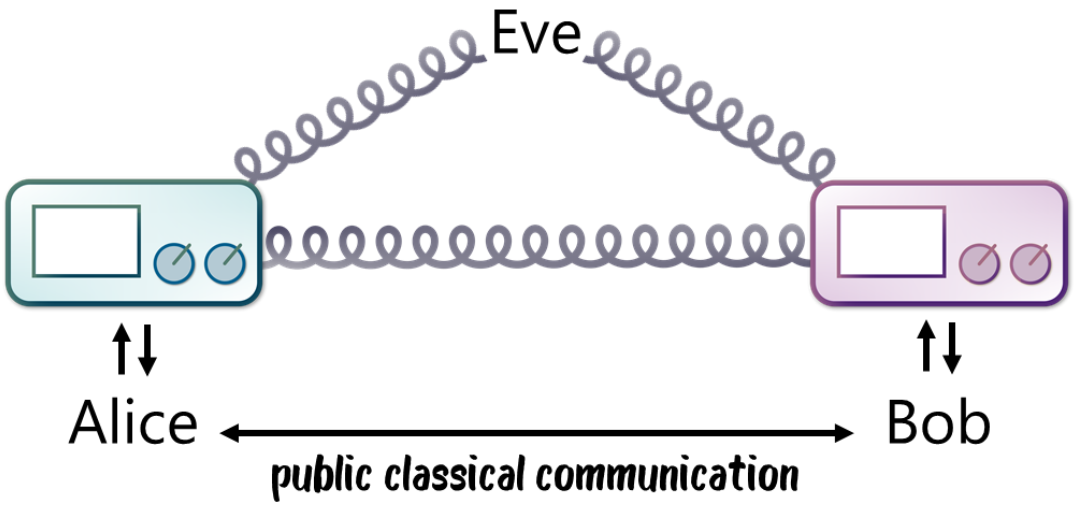
required only for duration of the protocol

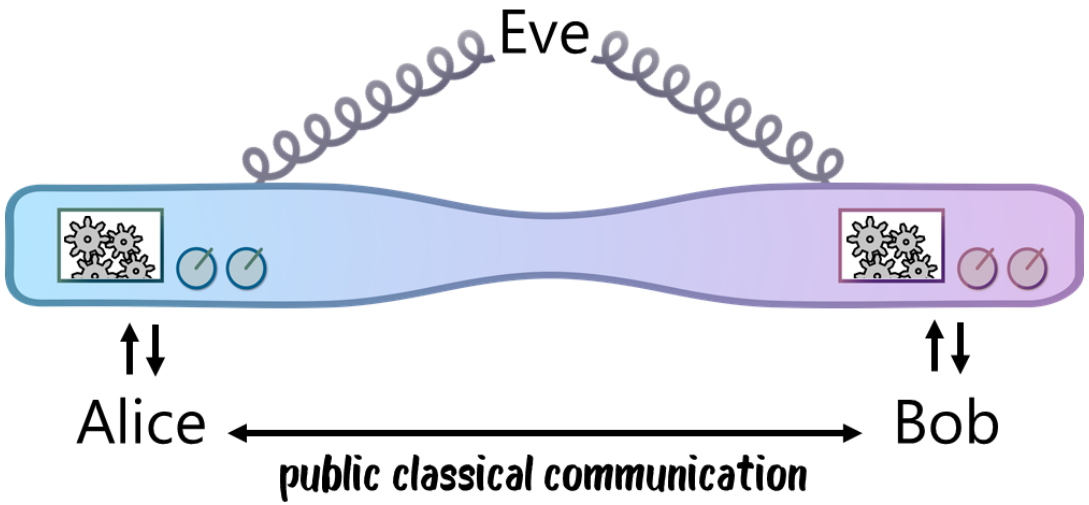
Brakerski et al., A cryptographic test of quantumness and certifiable randomness from a single quantum device, FOCS 2018.
Mahadev, Classical Verification of Quantum Computations, FOCS 2018
Gheorghiu & Vidick, Computationally-secure and composable remote state preparation, FOCS 2019.


Eve
Alice
Bob
public classical communication


Eve
Alice
Bob
public classical communication


Eve
Alice
Bob
public classical communication





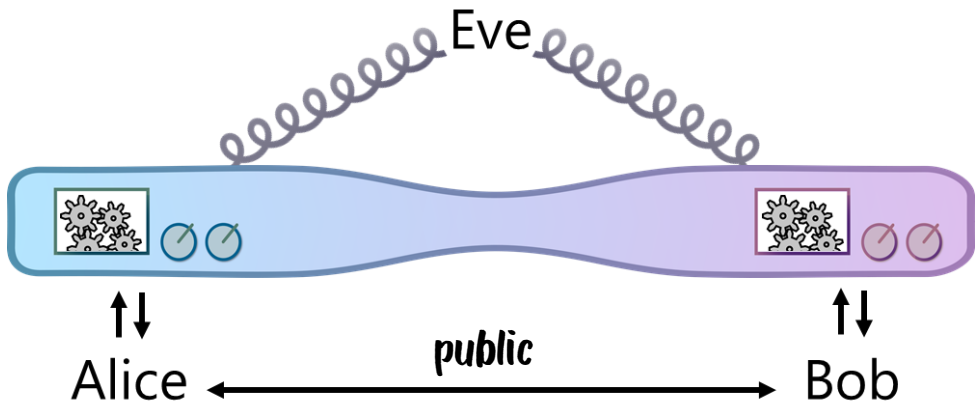
Extra requirement: **honest** devices should be able to succeed in the protocol with pre-shared EPR pairs and local operations

Computational self-testing protocol

Computational self-testing

Classical **interactive protocol** run by Alice and Bob

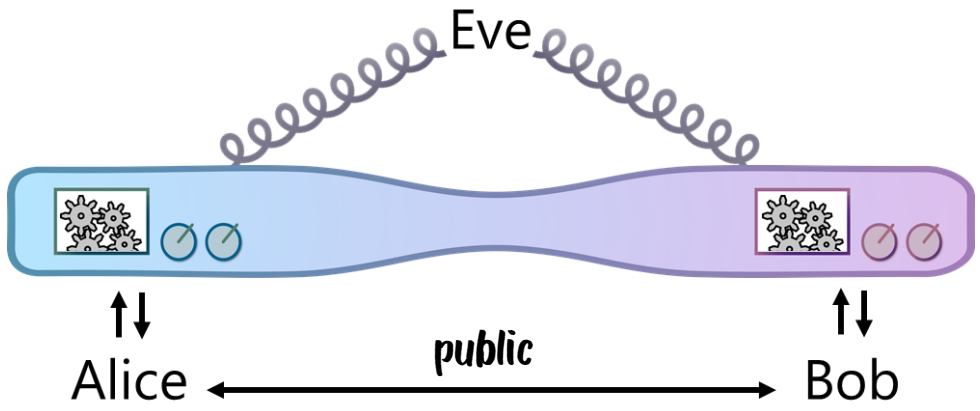
Device can win or lose



Computational self-testing

Classical **interactive protocol** run by Alice and Bob

Device can win or lose

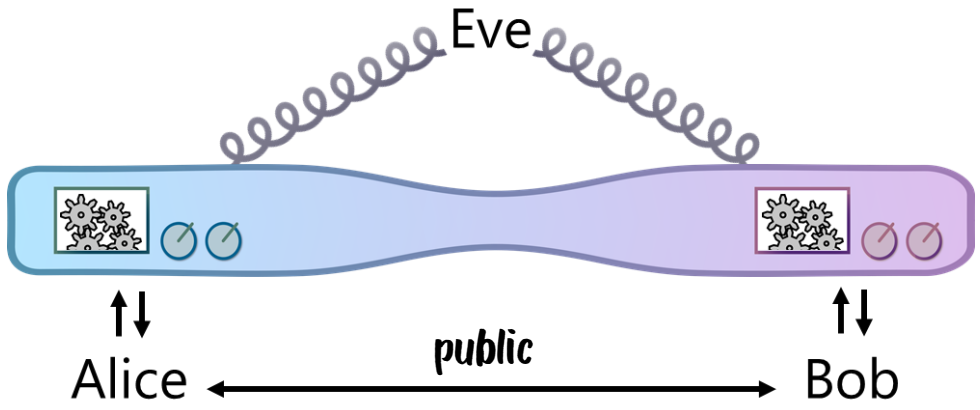


If a **computationally bounded device** wins with probability (close to) 1:

Computational self-testing

Classical **interactive protocol** run by Alice and Bob

Device can win or lose



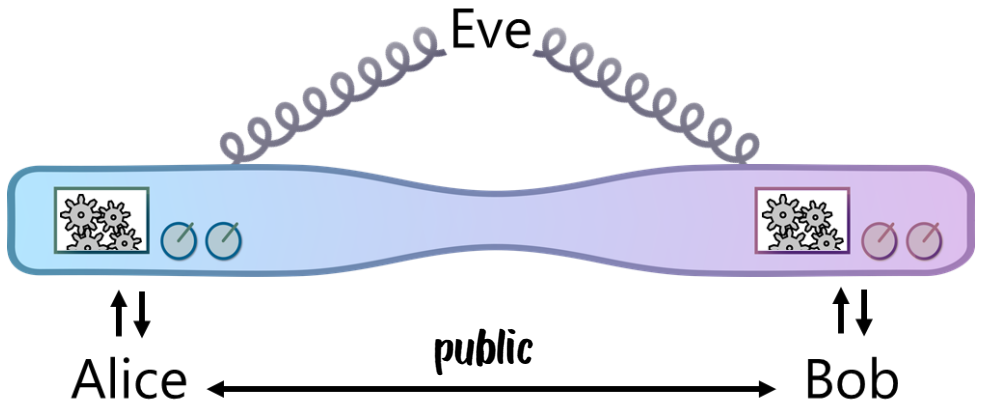
If a **computationally bounded device** wins with probability (close to) 1:

- the **state** prepared by the device must have been an EPR pair

Computational self-testing

Classical **interactive protocol** run by Alice and Bob

Device can win or lose



If a **computationally bounded device** wins with probability (close to) 1:

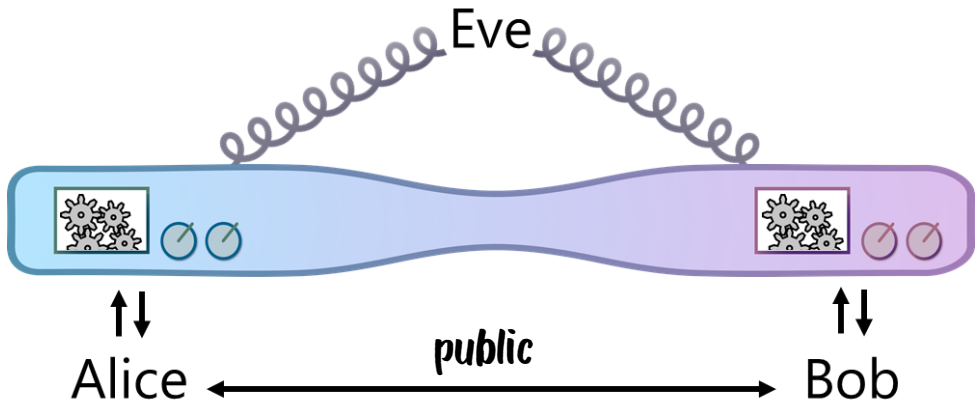
- the **state** prepared by the device must have been an EPR pair
- the device must have **measured** each qubit in the bases requested by Alice and Bob, respectively

Computational self-testing

Classical **interactive protocol** run by

Alice and Bob

Device can win or lose



If a **computationally bounded device** wins with probability (close to) 1:

- the **state** prepared by the device must have been an EPR pair
- the device must have **measured** each qubit in the bases requested by Alice and Bob, respectively

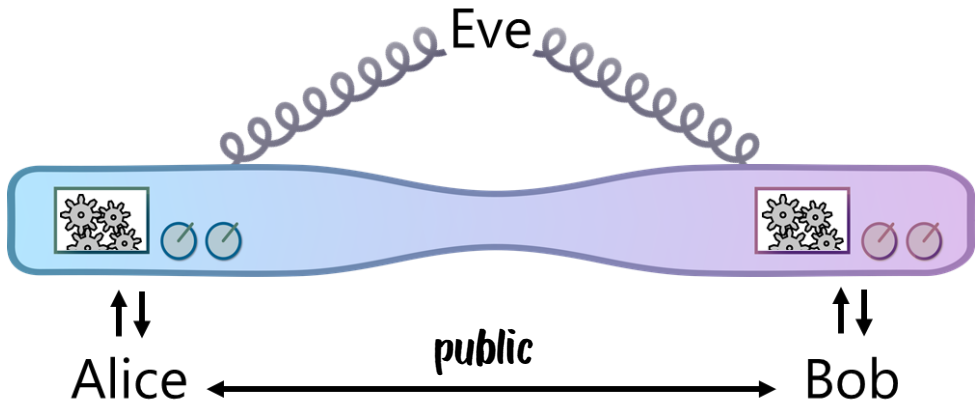
up to **global** changes of basis.

Computational self-testing

Classical **interactive protocol** run by

Alice and Bob

Device can win or lose

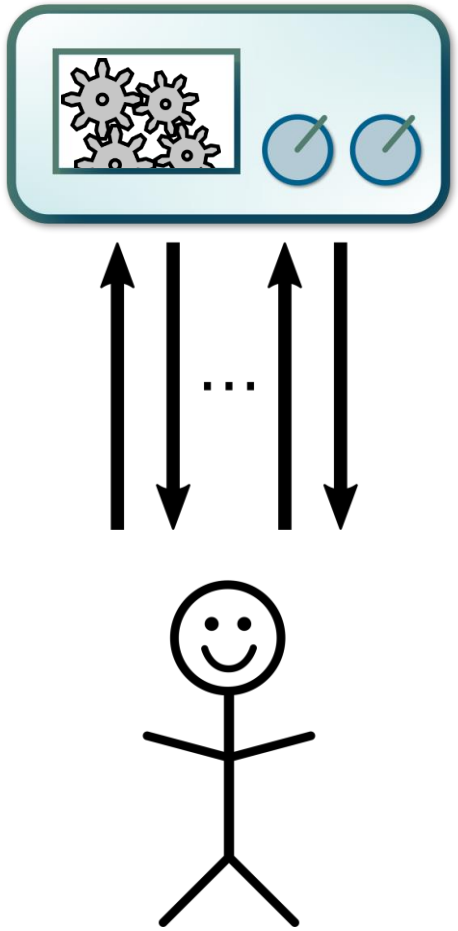


If a **computationally bounded device** wins with probability (close to) 1:

- the **state** prepared by the device must have been an EPR pair
- the device must have **measured** each qubit in the bases requested by Alice and Bob, respectively

up to **global** changes of basis.

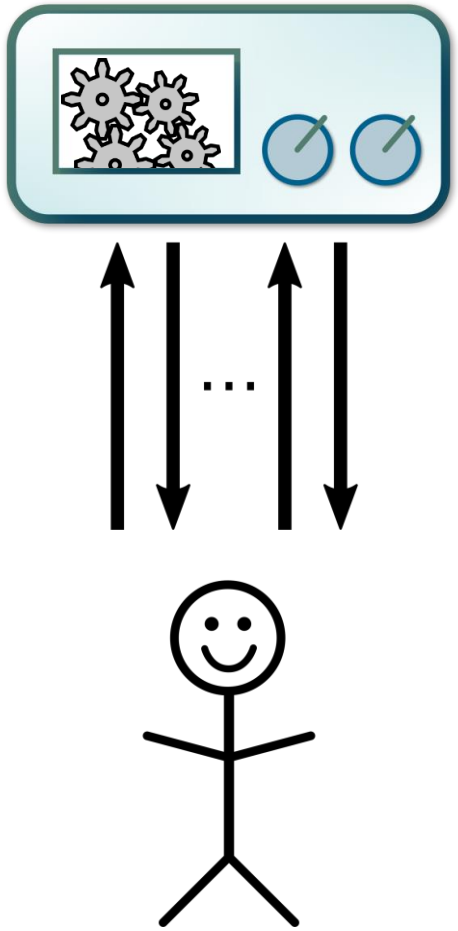
Previous work



- Certifiable information-theoretic randomness expansion (Brakerski et al. 2018)

Brakerski et al., A cryptographic test of quantumness and certifiable randomness from a single quantum device, FOCS 2018.
Mahadev, Classical Verification of Quantum Computations, FOCS 2018
Gheorghiu & Vidick, Computationally-secure and composable remote state preparation, FOCS 2019.

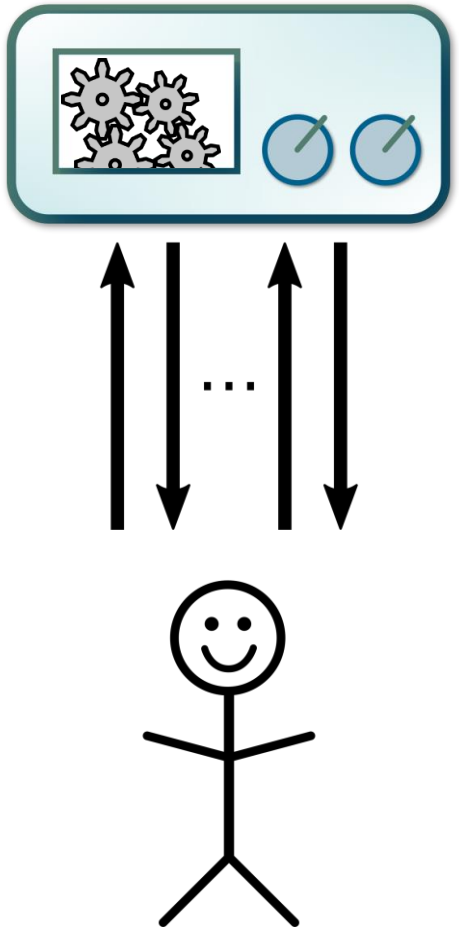
Previous work



- Certifiable information-theoretic randomness expansion (Brakerski et al. 2018)
- **Verification** of quantum computation (Mahadev 2018)

Brakerski et al., A cryptographic test of quantumness and certifiable randomness from a single quantum device, FOCS 2018.
Mahadev, Classical Verification of Quantum Computations, FOCS 2018
Gheorghiu & Vidick, Computationally-secure and composable remote state preparation, FOCS 2019.

Previous work

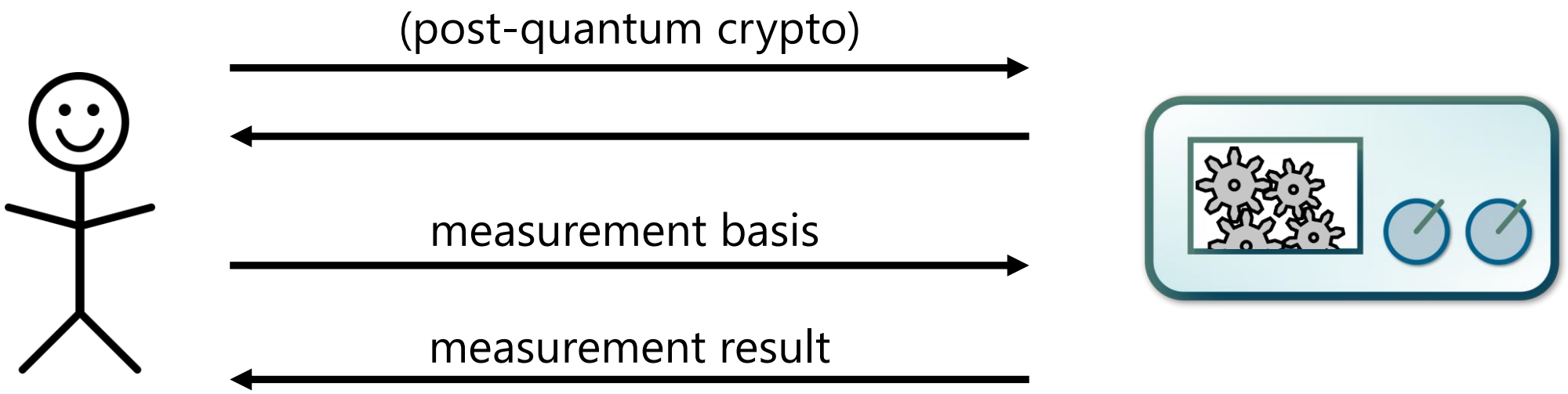


- Certifiable information-theoretic randomness expansion (Brakerski et al. 2018)
- **Verification** of quantum computation (Mahadev 2018)
- **Remote state preparation** (Gheorghiu, Vidick 2019)

Brakerski et al., A cryptographic test of quantumness and certifiable randomness from a single quantum device, FOCS 2018.
Mahadev, Classical Verification of Quantum Computations, FOCS 2018
Gheorghiu & Vidick, Computationally-secure and composable remote state preparation, FOCS 2019.

Remote state preparation [GV'19]

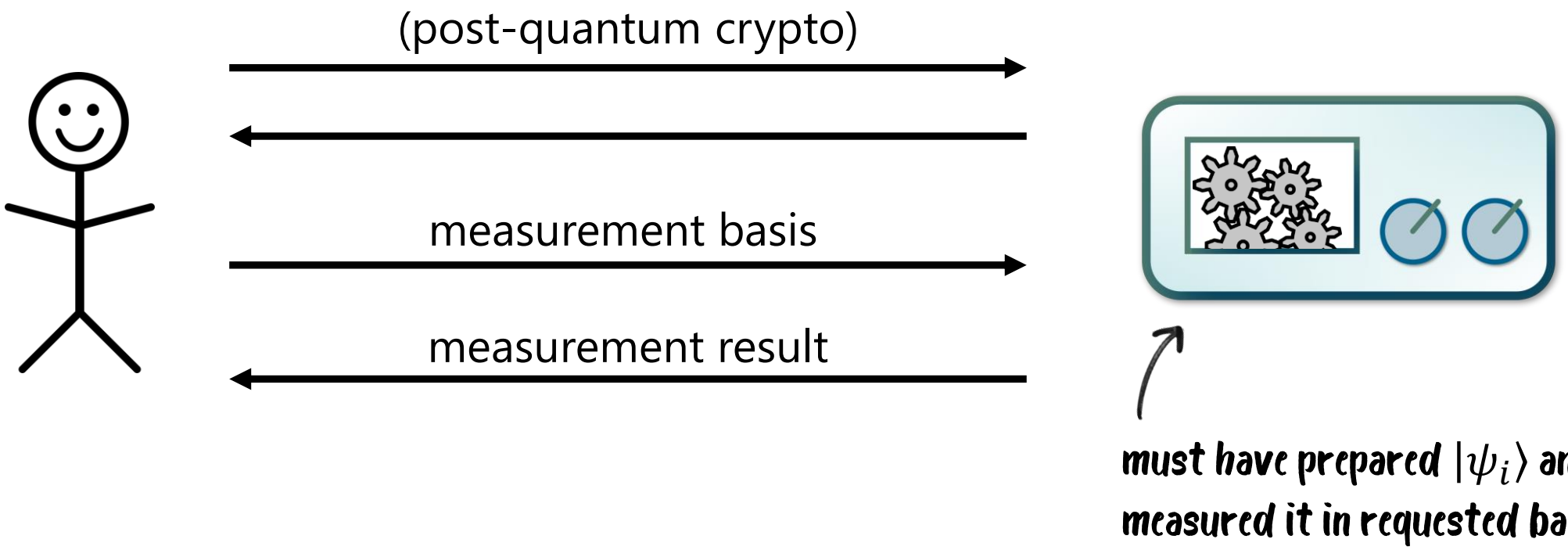
Given: set of **single-qubit** states $\{|\psi_i\rangle\} = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$



Gheorghiu & Vidick, Computationally-secure and composable remote state preparation, FOCS 2019.

Remote state preparation [GV'19]

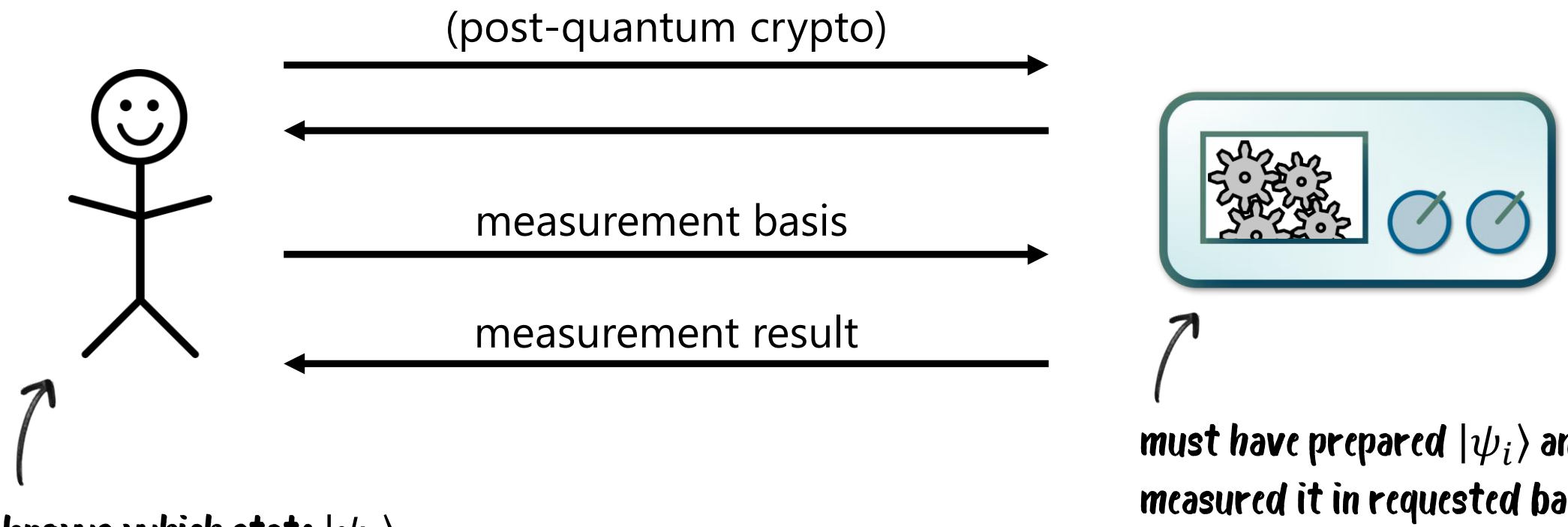
Given: set of **single-qubit** states $\{|\psi_i\rangle\} = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$



Gheorghiu & Vidick, Computationally-secure and composable remote state preparation, FOCS 2019.

Remote state preparation [GV'19]

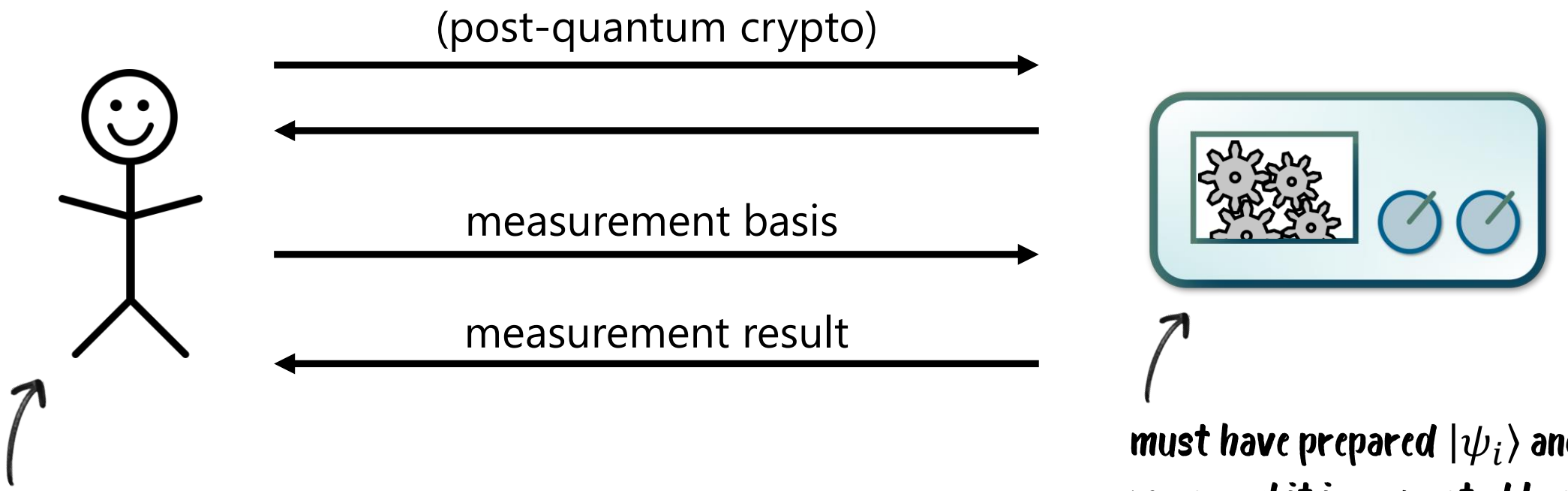
Given: set of **single-qubit** states $\{|\psi_i\rangle\} = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$



Gheorghiu & Vidick, Computationally-secure and composable remote state preparation, FOCS 2019.

Remote state preparation [GV'19]

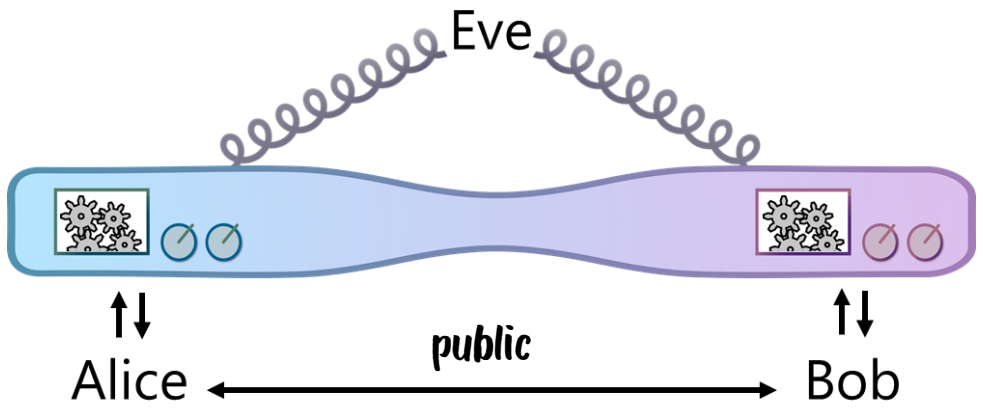
Given: set of **single-qubit** states $\{|\psi_i\rangle\} = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$



Gheorghiu & Vidick, Computationally-secure and composable remote state preparation, FOCS 2019.

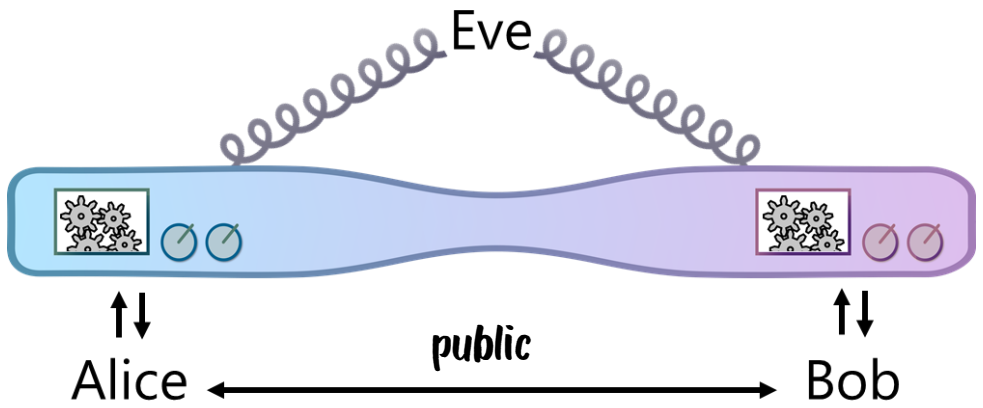
Main challenges for self-testing EPR states

- Device should prepare two qubits and perform single-qubit measurements
  → Alice and Bob need to enforce **tensor product structure** on device's global space



Main challenges for self-testing EPR states

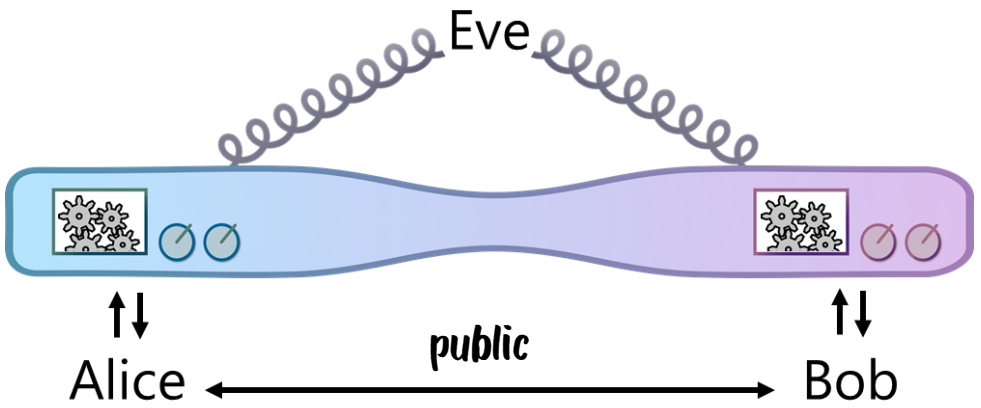
- Device should prepare two qubits and perform single-qubit measurements
  → Alice and Bob need to enforce **tensor product structure** on device's global space



- Device should **entangle** qubits with respect to this tensor product structure

Main challenges for self-testing EPR states

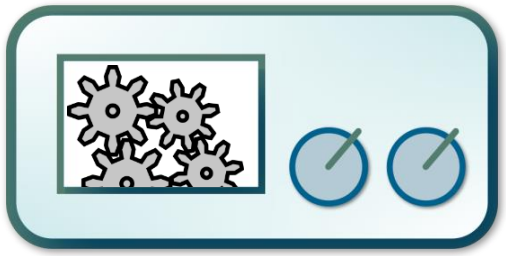
- Device should prepare two qubits and perform single-qubit measurements
  → Alice and Bob need to enforce **tensor product structure** on device's global space



- Device should **entangle** qubits with respect to this tensor product structure
- **Honest** device should only have to use **local operations** and pre-shared EPR pairs

Remote state preparation with two isolated devices

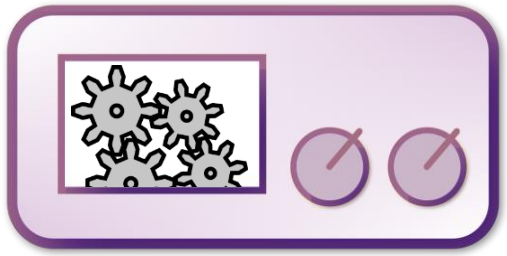
$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$



RSP

Alice

$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$



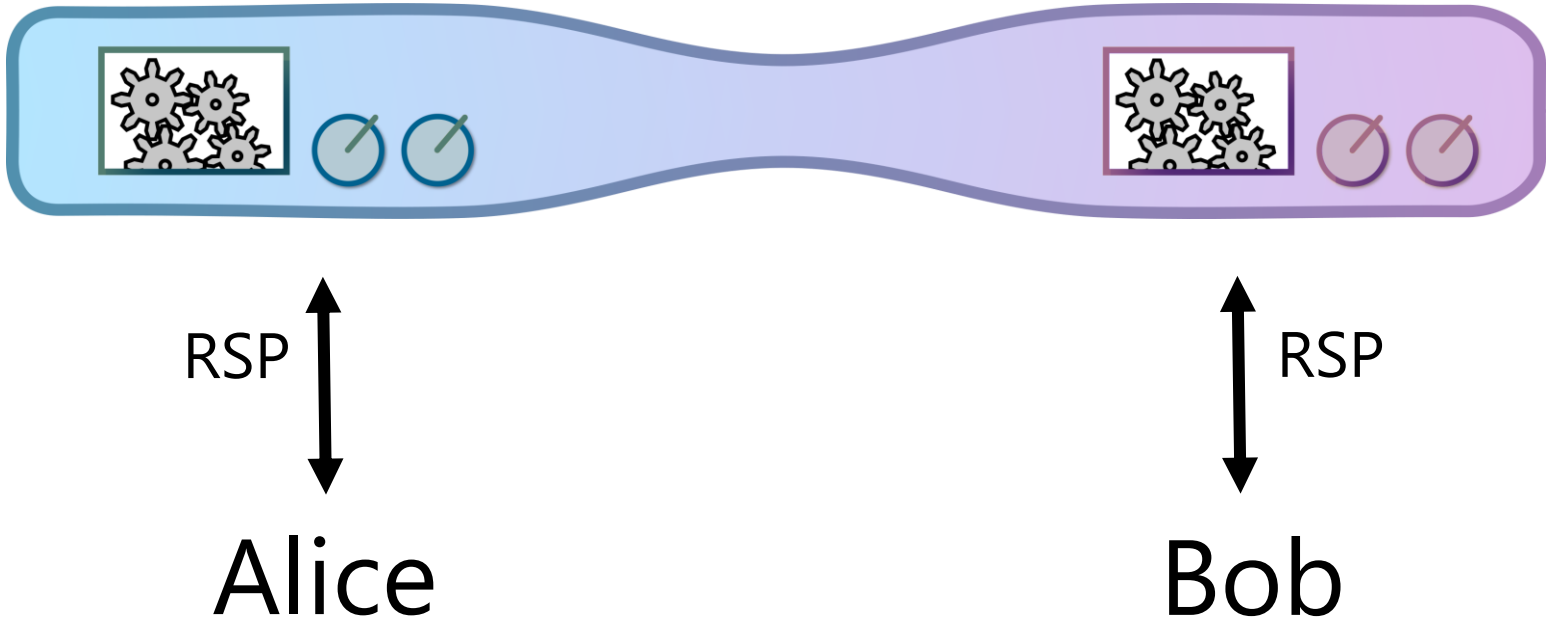
RSP

Bob

Remote State Preparation [GV'19]

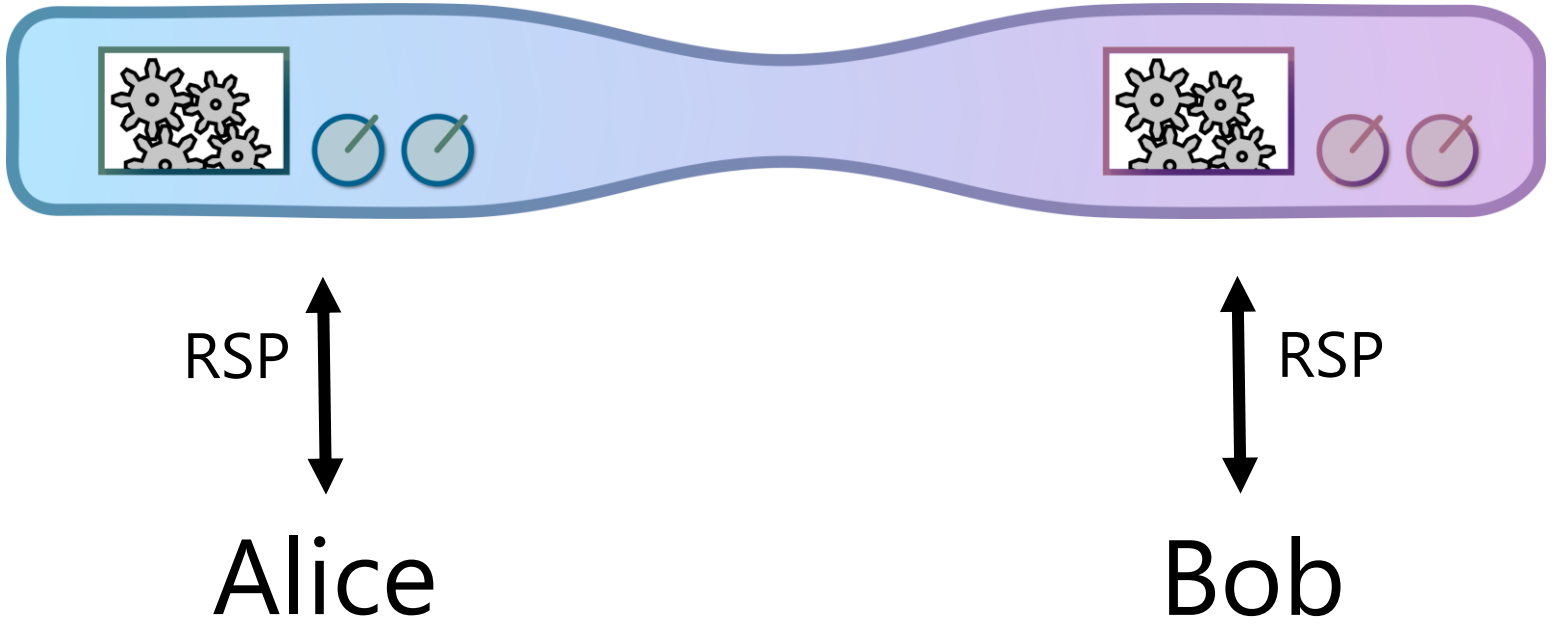
Parallel implementation with single device

$$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\} \times \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$$



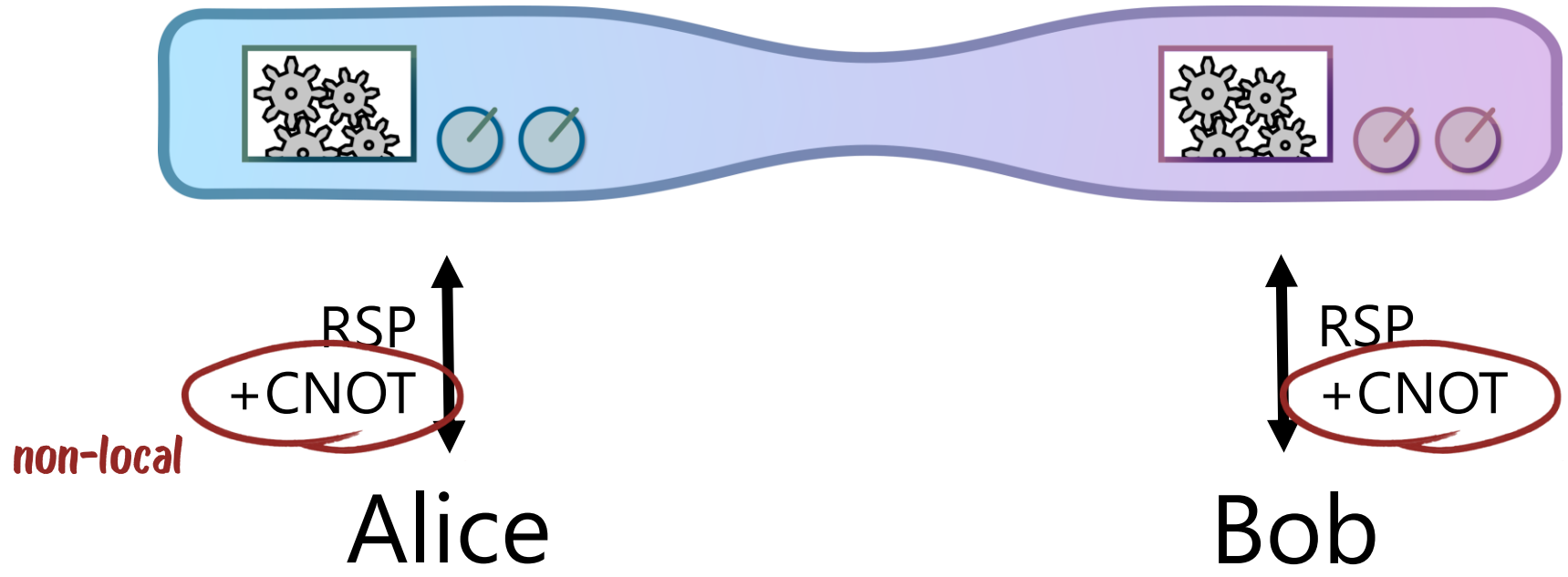
$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

$|\pm\rangle|0/1\rangle$



$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

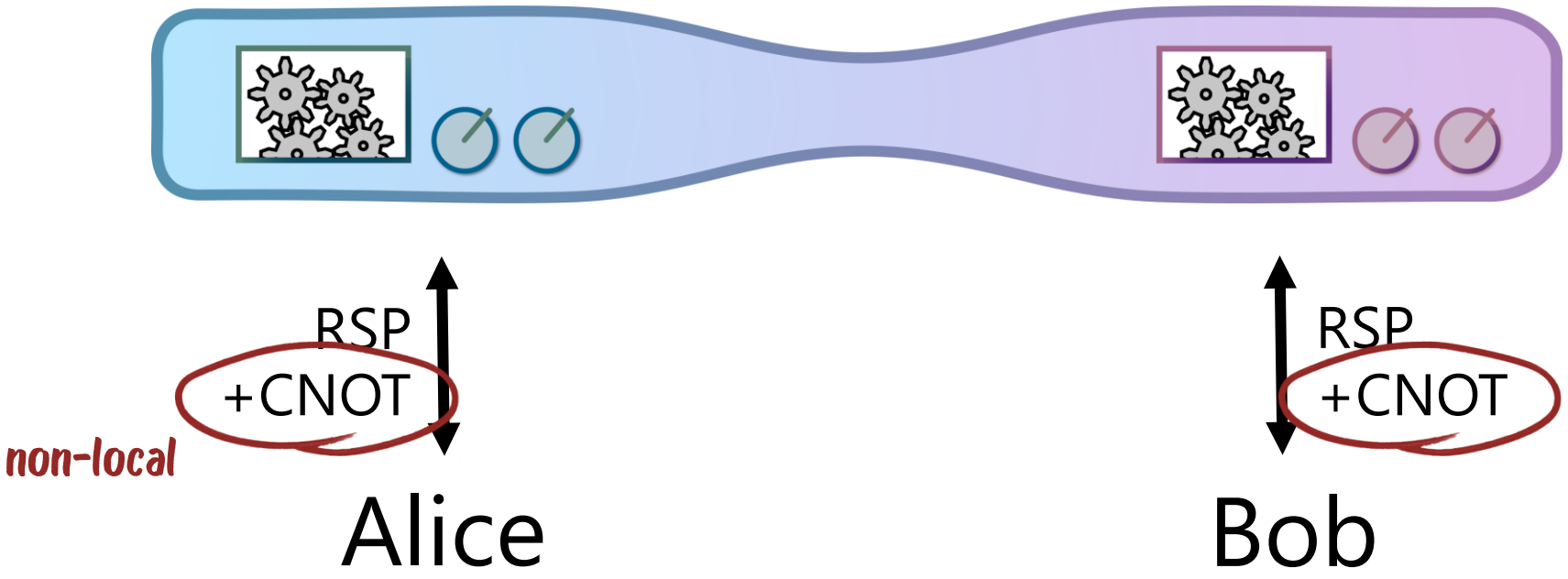
$|\pm\rangle|0/1\rangle$



$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

CNOT

$|\pm\rangle|0/1\rangle$

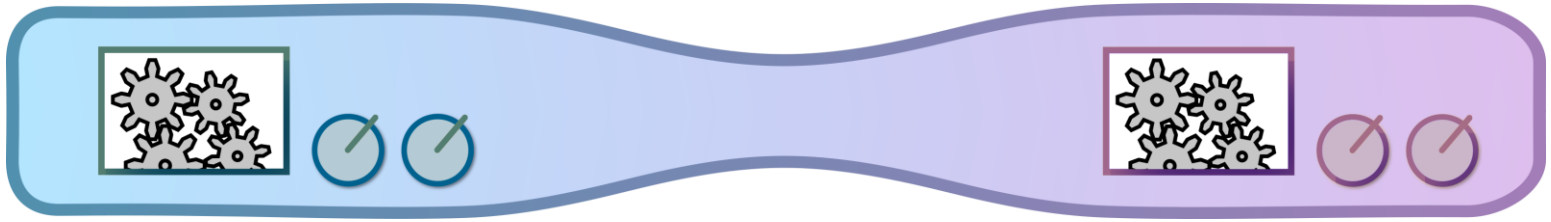


$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

$|\pm\rangle|0/1\rangle$

CNOT

$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$



RSP
+CNOT

non-local

RSP
+CNOT

Alice

Bob

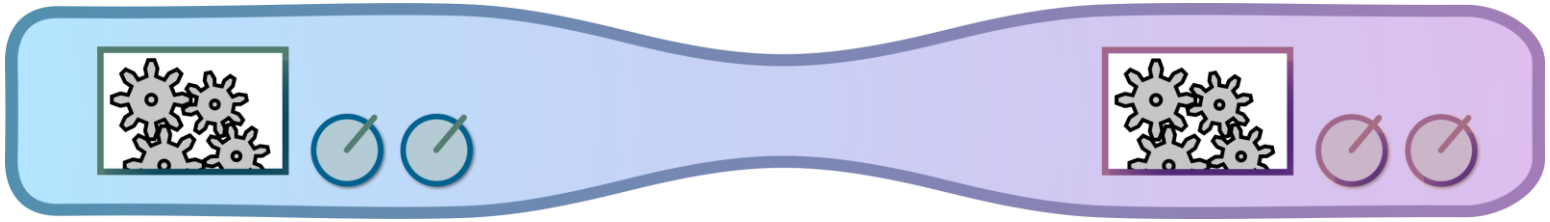
$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

CNOT

$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

$|\pm\rangle|0/1\rangle$

$|00\rangle \pm |11\rangle, |01\rangle \pm |10\rangle$



RSP
+CNOT

non-local

RSP
+CNOT

Alice

Bob

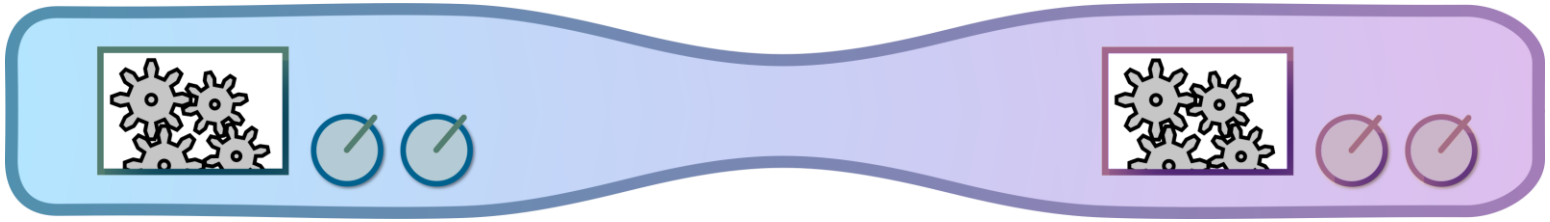
$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

CNOT ⟼

$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

$|\pm\rangle|0/1\rangle$

$|00\rangle \pm |11\rangle, |01\rangle \pm |10\rangle$



RSP
+CNOT

non-local

RSP
+CNOT

Alice

Bob

$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

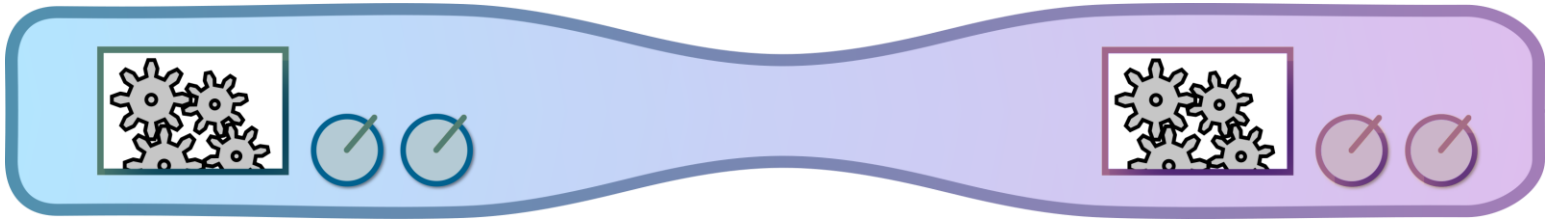
CNOT

$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

Certify **single-qubit** measurements

$|\pm\rangle|0/1\rangle$

$|00\rangle \pm |11\rangle, |01\rangle \pm |10\rangle$



RSP
+CNOT

non-local

RSP
+CNOT

Alice

Bob

$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

CNOT

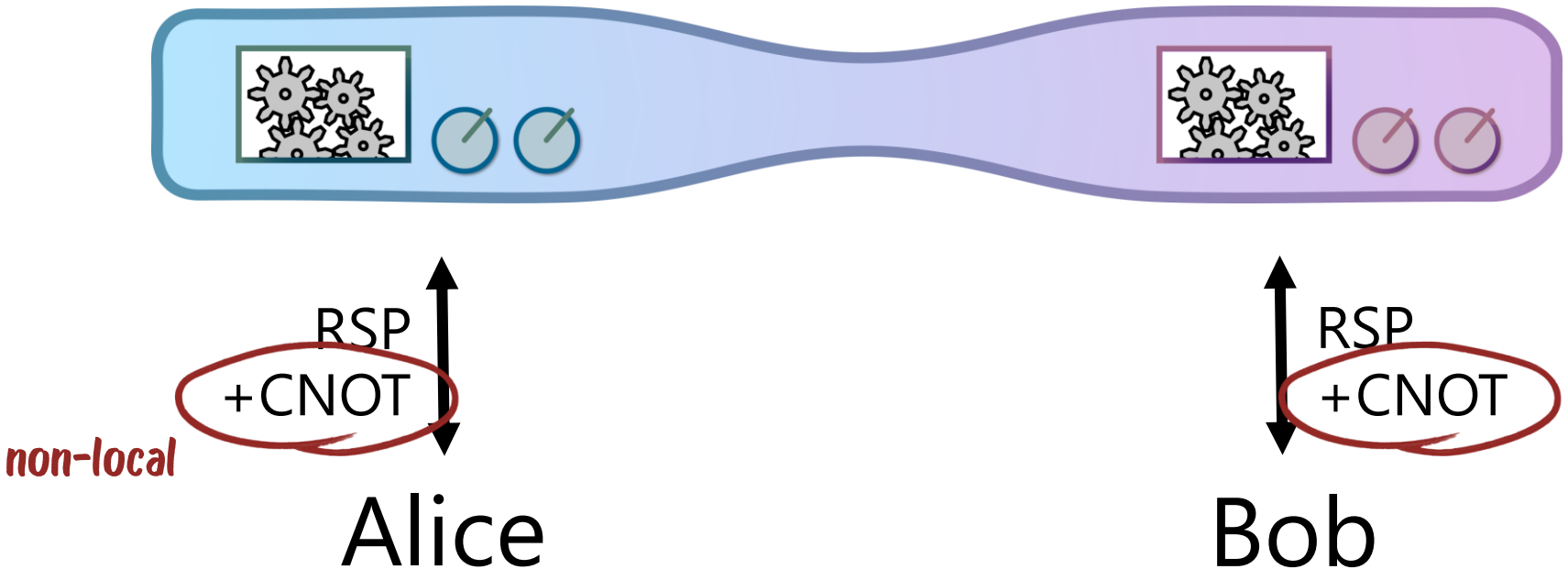
$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

Certify **single-qubit** measurements

$|\pm\rangle|0/1\rangle$

$|00\rangle \pm |11\rangle, |01\rangle \pm |10\rangle$

Certify **Bell**-like correlations



$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

CNOT

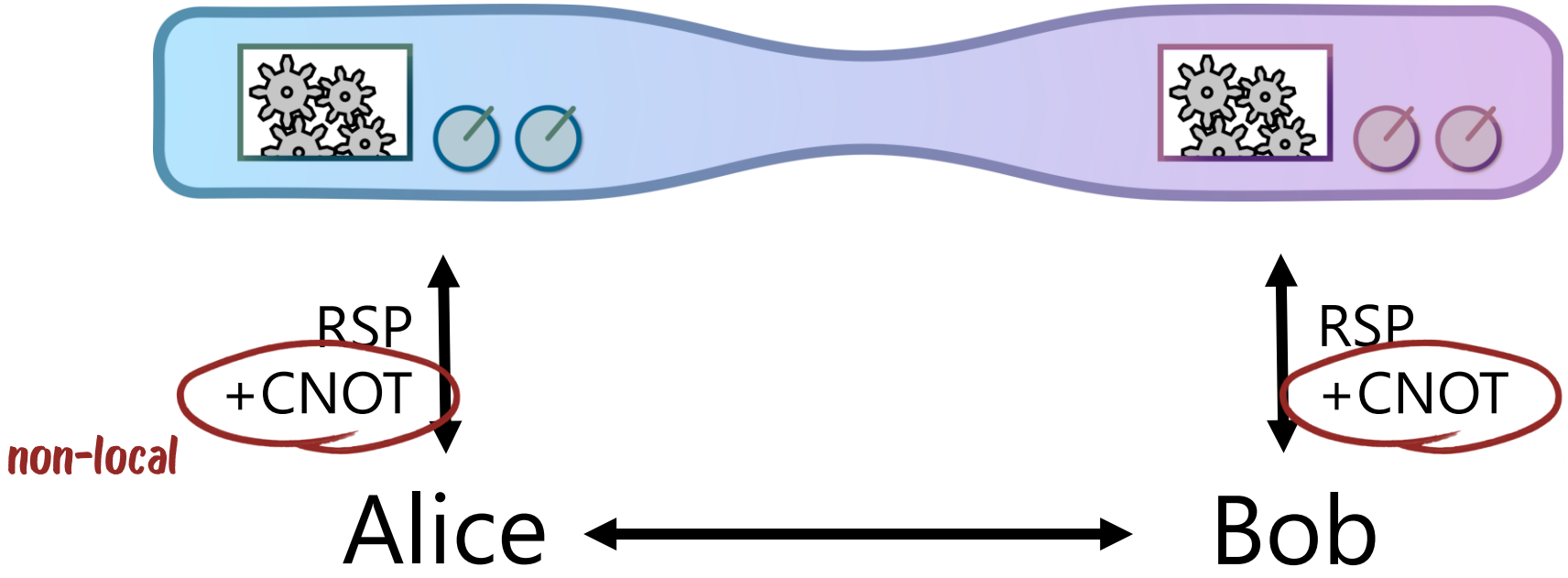
$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

Certify **single-qubit** measurements

$|\pm\rangle|0/1\rangle$

$|00\rangle \pm |11\rangle, |01\rangle \pm |10\rangle$

Certify **Bell**-like correlations

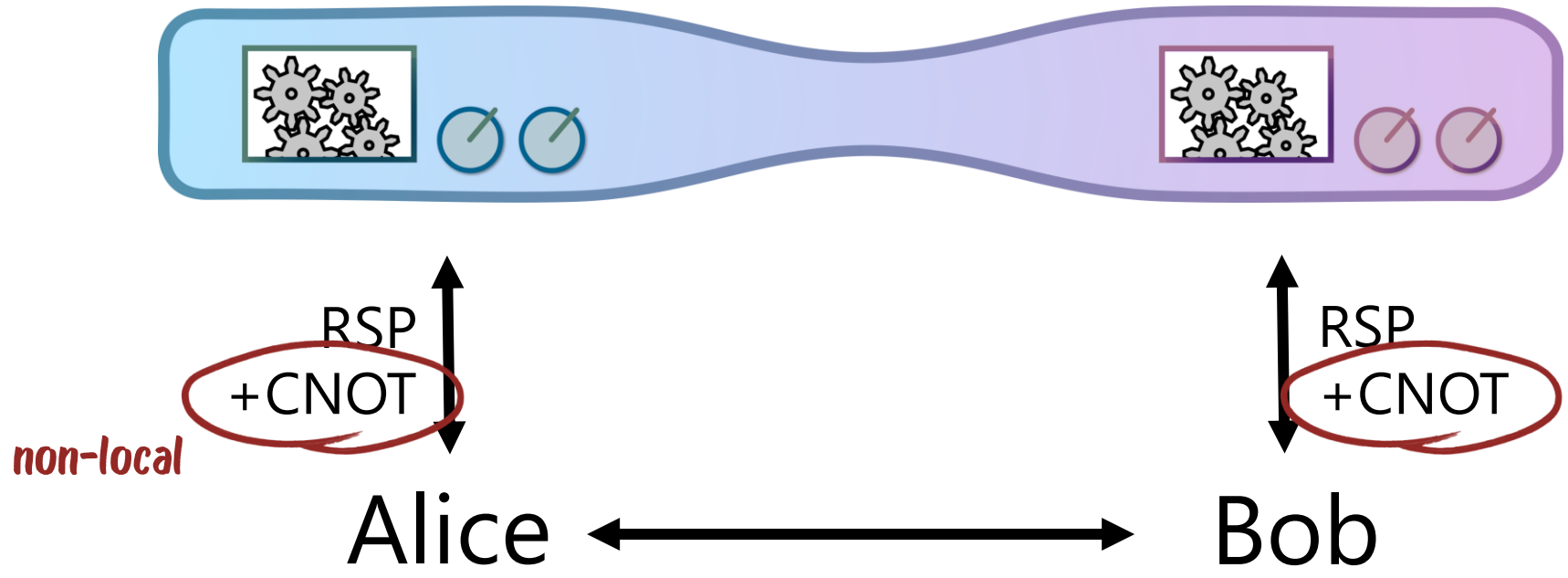


$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

Certify **single-qubit** measurements

$|00\rangle \pm |11\rangle, |01\rangle \pm |10\rangle$

Certify **Bell**-like correlations



$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

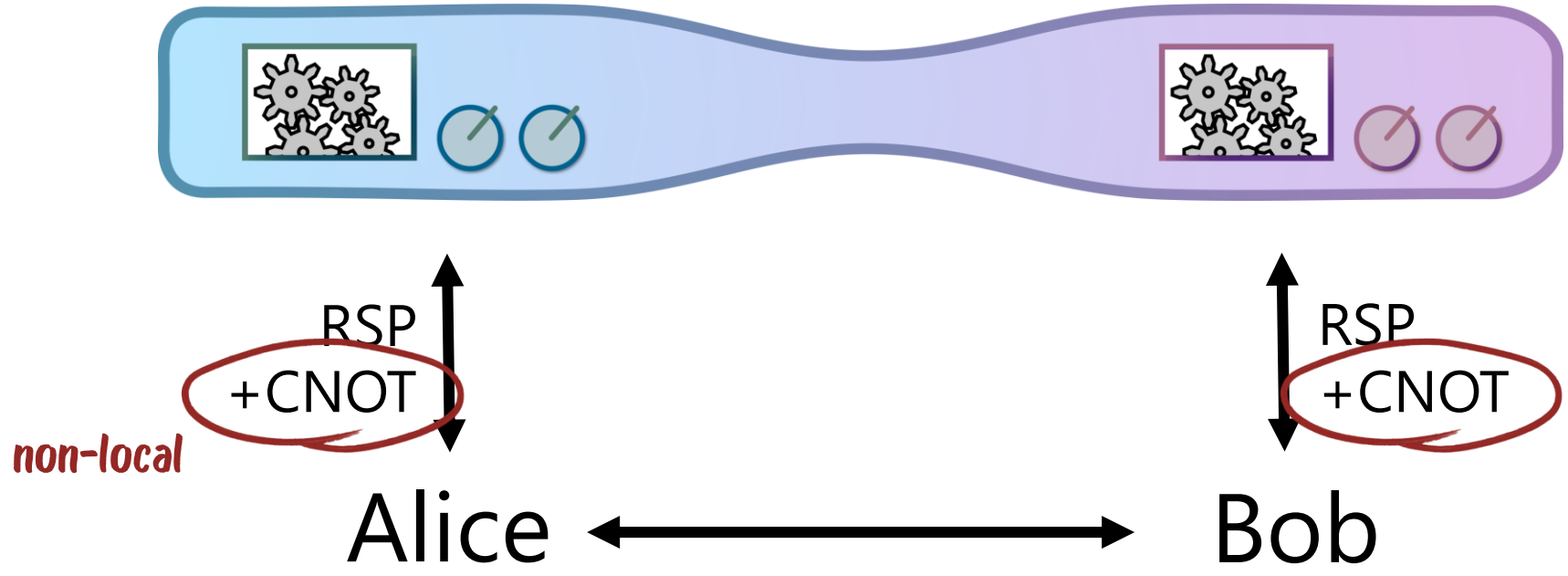
$|00\rangle \pm |11\rangle, |01\rangle \pm |10\rangle$

Certify **single-qubit** measurements

Certify **Bell**-like correlations

$\Rightarrow$ Blindness

Certify **single-qubit measurements** on **Bell state**



$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

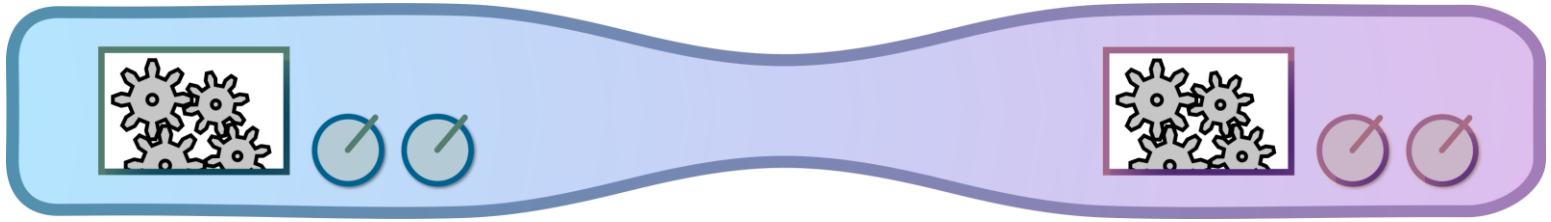
$|00\rangle \pm |11\rangle, |01\rangle \pm |10\rangle$

Certify **single-qubit** measurements

Certify **Bell**-like correlations

$\Rightarrow$ Blindness

Certify **single-qubit measurements** on **Bell state**



RSP
+gate teleportation

RSP
+gate teleportation

Alice $\longleftrightarrow$ Bob

Honest **local** strategy with pre-shared EPR pairs

- Goal:

$$CNOT|\phi\rangle_{Alice}|\psi\rangle_{Bob}$$

non-local gate

Honest **local** strategy with pre-shared EPR pairs

- Goal:

$$CNOT|\phi\rangle_{Alice}|\psi\rangle_{Bob}$$

non-local gate

- With local operations and pre-shared EPR pairs: use gate teleportation

Gottesman & Chuang, Quantum Teleportation is a Universal Computational Primitive. Nature. 402: 390–393

Honest **local** strategy with pre-shared EPR pairs

- Goal:

$$CNOT|\phi\rangle_{Alice}|\psi\rangle_{Bob}$$

non-local gate

- With local operations and pre-shared EPR pairs: use gate teleportation

$$|\phi\rangle_{Alice}|\psi\rangle_{Bob}|EPR\rangle_{AB}$$

Gottesman & Chuang, Quantum Teleportation is a Universal Computational Primitive. Nature. 402: 390–393

Honest **local** strategy with pre-shared EPR pairs

- Goal:

$$CNOT|\phi\rangle_{Alice}|\psi\rangle_{Bob}$$

non-local gate

- With local operations and pre-shared EPR pairs: use gate teleportation

$$|\phi\rangle_{Alice}|\psi\rangle_{Bob}|EPR\rangle_{AB}$$

↓ Local measurements with measurement results $a, b \in \{0,1\}$

Gottesman & Chuang, Quantum Teleportation is a Universal Computational Primitive. Nature. 402: 390–393

Honest **local** strategy with pre-shared EPR pairs

- Goal:

$$CNOT|\phi\rangle_{Alice}|\psi\rangle_{Bob}$$

non-local gate

- With local operations and pre-shared EPR pairs: use gate teleportation

$$|\phi\rangle_{Alice}|\psi\rangle_{Bob}|EPR\rangle_{AB}$$

Local measurements with measurement results $a, b \in \{0,1\}$

$$(\sigma_Z^a \sigma_X^b \otimes \sigma_Z^b \sigma_X^a) CNOT|\phi\rangle_{Alice}|\psi\rangle_{Bob}$$

Gottesman & Chuang, Quantum Teleportation is a Universal Computational Primitive. Nature. 402: 390–393

Honest **local** strategy with pre-shared EPR pairs

- Goal:

$$CNOT|\phi\rangle_{Alice}|\psi\rangle_{Bob}$$

non-local gate

- With local operations and pre-shared EPR pairs: use gate teleportation

$$|\phi\rangle_{Alice}|\psi\rangle_{Bob}|EPR\rangle_{AB}$$

Local measurements with measurement results $a, b \in \{0,1\}$

send a to Alice, b to Bob

Alice and Bob adapt checks to account for correction operator

$$(\sigma_Z^a \sigma_X^b \otimes \sigma_Z^b \sigma_X^a) CNOT|\phi\rangle_{Alice}|\psi\rangle_{Bob}$$

Gottesman & Chuang, Quantum Teleportation is a Universal Computational Primitive. Nature. 402: 390–393

Summary

T. Metger and T. Vidick, Self-testing of a single quantum device under computational assumptions, arXiv:2001.09161
T. Metger, Y. Dulek, A. Coladangelo, and R. Arnon-Friedman, Device-independent quantum key distribution from computational assumptions, arXiv:2010.04175

Summary

- Main result: self-testing and DIQKD protocols that don't rely on Bell inequalities
  → don't need non-communication assumption

T. Metger and T. Vidick, Self-testing of a single quantum device under computational assumptions, arXiv:2001.09161
T. Metger, Y. Dulek, A. Coladangelo, and R. Arnon-Friedman, Device-independent quantum key distribution from computational assumptions, arXiv:2010.04175

Summary

- Main result: self-testing and DIQKD protocols that don't rely on Bell inequalities
  → don't need non-communication assumption
- Alternative assumption: device cannot break post-quantum cryptography during protocol
  → final key remains information-theoretically secure

T. Metger and T. Vidick, Self-testing of a single quantum device under computational assumptions, arXiv:2001.09161
T. Metger, Y. Dulek, A. Coladangelo, and R. Arnon-Friedman, Device-independent quantum key distribution from computational assumptions, arXiv:2010.04175

Summary

- Main result: self-testing and DIQKD protocols that don't rely on Bell inequalities
  → don't need non-communication assumption
- Alternative assumption: device cannot break post-quantum cryptography during protocol
  → final key remains information-theoretically secure
- Main technique: tight **cryptographic leash** for black-box quantum devices
  (Brakerski et al. (2018), Mahadev (2018))

T. Metger and T. Vidick, Self-testing of a single quantum device under computational assumptions, arXiv:2001.09161
T. Metger, Y. Dulek, A. Coladangelo, and R. Arnon-Friedman, Device-independent quantum key distribution from computational assumptions, arXiv:2010.04175

Summary

- Main result: self-testing and DIQKD protocols that don't rely on Bell inequalities
  → don't need non-communication assumption
- Alternative assumption: device cannot break post-quantum cryptography during protocol
  → final key remains information-theoretically secure
- Main technique: tight **cryptographic leash** for black-box quantum devices
  (Brakerski et al. (2018), Mahadev (2018))

Future work

T. Metger and T. Vidick, Self-testing of a single quantum device under computational assumptions, arXiv:2001.09161
T. Metger, Y. Dulek, A. Coladangelo, and R. Arnon-Friedman, Device-independent quantum key distribution from computational assumptions, arXiv:2010.04175

Summary

- Main result: self-testing and DIQKD protocols that don't rely on Bell inequalities
  → don't need non-communication assumption
- Alternative assumption: device cannot break post-quantum cryptography during protocol
  → final key remains information-theoretically secure
- Main technique: tight **cryptographic leash** for black-box quantum devices
  (Brakerski et al. (2018), Mahadev (2018))

Future work

- Self-test arbitrary states

T. Metger and T. Vidick, Self-testing of a single quantum device under computational assumptions, arXiv:2001.09161
T. Metger, Y. Dulek, A. Coladangelo, and R. Arnon-Friedman, Device-independent quantum key distribution from computational assumptions, arXiv:2010.04175

Summary

- Main result: self-testing and DIQKD protocols that don't rely on Bell inequalities
  → don't need non-communication assumption
- Alternative assumption: device cannot break post-quantum cryptography during protocol
  → final key remains information-theoretically secure
- Main technique: tight **cryptographic leash** for black-box quantum devices
  (Brakerski et al. (2018), Mahadev (2018))

Future work

- Self-test arbitrary states
- Non-IID analysis for computational DIQKD protocol

T. Metger and T. Vidick, Self-testing of a single quantum device under computational assumptions, arXiv:2001.09161
T. Metger, Y. Dulek, A. Coladangelo, and R. Arnon-Friedman, Device-independent quantum key distribution from computational assumptions, arXiv:2010.04175

Summary

- Main result: self-testing and DIQKD protocols that don't rely on Bell inequalities
  → don't need non-communication assumption
- Alternative assumption: device cannot break post-quantum cryptography during protocol
  → final key remains information-theoretically secure
- Main technique: tight **cryptographic leash** for black-box quantum devices
  (Brakerski et al. (2018), Mahadev (2018))

Future work

- Self-test arbitrary states
- Non-IID analysis for computational DIQKD protocol
- Computational DIQKD without self-testing

T. Metger and T. Vidick, Self-testing of a single quantum device under computational assumptions, arXiv:2001.09161
T. Metger, Y. Dulek, A. Coladangelo, and R. Arnon-Friedman, Device-independent quantum key distribution from computational assumptions, arXiv:2010.04175

Summary

- Main result: self-testing and DIQKD protocols that don't rely on Bell inequalities
  → don't need non-communication assumption
- Alternative assumption: device cannot break post-quantum cryptography during protocol
  → final key remains information-theoretically secure
- Main technique: tight **cryptographic leash** for black-box quantum devices
  (Brakerski et al. (2018), Mahadev (2018))

Future work

- Self-test arbitrary states
- Non-IID analysis for computational DIQKD protocol
- Computational DIQKD without self-testing
- Other applications of cryptographic leash

T. Metger and T. Vidick, Self-testing of a single quantum device under computational assumptions, arXiv:2001.09161
T. Metger, Y. Dulek, A. Coladangelo, and R. Arnon-Friedman, Device-independent quantum key distribution from computational assumptions, arXiv:2010.04175