Device-independent protocols from computational assumptions

Tony Metger (ETH Zürich)

Self-testing: arXiv:2001.09161, with Thomas Vidick

DIQKD: arXiv:2010.04175, with Rotem Arnon-Friedman, Andrea Coladangelo, and Yfke Dulek

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

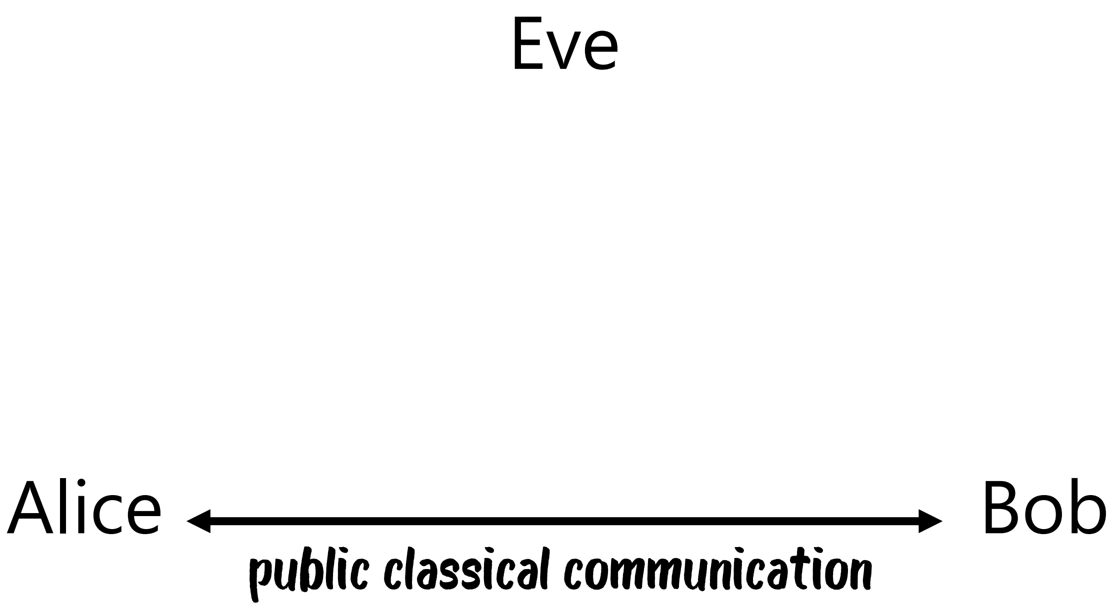
Eve

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



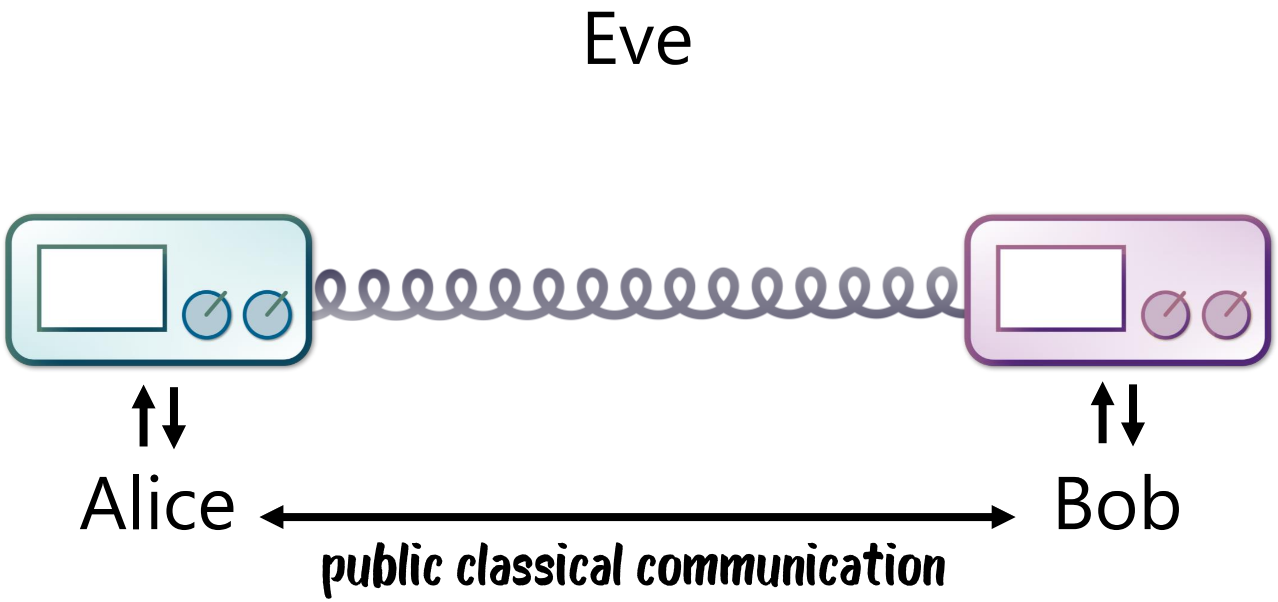
Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.

Device-independent QKD

Eve

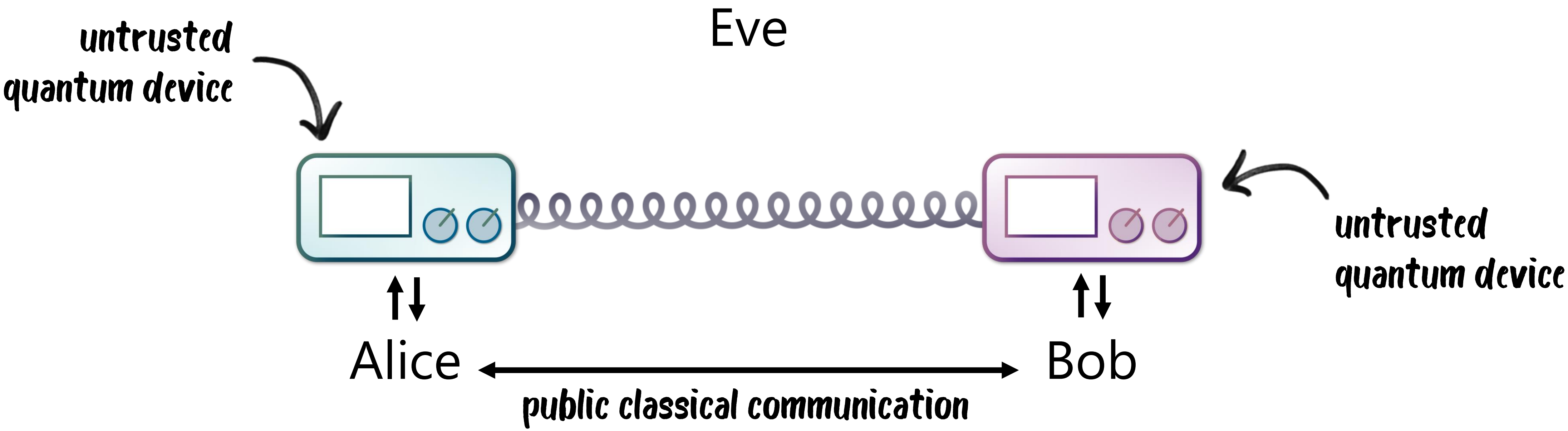
Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.

Device-independent QKD



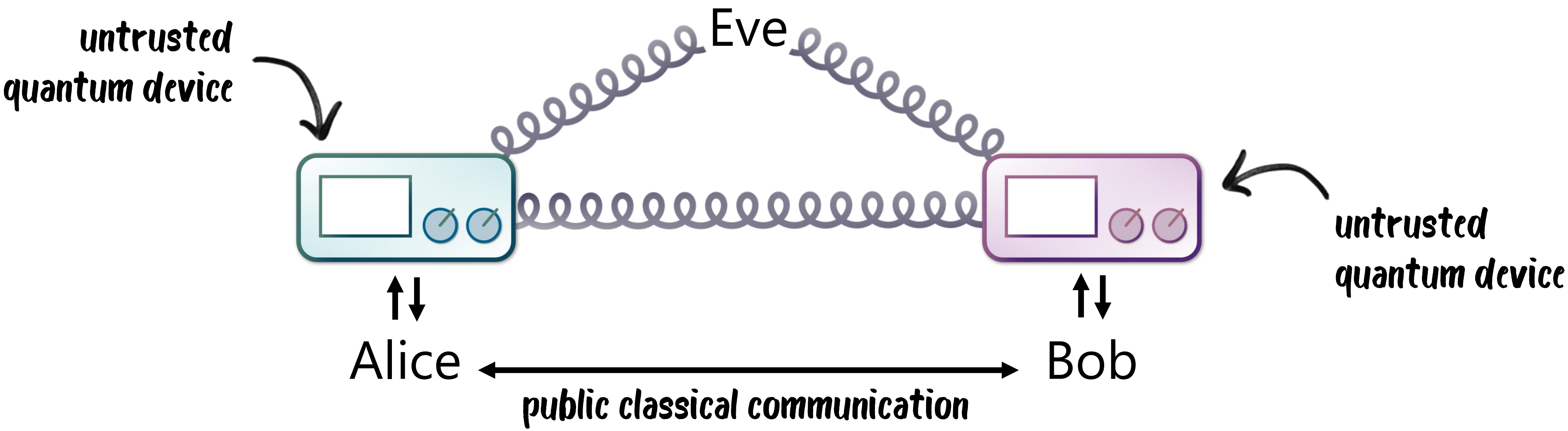
Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.

Device-independent QKD



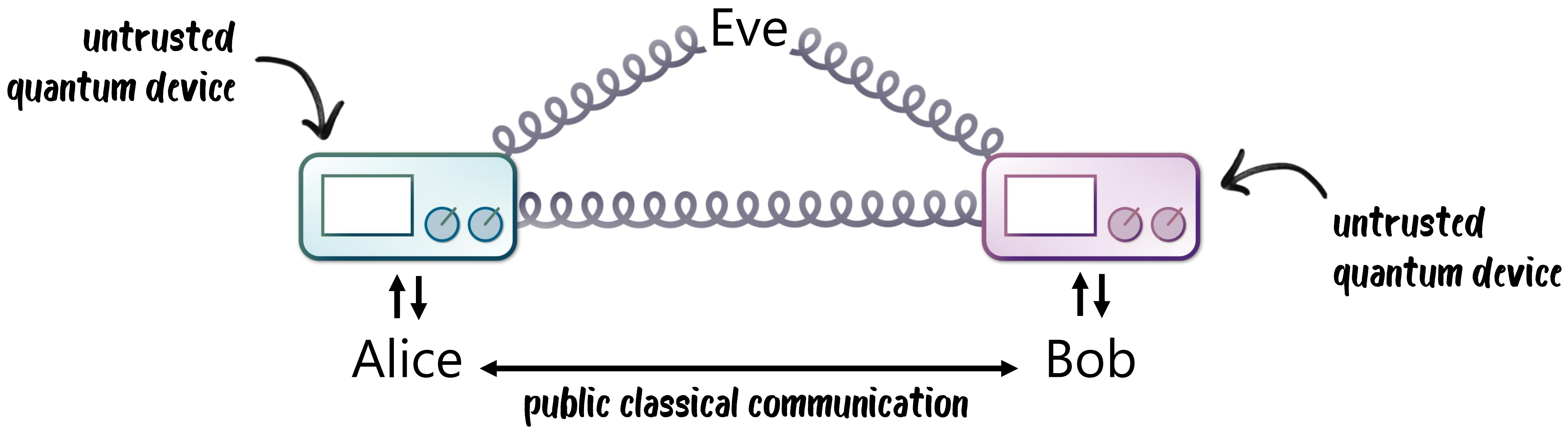
Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.

Device-independent QKD



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

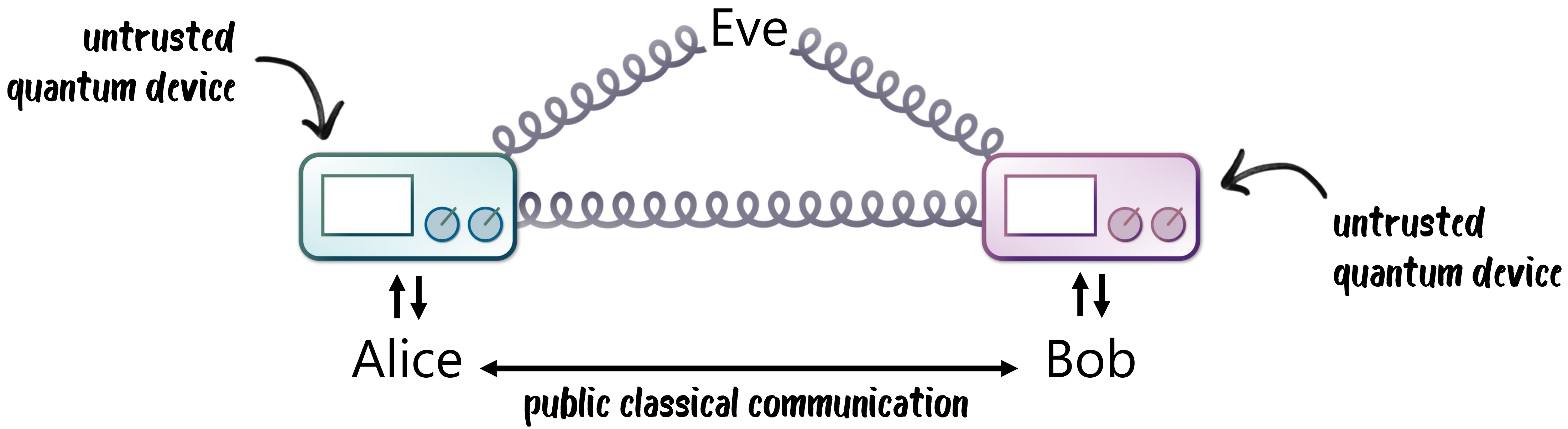
Device-independent QKD



Bell inequality
violation

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

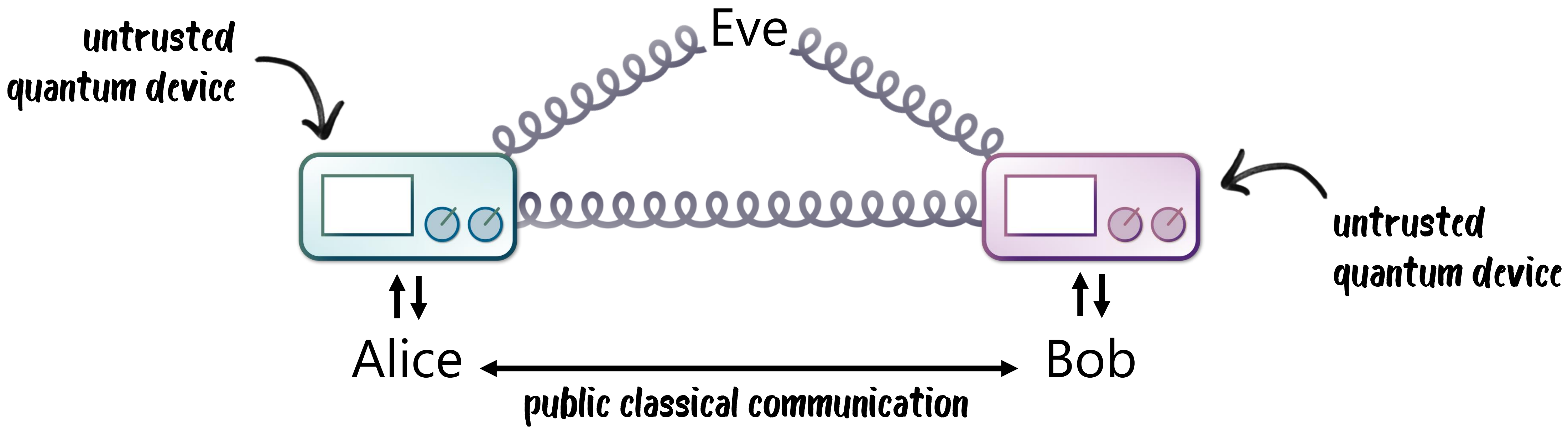
Device-independent QKD



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.

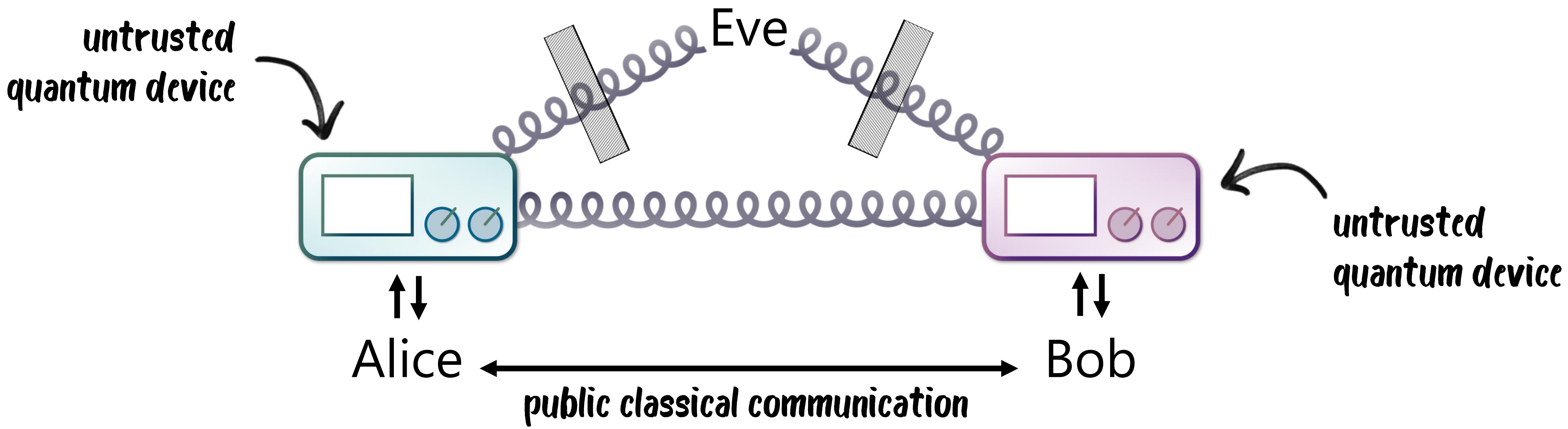
Device-independent QKD



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.

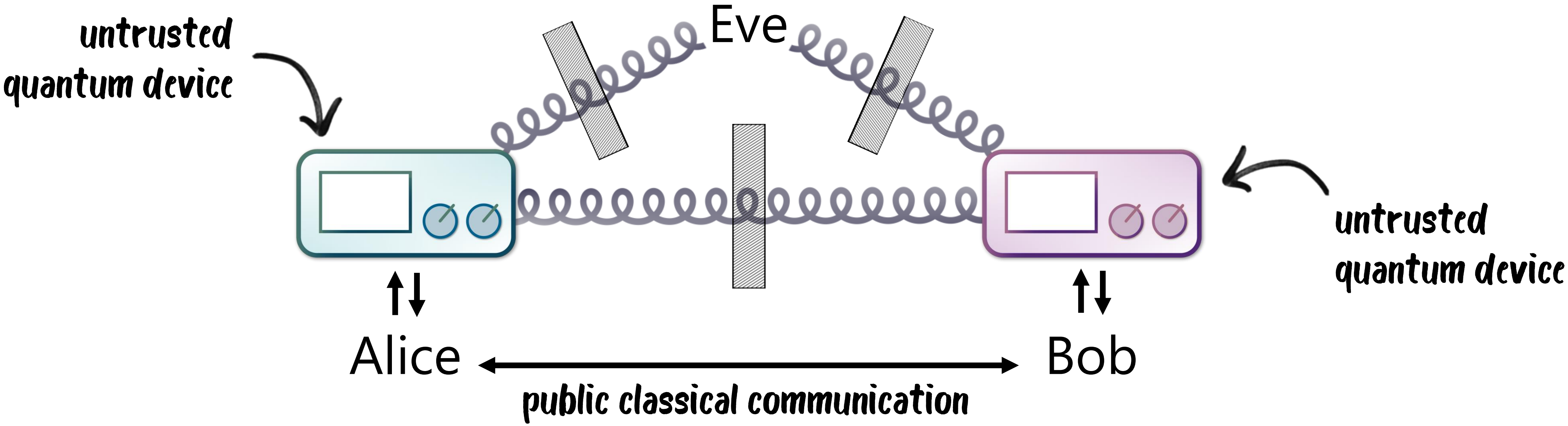
Device-independent QKD



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.

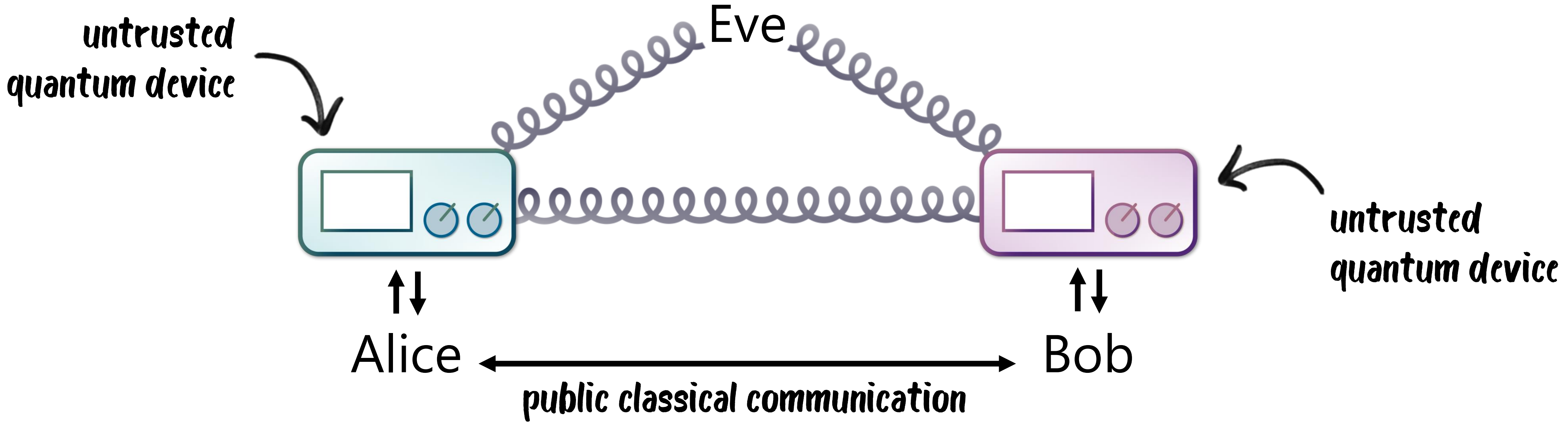
Device-independent QKD



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

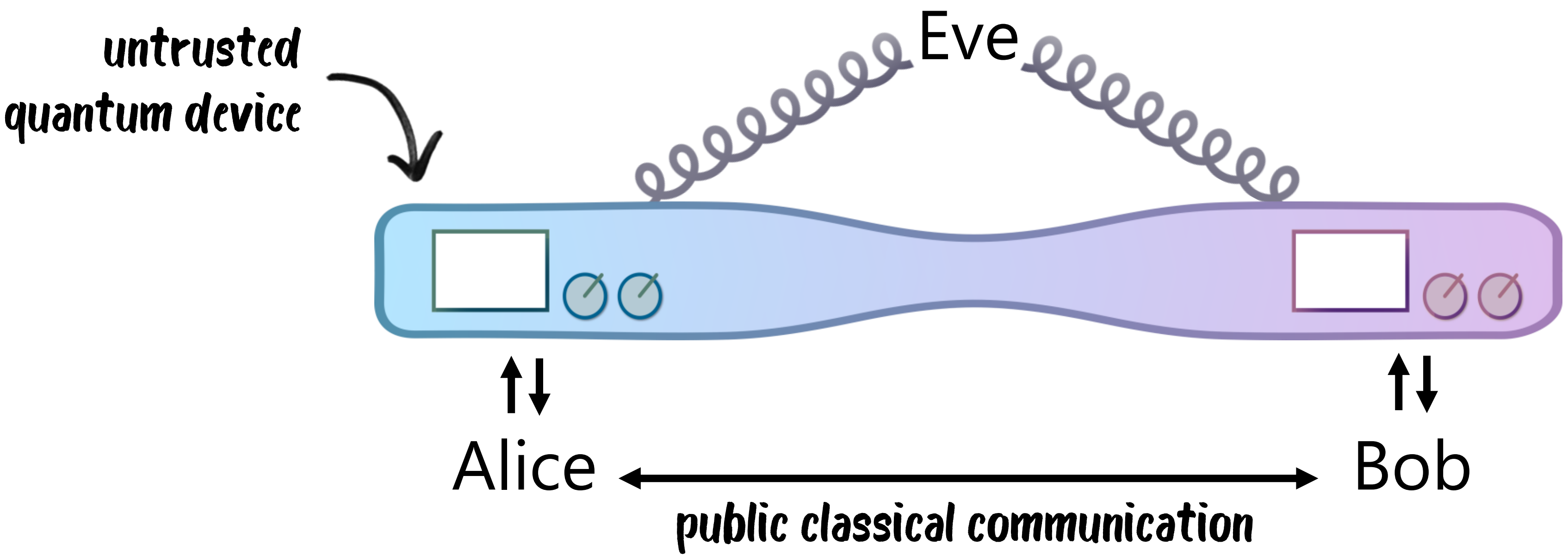
Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.

Device-independent QKD



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

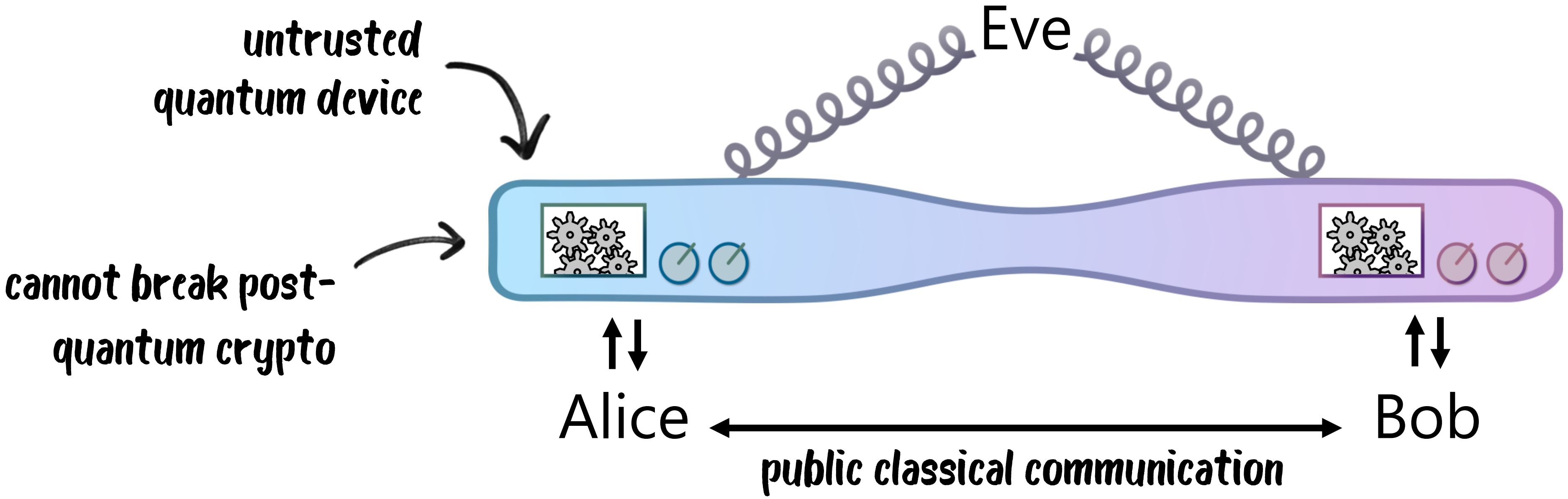
Ekert, Quantum cryptography based on Bell's theorem, PRL 67, 661 (1991).
Mayers & Yao, Quantum cryptography with imperfect apparatus, FOCS 1998.



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.

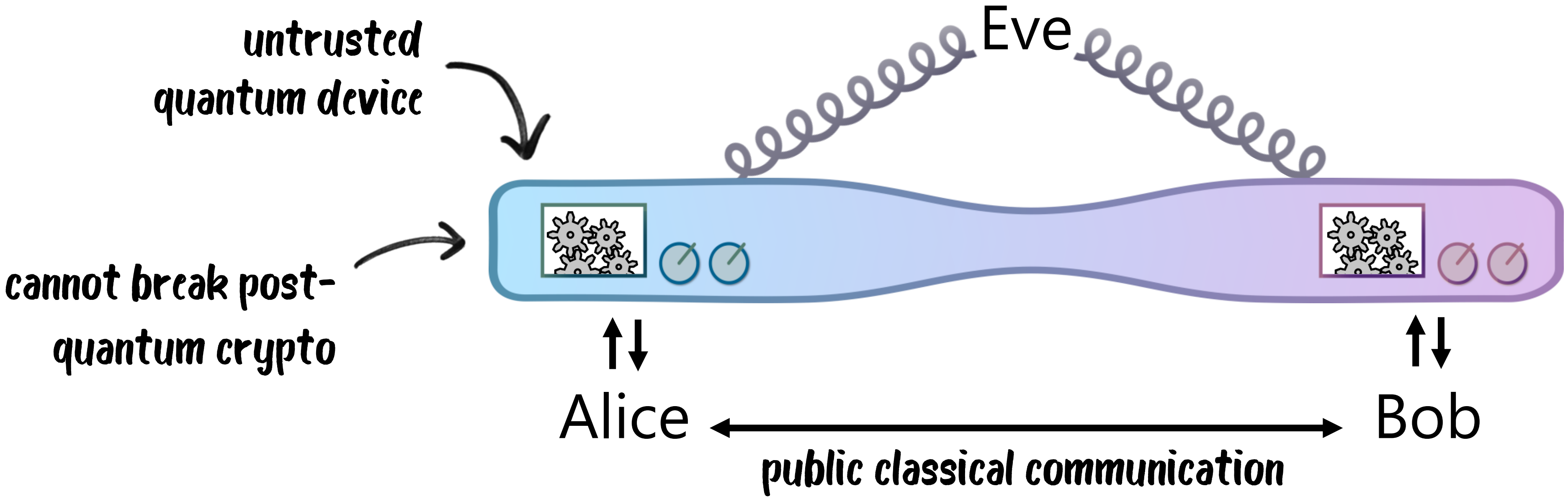
Computational DIQKD setting



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.

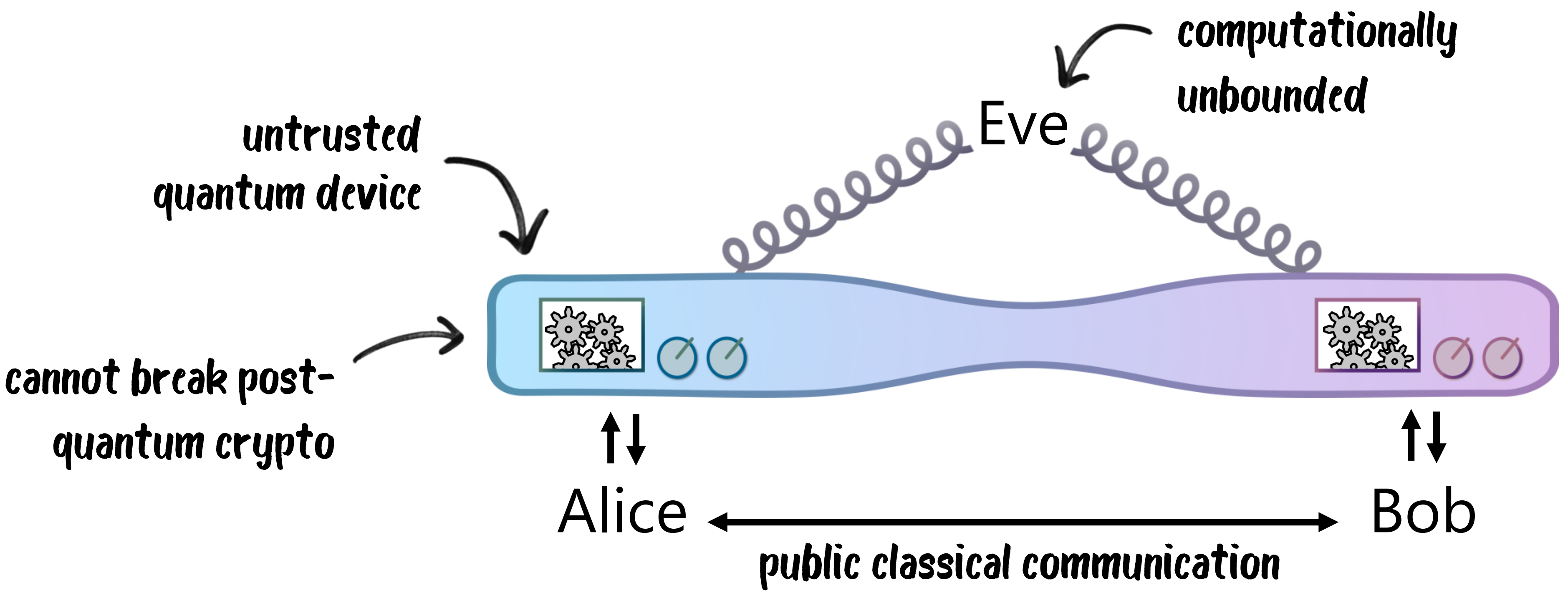
Computational DIQKD setting



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

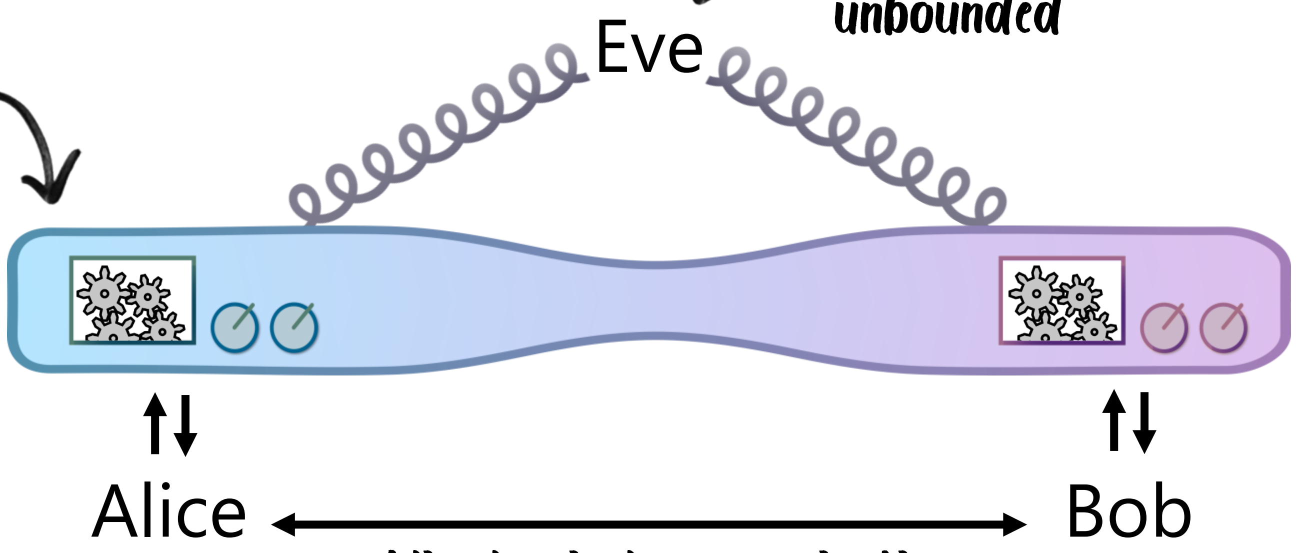
Brakerski et al., A cryptographic test of quantumness and certifiable randomness from a single quantum device, FOCS 2018.
Mahadev, Classical Verification of Quantum Computations, FOCS 2018
Gheorghiu & Vidick, Computationally-secure and composable remote state preparation, FOCS 2019.

Computational DIQKD setting

computationally unbounded

untrusted quantum device

cannot break post-quantum crypto

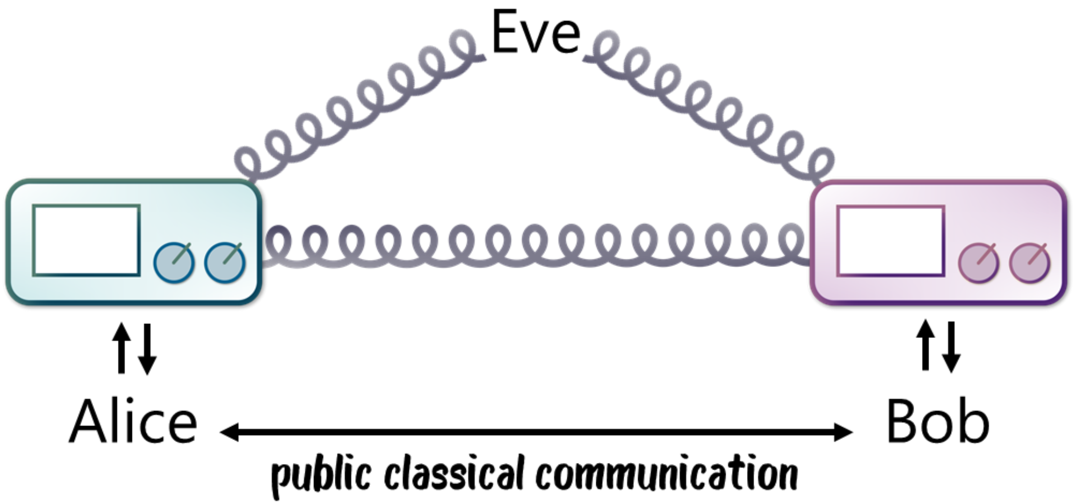


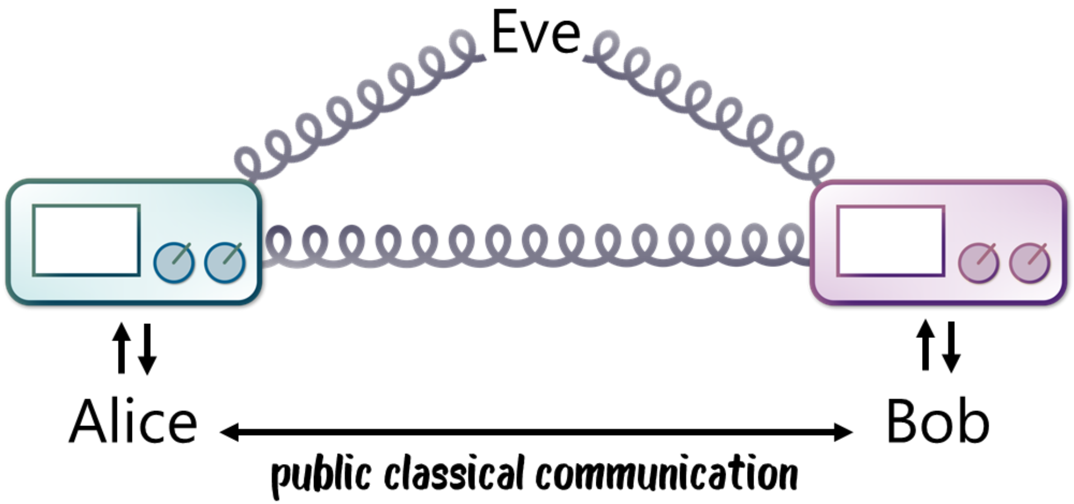
public classical communication

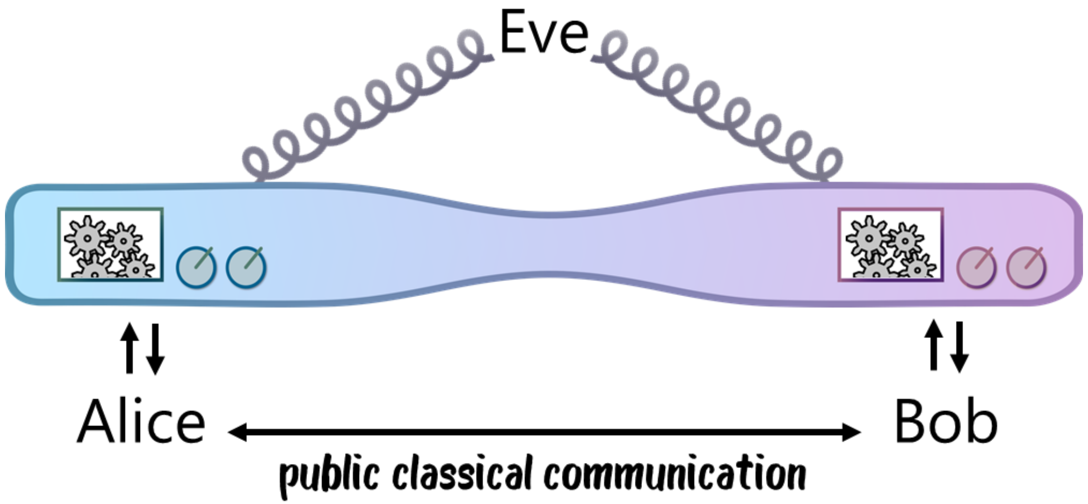
Interactive protocol with **computational assumption** → Statement about devices' states and measurements → **Information-theoretic security** of final key

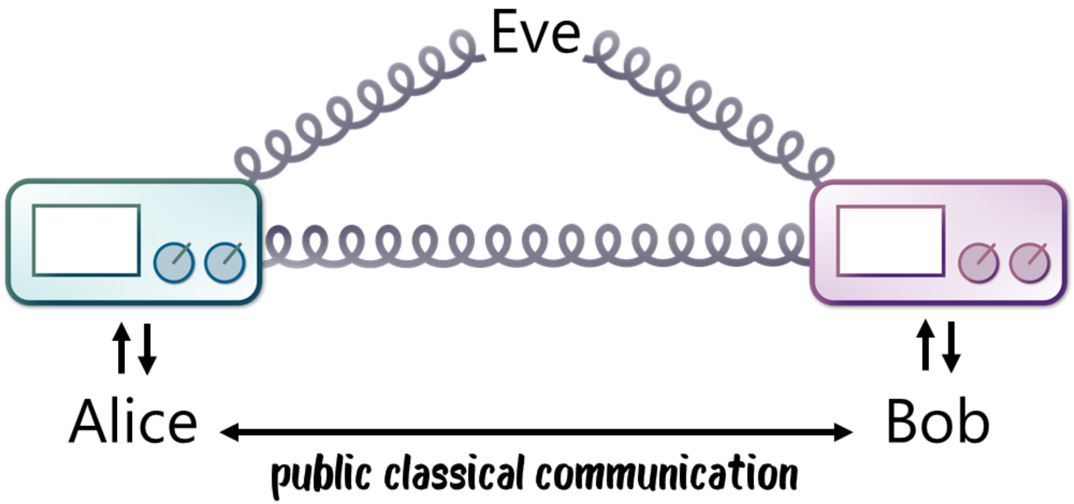
required only for duration of the protocol

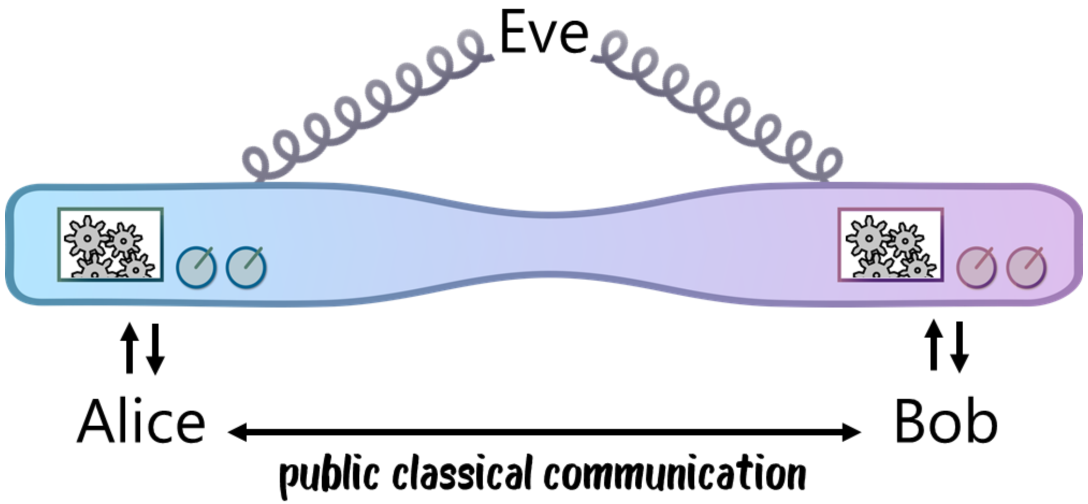
Brakerski et al., A cryptographic test of quantumness and certifiable randomness from a single quantum device, FOCS 2018.
Mahadev, Classical Verification of Quantum Computations, FOCS 2018
Gheorghiu & Vidick, Computationally-secure and composable remote state preparation, FOCS 2019.


Eve
Alice
Bob
public classical communication


Eve
Alice
Bob
public classical communication

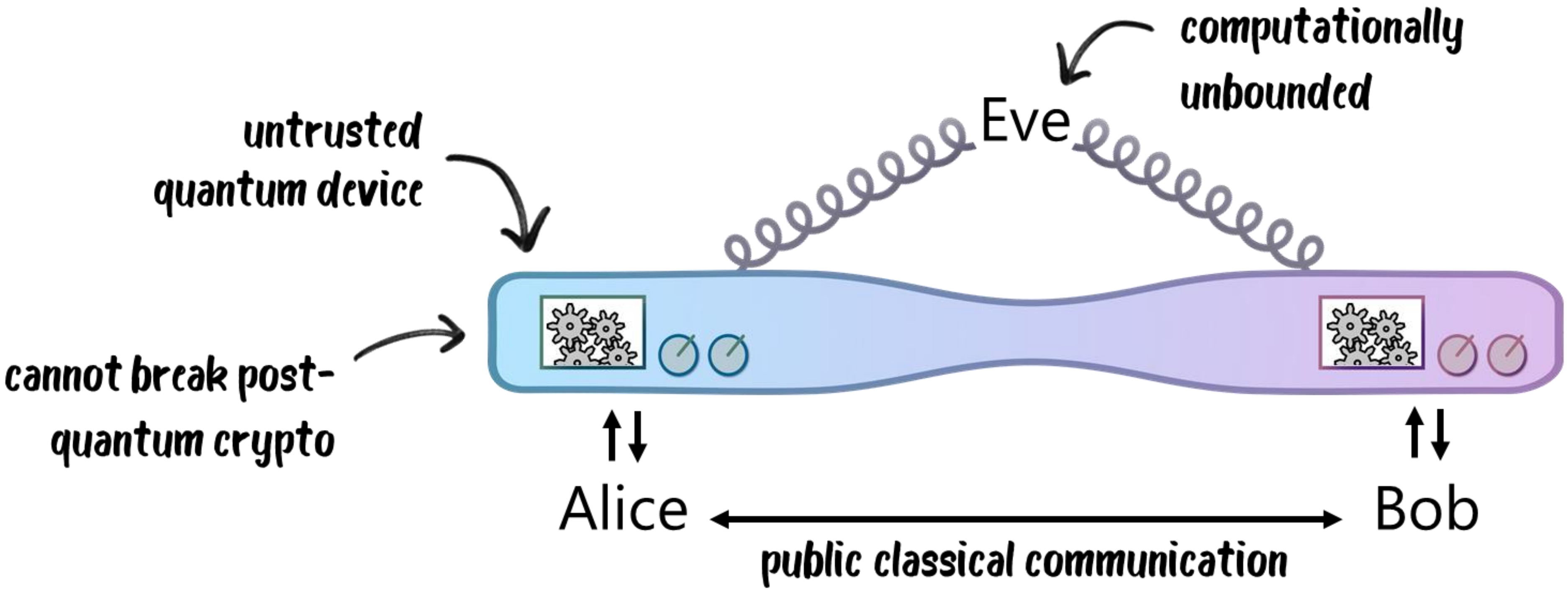

Eve
Alice
Bob
public classical communication





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

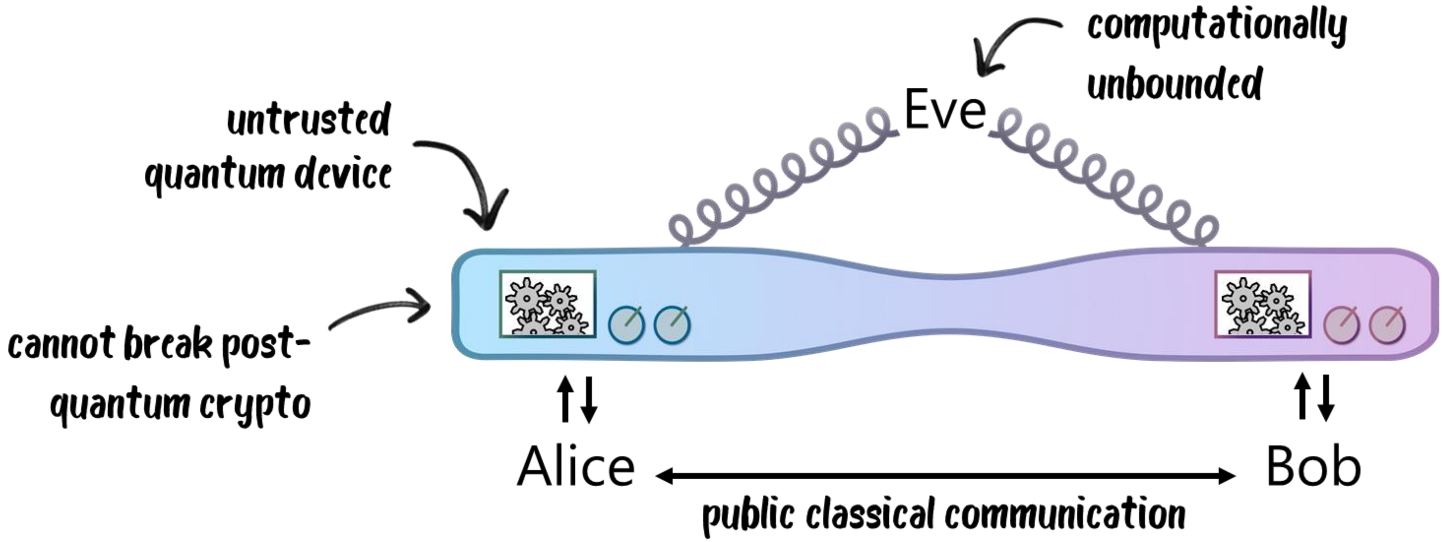
Computational DIQKD setting



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

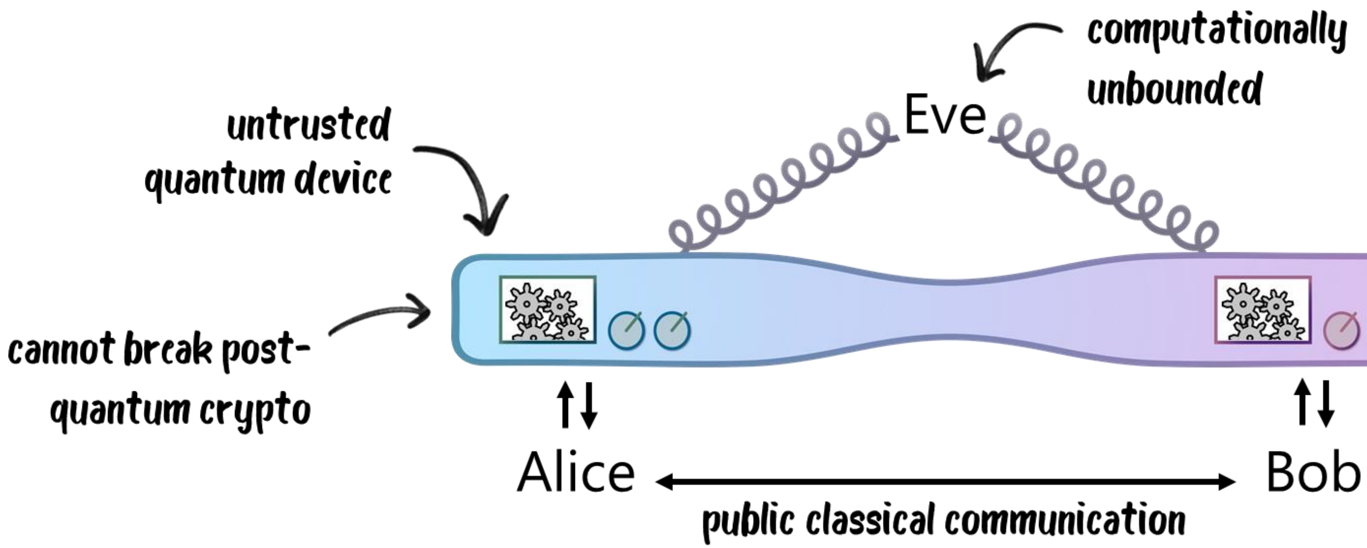
required only for duration of the protocol

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.



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

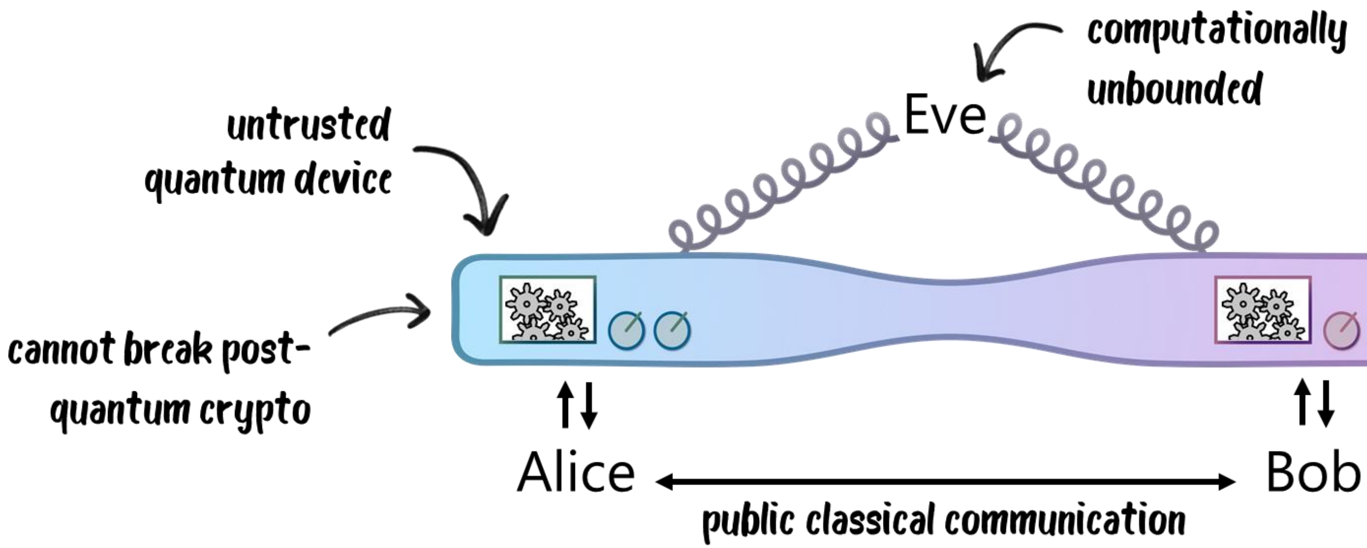
required only for duration of the protocol



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

required only for duration of the protocol

Computational self-testing protocol

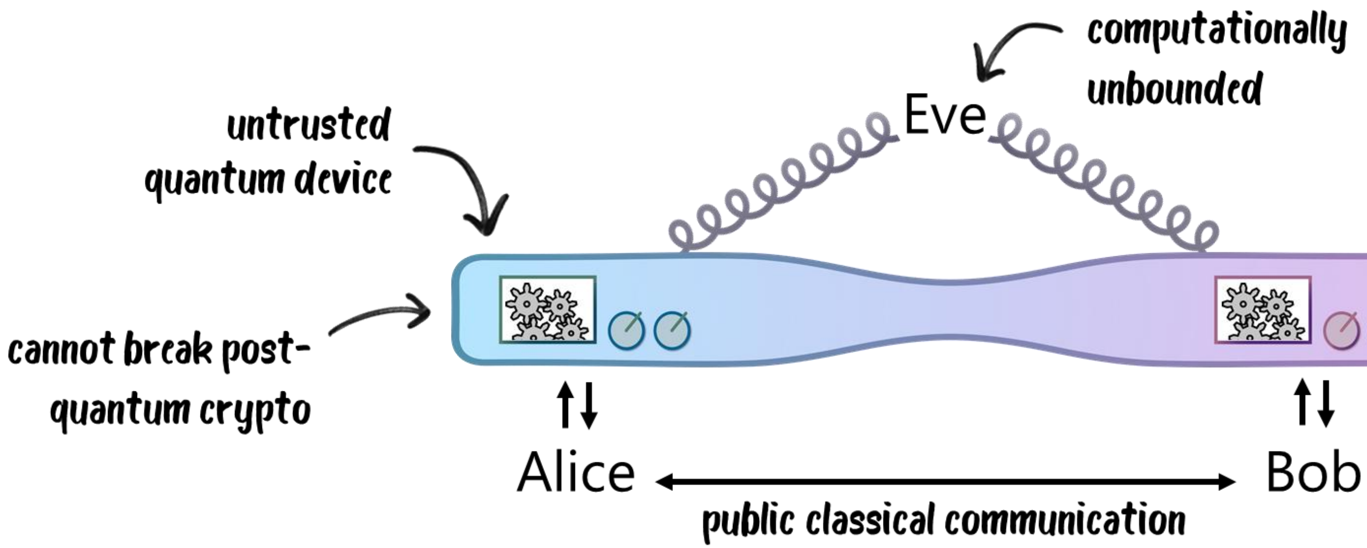


Interactive protocol with **computational assumption** → Statement about devices' states and measurements → **Information-theoretic security** of final key

required only for duration of the protocol

Computational self-testing protocol

Device must have prepared EPR pair and measured single qubits in computational or Hadamard basis



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

required only for duration of the protocol

Computational self-testing protocol

Device must have prepared EPR pair and measured single qubits in computational or Hadamard basis

Certified entropy of device's measurement outcomes conditioned on side information

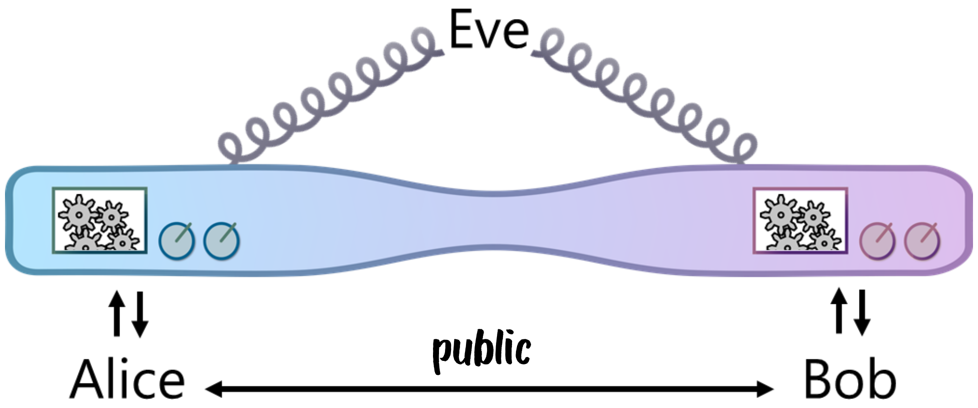
Devetak & Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. A. 461207–235 (2005)

Computational self-testing protocol

Computational self-testing

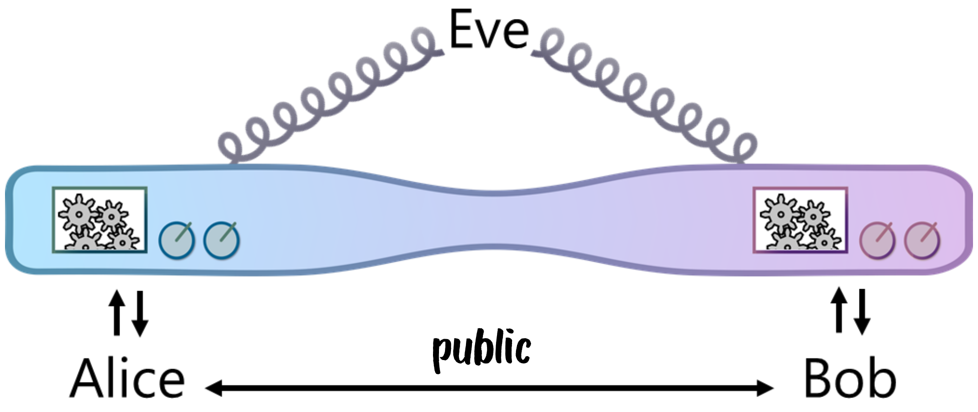
Classical **interactive protocol** run by Alice and Bob

Device can win or lose



Computational self-testing

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



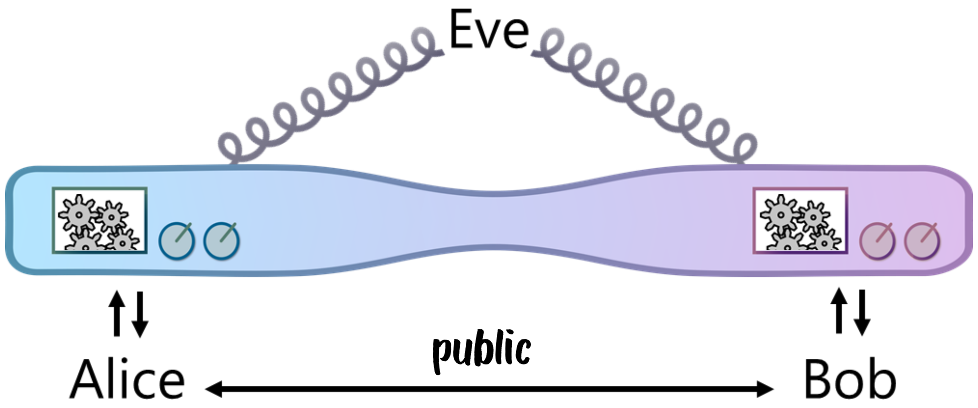
Device can win or lose

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



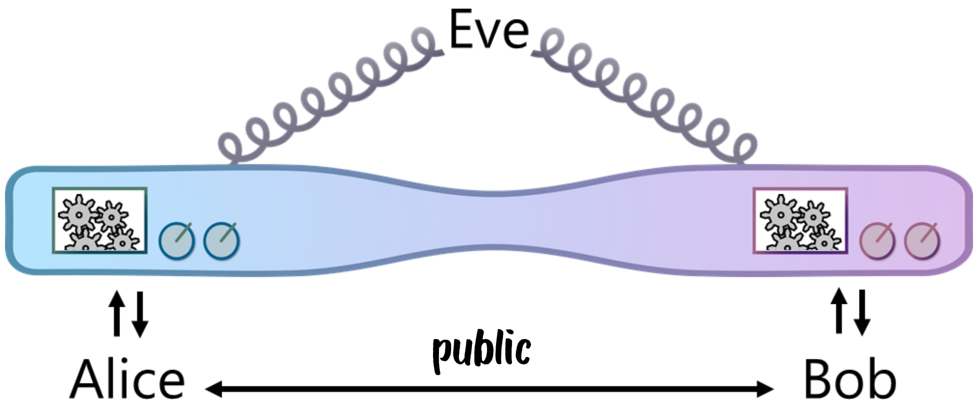
If a **computationally bounded device** wins with probability (close to) 1:

- 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



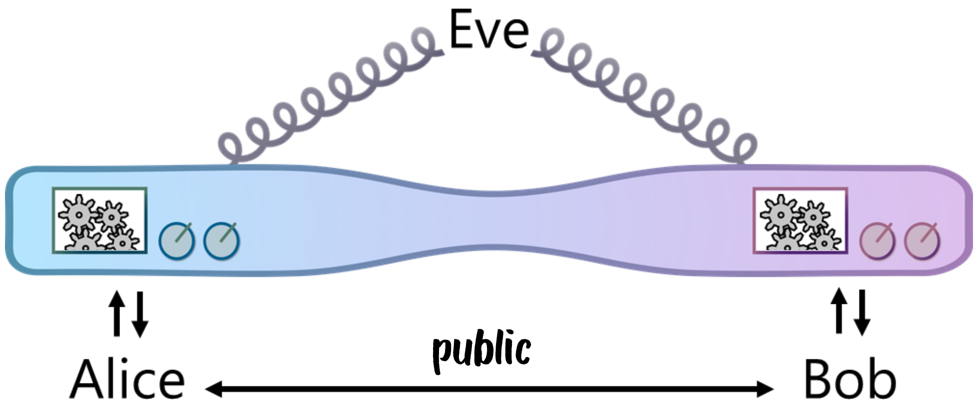
If a **computationally bounded device** wins with probability (close to) 1:

- 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:

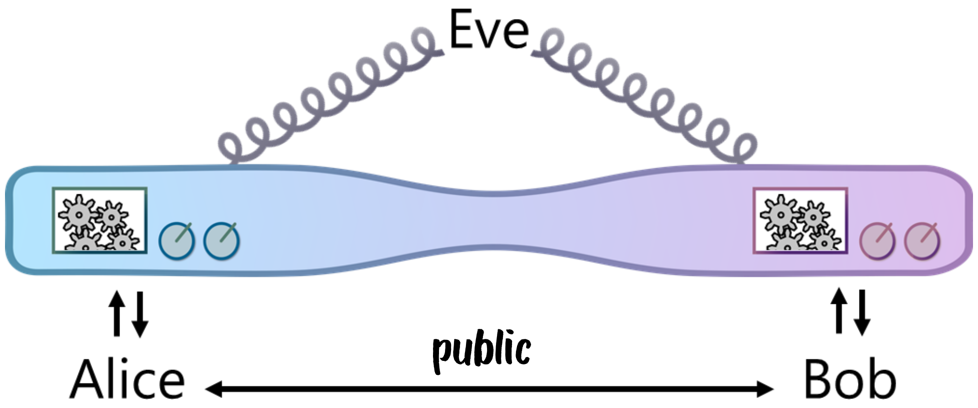
- the **state** prepared by the device must have been an EPR pair
- the device must have **measured** each qubit in the bases requested by Alice and Bob, respectively

up to **global** changes of basis.

Computational self-testing

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

Device can win or lose



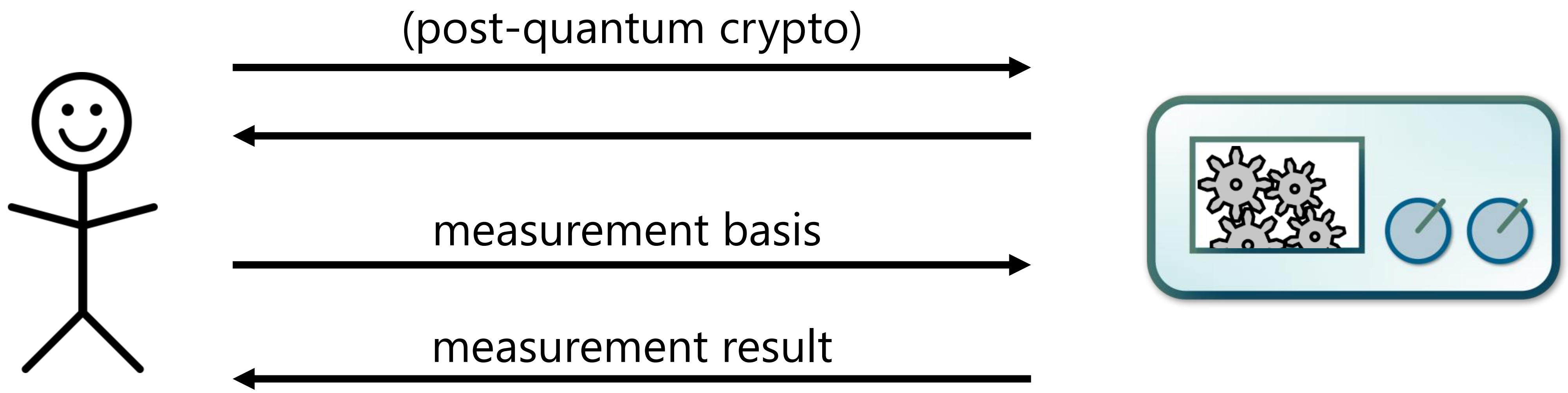
If a **computationally bounded device** wins with probability (close to) 1:

- 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.

Remote state preparation [GV’19]

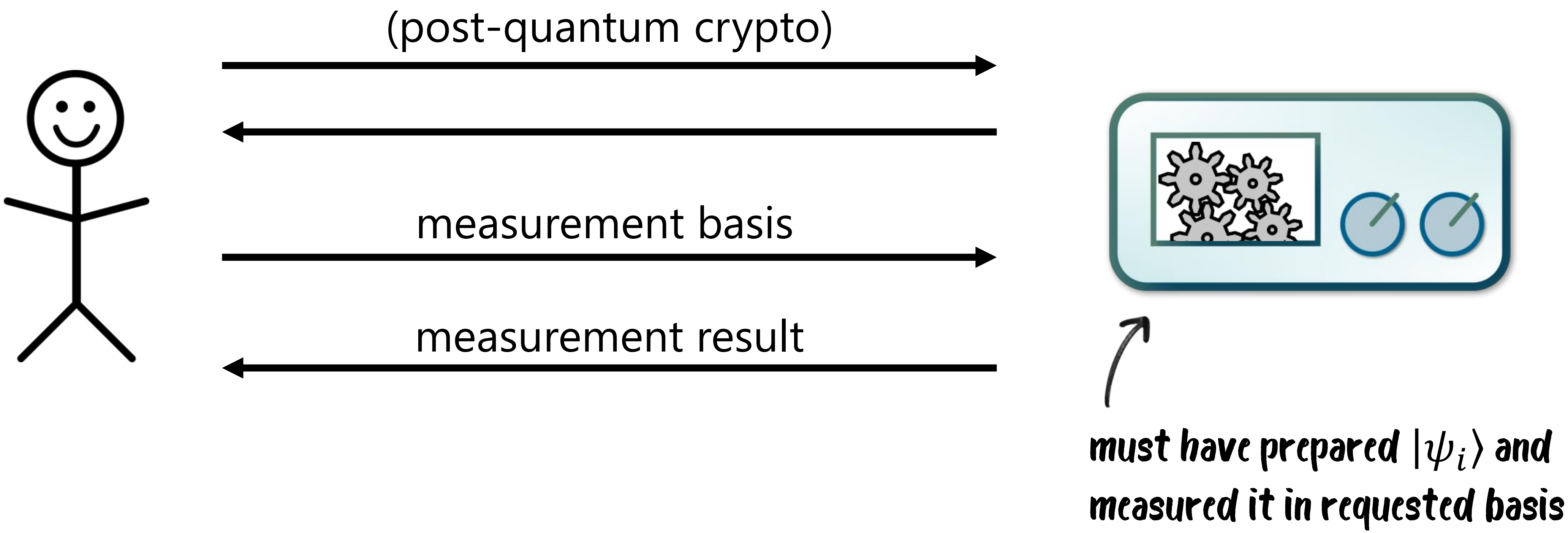
Given: set of **single-qubit** states $\{|\psi_i\rangle\} = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$



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

Remote state preparation [GV'19]

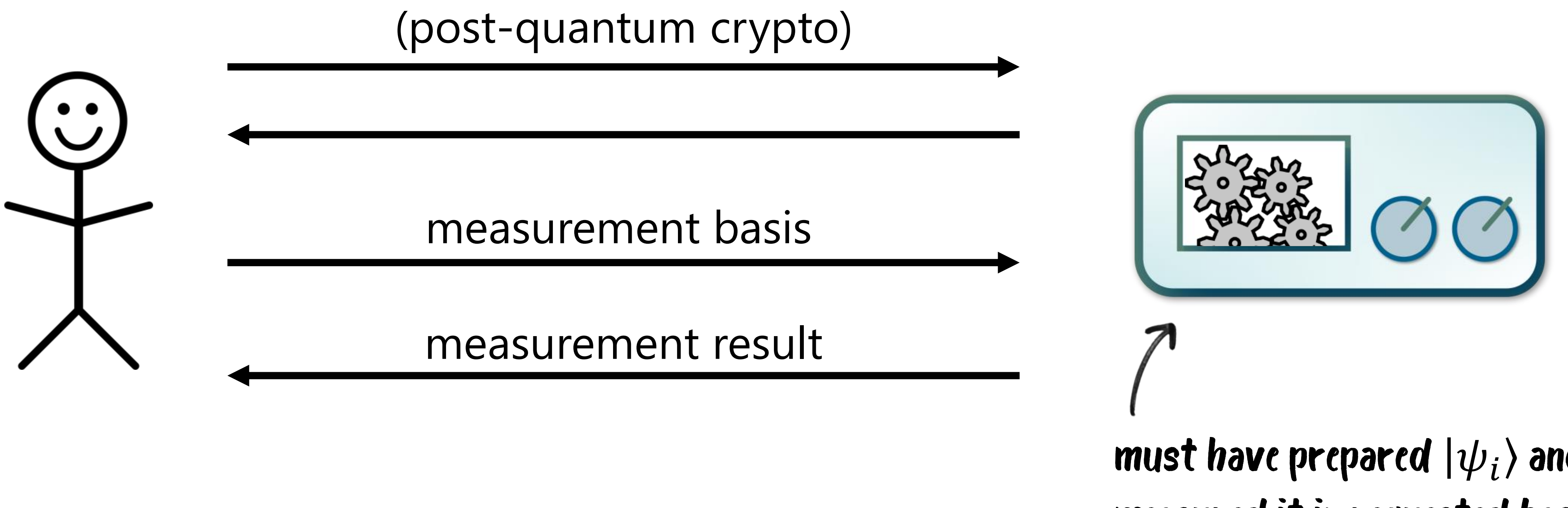
Given: set of **single-qubit** states $\{|\psi_i\rangle\} = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$



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

Remote state preparation [GV'19]

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



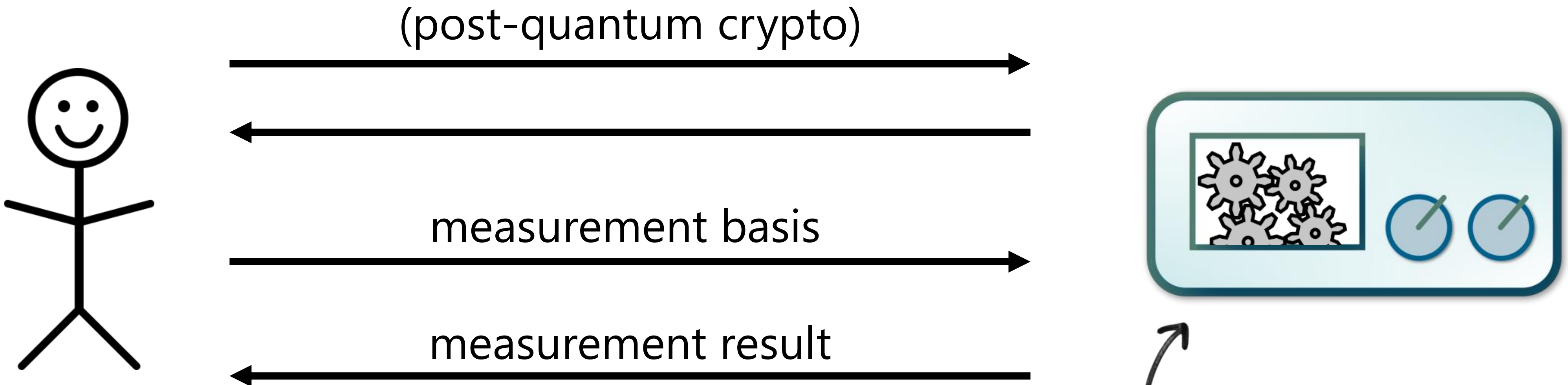
knows which state $|\psi_i\rangle$ the device has prepared

must have prepared $|\psi_i\rangle$ and measured it in requested basis

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

Remote state preparation [GV'19]

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



knows which state $|\psi_i\rangle$
the device has prepared

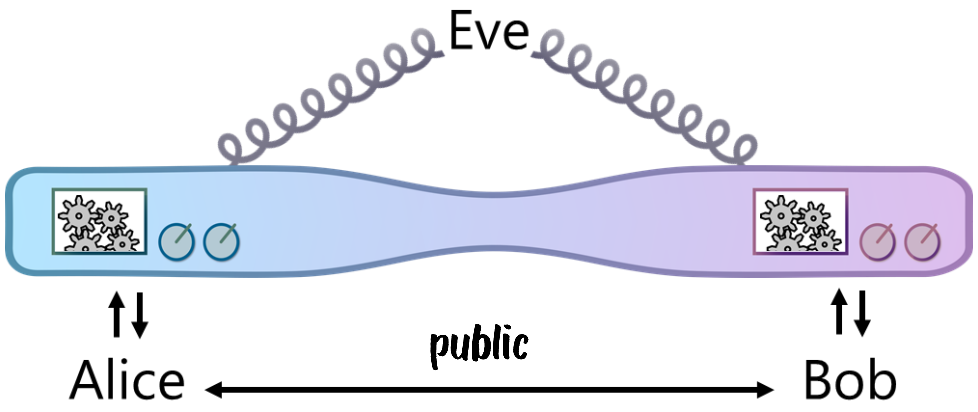
must have prepared $|\psi_i\rangle$ and
measured it in requested basis

But: device does not which $|\psi_i\rangle$
it has prepared

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

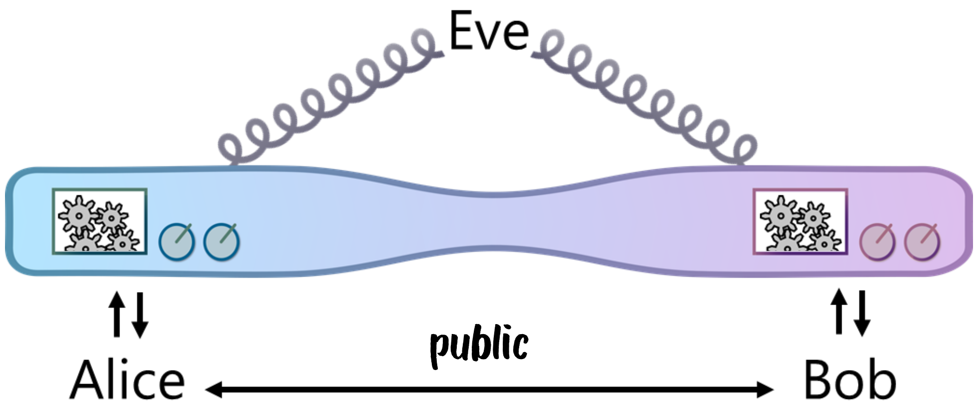
Main challenges for self-testing EPR states

- 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

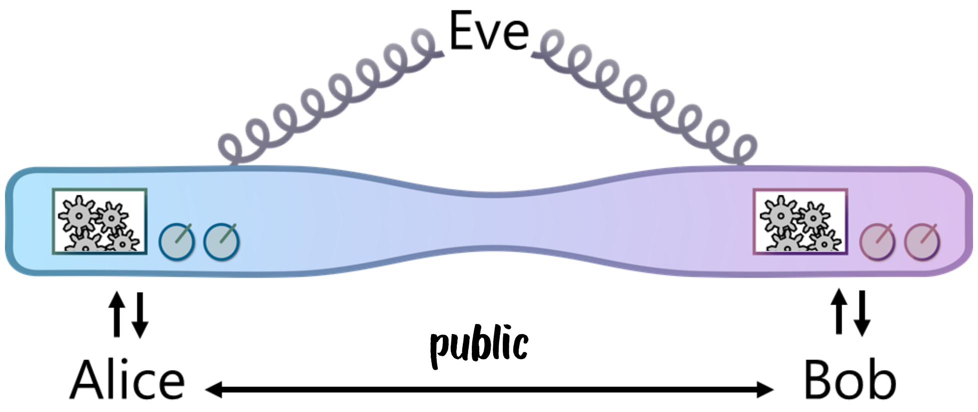
- Device should prepare two qubits and perform single-qubit measurements
  → Alice and Bob need to enforce **tensor product structure** on device's global space



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

Main challenges for self-testing EPR states

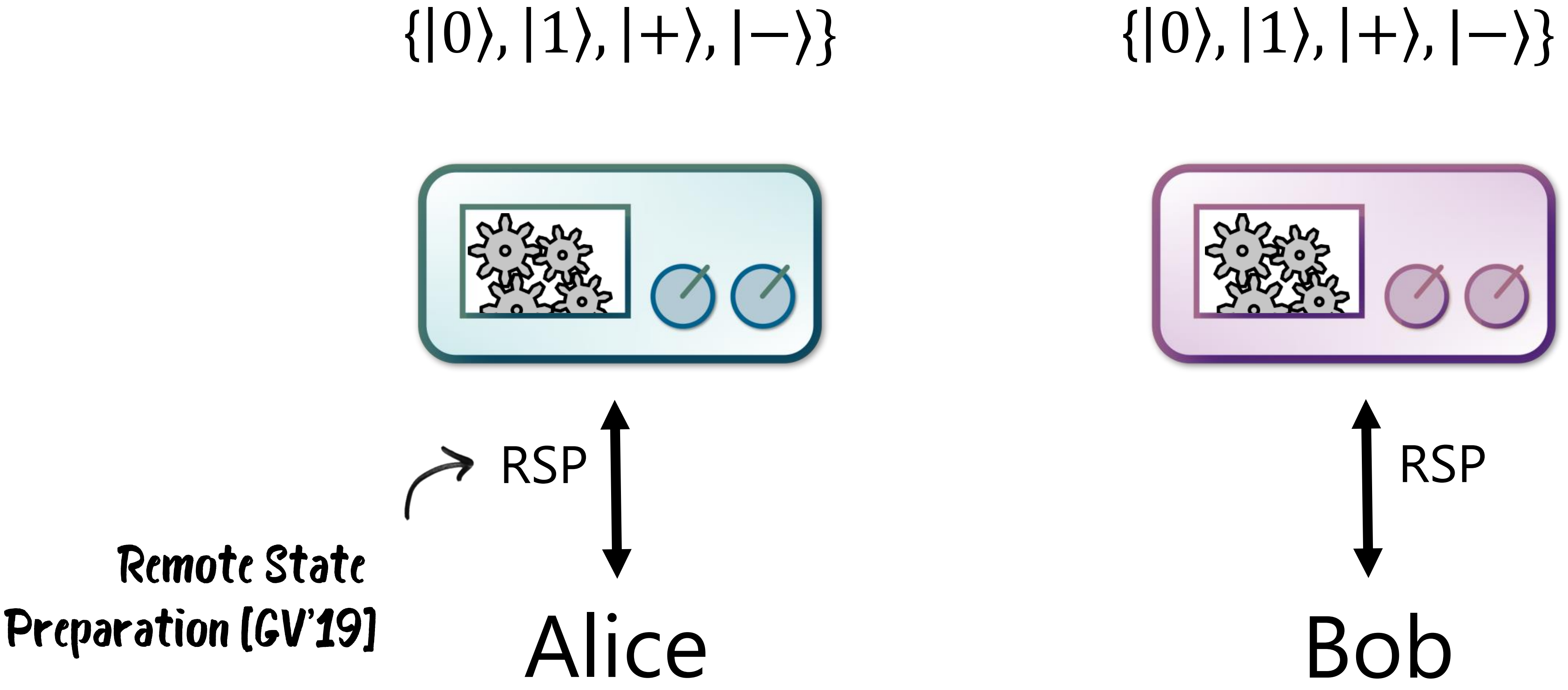
- Device should prepare two qubits and perform single-qubit measurements
  → Alice and Bob need to enforce **tensor product structure** on device's global space



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

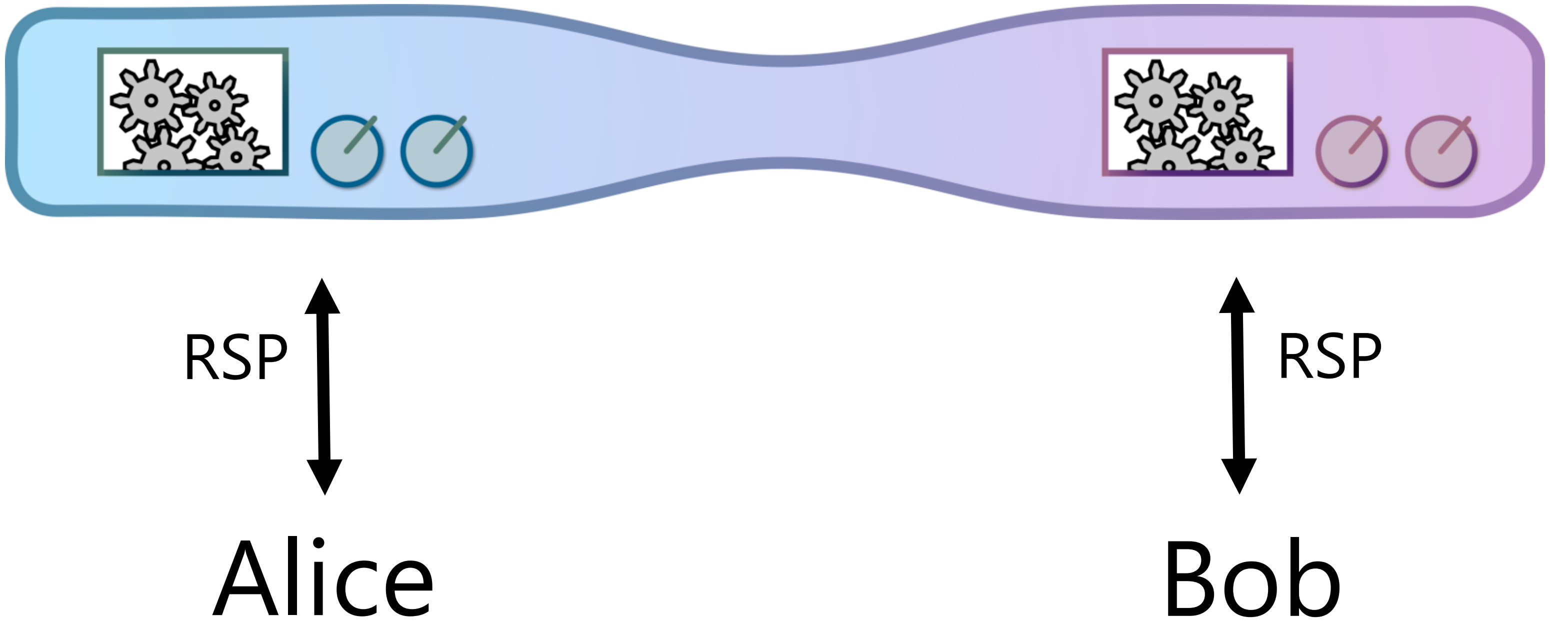
- **Honest** device should only have to use **local operations** and pre-shared EPR pairs

Remote state preparation with two isolated devices



Parallel implementation with single device

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

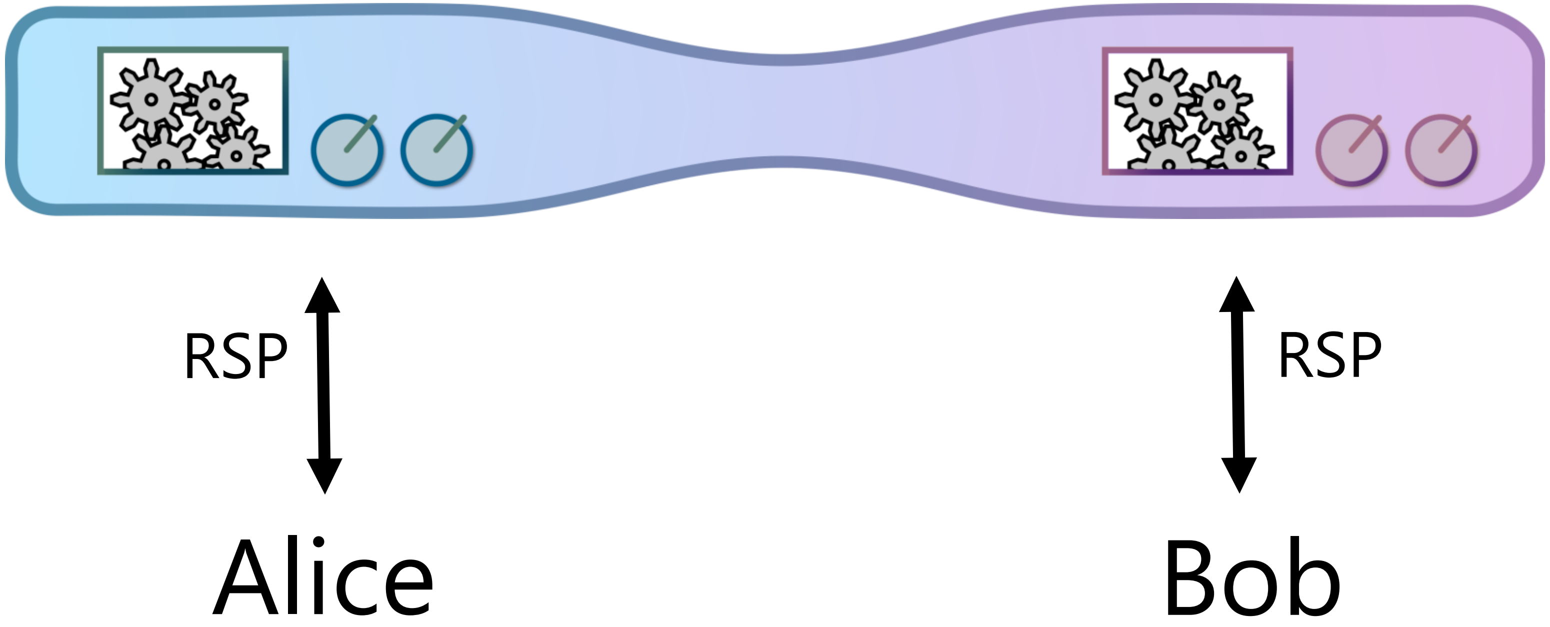


$$|0/1\rangle|0/1\rangle$$

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

$$|\pm\rangle|\pm\rangle$$

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

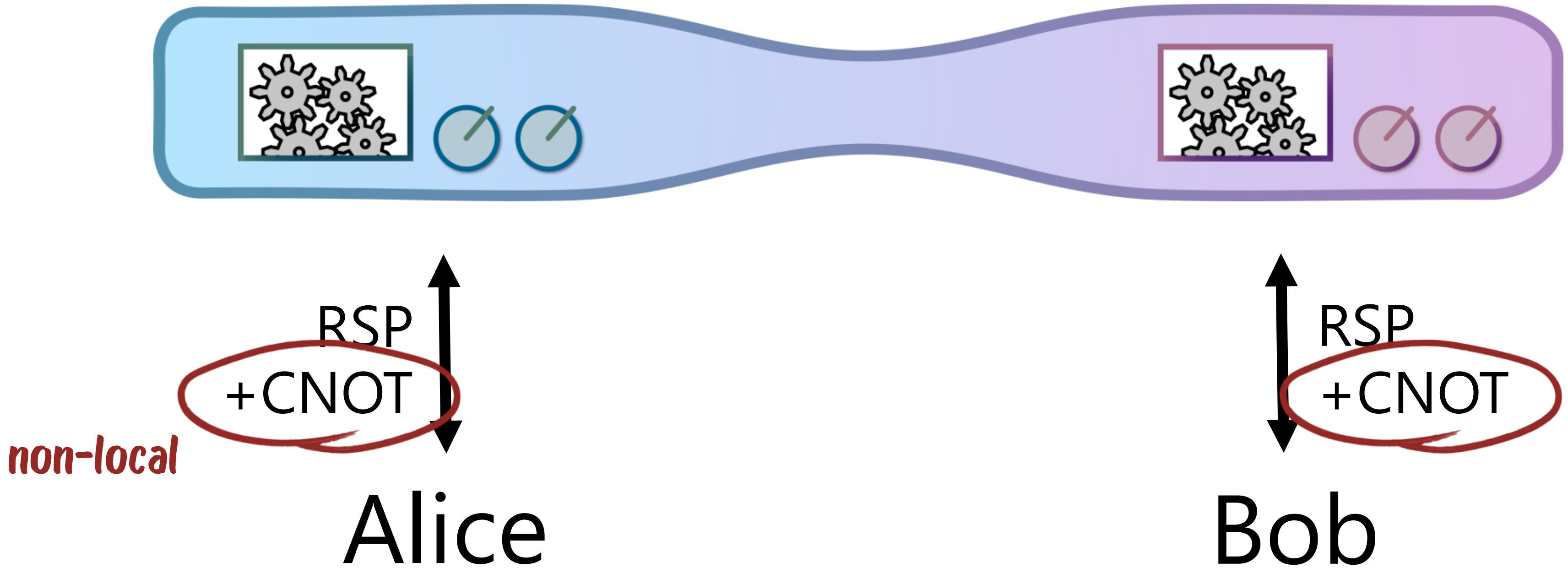


$|0/1\rangle|0/1\rangle$

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

$|\pm\rangle|\pm\rangle$

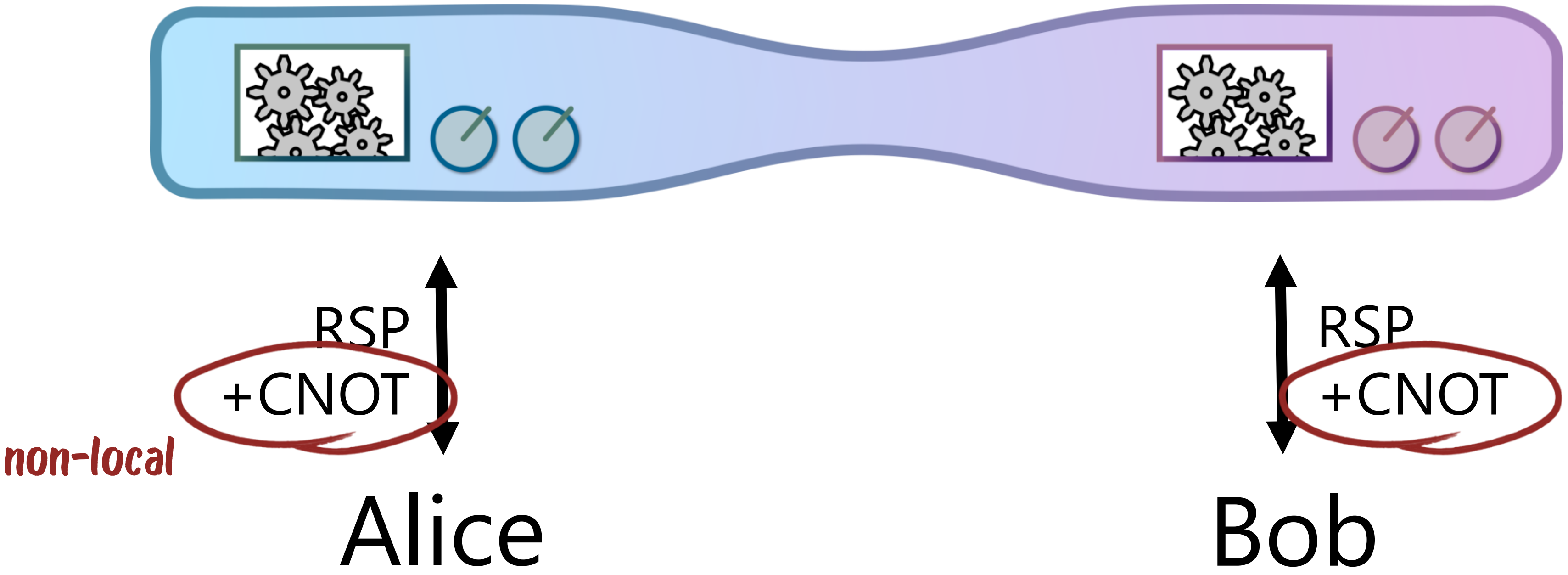
$|\pm\rangle|0/1\rangle$



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

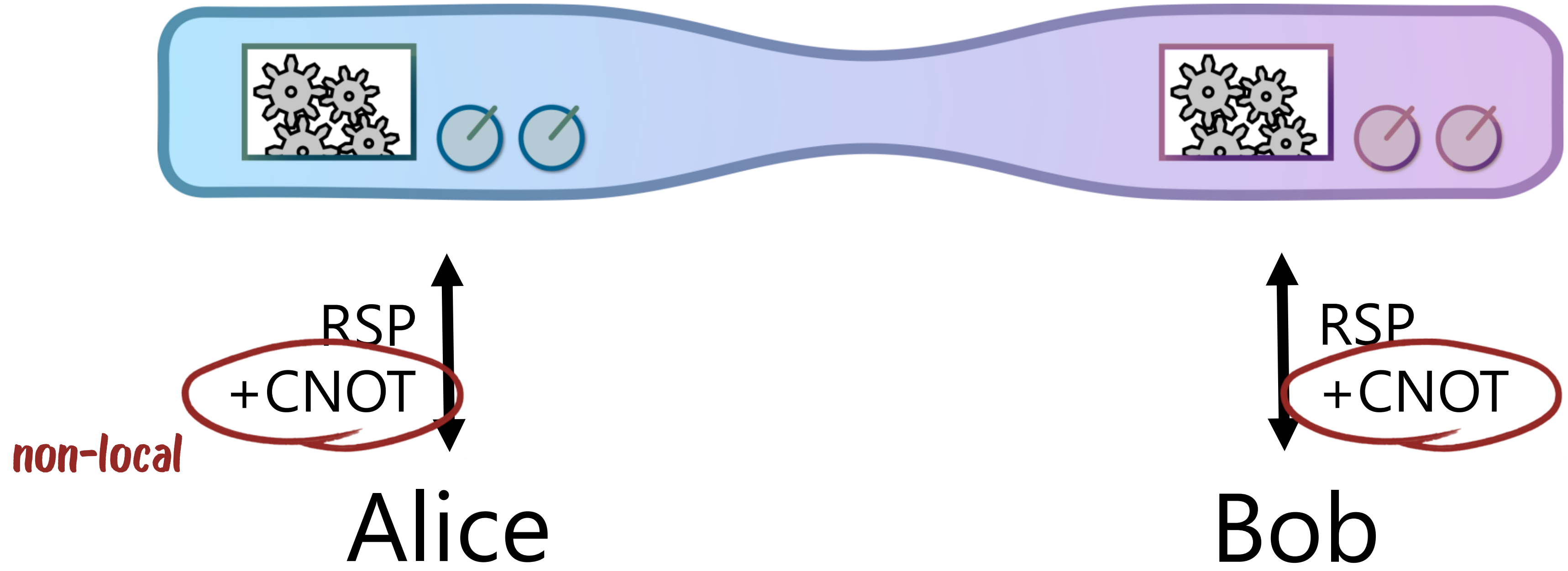
$|\pm\rangle|0/1\rangle$

CNOT $\longmapsto$



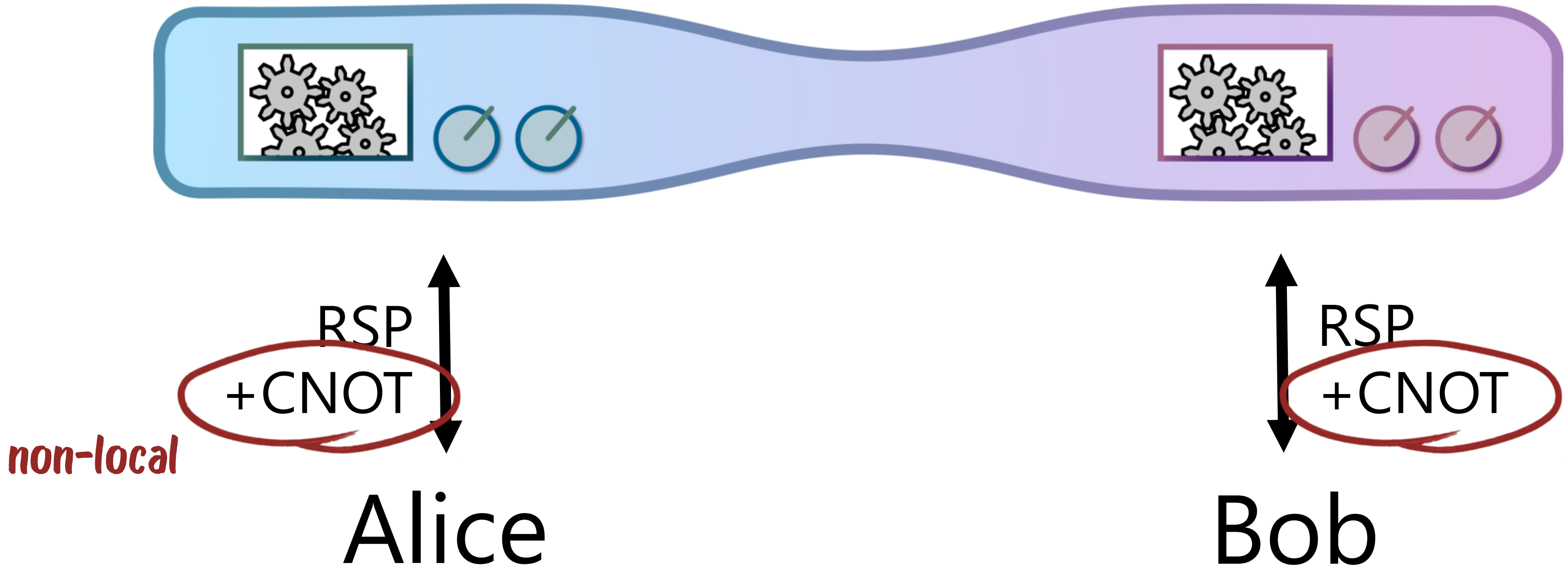
$$|0/1\rangle|0/1\rangle \qquad\qquad |0/1\rangle|0/1\rangle$$
$$|0/1\rangle|\pm\rangle \quad \xmapsto{\text{CNOT}} \quad |0/1\rangle|\pm\rangle$$
$$|\pm\rangle|\pm\rangle \qquad\qquad |\pm\rangle|\pm\rangle$$

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



$$|0/1\rangle|0/1\rangle \qquad\qquad |0/1\rangle|0/1\rangle$$
$$|0/1\rangle|\pm\rangle \quad \xmapsto{\text{CNOT}} \quad |0/1\rangle|\pm\rangle$$
$$|\pm\rangle|\pm\rangle \qquad\qquad |\pm\rangle|\pm\rangle$$

$$|\pm\rangle|0/1\rangle \qquad\qquad |00\rangle \pm |11\rangle, |01\rangle \pm |10\rangle$$

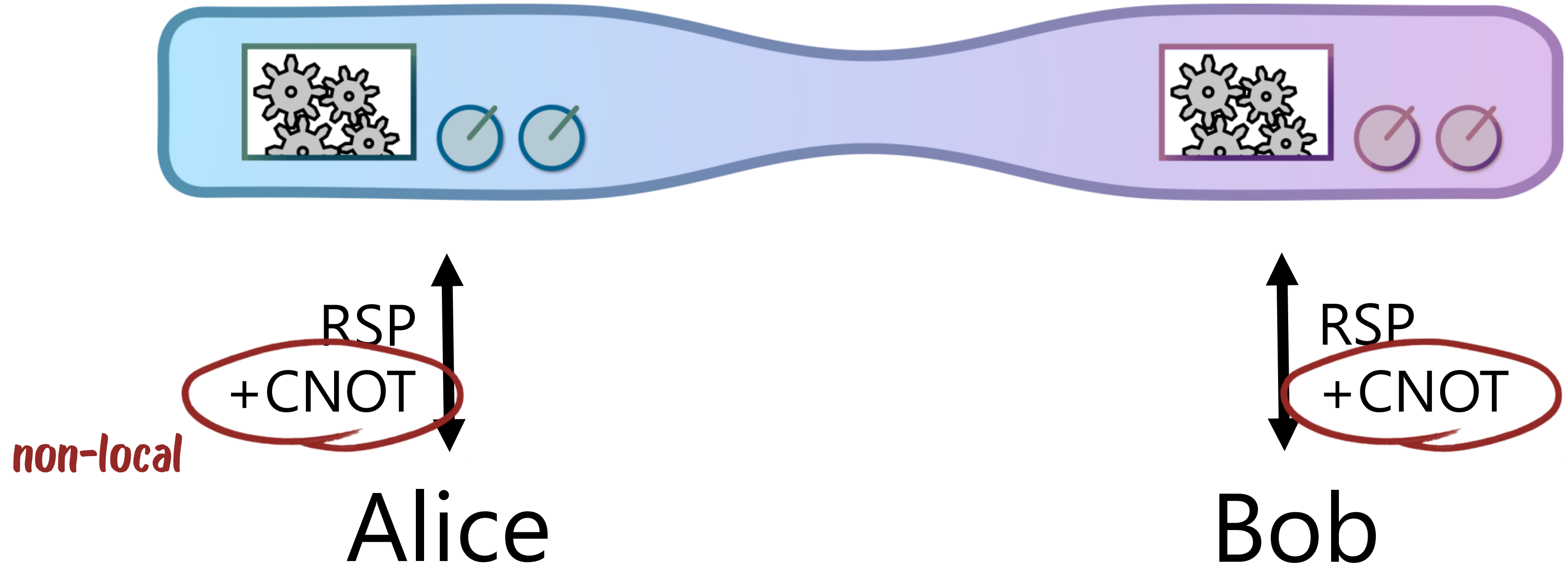


$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

CNOT $\longmapsto$

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

$|\pm\rangle|0/1\rangle$ $\quad$ $|00\rangle \pm |11\rangle, |01\rangle \pm |10\rangle$



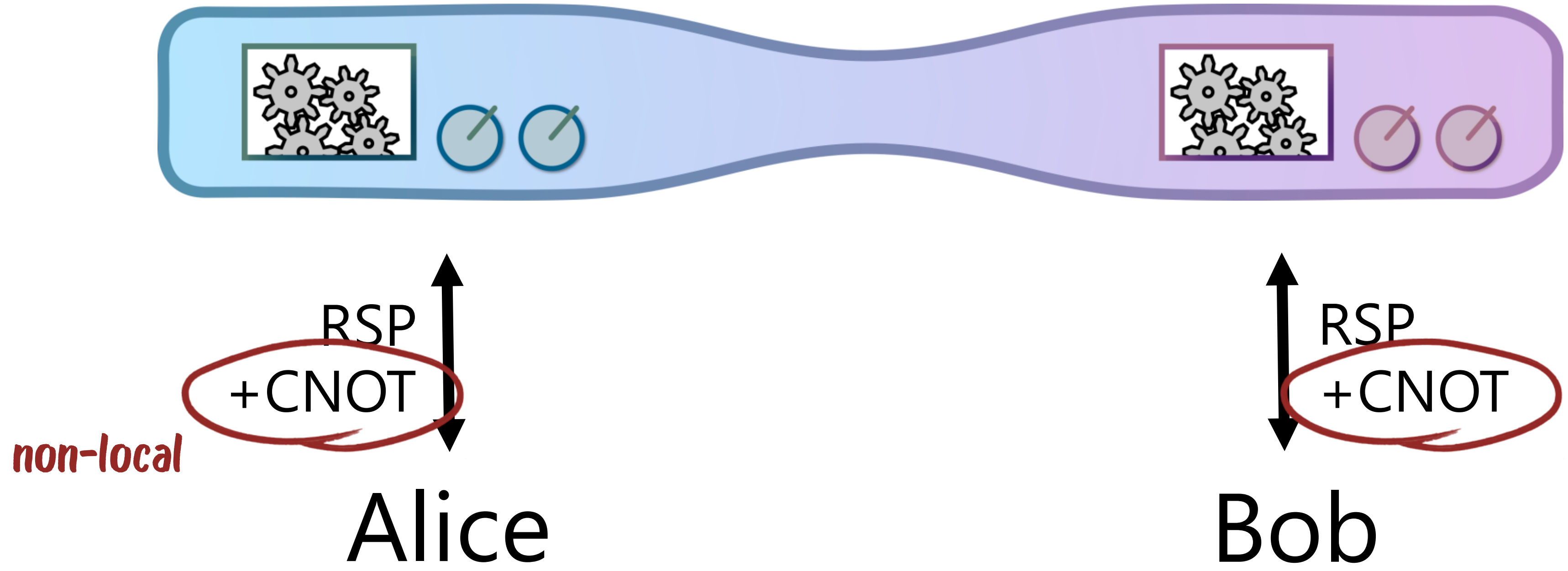
$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

CNOT $\longmapsto$

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

} Certify **single-qubit** measurements

$|\pm\rangle|0/1\rangle$ $\qquad$ $|00\rangle \pm |11\rangle, |01\rangle \pm |10\rangle$



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

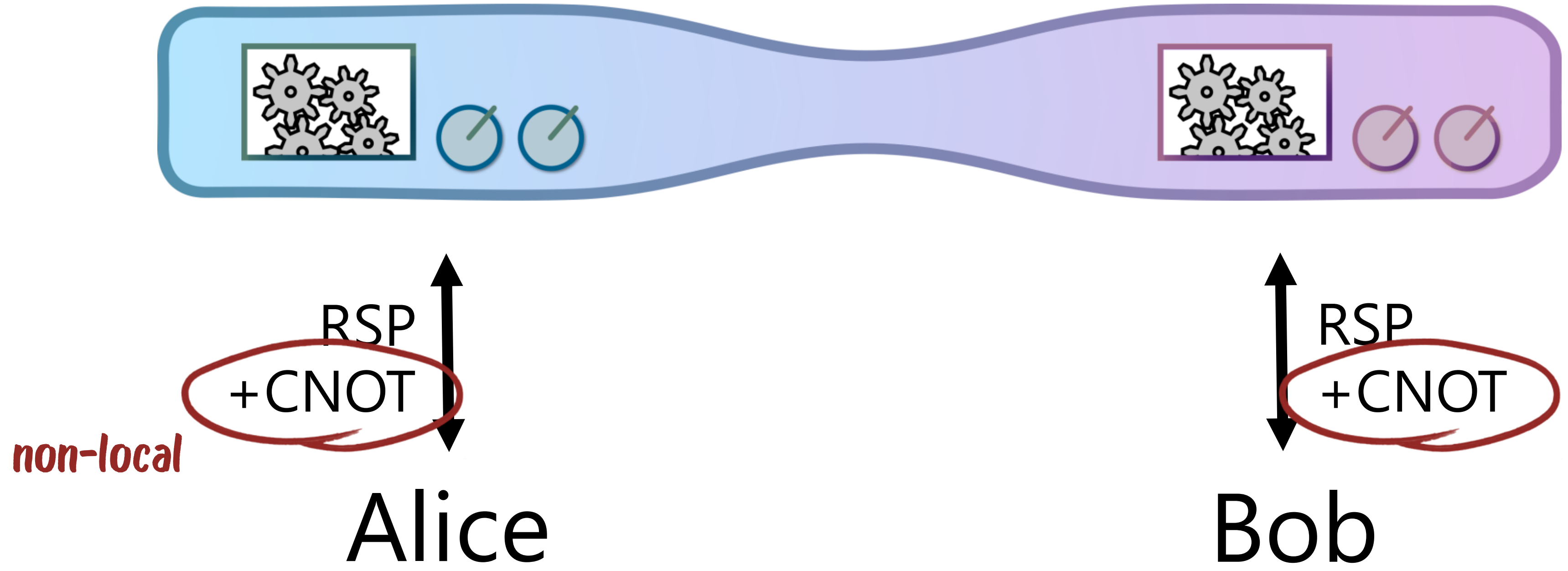
CNOT $\longmapsto$

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

Certify **single-qubit** measurements

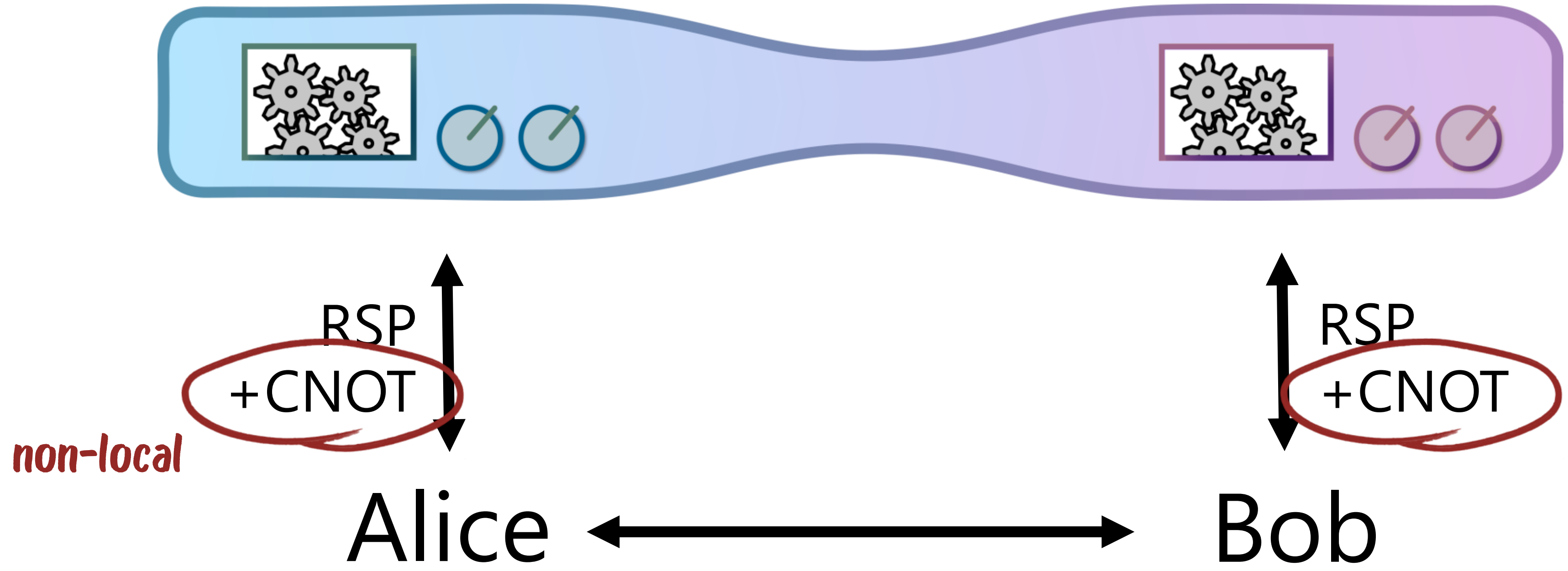
$|\pm\rangle|0/1\rangle$ $\quad$ $|00\rangle \pm |11\rangle, |01\rangle \pm |10\rangle$

Certify **Bell**-like correlations



$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$ $\xrightarrow{\text{CNOT}}$ $|0/1\rangle|0/1\rangle$, $|0/1\rangle|\pm\rangle$, $|\pm\rangle|\pm\rangle$ } Certify **single-qubit** measurements

$|\pm\rangle|0/1\rangle$ $\longmapsto$ $|00\rangle \pm |11\rangle, |01\rangle \pm |10\rangle$ Certify **Bell**-like correlations

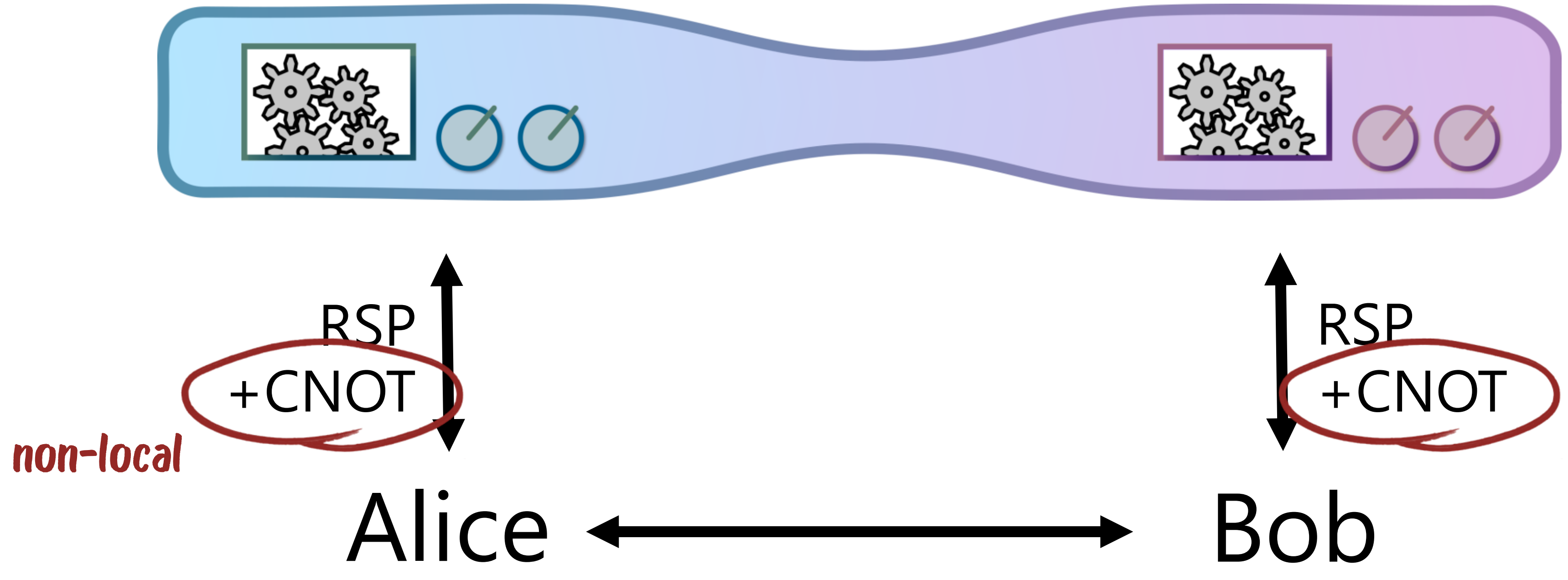


$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

Certify **single-qubit** measurements

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

Certify **Bell**-like correlations



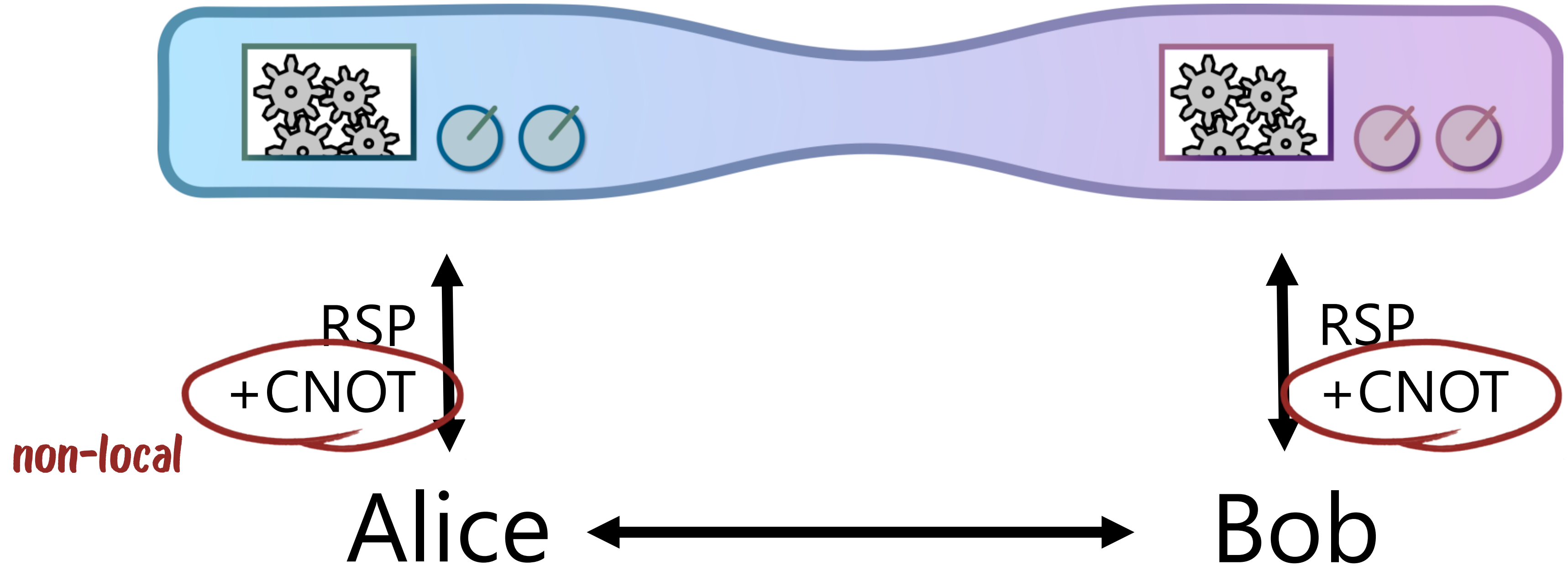
$|0/1\rangle|0/1\rangle$
$|0/1\rangle|\pm\rangle$
$|\pm\rangle|\pm\rangle$

} Certify **single-qubit** measurements

$|00\rangle \pm |11\rangle, |01\rangle \pm |10\rangle$ Certify **Bell**-like correlations

=> Blindness

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



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

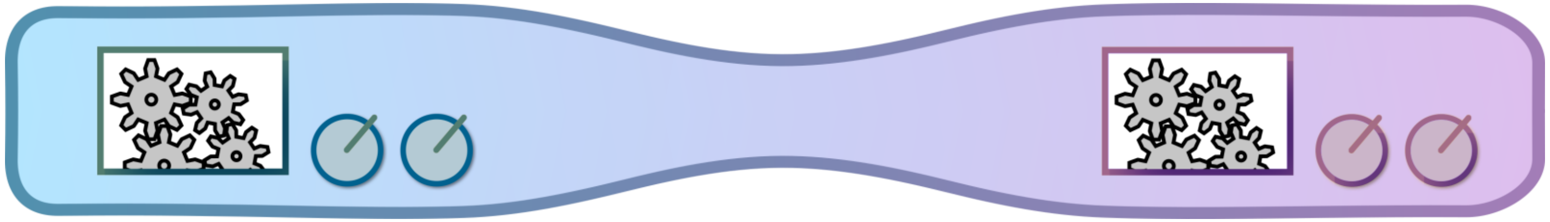
Certify **single-qubit** measurements

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

Certify **Bell**-like correlations

=> Blindness

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



RSP +gate teleportation

RSP +gate teleportation

Alice ⟷ Bob

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

(Incomplete) Genealogy

Proof of quantumness (1804.00640)

Verification of quantum computation (1804.01082)

(Incomplete) Genealogy

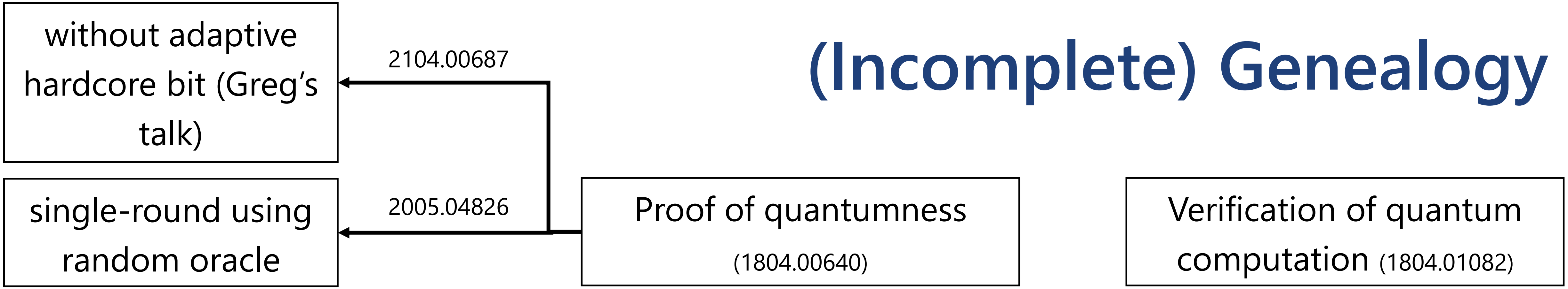
without adaptive hardcore bit (Greg's talk)

2104.00687

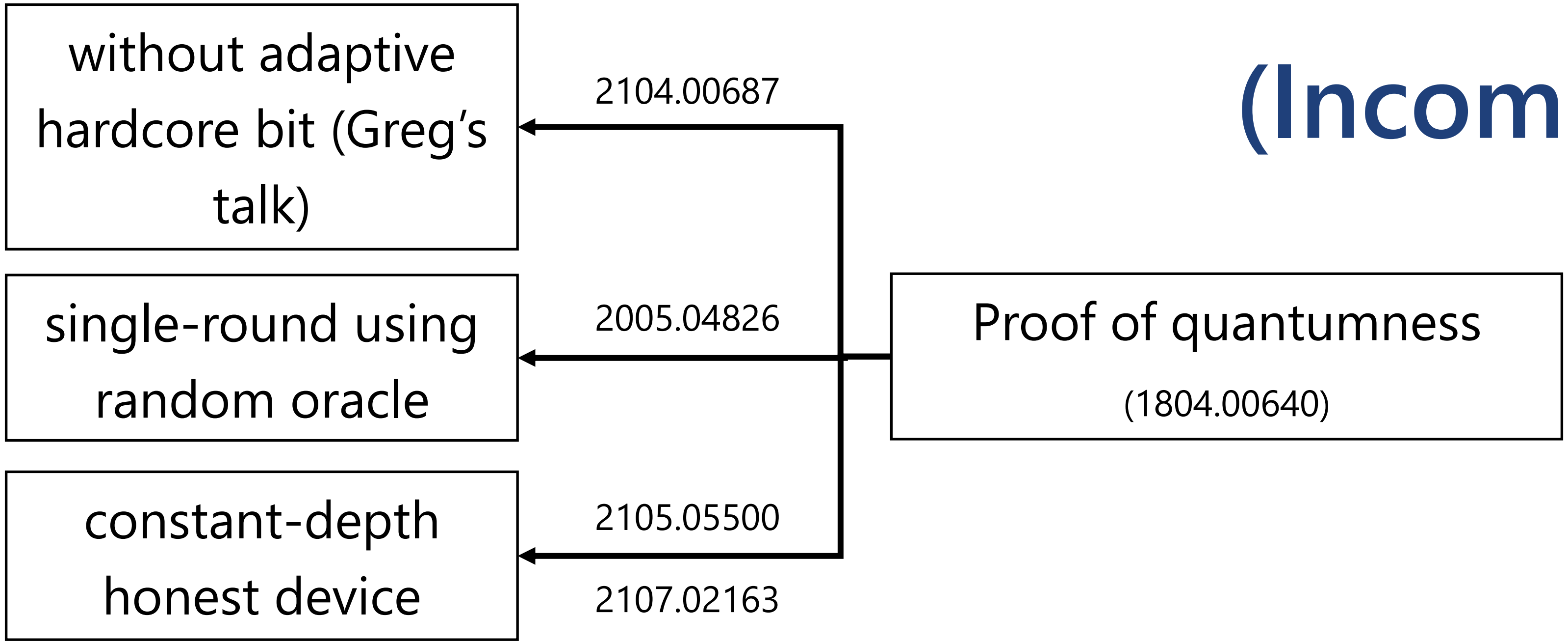
Proof of quantumness (1804.00640)

Verification of quantum computation (1804.01082)

(Incomplete) Genealogy

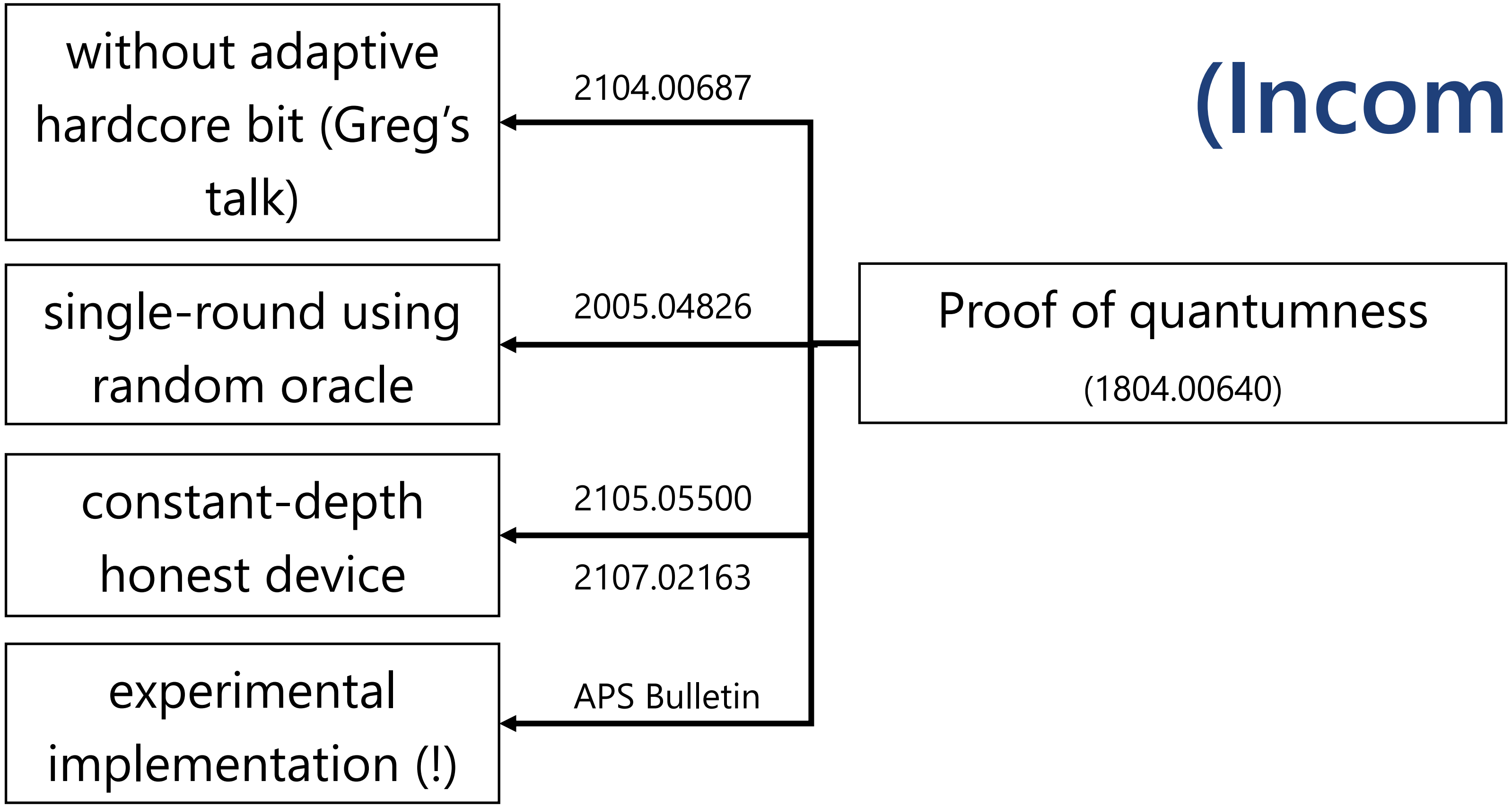


(Incomplete) Genealogy



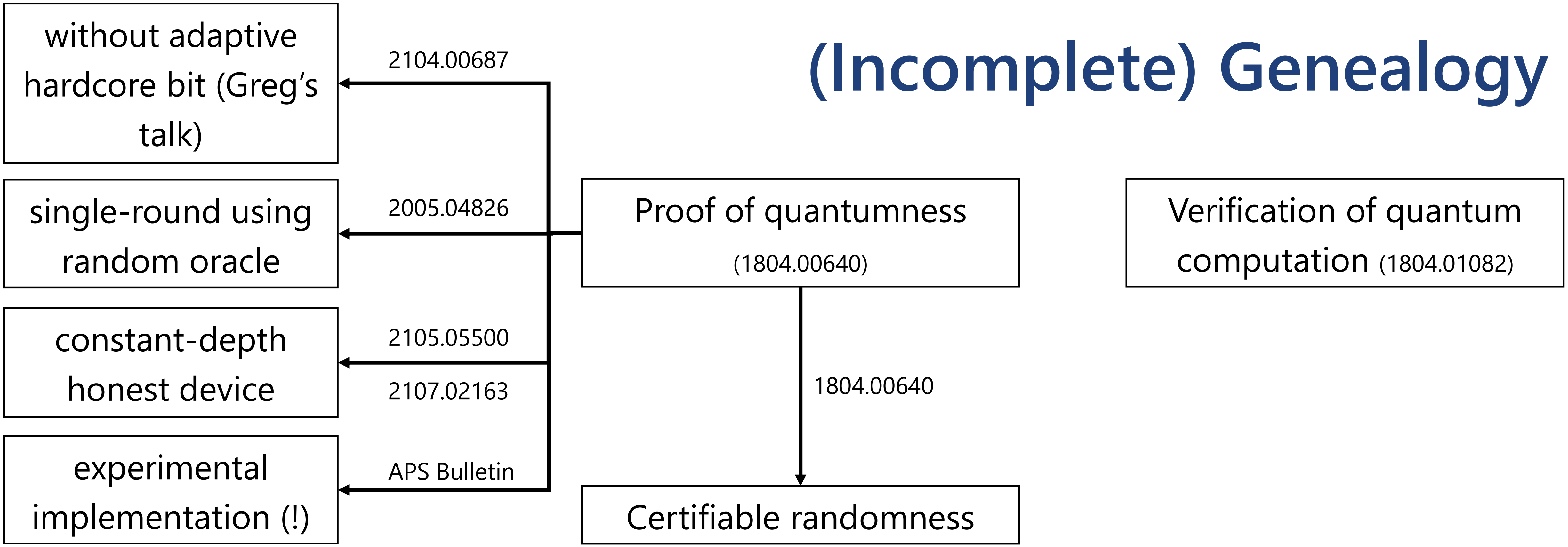
Verification of quantum computation (1804.01082)

(Incomplete) Genealogy

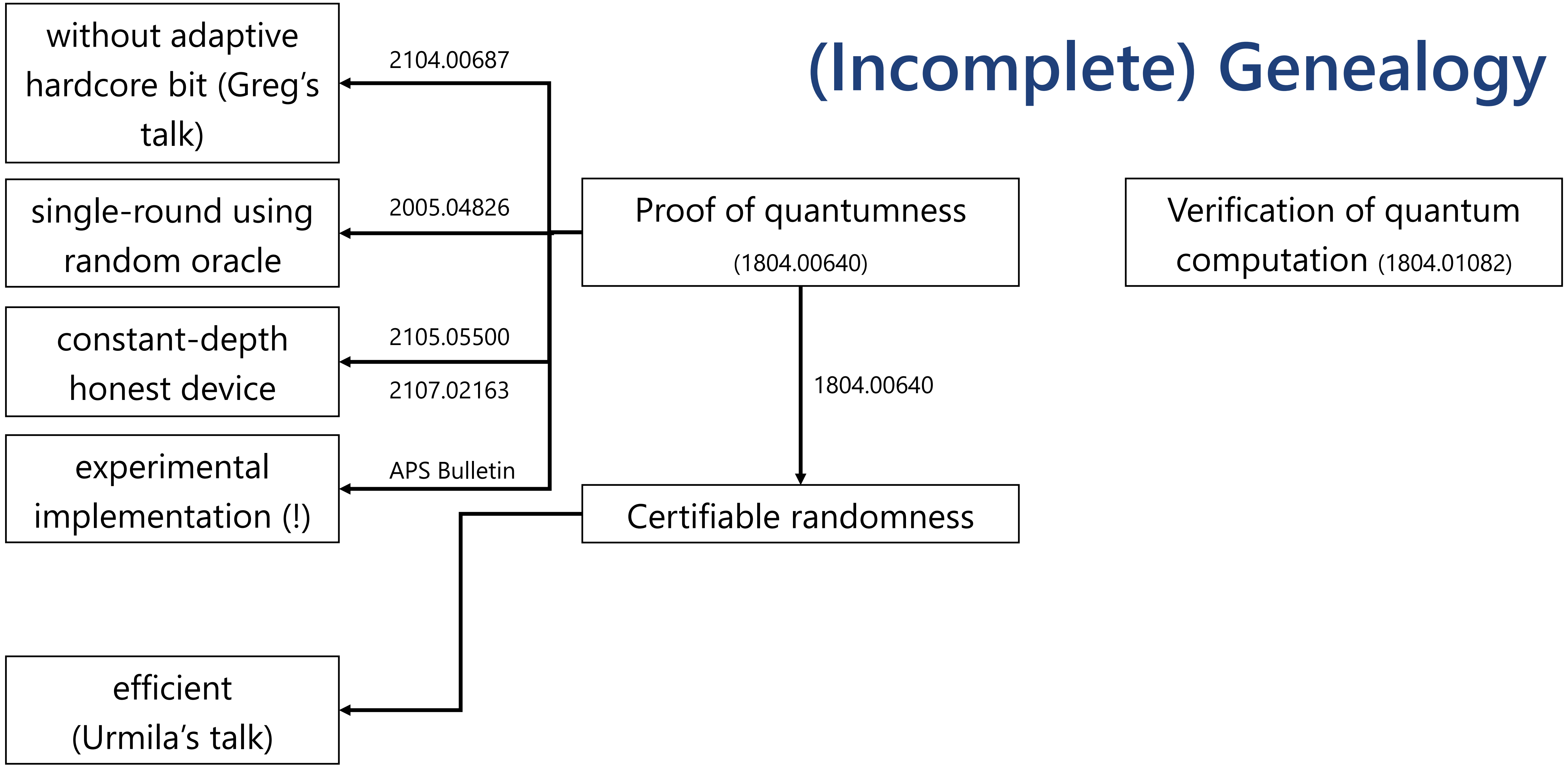


Verification of quantum computation (1804.01082)

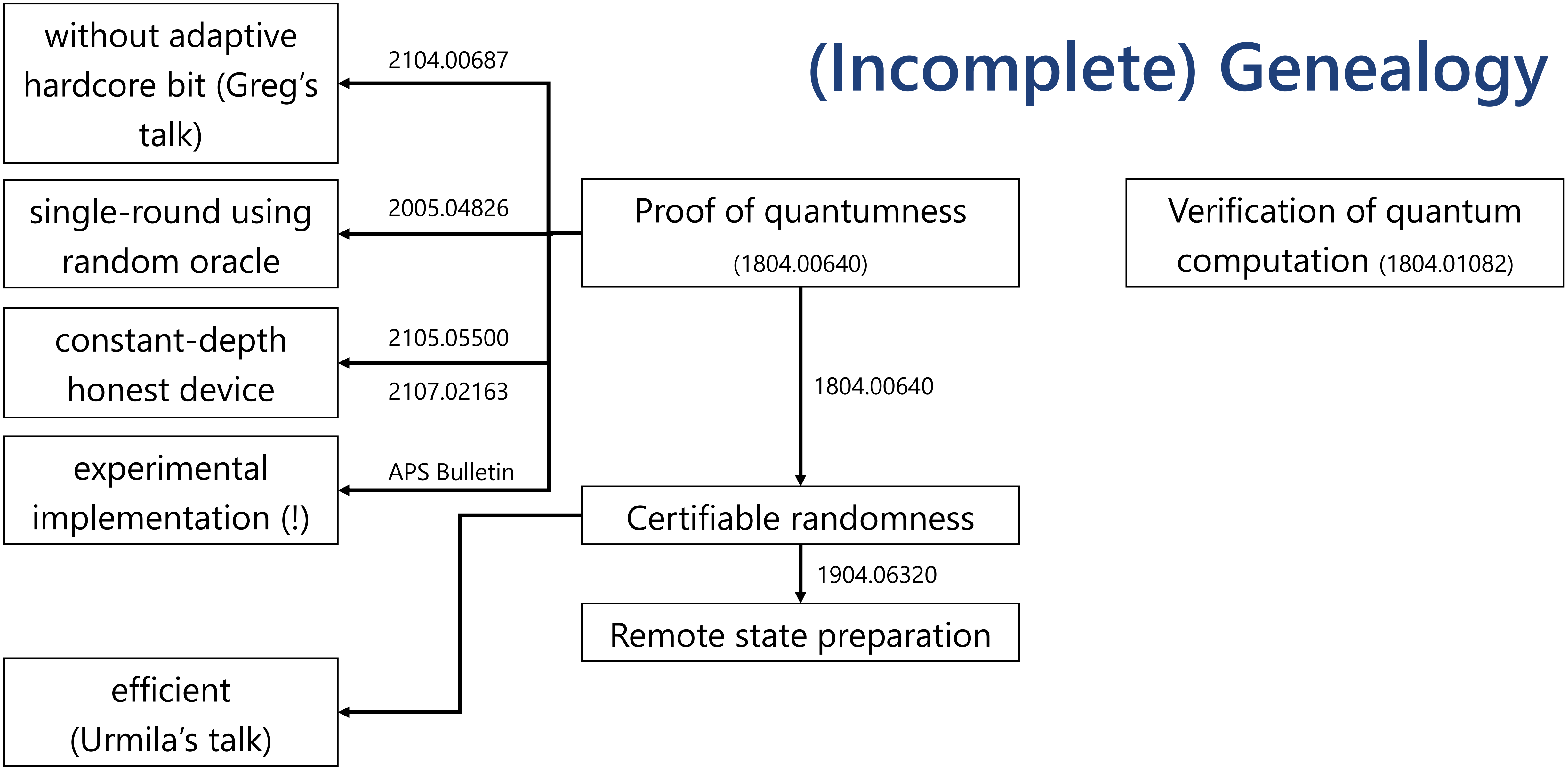
(Incomplete) Genealogy



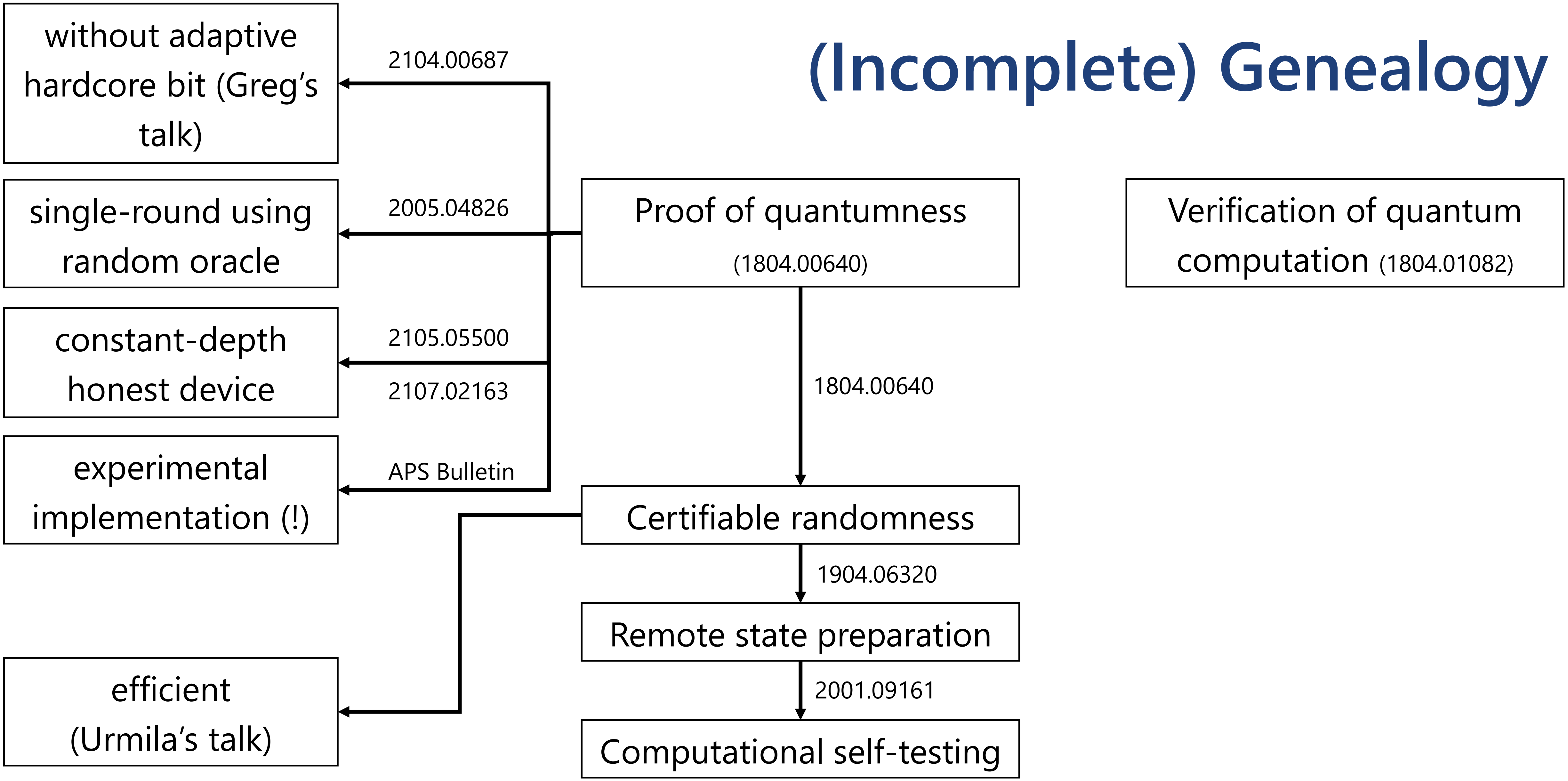
(Incomplete) Genealogy



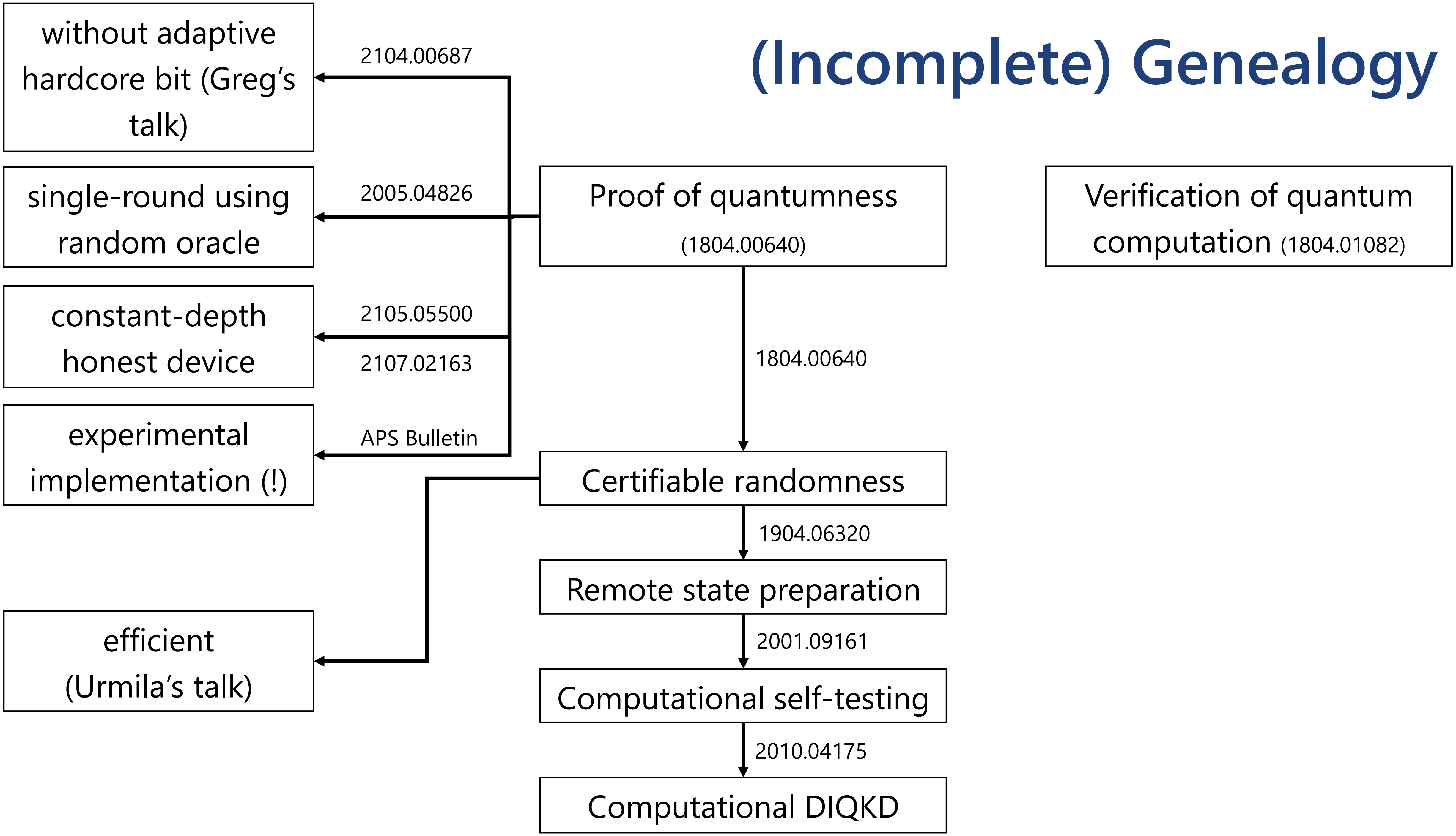
(Incomplete) Genealogy



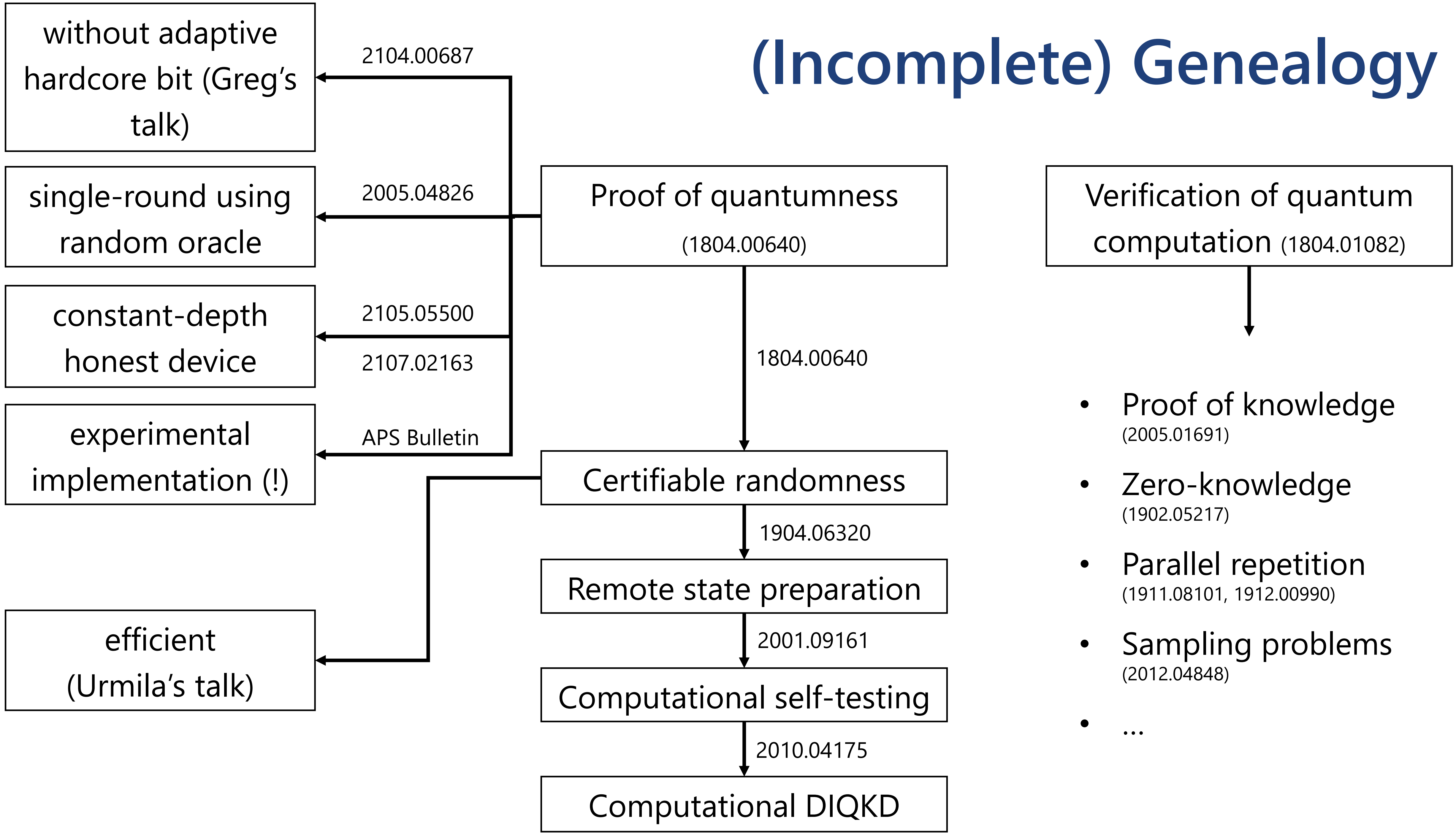
(Incomplete) Genealogy



(Incomplete) Genealogy



(Incomplete) Genealogy



References

(on previous slide: column by column, top to bottom)

Kahanamoku-Meyer, G.D., Choi, S., Vazirani, U.V. and Yao, N.Y., 2021. Classically-Verifiable Quantum Advantage from a Computational Bell Test. *arXiv preprint arXiv:2104.00687*.

Brakerski, Z., Koppula, V., Vazirani, U. and Vidick, T., 2020. Simpler proofs of quantumness. *arXiv preprint arXiv:2005.04826*.

Hirahara, S. and Gall, F.L., 2021. Test of Quantumness with Small-Depth Quantum Circuits. *arXiv preprint arXiv:2105.05500*.

Liu, Z. and Gheorghiu, A., 2021. Depth-efficient proofs of quantumness. *arXiv preprint arXiv:2107.02163*.

Zhu, D., Noel, C., Risinger, A., Egan, L., Biswas, D., Wang, Q., Nam, Y., Meyer, G., Vazirani, U., Yao, N. and Gheorghiu, A., 2021. Demonstration of Interactive Protocols for Classically-Verifiable Quantum Advantage. *Bulletin of the American Physical Society*.

Brakerski, Z., Christiano, P., Mahadev, U., Vazirani, U. and Vidick, T., 2018, October. A cryptographic test of quantumness and certifiable randomness from a single quantum device. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)* (pp. 320-331). IEEE.

Gheorghiu, A. and Vidick, T., 2019, November. Computationally-secure and composable remote state preparation. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)* (pp. 1024-1033). IEEE.

Metger, T. and Vidick, T., 2020. Self-testing of a single quantum device under computational assumptions. *arXiv preprint arXiv:2001.09161*.

Metger, T., Dulek, Y., Coladangelo, A. and Arnon-Friedman, R., 2020. Device-independent quantum key distribution from computational assumptions. *arXiv preprint arXiv:2010.04175*.

Mahadev, U., 2018, October. Classical verification of quantum computations. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)* (pp. 259-267). IEEE.

Vidick, T. and Zhang, T., 2021, October. Classical proofs of quantum knowledge. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 630-660). Springer, Cham.

Vidick, T. and Zhang, T., 2020. Classical zero-knowledge arguments for quantum computations. *Quantum*, *4*, p.266.

Alagic, G., Childs, A.M., Grilo, A.B. and Hung, S.H., 2020, November. Non-interactive classical verification of quantum computation. In *Theory of Cryptography Conference* (pp. 153-180). Springer, Cham.

Chia, N.H., Chung, K.M. and Yamakawa, T., 2019. Classical verification of quantum computations with efficient verifier. *arXiv preprint arXiv:1912.00990*.

Chung, K.M., Lee, Y., Lin, H.H. and Wu, X., 2020. Constant-round Blind Classical Verification of Quantum Sampling. *arXiv preprint arXiv:2012.04848*.