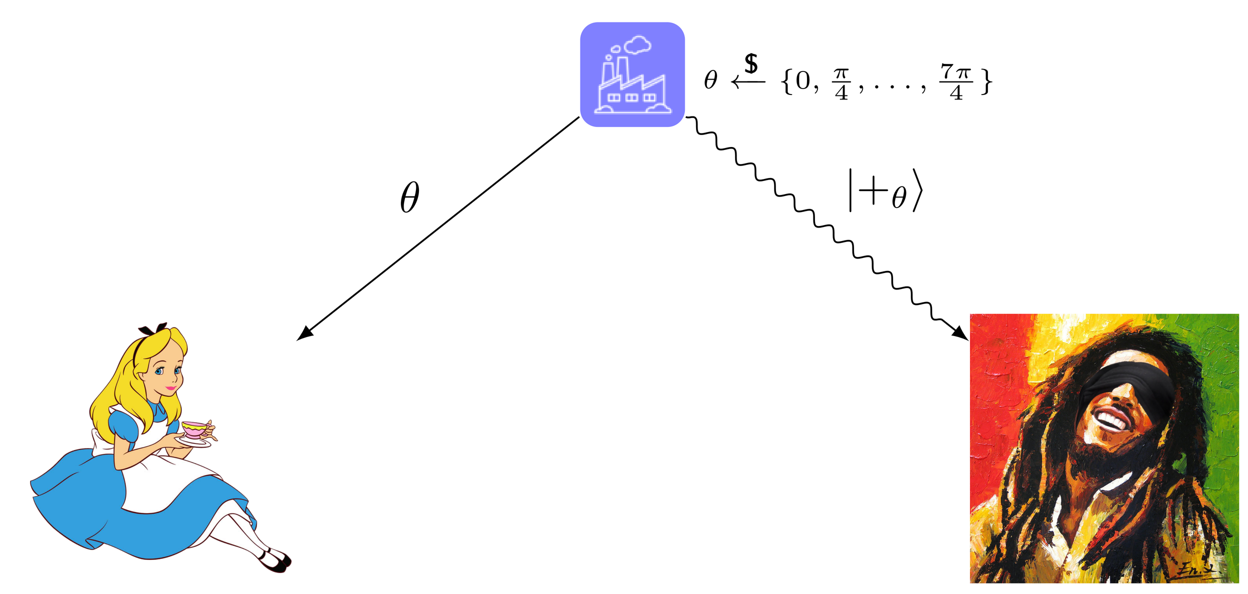
Security Limitations of Classical-Client Delegated Quantum Computing

Christian Badertscher, Alexandru Cojocaru, Léo Colisson,
Elham Kashefi, Dominik Leichtle, Atul Mantri, Petros Wallden

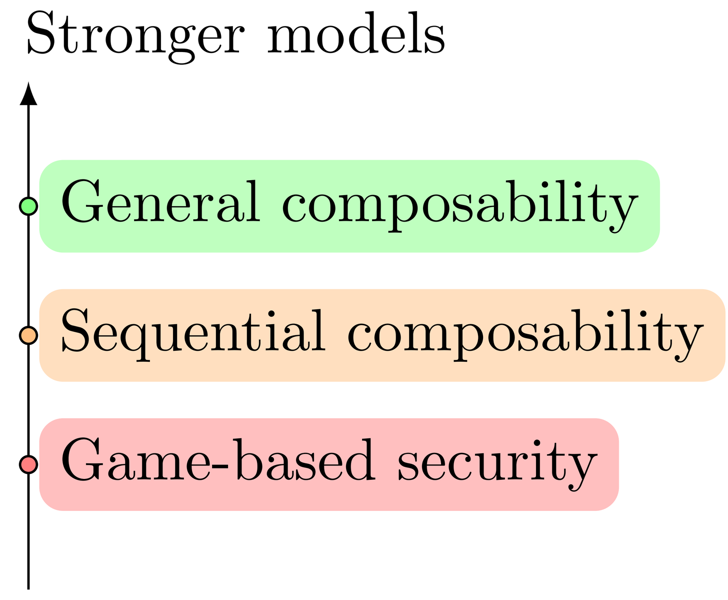
Full paper: arXiv:2007.01668

Intuitive definition of Remote State Preparation

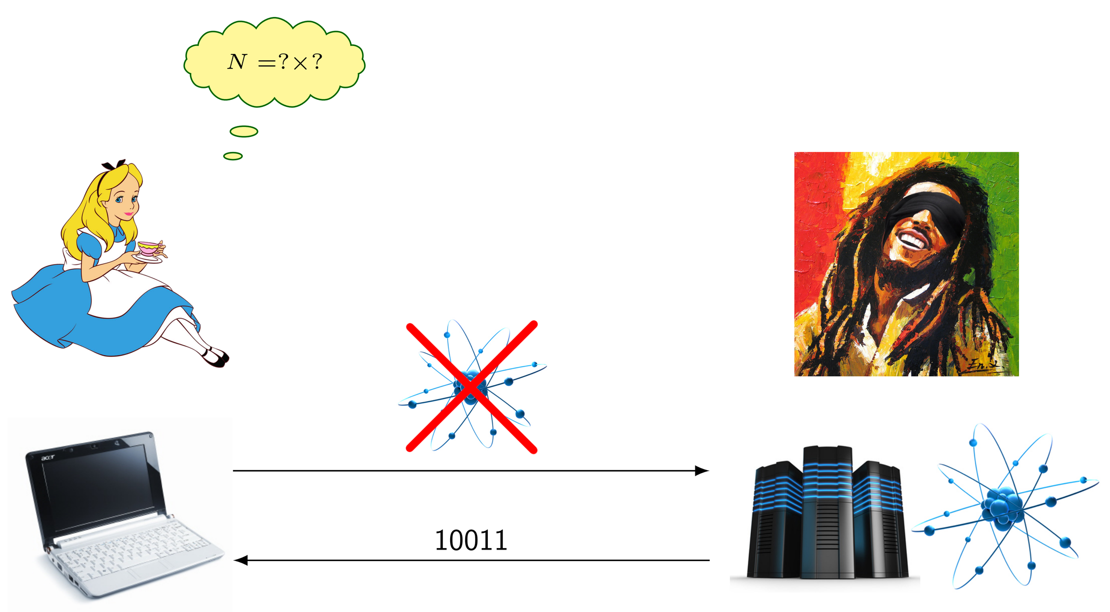


Intuitively, a **remote state preparation protocol** is a 2-party protocol that can be used to prepare a (unknown) quantum state on the server side, such that the classical description of this state is known to the client.
While this is easy to achieve in the presence of a quantum channel between the parties, there are also candidates when the **client is purely classical**.

Models of security



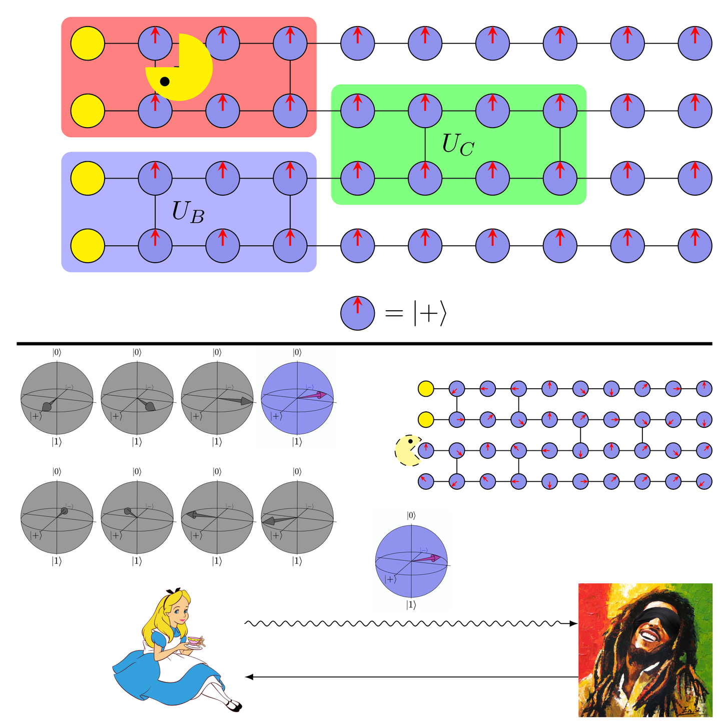
Why is it useful?



Classical-client Remote State Preparation protocols could be used to remove quantum channels in a **wide range of protocols**, including in:

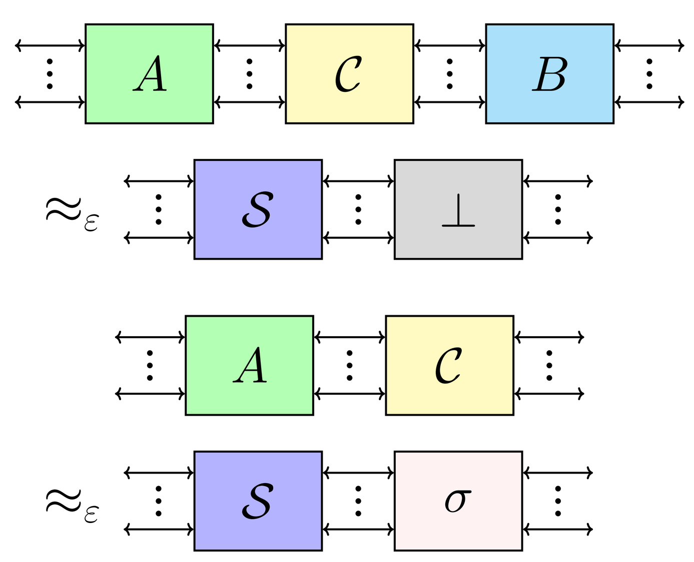
- Universal Blind Quantum Computing (UBQC, pictured on the right)
- verifiable quantum computing
- multi-party computing

However, the security of the combined protocol needs to be **proven separately for each protocol**.



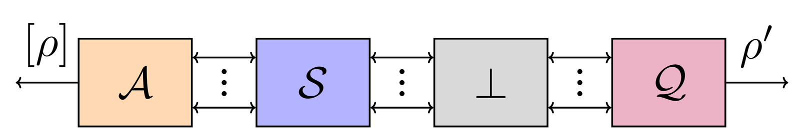
Constructive Crypto

Constructive Cryptography (CC) is a model of security that provides the strongest guarantee of **general (sequential + parallel) composability**. To prove that the protocol (A, B) securely realizes a resource $\mathcal{S}$ from a classical channel $\mathcal{C}$, one needs to find a simulator σ such that the following hold for a **computationally bounded distinguisher**:



Formalization of RSP

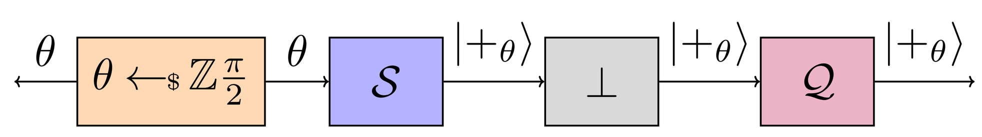
In order to have a more generic result, we introduce two converters $\mathcal{A}$ and $\mathcal{Q}$. Then, we say that a resource $\mathcal{S}$ is a **remote state preparation** (RSP) within ε with respect to $\mathcal{A}$ and $\mathcal{Q}$ if $\mathcal{S}$ can be used (with the help of $\mathcal{A}$ and $\mathcal{Q}$) to prepare (during an honest run) a quantum state ρ and a classical description $[\rho']$:



such that on average ρ is "close" to ρ':

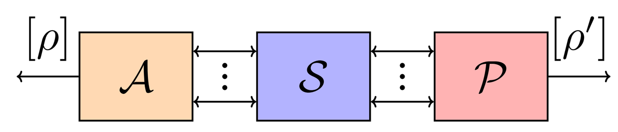
$$\mathop{\mathbb{E}}_{([\rho],\rho')\leftarrow\mathcal{A}\mathcal{S}\vdash\mathcal{Q}}[\operatorname{Tr}(\rho\rho')] \geq 1-\varepsilon$$

For example, the trivial resource that turns θ into $|+_\theta\rangle$ is a RSP resource within 0:



Describability

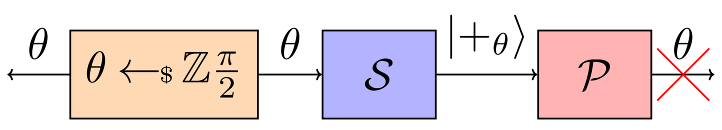
"Describability" is a notion that expresses the fact that a malicious party can extract the description of a state outputted on the left interface given only access to the right interface. Formally, we say that $\mathcal{S}$ is **describable** within ε with respect to a converter $\mathcal{A}$ if there exists a (possibly unbounded) converter $\mathcal{P}$ outputting a classical description $[\rho']$:



such that on average, ρ' is "close" to ρ:

$$\mathop{\mathbb{E}}_{([\rho],[\rho'])\leftarrow\mathcal{A}\mathcal{S}\mathcal{P}}[\operatorname{Tr}(\rho\rho')] \geq 1-\varepsilon$$

The previous resource is **not** describable within 0 due to the no-cloning principle:



Result 1

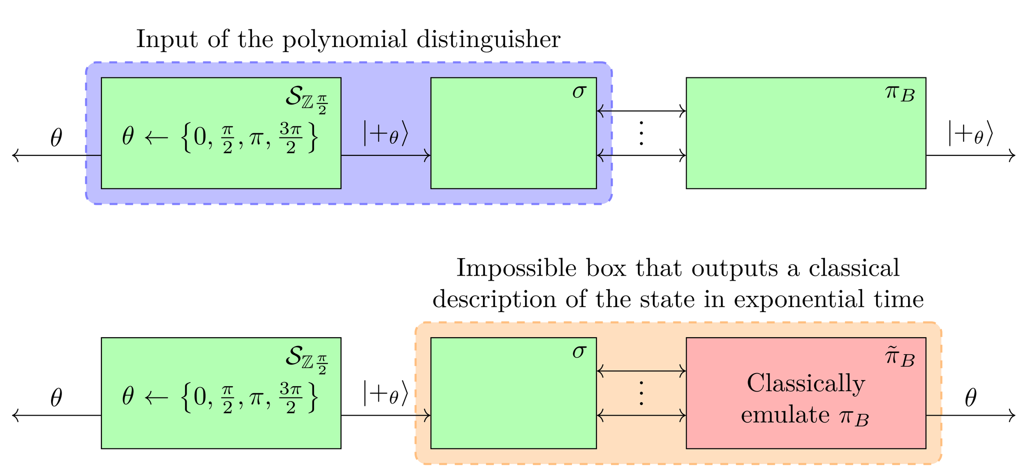
Theorem: RSP ⇒ describable

If an ideal resource $\mathcal{S}$ is both RSP within ε_1 with respect to some $\mathcal{A}$ and $\mathcal{Q}$ and classically-realizable within ε_2 (including against only polynomially bounded distinguishers), then it is describable within $\varepsilon_1 + 2\varepsilon_2$ with respect to $\mathcal{A}$.

Corollary: No-go RSP

"Useful" RSP resources are impossible.

Proof: classically simulate the honest server



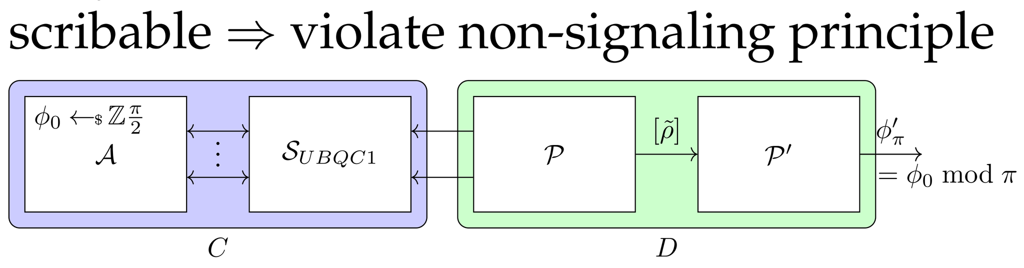
Result 2

Since our first result shows that the RSP resources classically-realizable of interest are impossible, it means that everytime we replace a quantum channel with a classical protocol, we **need to prove the security of the new combined protocol**. One important protocol is the UBQC protocol, but…

Theorem: No-go classical-client UBQC

If we replace the quantum channel of the UBQC protocol with a sub-protocol that uses only a classical channel, the combined protocol cannot be proven secure in the Constructive Cryptography framework.

Proof: UBQC ⇒ can be turned in RSP ⇒ describable ⇒ violate non-signaling principle



Result 3

We proved that classical-client UBQC cannot be shown secure in CC. Therefore, to prove the security of classical-client UBQC, we **need to target weaker models of security**:

Theorem: game-based QFactory + UBQC

The protocol consisting of UBQC with the quantum communication replaced by the QFactory protocol of [CCKW19] is secure in a game-based setting, i.e. the server cannot learn any information about the chosen circuit.

Proof: sequence of games reducing to the semantic security of the cryptographic primitive.

[CCKW19] A. Cojocaru, L. Colisson, E. Kashefi and P. Wallden. QFactory: Classically-instructed remote secret qubit preparation. *Asiacrypt 2019*.