**Stronger models**

- General composability
- Sequential composability
- Game-based 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:

- 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.

---

**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.

---

**Construction of 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 $S$ from a classical channel $C$, one needs to find a simulator $\sigma$ such that the following hold for a computationally bounded distinguisher:

\[
\begin{align*}
\Pr[A \rightarrow C \rightarrow B] & \approx \Pr[A \rightarrow S \rightarrow B] \\
\Pr[A \rightarrow C \rightarrow B] & \approx \Pr[A \rightarrow \sigma \rightarrow B]
\end{align*}
\]

---

**Formalization of RSP**

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

\[
\begin{align*}
\Pr[A \rightarrow S \rightarrow B | \rho] & \approx \Pr[A \rightarrow \mu | \rho]
\end{align*}
\]

such that on average $\rho$ is “close” to $\rho'$:

\[
\mathbb{E}_{\rho \sim \mathcal{D}_{\text{RSP}}} \Tr[\rho \rho'] \geq 1 - \varepsilon
\]

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

\[
\begin{align*}
\theta & \rightarrow |+\rangle \\
\theta & \rightarrow |+\rangle
\end{align*}
\]

---

**Result 1**

**Theorem: RSP is describable**

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

**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...

---

**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 $\text{QFactory} + \text{UBQC}$**

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.