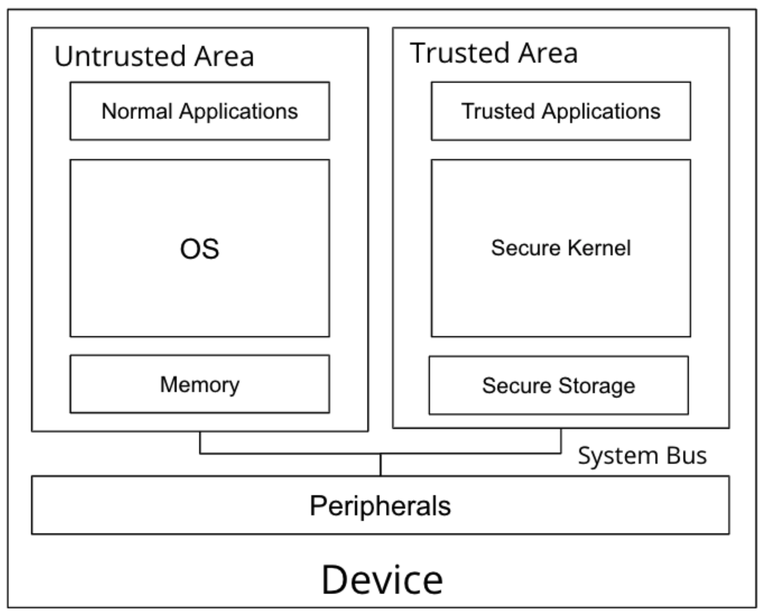
QEnclave - A composable treatment of quantum trusted execution environment

Yao Ma, Elham Kashefi, Myrto Arapinis, Kaushik Chakraborty, Marc Kaplan

Abstract

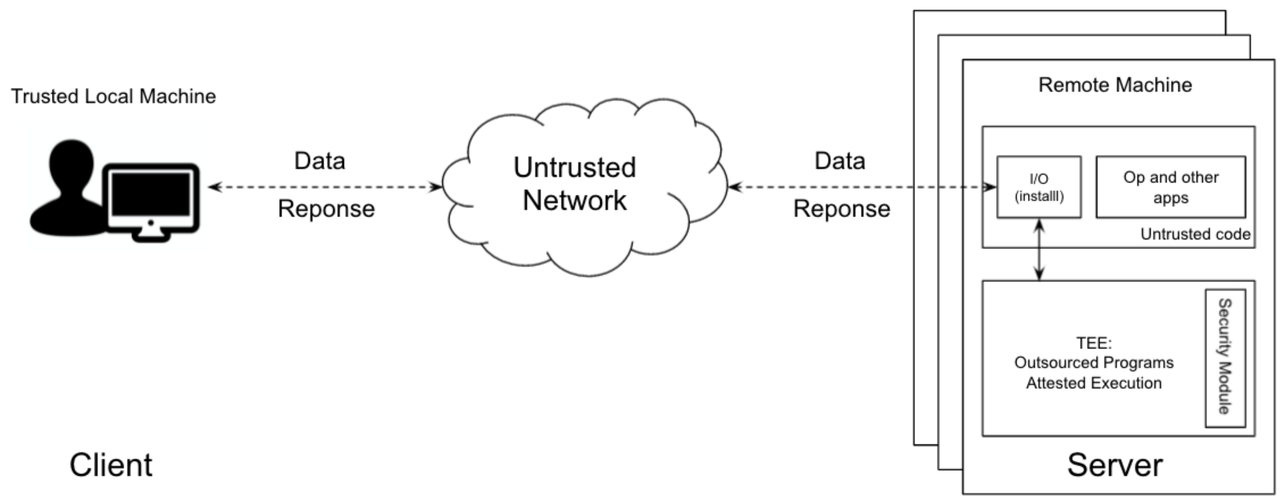
We introduce a secure hardware device prototype named a QEnclave that can secure the remote execution of quantum operations while only using classical controls. This device extends to quantum computing the classical concept of a secure enclave which isolates a computation from its environment to provide privacy and tamper-resistance. Remarkably, our QEnclave only performs single-qubit rotations, but can nevertheless be used to secure an arbitrary quantum computation even if the qubit source is controlled by an adversary. More precisely, attaching a QEnclave to a quantum computer, a remote client controlling the QEnclave can securely delegate its computation to the server solely using classical communication.

Trusted Execution Environment (TEE)



A TEE is a tamper-resistant processing environment that runs on a kernel separated from its environment, named the rich execution environment (REE). It guarantees the authenticity of the executed code, the integrity of the run-time states, and the confidentiality of its code and data.

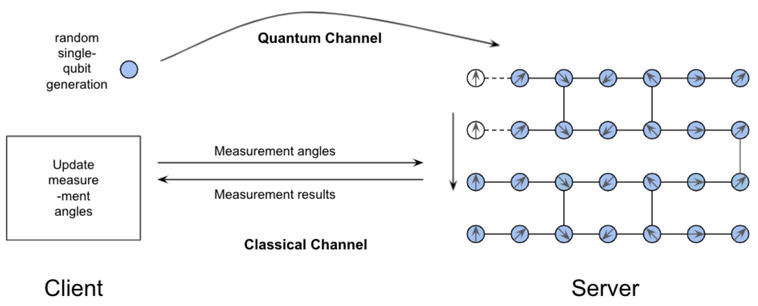
Application: TEE-enabled Secure Outsourcing Computation



For remote machine with TEE-enabled secure processor, the client firstly executes a key-exchange within an attested execution of secure processor; While the key exchange finished, the key is used to establish a secure channel in between the client and secure processor; After the outsourced program is executed inside secure processor, the output is encrypted within secure processor and sent to the client, while the responses are passed through the intermediary server. So the security of the overall design is reduced to the security of key exchange and authenticated encryption.

Delegated Quantum Computation (DQC)

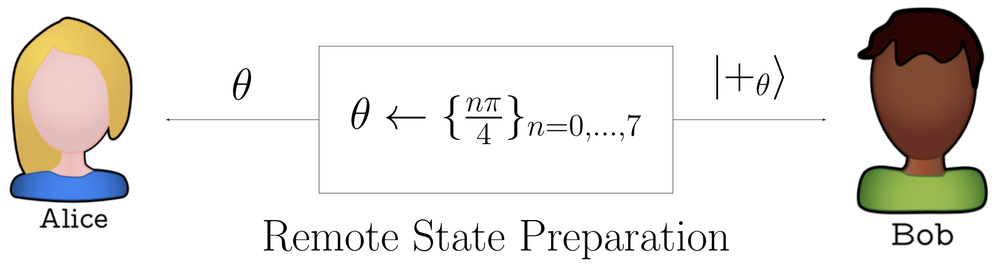
A client with limited computational power asks a server to run a quantum computation, whose result is then returned to the client. A type of protocols of DQC is *prepare-and-send* protocols, including **Universal Blind Quantum Computation**, Verifiable Quantum Computation, etc.



However, a quantum communication channel is necessary in between the client and the server, which is impractical and scales badly with the number of clients.

Classical Client DQC: Remote State Preparation (RSP)

The construction of **remote state preparation** functionality enables a process of quantum state preparation on the server side, and client gets the classical description of prepared states.

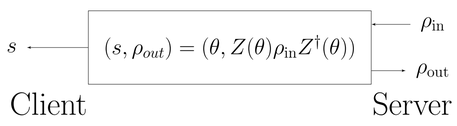


Remote State Preparation

The security of prepare-and-send protocols comes from the fact that the classical description of prepared quantum state is only known to the client and the qubits obtained by the server are always in maximally mixed states, in which case the server knows nothing about the computation except the universal graph. It is a very strong notion that it requires additional computational assumptions or hardware assumptions.

Resource and Security Model

We define a resource named Remote State Rotation for blindness (RSR_B). It receives a single-qubit state ρ_{in} from the server and performs a rotation $Z(\theta)$ with θ chosen uniformly at random from the set $\mathbb{Z}_{\frac{\pi}{4}}$. It then outputs ($\rho_{out}$) at the server's side and the angle θ at the client's side.



We use *Constructive Cryptography* framework as security model which provides the composable security by constructing a desired resource ($\mathcal{S}$) from an assumed resource ($\mathcal{R}$) with protocol π. π securely realizes $\mathcal{S}$ from $\mathcal{R}$ if correctness and security holds with a simulator σ and a computationally bounded distinguisher $\mathcal{D}$:

$\pi_A \mathcal{R} \pi_B \approx_\varepsilon \mathcal{S} \perp$ (Correctness); $\pi_A \mathcal{R} \approx_\varepsilon \mathcal{S}\sigma$ (Security)

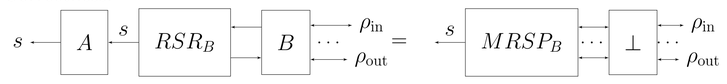
Result 1

Our first result reduces the ideal RSP resource to a RSR_B resource with same output and proves the composable security. It requires no quantum source inside RSP but an external quantum source from the server.

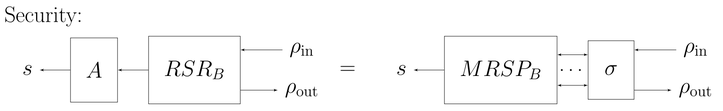
Theorem (Composable security of RSR)**.** *The UBQC protocol with the client accessing to the RSR_B constructs the ideal resource of DQC with perfect blindness.*

Proof. We exploit an intermediary resource called *measured-based RSP* ($MRSP_B$) which has been proven composable security and proves the indistinguishability of these resources with protocol (A, B).

Correctness:



Security:



Result 2

Our second result proposes a minimal construction of quantum-capable TEE so-called QEnclave using a standard classical TEE, together with a post-quantum protection of the flow between TEE and the quantum apparatus which implements the single-qubit rotations. The composable security achieves while the client also equips a TEE or minimally with a global augmented common reference string (ACRS) implemented by trusted hardware manufacturer.