Composable security of delegated quantum computation

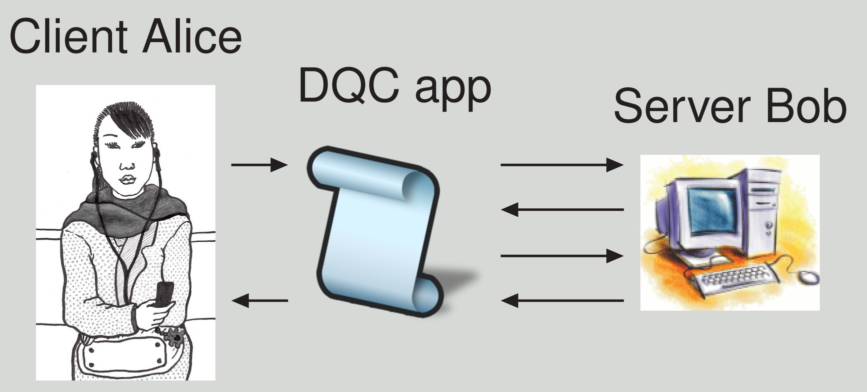
Christopher Portmann*[1] Vedran Dunjko†[2]
Joseph F. Fitzsimons‡[3] Renato Renner§[1]

[1]Institute for Theoretical Physics, ETH Zurich, Switzerland.
[2]School of Informatics, The University of Edinburgh, U.K.
[3]Centre for Quantum Technologies, National University of Singapore, Singapore.

Delegated Quantum Computation (DQC)

DQC: asking a server to perform some (heavy) quantum computation.

Security concerns:
- the server, Bob, learns nothing about the computation: blindness.
- the client, Alice, can verify that the correct computation was performed: verifiability.



What are the factors of 1983745987234?

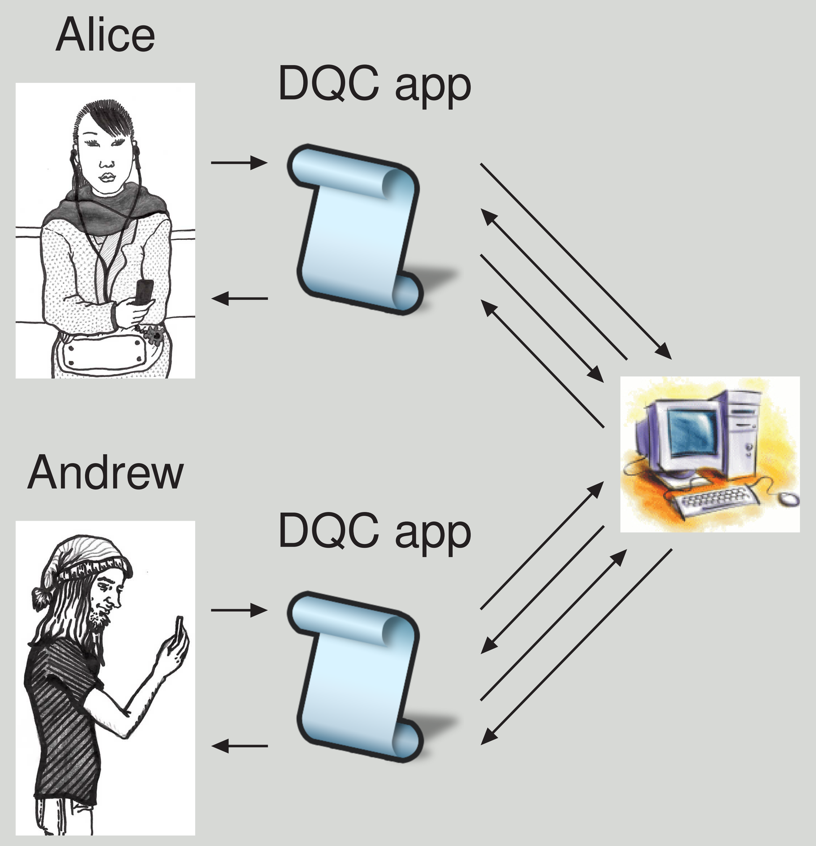
Composability

Stand-alone security: secure for one run in an isolated environment.

Composable security: secure in an arbitrary environment,
- input and output can be used in other protocols,
- instances can be run in parallel.

Cryptography is inherently modular:
- protocols are used as subroutines in other protocols,
- players can interact with many parties, run various protocols simultaneously.

Not composable
= cryptographically insecure



Is this also secure?

Toy example

Problem: find a witness for a positive instance of an NP problem.
Protocol: Bob sends Alice a random witness.
Blindness: no information was sent from Alice to Bob, so he obviously learnt nothing of the input.
Verifiability: Alice can easily check if the witness is correct, she never accepts a wrong solution.
Not secure: if Bob learns whether Alice accepted the solution, he learns something about the problem; e.g.,
- Alice sends a letter of complaint,
- Alice renews the membership for another month of service.

These intuitive notions of security are insufficient.

Results

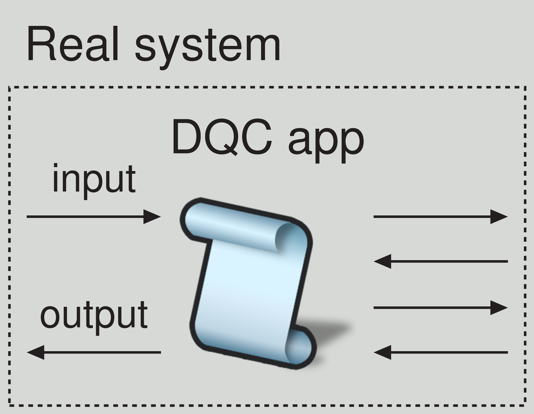
- Composable security definitions for
  - blindness,
  - blindness+verifiability.
- Proof of composable blindness for DQC protocol of
  - Broadbent, Fitzsimons, Kashefi [STOC 2009],
  - Morimae, Fujii [eprint 2012].
- Reduction of blindness+verifiability to a set of stand-alone definitions.
  - Proves the security of Fitzsimons, Kashefi [eprint 2012],

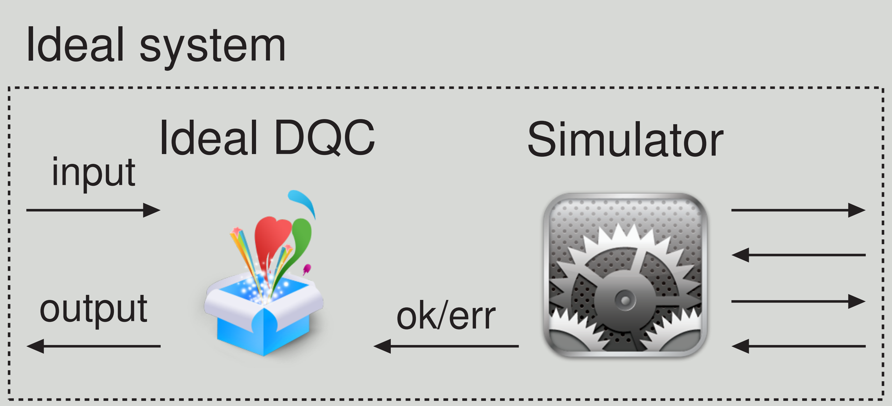
Blindness+verifiability

Composable security: is the real protocol distinguishable from an ideal DQC resource?

Ideal blind and verifiable DQC:
- Alice gives it her input.
- Bob decides whether to compute the correct outcome, inputs `ok/err`.
- Ideal resource performs the correct computation or returns an error depending on Bob's decision.

Distinguishability:
- Can anything that is possible in the real world be achieved in the ideal world?
- Can Bob / a simulator generate the transcript and bit `ok/err` on its own without knowledge of the input?
- If given a box running the real protocol or the ideal one and simulator, what is the distinguishing advantage?





Reduction of blindness+verifiability to stand-alone notions

Composable security

$$\iff \mathcal{P}_{AB} \approx \mathcal{U} \otimes \mathcal{F}^{\text{ok}} + \mathcal{E}^{\text{err}} \otimes \mathcal{F}^{\text{err}}.$$

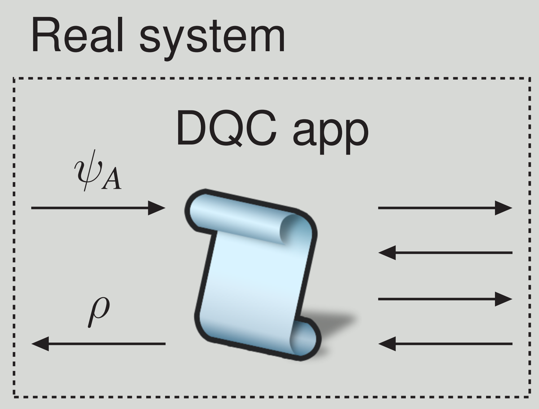
$\mathcal{P}_{AB}$ protocol with honest Alice and dishonest Bob.
$\mathcal{U}$ transformation implemented by the protocol.
$\mathcal{E}^{\text{err}}$ map that outputs an error flag.
$\mathcal{F}^{\text{ok}}_{\text{err}}$ some local (subnormalized) maps on Bob's system.

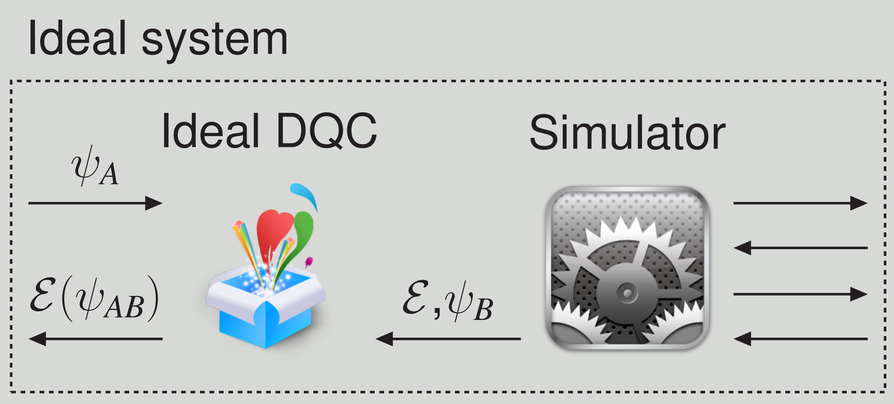
Independent verifiability: test of correctness is independent from the input.
- Stand-alone blindness and independent verifiability $\implies \mathcal{P}_{AB} \approx \mathcal{U} \otimes \mathcal{F}^{\text{ok}} + \mathcal{E}^{\text{err}} \otimes \mathcal{F}^{\text{err}}$.
- If the input $\psi_{AB} = \psi_A \otimes \psi_B$, the error parameter is similar in the stand-alone and composable cases.
- If the input is entangled, the error increases by a factor $(\dim \mathcal{H}_A)^2$.

Blindness

Ideal blind DQC:
- Does not leak the input ψ_A to Bob, but does not guarantee that Alice gets the correct outcome.
- Allows Bob to input a map $\mathcal{E}$ and state ψ_B, that control the output.
- Returns $\mathcal{E}(\psi_{AB})$ to Alice.

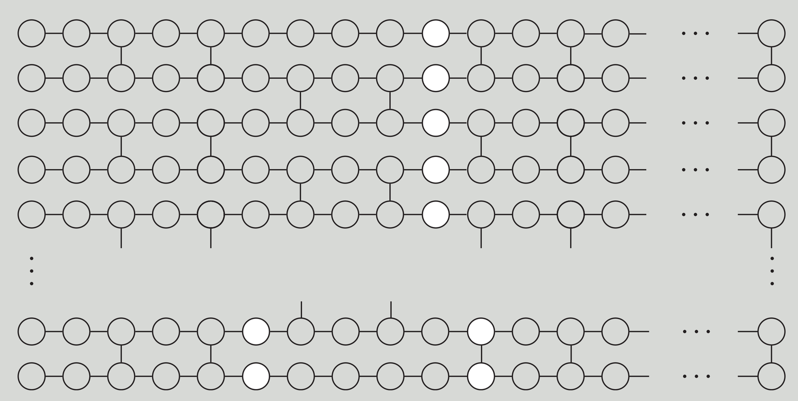
Distinguishability:
- The task of the simulator is to find $\mathcal{E}$ and ψ_B (without any knowledge of ψ_A), such that the output in the real and ideal settings are indistinguishable.





Blind DQC of Broadbent, Fitzsimons and Kashefi

Protocol (simplified):
- Alice sends Bob a one-time padded input $X^x Z^z \psi Z^z X^x$.
- Alice picks random angles θ_j, and sends Bob qubits $|+_{\theta_j}\rangle = (|0\rangle + e^{i\theta_j}|1\rangle)/\sqrt{2}$.
- Bob entangles them according to a predefined brickwork pattern.
- Alice sends one-time padded measurement angles $\phi_j + \theta_j$.
- Bob carries out the measurements, returns the last column to Alice.



Pattern of a brickwork state

Proof (sketch):
- The simulator runs the protocol with EPR halves and random strings.
- It sends the other EPR halves and transcript to the ideal blind DQC.
- Ideal blind DQC teleports the correct values using the EPR halves.
- Example: $X^x Z^z \psi_3 Z^z X^x \equiv$ Bell $\text{proj}_{12}(\psi_1 \otimes \text{EPR}_{23})$.

Abstract cryptography [Maurer, Renner]

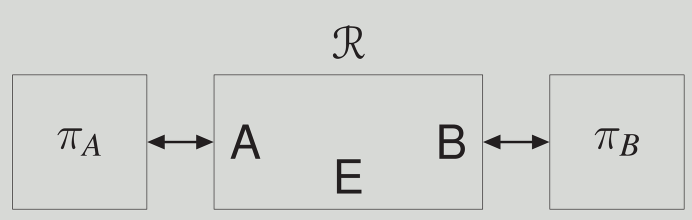
- Models composability in an abstract way, independently from the underlying computational model.
  - Applies immediately to both classical and quantum crypto!
- Simplifies and generalizes previous frameworks, e.g., Universal Composability (UC) [Canetti].
- Strictly more powerful than previous frameworks
  - Can directly model mutually distrustful dishonest players (e.g., coercibility).
  - Can directly model non-communicating adversarial devices (e.g., device independent crypto).

AC security

Resources:
- Protocols π modelled as mapping some (weak) resource $\mathcal{R}$ into another (stronger) resource $\mathcal{S}$.

$$\mathcal{R} \xrightarrow{\pi,\varepsilon} \mathcal{S}.$$

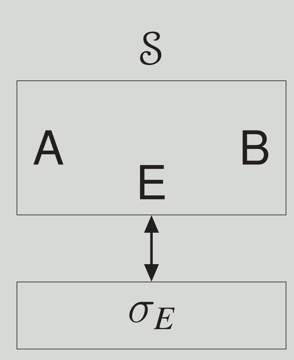
- A resource can be modeled by a box with an interface for each player.
  - Guaranteed functionalities for parties following the protocol.
  - Other functionalities for parties not following the protocol.



Security:
- $\mathcal{R} \xrightarrow{\pi,\varepsilon} \mathcal{S}$, if there exist simulators $\sigma = \{\sigma_i\}_{i \in \mathcal{I}}$ such that,

$$\forall \mathcal{P} \subseteq \mathcal{I}, \quad d(\pi_{\mathcal{P}} \phi_{\mathcal{P}} \mathcal{R}, \sigma_{\mathcal{I} \setminus \mathcal{P}} \psi_{\mathcal{P}} \mathcal{S}) \leq \varepsilon.$$

$\mathcal{I}$ Interface set, e.g., $\mathcal{I} = \{$A,B,E$\}$.
ϕ, ψ filters on dishonest functionalities.
$\mathcal{R}, \mathcal{S}$ resources.
π, σ converters (protocol and simulator).



*chportma@phys.ethz.ch †vdunjko@inf.ed.ac.uk ‡joe.fitzsimons@nus.edu.sg §renner@phys.ethz.ch