# On the possibility of classical client blind quantum computing

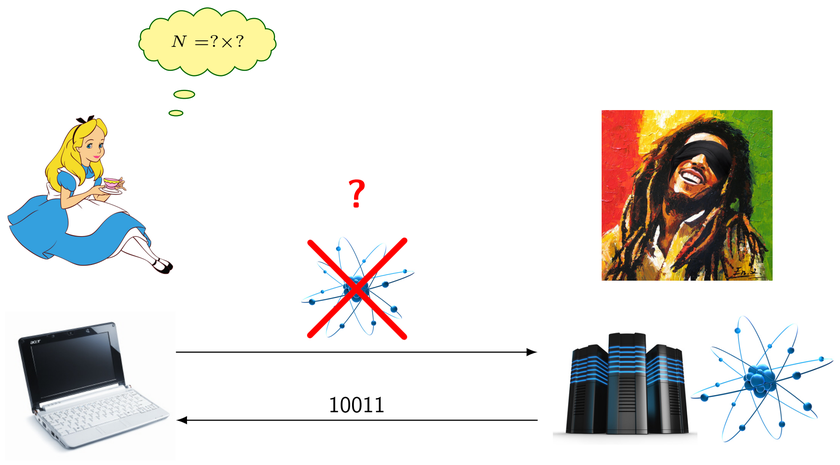
QFactory

Alexandru Cojocaru, Léo Colisson, Elham Kashefi and Petros Wallden

The University of Edinburgh

Sorbonne Université

## Problem



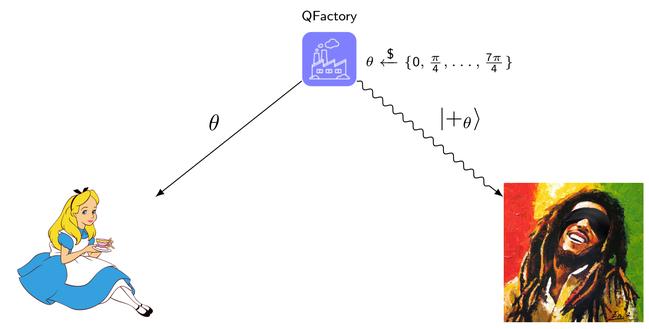

Alice has a classical computer, and Bob has a full quantum computer. Alice would like to **perform a quantum computation on Bob's side**, but she also wants to **hide everything to Bob**:

- the input of the computation
- the output of the computation
- the computation

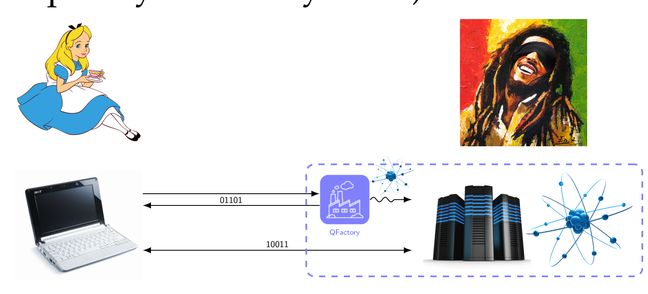
It is **known to be possible if she can prepare and send some qubits** $|+_\theta\rangle$ with $\theta \in \{0, \pi/4, \ldots, 7\pi/4\}$ using a protocol named Universal Blind Quantum Computing (UBQC).

## Ideal functionality

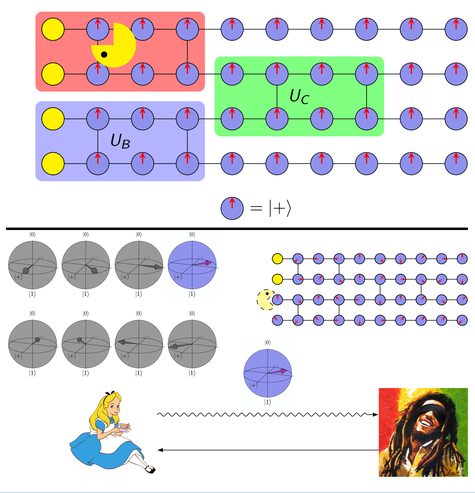
Our solution, named QFactory, **simulates the quantum channel** needed in UBQC with an equivalent channel that is **completely classical**. Here is the ideal functionality we want to achieve:




Once we have this ideal functionality, we can **combine it with UBQC** (or actually with any protocol that would need to send pure states completely known by Alice):



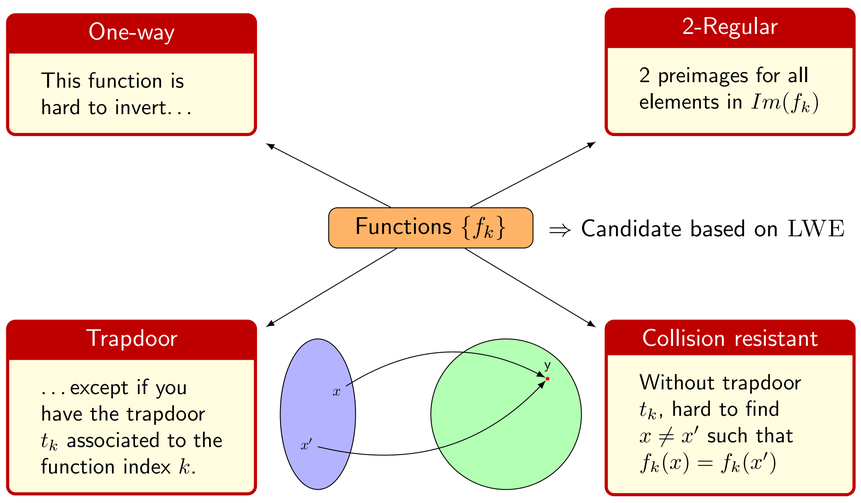

## UBQC in a nutshell




All quantum circuits can be **translated into another circuit** (see top picture) where each gate is replaced by eight entangled (with Ctrl-Z) qubits in the $|+\rangle$ state, and each qubit has an associated measurement angle. **The computation is done by measuring** these qubits with the corresponding angles (up to some small corrections). **To hide** the computation (see bottom picture), **Alice needs to send to Bob some rotated input qubits**, and correct the angles accordingly. This is the only quantum communication needed, and our protocol **QFactory will be used to replace this communication**.

## Cryptographic assumptions

In order to counterbalance the power of the quantum server Bob, Alice will need the **help of cryptography**, and more specifically a familly of functions having the following properties:




## Protocol

$$|0\rangle^{\otimes n}|0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle|0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle|f_k(x)\rangle = \sum_y (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (\bigotimes_i |b_i\rangle) \otimes |+_\theta\rangle \otimes |y\rangle$$

$t_k, k$

$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \ldots \frac{7\pi}{4}\})_{i=1}^{n-1}$

$k, (\alpha_i)$ →

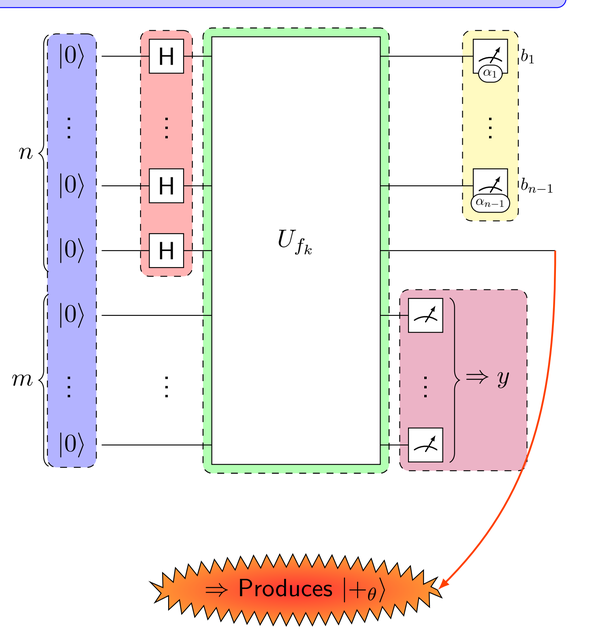
Computes circuit

← $y, (b_i)$

$(x, x') := \texttt{Inv}(t_k, y)$

$\theta := (-1)^{x_n} \sum_{i=1}^{n-1} (x_i - x'_i)(b_i \pi + \alpha_i)$

⇒ Gets $\theta$

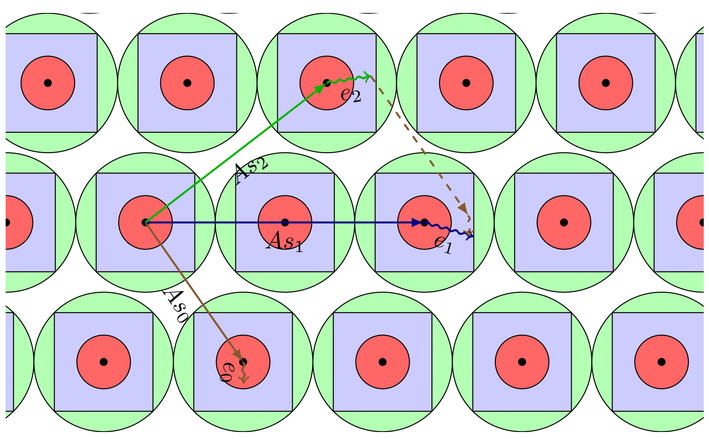



⇒ Produces $|+_\theta\rangle$

## Function construction

Our candidate function is based on the cryptosystem [Micciancio, Peikert 2011] and is proven **secure under the standard LWE$_\gamma$ assumption**, with $\gamma = \text{poly}(n)$.

$$f_{A,y_0}((s,e),c) = Ax + e + c \times y_0$$




## Security

For now, this protocol is proven secure against an **honest-but-curious adversary**, and we showed that $\theta$ was an hardcore function. The proof is mainly based on the **Goldreich-Levin theorem**:

**Theorem** (Goldreich-Levin theorem)**.** *If $f$ is a one-way function, then the predicate $hc(x,r) = \sum x_i r_i \mod 2$ cannot be distinguished from a random bit, given $r$ and $f(x)$.*

Moreover, we have nearly finished the proof of a variant of QFactory in the **fully malicious setting**

## Applications

This protocol could be used to **replace quantum client by classical clients** in lots of protocols. Moreover, by combining QFactory and Zero-Knowledge proofs, we conjecture that **some quantum protocols could be greatly improved** in efficiency/security (MPC, OTP...).