QCrypt 2018:
On the possibility of classical client blind quantum computing

Alexandru Cojocaru, Léo Colisson,
Elham Kashefi, Petros Wallden

August 30, 2018

Robin Hood

Main Goal

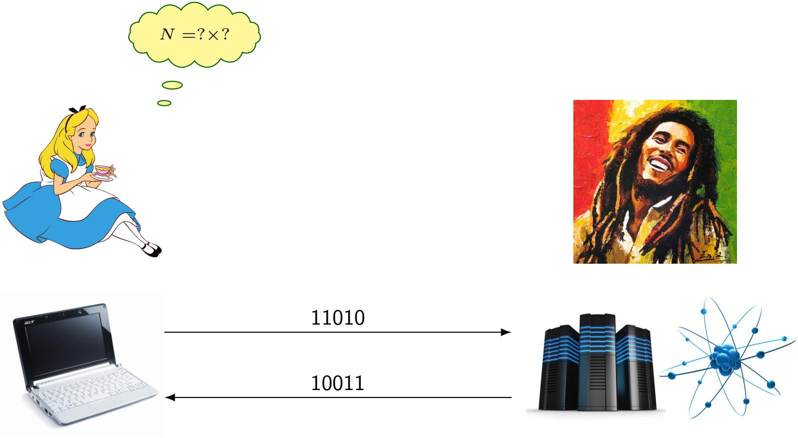


Figure: (Blind) Quantum Computing

Main Goal

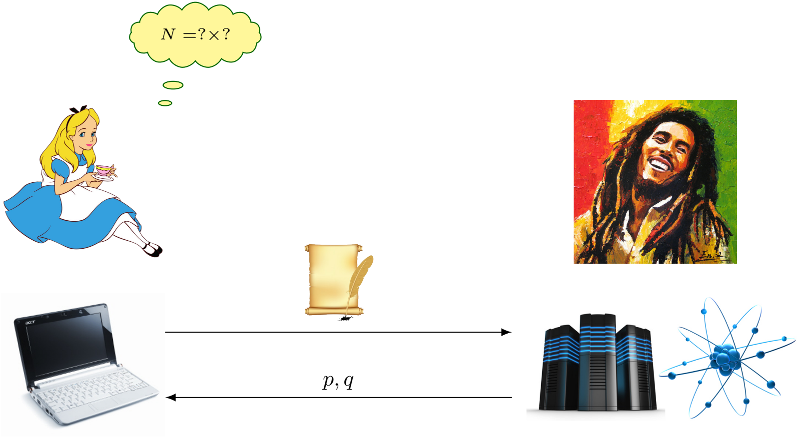


Figure: (Blind) Quantum Computing

Main Goal

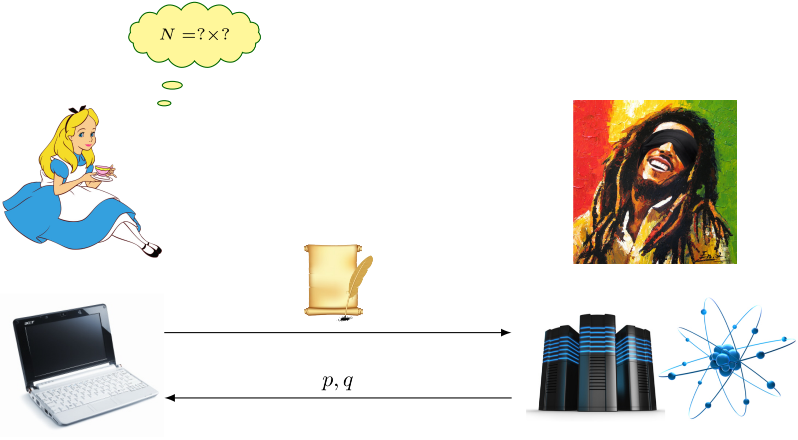


Figure: (Blind) Quantum Computing

Main Goal

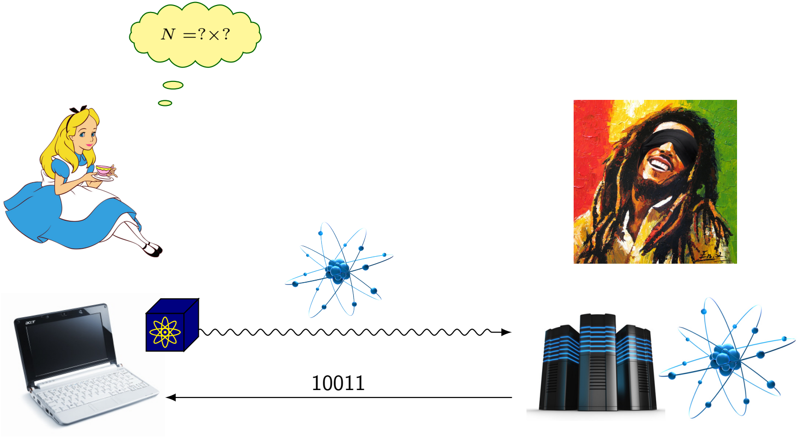


Figure: (Blind) Quantum Computing

Main Goal

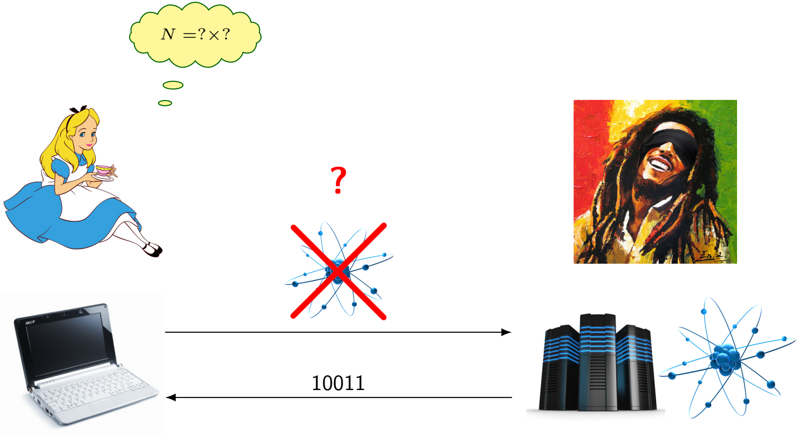


Figure: (Blind) Quantum Computing

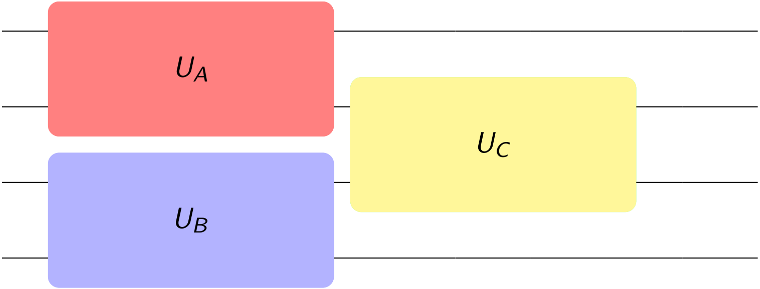
Our solution

Universal Blind Quantum Computing (UBQC)
[A. Broadbent, J. Fitzsimons, E. Kashefi]

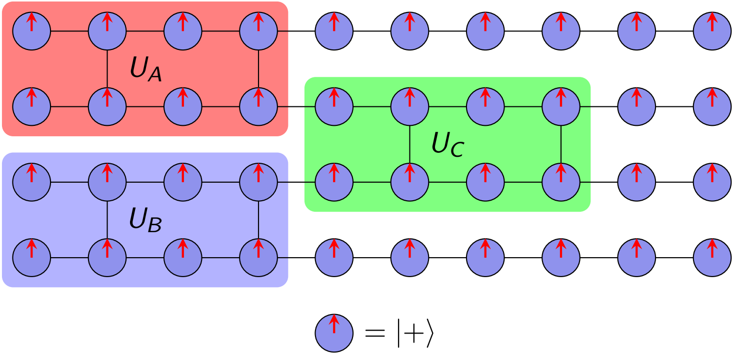
$+$

QFactory

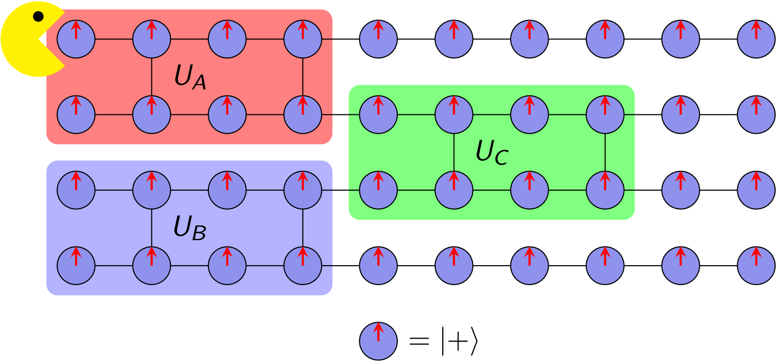
UBQC in a nutshell



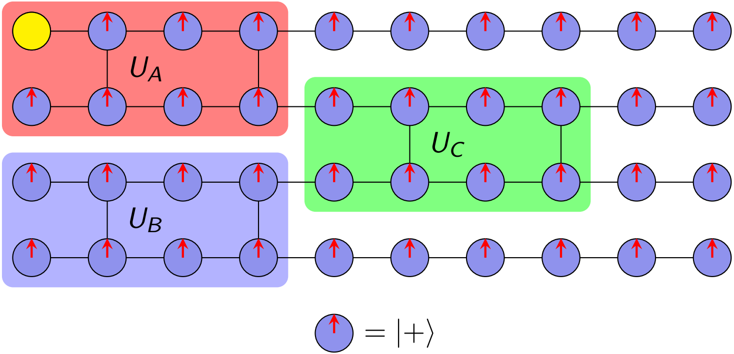
UBQC in a nutshell



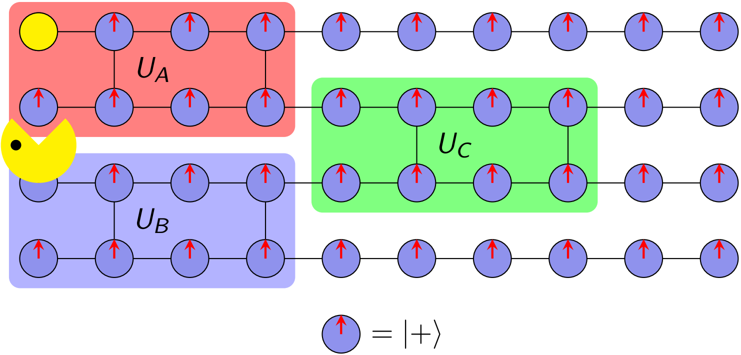
UBQC in a nutshell



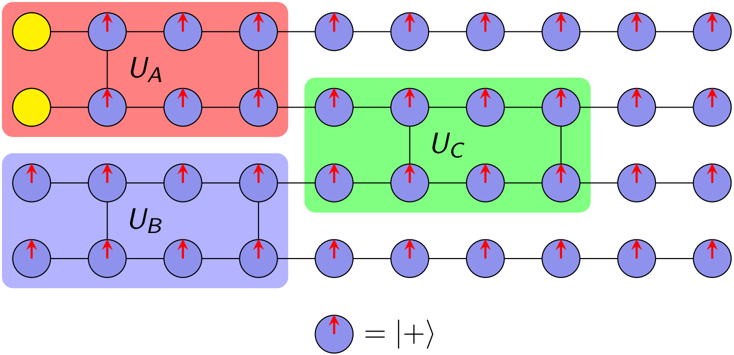
UBQC in a nutshell



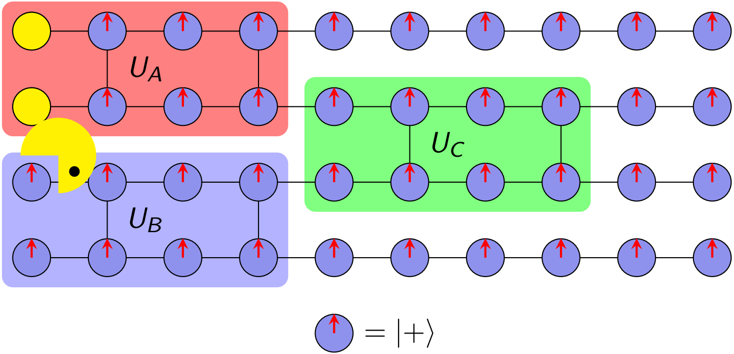
UBQC in a nutshell



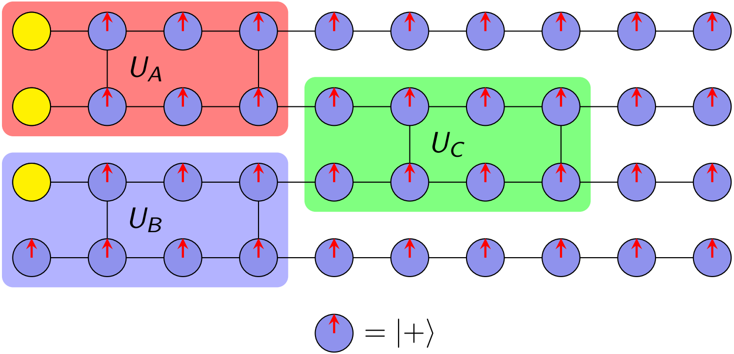
UBQC in a nutshell



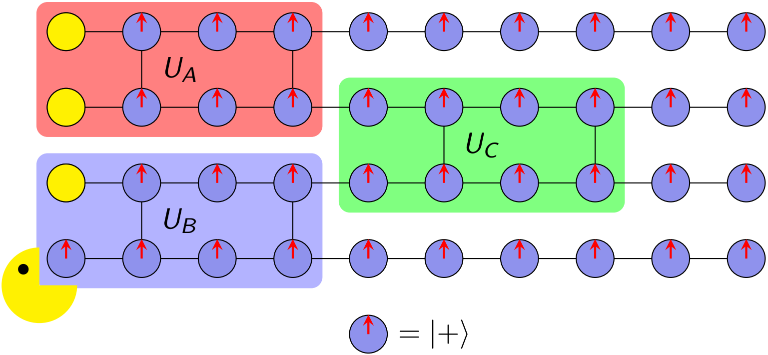
UBQC in a nutshell



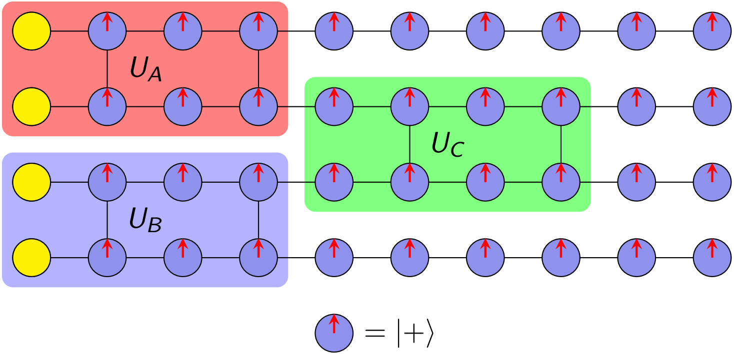
UBQC in a nutshell



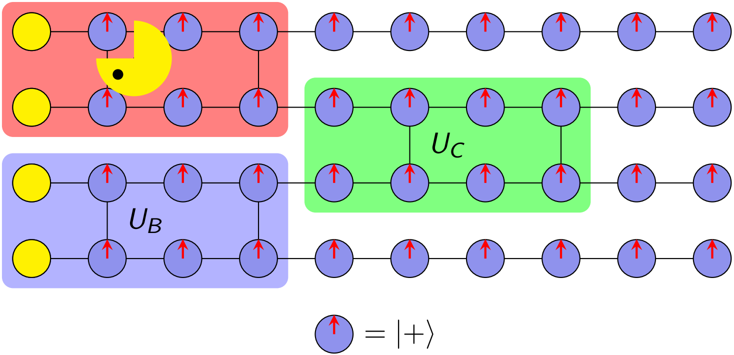
UBQC in a nutshell



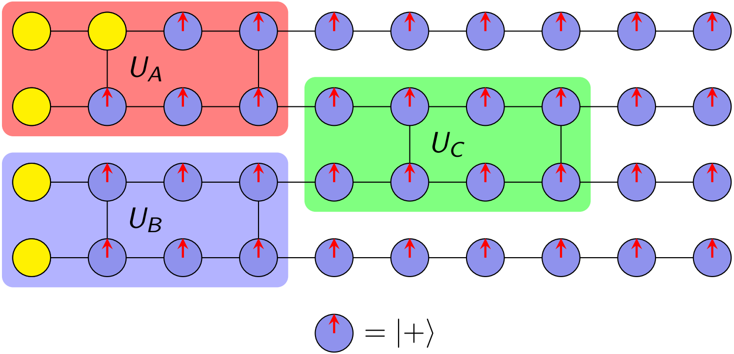
UBQC in a nutshell



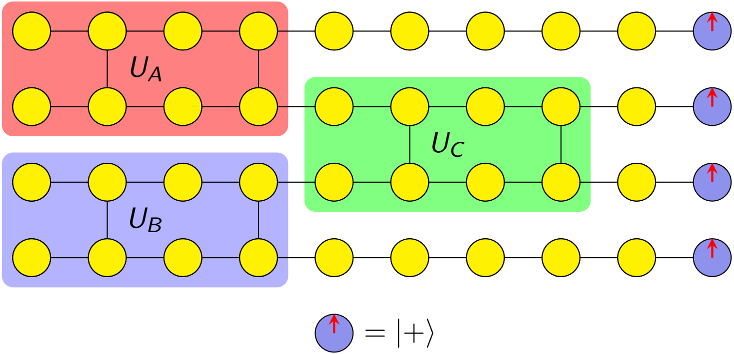
UBQC in a nutshell



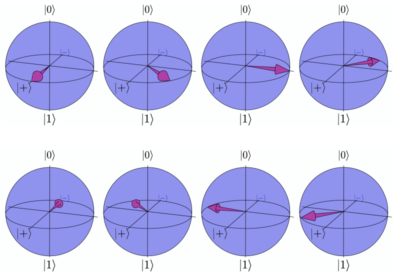
UBQC in a nutshell

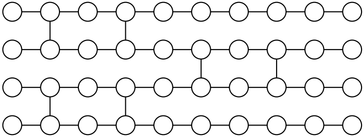


UBQC in a nutshell

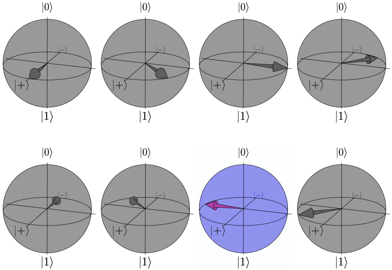


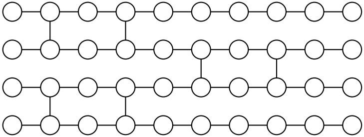
UBQC in a nutshell



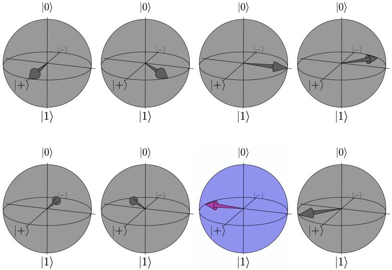


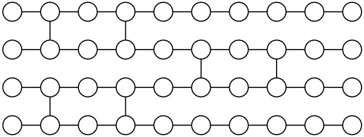
UBQC in a nutshell

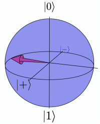




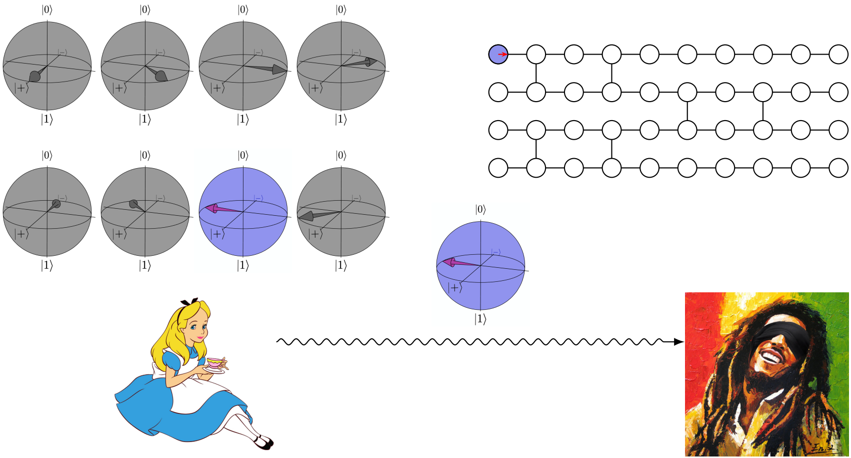
UBQC in a nutshell



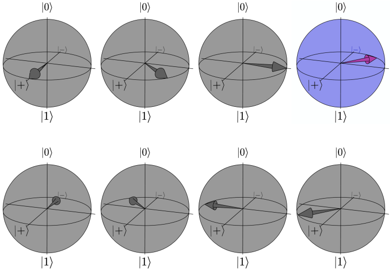


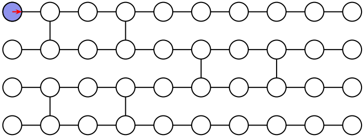


UBQC in a nutshell

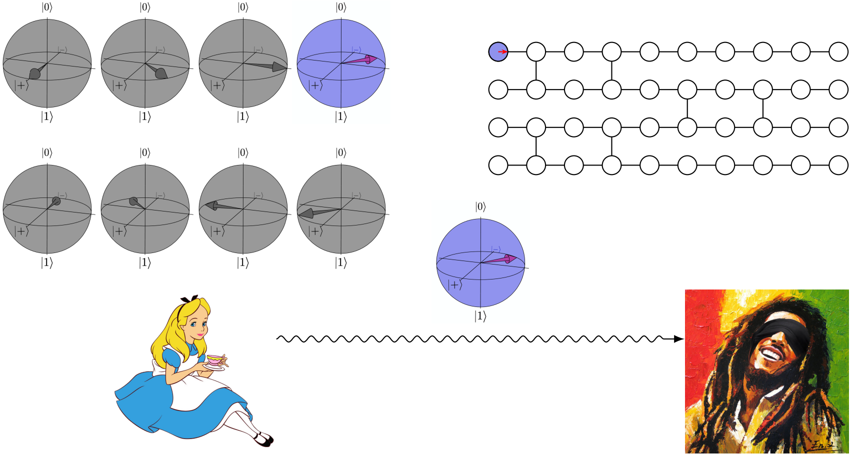


UBQC in a nutshell

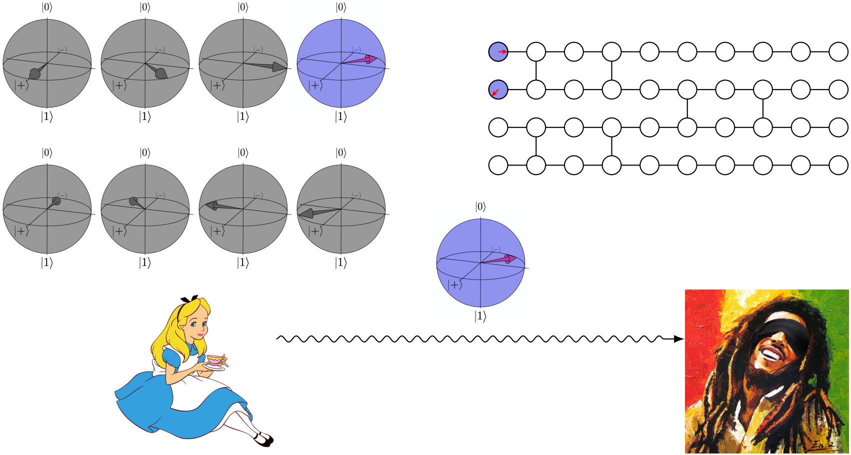




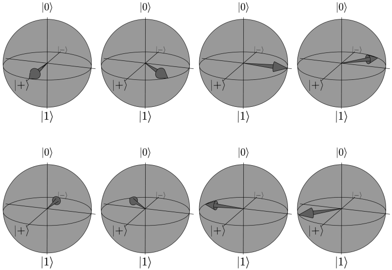
UBQC in a nutshell

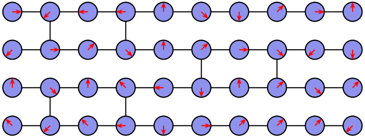


UBQC in a nutshell

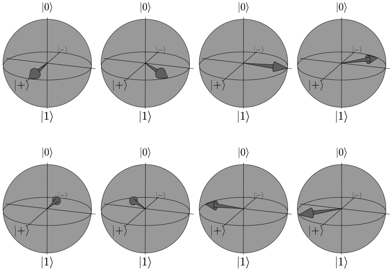


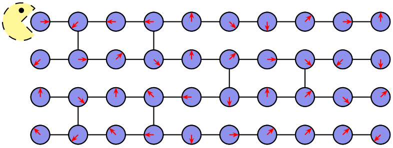
UBQC in a nutshell



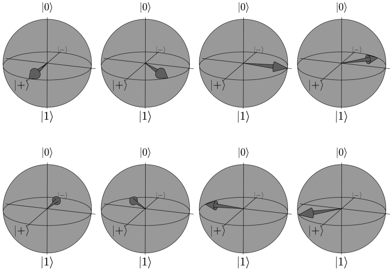


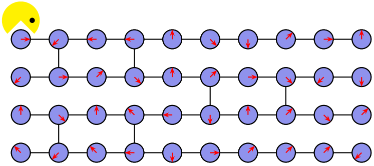
UBQC in a nutshell



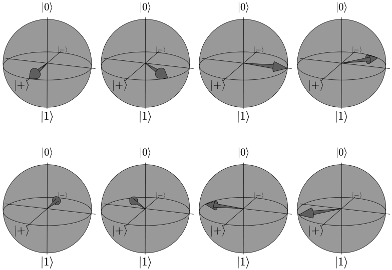


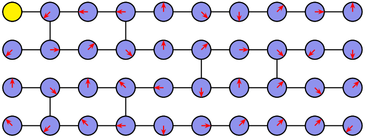
UBQC in a nutshell



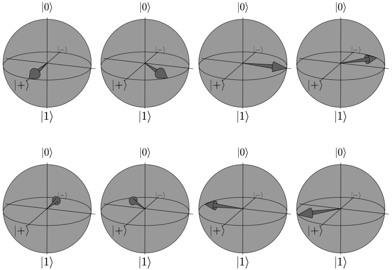


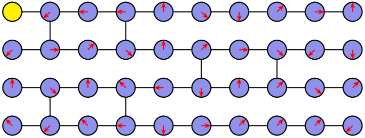
UBQC in a nutshell



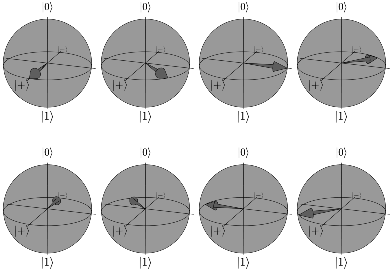


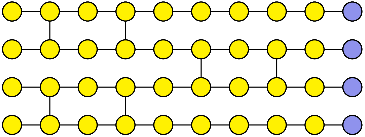
UBQC in a nutshell



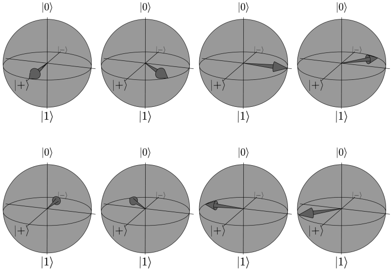


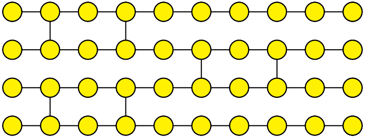
UBQC in a nutshell





UBQC in a nutshell





QFactory: description

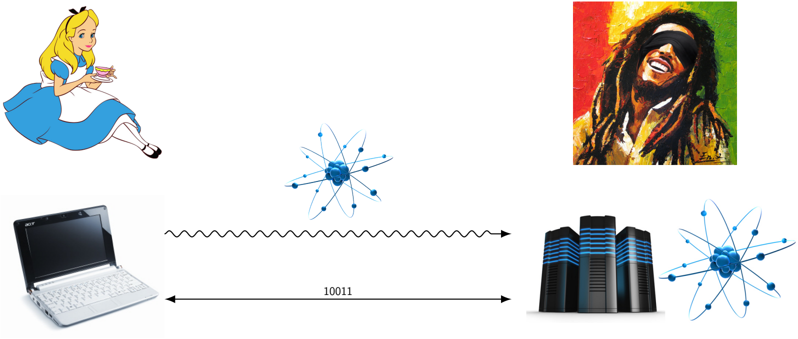


Figure: QFactory gadget: simulate quantum channel

QFactory: description

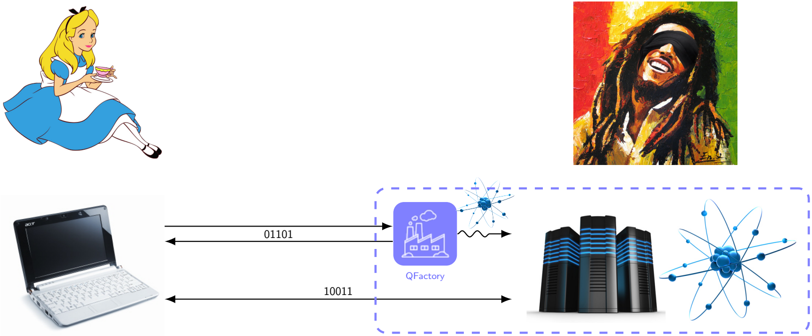


Figure: QFactory gadget: simulate quantum channel

QFactory: description

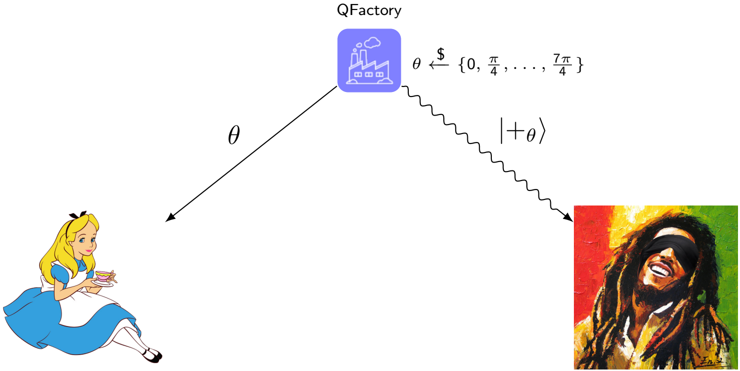


Figure: QFactory: ideal functionality

Cryptographic assumptions

Functions $\{f_k\}$

One-way

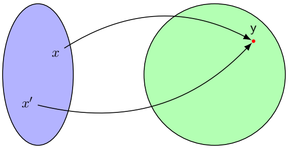
This function is hard to invert. . .

2-Regular

2 preimages for all elements in $Im(f_k)$

Trapdoor

. . . except if you have the trapdoor t_k associated to the function index k.



Collision resistant

Without trapdoor t_k, hard to find $x \neq x'$ such that $f_k(x) = f_k(x')$

Cryptographic assumptions

One-way

This function is hard to invert...

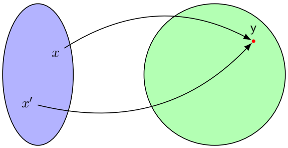
2-Regular

2 preimages for all elements in $Im(f_k)$

Functions $\{f_k\}$ $\Rightarrow$ Candidate based on [MP11]

Trapdoor

...except if you have the trapdoor t_k associated to the function index k.



Collision resistant

Without trapdoor t_k, hard to find $x \neq x'$ such that $f_k(x) = f_k(x')$

Construction

Construction

t_k, k

Construction

t_k, k

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

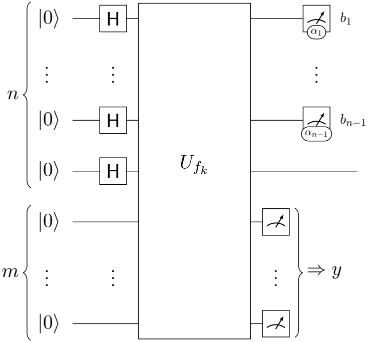
Construction

t_k, k

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

$k, (\alpha_i)$ →

Construction



t_k, k

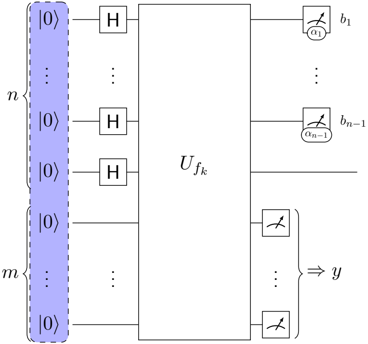
$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\})_{i=1}^{n-1}$

$k, (\alpha_i)$ →

Compute circuit

Construction

$|0\rangle^{\otimes n}|0\rangle^{\otimes m}$



t_k, k

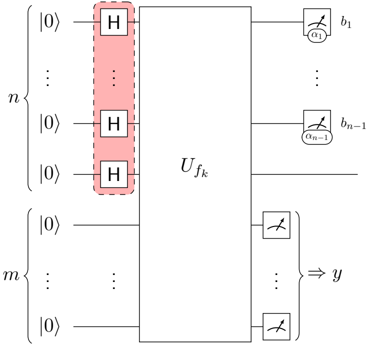
$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\})_{i=1}^{n-1}$

$k, (\alpha_i)$ →

Compute circuit

Construction

$|0\rangle^{\otimes n}|0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle|0\rangle^{\otimes m}$



t_k, k

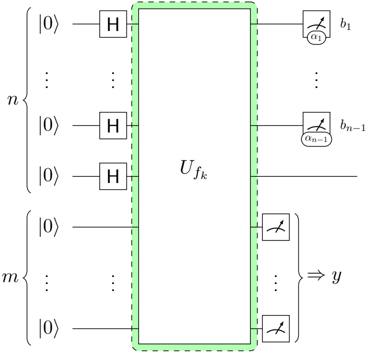
$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\})_{i=1}^{n-1}$

$k, (\alpha_i)$ →

Compute circuit

Construction

$|0\rangle^{\otimes n}|0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle|0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle|f_k(x)\rangle$



t_k, k

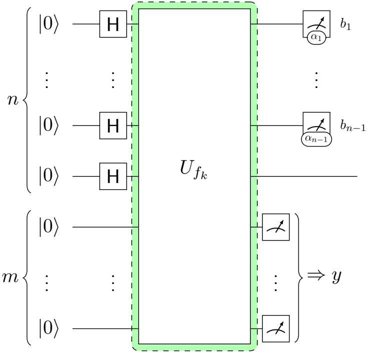
$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\})_{i=1}^{n-1}$

$k, (\alpha_i)$ →

Compute circuit

Construction

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



t_k, k

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

$k, (\alpha_i)$ $\longrightarrow$

Compute circuit

Construction

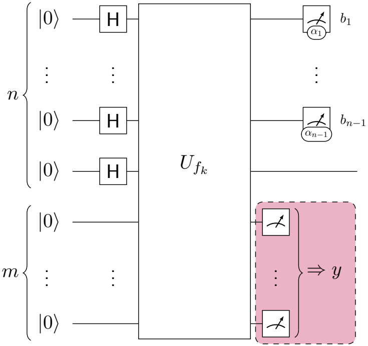
$|0\rangle^{\otimes n}|0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle|0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle|f_k(x)\rangle = \sum_y (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (|x\rangle + |x'\rangle) \otimes |y\rangle$

t_k, k

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

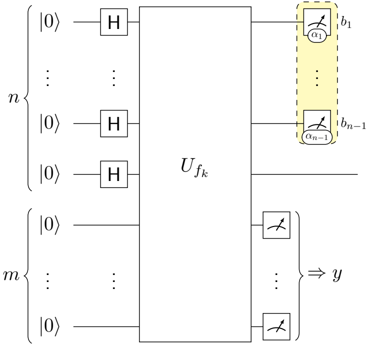
$k, (\alpha_i)$ →

Compute circuit



Construction

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



t_k, k

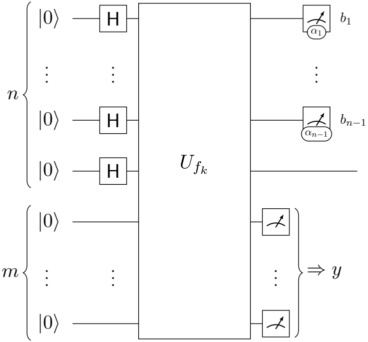
$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\})_{i=1}^{n-1}$

$k, (\alpha_i)$ →

Compute circuit

Construction

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



t_k, k

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

$k, (\alpha_i)$ →

Compute circuit

$\Rightarrow$ Produces $|+_\theta\rangle$

Construction

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

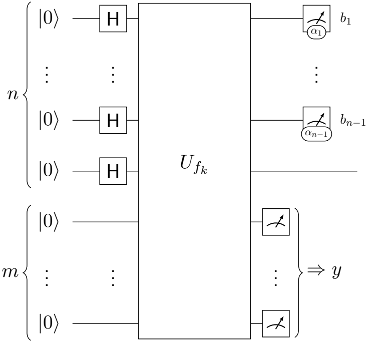
t_k, k

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

$k, (\alpha_i)$ →

Compute circuit

← $y, (b_i)$



$\Rightarrow$ Produces $|+_\theta\rangle$

Construction

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

t_k, k

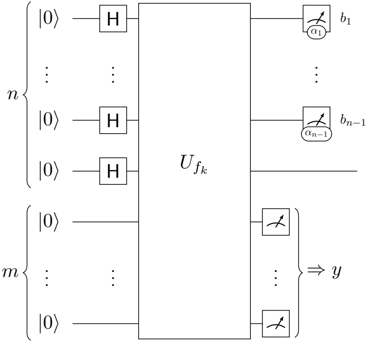
$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\})_{i=1}^{n-1}$

$k, (\alpha_i)$ →

Compute circuit

← $y, (b_i)$

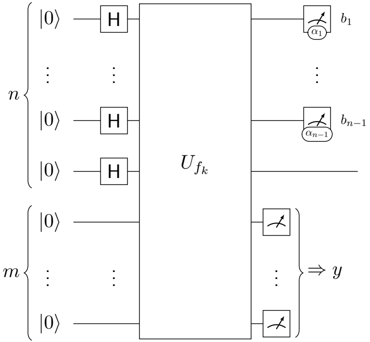
$(x, x') := \texttt{Inv}(t_k, y)$



$\Rightarrow$ Produces $|+_\theta\rangle$

Construction

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



t_k, k

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

$k, (\alpha_i)$ →

Compute circuit

← $y, (b_i)$

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

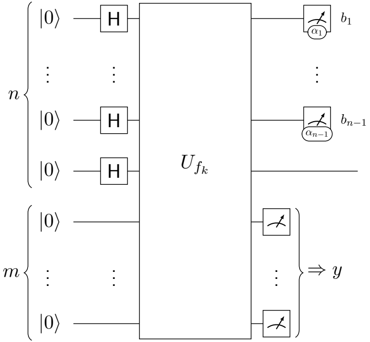
$\theta := (-1)^{x_n} \sum_{i=1}^{n-1}(x_i - x'_i)(b_i\pi + \alpha_i)$

$\Rightarrow$ Produces $|+_\theta\rangle$

Construction

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

t_k, k



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

$k, (\alpha_i)$ →

Compute circuit

← $y, (b_i)$

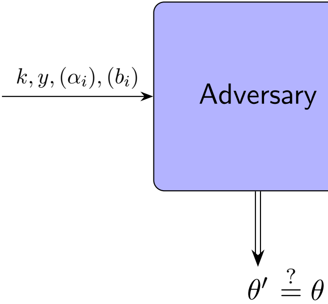
$(x, x') := \texttt{Inv}(t_k, y)$

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

$\Rightarrow$ Gets θ

$\Rightarrow$ Produces $|+_\theta\rangle$

Hardcore function and Honest-but-curious model



Cannot be better than random guess: θ **hard-core** function.

Security

Blindness of the output θ.
Corollary: QFactory is secure in the honest-but-curious model.
If adversary:

- follows the protocol
- can only access classical registers

$\Rightarrow$ he cannot determine θ

Intuition of proof

θ is a hardcore function: proof based on Goldreich-Levin Theorem:

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 $f(x)$.

Recall, in our case: $f(x) \approx y$ and

$$\theta \approx \sum \underbrace{(x_i - x_i')}_{\text{Unknown to server}} \underbrace{(4b_i + \alpha_i)}_{\text{Known to server}} \mod 8$$

Summary and future work

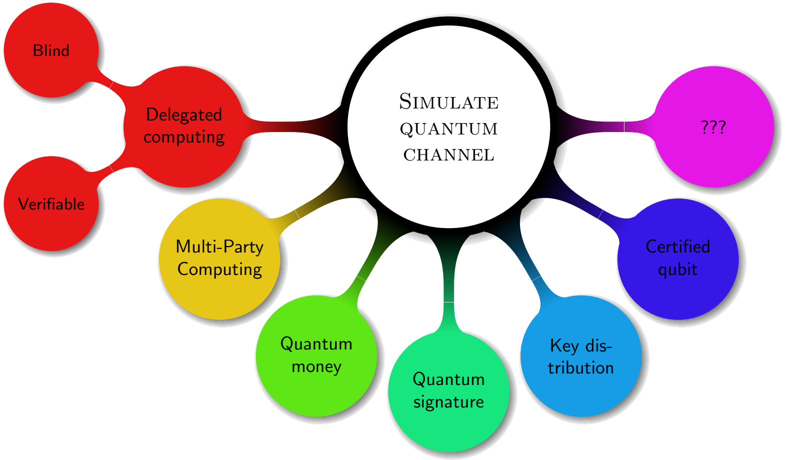
Summary

- QFactory: simulate quantum channel from classical channel
- ~~quantum client~~ $\rightarrow$ classical clients
- For now, proof in honest-but-curious model

Future work

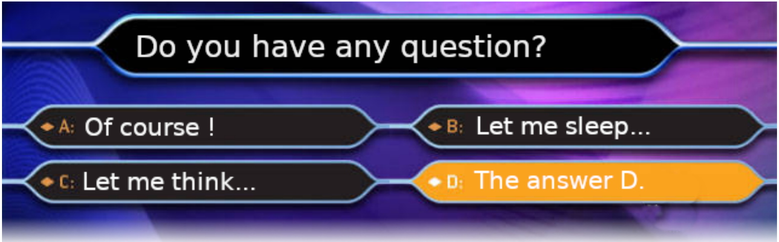
- Improve proof of security in Universal Composability model
- Improve efficiency in blind computing
- Explore new possible applications, certified qubits (QFactory + Zero Knowledge proof) that could improve MPC, GHZ state. . . . . .

Applications of QFactory



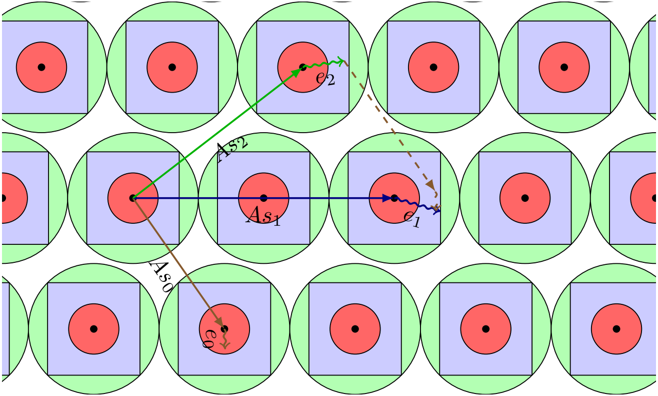
Questions

Thank you for your attention!



arxiv.org/abs/1802.08759

Function construction



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

Comparison with other works

Paper	Classical Homomorphic Encryption for Quantum Circuits	On the possibility of blind quantum computing	Classical Verification of Quantum Computations
Blind input			
Blind algorithm			
Verifiability			
Non-Interactive			
Efficiency/Requirements	FHE	UBQC/VBQC, Linear	Post-hoc, poly degree 9?