Classical leakage resilience from quantum fault tolerance

Felipe Lacerda[1,2] Joe Renes[1] Renato Renner[1]

[1]Institute of Theoretical Physics
ETH Zürich

[2]Department of Computer Science
University of Brasília

arXiv:1404.7516

Alice

Bob

Eve

Alice

Side channel

Bob

Eve

Side channel attacks can often be prevented by shielding the hardware.

But it's hard and costly to design mechanisms that can keep up with the technological advances in attacks on the devices.

Can we mitigate these attacks via software only?

Short answer: **yes**. Enter **leakage-resilient cryptography**

In this talk:

- A way to design general leakage-resilient circuits via a detour to quantum computation
- A classical result through a quantum argument

Not covered in this talk:

- Abstract definition of leakage resilience.
- All the ways to do (classical) leakage-resilient circuits through fully classical means. (It's a large field)

Leakage in this talk

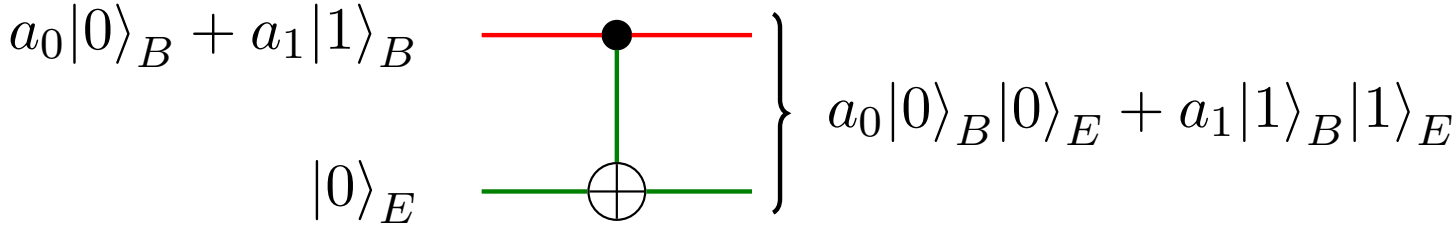
Setup:

- A circuit is initialized with a secret.
- Adversary has black-box access to the device, and gets some additional information (leakage) as a function of the circuit's wires.

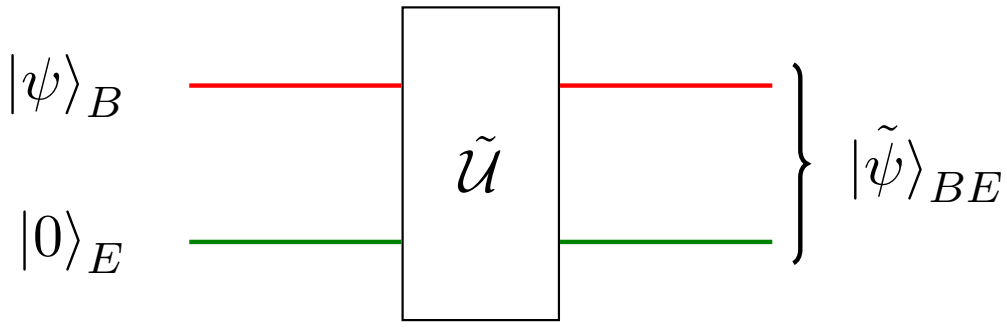
Goal:

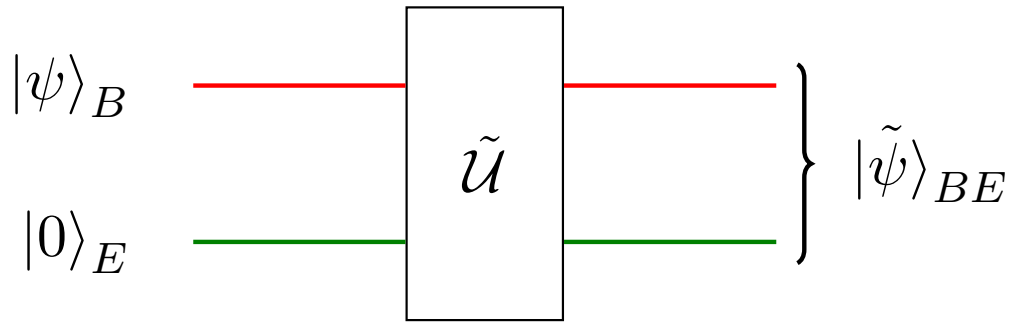
- Design circuit so that leakage is useless to adversary

What is leakage quantum-mechanically?

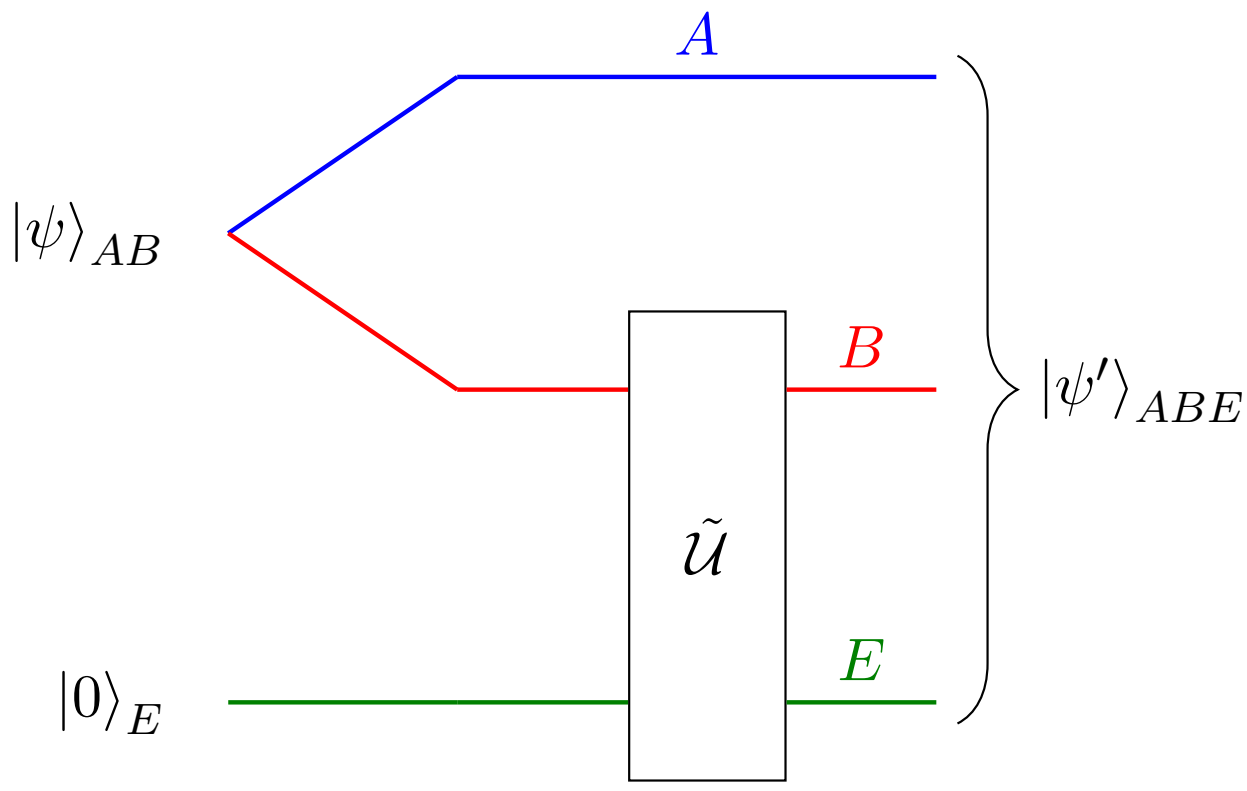


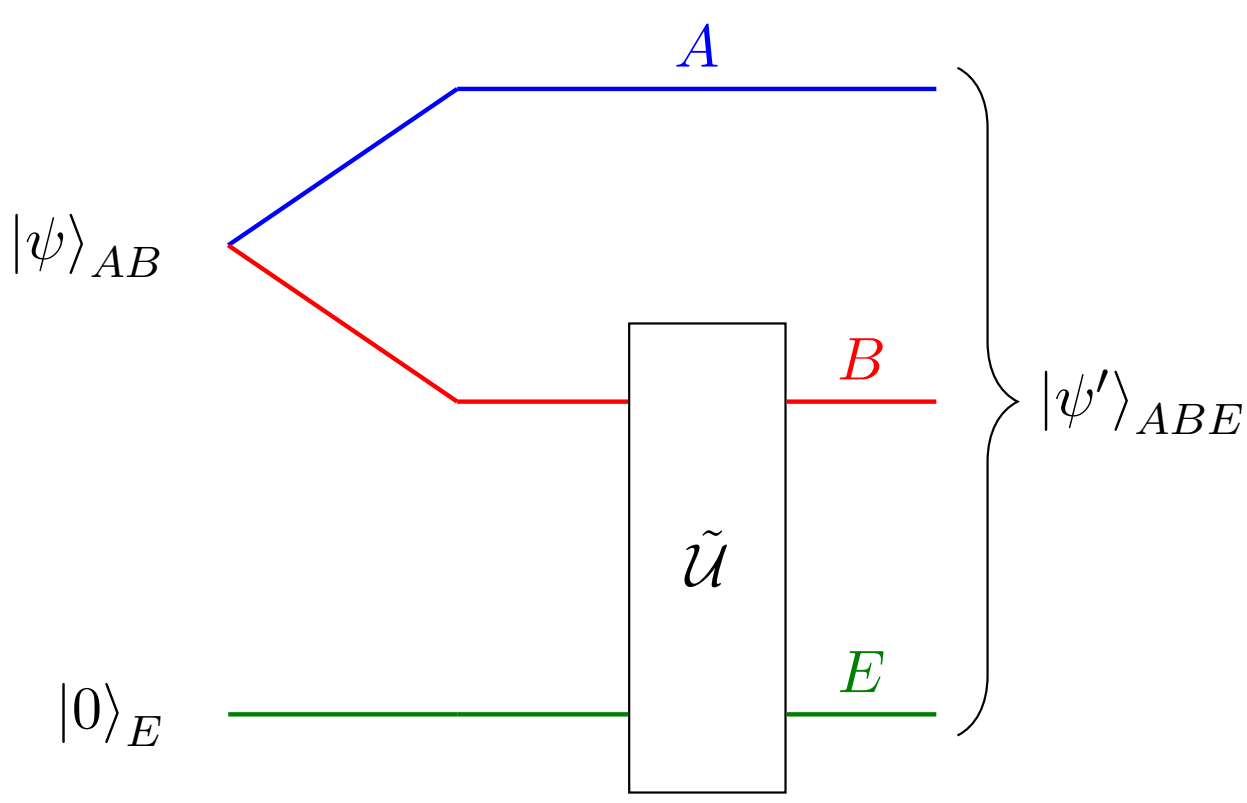
Leaking the value of one wire produces entanglement with the eavesdropper.

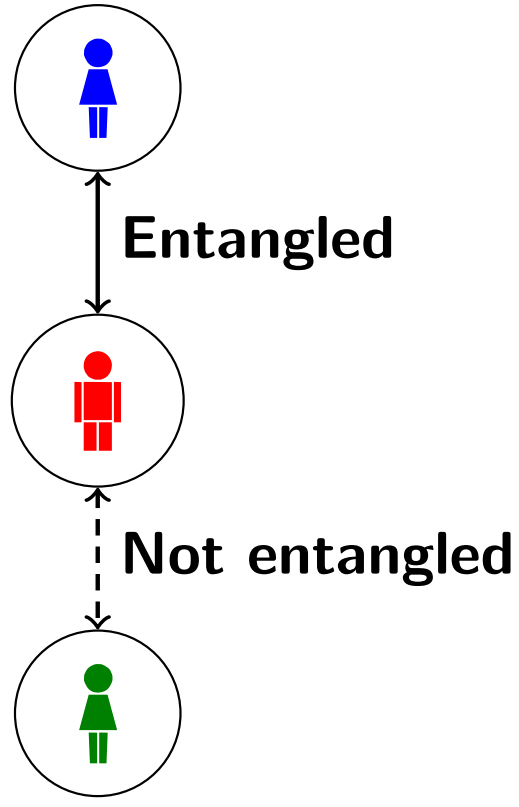

$|\psi\rangle_B$
$|0\rangle_E$
$\tilde{\mathcal{U}}$
$|\tilde{\psi}\rangle_{BE}$

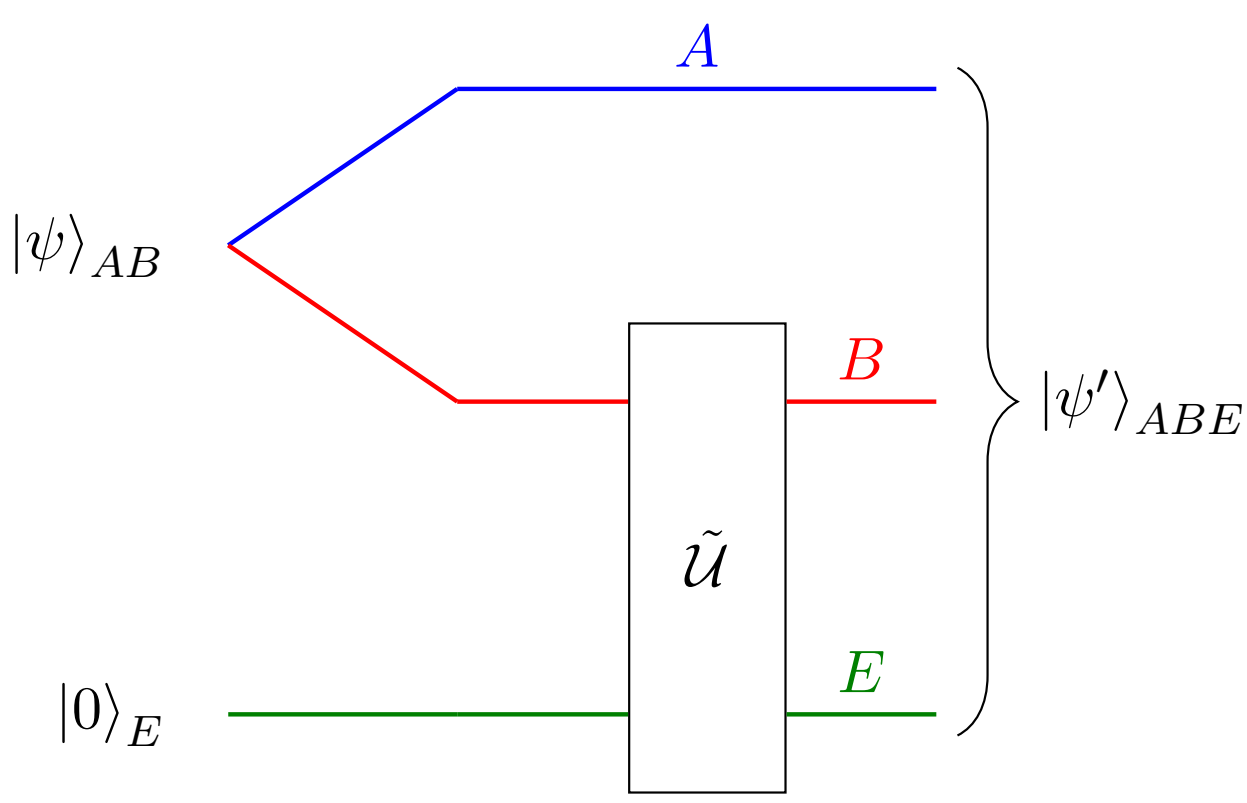


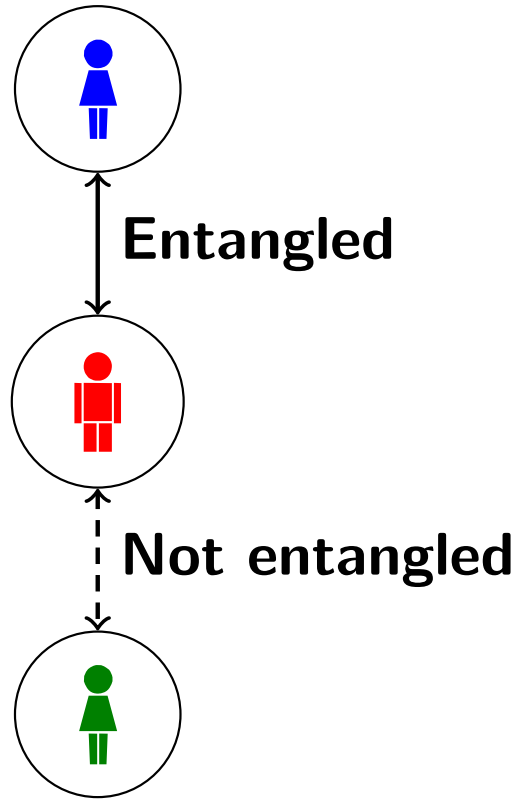
For quantum circuits, leakage is a form of noise.


A
$|\psi\rangle_{AB}$
B
$\tilde{\mathcal{U}}$
$|0\rangle_E$
E
$|\psi'\rangle_{ABE}$


A
$|\psi\rangle_{AB}$
B
$\tilde{\mathcal{U}}$
$|0\rangle_E$
E
$|\psi'\rangle_{ABE}$


Entangled
Not entangled





Reliable circuits are leakage-resilient

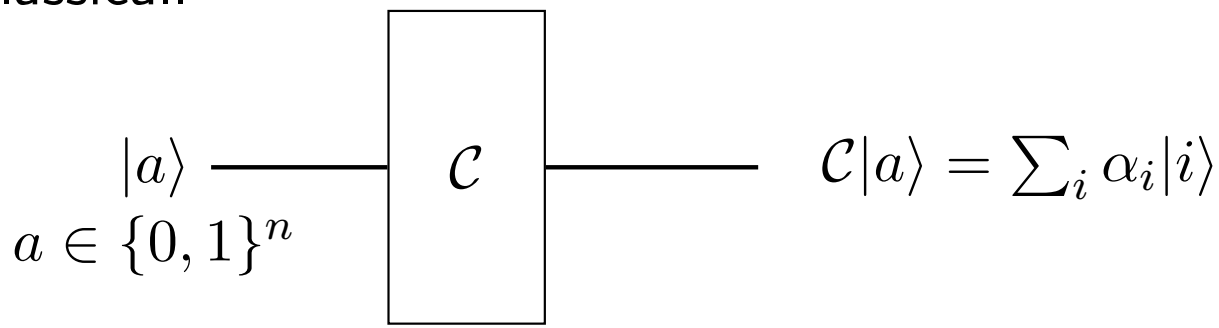
Next steps:

- Implement reliable computation. (spoiler: fault tolerance)
- Only part of the implementation is necessary for classical leakage-resilient circuits. Show how to do this part classically

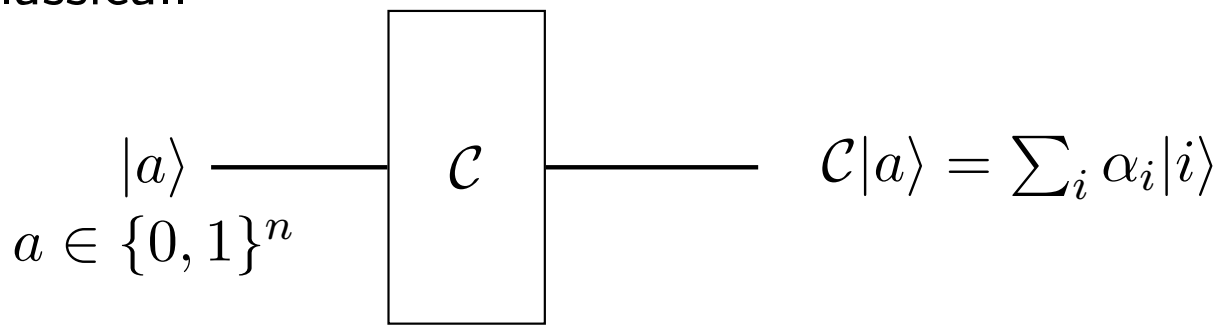
Making quantum circuits classical

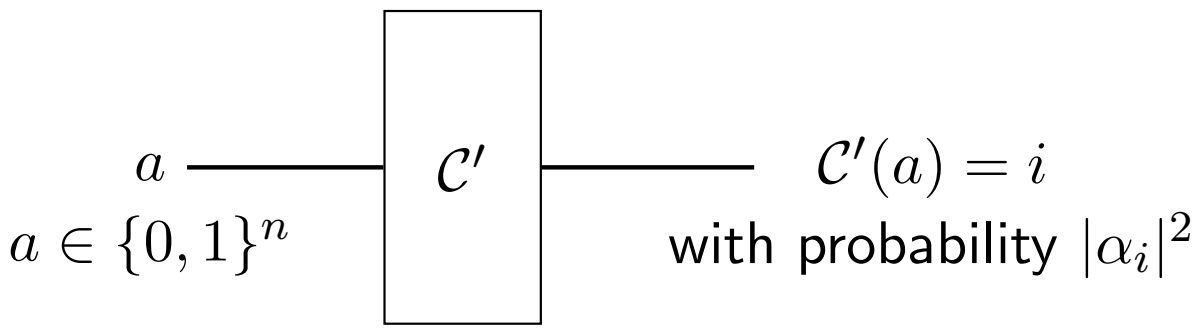
We only need to perform classical computation, but there's no guarantee that an implementation of a reliable circuit will be fully classical.

We only need to perform classical computation, but there's no guarantee that an implementation of a reliable circuit will be fully classical.

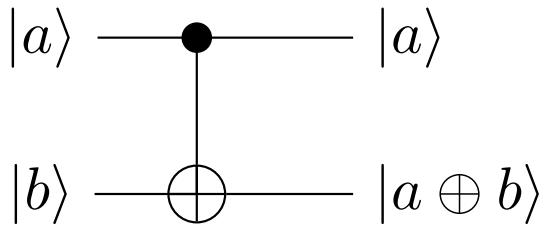


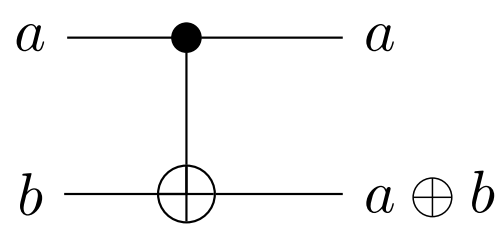
We only need to perform classical computation, but there's no guarantee that an implementation of a reliable circuit will be fully classical.

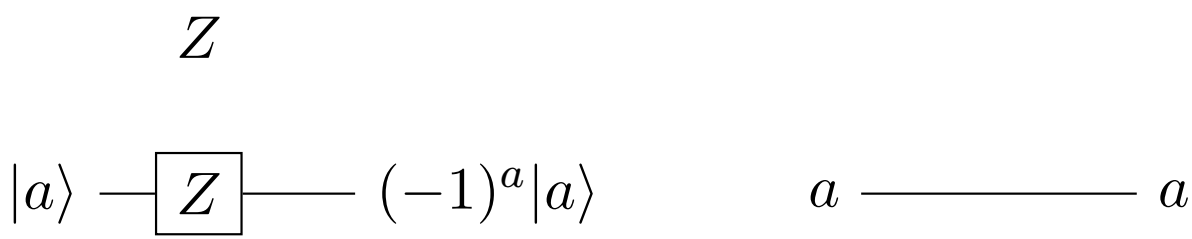




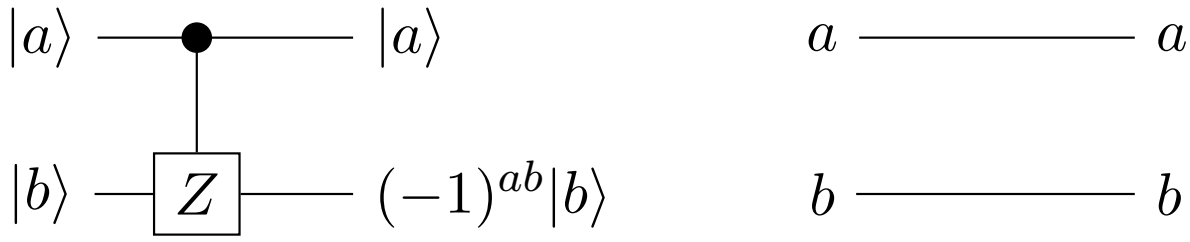
CNOT






Z
$|a\rangle$
Z
$(-1)^a|a\rangle$
a
a

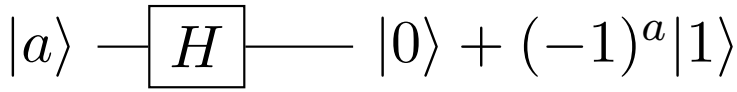
CZ



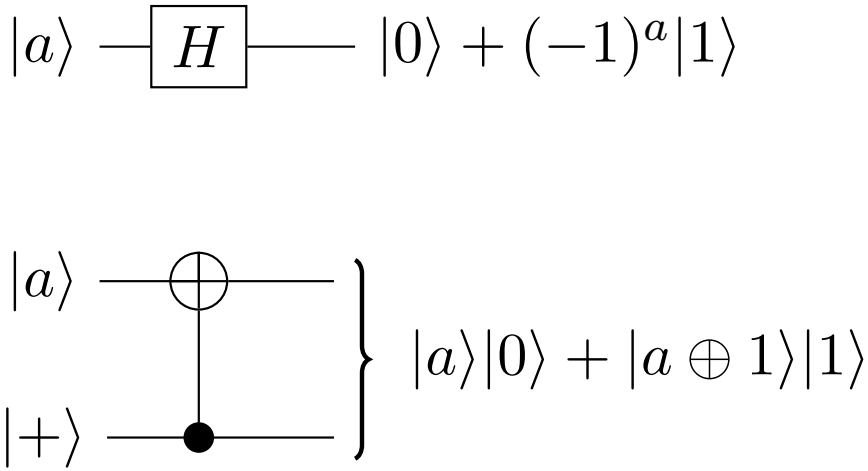
State preparation

Have to assume random bit is generated leak-free

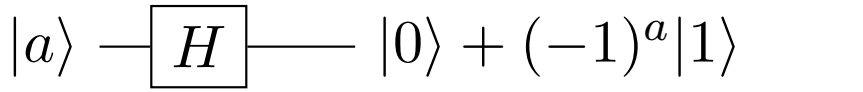
Phase measurement

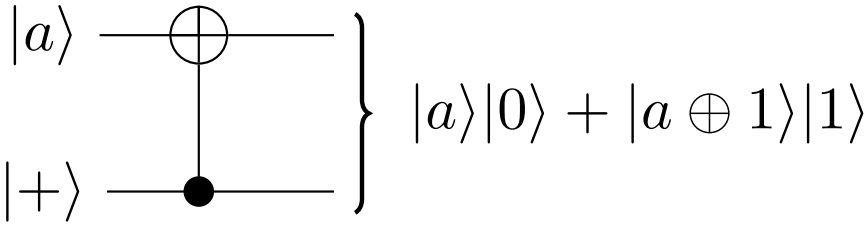


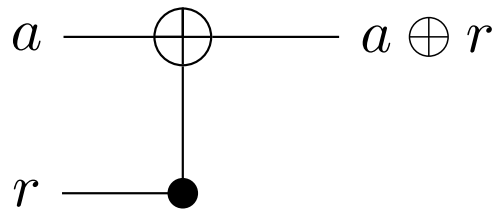
Phase measurement



Phase measurement

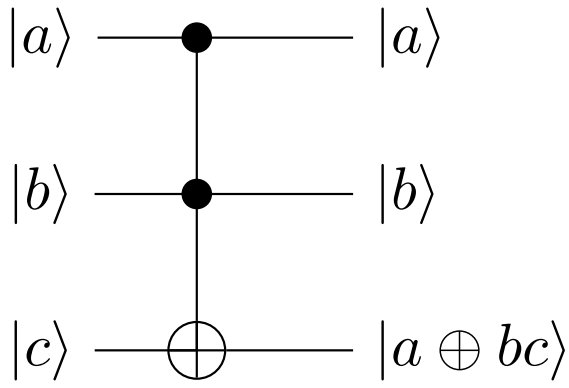


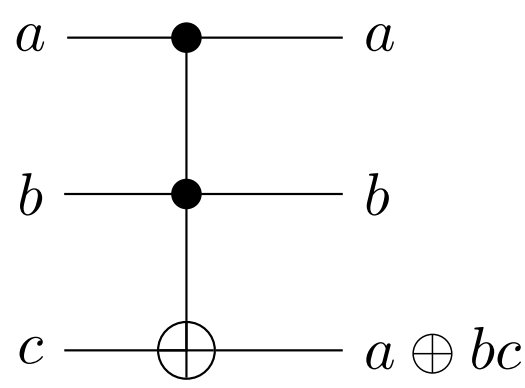




$r \leftarrow \{0, 1\}$

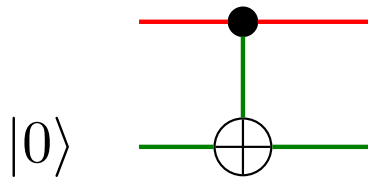
Toffoli


$|a\rangle$
$|b\rangle$
$|c\rangle$
$|a\rangle$
$|b\rangle$
$|a \oplus bc\rangle$

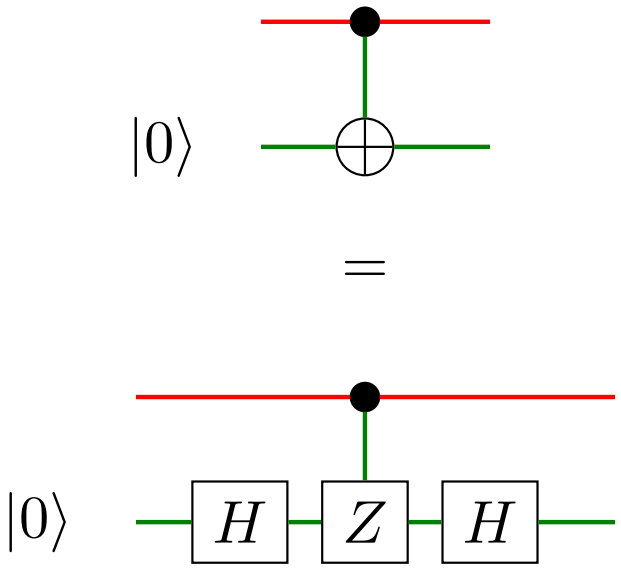

a
b
c
a
b
$a \oplus bc$

Fault tolerance

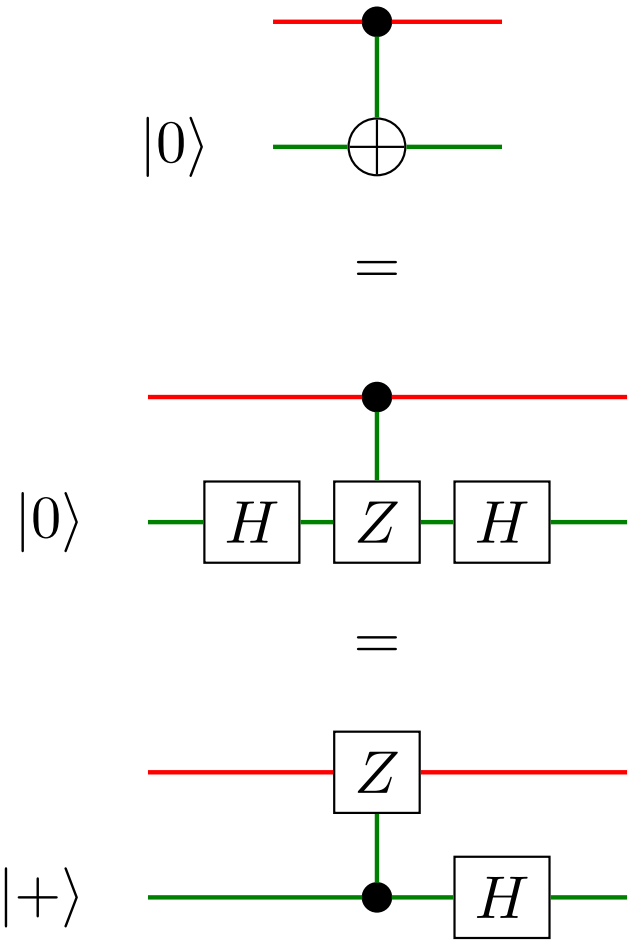
Leakage and quantum noise



Leakage and quantum noise

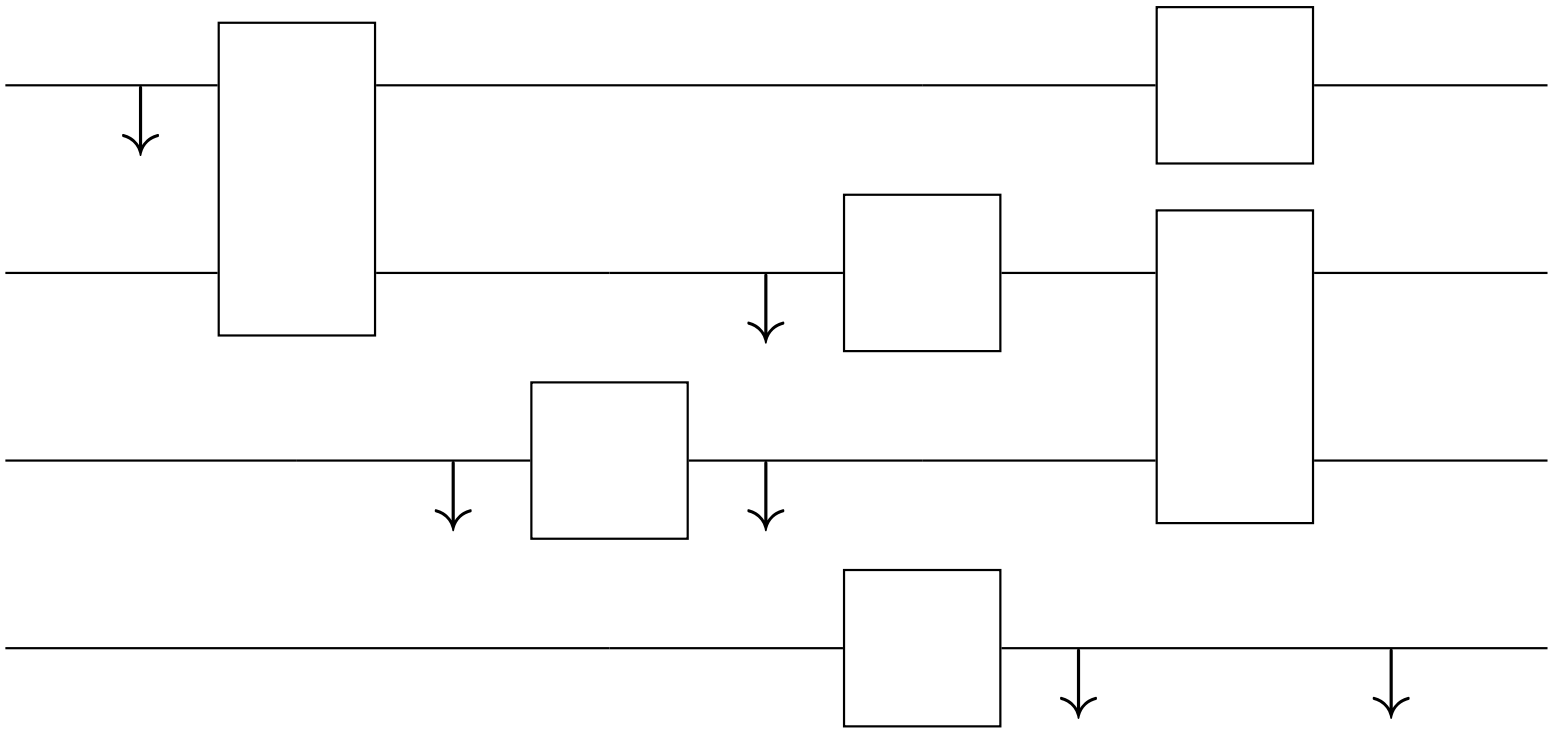


Leakage and quantum noise



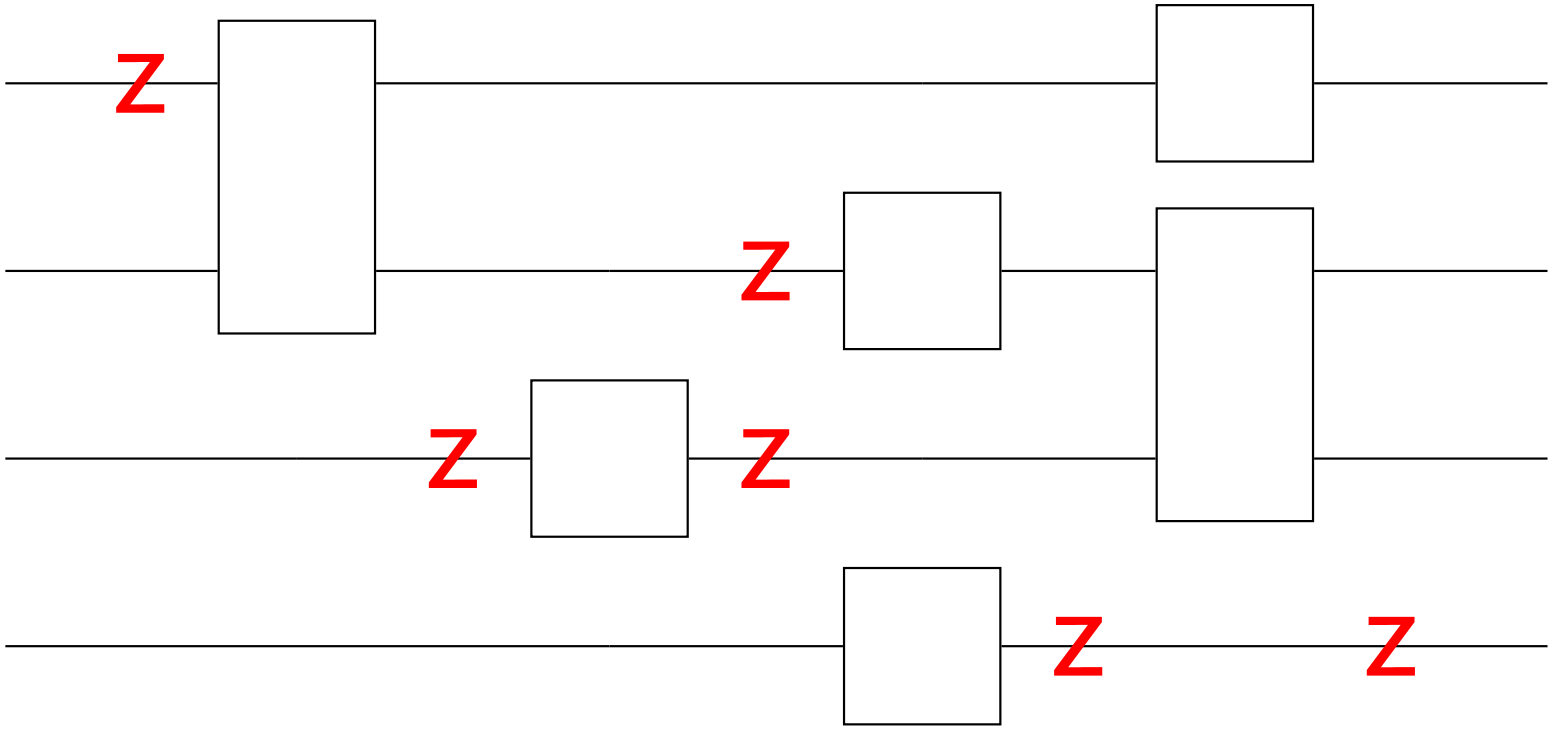
Leakage models and quantum noise

Independent leakage: each wire leaks with probability p.



Leakage models and quantum noise

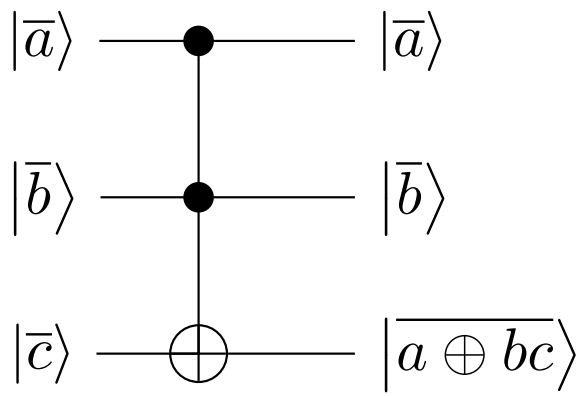
Independent leakage: each wire leaks with probability p.



Independent **phase noise**: each wire has a phase error with probability p

(Aliferis, Gottesman, Preskill, 2005): universal fault-tolerant computation in the independent noise model

(Aliferis, Gottesman, Preskill, 2005): universal fault-tolerant computation in the independent noise model



Toffoli gate: universal for classical computation

Bringing it all together

Theorem

Let $\mathcal{C}$ be an arbitrary quantum circuit with L locations and depth D. Then for any $\varepsilon > 0$ there exists a quantum circuit $\mathcal{C}'$, functionally equivalent to $\mathcal{C}$, with $L' = O(L \operatorname{polylog}(L))$ and depth $D' = O(D \operatorname{polylog}(L))$, that is ε-reliable against independent noise, as long as the probability of faults p satisfies $p < 10^{-5}$.

Bringing it all together

Theorem

*Let $\mathcal{C}$ be an arbitrary quantum circuit with L locations and depth D. Then for any $\varepsilon > 0$ there exists a quantum circuit $\mathcal{C}'$, functionally equivalent to $\mathcal{C}$, with $L' = O(L \operatorname{polylog}(L))$ and depth $D' = O(D \operatorname{polylog}(L))$, that is ~~$\varepsilon$-reliable~~ ε-**leakage-resilient** against ~~independent noise~~ **independent leakage**, as long as the probability of ~~faults~~ **leakage** p satisfies $p < 10^{-5}$.*

Bringing it all together

Theorem

Let $\mathcal{C}$ be an arbitrary ~~quantum~~ **reversible classical** *circuit with L locations and depth D. Then for any $\varepsilon > 0$ there exists a quantum circuit $\mathcal{C}'$, functionally equivalent to $\mathcal{C}$, with $L' = O(L \operatorname{polylog}(L))$ and depth $D' = O(D \operatorname{polylog}(L))$, that is ~~$\varepsilon$-reliable~~* **$\varepsilon$-leakage-resilient** *against ~~independent noise~~* **independent leakage**, *as long as the probability of ~~faults~~* **leakage** *p satisfies $p < 10^{-5}$.*

Bringing it all together

Theorem

Let $\mathcal{C}$ be an arbitrary ~~quantum~~ **reversible classical** *circuit with L locations and depth D. Then for any $\varepsilon > 0$ there exists a ~~quantum~~* **classical** *circuit $\mathcal{C}'$, functionally equivalent to $\mathcal{C}$, with $L' = O(L \operatorname{polylog}(L))$ and depth $D' = O(D \operatorname{polylog}(L))$, that is ~~$\varepsilon$-reliable~~ ε-***leakage-resilient** *~~against independent noise~~* **independent leakage**, *as long as the probability of ~~faults~~* **leakage** *p satisfies $p < 10^{-5}$.*

To conclude

Classical cryptographers could profit from knowing more about quantum information.

To conclude

Classical cryptographers could profit from knowing more about quantum information.

Thanks!