# Quantum fully homomorphic encryption with verification

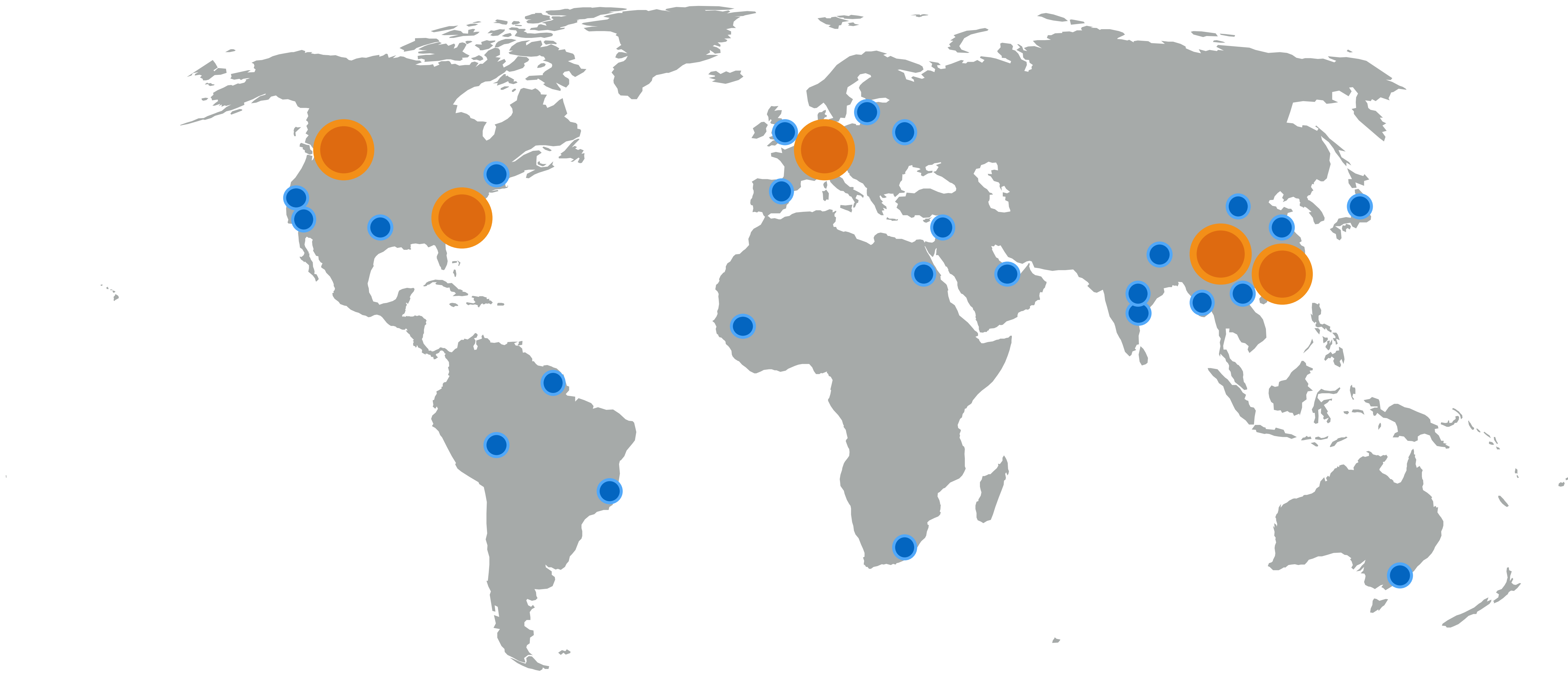

Gorjan Alagic,

Yfke Dulek,
Christian Schaffner,

and **Florian Speelman**


arXiv:1708.09156

# A Possible Future for Quantum Computing



private — efficient — verifiable

Disclaimer: dots placed carelessly

# Outline

1. (Quantum) Fully Homomorphic Encryption
2. Classical application: zero-knowledge proofs
3. Our contributions:
   - Definitions
   - Construction
   - Application

# Classical Fully Homomorphic Encryption

| | |
|---|---|
| KeyGen | $k\ ,\ evk$ |
| Enc | $k, x \to \bar{x}$ |
| Eval | $evk, f, \bar{x} \to \bar{y}$ |
| Dec | $k, \bar{y} \to y$ |

**Homomorphic** if $y = f(x)$

**Classical FHE** possible [Gen09] under comp assumptions.
Current focus: efficiency

[Gen09] Gentry. A fully homomorphic encryption scheme. PhD thesis, 2009.

# Quantum Fully Homomorphic Encryption

| | |
|---|---|
| KeyGen | $k, evk$ |
| Enc | $k, \sigma \rightarrow \bar{\sigma}$ |
| Eval | $evk, C, \bar{\sigma} \rightarrow \bar{\rho}$ |
| Dec | $k, \bar{\rho} \rightarrow \rho$ |

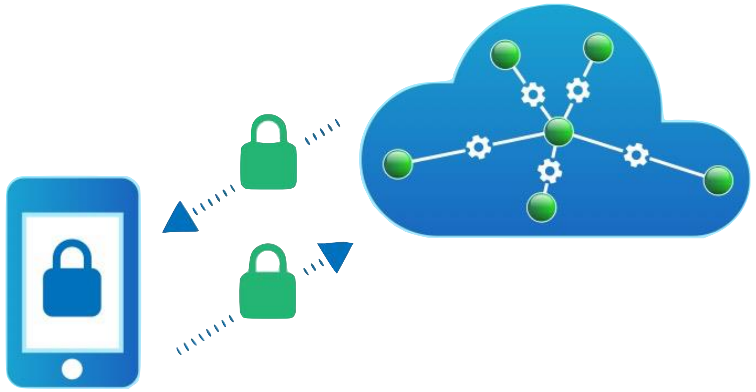
**Homomorphic** if $\rho = C(\sigma)$

**Quantum FHE** possible [DSS16] under comp assumptions.
Current focus: efficiency

[DSS16] Dulek, Schaffner, and Speelman. Quantum homomorphic encryption for polynomial-sized circuits. CRYPTO 2016.

# Applications of Fully Homomorphic Encryption

**Practical application:**
outsourcing computations



**Theoretical applications (classical):**
multiparty computation, functional encryption, private information retrieval, zero-knowledge proofs, and more…

**Theoretical applications (quantum):** ???

# Zero-knowledge proofs (classical)

SAT: given a formula $\phi$, is $\phi$ satisfiable?

I know! $\phi$ is satisfiable!

Wonderful! Can you prove it to me?
I am only a polynomial-time human…

Well, I know a satisfying assignment $w$,
but I am not going to tell YOU…

Let's do a zero-knowledge proof!

# Zero-knowledge from FHE (classical)

$\bar{w} \leftarrow Enc_k(w)$

$b \in_R \{0,1\}$

(prover)

if $b = 1$: $\bar{c} \leftarrow \mathrm{Eval}_{evk}(\texttt{witness-check-fn}, \bar{w})$
if $b = 0$: $\bar{c} \leftarrow \mathrm{Eval}_{evk}(\texttt{set-to-0}, \bar{w})$

$\mathrm{c} \leftarrow \mathrm{Dec}_k(\bar{c})$

if $c = b$, **accept** (otherwise **reject**)

*(verifier)*

Prover cannot cheat… but verifier can!

[Bar12] Barak. The Swiss Army Knife of Cryptography. "Windows on Theory" blog post, 2012.

# Zero-knowledge from FHE (classical)

$\bar{w} \leftarrow \mathrm{Enc}_k(w)$

$b \in_R \{0,1\}$

*(prover)*

if $b = 1$: $\bar{c} \leftarrow \mathrm{Eval}_{evk}(\texttt{witness-check-fn}, \bar{w})$
if $b = 0$: $\bar{c} \leftarrow \mathrm{Eval}_{evk}(\texttt{set-to-0}, \bar{w})$

**commit to** c $\leftarrow \mathrm{Dec}_k(\bar{c})$

proof of computation (transcript)

if transcript is ok, **reveal** $c$

if $c = b$, **accept** (otherwise **reject**)

*(verifier)*

[Bar12] Barak. The Swiss Army Knife of Cryptography. "Windows on Theory" blog post, 2012.

# Verification in (Q)FHE

- **Verification of computation** is crucial in applications
- **Classical FHE** has verification "automatically"
- **Quantum FHE** does not

# Verification in (Q)FHE

- **Verification of computation** is crucial in applications

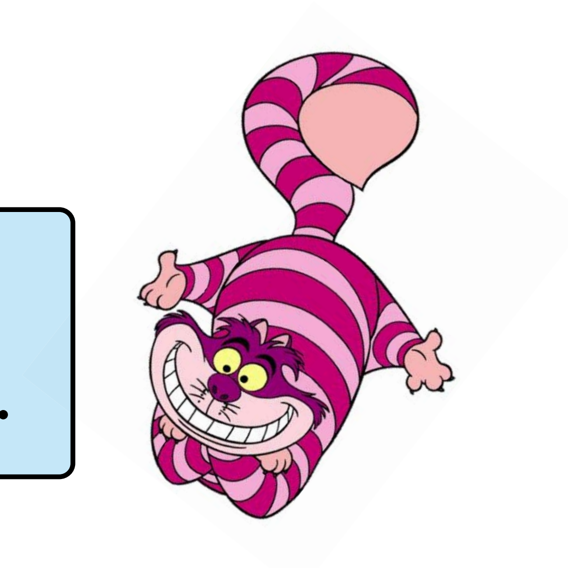
I will only accept your output if I can
verify that you applied
the right circuit to my input!

- **Classical FHE** has verification "automatically"
- **Quantum FHE** does not

# Verification in (Q)FHE

- **Verification of computation** is crucial in applications
- **Classical FHE** has verification “automatically”

> Here is a transcript of all the steps in my computation, please check them all.



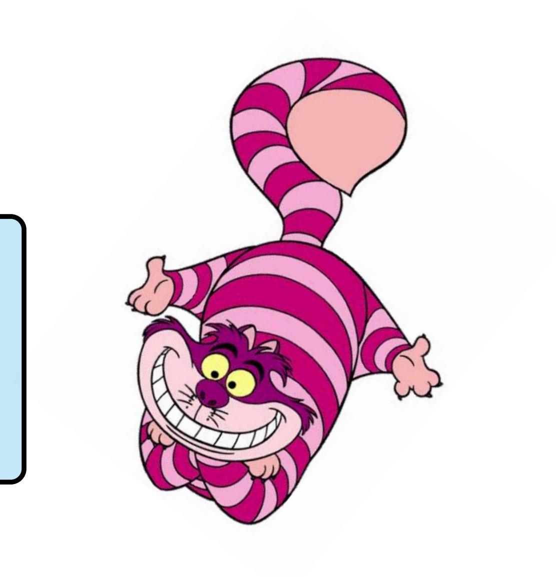
- **Quantum FHE** does not

# Verification in (Q)FHE

- **Verification of computation** is crucial in applications
- **Classical FHE** has verification "automatically"
- **Quantum FHE** does not

  Measurement and no-cloning prevent this easy solution

The outcome of that measurement was 0, truly! You must believe me!



# Related topics

- Quantum authentication
- Quantum computing on authenticated data
- Quantum fully homomorphic encryption

# Related topics

- **Quantum authentication**
  - “verifiable HE” for the identity circuit
  - e.g. polynomial code [BCG+06] , Clifford code [ABE10], trap code [BGS12]

Hold this qubit, I will be *right* back!

- **Quantum computing on authenticated data**
- **Quantum fully homomorphic encryption**

[BCG+02] Barnum, Crepeau, Gottesman, Smith, and Tapp. Authentication of quantum messages. FOCS 2002.
[ABE10] Aharonov, Ben-Or, and Eban. Interactive proofs for quantum computations. ICS 2010.
[BGS12] Broadbent, Gutoski, and Stebila. Quantum one-time programs. CRYPTO 2013.

# Related topics

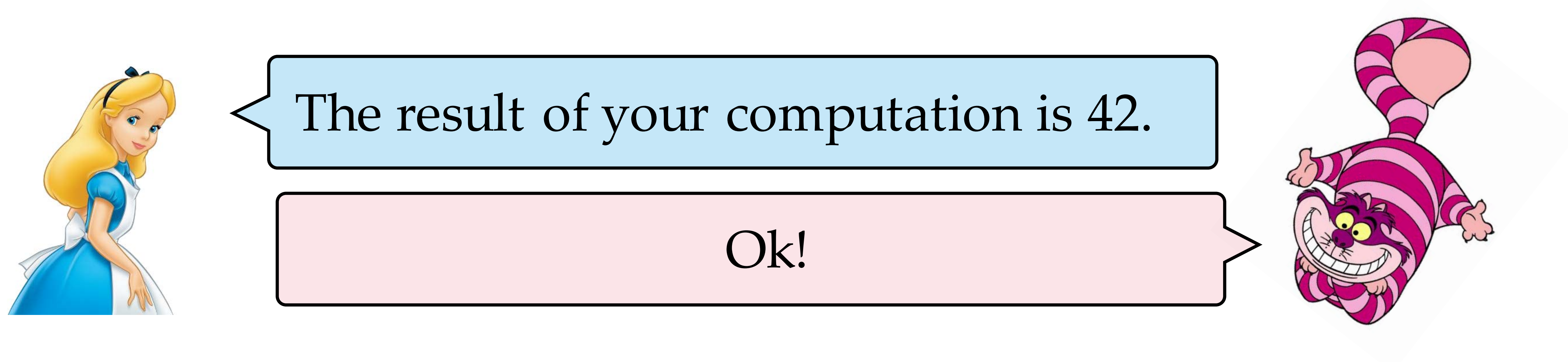
- **Quantum authentication**
- **Quantum computing on authenticated data**
  - interaction during evaluation
  - verification

- **Quantum fully homomorphic encryption**

[BCG+02] Barnum, Crepeau, Gottesman, Smith, and Tapp. Authentication of quantum messages. FOCS 2002.
[ABE10] Aharonov, Ben-Or, and Eban. Interactive proofs for quantum computations. ICS 2010.
[BGS12] Broadbent, Gutoski, and Stebila. Quantum one-time programs. CRYPTO 2013.

# Related topics

- **Quantum authentication**
- **Quantum computing on authenticated data**
- **Quantum fully homomorphic encryption**
  - no interaction during evaluation
  - no verification




[BCG+02] Barnum, Crepeau, Gottesman, Smith, and Tapp. Authentication of quantum messages. FOCS 2002.
[ABE10] Aharonov, Ben-Or, and Eban. Interactive proofs for quantum computations. ICS 2010.
[BGS12] Broadbent, Gutoski, and Stebila. Quantum one-time programs. CRYPTO 2013.

# Our contributions

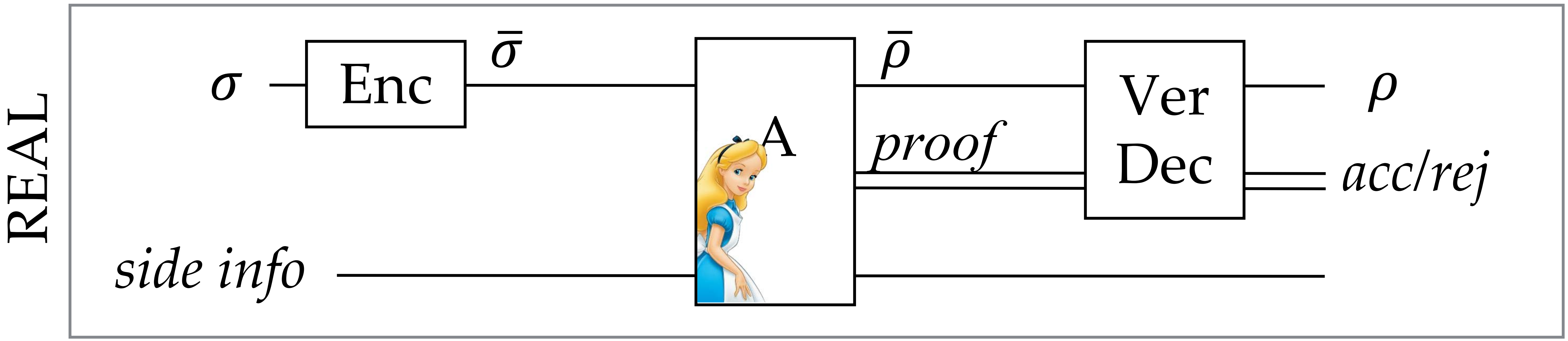
**Definitions**

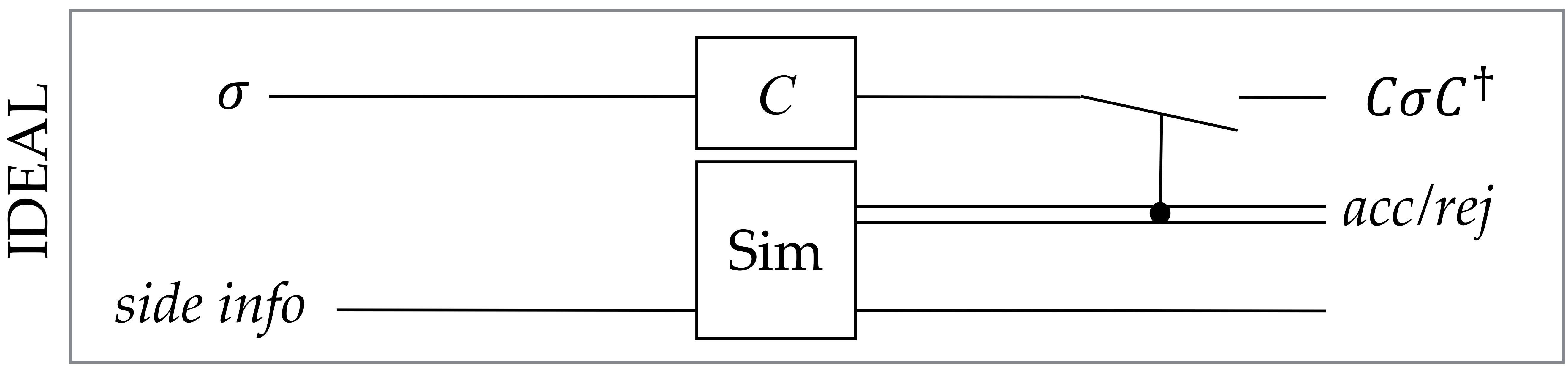
**Construction: a verifiable QFHE scheme**

**Application: quantum one-time programs**

# Defns: Verification in QFHE

Dec replaced by **VerDec**: $k, \bar{\rho}, C,$ *proof* $\rightarrow \rho,$ *accept/reject*




**Verifiability:** ∀poly A ∃ poly Sim ∀$\sigma$, *side info*, C:
REAL and IDEAL are indistinguishable

# Defns: Verification in QFHE

**Variant (indistinguishability)**

- Alternative security definition in terms of a guessing game
  - Adversary has to guess whether he interacts with actual or idealized functionality
- Proven equivalent to semantic definition

**Compactness**

- Verification: (classical) proof, output accept/reject
- Decryption: quantum input, runtime should **not** depend on circuit

# Construction: Verifiable QFHE

**Ingredients**

- Quantum authentication code: trap code
- Classical FHE: any quantum-secure scheme
  with low-depth decryption
- Classical MAC: any quantum-secure scheme

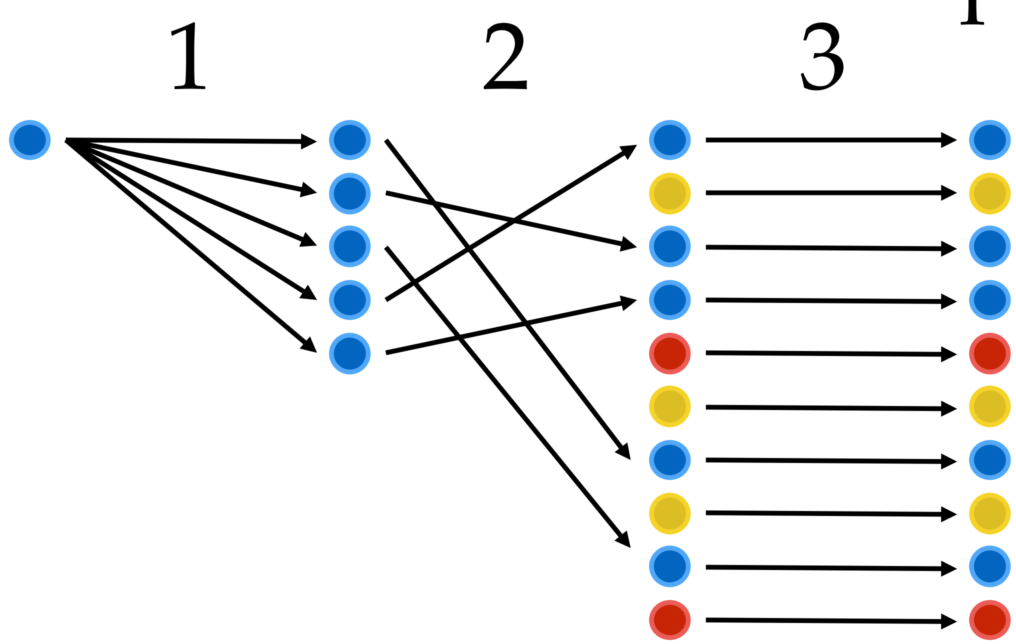
[BGS12] Broadbent, Gutoski, and Stebila. Quantum one-time programs. CRYPTO 2013.

# Construction: Verifiable QFHE

traps: $|0\rangle$, $|+\rangle$

**Encryption**

Authenticate with trap code




1. error-correcting code
2. traps in random positions
3. quantum one-time pad

**secret key:** positions + pad keys

Encode secret key with classical FHE+MAC

Encrypted qubit:

(classical encrypted info, trap code qubits)

# Construction: Verifiable QFHE

**Evaluation**

Clifford operations (X, Z, H, P, CNOT):

- Apply transversally (magic states)
- Update encoded keys using FHE

T gate:

- After applying, unwanted P error
- Use (new, extended) gadget to remove the error
  - (using ideas from [DSS16])

**Verify & Decrypt**

Check (classical) MAC+FHE transcript of key updates

Decrypt trap code if everything checks out

[DSS16] Dulek, Schaffner, and Speelman. Quantum homomorphic encryption for polynomial-sized circuits. CRYPTO 2016.

# Application: one-time programs

- Idea: Programs that 'self-destruct' after a single execution
- Ingredients:
  - Classical one-time program
  - Verifiable QFHE scheme
- Simple construction
  - Q-OTP for C: (evk, OTP for VerDec(C,k,·), $Enc_k$(C))

    Proof of correct execution is classical
- Not a new result [BGS12]

[BGS12] Broadbent, Gutoski, and Stebila. Quantum one-time programs. CRYPTO 2013.

# Summary

- **Definitions**
  - verifiability (semantic)
  - verifiability (indistinguishability)
  - compactness
- **Construction: a verifiable QFHE scheme**
- **Application: quantum one-time programs**

# Summary

- **Definitions**
- **Construction: a verifiable QFHE scheme**

  Ingredients:
  - classical FHE
  - classical authentication code (MAC)
  - quantum authentication code (trap code)

- **Application: quantum one-time programs**

# Summary

- **Definitions**
- **Construction: a verifiable QFHE scheme**
- **Application: quantum one-time programs**

  Alternative construction to [BGS12]. Ingredients:
  - classical one-time programs
  - QFHE with verification

[BGS12] Broadbent, Gutoski, and Stebila. Quantum one-time programs. CRYPTO 2013.

# Future work / open questions

- Apply verifiable QFHE to build other advanced cryptographic primitives
- Are non-leveled schemes possible?
- Reduce client quantum capabilities

Thank you