Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model

Jelle Don, Serge Fehr, **Christian Majenz**
and Christian Schaffner

QIP 2020
Hilton Shenzhen Shekou Nanhai Hotel, Shenzhen, China

QuSoft
Research Center for Quantum Software

CWI
Centrum Wiskunde & Informatica

University of Amsterdam

Universiteit Leiden

NWO

Two facts of life

Two facts of life

1. Interaction is exhausting (=costly).

Two facts of life

1. Interaction is exhausting (=costly).

2. Testing/verification is more efficient interactively than noninteractively

Two facts of life

1. Interaction is exhausting (=costly).

2. Testing/verification is more efficient interactively than noninteractively

Fiat-Shamir reconciles the two in certain cases.

Outline

1. Introduction
   - Interactive proof systems
   - The Fiat Shamir transformation
2. Results
   - Overview
   - Reduction
   - Techniques
3. Application: Digital Signatures

1. Introduction

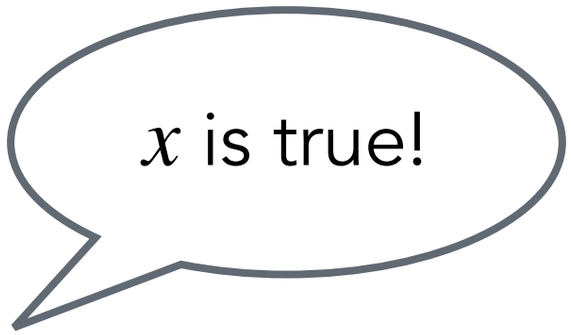
Interactive proof system

Interactive proof system

Prover

Verifier

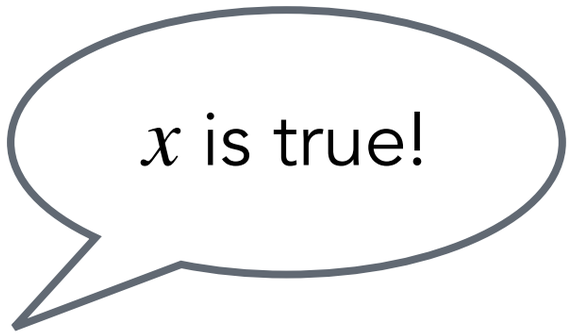
Interactive proof system



Prover

Verifier

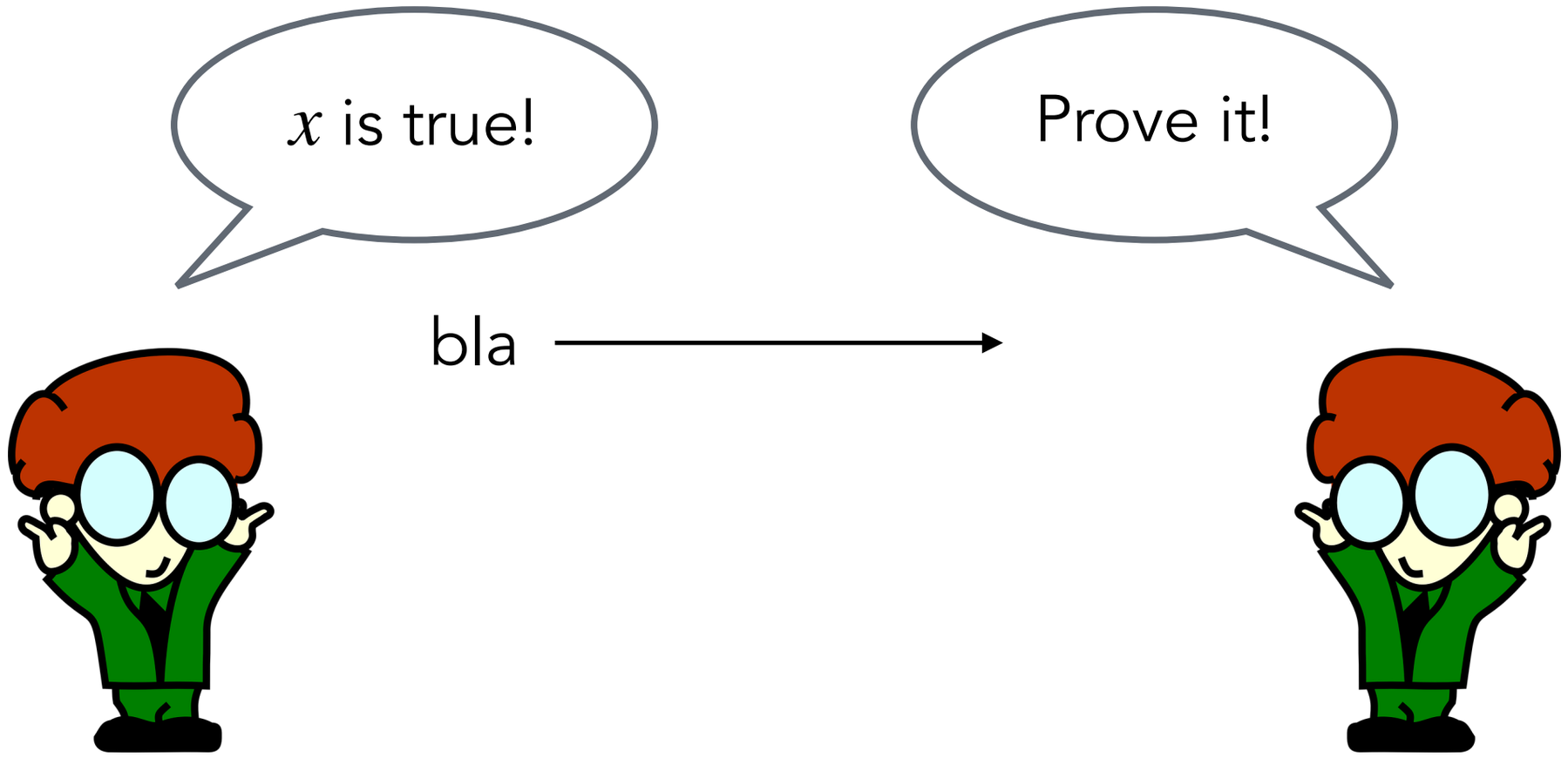
Interactive proof system



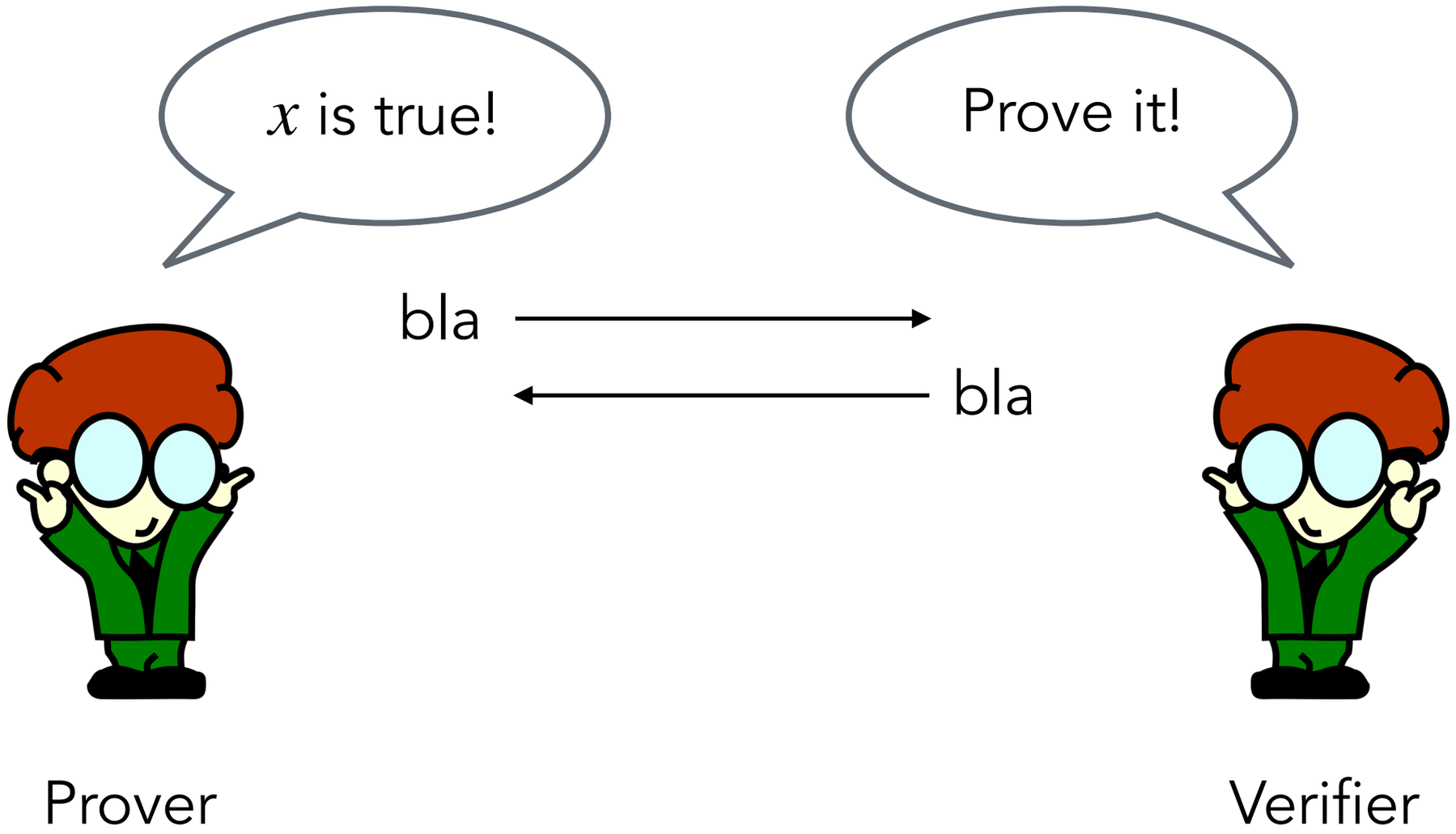
Prover

Verifier

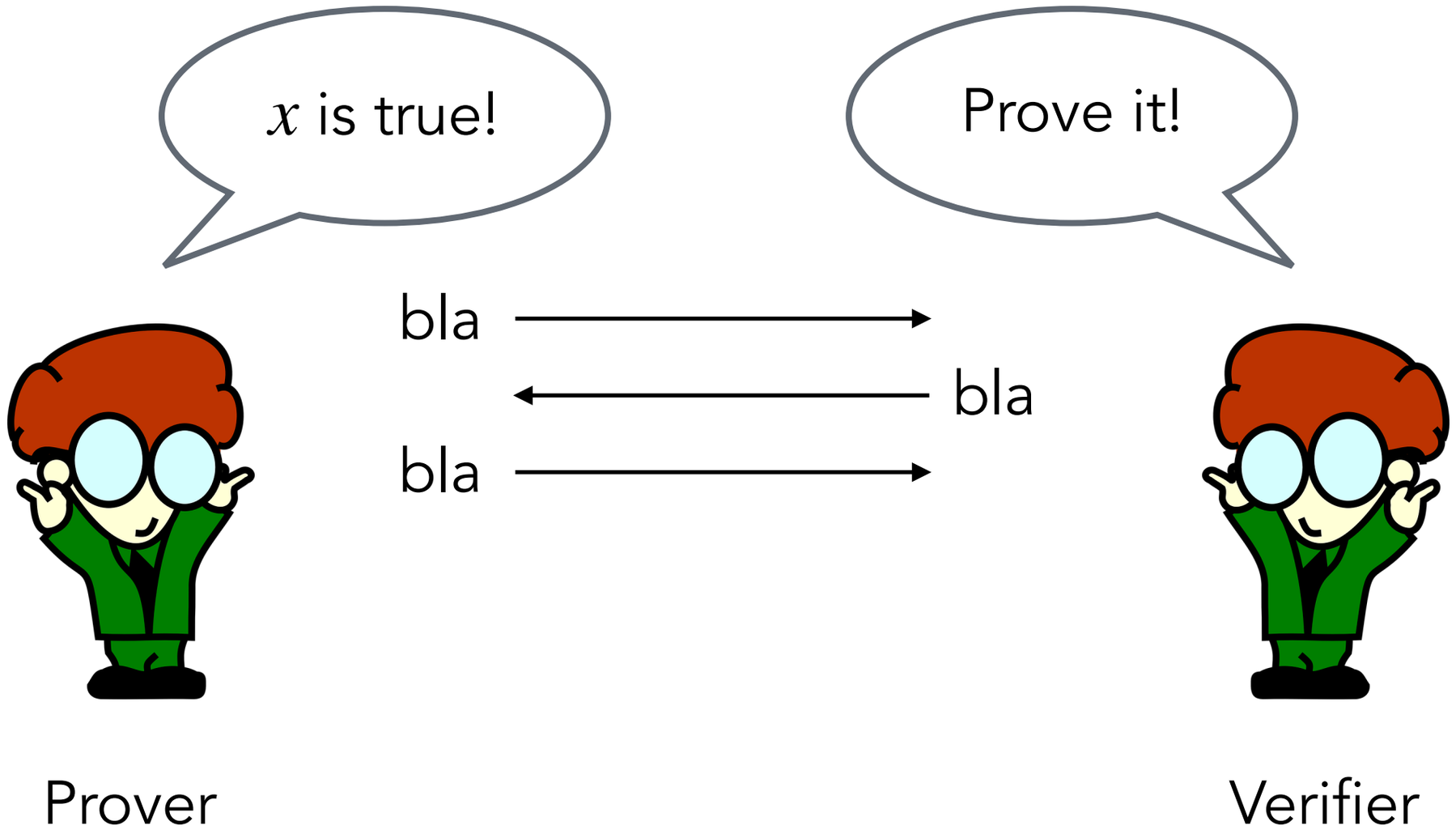
Interactive proof system



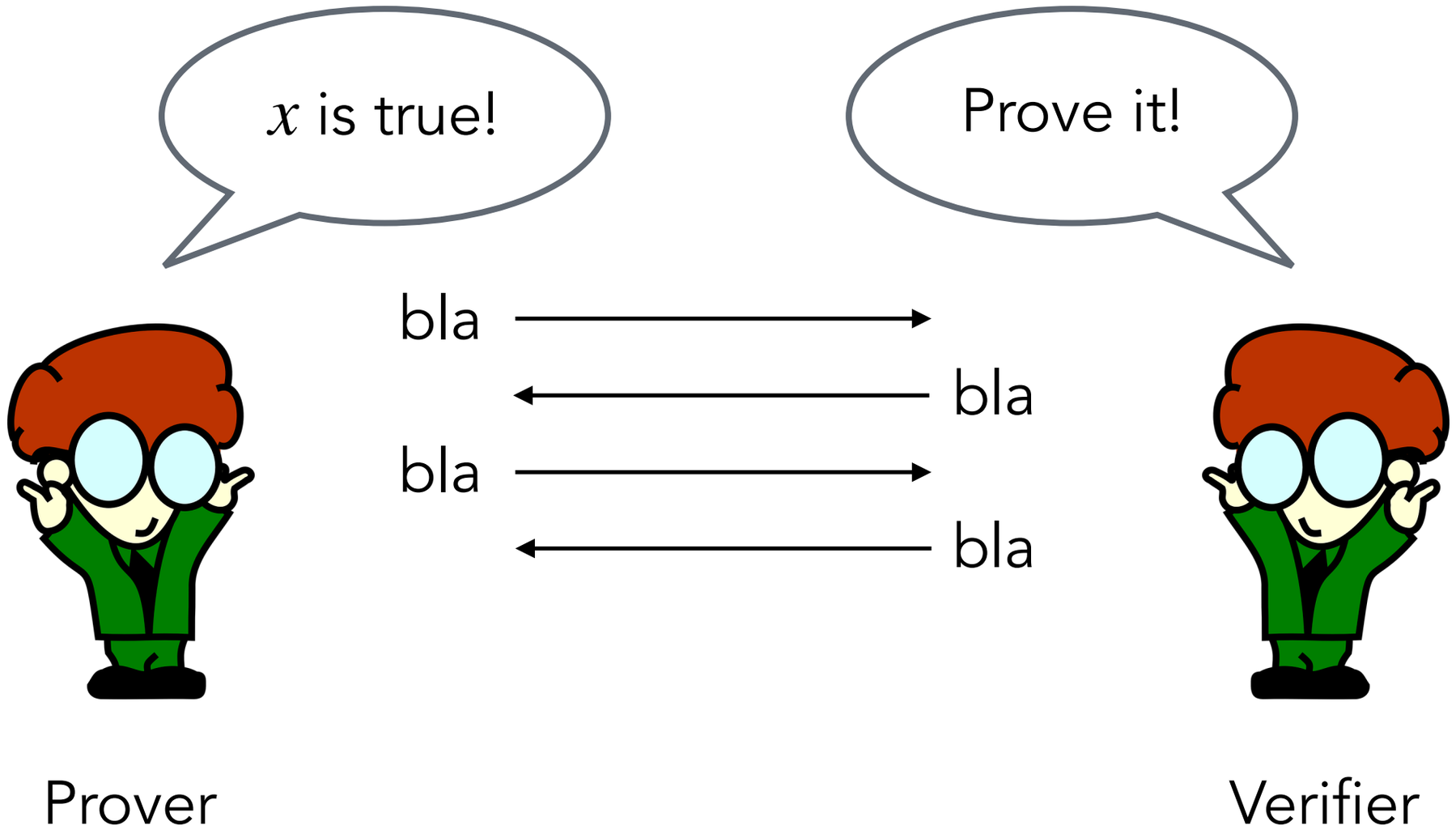
Interactive proof system



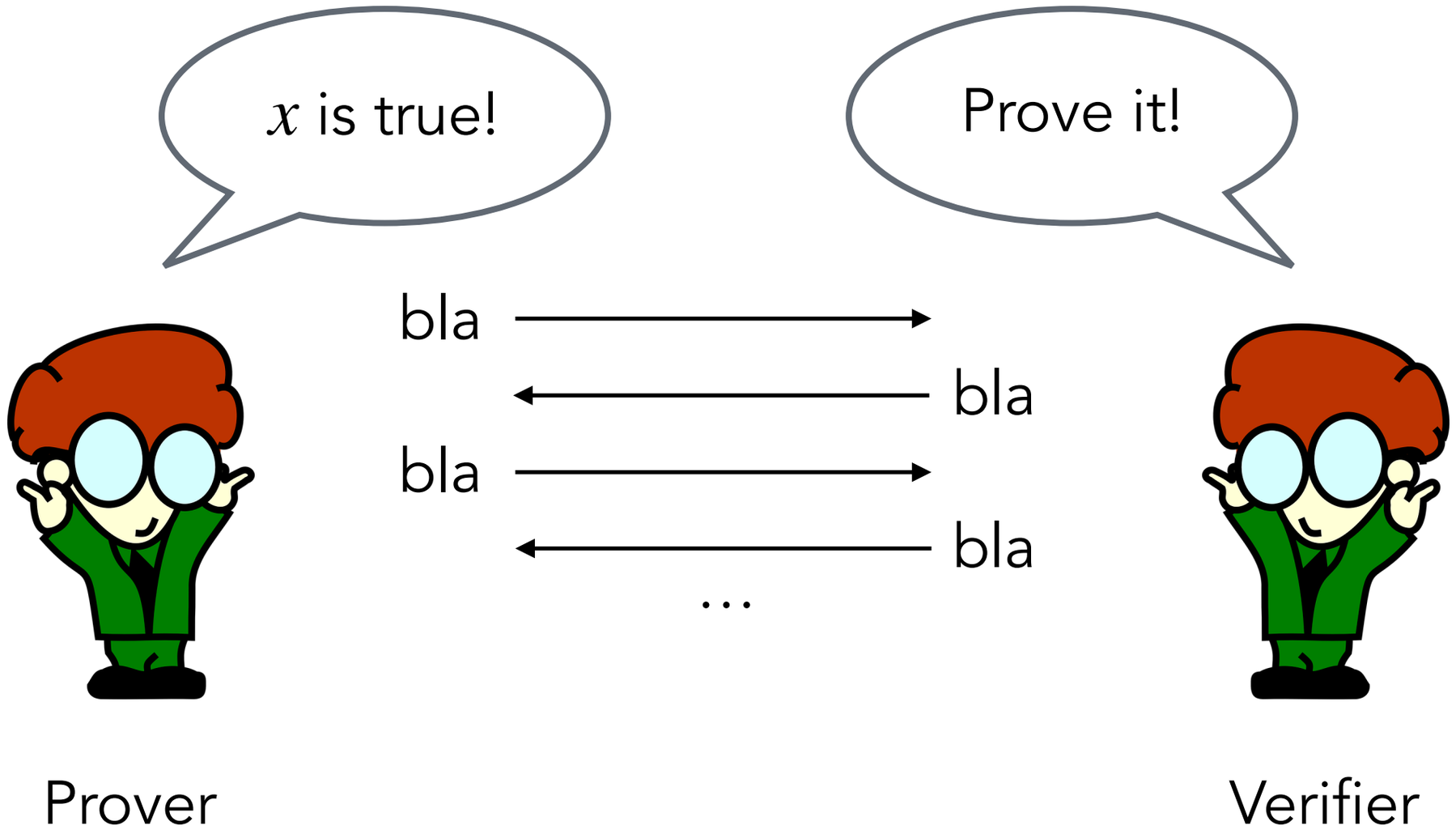
Interactive proof system



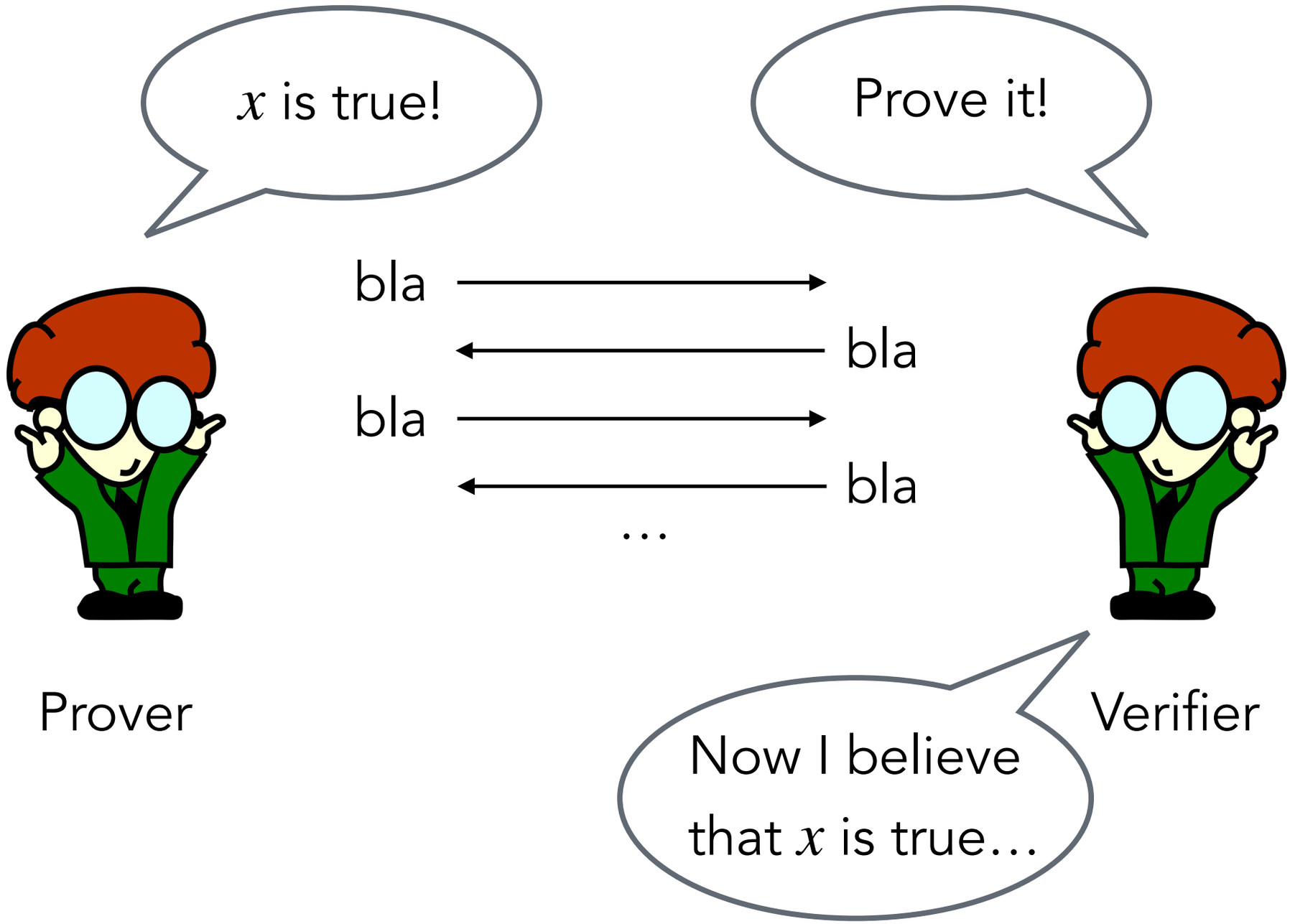
Interactive proof system



Interactive proof system



Interactive proof system



Interactive proof system

Interactive proof system

Many cryptographic properties:

Interactive proof system

Many cryptographic properties:

- Completeness

Interactive proof system

Many cryptographic properties:

- Completeness
- Soundness

Interactive proof system

Many cryptographic properties:

- Completeness
- Soundness
- Zero-knowledge

Interactive proof system

Many cryptographic properties:

- Completeness
- Soundness
- Zero-knowledge
- Proof-of-knowledge

Interactive proof system

Many cryptographic properties:

- Completeness
- Soundness
- Zero-knowledge
- Proof-of-knowledge
- …

Interactive proof system

Many cryptographic properties:

- Completeness
- Soundness
- Zero-knowledge
- Proof-of-knowledge
- …

} perfect/statistical/computational

Interactive proof system

Many cryptographic properties:

- Completeness
- Soundness
- Zero-knowledge
- Proof-of-knowledge
- …

} perfect/statistical/computational

Can we do the same without interaction?

Interactive proof system

Many cryptographic properties:

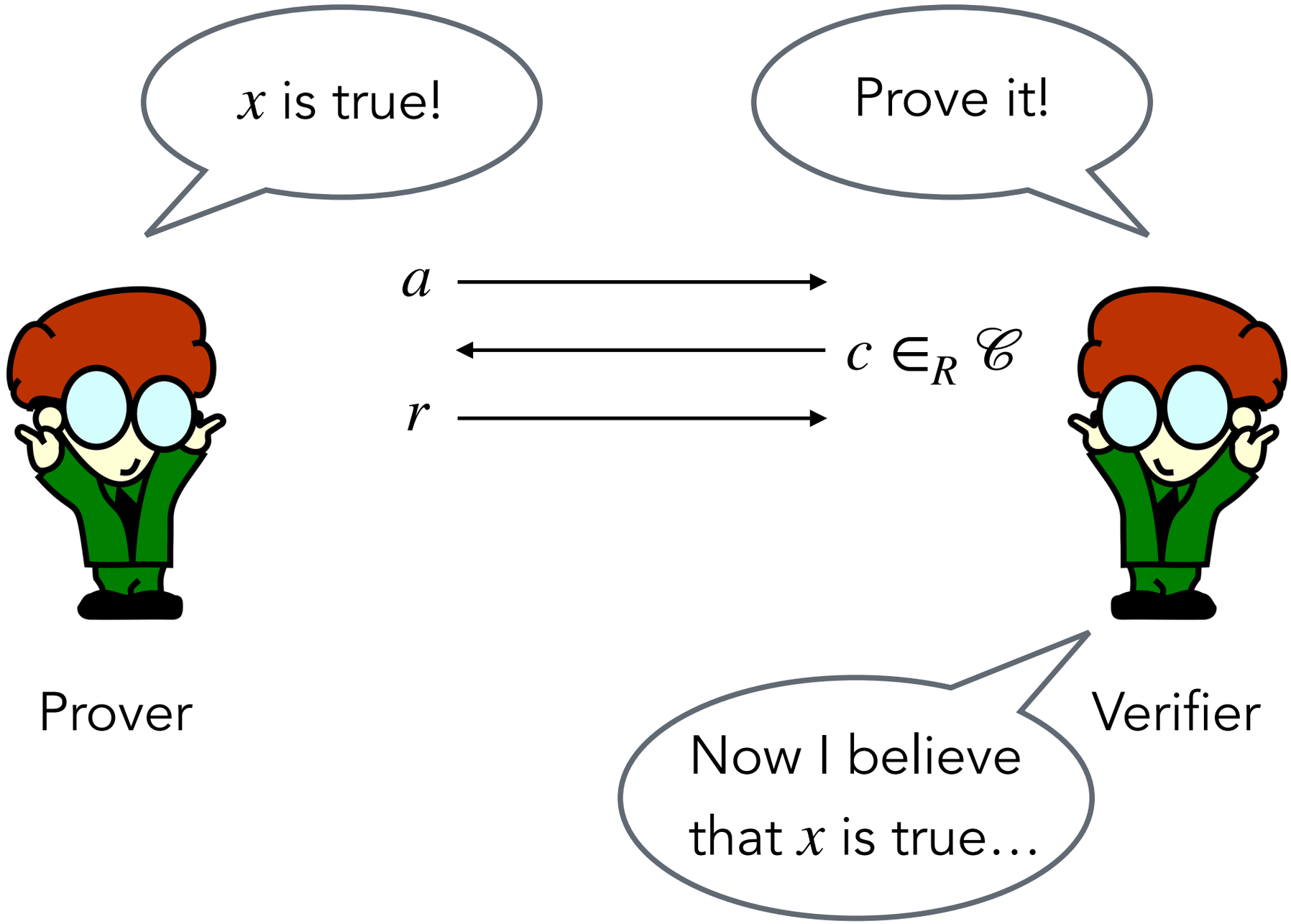
- Completeness
- Soundness
- Zero-knowledge
- Proof-of-knowledge
- …

} perfect/statistical/computational

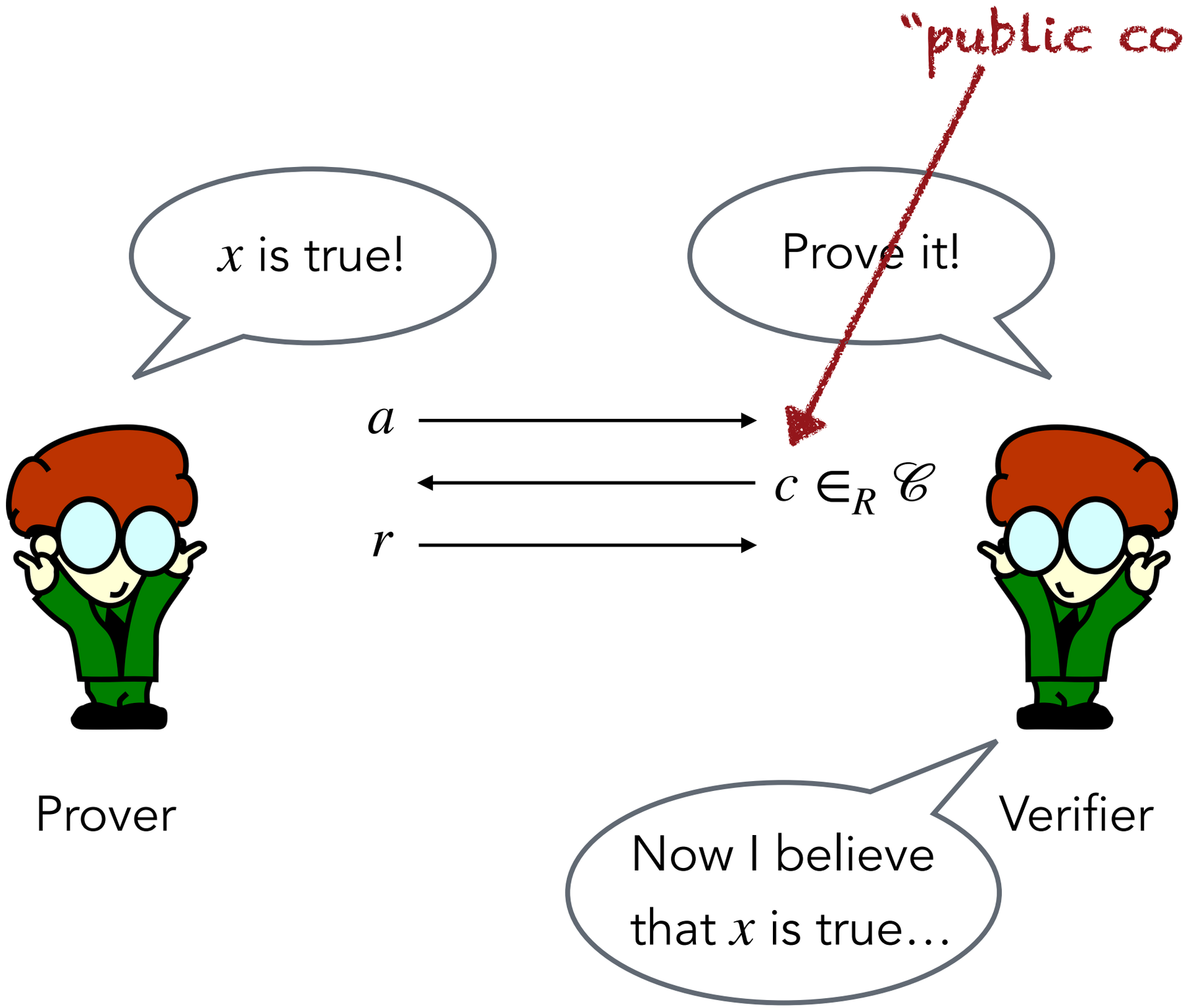
Can we do the same without interaction?

Yes, at least in some cases, using the Fiat Shamir transformation

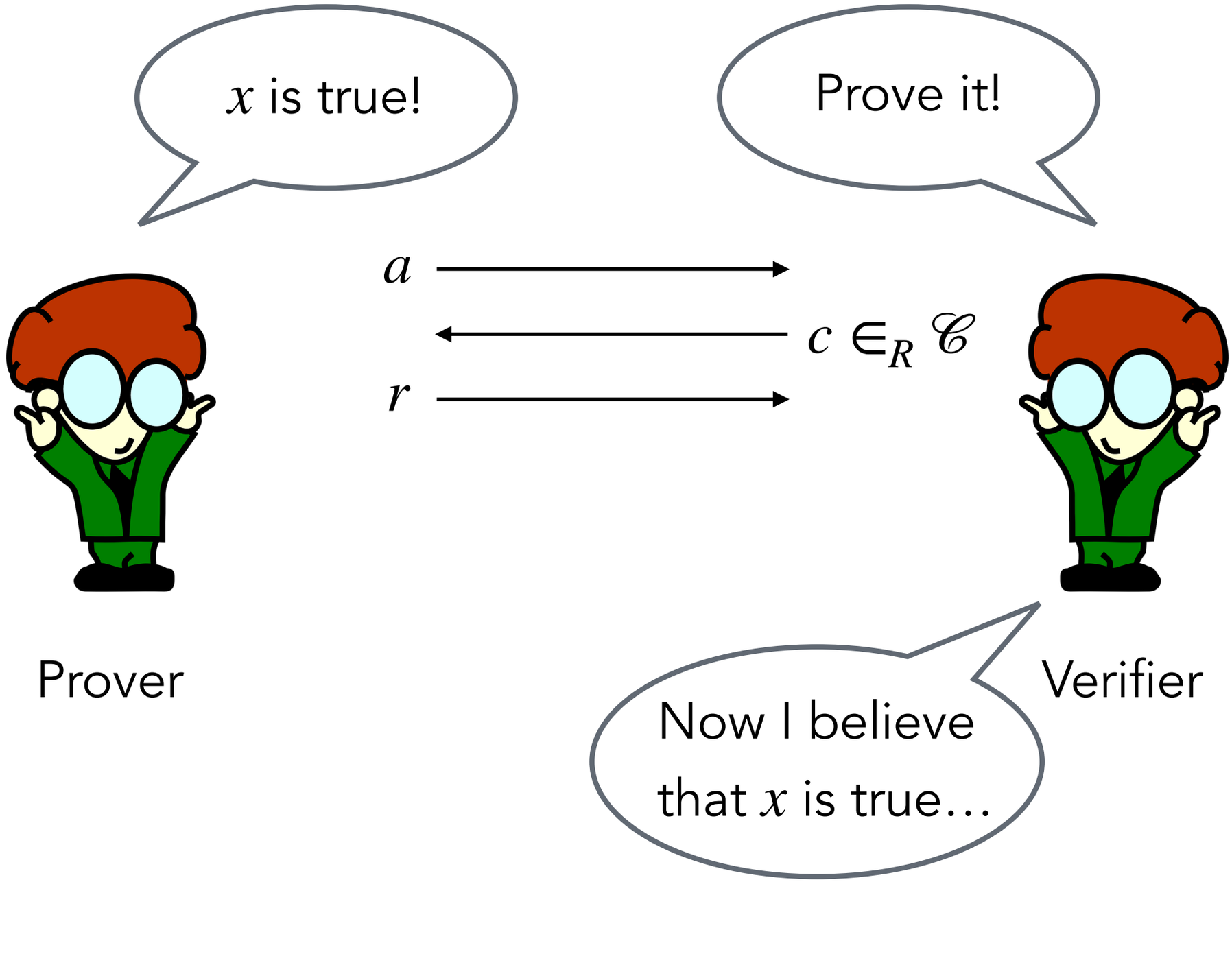
Σ-protocol


x is true!
Prove it!
a
$c \in_R \mathcal{C}$
r
Prover
Verifier
Now I believe that x is true…

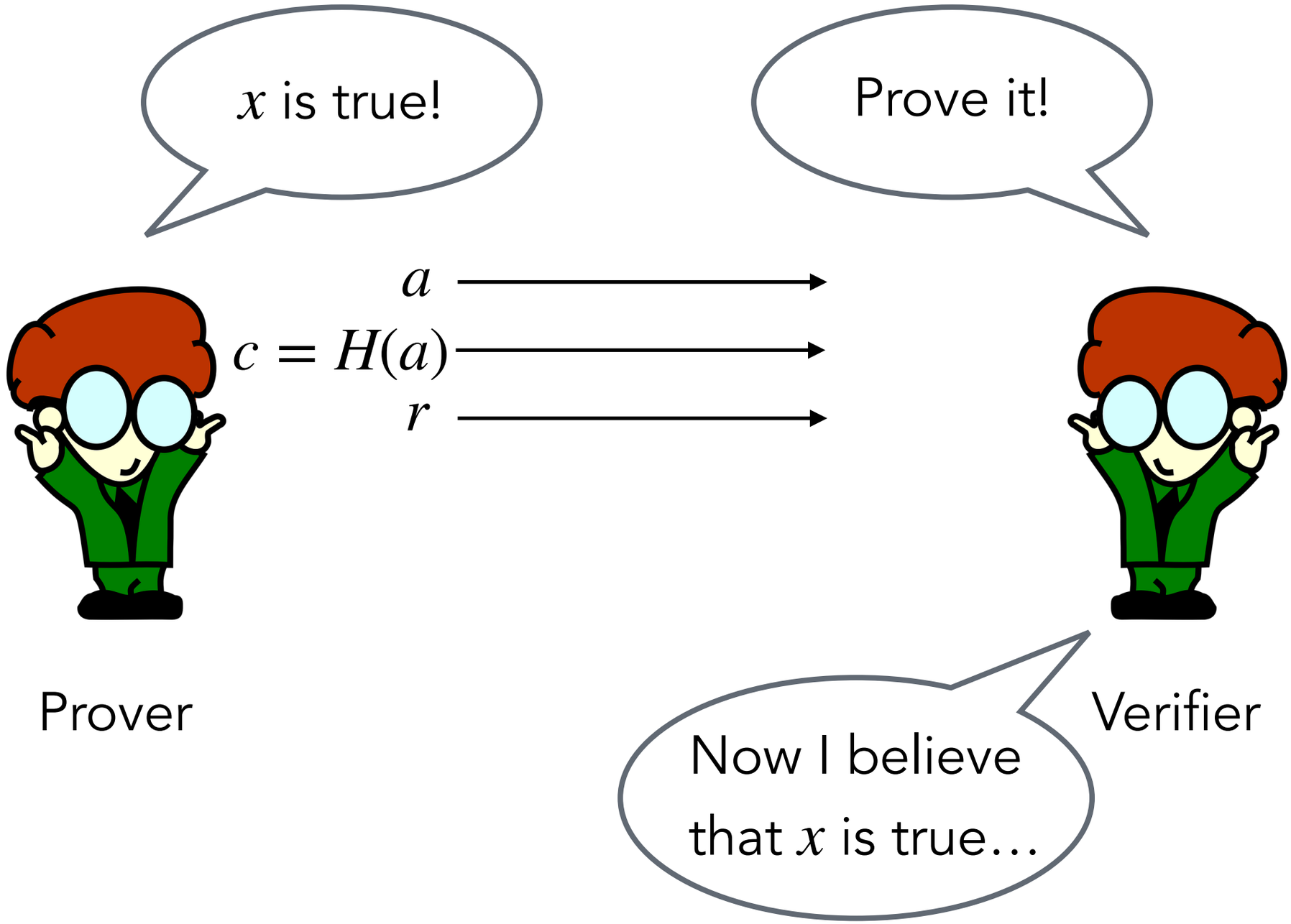
Σ-protocol


"public coin"
x is true!
Prove it!
a
$c \in_R \mathscr{C}$
r
Prover
Verifier
Now I believe that x is true…

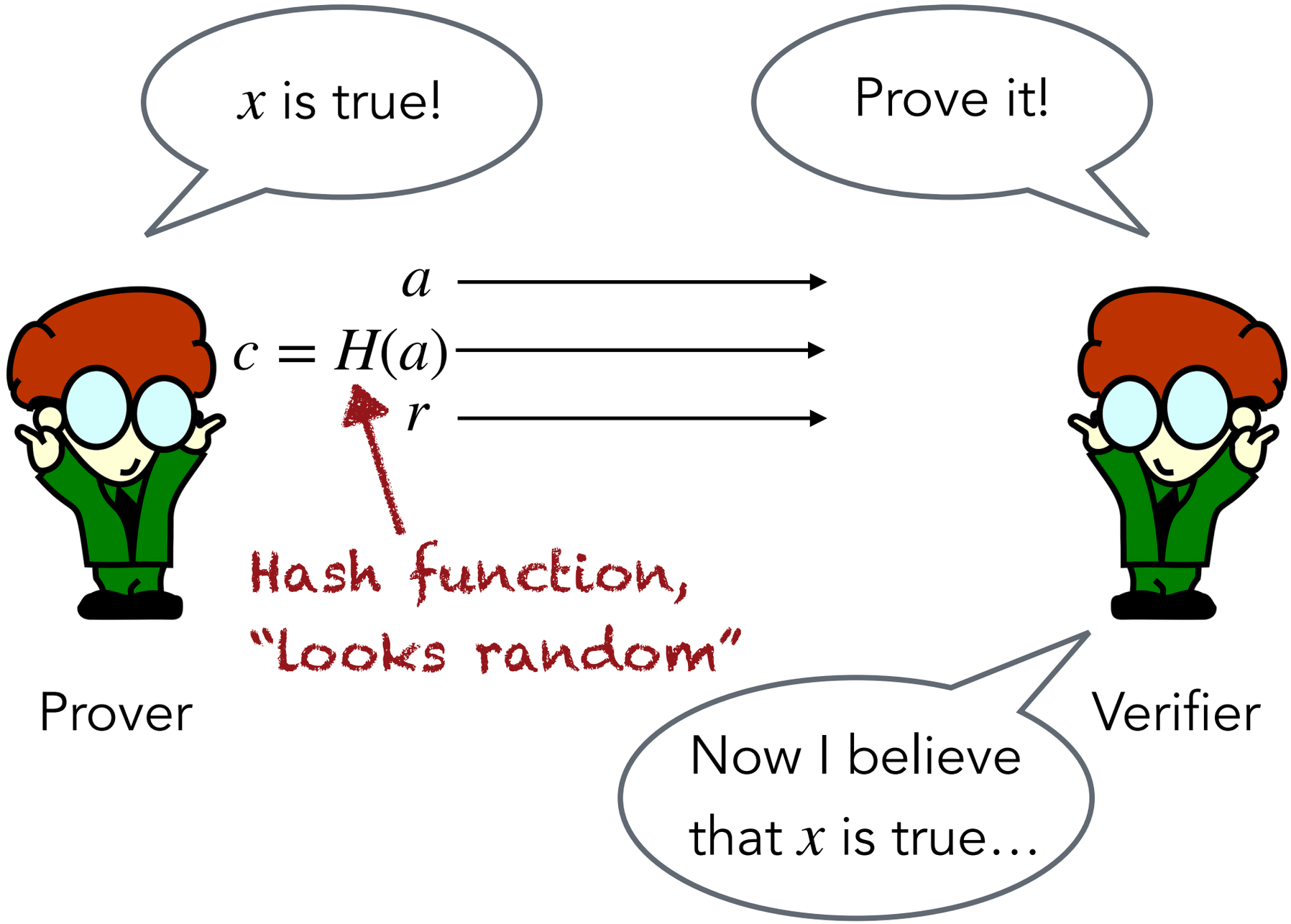
Fiat Shamir transformation



Fiat Shamir transformation



Fiat Shamir transformation



Fiat Shamir transformation

- Intractability of hash function replaces interaction

Fiat Shamir transformation

- Intractability of hash function replaces interaction
- Yields non-interactive proof system

Fiat Shamir transformation

- Intractability of hash function replaces interaction
- Yields non-interactive proof system
- Used for digital signature schemes

Fiat Shamir transformation

- Intractability of hash function replaces interaction
- Yields non-interactive proof system
- Used for digital signature schemes
- Preserves properties in the Random Oracle Model (ROM) (Pointcheval & Stern ‘00)

Fiat Shamir transformation

- Intractability of hash function replaces interaction
- Yields non-interactive proof system
- Used for digital signature schemes
- Preserves properties in the Random Oracle Model (ROM) (Pointcheval & Stern ‘00)

Pretend that hash function is random and everybody has oracle access

Fiat Shamir transformation

- Intractability of hash function replaces interaction
- Yields non-interactive proof system
- Used for digital signature schemes
- Preserves properties in the Random Oracle Model (ROM) (Pointcheval & Stern ‘00)

? What about the quantum ROM (QROM)?

Fiat Shamir transformation

- Intractability of hash function replaces interaction
- Yields non-interactive proof system
- Used for digital signature schemes
- Preserves properties in the Random Oracle Model (ROM) (Pointcheval & Stern ‘00)

? What about the quantum ROM (QROM)?

Unruh ‘17: The Fiat Shamir transformation preserves some security properties in the QROM if the underlying Σ-protocol is statistically sound.

Fiat Shamir transformation

- Intractability of hash function replaces interaction
- Yields non-interactive proof system
- Used for digital signature schemes
- Preserves properties in the Random Oracle Model (ROM) (Pointcheval & Stern ‘00)

? What about the quantum ROM (QROM)?

Unruh ‘17: The Fiat Shamir transformation preserves some security properties in the QROM if the underlying Σ-protocol is statistically sound.

Many cases important for post-quantum crypto still open.

2. Results

Our results

1. A general reduction for the Fiat Shamir transform in the QROM.

Our results

1. A general reduction for the Fiat Shamir transform in the QROM.

Theorem (Don, Fehr, M, Schaffner):
The Fiat Shamir transformation of a Σ-protocol inherits all its security properties in the QROM.

Our results

1. A general reduction for the Fiat Shamir transform in the QROM.

Theorem (Don, Fehr, M, Schaffner):
The Fiat Shamir transformation of a Σ-protocol inherits all its security properties in the QROM.

Concurrent work: Liu and Zhandry, less tight reduction.

Our results

1. A general reduction for the Fiat Shamir transform in the QROM.

> **Theorem (Don, Fehr, M, Schaffner):**
> The Fiat Shamir transformation of a Σ-protocol inherits all its security properties in the QROM.

Concurrent work: Liu and Zhandry, less tight reduction.

2. A novel criterion for the computational proof-of-knowledge property for sigma protocols (related to collapsingness)

Our results

1. A general reduction for the Fiat Shamir transform in the QROM.

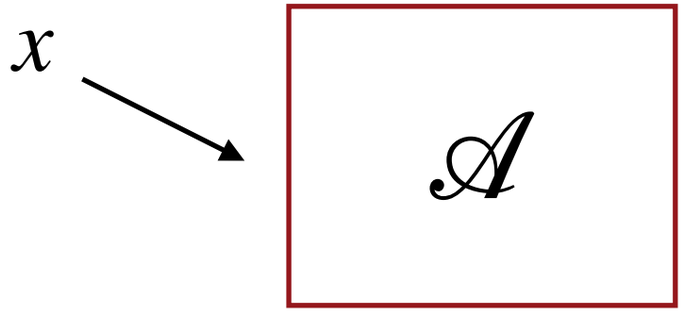
> **Theorem (Don, Fehr, M, Schaffner):**
> The Fiat Shamir transformation of a Σ-protocol inherits all its security properties in the QROM.

Concurrent work: Liu and Zhandry, less tight reduction.

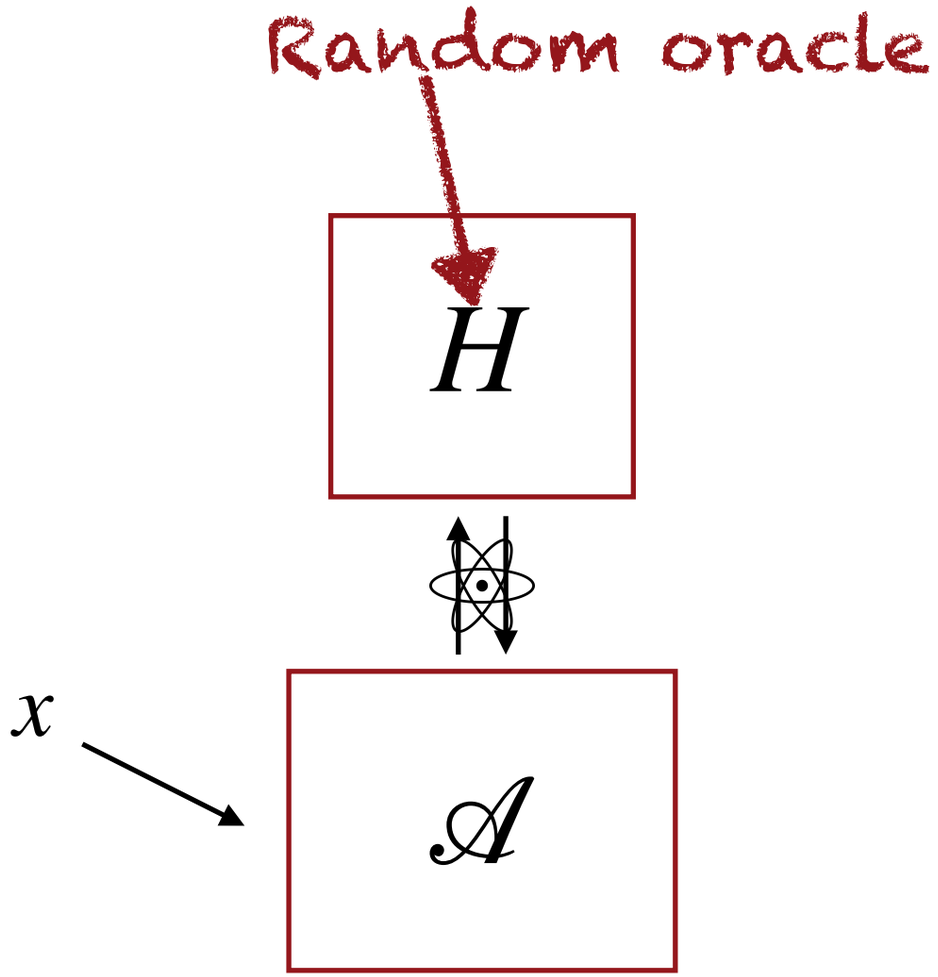
2. A novel criterion for the computational proof-of-knowledge property for sigma protocols (related to collapsingness)

The reduction

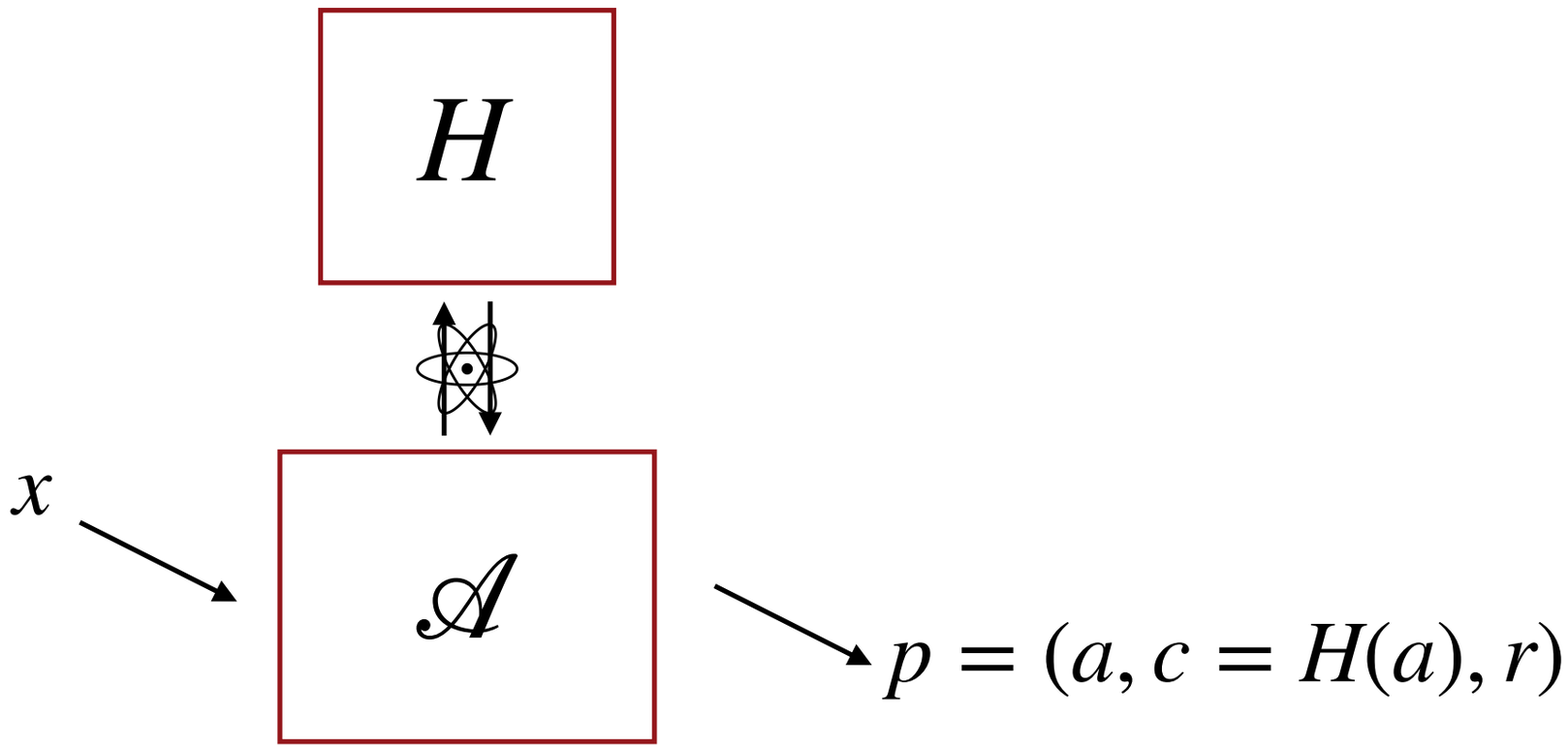
The reduction



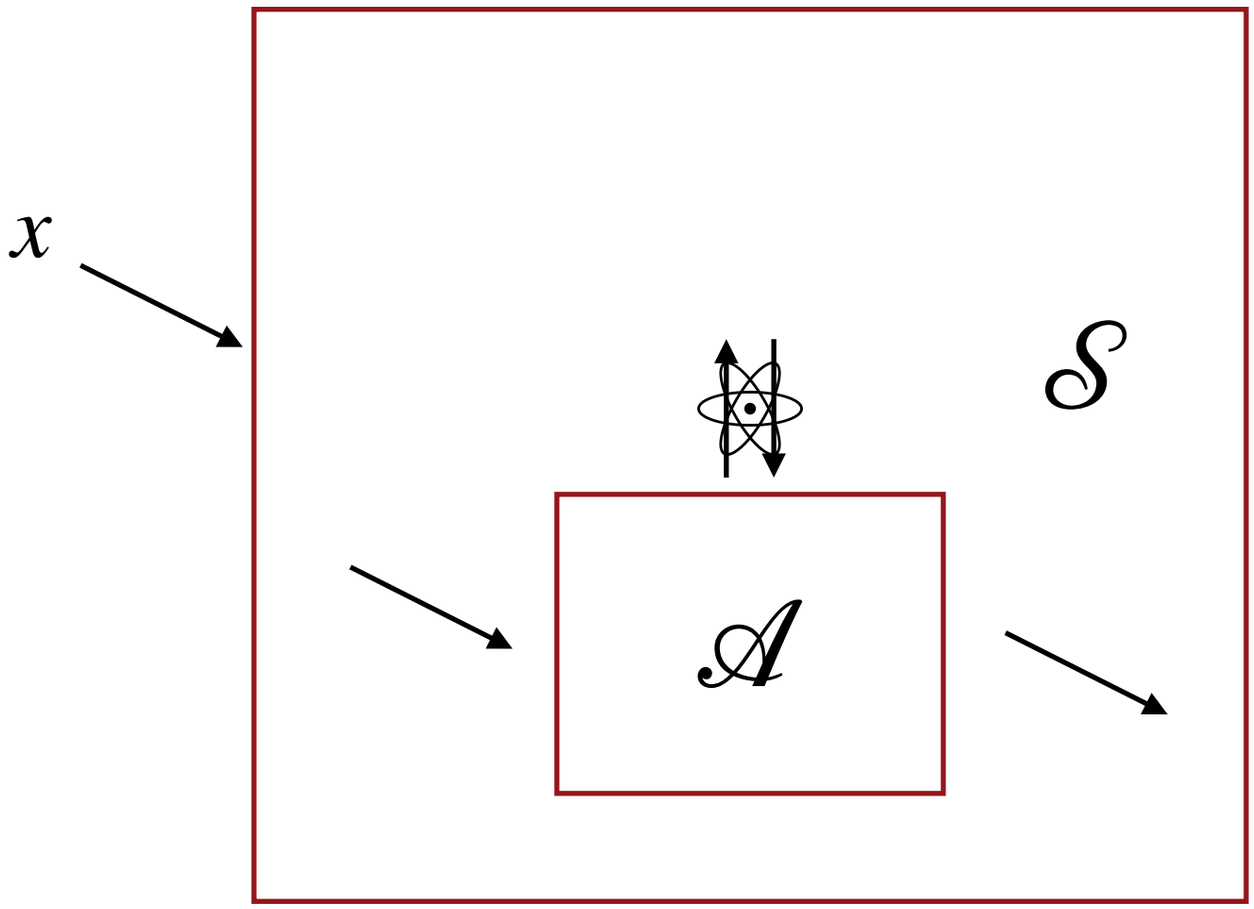
The reduction



The reduction

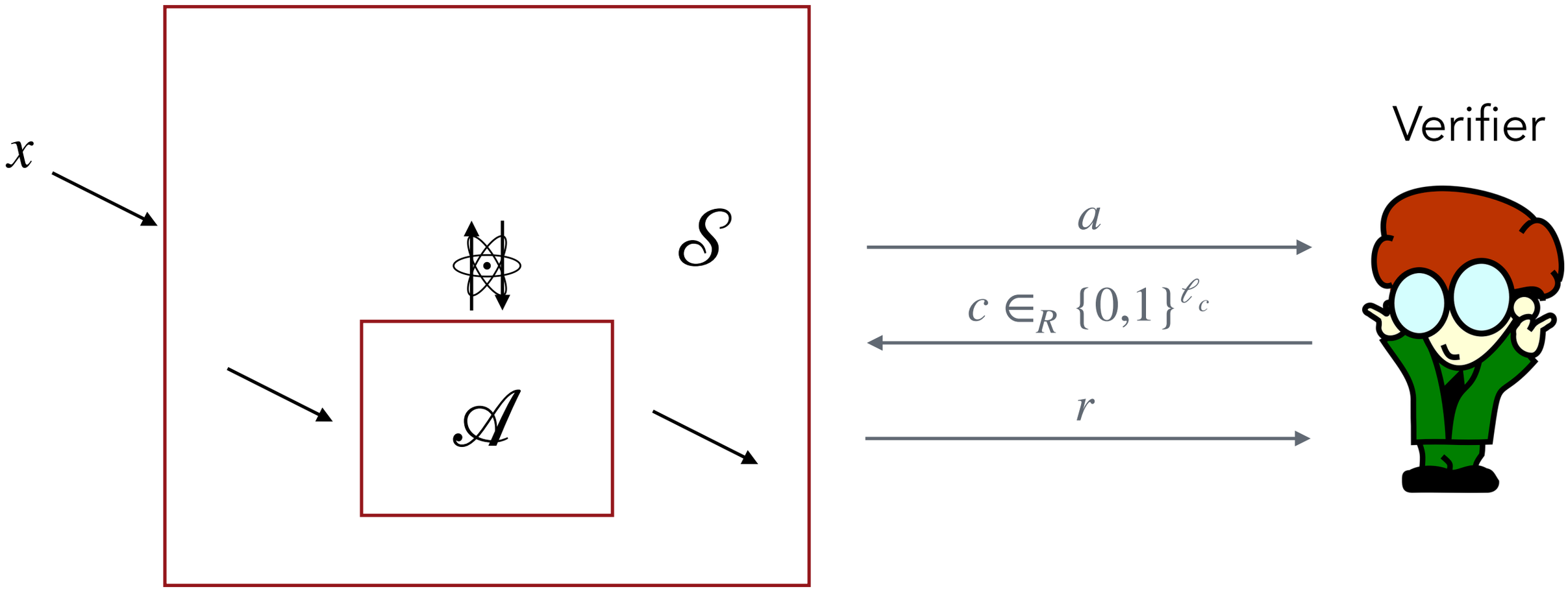


The reduction

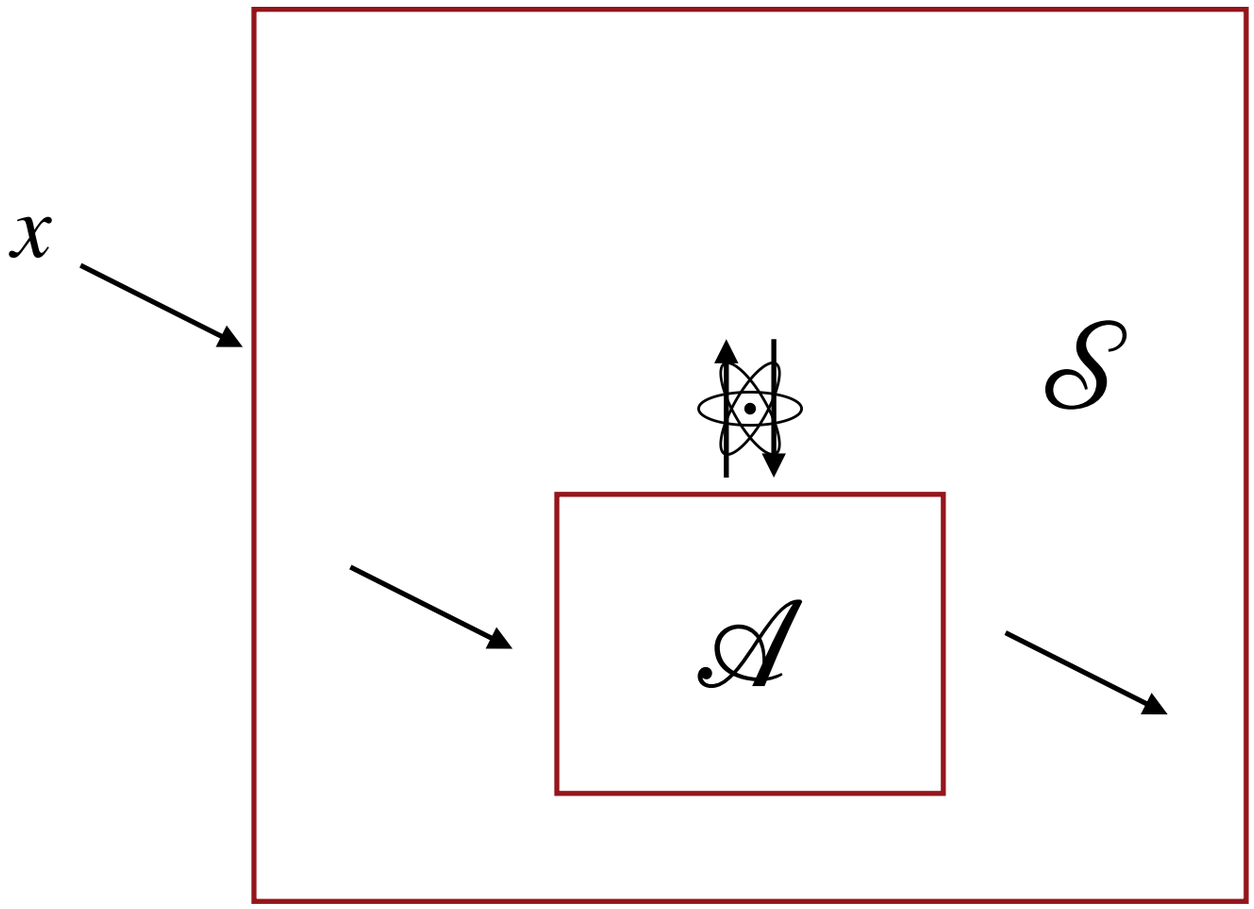


Verifier

The reduction

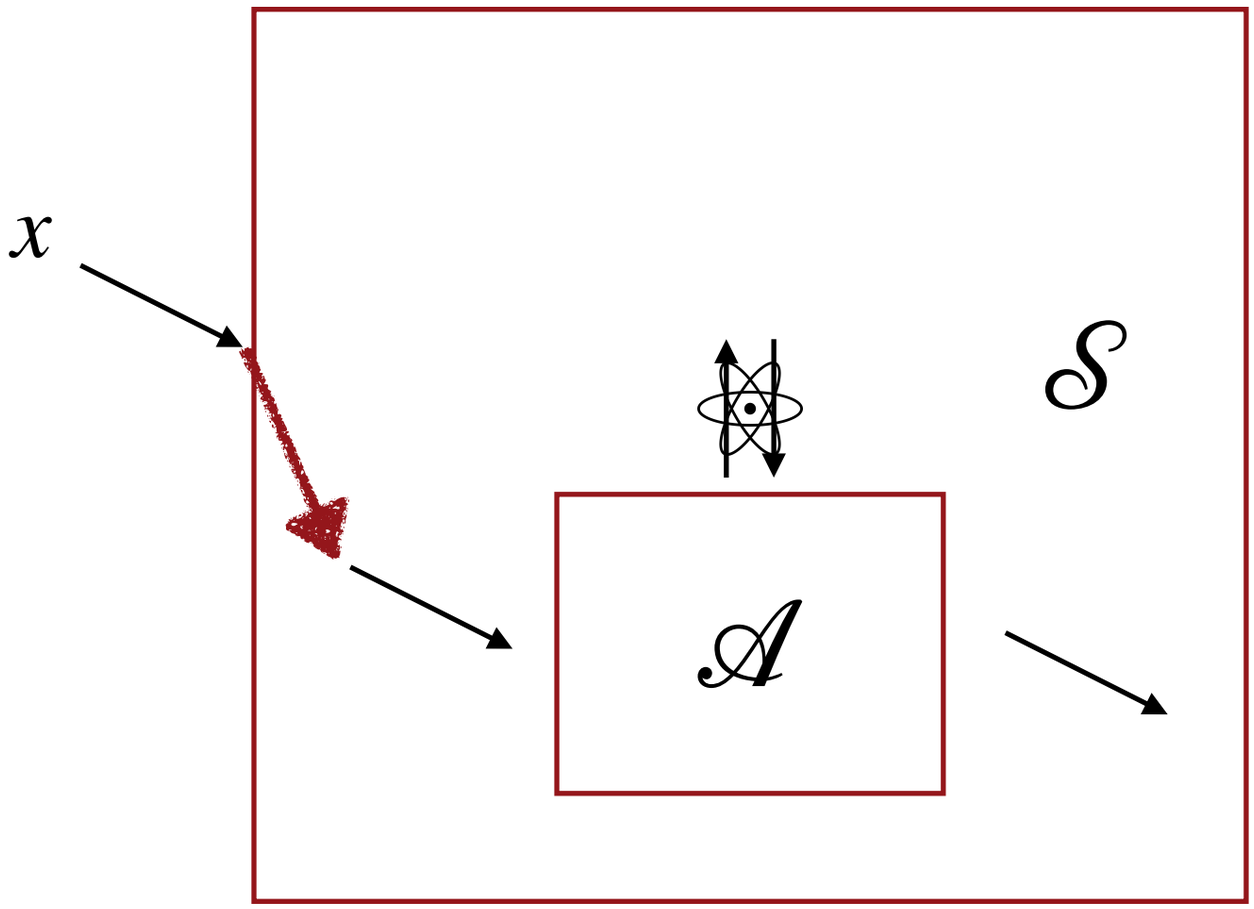


The reduction



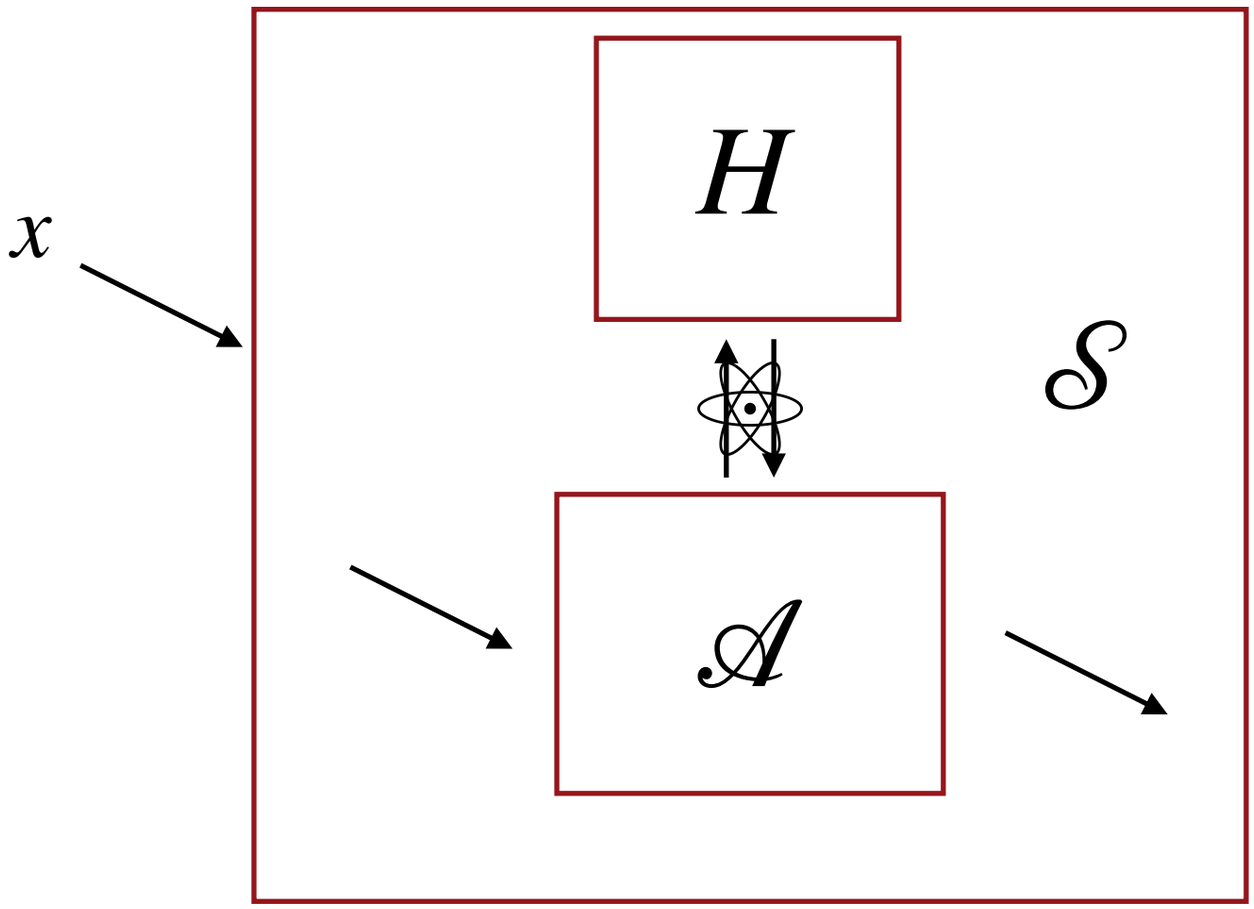
Verifier

The reduction



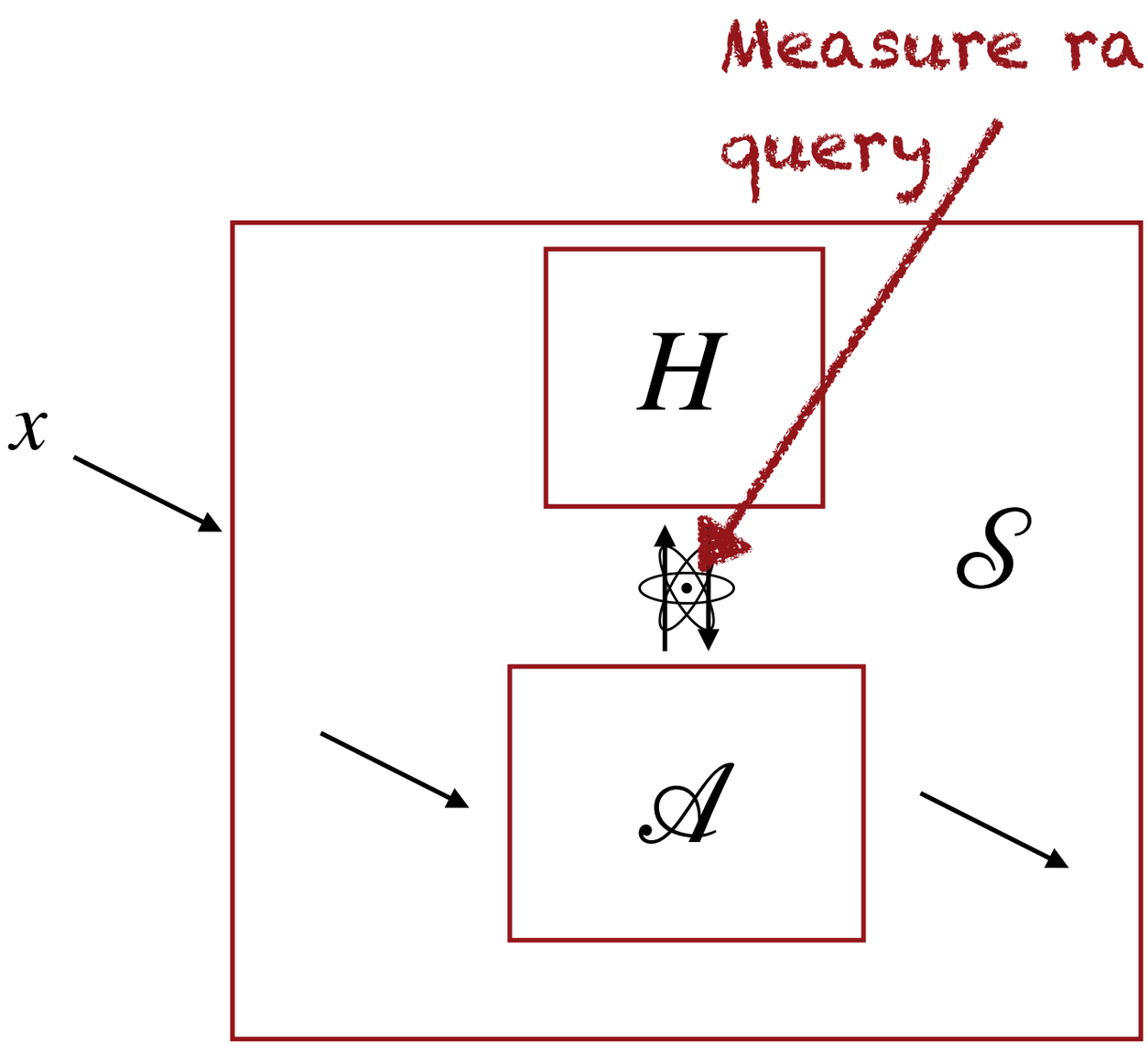
Verifier

The reduction



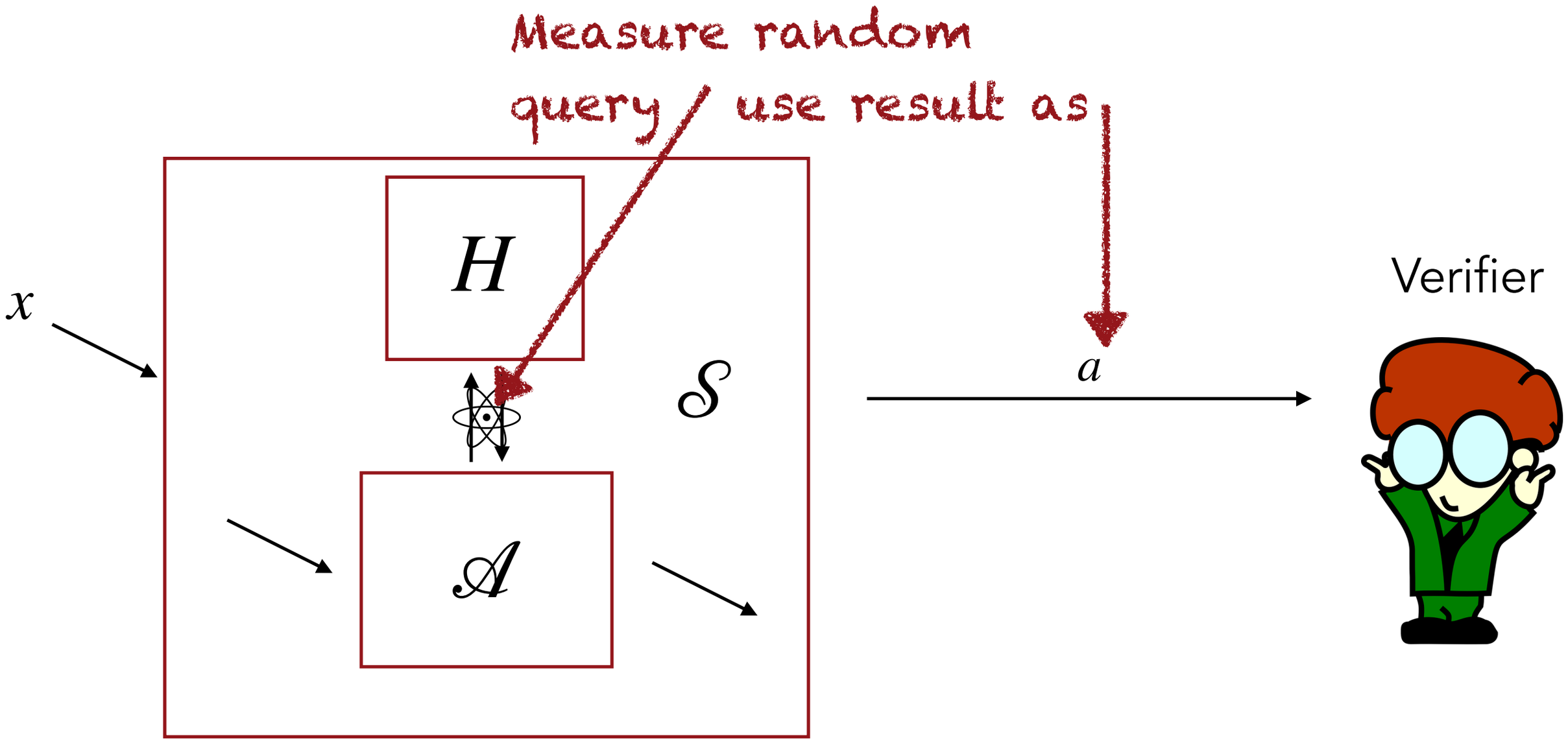
Verifier

The reduction

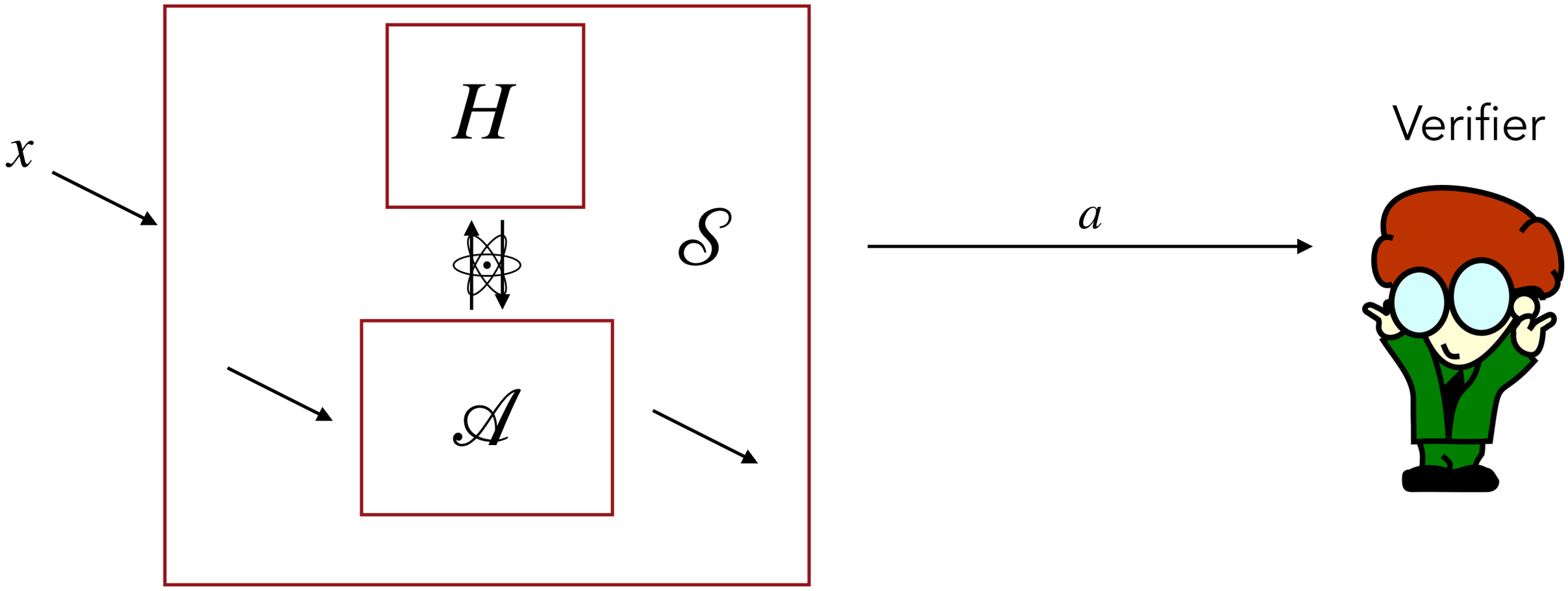


Verifier

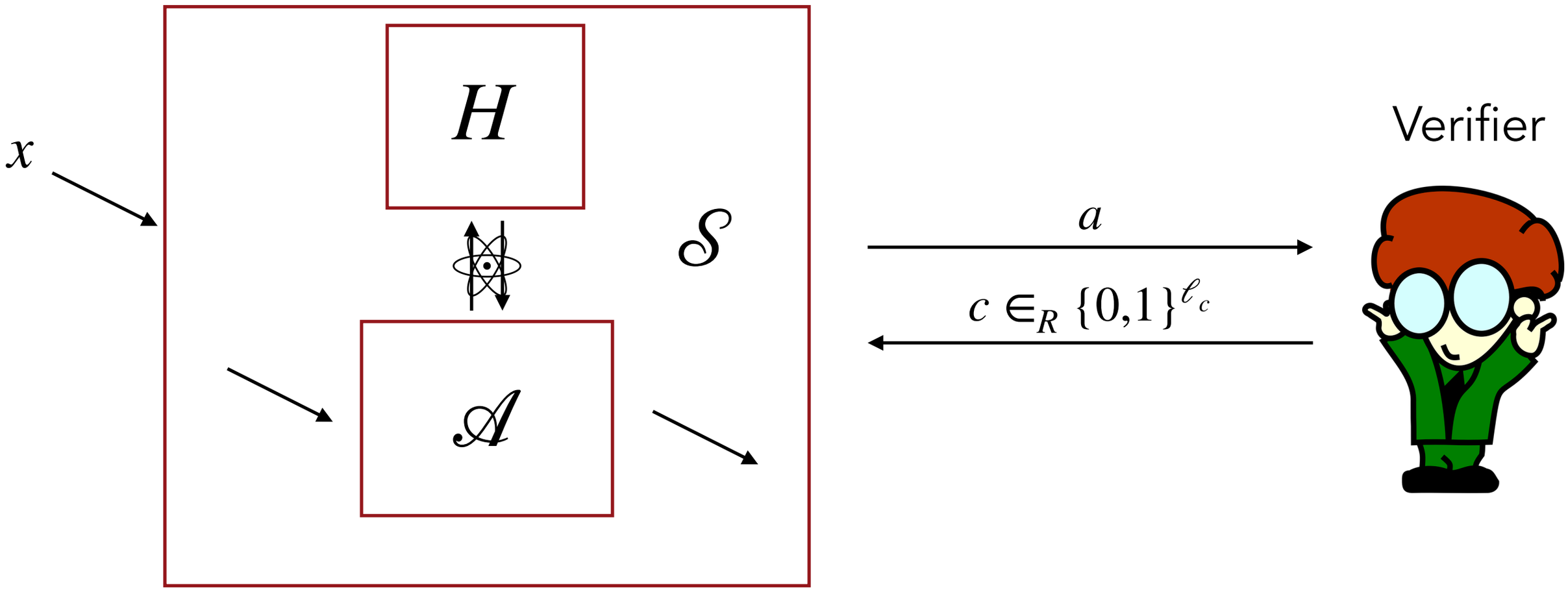
The reduction



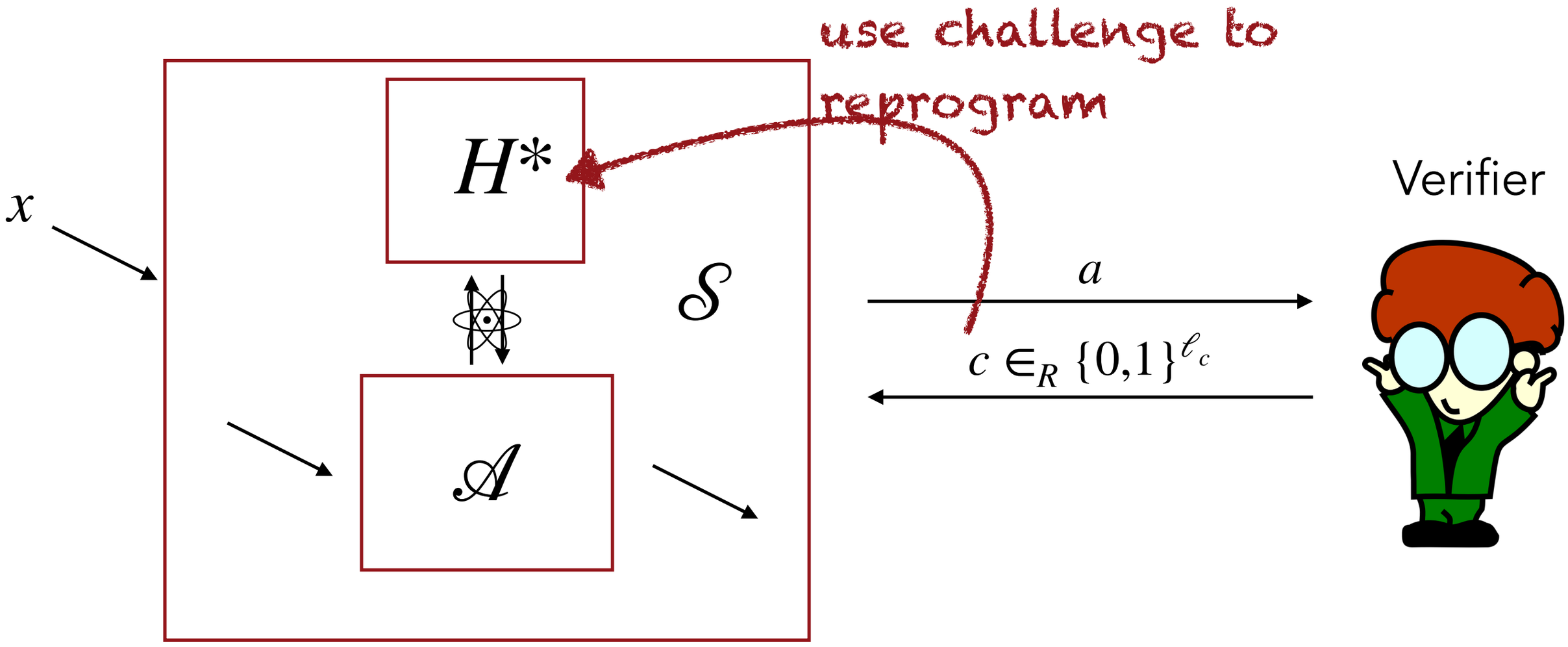
The reduction



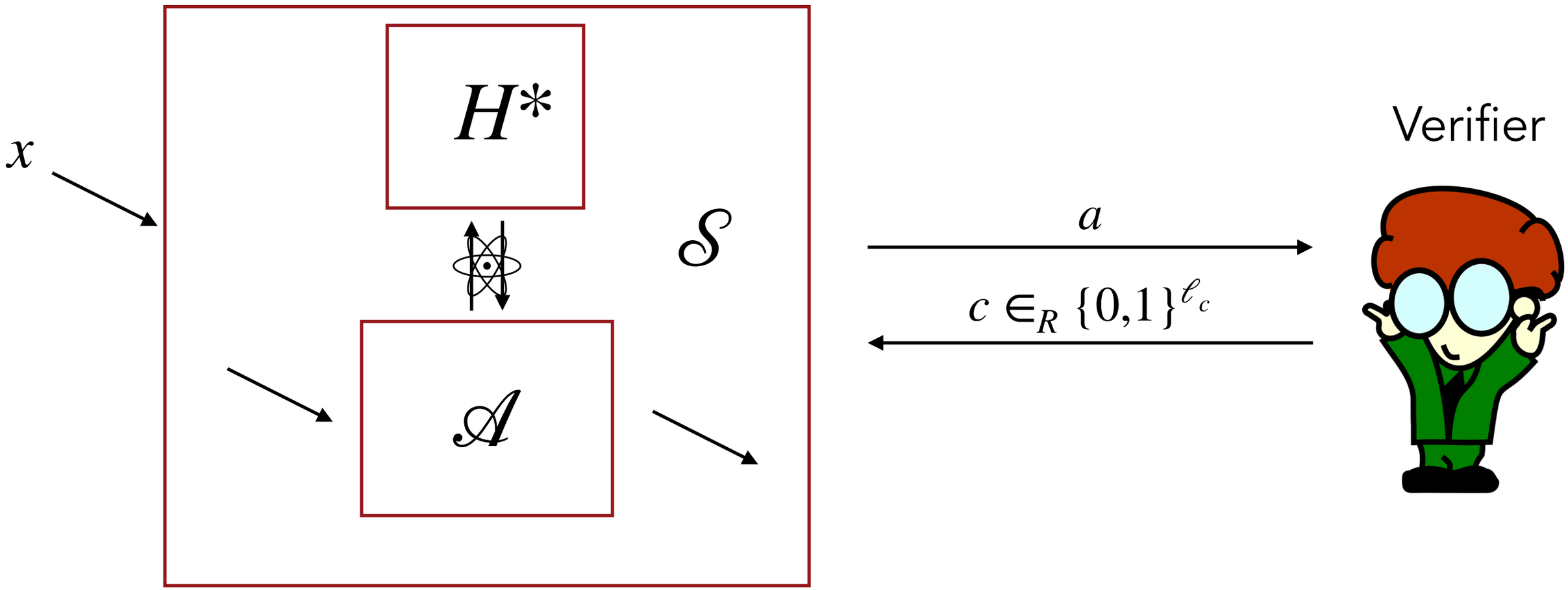
The reduction



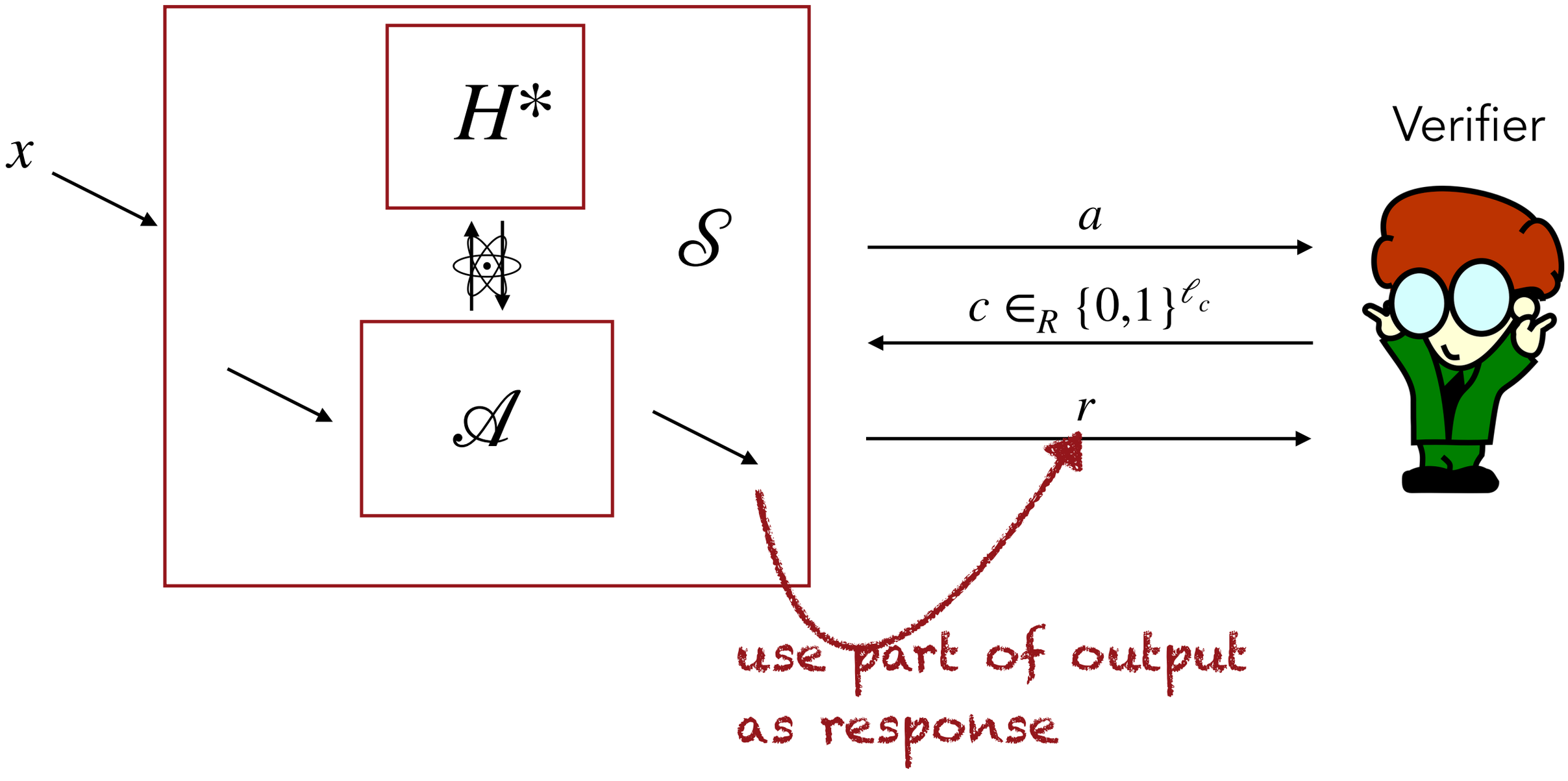
The reduction



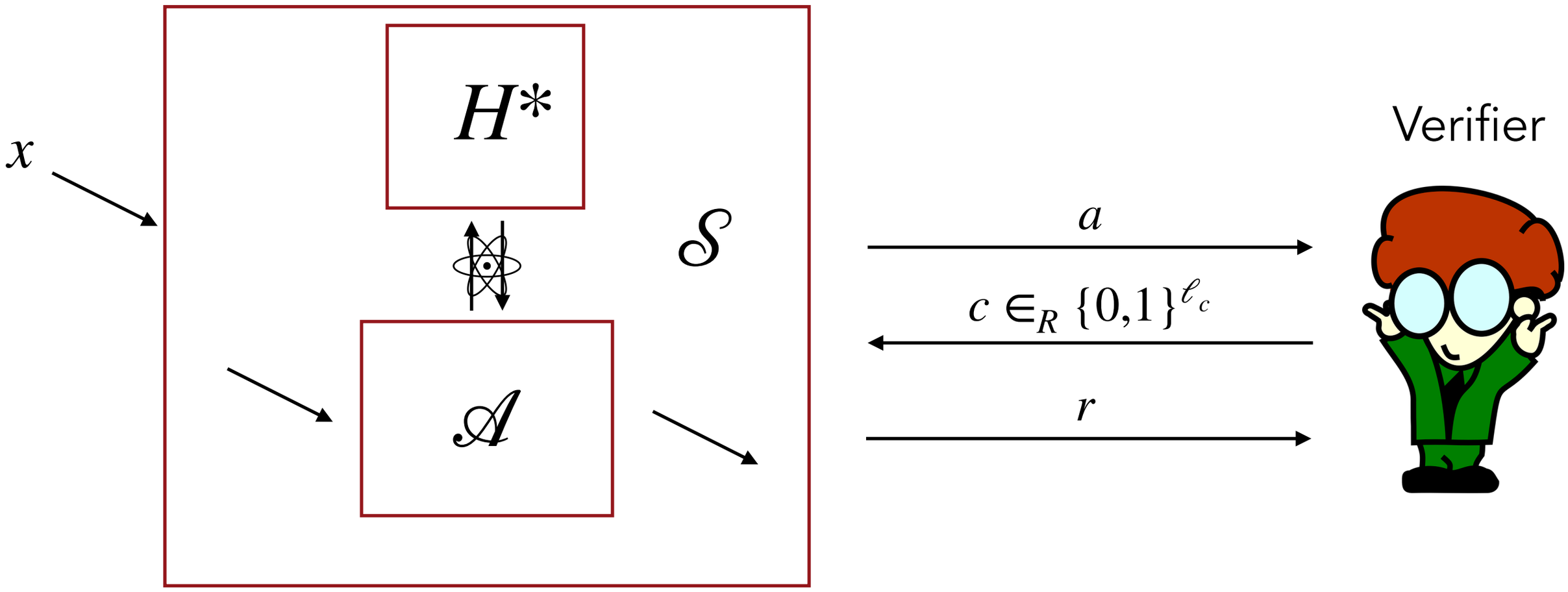
The reduction



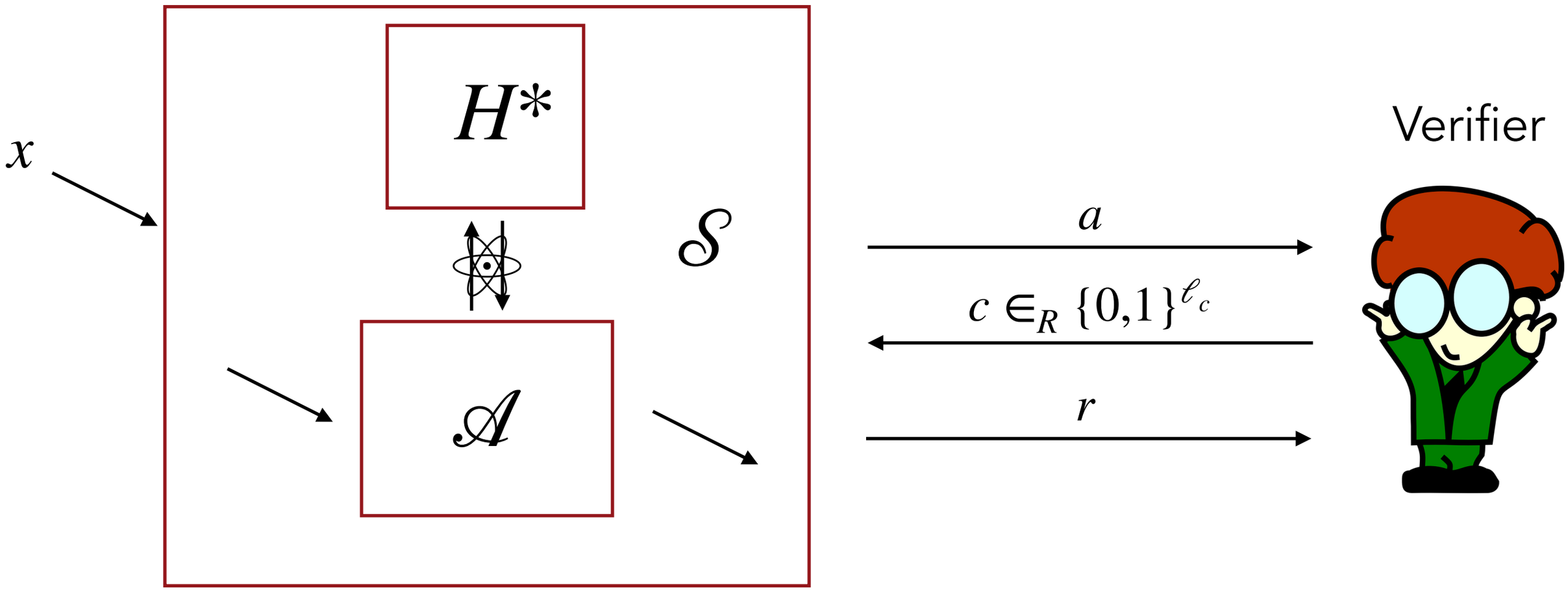
The reduction



The reduction

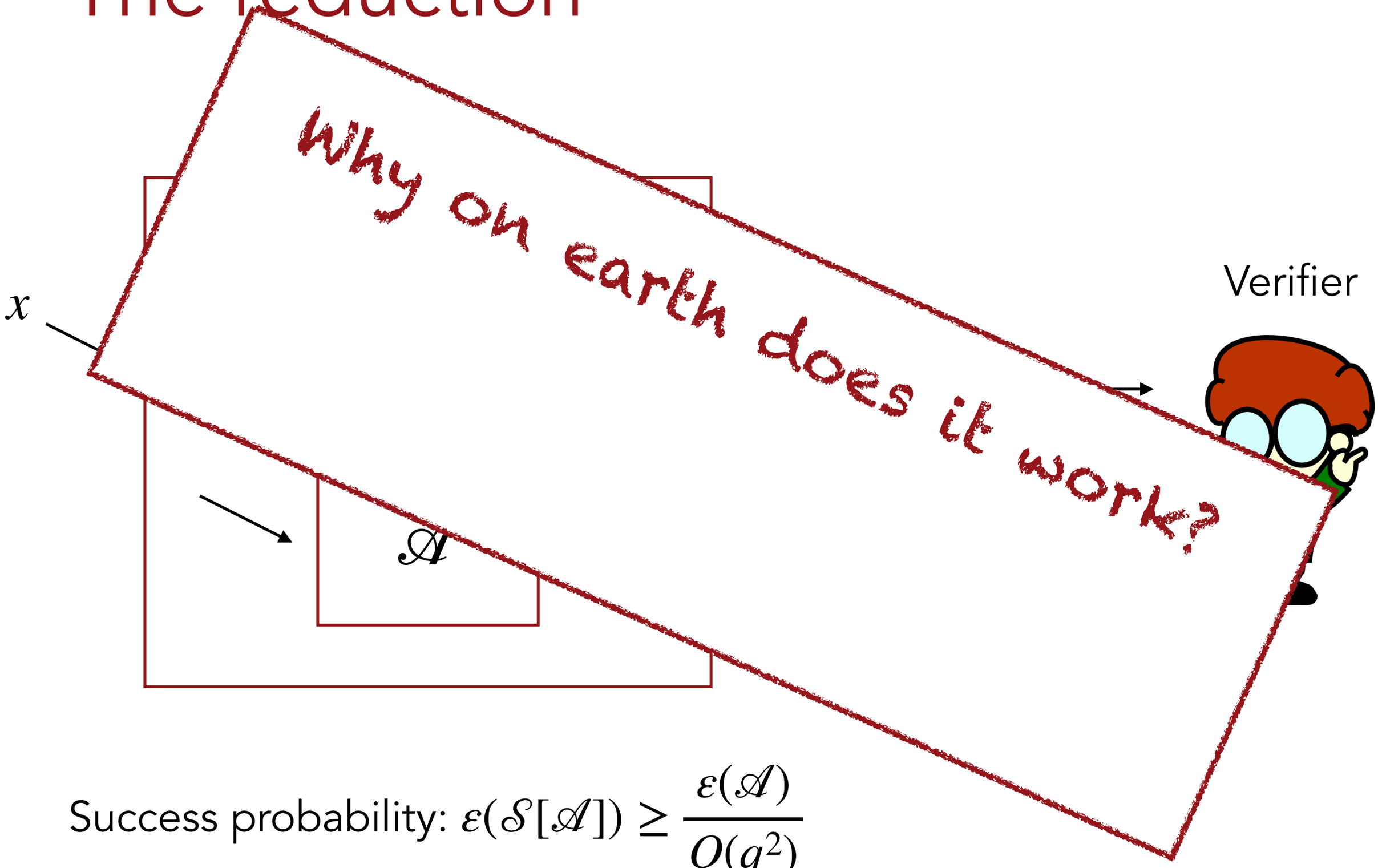


The reduction



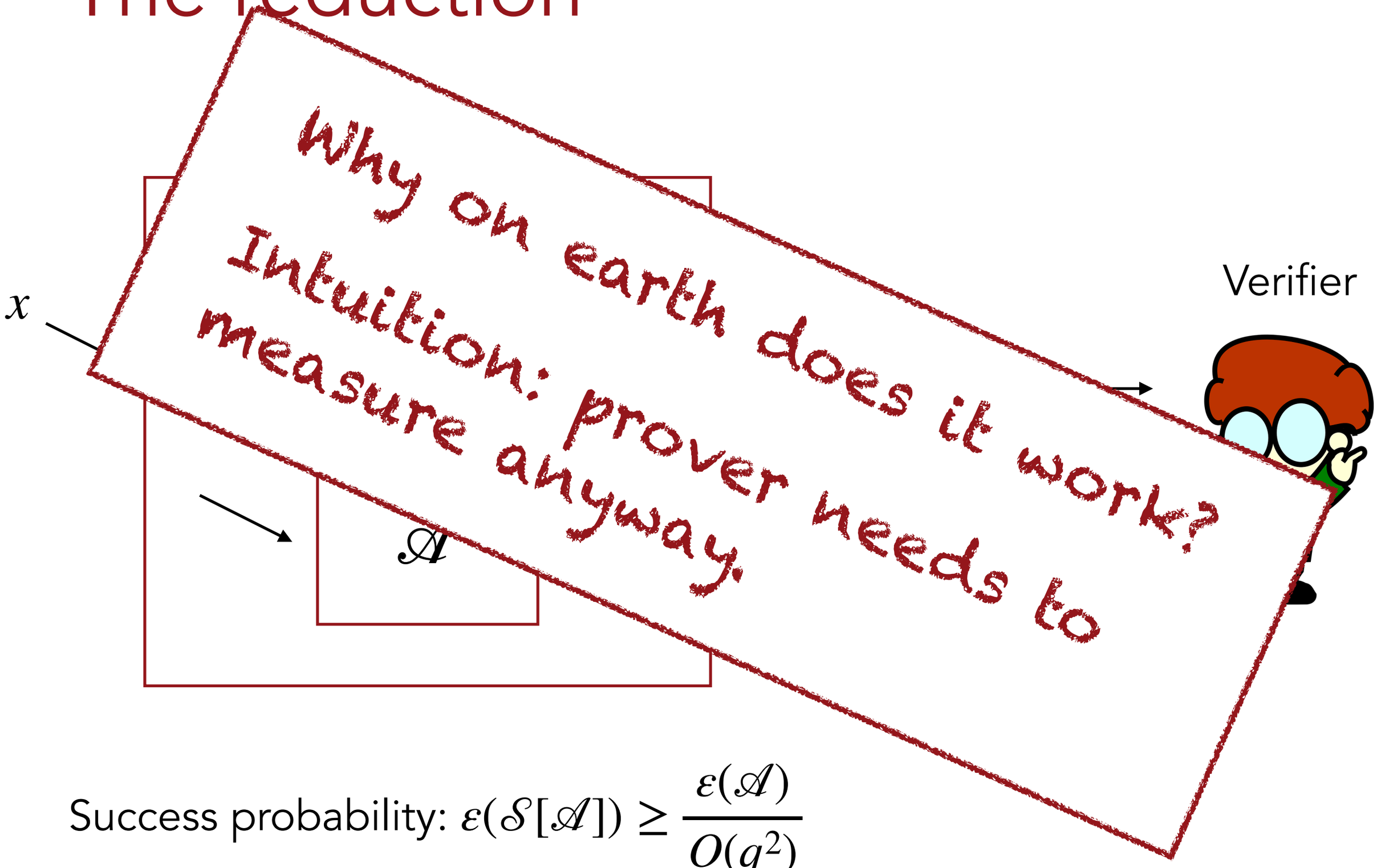
Success probability: $\varepsilon(\mathcal{S}[\mathcal{A}]) \geq \dfrac{\varepsilon(\mathcal{A})}{O(q^2)}$

The reduction



Success probability: $\varepsilon(\mathcal{S}[\mathscr{A}]) \geq \dfrac{\varepsilon(\mathscr{A})}{O(q^2)}$

The reduction



Success probability: $\varepsilon(\mathcal{S}[\mathcal{A}]) \geq \dfrac{\varepsilon(\mathcal{A})}{O(q^2)}$

Technique

Simplified picture: one query.

Technique

Simplified picture: one query.

$\mathcal{A}^H |\phi\rangle = U_2 O_H U_1 |\phi\rangle$ (without final measurement)

Technique

Simplified picture: one query.

$\mathcal{A}^H|\phi\rangle = U_2 O_H U_1 |\phi\rangle$ (without final measurement)

$H^*(x) = H(x)$ for $x \neq x_0$, $H^*(x_0)$ independently uniformly random

Technique

Simplified picture: one query.

$\mathcal{A}^H|\phi\rangle = U_2 O_H U_1 |\phi\rangle$ (without final measurement)

$H^*(x) = H(x)$ for $x \neq x_0$, $H^*(x_0)$ independently uniformly random

$\Rightarrow$ "$\mathcal{A}^H = \mathcal{A}^{H^*}$ unless $\mathcal{A}$ queries on x_0", i.e.

Technique

Simplified picture: one query.

$\mathcal{A}^H|\phi\rangle = U_2 O_H U_1 |\phi\rangle$ (without final measurement)

$H^*(x) = H(x)$ for $x \neq x_0$, $H^*(x_0)$ independently uniformly random

$\Rightarrow$ "$\mathcal{A}^H = \mathcal{A}^{H^*}$ unless $\mathcal{A}$ queries on x_0", i.e.

$$\mathcal{A}^{H^*}|\phi\rangle = \mathcal{A}^H|\phi\rangle + U_2 O_{H^*}|x_0\rangle\langle x_0|U_1|\phi\rangle - U_2 O_H|x_0\rangle\langle x_0|U_1|\phi\rangle \quad (*)$$

(à la BBBV)

Technique

Simplified picture: one query.

$\mathcal{A}^H|\phi\rangle = U_2 O_H U_1 |\phi\rangle$ (without final measurement)

$H^*(x) = H(x)$ for $x \neq x_0$, $H^*(x_0)$ independently uniformly random

$\Rightarrow$ "$\mathcal{A}^H = \mathcal{A}^{H^*}$ unless $\mathcal{A}$ queries on x_0", i.e.

$$\mathcal{A}^{H^*}|\phi\rangle = \mathcal{A}^H|\phi\rangle + U_2 O_{H^*}|x_0\rangle\langle x_0|U_1|\phi\rangle - U_2 O_H|x_0\rangle\langle x_0|U_1|\phi\rangle \quad (*)$$

(à la BBBV)

Successful $\mathcal{A}^{H^*}$ outputs $|x\rangle|H^*(x)\rangle$ for some x

Technique

Simplified picture: one query.

$\mathcal{A}^H|\phi\rangle = U_2 O_H U_1 |\phi\rangle$ (without final measurement)

$H^*(x) = H(x)$ for $x \neq x_0$, $H^*(x_0)$ independently uniformly random

$\Rightarrow$ "$\mathcal{A}^H = \mathcal{A}^{H^*}$ unless $\mathcal{A}$ queries on x_0", i.e.

$$\mathcal{A}^{H^*}|\phi\rangle = \mathcal{A}^H|\phi\rangle + U_2 O_{H^*}|x_0\rangle\langle x_0|U_1|\phi\rangle - U_2 O_H|x_0\rangle\langle x_0|U_1|\phi\rangle \quad (*)$$

(à la BBBV)

Successful $\mathcal{A}^{H^*}$ outputs $|x\rangle|H^*(x)\rangle$ for some x

Plan: 1. Use (*) to test whether $\mathcal{A}^{H^*}$ outputs $|x_0\rangle|H^*(x_0)\rangle$

Technique

Simplified picture: one query.

$\mathcal{A}^H|\phi\rangle = U_2 O_H U_1 |\phi\rangle$ (without final measurement)

$H^*(x) = H(x)$ for $x \neq x_0$, $H^*(x_0)$ independently uniformly random

$\Rightarrow$ "$\mathcal{A}^H = \mathcal{A}^{H^*}$ unless $\mathcal{A}$ queries on x_0", i.e.

$$\mathcal{A}^{H^*}|\phi\rangle = \mathcal{A}^H|\phi\rangle + U_2 O_{H^*}|x_0\rangle\langle x_0|U_1|\phi\rangle - U_2 O_H|x_0\rangle\langle x_0|U_1|\phi\rangle \quad (*)$$

(à la BBBV)

Successful $\mathcal{A}^{H^*}$ outputs $|x\rangle|H^*(x)\rangle$ for some x

Plan: 1. Use (*) to test whether $\mathcal{A}^{H^*}$ outputs $|x_0\rangle|H^*(x_0)\rangle$

2. Interpret RHS as algorithm

Technique

$$\mathcal{A}^{H^*}|\phi\rangle = \mathcal{A}^{H}|\phi\rangle + U_2 O_{H^*}|x_0\rangle\langle x_0|U_1|\phi\rangle - U_2 O_H|x_0\rangle\langle x_0|U_1|\phi\rangle \text{ (*)}$$

Plan: 1. Use (*) to test whether $\mathcal{A}^{H^*}$ outputs $|x_0\rangle|H^*(x_0)\rangle$

2. Interpret RHS as algorithm

Technique

$$\mathscr{A}^{H^*}|\phi\rangle = \mathscr{A}^{H}|\phi\rangle + U_2 O_{H^*}|x_0\rangle\langle x_0|U_1|\phi\rangle - U_2 O_H|x_0\rangle\langle x_0|U_1|\phi\rangle \text{ (*)}$$

Plan: 1. Use (*) to test whether $\mathscr{A}^{H^*}$ outputs $|x_0\rangle|H^*(x_0)\rangle$

2. Interpret RHS as algorithm

$$\langle x_0|\langle H^*(x_0)|\mathscr{A}^{H^*}|\phi\rangle = \langle x_0|\langle H^*(x_0)|\mathscr{A}^{H}|\phi\rangle$$

$$+\langle x_0|\langle H^*(x_0)|U_2 O_{H^*}|x_0\rangle\langle x_0|U_1|\phi\rangle - \langle x_0|\langle H^*(x_0)|U_2 O_H|x_0\rangle\langle x_0|U_1|\phi\rangle$$

Technique

$$\mathscr{A}^{H}|\phi\rangle = \mathscr{A}^{H^*}|\phi\rangle + U_2 O_H |x_0\rangle\langle x_0| U_1 |\phi\rangle - U_2 O_{H^*} |x_0\rangle\langle x_0| U_1 |\phi\rangle \quad (*)$$

Plan: 1. Use (*) to test whether $\mathscr{A}^{H}$ outputs $|x_0\rangle|H(x_0)\rangle$

2. Interpret RHS as algorithm

$$\| \langle x_0| \langle H^*(x_0)| \mathscr{A}^{H^*} |\phi\rangle \|_2 \leq \| \langle x_0| \langle H^*(x_0)| \mathscr{A}^{H} |\phi\rangle \|_2$$

$$+ \| \langle x_0| \langle H^*(x_0)| U_2 O_{H^*} |x_0\rangle\langle x_0| U_1 |\phi\rangle \|_2 + \| \langle x_0| \langle H^*(x_0)| U_2 O_{H} |x_0\rangle\langle x_0| U_1 |\phi\rangle \|_2$$

Technique

$$\mathscr{A}^{H}|\phi\rangle = \mathscr{A}^{H^*}|\phi\rangle + U_2 O_H |x_0\rangle\langle x_0| U_1 |\phi\rangle - U_2 O_{H^*} |x_0\rangle\langle x_0| U_1 |\phi\rangle \quad (*)$$

Plan: 1. Use (*) to test whether $\mathscr{A}^{H}$ outputs $|x_0\rangle|H(x_0)\rangle$

2. Interpret RHS as algorithm

$$\| \langle x_0| \langle H^*(x_0)| \mathscr{A}^{H^*} |\phi\rangle \|_2 \leq \| \langle x_0| \langle H^*(x_0)| \mathscr{A}^{H} |\phi\rangle \|_2$$

$$+ \| \langle x_0| \langle H^*(x_0)| U_2 O_{H^*} |x_0\rangle\langle x_0| U_1 |\phi\rangle \|_2 + \| \langle x_0| \langle H^*(x_0)| U_2 O_{H} |x_0\rangle\langle x_0| U_1 |\phi\rangle \|_2$$

Small even after summing over x_0

Technique

$$\mathscr{A}^{H}|\phi\rangle = \mathscr{A}^{H^*}|\phi\rangle + U_2 O_H |x_0\rangle\langle x_0| U_1 |\phi\rangle - U_2 O_{H^*} |x_0\rangle\langle x_0| U_1 |\phi\rangle \quad (*)$$

Plan: 1. Use (*) to test whether $\mathscr{A}^{H}$ outputs $|x_0\rangle|H(x_0)\rangle$

2. Interpret RHS as algorithm

$$\| \langle x_0| \langle H^*(x_0)| \mathscr{A}^{H^*} |\phi\rangle \|_2 \leq \| \langle x_0| \langle H^*(x_0)| \mathscr{A}^{H} |\phi\rangle \|_2$$

$$+ \| \langle x_0| \langle H^*(x_0)| U_2 O_{H^*} |x_0\rangle\langle x_0| U_1 |\phi\rangle \|_2 + \| \langle x_0| \langle H^*(x_0)| U_2 O_{H} |x_0\rangle\langle x_0| U_1 |\phi\rangle \|_2$$

Measure query, outcome x_0, reprogram before answering

Technique

$$\mathscr{A}^{H}|\phi\rangle = \mathscr{A}^{H^*}|\phi\rangle + U_2 O_H |x_0\rangle\langle x_0| U_1 |\phi\rangle - U_2 O_{H^*} |x_0\rangle\langle x_0| U_1 |\phi\rangle \quad (*)$$

Plan: 1. Use (*) to test whether $\mathscr{A}^{H}$ outputs $|x_0\rangle|H(x_0)\rangle$

2. Interpret RHS as algorithm

$$\| \langle x_0| \langle H^*(x_0)| \mathscr{A}^{H^*} |\phi\rangle \|_2 \leq \| \langle x_0| \langle H^*(x_0)| \mathscr{A}^{H} |\phi\rangle \|_2$$

$$+ \| \langle x_0| \langle H^*(x_0)| U_2 O_{H^*} |x_0\rangle\langle x_0| U_1 |\phi\rangle \|_2 + \| \langle x_0| \langle H^*(x_0)| U_2 O_{H} |x_0\rangle\langle x_0| U_1 |\phi\rangle \|_2$$

Measure query, outcome x_0, reprogram after answering

Technique

$$\mathscr{A}^{H}|\phi\rangle = \mathscr{A}^{H^*}|\phi\rangle + U_2 O_H |x_0\rangle\langle x_0| U_1 |\phi\rangle - U_2 O_{H^*} |x_0\rangle\langle x_0| U_1 |\phi\rangle \quad (*)$$

Plan: 1. Use (*) to test whether $\mathscr{A}^{H}$ outputs $|x_0\rangle|H(x_0)\rangle$

2. Interpret RHS as algorithm

$$\| \langle x_0| \langle H^*(x_0)| \mathscr{A}^{H^*} |\phi\rangle \|_2 \leq \| \langle x_0| \langle H^*(x_0)| \mathscr{A}^{H} |\phi\rangle \|_2$$

$$+ \| \langle x_0| \langle H^*(x_0)| U_2 O_{H^*} |x_0\rangle\langle x_0| U_1 |\phi\rangle \|_2 + \| \langle x_0| \langle H^*(x_0)| U_2 O_{H} |x_0\rangle\langle x_0| U_1 |\phi\rangle \|_2$$

Technique

$$\mathcal{A}^{H}|\phi\rangle = \mathcal{A}^{H^*}|\phi\rangle + U_2 O_H |x_0\rangle\langle x_0| U_1 |\phi\rangle - U_2 O_{H^*} |x_0\rangle\langle x_0| U_1 |\phi\rangle \quad (*)$$

Plan: 1. Use (*) to test whether $\mathcal{A}^{H}$ outputs $|x_0\rangle|H(x_0)\rangle$

2. Interpret RHS as algorithm

$$\| \langle x_0| \langle H^*(x_0)| \mathcal{A}^{H^*} |\phi\rangle \|_2 \leq \| \langle x_0| \langle H^*(x_0)| \mathcal{A}^{H} |\phi\rangle \|_2$$
$$+ \| \langle x_0| \langle H^*(x_0)| U_2 O_{H^*} |x_0\rangle\langle x_0| U_1 |\phi\rangle \|_2 + \| \langle x_0| \langle H^*(x_0)| U_2 O_{H} |x_0\rangle\langle x_0| U_1 |\phi\rangle \|_2$$

Square, Jensen's inequality ⇒RHS: success probability of reduction, reprogramming before/after the measured query at random

Technique

$$\mathcal{A}^{H}|\phi\rangle = \mathcal{A}^{H^*}|\phi\rangle + U_2 O_H |x_0\rangle\langle x_0| U_1 |\phi\rangle - U_2 O_{H^*} |x_0\rangle\langle x_0| U_1 |\phi\rangle \quad (*)$$

Plan: 1. Use (*) to test whether $\mathcal{A}^{H}$ outputs $|x_0\rangle|H(x_0)\rangle$

2. Interpret RHS as algorithm

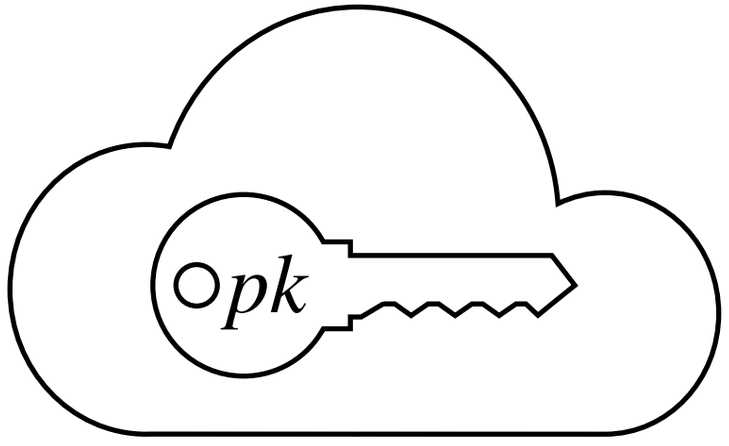
$$\| \langle x_0| \langle H^*(x_0)| \mathcal{A}^{H^*} |\phi\rangle \|_2 \leq \| \langle x_0| \langle H^*(x_0)| \mathcal{A}^{H} |\phi\rangle \|_2$$
$$+ \| \langle x_0| \langle H^*(x_0)| U_2 O_{H^*} |x_0\rangle\langle x_0| U_1 |\phi\rangle \|_2 + \| \langle x_0| \langle H^*(x_0)| U_2 O_{H} |x_0\rangle\langle x_0| U_1 |\phi\rangle \|_2$$

Square, Jensen's inequality ⇒RHS: success probability of reduction, reprogramming before/after the measured query at random

q **queries:** use (*) for each query. $O(q^2)$ loss from Jensen, interpretation as expectation value

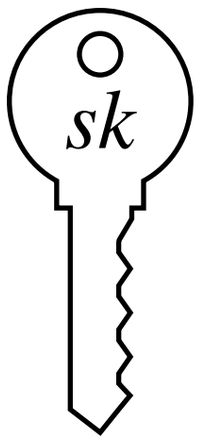
3. Application: Digital Signatures

Identification scheme



∃*sk* for *pk*!

Prove it!



Prover

a →

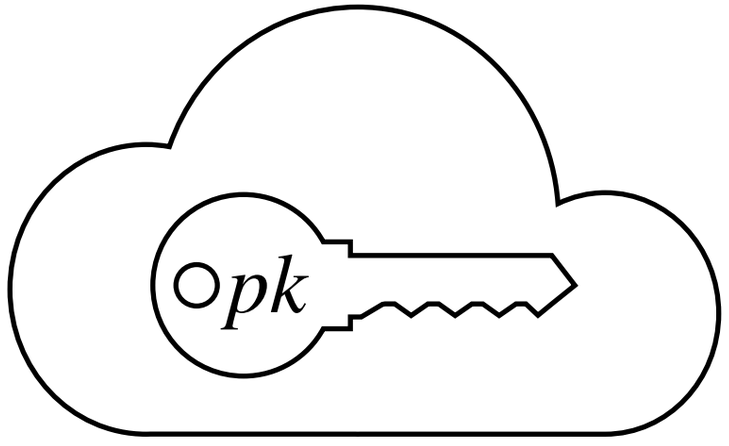
← $c \in_R \mathscr{C}$

r →

Verifier

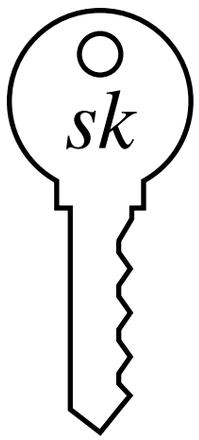
Now I believe
∃*sk* for *pk*…

Identification scheme



∃sk for pk!

Prove it!



Prover

a →

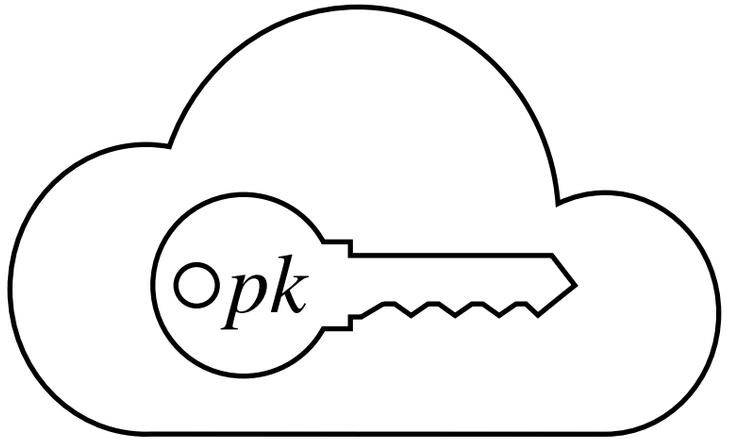
← $c \in_R \mathcal{C}$

r →

Verifier

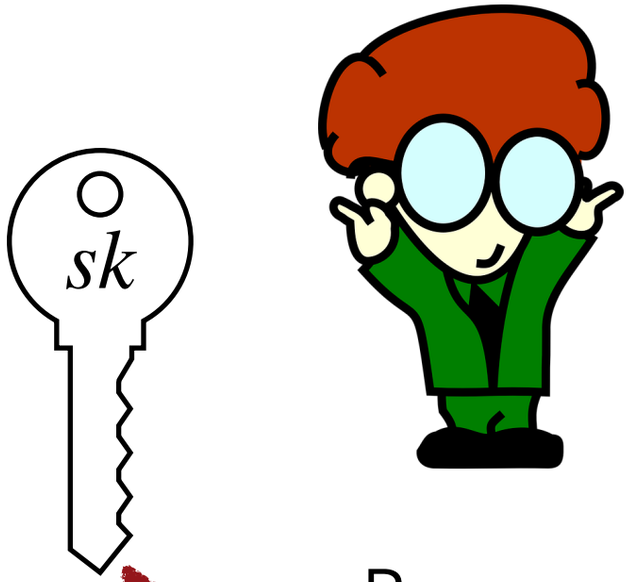
Now I believe that
Prover has sk for pk…

Identification scheme



∃*sk* for *pk*!

Prove it!



Prover

a

$c \in_R \mathcal{C}$

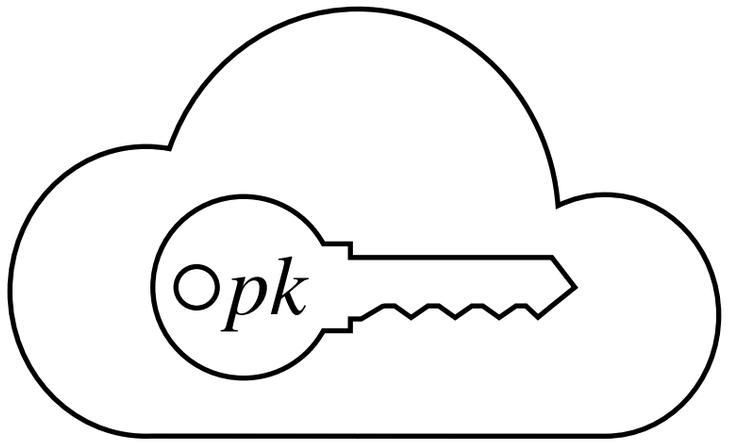
r

Verifier

Still private!

Now I believe that Prover has *sk* for *pk*…

Identification scheme



∃sk for pk!

Prove it!

An Identification scheme is a zero-knowledge proof of knowledge of a private key.

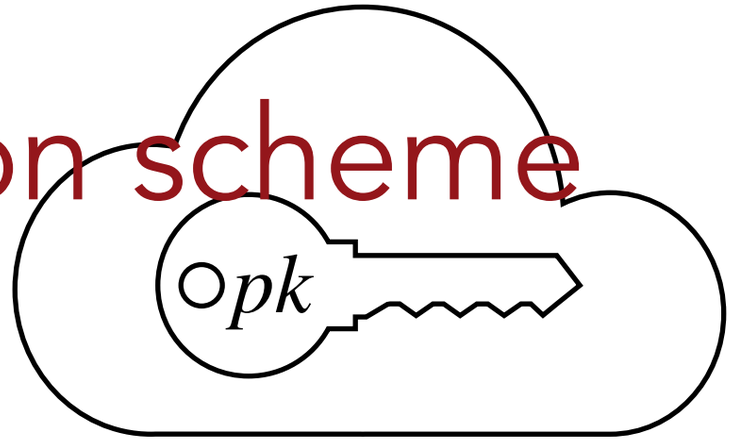
Still private!

Prover

Verifier

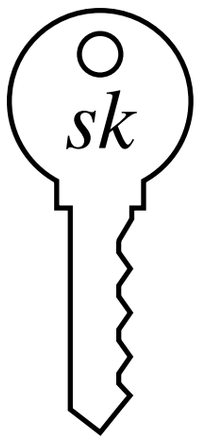
Now I believe that Prover has sk for pk…

Noninteractive Identification scheme



∃*sk* for *pk*!

Prove it!



Prover

a →

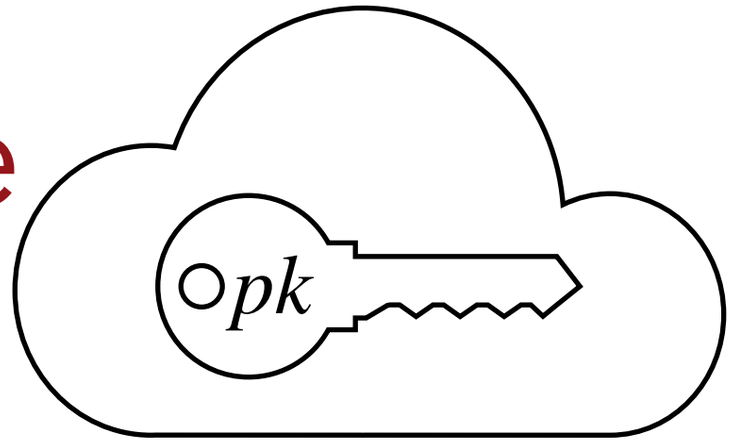
$c = H(a)$ →

r →

Verifier

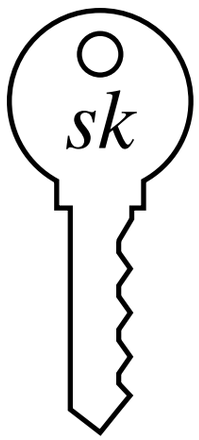
Now I believe that
Prover has *sk* for *pk*…

Digital signature scheme



$\exists sk$ for pk!

Prove it!



Prover

a →

$c = H(a \| m)$ →

r →

Verifier

Now I believe that Prover has used sk to sign m

Fiat Shamir signatures

Several NIST post-quantum candidates use Fiat Shamir:

Fiat Shamir signatures

Several NIST post-quantum candidates use Fiat Shamir:

- Picnic
- Dilithium
- MQDSS
- QTesla

Fiat Shamir signatures

Several NIST post-quantum candidates use Fiat Shamir:

- Picnic
- Dilithium
- MQDSS
- QTesla

Our result ⇒ QROM security

Fiat Shamir signatures

Several NIST post-quantum candidates use Fiat Shamir:

- Picnic
- Dilithium
- MQDSS
- QTesla

Our result ⇒ QROM security

Improved efficiency!

Fiat Shamir signatures

Several NIST post-quantum candidates use Fiat Shamir:

- Picnic
- Dilithium
- MQDSS
- QTesla

Our result ⇒ QROM security

Improved efficiency!

Further applications

Remove almost all interaction from Mahadev's verification for BQP (Alagic, Childs, Hung '19)

Summary

The Fiat Shamir transformation is secure in the quantum random oracle model.

This fact has nice applications, in particular for post-quantum secure digital signature schemes.

Open problem: ∃ quantum forking lemma?

Thanks!