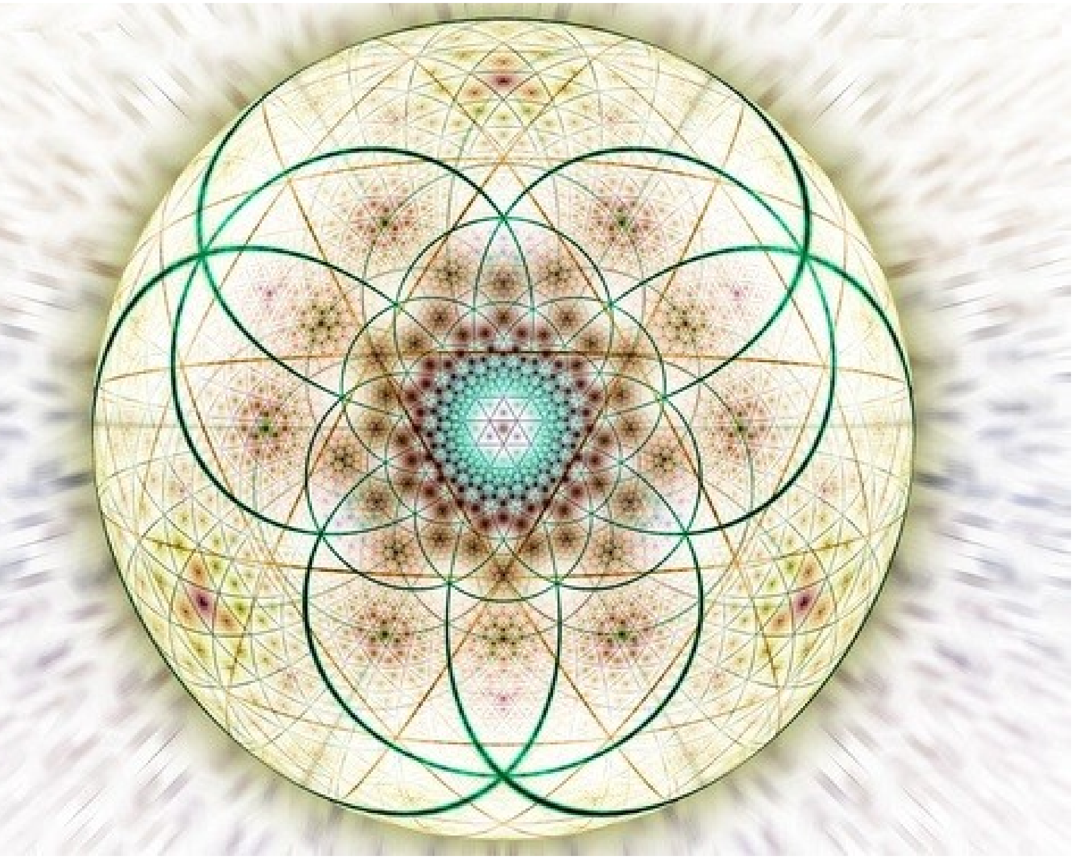
Quantum Cryptography

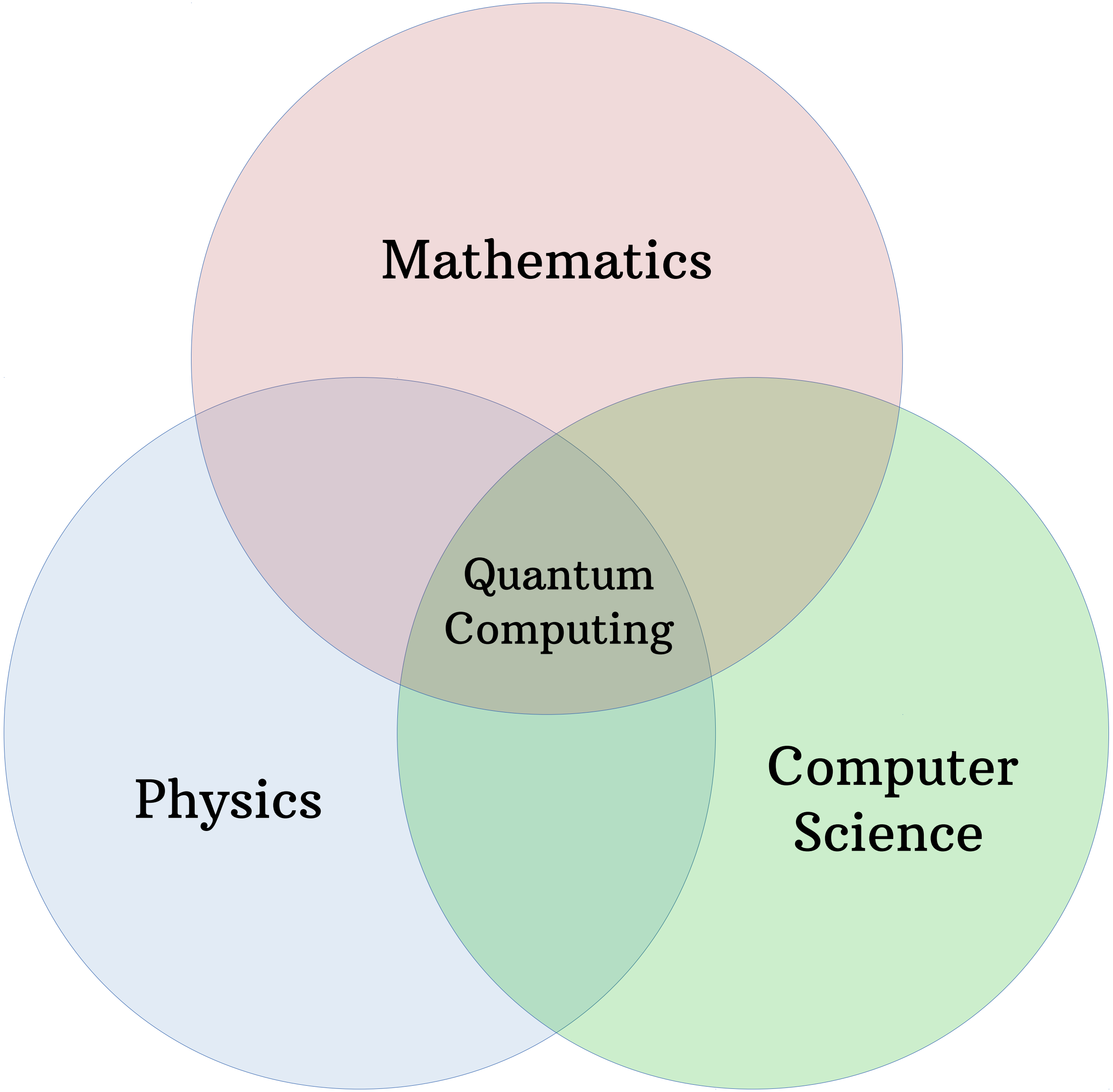


Māris Ozols
University of Cambridge

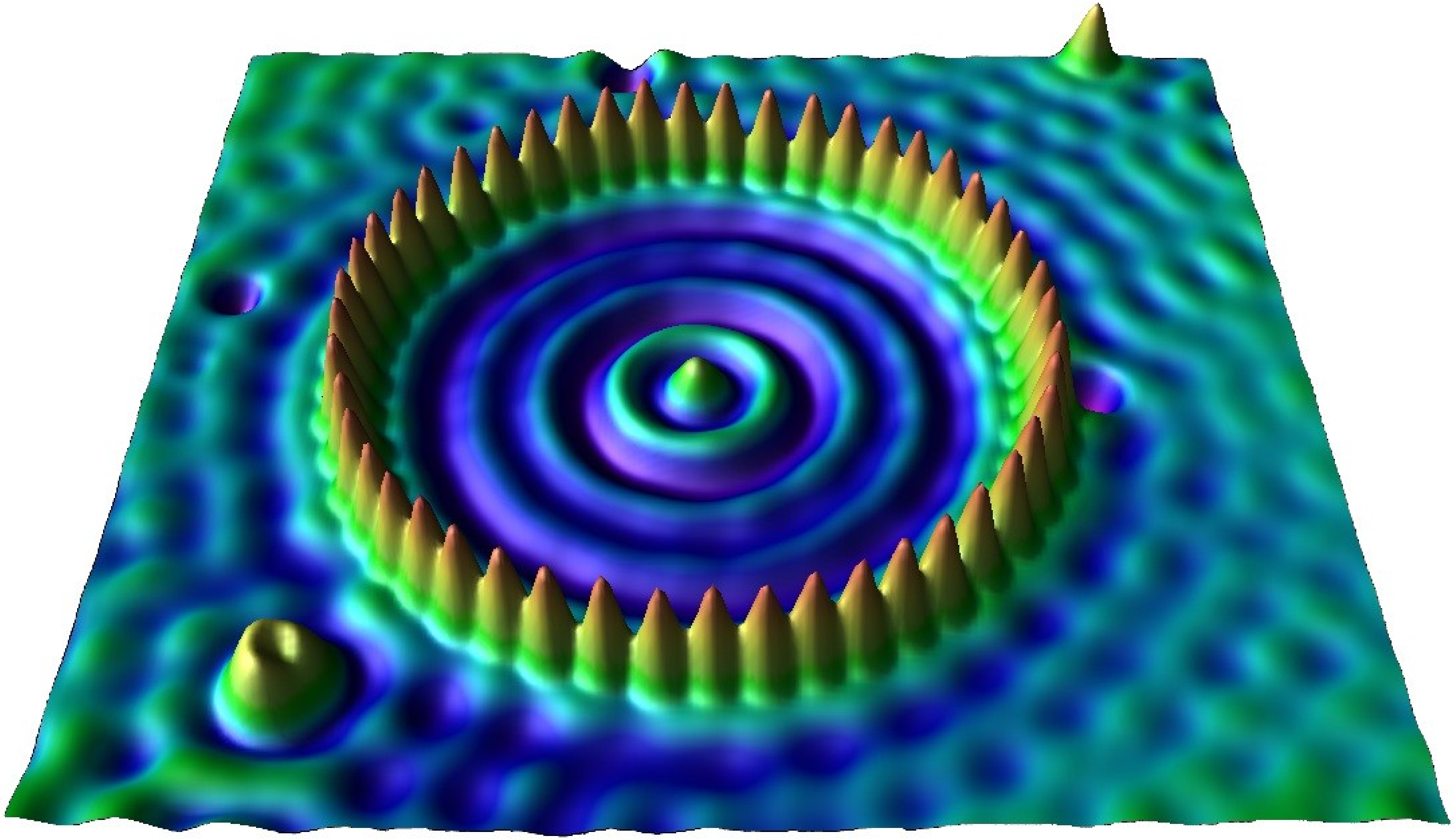
Overview

- What are quantum computers?
- What is quantum cryptography?
  - Shor's algorithm for factoring
  - Quantum key distribution
  - Device-independent quantum cryptography

What is quantum computing?



Quantum mechanics



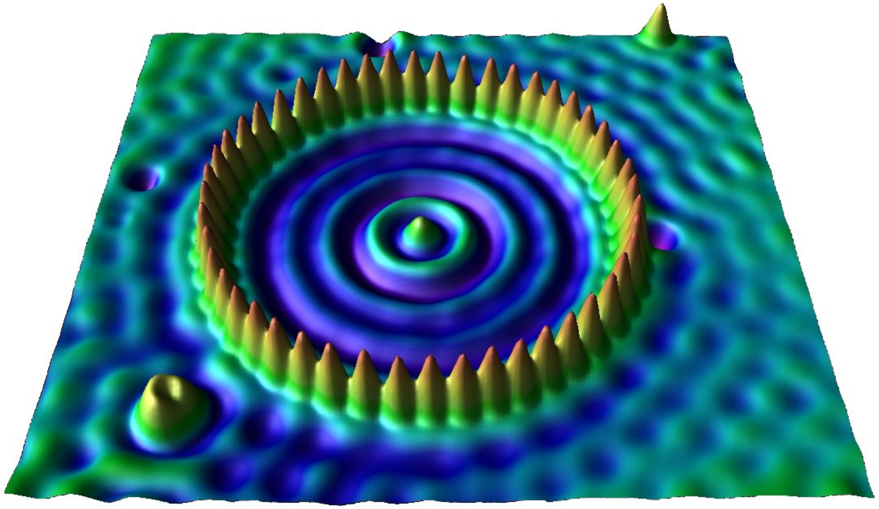
How to simulate quantum physics?

Richard Feynman

Simulating quantum systems on a regular computer is very hard...

Wouldn't it be easier if the computer itself would operate based on the laws of quantum physics?

What is a quantum computer?



Quantum mechanics

+

Computer

Quantum computer is a device that processes information by using quantum phenomena

What quantum computers are **not**…

What quantum computers are **not**…

just

smaller

What quantum computers are **not**…

just
smaller

just
FASTER

What quantum computers are **not**…

just
smaller

exponentially
faster

just
FASTER

What quantum computers are **not**...

just
smaller

exponentially
faster

just
FASTER

science
FICTION

What quantum computers are **not**…

just
smaller

exponentially
faster

just
FASTER

science
FICTION

available
for $ale

Quantum cryptography

- Quantum algorithms for breaking existing cryptosystems
  - Shor's algorithm for factoring

Quantum cryptography

- Quantum algorithms for breaking existing cryptosystems
  - Shor's algorithm for factoring
- Enabling secure communication
  - Quantum key distribution

Quantum cryptography

- Quantum algorithms for breaking existing cryptosystems
  - Shor's algorithm for factoring
- Enabling secure communication
  - Quantum key distribution
- Computation with untrusted devices
  - Device-independent quantum cryptography

Multiplying vs factoring

Multiplying is easy…

$3 \times 5 =$

$11 \times 13 =$

$28423087481 \times 25162321141 =$

Multiplying vs factoring

Multiplying is easy…

3 × 5 = 15

11 × 13 = 143

28423087481 × 25162321141 = 715190855015658735821

Multiplying vs factoring

Multiplying is easy...

3 × 5 = 15

11 × 13 = 143

28423087481 × 25162321141 = 715190855015658735821

Factoring is not...

12 =

377 =

57249035862524887649 =

Multiplying vs factoring

Multiplying is easy...

$3 \times 5 = 15$

$11 \times 13 = 143$

$28423087481 \times 25162321141 = 715190855015658735821$

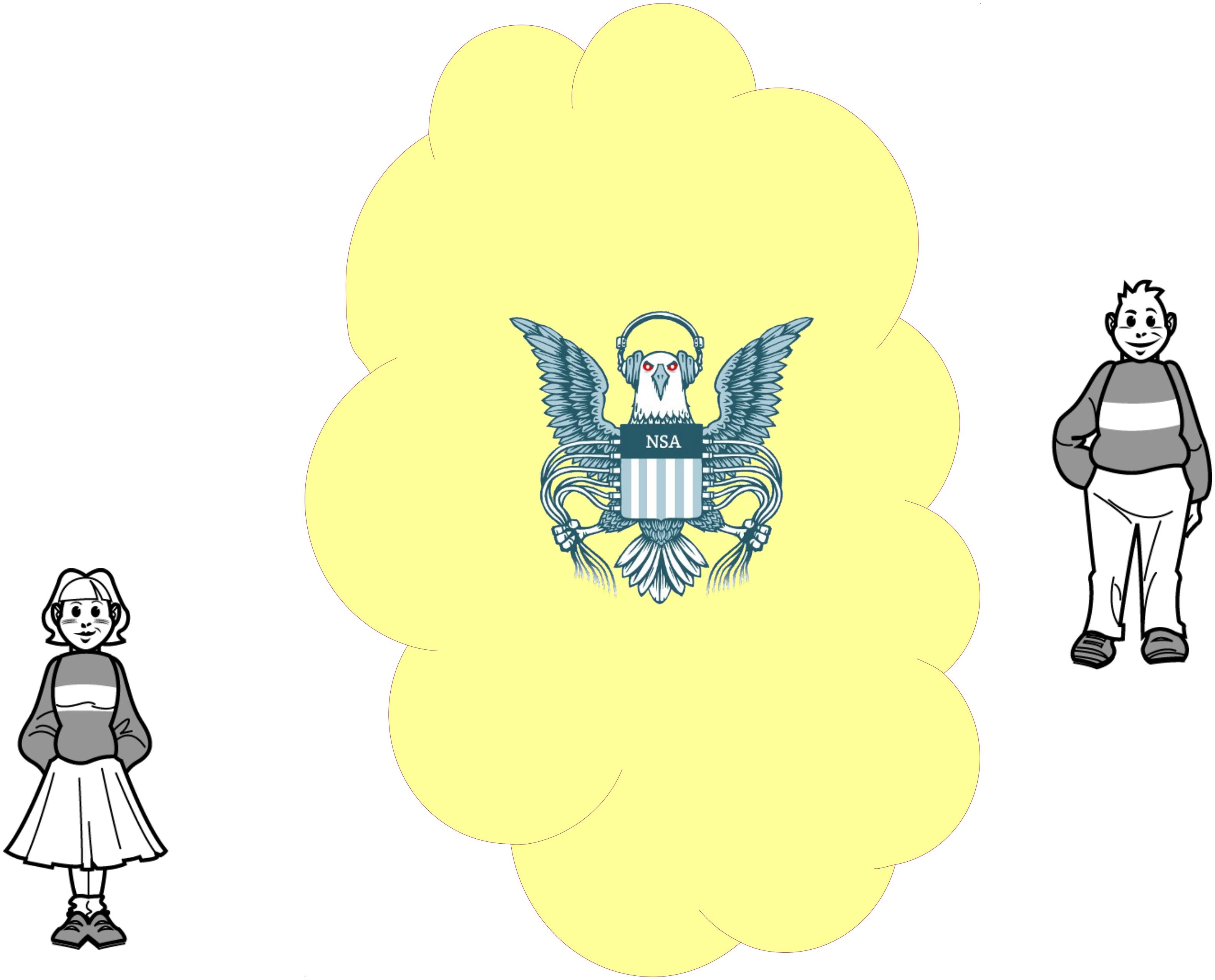
Factoring is not...

$12 = 3 \times 4$

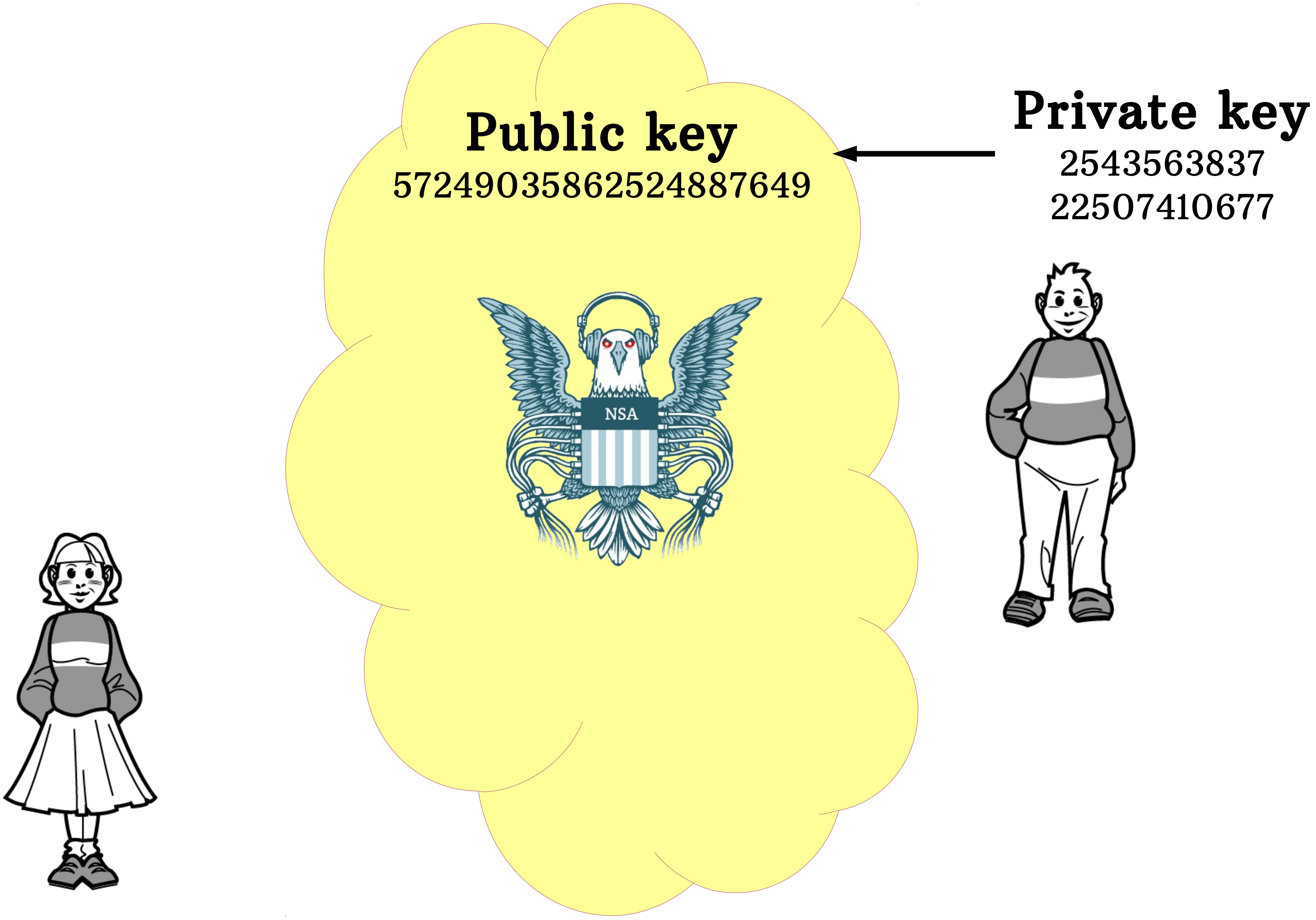
$377 = 13 \times 29$

$572490358625248876649 = 2543563837 \times 22507410677$

Public-key cryptography (RSA)



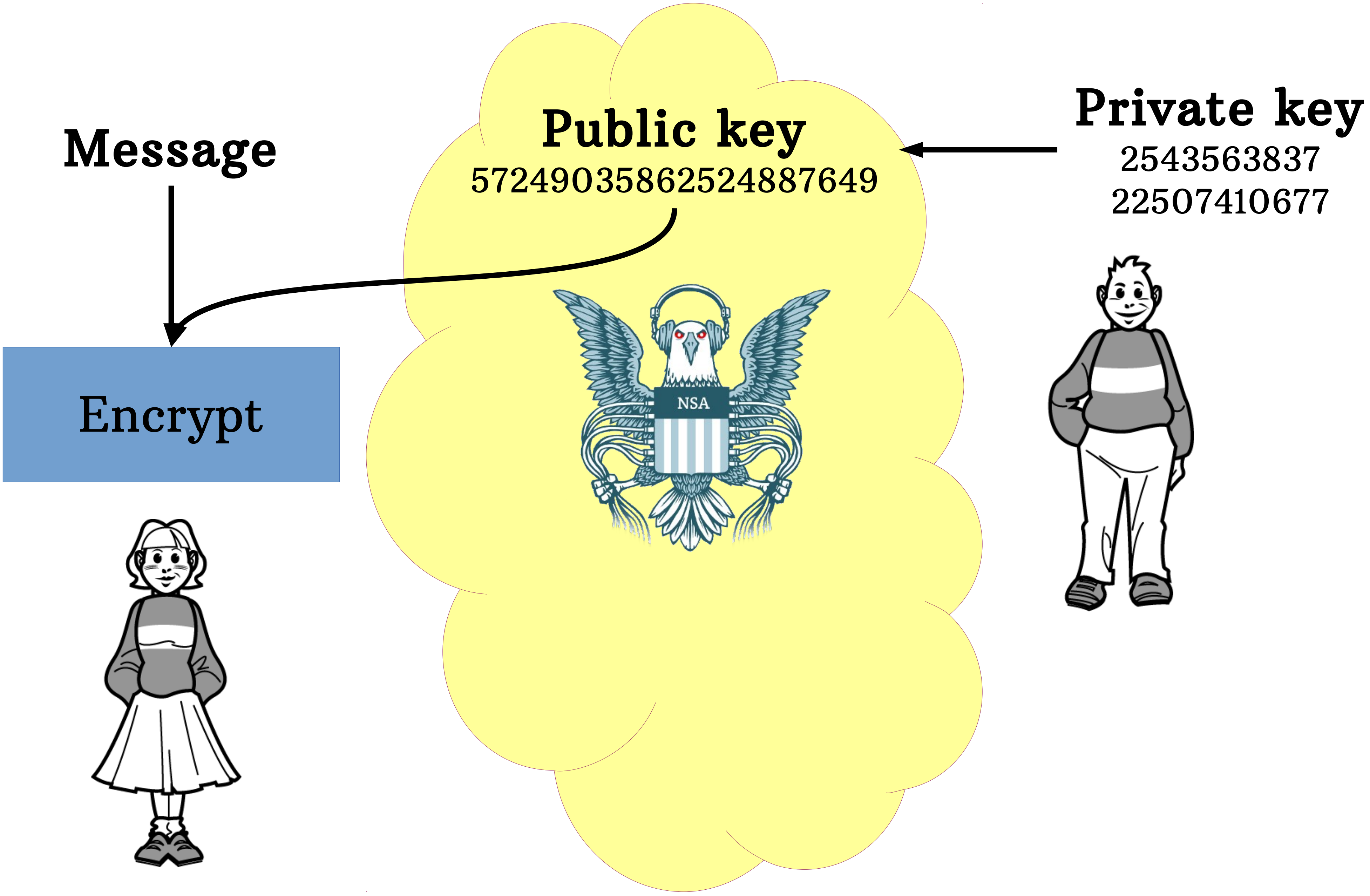
Public-key cryptography (RSA)



Public key
57249035862524887649

Private key
2543563837
22507410677

Public-key cryptography (RSA)



Message

Encrypt

Public key

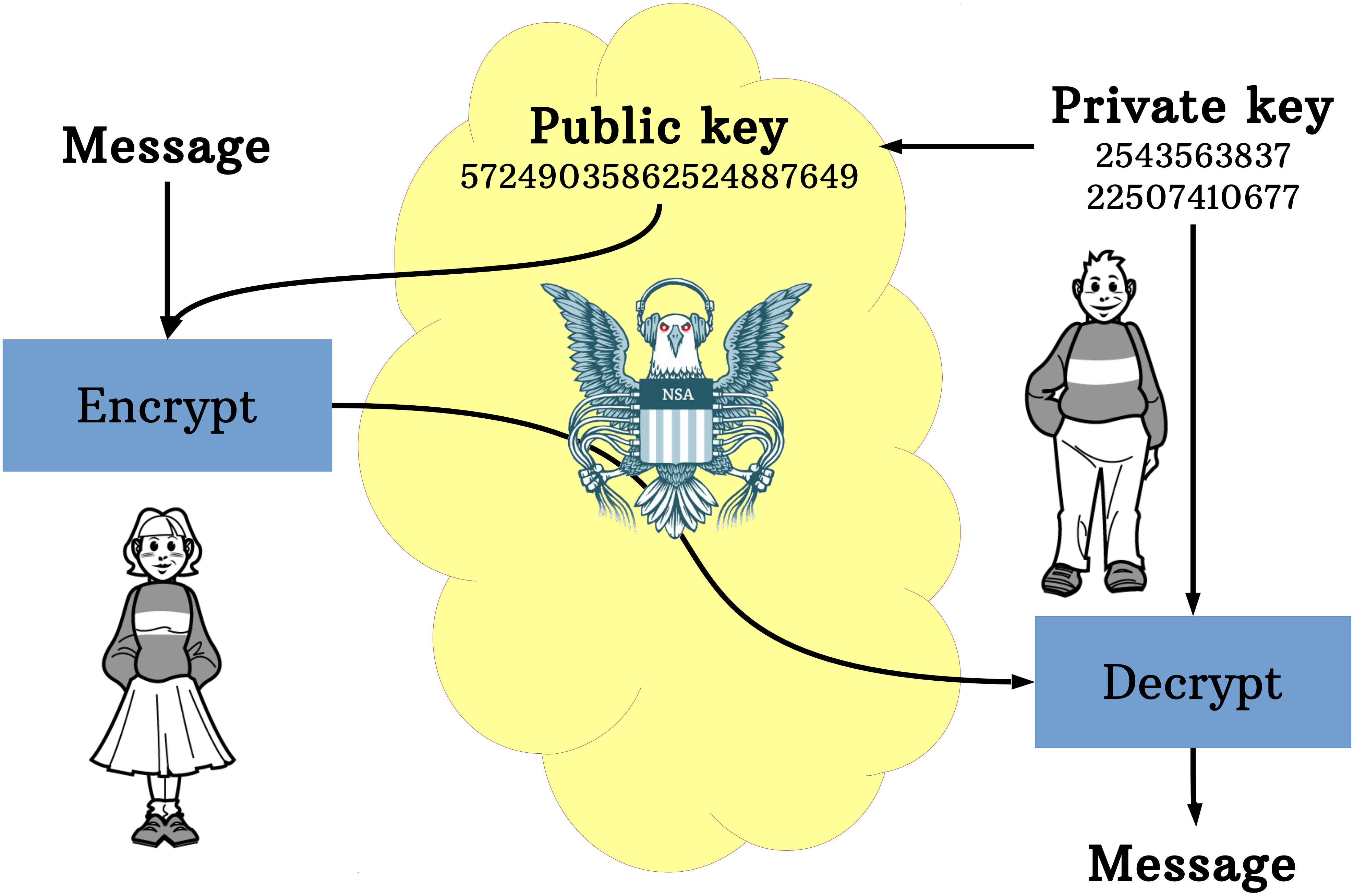
57249035862524887649

Private key

2543563837

22507410677

Public-key cryptography (RSA)



Message

Public key
57249035862524887649

Private key
2543563837
22507410677

Encrypt

Decrypt

Message

Shor's algorithm breaks RSA

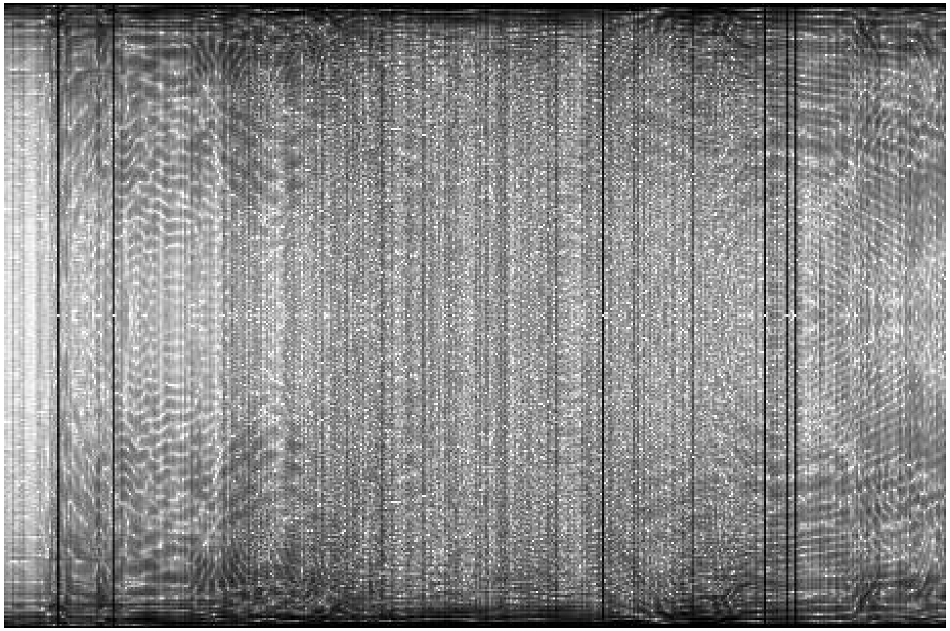
- Produces prime factors of a given integer
- Runs in polynomial time
  (best known classical algorithm runs in exponential time)

Peter Shor

Shor's algorithm breaks RSA

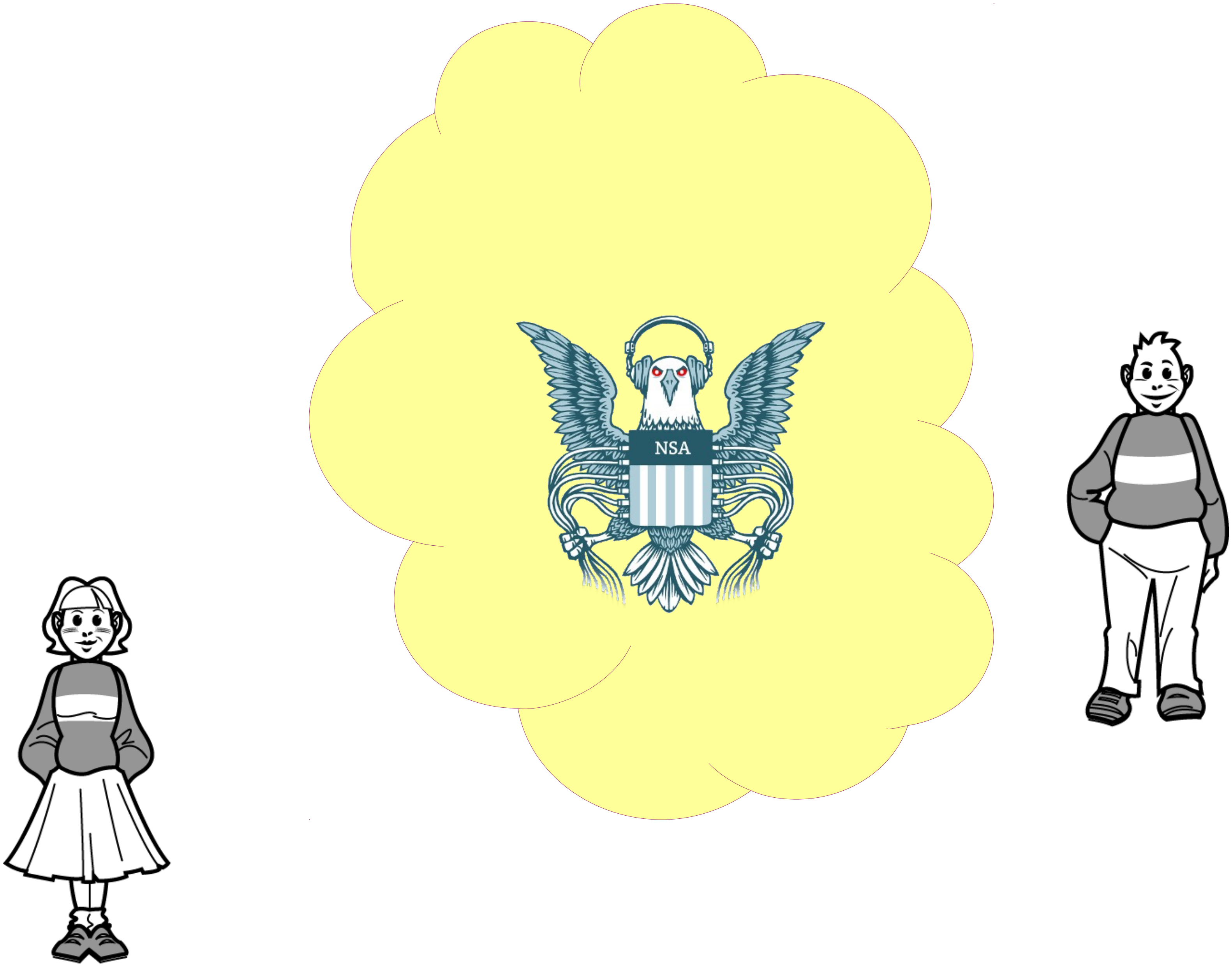
- Produces prime factors of a given integer
- Runs in polynomial time
  (best known classical algorithm runs in exponential time)
- Based on quantum Fourier transform

Peter Shor

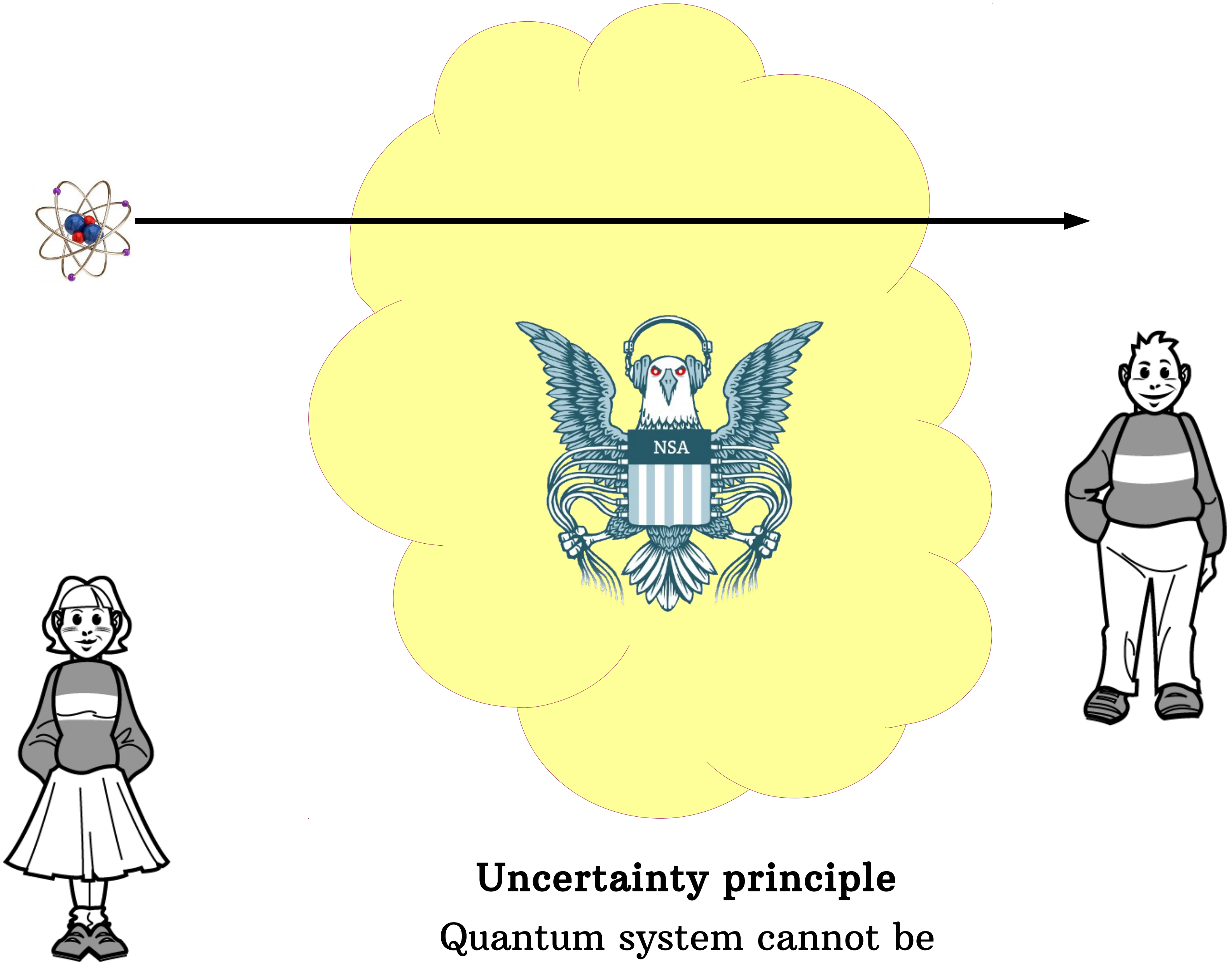


Fourier transform of Peter Shor

Quantum key distribution



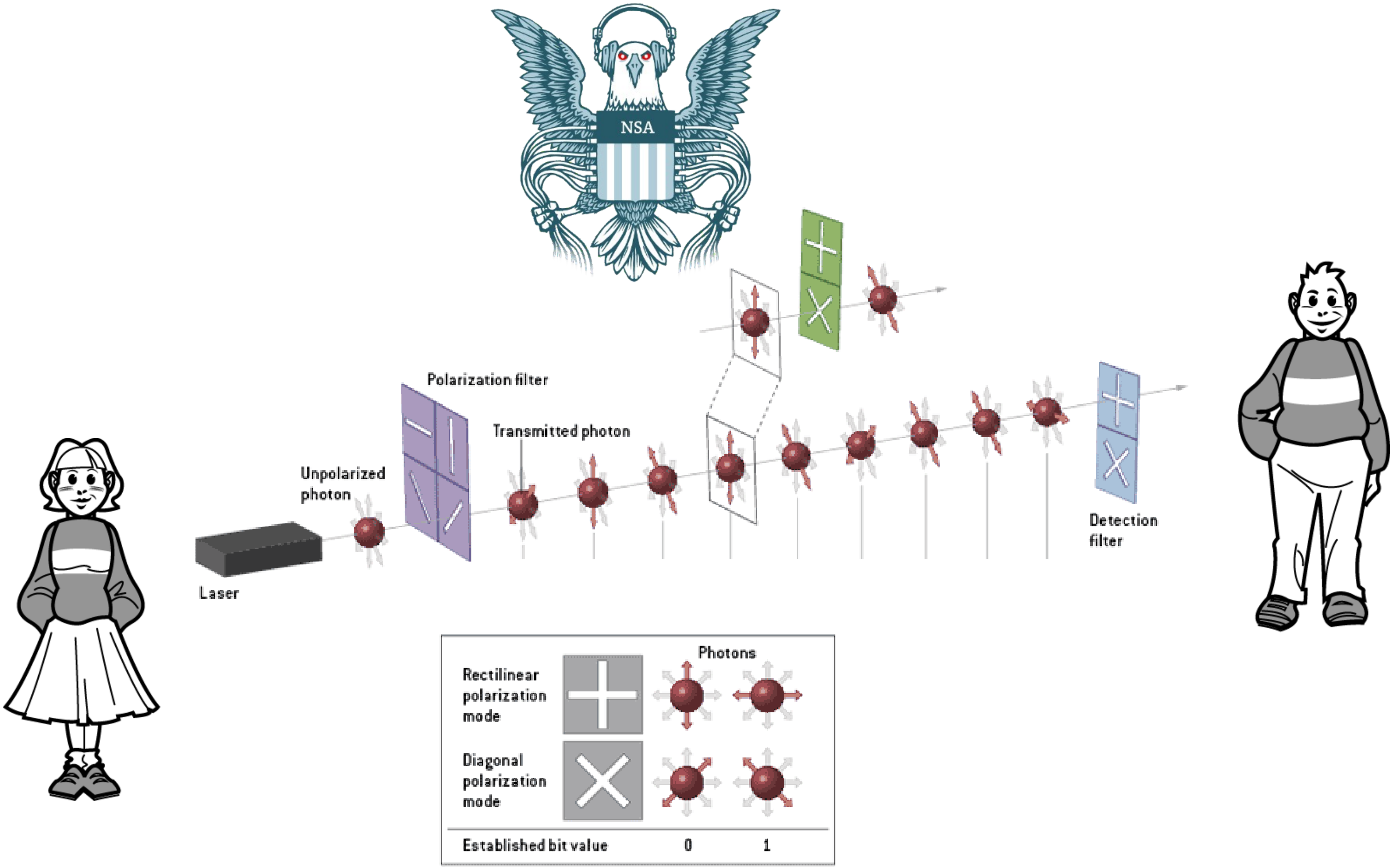
Quantum key distribution



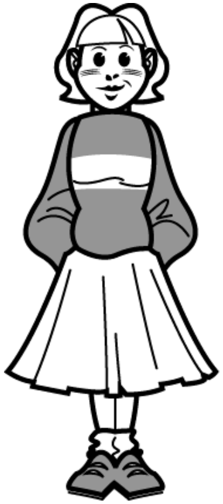
Uncertainty principle

Quantum system cannot be
observed without disturbing it

Quantum key distribution

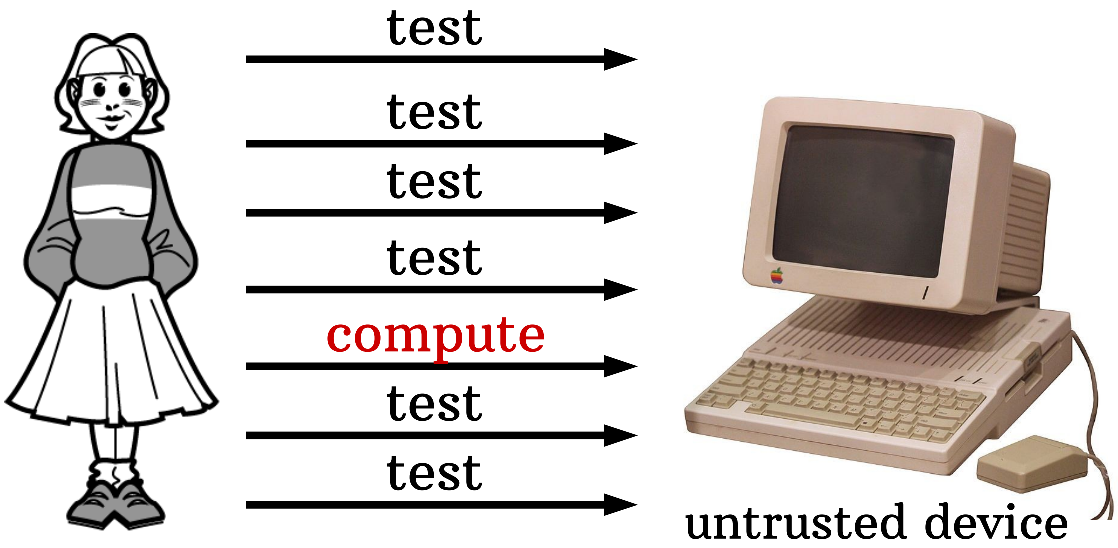


Device-independent quantum cryptography



untrusted device

Device-independent quantum cryptography



test

test

test

test

compute

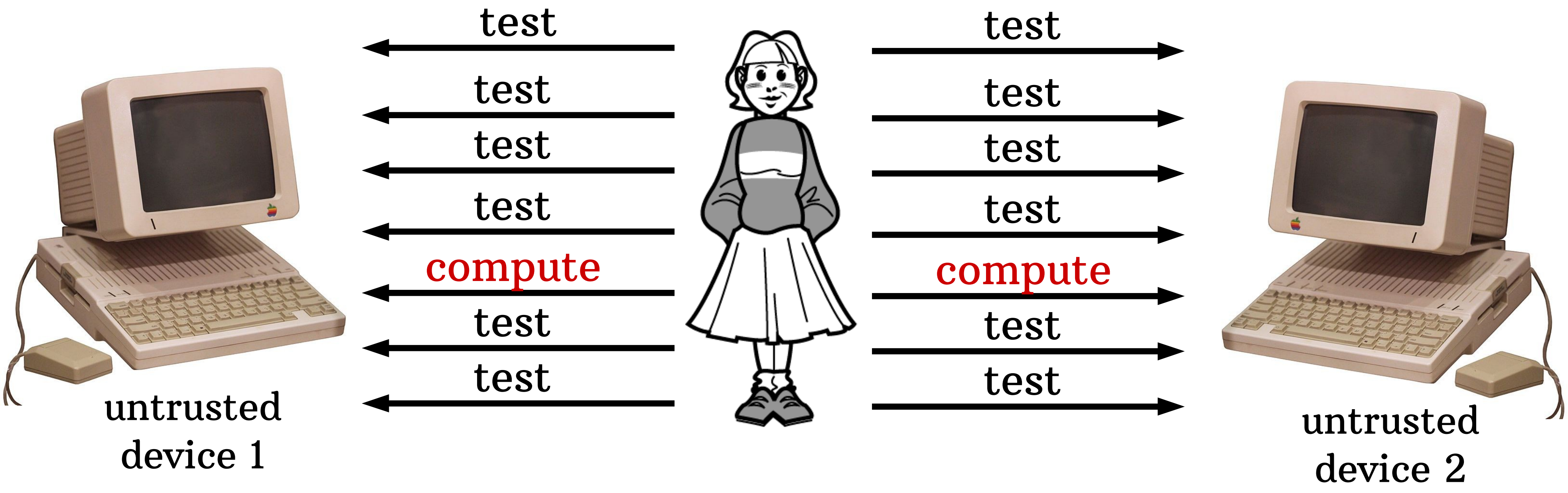
test

test

untrusted device

Strategy 1: Self-testing

Device-independent quantum cryptography



test

test

test

test

compute

test

test

untrusted device 1

test

test

test

test

compute

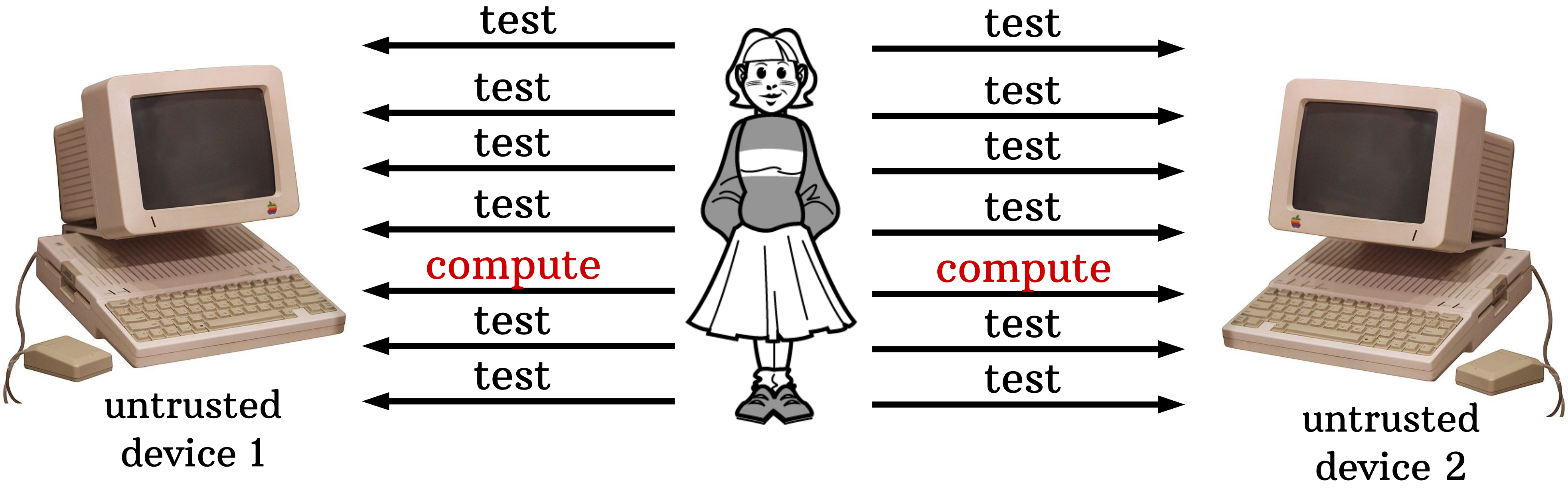
test

test

untrusted device 2

Strategy 2: Cross-checking

Device-independent quantum cryptography



Device-independent quantum protocols exist for

- quantum key distribution
- randomness expansion
- randomness amplification

Long-term implications

Security vs Privacy

Thank you!