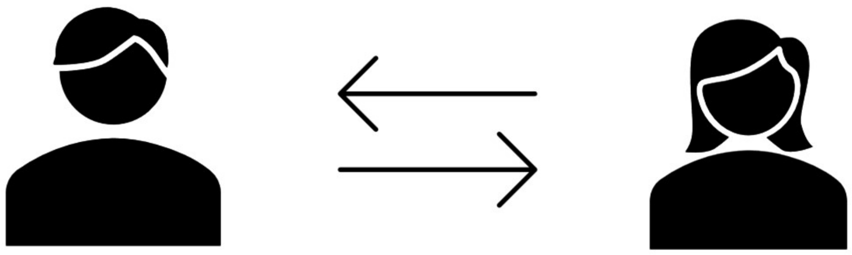
Blockchain and the Quantum Threat

post-quantum signatures

Leonardo Errati – De Componendis Cifris & Polytechnic of Turin

2025-03-21, Paris

The sender’s dilemma



Paul

Viki

The sender’s dilemma

Paul

Viki

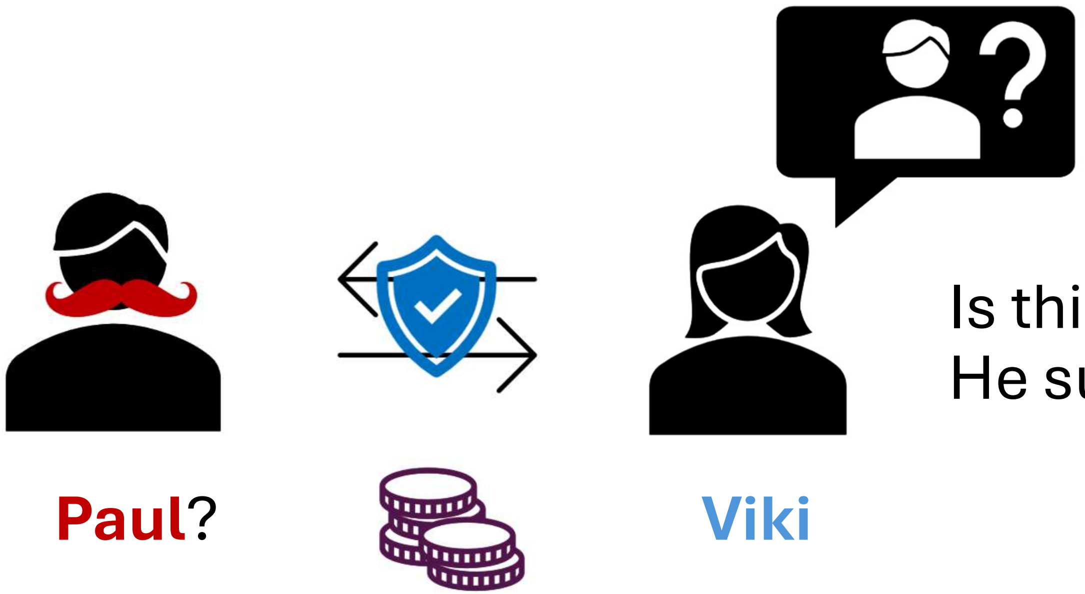
The sender’s dilemma

Paul?

Viki

Is this **document** **Paul**’s?
He sure seems like **Paul**...

The sender’s dilemma

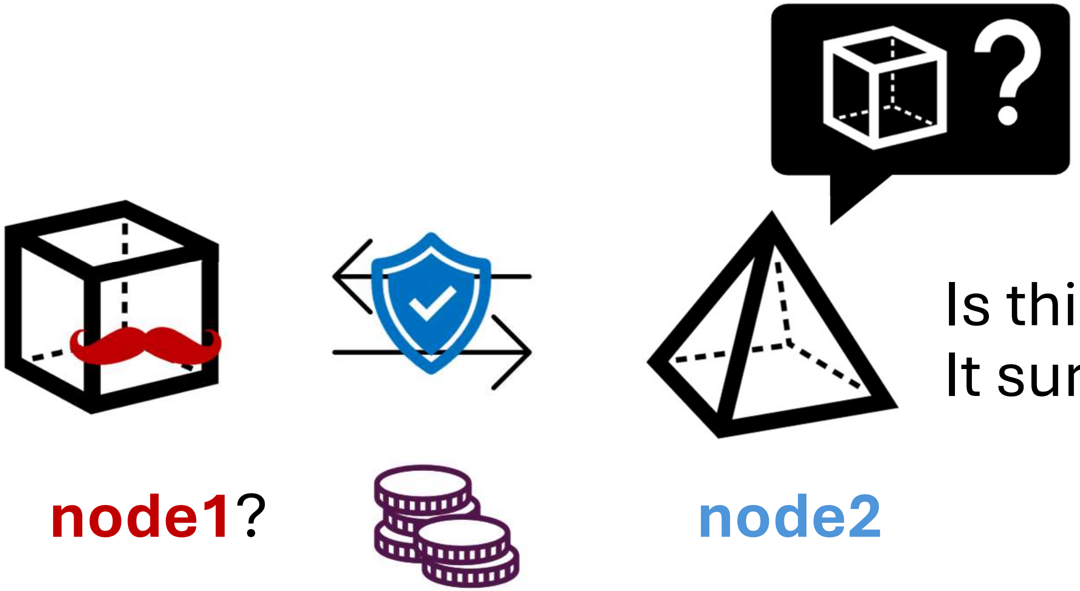


Paul?

Viki

Is this **money** **Paul**’s?
He sure seems like **Paul**...

The sender’s dilemma

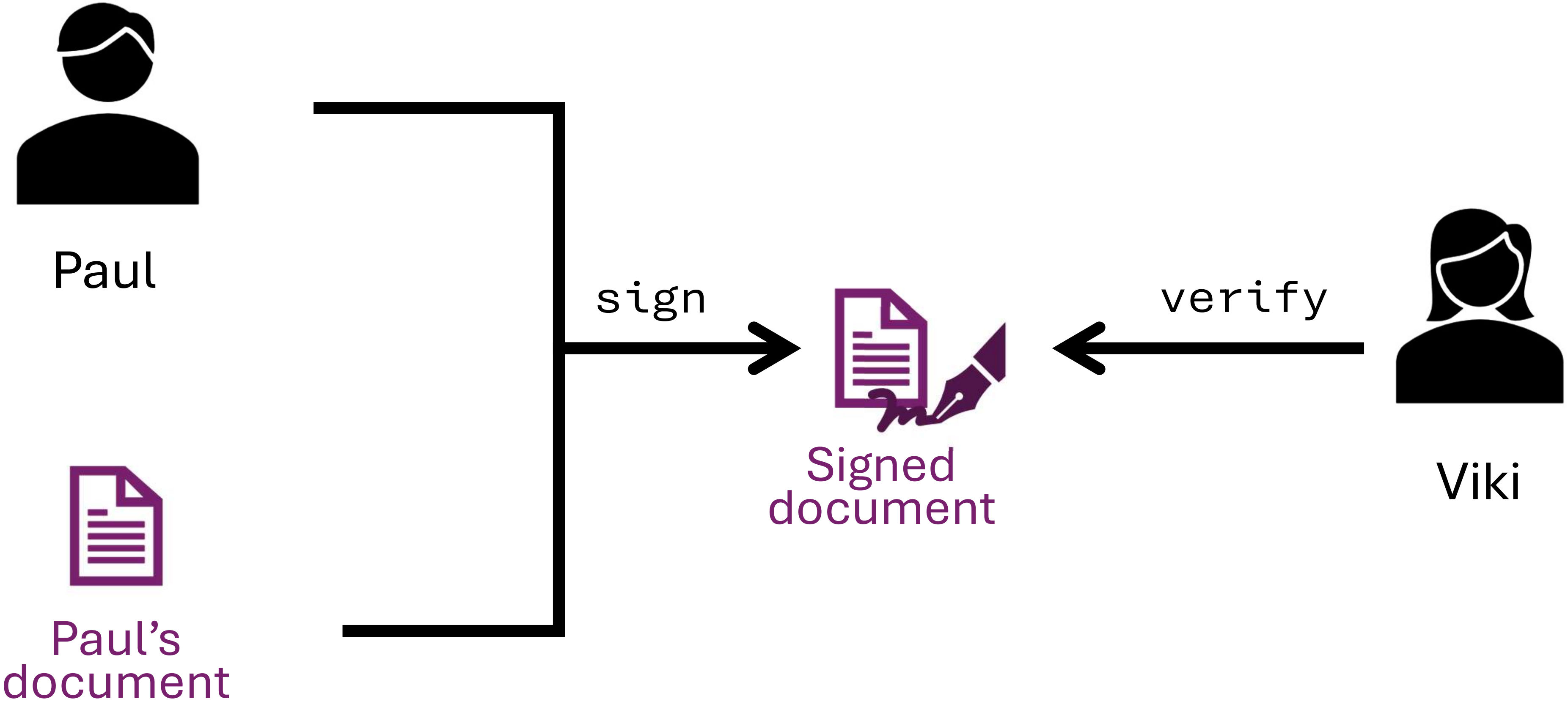


node1?

node2

Is this **money** **node1**’s?
It sure seems like **node1**…

Classical signature



Paul

Paul's document

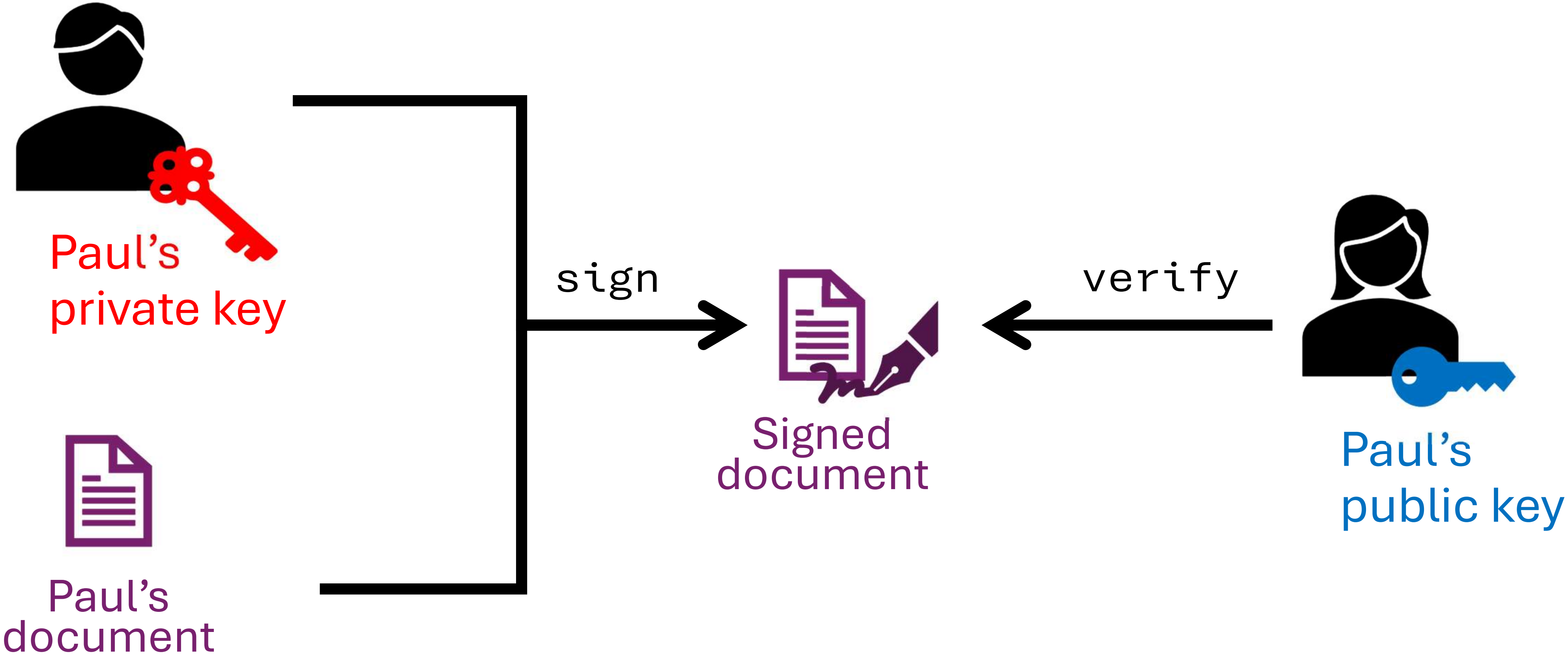
sign

Signed document

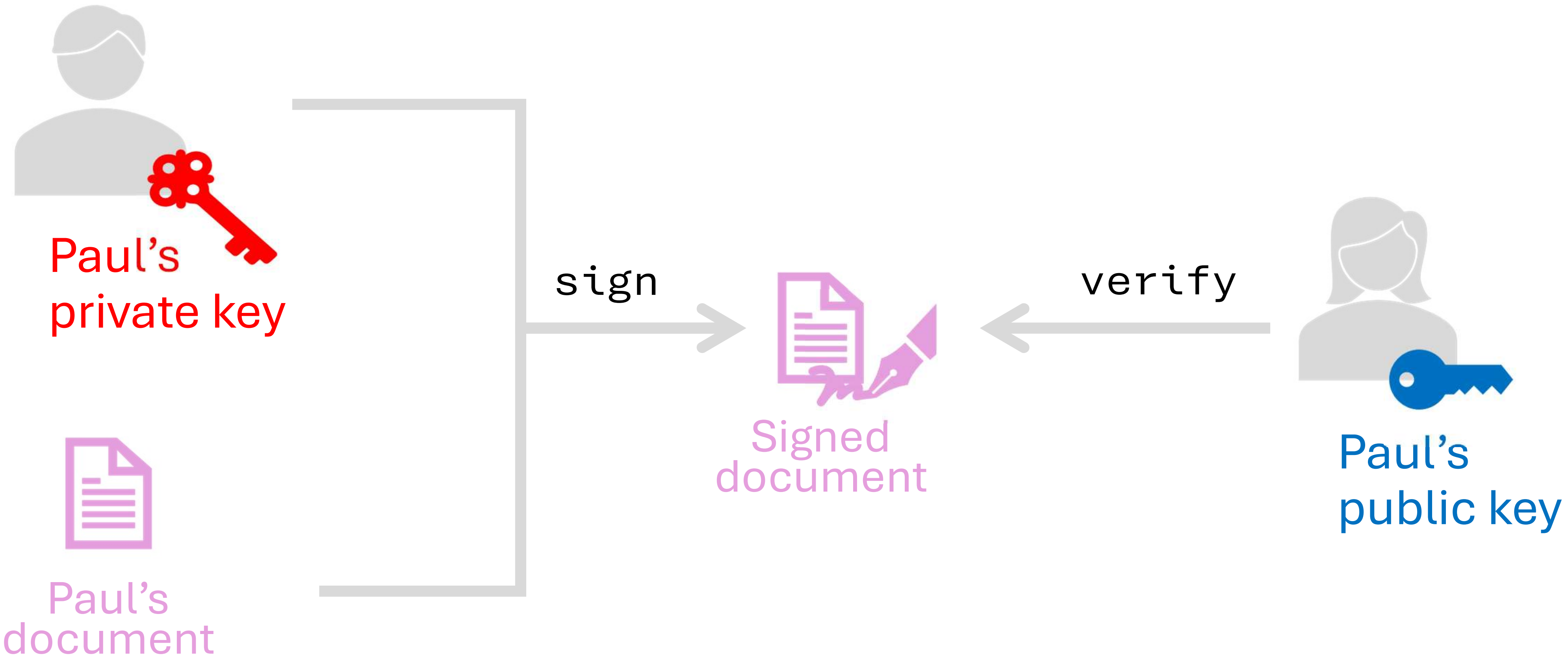
verify

Viki

Cryptographic signature



Cryptographic signature



Paul’s private key

Paul’s document

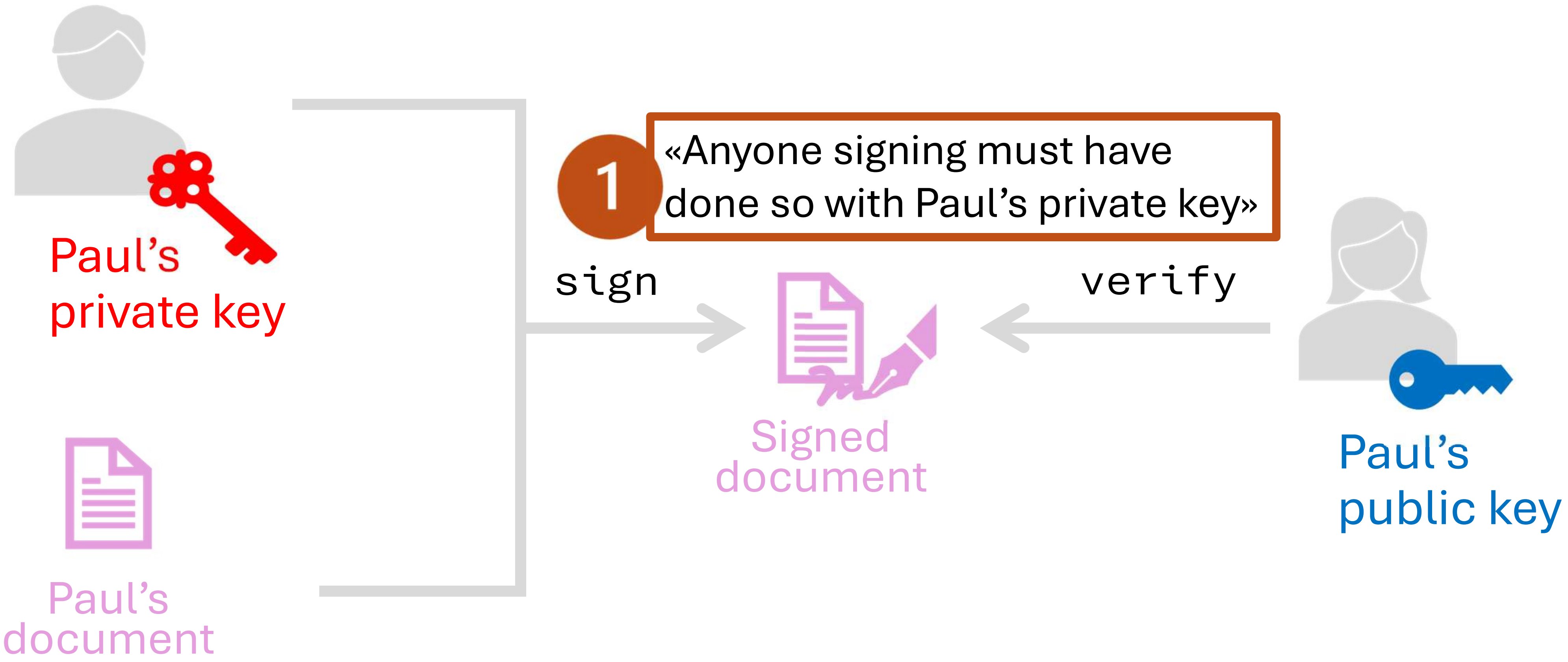
sign

Signed document

verify

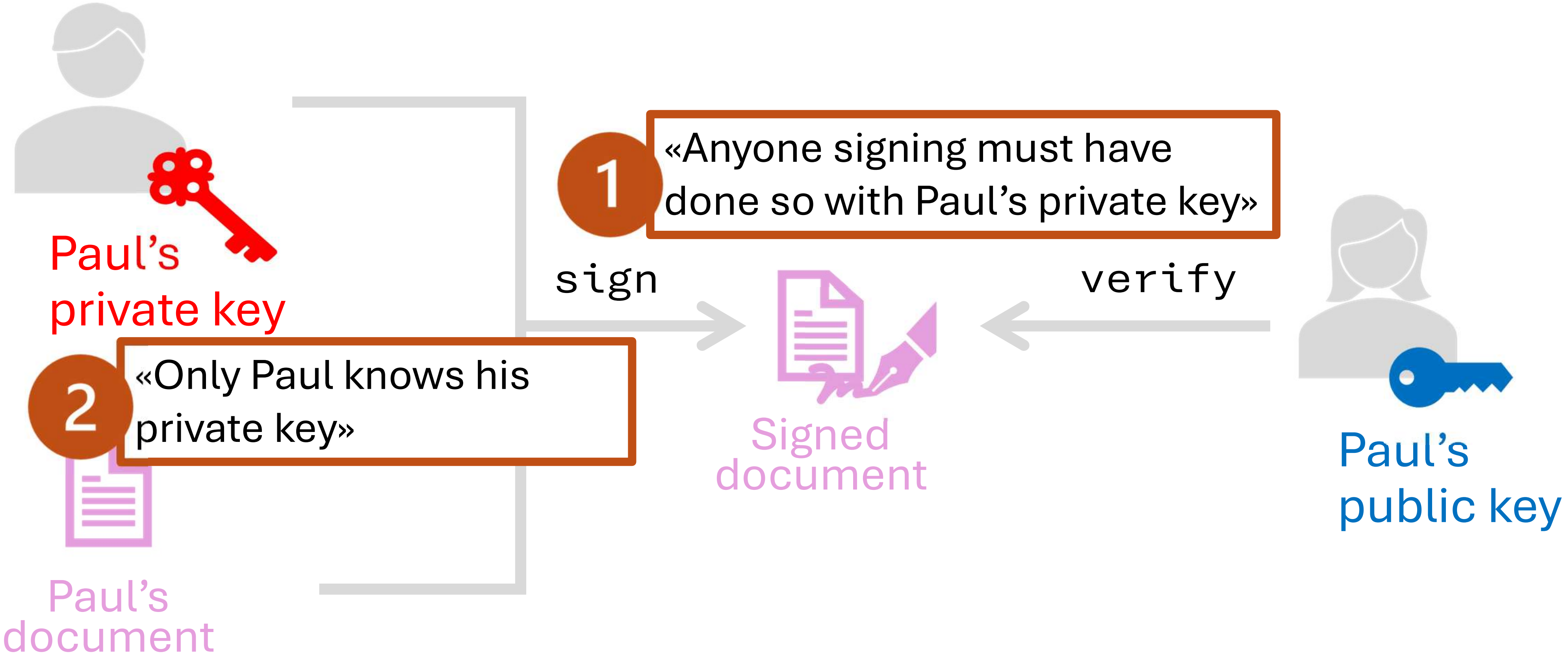
Paul’s public key

Cryptographic signature



«Anyone signing must have done so with Paul’s private key»

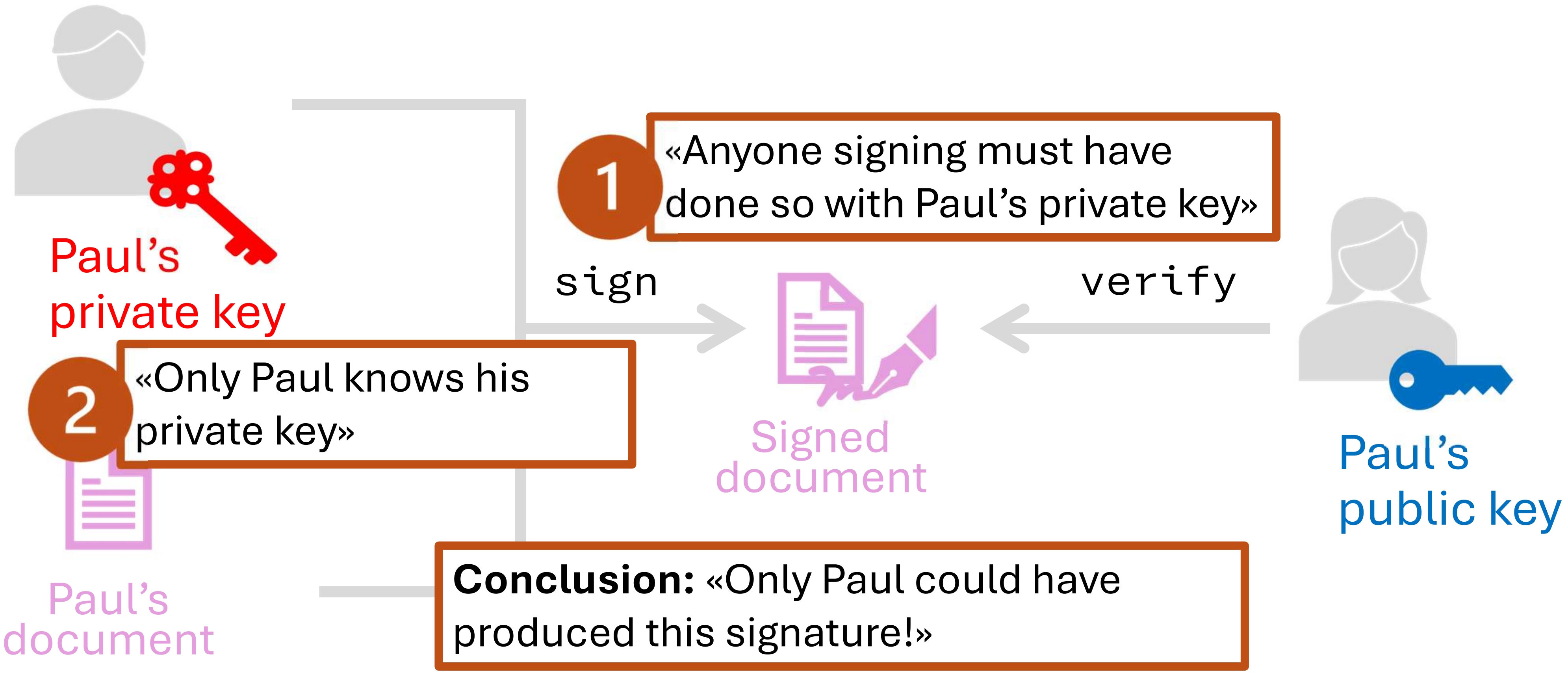
Cryptographic signature



1 «Anyone signing must have done so with Paul’s private key»

2 «Only Paul knows his private key»

Cryptographic signature



Paul's private key

1 «Anyone signing must have done so with Paul's private key»

sign

verify

2 «Only Paul knows his private key»

Signed document

Paul's public key

Paul's document

Conclusion: «Only Paul could have produced this signature!»

Cryptographic signature

Attack: sign without the private key (forgery)

1 «Anyone signing must have done so with Paul’s private key»

2 «Only Paul knows his private key»

Attack: derive the private key (total break)

Conclusion: «Only Paul could have produced this signature!»

Cryptographic signature

Attack: sign without the private key (forgery)

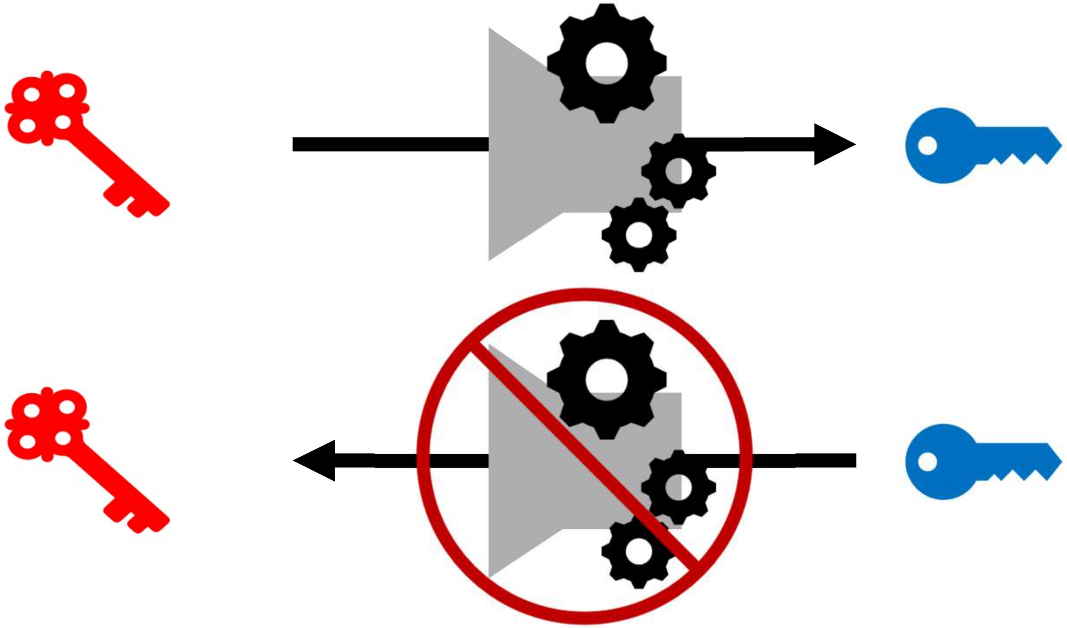
1 «Anyone signing must have done so with Paul’s private key»

2 «Only Paul knows his private key»

Attack: derive the private key (total break)

Conclusion: «Only Paul could have produced this signature... probably?»

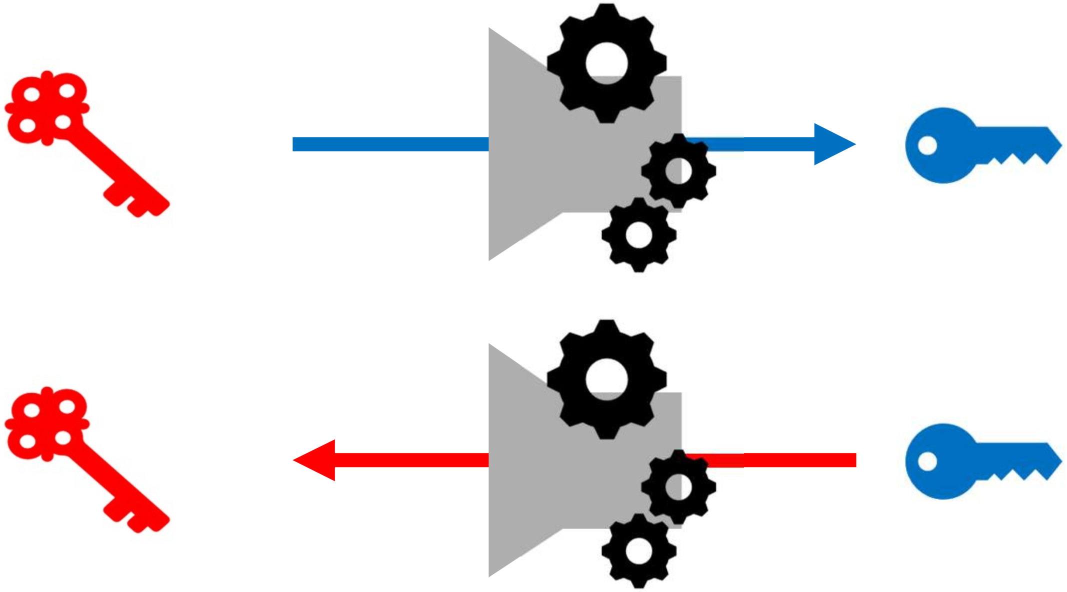
How to build a signature: ideal



known

impossible to invert

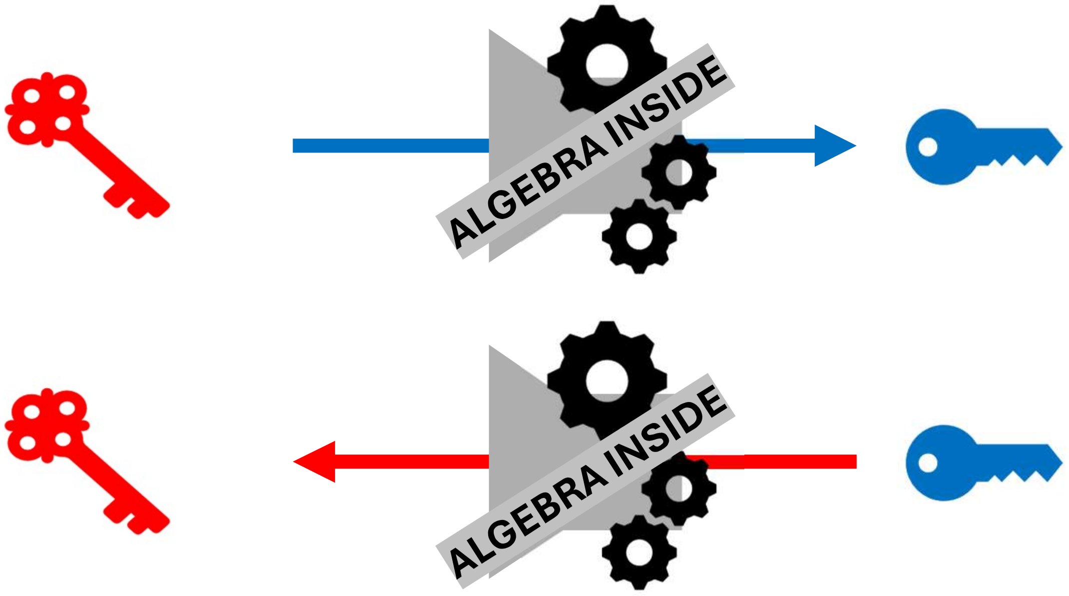
How to build a signature: real



easy to calculate

hard to invert

How to build a signature: real



easy to calculate

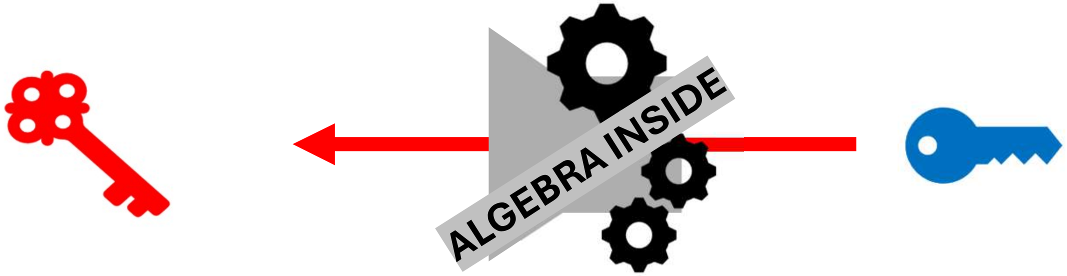
hard to invert

How to build a signature: real

attack probability:

2^{-60}

2^{-80} 2^{-120}



hard to invert

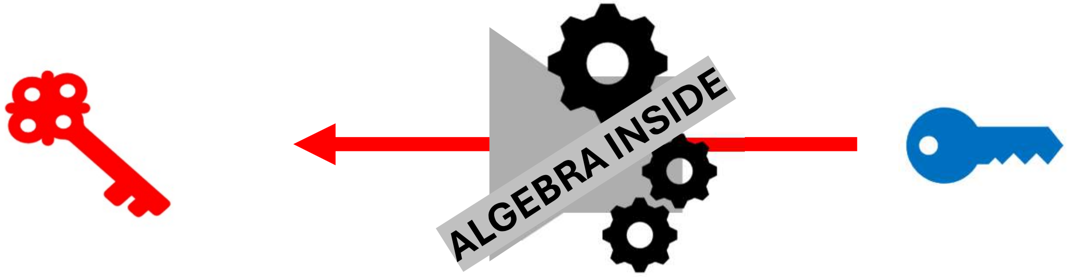
How to build a signature: real

?

attack probability:

? ?

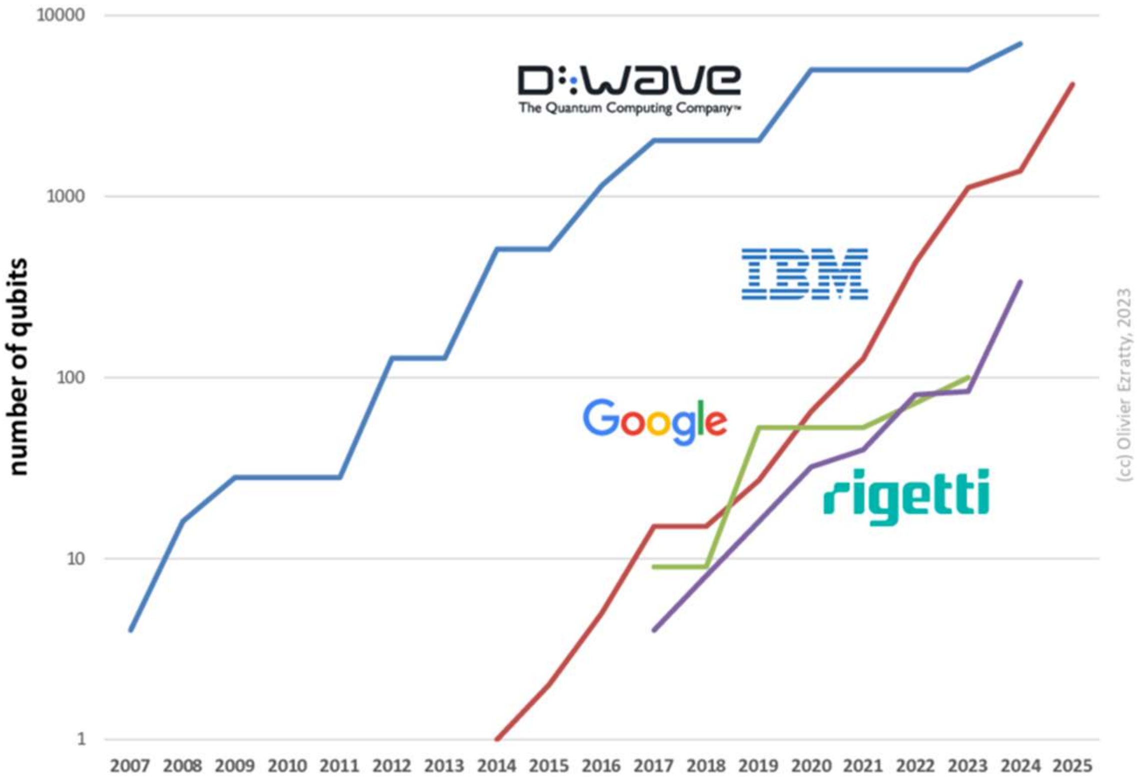
quantum attacker



hard to
invert

for who?

How bad is it?

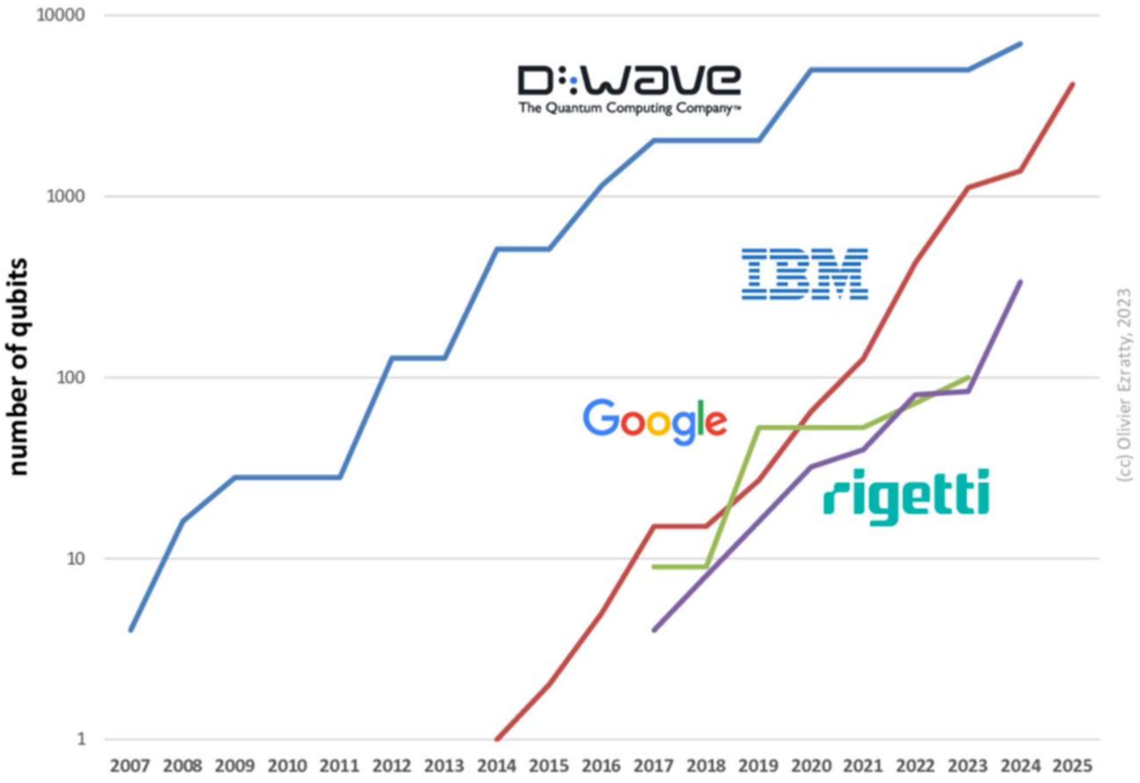


Ezratty, Olivier. (2023). *Is there a Moore's law for quantum computing?*

How bad is it?

RSA	LOGICAL QUBITS
RSA 2048	4098
RSA 3072	6146
RSA 7680	15362

Logical qubits are not total qubits!



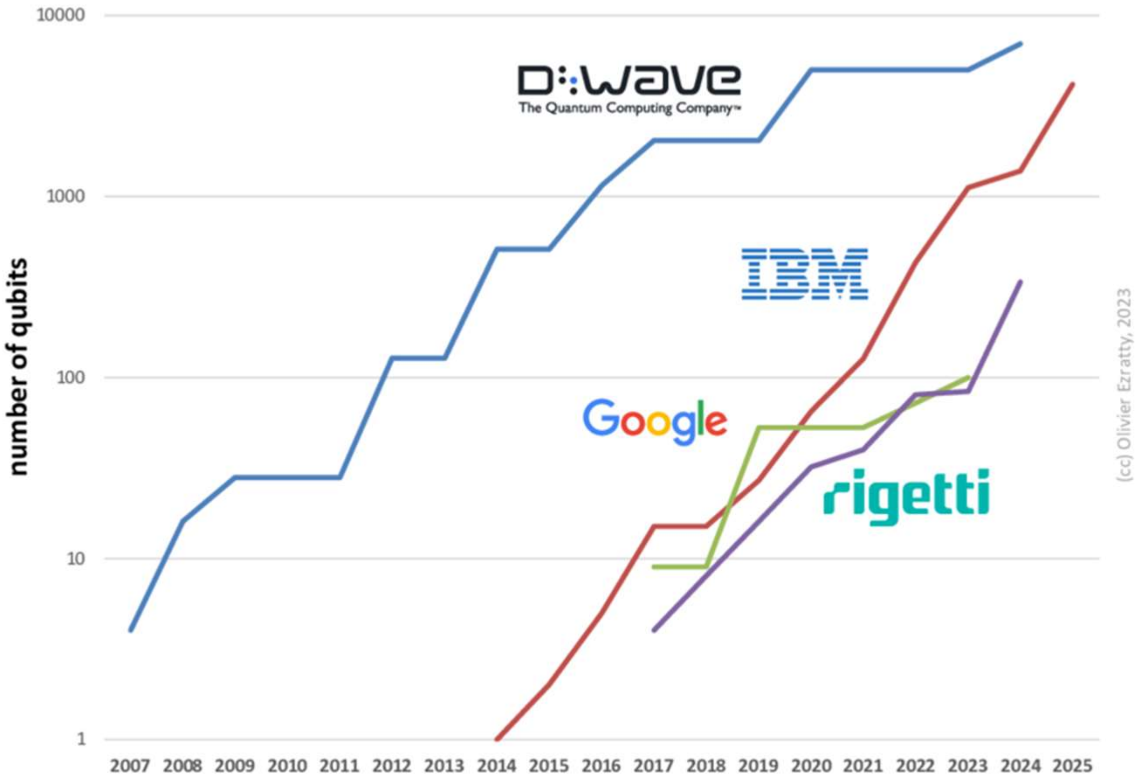
Tommaso Gagliardoni (2021), *Quantum Attack Resource Estimate*

Ezratty, Olivier. (2023). *Is there a Moore's law for quantum computing?*

How bad is it?

RSA	LOGICAL QUBITS
RSA 2048	**372**
RSA 3072	
RSA 7680	

Logical qubits are not total qubits!



Yan et al. (2022), *Factoring integers with sublinear resources on a superconducting quantum processor*
Tommaso Gagliardoni (2021), *Quantum Attack Resource Estimate*

Ezratty, Olivier. (2023). *Is there a Moore's law for quantum computing?*

Push for PQ-transition

«In order to [..] prepare for the security threats caused by quantum computers [..] we intend to select a quantum resistant algorithm through the *KpqC Competition*. »

KPQC call for standardisation, Nov. 2021

Push for PQ-transition

«[..] quantum computers [..] break [..] cryptography, [..] the Biden-Harris Administration is preparing for [..] risks to government and critical infrastructure»

White House Memorandum, Nov. 2022

«In order to [..] prepare for the security threats caused by quantum computers [..] we intend to select a quantum resistant algorithm through the *KpqC Competition*. »

KPQC call for standardisation, Nov. 2021

Push for PQ-transition

«[..] quantum computers [..] break [..] cryptography, [..] the Biden-Harris Administration is preparing for [..] risks to government and critical infrastructure»

White House Memorandum, Nov. 2022

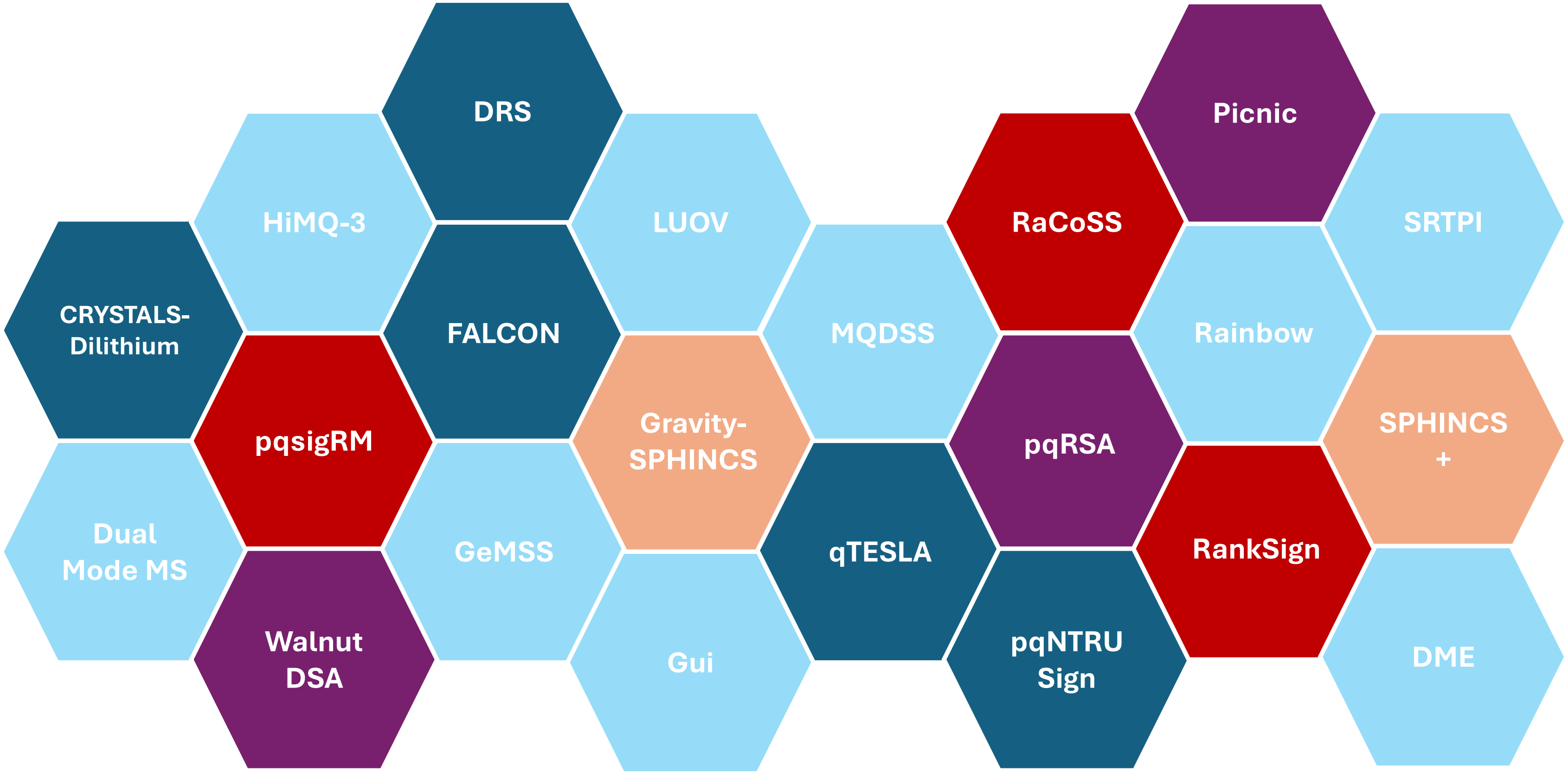
«This [..] encourages [..] a coordinated [..] transition among the different Member States and their public sectors [..] and critical infrastructures [..].»

Commission Recommendation, Apr. 2024

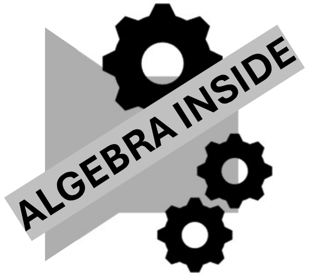
«In order to [..] prepare for the security threats caused by quantum computers [..] we intend to select a quantum resistant algorithm through the *KpqC Competition*. »

KPQC call for standardisation, Nov. 2021

NIST candidates


DRS
HiMQ-3
LUOV
Picnic
RaCoSS
SRTPI
CRYSTALS-Dilithium
FALCON
MQDSS
Rainbow
pqsigRM
Gravity-SPHINCS
pqRSA
SPHINCS +
Dual Mode MS
GeMSS
qTESLA
RankSign
Walnut DSA
Gui
pqNTRU Sign
DME

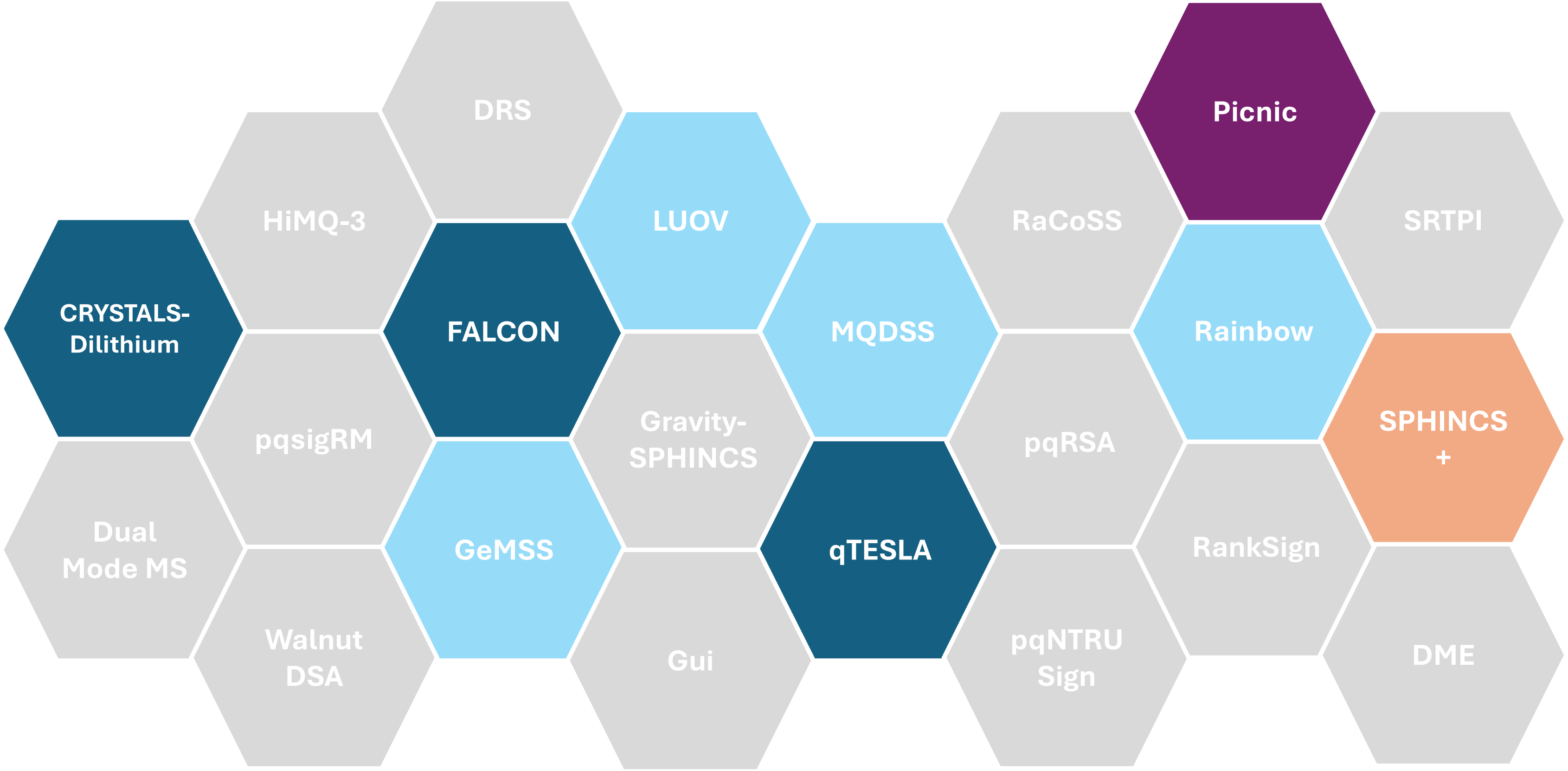
- 🟦 Lattices
- 🟥 Codes
- 🟧 Hash
- 🟦 Multivariate
- 🟪 Others



NIST candidates: round 1

- 🟦 Lattices
- ⬜ Codes
- 🟧 Hash
- 🟦 Multivariate
- 🟪 Others

ALGEBRA INSIDE



DRS

Picnic

HiMQ-3

LUOV

RaCoSS

SRTPI

CRYSTALS-Dilithium

FALCON

MQDSS

Rainbow

pqsigRM

Gravity-SPHINCS

pqRSA

SPHINCS+

Dual Mode MS

GeMSS

qTESLA

RankSign

Walnut DSA

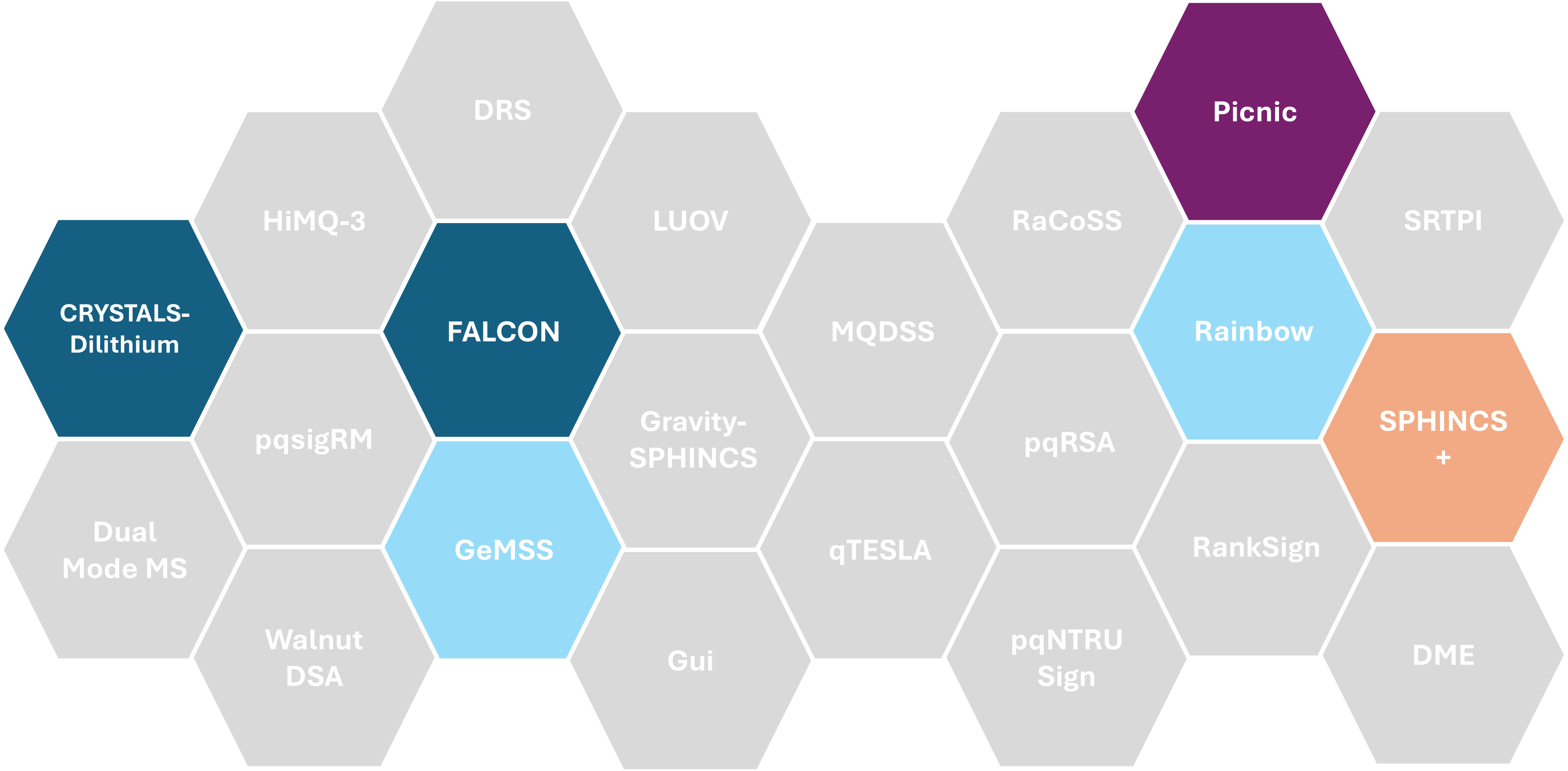
Gui

pqNTRU Sign

DME

NIST candidates: round 2

- 🟦 Lattices
- ⬜ Codes
- 🟧 Hash
- 🟦 Multivariate
- 🟪 Others



CRYSTALS-Dilithium

Dual Mode MS

HiMQ-3

pqsigRM

Walnut DSA

DRS

FALCON

GeMSS

LUOV

Gravity-SPHINCS

Gui

MQDSS

qTESLA

RaCoSS

pqRSA

pqNTRU Sign

Picnic

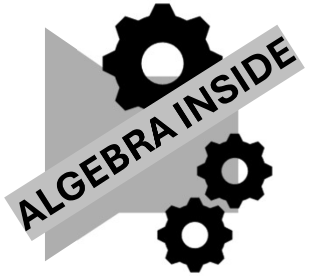
Rainbow

RankSign

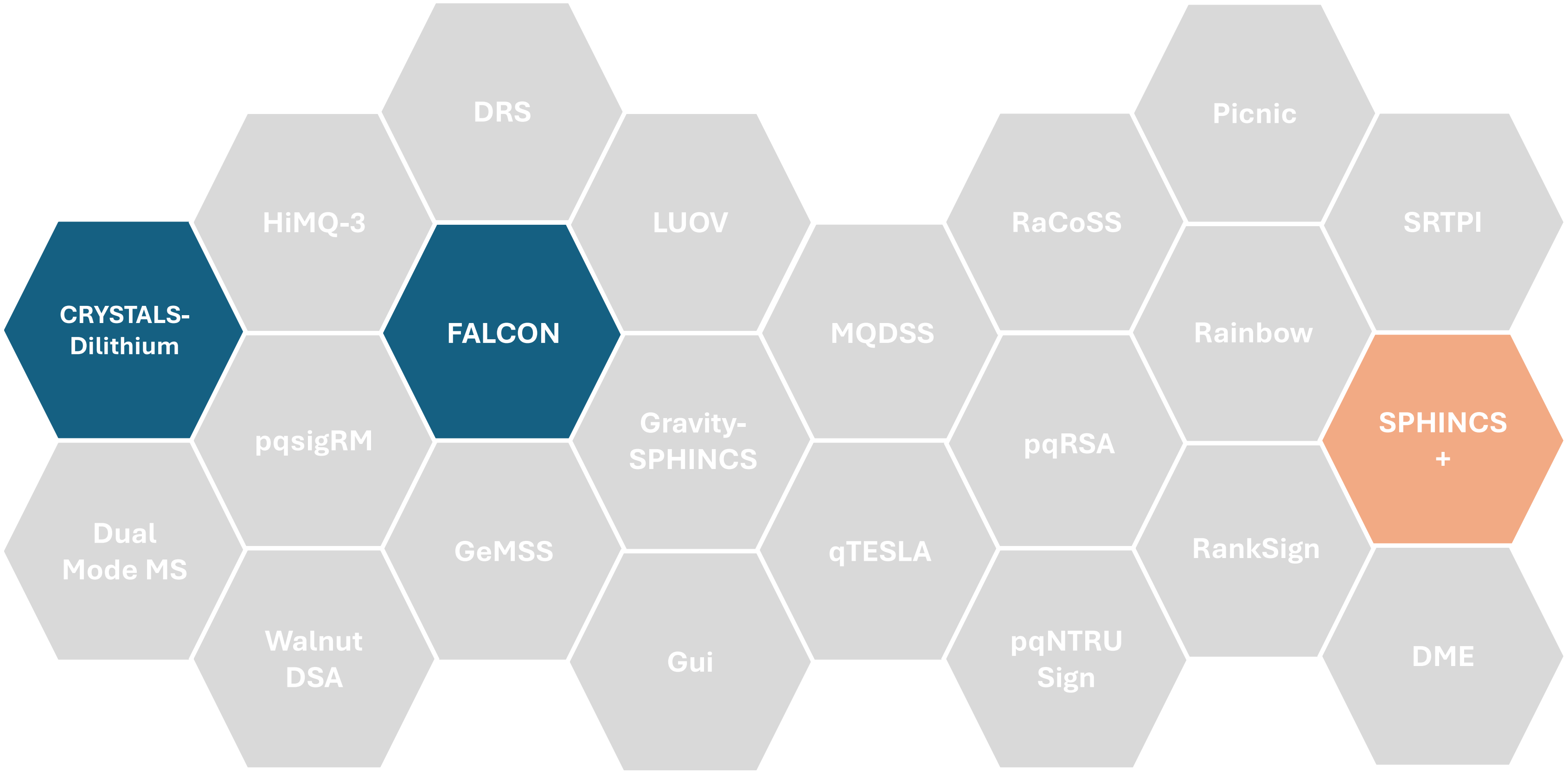
SRTPI

SPHINCS +

DME



NIST candidates: winners


CRYSTALS-Dilithium

Dual Mode MS

HiMQ-3

pqsigRM

Walnut DSA

DRS

FALCON

GeMSS

LUOV

Gravity-SPHINCS

Gui

MQDSS

qTESLA

RaCoSS

pqRSA

pqNTRU Sign

Picnic

Rainbow

RankSign

SRTPI

SPHINCS +

DME

- 🟦 Lattices
- ⬜ Codes
- 🟧 Hash
- ⬜ Multivariate
- ⬜ Others

ALGEBRA INSIDE

The toll of PQ-resistance

- ⊕ PQ-resistance
- ⊕ diversification

- ⊖ computational effort*
- ⊖ memory effort*
- ⊖ compatibility*

* widely varies between standards

XRP turns PQ-resistant

⊕ PQ-resistance

⊕ diversification

⊖ computational effort*

⊖ memory effort*

⊖ compatibility*

ripple | University Blockchain Research Initiative

UNIVERSITÀ DI TRENTO

rippleLabs

* widely varies between standards

XRP turns PQ-resistant

⊖ compatibility*

which standards?

⊖ computational effort*

⊖ memory effort*

which parameters?

ripple | University Blockchain Research Initiative

UNIVERSITÀ DI TRENTO

rippleLabs

Joint projects

- identifying promising **PQ signatures**
- studying the efficiency of **threshold signatures**
- **more?**

ripple | University Blockchain Research Initiative

UNIVERSITÀ DI TRENTO

rippleLabs

Joint projects

DE CIFRIS

Politecnico di Torino

1859

Thank you! Any questions?

ripple | University Blockchain Research Initiative

UNIVERSITÀ DI TRENTO

rippleLabs