Revisiting cycles of pairing-friendly elliptic curves

Marta Bellés
marta@dusk.network

Joint work with Jorge Jimenez-Urroz and Javier Silva

DUSK
Universitat Pompeu Fabra Barcelona

1. THE PROBLEM

THE 2-CYCLE PROBLEM

Find two (ordinary) elliptic curves $E/\mathbb{F}_q$ and $E'/\mathbb{F}_p$ such that

$$|E(\mathbb{F}_q)| = p \text{ and } |E'(\mathbb{F}_p)| = q.$$

base field order

scalar field order

THE 2-CYCLE PROBLEM

Find two elliptic curves $E/\mathbb{F}_q$ and $E'/\mathbb{F}_p$ such that

$$|E(\mathbb{F}_q)| = p \text{ and } |E'(\mathbb{F}_p)| = q.$$

EASY

THE PAIRING-FRIENDLY 2-CYCLE PROBLEM

Find two elliptic curves $E/\mathbb{F}_q$ and $E'/\mathbb{F}_p$ such that

$$|E(\mathbb{F}_q)| = p \text{ and } |E'(\mathbb{F}_p)| = q,$$

with *low* embedding degree (*pairing-friendly*).

THE PAIRING-FRIENDLY 2-CYCLE PROBLEM

Find two elliptic curves $E/\mathbb{F}_q$ and $E'/\mathbb{F}_p$ such that

$$|E(\mathbb{F}_q)| = p \text{ and } |E'(\mathbb{F}_p)| = q,$$

with *low* embedding degree (*pairing-friendly*).

Embedding degree

- E: smallest k such that $p \mid q^k - 1$.
- E': smallest l such that $q \mid p^l - 1$.

Pairing

- *Small* embedding degree: DL attacks
- *Large* embedding degree: inefficiency

THE PAIRING-FRIENDLY 2-CYCLE PROBLEM

Find two elliptic curves $E/\mathbb{F}_q$ and $E'/\mathbb{F}_p$ such that

$$|E(\mathbb{F}_q)| = p \text{ and } |E'(\mathbb{F}_p)| = q,$$

with *low* embedding degree (*pairing-friendly*).

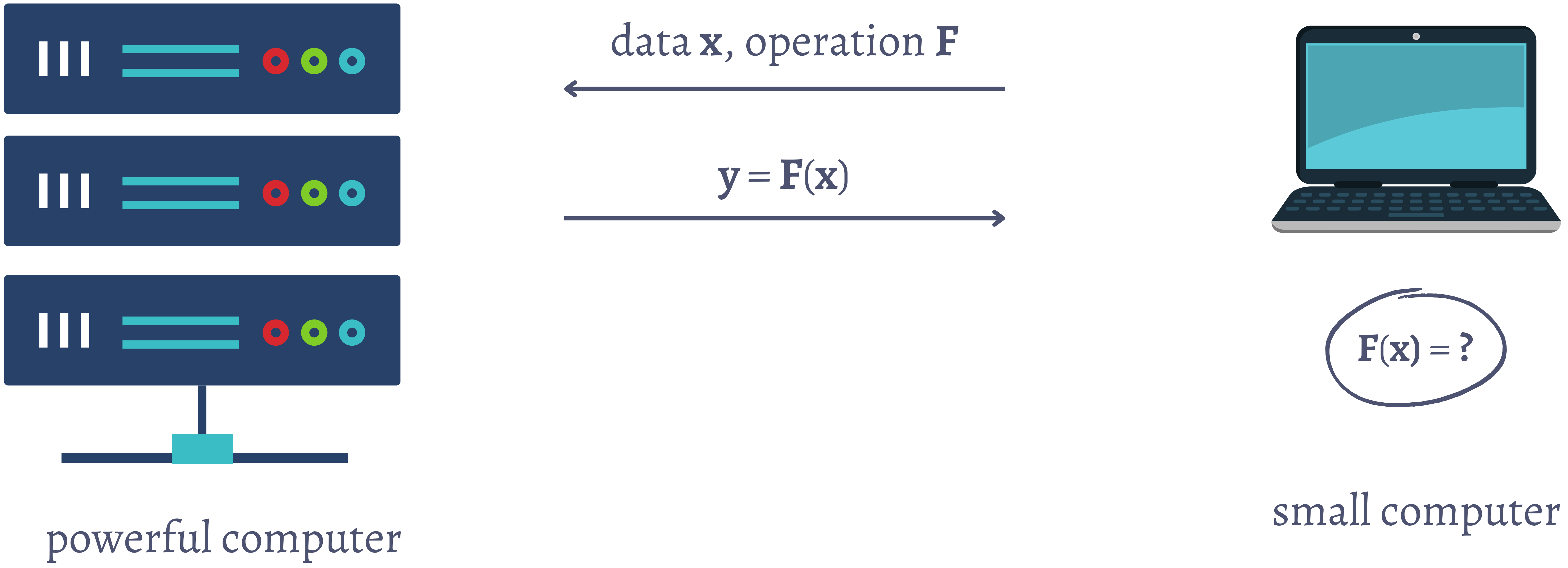
DIFFICULT

2. MOTIVATION

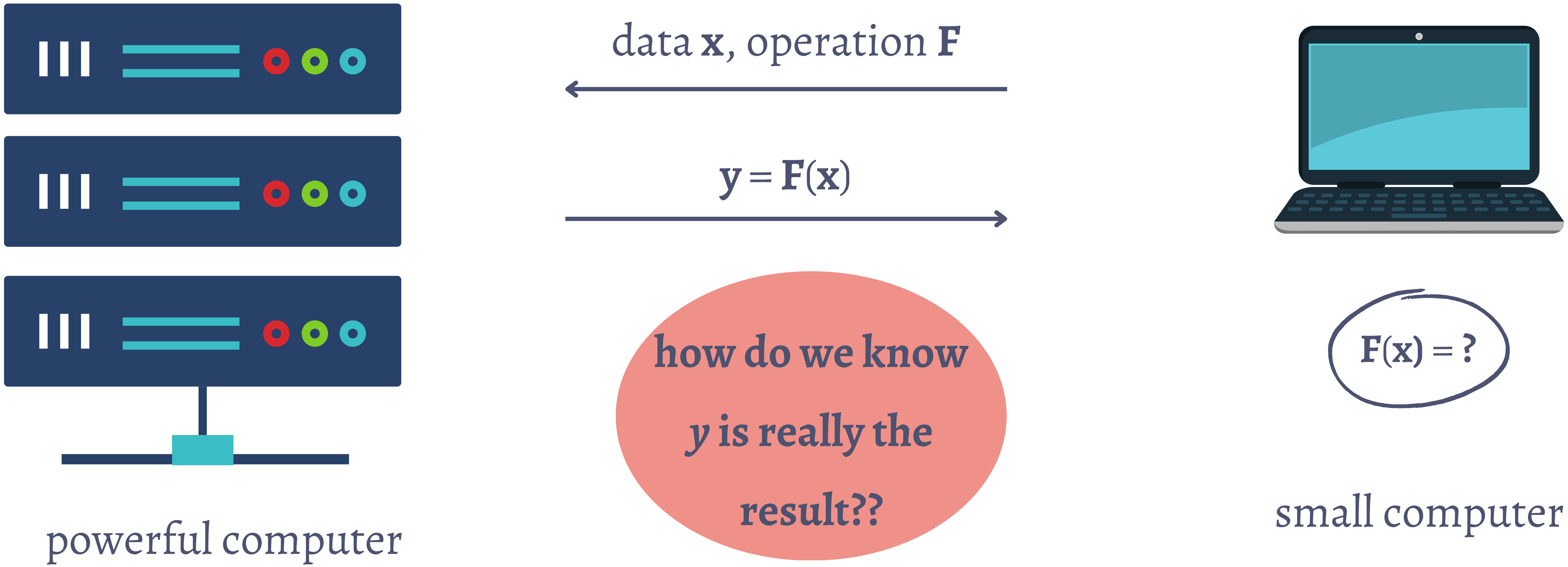
VERIFIABLE COMPUTATION

$F(x) = ?$

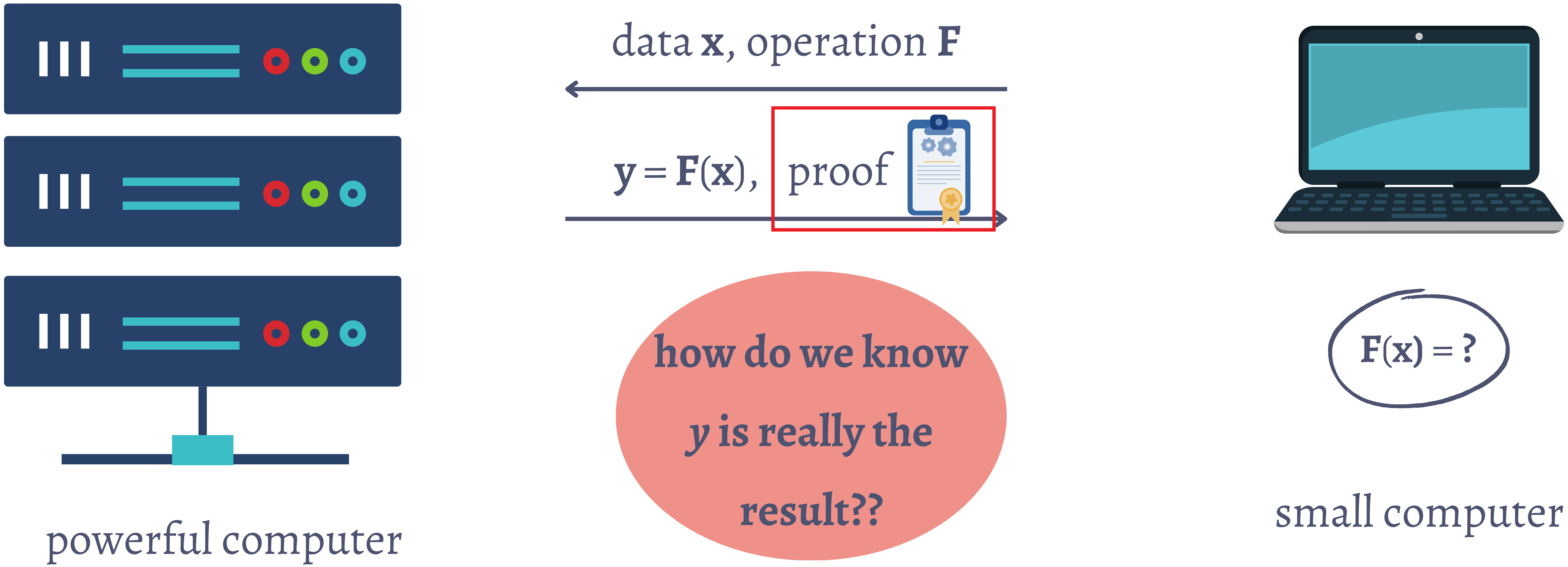
VERIFIABLE COMPUTATION



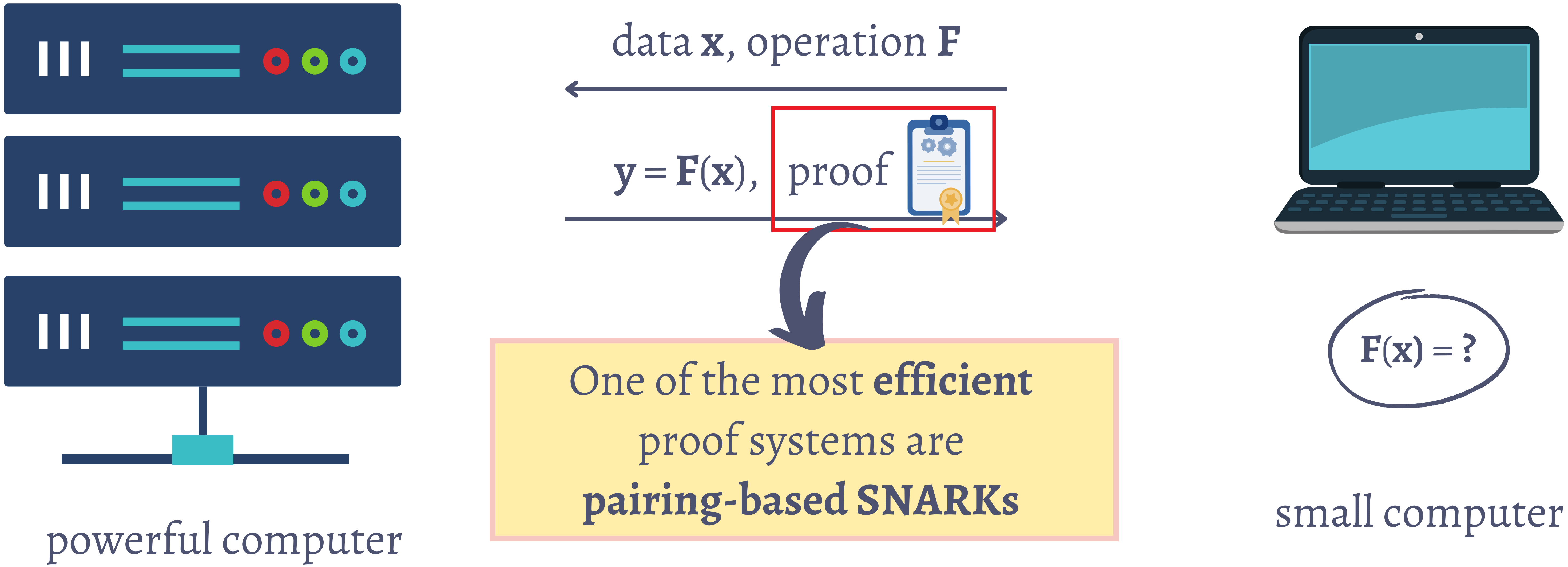
VERIFIABLE COMPUTATION



VERIFIABLE COMPUTATION



VERIFIABLE COMPUTATION

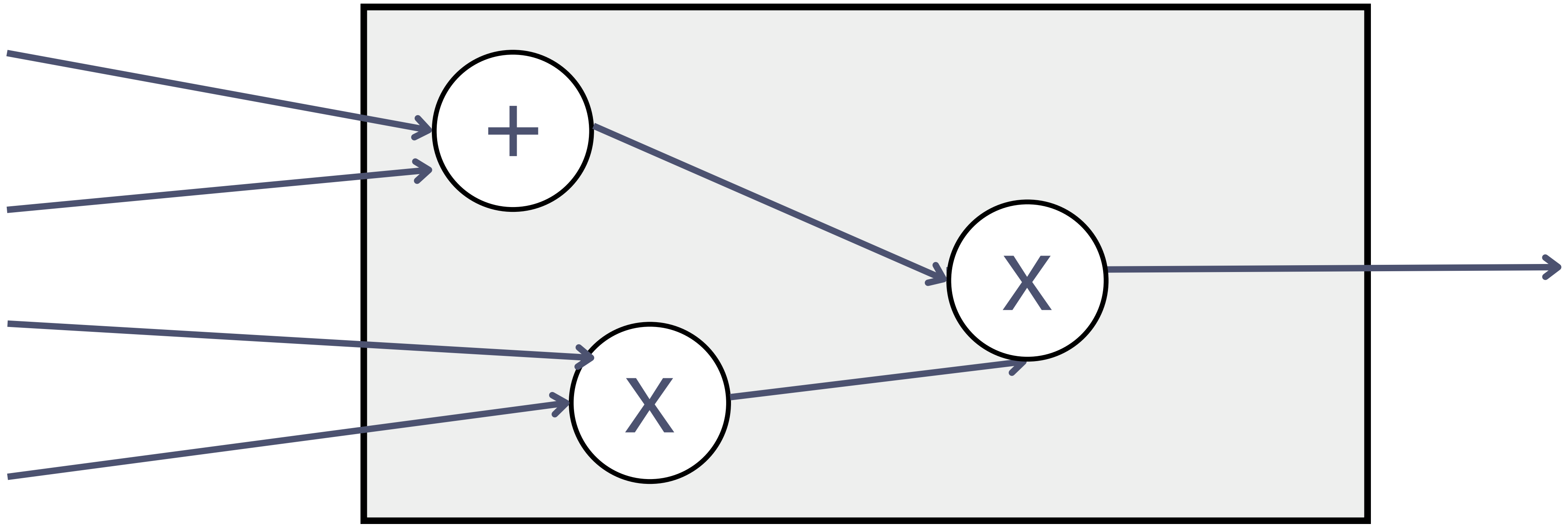


PAIRING-BASED SNARKS PROOF SYSTEMS

- **proof is small**
- **fast verification**

$\mathbb{F}_p$-ARITHMETIC CIRCUIT SATISFIABILITY

inputs
(elements of $\mathbb{F}_p$)



outputs
(elements of $\mathbb{F}_p$)

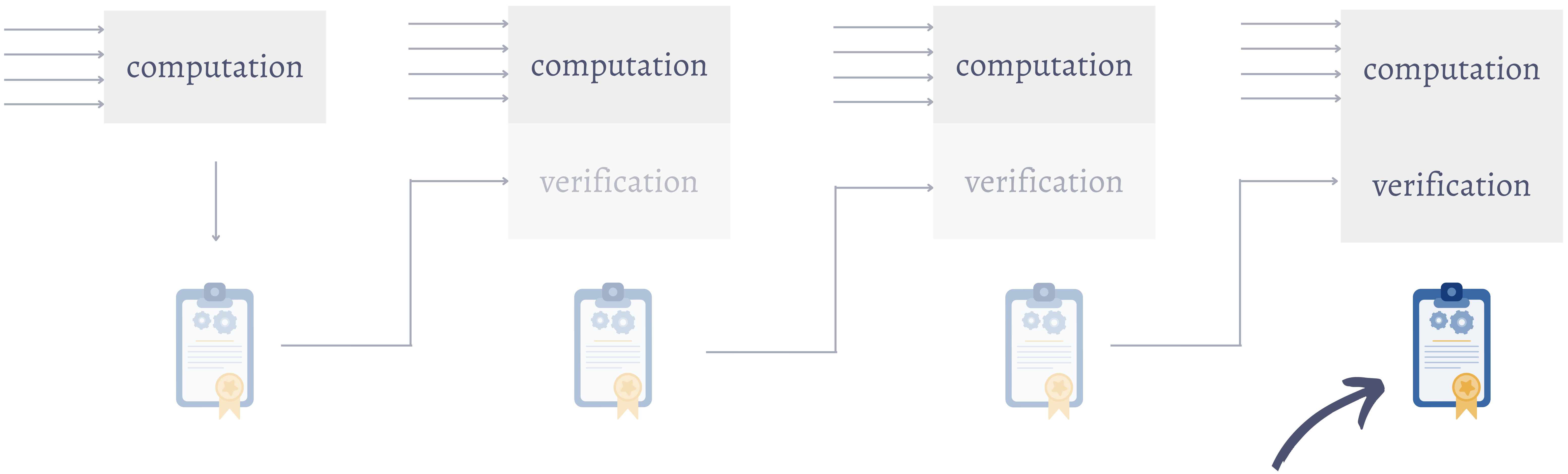
circuit
(arithmetic modulo p)

A **proof** asserts that a set of **inputs** and **outputs** satisfy the relations defined in the **circuit**.

PAIRING-BASED SNARKS PROOF SYSTEMS

$\mathbb{F}_p$-arithmetic circuit

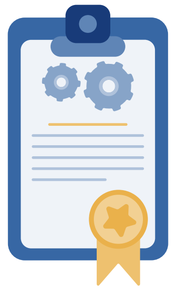
RECURSIVE PROOF COMPOSITION



By verifying one single proof, we can verify that all computations (and proofs) are correct.

PAIRING-BASED SNARKS PROOF SYSTEMS

$\mathbb{F}_p$-arithmetic circuit



Pairs (x,y) in $\mathbb{F}_q^2$.

Prover

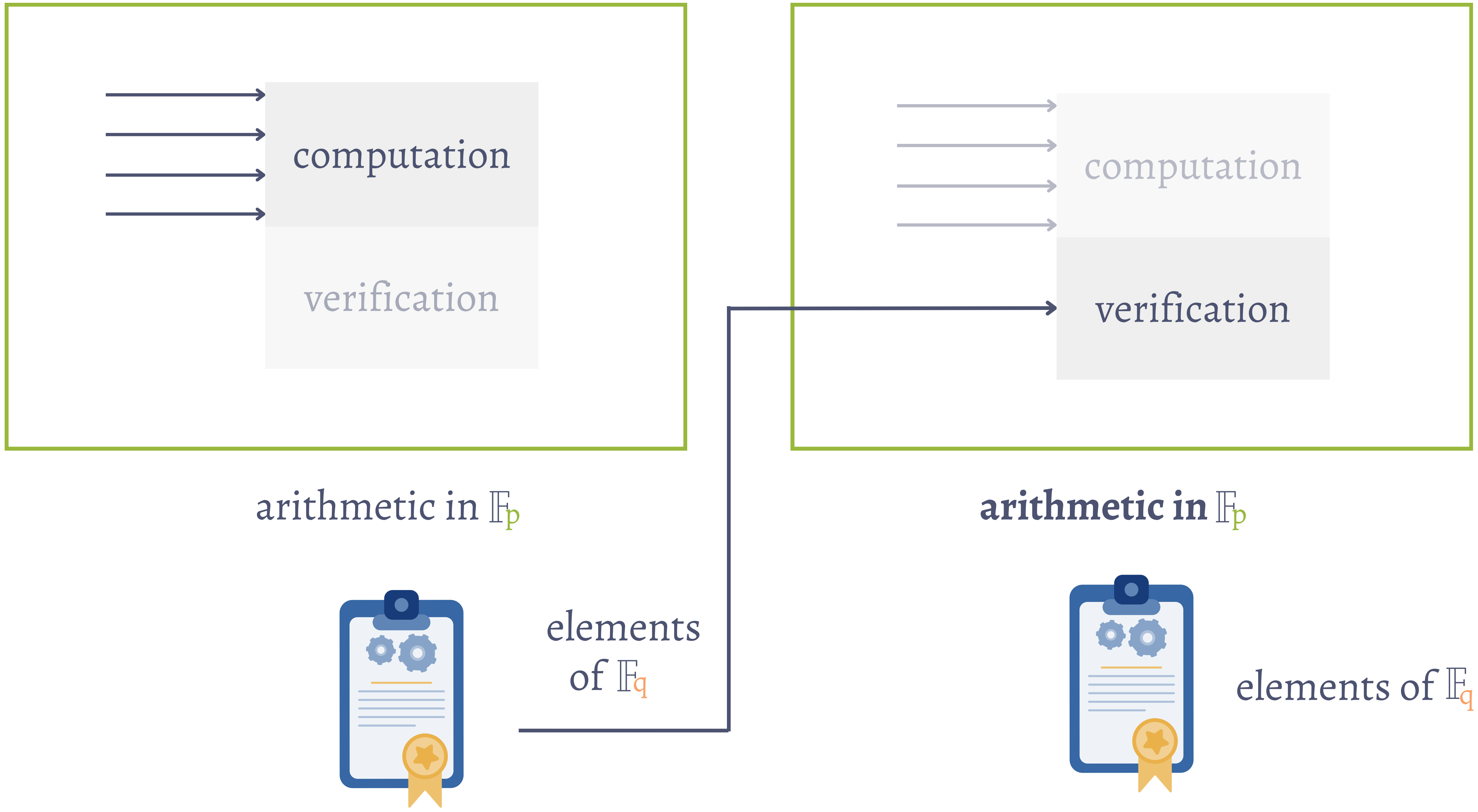
Elliptic curve $E/\mathbb{F}_q$ such that $|E(\mathbb{F}_q)| = p$.

Verifier

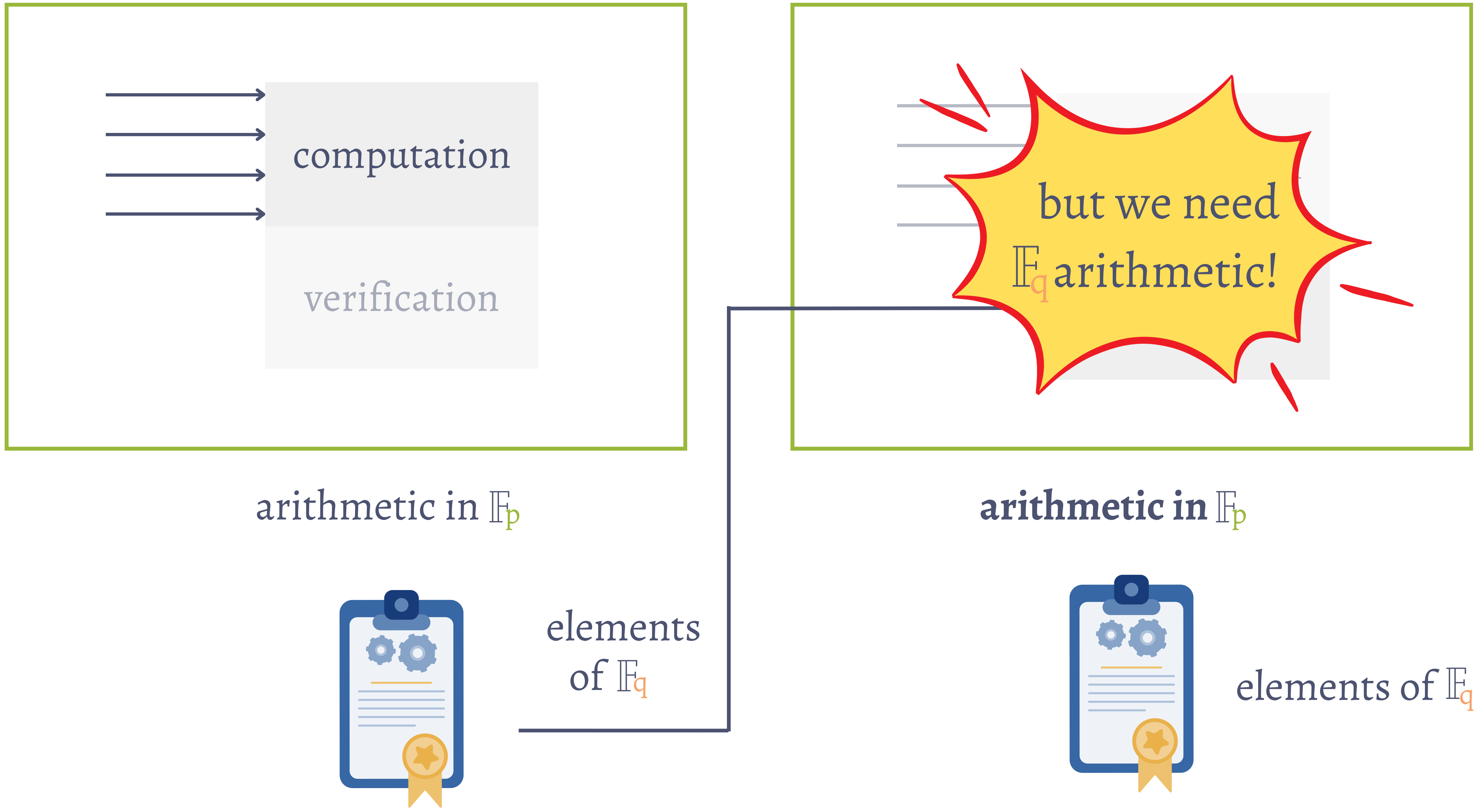
It needs to be efficient!

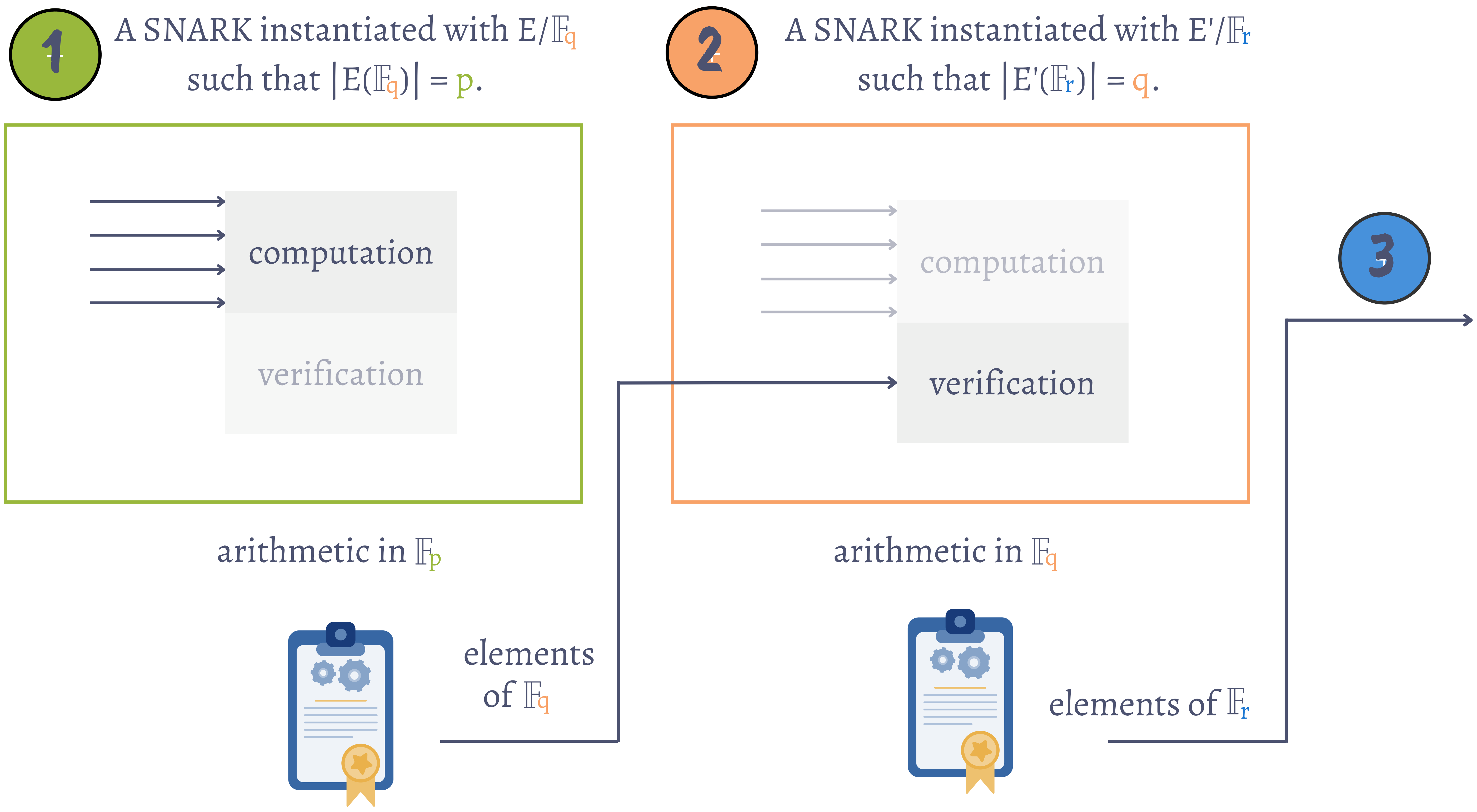
Pairing operation on points of E (arithmetic over $\mathbb{F}_q$).

1 A SNARK instantiated with $E/\mathbb{F}_q$ such that $|E(\mathbb{F}_q)| = p$.

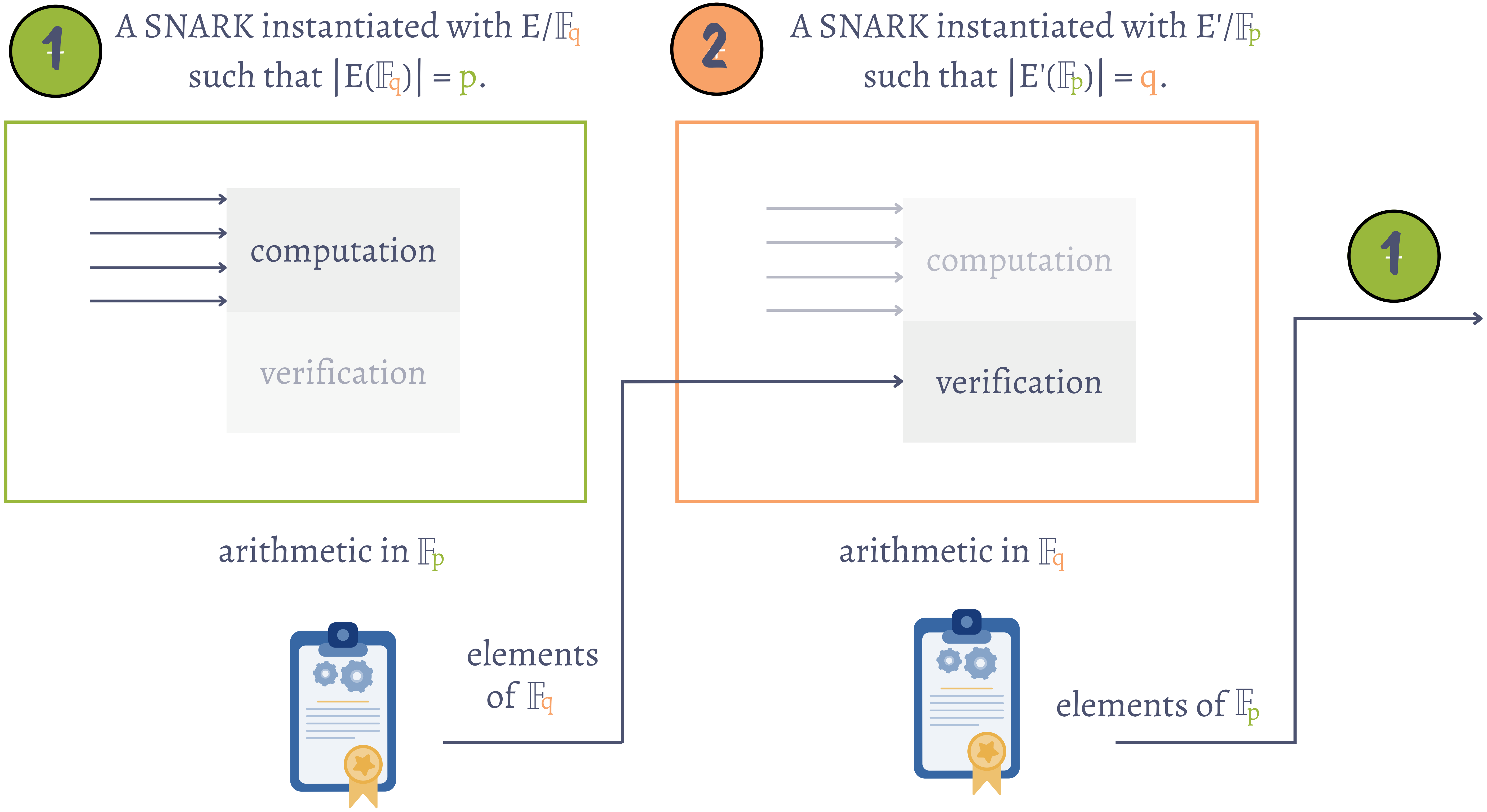


1 A SNARK instantiated with $E/\mathbb{F}_q$ such that $|E(\mathbb{F}_q)| = p$.





1
A SNARK instantiated with $E/\mathbb{F}_q$
such that $|E(\mathbb{F}_q)| = p$.
computation
verification
arithmetic in $\mathbb{F}_p$
elements of $\mathbb{F}_q$
2
A SNARK instantiated with $E'/\mathbb{F}_r$
such that $|E'(\mathbb{F}_r)| = q$.
computation
verification
arithmetic in $\mathbb{F}_q$
elements of $\mathbb{F}_r$
3


1
A SNARK instantiated with $E/\mathbb{F}_q$
such that $|E(\mathbb{F}_q)| = p$.
2
A SNARK instantiated with $E'/\mathbb{F}_p$
such that $|E'(\mathbb{F}_p)| = q$.
computation
verification
computation
verification
1
arithmetic in $\mathbb{F}_p$
arithmetic in $\mathbb{F}_q$
elements of $\mathbb{F}_q$
elements of $\mathbb{F}_p$

1 A SNARK instantiated with $E/\mathbb{F}_q$ such that $|E(\mathbb{F}_q)| = p$.

2 A SNARK instantiated with $E'/\mathbb{F}_p$ such that $|E'(\mathbb{F}_p)| = q$.

THE PAIRING-FRIENDLY 2-CYCLE PROBLEM

Find two elliptic curves $E/\mathbb{F}_q$ and $E'/\mathbb{F}_p$ such that

$$|E(\mathbb{F}_q)| = p \text{ and } |E'(\mathbb{F}_p)| = q,$$

with *low* embedding degree (*pairing-friendly*).

3. WHAT WAS KNOWN

CONDITIONS

- **Curves involved in a cycle must be of prime order.**
- The only known method to produce prime-order curves is via **families of curves parameterized by polynomials** **q**(X), **p**(X), and **t**(X) with embedding degree *k* and discriminant *d*. This means:

1. **p**(X) = **q**(X) + 1 - **t**(X).
2. **p**(X) is integer-valued.
3. **p**(X) and **q**(X) represent primes.
4. **p**(X) | Φ_k(**t**(X) - 1).
5. The equation 4**q**(X) = **t**(X)^2 + |d|Y^2 has infinitely many integer solutions *(x,y)*.

$\xrightarrow{(1\text{-}3)}$ infinitely many parameters compatible with elliptic curves

$\xrightarrow{(4)}$ the embedding degree is at most *k*

$\xrightarrow{(5)}$ infinitely many curves in the family with same discriminant

FAMILIES OF PAIRING-FRIENDLY CURVES OF PRIME ORDER

- There are **no elliptic curves with prime order** and embedding degree **$k < 3$**.
- For **$k = 3, 4, 6$** we have the families of curves Miyaji-Nakabayashi-Takano (**MNT**).

  (exhaustive)

MNT3	$p(X) = 12X^2 - 6X + 1$	$q(X) = 12X^2 - 1$
MNT4	$p(X) = X^2 + 2X + 2$	$q(X) = X^2 + X + 1$
MNT6	$p(X) = 4X^2 - 2X + 1$	$q(X) = 4X^2 + 1$

- For **$k = 10$** we have the **Freeman** family of curves.

Freeman
$$p(X) = 25X^4 + 25X^3 + 15X^2 + 5X + 1$$
$$q(X) = 25X^4 + 25X^3 + 25X^2 + 10X + 3$$

- For **$k = 12$** we have the Barreto-Naehrig (**BN**) family of curves.

BN
$$p(X) = 36X^4 + 36X^3 + 24X^2 + 6X + 1$$
$$q(X) = 36X^4 + 36X^3 + 18X^2 + 6X + 1$$

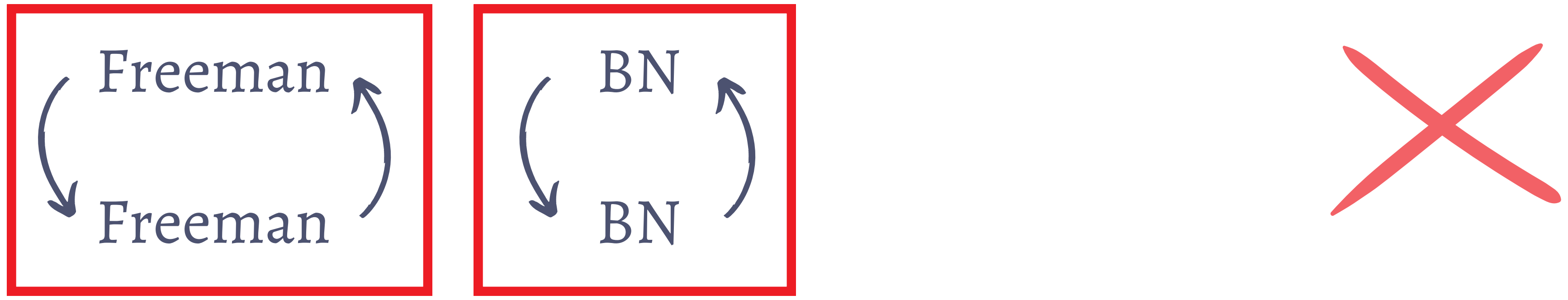
DO THEY FORM CYCLES?

- MNT4 and MNT6 curves **do** form cycles.

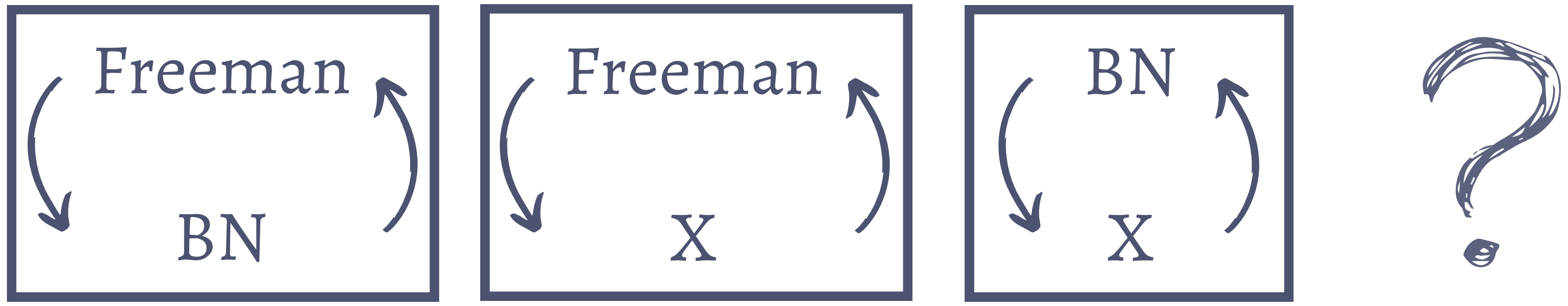
  <u>But:</u> Low embedding degree -> large parameters.

  Unbalanced embedding degrees.

- Freeman and BN curves **do not** form cycles with curves from their own family.



- **Can they form cycles with other curves?**



4. MAIN CONTRIBUTION

THEOREM

Consider a family of elliptic curves with embedding degree k parameterized by polynomials $p(X)$, $q(X)$. Let l be a natural number. Then either:

- $q(X) \mid p(X)^l - 1$, or
- there are at most finitely many 2-cycles formed by a curve form the family and a curve with embedding degree l.

In particular, we did an exhaustive search for the known families of curves.

COROLLARY

Except for the few cases described in the table below, we have that:

- An **MNT3** curve **cannot form 2-cycles** with a curve of embedding degree $l < 23$.
- A **Freeman** curve **cannot form 2-cycles** with a curve of embedding degree $l < 26$.
- A **BN** curve **cannot form 2-cycles** with a curve of embedding degree $l < 33$.

Exceptions

	k	l	q	p
MNT3	3	10	11	19
MNT3	3	10	11	7
BN	12	18	19	13

5. FUTURE WORK

FUTURE WORK

- Improve our bounds (code) to all $k < 56$.
- Generalize our result to s-cycles with $s > 2$.
- Do there exist cycles consisting of elliptic curves with the same embedding degree?

  It is already known that this is not the case for $k = 4, 6, 8, 12$.

You can find more open problems in:

A. Chiesa, L. Chua, M. Weidner, *On cycles of pairing-friendly elliptic curves*, arXiv: 1803.02067.

Revisiting cycles of pairing-friendly elliptic curves

Marta Bellés, Jorge Urroz, Javier Silva

Paper

https://eprint.iacr/2022/1662

Code

https://github.com/pairingfriendlycycles/
pairing-friendly-cycles/tree/main

Revisiting cycles of pairing-friendly elliptic curves

Marta Bellés
marta@dusk.network

Joint work with Jorge Jimenez-Urroz and Javier Silva

DUSK
Universitat Pompeu Fabra Barcelona