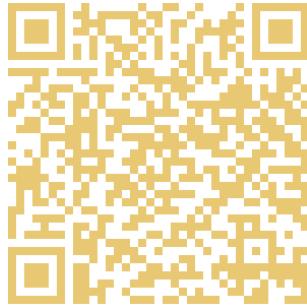


Get these
slides ➔



typst

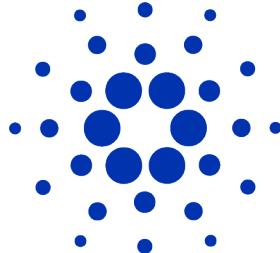
$$\mathcal{L} = \nabla \cdot \mathbf{E} \quad (15)$$

The first term has been chosen to be quadratic in the field tensor because we want to derive a linear field equation in which the superposition theorem holds. The action has to be a scalar, the simplest quadratic scalar is the sum of the two terms of the product given in Eq.

$$S = \frac{1}{2} \int d^3x \frac{1}{\mu_0} \epsilon_{ijk} \partial_i E_j \partial_k E_i \quad (16)$$

The three spatial components of Eq. (26) yield the magnetic induction law

$$\nabla \times \mathbf{B} = \frac{1}{\mu_0} \partial_i \mathbf{E} + \frac{4\pi}{\mu_0} \mathbf{j} \quad (28)$$



Zero-knowledge-proofs - part 1

ENGINEERING WORKSHOP - DEC 2025
(IRELAND)

Pawel Jakubas

Plan of the tutorial

Plan of the tutorial

Let's get a little deeper than usual and understand what main building blocks of ZKP looks like

This tutorial will focus on

Plan of the tutorial

Let's get a little deeper than usual and understand what main building blocks of ZKP looks like

This tutorial will focus on

1. sketching the landscape of what we want to understand during 3-4 parts
- 2.

Plan of the tutorial

Let's get a little deeper than usual and understand what main building blocks of ZKP looks like

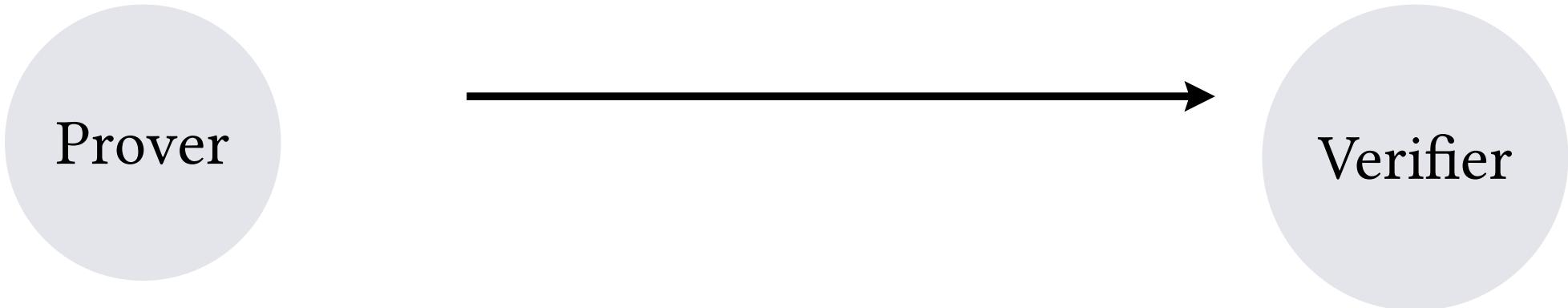
This tutorial will focus on

1. sketching the landscape of what we want to understand during 3-4 parts
2. cover the first part in some detail **elliptic curves**

Verifiable computing vs ZKP (1)

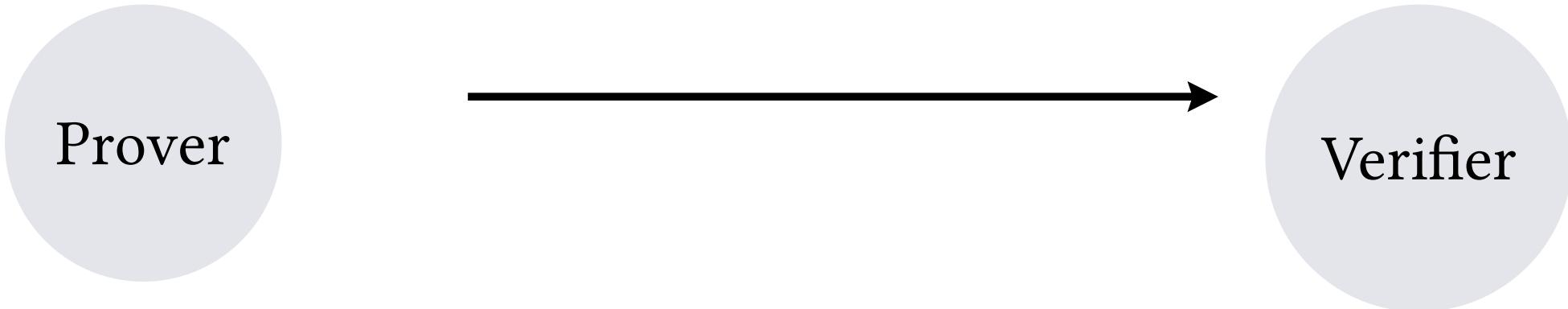
Verifiable computing vs ZKP (1)

There is **asymmetry** built into those systems. It is much easier to get public key from secret. But not the other way



Verifiable computing vs ZKP (1)

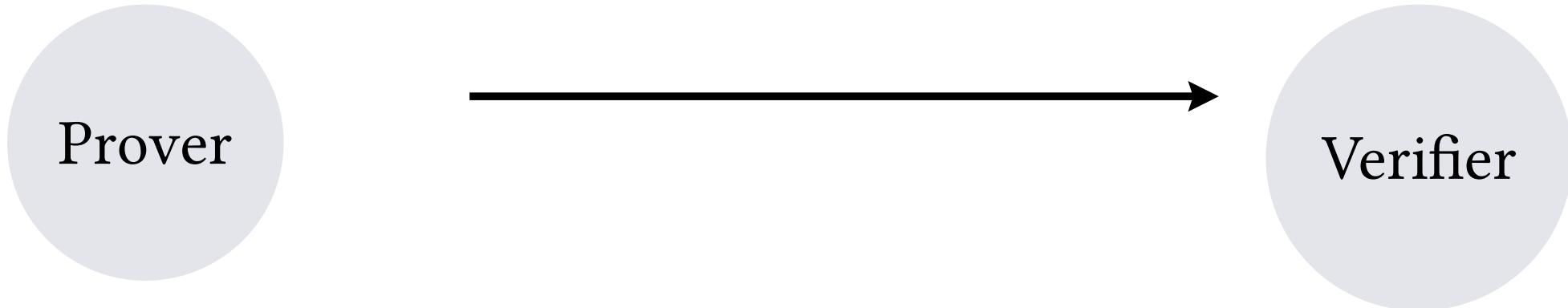
There is **asymmetry** built into those systems. It is much easier to get public key from secret. But not the other way



secret -> (easy) -> public

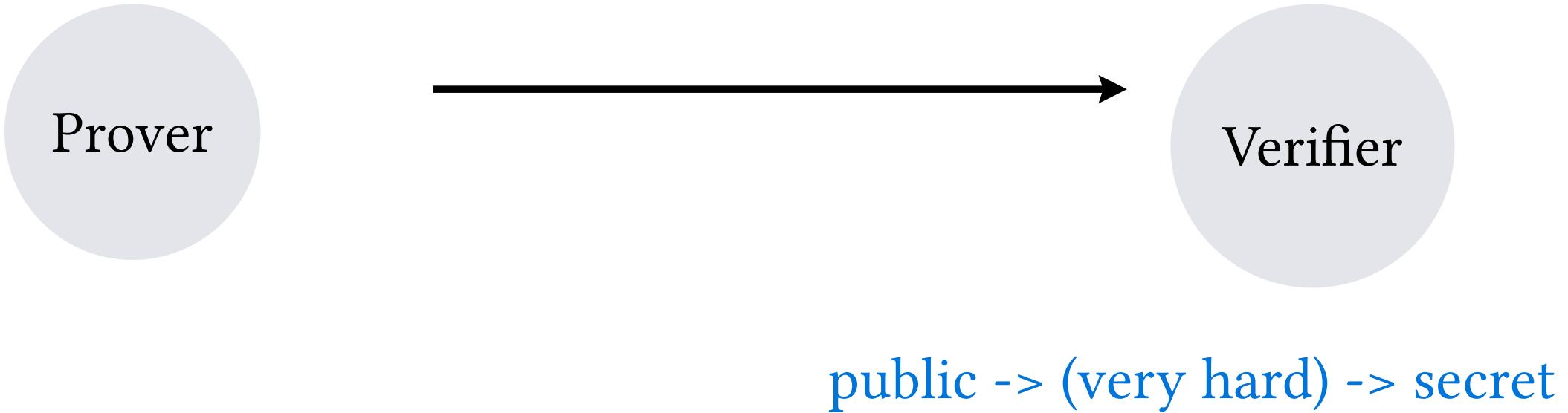
Verifiable computing vs ZKP (1)

There is **asymmetry** built into those systems. It is much easier to get public key from secret. But not the other way



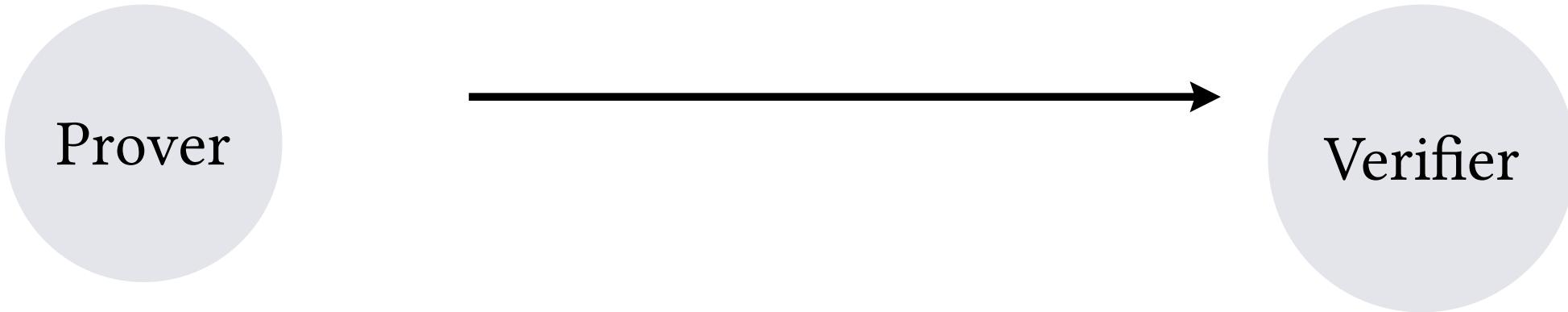
Verifiable computing vs ZKP (1)

There is **asymmetry** built into those systems. It is much easier to get public key from secret. But not the other way



Verifiable computing vs ZKP (1)

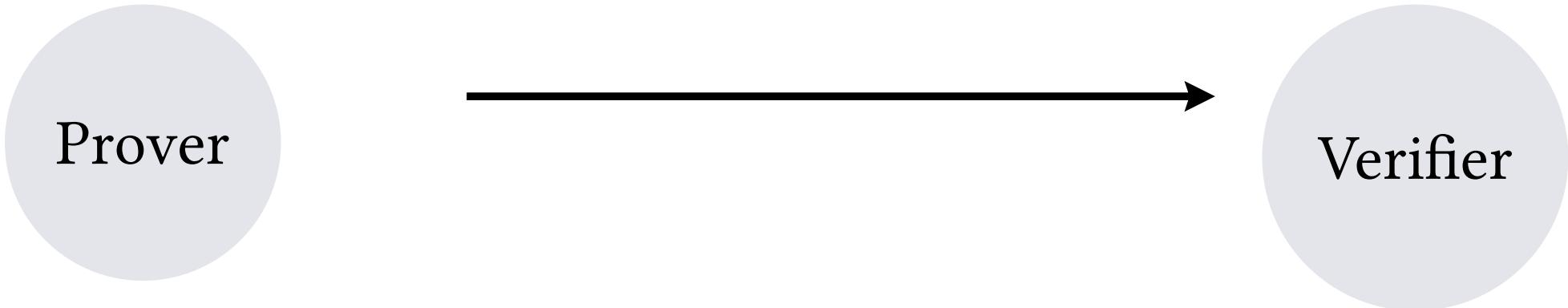
There is **asymmetry** built into those systems. It is much easier to get public key from secret. But not the other way



proof verified using public data

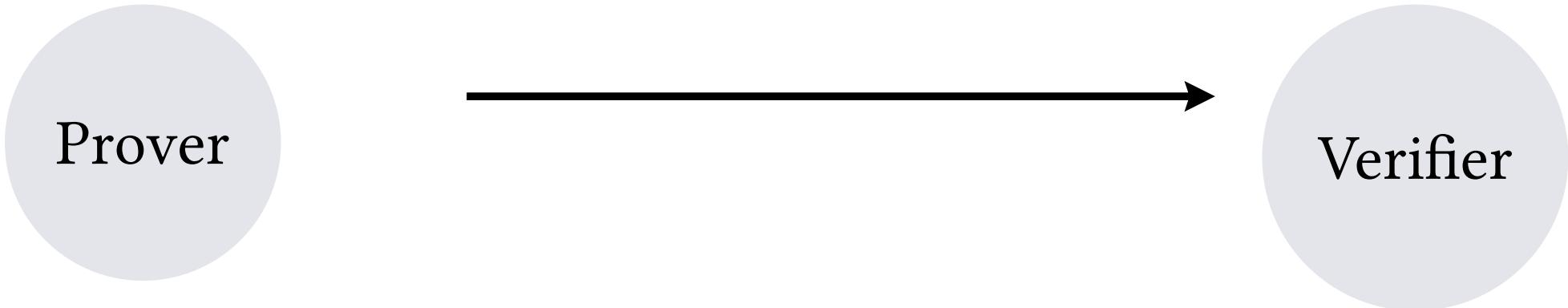
Verifiable computing vs ZKP (2)

There is **asymmetry** built into those systems. It is much quicker to verify than prove something.



Verifiable computing vs ZKP (2)

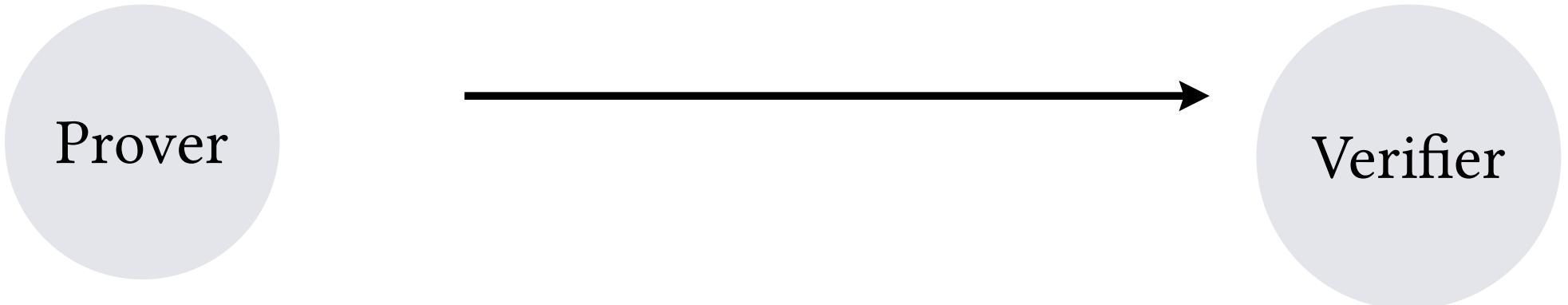
There is **asymmetry** built into those systems. It is much quicker to verify than prove something.



$O(n)$ off-chain

Verifiable computing vs ZKP (2)

There is **asymmetry** built into those systems. It is much quicker to verify than prove something.

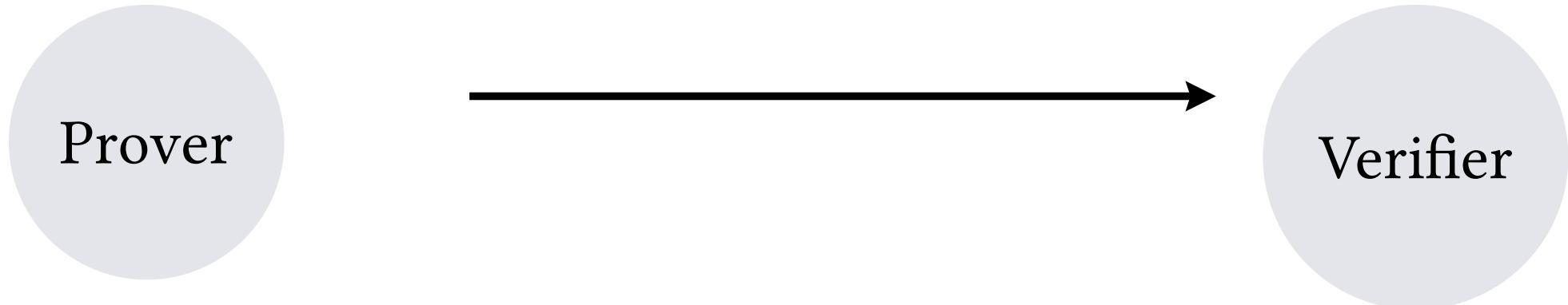


$O(n)$ off-chain

$O(\log n)$ on-chain

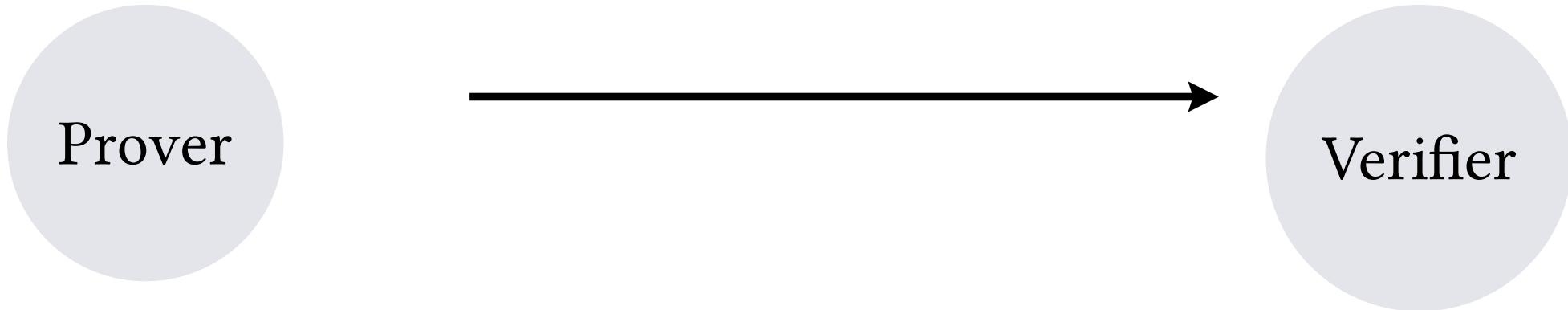
ZKP (3)

Data sent to verifier is compressed, and can be hidden



ZKP (3)

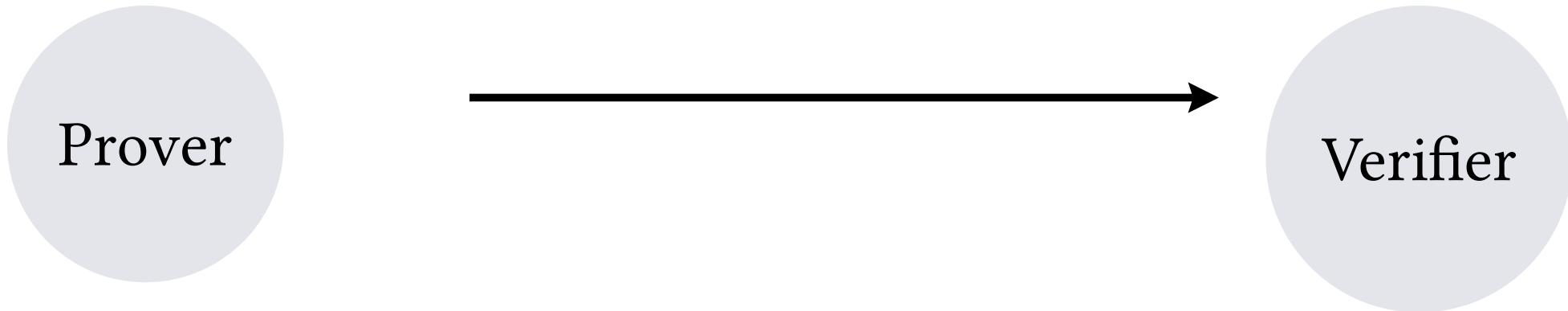
Data sent to verifier is compressed, and can be hidden



size: n

ZKP (3)

Data sent to verifier is compressed, and can be hidden

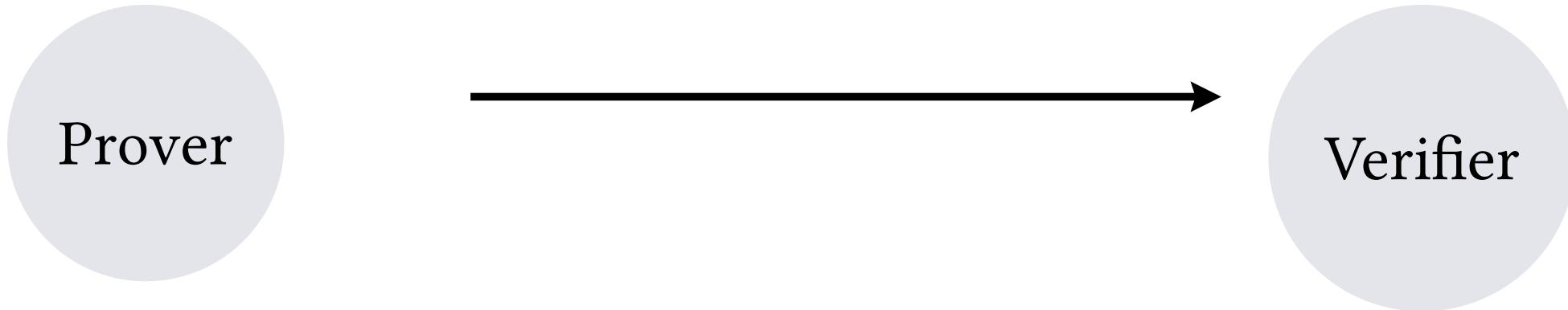


size: n

size: at least $\log n$

ZKP (3)

Data sent to verifier is compressed, and can be hidden



size: n

size: at least $\log n$

size: at least $\log n$

Modular arithmetics (1)

It is about integers.

Modular arithmetics (1)

It is about integers.

Let's assume we arithmetics **mod 8**. It means the possible values are $0, 1, 2, 3, 4, 5, 6, 7$. if we move below or above we need to wrap up.

Modular arithmetics (1)

$$3 + 3 \bmod 8 = 6 \bmod 8$$

$$10 \bmod 8 = 2 \bmod 8$$

$$5 + 5 \bmod 8 = 2 \bmod 8$$

$$5 \cdot 5 \bmod 8 = 25 \bmod 8 = (3 \cdot 8 + 1) \bmod 8 = 1 \bmod 8$$

Modular arithmetics (1)

$$3 + 3 \bmod 8 = 6 \bmod 8$$

$$10 \bmod 8 = 2 \bmod 8$$

$$5 + 5 \bmod 8 = 2 \bmod 8$$

$$5 \cdot 5 \bmod 8 = 25 \bmod 8 = (3 \cdot 8 + 1) \bmod 8 = 1 \bmod 8$$

congruent groups

Modular arithmetics (2)

addition mod 8 multiplication mod 8

0 1 2 3 4 5 6 7 1 2 3 4 5 6 7

1 2 3 4 5 6 7 0 2 4 6 0 2 4 6

2 3 4 5 6 7 0 1 3 6 1 4 7 2 5

3 4 5 6 7 0 1 2 4 0 4 0 4 0 4

4 5 6 7 0 1 2 3 5 2 7 4 1 6 3

5 6 7 0 1 2 3 4 6 4 2 0 6 4 2

6 7 0 1 2 3 4 5 7 6 5 4 3 2 1

7 0 1 2 3 4 5 6

Modular arithmetics (2)

addition mod 8 multiplication mod 8 Let's solve the eq in mod 8:

0 1 2 3 4 5 6 7

1 2 3 4 5 6 7

$$9(2x + 7) - 6 \equiv 2x + 6$$

1 2 3 4 5 6 7 0

2 4 6 0 2 4 6

2 3 4 5 6 7 0 1

3 6 1 4 7 2 5

3 4 5 6 7 0 1 2

4 0 4 0 4 0 4

4 5 6 7 0 1 2 3

5 2 7 4 1 6 3

5 6 7 0 1 2 3 4

6 4 2 0 6 4 2

6 7 0 1 2 3 4 5

7 6 5 4 3 2 1

7 0 1 2 3 4 5 6

Modular arithmetics (2)

addition mod 8 multiplication mod 8 Let's solve the eq in mod 8:

0 1 2 3 4 5 6 7

1 2 3 4 5 6 7

$$9(2x + 7) - 6 \equiv 2x + 6$$

1 2 3 4 5 6 7 0

2 4 6 0 2 4 6

$$19^*2x + 19^*7 - 6 \equiv 2x + 6$$

2 3 4 5 6 7 0 1

3 6 1 4 7 2 5

3 4 5 6 7 0 1 2

4 0 4 0 4 0 4

4 5 6 7 0 1 2 3

5 2 7 4 1 6 3

5 6 7 0 1 2 3 4

6 4 2 0 6 4 2

6 7 0 1 2 3 4 5

7 6 5 4 3 2 1

7 0 1 2 3 4 5 6

Modular arithmetics (2)

addition mod 8 multiplication mod 8 Let's solve the eq in mod 8:

0 1 2 3 4 5 6 7

1 2 3 4 5 6 7

$$9(2x + 7) - 6 \equiv 2x + 6$$

1 2 3 4 5 6 7 0

2 4 6 0 2 4 6

$$19^*2x + 19^*7 - 6 \equiv 2x + 6$$

2 3 4 5 6 7 0 1

3 6 1 4 7 2 5

$$38x + 133 - 6 \equiv 2x + 6 \ # 133 \text{ mod } 8 = 5$$

3 4 5 6 7 0 1 2

4 0 4 0 4 0 4

4 5 6 7 0 1 2 3

5 2 7 4 1 6 3

5 6 7 0 1 2 3 4

6 4 2 0 6 4 2

6 7 0 1 2 3 4 5

7 6 5 4 3 2 1

7 0 1 2 3 4 5 6

Modular arithmetics (2)

addition mod 8 multiplication mod 8 Let's solve the eq in mod 8:

0 1 2 3 4 5 6 7

1 2 3 4 5 6 7

$$9(2x + 7) - 6 \equiv 2x + 6$$

1 2 3 4 5 6 7 0

2 4 6 0 2 4 6

$$19^*2x + 19^*7 - 6 \equiv 2x + 6$$

2 3 4 5 6 7 0 1

3 6 1 4 7 2 5

$$38x + 133 - 6 \equiv 2x + 6 \quad \# \text{ } 133 \text{ mod } 8 = 5$$

3 4 5 6 7 0 1 2

4 0 4 0 4 0 4

$$6x + 5 - 6 \equiv 2x + 6$$

4 5 6 7 0 1 2 3

5 2 7 4 1 6 3

5 6 7 0 1 2 3 4

6 4 2 0 6 4 2

6 7 0 1 2 3 4 5

7 6 5 4 3 2 1

7 0 1 2 3 4 5 6

Modular arithmetics (2)

addition mod 8 multiplication mod 8 Let's solve the eq in mod 8:

0 1 2 3 4 5 6 7

1 2 3 4 5 6 7

$$9(2x + 7) - 6 \equiv 2x + 6$$

1 2 3 4 5 6 7 0

2 4 6 0 2 4 6

$$19^*2x + 19^*7 - 6 \equiv 2x + 6$$

2 3 4 5 6 7 0 1

3 6 1 4 7 2 5

$$38x + 133 - 6 \equiv 2x + 6 \ # 133 \text{ mod } 8 = 5$$

3 4 5 6 7 0 1 2

4 0 4 0 4 0 4

$$6x + 5 - 6 \equiv 2x + 6$$

4 5 6 7 0 1 2 3

5 2 7 4 1 6 3

$$6x + 5 - 6 + 6 \equiv 2x + 6 + 6$$

5 6 7 0 1 2 3 4

6 4 2 0 6 4 2

6 7 0 1 2 3 4 5

7 6 5 4 3 2 1

7 0 1 2 3 4 5 6

Modular arithmetics (2)

addition mod 8 multiplication mod 8 Let's solve the eq in mod 8:

0 1 2 3 4 5 6 7

1 2 3 4 5 6 7

$$9(2x + 7) - 6 \equiv 2x + 6$$

1 2 3 4 5 6 7 0

2 4 6 0 2 4 6

$$19^*2x + 19^*7 - 6 \equiv 2x + 6$$

2 3 4 5 6 7 0 1

3 6 1 4 7 2 5

$$38x + 133 - 6 \equiv 2x + 6 \quad \# 133 \text{ mod } 8 = 5$$

3 4 5 6 7 0 1 2

4 0 4 0 4 0 4

$$6x + 5 - 6 \equiv 2x + 6$$

4 5 6 7 0 1 2 3

5 2 7 4 1 6 3

$$6x + 5 - 6 + 6 \equiv 2x + 6 + 6$$

5 6 7 0 1 2 3 4

6 4 2 0 6 4 2

$$6x + 5 \equiv 2x + 4 \quad \# 12 \text{ mod } 8 = 4$$

6 7 0 1 2 3 4 5

7 6 5 4 3 2 1

$$6x - 2x + 5 - 5 \equiv 2x - 2x + 4 - 5$$

7 0 1 2 3 4 5 6

Modular arithmetics (2)

addition mod 8 multiplication mod 8 Let's solve the eq in mod 8:

0 1 2 3 4 5 6 7

1 2 3 4 5 6 7

$$9(2x + 7) - 6 \equiv 2x + 6$$

1 2 3 4 5 6 7 0

2 4 6 0 2 4 6

$$19^*2x + 19^*7 - 6 \equiv 2x + 6$$

2 3 4 5 6 7 0 1

3 6 1 4 7 2 5

$$38x + 133 - 6 \equiv 2x + 6 \ # 133 \text{ mod } 8 = 5$$

3 4 5 6 7 0 1 2

4 0 4 0 4 0 4

$$6x + 5 - 6 \equiv 2x + 6$$

4 5 6 7 0 1 2 3

5 2 7 4 1 6 3

$$6x + 5 - 6 + 6 \equiv 2x + 6 + 6$$

5 6 7 0 1 2 3 4

6 4 2 0 6 4 2

$$6x + 5 \equiv 2x + 4 \ # 12 \text{ mod } 8 = 4$$

6 7 0 1 2 3 4 5

7 6 5 4 3 2 1

$$6x - 2x + 5 - 5 \equiv 2x - 2x + 4 - 5$$

7 0 1 2 3 4 5 6

Modular arithmetics (2)

addition mod 8

0 1 2 3 4 5 6 7

1 2 3 4 5 6 7 0

2 3 4 5 6 7 0 1

3 4 5 6 7 0 1 2

4 5 6 7 0 1 2 3

5 6 7 0 1 2 3 4

6 7 0 1 2 3 4 5

7 0 1 2 3 4 5 6

multiplication mod 8

1 2 3 4 5 6 7

2 4 6 0 2 4 6

3 6 1 4 7 2 5

4 0 4 0 4 0 4

5 2 7 4 1 6 3

6 4 2 0 6 4 2

7 6 5 4 3 2 1

Let's solve the eq in mod 8:

$$9(2x + 7) - 6 \equiv 2x + 6$$

$$19^*2x + 19^*7 - 6 \equiv 2x + 6$$

$$38x + 133 - 6 \equiv 2x + 6 \ # 133 \text{ mod } 8 = 5$$

$$6x + 5 - 6 \equiv 2x + 6$$

$$6x + 5 - 6 + 6 \equiv 2x + 6 + 6$$

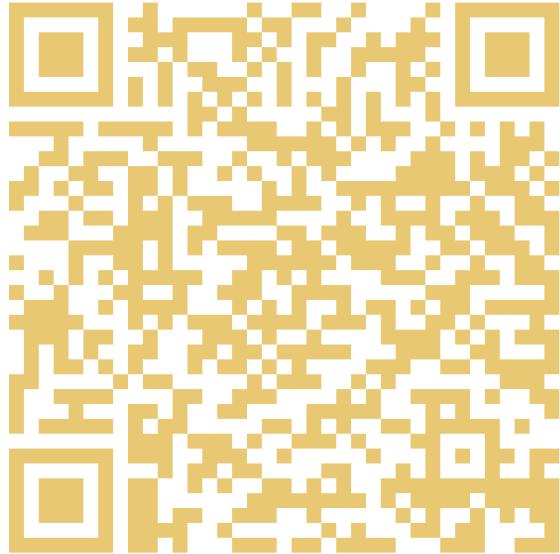
$$6x + 5 \equiv 2x + 4 \ # 12 \text{ mod } 8 = 4$$

$$6x - 2x + 5 - 5 \equiv 2x - 2x + 4 - 5$$

$$4x \equiv 7 \ # -1 \text{ mod } 8 = 7$$

Now we do **NOT have multiplication inverse** for 4, ie. we cannot divide by 4 in modulo 8, ie. solve this equation We have only multiplication inverse for 1 which is 1; 3 which is 3; 5 which is 5, and 7 which is 7.

That's it! More to come in the future



Get in touch 

↗ My notes on GitHub