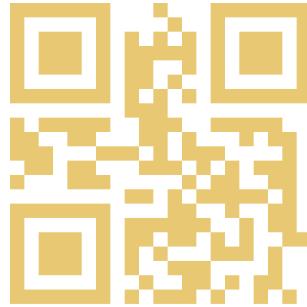


Get these
slides ➔



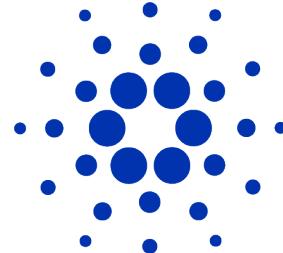
typst

$$\vec{B} = \nabla \times \vec{A} \quad (15)$$

The time dependent part 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 last term of the product given in Eq. (20).

The three spatial components of Eq. (20) yield the magnetic induction law

$$\nabla \times \vec{B} = \frac{1}{c} \frac{\partial \vec{E}}{\partial t} + \frac{4\pi}{c} \vec{j} \quad (28)$$



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

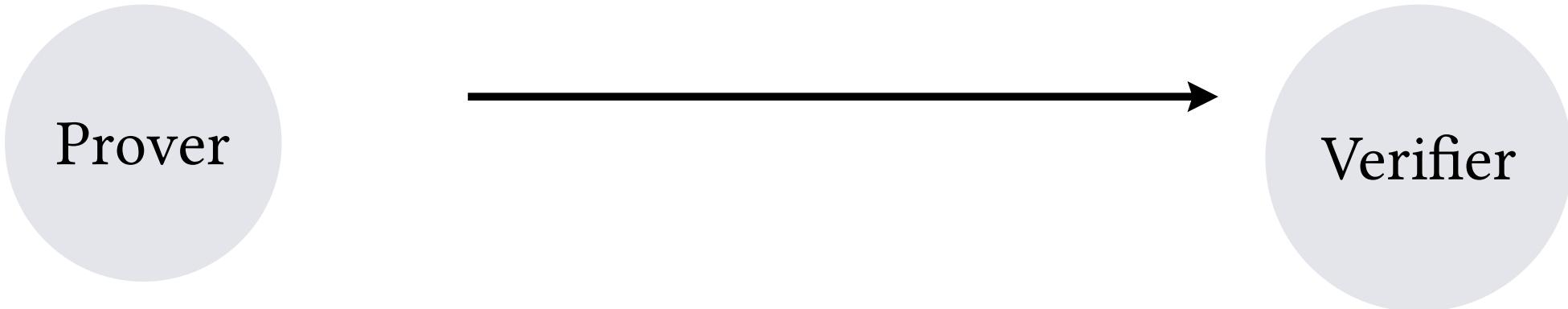
This tutorial will focus on

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)

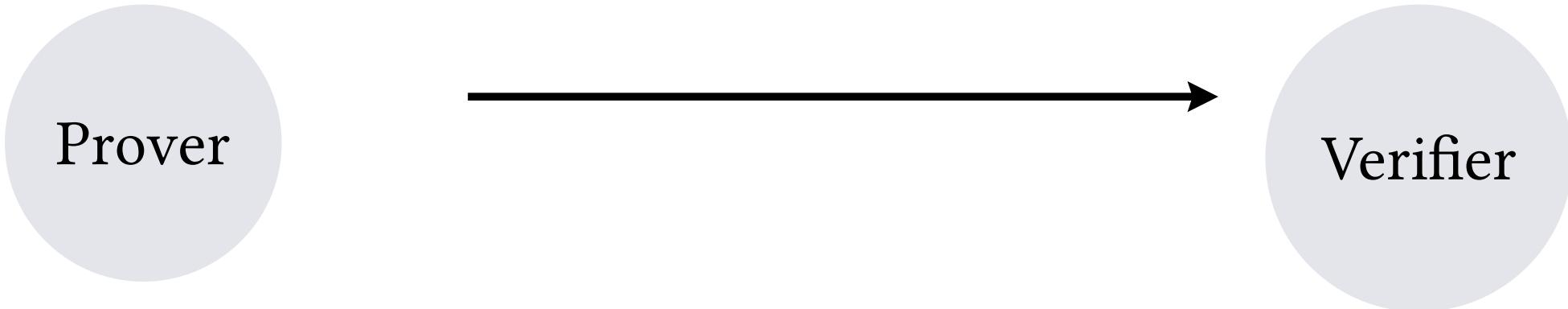
Verifiable computing vs ZKP (1)

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)

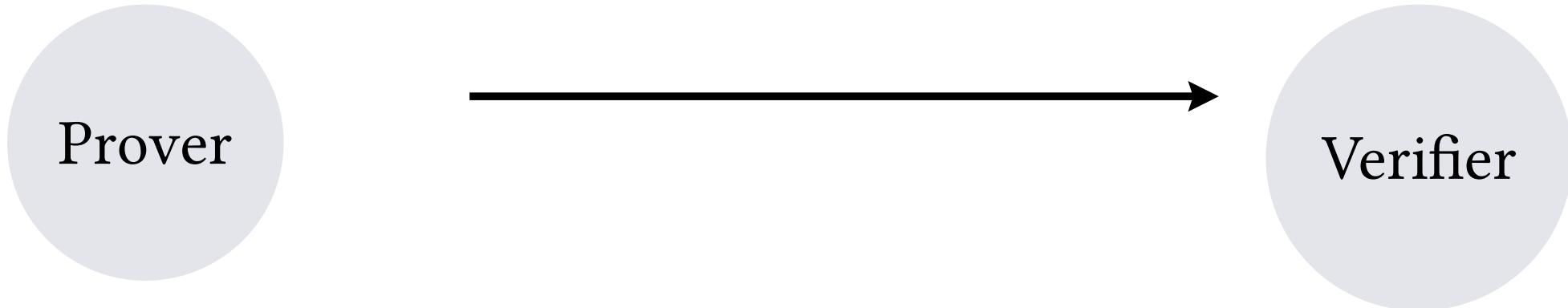
There is **asymmetry** built into those systems. It is much easier to get public key from secret. But not the other way



secret -> (easy) -> public

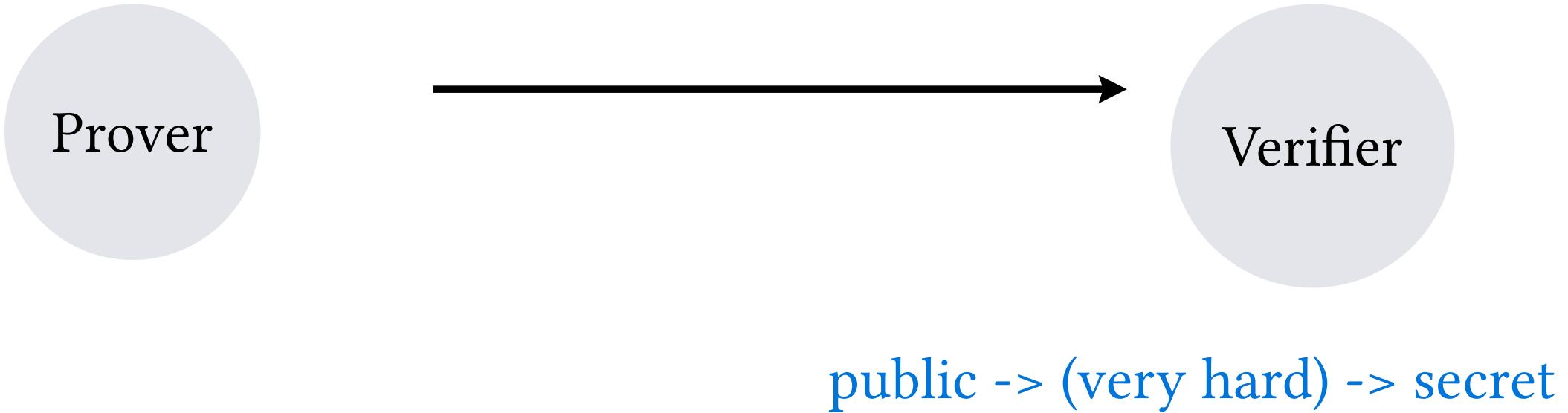
Verifiable computing vs ZKP (1)

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



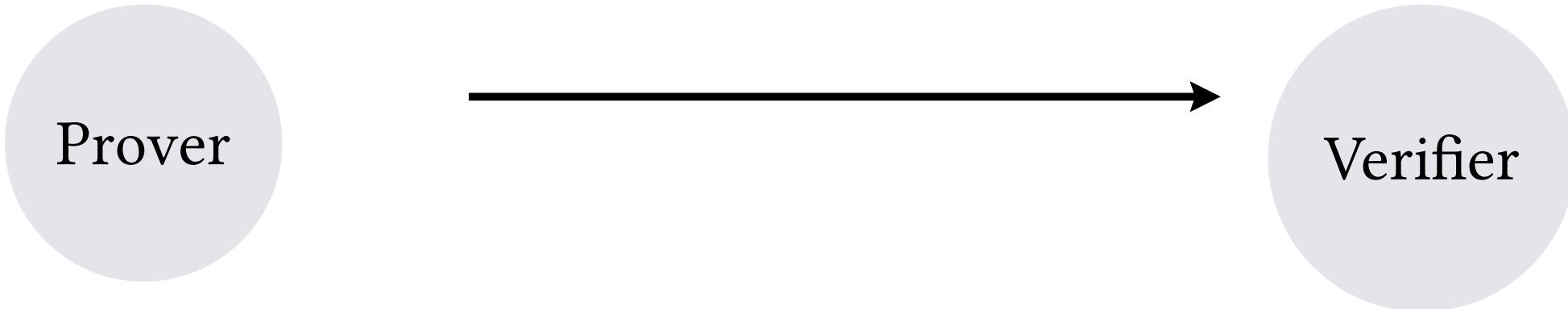
Verifiable computing vs ZKP (1)

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)

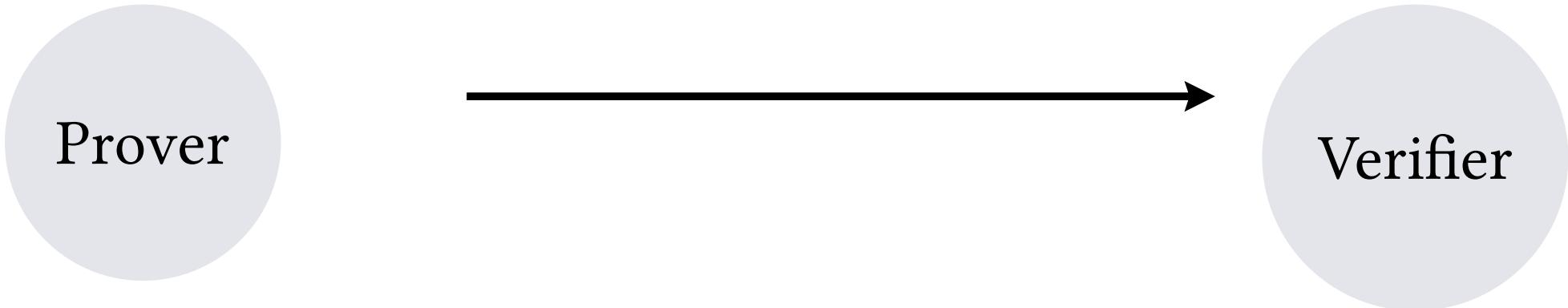
There is **asymmetry** built into those systems. It is much easier to get public key from secret. But not the other way



proof verified using public data

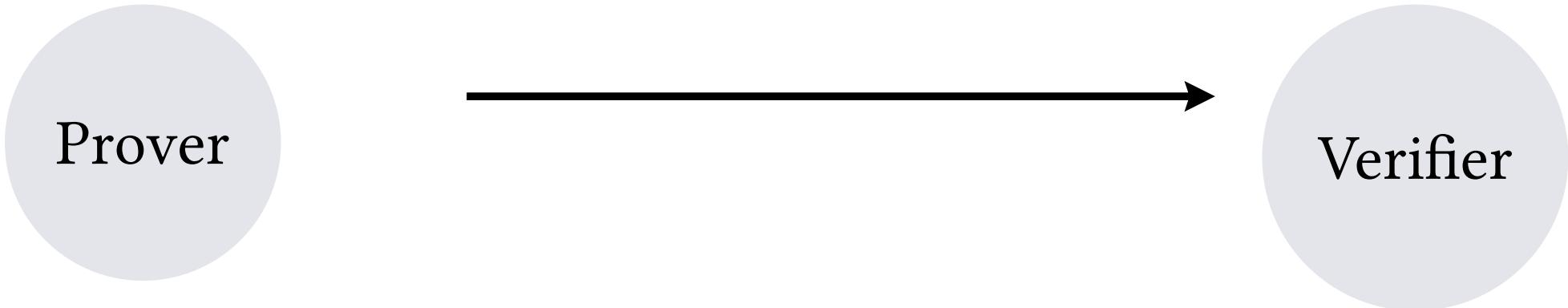
Verifiable computing vs ZKP (2)

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



Verifiable computing vs ZKP (2)

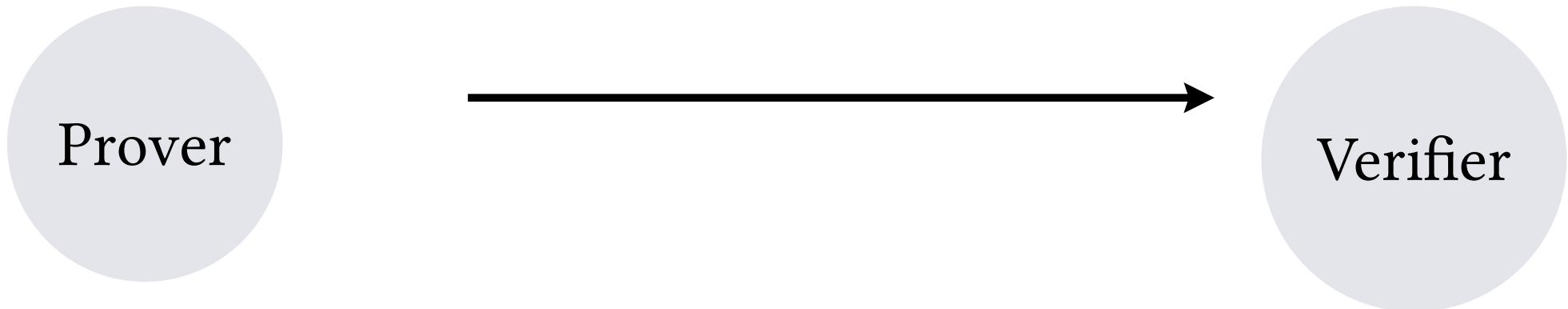
There is **asymmetry** built into those systems. It is much quicker to verify than prove something.



$O(n)$ off-chain

Verifiable computing vs ZKP (2)

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

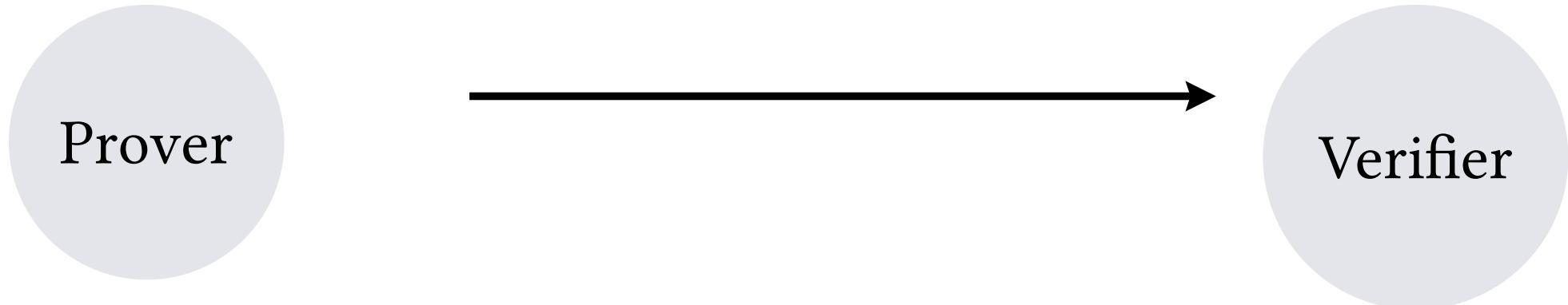


$O(n)$ off-chain

$O(\log n)$ on-chain

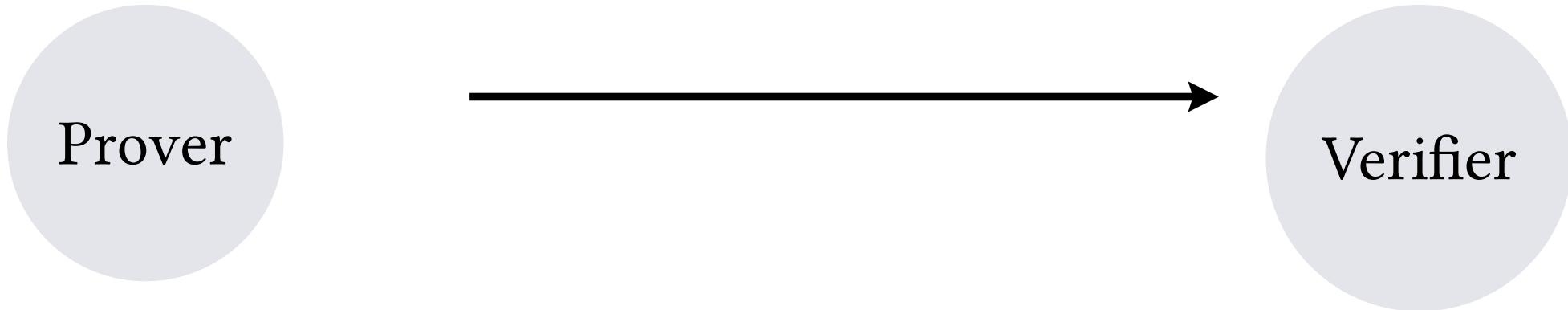
ZKP (3)

Data sent to verifier is compressed, and can be hidden



ZKP (3)

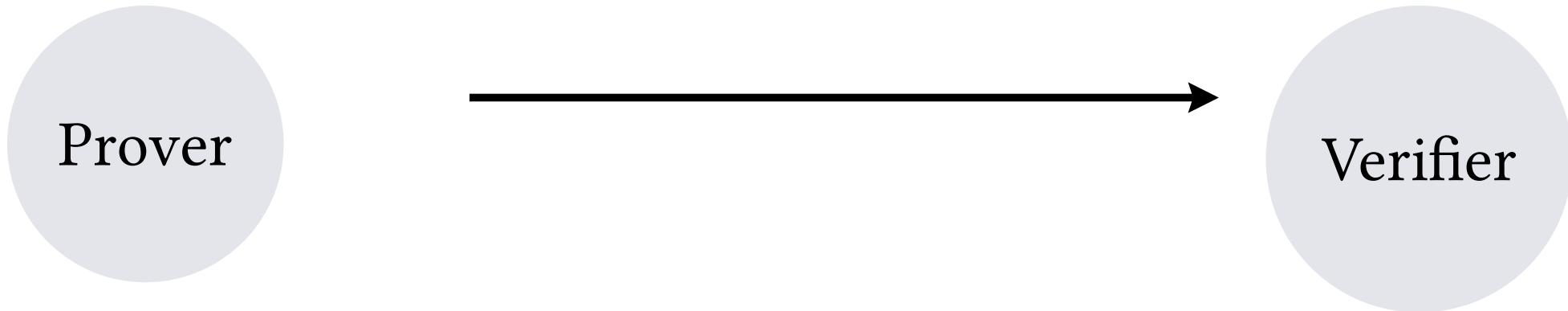
Data sent to verifier is compressed, and can be hidden



size: n

ZKP (3)

Data sent to verifier is compressed, and can be hidden

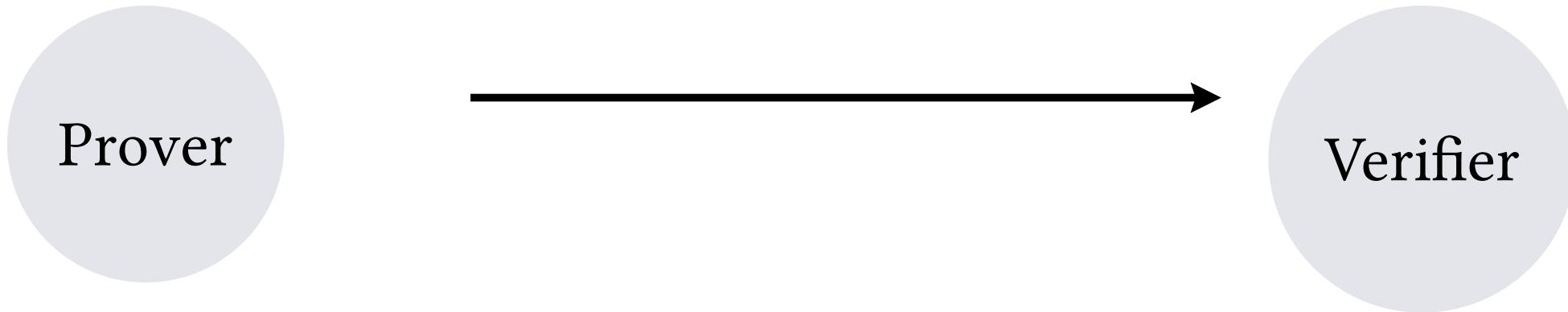


size: n

size: at least $\log n$

ZKP (3)

Data sent to verifier is compressed, and can be hidden

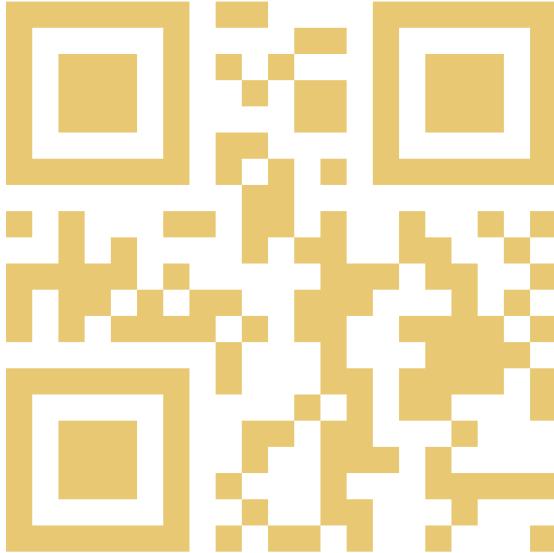


size: n

size: at least $\log n$

size: at least $\log n$

That's it! More to come in the future



Get in touch 

↗ My notes on GitHub