Zero Knowledge Proof — Prove It Without Telling the Secret

Prove you know a secret without ever saying the secret — the clever idea behind modern private logins.

Introduction

Imagine a cave with two paths that join in a circle, and a secret door in the middle that opens only with a magic word. You want to prove to a friend that you know the magic word — but you do not want to tell them the word. How?

You go into the cave. Your friend waits outside and shouts "come out from the left!" or "come out from the right!" — at random. If you know the magic word, you can always come out from the side they asked, because the secret door lets you cross between the two paths. If you do not know it, you can only come out from the side you entered — so half the time you fail. After 20 rounds, if you succeeded every time, your friend is almost certain you know the word — and you never said it once.

That is a **Zero Knowledge Proof (ZKP)**: you prove a statement is true without revealing anything except that it is true. One person is the **prover** (you know the secret), the other is the **verifier** (they check the proof). The proof is interactive: the verifier keeps challenging, and the prover keeps answering.

In this lesson you will learn the cave story properly, the three rules every ZKP must follow, and where ZKPs are used in real life — from private logins to private payments.

(Roman Urdu: Zero Knowledge Proof ka matlab hai — saboot do, raaz bataye baghair. Ghaar wali misaal: tum magic word jaante ho, dost ko yaqeen dila do, magar word kabhi na batao. Aisa baar baar challenge se hota hai.)

This lesson has a companion video, already built Oct 20, 2026 — it will be uploaded with the series launch. The notes below cover the full idea, so you can learn it even before the video is public.

Key points

- **A Zero Knowledge Proof proves a statement without revealing the secret behind it.** The verifier learns only one thing: the statement is true.
- **The cave story is the classic example.** The secret is the magic word; the proof is coming out of the asked side, again and again.
- **Three rules make a proof a ZKP: completeness, soundness, and zero knowledge.** Completeness: an honest prover always convinces an honest verifier. Soundness: a cheater almost never convinces anyone. Zero knowledge: the verifier learns nothing except that the statement is true.
- **One round proves little; many rounds prove a lot.** A cheater passes one round half the time. After 20 rounds, a cheater's chance is 1 in about a million (1/2 to the power of 20).

- **The verifier's challenges must be random.** If the prover knows the challenge in advance, they can cheat. Randomness is what makes the proof strong.
- **ZKPs are used where privacy matters.** Prove you are over 18 without showing your birth date. Prove you own enough money for a payment without showing your balance. Prove your password is right without sending the password.
- **A ZKP is not magic and not free.** Real ZKPs use heavy maths and take computing power. They are used where the privacy is worth the cost.

Examples

Example 1 — The cave, round by round

```
Round 1:  friend shouts "LEFT".  You come out left.  (A cheater could too — 50%)
Round 2:  friend shouts "RIGHT". You come out right. (Cheater: 25% now)
Round 3:  friend shouts "LEFT".  You come out left.  (Cheater: 12.5%)
...
Round 20: friend is now 99.9999% sure you know the word.
```

Each round halves the cheater's chance. After 20 rounds the chance a cheater survived is 1 in 1,048,576. You never said the word.

Example 2 — The numbers behind the rounds

```
rounds = 20
cheater_chance = (1/2) ** rounds
print("Cheater survives 20 rounds with chance:", cheater_chance)
print("That is about 1 in", round(1 / cheater_chance))
```

What you will get:

```
Cheater survives 20 rounds with chance: 9.5367431640625e-07
That is about 1 in 1048576
```

Change `rounds` to 10 and the chance is about 1 in 1,000 — too weak for real use. Change it to 30 and it is about 1 in a billion. More rounds, stronger proof.

Example 3 — Prove you are over 18, without your birth date

```
Old way:   show your ID card — the checker learns your full birth
           date, your address, your ID number. Too much.

ZKP way:   prove "my age is 18 or more" and nothing else.
           The checker learns one fact: old enough. Nothing more.
```

This is the real promise of ZKPs: prove exactly what is needed, and reveal nothing extra.

Example 4 — Prove a password without sending it

```
Old way:   send your password to the website — it travels the
           internet and sits on their server.

ZKP way:   prove "I know the password that matches this account"
           without the password ever leaving your device.
```

The server never holds your password, so a server leak cannot expose it. This idea is already used in modern login systems.

Example 5 — Where ZKPs already work today

```
Private payments:  prove a payment is valid without showing the
                   amount or the sender (used by privacy coins).

Identity checks:   prove you hold a valid licence without
                   showing the licence itself.

Voting:            prove your vote is valid without showing
                   who you voted for.
```

In each case the pattern is the same: prove the statement, hide everything else.

Quick recap

- A Zero Knowledge Proof proves something is true without revealing the secret.
- The cave story: random challenges, many rounds, never say the magic word.
- Three rules: completeness (honest prover succeeds), soundness (cheater fails), zero knowledge (verifier learns nothing extra).
- Each round halves a cheater's chance — 20 rounds means about 1 in a million.
- Real uses: private age checks, private payments, logins without sending passwords.

Common mistakes

1. **Thinking "zero knowledge" means "zero proof"** — the verifier ends up very sure; they just learn nothing extra. Fix: the proof is strong, the leakage is zero.
2. **Trusting one round** — a cheater passes a single round half the time. Fix: many rounds, or one strong non-interactive proof.
3. **Letting the prover predict the challenge** — if the challenge is not random, the prover can prepare the answer. Fix: the verifier chooses at random, every round.

4. **Using a ZKP where a simple check would do** — ZKPs cost computing power. Fix: use them where privacy is truly needed, not everywhere.
5. **Believing the secret is "safe because it was never said"** — the proof must also be built correctly; a badly built ZKP can leak the secret. Fix: use tested, standard ZKP systems, never a home-made one.

Practice

1. Retell the cave story to a friend in your own words: what is the secret, what does the friend shout, and why does 20 rounds convince them?
2. Run the Python example with rounds = 5, 10, and 30. Write down the cheater's chance for each. How many rounds would you demand before trusting a stranger?
3. Write one real-life situation where you would like to prove something without revealing more — for example, your age, your marks, or your income. What exactly should the checker learn, and what should stay hidden?
4. Name the three rules of a ZKP (completeness, soundness, zero knowledge) and explain each in one line.
5. Watch for the companion video of this lesson when the series launches — compare its cave explanation with the one in these notes and note one detail the video adds.

Practice quiz

1. What does a Zero Knowledge Proof let you do?

- Prove a statement is true without revealing the secret behind it
- Hide a message so nobody can ever find it
- Encrypt a file with no key
- Prove something with zero evidence

Answer: Prove a statement is true without revealing the secret behind it

2. In the cave story, why must the friend's challenges be random?

- To make the story longer
- So the prover cannot prepare the answer in advance and cheat
- So the cave stays dark
- Randomness is not needed, one challenge is enough

Answer: So the prover cannot prepare the answer in advance and cheat

3. A cheater passes one round of the cave test half the time. What is their chance after 20 rounds?

- Still half
- About 1 in 1,000
- About 1 in a million
- Zero, exactly

Answer: About 1 in a million

Watch the Code Scope channel: https://www.youtube.com/@CodeScopePK — this lesson's own video joins the channel when it is recorded.

Read online: https://scopetreasure.com/notes/cs-zero-knowledge-proof · More free tools and notes at https://scopetreasure.com