Thema: Zero-Knowledge Proof

erstellt von anonym am Sonntag 10. Februar 2019, 19:51

Hi,
Can someone help me with the 'Ali baba' cave example that was discussed during the 'Zero-Knowledge Proof' topic? I remember that the proof is not transferable in this case, but I don't recall what was the proof exactly?

Thanks!

No title
erstellt von Denis Arnst am Sonntag 10. Februar 2019, 20:06

This picture
helps: https://de.wikipedia.org/wiki/Zero-Knowledge-Beweis#/media/File:Zero_knowledge_cave_1.svg
You stand at position 3. You want to know from some person (B) if he knows how to get through the gate at 1/2. The person B can prove to you that he knows how to get through the gate, by simply going into Position 2 (right side) and coming out of Position 1 (left side). As you can't see how B opens the gate, you don't know the secret, but you know that B must know it.
It is not transferable as a person in position 4 doesn't know wether B really did this experiment (even a movie of B doing it could be cut/faked).

---

erstellt von anonym am Sonntag 10. Februar 2019, 20:40

Great! Exactly what I needed. Thanks a lot!

---

erstellt von Denis Arnst am Sonntag 10. Februar 2019, 20:56

One more hint: My example is simplified. The original proof works by statistical means. You stand outside the cave, and B goes into 1 or 2. You go to 3 and make a challenge to B, that she should return on either 1 or 2 (you specify the return path). Note that the probability of someone solving one iteration of the experiment is 50%. You'll repeat this experiment several times. Now, if B does this n times right, the probability that B knows the secret is 1-(2)^(-n)