Zero Knowledge

Rohit Musti

CUNY - Hunter College

April 6, 2022

Intuition

- How can we prove a statement x is true without revealing anything other than that statement is true (without resorting to a trusted actor)?
- How can we prove we know where Waldo is in a Where's waldo game without revealing Waldo's location?
- How do we prove a child is tall enough to ride a ride at an amusement park without revealing the child's true height, hair color, etc.?
- How can we approve you can afford to buy a coffee without revealing your networth, bank account total, preferred currency, etc.?
- How can we prove N is the product of two primes p, q without revealing its factorization?

Definitions

- What is knowledge? In cryptography, we refer to knowledge as things that can be computed efficiently. If you know N, p, you *know* q.
- It follows that a zero knowledge protocol is a protocol that doesn't reveal any information that the adversary could not otherwise efficiently compute.
- If you had a protocol that proved you knew the m that a c encrypted, you wouldn't reveal any information that an adversary could easily compute from c directly

2 Examples

Ali Baba Cave

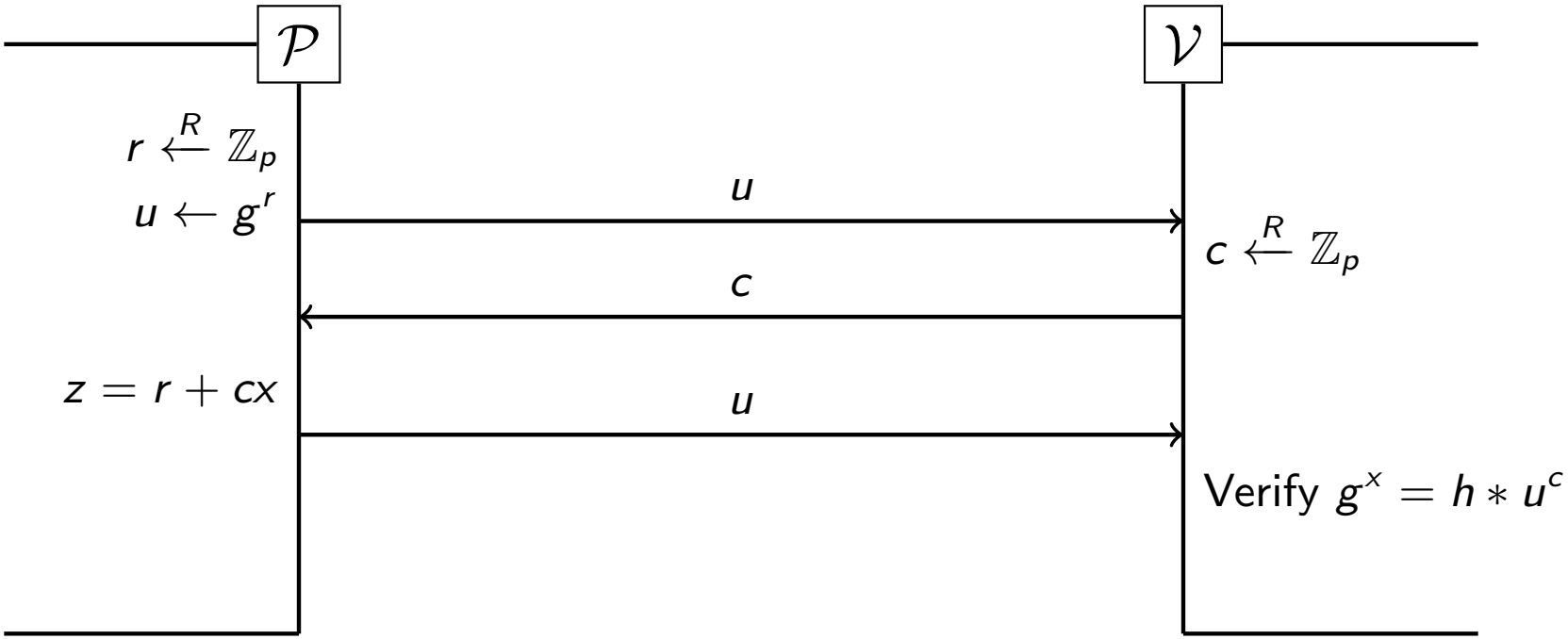
- Our two friends and protagonists, Alice and Bob, are on an adventure and stumble onto a Cave
- There are two different entrances to two different paths and there is a door somewhere in the cave connecting the two paths!
- Alice knows this door's code and offers to sell it to Bob! However, Bob wants proof that the code works and Alice refuses to reveal the code without Bob purchasing it!
- Bob offers to follow Alice into the cave and then close his eyes while Alice taps in the code, but it is dark in the cave and Alice has no way to be sure that Bob actually has his eyes closed!

Ali Baba Cave

- Our two friends are at an impasse, but then their hip friend Suhail wanders by fresh from his Introduction to Cryptography lecture and offers this solution!
- Suhail suggests that Alice picks any one of the paths to enter into the cave. Then, then Bob can call out which path he wants Alice to exit from.
- There is a 50% chance that Alice and Bob select the same path. However, over multiple runs, it is unlikely that they repeatedly choose the same path

Discrete Log

prove you know x such that $h = g^x$, assuming $g, h \in \mathbb{G}$



Discrete Log ZK Authentication Protocol

- What if an adversary has hacked the server and can see clients interaction with the server!
- Non-Zero Knowledge protocols will lead to compromise identities for people who try and log in.
- If the server stores g, g^x and the server and client complete the zero-knowledge proof without ever revealing the client's secret x, this woukld accomplish a zero knowledge authentication!

3 Properties

Proof System Properties

- The goal of proof systems is to convince a verifier that a statement is true
- Completeness: an honest prover will be able to convince a verifier of all true statements
- Soundness: a dishonest provers cannot convince an honest verifier of a false statement
- Interactive and Randomness, enables zero knowledge proofs!

Zero Knowledge Properties

- We need a "simulator" to define zero knowledge; the intuition is that anything a verifier can learn from a prover, they should be able to learn from a simulator
- The more precise definition: the distribution of interactions with prover needs to be indistingiushable from the distributions of interactions with a simulator
- a really interesting zero knowledge property is that if one way functions actually exist, then any proof can be proven with zero knowledge

3 color graph problem

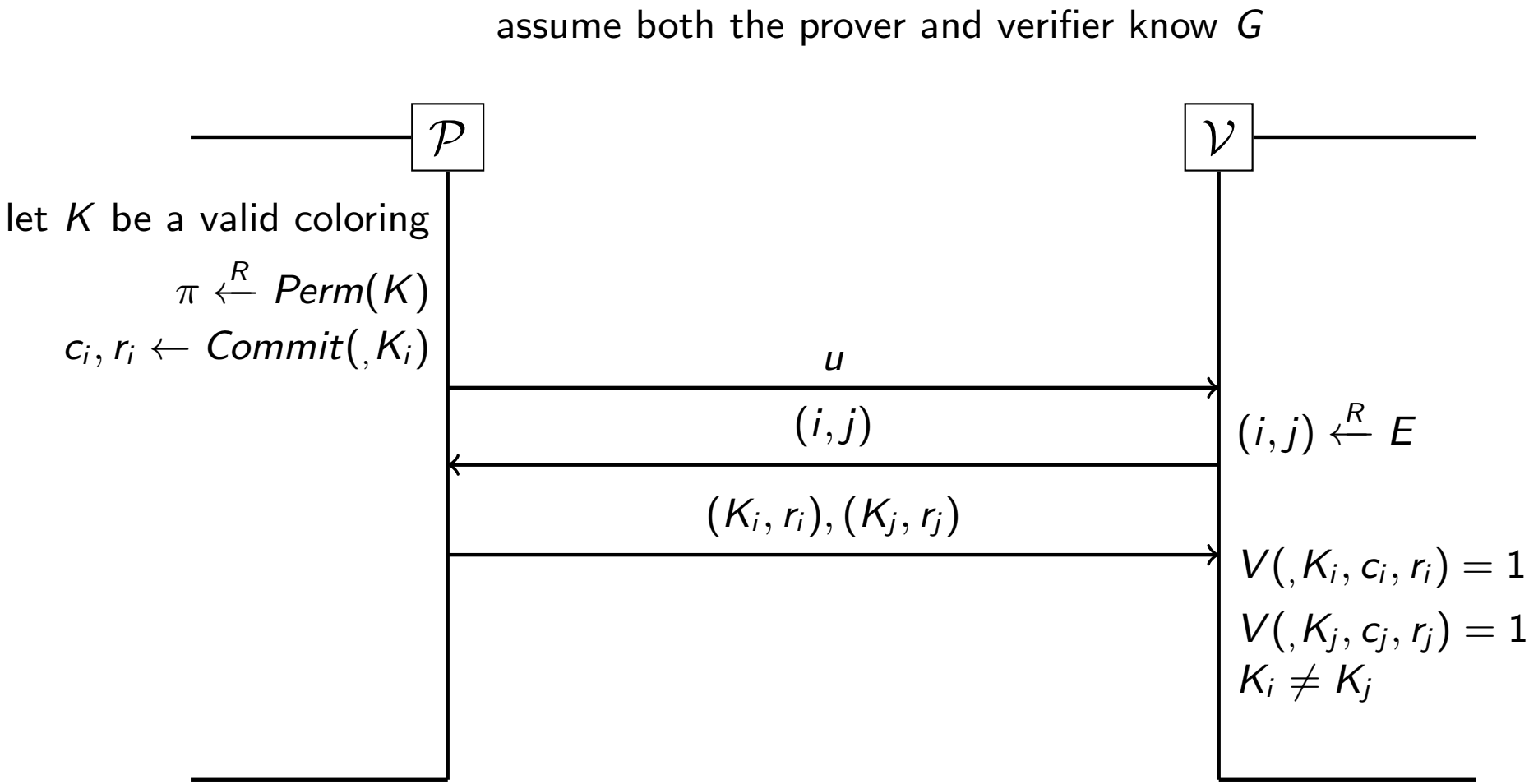
- Can you color a given graph s.t. no adjacent vertices share the same coloring?
- We need a commitment scheme with two functions:

$$Commit(,m) \rightarrow (c, r)$$

$$Verify(,m, c, r) \rightarrow b$$

- Potential HW/Exam Queston: This scheme needs to be correct (shannon correctness), hiding (adversaries cannot distinguish whcih commitment corresponds to which message), and binding (the same commitment working for multiple messages and openings needs to be negligible)

3 Color Graph Problem



Schnorr Signatures

- Verification Key is (g, g^x)
- To sign use a non-interactive zero knowledge proof of discrete log of x where the challenge c is derived from the message using a hash function
- We use something very similar to this in practice called DSA/ECDSA

Failed Implementations

- For playstation 3 updates (and some bitcoin wallets), the updates are signed using schnorr signatures.
- If the randomness of the constant r is not very good, then the signature isn't very secure
- Some systems use fixed constants for the randomness and this allows hackers to deploy arbitrary firmware and other updates/signed messages!
- lesson: avoid randomness reuse