Zero-Knowledge Proofs

Cryptography - CS 411 / CS 507

Erkay Savaş

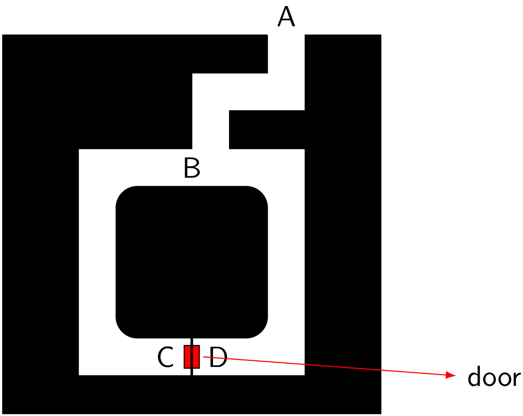
Department of Computer Science and Engineering
Sabancı University

December 13, 2019

The Basic Setup

- There are circumstances where one party is to prove to the other party that she is in possession of certain secret information without revealing the actual secret (e.g., remote identification)
- The zero-knowledge proofs take the form of interactive protocols.
  - Victor (the verifier) asks Peggy (the prover) a series of questions.
  - If Peggy knows the secret, she can answer all the questions correctly.
  - If she does not, then she has some chance of answering each question correctly.

Zero-Knowledge Cave

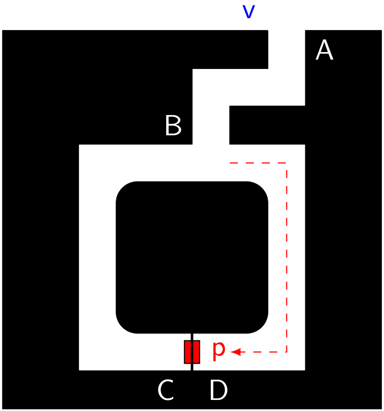


- Due to Jean-Jacques Quisquater & Louis Guillou

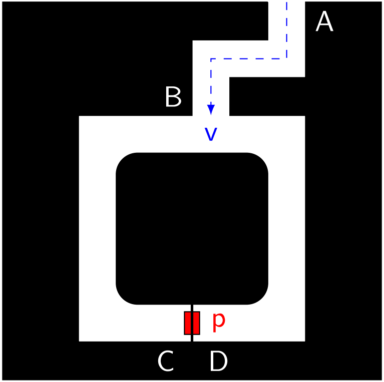
Zero-Knowledge Cave

- Peggy claims that she can go through the door between C and D.
- She wants to prove this to Victor.
  - But she does not want anyone else to know she can do it or how she can do it.
- The Method
  1. Victor stands at point A.
  2. Peggy walks all the way into the cave, either to point C or point D (she chooses which way to go at random)
  3. After Peggy has disappeared into the cave, Victor walks to point B.

Zero-Knowledge Cave



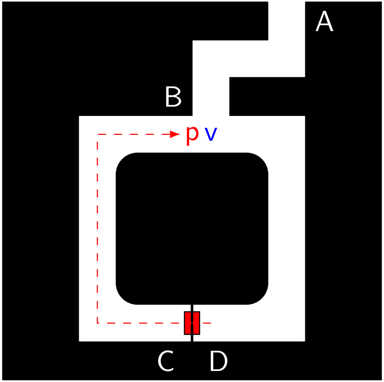
Zero-Knowledge Cave



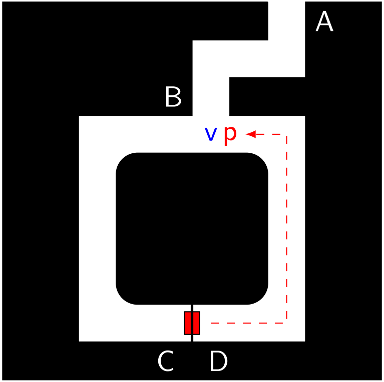
Zero-Knowledge Cave

- The Method (cont.)
  4. Victor shouts to Peggy asking her either to:
     - come out of the left passage or
     - come out of the right passage
  5. Peggy complies, using the magic word to open the secret door if she has to.
  6. They repeat steps (1) through (5) t times.

Zero-Knowledge Cave



Zero-Knowledge Cave



Zero-Knowledge Cave

- What are the odds that Peggy comes out of the correct passage if she cannot really go through the door?
  - Victor chooses left or right passage randomly,
  - Peggy can guess this choice of Victor beforehand correctly with possibility of 50% or $\frac{1}{2}$.
- They repeat the protocol $\{t\}$ times,
  - the possibility that Peggy can deceive Victor every time successfully is only 2^{-t}.
  - Victor is probably convinced after sufficiently large number of trials.

Zero-Knowledge Cave

- Can Victor convince Carol, too?
  - Victor records everything he sees and shows the recording to Carol
  - Carol might be convinced if she trusts Victor
    - But she might also think that Victor and Peggy had agreed ahead of time what side Victor shout out each time.
  - It is impossible to prove what Victor is convinced of to a third party.

Mathematical ZK System

- Setting
  - Let $n = p \cdot q$ is a product of two large primes.
  - Let y be a square $\pmod{n}$.
  - Peggy claims to know a square root s of y.
  - Victor wants to verify this, but Peggy does not want to reveal s.
- Protocol
  1. Peggy chooses two random numbers r_0 and r_1 with
     $$s = r_0 r_1 \bmod n$$
  2. She computes
     $$x_0 = {r_0}^2 \bmod n \text{ and } x_1 = {r_1}^2 \bmod n$$
     and sends x_0 and x_1 to Victor.

A Basic Zero-Knowledge Protocol

- The protocol (cont.)
  3. Victor checks that
     $y = x_0 x_1 \bmod n$,
  4. He then picks either x_0 or x_1 at random and
     - asks Peggy to supply the square root of it.
     - He checks if it is an actual square root.
  5. The first two steps are repeated until Victor is convinced.
- If Peggy knows s, everything proceeds without any problem.
- What if she does not know it, can she still supply the correct numbers?

A Basic Zero-Knowledge Protocol

- If she does not know the square root of y, she can still send two numbers x_0 and x_1 with $y = x_0 x_1 \bmod n$.
- She picks a random r_i and computes $x_i = r_i^2 \bmod n$, where $i \in \{0, 1\}$.
- She then computes $x_{1-i} = y x_i^{-1} \bmod n$
  - if $x_i^{-1} \bmod n$ does not exists, she picks another r_i.
- She knows one of the square roots.
- At least half the time, Victor will ask her for a square root she doesn't know.
  - Peggy can correctly predict which square root Victor will ask her to send with a probability of $\frac{1}{2}$.

A Basic Zero-Knowledge Protocol

- Therefore, she has 50% chance of fooling Victor on any given round.
- Victor verifies that Peggy knows the square root; but he obtains no information about the square root.
- Peggy shouldn't use the same random numbers more than once.
- Eve sees only the square roots of random numbers.

Properties of ZK Protocols

- Completeness:
  - Given honest verifier and prover, the protocol succeeds with overwhelming probability (i.e., the verifier accepts the prover's claim)
- Soundness:
  - No cheating prover can convince the honest verifier that it has the secret, except with some small probability.
- Zero-knowledge:
  - No cheating verifier learns anything.
  - Every cheating verifier has some *simulator* which, can produce a transcript that "looks like" an interaction between the honest prover and the cheating verifier.

Schnorr Identification Scheme

- Setting
  - p and q large primes with $q|p-1$, g is a generator in $G_q \subset \mathbb{Z}_p^*$
  - $1 < s < q-1$ is known only to Peggy
  - $\beta = g^s \bmod p$ is public
- Protocol

Peggy	Victor
1. $\gamma = g^k \bmod p$ (witness) random $k, 1 \leq k < q$	
	2. random $r, 1 \leq r < q$ (challenge)
3. $y = k - sr \pmod q$ (response)	
	4. $\gamma = g^y \beta^r \bmod p$

Can Victor Simulate Schnorr's Scheme?

Peggy		Victor		Simulator
			1) $y', r' \leftarrow G_q$ 2) $\gamma' = g^{y'} \beta^{r'} \bmod p$	
	$\xrightarrow{\gamma}$		$\xleftarrow{\gamma'}$	
	$\xleftarrow{r}$		$\xrightarrow{r'}$	
	$\xrightarrow{y}$		$\xleftarrow{y'}$	

Signatures from ZK Protocols

- Shamir's heuristic
  - use the message (or its hash) as the "challenge"
- Protocol
  - Signature generation
    - $\gamma = g^k \mod p, 1 \leq k < q$
    - $y = k - sH(m) \mod q$
    - signature for m is (γ, y)
  - Signature verification
    - $\gamma = g^y \beta^{H(m)} \bmod p$