Zero-Knowledge Proofs

Cryptography - CS 411 / CS 507

Erkay Savaş

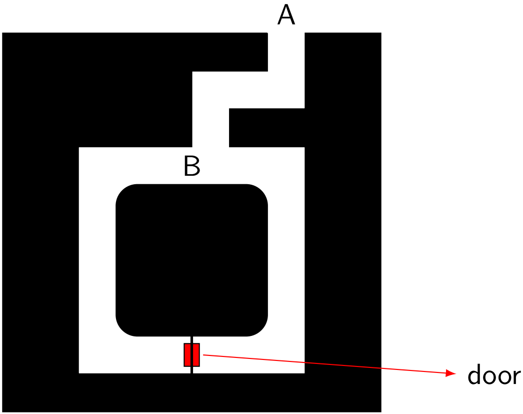
Department of Computer Science and Engineering
Sabancı University

December 12, 2023

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.
- 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 - say $\varepsilon\%$ - of answering each question correctly.

Zero-Knowledge Cave

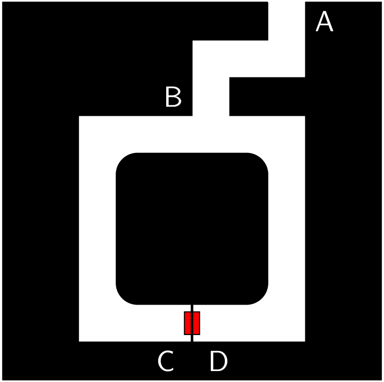


- Due to Jean-Jacques Quisquater & Louis Guillou

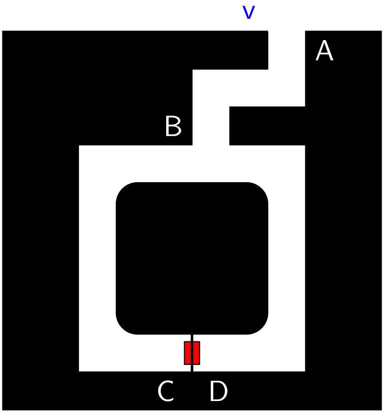
Zero-Knowledge Cave

- 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.

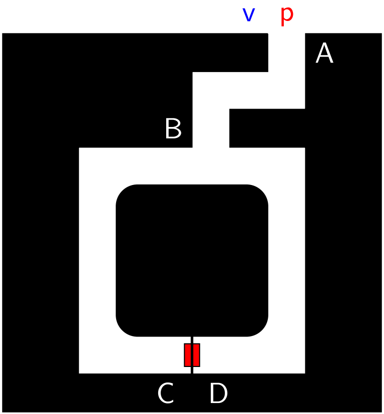
Zero-Knowledge Cave



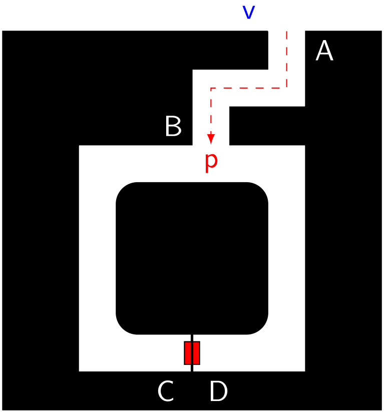
Zero-Knowledge Cave



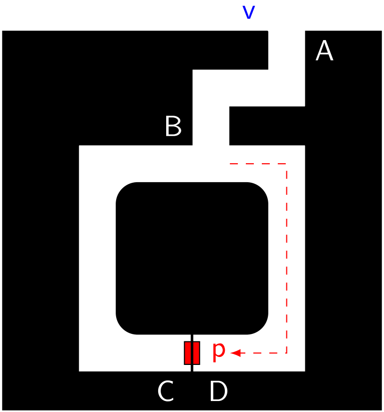
Zero-Knowledge Cave

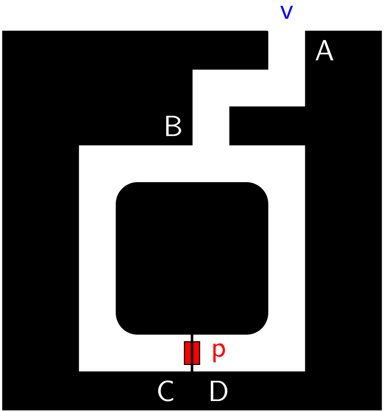


Zero-Knowledge Cave

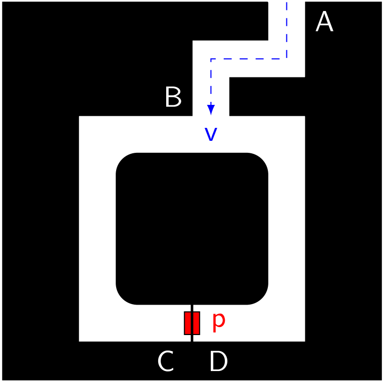


Zero-Knowledge Cave



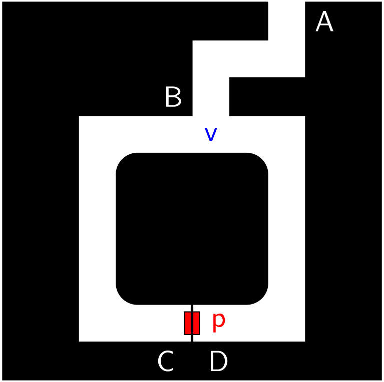

v
A
B
p
C
D

Zero-Knowledge Cave

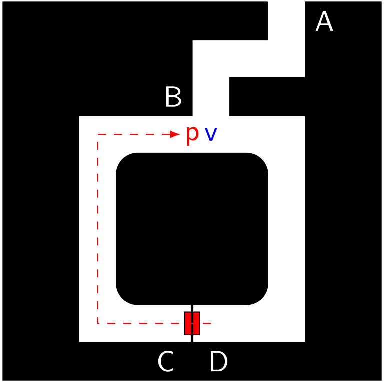


- The Method (cont.)
  4. Victor shouts to Peggy asking her either to:
     - come out of the left passage or
     - come out of the right passage
  5. Peggy complies, using the magic word to open the secret door if she has to.
  6. They repeat steps (1) through (5) t times.

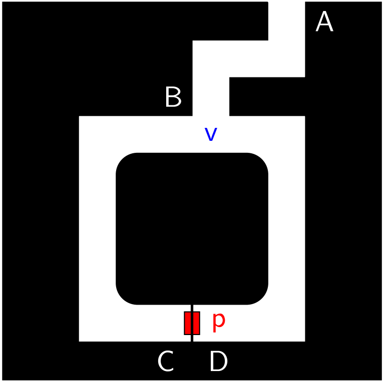
Zero-Knowledge Cave



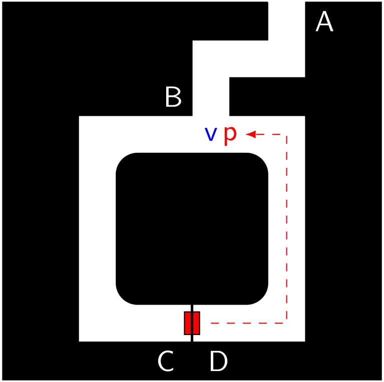
Zero-Knowledge Cave



Zero-Knowledge Cave



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.

- 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

- Hardness of computing a square root of number modulo a composite number, n
  - Given y and n; find an integer s such that $y = s^2 \bmod n$
  - Furthermore, such s may not exist
  - It may be even hard to say whether s exists or not
- If factoring n is hard, then computing square root is also hard
  - If you know the factors of n, you can compute square roots if they exist.
  - If you know all square roots of $y \bmod n$, then you can factor n.

Mathematical ZK System

- Setting
  - Let $n = p \cdot q$ is a product of two large primes.
  - Let y be a square $\bmod n$ with $\gcd(y, n) = 1$.
  - 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

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 $x_0 x_1 \equiv y \bmod n$.
- She picks a random r_i and computes $x_i = r_i^2 \bmod n$, where $i \in \{0, 1\}$.
  - She, then, computes $x_{1-i} = y \cdot x_i^{-1} \bmod n$
  - If $x_i^{-1} \bmod n$ does not exist, she picks another r_i.
- She knows only one of the square roots
- Half the time, on average, 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 is a large prime, q is a smaller prime, g is a generator in ${G_q}^*$
  - $\{s\}$ is known to Peggy
  - $h = g^s \bmod p$ 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. $y = k - sr \bmod q$ (response)	
	4. $\gamma = g^y h^r \bmod p$

Can Victor Simulate Schnorr's Scheme?

Can Victor Simulate Schnorr's Scheme?

<u>Victor</u>

Can Victor Simulate Schnorr's Scheme?

<u>Peggy</u> <u>Victor</u>

Can Victor Simulate Schnorr's Scheme?

Simulator

Can Victor Simulate Schnorr's Scheme?

<u>Victor</u>	<u>Simulator</u>

Can Victor Simulate Schnorr's Scheme?

Victor		Simulator
	1) $y' \in_R G_q$ and $r' \in_R \mathbb{Z}_q$	

Can Victor Simulate Schnorr's Scheme?

<u>Victor</u> <u>Simulator</u>

1) $y' \in_R G_q$ and $r' \in_R \mathbb{Z}_q$
2) $\gamma' = g^{y'} h^{r'} \bmod p$

Can Victor Simulate Schnorr's Scheme?

Victor		Simulator
	1) $y' \in_R G_q$ and $r' \in_R \mathbb{Z}_q$	
	2) $\gamma' = g^{y'} h^{r'} \bmod p$	
	$\xleftarrow{\quad \gamma' \quad}$	

Can Victor Simulate Schnorr's Scheme?

$$\begin{array}{ccc}
\underline{\text{Victor}} & & \underline{\text{Simulator}} \\
& & \text{1) } y' \in_R G_q \text{ and } r' \in_R \mathbb{Z}_q \\
& & \text{2) } \gamma' = g^{y'} h^{r'} \bmod p \\
& \xleftarrow{\quad\quad\gamma'\quad\quad} & \\
& \xrightarrow{\quad\quad r'\quad\quad} &
\end{array}$$

Can Victor Simulate Schnorr's Scheme?

Victor | Simulator

1) $y' \in_R G_q$ and $r' \in_R \mathbb{Z}_q$

2) $\gamma' = g^{y'} h^{r'} \bmod p$

$$\xleftarrow{\quad \gamma' \quad}$$

$$\xrightarrow{\quad r' \quad}$$

$$\xleftarrow{\quad y' \quad}$$

Can Victor Simulate Schnorr's Scheme?

Peggy		Victor		Simulator
				1) $y' \in_R \mathbb{Z}_q$ and $r' \in_R \mathbb{Z}_q$
				2) $\gamma' = g^{y'} h^{r'} \bmod p$
	$\xrightarrow{\quad\gamma\quad}$		$\xleftarrow{\quad\gamma'\quad}$	
	$\xleftarrow{\quad r\quad}$		$\xrightarrow{\quad r'\quad}$	
	$\xrightarrow{\quad y\quad}$		$\xleftarrow{\quad y'\quad}$	

Signatures from ZK Protocols

- Shamir's heuristic
  - use the message (or its representative) as the "challenge"
- Protocol
  - Signature generation
    - $\gamma = g^k \mod p, 1 \leq k < q$
    - $c = H(m||\gamma)$
    - $y = k - sc \mod q$
    - signature for m is (c, y)
  - Signature verification
    - $\gamma = g^y h^c \bmod p$
    - $\tilde{c} = H(m||\gamma)$
    - Accept the signature if $\tilde{c} = c$