Zero Knowledge Proof

Seewoo

> Can we (prover) convince someone else (verifier) that a statement is true, without conveying the verifier any information beyond the fact that statement is true?

Ex) You solved a very hard sudoku. You want to convince that you solved it, but you don't want to reveal the solution. How can we achieve this?

Zero-Knowledge Proof (ZKP)

First conceived by Goldwasser-Micali-Rackoff (1985)

"The Knowledge Complexity of Interactive Proof Systems"

They give first ZKP for Quadratic (Non-)Residue problem (Q(N)R):

- Two (large) integer x, N are given. Peggy knows that x is (not) a quadratic residue modulo N, i.e. (no) y satisfy $x \equiv y^2 \pmod N$.
- She can (interactively) prove (convince Victor) this without revealing any additional knowledge.

Def A zero-knowledge proof of a statement satisfies

- Completeness If the statement is true, then an honest verifier will be convinced of this fact by an honest prover.
- Soundness If the statement is false, then no cheating prover can convince an honest verifier that it is true, except with some negligable probability.
- Zero-Knowledge If the statement is true, then no verifier learns anything other than the fact that the statement is true.
  This is formalized by showing that every verifier has some "simulator" that, given only the statement is proved, can produce a transcript that "looks like" an interaction between an honest prover and verifier in question.

Examples)

- Ali Baba Cave (by Quisquater, "How to explain Zero-Knowledge Protocols to Your Children")

Peggy want to convince Victor that she knows "magic word" for a door inside cave.

ZKP (Interactive)

① Peggy enter to the cave through A or B, randomly chosen.

② Victor ask Peggy to exit through A or B, randomly chosen

③ Repeat ① and ②.

⇒ P(Peggy correctly guess | Don't know magic word)

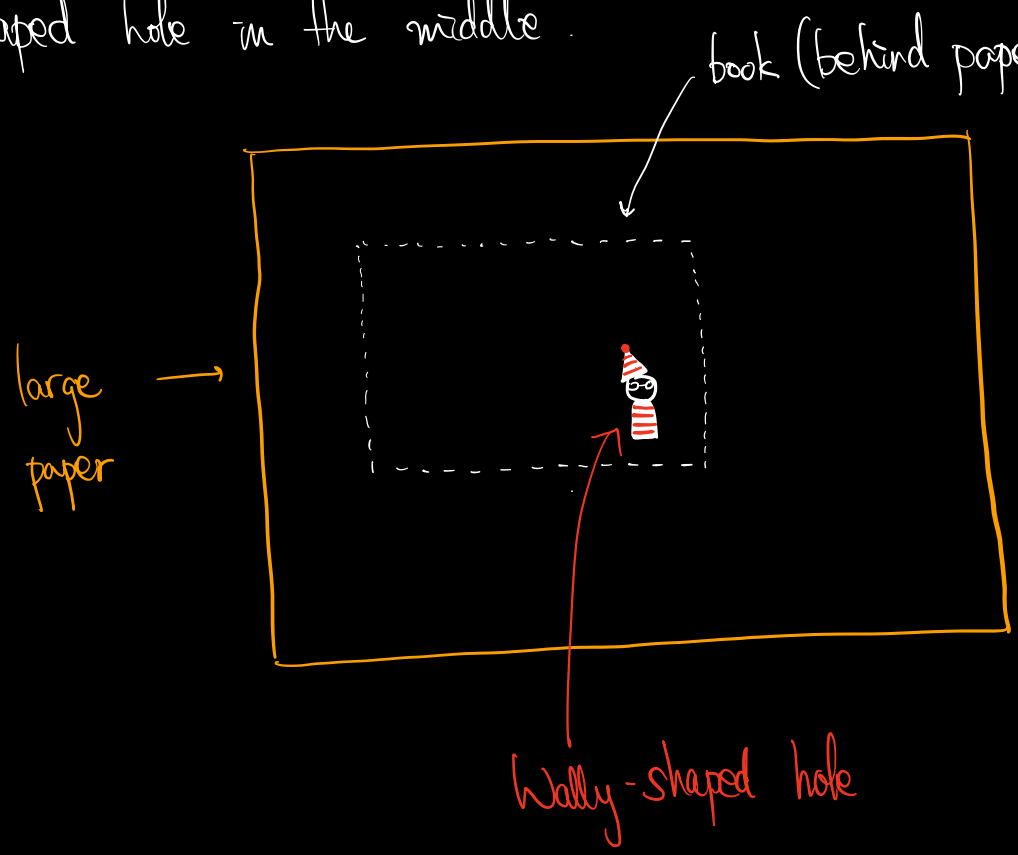
$= \frac{1}{2}$. As # of rounds grow, the probability Peggy success all the time decreases exponentially.

Also, Victor can't figure out magic word (assuming cave is big enough).

- Where's Wally (Waldo)?

Peggy want to convince that she found Wally, without revealing the position.

ZKP : Prepare large piece of paper with Wally-shaped hole in the middle.



- Playing card's color

Peggy choose a card from a deck. She want to convince that she draw red card.

ZKP : Show that all black cards are in the deck.

- Discrete logarithm

Large prime p and primitive root $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ are given. $y \in \mathbb{Z}$ is also given. Peggy want to convince that she knows discrete log of y, i.e. $\alpha \in \mathbb{Z}$ s.t. $g^\alpha \equiv y \bmod p$.

ZKP (Interactive). For each round:

① Peggy generate random $r \in \mathbb{Z}$ and compute $C = g^r \pmod p$.

② Victor randomly issues one of the following requests:

1) Peggy discloses r. Victor check if g^r matches C.

2) Peggy discloses $\alpha + r \pmod{p-1}$. Victor check if $g^{\alpha+r}$ matches with $C \cdot y \pmod p$.

* If Peggy can predict Victor's move, she can always cheat. For example, if Victor's move is 2), she can: randomly generate r', "pretend it as $\alpha+r$". Now send $C' = y^{-1} \cdot g^{r'}$ to Victor. Then Victor can check "$g^{\alpha+r}$" $= g^{r'} = C' \cdot y =$ "$C \cdot y$" and Peggy passes the test.

But if not, she can't cheat (assuming discrete log problem is hard)

- Quadratic Residue (QR)

p, q large primes and $N = pq$. Peggy want to prove that a certain number y is a square mod N, i.e. $\exists\ x$ s.t. $y \equiv x^2 \pmod N$.

without revealing e.g. x.

- (Believe) QR is hard problem unless you know factorization of N.

(If factorization is known, use Legendre symbol & quadratic reciprocity)

ZKP (Interactive)

① Peggy chooses random r mod N and send $s = r^2 \bmod N$ to Victor.

② Victor randomly chooses $b \in \{0,1\}$ and sends it to Peggy.

③ Peggy computes

$$z = \begin{cases} r \bmod N & \text{if } b = 0 \\ xr \bmod N & \text{if } b = 1 \end{cases} \qquad (= x^b r)$$

and sends it to Victor.

④ Victor computes $z^2 \bmod N$ and check if

$$z^2 = \begin{cases} s \bmod N & \text{if } b = 0 \\ ys \bmod N. & \text{if } b = 1. \end{cases}$$

Exercise) Prove the protocol is sound and complete.

Why Zero-knowledge? Victor can "simulate" Peggy's response without knowing additional information. He can generate sequence

(s_1, β_1, z_1), (s_2, β_2, z_2), (s_3, β_3, z_3), ...

by: choose $\beta_i \in \{0,1\}$, $z_i \bmod N$ randomly at each step and set $s_i = z_i^2 (y^{\beta_i})^{-1} \bmod N$. If the protocol was not ZK, then Victor should be able to figure out some knowledge himself with simulated sequence.

- Sudoku (non-interactive)

Prepare $3^5 = 243$ cell-sized papers. For each cell, write the corresponding number on 3 papers and put upside down. Now, for each row / column / 3×3 boxes, Victor collect 9 papers and shuffle. Then reveal if the papers have $1 \sim 9$ exactly once.

Victor can't get any information about the actual soln since papers are shuffled.

Other examples:

- Graph (3-) coloring
- Hamiltonian cycle
- Rubik's Cube / Rush hour / Kakuro / ...

(See Ripsom-Gardiner's Honor's thesis "Zero Knowledge Proofs for Puzzles")

Applications

- Proof of Identity (Passport, Covid pass, ...)
- ML/AI. (Peggy wants to serve ML model without revealing model, or even proof of training, Garg et.al 2023)
- Online Voting
- Blockchain (ZCash)
- zkCrush / zkMultiCrush