Zero-Knowledge Proofs

Mihai Prunescu

Blockchain 2023 Conference

Bucuresti

March 22 – 23, 2023

This talk is mainly based on excerpts from the book:

Cryptography, an introduction

by Nigel Smart

The Prover Peggy knows a secret.

The Verifier Victor must be convinced that Peggy really knows the secret, but without learning anything about it.

They change some public information.

The protocol has to run relatively fast.

Completeness: If Peggy really knows the thing to be proved, then Victor should accept her proof with probability 1.

Soundness: If Peggy does not know the thing to be proved, then Victor should only have a small probability of actually accepting the proof.

Protocols in Graphs

Graph Isomorphism

$$\phi : G_0 \to G_1$$

permutation of vertexes, so

$$(a, b) \in E_0 \longleftrightarrow (\phi(a), \phi(b)) \in E_1$$

Peggy

Chooses $i \in \{0, 1\}$ and $\sigma \in S(G_i)$.

Produces the **commitment** $H = \sigma(G_i)$.

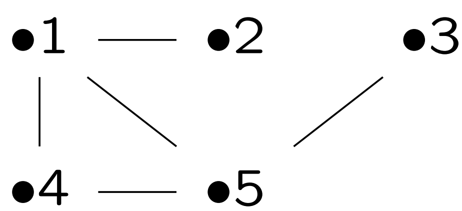
She knows:

$$\phi : G_0 \to G_1$$

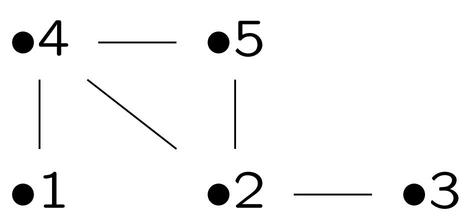
$$\sigma : G_i \to H$$

$$\psi : G_{1-i} \to H$$

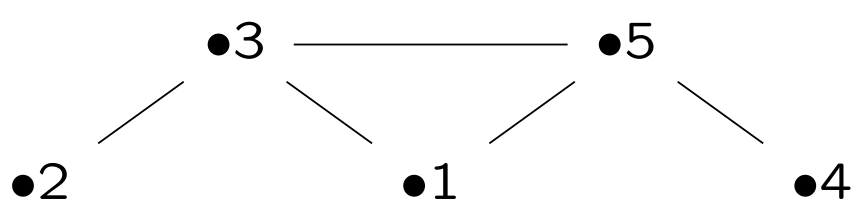
- G_1



- G_2



- H



Victor

gives Peggy a **challenge**: he chooses $j \in \{0, 1\}$ and asks for an isomorphism χ between H and G_j.

Peggy

If she knows ϕ, she can give a fast and correct **response**.

If she does not know ϕ, she can give a fast and correct response only if $i = j$, which happens with probability $1/2$.

By repeating the protocol k times, she can cheat only with probability $1/2^k$, which is rapidly decreasing.

Transcript of a Zero-Knowledge Protocol

P : Commitment r

V: Chalenge c

P: Response s

If there is a **simulator** $S'(c, s)$ such that

$$r = S'(c, s)$$

the protocol is Zero Knowledge, because we do not need the secret to find out the commitment.

3-Coloring

$CZK =$ class of all decision problems which can be verified to be true using a computational zero-knowledge proof.

Theorem 1 *The problem of 3-colourability of a graph lies in* CZK*, assuming a computationally hiding commitment scheme exists.*

Theorem 2 *If one-way functions exist then* $CZK = IP$*, and hence* $CZK = PSPACE$*.*

$IP =$ interactive proof systems

Commitments

Bob: $r = \mathrm{R}(\text{scissors}, k)$

Alice: paper

Bob: I said scissors, the proof is k.

Alice computes $\mathrm{R}(\text{scissors}, k) = r$.

Alice: You won!

As the preimages of R are hard to compute, Alice has no time to find out that Bob actually encrypted scissors. Also, If Alice says rock, Bob has no time to find a k' such that:

$\mathrm{R}(\text{scissors}, k) = \mathrm{R}(\text{paper}, k')$.

Proof of Theorem 1

Consider a graph $G = (V, E)$ in which the prover knows a colouring ψ of G, i.e. a map $\psi : V \to \{1, 2, 3\}$ such that $\psi(v_1) \neq \psi(v_2)$ if $(v_1, v_2) \in E$. The prover first selects a commitment scheme $R(x; k)$ and a random permutation π of the set $\{1, 2, 3\}$. The function $\pi(\psi(v))$ defines another 3-colouring of the graph. Now the prover commits to this second 3-colouring by sending to the verifier the commitments

$$c_i = R(\pi(\psi(v_i)); k_i)$$

for all $v_i \in V$. The verifier then selects a random edge $(v_i, v_j) \in E$ and sends this to the prover. The prover now decommits to the values of $\pi(\psi(v_i))$ and $\pi(\psi(v_j))$, and the verifier checks that $\pi(\psi(v_i)) \neq \pi(\psi(v_j))$. $\square$

Proof

Completeness: The above protocol is complete since any valid prover will get the verifier to accept with probability one.

Soundness: If we have a cheating prover then at least one edge is invalid, and with probability at least $1/|E|$ the verifier will select an invalid edge. Thus with probability at most $1 - 1/|E|$ a cheating prover will get a verifier to accept. By repeating the above proof many times one can reduce this probability to as low a value as we require.

Zero-Knowledge: Assuming the commitment scheme is computationally hiding, the obvious simulation and the real protocol will be computationally indistinguishable.

Manuel Blum, 1986

S logical proof system (Russel - Whitehead), ϕ theorem provable in S, L bound of the length of the proof π

Theorem 3 *It is possible to efficiently transform π into a* zero-knowledge proof *of ϕ. P persuades V that with high probability,*

1. *the theorem ϕ has a proof π in S of length $< L$, and*

2. *P knows π.*

Protocols in Cyclic Groups

Discrete Logarithm difficult to compute in cyclic groups

Not really.

$$\langle g \rangle = (\mathbb{Z}_n, +, 0) \leftrightarrow$$

$$\leftrightarrow \mathrm{gcd}(g, n) = 1 \leftrightarrow g \in (\mathbb{Z}_n^{\times}, \cdot, 1)$$

- Compute $g^{-1} \bmod n$.

- $\log_g x = xg^{-1} \bmod n$.

Instead

- Take a prime q.

- Find a prime $p = sq + 1$.

- Find element $x \in \mathbb{F}_p$ such that

$$g = x^s \neq 1$$

- $\langle g \rangle \leq \mathbb{F}_p^\times$ is a cyclic group of order q. Computations are done modulo p and the discrete logarithm is hard to compute.

Schnorr's Identification Protocol

Peggy's secret is now the discrete logarithm x of y with respect to g in some finite abelian group G of prime order q.

P$\rightarrow$V: $r = g^k$ for a random k,

V$\rightarrow$P: e,

P$\rightarrow$V: $s = (k + xe) \bmod q$,

V: $r = g^s y^{-e}$.

Probability of successful cheating $= 1/q$.

No Commitment Used Twice!

(r, e, s) and (r, e', s')

$$r = g^s y^{-e} = g^{s'} y^{-e'}$$

$$s + x(-e) = s' + x(-e') \mod q$$

$$x = \frac{s'-s}{e'-e} \mod q$$

Abstractisation

$R(x, k)$ computes the commitmemt r of P, k random nonce.

c is the challenge of V.

$S(c, x, k)$ computes the response s of P.

$V(r, c, s)$ the verification algorithm of V.

$S'(c, s)$ simulator's algorithm which creates a value of a commitment r which will verify the transcript (r, c, s). [Schnorr: $r = c^s y^c$].

Chaum–Pedersen Protocol

Peggy wishes to prove she knows two discrete logarithms

$$y_1 = g^{x_1} \text{ and } y_2 = h^{x_2}$$

such that $x_1 = x_2$, i.e. we wish to present both a proof of knowledge of the discrete logarithms, but also a proof of equality of the hidden discrete logarithms.

$x_1 = x_2 = x$

g, h generate groups of prime order q

$$R(x, k): \quad (r_1, r_2) = (g^k, h^k)$$

$$S(c, x, k): \quad s = k - c \cdot x \mod q$$

$$V((r_1, r_2), c, s): \quad r_1 = g^s \cdot {y_1}^c \wedge r_2 = h^s \cdot {y_2}^c$$

$$S'(c, s): \quad (r_1, r_2) = (g^s \cdot {y_1}^c, h^s \cdot {y_2}^c)$$

Proving Knowledge of Commitments

Often one commits to a value using a commitment scheme, but the receiver is not willing to proceed unless one proves one knows the value committed to.

For the commitment scheme

$$B(x) = g^x$$

Schnorr's protocol does this.

For Pedersen's Commitment

$$B_a(x) = h^x g^a$$

we need something different.

Prove knowledge of x_1 and x_2 such that

$$y = {g_1}^{x_1} \cdot {g_2}^{x_2}$$

where g_1 and g_2 are elements in a group of prime order q.

$R(x, k)$: $(r_1, r_2) = ({g_1}^{k_1}, {g_2}^{k_2})$

$S(c, \{x_1, x_2\}, \{k_1, k_2\})$:

$$(s_1, s_2) = (k_1 + c \cdot x_1, k_2 + c \cdot x_2) \bmod q$$

$V((r_1, r_2), c, (s_1, s_2))$:

$$ {g_1}^{s_1} \cdot {g_2}^{s_2} = y^c \cdot r_1 \cdot r_2 $$

$S'(c, (s_1, s_2))$: (r_1, r_2) where r_1 is chosen at random and

$$ r_2 = \frac{{g_1}^{s_1} \cdot {g_2}^{s_2}}{y^c \cdot r_1} $$

Disjunctive Zero-Knowledge Proofs

We wish to show we know either a secret x or a secret y, without revealing which of the two secrets we know. Protocol due to Cramer, Damgård and Schoenmakers.

For proving knowledge of x:

$$R_1(x, k_1), S_1(c_1, x, k_1), V_1(r_1, c_1, s_1), S_1'(c_1, s_1)$$

For proving knowledge of y:

$$R_2(y, k_2), S_2(c_2, y, k_2), V_2(r_2, c_2, s_2), S_2'(c_2, s_2)$$

Suppose that we know x but not y. We choose c_2 and s_2 from their correct domains.

$$R(x, k_1) = (r_1, r_2) = (R_1(x, k_1), S_2'(c_2, s_2))$$

$$V \to c$$

$$S(c, x, k_1) = (c_1, c_2, s_1, s_2) =$$

$$= (c \oplus c_2, c_2, S_1(c \oplus c_2, x, k_1), s_2)$$

$$V((r_1, r_2), c, (c_1, c_2, s_1, s_2)) :$$

$$c = c_1 \oplus c_2 \ \wedge \ V_1(r_1, c_1, s_1) \ \wedge \ V_2(r_2, c_2, s_2)$$

$$S'(c, (c_1, c_2, s_1, s_2)) = (r_1, r_2) =$$

$$= (S_1'(c_1, s_1), S_2'(c_2, s_2))$$

Disjunctive Schnorr Protocol

We prove knowledge of either x_1 or x_2 such that

$$y_1 = g^{x_1} \;\wedge\; y_2 = g^{x_2}$$

where $g \in G$ of prime order q.

We know x_i but not x_j.

We randomly select $c_j, k_i \in \mathbb{F}_q^{\times}$ and $s_j \in G$, and the commitment is

$$R(x_i, k_i) = (r_1, r_2)$$

where $r_i = g^{k_i}$ and $r_j = g^{s_j} \cdot {y_j}^{-c_j}$.

Let $c \in \mathbb{F}_q^{\times}$ be the challenge of V.

P computes:

$$\begin{aligned} c_i &= c - c_j \mod q \\ s_i &= k_i + c_i \cdot x_i \mod q \end{aligned}$$

The response is: (c_1, c_2, s_1, s_2)

The verifier checks the proof:

$$c = c_1 + c_2 \wedge r_1 = g^{s_1} \cdot {y_1}^{-c_1} \wedge r_2 = g^{s_2} \cdot {y_2}^{-c_2}$$

How to prove a binary choice

The prover makes a binary choice $v \in \{-1, 1\}$ and wants to convince the verifier that the choice does respect the condition, without revealing it. This works over the Pedersen Commitment $B = g^{\alpha} h^{v}$. Let G be a group of prime order q, and two elements $g, h \in G$.

Cramer, Franklin, Schoenmakers, Yung for a complicated system of electronic vote.

Commitment

$v = 1$

P chooses randomly $\alpha, r_1, d_1, w_2 \in \mathbb{F}_q$.

$$B = g^{\alpha} h,$$

$$a_1 = g^{r_1} (Bh)^{-d_1},$$

$$a_2 = g^{w_2}.$$

$v = -1$

P chooses randomly $\alpha, r_2, d_2, w_1 \in \mathbb{F}_q$.

$$B = g^{\alpha}/h,$$

$$a_1 = g^{w_1},$$

$$a_2 = g^{r_2} (B/h)^{-d_2}.$$

(B, a_1, a_2)

Challenge and Response

V makes a challenge $c \in \mathbb{F}_q$.

P computes a response.

$v = 1$

$$d_2 = c - d_1,$$

$$r_2 = w_2 + \alpha d_2.$$

$v = -1$

$$d_1 = c - d_2,$$

$$r_1 = w_1 + \alpha d_1.$$

(d_1, d_2, r_1, r_2)

Verification

$$d_1 + d_2 = c,$$

$$g^{r_1} = a_1 (Bh)^{d_1},$$

$$g^{r_2} = a_2 (B/h)^{d_2}.$$

Exercise

Imagine a protocol in which I prove you that I know the content of this presentation, but without revealing this content to you.