3 Zero-knowledge proofs

A perfect zero-knowledge proof is an interactive proof in which the prover P convinces the verifier V that an input x possesses some specific property but at the end of the protocol V has learnt nothing on how to prove that x has the given property. let us illustrate this by way of example.

GRAPH ISOMORPHISM
Input: two grpahs G_1 and G_2 with vertex set $\{1, 2, \ldots, n\}$
Question: Are G_1 and G_2 isomorphic?

Consider the following interactive proof system;

(1) The prover P chooses a random permutation $\pi \in S_n$. He then computes $H = \pi(G_1)$ and sends H to V.

(2) The verifier V chooses a random index $i \in \{1, 2\}$ and sends this to P.

(3) The prover P computes a permutation $\sigma \in S_n$ such that $H = \sigma(G_i)$ and sends σ to V.

(4) The verifier V checks that H is the image of $G - i$ under the permutation σ.

Steps (1)–(4) are repeated t times and V accepts P's proof iff the check in step (4) is successful everytime, otherwise V rejects the proof.

Now consider the probability that V accepts $(G-1, G_2)$. If G_1 and G_2 are isomorphic then P can in each case find a permutation σ such that $H = \sigma(G_i)$ so the probability of V accepting is 1.

If G_1 and G_2 are not isomorphic then no matter what dishonest strategy the prover employs, he can fool V at most half of the time since either he chooses $H = \pi(G_1)$ so he can give the correct response when $i = 1$, or he chooses $H = \pi(G_2)$ and so can give the correct response when $i = 2$. However, to fool V he needs to answer correctly all t times and the probability that this occurs is at most

$$\Pr(\text{ V accepts } (G_1, G_2)) = \left(\frac{1}{2}\right)^t .$$

It is easy to see that all of V's computations may be performed in polynomial time. hence this is a polynomial time interactive proof.

Intuitively this must be a zero-knowledge proof because all that V learns in each round is a random isomorphic copy H of G_1 or G_2 and a permutation which takes either $H \to G_1$ or $H \to G_2$ but not both. Crucially V could have computed these for himself without interacting with P. he could simply have chosen a random index $i \in \{1, 2\}$ and a random permutation $\sigma \in S_n$.

To make this idea more precise we say that V's transcript of the interactive proof consists of the following:

(1) the graphs G_1 and G_2;

(2) the messages exchanged between P and V;

(3) the random numbers $I_1, i_2, \ldots, i_t$.

In other words the transcript is

$$T = [(G_1, G_2), (H_1, i_1, \sigma_1), (H_2, i_2, \sigma_2), \ldots, (H_t, i_t, \sigma_t)].$$

The key reason why this reason is zero-knowledge is that if G_1 and G_2 are isomorphic then anyone can forge these transcripts, whether or not they actually participate in an interactive proof with P. All a forger requires is the input and a polynomial time probabilistic Turing machine.

Formally, we can define a forger to be a polynomial time probabilistic Turing machine, F, which produces forged transcripts. For such a machine and an input x we let $\mathcal{F}(x)$ denote the set of all forged transcripts and $\mathcal{T}(x)$ denote that set of all possible true transcripts. We have two probability distributions on the set of all possible transcripts, both true or forged.

First, we have $\Pr_{\mathcal{T}}[T]$, the probability that T occurs as a transcript of an actual true interactive proof conducted by V with P on input x. This depends on the random bits used by by V and P. Second, we have $\Pr_{\mathcal{F}}[T]$, the probability that T is the transcript produced by the forger F, given the input x. This depends on the random bits used by F, since P and V play no part in producing the forgery.

An interactive proof system for a language L is *perfect zero knowledge* iff there exists a forger F such that for any $x \in L$ we have

(i) the set fo forged transcripts is identical to the set of true transcripts, i.e. $\mathcal{F}(x) = \mathcal{T}(x)$;

(ii) the two associated probability distributions are identical, i.e. i.e. for any transcript $T \in \mathcal{T}(x)$ we have $\Pr_{\mathcal{T}}[T] = \Pr_{\mathcal{F}}[T]$.

Theorem 13. The interactive proof system for `GRAPH ISOMORPHISM` given above is perfect zero knowledge.

Proof. To simplify matters, assume that the verifier is honest and follows the protocol correctly

Suppose G_1 and G_2 are isomorphic. A possible transcript looks a s follows

$$T = [(G_1, G_2), (H_1, i_1, \sigma_1), (H_2, i_2, \sigma_2), \ldots, (H_t, i_t, \sigma_t)],$$

where each $i_j \in \{1, 2\}$, each $\sigma \in S_n$ and each $H_j = \sigma_j(G_{i_j})$. The forger F knows the input (G_1, G_2) and so can easily produce any of the possible true transcripts. All he needs to do is first write down the input and then choose random $i \in \{1, 2\}$ and $\sigma \in S_n$ and form the triple $(\sigma(G_i), i, \sigma)$. He then repeats this t times to produce a transcript. Clearly the set of forged transcripts and the set of true transcripts will be identical, so $\mathcal{F}(G_1, G_2) = \mathcal{T}(G_1, G_2)$.

Moreover the forger F will have an equal chance of producing any possible transcript. But it is also the case that true transcripts produced by the interaction of V with P will also occur with equal probability. Hence if the total number of transcripts is N and T is a transcript then

$$\Pr_{\mathcal{T}}[T] = \Pr_{\mathcal{F}}[T] = \frac{1}{N}.$$

So both conditions hold. □

Te above proof is incomplete. To show that the protocol is reall perfect zero knowledge we need to deal with the possibility that the verifier may be dishonest

Now we are going to describe a perfect zero knowledge proof for `QUADRATIC RESIDUE`

`QUADRATIC RESIDUE`

Input: integer n the product of two unknown distinct primes and an integer $b \in \mathbb{Z}_n^*$
Question: is b a quadratic residue modulo n?

Obviously there is a protocol showing that QR belongs to IP, the prover simply gives a square root of b modulo n. Clearly this is not a zero knowledge proof. However there is a zero knowledge interactive proof which we describe below.

(1) The prover P chooses a random $x \in \mathbb{Z}_n^*$ and sends $y = x^2 \pmod{n}$ to V.

(2) The verifier chooses a arndom integer $i \in \{0, 1\}$ and sends i to P.

(3) The orver P computes

$$z = \begin{cases} x \pmod{n}, & \text{if } i = 0, \\ x\sqrt{b} \pmod{n}, & \text{if } i = 1, \end{cases}$$

and sends this to V.

(4) The verifier V accepts iff $z^2 = b^i y \pmod{n}$.

If b is not a quadratic residue modulo n then any prover will always fail one of the possible tests no matter what he chooses as y. To be precise, if a prover send $y = x^2 \pmod{n}$ then he will be able to respond correctly to the challenge $i = 0$ but not to the challenge $i = 1$ (since $\sqrt{b}$ does not exist). While if he tries to cheat and chooses $y = b^{-1}x^2 \pmod{n}$ then he will now be able to respond correctly to the challenge $i = 1$ by sending $z = x$ but not to the challenge $i = 0$ (again since $\sqrt{b}$ does not exist). So whatever a prover does if b is a quadratic non-residue then

$$\Pr[\text{ V accepts } b] \leq \frac{1}{2}.$$

Hence this is a polynomial time interactive proof. Is this a perfect zero knowledge proof?

We need to consider what V learns in the process of interacting with P. After t rounds of interaction with P, the verifier V has the following transcript

$$T = [(n, b), (x_1^2, i_1, x_1^{b^{i_1/2}}, (x_2^2, i_2, x_2^{b^{i_2/2}}, \ldots, (x_t^2, i_t, x_t^{b^{i_t/2}})],$$

where each $x_j \in \mathbb{Z}_n^*$ and $i_j \in \{0, 1\}$.

We now consider how a forger might produce such a transcript. First he wries down the input (n, b). He then chooses $i \in \{0, 1\}$. If $i = 0$ he chooses $x \in \mathbb{Z}_n^*$ and calculates $y = x^2 \pmod{n}$. If $i = 1$ he chooses $x \in \mathbb{Z}_n^*$ and computes $b^{-1} \pmod{n}$ and $y = x^2 b^{-1} \pmod{n}$. Finally he produces the forged triple (y, i, x).

It is straightforward to check that this forging algorithm produces transcripts with an identical probability distribution to that of the true transcripts.

Problems.

3.1 Complete the proof that the interactive proof system for `QR` given above is perfect zero knowledge, assuming the verifier is honest.

References

[1] O. Goldreich, Modern Cryptography, probabilistic Proofs amd Pseudo-randomness, Algorithms and Combinatorics Series, 17, Springer Verlag, 1999.

[2] O. Goldreich, Foundations of Cryptography, Cambridge University Press, 2001.

[3] O. Goldreich, Foundations of Cryptography, Cambridge University Press, 2004.

[4] O. Goldreich, S. Micali, A. Widgerson, Proofs that yield nothing but their validity in all languages in NP have zero knowledge proof systems, Journal of the ACM 38(1991), 691-729.

[5] A. Salomaa, Public-key Cryptography, Springer, Berlin-Heidelberg-New York, 1990.

[6] D. Stinson, Cryptography: Theory and Practice (2nd edn) Boca Raton, FL, Chapman& Hall/CRC, 2002.

[7] J. Talbot, D. Welsh, Complexity and Cryptography - an Introduction, Cambridge University Press, 2006.