An almost zero-knowledge proof of my knowledge on zero-knowledge proof

Naoki Hiratani

Tea talk

2019-05-29

What’s zero-knowledge proof?

Proving the knowledge on what *x* is, without revealing what *x* is.

Examples

- Wally/Waldo problem:

  Proving that you found Wally, without revealing the location of Wally.

- Cryptocurrency (Zcash, Zcoin…):

  Validating the transaction, without information on the sender, the recipient and the transaction amount

- Nuclear disarmament

  Proving destruction of nuclear weapons without revealing all the military secrets

How does it work?

Consider the Wally problem: Peggy wants to convince Victor that she found Wally.

Suppose there are two illustrations: one contains Wally, the other doesn’t, otherwise identical.

For Victor, two illustrations look exactly the same, due to his Wally-blindness.

Given that, Peggy has to convince Victor that two illustrations are different.

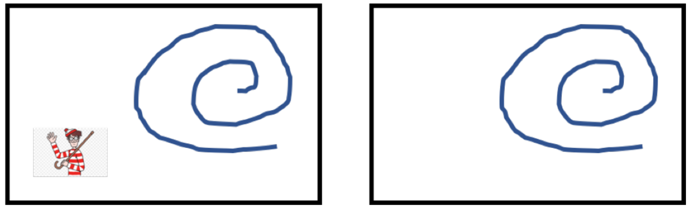
Repeat following procedure:

1. Victor shows Peggy one of the illustrations.
2. Victor randomly switch, or doesn’t switch the illustrations behind Peggy’s back.
3. Peggy answers if Victor switched the illustrations, or not.

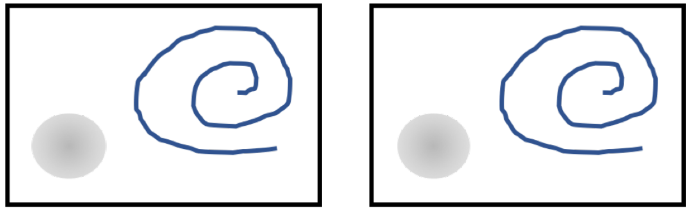
If Peggy correctly guesses if they are switched or not for *K* continuous time, Victor is convinced of her statement with *p*-value: 2^{-K}

Peggy doesn’t need to disclose where Wally is, nor which illustration contains Wally.

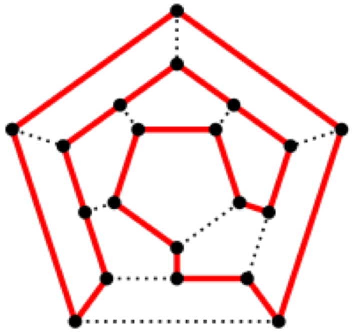
Peggy’s perspective



Victor’s perspective



Application: Hamilton cycle problem



Remember that

- Hamilton cycle problem is NP-complete
- No known polynomial algorithm exists for graph isomorphism problem

Peggy wants to convince Victor that she found a Hamilton cycle on a graph *G*, without revealing the cycle.

Repeat the following procedure:
1. Peggy generates a graph *H* isomorphic to *G*, by randomly permutating the labels of the nodes.

2. Victor asks Peggy to either
   a) show the isomorphism between *H* and *G*
   b) show a Hamiltonian cycle of *H*

If Peggy knows a true Hamilton cycle on *G*, both **a)** and **b)** are easy.

a) doesn’t reveal anything about the cycle, and given **b)**, Victor still has to solve a graph isomorphism problem.

Peggy can fabricate a graph which is either isomorphic to *G*, or having a known Hamiltonian cycle, but cannot do both at the same time.