Homework 26

Joe Baker, Brett Schreiber, Brian Knotten

March 26, 2018

46

a

In the protocol described in 9.17 b, the prover attempts to convince the verifier that a graph G with n vertices contains a Hamiltonian cycle C. First, the prover randomly permutes the the vertices of G and encrypts every element of the adjacency matrix of G such that for any given ciphertext c, it is equally probable that any of the elements was the original plaintext. The encrypted elements are then presented to the verifier. Next, the verifier randomly chooses $b = 0$or $b = 1$ and sends b to the prover. If the verifier sends 0, then the prover reveals to the verifier the permutation used on G's vertices, the permutation's adjacency matrix, and the randomness used to encrypt the elements of the adjacency matrix. If the verifier sends 1, then the prover sends the verifier a permutation of the cycle C and the randomness used to encrypt the edges of the cycle in the adjacency matrix. The verifier then checks either if the permuted adjacency matrix corresponds with G properly (if $b = 0$) or if the permuted cycle is indeed a Hamiltonian cycle and if the corresponding edges match with the the prover's original message.

b

An interactive proof for an NP-language L is computationally zero knowledge if, for all probabilistic poly-time interactive strategies V^* there is a probabilistic poly-time algorithm S^* such that for all $x \in L$, the distributions produces by V^* and S^* on x are indistinguishable to all efficient algorithms.

c

The protocol described in section a is intuitively computationally zero knowledge because, if the the verifier did have an algorithm to obtain useful information while conversing with the prover, then the algorithm could be used to obtain the information without talking to the prover: The verifier can first simulate the prover by randomly encrypting either the graph or any n-cycle and presenting it to the verifier. Next, the verifier acts as itself and uses the algorithm to decide whether to request a graph or cycle. The algorithm cannot guess with probability above $\frac{1}{2}$ that the encrypted information is either a graph or a cycle. Clearly, the verifier can obtain the benefit of the algorithm without interacting with the prover, so it is computationally zero knowledge.

47

Let's define the Toffoli gate on 3 input wires: a, b, c as the output a', b', c', where $a' = a$, $b' = b$, and $c' = \neg c$ if $a = b = 1$, else $c' = c$.

The Toffoli gate is reversible, because every combination of outputs indicate what inputs were used. The input wires can be determined from the following procedure: given output wires a', b', c', the input wires $a = a', b = b'$, and $c = \neg c'$ if $a = b = 1$, else $c = c'$.

The Toffoli gate is universal, because two Toffoli gates can be used to construct a NAND gate, which is universal. We will make a NAND gate for input wires x and y. Feed x, y, and 1 into a Toffoli gate such that $a = x, b = y, c = 1$. The output wire $c' = \neg 1 = 0$ if and only if $x = y = 1$, therefore $c' = \neg(x \wedge y)$. Thus a Toffoli gates can be used to construct a NAND gate, and so the Toffoli gate is universal.

Alternatively, one can construct a NOT gate and an AND gate as follows:

NOT where x is the input and c' is the output: $a = 1, b = 1, c = x$. Then $a' = 1, b' = 1, c' = \neg x$.
AND where x and y are inputs and c' is the output: $a = x, b = y, c = 0$. Then $a' = x, b' = y, c' = 1$ iff a and b are both 1. So $c' = a \wedge b$.

48

a

0. The photon starts in super-positional state:

$$a\,|H\rangle + b\,|V\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$$

1. Then a half-silvered mirror (Hadamard Operation):

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} \frac{a+b}{\sqrt{2}} \\ \frac{a-b}{\sqrt{2}} \end{bmatrix}$$

2. Then a full-silvered mirror (Not Operation):

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{a+b}{\sqrt{2}} \\ \frac{a-b}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{a-b}{\sqrt{2}} \\ \frac{a+b}{\sqrt{2}} \end{bmatrix}$$

3. Then a half-silvered mirror (Hadamard Operation):

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{a-b}{\sqrt{2}} \\ \frac{a+b}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} a \\ -b \end{bmatrix}$$

So the outgoing state of the photon is $a\,|H\rangle - b\,|V\rangle$

b

The probability of the observer seeing the photon come out of the mirror horizontally is: a^2

c

The probability of the observer seeing the photon come out of the mirror vertically is: $(-b)^2 = b^2$