CHAPTER 21

Zero-Knowledge Proofs

Chapter Goals

- To introduce zero-knowledge proofs.
- To explain the notion of simulation.
- To introduce Sigma protocols.
- To explain how these can be used in a voting protocol.

21.1. Showing a Graph Isomorphism in Zero-Knowledge

Suppose Alice has a password and wants to log in to a website run by Bob, but she does not quite trust the computer Bob is using to verify the password. If she just sends the password to Bob then Bob's computer will learn the whole password. To get around this problem one often sees websites that ask for the first, fourth and tenth letter of a password one time, and then maybe the first, second and fifth the second time and so on. In this way Bob's computer only learns three letters at a time. So the password can be checked but in each iteration of checking only three letters are leaked. It clearly would be better if Bob could verify that Alice has the password in such a way that Alice never has to reveal *any* of the password to Bob. This is the problem this chapter will try to solve.

So we suppose that Alice wants to convince Bob that she knows something without Bob finding out exactly what Alice knows. This apparently contradictory state of affairs is dealt with using zero-knowledge proofs. In the literature of zero-knowledge proofs, the role of Alice is called the prover, since she wishes to prove something, whilst the role of Bob is called the verifier, since he wishes to verify that the prover actually knows something. Often, and we shall also follow this convention, the prover is called Peggy and the verifier is called Victor.

The classic example of a zero-knowledge proof is based on the graph isomorphism problem. Given two graphs G_1 and G_2, with the same number of vertices, we say that the two graphs are isomorphic if there is a relabelling (i.e. a permutation) of the vertices of one graph which produces the second graph. This relabelling ϕ is called a graph isomorphism, which is denoted by

$$\phi : G_1 \longrightarrow G_2.$$

It is a computationally hard problem to determine a graph isomorphism between two graphs. As a running example consider the two graphs in Figure 21.1, linked by the permutation $\phi = (1, 2, 4, 3)$.

Suppose Peggy knows the graph isomorphism ϕ between two public graphs G_1 and G_2, so we have $G_2 = \phi(G_1)$. We call ϕ the prover's private input, whilst the graphs G_1 and G_2 are the public or common input. Peggy wishes to convince Victor that she knows the graph isomorphism, without revealing to Victor the precise nature of the graph isomorphism. This is done using the following zero-knowledge proof.

N.P. Smart, *Cryptography Made Simple*, Information Security and Cryptography, DOI 10.1007/978-3-319-21936-3_21

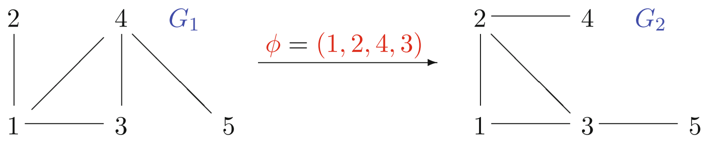

FIGURE 21.1. Example graph isomorphism

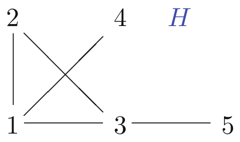

FIGURE 21.2. Peggy's committed graph

- Peggy takes the graph G_2 and applies a secret random permutation ψ to the vertices of G_2 to produce another isomorphic graph $H \leftarrow \psi(G_2)$. In our running example we take $\psi = (1,2)$; the isomorphic graph H is then given by Figure 21.2.
- Peggy now publishes H as a **commitment**. She of course knows the following secret graph isomorphisms

$$\begin{aligned} \phi : G_1 &\longrightarrow G_2, \\ \psi : G_2 &\longrightarrow H, \\ \psi \circ \phi : G_1 &\longrightarrow H. \end{aligned}$$

- Victor now gives Peggy a **challenge**. He selects[1] $b \in \{1,2\}$ and asks for the graph isomorphism between G_b and H
- Peggy now gives her **response** by returning either $\chi = \psi$ or $\chi = \psi \circ \phi$, depending on the value of b.
- Victor now verifies whether $\chi(G_b) = H$.

The transcript of the protocol then looks like

$$\begin{aligned} P &\longrightarrow V : H, \\ V &\longrightarrow P : b, \\ P &\longrightarrow V : \chi. \end{aligned}$$

In our example if Victor chooses $b = 2$ then Peggy simply needs to publish ψ. However, if Victor chooses $b = 1$ then Peggy publishes

$$\psi \circ \phi = (1,2) \circ (1,2,4,3) = (2,4,3).$$

We can then see that $(2,4,3)$ is the permutation which maps graph G_1 onto graph H. But to compute this we needed to know the hidden isomorphism ϕ. Thus when $b = 2$ Victor is checking whether Peggy is honest in her commitment, whilst if $b = 1$ he is checking whether Peggy is honest in her claim to know the isomorphism from G_1 to G_2.

If Peggy does not know the graph isomorphism ϕ then, before Victor gives his challenge, she will need to know the graph G_b which Victor is going to pick. Hence, if Peggy is cheating she will

[1] Since it is seleted by Victor we denote the value b in blue.