XI. Zero Knowledge

Idee: Wir wollen (interaktiv) beweisen, dass wir ein Geheimnis kennen, ohne das Geheimnis selbst zu verraten.

XI.1. Eigenschaften:

- Korrektheit: Ein Beweiser, der das Geheimnis nicht kennt, soll einen Prüfer nur mit vernachlässigbarer Wahrscheinlichkeit davon überzeugen können, es zu kennen.
- Zero Knowledge: Für jeden Prüfer gibt es einen Simulator, der einen Mitschrieb der Beweiskommunikation selbst erzeugen kann, ohne den Beweis zu kennen.

XI.2. Beispiel: Graph-Isomorphismus

XI.2.1. Ablauf

- allen bekannt: zwei Graphen G_1 und G_2
- Geheimnis des Beweisers: ein Graph-Isomorphismus zwischen G_1 und G_2
- der Beweiser erzeugt einen weiteren zufälligen Graphen, der isomorph zu G_1 und G_2 ist, und gibt ihn dem Prüfer
- der Prüfer fordert den Isomorphismus vom neuen Graphen zu einem der beiden Graphen G_i
- der Beweiser gibt den Isomorphismus bekannt
- das Spiel wird häufig wiederholt

XI.2.2. Eigenschaften

- kennt der Beweiser das Geheimnis, so kann er dem Prüfer immer den geforderten Isomorphismus angeben
- Korrektheit: kennt er ihn nicht, kann er nur einen der beiden Isomorphismen angeben (den, mit dem er den neuen Graphen erzeugt hat), und wird bei häufigem Wiederholen erwischt
- Zero Knowledge: weiß der Beweiser vorher, welchen Isomorphismus der Prüfer sehen will, so bereitet er genau diesen vor

XI.3. Beispiel: Graph-3-Färbbarkeit

Mit Graph-3-Färbbarkeit wird die Frage bezeichnet, ob zu einem gegebenen Graphen eine Knotenfärbung mit 3 Farben existiert, sodass direkt verbundene Knoten immer ungleiche Farben haben. Graph-3-Färbbarkeit ist ein NP-vollständiges Problem.

XI.3.1. Ablauf

- allen bekannt: ein Graph G
- Geheimnis des Beweisers: eine 3-Färbung von G
- der Beweiser benennt die Farben zufällig um (dabei bleibt die Färbung eine 3-Färbung)
- der Beweiser verschlüsselt alle Knoten und zeigt dies dem Prüfer
- der Prüfer wählt eine Kante
- der Beweiser entschlüsselt die zugehörigen Knoten
- dieses Spiel wird häufig wiederholt (mit immer neuer Vertauschung der drei Farben, damit der Prüfer das Geheimnis nicht lernen kann)

XI.3.2. Eigenschaften

- Korrektheit: gibt es keine 3-Färbung, so sind immer irgendwo zwei Farben gleich und der Beweiser wird bei häufigem Wiederholen erwischt
- Zero Knowledge: weiß der Beweiser vorher, welche Kante gefragt wird, verschlüsselt er dort zwei zufällige, verschiedene Farben