Universität Siegen
Lehrstuhl Theoretische Informatik
Markus Lohrey

Übungsblatt 13

Aufgabe 1 (Interaktive Socken)**.** Alice hat eine rote Socke und eine grüne Socke. Bob hat eine Rot-Grün-Schwäche und glaubt Alice nicht, dass ihre Socken unterschiedliche Farben haben. Geben Sie ein interaktives Protokoll an, mit dem Alice Bob überzeugen kann, dass ihre Socken tatsächlich unterschiedliche Farben haben.

Lösung. Alice zeigt Bob zwei Socken und behauptet, dass eine Socke rot und die andere grün ist. Bob hat nun die Möglichkeit, die beiden Socken zu vertauschen, ohne dass Alice dies sehen darf. Danach muss Alice beantworten, ob diese getauscht wurden oder nicht. Da Bob weiß, welche der Socken rot bzw. grün sein sollen, kann er sofort erkennen, wenn Alice die Frage falsch beantwortet. Er weiß dann also, dass beide Socken dieselbe Farbe haben. Wenn Alice die Frage richtig beantwortet, so können die Socken entweder dieselbe Farbe haben und Alice hat „geraten“ (Wahrscheinlichkeit $1/2$), ob Bob die Socken vertauscht hat, oder sie haben tatsächlich unterschiedliche Farben. Wiederholt man obiges Vorgehen n mal und Alice antwortet immer richtig, so haben die Socken entweder unterschiedliche Farben oder sie haben dieselben Farben und Alice hat mit Wahrscheinlichkeit $1/2^n$ richtig geraten.

Aufgabe 2 (3-Färbbarkeit)**.** Sei $G = (V, E)$ ein Graph, für den Alice eine 3-Färbung kennt. Sie möchte nun Bob davon überzeugen, ohne Bob die genaue 3-Färbung mitzuteilen (Zero Knowledge). Geben Sie dazu ein interaktives Protokoll an.

Lösung. Alice wählt in jeder Runde zufällig eine Permutation π der 3-Färbung χ. Außerdem erzeugt sie ein Public-Private-Keypair (d_i, e_i) für jeden Knoten $i \in V$. Sie überträgt dann die verschlüsselte Version von $\pi(\chi(i))$ und d_i für jeden Knoten i. Mit genug Rechenaufwand könnte Bob also alle privaten Schlüssel ausrechnen und damit überprüfen, ob Alice ihm wirklich eine 3-Färbung mitgeteilt hat. Da Bob allerdings nur polynomiell rechnen kann, wählt er eine Kante $(i, j) \in E$ aus und fragt Alice nach den privaten Schlüsseln e_i und e_j. Er kann dann also für zwei benachbarte Knoten verifizieren, ob diese wirklich unterschiedliche Farben haben. Sollte Alice ihm keine 3-Färbung mitgeteilt haben, gibt es eine Kante, an der beide Knoten dieselbe Farbe haben. Bob hat dann also in jeder Runde mindestens die Chance $1/|E|$, einen Fehler zu entdecken.