Technische Universität Braunschweig

Institut für Theoretische Informatik

Dr. Jürgen Koslowski

Cryptologie 3

Aufgabenblatt 2, 2017-05-08

Aufgabe 1 [10 PUNKTE]

(a) [10 PUNKTE] Weisen Sie nach, dass Protokoll 11.3 für diskrete Logarithmen vollständig, korrekt und valide ist.

[10 PUNKTE] Untersuchen Sie Protikoll 11.3 auf die perfekte Zero-Knowledge-Eigenschaft.

Aufgabe 2 [10 PUNKTE]

In dieser Aufgabe soll ein Zero-Knowledge-Protokoll für das $\boldsymbol{NP}$-vollständige Problem HAMILTONSCHER KREIS entwickelt werden. Dessen Eingabe besteht aus einem ungerichteten Graphen G. Zu entscheiden ist, ob es einen Rundweg gibt, der alle Knoten genau einmal besucht.

(a) [4 PUNKTE] Geben Sie ein Zero-Knowledge-Protokoll an, mit dem die Beweiserin Alice den Prüfer Bob überzeugen kann, daß sie einen Hamiltonschen Kreis in einem gegebenen Graphen kennt.

Hinweis: Verwenden Sie, wie in Protokoll 11.4, verschließbare Schachteln für die Knoten und Kanten des Graphen. Alice öffnet auf Bobs Herausforderung hin entweder alle Schachteln, oder nur die Kantenschachteln, die zu dem Hamiltonschen Kreis gehören.

(b) [6 PUNKTE] Beweisen Sie für Ihr Protokoll Vollständigkeit, Korrektheit und schwache Korrektheit.

Lösungsvorschlag:

(a) **Eingabe:** ungerichteter Graph $G = \langle V, E\rangle$ mit n Knoten, etwa $V = n = \{0, 1, \ldots, n-1\}$; diese Daten sind Alice und Bob bekannt.

Wie üblich läuft das Protokoll in k Runden ab.

(1) Alice wählt eine Permutation π der Knoten in G und bereitet Schachteln B_i, $i < n$, für die Knoten und $B_{i,j}$, $i, j < n$ für die Kanten vor: B_i enthält $\pi(i)$ und $B_{i,j} = 1$ falls $\{\pi(i), \pi(j)\} \in E$, anderfalls gilt $B_{i,j} = 0$.
Alle Schachteln werden verschlossen an Bob geschickt.

(2) Bob wählt zufällig ein Bit $b \in 2 = \{0, 1\}$ und schickt dies an Alice.

(3) Falls $b = 1$ erhält Bob von Alice die Schlüssel für alle Schachteln. Damit erfährt Bob insbesiondere die Permutation π.
Falls $b = 0$ erhält Bob von Alice nur die Schlüssel für die Kantenschachteln, die Teil des Alice bekannten Hamiltonschen Kreises sind. Die Permutation π bleibt Bob aber verborgen.

(4) Bob öffnet alle Schachteln, deren Schlüssel er von Alice erhält.

Falls $b = 1$ überprüft Bob, ob die Schachteln wirklich G enthalten. Zu diesem Zweck bestimmt er die Umkehrpermutation aus den Knotenschachteln und vergleicht die resultierende Kantenmenge mit E. Dies erfordert polynomiale Zeit.

Falls $b = 0$ überprüft Bob, ob die geöffneten Kantenschachteln einen Hamiltonschen Kreis enthalten. Dazu

* muß n mit der Anzahl der geöffneten Kantenschachteln übereinstimmen;
* alle solchen müssen eine 1 enthalten;
* die Indizes der geöffneten Schachteln müssen sich zu einem(!) Kreis arrangieren lassen. (Dabei reicht es *nicht* aus, daß zu jeder Zahl $i < n$ genau zwei Schachteln existieren, in deren Index i vorkommt. Das würde auch von einer Vereinigung von zwei oder mehr Kreisen erfüllt.)

All dies erfordert ebenfalls polynomiale Zeit.

(5) Bob akzeptiert Alices Kenntnis, wenn alle k Tests positiv ausfallen.

Bemerkungen: Die jeweils neue Permutation der Knoten in jeder Runde ist nötig, damit Bob nicht durch Wahl von $b = 1$ in der ersten und $b = 0$ in der zweiten Runde den Alice bekannten Hamilton'schen Kreis bestimmen kann.

Die Möglichkeit für Bob, mittels der Wahl von $b = 1$ den von Alice verwendeten Graphen mit G abzugleichen, erschwert es Alice, statt G einen Graphen G' mit gleich vielen Knoten zu verwenden, in dem sie tatsächlich einen Hamiltonschen Kreis kennt. Aus dem gleichen Grund muß ein Betrüger Oskar an diesem Punkt des Protokolls mit Entdeckung rechnen, wenn er den Graphen G nicht kennt.

(b) **Vollständigkeit:** Falls G einen Hamiltonschen Kreis besitzt und beide Teilnehmer ehrlich spielen, fallen die Tests in (4) immer positiv aus.

Korrektheit: Hat G keinen Hamiltonschen Kreis, so kann Alice nach Erhalt von $b = 0$ Bob keine Schlüssel für eine Schachtelmenge schicken, die den entsprechenden Test in Schritt (4) besteht. Also schlägt dieser Test mit Wahrscheinlichkeit $\frac{1}{2}$ pro Runde fehl. Umgekehrt akzeptiert Bob den Beweis mit Wahrscheinlichkeit 2^{-k}.

Schwache Korrektheit: Um Bob mit Sicherheit zu betrügen (ohne einen Hamilton'schen Kreis in G zu kennen), muß Oskar den Graphen G kennen und zu Beginn jeder Runde den Wert b korrekt vorhersagen: Falls er $b = 1$ vorhersieht, schickt Oskar Bob zu Rundenbeginn eine Permutation von G, andernfalls einen Graphen G' gleicher Knotenzahl mit ihm bekannten Hamiltonschen Kreis, z.B. einen Kreis mit n Knoten oder K_n.

Da Oskar kein Hellseher ist, kann er in k Runden nur mit einer Wahrscheinlichkeit von $\leq 2^{-k}$ Bobs Herausforderung korrekt vorhersagen. Im Falle von falsch geratenem $b = 1$ muß Oskar auch einen Hamiltonscher Kreis des Graphen G raten. Dies gelingt, je nach Graph, mit einer Wahrscheinlichkeit zwischen $\frac{2}{n!}$ (falls G ein Kreis ist) bis 1 (falls $G = K_n$). Im Falle von falsch geratenem $b = 0$ kann Oskar keine nachträgliche Korrektur vornehmen. Die Wahrscheinlichkeit, daß der von Oskar verwendete Graph G' mit G übereinstimmt liegt bei 2^{n-1} (Anzahl der symmetrischen Relationen auf einer n-elementigen Menge).

Die einzige Möglichkeit für Oskar, seine Erfolgswahrscheinlichkeit bei obiger Strategie "nicht vernachlässigbar" zu erhöhen, liegt also darin, bei falsch geratenem $b = 1$ einen korrekten Hamiltonschen Kreis für G zu berechnen (in polynomialer Zeit). Aber wenn das möglich ist, kann Oskar seine Strategie für den Fall ändern, daß er $b = 0$ rät: statt eines Graphen G' mit ihm bekannten Hamiltonschen Kreis, kann er den Originalgraphen G mit berechnetem Hamiltonschen Kreis verschicken. Somit kann er mit "überwältigend großer" Wahrscheinlichkeit Alice erfolgreich imitieren.