Institut für Informatik
Prof. Dr. J. Rothe

Sommersemester 2024
Übungsblatt 8

Übung zur Vorlesung

Kryptokomplexität II

Bearbeitungszeit: 28. Mai bis 7. Juni
Verantwortlich: Roman Zorn

Begründen Sie Ihre Antworten und bereiten Sie sie so vor, dass Sie sie in der Übung präsentieren können.

Aufgabe 1: NP-Vollständigkeitsbeweis von SOS

Gegeben sei die X-3-Cover-Instanz $\langle U, \mathcal{S} \rangle$ mit

$$U = \{1, ..., 9\},$$
$$\mathcal{S} = \{S_1, ..., S_5\},$$
$$S_1 = \{1, 4, 5\}, S_2 = \{5, 6, 7\}, S_3 = \{7, 8, 9\}, S_4 = \{1, 2, 3\}, S_5 = \{1, 3, 8\}.$$

In der Vorlesung wurde gezeigt, dass SOS NP-vollständig ist. Vollziehen Sie den Beweis nach.

- Zeigen Sie zunächst, dass SOS in NP ist.
- Führen Sie anschließend die Reduktion von X-3-Cover auf SOS durch.
- Argumentieren Sie abschließend über die SOS-Instanz, ob die gegebene X-3-Cover-Instanz eine Ja- oder Nein-Instanz ist.

Aufgabe 2: Superwachsende Folgen in SOS

Zeigen Sie den Fakt aus der Vorlesung: Für Instanzen $\langle \vec{s}, T \rangle$ mit einer superwachsenden (superincreasing) Folge $\vec{s}$ kann das Problem SOS in deterministischer Polynomialzeit gelöst werden.

- Geben Sie dazu einen deterministischen Algorithmus an, der SOS für diesen speziellen Fall in Polynomialzeit löst.
- Beweisen Sie, dass Ihr Algorithmus korrekt ist.

Aufgabe 3: Rivest-Sherman-Schlüsselaustausch und -Signatur I

Definition. Eine zweistellige, totale Funktion $f : A \times A \to A$ heißt *assoziativ*, wenn für alle $x, y, z \in A$ gilt, dass $f(x, f(y, z)) = f(f(x, y), z)$ (bzw. in Infixnotation: $xf(yfz) = (xfy)fz$).

Betrachten Sie das Rivest-Sherman-Protokoll zum Schlüsselaustausch. Gegeben sei die stark nichtinvertierbare, assoziative, totale Einwegfunktion $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$.

▶ Modifizieren Sie das Schlüsselaustauschprotokoll so, dass ein Protokoll für digitale Signaturen entsteht. Geben Sie das Protokoll explizit an.

▶ Zeigen Sie, dass die Verifikationsbedingung von Ihrem Protokoll erfüllt wird.

Aufgabe 4: Rivest-Sherman-Schlüsselaustausch und -Signatur II

Definition. Eine zweistellige, totale Funktion $f : A \times A \to A$ heißt *kommutativ*, wenn für alle $x, y \in A$ gilt, dass $f(x, y) = f(y, x)$ (bzw. in Infixnotation: $xfy = yfx$).

Betrachten Sie erneut das Rivest-Sherman-Protokoll zum Schlüsselaustausch. Sei $\sigma : \Sigma^* \times \Sigma^* \to \Sigma^*$ nun eine totale, stark nichtinvertierbare, assoziative und kommutative Einwegfunktion.

▶ Modifizieren Sie mittels der Funktion σ das Schlüsselaustauschprotokoll von Rivest-Sherman zu einem Protokoll mit beliebig vielen Parteien.