Institut für Informatik
Algorithmen und Komplexität II
Prof. Dr. Johannes Köbler

SS 2001

Übungen zur Kryptologie II

5. Übung

Aufgabe 1 (2 Punkte)

Für die Zugriffs-Strukturen mit den unten angebenen Basen soll ein Secret Sharing System entworfen werden. Verwenden Sie hierfür die Schaltkreiskonstruktion von Benaloh und Leichter.

a) $\Gamma_0 = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_2, P_4\}, \{P_3, P_4\}\}$

b) $\Gamma_0 = \{\{P_1, P_3, P_4\}, \{P_1, P_2\}, \{P_2, P_3\}, \{P_2, P_4\}\}$

c) $\Gamma_0 = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_2, P_3, P_4\}, \{P_2, P_4, P_5\}, \{P_3, P_4, P_5\}\}$

Achten Sie darauf, daß die Teilschlüssel möglichst kleine Länge haben.

Aufgabe 2 (2 Punkte)

Für die Zugriffsstrukturen mit den unten angebenen Basen soll ein Secret Sharing Verfahren entworfen werden. Verwenden Sie hierfür die Vektorraum-Konstruktion von Brickell.

a) $\Gamma_0 = \{\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_3, P_4\}\}$.

b) $\Gamma_0 = \{\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}\}$.

c) $\Gamma_0 = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_2, P_3\}, \{P_1, P_4, P_5\}, \{P_2, P_4, P_5\}\}$.

Aufgabe 3

Shamirs (t, n)-Schwellwertverfahren ist ein Spezialfall der Vektorraum-Konstruktion von Brickell, wobei die vom Dealer bestimmte Menge der Vektoren $X = \{\vec{x}_1, \ldots, \vec{x}_n\}$ durch

$$\vec{x}_i = (1, x_i, x_i^2, \ldots, x_i^{t-1})$$

gegeben ist. Zeigen Sie hierzu, daß für jedes $B \subseteq \{1, \ldots, n\}$,

$$(1, 0, \ldots, 0) \in \langle \{\vec{x}_i : i \in B\} \rangle$$

genau dann gilt, wenn $\|B\| \geq t$.