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

SS 2001

Übungen zur Kryptologie II

6. Übung

Aufgabe 1

Ermitteln Sie alle Zugriffsstrukturen, für die es ein (informationstheoretisch sicheres) Secret Sharing Verfahren mit einem *deterministischen* Dealer-Algorithmus D gibt.

Aufgabe 2 (2 Punkte)

Für die Zugriffs-Strukturen mit den unten angebenen Basen soll ein Secret Sharing Verfahren entworfen werden. Verwenden Sie hierfür die Zerlegungs-Konstruktion.

a) $\Gamma_0 = \{\{1,3,4\},\{1,2\},\{2,3\}\}$, und $\rho = 3/5$.

b) $\Gamma_0 = \{\{1,3,4\},\{1,2\},\{2,3\},\{2,4\}\}$, und $\rho = 4/7$.

Aufgabe 3 (2 Punkte)

Betrachten Sie alle Zugriffsstrukturen über der Teilnehmermenge $T = \{1,2,3,4\}$. Unterteilen Sie diese in die folgenden Gruppen, indem Sie jede Zugriffsstruktur der Gruppe mit dem kleinsten Index zuordnen, zu der sie gehört.

(1) Die Basis Γ_0 besitzt eine Zerlegung $\{\Gamma_1,\ldots,\Gamma_l\}$, $l \geq 2$, so daß die zugehörigen Teilnehmermengen $T_j = \bigcup_{B\in\Gamma_j} B$ für $j = 1,\ldots,l$ paarweise disjunkt sind. (z.B. läßt sich $\Gamma_0 = \{\{1,2\},\{2,3\},\{4\}\}$ in die beiden disjunkten Teilnehmermengen $T_1 = \{1,2,3\}$ und $T_2 = \{4\}$ zerlegen).

(2) Es gibt ein Schwellwertverfahren für Γ_0.

(3) (T,Γ_0) ist ein vollständiger multipartiter Graph.

(((T,Γ_0) ist ein Graph, falls Γ_0 nur aus Paaren $\{x,y\}$ besteht. Ein solcher Graph $G = (T,\Gamma_0)$ ist *vollständig multipartit*, falls es eine disjunkte Zerlegung $\{T_1,\ldots,T_l\}$, $l \geq 2$, von T gibt, so daß $\Gamma_0 = \{\{x,y\} \mid \exists i \neq j : x \in T_i \wedge y \in T_j\}$.)

(4) (T,Γ_0) ist ein Graph.

(5) Die restlichen Zugriffsstrukturen.

Welche dieser Kategorien lassen ideale Zugriffsstrukturen zu?