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

SS 2001

Übungen zur Kryptologie II

8. Übung

Aufgabe 1

Zeigen Sie, daß es keine Einschränkung bedeutet, bei einem optischen Secret Sharing Verfahren $\|\mathcal{C}_0\| = \|\mathcal{C}_1\|$ zu fordern.

Aufgabe 2

Entwerfen Sie für die Zugriffsstruktur Γ mit der Basis $\Gamma_0 = \{\{1,2\},\{2,3\},\{3,4\}\}$ ein optisches Secret Sharing Verfahren mit $\alpha = 1/3$ und $m = 3$.
Hinweis: d darf für verschiedene $B \in \Gamma_0$ unterschiedliche Werte annehmen.

Aufgabe 3 (4 Punkte)

Seien $A_1, \ldots, A_k, B_1, \ldots, B_k \subseteq \{1, \ldots, l\}$ Mengen, so daß für jede echte Teilmenge $I \subset \{1, \ldots, k\}$ gilt:

$$\|\bigcap_{i \in I} A_i\| = \|\bigcap_{i \in I} B_i\|$$

Zeigen Sie:

a) $$\left| \|\bigcup_{i=1}^{k} A_i\| - \|\bigcup_{i=1}^{k} B_i\| \right| = \left| \|\bigcap_{i=1}^{k} A_i\| - \|\bigcap_{i=1}^{k} B_i\| \right|.$$

b) $\|\bigcup_{i=1}^{k} A_i\| \leq \frac{l}{2^{k-1}} + \|\bigcup_{i=1}^{k} B_i\|$.
(*Hinweis:* Betrachten Sie zunächst die Fälle $k = 2$ und $k = 3$.)

c) Für jedes optische (k,k)-Schwellwertverfahren gilt $m \geq 2^{k-1}$.

d) Für jedes optische SSV für eine Zugriffsstruktur mit Basis Γ_0 gilt $m \geq 2^{k-1}$, wobei $k = \max_{B \in \Gamma_0} \|B\|$.