INSTITUT FÜR INFORMATIK
KOMPLEXITÄT UND KRYPTOGRAFIE
PROF. DR. JOHANNES KÖBLER

SOMMERSEMESTER 2004

Übungen zur Kryptologie 2

10. Übung

Aufgabe 1

Benutzen Sie die Vektorraumkonstruktion, um ideale Dealeralgorithmen für die Zugriffsstrukturen mit den folgenden Basen zu erhalten.

a) $\Gamma_0 = \{\{1,2,3\},\{1,2,4\},\{3,4\}\}$,

b) $\Gamma_0 = \{\{1,2,3\},\{1,2,4\},\{1,3,4\}\}$,

c) $\Gamma_0 = \{\{1,2\},\{1,3\},\{2,3\},\{1,4,5\},\{2,4,5\}\}$.

Aufgabe 2

Benutzen Sie die Schaltkreiskonstruktion, um Dealeralgorithmen mit einer Informationsrate von 1/2 für die Zugriffsstrukturen mit den folgenden Basen zu erhalten.

a) $\Gamma_0 = \{\{1,2\},\{2,3\},\{2,4\},\{3,4\}\}$,

b) $\Gamma_0 = \{\{1,3,4\},\{1,2\},\{2,3\},\{2,4\}\}$,

c) $\Gamma_0 = \{\{1,2\},\{1,3\},\{2,3,4\},\{2,4,5\},\{3,4,5\}\}$.

Aufgabe 3

Benutzen Sie die Zerlegungskonstruktion, um Dealeralgorithmen mit der angegebenen Informationsrate für die Zugriffsstrukturen mit den folgenden Basen zu erhalten.

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

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

Aufgabe 4

Konstruieren Sie Dealeralgorithmen mit einer möglichst großen Informationsrate für alle Zugriffsstrukturen über bis zu vier Teilnehmern.