

# XVI. Data Base Privacy

## XVI.1. k-Anonymität

**FIXME:** Bild k-Anonymität, S. 57

für jede Kombination der QI in der Datenbank gibt es k Zeilen mit dieser Kombination (z.B. durch Vergrößern der QIs)

### XVI.1.1. Kritik

1. nur das Ergebnis wird beurteilt, nicht der Prozess (Seitenkanäle)
2. komponiert nicht
3. Homogenitätsattacke

## XVI.2. Differential Privacy

Datenbanken sind Mengen von Tupeln aus  $\mathbb{R}^d$ . Ein Release Mechanism nimmt eine Datenbank und liefert eine Zahl aus  $\mathbb{R}$ . Zwei Datenbanken haben „Hammingabstand“ 1, wenn sie sich nur in einem Tupel unterscheiden. Für zwei beliebige Datenbanken (aus einem gegebenen Universum) mit Hammingabstand 1 soll der Release sich höchstens um  $\epsilon$  unterscheiden: „ $\epsilon$ -differentially private“.

Methode für Release: Verrauschen

