Private Computation mit Hilfe von Quanten-Bits

Andreas Jakoby

Institut für Theoretische Informatik,
Universität zu Lübeck, Ratzeburger Allee 160, 23538 Lübeck, Germany

jakoby@tcs.uni-luebeck.de

Private Computation ist eine intensiv untersuchte Problemstellung der modernen Kryptographie. Hierbei betrachten wir das folgende Szenario: Gegeben ist eine Menge von Personen, die jeweils ein individuelles Geheimnis bewahren. Das Ziel einer *privaten Berechnung* ist es, eine von diesen Geheimnissen abhängige Funktion so zu berechnen, dass hierbei keine der Personen Informationen über die Geheimnisse der anderen Personen gewinnt, welche nicht aus dem jeweiligen Geheimnis und dem Ergebnis hergeleitet werden können.

Es ist bekannt, dass jede Boolesche Funktion von $n \geq 3$ Personen privat berechnet werden kann, wenn die zur Verfügung stehende Kommunikationsstruktur zweifach zusammenhängend ist. 1992 wurde von Kushilevitz eine exakte Klassifikation der privat berechenbaren Funktionen für den Zwei-Personen-Fall angegeben. Ist die Kommunikationsstruktur nicht zweifach zusammenhängend, so können nur wenige Funktionen privat berechnet werden (s. Bläser, Jakoby, Liskiewicz, Manthey 2002). In diesem Vortrag wollen wir zeigen, dass diese Klassifikationen ihre Gültigkeit verliert, wenn zur Kommunikation Quanten-Bits benutzt werden können.

Wir unterscheiden hierbei *nachprüfbare Sicherheit* (detectable quantum security, kurz DQS) und *schwache nachprüfbare Sicherheit* (weak detectable quantum security, kurz w-DQS). Wir werden die Funktion *pixy* vorstellen, die auf einer Kette nicht unter der ausschließlichen Benutzung von klassischen Bits privat berechnet werden kann und für diese ein DQS-Protokoll angeben. Ferner werden wir unter Benutzung von *pixy* zeigen, dass für jede Boolesche Funktion und auf jedem zusammenhängenden Netzwerk ein w-DQS Protokoll existiert. Diese Beobachtung gilt insbesondere auch für das Problem der *Quantum-Key-Distribution*.