Thema: "Kryptographie mit Spielkarten"

Vortragender: Stefan Walzer

Kurzbeschreibung:
Zuweilen kommt es vor, dass eine Gruppe von Akteuren etwas ausrechnen will, die Parameter der Rechnung aber Geheimnisse einzelner Akteure sind, also nicht öffentlich werden dürfen. Im Extremfall wird uns aufgetragen, etwas auszurechen dabei aber *gar nichts* über die Eingabe oder Ausgabe zu erfahren. Alles was wir tun und sehen, muss also stochastisch unabhängig von den Daten sein auf denen wir rechnen. Erstaunlicherweise geht das. Ein Protokoll um ein logisches AND mithilfe von 6 Spielkarten auszurechnen ist schon lange bekannt (darauf aufbauend lassen sich natürlich auch kompliziertere Funktionen auswerten).

Im Hauptteil des Vortrags soll diskutiert werden, ob weniger als 6 Karten auch ausreichen um $a \wedge b$ zu berechnen. Die Antwort ist erstaunlich facettenreich, d.h. subtile Änderungen am Berechnungsmodell machen bedeutende Unterschiede.