UELI MAURER, Zürich

Kryptografie – Paradoxa der Mathematik

Die Faszination, die von der Kryptografie ausgeht, hat mehrere Gruende. Aus historischer Sicht ist es die Tatsache, dass Erfolge der Kryptoanalyse das Weltgeschehen massgebend gepraegt haben. Aus wissenschaftlicher Sicht sind es die vielen paradoxen Resultate. Wie kann es z.B. moeglich sein, dass zwei Parteien rein durch oeffentliche Kommunikation, ohne jegliche Geheimhaltung, einen geheimen Schluessel erzeugen koennen? Und wie ist es moeglich, einen mathematischen Beweis zu fuehren, ohne dabei jegliche Information ueber den Beweis wegzugeben, ausser der Tatsache, dass er stimmt? In diesem Vortrag diskutieren wir diese und weitere mathematische Paradoxa der Kryptografie.