Vortrag von

Prof. Dr. Marian Margraf

(Freie Universität Berlin,
Fraunhofer-Institut für Angewandte und Integrierte Sicherheit)

PERFEKT SICHERE VERSCHLÜSSELUNGSVERFAHREN

13.12.2022, 18:00 Uhr
Freie Universität Berlin
Arnimallee 3, Hörsaal 001

Der Vortrag führt zunächst Verschlüsselungsverfahren ein, gibt einfache Beispiele und diskutiert verschiedene Sicherheitsbegriffe. Im Hauptteil des Vortrags wird auf den Begriff der perfekten Sicherheit eingegangen, ein Verfahren ist perfekt sicher, wenn selbst Angreifer mit unbeschränkten Ressourcen dieses Verfahren nicht brechen können. Wir definieren den Begriff formal, geben eine äquivalente Beschreibung an (ein Resultat von Shannon aus dem Jahr 1949) und zeigen, dass perfekt sichere Verschlüsselungsverfahren tatsächlich existieren. Allerdings haben sie den großen Nachteil, dass die für die Verschlüsselung eingesetzten Schlüssel mindestens so groß sein müssen wie der Informationsgehalt des zu verschlüsselnden Textes.

Unterstützt von

Deutsche Mathematiker-Vereinigung

B M G