Informatik Kolloquium
Beweisbar sichere und effiziente Kryptographie

Dr. Tsuyoshi Takagi, TU Darmstadt

16. Juni 2004, 14:00 Uhr, Gebäude 57 (Rotunde)

Zusammenfassung

Sicherheitstechniken wie Verschlüsselung und digitale Signaturen sind heute weitgehend formalisierbar. Es ist möglich, solche Systeme mit den Mitteln der Logik und der Komplexitätstheorie zu beschreiben. Die Aussagen, solche Systeme seien sicher und korrekt implementiert, sind als mathematische Sätze formulierbar.
Um den Sicherheitslevel der kryptographischen Protokolle korrekt einschätzen zu können, benötigen wir Sicherheitsmodelle. Eines dieser Standardmodelle ist die sog. Semantische Sicherheit. Ein beweisbar sicheres Kryptoverfahren ist ein solches Kryptoverfahren, welches innerhalb eines Sicherheitssystems mathematisch beweisbar ist. Das semantisch sichere Kryptoverfahren kann man mit den wichtigsten kryptographische Protokolle, nämlich SSL/TSL, IPSEC, usw., anwenden. Ich präsentiere eine sichere Konstruktion des bekannten RSA-Verfahren. Mit dieser Modellierung kann man das RSA-Verfahren semantisch sicher im an sich Standard-Modellkonvertieren.
Die Sicherheit ist nicht nur ein statistischer sondern auch ein dynamischer Prozess. Obwohl ein Sicherheitssystem sicher gegen alle bisher bekannten Angriffe ist, kann ein solches System jeder Zeit mit einem neuen Angriff zerstört werden. Gerade in letzter Zeit werden neuartige und immer raffiniertere Angriffe vorgestellt, nämlich die Fehlerattacken und die Side-Channel-Attack (SCA). In meinem Vortrag werde ich ein paar relevante Angriffe und deren Gegenmaßnahmen präsentieren.
Anschließend werde ich einen Ausblick auf meine zukünftigen Forschungspläne zum Thema Sicherheit geben und weitere wichtige Aspekte meiner Arbeit darlegen.