Effiziente und Beweisbar Sichere Digitale Signaturen im Standardmodell (Efficient and Provably Secure Signature Schemes in the Standard Model)

Dipl.-Ing. Sven Schäge, Lehrstuhl für Netz- und Datensicherheit

Digitale Signaturschemata stellen das elektronische Pendant zu klassischen Signaturen dar: Alice kann zu jedem gegebenen Dokument eine Signatur erstellen. Mit Hilfe dieser Signatur kann öffentlich überprüft werden, dass das entsprechende Dokument tatsächlich von Alice unterzeichnet wurde. Die Sicherheitseigenschaften eines Signaturschemas müssen dabei insbesondere garantieren, dass niemand außer Alice gültige Signaturen erzeugen kann, welche auf Alice als Urheber hinweisen. Neben Verschlüsselungssystemen gehören digitale Signaturen zu den wichtigsten Bausteine der modernen Kryptografie und stellen einen unverzichtbares Werkzeug für den elektronischen Geschäftsverkehrs dar. Für den praktischen Einsatz ist wichtig, dass sie nicht nur starken Angriffen widerstehen können sondern auch gleichzeitig hohe Effizienz bieten. Die vorliegende Arbeit präsentiert vier Ergebnisse aus dem Forschungsgebiet der effizienten und beweisbar sicheren digitalen Signaturen: ein effizientes digitales Signaturschema, das sicher unter der Strong Diffie-Hellman Annahme ist; neue und effizientere Sicherheitsreduktionen für zwei allgemeine Klassen von digitalen Signaturschemata; neue Sicherheitsdefinitionen, Transformationen und Konstruktionen von Two-Tier Signaturschemata; und ein neues und besonders effizientes Ringsignaturschema, welches nur auf der Computational Diffie-Hellman Annahme basiert. Alle betrachteten Schemata sind sicher im Standardmodell und basieren auf schwachen und gut untersuchten Komplexitätsannahmen.