Kryptodebatten

Durchblättert man frühere Jahrgänge der DuD, so zeigt sich, dass die in dieser Zeitschrift diskutierten Fragen der Kryptografie die Hauptentwicklungslinien der vergangenen 15 Jahren nachzeichnen. So war es Ende der neunziger Jahre die Angst vor einer möglichen staatlichen Regulierung starker kryptografischer Verfahren – sei es durch Schlüsselhinterlegung, sei es durch Verbot – gegen die zahlreiche Autoren mit Verve und guten Argumenten zu Felde zogen (u. a. Hamm, Kelm/Kossakowski, Hortmann und Blaze, DuD 4/1997; Kuner und Abelson/Anderson/Bellowin, DuD 1/1998).

Als dieser Kelch glücklich an dem noch vergleichsweise jungen Forschungsgebiet vorbeigegangen war, prägte das nach den vorausgegangenen Diskussionen überraschend offene Auswahlverfahren des US-amerikanischen NIST für den DES-Nachfolger AES, einem standardisierten symmetrischen Kryptoverfahren für die Wirtschaft, die Diskussion (Weis/Lucks, DuD 10/1999, 7 und 12/2000 und Welschenbach, 6/2001).

Anschließend zerfiel die Entwicklung in zwei Linien: Auf der einen Seite begannen sich Verfahren der „modernen", asymmetrischen Kryptographie durchzusetzen: in Public Key Infrastrukturen (u. a. Thiel, DuD 9/2000 und Böhmer, DuD 8/2001), zum Schutz digitaler Güter (siehe Watermarking, DuD 5/1998, Trusted Computing, DuD 9/2004 und 9/2005, und Digital Rights Management, DuD 2/2006) und in Gestalt von Algorithmen auf elliptischen Kurven (Paulus/Müller, DuD 9/1998; Bertsch/Bourseau/Fox, DuD 2/2002).

Gleichzeitig wurde die Suche nach Krypto-Verfahren intensiviert, deren Sicherheit nicht von dem der Sicherheit des RSA-Verfahrens zu Grunde liegenden Faktorisierungsproblem abhängt, um rechtzeitig geeignete Ersatzverfahren verfügbar zu haben, falls sich eines Tages eine Möglichkeit finden lassen sollte, RSA zu brechen oder große Zahlen mit vertretbarem Aufwand in ihre Primfaktoren zu zerlegen. Als ein viel versprechender Ansatz gilt dabei die Quantenkryptografie (Geiselmann/Müller-Quade/Steinwandt/Beth, DuD 8/2002; Kaijser/Markwitz, DuD 6/2008).

Seit einigen Jahren zeichnet sich nun eine dritte Linie ab: Die Entwicklung leistungsfähiger Hardware mit sehr geringem Strombedarf (z. B. für RFID-Systeme), die die Nutzung starker kryptografischer Verfahren erlaubt, begleitet von Fortschritten beim Reverse-Engineering, beschleunigte die Aufdeckung proprietärer – wie sich zeigte: überwiegend schwacher – kryptografischer Verfahren und deren Ersetzung in zahlreichen „eingebetteten Systemen" – wie Mobilfunksystemen (Weis/Lucks, DuD 9/1998; Zenner/Weis/Lucks, DuD 7/2000), kontaktlosen Zugangskarten (Fox, DuD 5/2008) oder „Funkschlüsseln" für Kraftfahrzeuge und Garagentore (Eisenbarth/Kasper/Paar, DuD 8/2008).

Mit der Quantenkryptografie wird ein Nachfolger für RSA am Horizont sichtbar, wie Stefan Rass und Peter Schartner in ihrem Beitrag zeigen. Dafür „fallen" weitere proprietäre Algorithmen, so dass auch der DECT-Standard inzwischen als unsicher gelten muss (siehe den Beitrag von Karsten Nohl und Erik Tews in diesem Heft). Noch reicht die Leistungsfähigkeit vieler neuer Anwendungsumgebungen, in die die Kryptografie erfreulicherweise inzwischen Einzug hält, nicht, um überall aktuelle Verfahren der modernen Kryptografie nutzen zu können. Daher wird uns die Suche nach speicher-, rechen- und energieeffizienten, aber dennoch sicheren kryptografischen Verfahren weiter beschäftigen (siehe den Beitrag von Axel Poschmann in diesem Heft).

Am Ziel dürfen wir uns wohl erst wähnen, wenn die Nutzung gut untersuchter, starker Kryptoverfahren und –protokolle auch in der ungewöhnlichsten Anwendung der nach Prognosen bald allgegenwärtigen Prozessoren („Ubiquitous Computing") eine Selbstverständlichkeit geworden ist. Bis dahin ist es – trotz aller Fortschritte – aber noch ein längerer Weg. Und selbst an diesem Ziel angelangt werden sich Kryptologen nicht ausruhen dürfen – denn an jedem Kryptoverfahren nagt der Zahn der Zeit, mindestens solange das Mooresche Gesetz gültig bleibt.

Dirk Fox