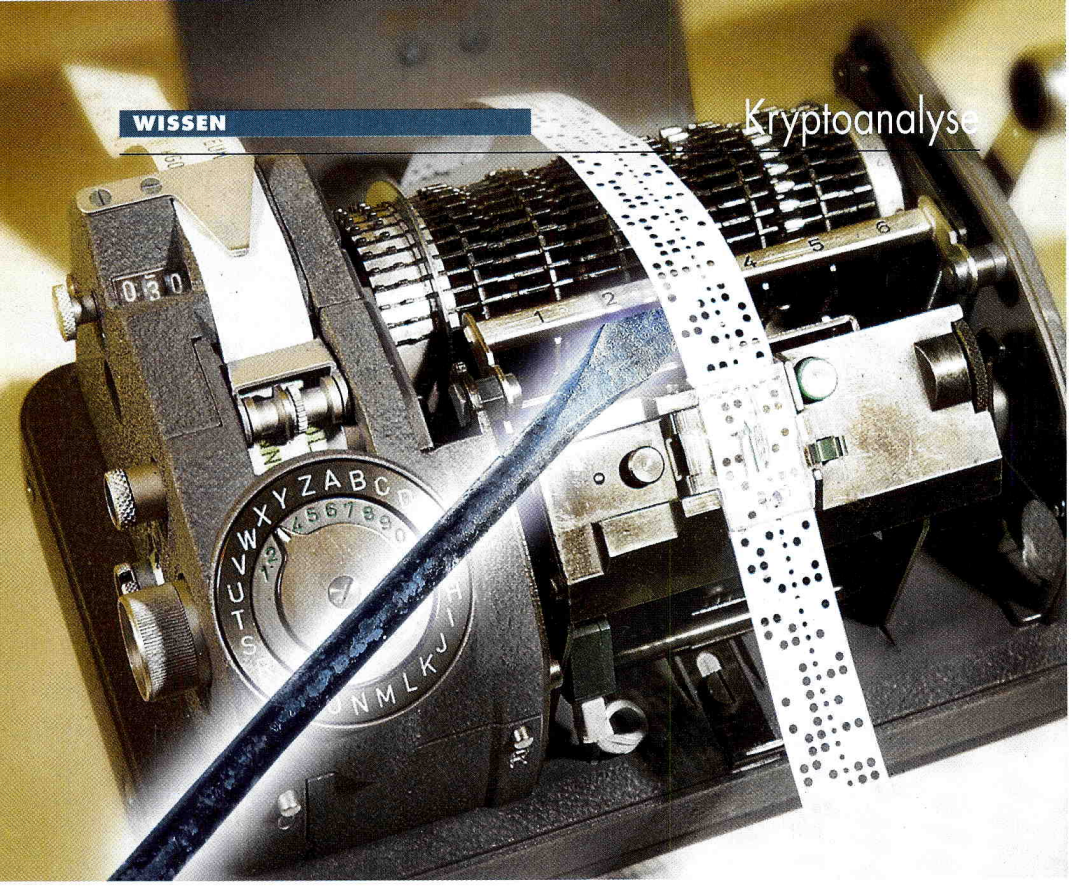


Wie sicher ist Kryptografie?

Knackige Maschinen

Christine Priplata, Colin Stahlke

Ob am Geldautomaten, im Auto, beim E-Mail-Versenden oder Onlinebestellen, im WM-Ticket, Handy oder PDA – überall gibt es kryptografische Sicherheitsmechanismen. Kryptoanalyse ist die Kunst, solche Systeme zu brechen. Zur realistischen Beurteilung von Produkten und anstehenden Entwicklungen im Bereich IT-Sicherheit ist ein regelmäßiger Blick hinter die Kulissen unerlässlich.

Wie Künstler kennen Codeknacker keine Grenzen und halten sich nicht an Regeln. Sie greifen kryptografisch gesicherte Daten auf allen Ebenen und mit allen Mitteln an. Das Finden der schwächsten Stelle genügt. Erfolgreiche Kryptoanalyse beruht auf cleveren Ideen, Neugier, mathematischen Fortschritten, immenser Rechenleistung, Hartnäckigkeit, Intuition für die übersehene Kleinigkeit – und oft genug auf Glück oder „einfach fragen".

Kryptografische Mechanismen eignen sich zum Schutz vertraulicher Daten gegen unbefugtes Mitlesen oder Verändern. Der Angreifer möchte den Klartext oder geheimgehaltene Schlüssel herausfinden, eine falsche Identität vorspiegeln oder die Aussagekraft von Prüfsummen aushebeln. Schon das Verschlüsseln und Signieren einer E-Mail schöpft kryptografisch aus dem Vollen: Die Nachricht ist symmetrisch verschlüsselt, die zugehörigen Schlüssel sind wiederum asymmetrisch verschlüsselt. Signiert wird auch asymmetrisch, jedoch nicht die Nachricht, sondern eine kryptografische Prüfsumme, erzeugt durch Hash-Funktionen. Das lässt erahnen, was bei aufwendigen Protokollen (von IPSec bis zu elektronischem Geld) oder beim Design komplexer Anwendungen alles zusammenzuschmieden ist, ohne am Ende mit einem Kartenhaus dazustehen.

Schlüssel im Visier

Im Zentrum der Sicherheit steht also das Geheimhalten der Schlüssel beziehungsweise bei Hashes das Verhindern identischer Prüfsummen für unterschiedliche Texte. Damit steht das Ziel des Angreifers fest. Austoben kann er sich auf vier Spielwiesen: Bei den Algorithmen selbst, bei ihrer Implementierung, bei physikalischen Effekten und schließlich beim Anwender.

Direkte Angriffe auf Algorithmen nutzen grundsätzliche Schwächen in der Struktur oder im Design der Verfahren, mathematische Einsichten, die bestimmte Berechnungen unerwartet beschleunigen, statistische Analysen, das Spielen mit Paaren aus Klar- und Ciphertexten und das Finden von Mustern. Ein symmetrisches Verfahren gilt als gut, wenn der beste Angriff im Wesentlichen das Durchprobieren aller Schlüssel ist (Brute Force). Schlechte Verfahren findet man unter anderem beim WEP-Verfahren alter WLAN-Geräte und bei GSM-Handys. Die Sicherheit der bekannten asymmetrischen Verfahren beruht auf mathematischen Aufgaben, deren Lösung bei ausreichender Schlüssellänge als praktisch unmöglich gilt, etwa die Zerlegung großer Zahlen in ihre Primfaktoren. Die Analyse umfasst die gesamte Kette von der Theorie und dem Entwurf der zum Knacken eingesetzten Algorithmen über deren Parallelisierung und Implementierung in Software bis zum optimierten Design von Spezialhardware.

Meist gründlich unterschätzt und daher erfolgreich sind Angriffe auf die Implementierung von Kryptoalgorithmen und auf das Design komplexerer Anwendungen. Nicht selten verwenden Entwickler ungeeignete Parameter oder Spezialfälle, optimieren mit undurchdachten Vereinfachungen oder hantieren sorglos mit schwachen Zufallszahlen, ganz zu schweigen von Fehlern bei der Realisierung des Schlüsselmanagements oder beim Zusammensetzen von Algorithmen. Vielleicht ist der Schlüssel der geschützten Da-

ten nicht einmal geheim. Zu hinterfragen ist in jedem Fall, ob Kryptografie oder andere Schutzmechanismen das Gewünschte überhaupt schützen können beziehungsweise ob die geplante Realisierung in erwarteter Weise wirkt. Zur Implementierung im weiteren Sinne gehören auch Anforderungen an die Umgebung. Werden diese nicht erfüllt oder ausgehebelt, ist die ganze Kryptografie nutzlos.

Eine dritte Fundgrube ist die Physik oder die Welt der so genannten Seitenkanalattacken [1]. Bei Smartcards, Tokens oder RFIDs kann der Angreifer leicht das ganze System unter die Lupe nehmen. Er misst zum Beispiel den Stromverbrauch, Ausführungszeiten, die elektromagnetische Abstrahlung, Reaktionen auf falsche Signale oder Strahlung. Durch geschickte Analyse der Daten kann er oft den ganzen Schlüssel auslesen, etwa weil die Implementierung gar zu laut verrät, wann und wie oft sie multipliziert. Andererseits gibt es eine breite Palette ausgeklügelter Gegenmaßnahmen, um diese Informationen zu verschleiern – die übliche Endlosschleife von Angriff und Verteidigung.

Der berühmt-berüchtigte schwächste Punkt ist oft der Mensch. In vielen Fällen ist dem Nutzer gar nicht bewusst, dass er eine sensible Kryptoanwendung benutzt und schon gar nicht, was er dabei alles falsch machen kann. Andernfalls kostet Regeleinhalten viel Zeit, und Termindruck zwingt zur „Kreativität". Dem Angreifer hilft oft einfaches Fragen, und mit viel Geduld kann er per Social Engineering menschliche und organisatorische Schwächen ausnutzen [2].

Unter der Lupe

Ziel der Analysen zum Brechen von Algorithmen ist es, realistische Einschätzungen für die praktische Sicherheit der Mechanismen beziehungsweise für notwendige Schlüssellängen zu erhalten. Das Konvergenzverhalten bei wachsender Schlüssellänge und ein paar PC-Experimente alleine liefern eine unzureichende Vorstellung von den tatsächlichen Kosten. Bessere Daten bekommt man, wenn man die zum Teil komplexen kryptoanalytischen Algorithmen im Detail optimiert, geeignet parallelisiert und schließlich an den richtigen Stellen geschickt in Spezialhardware auslagert. Erfreulicherweise hat die Forschung dieses Thema in den letzten Jahren aktiv bearbeitet, sodass im Netz aktuelle und fundierte Informationen zu finden sind, zum Beispiel auf den Seiten der einschlägigen Sharcs-Konferenz über in Hardware implementierte Cracker [3]. Mehr zu aktuellen Krypto-Entwicklungen findet man unter den Links und Dokumenten des europäischen Krypto-Netzwerks Ecrypt [4] oder auf den Seiten der internationalen Krypto-Forscher-Szene (www.iacr.org).

Neben einem Brute-Force-Angriff sind insbesondere die lineare und die differenzielle Kryptoanalyse ernstzunehmende Attacken auf symmetrische Algorithmen. Ein gutes symmetrisches Verfahren sollte gegen diese beiden etablierten Klassen von Angriffen resistent sein. Die verbreiteten Blockchiffren AES und Triple-DES (in der Praxis mit 168 Bit empfohlen) gelten als vergleichsweise sicher, wie auch viele andere symmetrische Verfahren. Der veraltete DES war bei seiner Einführung circa 1977 ein Algorithmus mit gutem Design, hatte aber mit 56 Bit eine viel zu kleine Schlüssellänge. Ein Angriff auf seinen Nachfolger AES wäre heute ähnlich aufwendig wie Brute Force. Auch neuere Ideen, wie gewisse algebraische Angriffe, sind für AES bisher derart aufwendig, dass zumindest AES mit 256 Bit für längere Zeit sicher zu sein scheint. Symmetrische Algorithmen mit gutem Design sollten mittels Brute Force selbst für die größten Organisationen jenseits von 90 Bit nicht mehr zu knacken sein.

DES in 3 Tagen geknackt

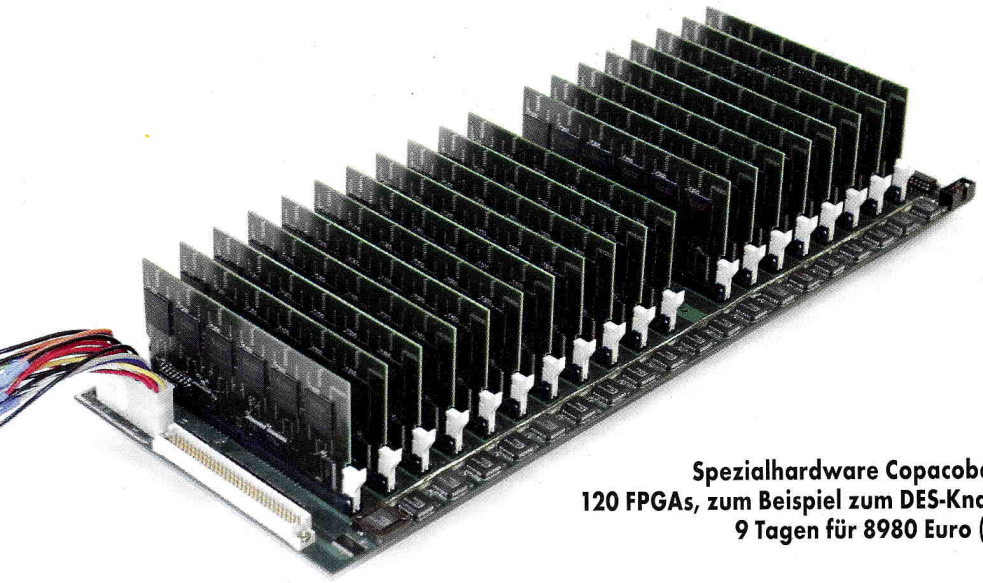
Brute-Force-Angriffe auf DES gibt es schon lange. Bereits bei seiner Einführung schlugen W. Diffie und M. Hellmann 1977 eine 20-Millionen-Dollar-Maschine vor, die DES in 12 Stunden knacken könnte. Sie vermuteten, DES werde 1990 vollkommen unsicher. 1993 präsentierte M. Wiener ein Design für einen Rechner, der DES für eine Million US-Dollar in 3,5 Stunden brechen könnte. 1998 baute die Electronic Frontier Foundation den ersten öffentlichen DES-Cracker für unter 200 000 US-Dollar und knackte eine von den RSA Laboratories ausgeschriebene DES-Aufgabe in weniger als drei Tagen. Das übertraf den kurz zuvor durch ein Netzwerk von über 10 000 PCs zur Lösung desselben Problems in 39 Tagen erzielten Erfolg.

Trotz dieser Ergebnisse ging die Forschung für diese Art der Schlüsselsuche weiter, zum Beispiel unter Verwendung rekonfigurierbarer Hardware (FPGAs). Sie liefert wertvolle Einsichten in das Design und die Möglichkeiten von Maschinen, die sich für unterschiedliche kryptoanalytische Aufgaben einsetzen lassen, zum Beispiel für Unix-Passwortsuche, das Finden von Kollisionen in Hash-Funktionen, zur Kryptoanalyse von Stromchiffren, zur Unterstützung des Siebschritts beim RSA-Knacken oder für das Pollard-Rho-Verfahren zur Kryptoanalyse von Eliptic Curve Cryptography (ECC) – alles bestens parallelisierbare Verfahren. Zudem können solche Maschinen auch verschiedene schwache Algorithmen einfach knacken. Innerhalb von Ecrypt stellte die Universität Bochum zur Sharcs 2006 mit Copacobana eine solche FPGA-Maschine zum Knacken von DES in circa neun Tagen für 8980 Euro vor (www.copacobana.org, siehe Abb. 1). Es handelt sich um eine parallele Architektur aus 120 preiswerten FPGAs. Um dasselbe zu erreichen, müsste man über 20 000 Pentium4-Prozessoren à circa 160 Euro bemühen. Copacobana hilft auch beim Auslesen von Daten aus dem ePass (events.iaik.tugraz/RFIDSec06).

Schon lange spukt in den Köpfen der Kryptoanalytiker die Idee, statt solcher Architekturen, die viel Entwicklungszeit verschlingen, Spielekonsolen zu verwenden. So stellte E. Tromer vom Weizmann-Institut einige mit dem Simulator für die Playstation 3 erzielte Ergebnisse vor und kam zu dem Schluss: Man kann die Entwicklungszeit sparen, nimmt 52 solche Playstations (jede ein Linux-Computer mit einem Cell-Prozessor, bestehend aus einem PowerPC-Core und 8 weiteren Cores) für je 700 US-Dollar und bezahlt für das Knacken von DES in neun Tagen

iX-TRACT

- Kryptoanalyse bedient sich bei den Algorithmen, Mängeln in den Implementierungen, aus den Seitenkanälen und nicht zuletzt beim Nutzer von Anwendungen.
- Neben der theoretischen Analyse der Algorithmen ergeben sich aus Kostenabschätzungen für Spezialhardware realistische Bewertungen zu Schlüssellängen.
- Eine aktuelle Herausforderung im Bereich Kryptografie ist das Design neuer, guter Hash-Funktionen.



Spezialhardware Copacobana aus 120 FPGAs, zum Beispiel zum DES-Knacken in 9 Tagen für 8980 Euro (Abb. 1)

rund 30 000 Euro. Alternativ kann man das Ganze auf einer LAN-Party mit circa 6000 PCs in einer Stunde erledigen. Zweifellos brechen hier gute Zeiten für die Kryptoanalyse an, da Multi-Core-Prozessoren in allgemein verfügbarer Hardware in Zukunft üblich sein dürften.

Gut gehasht?

Hash-Funktionen erzeugen Prüfsummen (Hashes), indem sie größere Datenmengen auf wenige Bytes abbilden. So erzeugt *md5sum* unter Linux 128 Bit lange MD5-Hash-Werte von Dateien. Findet man zwei Dateien mit gleichem Hash, spricht man von einer Kollision. Für eine kryptografisch gute Hash-Funktion muss das Finden einer Kollision praktisch unmöglich sein. Hashes kommen unter anderem für digitale Signaturen zum Einsatz, die sich nur auf den Hash-Wert eines Dokuments beziehen. Findet jemand eine Kollision der Hash-Funktion, kann er eventuell ein anderes Dokument mit demselbem Hash vorzeigen, obwohl dieser Wert als „Beweis" für die Vertragsunterzeichnung galt. Früher galt MD5 als kryptografisch gut. Mitte der 90er-Jahre knackte H. Dobbertin zunächst MD4 und zeigte erhebliche Schwächen von RIPE-MD und MD5 auf. Inzwischen findet man zum Beispiel unter [5] zwei verschiedene Verträge im Postscript-Format mit demselbem MD5-Hash.

Heutzutage fungiert als Hash-Funktion meist SHA-1 mit 160 Bit. Für jede Hash-Funktion gibt es Angriffe mit einer Komplexität, die der halben Bitlänge entspricht. Man müsste also 2^{80} Dateien untersuchen, um zwei mit demselben Hash-Wert zu finden. Nach dieser Rechnung sollte man ein übliches symmetrisches Verfahren wie 128-Bit-AES besser mit 256-Bit-Hashes kombinieren. Einerseits sind 2^{80} Dateien eine riesige Menge, andererseits gibt es große Fortschritte bei den Angriffen auf SHA-1. So gelang es chinesischen Wissenschaftlern 2005, die Komplexität auf 2^{66} zu drücken. Wahrscheinlich dauert es nicht mehr lange, bis jemand eine Kollision findet, sodass die Industrie allmählich zu SHA-256 wechseln wird. Allerdings ähnelt sich das Design aller bisher vorgeschlagenen Hash-Funktionen, weshalb das Finden grundsätzlich neuer guter Hash-Funktionen eine echte Herausforderung darstellt – zudem sollen die Auserwählten schnell laufen und Platz sparen.

NSA setzt auf ECC

Aufgrund der mathematischen Struktur gibt es bei asymmetrischen Verfahren bessere Angriffe als Brute Force (daher die längeren Schlüssel). Trotzdem sollen sie zum Beispiel in Chipkarten oder RFIDs mit wenigen Ressourcen zum Einsatz kommen und können so das schwächste Glied in der Algorithmenkette sein. Zurzeit ist RSA mit 1024 Bit am weitesten verbreitet, obwohl dies eher der Sicherheit von 80 Bit eines symmetrischen Verfahrens entspricht. Nicht selten wird es unausgewogen mit 256 Bit AES kombiniert. Zum Knacken von 1024-Bit-RSA genügt das Faktorisieren einer 1024 Bit langen Zahl. Da der Aufwand bei ECC exponentiell mit der Schlüssellänge wächst, kommt man mit kürzeren Schlüsseln als bei RSA aus. Die US-amerikanische National Security Agency hat die RSA-Ära inzwischen hinter sich gelassen und fordert für staatliche Anwendungen ECC mit mindestens 512 Bit. Mit heutigen und absehbaren Bordmitteln liegt deren Knacken außerhalb jeder Reichweite. Auch dem Bau hinreichend großer Quantencomputer (bis jetzt kann man die Zahl 15 faktorisieren) stehen bisher scheinbar unüberwindbare Hürden im Weg, doch sicherheitshalber beschäftigen sich Forscher bereits fleißig mit der Post-Quantum-Welt (post quantum.cr.yp.to). Schließlich wurden Kryptoanalytiker immer unterschätzt: In beiden Weltkriegen knackten sie erfolgreich die Codes der jeweiligen Gegner.

Der beste Algorithmus zum Faktorisieren heißt Zahlkörpersieb. Teuer sind darin der Siebschritt (Sammeln von Relationen) und der Matrixschritt (Lösen eines riesigen linearen Gleichungssystems). Innerhalb dieser Schritte gibt es zahlreiche Parameter und Routinen zum Optimieren. Da nach wie vor viele Anwendungen mit geringen Schlüssellängen arbeiten, gilt dem Abschätzen der Kosten für optimale Maschinen für verschiedene Bitlängen besonderes Interesse. Bemerkenswert sind die letzten Fortschritte beim Faktorisieren in Software (PCs, Linux-Cluster und gute Workstations) – von 512 Bit durch ein Team rund um das CWI in Amsterdam (1999) bis zu den Ergebnissen des Teams um J. Franke und T. Kleinjung von der Universität Bonn aus den Jahren 2003 (576 Bit) und 2005 (663 Bit, [6]).

Im gleichen Zeitraum gab es eine Reihe von Vorschlägen für Spezialhardware, insbesondere für den Siebschritt, mit klingenden Namen wie Twinkle, Twirl, Yasd und Shark [3,7]. Während Twinkle für ein optisches Gerät steht, setzen die anderen Designs auf entwicklungsintensive ASICs (optimierte Chips für spezielle Aufgaben), so Twirl auf riesige ASICs von der Größe eines ganzen Wafers für geschätzte 1,1 Millionen US-Dollar oder Shark auf eine modulare Architektur aus vielen kleinen ASICs für konservative 200 Millionen US-Dollar. Zum Beschleunigen des Siebschritts dienen Implementierungen von ECM (Elliptic Curve Method) in ASICs beziehungsweise zur Vorab-Analyse in FPGAs. Der aktuelle Rekord zum Brechen von ECC in Software liegt bei 109 Bit (2002, [8]), auf der Sharcs 2006 wurden auch ein erstes Design

und Abschätzungen für Pollard-Rho-Spezialhardware vorgestellt.

In Zukunft nur noch heiße Chips?

Die Sicherheit guter Kryptoalgorithmen ist also eine Frage der Wirtschaftlichkeit von Maschinen, die sie brechen. Zu Recht erwarten Nutzer langfristige Sicherheit, damit auch in 10 Jahren niemand die Wegfahrsperre des Autos überwinden oder eine digitale Unterschrift fälschen kann. Deshalb sind Aussagen über die Zukunft der Computertechnik wichtig. Seit 40 Jahren gilt Moore's Law: Verdopplung der Rechenleistung alle 18 Monate. Das diesem rasanten Forschritt häufig prophezeite nahe Ende ist bislang nicht eingetreten. Aber vielleicht ist es nun doch in Sicht, wie Y. Leblebici (EPFL Lausanne) auf der Sharcs 2006 ausführte („How much faster can we go? A technolgy outlook" [3]).

Mit der Transistordichte auf den Chips fällt der so genannte Yield, die Ausbeute fehlerloser Chips aus der Herstellung, dramatisch – zum Beispiel vom 386er bis zum Pentium I von 71 % auf nur 9 %. Die heute vermutlich noch kleinere Ausbeute stellt die Wirtschaftlichkeit von Crack-Maschinen mit großen Chips in Frage. 2015 sollen auf einem Chip 15-mal mehr Transistoren sitzen als 2004 und die Taktfrequenz auf 40 GHz steigen. Dabei genügen hohe Taktfrequenzen für lokale Bereiche des Chips, und der Trend geht zu Multi-Core-Prozessoren, das heißt zu mehreren Prozessoren auf einem Chip. Der Cell-Prozessor mit neun Cores in der Playstation 3 hat eine Rechenleistung von bis zu 256 Gigaflops. Demgegenüber erreicht der schnellste Supercomputer, IBMs Blue Gene, 70 Teraflops. Zwar lässt sich mit 300 Playstations nicht die Leistung des Blue Gene erreichen, weil die dafür nötige schnelle Kommunikation zwischen den einzelnen Playstations nicht realisierbar ist. Jedoch könnten sie sich für lokalere Probleme, wie Brute-Force-Angriffe auf symmetrische Algorithmen, genauso gut eignen. Die Speicherkapazität von DRAMs soll um den Faktor 35 steigen. Speicher wird also zunächst keine Hürde darstellen.

Bemerkenswert ist jedoch, dass die geplante Leistungsaufnahme von 550-Quadratmillimeter-Chips über Jahre konstant bei maximal 200 Watt bleiben soll. Dies ist nicht etwa das Resultat besonders pfiffiger Stromspar-Techniken. Es weiß einfach niemand, wie man eine noch größere Hitzeentwicklung von dieser Fläche schnell genug abführen könnte. Hier zeigt sich die erste Grenze der Chip-Entwicklung. Bei ihrer Einführung beseitigte die CMOS-Technik den Nachteil der großen Leistungsaufnahme. Nun stößt sie selbst an eine Grenze. Wenn Moore's Law Bestand haben soll, muss dieser Technik etwas grundlegend Neues folgen. Es gibt zahlreiche Ideen, jedoch ist noch kein erfolgversprechender Nachfolger in Sicht. Gegen Moore sprechen in Zukunft auch prinzipielle physikalische Grenzen: Hat man vielleicht im Jahr 2020 die 4nm-MOSFET-Technik entwickelt, ist die Siliziumschicht eines Transistors nur noch 10 Atome dick. Die Fremdatome zum Dotieren sind darin zwangsweise unregelmäßig verteilt, sodass theoretisch gleiche Transistoren in der Praxis ein stark unterschiedliches Verhalten zeigen werden.

Die Technik setzt Grenzen, aber Spielräume für gute Ideen zum Design neuer Algorithmen und besserer Maschinen gibt es viele. Spannend bleibt, wie es weitergeht beim Absichern und beim Angreifen. (ck)

DR. CHRISTINE PRIPLATA UND DR. COLIN STAHLKE

sind promovierte Mathematiker, beschäftigen sich seit vielen Jahren mit Kryptografie und gehören zur Geschäftsleitung der Bonner EDIZONE GmbH mit Schwerpunkt Krypto-Anwendungen und IT-Sicherheit.

Literatur

[1] ECRYPT Side Channel Cryptanalysis Lounge, www.crypto.ruhr-uni-bochum.de/en_sclounge.html

[2] K. Mitnick und W. Simon, Die Kunst der Täuschung (Risikofaktor Mensch), mitp-Verlag, 2003

[3] SHARCS: Workshop on Special-Purpose Hardware for Attacking Cryptographic Systems, www.sharcs.org

[4] ECRYPT: European Network of Excellence in Cryptology, www.ecrypt.eu.org

[5] Links zu MD5-Kollisionen: www.cits.rub.de/MD5Collisions, www.mscs.dal.ca/~selinger/md5collision/

[6] Link zur Faktorisierung von 663 Bit RSA: www.crypto-world.com/announcements/rsa200.txt

[7] Website on Special-Purpose Cryptanalytic Devices, Stand 2005: www.wisdom.weizmann.ac.il/~tromer/cryptodev

[8] Links zum Knacken von ECC mit 109 Bit: ECC Challenges unter www.certicom.com/index.php?action=ecc,ecc_challenge