Besprechungen zu Büchern der Computeralgebra

Erschienen im Computeralgebra Rundbrief 25, Oktober 1999.

- **N. Koblitz, Algebraic Aspects of Cryptography**

  Band 3 der Reihe *Algorithms and Computations in Mathematics*, Springer-Verlag Berlin, Heidelberg, New York 1998, ISBN 3-540-63446-0, pp. 206, DM 98.

  Der Autor, der durch seine Bücher "Introduction to Elliptic Curves and Modular Forms" (GTM 97, Springer 1984) und "A Course in Number Theory and Cryptography" (GTM 114, Springer 1987) vielen Lesern dieses Rundbriefs gut bekannt sein wird, hat hier ein kleines Werk vorgelegt, das man wohl am Besten als "Lesebuch zu algebraischen Aspekten der Kryptographie mit öffentlichem Schlüssel" charakterisieren kann.

  Bis Mitte der 70er Jahre (der Autor setzt den Schnitt im Jahr 1976) spielten derartige Verfahren in der Kryptographie im Vergleich zu symmetrischen Verfahren bekanntlich eine untergeordnete Rolle. Dies änderte sich erst unter dem Druck verschiedener Computeranwendungsmöglichkeiten. Die generelle Aufgabenstellung für den Entwurf eines Kryptosystems mit öffentlichem Schlüssel kann man wie folgt formulieren: Es ist eine (injektive) Funktion $f : X \longrightarrow Y$ von der Menge der Quelltexteinheiten X in die Menge Y der verschlüsselten Nachrichteneinheiten zu entwerfen, die für alle $x \in X$ einfach zu berechnen ist, für die aber $f^{-1}(y)$ für die meisten $y \in im(f)$ ohne zusätzliche, öffentlich nicht zugängliche Information nicht mit zumutbarem Aufwand zu ermitteln ist. Allerdings soll es eine geheime Zusatzinformation, den privaten Schlüssel, geben, mit dessen Hilfe auch die Umkehraufgabe, das Dechiffrieren, einfach wird.

  Viele schwierige mathematische Probleme gaben bisher Anlass für sichere oder vermeintlich sichere Verschlüsselungsverfahren. Die von einer Kryptanalyse zu beantwortenden Fragen sind dabei vor allem komplexitätstheoretischer Natur. Allerdings fortgeschrittener Art, denn die Existenz eines privaten Schlüssels legt die Frage nahe, ob man nicht durch geschickte Kombination öffentlich erzeugbarer Zusatzinformationen diesen Schlüssel doch irgendwie berechnen kann. Die "Code-Knacker" setzen gerade hier an.

  Da sich damit in der Kryptanalyse die gesamte Mathematik wie in einem Brennglas sammelt, wird man in einem Büchlein wie dem des Autors immer nur einen kleinen Ausschnitt dieses großen Gebiets einfangen können. Der Autor hat hierfür drei Themenkreise (Monomsysteme, polynomiale Gleichungssysteme und Verallgemeinerungen des Diffie-Hellman-Verfahrens auf elliptische und hyperelliptische Kurven) mit algebraischem Hintergrund gewählt, die bisher nicht in monographischer Form vorlagen.

  Das Buch kann man grob in zwei (auch umfangmäßig etwa gleich große) Teile teilen. Im ersten Teil (Kap. 1 – 3) werden wichtige Begriffe und Zusammenhänge der im Weiteren benötigten mathematischen und kryptographischen Grundlagen erläutert und teilweise bewiesen. Der Umfang dieses Teils ist vor allem einer recht detaillierten Darlegung algorithmischer Aspekte geschuldet. Diese fände man zwar auch anderswo, jedoch gewinnt das Buch damit selbst für fortgeschrittene Studenten eine gewisse Abgeschlossenheit. Ein Teil des Materials wurde (für den fleißigen Leser) in eine Fülle von Übungsaufgaben ausgelagert, zu denen im Anhang Lösungen bzw. Lösungshinweise enthalten sind.

  Der erste Teil umfasst im Einzelnen eine Tour durch kryptographische Fragen (Aufgabenstellung und Geschichte; das RSA-Kryptosystem; der Ansatz von Diffie-Hellman zur Verwendung von Logarithmus-Abbildungen; Anwendungen auf digitale Signaturen, Passwörter, Auswertung verdeckter Information), die Diskussion relevanter Komplexitätsklassen (polynomial vs. exponentiell; P, NP und NP-hart; Berechnungsaufgaben mit Zusatzinformationen; probabilistische Verfahren) an Beispielen aus Kombinatorik und Zahlentheorie sowie Fragen aus der Theorie endlicher

Körper (Existenz- und Eindeutigkeitssatz; konstruktive Aspekte) und der Polynomringe (bis hin zu Hilberts Nullstellensatz, S-Polynomen und Gröbnerbasen).

Im zweiten Teil wird der Leser, begleitet von Alice, Bob und Catherine, durch die bereits oben genannten drei Themenkreise geführt. Der Autor legt großen Wert auf eine ausführliche und verständliche Darlegung des jeweils betrachteten kryptographischen Verfahrens, das in den zugehörigen Übungsaufgaben weiter vertieft werden kann. Die Kryptanalyse erfolgt in der Regel von einer einfach zu brechenden Variante aus, die sich verstärken, aber mit mehr Einsatz von Mathematik auch wieder brechen lässt. Der dabei gezeichnete Weg führt von einer guten Straße über unebenes Gelände bis hin zum Dickicht moderner Forschungen und (noch) ungelöster Fragen.

Kap. 4 befasst sich mit dem Imai-Matsumoto-System. Die Idee des Systems besteht darin, die Abbildung $u \mapsto u^h$ zum Verschlüsseln zu verwenden, wobei u aus einer endlichen Erweiterung von $\mathbf{F}_q$ stammt. Zusätzlich werden affine Transformationen vor- und nachgeschaltet, um "die Spuren zu verwischen". Für geeignete Exponenten h (Summen von wenigen q-Potenzen) lässt sich daraus ein polynomiales Kodierungssystem herleiten. Die Kryptanalyse zeigt, dass in einigen Fällen aus diesen Gleichungen die Existenz bilinearer Gleichungen folgt, die man zum Kodebrechen mit linearar Algebra verwenden kann.

Kap. 5 befasst sich mit dem "Polly Cracker". Hierbei ist $X = F$ ein Körper und $Y = F[T_1, \ldots, T_n]$ ein Polynomring. Eine Nachricht $x \in X$ wird durch ein zufälliges Polynom $p \in I(B)$ bzgl. eines (öffentlich bekannten) Polynomsystems $B \subset Y$ zu $c = x + p$ verfälscht. Die Dechiffrierung erfolgt mit Kenntnis einer (geheimen) Nullstelle $y \in F^n$ von B. Die Kryptanalyse muss also feststellen, wie schwierig es ist, eine solche Nullstelle allein aus den Gleichungen B zu bestimmen. Hierzu werden Gleichungssysteme betrachtet, die sich aus verschiedenen NP-harten kombinatorischen Problemen ableiten lassen, womit das Erstellen eines solchen Systems in **P**, sein Knacken aber (wahrscheinlich) in **NP** liegt. Abschließend wird eine Verallgemeinerung des Polly Crackers betrachtet, wo X eine Teilmenge der Standardmonome bzgl. $I(B)$ ist. Der Autor folgt den Argumenten von T. Mora (1993), der vermutet, dass es mit Blick auf intelligente Attacken mit linearer Algebra einen solchen "Krypto-Gröbner" nicht geben kann.

Kap. 6 ist schließlich Kryptosystemen auf der Basis elliptischer und hyperelliptischer Kurven gewidmet. Diese basieren auf der Idee von Diffie-Hellman, die auf die additive Gruppe der Kurve (im elliptischen Fall) bzw. deren Jacobischer (im hyperelliptischen Fall) angewendet wird. Damit vergrößert sich der Fundus von Gruppen, wo man die Anwendung der genannten Idee studiert hat, beträchtlich. Die Ausführungen beginnen mit einer Zusammenstellung der wichtigsten Fakten aus der Theorie elliptischer Kurven, die im weiteren benötigt werden. Es schließt sich eine ausführliche Erörterung verschiedener Aspekte von Kryptosystemen an, die elliptische Kurven verwenden (subexponentielles Verhalten des Originalverfahrens von Diffie und Hellman für $G = \mathbf{F}_q^*$; Diskreter Logarithmus und "schlechte" Gruppenordnungen; ECDSA-Verfahren zur digitalen Signatur; Auswahl "guter" Kurven und Probleme der klassischen Zahlentheorie). Im abschließenden Teil werden die Fragen auf hyperelliptische Kurven übertragen. Wichtigstes neues Problem ist dabei die effiziente Ausführung der Addition auf der Jacobischen, das in einem Anhang ("An Elementary Introduction to Hyperelliptic Curves" von A.J. Menezes, Yi-Hong Wu und R.J. Zuccherato) abgehandelt wird.

Mit zunehmender Schwierigkeit des Materials werden die Ausführungen dabei skizzenhafter und beschränken sich immer stärker auf den Hinweis auf entsprechende Quellen, was den Charakter eines guten "Lesebuchs", wie ich es oben bezeichnet habe, ausmachen sollte. Das Buch eignet sich damit selbst für "advanced undergraduates", wie es im Klappentext heißt, als Einstieg und erster Überblick über ein Gebiet, in dem sich in den letzten Jahren auf überraschende Weise praktische Anwendungsmöglichkeiten für tief innermathematische Themen ergeben haben.

Hans-Gert Gräbe (Leipzig)