Katharina KLEMBALSKI, Berlin

Sogar mathematisch bewiesen? Formen mathematischen Schließens

Einleitung

Anlass für die hier vorgestellten Überlegungen ist die Beobachtung des unterschiedlichen Gebrauchs der Begriffe *sicher* bzw. *Sicherheit* in der Kryptografie. So ist die Einwegeigenschaft von in der Kryptografie eingesetzten Funktionen nicht bewiesen, die entsprechenden Verfahren sind mathematisch also nicht sicher. Dennoch werden Verfahren wie RSA täglich millionenfach eingesetzt und von Experten als sicher eingeschätzt. Das dient als Motivation, die jeweils zugrunde liegenden Schlussweisen zu charakterisieren und voneinander abzugrenzen.

Zwei Formen mathematischen Schließens - drei Beispiele

Orientiert an Pólya (1988/1975) und Blechman et al. (1984) wird im Folgenden zwischen deduktivem und plausiblem Schließen unterschieden. Um diese Formen mathematischen Schließens zu charakterisieren, werden zunächst zwei Beispiele betrachtet und in einem dritten die Frage der Sicherheit von RSA wieder aufgegriffen. Die betrachteten Charakteristika gehen zurück auf Pólya (1975, S. 172f).

Beispiel 1. Wenn p eine Primzahl und $(a, p) = 1$ ist, so ist $a^{p-1} \equiv 1 \bmod p$ (Kleiner Fermat). Daraus folgt für $p = 147$ wegen $2^{147-1} \bmod 147 = 25$ sofort, dass 147 keine Primzahl ist.

Die einzelnen Schritte der Argumentation in Beispiel l lassen sich entsprechend den Regeln der formalen Logik nachprüfen und gelten unabhängig von der Person, die diese Prüfung durchführt. Um den Schluss zu bestätigen, wird neben den Regeln der Logik nichts über die Voraussetzungen Hinausgehendes benutzt. Da die Voraussetzungen dauerhaft sind, gilt das ebenso für den Schluss. Hier wurde *deduktiv* geschlossen, d.h. insbesondere *unpersönlich*, *in sich vollständig* und *dauerhaft* (Pólya 1975, S. 172).

Beispiel 2. Die Berechnung des Produkts $123 \cdot 11 = 1353$ soll geprüft werden. Es wird die 9er-Probe angewandt, d.h. das Produkt der Quersummen der Faktoren $(6 \cdot 2)$ mit der Quersumme des Ergebnisses (12) verglichen. Aus der Übereinstimmung lässt sich schließen, dass die Rechnung *möglicherweise* richtig ist. Das Ergebnis 1353 erscheint *plausibel*.

Die zugrunde liegende Aussage $A \rightarrow B$ ist die folgende: Wenn $123 \cdot 11 = 1353$, dann gilt für die Quersummen:
$Q(123) \cdot Q(11) \equiv Q(1353) \pmod 9$. Im Beispiel wird aus der Beobachtung

B auf die Gültigkeit von *A* geschlossen, bzw. genauer die Annahme gestärkt, dass auch *A* gilt.

Die angewandten Schlussweisen in den Beispielen l und 2 lassen sich durch folgende Schemata darstellen (Pólya, 1975, S. 15):

$$\text{Deduktives Schließen: } \frac{\begin{array}{c}\text{Aus } A \text{ folgt } B\\ B \text{ falsch}\end{array}}{A \text{ falsch}} \qquad \text{Plausibles Schließen: } \frac{\begin{array}{c}\text{Aus } A \text{ folgt } B\\ B \text{ wahr}\end{array}}{A \text{ glaubwürdiger}}$$

Der Zugewinn an Glaubwürdigkeit von *A* durch die Gültigkeit von *B* ist abhängig vom Kontext – wie in Beispiel 2 – und davon von wem der Schluss durchgeführt wird. Plausibles Schließen ist daher nicht *unpersönlich*. Das folgende Beispiel wird zusätzlich auf die Merkmale in *sich vollständig zu sein* und *dauerhaft* untersucht. Das Beispiel ist zunächst von deduktiver Gestalt, unterscheidet sich von einem mathematischen Satz wie in Beispiel 1 jedoch in den Voraussetzungen, die plausibel gewonnen werden.

Beispiel 3. Wenn (i) die Faktorisierung schwer ist und
(ii) Angriffe ohne Faktorisierung ausgeschlossen sind,
dann ist RSA sicher.

Zu (i). Ob die Faktorisierung schwer ist (also nicht in Polynomialzeit durchzuführen), ist nicht bewiesen. Die Frage verweist jedoch auf ein übergeordnetes Problem der Komplexitätstheorie, nämlich ob $P \neq NP$ ist und ist dadurch auch Gegenstand mathematischer Forschung jenseits der Kryptografie. Dass trotz intensiver Forschung aus unterschiedlichen Richtungen keine Fortschritte über Nachweis der Existenz oder sogar die Angabe eines polynomialen Algorithmus erkennbar sind, stärkt die Annahme (vgl. Buchmann 2003, S. 148).

In der Praxis werden die Laufzeiten bekannter Faktorisierungsverfahren (langsam) gegen die zur Durchführung von RSA (schnell) abgewogen und daraus Empfehlungen für die Schlüssellänge (Stellenzahl des Moduls *n*) abgeleitet, die voraussichtlich Sicherheit gewährt. Die zugrunde liegenden Annahmen zur Rechenleistung werden immer wieder neu an die tatsächlichen Gegebenheiten angepasst und schließen erfahrungsbasierte Prognosen zur zukünftigen Entwicklung mit ein.

Zu (ii). Argumentativ wird zwischen Angriffen auf die Einwegfunktion, bei RSA dem Potenzieren modulo *n*, und Angriffen auf die Implementierung unterschieden. Im ersten Fall wäre es denkbar, eine Nachricht direkt, d.h. ohne Bestimmung des geheimen Schlüssels (äquivalent zum Faktorisierungsproblem), zu entschlüsseln (vgl. Buchmann, S. 141). Ein Algorithmus, der das (in Polynomialzeit) leistet, ist aber nicht bekannt. Angriffe,

die Details der Implementierung ausnutzen, beschreibt u.a. Buchmann (2003). Sie sind durch entsprechende Modifikation des Protokolls, in dem RSA verwendet wird, leicht zu vermeiden (ebd., S. 147). Aus diesem Grund sind übliche Aussagen zur Sicherheit eines kryptografischen Verfahrens immer konditionaler Natur und schließen das Protokoll ein, in dem es angewendet wird. Solche „Sicherheitsbeweise" besitzen oft folgende Form: „Unser Protokoll ist immun gegen einen Angriff der Art *X*, vorausgesetzt das mathematische Problem *Y* ist schwer berechenbar." (vgl. Koblitz 2007, S. 976) Da auf diese Weise nur die Sicherheit gegenüber bekannten Angriffen gewährleistet wird, wird die Mehrzahl moderner kryptografischer Verfahren vor ihrem Einsatz veröffentlicht. So können sie bereits vor ihrem Einsatz auf mögliche Angriffe getestet werden.

Die Argumentation für die Gültigkeit der Voraussetzungen (i) und (ii) in Beispiel 3 folgt dem angegebenen Schema plausiblen Schließens: Angenommen (i) und (ii) sind wahr, dann folgen die dargestellten Beobachtungen (keine Entdeckungen von polynomialen Algorithmen, keine alternativen Angriffe). Die Plausibilität wird durch verschiedene (und möglichst unabhängige) beobachtete Folgerungen aus den Annahmen (i) und (ii) gestärkt und dadurch insbesondere *B* ohne *A* als unwahrscheinlich charakterisiert (Pólya, 1975, S. 49f).

Damit enthält der deduktive Schluss in Beispiel 3 plausible Elemente, die gesamte Schlusskette ist „nur" plausibel. Die Verwendung des Begriffs *Sicherheit* bezogen auf RSA lässt sich nun präzisieren: Die Sicherheit von RSA lässt sich nicht (vollständig) deduktiv erschließen, sie ist jedoch plausibel. Der Schluss erfolgt auf Kosten der Eigenschaft, *in sich vollständig zu sein* (Festlegung geeigneter Schlüssellängen; Berücksichtigung der (bis dahin!) bekannten Angriffe). Die Einschätzungen zur Sicherheit von RSA (mit festgelegten Parametern) sind daher nur vorläufig, also *nicht dauerhaft*. Inwieweit eine konkrete Argumentation einschließlich Empfehlung zur Schlüssellänge als plausibel empfunden wird, ist individuell verschieden und daher *nicht unpersönlich*.

Ausblick - Plausibles Schließen und Allgemeinbildung

Missverständnisse über Mathematik bzw. zur Rolle der Mathematik in Anwendungen, die aus einer einseitigen Orientierung an den Merkmalen des Deduktiven entstehen, beschreibt Koblitz (2007, S. 977) in seinen Ausführungen zu *provable security*:

> "The first is the notion of 100% certainty. Most people not working in a given specialty regard a "theorem" that is "proved" as something that they should accept without question. The second connotation is

> of an intricate, highly technical sequence of steps. From a psychological and sociological point of view, a "proof of a theorem" is an intimidating notion: it is something that no one outside an elite of narrow specialists is likely to understand in detail or raise doubts about. That is, a "proof" is something that a non-specialist does not expect to really have to read and think about."

Koblitz verweist insbesondere auf die Merkmale *dauerhaft* und *unpersönlich*. Diese Merkmale des Deduktiven beziehen sich jedoch auf „fertige Mathematik", das gesicherte Wissen, das „sicher, unbestreitbar und endgültig" erscheint. Anwendungen von Mathematik, wie die Kryptografie, sind jedoch nie vollständig deduktiv beschreibbar, was innermathematische Grenzen mit einschließt, und enthalten immer auch Elemente plausiblen Schließens. Sie sind damit „gewagt, strittig und provisorisch" (vgl. Pólya 1988, S. 9). Die letztgenannten Eigenschaften sind nicht als Mangel, sondern als Merkmal aufzufassen, welches es beim Nachvollziehen mathematikhaltiger Argumentation zu beachten gilt (vgl. auch Führer 1988, S. 101). Ein Mittel dazu ist eine höhere Gewichtung bzw. Reflexion von Elementen plausiblen Schließens im Unterricht. Die hier vorgestellten kryptografischen Inhalte können als Ausgangspunkt derartiger Reflexionen im Unterricht dienen.

Bemerkung: Die Ausführungen sind ein verkürzter Teil des Kapitels „Allgemeinbildung und Kryptografie" aus der Dissertation der Autorin über Kryptografie in der Schule, die nächstes Jahr erscheint.

Literatur

Blechman, I. L; Myskis, A.D.; Panovko, J. G. (1984): Angewandte Mathematik: Gegenstand, Logik, Besonderheiten. Berlin, Deutscher Verlag der Wissenschaften

Buchmann, Johannes (2003): Einführung in die Kryptografie. Berlin: Springer

Führer, Lutz (1988): Mattematik – Laterna magica der Späth-Renaissance. Staatliches Studienseminar Hameln 1978-1988, Festschrift, 1988

Koblitz, Neal (2007): The uneasy relationship between mathematics and cryptography. In: Notices of the AMS 54, Nr. 8, S. 972-979

Pólya, Georg (1975): Mathematik und plausibles Schliessen. Bd. 2. Typen und Strukturen plausibler Folgerung. Basel u.a., Birkhäuser

Pólya, Georg (1988): Mathematik und plausibles Schliessen. Bd. 1. Induktion und Analogie in der Mathematik. Basel u.a., Birkhäuser