Komplexitätstheorie und Kryptographie

Marl Joos, Betreuer: Wolfgang Mulzer

***Zusammenfassung*—In dieser Arbeit wird der Zusammenhang zwischen der modernen Kryptographie und der Komplexitätstheorie erläutert.**

Zuerst wird die Geschichte der Sicherheit der Kryptographie skizziert, in der gezeigt wird, wie sich die Kryptographie von einer Kunst zu einer formalisierten Wissenschaft mit präzisen Definition und klaren Annahmen entwickelt hat.

Danach werden komplexitätstheoretische Konzepte wie z. B. die Einwegfunktion und die Falltürfunktion definiert und ihre Bedeutung für das theoretische Fundament der modernen Kryptographie und der Komplexitätstheorie hervorgehoben. Dabei wird sich herausstellen, dass die Existenz von Falltürfunktionen die Konstruktion von Public-Key-Kryptographie ermöglicht und die Existenz von Einwegfunktionen nicht nur äquivalent zur Existenz aller nicht-trivialer Private-Key-Kryptographie ist, sondern auch $P \neq NP$ impliziert.

Zum Schluss wird die Bedeutung der *average-case*-Komplexität auf Basis eines Papers von Impagliazzo[1] hervorgehoben. Dabei werden die von ihm vorgestellten möglichen "Welten" erläutert, in denen unterschiedliche Situationen bzgl. der Existenz kryptographischer Konzepte und komplexitätstheoretischen Aussagen angenommen werden, und deren Auswirkungen auf die Kryptographie beschrieben wird.

I. Was ist Kryptographie?

Die moderne Kryptographie befasst sich mit der Erforschung mathematischer Verfahren, um digitale Informationen, Systeme und verteilte Berechnungen vor Angriffen zu schützen.

Neben dem Entwurf von Verschlüsselungsverfahren, beschäftigt sich die modernen Kryptographie unter Anderem mit Mechanismen, um Integrität sicherzustellen, Techniken, um geheime Schlüssel auszutauschen, Authentifizierungsprotokolle, elektronische Auktionen und Wahlen sowie mit digitalem Geld. [3, 3]

Die Kryptoanalyse, die sich mit dem Brechen von kryptographischen Verfahren beschäftigt, und Kryptographie werden als Teilgebiete der Kryptologie betrachtet.

II. Geschichte der Sicherheit von kryptographischen Verfahren

Die Geschichte der Kryptographie beginnt schon vor unserer Zeitrechnung. Schon Julius Caesar übermittelte seinen Generälen, verschlüsselte Nachrichten mittels einer Verschiebechiffre, bei der Buchstaben um 3 Stellen im Alphabet verschoben wurden. Alan Turing trug maßgeblich zur Entzifferung des elektro-mechanischen Chiffriergeräts Enigma der Deutschen im 2. Weltkrieg bei.

Bis in die zweiten Hälfte des 20. Jahrhunderts war die Kryptographie größtenteils eine Kunst. Die Konstruktion guter Verfahren und das Brechen existierender basierte auf Kreativität und ein entwickeltes Gespür wie kryptographische Verfahren funktionieren. [3, 3]

Vor dem 20. Jahrhundert gab es Ansätze zur Beschreibung guter Verfahren, wovon das Kerckhoff's Prinzip von *Auguste Kerckhoff* zu den wichtigsten gehört und besagt, dass ein kryptographisches Verfahren nicht als geheim betrachtet werden sollte und ohne Nachteile in die Hände des Feindes fallen könnte. Dies bedeutet, dass die Sicherheit kryptographischer Verfahren nur auf die Geheimhaltung des Schlüssels basieren sollte. [3, 7]

Das Prinzip wird heute als Befürwortung der Veröffentlichung von Entwürfen kryptographischer Verfahren verstanden, d. h. als Gegensatz zu "security by obscurity" ("Sicherheit durch Unklarheit"), was behauptet, dass die Geheimhaltung der Verfahren die Sicherheit erhöht. [3, 8]

Trotz alledem blieb eine Formalisierung der Kryptographie aus. Erst 1954 verfolgte *Claude Shannon* den rigorosen Ansatz, Kryptographie auf präzisen Definitionen und mathematischen Beweisen aufzubauen. [3, 23]

In den 1970er und 1980er, als eine reichhaltige Theorie zu entstehen begann, die es ermöglichte die Kryptographie als Wissenschaft und mathematische Disziplin zu erforschen, wandelte sich das Bild der Kryptographie radikal. Die klassische Kryptographie entwickelte sich zur modernen Kryptographie. [3, 3]

In den vergangenen Jahren führte die Komplexitätstheorie zu einer Revolution beim Entwurf kryptographischer Verfahren. Sie erweiterte die Kryptographie und adressierte zahlreiche Themen bzgl. der Sicherheit von Informationen. So sind heute digitale Unterschriften und elektronische Wahlen möglich, die es erlauben die Herkunft einer Nachricht zu verifizieren oder Wahlen über ein Netzwerk erlauben, die überprüfbar sind, zugleich das Wahlgeheimnis schützen, Mehrfachwahl verbieten und andere Regeln forcieren. [2, 405]

III. Symmetrische und asymmetrische Kryptographie

Bevor erläutert wird, wie die Komplexitätstheorie als Basis der modernen Kryptographie fungiert, seien zwei Konzepte der Kryptographie informell beschrieben, um später einen Bezug herstellen zu können.

Symmetrische Kryptosysteme (in engl. auch: "private-key cryptosystem") verwenden für die Ver- und Entschlüsselung den gleichen Schlüssel, den geheimen Schlüssel.

Asymmetrische Kryptosysteme - auch Public-Key-Kryptosysteme genannt - verwenden für die Ver- und Entschlüsselung einen unterschiedlichen Schlüssel. Der

Schlüssel für die Verschlüsselung wird dabei als öffentlicher Schlüssel bezeichnet, der Schlüssel für die Entschlüsselung wird als geheimer Schlüssel bezeichnet.

IV. Komplexitätstheorie als Basis der modernen Kryptographie

In diesem Abschnitt werden Teile des theoretischen Fundaments der modernen Kryptographie vorgestellt, die auf komplexitätstheoretischen Überlegungen basieren: Einwegfunktionen (engl. one-way functions) und Falltürfunktionen (engl. trapdoor functions).

Der Vorteil von Komplexitätstheorie als Fundament der Kryptographie besteht darin, dass Annahmen bei der Betrachtung der Sicherheit verdeutlicht werden. [2, 407]

Bevor Einwegfunktionen und Falltürfunktionen definiert werden, werden Defintionen der probabilistischen Turingmaschine (engl. probabilistic Turing machine), der längenerhaltenden Funktionen (engl. length-preserving functions) und der Indizierungsfunktion benötigt.

A. Probabilistische Turingmaschine [2, 368;404]

Definition 1 Eine **probabilistische Turingmaschine** (Abk. PTM) M ist ein Typ der nicht-deterministischen Turingmaschine, in der jeder nicht-deterministische Schritt coin-flip step genannt wird - d. h. auf einem idealen Münzwurf basiert - und über zwei gültige nächste Schritte verfügt.

Wir weisen jedem Zweig b von M's-Berechnung mit der Eingabe w eine Wahrscheinlichkeit wie folgt zu:

$$Pr[b] = 2^{-k} \,, \tag{1}$$

wobei k die Anzahl der coin-flip steps, die im Zweig b auftreten, entspricht.

Die Wahrscheinlichkeit, dass M w akzeptiert wird wie folgt definiert:

$$Pr[M\, akzeptiert\, w] = \sum_{\substack{b\, ist\, ein \\ akzeptierender\, Zweig}} Pr[b] \,. \tag{2}$$

Berechne eine probabilistische Turingmaschine M eine **probabilistische Funktion** $M : \Sigma^* \to \Sigma^*$, wobei w die Eingabe und x die Ausgabe widerspiegelt, so wird

$$Pr[M(w) = x] \tag{3}$$

als Wahrscheinlichkeit, dass M mit der Eingabe w in einem akzeptierenden Zustand hält, in dem x auf dem Band steht, definiert.

B. Längen-erhaltende Funktion[2, 408]

Definition 2 Eine Funktion $f : \Sigma^* \to \Sigma^*$ ist **längenerhaltend** (engl. length-preserving), wenn die Längen von w und $f(w)$ für jedes w gleich sind.

C. Einwegfunktionen

Informell ausgedrückt sind Einwegfunktionen, Funktionen die im komplexitätstheoretischen Sinne leicht berechenbar sind, aber schwer zu invertierend sind.

In der folgenden Definition bezeichnet M den in polynomieller Zeit berechenbare probabilistische Algorithmus, der versucht eine Einwegfunktion f zu invertieren.

Definition 3 Eine **Einwegfunktion** ist eine längenerhaltende Funktion f mit folgenden Eigenschaften:

1) f ist in polynomieller Zeit berechenbar.
2) Für jede in polynomieller Zeit berechenbare probabilistische Turingmaschine M, für jedes k, gibt es ein genügend großes n, sodass wenn wir ein zufälliges w der Länge n wählen und w als Eingabe für M wählen, gilt:

$$Pr[M(f(w)) = y, \text{ wobei } f(y) = f(w)] \leq n^{-k} \,. \tag{4}$$

Dabei bedeutet Bedingung 2, dass die Funktion schwer invertierbar ist. D. h., wenn M es schafft, eine Eingabe für f zu finden, die zur gleichen Ausgabe führt, wenn w als Eingabe für f w gewählt wird, dann nur mit vernachlässigbarer Wahrscheinlichkeit.

D. Indizierungsfunktion [2, 409]

Definition 4 Eine Funktion $f : \Sigma^* \times \Sigma^* \to \Sigma^*$ ist eine **Indizierungsfunktion**, wenn für Familie von Funktionen $\{f_i\}$, wobei $i \in \Sigma^*$, $f(i, w) = f_i(w)$ entspricht.

Definition 5 Eine Indizierungsfunktion wird längenerhaltend genannt, wenn jede indizierte Funktion f_i längen-erhaltend ist.

E. Falltür-Funktionen [2, 410]

Definition 6 Eine **Falltür-Funktion** $f : \Sigma^* \to \Sigma^*$ ist eine längen-erhaltende Indizierungsfunktion, der eine polynomieller Hilfs-PTM G und eine Hilfsfunktion $h : \Sigma^* \times \Sigma^* \to \Sigma^*$ zugeordnet ist. Für f, G, und h gelten folgende Bedingungen:

1) f und h sind in polynomieller Zeit berechenbare Funktionen.
2) Für jede polynomielle PTM E, jedes k, gibt es ein genügend großes n und wenn wir eine zufällige Ausgabe $< i, t >$ von G mit der Eingabe 1^n und ein zufälliges $w \in \Sigma^n$ wählen, dann gilt:

$$Pr[E(i, f_i(w)) = y, \text{ wobei } f_i(y) = f_i(w)] \leq n^{-k} \tag{5}$$

3) Für jedes n, jedes w der Länge n, und jede Ausgabe $< i, t >$ von G, die bei irgend einer Eingabe mit einer Wahrscheinlichkeit > 0 auftritt gilt:

$$h(t, f_i(w)) = y, \text{ wobei } f_i(y) = f_i(w) \,. \tag{6}$$

G fungiert hierbei als Generator, der einen Index i einer Funktion in der Indexfamilie und einen Wert t, mit dem f_i leicht invertiert werden kann, ausgibt. Bedingung 2 gibt

an, dass f_i ohne t schwer zu invertieren ist. Bedingung 3 gibt an, dass f_i leicht zu invertieren ist, wenn t bekannt ist. h widerspiegelt die Invertierungsfunktion.

F. Implikation der Existenz von Einweg- und Falltürfunktionen

Der derzeitige Kenntnisstand reicht nicht aus, um die Existenz von Einwegfunktionen zu beweisen. Die Existenz von Einwegfunktionen würde implizieren, dass NP nicht in P enthalten ist und so eines der bekanntesten offenen Probleme der Informatik lösen. [4, xiv]

Kryptographisch betrachtet ist die Existenz von Einwegfunktionen äquivalent zu der Existenz aller (nicht-trivialer) symmetrischer Kryptosysteme. [3, 242] Mit der Annahme der Existenz von Einwegfunktionen, lassen sich Pseudozufallszahlengeneratoren konstruieren, die wiederum die Konstruktion von symmetrischen Kryptosystemen ermöglichen. [3, 273]

Die Existenz von Falltür-Funktionen ermöglicht die Konstruktion von Public-Key-Kryptosystemen. Ob die Existenz von Einwegfunktionen allein die Konstruktion von Public-Key-Kryptosystemen ermöglicht, ist unbekannt. [2, 430]

Das Problem der effizienten Primfaktorzerlegung und das Diskrete-Logarithmus-Problem, welche beim RSA- bzw. beim Elgamal-Kryptosystem verwendet werden, werden als Kandidaten für Einwegfunktionen angesehen.[3, 245-246]

Der Grund für die Auswahl dieser Probleme besteht darin, dass diese schwer im *average-case* angenommen werden und insbesondere die Primfaktorzerlegung nach jahrhundertelanger Untersuchung als relativ gut untersucht gilt. Das Brechen eines Kryptosystems aufgrund der Lösung der Primfaktorzerlegung würde eine außergewöhnliche Entwicklung der algorithmischen Zahlentheorie bedeuten.[2, 407]

V. Average-case complexity: Impagliazzo's fünf Welten [1]

Schwere Probleme wie z. B. NP-vollständige Probleme sind für die Kryptographie nicht ausreichend, da die Definition der NP-schwere nur den *worst-case* betrachtet.

Für die Kryptographie sind Probleme wichtig, die in fast allen Instanzen bzw. in Instanzen, die in der Praxis auftreten schwer sind Aus diesem Grund hilft die Betrachtung der Eingaben der Probleme, die die Probleme erst schwer lösbar machen ("structural theory of distributional complexity").

Die *structural theory of average-case complexity*, die durch *Levin* eingeführt wurde, leistete u. A. durch die Idee der *distributional problems* (Berechnungsprobleme zusammen mit der Betrachtung Verteilung der Instanzen), einer maschinen-unabhängigen Definition der *average-case performance* von Algorithmen, sowie die Idee, *distributional problems* untereinander zu reduzieren, einen Beitrag zu diesem Themengebiet.

Zur Veranschaulichung von Fragen in Bezug auf die *average-case*-Komplexität von Problemen in NP, stellte *Russell Impagliazzo* 1995 in einem Paper[1] fünf mögliche Welten vor, in denen komplexitätstheoretische und kryptographische Aussagen (z. B. $P = NP$ oder "Public-Key-Kryptographie existiert nicht") als wahr angenommen werden, und untersucht dabei die Auswirkungen der Annahmen auf verschiedene Gebiete der Informatik.

Zu diesen Welten gehören *Algorithmica*, *Heuristica*, *Pessiland*, *Minicrypt* und *Cryptomania*.

In diesem Abschnitt werden die Welten vorgestellt, wobei bei den Auswirkungen der Fokus überwiegend auf die Kryptographie gelegt wird.

A. Algorithmica

In dieser Welt gilt $P = NP$. Dieser Zustand, der durch die einfach Verifizierung von Lösungen von NP-Problemen zur automatischen Lösung von NP-Problemen führen würde, würde die Informatik revolutionieren. Hartnäckig scheinende Probleme würden trivial werden und fast jeder Typ von Optimierungsproblem wäre leicht und automatisiert lösbar.

Neben der Vereinfachung von Problemen in der künstlichen Intelligenz, wäre nicht-triviale Kryptographie unmöglich. Jedes nicht-triviale Kryptosystem wäre durch die Analyse einer kleine Anzahl von Klar- und Chiffretextpaaren leicht knackbar. Folglich wären Identifikationsprotokolle nur durch physische Maßnahmen möglich.

Um zu zeigen, dass *Algorithmica* existiert, muss ein effizienter Algorithmus für ein NP-vollständiges Problem aufgezeigt werden.

B. Heuristica

In dieser Welt sind NP-Probleme im *worst-case* schwer lösbar, im *best-case* jedoch leicht lösbar.

In einem gewissen Sinn ist *Heuristica* paradox, da schwere Instanzen von NP-Problemen existieren, aber diese zu finden selbst ein schweres Problem ist.

Angenommen, dass in der Praxis die Lösung schwerer Probleme selten ist, ist diese Welt für praktische Zwecke ähnlich *Algorithmica*, mit Unterschieden, die den Rahmen dieser Arbeit sprengen würde.

In Bezug auf die Kryptographie gibt es vergleichbar wenig Unterschiede zu *Algorithmica*, da Kommunikationspartner mit hohem Zeitaufwand Probleme generieren müssten, die von Lauschern in vergleichbarer Zeit gelöst werden würden. In vernünftiger Annahme, dass Lauscher mehr Ressourcen verwenden als die Kommunikationspartner gewohnheitsmäßig für die Kryptographie, gibt es praktisch keinen Nutzen an der Kryptographie in dieser Welt.

Um zu zeigen, dass *Heuristica* existiert, muss eine Methode aufgezeigt werden, mit der fast alle Instanzen eines *average-case*-vollständigen Problems schnell gelöst werden kann und zusätzlich nachgewiesen werden, dass es eine untere Schranke der *worst-case*-Komplexität einiger NP-vollständigen Probleme gibt.

C. Pessiland

In *Pessiland*, die aus Sicht von *Impagliazzo* die schlechteste aller Welten ist, existieren schwere *average-case*-Probleme, aber keine Einwegfunktionen.

Es ist möglich, viele schwere Instanzen von NP-Problemen zu generieren, aber es gibt keine Möglichkeit, gelöste Instanzen von Problemen zu generieren.

Viele Probleme in vielen Anwendungsgebieten wären nicht leicht lösbar und Fortschritt würde wie in unserer Welt langsam wie u. A. durch unbefriedigende Heuristiken erzielt werden.

Trotz dieser Situation impliziert die Nichtexistenz von Einwegfunktionen Fortschritte in anderen Gebieten wie u. A. in der Datenkompression.

Wie schon in Unterabschnitt IV-F genannt, ist die Existenz von Einwegfunktionen für viele kryptographische Anwendungen erforderlich. Ob sich Kryptographie auf Basis der Nichtexistenz von Einwegfunktionen aufbauen lässt, ist unklar. Folglich scheint in *Pessiland* keinen Weg zu geben, schwere Probleme für Kryptographie zu benutzen. Ein Problem, dessen Lösung keiner kennt, kann nicht benutzt werden, um legitime Kommunikationspartner von Lauschern zu unterscheiden.

Um zu zeigen, dass *Pessiland* existiert, müsste ein Algorithmus gefunden werden, die eine Funktion invertiert (eine solche Funktion wurde von *Levin* aufgezeigt), die vollständig im Sinne der Einwegeigenschaft ist. Zusätzlich müsste eine untere Schranke der *average-case*-Komplexität für einige Probleme in NP aufgezeigt werden.

D. Minicrypt

In *Minicrypt* existieren Einwegfunktionen, aber keine Public-Key-Kryptographie.

Wie auch in Unterabschnitt IV-F genannt, ist die Existenz von Einwegfunktionen äquivalent zur Existenz (nichttrivialer) symmetrischer Kryptographie. Andere kryptographische Anwendungen wie sichere digitale Wahlen sind nicht möglich oder es ist wie beim digitalen Geld unbekannt, ob sie möglich sind.

Um zu zeigen, dass *Minicrypt* existiert, müsste man beweisen, dass kein effizienter Algorithmus für die Invertierung einiger Einwegfunktionen existiert und zusätzlich aufzeigen, wie jedes *secret-key agreement protocol* gebrochen werden kann. Da für das letztere keine günstige Beschreibung existiert, ist nicht einmal klar, inwiefern man bei diesem Beweis beginnen würde.

E. Cryptomania

In *Cryptomania*, die *Impagliazzo* als unserer Welt am nächsten bezeichnet, existiert Public-Key-Kryptographie.

Da dies die Existenz von Einwegfunktionen impliziert, existieren fast alle kryptographische Konstrukte bzw. Anwendungen wie u. A. Pseudozufall, Signaturen, Zero-Knowledge-Protokolle, sichere elektronische Wahlen und digitales Geld, wobei bei den letzten beiden die Praxistauglichkeit nicht notwendigerweise gegeben sein muss.

Um zu zeigen, dass *Cryptomania* existiert, müsste gezeigt werden, dass ein *secret-key exchange protocol* sicher ist. Der Beweis für eine starke untere Grenze der average-case-Komplexität von Primfaktorzerlegung oder vom Bilden diskreter Logarithmen würde ausreichen.

VI. Fazit

Da komplexitätstheoretische Konzepte wie Einwegfunktionen und Falltürfunktionen das theoretische Fundament der modernen Kryptographie bilden, besteht ein untrennbarer Zusammenhang zwischen der Komplexitätstheorie und der modernen Kryptographie.

Die Komplexitätstheorie erlaubt es der Kryptographie mit präzisen Definitionen und klaren Annahmen zu arbeiten, um Sicherheitsbeweise zu formalisieren.

So ist unter der Annahme der Existenz von Einweg- und Falltürfunktionen die Konstruktion von symmetrischer und asymmetrischer Kryptographie möglich.

Obwohl die Existenz von Einwegfunktionen nicht bewiesen ist bzw. der Beweis der Existenz eines der bedeutendsten Probleme in der Informatik lösen würde, werden NP-Probleme wie die Primfaktorzerlegung und das diskrete-Logarithmus-Problem dazu verwendet, um kryptographische Verfahren aufzubauen.

Dabei spielt es eine wichtige Rolle, wie *Impagliazzo* in seinem Paper[1] ausführte, dass NP-vollständige Probleme zur Konstruktion von sicherer Kryptographie nicht ausreichen, da die Definition nur die *worst-case*-Komplexität betrachtet. Für die Kryptographie ist es wichtig, dass Probleme im *average-case* schwer sind, d. h. leicht Instanzen generiert werden können, die schwer lösbar sind.

Für die in dieser Arbeit besprochenen Kandidaten für Einwegfunktionen, die Primfaktorzerlegung und das diskrete-Logarithmus-Problem, existieren Algorithmen (Shor-Algorithmus), die diese Probleme auf Quantencomputern in polynomieller Zeit berechnen.

In der Zwischenzeit hat sich ein neues Forschungsgebiet in der Kryptographie entwickelt - die Post-Quanten-Kryptographie - die die Entwicklung von kryptographischen Verfahren erforscht, die selbst bei Existenz von Quantencomputern, Sicherheit gewährleisten. Als Basis für diese Verfahren werden bspw. mathematische Gitter (engl. lattice) verwendet.

Literatur

[1] Impagliazzo, R., & Proceedings of Structure in Complexity Theory. Tenth Annual IEEE Conference. (January 01, 1995). A personal view of average-case complexity. 134-147.

[2] Sipser, M. (2006). Introduction to the theory of computation. Boston: Thomson Course Technology. 405-411.

[3] Katz, J., & Lindell, Y. (2015). Introduction to modern cryptography.

[4] Goldreich, O. (2001). Foundations of Cryptography: Volume 1. Cambridge: Cambridge University Press.