Handout zum Algorithmikseminar
Kryptographie
von Gerrit Gruben

I Einführung

Die Kryptographie ist eine uralte Wissenschaft, die sich aus dem Bedürfnis heraus entwickelt, Kommunikation gegen Unbefugte zu schützen, also seine Daten zu sichern. In dieser Arbeit werden grundlegende Fragen der Kryptographie beantwortet: Wann ist ein Kryptographiesystem sicher? Was ist Pseudozufall und Einwegfunktionen? Was haben diese mit der Kryptographie zu tun?

1. **Datensicherheit** Schutz vor unbefugtem Lesen von Daten.
2. **Datenintegrität** Schutz vor ungewollter Modifikation der Daten.
3. **Authentifikation** Nachweis einer Identität in dem man
   (a) Etwas weiß
   (b) oder etwas besitzt
   (c) oder etwas ist.

Definition 1 (Kryptosystem).
Ein Paar $(\mathbf{Enc}, \mathbf{Dec})$ von Funktionen

$$\mathbf{Enc} : \mathcal{K} \times \mathcal{M} \to \mathcal{C},\ (k, x) \mapsto \mathbf{Enc}_k(x)$$

$$\mathbf{Dec} : \mathcal{K} \times \mathcal{C} \to \mathcal{M},\ (k, y) \mapsto \mathbf{Dec}_K(y)$$

mit den Mengen $\mathcal{M}, \mathcal{C}, \mathcal{K}$ (**Klartext-**,**Chiffretext-** und **Schlüsselmenge**) heißt **Kryptosystem**, wenn zusätzlich die Bedingung gilt

$$\mathbf{Dec}_k \circ \mathbf{Enc}_k = \mathrm{Id}_{\mathcal{M}}\ (\forall k \in \mathcal{K})$$

II Perfekte Geheimhaltung

Definition 2.
Ein Kryptosystem $(\mathbf{Enc}, \mathbf{Dec})$ über $\mathbb{B}^n$ bietet **perfekte Geheimhaltung**, falls für jede Verteilung $\mathcal{D}$ von Nachrichten, jeder Nachricht m und jeden auftretenden Chiffretext c gilt

$$\mathbf{Pr}\left[M = x \mid C = c\right] = \mathbf{Pr}\left[M = x\right]$$

Äquivalent: $\mathbf{Enc}_{U_n}(x) = \mathbf{Enc}_{U_n}(x')$

Lemma 1 Für ein Kryptosystem $\Pi = (\mathbf{Enc}, \mathbf{Dec})$ sind die folgenden Aussagen äquivalent

1. Π bietet perfekte Geheimhaltung.
2. Für jede Verteilung auf $\mathcal{M}$ und allen $x \in \mathcal{M}$, $y \in \mathcal{C}$ gilt:
$$\mathbf{Pr}\left[C = y \mid M = x\right] = \mathbf{Pr}\left[C = y\right].$$
3. Für jede Verteilung auf $\mathcal{M}$ und allen $x_0, x_1 \in \mathcal{M}$ und $c \in \mathcal{C}$ gilt
$$\mathbf{Pr}\left[C = y \mid M = x_0\right] = \mathbf{Pr}\left[C = y \mid M = x_1\right]$$

Lemma 2 Ein Kryptosystem $(\mathbf{Enc}, \mathbf{Dec})$ mit Klartextmenge $\mathcal{M}$ und Schlüsselmenge $\mathcal{K}$ bietet perfekte Geheimhaltung, dann gilt

$$|\mathcal{K}| \geq |\mathcal{M}|$$

Satz 1 (von Shannon).
Sei $(\mathbf{Enc}, \mathbf{Dec})$ ein Kryptosystem mit $|\mathcal{K}| = |\mathcal{M}| = |\mathcal{C}|$. Dann bietet das Kryptosysteme perfekte Geheimhaltung genau dann wenn folgende Bedingungen gelten:

1. Die Schlüssel werden gleichverteilt gewählt, d. h. $K \sim U_{\mathcal{K}}$.
2. Für alle Nachrichten $x \in M$ und Chiffretexten $y \in C$ existiert genau ein $k \in K$ mit $y = \mathbf{Enc}_k(x)$.

Definition 3 (One-Time-Pad).
Seien $\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0,1\}^n$ für ein $n \in \mathbb{N}$. Dann heisst $(\mathbf{Enc}, \mathbf{Dec})$

$$\mathbf{Enc}_k(x) := x \oplus k,\ \mathbf{Dec}_k(y) := y \oplus k$$

One-Time-Pad (Vernam Chiffre).

Der Satz von Shannon zeigt, dass das One-Time-Pad perfekte Geheimhaltung bietet.

III Berechnungssicherheit

Lemma 3 Sei $\mathcal{P} = \mathcal{NP}$ und $(\mathbf{Enc}, \mathbf{Dec})$ in Polynomialzeit berechenbar mit einer Schlüssellänge von $n = n(m) < m$ bei Nachrichtenlänge m. Dann existiert ein Polynomialzeitalgorithmus A, so dass für alle Eingabelängen m gilt: es gibt es ein Paar $x_0, x_1 \in \{0,1\}^m$ mit

$$\Pr_{\substack{b \in_R \{0,1\} \\ k \in_R \{0,1\}}} [A(\mathbf{Enc}_k(x_b)) = b] \geq \frac{3}{4}$$

Definition 4 (Vernachlässigbare Funktionen).
Sei $\epsilon : \mathbb{N} \to [0,1] \subseteq \mathbb{R}$, dann heisst ϵ **vernachlässigbar**, wenn $\epsilon(n) = n^{-\omega(1)}$. D. h. für alle $c > 0$ existiert ein $N \in \mathbb{N}$, sodass $\epsilon(n) < n^{-c}$ für alle $n \geq N$ gilt.

Mit vernachlässigbaren Funktionen wollen wir Ereignisse modellieren, welche praktisch nie eintreten.

Definition 5 (Einwegfunktionen).
Eine in Polynomialzeit berechenbare Funktion $f : \mathbb{B}^* \to \mathbb{B}^*$ heißt **Einwegfunktion**, falls für alle $A \in \mathcal{PPT}$ gilt:

$$\Pr_{\substack{x \in \mathbb{B}^n \\ y = f(x)}} [A(y) = x' \text{ mit } f(x') = y]$$

ist vernachlässigbar in $n \in \mathbb{N}$. Gilt $|f(x)| = |x|$ für $x \in \mathbb{B}^*$, so heisst f **längenerhaltend**. Ist f eine injektive , längenerhaltende Einwegfunktion, dann heisst f **Einwegpermutation**.

Vermutung: Es existiert eine Einwegfunktion.

Satz 2.
Wenn $P = \mathcal{NP}$, dann existieren keine Einwegfunktionen.

Beispiel (Faktorisierung):
Betrachtet man die Multiplikation $a \cdot b =: N$ zweier Zahlen $a, b \in \mathbb{N}$, so ist die Umkehrung im gewissen Sinne die Faktorisierung einer Zahl in ihren Primfaktoren. Der naive Algorithmus, die Probedivision von Teilern bis $\sqrt{N}$ ist exponentiell in der Eingabegröße $\log(N)$. Es gibt einen Faktorisierungsalgorithmus mit einer oberen Laufzeitschranke von $2^{\mathcal{O}(\log^{1/3} N \sqrt{\log \log N})}$.

Das nächste Beispiel benötigt die **eulersche φ-Funktion** für diese gilt

$$\varphi(n) := |\{1 \leq j < n \mid \mathrm{ggT}(j,n) = 1\}| = \left|\left(\mathbb{Z}/n\,\mathbb{Z}\right)^*\right|$$

Beispiel (RSA):
Für ein $n \in \mathbb{N}$ sei $N = N(n) \in \mathbb{N}$ eine zusammengesetzte Zahl und $e \in \mathbb{N}$ mit $\mathrm{ggT}(\varphi(n), e) = 1$. Im Regelfall ist N das Produkt zweier verschiedener Primzahlen $p, q \neq 2$. Es ist dann für $x \in \left(\mathbb{Z}/N\,\mathbb{Z}\right)^*$:

$$\mathbf{Enc}_{(N,e)}(x) = RSA_{(N,e)}(x) = \rho_N(x^e)$$

die Chiffrierungsfunktion vom **RSA-Kryptosystem** mit $\rho_N : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/N\,\mathbb{Z}$ der Reduktion modulo N. Dechiffriert werden kann ein Chiffretext y mit einem geheim gehaltenen d, welches die Gleichung

$$ed \equiv 1 \mod \varphi(N)$$

erfüllt und zwar mit

$$\mathbf{Dec}_{(N,e)}(y) = \rho_N(y^d)$$

Kennt man den Wert von $\varphi(N)$, so lässt sich d effizient mit dem euklidischen Algorithmus bestimmen. Es lässt sich $\varphi(N)$ effizient unter Kenntnis der Primfaktorzerlegung berechnen. Im allgemeinen Fall gilt für $n = \prod_{i=1}^{r} p_i^{\nu_i}$ mit verschiedenen Primzahlen p_i:

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\nu_i - 1}(p_i - 1)$$

wie man z. B. mit dem Inklusion-Exklusionsprinzip zeigen kann.

Beispiel (Rabin):
Sei $N = PQ$ wieder das Produkt zweier verschiedener Primzahlen größer 2. Zusätzlich gelte $P, Q \equiv 3 \mod 4$. Wir betrachten die Menge der quadratischen Reste

$$QR_N := \{z \in \mathbb{Z}_N^* \mid \exists y \in \mathbb{Z}_n^* : y^2 = z\}$$

wobei $\mathbb{Z}_n := \mathbb{Z}/n\,\mathbb{Z}$ für $n \in \mathbb{N}$. Das Verschlüsseln ist nun das quadrieren einer Zahl $\mod N$. Die Dechiffrierung ist das Quadratwurzel ziehen in $\mathbb{Z}_N$. Da der Empfänger die Faktorisierung von N kennt, kann er mit Hilfe des chinesischen Restsatzes das Problem auf die simultane Quadratwurzelbestimmung in $\mathbb{Z}_P$ und $\mathbb{Z}_Q$ reduzieren. Wegen $P, Q \equiv 3 \mod 4$ gilt aber:

$$z^{(P+1)/4} = \sqrt{z} \mod P$$

und analog für Q. Mit Hilfe des schnellen Exponentierens lässt sich so die Quadratwurzel effizient bestimmen.

Definition 6 (Levins universelle Einwegfunktion).
Es ist $f_{\mathcal{U}}$ **Levins universelle Einwegfunktion** wie folgt definiert: Die Eingabe wird geeignet zerteilt: $x = x_1 \cdots x_{\log n}$ ($n := |x|$) mit $|x_i| = \frac{n}{\log n}$ für $i = 1, \ldots, \log n$. Sei $(M_i)_{i \in \mathbb{N}}$ eine Abzählung aller Turingmaschinen. Dann gilt

$$f_{\mathcal{U}}(x) = M_1^{n^2}(x_1) \cdots M_{\log n}^{n^2}(x_{\log n})$$

wobei

$$M_i^t(x) = \begin{cases} M_i(x), & M_i \text{ terminiert nach } \leq t \text{ Schritten.} \\ 0^{|x|}, & \text{sonst} \end{cases}$$

Satz 3.
Falls es eine Einwegfunktion gibt, dann ist $f_{\mathcal{U}}$ eine Einwegfunktion.

Satz 4.
Wenn Einwegfunktionen existieren, dann gibt es ein $c \in \mathbb{N}$, sodass es ein berechnungssicheres Kryptosystem $(\mathbf{Enc}, \mathbf{Dec})$ gibt, welches eine Schlüssellänge von n und Nachrichtenlänge von n^c hat.

Berechnungssicherheit bedeutet für ein Kryptosystem $(\mathbf{Enc}, \mathbf{Dec})$ mit Schlüssellänge n und Eingabelänge m, dass wir für alle $A \in \mathcal{PPT}$ eine vernachlässigebare Funktion ϵ haben, so dass (x_i bezeichne das i-te Bit von der Nachricht x):

$$\mathop{\mathbf{Pr}}_{\substack{k\in_R\{0,1\}^n \\ x\in_R\{0,1\}^m}} [A(E_k(x)) = (i, b) \text{ s. d. } x_i = b] \geq \frac{1}{2} + \epsilon(n)$$

gilt. Das heisst über kein Bit der Nachricht x kann ein Angreifer mit nicht vernachlässigbarer Wahrscheinlichkeit Informationen in Polynomialzeit errechnen.

IV Pseudozufall

Was ist Zufall? **Kolmogorow** definiert eine Zeichenkette der Länge n als zufällig, wenn keine Turingmaschine mit einer Codierungslänge von $< \frac{99}{100}n$ die Zeichenkette n bei einer leeren Eingabe ausgibt. Dies führt zum Begriff der **Kolmogorow-Komplexität**. Leider ist die Frage i. A. unentscheidbar, daher für die Zwecke der Kryptographie ungeeignet. Ein alternativer Ansatz stammt aus der Statistik. Dort müssen zufälligen Zeichenketten bzw. deren Teilmuster die Gesetze der Statistik genügen. Jedoch existiert eine Verteilung die diese Definition erfüllt, aber für Zwecke der Kryptographie ungeeignet ist. Die Definition von Pseudozufall die der heutigen Kryptographie genügt ist: Eine Verteilung ist pseudozufällig, wenn sie nicht effizient vom wahren Zufall zuverlässig unterscheidbar ist.

Definition 7 (Pseudozufallsgenerator (PZG)).
Seien $G : \mathbb{B}^* \to \mathbb{B}^*, \ell : \mathbb{N} \to \mathbb{N}$ in Polynomialzeit berechenbar und gelte $\ell(n) > n$ für alle $n \in \mathbb{N}$. (G, ℓ) heisst **Pseudozufallsgenerator** (kurz: **PZG**) mit Dehnung ℓ, wenn gilt $|G(x)| = \ell(|x|)$ für alle $x \in \mathbb{B}^*$ und für alle $A \in \mathcal{PPT}$ existiert ein vernachlässigbares ϵ, sodass

$$\left|\mathbf{Pr}\left[A(G(U_n)) = 1\right] - \mathbf{Pr}\left[A(U_{\ell(n)}) = 1\right]\right| < \epsilon(n) \ (n \in \mathbb{N})$$

gilt.

Satz 5 (Einwegfunktionen $\Rightarrow$ PZG).
Existiert eine Einwegfunktion, dann existieren für alle Polynome ℓ mit $\ell(n) > n$ für $n \in \mathbb{N}$ ein PZG (G, ℓ).

Definition 8.
Sei $G : \mathbb{B}^* \to \mathbb{B}^*$ mit Dehnung ℓ. G und ℓ sind in Polynomialzeit berechenbar. G heißt **unvorhersehbar**, wenn für alle $B \in \mathcal{PPT}$ gilt:

$$\mathop{\mathbf{Pr}}_{\substack{x\in_r\mathbb{B}^n \\ y=G(x) \\ i\in_R[\ell(n)]}} [B(1^n, y_1, \ldots, y_{i-1}) = y_i] \leq 1/2 + \epsilon(n) \ (n \in \mathbb{N})$$

mit vernachlässigbaren ϵ.

Lemma 4 (Yao) Sei (G, ℓ) ein PZG, dann existieren für alle $A \in \mathcal{PPT}$ ein $B \in \mathcal{PPT}$, so dass für alle $n \in \mathbb{N}$ und $\epsilon > 0$ aus $\mathbf{Pr}\left[A(G(U_n))\right] - \mathbf{Pr}\left[A(U_{\ell(n))}\right] \geq \epsilon$, folgt

$$\mathop{\mathbf{Pr}}_{\substack{x\in_R\{0,1\}^n \\ y=G(x) \\ i\in_R[\ell(n)]}} [B(1^n, y_1, \ldots, y_{i-1}) = y_i] \geq 1/2 + \epsilon/\ell(n).$$

Satz 6.
Existiert eine Einwegpermutation, dann existiert ein PZG G mit Dehnung $n + 1$.

Satz 7 (Goldreich-Levin Theorem).
Sei $f : \mathbb{B}^* \to \mathbb{B}^*$ eine Einwegpermutation. Dann gibt es für alle $A \in \mathcal{PPT}$ ein vernachlässigbares ϵ mit

$$\mathop{\mathbf{Pr}}_{\substack{x\in_R\mathbb{B}^n \\ r\in_R\mathbb{B}^n}} \left[A(f(x), r) = x^t \cdot r = \sum_{i=1}^{n} x_i r_i\right] \leq 1/2 + \epsilon(n)$$

Satz 8 (PZGs mit polynomieller Dehnung).
Sei f eine Einwegpermutation, $c \in \mathbb{N}$ und $x, r \in \mathbb{B}^n$, setze:

$$G(x,r) := r, f(x)^t \cdot r, f^2(x)^t \cdot r, \ldots, f^l(x)^t \cdot r$$

mit $l = n^c$. Dann ist G ein PZG mit Dehnung $l(2n) = n + n^c$.

V Zero-Knowledge Beweise

In mathematischen Beweisen von Aussagen wird mehr Information preisgegeben als nur die Wahrheit der bewiesenen Aussage. Es gibt Fälle in denen diese Preisgabe an zusätzlichen Informationen nicht gewollt ist, dies führt zum Begriff der Zero-Knowledge Beweise. Modelliert wird dies mit einer Interaktion zwischen einem Beweiser P (für Prover) und Verifizier V.

Definition 9 (Zero-Knowledge Beweise).
Sei $L \in \mathcal{NP}$ und M eine Turingmaschine, die in Polynomialzeit läuft, mit

$$x \in L \Leftrightarrow \exists u \in \{0,1\}^{p(|x|)} : M(x,h) = 1. \ (p \text{ Polynom})$$

M entscheidet also L mit Hilfe eines Zeugen u.

Ein Paar (P, V) von interaktiven Polynomialzeitalgorithmen heißt Zero-Knowledge Beweis für L, falls die folgenden Eigenschaften erfüllt sind: **Vollständigkeit** (Completeness): Für jedes $x \in L$ und Zertifikat $u = u(x)$ gilt

$$\mathbf{Pr}\left[\text{out}_V \langle P(x,), V(x)\rangle\right] \geq \frac{2}{3}$$

Wobei $\langle P(x,u), V(x)\rangle$ die Interaktion zwischen P und V mit den gegebenen Eingaben bezeichnet und $\text{out}_V\, I$ beschreibt die Ausgabe von V am Ende der Interaktion I.

Zuverlässigkeit (Soundness): Wenn $x \notin L$, dann gilt für jede Strategie P^* und Eingabe u, dass

$$\mathbf{Pr}\left[\text{out}_V \langle P^*(x,u), V(x)\rangle\right] \leq \frac{1}{3}$$

dabei ist P^* in keiner Weise beschränkt.

Perfect-Zero-Knowledge-Eigenschaft: Für alle Verifizierstrategien $V^* \in \mathcal{PPT}$ existiert ein S^* mit erwarteter probabilistischer Polynomiallaufzeit, so dass für alle $x \in L$ und u Zeuge dafür gilt:

$$\text{out}_{V^*} \langle P(x,u), V^*(x)\rangle \equiv S^*(x)$$

Die Gleichheit bezieht sich auf die Gleichheit der Verteilungen. S^* **simuliert** V^*.

Beispiel (Zero-Knowledge Beweis für Graphenisomorphie (GI)):
Das Entscheidungsproblem der Graphenisomorphie ist es für Graphen G_0 und G_1 zu entscheiden, ob $G_0 \cong G_1$, d. h. ob es eine Bijektion $\Phi : V(G_0) \to V(G_1)$ gibt, so dass

$$vw \in E(G_0) \Leftrightarrow \Phi(v)\Phi(w) \in E(G_1)$$

oder anders formuliert, ob $V(G_0) = V(G_1)$ und ob eine Permutation (o. E. $V(G_0) = [n]$) $\pi : [n] \to [n]$ existiert, sodass $G_1 = \pi(G_0)$ gilt. Hierfür existiert ein Zero-Knowledge Beweis mit der Interaktion:
Eingabe: Graphen G_0, G_1 mit $V(G_i) = [n]$ in Adjazenzmatrixform gegeben.
Eingabe von P: $\pi : [n] \to [n]$ mit $G_1 = \pi(G_0)$. *Interaktion*: P wählt Permutation $\pi_1 \in_R S_n$ und sendet V die Adjazenzmatrix von $\pi_1(G_1)$ dieser Graph soll H heißen (dies wird inbesondere dann wichtig, wenn P kein Isomorphismus kennt). V wählt ein $b \in_R \{0,1\}$ zufällig und schickt es zu P. Nun antwortet P mit π_1 falls $b = 1$ und sonst mit $\pi_1 \circ \pi$. Diese Antwort sei mit $\widetilde{\pi}$ bezeichnet. Jetzt akzeptiert V genau dann wenn $\pi_1(G_1) = \widetilde{\pi}(G_b)$. Als Bild