Komplexitätstheorie

Sommersemester 2019

Mario Holldack, M. Sc.
Prof. Dr. Georg Schnitger
Hannes Seiwert, M. Sc.

GOETHE UNIVERSITÄT
FRANKFURT AM MAIN

Institut für Informatik
AG Theoretische Informatik

Übungsblatt 6

Ausgabe: 27.05.2019
Abgabe: 03.06.2019

Aufgabe 6.1 *Verkettung von One-Way-Permutationen* (4 Punkte + 4* Extrapunkte)

a) Sei $k = \texttt{poly}(n)$. Zeigen Sie: Wenn $\pi_n : \{0,1\}^n \to \{0,1\}^n$ eine One-Way-Permutation ist, dann ist

$$\pi_n^k := \underbrace{\pi_n \circ \pi_n \circ \cdots \circ \pi_n}_{k\text{-mal}}$$

eine One-Way-Permutation, wobei $\pi_n \circ \pi_n \circ \cdots \circ \pi_n(x) = \pi_n(\pi_n(\cdots \pi_n(x) \cdots))$ die k-fache Verkettung von π_n mit sich selbst ist.

b*) Sei $1 \leq k \leq n$. Annahme: Es gibt One-Way-Permutationen.

Zeigen Sie: Es gibt eine One-Way-Funktion $f_n : \{0,1\}^n \to \{0,1\}^n$, sodass

$$f_n^k := \underbrace{f_n \circ f_n \circ \cdots \circ f_n}_{k\text{-mal}}$$

keine One-Way-Funktion ist.

Hinweis: Bestimmen Sie f_n so, dass $|\text{Bild}(f_n^i)| = |\{f_n^i(x) : x \in \{0,1\}^n\}| = 2^{n-i+1}$ für alle $i \in \{1, \ldots, n\}$, d. h. bei jeder weiteren Verkettung von f_n mit sich selbst halbiert sich die Anzahl der getroffenen Bitstrings.

Aufgabe 6.2 *Der Generator der polynomiellen Kongruenzen* (4 Punkte + 4 Extrapunkte)

Für eine Primzahl p und Koeffizienten $a = (a_0, \ldots, a_d)$ sei $G_{a,p}(x) := \sum_{i=0}^{d} a_i x^i \bmod p$ der Generator der polynomiellen Kongruenzen vom Grad d, der die Folge

$$x_0 := s$$
$$x_{k+1} := \sum_{i=0}^{d} a_i x_k^i \bmod p$$

mit $s \not\equiv 0 \bmod p$ und $a_i \not\equiv 0 \bmod p$ für alle $i \in \{0, \ldots, d\}$ erzeugt.

Sei $k \geq d+1$ beliebig. Nach k-facher Anwendung von $G_{a,p}$ möchten wir x_{k+1} ohne direkten Zugriff auf den Generator *vorhersagen*. Einen Algorithmus, der x_{k+1} vorhersagt, bezeichnen wir als *effizient*, wenn seine Laufzeit polynomiell in k und $\log p$ ist.

a) Angenommen, wir kennen die Primzahl p, aber nicht die Koeffizienten $a_0, \ldots, a_d$. Geben Sie einen effizienten, deterministischen Algorithmus an, der x_{k+1} vorhersagt.

Hinweis: Bestimmen Sie die Koeffizienten $a_0, \ldots, a_d$ mithilfe der Folgenglieder $x_0, \ldots, x_{d+1}$.

b∗) Seien die Primzahl p und die Koeffizienten $a_0, \ldots, a_d$ unbekannt und $p = \Theta(k)$ mit $p > k$. Geben Sie einen effizienten, deterministischen Algorithmus an, der x_{k+1} vorhersagt.

Hinweis: Wie viele verschiedene Werte tauchen in der Folge $x_0, x_1, x_2, \ldots$ höchstens auf?

Anmerkung: Für eine frühere Version der Aufgabe war der gegebene Hinweis nicht zielführend. Sie wurde nachträglich als Extrapunkte-Aufgabe deklariert.

Sie können Teilpunkte erhalten, wenn Sie die Aufgabe für den Spezialfall $d = 1$ lösen.

Fazit: Für Generatoren polynomieller Kongruenzen reichen Moduli polynomieller Größe nicht aus. Tatsächlich kann man für lineare und quadratische Kongruenzen zeigen, dass selbst Moduli exponentieller Größe nicht ausreichen.[1]

Aufgabe 6.3 *Informationstheoretische und algorithmische Sicherheit* (6 + 6 = 12 Punkte)

Sei z ein geheimer Schlüssel, der sowohl Alice als auch Bob bekannt ist. In dieser Aufgabe zeigen wir, dass in vielen kryptographischen Anwendungen die informationstheoretische Sicherheit nicht gewährleistet werden kann, da z typischerweise kürzer ist als die zu verschlüsselnde Nachricht x. Sofern Pseudo-Random-Generatoren existieren, können wir jedoch zeigen, dass algorithmisch sichere Private-Key-Kryptographie auch für kurze geheime Schlüssel möglich ist.

a) Bob schickt eine verschlüsselte Nachricht $y = f(x, z)$ an Alice, die die Klartextnachricht x mit Hilfe einer Funktion h wiederherstellen kann, d. h. es gilt $h(f(x, z), z) = x$.

Zeigen Sie: Wenn f informationstheoretisch sicher ist, dann ist $|z| \geq |x|$, d. h. der private Schlüssel z ist mindestens so lang wie die Nachricht x.

Hinweis: Wie viele verschlüsselte Nachrichten $f(x, z)$ gibt es, wenn x fixiert ist? Wie viele Klartextnachrichten x gibt es, wenn $y = f(x, z)$ fixiert ist?

Definition (Informationstheoretische Sicherheit). *Sei $f : \{0,1\}^n \to \{0,1\}^n$ eine Funktion und (X, Z) eine uniform über $\{0,1\}^n$ verteilte Zufallsvariable. Dann heißt f* informationstheoretisch sicher*, wenn*

$$\boldsymbol{pr}_{(x,z)\in_R\{0,1\}^n}\big[(X, Z) = (x, z) \mid f(x, z) = y\big] = \boldsymbol{pr}_{(x,z)\in_R\{0,1\}^n}[(X, Z) = (x, z)],$$

d. h. für jede verschlüsselte Nachricht y liefert f die Gleichverteilung auf der Menge aller Nachrichten und Schlüssel. Es gibt also kein effizientes Verfahren, das y mit nicht-trivialer Erfolgswahrscheinlichkeit entschlüsselt. ◇

Fazit: Das One-Time-Pad $f(x, z) = x \oplus z$ ist bezüglich der Schlüssellänge $|z|$ optimal unter den informationstheoretisch sicheren Verschlüsselungsverfahren.

b) Sei $m := |z| < |x| =: n$ mit $|x| = \texttt{poly}(|z|)$ und G ein Pseudo-Random-Generator mit $|G(z)| = |x|$. Bob schickt eine verschlüsselte Nachricht $y = f(x, z) = x \oplus G(z)$ an Alice, die die Klartextnachricht x mit Hilfe einer Funktion h wiederherstellen kann: $h(y, z) := y \oplus G(z) = x$.

Zeigen Sie:

Für jede Schaltkreisfamilie $T = (T_n : n \in \mathbb{N})$ polynomieller Größe und für jedes $x \in \{0,1\}^n$ ist die absolute Differenz

$$\Big|\mathbf{pr}_{z\in_R\{0,1\}^m}\big[T_n(x \oplus G(z)) = 1\big] - \mathbf{pr}_{u\in_R\{0,1\}^n}\big[T_n(u) = 1\big]\Big|$$

als Funktion von m und n vernachlässigbar.

[1] J. Boyar, Infering sequences produced by random number generators, JACM 36(1), pp. 129-141, 1989.