Kryptographie und Kodierungstheorie

Definitionen

Inhaltsverzeichnis

1 Symmetrische Kryptographie

1.1 Klassische Kryptographische Verfahren

1.2 Symmetrische Kryptosysteme

1.2.1 Definition: (Symmetrisches) Kryptosystem

Ein Tupel $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ bestehend aus einer *Klartextmenge* $\mathcal{M}$, einer *Schlüsselmenge* $\mathcal{K}$, einer *Chiffretextmenge* $\mathcal{C}$, einer *Verschlüsselungsfunktion* $e : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ und einer *Entschlüsslungsfunktion* $d : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$ heißt *Kryptosystem*, wenn die Mengen $\mathcal{M}, \mathcal{K}$ und $\mathcal{C}$ nichtleer sind und $d(k, e(k, m)) = m$ für alle $k \in \mathcal{K}$ und $m \in \mathcal{M}$ gilt.

1.2.6 Definition: Quotient, Rest

Sei $a \in \mathbb{Z}$ und $m \in \mathbb{N}$. Sind r und q wie in 1.2.5 gewählt, so heißt q *Quotient* und r *Rest* von a bei ganzzahliger Division durch m. Für den Quotient schreibt man dann $q = [a/m]$ und für den Rest $r = a \mod m$

1.2.7 Definition: Restklasse

Sei $a \in \mathbb{Z}$ und $m \in \mathbb{N}$. Die *Restklasse* $[a]_m$ von a modulo m wird definiert durch $[a]_m = \{a+mq | q \in \mathbb{Z}\}$ und auch als $a+\mathbb{Z}m$ geschrieben. Wenn klar ist, dass Restklassen modulo m betrachtet werden, schreibt man häufig nur a statt $[a]_m$. Die Menge $\{[a]_m | a \in \mathbb{Z}\}$ aller Restklassen modulo m wird mit $\mathbb{Z}_m$ oder $\mathbb{Z}/m\mathbb{Z}$ bezeichnet und heit *Restklassenring* modulo m.

1.2.9 Definition

Seien $a, b \in \mathbb{Z}$ und sei $m \in \mathbb{N}$ sowie $n \in \mathbb{N}_0$. Dann definiert man die *Summe*, die *Negation*, die *Differenz*, das *Produkt* und die *Potenz* von Restklassen durch

$$\begin{aligned}
[a]_m + [b]_m &= [a + b]_m, \\
-[a]_m &= [-a]_m, \\
[a]_m - [b]_m &= [a - b]_m, \\
[a]_m \cdot [b]_m &= [a \cdot b]_m, \\
[a]_m^n &= [a^n]_m.
\end{aligned}$$

1.2.12 Definition: Inverses, prime Restklassengruppe

Sei $a \in \mathbb{Z}$ und $m \in \mathbb{N}$. Gibt es $b \in \mathbb{Z}$ mit $[a]_m \cdot [b]_m = [1]_m$, so heißt $[a]_m$ *invertierbar*, und $[b]_m$ wird *Inverses* von $[a]_m$ genannt und mit $[a]_m^{-1}$ bezeichnet. Man sagt dann auch, dass b ein Inverses von a modulo m ist. Die Menge aller invertierbaren Restklassen aus $\mathbb{Z}_m$ wird mit $\mathbb{Z}_m^*$ bezeichnet und heißt *prime Restklassengruppe*.

1.2.17 Definition

- *Alphabet* Σ*:* nichtleere Menge
- *Wort der Länge* n *über* Σ*:* n-Tupel $(s_1, \ldots, s_n)$ mit $s_1, \ldots, s_n \in \Sigma$. Kurz: $s_1, \ldots, s_n$
- *Länge eines Wortes* w*:* $|w|$
- *Menge der Worte der Länge* n *über* Σ*:* Σ^n
- $a \ldots a \in \Sigma^n$: a^n
- *leeres Wort ist einziges Wort der Länge 0. Schreibe auch* ε*.*
- *Menge aller nichtleeren Wörter:* $\Sigma^+ = \bigcup_{n \in \mathbb{N}} \Sigma^n$
- *Menge aller Wörter:* $\Sigma^{0+} = \bigcup_{n \in \mathbb{N}_0} \Sigma^n$
- *Verkettung:*
  $((s_1, \ldots, s_n), (t_1, \ldots, t_m)) \mapsto (s_1, \ldots, s_n)(t_1, \ldots, t_m) = s_1 \ldots s_n t_1 \ldots t_m)$

1.3 Perfekte Sicherheit

1.3.3 Definition: Wahrscheinlichkeitsverteilung, Gleichverteilung

Gilt
$P(X \in \Omega_2) = 1$ und $P(X \in A \cup B) = P(X \in A) + P(X \in B)$ für alle disjunkten $A, B \subseteq \Omega_2$, so heißt P^X *Wahrscheinlichkeitsverteilung der Zufallsvariable* X. Ist $P^X(\{a\}) = \frac{1}{|\Omega_2|}$ für alle $a \in \Omega_2$, so heißt P^X *Gleichverteilung* auf Ω_2.

1.3.4 Definition: Identische Verteilung, Stochastische Unabhängigkeit

Sei
Ω_3 eine endliche Menge und $Y : \Omega_1 \to \Omega_3$ eine Zufallsvariable mit Wahrscheinlichkeitsverteilung P^Y. Gilt $\Omega_3 = \Omega_2$ und $P^X = P^Y$, also $P(X \in A) = P(Y \in A)$ für alle $A \subseteq \Omega_2$ (oder äquivalent $P(X = a) = P(Y = a)$ für alle $a \; in \Omega_2$), so heißen X und Y *identisch verteilt.* Gilt $P(X \in A, Y \in B) = P(X \in A) \cdot P(Y \in B)$ für alle $A \subseteq \Omega_2$ und $B \subseteq \Omega_3$ (oder äquivalent $P(X = a, Y = b) = P(X = a) \cdot P(Y = b)$ für alle $a \in \Omega_2$ und $b \in \Omega_3$), so heißen X und Y *stochastisch unabhängig.*

1.3.5 Definition: Bedingte Wahrscheinlichkeit

Seien X und Y Zufallsvariablen mit demselben Definitionsbereich und Wahrscheinlichkeitsverteilungen P^X und P^Y. Weiter seien A und B Teilmengen des Zielbereichs von X beziehungsweise Y, wobei $P(Y \in B) > 0$ gelte. Dann definiert man die *bedingte Wahrscheinlichkeit* von $X \in A$ unter $Y \in B$ durch

$$P(X \in A | Y \in B) = \frac{P(X \in A, Y \in B)}{P(Y \in B)}.$$

Analog werden auch Schreibweisen wie $P(X = a|Y = b)$ definiert.

1.3.7 Definition: Erwartungswert

Sei X eine Zufallsvariable mit Wertemenge
$\{x_1, \ldots, x_m\} \subseteq \mathbb{R}$ und Wahrscheinlichkeitsverteilung P^X. Dann definiert man den *Erwartungswert* von X durch

$$E(X) = \sum_{i=1}^{m} x_i P(X = x_i).$$

Betrachtet man zwei Zufallsexperimente mit drei möglichen Ausgängen, wobei die Wahrscheinlichkeiten für die einzelnen Ausgänge im einen Fall $\frac{9}{10}$, $\frac{1}{20}$ sowie $\frac{1}{20}$ und im anderen Fall jeweils $\frac{1}{3}$ sind, so hat man die Vorstellung, daß der Ausgang des zweiten Experiments unbestimmter ist als der des ersten Experiments. Diese Unbestimmtheit soll nun quantitativ gefaßt werden.

1.3.8 Definition: (Gemeinsame) Entropie

Sei $C \in \mathbb{R}$ mit $C > 1$ und X eine Zufallsvariable mit Wertemenge $\{x_1, \ldots, x_m\}$. Dann heißt

$$H_C^P(X) = -\sum_{i=1}^{m} P(X = x_i) \log_C P(X = x_i),$$

wobei man $0 \cdot \log_c 0 = 0$ setzt, *Entropie* von X (zur Basis C). Ist zusätzlich Y eine Zufallsvariable mit Wertemenge $\{y_1, \ldots, y_n\}$, so definiert man

$$H_C^P(X, Y) = -\sum_{\substack{i \in \{1,\ldots,m\} \\ j \in \{1,\ldots,n\}}} P(X = x_i, Y = y_j) \log_C P(X = x_i, Y = y_j),$$

die *gemeinsame Entropie* von X und Y. Hier und bei den folgenden Bezeichnungen wird die Basis C gelegentlich weggelassen, wenn die Aussage unabhängig von der gewählten Basis gilt. (Treten in einer Aussage dabei mehrere solche Bezeichnungen auf, muss aber überall dieselbe Basis verwendet werden.) Das P kann in den Bezeichnungen ebenfalls entfallen, wenn die Abhängigkeit von P nicht betont wird.

1.3.11 Definition: Bedingte Entropie, Transinformation

Bezeichnungen wie bei Entropie. Dann definiert man

$$\begin{aligned} H_C(X|Y) &= -\sum_{j=1}^{n} P(Y = y_j) \sum_{i=1}^{m} P(X = x_i|Y = y_j) \log_C P(X = x_i|Y = y_j) \\ &= -\sum_{\substack{i \in \{1,\ldots,m\} \\ j \in \{1,\ldots,n\}}} P(X = x_i, Y = y_j) \log_C P(X = x_i|Y = y_j), \end{aligned}$$

die *bedingte Entropie* von X unter Y. Weiter definiert man $I_C(X, Y) = H_C(X) - H_C(X|Y)$, die *Transinformation* von X und Y.

1.3.17 Definition: Schlüsselaquivokation, Klartextäquivokation

Die Entropie $H(K|C)$ heißt *Schlüsselaquivokation*, und $H(M|C)$ heißt *Klartextäquivokation*.

1.4 Blockchiffren

2 Asymmetrische Kryptographie

2.1 RSA-Verschlüsselung

2.2 ElGamal-Verschlüsselung

2.3 Elliptische Kurven in der Kryptogaphie

2.4 Kryptographische Hashfunktionen

2.5 Kryptographische Protokolle

3 Quellenkodierung

3.1 Eindeutig dekodierbare Kodes

3.2 Diskrete gedächtnislose Quellen

3.3 Konstruktion von Kodes

4 Kanalkodierung

4.1 Kanäle

4.2 Parameter fehlerkorrigierender Kodes

4.3 Lineare Kodes

4.4 Zyklische Kodes

4.5 Dualität