III. Perfekte Geheimhaltung

- perfekte Geheimhaltung als Formalisierung absolut sicherer Verschlüsselungsverfahren
- eingeführt von Claude Shannon 1949
- C.Shannon zeigte auch Existenz von Verfahren mit perfekter Geheimhaltung
- perfekt geheime Verschlüsselungsverfahren müssen ineffizient sein
- perfekte Geheimhaltung garantiert nur Sicherheit gegen passive Angriffe

III.1 Diskrete Wahrscheinlichkeiten

Definition 3.1 Sei S eine endliche Menge. Eine Wahrscheinlichkeitsverteilung Pr auf S ist eine Abbildung $\Pr : P(S) \to \mathbb{R}$, die die folgenden drei Eigenschaften besitzt

1. $\Pr(A) \geq 0$ für alle $A \subseteq S$,
2. $\Pr(S) = 1$,
3. $\Pr(A \cup B) = \Pr(A) + \Pr(B)$ für alle A,B mit $A \cap B = \emptyset$.

$A \subseteq S$ heißt Ereignis.

$a \in S$ heißt Elementarereignis, $\Pr(a) = \Pr(\{a\})$.

Wahrscheinlichkeiten - Eigenschaften

1. $\Pr(\varnothing) = 0$;
2. $\Pr(A) \leq \Pr(B)$ für $A \subseteq B$;
3. $0 \leq \Pr(A) \leq 1$ für alle $A \subseteq S$;
4. $\Pr(S \setminus A) = 1 - \Pr(A)$;
5. $\Pr\left(\bigcup_{i=1}^{m} A_i\right) = \sum_{i=1}^{m} \Pr(A_i)$ für $A_i \subseteq S$ mit $A_i \cap A_j = \varnothing$

   für alle $i,j, i \neq j$.

Bedingte Wahrscheinlichkeiten

Definition 3.2 A,B seien Ereignisse mit $\Pr(B) > 0$. Die Wahrscheinlichkeit "A unter der Bedingung B" ist definiert als

$$\Pr(A \mid B) = \frac{\Pr(A \cap B)}{\Pr(B)}.$$

Definition 3.3 Zwei Ereignisse A,B heißen unabhängig, falls $\Pr(A \cap B) = \Pr(A) \cdot \Pr(B)$.

Äquivalent $\Pr(A \mid B) = \Pr(A)$. (Übung)

Satz von Bayes

Satz 3.4 Sind A,B Ereignisse mit $\Pr(A), \Pr(B) > 0$, so gilt

$$\Pr(B) \cdot \Pr(A \mid B) = \Pr(A) \cdot \Pr(B \mid A).$$

Satz 3.5 Seien A ein Ereignis und $B_1, \ldots, B_n$ eine disjunkte Zerlegung von S. Dann gilt

$$\Pr(A) = \sum_{i=1}^{n} \Pr(A \mid B_i) \cdot \Pr(B_i).$$

III.2 Perfekte Geheimhaltung

Szenario

- Alice und Bob benutzen Verfahren (P,C,K,E,D).
- Eve kann nur eine Nachricht abfangen und lesen (Ciphertext-Only Angriff).
- Schlüsselpaare (e,d) von der Form (k,k).

- Verteilung Pr_P auf Klartexten.
- Verteilung Pr_K auf Schlüsseln, d.h. Alice wählt Schlüssel k gemäß Verteilung Pr_K.
- Verteilung Pr auf $S = P \times K$ durch

$$Pr(p,k) = Pr_P(p) \cdot Pr_K(k),$$

d.h. Verteilungen auf P und K sind unabhängig.

Perfekte Geheimhaltung - Ereignisse

$p \in P$, Ereignis p $\quad \{(p,k) : k \in K\}$

$k \in K$, Ereignis k $\quad \{(p,k) : p \in P\}$

$c \in C$, Ereignis c $\quad \{(p,k) : E_k(p) = c\}$

$$
\begin{aligned}
Pr(p) &= \sum_{k \in K} Pr(p,k) \\
&= \sum_{k \in K} Pr_P(p) \cdot Pr_K(k) \\
&= Pr_P(p) \cdot \sum_{k \in K} Pr_K(k) \\
&= Pr_P(p)
\end{aligned}
$$

Perfekte Geheimhaltung - Ereignisse

$p \in P$, Ereignis p $\quad \{(p,k) : k \in K\}$

$k \in K$, Ereignis k $\quad \{(p,k) : p \in P\}$

$c \in C$, Ereignis c $\quad \{(p,k) : E_k(p) = c\}$

$$
\begin{aligned}
Pr(k) &= \sum_{p \in P} Pr(p,k) \\
&= \sum_{p \in P} Pr_P(p) \cdot Pr_K(k) \\
&= Pr_K(k) \cdot \sum_{p \in P} Pr_P(p) \\
&= Pr_K(k)
\end{aligned}
$$

Perfekte Geheimhaltung - Ereignisse

$p \in P$, Ereignis p $\{(p,k) : k \in K\}$

$k \in K$, Ereignis k $\{(p,k) : p \in P\}$

$c \in C$, Ereignis c $\{(p,k) : E_k(p) = c\}$

$$\Pr(c) = \sum_{\{(p,k):E_k(p)=c\}} \Pr(p,k)$$

$$= \sum_{\{(p,k):E_k(p)=c\}} \Pr_P(p) \cdot \Pr_K(k)$$

Ereignisse - Beispiel

$P = \{0,1\}; C = \{a,b\}; K = \{X,Y\}$

E	0	1
X	a	b
Y	b	a

$Pr_P(0) = 1/4, \quad Pr_P(1) = 3/4.$

$Pr_K(X) = 3/8, \quad Pr_K(Y) = 5/8.$

$Pr(a) = 9/16, \quad Pr(b) = 7/16.$

Perfekte Geheimhaltung - Definition

Idee Eve darf aus dem Chiffretext c nichts Neues über den Klartext p lernen.

Definition 3.6 Ein Verschlüsselungsverfahren (P,C,K,E,D) mit Verteilungen Pr_P und Pr_K heißt perfekt geheim, wenn für alle $p \in P$ und alle $c \in C$ gilt

$$Pr(p \mid c) = Pr(p).$$

$$\begin{aligned} Pr(p|c) &= Pr((p,c)) / Pr(c) \\ &= \sum_{\{k:E_k(p)=c\}} Pr_P(p) \cdot Pr_K(k) \Big/ Pr(c) \end{aligned}$$

Ereignisse - Beispiel

$P = \{0,1\}; C = \{a,b\}; K = \{X,Y\}$

E	0	1
X	a	b
Y	b	a

$Pr_P(0) = 1/4, \quad Pr_P(1) = 3/4.$

$Pr_K(X) = 3/8, \quad Pr_K(Y) = 5/8.$

$Pr(a) = 9/16, \quad Pr(b) = 7/16.$

$Pr(0|a) = 3/18, \quad Pr(1|a) = 15/18.$

$Pr(0|b) = 5/14 \quad Pr(1|b) = 9/14$

Verfahren ist nicht perfekt geheim!

Perfekte Geheimhaltung – Satz von Shannon

Satz 3.7 Sei (P,C,K,E,D) ein Verschlüsselungsverfahren mit $|P| = |C| = |K| < \infty$ und mit Verteilungen Pr_P und Pr_K. Ferner gelte $Pr_P(p) > 0$ für alle $p \in P$. Das Verschlüsselungsverfahren ist genau dann perfekt geheim, wenn gilt

1. Pr_K ist die Gleichverteilung;
2. Für jeden Klartext p und jeden Chiffetext c existiert genau ein Schlüssel k mit $E_k(p) = c$.

Beobachtung Bis auf die Bedingung $Pr_P(p) > 0$ ist diese Charakterisierung unabhängig von Pr_P.

Perfekte Geheimhaltung - Ereignisse

$p \in P$, Ereignis p $\quad \{(p,k) : k \in K\}$

$k \in K$, Ereignis k $\quad \{(p,k) : p \in P\}$

$c \in C$, Ereignis c $\quad \{(p,k) : E_k(p) = c\}$

$$\Pr(c) = \sum_{\{(p,k):E_k(p)=c\}} \Pr(p,k)$$

$$= \sum_{\{(p,k):E_k(p)=c\}} \Pr_P(p) \cdot \Pr_K(k)$$

Perfekte Geheimhaltung – One-time-pad

Beispiel Wird beim One-time-pad die Gleichverteilung auf den Schlüsseln aus $\{0,1\}^n$ verwendet, so ist das One-time-pad perfekt geheim, solange $Pr_P(p) > 0$ für alle $p \in P$ gilt.

OTP: $P = C = K = \{0,1\}^n$

$E_k(p) = p \oplus k$

Zusammenfassung

- Es existieren perfekt sichere Kryptosysteme, bei denen ein Angreifer aus dem Chiffretext c nichts über die Nachricht p lernt (Beispiel: One-time-pad)

- Wegen der notwendigen Bedingung $|K| \geq |P|$ sind perfekt sichere Kryptosysteme stets ineffizient

- Perfekt sichere Kryptosysteme nur sicher gegen passive Angreifer (Ciphertext-only), vgl. One-time-pad