

# Ununterscheidbarkeit von Chiffretexten

## Spiel Ununterscheidbarkeit von Chiffretexten $\text{PrivK}_{\mathcal{A},\Pi}^{\text{eav}}(n)$

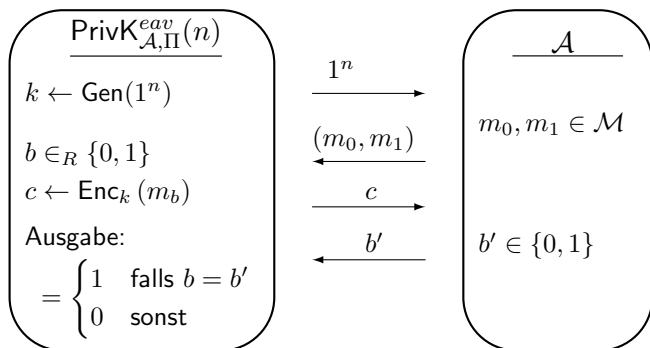
Sei  $\Pi$  ein Verschlüsselungsverfahren und  $\mathcal{A}$  ein Angreifer.

- 1  $(m_0, m_1) \leftarrow \mathcal{A}$ .
- 2  $k \leftarrow \text{Gen}(1^n)$ .
- 3 Wähle  $b \in_R \{0, 1\}$ .  $b' \leftarrow \mathcal{A}(\text{Enc}_k(m_b))$ .
- 4  $\text{PrivK}_{\mathcal{A},\Pi}^{\text{eav}}(n) = \begin{cases} 1 & \text{für } b = b' \\ 0 & \text{sonst} \end{cases}$ .

### Anmerkungen:

- $\mathcal{A}$  wählt die zu verschlüsselnden Nachrichten  $m_0, m_1$  selbst.
- $\mathcal{A}$  gewinnt das Spiel, d.h.  $b = b'$ , durch Raten von  $b'$  mit Ws  $\frac{1}{2}$ .
- Wir bezeichnen  $\text{Ws}[\text{PrivK}_{\mathcal{A},\Pi}^{\text{eav}}(n) = 1] - \frac{1}{2}$  als Vorteil von  $\mathcal{A}$ .

# Ununterscheidbarkeit von Chiffretexten



# Raten ist optimal

## Satz Perfekte Sicherheit und $\text{PrivK}_{\mathcal{A},\Pi}^{\text{eav}}$

Ein Verschlüsselungsverfahren  $\Pi$  ist perfekt sicher gdw für alle Angreifer  $\mathcal{A}$  gilt  $\text{Ws}[\text{PrivK}_{\mathcal{A},\Pi}^{\text{eav}}(n) = 1] = \frac{1}{2}$ .

### Beweis:

- " $\Leftarrow$ ": Sei  $\Pi$  nicht perfekt sicher. Dann existieren  $m_0, m_1 \in \mathcal{M}$  und  $c \in \mathcal{C}$  mit  $\text{Ws}[C = c \mid M = m_0] \neq \text{Ws}[C = c \mid M = m_1]$ .
- OBdA  $\text{Ws}[C = c \mid M = m_0] > \text{Ws}[C = c \mid M = m_1]$ .
- Wir definieren den folgenden Angreifer  $\mathcal{A}$  für das Spiel  $\text{PrivK}_{\mathcal{A},\Pi}^{\text{eav}}$ .

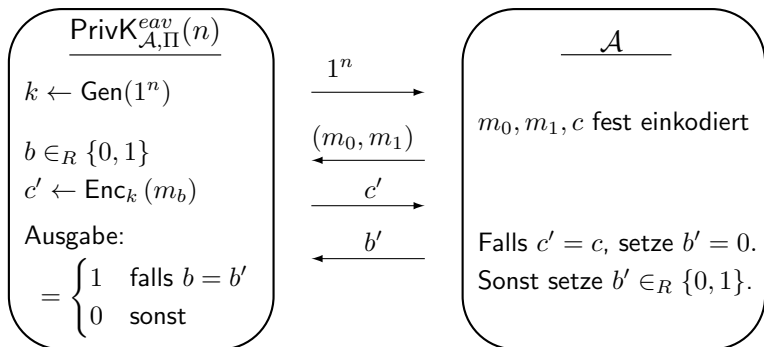
# Algorithmus Angreifer $\mathcal{A}$

## Algorithmus Angreifer $\mathcal{A}$

EINGABE:  $m_0, m_1, c$

- 1 Versende Nachrichten  $m_0, m_1$ . Erhalte  $c' \leftarrow \text{Enc}_k(m_b)$ .
- 2 Falls  $c' = c$ , setze  $b' = 0$ . Sonst setze  $b' \in_R \{0, 1\}$ .

AUSGABE:  $b'$



# Nicht perfekt sicher $\Rightarrow$ Vorteil

## Beweis (Fortsetzung):

- Es gilt  $\text{Ws}[\text{PrivK}_{\mathcal{A},\Pi}^{\text{eav}} = 1] = \text{Ws}[\mathcal{A}(\text{Enc}(m_b)) = b]$ 
$$= \frac{1}{2} \cdot \text{Ws}[C \neq c] + \text{Ws}[M = m_0 \mid C = c] \cdot \text{Ws}[C = c]$$
$$= \frac{1}{2}(1 - \text{Ws}[C = c]) + \text{Ws}[M = m_0 \mid C = c] \cdot \text{Ws}[C = c].$$
- Falls  $\text{Ws}[M = m_0 \mid C = c] > \frac{1}{2}$ , so folgt  $\text{Ws}[\text{PrivK}_{\mathcal{A},\Pi}^{\text{eav}} = 1] > \frac{1}{2}$ .

- Es gilt  $\text{Ws}[M = m_0 \mid C = c]$ 
$$= \frac{\text{Ws}[C = c \mid M = m_0] \cdot \overbrace{\text{Ws}[M = m_0]}^{\frac{1}{2}}}{\sum_{i=0}^1 \text{Ws}[C = c \mid M = m_i] \cdot \underbrace{\text{Ws}[M = m_i]}_{\frac{1}{2}}}$$
$$= \frac{\text{Ws}[C = c \mid M = m_0]^{\frac{1}{2}}}{\underbrace{\text{Ws}[C = c \mid M = m_0] + \text{Ws}[C = c \mid M = m_1]}_{< 2 \cdot \text{Ws}[C=c \mid M=m_0]}} > \frac{1}{2}.$$

## Perfekt sicher $\Rightarrow$ kein Vorteil

**Beweis (Fortsetzung):** Perfekt sicher  $\Rightarrow \text{Ws}[PrivK_{\mathcal{A}, \Pi}^{eav} = 1] = \frac{1}{2}$

- Sei  $\Pi$  perfekt sicher. Dann gilt für alle  $m_0, m_1 \in \mathcal{M}$ ,  $c \in \mathcal{C}$   
 $\text{Ws}[C = c \mid M = m_0] = \text{Ws}[C = c] = \text{Ws}[C = c \mid M = m_1]$ .
- D.h. es gilt  $\{c \mid c \in \text{Enc}_k(m)\} = \mathcal{C}$  für alle  $m \in \mathcal{M}$ .
- Daraus folgt  $\text{Ws}[PrivK_{\mathcal{A}, \Pi}^{eav} = 1] = \text{Ws}[\mathcal{A}(\text{Enc}(m_b)) = b]$

$$= \text{Ws}[b = 0] \cdot \text{Ws}[\mathcal{A}(\text{Enc}(m_0)) = 0] + \text{Ws}[b = 1] \cdot \text{Ws}[\mathcal{A}(\text{Enc}(m_1)) = 1]$$

$$= \frac{1}{2} \cdot \left( \sum_{c \in \text{Enc}(m_0)} \text{Ws}[\mathcal{A}(c) = 0 \mid C = c] \cdot \text{Ws}[C = c] \right.$$

$$\left. + \sum_{c \in \text{Enc}(m_1)} \underbrace{\text{Ws}[\mathcal{A}(c) = 1 \mid C = c]}_{1 - \text{Ws}[\mathcal{A}(c) = 0 \mid C = c]} \cdot \text{Ws}[C = c] \right)$$

$$= \frac{1}{2} \cdot \sum_{c \in \mathcal{C}} \text{Ws}[C = c] = \frac{1}{2}.$$

# Computational Security

## Perfekte Sicherheit:

- Liefert Sicherheit im informationstheoretischen Sinn, d.h. der Angreifer erhält nicht genügend Information, um zu entschlüsseln.
- Benötigen Schlüssel der Länge aller zu verschlüsselnden Nachrichten. Dies ist unpraktikabel in der Praxis.

## Computational Security Ansatz:

- Wir verwenden kurze Schlüssel (z.B. 128 Bit).
- Liefert Sicherheit nur gegenüber ppt Angreifern.
- Unbeschränkte Angreifer können bei KPA-Angriff  $\mathcal{K}$  durchsuchen.
- Seien  $(m_1, c_1), \dots, (m_n, c_n)$  die Plaintext/Chiffretext Paare.
- Mit hoher Ws existiert eindeutiges  $k$  mit  $m_i = Dec_k(c_i), i \in [n]$ .
- Mit obigem KPA-Angriff kann der Angreifer in Polynomial-Zeit auch ein einzelnes  $k \in \mathcal{K}$  raten, dieses ist korrekt mit Ws  $\frac{1}{|\mathcal{K}|}$ .
- D.h. ppt Angreifer besitzen nur vernachlässigbare Erfolgsws im Sicherheitsparameter.

# Vernachlässigbare Wahrscheinlichkeit

## Definition Vernachlässigbare Wahrscheinlichkeit

Eine Funktion  $f : \mathbb{N} \rightarrow \mathbb{R}$  heißt *vernachlässigbar*, falls für jedes Polynom  $p$  ein  $N \in \mathbb{N}$  existiert, so dass für alle  $n \geq N$  gilt  $f(n) < \frac{1}{p(n)}$ .  
Notation:  $f(n) = \text{negl}(n)$ .

## Bsp:

- Vernachlässigbare Funktionen:  $\frac{1}{2^n}$ ,  $\frac{1}{2^{\sqrt{n}}}$ ,  $\frac{1}{2^{\log^2 n}}$ ,  $\frac{1}{n^{\frac{\log n}{\log \log n}}}$ .
- Nicht vernachlässigbare Funktionen:  $\frac{1}{n^2}$ ,  $\frac{1}{\log n}$ ,  $\frac{1}{2^{\mathcal{O}(\log n)}}$ .

## Korollar Komposition vernachlässigbarer Funktionen

Seien  $f_1, f_2$  vernachlässigbare Funktionen. Dann ist

- 1  $f_1 + f_2$  vernachlässigbar.
- 2  $q(n) \cdot f_1$  vernachlässigbar für jedes Polynom  $q$ .



# Sicherheitsbeweis per Reduktion

**Annahme:** Problem  $X$  lässt sich in ppt nur mit Ws  $\text{negl}(n)$  lösen.

- Sei  $\Pi$  ein Krypto-Verfahren mit Sicherheitsparameter  $n$ .
- Sei  $\mathcal{A}$  ein ppt Angreifer auf  $\Pi$  mit Erfolgsws  $\epsilon(n)$ .
- Wir konstruieren eine polynomielle Reduktion  $\mathcal{A}'$  für  $X \leq_p \mathcal{A}$ .  
(Erinnerung: Diskrete Mathematik II)

## Algorithmus Reduktion $\mathcal{A}'$ für $X \leq_p \mathcal{A}$

EINGABE: Instanz  $x$  des Problems  $X$

- 1 Konstruieren aus  $x$  Instanz von  $\Pi$ , senden diese an  $\mathcal{A}$ .
- 2 Sofern  $\mathcal{A}$ s Angriff eine Interaktion erfordert (z.B. bei CCA), wird diese von der Reduktion  $\mathcal{A}'$  simuliert.  $\mathcal{A}$ s Sicht soll dabei identisch zu einem realen Angriff sein.
- 3  $\mathcal{A}$  bricht schließlich  $\Pi$  mittels Ausgabe  $y'$  mit Ws  $\epsilon(n)$ .
- 4 Verwenden  $y'$ , um eine Lösung  $y$  für die Instanz  $x$  zu berechnen.

AUSGABE: Lösung  $y$  für  $x$

# Sicherheitsbeweis per Reduktion

- Alle Schritte der Reduktion laufen in polynomial-Zeit.
- Angenommen Schritt 4 besitze Erfolgsws  $\frac{1}{p(n)}$  für ein Polynom  $p(n)$ .
- Dann besitzt die Reduktion insgesamt Erfolgsws  $\frac{\epsilon(n)}{p(n)}$ .
- Nach Annahme lässt sich  $X$  nur mit Ws  $\text{negl}(n)$  lösen.
- D.h.  $\frac{\epsilon(n)}{p(n)} \leq \text{negl}(n)$ , und damit folgt  $\epsilon(n) \leq \text{negl}(n)$ .
- Damit besitzt **jeder** Angreifer  $\mathcal{A}$  vernachlässigbare Erfolgsws.

# Reduktionsbeweis bildlich

