# CPA Spiel

**Szenario:** Wir betrachten aktive Angriffe.

- D.h. $\mathcal{A}$ darf sich Nachrichten nach Wahl verschlüsseln lassen.
- $\mathcal{A}$ erhält dazu Zugriff auf ein Verschlüsselungsorakel $Enc_k(\cdot)$.
- Notation für die Fähigkeit des Orakelzugriffs: $\mathcal{A}^{Enc_k(\cdot)}$.

## **Spiel** CPA Ununterscheidbarkeit von Chiffretexten $PrivK^{cpa}_{\mathcal{A},\Pi}(n)$

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

1. $k \leftarrow Gen(1^n)$.
2. $(m_0, m_1) \leftarrow \mathcal{A}^{Enc_k(\cdot)}(1^n)$, d.h. $\mathcal{A}$ darf $Enc_k(m)$ für beliebige $m$ anfragen.
3. Wähle $b \in_R \{0,1\}$ und verschlüssele $c \leftarrow Enc_k(m_b)$.
4. $b' \leftarrow \mathcal{A}^{Enc_k(\cdot)}(c)$, d.h. $\mathcal{A}$ darf $Enc_k(m)$ für beliebige $m$ anfragen.
5. $PrivK^{eav}_{\mathcal{A},\Pi}(n) = \begin{cases} 1 & \text{für } b = b' \\ 0 & \text{sonst} \end{cases}$.

# CPA Sicherheit

## **Definition** CPA Sicherheit

Ein Verschlüsselungsschema $\Pi = (\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ besitzt *ununterscheidbare Chiffretexte gegenüber CPA* falls für alle ppt $\mathcal{A}$:

$$\mathrm{Ws}[\mathit{PrivK}^{\mathit{cpa}}_{\mathcal{A},\Pi}(n) = 1] \leq \tfrac{1}{2} + \mathrm{negl}(n).$$

Der Wsraum ist definiert über die Münzwürfe von $\mathcal{A}$ und $\mathit{PrivK}^{\mathit{cpa}}_{\mathcal{A},\Pi}$.

Notation: Wir bezeichnen $\Pi$ als *CPA sicher*.

# CPA-Unsicherheit deterministischer Verschlüsselung

## **Satz** Unsicherheit deterministischer Verschlüsselung

Sei $\Pi = (Gen, Enc, Dec)$ ein Verschlüsselungsschema mit deterministischem $Enc$. Dann ist $\Pi$ **nicht** CPA-sicher.

**Beweis:** Konstruieren folgenden CPA Angreifer $\mathcal{A}$.

## **Algorithmus** CPA Angreifer $\mathcal{A}$

EINGABE: $1^n$

1. Sende $(m_0, m_1)$ für beliebige verschiedene $m_0, m_1 \in \mathcal{M}$.
2. Erhalte $c := Enc_k(m_b)$ für $b \in_R \{0, 1\}$.
3. Stelle Orakelanfrage $c_0 := Enc_k(m_0)$.

AUSGABE: $b' = \begin{cases} 0 & \text{falls } c = c' \\ 1 & \text{sonst} \end{cases}$.

- Es gilt $\mathrm{Ws}[PrivK^{cpa}_{\mathcal{A},\Pi}(n) = 1] = 1$.

# Mult-CPA Spiel

Wie CPA-Spiel, nur dass mehrfache Verschlüsselungen erlaubt sind.

## **Spiel** Mehrfache Verschlüsselung $PrivK^{mult-cpa}_{\mathcal{A},\Pi}(n)$

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

1. $(M_0, M_1) \leftarrow \mathcal{A}^{Enc_k(\cdot)}(1^n)$ mit $M_0 = (m_0^1, \ldots, m_0^t)$, $M_1 = (m_1^1, \ldots, m_1^t)$ und $|m_0^i| = |m_1^i|$ für alle $i \in [t]$.
2. $k \leftarrow Gen(1^n)$.
3. Wähle $b \in_R \{0,1\}$. $b' \leftarrow \mathcal{A}^{Enc_k(\cdot)}((Enc_k(m_b^1), \ldots, Enc_k(m_b^t))$.
4. $PrivK^{mult}_{\mathcal{A},\Pi}(n) = \begin{cases} 1 & \text{für } b = b' \\ 0 & \text{sonst} \end{cases}$.

## **Definition** Mult-CPA Sicherheit

$\Pi$ heißt *mult-CPA* sicher, falls für alle ppt $\mathcal{A}$ gilt

$$\mathrm{Ws}[PrivK^{mult-cpa}_{\mathcal{A},\Pi}(n) = 1] \leq \tfrac{1}{2} + \mathrm{negl}(n).$$

# CPA-Sicherheit mehrfacher Verschlüsselung

**Satz** CPA-Sicherheit mehrfacher Verschlüsselung

Sei $\Pi$ ein Verschlüsselungsschema. Dann ist $\Pi$ CPA-sicher gdw $\Pi$ mult-CPA sicher ist.

**Beweis** "$\Rightarrow$": Für $t = 2$. Rückrichtung ist trivial.

- Ein Angreifer $\mathcal{A}$ gewinnt das Spiel $PrivK^{mult-cpa}_{\mathcal{A},\Pi}(n)$ mit Ws

$$\frac{1}{2}\mathrm{Ws}[\mathcal{A}(Enc_k(m_0^1), Enc_k(m_0^2)) = 0] + \frac{1}{2}\mathrm{Ws}[\mathcal{A}(Enc_k(m_1^1), Enc_k(m_1^2)) = 1].$$

- Daraus folgt $\mathrm{Ws}[PrivK^{mult-cpa}_{\mathcal{A},\Pi}(n)] + \frac{1}{2} =$

$$\frac{1}{2}\mathrm{Ws}[\mathcal{A}(Enc_k(m_0^1), Enc_k(m_0^2)) = 0] + \frac{1}{2}\mathrm{Ws}[\mathcal{A}(Enc_k(m_1^1), Enc_k(m_1^2)) = 1]$$
$$+ \quad \frac{1}{2}\left(\mathrm{Ws}[\mathcal{A}(Enc_k(m_0^1), Enc_k(m_1^2)) = 0] + \mathrm{Ws}[\mathcal{A}(Enc_k(m_0^1), Enc_k(m_1^2)) = 1]\right)$$

- **Ziel:** Zeigen, dass $\mathrm{Ws}[PrivK^{mult-cpa}_{\mathcal{A},\Pi}(n)] + \frac{1}{2} \leq 1 + \mathrm{negl}(n)$.

# Betrachten der Hybride

## Lemma

$\frac{1}{2}\mathrm{Ws}[\mathcal{A}(Enc_k(m_0^1), Enc_k(m_0^2)) = 0] + \frac{1}{2}\mathrm{Ws}[\mathcal{A}(Enc_k(m_0^1), Enc_k(m_1^2)) = 1] \leq \frac{1}{2} + \mathrm{negl}(n)$.

**Beweis:** Sei $\mathcal{A}'$ Angreifer für *einfache* Verschlüsselungen.

- $\mathcal{A}'$ versucht mittels $\mathcal{A}$ das Spiel $PrivK^{cpa}_{\mathcal{A}',\Pi}(n)$ zu gewinnnen.

## **Strategie** von CPA Angreifer $\mathcal{A}'$

EINGABE: $1^n$ und Orakelzugriff $Enc_k(\cdot)$

1. $\mathcal{A}'$ gibt $1^n$ und Orakelzugriff $Enc_k(\cdot)$ an $\mathcal{A}$ weiter.
2. $(M_0, M_1) \leftarrow \mathcal{A}^{Enc_k(\cdot)}(1^n)$ mit $M_0 = (m_0^1, m_0^2)$ und $M_1 = (m_1^1, m_1^2)$.
3. $\mathcal{A}'$ gibt $(m_0^2, m_1^2)$ aus. $\mathcal{A}'$ erhält Chiffretext $c := Enc_k(m_b^2)$.
4. $b' \leftarrow \mathcal{A}(Enc_k(m_0^1), c(b))$.

AUSGABE: $b'$

- $\mathrm{Ws}[\mathcal{A}'(Enc_k(m_0^2)) = 0] = \mathrm{Ws}[\mathcal{A}((Enc_k(m_0^1), Enc_k(m_0^2)) = 0]$ und
- $\mathrm{Ws}[\mathcal{A}'(Enc_k(m_1^2)) = 1] = \mathrm{Ws}[\mathcal{A}((Enc_k(m_0^1), Enc_k(m_1^2)) = 1]$.

# Fortsetzung Hybridtechnik

**Beweis(Fortsetzung):**

- CPA Sicherheit von $\Pi$ bei einzelnen Nachrichten impliziert

$$\begin{aligned}
\frac{1}{2} + \mathrm{negl}(n) &\geq \mathrm{Ws}[PrivK^{cpa}_{\mathcal{A}',\Pi}(n) = 1] \\
&= \frac{1}{2}\mathrm{Ws}[\mathcal{A}'(Enc_k(m_0^2)) = 0] + \frac{1}{2}\mathrm{Ws}[\mathcal{A}'(Enc_k(m_1^2)) = 1] \\
&= \frac{1}{2}\mathrm{Ws}[\mathcal{A}((Enc_k(m_0^1), Enc_k(m_0^2)) = 0] + \\
&\quad \frac{1}{2}\mathrm{Ws}[\mathcal{A}((Enc_k(m_0^1), Enc_k(m_1^2)) = 1] \quad \square_{\text{Lemma}}
\end{aligned}$$

- Analog kann gezeigt werden, dass

$$\begin{aligned}
\frac{1}{2} + \mathrm{negl}(n) &\geq \frac{1}{2}\mathrm{Ws}[\mathcal{A}((Enc_k(m_0^1), Enc_k(m_1^2)) = 0] + \\
&\quad \frac{1}{2}\mathrm{Ws}[\mathcal{A}((Enc_k(m_1^1), Enc_k(m_1^2)) = 1]
\end{aligned}$$

- Daraus folgt $\mathrm{Ws}[PrivK^{mult}_{\mathcal{A},\Pi}(n)] + \frac{1}{2} \leq 1 + \mathrm{negl}(n)$. $\square_{\text{Satz für } t=2}$

# Von fester zu beliebiger Nachrichtenlänge

- Beweistechnik für allgemeines $t$: Definiere für $i \in [t]$ Hybride
$$C^{(i)} = (Enc_k(m_0^1), \ldots, Enc_k(m_0^i), Enc_k(m_1^{i+1}), \ldots, Enc_k(m_1^t)).$$
- $\mathrm{Ws}[PrivK^{mult-cpa}_{\mathcal{A},\Pi}(n) = 1] = \frac{1}{2} \cdot \mathrm{Ws}[\mathcal{A}(C^{(t)}) = 0] + \frac{1}{2} \cdot \mathrm{Ws}[\mathcal{A}(C^{(0)} = 1]$.
- $\mathcal{A}'$ unterscheidet $Enc_k(m_0^i)$ und $Enc_k(m_1^i)$ für zufälliges $i \in [t]$.
- Entspricht dem Unterscheiden von $C^{(i)}$ und $C^{(i-1)}$.
- Liefert $\Pr[PrivK^{mult-cpa}_{\mathcal{A},\Pi}(n)] \leq \frac{1}{2} + t \cdot \mathrm{negl}(n)$ $\square_{\text{Satz}}$.

**Von fester zu beliebiger Nachrichtenlänge**

- Sei $\Pi$ ein Verschlüsselungsverfahren mit Klartexten aus $\{0,1\}^n$.
- Splitte $m \in \{0,1\}^*$ in $m_1, \ldots m_t$ mit $m_i \in \{0,1\}^n$.
- Definiere $\Pi'$ vermöge $Enc'_k(m) = Enc_k(m_1) \ldots Enc_k(m_t)$.
- Aus vorigem Satz folgt: $\Pi'$ ist CPA-sicher, falls $\Pi$ CPA-sicher ist.

# Zufallsfunktionen

## **Definition** Echte Zufallsfunktionen:

Sei $Func_n = \{f \mid f : \{0,1\}^n \to \{0,1\}^n\}$. Wir bezeichnen $f \in_R Func_n$ als *echte Zufallsfunktion* auf $n$ Bits.

**Anmerkungen:**

- Können $f \in Func_n$ mittels vollständiger Wertetabelle beschreiben.
- Damit kann $f$ als Bitstring der Länge $n \cdot 2^n$ dargestellt werden: $n$ Bits pro $f(x)$ für alle $x \in \{0,1\}^n$.
- Es gibt $2^{n \cdot 2^n}$ Strings dieser Länge $n \cdot 2^n$, d.h. $|Func_n| = 2^{n \cdot 2^n}$.

## **Definition** längenerhaltende, schlüsselabhängige Funktion

Sei $F$ ein pt Algorithmus. $F$ heißt *längenerhaltende, schlüsselabhängige Funktion* falls $F$ eine Fkt. $\{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ berechnet. Notation: $F_k(x) := F(k,x)$, wobei $k$ der Schlüssel ist.

**Anmerkung:**

- Zur Übersichtlichkeit der Notation verwenden wir stets $m = n$.

# Pseudozufallsfunktion

## **Definition** Pseudozufallsfunktion

Sei $F$ ein längenerhaltende, schlüsselabhängige Funktion. Wir bezeichnen $F$ als *Pseudozufallsfunktion*, falls für alle ppt $D$ gilt

$$\left|\mathrm{Ws}[D^{F_k(\cdot)}(1^n) = 1] - \mathrm{Ws}[D^{f(\cdot)}(1^n) = 1]\right| \leq \mathrm{negl}(n),$$

wobei $k \in_R \{0,1\}^n$ und $f \in_R Func_n$.

**Anmerkungen:**

- Die Beschreibungslänge von $f$ ist $n2^n$ Bits, d.h. exponentiell in $n$.
- Daher erhält ein ppt $D$ nicht $f$, sondern Orakelzugriff auf $f$ und $F_k$.
- $D$ kann nur polynomiell viele Anfragen an sein Orakel stellen.
- Danach muss $D$ entscheiden, ob sein Orakel einer echten Zufallsfunktion oder einer Pseudozufallsfunktion entspricht.

# Existenz und Verschlüsselung mit Pseudozufallsfkt

**Fakt** Existenz von Pseudozufallsfunktionen

Pseudozufallsfunktionen existieren gdw Pseudozufallsgeneratoren existieren.

$\Rightarrow$: siehe Übung

**Algorithmus** Verschlüsselung $\Pi_B$

Sei $F$ eine längenerhaltende, schlüsselabhängige Funktion auf $n$ Bits. Wir definieren $\Pi_B = (Gen, Enc, Dec)$ für Nachrichten der Länge $n$.

1. **Gen:** Wähle $k \in_R \{0,1\}^n$.
2. **Enc:** Für $m \in \{0,1\}^n$ wähle $r \in_R \{0,1\}^n$ und berechne
$$c := (r, F_k(r) \oplus m).$$
3. **Dec:** Für $c = (c_1, c_2) \in \{0,1\}^n \times \{0,1\}^n$ berechne
$$m := F_k(c_1) \oplus c_2.$$

# Sicherheit von $\Pi_B$

**Satz** Sicherheit von $\Pi_B$

Sei $F$ eine Pseudozufallsfunktion. Dann ist $\Pi_B$ CPA-sicher.

**Intuition:**

- $F_k(r)$ ist nicht unterscheidbar von $n$-Bit Zufallsstring.
- D.h. in der zweiten Komponente ist die Verteilung ununterscheidbar von einem One-Time Pad.
- Vorsicht: Benötigen, dass $r$ niemals wiederverwendet wird.