

# 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 Verschlüsselungsortakel  $Enc_k(\cdot)$ .
- Notation für die Fähigkeit des Orakelzugriffs:  $\mathcal{A}^{Enc_k(\cdot)}$ .

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

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  $PrivK_{\mathcal{A},\Pi}^{cpa}(n) = \begin{cases} 1 & \text{für } b = b' \\ 0 & \text{sonst} \end{cases}$ .

# CPA Spiel

$\text{PrivK}_{\mathcal{A}, \Pi}^{\text{cpa}}(n)$

$k \leftarrow \text{Gen}(1^n)$

$c'_1 = \text{Enc}_k(m'_1)$

$c'_i = \text{Enc}_k(m'_i)$

$b \in_R \{0, 1\}$

$c = \text{Enc}_k(m_b)$

$c'_{i+1} = \text{Enc}_k(m'_{i+1})$

$c'_q = \text{Enc}_k(m'_q)$

Ausgabe:

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

$1^n$

$m'_1$

$c'_1$

$\vdots$

$m'_i$

$c'_i$

$(m_0, m_1)$

$c$

$m'_{i+1}$

$c'_{i+1}$

$\vdots$

$m'_q$

$c'_q$

$b'$

$\mathcal{A}$

$m'_1 \in \mathcal{M}$

$m'_i \in \mathcal{M}$

$m_0, m_1 \in \mathcal{M}$

mit  $|m_0| = |m_1|$

$m'_{i+1} \in \mathcal{M}$

$m'_q \in \mathcal{M}$

$b' \in \{0, 1\}$

## Definition CPA Sicherheit

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

$$\mathbb{W}_s[\text{PrivK}_{\mathcal{A}, \Pi}^{cpa}(n) = 1] \leq \frac{1}{2} + \text{negl}(n).$$

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

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

# CPA-Unsicherheit deterministischer Verschlüsselung

## Satz Unsicherheit deterministischer Verschlüsselung

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

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

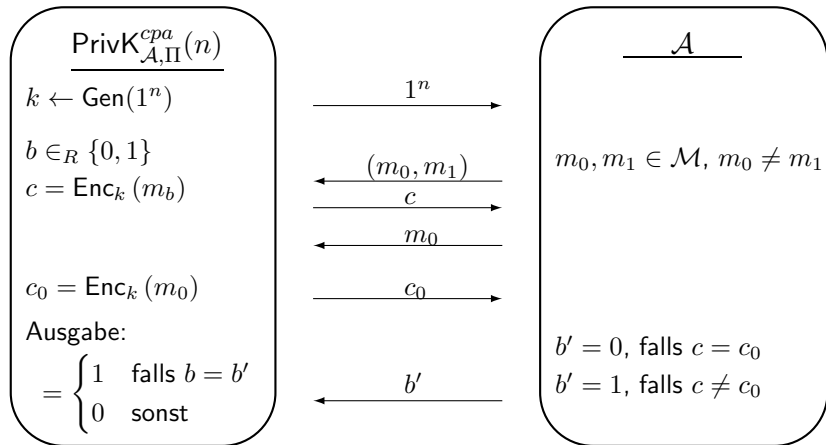
## Algorithmus CPA Angreifer $\mathcal{A}$

EINGABE:  $1^n$

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

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

# CPA Angreifer für deterministische Verschlüsselungen



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

# Multi-CPA Spiel

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

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

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

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

## Definition Multi-CPA Sicherheit

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

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

# Mult-CPA Spiel

$\text{PrivK}_{\mathcal{A}, \Pi}^{\text{mult-cpa}}(n)$

$k \leftarrow \text{Gen}(1^n)$

$c'_i = \text{Enc}_k(m'_i)$

$b \in_R \{0, 1\}$

$c^j = \text{Enc}_k(m_b^j)$

$C = (c^1, \dots, c^t)$

Ausgabe:

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

$\xrightarrow{1^n}$

$\xleftarrow{m'_i}$

$\xrightarrow{c'_i}$

$\xleftarrow{(M_0, M_1)}$

$\xrightarrow{C}$

$\xleftarrow{m'_i}$

$\xrightarrow{c'_i}$

$\xleftarrow{b'}$

Angreifer  $\mathcal{A}$

Wähle  $m'_i \in \mathcal{M}$

für  $i = 1, \dots, q$ .

Wähle  $M_0 = (m_0^1, \dots, m_0^t)$

und  $M_1 = (m_1^1, \dots, m_1^t)$

mit  $|m_0^j| = |m_1^j|$ .

$b' \in \{0, 1\}$

# 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.

- Sei  $\mathcal{A}$  ein Angreifer für  $\text{PrivK}_{\mathcal{A},\Pi}^{\text{mult-cpa}}(n)$ . Wir konstruieren einen Angreifer  $\mathcal{A}'$  für  $\text{PrivK}_{\mathcal{A}',\Pi}^{\text{cpa}}(n)$ .  $\mathcal{A}$  gewinnt mit  $W_s$

$$W_s[b = 0] \cdot W_s[\mathcal{A}(\text{Enc}_k(m_0^1), \text{Enc}_k(m_0^2)) = 0] + W_s[b = 1] \cdot W_s[\mathcal{A}(\text{Enc}_k(m_1^1), \text{Enc}_k(m_1^2)) = 1].$$

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

$$\begin{aligned} & \frac{1}{2} W_s[\mathcal{A}(\text{Enc}_k(m_0^1), \text{Enc}_k(m_0^2)) = 0] + \frac{1}{2} W_s[\mathcal{A}(\text{Enc}_k(m_1^1), \text{Enc}_k(m_1^2)) = 1] \\ & + \frac{1}{2} (W_s[\mathcal{A}(\text{Enc}_k(m_0^1), \text{Enc}_k(m_1^2)) = 0] + W_s[\mathcal{A}(\text{Enc}_k(m_0^1), \text{Enc}_k(m_1^2)) = 1]) \end{aligned}$$

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



# Betrachten der Hybride

## Lemma

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

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

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

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

EINGABE:  $1^n$  und Orakelzugriff  $\text{Enc}_k(\cdot)$

- 1  $\mathcal{A}'$  gibt  $1^n$  und Orakelzugriff  $\text{Enc}_k(\cdot)$  an  $\mathcal{A}$  weiter.
- 2  $(M_0, M_1) \leftarrow \mathcal{A}^{\text{Enc}_k(\cdot)}(1^n)$  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  $c := \text{Enc}_k(m_b^2)$ .
- 4  $b' \leftarrow \mathcal{A}(\text{Enc}_k(m_0^1), c)$ .

AUSGABE:  $b'$

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



# Fortsetzung Hybridtechnik

## Beweis(Fortsetzung):

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

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

- Analog kann gezeigt werden, dass

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

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

## Von fester zu beliebiger Nachrichtenlänge

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

## Von fester zu beliebiger Nachrichtenlänge

- Sei  $\Pi$  ein Verschlüsselungsverfahren mit Klartexten aus  $\{0, 1\}^n$ .
- Splitte  $m \in \{0, 1\}^*$  in  $m_1, \dots, m_t$  mit  $m_i \in \{0, 1\}^n$ .
- Definiere  $\Pi'$  vermöge  $Enc'_k(m) = Enc_k(m_1) \dots Enc_k(m_t)$ .
- Voriger Satz: Falls  $\Pi$  CPA-sicher ist, so ist auch  $\Pi'$  CPA-sicher.

# Zufallsfunktionen

## Definition Echte Zufallsfunktionen:

Sei  $Func_n = \{f \mid f : \{0, 1\}^n \rightarrow \{0, 1\}^n\}$ . 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.  $\{0, 1\}^m \times \{0, 1\}^n \rightarrow \{0, 1\}^n$  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 (PRF)

Sei  $F$  eine längenerhaltende, schlüsselabhängige Funktion. Wir bezeichnen  $F$  als *Pseudozufallsfunktion* (PRF), falls für alle ppt  $D$  gilt

$$|\mathbb{W}_s[D^{F_k(\cdot)}(1^n) = 1] - \mathbb{W}_s[D^{f(\cdot)}(1^n) = 1]| \leq \text{negl}(n),$$

wobei  $k \in_R \{0, 1\}^n$  und  $f \in_R \text{Func}_n$ .

## 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.