CPA Spiel

Szenario: Wir betrachten aktive Angriffe.

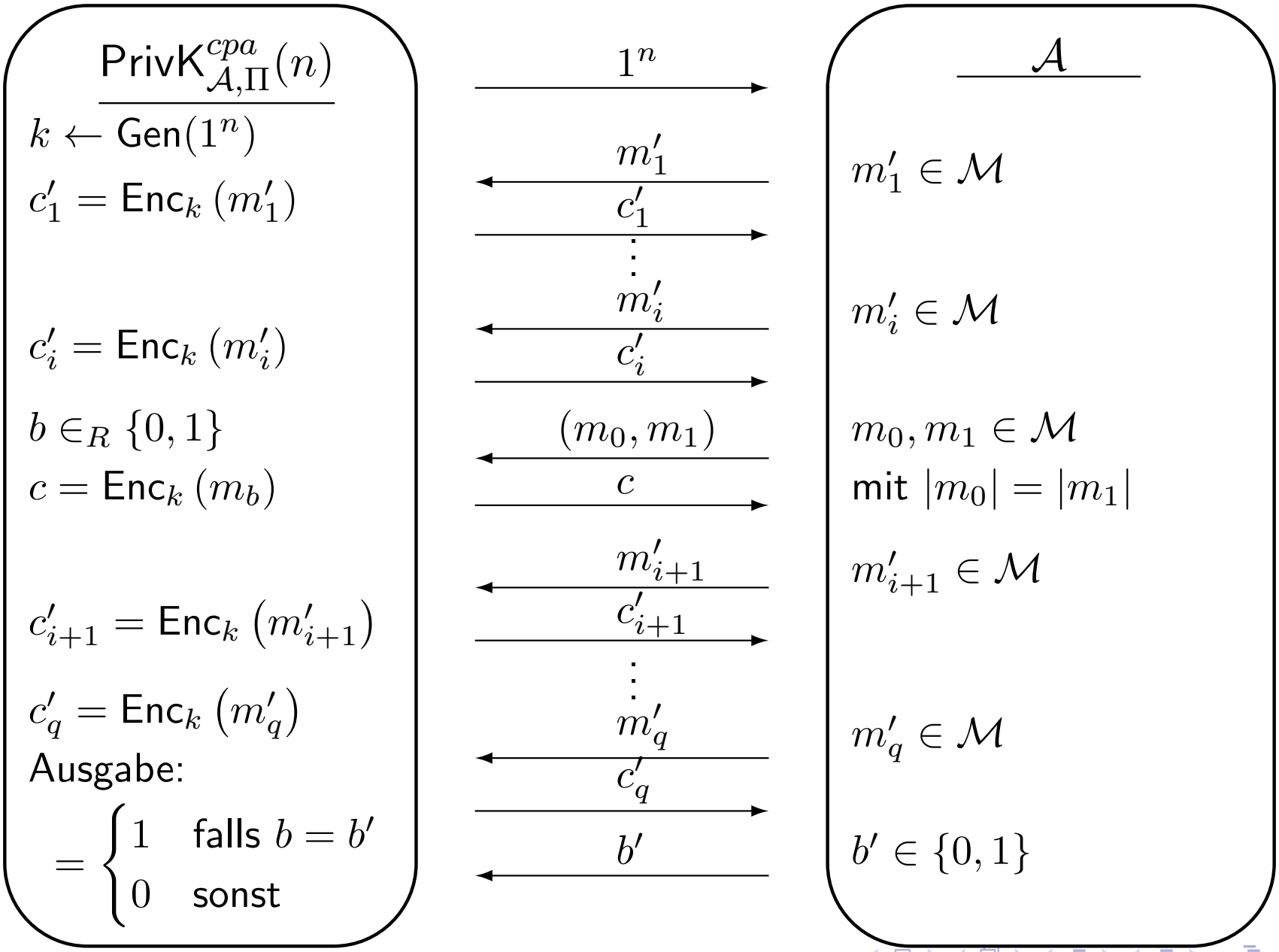
- D.h. $\mathcal{A}$ darf sich Nachrichten nach Wahl verschlüsseln lassen.
- $\mathcal{A}$ erhält dazu Zugriff auf ein Verschlüsselungsorakel $Enc_k(\cdot)$.
- Notation für die Fähigkeit des Orakelzugriffs: $\mathcal{A}^{Enc_k(\cdot)}$.

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

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

CPA Spiel


$\mathsf{PrivK}^{cpa}_{\mathcal{A},\Pi}(n)$
$k \leftarrow \mathsf{Gen}(1^n)$
$c'_1 = \mathsf{Enc}_k(m'_1)$
$c'_i = \mathsf{Enc}_k(m'_i)$
$b \in_R \{0,1\}$
$c = \mathsf{Enc}_k(m_b)$
$c'_{i+1} = \mathsf{Enc}_k(m'_{i+1})$
$c'_q = \mathsf{Enc}_k(m'_q)$
Ausgabe:
$= \begin{cases} 1 & \text{falls } b = b' \\ 0 & \text{sonst} \end{cases}$
1^n
m'_1
c'_1
m'_i
c'_i
(m_0, m_1)
c
m'_{i+1}
c'_{i+1}
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 $|m_0| = |m_1|$
$m'_{i+1} \in \mathcal{M}$
$m'_q \in \mathcal{M}$
$b' \in \{0,1\}$

CPA Sicherheit

Definition CPA Sicherheit

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

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

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

Notation: Wir bezeichnen Π als *CPA sicher*.

CPA-Unsicherheit deterministischer Verschlüsselung

Satz Unsicherheit deterministischer Verschlüsselung

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

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

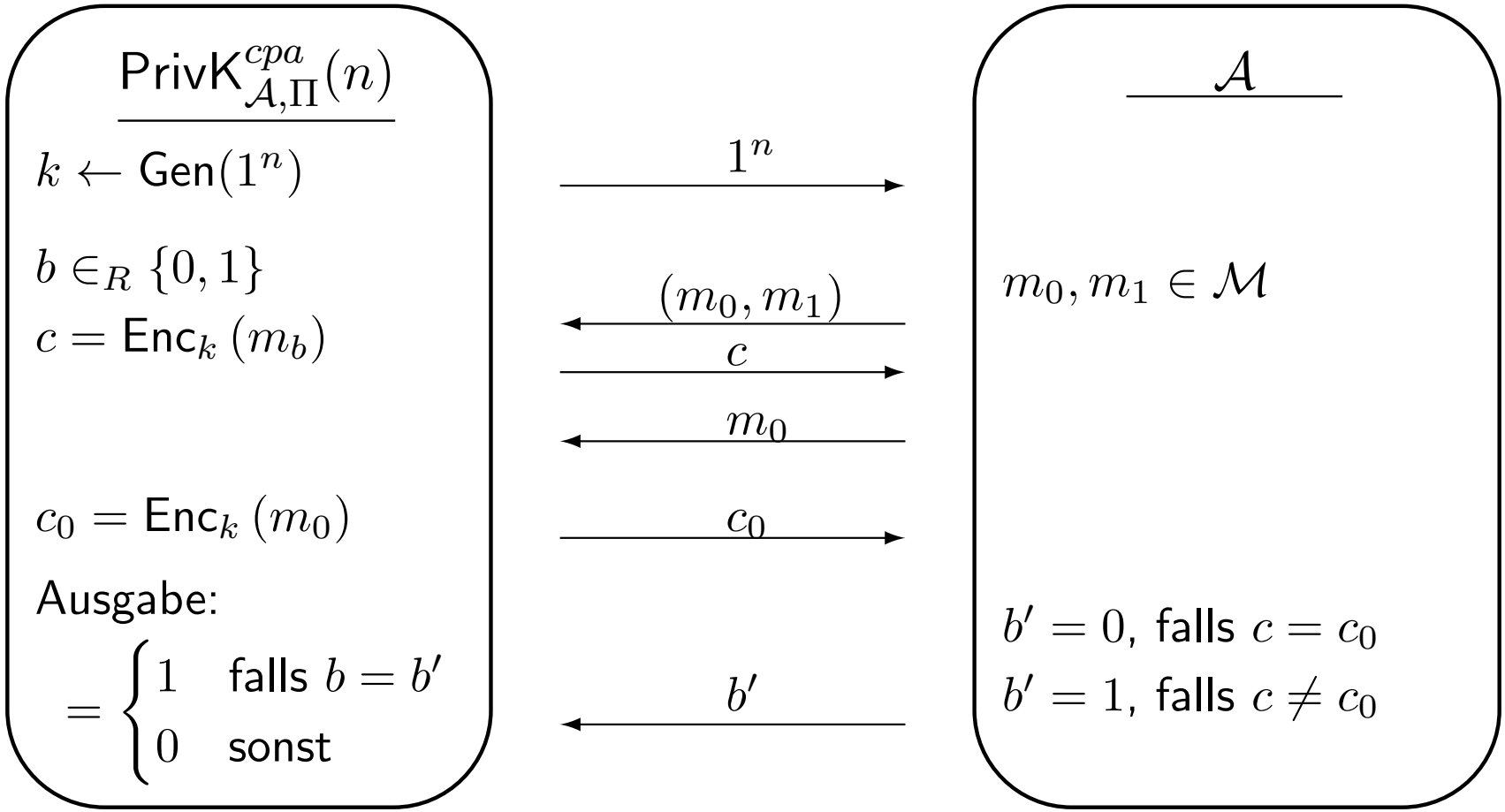
Algorithmus CPA Angreifer $\mathcal{A}$

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

CPA Angreifer für deterministische Verschlüsselungen



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

Mult-CPA Spiel

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

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

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

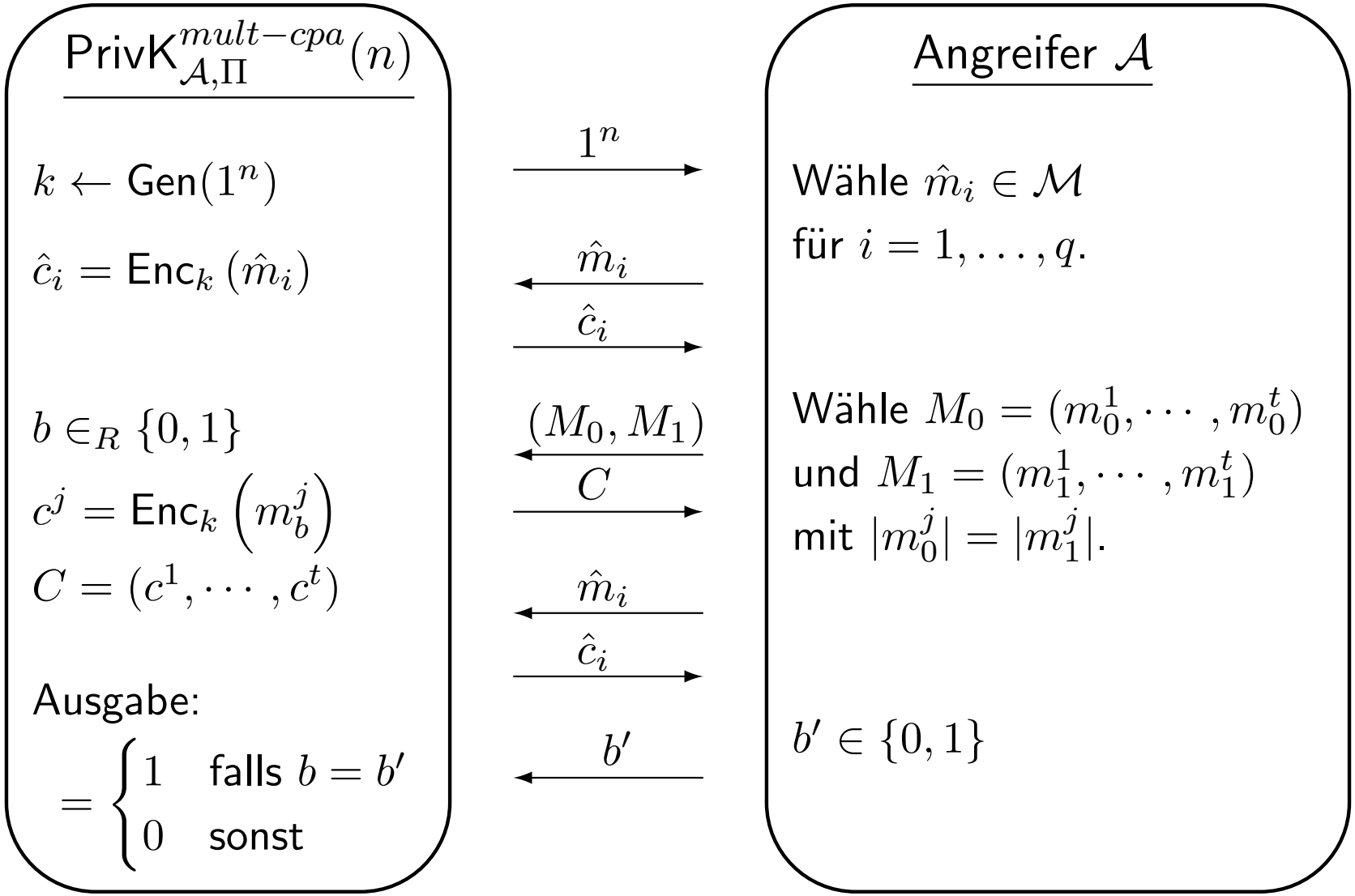
1. $(M_0, M_1) \leftarrow \mathcal{A}^{Enc_k(\cdot)}(1^n)$ mit $M_0 = (m_0^1, \ldots, m_0^t)$, $M_1 = (m_1^1, \ldots, m_1^t)$ und $|m_0^i| = |m_1^i|$ für alle $i \in [t]$.
2. $k \leftarrow Gen(1^n)$.
3. Wähle $b \in_R \{0,1\}$. $b' \leftarrow \mathcal{A}^{Enc_k(\cdot)}((Enc_k(m_b^1), \ldots, Enc_k(m_b^t))$.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

Definition Mult-CPA Sicherheit

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

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

Mult-CPA Spiel



CPA-Sicherheit mehrfacher Verschlüsselung

Satz CPA-Sicherheit mehrfacher Verschlüsselung

Sei Π ein Verschlüsselungsschema. Dann ist Π CPA-sicher gdw Π mult-CPA sicher ist.

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

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

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

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

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 $\mathcal{A}'$

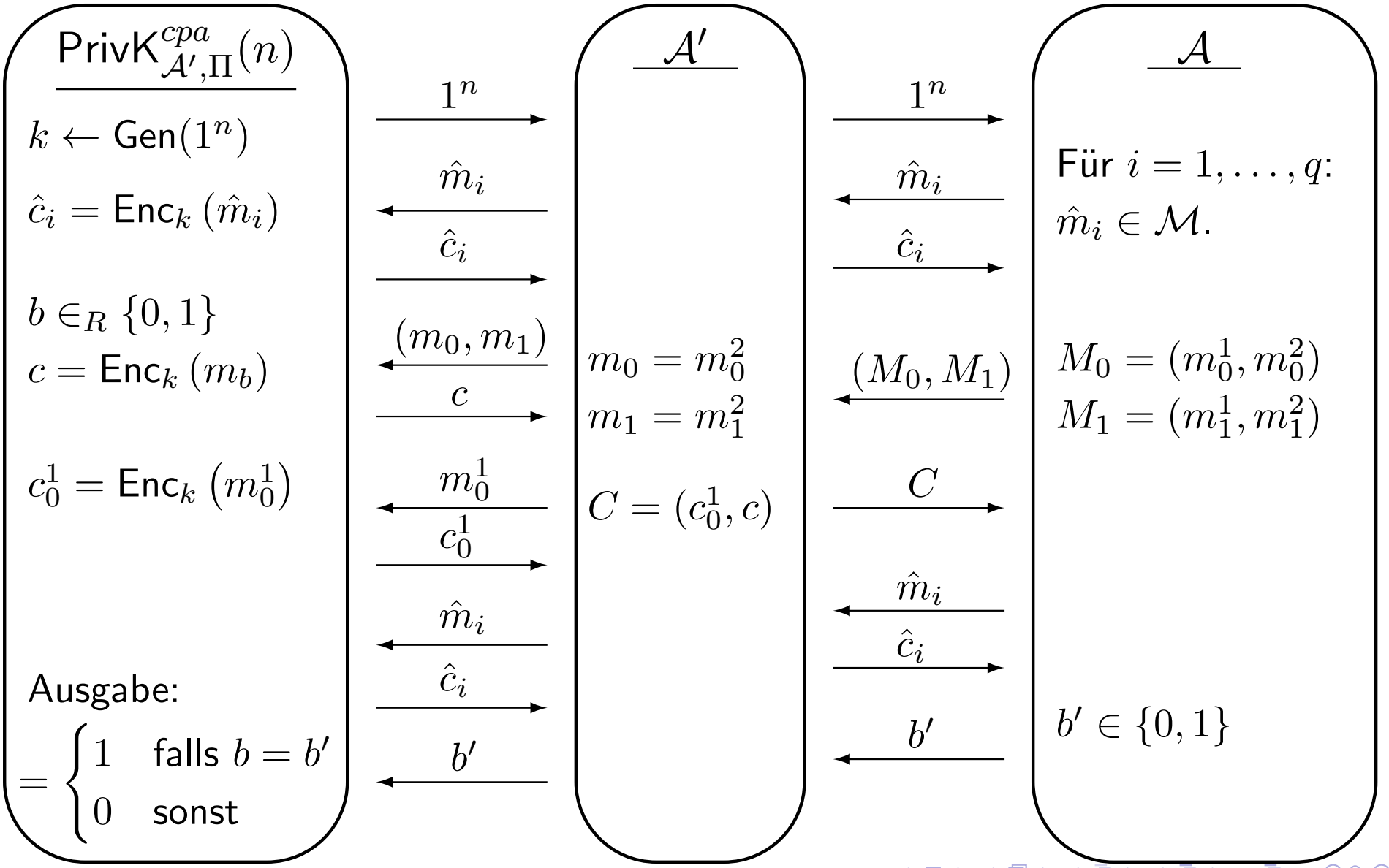
EINGABE: 1^n und Orakelzugriff $Enc_k(\cdot)$

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. $b' \leftarrow \mathcal{A}(Enc_k(m_0^1), c)$.

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

Betrachten der Hybride



Fortsetzung Hybridtechnik

Beweis(Fortsetzung):

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

Beweistechnik für allgemeines t

- Definiere für $0 \leq i \leq t$ Hybride
$$C^{(i)} = (Enc_k(m_0^1), \ldots, Enc_k(m_0^i), Enc_k(m_1^{i+1}), \ldots, Enc_k(m_1^t)).$$
- $\mathrm{Ws}[PrivK^{mult-cpa}_{\mathcal{A},\Pi}(n) = 1] = \frac{1}{2} \cdot \mathrm{Ws}[\mathcal{A}(C^{(t)}) = 0] + \frac{1}{2} \cdot \mathrm{Ws}[\mathcal{A}(C^{(0)} = 1]$.
- Daraus folgt $\mathrm{Ws}[PrivK^{mult-cpa}_{\mathcal{A},\Pi}(n) = 1] + \frac{t-1}{2} =$

$$\begin{aligned} & \frac{1}{2}\mathrm{Ws}[\mathcal{A}(C^{(t)}) = 0] + \frac{1}{2}\mathrm{Ws}[\mathcal{A}(C^{(0)}) = 1] \\ + & \sum_{i=1}^{t-1} \frac{1}{2} \left(\mathrm{Ws}[\mathcal{A}(C^{(i)}) = 0] + \frac{1}{2}\mathrm{Ws}[\mathcal{A}(C^{(i)}) = 1] \right) \\ = & \sum_{i=1}^{t} \frac{1}{2} \left(\mathrm{Ws}[\mathcal{A}(C^{(i-1)}) = 1] + \mathrm{Ws}[\mathcal{A}(C^{(i)}) = 0] \right) \end{aligned}$$

- $\mathcal{A}'$ 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 $\mathrm{Ws}[PrivK^{mult-cpa}_{\mathcal{A},\Pi}(n)] \leq \frac{1}{2} + t \cdot \mathrm{negl}(n)$ $\square_{\text{Satz}}$.

Von fester zu beliebiger Nachrichtenlänge

Von fester zu beliebiger Nachrichtenlänge

- Sei Π 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 Π' vermöge $Enc'_k(m) = Enc_k(m_1) \ldots Enc_k(m_t)$.
- Aus vorigem Satz folgt: Π' ist CPA-sicher, falls Π CPA-sicher ist.