DDH Problem

Definition Decisional Diffie-Hellman (DDH) Annahme

Das *Decisional Diffie-Hellman Problem* ist hart bezüglich $\mathcal{G}$, falls für alle ppt Algorithmen $\mathcal{A}$ gilt

$$|\mathrm{Ws}[\mathcal{A}(g,q,g^x,g^y,g^{xy})=1]-\mathrm{Ws}[\mathcal{A}(g,q,g^x,g^y,g^z)=1]|\leq \mathrm{negl}.$$

Wsraum: zufällige Wahl von $x,y,z\in_R\mathbb{Z}_q$, interne Münzwürfe von $\mathcal{A}$, $\mathcal{G}$.

DDH Annahme: Das DDH Problem ist hart bezüglich $\mathcal{G}$.

- Unter der DDH-Annahme kann Eve den DH-Schlüssel g^{xy} nicht von einem zufälligen Gruppenelement unterscheiden.

Sicherheitsbeweis des DH-Protokolls

Satz Sicherheit des Diffie-Hellman Protokolls

Unter der DDH-Annahme ist das DH-Protokoll Π sicher gegen passive Angreifer $\mathcal{A}$.

Beweis: Es gilt $\mathrm{Ws}[KE_{\mathcal{A},\Pi}(n) = 1]$

$$
\begin{aligned}
&= \frac{1}{2} \cdot \mathrm{Ws}[KE_{\mathcal{A},\Pi}(n) = 1 \mid b = 0] + \frac{1}{2} \cdot \mathrm{Ws}[KE_{\mathcal{A},\Pi}(n) = 1 \mid b = 1] \\
&= \frac{1}{2} \cdot \mathrm{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^{xy}) = 0] + \frac{1}{2} \cdot \mathrm{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^z) = 1] \\
&= \frac{1}{2} \cdot (1 - \mathrm{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^{xy}) = 1]) + \frac{1}{2}\mathrm{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^z) = 1] \\
&= \frac{1}{2} + \frac{1}{2} \cdot (\mathrm{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^z) = 1] - \mathrm{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^{xy}) = 1]) \\
&\leq \frac{1}{2} + \frac{1}{2} \cdot |\mathrm{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^{xy}) = 1] - \mathrm{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^z) = 1]| \\
&\leq \frac{1}{2} + \frac{1}{2} \cdot \mathrm{negl}(n) = \frac{1}{2} + \mathrm{negl}(n) \quad \text{nach DDH-Annahme.}
\end{aligned}
$$

Public-Key Verschlüsselung

Szenario: Asymmetrische/Public Key Verschlüsselung

- Schlüsselpaar (pk, sk) aus öffentlichem/geheimem Schlüssel.
- Verschlüsselung Enc_{pk} ist Funktion des öffentlichen Schlüssels.
- Entschlüsselung Dec_{sk} ist Funktion des geheimen Schlüssels.
- pk kann veröffentlicht werden, z.B. auf Webseite, Visitenkarte.
- pk kann über öffentlichen (authentisierten) Kanal verschickt werden.

Vorteile:

- Löst Schlüsselverteilungsproblem.
- Erfordert die sichere Speicherung eines einzigen Schlüssels.

Nachteil:

- Heutzutage deutlich langsamer als sym. Verschlüsselung.

Public-Key Verschlüsselung

Definition Public-Key Verschlüsselung

Ein *Public-Key Verschlüsselungsverfahren* ist ein 3-Tupel $\Pi = (Gen, Enc, Dec)$ von ppt Algorithmen mit

1. **Gen:** $(pk, sk) \leftarrow Gen(1^n)$, wobei pk der öffentliche und sk der geheime Schlüssel ist. Beide Schlüssel besitzen Länge mind. n.
2. **Enc:** Für eine Nachricht $m \in \mathcal{M}$ und Schlüssel pk berechne
$$c \leftarrow Enc_{pk}(m).$$
3. **Dec:** Für einen Chiffretext $c \in \mathcal{C}$ und Schlüssel sk berechne
$$m' := Dec_{sk}(c).$$

Es gilt $\mathrm{Ws}[Dec_{sk}(Enc_{pk}(m)) = m] = 1 - \mathrm{negl}(n)$.

Ununterscheidbarkeit von Chiffretexten

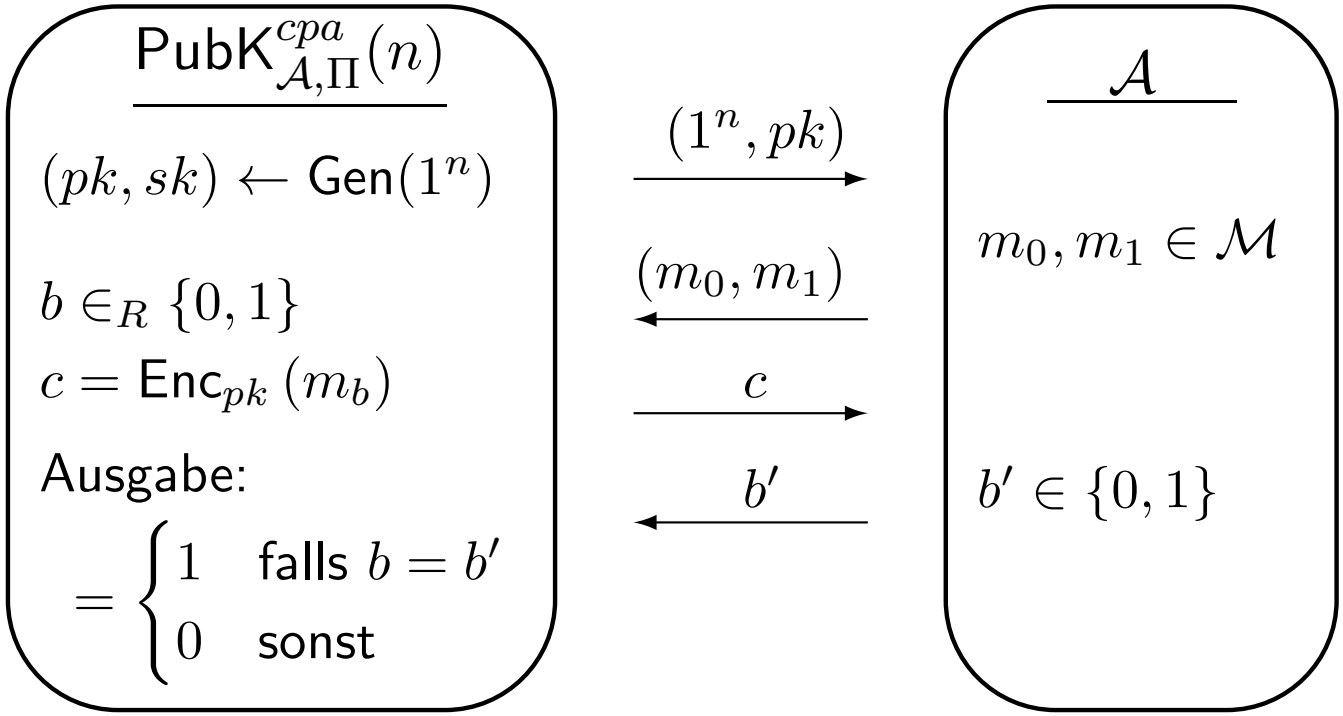
Spiel CPA Ununterscheidbarkeit von Chiffretexten $PubK^{cpa}_{\mathcal{A},\Pi}(n)$

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

1. $(pk, sk) \leftarrow Gen(1^n)$
2. $(m_0, m_1) \leftarrow \mathcal{A}(pk)$
3. Wähle $b \in_R \{0,1\}$. $b' \leftarrow \mathcal{A}(Enc_{pk}(m_b))$.
4. $$PubK^{cpa}_{\mathcal{A},\Pi}(n) = \begin{cases} 1 & \text{für } b = b' \\ 0 & \text{sonst} \end{cases}$$

- Man beachte, dass $\mathcal{A}$ Orakelzugriff auf Enc_{pk} besitzt.
- D.h. $\mathcal{A}$ kann sich beliebig gewählte Klartexte verschlüsseln lassen. (chosen plaintext attack = CPA)

CPA-Spiel


$\mathsf{PubK}^{cpa}_{\mathcal{A},\Pi}(n)$
$(pk, sk) \leftarrow \mathsf{Gen}(1^n)$
$b \in_R \{0,1\}$
$c = \mathsf{Enc}_{pk}(m_b)$
Ausgabe:
$= \begin{cases} 1 & \text{falls } b = b' \\ 0 & \text{sonst} \end{cases}$
$(1^n, pk)$
(m_0, m_1)
c
b'
$\mathcal{A}$
$m_0, m_1 \in \mathcal{M}$
$b' \in \{0,1\}$

CPA Sicherheit

Definition CPA Sicherheit von Verschlüsselung

Ein PK-Verschlüsselungsverfahren $\Pi = (Gen, Enc, Dec)$ heißt *CPA-sicher*, d.h. Π besitzt ununterscheidbare Verschlüsselungen unter CPA, falls für alle ppt $\mathcal{A}$ gilt

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

- **Übung:** *Unbeschränkte* $\mathcal{A}$ können das Spiel $PubK^{cpa}_{\mathcal{A},\Pi}(n)$ mit Ws $1 - \mathrm{negl}(n)$ gewinnen.

Unsicherheit deterministischer Verschlüsselung

Satz Deterministische Verschlüsselung

Deterministische PK-Verschlüsselung ist unsicher gegenüber CPA.

Beweis:

- $\mathcal{A}$ kann sich $Enc_{pk}(m_0)$ und $Enc_{pk}(m_1)$ selbst berechnen.
- D.h. ein Angreifer $\mathcal{A}$ gewinnt $PubK^{cpa}_{\mathcal{A},\Pi}(n)$ mit Ws 1.

Mehrfache Verschlüsselung

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

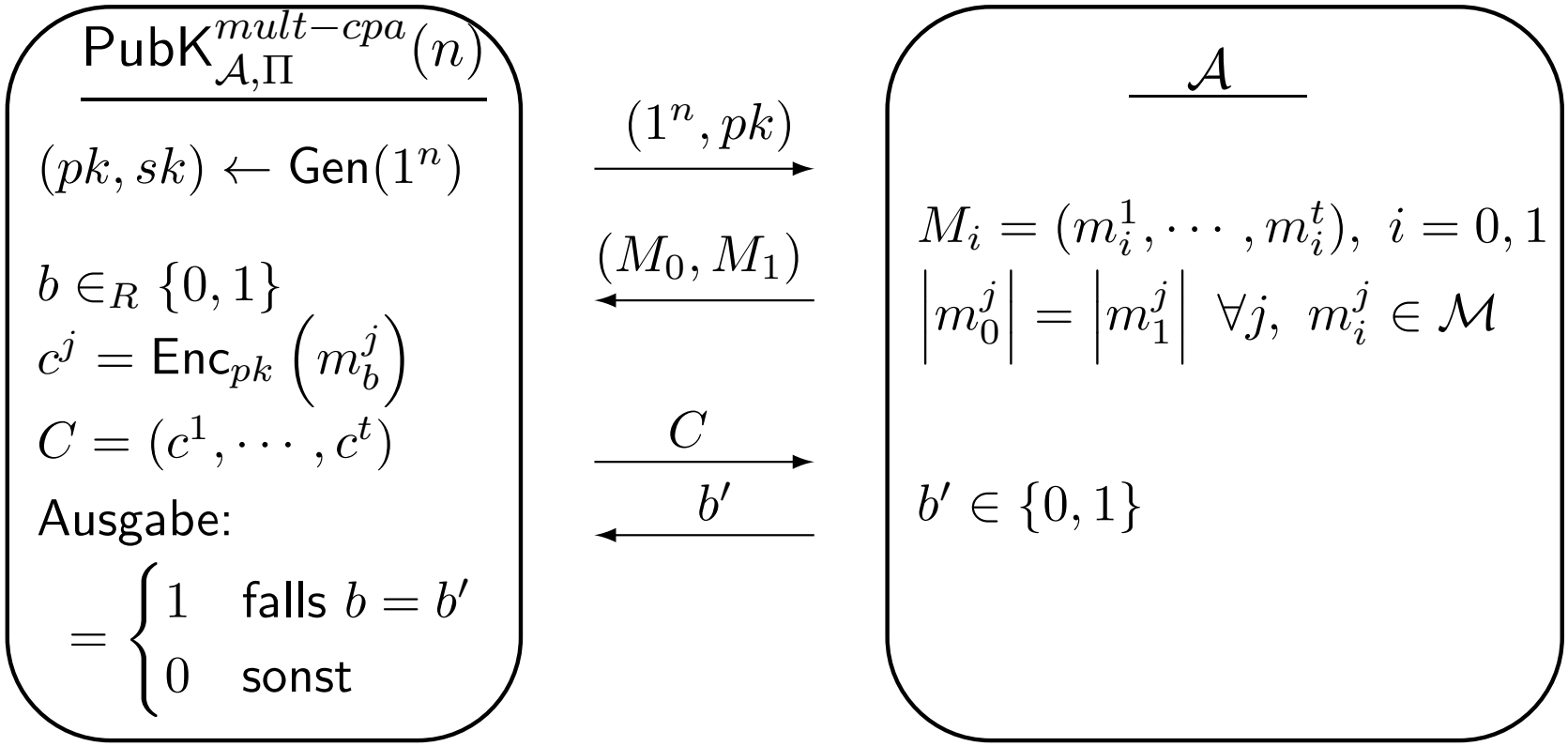
Sei Π ein PK-Verschlüsselungsverfahren und $\mathcal{A}$ ein Angreifer.

1. $(pk, sk) \leftarrow Gen(1^n)$
2. $(M_0, M_1) \leftarrow \mathcal{A}(pk)$, wobei $M_i = (m_i^1, \ldots, m_i^t), i = 0, 1$ und $|m_0^j| = |m_1^j|$ für $j \in [t]$.
3. Wähle $b \in_R \{0, 1\}$. $b' \leftarrow \mathcal{A}(Enc_{pk}(m_b^1), \ldots, Enc_{pk}(m_b^t))$.
4. $$PubK^{mult}_{\mathcal{A},\Pi}(n) = \begin{cases} 1 & \text{für } b = b' \\ 0 & \text{sonst} \end{cases}.$$

Definition CPA Sicherheit von mehrfacher Verschlüsselung

Ein PK-Verschlüsselungsverfahren $\Pi = (Gen, Enc, Dec)$ heißt *mult-CPA sicher*, d.h. besitzt ununterscheidbare mehrfache Verschlüsselungen unter CPA, falls für alle ppt $\mathcal{A}$ gilt $\text{Ws}[PubK^{mult}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \text{negl}(n)$.

multCPA-Spiel



Sicherheit mehrfacher Verschlüsselung

Satz Sicherheit mehrfacher Verschlüsselung *(analog zu Krypto I)*

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

Beweis "⇐": Für $t = 2$.

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

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

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

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

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

Betrachten der Hybride

Lemma

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

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

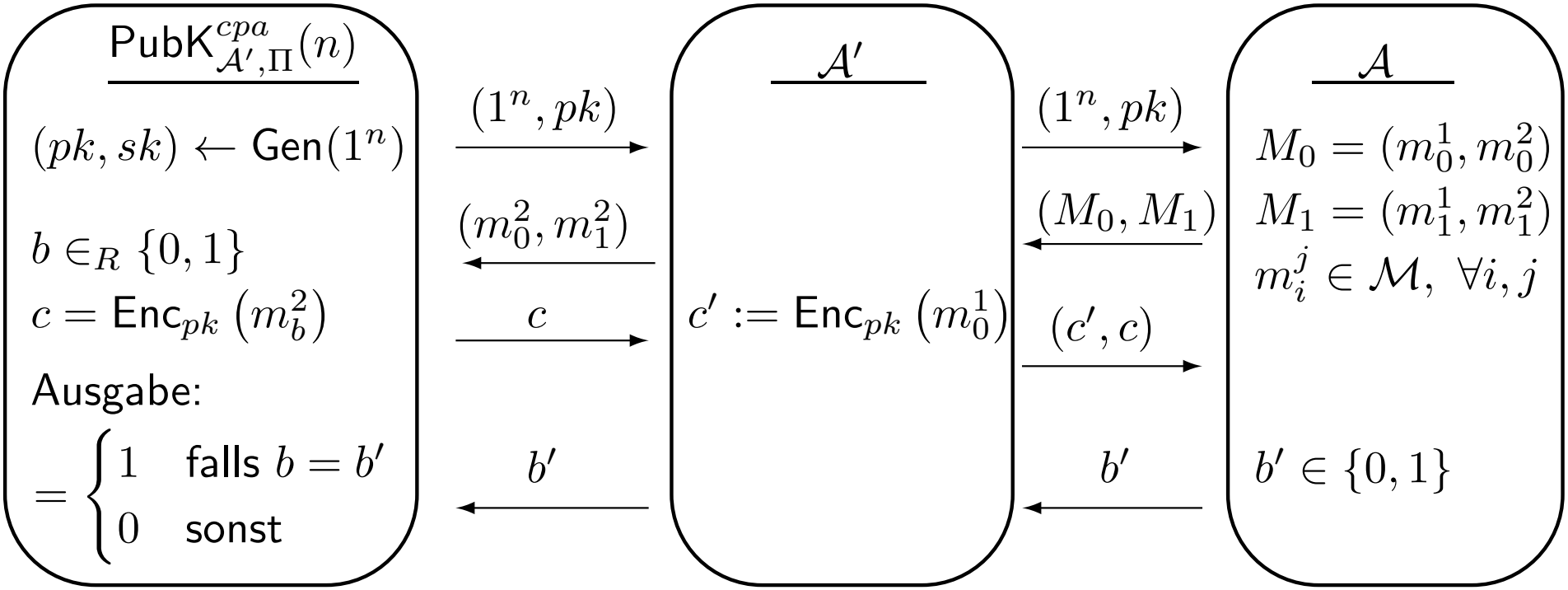
- $\mathcal{A}'$ versucht mittels $\mathcal{A}$ das Spiel $PubK^{cpa}_{\mathcal{A}',\Pi}(n)$ zu gewinnnen.

Strategie von Angreifer $\mathcal{A}'$

1. $\mathcal{A}'$ gibt pk an $\mathcal{A}$ weiter.
2. $(M_0, M_1) \leftarrow \mathcal{A}(pk)$ 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 $c(b) = Enc_{pk}(m_b^2)$.
4. $b' \leftarrow \mathcal{A}(Enc_{pk}(m_0^1), c(b))$.
5. $\mathcal{A}'$ gibt Bit b' aus.

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

Strategie des Angreifers bei Hybriden



Fortsetzung Hybridtechnik

Beweis(Fortsetzung):

- CPA Sicherheit von Π bei einzelnen Nachrichten impliziert

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

- Analog kann gezeigt werden, dass

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

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

Von fester zu beliebiger Nachrichtenlänge

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

Von fester zu beliebiger Nachrichtenlänge

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

Hybride Verschlüsselungsverfahren

Ziel: Flexibilität von asym. Verfahren und Effizienz von sym. Verfahren.
Szenario:

- Sei $\Pi = (Gen, Enc, Dec)$ ein PK-Verschlüsselungsverfahren und $\Pi' = (Gen', Enc', Dec')$ ein SK-Verschlüsselungsverfahren.
- Berechne $(pk, sk) \leftarrow Gen(1^n)$.

Algorithmus Hybride Verschlüsselung

Eingabe: m, pk

1. Wähle $k \in_R \{0,1\}^n$.
2. Verschlüssele $c_1 \leftarrow Enc_{pk}(k)$ mit asym. Verschlüsselung.
3. Verschlüssele $c_2 \leftarrow Enc'_k(m)$ mit sym. Verschlüsselung.

Ausgabe: Chiffretext $c = (c_1, c_2)$

Hybride Entschlüsselung

Algorithmus Hybride Entschlüsselung

Eingabe: $c = (c_1, c_2)$, sk

1. Entschlüssele $k \leftarrow Dec_{sk}(c_1)$.
2. Entschlüssele $m \leftarrow Dec'_k(c_2)$.

Ausgabe: Klartext m

- Effizienzgewinn für $|m| \gg n$, sofern Π' effizienter isals Π.
- **Frage:** Ist hybride Verschlüsselung sicher, falls Π, Π' sicher?