Mehrfache Verschlüsselung

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

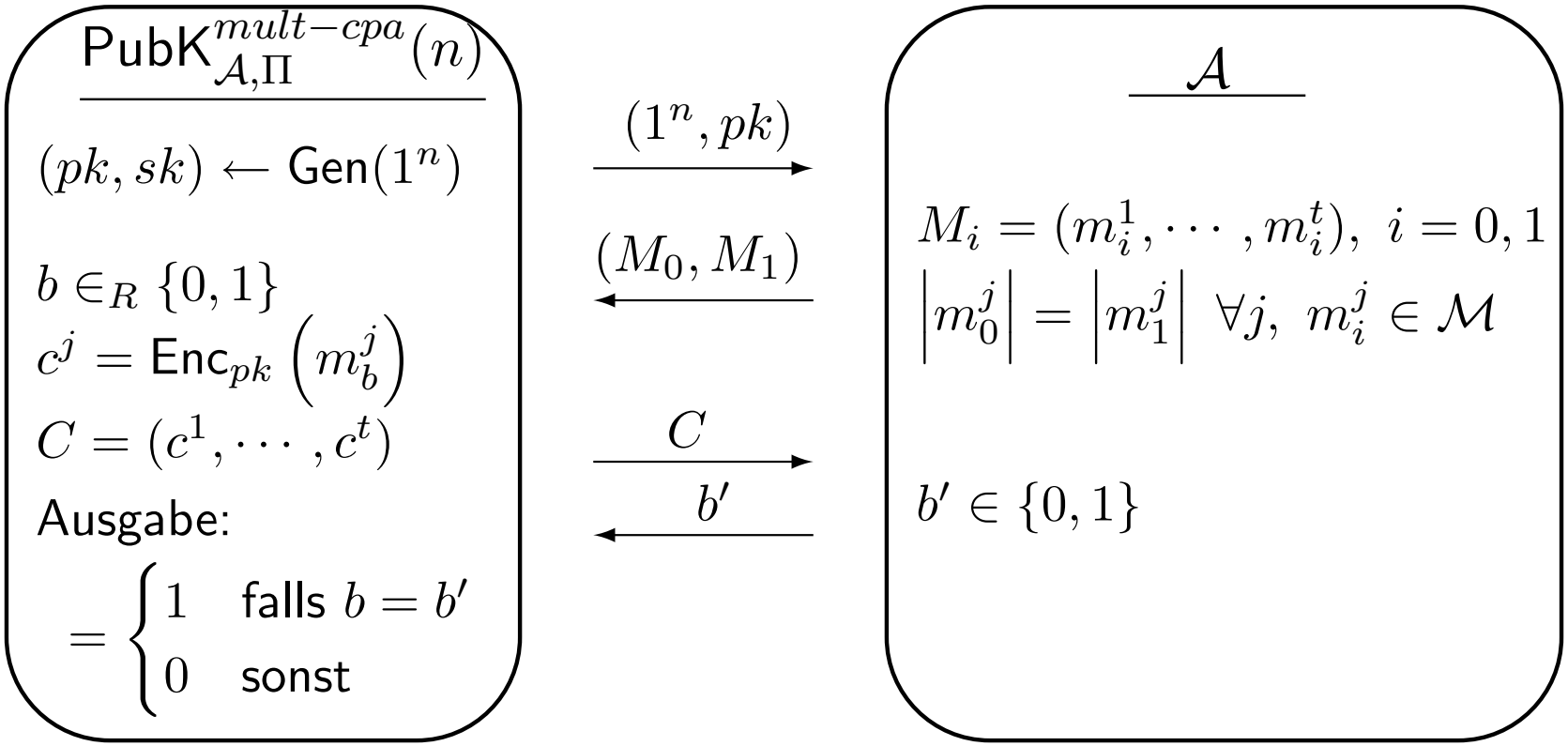
Sei Π ein PK-Verschlüsselungsverfahren und $\mathcal{A}$ ein Angreifer.

1. $(pk, sk) \leftarrow Gen(1^n)$
2. $(M_0, M_1) \leftarrow \mathcal{A}(pk)$, wobei $M_i = (m_i^1, \ldots, m_i^t), i = 1, 2$ 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 $\Pi = (Gen, Enc, Dec)$ besitzt ununterscheidbare mehrfache Verschlüsselungen unter CPA falls für alle ppt $\mathcal{A}$ gilt $\mathrm{Ws}[PubK^{mult}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathrm{negl}(n)$.

multCPA-Spiel



Sicherheit mehrfacher Verschlüsselung

Satz Sicherheit mehrfacher Verschlüsselung

Sei Π ein PK-Verschlüsselungsschema. Π besitzt ununterscheidbare mehrfache Verschlüsselung unter CPA gdw Π ununterscheidbare Verschlüsselung unter CPA besitzt.

Beweis "$\Leftarrow$": 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 $\mathrm{Ws}[PubK^{mult}_{\mathcal{A},\Pi}(n)] + \frac{1}{2} =$

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

- **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.

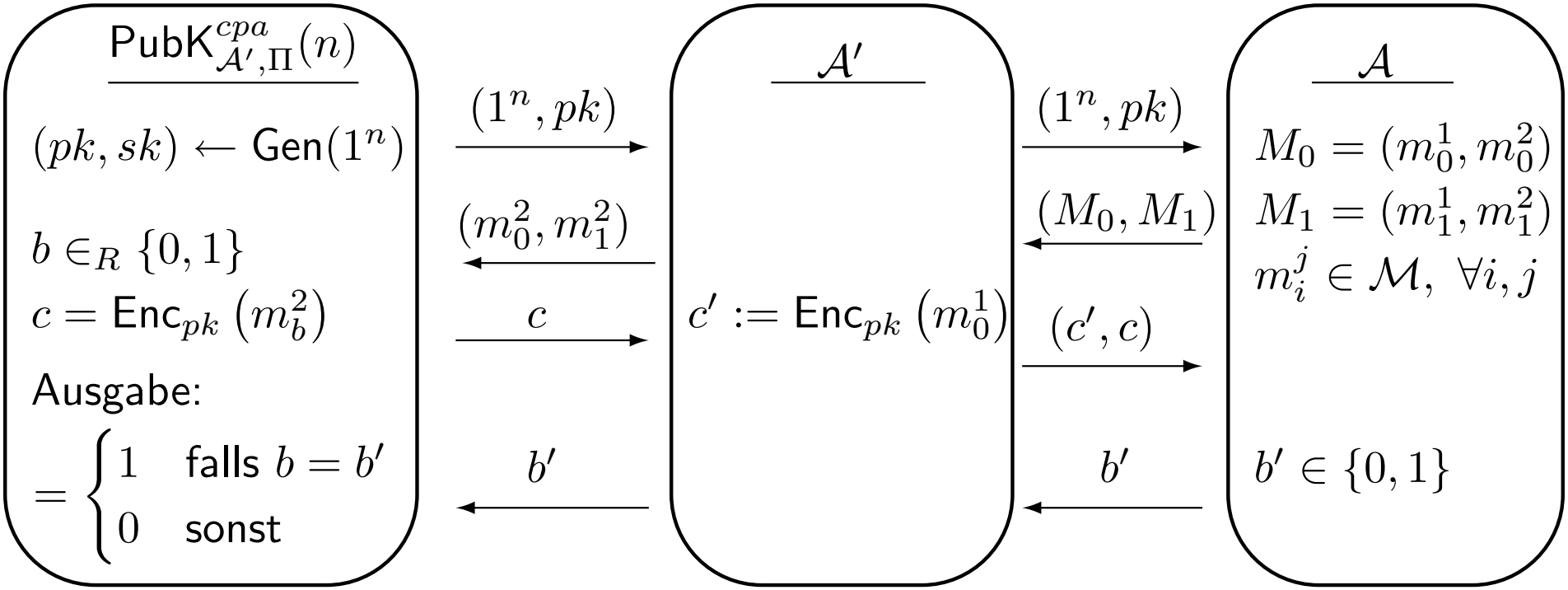
- $\mathcal{A}'$ versucht mittels $\mathcal{A}$ das Spiel $PubK^{cpa}_{\mathcal{A}',\Pi}(n)$ zu gewinnnen.

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

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

- Analog kann gezeigt werden, dass

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

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

Von fester zu beliebiger Nachrichtenlänge

- Beweistechnik für allgemeines t: Definiere für $i \in [t]$ Hybride
  $C^{(i)} = (Enc_{pk}(m_0^1), \ldots, Enc_{pk}(m_0^i), Enc_{pk}(m_1^{i+1}), \ldots, Enc_{pk}(m_1^t))$.
- $\mathrm{Ws}[PubK^{mult}_{\mathcal{A},\Pi}(n) = 1] = \frac{1}{2} \cdot \mathrm{Ws}[\mathcal{A}(C^{(t)}) = 0] + \frac{1}{2} \cdot \mathrm{Ws}[\mathcal{A}(C^{(0)} = 1]$.
- $\mathcal{A}'$ 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 $m \in \{0,1\}^*$ in $m_1, \ldots m_t$ mit $m_i \in \{0,1\}^n$.
- Definiere Π' vermöge $Enc'_{pk}(m) = Enc_{pk}(m_1) \ldots Enc_{pk}(m_t)$.
- 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.

- 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 $c = (c_1, c_2)$