dlog Problem

Definition Diskrete Logarithmus (dlog) Annahme

Das *Diskrete Logarithmus Problem* ist hart bezüglich $\mathcal{G}$, falls für alle ppt Algorithmen $\mathcal{A}$ gilt

$$|\mathrm{Ws}[\mathcal{A}(G, q, g, g^x) = x]| \leq \mathrm{negl}(n).$$

Der Wsraum ist definiert bezüglich $(G, q, g) \leftarrow \mathcal{G}(1^n)$, der zufälligen Wahl von $x \in_R \mathbb{Z}_q$ und der internen Münzwürfe von $\mathcal{A}$ und $\mathcal{G}$.

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

- Unter der dlog Annahme können die geheimen Schlüssel x, y bei Diffie-Hellman nur mit vernachlässigbarer Ws berechnet werden.
- D.h. die dlog Annahme ist eine notwendige Sicherheitsannahme.
- Problem: Die Berechnung von g^{xy} aus g^x, g^y könnte einfach sein.

CDH Problem

Definition Computational Diffie-Hellman (CDH) Annahme

Das *Computational Diffie-Hellman Problem* ist hart bezüglich $\mathcal{G}$, falls für alle ppt Algorithmen $\mathcal{A}$ gilt $\mathrm{Ws}[\mathcal{A}(G, q, g, g^x, g^y) = g^{xy}] \leq \mathrm{negl}(n)$.

Wsraum: zufällige Wahl von $x, y \in_R \mathbb{Z}_q$, Münzwürfe von $\mathcal{A}$, $\mathcal{G}(1^n)$.

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

- Unter der CDH-Annahme kann ein DH-Angreifer Eve den Schlüssel $k_A = g^{xy}$ nur mit vernachlässigbarer Ws berechnen.

Problem:

- Sei CDH schwer, so dass Angreifer Eve k_A nicht berechnen kann.
- Benötigen aber, dass k_A ein zufälliges Gruppenelement in G ist.
- Unterscheiden von g^{xy} und $g^z, z \in_R \mathbb{Z}_q$ könnte einfach sein. (Bsp: $G = \mathbb{Z}_p^*$ für p=prim.)

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

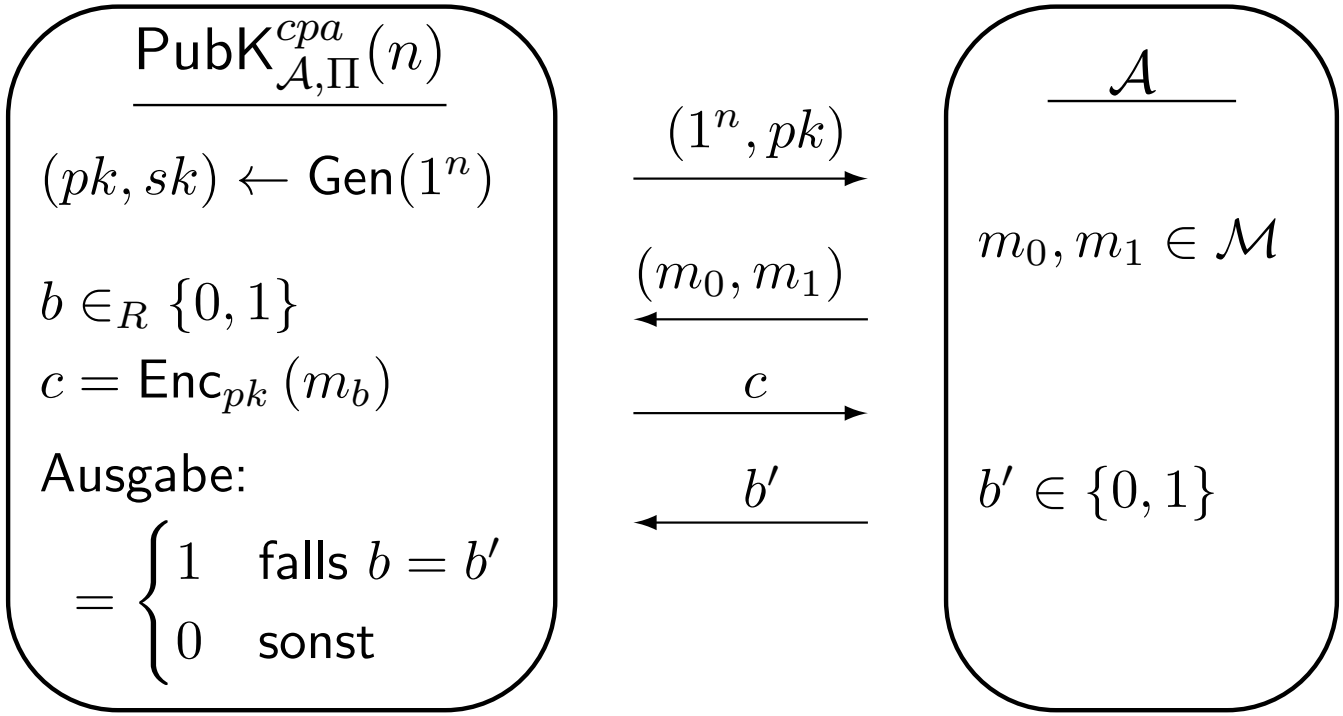
Spiel CPA Ununterscheidbarkeit von Chiffretexten $PubK^{cpa}_{\mathcal{A},\Pi}(n)$

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 $\mathcal{A}$ (implizit) 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 $PubK^{mult}_{\mathcal{A},\Pi}(n)$

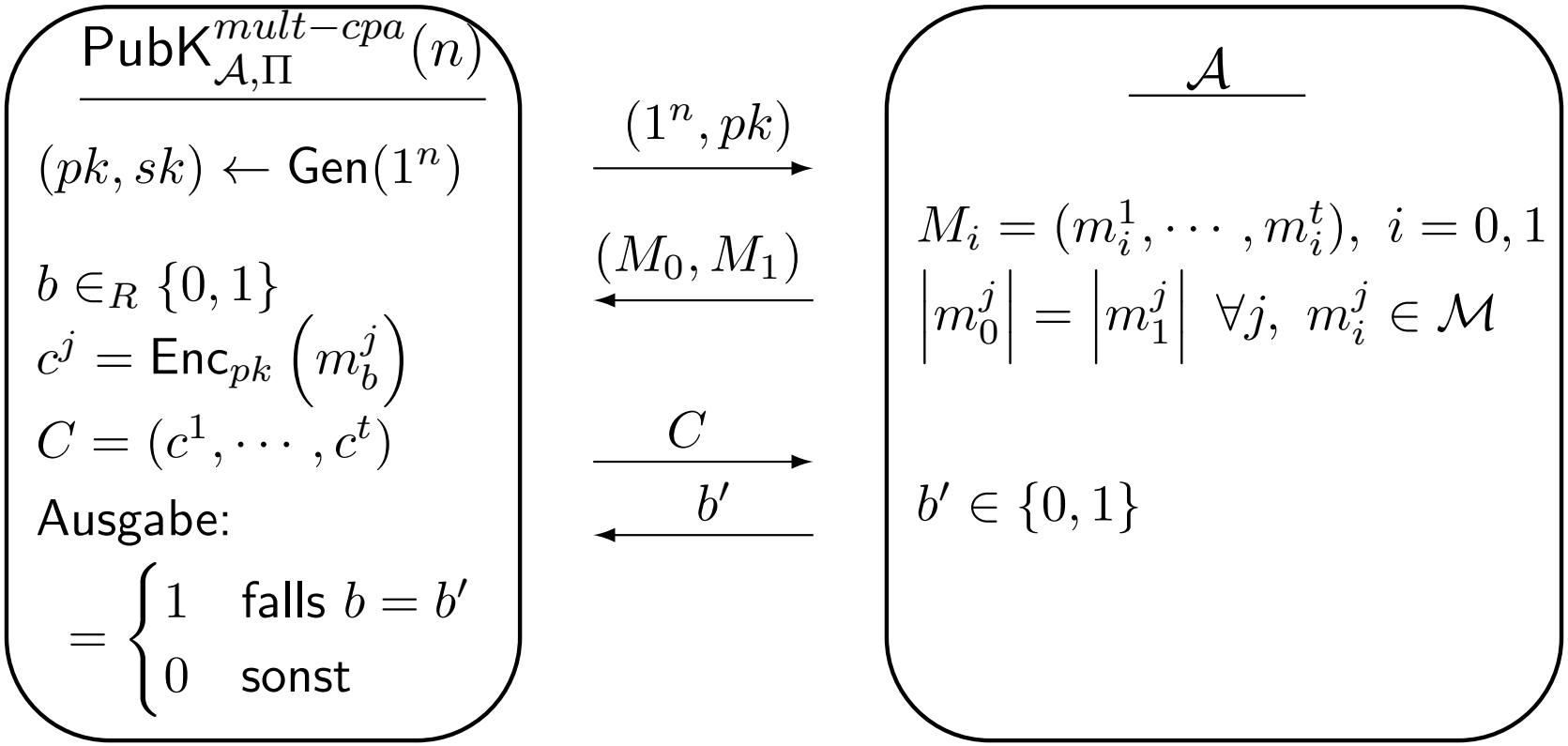
Sei Π ein PK-Verschlüsselungsverfahren und $\mathcal{A}$ ein Angreifer.

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

multCPA-Spiel



Sicherheit mehrfacher Verschlüsselung

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

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

Beweis "$\Leftarrow$":

- Sei $\mathcal{A}$ ein Angreifer im Spiel $PubK^{mult}_{\mathcal{A},\Pi}(n)$. Für $i \in \{0,\ldots,t\}$ definiere die Hybride $C^{(i)} = (Enc_{pk}(m_1^1),\ldots,Enc_{pk}(m_1^i),Enc_{pk}(m_0^{i+1}),\ldots,Enc_{pk}(m_0^t))$.
  Es gilt: $\mathrm{Ws}[PubK^{mult}_{\mathcal{A},\Pi}(n)=1]-\frac{1}{2}$

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

Betrachten der Hybride

Lemma

Für alle i: $\frac{1}{2}\mathrm{Ws}[\mathcal{A}(C^{(i)}) = 0] + \frac{1}{2}\mathrm{Ws}[\mathcal{A}(C^{(i+1)}) = 1] \leq \frac{1}{2} + \mathrm{negl}(n)$.

Beweis ($t = 2, i = 0$): Sei $\mathcal{A}'$ Angreifer für *einfache* Verschl.

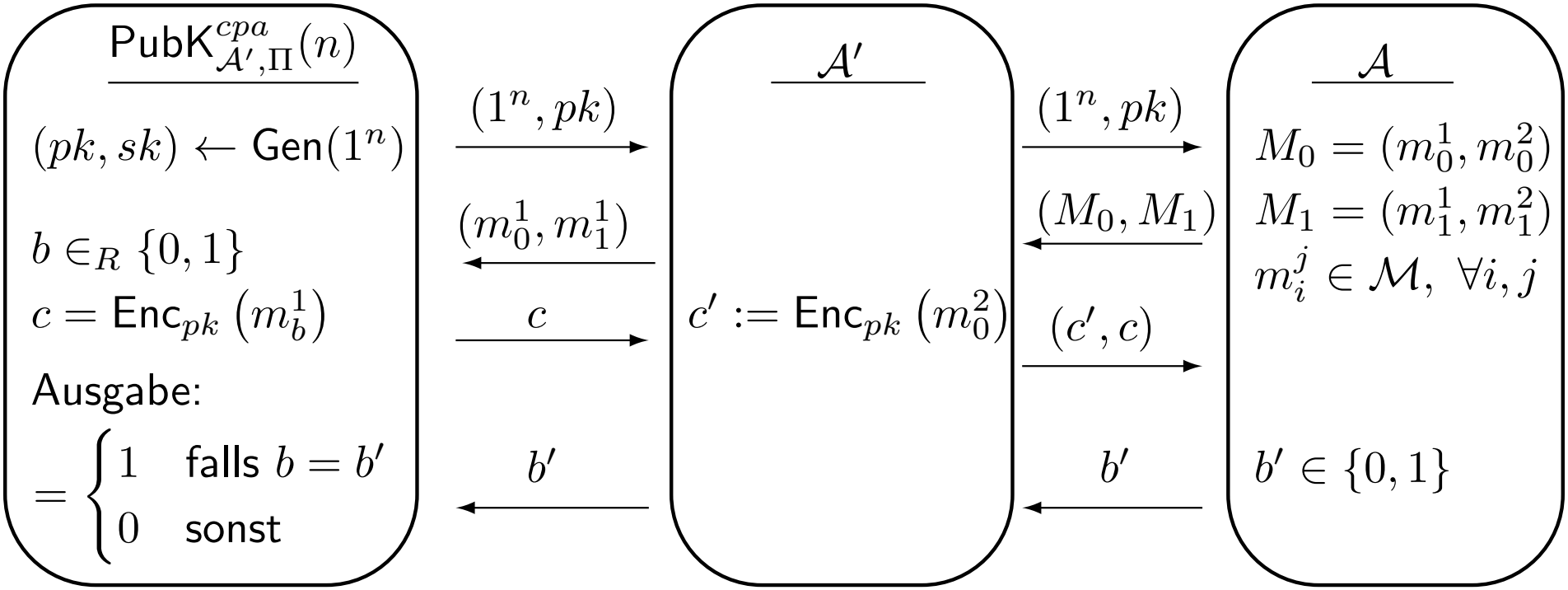
- $\mathcal{A}'$ versucht mittels $\mathcal{A}$ das Spiel $PubK^{cpa}_{\mathcal{A}',\Pi}(n)$ zu gewinnnen.

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_0^1, m_1^1) aus. $\mathcal{A}'$ erhält Chiffretext $c(b) = Enc_{pk}(m_b^1)$.
4. $b' \leftarrow \mathcal{A}(c(b), Enc_{pk}(m_0^2))$.
5. $\mathcal{A}'$ gibt Bit b' aus.

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

Strategie des Angreifers bei Hybriden



Fortsetzung Hybridtechnik

Beweis (Fortsetzung):

- CPA Sicherheit von Π bei einzelnen Nachrichten impliziert

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

- Beweis für allgemeine t, i analog
- Aus Lemma folgt $\mathrm{Ws}[PubK^{mult}_{\mathcal{A},\Pi}(n) = 1] - \frac{1}{2} \leq t \cdot \mathrm{negl}(n)$. $\square$

Von fester zu beliebiger Nachrichtenlänge

Von fester zu beliebiger Nachrichtenlänge

- Sei Π ein Verschlüsselungsverfahren mit Klartexten aus $\{0,1\}^n$.
- Splitte $m \in \{0,1\}^*$ 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.