Sicherheit von ElGamal

Satz CPA-Sicherheit ElGamal

ElGamal Π ist CPA-sicher unter der DDH-Annahme.

Beweis:

- Sei $\mathcal{A}$ ein Angreifer auf ElGamal Π mit Erfolgsws
$$\epsilon(n) := \mathrm{Ws}[PubK^{cpa}_{\mathcal{A},\Pi}(n) = 1].$$
- Wir konstruieren mittels $\mathcal{A}$ einen Unterscheider D zum Unterscheiden von DDH-Instanzen
$$(q, g, g^x, g^y, g') \text{ mit } g' = g^{xy} \text{ oder } g' = g^z.$$

Unterscheider für DDH durch $\mathcal{A}$

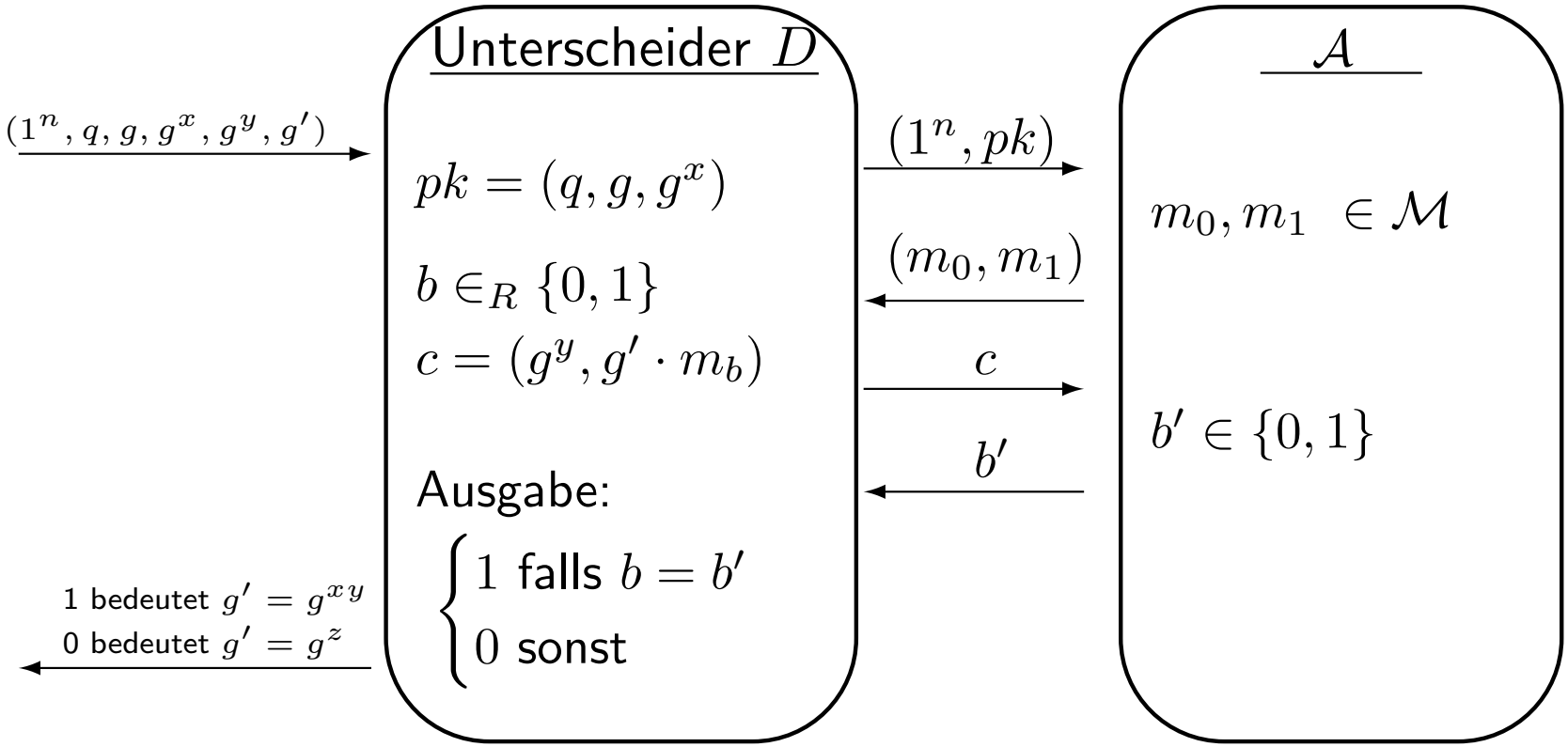
Algorithmus DDH-Unterscheider D

EINGABE: (q, g, g^x, g^y, g')

1. Setze $pk = (G, q, g, g^x)$.
2. $(m_0, m_1) \leftarrow \mathcal{A}(pk)$.
3. Wähle $b \in_R \{0, 1\}$ und berechne $b' \leftarrow \mathcal{A}(g^y, g' \cdot m_b)$.
4. Falls $b' = b$ Ausgabe 1, sonst Ausgabe 0.

AUSGABE: $\begin{cases} 1 & \text{wird interpretiert als } g' = g^{xy} \\ 0 & \text{wird interpretiert als } g' = g^z \end{cases}$.

DDH-Unterscheider mit Angreifer $\mathcal{A}$



Analyse von D

Fall 1: DDH-Tupel, d.h. $g' = g^{xy}$.

- $c = (g^y, g^{xy} \cdot m_b)$ ist identisch zu ElGamal-Chiffretexten verteilt.
- D.h. $\mathrm{Ws}[D(q, g, g^x, g^y, g^{xy}) = 1] = \mathrm{Ws}[PubK_{\mathcal{A},\Pi}(n) = 1] = \epsilon(n)$.

Fall 2: kein DDH-Tupel, d.h. $g' = g^z$ für $z \in_R \mathbb{Z}_q$.

- Chiffretext $c = (c_1, c_2)$ ist von der Form $(g^y, g^z \cdot m_b)$.
- c_2 ist identisch verteilt zu ONE TIME ELEMENT.
- Die erste Komponente c_1 ist unabhängig von c_2, d.h.

$$\mathrm{Ws}[PrivK_{\mathcal{A},\Pi}(n) = 1] = \tfrac{1}{2}.$$

- Es folgt $\mathrm{Ws}[D(G, q, g, g^x, g^y, g^z) = 1] = \mathrm{Ws}[PubK_{\mathcal{A},\Pi}(n) = 1] = \frac{1}{2}$.

Aus der DDH-Annahme folgt

$$\begin{aligned} \mathrm{negl}(n) &\geq |\mathrm{Ws}[D(G, q, g, g^x, g^y, g^z) = 1] - \mathrm{Ws}[D(G, q, g, g^x, g^y, g^{xy}) = 1]| \\ &= \left|\frac{1}{2} - \epsilon(n)\right|. \end{aligned}$$

Damit gilt $\epsilon(n) \leq \frac{1}{2} + \mathrm{negl}(n)$. □

Parameterwahl bei ElGamal

Einbetten von Nachrichten $\mathbf{m}' \in \{\mathbf{0},\mathbf{1}\}^*$

- Beliebte Parameterwahl: $\mathbb{Z}_p^*$, $p = 2q + 1$ mit p, q prim.
- D.h. p ist eine sogenannte starke Primzahl.
- **Ziel:** Konstruktion einer Untergruppe G mit Ordnung q.

- Quadrieren $\mathbb{Z}_p^* \to \mathbb{Z}_p^*$, $x \mapsto x^2$ ist eine $(2:1)$-Abbildung.
- Urbilder $x, p - x$ kollidieren, genau eines ist in $[\frac{p-1}{2}] = [q]$.
- Wir bezeichnen den Bildraum mit QR_p.
- QR_p ist Untergruppe von $\mathbb{Z}_p^*$ mit Ordnung q.
- Wählen g als Generator von QR_p. Sei $|q| = n$.
- Interpretieren $m' \in \{0,1\}^{n-1}$ als natürliche Zahl kleiner q.
- Es gilt $m' + 1 \in [q]$. Einbettung von m' ist $m = (m' + 1)^2 \bmod p$.
- Umkehren der Einbettung ist effizient berechenbar.

CPA-Sicherheit ist ungenügend

Definition CCA (informal)

CCA (=Chosen Ciphertext Attack) ist ein Angriff, bei dem der Angreifer sich Chiffretext seiner Wahl entschlüsseln lassen kann.

Beispiele in denen CPA-Sicherheit nicht genügt:

- Eve fängt verschlüsselte Email $c = Enc(m)$ an Bob ab.
- Eve verschickt c selbst an Bob.
- Bob antwortet Eve und hängt dabei m an die Antwort an.
- D.h. Bob fungiert als Entschlüsselungsorakel.

- Alice und Eve nehmen als Bieter an einer Auktion von Bob teil.
- Alice sendet ihr Gebot $c = Enc(m)$ verschlüsselt an Bob.
- *Enc* soll CPA-sicher sein, d.h. Eve erhält keine Information über m.
- **Frage:** Ist es Eve möglich, $c' = Enc(2m)$ aus c zu berechnen, ohne m zu kennen, und damit Alice zu überbieten? (Malleability)
- Es gilt: CCA-Sicherheit impliziert Non-Malleability. (ohne Beweis)

CCA Ununterscheidbarkeit

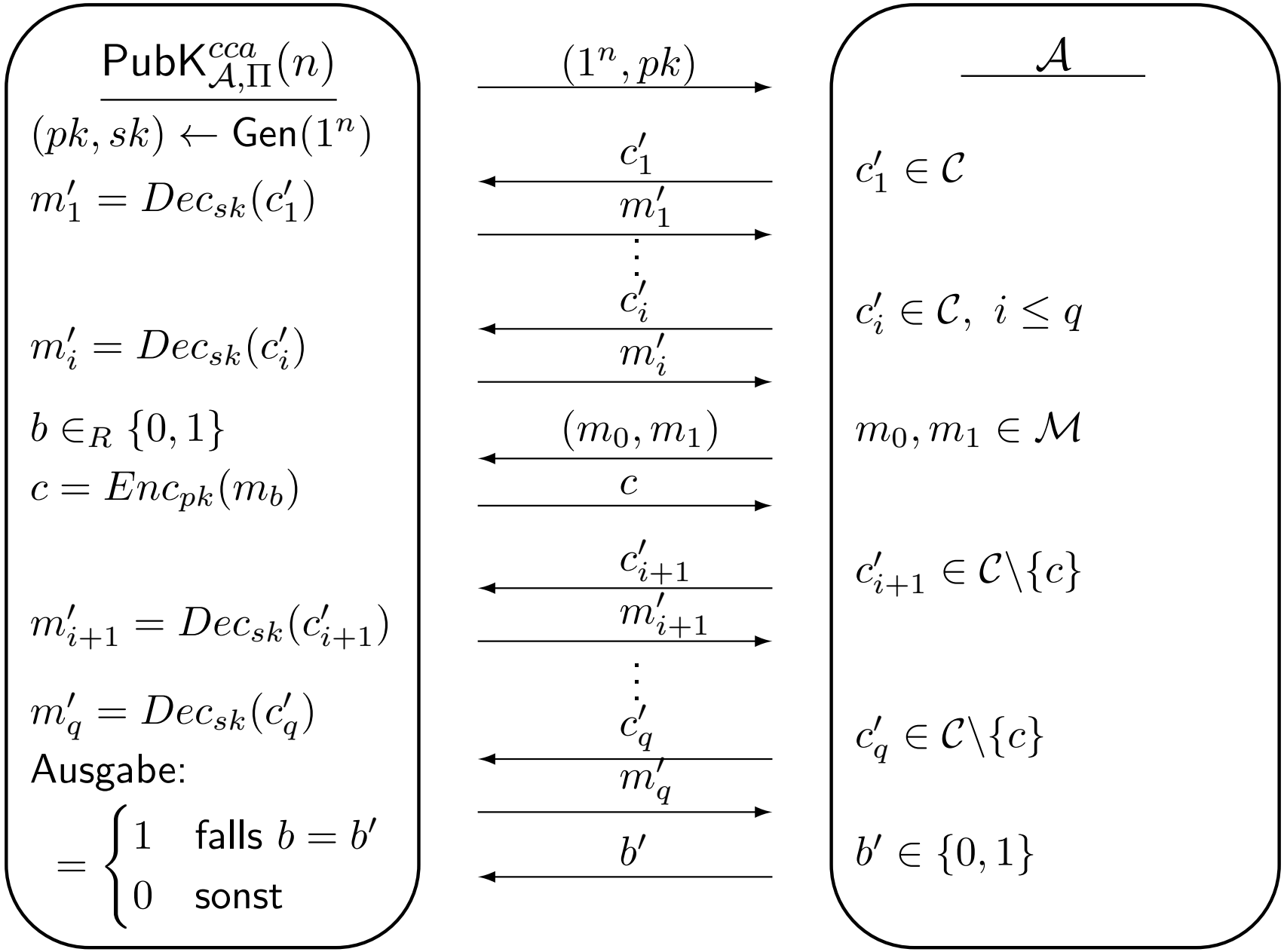
Spiel CCA Ununterscheidbarkeit von Chiffretexten $PubK^{cca}_{\mathcal{A},\Pi}(n)$

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

1. $(pk, sk) \leftarrow Gen(1^n)$
2. $(m_0, m_1) \leftarrow \mathcal{A}^{Dec_{sk}(\cdot)}(pk)$, wobei $Dec_{sk}(\cdot)$ ein Entschlüsselungsorakel für $\mathcal{A}$ für beliebige Chiffretexte ist.
3. Wähle $b \in_R \{0, 1\}$. Verschlüssele $c \leftarrow Enc_{pk}(m_b)$.
4. $b' \leftarrow \mathcal{A}^{Dec_{sk}(\cdot)}(c)$, wobei $\mathcal{A}$ beliebige Chiffretexte $c' \neq c$ durch das Orakel $Dec_{sk}(\cdot)$ entschlüsseln lassen darf.
5. $$PubK^{cca}_{\mathcal{A},\Pi}(n) = \begin{cases} 1 & \text{für } b = b' \\ 0 & \text{sonst} \end{cases}$$

Anmerkungen:

- Zusätzlich zum Verschlüsselungs-Orakel bei CPA besitzt $\mathcal{A}$ bei CCA ein weiteres Entschlüsselungs-Orakel $Dec_{sk}(\cdot)$.
- Falls $\mathcal{A}$ in Schritt 4 auch c entschlüsseln darf, ist das Spiel trivial.


$\mathsf{PubK}^{cca}_{\mathcal{A},\Pi}(n)$
$(pk, sk) \leftarrow \mathsf{Gen}(1^n)$
$m'_1 = Dec_{sk}(c'_1)$
$m'_i = Dec_{sk}(c'_i)$
$b \in_R \{0,1\}$
$c = Enc_{pk}(m_b)$
$m'_{i+1} = Dec_{sk}(c'_{i+1})$
$m'_q = Dec_{sk}(c'_q)$
Ausgabe:
$= \begin{cases} 1 & \text{falls } b = b' \\ 0 & \text{sonst} \end{cases}$
$(1^n, pk)$
c'_1
m'_1
c'_i
m'_i
(m_0, m_1)
c
c'_{i+1}
m'_{i+1}
c'_q
m'_q
b'
$\mathcal{A}$
$c'_1 \in \mathcal{C}$
$c'_i \in \mathcal{C},\ i \leq q$
$m_0, m_1 \in \mathcal{M}$
$c'_{i+1} \in \mathcal{C} \backslash \{c\}$
$c'_q \in \mathcal{C} \backslash \{c\}$
$b' \in \{0,1\}$

CCA-Sicherheit

Definition CCA-Sicherheit

Ein Verschlüsselungsverfahren Π heißt *CCA-sicher* (bzw. besitzt *ununterscheidbare Chiffretexte unter CCA*), falls für alle ppt Angreifer $\mathcal{A}$ gilt $\mathrm{Ws}[PubK^{cca}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathrm{negl}(n)$.

CCA Angriff und Malleability von Textbuch RSA

CCA Angriff auf Textbuch RSA

- Wollen $c = m^e \bmod N$ entschlüsseln.
- Man beachte: c darf nicht direkt angefragt werden.
- Berechne $c' = c \cdot r^e = (mr)^e \bmod N$ für $r \in \mathbb{Z}_N^* \setminus \{1\}$.
- Berechne $mr \leftarrow Dec_{sk}(c')$ mittels Entschlüsselungs-Orakel.
- Berechne $mr \cdot r^{-1} = m \bmod N$.

Malleability von Textbuch RSA

- Voriger Angriff zeigt: Für $c = m^e \bmod N$ kann die Verschlüsselung von mr berechnet werden, ohne m selbst zu kennen.
- D.h. Textbuch RSA ist malleable.

CCA Angriff und Malleability von ElGamal

Praktischer CCA-Angriff auf Padded RSA Variante PKCS #1 v1.5

- Bleichenbacher Angriff: Sende adaptiv Chiffretexte an Server.
- Falls die Entschlüsselung nicht das korrekte Format besitzt, sendet der Server eine Fehlermeldung zurück.
- Genügt, um einen beliebigen Chiffretext c zu entschlüsseln.

CCA Angriff auf ElGamal

- Ziel: Entschlüssele $c = (g^y, g^{xy} \cdot m)$.
- Lasse $c' = (g^y, g^{xy} \cdot m \cdot r)$ für $r \in G \setminus \{1\}$ entschlüsseln.
- Berechne $mr \cdot r^{-1} = m$.
- ElGamal ist malleable, da c' korrekte Verschlüsselung von mr.

Cramer-Shoup Verschlüsselungsverfahren (1998)

Definition Cramer-Shoup Verschlüsselungsverfahren Π_{CS}

Sei n ein Sicherheitsparameter.

1. **Gen** : $(q, g_1) \leftarrow \mathcal{G}(1^n)$, wobei g_1 eine Gruppe G der Ordnung q generiert. Wähle $\omega, x_1, x_2, y_1, y_2, z_1, z_2 \in_R \mathbb{Z}_q$, $s \in_R \{0,1\}^n$ und berechne $g_2 \leftarrow g_1^{\omega}$, $X = g_1^{x_1} g_2^{x_2}$, $Y = g_1^{y_1} g_2^{y_2}$, $Z = g_1^{z_1} g_2^{z_2}$.
   Schlüssel: $pk = (q, g_1, g_2, X, Y, Z, s)$, $sk = (x_1, x_2, y_1, y_2, z_1, z_2)$
2. **Enc** : Für eine Nachricht $m \in G$ wähle ein $r \in_R \mathbb{Z}_q$ und berechne
   $$c = (c_1, c_2, c_3, c_3) = (g_1^r, g_2^r, Z^r \cdot m, (X^t Y)^r), mit\ t = H_s(c_1, c_2, c_3)$$
3. **Dec** : Für einen Chiffretext $c = (c_1, c_2, c_3, c_4)$ berechne $m := \frac{c_3}{c_1^{z_1} c_2^{z_2}}$, falls $c_4 = c_1^{x_1 t + y_1} c_2^{x_2 t + y_2}$ gilt.

- **Korrektheit:** $\frac{c_3}{c_1^{z_1} c_2^{z_2}} = \frac{Z^r \cdot m}{(g_1^r)^{z_1} (g_2^r)^{z_2}} = \frac{Z^r \cdot m}{(g_1^{z_1} g_2^{z_2})^r} = m$ und
  $c_1^{x_1 t + y_1} c_2^{x_2 t + y_2} = (c_1^{x_1} c_2^{x_2})^t c_1^{y_1} c_2^{y_2} = (X^t Y)^r = c_4$.

Cramer-Shoup

Satz (ohne Beweis) CCA-Sicherheit Cramer-Shoup

Wenn die DDH-Annahme gilt und H kollisionsresistent ist, dann ist Π_{CS} CCA-sicher.

Anmerkungen:

- Erstes effizientes CCA-sicheres Verfahren (1998).
- Chiffretexte sind 3mal so lang wie bei ElGamal.
- Sicherheitsbeweis von Cramer-Shoup ist nicht-trivial.
- Verbesserung: Kurosawa-Desmedt Verfahren.
- Später in der Vorlesung: CCA-sichere Verfahren im sogenannten Random Oracle Modell.