

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 Verschlüsselungsurakel $Enc_k(\cdot)$.
- Notation für die Fähigkeit des Orakelzugriffs: $\mathcal{A}^{Enc_k(\cdot)}$.

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

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

Definition CPA Sicherheit

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

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

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

Notation: Wir bezeichnen Π als *CPA sicher*.

CPA-Unsicherheit deterministischer Verschlüsselung

Satz Unsicherheit deterministischer Verschlüsselung

Sei $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ 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 $c := \text{Enc}_k(m_b)$ für $b \in_R \{0, 1\}$.
- ③ Stelle Orakelanfrage $c_0 := \text{Enc}_k(m_0)$.

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

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

Mult-CPA Spiel

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

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

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

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

Definition Mult-CPA Sicherheit

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

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

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

$$\frac{1}{2} \text{Ws}[\mathcal{A}(\text{Enc}_k(m_0^1), \text{Enc}_k(m_0^2)) = 0] + \frac{1}{2} \text{Ws}[\mathcal{A}(\text{Enc}_k(m_1^1), \text{Enc}_k(m_1^2)) = 1].$$

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

$$\begin{aligned} & \frac{1}{2} \text{Ws}[\mathcal{A}(\text{Enc}_k(m_0^1), \text{Enc}_k(m_0^2)) = 0] + \frac{1}{2} \text{Ws}[\mathcal{A}(\text{Enc}_k(m_1^1), \text{Enc}_k(m_1^2)) = 1] \\ & + \frac{1}{2} \left(\text{Ws}[\mathcal{A}(\text{Enc}_k(m_0^1), \text{Enc}_k(m_1^2)) = 0] + \text{Ws}[\mathcal{A}(\text{Enc}_k(m_0^1), \text{Enc}_k(m_1^2)) = 1] \right) \end{aligned}$$

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

Betrachten der Hybride

Lemma

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

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

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

Strategie von CPA Angreifer $\mathcal{A}'$

EINGABE: 1^n und Orakelzugriff $\text{Enc}_k(\cdot)$

- 1 $\mathcal{A}'$ gibt 1^n und Orakelzugriff $\text{Enc}_k(\cdot)$ an $\mathcal{A}$ weiter.
- 2 $(M_0, M_1) \leftarrow \mathcal{A}^{\text{Enc}_k(\cdot)}(1^n)$ 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 $c := \text{Enc}_k(m_b^2)$.
- 4 $b' \leftarrow \mathcal{A}(\text{Enc}_k(m_0^1), c)$.

AUSGABE: b'

- $\text{Ws}[\mathcal{A}'(\text{Enc}_k(m_0^2)) = 0] = \text{Ws}[\mathcal{A}((\text{Enc}_k(m_0^1), \text{Enc}_k(m_0^2))) = 0]$ und
- $\text{Ws}[\mathcal{A}'(\text{Enc}_k(m_1^2)) = 1] = \text{Ws}[\mathcal{A}((\text{Enc}_k(m_0^1), \text{Enc}_k(m_1^2))) = 1]$. 

Fortsetzung Hybridtechnik

Beweis(Fortsetzung):

- CPA Sicherheit von Π bei einzelnen Nachrichten impliziert

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

- Analog kann gezeigt werden, dass

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

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

Von fester zu beliebiger Nachrichtenlänge

- Beweistechnik für allgemeines t : Definiere für $0 \leq i \leq t$ Hybride $C^{(i)} = (Enc_k(m_0^1), \dots, Enc_k(m_0^i), Enc_k(m_1^{i+1}), \dots, Enc_k(m_1^t))$.
- $Ws[PrivK_{\mathcal{A}, \Pi}^{mult-cpa}(n) = 1] = \frac{1}{2} \cdot Ws[\mathcal{A}(C^{(t)}) = 0] + \frac{1}{2} \cdot Ws[\mathcal{A}(C^{(0)}) = 1]$.
- $\mathcal{A}'$ 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 $Pr[PrivK_{\mathcal{A}, \Pi}^{mult-cpa}(n)] \leq \frac{1}{2} + t \cdot \text{negl}(n) \quad \square_{\text{Satz}}$.

Von fester zu beliebiger Nachrichtenlänge

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

Zufallsfunktionen

Definition Echte Zufallsfunktionen:

Sei $Func_n = \{f \mid f : \{0, 1\}^n \rightarrow \{0, 1\}^n\}$. Wir bezeichnen $f \in_R Func_n$ als *echte Zufallsfunktion* auf n Bits.

Anmerkungen:

- Können $f \in Func_n$ mittels vollständiger Wertetabelle beschreiben.
- Damit kann f als Bitstring der Länge $n \cdot 2^n$ dargestellt werden:
 n Bits pro $f(x)$ für alle $x \in \{0, 1\}^n$.
- Es gibt $2^{n \cdot 2^n}$ Strings dieser Länge $n \cdot 2^n$, d.h. $|Func_n| = 2^{n \cdot 2^n}$.

Definition längenerhaltende, schlüsselabhängige Funktion

Sei F ein pt Algorithmus. F heißt *längenerhaltende, schlüsselabhängige Funktion* falls F eine Fkt. $\{0, 1\}^m \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ berechnet.

Notation: $F_k(x) := F(k, x)$, wobei k der Schlüssel ist.

Anmerkung:

- Zur Übersichtlichkeit der Notation verwenden wir stets $m = n$.

Pseudozufallsfunktion

Definition Pseudozufallsfunktion

Sei F ein längenerhaltende, schlüsselabhängige Funktion. Wir bezeichnen F als *Pseudozufallsfunktion*, falls für alle ppt D gilt

$$|\mathsf{Ws}[D^{F_k(\cdot)}(1^n) = 1] - \mathsf{Ws}[D^{f(\cdot)}(1^n) = 1]| \leq \mathsf{negl}(n),$$

wobei $k \in_R \{0, 1\}^n$ und $f \in_R \mathsf{Func}_n$.

Anmerkungen:

- Die Beschreibungslänge von f ist $n2^n$ Bits, d.h. exponentiell in n .
- Daher erhält ein ppt D nicht f , sondern Orakelzugriff auf f und F_k .
- D kann nur polynomiell viele Anfragen an sein Orakel stellen.
- Danach muss D entscheiden, ob sein Orakel einer echten Zufallsfunktion oder einer Pseudozufallsfunktion entspricht.