

Existenz und Verschlüsselung mit Pseudozufallsfkt

Fakt Existenz von Pseudozufallsfunktionen

Pseudozufallsfunktionen existieren gdw Pseudozufallsgeneratoren existieren.

⇒: siehe Übung

Algorithmus Verschlüsselung Π_B

Sei F eine längenerhaltende, schlüsselabhängige Funktion auf n Bits. Wir definieren $\Pi_B = (Gen, Enc, Dec)$ für Nachrichten der Länge n .

- 1 **Gen:** Wähle $k \in_R \{0, 1\}^n$.
- 2 **Enc:** Für $m \in \{0, 1\}^n$ wähle $r \in_R \{0, 1\}^n$ und berechne
$$c := (r, F_k(r) \oplus m).$$
- 3 **Dec:** Für $c = (c_1, c_2) \in \{0, 1\}^n \times \{0, 1\}^n$ berechne
$$m := F_k(c_1) \oplus c_2.$$

Sicherheit von Π_B

Satz Sicherheit von Π_B

Sei F eine Pseudozufallsfunktion. Dann ist Π_B CPA-sicher.

Intuition:

- $F_k(r)$ ist nicht unterscheidbar von n -Bit Zufallsstring.
- D.h. in der zweiten Komponente ist die Verteilung ununterscheidbar von einem One-Time Pad.
- Vorsicht: Benötigen, dass r nicht wiederverwendet wird.

Beweis:

- Sei \mathcal{A} ein CPA-Angreifer mit Vorteil $\epsilon(n)$.
- Konstruieren mittels \mathcal{A} einen Unterscheider D für $F_k(\cdot)$ und $f(\cdot)$.

Unterscheider D

Algorithmus Unterscheider D

EINGABE: 1^n , $\mathcal{O} : \{0, 1\}^n \leftarrow \{0, 1\}^n$ (mit $\mathcal{O} = F_k(\cdot)$ oder $\mathcal{O} = f(\cdot)$)

- 1 Beantworte Verschlüsselungsanfragen $Enc_k(m'_i)$ von \mathcal{A} wie folgt:
Wähle $r_i \in_R \{0, 1\}^n$ und sende $(r_i, \mathcal{O}(r_i) \oplus m)$ an \mathcal{A} .
- 2 Beantworte Challenge (m_0, m_1) von \mathcal{A} wie folgt:
Wähle $r \in_R \{0, 1\}^n$, $b \in_R \{0, 1\}$ und sende $(r, \mathcal{O}(r) \oplus m_b)$ an \mathcal{A} .
- 3 Erhalte nach weiteren Verschlüsselungsanfragen von \mathcal{A} Bit b' .

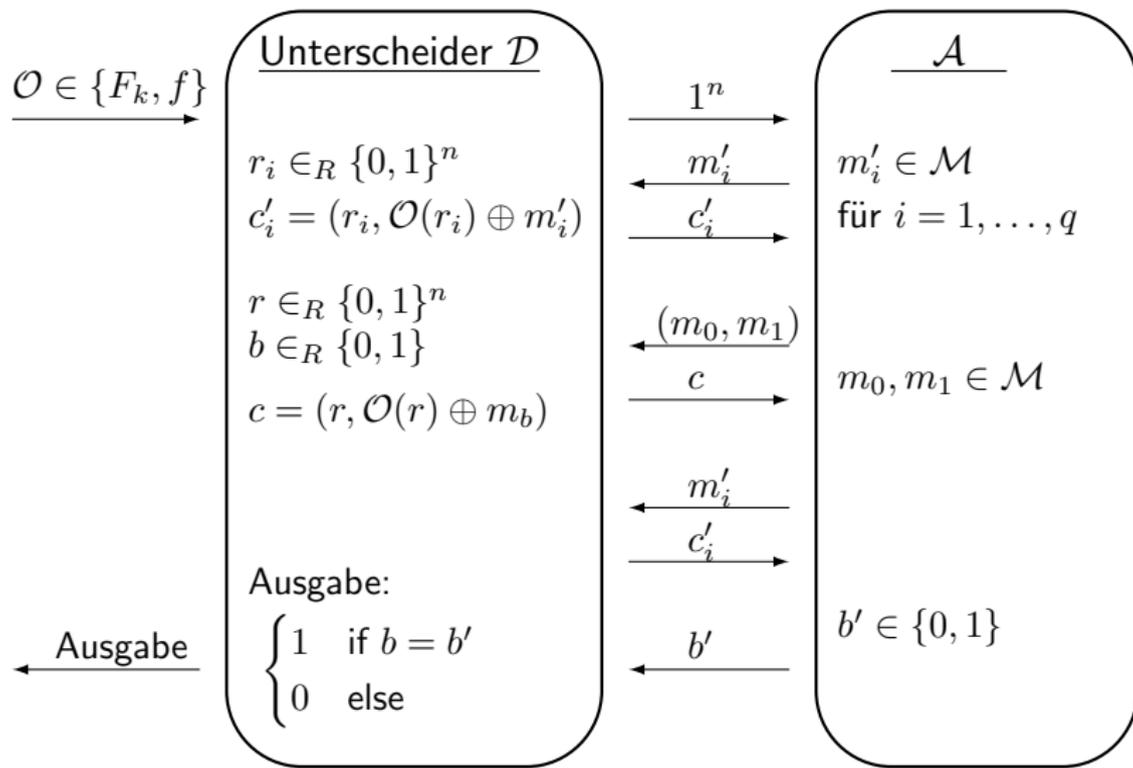
AUSGABE: $= \begin{cases} 1 & \text{falls } b' = b, \text{ Interpretation: } \mathcal{O} = F_k(\cdot) \\ 0 & \text{sonst, Interpretation: } \mathcal{O} = f(\cdot) \end{cases}$.

Fall 1: $\mathcal{O} = F_k(\cdot)$, d.h. wir verwenden eine Pseudozufallsfunktion.

- Dann ist die Verteilung von \mathcal{A} identisch zu Π_B . Damit gilt

$$\mathbb{W}_S[D^{F_k(\cdot)}(1^n) = 1] = \mathbb{W}_S[\text{PrivK}_{\mathcal{A}, \Pi_B}^{\text{cpa}}(n) = 1] = \frac{1}{2} + \epsilon(n).$$

Unterscheider D



Verwenden einer echten Zufallsfunktion

Fall 2: $\mathcal{O} = f(\cdot)$, d.h. wir verwenden eine echte Zufallsfunktion.

- Sei Π' das Protokoll Π_B unter Verwendung von $f(\cdot)$ statt $F_k(\cdot)$.
- Sei *Repeat* das Ereignis, dass r in einer der Verschlüsselungsanfragen verwendet wurde.
- Für alle Angreifer \mathcal{A} gilt $\text{Ws}[\text{PrivK}_{\mathcal{A}, \Pi'}^{\text{cpa}}(n) = 1]$

$$\begin{aligned} &= \text{Ws}[\text{PrivK}_{\mathcal{A}, \Pi'}^{\text{cpa}}(n) = 1 \cap \text{Repeat}] + \text{Ws}[\text{PrivK}_{\mathcal{A}, \Pi'}^{\text{cpa}}(n) = 1 \cap \overline{\text{Repeat}}] \\ &\leq \text{Ws}[\text{Repeat}] + \text{Ws}[\text{PrivK}_{\mathcal{A}, \Pi'}^{\text{cpa}}(n) = 1 \mid \overline{\text{Repeat}}] \end{aligned}$$

- Ein ppt Angreifer \mathcal{A} stelle insgesamt polynomiell viele Anfragen.
- Sei $q(n)$ die Anzahl der Anfragen. Dann gilt

$$\begin{aligned} \text{Ws}[\text{Repeat}] &= \text{Ws}[r = r_1 \cup \dots \cup r = r_q] \\ &\leq \text{Ws}[r = r_1] + \dots + \text{Ws}[r = r_q] = \frac{q}{2^n} = \text{negl}(n). \end{aligned}$$

Fall 2: (Fortsetzung)

- Aufgrund der perfekten Sicherheit des One-Time Pads gilt

$$\text{Ws}[PrivK_{\mathcal{A}, \Pi'}^{cpa}(n) = 1 \mid \overline{Repeat}] = \frac{1}{2}.$$

- Es folgt $\text{Ws}[D^{f(\cdot)}(1^n) = 1] = \text{Ws}[PrivK_{\mathcal{A}, \Pi'}^{cpa}(n) = 1] \leq \frac{1}{2} + \text{negl}(n)$.

- Aus der Pseudozufälligkeit von F folgt insgesamt

$$\text{negl}(n) \geq \left| \underbrace{\text{Ws}[D^{F_k(\cdot)}(1^n) = 1]}_{\frac{1}{2} + \epsilon(n)} - \underbrace{\text{Ws}[D^{f(\cdot)}(1^n) = 1]}_{\leq \frac{1}{2} + \text{negl}(n)} \right|.$$

- Es folgt $\epsilon \leq \text{negl}(n)$ für alle polynomiellen Angreifer \mathcal{A} .

Nachrichten beliebiger Länge

Algorithmus Verschlüsselung Π'_B

Sei F eine längenerhaltende, schlüsselabhängige Funktion auf n Bits. Wir definieren $\Pi'_B = (Gen, Enc, Dec)$ für Nachrichten $m \in \{0, 1\}^*$.

- 1 **Gen:** Wähle $k \in_R \{0, 1\}^n$.
- 2 **Enc:** Für $m = m_1 \dots m_\ell$ mit $m_i \in \{0, 1\}^n$ wähle r_1, \dots, r_ℓ mit $r_i \in_R \{0, 1\}^n$ und berechne

$$c := (r_1, \dots, r_\ell, F_k(r_1) \oplus m_1, \dots, F_k(r_\ell) \oplus m_\ell).$$

- 3 **Dec:** Für $c = (c_1, \dots, c_{2\ell}) \in (\{0, 1\}^n)^{2\ell}$ berechne

$$m := F_k(c_1) \oplus c_{\ell+1} \dots F_k(c_\ell) \oplus F_k(c_{2\ell}).$$

CPA-Sicherheit von Π'_B

Satz CPA-Sicherheit von Π'_B

Sei F eine Pseudozufallsfunktion. Dann ist Π'_B CPA-sicher.

Beweis:

- Aus der CPA-Sicherheit von Π_B folgt die mult-CPA Sicherheit von Π_B und damit die CPA-Sicherheit von Π'_B .

Nachteil: Chiffertexte sind doppelt so lang wie Klartexte (Nachrichtenexpansion 2).

Pseudozufallspermutationen

Definition schlüsselabhängige Permutation

Seien F, F^{-1} ppt Algorithmen. F heißt *schlüsselabhängige Permutation* auf n Bits falls

- 1 F berechnet eine Funktion $\{0, 1\}^m \times \{0, 1\}^n \rightarrow \{0, 1\}^n$, so dass für alle $k \in \{0, 1\}^m$ die Funktion $F_k(\cdot)$ eine Bijektion ist.
- 2 $F_k^{-1}(\cdot)$ berechnet die Umkehrfunktion von $F_k(\cdot)$.

Definition Pseudozufallspermutation

Sei F eine schlüsselabhängige Permutation auf n Bits. Wir bezeichnen F als *Pseudozufallspermutation*, falls für alle ppt D gilt

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

mit $k \in_R \{0, 1\}^m$ und $f \in_R \text{Perm}_n$, wobei Perm_n die Menge aller Permutationen auf n Bits ist.

Starke Pseudozufallspermutationen

Satz Pseudozufallspermutationen und Pseudozufallsfunktionen

Jede Pseudozufallspermutation ist eine Pseudozufallsfunktion.

Beweis: Übung.

Definition Starke Pseudozufallspermutation (Blockchiffre)

Sei F eine schlüsselabhängige Permutation auf n Bits. Wir bezeichnen F als *starke Pseudozufallspermutation (Blockchiffre)*, falls für alle ppt D gilt

$$\left| \mathbb{W}_S[D^{F_k(\cdot), F_k^{-1}(\cdot)}(1^n) = 1] - \mathbb{W}_S[D^{f(\cdot), f^{-1}(\cdot)}(1^n) = 1] \right| \leq \text{negl}(n),$$

mit $k \in_R \{0, 1\}^n$ und $f \in_R \text{Perm}_n$.

Blockchiffren als kryptographische Primitive

Anmerkungen: Blockchiffren

- Praktische Realisierungen von starken Pseudozufallspermutationen bezeichnet man als *Blockchiffren*.
- Wir haben gesehen, dass Blockchiffren $F_k(\cdot)$ zur Konstruktion CPA-sicherer Verschlüsselung verwendet werden können.
- Vorsicht: Blockchiffren selbst sind keine sicheren Verschlüsselungsverfahren.
- $c := F_k(m)$ ist eine deterministische, unsichere Verschlüsselung.
- D.h. wir benötigen einen Randomisierungsprozess bei Enc.

Bsp: DES (Data Encryption Standard, 1976)

- $F : \{0, 1\}^{56} \times \{0, 1\}^{64} \rightarrow \{0, 1\}^{64}$
- Problem des zu kleinen Schlüsselraums
- bester bekannter KPA Angriff mit 2^{43} Klartexten

AES (Advanced Encryption Standard, 2002)

- $F : \{0, 1\}^k \times \{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$ mit $k \in \{128, 192, 256\}$
- Derzeit kein erfolgreicher Angriff bekannt.