Ununterscheidbarkeit von Chiffretexten

Spiel Ununterscheidbarkeit von Chiffretexten $PrivK^{eav}_{\mathcal{A},\Pi}(n)$

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

1. $(m_0, m_1) \leftarrow \mathcal{A}$.
2. $k \leftarrow Gen(1^n)$.
3. Wähle $b \in_R \{0,1\}$. $b' \leftarrow \mathcal{A}(Enc_k(m_b))$.
4. $PrivK^{eav}_{\mathcal{A},\Pi}(n) = \begin{cases} 1 & \text{für } b = b' \\ 0 & \text{sonst} \end{cases}$.

Anmerkungen:

- $\mathcal{A}$ wählt die zu verschlüsselnden Nachrichten m_0, m_1 selbst.
- $\mathcal{A}$ gewinnt das Spiel, d.h. $b = b'$, durch Raten von b' mit Ws $\frac{1}{2}$.
- Wir bezeichnen $\mathrm{Ws}[PrivK^{eav}_{\mathcal{A},\Pi}(n) = 1] - \frac{1}{2}$ als Vorteil von $\mathcal{A}$.

Ununterscheidbarkeit von Chiffretexten

$\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}(n)$		$\mathcal{A}$
$k \leftarrow \mathsf{Gen}(1^n)$	$\xrightarrow{1^n}$	
	$\xleftarrow{(m_0, m_1)}$	$m_0, m_1 \in \mathcal{M}$
$b \in_R \{0,1\}$		
$c \leftarrow \mathsf{Enc}_k(m_b)$	$\xrightarrow{c}$	
Ausgabe:	$\xleftarrow{b'}$	$b' \in \{0,1\}$
$= \begin{cases} 1 & \text{falls } b = b' \\ 0 & \text{sonst} \end{cases}$		

Raten ist optimal

Satz Perfekte Sicherheit und $PrivK^{eav}_{\mathcal{A},\Pi}$

Ein Verschlüsselungsverfahren Π ist perfekt sicher gdw für alle (unbeschränkten) Angreifer $\mathcal{A}$ gilt $\mathrm{Ws}[PrivK^{eav}_{\mathcal{A},\Pi}(n) = 1] = \frac{1}{2}$.

Beweis:

- "$\Leftarrow$": Sei Π nicht perfekt sicher. Dann existieren $m_0, m_1 \in \mathcal{M}$ und $c \in \mathcal{C}$ mit $\mathrm{Ws}[C = c \mid M = m_0] \neq \mathrm{Ws}[C = c \mid M = m_1]$.
- OBdA $\mathrm{Ws}[C = c \mid M = m_0] > \mathrm{Ws}[C = c \mid M = m_1]$.
- Wir definieren den folgenden Angreifer $\mathcal{A}$ für das Spiel $PrivK^{eav}_{\mathcal{A},\Pi}$.

Algorithmus Angreifer $\mathcal{A}$

Algorithmus Angreifer $\mathcal{A}$

EINGABE: $1^n, m_0, m_1, c$

1. Berechne m_0, m_1, c mit $\mathrm{Ws}[C = c | M = m_0] > \mathrm{Ws}[C = c \mid M = m_1]$.
2. Versende Nachrichten m_0, m_1. Erhalte $c' \leftarrow Enc_k(m_b)$.
3. Falls $c' = c$, setze $b' = 0$. Sonst setze $b' \in_R \{0, 1\}$.

AUSGABE: b'

$\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi}(n)$

$k \leftarrow \mathsf{Gen}(1^n)$

$b \in_R \{0, 1\}$

$c' \leftarrow \mathsf{Enc}_k(m_b)$

Ausgabe:

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

$\xrightarrow{1^n}$

$\xleftarrow{(m_0, m_1)}$

$\xrightarrow{c'}$

$\xleftarrow{b'}$

$\mathcal{A}$

Berechne m_0, m_1, c.

Falls $c' = c$, setze $b' = 0$.

Sonst setze $b' \in_R \{0, 1\}$.

Nicht perfekt sicher $\Rightarrow$ Vorteil

Beweis (Fortsetzung):

- Es gilt $\mathrm{Ws}[PrivK^{eav}_{\mathcal{A},\Pi}(n) = 1] = \mathrm{Ws}[\mathcal{A}(Enc(m_b)) = b]$

$$= \frac{1}{2} \cdot \mathrm{Ws}[C \neq c] + \mathrm{Ws}[M = m_0 \mid C = c] \cdot \mathrm{Ws}[C = c]$$

$$= \frac{1}{2}\big(1 - \mathrm{Ws}[C = c]\big) + \mathrm{Ws}[M = m_0 \mid C = c] \cdot \mathrm{Ws}[C = c].$$

- Falls $\mathrm{Ws}[M = m_0 \mid C = c] > \frac{1}{2}$, so folgt $\mathrm{Ws}[PrivK^{eav}_{\mathcal{A},\Pi} = 1] > \frac{1}{2}$.

- Es gilt $\mathrm{Ws}[M = m_0 \mid C = c]$

$$= \frac{\mathrm{Ws}[C = c \mid M = m_0] \cdot \overbrace{\mathrm{Ws}[M = m_0]}^{\frac{1}{2}}}{\sum_{i=0}^{1} \mathrm{Ws}[C = c \mid M = m_i] \cdot \underbrace{\mathrm{Ws}[M = m_i]}_{\frac{1}{2}}}$$

$$= \frac{\mathrm{Ws}[C = c \mid M = m_0]}{\underbrace{\mathrm{Ws}[C = c \mid M = m_0] + \mathrm{Ws}[C = c \mid M = m_1]}_{< 2 \cdot \mathrm{Ws}[C = c \mid M = m_0]}} > \frac{1}{2}.$$

Perfekt sicher $\Rightarrow$ kein Vorteil

Beweis (Fortsetzung): Perfekt sicher $\Rightarrow \mathrm{Ws}[PrivK^{eav}_{\mathcal{A},\Pi} = 1] = \frac{1}{2}$

- Sei Π perfekt sicher. Dann gilt für alle $m_0, m_1 \in \mathcal{M}$, $c \in \mathcal{C}$
  $\mathrm{Ws}[C = c \mid M = m_0] = \mathrm{Ws}[C = c] = \mathrm{Ws}[C = c \mid M = m_1]$.
- D.h. es gilt $\{c \mid c \in Enc_k(m)\} = \mathcal{C}$ für alle $m \in M$.
- Daraus folgt $\mathrm{Ws}[PrivK^{eav}_{\mathcal{A},\Pi} = 1] = \mathrm{Ws}[\mathcal{A}(Enc(m_b)) = b)]$

$$
\begin{aligned}
&= \mathrm{Ws}[b = 0] \cdot \mathrm{Ws}[\mathcal{A}(Enc(m_0)) = 0] + \mathrm{Ws}[b = 1] \cdot \mathrm{Ws}[\mathcal{A}(Enc(m_1)) = 1] \\
&= \frac{1}{2} \cdot \Bigg(\sum_{c \in Enc(m_0)} \mathrm{Ws}[\mathcal{A}(c) = 0 \mid C = c] \cdot \mathrm{Ws}[C = c] \\
&\qquad + \sum_{c \in Enc(m_1)} \underbrace{\mathrm{Ws}[\mathcal{A}(c) = 1 \mid C = c]}_{1 - \mathrm{Ws}[\mathcal{A}(c) = 0 \mid C = c]} \cdot \mathrm{Ws}[C = c] \Bigg) \\
&= \frac{1}{2} \cdot \sum_{c \in \mathcal{C}} \mathrm{Ws}[C = c] = \frac{1}{2}.
\end{aligned}
$$

Computational Security

Perfekte Sicherheit:

- Liefert Sicherheit im informationstheoretischen Sinn, d.h. der Angreifer erhält nicht genügend Information, um zu entschlüsseln.
- Benötigen Schlüssel der Länge aller zu verschlüsselnden Nachrichten. Dies ist unpraktikabel in der Praxis.

Computational Security Ansatz:

- Wir verwenden kurze Schlüssel (z.B. 128 Bit).
- Liefert Sicherheit nur gegenüber ppt Angreifern.
- Unbeschränkte Angreifer können bei KPA-Angriff $\mathcal{K}$ durchsuchen.
- Seien $(m_1, c_1), \ldots, (m_n, c_n)$ die Plaintext/Chiffretext Paare.
- Mit hoher Ws existiert eindeutiges k mit $m_i = Dec_k(c_i)$, $i \in [n]$.
- Mit obigem KPA-Angriff kann der Angreifer in Polynomial-Zeit auch ein einzelnes $k \in \mathcal{K}$ raten, dieses ist korrekt mit Ws $\frac{1}{|\mathcal{K}|}$.
- D.h. ppt Angreifer besitzen nur vernachlässigbare Erfolgsws im Sicherheitsparameter.

Vernachlässigbare Wahrscheinlichkeit

Definition Vernachlässigbare Wahrscheinlichkeit

Eine Funktion $f : \mathbb{N} \rightarrow \mathbb{R}$ heißt *vernachlässigbar*, falls für jedes Polynom p ein $N \in \mathbb{N}$ existiert, so dass für alle $n \geq N$ gilt $f(n) < \frac{1}{p(n)}$.
Notation: $f(n) = \mathrm{negl}(n)$.

Bsp:

- Vernachlässigbare Funktionen: $\frac{1}{2^n}$, $\frac{1}{2^{\sqrt{n}}}$, $\frac{1}{2^{\log^2 n}}$, $\frac{1}{n^{\frac{\log n}{\log \log n}}}$.
- Nicht vernachlässigbare Funktionen: $\frac{1}{n^2}$, $\frac{1}{\log n}$, $\frac{1}{2^{\mathcal{O}(\log n)}}$.

Korollar Komposition vernachlässigbarer Funktionen

Seien f_1, f_2 vernachlässigbare Funktionen. Dann ist

1. $f_1 + f_2$ vernachlässigbar.
2. $q(n) \cdot f_1$ vernachlässigbar für jedes Polynom q.

Sicherheitsbeweis per Reduktion

Annahme: Problem X lässt sich in ppt nur mit Ws $\mathrm{negl}(n)$ lösen.

- Sei Π ein Krypto-Verfahren mit Sicherheitsparameter n.
- Sei $\mathcal{A}$ ein ppt Angreifer auf Π mit Erfolgsws $\epsilon(n)$.
- Wir konstruieren eine polynomielle Reduktion $\mathcal{A}$' für $X \leq_p \mathcal{A}$. (Erinnerung: Diskrete Mathematik II)

Algorithmus Reduktion $\mathcal{A}'$ für $X \leq_p \mathcal{A}$

EINGABE: Instanz x des Problems X

1. Konstruieren aus x Instanz von Π, senden diese an $\mathcal{A}$.
2. Sofern $\mathcal{A}$s Angriff eine Interaktion erfordert (z.B. bei CCA), wird diese von der Reduktion $\mathcal{A}'$ simuliert. $\mathcal{A}$s Sicht soll dabei identisch zu einem realen Angriff sein.
3. $\mathcal{A}$ bricht schließlich Π mittels Ausgabe y' mit Ws $\epsilon(n)$.
4. Verwenden y', um eine Lösung y für die Instanz x zu berechnen.

AUSGABE: Lösung y für x

Sicherheitsbeweis per Reduktion

- Alle Schritte der Reduktion laufen in polynomial-Zeit.
- Angenommen Schritt 4 besitze Erfolgws $\frac{1}{p(n)}$ für ein Polynom $p(n)$.
- Dann besitzt die Reduktion insgesamt Erfolgsws $\frac{\epsilon(n)}{p(n)}$.
- Nach Annahme lässt sich X nur mit Ws $\mathrm{negl}(n)$ lösen.
- D.h. $\frac{\epsilon(n)}{p(n)} \leq \mathrm{negl}(n)$, und damit folgt $\epsilon(n) \leq \mathrm{negl}(n)$.
- Damit besitzt **jeder** Angreifer $\mathcal{A}$ vernachlässigbare Erfolgws.

Reduktionsbeweis bildlich