Prinzipien der modernen Kryptographie – Sicherheit

Prinzip 1 Sicherheitsmodell

Das Sicherheitsmodell (Berechnungsmodell, Angriffstypen, Sicherheitsziele) muss präzise definiert werden.

- Berechnungsmodell: wir müssen das Berechnungsmodell des Angreifers definieren, z.B. eine Beschränkung auf ppt Angreifer.
- Mögliche Angriffstypen: COA, KPA, CPA oder CCA muss definiert werden.

Prinzipien der modernen Kryptographie – Sicherheit

Prinzip 1 Sicherheitsmodell

Das Sicherheitsmodell (Berechnungsmodell, Angriffstypen, Sicherheitsziele) muss präzise definiert werden.

Beispiele für ungenügende Definitionen von Sicherheitzielen

- *Kein Angreifer kann k finden.* Betrachte $Enc_k(\cdot)$, das die Identität berechnet: k wird zum Entschlüsseln nicht benötigt.
- *Kein Angreifer kann die zugrundeliegende Nachricht bestimmen.* Möglicherweise können 90% der Nachricht bestimmt werden.
- *Kein Angreifer erhält Information über den Klartext vom Chiffretext.* Möglicherweise kann der Angreifer zwischen zwei Nachrichten – z.B. JA und NEIN – unterscheiden.
- *Kein Angreifer erhält zusätzliche Information über den Klartext vom Chiffretext.* Gut, erfordert aber Spezifikation des Begriffs zusätzliche Information.

Prinzip 2 – Präzisierung der Annahmen

Prinzip 2 Komplexitätsannahme

Es muss spezifiziert werden, unter welchen Annahmen das System als sicher gilt.

Eigenschaften:

- Annahmen sollten unabhängig von der Kryptographie sein.
- Bsp: Das Faktorisierungsproblem ist nicht in polynomial-Zeit lösbar.
- Bsp: Das Finden von kürzesten Vektoren in Gittern ist nicht in polynomial-Zeit möglich.

Prinzip 3 – Reduktionsbeweis der Sicherheit

Prinzip 3 Beweis der Sicherheit

Wir beweisen, dass unter den gegebenen Annahmen *kein* Angreifer die Sicherheit brechen kann.

Anmerkungen:

- D.h. wir beweisen, dass das System gegen **alle** Angreifer sicher ist, unabhängig von der Herangehensweise des Angreifers!
- Typische Beweisaussage: “Unter Annahme X folgt die Sicherheit von Konstruktion Y bezüglich der Sicherheitsdefinition Z”.
- Der Beweis erfolgt per Reduktion: Ein erfolgreicher Angreifer $\mathcal{A}$ für Y bezüglich Z wird transformiert in einen Algorithmus $\mathcal{B}$, der Annahme X verletzt.

  Bsp: Angreifer $\mathcal{A}$ auf die CCA-Sicherheit einer Verschlüsselung liefert einen Algorithmus $\mathcal{B}$ zum Faktorisieren.

Perfekte Sicherheit

Szenario:

- Angreifer besitzt *unbeschränkte* Berechnungskraft.
- Seien $\mathcal{M}, \mathcal{K}, \mathcal{C}$ versehen mit folgenden Ws-Verteilungen.
  - Sei M eine Zufallsvariable für eine beliebige Ws-Verteilung auf $\mathcal{M}$, d.h. wir ziehen ein $m \in \mathcal{M}$ mit $\mathrm{Ws}[M = m]$.
  - Sei K eine Zufallsvariable induziert durch $K \leftarrow \mathit{Gen}(1^n)$.
  - Sei $C \leftarrow \mathit{Enc}_K(M)$ eine Zufallsvariable für die Ws-Verteilung auf $\mathcal{C}$.
  - K und M sind unabhängig, C hängt von K und M ab.
- Es gelte oBdA $\mathrm{Ws}[M = m] > 0$ und $\mathrm{Ws}[C = c] > 0$ für alle $m \in \mathcal{M}, c \in \mathcal{C}$. (Andernfalls entferne m aus $\mathcal{M}$ bzw. c aus $\mathcal{C}$.)

Definition Perfekte Sicherheit

Ein Verschlüsselungsverfahren $\Pi = (\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ heißt *perfekt sicher*, falls für alle WS-Verteilungen auf $\mathcal{M}$, $m \in \mathcal{M}$, $c \in \mathcal{C}$: $\mathrm{Ws}[M = m \mid C = c] = \mathrm{Ws}[M = m]$.

Interpretation: c liefert dem Angreifer keine Informationen über m.

Verteilung auf Chiffretexten unabhängig vom Plaintext

Satz Chiffretext-Verteilung

Ein Verschlüsselungsverfahren Π ist perfekt sicher gdw $\mathrm{Ws}[C = c \mid M = m] = \mathrm{Ws}[C = c]$ für alle $m \in \mathcal{M}, c \in \mathcal{C}$.

Satz von Beyes: Für zwei Ereignisse A, B mit $\mathrm{Ws}[B] > 0$ gilt:

$$\mathrm{Ws}[A \mid B] = \frac{\mathrm{Ws}[B \mid A] \cdot \mathrm{Ws}[A]}{\mathrm{Ws}[B]}.$$

Beweis:

- "$\Rightarrow$": Sei Π perfekt sicher. Nach dem Satz von Bayes gilt

$$\mathrm{Ws}[C = c \mid M = m] = \frac{\mathrm{Ws}[M = m \mid C = c] \cdot \mathrm{Ws}[C = c]}{\mathrm{Ws}[M = m]} = \mathrm{Ws}[C = c].$$

- "$\Leftarrow$": Aus $\mathrm{Ws}[C = c \mid M = m] = \mathrm{Ws}[C = c]$ folgt mit dem Satz von Bayes $\mathrm{Ws}[M = m \mid C = c] = \mathrm{Ws}[M = m]$.
- Damit ist Π perfekt sicher.

Ununterscheidbarkeit von Verschlüsselungen

Satz Ununterscheidbarkeit von Verschlüsselungen

Ein Verschlüsselungsverfahren Π ist perfekt sicher gdw für alle $m_0, m_1 \in \mathcal{M}$, $c \in \mathcal{C}$ gilt $\mathrm{Ws}[C = c \mid M = m_0] = \mathrm{Ws}[C = c \mid M = m_1]$.

Beweis:

- "$\Rightarrow$": Mit dem Satz auf voriger Folie gilt für perfekt sichere Π
$$\mathrm{Ws}[C = c \mid M = m_0] = \mathrm{Ws}[C = c] = \mathrm{Ws}[C = c \mid M = m_1].$$
- "$\Leftarrow$": Sei $m' \in \mathcal{M}$ beliebig. Es gilt
$$\begin{aligned} \mathrm{Ws}[C = c] &= \sum_{m \in \mathcal{M}} \mathrm{Ws}[C = c \mid M = m] \cdot \mathrm{Ws}[M = m] \\ &= \mathrm{Ws}[C = c \mid M = m'] \cdot \sum_{m \in \mathcal{M}} \mathrm{Ws}[M = m] \\ &= \mathrm{Ws}[C = c \mid M = m']. \end{aligned}$$
- Die perfekte Sicherheit von Π folgt mit dem Satz auf voriger Folie.

Das One-Time Pad (Vernam Verschlüsselung)

Definition One-Time Pad (1918)

Sei $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^\ell$.

1. **Gen:** Ausgabe $k \in_R \{0,1\}^\ell$
2. **Enc:** Für $m \in \{0,1\}^\ell$ berechne $c = Enc_k(m) := m \oplus k$.
3. **Dec:** Für $c \in \{0,1\}^\ell$ berechne $m = Dec_k(c) := c \oplus k$.

Satz Sicherheit des One-Time Pads

Das One-Time Pad ist perfekt sicher gegenüber COA Angriffen.

Beweis:

- Wegen $C = Enc_K(M) = M \oplus K$ gilt für alle $m_0, m_1 \in \mathcal{M}$ und $c \in \mathcal{C}$

$$\begin{aligned} \text{Ws}[C = c \mid M = m_0] &= \text{Ws}[M \oplus K = c \mid M = m_0] = \text{Ws}[K = m_0 \oplus c] \\ &= \frac{1}{2^\ell} = \text{Ws}[C = c \mid M = m_1]. \end{aligned}$$

- Damit ist das One-Time Pad perfekt sicher.

Nachteil: Schlüsselraum ist so groß wie der Nachrichtenraum.

Beschränkungen perfekter Sicherheit

Satz Größe des Schlüsselraums

Sei Π perfekt sicher. Dann gilt $|\mathcal{K}| \geq |\mathcal{M}|$.

Beweis: Angenommen $|\mathcal{K}| < |\mathcal{M}|$.

- Sei M die Gleichverteilung auf $\mathcal{M}$.
- Für $c \in \mathcal{C}$ definiere $D(c) = \{m \mid m = Dec_k(c) \text{ für ein } k \in \mathcal{K}\}$.
- Es gilt $|D(c)| \leq |\mathcal{K}|$, da jeder Schlüssel k höchstens ein m liefert.
- Wegen $|\mathcal{K}| < |\mathcal{M}|$ folgt $|D(c)| < |\mathcal{M}|$. D.h. es gibt ein $m \in \mathcal{M} \setminus D(c)$ mit

$$0 = \mathrm{Ws}[M = m \mid C = c] < \mathrm{Ws}[M = m].$$

- Damit ist Π nicht perfekt sicher.

Satz von Shannon (1949)

Satz von Shannon

Sei $\Pi = (Gen, Enc, Dec)$ mit $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$. Π ist perfekt sicher gdw

1. *Gen* wählt alle $k \in_R \mathcal{K}$
2. Für alle $m \in \mathcal{M}, c \in \mathcal{C}$ existiert genau ein $k \in \mathcal{K}$: $c = Enc_k(m)$.

Beweisidee:

- "$\Leftarrow$": Jedes $m \in \mathcal{M}$ korrespondiert zu genau einem $c \in \mathcal{C}$ via k.
- D.h. m wird zu c verschlüsselt, falls k verwendet wird.
- Damit gilt

$$\mathrm{Ws}[C = c \mid M = m] = \mathrm{Ws}[K = k] = \frac{1}{|\mathcal{K}|} \text{ für alle } m \in \mathcal{M}.$$

- Es folgt $\mathrm{Ws}[C = c \mid M = m_0] = \frac{1}{|\mathcal{K}|} = \mathrm{Ws}[C = c \mid M = m_1]$.
- Damit ist Π perfekt sicher.

Satz von Shannon (1949)

Beweisidee (Fortsetzung):

- "$\Rightarrow$": Sei Π perfekt sicher mit $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$.
- Definiere $S(m) = \{Enc_k(m) \mid k \in \mathcal{K}\}$.
- Für alle (m, c) existiert mindestens ein $k \in \mathcal{K}$ mit $c = Enc_k(m)$. (Sonst: $\exists (m, c)$ mit $c \neq Enc_k(m)$ für alle $k \in \mathcal{K}$. Dann gilt $\mathrm{Ws}[M = m | C = c] = 0 < \mathrm{Ws}[M = m]$. Widerspruch.)
- $\Rightarrow |\mathcal{C}| \leq |S(m)| \leq |\mathcal{C}|$ und deshalb $|S(m)| = |\mathcal{C}| = |\mathcal{K}|$.
- Also: für jedes (m, c) gibt es genau einen Schlüssel $k_{m,c}$ mit $c = Enc_{k_{m,c}}(m)$.
- Daraus folgt für alle m, m'

$$\begin{aligned} \mathrm{Ws}[K = k_{m,c}] &= \mathrm{Ws}[C = c \mid M = m] \\ &= \mathrm{Ws}[C = c \mid M = m'] = \mathrm{Ws}[K = k_{m',c}]. \end{aligned}$$

- D.h. es gilt $\mathrm{Ws}[K = k] = \frac{1}{|\mathcal{K}|}$ für alle $k \in \mathcal{K}$.