Sicherheit Schlüsselaustausch

Definition negl

Eine Funktion $f : \mathbb{N} \to \mathbb{R}^+$ heißt *vernachlässigbar*, falls für jedes Polynom $p(n)$ und alle hinreichend großen n gilt $f(n) < \frac{1}{p(n)}$.
Notation: Wir bezeichnen eine bel. vernachlässigbare Fkt mit $\mathrm{negl}(n)$.

Bsp:

- $\frac{1}{2^n}$, $\frac{1}{2^{\sqrt{n}}}$, $\frac{1}{n^{\log\log n}}$ sind vernachlässigbar.
- $\frac{1}{2^{\mathcal{O}(\log n)}}$ ist nicht vernachlässigbar.
- Es gilt $q(n) \cdot \mathrm{negl}(n) = \mathrm{negl}(n)$ für jedes Polynom $q(n)$.

Definition Sicherheit Schlüsselaustausch

Ein Schlüsselaustausch Protokoll Π ist sicher gegen passive Angriffe, falls für alle probabilistischen Polynomialzeit (ppt) Angreifer $\mathcal{A}$ gilt $\mathrm{Ws}[KE_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathrm{negl}(n)$.

Der Wsraum ist definiert über die zufälligen Münzwürfe von $\mathcal{A}$ und Π.

dlog Problem

Definition Diskrete Logarithmus (dlog) Annahme

Das *Diskrete Logarithmus Problem* ist hart bezüglich $\mathcal{G}$, falls für alle ppt Algorithmen $\mathcal{A}$ gilt

$$|\mathrm{Ws}[\mathcal{A}(G, g, q, g^x) = x]| \leq \mathrm{negl}.$$

Der Wsraum ist definiert bezüglich der zufälligen Wahl von $x \in \mathbb{Z}_q$ und der internen Münzwürfe von $\mathcal{A}$ und $\mathcal{G}$.

dlog Annahme: Das dlog Problem ist hart bezüglich $\mathcal{G}$.

- Unter der dlog Annahme können die geheimen Schlüssel x, y bei Diffie-Hellman nur mit vernachlässigbarer Ws berechnet werden.
- D.h. die dlog Annahme ist eine notwendige Sicherheitsannahme.

CDH Problem

Definition Computational Diffie-Hellman (CDH) Annahme

Das *Computational Diffie-Hellman Problem* ist hart bezüglich $\mathcal{G}$, falls für alle ppt Algorithmen $\mathcal{A}$ gilt $\mathrm{Ws}[A(G, g, q, g^x, g^y) = g^{xy}] \leq \mathrm{negl}$.

Wsraum: zufällige Wahl von $x, y \in \mathbb{Z}_q$, interne Münzwürfe von $\mathcal{A}$, $\mathcal{G}$.

CDH Annahme: Das CDH Problem ist hart bezüglich $\mathcal{G}$.

- Unter der CDH-Annahme kann ein DH-Angreifer Eve den Schlüssel $k_A = g^{xy}$ nur mit vernachlässigbarer Ws berechnen.

Problem:

- Sei CDH schwer, so dass Angreifer Eve k_A nicht berechnen kann.
- Benötigen aber, dass k_A ein zufälliges Gruppenelement in G ist.
- Unterscheiden von g^{xy} und $g^z, z \in_R \mathbb{Z}_q$ könnte einfach sein.

DDH Problem

Definition Decisional Diffie-Hellman (DDH) Annahme

Das *Decisional Diffie-Hellman Problem* ist hart bezüglich $\mathcal{G}$, falls für alle ppt Algorithmen $\mathcal{A}$ gilt

$$|\mathrm{Ws}[\mathcal{A}(G, q, g, g^x, g^y, g^{xy}) = 1] - \mathrm{Ws}[\mathcal{A}(G, q, g, g^x, g^y, g^z) = 1]| \leq \mathrm{negl}.$$

Wsraum: zufällige Wahl von $x, y, z \in \mathbb{Z}_q$, interne Münzwürfe von $\mathcal{A}$, $\mathcal{G}$.

DDH Annahme: Das DDH Problem ist hart bezüglich $\mathcal{G}$.

- Unter der DDH-Annahme kann Eve den DH-Schlüssel g^{xy} nicht von einem zufälligen Gruppenelement unterscheiden.

Sicherheitsbeweis des DH-Protokolls

Satz Sicherheit des Diffie-Hellman Protokolls

Unter der DDH-Annahme ist das DH-Protokoll Π sicher gegen passive Angreifer $\mathcal{A}$.

Beweis: Es gilt $\mathrm{Ws}[KE_{\mathcal{A},\Pi}(n) = 1]$

$$
\begin{aligned}
&= \frac{1}{2} \cdot \mathrm{Ws}[KE_{\mathcal{A},\Pi}(n) = 1 \mid b = 1] + \frac{1}{2} \cdot \mathrm{Ws}[KE_{\mathcal{A},\Pi}(n) = 1 \mid b = 0] \\
&= \frac{1}{2} \cdot \mathrm{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^{xy}) = 1] + \frac{1}{2} \cdot \mathrm{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^z) = 0] \\
&= \frac{1}{2} \cdot \mathrm{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^{xy}) = 1] + \frac{1}{2} \cdot (1 - \mathrm{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^z) = 1] \\
&= \frac{1}{2} + \frac{1}{2} \cdot (\mathrm{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^{xy}) = 1] - \mathrm{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^z) = 1]) \\
&\leq \frac{1}{2} + \frac{1}{2} \cdot |\mathrm{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^{xy}) = 1] - \mathrm{Ws}[\mathcal{A}(G, g, q, g^x, g^y, g^z) = 1]| \\
&\leq \frac{1}{2} + \frac{1}{2} \cdot \mathrm{negl} \quad \text{nach DDH-Annahme.}
\end{aligned}
$$

Public-Key Verschlüsselung

Szenario: Asymmetrische/Public Key Verschlüsselung

- Schlüsselpaar (pk, sk) aus öffentlichem/geheimem Schlüssel.
- Verschlüsselung Enc_{pk} ist Funktion des öffentlichen Schlüssels.
- Entschlüsselung Dec_{sk} ist Funktion des geheimen Schlüssels.
- pk kann veröffentlicht werden, z.B. auf Webseite, Visitenkarte.
- pk kann über öffentlichen (authentisierten) Kanal verschickt werden.

Vorteile:

- Löst Schlüsselverteilungsproblem.
- Erfordert die sichere Speicherung eines einzigen Schlüssels.

Nachteil:

- Heutzutage deutlich langsamer als sym. Verschlüsselung.

Public-Key Verschlüsselung

Definition Public-Key Verschlüsselung

Ein *Public-Key Verschlüsselungsverfahren* ist ein 3-Tupel (Gen, Enc, Dec) von ppt Algorithmen mit

1. $(pk, sk) \leftarrow Gen(1^n)$, wobei pk, sk Länge mindestens n besitzen.
2. $c \leftarrow Enc_{pk}(m)$, wobei m aus dem Nachrichtenraum und c aus dem Chiffretextraum ist.
3. $Dec_{sk}(c)$ liefert Nachricht m oder $\perp$ (Entschlüsselungsfehler). Es gilt $\mathrm{Ws}[Dec_{sk}(Enc_{pk}(m)) = m] = 1 - \mathrm{negl}(n)$.

Ununterscheidbarkeit von Chiffretexten

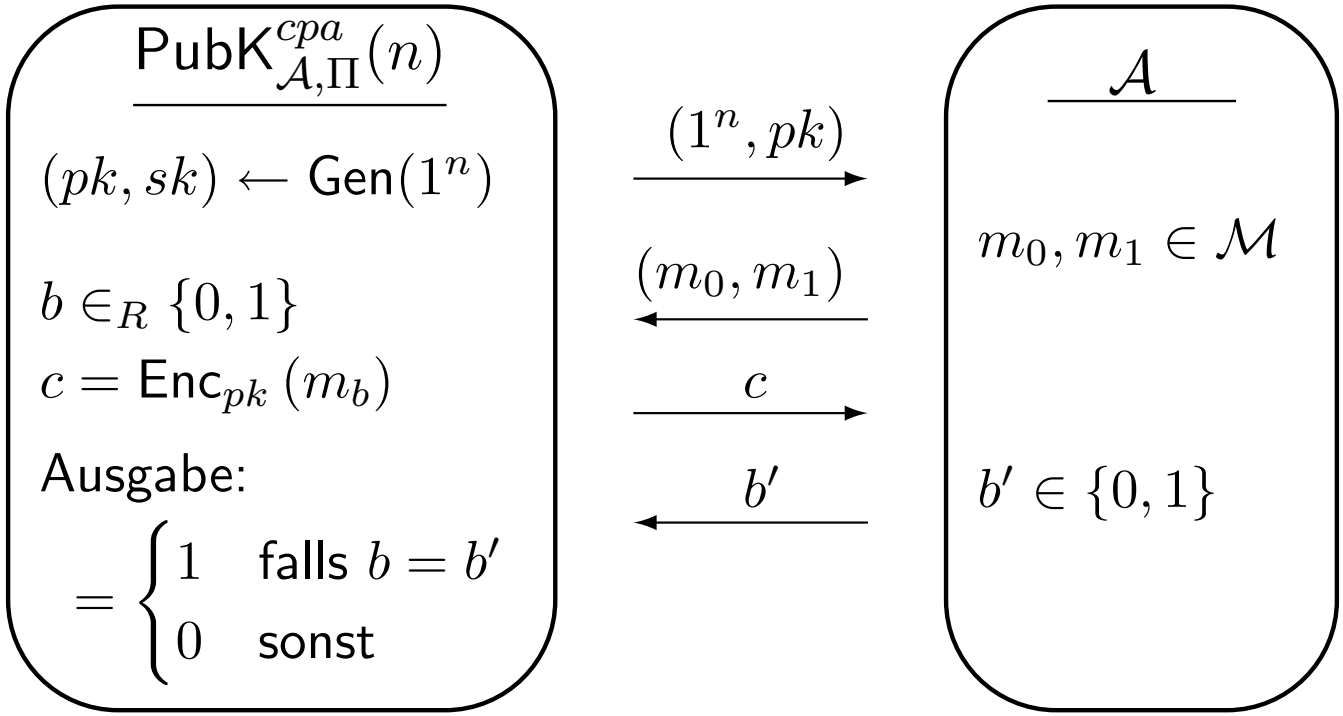
Spiel CPA Ununterscheidbarkeit von Chiffretexten $PubK^{cpa}_{\mathcal{A},\Pi}(n)$

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

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

- Man beachte, dass $\mathcal{A}$ Orakelzugriff auf Enc_{pk} besitzt.
- D.h. $\mathcal{A}$ kann sich beliebig gewählte Klartexte verschlüsseln lassen. (chosen plaintext attack = CPA)

CPA-Spiel


$\mathsf{PubK}^{cpa}_{\mathcal{A},\Pi}(n)$
$(pk, sk) \leftarrow \mathsf{Gen}(1^n)$
$b \in_R \{0,1\}$
$c = \mathsf{Enc}_{pk}(m_b)$
Ausgabe:
$= \begin{cases} 1 & \text{falls } b = b' \\ 0 & \text{sonst} \end{cases}$
$(1^n, pk)$
(m_0, m_1)
c
b'
$\mathcal{A}$
$m_0, m_1 \in \mathcal{M}$
$b' \in \{0,1\}$

CPA Sicherheit

Definition CPA Sicherheit von Verschlüsselung

Ein PK-Verschlüsselungsverfahren $\Pi = (Gen, Enc, Dec)$ besitzt ununterscheidbare Verschlüsselungen unter CPA falls für alle ppt $\mathcal{A}$ gilt

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

- **Übung:** *Unbeschränkte* $\mathcal{A}$ können das Spiel $PubK^{cpa}_{\mathcal{A},\Pi}(n)$ mit Ws $1 - \mathrm{negl}(n)$ gewinnen.
- Man beachte: Im symmetrischen Fall existiert perfekte Sicherheit, d.h. Ws genau $\frac{1}{2}$, gegenüber unbeschränkten $\mathcal{A}$. (One-time pad)

Unsicherheit deterministischer Verschlüsselung

Satz Deterministische Verschlüsselung

Deterministische PK-Verschlüsselung ist unsicher gegenüber CPA.

Beweis:

- $\mathcal{A}$ kann sich $Enc_{pk}(m_0)$ und $Enc_{pk}(m_1)$ selbst berechnen.
- D.h. ein Angreifer $\mathcal{A}$ gewinnt $PubK^{cpa}_{\mathcal{A},\Pi}(n)$ mit Ws 1.