Padded RSA

Definition Padded RSA Verschlüsselungsverfahren

Sei n ein Sicherheitsparameter und ℓ eine Fkt. mit $\ell(n) \leq 2n - 2$.

1. **Gen** : $(N, e, d) \leftarrow \mathit{GenRSA}(1^n)$
2. **Enc** : Für $m \in \{0,1\}^{\ell(n)}$ und $r \in_R \{0,1\}^{|N|-\ell(n)-1}$ berechne
$$c \leftarrow (r||m)^e \bmod N\ .$$
3. **Dec** : $r||m \leftarrow c^d \bmod N$. Gib die untersten $\ell(n)$ Bits aus.

Anmerkungen

- Für $\ell(n) = 2n - \mathcal{O}(\log n)$ kann r in polyn. Zeit geraten werden.
- Für $\ell(n) = cn$, konstantes $c < 2$, ist kein CPA Angriff bekannt.
- Für $\ell(n) = \mathcal{O}(\log n)$ kann CPA-Sicherheit gezeigt werden.
- Weitverbreitete standardisierte Variante von Padded RSA: PKCS #1 version 1.5 mit $c := (0^8||0^6 10||r||0^8||m)^e \bmod N$.
- Angriff mit gewählten Chiffretexten bekannt (Bleichenbacher '98). CCA = Chosen Ciphertext Attack

Einfache **symmetrische** Verschlüsselung

Algorithmus One-Time Gruppenelement

Sei n ein Sicherheitsparameter.

1. **Gen**: Schlüsselerzeugung $(G, g) \leftarrow \mathcal{G}(1^n)$, wobei G eine Gruppe und $g \in_R G$ ein zufälliger gemeinsamer geheimer Schlüssel ist.
2. **Enc**: Verschlüssele $m \in G$ als $c \leftarrow m \cdot g$.
3. **Dec**: Entschlüssele $c \in G$ als $m \leftarrow c \cdot g^{-1}$.

Perfekte Sicherheit von ONE-TIME GRUPPENELEMENT

Satz Perfekte Sicherheit von ONE-TIME GRUPPENELEMENT

ONE-TIME GRUPPENELEMENT ist ein perfekt sicheres **symmetrisches** Verschlüsselungsverfahren, d.h. für alle Angreifer $\mathcal{A}$ gilt

$$\mathrm{Ws}[\mathcal{A}(G, c) = m] = \frac{1}{|G|}.$$

Beweis:

- Sei $g' \in G$ beliebig. Da g ein zufälliges Gruppenelement ist, gilt
$$\mathrm{Ws}[c = g'] = \mathrm{Ws}[m \cdot g = g'] = \frac{1}{|G|}.$$
- Die Wsverteilung auf den Chiffretexten ist die Gleichverteilung.
- Insbesondere ist die Verteilung unabhängig von der Nachricht m.

Anmerkungen:

- Geheimer Schlüssel $sk = g$ muss stets neu gewählt werden.
- Idee für PK-Verfahren: Ersetze das zufällige g durch ein stets neu gewähltes "pseudozufälliges" Gruppenelement.

ElGamal Verschlüsselungsverfahren (1984)

Definition ElGamal Verschlüsselungsverfahren

Sei n ein Sicherheitsparameter.

1. **Gen** : $(G, q, g) \leftarrow \mathcal{G}(1^n)$, wobei G eine Gruppe der Ordnung q mit Generator g ist. Wähle $x \in_R \mathbb{Z}_q$ und berechne $h \leftarrow g^x$.
   Schlüssel: $pk = (G, q, g, h)$, $sk = (G, q, g, x)$
2. **Enc** : Für eine Nachricht $m \in G$ wähle ein $y \in_R \mathbb{Z}_q$ und berechne
   $$c \leftarrow (g^y, h^y \cdot m).$$
3. **Dec** : Für einen Chiffretext $c = (c_1, c_2)$ berechne $m \leftarrow \frac{c_2}{c_1^x}$.

- **Korrektheit:** $\frac{c_2}{c_1^x} = \frac{h^y \cdot m}{(g^y)^x} = \frac{(g^x)^y \cdot m}{g^{xy}} = m$.
- c_2 ist ein Analog von *Enc* bei ONE-TIME GRUPPENELEMENT mit einem DH-Schlüssel g^{xy} als "pseudozufälligem" Gruppenelement.

Anmerkung:

- G, q, g können global für alle Teilnehmer gewählt werden.

Sicherheit von ElGamal

Satz CPA-Sicherheit ElGamal

Falls DDH schwer ist bezüglich $\mathcal{G}$, besitzt ElGamal ununterscheidbare Chiffretexte unter CPA.

Beweis:

- Sei $\mathcal{A}$ ein Angreifer auf das ElGamal-Protokoll Π mit Erfolgsws
$$\epsilon(n) := \mathrm{Ws}[PubK^{cpa}_{\mathcal{A},\Pi}(n) = 1].$$
- Betrachten modifiziertes Verschlüsselungsverfahren Π' mit
$$c' = (c'_1, c'_2) = (g^y, g^z \cdot m) \text{ mit } y, z \in_R \mathbb{Z}_q.$$
- c' ist unabhängig gleichverteilt in G^2, d.h. unabhängig von m.
- Daher gilt $\mathrm{Ws}[PubK^{cpa}_{\mathcal{A},\Pi'}(n) = 1] = \frac{1}{2}$.
- **Idee:** Lösen von DDH durch Unterscheiden von Π und Π'.
- DDH-Instanz: (G, q, g, g^x, g^y, g') mit $g' = g^{xy}$ oder $g' = g^z$.

Unterscheider für DDH durch $\mathcal{A}$

Algorithmus DDH-Unterscheider D

EINGABE: (G, q, g, g^x, g^y, g')

1. Setze $pk = (G, q, g, g^x)$.
2. $(m_0, m_1) \leftarrow \mathcal{A}(pk)$.
3. Wähle $b \in_R \{0, 1\}$ und berechne $b' \leftarrow \mathcal{A}(g^y, g' \cdot m_b)$.
4. Falls $b' = b$ Ausgabe 1, sonst Ausgabe 0.

AUSGABE: $\begin{cases} 1 & \text{wird interpretiert als } g' = g^{xy} \\ 0 & \text{wird interpretiert als } g' = g^z \end{cases}$.

Fall 1: Eingabe ist kein DDH-Tupel, d.h. $g' = g^z$ für $z \in_R \mathbb{Z}_q$.

- Chiffretext c ist wie bei Π' von der Form $(g^y, g^z \cdot m_b)$.
- Damit $\mathrm{Ws}[D(G, q, g, g^x, g^y, g^z) = 1] = \mathrm{Ws}[PubK_{\mathcal{A},\Pi'}(n) = 1] = \frac{1}{2}$.

Fall DDH-Tupel

Fall 2: Eingabe ist ein DDH-Tupel, d.h. $g' = g^{xy}$.

- $c = (g^y, g^{xy} \cdot m_b)$ ist identisch zu ElGamal-Chiffretexten verteilt.
- D.h. $\mathrm{Ws}[D(G, q, g, g^x, g^y, g^{xy}) = 1] = \mathrm{Ws}[PubK_{\mathcal{A},\Pi}(n) = 1] = \epsilon(n)$.
- Aus der DDH-Annahme folgt

$$\begin{aligned} \mathrm{negl}(n) &\geq |\mathrm{Ws}[D(G, q, g, g^x, g^y, g^z) = 1] - \mathrm{Ws}[D(G, q, g, g^x, g^y, g^{xy}) = 1]| \\ &= \left|\frac{1}{2} - \epsilon(n)\right|. \end{aligned}$$

- Daraus folgt $\epsilon(n) \leq \frac{1}{2} + \mathrm{negl}(n)$. □

Parameterwahl bei ElGamal

Einbetten von Nachrichten $\mathbf{m' \in \{0,1\}^*}$

- Beliebte Parameterwahl: $\mathbb{Z}_p^*$, $p = 2q + 1$ mit p, q prim.
- D.h. p ist eine sogenannte starke Primzahl.
- **Ziel:** Untergruppe G mit primer Ordnung q.

- Quadrieren $\mathbb{Z}_p^* \to \mathbb{Z}_p^*$, $x \mapsto x^2$ ist eine $2-1$-Abbildung.
- Urbilder $x, p - x$ kollidieren, genau eines ist in $[\frac{p-1}{2}] = [q]$.
- Wir bezeichnen den Bildraum mit QR_p.
- QR_p ist Untergruppe von $\mathbb{Z}_p^*$ mit Ordnung q.
- Wählen g als Generator von QR_p. Sei $|q| = n$.
- Interpretieren $m' \in \{0,1\}^{n-1}$ als natürliche Zahl kleiner q.
- Es gilt $m' + 1 \in [q]$. Einbettung von m' ist $m = (m' + 1)^2 \bmod p$.
- Umkehren der Einbettung ist effizient berechenbar.