Mehrfache Verschlüsselung

Spiel Mehrfache Verschlüsselung $PubK_{\mathcal{A},\Pi}^{mult}(n)$

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

- 1 $(pk, sk) \leftarrow Gen(1^n)$
- 2 $(M_0, M_1) \leftarrow \mathcal{A}(pk)$, wobei $M_i = (m_i^1, \dots, m_i^t)$, $i = 1, 2$ und $|m_0^j| = |m_1^j|$ für $j \in [t]$.
- 3 Wähle $b \in_R \{0, 1\}$. $b' \leftarrow \mathcal{A}(Enc_{pk}(m_b^1), \dots, Enc_{pk}(m_b^t))$.
- 4 $PubK_{\mathcal{A},\Pi}^{mult}(n) = \begin{cases} 1 & \text{für } b = b' \\ 0 & \text{sonst} \end{cases}$.

Definition CPA Sicherheit von mehrfacher Verschlüsselung

Ein PK-Verschlüsselungsverfahren $\Pi = (Gen, Enc, Dec)$ besitzt ununterscheidbare mehrfache Verschlüsselungen unter CPA falls für alle ppt $\mathcal{A}$ gilt $Ws[PubK_{\mathcal{A},\Pi}^{mult}(n) = 1] \leq \frac{1}{2} + \text{negl}(n)$.

Sicherheit mehrfacher Verschlüsselung

Satz Sicherheit mehrfacher Verschlüsselung

Sei Π ein PK-Verschlüsselungsschema. Π besitzt ununterscheidbare mehrfache Verschlüsselung unter CPA gdw Π ununterscheidbare Verschlüsselung unter CPA besitzt.

Beweis “ $\Leftarrow$ ”: Für $t = 2$.

- Ein Angreifer $\mathcal{A}$ gewinnt das Spiel $PubK_{\mathcal{A},\Pi}^{mult}(n)$ mit Ws

$$\frac{1}{2} Ws[\mathcal{A}(Enc_{pk}(m_0), Enc_{pk}(m_0)) = 0] + \frac{1}{2} Ws[\mathcal{A}(Enc_{pk}(m_1), Enc_{pk}(m_1)) = 1].$$

- Daraus folgt $Ws[PubK_{\mathcal{A},\Pi}^{mult}(n)] + \frac{1}{2} =$

$$\begin{aligned} & \frac{1}{2} Ws[\mathcal{A}(Enc_{pk}(m_0), Enc_{pk}(m_0)) = 0] + \frac{1}{2} Ws[\mathcal{A}(Enc_{pk}(m_1), Enc_{pk}(m_1)) = 1] \\ & + \frac{1}{2} (Ws[\mathcal{A}(Enc_{pk}(m_0), Enc_{pk}(m_1)) = 0] + Ws[\mathcal{A}(Enc_{pk}(m_1), Enc_{pk}(m_0)) = 1]) \end{aligned}$$

- **Ziel:** Zeigen, dass $Ws[PubK_{\mathcal{A},\Pi}^{mult}(n)] + \frac{1}{2} \leq 1 + \text{negl}(n)$.

Betrachten der Hybride

Lemma

$$\frac{1}{2} \text{Ws}[\mathcal{A}(\text{Enc}_{pk}(m_0^1), \text{Enc}_{pk}(m_0^2)) = 0] + \frac{1}{2} \text{Ws}[\mathcal{A}(\text{Enc}_{pk}(m_0^1), \text{Enc}_{pk}(m_1^2)) = 1] \leq \frac{1}{2} + \text{negl}(n).$$

Beweis: Sei $\mathcal{A}'$ Angreifer für *einfache* Verschlüsselungen.

- $\mathcal{A}'$ versucht mittels $\mathcal{A}$ das Spiel $\text{PubK}_{\mathcal{A}', \Pi}^{\text{cpa}}(n)$ zu gewinnen.

Strategie von Angreifer $\mathcal{A}'$

- 1 $\mathcal{A}'$ gibt pk an $\mathcal{A}$ weiter.
 - 2 $(M_0, M_1) \leftarrow \mathcal{A}(pk)$ mit $M_0 = (m_0^1, m_0^2)$ und $M_1 = (m_1^1, m_1^2)$.
 - 3 $\mathcal{A}'$ gibt (m_0^2, m_1^2) aus. $\mathcal{A}'$ erhält Chiffretext $c(b) = \text{Enc}(m_b^2)$.
 - 4 $b' \leftarrow \mathcal{A}(\text{Enc}_{pk}(m_0^1), c(b))$.
 - 5 $\mathcal{A}'$ gibt Bit b' aus.
- $\text{Ws}[\mathcal{A}'(\text{Enc}(m_0^2)) = 0] = \text{Ws}[\mathcal{A}(\text{Enc}_{pk}(m_0^1), \text{Enc}_{pk}(m_0^2)) = 0]$ und
 - $\text{Ws}[\mathcal{A}'(\text{Enc}(m_1^2)) = 1] = \text{Ws}[\mathcal{A}(\text{Enc}_{pk}(m_0^1), \text{Enc}_{pk}(m_1^2)) = 1]$.

Fortsetzung Hybridtechnik

Beweis(Fortsetzung):

- CPA Sicherheit von Π bei einzelnen Nachrichten impliziert

$$\begin{aligned} \frac{1}{2} + \text{negl}(n) &\geq \text{Ws}[PubK_{\mathcal{A}', \Pi}^{cpa}(n) = 1] \\ &= \frac{1}{2} \text{Ws}[\mathcal{A}'(Enc(m_0^2)) = 0] + \frac{1}{2} \text{Ws}[\mathcal{A}'(Enc(m_1^2)) = 1] \\ &= \frac{1}{2} \text{Ws}[\mathcal{A}((Enc_{pk}(m_0^1), Enc_{pk}(m_0^2)) = 0) + \\ &\quad \frac{1}{2} \text{Ws}[\mathcal{A}((Enc_{pk}(m_0^1), Enc_{pk}(m_1^2)) = 1)] \quad \square_{\text{Lemma}} \end{aligned}$$

- Analog kann gezeigt werden, dass

$$\begin{aligned} \frac{1}{2} + \text{negl}(n) &\geq \frac{1}{2} \text{Ws}[\mathcal{A}((Enc_{pk}(m_0^1), Enc_{pk}(m_1^2)) = 0) + \\ &\quad \frac{1}{2} \text{Ws}[\mathcal{A}((Enc_{pk}(m_1^1), Enc_{pk}(m_1^2)) = 1)] \end{aligned}$$

- Daraus folgt $\text{Ws}[PubK_{\mathcal{A}, \Pi}^{mult}(n)] + \frac{1}{2} \geq 1 + \text{negl}(n)$. $\square$ Satz für $t = 2$

Von fester zu beliebiger Nachrichtenlänge

- Beweistechnik für allgemeines t : Definiere für $i \in [t]$ Hybride $C^{(i)} = (Enc_{pk}(m_0^1), \dots, Enc_{pk}(m_0^i), Enc_{pk}(m_1^{i+1}), \dots, Enc_{pk}(m_1^t))$.
- $Ws[PubK_{\mathcal{A}, \Pi}^{mult}(n) = 1] = \frac{1}{2} \cdot Ws[\mathcal{A}(C^{(t)}) = 0] + \frac{1}{2} \cdot Ws[\mathcal{A}(C^{(0)}) = 1]$.
- $\mathcal{A}'$ unterscheidet $Enc_{pk}(m_0^i)$ und $Enc_{pk}(m_1^i)$ für zufälliges $i \in [t]$.
- Entspricht dem Unterscheiden von $C^{(i)}$ und $C^{(i-1)}$.
- Liefert $Pr[PubK_{\mathcal{A}, \Pi}^{mult}(n)] \leq \frac{1}{2} + t \cdot \text{negl}(n)$ $\square$ Satz.

Von fester zu beliebiger Nachrichtenlänge

- Sei Π ein Verschlüsselungsverfahren mit Klartexten aus $\{0, 1\}^n$.
- Splitte $m \in \{0, 1\}^*$ in $m_1, \dots, m_t$ mit $m_i \in \{0, 1\}^n$.
- Definiere Π' vermöge $Enc'_{pk}(m) = Enc_{pk}(m_1) \dots Enc_{pk}(m_t)$.
- Aus vorigem Satz folgt: Π' ist CPA-sicher, falls Π CPA-sicher ist.

Hybride Verschlüsselungsverfahren

Ziel: Flexibilität von asym. Verfahren und Effizienz von sym. Verfahren.

- Sei $\Pi = (Gen, Enc, Dec)$ ein PK-Verschlüsselungsverfahren und $\Pi' = (Gen', Enc', Dec')$ ein SK-Verschlüsselungsverfahren.
- Berechne $(pk, sk) \leftarrow Gen(1^n)$.

Algorithmus Hybride Verschlüsselung

Eingabe: m, pk

- 1 Wähle $k \in_R \{0, 1\}^n$.
- 2 Verschlüssele $c_1 \leftarrow Enc_{pk}(k)$ mit asym. Verschlüsselung.
- 3 Verschlüssele $c_2 \leftarrow Enc'_k(m)$ mit sym. Verschlüsselung.

Ausgabe: Chiffretext $c = (c_1, c_2)$

Hybride Entschlüsselung

Algorithmus Hybride Entschlüsselung

Eingabe: $c = (c_1, c_2)$, sk

- 1 Entschlüssele $k \leftarrow Dec_{sk}(c_1)$.
- 2 Entschlüssele $m \leftarrow Dec'_k(c_2)$.

Ausgabe: Klartext m

- Effizienzgewinn für $|m| \gg n$, sofern Π' effizienter als Π .
- **Frage:** Ist hybride Verschlüsselung sicher, falls Π, Π' sicher?

Sicherheit von hybrider Verschlüsselung

Satz Sicherheit hybrider Verschlüsselung

Sei Π ein CPA-sicheres PK-Verschlüsselungsverfahren und Π' ein SK-Verschlüsselungsverfahren mit ununterscheidbaren Chiffretexten gegenüber passiven Angreifern.

Dann ist das hybride Verfahren Π^{hy} CPA-sicher.

Beweisskizze:

- **Notation** $X \equiv Y$: Kein ppt Angreifer kann X und Y unterscheiden.
- Sicherheit von Π' : $Enc_k(m_0) \equiv Enc_k(m_1)$ für $k \in_R \{0, 1\}^n$.
- Sicherheit von Π^{hy} : Müssen zeigen dass

$$(Enc_{pk}(k), Enc'_k(m_0)) \equiv (Enc_{pk}(k), Enc'_k(m_1)).$$

- Problem: Erstes Argument könnte beim Unterscheiden des zweiten Arguments helfen.

Beweis Sicherheit hybrider Verschlüsselung

Beweisskizze: Zeigen die folgenden 3 Schritte

- 1 Sicherheit von Π liefert

$$(Enc_{pk}(k), Enc'_k(m_0)) \equiv (Enc_{pk}(0^n), Enc'_k(m_0)).$$

Gilt sogar falls $\mathcal{A}$ die Werte $k, 0^n$ kennt.

Dass das zweite Argument k beinhaltet ist daher kein Problem.

- 2 Sicherheit von Π' liefert

$$(Enc_{pk}(0^n), Enc'_k(m_0)) \equiv (Enc_{pk}(0^n), Enc'_k(m_1)).$$

Kein Problem mehr, da 2. Argument nicht vom ersten abhängt.

- 3 Sicherheit von Π liefert

$$(Enc_{pk}(0^n), Enc'_k(m_1)) \equiv (Enc_{pk}(k), Enc'_k(m_1)).$$

Transitivität der 3 Ergebnisse liefert schließlich wie gewünscht

$$(Enc_{pk}(k), Enc'_k(m_0)) \equiv (Enc_{pk}(k), Enc'_k(m_1)).$$

Textbook RSA

Algorithmus Schlüsselerzeugung *GenRSA*

Eingabe: 1^n

- 1 $(N, p, q) \leftarrow \text{GenModulus}(1^n)$ mit primen n -Bit p, q und $N = pq$.
- 2 $\phi(N) \leftarrow (p - 1)(q - 1)$
- 3 Wähle $e \in \mathbb{Z}_{\phi(N)}^*$.
- 4 Berechne $d \leftarrow e^{-1} \bmod \phi(N)$.

Ausgabe: (N, e, d) mit $pk = (N, e)$ und $sk = (N, d)$.

Definition Textbook RSA Verschlüsselungsverfahren

Sei n ein Sicherheitsparameter.

- 1 **Gen** : $(N, e, d) \leftarrow \text{GenRSA}(1^n)$
- 2 **Enc** : $c \leftarrow m^e \bmod N$ für eine Nachricht $m \in \mathbb{Z}_N$.
- 3 **Dec** : $m \leftarrow c^d \bmod N$

RSA Problem und Sicherheit von RSA

Definition RSA Problem

Das *RSA Problem* ist hart bezüglich $GenRSA(1^n)$, falls für alle ppt Algorithmen $\mathcal{A}$ gilt $Ws[\mathcal{A}(N, e, m^e \bmod N) = m] \leq \text{negl}(n)$.

Wsraum: Wahl $m \in_R \mathbb{Z}_N$ und interne Münzwürfe von $\mathcal{A}$, $GenRSA$.

RSA Annahme: Das RSA Problem ist hart bezüglich $GenRSA$.

Anmerkungen:

- Falls N effizient faktorisiert werden kann, ist das RSA Problem nicht hart. (Warum?)
- Berechnen von d ist so schwer wie Faktorisieren von N .
- **Offenes Problem**: Impliziert eine Lösung des RSA Problem eine Lösung des Faktorisierungsproblems?
- *Enc* ist deterministisch, d.h. Textbook RSA ist nicht CPA-sicher.
- Unter der RSA-Annahme: Kein ppt Angreifer kann für zufällige $m \in \mathbb{Z}_N^*$ aus $(N, e, m^e \bmod N)$ die ganze Nachricht m berechnen.

Angriffe auf Textbuch RSA

Verschlüsseln von kurzen Nachrichten mit kleinem e

- Sei $m < N^{\frac{1}{e}}$. Dann gilt $c = m^e < N$. D.h. $c^{\frac{1}{e}}$ über $\mathbb{Z}$ liefert m .
- Realistisch bei hybrider Verschlüsselung: N 1024-Bit und $e = 3$, m ist 128-Bit Schlüssel für symmetrische Verschlüsselung.

Hastad Angriff auf RSA

- **Szenario:** Verschlüsselung desselben m unter verschiedenen pk .
- Sei $pk_1 = (N_1, 3)$, $pk_2 = (N_2, 3)$, $pk_3 = (N_3, 3)$. Angreifer erhält $c_1 = m^3 \bmod N_1$, $c_2 = m^3 \bmod N_2$ und $c_3 = m^3 \bmod N_3$.
- Berechne mittels Chinesischem Restsatz eind. $c \in \mathbb{Z}_{N_1 N_2 N_3}$ mit

$$\begin{cases} c = c_1 \bmod N_1 \\ c = c_2 \bmod N_2 \\ c = c_3 \bmod N_3 \end{cases}.$$

- Es gilt $c = m^3 < (\min\{N_1, N_2, N_3\})^3 < N_1 N_2 N_3$, d.h. $m = c^{\frac{1}{3}}$.

Weitere Angriffe: Übung bzw. Vorlesung Kryptanalyse (WS 2009/10)