Sicherheit gegenüber CCA

Idee:

- Ersetze One-Time Pad durch CCA-sicheres Secret Key Verfahren.
- *Erinnerung Krypto I:* Konstruktion von CCA-sicherem Secret Key Verfahren mittels Pseudozufallsfunktion (und MAC) möglich.

Verschlüsselung ROM-RSA-2

Sei $H : \mathbb{Z}_N^* \to \{0,1\}^{\ell(n)}$ ein Random Oracle, $\Pi' = (Gen', Enc', Dec')$ ein CCA-sicheres Secret Key Verschlüsselungsverfahren.

1. **Gen:** $(N, e, d) \leftarrow GenRSA(1^n)$ mit $pk = (N, e), sk = (N, d)$.
2. **Enc:** Für $m \in \{0,1\}^{\ell(n)}$, wähle $r \in_R \mathbb{Z}_N^*$. Berechne $k = H(r)$ und
$$c \leftarrow (r^e \bmod N, Enc'_k(m)).$$
3. **Dec:** Für $c = (c_1, c_2)$ berechne
$$r \leftarrow c_1^d \bmod N, k \leftarrow H(r) \text{ und } m \leftarrow Dec'_k(c_2).$$

Sicherheit von ROM-RSA-2

Satz Sicherheit von ROM-RSA-2

Unter der RSA-Annahme, für ein Random Oracle H und ein CCA-sicheres Π' liefert ROM-RSA-2 CCA-sichere Verschlüsselung.

Anmerkungen:

- Wir werden den Satz hier nicht formal beweisen.
- Der Beweis verläuft großteils analog zum vorigen Beweis.
- Problem: Müssen Orakel $Dec_{sk}(\cdot)$ simulieren, ohne sk zu kennen.
- Verwende dazu geschicktes Simulieren des Random Oracles $H(\cdot)$.
- Bsp. für geschicktes Simulieren: s. Beweis zu RSA-FDH (später).

Jacobi-Symbol

Erinnerung Jacobi-Symbol: Beweise siehe Diskrete Mathematik II

Definition Quadratischer Rest

Sei $N \in \mathbb{N}$. Ein Element $a \in \mathbb{Z}_N$ heißt *quadratischer Rest* in $\mathbb{Z}_N$, falls es ein $b \in \mathbb{Z}_N$ gibt mit $b^2 = a \bmod N$. Wir definieren

$$QR_N = \{a \in \mathbb{Z}_N^* \mid a \text{ ist quadratischer Rest }\} \text{ und } QNR_N = \mathbb{Z}_N^* \setminus QR_N.$$

Lemma Anzahl quadratischer Reste in primen Restklassen

Sei $p > 2$ prim. Dann gilt $|QR_p| = \frac{|\mathbb{Z}_p^*|}{2} = \frac{p-1}{2}$.

Beweisidee:

- Quadrieren auf $\mathbb{Z}_p^*$, $x \mapsto x^2$, ist eine 2:1-Abbildung.
- Die verschiedenen Werte $x, (-x)$ werden beide auf x^2 abgebildet.

Legendre-Symbol

Definition Legendre Symbol

Sei $p > 2$ prim und $a \in \mathbb{N}$. Das *Legendre Symbol* ist definiert als

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{falls } p|a \\ 1 & \text{falls } (a \bmod p) \in QR_p \\ -1 & \text{falls } (a \bmod p) \in QNR_p \end{cases} .$$

Satz

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$$

Eigenschaften Quadratischer Reste

1. Multiplikativität: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
2. $(QR_p, \cdot)$ ist eine multiplikative Gruppe.

Das Jacobi Symbol

Definition Jacobi Symbol

Sei $N = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k} \in \mathbb{N}$ ungerade und $a \in \mathbb{N}$. Dann ist das *Jacobi Symbol* definiert als

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p_1}\right)^{e_i} \cdot \ldots \cdot \left(\frac{a}{p_k}\right)^{e_k}.$$

- **Warnung:** $\left(\frac{a}{N}\right) = 1$ impliziert nicht, dass $a \in QR_N$ ist.
- Bsp: $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1)(-1) = 1$.
- D.h. $2 \in QNR_3$ und $2 \in QNR_5$. Damit besitzt $x^2 = 2$ weder Lösungen modulo 3 noch modulo 5.
- Nach CRT besitzt $x^2 = 2 \mod 15$ ebenfalls keine Lösung.

Pseudoquadrate

Berechnung des Jacobi-Symbols: Sei $a \in \mathbb{Z}_N$.

- Berechnung von $\left(\frac{a}{N}\right)$ ist in Zeit $\log^2(\max\{N, a\})$ möglich, **ohne** die Faktorisierung von N zu kennen.
- Algorithmus ist ähnlich zum Euklidischen Algorithmus, verwendet das Gaußsche Reziprozitätsgesetz.

Definition Pseudoquadrat

Sei $N \in \mathbb{N}$. Die Menge der *Pseudoquadrate* ist definiert als

$$QNR_N^{+1} = \{a \in \mathbb{Z}_N^* \mid \left(\frac{a}{N}\right) = 1 \text{ und } a \notin QR_N\}.$$

Multiplikation von Resten/Nichtresten

Lemma Multiplikation von Resten/Nichtresten

Sei $N = pq$ ein RSA-Modul. Seien $x, x' \in QR_N$ und $y, y' \in QNR_N^{+1}$.

1. $xx' \in QR_N$
2. $yy' \in QR_N$
3. $xy \in QNR_N^{+1}$

Beweis: für 3 (1+2 folgen analog)

- Nach Chinesischem Restsatz gilt
$$QR_N \simeq QR_p \times QR_q \text{ und } QNR_N^{+1} \simeq QNR_p \times QNR_q.$$
- Aus der Multiplikativität des Legendre-Symbols folgt
$$\left(\frac{xy}{N}\right) = \left(\frac{xy}{p}\right)\left(\frac{xy}{q}\right) = \left(\frac{x}{p}\right)\left(\frac{x}{q}\right)\left(\frac{y}{p}\right)\left(\frac{y}{q}\right) = 1 \cdot 1 \cdot (-1) \cdot (-1) = 1.$$
- Analog gilt
$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = (-1).$$
- Daraus folgt $xy \in QNR_N^{+1}$.

Quadratische Residuositätsannahme

Definition Quadratische Residuosität

Das *Unterscheiden quadratischer Reste* ist hart bezüglich $\mathit{GenModulus}(1^n)$ falls für alle ppt $\mathcal{D}$ gilt

$$|\mathrm{Ws}[\mathcal{D}(1^n, N, qr) = 1] - \mathrm{Ws}[\mathcal{D}(1^n, N, qnr) = 1]| \leq \mathrm{negl}(n),$$

wobei $qr \in_R QR_N$ und $qnr \in_R QNR_N^{+1}$.

QR-Annahme: Unterscheiden quadratischer Reste ist hart.

Idee des Goldwasser-Micali Kryptosystems

- $pk = N$, $sk = (p, q)$
- Verschlüsselung von 0 ist zufälliges $x' \in_R QR_N$.
- Wähle $x \in_R \mathbb{Z}_N^*$ und berechne $x' \leftarrow x^2 \bmod N$.
- Verschlüsselung von 1 ist zufälliges $y \in_R QNR_N^{+1}$.
- **Problem:** Wie wählt man y ohne p, q zu kennen?
- Abhilfe: Public-Key enthält $z \in_R QNR_N^{+1}$.
- Sender wählt $x \in_R \mathbb{Z}_N^*$ und berechnet $y \leftarrow z \cdot x^2 \bmod N \in QNR_N^{+1}$.

GOLDWASSER-MICALI Verschlüsselung (1984)

Definition GOLDWASSER-MICALI Verschlüsselung

Sei n ein Sicherheitsparameter.

1. **Gen:** $(N, p, q) \leftarrow \mathit{GenModulus}(1^n)$. Wähle $z \in_R QNR_N^{+1}$. (Wie?) Schlüssel: $pk = (N, z)$ und $sk = (p, q)$
2. **Enc:** Für $m \in \{0,1\}$ wähle $x \in_R \{0,1\}$ und berechne
$$c \leftarrow z^m \cdot x^2 \bmod N.$$
3. **Dec:** Berechne $m = \begin{cases} 0 & \text{falls } \left(\frac{c}{p}\right) = 1 \\ 1 & \mathit{sonst} \end{cases}$.

Korrektheit:

- Für $m = 0$ ist $c \in QR_N \simeq QR_p \times QR_q$, d.h. $\left(\frac{c}{p}\right) = 1$.
- Für $m = 1$ ist $c \in QNR_N^{+1} \simeq QNR_p \times QNR_q$, d.h. $\left(\frac{c}{p}\right) = (-1)$.

Sicherheit von GOLDWASSER-MICALI Verschlüsselung

Satz Sicherheit von GOLDWASSER-MICALI

Unter der QR-Annahme ist GOLDWASSER-MICALI Π CPA-sicher.

Beweis:

- Sei $\mathcal{A}$ ein Angreifer für Π mit $\epsilon(n) = \mathrm{Ws}[PubK^{cpa}_{\mathcal{A},\Pi}(n) = 1]$.
- Konstruieren Unterscheider $\mathcal{D}$ für Quadratische Residuosität.

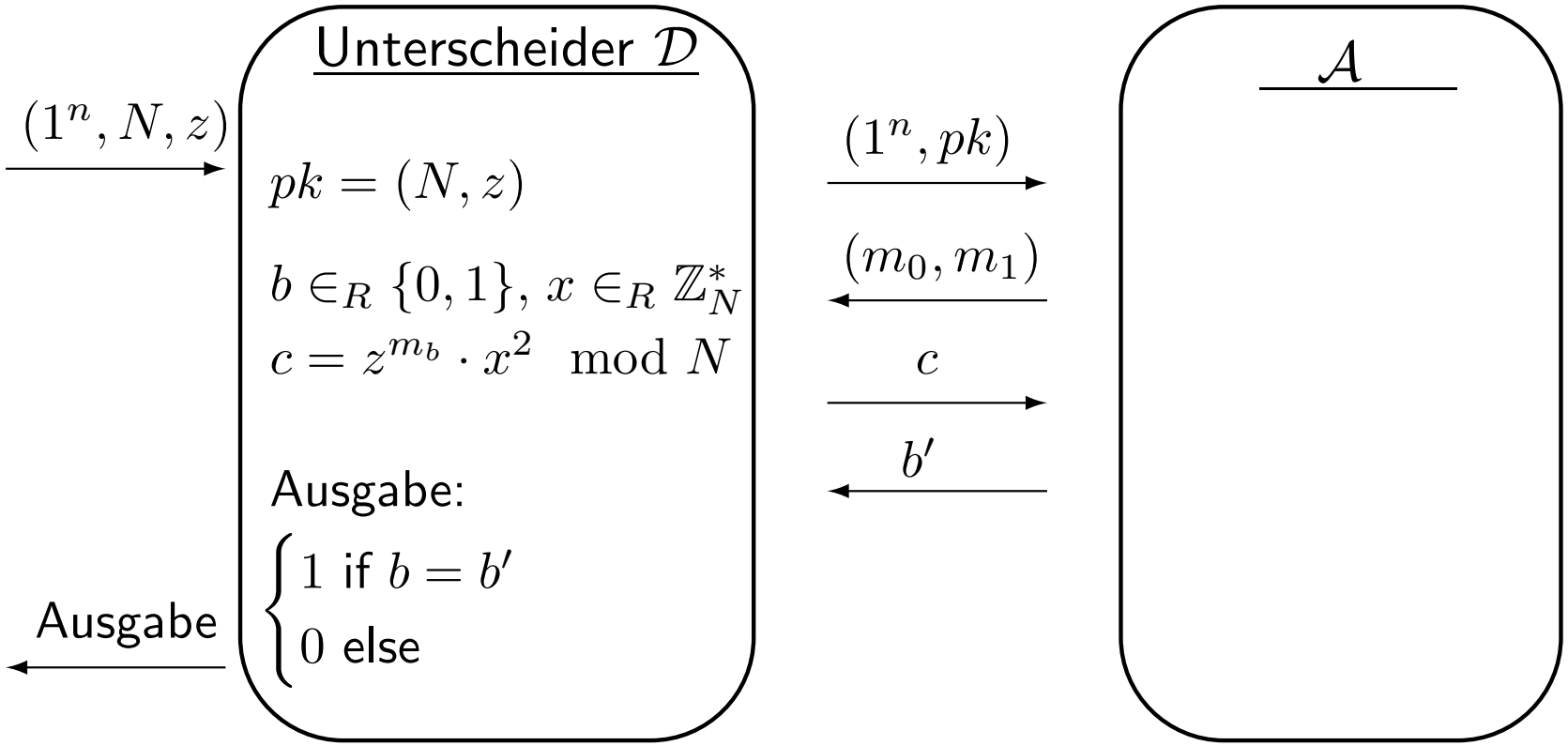
Algoritmus QR-Unterscheider *D*

EINGABE: (N, z) mit $\left(\frac{z}{N}\right) = 1$

1. Setze $pk = (N, z)$ und berechne $(m_0, m_1) \leftarrow \mathcal{A}(pk)$.
   OBdA gilt $\{m_0, m_1\} = \{0, 1\}$.
2. Wähle $b \in_R \{0, 1\}$ und $x \in_R \mathbb{Z}_N^*$. Berechne $c \leftarrow z^{m_b} \cdot x^2 \bmod N$.
3. $b' \leftarrow \mathcal{A}(c)$

AUSGABE: $\begin{cases} 1 & \text{falls } b = b', \text{ Interpretation } z \in QNR_N^{+1} \\ 0 & \text{sonst,} \qquad\quad \text{Interpretation } z \in QR_N \end{cases}$

Algorithmus QR-Unterscheider



Sicherheit von GOLDWASSER-MICALI Verschlüsselung

Fall 1: $z \in QNR_N^{+1}$

- Verteilung von c ist identisch zu GOLDWASSER-MICALI.
- D.h. $\mathrm{Ws}[\mathcal{D}(1^n, N, qnr) = 1] = \epsilon(n)$.

Fall 2: $z \in QR_N$

- Falls 0 verschlüsselt wird, gilt $c = x^2 \in_R QR_N$.
- Falls 1 verschlüsselt wird, gilt $c = z \cdot x^2 \in_R QR_N$.
- D.h. die Verteilung von c ist unabhängig von der Wahl von b.
- Sei Π' GOLDWASSER-MICALI Verschlüsselung mit $z \in QR_N$.
- Dann gilt $\mathrm{Ws}[\mathcal{D}(1^n, N, qr) = 1] = \mathrm{Ws}[PubK^{cpa}_{\mathcal{A},\Pi'}(n) = 1] = \frac{1}{2}$.

Unter der Quadratischen Residuositäts-Annahme folgt

$$\mathrm{negl}(n) \geq |\mathrm{Ws}[D(N, qr) = 1] - \mathrm{Ws}[D(N, qnr) = 1]| = \left|\tfrac{1}{2} - \epsilon(n)\right|.$$

Damit gilt $\epsilon(n) \leq \frac{1}{2} + \mathrm{negl}(n)$.