

Quadratische Reste

Definition Quadratischer Rest

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

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

Definition Legendre Symbol

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

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

Das Legendre Symbol

Eigenschaften Quadratischer Reste

Sei $p > 2$ prim und $a, b \in \mathbb{N}$.

- 1 $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$
- 2 Multiplikativität: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$
- 3 $(QR_p, \cdot)$ ist eine multiplikative Gruppe mit $|QR_p| = \frac{|\mathbb{Z}_p^*|}{2} = \frac{p-1}{2}$.

Beweise siehe Diskrete Mathematik II.

Das Jacobi Symbol

Definition Jacobi Symbol

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

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdot \dots \cdot \left(\frac{a}{p_k}\right)^{e_k}.$$

Definiere $J_N^{+1} = \{a \in \mathbb{Z}_N^* \mid \left(\frac{a}{N}\right) = 1\}$ und $J_N^{-1} = \{a \in \mathbb{Z}_N^* \mid \left(\frac{a}{N}\right) = -1\}$.

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.

Pseudoquadrate

- **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 $x^2 = 2 \bmod 15$ ebenfalls keine Lösung.

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 $\text{GenModulus}(1^n)$ falls für alle ppt $\mathcal{D}$ gilt

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

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.

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

Korrektheit:

- Für $m = 0$ ist $c \in \text{QR}_N \simeq \text{QR}_p \times \text{QR}_q$, d.h. $\left(\frac{c}{p}\right) = \left(\frac{c}{q}\right) = 1$.
- Für $m = 1$ ist $c \in \text{QNR}_N^{+1} \simeq \text{QNR}_p \times \text{QNR}_q$, d.h.
 $\left(\frac{c}{p}\right) = \left(\frac{c}{q}\right) = -1$.

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 $\epsilon(n) = \text{Ws}[PubK_{\mathcal{A}, \Pi}^{cpa}(n) = 1]$.
- Konstruieren Unterscheider $\mathcal{D}$ für Quadratische Residuosität.

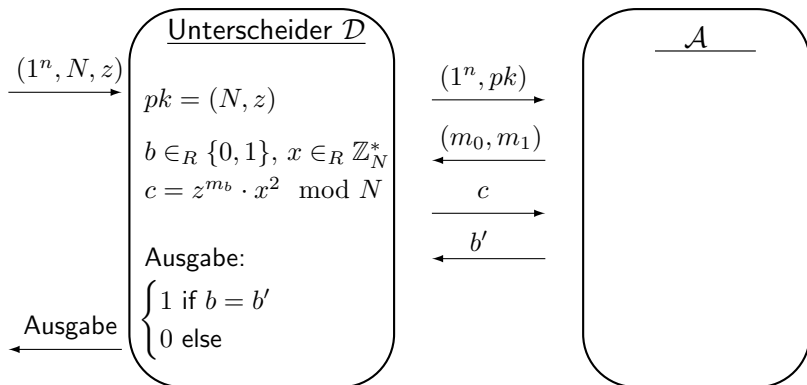
Algorithmus QR-Unterscheider $\mathcal{D}$

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

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

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. $\text{Ws}[\mathcal{D}(1^n, N, qnr) = 1] = \epsilon(n)$.

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 $\text{Ws}[\mathcal{D}(1^n, N, qr) = 1] = \text{Ws}[PubK_{\mathcal{A}, \Pi'}^{cpa}(n) = 1] = \frac{1}{2}$.

Unter der Quadratischen Residuositäts-Annahme folgt

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

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