Pseudoquadrate

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

- Berechnung von $\left(\frac{a}{N}\right)$ ist in Zeit $\log^2(N)$ 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

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

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

$$|\mathrm{Ws}[\mathcal{A}(N, qr) = 1] - \mathrm{Ws}[\mathcal{A}(N, qnr) = 1]| \leq \tfrac{1}{2} + \mathrm{negl}(n),$$

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 $m \in \{0, 1\}$ 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

GOLDWASSER-MICALI ist CPA-sicher.

Beweis: Sei Π die GOLDWASSER-MICALI Verschlüsselung.

- Sei $\mathcal{A}$ ein Angreifer für Π mit $\epsilon(n) = \mathrm{Ws}[PubK^{cpa}_{\mathcal{A},N}(n) = 1]$.
- Konstruieren Unterscheider 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: $\begin{cases} 1 & \text{falls } b = b', \text{ Interpretation } z \in QR_N \\ 0 & \text{sonst,} \qquad\quad \text{Interpretation } z \in QNR_N \end{cases}$

Sicherheit von GOLDWASSER-MICALI Verschlüsselung

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

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

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 $\mathrm{Ws}[D(N, qr) = 1] = \mathrm{Ws}[PubK_{\mathcal{A},\Pi'}(n)] = \frac{1}{2}$.
- Unter der Quadratischen Residuositäts-Annahme folgt

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

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

Rabin Verschlüsselung 1979

Idee: Rabin Verschlüsselung

- Beobachtung: Berechnen von Wurzeln in $\mathbb{Z}_p$ ist effizient möglich.
- Ziehen von Quadratwurzeln in $\mathbb{Z}_N$ ist äquivalent zum Faktorisieren.

Vorteil: CPA-Sicherheit beruht nur auf Faktorisierungsannahme.

- RSA: Berechnen von e-ten Wurzeln in $\mathbb{Z}_n$.
- Goldwasser-Micali: Unterscheiden von QR_N und QNR_N.

Satz Ziehen von Wurzeln in $\mathbb{Z}_p$

Sei p prim mit $p = 3 \bmod 4$ und $a \in QR_p$. Dann gilt für $b = a^{\frac{p+1}{4}} \bmod p$, dass $b^2 = a \bmod p$.

Beweis:

- Es gilt $\left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \cdot a = a \bmod p$.
- Man beachte, dass $\frac{p+1}{4} \in \mathbb{N}$ wegen $p = 3 \bmod 4$.

Quadratwurzel bei bekannter Faktorisierung

Definition Blum-Zahl

Sei $N = pq$ ein RSA-Modul. N heißt *Blum-Zahl* falls $p = q = 3 \bmod 4$.

Satz Quadratwurzeln in $\mathbb{Z}_N$

Sei $N = pq$ eine Blum-Zahl mit bekannten p, q. Dann können die vier Quadratwurzeln von $a \in QR_N$ in Zeit $\mathcal{O}(\log^3 N)$ berechnet werden.

Beweis:

Algorithmus QUADRATWURZEL

EINGABE: $N, p, q, a \in QR_N$

1. Berechne $x_p \leftarrow a^{\frac{p+1}{4}} \bmod p$, $x_q \leftarrow a^{\frac{q+1}{4}} \bmod q$.
2. Berechne mittels Chinesischem Restsatz die Lösungen von
$$\left| \begin{array}{l} b_1 = x_p \bmod p \\ b_1 = x_q \bmod q \end{array} \right|, \left| \begin{array}{l} b_2 = -x_p \bmod p \\ b_2 = x_q \bmod q \end{array} \right|, \left| \begin{array}{l} b_3 = x_p \bmod p \\ b_3 = -x_q \bmod q \end{array} \right|, \left| \begin{array}{l} b_4 = -x_p \bmod p \\ b_4 = -x_q \bmod q \end{array} \right|$$

AUSGABE: $b_1, \ldots, b_4$ mit $b_i^2 = a \bmod N$

Quadratwurzeln ohne Faktorisierung

Spiel Wurzelziehen $SQR_{\mathcal{A},GenModulus}(n)$

1. $(N, p, q) \leftarrow Genmodulus(n)$
2. Wähle $z \in QR_N$.
3. $y \leftarrow \mathcal{A}(N, z)$
4. $$SQR_{\mathcal{A},GenModulus}(n) = \begin{cases} 1 & \text{falls } y^2 = z \bmod N \\ 0 & \text{sonst} \end{cases}.$$

Definition Quadratwurzelannahme

Das *Berechnen von Quadratwurzeln* ist hart bezüglich *GenModulus*, falls für alle ppt $\mathcal{A}$ gilt $\mathrm{Ws}[SRQ_{\mathcal{A},GenModulus}(n) = 1] \leq \mathrm{negl}(n)$.
Quadratwurzelannahme: Berechnen von Quadratwurzeln ist hart.

Nicht-triviale Quadratwurzeln

Satz Faktorisieren mit Wurzeln

Sei $N = pq$ ein RSA-Modul. Seien $x, y \in \mathbb{Z}_N^*$ mit $x^2 = y^2 \bmod N$ und $x \neq \pm y \bmod N$. Dann können p, q in Zeit $\mathcal{O}(\log^2 N)$ berechnet werden.

Beweis:

- Mittels CRT erhalten wir $x \simeq (x_p, x_q) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$.
- Es gilt $y = (x_p, -x_q)$ oder $y = (-x_p, x_q)$.
- Wir betrachten den Fall $y = (x_p, -x_q)$. Der zweite Fall ist analog.
- Es gilt $x + y = (2x_p, 0)$ bzw. $x - y = (0, 2x_q)$.
- Damit folgt $\mathrm{ggT}(N, x + y) = q$ bzw. $\mathrm{ggT}(N, x - y) = p$ wegen $2x_p \in \mathbb{Z}_p^*$ und $2x_q \in \mathbb{Z}_q^*$.

Quadratwurzeln implizieren Faktorisierung

Satz Quadratwurzeln implizieren Faktorisierung

Quadratwurzel- und Faktorisierungsannahme sind äquivalent.

Beweis:

- Bereits gezeigt: Faktorisierung impliziert Quadratwurzeln.
- z.z.: $\mathcal{A}$ für Quadratwurzel impliziert $\mathcal{A}_{factor}$ für Faktorisierung.
- Sei $\epsilon(n) = \mathrm{Ws}[SQR_{\mathcal{A},GenModulus}(n) = 1]$.

Algorithmus $\mathcal{A}_{factor}$

EINGABE: N

1. Wähle $x \in \mathbb{Z}_N^*$ und berechne $z \leftarrow x^2 \bmod N$.
2. $y \leftarrow \mathcal{A}(N, z)$
3. Falls $x = \pm y$, Abbruch.

AUSGABE: $p, q = \{\mathrm{ggT}(N, x + y), \mathrm{ggT}(N, x - y)\}$

Faktorisieren mit Quadratwurzeln

- Unter der Faktorisierungsannahme gilt

$$\begin{aligned}
\mathrm{negl}(n) &\geq \mathrm{Ws}[\mathit{Factor}_{\mathcal{A}_{\mathit{factor}},\mathit{GenModulus}}(n) = 1] \\
&= \mathrm{Ws}[x \neq \pm y \bmod N \wedge x^2 = y^2 \bmod N] \\
&= \mathrm{Ws}[x \neq \pm y \bmod N \mid y^2 = z \bmod N] \cdot \mathrm{Ws}[y^2 = z \bmod N] \\
&= \mathrm{Ws}[x \neq \pm y \bmod N \mid y^2 = z \bmod N] \cdot \epsilon(n) \\
&= \frac{1}{2} \cdot \epsilon(n)
\end{aligned}$$

- Die letzte Gleichung folgt, da z exakt vier Wurzeln in $\mathbb{Z}_N^*$ besitzt.