Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Felix Heuer

RUHR UNIVERSITÄT BOCHUM RUB

Präsenzübungen zur Vorlesung

Kryptographie 2

SS 2011

Blatt 5 / 8. und 10. Juni 2011

AUFGABE 1. Illustratives.

Wir erinnern kurz an die Definition folgender Mengen: Sei

$$\mathcal{J}_N^{+1} := \left\{ x \in \mathbb{Z}_N^* : \left(\frac{x}{N}\right) = +1 \right\}$$

die Menge aller x mit Jacobi-Symbol $+1$ und

$$\mathcal{QR}_N := \left\{ y \in \mathbb{Z}_N^* : \exists x \in \mathbb{Z}_N^* \text{ mit } y = x^2 \bmod N \right\}$$

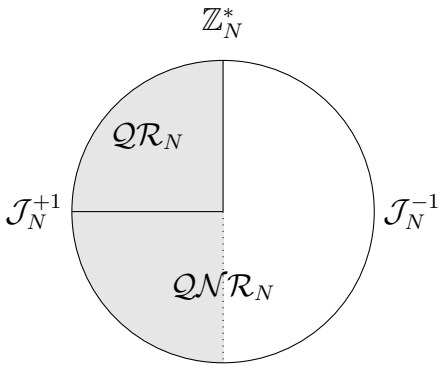
die Menge aller quadratischen Reste. Sei außerdem

$$\mathcal{QNR}_N := \mathbb{Z}_N^* \setminus \mathcal{QR}_N$$

die Menge der quadratischen Nichtreste und

$$\mathcal{QNR}_N^{+1} := \mathcal{J}_N^{+1} \setminus \mathcal{QR}_N$$

die Menge der quadratischen Nichtreste mit Jacobi-Symbol $+1$.
Sei $N = pq$ für prime, ungerade $p \neq q$. Beweisen Sie das folgende anschauliche Bild für die Verteilung der obigen Mengen in $\mathbb{Z}_N^*$.



Zeigen Sie hierfür:

a) $\frac{|\mathcal{J}_N^{+1}|}{|\mathbb{Z}_N^*|} = \frac{1}{2}$

b) $\mathcal{QR}_N \subset \mathcal{J}_N^{+1}$

c) $\frac{|\mathcal{QR}_N|}{|\mathcal{J}_N^{+1}|} = \frac{1}{2}$.

AUFGABE 2. Subtiles.
Betrachten Sie folgende modifizierte Version der *quadratischen Residuositätsannahme* (vgl. Folie 88), in welcher der Unterscheider $y \in_R \mathcal{QNR}_N$ anstelle von $y \in_R \mathcal{QNR}_N^{+1}$ erhält.

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

$$\left| \mathop{\mathbf{Ws}}_{x \in_R \mathcal{QR}_N} [\mathcal{D}(1^n, N, x) = 1] - \mathop{\mathbf{Ws}}_{y \in_R \mathcal{QNR}_N} [\mathcal{D}(1^n, N, y) = 1] \right| \leq \mathsf{negl}(n) \ .$$

Zeigen Sie, dass die modifizierte Annahme nie gelten kann, indem Sie einen Unterscheider $\mathcal{D}$ konstruieren, der die beiden Verteilungen mit Wahrscheinlichkeit $\geq \frac{2}{3}$ unterscheidet.

AUFGABE 3. Beweisdetail.
Im Beweis der CPA-Sicherheit der Goldwasser-Micali Verschlüsselung (Folie 92) benutzen wir, dass für $x \in_R \mathbb{Z}_N^*$ das zugehörige x^2 uniform in der Menge $\mathcal{QR}_N$ verteilt ist. Beweisen Sie diese Behauptung formal. Zeigen Sie, dass für beliebiges $y \in \mathcal{QR}_N$ gilt

$$\mathop{\mathbf{Ws}}_{x \in_R \mathbb{Z}_N^*} \left[x^2 = y \right] = \frac{1}{|\mathcal{QR}_N|} \ .$$

AUFGABE 4. Wurzelbehandlung.
In der Vorlesung haben wir einen einfachen Algorithmus zur Berechnung von Quadratwurzeln $\bmod p$ kennengelernt, sofern $p \equiv 3 \bmod 4$ gilt (Folie 94). Wir wollen nun den folgenden *probabilistischen* Algorithmus für den anderen Fall $p \equiv 1 \bmod 4$ studieren.

Algorithmus WURZEL(p, a)
Input: Primzahl p mit $p \equiv 1 \bmod 4$ und $a \in \mathcal{QR}_p$.
Output: Eine Quadratwurzel $x \in \mathbb{Z}_p^*$ von a, d.h. $x^2 \equiv a \bmod p$.

01 Wähle $b \in \mathcal{QNR}_p$.
02 Berechne $\ell \in \mathbb{N}$ und m ungerade mit $2^\ell m = \frac{p-1}{2}$.
03 Setze $r := 2^\ell m$ und $r' := 0$.
04 **For** $i = \ell$ **to** 1 **do**
05 $\quad r := r/2$ und $r' := r'/2$.
06 $\quad$ **If** $a^r b^{r'} = -1 \bmod p$ **then** $r' := r' + 2^\ell m$.
07 **End For**
08 Output $x := a^{\frac{r+1}{2}} b^{\frac{r'}{2}} \bmod p$.

Wieso ist WURZEL probabilistisch? Zeigen Sie ferner:

a) WURZEL ist *korrekt* ist, d.h. das die Ausgabe x tatsächlich eine Quadratwurzel von a ist. Begründen Sie, wieso x wohldefiniert ist (dafür müssen $r+1$ und r' gerade sein).

b) WURZEL hat Laufzeit $\mathsf{poly}(\log_2 p)$ wobei $\log_2 p$ die Bitlänge von p ist.

Hinweis: Teil a) ist leicht, wenn man zeigt, das zu jedem Zeitpunkt die Gleichung $a^r b^{r'} = 1 \bmod p$ erfüllt ist.