Prof. C. P. Schnorr Sommersemester 2011

Kryptographie

Blatt 3, 04.05.2011, Abgabe 11.05.2011

Aufgabe 1. Sei $n = p \cdot q$, p, q prim mit $p, q = 3 \bmod 4$, n heisst *Blum–Zahl.*

Zeige 1. $|QR_n| = \varphi(n)/4 = 1 \bmod 2$, für $QR_n := (\mathbb{Z}_n^*)^2$

2. $x \mapsto x^2 \bmod n$ ist bijektiv auf QR_n

3. Die Berechnung $x \mapsto \sqrt{x}$ für $x \in QR_n$ geht in polynomialer Zeit, sofern $\varphi(n)$ gegeben ist.

Hinweis zu 3: Berechnung von p, q aus $\varphi(n)$:

$$p + q = n - \varphi(n) + 1\ , \quad (p-q)^2 = (p+q)^2 - 4n,$$

Für $b \in QR_p$ gilt $\sqrt{b} = b^a$ für $a := 2^{-1} \bmod |QR_p|$.

Aufgabe 2. Sei $p = 1 \bmod 4$ prim.

Zeige: $QR_p \ni b \mapsto \sqrt{b}$ geht in prob. polynomial-Zeit.

Hinweis: Algorithm 3.34 in Handbook of Applied Cryptography.

Aufgabe 3. Zeige, dass für die generische ElGamal-Verschl. die Aufgabe zu gegebenem m gültige von ungültigen Ziffertexten von m zu unterscheiden, so schwierig ist wie DDH: DDH $\leq_{\text{pol}}$ IND.

Punktzahl pro Aufgabe 5.