

8. Woche

Quadratische Reste und Anwendungen

Quadratische Reste

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

$$QR_n = \{a \in \mathbb{Z}_n^* \mid a \text{ ist ein quadratischer Rest}\} \text{ und } QNR_n = \mathbb{Z}_n^* \setminus QR.$$

Lemma Anzahl quadratischer Reste in primen Restklassen

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

- Sei $a \in QR_p$. Dann gilt $a = b^2 = (-b)^2$.
- ⇒ jeder quadratische Rest besitzt ≥ 2 Quadratwurzeln.
- Da $\mathbb{F}_p$ ein Körper ist, besitzt das Polynom $p(x) = x^2 - a$ hat höchstens zwei Nullstellen in $\mathbb{F}_p$. D.h. a hat ≤ 2 Quadratwurzeln.
 - Damit bildet $f : \mathbb{Z}_p^* \rightarrow QR, x \mapsto x^2 \bmod p$ jeweils genau zwei Elemente $\pm b$ auf einen quadratischen Rest $a \in QR$ ab.
- ⇒ genau die Hälfte der Elemente in $\mathbb{Z}_p^*$ ist in QR .

Das Legendre Symbol

Definition Legendre Symbol

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

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

Notation, Fakte (aus DiMa I)

$\mathbb{F}_p := \left(\frac{\mathbb{Z}}{p\mathbb{Z}}, +, \cdot, 0, 1\right)$ Körper.

Die multiplikative Gruppe $\mathbb{F}_p^* = \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ ist zyklisch.

Berechnung des Legendre Symbols

Satz

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

Beweis

- 1 Für $p|a$ sind beide Seiten Null. Gelte also $p \nmid a$.
- 2 Da $a^{p-1} = 1 \bmod p$, folgt $a^{\frac{p-1}{2}} = \pm 1$.
- 3 Sei g Generator von $\mathbb{Z}_p^*$ und $a = g^j$ für ein $j \in \mathbb{Z}_{p-1}$.
- 4 Es gilt für die linke Seite $a \in QR_p$ gdw. j gerade ist.
- 5 Andererseits $a^{\frac{p-1}{2}} = g^{\frac{j(p-1)}{2}} = 1$ gdw $p-1$ teilt $\frac{j(p-1)}{2}$.
- 6 Damit ist die rechte Seite ebenfalls 1 gdw j gerade ist.

Das Legendresymbol lässt sich in Zeit $\mathcal{O}(\log a \log^2 p)$ berechnen.

Eigenschaften des Legendre Symbols

Eigenschaften Quadratischer Reste mod p

- ➊ Multiplikativität: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
 - ➋ $(QR_p, \cdot)$ ist eine multiplikative Gruppe.
 - ➌ $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{für } p \equiv \pm 1 \pmod{8} \\ -1 & \text{für } p \equiv \pm 3 \pmod{8}. \end{cases}$
-
- ➊ Zwei Beweise:
 - ➊ 1. Beweis: $\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} \pmod{p} = a^{\frac{p-1}{2}} \pmod{p} \cdot b^{\frac{p-1}{2}} \pmod{p} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
 - ➋ 2. Beweis: Schreibe $a = g^j$ und $b = g^k$. Dann $ab = g^{j+k}$. Wenn j, k beide gerade (a, b Quadrate) dann $j+k$ gerade (also ab Quadrat), usw ...
 - ➋ Es bleibt zu Zeigen, dass $a \in QR \Rightarrow a^{-1} \in QR$. Wieder zwei Beweise.
 - ➊ 1. Beweis: $a = g^j$, also $a^{-1} = g^{p-1-j}$. j gerade $\Rightarrow p-1-j$
 - ➋ 2. Beweis: $a = b^2$, und $b \neq 0$. Also $\exists b^{-1} \Rightarrow (b^{-1})^2 = a^{-1} \Rightarrow a^{-1} \in QR$.
 - ➌ ohne Beweis (nicht-trivial)

Das Quadratische Reziprozitätsgesetz

Satz Quadratisches Reziprozitätsgesetz (Gauß)

Seien $p, q > 2$ prim. Dann gilt

$$\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{für } p = q = 3 \bmod 4 \\ \left(\frac{p}{q}\right) & \text{sonst.} \end{cases}$$

ohne Beweis (nicht-trivial)

- Liefert alternativen Algorithmus zur Berechnung des Legendre Symbols.

- **Bsp:**
$$\begin{aligned} \left(\frac{6}{11}\right) &= \left(\frac{3}{11}\right) \cdot \left(\frac{2}{11}\right) = -\left(\frac{11}{3}\right) \cdot (-1) \\ &= -\left(\frac{2}{3}\right) \cdot (-1) = -(-1) \cdot (-1) = (-1). \end{aligned}$$

- D.h. 6 ist quadratischer Nichtrest in $\mathbb{Z}_{11}^*$.
- Benötigen Primfaktorzerlegung, um das QR-Gesetz anzuwenden.

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

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

- **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.

Verallgemeinerungen für das Jacobi Symbol

Satz

Für alle ungeraden m, n gilt

$$\textcircled{1} \quad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

$$\textcircled{2} \quad \left(\frac{m}{n}\right) = (-1)^{\frac{(m-1)(n-1)}{4}} \left(\frac{n}{m}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{für } m = n = 3 \bmod 4 \\ \text{sonst.} \end{cases}.$$

Wir beweisen hier nur das Analog des Reziprozitätsgesetzes.

- Falls $\text{ggT}(m, n) > 1$, sind beide Seiten 0. Sei also $\text{ggT}(m, n) = 1$.
- Schreiben Primfaktorzerlegung $m = p_1 \dots p_r$ und $n = q_1 \dots q_s$. (p_i 's und q_j 's können dabei jeweils mehrmals auftreten)
- Wandeln $\left(\frac{m}{n}\right) = \prod_{i,j} \left(\frac{p_i}{q_j}\right)$ zu $\left(\frac{n}{m}\right) = \prod_{i,j} \left(\frac{q_j}{p_i}\right)$ durch rs -malige Anwendung des Reziprozitätsgesetzes.
- Anzahl (-1) entspricht Anzahl Paare (i, j) mit $p_i = q_j = 3 \bmod 4$.
- D.h. $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$ gdw. ungerade viele p_i, q_j kongruent $3 \bmod 4$.
- Es gibt ungerade viele $p_i, q_j = 3 \bmod 4$ gdw. $m = n = 3 \bmod 4$ ist.

Rekursive Berechnung des Jacobi Symbols

Algorithmus Jacobi-Symbol

EINGABE: m, n mit n ungerade

- 1 Falls $\text{ggT}(m, n) > 1$, Ausgabe 0.
- 2 Sei $m = 2^k m'$ mit m' ungerade.
- 3 Ausgabe $(-1)^{\frac{k(n^2-1)}{8}} \cdot (-1)^{\frac{(m'-1)(n-1)}{4}} \cdot \text{Jacobi-Symbol}(n \bmod m', m')$

AUSGABE: $\left(\frac{m}{n}\right)$

Bsp: $\left(\frac{14}{15}\right) = \left(\frac{2}{15}\right) \cdot \left(\frac{7}{15}\right) = (-1) \cdot \left(\frac{15 \bmod 7}{7}\right) = (-1).$

- **Laufzeit:** Analog zum Euklidischen Algorithmus: $\mathcal{O}(\log \max\{m, n\})$ rekursive Aufrufe.
- Jeder Aufruf kostet $\mathcal{O}(\log^2 \max\{m, n\})$.
- **Korrektheit:** Für ungerades n gilt

$$\left(\frac{m}{n}\right) = \left(\frac{2}{n}\right)^k \cdot \left(\frac{m'}{n}\right) = \left(\frac{2}{n}\right)^k \cdot (-1)^{\frac{(m'-1)(n-1)}{4}} \left(\frac{n \bmod m'}{m'}\right).$$

Das Quadratische Reste Problem

Definition Pseudoquadrates

Sei $N = pq$ mit p, q prim. Eine Zahl a heißt *Pseudoquadrat* bezüglich N , falls

$$\left(\frac{a}{N}\right) = 1 \quad \text{und} \quad a \notin QR_N.$$

Wir definieren die Sprache

$$\text{QUADRAT} := \{a \in \mathbb{Z}_N^* \mid a \in QR_N\}.$$

Sprache = Teilmenge der Menge aller Worte über einem Alphabet.

Sprache entscheiden = bestimmen, ob Wort in Sprache ist.

Distinguisher = Entscheider = Algorithmus, der entscheidet.

- Für alle Pseudoquadrates a gilt: $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = (-1)$.
- D.h. die Sprache QUADRAT kann effizient entschieden werden, falls p, q bekannt sind. Im Allgemeinen ist nur N bekannt.

Quadratische Reduktionsannahme (QR-Annahme)

Es gibt keinen polynomiellen Algorithmus, der QUADRAT entscheidet.

Quadratwurzeln in $\mathbb{Z}_N^*$

Satz Quadratwurzeln in $\mathbb{Z}_N^*$

Sei $N = pq$ mit p, q prim und $p \equiv q \equiv 3 \pmod{4}$ (sogenannte Blum-Zahl). Dann besitzt jedes $a = x^2 \in QR_N$ genau eine Quadratwurzel in QR_N , die sogenannte Hauptwurzel.

- Die Lösungen des Gleichungssystems $\begin{cases} y \equiv \pm x \pmod{p} \\ y \equiv \pm x \pmod{q} \end{cases}$ liefern mittels Chinesischem Restsatz 4 Lösungen in $\mathbb{Z}_N^*$.
- Eine Lösung y ist in QR_N gdw sie in $QR_p \times QR_q$ (d.h. wenn $y \pmod{p}$, bzw. $y \pmod{q}$ Quadrat mod p , bzw. q ist).
- Betrachten Lösung modulo p (analog mod q): Es ist $\left(\frac{x}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{-x}{p}\right) = (-1) \cdot \left(\frac{-x}{p}\right)$ da $p \equiv 3 \pmod{4}$.
- D.h. $\left(\frac{x}{p}\right) = -\left(\frac{-x}{p}\right)$ und entweder x oder $-x$ ist in QR_p .
- Damit ist genau eine der 4 Lösungen in QR_N , nämlich die Lösung von $\begin{cases} y \equiv \epsilon_p x \pmod{p} \\ y \equiv \epsilon_q x \pmod{q} \end{cases}$ mit $\epsilon_p, \epsilon_q \in \{\pm 1\}$ und $\epsilon_p x$ bzw. $\epsilon_q x \in QR_p$ bzw. QR_q .

Berechnen von Quadratwurzeln modulo p

Satz Quadratwurzeln mod p

Sei p prim, $p \equiv 3 \pmod{4}$ und $a \in QR_p$. Dann sind die beiden Quadratwurzeln von a von der Form

$$x = \pm a^{\frac{p+1}{4}} \pmod{p}, \text{ wobei } a^{\frac{p+1}{4}} \in QR_p.$$

- Es gilt

$$x^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \cdot a = \left(\frac{a}{p}\right) \cdot a = a \pmod{p}.$$

- Ferner gilt $a^{\frac{p+1}{4}} \pmod{p} \in QR_p$ wegen

$$\left(\frac{a^{\frac{p+1}{4}}}{p}\right) = \left(\frac{a}{p}\right)^{\frac{p+1}{4}} = 1.$$

D.h. Quadratwurzeln können in Zeit $\mathcal{O}(\log^3 p)$ berechnet werden.

Kryptographische Anwendungen von Quadratischen Resten.

1. Blum-Blum-Shub (BBS) Pseudozufallsgenerator

Korollar vom Satz Quadratwurzeln in $\mathbb{Z}_N^*$

Die Abb. $f : QR_N \rightarrow QR_N, x \mapsto x^2 \bmod N$ ist eine Bijektion auf QR_N .

- (k, ℓ) Pseudozufallsgeneratoren generieren aus k Zufallsbits eine Sequenz von $\ell > k$ Zufallsbits.
- Der (k, ℓ) BBS Generator verwendet obige Bijektion.

Algorithmus BBS Pseudozufallsgenerator (1986)

EINGABE: $N = pq$ Blumzahl der Bitlänge $|N| = k$,
 1^ℓ mit $\ell \in \mathbb{N}$ und $\ell > k$

- 1 Wähle $a \in \mathbb{Z}_N^*$ und setze $s_0 = a^2 \bmod N$.
- 2 For $i = 1$ to ℓ
 - 1 Setze $s_i \leftarrow s_{i-1}^2 \bmod N$. Gib $z_i = s_i \bmod 2$ aus.

AUSGABE: $(z_1, \dots, z_\ell) \in \{0, 1\}^\ell$.

Laufzeit: $\mathcal{O}(\ell \log^2 N)$, d.h. polynomiell in der Eingabelänge.

Die Sicherheit des BBS Generators

Sicherheit: Man kann die Verteilung der $(z_1, \dots, z_\ell)$ nicht von der uniformen Verteilung auf $\{0, 1\}^\ell$ unterscheiden.

Man kann folgendes zeigen:

- Sei A ein polynomieller Unterscheider für $(z_1, \dots, z_\ell)$.
- Dann gibt es einen polyn. Algorithmus B , der $s_0 \bmod 2$ berechnet.

Satz Sicherheit des BBS Generators

Die Ausgabe des BBS Generators ist von der Gleichverteilung in polynomieller Zeit ununterscheidbar unter der QR-Annahme.

- Annahme: $\exists$ polyn. Unterscheider A für den BBS Generator.
- Sei B ein Algorithmus, der $s_0 \bmod 2$ berechnet.
- Zeigen, dass dann ein polyn. Algorithmus für QUADRAT existiert.
(Widerspruch zur Quadratischen Residuositätsannahme)

Entscheiden der Sprache QUADRAT

Algorithmus für QUADRAT

EINGABE: $a \in \mathbb{Z}_N^*$ mit $\left(\frac{a}{N}\right) = 1$

- 1 Setze $s_0 \leftarrow a \bmod N$.
- 2 Berechne $(z_1, \dots, z_\ell)$ mittels BBS Generator.
- 3 Berechne $z_0 \leftarrow B(z_1, \dots, z_\ell)$.
- 4 Falls $z_0 = (a \bmod 2)$, Ausgabe " $x \in QR_N$ ".
Sonst Ausgabe " $x \notin QR_N$ ".

Laufzeit: $\mathcal{O}(\ell \cdot \log^2 N + T(B))$

Korrektheit:

- Wegen $\left(\frac{a}{N}\right) = 1$ ist entweder a oder $(-a) = N - a$ in QR_N .
- D.h. a oder $(-a)$ ist eine Hauptwurzel von $s_1 = a^2 \bmod N$.
- Genau eine der beiden Zahlen $a, (-a)$ ist gerade.
- z_0 ist das unterste Bit der Hauptwurzel von $s_1 = a^2 \bmod N$.
- D.h. a ist eine Hauptwurzel gdw z_0 und $a \bmod 2$ übereinstimmen.

2. Probabilistische Verschlüsselung

Parameter des Goldwasser-Micali Kryptosystems (1984):

- Sei $N = pq$.
- Sei $a \in \mathbb{Z}_N^*$ ein Pseudoquadrat (falls N Blumzahl, kann man $N - 1$ nehmen).
- Verschlüsselt werden Bits $m \in \{0, 1\}$.

Goldwasser-Micali Kryptosystem

- 1 Verschlüsselung von m unter Verwendung von N, a .
 - ▶ Wähle $r \in \mathbb{Z}_N^*$.
 - ▶ Berechne $e(m, r) = a^m r^2 \bmod N$.
- 2 Entschlüsselung von $c = e(m, r)$ unter Verwendung von p, q .
 - ▶ Berechne $\left(\frac{c}{p}\right) = c^{\frac{p-1}{2}} \bmod p$.
 - ▶ Setze $m = d(c) = \begin{cases} 0 & \text{falls } c \in QR_N, \text{ d.h. falls } \left(\frac{c}{p}\right) = 1. \\ 1 & \text{falls } c \notin QR_N, \text{ d.h. falls } \left(\frac{c}{p}\right) = (-1). \end{cases}$

Sicherheit des Goldwasser-Micali Kryptosystems

Korrektheit

- Falls $m = 0$ ist $c = r^2$ ein zufälliger quadratischer Rest in $\mathbb{Z}_N^*$.
- Falls $m = 1$ ist $c = x \cdot r^2$ ein zufälliges Pseudoquadrat.
- Es gilt $\left(\frac{c}{N}\right) = \left(\frac{a^m r^2}{N}\right) = \left(\frac{a}{N}\right)^m \cdot \left(\frac{r^2}{N}\right) = 1$.
- D.h. entweder $\left(\frac{c}{p}\right) = \left(\frac{c}{q}\right) = 1$ oder $\left(\frac{c}{p}\right) = \left(\frac{c}{q}\right) = (-1)$.
- Im ersten Fall ist $c \in QR_N$, im zweiten Fall gilt $c \notin QR_N$.

Laufzeit:

- Verschlüsselung: $\mathcal{O}(\log^2 N)$
- Entschlüsselung: $\mathcal{O}(\log^3 N)$ (verbessert: $\mathcal{O}(\log^2 N)$)

Satz Sicherheit des Goldwasser-Micali Kryptosystems

Das GM Kryptosystem ist sicher unter der QR-Annahme.

- Unterscheiden von Verschlüsselungen von 0 und 1 ist äquivalent zum Entscheiden der Sprache QUADRAT.

2.1. Bit Commitments

Szenario informal:

1 Commitment-Phase:

- ▶ Alice platziert ein Bit $b \in \{0, 1\}$ in einem Safe, der in Bob's Zimmer steht. Bob besitzt keinen Safeschlüssel.
- ▶ Bob kann den Safe nicht einsehen, lernt also nichts über b .
(Concealing Eigenschaft)

2 Revealing-Phase:

- ▶ Alice öffnet den Safe und zeigt Bob das Bit b .
- ▶ Alice kann ihr Bit dabei nicht ändern.
(Binding Eigenschaft)

Mathematische Modellierung

- Commitment mittels $f : \{0, 1\} \times X \rightarrow Y$ für endliche Mengen X, Y .
- Commitment (sog. Blob): Wähle $x \in X$ und sende $f(b, x)$ an Bob.
- Öffnen des Commitments: Sende b und x an Bob.

Bit Commitment via Goldwasser-Micali Kryptosystem

Öffentliche Parameter:

- Blumzahl N , Pseudoquadrat $a \in \mathbb{Z}_N^*$
- $X = Y = \mathbb{Z}_N^*$

Algorithmus Goldwasser-Micali Bit Commitment

1 Commitment-Phase

- ▶ Wähle $x \in \mathbb{Z}_N^*$.
- ▶ Sende Blob $f(b, x) = a^b x^2 \bmod N$ an Bob.

2 Revealing-Phase

- ▶ Sende b, x an Bob.
- ▶ Bob überprüft die Korrektheit von $f(b, x) = a^b x^2 \bmod N$.

Concealing Eigenschaft:

- Unter der QR-Annahme lernt Bob nichts über das Bit $b \in \{0, 1\}$.

Binding Eigenschaft

Satz

Goldwasser-Micali Commitments besitzen die Binding Eigenschaft.

- **Annahme:** Alice kann Blob $f(b, x)$ für $b = 0$ und $b = 1$ öffnen.
- D.h. Alice kann $x_1, x_2 \in \mathbb{Z}_N^*$ berechnen mit

$$f(b, x) = a^0 x_1^2 = a^1 x_2^2 \bmod N.$$

- Daraus folgt $a = \left(\frac{x_1}{x_2}\right)^2 \bmod N$, d.h. $\frac{x_1}{x_2}$ ist Quadratwurzel von a .
(Widerspruch: a ist ein Pseudoquadrat in $\mathbb{Z}_N^*$.)

2.2. Münzwurf über das Telefon

- Bit Commitments haben zahlreiche Anwendungen in kryptographischen Protokollen.
- Exemplarisch hier ein Protokoll für einen fairen Münzwurf.

Algorithmus Münzwurf via Internet

- 1 Alice sendet Bob Commitment für Bit $b \in \{0, 1\}$.
 - 2 Bob rät ein Bit $b' \in \{0, 1\}$.
 - 3 Alice öffnet ihr Bit. Bob gewinnt gdw $b' = b$.
- Concealing-Eigenschaft verhindert, dass Bob etwas über b lernt.
 - Binding-Eigenschaft verhindert, dass Alice b in $1 - b'$ ändert.

3. Das Blum-Goldwasser Kryptosystem

- Öffentlicher Parameter: Blumzahl $N = pq$
- Klartextraum: $\{0, 1\}^\ell$ für ein beliebiges ℓ
- Chiffretextraum: $\{0, 1\}^\ell \times \mathbb{Z}_N^*$

Blum-Goldwasser Kryptosystem (1985)

❶ Verschlüsselung von $m = (m_1, \dots, m_\ell) \in \{0, 1\}^\ell$ mittels N

- ▶ Wähle $r \in \mathbb{Z}_N^*$.
- ▶ $\mathbf{z} = (z_1, \dots, z_\ell) \leftarrow$ BBS Generator auf $s_0 = r^2 \bmod N$.
- ▶ Berechne $\mathbf{c} = \mathbf{m} \oplus \mathbf{z}$ (Komponentenweise).
- ▶ Berechne $s_{\ell+1} = s_0^{2^{\ell+1}} \bmod N$.
- ▶ AUSGABE: Chiffretext $(\mathbf{c}, s_{\ell+1}) \in \{0, 1\}^\ell \times \mathbb{Z}_N^*$.

❷ Entschlüsselung von c mittels p, q .

- ▶ Berechne $s_0 \in \mathbb{Z}_N^*$ als Lösung von
$$\begin{cases} s_0 = s_{\ell+1}^{\left(\frac{p+1}{4}\right)^{\ell+1}} \bmod p \\ s_0 = s_{\ell+1}^{\left(\frac{q+1}{4}\right)^{\ell+1}} \bmod q \end{cases}.$$
- ▶ $\mathbf{z} = (z_1, \dots, z_\ell) \leftarrow$ BBS Generator auf $s_0 = r^2 \bmod N$.
- ▶ AUSGABE: $\mathbf{m} = \mathbf{c} \oplus \mathbf{z}$

Laufzeit und Korrektheit

Korrektheit:

- $(z_1, \dots, z_\ell)$ wird als One-Time Pad für m verwendet.
- Entschlüsselung berechnet $\ell + 1$ -malig die Hauptwurzel von $s_{\ell+1}$.
- Dies rekonstruiert die Saat s_0 des BBS Generators.

Laufzeit:

- Verschlüsselung: $\mathcal{O}(\ell \cdot \log^2 N)$
- Entschlüsselung: $\mathcal{O}(\log^3 N + \ell \cdot \log^2 N)$.

Fakt Sicherheit des BG-Kryptosystems

Das Blum Goldwasser Kryptosystem ist sicher unter der Annahme, dass Blumzahlen $N = pq$ schwer zu faktorisieren sind.