

Das Quadratische Reste Problem

Definition Pseudoquadrate

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

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

Wir definieren die Sprache

$$\text{QUADRAT} := \{a \in \mathbb{Z}_N^* \mid \left(\frac{a}{N}\right) = 1 \text{ und } a \in QR_N\}.$$

- Für alle Pseudoquadrate 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 Reduzibilitätsannahme (QR-Annahme)

Es gibt keinen polynomiellen Algorithmus, der QUADRAT entscheidet.

Quadratwurzeln in \mathbb{Z}_N^*

Lemma

Sei $N = pq$ mit p, q prim und $p = q = 3 \pmod 4$ (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 $\left| \begin{array}{l} y = \pm x \pmod p \\ y = \pm x \pmod q \end{array} \right|$ liefern mittels Chinesischem Restsatz 4 Lösungen in \mathbb{Z}_N^* .
- Eine Lösung ist in QR_N gdw sie in $QR_p \times QR_q$ ist.
- Betrachten Lösung modulo p (analog mod q):

$$\left(\frac{x}{p}\right) = \left(\frac{(-1)(-x)}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{-x}{p}\right).$$

- Für $p = 3 \pmod 4$ gilt $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)$.
- 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 .

Der Blum-Blum-Shub (BBS) Pseudozufallsgenerator

Korollar

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 $a \in_R \mathbb{Z}_N^*$ 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_ℓ) nicht von der uniformen Verteilung auf $\{0, 1\}^\ell$ unterscheiden.

Man kann folgendes zeigen:

- Sei A ein polynomieller Unterscheider für (z_1, \dots, z_ℓ) .
- 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_ℓ) 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.

Probabilistische Verschlüsselung

Parameter des Goldwasser-Micali Kryptosystems (1984):

- Sei $N = pq$ eine Blumzahl, d.h. $p = q = 3 \pmod{4}$.
- Sei $a \in \mathbb{Z}_N^*$ ein Pseudoquadrat.
- Verschlüsselt werden Bits $m \in \{0, 1\}$.

Goldwasser-Micali Kryptosystem

- 1 Verschlüsselung von m unter Verwendung von N, a .
 - ▶ Wähle $r \in_R \mathbb{Z}_N^*$.
 - ▶ Berechne $e(m, r) = a^m r^2 \pmod{N}$.
- 2 Entschlüsselung von $c = e(m, r)$ unter Verwendung von p, q .
 - ▶ Berechne $\left(\frac{c}{p}\right) = c^{\frac{p-1}{2}} \pmod{p}$.
 - ▶ 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.

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 $x \in_R \mathbb{Z}_N^*$.
- ▶ 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

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

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

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.

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.

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)

- 1 Verschlüsselung von $m = (m_1, \dots, m_\ell) \in \{0, 1\}^\ell$ mittels N
 - ▶ Wähle $r \in_R \mathbb{Z}_N^*$.
 - ▶ $(z_1, \dots, z_\ell) \leftarrow$ BBS Generator auf $s_0 = r^2 \bmod N$.
 - ▶ For $i = 1$ to ℓ : Berechne $c_i = m_i + z_i \bmod 2$.
 - ▶ Berechne $s_{\ell+1} = s_0^{2^{\ell+1}} \bmod N$.
 - ▶ AUSGABE: Chiffretext $c = (c_1, \dots, c_\ell, s_{\ell+1}) \in \{0, 1\}^\ell \times \mathbb{Z}_N^*$.
- 2 Entschlüsselung von c mittels p, q .
 - ▶ Berechne $s_0 \in \mathbb{Z}_N^*$ als Lösung von
$$\left\{ \begin{array}{l} s_0 = s_{\ell+1}^{\left(\frac{p+1}{4}\right)^{\ell+1}} \bmod p \\ s_0 = s_{\ell+1}^{\left(\frac{q+1}{4}\right)^{\ell+1}} \bmod q \end{array} \right\}.$$
 - ▶ $(z_1, \dots, z_\ell) \leftarrow$ BBS Generator auf $s_0 = r^2 \bmod N$.
 - ▶ For $i = 1$ to ℓ : Berechne $m_i = c_i + z_i \bmod N$.

Laufzeit und Korrektheit

Korrektheit:

- (z_1, \dots, z_ℓ) 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.

Da war noch was ...

See you in August.

Viel Erfolg bei der Klausur!