Seminar Pseudozufall
bei Prof. Dr.rer.nat. Johannes Blömer

Der Blum-Blum-Shub Generator

Olga Anhalt

Universität Paderborn

Inhalt

Einführung

Konstruktion eines Pseudozufallsgenerators:

- $f : \{0,1\}^\star \longrightarrow \{0,1\}^\star$ eine Einwegpermutation
- $B : \{0,1\}^\star \longrightarrow \{0,1\}$ Hardcore Prädikat für f

$\forall$ Polynom l ist PZG $G^l : \{0,1\}^n \longrightarrow \{0,1\}^{l(n)}$ definiert durch

$$G^l(x) = B(x) \circ B(f(x)) \circ B(f(f(x))) \circ \ldots \circ B\left(f^{l(n)-1}(x)\right).$$

Der Blum-Blum-Shub Generator

Definition : Sei $N = P \cdot Q$ gegeben, wobei P und Q verschiedene Primzahlen gleicher Länge mit $P \equiv Q \equiv 3 \bmod 4$ sind. Man wählt x aus $\mathbb{Z}_N^\star$ zufällig und berechnet $x_0 := x^2 \bmod N$. Die folgenden Werte berechnen sich nach der Vorschrift:

$$x_{i+1} = x_i^2 \bmod N,$$
$$b_i = \text{das unterste Bit von } x_i \quad (i \geq 0)\,.$$

Dann ist die Folge $b_0, b_1, b_2, \ldots$ die Ausgabe des Blum-Blum-Shub Generators.

Beispiel: $N = P \cdot Q = 7 \cdot 19 = 133$, $x = 16$.
$x_0 = 16^2 \bmod 133 = 123$,
$x_1 = 123^2 \bmod 133 = 100$,
$x_2 = 100^2 \bmod 133 = 25$,
$x_3 = 25^2 \bmod 133 = 93$,
$x_4 = 93^2 \bmod 133 = 4$.

Somit erhalten wir: 10110.

Der Blum-Blum-Shub Generator

Effizienz:
Finde zwei Primzahlen P, Q, $P \neq Q$ mit $|P| = |Q|$ und $P \equiv Q \equiv 3 \bmod 4$:

- Die Hälfte der Primzahlen sind kongruent 3 modulo 4.

- Primzahltests benötigen polynomielle Laufzeit.

Die Werte $x_0, x_1, x_2, \ldots$ (und auch $b_0, b_1, b_2, \ldots$) sind in polynomieller Zeit berechenbar.

Ergebnisse der Zahlentheorie

$$\mathbb{Z}_N^\star = \{x \in \mathbb{N} \mid 0 < x < N \text{ und } \operatorname{ggT}(x, N) = 1\}$$

ist die multiplikative Gruppe der Ordnung $\varphi(N)$.

Ist P eine Primzahl, so ist

$$\mathbb{Z}_P^\star = \{x \in \mathbb{N} \mid 1 \leq x \leq P - 1\}$$

zyklisch.

Ergebnisse der Zahlentheorie

Ein $x \in \mathbb{Z}_N^\star$ heißt *quadratischer Rest modulo* N, falls ein $y \in \mathbb{Z}_N^\star$ existiert, so dass $y^2 = x \bmod N$ gilt.

Sei P ungerade Primzahl. Dann ist

$$QR_P = \left\{ x \in \mathbb{Z}_P^\star \mid x^{\frac{P-1}{2}} = 1 \bmod P \right\}$$

die Menge der quadratischen Reste modulo P.

QR_P ist eine Untergruppe von $\mathbb{Z}_P^\star$ der Ordnung $\frac{\varphi(P)}{2} = \frac{P-1}{2}$.

Ist $x \in QR_P$, d.h. es existiert ein $y \in \mathbb{Z}_P^\star$ mit $y^2 = x \bmod P$, so sind y und $-y$ *die Quadratwurzeln* von x.

Ergebnisse der Zahlentheorie

Definition 1.1. Sei P eine ungerade Primzahl. Für eine ganze Zahl a ist das *Legendresymbol* wie folgt definiert:

$$\left(\frac{a}{P}\right) = \begin{cases} 0 \text{ , falls } a \equiv 0 \bmod P \\ 1 \text{ , falls } a \text{ quadratischer Rest modulo } P \text{ ist} \\ -1 \text{ , falls } a \text{ kein quadratischer Rest modulo } P \text{ ist.} \end{cases}$$

Definition 1.2. Sei N eine ungerade natürliche Zahl mit der Primfaktorzerlegung

$$N = \prod_{i=1}^{k} P_i^{e_i}.$$

Sei a eine ganze Zahl. Dann ist das *Jacobisymbol* $\left(\frac{a}{N}\right)$ definiert durch

$$\left(\frac{a}{N}\right) = \prod_{i=1}^{k} \left(\frac{a}{P_i}\right)^{e_i}.$$

Ergebnisse der Zahlentheorie

Lemma 1.3. Für das Jacobisymbol gelten folgende Eigenschaften:

(a) Für $N \in \mathbb{N}$ ungerade und $a \in \mathbb{Z}$ mit $\operatorname{ggT}(a, N) \neq 1$ gilt $\left(\frac{a}{N}\right) = 0$.

(b) Für $N \in \mathbb{N}$ ungerade und $a, b \in \mathbb{Z}$ gilt $\left(\frac{ab}{N}\right) = \left(\frac{a}{N}\right) \cdot \left(\frac{b}{N}\right)$.

(c) Falls $N \in \mathbb{N}$ ungerade und $a \equiv b \bmod N$ ist, dann gilt $\left(\frac{a}{N}\right) = \left(\frac{b}{N}\right)$.

(d) Für $N \in \mathbb{N}$ ungerade gilt:

$$\left(\frac{2}{N}\right) = \begin{cases} 1 \text{ , falls } N \equiv \pm 1 \bmod 8 \\ -1 \text{ , falls } N \equiv \pm 3 \bmod 8. \end{cases}$$

(e) Für positive ungerade ganze Zahlen a und b gilt:

$$\left(\frac{a}{b}\right) = \begin{cases} -\left(\frac{b}{a}\right) & \text{, falls } a \equiv b \equiv 3 \bmod 4 \\ \left(\frac{b}{a}\right) & \text{, sonst.} \end{cases}$$

(f) Für $N \in \mathbb{N}$ ungerade gilt

$$\left(\frac{-1}{N}\right) = \begin{cases} 1 \text{ , falls } N \equiv 1 \bmod 4 \\ -1 \text{ , falls } N \equiv 3 \bmod 4. \end{cases}$$

Ergebnisse der Zahlentheorie

Im folgenden sei $N = P \cdot Q$, so dass P und Q verschiedene Primzahlen gleicher Länge mit $P \equiv Q \equiv 3 \bmod 4$ sind. Dann ist N sogenannte *Blum-Zahl* .

Mit $\mathbb{Z}_N^\star(+1)$ und $\mathbb{Z}_N^\star(-1)$ bezeichen wir die Mengen der Elementen von $\mathbb{Z}_N^\star$, die das Jacobisymbol $+1$ bzw. -1 haben.

Bemerkung: Kein Element von $\mathbb{Z}_N^\star(-1)$ und genau die Hälfte der Elementen von $\mathbb{Z}_N^\star(+1)$ sind quadratische Reste modulo N.

Mit QR_N bezeichnen wir die Menge der qudratischer Reste modulo N. QR_N ist eine Untergruppe von $\mathbb{Z}_N^\star$ der Ordnung $\frac{\varphi(N)}{4}$.

Das Quadratrest-Problem

Definition 1.4. (Quadratrest-Problem)
Seien N eine Blum-Zahl und $x \in \mathbb{Z}_N^\star(+1)$. Das Quadratrest-Problem mit Parameter N und x ist zu entscheiden, ob $x \in QR_N$ oder $x \in \mathbb{Z}_N^\star(+1) \setminus QR_N$ ist.

Quadratrest-Annahme: Seien $0 < \delta < 1$ eine feste Konstante, $t \in \mathbb{N}$ und N das Produkt zweier verschiedener ungerader Primzahlen gleicher Länge. Sei $\mathbf{A}[N, x]$ ein Algorithmus, der in polynomieller Zeit das Quadratrest-Problem löst, d.h. bei Eingabe N, x mit $|N| = |x| = n$ liefert $\mathbf{A}$ 1, falls $x \in QR_N$ ist, und 0 sonst. Dann ist für genügend große n und für alle bis auf δ-Anteil der Zahlen N der Länge n, die Wahrscheinlichkeit, dass $\mathbf{A}[N, x]$ nicht korrekt entscheidet, ob $x \in QR_N$ ist oder nicht, für ein uniform gewähltes x aus $\mathbb{Z}_N^\star(+1)$, größer als $\frac{1}{n^t}$:

$$\frac{\sum_{x \in \mathbb{Z}_N^\star(+1)} \Pr\left(\mathbf{A}\left[N, x\right] \text{ist nicht korrekt}\right)}{\varphi\left(N\right)/2} > \frac{1}{n^t}.$$

Das Quadratrest-Problem

Lemma 1.5. Sei $N = P \cdot Q$, so dass P und Q verschiedene Primzahlen mit $P \equiv Q \equiv 3 \bmod 4$ sind. Dann hat jeder quadratische Rest modulo N genau eine Quadratwurzel, die auch quadratischer Rest modulo N ist.

Satz 1.6. Sei N eine Blum-Zahl. Dann sind die Faktoren von N notwendig und hinreichend, um für ein beliebiges $x_0 \in QR_N$ das eindeutig bestimmte $x_{-1} \in QR_N$ mit $(x_{-1})^2 = x_0 \bmod N$ zu bestimmen.

Die Sicherheit des BBS Generators

Definition 2.2. Sei $0 < \epsilon \leq \frac{1}{2}$. Ein $0-1$ wertiger probabilistischer polynomialzeit Algorithmus $\mathbf{A}[\cdot,\cdot]$ hat einen ϵ-*Vorteil* für N beim Bestimmen des untersten Bits von x_{-1} (beim gegebenen $x_0 \in_R QR_N$) genau dann, wenn

$$\frac{\sum_{x_0 \in QR_N} Pr\left(\mathbf{A}\left[N, x_0\right] = \text{das unterste Bit von } x_{-1}\right)}{\frac{\varphi(N)}{4}} \geq \frac{1}{2} + \epsilon.$$

Definition 2.3. Sei $0 < \epsilon \leq \frac{1}{2}$. Ein $0-1$ wertiger probabilistischer polynomialzeit Algorithmus $\mathbf{B}[\cdot,\cdot]$ hat einen ϵ-*Vorteil* für N beim Entscheiden für ein beliebiges $x_0 \in_R \mathbb{Z}_N^\star(+1)$, ob x_0 quadratischer Rest modulo N ist oder nicht, genau dann, wenn

$$\frac{\sum_{x_0 \in QR_N} Pr\left(\mathbf{B}\left[N, x_0\right] = 1\right) + \sum_{x_0 \in \mathbb{Z}_N^\star(+1) \setminus QR_N} Pr\left(\mathbf{B}\left[N, x_0\right] = 0\right)}{\frac{\varphi(N)}{2}} \geq \frac{1}{2} + \epsilon.$$

Die Sicherheit des BBS Generators

Lemma 2.4. Ein ϵ-Vorteil für das Bestimmen des untersten Bits von x_{-1} für ein gegebenes $x_0 \in QR_N$ kann effizient zu einem ϵ-Vorteil für das Entscheiden, ob ein $x \in \mathbb{Z}_N^\star(+1)$ der quadratische Rest modulo N ist oder nicht, umgewandelt werden.

Lemma 2.5. Ein ϵ-Vorteil für das Entscheiden, ob ein $x \in \mathbb{Z}_N^\star(+1)$ der quadratische Rest modulo N ist oder nicht, kann effizient zu einem $\frac{1}{2} - \epsilon$ Vorteil erweitert werden.

Die Sicherheit des BBS Generators

Definition 2.6.

(a) Sei *poly* ein Polynom. Ein *Vorhersager* $\mathbf{A}[\cdot,\cdot]$ ist ein probabilistischer polynomialzeit Algorithmus, der bei Eingabe $N, b_1, \ldots, b_k$ mit $b_i \in \{0,1\}$ und $k \leq poly(|N|)$, die Ausgabe 0 oder 1 hat.

(b) $\mathbf{A}$ hat einen ϵ-*Vorteil* für N beim Vorhersagen des vorhergehenden Bits der vom Blum-Blum-Shub Generator erzeugten Folge genau dann, wenn für ein $k \leq poly(|N|)$ gilt:

$$\frac{\sum_{x \in QR_N} Pr\left(\mathbf{A}\left[N, b_1(x), \ldots, b_k(x)\right] = b_0(x)\right)}{\frac{\varphi(N)}{4}} \geq \frac{1}{2} + \epsilon,$$

wobei $b_i(x) =$ das unterste Bit von $\left(x^{2^i} \bmod N\right)$ ist.

Die Sicherheit des BBS Generators

Theorem 2.7. Der Blum-Blum-Shub Generator ist ein unvorhersagbarer (kryptographisch sicherer) Pseudozufallsgenerator. D.h., für jeden probabilistischen polynomialzeit Vorhersager $\mathbf{A}$, jede Konstante $0 < \delta < 1$ und $t \in \mathbb{N}$, hat $\mathbf{A}$ höchstens einen $\frac{1}{n^t}$-Vorteil für N beim Vorhersagen des vorhergehenden Bits der vom Blum-Blum-Shub Generator erzeugten Folge, für genügend große n und für alle bis auf einen δ Anteil der Zahlen N von der Länge n.

Theorem 2.8. Die vom Blum-Blum-Shub Generator erzeugten Folgen sind ununterscheidbar.