Prof. C. P. Schnorr Sommersemester 2007

Kryptographie

Blatt 11, 29.06.07, Abgabe 06.07.07

Aufgabe 1. Sei $N = \prod_{i=1}^{k} p_i^{e_i}$ mit paarweise verschiedenen Primzahlen p_i.
Zeige: Der LCG

$$x_{i+1} := ax_i + c \bmod N$$

hat Periode N genau dann, wenn gilt:

i) $a \equiv 1 \bmod p_i$ für alle i ;

ii) $(c, N) = 1$;

iii) wenn $4|N$, dann $a \equiv 1 \bmod 4$.

Insbesondere ist die Periode unabhängig vom Startwert.

Aufgabe 2. Sei $l(x) \in \mathbf{Z}[x]$ ein Polynom und F ein Pseudozufallsgenerator vom Typ $x + 1$.
Zeige: $F_{l(x)}$ (wie in der Vorlesung definiert) ist ein Pseudozufallsgenerator vom Typ $l(x)$.

Aufgabe 3. Seien $a, b, c, N \in \mathbf{Z}$.
Zeige: Die Iteration

$$x_{i+1} := ax_i + bx_{i-1} + c$$

mit x_{-1}, x_0 unabhängig und gleichverteilt auf $\mathbf{Z}_N$ ist nicht pseudozufällig.
Ist sie deshalb genauso schlecht wie der LCG ?

Aufgabe 4. Sei p prim und $< g >= \mathbb{Z}_p^*$.

i) Wir betrachten den folgenden Generator:

Eingabe: $x \in [1, p-1]$

Berechne $x_1 = g^x, x_2 = g^{x_1}, \cdots, x_n = g^{x_{n-1}}$.

Ausgabe: $(x_n, x_{n-1}, \cdots, x_1)$

Zeige: Dies ist kein PRG (bzw. man kann Bits vorhersagen).

ii) **Blum-Micali Generator**

Sei B: $\mathbb{Z}_p \to \{0,1\}$

$$B(x) = \begin{cases} 0 & \text{wenn } x < \frac{p-1}{2} \\ 1 & \text{wenn } x \geq \frac{p-1}{2} \end{cases}$$

Wir betrachten den folgenden Generator:

Eingabe: $0 < x < p-1$

Berechne $x_1 = g^x, x_2 = g^{x_1}, \cdots, x_n = g^{x_{n-1}}$

Ausgabe: $(B(x_n), B(x_{n-1}), \cdots, B(x_1))$

Zeige: Dieser Generator ist ein PRG unter der DL-Annahme, bzw. wenn man die Bits dieses Generators vorhersagen kann, kann damit das DL Problem lï¿½sen.