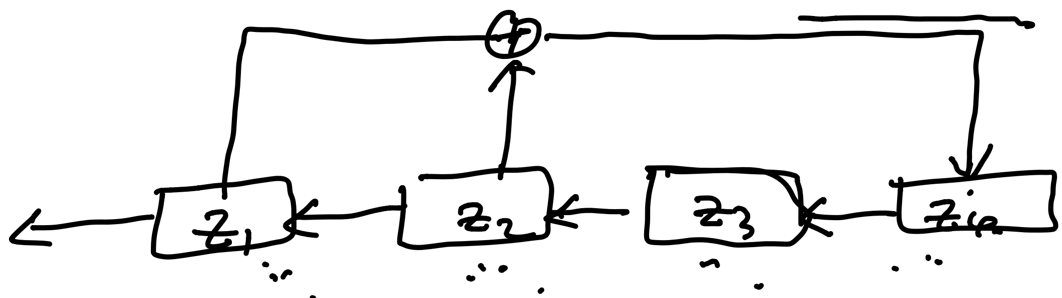
ECE 471/571 pseudorandom numbers (cont'd)

Linear Feedback Shift Register. LFSR

seed. length ~~m~~ = 4. $2^4 = 16.$

$2^4 - 1 = 15$



$z_5 = z_1 + z_2 \bmod 2$

$z_6 = z_2 + z_3 \bmod 2$

$z_{i+4} = (z_i + z_{i+1}) \bmod 2$

$z_1\ z_2\ z_3\ z_4\ z_5\ z_6$

seed: 1000 1 0 011 0 10111 | 100010

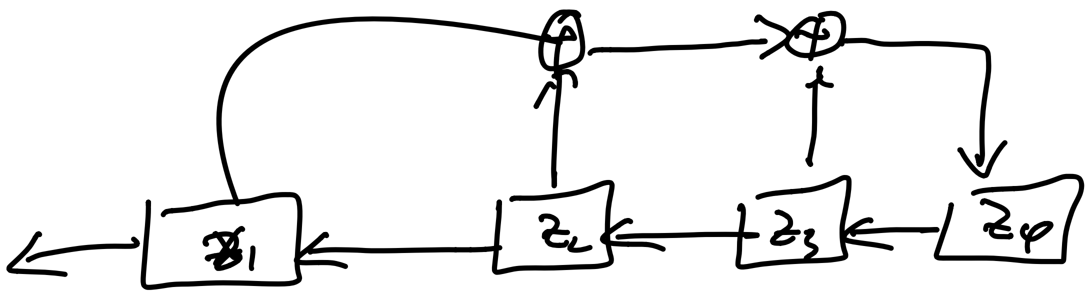
periodic 15 0000 X

in general $z_m = \sum_{j=0}^{m-1} c_j z_{j+1} \bmod 2.$

if attacker observes $\geq 2m$ known bits in the bit stream.

can solve for c_i (s)

· recover the seed.



$2^4 = 16$ $\quad$ $2^4 - 1 = 15$.

0000 → 000000000000000

0001

⋮

1111

LCG. Linear congruential generator

m	modulus.	$m > 0$
a	multiplier	$0 < a < m$
c	increment	$0 \le c < m$.
x_0	seed.	$0 \le x_0 < m$

$$x_{n+1} = (a \cdot \underline{x_n} + c) \bmod m$$

if $\underline{a = c = 1}$. $\quad x_{n+1} = \underline{x_n} + 1 \bmod m$

e.g $a=5$, $x_0=1$. $m=32$. $c=0$.

$\therefore$ $x_{n+1} = 5 \cdot x_n \bmod 32$.

1., 5, 25, 29, 17, 21, 9, 13,

1, 5. period $=8$

e.g $a=7$, $c=0$, $x_0=1$.

$x_{n+1} = 7 x_n \bmod 32$.

$\underbrace{1, 7, 17, 23}_{\text{period}=4}$, 1, 7.

1. full-period $m-1$.
2. appear random
3. 32-bit arithmetic

$\boxed{\text{max. representable nonnegative integer in computer}}$ $m = 2^{31}$ ..... $\underline{m = 2^{31}-1}$. $\to$ prime.

a must a generator of Z_m^* $= \{1, 2, \dots, m-1\}$

$a \cdot a$. $a^2 \bmod m$ ....

$a \cdot a \cdot a$. a^3 $i = \{1, 2, \dots, m-1\}$.

a^i

Example $\quad x_{n+1} = 7 x_n \mod 13.$

1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1.

period = 12. $\quad$ not random

security?

$$x_k = a\, x_{k-1} + c \mod m.$$

$$x_2 = a\, x_1 + c \mod m$$

$$x_3 = a\, x_2 + c \mod m.$$

Can solve a, c, m.

not secure.

BBS.

p. q. primes.

$p \times q = n$ modulus.

$p \equiv q \equiv 3 \mod 4.$

$$x_{i+1} = x_i^2 \mod n.$$

$\rightarrow$ LSB of x_{i+1}

Hard problem Quadratic Residuosity problem

QR. mod n

$$a = x^2 \bmod n. \qquad n = p \times q.$$

if factorization of n is unknown.

(hard).