

# Generation of Pseudo-Random Bits

## ***Abstract***

*This section presents two algorithms for pseudo-random bit generation: the Quadratic Residue Generator by Blum, Blum, Shub, and the Linear Feedback Shift Register Generator. The properties of the two algorithms are discussed, in particular their unpredictability and period. The application of pseudo-random bit sequences to data ciphering and data scrambling in transmission systems is outlined.*

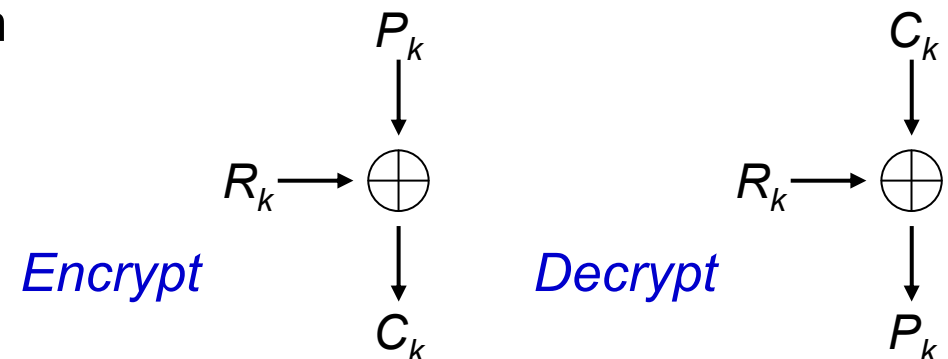
# Outline

---

- **One-time pad**
- Generation of a Pseudo-Random Bit Sequence (PRBS)
- Blum-Blum-Shub pseudo-random bit generator
- Linear Feedback Shift Register (LFSR) sequences
- Data scrambling in transmission systems

# One-Time Pad

- **Unbreakable** cryptosystem by G. Vernam and J. Mauborge (1918)
  - ◆  $C_i = P_i \oplus R_i$
  - ◆  $P_i = C_i \oplus R_i$
- The key  $\{R_i\}$ 
  - ◆ has the *same length of the message to encrypt*
  - ◆ must be *random*
  - ◆ is used one time only
- To be the cryptosystem really secure
  - ◆ the key has to be transferred in advance securely
  - ◆ the key must be really *random* (*unpredictable*)



# Outline

---

- One-time pad
- **Generation of a Pseudo-Random Bit Sequence (PRBS)**
- Blum-Blum-Shub pseudo-random bit generator
- Linear Feedback Shift Register (LFSR) sequences
- Data scrambling in transmission systems

# Generation of a Pseudo-Random Bit Sequence

- Real random data can be generated by natural chaotic phenomena
  - ◆ usually no correlations of any order (white sequence)
  - ◆ unpredictable
- Pseudo-random data
  - ◆ from  $\psi\epsilon\upsilon\delta\eta\varsigma = \text{false}$   $\rightarrow$  it *appears* as truly random
  - ◆ can be generated by simple algorithms with few parameters, to avoid transferring long data sequences
  - ◆ approximation of real random data
  - ◆ example: *linear congruential generator*
$$x_k \equiv ax_{k-1} + b \pmod{m} \quad x_0 = \text{seed}$$
$$b_k = \text{LSB}(x_k)$$
easy to predict, poor pseudo-randomness

# Unpredictable Pseudo-Random Bits

- For cryptographic applications, we need a source of pseudo-random bits that is **non-predictable** (or hard to predict)
- Methods based on a truly *one-way function*
  - ◆  $y = f(x)$  fast to compute (invertible or not)
  - ◆ given  $y$ , find any  $x$  for which  $f(x) = y$  must be computationally impossible
  - ◆ example:
$$x_k = f(s+k) \quad s = \text{seed}$$
$$b_k = \text{LSB}(x_k)$$
  - ◆ not all one-way functions are suitable
- Methods based on hard problems of Number Theory
  - ◆ example: *Quadratic Residue Generator* (Blum-Blum-Shub)

# Outline

---

- One-time pad
- Generation of a Pseudo-Random Bit Sequence (PRBS)
- **Blum-Blum-Shub pseudo-random bit generator**
- Linear Feedback Shift Register (LFSR) sequences
- Data scrambling in transmission systems

# Blum-Blum-Shub Pseudo-Random Bit Generator

- Lenore Blum, Manuel Blum, Michael Shub (1982-86)
- Two large primes  $p, q \equiv 3 \pmod{4}$
- Let  $n = pq$ , choose a seed  $x \perp n$
- $x_0 \equiv x^2 \pmod{n}$
- $x_j \equiv x_{j-1}^2 \pmod{n}$   
 $b_j = \text{LSB}(x_j)$
- The BBS Generator is not predictable backwards (square root problem, i.e. factorizing  $n$ ), probably not predictable onwards
- Slow





# Examples of BBS Sequences

$p = 31$        $p \bmod 4 = 3$   
 $q = 43$        $q \bmod 4 = 3$   
 $n = 1333$   
 $x = 50$        $\text{MCD}(x, n) = 1$

$j$	$x_j$	$b_j$
0	1167	1
1	896	0
2	350	0
3	1197	1
4	1167	1
5	896	0
6	350	0
7	1197	1
8	1167	1
9	896	0

$p = 23$        $p \bmod 4 = 3$   
 $q = 43$        $q \bmod 4 = 3$   
 $n = 989$   
 $x = 42$        $\text{MCD}(x, n) = 1$

$j$	$x_j$	$b_j$
0	775	1
1	302	0
2	216	0
3	173	1
4	259	1
5	818	0
6	560	0
7	87	1
8	646	0
9	947	1
10	775	1
11	302	0

# About the Period of a BBS Sequence

- The period  $P$  of the BBS Generator

- $P = \pi(x_0) \quad x_0 = x^2 \in \mathbb{Z}_n$
- $P$  divides  $\lambda[\lambda(n)]$ , that is at most  $P = \lambda[\lambda(n)]$

- $\lambda(n)$  is the Carmichael's Function

- $\lambda(n)$  divides  $\phi(n)$
- $\lambda(n)$  defined as the smallest positive integer  $m$  such that  $a^m \equiv 1 \pmod{n}$  for every  $a \perp n$
- $n \in \mathbb{N} \setminus \{0\} \quad n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdot \dots$

$$\lambda(n) = \text{lcm}\left(\left\{\lambda\left(p_i^{a_i}\right)\right\}\right)$$

$$\lambda(p^k) = \begin{cases} \frac{1}{2}\phi(p^k) & \text{se } p = 2, k \geq 3 \\ \phi(p^k) & \text{altrimenti} \end{cases}$$

- To maximize  $P$

- choose appropriately  $x_0$
- choose  $p = 2p_1 + 1, p_1 = 2p_2 + 1$ , with  $p, p_1, p_2$  primes  
 $q = 2q_1 + 1, q_1 = 2q_2 + 1$ , with  $q, q_1, q_2$  primes

# Examples of Period of a BBS Sequence (1a)

$p = 31$        $p \bmod 4 = 3$   
 $q = 43$        $q \bmod 4 = 3$   
 $n = 1333$   
 $x = 50$        $\text{MCD}(x, n) = 1$

$j$	$x_j$	$b_j$
0	1167	1
1	896	0
2	350	0
3	1197	1
4	1167	1
5	896	0
6	350	0
7	1197	1
8	1167	1
9	896	0

- $\lambda(n) = \text{mcm}(30, 42) = 210 = 2 \cdot 3 \cdot 5 \cdot 7$
- $\lambda[\lambda(n)] = \text{mcm}(2, 4, 6) = 12$
- $P = \{1, 2, 3, 4, 6, 12\}$

# Examples of Period of a BBS Sequence (1b)

$p = 31$        $p \bmod 4 = 3$   
 $q = 43$        $q \bmod 4 = 3$   
 $n = 1333$   
 $x = 6$        $\text{MCD}(x, n) = 1$

$j$	$x_j$	$b_j$
0	36	0
1	1296	0
2	36	0
3	1296	0
4	36	0
5	1296	0
6	36	0
7	1296	0
8	36	0
9	1296	0

- $\lambda(n) = \text{mcm}(30, 42) = 210 = 2 \cdot 3 \cdot 5 \cdot 7$
- $\lambda[\lambda(n)] = \text{mcm}(2, 4, 6) = 12$
- $P = \{1, 2, 3, 4, 6, 12\}$

# Examples of Period of a BBS Sequence (1c)

$p = 31$        $p \bmod 4 = 3$   
 $q = 43$        $q \bmod 4 = 3$   
 $n = 1333$   
 $x = 8$        $\text{MCD}(x, n) = 1$

$j$	$x_j$	$b_j$
0	64	0
1	97	1
2	78	0
3	752	0
4	312	0
5	35	1
6	1225	1
7	1000	0
8	250	0
9	1182	0
10	140	0
11	938	0
12	64	0
13	97	1

- $\lambda(n) = \text{mcm}(30, 42) = 210 = 2 \cdot 3 \cdot 5 \cdot 7$
- $\lambda[\lambda(n)] = \text{mcm}(2, 4, 6) = 12$
- $P = \{1, 2, 3, 4, 6, 12\}$

# Examples of Period of a BBS Sequence (2a)

$p = 23$        $p \bmod 4 = 3$   
 $q = 19$        $q \bmod 4 = 3$   
 $n = 437$   
 $x = 7$        $\text{MCD}(x, n) = 1$

$j$	$x_j$	$b_j$
0	49	1
1	216	0
2	334	0
3	121	1
4	220	0
5	330	0
6	87	1
7	140	0
8	372	0
9	292	0
10	49	1
11	216	0
12	334	0
13	121	1
14	220	0
15	330	0
16	87	1

- $\lambda(n) = \text{mcm}(18, 22) = 198 = 2 \cdot 3^2 \cdot 11$
- $\lambda[\lambda(n)] = \text{mcm}(1, 6, 10) = 30$
- $P = \{1, 2, 3, 5, 6, 10, 15, 30\}$

# Examples of Period of a BBS Sequence (2b)

$p = 23$   
 $q = 19$   
 $n = 437$   
 $x = 22$

$p \bmod 4 = 3$   
 $q \bmod 4 = 3$   
 $\text{MCD}(x, n) = 1$

$j$	$x_j$	$b_j$
0	47	1
1	24	0
2	139	1
3	93	1
4	346	0
5	415	1
6	47	1
7	24	0
8	139	1
9	93	1
10	346	0
11	415	1
12	47	1
13	24	0

- $\lambda(n) = \text{mcm}(18, 22) = 198 = 2 \cdot 3^2 \cdot 11$
- $\lambda[\lambda(n)] = \text{mcm}(1, 6, 10) = 30$
- $P = \{1, 2, 3, 5, 6, 10, 15, 30\}$

# Examples of Period of a BBS Sequence (2c)

$p = 23$        $p \bmod 4 = 3$   
 $q = 19$        $q \bmod 4 = 3$   
 $n = 437$   
 $x = 9$        $\text{MCD}(x, n) = 1$

- $\lambda(n) = \text{mcm}(18, 22) = 198 = 2 \cdot 3^2 \cdot 11$
- $\lambda[\lambda(n)] = \text{mcm}(1, 6, 10) = 30$
- $P = \{1, 2, 3, 5, 6, 10, 15, \mathbf{30}\}$

$j$	$x_j$	$b_j$
0	<b>81</b>	1
1	6	0
2	36	0
3	422	0
4	225	1
5	370	0
6	119	1
7	177	1
8	302	0
9	308	0
10	35	1
11	351	1
12	404	0
13	215	1
14	340	0
15	232	0
16	73	1
17	85	1
18	233	1
19	101	1
20	150	0
21	213	1
22	358	0
23	123	1
24	271	1
25	25	1
26	122	0



# Outline

---

- One-time pad
- Generation of a Pseudo-Random Bit Sequence (PRBS)
- Blum-Blum-Shub pseudo-random bit generator
- **Linear Feedback Shift Register (LFSR) sequences**
- Data scrambling in transmission systems

# Linear Feedback Shift Register Sequences

- A trade-off between speed and security is sought (e.g. cable TV)
- Linear recurrence relation (mod 2) of order  $M$

$$x_{n+M} = c_M x_n + c_{M-1} x_{n+1} + \cdots + c_1 x_{n+M-1}$$

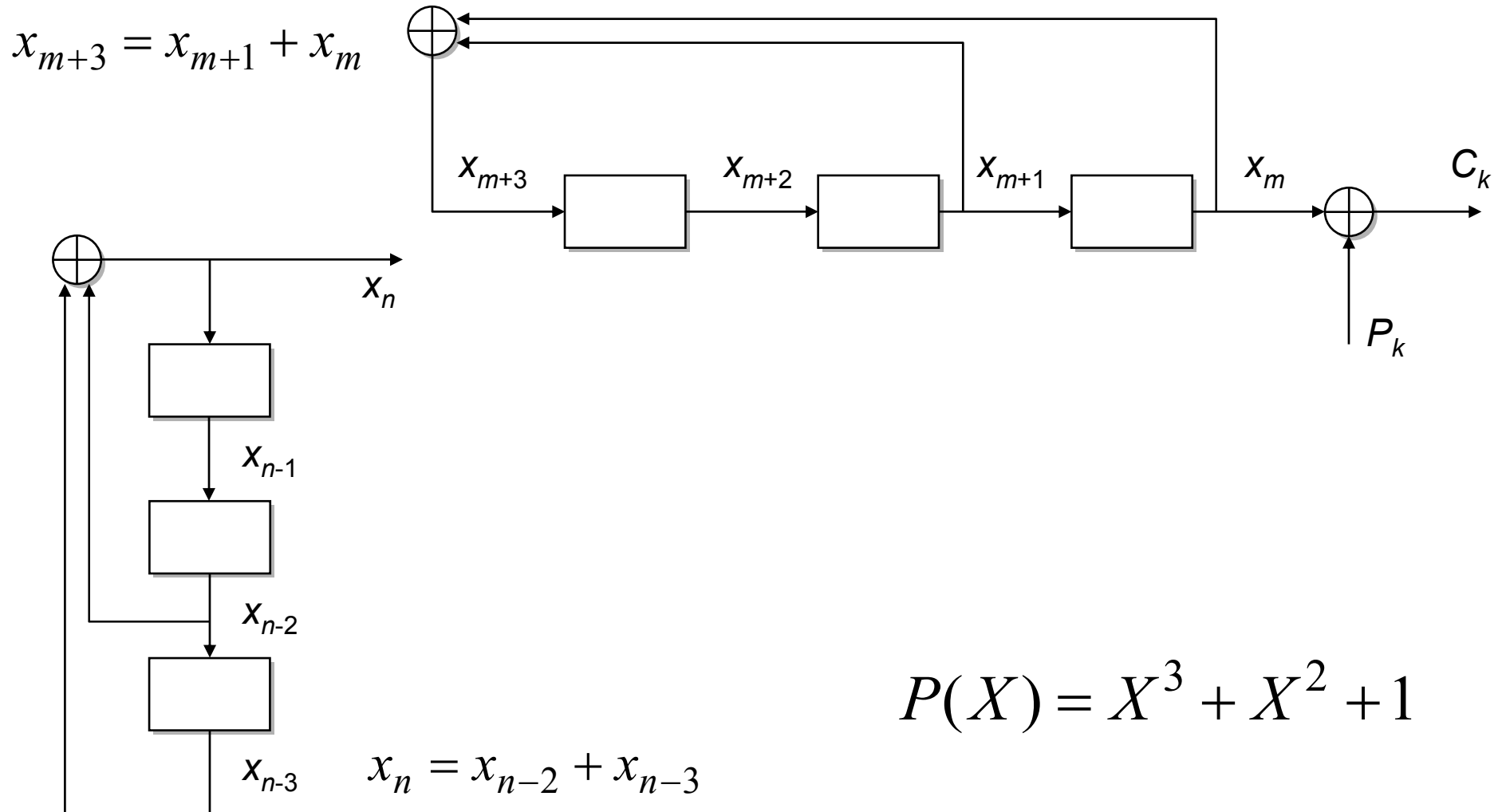
$$x_n = c_M x_{n-M} + c_{M-1} x_{n-M+1} + \cdots + c_1 x_{n-1}$$

- Defined by the polynomial of order  $M$  (coefficients mod 2)

$$P(X) = X^M + c_{M-1} X^{M-1} + \cdots + c_1 X + c_0$$

$$c_0 = 1, \quad c_M = 1$$

# Example: LFSR of Order $M=5$



# Properties of LFSR Order $M$

- Key length:  $M$  bit (initialization) +  $M$  bit (coefficients)
- Exposed to a *known plaintext attack*
  - ◆ from  $2M$  consecutive values,  $2M$  unknowns can be computed
- Period is at most  $2^M - 1$  ( $P \leq 2^M - 1$ )
- Period  $P \mid (2^M - 1)$  if
  - ◆  $P(X)$  irreducible mod 2
- Period  $P = 2^M - 1$  if
  - ◆  $P(X)$  irreducible mod 2
  - ◆  $2^M - 1$  is prime (Mersenne Prime)

(as demonstrated by Galois Fields Theory)

# Outline

---

- One-time pad
- Generation of a Pseudo-Random Bit Sequence (PRBS)
- Blum-Blum-Shub pseudo-random bit generator
- Linear Feedback Shift Register (LFSR) sequences
- **Data scrambling in transmission systems**

# Why Scrambling?

---

- The statistical properties of bit sequences transmitted by a digital multiplexer vary very much, depending on operation conditions
  - ◆ unequipped tributaries:  $P(0) = 1$
  - ◆ alarmed tributaries:  $P(0) = 0$
- Clock recovery circuits would work in very different conditions, should they do directly on these signals (e.g., NRZ coding in optical systems)

# What is Scrambling?

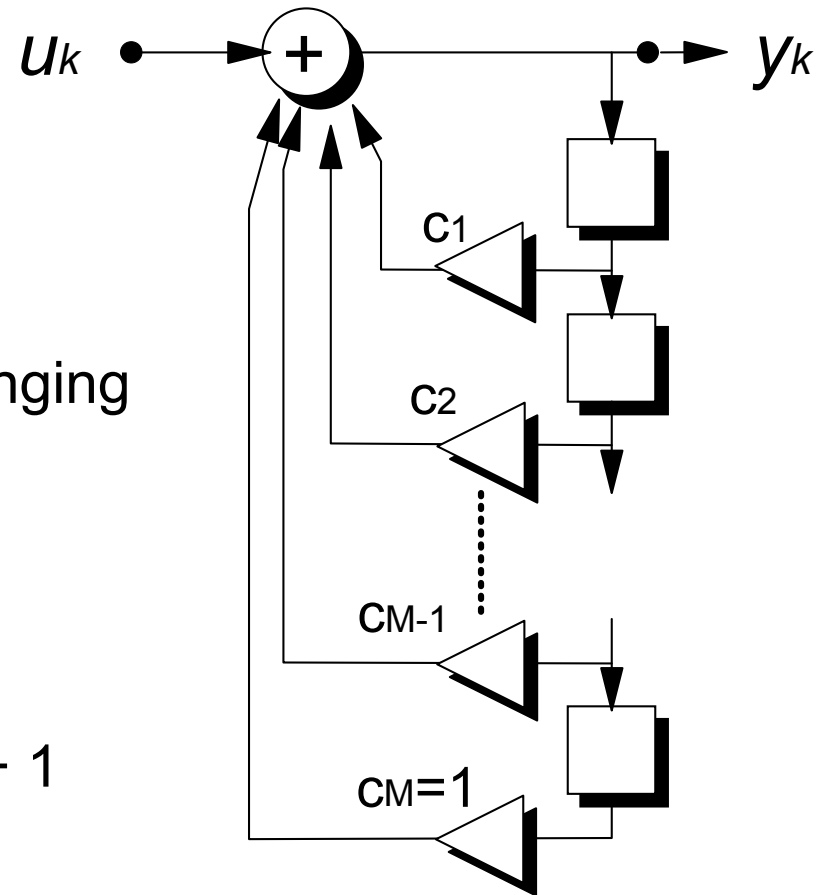
---

- Equalization of statistics, on moments of both 1° and 2° order
  - ◆ ensure the same probability of “1” and “0” in the transmitted signal (equalize the *average*)
  - ◆ diminish the probability of long sequences of consecutive identical digits (CID) “1111111111...” and “0000000000...” in the transmitted signal (whitening the *autocorrelation* and the *power spectral density*)
- Two types of scramblers
  - ◆ *basic self-synchronizing scrambler*
  - ◆ *additive scrambler*

# Basic Self-Synchronizing Scrambler

- Basic self-synchronizing scrambler of order  $M$ 
  - 1 adder mod 2 (XOR)
  - $M$  delay elements
  - $M$  binary multipliers  $c_m$  ( $c_M = 1$ )
- The *basic self-synchronizing descrambler* is obtained by exchanging the input with the output
- Defined by the *characteristic polynomial*

$$P(X) = x^M + c_{M-1}x^{M-1} + c_{M-2}x^{M-2} + \dots + c_1x + 1$$

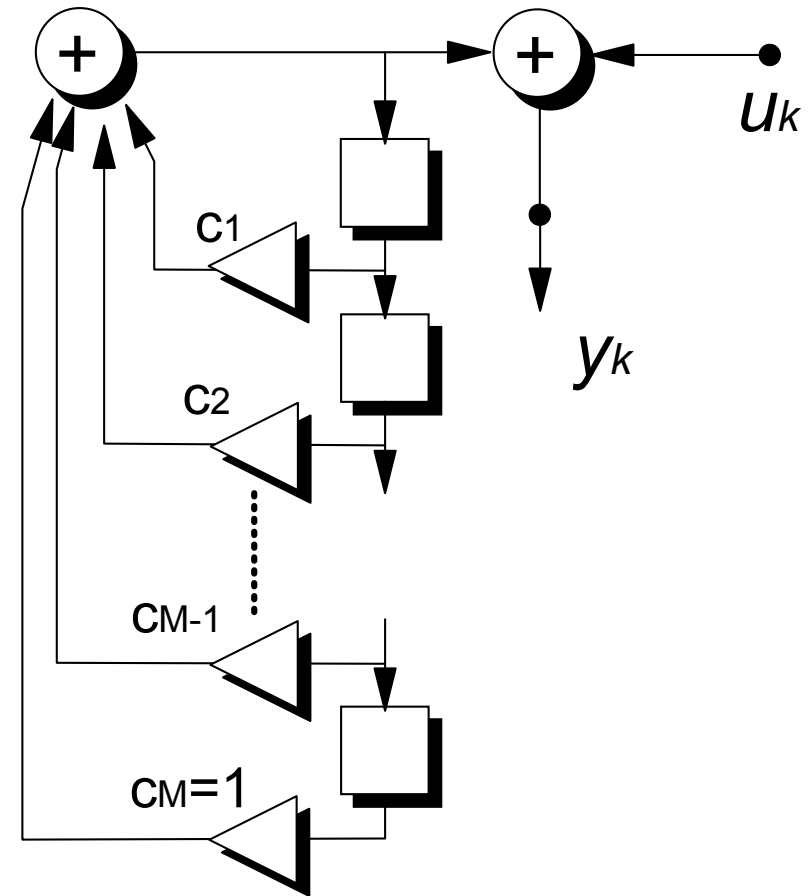




# Additive Scrambler

- Uses the basic self-synchronizing scrambler as *pseudo-random binary sequence (PRBS) generator*
- The *additive descrambler* is the same as the scrambler
  - adding twice the same binary sequence yields the original sequence
- This scrambler is *not* self-synchronizing!
- Defined by the *characteristic polynomial*

$$P(X) = x^M + c_{M-1}x^{M-1} + c_{M-2}x^{M-2} + \dots + c_1x + 1$$



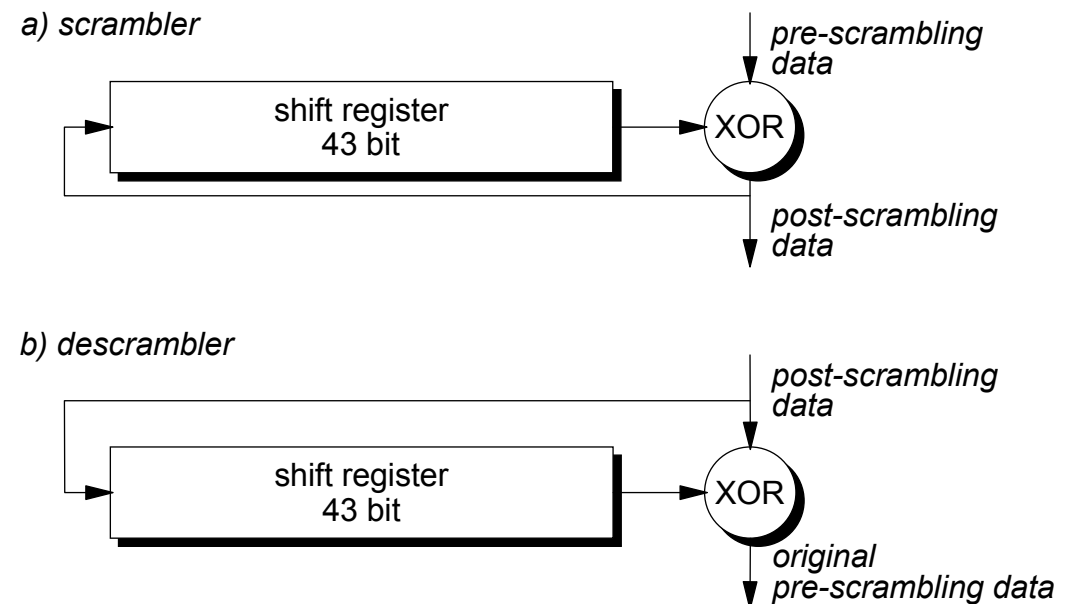
# Scrambling in SDH Transmission Systems

---

- To avoid transmission of long sequences of *consecutive identical digits* (CID)
  - ◆ NRZ coding is used in SDH optical systems
- In the RST block, after having added the RSOH, the STM-*N* output signal is scrambled (first row of RSOH excluded) before line coding
  - ◆ additive scrambler with characteristic polynomial  $x^7+x^6+1$
  - ◆ reset to the “1111111” status each STM-*N* frame on the first bit of the first byte after the first row of RSOH
  - ◆ the first row of RSOH is not scrambled to allow the descrambler to synchronize....
  - ◆ ...and therefore should not include long CID sequences in J0 and X bytes!

# Scrambling of PPP/HDLC frames in IP over SDH

- PPP/HDLC frames are scrambled before mapping into SDH VC
- Scrambling is needed to avoid that malicious users can transmit the SDH alignment word or long sequences of consecutive identical digits in the payload
  - ◆ the SDH scrambler has only 127 possible alignments
- Same scrambler as for ATM mapping in SDH
  - ◆ self-synchronizer scrambler  $x^{43}+1$
- During SDH overhead and fixed stuff, the scrambler is suspended, but its state is retained



# Example: Self-Synchronizing Scrambler $M=3$

$M = 3$

$c_0 = 1$

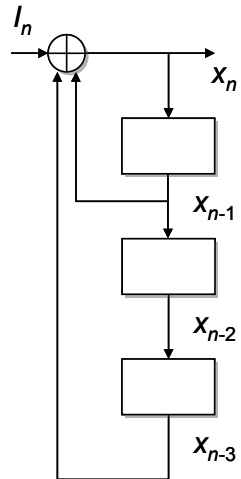
$c_1 = 1$

$c_2 = 0$

$c_3 = 1$

$k$	$I_k$	$D_{1k}$	$D_{2k}$	$D_{3k}$	$U_k$
0	1	0	0	0	1
1	1	1	0	0	0
2	1	0	1	0	1
3	1	1	0	1	1
4	1	1	1	0	0
5	1	0	1	1	0
6	1	0	0	1	0
7	1	0	0	0	1
8	1	1	0	0	0
9	1	0	1	0	1
10	1	1	0	1	1
11	1	1	1	0	0
12	1	0	1	1	0
13	1	0	0	1	0

$k$	$I_k$	$D_{1k}$	$D_{2k}$	$D_{3k}$	$U_k$	
0	1	1	0	0	0	NO
1	0	1	1	0	1	OK
2	1	0	1	1	0	NO
3	1	1	0	1	1	OK
4	0	1	1	0	1	OK
5	0	0	1	1	1	OK
6	0	0	0	1	1	OK
7	1	0	0	0	1	OK
8	0	1	0	0	1	OK
9	1	0	1	0	1	OK
10	1	1	0	1	1	OK
11	0	1	1	0	1	OK
12	0	0	1	1	1	OK
13	0	0	0	1	1	OK



- Is  $P(X)$  irreducible?
- What are possible periods of the PRBS?

# Example: Self-Synchronizing Scrambler $M=4$

**$M = 4$**

$c_0 = 1$

$c_1 = 1$

$c_2 = 1$

$c_3 = 0$

$c_4 = 1$

$k$	$I_k$	$D_{1k}$	$D_{2k}$	$D_{3k}$	$D_{4k}$	$U_k$
0	0	1	0	0	0	1
1	0	1	1	0	0	0
2	0	0	1	1	0	1
3	0	1	0	1	1	0
4	0	0	1	0	1	0
5	0	0	0	1	0	0
6	0	0	0	0	1	1
7	0	1	0	0	0	1
8	0	1	1	0	0	0
9	0	0	1	1	0	1
10	0	1	0	1	1	0
11	0	0	1	0	1	0
12	0	0	0	1	0	0
13	0	0	0	0	1	1
14	0	1	0	0	0	1
15	0	1	1	0	0	0

$k$	$I_k$	$D_{1k}$	$D_{2k}$	$D_{3k}$	$D_{4k}$	$U_k$	
0	1	1	1	1	1	0	OK
1	0	1	1	1	1	1	NO
2	1	0	1	1	1	1	NO
3	0	1	0	1	1	0	OK
4	0	0	1	0	1	0	OK
5	0	0	0	1	0	0	OK
6	1	0	0	0	1	0	OK
7	1	1	0	0	0	0	OK
8	0	1	1	0	0	0	OK
9	1	0	1	1	0	0	OK
10	0	1	0	1	1	0	OK
11	0	0	1	0	1	0	OK
12	0	0	0	1	0	0	OK
13	1	0	0	0	1	0	OK
14	1	1	0	0	0	0	OK
15	0	1	1	0	0	0	OK

- Is  $P(X)$  irreducible?
- What are possible periods of the PRBS?

# Example: Additive Scrambler $M=3$

$M = 3$

$c_0 = 1$

$c_1 = 0$

$c_2 = 1$

$c_3 = 1$

$k$	$I_k$	$D_{1k}$	$D_{2k}$	$D_{3k}$	$R_k$	$U_k$
0	1	1	1	1	0	1
1	1	0	1	1	0	1
2	1	0	0	1	1	0
3	1	1	0	0	0	1
4	1	0	1	0	1	0
5	1	1	0	1	1	0
6	1	1	1	0	1	0
7	1	1	1	1	0	1
8	1	0	1	1	0	1
9	1	0	0	1	1	0

$k$	$I_k$	$D_{1k}$	$D_{2k}$	$D_{3k}$	$R_k$	$U_k$
0	1	1	1	1	0	1
1	1	0	1	1	0	1
2	0	0	0	1	1	1
3	1	1	0	0	0	1
4	0	0	1	0	1	1
5	0	1	0	1	1	1
6	0	1	1	0	1	1
7	1	1	1	1	0	1
8	1	0	1	1	0	1
9	0	0	0	1	1	1

- Is  $P(X)$  irreducible?
- What are possible periods of the PRBS?

# Example: Additive Scrambler $M=4$

$M = 4$

$c_0 = 1$

$c_1 = 1$

$c_2 = 1$

$c_3 = 0$

$c_4 = 1$

$K$	$I_k$	$D_{1k}$	$D_{2k}$	$D_{3k}$	$D_{4k}$	$R_k$	$U_k$
0	0	1	1	0	0	0	0
1	0	0	1	1	0	1	1
2	0	1	0	1	1	0	0
3	0	0	1	0	1	0	0
4	0	0	0	1	0	0	0
5	0	0	0	0	1	1	1
6	0	1	0	0	0	1	1
7	0	1	1	0	0	0	0
8	0	0	1	1	0	1	1
9	0	1	0	1	1	0	0
10	0	0	1	0	1	0	0
11	0	0	0	1	0	0	0
12	0	0	0	0	1	1	1
13	0	1	0	0	0	1	1
14	0	1	1	0	0	0	0
15	0	0	1	1	0	1	1

$K$	$I_k$	$D_{1k}$	$D_{2k}$	$D_{3k}$	$D_{4k}$	$R_k$	$U_k$
0	0	1	0	0	0	1	1
1	1	1	1	0	0	0	1
2	0	0	1	1	0	1	1
3	0	1	0	1	1	0	0
4	0	0	1	0	1	0	0
5	1	0	0	1	0	0	1
6	1	0	0	0	1	1	0
7	0	1	0	0	0	1	1
8	1	1	1	0	0	0	1
9	0	0	1	1	0	1	1
10	0	1	0	1	1	0	0
11	0	0	1	0	1	0	0
12	1	0	0	1	0	0	1
13	1	0	0	0	1	1	0
14	0	1	0	0	0	1	1
15	1	1	1	0	0	0	1

- Is  $P(X)$  irreducible?
- What are possible periods of the PRBS?