

Cryptography CS 555

Lecture 4 Part B



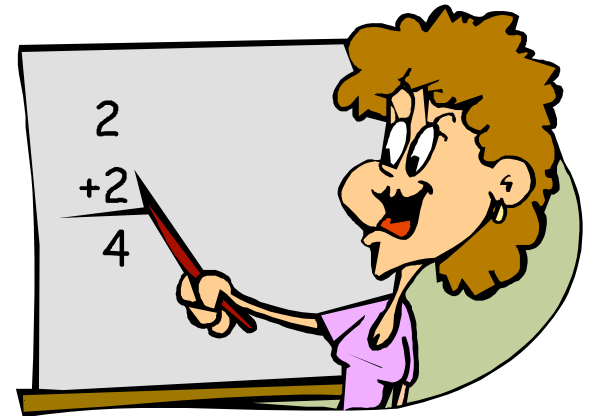
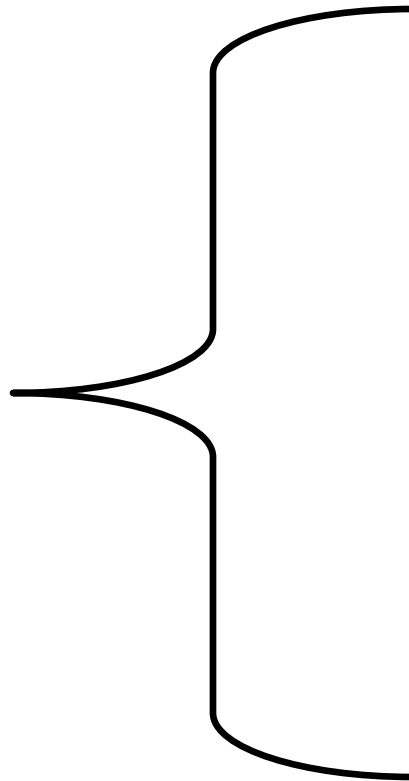
LFSR

Lecture Outline

- Ring and Field
- LFSR
- CSS (in)security



Begin Math



Ring

- **Definition:** $(R, +, \times)$ is called a ring if
 - $(R, +)$ is an abelian group with identity denoted 0,
 - (R, \times) is a monoid,
 - i.e., \times is associative, and
 - there is a multiplicative identity denoted 1, with $1 \neq 0$,
 - and \times is distributive over +,
 - $a \times (b + c) = (a \times b) + (a \times c)$ and $(b + c) \times a = (b \times a) + (c \times a)$
- **Definition:** A ring is commutative if $a \times b = b \times a$

Field

- **Definition:** $(R, +, \times)$ is called a field if
 - $(R, +, \times)$ is a commutative ring, and
 - $(R - \{0\}, \times)$ is a group
- **Example:** $(\mathbb{Z}_p, +, \times)$ is a field.

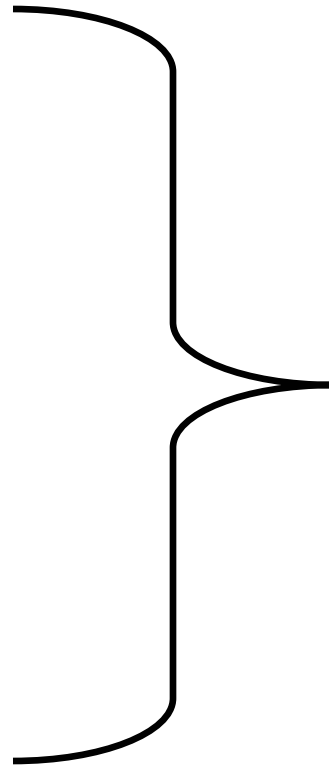
Polynomial Rings

- **Definition:** If R is a commutative ring, then a polynomial in x over the ring R is an expression of the form $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$
– where each $a_i \in R$ and $n \geq 0$
- **Definition:** If R is a commutative ring, the polynomial ring $R[x]$ is the ring formed by the set of all polynomials in x having coefficients from R .

Example of Polynomial Rings

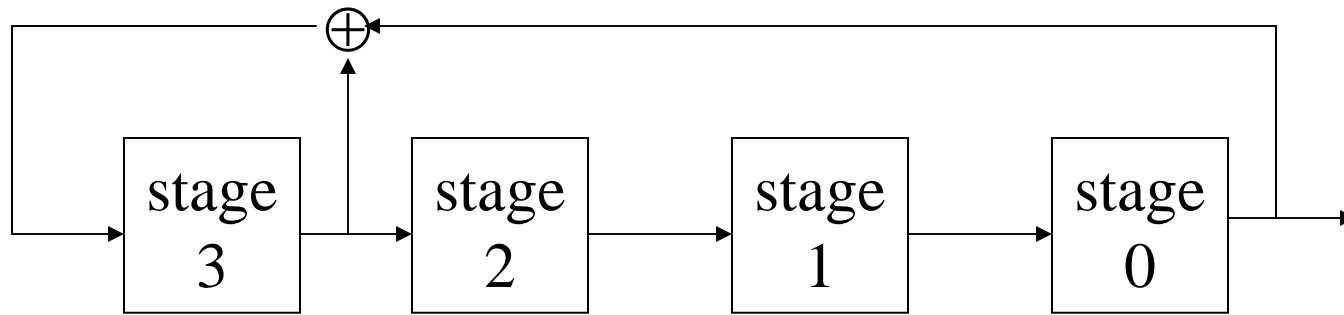
- **Example** : Let $f(x)=x^3+x+1$ and $g(x)=x^2+x$ be elements in $Z_2[x]$. Working in $Z_2[x]$
 - $f(x)+g(x)=x^3+x^2+1$
 - $f(x)\times g(x)=x^5+x^4+x^3+x$

End Math



Linear Feedback Shift Register (LFSR)

- Example:



- $$z_i = z_{i-4} + z_{i-1} \pmod{2}$$
$$= 1 \cdot z_{i-1} + 0 \cdot z_{i-2} + 0 \cdot z_{i-3} + 1 \cdot z_{i-4} \pmod{2}$$
- Connection polynomial
 - $C(D) = 1 + 1 \cdot D + 0 \cdot D^2 + 0 \cdot D^3 + 1 \cdot D^4$

Properties of LFSR

- **Fact:** given a L-stage LFSR with polynomial $C(D)$, every output sequence is periodic if and only if $C(D)$ has degree L
- **Fact:** given a L-stage LFSR with polynomial $C(D)$, if $C(D)$ is a primitive polynomial over $\mathbb{Z}_2[x]$,
 - i.e., $C(D)$ is irreducible, and
 - $C(D)$ divides x^k-1 for $k=2^L-1$ and for no smaller positive integer k ,then the LFSR is a maximum-length LFSR

Maximum-length LFSR

- **Definition:** For a L -stage maximum-length LFSR, any non-zero initial state produces an output sequence with period equal to $2^L - 1$, this is called a m-sequence.
- **Fact:** The distribution of patterns having fixed length is almost uniform in a m-sequence.

- Given a 4-stage LFSR, we know
 - $z_4 = z_3c_3 + z_2c_2 + z_1c_1 + z_0c_0 \pmod 2$
 - $z_5 = z_4c_3 + z_3c_2 + z_2c_1 + z_1c_0 \pmod 2$
 - $z_6 = z_5c_3 + z_4c_2 + z_3c_1 + z_2c_0 \pmod 2$
 - $z_7 = z_6c_3 + z_5c_2 + z_4c_1 + z_3c_0 \pmod 2$
- Knowing z_0, z_1, \dots, z_7 , one can compute c_0, c_1, c_2, c_4 .
- In general, knowing

Usage of LFSR

- Easy to implement in hardware
- Multiple LFSR's are often combined to achieve better security

Content Scrambling System (CSS)

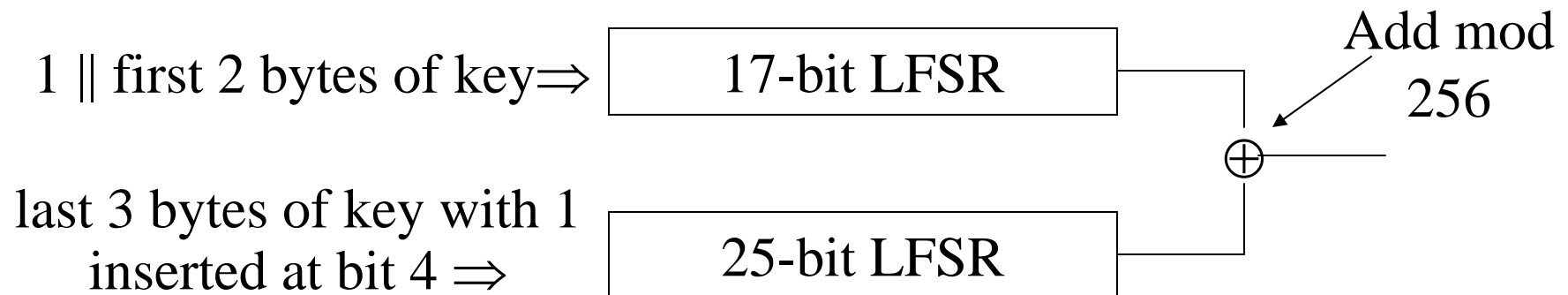
- Designed by Matsushita and Toshiba, and used for encrypting DVD videos
- There is a set of 409 player keys
- Each DVD player has one player key
- Each disk has a key data block
 - the disk key encrypted under the disk key (hash)
 - disk key encrypted with player key 1
 - ...
 - disk key encrypted with player key 409
- The disk key is used to encrypt title keys

Attacking CSS

- Knowing a disk key, by attacking the CSS cipher, one can recover all player keys
 - takes about 2^{25} time
 - breaks the revocation model of CSS
- It is possible to attack the hash to recover the disk key
 - takes about 2^{25} time

CSS Stream Cipher

- Key = 5 bytes = 40 bits
 - brute-force attack is possible
 - more efficient attacks exist



Given 6 output bytes, a trivial 2^{16} attack exists

A similar attack with 5 output bytes exists

The A5 Cipher in GSM

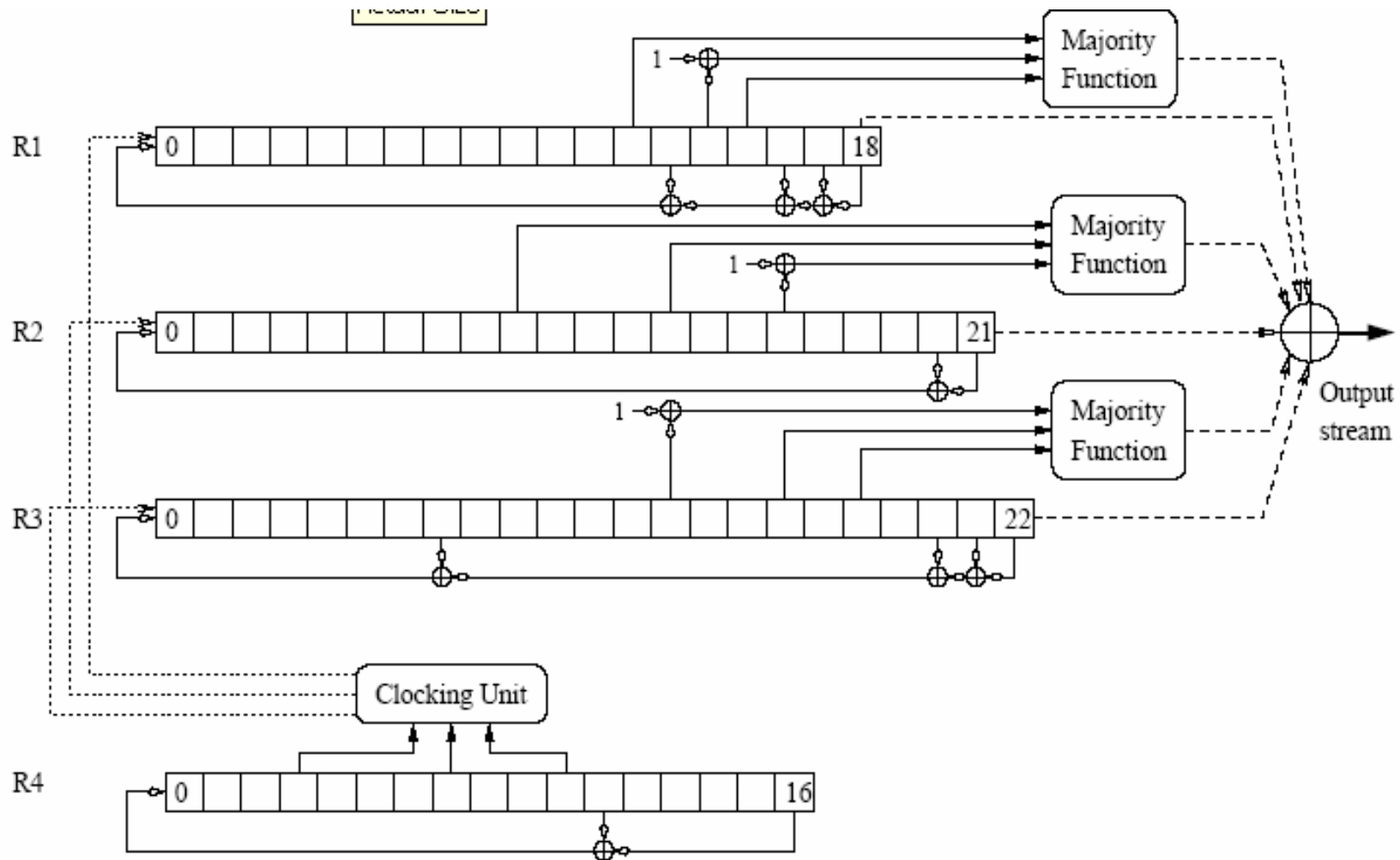


Fig. 1. The A5/2 internal structure