暨南大學
JINAN UNIVERSITY

Lecture 2 – Supplement

-Cryptographic Algorithms and Protocols

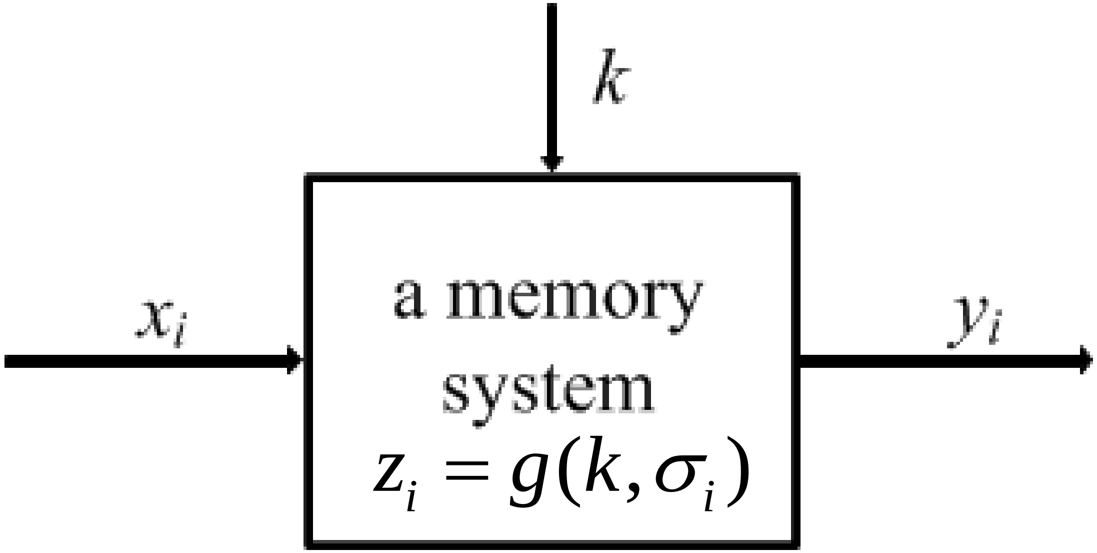
Huang, Xiujie (黄秀姐)

Office: Nanhai Building, #411

E-mail: t_xiujie@jnu.edu.cn

Dept. Computer Science

Stream Ciphers



$$y_i = E_{z_i}(x_i)$$

$$z_i = g(k, \sigma_i)$$

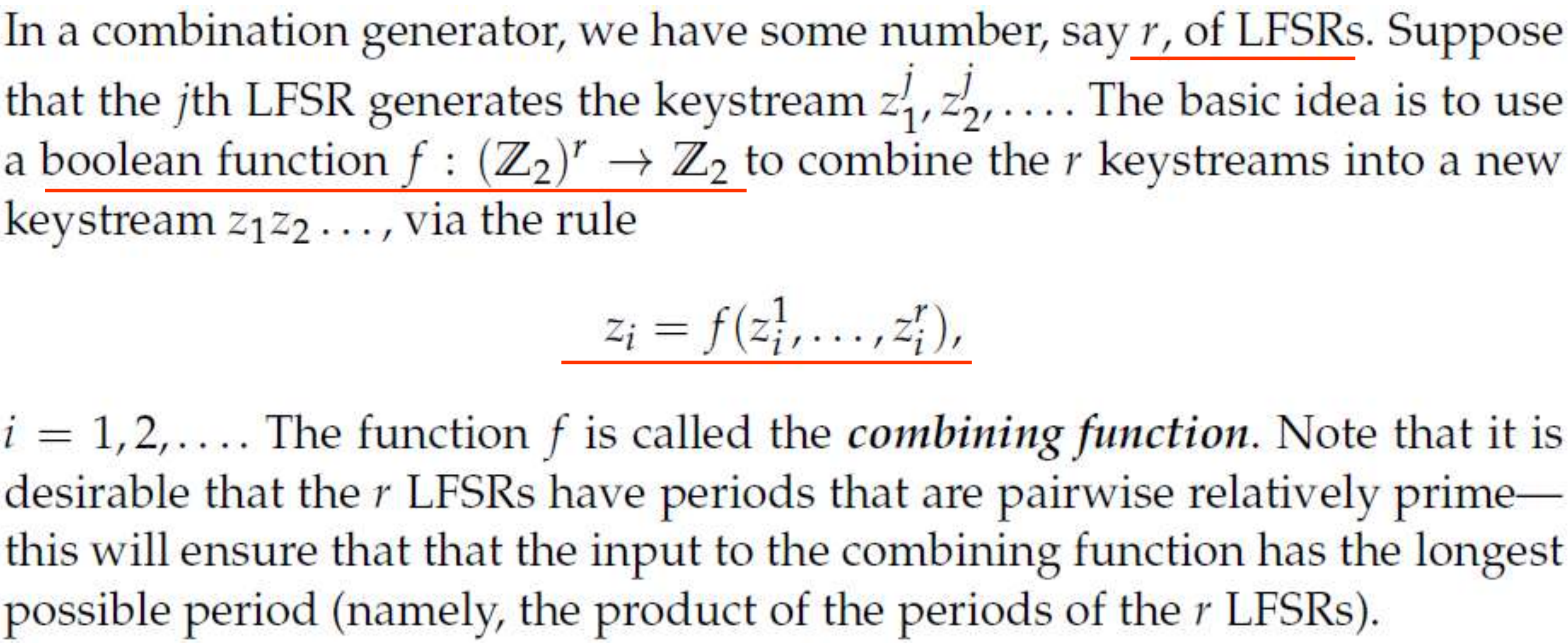
z_i is from a keystream generated by the function g

Practical Stream Ciphers

See Section 4.8 on Pages122-131

- the idea of LFSR is still used:
  - Efficiency (in software and hardware)
  - Large period
- Three of the most common methods of generating keystream
  - Combination generator
  - Filter generator
  - Shrinking generator
- Cryptanalysis:
  - Correlation attack on a combination generator
  - Algebraic attack on a filter generator

Combination generator



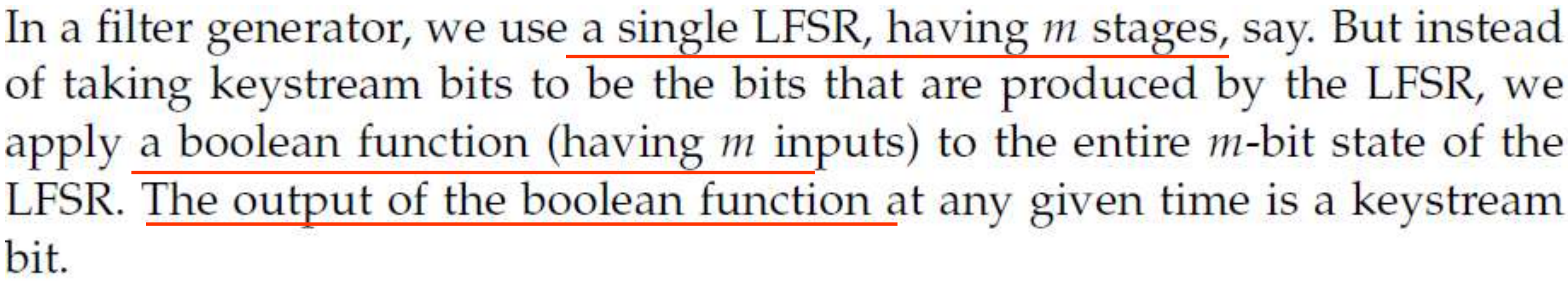
In a combination generator, we have some number, say r, of LFSRs. Suppose that the jth LFSR generates the keystream $z_1^j, z_2^j, \ldots$. The basic idea is to use a boolean function $f : (\mathbb{Z}_2)^r \rightarrow \mathbb{Z}_2$ to combine the r keystreams into a new keystream $z_1 z_2 \ldots$, via the rule

$$z_i = f(z_i^1, \ldots, z_i^r),$$

$i = 1, 2, \ldots$. The function f is called the ***combining function***. Note that it is desirable that the r LFSRs have periods that are pairwise relatively prime—this will ensure that that the input to the combining function has the longest possible period (namely, the product of the periods of the r LFSRs).

Correlation Attack on a Combination Generator

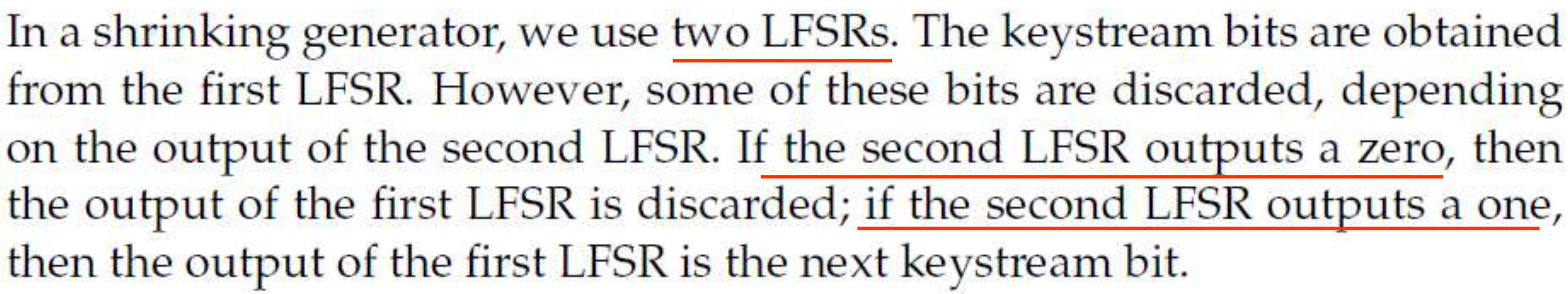
Filter generator



In a filter generator, we use a single LFSR, having m stages, say. But instead of taking keystream bits to be the bits that are produced by the LFSR, we apply a boolean function (having m inputs) to the entire m-bit state of the LFSR. The output of the boolean function at any given time is a keystream bit.

Algebraic Attack on a Filter Generator

Shrinking generator



In a shrinking generator, we use two LFSRs. The keystream bits are obtained from the first LFSR. However, some of these bits are discarded, depending on the output of the second LFSR. If the second LFSR outputs a zero, then the output of the first LFSR is discarded; if the second LFSR outputs a one, then the output of the first LFSR is the next keystream bit.

Applications of Stream Ciphers

Some already broken but still used stream ciphers：

- **1. CSS (Content Scramble System)(2 LFSRs): DVD encryption** 用于加密DVD的内容扰乱系统
- **2. A5 (3 LFSRs): GSM encryption**
- **3. E0 (4 LFSRs): Bluetooth encryption**
- **4. RC4:**
  - **designed by Ron Rivest in 1987, revealed anonymously in 1994**
  - **Used in HTTPS, WEP (IEEE 801.11), WAP, SQL Database**

Applications of Stream Ciphers

Some modern stream ciphers：

- 1. SEAL (8 LFSRs):
  - designed by Rogaway & Coppermfith in IBM in 1994
  - Suitable in software
- 2. Salsa20:
  - From eStream Project (2005-2008)
  - Suitable both in software and hardware
  - https://www.ecrypt.eu.org/stream/e2-salsa20.html
- 3. Trivium:
  - Designed by De Canniere and Preneel in 2005
  - From eStream Project (2005-2008)
  - https://www.ecrypt.eu.org/stream/e2-trivium.html

Applications of Stream Ciphers

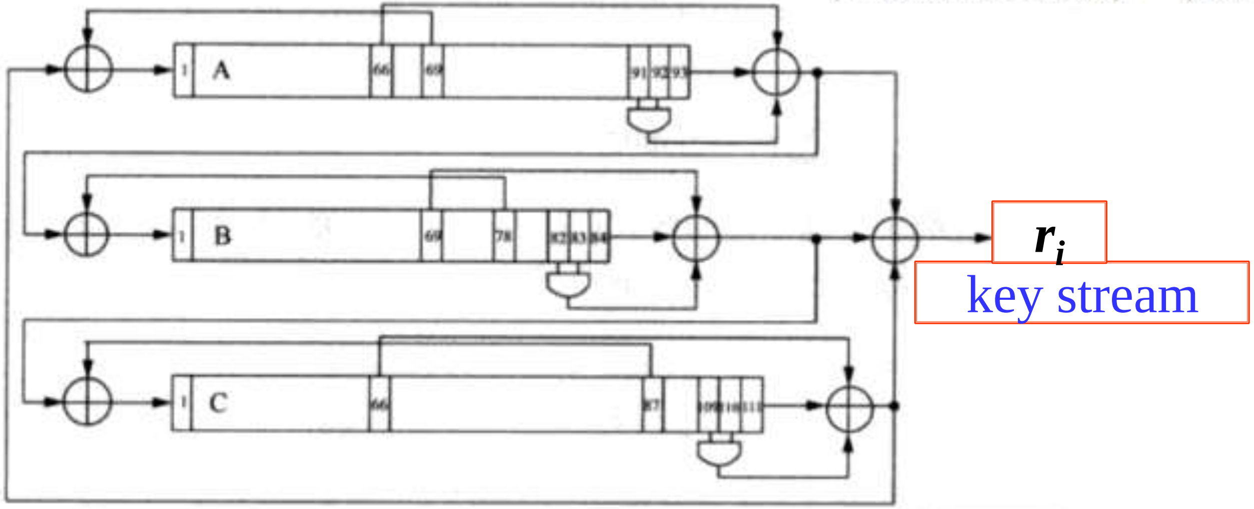
3. Trivium:

- Efficient and secure against known attacks
- Key size: 80 bits; IV size: 80 bits; Internal state: 288 bits (93+84+111)
- Three registers A , B, C

A $(s_1, s_2, \ldots, s_{93}) \leftarrow (K_1, \ldots, K_{80}, 0, \ldots, 0)$

B $(s_{94}, s_{95}, \ldots, s_{177}) \leftarrow (IV_1, \ldots, IV_{80}, 0, \ldots, 0)$

C $(s_{178}, s_{279}, \ldots, s_{288}) \leftarrow (0, \ldots, 0, 1, 1, 1)$



$$
\begin{aligned}
a_i &= c_{i-66} \oplus c_{i-111} \oplus (c_{i-110} \wedge c_{i-109}) \oplus a_{i-69} \\
b_i &= a_{i-66} \oplus a_{i-93} \oplus (a_{i-92} \wedge a_{i-91}) \oplus b_{i-78} \\
c_i &= b_{i-69} \oplus b_{i-84} \oplus (b_{i-83} \wedge b_{i-82}) \oplus c_{i-87}. \\
r_i &= c_{i-66} \oplus c_{i-111} \oplus a_{i-66} \oplus a_{i-93} \oplus b_{i-69} \oplus b_{i-84}.
\end{aligned}
$$

The Stream Cipher is an Interesting Topic!

- **Design keystream generator *g*:**
  - **Randomicity of the keystream: sequence design**
  - **Efficiency;**
  - **Large period (> 10^{16}bit);**
  - **……**
- **Cryptanalysis:**
  - **Evaluation criteria for security;**
  - **Attack methods;**
  - **……**

Some examples of research on stream ciphers:

1. P. Yadav, I. Gupta, S.K. Murthy, "Study and analysis of eSTREAM cipher Salsa and ChaCha", IEEE ICETECH 2016
2. Lin Ding, "Improved Related-Cipher Attack on Salsa20 Stream Cipher", IEEE ACCESS, 2019

Team Projects on Stream Cipher

Topics:

- 1. What is CSS? Cryptanalysis on CSS.
- 2. What is A5? Cryptanalysis on A5.
- 3. What is E0? Cryptanalysis on E0.
- 4. What is RC4? Cryptanalysis on RC4.
- 5. Other topics related to Stream Cipher.

Group work:

- each group has 2-3 persons, each group chooses one topic;
- Write a paper for your project; at least for 5 pages (A4);
- Please clearly claim personal contribution for your project;
- Due to 04/03/2024.