Stream Ciphers using TOA

Muhammad Sunaam
Abdul Basit
Hafiz Ahmad Raza Khan

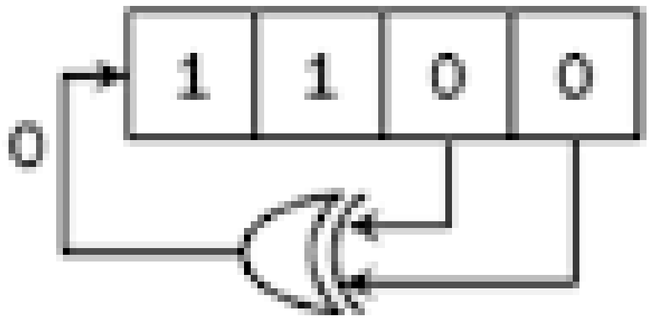
Stream Ciphers

- Symmetric encryption method.
- Generates a pseudorandom key stream to encrypt plaintext using XOR.

- Lightweight and efficient for real-time encryption.
- Suitable for hardware implementations

Linear Feedback Shift Register

- A shift register where the input bit is a linear function of its previous state.
- Feedback function is typically XOR of selected bits.
- Generates pseudorandom sequences
- Periodicity depends on the feedback function and register length.



Working of LFSRs

01 **Registers**
4-bit flip flops

02 **Feedback Function**
x^(4)+x^(3)+1

03 **Seed Value**
Initialized with a seed value (secret)

04 **Generated Sequence**
XORed with plaintext

Working of LFSRs

01 **Registers**
4-bit flip flops

02 **Feedback Function**
x^(4)+x^(3)+1

03 **Seed Value**
Initialized with a seed value (secret)

04 **Generated Sequence**
XORed with plaintext

Working of LFSRs

01

Registers

4-bit flip flops

02

Feedback Function

x^(4)+x^(3)+1

03

Seed Value

Initialized with a seed value (secret)

04

Generated Sequence

XORed with plaintext

Working of LFSRs

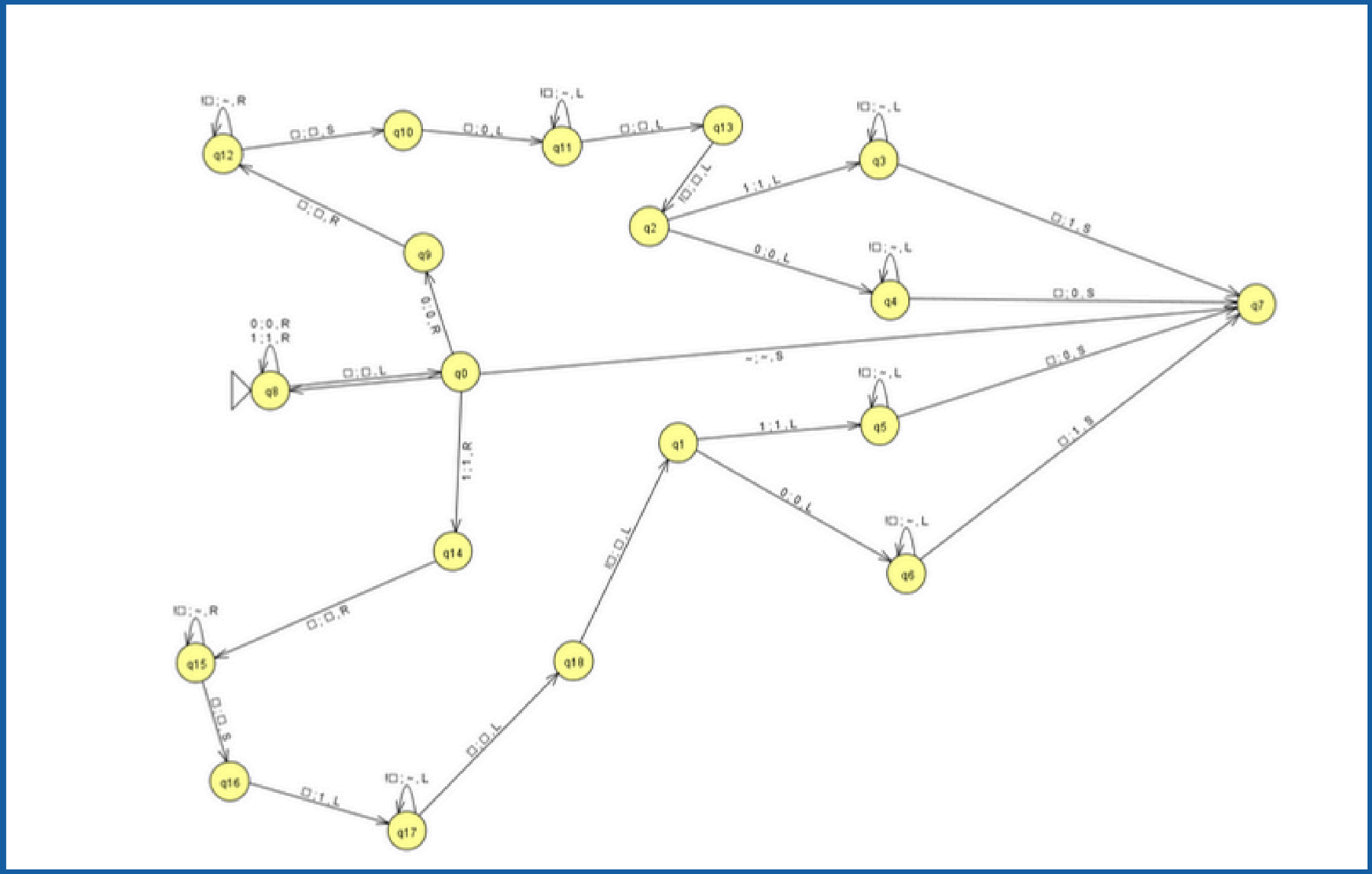
01 **Registers**
4-bit flip flops

02 **Feedback Function**
x^(4)+x^(3)+1

03 **Seed Value**
Initialized with a seed value (secret)

04 **Generated Sequence**
XORed with plaintext

Demonstration using JFLap



A5/1 Encryption

A5/1 is a stream cipher used to provide over-the-air communication privacy in the GSM cellular telephone standard.

Stream Cipher

Generates a pseudorandom key stream XOR-ed with plaintext to produce ciphertext.

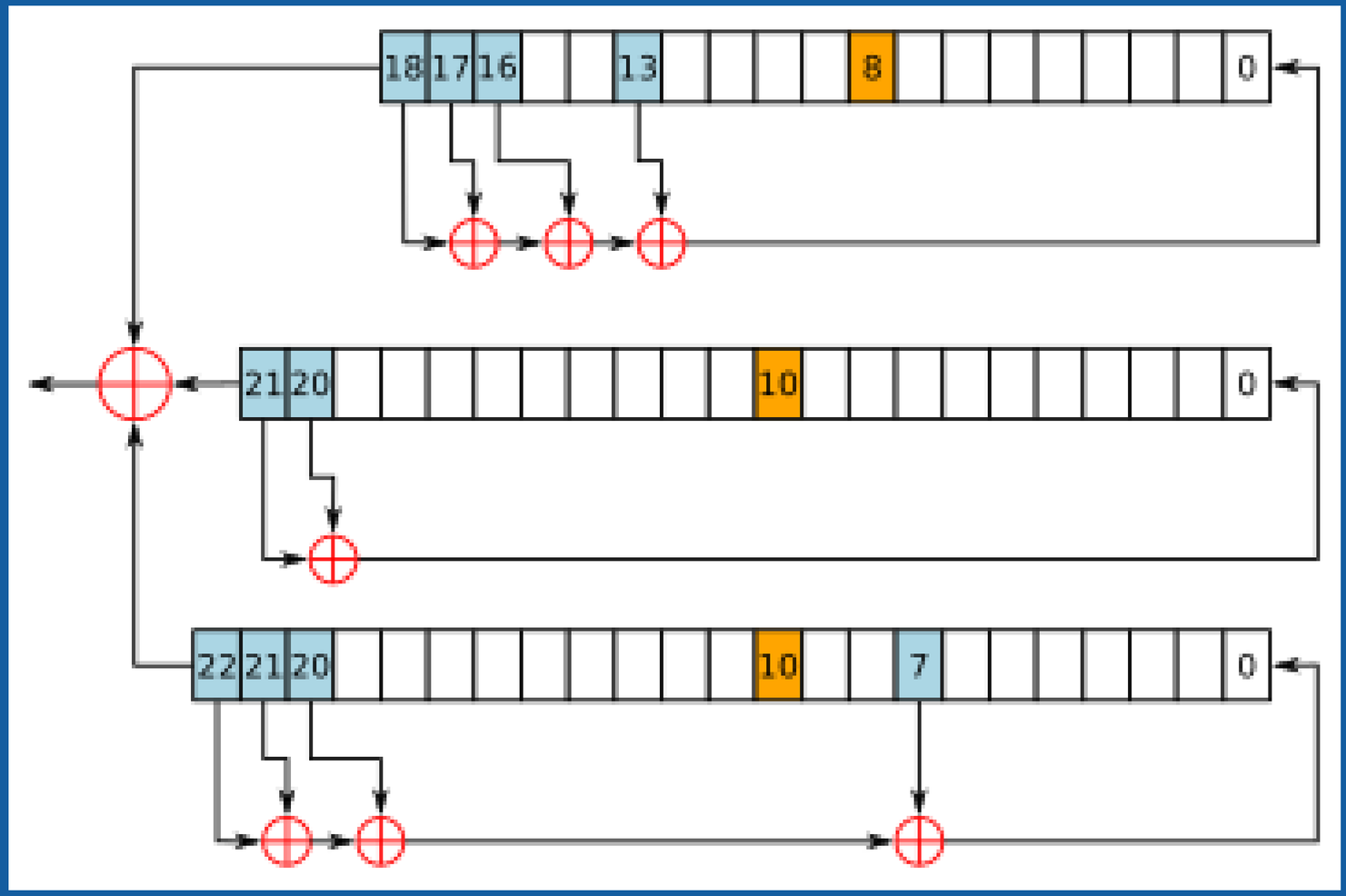
Three LFSRs

The core consists of three Linear Feedback Shift Registers (LFSRs) with distinct lengths and feedback polynomials.

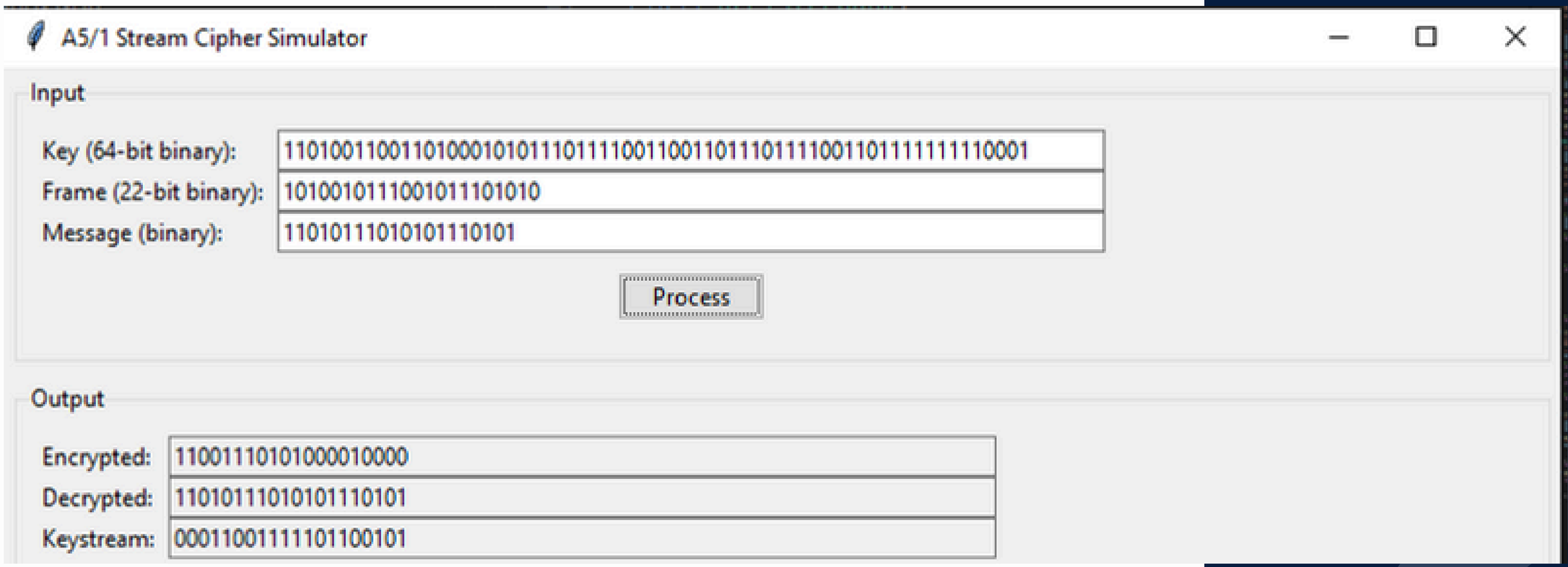
Clocking Mechanism

Uses a majority-rule clocking system to enhance security.

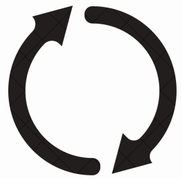
A5/1 Encryption



Implementation



Analysis



Periodicity

The sequence repeats after 4 steps for a 4-bit LFSR with certain feedback functions.

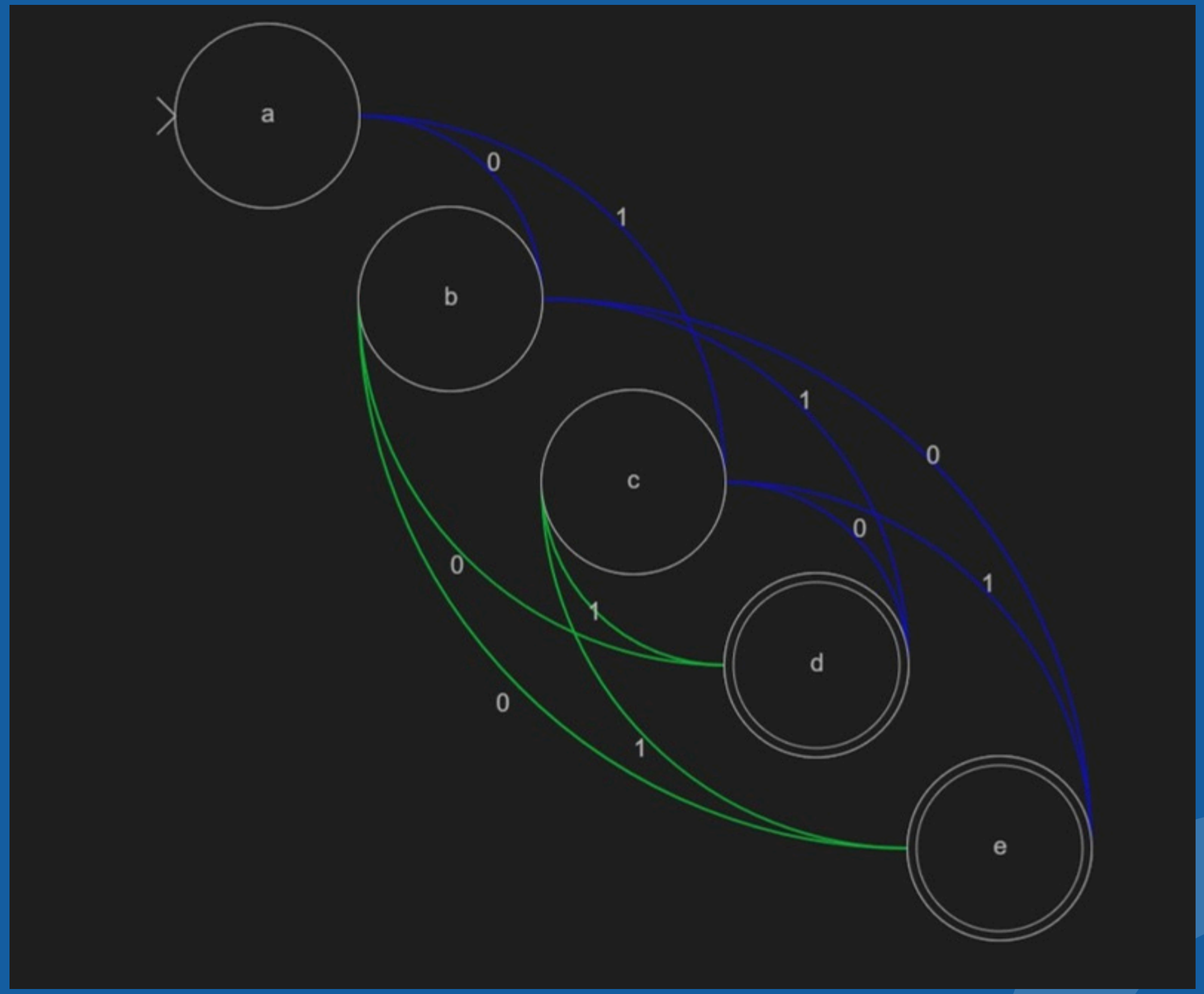
Randomness

Pseudo-randomness having (2^(n)-1) states.

Security

Can be improved with non-linear feedback or larger registers.

Finite State Transducer for XOR

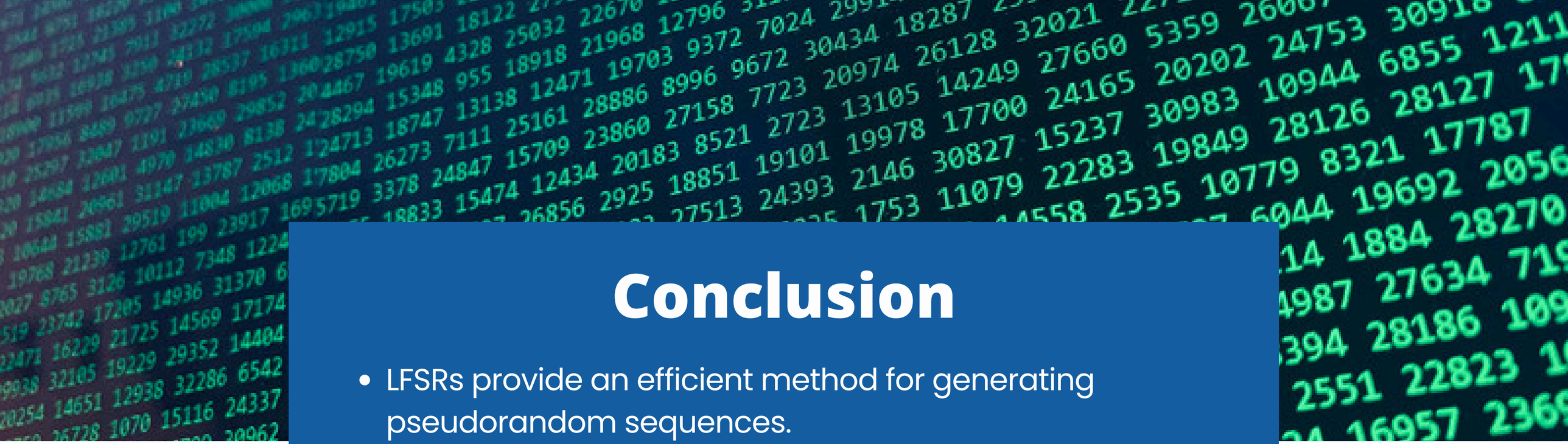


Advantages

- Simple and fast key stream generation.
- Easy to analyze and visualize using automata.

Limitations

- Predictable if feedback and seed are known.
- Not suitable for modern cryptographic standards.



Conclusion

- LFSRs provide an efficient method for generating pseudorandom sequences.
- Modeling LFSR as an automaton simplifies understanding.
- Encryption and decryption rely on XORing the plaintext and key stream.
- Can extend to non-linear feedback for improved security.

THANK YOU!