Security Evaluations on Lightweight Cryptographic Algorithms

Lightweight Stream ciphers and their cryptanalysis

Mohammad Ali Orumiehchiha

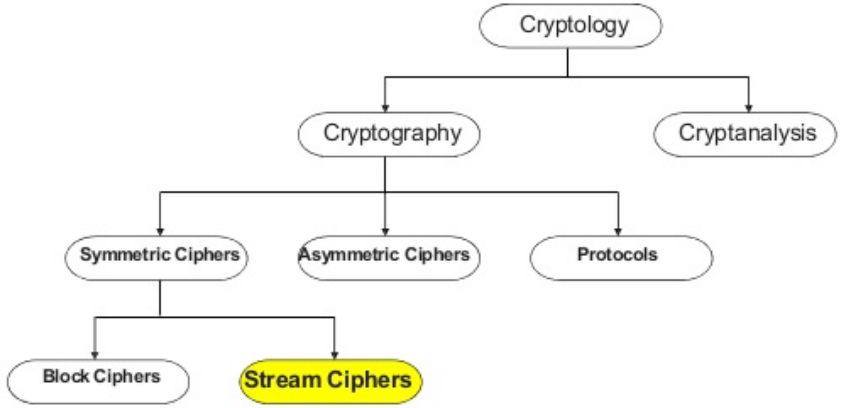
RCDAT

Orumiehchiha@rcdat.it

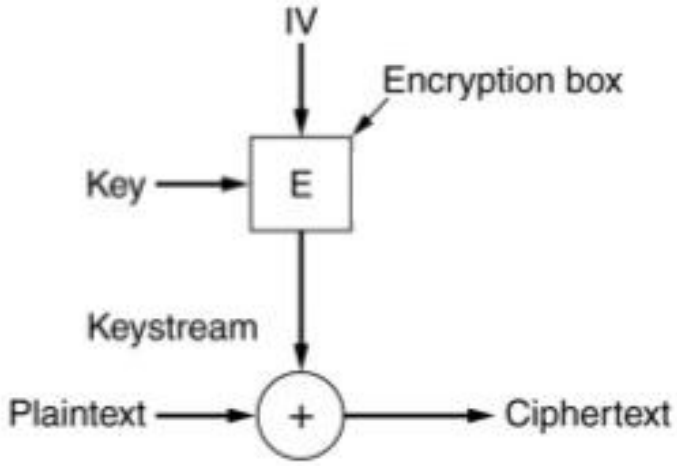
Outline

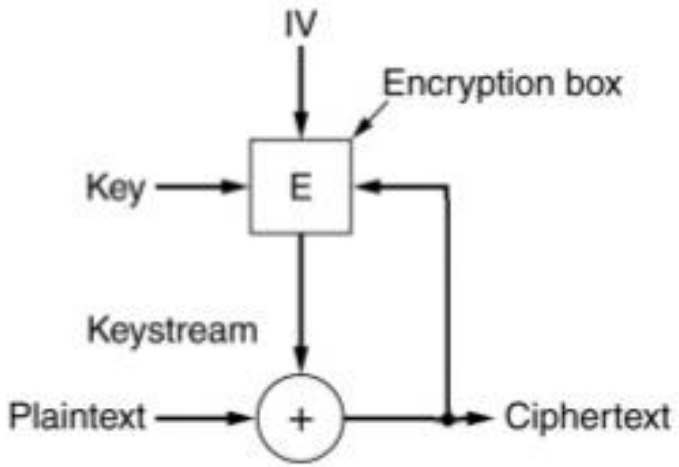
- Stream ciphers
- Lightweight Stream ciphers
- Some proposed ciphers
- The challenges
  - to design
  - to implement
- Some cryptanalysis points

Stream ciphers



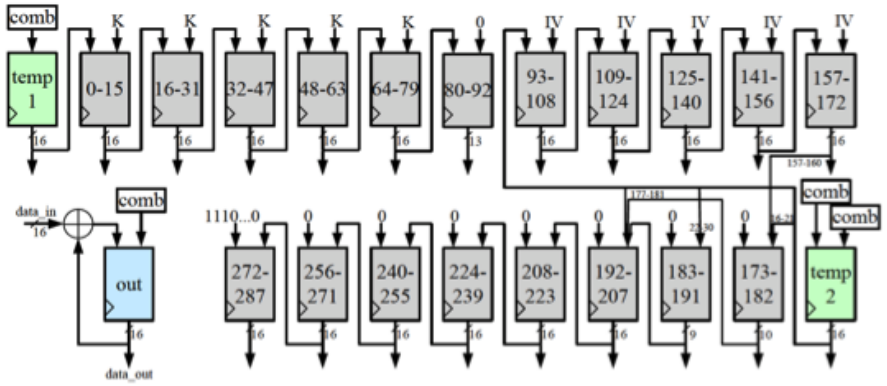
- Symmetric ciphers
  - Block Ciphers
  - Stream Ciphers (Synchronous, Asynchronous)
    - Some modes of operation transform a BC to SC

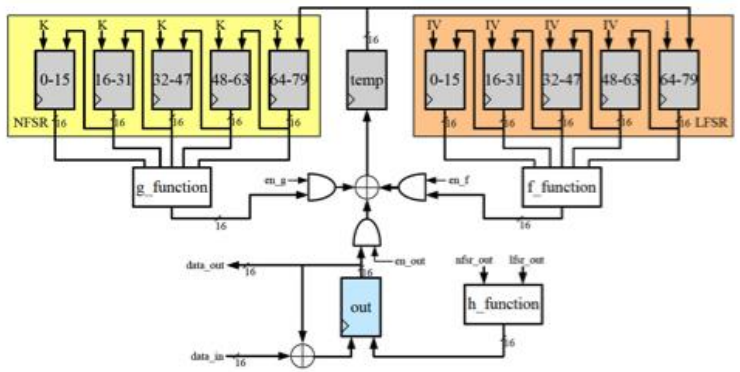




Applications

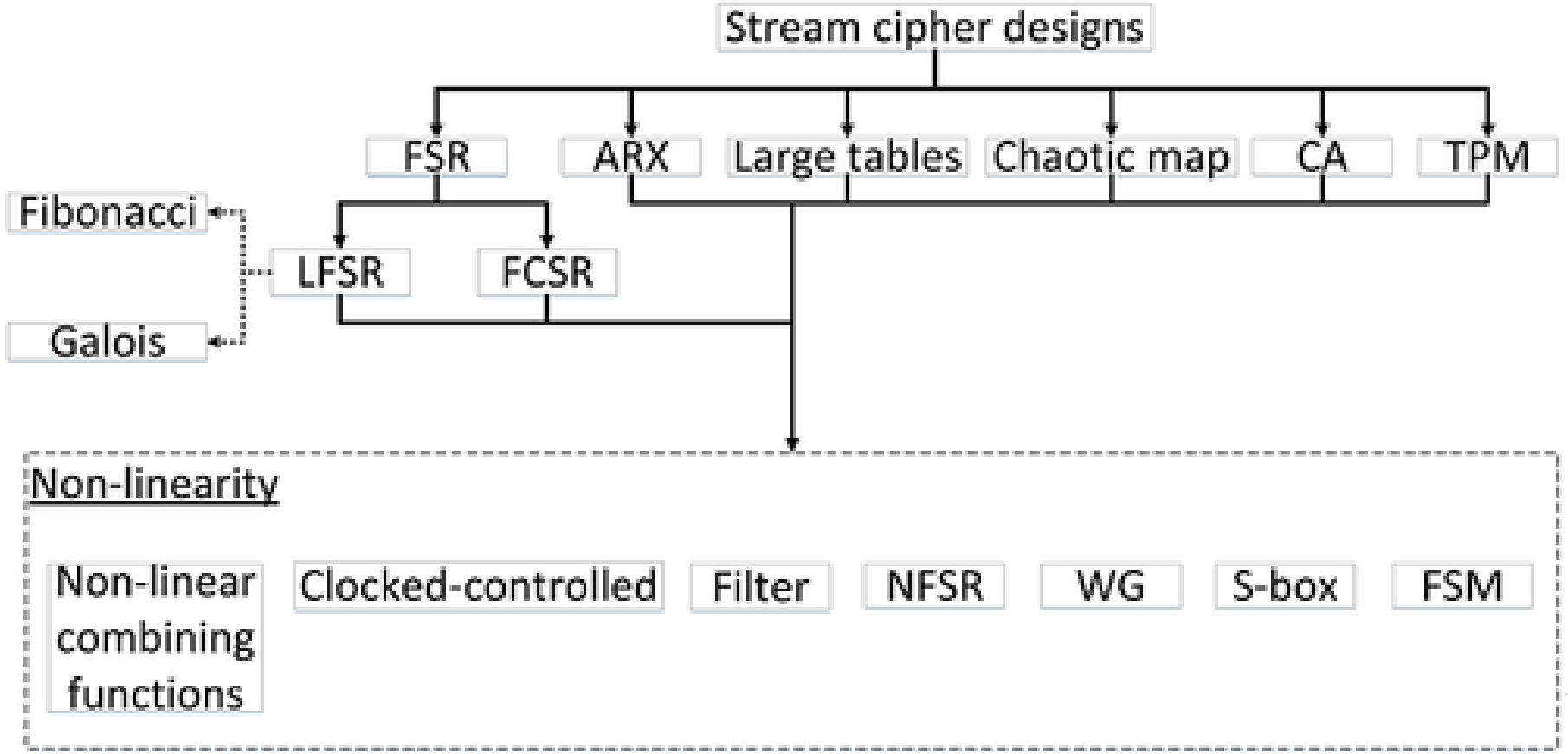
- Lightweight ciphers on RFID tags, Sensor Networks, IoT devices
- Generally
  - Encryption-Decryption are the same.
  - Faster, lighter, simpler than Block ciphers





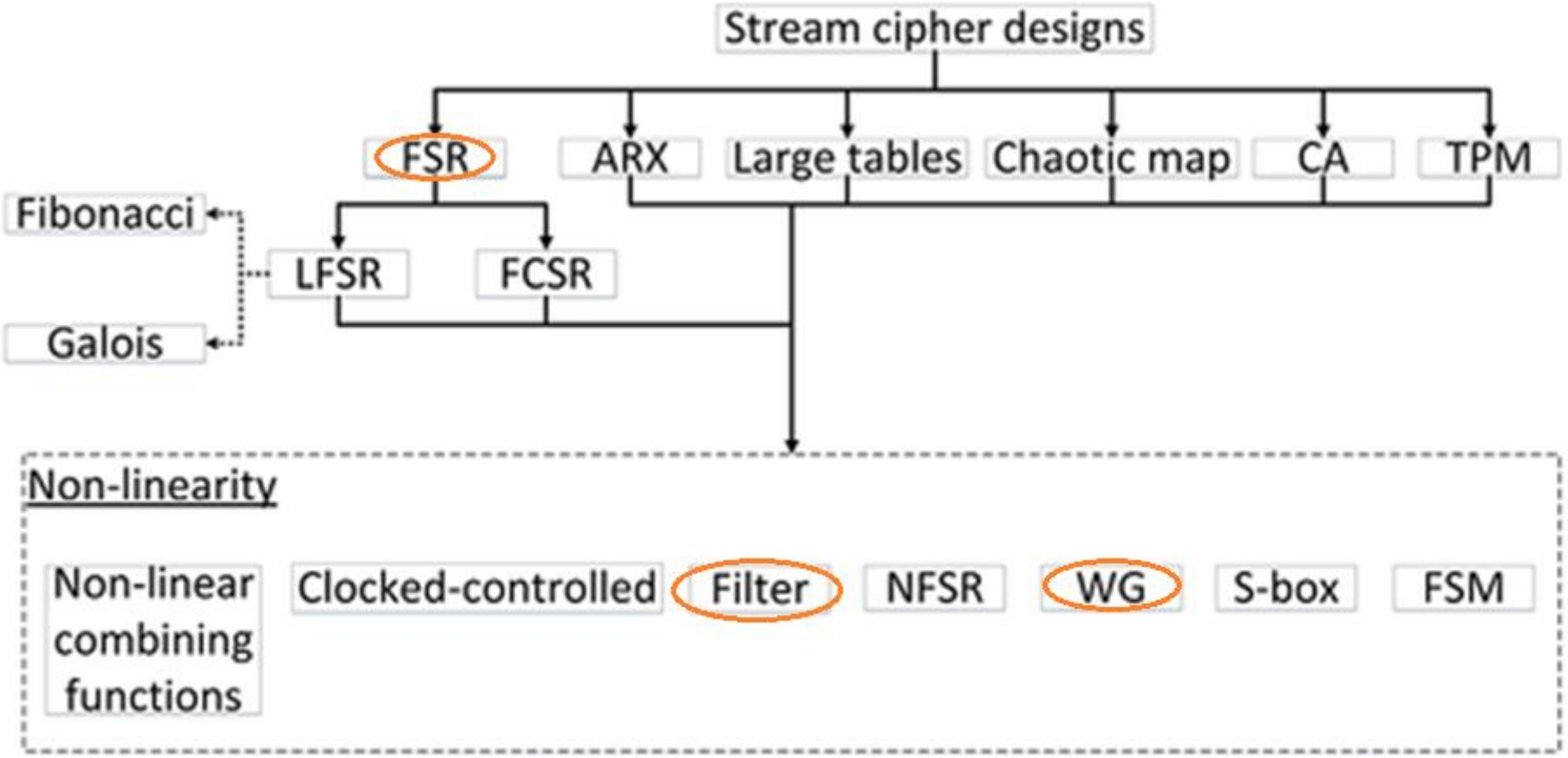
- A5/1,/2,/3, RC4, Grain, WG, …

The taxonomy



Refer to “A survey of lightweight stream ciphers for embedded systems”, Secur. Commun. Netw,2015

The taxonomy



Refer to “A survey of lightweight stream ciphers for embedded systems”, Secur. Commun. Netw,2015

Lightweight Cryptography: Critical Points

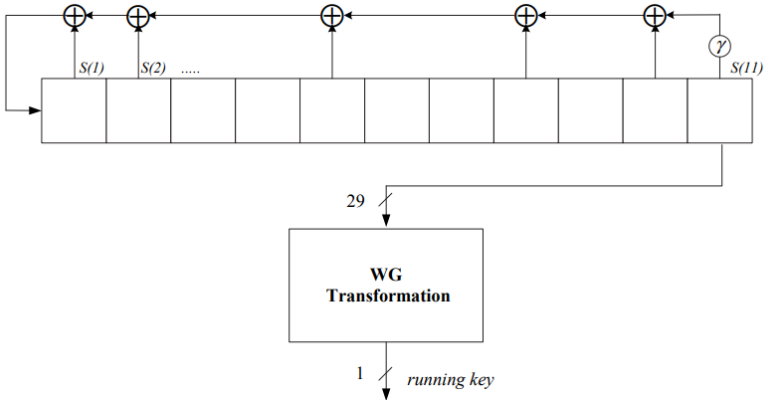
- Size:
  - Internal state (bits)
  - Key IV size (bits)
- Area (#GE)
- Power consumption
- Speed
  - Software/Hardware
- Security!
  - Mathematical Attacks
  - Implementation Attacks (countermeasures Cost)
    - Function and Protected Function (more than 2.5 times GE)

Trade off Between
Security and Lightweightness

A Case Study: WG Stream ciphers

- A Family of ciphers:
  - WG; proposed at eStream project.
  - WG-7 and WG-8; designed for encryption in resource restricted environments
  - WG-16; recommended for securing LTE applications.
  - And WG-t; uses computations in GF(2^t).

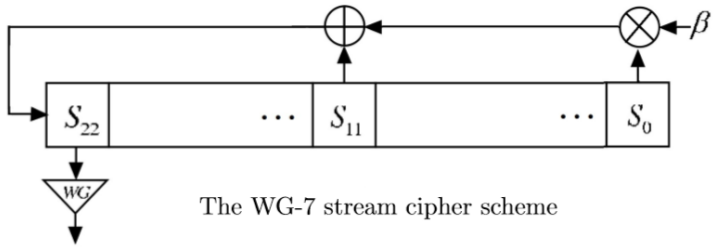
Cipher	Length of LFSR	Finite Field	The proposed application	Proposed bit-Security
$WG-7$	23	$GF(2^7)$	*RFID*	80
$WG-8$	20	$GF(2^8)$	*RFID*	128
$WG-16$	32	$GF(2^{16})$	*Communication, 5G*	128
$WG-29$	12	$GF(2^{29})$	*General Hardware*	80



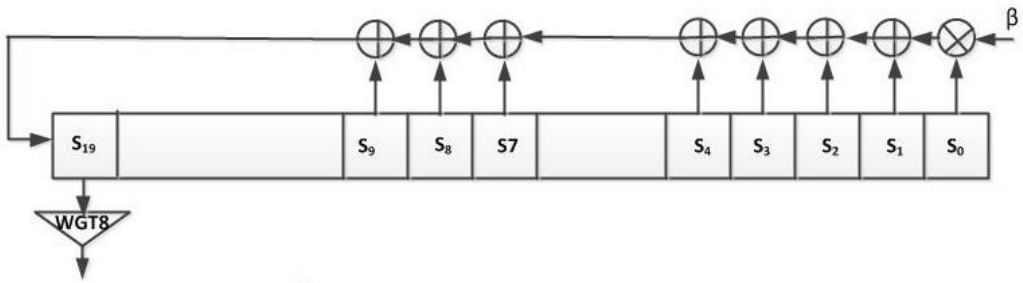
  - A filter structure
    - LFSR
    - WG transformation

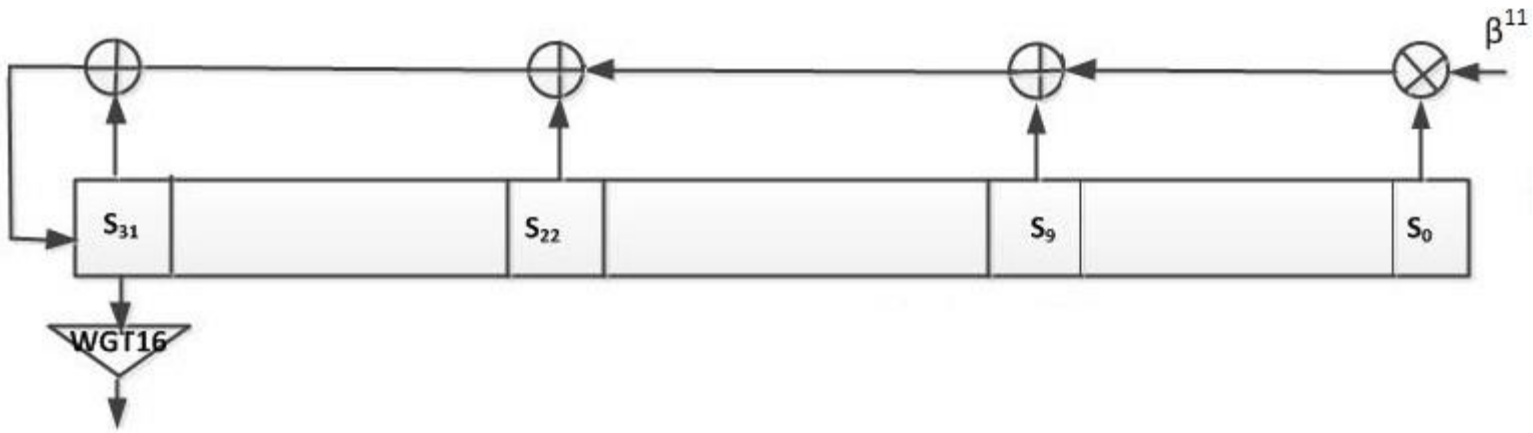
General properties

- Very simple and light cipher to be implemented
- Suitable cryptographic specifications
- Implementation points



The WG-7 stream cipher scheme





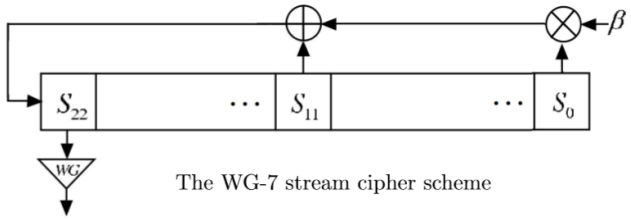
Cryptanalysis

- Distinguishing and key recovery attacks
  - Chosen IV attack on WG; Wu and Preneel (2006)
  - Algebraic attack on WG-7; Orumiehchiha, Pieprzyk, Steinfeld (2012)
  - Distinguishing on WG-8: Ding, Jin, Guan, Wang (2014)
  - Distinguishing attack; Joseph, Sekar, Balasubramanian (2016)
  - MILP-Based Cube Attack: Rohit, AlTawy, Guang Gong (2017)
  - Distinguishing on WG-8, -16: Rostami, Shakour, Orumiehchiha, Pieprzyk (2019)
- Implementation attack
  - Differential Fault Attack: Orumiehchiha, Rostami, Shakour, Pieprzyk (2020)

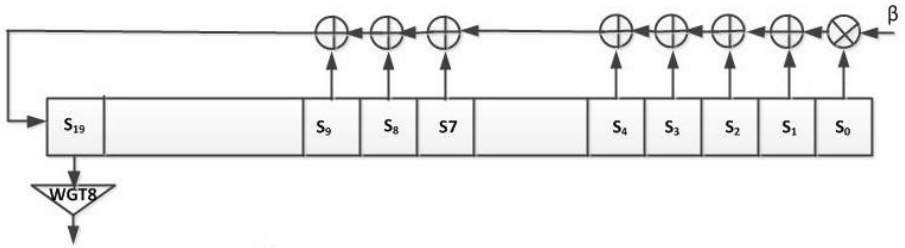
- Why they are still vulnerable!?

Why they are vulnerable!?

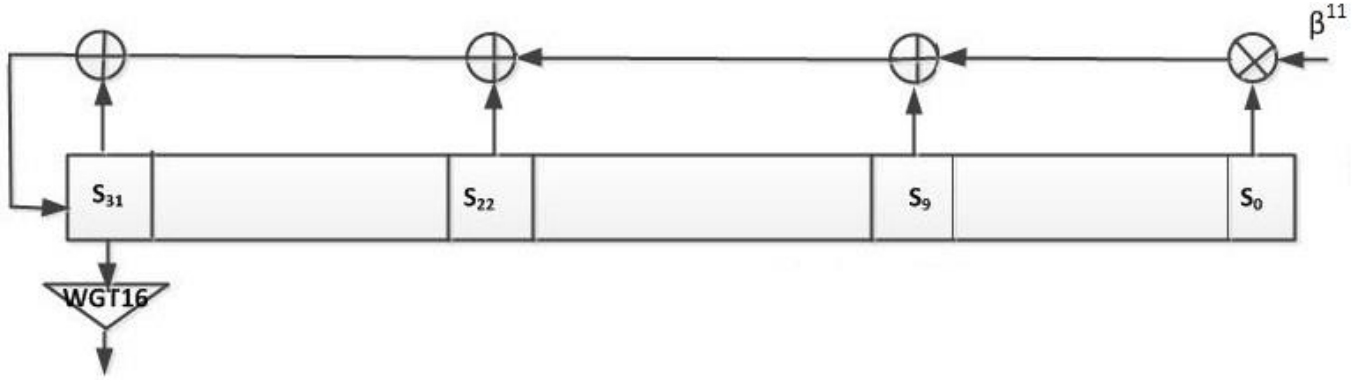
- The Filter Function
  - the algebraic properties
  - the number of input variables



The WG-7 stream cipher scheme



- The internal state
  - low diffusion-confusion of the state



The Challenges

- Understanding
  - the security limitations to design lightweight ciphers
  - the industry requirements for lightweight ciphers
- Need to
  - find new different security properties than what we know!
  - new recommendations to use lightweight cryptography.
  - provide crypto solutions in constrained environments.

Conclusions

- Had a look at
  - Stream ciphers as not-standard schemes to design lightweight ciphers
  - the Critical points to exploit ciphers in the constrained environments
  - a case study to see the limitations
  - Checking out the challenges

Thank you

If you are looking for a research position on cryptography, please send us your resume to **CRYPTO@RCDAT.IR**