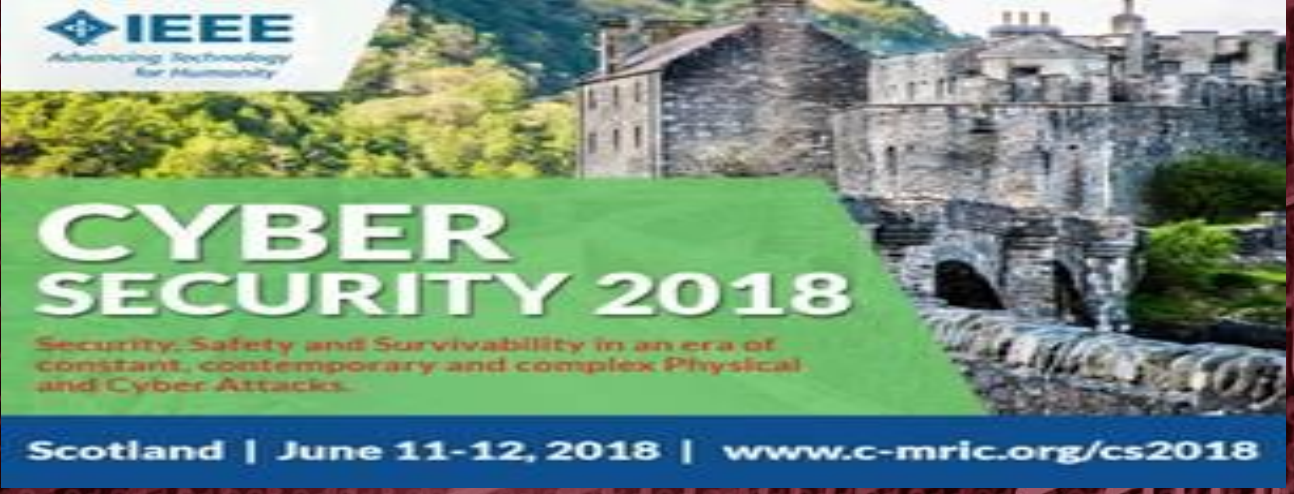


Combined and Robust SNOW-ZUC Algorithm Based on Chaotic System

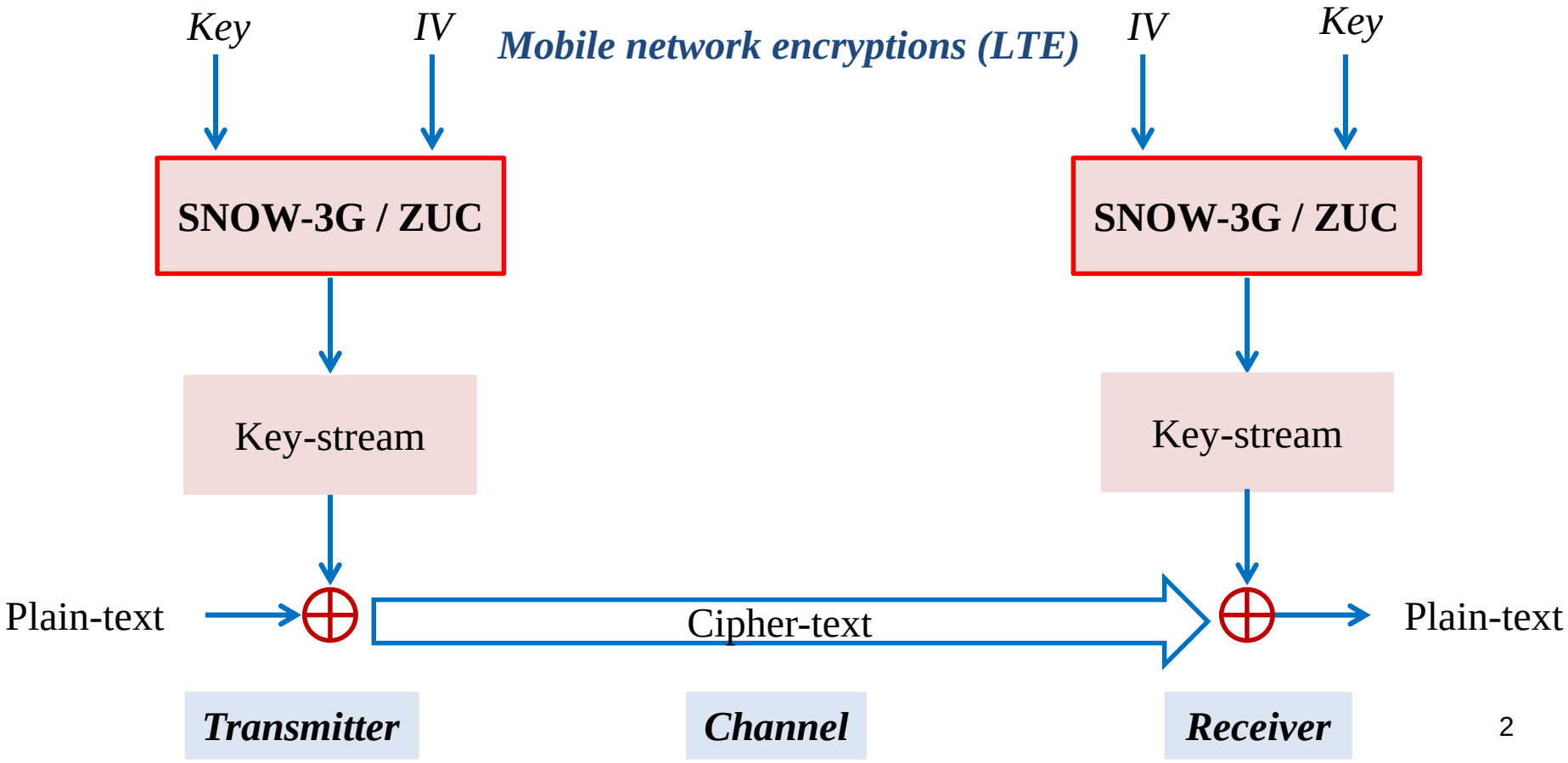
M. MADANI and C. TANOUGAST

UNIVERSITÉ DE LORRAINE

lcoms

Context

- The mobile networks are the most widely used networks in the world (GSM, UMTS, LTE).
- Sensitive information must be transmitted ➔ Security is required.
- The security is ensured by a cryptographic algorithms (stream ciphers or bloc ciphers).
- LTE security is based on SNOW-3G and ZUC algorithms.

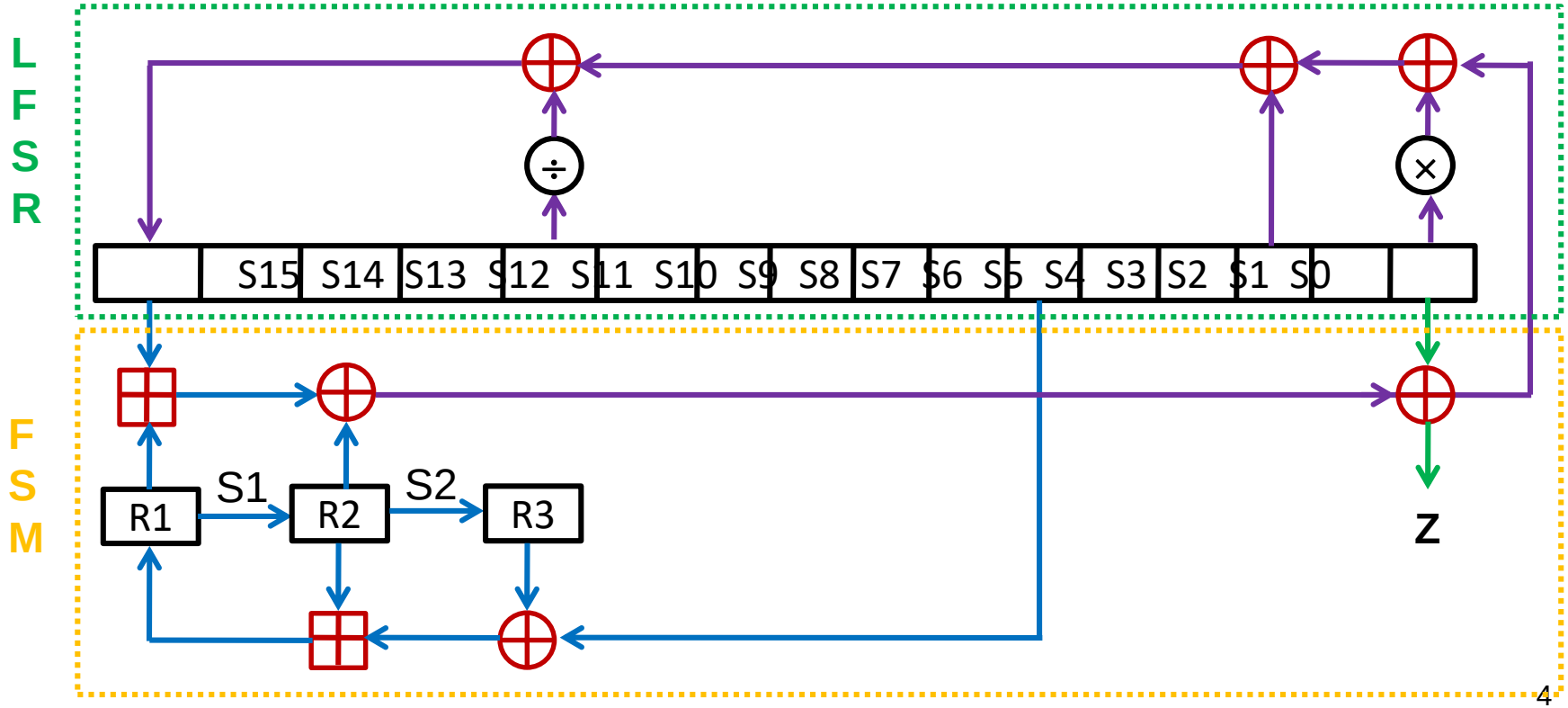


Outline

- Standardized *SNOW-3G* algorithm:
  - *Description, architecture, Internal functions*
- Standardized *ZUC* algorithm:
  - *Description, architecture, internal functions*
- Proposed combined *SNOW-3G* and *ZUC* algorithm:
  - *Based chaotic generator*
- FPGA implementation results
- Security evaluation results
- Discussion
- Conclusion and perspectives

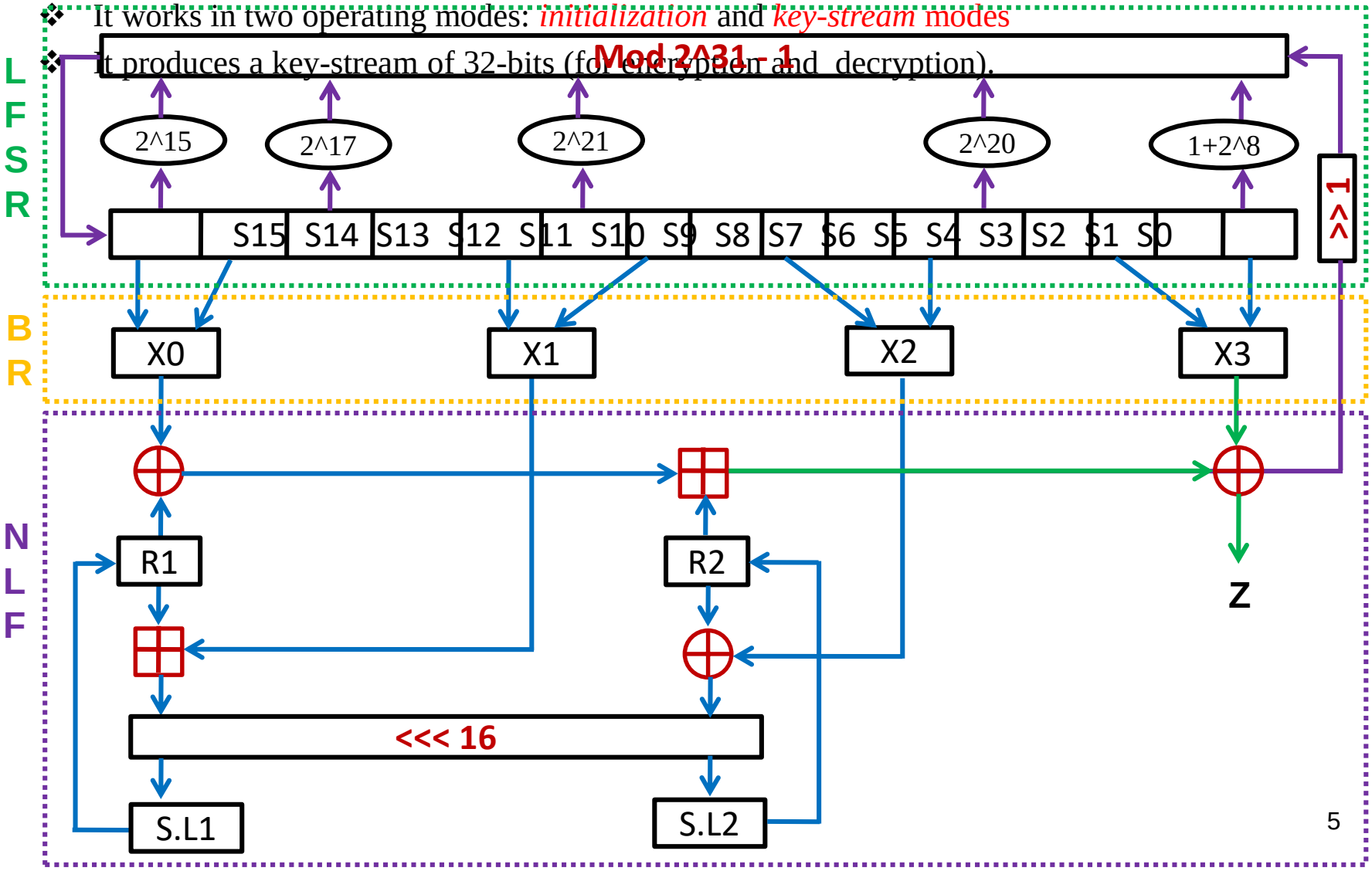
SNOW-3G algorithm

- Stream cipher used to protect voice and data in LTE networks.
- It is formed by two internal modules: *LFSR* and *FSM* modules
- Controlled by using two input parameters: *Ciphering Key* (***CK***, 128-bits) and *Initialization Vector* (***IV***, 128-bits)
- It works in two operating modes: *initialization* and *key-stream* modes
- It produces a key-stream of 32-bits (for encryption and decryption).



ZUC algorithm

- Stream cipher used to protect voice and data in LTE networks.
- It is formed by three internal modules: *LFSR*, *BR* and *NLF* modules
- Controlled using two input parameters: ***CK*** (128-bits) and ***IV*** (128-bits)
- It works in two operating modes: *initialization* and *key-stream* modes
- It produces a key-stream of 32-bits (for encryption and decryption).



SNOW-3G and ZUC weaknesses

SNOW-3G robustness was analysed and its weakness against cryptanalyses attacks has been proved.

- Short key-stream data set attack.
- IHGD (Improved Heuristic Guess and Determine) attack.
- Fault attack.
- Cachetiming attack.
- Multiset collision attack.
- Sliding property attack.

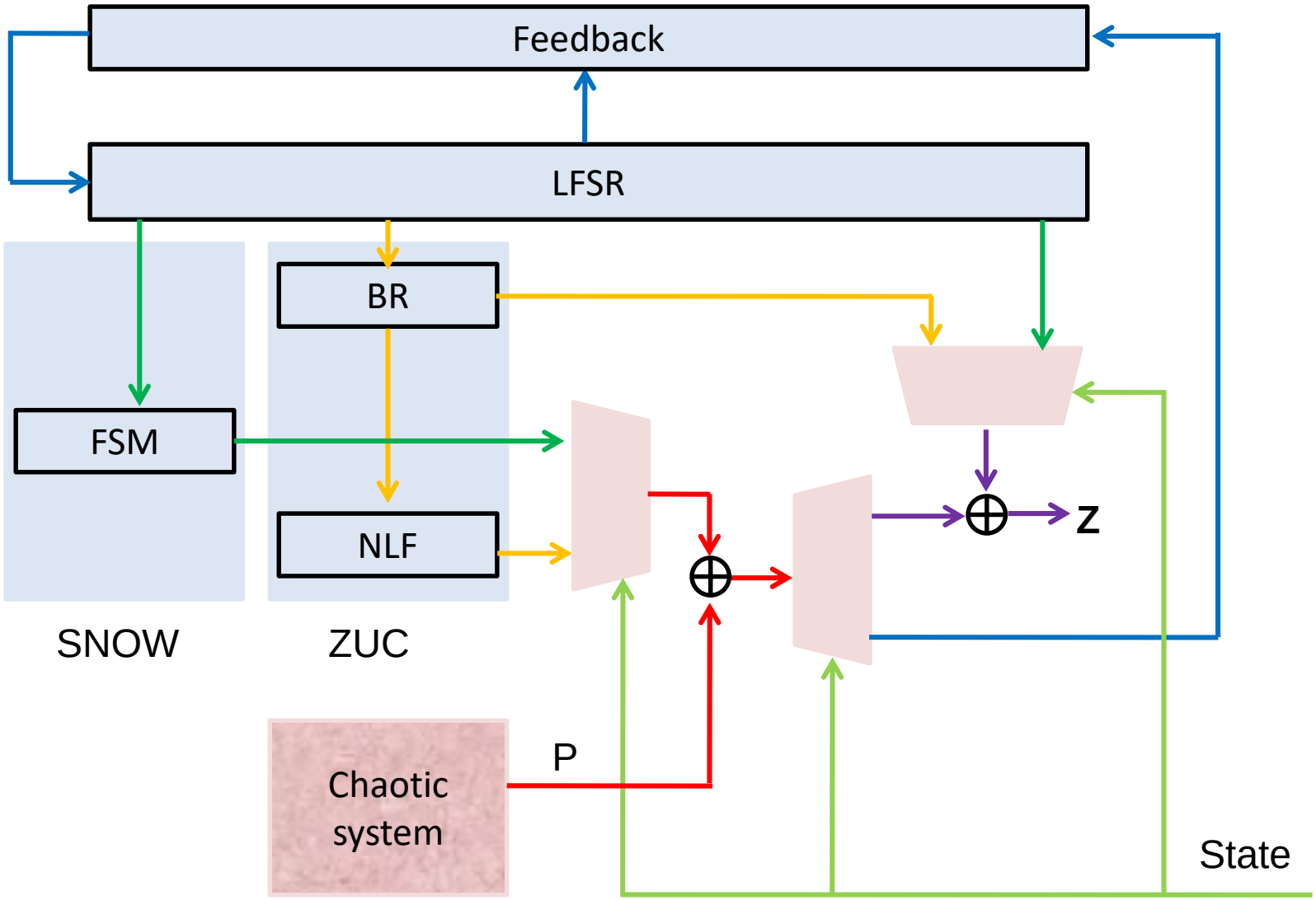
The ZUC robustness was also analyzed and some drawbacks have been found.

- Alternative algebraic analysis.
- Differential attacks.
- Satisfiability solvers based analysis.
- NIST statistical analysis.

Combined *SNOW-3G* and *ZUC* architecture

❖ **The proposed architecture is based on two main contributions:**

1. Optimized implementation of SNOW-3G and ZUC stream cipher functionalities in one scheme.
2. Enhanced robustness using a chaotic generator.

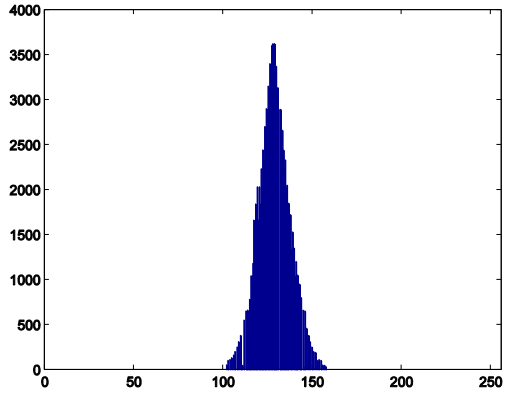


FPGA implementation results

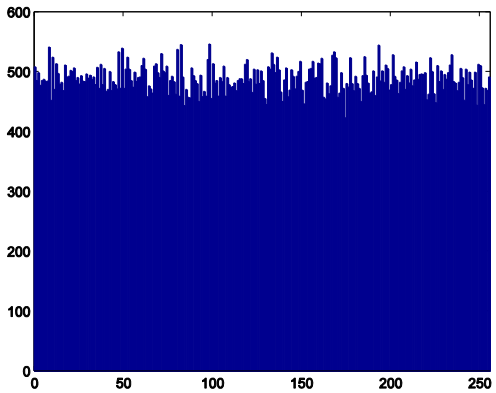
Architecture	***SNOW-3G***	***ZUC***	***SNOW-ZUC***	***SNOW-ZUC based chaos***
Device	***Virtex XC5vfx70t-1ff1136***			
Number of slice registers	1020	1100	1151	2729
Number of slice LUTs	889	1150	1799	10602
Number of fully used LUT-FFpairs	760	875	964	2060
Total memory (KB)	360	72	432	432
Maximum frequency (Mhz)	309.119	196.425	196.194	21.201
Throughput (Mbps)	9891.808	6285.6	6278.208	678.432
Power (Watts)	1.448	1.449	1.449	1.467

Security evaluation results

Key-stream distribution test

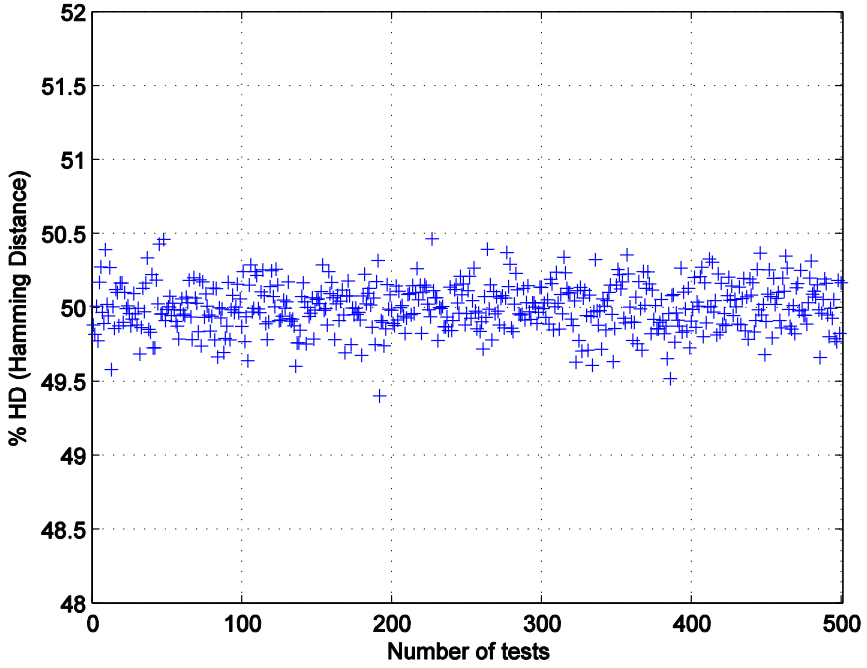


Plain-text distribution



Cipher-text distributio

Key sensitivity test



Key space test

Algorithm	*Key space*
SNOW-3G	2^128
ZUC	2^128
Chaotic generator	2^398
Proposed chaotic SNOW-ZUC	2^526

Security evaluation results – *NIST tests*

Type of test	*Regular SNOW-3G*	*Regular ZUC*	*Proposed chaotic SNOW-ZUC*
Frequency (mono-bit) Test	Success	Success	Success
Frequency Test within a Block	Success	Success	Success
Runs Test	Fail	Success	Success
Tests for the longest-Run-of-ones in a Block	Fail	Success	Success
Binary Matrix Rank Test	Fail	Success	Success
Discrete Fourier Transform (Spectral) Test	Fail	Success	Success
Non-overlapping Template Matching Test	Fail	Fail	Success
Overlapping Template Matching Test	Fail	Success	Success
Maurer's "Universal Statistical" Test	success	Success	Success
Linear Complexity Test	success	Success	Success
Serial Test	Fail	Success	Success
Approximate Entropy Test	Fail	Success	Success
Cumulative sums Test	Success	Success	Success
Random excursion Test	Success	Success	Success
Random excursion variant Test	Success	Success	Success

Discussion

- The proposed architecture is more resistant against cryptanalysis attacks.
- The Key-stream distribution test proves the good randomness and imperfectible properties of the generated outputs.
- The sensitivity to small change (1-bit) in secret key proves the satisfactory of the avalanche effect and Shannon’s theory.
- The improved key space from 2^128 to 2^526 enhances the resistance against exhaustive and brute-force attacks.
- Resistance against linear, differential, and statistical attacks was proved by NIST tests.

Conclusion & Perspectives

- This work proposes a new LTE security from the combination of used standard cipher algorithms.
- A combined SNOW-ZUC architecture with chaotic generator to generate a robust key-stream has been proposed.
- A *Lorenz's* 4D chaotic generator is added to enhance the robustness.
- The standardized fonctionnalities of SNOW-3G and ZUC are considered and preserved.
- A limited additional cost for the hardware implementation.
- The proposed solution is robust against the usual cryptanalysis attacks.
- As future work ➔ *Integrate the proposed architecture to ensure confidentiality and integrity functions of the LTE network.*