INSTITUT D'ELECTRONIQUE ET
DE TELECOMMUNICATIONS
DE RENNES

Palestine Polytechnic University
جامعة بوليتكنك فلسطين
رابطة الجامعيين - الخليل

Chaos-based Crypto Compression Systems and Blockchain

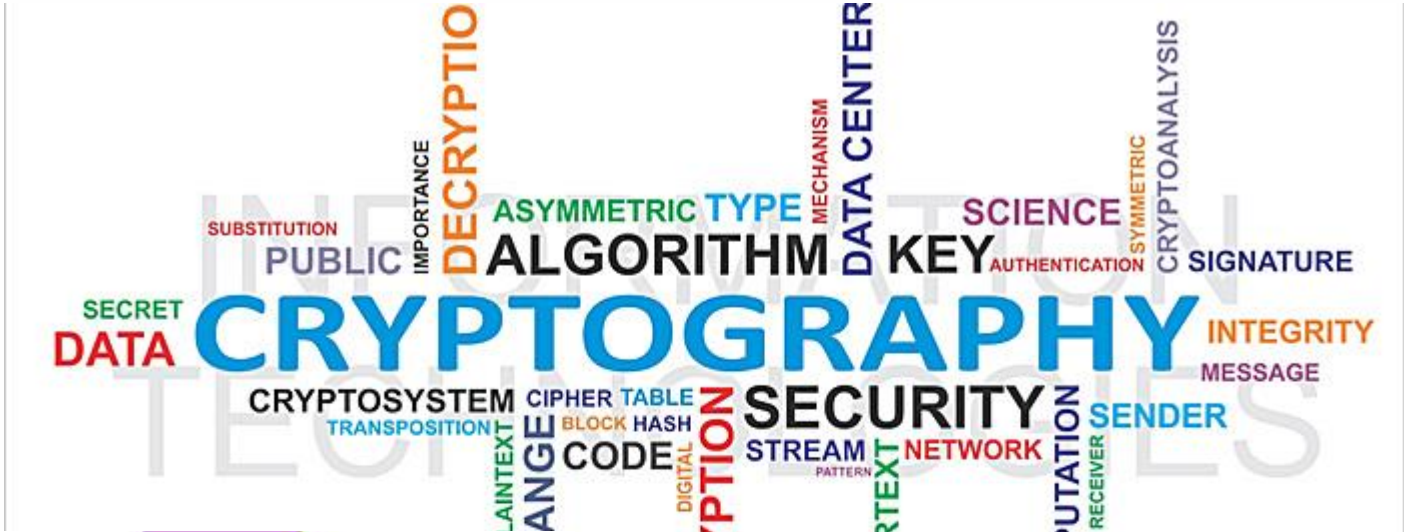
Dr. Mohammed Abutaha
PhD. Information Security

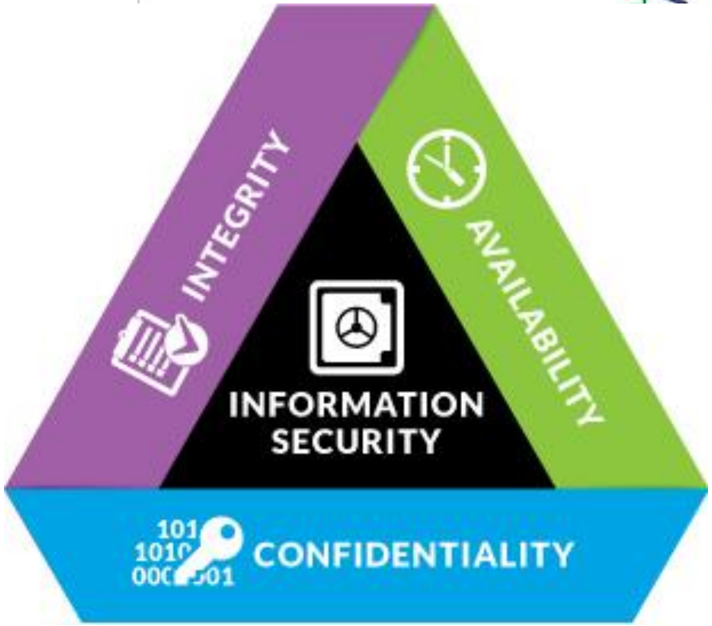
cnrs
INSA RENNES
CentraleSupélec
UNIVERSITÉ DE NANTES
UNIVERSITÉ DE RENNES 1
IETR

Outline

- ❑ Introduction
- ❑ Chaos based stream cipher
- ❑ Selective encryption on HEVC
- ❑ Chaos crypto and blockchain
- ❑ Demo

Introduction

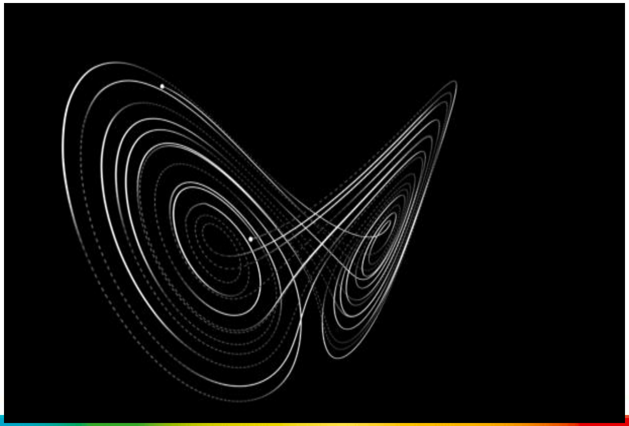




- ❖ Refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms to transform messages in ways that are hard to decipher.

Chaos and cryptography

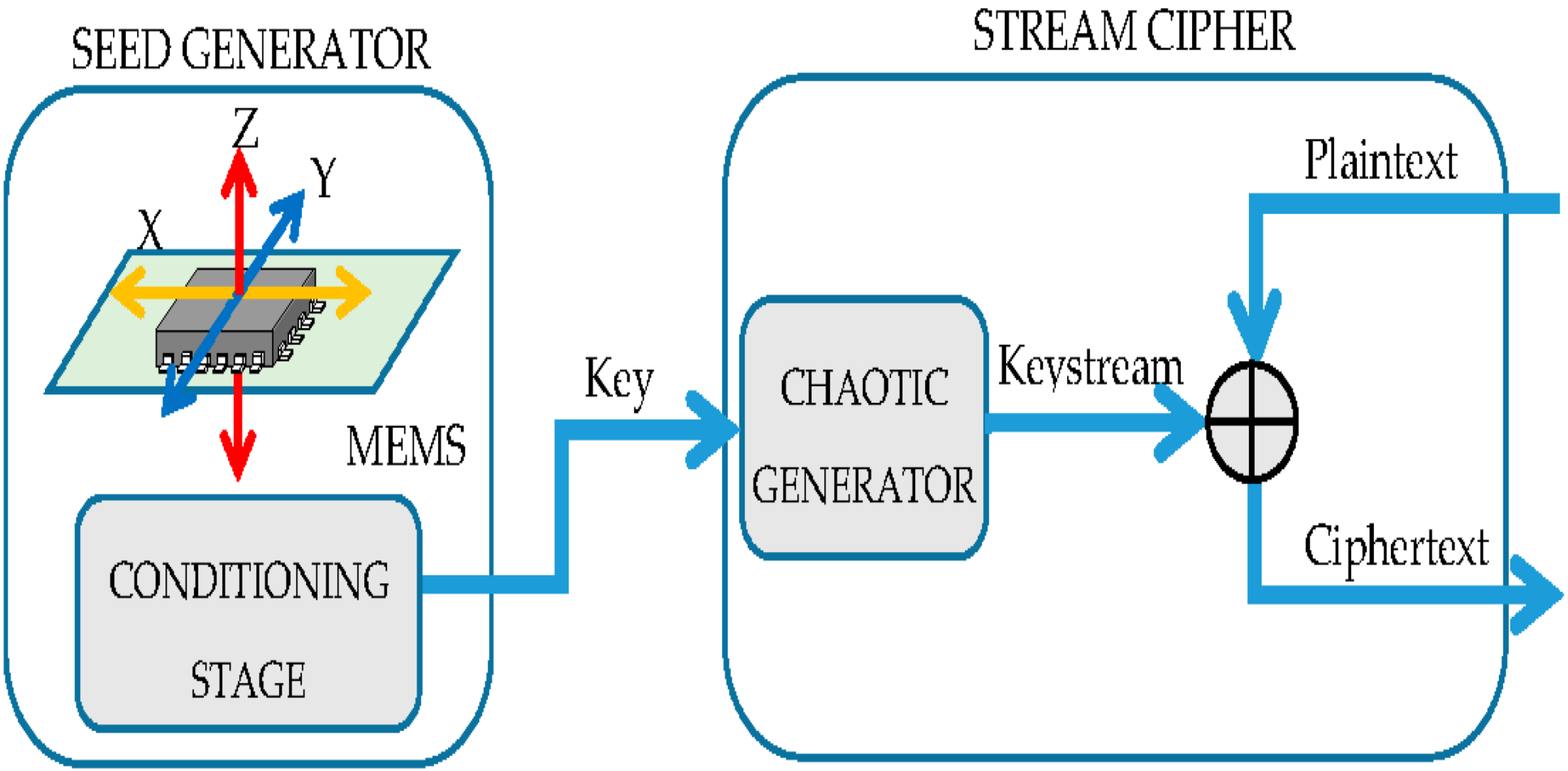
- ❑ **Chaos theory**
- ❖ **Definition:** State of Turmoil, Disorder & Disarray
- ❖ **Scientific Definition:** New field of study in mathematics, studying the behavior of dynamical systems sensitive to changes of initial conditions
- ❑ Chaos in cryptography was discovered by Matthews in 1990s.



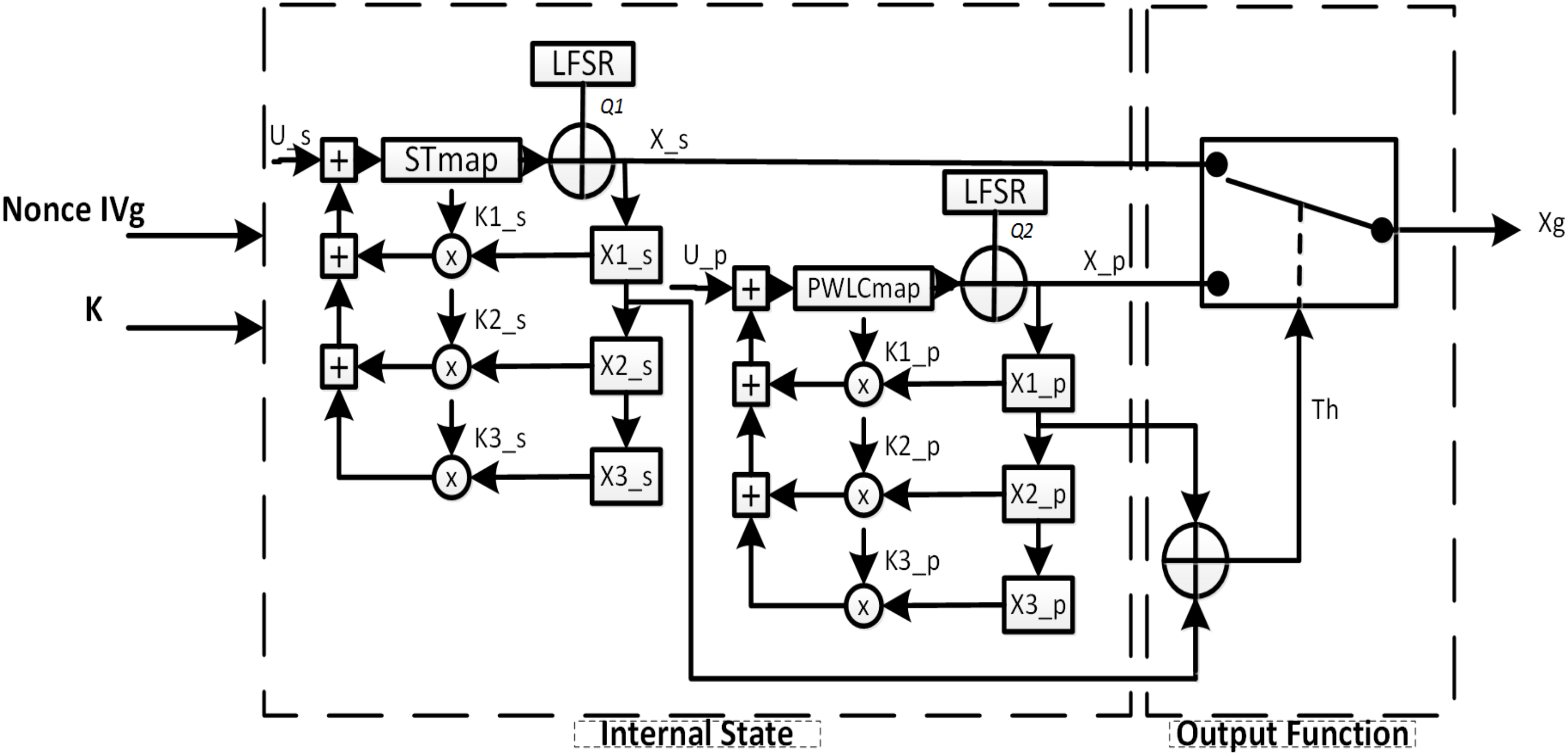
Why using chaos to secure information?

Chaotic property	Cryptographic property	Description
Ergodicity	Confusion	The output has the same distribution for any input
Sensitivity to initial conditions	Diffusion	A small deviation in the input can cause a large change at the output
Deterministic dynamics	Deterministic pseudo-randomness	A deterministic process can cause a random-like (pseudo-random) behavior
Structure complexity	Algorithm (attack) complexity	A simple process has a very high complexity

Chaos based stream cipher

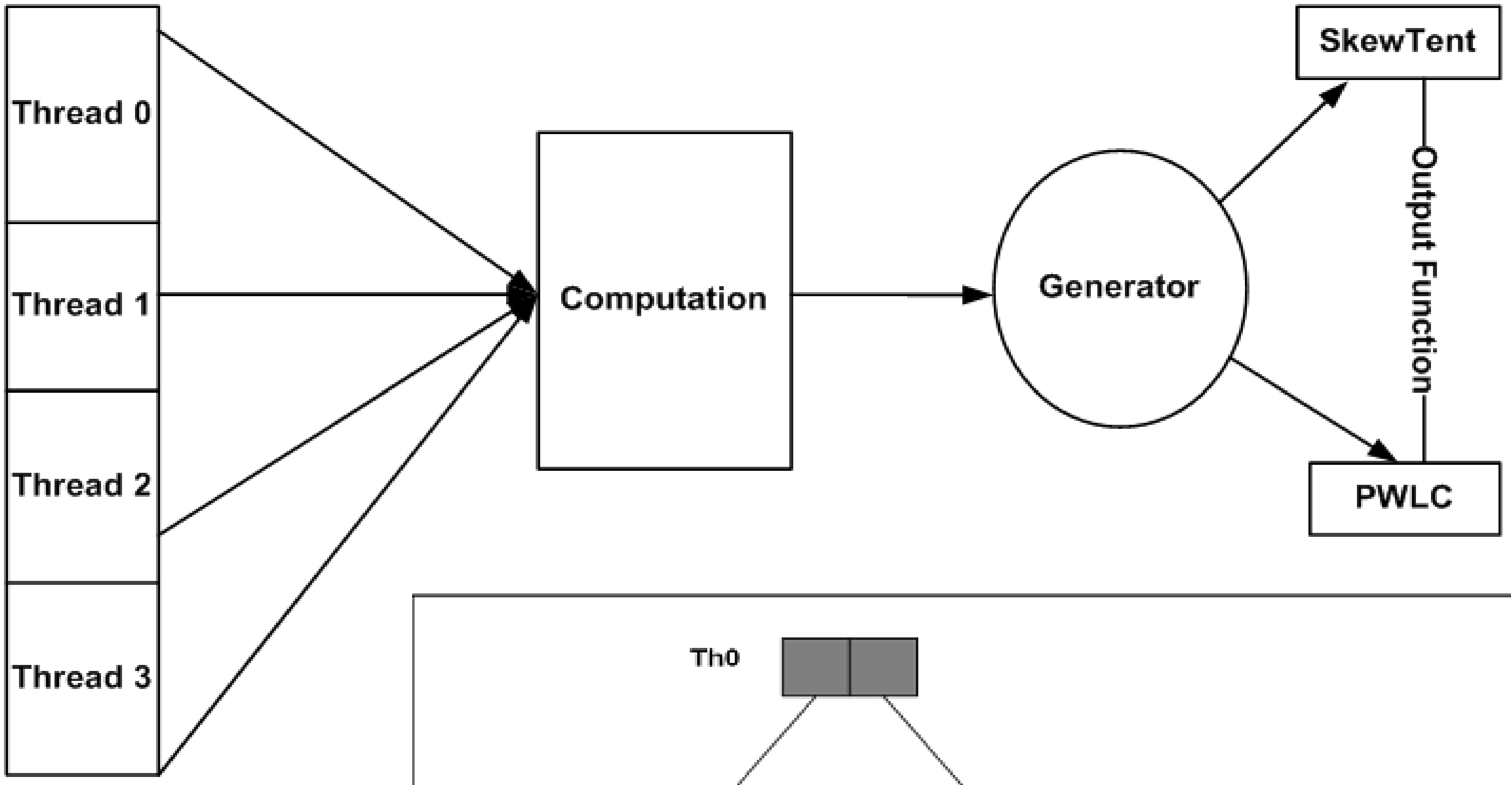


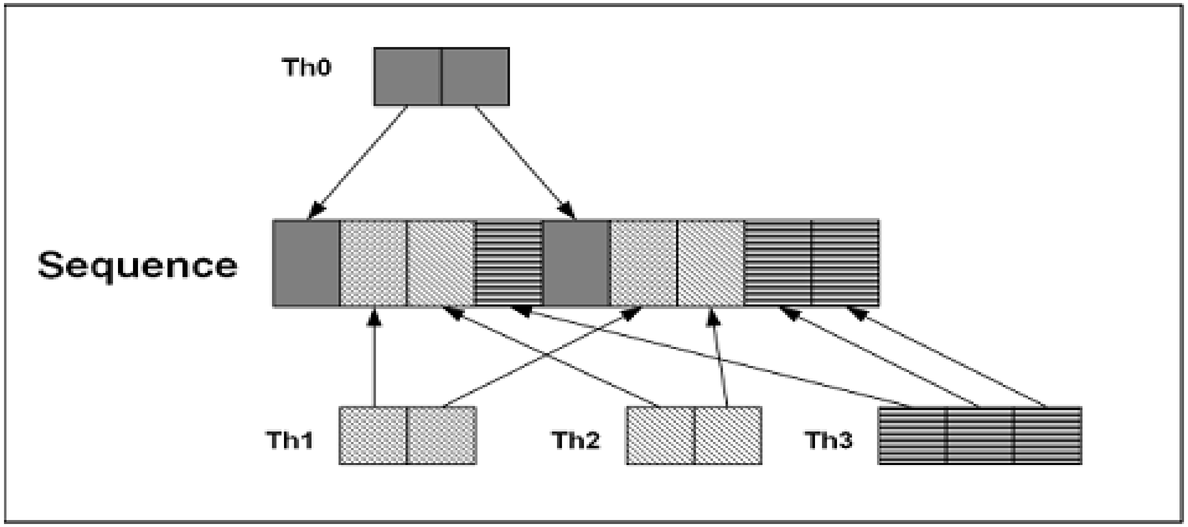
Chaotic Generator



- ❑ Recursive structure (El Assad et. al., 2008 & 2011)
- ❑ Perturbation Technique (Tao, 2005, El Assad 2008)
- ❑ Chaotic mixing (Lozi, 2007 & 2012)

Chaotic samples production using Pthread

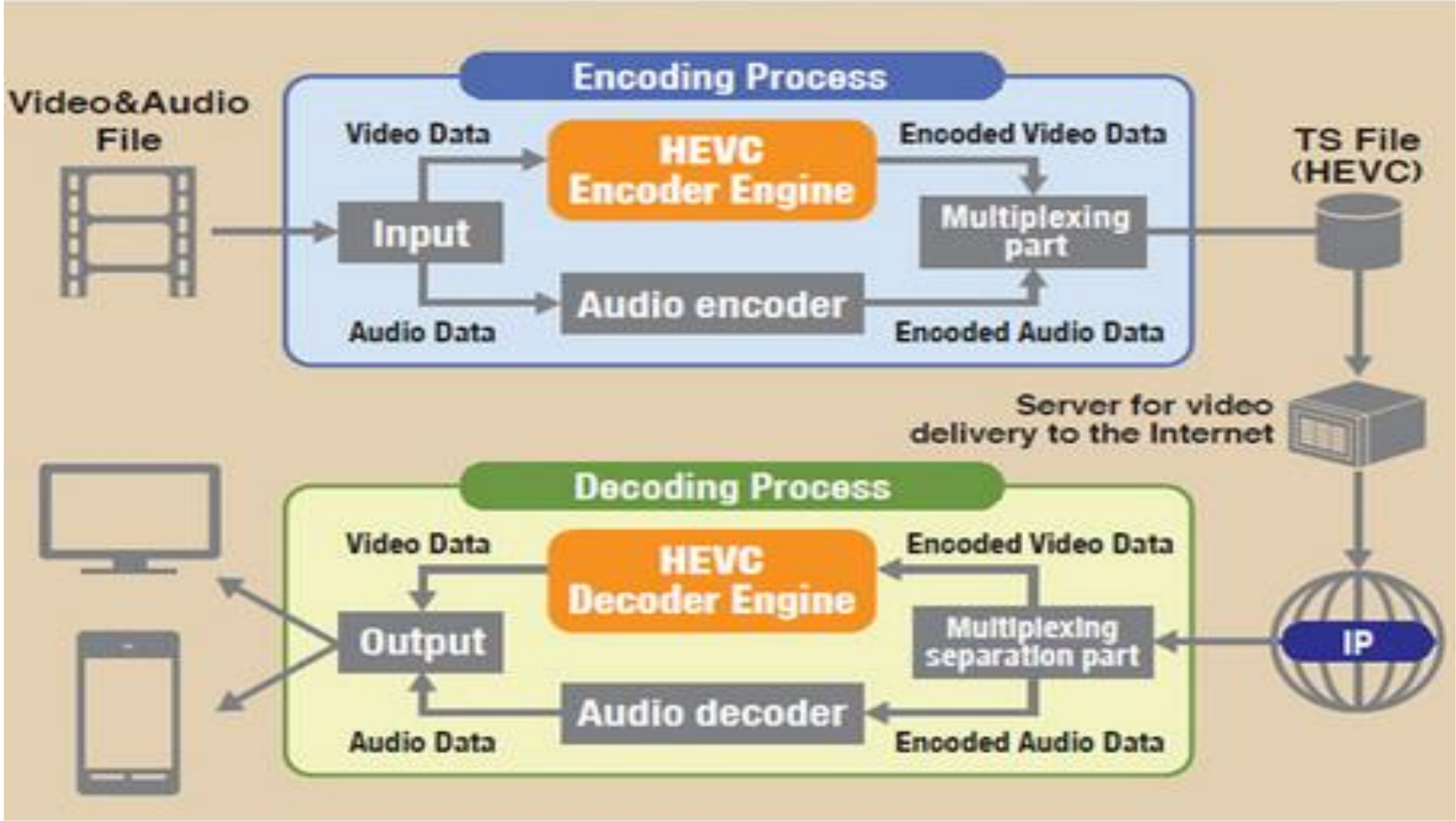




HEVC

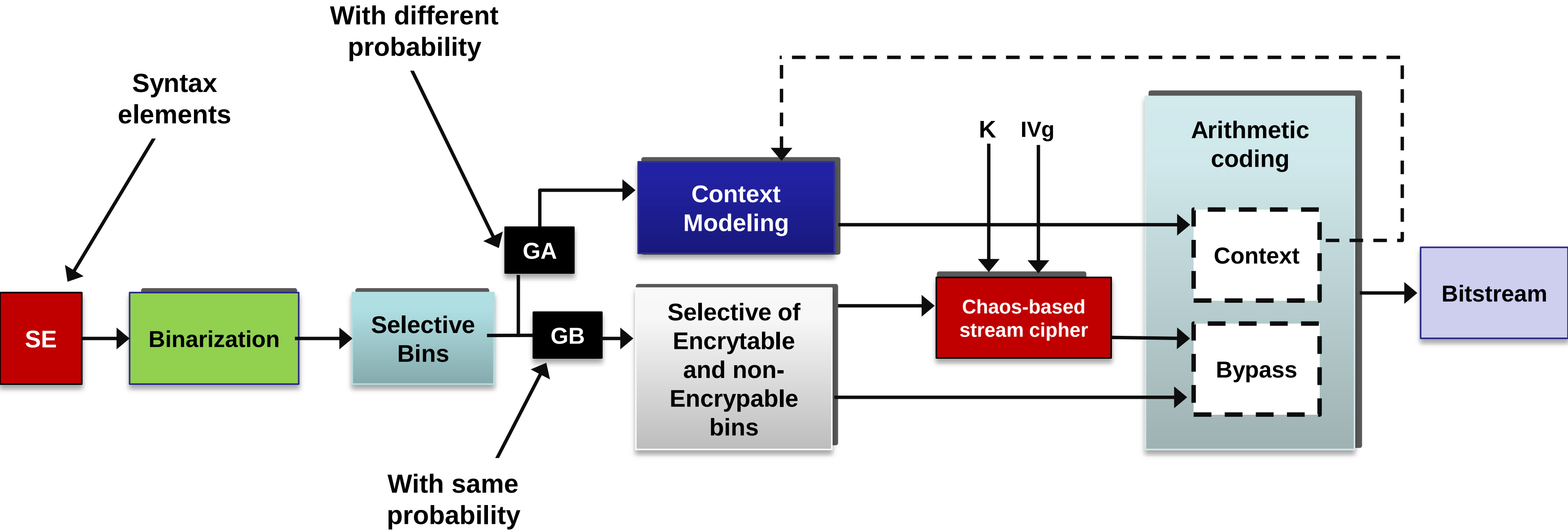
HEVC Software CODEC

HEVC-1000 SDK



Selective Encryption

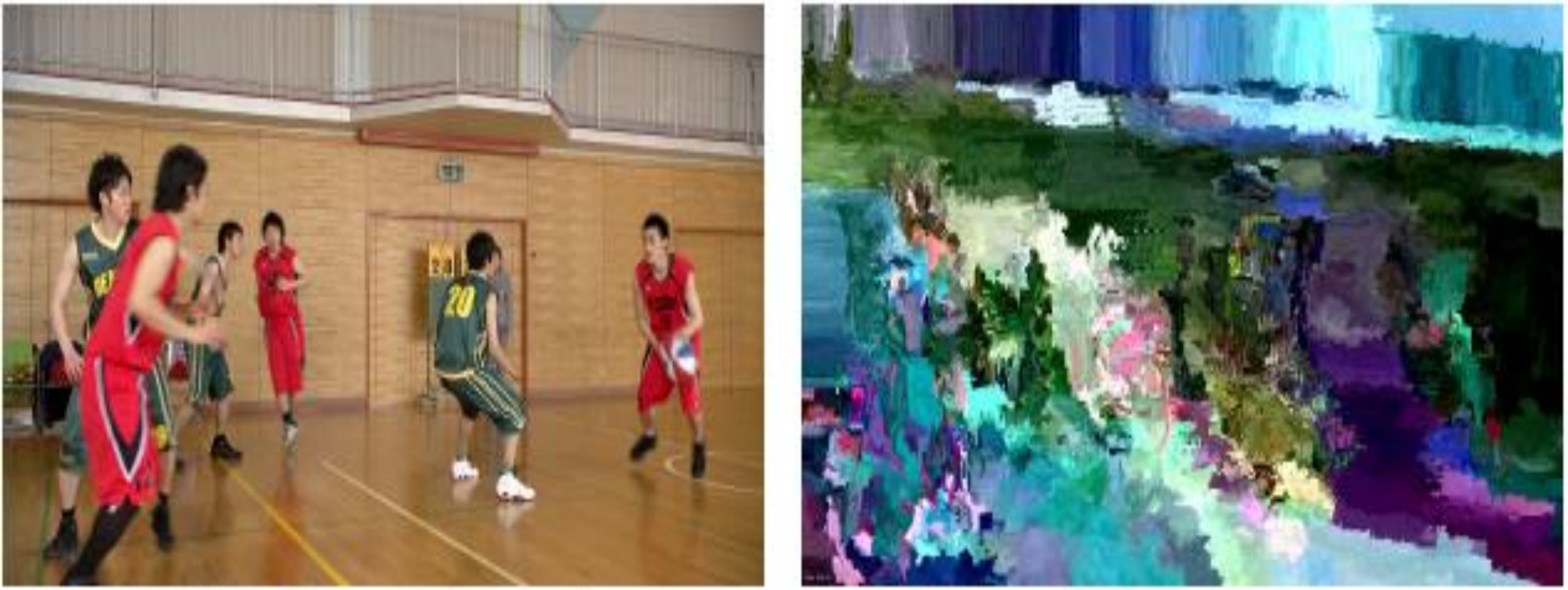
Context based adaptive binary arithmetic (CABAC)



- ❖ Selective encryption is a new trend in image and video content protection. It consists of encrypting only a subset of the data.

- ❖ The aim of selective encryption is to reduce the amount of data to encrypt while preserving a sufficient level of security.

Full level Selective Encryption

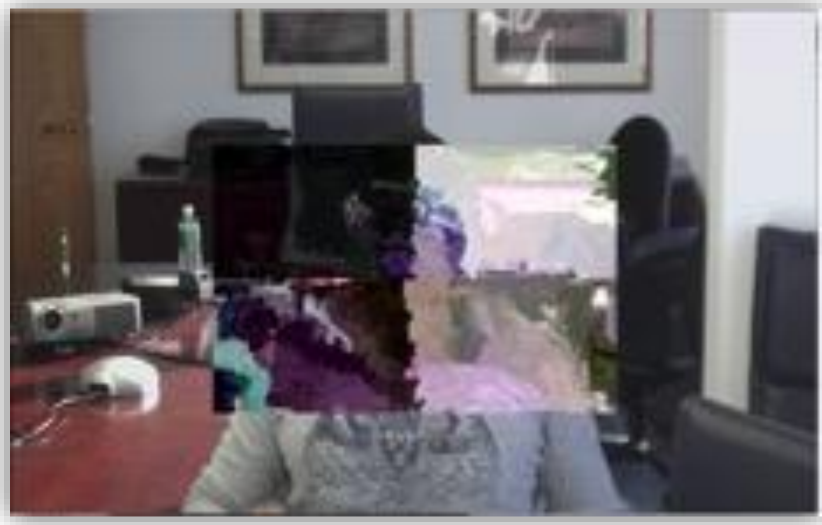


(a) Original frame without encrption

(b) Encrypted frame

- ➢ Figure (b) clarifies the visual impact of the proposed scheme on the frame content, it shows the distorsion of the visual content quality.

ROI Encryption



- The proposed encryption solution conceals the objective quality of the ROI zone, while the background remains clean.

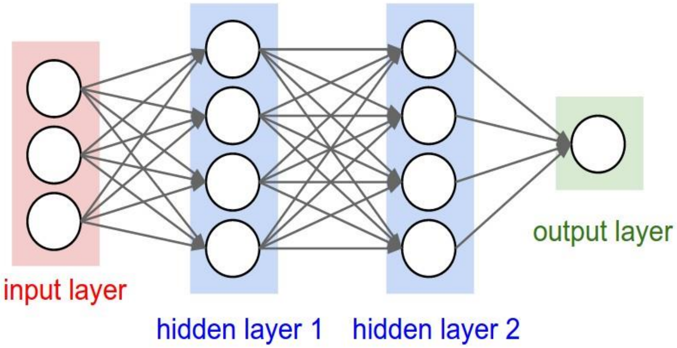
Chaos based security and blockchain

- we developed a chaos hash function used in secure the connections between blocks

- A **blockchain** is a growing list of records, called *blocks*, which are linked using cryptography. Each block contains a cryptographic hash of the previous block.

Structures of the proposed Hash functions

- ❑Chaotic system & Secret key
- ❑ Chaotic Neural Network
- ❑ Multi-block Hash scheme



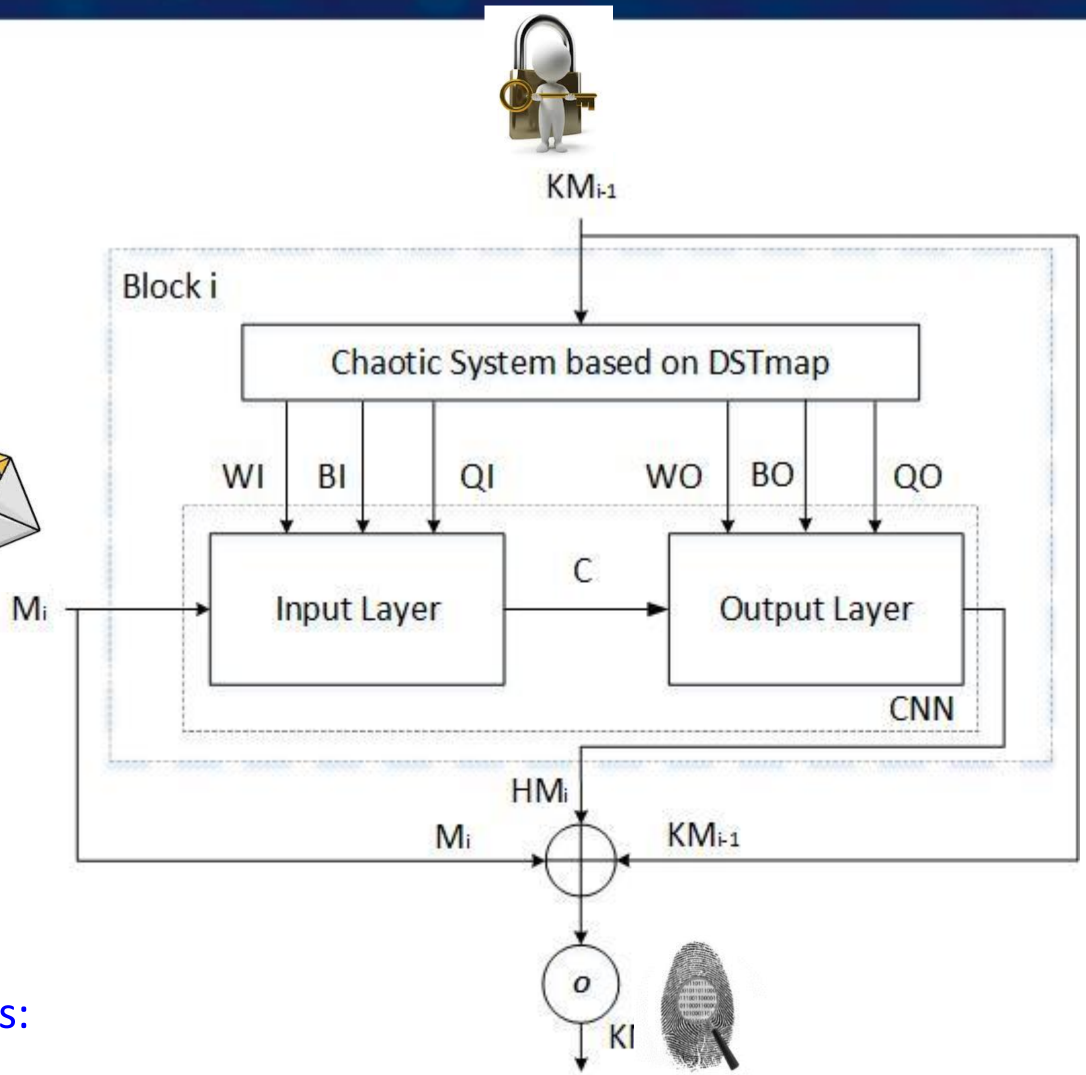


Fig.7: Structure of the block i in the proposed hash function

❑Neural Network - main characteristics:

1. One way property
2. Diffusion
3. Compression

Hashing bitcoin

- ❑ An important property of hashes is that if a tiny amount of input data is changed the output changes significantly.

We can use the chaos based hash function to hash the bitcoin

- ❑ The corresponding chaos hash of the sentence “**Bitcoin?**” looks like this:

156aedcfab1d49f73abddd89faf78d9930e4b523ab804026310c973bfa707d37

- ❑ If we remove only one symbol – for example the question mark “?” – the hash of “**Bitcoin**” looks like this:

4314d903f04e90e4a5057685243c903fbcfa4f8ec75ec797e1780ed5c891b1bf

Demo

- Selective encryption on HEVC

- ROI encryption on HEVC

Thanks for your attention

Questions ?