National Institute of
Advanced Industrial Science
and Technology
AIST

Research Center for
Information Security

Symmetric Key Cryptographic Primitives Based on Pseudo-Randomness, Randomness and Dedicated Coding

Power of Randomness for Enhancing Security and Low Implementation Complexity

Miodrag Mihaljevic

National Institute of Advanced Industrial Science and Technology
AIST

Power of Randomness for High Security and Low Implementation Complexity

Research Center for Information Security

- **Goal**: Design of Cryptographic Primitives with Enhanced Security and Low Implementation Complexity

- Encryption - Compact Stream Ciphers
- Authentication Protocols for RFID and related applications

National Institute of Advanced Industrial Science and Technology
AIST

Power of Randomness for High Security and Low Implementation Complexity

Research Center for Information Security

Design Components:

- Simple Finite State Machine for the Pseudo-Randomness
- Dedicated Coding: Homophonic and Error-Correction Ones
- Randomness

Effects:

- Enhanced Security Implied by Randomness
- Low Implementation Complexity

National Institute of Advanced Industrial Science and Technology
AIST

Stream Cipher Approaches

Research Center for Information Security

- **One-Time Pad** – pure random approach (provable security)
- Traditional **Keystream Generator** – finite state machine: a deterministic approach (heuristic security)

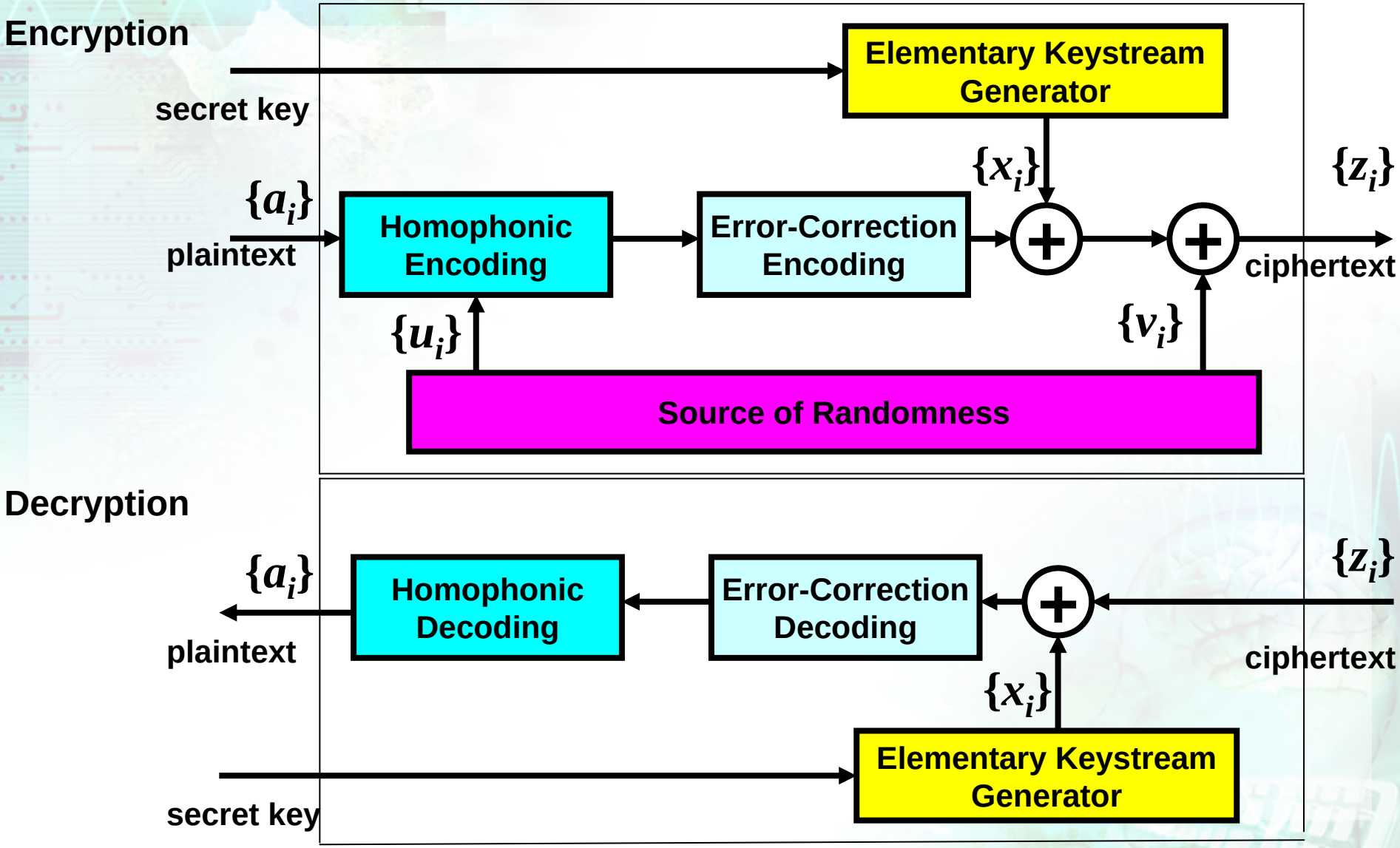
Randomized approach:

- A stream cipher based on employment of **Pseudorandomness, Randomness and Dedicated Coding**
- **Towards provable security implied by the dimension of secret key**

National Institute of Advanced Industrial Science and Technology
AIST

Framework for a Stream Ciphers Design

Research Center for Information Security



National Institute of Advanced Industrial Science and Technology
AIST

References

Research Center for Information Security

- [1] M. Mihaljevic and H. Imai, ”**An approach for stream ciphers design based on joint computing over random and secret data**”, *Computing*, vol. 85, no. 1-2, pp. 153-168, June 2009.
- [2] M. Mihaljevic, "**A Framework for Stream Ciphers Based on Pseudorandomness, Randomness and Error-Correcting Coding**", in Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes, Vol. 23 in the *Series: Information and Communication Security*, pp. 117-139, IOS Press, June 2009.
- [3] M. Mihaljevic and F. Oggier, "**A Wire-tap Approach to Enhance Security in Communication Systems using the Encoding-Encryption Paradigm**", *IEEE ICT 2010 - Int. Comm. Conf., Proceedings*, pp. 484-489, April 2010.
- [4] M. Mihaljevic and H. Imai, "**A Stream Cipher Design Based on Embedding of Random Bits**", *IEEE 2008 Int. Symp. on Inform. Theory and its Appl. - ISITA2008*, *Proceedings*, pp. 1497-1502, Dec. 2008
- [5] M. Mihaljevic, H. Watanabe and H. Imai, "**A Cellular Automata Based HB#-like Low Complexity Authentication Technique**", *IEEE 2008 Int. Symp. on Inform. Theory and its Appl. - ISITA2008*, *Proceedings*, pp. 1355-1360, Dec. 2008