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

Miodrag Mihaljevic

Power of Randomness for High Security and Low Implementation Complexity

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

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

Design Components:

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

Effects:

➢Enhanced Security Implied by Randomness
➢Low Implementation Complexity

References:

[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.

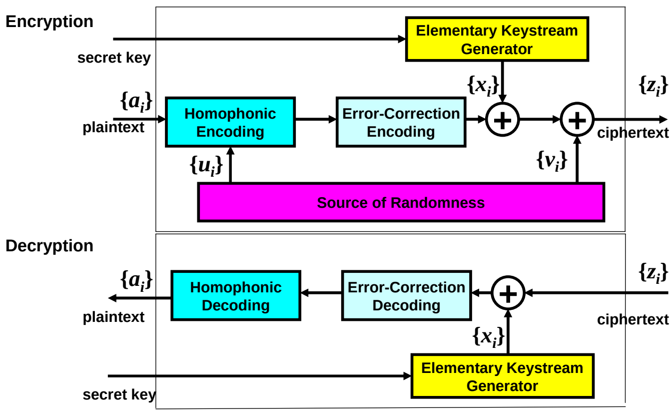
[2] M. Mihaljevic, "**A Framework for Stream Ciphers Based on Pseudorandomness, Randomness and Error-Correcting Coding**", in Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes, Vol. 23 in the *NATO Science for Peace and Security Series - D: Information and Communication Security*, pp. 117-139, IOS Press, Amsterdam, The Netherlands, 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

Design of a Stream Cipher



An Authentication Protocol

- Party $\mathcal{B}$ sends vector $\mathbf{r}_{\mathcal{B}}$ to party $\mathcal{A}$;
- Party $\mathcal{A}$ sends vector $\mathbf{r}_{\mathcal{A}}$ to party $\mathcal{B}$;
- Party $\mathcal{B}$ performs the following:
  - Employing the keystream generator seeded by the secret key $\mathbf{k} = [k_i]_{i=1}^{k}$ and the vectors $\mathbf{r}_{\mathcal{A}}$ and $\mathbf{r}_{\mathcal{B}}$ generate the vector $\mathbf{x}$;
  - Generate n-dimensional binary vector $\mathbf{z} = [z_i]_{i=1}^{n}$
    $$\mathbf{z} = C_{ECC}(C_H(\mathbf{a}||\mathbf{u})) \oplus \mathbf{x} \oplus \mathbf{v}$$
    where $\mathbf{a} = \mathbf{r}_{\mathcal{A}}||\mathbf{r}_{\mathcal{B}}$;
  - Sends the response vector $\mathbf{z}$ to party $\mathcal{A}$.
- Party $\mathcal{A}$ performs the following:
  - Employing the keystream generator seeded by the secret key $\mathbf{k} = [k_i]_{i=1}^{k}$ and the vectors $\mathbf{r}_{\mathcal{A}}$ and $\mathbf{r}_{\mathcal{B}}$ generate the vector $\mathbf{x}$;
  - Employing the received vector $\mathbf{z}$ calculate:
    $$\hat{\mathbf{a}} = tcat_{\ell}(C_H^{-1}(C_{ECC}^{-1}(\mathbf{z} \oplus \mathbf{x})))$$
  - Assuming that the employed ECC has cancelled the error-vector $\mathbf{v}$ make the authentication decision as follows: If $\hat{\mathbf{a}} = \mathbf{r}_{\mathcal{A}}||\mathbf{r}_{\mathcal{B}}$ the party $\mathcal{B}$ is authentic, and otherwise not authentic.