MINISTRY OF EDUCATION AND SCIENCE
OF THE REPUBLIC OF KAZAKHSTAN
COMMITTEE OF SCIENCE

INSTITUTE OF INFORMATION AND COMPUTATIONAL TECHNOLOGIES
Information Security Laboratory

Cryptographic systems based on nonpositional polynomial notation system

---

CTCrypt 2016

Main research directions

- Symmetric and asymmetric encryption based on nonpositional polynomial notations (NPNs)
- System of digital signature based on NPNs
- PRN generators
- System of multicriterial access restriction

Symmetric encryption algorithm

For a data block of length of *N* bits form a system of moduli from the set of all irreducible polynomials of degree not exceeding *N*

$$p_1(x), p_2(x), \ldots, p_S(x)$$

The data block is represented as a sequence of remainders of division of some polynomial with binary coefficients

$$F(x) = (\alpha_1(x), \alpha_2(x), \ldots, \alpha_S(x))$$

where $F(x) = \alpha_i(x) (\mathrm{mod}\ p_i(x))$, $i = 1 \ldots S$.

It is demonstrated that polynomial representation of the polynomial in the form *F(x)* is unique (similar to Chinese remainder theorem for polynomials)

Symmetric encryption algorithm

Then the secret key of length of N bits is also interpreted as

$$G(x) = (\beta_1(x), \beta_2(x),\ldots,\beta_S(x))$$

where $G(x) = \beta_i(x) (\mathrm{mod}\ p_i(x))$, $i = 1\ldots S$.

This ciphertext is considered as a function $H(x)$:

$$H(x) = (\omega_1(x), \omega_2(x),\ldots,\omega_S(x))$$

For instance,

$$F(x)G(x) = H(x) (\mathrm{mod}\ P(x))$$

Symmetric encryption algorithm

- Current researches
  - Application of Feistel scheme
  - Application of encryption modes
  - Strength against cryptanalysis
- Future work
  - Investigate the practical possibility of parallel processing
  - Research the possibility of hardware implementation