Activities of IMI-BAS in data protection

Tsonka Baicheva, Peter Boyvalenkov

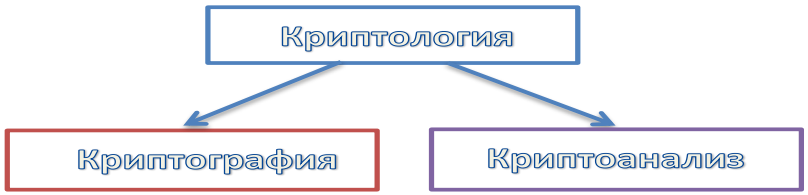
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences

November 11, 2013
Sofia

Department of Mathematical Foundations of Informatics - since 1988, founded by Stefan Dodunekov (1945-2012)
Coding Theory – Cryptology
Theory and Applications

Cryptology

- The cryptology studies the mathematical techniques to ensure data security and methods for attack and defence.
- Mathematics in Cryptology:
  - Discrete Mathematics
  - Number theory, Algebra
  - Geometry
  - Coding theory – over 300 papers since 1975 in specialized international journals



Challenges to the Cryptography

- Post quantum Cryptography
- Longlasting security: 50 - 100 years
- Security for cloud technologies
- Authentification Cryptology
- Low-energy applications (lightweight cryptography)

McElliece public key system

- Proposed in 1978 by Robert McElliece
- Strong candidate for post-quantum algorithm
- Based on the difficulties in solving decoding problems
  - The private key uses a linear code with known effective decoding
  - The public key proposes difficult decoding problem
- No known successfull attacks
- In particular – resistent to Shor attack

Mathematics behind the McElliece system

Let C be a binary $[n, k]$ code which is able to correct t errors, S be a binary non-singular $k \times k$ matrix, P be a permutation $n \times n$ matrix. Calculate the matrix

$$G^* = SGP,$$

where G is a $k \times n$ generator matrix of C.

Encryption:

(1) Divide the message into blocks of length k; let v be such a block;

(2) Calculate vG^*;

(3) Invert randomly t bits in vG^*;

(4) The cryptotext is

$$w = vG^* + e,$$

where e is random vector (corresponding to the changes in (3)) of weight t.

The matrix G^* (the encryption key) is public, the matrices S, G and P are kept secret.

Advanced Encryption Standard (AES)

- Accepted by National Institute of Standards and Technology (NIST) of USA in 2001
- According to the validation list of NIST (http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html) there are (at least) 2662 implementations
- 2003: AES-128 for classified information, AES-192/-256 for top secret information
- Many attack; no known sucessfull attack
- The diffusion in the algorithm is ensured by MDS codes

- Bulgarian contributions to the theory of MDS codes – Dodunekov, Landjev (over 10 papers)

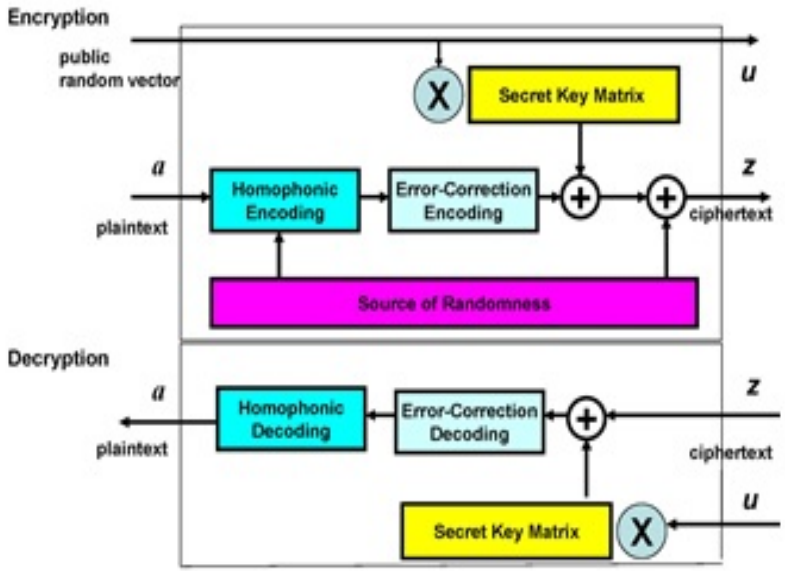
Lightweight криптография

- Low:
  - energy consumption
  - implementation resourses
  - computational efforts

- Authentification by Niederreiter cryptosystem
  - Modification from a McElliece system; developed in 1986 by Harald Niederreiter
  - Uses the syndrome as cryptotext; the message is the error vector

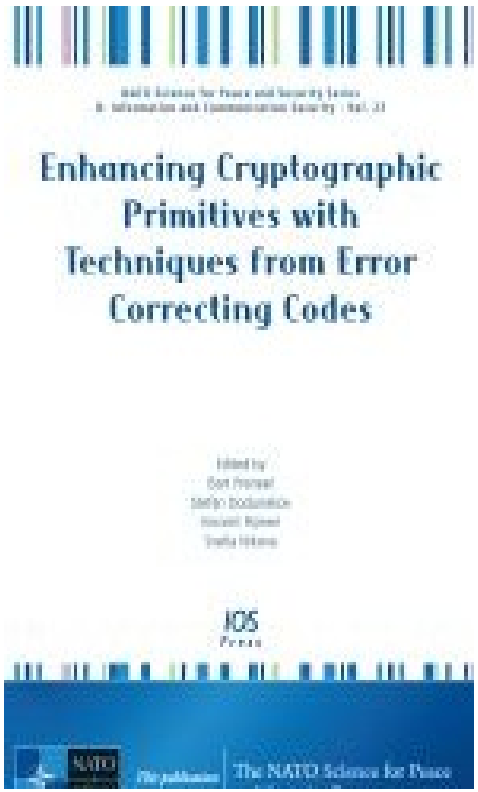
Homophonic coding and error-correcting coding

- The homophonic coding ensures randomization of the plaintext
- Against statistical attacks



Seminars and schools I

- Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes Veliko Tarnovo, October 6-9, 2008



Seminars and schools II

- Design and Security of Cryptographic Functions, Algorithms and Devices
  (https://www.cosic.esat.kuleuven.be/summer_school_albena/)
  Albena, June 30 - July 5, 2013
  - 24 lecturers from Austria, Belgium, Germany, Denmark, Israel, Ireland, Norway, USA, France, The Netherlands, Switzerland
  - Bart Preneel - chair of International Association for Cryptologic Research
  - Vincent Rijemen - one of the proposers of AES

Seminars and schools III

- BalkanCrypt Kickoff Meeting and Workshop (http://balkancrypt.uist.edu.mk/) Sofia, November 7-8, 2013
  - 40 participans from Balcan countries, Belgium, Germany, Norway, Japan
  - Bart Preenel
  - Hideki Imai - chair of CRYPTREC (Cryptography Techniques Research and Evaluation Committee of Japan)

- Bulgaria will organize EUROCRYPT 2015