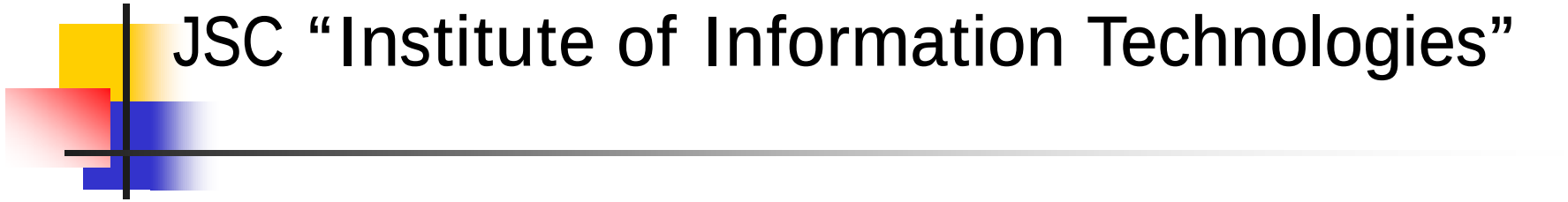
Kharkov National University of Radioelectronics
JSC “Institute of Information Technologies”

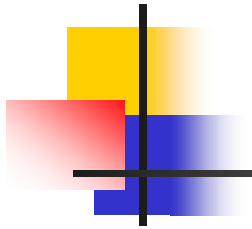


Results of public cryptographic competition in Ukraine

Roman Oliynykov
ROliynykov@gmail.com
Ivan Gorbenko
GorbenkoI@iit.kharkov.ua

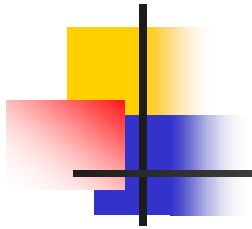
Kharkov, Ukraine
2009

Public cryptographic competition



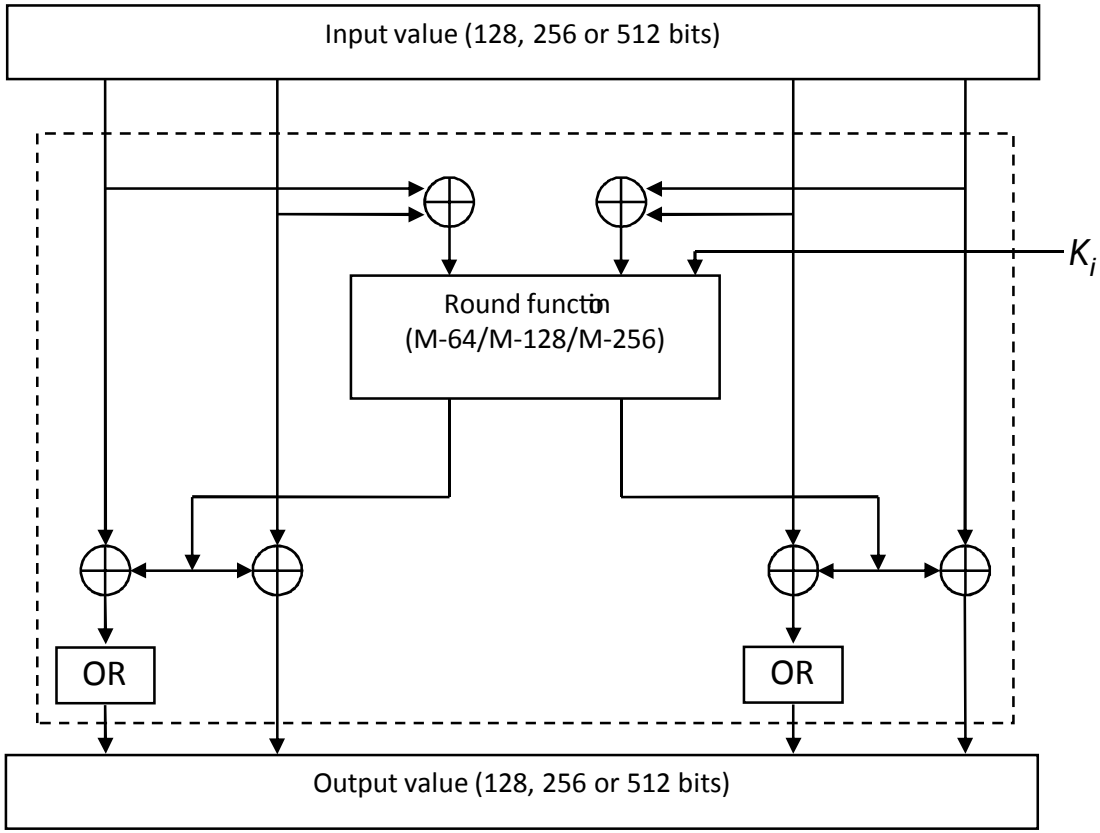
- Announced in 2006
- General aim – selection of algorithm-prototype for standard of symmetric block ciphers of Ukraine instead of Soviet GOST
- Five symmetric block ciphers proposed to the competition during the first stage (2006-2007)
- Three ciphers were accepted to the second stage (2008-2009)
- Final selection of winner is expected in 2009

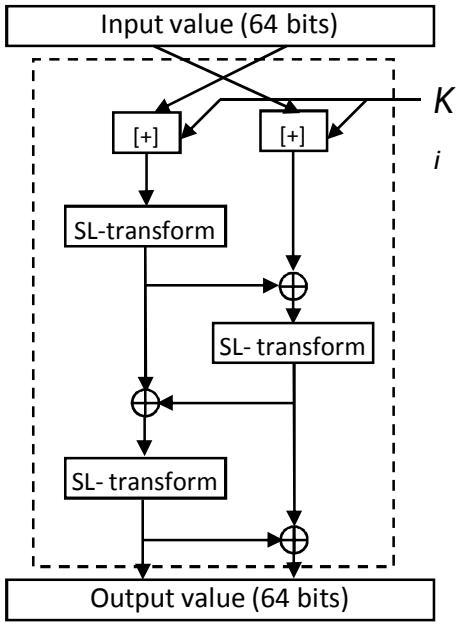
Symmetric block ciphers proposed to the competition

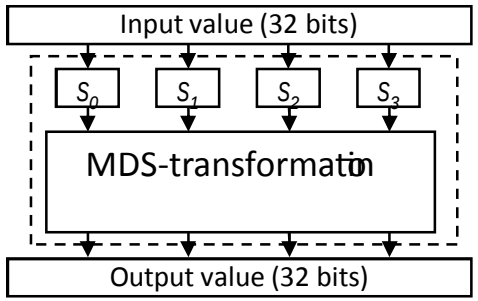


- "**Kalyna**" (JSC "Institute of Information Technologies", Kharkov)
- "**Mukhomor**" (Kharkov National University of Radioelectronics)
- **ADE** (Kozhedub Air Force University, Kiev/Kharkov)
- "**Labirynth**" (JSC "Cryptomach", Kharkov, Ukraine)
- **RSB** (National Aviation University, Kiev)

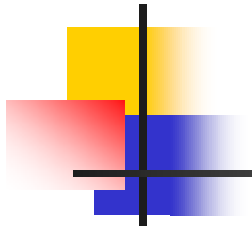
Symmetric block cipher “Mukhomor”





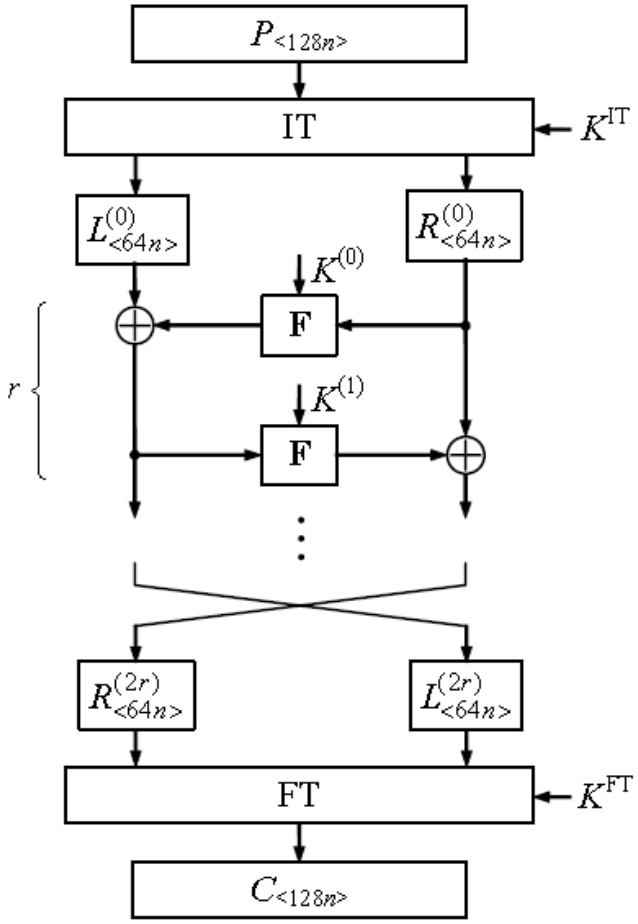


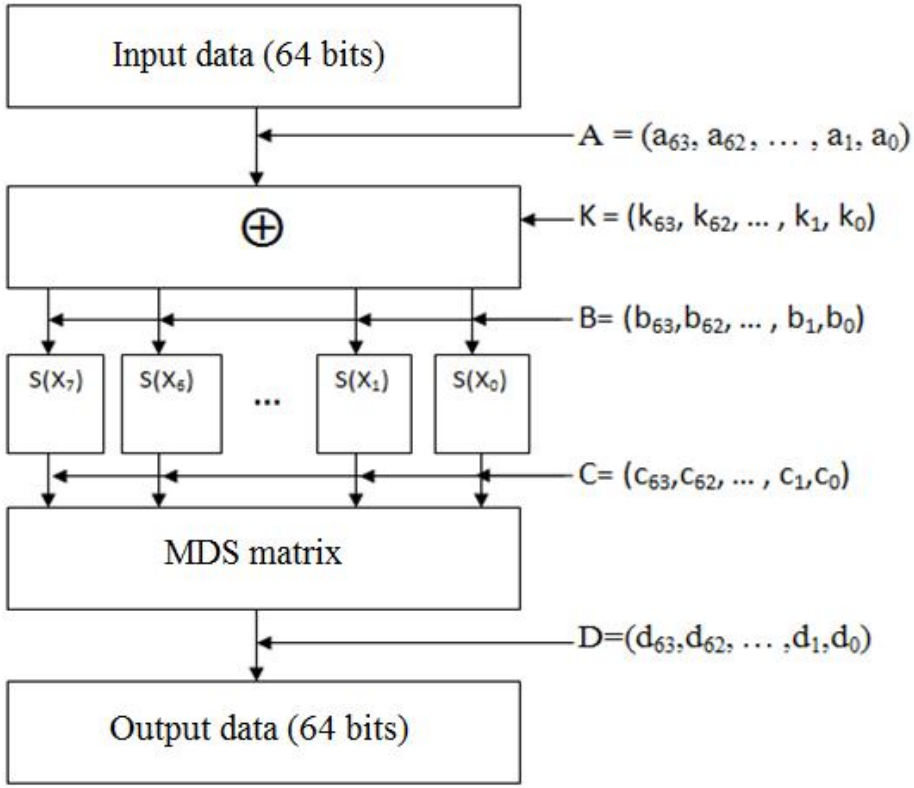
Properties of “Mukhomor”



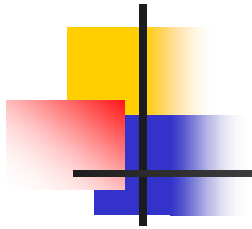
- High speed of encryption and decryption (~125% of AES)
- Small security margin of the cipher
- Random S-boxes optimized against DC, LC and algebraic analysis
- Good key agility properties (key schedule takes less time than one encryption)
- New construction of key schedule

Symmetric block cipher “Labirynth”





Properties of “Labirynth”



- Classical Feistel cipher
- AES elements in the round function
- Nyberg construction of the S-box
- Good security margin for DC and LC
- Rather good speed characteristics (~75% of AES)
- Potentially vulnerable to algebraic attack

Symmetric block cipher ADE

$$ADE_{K_0} = s_{K_{10}} \circ p_{K_{10}} \circ g_{K_{10}} \circ s_{K_9} \circ \prod_{i=0}^{8} \left(q_{K_i} \circ p_{K_i} \circ g_{K_i} \circ s_{K_i} \right)$$

s_{K_j} – AddRoundKey(State, RoundKey)

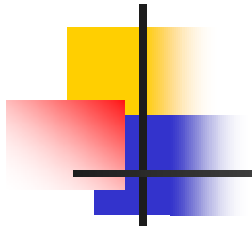
p_{K_j} – ShiftRows(State, RoundKey)

g_{K_j} – ByteSub(State, RoundKey)

q_{K_i} – MixColumn(State, RoundKey)

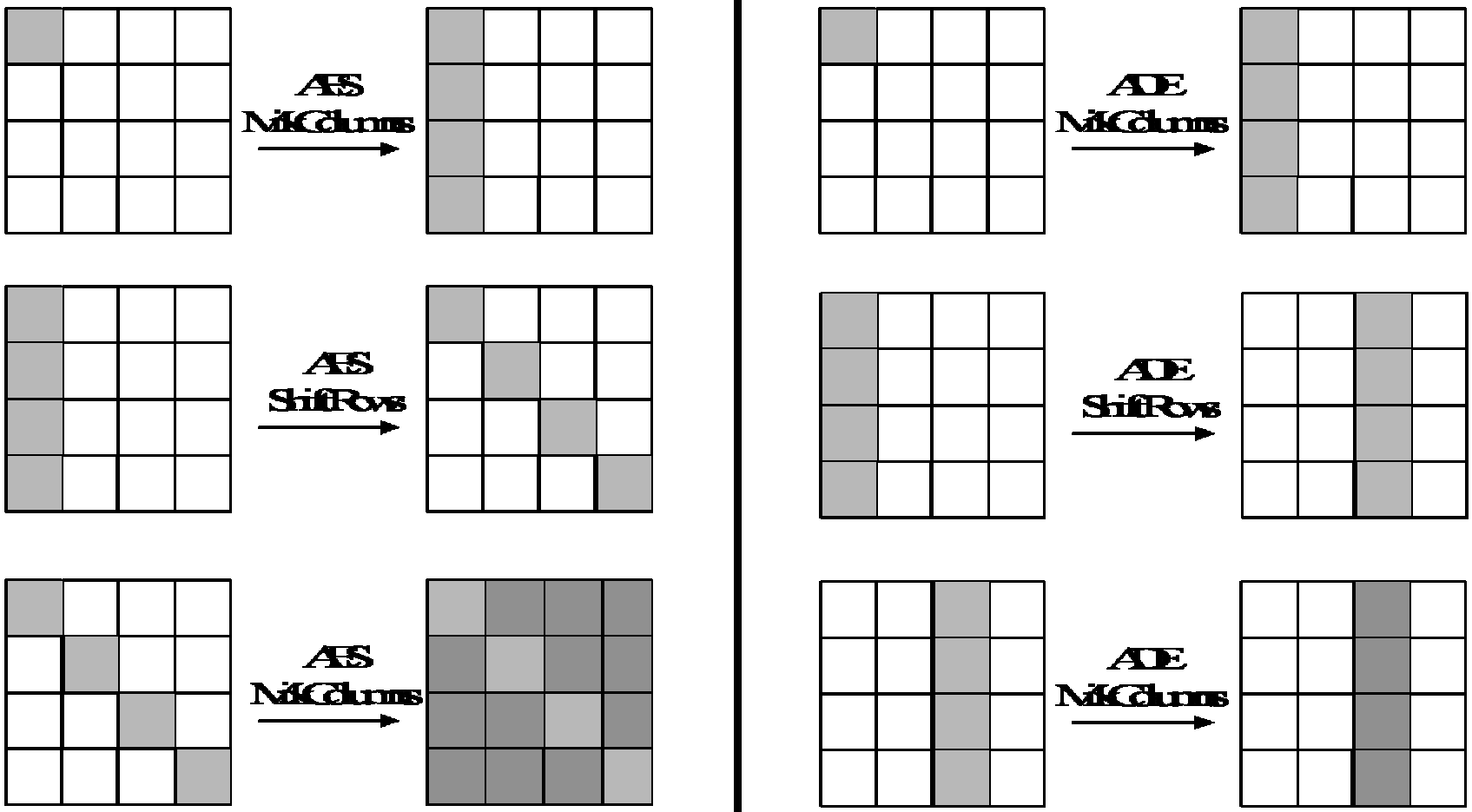
All operations are key-dependent

Properties of ADE



- Rijndael structure of the cipher
- All operations (S-boxes, ShiftRows, MixColumns) are key-dependent
- Good speed characteristics (like AES)
- Large amount of memory for implementation
- Bad key agility properties (key schedule and table precomputaion takes huge time)
- Large class of weak keys is known (on these keys 128-bit cipher is equal to four 32-bit ciphers)

ADE ShiftRows on weak encryption key



Symmetric block cipher “Kalyna”

$$Kalina_{K_M} = c_{K_{N_r+1}} \circ g \circ \prod_{i=1}^{N_r/2} \left(s_{K_{2i}} \circ q \circ p \circ g \circ c_{K_{2i-1}} \circ q \circ p \circ g \right) \circ s_{K_0}$$

s_{K_i} – XorRoundKey(State, K_i)

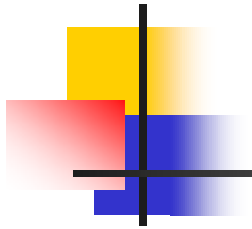
c_{K_i} – AddRoundKey(State, K_i)

p – ShiftRows(State)

g – Kalina_S_boxes(State)

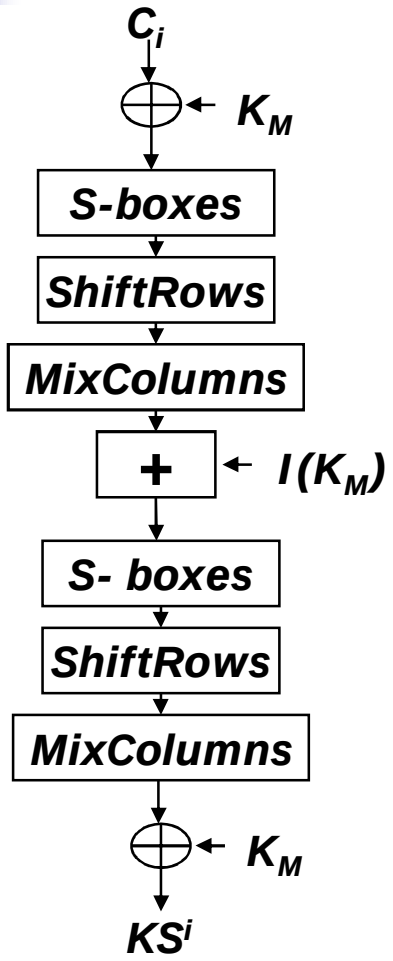
q – MixColumns(State)

Properties of “Kalyna”



- Strength to cryptanalytic attacks and high level of security (main criteria)
- Random S-boxes optimized against DC, LC and algebraic analysis
- Good key agility properties (key schedule takes less time than one encryption)
- New construction of key schedule
- Different speed of encryption (~85% of AES) and decryption (~65% of AES) in ECB mode

Key schedule properties of “Kalyna”



$DC_i = 0$

$DK_M = K_M$ Å K_M’[1] 0

DS_1

DM_1

D_+

DS_2

DM_2

$DKS^i = 0$

$$p\left(\Delta S_1 / \Delta K_M\right) \le \left(\Delta_{\oplus}^{\max}\right)^{wt(\Delta K_M)} < 1 \; on \; \Delta K_M \neq 0$$

$$p\left(\Delta M_1 / \Delta S_1\right) = 1, \;\; wt(\Delta M_1) + wt(\Delta S_1) \ge B_N = 9$$

$$p\left(\Delta + / \Delta M_1\right) \le 1$$

$$p\left(\Delta S_2 / \Delta_+\right) \le \left(\Delta_{\oplus,+}^{\max}\right)^{wt(\Delta_+)} < 1$$

$$p\left(\Delta M_2 / \Delta S_2\right) = 1, \;\; wt(\Delta M_2) + wt(\Delta S_2) \ge B_N = 9$$

Expected probability of most-effective DC attack on key schedule

$$p_{coll}^{KS} \leq p\left(\Delta S_1 / \Delta K_M\right) \cdot p\left(\Delta_+ / \Delta M_1\right) \cdot p\left(\Delta S_2 / \Delta_+\right) \leq \left(\Delta_{\oplus}^{\max}\right)^{wt(\Delta K_M)} \cdot 1 \cdot \left(\Delta_{\oplus,+}^{\max}\right)^{wt(\Delta_+)}$$

$$p_{coll}^{KS} \leq \left(2^{-5}\right)^9 = 2^{-45}$$

$$p_{eq} \leq \left(p_{coll}^{KS}\right)^{N_{KS}} = 2^{-135} << 2^{-128}$$

Implementations of “Kalyna”

- Hardware security module “**Gryada-41**” (**PCI**)

  (Kalyna/GOST/AES encryption, DSTU/DSS/ECDSA/GOST digital signatures, key generation, etc.)

- Network security and **VPN module** “**Gryada-301**”

  (network traffic protection with IPSec using Kalyna/GOST/AES encryption, high-speed cryptographic services for local network)

Implementations of “Kalyna”

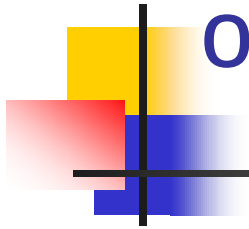
- Hardware security module “**Gryada-61**” (**USB**)

  (Kalyna/GOST/AES encryption, DSTU/DSS/ECDSA/GOST digital signatures, key generation, etc.)

- **USB security token “Crystall-1”**

  (Kalyna/GOST/AES encryption, DSTU/DSS/ECDSA/GOST digital signatures, key generation using physical noise diods, etc.)

Finalists of the second stage of the public cryptographic competition



- “**Kalyna**”
  (high security margin, slower than AES)
- “**Mukhomor**”
  (faster than AES, small security margin)
- “**Labirynth**”
  (slower than AES, potentially vulnerable to algebraic analysis)

Final selection is expected in 2009