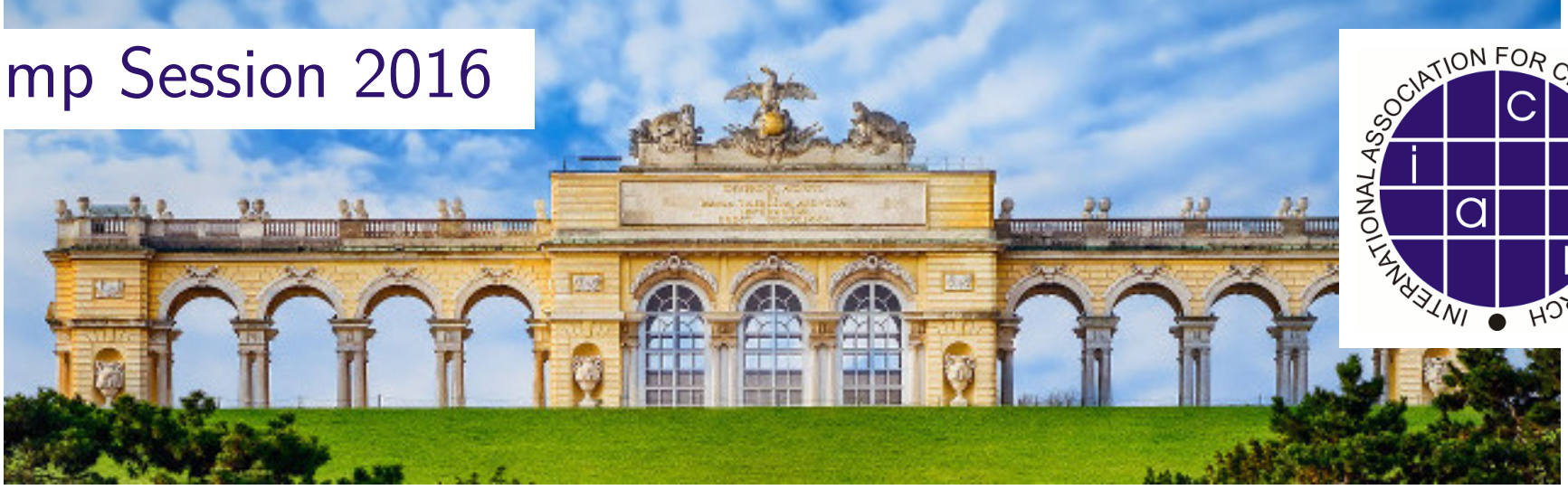
Rump Session 2016



New block Cipher

Anatoly Lebedev; Andrey Karondeev; Alexandre Kozlov

BMSTU

John Nash to NSA

In 1950-es mathematician and Nobel Prize winner John Nash wrote several letters to NSA offering some new ideas of „enciphering algorithms“.

2001. NESSIE

LAN Crypto Ltd. offered a block cipher called NUSH.

The NUSH cipher later was found not secure with respect to linear cryptanalysis.

Change NUSH to NASH

Make round function key-dependent.

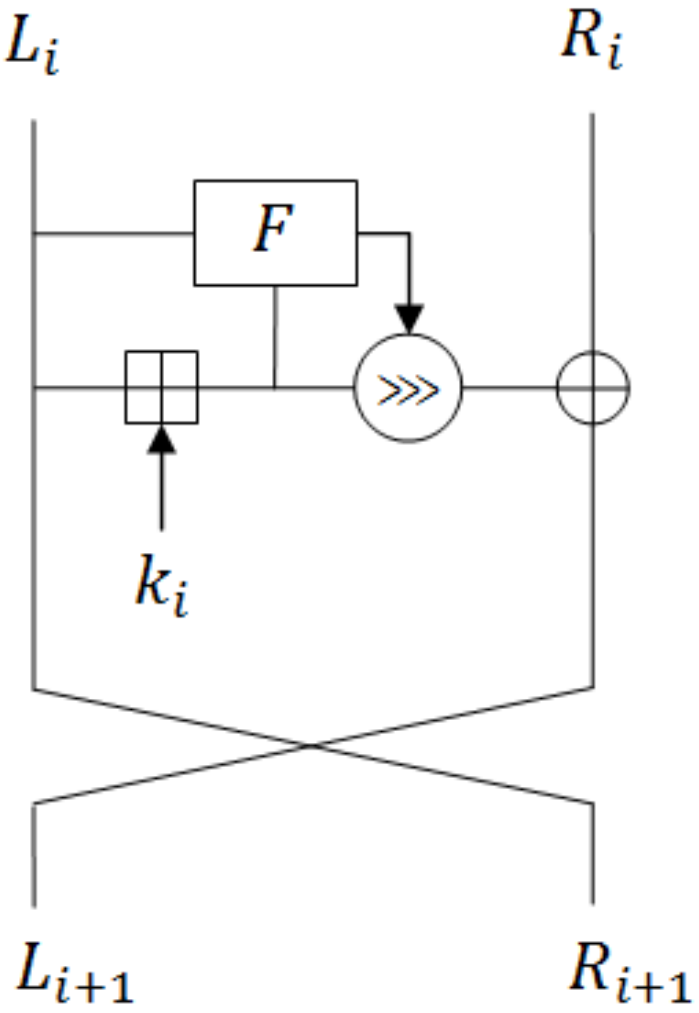
We make round transformations dependent of
an intermediate information block and a key.

Implementation

Variable cyclic rotation.

Cyclic rotations dependent of an information block and a key.

Round Function



Basic Formulas

Addition of a key with an information semiblock (mod 2^n) makes cycle variation function nonlinear:

$$R_{i+1} = L_i$$

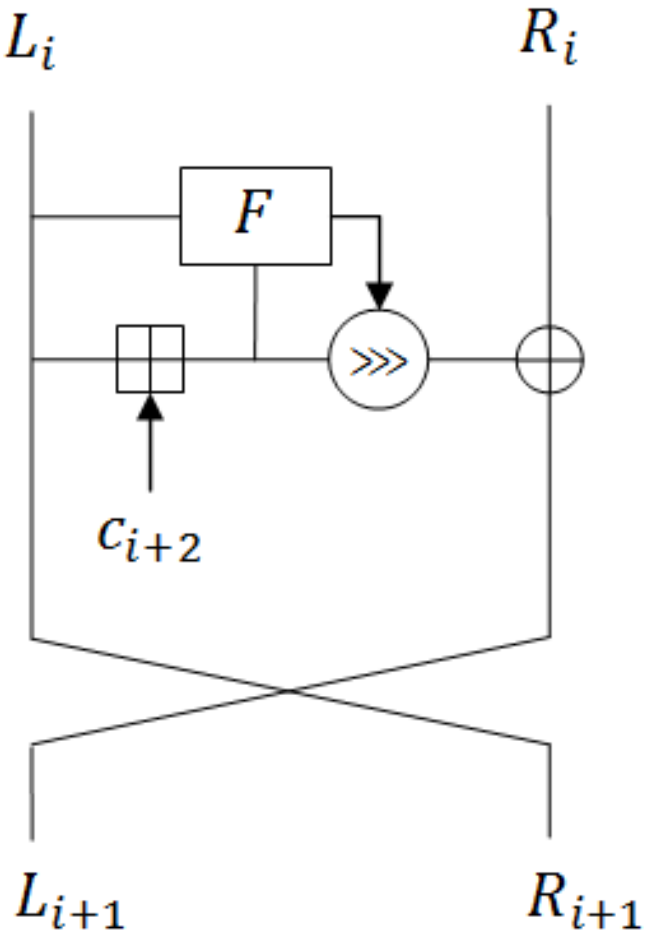
$$L_{i+1} = \left(R_{i+1} \ggg F(L_i, L_i \boxplus k_i)\right) \oplus R_i$$

Variable Cyclic Rotation

Rotations : 11, 14, 10, or 19
for the 64 bit block.

Rotations: 37, 34, 38, or 29
for the 128 bit block.

Key Schedule



Thank you!

Authors:
Anatoly Lebedev, Andrey Karondeev, Alexander Kozlov.
Bauman Moscow State University (RUSSIA)

For requests: lan@lancrypto.com