Problem 6. «Open competition: NSUCRYPTO lightweight cipher»

Problem for a special prize!

NSUCRYPTO team organizes an open competition to develop a new light-weight block cipher. There are some requirements for it.

Block size — 64 bits.
Key size — 80, 96 or 128 bits.
Number of rounds — 32.
Structure — arbitrary. So, SPN, ARX, Feistel schemes can be applied or some new types of the structure can be proposed.

We kindly ask you first to study the well-known light-weight cipher PRESENT (2007). Try to realize what can be done better than in this cipher. Compare your solution with PRESENT: in realization, in cryptanalysis (linear, differential, algebraic, etc.). Give necessary arguments in favor of your decision.