УДК 681.03.245

Е.А. Маро
Южный федеральный университет, г. Таганрог

АЛГЕБРАИЧЕСКИЙ АНАЛИЗ СИММЕТРИЧНОГО БЛОЧНОГО ШИФРА MISTY1

В данной статье рассмотрено применение подходов алгебраического анализа к симметричному блочному шифру MISTY1. Описана структура используемых криптографических преобразований шифра MISTY1, выделены нелинейные преобразования, являющиеся основой описания шифра в виде системы булевых нелинейных уравнений (блоки замены S7 и S9, функция FL), и сформированы соответствующие подсистемы уравнений.

Ключевые слова: алгебраический анализ; симметричные блочные шифры; шифр MISTY1, система булевых нелинейных уравнений.

E.A. Maro
Southern Federal University, Taganrog

ALGEBRAIC ANALYSIS OF THE SYMMETRIC BLOCK CIPHER MISTY1

In this article discusses the application of algebraic analysis approaches to the symmetric block cipher MISTY1. The structure of the used cryptographic transformations of the MISTY1 cipher is described, the nonlinear transformations that are the basis for describing the cipher in form of a system of Boolean nonlinear equations (substitution boxes S7 and S9, FL function) are observed, and the corresponding subsystems of equations are formed.

Keywords: algebraic analysis; symmetric block ciphers; MISTY1 cipher, system of Boolean nonlinear equations.

Шифр MISTY1

Шифр MISTY1 является международным стандартом в соответствии с ISO / IEC 18033-3 [1], а также рекомендуется к применению NESSIE [2]. Подробное описание шифра дано в RFC 2994 [3]. Шифр MISTY1 представляет собой итерационный блочный шифр, построенный по схеме сети Фейстеля (рис. 1).

Длина блока текста составляет 64 бита, длина ключа 128 бит. Минимальное рекомендуемое число раундов шифрования составляет 8 раундов.

Шифр MISTY1 содержит следующие преобразования:

Функция FL – на основе структуры сети Фейстеля выполняет над двумя 16-битовыми блоками операции сложения по модулю 2 и побитные логические операции «И» и «ИЛИ» с раундовыми ключами.

Функция FO – на основе структуры сети Фейстеля выполняет над двумя 16-битовыми блоками операции сложения по модулю 2 с раундовыми ключами и функцией FI.

Функция FI – на основе несбалансированной структуры сети Фейстеля выполняет над 9-битным и 7-битным блоками операции замены по таблицам S9 и S7 соответственно. Структура замен S9 и S7 приведена в Таблице 1.

Преобразования входных блоков функциями FL, FO и FI приведены на рисунке 2.

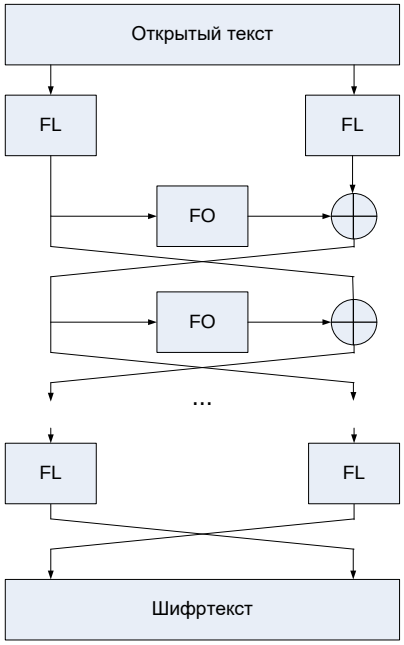

Рисунок 1 – Структура шифра MYSTY1.

Таблица 1 – Структура замен в блоках S7 и S9

S7	27, 50, 51, 90, 59, 16, 23, 84, 91, 26, 114, 115, 107, 44, 102, 73, 31, 36, 19, 108, 55, 46, 63, 74, 93, 15, 64, 86, 37, 81, 28, 4, 11, 70, 32, 13, 123, 53, 68, 66, 43, 30, 65, 20, 75, 121, 21, 111, 14, 85, 9, 54, 116, 12, 103, 83, 40, 10, 126, 56, 2, 7, 96, 41, 25, 18, 101, 47, 48, 57, 8, 104, 95, 120, 42, 76, 100, 69, 117, 61, 89, 72, 3, 87, 124, 79, 98, 60, 29, 33, 94, 39, 106, 112, 77, 58, 1, 109, 110, 99, 24, 119, 35, 5, 38, 118, 0, 49, 45, 122, 127, 97, 80, 34, 17, 6, 71, 22, 82, 78, 113, 62, 105, 67, 52, 92, 88, 125
S9	451, 203, 339, 415, 483, 233, 251, 53, 385, 185, 279, 491, 307, 9, 45, 211, 199, 330, 55, 126, 235, 356, 403, 472, 163, 286, 85, 44, 29, 418, 355, 280, 331, 338, 466, 15, 43, 48, 314, 229, 273, 312, 398, 99, 227, 200, 500, 27, 1, 157, 248, 416, 365, 499, 28, 326, 125, 209, 130, 490, 387, 301, 244, 414, 467, 221, 482, 296, 480, 236, 89, 145, 17, 303, 38, 220, 176, 396, 271, 503, 231, 364, 182, 249, 216, 337, 257, 332, 259, 184, 340, 299, 430, 23, 113, 12, 71, 88, 127, 420, 308, 297, 132, 349, 413, 434, 419, 72, 124, 81, 458, 35, 317, 423, 357, 59, 66, 218, 402, 206, 193, 107, 159, 497, 300, 388, 250, 406, 481, 361, 381, 49, 384, 266, 148, 474, 390, 318, 284, 96, 373, 463, 103, 281, 101, 104, 153, 336, 8, 7, 380, 183, 36, 25, 222, 295, 219, 228, 425, 82, 265, 144, 412, 449, 40, 435, 309, 362, 374, 223, 485, 392, 197, 366, 478, 433, 195, 479, 54, 238, 494, 240, 147, 73, 154, 438, 105, 129, 293, 11, 94, 180, 329, 455, 372, 62, 315, 439, 142, 454, 174, 16, 149, 495, 78, 242, 509, 133, 253, 246, 160, 367, 131, 138, 342, 155, 316, 263, 359, 152, 464, 489, 3, 510, 189, 290, 137, 210, 399, 18, 51, 106, 322, 237, 368, 283, 226, 335, 344, 305, 327, 93, 275, 461, 121, 353, 421, 377, 158, 436, 204, 34, 306, 26, 232, 4, 391, 493, 407, 57, 447, 471, 39, 395, 198, 156, 208, 334, 108, 52, 498, 110, 202, 37, 186, 401, 254, 19, 262, 47, 429, 370, 475, 192, 267, 470, 245, 492, 269, 118, 276, 427, 117, 268, 484, 345, 84, 287, 75, 196, 446, 247, 41, 164, 14, 496, 119, 77, 378, 134, 139, 179, 369, 191, 270, 260, 151, 347, 352, 360, 215, 187, 102, 462, 252, 146, 453, 111, 22, 74, 161, 313, 175, 241, 400, 10, 426, 323, 379, 86, 397, 358, 212, 507, 333, 404, 410, 135, 504, 291, 167, 440, 321, 60, 505, 320, 42, 341, 282, 417, 408, 213, 294, 431, 97, 302, 343, 476, 114, 394, 170, 150, 277, 239, 69, 123, 141, 325, 83, 95, 376, 178, 46, 32, 469, 63, 457, 487, 428, 68, 56, 20, 177, 363, 171, 181, 90, 386, 456, 468, 24, 375, 100, 207, 109, 256, 409, 304, 346, 5, 288, 443, 445, 224, 79, 214, 319, 452, 298, 21, 6, 255, 411, 166, 67, 136, 80, 351, 488, 289, 115, 382, 188, 194, 201, 371, 393, 501, 116, 460, 486, 424, 405, 31, 65, 13, 442, 50, 61, 465, 128, 168, 87, 441, 354, 328, 217, 261, 98, 122, 33, 511, 274, 264, 448, 169, 285, 432, 422, 205, 243, 92, 258, 91, 473, 324, 502, 173, 165, 58, 459, 310, 383, 70, 225, 30, 477, 230, 311, 506, 389, 140, 143, 64, 437, 190, 120, 0, 172, 272, 350, 292, 2, 444, 162, 234, 112, 508, 278, 348, 76, 450

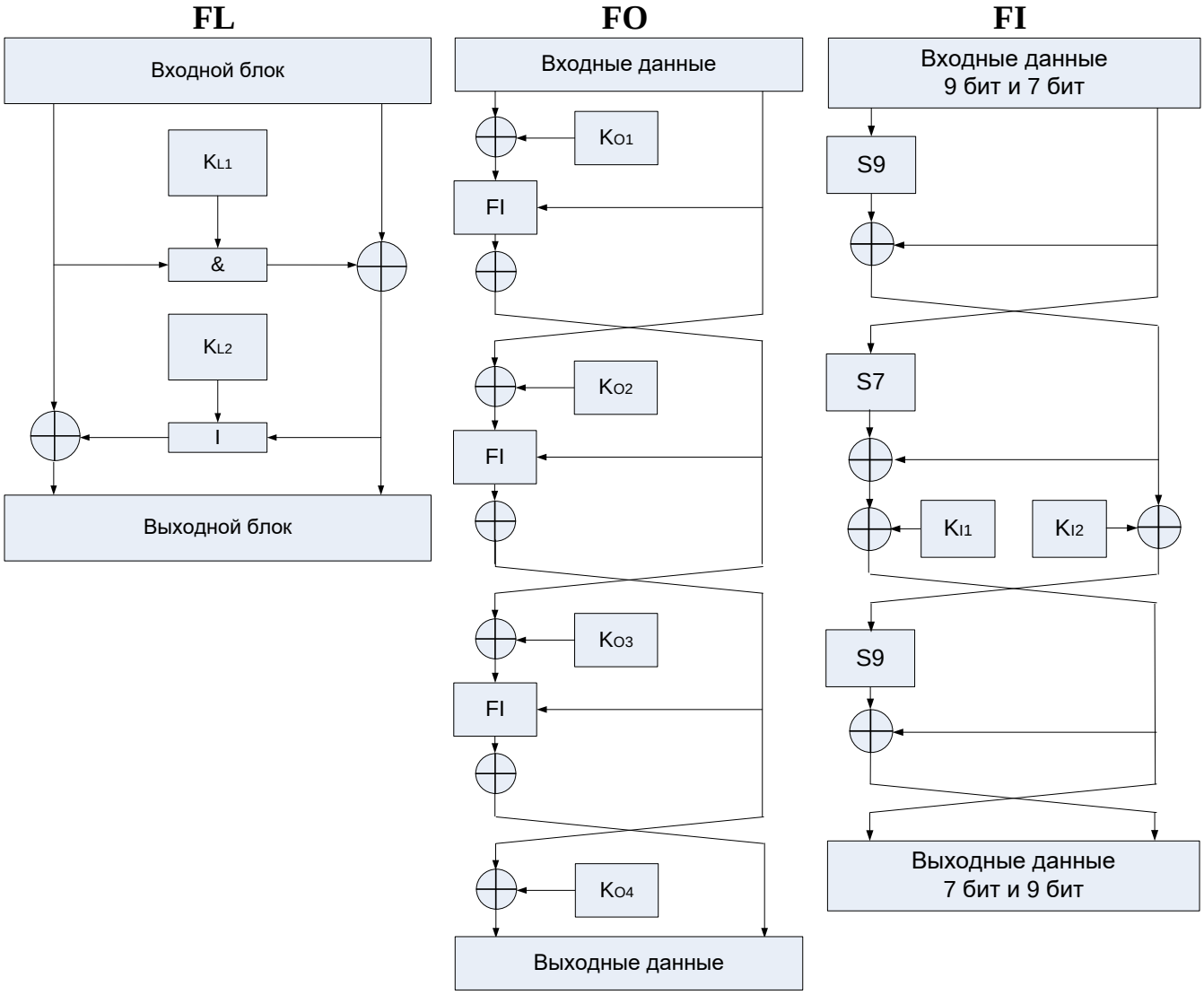

Рисунок 2 – Структура преобразований функций FL, FO и FI шифра MISTY1.

Формирование системы булевых уравнений для шифра MISTY1

Теоретически большинство блочных шифров можно представить в виде уравнения с полиномами высокой степени, также любой шифр можно описать как систему полиномиальных уравнений [4]. Современные блочные шифры предназначены либо для аппаратной реализации, либо для выполнения на компьютерах, поэтому выбор GF(2) в качестве основного поля является очевидным для формирования системы полиномиальных уравнений. Для шифров, использующих S-блоки по различным полям с характеристикой два, таких как семейство шифров MISTY, или шифров с сужающими или расширяющими S-блоками, например DES, запись уравнений над GF(2) – наиболее оптимальный выбор для получения полиномиальной системы, описывающей полный шифр.

Поскольку в ходе алгебраического анализа сложно спрогнозировать сложность поиска решения, то при формировании системы следует исходить из следующих рекомендаций:

1. Максимально сократить общее количество условных обозначений (переменных) с помощью минимизации степени формируемых уравнений и разницы между общим количеством мономов и общим количеством линейно независимых уравнений.
2. Минимизировать размер отдельных уравнений системы.

Основой алгебраического анализа является описание нелинейных преобразований шифра в виде системы булевых нелинейных уравнений. Как видно из структуры шифра MISTY1, системы могут быть сформированы для преобразований замены S7 и S9. На основе известных таблиц замен были составлены уравнения в алгебраической нормальной форме (АНФ), описывающие данные преобразования.

Преобразование S7 может быть описано в АНФ следующим образом (1):

y0 =x0⊕x1x3⊕x0x3x4⊕x1x5⊕x0x2x5⊕x4x5⊕x0x1x6⊕x2x6⊕x0x5x6⊕x3x5x6⊕1,
y1 =x0x2⊕x0x4⊕x3x4⊕x1x5⊕x2x4x5⊕x6⊕x0x6⊕x3x6⊕x2x3x6⊕x1x4x6⊕x0x5x6⊕1,
y2 =x1x2⊕x0x2x3⊕x4⊕x1x4⊕x0x1x4⊕x0x5⊕x0x4x5⊕x3x4x5⊕x1x6⊕x3x6⊕x0x3x6⊕x4x6⊕x2x4x6,
y3 =x0⊕x1⊕x0x1x2⊕x0x3⊕x2x4⊕x1x4x5⊕x2x6⊕x1x3x6⊕x0x4x6⊕x5x6⊕1, (1)
y4 =x2x3⊕x0x4⊕x1x3x4⊕x5⊕x2x5⊕x1x2x5⊕x0x3x5⊕x1x6⊕x1x5x6⊕x4x5x6⊕1,
y5 =x0⊕x1⊕x2⊕x0x1x2⊕x0x3⊕x1x2x3⊕x1x4⊕x0x2x4⊕x0x5⊕x0x1x5⊕x3x5⊕x0x6⊕x2x5x6,
y6 =x0x1⊕x3⊕x0x3⊕x2x3x4⊕x0x5⊕x2x5⊕x3x5⊕x1x3x5⊕x1x6⊕x1x2x6⊕x0x3x6⊕x4x6⊕x2x5x6.

Преобразование S9 может быть описано в АНФ следующим образом:

y0 =x0x4⊕x0x5⊕x1x5⊕x1x6⊕x2x6⊕x2x7⊕x3x7⊕x3x8⊕x4x8⊕1,
y1 =x0x2⊕x3⊕x1x3⊕x2x3⊕x3x4⊕x4x5⊕x0x6⊕x2x6⊕x7⊕x0x8⊕x3x8⊕x5x8⊕1,
y2 =x0x1⊕x1x3⊕x4⊕x0x4⊕x2x4⊕x3x4⊕x4x5⊕x0x6⊕x5x6⊕x1x7⊕x3x7⊕x8,
y3 =x0⊕x1x2⊕x2x4⊕x5⊕x1x5⊕x3x5⊕x4x5⊕x5x6⊕x1x7⊕x6x7⊕x2x8⊕x4x8,
y4 =x1⊕x0x3⊕x2x3⊕x0x5⊕x3x5⊕x6⊕x2x6⊕x4x6⊕x5x6⊕x6x7⊕x2x8⊕x7x8, (2)
y5 =x2⊕x0x3⊕x1x4⊕x3x4⊕x1x6⊕x4x6⊕x7⊕x3x7⊕x5x7⊕x6x7⊕x0x8⊕x7x8,
y6 =x0x1⊕x3⊕x1x4⊕x2x5⊕x4x5⊕x2x7⊕x5x7⊕x8⊕x0x8⊕x4x8⊕x6x8⊕x7x8⊕1,
y7 =x1⊕x0x1⊕x1x2⊕x2x3⊕x0x4⊕x5⊕x1x6⊕x3x6⊕x0x7⊕x4x7⊕x6x7⊕x1x8⊕1,
y8 =x0⊕x0x1⊕x1x2⊕x4⊕x0x5⊕x2x5⊕x3x6⊕x5x6⊕x0x7⊕x0x8⊕x3x8⊕x6x8⊕1.

Шифр MISTY1 содержит дополнительный нелинейный компонент - FL функцию. Выходные значения Y_L и Y_R функции FL являются функциями от входного слова X и ключевого слова K, определяемые формулой (3):

$$Y_R = X_R \oplus (X_L \cap K_L)$$
$$Y_L = X_L \oplus (Y_R \cup K_R) \quad (3)$$

Приведенное выше определение можно напрямую перевести в систему квадратичных уравнений в GF(2), как показано в формуле (4):

$$y_{R,i} = x_{R,i} + y_{L,i} \cdot k_{L,i}$$
$$y_{L,i} = x_{L,i} + y_{R,i} + k_{R,i} + y_{R,i} \cdot k_{R,i} \quad (4)$$

где $i \in [0, 32)$.

Таким образом, для функции FL получено 64 нелинейных уравнений, содержащих 192 линейных и 64 квадратичных одночленов.

Один раунд шифра MISTY1 может быть описан с помощью 203 булевых нелинейных уравнений и 112 битов раундовых ключей K_{L1}, K_{L2}, K_{O1}, K_{O2}, K_{O3}, K_{O4}, K_{I1}, K_{I2}

Список литературы

1. ISO/IEC: JTC1: ISO/IEC 18033, Security techniques—encryption algorithms—part 3: block ciphers (2005)
2. NESSIE: New European schemes for signatures, integrity, and encryption (2004). https://www.cosic.esat.kuleuven.be/nessie/
3. H. Ohta, M. Matsui, A description of the MISTY1 encryption algorithm (2000). https://tools.ietf.org/html/rfc2994
4. Carlos Cid, Martin Albrecht, Daniel Augot, Anne Canteaut, Ralf-Philipp Weinmann. D.STVL.7 -Algebraic cryptanalysis of symmetric primitives. 2008. hal-00328626

Сведения об авторах

Маро Екатерина Александровна – кандидат технических наук, доцент кафедры «Безопасности информационных технологий», Южный федеральный университет, Таганрог, email: eamaro@sfedu.ru

About the authors

Maro Ekaterina Aleksandrovna – PhD, Associate Professor of the Department of Information Security, Southern Federal University, Taganrog, email: eamaro@sfedu.ru