иерархию доступа. Предложены также конструкции линейных ПМРС с МС над примарными кольцами вычетов, для которых выполняются полученные условия (утверждения 1 – 3).

Применение оптимальных протоколов разделения секрета при построении подсистем управления доступом современных информационно-телекоммуникационных систем позволит повысить надежностные и эксплуатационные характеристики данных систем, а, значит, и уровень защищенности информации в таких системах в целом [5, 6].

Литература: ***1.*** *НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.* ***2.*** *ISO/IEC 15408:2000 – Information technologies – Security techniques – Evaluation criteria for IT security.* ***3.*** *НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.* ***4.*** *McLean J. Reasoning about security models // Proceeding IEEE Symposium on privacy and security. – IEEE Computer Society Press. – 1987. – P. 123-131.* ***5.*** *Zhu B. B., Feng M., Li S. An efficient key scheme for layered access control of MPEG-4 FGS Video // ICME. – 2004. – P. 443 – 446.* ***6.*** *Wu J., Wei R. An access control scheme for partially ordered set hierarchy with probable security // Cryptology ePrint Archive. – Report. – 2004/295.* ***7.*** *Sklavos N., Koufopavlou O. Access control in network hierarchy: implementation of key management protocol // International Journal of Network Security. – 2005. – Vol.1. – № 2. – P.103 – 109.* ***8.*** *Алексейчук А. Н., Волошин А. Л. Схема разделения нескольких секретов с многоадресным сообщением на основе линейных преобразований над кольцом вычетов по модулю m // Реєстрація, зберігання і обробка даних. – 2006. – Т. 8. – № 1. – С. 92 – 102.* ***9.*** *Алексейчук А. Н., Волошин А. Л. Аналитическое описание конструкций протоколов множественного разделения секрета с многоадресным сообщением, реализующих заданную иерархию доступа // Прикладная радиоэлектроника. – 2007. – Т. 6. – № 3. – С. 391 – 396.* ***10.*** *Волошин А. Л. Метод построения совершенных протоколов множественного разделения секрета с многоадресным сообщением, реализующих семейства иерархий доступа, для подсистем управления доступом информационно-телекоммуникационных систем // Захист інформації. – 2007. – № 3. – С.88 – 94.* ***11.*** *Brickell E. F. Some ideal secret sharing schemes // J. Combin. Math. and Combin. Comput. – 1989. – № 9. – P. 105 – 113.* ***12.*** *Van Dijk M. A linear construction of perfect secret sharing schemes // Advances in Cryptology – EUROCRYPT'94. – Lecture Notes in Comput. Science. – V. 950. – P. 23 – 34.* ***13.*** *Ashikhmin A., Barg A. Minimal vectors in linear codes // IEEE Trans. on Inform. Theory. – 1998. – V. 5. – P. 2010 – 2018.* ***14.*** *Blundo C., Cresti A., de Santis A., Vaccaro U. Fully dynamic secret sharing schemes // Advances in Cryptology – CRYPTO'93. – Proceedings. – Springer Verlag, 1994. – P. 110 –125.* ***15.*** *Brickell E. F., Davenport D. M. On the classification of ideal secret sharing schemes // J. Cryptology. – 1991. – № 4. – P. 123 – 134.* ***16.*** *Блейкли Р. Г., Кабатянский Г. А. Обобщенные идеальные схемы, разделяющие секрет, и матроиды // Проблемы передачи информации. – 1997. – Т. 33. – Вып. 3. – С. 102 – 110.* ***17.*** *Лидл Р., Нидеррайтер Г. Конечные поля: В 2 т. / Пер. с англ. – М.: Мир, 1988. – 818 с.*

УДК 621.391:519.2

КАСКАДНА СХЕМА ФЕЙСТЕЛЯ ТА ЇЇ СТІЙКІСТЬ ДО ДИФЕРЕНЦІАЛЬНОГО ТА ЛІНІЙНОГО КРИПТОАНАЛІЗУ

Сергій Яковлєв
Фізико-технічний інститут НТУУ "КПІ"

Анотація: **Запропоновано та проаналізовано нову конструкцію блочних шифрів – каскадну схему Фейстеля, виведені оцінки її стійкості до диференціального та лінійного криптоаналізу.**

Summary: **New construction of block ciphers' design, a cascade Feistel network, is proposed and analysed, its resistance to differential and linear cryptanalysis is evaluated.**

Ключові слова: **Блочний шифр, схема Фейстеля, диференціальний криптоаналіз, лінійний криптоаналіз.**

І Вступ

Запропонована ще у 1971 році схема Фейстеля [1] – один з найпоширеніших в наш час варіантів побудови блочних шифрів. Проста для криптоаналізу та зручна в реалізації схема Фейстеля лягла в основу таких відомих алгоритмів, як DES, Blowfish та ГОСТ 28147-89.

Однією з властивостей схеми є те, що за один раунд обробляється лише половина блоку даних; наприклад, для 64-бітового блоку за раунд обробляється тільки 32 біти. Це дозволяло ефективно

реалізовувати алгоритми на 32-бітній архітектурі. В наш час, однак, розвиток так званих tradeoff-атак ставить під сумнів стійкість блочних шифрів із блоком у 64 біти; рекомендації проекту NESSIE визначають як прийнятний блок у 128 біт. Для таких алгоритмів раундова функція схеми Фейстеля має обробляти по 64 біти, що наразі не завжди можно виконати ефективно.

В даній роботі запропоновано підхід, що дозволяє зберегти ефективність реалізації алгоритмів на архітектурах невеликої розрядності та не зменшити криптостійкість до диференціального та лінійного криптоаналізу, – каскадна схема Фейстеля. Ідея полягає у використанні в схемі Фейстеля як раундової функції іншої схеми Фейстеля вдвічі меншої розмірності. Ми покажемо, що запропонована нами конструкція є марківським шифром за деяких умов; також ми виведемо оцінки для диференціальних та лінійних характеристик побудованого каскаду.

Зауважимо, що схожі ідеї використовувались при побудові алгоритмів блочного шифрування MISTY1 та SEED: кожен з них використовує спеціально підібрані трираундові перетворення як раундові функції. В той же час розробники цих алгоритмів не використовували всі властивості, що притаманні схемам Фейстеля, при оцінці стійкості своїх алгоритмів (оцінка проводилась безпосередніми обчисленнями [2, 3]), акцентуючи в першу чергу на зручності реалізації.

II Опис каскадної схеми Фейстеля

Розглянемо блок m_i довжини $2n$ біт та відповідний йому ключ k_i (зазвичай довжини n біт, але необов'язково). *Раундовим перетворенням* назвемо перетворення вигляду:

$$m_{i+1} = (x_{i+1}, y_{i+1}) = \varphi(x_i, y_i) = x_i \oplus f(y_i, k_i), x_i),$$

де функція $f : V_n \times V_n \to V_n$ називається *раундовою функцією*, V_n – простір n-бітових векторів.

Схема Фейстеля із r раундів – це перетворення

$$F(m_0, k_0, r) = (y_r, x_r),$$

тобто послідовність з r раундових перетворень над блоком m_0 та фінальної перестановки половин блоку m_r. Відповідні раундові ключі k_i одержують із початкового ключа k_0 за допомогою деякої процедури K: $k_i = K(k_0, i)$; процедура K може бути довільною, що продукує раундові ключі, близькі до випадкових.

Нехай у нас є схема Фейстеля F із r_{in} раундів, що обробляє блоки довжиною $2n$ біт.

Каскадна схема Фейстеля із r_{out} раундів – це перетворення вхідного блоку $m = (u, v)$ довжини $4n$ біт (u та v – довжини $2n$ біт) та початкового ключа k_0 вигляду:

$$\Phi(m, k_0, r_{out}) = (v_r, u_r),$$

де кожне раундове перетворення має такий вид:

$$m_{i+1} = (u_{i+1}, v_{i+1}) = \psi(u_i, v_i) = (u_i \oplus F(v_i \oplus k'_i, k_i, r_{in}), u_i),$$

відповідні раундові ключі k_i потрібної довжини, які одержують із початкового ключа k_0 за допомогою деякої процедури K: $k_i = K(k_0, i)$, а раундові ключі k'_i довжини $2n$ біт – за допомогою деякої процедури K': $k'_i = K'(k_0, i)$.

Схему F будемо називати *опорною* для каскадної схеми Ф.

Наведемо очевидні властивості каскадної схеми Фейстеля Ф:

1) каскадна схема Фейстеля може розглядатись як звичайна схема Фейстеля – це випливає із структури раундового перетворення; таким чином, можна будувати каскадні схеми ще більшої розмірності, використовуючи Ф як опорну схему;

2) для зручності опису каскадна схема Фейстеля вимагає дві серії раундових ключів; однак можна розглядати пару (k_i, k'_i) як єдиний раундовий ключ з двох частин;

3) уся обчислювальна складність каскадної схеми Ф припадає на раундову функцію f опорної схеми F; усі інші використовувані операції (додавання за модулем 2 та swap) не несуть значного обчислюваного навантаження.

В наступних розділах ми покажемо, як оцінювати стійкість каскадної схеми до диференціального та лінійного криптоаналізу.

III Диференціальна характеристика каскадної схеми Фейстеля

Диференціал функції f – це пара ненульових бітових векторів (a,b) таких, що для деяких бітових векторів *m* виконується співвідношення: $f(m \oplus a) = f(m) \oplus b$.

Ймовірність диференціала функції f – це величина

$$d_f(a,b) = 2^{-n} \sum_{m \in V_n} d_f(a,b,m) = 2^{-n} \sum_{m \in V_n} I\{f(m \oplus a) = f(m) \oplus b\},$$

де *n* – розмірність входу функції *f*, *I*{.} – індикатор, що дорівнює 1, якщо записана умова виконується, та 0, якщо не виконується.

Також введемо позначення

$$D_f = \max_{(a,b)}(d_f(a,b)).$$

Диференціальна характеристика r-раундової схеми Фейстеля F – вектор $(a_0, a_1, ..., a_r)$, де (a_0, a_1) є диференціалом першого раундового перетворення, (a_1, a_2) – диференціалом другого раундового перетворення тощо. Ймовірність виникнення диференціальної характеристики будемо позначати через $d_F(a_0, a_1, ..., a_r)$.

Стійкість схеми Фейстеля *F* до диференціального аналізу визначається ймовірністю

$$D_F = \max_{(a_0, a_1, ..., a_r)}(d_F(a_0, a_1, ..., a_r)).$$

Якщо ця ймовірність дорівнює *p*, то криптоаналітику потрібно накопичити $O(p^{-2})$ пар "відкритий текст – шифртекст" для проведення атаки; тому чим менше максимальна ймовірність виникнення диференціальної характеристики, тим стійкіший алгоритм. В наш час при практичному застосуванні вважається, що при $D_F \le 2^{-80}$ шифр є практично стійким до диференціального аналізу.

Детальніше із теоретичними підходами можна ознайомитись у [4, 6, 7].

Покажемо, як оцінюється стійкість запропонованої схеми Фейстеля до диференціального криптоаналізу.

Обчислимо ймовірність диференціала раундового перетворення ψ каскадної схеми Фейстеля. Ми вважаємо, що *m*, *a*, *b* мають довжину 4*n* біт та розглядаються як пари із двох частин по 2*n* біт кожна: $m = (u, v)$, $a = (a_1, a_2)$, $b = (b_1, b_2)$. Також ми для зручності вважаємо, що ключ *k* також має довжину 2*n* біт (нижче буде показано, що це несуттєво).

За цих умов ймовірність диференціала ψ обчислюється так:

$$d_\psi(a,b) = 2^{-2n} \sum_{u \in V_{2n}} 2^{-2n} \sum_{v \in V_{2n}} 2^{-2n} \sum_{k \in V_{2n}} 2^{-2n} \sum_{k' \in V_{2n}} I\{\psi(u \oplus a_1, v \oplus a_2) = \psi(u,v) \oplus b\}.$$

Розлянемо індикатор окремо:

$$I\{\psi(u \oplus a_1, v \oplus a_2) = \psi(u,v) \oplus b\} =$$
$$= I\{(u \oplus a_1 \oplus F(v \oplus a_2 \oplus k', k, r_{in}), u \oplus a_1) = (u \oplus F(v \oplus k', k, r_{in}) \oplus b_1, u \oplus b_2)\}.$$

Якщо $a_1 \ne b_2$, то умова в дужках ніколи не виконується, а тому індикатор дорівнює нулю; надалі будемо вважати, що $a_1 = b_2$. Тоді другі частини векторів будуть рівні, а індикатор матиме такий вигляд:

$$I\{F(v \oplus a_2 \oplus k', k, r_{in}) = F(v \oplus k', k, r_{in}) \oplus b_1 \oplus b_2\}.$$

Отже,

$$d_\psi(a,b) = 2^{-2n} \sum_{u \in V_{2n}} 2^{-2n} \sum_{v \in V_{2n}} 2^{-2n} \sum_{k \in V_{2n}} 2^{-2n} \sum_{k' \in V_{2n}} I\{F(v \oplus a_2 \oplus k', k, r_{in}) = F(v \oplus k', k, r_{in}) \oplus b_1 \oplus b_2\} =$$
$$= 2^{-2n} \sum_{v \in V_{2n}} 2^{-2n} \sum_{k \in V_{2n}} 2^{-2n} \sum_{k' \in V_{2n}} I\{F(v \oplus a_2 \oplus k', k, r_{in}) = F(v \oplus k', k, r_{in}) \oplus b_1 \oplus b_2\}.$$

Якщо зафіксувати довільне значення k', то $v \oplus k'$ буде приймати всі можливі значення при сумуванні за *v*. Отже, якщо ввести нову змінну $k'' = v \oplus k'$, то шукана ймовірність набуде вигляду:

$$d_\psi(a,b) = 2^{-2n} \sum_{k \in V_{2n}} 2^{-2n} \sum_{k'' \in V_{2n}} I\{F(a_2 \oplus k'', k, r_{in}) = F(k'', k, r_{in}) \oplus b_1 \oplus b_2\} = d_F(a_2, b_1 \oplus b_2).$$

Отже, ймовірність диференціала раундового перетворення каскадної схеми Фейстеля обчислюється через ймовірність диференціала опорної схеми *F*.

Нагадаємо, що шифр називається *марківським*, якщо ймовірності його диференціалів приймають значення, що залежать лише від *a* та *b* і не залежать від вхідних даних.

Лема 1. Якщо опорна схема *F* є марківським шифром, то каскадна схема Ф також є марківським шифром.

Дійсно, якщо ймовірності диференціалів $d_F(.,.)$ не залежать від вхідних даних, то й ймовірності диференціалів $d_\psi(.,.)$ від них не залежать, а тому не залежить і ймовірність будь-якої диференціальної характеристики схеми Ф.

Лема 2. Якщо Ф є марківським шифром, то справедлива така оцінка:

$$D_\Phi \le \left(D_f\right)^{r_{in} \cdot r_{out}}$$

Дійсно, для схеми Фейстеля *F* із раундовою функцією *f* та кількістю раундів *r*, за умови, що *F* – марківський шифр, справедлива оцінка: $D_F \le \left(D_f\right)^r$.

В нашому випадку каскадна схема Ф та опорна схема *F* обидві є марківськими, тому маємо: $D_\Phi \le \left(D_\psi\right)^{r_{out}} = \left(D_F\right)^{r_{out}} \le \left(D_f\right)^{r_{in} \cdot r_{out}}$.

Таким чином, за умови, що опорна схема *F* є марківським шифром, ймовірність диференціальної характеристики каскадної схеми Ф обчислюються через ймовірність диференціала раундової функції *f*, що має вчетверо меншу розмірність; оцінити таку величину простіше навіть при безпосередньому обчисленні порівняно зі звичайною схемою Фейстеля тієї ж розмірності, що й Ф.

Якщо опорна схема *F* не є марківським шифром, то питання оцінки ймовірності диференціальної характеристики Ф поки що залишається відкритим. З іншого боку, для того, щоб *F* була марківським шифром, достатньо, щоб раундова функція *f* мала вигляд: $f(x,k) = g(x \oplus k)$, де *g* – деяка (нелінійна) функція.

IV Лінійна характеристика каскадної схеми Фейстеля

Лінійна структура функції f – це пара ненульових бітових векторів (a,b) таких, що для деяких бітових векторів *m* виконується співвідношення: $am = bf(m)$ (тут *am* – скалярний добуток векторів).

Ймовірність лінійної структури функції f – це величина

$$l_f(a,b) = \left|0.5 - 2^{-n} \sum_{m \in V_n} l_f(a,b,m)\right| = \left|0.5 - 2^{-n} \sum_{m \in V_n} I\{am = bf(m)\}\right|,$$

де *n* – розмірність входу функції *f*.

Зауважимо окремо, що має місце рівність:

$$l_f(a,b) = \left|0.5 - 2^{-n} \sum_{m \in V_n} I\{am \ne bf(m)\}\right|,$$

тобто значення ймовірності лінійної структури збережеться, якщо індикатор замінити на протилежний йому.

Також введемо позначення

$$L_f = \max_{(a,b)}(l_f(a,b)).$$

Лінійна характеристика r-раундової схеми Фейстеля F – вектор $(a_0, a_1, ..., a_r)$, де (a_0, a_1) є лінійною структурою першого раундового перетворення, (a_1, a_2) – лінійною структурою другого раундового перетворення тощо. Ймовірність виникнення лінійної характеристики будемо позначати через $l_F(a_0, a_1, ..., a_r)$.

Аналогічно до диференціального аналізу, стійкість схеми Фейстеля *F* до лінійного аналізу визначається ймовірністю

$$L_F = \max_{(a_0, a_1, ..., a_r)} (l_F(a_0, a_1, ..., a_r)).$$

Якщо ця ймовірність дорівнює *p*, то криптоаналітику потрібно накопичити так само $O(p^{-2})$ пар "відкритий текст – шифртекст" для проведення атаки; тому чим менше максимальна ймовірність виникнення

лінійної характеристики, тим стійкіший алгоритм. В наш час при практичному застосуванні вважається, що при $L_F \le 2^{-80}$ шифр є практично стійким до лінійного аналізу.

Детальніше із теоретичними підходами можна ознайомитись у [5, 6, 7].

Покажемо, як оцінюється стійкість запропонованої схеми Фейстеля до лінійного криптоаналізу.

Обчислимо ймовірність лінійної структури раундового перетворення ψ каскадної схеми Фейстеля. У позначеннях попереднього розділу маємо:

$$l_\psi(a,b) = \left| 0.5 - 2^{-2n} \sum_{u \in V_{2n}} 2^{-2n} \sum_{v \in V_{2n}} 2^{-2n} \sum_{k \in V_{2n}} 2^{-2n} \sum_{k' \in V_{2n}} I\{a_1 u \oplus a_2 v = b_1 (u \oplus F(v \oplus k', k, r_{in})) \oplus b_2 u\} \right|.$$

Розлянемо індикатор окремо:

$$I\{a_1 u \oplus a_2 v = b_1 (u \oplus F(v \oplus k', k, r_{in})) \oplus b_2 u\} =$$
$$= I\{(a_1 \oplus b_1 \oplus b_2) u \oplus a_2 v = b_1 F(v \oplus k', k, r_{in})\}$$

Якщо $a_1 \oplus b_1 \oplus b_2 \ne 0$, то умова індикатора виконуватиметься рівно в половині випадків (буде порівняння двох величин, одна з яких залежить лише від *u*, а інша – від *v*), а тому $l_\psi(a,b)$ буде дорівнювати нулю; надалі будемо вважати, що $a_1 \oplus b_1 \oplus b_2 = 0$. Тоді індикатор матиме такий вигляд:

$$I\{a_2 v = b_1 F(v \oplus k', k, r_{in})\}.$$

Таким чином,

$$l_\psi(a,b) = \left| 0.5 - 2^{-2n} \sum_{u \in V_{2n}} 2^{-2n} \sum_{v \in V_{2n}} 2^{-2n} \sum_{k \in V_{2n}} 2^{-2n} \sum_{k' \in V_{2n}} I\{a_2 v = b_1 F(v \oplus k', k, r_{in})\} \right| =$$

$$= \left| 0.5 - 2^{-2n} \sum_{v \in V_{2n}} 2^{-2n} \sum_{k \in V_{2n}} 2^{-2n} \sum_{k' \in V_{2n}} I\{a_2 v = b_1 F(v \oplus k', k, r_{in})\} \right|.$$

Якщо зафіксувати довільне значення k', то $v \oplus k'$ буде приймати всі можливі значення при сумуванні за *v*. Отже, якщо ввести нову змінну $k'' = v \oplus k'$, то шуканий диференціал набуде вигляду:

$$l_\psi(a,b) = \left| 0.5 - 2^{-2n} \sum_{k' \in V_{2n}} 2^{-2n} \sum_{k \in V_{2n}} 2^{-2n} \sum_{k'' \in V_{2n}} I\{a_2 k'' \oplus a_2 k' = b_1 F(k'', k, r_{in})\} \right| =$$

$$= \left| 2^{-2n} \sum_{k' \in V_{2n}} \left(0.5 - 2^{-2n} \sum_{k \in V_{2n}} 2^{-2n} \sum_{k'' \in V_{2n}} I\{a_2 k'' \oplus a_2 k' = b_1 F(k'', k, r_{in})\} \right) \right| \le$$

$$\le 2^{-2n} \sum_{k' \in V_{2n}} \left| 0.5 - 2^{-2n} \sum_{k \in V_{2n}} 2^{-2n} \sum_{k'' \in V_{2n}} I\{a_2 k'' \oplus a_2 k' = b_1 F(k'', k, r_{in})\} \right|.$$

Для кожного фіксованого значення k' вираз $a_2 k'$ є константою (0 або 1), що або не змінює значення індикатору, або його інвертує. В будь-якому з цих випадків значення підмодульного виразу не змінюється за властивістю ймовірності лінійної структури. Тому:

$$l_\psi(a,b) \le \left| 0.5 - 2^{-2n} \sum_{k \in V_{2n}} 2^{-2n} \sum_{k'' \in V_{2n}} I\{a_2 k'' = b_1 F(k'', k, r_{in})\} \right| = l_F(a_2, b_1).$$

Отже, ймовірність лінійної структури раундового перетворення каскадної схеми Фейстеля оцінюється зверху через ймовірність лінійної структури опорної схеми *F*. За такої оцінки, якщо *F* є марківським шифром, то Ф також є марківським шифром.

Лема 3. Якщо Ф є марківським шифром, то справедлива така оцінка:

$$L_\Phi \le \left(L_f\right)^{r_{in} \cdot r_{out}}.$$

Дійсно, для схеми Фейстеля *F* із раундовою функцією *f* та кількістю раундів *r*, за умови, що *F* – марківський шифр, справедлива оцінка: $L_F \le \left(L_f\right)^r$.

В нашому випадку каскадна схема Ф та опорна схема F обидві є марківськими, тому маємо: $L_{\Phi} \le \left(L_{\psi}\right)^{r_{out}} \le \left(L_F\right)^{r_{out}} \le \left(L_f\right)^{r_{in} \cdot r_{out}}$.

Таким чином, за умови, що опорна схема F є марківським шифром, ймовірність лінійної характеристики каскадної схеми Ф оцінюється зверху через ймовірність лінійної структури раундової функції f, що має вчетверо меншу розмірність.

Якщо опорна схема F не є марківським шифром, то питання оцінки ймовірності лінійних характеристик Ф теж поки що відкрите.

V Висновки

Запропонована нова схема побудови блочних шифрів – каскадна схема Фейстеля. Сформульовані умови, коли наведена конструкція описує марківський шифр, виведені оцінки стійкості до диференціального та лінійного криптоаналізу.

Каскадна схема дозволяє будувати блочні шифри з великою довжиною блоку (наприклад, 128 або 256 біт), обчислювальна складність та криптографічна стійкість яких буде визначатись раундовою функцією опорної схеми, розмірність якої менша в чотири рази, що сприяє ефективній реалізації та спрощує аналіз. Враховуючи бурхливий розвиток обчислювальної техніки та методик tradeoff-атак, ефективність яких залежить лише від довжини блоку та не залежить від внутрішньої структури шифрів, побудова стійких алгоритмів шифрування із великою довжиною блоку та низькою обчислювальною складністю є перспективним для практичного застосування напрямком. Використовуючи запропонований метод можна також збільшувати розмірність існуючих алгоритмів шифрування із збереженням стійкості до лінійного та диференціального криптоаналізу.

Лишається відкритим питання оцінки стійкості каскадної схеми до зазначених криптоаналітичних атак у випадку, коли опорна схема не є марковським шифром. Також цікавим є питання оцінки стійкості до інших відомих атак, зокрема, аналізу неможливих диференціалів та диференціалів високого порядку.

Література: ***1.*** *Хорст Фейстель, Криптография и компьютерная безопасность / пер. А. Винокурова – http://www.enlight.ru/crypto/articles/feistel/feist_i.htm.* ***2.*** *Mitsuru Matsui, Supporting Document of MISTY1 – http://www.cs.utk.edu/~dunigan/cs494-cns01/misty.pdf.* ***3.*** *SEED Algorithm Self Evaluation (Korea Information Security Agency report) - http://www.kisa.or.kr/kisa/seed/down/SEED_Self_Evaluation-English.pdf.* ***4.*** *Lai X., Massey J. L., Murphy S. Markov ciphers and differential cryptanalysis // Advances in Cryptology – EUROCRYPT'91, Proceedings. – Springer Verlag, 1991. – P. 17-38.* ***5.*** *Matsui M. Linear cryptanalysis methods for DES cipher // Advances in Cryptology – EUROCRYPT'93, Proceedings. – Springer Verlag, 1994. – P. 386-397.* ***6.*** *Biryukov A. Block ciphers and stream ciphers: the state of the art – http://eprint.iacr.org/2004/094.* ***7.*** *Jongsung Kim, Combined Differential, Linear and Related-Key Attacks on Block Ciphers and MAC Algorithms – http://eprint.iacr.org/2006/451.*