УДК 004.056.55:519.2+519.688

УТОЧНЕНИЙ МЕТОД АВТОМАТИЧНОГО ОЦІНЮВАННЯ СТІЙКОСТІ SP-МЕРЕЖ ДО ДИФЕРЕНЦІАЛЬНОГО КРИПТОАНАЛІЗУ НА ПРИКЛАДІ АЛГОРИТМУ ШИФРУВАННЯ ДСТУ 7624:2014

М. А. Байбуз[1, a]

[1] *Національний технічний університет України «Київський політехнічний інститут»*

Анотація

В роботі наводиться уточнений метод автоматичного оцінювання верхніх меж імовірностей диференціалів SP-мереж. Метод пропонується для каласу SP-мереж. Застосування данного методу проілюстровано на прикладі алгоритму шифрування ДСТУ 7624:2014, який являється національним стандартом шифрування України. Цей метод дозволяє встановити теоретичну (доказову) стійкість шифрів даного класу до диференціального криптоаналізу.

Ключові слова: диференціальний криптоаналіз, SP-мережі, ДСТУ 7624:2014, "Калина"

Вступ

Стійкість до диференціального криптоаналізу в наш час є необхідною умовою для будь-якого блочного шифру. В даній роботі пропонується метод для обчислення параметрів стійкості до диференціального криптоаналізу для SP-мереж на прикладі алгоритму шифрування ДСТУ 7624:2014.

Новий стандарт шифрування ДСТУ 7624:2014 [1] був розроблений колективом харківських криптографів на основі алгоритму шифрування «Калина» [1]. Він прийшов на заміну міждержавному стандарту ГОСТ 28147-89 (гармонізованому як ДСТУ ГОСТ 28147:2009 [1]).

Ці параметри дозволяють встановити теоретичну (доказову) стійкість алгоритму шифрування до диференціального криптоаналізу.

1. Формальний опис SP-мереж

1.1. Необхідні терміни та позначення

Нехай V_u – простір u бітних векторів, $(V_u)^m$ – простір m бітних векторів з u бітними координатами. Кожен елемент $x \in (V_u)^m$ будемо розглядати як вектор-стовпчик, де $x_i \in V_u$. Через $wt(x)$ позначимо кількість ненульових біт у векторі x. Нехай на просторі $(V_u)^m$ задано деякі операції $\circ$ та $\bullet$. Нехай $L\colon (V_u)^m \to (V_u)^m$ – лінійне перетворення (відносно операції $\circ$), тоді індексом розгалудження L називається величина B:

$$B = B(L) = \min_{x \neq 0}\{wt(x) + wt(L(x))\}.$$

1.2. SP-мережа

SP-мережею будемо називати ітеративний блочний шифр виду:

$$E_k(X) = F_{K_r}(F_{K_{r-1}}(...(F_{K_1}(X)))),$$

де $K = (K_1, .., K_r) \in (V_u)^{mr}$ – ключ шифрування, а F раундове перетворення, яке визначається таким чином:

$$F : (V_u)^m \times (V_u)^m \to (V_u)^m,$$

$$F(X, K) = f(X \bullet K),$$

$$f(X) = L(S(X)),$$

де f – раундова функція, $S = (S_1, ..., S_m)$ – рівень нелінійних підстановок, в якому всі S блоки $S_i : V_u \to V_u$ – бієктивні, $L : (V_u)^m \to (V_u)^m$ лінійне перетворення (відносно операції $\circ$).

1.3. Приклад SP-мережі: алгоритм шифрування ДСТУ 7624:2014

Алгоритм ДСТУ 7624:2014 побудований на основі AES-подібної SP-мережі. Він перетворює блоки вхідного тексту довжиною 128, 256 або 512 біт у відповідні блоки шифртексту, за допомогою ключа довжиною 128, 256 або 512 біт. Розмір ключа може бути рівний розміру блоку, або може бути вдвічі більший за розмір блоку. Кількість раундів шифрування визначається довжиною ключа.

Вхідний блок даних розташовується у матриці стану; на кожному раунді шифрування над матрицею стану виконуються такі операції:

- додавання із раундовим ключем;
- нелінійна заміна($SubBytes$);
- зсув рядків($ShiftRows$);
- перемішування стовпчиків($MixColumns$).

Після останнього раунду відбувається додаткове забілювання даних із окремим раундовим ключем. На першому раунді та після останнього раунду ключі додаються до матриці стану із використанням операції додавання за модулем 2^{64}, а в усіх інших раундах використовується побітове додавання.

Нелінійна заміна байт матриці стану відбувається за допомогою чотирьох підстановок зафіксованих

[a] kolr@ukr.net

у стандарті π_0, π_1, π_2, π_3. Перемішування стовпчиків відбувається шляхом множення на циркулянтну матрицю над полем $GF(2^8)$; це перетворення має максимально можливий індекс розгалуження $B = 9$.

2. Алгоритм оцінювання верхніх меж диференціальних імовірностей

2.1. Теоретичне підґрунтя

В основі алгоритму лежить ідея Келіхера, а саме: заміна точних значень різниць α, β на так звані «шаблони». $T\alpha = \widehat{\alpha} \in V_m$ за таким правилом: $\widehat{\alpha}_i = 0$, якщо $\alpha_i = 0$ та $\widehat{\alpha}_i = 1$, якщо $\alpha_i \neq 0$. Використовуючи шаблони, ми можемо побудувати для кожного r матрицю верхніх меж імовірностей диференціалів $(UB^{[r]}(\widehat{\alpha}, \widehat{\beta}))$ таку, щоб для довільних векторів α, β виконувалась рівність:

$$d(\alpha, \beta)^{[r]} \leq UB^{[r]}(\widehat{\alpha}, \widehat{\beta}),$$

під $d(\alpha, \beta)^{[r]}$ маємо на увазі імовірність r раундового диференціалу α, β.

Нехай L – лінійне перетворення алгоритму шифрування, для того, щоб встановити кількість векторів γ, які відповідають таким умовам: $T\gamma = \widehat{\gamma}$ та $T(L(\gamma)) = \widehat{\beta}$. Вводимо допоміжну матрицю $W[\widehat{\alpha}, \widehat{\beta}]$:

$$W[\widehat{\alpha}, \widehat{\beta}] = \{x \in V_n : Tx = \widehat{\alpha}, T(L(x)) = \widehat{\beta}\}.$$

Матриця W показує кількість способів отримати із заданого вхідного шаблону $\widehat{\alpha}$ заданий вихідний шаблон $\widehat{\beta}$ для лінійного перетворення L. Таким чином маємо наступну оцінку:

$$d(\alpha, \beta)^{[r]} \leq \sum_{\widehat{\gamma}} UB^{[r-1]}(\widehat{\alpha}, \widehat{\gamma}) \cdot W[\widehat{\gamma}, \widehat{\beta}] \cdot p^{wt(\widehat{\beta})},$$

де $p = \max(MDP(s_i))$, $MDP(f)$ – максимальна диференціальна імовірність функції f.

2.2. Побудова алгоритму

Алгоритм будується за допомогою індукції. Початкове значення має вигляд:

$$UB^{[2]}(\widehat{\alpha}, \widehat{\beta}) =$$
$$= \begin{cases} \min\{p^{B-1}, p^{wt(\widehat{\alpha})}, p^{wt(\widehat{\beta})}\}, & wt(\widehat{\alpha}) + wt(\widehat{\beta}) \geq B \\ 0, & \text{в інших випадках} \end{cases}$$

де B – це індекс розсіювання лінійного перетворення L.

Для підрахунку наступних значень $UB^{[t]}(\widehat{\alpha}, \widehat{\beta})$ необхідно знати величину $M = \min_{\widehat{\gamma}} UB^{[t-1]}(\widehat{\gamma}, \widehat{\beta})$ для кожного $\widehat{\beta}$ та передобчислену матрицю W.

Тоді $UB^{[t]}(\widehat{\alpha}, \widehat{\beta})$ має вигляд:

$$UB^{[t]}(\widehat{\alpha}, \widehat{\beta}) =$$
$$= \min\{M, \sum_{\widehat{\gamma}} UB^{[t-1]}(\widehat{\alpha}, \widehat{\gamma}) \cdot W[\widehat{\gamma}, \widehat{\beta}] \cdot p^{wt(\widehat{\beta})}\},$$

де $t = 3, 4, ...r$.

2.3. Передобчислення матриці W

Лінійне перетворення $L : V_n \to V_n$ задано матрицею L над V_u. Через матрицю $L_{\widehat{\alpha},\widehat{\beta}}$ позначимо такі підматриці матриці L, які розташовані на перетині $\widehat{\alpha}_i = 1$ стовчиків та $\widehat{\beta}_i = 0$ рядків. Позначимо через $W_{\geq}[\widehat{\alpha}, \widehat{\beta}]$ кількість розв'язків рівняння $L_{\widehat{\alpha},\widehat{\beta}} \cdot z = 0$. Звідси маємо:

$$W_{\geq}[\widehat{\alpha}, \widehat{\beta}] = (2^u)^{wt(\widehat{\alpha}) - rank(L_{\widehat{\alpha},\widehat{\beta}})}.$$

Якщо лінійне перетворення задається MDS-матрицею, можна значно спростити підрахунок $W_{\geq}[\widehat{\alpha}, \widehat{\beta}]$. Так як довільна підматриця MDS-матриці є невиродженою то ранг будь-якої довільної підматриці MDS-матриці буде рівний $rank(L_{\widehat{\alpha},\widehat{\beta}}) = min(wt(\widehat{\alpha}), wt(\widehat{\beta}))$. Звідси випливає рівність:

$$W_{\geq}[\widehat{\alpha}, \widehat{\beta}] = (2^u)^{wt(\widehat{\alpha}) - min(wt(\widehat{\alpha}), wt(\widehat{\beta}))}.$$

Із значень $W_{\geq}[\widehat{\alpha}, \widehat{\beta}]$ знаходяться значення $W[\widehat{\alpha}, \widehat{\beta}]$ за допомогою формул включення-виключення:

$$W'[\widehat{\alpha}, \widehat{\beta}] = \sum_{k=0}^{wt(\widehat{\alpha})} \sum_{\substack{\widehat{c}:\widehat{c} \prec \widehat{\alpha}, \\ wt(\widehat{c})=k}} (-1)^{wt(\widehat{\alpha})-k} \cdot W_{\geq}[\widehat{\alpha}, \widehat{c}],$$

$$W[\widehat{\alpha}, \widehat{\beta}] = \sum_{k=0}^{wt(\widehat{\beta})} \sum_{\substack{\widehat{c}:\widehat{c} \prec \widehat{\beta}, \\ wt(\widehat{c})=k}} (-1)^{wt(\widehat{\beta})-k} \cdot W'[\widehat{c}, \widehat{\beta}],$$

де символом $\prec$ позначено відношення домінування на бітових векторах.

Висновки

В даній роботі був наведений метод автоматичного оцінювання верхніх меж імовірностей диференціалів SP-мереж. Для прикладу був взятий національний стандарт шифрування України ДСТУ 7624:2014. В ході роботи були наведені труднощі, з якими можна зіткнутися при реалізації цього методу для оцінювання стійкості алгоритму шифрування ДСТУ 7624:2014. В наш час даний метод може бути реалізований на ЕОМ.

Слід зауважити, що данний метод може бути покращений шляхом уточнення розподілів диференціальних імовірностей S-блоків, через які проходять різниці на раундах шифрування.

Перелік використаних джерел

1. Інформаційні технології. Криптографічний захист інфомації. Алгоритм симетричного блокового перетворення: ДСТУ 7624:2014. К. : Держспоживстандарт України — 2015. — 238 с.