Людмила Завадська, Віталій Сергієнко
ФТІ НТУУ «КПІ»
УДК 681.3.06:519.248.681

ДОСЛІДЖЕННЯ КУБІЧНИХ АТАК З МАЛИМИ СТЕПЕНЯМИ МАКСТЕРМІВ

Анотація: **Отримано математичний вираз для залежності кількості булевих функцій, "сприятливих" для кубічної атаки, від кількості відкритих і секретних змінних криптосистеми, а також степеня функції за умови використання виключно макстермів першого степеня. Теоретичні результати перевірено за допомогою програмних розрахунків. Проаналізована імовірність успіху атаки для функцій з різними кількостями змінних.**
Summary: **In this paper, we present mathematical expression for number of Boolean functions, 'good' for cube attack with maxterms of degree 1. It depends on encryption function's degree and on the number of its secret and public variables. Theoretical results were verified using computer calculations. This paper also provides analysis of cube attack's success rate for encryption functions with different numbers of variables.**
Ключові слова: **Криптоаналіз, кубічні атаки, макстерми, булеві функції.**

I Вступ

В умовах сучасних масштабів електронного документообігу важливим питанням є захист інформаційних ресурсів. Для забезпечення надійного захисту необхідне поєднання організаційних, технічних і криптографічних методів. Зокрема, важливу роль у криптографічному захисті інформації відіграють симетричні криптосистеми. Оскільки вони є широко розповсюдженими, то задача розробки, дослідження, удосконалення методів криптоаналізу таких схем шифрування задля забезпечення їх стійкості є важливою в практичному і теоретичному аспекті. Інструментом для аналізу в цьому випадку можуть виступати різні види криптоатак, одним з яких є новий перспективний вид атаки – кубічні атаки, вперше описані у статті [1], опублікованій Дінуром та Шаміром (Itai Dinur, Adi Shamir) у 2008 році й застосовані до учасника конкурсу eStream потокових шифрів під назвою Trivium. Пізніше, у 2009 році, світ побачила оновлена і доповнена версія цієї статті [2]. І хоч цей вид атаки розроблявся з прицілом на потокові криптосистеми, основні ідеї кубічної атаки пізніше були застосовані для криптоаналізу блокових шифрів та хеш-функцій [3 – 5].

Об'єктом дослідження даної статті є *кубічні атаки* на криптосистеми з наявними відкритими змінними. У роботі розглядається питання застосовності кубічних атак за умови використання лише макстермів малого степеня. Вводиться поняття сприятливої функції для кубічної атаки. Функція визнається сприятливою, якщо можливе успішне застосування до неї кубічної атаки з макстермами тільки першого степеня. Як результат досліджень отримано математичний вираз для кількості сприятливих функцій залежно від кількості відкритих і секретних змінних. Теоретичні результати перевірено за допомогою програмних розрахунків. Також у роботі проаналізована імовірність успіху атаки для функцій з різними кількостями змінних.

II Кубічні атаки

Майже кожен криптографічний алгоритм може бути описаний як деяка булева функція, що залежить як від секретних (біти ключа), так і відкритих змінних (біти відкритого тексту або вектору ініціалізації). Криптоаналітик може підбирати значення відкритих змінних таким чином, щоб отримати систему рівнянь певного виду, що залежить від секретних змінних, і знайти її розв'язок. Таким чином, необхідний опис підходу, що визначає, як саме треба змінювати відкриті змінні, щоб мати змогу побудувати розв'язувану систему рівнянь. Цей опис надається у роботах [1, 2].

Кубічна атака є однією з різновидів алгебраїчних атак, що можуть застосовуватися до потокових криптосистем. Кожен біт вихідної послідовності потокового шифру інтерпретується як значення деякої булевої функції (поліному), що залежить від бітів вектора ключа та деяких відкритих змінних. Таким чином, нехай K – множина секретних змінних, а IV – відкритих (за аналогією з потоковими криптосистемами називатимемо їх бітами вектора ініціалізації). Тоді вищевказана функція має вигляд: $f:\{0,1\}^{|K|+|IV|}\to\{0,1\}$. Якщо $|K|+|IV|=n$, то $f(x_1,...,x_n)$ – булева функція від n змінних.

Нехай $I\subseteq S=\{x_1,...,x_n\}$ – деяка підмножина множини змінних, $|I|=k$.

Тоді функцію f можна представити у вигляді:

$$f(x_1,...,x_n)=p_m(I)\cdot p_S(x_j\mid j\in S\setminus I)\oplus r(x_j\mid j\in S), \qquad (1)$$

де $p_m(I) = x_{i_1} \cdot x_{i_2} \cdot ... \cdot x_{i_k}$; $p_S(x_j \mid j \in S \setminus I)$ – деякий многочлен від змінних $\{x_j \mid j \in S \setminus I\}$; поліном $r(x_j \mid j \in S)$ (назвемо його поліномом-залишком) такий, що будь-яка кон'юнкція, що входить у цей поліном, не містить хоча б однієї змінної з множини I [2].

Поліном $p_m(I)$ називається макстермом (англ. maxterm), якщо степінь полінома $p_S(I)$ дорівнює 1 (тобто, $p_S(I)$ – лінійна булева функція, що тотожно не дорівнює константі). При цьому $p_S(I)$ називається суперполіномом (англ. superpoly), а множина I називається кубом.

Таке зображення функції має корисну властивість:

$$\bigoplus_{x_i \in I} f(x_1,...,x_n) = p_S(x_j \mid j \in S \setminus I). \quad (2)$$

Атака має кілька стадій обчислень [6]:

попередні обчислення (англ. preprocessing) – пошук макстермів та суперполіномів;

відновлення бітів ключа (англ. key bit recovery) – отримання та розв'язання системи лінійних рівнянь від бітів секретного ключа.

Розглянемо ці стадії докладніше.

На стадії попередніх обчислень виконується пошук кубів, тобто макстермів та відповідних їм суперполіномів. При цьому передбачається, що криптоаналітик може змінювати як секретні ключі криптосистеми, так і вектори ініціалізації, що в ній використовуються.

Розглянемо процес пошуку кубів більш детально. Для знаходження куба за властивістю (2) підраховується сума (у полі GF(2)) всіх значень досліджуваної булевої функції за всіма значеннями змінних, що входять у деякий можливий макстерм (при цьому множина змінних макстерма I є підмножиною IV). Вважається, що змінні, які не входять у макстерм, є фіксованими (наприклад, їх можна проініціалізувати нулями). Після цього перевіряється, чи є результат підсумовування лінійним поліномом від бітів секретного ключа, тобто суперполіномом. Якщо суперполіном знайдено, то коефіцієнти в ньому визначаються за допомогою встановлення відповідних значень бітів ключа, рівними 1, а решту бітів ключа покладають рівною 0. Вільний член у суперполіномі можна знайти, якщо всі біти ключа покласти рівними 0.

На практиці зазвичай виконують пошук макстермів і суперполіномів наступного виду: $v_{i_1} \cdot v_{i_2} \cdot ... \cdot v_{i_m} \cdot (k_{j_1} \oplus k_{j_2} \oplus ... \oplus k_{j_n} \oplus c)$, де $v_{i_t} \in IV, 1 \le m \le |IV|, k_{j_s} \in K, 1 \le n \le |K|$, $c \in \{0,1\}$ – константа.

Варто зазначити, що кожному такту роботи потокового шифру відповідає своя булева функція виходу. Тому пошук кубів можна поширити на багато тактів роботи, щоб отримати достатню кількість пар макстерм-суперполіном для наступної стадії атаки.

Стадія попередніх обчислень є ресурсоємною, але виконується лише один раз для кожної конкретної криптосистеми. Основними проблемами цього етапу є ефективний перебір можливих кубів та алгоритм перевірки лінійності полінома p_S.

Перебір макстермів (кубів) для перевірки відповідних суперполіномів на лінійність є тривалою операцією і тому потребує ефективних підходів для її здійснення. Одним із таких підходів є обмеження степеня макстермів, що беруться до розгляду. Таке обмеження можна робити як знизу, так і зверху (наприклад, перебирати лише макстерми, степінь яких більший за 2, але менший за 5). Джерелом обмежень може виступати просто уявлення про можливий степінь функції, що описує вихід шифру (наприклад, у схемі нелінійної фільтрації за умови відкритості алгоритму степінь функції шифрування є наперед заданим і постійним, тобто, не залежить від такту роботи шифру), або, при більш строгому підході, знаходження степеня нелінійної функції за допомогою відповідних тестів, які, однак, є досить складними і важкими для реалізації.

Стадія відновлення бітів ключа – це етап кубічної атаки, на якому розв'язується система лінійних рівнянь, отриманих на основі знайдених на попередній стадії кубів та заданого фіксованого секретного ключа (при цьому криптоаналітик може довільно змінювати вектор ініціалізації). Кожне рівняння системи отримується як сума виходів функції за всіма значеннями змінних, що входять у відповідний знайдений макстерм. Оскільки ключ фіксований і заданий, то таким чином ми дізнаємось, яке значення приймає відповідний суперполіном на цьому ключі. Система має наступний вигляд:

$$\begin{cases} p_s^1(x_j \mid j \in S \setminus I_1) = b_1 \\ p_s^2(x_j \mid j \in S \setminus I_2) = b_2 \\ \vdots \\ p_s^N(x_j \mid j \in S \setminus I_N) = b_N \end{cases}, \tag{3}$$

де N – кількість рівнянь, $p_s^i(x_j \mid j \in S \setminus I_i)$ – і-тий суперполіном, а bi – сума значень функції шифрування за всіма значеннями змінних, що входять в і-тий макстерм, $b_i \in \{0,1\}$.

Система лінійних рівнянь з двійковими коефіцієнтами може бути розв'язана, наприклад, методом Гауса (якщо на попередній стадії не проводився пошук оберненої матриці системи, оскільки в цьому разі достатньо просто перемножити цю матрицю на стовпець $\overline{b}$). При цьому необхідно проводити відбір лінійно незалежних рівнянь (тому потенційно кількість кубів, що отримуються під час попередніх обчислень, має бути набагато більшою, аніж потужність K).

III Кількість булевих функцій, сприятливих для кубічної атаки з макстермами першого степеня

Нехай $|IV| = t$, $|K| = s$, $v_1,...,v_t$ – відкриті, а $x_1,...x_s$ – секретні змінні. Позначимо $N_r^k(t,s)$ кількість «гарних» функцій $f = f(v_1,...,v_t,x_1,...,x_s)$ степеня r, тобто функцій, у яких за допомогою макстермів степенів, що не перевищують k, можна знайти щонайменше s лінійно незалежних суперполіномів, вважаючи, що всі відкриті змінні, що не входять до куба, покладаються нулями. У даній роботі виводяться формули лише для $N_r^1(t,s)$ при будь-яких r, тобто $1 \le r \le t+s$, та будь-якому співвідношенні t та s. У результаті знаходиться ймовірність успішної кубічної атаки з використанням макстермів тільки першого степеня $P_{усп}^1$ – ймовірність набрати таким чином систему з s лінійно незалежних рівнянь відносно секретних змінних.

Зрозуміло, що при $t < s$ $N_r^1(t,s) = 0$. Отже, в подальшому вважаємо, що $t \ge s$. У загальному випадку, тобто, для більших степенів макстерма d, вимагається виконання умови $s \le C_t^d$.

Будемо виводити формули для $N_r^1(t,s)$, поступово збільшуючи степінь функції r від 1 до $t+s$.

Очевидно, що $N_1^1(t,s) = 0$ при будь-яких t, s.

Розглянемо $N_2^1(t,s)$. Функція 2-го степеня від змінних $v_1,...,v_t,x_1,...,x_s$ містить хоча б один терм 2-го степеня виду $v_i v_j$, $1 \le i,j \le t$ або $v_i x_j$, $1 \le i \le t, 1 \le j \le s$, або $x_i x_j$, $1 \le i,j \le s$ та лінійну частину (можливо нульову), яку загалом позначимо L. Терми, які не впливають на наявність або відсутність макстермів і, відповідно, суперполіномів, будемо називати нейтральними, терми, які утворюють макстерми 1-го степеня, будемо називати сприятливими і терми, які унеможливлюють існування відповідних макстермів – несприятливими. Так, наприклад, всі терми 0-го та 1-го степенів – нейтральні, від їх наявності або відсутності кількість суперполіномів не залежить. Таким чином, уся лінійна частина є нейтральною. Нейтральними є також терми виду $v_i v_j$ та $x_i x_j$, а терми виду $v_i x_j$ - сприятливі.

Кількість можливих варіантів для L становить 2^{t+s+1} – кількість лінійних функцій від $t+s$ змінних.

Кількість можливих лінійних комбінацій з нейтральних термів 2-го степеня дорівнює $2^{C_t^2+C_s^2}$ (таких термів може й взагалі не бути, бо у «гарній» функції повинен бути хоча б один сприятливий терм, що гарантує 2-й степінь функції).

Позначимо кількість всіх можливих лінійних комбінацій нейтральних термів у функції 2-го степеня від $t+s$ змінних через $N_2^0(t,s)$. Тоді $N_2^0(t,s) = 2^{C_t^2+C_s^2} 2^{t+s+1} = 2^{C_t^2+C_t^1+C_t^0+C_s^2+C_s^1+C_s^0-1}$.

Порахуємо кількість можливих лінійних комбінацій сприятливих термів, при яких гарантується наявність s лінійно незалежних суперполіномів. Для початку розглянемо випадок, коли $s = 1$, тобто маємо лише одну секретну змінну. Тоді кількість можливих варіантів побудови пар макстерм-суперполіном становить $2^t - 1$. Це є число усіх можливих лінійних комбінацій відкритих змінних, окрім нульової.

При $s = 2$ для першої секретної змінної число можливих комбінацій відкритих змінних дорівнює $2^t - 1$, а для другої – вже $2^t - 2$, оскільки використану для першої змінної комбінацію відкритих змінних ми

відкидаємо (одна і та сама комбінація не додає нових макстермів, а отже, і нових рівнянь у систему). При $s=3$ для третьої секретної змінної кількість комбінацій відкритих становить 2^t-2^2, цього разу не враховуються лінійні комбінації термів, використаних для попередніх секретних змінних. Аналогічно, при збільшенні величини s для кожної наступної змінної кількість комбінацій відкритих змінних становить 2^t-2^i, де і – індекс, що відповідає секретній змінній, $i=0,...,s-1$. Отже, кількість варіантів побудови системи незалежних рівнянь дорівнює $\prod_{i=0}^{s-1}(2^t-2^i)$. Позначимо даний вираз як $K(t,s)$ (від англ. kernel - ядро).

Спробуємо представити $K(t,s)$ в іншому вигляді. Для цього розпишемо $\prod_{i=0}^{s-1}(2^t-2^i)$ наступним чином:

$$K(t,s)=\prod_{i=0}^{s-1}2^i(2^{t-i}-1)=\prod_{i=s-1}^{0}2^i\cdot\prod_{i=0}^{s-1}(2^{t-i}-1)=2^{s-1}(2^t-1)\cdot 2^{s-2}(2^{t-1}-1)\cdot\ldots\cdot 2^0(2^{t-s+1}-1).$$

У даному представленні легко бачити рекурентну залежність, а саме:

$$K(t,s)=2^{s-1}\cdot(2^t-1)\cdot K(t-1,s-1)\ . \tag{4}$$

Повне визначення $K(t,s)$ має наступний вигляд:

$$K(t,s)=\begin{cases}0,(t<s)\,або\,(s=0)\\ 2^t-1,s=1\\ 2^{s-1}\cdot(2^t-1)\cdot K(t-1,s-1),\ інакше\end{cases}. \tag{5}$$

Підсумовуючи вищесказане, приходимо до висновку, що

$$N_2^1(t,s)=N_2^0(t,s)K(t,s). \tag{6}$$

Формула для $N_2^1(t,s)$ є базовою. Терми степенів вище за 2, не можуть бути сприятливими при $k=1$, вони можуть бути лише нейтральними або несприятливими, і нам залишається врахувати їх вплив для функцій степенів $r>2$.

Розглянемо $N_3^1(t,s)$. У функції 3-го степеня додатково до термів 0, 1, 2-го степенів з'являється хоча б один доданок виду:

1) $v_{i_1}v_{i_2}v_{i_3}$, 2) $v_{i_1}v_{i_2}x_{j_1}$, 3) $v_{i_1}x_{j_1}x_{j_2}$, 4) $x_{j_1}x_{j_2}x_{j_3}$.

Терми виду 1), 2), 4) – нейтральні, виду 3) – несприятливі. Кількість можливих нейтральних термів дорівнює $C_t^3C_s^0+C_t^2C_s^1+C_t^0C_s^3$, звідки кількість можливих варіантів для нейтральних термів 3-го степеня дорівнює $N_3^0(t,s)=2^{C_t^3C_s^0+C_t^2C_s^1+C_t^0C_s^3}$.

Якщо функція 3-го степеня не має несприятливих доданків, то кількість таких «гарних» функцій дорівнює $[N_3^0(t,s)-1]N_2^1(t,s)$.

Якщо функція 3-го степеня має несприятливі доданки виду 3) тільки з одним макстермом, наприклад, виду $v_1x_{j_1}x_{j_2}$, то кількість таких функцій дорівнює $N_3^0(t,s)(2^{C_s^2}-1)2^{s+t}N_2^1(t-1,s)$.

Множник $2^{s+t}=2^{s+(t-1)+1}$ виникає з тої причини, що в цьому випадку всі доданки виду v_1x_j та v_1v_j стають нейтральними, і доданок v_1 також нейтральний. При підрахунку N_2^1 на них можна не зважати; решта термів виду $v_2x_j,...,v_tx_j$ залишаються сприятливими. Враховуючи, що «гарна» функція f може мати терми виду 3), де індекс i_1 пробігає будь-яку підмножину множини індексів {1,…,t}, в тому числі і порожню (але крім усієї множини, бо в цьому випадку функція не буде «гарною»), отримуємо формулу для $N_3^1(t,s)$:

$$N_3^1(t,s)=N_3^0(t,s)\sum_{i=1}^{t-s}C_t^i[(2^{C_s^2}-1)2^{s+t}]^iN_2^1(t-i,s)+[N_3^0(t,s)-1]N_2^1(t,s)=$$

$$=N_3^0(t,s)\sum_{i=0}^{t-s}C_t^i[(2^{C_s^2}-1)2^{s+t}]^iN_2^1(t-i,s)-N_2^1(t,s). \tag{7}$$

Таким чином, загальна кількість «гарних» функцій степеня, не більшого за 3, дорівнює:

$$N_2^1(t,s)+N_3^1(t,s)=N_3^0(t,s)\sum_{i=0}^{t-s}C_t^i[(2^{C_s^2}-1)2^{s+t}]^i N_2^1(t-i,s) \tag{8}$$

Аналогічно можна показати, що кількість «гарних» функцій степеня $r \le s+1$ дорівнює:

$$N_r^1(t,s)=N_r^0(t,s)\sum_{i=0}^{t-s}C_t^i(2^{C_s^{r-1}}-1)^i 2^{\sum_{k=1}^{i}\sum_{j=0}^{r-2}C_{t+s-k}^j}\sum_{k=2}^{r-1}N_k^1(t-i,s)-\sum_{k=2}^{r-1}N_k^1(t,s) \tag{9}$$

Тут $N_r^0=2^A$,

де

$$A=C_t^rC_s^0+C_t^{r-1}C_s^1+\ldots+C_t^2C_s^{r-2}+C_t^0C_s^r=C_{t+s}^r-C_t^1C_s^{r-1}, \tag{10}$$

бо всі терми r-го степеня, за вийнятком термів виду $v_{i_1}x_{j_1}\ldots x_{j_{r-1}}$, є нейтральними.

При $s+1<r\le t+s$:

$$N_r^1(t,s)=[N_r^0(t,s)-1]\sum_{k=2}^{r-1}N_k^1(t,s), \tag{11}$$

бо всі терми r-го степеня в цьому випадку є нейтральними і хоча б один з них має бути присутнім. $N_r^0=2^A$, але при $s+1<r\le t$

$$A=C_t^rC_s^0+C_t^{r-1}C_s^1+\ldots+C_t^{r-s}C_s^s, \tag{12}$$

а при $t<r\le t+s$

$$A=C_t^tC_s^{r-t}+C_t^{t-1}C_s^{r-t+1}+\ldots+C_t^{r-s}C_s^s. \tag{13}$$

Отже, ймовірність успішної атаки з використанням макстермів тільки першого степеня за умови рівноймовірності всіх булевих функцій від $t+s$ змінних становить

$$P_{усп}^1=\frac{\sum_{r=1}^{t+s}N_r^1(t,s)}{2^{2^{t+s}}}, \tag{14}$$

де величини $N_r^1(t,s)$ визначаються за формулами (4) – (14).

IV Результати чисельних підрахунків

Задля перевірки правильності аналітичних результатів було здійснено комп'ютерний підрахунок кількості сприятливих функцій із макстермами тільки першого степеня залежно від різних параметрів атаки. Для виконання даної процедури у загальному випадку необхідно здійснити повний перебір всіх можливих булевих функцій із заданою кількістю змінних, а кожну функцію перевіряти на «сприятливість» шляхом застосування алгоритмів кубічної атаки (перебір макстермів, тест лінійності отриманих суперполіномів і пошук рангу побудованої системи лінійних рівнянь). Але це є дуже ресурсоємною задачею, тому перебір було пришвидшено за рахунок певних програмних і аналітичних оптимізацій. Зокрема, зі списку всіх можливих булевих функцій виключалися ті, що завше не є сприятливими, наприклад, за ознакою степеня або довжини полінома, наявністю несприятливих доданків тощо.

У табл. 1 наведені числові значення кількості сприятливих функцій із макстермами першого степеня $N_r^1(t,s)$ залежно від кількості відкритих змінних t, кількості секретних змінних s і степеня функції r.

Таблиця 1 – Числові значення кількості сприятливих функцій з різною кількістю змінних

s	t	$N_r^1(t,s)$				
		r = 2	r = 3	r = 4	r = 5	r = 6
1	1	8	-	-	-	-
1	2	96	96	-	-	-
1	3	1792	26880	28672	-	-
2	2	768	2304	3072	-	-

1	4	61440	62853120	1950351360	2013265920	-
2	3	43008	14899200	463208448	478150656	-
1	5	4063232	4260603494400	139607194701004800	8795530072254578688	8935141660703064064
2	4	3440640	1565512138752	51297136250486784	3231825313847574528	3283124128353091584
3	3	1376256	2817196032	11536417751040	727326941773824	738871813865472

На основі отриманих числових даних можна вирахувати імовірність успіху кубічної атаки при розгляді макстермів лише першого степеня, скориставшись формулою (14). Значення імовірності для різної кількості змінних наведені у таблиці 2.

Таблиця 2 – Значення імовірності успіху кубічної атаки з макстермами першого степеня для різної кількості змінних булевої функції

s	t	Загальна кількість функцій: $N_{заг} = 2^{2^{t+s}}$	$P^1_{усп}$
1	1	16	0,50000
1	2	256	0,75000
1	3	65536	0,87500
2	2	65536	0,09375
1	4	4294967296	0,93750
2	3	4294967296	0,22266
1	5	18446744073709551616	0,96875
2	4	18446744073709551616	0,35596
3	3	18446744073709551616	8,01086E-05

Як бачимо, чим більшою є різниця між t та s, тим більшою є імовірність успіху. Але в реальних криптоалгоритмах зазвичай виконується умова $t \le s$, тому більш цікавим є випадок $t = s$ (мінімально допустиме значення t, за якого атака ще може бути успішною). А із зростанням суми кількостей секретних і відкритих змінних за такої умови імовірність має тенденцію до стрімкого спаду. Можна стверджувати, що при $t = s$ для достатньо великих значень t, s (наприклад, $t = s = 32$), імовірність успіху атаки при використанні лише макстермів першого степеня є близькою до 0. Отже, для забезпечення більш прийнятого рівня імовірності успіху необхідний розгляд макстермів вищих степенів.

V Висновки

Проведено дослідження перспективного інструменту криптоаналізу – кубічних атак, ключовими поняттями для яких є поняття макстерму та суперполіному. Наявність достатньої кількості лінійно незалежних суперполіномів дозволяє знайти секретний ключ. Складність атаки експоненціально зростає при збільшенні степеня макстермів. Тому, задля уникнення ресурсоємного перебору, доцільніше застосовувати атаку при відносно невеликих значеннях степеня. Верхнє обмеження для степеня макстермів можна отримати знаючи степінь функції, що описує криптосистему, але в загальному випадку цей степінь є невідомим і необхідні досить ресурсоємні обчислення для його визначення. У роботі проведено аналіз випадку, коли в атаці використовуються макстерми лише першого степеня.

Функція визнається сприятливою, якщо можливе успішне застосування до неї кубічної атаки з макстермами тільки першого степеня. Основним результатом роботи є виведені формули для кількості сприятливих функцій залежно від степеня функції та кількості відкритих і секретних змінних. Розраховані за цими формулами значення перевірено шляхом порівняння із результатами безпосереднього комп'ютерного перебору.

Також були розраховані імовірності успіху кубічної атаки з макстермами першого степеня для різних комбінацій кількостей відкритих і секретних змінних. Звісно, за умови використання макстермів малих степенів імовірність успішної атаки є дуже малою за реальних значень кількості відкритих та секретних змінних. Проте, знаючи величину цієї імовірності можна оцінити максимальний степінь макстермів, що забезпечує прийнятний рівень імовірності успіху кубічної атаки.

Отримані результати є підґрунтям для подальших досліджень, зокрема, для аналізу кубічних атак із більшими степенями макстермів. У той же час розглядувана задача має самостійний інтерес з точки зору теорії булевих функцій та комбінаторики.

Список використаної літератури: 1. Dinur I. Cube attacks on tweakable black box polynomials / Dinur I., Shamir A. – Cryptology ePrint Archive, 2008/385. [Online] Available at: http://eprint.iacr.org/2008/385.pdf. 2. Dinur I. Cube attacks on tweakable black box polynomials / Dinur I., Shamir A. // EUROCRYPT, vol. 5479 of Lecture Notes in Computer Science – Springer, 2009. – P. 278-299. 3. Dinur I. Side Channel Cube Attacks on Block Ciphers / Dinur I., Shamir A. – Cryptology ePrint Archive, 2009/127. [Online] Available at: http://eprint.iacr.org/2009/127.pdf. 4. Aumasson J-P. Cube Testers and Key Recovery Attacks on Reduced Round MD6 and Trivium / Aumasson J-P., Meier W., Dinur I., Shamir A. // Fast Software Encryption 2009, LNCS, vol 5665 – Springer, 2009. – P. 1-22. 5. Dinur I. Cube Attacks and Cube-attack-like Cryptanalysis on the Round-reduced Keccak Sponge Function / Dinur I., Morawiecki P., Pieprzyk J., Srebrny M., Straus M. – Cryptology ePrint Archive, 2014/736. [Online] Available at: http://eprint.iacr.org/2014/736.pdf. 6. Meier W. Cube Testers and Key Recovery in Symmetric Cryptography / Meier W. – 2009. [Online] Available at: http://indocrypt09.inria.fr/slides_cube_ind09.pdf.

Анатолій Кочубінський, Володимир Синявський, Олександр Шаталов
Інститут кібернетики імені В. М. Глушкова НАН України

УДК 002:651.928(083.73)

АЛГОРИТМ ВСТАНОВЛЕННЯ СПІЛЬНОГО СЕКРЕТНОГО ЗНАЧЕННЯ, ЩО ҐРУНТУЄТЬСЯ НА ЕЛІПТИЧНИХ КРИВИХ

Анотація: **Пропонується алгоритм встановлення спільного секретного значення, який розроблено з використанням криптографічного перетворення, визначеного національним стандартом України ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, заснований на еліптичних кривих. Формування і перевіряння», та криптографічних стандартів, що діють в Україні. Цей алгоритм забезпечує автентичність сторін інформаційного обміну.**

Summary: **An algorithm of establishment of shared secret value is presented. The algorithm is based on the cryptographic transformation defined by the national standard of Ukraine DSTU 4145-2002 «Information technology. Cryptographic techniques. Digital signatures based on elliptic curves. Generation and verification» and cryptographic standards which operate in Ukraine. This algorithm provides mutual authenticity of information exchange parties.**

Ключові слова: **Асиметричне шифрування, симетричне шифрування, еліптичні криві, спільний секретний ключ.**

Вступ

Конфіденційність повідомлення забезпечується шифруванням повідомлення за допомогою алгоритму шифрування даних. При великому розмірі документа таким алгоритмом може бути тільки алгоритм симетричного шифрування. Використання симетричного алгоритму шифрування пов'язано з необхідністю вирішення проблеми розподілу секретних ключів шифрування. Одним з можливих рішень є використання алгоритму асиметричного шифрування, яким шифрується разовий ключ симетричного шифрування, однак в системах передачі даних в реальному часі потрібне інше рішення, яке дозволить швидко з'єднатися з будь яким абонентом, встановити спільний секретний ключ та за певним розкладом або у разі потреби сформувати новий спільний ключ та перейти на використання нового спільного ключа. Під час встановлення спільного секретного ключа обов'язково повинна забезпечуватися автентичність сторін інформаційного обміну. Алгоритми цього типу є необхідною складовою частиною основних на цей час методів захисту трафіку в мережі Інтернет, а саме протоколів SSL/TSL та IPSec.

Найбільше поширення як алгоритм встановлення спільного секретного значення мають алгоритми, що базуються на алгоритмі Діффі-Хеллмана. В своєму стандартному вигляді цей алгоритм не забезпечує автентифікації сторін і тому не може протистояти засобам криптоаналізу, що використовують можливість порушення автентичності. Алгоритм встановлення спільного секретного значення має також гарантувати стійкість обчисленого спільного секретного значення, не меншу за стійкість симетричного алгоритму шифрування даних. Реально це можливо тільки за умови застосування криптографічних перетворень у групі точок належно обраних еліптичних кривих. З практичної точки зору важливо уніфікувати обчислювальні засоби, що використовуються для реалізації криптографічних перетворень різного типу.