УДК 681.3.06

О.О. Кузнецов, Ю.А. Ізбенко, І. В. Московченко

Харківський університет Повітряних Сил імені Івана Кожедуба, Харків

ПОБУДОВА КРИПТОГРАФІЧНИХ ФУНКЦІЙ З ВИКОРИСТАННЯМ МЕТОДУ ГРАДІЄНТНОГО СПУСКУ

Досліджуються методи побудови криптографічних булевих функцій. Теоретично обґрунтовується можливість формування збалансованих криптографічних булевих функцій з високими показниками нелінійності та алгебраїчного ступіня, що задовольняють строгий лавинний критерій.

криптографічна булева функція, лавинний критерій, збалансованість

ВЯтуп

Безпека інформації в сучасних АСУ забезпечується механізмами криптографічного перетворення даних [1, 2]. Побудова ефективних криптоалгоритмів описується в термінах булевої алгебри криптографічними булевими функціями [3].

Як показує аналіз відкритої літератури [4 – 7], відомі методи побудови криптографічних функцій з необхідними показниками стійкості можна умовно розділити на три класи: методи випадкової генерації; методи алгебри; евристичні методи. До першого класу відносяться методи, які ґрунтуються на процедурах випадкової генерації з подальшим відбором функцій, що задовольняють задані показники [4]. Їх достоїнство полягає в очевидній простоті практичної реалізації. Істотним недоліком є швидке зростання обчислювальної складності – пошук функцій від восьми та більшої кількості змінних обчислювально не доступний. До другого класу [6 – 9] відносяться методи, що використовують ітеративні процедури побудови, які ґрунтуються на алгоритмах модифікації булевих функцій, що задовольняють певні вимоги (наприклад, бент-функцій). Достоїнством методів алгебри є низька обчислювальна складність. Їх основним недоліком є зниження в процесі ітеративного пошуку деяких інших показників стійкості, наприклад, показника нелінійності [9].

В основі евристичних методів [10 – 14] лежать інтуїтивні підходи до побудови криптографічних булевих функцій. Більшість відомих евристичних підходів мають усі переваги процедур випадкового пошуку та методів алгебри [13]. Дійсно, усі евристичні методи дозволяють конструювати функції з нелінійністю, максимально наближеною до верхньої межі. Так, у класі евристичних методів генетичні методи [11] і методи імітації відпалу [12] дозволяють будувати функції з найвищими показниками стійкості. Обмеженням на практичне застосування даних методів може служити тільки їх висока обчислювальна складність. Отже, актуальним науково-технічним завданням є розробка методу побудови криптографічних булевих функцій, що має низьку обчислювальну складність, на основі подальшого вдосконалення евристичних методів. Найбільший потенціал має метод градієнтного підйому як спосіб, що є базовим для решти методів даного класу [10, 14]. Метою статті є обґрунтування підходу до побудови криптографічних булевих функцій на основі градієнтного пошуку.

Результати доЯліджень

Обґрунтування підходу до побудови криптографічних булевих функцій на основі градієнтного пошуку. Розглянемо основні положення булевої алгебри стосовно побудови криптографічних булевих функцій [3].

Булевою функцією f від n змінних є функція [3], що здійснює відображення з поля $GF(2^n)$ всіх двійкових векторів $x = (x_1, \ldots, x_n)$ довжини n у полі GF(2). Зазвичай булеві функції представляються в нормальній формі алгебри і розглядаються як сума добутків координат, що їх складають. Поле $GF(2^n)$ складається з 2^n векторів α_i: $\alpha_0 = (0,\ldots,0,0)$;

α_1 =(0,...,0,1),..., α_{2^n-1}= (1,...,1,1), $\alpha_i \in V_n$, де V_n – векторний простір у GF(2^n). Послідовністю функції f називається (1,-1)-послідовність, визначена як ($(-1)^{f(\alpha 0)}$, $(-1)^{f(\alpha 1)}$, …, $(-1)^{f(\alpha 2n-1)}$). Таблицею істинності функції f називається (0,1) – послідовність, визначена як (f(α_0), f(α_1), f(α_{2n-1})). Послідовність функції f є збалансованою, якщо її (0,1) - послідовність ((1,-1) – послідовність) містить однакову кількість нулів та одиниць (одиниць та мінус одиниць). Функція f є збалансованою, якщо збалансована її послідовність. Вагою Хеммінга вектора α ((0,1)-послідовності α), що позначається як W(α), є кількість одиниць у векторі (послідовності). Відстанню Хеммінга d(f,g) між послідовностями двох функцій f та g є кількість позицій, в яких різні послідовності цих функцій. Нелінійність N_S перетворення – мінімальна відстань Хеммінга між вихідною послідовністю *S* та всіма вихідними послідовностями афінних функцій над деяким полем:

$$N_S = \min \{d(S,\varphi)\},$$

де φ – множина афінних функцій.

Нелінійність функції N_f – мінімальна відстань Хеммінга N_f між функцією f та всіма афінними функціями над GF(2^n) [3]:

$$N_f = \min \{d(f,\varphi)\},$$

де φ – множина афінних функцій.

При розробці пропонованого підходу за основу взятий евристичний метод градієнтного підйому В.Міллана, Е.Кларка, Е.Доусона, 1997 р. [10] (далі – метод градієнтного підйому). Даний метод ґрунтується на перетворенні вихідних послідовностей нелінійних функцій. Суть методу градієнтного підйому полягає в підвищенні нелінійності довільної булевої функції шляхом комплементації деякої позиції в таблиці істинності даної функції. Кожна позиція таблиці істинності відповідає унікальним вхідним даним функції. Метод дозволяє створити повний список/перелік таких вхідних даних функції, що комплементація будь-якої вихідної позиції в таблиці істинності, яка відповідає даному входу, збільшуватиме нелінійність даної функції. Список/перелік таких позицій у таблиці істинності позначимо як 1 – *Improvement Set* функції f(x), або 1 – IS_f.

Визначення 1 [10]. Нехай g(x) = f(x) ⊕ 1 для x = x_a та g(x) = f(x) для всіх інших x. Якщо $N_g > N_f$, то $x_a \in 1 - IS_f$.

Можливі випадки, коли дана множина буде пустою, і тоді функція f(x) позначається як функція з максимальною нелінійністю і техніка, використовувана в описуваному методі, є не застосовною. Оскільки всі бент-функції є глобально-максимальними, їх 1 – *Improvement Set* множина є пустою. Існує також субоптимальний локальний максимум, який може бути знайдений за допомогою використання методів градієнтного підйому. Розв'язання даної задачі є обчислювально трудомістким, оскільки використовується принцип інвертування позицій таблиці істинності функції випадковим чином, знаходження нових значень WHT (Walsh–Hadamar transform – перетворення Уолша-Адамара) і визначення множини 1 – IS_f.

У [10] представлено швидкий систематичний метод визначення множини 1 – IS_f заданої булевої функції шляхом використання її таблиці істинності та перетворень Уолша-Адамара. Нижче представлені визначення, на яких базується метод визначення того, чи є вхід елементом множини 1 – IS_f.

Для знаходження множини 1 – IS_f заданій булевій функції необхідно спочатку визначити значення коефіцієнтів перетворення Уолша-Адамара, які відповідали б величинам, близьким до абсолютного значення максимального коефіцієнта WH_{max}.

Визначення 2. Нехай f(x) є булевою функцією з перетворенням Уолша-Адамара F(w), де WH_{max} означає максимальне абсолютне значення F(w). Тоді існуватимуть одна або більше лінійних функцій $L_w(x)$, що мають мінімальну відстань до функції, і для даних w буде справедлива рівність $|F(w)| = WH_{max}$.

Визначається така множина:

$$W_1^+ = \{w: F(w) = WH_{max}\};\ W_1^- = \{w: F(w) = -WH_{max}\}.$$

Визначаються множини w, для яких WHT наближені до максимуму:

$$W_2^+ = \{w: F(w) = WH_{max} - 2\};\ W_2^- = \{w: F(w) = -(WH_{max} - 2)\};$$

$$W_3^+ = \{w: F(w) = WH_{max} - 4\};\ W_3^- = \{w: F(w) = -(WH_{max} - 4)\}.$$

Коли таблиця істинності змінюється рівно в одному місці, всі *WHT* значення змінюються на +2 або -2. З цього виходить, що для збільшення нелінійності всі *WHT* значення в множині W_1^+ повинні бути змінені на -2, всі *WHT* значення в множині W_1^- повинні бути змінені на 2, а також всі *WHT* значення в множині W_2^+ повинні бути змінені на -2, всі *WHT* значення в множині W_2^- повинні бути змінені на 2. Якщо перші дві умови є очевидними, то наступні дві умови потрібні для того, щоб всі інші значення |F(w)| залишалися меншими, ніж WH_{max}. Дані умови можуть бути представлені у вигляді простих тестів.

Теорема 1 [10]. Нехай дана булева функція f(x) з WHT F(w), і визначені множини W+ = $W_1^+ \cup W_2^+$ і W- = $W_1^- \cup W_2^-$. Тоді для входу x існує елемент з *Improvement Set* і виконуються такі дві умови:

(i) f(x)= Lw(x) для всіх w ∈ W+, і

(ii) f(x) X Lw(x) для всіх w ∈ W-.

Якщо функція *f(x)* не збалансована, пониження незбалансованості може бути досягнуте використанням додаткового обмеження:

(iii) якщо F(0)> 0, f(x)= 0, інакше f(x)= 0.

Розглянемо наступний *приклад*. Нехай дана таблиця істинності (стовпець 2 табл. 1) деякої булевої функції, а також відповідні значення перетворення Уолша-Адамара *WHT* (стовпець 3 табл. 1). Необхідно, якщо це можливо, підвищити нелінійність заданої послідовності.

Як видно з наведеної таблиці, максимальне значення WH_{max} = 8 досяжно для w = 0101 і w = 1110. Значень перетворень, рівних $WH_{max} - 2 = 6$, не існує, тому W_1^+ = {0101, 1110} і $W_1^- = W_2^+ = W_2^-$ =

ϕ. Тоді згідно з теоремою 1 значеннями-кандидатами для множини $1 - IS_f$ будуть такі значення x, для яких L0101(x)= L1110(x)= f(x). Таким чином, $1 - IS_f$ = = {0000, 0011, 0100, 0111, 1001, 1010, 1101, 1110} і комплементація будь-якого біта у відповідній позиції таблиці істинності (стовпець 2) спричинить за собою збільшення нелінійності з $N_f = 0{,}5(2n - WH_{max}) = 4$ до $N_f = 5$.

Таблиця 1

Демонстрація методу градієнтного підйому

x/w	f(x)	F(w)	$L_{0101}(x)$	$L_{1110}(x)$	$x \in 1 - IS_f$
0000	0	0	0	0	√
0001	1	4	1	0	
0010	0	0	0	1	
0011	1	4	1	1	√
0100	1	4	1	1	√
0101	1	8	0	1	
0110	1	-4	1	0	
0111	0	0	0	0	√
1000	0	-4	0	1	
1001	1	0	1	1	√
1010	0	-4	0	0	√
1011	0	0	1	0	
1100	0	0	1	0	
1101	0	4	0	0	√
1110	1	8	1	1	√
1111	1	-4	0	1	

Таким чином, теорема 1 дає конструктивний механізм підвищення нелінійності початкової булевої функції за допомогою ітеративної покрокової комплементації позицій у таблиці істинності. Крім того, зауваження (iii) дає механізм пониження незбалансованості даної послідовності. Як видно з наведеного прикладу, використання результатів теореми 1 дозволяє за кінцеве число кроків підвищити нелінійність булевої функції при збереженні її збалансованості.

Обговорюючи наведений метод, можна відзначити, що отримані послідовності мають вищу нелінійність, ніж послідовності, що генеруються функціями, побудованими відповідно до методів алгебри, і, нарівні з іншими евристичними методами, розглянутий підхід гарантує досягнення нелінійності, найбільш близької до верхньої межі нелінійності. У той же час даний метод має меншу обчислювальну складність у порівнянні з іншими евристичними методами і є їх складовою частиною як метод, що дозволяє досягати високої нелінійності.

Аналіз евристичних методів показує, що основні обчислювальні витрати відбуваються за рахунок повторюваних ітеративних процедур, покликаних підвищити певні показники стійкості. Відповідно, знизити дані обчислювальні витрати можна за рахунок зменшення кількості відповідних процедур. Як наслідок, це має на увазі, що початковими даними для цих методів повинні бути функції, що вже мають достатньо високі показники стійкості.

Проте всі евристичні методи припускають, що початковими даними є довільно вибрані функції, іншими словами, це в кращому разі випадковим чином збалансовані нелінійні послідовності. Саме за рахунок багатокрокової процедури підвищення нелінійності евристичні методи стають такими трудомісткими, не гарантуючи при цьому успішної модифікації кожної вхідної послідовності.

Ефективним шляхом вирішення даної проблеми, на наш погляд, є використання як вхідних даних не послідовностей, які згенеровані випадковим чином, а бент-послідовностей (бент-функцій), що дозволить якісним чином знизити обчислювальну складність даних методів і досягти високих показників стійкості. Для аргументації викладеного використовуємо такі міркування. Відомо, що стійкість перетворень у симетричних схемах перетворення інформації визначається, перш за все, ступенем нелінійності перетворень. При цьому верхньої межі нелінійності N_f над $GF(2^n)$ можуть досягати тільки бент-функції [4]. Дані функції мають декілька привабливих властивостей [4]: бент-функції мають максимальну нелінійність; бент-функції задовольняють критерій поширення КР(n); бент-функції мають нульові значення автокореляції. Так, для бент-функцій справедливі такі вирази [4]:

$$d(f_б, A) = N_f = 2^{n-1} - 2^{n/2-1}; \quad (1)$$

$$d(f_б, £) = 2^{n-2}; \quad (2)$$

$$AC(f) = 0, \quad (3)$$

де A і £ – множина афінних функцій і лінійних структур відповідно.

Проте використанню бент-функцій у чистому вигляді перешкоджає той факт, що їх послідовності не збалансовані, що робить їх уразливими до статистичного аналізу [4]:

$$|\{x \mid f(x)= 0\}| \neq |\{x \mid f(x)= 1\}| \neq 2^{n-1}.$$

Оскільки бент-функції мають три максимально досяжні показники стійкості, видається доцільним знайти способи перетворення бент-послідовностей у збалансовані послідовності з мінімально можливими втратами щодо інших показників.

Твердження 1 [4]. Нехай задана бент-послідовність довжини 2^n, що містить $2^{n-1} + 2^{n/2-1}$ одиниць і $2^{n-1} - 2^{n/2-1}$ нулів, або навпаки. Тоді комплементарне доповнення $2^{n/2-1}$ позицій у бент-послідовності приводить до збалансованої функції над V_n, що має нелінійність принаймні

$$Nf \leq 2n-1 - 2n/2. \quad (4)$$

Відзначимо, що дана нелінійність є задовільною, проте запропонований спосіб не надає ефективного інструментарію, використання якого забезпечувало б не тільки отримання збалансованих послідовностей, але й послідовностей, нелінійність яких була б максимально наближеною до теоретично досяжною; сама по собі збалансованість ще не свідчить про те, що і інші показники стійкості будуть високими.

Концепція побудови нашого методу базується на розвитку ідей, запропонованих у [4] та [10]. Як вхідні дані розглядаються бент-послідовності, що мають свідомо привабливими криптографічними властивості. Для перетворення бент-послідовностей

у збалансовані послідовності використовується ідея Майєра-Штаффельбаха [4], згідно з якою необхідно комплементувати $2^{n/2-1}$ позицій у бент-послідовності. Як інструментарій, що дозволяє ефективно здійснювати дану комплементацію, використовується ідея Міллана-Кларка [10]. Основною відмінною рисою запропонованого методу від методу Міллана-Кларка (методу градієнтного підйому) є те, що він дозволяє не підвищувати, а знижувати нелінійність функцій, які мають максимальну нелінійність. Метою методу є мінімально-можливе пониження нелінійності при кожній з $2^{n/2-1}$ обов'язкової комплементації послідовності. Пониження нелінійності функції, що свідомо мають високі показники стійкості, шляхом приведення її до збалансованого вигляду за рахунок покрокового градієнтного спуску дозволяє при мінімальних втратах нелінійності отримати криптографічнн стійку функцію з високими показниками стійкості.

Теорема 1. Булева функція, яка відповідає послідовності, утвореній комплементарним доповненням $2^{n/2-1}$ позицій у бент-послідовності над векторним простором V_n, є збалансованою криптографічною функцією з показником нелінійності, що задовольняє вираз (4).

Доведення. Відповідно до твердження 1 послідовність, утворена комплементарним доповненням $2^{n/2-1}$ позицій у бент-послідовності над векторним простором V_n, є збалансованою послідовністю з показником нелінійності, що задовольняє виразу (4). Відповідно до визначення нелінійність булевої функції визначається нелінійністю відповідної послідовності і навпаки. Отже, булева функція, яка відповідає послідовності, утвореній комплементарним доповненням $2^{n/2-1}$ позицій у бент-послідовності, є криптографічною збалансованою функцією з показником нелінійності, що задовольняє (4).

Теорема 1 дає конструктивний механізм визначення криптографічних булевих функцій шляхом пониження ступеня нелінійності бент - послідовності для приведення її до збалансованого вигляду. Сукупність виконуваних процедур і операцій надалі називатимемо *методом градієнтного спуску*.

Вихідними даними етапу приведення функції до збалансованого вигляду є високонелінійні збалансовані послідовності. У зв'язку з цим за наявності високо нелінійних послідовностей $\xi = \varepsilon_0\varepsilon_1\ldots\varepsilon_{2^n-1}$, де n – розмірність векторного простору, викликає інтерес відновлення зовнішнього вигляду функції, яка згенерувала задану послідовність, з метою обговорення інших показників стійкості і, у разі потреби, подальшої модифікації функції з метою поліпшення її стійкості, а також можливості відбору функцій з якнайкращими показниками стійкості.

У рамках запропонованого методу вихідні дані етапу приведення функції до збалансованого вигляду приводяться до алгебраїчної нормальної форми способом, указаним у [16], після чого отримані функції перетворяться у функції, що задовольняють критерій поширення за допомогою способу, указаного в [15]. Так, у [16] представлений спосіб відновлення алгебраїчної нормальної форми функції за її вихідною послідовністю ξ. Даний спосіб ґрунтується на використанні такі леми.

Лема 1 [16]. Нехай ξ – послідовність деякої функції *f* над V_n. Тоді існують процедури відновлення алгебраїчної нормальної форми функції $f(x_1,\ldots,x_n)$ за відомою послідовністю $\xi = \varepsilon_0\varepsilon_1\ldots\varepsilon_{2^n-1}$.

Таким чином, використання леми 1 дозволить нам, за наявності деяких високо нелінійних послідовностей, відновлювати алгебраїчно нормальні форми булевих функцій, отриманих в процесі застосування запропонованого методу. Наявність алгебраїчної нормальних форм дозволить, у свою чергу, обговорювати такі показники стійкості, як алгебраїчна ступінь і критерій поширення (строгий лавинний критерій).

Далі, для отримання функцій, що задовольняють критерій поширення доцільним видається використання такої леми і теореми.

Лема 2 [16]. Збалансованість, нелінійність і кількість векторів, відповідно яких функція задовольняє критерій поширення, є інваріантними відносно афінних перетворень координат функції.

Теорема 2 [16]. Нехай *f* є функцією над V_n і A є несингулярною матрицею порядку n над GF(2). Якщо $f(x) \oplus f(x \oplus \gamma)$ є збалансованою для кожного рядка γ матриці A, то $\psi(x) = f(xA)$ задовольняє строгий лавинний критерій.

Таким чином, лема 2 і теорема 2 свідчать про те, що за наявності деякої нелінійної булевої функції можлива модифікація даної функції шляхом афінних перетворень, результатом яких, при фіксованій нелінійності, збалансованості і кількості векторів, що задовольняють критерію поширення, буде функція, яка задовольняє строгий лавинний критерій.

На підставі викладених теорем і лем сформулюємо таку теорему.

Теорема 4. Функції, побудовані на основі використання методу градієнтного спуску з подальшим застосуванням процедур відновлення алгебраїчної нормальної форми булевої функції та аффінних перетворень, є збалансованими, мають нелінійністю $N_f \geq 2^{n-1} - 2^{n/2}$, задовольняють строгий лавинний критерій і мають високий алгебраїчний ступінь, рівний $\deg(f) \leq n - 1$, де n – розмірність векторного простору.

Доведення. Відповідно до теореми 1 булеві функції, отримані в результаті виконання градієнтного спуску, є збалансованими і мають нелінійність, що задовольняє співвідношення (4). Конструктивність процедури відновлення алгебраїчної нормальної форми, функції задається лемою 1, при цьому ступінь функції, що відповідає модифікованій бент-послідовності, задовольняє співвідношення $\deg(f) \leq n - 1$, де n – розмірність векторного простору. Лема 2 встановлює інваріантність нелінійності відносно афінних перетворень, а теорема 2 гарантує при цьому приведення функції до вигляду, який задовольняє строгий лавинний критерій. Отже, функції, побудовані на основі використання методу градієнтного спуску з подальшим застосуванням процедур відновлення алгеб-

раїчної нормальної форми булевої функції і відповідних афінних перетворень крім збалансованості та високої нелінійності задовольнятимуть строгий лавинний критерій, що і завершує доведення.

ВиЯновки

Таким чином, теоретично обгрунтована можливість формування збалансованих криптографічних булевих функцій з високими показниками нелінійності і ступеня алгебри, що задовольняють строгий лавинний критерій. Сформульована і доведена теорема 4, яка встановлює параметри криптографічних булевих функцій, що формуються в результаті пропонованого підходу. Важливим напрямом подальших досліджень є розробка практичних алгоритмів, які реалізують запропонований підхід.

СпиЯок літератури

1. *Барсуков В.С., Дворянкин С.В., Шеремет И.И. Технологии электронных коммуникаций; В 20 т. Т. 20: Безопасность связи в каналах телекоммуникаций – М.: Электронные знания, 1992. – 122 с.*
2. *Захист інформації в комп'ютерних системах від несанкціонованого доступу / За ред. С.Г. Лаптєва. – К.: Наук. думка,, 2001. – 321 с.*
3. *Горбенко И.Д., Потий А.В., Избенко Ю.А. Исследование аналитических и статистических свойств булевых функций криптоалгоритма Rijndael (FIPS 197) // Радиотехника: Всеукраинский межведомственный научно-технический сборник. – Х.: ХНУРЭ, 2004. – № 126. – С. 132-138.*
4. *Maier W., Staffelbach O. Nonlinearity criteria for cryptographic functions // Advances in Cryptology – EUROCRYPT'89, vol.434, Lecture Notes in Computer Science, Springer-Verlag, 1990. – P. 549-562.*
5. *Кузнецов А.А., Избенко Ю.А., Юкальчук А.А. Анализ известных методов построения высоко нелинейных булевых функций // Вісник НТУ "ХПІ". – Х.: НТУ "ХПІ", 2004. – № 18. – С. 91-96.*
6. *Maitra S., Pasalic E. Further constructions of resilient Boolean functions with very high nonlinearity // Accepted in SETA, May, 2001, Norway.*
7. *Pasalic E., Johansson T. Further Results on the Relation Between Nonlinearity and Resiliency // IEEE Trans. on Information Theory, Vol 48, No. 7, July 2002. – P. 1825-1834.*
8. *Pasalic E., Johansson T., Maitra S., Sarkar P. New constructions of resilient and correlation immune Boolean functions achieving upper bounds of nonlinearity // Workshop of Coding and Cryptography, Electronic Notes in Discrete Mathematics. Elsevier, January 2001.*
9. *Maity S., Johansson T. Construction of Cryptographically Important Boolean Functions // INDOCRYPT 2002, Volume 2551 in Lecture Notes in Computer Science, , Springer Verlag, 2002.– P. 234–245.*
10. *Millan W., Clark A., Dawson E. Smart Hill Climbing Finds Better Boolean Functions // Workshop on Selected Areas in Cryptography. (SAC'97), 1997. – P. 50.*
11. *Millan W., Clark A., Dawson E. An effective genetic algorithm for finding highly nonlinear Boolean functions // First International Conference on Information and Communications Security, 1997. – P. 149-158.*
12. *Clark J., Jacob J., Stepney S., Maitra S., Millan W. Evolving of Boolean functions satisfying multiple criteria // Proc. of INDOCRYPT'02. – LNCS vol 2551. – P. 246-259.*
13. *Millan W., Clark A., Dawson E. Heuristic Design of Cryptographically Strong Balanced Boolean Functions // Advances in Cryptology EUROCRYPT'98. – Springer Verlag LNCS 1403, 1998. – P. 489–499.*
14. *Millan W., Clark A., Dawson E. Boolean function design using hill climbing methods // 4th Australasian Conference on Information, Security and Privacy, number 1587 in Lecture Notes in Computer Science. – Springer Verlag, April 1999. – P. 1–11.*
15. *Потий А.В., Избенко Ю.А. Обоснование выбора метода построения криптографически стойких булевых функций // Радиотехника: Всеукр. начно-техн. сборн. – Х.: ХНУРЭ, 2002. – Вып. 126. – С. 132-137.*
16. *Seberry J., Zhang M., Zheng Y. Nonlinearity and Propagation Characteristics of Balanced Boolean Functions // Information and Computation. – 1995. – Vol. 119. – P. 1-13.*

Надійшла до редколегії 5.10.2006

Рецензент: д-р техн. наук, проф. Ю.В. Стасєв, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

трафіка тощо). Вирішенню завдання статистичного аналізу присвячена значна кількість робіт [1 – 5]. У них розглядаються алгоритми статистичного аналізу випадкових величин і пропонуються оптимальні алгоритми ухвалення рішень при заданих критеріях якості. Одним з найбільш поширених у теперішній час критеріїв є критерій максимальної правдоподібності, згідно з яким при спостереженні вибірки приймається та з гіпотез, якій відповідає більше значення функції правдоподібності вибірки. Алгоритм, який ґрунтується на цьому критерії, одержав назву алгоритму максимальної правдоподібності, і у ряді випадків (наприклад, для гаусового розподілу стохастичної величини) достатньо повно збігається з оптимальним алгоритмом. Але останнім часом значний практичний інтерес здобули процеси, які не можна описувати як нормальні випадкові процеси, і для таких процесів, які підлягають негаусовим розподілам (наприклад, гіперболічний, ступеневий, Вейбулла та ін.) [6 – 8], застосовність алгоритму максимальної правдоподібності викликає сумніви. От чому аналіз негаусових розподілів випадкових величин і аналіз поведінки оцінки параметрів такого розподілу є **актуальним науковим завданням**.

Метою даної статті є аналіз застосовності методу максимальної правдоподібності та розробка методів оцінювання невідомих параметрів.

Результати теоретичних досліджень

Розглянемо ряд прикладів, до яких метод максимальної правдоподібності не придатний, і слід проводити оцінки невідомих параметрів іншими методами. Уявимо, що проводиться прийом або подовжньої, або поперечної складової вектора поляризації електромагнітного поля $\vec{E}$. Припустимо, що можливо зміряти тільки подовжню компоненту даного вектора (рис. 1) E_t, яка може набувати значень від $E = \left|\vec{E}\right|$ до 0.

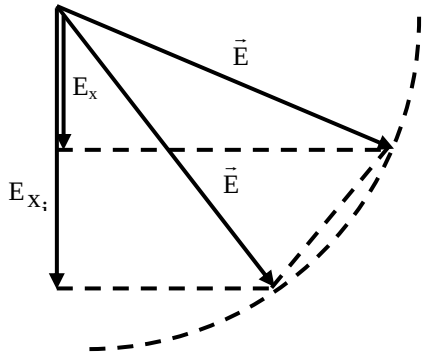

Рис. 1. Розклад вектора поляризації
на подовжню компоненту електромагнітного поля

Як легко бачити з простих геометричних міркувань, щільність імовірності того, що в довільний момент часу значення подовжньої компоненти E_t дорівнює E_x, має вигляд:

$$p(E;E_x)=\begin{cases}\dfrac{1}{E} & \text{при} \quad 0 \le E_x \le E;\\ 0 & \text{при} \quad E_x > E.\end{cases} \qquad (1)$$

Припустимо, що ми вимірювали подовжню компоненту вектора електромагнітного поля N разів, тобто одержали такий набір вимірювань:

$$\tilde{E}_x = E_{x_1}, E_{x_2}, ..., E_{x_N}.$$

Імовірність одержати набір $\tilde{E}_x$ дорівнює:

$$p(E,\tilde{E}_x)=\begin{cases}\left(\dfrac{1}{E}\right)^N & \text{при } 0 \le \tilde{E}_x \le E;\\ 0 & \text{при } \tilde{E}_x > E.\end{cases} \qquad (2)$$

Застосуємо для оцінки (2) принцип максимальної правдоподібності:

$$p(E';\tilde{E}_x) = \max \text{ при} \quad E' = \overline{E}. \qquad (3)$$

Із співвідношення (3) випливає умова:

$$\overline{E} = E_{x_{max}},$$

де $E_{x_{max}}$ – найбільша з компонент величини $\tilde{E}_x$.

Насправді, із спаданням E' ймовірність $p(E';\tilde{E}_x)$ зростає доти, поки E' не стане меншим за яке-небудь зміряне значення E_{x_i}.

Очевидно, що оцінка (3) дає прийнятне значення $\overline{E}$, але в той же час цей результат є випадковим, оскільки даний розподіл істотно відрізняється від гаусового, і тому умову максимальної правдоподібності не можна строго обґрунтувати, як це зроблено в [1]. Крім того, значення величини E більше значення $E_{x_{max}}$ через те, що ймовірність появи серед усіх можливих значень компонент вектора $E_{x_{max}}$ компоненти, яка в точності дорівнює E, нульова.

Для отримання більш обґрунтованої оцінки величини E розглянемо ймовірність того, що всі N значень величини E_x лежать у заданому інтервалі

$$0 \le E_{x_i} \le E_x < E \quad \text{при} \quad i = 1,2,...,N. \qquad (4)$$

Імовірність виконання нерівності (4) має вигляд:

$$p_N(E;E_x)=\left(\frac{E_x}{E}\right)^N.$$

Введемо дві величини $E_{x_1}(\varepsilon)$ і $E_{x_2}(\varepsilon)$ такі, що імовірність виконання кожної з умов

$$E_{x_{max}} < E_{x_2}(\varepsilon) \quad \text{та} \quad E_{x_{max}} > E_{x_1}(\varepsilon)$$

дорівнює $1-\varepsilon$.

Тоді маємо:

$$\left(\frac{E_{x_1}(\varepsilon)}{E}\right)^N = \varepsilon \quad \text{та} \quad \left(\frac{E_{x_2}(\varepsilon)}{E}\right)^N = 1-\varepsilon,$$

звідки з урахуванням того, що $-\ln\varepsilon << N$, можна одержати такі співвідношення:

$$E_{x_1} = E\varepsilon^{1/N} \sim E\left(1+\frac{\ln\varepsilon}{N}\right);$$

$$E_{x_2} = E(1-\varepsilon)^{1/N} \sim E\left(1-\frac{\varepsilon}{N}\right).$$

Тому можна стверджувати, що з великою імовірністю виконується нерівність:

$$E_{x_{max}}(1-\varepsilon)^{-1/N} < E < E_{x_{max}}\varepsilon^{-1/N},$$

якщо припустити, що

$$-\frac{\ln\varepsilon}{N} << 1.$$

Також можна скласти і таке співвідношення:

$$E_{x_{max}}\left(1+\frac{\varepsilon}{N}\right) < E < E_{x_{max}}\left(1-\frac{\ln\varepsilon}{N}\right). \qquad (5)$$

Одержана оцінка (5) при достатньо великих N виявляється дуже точною. Особливо цікаво те, що інтервал (5) спадає пропорційно, а не як $1/\sqrt{N}$, що характерне для розподілу Пуассона.

Знайдемо ще одну оцінку, використовуючи середнє значення $\overline{E}_x$ результатів вимірювань. Якщо визначити середнє значення як:

$$\overline{E}_x = \frac{1}{N}\sum_{i=1}^{N} E_{x_i}$$

і враховуючи незалежність всіх значень E_{x_i}, можна набути значення математичного сподівання і дисперсії величини $\overline{E}_x$:

$$M\left[\overline{E}_x\right] = \frac{1}{2}E, \quad D\left[(\overline{E}_x)\right] = \frac{E^2}{12N}.$$

Розподіл величини $\overline{E}_x$ (при не дуже малих N) схожий на гаусовий розподіл, і тому можна припустити:

$$\left|\overline{E}_x - \frac{E}{2}\right| < \frac{\alpha E}{\sqrt{12N}}, \quad \text{при } \alpha = 3 \quad \text{або } \alpha = 4,$$

і тоді, цілком імовірно, можна одержати такі оцінки для величини E:

$$2\overline{E}_x \Big/ \left(1+\frac{\alpha}{\sqrt{3N}}\right) < E < 2\overline{E}_x \Big/ \left(1=\frac{\alpha}{\sqrt{3N}}\right). \qquad (6)$$

Межі помилки визначення модуля напруженості електричного поля, одержані в результаті оцінки N вимірювань його подовжньої складової, представлені на рис. 2, як функції від кількості вимірювань при фіксованому значенні $\varepsilon = 3\cdot10^{-3}$.

Внутрішні криві графіка одержані на підставі співвідношення (5), а зовнішні – співвідношення (6). Відмітимо, що оцінка (5), що дає інтервал значень, який змінюється обернено пропорційно до кількості вимірювань N, не враховує помилку вимірювання величини E. Урахування такої помилки призводить до того, що для великих значень N інтервал значень визначається в основному стандартною помилкою вимірювання величини E і змінюється обернено пропорційно до квадратного кореня з кількості вимірювань.

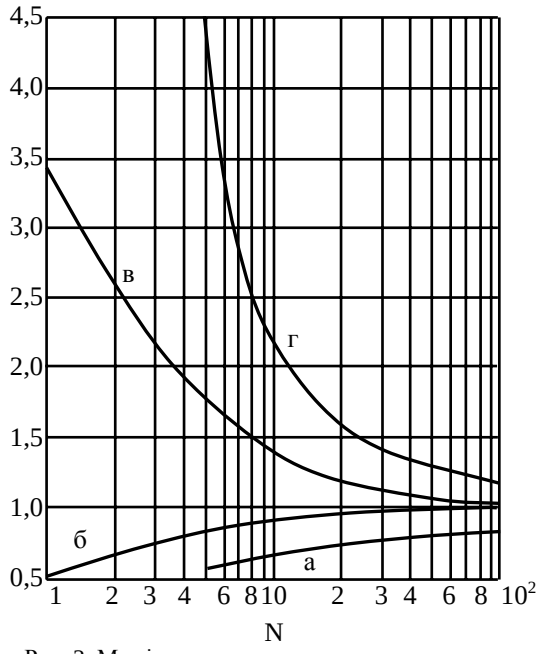

Рис. 2. Межі помилки визначення модуля напруженості електричного поля:
а, г – межі помилки при $N \sim 3\cdot10 - 3\cdot10^2$
б, в – межі помилки при $N > 3\cdot10^3$

ВиЯновки

У результаті проведених досліджень установлено. що:

– для випадкової величини, функція розподілу якої описується показовою функцією, метод максимальної правдоподібності не може бути застосовний;

– запропонований спосіб визначення невідомих параметрів розподілу дозволив провести оцінки математичного сподівання та дисперсії стохастичної величини;

– у результаті аналізу наведеного розподілу встановлено, помилка вимірювання невідомої величини змінюється обернено пропорційно до квадратного кореня з кількості вимірювань, а не обернено пропорційно до кількості вимірювань, що характерне для нормального розподілу.

СпиЯок літератури

1. *Левин Б.Р. Теоретические основы статистической радиотехники. Кн. 1. – М.: Сов. радио, 1974. – 552 с.*

2. *Директор С., Рорер Р. Введение в теорию систем. – М.: Мир, 1974. – 644 с.*

3. *Стрелков А.И.,. Можаев А.А., Марченко В.В. К вопросу о разрешающей способности монохроматических радиосигналов по частоте акустооптических спектроанализаторов // Системи обробки інформації. – Х.: ХВУ, 2002. – Вип. 6 (22). – С. 46-50.*

4. *Стрелков А.И., Барсов В.И., Можаев А.А., Лытюга А.П., Коротков В.В. Пространственно-временная обра-*

ботка сигналов малой длительности в акустооптических анализаторах спектра // Моделювання та інформаційні технології. – К.: ІПМЕ, 2003. – Вип. 22. – С. 184-195.

5. *Можаев А.А. Оценка достоверности определения параметров телекоммуникационнного трафика // Системи обробки інформації. – Х.: ХУ ПС, 2006. – Вип. 9(58). – С. 59-61.*

6. *Фрактальный анализ процессов, структур и сигналов // Кучук Г.А., Можаев А.А., Пащенко Р.Э, Рук кас К.М. Коллективная монография. – Х.: ЭкоПерспектива, 2006. – 360 с.*

7. *Кучук Г.А., Можаєв О.О., Воробйов О.В. Метод прогнозування фрактального трафіка // Радіоелектронні і комп'ютерні системи. – 2006. – № 6(18). – С. 181-188.*

8. *Кучук Г.А., Можаєв О.О., Воробйов О.В. Аналіз та моделі самоподібного трафіка // Авиационно-космическая техника и технология. – 2006. – № 9(35). – С. 173-180.*

Надійшла до редколегії 16.08.2006

Рецензент: доктор технічних наук, професор І.І. Обод, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.