Мохор Владимир Владимирович, доктор технических наук, профессор, директор Института проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины.
E-mail: v.mokhor@gmail.com
Мохор Володимир Володимирович, доктор технічних наук, професор, директор Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України.
Mokhor Volodymyr, doctor of engineering science, professor, Director of Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine.

Бакалинский Александр Олегович, заместитель заведующего кафедрой Института специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского».
E-mail: baov@meta.ua
Бакалинский Олександр Олегович, заступник завідувача кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
Bakalynskyi Oleksandr, deputy head of department, Institute of special communications and information security National technical university of Ukraine «Igor Sikorsky Kyiv polytechnic institute».

Богданов Александр Михайлович, доктор технических наук, профессор, заведующий кафедрой Института специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского».
E-mail: a_m_bogdanov@inbox.ru
Богданов Олександр Михайлович, доктор технічних наук, професор, завідувач кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
Bohdanov Oleksandr, doctor of engineering science, professor, head of department, Institute of special communications and information security National technical university of Ukraine «Igor Sikorsky Kyiv polytechnic institute».

Цуркан Василий Васильевич, кандидат технических наук, доцент кафедры Института специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского».
E-mail: v.v.tsurkan@gmail.com
Цуркан Василь Васильович, кандидат технічних наук, доцент кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
Tsurkan Vasyl, candidate of engineering science, associate professor, Institute of special communications and information security National technical university of Ukraine « Igor Sikorsky Kyiv polytechnic institute».

DOI: 10.18372/2410-7840.19.11435
УДК 621.391:519.2

НИЖНІ МЕЖІ ІНФОРМАЦІЙНОЇ СКЛАДНОСТІ КОРЕЛЯЦІЙНИХ АТАК НА ПОТОКОВІ ШИФРИ НАД ПОЛЯМИ ПОРЯДКУ 2^r

Антон Олексійчук, Михайло Поремський

Кореляційні атаки відносяться до найбільш потужних атак на потокові шифри, а методи побудови таких атак та обґрунтування стійкості потокових шифрів відносно них утворюють розвинутий напрям сучасної криптології. Протягом останніх років у зв'язку з появою словоорієнтованих потокових шифрів спостерігається розвиток методів побудови кореляційних атак, що базуються на розв'язанні систем лінійних рівнянь зі спотвореними правими частинами над скінченними полями або кільцями лишків порядку $q \geq 2$. *В даній статті досліджується два таких методи, перший з яких полягає у розв'язанні зазначених систем рівнянь над полями порядку* 2^r, *де* $r \geq 2$, *а другий – у розв'язанні аналогічних систем рівнянь над полем з двох елементів. Отримано неасимптотичні нижні межі інформаційної складності зазначених атак, які уточнюють раніше відому евристичну оцінку. Отримані результати можуть бути використані при обґрунтуванні стійкості словоорієнтованих потокових шифрів відносно сучасних кореляційних атак.*
Ключові слова: *потоковий шифр, кореляційеа атака, система рівнянь зі спотвореними правими частинами над скінченним полем, інформаційна складність.*

Вступ. Один з найбільш потужних класів атак на потокові шифри утворюють кореляційні атаки, сутність яких полягає у складанні та розв'язанні булевих систем лінійних рівнянь зі спотвореними правими частинами [3, 5, 11, 12]. Протягом останніх років у зв'язку з появою словоорієнтованих потокових шифрів спостерігається розвиток методів розв'язання систем лінійних рівнянь зі спотвореними правими частинами над скінченними полями або кільцями лишків порядку 2^r, де $r \geq 2$. Відзначимо роботи [1, 2] та [13], в останній з яких запропоновано кореляційну атаку на потоковий шифр SNOW 2.0, яка базується на розв'язанні системи рівнянь (СР) зі спотвореними правими частинами над полем порядку 2^8.

Як правило, будь-яка кореляційна атака складається з двох етапів, на першому з яких, виходячи з аналізу потокового шифру, тим чи іншим способом будується (не обов'язково булева) система лінійних рівнянь зі спотвореними правими частинами відносно початкового стану генератора гами шифру. Далі, на другому етапі атаки, зазначена система рівнянь розв'язується за допомогою відомих методів. При цьому одним з найважливіших параметрів, що характеризують ефективність кореляційної атаки, є її *інформаційна складність* (date complexity) – мінімальна кількість рівнянь у зазначеній системі, необхідних для її розв'язання із заданою ймовірністю помилки.

Звичайно отримання нижніх меж інформаційної складності, які надають можливість оцінювати найменшу кількість рівнянь у системах зі спотвореними правими частинами, необхідних для їх надійного розв'язання *незалежно від способу отримання та методу розв'язання таких систем*, є першим кроком на шляху обґрунтування стійкості довільного потокового шифру відносно кореляційних атак (див., наприклад, [4]). Проте на сьогодні для шифрів, що будуються над полями порядку 2^r, де $r \geq 2$, відома лише евристична оцінка інформаційної складності [13], яка (саме внаслідок її евристичного характеру) не може бути покладена в основу належного наукового обґрунтування стійкості потокових шифрів відносно кореляційних атак.

Метою даної статті є отримання обґрунтованих неасимптотичних нижніх меж інформаційної складності двох видів атак, які базуються на розв'язанні систем лінійних рівнянь зі спотвореними правими частинами над полями порядку 2^r, де $r \geq 2$, та над полем з двох елементів відповідно. Отримані межі є справедливими *для будь-яких кореляційних атак на довільні словоорієнтовані потокові шифри незалежно від способу побудови* (*або методу розв'язання*) *системи лінійних рівнянь зі спотвореними правими частинами*, *яка складається на першому етапі атаки*. Ці межі уточнюють раніше відому евристичну оцінку інформаційної складності [13] та можуть бути використані для обґрунтування стійкості сучасних потокових шифрів відносно як відомих, так і перспективних кореляційних атак.

Показано також, що інформаційна складність атак, які базуються на розв'язанні булевих систем лінійних рівнянь, є не менше (проте, може і дорівнювати) складності атак, що базуються на безпосередньому розв'язанні систем лінійних рівнянь зі спотвореними правими частина над полями порядку більшого ніж 2.

Постановка задачі та основні результати. Розглянемо систему рівнянь зі спотвореними правими частинами

$$Ax = b, \qquad (1)$$

де A – $m \times n$-матриця над полем F_q, $q = 2^r$, b – вектор довжини m з координатами

$$b_i = A_i a \oplus \xi_i, \; i \in \overline{1, m}, \qquad (2)$$

де $A_1, \ldots, A_m$ – рядки матриці A, $a = (a_1, \ldots, a_n)^{\mathrm{T}}$ – невідомий вектор над полем F_q (істинний розв'язок СР (1)), $\xi_1, \ldots, \xi_m$ – незалежні випадкові величини, розподілені за законом $\mathbf{P}\{\xi_i = z\} = p(z)$, де $p(z) \geq 0$ для кожного $z \in F_q$, $\sum_{z \in F_q} p(z) = 1$. Далі вважатимемо, що стовпці матриці A є лінійно незалежними векторами над полем F_q. Задача розв'язання СР (1) полягає у відновленні вектора a за відомими матрицею A, вектором b і розподілом ймовірностей $p_\xi = (p(z) : z \in F_q)$.

Звичайно до розв'язанні СР зі спотвореними правими частинами приводить побудова кореляційних атак на потокові шифри. При цьому, як правило, вектор a є початковим заповненням одного чи декількох лінійних регістрів зсуву, що входять до складу генератора гами шифру, вектор b є відповідним відрізком гами, а вектор спотворень $\xi = (\xi_1, \ldots, \xi_m)$ отримується в результаті заміни нелінійних компонент генератора їх лінійними наближеннями над полем F_q.

Припустимо, що матриця A є фіксованою. В цьому випадку будь-який алгоритм відновлення вектора a з системи рівнянь (1) задається певним

відображенням $D_A : F_q^{\,m} \to F_q^{\,n}$, яке ставить у відповідність вектору b з координатами (2) "оцінку" вектора a. При цьому (середня) ймовірність помилки алгоритму визначається за формулою $\delta(D_A) = q^{-n} \sum_{a \in F_q^{\,n}} \mathbf{P}\{D_A(b) \neq a\}$.

Для будь-якого $\delta \in (0, 1/2)$ інформаційна складність атаки, що базується на розв'язанні СР вигляду (1), визначається як найменше число m рівнянь у системі, для якого існує алгоритм її розв'язання з ймовірністю помилки не більше ніж δ. Іншими словами, інформаційна складність – це найменший обсяг матеріалу, необхідного для відновлення вектора a з ймовірністю не менше ніж $1-\delta$.

В [13] (теор. 5) наведено евристичну межу інформаційної складності кореляційних атак, що базуються на розв'язанні СР вигляду (1):

$$m \approx \frac{2nr}{\Delta(p_\xi)} \ln 2, \qquad (3)$$

де

$$\Delta(p_\xi) = q^{-1} \sum_{z \in F_q} (qp(z) - 1)^2. \qquad (4)$$

Наступна теорема уточнює зазначений результат.

Теорема 1. Нехай m є найменшим числом рівнянь у системі (1), для якого існує алгоритм її розв'язання з ймовірністю помилки не більше ніж $\delta \in (0, 1/2)$. Тоді

$$m \geq \frac{nr(1-\delta) - h(\delta)}{\Delta(p_\xi)} \ln 2, \qquad (5)$$

де $\Delta(p_\xi)$ визначається за формулою (4), $h(\delta) = -\delta \log_2 \delta - (1-\delta)\log_2(1-\delta)$.

Доведення. Помітимо, що вектор b з координатами (2) є результатом передачі випадкового повідомлення Aa (де вектор a має рівномірний розподіл на множині $F_q^{\,n}$) дискретним симетричним каналом без пам'яті, а саме, каналом з адитивним шумом на групі $(F_q, +)$. Пропускна здатність такого каналу дорівнює $C_\xi = \log_2 q - H(p_\xi) = r - H(p_\xi)$, де $H(p_\xi) = -\sum_{z \in R} p(z) \log_2 p(z)$ – ентропія розподілу p_ξ [9, с. 118].

Розглянемо довільне відображення $D_A : F_q^{\,m} \to F_q^{\,n}$ таке, що $\delta(D_A) \leq \delta$. На підставі відомих властивостей взаємної інформації та ентропії (див., наприклад, [9, с. 22]), а також лінійної незалежності стовпців матриці A над полем F_q справедливі такі співвідношення:

$$nr - H(Aa / D_A(b)) = H(Aa) - H(Aa / D_A(b)) =$$
$$= I(Aa; D_A(b)) \leq I(Aa; b) \leq mC_\xi = m(r - H(p_\xi)).$$

З іншого боку, використовуючи нерівність Фано [9, с. 142], отримаємо, що

$$H(Aa / D_A(b)) \leq \delta(D_A(b))(n \log q - 1) +$$
$$+ h(\delta(D_A(b))) \leq \delta nr + h(\delta).$$

Отже, справедлива нерівність

$$nr - \delta nr + h(\delta) \leq m(r - H(p_\xi)). \qquad (6)$$

Нарешті, використовуючи оцінку $\ln x \leq x - 1$, $x > 0$, отримаємо, що

$$r - H(p_\xi) = (\ln 2)^{-1} \sum_{z \in F_q} p(z) \ln(qp(z)) \leq$$
$$(\ln 2)^{-1} \sum_{z \in F_q} p(z)(qp(z) - 1) = (\ln 2)^{-1} \Delta(p_\xi). \qquad (7)$$

Безпосередньо з формул (6), (7) випливає нерівність (5). Теорему доведено.

Зауважимо, що на відміну від формули (3), вираз у правій частині нерівності (5) явно залежить від параметра δ.

Розглянемо зараз інший підхід до побудови кореляційних атак на потокові шифри, який полягає у розв'язанні СР зі спотвореними правими частинами над полем F_2. Перевагою цього підходу є наявність розвинутих методів розв'язання таких систем рівнянь, на відміну від аналогічних систем над полями більшого порядку (див., наприклад, роботи [8, 10] та наведені там посилання).

Зафіксуємо елемент $c \in F_q \setminus \{0\}$ та пару дуальних базисів α і β поля F_q над полем F_2. Позначимо $\mathrm{Tr}(z) = z \oplus z^2 \oplus \cdots \oplus z^{2^{r-1}}$ абсолютний слід елемента $z \in F_q$ (див., наприклад, [6, 7]). Помітимо, що з рівностей (2) випливають рівності $\mathrm{Tr}(cb_i) = \mathrm{Tr}(A_i(ca)) \oplus \mathrm{Tr}(c\xi_i)$, $i \in \overline{1,m}$, причому $\mathrm{Tr}(A_i(ca))$ є скалярним добутком векторів A_i' та a' над полем F_2, які отримуються в результаті заміни кожної координати вектора A_i (відповідно, вектора ca) її двійковим представленням у базисі α (відповідно, у базисі β). Звідси випливає, що вектор $a' \in F_2^{\,nr}$ співпадає с істинним розв'язком системи рівнянь зі спотвореними правими частинами

$$A_i' x = b_i' = A_i' a' \oplus \eta_i, \; i \in \overline{1,m}, \qquad (8)$$

де $b_i' = \mathrm{Tr}(cb_i)$, $\eta_i = \mathrm{Tr}(c\xi_i)$ для кожного $i \in \overline{1,m}$.

Таким чином, для відновлення вектора a з системи рівнянь (1) достатньо побудувати для заздалегідь вибраного елемента $c \in F_q \setminus \{0\}$ СР вигляду (8) над полем F_2 та відновити її істинний розв'язок a' одним з відомих методів [8, 10]. Знаючи вектор a' та базис β, можна отримати вектор ca, а отже, і шуканий вектор a.

Наступна теорема встановлює нижню межу інформаційної складності кореляційних атак, які будуються за наведеною вище схемою.

Теорема 2. Нехай m є найменшим числом рівнянь у системі (6), для якого існує алгоритм її розв'язання з ймовірністю помилки не більше ніж $\delta \in (0, 1/2)$. Тоді

$$m \geq \frac{nr(1-\delta) - h(\delta)}{|\hat{p}(c)|^2} \ln 2, \qquad (9)$$

де $\hat{p}(c) = \sum_{z \in F_q} p(z)(-1)^{\mathrm{Tr}(cz)}$ є коефіцієнт Фур'є розподілу ймовірностей $p_\xi = (p(z) : z \in F_q)$.

Доведення. Покажемо, що розподіл ймовірностей випадкової величини $\eta_i = \mathrm{Tr}(c\xi_i)$ визначається за формулою

$$\mathbf{P}\{\eta_i = 0\} = 1 - \mathbf{P}\{\eta_i = 1\} = 1/2 \cdot (1 + \hat{p}(c)). \qquad (10)$$

Тоді, згідно з рівністю (4), $\Delta(p_{\eta_i}) = 2^{-1} \sum_{z \in F_2} (2\mathbf{P}\{\eta_i = 0\} - 1)^2 = |\hat{p}(c)|^2$, $i \in \overline{1, m}$, і справедливість нерівності (9) випливає безпосередньо з теореми 1.

Використовуючи послідовно означення випадкової величини η_i, формулу обернення для перетворення Фур'є та лінійність функції сліду (див., наприклад, [7]), отримаємо, що

$$\mathbf{P}\{\eta_i = 0\} = \sum_{x \in F_q : \mathrm{Tr}(cx) = 0} p(x) =$$

$$= \sum_{x \in F_q : \mathrm{Tr}(cx) = 0} \left(q^{-1} \sum_{y \in F_q} \hat{p}(y)(-1)^{\mathrm{Tr}(xy)} \right) =$$

$$= q^{-1} \sum_{y \in F_q} \hat{p}(y) \sum_{x \in F_q : \mathrm{Tr}(cx) = 0} (-1)^{\mathrm{Tr}(xy)} =$$

$$= 2^{-r} \left(2^{r-1} \hat{p}(0) + 2^{r-1} \hat{p}(c) + \sum_{y \in F_q \setminus \{0, c\}} \hat{p}(y) \sum_{x \in F_q : \mathrm{Tr}(cx) = 0} (-1)^{\mathrm{Tr}(xy)} \right) =$$

$$= 1/2 \cdot (1 + \hat{p}(c)),$$

де остання рівність випливає зі співвідношень

$$\sum_{x \in F_q : \mathrm{Tr}(cx) = 0} (-1)^{\mathrm{Tr}(xy)} =$$

$$= |\{x \in F_q : \mathrm{Tr}(xy) = \mathrm{Tr}(cx) = 0)\}| -$$

$$- |\{x \in F_q : \mathrm{Tr}(xy) = 1, \mathrm{Tr}(cx) = 0)\}| = 2^{r-1} - 2^{r-1} = 0,$$

$$y \notin \{0, c\}.$$

Отже, справедлива формула (10), що й треба було довести.

Зауважимо, що на підставі рівності Парсеваля (див, наприклад, [7]), параметр (4) задовольняє рівності $\Delta(p_\xi) = \sum_{c \in F_q \setminus \{0\}} |\hat{p}(c)|^2$, звідки випливає, що значення у правій частині нерівності (9) є не менше значення у правій частині нерівності (5). Таким чином, інформаційна складність кореляційних атак, що базуються на розв'язанні систем рівнянь зі спотвореними правими частинами вигляду (8) є не менше інформаційної складності атак, які базуються на безпосередньому розв'язання СР вигляду (1).

Розглянемо два приклади, що ілюструють наведені вище результати.

Приклад 1. Нехай закон розподілу спотворень у правій частині СР (1) визначається за формулою

$$p(z) = q^{-1}(1 + (-1)^{f(z)}\theta), \; z \in F_q, \qquad (11)$$

де f є (відмінною від константи) лінійною булевою функцією від r змінних, $\theta \in (0,1)$. Тоді, як неважко переконатися,

$$\max_{c \in F_q \setminus \{0\}} |\hat{p}(c)|^2 = \Delta(p_\xi) = \theta^2,$$

і оцінки інформаційної складності кореляційних атак над полями F_q та F_2 відповідно співпадають. Таким чином, в цьому випадку є доцільним розв'язання нової системи рівнянь (8) замість вхідної СР зі спотвореними правими частинами (1).

Приклад 2. Нехай закон розподілу спотворень у правій частині СР (1) визначається за формулою (11), де $f(z) = z_1 \oplus z_2 \oplus g(z_3, ..., z_r)$, $z = (z_1, ..., z_r) \in F_q$, r є парним числом, а g є бент-функцією. Тоді справедлива рівність $\max_{c \in F_q \setminus \{0\}} |\hat{p}(c)|^2 = 2^{2-r}\theta^2 = 2^{2-r}\Delta(p_\xi)$, і інформаційна складність атаки, що базується на розв'язанні СР (8), є у 2^{r-2} разів більше. Таким чином, в цьому випадку перехід від СР (1) до СР (8) є малодоцільним.

Висновки.

1. Основними результатами статті є теореми 1 і 2, які встановлюють неасимптотичні нижні межі інформаційної складності двох видів кореляційних атак, які базуються на розв'язанні систем лі-

нійних рівнянь зі спотвореними правими частинами над полями порядку 2^r, де $r \geq 2$, та над полем з двох елементів відповідно. Отримані межі показують, якою повинна бути найменша кількість рівнянь у системі (незалежно від способу її побудови або методу розв'язання) для того, щоби ймовірність помилкового відновлення істинного розв'язку такої системи рівнянь не перевищувала будь-яке заздалегідь визначене число $\delta \in (0, 1/2)$.

2. Нижня межа інформаційної складності кореляційних атак, які базуються на розв'язанні СР вигляду (1), визначається виразом у правій частині нерівності (5), який, на відміну від евристичної формули (3) [13], містить явну залежність від ймовірності помилки атаки.

3. Для проведення кореляційних атак на словоорієнтовані потокові шифри над полем F_q можна використовувати відомі методи розв'язання систем лінійних рівнянь зі спотвореними правими частинами над полем F_2 [8, 10], будуючи за системою (1) систему рівнянь (8).

4. Інформаційна складність атак останнього виду визначається виразом у правій частині нерівності (9) та є не менше інформаційної складності атак, що базуються на безпосередньому розв'язанні СР (1).

5. При побудові СР вигляду (8) ненулевий елемент c поля F_q слід вибирати, виходячи з умови $|\hat{p}(c)| = \max\limits_{z \in F_q \setminus \{0\}} |\hat{p}(z)|$; це забезпечує найменшу можливу ймовірність спотворень у правій частині СР (9), а, отже, мінімізує інформаційну складність відповідних кореляційних атак.

6. В цілому, отримані результати складають наукову основу майбутнього методу обґрунтування стійкості сучасних словоорієнтованих потокових шифрів відносно як відомих, так і перспективних кореляційних атак. Розробка такого методу є задачею подальших досліджень.

ЛІТЕРАТУРА

[1]. А. Алексейчук, С. Игнатенко, "Метод оптимизации алгоритмов решения систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N", *Реєстрація, зберігання і обробка даних*, Т. 7, № 1, С. 21-29, 2005.

[2]. А. Алексейчук, С. Игнатенко, "Нижняя граница вероятности восстановления истинного решения системы линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N", *Захист інформації,* № 4, С. 6-12, 2006.

[3]. Г. Балакин, "Введение в теорию случайных систем уравнений", *Труды по дискретной математике,* Т. 1, С. 1-18, 1997.

[4]. Г. Балакин, "Эффективно решаемые классы систем булевых уравнений", *Обозрение прикл. промышл. Матем*, Т. 2, № 3, С. 494 – 501, 1995.

[5]. А. Левитская, "Системы случайных уравнений над конечными алгебраическими структурами", *Кибернетика и системный анализ*, Т. 41, № 1, С. 82-116, 2005.

[6]. Р. Лидл, Г. Нидеррайтер, *Конечные поля: В 2 т.* М.: Мир, 1988, 818 с.

[7]. О. Логачев, А. Сальников, В. Ященко, *Булевы функции в теории кодирования и криптологии.* М.: МЦНМО, 2004, 470 с.

[8]. А. Олексійчук, "Субекспоненційні алгоритми розв'язання систем лінійних булевих рівнянь зі спотвореними правими частинами", *Прикладная радиоэлектроника*, Т. 11, № 2, С. 3-11, 2012.

[9]. С. Чечёта, *Введение в дискретную теорию информации и кодирования: учебное издание.* М.: МЦНМО, 2011, 224 с.

[10]. S. Bogos, F. Tram′er, S. Vaudenay, *On solving LPN using BKW and variants. Implementation and analysis.* Cryptology ePrint Archive.

[11]. A. Canteaut, "Fast correlation attacks against stream ciphers and related open problems", *The 2005 IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security*, pp. 49-54, 2005.

[12]. W. Meier, "Fast correlation attacks: methods and countermeasures Lecture Notes in Computer Science", *FSE'2011, Proceedings*, pp. 55 – 67, 2011.

[13]. B. Zhang, C. Xu, W. Meier, *Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0.* Cryptology ePrint Archive.

REFERENCES

[1]. A. Alekseychuk, S. Ignatenko, "A method for optimization of algorithms of solving systems of linear equations corrupted by noise over residue ring modulo 2^N", *Data Recording, Storage and Processing*, vol. 7, no. 1, pp. 21-29, 2005.

[2]. A. Alekseychuk, S. Ignatenko, "Lover bound of probability of recovering a true solution of a system of linear equations corrupted by noise over residue ring modulo 2^N", *Zahist informatsii*, no. 4, pp. 6-12, 2006.

[3]. G. Balakin, "Introduction to the theory of random systems of equations", *Trudui po diskretnoy matematike,* no. 1, pp. 1-18, 1997.

[4]. G. Balakin, "Efficiently solvable classes of systems of Boolean equation", *Obozrenie prikladnoy i promyshlennoy matematiki,* vol. 2, no. 3, pp. 494-501, 1995.

[5]. A. Levitskaya, "Systems of random equations over finite algebraic structures", *Kibernetika I Sistemnyi Analiz,* vol. 41, no. 1, pp. 82-116, 2005.

[6]. R. Lidl, G. Niderrayter, *Finite fields: In 2 vol.* M.: Mir, 1988, 818 p.

[7]. O. Logachev, A. Salnikov, V. Yashchenko, *Boolean functions in the theory of coding and cryptology*. M.: MCCME Press, 2004, 470 p.

[8]. A. Alekseychuk "Subexponential of algorithms of solving systems of linear equations corrupted by noise", *Prikladnaya radioelektronika*, vol. 11, no. 2, pp. 3-11, 2012.

[9]. S. Chechyota, *Introduction to discrete information and coding theoty: a training edition*. M.: MCCME Press, 2011, 224 p.

[10]. S. Bogos, F. Tram′er, S. Vaudenay *On solving LPN using BKW and variants. Implementation and analysis*. Cryptology ePrint Archive.

[11]. A. Canteaut "Fast correlation attacks against stream ciphers and related open problems", *The 2005 IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security*, pp. 49-54, 2005.

[12]. W. Meier "Fast correlation attacks: methods and countermeasures Lecture Notes in Computer Science", *FSE'2011, Proceedings,* pp. 55-67, 2011.

[13]. B. Zhang, C. Xu, W. Meier, Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0. Cryptology ePrint Archive.

НИЖНИЕ ГРАНИЦЫ ИНФОРМАЦИОННОЙ СЛОЖНОСТИ КОРРЕЛЯЦИОННЫХ АТАК НА ПОТОЧНЫЕ ШИФРЫ НАД ПОЛЯМИ ПОРЯДКА 2^r

Корреляционные атаки относятся к наиболее мощным атакам на поточные шифры, а методы построения таких атак и обоснования стойкости поточных шифров относительно них образуют развитое направление современной криптологии. На протяжении последних лет в связи с появлением словоориентированных поточных шифров наблюдается развитие методов построения корреляционных атак, основанных на решении систем линейных уравнений с искаженными правыми частями над конечными полями или кольцами вычентов порядка $q \geq 2$. В данной статье исследуется два таких способа, первый из которых состоит в решении указанных систем уравнений над полями порядка 2^r, где $r \geq 2$, а второй – в решении аналогичных систем уравнений над полем из двух элементов. Получены неасимптотические нижние границы информационной сложности указанных атак, уточняющие ранее известную эвристическую оценку. Полученные результаты могут быть использованы при обосновании стойкости словоориентированных поточных шифров относительно современных корреляционных атак.

Ключевые слова: поточный шифр, корреляционная атака, система уравнений с искаженными правыми частями над конечным полем, информационная сложность.

LOVER BOUNSD FOR THE DATA COMPLEXITY OF CORRELATION ATTACKS ON STREAM CIPHERS OVER FIELDS OF ORDER 2^r

Correlation attacks are one of the most powerful attacks on stream ciphers, and methods of building such kind of attacks and security proofs of stream ciphers against them form a developed direction of modern cryptography. Over the past few years in connection with emergence of word-oriented stream ciphers, methods for building correlation attacks based on solving systems of linear equations corrupted by noise over finite fields or residue rings of order $q \geq 2$ are developed. In this article we investigate two such methods, the first of them consists of solving these systems of equations over fields of order 2^r, where $r \geq 2$, and the second one – in solving analogous systems of equations over a field of two elements. The obtained results can be used in security proofs of word-oriented stream ciphers against modern correlation attacks.

Keywords: stream cipher, correlation attacks, system of linear equations corrupted by noise over finite field, data complexity.

Олексійчук Антон Миколайович, доктор технічних наук, доцент, головний науковий співробітник науково-дослідного центру Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
E-mail: alex-dtn@ukr.net

Алексейчук Антон Николаевич, доктор технических наук, доцент, главный научный сотрудник научно-исследовательского центра Института специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского».

Alekseychuk Anton, Doctor of Technical Sciences, Assistant professor, Head of Research and Development Department of The Institute of Special Communication and Information Protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

Поремський Михайло Васильович, аспірант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
E-mail: undermyclouds@gmail.com

Поремский Михаил Васильевич, аспирант, Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского».

Poremskyi Mikhailo, post-graduate student, Institute of Special Communication and Information Protection National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".