УДК 519.2:519.85

ЯКОВЛЄВ Сергій Володимирович

АТАКИ ЗБОЇВ НА ШИФР ДСТУ ГОСТ 28147:2009

Постановка проблеми. Атаки збоїв відносяться до так званих активних атак за побічними каналами на криптосистеми. Основним об'єктом таких атак є не криптографічний алгоритм з точки зору математики, а його реалізація у конкретному обчислювальному середовищі. Через недосконалість апаратури, наявність витоку додаткової інформації про внутрішні стани обчислювальних процесів та можливість втручатись у роботу пристроїв у аналітика з'являються додаткові можливості щодо зламу криптосистем – наприклад, знаходження ключів шифрування.

Криптоаналітичні атаки, що використовують збої під час виконання шифрування, мало досліджені в царині симетричних шифрів. Практично всі методи аналізу, що розглядаються, зводяться до так званих *диференціальних атак збоїв* (differential fault attacks), оскільки аналітик використовує для відновлення ключа шифрування як коректні шифртексти, так і шифртексти, одержані після втручання у процес шифрування (збійні шифртексти); знання відкритого тексту, що шифрується, не вимагається.

Аналіз останніх досліджень і публікацій. Увага дослідників зосереджена здебільшого на шифрі AES та подібних до нього. Втім існує декілька атак на шифри зі структурою схеми Фейстеля – зокрема, це атаки Біхама, Аккара та Рівайна [1; 2]. Остання виявилась найефективнішою для попереднього стандарту шифрування США (Data Encryption Standard, DES). Атака Рівайна так само легко переноситься на довільні схеми Фейстеля, раундові перетворення яких є SP-мережею із блоковою структурою нелінійної частини, а ключовий суматор також можна подати у блоковому вигляді.

Національний стандарт шифрування ДСТУ ГОСТ 28147:2009 [3] (далі – шифр ГОСТ) має раундове перетворення, що задовольняє вимогам атаки Рівайна, однак використання у ключовому суматорі додавання за модулем 2^{32} унеможливлює розбиття замішаних ключем даних на незалежні блоки. У відкритих джерелах аналіз стійкості шифру ГОСТ до атак збоїв практично відсутній.

Метою роботи є розгляд атаки збоїв на шифр ГОСТ, що узагальнює ідеї Рівайна на випадок використання звичайного та модульного додавання у ключовому суматорі. Розглядались різні моделі збоїв: модель із фіксованим збоєм та модель із випадковим збоєм, – а також можливі шляхи підсилення атаки через використання додаткової інформації.

Виклад основного матеріалу. ГОСТ-шифр є класичною схемою Фейстеля, що обробляє 64-бітові блоки. Детальний опис алгоритму та режимів його застосування наведено у [3], ми наведемо лише необхідні позначення. Нехай вхідне повідомлення розбите на ліву та праву частину (L_0, R_0) по 32 біта; шифратор виконує 32 раунди:

$$L_{m+1} = R_m$$
$$R_{m+1} = L_m \oplus F(R_m, k_{m+1}),$$

і вихідним повідомленням є (R_{32}, L_{32}).

Раундове перетворення має такий вигляд: $F(X, K) = \rho\big(S\big(X + K\big)\big)$, де «+» – операція додавання за модулем 2^{32}, $\rho(.)$ – циклічний зсув 32-бітного двійкового вектору на 11 біт вліво (лінійне перетворення відносно побітового додавання), а $S(.)$ – так званий *довгостроковий ключовий елемент* (ДКЕ): нелінійне перетворення спеціального виду; якщо розглядати 32-бітну змінну X як вектор чотирибітових змінних $X = \big(x_8, ..., x_1\big)$, то $S(X) = \big(s_8\big(x_8\big), ..., s_1\big(x_1\big)\big)$, де всі $s_i : V_4 \to V_4$ – спеціально обрані перетворення, що у визначеннях стандарту ДСТУ ГОСТ 28147:2009 є додатковими ключовими елементами.

У цій роботі ми вважаємо довгострокові ключові елементи відомими аналітику, оскільки існує атака Саарінена [4], яка дозволяє встановити значення ДКЕ, зафіксовані у пристрою; ця атака потребує трохи більше за 2^{32} операцій. Зауважимо, що атака Саарінена є детермінованою атакою, що не використовує інформацію з побічних каналів та збої у роботі шифратора.

В експериментальній частині роботи використовувались наведені в [5] довгострокові ключові елементи, що мають хороші криптографічні властивості, а також таблиця ДКЕ № 1 з [6], що наразі є таблицею за умовчанням в Національній системі електронного цифрового підпису [7].

Раундові ключі $k_1, ..., k_{32}$, що подаються на вхід відповідної раундової функції, одержуються з вхідного ключа шифрування за таким правилом:

1) вхідний 256-бітовий ключ шифрування ділиться на вісім 32-бітових змінних $K(1),...,K(8)$;

2) раундові ключі визначаються за схемою: для $i = \overline{1, 8}$ маємо $k_i = K(i)$, $k_{8+i} = K(i)$, $k_{16+i} = K(i)$, $k_{24+i} = K(9-i)$.

Зі схеми розгортання раундових ключів ГОСТ-шифру випливає, що достатньо визначити раундові ключі останніх восьми раундів, щоб встановити значення всього ключа шифрування. Крім того, на останніх восьми раундах фактично можна розглядати раундові ключі як незалежні випадкові змінні.

Під час проведення атаки зі збоями аналітик повинен одержати пари «коректний шифртекст» (шифртекст, одержаний з відкритого тексту шляхом коректного шифрування на ключі, який треба визначити) та «збитий шифртекст» (шифртекст, одержаний з того самого відкритого тексту на тому самому ключі, але коли у процедуру шифрування був внесений збій).

Будемо позначати коректні шифртексти, одержані після *r*-го раунду, через (L_r, R_r), а шифртексти, що одержані зі збоями у процесі виконання, через $(\tilde{L}_r, \tilde{R}_r)$.

Тоді для *r*-го раунду виконання ГОСТ-шифру матимуть місце такі рівності:

$$L_r = R_{r-1}; \quad R_r = L_{r-1} \oplus F(R_{r-1}, k_r);$$
$$\tilde{L}_r = \tilde{R}_{r-1}; \quad \tilde{R}_r = \tilde{L}_{r-1} \oplus F(\tilde{R}_{r-1}, k_r).$$

Додаючи другі рівності одне до одного та підставляючи структурну формулу для *F*, одержуємо:

$$R_r \oplus \tilde{R}_r = L_{r-1} \oplus \tilde{L}_{r-1} \oplus F(R_{r-1}, k_r) \oplus F(\tilde{R}_{r-1}, k_r),$$
$$L_{r-1} \oplus \tilde{L}_{r-1} = R_r \oplus \tilde{R}_r \oplus F(L_r, k_r) \oplus F(\tilde{L}_r, k_r) =$$
$$= R_r \oplus \tilde{R}_r \oplus \rho\left(S(L_r + k_r) \oplus S(\tilde{L}_r + k_r)\right)$$

та

$$\rho^{-1}\left(L_{r-1} \oplus \tilde{L}_{r-1}\right) = \rho^{-1}\left(R_r \oplus \tilde{R}_r\right) \oplus S(L_r + k_r) \oplus S(\tilde{L}_r + k_r).$$

Композицію нелінійного перетворення *S* та додавання із ключем можна представити в такому вигляді:

$$S(X + k) = \left(s_8(x_8 + k_8 + c_8), ..., s_1(x_1 + k_1 + c_1)\right),$$
$$S(\tilde{X} + k) = \left(s_8(\tilde{x}_8 + k_8 + \tilde{c}_8), ..., s_1(\tilde{x}_1 + k_1 + \tilde{c}_1)\right),$$

де 32-бітні змінні додаються за модулем 2^{32}, 4-бітні змінні додаються за модулем 2^4, а c_i та $\tilde{c}_i$ – послідовності бітів переносу, що виникають при додаванні попередніх 4-бітових регістрів; ці послідовності можна визначити рекурентним шляхом:

$$c_i = \begin{cases} 0, & i = 1 \\ carry(x_{i-1}, k_{i-1}, c_{i-1}), & i > 1, \end{cases}$$

де функція $carry(x,k,c)$ – біт переносу, що виникає при додаванні вхідних змінних:

$$carry(x,k,c) = \left\lfloor \frac{x+k+c}{16} \right\rfloor$$

(тут через «+» позначене звичайне додавання). Очевидно, що визначена таким чином послідовність c_i є бітовою послідовністю. Послідовність $\tilde{c}_i$ визначається аналогічно.

Отже, якщо позначити через X_i i-ту тетраду 32-бітної змінної X, то можемо записати серію рівностей:

$$\left(\rho^{-1}\left(L_{r-1} \oplus \tilde{L}_{r-1}\right)\right)_i = \left(\rho^{-1}\left(R_r \oplus \tilde{R}_r\right)\right)_i \oplus s_i(L_{r,i} + k_{r,i} + c_i) \oplus s_i(\tilde{L}_{r,i} + k_{r,i} + \tilde{c}_i).$$

Для сукупності пар «коректний шифртекст» – «збитий шифртекст» визначимо серію розпізнаваючих функцій для тетрад ключа:

$$g_i(k) = \left(\rho^{-1}\left(R_r \oplus \tilde{R}_r\right)\right)_i \oplus s_i(L_{r,i} + k_{r,i} + c_i) \oplus s_i(\tilde{L}_{r,i} + k_{r,i} + \tilde{c}_i).$$

Тоді, якщо $k = k_{r,i}$, то $g_i(k) = \left(\rho^{-1}\left(L_{r-1} \oplus \tilde{L}_{r-1}\right)\right)_i$, тобто значення $g_i(k)$ буде мати такий саме розподіл, що й $\left(\rho^{-1}\left(L_{r-1} \oplus \tilde{L}_{r-1}\right)\right)_i$; інакше значення $g_i(k)$ буде розподілене рівномірно. Для перевірки гіпотези про рівномірний розподіл використовується квадратична евклідова відстань:

$$d(k) = \sum_{x=0}^{15} \left(\frac{\#\{g_i(k) = x\}}{N} - \frac{1}{16} \right)^2.$$

Ми обираємо таке k як правильне значення раундового ключа, для якого $d(k)$ є максимальним.

Отже, пропонована атака на r-й раунд ГОСТ-шифру представлена у вигляді такого алгоритму.

Алгоритм 1:

1) накопичити достатню кількість пар «коректний шифртекст» – «збитий шифртекст»; позначимо цю кількість через N;

2) встановити $i = 1$; тоді $c_i = \tilde{c}_i = 0$;

3) для всіх $k \in V_4$ обчислили значення $g_i(k)$ на кожній парі та обчислити відповідні значення $d(k)$;

4) визначити коректне значення $k_{r,i}$: $k_{r,i} = \arg\max_k d(k)$;

5) для кожної пари обчислити значення бітів переносу c_{i+1} та $\tilde{c}_{i+1}$;

6) повторити кроки 3-5 для i = 2, ..., 8.

Зауважимо, що ми визначаємо тетради раундового ключа послідовно, починаючи з першої; це необхідно для коректного обчислення послідовностей бітів переносу. Якщо аналітик хоче шукати значення довільної тетради (користуючись кроками 3-4 алгоритму 1) у припущеннях щодо значення відповідних c_i та $\tilde{c}_i$, то таких припущень можна зробити 2 для c_i (за умови використання завжди одного відкритого тексту) та ще по 2 для $\tilde{c}_i$ у кожної згенерованої пари; при використанні більш ніж чотирьох пар складність атаки з таким підходом стає більшою, ніж простий перебір. Такий підхід майже завжди є неефективним.

Запропонована атака дозволяє практично незалежно визначати тетради бітів раундового ключа. Додавання із ключем за модулем 2^{32}, що створює додаткові залежності між тетрадами завдяки переносу бітів, корегуються послідовностями c_i. Однак, з одного боку, саме використання штучно створених послідовностей бітів переносу не дозволяє розпізнавати тетради ключа паралельно; з іншого боку, для послідовного визначення тетрад не треба буде додаткових ресурсів чи виконання додаткових збоїв.

Оцінка ефективності наведеної атаки проводилась за двома параметрами: визначалась імовірність успішного розпізнавання ключа при обмеженій кількості збоїв та визначалась кількість збоїв, необхідна для успішного розпізнавання ключа. У цьому розділі наведені результати модельних випробувань за умови, що аналітик має змогу виконувати збої у конкретній фіксованій позиції проміжних шифртекстів. Результати експериментальних досліджень, наведені у розділі, були одержані автором разом із магістром Фізико-технічного інституту НТУУ «КПІ» П. Огнєвим.

Завдяки лавинним ефектам чим раніш був виконаний збій, тим менше розподіл $\rho^{-1}\left(L_{r-1} \oplus \tilde{L}_{r-1}\right)$ буде відрізнятись від рівноймовірного (див., наприклад, [8]). Однак раундове перетворення ГОСТ-шифру (зокрема, циклічний бітовий зсув) має слабкі лавинні ефекти, що може призвести до того, що виконаний збій ніяк не проявиться на досліджуваній тетраді ($L_{r,i} = \tilde{L}_{r,i}$), а тому функції розпізнавання $g_i(k)$ будуть рівноймовірні для будь-якого значення k. Отже, для успішного застосування атаки треба знайти баланс за номером раунду та кількості необхідних пар. Більш того, дослідження виявили, що фіксовані збої (тобто збої у фіксованій позиції) не впливають на деякі тетради ключа; найбільш імовірне пояснення цього спостереження полягає в тому, що лавинний вплив збою змішується із горизонтальним впливом, що

виникає за рахунок переносу бітів між тетрадами у ключовому суматорі, й результуючий вплив не має чітко виражених статистичних властивостей. Таким чином, виявилось, що атака, яка використовує одну фіксовану позицію збою, не може відновити раундовий ключ повністю – здебільшого відновлюються три-чотири тетради ключа, а інші тетради – з деякою не дуже великою імовірністю; для успішного застосування атак із фіксованими збоями потрібно виконувати збої у декількох (спеціально підібраних) фіксованих позиціях.

Зауважимо, що використання під час експериментів різних ДКЕ (із різними лавинними характеристиками) не виявило значного впливу на розподіл різниць. Отже, можна стверджувати, що слабкий лавинний ефект циклічного бітового зсуву є більш суттєвим для атак збоїв, аніж лавинні ефекти нелінійної частини раундового перетворення.

Дослідження ефективності запропонованої атаки відбувалось у такі етапи:

1) побудова мап лавинних ефектів, що показують вплив збою в заданій позиції після заданого раунду шифрування на біти вихідного шифртексту;

2) оцінювання кількості збоїв, яке необхідне для визначення окремих тетрад ключа 32-го раунду, залежно від місця виконання збою;

3) оцінювання імовірності успіху атаки за умови використання обмеженої кількості збоїв.

Оцінювання відбувалося на вибірці з $2^{18} = 262144$ випадкових ключів шифрування зі встановленою верхньою межею у 1024 необхідні збої. Збої виконувались лише в правій частині блоку (для збоїв у лівій частині, виходячи зі структури схеми Фейстеля, необхідно взяти відповідні значення для правої частини на $(r+1)$ раунді збою). Кількість збоїв, необхідна для встановлення правильних значень тетрад ключа, визначалась двома способами: через мінімальну кількість збоїв, для якої розпізнавач повернув коректне значення тетради ключа, та через кількість збоїв, починаючи з якої розпізнавач повертав коректне значення стабільно (тобто збільшення кількості збоїв не впливало на роботу розпізнавача).

Імовірність успіху атаки визначалась через відсоткове значення кількості ключів, що були коректно розпізнані не більш ніж за 1024 збої; це значення наближає імовірність успішного застосування атаки за такої кількості збоїв. Зауважимо, що значення встановлювались для стабільного розпізнавання ключа, як це описано в попередньому абзаці.

На жаль, обмежений обсяг статті не дозволяє навести всі одержані експериментальні дані. Однак з результатів експерименту випливає, що, на відміну від DES, шифр ГОСТ дуже чутливий до позиції, в якій був збій: в деяких випадках коректний ключ розпізнається за декілька збоїв навіть

у високих раундах, в інших недостатньо й тисячі збоїв (Рівайн для шифру DES наводить значення у 10^8 збоїв). Водночас запропонована атака може бути ефективно реалізована навіть за збоїв у раундах, що досить віддалені від останнього – зокрема, при виконанні збоїв у семи-восьми останніх раундах шифрування. Це суттєво спрощує реалізацію атаки (для порівняння: атаки Біхама та Аккара потребували збоїв точно у передостанньому раунді).

Слабкі лавинні ефекти циклічного зсуву, що використовується у раундовій функції ГОСТ-шифру, спричиняють такі практичні властивості досліджуваної атаки: використання збоїв на раундах, близьких до останнього, дозволяє за малу кількість втручань гарантовано відновити деякі тетради ключа, однак окремі тетради виявляються взагалі не афектованими і для них розпізнавач не працює. Водночас використання збоїв на досить віддалених раундах не дозволяє відновлювати тетради гарантовано, але імовірність успішного проведення атаки для кожної тетради усереднюється до суттєво високої (перевищує 0,5, а для більшості тетрад – 0,7). У цілому для успішної атаки із мінімальним втручанням в роботу шифру треба використовувати збої у двох-трьох спеціально обраних позиціях; одержані дані дозволяють обирати такі фіксовані позиції та будувати відповідну атаку.

Для перевірки одержаних результатів була побудована модельна атака на шифр ГОСТ із використанням фіксованих позицій для збоїв, що максимально використовує інформацію з мап лавинних ефектів та таблиць імовірностей успішного розпізнавання ключа. Аналітику необхідно послідовно накопичити статистику, використовуючи збої у позиціях 1, 9, 17 та 25 правої частини блоку після 22-го та після 26-го раунду шифрування (загалом вісім позицій та вісім масивів статистичних даних, що обчислюються незалежно); з накопиченої статистики він може відновити всі раундові ключі останніх восьми раундів шифрування (тобто весь ключ шифрування).

Для оцінювання ефективності побудованої атаки було проведено її реалізацію на вибірці з 2^{25} випадкових ключів шифрування. Виявилось, що побудована атака при використанні 12 збоїв на кожній позиції (загалом 96 збоїв) встановлює повністю ключ шифрування із імовірністю 91,8 %, а при 16 збоях на кожній позиції (загалом 128 збоїв) – із імовірністю 97,8 %. Випадки неповного розпізнавання відповідали некоректному встановленню значень тетрад, що найгірше охоплювались лавинними ефектами збоїв; використання часткового перебору значень таких тетрад (замість статистичного розпізнавання) дозволило підвищити імовірність успіху до 99,2 % при 16 збоях на кожній позиції.

Дослідження попереднього розділу природним чином поширюються на модель збоїв, що виникають у випадковому біті блоку; біт збою обирається

рівноймовірно та невідомий досліднику. Така модель є значно м'якшою для криптоаналітика, оскільки легше реалізується з фізичної точки зору. При дослідженні очікувалось, що для успішного визначення окремої тетради атака буде потребувати більшої кількості збоїв (у 2–4 рази), оскільки не всі випадкові збої будуть впливати на потрібну тетраду; однак за рахунок взаємовпливів (своєрідної «синергії» збоїв) атака в цій моделі виявиться ефективнішою для визначення раундового ключа загалом.

Оцінювання ефективності атаки у моделі випадкового збою велось на вибірці з 2^{24} = 16777216 випадкових ключів шифрування зі встановленою верхньою межею у 512 необхідних збоїв. Збої виконувались лише в правій частині блоку (для збоїв у лівій частині, виходячи зі структури схеми Фейстеля, необхідно взяти відповідні значення для правої частини на $(r+1)$ раунді збою). Як і в попередньому розділі, обраховувалось дві величини: мінімальна кількість збоїв, для якої розпізнавач повернув коректне значення тетради ключа, та кількість збоїв, починаючи з якої розпізнавач повертав коректне значення стабільно (тобто збільшення кількості збоїв не впливало на роботу розпізнавача).

У таблиці 1 наводиться відсоткове значення кількості ключів, що були коректно розпізнані не більш ніж за 512 збоїв; це значення наближає імовірність успішного застосування атаки за такої кількості збоїв. Зауважимо, що значення наведені для стабільного розпізнавання ключа, як це описано в попередньому абзаці.

З наведених результатів випливає дещо парадоксальний результат. Модель із випадковим збоєм дійсно виявилась ефективною для визначення окремих тетрад ключа – зокрема, при збоях на 28-му та особливо на 27-му раундах, де спостерігається очікуваний зріст необхідної кількості статистики у 2–4 рази, однак, оскільки при відповідних фіксованих збоях в цих раундах потребувалось зовсім мало збоїв, кількість випадкових збоїв все ще залишається невеликою.

Проте для визначення раундового ключа в цілому модель випадкового збою виявляється абсолютно неефективною. Тільки збої на 27-му раунді дозволили обчислити раундовий ключ, але для цього потребувалось до сотні збоїв – значно більше за атаку, що використовує окремі фіксовані збої. Використання збоїв у інших раундах не дає повноцінної гарантії відновлення ключа: якщо збої у 25-му та 29-му раунді дозволяли відновити окремі тетради із похибкою менш за 1 %, то стабільне відновлення ключа відбувалось вже із імовірністю 10-15%, що є екстремально малим значенням.

Таким чином, виходячи з результатів емпіричних досліджень, ми повинні констатувати, що атака із фіксованими збоями значно ефективніша за

атаку із випадковими збоями для відновлення раундового ключа загалом. Водночас атаку із випадковими збоями доволі успішно можна використовувати для відновлення окремих тетрад раундового ключа.

Таблиця 1

Імовірності стабільного розпізнавання ключа k_{32} та його тетрад у моделі випадкового збою

Номер тетради	Кількість збоїв	Раунд виконання збою r (в %)					
		r = 29	**r = 28**	**r = 27**	**r = 26**	**r = 25**	**r = 24**
1	мінімальна	99,6	100,0	100,0	100,0	99,8	95,4
	стабільна	97,7	100,0	100,0	100,0	98,8	79,5
2	мінімальна	98,8	100,0	100,0	100,0	100,0	95,5
	стабільна	94,0	100,0	100,0	100,0	99,8	80,0
3	мінімальна	99,5	100,0	100,0	100,0	99,7	95,4
	стабільна	96,9	100,0	100,0	100,0	98,5	79,3
4	мінімальна	99,4	100,0	100,0	100,0	99,8	95,6
	стабільна	96,4	100,0	100,0	100,0	99,1	80,2
5	мінімальна	99,1	100,0	100,0	100,0	99,9	96,6
	стабільна	95,3	100,0	100,0	100,0	99,5	84,3
6	мінімальна	99,3	100,0	100,0	100,0	99,8	95,5
	стабільна	96,2	100,0	100,0	99,9	98,9	79,7
7	мінімальна	99,2	100,0	100,0	100,0	99,9	95,8
	стабільна	95,4	100,0	100,0	100,0	99,4	81,0
8	мінімальна	97,5	100,0	100,0	100,0	100,0	96,7
	стабільна	89,8	100,0	100,0	100,0	100,0	85,1
Ключ у цілому	мінімальна	65,7	97,7	100,0	85,5	32,0	0,0
	стабільна	11,8	87,8	100,0	65,8	14,7	0,0

Існує щонайменше два шляхи можливого підсилення запропонованої атаки збоїв на шифр ГОСТ.

Перший шлях полягає в дослідженні таких тетрад ключа, для яких функція розпізнавання $g_i(k)$ повинна дорівнювати тотожному нулю або слабко відрізнятись від тотожного нуля. Така ситуація можлива, якщо лавинні ефекти від збою афектують вхід на раундове перетворення (або конкретну тетраду раунду), але не афектують чи слабко афектують відповідний вихід. У цьому випадку можливі значення відповідної тетради ключа можна знайти не статистично, а аналітично, розв'язавши рівняння

$$s_i(x+k) \oplus s_i(y+k) = z$$

для S-блоку s_i та відомих значень *x, y, z*. Через малий розмір S-блоків та умови стійкості до диференціального криптоаналізу, які висуваються до сучасних S-блоків, подібні рівняння розв'язуються швидко навіть повним перебором та мають дуже невелику кількість розв'язок (зазвичай 2 або 4), що дозволяє навіть за один збій суттєво скоротити кількість потенційних раундових ключів.

Цей підхід був детально досліджений П. Огнєвим [9]. Ним встановлено, що за рахунок використання мап лавинних ефектів (про які зазначалось у розділі 3) можна ефективно використати модель із фіксованим збоєм для використання зазначеної ситуації. Кожна знайдена ситуація $g_i(k) \equiv 0$ зменшувала простір можливих раундових ключів в середньому в 16 разів причому, залежно від позиції збою, такі ситуації могли виникати сукупностями для різних раундових ключів. Це дозволило побудувати стратегію атаки, яка із використанням приблизно 16 збоїв зменшувала простір можливих ключів шифрування з 2^{256} до 1,8 млн. Таку кількість вже можна ефективно перебрати на сучасній обчислювальній техніці.

Інший підхід полягає у тому, що замість використання евклідової відстані можна встановити теоретичний розподіл функцій розпізнавання та використовувати логнормальну відстань емпіричного розподілу $g_i(k)$ до теоретичного:

$$d(k) = \sum_{j=1}^{N} \log(\, p_i(g_i^{(j)}(k))) \,.$$

Потенційно використання інформації про точний вид розподілу функцій розпізнавання може підвищити точність та вимогливість статистичного розпізнавача для раундових ключів (менше статистики – більша імовірність успіху). Однак теоретичний розподіл функцій розпізнавання для шифру ГОСТ залежить від використовуваних ДКЕ та потенційно може бути спотворений завдяки бітам переносу, що виникають у ключовому суматорі. Автором разом із магістром Фізико-технічного інституту НТУУ «КПІ» І. Богатченком були проведені експериментальні дослідження з оцінювання ефективності такого підходу.

Експеримент складався з таких етапів.

1. Для випадково обраного значення ключа шифрування будувався емпіричний розподіл функцій розпізнавання (для побудови використовувались 100000 пар текстів).

2. Одержаний розподіл застосовувався в атаці збоїв на інший ключ шифрування як теоретичний. Для спрощення використовувались лише збої

на вході у 28-й раунд шифрування (такі збої давали найбільш нерівномірний розподіл функцій розпізнавання).

3. Ефективність цієї атаки порівнювалась із ефективністю атаки, що використовувала евклідову відстань.

Результати експериментів показали, що, хоча побудовані емпіричні розподіли слабко відрізнялись для різних значень ключів, їх використання не спричиняло значного (або взагалі хоч якогось) підвищення ефективності атаки збоїв: обидва варіанти атаки вимагали приблизно однакової кількості збоїв та мали приблизно однакову імовірність успіху, що суттєво відрізняється від результатів, одержаних Рівайном для DES [2]. Отримані дані можна пояснити як загальною складністю визначення параметрів атаки (розподілів функцій розпізнавання), обчислення точних значень яких вимагає занадто великих ресурсів, так і, можливо, малими порівняно із загальним розміром ключового простору шифру ГОСТ вибірками, на яких здійснювалися модельні експерименти.

Висновки. У роботі була запропонована узагальнена атака збоїв на шифр ДСТУ ГОСТ 28147:2009, що поширює ідеї атаки Рівайна на схеми Фейстеля із ключовим суматором за модулем 2^{32}; наведена методика представлення такого суматора у блоковому вигляді за допомогою допоміжних послідовностей бітів переносу. Такий підхід дозволив зберегти основну ідею атаки: визначення раундового ключа по частинах (у випадку ГОСТ-шифру – по тетрадах); однак, на відміну від DES, тетради раундового ключа необхідно визначати послідовно. Практичне дослідження мапи лавинних ефектів шифру ГОСТ показало можливість ефективного застосування пропонованої атаки для ГОСТ-подібних шифрів (в яких відбувається горизонтальне перемішування даних в блоку шифрування), коли збої виникають на останніх семи-восьми раундах шифрування.

Було розглянуто різні моделі збоїв: збої у фіксованій позиції та випадкові збої. Виявилось, що збої у фіксованій позиції на передостанніх раундах дозволяють відновлювати окремі тетради раундового ключа за мінімальної статистики (два-три збої), однак інші тетради ключа в цьому випадку можуть взагалі не розпізнаватись. Водночас фіксовані збої у віддалених раундах потребують більше матеріалу для проведення атаки, проте для будь-якої позиції імовірності визначення довільної тетради в середньому зростає (досягає значення 0,5–0,7). Модель випадкових збоїв потребує значно більшої кількості збоїв взагалі та, як не дивно, також не дозволяє гарантовано відновити всі тетради ключа, хоча для відновлення окремих тетрад випадкові збої працюють задовільно. Наведені дані дозволяють оцінювати граничні умови ефективності спрямованої атаки.

Загалом можна зауважити, що найкращим з точки зору мінімальності втручання у роботу шифратора та максимально ефективного розпізнавання раундових ключів є проведення атаки зі збоями у декількох обраних фіксованих позиціях. Тоді для гарантованого відновлення раундового ключа 32-го раунду виявляється достатньо близько 10–20 збоїв на 27-му раунді шифрування. При цьому завдяки віддаленості збоїв від раунду, що аналізується, накопичений матеріал можна використовувати для визначення інших раундових ключів.

Також розглянуто різні шляхи підвищення ефективності запропонованої атаки шляхом використання додаткової інформації. Показано, що використання частково афектованих збоями місць дозволяє знаходити окремі тетради ключа аналітично або суттєво зменшувати кількість можливих кандидатів у ключі. Водночас використання емпірично знайденої інформації щодо істинних розподілів функцій розпізнавання, яке з теоретичної точки зору повинно підвищувати ефективність атаки, на практиці очікуваного підвищення не дало.

Також відкритою залишається проблема побудови оптимальної стратегії проведення пропонованої атаки збоїв для відновлення ключа шифрування загалом. Одержані під час аналізу відомості щодо необхідної кількості даних для успішної атаки на окремий раундовий ключ та/або його частини, а також стосовно поведінки функцій розпізнавання дозволяють побудувати атаку на ключ шифрування в цілому в кожному конкретному випадку. Однак обґрунтоване оптимальне використання знайдених даних для побудови атаки, яка б мінімізувала необхідну для її проведення кількість статистичних даних, та аналіз інших імовірних шляхів підвищення ефективності атаки збоїв на шифр ГОСТ і ГОСТ-подібні шифри усе ж таки залишає можливості для подальших досліджень.

Список використаних джерел

1. Biham E. Differential fault analysis of secret key cryptosystems / E. Biham, A. Shamir // Lecture Notes in Computer Science. – #1294. – Springer-Verlag, 1997. – pp. 513–525.

2. Rivain M. Differential Fault Analysis on DES Middle Rounds / M. Rivain // Proceedings of CHES 2009. – LNCS #5747. – Springer-Verlag, 2009. – pp. 457–469.

3. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования: ДСТУ ГОСТ 28147:2009. – [Чинний від 2009-02-01]. – К. : Держспоживстандарт України, 2008. – 28 с. – (Національний стандарт України).

4. Saarinen M.-J. A Chosen Key Attack against the Secret S-boxes of GOST [Електронний ресурс] / M.-J. Saarinen. – Режим доступу : http://www.researchgate.net/publication/2598060_A_chosen_key_attack_against_the_secret_S-boxes_of_GOST.

5. Яковлєв С. В. Збалансовані критерії якості довгострокових ключових елементів алгоритму шифрування ГОСТ 28147-89 / С. В. Яковлєв // Інформаційні технології та комп'ютерна інженерія. – 2009. – № 1(14). – С. 48–55.

6. Інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації (введено в дію наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 114 від 12.06.2007).

7. Технічні специфікації форматів представлення базових об'єктів національної системи електронного цифрового підпису. Формат підписаних даних (введено в дію спільним наказом Міністерства юстиції України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 1236/5/453 від 20.08.2012).

8. Daemen J. Probability distributions of Correlation and Differentials in Block Ciphers [Електронний ресурс] / J. Daemen, V. Rijmen. – Режим доступу : https://eprint.iacr.org/2005/212.pdf.

9. Огнєв П. Вдосконалення атак збоїв на ДСТУ ГОСТ 28147:2009 з урахуванням особливостей довгострокових ключових елементів : дипломна робота на здобуття освітньо-кваліфікаційного рівня «магістр» / П. Огнєв. – К. : НТУУ «КПІ», Фізико-технічний інститут, 2013. – 71 с.

Рецензенти:
доктор технічних наук, професор
Л. Ковальчук,
доктор фізико-математичних наук,
доцент М. Савчук

Аннотация: В работе рассмотрены атаки сбоев на национальный стандарт шифрования Украины – шифр ДСТУ ГОСТ 28147:2009. Предложен общий алгоритм атаки на данный шифр, проведено экспериментальное оценивание вероятности успеха и количества необходимого статистического материала для атаки при различных условиях на возможности криптоаналитика.

Ключевые слова: блочные шифры, ДСТУ ГОСТ 28147:2009, шифр ГОСТ, атаки по побочным каналам, атаки сбоев.

Annotation: This article considers fault attacks on DSTU GOST 28147:2009 cipher, which is the national encryption standard of Ukraine. General attack algorithm for this cipher is proposed. Probability of success and amount of necessary statistics material for attack on cryptanalytic possibilities under different conditions were experimentally evaluated.

Key words: block ciphers, DSTU GOST 28147:2009, GOST cipher, side-channel attacks, fault attacks.