УДК 004.056.5

Ломаченко І.О. (КПІ ім. Ігоря Сікорського)
к.т.н. Яковлєв С.В. (ВІТІ)

ОЦІНКИ ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ ОДНІЄЇ СХЕМИ ТВІКОВОГО ШИФРУВАННЯ НА ОСНОВІ ШИФРУ „КАЛИНА”

Твікові шифри є новітнім криптографічним примітивом, який використовується як складовий елемент у сучасних алгоритмах автентифікації, автентифікованого шифрування, онлайн-шифрування тощо. На відміну від звичайного шифру, твіковий використовує додатковий відкритий параметр (твік), який суттєво впливає на процес шифрування, але при цьому зміна твіку відбувається значно простіше, аніж зміна ключа шифрування. Серед основних підходів до побудови твікових шифрів можна виокремити побудову схеми твікового шифрування на основі існуючого звичайного блокового шифру, який використовується у режимі „чорної скриньки”, тобто структура шифру не зазнає змін, а усі маніпуляції відбуваються над вхідними та вихідними даними. У роботі розглядається одна з таких схем твікового шифрування; в якості шифру-основи для схеми обрано шифр „Калина”. Досліджено окремі складові такої схеми (раунд шифрування, генерування раундових ключів, обчислення твіку) при обробці одного блоку вхідних даних та наведено аналітичні вирази для обчислювальної складності цих складових у термінах раундів шифрування та базових операцій – побітового та модульного додавання 64-бітових векторів. Окремо розглянуто варіанти реалізації, які використовують таблиці передобчислень для функції шифрування „Калини”, та одержано складність такої реалізації у базових операціях. Показано, що схема, яка розглядається, дозволяє суттєво пришвидшити роботу за рахунок передобчислень певних раундових ключів, пов’язаних із використанням константного ключа шифрування у одному з викликів блокового шифру: кількість необхідних операцій в реалізації з передобчисленням скорочується для різних варіантів шифру „Калина” на 25-35%.

Ключові слова: *блоковий шифр, твік, схема твікового шифрування, шифр «Калина».*

Ломаченко И.О., Яковлев С.В. Оценки вычислительной сложности одной схемы твикового шифрования на основе шифра „Калина”.

Твиковые шифры являются новым криптографическим примитивом, который используется как элемент построения современных алгоритмов аутентификации, аутентифицирующего шифрования, онлайн – шифрования и т.д. В отличие от обычного шифра, твиковый использует дополнительный открытый параметр (твик), который существенно влияет на процесс шифрования, однако его замена происходит гораздо проще, чем замена ключа шифрования. Среди основных подходов к построению твиковых шифров можно выделить построение схемы твикового шифрования на основе существующего блочного шифра, который используется в режиме „чёрного ящика”, т.е. структура шифра не изменяется, а все манипуляции выполняются над входными и выходными данными. В работе рассматривается одна из таких схем твикового шифрования; в качестве шифра-основы для схемы выбран шифр „Калина”. Исследованы отдельные составляющие такой схемы (раунд шифрования, генерирование раундовых ключей, вычисление твика) при обработке одного блока входных данных и приведены аналитические выражения для вычислительной сложности этих составляющих в терминах раундов шифрования и базовых операций – побитового и модульного сложения 64-битовых векторов. Отдельно рассмотрены варианты реализации, которые используют таблицы предвычислений для функции шифрования „Калины”, и получена сложность такой реализации в базовых операциях. Показано, что рассматриваемая схема позволяет существенно ускорить работу за счёт предвычислений некоторых раундовых ключей, связанных с использованием константного ключа шифрования в одном из вызовов блочного шифра: количество необходимых операций в реализации с предвычислениями сокращается для разных вариантов шифра „Калина” на 25-35%.

Ключевые слова: *блочный шифр, твик, схема твиков шифрования, шифр «Калина».*

I. Lomachenko, S. Yakovliev. Computation Complexity Evaluations for One Tweakable Cipher Scheme Based on “Kalyna” Cipher.

Tweakable cipher is a novel cryptographic primitive, which is widely used as a component in modern algorithms for authentication, authenticated encryption, online encryption and so on. Unlike usual block cipher, tweakable cipher uses additional public parameter (tweak), which significantly affects encryption process, but tweak replacement is much easier than encryption key replacement. Among basic tweakable cipher constructions we may highlight schemes based on an existing block cipher as „black box”. In this approach the structure of block cipher is not altered, but all changes and tweak affects are done to input and output data. We studi one of such tweakable cipher scheme based on block cipher with „Kalyna” as underlying cipher. We study individual components of this scheme (e.g. encryption round, key schedule, tweak calculation) for single input block processing; we give analytic expressions for computation complexity of these components in terms of encryption rounds and basic operations (bitwise and modular additions). We examine implementations with precalculation tables for „Kalyna” encryption round and give computation complexity of such implementations in terms of basic operations. The results show that considered tweakable cipher scheme allows significantly speed up computations due to precomputation of some round keys, related to usage of constant encryption

key in one of cipher calls. The number of required operations in the "precomputed" implementations is reduced by 25-35% with different variants of "Kalyna" cipher.

Key words: *block cipher, tweak, encryption tweak scheme, Kalina cipher.*

Постановка завдання

Твіковий блоковий шифр є узагальненням класичного блокового шифру, в якому поряд із вхідним повідомленням та ключем шифрування вводиться додатковий відкритий параметр – „твік", який дозволяє вносити непередбачувані зміни у процес шифрування. Однією з головних функціональних переваг твікових шифрів є можливість заміни твіку на новий із суттєво меншою складністю, ніж заміна ключа шифрування. Було знайдено широкий спектр застосувань твікових шифрів, зокрема, у схемах автентифікації повідомлень (MAC-кодах), схемах шифрування з автентифікацією, онлайн-шифрах тощо. Теорія аналізу та синтезу твікових шифрів є відносно новітньою галуззю. Серед основних підходів до побудови твікових шифрів є використання існуючих криптографічно надійних блокових шифрів в якості основи; в такому випадку дослідження стійкості та властивостей твікового шифру буде здебільшого апелювати до дослідження шифру-основи. Це дозволяє суттєво зменшити складність аналізу твікового шифру. Державним стандартом блокового шифрування в Україні є шифр ДСТУ 7624:2014, відомий під назвою „Калина". Наразі у відкритих джерелах не проводилось аналізу схем твікового шифрування на основі шифру „Калина", тому такі дослідження не тільки є цікавими самі по собі, але й мають суто практичний інтерес з точки зору застосування національних стандартів у сферах використання твікових шифрів.

Аналіз публікацій за темою дослідження

Твікові шифри були формалізовані Лісковим, Рівестом та Вагнером [1], в першу чергу, для задач побудови кодів автентифікації повідомлень. Їх властивості, можливі недоліки, уразливості та потенційні сфери застосування були уточнені у серії подальших робіт (див., наприклад, [2-11]).

Існує щонайменше три підходи до проектування твікових блокових шифрів:

– побудова твікового шифру з нуля;

– побудова на основі наявного блокового шифру шляхом додавання твікового параметру до самої конструкції шифру;

– використання класичного блокового шифру (шифру-основи) в якості „чорної скриньки", вхідні параметри якого модифікуються за допомогою твіку.

Недоліком першого підходу є недостатній рівень дослідженості новоутвореного шифру та складність його аналізу. Здебільшого це викликано відсутністю підходів та методологічної бази для дослідження подібних конструкцій. Другий та третій підходи дають змогу значно легше проводити аналіз шифру. Ми зосередимось саме на третьому підході до побудови твікового шифру, ґрунтуючись на дослідженнях Ваня і Гуо [11]. У своїй роботі ці дослідники побудували атаку відновлення ключа на схему твікового шифрування, розроблену Меннінком [10], і тим самим довели її принципову вразливість. Проаналізувавши виявлені недоліки, Вань та Гуо запропонували свій набір схем твікового шифрування, що використовують блоковий шифр в якості чорного ящика, та довели ряд тверджень стосовно стійкості запропонованих ними конструкцій. Однак ними не розглядалось питання ефективності реалізації таких схем.

Метою даної роботи є одержання оцінок обчислювальної складності реалізації перспективної схеми твікового шифрування на основі шифру «Калина» та аналіз можливого прискорення роботи такої схеми за рахунок деяких передобчислень.

Виклад основного матеріалу

Твіковий блоковий шифр (англ. *tweakable block cipher*) [1] є відображенням виду

$$\tilde{E}: K \times T \times M \to M,$$

де K, T, M – простори ключів, твіків та текстів відповідно (вважається, що простори відкритих текстів та шифротекстів співпадають). З суто практичних міркувань зазвичай вважається, що K, T, M є просторами двійкових векторів. Таким чином, твіковий шифр є сімейством підстановок на M, але параметризується не просто ключем $k \in K$, а ще й

твіковим параметром $t \in T$. Ключ шифрування, як і в звичайних шифрах, є секретним та визначає рівень захищеності, в той час як твік є відкритим параметром, призначеним для привнесення різноманітності у процес шифрування. Обрана нами для дослідження схема твікового шифрування вперше була запропонована Ванєм та Гуо [11]. Вона використовує лише два типи елементів: виклик блокового шифру $E: K \times M \to M$ на заданих параметрах та побітове додавання двох змінних (операція XOR). Формальний опис схеми виглядає таким чином (див. рис. 1):

$$y = E_0(k),$$
$$\tilde{E}_{k,t}(p) = E_{t \oplus y}(p \oplus k) \oplus k \oplus y,$$

де k – секретний ключ, p – відкритий текст, t – твіковий параметр, y – допоміжне значення: результат шифрування блоку, який збігається із ключем k, на ключі, що складається з усіх нульових бітів. Зауважимо, що дана схема вимагає, щоб довжина ключа шифрування, довжина твіку та довжина блоку збігались, тобто $K = T = M$.

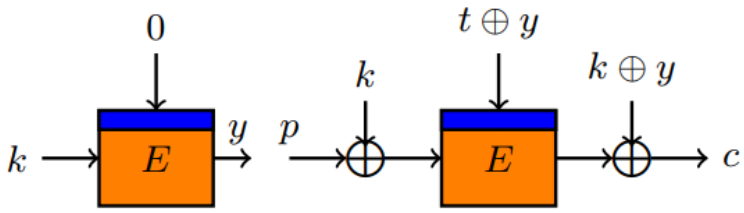

Рис. 1. Схема твікового шифрування, яка розглядається у даній роботі

Вибір в якості основи саме цієї схеми обумовлюється такими міркуваннями:

для даної схеми було наведено детальне обґрунтування її стійкості як твікового шифру за умови використання надійного блокового шифру [11];

схема може використовувати будь-який блоковий шифр в якості чорного ящику (з урахуванням обмежень на довжини ключа та блоку), а отже, не залежить від його специфіки;

схема використовує два виклики внутрішнього шифру, що є мінімальним значенням для забезпечення стійкості серед відомих схем твікового шифрування;

один з викликів шифру-основи відбувається на фіксованому константному ключі, що дозволяє підвищити швидкість роботи через передобчислення.

Далі розглянемо обрану схему твікового шифрування, в якій в якості шифру-основи взято шифр „Калина” [12], який є національним стандартом шифрування України, та одержимо оцінки обчислювальної складності виконання такої схеми.

Шифрування одного блоку відкритого тексту у схемі твікового шифрування потребує двох викликів шифру E на різних параметрах, а також 4 додаткові побітові додавання блоків. Таким чином, складність $Compl(\tilde{E})$ такої процедури дорівнює

$$Compl(\tilde{E}) = 2Compl(E) + 4Compl(XOR),$$

де $Compl(E)$ – складність одного шифрування за допомогою шифру E, $Compl(XOR)$ – складність виконання операції побітового додавання для даного розміру блоку. Зауважимо, що дана оцінка має місце для усього сімейства схем твікування, запропонованих у [11], з точністю до константи. Складність одного виклику шифру E дорівнює $Compl(E) = KS + CT$, де KS – складність виконання схеми розгортання ключів, CT – складність шифруючого перетворення. В свою чергу, складність CT визначається складністю RC виконання одного раундового перетворення шифрування, кількістю раундів r та складністю додавання усіх раундових ключів в процесі шифрування. Розглянемо схематичну структуру раундового перетворення та схеми розгортання ключів шифру „Калина”; детальний опис даного шифру наведено у [12]. Вхідний блок шифру „Калина” розглядається як матриця розміром $8 \times n$, де кількість стовпчиків n дорівнює 2, 4 або 8. Раундове перетворення складається з таких елементів, як заміна байтів у матриці стану (процедура SubBytes), циклічний зсув рядочків матриці (процедура ShiftRows) та перемішування стовпчиків шляхом їх множення на певну

матрицю (процедура MixColumns). Хоча раундове перетворення має доволі складну структуру, важливим є те, що усі необхідні обчислення можна зробити заздалегідь, використавши 16 кб допоміжної пам'яті; при такому підході кожен стовпчик виходу буде обчислюватись як побітове додавання восьми спеціальних передобчислених 64-бітових векторів, які визначаються байтами вхідного блоку. Шифр „Калина" використовує дві операції додавання раундового ключа: додавання за модулем 2^{64} (операція ADD) та побітове додавання (операція XOR). Шифруюче перетворення полягає в ітеративному застосуванні раундових перетворень, відокремлених додаваннями із раундовим ключем. Перед першим раундовим перетворенням та після останнього перетворення додавання із ключем здійснюється за модулем 2^{64}, а між раундовими перетвореннями – завжди побітове. Оскільки шифр „Калина" за своєю структурою орієнтований на реалізацію у 64-бітових обчислювальних архітектурах, доцільно розглядати в якості базових операцій для оцінювання складності операції над 64-бітовими векторами. Позначимо через c_1 складність виконання побітового додавання 64-бітових векторів, а через c_2 – складність виконання додавання за модулем 2^{64}. Тоді, оскільки блок шифру „Калина" складається з n 64-бітових стовпчиків, складності усіх наведених перетворень можна знайти за допомогою таких перетворень:

$$Compl(XOR) = c_1 \cdot n,$$
$$Compl(ADD) = c_2 \cdot n.$$

Відповідно, складність шифруючого перетворення дорівнює

$$CT = 2c_2 n + (r-1)c_1 n + r \cdot RC,$$

де r – кількість раундів шифрування, RC – складність раундового перетворення. При використанні таблиць передобчислень маємо $RC = 7n \cdot c_1$ та, відповідно,

$$CT = 2c_2 n + (8r-1)c_1 n.$$

Схема розгортання ключів шифру „Калина"складається з двох етапів:

– обчислення з ключа шифрування проміжного ключа;
– обчислення з проміжного ключа раундових ключів.

Проміжний ключ генерується трьома послідовними застосуваннями раундового перетворення до певної константи, перед кожним з яких іде модульне додавання із ключем шифрування. Складність цієї частини схеми розгортання дорівнює $3nc_2 + 3RC$.

Раундові ключі з парним індексом генеруються за допомогою процедури, яка складається з двох раундових перетворень, двох модульних додавань з проміжним ключем та одного побітового додавання з ключем. Відповідно, складність генерування раундових ключів із парними індексами дорівнює $2nc_2 + nc_1 + 2RC$. Раундові ключі з непарним індексом генеруються шляхом циклічного зсуву попереднього раундового ключа на кількість бітів, яка залежить від довжини блоку; в усіх випадках величина зсуву кратна 8 (тобто блок зсувається побайтно), але не кратна 64 (тобто 64-бітові вектори-стовпчики перемішуються між собою). Стандартна реалізація такої процедури вимагає для кожного стовпчика виходу одного побітового додавання частин двох стовпчиків входу, які одержуються нециклічними зсувами та операціями побітового логічного «ТА» із певними масками. Вважаючи, що складність логічного «ТА» та побітового додавання 64-бітових векторів співпадають, а складність нециклічного зсуву є знехтовно малою у порівнянні, одержимо складність генерування раундових ключів із непарними індексами $3nc_1$. Всього схема розгортання раундових ключів генерує $r+1$ ключ, причому r завжди є парним числом, а ключі індексуються з нуля (тобто ключів з парними індексами на один більше). Відповідно, маємо загальну складність схеми розгортання раундових ключів шифру „Калина":

$$KS = 3nc_2 + 3RC + \left(\frac{r}{2}+1\right)(2nc_2 + nc_1 + 2RC) + \frac{r}{2}(3nc_1) =$$
$$= (2r+1)nc_1 + (r+5)nc_2 + (r+5)RC.$$

Таким чином, складність одного виклику шифру «Калина» дорівнює

$$Compl(E) = KS + CT =$$
$$= 3rnc_1 + (r+7)nc_2 + (2r+5)RC,$$

а складність схеми твікового шифрування для обробки одного блоку –

$$Compl(\tilde{E}) = 2Compl(E) + 4Compl(XOR) =$$
$$= (6r + 4)nc_1 + (2r + 14)nc_2 + (4r + 10)RC.$$

При використанні таблиць передобчислень раундового перетворення одержуємо таку складність одного виклику шифру «Калина» та одного виклику схеми твікового шифрування:

$$Compl(E) = (17r + 35)nc_1 + (r + 7)nc_2,$$
$$Compl(\tilde{E}) = (34r + 74)nc_1 + (2r + 14)nc_2.$$

Однак необхідно зауважити, що при першому виклику шифру E у схемі твікового шифрування $\tilde{E}$ використовується один й той самий константний (нульовий) ключ. У цьому випадку раундові ключі можуть бути передобчислені заздалегідь та збережені для підвищення швидкості роботи схеми в цілому; витрати пам'яті при цьому незначні: в найгіршому випадку, для шифру «Калина-512», для зберігання усіх раундових ключів необхідно 1216 байтів. Позначимо такий варіант реалізації шифру із передобчисленими раундовими ключами як $E_{precalc}$, а відповідний варіант реалізації схеми твікового шифрування – як $\tilde{E}_{precalc}$. Тоді маємо такі значення для складностей:

$$Compl(E_{precalc}) = CT,$$
$$Compl(\tilde{E}_{precalc}) = Compl(E_{precalc}) + Compl(E) + 4Compl(XOR) =$$
$$= CT + Compl(E) + 4Compl(XOR).$$

Підставивши одержані вище вирази для складностей процедур, які використовуються, одержуємо остаточно

$$Compl(\tilde{E}_{precalc}) = (4r + 3)nc_1 + (r + 9)nc_2 + (3r + 5)RC,$$

а при використанні таблиць передобчислень для раундового перетворення –

$$Compl(\tilde{E}_{precalc}) = (25r + 38)nc_1 + (r + 9)nc_2.$$

У таблиці 1 наведено конкретні вирази складностей схеми твікового шифрування для усіх варіантів шифру „Калина" (із розмірами блоку 128, 256 та 512 бітів; нагадаймо, що в обраній схемі твікового шифрування довжина ключа повинна співпадати із довжиною блоку), а у таблиці 2 – аналогічні вирази для реалізації, яка використовує таблиці передобчислень для раундового перетворення. Порівнявши ці значення, можна побачити, що наявність константного ключа у схемі твікового шифрування, яка розглядалась у роботі, дозволяє з'економити від чверті до третини усіх операцій за рахунок передобчислень.

Таблиця 1

Складність схеми твікового шифрування $\tilde{E}$ на основі шифру «Калина»

Версія шифру	r	n	Складність схеми $\tilde{E}$	Складність схеми $\tilde{E}_{precalc}$
128	10	2	$128c_1 + 68c_2 + 50RC$	$86c_1 + 38c_2 + 35RC$
256	14	4	$352c_1 + 168c_2 + 66RC$	$236c_1 + 92c_2 + 47RC$
512	18	8	$896c_1 + 400c_2 + 82RC$	$600c_1 + 216c_2 + 59RC$

Висновки. У даній роботі розглядалась одна зі схем твікового шифрування, запропонованих Ванєм та Гуо, яка відрізняється використанням мінімально можливої кількості викликів блокового шифру-основи та використанням константного ключа шифрування в одному з викликів. У якості шифру-основи було обрано блоковий шифр „Калина". Було показано, що складність реалізації такої схеми суттєво зменшується за рахунок передобчислень раундових ключів, що має сенс при використанні константного ключа шифрування: загальна кількість операцій над 64-бітовими векторами скорочується на третину в найкращому випадку, хоча виграш у швидкості зменшується із кількістю раундів шифрування. Проведений аналіз дозволяє рекомендувати схему твікового шифрування, яка розглядалась, для практичних застосувань. Одержані результати природно поширюються на

інші схеми твікового шифрування (зокрема, запропоновані Ванєм та Гуо), які мають аналогічні конструктивні особливості.

Таблиця 2

Складність схеми твікового шифрування при використанні передобчислень раундового перетворення шифру «Калина»

Версія шифру	r	n	Складність схеми $\tilde{E}$	Складність схеми $\tilde{E}_{precalc}$
128	10	2	$828c_1 + 68c_2$	$576c_1 + 38c_2$
256	14	4	$2200c_1 + 168c_2$	$1152c_1 + 92c_2$
512	18	8	$5488c_1 + 400c_2$	$3906c_1 + 216c_2$

Напрямками подальших досліджень є пошук інших надійних схем твікового шифрування з ефективною реалізацією, інтеграція таких схем із національними стандартами блокового шифрування, а також побудова сучасних криптографічних алгоритмів (таких, як онлайн-шифри) на основі шифру „Калина”.

ЛІТЕРАТУРА

1. Liskov M. Tweakable block ciphers / M. Liskov, R. L. Rivest, D. Wagner // In Yung M., ed.: Advances in Cryptology – CRYPTO 2002. – LNCS, vol. 2442. – Springer, 2002. – pp. 31 – 46.

2. Halevi S. A Tweakable Enciphering Mode. / S. Halevi, P. Rogaway // In Boneh D., ed.: Advances in Cryptology – CRYPTO 2003. – LNCS, vol. 2729. – Springer, 2003. – pp. 482 – 499.

3. Chakraborty D. A General Construction of Tweakable Block Ciphers and Different Modes of Operations / D. Chakraborty, P. Sarkar // In Lipmaa H., Yung M., Lin D., eds.: Inscrypt 2006. – LNCS, vol. 4318. – Springer, 2006. – pp. 88 – 102.

4. OnTweaking Luby-Rackoff Blockciphers / [Goldenberg D., Hohenberger S., Liskov M., Schwartz E.C., Seyalioglu H.] // In Kurosawa K., ed.: Advances in Cryptology – ASIACRYPT 2007. – LNCS, vol. 4833. – Springer, 2007. – pp. 342 – 356.

5. Mitsuda A. Tweakable Pseudorandom Permutation from Generalized Feistel Structure / A. Mitsuda, T. Iwata // In Baek J., Bao F., Chen K., Lai X., eds.: ProvSec 2008. – LNCS, vol. 5324. – Springer, 2008. – pp. 22 – 37.

6. Landecker W. Tweakable Blockciphers with Beyond Birthday-Bound Security / W. Landecker, T. Shrimpton, R.S. Terashima // In Safavi-Naini R., Canetti R., eds.: Advances in Cryptology – CRYPTO 2012. – LNCS, vol. 7417. – Springer, 2012. – pp. 14 – 30.

7. Parallelizable and Authenticated Online Ciphers / [Andreeva E., Bogdanov A., Luykx A., Mennink B., Tischhauser E., Yasuda K.] // In Sako K., Sarkar P.,eds.: Advances in Cryptology – ASIACRYPT 2013, part I. – LNCS, vol. 8269. – Springer, 2013. – pp. 424 – 44.

8. Lampe R. Tweakable Blockciphers with Asymptotically Optimal Security. / R. Lampe, Y. Seurin // In Moriai S., ed.: FSE 2013. – LNCS, vol. 8424. – Springer, 2013. – pp. 133 – 151.

9. Jean J. Tweaks and Keys for Block Ciphers: The TWEAKEY Framework / J. Jean, I. Nikolic, T. Peyrin // In Sarkar P., Iwata T., eds.: Advances in Cryptology – ASIACRYPT 2014, part II. – LNCS, vol. 8874. – Springer, 2014. – pp. 274 – 288.

10. Mennik B. Optimally Secure Tweakable Blockciphers / B. Mennik // IACR Cryptology ePrint Archive, 2015, #363. – http://eprint.iacr.org/2015/363.

11. How to Build Fully Secure Tweakable Blockciphers from Classical Blockciphers / [Wang L., Guo J., Zhang G., Zhao J., Gu D.] // IACR Cryptology ePrint Archive, 2016, #876. – https://eprint.iacr.org/2016/876.pdf

12. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення: ДСТУ 7624:2014. – К.: Держспоживстандарт України, 2015. – 238 с.