УДК 004.056.55 **doi: 10.26906/SUNZ.2018.2.083**

И.В. Лысенко, Р.С. Нос

Национальный аэрокосмический университет имени М.Е. Жуковского «ХАИ», Харьков

МОДЕЛЬ КРИПТОПРЕОБРАЗОВАНИЯ ДАННЫХ ПО СХЕМЕ ЗАДАЧИ О РЮКЗАКЕ НА ОСНОВЕ ПРИНЦИПА ДИВЕРСНОСТИ

Рассматривается модель криптопреобразований, базирующихся на схеме задачи о рюкзаке на основе принципа диверсности. Для повышения криптостойкости предложено модифицировать рюкзачную криптосистему путем введения большего количества рюкзаков и произвольного шифрования блоков текста с их помощью. Предложенный на основе принципа диверсности подход позволяет снизить риски непарируемых ситуаций, связанных с возможностями со стороны производителей криптопродукции (несимметричных алгоритмов шифрования) встраивать потайные лазейки в схемы генерации ключей криптоалгритмов.

***Ключевые слова**: диверсность, криптоалгоритмы, криптостойкость, задача о рюкзаке*

Введение

Постановка задачи. Несмотря на многие достижения современной криптографии задача обеспечения конфиденциальности данных, передаваемых по незащищённым каналам, не потеряла своей актуальности. Традиционно эта задача решается путём разработки новых и совершенствования существующих криптогра-фических алгоритмов, преимущественно относящихся к классу несимметричных. Что касается несимметричных алгоритмов шифрования, то, как известно, наибольшую популярность приобрели RSA-подобные криптоалгоритмы, стойкость которых основана на трудоёмкости решения задачи факторизации большого числа, а также El Gamal-подобные криптоалгоритмы, стойкость которых определяется трудоёмкостью решения задачи дискретного логарифмирования в простом и расширенном конечном поле (в том числе и в группе точек эллиптической кривой). В то же время, начиная с конца 1970-х годов, для обеспечения конфиденциальности данных были предложены различные варианты криптоалгоритмов, в основу стойкости которых положена труднорешаемая задача о рюкзаке – так называемые рюкзачные криптоалгоритмы.

Первый такой криптоалгоритм в 1978 году был предложен американскими криптографами Мерклом и Хеллманом. Для проверки своего алгоритма на стойкость разработчики назначили награду за его компрометацию, и уже в 1982 году математик Ади Шамир успешно его «взломал». Однако, несмотря на компрометацию оригинальной схемы, вплоть до наших дней не прекращаются попытки улучшить и доработать алгоритм. Так, в 1980 году без помощи друг друга Рон Грэм и Ади Шамир нашли способ улучшить защищенность схемы Меркла-Хеллмана, но уже в 1983 году схема была скомпрометирована. В 1985 году был представлен алгоритм, базирующийся на модульных рюкзаках с использованием китайской теоремы об остатках. Позднее, в 1986 году Харальд Нидеррайтер предложил рюкзачную криптосистему на базе алгебраической теории кодирования, а затем в 1988 году мир увидела система с использованием принципа мультипликативного рюкзака, криптостойкость которой была дополнительно повышена в 2001 за счет использования алгоритма Пита Шальквейка. Удачной на длительное время оказалась и разработанная в 1991 идея многостадийной криптосистемы на основе задачи о рюкзаке. Суть схемы заключается в фиксировании рюкзачного вектора для каждого этапа, причем выходные данные после каждого цикла алгоритма используются в качестве исходного текста для следующего. В 1995 году был предложен новый подход к схеме Меркла-Хеллмана на основе диофантовых уравнений, но вскоре после этого несколько математиков независимо друг от друга показали, что эта криптосистема не является криптостойкой. Затем в 1996 году Куникацу Кобаяси и Масаки Кимура представили модернизированную рюкзачную криптосистему, базирующуюся на возможности отправителя выбирать ключ шифрования из целого набора. И наконец, в 2015 году Нэйтан Хэмлин и Уильям Уэбб из Вашингтонского государственного университета создали рюкзачный алгоритм, базирующийся на альтернативных способах представления чисел с использованием повторяющихся последовательностей. Данный алгоритм по сей день не был скомпрометирован в отличие от вышеприведенных модификаций, включающих модификации с использованием конечных групп; на основе прямого произведения циклических групп; на основе сплетения групп; с использованием мультипликативных рюкзаков и пр. Результаты исследований приведенных алгоритмов представлены в работах [1–4]. На наш взгляд, для обеспечения лучшей криптостойкости может быть также эффективно использован многоверсионный подход (принцип диверсности), который традиционно используется для успешного решения задачи обеспечения заданного уровня надёжности и гарантоспособности компьютерных и компьютеризированных систем. Некоторые результаты, полученные в рамках этого подхода, описаны в работах [5, 6].

© И.В. Лысенко, Р.С. Нос

Ещё одним аргументом в пользу применения принципа диверсности для построения криптосистем является то, что реализации некоторых криптоалгоритмов предполагают использование некоторых фиксированных (определяемых разработчиком) параметров, что, в принципе, может служить намёком на возможность использования потайных лазеек. При этом под потайной лазейкой (потайным входом) понимается наличие некоторого секрета, преднамеренно внедрённого разработчиком программной или аппаратной реализации криптоалгоритма с целью раскрытия содержимого зашифованных данных без знания секретного ключа пользователей либо раскрытия секретного ключа [7].

Кроме того, что касается несимметричной криптографии, в частности, несимметричных алгоритмов шифрования, имеет место принципиальная возможность встраивания лезеек в схемы генерации ключей этих алгоритмов со стороны кампаний-разработчиков криптопродукции, что потенциально даёт им возможность раскрыть секретный ключ пользователя-потребителя этой продукции [7].

В данном случае речь идёт о так называемом SETUP-механизме (SETUP – Secretly Embedded Trapdoor with Universal Protection – секретно встроенная лазейка с универсальной защитой), который видоизменяет криптоалгоритм таким образом, что позволяет производителю криптосистемы получать секретную информацию пользователя (чаще всего информацию о его секретных ключах). В то же время, для любого наблюдателя, отличного от разработчика, функционирование модифицированного крипто-алгоритма неотличима от работы исходного.

Цель данной работы: описание подхода, основанного на принципе диверсности, позволяющего повысить криптостойкость и свести к минимуму описанную выше угрозу на примере криптоалгоритма на базе классической схемы задачи о рюкзаке.

Основная часть

Принцип встраивания лазейки в криптоалгоритмы. Так, например, криптоалгоритм RSA модифицируется следующим образом. Производитель криптоалгоритма выбирает некоторое несимметричное криптопреобразование NST = {E(·), D(·)}, где E(·), D(·) – прямое (шифрующее) и обратное (дешифрующее) преобразования соответственно, которым соответствует пара ключей (открытый и секретный). В процессе генерации ключей SETUP-механизмом первоначально выбираются простые числа p и q, после чего вычисляется открытый ключ пользователя как функция от E(·), т.е. $K_o = E(p)$. Если выполняется условие взаимной простоты чисел E(p) и φ(N), где N = p·q, то K_o объявляется открытым ключом пользователя. В противном случае выбирается другое значение p и вычисляется значение секретного ключа Кс как величина Ко, обратная по модулю φ(N). По открытому ключу пользователя производитель программной или аппаратной реализации криптоалгоритма может рассчитать секретный параметр p: $p = D(K_o)$, после чего определить другой секретный параметр q = N/p, а затем, вычислив функцию Эйлера φ(N) = (p-1)(q-1), определить секретный ключ за полиномиальное время [5].

Далее опишем принцип встраивания лазейки в рюкзачный криптоалгоритм. Рюкзачным вектором называется $A = (a_1,...,a_n)$ – набор из n отличающихся упорядоченных натуральных чисел a_i. При этом $n \geq 3$. Начальными данными рюкзачной задачи называем пару (A, α). В данном случае в качестве A выступает рюкзачный вектор, а α — натуральное число. Решением для описанного выше входа (A, α) станет некоторое подмножество из A, в котором α будет суммой элементов. Так как речь идет о подмножестве, следует учитывать, что a_i не должны повторяться в сумме. Иногда рюкзачную задачу также называют «задачей о сумме размеров». Традиционно суть задачи о рюкзаке сводится к выяснению, обладает исходный набор данных (A, α) конкретным решением или нет. В случае с криптографией, необходимо для заданного входа (A, α) найти решение, зная точно при этом, что данное решение существует. И первый и второй варианты задачи являются NP-полными. Также известны варианты задачи, которые лежат за рамками класса NP [8].

Вектор A используется для шифрования блока C из n бинарных символов. Осуществляется это суммированием тех элементов A, для которых в соответствующих позициях C стоит единица. Если мы работаем с криптосистемой с открытым ключом, то обозначив эту сумму через α, расшифрование сводится к нахождению C по α или по A и α. Второй вариант как раз и является криптографическим вариантом рюкзачной задачи. Вектор C справедливо можно рассматривать как двоичный вектор-столбец. В таком случае α будет равно произведению AC. Продемонстрируем следующим образом: положим n = 6 и A = (4, 42, 6, 1, 22, 11). В таком случае двоичные блоки (1, 1, 0, 0, 1, 0) и (1, 0, 1, 1, 0, 1) будут шифроваться как 68 и 22 соответственно. Для конкретного вектора A все шифртексты будут числами, не превосходящими 86, и каждому шифртексту при этом будет соответствовать не более одного исходного текста. В случае A = (14, 28, 56, 82, 90, 132, 197, 284, 341, 455), α = 515 будет соответствовать нескольким исходным текстам (1, 1, 0, 0, 0, 1, 0, 0, 1, 0), (0, 1, 1, 0, 1, 0, 0, 0, 1, 0), (1, 0, 0, 1, 1, 1, 1, 0, 0, 0). Это становится понятным, если начинать читать A справа налево. Для примера, 455 не может входить в решение, так как 60 (515−455) нельзя выразить в виде суммы. Продолжая рассуждение, можно продемонстрировать, что для шифртекста α = 516 не существует верного исходного текста. Также становится очевидным, что в сумму не может входить ни одно из четырех последних чисел из рюкзачного вектора, тогда как сумма всех предыдущих чисел будет слишком маленькой. Для шиф-

ртекста α = 517 единственным исходным текстом является (1, 1, 1, 0, 1, 1, 1, 0, 0, 0). Подобные примеры демонстрируют тот факт, что криптоанализ для некоторых исходных данных крипторюкзачной задачи может быть достаточно легким. В случае, когда необходимо добиться однозначности расшифрования, для каждого α, все входы (A, α) должны иметь единственное решение. Будем называть подобные векторы A инъективными. Следовательно, и порожденная вектором A функция тоже является инъективной. В приведенных выше примерах первый вектор является инъективным, второй же — нет. Существуют векторы A, для которых все входы (A, α) легко решаемы. Работая с подобными векторами, не сложно построить двухстороннюю систему: и отправитель сообщения, и получатель будут знать исходный вектор A. Однако, если вектор B раскрыт как ключ шифрования, то непосредственный получатель должен обладать определенной секретной информацией. Необходима она для преобразования и ключа B, и шифртекста в легкорешаемый вход рюкзачной задачи. Этого можно достигнуть с помощью сверхвозрастающих векторов. Рюкзачный вектор $A = (a_1,...,a_n)$ называется сверхвозрастающим, если и только если $a_j > a_{j-1}$ справедливо для всех j = 2,...,n. Определим для вектора A: max A = max(a_j |1 ≤ j ≤ n).

Пусть x – неотрицательное число. Целую часть числа x обозначим через [x], т. е. наибольшее целое, меньшее или равное x. Для целых x и m ≥ 2 обозначим через (x, mod m) наименьший неотрицательный остаток от деления x на m. Очевидно, что (x, modm) = x − [x/m]·m. Далее необходимо определить 2 варианта понятия модульного умножения. Возьмем вектор A, целое число m > max A и натуральное число t < m, взаимно-простое с m. Если $B = (b_1, \ldots, b_n)$ такой вектор, что $b_i = (ta_i, \text{mod } m)$ для i = 1, … , n , то можно сказать, что вектор B получен из A с помощью модульного умножения относительно модуля m и множителя t. То, что числа взаимно-простые, гарантирует, что существует число $t^{-1} = u$, такое, что tu ≡ 1 (mod m) и 1 ≤ u < m. Следовательно, A так же получается из B модульным умножением относительно m и u. В случае если предыдущее условие $m > \max A$ заменить более сильным $m > \sum_{i=1}^{n} a_i$, то справедливо говорить, что B получается из A сильным модульным умножением относительно m и t. Стоит отметить, что сейчас нельзя также сказать, что A получается из B сильным модульным умножением относительно m и u. Так как условие $m > \sum_{i=1}^{n} b_i$, не всегда выполняется. При этом, A получается из B модульным умножением относительно m и u. Разработчик криптосистемы выбирает A, t, m, B так, что вектор A является сверхвозрастающим, а вектор B образуется из A сильным модульным умножением относительно m и t. Вектор B используется как ключ шифрования и бинарные блоки (длинной n) посылаются к проектировщику как числа β, которые получены с помощью вектора B (как описано выше). Криптоаналитик должен решать задачу о рюкзаке для исходных данных (B, β). Создатель же вычисляет α = (uβ, mod m) и решает задачу для данных (A, α) [8].

Модель реализации рюкзачной криптосистемы системы на основе принципа диверсности. В самом общем виде идея предлагаемого подхода заключается в том, чтобы производитель криптосистемы предоставлял возможность пользователю, во-первых, генерировать некоторое множество M_p сверхвозрастающих рюкзаков A_i, j = 1,…,n, которые могли бы использоваться для шифрования и расшифрования разных блоков одного сообщения неизвестным ни для кого образом (неопределённость в том, какому блоку шифруемого сообщения какой ключ A_i из множества M_p соответствует), и, во-вторых, чтобы пользователь имел возможность генерировать некоторый секретный параметр SP (например, на основе парольной фразы), благодаря чему возможно обеспечить упомянутую выше неопределённость (для злоумышленника) в шифровании блоков сообщения, а также обеспечить получателю зашифрованного сообщения возможность однозначного понимания того, какой блок зашифрованных данных каким рюкзаком A_j из множества M_p должен быть расшифрован.

На рис. 1 изображён пример, иллюстрирующий описанную идею для случая, когда сообщение N состоит из 10 блоков данных N_i (i = 1,….n) и $|M_p| = 3$.

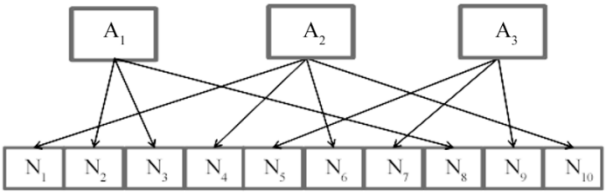

Рис. 1. Иллюстрация реализации принципа диверсности

Согласно данному рисунку, первый рюкзачный вектор используется для шифрова-ния/расшифрования 2, 3 и 8 блоков данных, второй – 1, 4, 6, 10 блоков данных, а третий – 5, 7, 9 блоков данных. Очевидно, что число вариантов распределения «рюкзаков» по блокам данных равно $3^{10} = 59049$, а в общем случае для n блоков данных и $|M_p| = h$ это число равно h^n.

Очевидно, что для реализации данного похода необходимо обеспечить однозначность (для отправителя и получателя зашифрованного сообщения) соответствия между блоками данных и используемыми ключами из множества M_p. Это может быть достигнуто, например, с помощью алгоритма:

0. $SP_{(2)} \rightarrow SP_{(10)}$.

1. $SP_{(10)}(\text{mod } h) = t_{1(10)}$.

2. $t_{1(10)} \rightarrow t_{1(2)}$; $SP_{(2)} \oplus t_{1(2)} = S_{1(2)}$; $S_{1(2)} \rightarrow S_{1(10)}$; $S_{1(10)}(\text{mod } h) = t_{2(10)}$.

for i = 3 … n do

$t_{i-1(10)} \rightarrow t_{i-1(2)}$; $S_{i-2(2)} \oplus t_{i-1(2)} = S_{i-1(2)}$; $S_{i-1(2)} \rightarrow S_{i-1(10)}$; $S_{i-1(10)}(\text{mod } h) = t_{i(10)}$.

В алгоритме приняты следующие обозначения: $SP_{(2)}$, $SP_{(10)}$ – двоичное и десятичное представление секретного параметра SP ; $S_{i(2)}$, $S_{i(10)}$ – двоичное и десятичное представление промежуточного параметра S, соответствующее i-му блоку данных; $t_{i(2)}$, $t_{i(10)}$ – двоичное и десятичное представление параметра t_i, устанавливающего соответствие между i-м блоком шифруемых/дешифруемых данных и используемым рюкзачным вектором A_i, j = = 1,…,h (например, если $t_7 = 5$, то это значит, что для шифрования и расшифрования седьмого блока данных используется пятый «рюкзак»); ⊕ – оператор суммирования по модулю 2. Как видно из алгоритма, вначале двоичное значение секретного параметра преобразовывается в десятичное и на первом шаге устанавливается то, какой «рюкзак» из множества M_p будет использован для шифрования/расшифрования первого блока данных. Затем (на втором шаге) на основании ранее полученных данных определятся, какая рюкзачный вектор будет использован для шифрования/расшифрования второго блока данных. По аналогии производятся вычисления для остальных блоков данных. В итоге, в результате вычислений по данному алгоритму будет получено соответствие между блоками данных и рюкзачными векторами.

Заключение

Таким образом, можно подытожить, что предложенный подход на основе принципа диверсности позволяет снизить риски неконтролируемых ситуаций, связанных с возможностями со стороны разработчиков криптопродукции встраивать секретные лазейки в схемы генерации ключей криптоалгоритмов. Недостатком похода является увеличение ключевого материала и, очевидно, некоторое увеличения времени криптопреобразования в сравнении с реализацией классической схемы рюкзачной криптосистемы.

Ввиду последнего обстоятельства нужно отметить, что речь может идти об определении того, для сообщений какого размера целесообразно использовать данный подход с точки зрения соотношения между заданным уровнем криптостойкости и времени криптопреобразований (т.к. криптостойкость в этом случае будет, очевидно, тем выше, чем больше блоков данных в сообщении). Кроме того, условием реализации данного подхода является знание отправителем и получателем сообщений некоторого общего секретного параметра, который может быть сформирован, например, по протоколу Диффи-Хеллмана. В таком случае, очевидно, можно говорить о том, что предлагаемый подход можно назвать гибридным.

Список литературы

1. Животова А.Е. Модификация криптосистемы с открытым ключом на основе «задачи о рюкзаке» / А.Е. Животова., Н. Д. Зюляркина, Ю. О. Костыгина // Вестник УрФО.. – 2014. – Вип. 1(11). – С. 16–20.

2. Сурина А. А. Рюкзачная криптосистема на основе прямого произведения циклических групп / А. А. Сурина // ОППМ. – 2015. – Вип. 2(22). – С. 95–97

3. Hamlin N. A Knapsack-like Code Using Recurrence Sequence Representations / N. Hamlin, B. Krishnamoorthy, W. Webb // The Fibbonachi Quarterly. – 2015. – 1(53). –24–34

4. Шнайер Б. Прикладная криптография: протоколы, алгоритмы, исходные тексты на языке Си: пер. с англ / Б. Шнайер – М.: «Триумф», 2002. – 820 с.

5. Лысенко И. В. Модели реализации принципа диверсности в несимметричной криптографии / И. В. Лысенко // Системи управління, навігації і зв'язку. – К.: ЦНДІ НіУ, 2012. – Вип. 1(21). Том 2. – С. 206–208..

6. Лысенко И. В. Модели обеспечения конфиденциальности сообщений средствами криптографии на основе принципа диверсности / И. В. Лысенко, Д. А. Филиппов // Системи обробки інформації. – Харків: ХУПС. – 2006. – Вип. 2(51). – С. 76–80.

7. Жуков А. Криптосистемы со встроенными лазейками / А. Жуков // BYTE. –2007. – №2. – С.45–51

8. Саломаа А. Криптография с открытым ключом: пер. с англ. / А. Саломаа – М.: Мир, 1995. – 318 с.

Надійшла до редколегії 21.02.2018

Рецензент: д-р техн. наук, проф. В.С. Харченко, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

МОДЕЛЬ КРИПТОПЕРЕТВОРЕННЯ ДАНИХ ЗА СХЕМОЮ ЗАДАЧІ ПРО РЮКЗАК НА ОСНОВІ ПРИНЦИПУ ДИВЕРСНОСТІ

І.В. Лисенко, Р.С. Нос

Розглядається модель криптоперетворень, що базуються на схемі завдання про рюкзак на основі принципу диверсності. Для підвищення криптостійкості запропоновано модифікувати рюкзачну криптосистему шляхом введення більшої кількості рюкзаків і довільного шифрування блоків тексту з їх допомогою. Запропонований на основі принципу диверсності підхід дозволяє знизити ризики неконтрольованих ситуацій, пов'язаних з можливостями з боку виробників криптопродукції (несиметричних алгоритмів шифрування) вбудовувати потаємні лазівки в схеми генерації ключів криптоалгоритмів.

***Ключові слова**: диверсність, криптоалгоритми, криптостійкість, задача про рюкзак.*

MODEL OF DATA CRYPTOTRANSFORMATION BY THE SCHEME OF KNAPSACK PROBLEM BASED ON THE DIVERSITY PRINCIPLE

I.V. Lysenko, R.S. Nos

The article considers the model of crypto-transformations, which are based on the knapsack problem scheme based on the principle of the diversity. To increase the cryptographic stability, it was proposed to modify the knapsack cryptosystem by increasing knapsacks number and randomly encrypting blocks of text with their help. The approach proposed on the basis of the principle of diversity allows us to reduce the risks of uncontrolled situations related to the opportunities on the possibilities of crypto products producers (asymmetric encryption algorithms) to build secret loopholes into crypto-algorithms key generation schemes.

***Key words:** derversity, cryptographic algorithms, cryptoscope, knapsack problem.*