УДК 004.056.55

КОМБИНАТОРНЫЕ СВОЙСТВА КЛЮЧЕВОГО РАСПИСАНИЯ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

А.А. КУЗНЕЦОВ, Ю.И. ГОРБЕНКО, Д.В. ИВАНЕНКО

Исследуются комбинаторные свойства ключевого расписания блочных симметричных шифров в предположении, что цикловые (раундовые) ключи формируются случайно, равновероятно и независимо друг от друга. Для абстрактного описания такого формирования используется модель случайной однородной подстановки. Полученные аналитические выражения позволяют оценить мощность множества реализуемых отображений зашифрования-расшифрования, получить оценки вероятностных свойств последовательностей раундовых ключей и отношений среднего числа различных ключевых последовательностей к мощности множества различных мастер-ключей. Результаты имитационного моделирования подтверждают достоверность и обоснованность полученных аналитических выражений.

Ключевые слова: ключевое расписание, цикловые ключи, комбинаторные свойства, блочные симметричные шифры.

1. ПОСТАНОВКА ПРОБЛЕМЫ И АНАЛИЗ ЛИТЕРАТУРЫ

Важным механизмом криптографической защиты информации является шифрование, под которым понимают обратимое преобразование открытых данных для сокрытия их смыслового содержания от неуполномоченного пользователя (противника, злоумышленника). Криптографическое преобразование осуществляется под управлением специальных (ключевых) данных, которые для симметричных функций зашифрования-расшифрования совпадают [1]. Блочный шифр, как разновидность симметричной системы, оперирует группами бит фиксированной длины (блоками). Взаимнооднозначные процессы зашифрования-расшифрования блоков открытого текста (англ. plaintext) и блоков шифртекста (англ. ciphertext) параметризируется ключевыми данными. То есть каждый секретный ключ шифрования (мастер-ключ) задает конкретный вид биективного отображения «открытый текст – шифртекст».

Большинство блочных симметричных шифров (БСШ) являются *итеративными* [1], в которых шифрование реализуется посредством циклически повторяющихся обратимых раундовых функций (рис. 1). На каждой итерации БСШ для параметризации раундовых преобразований используются т.н. *раундовые (цикловые) ключи* $K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}$. Они формируются посредством расширения (планирования, расписания) мастер-ключа $K^{(x)}$ (англ. keyscheduling) [1]. Структура ключевого расписания итеративных БСШ, простота формирования и/или взаимозависимость раундовых ключей, лежат в основе известных атак на схемы разворачивания. В частности, наибольшее развитие получили т.н. *сдвиговые атаки* (англ. slideattack) [2–4], *атаки на связанных ключах* (англ. related-keyattack) [5–7] и пр. [1].

В простейшем случае схема разворачивания может состоять в повторении мастер-ключа для каждого раунда. Подобный подход использовался при формирования цикловых ключей в советском алгоритме симметричного криптопреобразования ГОСТ 28147-89, являвшегося, до недавнего времени, и основным стандартом шифрования Украины ДСТУ ГОСТ 28147:2009 [1]. Однако в случае, когда на вход каждой раундовой функции (см. рис. 1) подается некоторый ключ, одинаковый для всех раундов, шифр становится уязвимым к сдвиговой атаке [2, 3]. К этому простейшему случаю легко сводится вариант, когда функция разворачивания предполагает циклическое повторение некоторого набора раундовых ключей (шифры с раундовым самоподобием, англ. roundself-similarityciphers) [4].

Для противодействия криптоаналитическим атакам на ключевое расписание современные БСШ используют усложненные схемы разво-

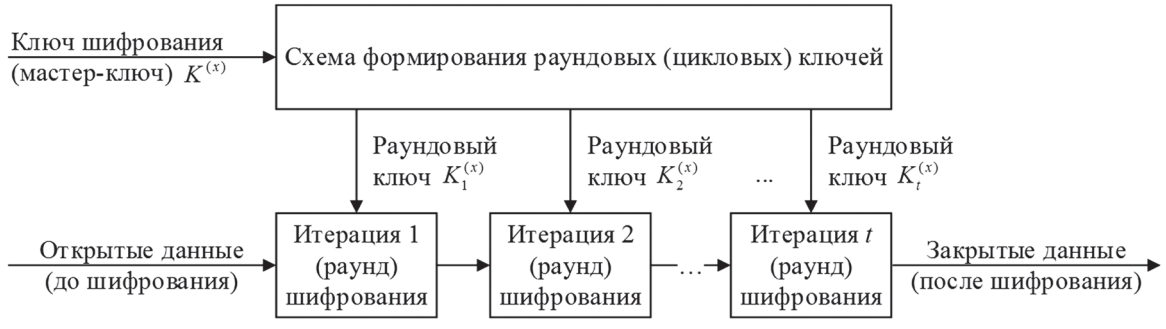

Рис. 1. Структурная схема итеративного блочного шифра

рачивания раундовых ключей, построенные, например, на использовании шифроподобных преобразований. К числу таких БСШ следует отнести, в первую очередь, национальный стандарт США FIPS-197 (AES) [8, 9], принятый в 2001 году и получивший наибольшее распространение в современных протоколах безопасности. Ключевое расписание БСШ AES представляет собой линейный массив 4-х байтовых слов. Первые элементы массива содержат мастер-ключ шифрования, остальные определяются рекурсивно посредством суммирования по модулю два предыдущих элементов. Для некоторых позиций массива дополнительно применяются шифроподобные преобразования, в частности, нелинейная подстановка блока данных, циклический сдвиг и пр. [8, 9]. В результате формируемая последовательность раундовых ключей $K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}$ нелинейно зависит от исходного мастер-ключа $K^{(x)}$, что позволяет противостоять сдвиговым атакам на ключевое расписание [1].

Атаки на связанных ключах впервые предложены в [5] и получили дальнейшее развитие в [6, 7]. В частности, в работе [7] предложена первая криптоаналитическая атака на основе связанных ключей на полнораундовые шифры AES-192 и AES-256 (варианты FIPS-197 с длиной ключа 192 и 256 бит). Следует отметить, что приведенные в [7] атаки эффективнее полного перебора мастер-ключей, т.е. можно с уверенностью утверждать о реальном снижении стойкости стандартизированного криптоалгоритма.

Таким образом, атаки на ключевое расписание непрерывно совершенствуются и их возможное использование представляет реальную угрозу безопасности современным информационным системам [1-7]. Перспективные БСШ должны эффективно противостоять атакам на ключевое расписание, схема разворачивания не должна содержать уязвимостей, обусловленных простотой формирования и взаимной зависимостью цикловых ключей [11].

Фактически, речь идет о таком «идеальном» разворачивании раундовых ключей, при котором каждый элемент последовательности $K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}$ формируется случайно, равновероятно и независимо от других цикловых ключей. Только в этом случае можно с уверенностью утверждать о бесполезности атак на ключевое расписание, т.к. каждый раунд БСШ параметризируется случайно выбранным значением и будет функционировать независимо от других итераций схемы шифрования (см. рис. 1).

В качестве яркой иллюстрации указанной тенденции в развитии схем ключевого расписания можно привести алгоритм «Калина», принятый в качестве национального стандарта БСШ Украины [12]. Он обладает усиленной схемой разворачивания цикловых ключей, основанной на использовании специальных однонаправленных функций. Цикловые ключи БСШ «Калина» формируются в результате нескольких раундов шифрования, параметризированных т.н. вспомогательным ключом. Вспомогательный ключ, в свою очередь, также формируется в результате нескольких раундов шифрования, параметризированных мастер-ключом. Другими словами, отдельные элементы последовательности цикловых ключей $K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}$ формируются посредством независимого шифрования различных входных блоков данных на различных ключах. Если предположить, что применяемое шифрование реализует случайную подстановку (перестановку) блоков данных [13, 14], тогда полученные раундовые ключи будут сформированы случайно, равновероятно и независимо друг от друга [11, 15]. В частности, в работе [15] исследуются свойства ключевого расписания БСШ «Калина», утверждается о стойкости шифра к атакам на связанных ключах и к атакам на реализацию.

Следует отметить, что при случайном, равновероятном и независимом формировании раундовых ключей соответствующие последовательности могут совпадать. Это явление носит крайне негативный аспект, т.к. любое совпадение сформированных последовательностей цикловых ключей для различных мастер-ключей эквивалентно снижению мощности множества реализуемых отображений зашифрования-расшифрования, т.е. уменьшится реализуемое ключевое пространство. Даже совпадение отдельных раундовых ключей может привести к снижению криптографических свойств БСШ. Например, в режиме шифрования Galois/CounterMode & GMAC (спецификация которого приведена в стандарте NIST SP 800-38D [16]) т.н. субключ хеширования формируется посредством шифрования на мастер-ключе специальной константы (нулевой последовательности). Сформированный субключ является некоторым эквивалентом раундового ключа и его совпадение (в результате случайной подстановки, заданной шифрованием), приведет к тождественности формируемых контрольных сумм, т.е. создаст предпосылки для нарушения целостности – одной из базовых услуг безопасности.

Вопросы оценки соотношений мощностей множеств цикловых ключей и мастер-ключей шифрования (в рамках допущения про схему разворачивания как про случайное отображение) исследовались в [15]. Однако полученное выражение (27) в [15], как будет показано ниже, дает правильное решение только для последовательностей из одного раундового ключа и только для случая совпадения длин блоков данных и мастер-ключей. В общем случае полученные в [15] соотношения не верны.

Целью данной работы является исследование комбинаторных свойств ключевого расписания БСШ, при условии, что цикловые ключи формируются случайно, равновероятно и неза-

висимо друг от друга. Для абстрактного описания такого формирования используется модель случайной однородной подстановки. Таким образом, проводимые исследования выполняются в рамках допущения о т.н. «идеальном» ключевом расписании БСШ, т.е. полученные оценки следует использовать как верхние теоретические границы для вероятностных свойств последовательностей раундовых ключей. Практическая полезность результатов исследования состоит в их интерпретации для оценки свойств ключевого расписания принятого недавно национального стандарта БСШ Украины. Действительно, если верно принятое предположение, тогда полученные в данной работе выражения и конкретные оценки свойств ключевого расписания следует непосредственно отнести к БСШ «Калина». Результаты будут также полезны при оценке вероятностных свойств ключевых и других специальных данных различных режимов шифрования, в частности, субключей хеширования в режиме Galois/CounterMode& GMAC.

2. СЛУЧАЙНАЯ ПОДСТАНОВКА КАК МОДЕЛЬ ФОРМИРОВАНИЯ ЦИКЛОВЫХ КЛЮЧЕЙ

Рассмотрим определение и основные свойства случайной подстановки (перестановки) [13, 14], которые будем использовать в дальнейшем для оценки вероятностных свойств последовательностей раундовых ключей.

В комбинаторике под перестановкой понимают упорядоченный набор чисел 1, 2, ..., n, обычно трактуемый как биекция на множестве {1, 2, ..., n}, которая числу i ставит в соответствие i-й элемент из набора. Число n при этом называют порядком (степенью) перестановки [13, 14].

Под подстановкой s произвольного множества $Y=\{y_1, y_2, ..., y_n\}$ понимают некоторое правило, по которому каждому элементу y_i множества Y ставится в соответствие некоторый другой элемент $s(y_i)$ [13, 14]:

$$s=\begin{pmatrix} y_1 & y_2 & y_n \\ s(y_1) & s(y_2) & s(y_n) \end{pmatrix}.$$

В теории групп под подстановкой понимают биекцию этого множества на себя, т.е. подстановку S степени n рассматривают как перестановку элементов множества $Y = \{y_1, y_2, ..., y_n\}$ и для всех $i = 1, 2, ..., n$ соответствующие $s(y_i)\in Y$.

Значение функции $s(y_i)$ для конкретного элемента $y_i \in Y$ будем называть *реализацией подстановки* s в i-й точке.

Композиция подстановок s_u и s_w степени n определяется как последовательное выполнение перестановок элементов множества Y [13, 14]:

$$s_u \circ s_w=\begin{pmatrix} y_1 & y_2 & y_n \\ s_u(s_w(y_1)) & s_u(s_w(y_2)) & s_u(s_w(y_n)) \end{pmatrix},$$
$$s_u(s_w(y_i))\in Y .$$

Относительно операции последовательного выполнения подстановок множество всех $n!$ перестановок порядка n образует группу, которую называют симметрической группой и обозначают $s_n=\{s_1,s_2,...,s_{n!}\}$.

По определению [13, 14], *случайной подстановкой* (перестановкой) s_x называют случайный вектор $\{s_x(y_1),s_x(y_2),...,s_x(y_n)\}$, все элементы которого принимают значения из множества Y и при этом вероятность совпадения любых двух элементов равна 0. Другими словами, случайная подстановка – это случайно выбранная из множества s_n перестановка

$$s_x=\begin{pmatrix} y_1 & y_2 & ... & y_n \\ s_x(y_1) & s_x(y_2) & ... & s_x(y_n) \end{pmatrix},$$
$$s_x\in s_n,\ x\in\{1,2,...,n!\},$$

задаваемая набором (вектором) случайных значений $\{s_x(y_1),s_x(y_2),...,s_x(y_n)\}$, вероятности совпадения которых удовлетворяют условию:

$$\forall i\neq j\in\{1,2,...,n\}: P(s_x(y_i)=s_x(y_j))=0 .$$

Таким образом, под *реализацией случайной подстановки* s_x будем понимать конкретную реализацию случайного вектора $\{s_x(y_1),s_x(y_2),...,s_x(y_n)\}$, а соответствующее значение функции $s_x(y_i)$ будем называть *реализацией случайной подстановки* s_x в i-й точке.

Независимой случайной подстановкой называют такую случайную перестановку

$$\{s_x(y_1),s_x(y_2),...,s_x(y_n)\},$$

для которой

$$P(s_x)=\frac{P(s_x(y_1))P(s_x(y_2))...P(s_x(y_n))}{\sum_{u=1}^{n!}P(s_u(y_1))P(s_u(y_2))...P(s_u(y_n))}.$$

Если $\forall i,u\in\{1,2,...,n\}: P(s_u(y_i))=n^{-1}$, тогда

$$P(s_x)=\frac{P(s_x(y_1))P(s_x(y_2))...P(s_x(y_n))}{\sum_{u=1}^{n!}P(s_u(y_1))P(s_u(y_2))...P(s_u(y_n))}=$$
$$=\frac{n^{-n}}{\sum_{u=1}^{n!}n^{-n}}=\frac{1}{n!} \qquad (1)$$

и s_x называют *случайной, равновероятной и независимой* (или, сокращенно, *однородной*) *случайной подстановкой*.

Таким образом, понятие однородной случайной подстановки соответствует равномерному вероятностному распределению на множестве $s_n=\{s_1,s_2,...,s_{n!}\}$ с независимой реализацией случайных векторов

$$\{s_x(y_1),s_x(y_2),...,s_x(y_n)\}, \qquad (2)$$
$$s_x\in S_n,\ \forall x\in\{1,2,...,n!\}: P(s_x)=(n!)^{-1}.$$

Современные БСШ принято описывать моделью однородной случайной подстановки [1, 11], т.е. принимается предположение, что реализуемая функцией шифрования биекция обрабатываемых блоков данных по своим вероятностным свойствам удовлетворяет характеристикам случайной подстановки. Действительно,

если случайный, равновероятный и независимый выбор мастер-ключа $K^{(x)}$ связать с выбором подстановки $s_x \in s_n$, тогда полученное шифрующее преобразование будет соответствовать случайному, равновероятному и независимому сопоставлению блоков шифртекста блокам открытого текста на всех возможных вариантах биективных отображений, параметризированных ключом. Например, для l -битного шифра с длиной мастер-ключа k бит модель случайной подстановки будет состоять из подмножества

$$s'_n = \{s'_1, s'_2, ..., s'_{2^k}\} \subset s_n = \{s_1, s_2, ..., s_{n!}\}$$

случайно, равновероятно и независимо выбранных 2^k подстановок степени $n = 2^l$ (действующих на множестве $Y = \{y_1, y_2, ..., y_{2^l}\}$ блоков двоичных данных), причем выбор подстановки $s'_x \in s'_n \subset s_n$ (реализация случайного вектора $\{s_x(y_1), s_x(y_2), ..., s_x(y_{2^l})\}$) задается случайно, равновероятно и независимо выбранным значением k -битного мастер-ключа $K^{(x)}$.

Воспользуемся свойствами однородной случайной подстановки для исследования вероятностных характеристик последовательностей раундовых ключей. Для этого на множестве s'_n зададим равномерное вероятностное распределение:

$$\forall i \in \{1,2,...,2^l\}, \forall u \in \{1,2,...,2^k\} : P(s_u(y_i)) = 2^{-l},$$

т.е. все вероятности сопоставления i -го блока y_i u -му блоку $s_u(y_i)$ равны друг другу и не зависят ни от i, ни от u. Следовательно, вероятность случайного выбора подстановки $s'_x \in s'_n \subset s_n$ (и соответствующего ей мастер-ключа шифрования) не зависит от вида этой подстановки, а определяется как величина, обратная мощности множества мастер-ключей, что с учетом (1) примет вид:

$$P(s'_x) = \frac{P(s'_x(y_1))P(s'_x(y_2))...P(s'_x(y_{2^l}))}{\sum_{u=1}^{2^k} P(s'_u(y_1))P(s'_u(y_2))...P(s'_u(y_{2^l}))} = \frac{2^{-nl}}{\sum_{u=1}^{2^k} 2^{-nl}} = 2^{-k}. \quad (3)$$

Применим рассмотренную модель однородной случайной подстановки к исследованию вероятностных свойств элементов ключевого расписания. Оценим вероятности совпадений отдельных цикловых ключей, а также их последовательностей, предположив, что раундовые ключи формируются случайно, равновероятно и независимо друг от друга.

3. ВЕРОЯТНОСТНЫЕ СВОЙСТВА ЦИКЛОВЫХ КЛЮЧЕЙ

Введем следующие обозначения. Пусть на вход схемы разворачивания ключей (см. рис. 1) поступает случайно, равновероятно (с вероятностью 2^{-k}) и независимо сформированный мастер-ключ $K^{(x)}$ длины k бит. Обозначим последовательность из t формируемых раундовых ключей в виде $K_{\text{рк}}^{(x)} = \{K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}\}$, где каждый $K_i^{(x)}$ является i-м цикловым ключом длины l-бит.

Предположим, что цикловые ключи $K_i^{(x)}$ являются независимыми реализациями однородной случайной подстановки в i-й точке:

$$\forall i \in \{1,2,...,t\} : K_i^{(x)} = s'_x(y_i),$$

т.е. формируются случайно, равновероятно и независимо друг от друга, причем для каждого $K_i^{(x)}$ конкретная реализация случайной подстановки $s'_x \in s'_n \subset s_n$ не зависит от $i \in \{1,2,...,t\}$.

Рассмотрим вероятностные свойства случайно формируемых значений раундовых ключей $K_i^{(x)}$ для некоторого фиксированного i, оценим среднее число различных значений цикловых ключей, которые могут быть сформированы при использовании всех 2^k значений мастер-ключей $K^{(x)}$.

Лемма. Среднее число различных l-битных цикловых ключей $K_i^{(x)}$, формируемых посредством 2^k реализаций случайной однородной подстановки, определяется выражением:

$$N(k,l) = 2^l(1-(1-2^{-l})^{2^k}) \approx 2^l\left(1-\left(\frac{1}{e}\right)^{2^{k-l}}\right) \approx 2^l\left(1-(0{,}37)^{2^{k-l}}\right). \quad (4)$$

Доказательство. Если схема формирования каждого циклового ключа из последовательности $K_{\text{рк}}^{(x)}$ описывается моделью случайной однородной подстановки с вероятностью (1) выбора $s'_x \in s'_n \subset s_n$ (по введенному мастер-ключу $K^{(x)}$), тогда, по определению, для любого фиксированного $i \in \{1,2,...,t\}$ вероятность появления $K_i^{(x)}$ не зависит ни от $y_i \in Y$, ни от $K^{(x)}$, а определяется как величина, обратная мощности множества Y, т. е. равна $P(s'_x(y_i) = K_i^{(x)}) = 2^{-l}$. Мастер-ключи $K^{(x)}$ выбираются независимо друг от друга и соответствующие события $s'_x(y_i) = K_i^{(x)}$ независимы. Следовательно, можем воспользоваться формулой для нахождения вероятности появления искомого события M раз в N испытаниях (формулой Бернулли):

$$P(N,M) = C_N^M(1-P(s'_x(y_i) = K_i^{(x)}))^{N-M}(P(s'_x(y_i) = K_i^{(x)}))^M = C_N^M(1-2^{-l})^{N-M}(2^{-l})^M.$$

Значение $P(N,M)$ задает вероятность того, что при N независимых реализациях случайной однородной подстановки в i -й точке конкретный раундовый ключ $K_i^{(x)} = s'_x(y_i)$ появится ровно M раз. Значение

$$P(2^k,0) = (1-2^{-l})^{2^k}$$

задает вероятность того, что при $N = 2^k$ независимых реализациях случайной подстановки в i -й точке (на всем множестве значений мастер-ключей $K^{(x)}$) раундовый ключ $K_i^{(x)} = s'_x(y_i)$ не появится ни разу.

Обратная величина

$$P(2^k,>0) = 1 - P(2^k,0) = \\ = \sum_{i=1}^{2^k} C_{2^k}^i (1-2^{-l})^{2^k-i} (2^{-l})^i = 1-(1-2^{-l})^{2^k} \quad (5)$$

задает вероятность такого события, когда при 2^k независимых испытаниях раундовый ключ $K_i^{(x)}$ длины l-бит будет сформирован хотя бы один раз.

Мощность множества различных l-битных значений равна 2^l, причем каждое из этих значений при 2^k независимых реализациях вектора (2) с вероятностью (5) появится в i -й точке случайной подстановки хотя бы один раз. То есть для 2^k различных мастер-ключей $K^{(x)}$, задающих реализацию вектора (2), схемой разворачивания будет сформировано в среднем

$$N(k,l) = 2^l P(2^k,>0) = 2^l (1-(1-2^{-l})^{2^k})$$

различных раундовых ключей $K_i^{(x)}$, что при подстановках $(1-2^{-l})^{2^l} \approx e^{-1}$ дает упрощенную формулу в правой части выражения (3), и, т.о., завершает доказательство.

Наиболее простой случай $k = l$ (равенство длин блоков шифртекста длине ключа) рассмотрен в докторской диссертационной работе Р.В. Олейникова, в которой получено «соотношение мощностей множества цикловых ключей и ключей шифрования» в виде рекуррентного выражения (27) в [15, с. 25]. Действительно, при $k = l$ вероятность(5),принимает вид

$$P(2^l,>0) = \sum_{i=1}^{2^l} C_{2^l}^i (1-2^{-l})^{2^l-i} (2^{-l})^i = 1 - P(2^l,0) = \\ = 1-(1-2^{-l})^{2^k} \approx 1 - e^{-1} \approx 0{,}63$$

и отношение среднего числа $N(k,l)$ различных раундовых ключей $K_i^{(x)}$ к числу 2^k различных мастер-ключей $K^{(x)}$ при $k = l$ определяется как

$$\delta(k,l) = \frac{N(k,l)}{2^k} = \frac{2^l(1-P(2^k,0))}{2^k} = \\ = P(2^l,>0) \approx 1 - e^{-1} \approx 0{,}63, \quad (6)$$

что соответствует формуле (27) в [15].

Следует, однако, отметить, что оценка среднего числа различных цикловых ключей в виде

$$N(k,l) = 2^l(1-P(2^k,0)) \approx 0{,}63 \cdot 2^l$$

справедлива только для случая $k = l$. При $k \neq l$ выражение (6), равно как и выражение (27) в [15, с. 25], выполняться не будет, отношение $\delta(k,l)$ необходимо оценивать по общей формуле

$$\delta(k,l) = \frac{N(k,l)}{2^k} = 2^{l-k}(1-(1-2^{-l})^{2^k}) \approx \\ \approx 2^{l-k}\left(1-\left(\frac{1}{e}\right)^{2^{k-l}}\right) \approx 2^{l-k}\left(1-(0{,}37)^{2^{k-l}}\right). \quad (7)$$

Приведем пример использования полученных соотношений. На рис. 2, 3 приведены, соответственно, зависимости вероятностей (5) и отношений (7) для длин блоков $0 \le l \le 16$ и ключей $0 \le k \le 16$. Очевидно, что даже для таких незначительных длин l и k, не превышающих 16 бит, наблюдается резкий переход от очень малых, практически равных нулю значений $P(2^k,>0)$ и $\delta(k,l)$, до очень больших, близких к единице. Это характерно, в особенности, для зависимости $P(2^k,>0)$, а множитель 2^{l-k} в (7) несколько «сглаживает» итоговую функцию (7), инвертируя качественный вид зависимости (5).

В табл. 1 сведены значения отношения среднего числа $N(k, l)$ различных цикловых ключей $K_i^{(x)}$ к числу 2^k различных мастер-ключей $K^{(x)}$ для наиболее распространенных в современных БСШ и их уменьшенных моделей значений l и K. Данные таблицы 1 рассчитаны по упрощенной формуле в правой части выражения (7) с использованием вычислительных алгоритмов системы WolframAlpha [17]. Приведенные значения демонстрируют конструктивность полученных аналитических выражений для оценки вероятностных характеристик раундовых ключей.

Для оценки вероятностных свойств последовательностей цикловых ключей обобщим положения леммы для случайно, равновероятно и независимо формируемых значений $K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}$. Оценим среднее число различных последовательностей $K_{\text{рк}}^{(x)}$, формируемых при использовании всех 2^k значений мастер-ключей $K^{(x)}$. Справедлива след. теорема.

Теорема. Среднее число различных последовательностей цикловых ключей $K_{\text{рк}}^{(x)}$, формируемых посредством 2^k независимых реализаций случайной однородной подстановки в i-й точке, определяется:

$$N(k,l,t) = 2^l(1-(1-2^{-tl})^{2^k}) \approx 2^{tl}\left(1-\left(\frac{1}{e}\right)^{2^{k-tl}}\right) \approx \\ \approx 2^{tl}\left(1-(0{,}37)^{2^{k-tl}}\right). \quad (8)$$

Доказательство состоит в обобщении результатов леммы на случай формирования последовательностей $K_{\text{рк}}^{(x)}$. Действительно, в соответствии с принятым допущением о формировании цикловых ключей $K_i^{(x)}$ независимыми реализациями однородной случайной подстановки в i -й точке, для каждого $i \in \{1,2,...,t\}$ вероятность появления $K_i^{(x)}$ не зависит ни от $y_i \in Y$, ни от $K^{(x)}$. Эта вероятность равна $P(s'_x(y_i) = K_i^{(x)}) = 2^{-l}$. Совместная вероятность появления независимых событий равна произведению вероятностей этих событий, т.е:

$$P(K_{\text{рк}}^{(x)} = \{K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}\}) = \\ = \prod_{i=1}^{t} P(s'_x(y_i) = K_i^{(x)}) = 2^{-tl}.$$

Мастер-ключи $K^{(x)}$ выбираются независимо друг от друга и соответствующие события $K_{\text{рк}}^{(x)}$ независимы. Следовательно, воспользовавшись формулой Бернулли, получим выражение

$$P(N,M,t) = C_N^M (1-2^{-tl})^{N-M} (2^{-tl})^M ,$$

которое задает вероятность того, что в N независимых реализациях последовательность $K_{\text{рк}}^{(x)}$ появится ровно M раз. Величина

$$P(2^k,>0,t) = \sum_{i=1}^{2^k} C_{2^k}^i (1-2^{-tl})^{2^k-i} (2^{-tl})^i = \\ = 1 - P(2^k,0,t) = 1-(1-2^{-tl})^{2^k} \quad (9)$$

задает вероятность того, что при 2^k независимых испытаниях конкретная последовательность $K_{\text{рк}}^{(x)}$ будет сформирована хотя бы один раз.

Мощность множества различных t-последовательностей l-битных значений равна 2^{tl}, причем каждая из этих последовательностей с вероятностью (9) появится на выходе схемы разворачивания раундовых ключей хотя бы один раз. То есть для 2^k различных мастер-ключей $K^{(x)}$, задающих реализации однородной случайной подстановки, схемой разворачивания будет сформировано в среднем $N(k,l,t) = 2^{tl}(1-P(2^k,0,t))$ различных $K_{\text{рк}}^{(x)}$, что при упрощении $(1-2^{-l})^{2^l} \approx e^{-1}$ дает формулу (8).

Доказанная теорема позволяет получить выражение для оценки отношения среднего числа различных последовательностей $K_{\text{рк}}^{(x)}$ к мощности множества различных мастер-ключей $K^{(x)}$:

$$\delta(k,l,t) = \frac{N(k,l,t)}{2^k} = 2^{tl-k}(1-(1-2^{-tl})^{2^k}) \approx \\ \approx 2^{tl-k}\left(1-\left(\frac{1}{e}\right)^{2^{k-tl}}\right) \approx 2^{tl-k}\left(1-(0{,}37)^{2^{k-tl}}\right). \quad (10)$$

Формула (10) отличается от известного выражения (27) в [15]. Результаты моделирования показывают, что оценки отношения $\delta(k,l,t)$, приведенные в работе [15], в общем случае не верны. Напротив, оценка (10), как будет показано ниже, подтверждается результатами моделирования.

Для удобства проведения расчетов соотношения $\delta(k,l,t)$ запишем формулу (10) иначе. В большинстве практически важных случаев блочного шифрования (например, для БСШ «Калина») длина мастер-ключа k кратна длине блока l, т.е. выполняется соотношение $k = ml$, что после подстановки в (10) дает форму:

$$\delta(ml,l,t) = 2^{l(t-m)}(1-(1-2^{-tl})^{2^{ml}}) \approx \\ \approx 2^{l(t-m)}\left(1-\left(\frac{1}{e}\right)^{2^{l(m-t)}}\right) \approx 2^{l(t-m)}\left(1-(0{,}37)^{2^{l(m-t)}}\right). \quad (11)$$

Выражение (11) показывает, что увеличение кратности m эквивалентно, в вероятностном смысле, соответствующему уменьшению длины t последовательности $K_{\text{рк}}^{(x)}$. И наоборот: увеличение длины t последовательности раундовых ключей уменьшает вероятность (9) также, как и кратное снижение длины мастер-ключа. Характерной демонстрацией подобного эффекта является симметричность относительно значений l и k графиков функций, приведенных на рис. 2, 3. В этом смысле, расчетные значения $\delta(ml,l,t)$ для случая $l \in \{16, 32\}$ и $m, t \in \{1, 2, 4, 8, 16\}$ могут быть полностью получены из данных таблицы 1 при выборе столбцов, с обозначениями ml, и строк, с обозначениями tl.

В качестве примера в табл. 2 приведены расчетные значения $\delta(ml,l,t)$ для $l = 32$, которые, очевидно, полностью сходятся с данными,

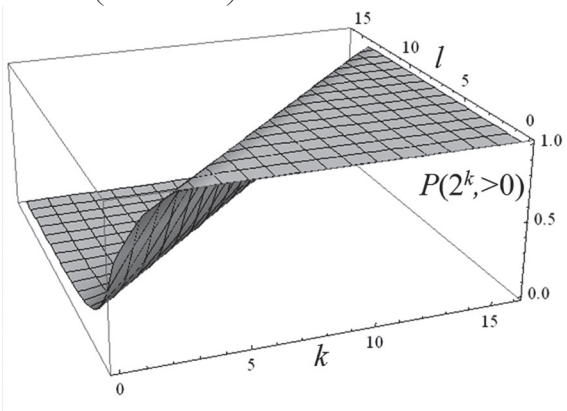

Рис. 2

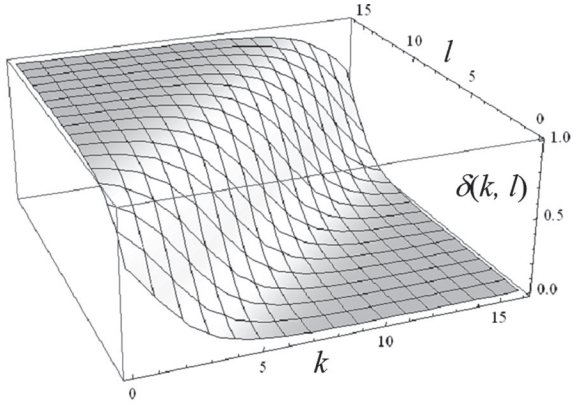

Рис. 3

Таблица 1

Отношение среднего числа различных l-битных цикловых ключей $K_i^{(x)}$, формируемых посредством $2k$ реализаций случайной однородной подстановки, к мощности множества различных мастер-ключей $K^{(x)}$

	K=16	K=32	K=64	K=128	K=256	K=512
l = 16	0,63	$1{,}52\cdot10^{-5}$	$3{,}55\cdot10^{-15}$	$1{,}93\cdot10^{-34}$	$5{,}66\cdot10^{-73}$	$4{,}89\cdot10^{-150}$
l = 32	$1-7{,}63\cdot10^{-6}$	0,63	$2{,}33\cdot10^{-10}$	$1{,}26\cdot10^{-29}$	$3{,}71\cdot10^{-68}$	$3{,}20\cdot10^{-145}$
l = 64	$1-1{,}78\cdot10^{-15}$	$1-1{,}16\cdot10^{-10}$	0,63	$5{,}42\cdot10^{-20}$	$1{,}59\cdot10^{-58}$	$1{,}38\cdot10^{-135}$
l = 128	$1-9{,}63\cdot10^{-35}$	$1-6{,}31\cdot10^{-30}$	$1-2{,}71\cdot10^{-20}$	0,63	$2{,}94\cdot10^{-39}$	$2{,}54\cdot10^{-116}$
l = 256	$1-2{,}83\cdot10^{-73}$	$1-1{,}85\cdot10^{-68}$	$1-7{,}97\cdot10^{-59}$	$1-1{,}47\cdot10^{-39}$	0,63	$8{,}64\cdot10^{-78}$
l = 512	$1-2{,}44\cdot10^{-150}$	$1-1{,}60\cdot10^{-145}$	$1-6{,}89\cdot10^{-136}$	$1-1{,}27\cdot10^{-116}$	$1-4{,}32\cdot10^{-78}$	0,63

приведенными в таблице 1. Расчетные значения $\delta(ml,l,t)$ для случаев $l\in\{64, 128, 256\}$, $m\in\{1, 2, 4, 8\}$ и $t\in\{1, 2, 4, 8, 16\}$ сведены в таблицу 3. Приведенные расчетные значения улучшают данные по оценке $\delta(k,l,t)$ в [15], т.к. основаны на выражениях (8)–(11), учитывающих соотношения длин блоков и мастер-ключей. Вывод о практическом совпадении мощностей последовательностей раундовых ключей и мастер-ключей шифрования в [15] следует считать верным, приведенные в таблице 3 данные подтверждают эту закономерность.

Для всех рассмотренных и практически значимых соотношений l и k при выполнении неравенства $t > m$ отношение среднего числа различных последовательностей раундовых ключей к мощности множества различных мастер-ключей лишь незначительно отличается от единицы. При дальнейшем повышении длины последовательности раундовых ключей t это расхождение стремительно убывает.

Для подтверждения адекватности и достоверности полученных результатов и сделанных по ним выводов проведен численный эксперимент, суть которого состояла в подсчете отношения среднего числа различных последовательностей раундовых ключей к мощности 2^k множества различных мастер-ключей. Для моделирования случайной подстановки использовалась простейшая функция генерации случайных чисел, интегрированная в среду быстрой разработки приложений Embarcadero RAD Studio [18]. Каждое наблюдение состояло в оценке выборочного (эмпирического) среднего по 100 реализациям (прогонам) модели. Каждая реализация модели состояла в подсчете отношения среднего числа различных последовательностей раундовых ключей к мощности 2^k множества различных мастер-ключей. При проведении эксперимента оценивались как выборочные средние $\delta^*(ml,l,t)$, так и выборочные дисперсии D при объеме выборки, состоящей из 100 элементов. Полученные результаты

Таблица 2

Отношение среднего числа различных последовательностей цикловых ключей к мощности множества различных мастер-ключей длины ($l = 32$)

	m=1	m=2	m=4	m=8	m=16
t=1	0,63	$2{,}33\cdot10^{-10}$	$1{,}26\cdot10^{-29}$	$3{,}71\cdot10^{-68}$	$3{,}20\cdot10^{-145}$
t=2	$1-1{,}16\cdot10^{-10}$	0,63	$5{,}42\cdot10^{-20}$	$1{,}59\cdot10^{-58}$	$1{,}38\cdot10^{-135}$
t=4	$1-6{,}31\cdot10^{-30}$	$1-2{,}71\cdot10^{-20}$	0,63	$2{,}94\cdot10^{-39}$	$2{,}54\cdot10^{-116}$
t=8	$1-1{,}85\cdot10^{-68}$	$1-7{,}97\cdot10^{-59}$	$1-1{,}47\cdot10^{-39}$	0,63	$8{,}64\cdot10^{-78}$
t=16	$1-1{,}60\cdot10^{-145}$	$1-6{,}89\cdot10^{-136}$	$1-1{,}27\cdot10^{-116}$	$1-4{,}32\cdot10^{-78}$	0,63

Таблица 3

Отношение среднего числа различных последовательностей раундовых ключей к мощности множества различных мастер-ключей

$l = 64$				
	$m = 1$	$m = 2$	$m = 4$	$m = 8$
$t = 1$	0,63	$1{,}52\cdot10^{-5}$	$5{,}66\cdot10^{-73}$	$4{,}89\cdot10^{-150}$
$t = 2$	$1-7{,}62\cdot10^{-6}$	0,63	$3{,}71\cdot10^{-68}$	$3{,}20\cdot10^{-145}$
$t = 4$	$1-1{,}78\cdot10^{-15}$	$1-1{,}16\cdot10^{-10}$	0,63	$8{,}64\cdot10^{-78}$
$t = 8$	$1-2{,}44\cdot10^{-150}$	$1-1{,}60\cdot10^{-145}$	$1-1{,}27\cdot10^{-116}$	0,63
t=16	$1-5{,}13\cdot10^{-290}$	$1-9{,}46\cdot10^{-271}$	$1-3{,}22\cdot10^{-232}$	$1-3{,}73\cdot10^{-155}$
$l = 128$				
$t = 1$	0,63	$2{,}94\cdot10^{-39}$	$2{,}54\cdot10^{-116}$	$1{,}89\cdot10^{-270}$
$t = 2$	$1-1{,}47\cdot10^{-39}$	0,63	$8{,}64\cdot10^{-78}$	$6{,}44\cdot10^{-232}$
$t = 4$	$1-1{,}27\cdot10^{-116}$	$1-4{,}32\cdot10^{-78}$	0,63	$7{,}45\cdot10^{-155}$
$t = 8$	$1-9{,}46\cdot10^{-271}$	$1-3{,}22\cdot10^{-232}$	$1-3{,}74\cdot10^{-155}$	0,63
t=16	$1-5{,}26\cdot10^{-579}$	$1-1{,}79\cdot10^{-540}$	$1-2{,}07\cdot10^{-463}$	$1-2{,}78\cdot10^{-309}$
$l = 256$				
$t = 1$	0,63	$8{,}64\cdot10^{-78}$	$6{,}44\cdot10^{-232}$	$3{,}58\cdot10^{-540}$
$t = 2$	$1-4{,}32\cdot10^{-78}$	0,63	$7{,}45\cdot10^{-155}$	$4{,}15\cdot10^{-463}$
$t = 4$	$1-3{,}22\cdot10^{-232}$	$1-3{,}73\cdot10^{-155}$	0,63	$5{,}56\cdot10^{-309}$
$t = 8$	$1-1{,}79\cdot10^{-540}$	$1-2{,}08\cdot10^{-463}$	$1-2{,}78\cdot10^{-309}$	0,63
t=16	$1-5{,}54\cdot10^{-1157}$	$1-6{,}42\cdot10^{-1080}$	$1-8{,}61\cdot10^{-926}$	$1-1{,}55\cdot10^{-617}$
$l = 512$				
$t = 1$	0,63	$7{,}46\cdot10^{-155}$	$4{,}15\cdot10^{-463}$	$1{,}28\cdot10^{-1079}$
$t = 2$	$1-3{,}73\cdot10^{-155}$	0,63	$5{,}56\cdot10^{-309}$	$1{,}72\cdot10^{-925}$
$t = 4$	$1-2{,}08\cdot10^{-463}$	$1-2{,}78\cdot10^{-309}$	0,63	$3{,}09\cdot10^{-617}$
$t = 8$	$1-6{,}42\cdot10^{-1080}$	$1-8{,}60\cdot10^{-926}$	$1-1{,}55\cdot10^{-617}$	0,63
t=16	≈1	≈1	≈1	$1-4{,}79\cdot10^{-1237}$

сведены в табл. 4. В последнем столбце таблицы приведены значения точности ε оцениваемой характеристики при заданном уровне значимости $\alpha = 0{,}05$.

Таблица 4

Результаты экспериментальных исследований и их сравнение с теоретическими расчетами

$l=4, m=1$				
	$\delta(ml,l,t)$	$\delta^*(ml,l,t)$	D	ε
t=1	0,632121	0,6453125	0,005716	0,014818
$t=2$	0,969391	0,969125	0,001758	0,008218
$t=3$	0,998049	0,9983125	0,000110	0,002056
$t=4$	0,999878	0,999875	0,000008	0,000554
$l=4, m=2$				
$t=1$	0,062500	0,062500	0	0
$t=2$	0,632121	0,633074	0,000372	0,003780
$t=3$	0,969391	0,969675	0,000103	0,001989
$t=4$	0,998049	0,997934	0,000008	0,000554
$l=4, m=3$				
$t=1$	0,003906	0,003906	0	0
$t=2$	0,062500	0,062500	0	0
$t=3$	0,632121	0,632152	0,000023	0,000940
$t=4$	0,969391	0,969492	0,000007	0,000519
$l=8, m=1$				
$t=1$	0,632121	0,632836	0,000360	0,003719
$t=2$	0,998049	0,998051	0,000007	0,000519
$t=3$	0,999992	0,999961	0,000002	0,000277
$l=8, m=2$				
$t=1$	0,003906	0,003906	0	0
$t=2$	0,632121	0,632176	0,000002	0,000277
$t=3$	0,998049	0,998063	$2{,}98\cdot10^{-8}$	$3{,}38\cdot10^{-5}$

Как видно из приведенных в табл. 4 значений, результаты экспериментальных исследований полностью подтверждают достоверность полученных теоретических положений. Для всех случаев расчетные значения $\delta(ml,l,t)$ и полученные эмпирические данные $\delta^*(ml,l,t)$ отличаются не более, чем на ε (абсолютное значение ошибки), причем вероятность, с которой достигается указанная точность (достоверность оценки) составляет 0,95. Поскольку достоверность характеризует повторяемость, устойчивость эксперимента [19], можно утверждать, что в 95% случаев величина $\delta^*(ml,l,t)$ будет отличаться от $\delta(ml,l,t)$ меньше, чем на ε.

4. ВЫВОДЫ И ПЕРСПЕКТИВЫ ДАЛЬНЕЙШИХ ИССЛЕДОВАНИЙ

Проведенные исследования вероятностных свойств раундовых ключей БСШ показали, что даже при случайном, равновероятном и независимом формировании используемые ключевые последовательности могут совпадать, что неизбежно снижает мощность множества реализуемых отображений зашифрования-расшифрования.

Для описания схемы разворачивания раундовых ключей использовалась абстрактная модель случайной подстановки, параметризированная значением мастер-ключа шифрования. Полученные с ее помощью аналитические соотношения позволяют оценить вероятностные свойства цикловых ключей БСШ. В частности, вероятность кратного совпадения раундовых ключей при заданном числе реализаций случайной однородной подстановки (заданном числе мастер-ключей) определяется по формуле Бернулли. Это соотношение дает оценку вероятности того события, когда на всем множестве мастер-ключей конкретный раундовый ключ будет сформирован хотя бы один раз, т.е. позволяет оценить среднее число различных раундовых ключей на выходе схемы формирования. Последний результат обобщается также на последовательности раундовых ключей произвольной длины, т.е. в рамках принятой модели удается получить численные оценки вероятностных свойств всех элементов ключевого расписания БСШ.

Приведенные в таблицах 2, 3 расчетные значения отношения среднего числа различных последовательностей раундовых ключей к мощности множества различных мастер-ключей дают представление о реализации шифром всего множества допустимых отображений зашифрования-расшифрования. В частности, приведенные расчетные значения для наиболее важных в практическом отношении случаев для длин блоков данных l и ключей $k = ml$ показывают, что при числе раундов $t < m$ с вероятностью, близкой к единице, конкретная последовательность раундовых ключей на всем множестве мастер-ключей сформирована не будет. Это равносильно тому, что среднее число различных последовательностей раундовых ключей будет пренебрежительно мало по сравнению с мощностью множества различных мастер-ключей, т.е. подавляющее число отображений «открытый текст – шифртекст» из всего множества 2^k отображений *реализованы не будут*. Напротив, для случая $t > m$, отношение среднего числа различных последовательностей раундовых ключей к мощности множества мастер-ключей практически не отличается от единицы. При дальнейшем повышении t это расхождение стремительно убывает и, следует полагать, что при таком ключевом расписании *будут реализованы* все допустимые отображения «открытый текст – шифртекст» из полного множества 2^k отображений.

Проведенное имитационное моделирование «идеальной» схемы разворачивания ключей позволило получить эмпирические оценки, которые совпадают с теоретическими расчетами по формулам (9) – (11), что подтверждает достоверность и обоснованность результатов исследования. В частности, для всех исследуемых случаев расчетные значения и полученные эмпирические данные отличаются незначительно (относительное значение ошибки < 3%), при-

чем вероятность, с которой указанная точность достигается (достоверность оценки) составляет 0,95. Следовательно, можно утверждать, что в 95% случаев расчетные и эмпирические данные отличаются меньше, чем на величину ошибки.

Следует отметить, что полученные аналитические выражения и приведенные расчетные значения соответствуют гипотетическому случаю случайного, равновероятного и независимого формирования раундовых ключей, т.е. «идеальному» с вероятностной точки зрения ключевому расписанию. Реальные схемы разворачивания ключей основаны на детерминированных алгоритмах, параметризованных значением мастер-ключа шифрования. Следовательно, полученные оценки на модели случайной однородной подстановки следует использовать как *верхние теоретические границы* для вероятностных свойств последовательностей раундовых ключей: ключевое расписание реального БСШ может лишь приближаться по своим характеристикам к этому «идеальному» случаю и не будет улучшать приведенные расчетные значения.

Практическая полезность полученных результатов состоит в их непосредственной интерпретации для *оценки вероятностных свойств элементов ключевого расписания нового национального стандарта БСШ Украины* [12]. Если верно предположение о том, что цикловые ключи БСШ «Калина» являются независимыми реализациями однородной случайной подстановки, т.е. формируются случайно, равновероятно и независимо друг от друга, тогда вывод о практическом совпадении мощностей последовательностей раундовых ключей и мастер-ключей шифрования следует считать теоретически доказанным, приведенные в таблице 3 расчетные значения наглядно подтверждают эту закономерность. Использование в новом стандарте «идеального» ключевого расписания помимо обеспечения стойкости шифра к атакам на связанных ключах и атакам на реализацию [15] позволяет полностью реализовать ключевое пространство мастер-ключей и соответствующее множество отображений «открытый текст - шифртекст».

Применение полученных теоретических результатов к оценке вероятностных свойств субключей хеширования в режиме Galois/Counter Mode & GMAC [16] показывает, что ключевое пространство мастер-ключей шифрования в этом режиме реализуется всего на 63%. Возможное совпадение формируемых субключей приведет к тождественности криптографических контрольных сумм, что создает реальные предпосылки для нарушения целостности информации. Изучение вероятностных свойств субключей хеширования в режиме Galois/Counter Mode & GMAC, оценка числа эквивалентных и слабых мастер-ключей является перспективным направлением дальнейших исследований.

В качестве *перспективного направления* дальнейших исследований следует также указать поиск или, по крайней мере, оценку вероятностных свойств подмножеств т.н. *эквивалентных ключей* БСШ, когда несколько различных по значению мастер-ключей приводят к формированию одинаковых последовательностей цикловых ключей, тождественно задающих биективные отображения зашифрования – расшифрования. Другими словами, наличие подмножеств эквивалентных ключей уменьшает мощность множества отображений «открытый текст – шифртекст», количество ключевой информации, численно равное мере неопределенности секретных параметров шифрования, также уменьшается. Кроме того, само существование отличных по значению, но эквивалентных по задаваемой функции шифрования нескольких мастер-ключей может быть использовано злоумышленником для реализации криптоаналитических атак, например, основанных на подмене защищаемой информации ложными данными в случае использования БСШ в режиме выработки имитовставок.

Литература

[1] *Горбенко І.Д., Горбенко Ю.І.* Прикладна криптологія. Теорія. Практика. Застосування: Підручник для вищих навч. закладів. – Харків: Вид-во «Форт», 2013. – 880 с.

[2] *Biryukov A., Wagner D.* Slide Attacks (англ.) //Fast Software Encryption. 6th International Workshop, FSE'99 Rome, Italy, March 24–26, 1999 Proceedings. - Springer Berlin Heidelberg, 1999. - С. 245-259.

[3] *Chalermpong Worawannotai, Isabelle Stanton* A Tutorial on Slide Attacks (англ.). [Електронний ресурс] – Режим доступа: http://www.eecs.berkeley.edu/~isabelle/slideattacks.pdf.

[4] *Biryukov A., Wagner D.* Advanced Slide Attacks (англ.) // Advances in Cryptology - EUROCRYPT 2000. International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14-18, 2000 Proceedings. – Springer Berlin Heidelberg, 2000. – С. 589–606

[5] *Biham E.* New types of cryptanalytic attacks using related keys (англ.) // Springer-Verlag : журнал. – 1994. – № 4. – С. 229–246.

[6] *Ciet M., Piret G., Quisquater J.-J.* Related-Key and Slide Attacks: Analysis, Connections, and Improvements (Extended Abstract). // http://citeseer.ist.psu.edu – 2002 – Universite catholique de Louvain, Louvain-la-Neuve, Belgium

[7] *Biryukov A., Khovratovich D.* Related-Key Cryptanalysis of the Full AES-192 and AES-256 (англ.) // Springer Berlin Heidelberg : журнал. – 2009. – С. 1–18.

[8] *Daemen J.* AES proposal: Rijndael [Електронний ресурс] / J. Daemen, V. Rijmen // 1998. Режим доступа: http://www.nist.gov/aes.

[9] FIPS-197: Advanced Encryption Standard (AES) [Електронний ресурс] // National Institute of Standards and Technology. – 2001. – Режим доступа: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[10] Положення про порядок здійснення криптографічного захисту інформації в Україні, затверджене Указом Президента України від 22 травня 1998 року N 505/98.

[11] Розробка нового блокового симетричного шифру [Текст]: звіт за перший етап НДР «Алгоритм» (проміжний) / кер. І. Д. Горбенко; АТ «ІІТ». – Харків, 2014. – Том 4. – 304 с.

[12] Інформаційні технології. Криптографічний захист інфомації. Алгоритм симетричного блокового перетворення: ДСТУ 7624:2014. – К.: Мінекономрозвитку України, 2015. – 238 с.

[13] *Сачков В.Н.* Введение в комбинаторные методы дискретной математики. – М.: Наука. Гл. ред. физ.-мат. лит., 1982. – 384 с.

[14] *Сачков В.Н.* Вероятностные методы в комбинаторном анализе. – М., Наука, 1978 г. – 287 с.

[15] Олійников Р. В. Методи аналізу і синтезу перспективних симетричних криптографічних перетворень: автореф. дис. ... д-ра техн. наук : 05.13.05 / Р. В. Олійников; Харків. нац. ун-т радіоелектрон. – Харків, 2014. – 42 с.

[16] NIST Special Publication 800-38D. Block Cipher Modes. [Електронний ресурс]. – Режим доступа: http://csrc.nist.gov/groups/ST/toolkit/BCM/current_modes.html

[17] Вопросно-ответная система WolframAlpha. [Электронный ресурс] – Режим доступа: http://www.wolframalpha.com/

[18] Интегрированная среда разработки Embarcadero RAD Studio. [Электронный ресурс] – Режим доступа: http://www.embarcadero.com/ products/rad-studio

[19] *Вентцель Е.С., Овчаров Л.А.* Теория вероятностей и ее инженерные приложения. Учеб. пособие для втузов.– 2-е изд., стер. – М.: Высш. шк., 2000. – 480 с.

Поступила в редколлегию 24.11.2015

Кузнецов Александр Александрович, фото и сведения об авторе см. на с. 334.

Горбенко Юрий Иванович, фото и сведения об авторе см. на с. 290.

Иваненко Дмитрий Викторович, фото и сведения об авторе см. на с. 334.

УДК 004.056.55

Комбінаторні властивості ключового розкладу блокових симетричних шифрів / О.О. Кузнєцов, Ю.І. Горбенко, Д.В. Іваненко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2015. – Том 14. – № 4. – С. 351–360.

Досліджуються комбінаторні властивості ключового розкладу блокових симетричних шифрів у припущенні, що циклічні (раундові) ключі формуються випадково, рівномірно та незалежно один від одного. Для абстрактного опису такого формування використовується модель випадкової однорідної підстановки, отримані аналітичні вирази дозволяють оцінити потужність множини, яка реалізує відображення зашифрування-розшифрування, отримати оцінки ймовірнісних властивостей послідовностей раундових ключів і відношень середнього числа різних ключових послідовностей до потужності множини різних майстер-ключів. Результати імітаційного моделювання підтверджують достовірність й обгрунтованість отриманих аналітичних виразів.

Ключові слова: ключовий розклад, циклічні ключі, комбінаторні властивості, блокові симетричні шифри.

Табл.: 4. Іл.: 3. Бібліогр.: 19 найм.

UDK 004.056.55

Combinatorial properties of the key schedule of block symmetric ciphers / A.A. Kuznetsov, Yu.I. Gorbenko, D.V. Ivanenko // Applied Radio Electronics: Sci. Journ. — 2015. — Vol. 14. — № 4. — P. 351–360.

The paper studies the combinatorial properties of the key schedule of block symmetric ciphers on the assumption that the cyclic (round) keys are generated randomly, with equal probability and independently. To abstractly describe such a formation a homogeneous random substitution model is used. The analytical expressions obtained allow to estimate the cardinality of a set of implemented encryption-decryption maps, to obtain estimates of the probability properties of sequences of round keys and relationships of the average number of different key sequences to the power of many different master keys. Simulation results have confirmed the reliability and validity of the obtained analytical expressions.

Keywords: key schedule, cyclic keys, combinatorial properties, block symmetric ciphers.

Tab.: 4. Fig.: 3. Ref.: 19 items.