УДК 621.3.06

А.В.ПОТИЙ, канд. техн. наук, Ю.А. ИЗБЕНКО

СИСТЕМА ПОКАЗАТЕЛЕЙ ОЦЕНКИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СХЕМ ПОТОЧНОГО ШИФРОВАНИЯ

Введение

Сегодня можно с уверенностью утверждать, что в международной практике в качестве основного подхода к решению разработки новых алгоритмов криптографического преобразования информации утвердился системный подход. Суть подхода заключается в том, что разработчики уделяют внимание не только обеспечению криптографической стойкости алгоритма, но и обеспечению эффективности функционирования алгоритма в целом. Действительно, при современном уровне развития вычислительной техники и средств связи, переходе к эксплуатации информационно-телекоммуникационных систем обеспечение эффективности функционирования алгоритмов шифрования становится таким же естественным требованием, как и обеспечение их криптографической стойкости.

К сожалению, зачастую эффективность и стойкость являются конфликтующими целями. С одной стороны, постоянно происходит ужесточение требований по безопасности, поскольку алгоритм должен обладать запасом стойкости не только к известным криптонападениям, но и к новым методам криптоанализа. С другой стороны, повышаются требования по производительности средств шифрования. Полное разрешение противоречия между стойкостью и эффективностью получить невозможно, однако если рассматривать стойкость как составляющую эффективности алгоритма, согласовать различные показатели, остроту решения этого вопроса можно снизить. Такой подход к разработке алгоритмов шифрования хорошо зарекомендовал себя при проведении конкурса на новый стандарт блочного шифрования AES [1]. Очевидно, что такой подход будет эффективен и при разработке схем поточного шифрования (ПШ).

Эффективность функционирования схем ПШ есть степень соответствия полученных результатов функционирования схемы R_p требуемым R_{mp}:

$$P = < R_p , R_{mp} >. \quad (1)$$

Требуемым результатом функционирования схемы R_{mp} является обеспечение функции конфиденциальности путем реализации механизма шифрования. Полученным результатом функционирования схемы R_p является реальный уровень обеспечения функции конфиденциальности. Оценка того, насколько полно реализована функция конфиденциальности или, другими словами, насколько R_p соответствует R_{mp}, осуществляется с помощью показателей, отражающих степень выполнения схемой функциональной задачи.

На сегодняшний день не существует систематизированного множества показателей, которые могли бы охарактеризовать эффективность функционирования схем ПШ. Как показал анализ [1], разработчики схем ПШ предлагают различные показатели, которые характеризуют отдельные стороны схем, но не позволяют представить картину в целом. В данной работе ставится задача обоснования и определения минимального множества требований и частных показателей эффективности схем ПШ. Другой задачей является формулировка критериев выбора схем ПШ.

В первой части работы представлена декомпозиция требований к схемам ПШ, общая классификация показателей и критериев эффективности, формируется векторный показатель эффективности схем ПШ.

Вторая часть работы содержит описание множества показателей и критериев эффективности схем ПШ, разбитых на группы показателей стойкости, показателей эффективности реализации, конструктивно-технологические показатели.

В заключении обсуждаются дальнейшие направления исследований в данной области.

1. Классификация критериев и показателей эффективности функционирования схем ПШ

Эффективность функционирования схем криптографического преобразования данных оценивается с точки зрения стойкости схем к аналитическим методам вскрытия информации. Анализ работ [3-8] показал, что при оценке стойкости используются следующие критерии:

1. Вычислительная сложность методов криптоанализа должна быть не меньше вычислительной сложности универсальных методов (полный перебор, парадокс дней рождения и т.п.).

2. Рассматриваемые схемы оцениваются согласно утверждениям разработчиков о стойкости схем. В случае нахождения метода анализа, имеющего вычислительную сложность меньшую, чем заявлено разработчиками, схема считается скомпрометированной.

3. Рассматриваемые схемы оцениваются в пределах заявленной области применения. Таким образом, рассмотрение уязвимости к побочным методам нападениям (например timing attack, силовые атаки) должно быть соответствующим.

Очевидно, что первоочередной задачей схем криптографического преобразования данных является обеспечение стойкости схем к известным на сегодняшний день методам криптоанализа. Однако в силу интенсивного развития средств телекоммуникаций, возрастания объемов циркулирующей в информационных системах информации, многообразия сред приложений, требующих выполнения криптопреобразований, неотъемлемыми требованиями к схемам криптопреобразований стали быстродействие, объемы требуемой памяти, многоплатформенность реализации и т.д. В рамках конкурса NESSIE для отбора кандидатов на европейский стандарт поточного шифрования предлагаются следующие показатели [2]:

– стойкость к методам анализа. Любая рассматриваемая схема должна быть стойкой к атакам заявленного уровня стойкости. Подверженность анализу каким-либо методом со сложностью меньше заявленной дисквалифицирует рассматриваемую схему;

– общая концепция конструкции схемы. Важным элементом оценки стойкости схемы криптопреобразований является используемая концепция построения и прозрачность конструкции анализируемой схемы. Ясность и прозрачность конструкторских решений, основанных на хорошо понятных и изученных математических и криптографических принципах, позволяют с бóльшим доверием относиться к результатам оценки стойкости исследуемых схем. Кроме того, данные принципы особенно уместны при проведении сравнений между исследуемыми схемами;

– стойкость модифицируемых схем. Под модифицированной схемой понимают схему, в которой модифицируют или удаляют некоторые ее составные части. В этом случае выводы относительно стойкости схемы делают на основе оценки стойкости модифицированной схемы;

– показатели относительной защиты. При оценке разработанных схем с идентичным функциональным назначением возникает задача сравнительного анализа стойкости предоставляемого ими уровня защиты. При проведении таких сравнений следует быть крайне осторожным в выборе критериев сравнения. Так, показателем, определяющим нижнюю границу стойкости блочных симметричных алгоритмов, является разница между количеством циклов алгоритма и количеством взломанных циклов. Однако при этом у аналитиков нет никакого общего согласия об определении или использовании такого показателя. Имеют место случаи, когда оцениваемые схемы имеют различные конструкции и концепции построения, при их анализе используются отличные друг от друга показатели. Все это затрудняет осуществление оценки схем с единых позиций. Таким образом, необходимо для всех схем определить некоторую нижнюю границу стойкости к методам анализа;

– характеристики среды эксплуатации и особенности применения схем. В определенных криптографических средах представленные схемы могут обладать свойственными им достоинствами и недостатками. В качестве примера можно рассматривать схемы, обладаю-

щие стойкостью по отношению к силовым атакам и timing attack, выполненным на смарт-картах. Рассмотрение других типов атак на данные схемы было бы нецелесообразным;

– статистическая стойкость. Рассматриваемые схемы подвергаются статистическому тестированию. Целью тестирования является выявление некоторых статистических отклонений в генерируемых последовательностях, что может указать на некоторую криптографическую слабость и потребует дальнейшего исследования схемы;

– быстродействие схем. Быстродействие представленных схем рассматривается на нескольких платформах с целью определения собственно быстродействия, а также гибкости реализации и многоплатформенности приложений;

– объем используемой памяти. В некоторых приложениях данный показатель является критичным. Любая конструкция должна гарантировать минимальный объем памяти без нанесения ущерба стойкости рассматриваемой схемы.

Таким образом, на данный момент в различных источниках рассмотрены показатели, относящиеся к оценке разных сторон схем преобразования. Анализ документов, представленных на конкурсы AES, NESSIE [2,9], показывает, что наряду с показателями стойкости немаловажную роль имеют и аппаратно-реализационные показатели.

При определении эффективности функционирования схем ПШ целесообразно рассмотрение следующих основных групп показателей (рис. 1).

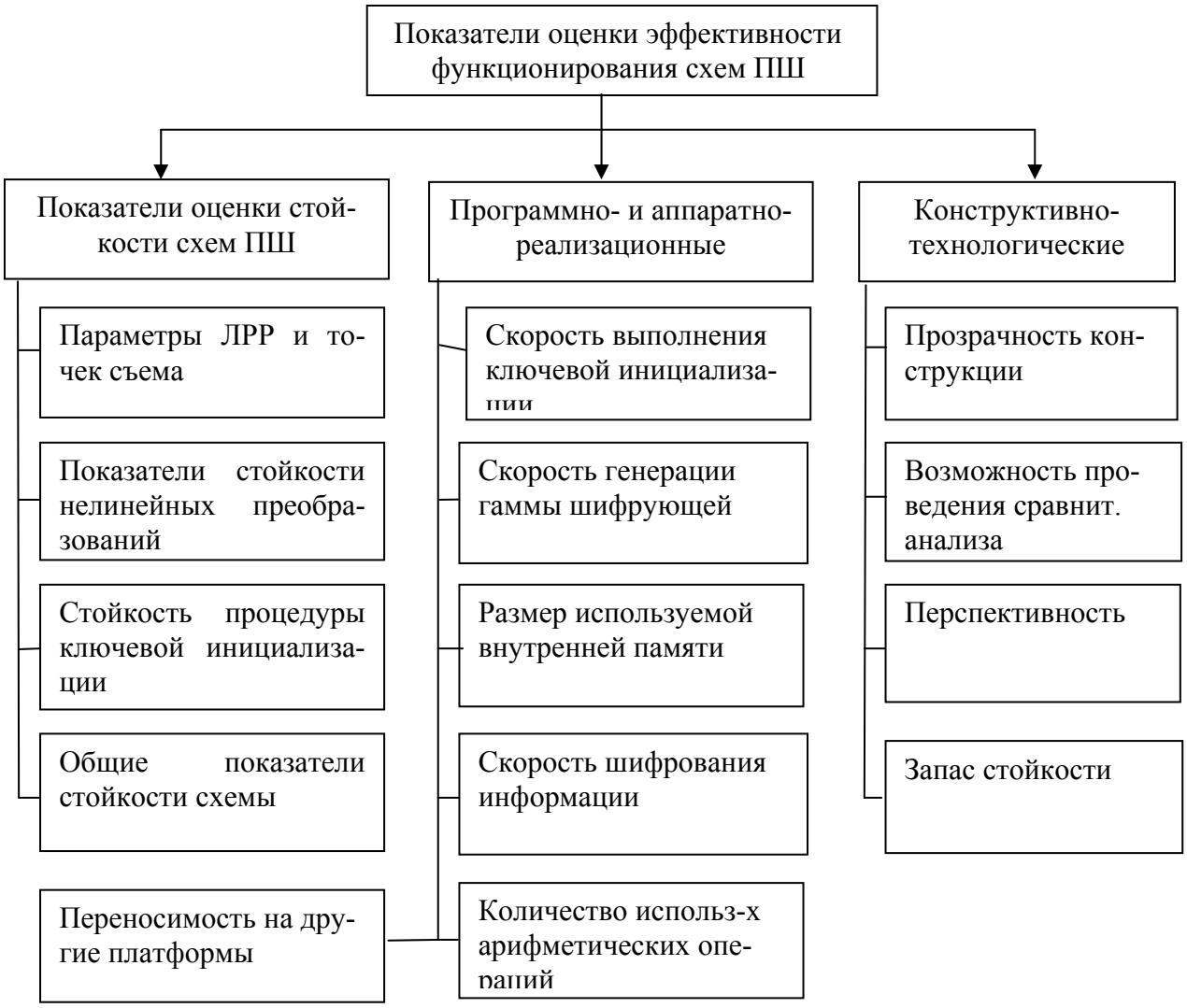

Рис.1

Требуемый результат функционирования схемы R_{mp} может быть представлен в виде

$$R_{mp} = < П_{СТ} , П_{Р}, П_{КТ} >, \quad (2)$$

где $П_{СТ}$ – показатели стойкости схем ПШ; $П_{Р}$ – программно- и аппаратно- реализационные показатели; $П_{КТ}$ - конструктивно-технологические показатели.

Показатели стойкости схем ПШ, $П_{СТ}$, характеризуют стойкость схем ПШ к аналитическим методам анализа и являются основными показателями, поскольку целесообразность применения любых схем криптопреобразования информации основывается, в первую очередь, на оценке стойкости данных схем к известным на сегодняшний день методам (атакам) криптоанализа, применимым к исследуемому классу схем.

Программно- и аппаратно- реализационные показатели, $П_{Р}$, характеризуют эффективность программной и аппаратной реализаций и являются показателями, характеризующими практичность схем криптопреобразований. Схема может обладать высокой стойкостью к различного рода методам криптоанализа, но тем не менее иметь ограничения на практическое использование из-за высокой стоимости аппаратной реализации, низкого быстродействия и т.п. Одним из важнейших преимуществ методов поточного шифрования информации, благодаря которому они получили широкое распространение, является высокая скорость преобразования информации. Как следствие, схемы, имеющие высокие показатели эффективности реализации, с наибольшей вероятностью будут отобраны для практических приложений. Применимость схем часто рассматривается с позиций унификации (универсальности): например, одна и та же схема должна быть одинаково успешно реализуема и в программном обеспечении, и в аппаратном, на смарт-картах и т.п. Некоторые области приложений налагают очень высокие требования к скорости связи (гигабитные трафики), для других областей применения приложения приемлют минимальные аппаратные платформы и/или компактные аппаратные средства (сотовые телефоны, смарт-карты). В идеале рассматриваемые схемы должны быть гибкими, т.е. быть реализуемыми более чем на одной платформе. Таким образом, при определении эффективности реализации рассматриваемых схем целесообразно производить отбор показателей, отражающих эффективность функционирования схем в заданных областях приложений, поскольку, очевидно, одна и та же схема вряд ли может быть эффективно реализована на всех платформах и во всех приложениях.

Конструктивно-технологические показатели, $П_{КТ}$, характеризуют прозрачность конструкции, перспективность схем, запас их стойкости, пригодность известных методов анализа к оценке характеристик схем криптопреобразований, возможность проведения сравнительного анализа схем данного класса и, как следствие, степень доверия пользователей.

2. Показатели эффективности функционирования схем ПШ

Каждая группа предложенных выше показателей включает в себя множество частных показателей. В данном разделе обосновывается и предлагается минимально необходимое множество показателей эффективности схем ПШ, формулируются критерии оценки эффективности. Показатели и критерии эффективности могут носить как количественный, так и качественный характер.

2.1. Показатели стойкости схем ПШ

На основе исследований, проведенных в [3-8, 10-12], для схем ПШ определим следующее множество показателей стойкости.

***Показатели, характеризующие параметры регистров и точек съема для нелинейной функции и обратных связей*, $П_{ЛРР}$** :

- *Примитивность образующего полинома*. Примитивный многочлен степени n – это неприводимый многочлен, который делит x, но не делит $x^{2^{n-1}} + 1$ для любого такого d, которое делит 2^n-1. Степень многочлена – это длина регистра сдвига. Только регистры, использующие в качестве образующего полинома примитивный полином, являются регистрами макси-

мального периода (проходят через все возможные 2^n-1 состояний) и генерируют последовательности максимального периода, так называемые *ml* – последовательности.

Критерием отбора является логическая переменная Да\Нет.

- *Взаимно простые степени образующих полиномов* (для комбинирующих генераторов). При выборе образующих полиномов, имеющих взаимно простые степени, линейная сложность (см. показатель *линейная сложность*) генерируемой последовательности z является максимальной $\Lambda(z) = f(\Lambda_1, \ldots, \Lambda_N)$, где Λ_j - линейная сложность j-го фильтр-генератора, $j = 1, \ldots, N$.

Критерием отбора является логическая переменная Да\Нет.

- *Степень образующего полинома*. При правильно подобранном образующем полиноме степень полинома n определяет период генерируемой последовательности. На сегодняшний день для противостояния аналитическим атакам минимальная длина регистра должна составлять не менее 128 бит.

Критерием отбора будем полагать $n \geq 128$ бит.

- *Плотность образующего полинома*. Для противостояния корреляционным атакам, основанным на низковесовых проверках четности, количество ненулевых коэффициентов k в образующем полиноме должно быть около $n/2$.

Критерием отбора будем полагать $k \rightarrow n/2$.

- *Правильность определения количества точек съема для нелинейной функции* (для фильтр-генераторов). Для противостояния аналитическим атакам количество точек съема r должно быть $r` \leq \sqrt{2n}$.

Критерием отбора является $r \rightarrow r`$.

- *Соответствие множества точек обратных связей B полному множеству положительных разностей* ΔB. Множество ΔB называют *полным множеством положительных разностей*, если все положительные попарные разности между его элементами различны. Требуемое соответствие обеспечивает противостояние аналитическим атакам.

Критерием отбора является логическая переменная Да\Нет.

- *Соответствие множества точек съема для нелинейной функции Г полному множеству положительных разностей* $\Delta \Gamma$ (для фильтр-генераторов). Требуемое соответствие обеспечивает противостояние аналитическим атакам.

Критерием отбора является логическая переменная Да\Нет.

- *Наибольший общий делитель двух парных (соседних) положительных разностей должен быть равен* 1.

Критерием отбора является логическая переменная Да\Нет.

Показатели, характеризующие стойкость нелинейной функции, $\mathbf{П_{НЛФ}}$:

- *Сбалансированность выходной последовательности*. Функция f над V_n является *сбалансированной* функцией, если ее выходные значения являются равновероятными:

$$| \{x \mid f(x) = 0 \} | = | \{x \mid f(x) = 1 \}| = 2^{n-1}. \quad (3)$$

Сбалансированность функции является показателем, отражающим стойкость гаммы к статистическим атакам.

Критерием отбора является логическая переменная Да\Нет.

- *Нелинейность*. *Нелинейность* функции f - минимальное расстояние Хэмминга N_f между функцией f и всеми аффинными функциями над V_n [12]:

$$N_f = \min \{d(f, \varphi)\}, \quad (4)$$

где φ - множество аффинных функций.

Для сбалансированной функции f над V_n ($n \geq 3$) нелинейность N_f может достигать [12]:

$$N_f \le \begin{cases} 2^{n-1} - 2^{n/2-1} - 2 \ , n = 2k, \\ \left\lfloor\!\left\lfloor 2^{n-1} - 2^{n/2-1} \right\rfloor\!\right\rfloor, n = 2k+1, \end{cases} \tag{5}$$

где $\left\lfloor\!\left\lfloor x \right\rfloor\!\right\rfloor$ - максимальное четное целое, меньшее либо равное x.

Верхняя граница нелинейности для произвольной функции f над V_n может достигать

$$N_f \le 2^{n-1} - 2^{n/2-1}. \tag{6}$$

Нелинейность функции является важным показателем, поскольку несоблюдение данного показателя делает возможным проведение корреляционных атак, использующих корреляцию данной функции со множеством слабых функций. При построении криптографически стойких булевых функций необходимо обеспечить ее минимальную корреляцию со множеством всех слабых функций, то есть стремиться, чтобы нелинейность данной функции стремилась к верхней границе нелинейности, определенной согласно (6).

Критерием отбора является $N_f = \max\limits_{N_j} \{N_1, \ldots, N_r\}$, где N_j – нелинейность j – й функции; $j = 1, \ldots, r$.

- *Алгебраическая степень*. Алгебраическая степень *deg*(*f*) является степенью самого длинного слагаемого функции, представленной в алгебраической нормальной форме. Алгебраической нормальной формой называется выражение вида

$$f(x_1,\ldots,x_n) = a_0 \oplus \bigoplus_{i=1}^{n} a_i x_i \oplus \bigoplus_{1 \le i < j \le 1} a_{ij} x_i x_j \oplus \ldots \oplus a_{12\ldots n} x_1 x_2 \cdots x_n . \tag{7}$$

Высокая алгебраическая степень позволяет противостоять различным аналитическим атакам, призванным свести данную функцию к криптографически слабой (линейной).

Критерием отбора является $deg(f) = \max\limits_{deg(f_j)} \{ deg(f_1), \ldots, deg(f_r)\}$, где $deg(f_j)$ – нелинейность j – й функции; $j = 1, \ldots, r$.

- *Коэффициент равномерной минимизации кросс-корреляции*. Характеризует равномерную минимизацию коэффициентов кросс-корреляции

$$k_{рм} = \frac{k_{гр}}{r \cdot c_{ср}}, \tag{8}$$

где $k_{гр}$ - граничный коэффициент кросс-корреляции; r – удельный вес ненулевых значений коэффициентов кросс-корреляции; $c_{ср}$ – среднее значение коэффициента кросс-корреляции. Приведенные значения имеют следующий вид:

$$r = \left| \frac{B}{2^n} - 2^{n-1} \right|, \tag{9}$$

$$c_{ср} = \frac{\sum\limits_{i=1}^{2^n} c_i}{2^n}, \tag{10}$$

$$k_{гр} = \frac{\left|1 - 2^n\right| \cdot (c_n + c_{n+2})}{2} \text{ для } V_{n+1} \quad \text{и} \quad k_{гр} = \left|1 - 2^n\right| \cdot c_n \text{ для } V_n, \tag{11}$$

где B – общее количество ненулевых значений коэффициентов кросс-корреляции; c_i – значение коэффициента кросс-корреляции; c_n - коэффициент корреляции бент-функции над V_n; c_{n+2} – коэффициент корреляции бент-функции над V_{n+2}.

Критерием отбора является $k_{рм} = \min\limits_{k_{рм_j}} \{ k_{рм\,1}, \ldots, k_{рм\,r}\}$, где $k_{рм\,j}$ – коэффициент равномерной минимизации кросс-корреляции j – й функции; $j = 1, \ldots, r$.

- Абсолютное значение кросс-корреляции функции

$$C_f = \max\limits_{l_i} | c(f, \ell_i)|. \tag{12}$$

Критерием отбора является $C_f = \min\limits_{l_i} \{ C_{f\,1}, \ldots, C_{f\,r}\}$, где C_{f_j} - абсолютное значение кросс-корреляции j-й функции; $j = 1, \ldots, r$.

- Количество векторов num_1, при которых функция не удовлетворяет критерию распространения

$$num_1 = !PC(k). \tag{13}$$

Критерием отбора является $num_1 = \min\limits_{num_{1j}} \{ num_{11}, \ldots, num_{1\,r}\}$, где num_{1_j} - количество векторов num_1, при которых j-я функция не удовлетворяет критерию распространения; $j = 1, \ldots, r$.

- Количество векторов num_2, при которых функция имеет линейную структуру

$$num_2 = PC_{ЛС}(k). \tag{14}$$

Критерием отбора является $num_2 = \min\limits_{num_{2j}} \{ num_{21}, \ldots, num_{2\,r}\}$, где num_{2_j} - количество векторов num_2, при которых j-я функция имеет линейную структуру; $j = 1, \ldots, r$.

Показатели, характеризующие стойкость процедуры ключевой инициализации, **$П_{КИ}$**:

- Нелинейность операций ключевой загрузки. Нелинейность операций повышает стойкость к алгоритмам, основанным на использовании ключевой загрузки.

Критерием отбора является логическая переменная Да\Нет.

- Каждый бит инициализированного регистра является результатом нелинейных преобразований всех бит ключа. Желательной является реализация, при которой каждый бит начального состояния регистра является функцией от нелинейного преобразования всех бит ключа, в таком случае

$$I(K_{out}^{n} \; ; \; K_{in}^{n-k}) \to 0, \tag{15}$$

где n - длина ключа; k - количество бит инициализированного ключа, введенных нелинейными преобразованиями, $k \to n$; K_{in}^{n-k} и K_{out}^{n} - вводимый и инициализированный ключи соответственно. Таким образом., знание вводимого ключа исключает знание инициализированного ключа (при гарантированной стойкости нелинейных преобразований).

Критерием отбора является логическая переменная Да\Нет.

Общие показатели**, $П_О$**:

- Период гаммы. Периодом гаммы шифрующей T именуется количество бит до того момента, когда последовательность начнет повторяться. Период — одна из наиболее важных характеристик при изучении свойств гаммы шифрующей. Если период гаммы шифрующей окажется слишком коротким, то различные части открытого текста окажутся преобразованными идентичным образом, что составляет серьезную слабость схемы. Зная фрагмент открытого текста, аналитик может восстановить соответствующий фрагмент гаммы шифрующей.

Тот факт, что данный участок гаммы шифрующей появляется и во множестве других мест гаммы шифрующей, позволяет аналитику успешно вскрывать другие зашифрованные тексты. Кроме того, если имеются только преобразованные тексты, зашифрованные одной и той же гаммой шифрующей, то их можно попарно складывать друг с другом для получения последовательности, которая равноценна сумме двух открытых сообщений и не зависит от гаммы шифрующей. Имея необходимую статистику открытого текста, на этой основе можно восстановить как открытые тексты сообщений, так и саму гамму шифрующую [3].

Поскольку ЛРР длиной n бит может находиться в одном из 2^n - 1 внутренних состояний, то теоретически он может иметь период $2^n - 1$. Вопрос о том, насколько большим должен быть период шифрующей последовательности, в открытой литературе является дискуссионным, и решение его зависит от конкретной области применения. Как отмечено в [3] , для схемы ПШ, работающей на скорости 1 Мбайт/сек, последовательность с периодом 2^{32} повторит сама себя всего через 2^9 секунд или 8.5 минут, поэтому средства засекречивания информации с подобной длиной периода не могут считаться адекватной защитой.

На проходящем в настоящее время открытом европейском криптографическом конкурсе NESSIE (New European Schemes for Signature, Integrity and Encryption), целью которого является определение европейских стандартов криптографического преобразования данных, для схем ПШ определено два уровня стойкости:

- "высокий", при котором схема должна обладать длиной ключа $\ell_{кл} \geq 256$ бит и иметь внутреннюю память $P_в \geq 256$ бит;
- "нормальный", при котором схема должна обладать длиной ключа $\ell_{кл} \geq 128$ бит и иметь внутреннюю память $P_в \geq 128$ бит.

Таким образом, согласно европейскому стандарту, длины регистров для обеспечения требуемой стойкости должны составлять по меньшей мере 256 и 128 бит соответственно. Как следствие, можем записать, что длины периодов $T_в$ для схем с "высоким" уровнем стойкости и $T_н$ для схем с "нормальным" уровнем стойкости должны составлять

$$T_в \geq 2^{256}, \text{ бит},$$
$$T_н \geq 2^{128}, \text{ бит}.$$

Тщательная оценка периода гаммы шифрующей, порождаемой схемой, совершенно необходима при разработке любой схемы ПШ. С практической точки зрения, гамма шифрующая должна быть достаточно длинной для того, чтобы в подавляющем большинстве случаев было маловероятным повторное использование одного и того же фрагмента в процессе шифрования информации.

Критерием отбора является $T_f = \max\limits_{T_j} \{T_1, \ldots, T_r\}$, где T_j – период j – й схемы; $j = 1, \ldots, r$.

- *Линейная сложность последовательности*. Линейная сложность $\Lambda(s^l)$ последовательности $s^l = s_0,s_1,\ldots,s_{l-1}$ - длина L самого короткого регистра сдвига, порождающего заданную периодическую последовательность s^l, когда первые L цифр последовательности s^l являются начальным заполнением регистра.

Данный критерий является основополагающим критерием. Как отмечено в [4], любая последовательность, которую можно сгенерировать конечным автоматом (линейным или нелинейным) над конечным полем, имеет конечную линейную сложность. Следовательно, возможно построение алгоритмов, определяющих линейную сложность любой последовательности вне зависимости от способа ее генерации. Так, существует эффективный алгоритм Берлекампа-Месси [5], который быстро находит такой кратчайший регистр после изучения всего $2L$ бит шифрующей последовательности.

По своей сути линейная сложность является мерой сложности сгенерированной последовательности. Рассматривая некоторый отрезок последовательности, аналитик пытается на основе имеющейся последовательности сконструировать свою собственную последователь-

ность. Определение линейной сложности рассматриваемой последовательности дает возможность на основе найденного линейного эквивалента построить схему, которая бы генерировала последовательность, аналогичную рассматриваемой, при этом знания о структуре схемы, сгенерировавшей заданную последовательность, являются излишними. Таким образом, большая линейная сложность гаммы шифрующей – необходимое, но не достаточное условие практической стойкости схем ПШ.

Критерием отбора является $\Lambda_f = \max\limits_{\Lambda_j} \{\Lambda_1, \ldots, \Lambda_r\}$, где Λ_j – линейная сложность последовательности j – й схемы; $j = 1, \ldots, r$.

- *Длина используемых ключей*. Длина ключа определяет стойкость к силовым атакам и составляет $k_в \geq 256$ бит для схем с "высоким" уровнем стойкости и $k_н \geq 128$ бит для схем с "нормальным" уровнем стойкости.

Критерием отбора является $k_f = \max\limits_{k_j} \{k_1, \ldots, k_r\}$, где k_j – длина ключа j - й схемы с заданным уровнем стойкости; $j = 1, \ldots, r$.

- *Внутреннее состояние генератора (внутренняя память) M должно быть не менее 2k бит при длине ключа k бит*. Данный показатель отражает стойкость к атакам “время-память”.

Критерием отбора является логическая переменная Да\Нет.

- *Длина генерируемой последовательности $\ell_п$ не должна превышать некоторого порогового значения N_{max}*, $\ell_п < N_{max}$. Данный показатель отражает стойкость к корреляционным атакам, позволяющим по имеющемуся фрагменту гаммы шифрующей восстановить начальное заполнение ЛРР. Целью введения N_{max} является недопущение генерации последовательности, длина которой гарантировала бы использование корреляции последовательности с последовательностью ЛРР [7].

Критерием отбора является логическая переменная Да\Нет.

- *Показатель, характеризующий стойкость схемы к аналитическим методам анализа*, $П_{АН}$. В целом, именно стойкость схемы к методам анализа определяет эффективность функционирования схем ПШ.

Критерием отбора является логическая переменная Да\Нет.

- *Показатель, характеризующий стойкость схемы к статистическим методам анализа*, $П_{СТАТ}$.

Статистические свойства шифрующей гаммы являются одной из составляющих, определяющей стойкость схемы шифрования. Стойкость схемы зависит от того, насколько близко она аппроксимирует генератор случайных чисел, то есть насколько гамма шифрующая будет вычислительно непредсказуемой и неотличимой от действительно случайной последовательности. Общепризнанной методикой оценки статистических свойств криптографических преобразований на сегодняшний день является методика, предложенная NIST [10]. В данной методике по выборке строится статистический портрет источника, который содержит значения вероятности $P_{ij} \in [0,1]$ – значения вероятности, полученной в результате тестирования i-й последовательности j-м тестом; $i = 1, \ldots, m$, $j = 1, \ldots, q$. Рекомендуемые значения: m=100 последовательностей по 10^6 бит (генеральная совокупность составляет 10^8 бит), $q = 189$. Затем при анализе статистического портрета применяются такие критерии. Первым критерием отбора полагается коэффициент прохождения тестов последовательностями

$$r_j = \frac{\#\{P_{ij} \geq \alpha \mid i = 1,2,...,m\}}{m}, \tag{16}$$

попавший в доверительный интервал $[r_{\max}, r_{\min}]$,

$$r_{\max(\min)} = \hat{p} \pm 3\sqrt{\frac{\hat{p}(1-\hat{p})}{m}}, \tag{17}$$

где $\hat{p} = 1 - \alpha$, α – уровень значимости, равный 0,01.

Второй критерий строится на основе расчета значения χ^2:

$$\chi_j^2 = \sum_{k=1}^{10} \frac{\left(F_k - m/10\right)^2}{m/10}. \qquad (18)$$

Считается, что схема прошла статистическое тестирование, если значения коэффициентов r_j для всех $j = 1, \ldots, q$ находятся внутри доверительного интервала $[r_{max}, r_{min}]$ и для (18) соблюдается условие $\chi_j^2 > 0{,}0001$ для всех $j = 1, \ldots, q$.

Таким образом, комплексный показатель стойкости $П_{СТ}$ схем ПШ имеет вид:

$$П_{СТ} = (П_{ЛРР}, П_{НЛФ}, П_{КИ}, П_{О}). \qquad (19)$$

2.2. Программно- и аппаратно- реализационные показатели

На основе исследований, проведенных в [2], для схем ПШ определим следующее множество показателей эффективности реализации $П_Р$:

- *Ключевая инициализация*, $П_{КИ}$, циклов/байт – отображает скорость выполнения инициализации схемы – количество загруженных байт $n_{бз}$ ключа за один полный цикл сдвига регистра.

Критерием отбора является $n_{бз} = \max_{n_j} \{ n_1, \ldots, n_г\}$, где n_j – количество загруженных байт $n_{бз}$ ключа за один полный цикл сдвига регистра j - й схемы; $j = 1, \ldots, r$.

- *Генерация выходной последовательности*, $П_{ВП}$, циклов/байт – отображает скорость генерации выходной последовательности схемы ― количество сгенерированных байт $m_{бв}$ выходной последовательности за один полный цикл сдвига регистра.

Критерием отбора является $m_{бв} = \max_{m_j} \{ m_1, \ldots, m_г\}$, где m_j – количество сгенерированных байт $n_{бв}$ выходной последовательности за один полный цикл сдвига регистра j - й схемы; $j = 1, \ldots, r$.

- *Размер используемой памяти*, $П_{ПАМ}$, Кб. Отображает размер используемой памяти, ОЗУ и ПЗУ.

Критерием отбора является $v_{mem} = \min_{v_j} \{v_1, \ldots, v_г\}$, где v_j – размер памяти, используемый j - й схемой; $j = 1, \ldots, r$.

- *Скорость шифрования/дешифрования информации*, $П_{СШ}$, Мб/сек.

Критерием отбора является $s = \max_{s_j} \{s_1, \ldots, s_г\}$, где s_j – скорость шифрования/ дешифрования информации j - й схемой; $j = 1, \ldots, r$.

- *Количество используемых различных арифметических операций*, $П_{РО}$.

Критерием отбора является $op = \min_{op_j} \{ op_1, \ldots, op_г\}$, где op_j – количество используемых различных арифметических операций j - й схемой; $j = 1, \ldots, r$.

- *Переносимость на другие платформы*, $П_{ПЕР}$.

Критерием отбора является логическая переменная Да\Нет.

При аппаратной реализации в качестве дополнительных показателей могут рассматриваться:

1. Габариты изделия.
2. Стоимость изделия.
3. Возможность сопряжения с другими типами аппаратуры.
4. Возможность реализации на различного рода микросхемах.

Таким образом, комплексный показатель эффективности программной и аппаратной реализации $П_Р$ схем ПШ имеет вид:

$$П_Р = (П_{КИ}, П_{ВП}, П_{ПАМ}, П_{СШ}, П_{РО}, П_{ПЕР}). \quad (20)$$

2.3. Конструктивно-технологические показатели

Определим следующее множество показателей эффективности реализации $П_{КТ}$:

- Прозрачность конструкции, $П_п$.

Критерием отбора является логическая переменная Да\Нет.

- Возможность проведения сравнительного анализа, $П_А$.

Критерием отбора является логическая переменная Да\Нет.

- Перспективность, $П_П$.

Критерием отбора является логическая переменная Да\Нет.

- Запас стойкости, $П_З$.

Критерием отбора является логическая переменная Да\Нет.

На сегодняшний день для оценки конструктивно-технологических показателей можно использовать методы экспертных оценок.

Таким образом, требуемый результат функционирования схемы $R_{тр}$ определяется следующим множеством показателей

$$R_{тр} = < (П_{ЛРР}, П_{НЛФ}, П_{КИ}, П_О), (П_{КИ}, П_{ВП}, П_{ПАМ}, П_{СШ}, П_{РО}, П_{ПЕР}), (П_п, П_А, П_П, П_З) >.$$

Заключение

Приведенные в статье показатели достаточно полно характеризуют конкретную схему поточного шифрования. Введенные критерии эффективности в совокупности с методиками оценки позволяют осуществить сравнение различных схем поточного шифрования. Использование количественных и качественных показателей приводит к снижению неопределенности эксперта относительно оцениваемой схемы. В целом, предложенное множество показателей и критериев эффективности, на наш взгляд, позволяют построить эффективный инструментарий оценки схем ПШ. Ниже представлена сводная таблица показателей и критериев оценки эффективности (табл. 1).

Таблица 1

Показатели эффективности функционирования схем ПШ	Критерии оценки эффективности функционирования схем ПШ
Показатели стойкости схем ПШ	
Показатели, характеризующие параметры регистров и точек съема для нелинейной функции и обратных связей	
Примитивность образующего полинома	Да/нет
Взаимно простые степени образующих полиномов	Да/нет
Степень образующего полинома, n	$n \geq 128$ бит
Плотность образующего полинома, k	$k \rightarrow n/2$
Правильность определения количества точек съема для нелинейной функции	Да/нет
Соответствие множества точек обратных связей B полному множеству положительных разностей ΔB	Да/нет
Соответствие множества точек съема для нелинейной функции $Г$ полному множеству положительных разностей $\Delta Г$	Да/нет
Наибольший общий делитель двух парных (соседних) положительных разностей должен быть равен 1	Да/нет
Показатели, характеризующие стойкость нелинейной функции	

Продолжение табл.1

Сбалансированность	Да/нет
Нелинейность, N_f	$N_f = \max\limits_{N_j} \{N_1, \ldots, N_r\}$
Алгебраическая степень, $deg(f)$	$deg(f) = \max\limits_{deg(f_j)} \{ deg(f_1), \ldots, deg(f_r)\}$
Коэффициент равномерной минимизации кросс-корреляции, $k_{рм}$	$k_{рм} = \min\limits_{k_{рм\,j}} \{ k_{рм\,1}, \ldots, k_{рм\,r}\}$
Абсолютное значение кросс-корреляции функции, C_f	$C_f = \min\limits_{l_i} \{ C_{f\,1}, \ldots, C_{f\,r}\}$
Количество векторов, при которых функция не удовлетворяет критерию распространения, num_1	$num_1 = \min\limits_{num_{1\,j}} \{ num_{11}, \ldots, num_{1\,r}\}$
Количество векторов, при которых функция имеет линейную структуру, num_2	$num_2 = \min\limits_{num_{2\,j}} \{ num_{21}, \ldots, num_{2\,r}\}$
Показатели, характеризующие стойкость процедуры ключевой инициализации	
Нелинейность операций ключевой загрузки	Да/нет
Каждый бит инициализированного регистра является результатом нелинейных преобразований всех бит ключа	Да/нет
Общие показатели	
Период гаммы, T_f	$T_f = \max\limits_{T_j} \{T_1, \ldots, T_r\}$
Линейная сложность последовательности, Λ_f	$\Lambda_f = \max\limits_{\Lambda_j} \{\Lambda_1, \ldots, \Lambda_r\}$
Длина используемых ключей, k_f	$k_f = \max\limits_{k_j} \{ k_1, \ldots, k_r\}$
Внутреннее состояние генератора (внутренняя память) M должно быть не менее $2k$ бит при длине ключа k бит	Да/нет
Длина генерируемой последовательности $\ell_п$ не должна превышать некоторого порогового значения N_{max}	Да/нет
Показатель, характеризующий стойкость схемы к аналитическим методам анализа	Да/нет
Показатели, характеризующие стойкость схемы к статистическим методам анализа, r_j и χ^2	$r_j = \dfrac{\#\{P_{ij} \ge \alpha \mid i = 1,2,\ldots,m\}}{m}$ $\chi_j^2 = \sum\limits_{k=1}^{10} \dfrac{\left(F_k - m/10\right)^2}{m/10}$
Программно- и аппаратно- реализационные показатели	
Ключевая инициализация, $n_{бз}$	$n_{бз} = \max\limits_{n_j} \{ n_1, \ldots, n_г\}$
Генерация выходной последовательности, $m_{бв}$	$m_{бв} = \max\limits_{m_j} \{ m_1, \ldots, m_г\}$
Размер используемой памяти, v_{mem}	$v_{mem} = \min\limits_{v_j} \{v_1, \ldots, v_г\}$
Скорость шифрования/дешифрования информации, s	$s = \max\limits_{s_j} \{s_1, \ldots, s_г\}$

Окончание табл.1

Количество используемых различных арифметических операций, *op*	$op = \min_{op_j} \{ op_1, \ldots, op_r \}$
Переносимость на другие платформы	Да/нет
Конструктивно-технологические показатели	
Прозрачность конструкции	Да/нет
Возможность проведения сравнительного анализа	Да/нет
Перспективность	Да/нет
Запас стойкости	Да/нет

Как видно из таблицы, вектор показателей эффективности содержит достаточно много частных показателей. На сегодняшний день до конца остаются неисследованными вопросы взаимного влияния этих показателей. Исследование сложных зависимостей и разработка методов построения оптимальных схем ПШ являются актуальными на сегодняшний день задачами.

Другим интересным направлением исследований является разработка комплексных показателей, которые интегрируют несколько частных показателей и характеризуют сразу несколько различных свойств схем. В этом случае, при обеспечении заданного уровня качества оценки (точности, доверия и т.д.) сокращается количество показателей и упрощается методика оценки эффективности схем.

Наконец, актуальной остается задача разработки методик оценки эффективности на основе использования методов системного анализа. В области оценки криптографических схем достаточно долго доминировал параметрический подход к оценке эффективности на основе показателей стойкости. Очевидно, что такой подход сегодня уже исчерпал себя. Более перспективным является использование методов определения общесистемных показателей, совместное использование методов расчета количественных показателей и определения качественных показателей (например, использование методов декомпозиции с последующими экспертными оценками). Исследования в данном направлении позволят разработать эффективные методики оценки схем ПШ.

Список литературы: 1.*А.В.Потий, О.И.Олешко*. Новые требования и принципы разработки современных алгоритмов блочного шифрования (по результатам анализа алгоритмов-кандидатов в AES)// Открытые информационные и компьютерные технологии. 2000. Вып. 12. С. 30-45. 2.*NESSIE security report*, deliverable D20, October 21, 2002, version 1.0, *http: //www.cryptonessie.org*. 3.*M.J.Robshaw*. Stream Ciphers. Technical Report TR-401, RSA Laboratories, revised July 1995. 4. *J.L.Massey*. “Cryptography and System Theory”, Proc. 24th Allerton Conf.Commun., Control, Comput., Oct. 1-3, 1986. 5.*J.L.Massey*. “Shift-register synthesis and BCH decoding”, IEEE Trans. Inform. Theory, vol. IT-15, pp. 122-127, Jan. 1969. 6.*J.D.Golic*. On the Security of Nonlinear Filter Generators. In Fast Software Encryption – Third International Workshop, Cambridge, February 1996, pp.173-188, Springer-Verlag, berlin, !996. 7.*V.Chepyzhov, T.Johansson, B.Smeets.* A simple algorithm for fast correlation attacks on stream ciphers. *http: //www.it.lth.se./thomas*/, 2000. 8.*Горбенко И, Потий А, Избенко Ю, Орлова С*. Анализ схем поточного шифрования, представленных на европейский конкурс NESSIE // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: ДСТСЗІ/СБУ; НТУ “КПІ”. 2002. Вып. 5. С. 92-110. 9.*FIPS PUB 197:2001*. Advanced Encryption Standard (AES). 10.*Andrew Rukhin, Juan Soto*. A Statistical Test Suite for Random and Pseudorandom Number Generator for Cryptographic Application. NIST Special Publication 800-22, September 2001. 11.*Потий А.В, Орлова С.Ю, Гриненко Т.А*. Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS // Правове, нормативне та метрологічне забезпечення захисту інформації в Україні: Наук.-техн. зб. 2001. Вип.2. С. 206 - 213. 12. *J. Seberry, X.-M. Zhang and Y.Zheng*. Nonlinearity and Propagation Characteristics of Balanced Boolean Functions. Information and Computation, Vol. 119, No 1, pp. 1 - 13, 1995.