УДК 004.056.57:656.2

Г.С. Безверхая

Украинская государственная академия железнодорожного транспорта, Харьков

АНАЛИЗ ПЕРСПЕКТИВЫ РАЗВИТИЯ ПОТОЧНОГО ШИФРОВАНИЯ

Проанализированы результаты предшествующих открытых конкурсов, на которых были представлены поточные шифры. Выделены перспективы развития исследований в области поточного шифрования.

Ключевые слова: *поточный шифр, стойкость, производительность, ключ.*

Введение

Постановка проблемы. В последнее время значительно увеличилось внимание ученых к поточных шифрам, в последние годы проходили ряд открытых конкурсов (NESSIE, eSTREAM и т.д.) для того чтобы отобрать новые алгоритмы поточного шифрования. Так как благодаря бурному развитию вычислительных мощностей раскрытие предшествующих шифров это вопрос времени.

Анализ последних исследований и публикаций. Последние исследования в области поточных шифров показывают, что возможно несколько вариантов определения понятия "поточный шифр", поскольку поточная архитектура, вообще говоря, не имеет четких границ [1]. Поточные шифры, так же как и блочные, являются частным случаем симметричных криптосистем шифрования (системы с секретным ключом). Разделение между этими шифрами не следует считать закостенелым. Так, например, блочные шифры, работающие в режиме обратной связи по выходу, аналогичны синхронным поточным шифрам, а самосинхронизирующимся поточным шифрам соответствуют блочные шифры с обратной связью по шифртексту. И хотя некоторые авторы предполагают довольно ограниченную область использования поточных шифров в низкопотребляющих устройствах с ограниченным объемом памяти и вычислительными ресурсами [2], значение исследований в области поточных шифров шире. Основными требованиями, предъявляемыми к поточным шифрам, являются большой период генерируемой гаммы, "хорошие" статистические свойства и высокая линейная сложность ее формирования. Именно "плохие" статистические свойства генераторов гаммы обусловили отрицательные результаты тестов алгоритмов, представленных на конкурсе NESSIE. Это же требование относится и к блочным шифрам, содержащим генератор гаммы. Особенностью поточных шифров является также то, что методы и решения их "взлома" более разнообразны по сравнению с блочными шифрами. Поэтому криптографические исследования поточных шифров явились источником ряда задач для фундаментальных направлений дискретной математики.

Целью статьи является проанализировать результаты прошедших конкурсов, а также выделить перспективы развития поточного шифрования в дальнейшем.

Основная часть

К потоковым шифрам предъявляется ряд требований: в первую очередь стойкость (безопасность и надежность). Именно поэтому зарубежные производители сейчас выбирают TripleDES, AES, Blowfish и другие блочные шифры (в частности, ГОСТ 28147-89), у которых относительно длительный и интенсивный криптоанализ не обнаружил слабостей.

Здесь следует отметить, что криптоанализ поточных шифров отнюдь не сводится исключительно к анализу свойств генератора гаммы. Помимо собственно генератора анализу подлежат процедуры инициализации. Требования стойкости иногда налагают явные ограничения на архитектуру. Например, для обеспечения стойкости схемы на уровне 2^n, где n - битовая длина ключа, необходимо, чтобы эффективная длина синхропосылки (initial vector, IV) была не меньше n бит. В противном случае для любого поточного шифра применима общая атака "балансировка время-память" (time-memory tradeoff). Для корреляционных, алгебраических и других классов атак таких простых рецептов защиты нет. При анализе программных и аппаратных реализаций поточных шифров в настоящее время все большее внимание уделяется побочным каналам: атаки по времени, простые и дифференциальные атаки по электропотреблению и электромагнитному излучению, атаки на основе аппаратных ошибок и т.д.

Следующим требованием является производительность, складывающаяся из двух основных показателей. Первый из них – непосредственно скорость шифрования, второй – быстрота процедур установки ключа и синхропосылки. При этом алгоритм с высокой скоростью шифрования может оказаться недостаточно производительным в реальных приложениях, если процедура установки синхропосылки, выполняемая часто для каждого пакета данных (как, на-

пример, в IEEE 802.11 или IPSEC), будет медленной.

Для программных шифров на производительность влияет размер исполняемого кода и данных. Если этот размер больше, чем кэш целевого процессора, то при исполнении кода возникнут неэффективные частые обращения процессора к памяти. Эти параметры в совокупности с возможностью эффективной реализации основных операций шифра определяют также применимость шифра во встроенных системах (смарт-карты, мобильные устройства, микросхемы FPGA и т.д.).

Еще одним из требований, предъявляемых к современным шифрам, как к потоковым, так и к блоковым, является создание ими шифротекста, неотличимого от случайной последовательности. Под случайной последовательностью подразумевается последовательность бит, в которой вероятности появления 0 и 1 равны ½, причём значение каждого последующего бита не зависит от предыдущих.

Методы, используемые для проверки этого условия, рассматриваются в рамках математической статистики. Сформулируем задачу: необходимо проверить гипотезу H_0 о том, что источник порождает символы алфавита {0,1} равновероятно и независимо, против альтернативной гипотезы H_1, говорящей, что последовательность создана стационарным и эргодическим источником и H_0 не выполняется.

В работах [2, 3] протестированы шифры участники двух конкурсов, а также тестировался RC4, для тестирования использовались следующие тесты:

1. Тест «ХИ-КВАДРАТ»;
2. Тест «Стопка книг».

Результаты тестирования показали, что статистический тест «Стопка книг», предложенный в [4], позволяет обнаружить неслучайность шифра RC4 при длине выходной последовательности 2^{32} бит [5]. Кроме того, новый тест позволил забраковать шифр ZK-Crypt, один из кандидатов конкурса eSTREAM: при длине выходной последовательности порядка 2^{25} бит тест различает выходную последовательность от случайной [6].

Следовательно, ранее разработанные, и новые шифры, которые были представлены на открытые конкурсы, с современным развитием вычислительных систем и разработкой новых способов взлома подвержены атакам.

Выводы

Таким образом, из сказанного ранее следует, что основной задачей построения потоковых шифров является разработка принципиально новых архитектур шифросистем.

В результате проведённого анализа выявлена перспективность развития направления исследований по выявлению возможности изменения длины ключа шифрования на регистрах сдвига с нелинейной обратной связью, а также формирования самого ключа в процессе шифрования с нелинейной зависимостью от открытого текста.

Список литературы

1. Анашин В.С. eSTREAM: быстрые и стойкие поточные шифры / В.С. Анашин, А.Ю. Богданов, И.С. Кижватов // Журнал Information Security – Информационная безопасность. – 2006. – №5. – 225 с.

2. Грибунин В.Г. eSTREAM: дитя лохнесского чудовища / В.Г. Грибунин // Журнал Information Security – Информационная безопасность. – 2006. – №3-4. – 264 с.

3. Дорошенко С.А. Экспериментальный анализ шифра rc4 и потоковых шифров, выдвинутых на конкурс ESTREAM / С.А. Дорошенко, А.М. Лубкин, Б.Я. Рябко, А.Н. Фионов. – [Электронный ресурс]. – Режим доступа к ресурсу: http://www.contrterror.tsure.ru/ site/ magazine 8/05-14-Doroshenko.htm.

4. Ryabko B. Ya. Using information theory approach to randomness testing / B. Ya. Ryabko, V.A. Monarev // Journal of Statistical Planning and Inference. – 2005. – Vol. 133, № 1. – P. 95-110.

5. Doroshenko S. The experimental distinguishing attack on RC4 / Sergey Doroshenko, Boris Ryabko. – [Электронный ресурс]. – url: http://eprint.iacr.org/2006/070.pdf.

6. Lubkin A. The distinguishing attack on ZK-Crypt cipher / Alexey Lubkin, Boris Ryabko. – [Электронный ресурс]. – url: http://www.ecrypt.eu.org/ stream/papersdir/076.pdf.

Поступила в редколлегию 3.03.2009

Рецензент: к-т техн. наук, доцент, С.И. Приходько, Украинская государственная академия железнодорожного транспорта, Харьков.

АНАЛІЗ ПЕРСПЕКТИВІ РОЗВИТКУ ПОТОКОВОГО ШИФРУВАННЯ

Г.С. Безверха

Проаналізовані результати попередніх відкритих конкурсів, на які були подані потокові шифри. Виділені перспективи розвитку досліджень в області потокового шифрування.

Ключові слова: *потоковий шифр, стійкість, продуктивність, ключ.*

ANALYSIS OF PROSPECTS OF DEVELOPMENT OF STREAM ENCRYPTION

G.S. Bezverkhaya

The are analysed results of the preceding opened competitions, which stream encryption were represented on. The are selected prospects of development of researches in area of stream encryption.

Keywords: *flow cipher, stability, capacity, key.*