Таким образом, по правилу два в целом тестирование прошли все генераторы. Однако генератор BBS выглядит предпочтительнее остальных.

Подводя итог тестированию генераторы по убыванию предпочтения можно расставить следующим образом. На первом месте находится генератор BBS, на втором – генератор на основе эллиптических кривых и, наконец, на третьем месте находится аппаратный датчик “Гряда-1М”.

Выводы

Пакет статистических тестов NIST STS является удобным и гибким инструментом исследования ГСЧ (ГПСЧ), применяемых в криптографических приложениях. Данный пакет может и должен быть взят на вооружение отечественными разработчиками соответствующих приложений. В отличие от пакета DIEHARD пакет NIST STS обладает большей гибкостью, расширяемостью и эффективностью (с точки зрения затрачиваемого времени на осуществление тестирования генератора). Кроме того, пакет NIST STS имеет большую криптографическую направленность, которая достигается путем введения в пакет таких тестов, как проверка линейной сложности и универсального теста Маурера.

Рассмотренная методика тестирования и полученные с ее использованием результаты могут рассматриваться как первичный анализ генератора. На основе пакета могут быть построены методики более глубокого статистического и структурного анализа последовательностей. Так для более надежной оценки генераторов целесообразно проводить не одно испытание, а как минимум три (одно испытание – построение одного полного статистического портрета). При повторении выводов по генератору на основе анализа каждого из трех статистических портретов степень неопределенности относительно свойств генератора существенно уменьшится и надежность решения увеличится.

Авторы в дальнейшем будут продолжать работы по разработке практических методик применения данного пакета с применением методов ранжирования объектов на основе теории нечетких множеств. Кроме того, представляет интерес сравнение результатов, полученных с использованием пакета NIST STS и пакета DIEHARD, а также выработка рекомендаций по совместному использованию этих пакетов.

Литература: 1. Д. Кнут. Искусство программирования для ЭВМ. Получисленные алгоритмы. Т. 2. – М.: Мир, 1977. – 700 с. 2. Н. П. Бусленко, Д. И. Голенко, И. М. Соболь и др. Метод статистических испытаний (Метод Монте-Карло). – М.: Физматгиз, 1962. – 337 с. 3. Ю. Л Левитан, И. М. Соболь. О датчике псевдослучайных чисел для ПК // Математическое моделирование – 1990. – Т. 2, №8. – С. 119-126. 4. А. В. Потий, А. К. Пестерев. Принципы системного подхода к сертификации генераторов псевдослучайных чисел в системах защиты информации // Радиотехника. Всеукраинский межведомственный научно-технический. сб. 1997. – Вып. 104. – С. 163-172. 5. Security requirements for Cryptographic Modules. FIPS 140-1. – U.S. Department of Commerce. 1994. 6. J. Soto Randomness Testing of the Advanced Encryption Candidate Algorithms. – NIST, 1999. 7. Helen Gustafson, et. al. Statistical test suite Crypt-SX. – Available on http://www.isrc.qut.edu.au/cryptx. 8. A. K. Leung, S. Tavares. Sequence Complexity as Test for Cryptographic Systems. – Advances in Cryptology – CRYPTO’84. Proc. LNCS, Vol. 196 – Springer-Verlag. 9. G. Marsaglia. DIEHARD Statistical Tests. – Available on http://stat.fsu.edu/~geo/diehard.html. 10. Alfred Menezes, et. al. Handbook af Applied Cryptography – CRC Press, 1997. 11. Горбенко Ю. И, Гриненко Т. А., Орлова С. Ю. Метод формирования и свойства псевдослучайных последовательностей на эллиптических кривых // Радиотехника. Всеукраинский межведомственный научно-технический. сб. 2001. – Вып. 119. – С. 163-172.

УДК 681.327.8

ОЦЕНКА СТОЙКОСТИ ПРЕОБРАЗОВАНИЙ В ГРУППЕ ТОЧЕК ЭЛЛИПТИЧЕСКИХ КРИВЫХ ПРИ ИСПОЛЬЗОВАНИИ ОТКРЫТЫХ ПАРАМЕТРОВ И КЛЮЧЕЙ В КАЧЕСТВЕ ЛИЧНЫХ

Павел Колесников

Харьковский технический университет радиоэлектроники

Аннотация: **Представлены результаты исследования криптографических преобразований в поле эллиптических кривых. Предложена новая схема работы и хранения открытых ключей и параметров в условиях, когда они хранятся в защищенном от внешних пользователей режиме. Даны расчеты стойкости новой схемы работы с ключами.**

 ISBN 966-622-022-9

Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

Summary: **In this article it is described results of research of elliptic curves. New schemes of public parameters operation and storage are proposed in the article. In article author made necessary calculations of cryptographic reliability of new proposed key operation scheme.**

Ключевые слова: **Эллиптические кривые, открытые ключи, поле Галуа, криптоанализ, стойкость.**

I Описание проблемы

В ряде источников [1, 2] исследованы свойства и характеристики систем преобразования в группе точек эллиптических кривых в общем виде E(F(Pm)). При этом, как доказывают многие авторы, основные преимущества эллиптических кривых – это уменьшение примерно в десять раз длины ключа и уменьшение вычислительной сложности прямых и обратных криптографических преобразований. Это достигается за счет меньшей длины ключей и общесистемных параметров и использования арифметики в проективных геометриях. Уравнение эллиптической кривой в расширенном поле Галуа имеет вид:

$$y^2+xy=x^3+ax^2+b\ (mod\ f(x),P)$$

где a и b являются элементами поля $GF(2^m)$, полиномами степени m.

Анализ источников [3] показывает, что стойкость систем, построенных на эллиптических кривых, базируется на сложности решения дискретного параметрического уравнения в группе точек эллиптической кривой вида

$$Q=d*G(mod\ f(x),P), \tag{1}$$

где G – базовая точка на эллиптической кривой, d – личный ключ (выбирается из интервала $0\le d\le n-1$), n – порядок базовой точки, Q – открытый ключ – точка на эллиптической кривой, $f(x)$ – примитивный полином степени m, P – второй модуль преобразований (обычно выбирается как P=2).

II Классическая атака на системы с открытыми ключами на эллиптических кривых

Решение уравнения (1) относительно d, при известных параметрах $\{Q, G, f(x), P\}$- называется решением дискретного уравнения на эллиптической кривой. Известно несколько методов решения уравнения, основные из которых – ρ-метод Полларда и λ-метод Полларда [4]. Сложность решения уравнения зависит от величины n. Для различных методов известны следующие оценки сложности:

$$I_\rho=\sqrt{\frac{\pi n}{2}}, \tag{2}$$

$$I_{\rho-опт}=\sqrt{\frac{\pi n}{4}}, \tag{3}$$

$$I_\lambda=2\cdot\sqrt{n}, \tag{4}$$

где I_ρ – сложность ρ-метода Полларда, $I_{\rho-опт}$ – сложность оптимального ρ-метода Полларда, I_λ – сложность λ-метода Полларда.

Сложность измеряется в количестве операций сложения на эллиптической кривой.

Рассмотрим криптографические системы шифрования и цифровой подписи, в которых могут быть использованы преобразования на эллиптической кривой. В настоящее время действующих стандартов Украины алгоритмов на эллиптической кривой нет. Существуют проекты стандартов цифровой подписи и направленного шифрования, в которых в качестве односторонней необратимой функции применяется функция возведения в степень в поле эллиптической кривой (1). Общесетевыми параметрами в этих системах будут $f(x)$, P, $\#E$ (порядок эллиптической кривой).

Порядок эллиптической кривой $\#E$ связан с порядком базовой точки соотношением:

$$\#E=l\cdot n,$$

где l – кофактор – коэффициент, обеспечивающий связь между величинами порядка базовой точки и $\#E$. Кофактор для практических задач принимают не больше l=8.

К общесетевым параметрам относятся также коэффициенты уравнения эллиптической кривой $\{a, b\}$. Общесетевые параметры, по стандартной схеме реализации криптоалгоритмов, генерируются один раз на

продолжительное время, хранятся в открытом виде и распространяются всем участникам обмена защищенными сообщениями. Таким образом, криптоаналитик для получения открытого сообщения или подделки цифровой подписи использует общесетевые параметры в качестве исходных данных, заранее ему известных. Кроме того, для криптоанализа ему необходимо знать открытый ключ, которым было зашифровано сообщение. Анализ отношений (2)-(4) показывает, что сложность решения зависит только от величины n, если все общесистемные параметры известны.

Очевидно, повышение стойкости может быть достигнуто, если ключи и/или общесетевые параметры $\{d, Q\}$, $\{G, f(x), P, a, b\}$ сделать личными. Рассмотрим несколько возможных случаев использования ключей и общесистемных параметров.

1. Ключевые параметры $\{d, Q\}$ объявим личными, а общесетевые параметры– открытыми.
2. Ключевые и общесетевые параметры объявим личными.

III Атака на алгоритм при неизвестном открытом ключе Q и известных общесетевых параметрах

Пусть ключи $\{Q, d\}$ неизвестны для криптоаналитика или внешнего пользователя, а общесетевые параметры $\{G, f(x), P, a, b\}$– известны. Для криптоаналитика в этом случае в уравнении (1) появляется два неизвестных Q и d. Уравнение не имеет однозначного решения и в предельном случае сложность I_1 криптоанализа является линейной функцией от n. В этом случае для нахождения пары ключей $\{Q, d\}$ необходимо применять атаку методом грубой силы по всем возможным парам ключей.

Будем осуществлять атаку в следующей последовательности. Сначала необходимо подобрать d_i. Все возможные d_i имеют равные вероятности появления. При длине ключа d в битах, равной l_n, криптоаналитик осуществляет грубый перебор. Можно считать, что самые высоко вероятные ключи с длиной l_n. Тогда I_1 раз выбирая d можно найти личный ключ, если известно G. Далее из (*1*) можно найти неизвестный ключ Q. Тогда сложность проведения криптоанализа $I_1 \sim (l_n - 1)$. Для рассмотренного режима использования шифра, где ключи являются равновероятными, результаты оценки стойкости приведены в таблице 1.

Таблица 1

Порядок базовой точки n	Сложность ρ-метода Полларда. I_ρ	Сложность оптимального ρ-метода Полларда. $I_{\rho\text{-}on}$	Сложность λ-метода Полларда. I_λ	Сложность I_1 при конфиденциальном ключе Q
2^{128}	$2^{64,72}$	$2^{64,22}$	$2^{65,39}$	2^{127}
2^{160}	$2^{80,17}$	$2^{79,68}$	$2^{80,85}$	2^{159}
2^{256}	$2^{128,31}$	$2^{127,83}$	$2^{82,49}$	2^{255}
2^{512}	$2^{256,30}$	$2^{255,82}$	$2^{256,99}$	2^{511}
2^{1024}	$2^{512,26}$	$2^{511,78}$	$2^{512,94}$	2^{1023}

Рассмотрим схему работы с ключами со стороны различных пользователей, приведенную на рис. 1.

1. Генерация общесетевых параметров и ключей, постановка подписи, расшифрование. **Криптоатака:** бессмысленна	**3.** Криптоаналитик **Криптоатака:** I_1 ⟷	**2.** Отправка сообщений, проверка подписи **Криптоатака:** $I_{\rho\text{-}on}$

Рисунок 1

Существует три типа пользователей в данной схеме. К первому типу относится пользователь, который генерирует общесетевые параметры и свой секретный ключ. Здесь известны все ключи и параметры. Ведение криптоанализа этим пользователем не имеет смысла.

Ко второму типу пользователей относится санкционированные пользователи системы, которые обмениваются защищенными сообщениями с первым пользователем. Известными здесь являются общесетевые параметры и открытый ключ первого пользователя Q, неизвестен ключ d. Криптоанализ со стороны этих пользователей может вестись с целью подделать цифровую подпись первого пользователя. Сложность криптоанализа в лучшем случае равна $I_{\rho\text{-}on}$.

К третьему типу пользователей относится внешние пользователи системы. В предложенной схеме им не

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

известны ключи d, Q. Известными являются общесетевые параметры. Криптоанализ этими пользователями может вестись с целью подделать цифровую подпись первого пользователя, расшифровать сообщение, зашифровать сообщение (защита от последней угрозы не может быть реализована в стандартной схеме ведения криптозащиты и схожа с симметричными системами). Сложность криптоанализа равна I_1.

По стойкости система, предложенная в пункте 1, близка к стойкости симметричных алгоритмов. Сравнивая сложности криптоанализа для случаев I_ρ, $I_{\rho\text{-опт}}$, I_λ и I_1 можно сделать вывод, что использование данного варианта хранения ключей позволяет либо при фиксированном требовании к стойкости системы уменьшить порядок точки G по сути в $\sqrt{n}$ раз или, оставив ту же длину ключа, повысить стойкость преобразований на эллиптических кривых до I_1, уменьшая n.

IV Атака на алгоритм при неизвестном открытом ключе Q и общесетевых параметрах

Рассмотрим вариант, когда неизвестны ключи $\{Q, d\}$ и общесистемный параметр G (предполагаем, что неизвестно все, кроме a, b, $f(x)$, P). Определим сложность криптоанализа в этом случае. Анализ показывает, что задачу криптоанализа можно решать двумя способами.

Рассмотрим подробнее первый способ. Он состоит в нахождения двух параметров d, G атакой грубая сила. Количество допустимых значений для базовой точки $|G|$ в предельном случае равно порядку эллиптической кривой. Сложность этой атаки оценивается как

$$I_2 = n \cdot \#E = l \cdot n^2 \qquad (5)$$

где n – порядок базовой точки, $\#E$ – порядок эллиптической кривой, l – кофактор.

Примем значение l=8 и рассчитаем сложность ведения криптоанализа в данном варианте хранения ключей и общесистемных параметров. В таблице 2 приведено значение стойкости I_2.

Таблица 2

Порядок базовой точки n	Сложность I_2 подбора ключей (Q, d) и общесетевого параметра G
2^{128}	2^{259}
2^{160}	2^{323}
2^{256}	2^{515}
2^{512}	2^{1027}
2^{1024}	2^{2051}

Сравнительный анализ по I показывает, что незнание дополнительной базовой точки G приводит к усложнению атаки и имеет квадратичную зависимость от n, сложность решения задачи большая, чем перебор, то есть больше, чем для симметричного алгоритма. В этих условиях при фиксированном n можно обеспечить более высокую стойкость системы, или n может быть уменьшено без потери стойкости системы относительно классического варианта.

Второй способ ведения криптоатаки можно считать случаем, когда неизвестен порядок кривой. Во втором случае можно искать все значения открытого ключа Q посредством рассмотрения группы точек эллиптической кривой последовательно. Затем, при известном Q, можно найти d (сложность перебора равна n), G (сложность перебора равна n). Сложность криптоанализа при неизвестном значении порядка эллиптической кривой можно оценить как

$$I_2' = \#E \cdot n^2 = l \cdot n^3 \qquad (6)$$

где $\#E$ – порядок эллиптической кривой на первом этапе.

В таблице 3 приведено значение стойкости в этом случае.

Таблица 3

Порядок базовой точки n	Сложность I_2' подбора ключа d и общесетевого параметра G
2^{128}	2^{387}
2^{160}	2^{483}
2^{256}	2^{771}
2^{512}	2^{1539}
2^{1024}	2^{3075}

ISBN 966-622-022-9

Приведенное выше убеждает нас, что при условии, если Q или G объявить конфиденциальными параметрами, то можно обеспечить сложность криптоанализа, превышающую сложность грубого перебора для симметричного алгоритма.

Выводы

Практическая реализация такой схемы может быть следующая. Очевидно, что обеспечить конфиденциальность базовой точки G, как общесетевого параметра, сложно. Хотя есть случай рассылки G по защищенному каналу с записью в качестве ключа. На практике вполне реализуем случай, когда Q хранится как конфиденциальный ключ. Ключи и параметры хранятся и пересылаются в защищенном виде, реальная стойкость такой системы может быть оценена по I_1 и может совпадать со стойкостью симметричных систем. Естественно, что для рассмотренного случая необходимо построить соответствующие протоколы управления параметрами d, Q, при которых они останутся конфиденциальными, аутентичными и целостными.

Литература:1. Бондаренко М. Ф., Горбенко И. Д., Качко Е. Г. Свинарев А. В., Гриненко Т. А. Сущность и результаты исследований свойств перспективных стандартов цифровой подписи X9.62-1998 и распределение ключей X9/63-199X на эллиптических кривых //Радиотехника 2000.- № 114- С. 15-24. 2. Горбенко И. Д., Збитнев С. И. Расширенное поле Галуа GF(2M). Вычислительная сложность простейших операций над расширенным полем GF(2M) // Радиотехника 2000.- 114- С. 80-89. 3. ANSI X9.63-199x: Elliptic curve key agreement and transport protocols, draft. 4. R. Gallent, R. Lambert And S. Vatsone Improving the paralelized Pollard lambda search on binary anomalous curves, to appear in Mathematics of Computation.

УДК 681.3.06

ТЕХНОЛОГИЯ БЕЗОПАСНОЙ ПАМЯТИ В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Даниил Меалковский, Юрий Горбенко, Виталий Вервейко, Сергей Полчанинов
Харьковский государственный технический университет радиоэлектроники

Аннотация: **Рассматривается задача построения и реализации модели безопасной памяти, создания программных компонентов работы с безопасной памятью в системах защиты информации.**

Summary: **This article describes a safe memory model construction and realization, creation a software component for working with safe memory in information security system.**

Ключевые слова: **Системы защиты информации, безопасная память, объект безопасности.**

Введение

Основной особенностью современных операционных систем является их объектная ориентированность. Преимущества использования системой объектов (objects) для регулирования доступа к системным ресурсам можно объяснить двумя основными причинами. Во-первых, использование объектов позволяет разработчику обновлять систему функционально, так как определенный интерфейс поддерживается. Во-вторых, использование объектов позволяет использовать возможность защиты функционирования системы на уровне защиты функционирования отдельных объектов. Преимущество использования объектов проявляется также на этапе разработки, так как позволяет упростить разработку сложных многокомпонентных систем и информационных технологий.

Для применения технологии объектов и дескрипторов при реализации систем защиты информации необходимо создать сервисы, обеспечивающие защищенность объекта безопасности от внешних компонентов системы, например, реализации модели безопасной памяти (secure memory model или SMM) и менеджеров объектов безопасности (secure objects или SO) для безопасного функционирования объектов в системе. Построение и реализация модели SMM являлись целью данной работы. Созданные программные компоненты работы с SMM встраиваются в платформы Microsoft® Win32® и используются Cryptographic Service Provider (CSP).

Дескрипторы и объекты

Объекты - это структуры данных, представляющие системный ресурс. Приложения не имеют прямого доступа к данным объекта или системному ресурсу, который представляет объект. Вместо этого приложения получают дескрипторы объектов, которые могут быть использованы для изменения системного ресурса.

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.