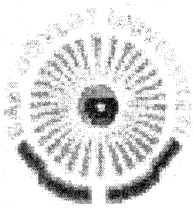
MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
ACADEMY OF PEDAGOGICAL SCIENCES OF UKRAINE
VINNYTSIA NATIONAL TECHNICAL UNIVERSITY
"STEFAN cel MARE" UNIVERSITY of SUCEAVA
BAKU STATE UNIVERSITY
NATIONAL INFORMATION CENTRE FOR
UKRAINE-EU SCIENCE AND TECHNOLOGY COOPERATION




PROCEEDINGS

of the Fifth International Conference

INTERNET - EDUCATION – SCIENCE

IES – 2006

Volume 2

10-14 October, 2006 *Vinnytsia - UKRAINE*

UNIVERSUM-VINNYTSIA
2006

УДК 378 + 681.324
І73

Друкується за рішенням Ученої ради Вінницького національного технічного університету Міністерства освіти і науки України

Відповідальний за випуск *В. В. Грабко*
Підготовлено до друку: *В. В. Грабко, В. І. Месюра, О. А. Дячок*

І 73 **ІНТЕРНЕТ-ОСВІТА-НАУКА-2006, п'ята міжнародна конференція ІОН–2006**, 10–14 жовтня, 2006. Збірник матеріалів конференції. Том 2. – Вінниця: УНІВЕРСУМ-Вінниця, 2006. – 420 с.

ISBN 966-641-193-8 (том 2)

П'ята міжнародна конференція "ІНТЕРНЕТ – ОСВІТА – НАУКА – 2006" (ІОН –2006) присвячена обговоренню питань застосування в освіті та наукових дослідженнях нових інформаційних технологій, що спираються на можливості Інтернет.

УДК 378 + 681.324

Доповіді у збірнику згруповані по секціях, відповідно до основних напрямків конференції:

Том1:

A Інтернет та інформаційні технології в освіті та наукових дослідженнях
B Методологія та практика дистанційної освіти
C Психологія кіберпростору
D Інформаційні технології в економіці
E Програмне забезпечення для Інтернет

Том2:

F Комп'ютерні мережі та захист інформації
G Технології обробки та передачі зображень
H Інтелектуальні інформаційні системи
I Комп'ютерне моделювання у наукових дослідженнях

Матеріали доповідей також представлені на Web-сайті конференції (http:/www.vstu.vinnica.ua/ies2006), що містить електронну версію даного збірника, і базу даних з відомостями про учасників конференції.

Тексти доповідей друкуються в авторській редакції.

ISBN 966-641-191-1 (загальний)

ISBN 966-641-193-8 (том 2)

ПРОБЛЕМЫ ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИ СТОЙКИХ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

К.В. Черняхович, Ю.Е. Яремчук

Винницкий национальный технический университет
21000, г. Винница, ул. Хмельницкое шоссе, 95, 2-ой корпус, кафедра ВТ.

Abstract

This work describes the main methods, approaches and claims of cryptographic stable pseudo random sequences generators construction. It was given the comparative analysis of generators defined by standard ANSI X9.17 and proposed the pseudo random sequences generator based on the elliptic curves mathematical tool that have better statistical characteristics. The statistical testing was done with the usage of NIST STS.

Сегодня актуальность методов защиты информации ни у кого не вызывает сомнения. При построении большинства методов защиты информации важным элементом являются генераторы псевдослучайных последовательностей, которые могут быть использованы для решения таких задач [1]:
1) Генерирование гаммирующих последовательностей, при построении синхронных поточных шифров.
2) Хеширование информации.
3) Построение самосинхронизирующихся потоковых шифров.
4) Формирование ключевой информации, на которой основывается стойкость криптоалгоритмов.
5) Формирование случайных запросов при реализации большого числа криптографических протоколов.
6) Внесение неопределенности в работу аппаратно-программных средств, которые защищаются.
7) Использование в построении вероятностных методов шифрования.

Для построения криптографически стойких систем существует необходимость использования генераторов псевдослучайных последовательностей удовлетворяющих таким требованиям [1]:

- обеспечение необходимой криптографической стойкости;
- обеспечение достаточной степени приближенности псевдослучайной последовательности к случайной, то есть обладать приемлемыми статистическими свойствами;
- большой период формируемой последовательности;
- возможность эффективной аппаратной и программной реализации.

Один из подходов к построению криптографически стойких генераторов псевдослучайных последовательностей заключается в построении такого генератора псевдослучайных последовательностей, для которого противнику будут неразрешимы за полиномиальное время такие три задачи [1]:

1) Определение $(i-1)$-го элемента γ_{i-1} последовательности на основе известного фрагмента гаммы $\gamma_i\gamma_{i+1}\gamma_{i+2}\cdots\gamma_{i+b-1}$ конечной длины b.
2) Определение $(i+1)$-го элемента γ_{i+1} последовательности на основе известного фрагмента гаммы $\gamma_{i-b+1}\cdots\gamma_{i-2}\gamma_{i-1}\gamma_i$ конечной длины b.
3) Определение ключевой информации по известному фрагменту гаммы конечной длины.

Однако применение такого подхода на практике вызывает ряд трудностей [1]. Поэтому широкое распространение получил другой подход, при котором задачу построения криптографически сильного генератора сводят к задаче построения статистически безопасного генератора. При этом статистически безопасный генератор должен удовлетворять таким требованиям [1]:
1) Статистические тесты не находят в псевдослучайной последовательности каких либо закономерностей.
2) Нелинейное преобразование, которое зависит от секретного ключа и используется для построения генератора на основе нелинейной функции, владеет свойством размножения искажений.
3) При инициализации псевдослучайными значениями генератор порождает статистически независимые псевдослучайные последовательности.

Для определения статистических характеристик и проведения анализа генераторов псевдослучайных последовательностей с точки зрения их статистической безопасности, существует ряд статистических тестов направленных на выявление различных дефектов генераторов псевдослучайных последовательностей. Среди известных программных пакетов, которые применяются для статистического тестирования, следует отметить DIEHARD, Crypt-SX и NIST STS [2-4]. Эти пакеты могут использоваться для [4]:
1) идентификации генераторов псевдослучайных чисел, которые формируют «плохие» двоичные последовательности;

2) разработки новых генераторов псевдослучайных последовательностей;
3) проверки корректности реализации алгоритмов для генерации псевдослучайных последовательностей;
4) изучения генераторов, которые описаны в стандартах;
5) изучения степени случайности реальных используемых генераторов.

Так, например, пакет NIST STS включает в себя 16 статистических тестов, результатом которых есть примерно 189 вероятностей в зависимости от исходных данных [4]. Прохождение теста определяется на основе выдвинутой гипотезы, вероятности и уровня значимости. Все тесты направлены на выявление дефектов случайности.

Сегодня среди генераторов, которые отвечают вышеприведенным требованиям к статистически безопасным генераторам, одним из самых распространенных является генератор, описанный в стандарте ANSI X9.17 [5]. Основными его преимуществами есть высокое быстродействие и достаточно высокая криптостойкость. Однако в процессе статистического анализа при помощи пакета NIST STS были выявлены некоторые недостатки присущие данному генератору, а именно для уровня значимости 0,01, количество тестов, которые прошли более 99% последовательностей сформированных генератором, который определен стандартом ANSI X9.17 равняется 110 из 189, что составляет всего 58,2%. Для уровня значимости 0,001, при тех же условиях это значение составляет 160 из 189, то есть 84,6% тестов было пройдено. В данном случае, под уровнем значимости понимается вероятность того, что статистика теста примет значение больше, чем наблюдается при опыте касательно случайности последовательности.

Таким образом, на основе проведенных тестов, можно говорить об относительной статистической безопасности генератора определенного стандартом ANSI X9.17, так как тест показал, что при уровне значимости 0,01 было выявлено 79 дефектов случайности тестируемых последовательностей сформированных при помощи данного генератора. В связи с этим, на сегодня актуальным остается вопрос разработки генераторов псевдослучайных последовательностей с улучшенными статистическими характеристиками.

В этой связи определенный интерес вызывают исследования относительно построения статистически безопасных генераторов псевдослучайных последовательностей основанных на математическом аппарате эллиптических кривых [6-9], криптостойкость таких генераторов базируется на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой [6, 10].

Предложено генератор псевдослучайных последовательностей на основе математического аппарата эллиптических кривых. В основу такого генератора положено операцию сложения двух точек эллиптической кривой с использованием рекурсивной формулы формирования псевдослучайной последовательности. При этом за один шаг работы генератора формируется последовательность длиной 160 бит, из которых за определенным законом выделяют 16 бит для формируемой псевдослучайной последовательности, то есть в данном случае каждый 10-й бит. Для данного генератора проведена оценка статистических свойств, которая показала, что для уровня значимости 0,01, количество тестов, которые прошли более 99% последовательностей сформированных таким генератором, составило 133 из 189, что на 23 теста или на 12,1% лучше, чем у генератора определенного ANSI X9.17. Это означает, что число дефектов генератора уменьшено на 12,1%. Такой результат является качественным показателем предложенного генератора. Однако проведенные тесты для уровня значимости 0,001 при тех же условиях показали улучшение характеристики только на 1,1%, что говорит о потребности дополнительных исследований в данной области.

Литература:

[1] Иванов М.А., Чугункою И.В. Теория, применение и оценка качества генераторов псевдослучаных последовательностей. – М.: «КУДИЦ-ОБРАЗ», 2003. – 240 с.: ил.
[2] G. Marsaglia. DIEHARD Statistical Tests. – Available on http://stat.fsu.edu/~geo/diehard.html.
[3] Helen Gustafson, et. al. Statistical test suite Crypt-SX. – Available on http://www.isrc.qut.edu.au/cryptx.
[4] Andrew Rukhin, Juan Soto et. oth. "A Statistical Test Suite For Random And Prseudorandom Number Generators For Cryptographyc Applications" // NIST Special Publication 800-22, 2001.
[5] ANSI X9.17 -1995 Financial Institution Key Management (Wholesale) Appendix C, American National Standards Institute, 1995. (Because ANSI has withdrawn X9.17, the appropriate reference is to ANSI X9.31).
[6] Blake I., Seroussi G., Smart N. Elliptic Curves in Cryptography. – Cambridge University Press, 1999. – p.204.
[7] Гриненко Т.А., Горбенко Ю.И., Орлова С.Ю. Метод формирования и свойства псевдослучайных последовательностей на эллиптических кривых // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2001. Вып. 119. С. 119-123.
[8] Гриненко Т.А., Збитнев С.И., Мялковский Д.В. Методы формирования псевдослучайных последовательностей в группах точек эллиптических кривых. // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2002.
[9] Guang Gong, Thomas A. Berson, Douglas R. Stinson. Elliptic Curve Pseudorandom Sequence Generators. University of Waterloo. 2001.
[10] Alfred Menezes. Evaluation of Security Level of Cryptography: The Elliptic Curve Discrete Logarithm Problem (ECDLP). University of Waterloo. December 14, 2001.