бирается из интервала [6,16]. Последовательность s^N разбивается на неперекрывающиеся L-битовые блоки. Первые Q блоков используются для инициализации теста, оставшиеся K блоков используются для вычисления тестовой функции.

Результаты тестирования. Тестирование проведено на 100 000 инициализирующих блоков и 2 000 000 тестовых блоков. Отклонение должно быть меньше допустимого в 99% случаев.

Таблица 3.

Результаты тестирования улучшенным тестом Маурера.

Размер блока, бит	Значение параметра	Отклонение параметра	Допустимое отклонение
6	6.0001889325	0.0001889325	0.0020178248
7	7.0004480509	0.0004480509	0.0020257965
8	7.9980061763	0.0019938237	0.0020492452
9	9.0015937271	0.0015937271	0.0020629726

Тест 6. Сжатие участка последовательности архиваторами WinZip и WinRar. Показывает, насколько предсказуема последовательность. Хорошая последовательность не должна сжиматься архиватором [1].

Результаты проведенного тестирования подтверждают достаточную статистическую устойчивость генератора псевдослучайных последовательность на основе ОА. В дальнейшем предполагается провести сравнительный анализ статистической устойчивости и других показателей качества генераторов на основе предложенного подхода с известными генераторами.

Архиватор	Исходный размер, байтов	Размер после сжатия, байтов
WinZip	3 000 000	3 000 460
WinRar	3 000 000	3 000 000

Работа поддержана грантами РФФИ № 01-07-90211 и 03-07-90075.

Библиографический список

1. *Варфоломеев А. А., Жуков А. А., Пудовкина М. А*. Поточные криптосистемы. Основные свойства и методы анализа стойкости: Учебное пособие. М.: ПАИМС, 2000.

2. *Pudovkina M.* Statistical weaknesses in the alleged RC4 keystream generator. - Proceedings of the 4th International Workshop on Computer Science and Information Technologies CSIT'2002, Patras, Greece, 2002. http://www.lar.ee.upatras.gr/csit2002/.

3. *Hedayat A.S., Sloane N.J.A., Stufken J.* Orthogonal arrays: theory and applications. - N.Y.: Springer-Verlag, New York, 1999.

4. *Мазурова Т.А., Чефранов А.Г.* О генерации ортогональных матриц произвольной силы//Известия ТРТУ. Специальный выпуск. Материалы XLVII НТК. Таганрог: ТРТУ, 2002, №1. С.81-82.

5. *Chefranov A.G., Mazurova T.A., Babenko L.K.* About application of orthogonal Arrays for generating of pseudorandom sequences. - Proceedings of the 4th International Workshop on Computer Science and Information Technologies CSIT'2002, Patras, Greece, 2002. http://www.lar.ee.upatras.gr/csit2002/.

6. *Мазурова Т.А., Чефранов А.Г., Бабенко Л.К., Сидоров И.Д.* О различных способах формирования псевдослучайных последовательностей на основе ортогональных матриц// 8-я Международная конференция «Теория и техника передачи, приема и обработки информации» («Интегрированные информационные системы, сети и технологии») «ИИСТ-2002»: Сб. научных трудов. Харьков: ХНУРЕ.2002, С.580-583.

7. *Д. Кнут.* Искусство программирования. Том 2. Получисленные алгоритмы. 3 издание. М, Вильямс, 2001.

В.В. Котенко, С.В. Поликарпов
Россия, г. Таганрог, ТРТУ

ФОРМИРОВАНИЕ ИСХОДНОЙ ПРОЕКЦИИ ВИРТУАЛЬНОГО ВЫБОРОЧНОГО ПРОСТРАНСТВА АНСАМБЛЯ КЛЮЧА

Here is researched questions of application virtual ensembles of a key for making decisions for tasks of information security that opens a prospect for practical decision of

a problem of theoretical maintenance of unencoding for the algorithms of information security.

Исследование вопросов применения виртуальных ансамблей ключа для решения задач информационной безопасности интересно тем, что открывает перспективу практического решения проблемы обеспечения теоретической недешифруемости (ТНДШ) алгоритмов защиты информации. С позиций теории информации данные алгоритмы отражают преобразования выборочного пространства ансамбля ключевых данных (X) в выборочное пространство ансамбля ключевых последовательностей (Y) и их использование для представления (F) ансамбля сообщений (M) ансамблем криптограмм (E). Результаты проведённых исследований показывают, что включение в состав этих преобразований (рис. 1) виртуального выборочного пространства ключа (SZ) открывает возможность обеспечения бесконечной энтропии ключевых последовательностей. Однако пока остаётся открытым практически важный для задач защиты информации вопрос: какие ограничения накладывает это включение на объём ключевых данных? Логика подсказывает, что данные ограничения должны определяться условиями формирования дискретной проекции (S) виртуального выборочного пространства ключа.

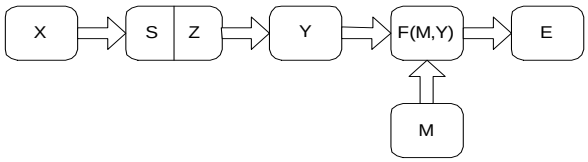

Рис. 1. Представление алгоритма защиты с позиций теории информации

Постановка задачи

Имеется виртуальное выборочное пространство ключа, заданное совместным виртуальным ансамблем SZ, где ансамбль S является дискретным, а ансамбль Z – непрерывным. Требуется определить минимально возможное число точек выборочного пространства ансамбля S, необходимое для того, чтобы совместный ансамбль SZ был способен обеспечить теоретическую недешифруемость алгоритма защиты информации.

Стратегия решения

Пусть XSZY является совместным ансамблем и выборочное пространство ансамбля S содержит N точек. Известно [1], что выражение для средней взаимной условной вероятности $I[XS;Y/Z]$ можно представить двумя способами:

$$I[XS;Y/Z]=I[X;Y/Z]+I[S;Y/ZX], \quad (1)$$

$$I[XS;Y/Z]=I[X;Y/Z\,S]+I[S;Y/Z]. \quad (2)$$

Последнее слагаемое в (1) и последнее слагаемое в (2) неотрицательны и ограничены сверху величиной $H(S)\le \log_2 N$. Отсюда, приравнивая правые части в (1) и (2), можно получить $\left|I[X;Y/Z\,S]-I[X;Y/Z]\right|\le \log_2 N$. (3)

Статистическая независимость X и Y, следующая из условий теоретической недешифруемости, определяет справедливость равенства

$$I[X;Y/Z]=0. \quad (4)$$

С учётом (4), неравенство (3) принимает вид

$$\log_2 N \ge I[X;Y/ZS]. \quad (5)$$

Так как среднее количество информации всегда положительно, знак модуля при переходе от (3) к (5) опускается.

Запишем выражение для $I[X;Y/ZS]$ в виде

$$I[X;Y/ZS]=H[X/ZS]-H[X/YZS], \quad (6)$$

где $H[X/YZS]=\sum_x\sum_y\sum_s\int_z p(x,y,z,s)\log\frac{1}{p(x/y,z,s)}dz=$

$$=H[X/YZS]=\sum_x\sum_y\sum_s\int_z p(x,y,z,s)\log\frac{p(x,y,z)}{p(x,y,zs)}dz\,. \quad (7)$$

Применяя цепную формулу для вероятности, имеем

$$H[X/YZS]=\sum_x\sum_y\sum_s\int_z p(x,y,z,s)\log\frac{p(y/zs)}{p(x/zs)p(y/xzs)}dz\,, \quad (8)$$

откуда, учитывая статистическую независимость X и Y

$P(y/xzs)=P(y/zs)$ для всех x,y,z,s при $P(xzs)>0$,

получаем $H[X/YZS]=\sum_x\sum_s\int_z p(xzs)\log\frac{1}{p(x/zs)}dz=H[X/ZS].$ (9)

На основании (6) с учётом (9) неравенство (5) приводится к виду $\log N\geq 0$, (10)

откуда следует *правило* выбора числа составляющих N дискретной проекции S виртуального выборочного пространства ансамбля ключа: $N\geq 1$. (11)

Проверка полученного правила проводилась из условия, что качество защиты сообщений M зависит от статистической независимости битов в ключевых последовательностях Y и статистической независимости ключевых последовательностей Y между собой. Для исследования статистических свойств ключевых последовательностей Y авторами был использован набор статистических тестов NIST STS (NIST Statistical Test Suite). Тестирование проводилось по методике, указанной в [2], при этом были получены результаты, подтверждающие, что достаточно одной точки дискретной проекции S для получения качественных статистических характеристик ключевых последовательностей Y. Пример корреляционной функции ключевой последовательности Y показан на рис. 2.

Рис. 2. Корреляционная функция ключевой последовательности Y

Выводы

Для обеспечения теоретической недешифруемости алгоритма защиты информации объём ключевых данных должен обеспечивать формирование не менее одной точки дискретной проекции виртуального выборочного пространства ансамбля ключа.

Библиографический список

1. *Котенко В.В.* Стратегия формирования виртуальных выборочных пространств. Новый подход к решению задач защиты информации, Радиоэлектронные технологии информационной безопасности: Сборник научных трудов; Под ред. К.Е. Румянцева. Таганрог: Изд-во ТРТУ, 2002.

2. A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22. May 15, 2001.