

$$B_0^h(t) = \sum_{k=-\infty}^{\infty} \left(c_{1h} U p(\pi k) + \frac{i}{\pi} c_{2h} u_k + \frac{2}{\pi^2} c_{3h} v_k \right) \frac{(-1)^k}{\alpha t - \pi k}.$$

Огибающие осциллирующих сигналов, прошедших через экран D , для двух поляризаций определяются формулами

$$T_1(t) = E_0 |\sin(\alpha t) B_0^h(t)|, \quad T_2(t) = E_0 |\sin(\alpha t) B_0^g(t)|. \quad (28)$$

Численный пример

Численно исследована структура поля (27). Расчеты производились для параметров: $\alpha = \pi 10^9$ Гц, $\omega_0 = 6\pi 10^9$ Гц, $\Delta = 5$ см, $\epsilon = 4\epsilon_0$, $\mu = \mu_0$, $G = \frac{1+i}{2c}$, $Z = \frac{1-i}{2c}$.

$$\hat{B}_0 = 0, \quad \theta_0 = \frac{\pi}{4}, \quad \varphi_0 = 0, \quad E_0 = 1.$$

На рисунке 1 изображены графики линий (26), (28). Показано, что импульс (график 3), падающего под углом $\theta_0 = \frac{\pi}{4}$ на экран TE -поля, при прохождении через экран D разлагается на сумму двух импульсов. Носителем первого импульса (график 1) является TE -поле, носителем второго импульса – TH -поле, распространяющееся за экраном под углом $\theta_0 = \frac{\pi}{4}$. Для частоты $\omega_0 = 5,36\pi 10^9$ Гц величина $T_1(0)$ уменьшается и принимает значение 0,093. Заметим, что в работе [9] представлены графики для экрана с аналогичными параметрами в случае монохроматических полей.

Заключение

Построено аналитическое решение краевой задачи проникновения радиоимпульса с финитным спектром через биизотропный плоский слой. В качестве носителя сигнала выбрано электромагнитное поле, распространяющееся в пространстве и подчиняющееся уравнениям Максвелла, для которых сформулирована краевая задача дифракции. Методика решения задачи основана на использовании нелокальных граничных условий, связывающих поля по обе стороны экрана. Для представления узкополосного сигнала использовались атомарные функции и теорема Котельникова-Шеннона, позволяющие представить сигнал через дискретные временные отсчеты. Решение задачи реализовано численно и исследованы искажения и преобразование сигналов

при прохождении через экран.

Литература:

1. Виноградов, А.П. Электродинамика композитных материалов / А.П. Виноградов. – М.: Эдиториал УРСС, 2001. – 208 с.
2. Лагарьков, А.Н. Радиопоглощающие материалы на основе метаматериалов / А.Н. Лагарьков, В.Н. Кисель, В.Н. Семенов. – Радиотехника и электроника, 2012. – Т. 57, № 10. – С. 1119–1127.
3. Гуляев, Ю.В. Метаматериалы: фундаментальные исследования и перспективы применения / Ю.В. Гуляев, А.Н. Лагарьков, С.А. Никитов. – Вестник РАН, 2008. – Т. 78, № 5. – С. 438–457.
4. Кравченко, В.Ф. Лекции по теории атомарных функций и некоторым их приложениям / В.Ф. Кравченко. – М.: Радиотехника, 2003. – 510 с.
5. Кравченко, В.Ф. Алгебра логики, атомарные функции и вейвлеты в физических приложениях / В.Ф. Кравченко, В.Л. Рвачев. – М.: Физматлит, 2006. – 416 с.
6. Басараб, М.А. Аппроксимация финитными функциями и теорема Уиттекера-Котельникова-Шеннона в цифровой обработке сигналов / М.А. Басараб, Е.Г. Зелкин, В.Ф. Кравченко, В.П. Яковлев. – Успехи современной радиоэлектроники. – 2003, – № 9. – С. 3–36.
7. Ерофеев, В.Т. Аналитическое моделирование в электродинамике / В.Т. Ерофеев, И.С. Козловская. – Мн.: БГУ, 2010. – 303 с.
8. Князев, П.Н. Интегральные преобразования / П.Н. Князев. – Мн.: Высшая школа, 1969. – 198 с.
9. Ерофеев, В.Т. Дифракция плоской электромагнитной волны на плоском слое из биизотропного материала / В.Т. Ерофеев, С.В. Малый. – Вестник БГУ. Сер. 1. – 2010, № 2. – С. 11–16.
10. Баскаков, С.И. Радиотехнические цепи и сигналы / С.И. Баскаков. – М.: Высшая школа, 1988. – 448 с.

Abstract

The analytical solution of the boundary-value problem of penetration of a radioimpulse with finite spectrum through a flat biisotropic screen with arbitrary complex parameters of media is obtained. The impulse signal by means of atomic functions is presented. The results of computational experiment for concrete screen are investigated.

Поступила в редакцию 18.05.2013 г.

ОБ ОДНОМ ПОДХОДЕ К СТАТИСТИЧЕСКОМУ РАСПОЗНАВАНИЮ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

УДК 004.421.6: 519.237

В.Ю. Палуха, БГУ, Ю.С. Харин, НИИ ППМИ БГУ, г. Минск

Аннотация

Для решения задачи статистического распознавания криптографических генераторов по их выходным последовательностям разработан общий подход к построению информативных признаков. Описаны признаки на основе

энтропии и рангов матриц, построенные в соответствии с этим подходом. Приводятся результаты компьютерных экспериментов применения построенных информативных признаков для статистического распознавания прореживающего и самосжимающего генераторов.

Введение и постановка задачи

Современная криптография невозможна без случайных и псевдослучайных последовательностей $x_1, x_2, \dots \in V = \{0, 1\}$ [1]. Практическую значимость имеют генераторы последовательностей, близких по своим свойствам к равномерно распределенной случайной последовательности (РПСП). Гипотезу о том, что выходная последовательность генератора $\{x_i\}$ является равномерно распределенной, будем обозначать $H_* = \{\{x_i\} \text{ есть РПСП}\}$.

При проведении испытаний средств криптографической защиты информации [1] часто возникает задача статистического распознавания генераторов случайных и псевдослучайных последовательностей, т.е. задача отнесения (классификации) наблюдаемой выходной последовательности генератора $x_1, x_2, \dots \in V = \{0, 1\}$ некоторой конечной длительности T к одному из L ($2 \leq L < +\infty$) классов $\Omega_1, \dots, \Omega_L$. Генераторы могут быть разделены на классы $\{\Omega_i\}$ различными способами: физические и программные генераторы; программные генераторы различных типов; программные генераторы одного типа, но с различными параметрами; программные генераторы с одинаковыми параметрами, но с различной инициализирующей информацией. Описание основных типов генераторов можно найти в [1–3]. Данная статья посвящена задаче построения пространства информативных признаков для статистического распознавания криптографических генераторов.

Подход к построению информативных признаков генераторов

Будем предполагать, что выходная последовательность генератора $x_i \in V$ является случайной последовательностью на некотором вероятностном пространстве $(\Omega, \mathcal{C}, P)$. Разобьем последовательность $x_1, x_2, \dots, x_T$ на $l = \lfloor T/n \rfloor$ фрагментов (n -грамм) длины n $X^{(1)}, X^{(2)}, \dots, X^{(l)}, X^{(k)} = (x_{(k-1)n+1}, \dots, x_{kn}) \in V^n$. Пусть наблюдается некоторая статистика $a_k(n) = f(X^{(k)})$, $k = 1, 2, \dots, l$, при различных длинах фрагмента $n \in [n_-, n_+]$, $1 \leq n_- < n_+$; $a_*(n) = E_H \{a_k(n)\}$ – математическое ожидание этой статистики при истинной гипотезе H_* ; $a(n)$ – наблюдаемое выборочное среднее значение статистики: $a(n) = \frac{1}{l} \sum_{k=1}^l a_k(n)$. В качестве признака предлагается использовать отклонение статистики $a(n)$ от математического ожидания в l_p -метрике ($p \in N$):

$$\rho^{(p)} = \frac{1}{n_+ - n_- + 1} \sqrt[p]{\sum_{n=n_-}^{n_+} |a(n) - a_*(n)|^p}. \quad (1)$$

Нелинейные признаки на основе энтропии

Пусть $p_{i_1, \dots, i_n} = P\{x_{t+1} = i_1, \dots, x_{t+n} = i_n\}$ – распределение вероятностей n -граммы $(x_{t+1}, \dots, x_{t+n}) \in V_n$, которое предполагается не зависящим от $t \in \square$. Многомерная (n -мерная) энтропия Шеннона для фрагмента длины n равна [1]:

$$h(n) = - \sum_{i_1, \dots, i_n} p_{i_1, \dots, i_n} \ln p_{i_1, \dots, i_n}. \quad (2)$$

Теорема 1. Если справедлива гипотеза H_* , то

$$h_*(n) = h(n)|_{H_*} = n \ln 2 = nh_*(1). \quad (3)$$

Используя подстановочный принцип, построим оценку энтропии (2):

$$\hat{h}(n) = - \sum_{i_1, \dots, i_n} \hat{p}_{i_1, \dots, i_n} \ln \hat{p}_{i_1, \dots, i_n}. \quad (4)$$

На основании статистик $\{\hat{h}(n) : n_- \leq n \leq n_+\}$, вычисленных по (4), и математического ожидания (3) построим информативные признаки согласно (1):

$$\rho^{(p)} = \frac{1}{n_+ - n_- + 1} \sqrt[p]{\sum_{n=n_-}^{n_+} |\hat{h}(n) - h_*(n)|^p}. \quad (5)$$

Нелинейные признаки на основе рангов матриц

Разбиваем наблюдаемый ряд $x_1, x_2, \dots$ на фрагменты $X^{(1)}, X^{(2)}, \dots \in V^{n^2}$ длины n^2 : $X^{(k)} = (x_{(k-1)n^2+1}, \dots, x_{kn^2})$. Используя k -й фрагмент $X^{(k)} = (x_1^{(k)}, \dots, x_{n^2}^{(k)}) \in V^{n^2}$ выходной последовательности, построим $(n \times n)$ -матрицу

$$A^{(k)} = (a_{ij}^{(k)}) = \begin{pmatrix} x_1^{(k)} & \dots & x_n^{(k)} \\ \dots & \dots & \dots \\ x_{(n-1)n+1}^{(k)} & \dots & x_{nn}^{(k)} \end{pmatrix} \in V^{n \times n}. \quad (6)$$

Ранг этой матрицы отражает наличие функциональной зависимости в последовательности. Если $\text{rank}(A^{(k)}) = r < n$, то в матрице $A^{(k)}$ имеется $n - r$ линейно зависимых над V_n строк. Поэтому в качестве признака для фрагмента $X^{(k)}$ будем использовать ранг матрицы (6) $r^{(k)} = \text{rank}(A^{(k)}) \in \{0, 1, \dots, \min\{n, N\}\}$. Пусть наблюдается l фрагментов, т.е. $T = l \cdot N^2$. Определим статистику

$$v(n) = \frac{1}{nl} \sum_{k=1}^l r^{(k)}, \quad (7)$$

имеющую смысл среднего относительного ранга.

Теорема 2. При верной гипотезе H_* математическое ожидание статистики (7) имеет вид:

$$E_{H_*} \{v(n)\} = v_*(n) = \frac{1}{n} \sum_{j=0}^n q_{nj} j, \quad (8)$$

где $q_{nj} = P_{H_0} \{r^{(k)} = j\} = 2^{j(2n-j)-n^2} \prod_{i=0}^{j-1} \frac{(1-2^{i-n})^2}{1-2^{i-j}}$,

$$j \in \{0, 1, \dots, n\}.$$

На основании статистик $\{v(n) : n_- \leq n \leq n_+\}$ и математического ожидания (8) построим информативные признаки согласно (1):

$$\rho^{(p)} = \frac{1}{n_+ - n_- + 1} \sqrt[p]{\sum_{n=n_-}^{n_+} |v(n) - v_*(n)|^p}. \quad (9)$$

Решающее правило

Пусть указанными выше методами построено пространство из M информативных признаков $p = (p_1, \dots, p_M) \in \mathbf{R}^M$. Опишем применение метода дискриминантного анализа [4] для решения задачи распознавания в случае двух равновероятных классов. Пусть по входной последовательности построен вектор признаков p и имеется $m_i > M$

обучающих реализаций $\rho_1^{(i)}, \dots, \rho_{m_i}^{(i)} \in \mathbf{R}^M$, принадлежащих классу Ω_i , $i \in \{1, 2\}$. Построим оценки математического ожидания вектора признаков и ковариационной матрицы для каждого из классов. Оценка для математического ожидания в классе Ω_i есть выборочное среднее:

$$\hat{\mu}_i = \frac{1}{m_i} \sum_{m=1}^{m_i} \rho_m^{(i)}, \quad (10)$$

а оценка для ковариационной матрицы – выборочная ковариационная матрица:

$$\hat{\Sigma}_i = \frac{1}{m_i - 1} \sum_{m=1}^{m_i} (\rho_m^{(i)} - \hat{\mu}_i)(\rho_m^{(i)} - \hat{\mu}_i)'. \quad (11)$$

Байесовское решающее правило имеет вид [4]:

$$d = d_0(\rho) = \arg \min_{i \in \{1, 2\}} (\ln |\hat{\Sigma}_i| + (\rho - \hat{\mu}_i)' \hat{\Sigma}_i^{-1} (\rho - \hat{\mu}_i)), \quad \rho \in \square^M, \quad (12)$$

где оценки $\hat{\mu}_i$ и $\hat{\Sigma}_i$ вычисляются по формулам (10) и (11) соответственно.

Результаты компьютерных экспериментов

Проведены две серии компьютерных экспериментов.

Серия 1. Пусть Ω_1 и Ω_2 – самосжимающиеся генераторы с различными характеристическими примитивными многочленами порождающего регистра сдвига. Описание самосжимающегося генератора приведено в [5].

В качестве признака ρ используется значение статистики (5). Заданы параметры:

$n_- = 1$, $n_+ = 20$, $p = 1$. В результате применения решающего правила (12) получена оценка безусловной вероятности ошибки 0,22.

Серия 2. Пусть Ω_1 – прореживающий генератор, Ω_2 – самосжимающийся генератор. Описание прореживающего генератора приведено в [6].

В качестве признака ρ используется значение статистики (9). Заданы параметры

$n_- = 1$, $n_+ = 2236$, $p = 1$. Можно применить метод дискриминантного анализа, описанный выше. Однако можно применить более простое линейное решающее правило. Эксперимент дает оценку безусловной вероятности ошибки, равную 0.

Заключение

Для решения актуальной задачи распознавания криптографических генераторов разработан общий подход к построению информативных признаков. Этот подход учитывает динамику изменения вероятностных характеристик генераторов при изменении длины используемого фрагмента. Построенные согласно этому подходу признаки универсальны, т.к. не используют специфических свойств генераторов, и поэтому их можно применять для распознавания различных типов генераторов. Проиллюстрировано применение одного из признаков для распознавания прореживающего и самосжимающегося генераторов, и другого – для распознавания самосжимающихся генераторов с различными параметрами.

Литература:

1. Харин, Ю.С. Математические и компьютерные основы криптологии / Ю.С. Харин [и др.]. – Минск: Новое знание, 2003. – 382 с.

2. Харин, Ю.С. Проблемы математики и информатики в области защиты информации / Ю.С. Харин // Весці Нацыянальнай акадэміі навук Беларусі. Серыя фізіка-матэматычных навук. – 2007. – № 4. – С. 84–95.

3. Иванов, М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. – Москва: КУДИЦ-ОБРАЗ, 2003. – 240 с.

4. Харин, Ю.С. Математическая и прикладная статистика / Ю.С. Харин, Е.Е. Жук. – Минск: БГУ, 2004. – 272 с.

5. Meier, W. Analysis of pseudo random sequences generated by cellular automata / W. Meier, O. Staffelbach // D.W. Davies, editor, Advances in Cryptology / Eurocrypt '91, Springer-Verlag, Berlin, 1992. – P. 186 – 199.

6. Coppersmith, D. The shrinking generator / D. Coppersmith, Y. Krawchuk, Y. Mansour // Advanced in Cryptology: Proceedings of Crypto 93, LNCS 773. – 1994. – P. 22 – 39.

Abstract

An approach to construction of informative features is proposed to solve the problem of statistical recognition of cryptographic generators by output sequences. Features based on entropy and ranks of matrices and constructed in accordance to this approach are described. The results of computer experiments on recognition of shrinking and self-pressed generators are presented.

Поступила в редакцию 18.05.2013 г.



тел. +375 17 287 85 66
факс +375 17 287 85 65
тел. моб. +375 29 684 43 09
220068, г. Минск, ул. Некрасова, 114,
оф. 238, 2 этаж, e-mail: info@belplata.by

Разработка и поставка печатных плат:
любой класс точности, широкий спектр покрытий, изготовление образцов от 5 дней.

Поставка фотошаблонов

Поставка трафаретов:
из нержавеющей стали и латуни.

Материалы для печатных плат:
защитные маски, маркировочные краски, фоторезисты, паяльные пасты.

Поставка изделий из феррита:
любые виды сердечников CI, EE, EEM, EP, EER, ETD, EC, EF, ED, EFD, EI, EPO, EPX, EPC и т.д.

Поставка электронных компонентов:
STMicroelectronics, NXP Semiconductors, Vishay, Holtek Semiconductor.

www.belplata.by