Кобозева А.А. Учет свойств нормального спектрального разложения матрицы контейнера при обеспечении надежности восприятия стегосообщения / А.А.Кобозева, Е.А.Трифонова // Вестник НТУ «ХПИ». — 2007. — №18. — С.81—93.

Рецензент: Хорошко В.О.
Поступила 24.11.2011

УДК 621.391+519.2

Попов А.А.
Национал. унив. обороны Украины

ИНВАРИАНТЫ ГРУПП ОТОБРАЖЕНИЙ СЛУЧАЙНЫХ СИГНАЛОВ (СООБЩЕНИЙ) В ПРИЛОЖЕНИИ К СТАТИСТИЧЕСКОМУ АНАЛИЗУ КРИПТОАЛГОРИТМОВ

Разработка любого криптоалгоритма предусматривает оценку его стойкости к практически разнообразным попыткам криптоанализа. Как известно, далеко не все разрабатываемые криптографические средства обеспечивают обещанный уровень защиты [1]. Криптографические средства защиты информации характеризуются тем, что для них не существует простых и однозначных тестов, позволяющих убедиться в надежной защите информации. Задача определения эффективности криптографических средств и методов защиты зачастую более трудоемкая, чем их разработка. Анализ разработанного криптоалгоритма является новой, прежде всего научной, а не инженерной задачей.

Фундаментальное допущение криптоанализа, сформулированное А. Керкгоффом (Kerckhoffs A.) [2], состоит в том, что секретность сообщения полностью зависит от ключа, т.е. весь криптоалгоритм, кроме значения ключа, известен противнику. Если статистически выявляемые закономерности каким-либо образом проявляются в зашифрованном тексте, у криптоаналитиков появляется возможность определить ключ криптоалгоритма (его составляющие) либо же сузить множество вероятных ключей. К. Шенноном введено понятие идеального шифра [3], т.е., такого, который полностью устраняет в криптограмме все статистические закономерности открытого текста.

Метод *разностного анализа, описанный в работах* [4], [5] сочетает в себе обобщение идеи общей линейной структуры с применением вероятностно-статистических методов исследования. Однако разностный анализ основан на использовании неравновероятности в распределении значений разности двух криптограмм, полученных из пары открытых текстов, имеющих некоторую фиксированную разность, и если все возможные значения разностей двух криптограмм будут появляться с близкими (в идеале – с равными) вероятностями, то метод разностного анализа не сможет работать эффективно.

Подобно разностному анализу, линейный криптоанализ [6] является обобщенным методом, сочетающим в себе поиск линейных статистических аналогов для уравнений криптоалгоритмов, статистический анализ имеющихся открытых и зашифрованных текстов, использующий также методы согласования и перебора. Этот метод эксплуатирует статистические линейные соотношения между отдельными координатами векторов открытого текста, соответствующего шифртекста и ключа и использует эти соотношения для определения статистическими методами отдельных координат ключевого вектора. На сегодняшний день метод линейного криптоанализа позволил получить наиболее сильные результаты по раскрытию ряда итерационных систем блочного шифрования.

Одним из показателей надежности криптоалгоритма является неотличимость распределения криптограммы от равномерного. В работе [7] с помощью статистического теста [8], предназначеного для проверки гипотезы о том, что элементы выборки из некоторого алфавита имеют равномерное распределение, проведено исследование ряда блочных шифров, участвовавших в конкурсе на стандартизацию криптографических протоколов AES (Advanced Encryption Standard), организованного Национальным институтом стандартов и технологий США [9]. Однако данный метод требует сравнительно большого объема статистических данных. Кроме того, равномерность распределения исследуемой выборки не означает выполнения условия статистической независимости между элементами криптограммы и открытого сообщения, выполнения которого требует теорема 6 [3].

Целью статьи является получение инвариантов групп взаимнооднозначных отображений непрерывных и дискретных случайных сигналов (сообщений), позволяющих осуществлять статистический анализ криптоалгоритмов на предмет выполнения требований теоремы 6 [3].

В работах [10,11] были введены понятия нормированной функции статистической взаимосвязи (НФСВ) и взаимной НФСВ, которые характеризуют меру статистической взаимосвязи между двумя мгновенными значениями (отсчетами) случайных сигналов в различные, в общем случае, моменты времени. Эта мера основана на метрических соотношениях между отсчетами случайных сигналов и определяется метрикой между совместной и произведением одномерных плотностей распределения вероятностей отсчетов. Последнее обстоятельство иногда может затруднять получение точных значений НФСВ и взаимной НФСВ отсчетов. Между тем, достаточно часто в задачах статистического анализа требуется знать степень статистической взаимосвязи между парой мгновенных значений (отсчетов) двух разных случайных сигналов в два различных момента времени. Для нахождения такой характеристики пары отсчетов двух случайных сигналов будут полезны соображения, изложенные ниже.

Всякую пару случайных сигналов $\xi(t),\eta(t)$ можно рассматривать как частично упорядоченное множество $\mathbf{\Gamma}$, в котором в каждые два момента времени $t_j,t_k\in T$ между двумя мгновенными значениями (отсчетами) $\xi_j=\xi(t_j),\eta_k=\eta(t_k)$ сигналов $\xi(t),\eta(t)\in\mathbf{\Gamma}$ определено отношение порядка $\xi_j\le\eta_k$ (или $\xi_j\ge\eta_k$). Тогда частично упорядоченное множество $\mathbf{\Gamma}$ является решеткой с операциями верхней и нижней граней соответственно: $\xi_j\vee\eta_k=\sup_L\{\xi_j,\eta_k\}$, $\xi_j\wedge\eta_k=\inf_L\{\xi_j,\eta_k\}$ и если $\xi_j\le\eta_k$, то $\xi_j\wedge\eta_k=\xi_j$ и $\xi_j\vee\eta_k=\eta_k$ [12]:

$$\xi_t\le\eta_t\Leftrightarrow\begin{cases}\xi_j\wedge\eta_k=\xi_j;\\ \xi_j\vee\eta_k=\eta_k.\end{cases}$$

Итак, пусть ξ_j,η_k – мгновенные значения (отсчеты) $\xi_j=\xi(t_j),\eta_k=\eta(t_k)$ случайных сигналов $\xi(t),\eta(t)\in\mathbf{\Gamma}$ с совместными функцией распределения вероятностей (ФРВ) $F_{\xi\eta}(x,y)$, плотностью распределения вероятностей (ПРВ) $p_{\xi\eta}(x,y)$ и с симметричными одномерными ПРВ $p_\xi(x),p_\eta(y)$ вида: $p_\xi(x)=p_\xi(-x)$; $p_\eta(y)=p_\eta(-y)$.

Тогда всякой паре случайных сигналов $\xi(t),\eta(t)\in\mathbf{\Gamma}$ можно поставить в соответствие следующую нормированную меру между отсчетами ξ_j,η_k.

Определение 1. Нормированной мерой статистической взаимосвязи (НМСВ) между парой отсчетов ξ_j, η_k случайных сигналов $\xi(t), \eta(t) \in \Gamma$ будем называть величину $\mu(\xi_j, \eta_k)$, равную:

$$\mu(\xi_j, \eta_k) = 3 - 4\mathbf{P}[\xi_j \vee \eta_k \geq 0], \quad (1)$$

где $\mathbf{P}[\xi_j \vee \eta_k \geq 0]$ – вероятность того, что случайная величина $\xi_j \vee \eta_k$, равная верхней грани отсчетов ξ_j, η_k, принимает значения больше или равные нулю.

Теорема 1. НМСВ $\mu(\xi_j, \eta_k)$ определяется через совместную ФРВ $F_{\xi\eta}(x, y)$ отсчетов ξ_j, η_k:

$$\mu(\xi_j, \eta_k) = 3 - 4[1 - F_{\xi\eta}(0,0)]. \quad (2)$$

Доказательство. В соответствии с формулой [13;(3.2.85)] случайная величина $\xi_j \vee \eta_k$ характеризуется ФРВ $F_{\xi\vee\eta}(z)$, равной: $F_{\xi\vee\eta}(z) = F_{\xi\eta}(z, z)$. Поэтому вероятность $\mathbf{P}[\xi_j \vee \eta_k \geq 0]$ равна: $\mathbf{P}[\xi_j \vee \eta_k \geq 0] = 1 - F_{\xi\vee\eta}(0) = 1 - F_{\xi\eta}(0,0)$. □

Теорема 2. НМСВ $\mu(\xi_j, \eta_k)$ может быть определена через вероятность $\mathbf{P}[\xi_j \wedge \eta_k \leq 0]$:

$$\mu(\xi_j, \eta_k) = 3 - 4\mathbf{P}[\xi_t \wedge \eta_t \leq 0] = 3 - 4[1 - F_{\xi\eta}(0,0)],$$

где $\mathbf{P}[\xi_j \wedge \eta_k \leq 0]$ – вероятность того, что случайная величина $\xi_j \wedge \eta_k$, равная нижней грани отсчетов ξ_j, η_k принимает значения меньше или равные нулю.

Доказательство. В соответствии с формулой [13;(3.2.82)] случайная величина $\xi_j \wedge \eta_k$ характеризуется ФРВ $F_{\xi\wedge\eta}(z)$, равной: $F_{\xi\wedge\eta}(z) = F_{\xi}(z) + F_{\eta}(z) - F_{\xi\eta}(z, z)$, где $F_{\xi}(u), F_{\eta}(v)$ – одномерные ФРВ отсчетов ξ_j, η_k соответственно. Поэтому вероятность $\mathbf{P}[\xi_j \wedge \eta_k \leq 0]$ равна:

$$\mathbf{P}[\xi_j \wedge \eta_k \leq 0] = F_{\xi}(0) + F_{\eta}(0) - F_{\xi\eta}(0,0) = 1 - F_{\xi\eta}(0,0). \quad \square$$

Теорема 3. Для пары отсчетов ξ_j, η_k *случайных сигналов* $\xi(t), \eta(t)$, *которые аддитивно взаимодействуют между собой в частично упорядоченном множестве* Γ: $\chi_i = \xi_j + \eta_k$ ($\chi_i := \xi(t_j) + \eta(t_k)$), $t_i, t_j, t_k \in T$, НМСВ $\mu(\xi_j, \eta_k)$, $\mu(\xi_j, \chi_i)$, $\mu(\eta_k, \chi_i)$ соответствующих пар отсчетов ξ_j, η_k; ξ_j, χ_i; η_k, χ_i являются инвариантами группы H нечетных отображений $\{h_\alpha\}$, $h_\alpha \in H$, $\alpha \in A$ случайных сигналов:

$$h_\alpha : \xi(t) \to \xi'(t), \eta(t) \to \eta'(t), \; h_\alpha^{-1} : \xi'(t) \to \xi(t), \eta'(t) \to \eta(t); \quad (3)$$

$$\mu(\xi_j, \eta_k) = \mu(\xi'_j, \eta'_k); \quad (4а)$$

$$\mu(\xi_j, \chi_i) = \mu(\xi'_j, \chi'_i); \quad (4б)$$

$$\mu(\eta_k, \chi_i) = \mu(\eta'_k, \chi'_i), \quad (4в)$$

где $h_\alpha(-u) = -h_\alpha(u)$; ξ'_j, η'_k – отсчеты случайных сигналов $\xi'(t), \eta'(t)$, которые аддитивно взаимодействуют между собой в частично упорядоченном множестве Γ': $\chi'_i = \xi'_j + \eta'_k$ ($\chi'_i := \xi'(t_j) + \eta'(t_k)$); χ'_i – отсчет, равный сумме отсчетов ξ'_j, η'_k сигналов $\xi'(t), \eta'(t)$.

Доказательство. При взаимнооднозначном отображении h_α (3) выполняется свойство инвариантности дифференциала вероятности, следствием которого является тождество

между совместными ФРВ $F_{\xi\eta}(x,y)$, $F_{\xi'\eta'}(x',y')$ пар отсчетов ξ_j,η_k; ξ'_j,η'_k соответственно:

$$F_{\xi'\eta'}(x',y')=F_{\xi\eta}(x,y). \qquad (5)$$

В свою очередь, совместные ФРВ $F_{\xi\chi}(x,w)$, $F_{\eta\chi}(y,w)$ пар отсчетов ξ_j,χ_i; η_k,χ_i определяются через ФРВ $F_{\xi\eta}(x,y)$ следующим образом:

$$F_{\xi\chi}(x,w)=F_{\xi\eta}(x,w-x); \qquad (6а)$$

$$F_{\eta\chi}(y,w)=F_{\xi\eta}(y,w-y). \qquad (6б)$$

Совершенно аналогично, совместные ФРВ $F_{\xi'\chi'}(x',w')$, $F_{\eta'\chi'}(y',w')$ пар отсчетов ξ'_j,χ'_i; η'_k,χ'_i определяются через ФРВ $F_{\xi'\eta'}(x',y')$ следующим образом:

$$F_{\xi'\chi'}(x',w')=F_{\xi'\eta'}(x',w'-x'); \qquad (6в)$$

$$F_{\eta'\chi'}(y',w')=F_{\xi'\eta'}(y',w'-y'). \qquad (6г)$$

Из совместного выполнения соотношений (6в), (6а), (5) и (6г), (6б), (5) следуют тождества:

$$F_{\xi'\chi'}(x',w')=F_{\xi\chi}(x,w); \qquad (7а)$$

$$F_{\eta'\chi'}(y',w')=F_{\eta\chi}(y,w). \qquad (7б)$$

При *взаимнооднозначном нечетном* отображении h_α (3) нуль 0 частично упорядоченного множества $\mathbf{\Gamma}$ отображается в нуль $0'$ частично упорядоченного множества $\mathbf{\Gamma'}$ таким образом, что они тождественны: $h:0\to 0'$, $0\equiv 0'$, поэтому тождества (5), (7а), (7б) выполняются в точках $(x',y')=(x,y)=(0,0)$, $(x',w')=(x,w)=(0,0)$, $(y',w')=(y,w)=(0,0)$. Поэтому, с учетом равенства (2), из соотношений (5), (7а), (7б) следуют тождества (4а), (4б), (4в) соответственно. □

Теорема 4. Для гауссовских случайных сигналов $\xi(t),\eta(t)$ с коэффициентом корреляции $\rho_{\xi\eta}$ между отсчетами ξ_j,η_k, их НМСВ $\mu(\xi_j,\eta_k)$ равна:

$$\mu(\xi_j,\eta_k)=\frac{2}{\pi}\arcsin[\rho_{\xi\eta}]. \qquad (8)$$

Доказательство. Найдем выражение для совместной ФРВ $F_{\xi\eta}(x,y)$ сигналов $\xi(t),\eta(t)$ в точке $x=0,y=0$, которое в соответствии с формулой (12) приложения II работы [14] определяется через двойной интеграл $K_{00}(\alpha)$:

$$F_{\xi\eta}(0,0)=\left(\frac{\sqrt{1-\rho_{\xi\eta}^2}}{\pi}\right)K_{00}(\alpha),$$

где $\alpha=\pi-\arccos(\rho_{\xi\eta})$, $K_{00}(\alpha)=\alpha/(2\sin\alpha)$ (см. формулу (14) там же), $\sin\alpha=\sqrt{1-\rho_{\xi\eta}^2}$. Тогда, после выполнения необходимых преобразований, получим результирующее выражение для $F_{\xi\eta}(0,0)$:

$$F_{\xi\eta}(0,0)=\left(1+\frac{2}{\pi}\arcsin[\rho_{\xi\eta}]\right)/4.$$

Подставив последнее выражение в формулу (2), получим требуемое тождество (8). □

Теорема 5. Для пары отсчетов ξ_j, η_k гауссовских случайных сигналов $\xi(t), \eta(t)$, которые аддитивно взаимодействуют в частично упорядоченном множестве Γ: $\chi_i = \xi_j + \eta_k$ $(\chi(t_i) = \xi(t_j) + \eta(t_k))$, $t_i, t_j, t_k \in T$, справедливо следующее соотношение между НМСВ $\mu(\xi_j, \chi_i)$, $\mu(\eta_k, \chi_i)$, $\mu(\xi_j, \eta_k)$ соответствующих пар их отсчетов ξ_j, χ_i; η_k, χ_i; ξ_j, η_k:

$$\mu(\xi_j, \chi_i) + \mu(\eta_k, \chi_i) - \mu(\xi_j, \eta_k) = 1. \qquad (9)$$

Доказательство. Пусть $q^2 = D_\eta / D_\xi$ – соотношение дисперсий D_ξ, D_η, а $\rho_{\xi\eta}$ – коэффициент корреляции между отсчетами ξ_j, η_k гауссовских сигналов $\xi(t), \eta(t)$. Тогда коэффициенты корреляций $\rho_{\xi\chi}, \rho_{\eta\chi}$ пар отсчетов ξ_j, χ_i и η_k, χ_i соответственно равны:

$$\rho_{\xi\chi} = (1 + \rho_{\xi\eta} q) / \sqrt{1 + 2\rho_{\xi\eta} q + q^2},$$

$$\rho_{\eta\chi} = (q + \rho_{\xi\eta}) / \sqrt{1 + 2\rho_{\xi\eta} q + q^2}.$$

Для гауссовских случайных сигналов НМСВ определяется соотношением (8). Поэтому выполняется тождество:

$$\mu(\xi_j, \chi_i) + \mu(\eta_k, \chi_i) - \mu(\xi_j, \eta_k) =$$

$$= \frac{2}{\pi}\arcsin[\rho_{\xi\chi}] + \frac{2}{\pi}\arcsin[\rho_{\eta\chi}] - \frac{2}{\pi}\arcsin[\rho_{\xi\eta}]. \qquad (10)$$

Воспользовавшись соотношениями [15;(I.3.5)], несложно получить значение суммы первых двух слагаемых в правой части равенства (10):

$$\frac{2}{\pi}\arcsin[\rho_{\xi\chi}] + \frac{2}{\pi}\arcsin[\rho_{\eta\chi}] = \frac{2}{\pi}(\pi - \arcsin[c]) = \frac{2}{\pi}(\pi - \arcsin[\sqrt{1 - \rho_{\xi\eta}^2}]),$$

где $c = \rho_{\xi\chi}\sqrt{1 - \rho_{\eta\chi}^2} + \rho_{\eta\chi}\sqrt{1 - \rho_{\xi\chi}^2}$.

Подставив полученное значение суммы арксинусов в правую часть равенства (10), вычисляем значение суммы НМСВ пар отсчетов ξ_j, χ_i; η_k, χ_i; ξ_j, η_k:

$$\mu(\xi_j, \chi_i) + \mu(\eta_k, \chi_i) - \mu(\xi_j, \eta_k) = \frac{2}{\pi}(\pi - \arcsin[\sqrt{1 - \rho_{\xi\eta}^2}]) - \frac{2}{\pi}\arcsin[\rho_{\xi\eta}] = 1. \quad \square$$

Таким образом, теорема 5 устанавливает инвариантное соотношение для НМСВ (9) пар отсчетов ξ_j, χ_i; η_k, χ_i; ξ_j, η_k аддитивно взаимодействующих гауссовских случайных сигналов $\xi(t), \eta(t)$, причем данное тождество не зависит от их энергетических соотношений, несмотря на то, что НМСВ $\mu(\xi_j, \chi_i)$, $\mu(\eta_k, \chi_i)$ являются функциями от соотношения дисперсий D_ξ, D_η отсчетов ξ_j, η_k гауссовских сигналов $\xi(t), \eta(t)$.

Результат (9) теоремы 5 можно обобщить на аддитивно взаимодействующие отсчеты сигналов $\xi(t), \eta(t)$ с достаточно произвольными вероятностно-статистическими свойствами, разнообразие которых ограничено мощностью группы отображений $H = \{h_\alpha\}, \alpha \in A$, причем каждое отображение h_α обладает свойствами отображения (3). Требуемое обобщение обеспечивает следующая теорема.

Теорема 6. Для пары отсчетов ξ'_j, η'_k случайных сигналов $\xi'(t), \eta'(t)$, которые аддитивно взаимодействуют в частично упорядоченном множестве Γ': $\chi'_i = \xi'_j + \eta'_k$, $t_i, t_j, t_k \in T$, справедливо следующее соотношение между НМСВ $\mu(\xi'_j, \chi'_i)$, $\mu(\eta'_k, \chi'_i)$, $\mu(\xi'_j, \eta'_k)$ соответствующих пар их отсчетов ξ'_j, χ'_i; η'_k, χ'_i; ξ'_j, η'_k:

$$\mu(\xi'_j,\chi'_i)+\mu(\eta'_k,\chi'_i)-\mu(\xi'_j,\eta'_k)=1. \qquad (11)$$

Доказательство. Взаимнооднозначным отображением h_α (3), $h_\alpha \in H$ группы H может быть осуществлено отображение упорядоченного множества гауссовских случайных сигналов Γ в множество, в общем случае, негауссовских случайных сигналов Γ'. При этом, в соответствии с теоремой 3, справедливы тождества (4а), (4б), (4в), устанавливающие инвариантность НМСВ указанных пар отсчетов, таким образом, из тождества (29) следует справедливость тождества (11). □

Для частично упорядоченного множества Γ со свойствами решетки, в котором отсчеты ξ_j,η_k сигналов $\xi(t),\eta(t)$ взаимодействуют между собой: $\chi_i=\xi_j\vee\eta_k$ $(\chi(t_i)=\xi(t_j)\vee\eta(t_k))$, $\tilde{\chi}_i=\xi_j\wedge\eta_k$ $(\tilde{\chi}(t_i)=\xi(t_j)\wedge\eta(t_k))$, $t_i,t_j,t_k\in T$ в виде бинарных операций решетки $\vee,\wedge$, понятие нормированной меры статистической взаимосвязи между отсчетами ξ_j,η_k случайных сигналов $\xi(t),\eta(t)\in\Gamma$ нуждается в уточнении.

Определение 2. Нормированной мерой статистической взаимосвязи (НМСВ) между парами отсчетов ξ_j,χ_i; и $\xi_j,\tilde{\chi}_i$ случайных сигналов $\xi(t),\chi(t),\tilde{\chi}(t)\in\Gamma$ в частично упорядоченном множестве Γ со свойствами решетки будем называть величины $\mu(\xi_j,\chi_i)$, $\mu(\xi_j,\tilde{\chi}_i)$ равные соответственно:

$$\mu(\xi_j,\chi_i)=3-4\mathbf{P}[\xi_j\wedge\chi_i\le 0]; \qquad (12а)$$

$$\mu(\xi_j,\tilde{\chi}_i)=3-4\mathbf{P}[\xi_j\vee\tilde{\chi}_i\ge 0], \qquad (12б)$$

где $\mathbf{P}[\xi_j\wedge\chi_i\le 0]$, $\mathbf{P}[\xi_j\vee\tilde{\chi}_i\ge 0]$ – вероятности того, что случайные величины $\xi_j\wedge\chi_i/\xi_j\vee\tilde{\chi}_i$, равные нижней/верхней грани пар отсчетов $\xi_j,\chi_i/\xi_j,\tilde{\chi}_i$ принимают значения меньше/больше или равные нулю соответственно.

Теорема 7. Для пары отсчетов ξ_j,η_k случайных сигналов $\xi(t),\eta(t)$, которые взаимодействуют в частично упорядоченном множестве Γ со свойствами решетки: $\chi_i=\xi_j\vee\eta_k$ $(\chi(t_i)=\xi(t_j)\vee\eta(t_k))$, $\tilde{\chi}_i=\xi_j\wedge\eta_k$ $(\tilde{\chi}(t_i)=\xi(t_j)\wedge\eta(t_k))$, $t_i,t_j,t_k\in T$, справедливы следующие соотношения между НМСВ $\mu(\xi_j,\chi_i)$, $\mu(\eta_k,\chi_i)$; $\mu(\xi_j,\tilde{\chi}_i)$, $\mu(\eta_k,\tilde{\chi}_i)$ соответствующих пар их отсчетов ξ_j,χ_i; η_k,χ_i и $\xi_j,\tilde{\chi}_i$; $\eta_k,\tilde{\chi}_i$:

$$\begin{cases}\mu(\xi_j,\chi_i)=1;\\ \mu(\eta_k,\chi_i)=1;\end{cases} \qquad (13а)$$

$$\begin{cases}\mu(\xi_j,\tilde{\chi}_i)=1;\\ \mu(\eta_k,\tilde{\chi}_i)=1.\end{cases} \qquad (13б)$$

Доказательство. В соответствии с аксиомой поглощения решетки справедливы тождества:

$$\xi_j\wedge\chi_i=\xi_j\wedge(\xi_j\vee\eta_i)=\xi_j; \qquad (14а)$$

$$\eta_k\wedge\chi_i=\eta_k\wedge(\xi_j\vee\eta_k)=\eta_k; \qquad (14б)$$

$$\xi_j\vee\tilde{\chi}_i=\xi_j\vee(\xi_j\wedge\eta_k)=\xi_j; \qquad (14в)$$

$$\eta_k\vee\tilde{\chi}_i=\eta_k\vee(\xi_j\wedge\eta_k)=\eta_k. \qquad (14г)$$

Подставляя результаты (14а,б), (14в,г) в формулы (12а), (12б) соответственно, с учетом симметричности одномерных ПРВ $p_\xi(x)$, $p_\eta(y)$ отсчетов ξ_j, η_k, вероятности в (12а), (12б) будут определяться одномерными ФРВ $F_\xi(x),F_\eta(y)$ при $x=y=0$:

$$\begin{cases} \mathbf{P}[\xi_j \wedge \chi_i \le 0] = F_\xi(0) = 1/2; \\ \mathbf{P}[\eta_k \wedge \chi_i \le 0] = F_\eta(0) = 1/2; \end{cases} \quad (15а)$$

$$\begin{cases} \mathbf{P}[\xi_j \vee \tilde{\chi}_i \ge 0] = F_\xi(0) = 1/2; \\ \mathbf{P}[\eta_k \vee \tilde{\chi}_i \ge 0] = F_\eta(0) = 1/2. \end{cases} \quad (15б)$$

Подставляя результаты (15а), (15б) в формулы (12а), (12б) соответственно, получим тождества (13а), (13б). □

Таким образом, теорема 7 определяет инвариантные соотношения для НМСВ пар отсчетов ξ_j, χ_i; η_k, χ_i и $\xi_j, \tilde{\chi}_i$; $\eta_k, \tilde{\chi}_i$ случайных сигналов $\xi(t), \eta(t)$, которые взаимодействуют в частично упорядоченном множестве Γ со свойствами решетки: $\chi_i = \xi_j \vee \eta_k$ $(\chi(t_i) = \xi(t_j) \vee \eta(t_k))$, $\tilde{\chi}_i = \xi_j \wedge \eta_k$ $(\tilde{\chi}(t_i) = \xi(t_j) \wedge \eta(t_k))$, $t_i, t_j, t_k \in T$, причем полные тождества не зависят от вероятностных распределений взаимодействующих сигналов и их энергетических соотношений.

Выводы. 1. Теоремы 3,5,6.7 устанавливают инварианты групп отображений случайных сигналов, основанных на вероятностных характеристиках результатов взаимодействия произвольной пары мгновенных значений (отсчетов) сигналов в частично упорядоченном множестве.

2. Полученные инвариантные соотношения между элементами сигналов в ряде случаев могут существенно упростить статистический анализ исследуемых случайных сигналов, и, в частности, разрабатываемых криптоалгоритмов, путем определения степени статистической зависимости между элементами криптограмм и соответствующих открытых сообщений (текстов).

3. Рассмотренные инвариантные соотношения могут успешно применяться для статистического анализа как дискретных, так и непрерывных случайных сигналов.

Литература

1. *Ferguson N., Schneier B., Kohno T. Cryptography Engineering: Design Principles and Practical Applications, John Wiley & Sons, 2010.*
2. *Kerckhoffs A. La cryptographie militaire // Journal des sciences militaires. 1883, vol. IX. pp. 5–38.*
3. *Shannon C.E. Communication Theory of Secrecy Systems// Bell System Technical Journal. 1949, 28 - pp.656–715.*
4. *Murphy S. The cryptanalysis of FEAL-4 with 20 chosen plaintexts // Journal of Cryptology, 1990, v. 3, № 2. pp. 145–154.*
5. *Biham E., Shamir A. Differential Cryptanalysis of DES-like cryptosystems // Journal of Cryptology. 1991. V.4. No. 1. pp. 3–72.*
6. *Matsui M., Yamagishi A. A new method for known plaintext attack of FEAL cipher // In Proceedings of Advances in Cryptology - EUROCRYPT'92. Lect. Notes in Comp. Sci. Berlin: Springler-Verlag. 1992, V. 658. pp. 1–91.*
7. *Пестунов А.И. Статистический анализ современных блочных шифров// Вычислительные технологии. ИВТ СО РАН, Новосибирск. Т. 12, № 2, 2007 с. 122–129.*
8. *Рябко Б.Я., Пестунов А.И. "Стопка книг" как новый статистический тест для случайных чисел // Проблемы передачи информации. 2004, Т. 40, вып. 1. с. 73–78.*
9. *Advanced Encryption Algorithm Development Effort // http://www.csrc.nist.gov/encryption/aes 1997–2000.*
10. *Попов А.А. Вероятностно-статистические и информационные характеристики случайных сигналов, инвариантные относительно группы взаимнооднозначных функциональных преобразований// Вісник Державного університету інформаційно-комунікаційних технологій.-2007.-5, №1.-С. 51-62.*

11. Попов А.А. Информационные соотношения между элементами пространства сигналов, построенного на обобщенной булевой алгебре с мерой// Вісник Державного університету інформаційно-комунікаційних технологій.-2007.-5, №2.-С. 175-184.
12. Биркгоф Г. Теория решеток. М.: Наука, 1984. — 568 с.
13. Тихонов В.И. Статистическая радиотехника. М.: Радио и связь, 1982. – 624 с.
14. Левин Б.Р. Теоретические основы статистической радиотехники. В 3-х т. Т.1. М.: Сов. радио, 1969. – 752 с.
15. Прудников А.П., Брычков Ю.А., Маричев О.И. Интегралы и ряды. В 3-х т. Т.1. Элементарные функции. М.: ФИЗМАТЛИТ, 2002. – 632 с.

Рецензент: Скрипник Л.В.
Поступила 12.12.2011

УДК 519.254

Борода А.В.
ГУИКТ

ПРИНЦИПЫ ПОСТРОЕНИЯ ПОТОЧНЫХ ШИФРСИСТЕМ И ПОДХОДЫ К ОЦЕНКЕ ИХ СТОЙКОСТИ

Современная шифрсистема (далее – ШС) представляет собой электронное устройство, которое осуществляет шифрование (расшифрование) информации и реализует криптопротокол согласования ключей криптографических алгоритмов приемной и передающей стороны. Для обеспечения достаточной гибкости в плане возможности изменения криптографических параметров, при технической реализации шифрсистем широко используется комбинация soft- и hardware технологий, предусматривающая выполнение части криптографического алгоритма аппаратным способом, а часть программными средствами. Обычно аппаратным способом реализуется *основа* криптографического алгоритма, то есть та часть, которая непосредственно производит шифрование и расшифрование данных, а предварительное преобразование ключевой информации при формировании *рабочего ключа* криптоалгоритма перед началом шифрования (расшифрования) выполняется программно.

Элементами *рабочего ключа* являются переменные параметры криптографического алгоритма, которые зависят от *ключевой установки* шифрсистемы. Ими могут быть переменные коммутаторы и подстановки, двоичные функции, таблицы замены, начальные заполнения регистров генератора гаммы и т.д. Под *ключевой установкой* обычно понимается совокупность *секретного ключа* и *разового ключа* шифрования (последний передается в открытом виде).

Шифрсистема является *поточной*, если она последовательно преобразует символы открытого текста в символы шифртекста с помощью шифра замены, который зависит от ключа и от внутреннего состояния шифрсистемы (номера такта шифрования). При работе поточной шифрсистемы для каждого шифруемого знака необходимо указать соответствующий ему шифр замены. Поэтому в конструкции поточных шифрсистем обычно выделяют два основных узла. Первый из них осуществляет выбор шифрующего преобразования, а второй выполняет собственно шифрование очередного знака открытого текста. Первый узел вырабатывает последовательность номеров шифрующих преобразований, то есть управляет порядком процедуры шифрования. Вырабатываемую им управляющую последовательность, представляющую собой номера используемых преобразований, обычно называют *управляющей гаммой* или *гаммой шифрования* (run keys), а сам этот узел – *генератором гаммы* (Run Key Generator). Второй узел, в