

Оператор  $H$  самосопряженный. Непрерывный спектр оператора  $H$  занимает полуось  $[0, \infty)$ . Для доказательства существования собственного значения оператора  $H$  достаточно показать [5], что существует элемент  $Z(z)$ , для которого отношение Рэлея

$$\frac{(Z', Z')_{L_2} - \mu_n((q-1)Z, Z)_{L_2}}{(qZ, Z)_{L_2}} < 0.$$

В качестве функции  $Z$  возьмем  $\eta(\alpha z)$ , где  $\eta(z) \in C^\infty$ ,  $0 \leq \eta(z) \leq 1$ :

$$\eta(z) = \begin{cases} 1, & |z| < 1, \\ 0, & |z| > 2. \end{cases}$$

При достаточно большом  $\alpha$  имеет место неравенство

$$\left( \eta'(\alpha z), \eta'(\alpha z) \right)_{L_2} - \mu_n \left( (q-1)\eta(\alpha z), \eta(\alpha z) \right)_{L_2} < 0. \quad (3)$$

Действительно,

$$\left( (q-1)\eta, \eta \right)_{L_2} = \int_{z_1}^{z_2} (q-1) dz > 0$$

при достаточно большом  $\alpha$ . Первое слагаемое в неравенстве (3) стремится к нулю:

$$\left( \eta'(\alpha z), \eta'(\alpha z) \right)_{L_2} = \alpha \int_{-2}^2 (\eta'(v))^2 dv \rightarrow 0, \quad \alpha \rightarrow 0.$$

Таким образом, существует бесконечное множество решений задачи (1), имеющих вид  $Z_n(z)\psi_n(x, y)$ .

#### Литература

1. Exner P., Seba P. // J. Math. Phys. 1989. **30**. P. 2574.
2. Bulla W., Gesztesy F., Renger W., Simon B. // Proc. AMS. 1997. **125**, No. 5. P. 1487.
3. Evans D.V., Levitin M., Vassiliev D. // J. Fluid Mech. 1994. **261**. P. 21-31.
4. Делицын А.Л. // ЖВМ и МФ. 2000. №4 (в печати).
5. Рид А., Саймон Б. Методы современной математической физики. М.: Мир, 1982.

Поступила в редакцию  
29.12.00

РАДИОФИЗИКА

УДК 621.391

## О ГЕНЕРАЦИИ НЕПРЕРЫВНЫХ КЛЮЧЕВЫХ ПОТОКОВ В СИММЕТРИЧНЫХ СИСТЕМАХ КРИПТОГРАФИЧЕСКОЙ СВЯЗИ

Н. В. Евдокимов, В. П. Комолов, П. В. Комолов, А. А. Руденко

(кафедра радиофизики)

E-mail: ne@nist.fss.ru

**Рассмотрена возможность формирования непрерывных ключевых потоков в симметричных криптосистемах с помощью использования интерференции радиоколечаний с иррационально-связанными частотами. Такие системы могут иметь скрытые параметры и «реакцию на подслушивание».**

При передаче сообщений с помощью криптографической связи потоковое шифрование обеспечивает наибольшую рабочую криптостойкость в случае непрерывных ключевых потоков с пуассоновским распределением. Это эквивалентно однократному использованию ключа (так же как ключа Вернама), что позволяет решить основные проблемы криптографии, относящиеся к передаче и хранению секретного ключа [1]. Естественно, что в таких системах ключевые потоки связанных абонентов должны быть когерентны. Решение этой проблемы возможно с помощью четырехлучевой интерференции радиосигналов, имеющих близкие иррационально-связанные частоты [2].

Несоизмеримость частот иррационально-связанных колебаний означает отсутствие у них общих резонансов. Поэтому их интерференция приводит к детерминированному динамическому хаосу. При ограничении амплитуды колебаний и регулярных выборках их знаковых корреляций такой динамический хаос представляет собой случайную битовую последовательность нулей и единиц, т.е. двоичное иррациональное число. Подобные хаотические последовательности могут быть когерентны в двух пространственно разнесенных точках радиоприема при следующих условиях: 1) в каждой точке прием и задержка колебаний проводятся с частотным разделением, 2) после задержки когерентные

колебания в этих точках синфазны, 3) выборки знаковой корреляции колебаний с несоизмеримыми частотами выполняются в этих точках синхронно, с частотой  $\Omega_s$ , не превышающей разностной частоты этих колебаний.

На рис. 1, а приведена классическая схема симметричной криптосистемы с передачей секретного ключа абонентам А и В по закрытому каналу связи. На рис. 1, б и в изображены схемы с когерентными ключевыми потоками  $Z_A$  и  $Z_B$ , создаваемыми связанными абонентами А и В из радиосигналов с несоизмеримыми частотами.

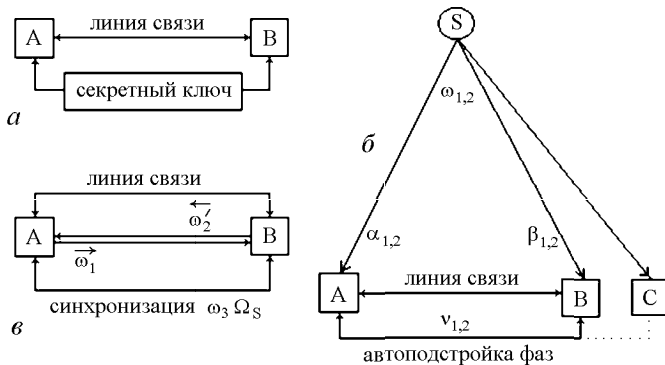


Рис. 1. Симметричные криптосистемы: а — классическая система с передачей секретного ключа по закрытому каналу связи; б, в — схемы формирования непрерывных ключевых потоков в симметричных криптосистемах

В схеме на рис. 1, б радиосигналы передаются с искусственного спутника Земли (S) службы единого времени и могут использоваться неограниченным числом абонентов. Любая пара связанных абонентов работает как двухканальный четырехлучевой интерферометр. Каждый абонент имеет двухканальный приемник для раздельного приема сигналов с несоизмеримыми частотами  $\omega_1$  и  $\omega_2$  и двухканальную систему фазовой автоподстройки этих сигналов с аналогичными сигналами, принятыми связанным с ним абонентом [3]. В общем случае такие интерферометры имеют разные базы (расстояния между абонентами) с неопределенным отклонением от равносигнального направления на передатчик S. Поэтому сигналы, принимаемые абонентами, имеют разные задержки. В криптосистеме А–В приемники абонента А принимают сигналы, пропорциональные  $\cos(\omega_1 t + \alpha_1)$  и  $\cos(\omega_2 t + \alpha_2)$ , а приемники абонента В — сигналы, пропорциональные  $\cos(\omega_1 t + \beta_1)$  и  $\cos(\omega_2 t + \beta_2)$ . Задержка сигналов с частотами  $\omega_1$  и  $\omega_2$  в контурах фазовой автоподстройки абонентов А и В одинакова и равна соответственно  $2\nu_1$  и  $2\nu_2$ . После автоподстройки фаз сигналы с когерентными частотами у абонентов А и В синфазны и пропорциональны  $\cos(\omega_1 t + 2\nu_1)$  для частоты  $\omega_1$  и  $\cos(\omega_2 t + 2\nu_2)$  для частоты  $\omega_2$ . Знаковые корреляции таких сигналов и их синхронные выборки с частотой  $\Omega_s$  дают когерентные ключевые потоки для шифрования и расшифровки передаваемых и принимаемых сообщений. Задержки  $\nu_1$  и  $\nu_2$  являются скрытыми

параметрами криптосистемы А–В. Свойства детерминированного хаоса (см., напр., [4]) обеспечивают некоррелированность ключевых потоков разных криптосистем.

На рис. 1, в показана схема формирования непрерывных ключевых потоков, рассчитанная на связь только двух абонентов, имеющих собственные невырожденные параметрические генераторы с синхронизированной накачкой и узкополосные приемники. В этой схеме абонент А передает абоненту В непрерывный сигнал на одной из частот генерации, например  $\omega_1$  (близкой к частоте  $\omega'_1$  абонента В), а сигнал на второй частоте  $\omega_2$  оставляет у себя в качестве скрытого опорного параметра для сравнения его фазы с фазой сигнала, принимаемого им от абонента В на частоте  $\omega'_2$  (близкой к частоте  $\omega_2$ ). При синхронных выборках знаковой корреляции фаз у каждого абонента формируются пуассоновские ключевые потоки, которые когерентны, поскольку у каждого невырожденного генератора фазы сигналов антикоррелированы [5]. Так, в двухконтурном генераторе А в соответствии с соотношением Менли–Роу частоты колебаний связаны с частотой накачки  $\omega_3$  соотношением  $\omega_1 + \omega_2 = \omega_3$ . Так же связаны и их фазы  $\varphi_1$  и  $\varphi_2$ , которые относительно фазы накачки  $\varphi_3$  в невырожденном режиме являются антикоррелированными функциями времени:  $\varphi_1(t) + \varphi_2(t) = \varphi_3(t) \equiv 0$ ;  $\varphi_1(t) = -\varphi_2(t)$ . При общей накачке генераторы А и В генерируют колебания с разными несоизмеримыми частотами: генератор А — колебания с частотами  $\omega_1, \omega_2$ , а генератор В — колебания с частотами  $\omega'_1, \omega'_2$ . Суммы фаз каждой пары колебаний равны фазе общей накачки, и если она синфазна, то  $\varphi_1(t) + \varphi_2(t) = \varphi'_1(t) + \varphi'_2(t)$ . Поэтому в синхронные моменты времени разности фаз близких частот разных генераторов ( $\omega_1, \omega'_1$ ) и ( $\omega_2, \omega'_2$ ) также антикоррелированы. Один из таких моментов ( $t_1$ ) стохастического фазового синхронизма для колебаний двух генераторов с синфазной накачкой показан на рис. 2, где  $\varphi_1(t) - \varphi'_1(t) = \Delta\varphi_1(t) = \varphi_2(t) - \varphi'_2(t) = -\Delta\varphi_2(t)$ .

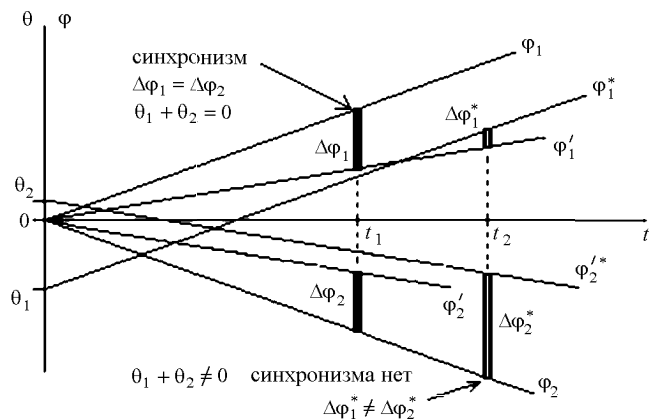


Рис. 2. Стохастический фазовый синхронизм в связанных невырожденных двухконтурных параметрических генераторах

При этом синхронная знаковая корреляция колебаний с частотами  $(\omega_1, \omega'_1)$  и  $(\omega_2, \omega'_2)$  дает когерентные отсчеты (когерентные ключевые потоки).

В схеме на рис. 1, *в* обмен сигналами вносит задержки и сдвиги фаз  $\theta_1$  и  $\theta_2$  в разности фаз  $\Delta\varphi_1(t)$  и  $\Delta\varphi_2(t)$ , по которым абоненты формируют последовательности  $Z_A$  и  $Z_B$ . В работе [6] было показано, что в зависимости от суммарного сдвига фаз  $0 \leq (\theta_1 + \theta_2) \leq \pi$  корреляция последовательностей меняется от полной до нулевой при  $(\theta_1 + \theta_2) = \pi/2$  и далее до антикорреляции при  $(\theta_1 + \theta_2) = \pi$ . На рис. 2 показан также результат синхронных выборок корреляции между опорными фазами и фазами  $\varphi_1^*$  и  $\varphi_2^*$  принятых сигналов, сдвинутых на углы  $\theta_1$  и  $\theta_2$  при их передаче от одного абонента к другому. Момент выборки  $t_2$  выбран отличным от  $t_1$  для наглядности результата:  $\Delta\varphi_1^*(t) = \varphi_1^*(t) - \varphi'_1(t) \neq |\Delta\varphi_2^*(t)| = |\varphi_2(t) - \varphi_2^*(t)|$ , т. е. различие в задержке сигналов разрушает когерентность ключевых потоков. Поэтому для управления корреляцией должна быть предусмотрена компенсация фазового сдвига  $(\theta_1 + \theta_2)$ . Этот сдвиг устраняется путем задержки опорного сигнала со стороны любого абонента с помощью фазовой автоподстройки по максимальной корреляции контрольных криптограмм, т. е. согласно принятому протоколу криптографической связи [1]. Управление корреляцией ключевых потоков в одной из таких криптосистем рассмотрено в работе [7].

Рабочая криптостойкость рассмотренных схем обеспечивается скрытыми параметрами. В схеме, показанной на рис. 1, *в*, помимо скрытых опорных частот скрытыми могут быть также частота и фаза накачки параметрических генераторов, задержка сигналов при их передаче, тактовая частота и, наконец, секретные ключи (в том числе и алгоритмические), которые можно использовать для дополнительного шифрования потоков. Классические криптосистемы, естественно, не могут обладать такой же реакцией на подслушивание, какой обладают квантовые криптосистемы, однако наличие у них скрытых параметров может придать им подобное свойство. Прослушивание сигналов без знания скрытых параметров не дает криптоаналитику С (третий «абонент» на рис. 1, *б*) доступа к информации, которой обмениваются абоненты А и В. При активном участии «абонента» С в фазовой автоподстройке криптосистем, показанных на рис. 1, *б* и *в*, абоненты А и В, сравнивая результаты передачи по секретному и открытому каналам, имеют возможность обнаружить потерю прямой синхронизации друг с другом из-за навязывания им фазы «абонента» С и тем самым установить факт подслушивания передачи информации.

В эксперименте для генерации иррационально-связанных радиокосильаний использовались невырожденные двухконтурные емкостные парамет-

рические генераторы с частотой накачки 3 МГц и частотами генерации  $\sim 1.2$  и  $\sim 1.8$  МГц. Колебания пропускались через узкополосные фильтры, соответствующие этим частотам, и формировались в меандры в отдельных делителях частоты. Заметим, что деление частот не разрушает их иррациональной связи, что может быть широко использовано при реализации рассмотренных схем. Знаковая корреляция сигналов проводилась в фазовых компараторах типа XOR [8]. На выходе XOR формировались последовательности длиной до  $10^4$  бит при частотах выборок  $\Omega_s$  до 30 кГц. Хаотические свойства последовательностей определялись функциями автокорреляции, которые имели единственный пик с отношением к пьедесталу порядка  $10^2$  и соответствовали контрольной функции автокорреляции клипированного шумового сигнала генератора Г2-37.

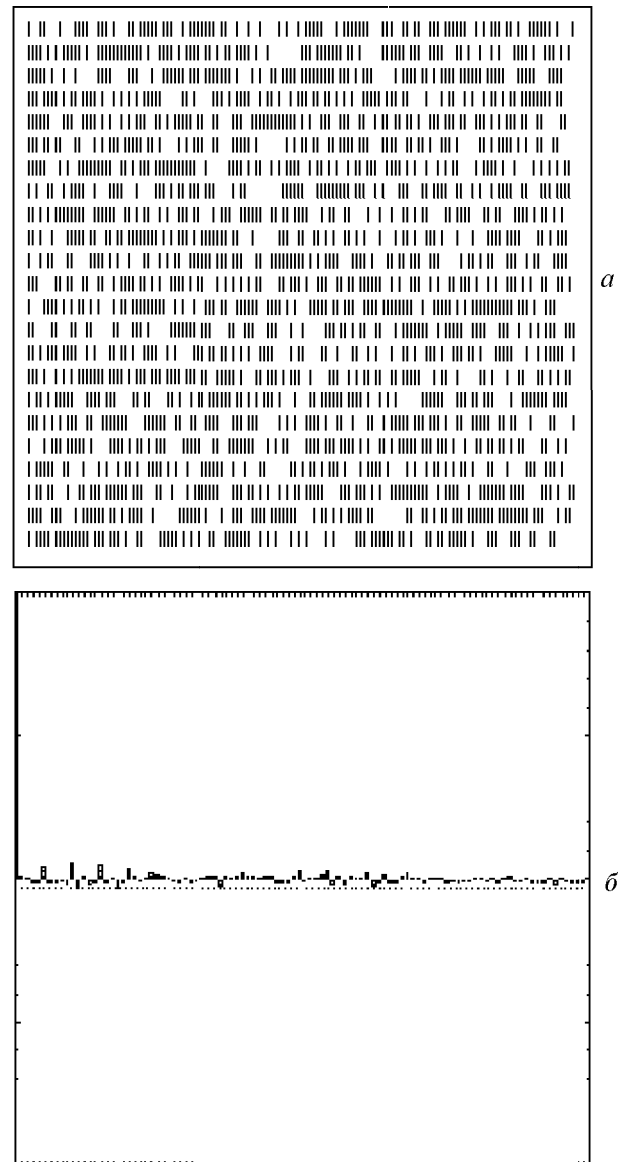


Рис. 3. Экспериментальный ключевой поток (фрагмент) — *а* и его функция автокорреляции — *б*; нули и единицы заменены пробелами и штрихами соответственно

Взаимная корреляция синхронных последовательностей при  $\Delta\varphi_1(t_1) = \Delta\varphi_2(t_1)$  составляла 95%. На рис. 3 показан фрагмент формируемых потоков (а) и соответствующая ему функция автокорреляции (б). Фрактальная случайность потоков, типичная для динамического хаоса, инвариантна к частоте выборки  $\Omega_s$ .

**Литература**

1. Месси Д.Л. // ТИИЭР. 1988. **76**, № 5. С. 24.
2. Евдокимов Н.В., Комолов В.П. // Вестн. Моск. ун-та. Физ. Астрон. 2000. № 5. С. 57 (Moscow University Phys. Bull. 2000. No. 5. P. 68).

3. Мартынов Е.М. Синхронизация в системах передачи дискретных сообщений. М.: Связь, 1972.
4. Шустер Г. Детерминированный хаос. М.: Мир, 1988.
5. Каплан А.Е., Кравцов Ю.А., Рылов В.А. Параметрические генераторы и делители частоты. М.: Сов. радио, 1966.
6. Евдокимов Н.В., Клышко Д.Н., Комолов В.П., Ярочкин В.А. // УФН. 1996. **166**, № 1. С. 91.
7. Евдокимов Н.В., Клышко Д.Н., Комолов В.П., Ярочкин В.А. Описание к патенту RU 2117402 С1. 1998.
8. Шило В.Л. Популярныe цифровые микросхемы. М.: Радио и связь, 1989.

Поступила в редакцию  
20.11.00

ФИЗИКА ТВЕРДОГО ТЕЛА

УДК 539.1

**ОСОБЕННОСТИ СТАТИЧЕСКИХ СМЕЩЕНИЙ ВОКРУГ ОДИНОЧНЫХ ПРИМЕСНЫХ АТОМОВ В ОЦК РЕШЕТКЕ**

**В. М. Силонов, И. В. Харламова, А. Ю. Гениев**

(кафедра физики твердого тела)

E-mail: silonov\_v@mail.ru

**Для ОЦК структуры в микроскопическом приближении выявлена нехаотичность в расположении векторов смещений атомов матрицы вокруг одиночных примесных атомов замещения.**

В работе [1] были предприняты попытки расчета полей статических смещений вокруг точечных дефектов в ГЦК структуре. При этом рассматривались лишь дефекты в твердом аргоне. В работах [2–4] в рамках макроскопической теории проводились расчеты статических смещений вдали от дефектов. В настоящей работе рассчитаны поля статических смещений в ОЦК металлах вблизи одиночной примеси замещения в рамках модели Борна–Бегби с целью выявления их возможных особенностей в ОЦК структуре.

В рамках метода флуктуационных волн [5] при внесении одного дефекта в кристалл его атомы смещаются из узлов идеальной периодической решетки на величину

$$\delta\mathbf{R}_s(\mathbf{r}) = \frac{1}{N} \sum_{\mathbf{k}} \mathbf{A}_{\mathbf{k}} \sin \mathbf{k}\mathbf{r}, \quad (1)$$

где  $\mathbf{k}$  — волновой вектор волны смещений,  $\mathbf{R}_s$  — вектор  $s$ -го узла идеальной решетки кристалла,  $N$  — число точек суммирования в зоне Бриллюэна. Амплитуды волн статических смещений  $\mathbf{A}_{\mathbf{k}}$  могут быть найдены в результате решения системы линейных уравнений

$$D_{\mathbf{k}ij} \mathbf{A}_{\mathbf{k}j} = \mathbf{P}_{\mathbf{k}i} \quad (i = 1, 2, 3). \quad (2)$$

Конкретные выражения для динамических матриц  $D_{\mathbf{k}ij}$  и квазиупругих сил были получены в модели Борна–Бегби [6, 7].

Расчеты полей статических смещений проводились для одиночных примесей атома алюминия в решетке железа. Были выбраны следующие параметры:

$$a_{\text{Fe}} = 2.866 \text{ \AA}, \quad c_{11} = 2.43 \cdot 10^{12}, \quad c_{12} = 1.38 \cdot 10^{12},$$

$$c_{44} = 1.22 \cdot 10^{12} \text{ дин/см}^2, \quad \frac{1}{V} \frac{\partial V}{\partial c} = 0.3,$$

где  $a$  — параметр решетки,  $V$  — объем элементарной ячейки,  $c$  — концентрация второго компонента,  $c_{ij}$  — упругие постоянные.

Правильность использованного в работе выражения для динамической матрицы проверялась с помощью расчетов фононных спектров  $\nu(\mathbf{k})$ . Рассчитанные и экспериментальные значения [8] удовлетворительно соответствовали друг другу. При вычислении величины  $\delta\mathbf{R}_s$  суммирование проводилось по неприводимой части зоны Бриллюэна с увеличением числа точек суммирования до достижения сходимости результатов.

Результаты расчета статических смещений при замещении какого-либо атома железа атомом примеси большего радиуса (Al) приведены на рисунке.