Таблица 1: Теоретическое распределение p-значений в зависимости от длины последовательности n для теста монобит

Интервал	Frequency test		
	$n = 192$	$n = 512$	$n = 1024$
[0.0,0.1)	0.096683	0.101917	0.097623
[0.1,0.2)	0.123088	0.098008	0.102459
[0.2,0.3)	0.059210	0.109480	0.102339
[0.3,0.4)	0.148373	0.091700	0.096399
[0.4,0.5)	0.088755	0.106320	0.112863
[0.5,0.6)	0.097438	0.119488	0.083584
[0.6,0.7)	0.104772	0.063943	0.089312
[0.7,0.8)	0.110345	0.134285	0.093956
[0.8,0.9)	0.113829	0.069399	0.097311
[0.9,1.0)	0.057507	0.105460	0.124154

ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ ПЛЕНОЧНЫМИ ЭКРАНЫМИ ОТ ВОЗДЕЙСТВИЯ УЗКИХ ПУЧКОВ ЭЛЕКТРОМАГНИТНЫХ ВОЛН

Ерофеенко В.Т.

Белгосуниверситет, НИИ прикладных проблем математики и информатики
Независимости 4, 220030 Минск, Беларусь bsu_erofeenko@tut.by

Введение. Разработана методика аналитического моделирования побочных электромагнитных излучений (ПЭМИ) в виде узких пучков монохроматических электромагнитных волн $\vec{E}_{\text{уз.п.}}, \vec{H}_{\text{уз.п.}}$, обобщающих гауссовы пучки волн [1]. Используются другие типы пучков волн [2]. Решена краевая задача экранирования узких пучков электромагнитных волн плоским экраном из магнитодиэлектрических материалов в случае ортогонального распространения пучка к экрану.

Краевая задача. При заданном первичном монохроматическом электромагнитном поле $\vec{E}_{\text{уз.п.}}, \vec{H}_{\text{уз.п.}}$ требуется определить поле $\vec{E}_2, \vec{H}_2$, прошедшее в область $D_2(z > \Delta)$ за экраном $D(0 < z < \Delta)$ и поле $\vec{E}_1', \vec{H}_1'$, отраженное от экрана в области $D_1(z < 0)$. Выполнены уравнения

$$\text{rot}\vec{E} = i\omega\mu\vec{H},\ \text{rot}\vec{H} = -i\omega\varepsilon\vec{E},\ \text{в } D, \tag{1}$$

$$\text{rot}\vec{E}_j = i\omega\mu_0\vec{H}_j,\ \text{rot}\vec{H}_j = -i\omega\varepsilon_0\vec{E}_j,\ \text{в } D_j, \tag{2}$$

где $\vec{E}_1 = \vec{E}_{\text{уз.п.}} + \vec{E}_1'$ — суммарное поле в области D_1; граничные условия на плоскостях экрана $\Gamma_1(z = 0)$, $\Gamma_2(z = 0)$

$$\left(\vec{E}_{1\tau} - \vec{E}_\tau\right)\Big|_{\Gamma_1} = 0, \left(\vec{H}_{1\tau} - \vec{H}_\tau\right)\Big|_{\Gamma_1} = 0, \left(\vec{E}_{2\tau} - \vec{E}_\tau\right)\Big|_{\Gamma_2} = 0, \left(\vec{H}_{2\tau} - \vec{H}_\tau\right)\Big|_{\Gamma_2} = 0, \tag{3}$$

и условия излучения на бесконечности в областях D_j.

Для аналитического решения задачи (1)–(3) используются двухсторонние граничные условия, связывающие электромагнитные поля по обе стороны экрана D. Поле пучка излучается плоскостью $\Gamma(z = -h)$, на которой сформировано касательное электрическое поле, сконцентрированное в окрестности точки $(0, 0, -h)$:

$$\vec{E}\Big|_{z=-h} = (f_1(\rho)\vec{e}_\rho + f_2(\rho)\vec{e}_\varphi)\,\Phi_m,$$

где $\Phi_m = \exp(im\varphi), m = 1, 2, ...,$ $f_1(\rho) = E_1 \left(\frac{\rho}{h}\right)^{m-1} e^{-\alpha\rho^n}$, $f_2(\rho) = E_2 \left(\frac{\rho}{h}\right)^{m-1} e^{-\alpha\rho^n}$, $0 \le \rho < \infty$, $\alpha = \frac{\alpha_0}{h^n}, \alpha_0 > 0$, E_1, E_2 — const, $n = 2, 3, \ldots$; при $n = 2$ образуется гауссов пучок волн, при $n = 3, 4$ плоскостью излучаются узкие пучки волн; α_0, n, m — параметры узких пучков волн.

Литература

1. Ерофеенко В.Т. *Краевая задача дифракции пучков электромагнитных волн на плоском экране из биизотропных материалов* // Известия НАН Беларуси. Сер. физ.-мат. наук. 2012. № 4. С. 72–79.

2. Ерофеенко В.Т., Бондаренко В.Ф. *Преобразование пучков электромагнитных волн при прохождении через экран из кирального метаматериала* // Информатика. 2013. № 1. С. 5–17.

СВОЙСТВА RSA-КРИПТОСИСТЕМЫ В АБСТРАКТНЫХ ЧИСЛОВЫХ КОЛЬЦАХ

Кондратёнок Н.В.[1]

[1]БГУ, ФПМИ, пр. Независимости, 4, Минск, Беларусь
nkondr2006@rambler.ru

Пусть R — абстрактное числовое кольцо [1]. Тогда для любого максимального идеала $\mathfrak{m}$ выполнено неравенство $|R/\mathfrak{m}| < \infty$. Нормой идеала $\mathfrak{m}$ назовем мощность этого множества и обозначим $\mathcal{N}(\mathfrak{m}) = |R/\mathfrak{m}|$.

Алгоритм генерации ключей для аналога RSA-криптосистемы в абстрактных числовых кольцах выглядит следующим образом. Выбираются два различных максимальных идеала $\mathfrak{p}, \mathfrak{q} \subset R$. Вычисляется их произведение $\mathfrak{N} = \mathfrak{pq}$, которое называется модулем RSA-криптосистемы. Затем вычисляется значение функции Эйлера $\varphi(\mathfrak{N}) = (\mathcal{N}(\mathfrak{p}) - 1)(\mathcal{N}(\mathfrak{q}) - 1)$. Выбирается целое число $e \in [1, \varphi(\mathfrak{N})]$, взаимнопростое с $\varphi(\mathfrak{N})$, и вычисляется такое число $d \in [1, \varphi(\mathfrak{N})]$, что $ed \equiv 1 (\mathrm{mod}\ \varphi(\mathfrak{N}))$.

Пара $(\mathfrak{N}, e)$ называется публичным ключом RSA-криптосистемы и публикуется. Пара $(\mathfrak{N}, d)$ называется приватным ключом RSA-криптосистемы и должна оставаться в тайне.

Сообщениями являются элементы фактор-группы $R/\mathfrak{N}$. Функция шифрования $f : R/\mathfrak{N} \to R/\mathfrak{N}$ задается следующим образом: $f(x) \equiv x^e (\mathrm{mod}\ \mathfrak{N})$. Функция расшифрования $f^{-1} : R/\mathfrak{N} \to R/\mathfrak{N}$ задается следующим образом: $f^{-1}(x) \equiv x^d (\mathrm{mod}\ \mathfrak{N})$. Корректность описанной криптосистемы вытекает из аналога теоремы Эйлера.

Следующая теорема является аналогом теоремы Винера о малой секретной экспоненте [2].

Теорема 1. *Пусть $\mathfrak{N} = \mathfrak{pq}$ — модуль RSA-криптосистемы в абстрактном числовом кольце R, а $(\mathfrak{N}, e), (\mathfrak{N}, d)$ публичный и приватный ключи соответственно. Пусть выполнено*

$$\mathcal{N}(\mathfrak{q}) < \mathcal{N}(\mathfrak{p}) < \alpha^2 \mathcal{N}(\mathfrak{q}),$$

где $\alpha > 1$, а так же

$$d < \frac{1}{\sqrt{2\alpha + 2}} (\mathcal{N}(\mathfrak{N}))^{1/4}.$$

Тогда d можно эффективно вычислить за полиномиальное относительно $\log \mathcal{N}(\mathfrak{N})$ число бинарных операций.

Методом повторного шифрования [2] называется метод взлома RSA-криптосистемы, при котором для получения исходного сообщения применяют следующую процедуру. Предположим, что $y = x^e (\mathrm{mod}\ \mathfrak{N})$ — некоторое зашифрованое сообщение. Вычисляем значения элементов последовательности $y_i = y^{e^i} (\mathrm{mod}\ \mathfrak{N})$, $i = 1, 2, \ldots$, пока не получим $y_m = y$. Тогда $y_{m-1} = x$.