2. Абловиц, М. Солитоны и метод обратной задачи / М. Абловиц, Х. Сигур – М.: Мир, 1987. – 479 с.
3. Кудрявцев, А.Е. О солитоноподобных решениях для скалярного поля Хиггса / А.Е. Кудрявцев // Письма в ЖЭТФ – 1975. – Т. 22, вып. 3. – С. 178-181.
4. Гетманов. Б.С. Связанные состояния солитонов в моделях теории поля ϕ_2^4 / Б.С. Гетманов // Письма в ЖЭТФ – 1976. – Т. 24, вып. 5. – С. 323-327.
5. Segur, H. Nonexistence of small-amplitude breather solutions in ϕ^4 theory / H. Segur, M.D. Kruskal // Phys. Rev. Lett. – 1987 – V. 58, № 8. – P. 747-750.
6. Лидский, Б.В. Периодические решения уравнения $u_{tt} - u_{xx} + u^3 = 0$ / Б.В. Лидский, Е.И. Шульман // Функциональный анализ и его приложения – 1988 – Т. 22. Вып. 4. – С. 88-89.
7. Rice, M.J. Charge П-phase kinks in lightly doped polyacetilene / M.J. Rice // Phys. Lett. A. – 1979 – V. 71, № 1. – P. 152-154.
8. Segur, H. Wobbling kink in ϕ^4 and sine-Gordon theory / H. Segur // J. of Math. Physics – 1983. – V. 24, № 6. – P. 1439-1443.

УДК 512.624.95:378.147.091.3

КРИПТОГРАФИЧЕСКАЯ СТОЙКОСТЬ КРИПТОСИСТЕМЫ РАБИНА

Крупенкова Т.Г.[1], Липницкий В.А.[2]

[1]Белорусский национальный технический университет, Минск, Республика Беларусь

[2]Военная академия Республики Беларусь, Минск, Республика Беларусь

Криптосистема Рабина явилась результатом переосмысления криптосистемы RSA. Рабин М. заинтересовался вопросом выбора ключа e в криптосистеме RSA. Там e всегда взаимно просто с $\varphi(n)$ и, в частности, всегда нечётно. А что произойдёт, если взять чётным? Да, а если возьмём наипростейший случай $e = 2$? В результате подробного рассмотрения неожиданно и появилась рассматриваемая здесь криптосистема Рабина.

Пусть p и q – два различных простых числа. Пусть $N = pq$. Зафиксируем число B, $0 \le B < N$. Пара $\{N, B\}$ есть пара открытых ключей криптосистемы Рабина. Сообщение C рассматривается как элемент кольца Z/NZ и шифруется формулой: $m = c(c + B)(\mathrm{mod} N)$. Ясно, что такой способ шифрования реализуется гораздо быстрее, чем в криптосистеме RSA.

Расшифровка здесь представляет гораздо более сложную процедуру даже для законного получателя криптотекста. Фактически, сообщение C есть один из корней квадратного уравнения $x^2 + Bx - m = 0$ в кольце Z/NZ. В этом кольце 2, очевидно, является обратимым элементом. Поэтому для решения данного квадратного уравнения вполне пригодны стандартные формулы: $x = \left(\sqrt{\frac{B^2}{4} + m} - \frac{B}{2}\right)\ (\mathrm{mod}\, N)$. Разумеется, деление на 2 здесь реализуется умножением на $2^{-1} \in Z/NZ^*$. Сложность этих вычислений в том, что из каждого квадрата в данном кольце Z/NZ извлекаются 4 различных корня.

Другая проблема – как найти быстро квадратные корни из данного элемента кольца Z/NZ – в общем случае остаётся открытой. Существенно облегчает её решение знание делителей числа N. Тогда можно воспользоваться китайской теоремой об остатках и формулой Гарнера. Поэтому сложность взлома криптосистемы Рабина такая же, как и криптосистемы RSA.

Если разложение $n = p \cdot q$ в произведение простых множителей p и q известно, то легко находится CRT-представление дискриминанта: $D \leftrightarrow (D_p, D_q)$. Квадратный корень из D извлекается в Z/nZ, тогда и только тогда, когда D принадлежит подгруппе квадратов Z/nZ^{*2} в группе Z/nZ^*. А это возможно тогда и только тогда, когда $D_p \in Z/pZ^{*2}$ и $D_q \in Z/qZ^{*2}$. Проверить это, а заодно и найти корни можно, в принципе, прямым перебором: вычисляем по модулю p последовательно 2^2, 3^2, и так далее, пока не найдём эмпирически $u \le (p\ \ 1)$, такое, что $u^2(\mathrm{mod} p) \equiv D_p$. Аналогично поступаем с D_q.

В трёх из четырёх случаев теория чисел даёт прямые формулы для квадратных корней из нечётных простых чисел, то есть решает проблему поиска квадратных корней.

Следует напомнить, что для всех простых p кольцо Z/pZ является полем. Классическая теория полиномов справедлива для всех полей. В частности, имеет место однозначность разложения всякого полинома в произведение неприводимых полиномов-сомножителей. Отсюда следует, что каждый полином степени $n \ge 1$ с коэффициентами из Z/pZ имеет не более n корней. В частности, полином $x^2 - \overline{1}$ имеет в точности два корня: $\overline{1}$ и $\overline{-1}$.

Проблема поиска квадратных корней остаётся открытой для полей Z/pZ с нечётными простыми $p \equiv 1(\mathrm{mod} 8)$. В этом случае прямых формул не существует, но есть вполне детерминированный процесс нахождения квадратных корней. Здесь $p - 1 = 2^e \cdot q$, где $e \ge 3$, q – нечётное число. Циклическая группа Z/pZ^* содержит единственную циклическую подгруппу G порядка 2^e. Пусть f – квадратичный невычет по модулю p из множества

$\{1, 2, \ldots, p-1\}$. Тогда $f^q \equiv g(\mathrm{mod}\,p)$ для некоторого $g \in \{1, 2, \ldots, p-1\}$. При этом $g \in G$ и одновременно остаётся квадратичным невычетом. Отсюда следует, что g является примитивным элементом группы G (предположение о не примитивности сразу же приводит к заключению, что g – квадратичный вычет).

При $p \equiv 1(\mathrm{mod}\,8)$ и 2 и –1 являются квадратичными вычетами. Но с вероятностью 1/2 можно наудачу достаточно быстро найти в поле Z/pZ квадратичный невычет, то есть элемент $f \in \{1, 2, \ldots, p-1\}$, удовлетворяющий соотношению $f^{(p-1)/2} \equiv -1(\mathrm{mod}\,p)$. После этого несложно найти образующую g подгруппы G по формуле: $f^q \equiv g(\mathrm{mod}\,p)$.

Перед нами стоит задача нахождения квадратного корня из конкретного числа $z \in \{1, 2, \ldots, p-1\}$ в поле Z/pZ с нечётными простыми $p \equiv 1(\mathrm{mod}\,8)$. Конечно, $\bar{z} \in Z/pZ^{*2}$. Иными словами, $z^{(p-1)/2} = (z^q)^{2^{e-1}} \equiv 1(\mathrm{mod}\,p)$.

Следовательно, $(z^q)\mathrm{mod}\,p = y$ принадлежит циклической группе G = <g>, порождённой элементом g, и является квадратичным вычетом.

Поэтому y не является образующей группы G. Найдётся чётное число k, $0 \le k \le 2^e$, такое, что $\bar{g}^k = \bar{y}^{-1}$. Тогда $z^q \cdot g^k \equiv 1(\mathrm{mod}\,p)$, а следовательно, $z^{q+1} \cdot g^k \equiv z(\mathrm{mod}\,p)$. Очевидно, $\bar{u}_1 = \bar{z}^{(q+1)/2} \cdot \bar{g}^{k/2}$ является квадратным корнем из $\bar{z}$ в поле Z/pZ. Прямой переборный метод элементов Z/pZ и вычисления их квадратов до получения $\bar{z}$ мы заменили двумя переборными процедурами – поиск квадратичного невычета $f \in \{1, 2, \ldots, p-1\}$ и поиск чётной степени k элемента $\bar{g} = \bar{f}^q$, равной $\bar{y}^{-1}$. Эти процедуры предполагаются быть достаточно короткими.

Литература

1. Венбо Мао. Современная криптография. Теория и практика: пер. с англ. – Издательство М.: Вильямс, 2005 – 768 с.
2. Липницкий В.А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа. – Мн.: БГУИР, 2006. – 88 с.
3. Крупенкова Т.Г. Криптографические средства зашиты информации: в 2 ч. – Электрон. дан. БНТУ, 2012. – Ч.1: учебно-методическое пособие.

УДК 681.2.082:621.3

ВЛИЯНИЕ ПРОЦЕССА ИМПУЛЬСНОГО НАГРЕВА НА ГАЗОВУЮ ЧУВСТВИТЕЛЬНОСТЬ ПОЛУПРОВОДНИКОВЫХ ДВУХСЕНСОРНЫХ МИКРОСИСТЕМ

Реутская О.Г.
Белорусский национальный технический университет, Минск, Республика Беларусь

В современной газовой сенсорике особое внимание уделяется вопросам повышения газовой чувствительности, снижения энергопотребления, упрощения технологий изготовления, уменьшения стоимости изделий без изменения газочувствительных качеств датчиков и систем.

В данной работе проведено исследование газочувствительных свойств двухсенсорной газовой микросистемы, описанной в работе [1] в различных режимах работы.

Режим постоянного нагрева заключается в подключении сенсоров микросистемы к источникам постоянного питания в выбранном режиме.

Экспериментально было установлено, что при использовании постоянного нагрева на сенсорах микросистемы наблюдается «дрейф» значений сопротивлений. Например, при токе 51 мА и мощности 83,4 мВт при постоянном нагреве в течение 8 ч изменение сопротивления на одном из сенсоров составило 0,89 кОм.

Для того, чтобы физико-химические процессы протекали на поверхности чувствительного слоя достаточно быстро, обеспечивая быстродействие на уровне нескольких секунд, сенсор периодически необходимо разогревать до температуры 450 – 500°С [2]. В результате характеристики сенсора способны восстанавливаться до исходного состояния. В период отжига происходит активное освобождение поверхностных слоев полупроводника от сорбированных «отравляющих» газовых компонент [3].

Целью данной работы являлось исследование эффективности режима импульсного нагрева для мультисенсорной микросистемы, состоящей из двух сенсоров на подложке из наноструктурированного оксида алюминия, по сравнению с режимом постоянного нагрева. Важной особенностью является сохранение параметров микросистемы в результате воздействия серии импульсных нагревов на конструкцию и газочувствительные слои, и обеспечение ее работоспособность на протяжении длительного периода времени.

В качестве чувствительных слоев были выбраны SnO_2+Pt+Pd для первого сенсора микросистемы, и In_2O_3+Al_2O_3+Pt – для второго. При формировании газочувствительных слоем применялась методика капельного послойного нанесения выбранных составов с промежуточными кратковременными отжигами. Подготовка к измерению газовой