кими многозарядными примесями. Особенности лазерной плазмы, в первую очередь, определяются высокой скоростью ввода энергии излучения в вещество. При плотности потока излучения $>10^9$ Вт/см^2 происходит бесфракционное испарение вещества и его лавинная ионизация со степенью близкой к 100 % вне зависимости от теплофизических свойств облучаемого вещества.

Расчеты показывают, что в случае мишени из меди или цинка количество ионов в ядре плазмы может достигать величины 10^{16}-10^{17} ионов в зависимости от энергии лазерного излучения и размера пятна фокусировки. В течение времени выращивания эпитаксиального слоя можно создать необходимое число ионов многозарядной примеси для легирования эпитаксиальной структуры в процессе роста. При формировании плазмы лазерным излучением снимается ограничение на величину электрической проводимости мишени, и, следовательно, существенно расширяется перечень материалов, доступных в технологии легирования структур ФЭПП многозарядными примесями, формирующих несколько глубоких энергетических уровней в запрещенной зоне Кроме того, воздействие лазерной плазмы на поверхность материалов мишени позволяет осуществить плазмохимический синтез легирующих соединений.

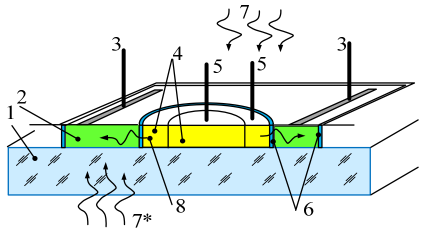
Данный способ лазерного легирования многозарядными примесями реализован в экспериментальной технологической установке, в которой использовался лазер с длиной волны излучения 1,064 мкм и частотой повторения импульсов в многомодовом режиме 12, 25 или 50 Гц. Оптическая система технологического реактора включает линзу (фокусное расстояние 10 см), полупрозрачное (10 %) зеркало для выделения части излучения и измеритель мощности лазерного излучения

При выращивании эпитаксиальных структур кремния перед входом в реактор эпитаксиального наращивания смешиваются четыре потока:

- водород H_2,
- $H_2 + SiCl_4$,
- H_2 + мелкая легирующая примесь,
- H_2 + многозарядная примесь.

Легирующая смесь с многозарядной примесью создается в реакционной камере путем воздействия излучения лазера на мишень, содержащую легирующий элемент (медь или цинк), при продувке зоны реакции водородом.

В хлоридном процессе эпитаксии при использовании мишеней из меди или цинка, облучаемых лазером, сформированы эпитаксиальные структуры кремния легированные цинком и фосфором, а также медью и фосфором, с концентрацией многозарядной примеси в диапазоне 10^{13}-2×10^{14} см$^{-3}$. Затем на их основе созданы фоторезистивные структуры ФЭПП с собственной фотопроводимостью, в которых за счет введения глубокой многозарядной примеси удалось расширить динамический диапазон энергетической характеристики ФЭПП и реализовать переключение характеристики спектральной чувствительности (со сдвигом «красной границы» на 2-4 мкм) под воздействием дополнительного оптического излучения.



1 – сапфировая подложка, 2 – фоторезистивный ФЭПП на основе полупроводника с глубокой многозарядной примесью, 3 – выводы ФЭП, 4 – управляющий *p-n* светодиод, 5 – выводы светодиода, 6 – слои изолирующего диэлектрика, 7 – входной оптический сигнал, 8 – управляющее излучение
Рисунок 1 – Структура управляемого ФЭПП на сапфировой подложке

Отметим, что предложенная технология формирования полупроводниковых структур с низкой концентрацией примеси хорошо совмещается с «около кремниевыми» технологиями и структурами *Si*, *Si:Ge* – A^3B^5 на сапфире. Одна из таких возможных совмещенных структур приведена на рисунке 1. Области 4 полупроводника типа A^3B^5 формируют управляющий светодиод, а область 2 представляет управляемый многофункциональный ФЭПП. Рядом могут быть расположены элементы усилителей или коммутирующих, часто выполняемых по КМОП-технологии, устройств. Многофункциональные одноэлементные ФЭПП на основе полупроводников с собственной проводимостью позволяют реализовать в одном измерительном преобразователе одновременное определение нескольких параметров оптического излучения, например, длины волны и мощности оптического излучения.

УДК 512.624.95:378.147.091.3

ЗАДАЧА ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ В КРИПТОГРАФИИ И ЕЕ МОДИФИКАЦИИ

Крупенкова Т.Г.[1], Липницкий В.А.[2]

[1]Белорусский национальный технический университет, Минск, Республика Беларусь
Военная академия Республики Беларусь, Минск, Республика Беларусь

Современная криптография своё рождение отсчитывает с 1976 года – с момента выхода в свет знаменитой статьи У. Диффи и М. Хелмана [1]. Основные идеи этой работы были революционными, крайне актуальными и своевременными в вопросах защиты информации. А именно, возможность открытого обмена ключами, построение криптографических систем на основе односторонних функций, применение в криптосистемах открытых ключей, идея цифровой подписи электронных документов. Авторы предложили двух кандидатов на роль односторонних функций: факторизация натурального числа на большие простые множители и задачу дискретного логарифма. Последняя заключается в решении уравнения

$$b^x = a \tag{1}$$

в поле классов вычетов $GF(p)$ для больших p.

Обе односторонние функции нашли широчайшее применение в современной криптографии, как в алгоритмах защиты информации, так и в протоколах цифровой подписи. Задача дискретного логарифмирования оказалась весьма эффективной в реализации (см. криптосистема Эль Гамаля [2] и многие национальные стандарты шифрования на её основе) и крайне неудобной и вязкой для прямого переборного взлома. Активная исследовательская работа привела к открытию, переоткрытию и/или нахождению в старых секретных лабораториях различных подходов к проблеме дискретного логарифма: метода «baby step giant step» [2] и его модификации [3], метода НСПХ или метода Нечаева-Силвера-Полига-Хелмана [4], а по сути, метода разложения абелевой конечной группы в прямое произведение циклических подгрупп примарных порядков, метода Шнорра. Эти методы приучили разработчиков к осторожному формированию криптосистем на основе данной задачи, к выбору p с обязательным большим простым делителем q числа p–1.

Наиболее осторожные и радикальные специалисты-криптографы стали предлагать отказаться от уже ставшей слишком популярной криптосистемы Эль Гамаля и ее вариаций. Но на смену пришли криптосистемы с той же задачей дискретного логарифма, но в другой оболочке – в других группах. Так, эллиптическая криптография базируется на абелевой группе точек эллиптической кривой относительно алгебраической операции сложения этих точек. Так как здесь операция аддитивная, вместо возведения в степень в уравнении (1) осуществляется многократное сложение точки с собою. Доказано, что криптографическая стойкость аддитивной задачи не уступает стойкости задачи дискретного логарифма из уравнения (1) [5].

XTR-криптосистема была впервые предложена в 2000 году на ежегодной международной научной конференции "Crypto-2000" авторами – Ленстрой А.К. и Верхейлом Э.Р. Название XTR явилось удачной аббревиатурой английского словосочетания "Efficient and Compact Subgroup Trace Representation". XTR-криптография основывается на вычислениях в конечных полях, а точнее, на взаимоотношениях в башне расширений конечных полей $GF(p)\subset GF(p^2)\subset GF(p^6)$ и вычислениях в полях $GF(p^2)$ с большими простыми p [6].

Идея Шнорра К. П. применяется и в XTR-криптографии. Здесь q достаточно большой (максимально большой) простой делитель порядка p^2-p+1 подгруппы мультипликативной группы $GF(p^6)^*$. Шифрование-дешифрование базируется здесь на вычислении следов из поля $GF(p^6)$ в поле $GF(p)$, аналогичным задаче дискретного логарифма. Эти вычисления искусно реализуются на нижних этажах приведенной выше башни расширений полей Галуа, а вязкость этих вычислений и служит гарантом криптостойкости XTR-криптосистемы. В [7] строго доказано, что криптографическая стойкость XTR-криптосистемы не уступает стойкости криптосистем на эллиптических кривых. Здесь же приводится обобщение данной криптосистемы на алгебраические торы.

Теоретики разрабатывают и некоммутативный аналог задачи дискретного логарифмирования. Здесь предполагается, что информация будет представлена элементами некоторой некоммутативной группы G, а шифрование реали-зуется традиционно умножением на специальный элемент $b\in G$. При этом элемент b получается кратным сопряжением, то есть многократным преобразованием вида:

$$f(x)=axa^{-1} \tag{2}$$

некоторого открытого ключа $x\in G$.

Предлагаем в качестве группы G взять мультипликативную группу H^* тела или алгебры с делением классических вещественных кватернионов: $H=\{h=x+yi+zj+tk\,|\,x,y,z,t\in R\}$ [8]. Здесь $i^2=j^2=k^2=-1$; $ij=k=-ji$; $jk=i=-kj$; $ki=j=-ik$. Для сопряжённого кватерниона $\bar{h}=x-yi-zj-tk$ норма $N(h)=h\bar{h}=x^2+y^2+z^2+t^2\in R^2$ – является положительным вещественным числом, если $h\neq 0$. Поэтому $h^{-1}=\dfrac{\bar{h}}{N(h)}$ и преобразование $f(x)=axa^{-1}$ легко реализуется.

Информационный вектор можно задавать в виде кватерниона из четырех целочисленных частей конечной конкретной разрядности: $\bar{i}=a+bi+cj+dk$. Для секретных ключей $a\in H,\ n,l\in Z$ преобразуем открытый ключ $x\in H^*$ по формуле (2) n – кратно в открытый ключ $c\in H$, который в свою очередь кратно l по формуле (2) преобразуем в сеансовый ключ $b\in H$. Шифрованное сообщение – кватернион $d=b\cdot\bar{i}$.

Приемной стороне все секретные ключи известны и расшифровать сообщение не составит труда. Конечно, возможны варианты с сеансовым ключом, подобные стандартной криптосистеме Эль Гамаля. Хакеру для взлома данной криптосистемы придется найти n из соотношения: $f^n(x)=c$, что представляется сложной задачей.

Литература

1. Diffie W. and Hellman M.E. New Direction in Criptography. // IEEE Trans. Inf. Theory, vol. IT-22, Nev. 1976. – P. 644 – 654.

2. Смарт Н. Криптография. – М.: Техносфера, 2005. – 528 с.

3. Липницкий В.А., Крупенкова Т.Г. Трехразрядный вариант алгоритма “baby-step giant-step” в проблеме дискретного логарифмирования. // Материалы МНТС «Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных». – Мн.: БГУИР, 2015. – С. 56 – 60.

4. Pohlig S.C. and Hellman M.E. An Improved Algorithm for Computing Logarithms Over $GF(p)$ and its Cryptographic Significance. // IEEE Trans. Inf. Theory, 1978. – Vol. 1, no 24. – P. 106 – 110.

5. Болотов А.А., Гашков С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. – М.: КомКнига, 2006. – 280 с.

6. Лидл Р., Нидеррайтер Г. Конечные поля. В 2-х т. Пер. с англ. – М.: Мир, 1988. – 822 с.

7. Rubin Karl., Silverberg Alice. Algebraic tory in cryptography. // CRYPTO 2003. / Lecture Notes in Computer Science, vol. 2442. Springer-Verlag. 2003. - P. 1–11.

8. Пирс Р. Ассоциативные алгебры. – М.: Мир, 1986. – 524 с.

УДК 519.6

НЕАДДИТИВНАЯ МЕРА

Романчак В.М.

Белорусский национальный технический университет, Минск, Республика Беларусь

Введение. В настоящее время величину определяют как “свойство материального объекта или явления, общее в качественном отношении для класса объектов или явлений, но в количественном отношении индивидуальное для каждого из них ”. А под измерением понимают “процесс экспериментального получения одного или более значений величины, которые могут быть обоснованно приписаны величине”. Эксперимент можно проводить с помощью объективных средств измерения или на основании субъективного мнения компетентного лица, которого мы будем называть экспертом. Поэтому будем считать, что измерение величины, в зависимости от метода получения измерительной информации, может быть объективным или субъективным. Например, можно измерять массу груза с помощью весов (объективное измерение, которое использует техническое средство), – а можно измерять ощущение веса, которое возникает у человека, когда он поднимает груз (субъективное измерение, использующее экспертные оценки).

Большинство объективных измерений использует единицу измерения и свойство аддитивности физических величин. В тех случаях, когда проводятся субъективные измерения, единица измерения отсутствует и измеряемая величина, как правило, не является аддитивной. Считаем, что измерить неаддитивную величину объектов можно в порядковой шкале, а значения величины будем находить косвенно. С этой целью аксиоматически введем понятие объектов A_i, i=1, 2, …, n величина которых изменяется равномерно. Номер объекта будем называть *рейтингом*. Введем в общем виде аксиоматическое определение рейтинга и выясним, каким образом рейтинг можно связать со значениями величины.

Аксиоматическое определение рейтинга. Чтобы формально ввести неаддитивную меру, введем область ее определения. Пусть задано конечное множество элементов $\Omega=\{\omega_1, \omega_2, \dots, \omega_n\}$. Пусть $\Im$ — множество всех подмножеств Ω (алгебра). Для множества $\Im$ аксиоматически введем неаддитивную меру (рейтинг).

Определение. Неаддитивная мера (рейтинг) – это числовая функция r, определенная на множествах из алгебры $\Im$, причем если $A\subseteq B$, то будет выполняться:

A_1. Если $A\neq B$, то $r(B\backslash A)>0$,

A_2. $r(B\backslash A)= r(B) - r(A)$.

Для множеств $A_i\subseteq\Im$, i=1, 2, …, n можно ввести отношение частичного порядка, определив операцию включения $\subseteq$. В случае отношения частичного порядка среди множества $\{A_1, A_2,\dots, A_n\}$ могут быть несравнимые элементы. Если во множестве $\{A_1, A_2, \dots, A_n\}$ любые два элементы сравнимы, то такое множество называют *упорядоченным множеством*.

Пример 1. Пусть $\Omega=\{\omega_1,\omega_2\}$ и $\omega_1\cdot\omega_2=\varnothing$, тогда $\Im=\{A_0, A_1, A_2, A_{12}\}$, где $A_0=\varnothing$, $A_1=\omega_1$, $A_2=\omega_2$, $A_{12}=\omega_1+\omega_2$. Можно выделить два упорядоченных подмножества $\Im$: $\{A_0, A_1, A_{12}\}$ и $\{A_0, A_2, A_{12}\}$.

Пусть $r(A_1\backslash A_0)=r(A_{12}\backslash A_1)$. Следовательно, выполняются равенства $r(A_1) - r(A_0)=\lambda$, $r(A_{12}) - r(A_1) = \lambda$, где λ – неизвестная положительная постоянная. Тогда $r(A_1)= \lambda+r(\varnothing)$, где $\lambda=(r(\Omega) - r(\varnothing))/2$. Причем $r(\Omega)$, $r(\varnothing)$ – любые числа, для которых выполняется неравенство $r(\Omega)>r(\varnothing)$. Если, например, $r(\Omega)=1$ и $r(\varnothing)=0$, то получим вероятностную меру с вероятностями $r(\omega_1) = 1/2$ и $r(\omega_2) = r(A_{12}\backslash A_1) = r(\Omega) - r(\omega_1)= 1/2$. Из примера следует, что аддитивная мера является частным случаем неаддитивной меры.

Величина объекта. Чтобы использовать определение неаддитивной меры для измерения величины объекта, определим величину объекта с позиций теории множеств. Определение приведем вначале для частного случая трех объектов. Пусть объекты A_1, A_2, A_3 упорядочены по величине Q (объекты упорядочены с помощью некоторого отношением порядка $\leq$) и выполняется $A_1\leq A_2\leq A_3$. Под величиной объектов A_1, A_2, A_3 будем понимать множества $\omega_1 = \{\{A_1\}\}$, $\omega_2 = \{\{A_1\}, \{A_1, A_2\}\}$, $\omega_3 = \{\{A_1\}, \{A_1, A_2\},$