

«Cardio». Программа состоит из основного модуля анализа и обработки данных, модуля сбора данных, графического модуля и блока, работающего с радиомодулем телефона. Кроме того, в программе реализованы модули управления питанием блока регистрации, блока формирования сигнальных данных отправляемых через службу коротких сообщений SMS, блока формирования ЭКГ передаваемой через Internet с помощью услуги GPRS и другие. Результат анализа выводится непосредственно на экран мобильного телефона «Smartphone», либо сохраняются на карту памяти.

Следует отметить также, в качестве существенного достоинства разработанной программы, реализацию в ней алгоритма определения местоположения пользователя с помощью технологии GSM, что очень важно для пользователя, оказавшегося в критической ситуации.

Литература

1. Суворов А. В. Клиническая электрокардиография.- НГМИ. Нижний Новгород, 1993.- с 5.-34
2. Ripley K. L., Bump T. E., and Arzbaecher R. C. Evaluation of techniques for recognition of ventricular arrhythmias by implanted devices. / *IEEE Trans. Biomed. Eng.* – Vol. 36, 1989/ – p. 618–624
3. Крекрафт Д., Джерджли С. Аналоговая электроника. Схемы, системы, обработка сигнала. – М., 2005. с. 34–101

СПОСОБЫ И АЛГОРИТМЫ ЭФФЕКТИВНОЙ ПРОГРАММНОЙ РЕАЛИЗАЦИИ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

В. А. Трофимчук

В процессе интенсивного развития беспроводных коммуникационных технологий возникает необходимость обеспечения безопасности при передаче данных. Одним из методов реализации конфиденциального трафика является применение криптографических преобразований. При реализации криптопреобразований, особенно несимметричных, возникают проблемы, связанные малым быстродействием используемых алгоритмов. В данной работе рассматриваются несколько способов вычисления произведения kP , где k – большое целое число, P – точка на плоскости. Данная операция является основной при реализации криптосистем на основе эллиптических кривых [1].

При создании криптографических систем нужно учитывать, что все вычисления производятся по модулю некоторого целого числа p . В частности, это означает, что используются не произведения и суммы чисел, а остатки от деления этих произведений и сумм на данный модуль. При

этом сохраняются все известные свойства арифметических операций (коммутативность, ассоциативность, дистрибутивность) и у всех чисел от нуля до p существуют противоположные элементы: $x+(-x)=0 \bmod p$. Если же используемый модуль p — простое число, то во множестве целых чисел $0, \dots, p$ можно задать операцию инверсии: для любого x кроме нуля существует $x^{-1} < p$ такое, что $xx^{-1}=1 \bmod p$. Таким образом, рассматриваемое множество представляет собой поле (поле Галуа $GF(p)$).

Существуют вычисления, представляющие собой многократное выполнение некоторой базовой ассоциативной операции. Например, вычисление произведения может быть сведено к многократному сложению, для модулярной экспоненты базовой операцией является умножение и т. д. В общем случае имеются два множества: $GF(p)$ и некоторая группа H (в частности, $H = GF(p)$ или $H = GF(p) \setminus \{0\}$). В группе H задана операция $\circ$. Требуется вычислить $kP = P \circ P \circ \dots \circ P$ (k раз), $k \in GF(p)$, $P \in H$. Здесь важно представить множитель k таким образом, чтобы число выполнений базовых операций было как можно меньшим.

Одним из вариантов представления множителя является следующий [2]:

$$k = k_0 + 2(k_1 + 2(\dots)),$$

где k_i равны нулю или единице. В результате kP запишется, например, в таком виде:

$$kP = P \circ 2 \cdot 2(P \circ 2 \cdot (\dots)).$$

В итоге количество выполнений базовых операций не превышает $2m-2$, где m — количество бит числа k .

Однако такое представление не является оптимальным. Оно опирается на двоичный вид числа k , но можно использовать систему счисления с основанием 2^n . Тогда k запишется в виде

$$k = k_0 + 2^n(k_1 + 2^n(\dots)),$$

где k_i принимают значения в диапазоне от 0 до $2^n - 1$. При этом должны быть предвычислены значения $2P, 3P, \dots, (2^n - 1)P$ — всего $2^n - 2$ предвычислений. Очевидно, что при увеличении n затраты на предвычисления быстро возрастают. Однако переход к другому основанию оправдан, так как максимальное число выполнений базовых операций, соответствующих знаку «+» («+—вычислений») в разложении числа k уменьшается. Следует сказать, что более интересно не максимальное, а среднее число этих вычислений. В случае двоичной системы счисления «+—вычисление» пропускается (за счет нулевого бита) с вероятностью 0,5. Таким образом, в данном случае среднее число «+—вычислений» равно $0,5m-1$. В случае основания 2^n вероятность пропуска равна $0,5^n$. Предположим, что m делится на n . Тогда среднее число «+—вычислений» равно

$(m/n)(1-0,5^n)-1$. Коэффициент при m уменьшается с ростом n : 0,5 для $n=1$, затем 0,375, 0,292, 0,234 и т. д.

Оптимальное значение n выбирается для каждого конкретного m . Оно может быть выбрано и более точно — для каждого конкретного k .

Можно отметить, что благодаря применению метода, использующего разложение множителя, для вычисления произведения автоматически исчезает проблема вычисления остатка от деления числа двойной длины на модуль p , так как выполнение сложения по модулю p как базовой операции приводит к получению результата в нужном виде.

Самой сложной операцией является вычисление инверсии. Для выполнения этой операции может быть использован расширенный алгоритм Эвклида. Он основан на алгоритме Эвклида для нахождения наибольшего общего делителя.

Пусть a и b положительные целые числа и $a > b$. a можно представить как

$$a = bq_0 + r_1,$$

где $q_0 = [a/b]$ и $0 \leq r_1 < b$. Затем то же самое можно сделать для пары b и r_1 и далее:

$$b = r_1q_1 + r_2,$$

$$\dots\dots\dots$$

$$r_{n-2} = r_{n-1}q_{n-1} + r_n,$$

$$r_{n-1} = r_nq_n + 0$$

Наибольший общий делитель здесь равен r_n .

Приведенный алгоритм можно использовать для решения Диофантова уравнения

$$by - ax = 1,$$

где, как нетрудно видеть, $y = b^{-1} \bmod a$. Здесь $\text{НОД}(a, b) = 1$, иначе обратный элемент отсутствует. Значит, предпоследнее уравнение, получающееся при нахождении $\text{НОД}(a, b)$ с помощью алгоритма Эвклида, можно переписать как

$$r_{n-2} - r_{n-1}q_{n-1} = 1,$$

а затем выразить r_{n-2} и r_{n-1} через предыдущие равенства. Входящие в эти выражения r_i представляются аналогичным образом. Таким образом, в самом конце остаются только a , b и коэффициенты, выраженные через q_i .

Очевидно, что алгоритм Эвклида требует выполнения большого числа элементарных операций. Это число зависит, в частности, от количества выполняемых делений с остатком. Можно найти максимальное количество этих делений.

Пусть используются числа, меньшие 2^m . Построим последовательность x_i , где x_1 равно модулю, x_2 – то число, инверсию которого требуется найти, $x_{i+1} = x_{i-1} \bmod x_i$. Последнее число $x_n = 1$. Задачу поиска максимального n при заданном x_1 можно заменить задачей поиска минимального x_1 при заданном n . Очевидно, что $x_{i-1} = k_i x_i + x_{i+1}$. x_1 будет минимальным, если все $k_i = 1$, т. е. если числа от x_n до x_1 образуют последовательность чисел Фибоначчи F_k , начиная со второго номера. Известно, что

$$F_k = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k}{\sqrt{5}} \approx \frac{\left(\frac{1+\sqrt{5}}{2}\right)^k}{\sqrt{5}}.$$

Отсюда

$$k = \log_{\frac{1+\sqrt{5}}{2}} (F_k \sqrt{5}) < \log_{\frac{1+\sqrt{5}}{2}} F_k + 2.$$

Таким образом, для максимального количества делений N можно записать

$$N < m \log_{\frac{1+\sqrt{5}}{2}} 2 - 1 = \frac{m}{\log_2(1+\sqrt{5}) - 1} - 1.$$

Таким образом, в данной работе предложен и разработан способ проведения вычислений (модулярное умножение и инверсия), представляющих собой многократное выполнение базовой ассоциативной операции, основанный на специальном представлении одного из аргументов и предвычислениях.

Литература

1. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – Официальное издание (03.04.2001). – с. 4–12.
2. *Lim C. H., Hwang H. S., Lee P. J.* Fast modular reduction with precomputation. – Information & communication research center, Future systems; Pohang univ. of science & technology, Korea, 2003, p. 1–6.

ИССЛЕДОВАНИЕ СТРУКТУРЫ ДЕФЕКТОВ, СОЗДАНЫХ ИМПУЛЬСНЫМ ЛАЗЕРНЫМ ИЗЛУЧЕНИЕМ В ОПТИЧЕСКИ ПРОЗРАЧНЫХ МАТЕРИАЛАХ

С. А. Циер

Практически одновременно с созданием мощных лазеров было выяснено, что под действием лазерного излучения возникают разрушения прозрачных твердых тел. На основе этого эффекта был предложен метод

создания с помощью сфокусированного лазерного импульсного излучения растрового изображения внутри прозрачного материала, представляющего собой совокупность микродефектов [1; 2]. Ведутся также работы по формированию многоцветных изображений в стекле, открываются перспективы создания трехмерных оптических запоминающих устройств со сверхвысокой плотностью упаковки [3]. Однако для развития этих направлений следует детально изучить процесс пробоя, построить математическую модель и научиться воспроизводить результаты эксперимента.

Разрушения, возникающие в прозрачных твердых телах под действием лазерного излучения, наиболее целесообразно разделить на разрушения, возникающие в идеально чистых средах, и разрушения, обусловленные примесями [4]. В этих случаях различны механизмы, приводящие к разрушению. В чистой среде это оптический пробой.

Процесс пробоя состоит из следующих этапов:

Мощное лазерное излучение создает свободные электроны. Ионизация атомов может происходить за счет многофотонного поглощения.

Действующее лазерное излучение ускоряет электроны, которые способны выбить связанный электрон из атома. Энергия, которую необходимо набрать электрону, должна превышать потенциал ионизации атома.

Развивается электронная лавина.

Происходит быстрый локальный нагрев и плавление среды.

Возникают механические напряжения между модифицированной областью и областью, в которой не происходило поглощение энергии лазерного импульса, что приводит к разрушению твердого тела и возникновению микродефекта.

При наличии в прозрачной среде локальных макроскопических примесей или дефектов с большим коэффициентом поглощения излучения эти локальные области быстро нагреваются, что и служит, в конечном счете, причиной разрушения прозрачной среды. Таким образом, при наличии примесей идет речь о тепловом разрушении прозрачных сред.

В результате поглощения энергии лазерного излучения этими локальными областями, в них очень быстро (за время лазерного импульса) увеличивается температура, соответственно, увеличивается давление, приводящее к растрескиванию стекла в небольшой области вокруг примеси.

Теоретическое описание теплового разрушения основано на решении уравнения теплопроводности для среды с примесями. Кроме теплофизических свойств среды (чистой и содержащей примеси) необходимо учесть размер локальных областей, среднее расстояние между ними и коэффициент поглощения излучения. В наиболее простой модели можно

пренебречь зависимостью коэффициента поглощения от температуры нагреваемой области. В качестве критерия разрушения среды принимается критическая температура области, при которой возникают необратимые изменения среды (например, плавление).

В лаборатории кафедры физической электроники на базе универсального автоматизированного лазерного комплекса и установки лазерной гравировки ELS-03 были проведены эксперименты по определению критической плотности мощности, необходимой для создания



Рис. 1. Увеличенная фотография микродефекта в стекле

микродефекта, измерены линейные размеры модифицированных областей. Анализ зависимости процесса образования дефектной области в стекле от энергии лазерного импульса показывает, что пробой носит пороговый характер; размер области разрушения зависит от параметров фокусирующей системы, энергии и длительности импульса лазерного излучения, а также марки стекла.

Изображение внутри стекла формируется из совокупности микродефектов, представляющих собой пробой в стекле. От того, какую форму и размер имеет пробой, будет зависеть качество изображения. Поэтому необходимо критически отнестись к параметрам лазерного излучения.

Контроль пробоя осуществлялся визуально и в оптический микроскоп. Проведённые измерения показали, что форма микродефекта соответствует эллипсоиду с размерами 0.1 – 0.2 мм в горизонтальном направлении и 0.15 – 0.3 в вертикальном направлении (Рис. 1). Размеры микродефекта возрастают с увеличением фокусного расстояния линзы. Дополнительные исследования показали, что если расстояние между дефектами не превышает размеров дефекта, то моделированные области можно рассматривать как независимые, а если расстояние между ними сравнимо или меньше размера дефекта, то может наступить расстеклование (разрушение) материала.

Для того чтобы определить зависимость линейных размеров микродефекта от плотности мощности лазерного импульса, была сформулирована математическая модель процесса пробоя в стекле. Моделирование проводилось в программной среде Mathematica 4.1.

В силу того, что длительность лазерного импульса порядка 10^{-8} с, предполагается, что поглощение энергии лазерного импульса в стекле происходит почти мгновенно. Затем тепло распространяется по объёму из области, в которой поглощается энергия.

Численное решение этой задачи предполагает разностную дискретизацию уравнения теплопроводности:

$$\frac{\partial T}{\partial t} = \nabla(k \nabla T), \quad (1)$$

где k – температуропроводность материала.

В итоге можно получить двумерное стационарное распределение температуры.

Зная распределение температуры в области поглощения энергии лазерного импульса, а также температуру и теплоту плавления стекла, можно определить линейные размеры микродефекта, созданного лазерным излучением.

В качестве граничных условий при моделировании процесса пробоя использовались следующие параметры:

- Температура плавления стекла – $T_{\text{плав.}} = 1973 \text{ К}$;
- Размер области моделирования – $0.1 \times 0.1 \text{ см}$ ($1000 \times 1000 \text{ мкм}$);
- Радиус пятна фокусировки – $r_f = 12.9 \text{ мкм}$;
- Высота начальной области мгновенного поглощения – 60 мкм .
- Для дискретизации задачи (1) было принято:
- Шаг дискретизации – $s = 3 \text{ мкм}$;
- Абсолютная погрешность определения температуры – $\varepsilon = 10 \text{ К}$.

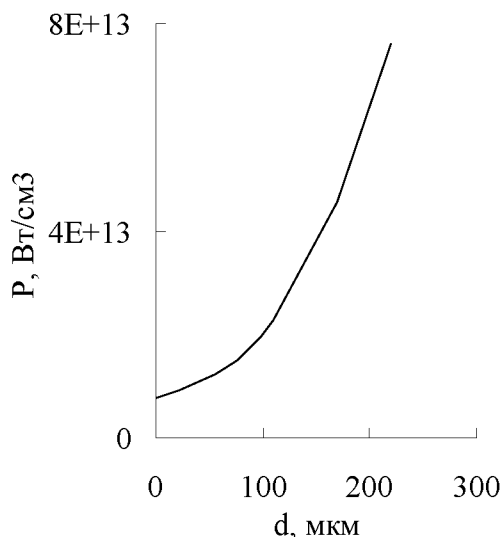


Рис. 2. Зависимость размера пробоя от плотности мощности лазерного импульса

Допустим, что энергия лазерного импульса 75 мДж . Доля поглощенной энергии составляет 20% , т.е. $Q_{\text{погл.}} = 15 \text{ мДж}$. В этом случае решение уравнения (1) дает почти сферическую форму области расплава (микродефекта) с диаметром 108 мкм и максимальную температуру в области пробоя, равную 3179 К . На Рис. 2 приведены результаты расчетов диаметра микродефекта для разных плотностей мощности лазерного излучения.

Из результатов моделирования видно, что область пробоя имеет форму, близкую к сферической, в то время как в эксперименте она имеет эллиптическую форму, что

объясняется, по-видимому, влиянием сферической aberrации фокусирующей линзы. Однако теоретические размеры диаметра микродефекта совпадают с экспериментальными. Для более точного расчета высоты области необходимо учесть поправки на aberrацию системы фокусировки. Используя экспериментальные данные о размерах микродефекта, с помощью разработанного алгоритма можно решить и обратную задачу по определению количества теплоты, поглощаемого стеклянным образцом в результате облучения лазерным импульсом.

ВЫВОДЫ

В данной работе проведены исследования процессов оптического пробоя в стекле марки К8. По результатам экспериментальных данных определена зависимость размера области пробоя от плотности мощности лазерного излучения. В результате математического моделирования процесса пробоя, основанного на приближении мгновенного поглощения лазерного излучения материалом и численном решении стационарного уравнения теплопроводности, рассчитаны линейные размеры модифицированных областей в стекле марки К8.

Литература

1. *Kazuyuki Hirao, Jianrong Qiu, Kiotaka Miura et al.* Femtosecond laser induced phenomena in active ion-doped glasses and their applications // Transactions of the Materials Research Society of Japan. 2004. № 29 [1]. P. 3–7.
2. U.S. Patent № 4, 843, 207. 1997
3. U.S. Patent № 5, 637, 244. 2000
4. *Делоне Н. Б.* Взаимодействие лазерного излучения с веществом / М.: Наука, 1989 г.

РАЗРАБОТКА И РЕАЛИЗАЦИЯ АЛГОРИТМА АНАЛИЗА РАСПРЕДЕЛЕНИЯ ИНТЕНСИВНОСТИ ФЛУОРЕСЦЕНЦИИ

И. П. Шингарёв

В связи с повышением требований к точности и надёжности определения параметров веществ, находящихся в растворе, все чаще используются методы флуоресцентной флуктуационной спектроскопии. Среди них выделяется метод, основанный на исследовании экспериментального распределения числа фотонов, полученных за время T – РСН-анализ, позволяющий получать информацию об излучательной способности и концентрации молекул вещества, находящегося в растворе. Процедура анализа распределения числа фотонов многоэтапна, поэтому возникает необходимость в разработке алгоритма для проведения такого анализа.

Идея алгоритма весьма проста. Необходимо построить теоретическое распределение числа фотонов, зависящее от физических параметров, ха-