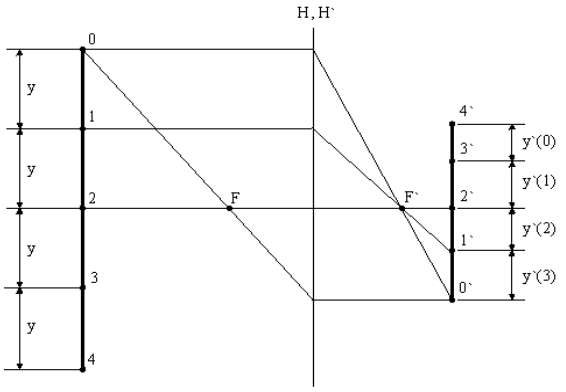

Рисунок 4. Плоскости объектов и изображений оптической системы

1. ГОСТ 20825-75. Объективы съемочные. Методы измерений дисторсии. – Введ. 01.07.1976. – М.: Издательство – стандартов. 12с.
2. Курков, В.М. Методы учёта систематических искажения аэроснимка. Самокалибровка / В.М. Курков // Изв. вузов. Геодезия и аэрофотосъёмка. – 1980. – № 6. – С. 75-79.
3. Cramer M. EUROSDR network on digital camera calibration // International Archives of Photogrammetry and Remote Sensing, 2004, Vol.35, Part B6, Istanbul, P.204-209.
4. Schuster R., Braunecker B. Calibration of the ADS40 airborne digital sensor // International Archives of Photogrammetry and Remote Sensing, 2000, Vol.33, Part B1, Amsterdam, P.288-294.
5. Alharthy A., Bethel J. Laboratory self-calibration of a multi-band sensor // International Archives of Photogrammetry and Remote Sensing, 2001, Vol.34, Part 3A, Graz, Austria, P.23-28.
6. Ежова, К.В. Математическое моделирование фотограмметрической дисторсии / К.В. Ежова // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. – 2006. – Вып. 26. – С. 235-239.

УДК 512.624.95:378.147.091.3

МАТЕМАТИЧЕСКИЕ И МЕТОДИЧЕСКИЕ АСПЕКТЫ ВВЕДЕНИЯ БАЗОВЫХ ПАРАМЕТРОВ ПРИ МОДЕЛИРОВАНИИ КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ XTR

Крупенкова Т.Г.[1], Липницкий В.А.[2]
[1]Белорусский национальный технический университет
[2]Военная академия Республики Беларусь
Минск, Республика Беларусь

Рассматриваемая криптографическая система, а также описываемый в данной работе подход в применении к криптографическим протоколам были впервые предложены в 2000 году на ежегодной международной научной конференции «Crypto-2000» авторами – Ленстрой А.К. и Верхейлом Э.Р. [1].

Название XTR явилось удачной аббревиатурой английского словосочетания «Efficient and Compact Subgroup Trace Representation».

Становящиеся классическими система обмена ключами Диффи-Хелмана, криптографические системы RSA и Эль Гамаля и созданные на их основе системы цифровой подписи, базируются на арифметике колец классов вычетов Z/nZ, где n либо является простым числом, либо произведением двух простых чисел. XTR-криптография основывается на 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 числами p.

Современный немецкий математик и криптограф Шнорр К.П. в 1991 году предложил использовать в криптосистеме Эль Гамаля следующую оригинальную идею – заменять образующие g мультипликативных групп $GF(p)^*$ полей $GF(p) = Z/pZ$ на образующие подгрупп максимально высокого простого порядка q этих мультипликативных групп [2].

Такой подход приводит практически к пятикратному уменьшению размеров применяемых ключей, отнюдь не снижая при этом вязкости вычислений и криптостойкости систем.

Идея Шнорра К. П. находит широкое применение и в XTR-криптографии. Здесь q - достаточно большой (максимально большой) простой делитель порядка $p^2 - p + 1$ подгруппы мультипликативной группы $GF(p^6)^*$.

Пусть p - нечетное простое число, сравнимое с 2 по модулю 3: $p = 2(\mathrm{mod}\,3)$. Тогда поле

Галуа $GF(p^6)$ содержит мультипликативную группу $GF(p^6)^*$ порядка

$$p^6-1=(p^3-1)(p+1)(p^2-p+1).$$

Приведенное вычисление свидетельствует о существовании в группе $GF(p^6)^*$ циклической подгруппы $<\tilde{g}>$ порядка p^2-p+1. При этом элемент $\tilde{g}\in GF(p^6)^*$ не может принадлежать ни одному из подполей поля $GF(p^6)$: ни $GF(p^3)$, ни $GF(p^2)$, ни $GF(p)=Z/pZ$, потому, что порядок p^2-p+1 элемента $\tilde{g}$ не делится ни один из порядков p^3-1, p^2-1, $p-1$ мультипликативных групп $GF(p^3)^*$, $GF(p^2)^*$, $GF(p)^*$ соответственно. Следовательно, минимальное подполе поля $GF(p^6)$, содержащее элемент $\tilde{g}$, должно совпадать с полем $GF(p^6)$.

Пусть мультипликативный порядок элемента g равен q - максимальному простому делителю числа p^2-p+1, что существенно меньше величины p^6-1. Таким образом, элемент g заведомо не является примитивным элементом поля $GF(p^6)$.

В криптографии общепринято не пользоваться стандартной арифметикой конечного поля, базирующейся на примитивных элементах.

Над полем $GF(p)=Z/pZ$ с условием $p=2(\mathrm{mod}3)$ полином x^2+x+1 неприводим. В этом можно убедиться сразу для всех указанных простых чисел p. Действительно, здесь $p=2+3t$ для некоторого натурального t. Поэтому $p-1=1+3t$ является величиной, не делящейся на 3. Это влечет за собой отсутствие в группе $GF(p)^*$ элементов третьего порядка. Так как рассматриваемый полином допускает представление $x^2+x+1=(x^3-1)/(x-1)$, то его корни являются корнями кубическими из 1. Таким образом, полином x^2+x+1 не имеет корней в поле $GF(p)=Z/pZ$ и, следовательно, не приводим над ним.

Проведенное рассуждение означает, что полином x^2+x+1 порождает квадратичное расширение поля $GF(p)=Z/pZ$:

$$GF(p^2)=Z/pZ[x]/<x^2+x+1>.$$

Поле $GF(p^2)$ совпадает с фактор-кольцом кольца полиномов Z/pZ по максимальному идеалу, порождённому неприводимым полиномом x^2+x+1.

Мультипликативная группа $GF(p^2)^*$ имеет порядок p^2-1, который при условии $p=2+3t$ делится на 3: $p^2-1=4+12t+9t^2-1=3\cdot(1+4t+3t^2)$.

Полином x^3-1 не имеет кратных корней при любом расширении поля $GF(p)=Z/pZ$. Этот полином взаимно прост со своей производной $3x^2$, имеющей двукратно вырожденный корень, равный 0. Значит, и делитель x^2+x+1 полинома x^3-1 имеет два различных корня. Очевидно, оба эти корня принадлежат полю $GF(p^2)=Z/pZ[x]/<x^2+x+1>$. Как уже отмечалось выше, мультипликативный порядок этих корней равен 3. Следовательно, эти корни не могут быть примитивными элементами поля $GF(p^2)$.

Вернемся к полю $GF(p^6)$. Теория конечных полей [3, 4] гарантирует, что над полем $GF(p)$ существует неприводимый и примитивный полином 6-й степени. Его корень π является примитивным элементом поля $GF(p^6)$. Тогда для целого числа

$$\xi=\frac{p^6-1}{p^2-p+1}$$

элемент π^{ξ} поля $GF(p^6)$ имеет, очевидно, мультипликативный порядок p^2-p+1. Именно его можно взять в качестве отмеченного выше элемента g.

Поле $GF(p^2)$ является расширением Галуа поля $GF(p)=Z/pZ$ с группой автоморфизмов второго порядка

$$Gal(GF(p^2)/GF(p))=<\varphi>=\{\varphi,\varphi^2=e\}$$

для автоморфизма Фробениуса φ, действующего на каждый элемент $a\in GF(p^2)$ по правилу: $\varphi(a)=a^p$.

Согласно теории расширений Галуа, если α - один из корней полинома x^2+x+1, то другим корнем является $\varphi(\alpha)=\alpha^p$. Непосредственная проверка показывает, что система α,α^p образует нормальный базис в поле $GF(p^2)$.

Базис α, α^p можно переписать в несколько иной форме: α, α^2, если учесть, что $\alpha^3 = 1$, $\alpha^p = \alpha^{2+3t} = \alpha^2 \cdot (\alpha^3)^t = \alpha^2$. Следовательно, каждый элемент z поля $GF(p^2)$ однозначно представим в виде $z = x_1\alpha + x_2\alpha^2$ для подходящих элементов $x_1, x_2 \in GF(p)$. К примеру, каждый элемент $t \in GF(p)$ имеет вид

$$t = (p-1)t \cdot \alpha + (p-1)t \cdot \alpha^2 .$$

Все вычисления в поле $GF(p^2)$, принятые в криптосистеме XTR, проводятся в нормальном базисе. Например, в построенном нами базисе α, α^2. Для их реализации необходимо предварительно осуществить вывод специфических формул для умножения, деления, возведения в степень элементов поля, а также иных операций выполняемых в выбранном нормальном базисе.

Одним из открытых ключей в XTR-криптосистеме является $Tr(g)$ – след элемента g над полем $GF(p^2)$. Вычисление следов также осроумно сводится к вычислениям в поле $GF(p^2)$, в базисе α, α^2.

Таким образом, новая криптографическая система вводит в ареал современной практической криптографии новый для неё математический объект - поля Галуа, требует глубокого освоения ее развитой алгебраической теории.

1. Lenstra, A. K., Verheul, E. R. The public key system. In CRYPTO 2000// Lecture Notes in Computer Science, vol. 1880. Springer-Verlag. 2000. - P. 1 – 19.
2. Криптология: учебник/ Ю.С. Харин [и др.]. – Мн.: БГУ, 2013. – 512 с. – (Классическое университетское издание).
3. Лидл Р., Нидеррайтер Г. Конечные поля. В 2-х т. Пер. с англ. – М.: Мир, 1988. – 822 с.
4. Липницкий В.А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа. – Мн.: БГУИР, 2006. – 88 с.

УДК 678.057.9

МНОГОФУНКЦИОНАЛЬНЫЙ РОБОТОТЕХНИЧЕСКИЙ КОМПЛЕКС ДЛЯ УПЛОТНЕНИЯ, ГЕРМЕТИЗАЦИИ И СКЛЕИВАНИЯ

Ксенофонтов М.А., Выдумчик С.В., Гавриленко О.О., Павлюкевич Т.Г., Чупрынский С.А.
Научно-исследовательское учреждение «Институт прикладных физических проблем им. А.Н. Севченко» Белорусского государственного университета
Минск, Республика Беларусь

В данной работе представлено робототехническое оборудование, применяемое для дозирования, смешения и нанесения по заданной траектории герметиков, различных клеевых составов, уплотнителя и уплотнительного контура из силикона и пенополиуретана (технология получение уплотнения по месту).

Суть технологии заключается в точном нанесении по программируемой траектории отдозированной и смешенной двухкомпонентной (возможно многокомпонентной) полиуретановой или силиконовой композиции. Компоненты смеси, вступая в реакцию после смешения, образуют на поверхности или в пазе изделия уплотнение с внешней защитной пленкой (оболочкой или поверхностной коркой).

Новизна разработки заключается в возможности использования комплекса для последовательного нанесения уплотнительных контуров из различных композиций без переналадки оборудования, что позволяет увеличить производительность и в одном технологическом цикле наносить полиуретановые и силиконовые уплотнения на изделия различного назначения.

Комплекс оснащен современной системой управления: промышленный компьютер с 12" цветным сенсорным дисплеем для программирования и визуализации; высокопроизводительный контроллер управления перемещением; программирование перемещения с помощью команд и по заранее подготовленным шаблонам; программирование соотношения компонентов и производительности без механической настройки; задание производительности в программе нанесения для получения требуемой геометрии контура.

Робототехнический комплекс обеспечивает необходимую точность позиционирования, имеет простой и интуитивно понятный интерфейс управления, обладает высокой производительностью и может успешно использоваться на предприятиях электронной, машиностроительной и других отраслях.

В основу работы комплекса положен принцип подачи дозированного количества двух жидких компонентов А и Б в смесительную головку с динамическим перемешиванием и последующим