В настоящее время в Республике Беларусь автоматизировано несколько расчетных методик в области противопожарного нормирования и стандартизации, которые размещены на web-сайте МЧС [4]. Однако, эти программные средства (далее – ПС) имеют ряд недостатков: 1. разработаны для локального использования и исключают возможность работы с ними через web-доступ, что не гарантирует использование пользователем актуальной версии программы; 2. не являются кроссплатформенными и работают только на операционной системе (далее – ОС) MicrosoftWindows, пользователи других ОС (в том числе мобильных) не могут воспользоваться этими программами; 3. для решения комплексных задач потребуется использование сразу нескольких приложений, в то же время функционал некоторых из них может быть объединен в одном ПС; 4. отсутствует возможность сохранения истории выполненных расчетов или создания шаблонов расчетов для их применения при формировании отчета.

В целях создания более совершенного программного обеспечения ведется разработка информационно-вычислительного комплекса (далее – ИВК) на базе web-технологий с доступом через сеть Интернет. ИВК позволит централизовать и унифицировать проведение инженерных расчетов и существенно сократить трудозатраты на экспертизу проектной документации. Использование ИВК работниками инспекции государственного пожарного надзора предоставит возможность осуществить достоверную экспресс-проверку инженерных расчетов в области противопожарного нормирования и стандартизации в сжатые сроки при осуществлении надзорной деятельности.

Список использованных источников:

1. Система стандартов безопасности труда. Пожарная безопасность. Общие требования: ГОСТ 12.1.004-91. – Введ. с 01.07.92 / Государственный стандарт союза ССР. – М.: Издательство стандартов, 1992. – 91 с.

2. Татарников С. Расчетные методы обеспечения пожарной безопасности при проектировании зданий и сооружений / С.Татарников // Служба спасения 101. – 2010. – №7(151). – С.27-29

3. О лицензировании отдельных видов деятельности: Указ Президента Республики Беларусь 1 сентября 2010 г. № 450. – М.: Зар-но в Нац. реестре правовых актов Республики Беларусь 03.09.2010 г. № 1/11914

4. Расчетные программы для проектировщиков [Электронный ресурс] / Официальный сайт Министерства по чрезвычайным ситуациям Республики Беларусь – Режим доступа: http://mchs.gov.by/rus/main/business/programs. – Дата доступа: 21.03.2016.

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ И ИХ ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Короткевич А. В.

Ярмолик В. Н. – д-р. техн. наук, профессор

Обеспечение безопасности информации является одной из важнейших проблем современного общества. Такая безопасность может быть достигнута с использованием различных криптографических методов, одними из самых передовых и перспективных среди которых являются криптосистемы, основанные на свойствах эллиптических кривых.

В общем случае уравнение эллиптической кривой имеет вид:

$$y^2 + axy + by = x^3 + cx^2 + dx + e,$$

где x, y – переменные; a, b, c, d, e – действительные числа.

Для определения операции сложения для точек на эллиптической кривой сделаем следующие предположения:

1. На плоскости существует бесконечно удаленная точка $0 \in E$, в которой сходятся все вертикальные прямые.

2. Будем считать, что касательная к кривой пересекает точку касания два раза.

3. Если три точки эллиптической кривой лежат на прямой линии, то их сумма есть 0.

Введем следующие правила сложения точек на эллиптической кривой [1]:

1. Точка 0 выступает в роли нулевого элемента. Так $0 = -0$ и для любой точки P на эллиптической кривой $P + 0 = P$.

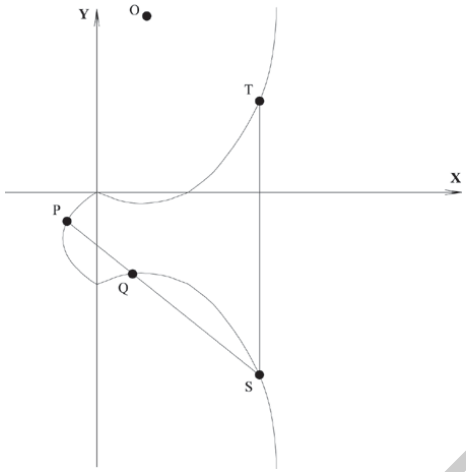
2. Вертикальная линия пересекает кривую в двух точках с одной и той же координатой x – скажем, $S = (x, y)$ и $T = (x, -y)$. Эта прямая пересекает кривую и в бесконечно удаленной точке. Поэтому $S + T + 0 = 0$ и $S = -T$.

3. Чтобы сложить две точки P и Q с разными координатами x, следует провести через эти точки прямую и найти точку пересечения ее с эллиптической кривой (рисунок 1). Если прямая не является касательной к кривой в точках P или Q, то существует только одна такая точка, обозначим ее S. Согласно нашему предположению $P + Q + S = 0$. Следовательно, $P + Q = -S$ или $P + Q = T$.

Чтобы удвоить точку Q следует провести касательную в точке Q и найти другую точку пересечения S с эллиптической кривой. Тогда $Q + Q = 2Q = -S$.

Введенная таким образом операция сложения подчиняется всем обычным правилам сложения, в частности коммутативному и ассоциативному законам. Умножение точки *P* эллиптической кривой на положительное число *k* определяется как сумма *k* точек *P*.

Как известно, стойкость алгоритмов ассиметричной криптографии базируется на вычислительной невозможности эффективного решения некоторых математических задач. Например, стойкость криптосистемы



RSA базируется на сложности задачи факторизации больших чисел, а стойкость современных схем ЭЦП, большинство из которых являются вариациями обобщенной схемы Эль-Гамаля, – на сложности задачи логарифмирования в конечных полях.

Рис. 1 – Сложение точек на эллиптической кривой

Для эллиптических криптосистем такой трудноразрешимой задачей является нахождение числа *k*, если известна точка *P* и точка, полученная в результате умножения точки *P* на *k* (задача дискретного логарифмирования на эллиптической кривой). Таким образом, операция умножения точки *P* на число *k* является ключевой в эллиптической криптографии, потому скорость ее выполнения напрямую влияет на производительность всей криптосистемы в целом. А именно высокая вычислительная сложность является основным недостатком ассиметричных криптосистем по сравнению с симметричными.

Для оптимизации операции вычисления произведения точки эллиптической группы *P* на число *k* можно предложить следующие подходы:

1. Бинарное представление числа *k* в виде массива бит длиной *t*. На начальном шаге итоговому результату присваивается значение нулевой точки. Затем при проходе бинарного массива, начиная со старшего индекса, на каждом шаге результирующее значение удваивается, а после этого, если текущий бит равен 1, дополнительно увеличивается на *P*. В результате итоговое значение будет содержать сумму произведений точки *P* на числа, являющиеся степенью числа 2 и в сумме дающие *k*, что эквивалентно искомому произведению *kP* . Среднее число единиц в бинарном представлении числа *k* равно $t/2$, потому сложность данного алгоритма можно представить как $\frac{t}{2}A+tD$, где *A* и *D* – сложности операций сложения и умножения соответственно.

2. Использование представления числа *k* с помощью несмежных форм (*NAF* – non-adjacent form). Несмежная форма числа *k* обладает следующими свойствами [2]:

– *k* имеет уникальную несмежную форму, обозначаемую как *NAF*(*k*);

– *NAF*(*k*) содержит минимально возможное количество ненулевых чисел в своем представлении;

– длина *NAF*(*k*) в худшем случае на 1 больше бинарного представления числа *k*;

– если длину *NAF*(*k*) обозначить как *l*, то $2^l/3 < k < 2^{l+1}/3$;

– среднее количество ненулевых цифр среди всех несмежных форм длины *l* составляет приблизительно $l/3$.

Как следует из свойств несмежной формы *k*, вычислительная сложность данного алгоритма составляет приблизительно $\frac{t}{3}A+tD$, где *t* – длина бинарного представления числа *k*, *A* и *D* – сложности операций сложения и умножения соответственно. Следовательно, данный алгоритм требует на $t/6$ меньше операций сложения, чем алгоритм, основанный на бинарном представлении числа *k*, однако, требует предварительного вычисления *NAF*(*k*). А раз алгоритм вычисления *NAF*(*k*) обладает логарифмической сложностью относительно *k*, что незначительно по сравнению с операцией сложения точек эллиптической группы, то в целом алгоритм на основе несмежных форм оказывается эффективнее.

3. Предыдущий подход может быть улучшен путем обработки нескольких цифр числа *k* одновременно (так называемые оконные методы), т.е. с использованием несмежных форм ширины *w*. Пусть $w \geq 2$ – целое положительное число. Несмежная форма ширины *w* положительного числа *k* выражается как $k=\sum_{i=0}^{l-1} k_i 2^i$, где

каждое ненулевое значение k_i нечетно, $|k_i| < 2^{w-1}$, $k_{l-1} \neq 0$ и по крайней мере одно из подряд идущих k чисел является ненулевым [3].

Свойства несмежной формы ширины w (k – целое положительное число):

– k имеет уникальную несмежную форму ширины w, обозначаемую как $NAF_w(k)$;

– $NAF_2(k) = NAF(k)$;

– длина $NAF_w(k)$ по крайней мере на единицу больше длины бинарного представления k;

– средняя плотность ненулевых чисел среди всех несмежных форм ширины w с длиной l составляет приблизительно $1/(w+1)$.

4. Если точка P является фиксированной для нескольких последовательных операций умножения, то можно скорость выполнения умножения может быть увеличена с использованием дополнительной памяти для хранения предварительно вычисленных данных, зависящих только от P. Например, если все точки $2P, 2^2P, ..., 2^{t-1}P$ вычислены заранее, то ожидаемое время выполнения бинарного метода составит $(t/2)A$ (все удвоения устранены). Использование предварительных вычислений для фиксированной точки также может быть успешно скомбинировано и с другими предыдущими методами.

Таким образом, была исследована математическая модель эллиптических кривых и их применимость в криптографических системах. Выделена основная операция (умножение точки эллиптической группы на число), применяемая в криптографических системах на базе эллиптических кривых, и предложены пути увеличения скорости ее выполнения. В планы дальнейших исследований входит практическая проверка предложенных методов оптимизации алгоритма умножения точки эллиптической группы на число, а также разработка криптографической системы, основанной на свойствах эллиптических кривых, и анализ ее производительности.

Список использованных источников:

1. Henri, C. Elliptic and Hyperelliptic Curve Cryptography: Theory and Practice / C. Henri, F. Gerhard. – Hcapman & Hall/CRC, 2006. – 808 с.

2. Аграновский, А.В. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади – М.: СОЛОН-Пресс, 2010. – 256 с.

3. Hankerson, D. Guide to elliptic curve cryptography / D. Hankerson, A. Menezes, S. Vanstone – Springer-Verlag New York, Inc, 2004. – с. 99.

ПРОГРАММНОЕ СРЕДСТВО ОРГАНИЗАЦИИ ТРЕНИНГА ПО КУРСУ «ОСНОВЫ АЛГОРИТМИЗАЦИИ И ПРОГРАММИРОВАНИЯ»

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Косик Д.Н.

Глухова Л.А. – к.т.н, доцент

В докладе рассмотрены достоинства и недостатки существующих обучающих систем. Сформулированы цели и особенности реализации программного средства организации тренинга по курсу «Основы алгоритмизации и программирования».

Для изучения нового материала, усовершенствования уже полученных знаний и приобретения практического опыта помимо выполнения лабораторных работ в университете необходимо заниматься самостоятельно. По этой причине всё большую популярность стали приобретать различные тренинговые системы, онлайн-курсы и вебинары. При анализе прототипов, таких как MyTestXPro и Quizful, был выявлен ряд недостатков: ограниченность в количестве проходимых тестов (Quizful), невозможность работы с программой в режиме online, платная лицензия для пользования программой по истечении пробного периода (MyTestXPro). Поэтому с целью устранения вышеназванных недостатков разработано программное средство организации тренинга по курсу «Основы алгоритмизации и программирования», предназначенное для автоматизации комплекса задач, связанных с усовершенствованием полученных знаний на лекциях и практических занятиях, изучением нового материала по курсу, получением практического опыта, а также проведением контроля знаний по данной дисциплине.

Основными целями создания программного средства являются:

1) Упростить процесс тестирования студентов – предоставить интуитивно понятный для пользователя интерфейс с возможностью проведения тестирования по курсу «Основы алгоритмизации и программирования».

2) Предоставить студентам быстрый доступ к теоретическим материалам и практическим примерам по заданной дисциплине.

3) Предоставить возможность для преподавателя (или администратора) создания новых тестов, редактирования уже существующих и удаления устаревших тестов.