рок составляет от 5 до 20 деталей. Объем объединенной выборки составляет 10 или более мгновенных, т. е. От 50 до 200 деталей.

Как видно из вышесказанного, проведение анализа точности технологического процесса требует больших затрат материальных ресурсов и времени, что не всегда возможно и целесообразно при проведении учебного процесса. Более целесообразно проведение вычислительного эксперимента и математическое моделирование погрешностей механической обработки на ЭВМ.

ЛИТЕРАТУРА

1. Кане М. М. Основы научных исследований в технологии машиностроения – Мн.: Высш. шк.,1987.

УДК 681.3.32

ИЛЬЯШЕВИЧ Д.А.

Научный руководитель: Костюк Д.А., доцент, к.т.н.

МОДИФИЦИРОВАННЫЙ АЛГОРИТМ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Целью настоящей работы является рассмотрение различных реализаций стандартного алгоритма электронной цифровой подписи (ЭЦП) на эллиптических кривых (ЭК) – ГОСТ Р 34.10-2001. На основе рассмотренных вариантов реализации делается вывод о качестве стандартной реализации протокола, неэффективности отдельных его этапов. В работе обсуждается проблема, которая может возникнуть перед разработчиком в выборе алгоритмов, эффективных по скорости и удовлетворительных по показателям стойкости.

Синтез криптографических конструкций на ЭК, удовлетворяющих показателям стойкости, требует, в первую очередь, выбора следующих параметров:

- вида конечного поля;
- характеристики поля и (или) его расширения;
- уравнения ЭК;
- порядка циклической подгруппы точек ЭК;
- генератора подгруппы точек ЭК.

От выбора данных параметров существенно зависит стойкость криптографических конструкций и безопасность протоколов на ЭК. Одним из главных условий является то, что подгруппа группы точек выбранной кривой должна быть циклической с точкой, играющей роль примитивного элемента (генератора) подгруппы. Если порядок группы – простое число, тогда любой элемент группы может служить ее генератором.

Для синтеза криптографических конструкций необходимо использовать ЭК над полем большой простой характеристики $p-GF(p)$ (кольцом целых чисел Z_p), либо над расширениями полей с характеристиками два, три – $GF(2^k)$, $GF(3^k)$. Правильно выбранный порядок группы обеспечивает высокую стойкость криптографических конструкций к различным методам анализа.

ЭЦП на основе использования операций группы точек ЭК, определенной над конечным полем, является новым стандартом на ЭЦП в РФ ГОСТ Р 34.10-2001 [1]. Криптографическая стойкость схемы ЭЦП основывается на сложности решения задачи дискретного логарифмирования в группе точек ЭК, а также на стойкости используемой хэш-функции (ГОСТ Р 34.11-94).

При формировании цифровой подписи используются следующие параметры:

- простое число $p > 2^{255}$ – модуль ЭК;
- ЭК E, задаваемая коэффициентами $a,b \in GF(p)$ или инвариантом $J(E)$;
- целое число $m=\#e(GF(p))$ – порядок группы точек ЭК;

- простое число q - порядок циклической подгруппы группы точек ЭК, значение которого удовлетворяет условиям:

$$\begin{cases} m = nq, n \in Z, n \geq 1, \\ 2^{254} < q < 2^{256} \end{cases} \quad (1)$$

- точка $P \in E(GF(p))$ с координатами (x_p, y_p): $P \neq O, qP = O$;
- хэш-функция в соответствии с ГОСТ Р 34.11 $h(.): V_* \to V_{256}$, отображающая сообщения, представленные в виде двоичных векторов произвольной конечной длины, в двоичные векторы длины 256 бит;
- ключ подписи – целое число d: $0 < d < q$;
- ключ проверки подписи – точка $Q \in E(GF(p))$ с координатами (x_q, y_q): $dp = Q$.

Кроме того, на параметры схемы ЭЦП накладывается ряд ограничений:

- выполнение условия $p^t \neq 1 \pmod q$, для всех $t = 1, 2, ...B$, где B удовлетворяет равенству $b \geq 31$;
- выполнение неравенства $m \neq p$;
- выполнение условия $J(E) \neq 0$ или $J(E) \neq 1728$.

Алгоритм криптозащиты документа с помощью цифровой подписи состоит из двух частей: формирования и проверки ЭЦП. С использованием описанных выше параметров алгоритм формирования цифровой подписи использует в качестве исходных данных сообщение $M \in V_*$, ключ подписи d и выглядит следующим образом:

1. Вычисляется значение хэш-функции: $\bar{h} = h(M)$;
2. По двоичному значению вектора $\bar{h}$ вычисляется целое число a и определяется $e \equiv a \pmod q$. Если e = 0, то выполняется операция присваивания e = 1.
3. Генерируется случайное целое число k, удовлетворяющее неравенству $0 < k < q$.
4. Вычисляется точка ЭК C = kP и определяется $r \equiv x_C \pmod q$, где x_c – координата точки C. Если r = 0, то происходит возвращение к шагу 3.
5. Вычисляется значение $s \equiv (rd + ke) \pmod q$. Если s = 0 – возврат к шагу 3.
6. Вычисляются двоичные вектора и $\bar{s}$, соответствующие целым числам r и s.

В результате формируется ЭЦП в виде конкатенации двух двоичных векторов $\zeta = (\bar{r} \square \bar{s})$.

Алгоритм проверки цифровой подписи включает в себя следующие шаги:

1. По полученной подписи $\zeta = (\bar{r} \square \bar{s})$ вычисляются целые числа r и s. Если $0 < r < q$, $0 < s < q$, то происходит переход к следующему шагу. Иначе подпись неверна.
2. Вычисляется значение хэш-функции полученного сообщения M: $\bar{h} = h(M)$
3. По двоичному значению вектора $\bar{h}$ вычисляется целое число a и определяется $e \equiv a \pmod q$. Если e = 0, то выполняется присваивание e = 1.
4. Вычисляется значение $v \equiv e^{-1} \pmod q$.
5. Вычисляются значения $z_1 \equiv sv \pmod q$, $z_2 \equiv -rv \pmod q$.
6. Вычисляется точка ЭК $C = z_q P + z_2 Q$ и определяется значение $R \equiv x_C \pmod q$.
7. Если выполняется равенство R = r, то подпись верна, в ином случае, подпись неверна.

Одной из основных задач в арифметике эллиптических кривых является вычисление параметра kP. Вообще говоря, вычисление kP является самой трудоемкой операцией в протоколе ГОСТ Р 34.10-2001 из-за применения операции инверсии в конечном поле. Ускорение вычислений может быть достигнуто (кроме выделения случая, когда точка P известна заранее), выбирая k с числом единиц в диапазоне 40-60. Альтернативный подход к ускорению вычислений связан с использованием аффинных или проективных координат.

Первый способ требует не более $\log_2 t$ умножений многочленов на двойку и не более 40-60 операций сложения многочленов, однако, на каждом шаге необходимо выполнять обращение многочленов, что влечет за собой значительные временные потери.

Исключить операцию инверсии за счет увеличения общего числа умножений можно, переходя к проективной плоскости. Не считая сложений и возведений в степень, для сложения точек в проективных координатах необходимо выполнить 9 умножений (в аффинных координатах только 2), но зато ни одного обращения. При вычислении $1{,}7 \cdot 10^{18}$ мы последовательно удваиваем точки (что не требует инверсий), а затем складываем некоторые из них, накапливая результат в Q. Окончательный результат, полученный в проективных координатах, преобразуем в аффинные делением z_3^{-1} (одна инверсия в самом конце). Таким образом, использование проективных координат должно сократить время вычисления точки kP.

В рамках данного исследования была разработана программная библиотека, реализующая алгоритм ЭЦП ГОСТ Р 34.10-2001 с описанными выше модификациями.

Таблицы 1 и 2 демонстрируют разницу в вычислительной сложности самой ресурсоемкой задачи алгоритма – вычислении точки kP с помощью классического метода и метода проективных координат. Как видно, наиболее ресурсоемкими являются функции сложения и приведения к модулю, которые и являются основными операциями в классическом алгоритме вычисления kP.

Таблица 1. Количество операций и инструкций вычисления подписи с использованием классического метода вычисления kP

Операция	*Количество операций*	*Средний размер (инструкций)*	*Максимальный размер (инструкций)*
Сложение	456	505	519
Произведение	122	250	255
Инверсия	12	383	510
Другие	132	20	349

Таблица 2. Количество операций и инструкций вычисления подписи с использованием проективных координат для вычисления kP

Операция	*Количество операций*	*Средний размер (инструкций)*	*Максимальный размер (инструкций)*
Сложение	324	509	509
Произведение	63	254	255
Инверсия	12	383	510
Другие	82	20	249

В таблице 3 приведены сравнительные данные вычисления ЭЦП по алгоритму DSA (Digital Signature Algorithm) [2]. Алгоритм основан на трудности проблемы дискретного логарифма мультипликативной группы поля F_p. Уровень секретности определяется сложностью проблемы дискретного логарифма.

Как видно из таблиц 1 – 3, алгоритм ЭЦП на эллиптических кривых более эффективен в плане трудоемкости. К тому же, для обеспечения одного и того же уровня секретности для алгоритма ЭЦП, основанного на трудности дискретного логарифма, необходимо использовать ключи длиной более 500 бит, когда в то же время для алгоритма ЭЦП на эллиптических кривых достаточно 160 бит.

Таблица 3. Количество операций и инструкций вычисления подписи для алгоритма DSS

Операция	*Количество операций*	*Средний размер (инструкций)*	*Максимальный размер (инструкций)*
Сложение	324	509	509
Произведение	63	254	255
Инверсия	12	383	510
Другие	82	20	249

Данная программная библиотека была разработана на языке высокого уровня *Objective Caml*. Основываясь на статистических данных, приведенных в «The Computer Language Shootout Benchmarks» [3], мы перевели показания скорости исполнения в коэффициентах для языков C, C++ и Java, как наиболее распространенных. Данные сравнения скорости исполнения модифицированного алгоритма ГОСТ Р 34.10-2001 приведены в таблице 4.

Таблица 4. Скорость исполнения модифицированного алгоритма ГОСТ Р 34.10-2001 на различных языках программирования

Операция	*опер./мс*
Язык C. Подпись	0,19
Язык C. Проверка подписи	0,32
Язык C++. Подпись	0,10
Язык C++. Проверка подписи	0,16
Язык Java. Подпись	0,07
Язык Java. Проверка подписи	0,11

Эффективность протокола ГОСТ Р 34.10-2001 очень сильно зависит от выбора реализации алгоритмов вычисления операций над точками эллиптической кривой. В данной работе была показана неэффективность использования классического метода нахождения точки kP , как определяющего звена эффективности реализации.

Основными проблемами эффективности реализации ГОСТ Р 34.10-2001 следует считать:

- жесткая привязанность к алгоритму хэширования ГОСТ Р 34.11-94, что влечет за собой снижение скорости получения подписи, из-за попыток ликвидировать очевидные оплошности конструирования усложнением функции сжатия;
- отсутствие обоснования выбора конструкции, функций, констант;
- отсутствие строгого определения процесса генерации параметров схемы цифровой подписи.

Подобные проблемы ставят разработчика реализации алгоритма перед проблемой выбора способа, эффективного по скорости, и удовлетворительного по показателям стойкости.

ЛИТЕРАТУРЫ

1. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – М. Издательство стандартов, 2001. – 18 с.

2. Digital Signature Standard (DSS). – Federal Information Processing Standard 186-2. New-York. – National Institute of Standards and Technology, 2000.

3. The Computer Language Shootout Benchmarks // http://shootout.alioth.debian.org/ - 2005.