УДК 681.3.32

ИЛЬЯШЕВИЧ Д.А.

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

ОСОБЕННОСТИ ПРИМЕНЕНИЯ МЕТОДА ЭЛЛИПТИЧЕСКИХ КРИВЫХ ДЛЯ КРИПТОЗАЩИТЫ ДОКУМЕНТОВ

Целью настоящей работы является рассмотрение перспектив алгоритма эллиптических кривых на фоне сложившейся ситуации в области формирования электронной цифровой подписи документов.

С началом применения электронных способов передачи и обработки информации задачи криптографии начали расширяться. Широкое применение компьютерных технологий в системах обработки данных и управления привело к обострению проблемы защиты информации от несанкционированного доступа. Ситуацию усугубляет то, что информация, циркулирующая в компьютерных системах, обладает рядом специфических особенностей: не является жестко связанной с носителем, может легко и быстро копироваться и передаваться по каналам связи. Известно большое число угроз информации, которые могут быть реализованы как со стороны внешних, так и внутренних нарушителей [1].

Современные проблемы криптографии включают разработку систем электронной цифровой подписи и тайного электронного голосования, протоколов электронной жеребьевки и аутентификации удаленных пользователей, методов защиты от навязывания ложных сообщений и т.п.

Потребности современной практической информатики привели к возникновению нетрадиционных задач защиты электронных данных, одной из которых является аутентификация электронной информации в условиях, когда обменивающиеся этой информацией стороны не доверяют друг другу. Эта проблема связана с созданием систем электронной цифровой подписи. Теоретической базой для решения этой проблемы стало открытие в середине 1970-х годов американскими исследователями У. Диффи и М.Е. Хеллманом *двухключевой криптографии* [2].

Двухключевые криптоалгоритмы позволяют обеспечить строгую доказательность факта составления того или иного сообщения конкретными абонентами (пользователями) криптосистемы. Доказательство основано на том, что двухключевые криптосистемы функционируют в условиях, когда пользователю нет необходимости сообщать свой секретный ключ какому-либо второму субъекту. Факт использования секретного ключа при выработке подписи к тому или иному электронному документу проверяется с использованием *открытого* ключа. При этом знание открытого ключа не дает возможности выработать правильную цифровую подпись. Секретный ключ позволяет составить сообщение со специфической внутренней структурой, связанной с подписываемым документом и открытым ключом. Тот факт, что сообщение имеет структуру, сформированную с помощью секретного ключа, проверяется посредством открытого ключа. Эта процедура называется проверкой электронной цифровой подписи (ЭЦП). Вероятность того, что некоторое сообщение, подписанное каким-либо абонентом системы ЭЦП, является чрезвычайно низкой, порядка 10^{-30}.

Таким образом, процедура проверки ЭЦП с помощью открытого ключа позволяет с высокой степенью гарантии удостовериться в том, что полученное сообщение было составлено владельцем секретного ключа. Общедоступный открытый ключ формируется на основе секретного ключа или оба вырабатываются одновременно по специальным процедурам, причем определение секретного ключа по открытому ключу является вычислительно сложной математической задачей.

Существует достаточно большое количество различных систем электронной цифровой подписи. Отличаются они друг от друга трудновычислимой задачей, на основе которой получается пара ключей.

Например, криптосистема RSA [3] основывается на известной из теории чисел теореме Эйлера, согласно которой для любых взаимно простых чисел M и n, где M < n, выполняется соотношение $M^{\varphi(n)} = 1(\mathrm{mod}\, n)$. Условие взаимной простоты чисел M и n обеспечивается тем, что число n выбирается равным произведению двух больших простых множителей. В этом случае вероятность того, что случайное сообщение не будет взаимно простым с модулем, является пренебрежительно малым. Стойкость криптосистемы RSA основана на сложности разложения модуля на два больших простых множителя. Если задачу такого разложения удалось бы решить, то тогда можно было бы легко вычислить функцию Эйлера от модуля и затем, используя расширенный алгоритм Евклида, определить секретный ключ по открытому. До настоящего времени не найдены практически реализуемые общие способы решения этой задачи при длине модуля 512 бит и более. Считается, что криптосистема RSA обладает высокой стойкостью при длине модуля 1024 бита и более.

Проблема оценки сложности заключается в ее зависимости от алгоритма поиска решения. Для разных алгоритмов в общем случае получаются различные значения сложности. Для симметричной криптографии стойкость определяется временем полного перебора всех возможных ключей. В асимметричной же задача упрощается в зависимости от используемой трудновычислимой задачи.

В последние годы интенсивно развивается криптография эллиптических кривых (эллиптическая криптография) [4], где роль основной криптографической функции выполняет операция вычисления кратного точки эллиптической кривой, т.е. операция вычисления кратного точки эллиптической кривой (ЭК) на скаляр на основе умножений точек кривой. Последняя, в свою очередь, реализуется с использованием операций умножения, возведения в степень и инвертирования многочленов в поле Галуа $GF(2^n)$. Особый интерес к эллиптической криптографии за такой короткий срок обусловлен теми преимуществами, которые дает ее использование в беспроводных коммуникациях, – быстродействие и небольшая длина ключа. Например, в построенных на основе ЭК криптосистемах бинарной размерности в диапазоне от 150 до 350 обеспечивается уровень криптографической стойкости, который требует использования в известных криптосистемах бинарной размерности от 600 до 1400 и более.

Эллиптические кривые применяются в криптографии с 1985 года, причем в начале применялись лишь для факторизации чисел и проверки простоты. Только в последнее время намечаются попытки их использования и для построения криптографических протоколов.

Эллиптической кривой E над полем *F* называется гладкая кривая, задаваемая уравнением вида:

$$Y^2 + a_1XY + a_3Y = x^3 + a_2X^2 + a_4X + a_6, \quad a_i \in F. \tag{1}$$

Множество точек $(x,y) \in F^2$, удовлетворяющих этому уравнению, и содержащие кроме того бесконечную удаленную точку, обозначаемую *O*, будем обозначать εF. Если K – расширение поля F, то εK обозначает множество точек $(x,y) \in K^2$, удовлетворяющих (1) вместе с точкой O. Чтобы кривая (1) была эллиптической кривой в F^2 или в K^2, она должна быть гладкой. Это означает, что в F^2 или в K^2 не должно быть точек, в которых равны 0 обе частные производные. Иными словами, два уравнения:

$$a_1Y = 3X^2 + 2a_2X + a_4, \tag{2}$$

$$2Y + a_1X + a_3 = 0, \tag{3}$$

не должны иметь решения ни в одной точке $(x,y) \in E(F^2)$ или $(x,y) \in E(K^2)$.

С уравнением (1) можно связать дискриминант $\Delta = -16(4a^3 + 27b^2)$. Эллиптическая кривая над полем R с ненулевым дискриминантом, $\Delta \neq 0$, представляет собой гладкую кривую, в каждой точке которой можно провести касательную.

Рис. 1 демонстрирует геометрическую интерпретацию термина «эллиптическая кривая» и операций над ее точками.

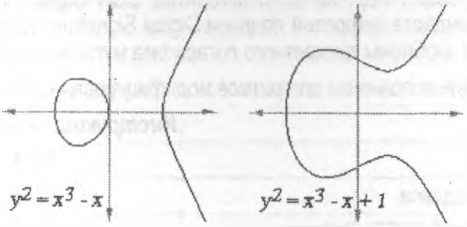

Рис. 1. Типичные эллиптические кривые над полем R

Если сравнить сложность задач факторизации целых чисел, дискретного логарифмирования в мультипликативных группах и дискретного логарифмирования в аддитивной абелевой группе точек ЭК, то последние выглядят предпочтительнее. Это показано в таблице 1, где предоставлено сравнение приблизительных оценок сложности криптоанализа методов, основанных на разложении целых чисел (РЦЧ), дискретном логарифмировании в конечном поле (ДЛКП) и дискретном логарифмировании в группе точек (ДЛГТ) ЭК для различных характеристик полей в зависимости от длины ключа.

Таблица 1. Приблизительная оценка сложности криптоанализа различных методов

Длина ключа (бит)	*Сложность анализа*			
	РЦЧ для $\forall p$	*ДЛКП для* $p = 2$	*ДЛКП для* $p \neq 2$	*ДЛГТ для* $\forall p$
100	$1{,}3 \cdot 10^{7}$	$1{,}3 \cdot 10^{7}$	$1{,}6 \cdot 10^{11}$	$1{,}1 \cdot 10^{15}$
200	$7{,}2 \cdot 10^{9}$	$7{,}2 \cdot 10^{9}$	$9{,}6 \cdot 10^{16}$	$1{,}3 \cdot 10^{30}$
300	$7{,}1 \cdot 10^{11}$	$7{,}1 \cdot 10^{11}$	$3{,}8 \cdot 10^{21}$	$1{,}4 \cdot 10^{45}$
400	$3 \cdot 10^{13}$	$3 \cdot 10^{13}$	$3{,}4 \cdot 10^{25}$	$1{,}6 \cdot 10^{60}$
500	$7{,}5 \cdot 10^{14}$	$7{,}5 \cdot 10^{14}$	$1{,}2 \cdot 10^{29}$	$1{,}8 \cdot 10^{75}$
600	$1{,}3 \cdot 10^{16}$	$1{,}3 \cdot 10^{16}$	$2{,}1 \cdot 10^{32}$	$2 \cdot 10^{90}$
700	$1{,}7 \cdot 10^{17}$	$1{,}7 \cdot 10^{17}$	$2{,}1 \cdot 10^{35}$	$2{,}3 \cdot 10^{105}$
800	$1{,}7 \cdot 10^{18}$	$1{,}8 \cdot 10^{18}$	$1{,}4 \cdot 10^{38}$	$2{,}6 \cdot 10^{120}$
900	$1{,}7 \cdot 10^{19}$	$1{,}7 \cdot 10^{19}$	$6{,}5 \cdot 10^{40}$	$2{,}9 \cdot 10^{135}$
1000	$1{,}3 \cdot 10^{20}$	$1{,}3 \cdot 10^{20}$	$2{,}3 \cdot 10^{43}$	$3{,}3 \cdot 10^{150}$

Принимая во внимание тот факт, что сложность выполнения преобразования в абелевой группе ЭК оценивается величиной $O(\log^2 q)$, а в мультипликативной группе поля – $O(\log^3 q)$, преимущества использования первых для построения криптосистем становятся очевидными.

Также необходимо отметить, что криптографические конструкции, сложность анализа которых превышает значение 10^{50}, нецелесообразно применять на практике [5], так как данные значения превосходят возможности современных технологий по обработке информации. Поэтому следует ограничиваться длиной ключа до 400 бит.

В рамках данного исследования было разработано программное обеспечение, реализующее одну из возможных разновидностей алгоритма ЭЦП на ЭК. В основу разработки положен ГОСТ Р 34.10-2001 [6], однако для вычисления шага нахождения точек ЭК использовался метод перехода к проективным координатам [4], а в качестве алгоритма хэширования использован приведенный в [7] Secure Hash Algorigthm – SHA (такое соче-

тание является наиболее эффективным из опробованных нами). Полученные результаты были проверены на скорость исполнения. В таблице 2 приведено сравнение скорости исполнения реализации ЭЦП на ЭК и алгоритма ЭЦП Digital Signature Algorithm (DSA) американского стандарта цифровой подписи Digital Signature Standard (DSS) [8], основанного на трудности проблемы дискретного логарифма мультипликативной группы поля F_p .

Таблица 2. Скорость исполнения алгоритмов модифицированного ГОСТ Р 34.10-2001 и DSA

Операция	***Инструкций на операцию***	***опер./мс***
DSA. Подпись	4444	0,11
DSA. Проверка подписи	2795	0,18
Модифицированный ГОСТ. Подпись	2629	0,19
Модифицированный ГОСТ. Проверка подписи	1618	0,31

Как видно из приведенных данных, реализованный алгоритм ЭЦП на ЭК показал на 65-70% лучшие результаты по скорости. К тому же для обеспечения равного уровня секретности для алгоритма не на ЭК необходимо использовать ключи длиной бинарной размерности более 500 бит, тогда как для алгоритма ЭЦП на ЭК достаточно 160 бит.

Таким образом, стойкость методов криптографического преобразования, основанных на использовании группового закона сложения элементов аддитивной абелевой группы на ЭК, существенно превосходит стойкость аналогичных методов, основанных на использовании мультипликативных полей. Выигрыш в стойкости особенно заметен при больших размерах ключа. Данное обстоятельство позволяет использовать криптографические конструкции подобного типа для построения криптографических протоколов различного назначения. Поэтому, несмотря на широкое распространение менее перспективных, но стандартизованных алгоритмов, а также медленный процесс обновления государственных стандартов, перспективы внедрения алгоритмов ЭК для криптостойкой защиты документов представляются весьма высокими.

ЛИТЕРАТУРА

1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. – М.: Энергоатомиздат, 1994. – 576 с.

2. Diffie W., Hellman M.E. New Directions in Cryptography// IEEE Transaction on Information Theory. – 1976. – V. IT-22. № 6. – P. 644–654.

3. Rivest. R.L., Shamir A., Adleman L. A method for Obtaining Digital Signatures and Public-Key Cryptosystems // Communication of the ACM. – 1978. – V. 21. – N. 2. – P. 120–126.

4. Rosing M. Implementing Elliptic Curve Cryptography. Manning, 1999.

5. Столлингс В. Криптография и защита сетей: принципы и практика., 2-е изд.: Пер. с англ. – Изд. дом «Вильямс», 2001. – 672 с.: ил.

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

7. Secure Hash Standard. Federal Information Processing Standard 180-2. New-York. – National Institute of Standards and Technology, 1995.

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