УДК 681.3

ИСПОЛЬЗОВАНИЕ СИЛЬНЫХ ПРОСТЫХ ЧИСЕЛ ПРИ КРИПТОПРЕОБРАЗОВАНИЯХ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

к.т.н. В.Н. Федорченко, А.А. Смирнов, Н.С. Гончарко
(представил д.т.н., проф. Ю.В. Стасев)

В статье рассмотрен один из подходов генерации системных параметров для преобразований в группе точек эллиптической кривой. Предложено использование сильного простого числа для формирования системных параметров. Предлагается методика вычисления простого сильного числа, позволяющая уменьшить вычислительные затраты на формирование цифровой подписи.

Постановка проблемы. На данный момент актуальна проблема развития, совершенствования и внедрения национальных автоматизированных систем управления и связи (АСУС). Исходя из этого, возникает необходимость решать задачи защиты информации, а именно обеспечение целостности, конфиденциальности, причастности и достоверности данных, циркулирующих в АСУС. Опыт применения и проведенные исследования [1] показали, что решение задач защиты информации, особенно по реализации функции причастности, может быть обеспечено за счет применения цифровой подписи (ЦП). Одним из криптографических алгоритмов, реализующих ЦП, является алгоритм, использующий преобразования в группе точек эллиптической кривой. Основным достоинством данного класса криптопреобразований является то, что при меньшем размере ключа обеспечивается большая степень защиты информации. Стойкость криптосистемы на эллиптических кривых основана на трудности решения проблемы дискретного логарифма (ECDLP). Проблема дискретного логарифма на эллиптической кривой сформулирована следующим образом: дана базовая точка G на эллиптической кривой и другая точка Y на этой же кривой, необходимо найти единственное число x такое, что Y = xG. Таким образом, при построении эллиптической кривой необходимо выбирать параметры, которые не позволят эффективно решить проблему дискретного логарифма, и, следовательно, повысят стойкость цифровой подписи.

Анализ литературы. Анализ литературы [2 – 5] показал, что в качестве

порядка базовой точки и порядка эллиптической кривой целесообразно использовать большие простые или почти простые числа (т.е. такие, в разложении которых есть большое простое число).

Целью данной статьи является разработка методики формирования сильных простых чисел для генерации порядка базовой точки и эллиптической кривой, а также метода уменьшения количества операций при нахождении таких чисел.

Основной материал. Предлагается для повышения стойкости цифровой подписи, основанной на криптографических преобразованиях в группе точек эллиптической кривой, вместо простых чисел использовать сильные простые числа, так как использование таких чисел позволит усложнить решение задачи нахождения дискретного логарифма.

Как показано в [6, 7, 9], сильным простым числом называется целое число p, обладающее следующими свойствами:

– p является простым числом;

– $p-1$ содержит в своем разложении большой простой сомножитель (скажем t);

– $p+1$ содержит в своем разложении большой простой сомножитель;

– $t-1$ содержит в своем разложении большой простой сомножитель;

Авторами предлагается следующая методика, которая может применяться в настоящее время.

1. Алгоритм формирования сильного простого числа вида $p = p_0 + 2ks$ заключается в выполнении следующих операций:

1а. В соответствии с алгоритмами, описанными в [6, 7], производится нахождение простого числа s, причем размер s должен быть на несколько бит меньше половины размера p.

1б. Согласно методам, описанным в [6, 7], производится нахождение простого числа t (размер t на несколько бит меньше размера s).

1в. Необходимо найти простое число r формы $2Lt+1$. Метод заключается в поиске в $2Lt+1$ пространстве последовательных значений L. Таким образом, поиск простого числа r производится в соответствии с методами нахождения простых чисел [6, 7]. Проверяемым на простоту числом является число вида $2Lt+1$, L = 1, n, причем увеличение значения L на 1 происходит вместо увеличения p на 2, предусмотренного алгоритмом вероятностного теста [3].

2. При полученных r и s необходимо найти простое число p, близкое по размеру к заданному и удовлетворяющему требованиям к сильному простому числу, изложенным в [6 – 10].

Для нахождения числа p в соответствии с [1, 9, 10], необходимо выполнить ряд промежуточных вычислений:

2а. Вычисляется U(r,s) в соответствии с выражением

$$U(r,s) = \left| s^{r-1} (\mathrm{mod}\, rs) - r^{s-1} (\mathrm{mod}\, rs) \right| .$$

2б. Вычисляется p_0 следующим образом:

$$p_0 = \begin{cases} U(r,s) & \text{ïðè} \quad U(r,s) \equiv 1 (\mathrm{mod}\, 2); \\ U(r,s) + rs & \text{ïðè} \quad U(r,s) \equiv 0 (\mathrm{mod}\, 2). \end{cases}$$

2в. Поиск искомого числа p производится по формуле

$$p = p_0 + 2krs ,$$

где k = 1, n.

Иными словами, необходимо найти простое число p в ($p_0 + 2krs$) пространстве. Поиск осуществляется аналогично этапу 2б.

2г. Проверяются свойства сильного простого числа [6, 7, 9].

Для реальных подсистем защиты информации АСУС важным требованием является сокращение вычислительных (временных) затрат при формировании сеансовых ключевых данных используемых криптоалгоритмов. Предлагается незначительно сократить вычислительные затраты на нахождение сильного простого числа p, путем замены двух операций возведения в степень по модулю, на этапе нахождения p_0, одной. Согласно вышесказанному

$$U(r,s) = s^{r-1} (\mathrm{mod}\, rs) - r^{s-1} (\mathrm{mod}\, rs) = s^{r-1} - r^{s-1} + krs . \qquad (1)$$

Пусть $x(\mathrm{mod}\, rs) = \{a, b\}$, где $a = x(\mathrm{mod}\, r)$, $b = x(\mathrm{mod}\, s)$, тогда, в соответствии с теоремой Эйлера:

$$r^{s-1} (\mathrm{mod}\, s) = 1 ; \; s^{r-1} (\mathrm{mod}\, r) = 1 , \text{ и } r^{s-1} (\mathrm{mod}\, r) = 0 ; \; s^{r-1} (\mathrm{mod}\, s) = 0 .$$

Следовательно:

$$r^{s-1} (\mathrm{mod}\, rs) = \{0,1\} ; \; s^{r-1} (\mathrm{mod}\, rs) = \{1,0\} ,$$

тогда:

$$r^{s-1} + s^{r-1} \equiv 1 (\mathrm{mod}\, rs) ; \quad r^{s-1} \equiv 1 - s^{r-1} (\mathrm{mod}\, rs) . \qquad (2)$$

Соответственно, подставляя (2) в (1), получим:

$$U(r,s) = 2 \cdot s^{r-1} - 1 + krs .$$

Выводы. Предлагаемая методика нахождения сильных простых чисел позволяет повысить стойкость цифровой подписи, основанной на преобразованиях в группе точек эллиптической кривой, а также заменить две вычислительно сложные операции дискретного возведения в степень одной, что дает выигрыш в вычислительных (временных) затра-

тах при формировании системных параметров. Однако отметим, что параллельно с развитием криптографических систем интенсивно развиваются математические методы криптоанализа, что влечет за собой повышение (пересмотр) требований к стойкости криптосистем, в частном случае к цифровой подписи. Поэтому проблема формирования общесистемных параметров эллиптической кривой, обеспечивающих необходимую стойкость цифровой подписи, требует дальнейших исследований в данной области.

ЛИТЕРАТУРА

1. *Симмонс Г.Дж. Обзор методов аутентификации информации // ТИИЭР, май 1988. – Т. 76. – № 5. – С. 105 – 125.*
2. *Menezes A.J., Vanstone S., Okamoto T.: Reducing elliptic curve logarithms to logarithms in a finite field // Proc. of STOC'91 (1991). – P. 80 – 89.*
3. *Pohlig S.C., Hellman M.E.: An improved algorithm for computing logarithm over GF(p) // IEEE Trans. Information Theory, IT-24, 1 (1978). – P. 106 – 110.*
4. *Adleman L.M.: A subexponential algorithm for the discrete logarithm problem with applications to cryptography // Proc. of IEEE 20th Symp. on Foundations of Comp. Sci. (1979.) P. 55 – 60.*
5. *Koblitz N.: Elliptic curve implementation of zero-knowledge blobs // Journal of Cryptology, vol. 4, No. 3 (1991). – P. 207 – 213.*
6. *Виноградов И.М. Основы теории чисел. – М.: Наука, 1981. – 176 с.*
7. *Кнут Д. Искусство программирования для ЭВМ. Т. 2. Получисленные алгоритмы / Под ред. К.И. Бабенко. – М.: Мир, 1977. – 724 с.*
8. *Knuth D. E. The art of computer programming // Sorting and searching, vol. 3, Addison Wesley (1973).*
9. *Gordon J., Strong Primes are Easy to Find // Lecture Notes in Computer Science. Edited by G. Goods, Advances in Cryptology – EUROCRYPT`84, W.Berlin, Springer-Verlag, 1985. – P. 215 – 223.*
10. *Davis J., Holdrige D., Simmons G. Status Report on Factoring // Lecture Notes in Computer Science. Edited by G .Goods and J. Hartmanis, Advances in Cryptology – EUROCRYPT`84. Springer-Verlag, Berlin, Heidelberg, NewYork, Tokyo. 1985. – P. 183 – 215.*

Поступила 17.10.2003

***ФЕДОРЧЕНКО Владимир Николаевич**, кандидат технических наук, старший преподаватель кафедры ХВУ. Окончил ХВВКИУ РВ в 1989 году. Область научных интересов – защита информации в автоматизированных системах управления и сетях.*

***СМИРНОВ Алексей Анатольевич**, адъюнкт ХВУ. В 1999 году окончил ХВУ. Область научных интересов – защита информации в автоматизированных системах управления и сетях.*

***ГОНЧАРКО Наталья Станиславовна,** начальник отделения учебной лаборатории кафедры ХВУ. В 1999 году окончила ХВУ. Область научных интересов – защита информации в автоматизированных системах управления и сетях.*