Math-Net.Ru

Общероссийский математический портал

А. Б. Спельников, Эллиптическая пороговая схема разделения секрета, *Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки*, 2009, выпуск 1(), 251–259

DOI: <https://doi.org/10.14498/vsgtu614>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.92.164.108

26 апреля 2023 г., 14:07:18

Информатика

УДК 519.68:612.8.001.57

ЭЛЛИПТИЧЕСКАЯ ПОРОГОВАЯ СХЕМА РАЗДЕЛЕНИЯ СЕКРЕТА

А. Б. Спельников

Северо-Кавказский государственный технический университет,
355029, г. Ставрополь, просп. Кулакова, 2.

E-mail: fissy_run@mail.ru

Разработан новый аспект реализации систем разделения секрета, в основу которого положена арифметика эллиптических кривых. Предложена нейросетевая модель $(k; t)$ схемы разделения секрета на эллиптической кривой. Разработан механизм пролонгации полученной схемы. Предложена нейросетевая модель восстановления общего секрета, а также разработана методика построения и протокол функционирования схемы разделения секрета. Выполнен расчёт оценки безопасного времени существования настроек генератора секретов.

Ключевые слова: нейронная сеть конечного кольца, схема разделения секрета, система остаточных классов, эллиптические кривые.

Сложность современных информационных систем требует особого подхода к проблематике сохранения и доступа к информации. Проблема распределения ключей является наиболее острой в современной криптографии. Одним из ее решений выделяют [1] использование «блуждающих ключей», основная задача которых — выбор эффективного правила смены сеансовых ключей для обоих участников криптографической схемы.

Усложнением метода «блуждающих ключей» является его применение для структуры доступа криптографической схемы разделения секрета.

Схема разделения секрета позволяет распределить секрет между участниками таким образом, чтобы заранее заданные разрешённые множества участников могли однозначно восстановить секрет, а неразрешённые — не получали никакой дополнительной к имеющейся априорной информации о возможном значении секрета. Разделение секрета применяется в достаточно широкой области задач: динамическое распределение данных по каналам при передаче; разделённое хранение данных; управление ключами в протоколах, содержащих большое количество участников; безопасная коллективная подпись [2].

Пусть E — эллиптическая кривая, определённая в конечном поле F_p . Применение эллиптических кривых в криптографических целях определяется в [3].

В [2, 4] свойства точек эллиптической кривой определяются как свойства аддитивных абелевых групп. Соответственно для них определяются операции сложения:

$$P(x, y) = P_1(x_1, y_1) + P_2(x_2, y_2). \quad (1)$$

Спельников Алан Борисович — аспирант кафедры информационных систем и технологий.

Рис. 1. Условное графическое отображение сумматора на эллиптической кривой

Рис. 2. Условное графическое отображение умножителя на эллиптической кривой

На рис. 1 представлено условное графическое отображение операции сложения.

Для точек эллиптической кривой значимой также является операция умножения точки на число:

$$P(x, y) = k \cdot P_1(x_1, y_1). \quad (2)$$

На рис. 2 представлено условное графическое отображение операции умножения.

Приведенное представление операций на эллиптической кривой позволяет провести аналогию с математическим аппаратом нейронных сетей конечного кольца и его адаптацией для систем разделения секрета. Выражение (1) описывает суммирование на нейроне, выражение (2) — весовую операцию.

Усложнением классической схемы разделения секрета является пороговая схема разделения секрета, для которой определяется структура доступа — совокупность участников, объединение которых позволит сформировать правильный общий секрет. Объединение меньшего числа участников не приведёт к получению сколь-либо определённого результата.

Очевидно, что применяя (1) и (2), а также аппарат нейронных сетей, можно сформировать полином следующего вида:

$$S = P_0 + tP_1 + t^2P_2 + \dots + t^{k-1}P_{k-1}, \quad (3)$$

где $P_1, P_2, \dots, P_{k-1}$ — случайные точки на эллиптической кривой, P_0 — общий секрет.

Выражение (3) описывает некий условный полином, состоящий из координат точек, операции над которыми выполняются по правилам сложения точек на эллиптической кривой.

Пусть $t_i^j = w_{ji}$, тогда можем сформировать матрицу весовых коэффициентов нейронной сети

$$W = \begin{pmatrix} w_{00} & w_{01} & : & w_{0(k-1)} \\ w_{10} & w_{11} & : & w_{1(k-1)} \\ \dots & \dots & \ddots & \dots \\ w_{(m-1)0} & w_{(m-1)1} & : & w_{(m-1)(k-1)} \end{pmatrix} = \begin{pmatrix} 1 & t_0 & : & t_0^{k-1} \\ 1 & t_1 & : & t_1^{k-1} \\ \dots & \dots & \ddots & \dots \\ 1 & t_{m-1} & : & t_{m-1}^{k-1} \end{pmatrix}. \quad (4)$$

Частные секреты получаем, подставляя в выражение различные t . Пусть i — номер абонента, которому отсылается секрет. Тогда частные секреты абонентов равны

$$S_i = P_0 + iP_1 + i^2P_2 + \dots + i^{k-1}P_{k-1}.$$

Выражение (4) примет вид

$$W = \begin{pmatrix} 1 & i_0 & : & i_0^{k-1} \\ 1 & i_1 & : & i_1^{k-1} \\ \dots & \dots & \ddots & \dots \\ 1 & i_{m-1} & : & i_{m-1}^{k-1} \end{pmatrix}.$$

На рис. 3 представлена нейронная сеть конечного кольца генератора частных секретов.

Рис. 3. Эллиптический генератор частных секретов

Частные секреты передают абонентам по закрытому каналу по следующей методике:

- 1) сервер случайным образом выбирает точку B эллиптической кривой и число d , после чего публикует B и $C = dB$;
- 2) абоненты случайным образом выбирают числа k_i и публикуют $K_i = k_i B$;
- 3) сервер публикует точки, найденные в соответствии с выражением $M_i = S_i + dK_i$;
- 4) абоненты вычисляют $S_i = M_i - k_i C$.

Восстановление общего секрета. Рассмотрим пороговую $(k; m)$ схему.

Частные секреты абонентов в общем случае получаются в соответствии с выражением

$$S_j \Big|_0^{m-1} = \sum_{i=0}^{k-1} P_i t_j^i, \quad (5)$$

где m — общее количество секретов на первом шаге, j — номер секрета.

Для структуры доступа выражение (5) преобразуется к виду

$$S_j \Big|_0^{k-1} = \sum_{i=0}^{k-1} P_i t_j^i = \sum_{i=0}^{k-1} P_i (k_i)_j.$$

Найдём общее выражение. Пусть на первом шаге

$$\begin{aligned} S_{1,j} \Big|_0^{k-2} &= S_j(k_1)_{j+1} - S_{j+1}(k_1)_j = \\ &= \sum_{i=0}^{k-1} P_i ((k_i)_j (k_1)_{j+1} - (k_i)_{j+1} (k_1)_j) = \sum_{i=0}^{k-1} P_i (k_2)_j. \end{aligned}$$

При этом, в силу приведенной операции, слагаемое при $i = 1$ равно нулю.

Путём аналогичных преобразований окончательно можно получить

$$R = S_{k-1,j} = S_{k-2,j}(k_{k-1})_{j+1} - S_{k-2,j+1}(k_{k-1})_j = P_0 k_k.$$

Значения R и k_k и есть восстановленный секрет.

На рис. 4 представлена модель сети генератора общего секрета по известным частным.

Рис. 4. Модель сети генератора общего секрета

Рассмотрим методику пролонгации полученной схемы разделения секрета. Для генерации нового частного секрета воспользуемся возможностью умножения точки на число на эллиптической кривой.

Процесс пролонгации секрета со стороны абонента состоит в получении шага пролонгации, умножении шага на внутреннюю константу и умножении полученного результата на известный частный секрет, что можно выразить по формуле

$$S_{i,v+1} = (gv)S_{i,v}. \quad (6)$$

Для сервера имеем:

$$\begin{aligned} S_{v+1} &= gv(P_{0,v} + tP_{1,v} + t^2P_{2,v} + \dots + t^{k-1}P_{k-1,v}), \\ S_{v+1} &= (gvP_{0,v}) + t(gvP_{1,v}) + t^2(gvP_{2,v}) + \dots + t^{k-1}(gvP_{k-1,v}), \end{aligned}$$

Примем $gvP_{i,v} = P_{i,v+1}$ для всех i от 0 до $m - 1$. Тогда

$$S_{v+1} = P_{0,v+1} + tP_{1,v+1} + t^2P_{2,v+1} + \dots + t^{k-1}P_{k-1,v+1}.$$

Алгоритм функционирования системы разделения секрета.

1. Определяются параметры схемы: полное число участников m , пороговое число участников k , основание p схемы, эллиптическая кривая E .

2. Случайным образом главный сервер выбирает точку-ключ P_0 и точки $P_1, P_2, \dots, P_k$ на эллиптической кривой.
3. Главный сервер рассчитывает частные секреты. Полученные данные шифруются и рассылаются абонентам.
4. Главный сервер случайным образом выбирает шаг синхронизации g и секретно рассылает его абонентам.

Алгоритм функционирования системы пролонгированной безопасности.

1. Главный сервер случайным образом выбирает шаг пролонгации t и рассылает его абонентам.
2. Главный сервер находит новое значение секрета.
3. Абоненты рассчитывают новые значения частных секретов в соответствии с известными параметрами.

Численный пример. Рассмотрим (3; 5) схему разделения секрета. Опирируем точками эллиптической кривой вида $y^2 = x^3 + 21x + 17$, определённой в поле порядка $p = 1361$.

Главный сервер выбирает секретные точки $P_0 = (62; 887)$, $P_1 = (1105; 605)$, $P_2 = (584; 515)$.

Сервер рассчитывает секреты:

$$\begin{aligned} S_0 &= (62; 887) + (1105; 605) + (584; 515) = (641; 1260), \\ S_1 &= (62; 887) + 2 \cdot (1105; 605) + 4 \cdot (584; 515) = (670; 936), \\ S_2 &= (62; 887) + 3 \cdot (1105; 605) + 9 \cdot (584; 515) = (46; 975), \\ S_3 &= (62; 887) + 4 \cdot (1105; 605) + 16 \cdot (584; 515) = (1344; 1311), \\ S_4 &= (62; 887) + 5 \cdot (1105; 605) + 25 \cdot (584; 515) = (789; 146). \end{aligned}$$

Сервер выбирает коэффициент синхронизации $g = 211$, и полученные значения секретно отправляются абонентам.

Рассмотрим один шаг пролонгации схемы.

Сервер публикует шаг синхронизации $v = 327$.

Сервер рассчитывает $P_{0,v+1} = gvP_{0,v} = 947 \cdot (62; 887) = (397; 460)$.

Абоненты рассчитывают новые частные секреты:

$$\begin{aligned} S_{0,v+1} &= gvS_{0,v} = 947 \cdot (641; 1260) = (836; 55), \\ S_{1,v+1} &= gvS_{1,v} = 947 \cdot (670; 936) = (908; 321), \\ S_{2,v+1} &= gvS_{2,v} = 947 \cdot (46; 975) = (454; 965), \\ S_{3,v+1} &= gvS_{3,v} = 947 \cdot (1344; 1311) = (917; 74), \\ S_{4,v+1} &= gvS_{4,v} = 947 \cdot (789; 146) = (674; 664). \end{aligned}$$

Произведём оценку безопасного времени существования настроек генератора секретов. При этом будем исходить из наихудшего предположения, что противник (нарушитель) на данном этапе функционирования схемы обладает знанием двух незашифрованных частных секретов нескомпрометированного генератора секретов, то есть имеет возможность каким-либо способом расшифровать передаваемые частные секреты и пытается скомпрометировать скрытый параметр генератора в соответствии с выражением (6). Тогда при использовании метода последовательных сложений и умножений точек период полуперебора ключей составит $T = \frac{(p-2)T_1}{2}$, где p — модуль эллиптической кривой, T_1 — среднее время, затрачиваемое на одну операцию сложения или удвоения точек.

Для современных вычислителей характерна суперскалярная конвейерная архитектура, для которой усредняется процессорное время на выполнение операций сложения, умножения, записи и считывания.

При использовании проективных координат для чисел разрядности 256 известна формула для объёма вычислений сложения и удвоения точек на эллиптической кривой:

$$S_e = 12M_{256} + 2S_{256}, \quad U_e = 7M_{256} + 5S_{256}.$$

Принимая во внимание алгоритмы умножения чисел большой разрядности, учитывая разрядность и производительность рассмотренных вычислителей и учитывая, что на умножение и сложение тратится одинаковое процессорное время, ориентировочно получим

$$S_e = 768M_{32} + 1552S_{32} = 2320, \quad U_e = 448M_{32} + 929S_{32} = 1377.$$

Учитывая, что количества сложений и умножений точек в алгоритмах для эллиптических кривых приблизительно равны, получим среднюю сложность

$$M_s = \frac{(S_e + U_e)}{2}.$$

Тогда среднее время на одну операцию сложения или удвоения определится из выражения

$$T_1 = \frac{(S_e + U_e)}{2f},$$

где f — количество универсальных операций, выполняемых вычислителем в секунду.

Учитывая, что $p > 2^{n-1}$ (см., например, [3]), получим

$$T = (2^{n-1} - 2) \frac{(S_e + U_e)}{4f} \approx \frac{2^{n-3}(S_e + U_e)}{f}. \quad (7)$$

Подставляя в выражение (7) скоростные характеристики проекта **Folding@home** ($f = 2,5 \cdot 10^6$ GIPS), получим $T = 2,14 \cdot 2^{64}$ с или $T = 6,79 \cdot 2^{56}$ лет, что представляется безопасным.

Использование вычислительных комплексов и средств распределённых вычислений, а также специализированных методов, способно уменьшить это соотношение, однако даже в наихудшем случае это не представляет опасности.

В соответствии с полученными расчётами можно сделать вывод, что разработанная схема разделения секрета не требует реинициализации внутренних параметров в период функционирования.

Оценка вычислительной нагрузки при выполнении основных операций разработанной модели.

Сложение двух чисел с редукцией можно выразить по формуле [5]:

$$S_C \approx 2n.$$

Известно [5], что при использовании алгоритма Тоома—Кука затраты на умножение

$$M_{TK} = n2^{\sqrt{2\log_2 n}} \log_2 n.$$

Соответственно при использовании метода Монтгомери получим

$$M_C = 2M_{TK} + 2n = 3n2^{\sqrt{2\log_2 n}} \log_2 n + 2n.$$

При использовании проективных координат и якобиана перехода вычислительная сложность сложения двух точек эллиптической кривой [6]

$$S_P = 4M_C + 6S_C.$$

Основываясь на [2, 6], можно получить выражение для расчёта вычислительной сложности умножения в проективных координатах и с использованием метода «окон»:

$$M_P = (n-1)(12M_C + 4S_C) + \left(\frac{n}{w} - 1\right)(4M_C + 6S_C),$$

где w — размер «окна», обычно $w = 4$.

Вычислительные затраты разработанной модели при пролонгации секретов абонентами можно рассчитать по формуле

$$M_{PE} = M_P + M_C,$$

Рис. 5. Зависимость вычислительной сложности алгоритма от разрядности оперируемых чисел

где M_P — затраты на умножение точки эллиптической кривой на число, M_C — затраты на модульное умножение двух чисел.

Отметим, что для схемы с «блуждающими» ключами производительность пролонгации не зависит от количества абонентов.

Найдем выражение для расчёта вычислительной сложности схемы, представленной в [7]:

$$M_{PO} = (k-1)(m-1)M_C + (k-2)(m-1)S_C + m(2M_P + 2S_P) + (k-1)S_C. \quad (8)$$

В (8) первое и второе слагаемые обусловлены генерацией абонентом данных для пролонгации, третье слагаемое выражает вычислительную сложность шифрования (с использованием эллиптических кривых), последнее слагаемое — получение нового секрета.

На рис. 5 представлена зависимость вычислительной сложности от разрядности чисел для разработанной схемы (M_{PE}) и схемы Шамира при различных k и m (3, 5 и 7 участников соответственно в графиках СШЗ, СШ5, СШ7).

Как видно, использование предложенной схемы позволяет добиться многократного снижения вычислительной нагрузки на абонентов при выполнении основной операции — пролонгации даже на пороговых схемах с малым числом абонентов.

Таким образом, разработанная схема позволяет абонентам удостоверять полученный частный секрет и обновлять его независимо друг от друга. Интересным следствием разработки является возможность идентифицировать группы пользователей при передаче вспомогательной переменной i_s серверу в процессе аутентификации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Баричев С. Г. Криптография без секретов. — М.: Наука, 1998. — 105 с.
2. Ростовцев А. Г., Маховенко Е. Б. Теоретическая криптография. — СПб.: Профессинал, 2005. — 478 с.
3. ГОСТ Р 34.10–2001. Процессы формирования и проверки электронной цифровой подписи. — Взамен ГОСТ 34.10–94; Введ. 12.09.2001. — М.: Изд-во стандартов, 2001.
4. Коблиц Н. Введение в эллиптические кривые и модулярные формы: пер. с англ. — М.: Мир, 1988. — 320 с.
5. Василенко О. Н. Теоретико числовые алгоритмы в криптографии. — М.: МЦНМО, 2003. — 328 с.
6. Cohen H., Miyaji A., Ono T. Efficient Elliptic Curve Exponentiation Using Mixed Coordinates / In: *Advances in Cryptology – ASIACRYPT’98*: Proc. of the Int. Conf. on the Theory and Applications of Cryptology and Information Security: Advances in Cryptology / Lecture Notes in Computer Science. — Berlin / Heidelberg: Springer, 1998. — Vol. 1514. — P. 51–65.
7. Herzberg A., Jarecki S., Krawczyk H., Yung M. Proactive secret sharing or how to cope with perpetual leakage / In: *Proc. of CRYPTO ’95*: Lecture Notes in Comp. Sci., Springer-Verlag, 1995. — Vol. 963. — P. 339–352.

Поступила в редакцию 30/VI/2008;
в окончательном варианте — 03/III/2009.

MSC: 14H52, 12E20

ELLIPTIC THRESHOLD SECRET DIVISION SCHEME

A. B. Spelnikov

North Caucasus State Technical University,
2, pr. Kulakova, Stavropol', 355029.

E-mail: `fiss_run@mail.ru`

The new aspect of proactive systems realization was developed based on elliptic curves arithmetic. Neural network model of secret division scheme at elliptic curve is introduced. Prolongation mechanism of the scheme was developed. Neural network model of secret regeneration is introduced. Method of construction and functioning report of the scheme were developed. Calculation of safe time period of secret generator settings existence is introduced. Calculation of complexity and time needed for prolongation of this model is introduced.

Key words: *neural network of a final ring, secret sharing schemes, system of residual classes, elliptic curves.*

Original article submitted 30/VI/2008;
revision submitted 03/III/2009.

Spel'nikov Alan Borisovich, Postgraduate Student, Dept. of Information Systems and Technologies.