УДК 512.6, 519.165, 519.725

Н.В. Медведев, С.С. Титов

Почти пороговые схемы разделения секрета на эллиптических кривых

Работа посвящена исследованию схем разделения секрета при помощи многочленов на эллиптических кривых. Изучены структуры доступа и основные свойства таких схем. Доказана теорема о неразрешенных коалициях, приведен пример.

Ключевые слова: схема разделения секрета, эллиптические кривые, многочлены, структура доступа, пороговые схемы, циклы, матроиды, конечные поля.

Схема разделения секрета (СРС) включает в себя дилера, формирующего секрет, и участников, получающих долю от этого секрета [1, 2]. Только объединившись, n участников пороговой схемы «n из N» могут восстановить секрет. Эту СРС описал Ади Шамир [3]. Он использовал многочлен, который может быть построен по n точкам, определяемым координатами из конечного поля. Таким образом, в СРС Шамира участники параметризуются элементами данного конечного поля, что геометрически означает ось абсцисс, а также еще одного «несобственного» участника, соответствующего «бесконечно удаленной» точке. В данной работе, в развитие статьи [4], предлагается использовать эллиптическую кривую и точки на ней для параметризации участников и исследуются свойства получающейся СРС.

Разделение секрета на эллиптической кривой происходит по следующему алгоритму: дилер выбирает эллиптическую кривую EC с необходимым количеством точек (не менее N). Каждому из участников СРС (в том числе хранителю секрета) ставится в соответствие точка на эллиптической кривой, включая «бесконечно удаленную». Затем дилер выбирает многочлен степени n на этой кривой. Коэффициенты данного многочлена известны только ему. Точка на эллиптической кривой, которая обозначает участника – хранителя секрета, известна всем. Дилер подставляет координаты этой точки в выбранный им многочлен, вычисляет значение секрета. Для того чтобы каждому участнику раздать свою долю секрета, дилер подставляет координаты точки участника в многочлен, получая долю секрета для него. В итоге участник имеет точку на эллиптической кривой (login) и долю секрета (password). Для восстановления секрета нескольким участникам необходимо объединиться, чтобы восстановить коэффициенты выбранного дилером многочлена. Математически это сводится к решению некоторой системы уравнений. Участники, составляющие разрешенную коалицию, получают искомый многочлен, куда подставляют координаты точки, обозначающей секрет. В итоге они получают секрет, который сформировал дилер [4].

Исследования требуют следующих свойств СРС: идеальность, линейность, совершенность и пороговость. СРС – идеальная, т.к. каждому из участников дается одинаковый размер доли секрета. Как известно [1, 5, 6], разрешенные коалиции идеальной схемы определяются циклами некоторого связного матроида, изучение которого и дает структуру доступа. Схема совершенная следует из ее линейности. Линейность и пороговость рассматриваются ниже.

Конструкция СРС

Напомним [7, 8], что в случае произвольного поля всякую эллиптическую кривую можно преобразовать к виду

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6. \quad (1)$$

Дискриминант определяется следующим образом:

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \quad (2)$$

где $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$, $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$ [7].

Над полем характеристики, не равной двум, эллиптическая кривая (1) может быть приведена к виду $y^2 = x^3 + ax^2 + bx + c$.

Теорема Хассе об эллиптических кривых утверждает, что количество N точек на эллиптической кривой $EC(GF(q))$ близко к мощности q конечного поля:

$$(\sqrt{q}-1)^2 \le \left|EC(GF(q))\right| \le (\sqrt{q}+1)^2. \quad (3)$$

В общем виде многочлен, который выбирает дилер, имеет вид $F(P)=\alpha(x)+\beta(x)y$, где $\alpha(x)$, $\beta(x)$ – многочлены над полем $GF(q)$. Степень многочлена F определяется по формуле $\deg F = \max\{2\deg\alpha, 2\deg\beta+3\}$. Если $F(P)=0$, то точка $P=(x,y)\in EC$ называется корнем многочлена. Так, для аналога схемы Шамира схемы «5 из N» необходимо задать многочлен степени пять. В общем виде многочлен степени, равной либо меньшей 5, имеет вид $F=\alpha(x)+\beta(x)y$, где $\alpha(x)=Ax^2+Bx+C$, $\beta(x)=Dx+E$. Здесь $A,B,C,D,E\in GF(q)$ и $\deg F=5$ при $D\neq 0$.

Доли секрета для пяти участников дают зависимость:

$$\begin{cases} (Ax_1^2+Bx_1+C)+(Dx_1+E)y_1=s_1, \\ (Ax_2^2+Bx_2+C)+(Dx_2+E)y_2=s_2, \\ (Ax_3^2+Bx_3+C)+(Dx_3+E)y_3=s_3, \\ (Ax_4^2+Bx_4+C)+(Dx_4+E)y_4=s_4, \\ (Ax_5^2+Bx_5+C)+(Dx_5+E)y_5=s_5. \end{cases} \quad (4)$$

Здесь точки $P_i=(x_i,y_i)$, $(i=1,...,n)$ соответствуют участникам: s_i, $(i=1,...,n)$ – их доли секрета. Для разделения секрета коалиция из $n=5$ участников должна объединиться и решить систему уравнений (4) для пяти неизвестных A,B,C,D,E. Если они однозначно найдут значения этих параметров, то смогут однозначно восстановить секрет, т.е. значение многочлена F в любой точке $P\in EC$, и, следовательно, эта коалиция является разрешенной.

Коалиция участников будет неразрешенной, если система линейных уравнений (4) не имеет однозначного решения, т.е. определитель d однородной системы равен нулю. Определитель d для коалиции участников с конечными точками равен

$$d=\begin{vmatrix} x_1^2 & x_1 & 1 & x_1y_1 & y_1 \\ x_2^2 & x_2 & 1 & x_2y_2 & y_2 \\ x_3^2 & x_3 & 1 & x_3y_3 & y_3 \\ x_4^2 & x_4 & 1 & x_4y_4 & y_4 \\ x_5^2 & x_5 & 1 & x_5y_5 & y_5 \end{vmatrix}. \quad (5)$$

Определитель для коалиции участников с «бесконечно удаленной» точкой P_5 имеет вид

$$d=\begin{vmatrix} x_1^2 & x_1 & 1 & x_1y_1 & y_1 \\ x_2^2 & x_2 & 1 & x_2y_2 & y_2 \\ x_3^2 & x_3 & 1 & x_3y_3 & y_3 \\ x_4^2 & x_4 & 1 & x_4y_4 & y_4 \\ 0 & 0 & 0 & 1 & 0 \end{vmatrix} = -\begin{vmatrix} x_1^2 & x_1 & 1 & y_1 \\ x_2^2 & x_2 & 1 & y_2 \\ x_3^2 & x_3 & 1 & y_3 \\ x_4^2 & x_4 & 1 & y_4 \end{vmatrix}. \quad (6)$$

Значение многочлена $F(x,y)=(Ax^2+Bx+C)+(Dx+E)y$ в точке $P(x,y)$ кривой EC можно представить в виде скалярного произведения двух векторов $(A,B,C,D,E)\cdot(x^2,x,1,xy,y)$. «Бесконечно удаленная» точка соответствует вектору $(0,0,0,1,0)$, т.е. старшему коэффициенту многочлена. Из этого представления следует линейность СРС [1].

Конечно же, хотелось бы получить хоть какое-то обоснование привлечения вычислительно затратных эллиптических кривых над конечным полем. В качестве подобного обоснования можно привести переход от ГОСТ ЭЦП 1994 г. к ГОСТ ЭЦП 2001 г. посредством замены мультипликативной группы поля вычетов на аддитивную группу точек эллиптической кривой, и эта замена позволила снизить длину ключа с 1024 до 256 бит при той же криптостойкости.

Свойства СРС

Напомним [7, 8], что для произвольной ненулевой рациональной функции f над кривой EC и произвольной точки P этой кривой можно определить целое число $\mathrm{ord}_P(f)$, называемое порядком этой функции в точке P. Тогда дивизором функции f называется $D=\mathrm{div}(f)=\sum_{P\in EC}\mathrm{ord}_P(f)(P)$. Такие дивизоры называются главными [7]. Степенью произвольного дивизора $D=\sum_{P\in EC}n_p(P)$, $n_p\in Z$, называется число $\deg(D)=\sum_{P\in EC}n_p$. Основой описания минимальных разрешенных коалиций и циклов соответствующего матроида является

Теорема 1. Для n различных точек на эллиптической кривой EC существует многочлен степени n, имеющий эти точки своими корнями, тогда и только тогда, когда сумма этих n точек равна нулю в группе точек данной кривой.

Доказательство. Пусть $P_1+P_2+...+P_n=\mathbf{0}$. Возьмем дивизор $D=1(P_1)+1(P_2)+...+1(P_n)-n(\mathbf{0})$. Воспользуемся теоремой, характеризующей группу главных дивизоров кривой как группу всех дивизоров D нулевой степени, удовлетворяющих условию

$$\sigma(P)=\sum_{P\in EC}n_pP=\mathbf{0}, \tag{7}$$

где $\mathbf{0}$ – нулевой элемент группы кривой, т.е. ее «бесконечно удаленная» точка [7]. Рассмотрим два параметра дивизора: $\sigma(D)$ и $\deg(D)$.

$$\begin{cases}\sigma(D)=1\cdot P_1+1\cdot P_2+...+1\cdot P_n-n\cdot\mathbf{0}=\mathbf{0},\\ \deg(D)=1+1+...+1-n=0.\end{cases} \tag{8}$$

Поскольку $\sigma(D)=\mathbf{0}$ и $\deg(D)=0$, этот дивизор является главным, и, по теореме о главных дивизорах [7], существует рациональная функция f такая, что $D=\mathrm{div}(f)$, а так как нет полюсов в конечных точках и корни имеют единичную кратность, то f есть многочлен.

Обратно, пусть многочлен f существует. Вычислим дивизор этого многочлена как частный случай рациональной функции

$$D=\mathrm{div}(f)=k_1\cdot(P_1)+k_2\cdot(P_2)+...+k_n\cdot(P_n)-n(\mathbf{0}), \tag{9}$$

где $k_1,k_2,...,k_n\geq 1$ – кратности корней. Порядок «бесконечно удаленной» точки равен $(-n)$, так как степень многочлена равна n. Поскольку все точки разные, то если для какого-то i имеем $k_i>1$, то степень дивизора D будет больше нуля: $\deg(D)=k_1+k_2+...+k_n-n>0$. А это противоречит теореме о главных дивизорах. Значит $k_1=k_2=...=k_n=1$, и тогда $\sigma(D)=1\cdot P_1+1\cdot P_2+...+1\cdot P_n-n\cdot\mathbf{0}=P_1+P_2+...+P_n$ и $\sigma(D)=\mathbf{0}$, поэтому $P_1+P_2+...+P_n=\mathbf{0}$. Теорема доказана.

Итак, если в коалиции участников меньше чем n, то такая коалиция будет неразрешенной. Если в коалиции участников ровно n, и сумма точек-участников не равна **0,** то это разрешенная коалиция. Если в коалиции участников ровно n, и сумма точек-участников равна **0**, то это неразрешенная коалиция. Если в коалиции более чем n участников, то она будет неразрешенной тогда и только тогда, когда сумма любых ее n точек-участников равна нулю.

Пусть сумма точек-участников в неразрешенной коалиции $\{P_1,...,P_n\}$ равна нулю, $P_1+...+P_n=\mathbf{0}$. Берем P – любую точку, не принадлежащую $\{P_1,...,P_n\}$, тогда $P+P_2+...+P_n=(P-P_1)+(P_1+P_2+...+P_n)=P-P_1+\mathbf{0}=P-P_1\neq\mathbf{0}$, так как $P\neq P_1$, поэтому $d\neq 0$ для $\{P,P_2,...,P_n\}$ и F однозначно определяется точками $\{P,P_1,...,P_n\}$. Значит, добавление в неразрешенную коалицию из n участников любого другого участника, не состоящего в этой коалиции, делает данную коалицию разрешенной [4, 9, 10]. Итак, циклы матроида данной схемы разделения секрета состоят либо из n, либо из $(n+1)$ точки. Для таких схем мы считаем естественным ввести термин **почти пороговые «$n,(n+1)$ из N» схемы**.

Для изучения вопроса о пороговости схемы рассмотрим следующую задачу. Пусть дана конечная абелева группа G, $|G|=N$ и дано целое число n такое, что $0\le n\le N$. Существуют ли такие n различные элементы $x_1,x_2,...,x_n$ группы G, что их сумма $x_1+x_2+...+x_n$ равна нулю? Посредством рутинных алгебраических выкладок, приведение которых здесь неуместно, доказана

Теорема 2. В конечной абелевой группе G для данного n такого, что $0\le n\le|G|$, не существует n-подмножества, сумма элементов которого равна нулю, в следующих лишь случаях: 1) G – элементарная абелева группа вида Z_2^s, причем $n=2$ при $s\ge1$ или $n=2^s-2$ при $s\ge2$; 2) в группе G имеется единственный (ненулевой) элемент второго порядка и $n=|G|$ (во втором случае группа G – циклическая четного порядка).

Для СРС на эллиптических кривых эта теорема означает, что схема разделения секрета будет пороговой лишь в двух тривиальных случаях: 1) группа изоморфна Z_2 или Z_2^2 (точки на оси абсцисс), $n=2$; 2) схема является пороговой «N из N» схемой, группа точек эллиптической кривой циклическая, ее порядок равен N, где N четно.

Теоремы 1 и 2 дают не только описание структуры доступа, но и показывают, что при случайном выборе коалиций они будут разрешенными с очень большой вероятностью. Так, число всех n-коалиций равно C_N^n, что соответствует латинской N-мерной таблице $N\times N\times...\times N$ [11]. В этой таблице N^{n-1} строк и в каждой содержится по одному нулю, т.е. всего N^{n-1} нулей в таблице. Тогда вероятность того, что коалиция участников будет неразрешенной, равна $\frac{N^{n-1}}{C_N^n}=O(N^{-1})\approx\frac{k}{N}\sim\frac{n!}{N}$ при $N\to\infty$. Только в малом количестве $O(N^{-1})$ случаев, когда сумма точек участников равняется нулю **0**, придется добавить еще одного участника.

Пример СРС

Рассматриваются кривые над полем $GF(9)$. Элементы поля представляются в виде: **0**=0+0i, **1**=1+0i, **2**=2+0i, **3**=0+1i, **4**=1+1i, **5**=2+1i, **6**=0+2i, **7**=1+2i, **8**=2+2i, где $i^2+1=0$. Расчет числа точек для всех эллиптических кривых на полем $GF(9)$ показал, что число точек находится в промежутке от 4 до 16, что соответствует теореме Хассе (3). Так, кривая $y^2=x^3+5x^2+x+4$ является эллиптической, так как $\Delta\ne0$ (2), и имеет 11 точек, включая «бесконечно удаленную». Координаты точек на кривой: $(x_1,y_1)=(3;3)$, $(x_2,y_2)=(3;6)$, $(x_3,y_3)=(5;1)$, $(x_4,y_4)=(5;2)$, $(x_5,y_5)=(6;3)$, $(x_6,y_6)=(6;6)$, $(x_7,y_7)=(7;3)$, $(x_8,y_8)=(7;6)$, $(x_9,y_9)=(8;4)$, $(x_{10},y_{10})=(8;8)$, ∞=**0**.

Для СРС «3,4 из M» существует C_{11}^3 вариантов коалиций участников при $n=3$, из них неразрешенные коалиции: 1 4 9, 1 5 7, 1 6 10, 2 3 10, 2 5 9, 2 6 8, 3 5 8, 3 7 9, 4 6 7, 5 8 10, 1 2 ∞, 3 4 ∞, 5 6 ∞, 7 8 ∞, 9 10 ∞. Итого 15 неразрешенных трехэлементных коалиций из 165. Примеры сложения точек на этой кривой: $P_2+P_5=P_{10}$, $2P_5=P_3$ и т.д. Нетрудно проверить, что сумма точек в неразрешенных коалициях равна нулю. В этом модельном примере $N=11$ точек, т.е. участников M может быть от 2 до 11, а мощность множества секретов $q=9$ (например, секрет и его «доли» – одна ненулевая цифра). В реальных же приложениях следует брать очень большие значения q и, в соответствии с теоремой Хассе, большие значения N, гарантирующие невозможность атаки методом грубой силы.

Заключение

Рассмотрен алгоритм разделения секрета при помощи многочленов на эллиптических кривых. Изучены структуры доступа и основные свойства таких схем. Доказана теорема о неразрешенных коалициях, которая устанавливает связь между суммой точек на кривой и коалицией. Выделен класс схем разделения секрета, названный почти пороговыми. Доказано, что для схем разделения секрета на эллиптических кривых существует лишь два тривиальных случая пороговой схемы. Приведен пример.

Авторы благодарят рецензента за конструктивные замечания.

Литература

1. Введение в криптографию / под общ. ред. В.В. Ященко. – СПб.: Питер, 2001. – 288 с.
2. Болотова Е.А. Свойства решеток разграничения доступа, совершенные шифры и схемы разделения секрета / Е.А. Болотова, С.С. Коновалова, С.С. Титов // Проблемы безопасности и противод. терроризму: матер. IV Междунар. науч. конф. – М.: МЦНМО, 2009. – Т. 2. – С. 71–86.
3. Shamir A. How to share a secret // Communications of the ACM. – NY, USA: ACM, 1979. – Vol. 22, №11. – P. 612–613.
4. Медведев Н.В. Проблема разделения секрета на эллиптических кривых / Н.В. Медведев, С.П. Баутин, С.С. Титов // Проблемы прикладной математики и механики: сб. научн. тр. / УрГУПС (Екатеринбург). – 2008. – № 65(148). – С. 160–174.
5. Глухов М.М. Алгебра: учеб. для вузов / М.М. Глухов, В.П. Елизаров, А.А. Нечаев. – М.: Гелиос АРВ, 2003. – 336 с.
6. Глухов М.М. О применениях квазигрупп в криптографии // Прикладная дискретная математика. – 2008. – № 2. – С. 28–32.
7. Болотов А.А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы / А.А. Болотов, С.Б. Гашков, А.Б. Фролов, А.А. Часовских. – М.: КомКнига, 2006. – 328 с.
8. Соловьев В.В. Эллиптические кривые и современные алгоритмы теории чисел / В.В. Соловьев, В.А. Садовничий, Е.Т. Щавгулидзе и др. – Ижевск: ИКИ, 2003. – 191 с.
9. Медведев Н.В. Алгоритм шифрования SAFER и возможности его улучшения // Проблемы теоретической и прикладной математики: тез. 41-й Всерос. молодежной конф. – Екатеринбург: Институт математики и механики УрО РАН, 2010. – С. 482–486.
10. Харин Ю.С. Математические и компьютерные основы криптологии: учеб. пособие для вузов / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Минск: Новое знание, 2003. – 381 с.
11. Белоусов В.Д. N-арные квазигруппы. – Кишинев: Штиница, 1972. – 227 с.

Медведев Никита Владимирович
Аспирант каф. прикладной математики
Уральского государственного университета путей сообщения (УрГУПС), г. Екатеринбург
Тел.: 8-903-079-51-53
Эл. почта: itcrypt@gmail.com

Титов Сергей Сергеевич
Д-р физ.-мат. наук, профессор каф. прикладной математики УрГУПС
Тел.: 8-950-194-88-81
Эл. почта: sergey.titov@usaaa.ru

Medvedev N.V., Titov S.S.

Almost-threshold secret sharing schemes on elliptic curves

The article describes secret sharing schemes based on polynomials on elliptic curves. The structure of access and basic properties of such schemes are studied. The theorem on qualified coalitions is proved. The example is given.

Keywords: secret sharing schemes, elliptic curves, polynomials, the structure of access, threshold schemes, cycles, matroids, finite fields.