УДК 519.7

О ПРИМЕНЕНИИ ЭЛЛИПТИЧЕСКИХ КРИВЫХ В НЕКОТОРЫХ ПРОТОКОЛАХ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

С. М. Рацеев, О. И. Череватенко

Рацеев Сергей Михайлович, доктор физико-математических наук, профессор кафедры информационной безопасности и теории управления, Ульяновский государственный университет, 432017, Россия, Ульяновск, Л. Толстого, 42, ratseevsm@mail.ru

Череватенко Ольга Ивановна, кандидат физико-математических наук, доцент кафедры высшей математики, Ульяновский государственный педагогический университет имени И. Н. Ульянова, 432063, Россия, Ульяновск, Площадь 100-летия со дня рождения В. И. Ленина, 4, chai@pisem.net

Протоколы электронного голосования позволяют проводить процедуру голосования, в которой избирательные бюллетени существуют только в электронной форме. Данные протоколы обеспечивают тайный характер голосования. Основное свойство протокола голосования — универсальная проверяемость, т. е. предоставление возможности всякому желающему, включая сторонних наблюдателей, в любой момент времени проверить правильность подсчета голосов. В работе рассматриваются криптографические протоколы электронного голосования на основе протоколов Шаума – Педерсона и Крамера – Франклина – Шонмейкерса – Янга. Данные протоколы приводятся на основе эллиптических кривых, применение которых позволяет значительно уменьшить размеры параметров протоколов и увеличить их криптографическую стойкость. Основное преимущество эллиптической криптографии заключается в том, что на данный момент не известно ни одного субэкспоненциального алгоритма решения задачи дискретного логарифмирования в группе точек эллиптической кривой.

Ключевые слова: протокол электронного голосования, битовое обязательство, схема разделения секрета.

DOI: 10.18500/1816-9791-2018-18-1-62-68

ВВЕДЕНИЕ

В данной работе приводятся модификации протоколов Шаума – Педерсона и Крамера – Франклина – Шонмейкерса – Янга на эллиптических кривых. Сам принцип функционирования криптосистем на эллиптических кривых подробно изложен в [1].

Безопасность криптосистем на эллиптических кривых ECC (Elliptic Curve Cryptography), как правило, основана на трудности решения задачи дискретного логарифмирования в группе точек эллиптической кривой [1]. Исследования показывают, что в классе криптосистем с открытым ключом криптосистемы на эллиптических кривых превосходят классические криптосистемы на основе модулярной арифметики, как минимум, по двум важным параметрам: степени защищенности в расчете на каждый бит ключа и быстродействию при аппаратной и программной реализации. Наглядно это демонстрирует следующая таблица (длины ключей для ECC и RSA при одинаковой криптостойкости согласно NIST [2]).

ECC key size (Bits)	RSA key size (Bits)	Key ratio	AES key size (Bits)
163	1024	1 : 6	
256	3072	1 : 12	128
384	7680	1 : 20	192
512	15360	1 : 30	256

1. МОДИФИКАЦИЯ ПРОТОКОЛА ГОЛОСОВАНИЯ НА ОСНОВЕ ПРОТОКОЛА ШАУМА – ПЕДЕРСЕНА

Рассмотрим модификацию протокола электронного голосования, приведенного в работе [3]. Пусть в голосовании участвуют n избирателей $P_1,\ldots,P_n$, которые являются абонентами некоторой сети и подают свои голоса в электронной форме: «за» и «против», которые соответственно представимы значениями 1 и -1. К протоколу предъявим два основных требования: 1) голосование должно быть тайным; 2) должна быть обеспечена правильность подсчета голосов.

Пусть T — центр подсчета голосов. Будем предполагать, что центр честный и пользуется безусловным доверием всех избирателей.

Пусть E — эллиптическая кривая над некоторым конечным полем F, q — некоторый достаточно большой простой делитель числа $|E|$, G, H — некоторые точки эллиптической кривой, имеющие порядок q. Доверенный центр T выбирает секретный ключ x, $0<x<q$, и публикует в открытом доступе открытый ключ $Y=[x]G$.

Каждый избиратель P_i посылает центру T сообщение, содержащее идентификатор этого избирателя и его голос $a_i\in\{-1,1\}$, зашифрованный с помощью вероятностного шифра на ключе Y следующим образом: $U_i=[k_i]G$, $V_i=[k_i]Y+[a_i]H$, (U_i,V_i) — бюллетень голосования (передается центру T), где k_i — некоторое случайное число, $0<k_i<q$. Центр расшифровывает бюллетени, подсчитывает и публикует итог. Расшифрование бюллетеня (U_i,V_i) происходит следующим образом: вычисляется $V_i+[q-x]U_i=[a_i]H$; так как $a_i\in\{-1,1\}$, то из $[a_i]H$ легко находится a_i.

После этого центр T вычисляет $S=\sum\limits_{i=1}^{n}a_i$ и публикует итог голосования S. Поскольку все бюллетени находятся в некотором хранилище данных, то любой избиратель, а также всякий сторонний наблюдатель может вычислить

$$A=\sum_{i=1}^{n}U_i=\sum_{i=1}^{n}[k_i]G,\qquad B=\sum_{i=1}^{n}V_i=\sum_{i=1}^{n}([k_i]Y+[a_i]H).$$

Обозначим $C=\sum\limits_{i=1}^{n}[k_i]Y$. При этом $C=[x]A$. Если центр правильно подсчитал голоса, то должно выполняться равенство $[S]H=\sum\limits_{i=1}^{n}[a_i]H$. Поэтому, если из B вычесть $[S]H$, то должно получиться значение C. Пусть $\widetilde{C}=B-[S]H$. Проверяющий не знает значения C и не может самостоятельно выяснить, верно ли, что $C=\widetilde{C}$. Но при этом нетрудно проверить, что должно выполняться равенство $\widetilde{C}=[x]A$. Поэтому проверяющий может потребовать от центра доказательство следующего факта: в группе точек эллиптической кривой дискретный логарифм $\widetilde{C}$ по основанию A равен дискретному логарифму Y по основанию G.

Приведем модификацию протокола Шаума и Педерсена [4,5] доказательства данного факта на эллиптических кривых.

1. Доказывающий случайным образом выбирает k, $0<k<q$, вычисляет $R_1=[k]G$, $R_2=[k]A$ и передает R_1,R_2 проверяющему.
2. Проверяющий генерирует случайное число a, $0\leqslant a<q$, которое передает доказывающему.

3. Доказывающий вычисляет $s = k + ax \pmod q$ и передает s проверяющему.

4. Проверяющий убеждается, что $[s]G = R_1 + [a]Y$ и $[s]A = R_2 + [a]\widetilde{C}$.

Таким образом, центр T может доказать утверждение $\widetilde{C} = [x]A$ каждому желающему.

2. МОДИФИКАЦИЯ ПРОТОКОЛА КРАМЕРА – ФРАНКЛИНА – ШОНМЕЙКЕРСА – ЯНГА НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Рассмотрим более сложный протокол электронного голосования [6, 7]. Задача ставится следующим образом. Пусть в голосовании участвуют n избирателей $P_1,\dots,$ P_n, которые являются абонентами некоторой сети и подают свои голоса в электронной форме: «за» и «против», которые соответственно представимы значениями 1 и -1. Имеется m счетных комиссий, которые создаются для обеспечения анонимности и предотвращения фальсификации итогов голосования. К протоколу предъявим следующие требования: 1) голосуют только уполномоченные избиратели; 2) любой участник имеет право отдать не более одного голоса; 3) ни один из участников не может знать, как проголосовал другой; 4) никто не может дублировать чужой голос; 5) конечный результат будет подсчитан корректно; 6) любой желающий может проверить правильность результата; 7) протокол должен работать и в тех случаях, когда некоторые участники ведут себя нечестно.

Приведем модификацию протокола, предложенного в 1996 г. [6], на эллиптических кривых. Сначала каждая комиссия фиксирует закрытый ключ и публикует открытый ключ.

Пусть E — эллиптическая кривая над некоторым конечным полем F, q — некоторый достаточно большой простой делитель числа $|E|$, G — некоторая точка эллиптической кривой, имеющая порядок q, $H = [u]G$ для некоторого $0 < u < q$, причем нахождение значения u по известному H должно являться трудной задачей.

1. Заполнение бюллетеня избирателями

1.1. Избиратель P_i выбирает голос $a_i \in \{-1, 1\}$ и случайный элемент $k_i \in \mathbb{Z}_q$. Затем он публикует свидетельство

$$R_{0i} = [k_i]G + [a_i]H, \qquad i = 1, \dots, n,$$

скрывающего поданный им голос (битовое обязательство). В результате в общем доступе будут свидетельства всех участников $R_{01},\dots, R_{0n}$.

1.2. Также каждый избиратель P_i выполняет автономную версию протокола доказательства знания следующим образом. Для краткости обозначим $b = a_i$, $R_0 = R_{0i}$. P_i выбирает случайные элементы $0 < d, z, w < q$, вычисляет

$$R_1 = \begin{cases} [z]G + [-d](R_0 + H), & b = 1, \\ [w]G, & b = -1, \end{cases}$$

$$R_2 = \begin{cases} [w]G, & b = 1, \\ [z]G + [-d](R_0 - H), & b = -1 \end{cases}$$

и находит значение хеш-функции $a = h(R_0, R_1, R_2) \pmod q$. После этого P_i вычисляет четверку значений

$$(d_1, d_2, s_1, s_2) = \begin{cases} (d, \widetilde{d}, z, \widetilde{z}), & b = 1, \\ (\widetilde{d}, d, \widetilde{z}, z), & b = -1, \end{cases}$$

где $\widetilde{d} = a - d \pmod q$, $\widetilde{z} = w + k\widetilde{d} \pmod q$. Затем избиратель P_i публикует значения (R_0, R_1, R_2), a, (d_1, d_2, s_1, s_2). Любой желающий может осуществить проверку корректного голосования участника P_i. Для этого проверяются равенства:

$$a = d_1 + d_2 \pmod q, \quad [s_1]G = R_1 + [d_1](R_0 + H), \quad [s_2]G = R_2 + [d_2](R_0 - H).$$

2. Передача бюллетеней комиссиям. Для передачи бюллетеней с голосами избирателей счетным комиссиям используется совершенная проверяемая схема разделения секрета Педерсена – Шамира [8]: i-й избиратель выбирает два многочлена над полем $\mathbb{Z}_q$ степени T, $0 < T < m$:

$$U_i(x) = k_i + k_{1i}x + \ldots + k_{Ti}x^T \in \mathbb{Z}_q[x],$$
$$V_i(x) = a_i + a_{1i}x + \ldots + a_{Ti}x^T \in \mathbb{Z}_q[x],$$

где коэффициенты k_{ji}, a_{ji} — случайные числа из $\mathbb{Z}_q$, $1 \leqslant j \leqslant T$. Значения $(x_j, y_{ij}, z_{ij}) = (x_j, U_i(x_j), V_i(x_j))$, $x_j \in \mathbb{Z}_q^*$, попарно различны, $j = 1, \ldots, m$, являются долями $(m, T+1)$ пороговой схемы разделения секрета (k_i, a_i). Здесь значение T определяется тем, что если не произошло никакого сговора более чем в T избирательных комиссиях, то невозможно вычислить, как голосовал отдельный участник. В то же время выборы будут успешны, если, по крайней мере, $T+1$ избирательных комиссий действуют правильно.

Также для данных коэффициентов P_i вычисляет проверочные значения:

$$B_{i0} = [k_i]G + [a_i]H, \quad B_{i1} = [k_{1i}]G + [a_{1i}]H, \quad \ldots, \quad B_{iT} = [k_{Ti}]G + [a_{Ti}]H,$$

которые публикуются в открытом доступе. Заметим, что значение $B_{i0} = [k_i + ua_i]G$ зависит от случайного числа k_i. Поэтому даже если кто-то и сможет вычислить значения u и $k_i + ua_i$ (решив задачу дискретного логарифмирования), то это не даст ему никакой информации о значении a_i. Заметим, что свойство совершенности играет очень важную роль при защите информации [9, 10].

Избиратель P_i шифрует значения (x_j, y_{ij}, z_{ij}) на открытом ключе j-й избирательной комиссии, после чего ей передаются полученные значения, $j = 1, \ldots, m$. j-я комиссия после расшифрования и восстановления значений (x_j, y_{ij}, z_{ij}) делает проверку

$$[y_{ij}]G + [z_{ij}]H = B_{i0} + [x_j]B_{i1} + \ldots + [x_j^T]B_{iT}.$$

Итак, каждая счетная комиссия имеет следующие наборы:

$$\begin{array}{lllll} 1: & (x_1, y_{11}, z_{11}), & \ldots, & (x_1, y_{n1}, z_{n1}), \\ & & \ldots & \\ m: & (x_m, y_{1m}, z_{1m}), & \ldots, & (x_m, y_{nm}, z_{nm}). \end{array}$$

3. Подсчет голосов. Каждая j-я комиссия подсчитывает и публикует значения

$$y_j = \sum_{i=1}^{n} y_{ij}, \quad z_j = \sum_{i=1}^{n} z_{ij}.$$

Теперь каждый желающий может проверить корректность опубликованных данных, проверив равенства:

$$\sum_{i=1}^{n} \left(R_{0i} + \sum_{l=1}^{T} [x_j^l] B_{il} \right) = [y_j]G + [z_j]H, \qquad j = 1, \ldots, m,$$

так как

$$\sum_{i=1}^{n}\left(R_{0i}+\sum_{l=1}^{T}[x_j^l]B_{il}\right)=\sum_{i=1}^{n}\left([k_i]G+[a_i]H+\sum_{l=1}^{T}[x_j^l]\left([k_{li}]G+[a_{li}]H\right)\right)=$$
$$=\sum_{i=1}^{n}([k_i+k_{1i}x_j+\ldots+k_{Ti}x_j^T]G+[a_i+a_{1i}x_j+\ldots+a_{Ti}x_j^T]H)=$$
$$=\sum_{i=1}^{n}([U_i(x_j)]G+[V_i(x_j)]H)=\sum_{i=1}^{n}([y_{ij}]G+[z_{ij}]H)=[y_j]G+[z_j]H.$$

Заметим, что для любого $j=1,\ldots,m$ значение z_j является значением некоторого многочлена над полем $\mathbb{Z}_q$ степени не более T:

$$z_j=\sum_{i=1}^{n}z_{ij}=\sum_{i=1}^{n}V_i(x_j)=\left(\sum_{i=1}^{n}a_i\right)+\left(\sum_{i=1}^{n}a_{1i}\right)x_j+\ldots+\left(\sum_{i=1}^{n}a_{Ti}\right)x_j^T.$$

Поэтому для определения итога голосования $\sum\limits_{i=1}^{n}a_i$ достаточно в множестве пар точек $\{(x_1,z_1),\ldots,(x_m,z_m)\}$ выделить любое $(T+1)$-элементное подмножество $\{(\widetilde{x}_0,\widetilde{z}_0),\ldots,(\widetilde{x}_T,\widetilde{z}_T)\}$ и вычислить

$$\sum_{i=0}^{T}\widetilde{z}_i\prod_{\substack{0\leqslant j\leqslant T\\ j\neq i}}\frac{\widetilde{x}_j}{\widetilde{x}_j-\widetilde{x}_i}=\sum_{i=1}^{n}a_i.$$

Библиографический список

1. *Hankerson D., Menezes A., Vanstone S.* Guide to Elliptic Curve Cryptography. N. Y. : Springer-Verlag, 2004. 358 p.
2. An Elliptic Curve Cryptography (ECC) Primer: why ECC is the next generation of public key cryptography. The Certicom Corp. 'Catch the Curve' White Paper Series, June 2004. 24 p. URL: https://www.certicom.com/content/dam/certicom/images/pdfs/WP-ECCprimer.pdf (дата обращения: 05.09.2017)
3. Введение в криптографию / под общ. ред. В. В. Ященко. М. : МЦНМО, 2012. 348 с.
4. *Chaum D., Pedersen T. P.* Wallet databases with observers // Proc. Crypto'92. Lect. Notes in Comput. Sci. 1993. Vol. 740. P. 89–105.
5. *Cramer R., Gennaro R., Schoenmakers B.* A secure and optimally efficient multi-authority election scheme // Proc. EUROCRYPT'97. Lect. Notes in Comput. Sci. 1997. Vol. 1233. P. 103–118.
6. *Cramer R., Franklin M., Schoenmakers B., Yung M.* Multi-Authority Secret-Ballot Elections with Linear Work // Proc. EUROCRYPT'96. Lect. Notes in Comput. Sci. 1996. Vol. 1070. P. 72–83.
7. *Черемушкин А. В.* Криптографические протоколы. Основные свойства и уязвимости. М. : Академия, 2009. 272 с.
8. *Pedersen T. P.* Non-interactive and information-theoretic secure verifiable secret sharing // Proc. EUROCRYPT'91. Lect. Notes in Comput. Sci. 1992. Vol. 576. P. 129–140.
9. *Зубов А. Ю.* Криптографические методы защиты информации. Совершенные шифры. М. : Гелиос АРВ, 2005. 192 с.
10. *Рацеев С.М.* Некоторые обобщения теории Шеннона о совершенных шифрах // Вестн. ЮУрГУ. Сер. Матем. моделирование и программирование. 2015. Т. 8, № 1. С. 111–127.

Образец для цитирования:
Рацеев С. М., Череватенко О. И. О применении эллиптических кривых в некоторых протоколах электронного голосования // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2018. Т. 18, вып. 1. С. 62–68. DOI: 10.18500/1816-9791-2018-18-1-62-68.

On Application of Elliptic Curves in Some Electronic Voting Protocols

S. M. Ratseev, O. I. Cherevatenko

Sergey M. Ratseev, https://orcid.org/0000-0003-4995-9418, Ulyanovsk State University, 42, Lev Tolstoy Str., Ulyanovsk, Russia, 432017, ratseevsm@mail.ru
Olga I. Cherevatenko, https://orcid.org/0000-0003-3931-9425, Ulyanovsk State I. N. Ulyanov Pedagogical University, 4, Ploshchad' 100-letiya so dnya rozhdeniya V. I. Lenina, Ulyanovsk, Russia, 432063, chai@pisem.net

Electronic voting protocols allow us to carry out voting procedure in which ballots exist only electronically. These protocols provide the secret nature of vote. The main property of electronic voting protocols is the universal checkability, i.e. provision of an opportunity to any person interested, including detached onlookers to check correctness of counting of votes at any moment. In operation cryptography protocols of electronic vote of Shauma – Pederson and Kramera – Franklin – Shoyenmeykersa – Yunga are considered. These protocols are provided on the basis of elliptic curves which application allows us to reduce considerably the sizes of parameters of protocols and to increase their cryptography firmness. Primary benefit of elliptic cryptography is that any subexponential algorithm of the decision of the task of the discrete logarithming in group of points of an elliptic curve is not known at the moment.

Key words: electronic voting protocol, bit obligation, diagram of division of a secret.

References

1. Hankerson D., Menezes A., Vanstone S. *Guide to Elliptic Curve Cryptography*. New York, Springer-Verlag, 2004. 358 p.
2. *An Elliptic Curve Cryptography (ECC) primer : Why ECC is the next generation of public key cryptography*. The Certicom Corp. 'Catch the Curve' White Paper Series, June 2004. 24 p. Available at: https://www.certicom.com/content/dam/certicom/images/pdfs/WP-ECCprimer.pdf (Accessed 5 September 2017).
3. *Vvedenie v kriptografiiu* [Introduction to cryptography]. Under a general edition of V. V. Yashchenko. Moscow, MTsNMO Publ., 2012. 348 p. (in Russian).
4. Chaum D., Pedersen T. P. Wallet databases with observers. *Proc. Crypto'92. Lect. Notes in Comput. Sci.*, 1993, vol. 740, pp. 89–105.
5. Cramer R., Gennaro R., Schoenmakers B. A secure and optimally efficient multi-authority election scheme. *Proc. EUROCRYPT'97. Lect. Notes in Comput. Sci.*, 1997, vol. 1233, pp. 103–118.
6. Cramer R., Franklin M., Schoenmakers B., Yung M. Multi-Authority Secret-Ballot Elections with Linear Work. *Proc. EUROCRYPT'96. Lect. Notes in Comput. Sci.*, 1996, vol. 1070, pp. 72–83.
7. Cheremushkin A. V. *Kriptograficheskie protokoly. Osnovnye svoistva i uiazvimosti* [Cryptography protocols. Main properties and vulnerabilities]. Moscow, Academy, 2009. 272 p. (in Russian).
8. Pedersen T. P. Non-interactive and information-theoretic secure verifiable secret sharing. *Proc. EUROCRYPT'91. Lect. Notes in Comput. Sci.*, 1992, vol. 576, pp. 129–140.

9. Zubov A. Yu. *Kriptograficheskie metody zashhity informacii. Sovershennye shifry* [Cryptographic Methods of Information Security. Perfect ciphers]. Moscow, Gelios ARV, 2005. 192 p. (in Russian).
10. Ratseev S. M. Some generalizations of Shannon's theory of perfect ciphers. *Vestnik YuUrGU. Ser. Mat. Model. Progr.* [Bulletin of the South Ural State University, Ser. : Mathematical Modelling, Programming and Computer Software], 2015, vol. 8, no. 1, pp. 111–127 (in Russian).

Cite this article as:
Ratseev S. M., Cherevatenko O. I. On Application of Elliptic Curves in Some Electronic Voting Protocols. *Izv. Saratov Univ. (N. S.), Ser. Math. Mech. Inform.*, 2018, vol. 18, iss. 1, pp. 62–68 (in Russian). DOI: 10.18500/1816-9791-2018-18-1-62-68.