Сергиенко Е.Н., Чурилов А.С., Черников С.В. Криптографические методы обеспечения конфиденциальности электронных выборов. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XVII Междунар. научно-техн. конф. – Пенза: ПДЗ, 2017. – С. 51-56.

УДК 004.56.23

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ЭЛЕКТРОННЫХ ВЫБОРОВ

Е.Н. Сергиенко, А.С. Чурилов, С.В. Черников

CRIPTOGRAPHIC METHODS OF PRIVACY PRACTICE OF ELECTRONIC ELECTIONS

E.N. Sergienko, A.S. Churilov, S.V. Chernikov

Аннотация. Описываются методы обеспечения конфиденциальности электронных выборов. Рассматриваются системы на основе слепой подписи, с применением микс-сетей, на основе гомоморфного шифрования и на основе блокчейн цепочки.

Ключевые слова: конфиденциальность, криптографические методы, электронные выборы, слепая подпись, микс-сети, гомоморфное шифрование, блокчейн цепочки.

Abstract. Methods for ensuring the confidentiality of electronic elections are described. Systems based on blind signatures, using mix networks, on the basis of homomorphic encryption, and on the basis of the blockchainsare considered.

Keywords: confidentiality, cryptographic methods, electronic choices, blind signature, mix-networks, homomorphic encryption, blockchains.

При разработке системы электронных выборов необходимо исходить из минимальных требований, предъявляемых к протоколам электронного голосования. Анонимность выборов может обеспечиваться одним из ниже перечисленных способов:

1. С применением слепой подписи [1, 2].
2. С применением микс-сетей [3, 4].
3. На основе гомоморфного шифрования [5].
4. На основе блокчейн цепочки [6].

Системы электронного голосования на основе слепой подписи предполагают наличие трех сторон в процессе голосования: избиратель, Центральное управление регистрации (ЦУР) и Центральная избирательная комиссия (ЦИК). В данной схеме анонимность обеспечивается за счет выдаваемых ЦУР «маркеров» для голосования, которые дают правомочность избирателю при процедуре голосования в ЦИК. Этот маркер «обезличивает» избирателя, однако ничто не мешает сговору ЦИК и ЦУР в передаче данных о владельце маркера между собой, нарушая, таким образом, свойство анонимности голосования.

Эстонская система голосования основана на криптосистеме RSA с использованием слепой подписи, однако она не раз подвергалась критике, так как уязвима перед большинством атак, связанных с возможностью подделки результатов, а также нарушениями установленного самими властями регламента проведения выборов. Исходный код данной системы за исключением клиентской части общедоступен, что позволило различным хакерским группировкам из России и Украины провести анализ уязвимостей и совершить полномасштабную атаку на эту систему.

Схемы на основе микс-сетей позволяют сделать голос избирателя анонимным благодаря многократному шифрованию и перестановкам списка кандидатов при передаче голоса от избирателя в урну ЦИК. При этом ЦИК разделен на несколько или более доверенных лиц, каждое из которых знает только свою часть общего ключа и свою перестановку. Таким образом, никто из доверенных лиц не сможет рассекретить голос без знания всех перестановок и общего секретного ключа. Микс-сети также используются для анонимизации платежей в системах электронных денег [7, 8] и для анонимного просмотра веб-страниц, примером реализации которого может служить популярный браузер Tor.

Микс-сервер работает как цепочка прокси-серверов, каждый из которых имеет собственные открытый и секретный ключи. Клиент шифрует сообщение один раз с использованием открытых ключей каждого из прокси-серверов в определенном порядке, который знает только клиент. Расшифровка криптограммы происходит в обратном порядке с помощью секретных ключей микс-серверов, но уже на стороне последних. Такая схема анонимизации данных имеет серьезный недостаток. При проведении выборов может выйти из строя любой из прокси-серверов, тем самым испортив бюллетень избирателя.

Кроме того, в данной схеме голосования необходима еще одна сторона – верификатор, который должен следить за честностью смешивания и правильностью расшифровки бюллетеня. В программных реализациях часто в качестве верификатора выступает каждый узел микс-сети. Также для такой системы голосования необходим контроллер, который будет следить за сервером голосования и выступать в качестве хранилища голосов. Это подразумевает большое доверие к контроллеру выборов. Сервер голосования отвечает за сбор зашифрованных голосов избирателей. Это значит, что он может заменить все голоса, если захочет, но такой сервер не сможет определить, какой избиратель за кого проголосовал, так как все голоса поступают на сервер в зашифрованном виде. Еще одним недостатком данной схемы является подверженность к атакам «Человек посередине».

Более того, как было показано в [9, 10], протоколы, основанные на микс-сетях, практически не защищены от нарушения конфиденциальности голосов при малом числе избирателей, а также не существует эффективной защиты от подкупа голосов. Примером e-voting системы на основе микс-сетей является система голосования, созданная в Испании и используемая в Норвегии и Испании. Однако, как было показано в [11], микс-сети обладают низкой эффективностью вычислений, поэтому перенастройка системы может занимать длительное время, что критично при возникновении внештатных ситуаций.

Схемы на основе гомоморфного шифрования позволяют сократить число сторон в процедуре голосования до двух: избирателя и ЦИК. Причем отличаются они достаточной эффективностью и простотой реализации, а безопасность таких схем обеспечивается криптостойкостью используемых криптосистем. Анонимность при применении гомоморфных криптосистем обеспечивается за счет гомоморфной суммы при подсчете количества голосов. Таким образом, вычисление конкретного голоса – задача вычисления дискретного логарифма в конечной циклической группе (DDH) [12-14]. Стоит отметить, что задача DDH используется для доказательства криптостойкости таких криптосистем, как ElGamal и Cramer-Shoup.

Рассмотрим пример, как можно использовать криптосистему ElGamal, обладающую гомоморфными свойствами, для анонимизации голосов избирателей.

Пусть p и q – большие простые числа, причем $q \mid p-1$. Пусть также G – конечная циклическая группа из Z_p^* порядка q и образующим элементомg ($G = \langle g \rangle$).

Генерация ключевой пары:

1. Выбирается случайное число $a \in Z_q^*$
2. Вычисляется $y = g^a \ mod \ p$
3. Открытым ключом будет кортеж(y, p, q)
4. Закрытый ключ – число a.

Шифрование сообщения $m \in Z_q$***:***

1. Выбирается случайное число $r \in Z_q^*$
2. Вычисляется шифротекст как:

$$c = (\alpha, \beta) = (g^r (mod\ p), y^r g^m (mod\ p)$$

Дешифровка шифротекста :

$$g^m = \beta y^{-r} = \beta (g^a)^{-r} = \beta \alpha^{-a}\ (mod\ p).$$

В данном протоколе используется экспоненциальная версия криптосистемы ElGamal, что дает нам аддитивный гомоморфизм:

$$Enc(m_1)\ *\ Enc(m_2) = Enc(m_1 + m_2).$$

Это свойство позволяет нам перемножить все бюллетени, а затем совместно расшифровать их, не раскрывая ни одного голоса. Это объясняет то, почему выбрана именно экспоненциальная версия данной криптосистемы.

$$\prod c_i = \left(\prod g^{r_i}, \prod y^{r_i} g^{m_i} \right) = (g^{\Sigma\ \ r_i} (mod\ p),\quad y^{\Sigma\ \ r_i} g^{\Sigma\ \ m_i}\ (mod\ p))$$

Для того чтобы получить итоговый результат $\sum m_i$, необходимо вычислить дискретный логарифм в группе G. Для небольших показателей m эта процедура не займет много времени, и мы сможем за короткие сроки произвести подсчет голосов.

Электронное голосование на основе блокчейна позволяет провести полностью анонимные выборы, конфиденциальность которых можно нарушить только сговором всех избирателей [15]. Чтобы иметь возможность проверки результатов выборов, необходима публичная “доска”, в качестве которой может выступать блокчейн. Существуют реализации, где блокчейн используется в качестве урны для голосования, а все избиратели обезличиваются с помощью обфускации до начала процедуры выборов [16]. Для разработки системы голосования на основе блокчейн можно использовать Etherium. Это криптоплатформа, которая позволяет создавать любые защищенные распределенные приложения. В основе Ethereum “умные контракты” на базе блокчейн, методы которых можно выполнить за определенную плату – газ.

Благодаря Chain архитектуре мы можем проверить подлинность проведенного голосования и удостовериться, что наш голос принимал участие в голосовании. Ethereum не подвержен атаки “человек посередине”, так как все данные хранятся распределенно, и никто не сможет подменить контракт. Газ при голосовании необходим для защиты от DDOS атак.

Библиографический список

1. David L Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communicationsofthe ACM, 24(2):84– 90, 1981.

2. Jannik Dreier, Pascal Lafourcade, and YassineLakhnech. Voteindependence: A powerful privacy notion for voting protocols. InFoundationsandPracticeofSecurity, pages 164–180. Springer, 2011.

3. Jannik Dreier, Pascal Lafourcade, and YassineLakhnech. A formal taxonomy of privacy in voting protocols. In Communica- tions (ICC), 2012 IEEE International Conference on, pages 6710– 6715. IEEE, 2012.

4. Hugo Jonker, SjoukeMauw, and Jun Pang. Privacy and veri- fiability in voting systems: Methods, developments and trends. ComputerScienceReview, 10:1–30, 2013.

5. Lucie Langer, Hugo Jonker, and WolterPieters. Anonymity and verifiability in voting: understanding (un) linkability. InInformationandCommunicationsSecurity, pages 296–310. Springer, 2010.

6. P. Boucher. What if blockchain technology revolutionised voting? Scientific Foresight Unit (STOA), European Parliamentary Research Service, Sept. 2016. URL: http://www.europarl.europa.eu/RegData/etudes/
ATAG/2016/58191/EPRS ATA(2016)581918 EN.pdf (дата обращения: 20.03.2017).

7. Чурилов А.С., Панарин С.А. Анализ свойства несвязываемости и эффективности в различных типах протоколов анонимных электронных денег // Труды Международной научно-технической конференции студентов, аспирантов и молодых ученых БГТУ им. В.Г. Шухова. Белгород, 2015.

8. Чурилов А.С., Панарин С.А. Анализ криптостойкости и эффективности протокола электронной наличности T. Nakanishi, M. Shiota, Y. Sugiyama // Труды Международной научно-технической конференции студентов, аспирантов и молодых ученых БГТУ им. В.Г. Шухова. Белгород, 2015.

9. Jivanyan A. New Receipt-Free E-Voting Scheme and Self-Proving Mix Net as New Paradigm. // IACR Cryptology ePrint Archive, 2011.

10. Escala, P. Morillo, P. Bibiloni. Vote validatability in Mix-Net-based eVoting. Proceedings of VoteID 2015. // Lecture Notes in Computer Science, 9269 (2015) 92-109. Bern, Switzerland, 2015.

11. Kulyk O. Efficiency Comparison of Various Approaches in E-Voting Protocols. // Practice Talk for Financial Crypto Voting Workshop. URL: https://eprint.iacr.org/2015/558.pdf (дата обращения: 10.05.2016).

12. Boneh D. (1998). The Decision Diffie–Hellman Problem // Proceedings of the Third Algorithmic Number Theory Symposium. LectureNotesinComputerScience 1423: pp. 48–63.

13. Gentry C. A fully homomorphic encryption scheme // [dissertation]. Stanford University; 2009. Available at: http://crypto.stanford.edu/craig/craig-thesis.pdf.

14. Baum, C., Damg˚ard, I., Orlandi, C.: Publicly auditable secure multi-party computation. // IACR Cryptology ePrint Archive 2014, 75 (2014)

15. K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, and E. G¨un. On scaling decentralized blockchains. In Proc. 3rd Workshop on Bitcoin and Blockchain Research, 2016.

16. A. Hertig. The First Bitcoin Voting Machine Is On Its Way. Motherboard Vice, Nov. 2015. URL: http://motherboard.vice.com/read/the-first-bitcoin-voting-machine-ison-its-way

Сергиенко Елена Николаевна
Белгородский государственный технологический университет им В.Г. Шухова,
г. Белгород, Россия
E-mail: selcha07@inbox.ru

Sergienko E.N.
Belgorod State Technological University named after V.G.Shukov,
Belgorod, Russia

Чурилов Антон Сергеевич
Белгородский государственный технологический университет им В.Г. Шухова,
г. Белгород, Россия

Churilov A.S.
Belgorod State Technological University named after V.G.Shukov,
Belgorod, Russia

Черников Сергей Викторович
Белгородский государственный технологический университет им В.Г. Шухова,
г. Белгород, Россия

Chernikov S.V.
Belgorod State Technological University named after V.G.Shukov,
Belgorod, Russia