UDC 519.7

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.

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

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.