5. 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: 05.09.2018).
6. *Рацеев С. М., Ростов М. А.* Методы ускорения и усовершенствования протокола аутентификации с нулевым разглашением на основе задачи о нахождении гамильтонова цикла в графе // Научные ведомости БелГУ. Экономика. Информатика. 2017. № 16(265), вып. 43. С. 131–137.
7. *Stone J. E., Phillips J. C., Freddolino P. L., Hardy D. J., Trabuco L. G., Schulten K.* Accelerating molecular modeling applications with graphics processors // J. Comput. Chem. 2007. Vol. 28, № 16. P. 2618–2640. DOI: https://doi.org/10.1002/jcc.20829
8. *Van Meel J. A., Arnold A., Frenkel D., Zwart S. P., Belleman R.* Harvesting graphics power for MD simulations // Molecular Simulation. 2008. Vol. 34, № 3. P. 259–266. DOI: https://doi.org10.1080/08927020701744295
9. *Harris C., Haines K., Staveley-Smith L.* GPU accelerated radio astronomy signal convolution // Exp. Astron. 2008. Vol. 22, iss. 1–2. P. 129–141. DOI: https://doi.org/10.1007/s10686-008-9114-9
10. *Muyan-Ozcelik P., Owens J. D., Xia J., Samant S. S.* Fast deformable registration on the GPU: A CUDA implementation of demons // Proc. Int. Conf. Computational Science and its Applications. Perugia, Italy, 2008. P. 223–233. DOI: https://doi.org/10.1109/ICCSA.2008.22
11. ISO/IEC 9798-5:2009(E) «Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero-knowledge technique». URL: https://www.iso.org/standard/50456.html (дата обращения: 05.09.2018).

Образец для цитирования:
Рацеев С. М., Ростов М. А. О протоколах аутентификации с нулевым разглашением знания // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2019. Т. 19, вып. 1. С. 114–121. DOI: https://doi.org/10.18500/1816-9791-2019-19-1-114-121

Zero-Knowledge Proof Authentication Protocols

S. M. Ratseev, M. A. Rostov

Sergey M. Ratseev, http://orcid.org/0000-0003-4995-9418, Ulyanovsk State University, 42 L. Tolstoy St., 432017 Ulyanovsk, Russia, ratseevsm@mail.ru

Mihail A. Rostov, Ulyanovsk State University, 42 L. Tolstoy St., 432017 Ulyanovsk, Russia

The paper presented the comparative analysis of the authentication Shnorr's protocol and the authentication protocol based on the task of finding a Hamilton cycle in the graph. It is shown that with the use of CUDA technology the productivity of protocols on graphs is as high as Shnorr's protocol productivity. The importance of such research is that protocols on graphs (the authentication protocol on the basis of the proof of graph isomorphism, the authentication protocol based on the task of finding a Hamilton cycle in the graph, etc.) have the property of zero-knowledge proof. These protocols are based on NP complete tasks therefore they are independent of quantum computings, namely, are resistant to the quantum attacks. Also the modified algorithms of two-step authentication protocols with zero-knowledge proof based on asymmetric ciphers with the use of elliptic curves are also given.

Keywords: authentication protocol, zero-knowledge proof, elliptic curve, CUDA technology.

Received: 24.05.2018 / Accepted: 18.12.2018 / Published online: 28.02.2019

References

1. Cheremushkin A. V. *Kriptograficheskie protokoly. Osnovnye svoistva i uyazvimosti* [Cryptographic Protocols. Basic Properties and Vulnerability]. Moscow, IC "Akademiya", 2009. 272 p. (in Russian).
2. Moldovyan A. A., Moldovyan D. N., Levina A. B. *Protokoly autentifikacii s nulevym razglasheniem sekreta* [Authentication protocols with zero-knowledge proof]. St. Petersburg, ITMO Univ., 2016. 55 p. (in Russian).
3. Schnorr C. P. Efficient Identification and Signatures for Smart Cards. *Advances in Cryptology – CRYPTO'89. Proceedings. CRYPTO 1989. Lecture Notes in Computer Science*, vol. 435. New York, Springer, 1990, pp. 239–252. DOI: https://doi.org/10.1007/0-387-34805-0_22
4. Hankerson D., Menezes A., Vanstone S. *Guide to Elliptic Curve Cryptography*. New York, Springer-Verlag, 2004. 358 p. DOI: https://doi.org/10.1007/b97644
5. *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 05 September 2017).
6. Ratseev S. M., Rostov M. A. Methods of an acceleration and enhancement of the cryptography authentication protocol with zero disclosure of knowledge on the basis of the task about finding of a hamilton cycle in the graph. *Belgorod State University Scientific Bulletin. Economics. Computer Science*, 2017, no. 16(265), iss. 43, pp. 131–137 (in Russian).
7. Stone J. E., Phillips J. C., Freddolino P. L., Hardy D. J., Trabuco L. G., Schulten K. Accelerating molecular modeling applications with graphics processors. *J. Comput. Chem.*, 2007, vol. 28, no. 16, pp. 2618–2640. DOI: https://doi.org/10.1002/jcc.20829
8. Van Meel J. A., Arnold A., Frenkel D., Zwart S. P., Belleman R. Harvesting graphics power for MD simulations. *Molecular Simulation*, 2008, vol. 34, no. 3, pp. 259–266. DOI: 10.1080/08927020701744295
9. Harris C., Haines K., Staveley-Smith L. GPU accelerated radio astronomy signal convolution. *Exp. Astron.*, 2008, vol. 22, iss. 1–2, pp. 129–141. DOI: https://doi.org/10.1007/s10686-008-9114-9
10. Muyan-Ozcelik P., Owens J. D., Xia J., Samant S. S. Fast deformable registration on the GPU: A CUDA implementation of demons. In: *Proc. Int. Conf. Computational Science and its Applications*, Perugia, Italy, 2008, pp. 223–233. DOI: https://doi.org/10.1109/ICCSA.2008.22
11. ISO/IEC 9798-5:2009(E): *Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero-knowledge technique*. Available at: https://www.iso.org/standard/50456.html (accessed 05 September 2018).

Cite this article as:
Ratseev S. M., Rostov M. A. Zero-Knowledge Proof Authentication Protocols. *Izv. Saratov Univ. (N. S.), Ser. Math. Mech. Inform.*, 2019, vol. 19, iss. 1, pp. 114–121 (in Russian). DOI: https://doi.org/10.18500/1816-9791-2019-19-1-114-121