IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

# Preserving Voter Privacy and Security in Online Voting through Diffie-Hellman Encryption

**Rosemarie C. Arcaya**
College of Arts and Sciences, Surigao del Norte State University, Surigao City, Philippines

**Abstract:** *This research paper presents an advanced online voting system, incorporating the Diffie-Hellman encryption algorithm, to ensure voter privacy and address key challenges in digital elections. The system offers additional features such as anonymous authentication, verifiable decryption, and secure ballot transmission. Through a rigorous evaluation process, the proposed approach received an overall evaluation score of 3.55 out of 5, indicating its effectiveness in upholding voter privacy and system efficiency. Specific evaluation criteria revealed accuracy with a score of 3.57 out of 5, efficiency at 3.53 out of 5, reliability at 3.54 out of 5, timeliness at 3.50 out of 5, and a commendable security rating of 3.59 out of 5. These results highlight the system's potential in providing a secure and user-friendly online voting platform, encouraging voter participation and reinforcing the democratic principles of transparency and integrity.*

**Keywords:** Diffie-Hellman algorithm, encryption, evaluation, privacy, online voting

## REFERENCES

**[1].** Waller, L. G. (2020). The Possibilities of Internet Voting in Jamaica: Moving from Convenience to Fixing the Problem of Voter Apathy among the Youth. *Electronic Journal of e-Government*, *18*(1), pp17-29.

**[2].** Yao, Y., & Murphy, L. (2007). Remote electronic voting systems: an exploration of voters' perceptions and intention to use. *European Journal of Information Systems*, *16*(2), 106-120.

**[3].** Kara, M., Laouid, A., AlShaikh, M., Bounceur, A., & Hammoudeh, M. (2021). Secure key exchange against man-in-the-middle attack: Modified diffie-hellman protocol. *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, *7*(3), 380-387.

**[4].** Huang, H., & Cao, Z. (2009, March). An ID-based authenticated key exchange protocol based on bilinear Diffie-Hellman problem. In *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security* (pp. 333-342).

**[5].** Jharbade, N. K., & Shrivastava, R. (2012). Network based Security model using Symmetric Key Cryptography (AES 256–Rijndael Algorithm) with Public Key Exchange Protocol (Diffie-Hellman Key Exchange Protocol). *IJCSNS International Journal of Computer Science and Network Security*, *12*(8), 69-74.

**[6].** Pappas, I. O., Mikalef, P., Giannakos, M. N., Krogstie, J., & Lekakos, G. (2018). Big data and business analytics ecosystems: paving the way towards digital transformation and sustainable societies. *Information Systems and e-Business Management*, *16*, 479-491.

**[7].** Jones, B., & Flannigan, S. L. (2006). Connecting the digital dots: Literacy of the 21st century. *Educause Quarterly*, *29*(2), 8-10.

**[8].** Selvarani, X. I., Shruthi, M., Geethanjali, R., Syamala, R., & Pavithra, S. (2017, February). Secure voting system through sms and using smart phone application. In *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)* (pp. 1-3). IEEE.

**[9].** Gibson, R. (2001). Elections online: Assessing Internet voting in light of the Arizona democratic primary. *Political Science Quarterly*, *116*(4), 561-583.

**[10].** Adida, B., De Marneffe, O., Pereira, O., & Quisquater, J. J. (2009). Electing a university president using open-audit voting: Analysis of real-world use of Helios. *EVT/WOTE*, *9*(10).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

**[11].** Halderman, J. A., & Teague, V. (2015). The New South Wales iVote system: Security failures and verification flaws in a live online election. In *E-Voting and Identity: 5th International Conference, VoteID 2015, Bern, Switzerland, September 2-4, 2015, Proceedings 5* (pp. 35-53). Springer International Publishing.

**[12].** Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, J. A. (2014, November). Security analysis of the Estonian internet voting system. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 703-715).

**[13].** Nwankwo, W., Chinedu, P. U., Masajuwa, F. U., Njoku, C. C., & Imoisi, S. E. (2023). Adoption of i-voting infrastructure: addressing network-level cybersecurity breaches. *Electronic Government, an International Journal*, *19*(3), 273-303.

**[14].** Khodzhanovna, S. K. (2023). Cybertech Activities Affecting The Fate Of PoliticaL Elections. *Best Journal of Innovation in Science, Research and Development*, *2*(7), 126-129..

**[15].** Rashed, M. G., Ullah, S., & Yasmin, R. (2013, January). Secured message data transactions with a Digital Envelope (DE)-A higher level cryptographic technique. In *International Conference on Engineering Research, Innovation and Education 2013*.

**[16].** Gupta, M., & Saini, H. (2015). Workload Characterization of Elliptic Curve Cryptography and Other Network Security Algorithms for Constrained Environments.

**[17].** Kajal, B., Vala, B., & Patel, W. (2021, May). A Review of Online Voting System Security based on Cryptography. In *Proceedings of the International Conference on Smart Data Intelligence (ICSMDI 2021)*.

**[18].** Ullah, S., Zheng, J., Din, N., Hussain, M. T., Ullah, F., & Yousaf, M. (2023). Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. *Computer Science Review*, *47*, 100530.

**[19].** Mohedas, I., Daly, S. R., & Sienko, K. H. (2015). Requirements development: Approaches and behaviors of novice designers. *Journal of Mechanical Design*, *137*(7), 071407.

**[20].** Slavin, S., & Schoech, R. (2017). *Human services technology: Understanding, designing, and implementing computer and Internet applications in the social services*. CRC Press.

**[21].** Van der Berg, J. S. (2007). *Generalizations of the Diffie-Hellman protocol: exposition and implementation* (Doctoral dissertation, University of Pretoria).

**[22].** Arancibia, J. D., Smith, V. F., & Fenner, J. L. (2019, November). On-The-Fly Diffie-Hellman for IoT. In *2019 38th International Conference of the Chilean Computer Science Society (SCCC)* (pp. 1-5). IEEE.