Computer Science and Information Technologies
Vol. 6, No. 1, March 2025, pp. 20~27
ISSN: 2722-3221, DOI: 10.11591/csit.v6i1.p20-27

Secure e-voting system using Schorr's zero-knowledge identification protocol

Indah Octaviani Laleb, Daniel M. D. U. Kasse
Department of Electrical Engineering-Computer and Networking, State Polytechnic of Kupang, Kupang, Indonesia

Article Info

Article history:

Received Jul 30, 2024
Revised Dec 13, 2024
Accepted Feb 20, 2025

Keywords:

Cryptography
E-voting
Privacy
Protocol schnorr
Zero-knowledge identification

ABSTRACT

In today's era of technological progress, the electoral system has changed significantly with the introduction of electronic voting (e-voting). The traditional voting system poses many vulnerabilities to manipulation, potential human error, and problems with voter privacy. These limitations can lead to reduced trust and participation in elections. E-voting has emerged to address this issue, aiming to improve the convenience, security, and privacy of voters. E-voting systems are evaluated on accuracy, security, privacy, and transparency; however, ensuring voter privacy while maintaining these principles remains a significant challenge. A potential solution to improving privacy in e-voting is Schorr's zero-knowledge identification protocol. This protocol allows voters to confirm their identity without revealing personal information, maintaining voter privacy throughout the process. By implementing these protocols, the e-voting system can strengthen security and privacy, making elections more transparent and trustworthy. As technology evolves, adopting solutions like Schorr's zero-knowledge identification protocol can help e-voting systems meet the growing demand for safe, fair, and private elections.

Corresponding Author:

Indah Octaviani Laleb
Department of Electrical Engineering-Computer and Networking, State Polytechnic of Kupang
Kupang, Indonesia
Email: indahlaleb2510@gmail.com

1. INTRODUCTION

Electronic voting (e-voting) systems are designed to emulate traditional voting processes [1] through computerized means, aiming to uphold the integrity of the electoral process alongside other essential attributes. However, the increasing interconnection between systems and individuals around the world, as well as the widespread cybersecurity problem, are the main obstacles to realizing this vision [2], [3]. The e-voting process can be deconstructed similarly to conventional voting process, dividing it into fundamental mechanisms [4]. Registration involves adding potential voters to a list of eligible participants. Voter validation is authenticated of voters based on their credentials and eligibility. The collection section includes all submitted votes. Tallying computes, the accumulated votes.

Throughout these specifics, particular prerequisites must be maintained for the e-voting system to remain valid [4]: accuracy, invulnerability, privacy and verifiability. In contrast, e-voting systems require additional and distinct properties due to the characteristics of computer applications [5]–[8], including unreusability, completeness, privacy, eligibility, fairness, verifiability and uncoercibility.

Additionally, e-voting systems must maintain privacy by preserving anonymity and precluding any association between a ballot and its caster. Ensuring the security and integrity of e-voting systems is a critical challenge that requires carefully balancing various, and at times conflicting, requirements [9], [10]. These

systems must maintain voter privacy by preserving anonymity and preventing any link between a ballot and its caster [10]–[13].

Ensuring fairness, security, and individual privacy in election processes is a delicate and complex challenge. Voting systems must uphold fairness by withholding partial election results until the conclusion of the voting session to prevent undue influence on subsequent voters [14]. They must also enable verifiability by allowing independent verification of the tally's accuracy while safeguarding privacy [15]. Additionally, they must maintain uncoercibility by preventing voters from disclosing their vote choices, thereby inhibiting potential coercion or vote buying [11].

To improve e-voting privacy, techniques like blind signatures and zero-knowledge proof (ZKP) are used [5], [16]. Blind signature is a digital signature mechanism used by the applicant to obtain a signature without informing information about the actual message where the message is blinded before being signed [17]. Although the blind signature system and this purpose protocol involve three entities: the validator, the voter or pollster, and the tallier, each of which serves distinct roles [5], [18] .Through the use of a blind signature, the validator and pollster exchange information on two separate occasions. While pairing-based cryptography is a complex cryptographic technique that enables secure, anonymous communication between voters and verifiers [19].

An example of a more secure system involves Schorr's zero-knowledge identification protocol, where a voter can prove their identity without revealing any personal information. Unlike previous systems that use blind signatures and require two exchanges of information, Schorr's zero-knowledge identification protocol uses a "triple message" exchange (a, c, r), requiring four interactions. This additional exchange enhances privacy by ensuring voter identity is protected while still proving eligibility.

2. METHOD

E-voting systems are designed to emulate traditional voting processes through computerized means, aiming to uphold the integrity of the electoral process alongside other essential attributes. The e-voting process can be deconstructed similarly to conventional voting instances, dividing it into four fundamental mechanisms [4]. Registration involves adding potential voters to a list of eligible participants. Validation ensures voters' votes are authenticated based on their credentials and eligibility when casting them. The collection aggregates all submitted votes. Tallying computes, the accumulated votes. Throughout these operations, specific prerequisites must be maintained for the e-voting system to remain valid [4]:

- Accuracy: ensuring the impossibility of vote manipulation. Preventing legal exclusion or illegal inclusion of votes in the final tally and detecting and correcting any inaccuracies to achieve a flawless final count.
- Invulnerability: ensuring that votes are cast only by eligible voters. They are restricting each eligible voter to a single vote.
- Privacy: precluding the ability to link a vote to its caster. Preventing voters from disclosing their vote choices, thus mitigating potential influences such as vote buying or coercion.
- Verifiability: facilitating independent entities to tally all valid votes accurately, allowing voters to verify their votes while maintaining privacy.

In contrast, e-voting systems require additional and distinct properties due to the characteristics of computer applications [5]:

a) Soundness, unreusability, completeness:
   - Soundness: ensuring the election cannot be invalidated by any voter, and rectifying any identified errors in the final tally.
   - Un-reusability: prohibiting voters from casting multiple votes.
   - Completeness: guaranteeing the absence of counterfeit votes, withdrawal of verified votes, or inclusion of invalid votes in the final tally.

b) Privacy: preserving anonymity by precluding any association between a ballot and its caster.
c) Eligibility: allowing all eligible and registered voters to participate in the voting process.
d) Fairness: withholding partial election results to maintain the secrecy of voted ballots until the conclusion of the voting session, thus preventing undue influence on subsequent voters.
e) Verifiability: enabling independent verification of the tally's accuracy, with the option for voters to verify their votes while safeguarding privacy.
f) Uncoercibility: preventing voters from disclosing their vote choices, thereby inhibiting potential coercion or vote buying.

The concept of securing e-voting using a blind signature was previously developed [16]. This approach to e-voting security has also been applied [5] by implementing a blind signature in the Applet system. Both methods enable anonymous communication between voters and verifiers without disclosing additional information. Compared to this report, their systems excel in terms of security protocol complexity, application implementation, and the efficiency of pairing-based cryptography. Although the secure e-voting Applet system

(SEAS) system and the protocol in question involve entities such as validator, voter/pollster, and tallier-there are notable differences between them [5], [18]. In the blind signature-based system, the validator and pollster exchange information twice. Conversely, in this report's system, utilizing ZKP requires four exchanges of information. This is because the voter identity verification relies on Schnorr's zero-knowledge identification protocol, which involves a triple-message protocol (a, c, r) to confirm voter identity without revealing additional information.

The design of e-voting systems involves a delicate balance between these competing requirements. Maintaining voter privacy, for example, can come into tension with the need for verifiability, as revealing the full tally of votes could compromise the anonymity of voters, particularly in elections with a small number of participants [20] and precluding any association between a ballot and its caster. The system ensure eligibility by allowing all eligible and registered voters to participate in the voting process, uphold fairness by withholding partial election results until the conclusion of the voting session to prevent undue influence on subsequent voters, enable verifiability by allowing independent verification of the tally's accuracy while safeguarding privacy, and maintain uncoercibility by preventing voters from disclosing their vote choices. Thus, the potential for coercion or vote buying can be inhibited.

Among the four fundamental properties, basic e-voting systems fail to ensure privacy. The system needs to protect the voter's identity, which is associated with a specific vote. To achieve this, the validator must offer a mechanism that enables voters to keep their identities hidden [8], [21]. One possible solution is to implement Schnorr's zero-knowledge identification protocol.

Imagine a scenario where voters, when casting a vote, must receive additional information from validators. This process starts with voter registration, during which the voter must verify their identity with the validator. Once the validator confirms the voter's identity, it validates the vote, allowing the voter to submit it to the tallier. It is important to note that Rivest-Shamir-Adleman (RSA) is employed for encryption and decryption throughout this process.

Voter

- Compute $x \leftarrow log_g h$, where $g \in G$ is a fixed public generator
- Select $u \in_R \mathbb{Z}_n$
- Compute $a \leftarrow g^u$
- Send a to the validator
- Upon receiving c
  - Compute $r \leftarrow_n u + cx$
  - Compute v_h hidden vote as $v_h = Enc_{V-PK}(v^R)$, where $V - PK$is the public key of the voter,$v$is the voting information and $R$is some random number
  - Send r and v_h vote to the validator
- Upon receiving DS_{Va}
  - Compute v_s as $v_s \leftarrow (Dec_{V-PrK}(DS_{Va}))^{-R}$ such that $v_s \leftarrow v^{Va-PrK} mod\ n$
  - Construct the vote as $Vote = Enc_{T-PK}(v, v_s)$, where $T - PK$ is the public key of the tallier
  - Send $Vote$ to tallier

Validator

- Upon receiving a
  - Select $c \in_R \mathbb{Z}_n$
  - Send c to the voter
- Upon receiving r and v_h
  - If $g^r = ah^c$
    - Compute DS_{Va} using the validator private key, $DS_{Va} \leftarrow Enc_{Va-PrK}(v_h)$

Send DS_{Va} to the voter

In the outlined protocol, a voter verifies their identity with the validator. If the validator confirms the voter's legitimacy, it signs the concealed vote submitted by the voter. This approach can be further enhanced to obscure the voter's identity by employing the OR composition of 1-to-l combinations, where l represents the number of voters.

RSA encryption and decryption techniques are used to generate hidden messages. RSA enables mathematical transformations to process the vote, allowing the voter to eliminate any connections between

their identity and the voting information. Once the vote is prepared, the voter submits it to the tallier. As the complexity of modern voting systems continues to escalate, the need for comprehensive security measures becomes paramount. Researchers have proposed various models and attack scenarios to evaluate the resilience of such systems, considering the potential corruption and computational capabilities of adversaries. [22]. In particular, the voting platforms themselves may be compromised, necessitating solutions that can safeguard the privacy and integrity of votes even in the face of such threats.

2.1. 1-to-l combination zero-knowledge solution

In a group of voters, when verifying eligibility, a voter can demonstrate their membership in the group without revealing their identity [23], ensuring anonymity through ZKP. To maintain anonymity, the voter must establish their relationship by executing l number of proofs, where one of the 1 of l triple (a, c, r) operations is valid, while the remaining l–l operations appear valid. This allows the voter to confirm their identity as one of the 1 authorized voter without disclosing their identity to the validator.

Voter

- Let x_1 be the real secret. Compute $x_1 \leftarrow log_g h_1$, where $g \in G$ is a fixed public generator
- Select $(u_1, (r_2, \ldots, r_l), (c_1, \ldots, c_l)) \in_R \mathbb{Z}_n$
- Compute $a_1 \leftarrow g^{u_1}$
- For $i \in \{2, \ldots, l\}$
  - $a_i \leftarrow g^{r_i} h_1^{-c_i}$
- Send $a = \{a_1, \ldots, a_l\}$ to the validator
- Upon receiving c
  - Compute $c_1 \leftarrow c - (\sum_{i=2}^{l} \quad c_i)$
  - Compute $r_1 \leftarrow u_1 + c_1 x_1$
  - Compute v_h hidden vote as $v_h = Enc_{V-PK}(v^R)$, where $V - PK$is the public key of the voter,$v$is the voting information and $R$is some random number
  - Send $((c_1, r_1), \ldots, (c_l, r_l))$ and v_h vote to the validator
- Upon receiving DS_{Va}
  - Compute v_s as $v_s \leftarrow (Dec_{V-PrK}(DS_{Va}))^{-R}$ such that $v_s \leftarrow v^{Va-PrK} mod\ n$
  - Construct the vote as $Vote \leftarrow Enc_{T-PK}(v, v_s)$, where $T - PK$ is the public key of the tallier
  - Send $Vote$ to tallier

Validator

- Upon receiving a
  - Select $c \in_R \mathbb{Z}_n$
  - Send c to the voter
- Upon receiving $((c_1, r_1), \ldots, (c_l, r_l))$ and v_h
  - If $c = \sum_{i=1}^{l} \quad c_i$
    - For $i \in \{1, \ldots, l\}$
      - If $g^{r_i} = a_i h_i^{c_i}$
        - Compute DS_{Va} using the validator private key, $DS_{Va} \leftarrow Enc_{Va-PrK}(v_h)$
        - Send DS_{Va} to the voter

Exit (only requires one relation to be true)

3. RESULTS AND DISCUSSION

A straightforward and intuitive Python code has been used to demonstrate the 'proof of concept' for the proposed functionality of this protocol. The code focuses on illustrating how the 1 in l zero-knowledge solution, as outlined in this paper, works, using Schnorr's ID as the core principle. The code simulates the calculations and validations expected from the voter and validator entities, but it does not handle values in the typical transactional manner. It uses standard cryptographic libraries available in Python to implement RSA encryption and decryption of votes, as well as the signing and verification of signatures to authenticate the Validator. A sample output from the program is shown in Figure 1.

3.1. Efficiency evaluation

For the practical application of the comprehensive library for this e-voting system, the zero-knowledge proof description language (ZKPDL) is the ideal framework. The framework efficiently integrates cryptographic and software components in the implementation while supporting verifiable encryption and other computational optimizations [24]. Integrating the ZKPDL compiler would enable the full recreation of the protocol. However, since only a single functionality needed to be evaluated in the implementation, this framework was deemed unnecessary for the scope of the project.

When evaluating the computation times for different numbers of users in the voting system, it was observed that the program's compilation time increased incrementally. Analysing the code and the loops within the execution process suggests that the time complexity is O(l), where l represents the number of voters in the system. This means that the protocol's execution time would scale in proportion to the value of l.

3.2. Security evaluation

3.2.1. Accuracy

To maintain the integrity of voting information, including voter IDs and unique government credentials sent over the network for data validation in databases, it must be protected from corruption. In addition, the selector's device is at risk of being infected with malware or malicious software that goes undetected. These malware scripts, or the process of sending information over a network, can open the system up to threats such as man-in-the-middle attacks, eavesdropping, and malware attacks, where attackers can manipulate, steal, or exploit data by intercepting network traffic. To protect e-voting systems from such threats, data is sent in an encrypted format, equipped with digital signatures, and secured using message authentication protocols [25]. The RSA encryption/decryption algorithm is used, while digital signatures ensure that information sent over the network is encrypted with the voter's public key, which can only be decrypted with the corresponding private key.

– Replay attack: this type of attack occurs when sensitive messages or information sent between the sender and receiver are intercepted. Then, the captured data is sent back to the network by posing as a legitimate node for malicious purposes. The proposed ZKP protocol for the e-voting system helps reduce the risk of such attacks by implementing several random challenge questions. The attacker cannot capture the data successfully, as they are unable to provide correct answers to all the challenge questions. Consequently, the authentication process fails, preventing the attack.
– Man-in-the-middle attack: in this attack, an attacker intercepts and establishes connections between the prover and verifier to alter and forward the data between them. According to our ZKP protocol model, the attacker would be unable to establish such connections, as they will not gain any information about the legitimate node's private key from the communication between the prover and verifier.

Figure 1. Sample output program

3.2.2. Invulnerability

This property can be ensured as follows:

- Clone attack: a clone attack occurs when a legitimate node or voter is duplicated, creating counterfeit cryptographic information. One method involves cloning the node with a different node ID but the same cryptographic data as the original node. In this situation, the ZKP authentication process will fail and prevent the continuation of data transfer because the base station cannot validate the cloned node ID due to a mismatch with the private key. Alternatively, other methods may use valid node IDs but with different cryptographic information, such as unequal private keys. However, ZKP authentication will still fail, stopping data transfer between nodes, as the cloned node ID and private key cannot be verified by the base station. As a result, any unauthorized individual would be unable to convince the verifier that they are the legitimate node [26].
- Interleaving attack: in this attack, an adversary attempts to predict the network pattern and engage with the legitimate voter using previously collected protocol information. The ZKP model's high complexity significantly reduces or eliminates the likelihood of an attacker gathering such protocol details. Even if an attacker manages to obtain this information, they would still be unable to predict the challenge questions, as these are randomly generated by the verifier for each round [4].

3.2.3. Privacy

Privacy is guaranteed through the implementation of Schnorr's zero-knowledge identification protocol. Ballots are encrypted using the public key of the back-end system, so voter anonymity is maintained, with only the appropriate private key being able to decrypt it. One of these threats to privacy is a secrecy attack, where perpetrators pose as verifiers to steal sensitive information from trusted parties. To address the threat, the proposed ZKP protocol implements two-way authentication, ensuring that the base station first authenticates the verifier before gaining access to personal information in the process of proving [4].

3.2.4. Verifiability

Voters can be verified using a receipt or message confirmation. Additionally, encrypted ballots can be accessed, allowing each voter to check the presence of their ballot. By utilizing the ZKP protocol, voter eligibility can be verified, ensuring that each voter casts only one vote in each election through a challenge and response mechanism [25].

4. CONCLUSION

Although Schnorr's zero-knowledge identification protocol is designed to ensure voter anonymity, securing the exchange of information between voters and verifiers should be a primary concern when designing this system. As a solution, implementing the Diffie–Hellman key exchange could enhance security during information exchange between the two parties. Additionally, since this protocol prioritizes voter anonymity, other aspects of the system, such as vote tallying, have been overlooked. For instance, the system does not include a method for counting votes. Therefore, another protocol is needed to utilize homomorphic encryption to verify the tally. Another aspect to consider is that this protocol is a basic application, offering only four properties: accuracy, invulnerability, privacy, and verifiability. E-voting, however, is a more complex application that emphasizes high security to protect the system and minimize inaccuracies in vote counting. Additionally, since this system involves four exchanges of information for assessment, it takes more time to complete the process. In contrast, a blind signature is more efficient, requiring only two information exchanges, thus saving time.

5. FUTURE WORKS

The proposed e-voting system offers significant security features, yet further advancements are essential to tackle additional complexities and elevate security measures comprehensively. The system aims to improve voter privacy and security by allowing voters to confirm their identities without revealing additional information, thus protecting their privacy during the voting process. However, ongoing improvements are necessary to ensure the system effectively addresses potential vulnerabilities and maintains the principles of accuracy, vulnerability, privacy, and verifiability in the voting process. Future work will focus on incorporating advanced cryptographic techniques, strengthening authentication protocols, and expanding the system's robustness against emerging security challenges, ensuring it is both reliable and resilient in real-world applications.

ACKNOWLEDGMENTS

We sincerely appreciate the Department of Electrical Engineering, Computer, and Network Program at the State Polytechnic of Kupang for their invaluable guidance, expertise, and unwavering support, which have been instrumental in the successful completion of this research.

FUNDING INFORMATION

This research was funded by the DIPA funds of the State Polytechnic of Kupang in 2024.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Indah Octaviani Laleb	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		
Daniel M.D.U. Kasse			✓	✓		✓	✓	✓	✓	✓			✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

No data are available for sharing as this study did not use an external dataset.

REFERENCES

[1] M. Bernhard, "Everything you should know about online voting," *XRDS: Crossroads, The ACM Magazine for Students*, vol. 27, no. 2, pp. 66–69, Dec. 2020, doi: 10.1145/3433138.

[2] L. Carr, A. J. Newtson, and J. Joshi, "Towards modernizing the future of american voting," in *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, Oct. 2018, pp. 130–135, doi: 10.1109/CIC.2018.00028.

[3] R. Casado-Vara and J. M. Corchado, "Blockchain for democratic voting: how blockchain could cast off voter fraud," *Oriental Journal of Computer Science and Technology*, vol. 11, no. 1, pp. 1–3, Mar. 2018, doi: 10.13005/ojcst11.01.01.

[4] L. F. Cranor and R. K. Cytron, "Sensus: a security-conscious electronic polling system for the internet," in *Proceedings of the Thirtieth Hawaii International Conference on System Sciences*, 1997, vol. 3, pp. 561–570, doi: 10.1109/HICSS.1997.661700.

[5] F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi, and A. Vaccarelli, "SEAS, a secure e-voting protocol: design and implementation," *Computers & Security*, vol. 24, no. 8, pp. 642–652, Nov. 2005, doi: 10.1016/j.cose.2005.07.008.

[6] D. Bernhard, V. Cortier, D. Galindo, O. Pereira, and B. Warinschi, "SoK: a comprehensive analysis of game-based ballot privacy definitions," in *2015 IEEE Symposium on Security and Privacy*, 2015, pp. 499–516, doi: 10.1109/SP.2015.37.

[7] P. Chaidos, V. Cortier, G. Fuchsbauer, and D. Galindo, "BeleniosRF: a non-interactive receipt-free electronic voting scheme," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Oct. 2016, pp. 1614–1625, doi: 10.1145/2976749.2978337.

[8] V. Cortier, D. Galindo, S. Glondu, and M. Izabachène, "Election verifiability for helios under weaker trust assumptions," in *Computer Security - ESORICS 2014*, 2014, pp. 327–344, doi: 10.1007/978-3-319-11212-1_19.

[9] D. Bernhard, O. Kulyk, and M. Volkamer, "Security proofs for participation privacy, receipt-freeness and ballot privacy for the helios voting scheme," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, Aug. 2017, pp. 1–10, doi: 10.1145/3098954.3098990.

[10] L. Langer, A. Schmidt, J. Buchmann, M. Volkamer, and A. Stolfik, "Towards a framework on the security requirements for electronic voting protocols," in *2009 First International Workshop on Requirements Engineering for e-Voting Systems*, Aug. 2009, pp. 61–68, doi: 10.1109/RE-VOTE.2009.9.

[11] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in *Advances in Cryptology – CRYPTO 2004*, 2004, pp. 56–72, doi: 10.1007/978-3-540-28628-8_4.

[12] S. Sundaresan, R. Doss, and W. Zhou, "Zero knowledge grouping proof protocol for RFID EPC C1G2 tags," *IEEE Transactions on Computers*, vol. 64, no. 10, pp. 2994–3008, Oct. 2015, doi: 10.1109/TC.2015.2389829.

[13] M. K. Mustafa and S. Waheed, "An e-voting framework with enterprise blockchain," in *Advances in Distributed Computing and Machine Learning*, 2021, pp. 135–145, doi: 10.1007/978-981-15-4218-3_14.

[14] M. Bernhard *et al.*, "Public evidence from secret ballots," in *Electronic Voting*, 2017, pp. 84–109, doi: 10.1007/978-3-319-68687-5_6.

[15] X. Zou, H. Li, F. Li, W. Peng, and Y. Sui, "Transparent, auditable, and stepwise verifiable online e-voting enabling an open and fair election," *Cryptography*, vol. 1, no. 2, Aug. 2017, doi: 10.3390/cryptography1020013.

[16] L. Lopez-Garcia, L. J. D. Perez, and F. Rodriguez-Henriquez, "A pairing-based blind signature e-voting scheme," *The Computer Journal*, vol. 57, no. 10, pp. 1460–1471, Oct. 2014, doi: 10.1093/comjnl/bxt069.
[17] A. A. Thu and K. T. Mya, "Implementation of an efficient blind signature scheme," *International Journal of Innovation, Management and Technology*, vol. 5, no. 6, 2014, doi: 10.7763/ijimt.2014.v5.556.
[18] A. Fujioka, T. Okamoto, and K. Ohta, "A practical secret voting scheme for large scale elections," in *Advances in Cryptology — AUSCRYPT '92*, 1993, pp. 244–251, doi: 10.1007/3-540-57220-1_66.
[19] N. Koblitz and A. Menezes, "Pairing-based cryptography at high security levels," in *Cryptography and Coding*, 2005, pp. 13–36, doi: 10.1007/11586821_2.
[20] R. Küsters, J. Liedtke, J. Müller, D. Rausch, and A. Vogt, "Ordinos: a verifiable tally-hiding remote e-voting system," in *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2020, pp. 216–235, doi: 10.1109/EuroSP48549.2020.00022.
[21] C. P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161–174, Jan. 1991, doi: 10.1007/BF00196725.
[22] S. Bursuc, C.-C. Dragan, and S. Kremer, "Private votes on untrusted platforms: models, attacks and provable scheme," in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2019, pp. 606–620, doi: 10.1109/EuroSP.2019.00050.
[23] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM Journal on Computing*, vol. 18, no. 1, pp. 186–208, Feb. 1989, doi: 10.1137/0218012.
[24] S. Meiklejohn, C. C. Erway, A. Küpçü, T. Hinkle, and A. Lysyanskaya, "ZKPDL: a language-based system for efficient zero-knowledge proofs and electronic cash," in *Proceedings of the 19th USENIX Security Symposium*, 2010, pp. 1–16.
[25] R. Abdelkader and M. Youssef, "UVote: a ubiquitous e-voting system," in *2012 Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing*, Jun. 2012, pp. 72–77, doi: 10.1109/MUSIC.2012.20.
[26] M. Mozumdar, M. Aliasgari, S. M. V. Venkata, and S. S. Renduchintala, "Ensuring authentication and security using zero knowledge protocol for wireless sensor network applications," *International Journal of Computing and Digital Systems*, vol. 5, no. 3, pp. 225–234, May 2016, doi: 10.12785/ijcds/050303.

BIOGRAPHIES OF AUTHORS

Indah Octaviani Laleb holds a master's degree in networks and security from the prestigious Faculty of Information Technology at Monash University, where she specialized in security and networking. With a wealth of knowledge and experience, she currently serves as a lecturer at the State Polytechnic of Kupang. She can be contacted at email: indahlaleb2510@gmail.com.

Daniel M. D. U Kasse, S.Kom., M.Eng. is a lecturer in the Computer and Network Engineering Study Program at STIKOM Uyelindo Kupang specializing in courses such as PC hardware, operating systems, and mobile applications. He holds a bachelor's degree in information systems from STIKOM Uyelindo Kupang (2010) and a master's degree in information technology from Gadjah Mada University (2015). His research includes developing an English learning assistant application with a rule-based system and studying the naïve Bayes classifier method for credit eligibility prediction, both in 2022. Active in community service, he worked on promoting mangrove tourism in Oesapa Barat Village in 2022. Additionally, he served as a field supervisor for the national Wirausaha Merdeka program in 2022. He can be contacted at email: adenndenny@gmail.com.