Using Ring Signatures For An Anonymous E-Voting System

Oleksandr Kurbatov
Department of information technologies security
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine,
olkurbatov@gmail.com

Pavel Kravchenko
Distributed Lab
Kharkiv, Ukraine
pavel@distributedlab.com

Nikolay Poluyanenko
Department of information systems and technologies security
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine
nlfsr01@gmail.com

Oleksiy Shapoval
Department of information systems and technologies security
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine
alex.shapoval@protonmail.com

Tetiana Kuznetsova
Department of information systems and technologies security
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine
kuznetsova.tatiana17@gmail.com

***Abstract*—This paper describes the mechanisms for using ring signatures to ensure anonymity in a decentralized e-voting system. Unlike standard signature algorithms that allow you to uniquely authenticate the authorship of the signature, a ring signature allows you to hide the true public key for verification among the public keys of other participants in the system. At the same time, the use of blockchain technology allows you to verify the integrity of the users votes, as well as verify their authenticity (binding with valid public keys) and to ensure transparency in the calculation of votes and verification of the correctness of the accounting of its votes by an individual user.**

Keywords—blockchain technology; public key infrastructure; decentralized system; e-voting system

I. Introduction

Voting is a way of making a single final decision regarding something within a certain group. Different voting systems put forward different requirements for the ongoing processes, but the goal remains the same - taking into account the decisions of voters regarding something [1-3].

Traditional voting systems have ceased to be effective in terms of their requirements [1, 4-7]: paper ballots, pseudo-anonymity of voters, non-transparency of the vote count (this is especially critical for our regions), the dependence of (the entire) voting procedure on the central organization. In fact, these are only the most critical problems existing in existing voting systems.

In recent years, the digitization of the voting process is developing more and more actively. The most prominent examples are the introduction of a digital voting system for electing local authorities in Estonia since 2005 and attempts to introduce such a system in Switzerland, Netherlands, India and Namibia [8-10]. However, existing solutions still have a number of flaws, in particular, vulnerabilities associated with the central authority checking all results [11-14].

The approach described above allows conduct e-voting while ensuring the transparency of processes and the integrity of the voting history [8, 9]. However, some voting systems also require another property for system users anonymity [14-17]. It is necessary to further investigate the methods and mechanisms of cryptographic protection of information [18-29], various protocols for ensuring integrity, authenticity, confidentiality and other security services [30-37].

Further, we will describe how to ensure voters' anonymity while maintaining all other properties of an accounting system.

II. Ring Signature Mechanism

Ring signatures are used to ensure the anonymity of users among a specific set of other members of a group (ring). To generate such a signature, the user uses the public keys of other users and his key pair. When verifying a signature, a verifier can verify that it was calculated by one of the members of the ring, but it is not known by whom exactly [38].

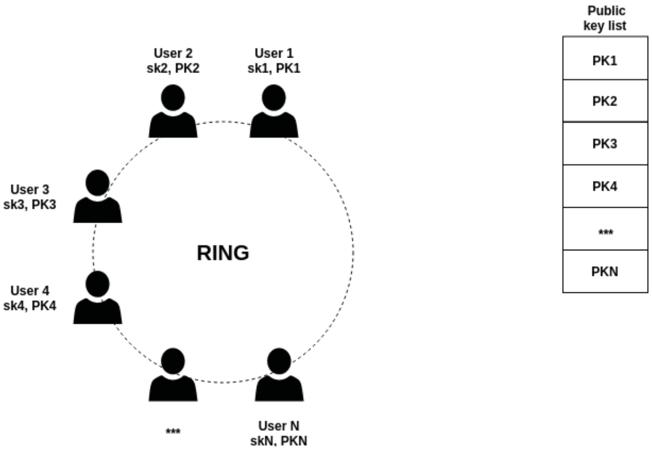

Fig. 1. Ring formation process

Imagine a group of n users, as in Figure 1. Each user has his own key pair — a secret and public key (sk, PK). Secret keys are known only to their owners, public keys - to all participants of the system.

IEEE ATIT 2019 ISBN 978-1-72-81-61-44-0/19/$31.00©2019 IEEE

In order to form a signature on behalf of the group, the user must input the public keys of all the ring participants (including his own) to the algorithm input, and use his own private key as a secret. Recall that the public keys of each of the participants are publicly available. Figure 2 shows how the ring signature is generated by the user number 4.

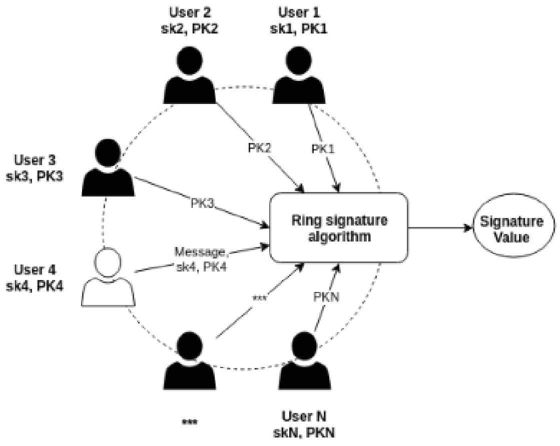

Fig. 2. Signature calculation process

When the verifier checks the value of the signature, he can verify that the signature was guaranteed to be calculated by one of the group members, however, he can only guess who it is with a certain probability. Only with a probability of 1 / n can he determine that the signature was calculated by a specific participant in the ring (Figure 3).

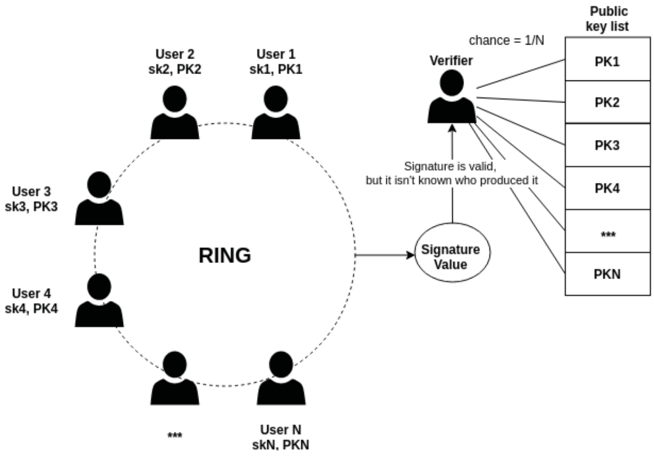

Fig. 3. Ring signature verification process

It is worth noting that the user can be disclosed only in the case of collusion of all the other members of the group [39].

III. Architecture of Decentralized E-Voting System

The decentralized anonymous voting system consists of the following elements: Validators; User identity system; End users.

Schematically, the arrangement of components and their interconnection can be represented in Figure 4. Nodes validators are the main nodes of the system. They process user transactions and reach consensus on a distributed database. User identification systems are required to provide information about user identifiers with which users will prove their right to vote. The identification system can be either a centralized internal (or external) identity provider, or a distributed identification and certification system. End users perform the role of voters in the system. They independently vote for making a certain decision. It is important to ensure their anonymity, and at the same time transparency in the voting process.

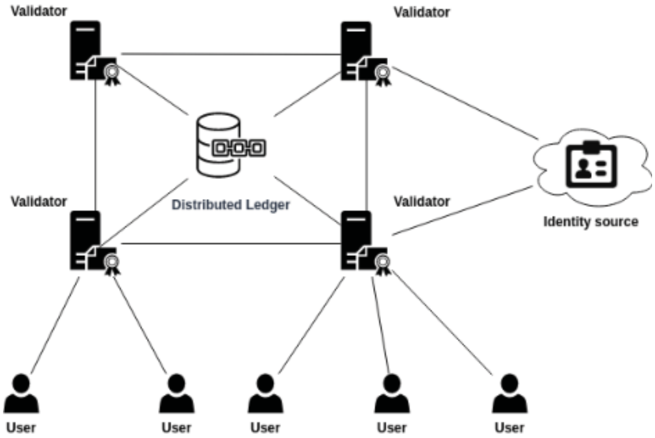

Fig. 4. E-voting system components

For voting, the user should form and sign the corresponding transaction. The transaction structure is as follows (Figure 5):

Transaction ID
Nonce
Candidate ID
Timestamp
Public keys of group
Signature

Fig. 5. Transaction structure

The transaction identifier is a hash value from all other transaction fields. The nonce field contains a random value and is used to make the transaction unique. Candidate ID contains the identifier of the voting entity for which the voter wants to cast his vote. Timestamp - UNIX value of the transaction formation time. Public keys of group is a list of public keys of the participants of the ring (those used to generate the signature). Among these keys is also the voter's public key, but his position is unknown. Signature is the transaction signature value. Note that this transaction structure is not strict, additional fields may be present.

In order to sign a transaction and at the same time ensure the anonymity of the vote, the user selects a list of keys of other users. At the same time, it is important that the selected public keys really belong to other voters (they had permission to vote). The list of public keys of voters should be open to all participants in the system. This list is formed before the start of voting (registered and provided the public key - got into the voter list). The number of selected keys depends on the level of anonymity of the voter. If the selected group is small, then the probability of de-anonymization of the voter is much higher [40]. After the user selects a set of public keys, he calculates the value of the ring signature for the transaction. After that, it sends the transaction to one of the platform validators (or several) as in Figure 6. After the validator receives a transaction, he must verify that the sender has the right to vote. Note that the validator does not know the identifier of the sender of the transaction (or rather, he does not know which of the public keys specified in the transaction belongs to the voter). Therefore, it needs to check the permissions of all keys specified in the transaction. If all the specified keys have permission to vote, then the transaction is correct and can be confirmed [41]. At this stage, there is also a need to check that the user cannot conduct several transactions from different groups (since the sender of each transaction is unknown, then without a protection mechanism, the attacker can conduct transactions by constantly changing groups, and all of them will be valid). The image of a secret key is used as a protective mechanism [39].

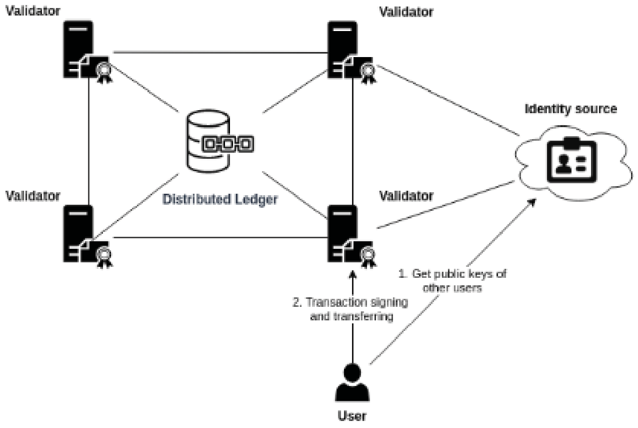

Fig. 6. Transaction formation process

Since this image is unique for each key pair (and it is used in creating and verifying signatures), the user cannot sign several transactions using the same secret key. The transaction confirmation process is shown in Figure 7.

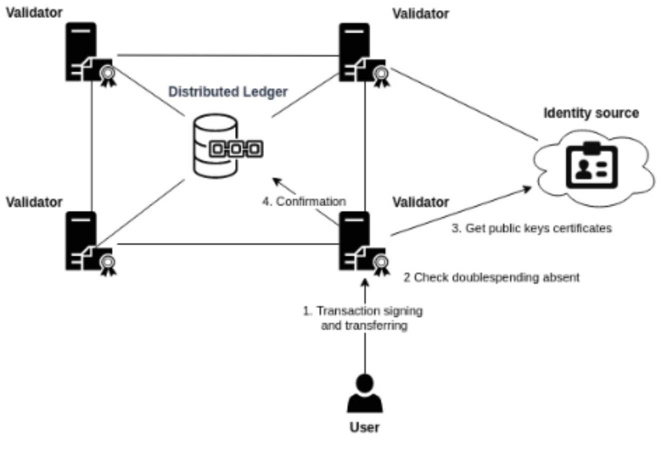
Validator
Validator
Distributed Ledger
Identity source
Validator
4. Confirmation
Validator
3. Get public keys certificates
2 Check doublespending absent
1. Transaction signing and transferring
User

Fig. 7. Transaction verification process

IV. CONCLUSION

Using the described approach to build an anonymous e-voting system allows you to achieve the following benefits:

- the ability to verify voter permissions (voting rights);
- anonymity;
- the ability of the voter to check the accuracy of his own voice;
- inability to conduct a double waste attack.

On the one hand, this approach allows validators to check whether the sender of a transaction has the right to vote (if he used the existing public keys of other participants to form the ring).

At the same time, a specific voter can only be determined by validators with a certain probability (the larger the ring size, the less likely it is). In addition, a user can be completely deanonymized if ALL of the other members of the group collude (and reveal their votes).

Each user can make sure that his voice has been added to the distributed registry. In addition, each owner of the complete site can verify that the voting results correspond to the set of completed transactions.

The user cannot create new transactions with different groups, if you use the mechanism of protection against attacks with double costs (the image of the private key).

Also based on this scheme, the user may be allowed to change the value of his voice. In this case, not one transaction will be counted, but the last transaction that was added to the block chain. However, in this case it is necessary to develop and implement security measures to prevent spam attacks and other attacks that may affect system performance [44-48], as well as data stored in the chain [49-53].

REFERENCES

[1] A. Rodríguez-Pérez, "Secret suffrage in remote electronic voting systems," 2017 Fourth International Conference on eDemocracy & eGovernment (ICEDEG), Quito, 2017, pp. 277-278.

[2] R. Stein and G. Wenda, "The Council of Europe and e-voting: history and impact of Rec(2004)11," 2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE), Lochau, 2014, pp. 1-6.

[3] J. Pomares, I. Levin, R. M. Alvarez, G. L. Mirau and T. Ovejero, "From piloting to roll-out: voting experience and trust in the first full e-election in Argentina," 2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE), Lochau, 2014, pp. 1-10.

[4] Bhuvanapriya R., Rozil Banu S., Sivapriya P. and Kalaiselvi V.K.G., "Smart voting," 2017 2nd International Conference on Computing and Communications Technologies (ICCCT), Chennai, 2017, pp. 143-147.

[5] K. Weldemariam, A. Mattioli and A. Villafiorita, "Managing Requirements for E-Voting Systems: Issues and Approaches," 2009 First International Workshop on Requirements Engineering for e-Voting Systems, Atlanta, GA, 2009, pp. 29-37.

[6] A. F. N. Al-Shammari, K. Weldemariam, A. Villafiorita and S. Tessaris, "Vote verification through open standard: A roadmap," 2011 International Workshop on Requirements Engineering for Electronic Voting Systems, Trento, 2011, pp. 22-26.

[7] A. Schmidt, L. Langer, J. Buchmann and M. Volkamer, "Specification of a Voting Service Provider," 2009 First International Workshop on Requirements Engineering for e-Voting Systems, Atlanta, GA, 2009, pp. 9-18.

[8] G. Schryen and E. Rich, "Security in Large-Scale Internet Elections: A Retrospective Analysis of Elections in Estonia, The Netherlands, and Switzerland," in IEEE Transactions on Information Forensics and Security, vol. 4, no. 4, pp. 729-744, Dec. 2009.

[9] V. P. Singh, H. Pasupuleti and N. S. C. Babu, "Analysis of internet voting in India," 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2017, pp. 1-6.

[10] N. Mpekoa and D. van Greunen, "E-voting experiences: A case of Namibia and Estonia," 2017 IST-Africa Week Conference (IST-Africa), Windhoek, 2017, pp. 1-8.

[11] J. Epstein, "Electronic Voting," in Computer, vol. 40, no. 8, pp. 92-95, Aug. 2007.

[12] C. Garcia-Zamora, F. Rodriguez-Henriquez and D. Ortiz-Arroyo, "SELES: an e-voting system for medium scale online election," Sixth Mexican International Conference on Computer Science (ENC'05), Puebla, Mexico, 2005, pp. 50-57.

[13] B. Kang, "Cryptanalysis on an E-voting Scheme over Computer Network," 2008 International Conference on Computer Science and Software Engineering, Hubei, 2008, pp. 826-829.

[14] A. D. Rubin and D. R. Jefferson, "New Research Results for Electronic Voting," in IEEE Security & Privacy, vol. 6, no. 3, pp. 12-13, May-June 2008.

[15] S. F. Mjølsnes, S. Mauw, and S. K. Katsikas, Eds., “Public Key Infrastructure,” Lecture Notes in Computer Science, 2008.

[16] A. Maeda, “PKI Solutions for Trusted E-Commerce: Survey of the De Facto Standard Competition in PKI Industries,” Information Technology Policy and the Digital Divide.

[17] D. Chadwick and G. Zhao, Eds., “Public Key Infrastructure,” Lecture Notes in Computer Science, 2005.

[18] A. Kuznetsov, Y. Yeromin, O. Shapoval, K. Chernov, M. Popova and K. Serdukov, "Automated Software Vulnerability Testing Using Deep Learning Methods," *2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON)*, Lviv, Ukraine, 2019, pp. 837-841. doi: 10.1109/UKRCON.2019.8879997

[19] J. Lopez, P. Samarati, and J. L. Ferrer, Eds., “Public Key Infrastructure,” Lecture Notes in Computer Science, 2007.

[20] J. Davies, “Implementing SSL/TLS Using Cryptography and PKI,” Dec. 2010.

[21] A. S. Atzeni and A. Lioy, Eds., “Public Key Infrastructure,” Lecture Notes in Computer Science, 2006.

[22] I. Gorbenko, A. Kuznetsov, Y. Gorbenko, A. Pushkar’ov, Y. Kotukh and K. Kuznetsova, "Random S-Boxes Generation Methods for Symmetric Cryptography," *2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON)*, Lviv, Ukraine, 2019, pp. 947-950. doi: 10.1109/UKRCON.2019.8879962

[23] Khader, D., Smyth, B., Ryan, P. and Hao, F., 2012. A fair and robust voting system by broadcast. Lecture Notes in Informatics (LNI), Proceedings-Series of the Gesellschaft fur Informatik (GI), pp.285-299.

[24] Blazy, O., Gaborit, P., Schrek, J. and Sendrier, N., 2017, June. A code-based blind signature. In 2017 IEEE International Symposium on Information Theory (ISIT) (pp. 2718-2722). IEEE.

[25] W. T. Polk and K. Seamons, “6th annual PKI R&D workshop ‘Applications-Driven PKI’ proceedings,” 2007.

[26] Liu, Y. and Wang, Q., 2017. An E-voting Protocol Based on Blockchain. IACR Cryptology ePrint Archive, 2017, p.1043.

[27] B. Schneier, “Applied Cryptography, Second Edition,” Oct. 2015.

[28] A. A. Kuznetsov, Yu. I. Gorbenko, D. I. Prokopovych-Tkachenko, M. S. Lutsenko, M. V. Pastukhov. “NIST PQC: Code-Based Cryptosystems.” Telecommunications and Radio Engineering, Volume 78, 2019, Issue 5, pp. 429-441.

[29] Young, A. and Yung, M., 1997, May. Kleptography: Using cryptography against cryptography. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 62-74). Springer, Berlin, Heidelberg.

[30] A. Kuznetsov, A. Kiian, M. Lutsenko, I. Chepurko and S. Kavun, "Code-based cryptosystems from NIST PQC," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 282-287.

[31] G. Guo, J. Zhang, and J. Vassileva, “Improving PGP Web of Trust through the Expansion of Trusted Neighborhood,” 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology, Aug. 2011.

[32] Liang, H., Zheli, L., Tao, S. and Fang, L., 2009. Survey of security on identity-based cryptography [j]. Journal of Computer Research and Development, 46(9), pp.1537-1548.

[33] D. Wueppelmann, “PGP Auth: Using Public Key Encryption for Authentication on the Web.”

[34] Chan, P.H., Li, H., Ugalde, J. and Stoller, Y., 2015. Private Decentralized E-Voting.

[35] Grishchenko, V.S., 2004, September. Redefining Web-of-Trust: reputation, recommendations, responsibility and trust among peers. In Proceedings of the First Workshop on Friend of a Friend, Social Networking and the Semantic Web (FOAF-04).

[36] M. Zhu and Z. Jin, “Trust Analysis of Web Services Based on a Trust Ontology,” Lecture Notes in Computer Science, pp. 642–648.

[37] Gómez, A.F., Martínez, G. and Cánovas, Ó., 2003. New security services based on PKI. Future Generation Computer Systems, 19(2), pp.251-262.

[38] Gregory Maxwell, Andrew Poelstra, 2015-06-02. Borromean ring signatures. [online] Available at: https://pdfs.semanticscholar.org/4160/470c7f6cf05ffc81a98e8fd67fb0c84836ea.pdf

[39] Nicolas van Saberhagen, 2013. CryptoNote v 2.0. [online] Available at: https://cryptonote.org/whitepaper.pdf

[40] Gamage, C., Gras, B., Crispo, B. and Tanenbaum, A.S., 2006, August. An identity-based ring signature scheme with enhanced privacy. In 2006 Securecomm and Workshops (pp. 1-5). IEEE.

[41] Zissis, D. and Lekkas, D., 2011. Securing e-Government and e-Voting with an open cloud computing architecture. Government Information Quarterly, 28(2), pp.239-251.

[42] Vaccaro, J.A., Spring, J. and Chefles, A., 2007. Quantum protocols for anonymous voting and surveying. Physical Review A, 75(1), p.012333.

[43] Hsiao, J.H., Tso, R., Chen, C.M. and Wu, M.E., 2017. Decentralized E-voting systems based on the blockchain technology. In Advances in Computer Science and Ubiquitous Computing (pp. 305-309). Springer, Singapore.

[44] Maus, S., Peters, H. and Storcken, T., 2007. Anonymous voting and minimal manipulability. Journal of Economic Theory, 135(1), pp.533-544.

[45] L. Li, Q. Dong, D. Liu and L. Zhu, "The Application of Fuzzing in Web Software Security Vulnerabilities Test," 2013 International Conference on Information Technology and Applications, Chengdu, 2013, pp. 130-133.

[46] Wood, D.J. and Rayes, A.G., 1981. Reliability of algorithms for pipe network analysis. Journal of the Hydraulics Division, 107(10), pp.1145-1161.

[47] S. Sedaghat, F. Adibniya and M. Sarram, "The investigation of vulnerability test in application software," 2009 International Conference on the Current Trends in Information Technology (CTIT), Dubai, 2009, pp. 1-5.

[48] M. Kumar and R. Mathur, "Unsupervised outlier detection technique for intrusion detection in cloud computing," International Conference for Convergence for Technology-2014, Pune, 2014, pp. 1-4.

[49] O. Cetinkaya, "Analysis of Security Requirements for Cryptographic Voting Protocols (Extended Abstract)," 2008 Third International Conference on Availability, Reliability and Security, Barcelona, 2008, pp. 1451-1456.

[50] Wu Jr, W., 2018. An efficient and effective Decentralized Anonymous Voting System. arXiv preprint arXiv:1804.06674.

[51] W. Zhang et al., "A Privacy-Preserving Voting Protocol on Blockchain," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 401-408.

[52] B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," in IEEE Access, vol. 7, pp. 24477-24488, 2019.

[53] Boontaetae, P., Sangpetch, A. and Sangpetch, O., 2018, November. RDI: Real Digital Identity Based on Decentralized PKI. In 2018 22nd International Computer Science and Engineering Conference (ICSEC) (pp. 1-6). IEEE.