Solomiia Fedushko
Sergiy Gnatyuk
Andriy Peleshchyshyn
Zhengbing Hu
Roman Odarchenko
Igor Korobiichuk
(Eds.)

International Workshop on Conflict Management in Global Information Networks

CMiGIN 2019

Lviv, Ukraine

November 29, 2019

Solomiia Fedushko, Sergiy Gnatyuk, Andriy Peleshchyshyn, Zhengbing Hu, Roman Odarchenko, Igor Korobiichuk (Eds.): International Workshop on Conflict Management in Global Information Networks (CMiGIN 2019), Lviv, Ukraine, 29 November, 2019, CEUR-WS.org, online.

This volume represents the Proceedings of the International Workshop on Conflict Management in Global Information Networks (CMiGIN 2019), held in Lviv, Ukraine, November 29, 2019.

Preface

It is our pleasure to present you the proceedings of International Workshop on Conflict Management in Global Information Networks (CMiGIN 2019), Lviv, Ukraine, 29 November, 2019.

CMiGIN is intended to attract researchers with a strong background in the field of on conflict management in global information networks with the main focus on analytical processing, optimization and control of global information networks. The workshop is soliciting literature review, survey and research papers including, whilst not limited to, the following areas of interest:

- Conflict Management on the Internet
- Analytical Processing of Social Networks
- Optimization of Online Information Networks
- Control of Global Information Networks
- Social Networking Services
- Digital Content Processing

The CMiGIN-2019 joined scientists from Ukraine, Poland, China, Georgia, Germany, Armenia, Kazakhstan, Belarus, North Macedonia, Hashemite Kingdom of Jordan, Pakistan, Kingdom of Saudi Arabia, Yemen, Nigeria, India, Portugal, Republic of Iraq, South Africa together with practical doctors.

The language of CMiGIN-2019 workshop is English. The workshop took the form of oral presentations of peer-reviewed regular papers.

The workshop would not have been possible without the support of many people. First of all, we would like to thank the program and organization staff, the members of the Technical Program Committees and external reviewers for their excellent and tireless work. We sincerely wish that all attendees benefited scientifically from the workshop and wish them every success in their research. It is the humble wish of the workshop organizers that the professional dialogue among the researchers, scientists, engineers and doctors continues beyond the event and that the friendships and collaborations forged will linger and prosper for many years to come.

2019

Solomiia Fedushko
Sergiy Gnatyuk
Andriy Peleshchyshyn
Zhengbing Hu
Roman Odarchenko
Igor Korobiichuk

Program Chairs

Yuriy Syerov	Lviv Polytechnic National University, Ukraine
Sergiy Gnatyuk	National Aviation University, Ukraine
Gevorg Margarov	State Engineering University of Armenia, Armenia
Vladyslav Kovtun	National Aviation University, Ukraine
Thierry Oscar Edoh	University of Bonn, Technical University of Münich, Germany
Oleksandr Kuznetsov	V.N. Karazin Kharkiv National University, Ukraine
Igor Korobiichuk	Warsaw University of Technology, Poland
Anoop Kumar Sahu	Engineering Management University of Johannesburg, South Africa
Ivan Izonin	Lviv Polytechnic National University, Ukraine
Santosh Kumar Behera	Sidho-Kanho-Birsha University, India
Mariya Nazarkevych	Lviv Polytechnic National University, Ukraine
Lídia Oliveira	University of Aveiro, Portugal
Andriy Peleschyshyn	Lviv Polytechnic National University, Ukraine
Solomiia Fedushko	Lviv Polytechnic National University, Ukraine
Irfan Ahmed	Career Point University KOTA, India
Ivanna Dronjuk	Lviv Polytechnic National University, Ukraine
Mykhailo Klymash	Lviv Polytechnic National University, Ukraine
Vishnu Narayan Mishra	Indira Gandhi National Tribal University, India
Zhengbing Hu	Central China Normal University, China
Natalia Shakhovska	Lviv Polytechnic National University, Ukraine
Haruna Chiroma	Abubakar Tafawa Balewa University, Nigeria

Organizing Committee

Organizing Committee Chairs

Sergiy Gnatyuk	National Aviation University, Ukraine
Solomiia Fedushko	Lviv Polytechnic National University, Ukraine

Organizing Committee Members

Roman Odarchenko	National Aviation University, Ukraine
Olha Trach	Lviv Polytechnic National University, Ukraine
Tetyana Okhrimenko	National Aviation University, Ukraine
Olena Kozhokhina	National Aviation University, Ukraine
Taras Ustyianovych	Lviv Polytechnic National University, Ukraine
Maksym Zalisky	National Aviation University, Ukraine
Jamil Al-Azzeh	Al Balqa Applied University, Jordan
Marek Aleksander	State Higher Vocational School in Nowy Sacz , Poland
Yuriy Syerov	Lviv Polytechnic National University, Ukraine
Maksim Iavich	Caucasus University, Georgia
Jugoslav Achkoski	Military Academy, North Macedonia
Nurgul Seilova	Satbayev University, Kazakhstan
Abdu Nagi	University of Science and Technology, Yemen

Anonymous Decentralized E-Voting System

Oleksandr Kurbatov [1[0000-0002-8237-4377]], Pavel Kravchenko [2[0000-0002-0456-3295]], Oleksiy Shapoval [3[0000-0003-4478-3193]], Nikolay Poluyanenko [3[0000-0001-9386-2547]], Mariana Malchyk [4[0000-0002-0917-191X]], Alina Sakun [5[0000-0002-0910-4055]] and Vladyslav Kovtun [6 [0000-0002-1408-5805]]

[1] Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
olkurbatov@gmail.com
[2] Distributed Lab, Kharkiv, Ukraine
pavel@distributedlab.com
[3] V. N. Karazin Kharkiv National University, Kharkiv, Ukraine
alex.shapoval@protonmail.com, nlfsr01@gmail.com
[4] National University of Water and Environmental Engineering, Rivne, Ukraine
m.malchyk@nuwm.edu.ua
[5] Kherson State Agricultural University, Kherson, Ukraine
agorg@ukr.net
[6] National Aviation University, Kyiv, Ukraine
vlad.kovtun@gmail.com

Abstract. This document describes the principles for building an anonymous decentralized e-voting system. It is proposed to use a ring signature mechanism to ensure anonymity of voters and blockchain technology to ensure the integrity and transparency of the transaction history. Thus, it can be beneficial to use such a combination to ensure the maximal robustness of the systems in the real-world conditions with the persistence of a potential malefactor that is interested to disrupt the work of the system, change the data in some way or influence the processes that are happening inside of the system.

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

1 Introduction

Voting is a method for a group, such as a meeting or an electorate, in order to make a collective decision or express an opinion, usually following discussions, debates or election campaigns [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 the current field of research), 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 several flaws, in particular, vulnerabilities associated with the central authority checking all results [11-14].

The described approach 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.

2 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].

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.

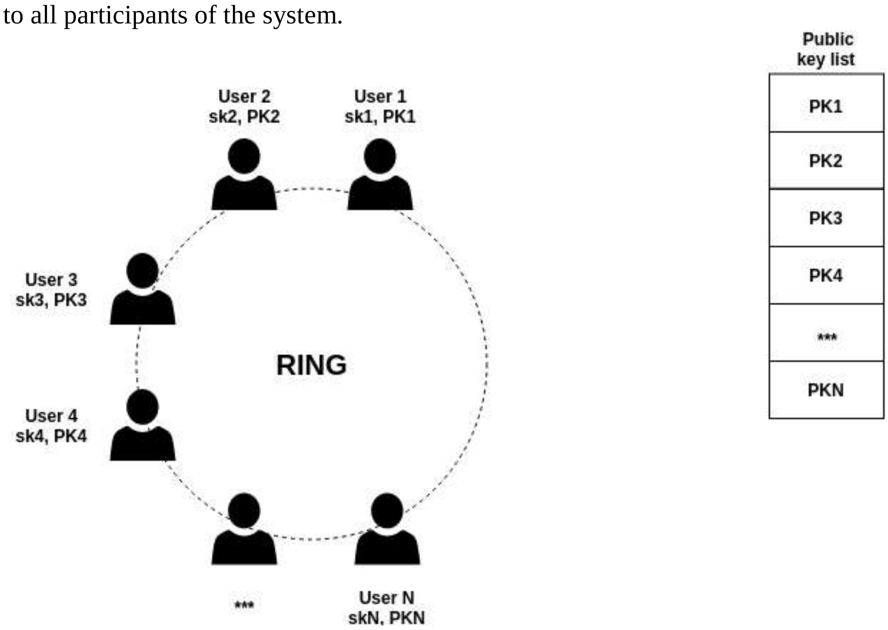

Fig. 1. Ring formation process

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.

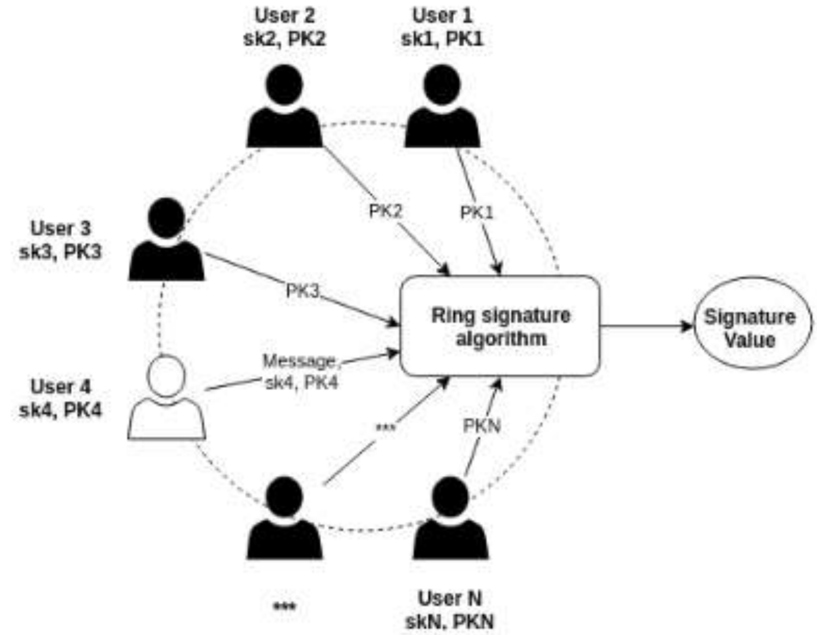

Fig. 2. Signature calculation process

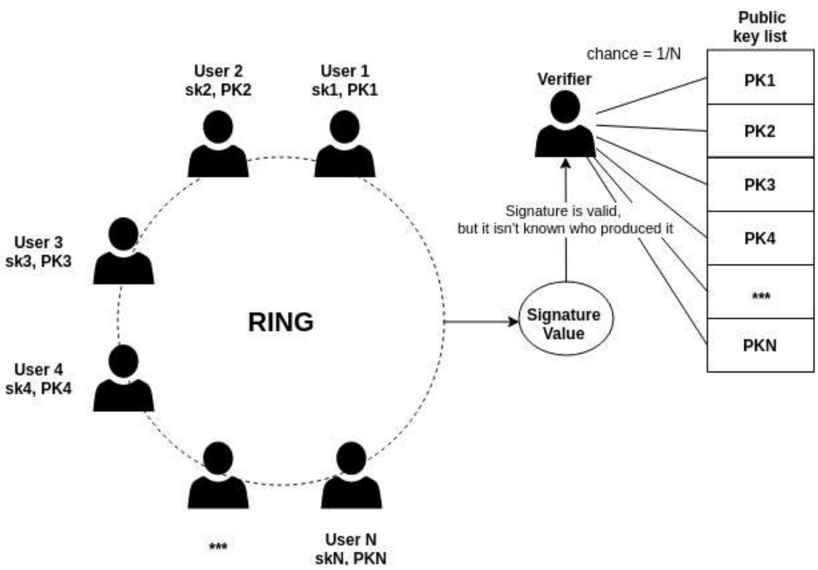

Fig. 3. Ring signature verification process

When the verifier verifies the value of the signature, he can verify that the signature was generated by one of the group members, however it is unknown by whom. Only with a probability of 1 / n can he determine that the signature was calculated by a specific participant in the ring (Figure 3). 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].

3 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.

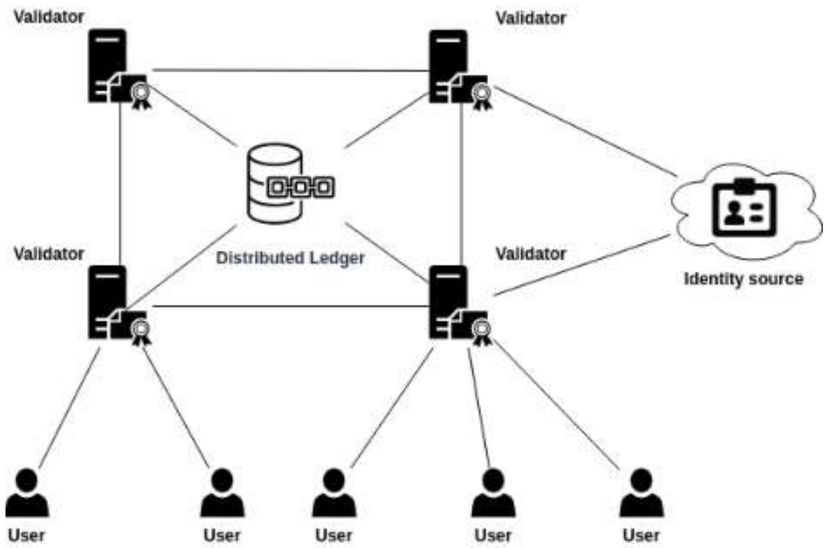

Fig. 4. E-voting system components

In order to vote, the user needs to 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

Transaction ID
Nonce
Candidate ID
Timestamp
Public keys of group
Signature

Fig. 5. Transaction structure

Now let's look at the transaction class that was implemented using the Java programming language and make a quick overview of its methods.

```
public class Transaction {
  private byte[] txID;
  private int nonce;
  private byte[] candidateID;
  private long timestamp;
  private byte[] signature;
}
...
public void printTxID();
private byte[] generateTxID(int nonce, byte[] candi-
dateID, long timestamp, byte[] signature);
public void printTransaction();
private byte[] signTransaction(int nonce, byte[] candi-
dateID, long timestamp);
```

- *printTxID* allows to see the transaction identifier in HEX form to verify it and use in other parts of the real system;
- *generateTxID* implements a SHA-256 algorithm to hash transaction contents. The resulting hash is used as an ID;

- *printTransaction* allows to see the transaction contents in the console and can be modified so these contents can be used in other parts of the real system;
- *signTransaction* implements the ring signature mechanism to sign the contents of transaction.

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].

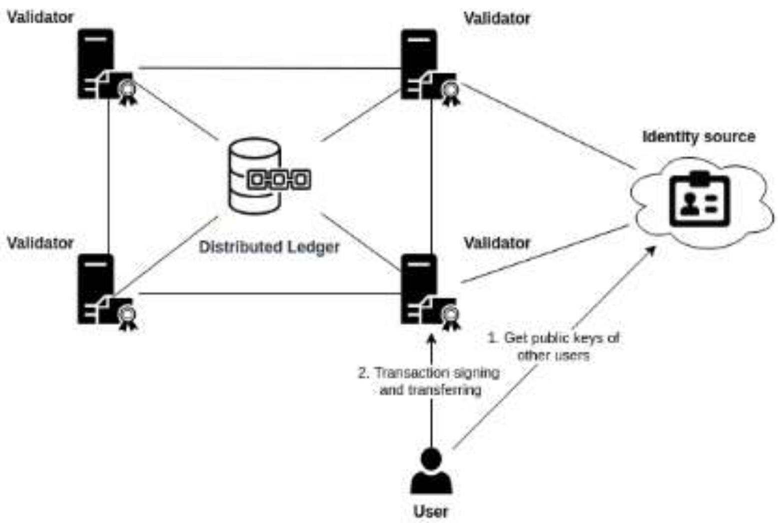

Fig. 6. Transaction formation process

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.

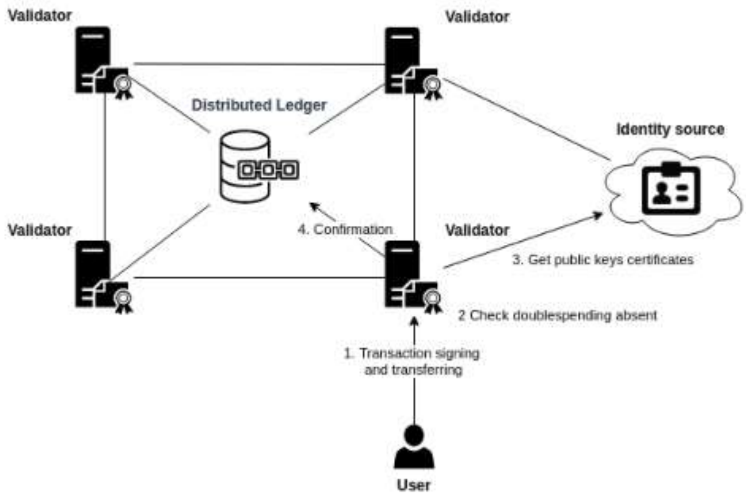

Fig. 7. Transaction verification process

4 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 verify the correctness of his vote;
- 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 (request to the validator or using SPV-approach [42-43]). In addition, each owner of the complete history 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, details with signature mechanism in [39]).

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. Yu.V. Stasev, A.A. Kuznetsov. "Asymmetric code-theoretical schemes constructed with the use of algebraic geometric codes". Kibernetika i Sistemnyi Analiz, No. 3, pp. 47-57, May-June 2005.
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, M. Yesina and V. Ponomar, "Anonymous electronic signature method," 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 47-50.
23. Krasnobayev V. A. Method for realization of transformations in public-key cryptography. Telecommunications and Radio Engineering. - Volume 66, 2007 Issue 17, pp. 1559-1572.
24. A. Kuznetsov, I. Svatovskij, N. Kiyan and A. Pushkar'ov, "Code-based public-key cryptosystems for the post-quantum period," 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 125-130. DOI: 10.1109/INFOCOMMST.2017.8246365

25. W. T. Polk and K. Seamons, “6th annual PKI R&D workshop ‘Applications-Driven PKI’ proceedings,” 2007.
26. A. Kuznetsov, M. Lutsenko, N. Kiian, T. Makushenko and T. Kuznetsova, "Code-based key encapsulation mechanisms for post-quantum standardization," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 276-281.
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. N. Ferguson, B. Schneier, and T. Kohno, “Cryptography Engineering,” Oct. 2015.
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. A. Kuznetsov, A. Pushkar'ov, N. Kiyan and T. Kuznetsova, "Code-based electronic digital signature," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 331-336.
33. D. Wueppelmann, “PGP Auth: Using Public Key Encryption for Authentication on the Web.”
34. Yu.V.Stasev, A.A.Kuznetsov, “Asymmetric Code-Theoretical Schemes Constructed with the Use of Algebraic Geometric Codes.” Cybernetics and Systems Analysis, vol. 41, Issue 3, pp. 354-363, May 2005.
35. K. Portz, J. M. Strong, and L. Sundby, “To Trust Or Not To Trust: The Impact Of WebTrust On The Perceivëed Trustworthiness Of A Web Site,” Review of Business Information Systems (RBIS), vol. 5, no. 3, p. 35, Jul. 2011.
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. K. Isirova and O. Potii, "Decentralized public key infrastructure development principles," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kiev, 2018, pp. 305-310.
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. Maus, S., Peters, H. and Storcken, T., 2007. Anonymous voting and minimal manipulability. Journal of Economic Theory, 135(1), pp.533-544.

44. 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.
45. A.A. Kuznetsov, Smirnov, A.A., D.A. Danilenko, A. Berezovsky. "The statistical analysis of a network traffic for the intrusion detection and prevention systems." Telecommunications and Radio Engineering, Volume 74, 2015 Issue 1, pp. 61-78.
46. 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.
47. Alexandr Kuznetsov, Oleksiy Shapoval, Kyrylo Chernov, Yehor Yeromin, Mariia Popova, Olga Syniavska. Automated software vulnerability testing using in-depth training methods. In Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019), Zaporizhzhia, Ukraine, April 15-19, 2019., pp. 227–240. 2019.
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. H. Orman, "Blockchain: the Emperors New PKI?," in IEEE Internet Computing, vol. 22, no. 2, pp. 23-28, Mar./Apr. 2018.
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. S. Nakamoto, "Bitcoin:A peer-to-peer electronic cash system.", 2008.