Yet Another E-Voting Scheme Implemented Using Hyperledger Fabric Blockchain

Sergey Kyazhin(✉) and Vladimir Popov

Blockchain Laboratory, Sberbank, Moscow, Russia
blockchain-research@sberbank.ru

Abstract. There are many papers whose authors propose various approaches to the construction of electronic voting (e-voting) systems that are resistant to various types of attacks. The two main properties of such systems are anonymity and verifiability. To provide anonymity, a blind signature or a ring signature is often used. To provide verifiability, distributed ledger technologies, in particular blockchain, have recently been used. One of these systems has been presented at ICCSA 2019. This system is implemented using Hyperledger Fabric blockchain platform and uses a blind signature to provide anonymity. One of the disadvantages of this system is that a compromised signer (an organizer generating a blind signature) could independently create valid ballots without detection. In this paper, we modify this system by replacing a blind signature with a linkable ring signature in order to eliminate this disadvantage. As a result, we combine linkable ring signature, Idemix and blockchain technologies to construct a decentralized anonymous e-voting system that does not rely on a trusted signer and can achieve the following properties: eligibility, unreusability, anonymity, and verifiability. In addition, the use of both a linkable ring signature and Idemix allows us to construct a two-stage anonymization, that increases the versatility of the proposed system. This allows us to use a blockchain platform (for example, Hyperledger Fabric) to implement the e-voting system, without making changes to platform standard signature scheme.

Keywords: E-voting · Blockchain · Ring signature · Idemix · Distributed ledger technologies

1 Introduction

The traditional voting procedure, depending on specific circumstances, may have various disadvantages. The main ones are the following:

- non-verifiability the correctness of the result counting;
- voting by the organizer instead of the voter;
- double voting (if the organizer and the voter are in collusion).

© Springer Nature Switzerland AG 2020
O. Gervasi et al. (Eds.): ICCSA 2020, LNCS 12251, pp. 37–47, 2020.
https://doi.org/10.1007/978-3-030-58808-3_4

Therefore, electronic voting (e-voting) is continuously developing. It empowers voters to cast their ballots remotely (through a local or global network), but has some problems. For example, attempts to make voting anonymous often reduce the ability to verify the correctness of the result counting. Therefore, the voting procedure requires public trusted ballot box. To solve this problem, in recent papers, e-voting systems use a distributed ledger technologies to create a public ballot box.

In this paper, we modify one of the existing e-voting systems that uses blockchain technology.

1.1 Security Properties

In various papers, the security requirements that an e-voting system must satisfy are formulated differently. We use the following five properties used in [1].

Eligibility. This property requires that only eligible voters are allowed to vote. In addition, only valid ballots should be counted.

Unreusability or Double Voting Prevention. This property means that voters are allowed to vote only once.

Untraceability or Anonymity. This property requires that no one can reveal the owner of the ballot. In other words, voters are allowed to vote anonymously.

Verifiability. This property means that each voter can verify whether his ballot has been counted correctly.

Receipt-Freeness. This property prevents the voter from proving to others that he has voted for a particular candidate (for example, to sell his vote).

1.2 Related Work

Common cryptographic techniques used to achieve anonymity in e-voting systems are blind signature [2] and linkable ring signature [3].

A blind signature is commonly used in the voter registration phase. Specifically, a legitimate voter receives a blind signature on a random value. The signature value and the random value are then used to prove the authenticity of the voter. This method was first used in the secret e-voting system [4]. However, the use of blind signature requires the signer to be trusted. If the signer is compromised, the attacker will be able to vote as many times as he wants [5].

A linkable ring signature is commonly used as a replacement for a standard signature to provide the authenticity of ballots. With it, you can prevent unauthorized voting while maintain the privacy of legitimate voters. The first e-voting

system using a linkable ring signature was proposed in the paper with the first linkable ring signature scheme [3].

In [1], a blind signature is used to construct an e-voting system. User registration includes the step of obtaining a blind signature for a new voting key. Indeed, the system has all the declared security properties. However, there is also a drawback: a compromised organizer can independently create valid ballots.

If the smart contract generates a blind signature, then the secret key for blind signature is available to all peer owners. If the organizer generates a blind signature, then the secret key for blind signature is available to him.

Thus, anyone who has access to a secret key for blind signature can generate and sign as many new voting keys as he wants. Then, having received an anonymous Idemix-certificate (for example, using one of the valid users), he will be able to use each of these keys for voting, since the signatures are valid.

Therefore, we decided to modify the system proposed in [1]. In our construction, we use a linkable ring signature. The described attack is impossible for it. Since neither the organizer nor the smart contract generates any signatures for registration, neither the organizer nor the peer owners will be able to generate additional ballots.

Therefore, when we use a linkable ring signature, we may not require a trusted signer. However, the disadvantage of this approach is that the procedures for generating and verifying the signature have a computation complexity linear to the size of the anonymity set (i. e. the number of legitimate voters).

There are many papers devoted to methods and systems for e-voting, including those that use blockchain technologies and linkable ring signatures, for example, [6–8]. However, we, like [1], also use Idemix technology to anonymize the participants.

1.3 Our Contributions

In this paper, we propose an e-voting system that uses linkable ring signature, Idemix and blockchain technologies. The proposed system is a modification of the system described in [1]. Namely, a blind signature was replaced by a linked ring signature. This modification allows us to improve the scheme, since it eliminates the disadvantage associated with the ability to create valid votes by the compromised organizer.

Thus, we propose a decentralized anonymous e-voting system, which does not rely on a trusted signer, and can achieve the following properties: eligibility, unreusability, anonymity, and verifiability.

Note that the e-voting system described in [3] uses only a linkable ring signature instead of the standard one to provide the anonymity. However, we use both a linkable ring signature and Idemix, because it allows us to construct a two-stage anonymization, that increases the versatility of the proposed system. To implement e-voting system, a blockchain platform (for example, Hyperledger Fabric [9]) can be used without changing the platform standard signature scheme.

1.4 Outline

In the next section, we describe the following used technologies: a linkable ring signature, Idemix, and Hyperledger Fabric blockchain. We propose the e-voting system in Sect. 3. In Sects. 4 and Sect. 5, we provide remarks on the system security and performance properties. We conclude the paper in Sect. 6.

2 Used Technologies

To construct our e-voting system, we use blockchain, Idemix and linkable ring signature technologies.

2.1 Blockchain

Depending on the user access control, all blockchain systems can be divided into two groups: permissionless and permissioned blockchain systems. The presented implementation involves the use of a permissioned system. That is, all voting entities, and their rights are known in advance. Specifically, we use Hyperledger Fabric permissioned blockchain platform.

In the proposed implementation, the blockchain system is used:

- to provide the impossibility of censorship;
- to verify the results by both voters and inspectors.

2.2 Idemix

Suppose there are three parties: the user, the certification authority (can identify the user), and the verifier (wants to verify some user attributes). Idemix technology (details are described in [10–13] and other papers) solves the problem of proving that the user has certain attributes without revealing other information about the user and making it impossible to link two different requests of the same user. The proposed implementation uses the user's entry into the list of system users as an attribute.

2.3 Linkable Ring Signature

Let there be a group of n participants and some message m that needs to be signed. The linkable ring signature scheme consists of the following four algorithms:

- $KGen(1^\lambda)$ is a key generation algorithm that uses a security parameter λ as an input and returns to the i-th participant a secret key sk_i and a public key pk_i, $i = 1, \ldots, n$;
- $Sign(m, pk_1, \ldots, pk_n, i, sk_i)$ is a signature generation algorithm that uses a message m, public keys $pk_1, \ldots, pk_n$ of all group members, a number i of the signer, and his secret key sk_i as inputs, and returns the signature σ;

- $Verify(m, pk_1, \ldots, pk_n, \sigma)$ is a signature verification algorithm that uses a message m, the public keys $pk_1, \ldots, pk_n$ of all group members and the signature σ as inputs, and returns 1 if the signature is valid, 0 otherwise;
- $Link(\sigma_1, \sigma_2)$ is a linking algorithm that uses signatures σ_1, σ_2 as inputs, and returns 1 if these signatures are generated using the same key, 0 otherwise.

Therefore:

- the verifier (the one who runs the algorithm $Verify$) can find out that the signer is a group member, but cannot find out who exactly;
- the linker (the one who runs the algorithm $Link$) can find out that the same signer calculated two signatures on the same or different messages, but cannot find out who exactly.

In the proposed system, a linkable ring signature is used to provide:

- the anonymity of voters (if the user casts a signed ballot, it is known that he is a legitimate voter, but his identity is unknown);
- the impossibility of double voting (if the voter casts the second signed ballot, it is known that he is a double voter, but his identity is unknown).

2.4 Encryption and Secret Sharing

In [1], the voters can send encrypted ballots (a public key cryptosystem is used). After the voting, the decryption key is published, and anyone can decrypt the ballots and verify the results. Secret sharing schemes can be used to prevent intermediate result counting.

For the scheme proposed in this paper we also can use of a public key encryption and secret sharing schemes. However, for simplicity of presentation, we will not describe the corresponding steps, since they are optional.

3 Construction

The described system is a protocol for the interaction of several components.

3.1 System Components

To make it easier to compare our scheme with [1], we do not make changes to the network architecture (see Fig. 1 in [1]). The four types of components involved in the e-voting system is described as follows.

User Applications. The system includes user software applications according to user roles. They are needed for users to interact with the blockchain network. For example:

- the organizer application allows us to initiate a voting;
- the voter application allows us to register, vote and verify the voting results.

Certification Authority. The system includes a certification authority that can operate in two modes: a standard mode (working with user public key certificates) and Idemix mode (working with anonymous Idemix certificates).

Peers. The system includes one or more nodes of the blockchain network (in our implementation, nodes are based on Hyperledger Fabric). This component performs the functions of storing and writing information in the ledger, as well as executing the logic of voting smart contracts (chaincode in Hyperledger Fabric terminology).

Ordering Service. The system includes an ordering service. This component is required to ordering changes in the ledger.

3.2 Entities

The e-voting system contains the following three types of entities, namely, Organizer, Voter and Inspector (optional).

Organizer. This entity makes a list of voting questions and a list of voters, sets the time frames for the registration and voting phases (the entity has nodes of the blockchain network and an organizer application).

Voter. This entity is a voting participant (the entity may have nodes of the blockchain network and has a voter application).

Inspector. This optional entity observes the correct operation of the system (the entity may have nodes of the blockchain network and has an inspector application).

3.3 E-Voting Protocol

In this subsection, we describe the process of e-voting protocol illustrated in Fig. 1. The protocol consists of the following five phases: blockchain network configuration, voting configuration, registration, voting, and result counting.

Blockchain Network Configuration. The administrator creates users in the system, determines their rights in accordance with the roles, configures a certification authority, uploads smart contracts, determines nodes and ordering service.

The certification authority creates key pairs and issues public key certificates for users (1, 2 in Fig. 1). In the paper, it is assumed that:

- each user interaction with the blockchain network involves authentication using the public key certificate;
- writing information to the ledger involves generating requests to change the ledger, its processing on the peers and ordering on the ordering service, and then writing the corresponding information to the ledger.

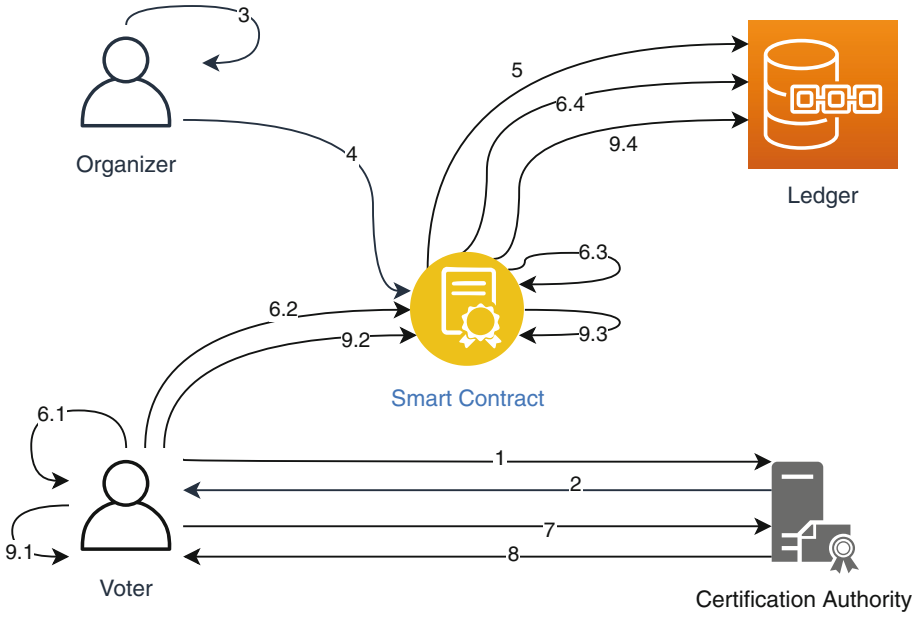

Fig. 1. Overview of our blockchain-based e-voting protocol

Voting Configuration. The organizer:

- creates a voting session, i. e. determines its parameters, including a voting ID, a list of voting questions, a list of voter public keys, a time frames for registration and voting phases (3 in Fig. 1);
- sends this data to the peers that write it in the ledger (4, 5 in Fig. 1).

Registration. Each voter (j is the voter number):

- generates a new voting key pair (public key VP_j and secret key VS_j), where for the linkable ring signature scheme without interaction with a certification authority and despite the existing key pair (6.1 in Fig. 1);
- sends the public key VP_j and the voting ID to the peers, using the public key certificate for authentication (6.2 in Fig. 1).

The smart contract verifies that the current user can participate in this voting by verifying the availability of the corresponding public key in the voting parameters (6.3 in Fig. 1). Then the peers write the key VP_j in the ledger according to the participant's public key certificate (6.4 in Fig. 1).

Voting. Each voter who has registered their voting key:

- receives an anonymous Idemix certificate, interacting with the certification authority, that operates in Idemix mode (7, 8 in Fig. 1);

– downloads the public keys for voting of all voters;
– generates his answers to the questions, calculates the value of the linkable ring signature on these answers, using his private key VS_j and the set of the downloaded public keys for voting (9.1 in Fig. 1);
– sends the voting answers and the linkable ring signature to the peers, using the anonymous Idemix certificate instead of the standard certificate for authentication (9.2 in Fig. 1).

The smart contract:

– verifies that the linkable ring signature is correct by running the algorithm $Verify$ with the voting answers, the public keys for voting of all voters, and the linkable ring signature as inputs (9.3 in Fig. 1);
– verifies that the voter voted earlier (runs the algorithm $Link$ with this signature and each of previously written in the ledger as inputs).

If the signature is valid, the peers write (rewrite if the voter voted earlier) its value and the voter's answers in the ledger (9.4 in Fig. 1).

Before the end of the voting procedure, the voter may revote, having received a new anonymous Idemix certificate and sending new answers. His answers will be rewritten in the ledger because the same voting secret key will be used to calculate the linkable ring signature.

Result Counting. If encryption is not used, the results are counted simultaneously with the voting. The results can be updated after each vote.

4 Remarks on Security Properties

Like the scheme [1], the e-voting system presented in this paper can achieve four of the five properties listed in the introduction, namely, eligibility, unreusability, anonymity, and verifiability.

The **receipt-freeness** property is not fulfilled in this system, because the voter can prove that he has generated a certain linkable ring signature (due to the linkability), thereby proving his answers.

4.1 Eligibility

This property is provided:

– at the registration phase by the security of the authentication procedure in Hyperledger Fabric (an attacker cannot pass the authentication procedure, therefore, cannot add his voting key on the registration phase);
– at the voting phase by the security of the linkable ring signature (an attacker cannot fake the linkable ring signature, therefore, cannot fake the ballot).

4.2 Unreusability

This property is provided:

- at the registration phase by the security of the authentication procedure in Hyperledger Fabric (an attacker cannot register two different voting keys, because the user identity (certificate) is used for authentication);
- at the voting phase by the linkability of the linkable ring signature (an attacker cannot vote twice with the same voting key, because a smart contract can find out that two linkable ring signatures calculated using the same key correspond to the same voter, even if he used different anonymous Idemix certificates).

4.3 Anonymity

This property is provided by the anonymity of the linkable ring signature and the security of Idemix (the identity of the voters cannot be disclosed).

4.4 Verifiability

All votes are written in the ledger according to the linkable ring signatures. Each user can verify whether his ballot has been counted correctly.

5 Remarks on Performance Properties

In this paper, we describe only the e-voting scheme. We don't present the results of experiments evaluating its performance and corresponding comparison with other solutions.

We can give a remark on **scalability**. Compared to the scheme [1], our scheme scales worse because it uses a linkable ring signature. The procedures for its generation and verification have a computational complexity linear to the number of voters.

6 Conclusion and Future Work

In this paper, we modify e-voting scheme [1]. Namely, we replace a blind signature with a linkable ring signature in order to eliminate the disadvantage associated with the ability to cast votes by the compromised organizer.

Thus, we combine linkable ring signature, Idemix and blockchain technologies to construct a decentralized anonymous e-voting system, which does not rely on a trusted signer, and can achieve the following properties: eligibility, unreusability, anonymity, and verifiability.

The use of both a linkable ring signature and Idemix allows us to construct a two-stage anonymization, that increases the versatility of the proposed system. This allows us to use a blockchain platform (for example, Hyperledger Fabric) to implement the e-voting system, without making changes to platform standard signature scheme.

In future work, we would like:

- to carry out experiments for evaluation the performance of our scheme;
- to continue the modification of this scheme to achieve the receipt-freeness.

References

1. Kirillov, D., Korkhov, V., Petrunin, V., Makarov, M., Khamitov, I.M., Dostov, V.: Implementation of an E-voting scheme using hyperledger fabric permissioned blockchain. In: Misra, S., et al. (eds.) ICCSA 2019. LNCS, vol. 11620, pp. 509–521. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-24296-1_40
2. Chaum, D.: Blind signatures for untraceable payments. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) Advances in Cryptology, pp. 199–203. Springer, Boston (1983). https://doi.org/10.1007/978-1-4757-0602-4_18
3. Liu, J.K., Wei, V.K., Wong, D.S.: Linkable Spontaneous anonymous group signature for ad hoc groups. In: Wang, H., Pieprzyk, J., Varadharajan, V. (eds.) ACISP 2004. LNCS, vol. 3108, pp. 325–335. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-27800-9_28
4. Fujioka, A., Okamoto, T., Ohta, K.: A practical secret voting scheme for large scale elections. In: Seberry, J., Zheng, Y. (eds.) AUSCRYPT 1992. LNCS, vol. 718, pp. 244–251. Springer, Heidelberg (1993). https://doi.org/10.1007/3-540-57220-1_66
5. Gong, B., Lu, X., Fat, L.W., Au, M.H.: Blockchain-based threshold electronic voting system. In: Meng, W., Furnell, S. (eds.) SocialSec 2019. LNCS, vol. 1095, pp. 238–250. Springer, Singapore (2019). https://doi.org/10.1007/978-981-15-0758-8_18
6. Lyu, J., Jiang, Z.L., Wang, X., Nong, Z., Au, M.H., Fang, J.: A secure decentralized trustless e-voting system based on smart contract. In: 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 13th IEEE International Conference on Big Data Science and Engineering (TrustCom/ BigDataSE), pp. 570–577. Rotorua, New Zealand (2019). https://doi.org/10.1109/TrustCom/BigDataSE.2019.00082
7. Yu, B., et al.: Platform-independent secure blockchain-based voting system. In: Chen, L., Manulis, M., Schneider, S. (eds.) ISC 2018. LNCS, vol. 11060, pp. 369–386. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-99136-8_20
8. Hjlmarsson, F., Hreiarsson, G.K., Hamdaqa, M., Hjlmtsson, G.: Blockchain-based E-voting system. In: 11th International Conference on Cloud Computing (CLOUD), pp. 983–986. San Francisco, CA (2018). https://doi.org/10.1109/CLOUD.2018.00151
9. Androulaki, E. et al.: Hyperledger fabric: A distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference (EuroSys18), pp. 1–15. ACM, New York (2018). https://doi.org/10.1145/3190508.3190538
10. Camenisch, J., Van Herreweghen, E.: Design and implementation of the idemix anonymous credential system. In: Proceedings of the 9th ACM conference on Computer and communications security (CCS02), pp. 21–30. ACM, New York (2002). https://doi.org/10.1145/586110.586114
11. Camenisch, J., Lysyanskaya, A.: Signature schemes and anonymous credentials from bilinear maps. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 56–72. Springer, Berlin, Heidelberg (2004). https://doi.org/10.1007/978-3-540-28628-8_4

12. Camenisch, J., Drijvers, M., Lehmann, A.: Anonymous attestation using the strong diffie hellman assumption revisited. In: Franz, M., Papadimitratos, P. (eds.) Trust 2016. LNCS, vol. 9824, pp. 1–20. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-45572-3_1
13. Camenisch, J., Drijvers, M., Dubovitskaya, M.: Practical UC-secure delegatable credentials with attributes and their application to blockchain. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS17), pp. 683–699. ACM, New York (2017). https://doi.org/10.1145/3133956.3134025