Anonymous Remote Voting System

Irina Dyachkova
Department of Applied Mathematics and Cybernetics,
Siberian State University of Telecommunications and Information Sciences
Novosibirsk, Russia
dyach199@gmail.com

Anton Rakitskiy
Nonlinear Photonics Laboratory, Novosibirsk State Uiversity
Laboratory of digital twins and big data analysis
Institute of Computationa Technologies SB RAS
Department of Applied Mathematics and Cybernetics,
Siberian State University of Telecommunications and Information Sciences
Novosibirsk, Russia
rakitsky.anton@gmai.com

In this paper we describe the cryptographic protocol of anonymous remote voting, which reliability is provided by proof and justification of its properties. This protocol was used in the real anonymous voting system developed in Institute of Computational Technologies SB RAS. In addition to the system operation protocol we describe algorithm of creating an anonymous data transfer channel and also show the possibility of applying blockchain technology to this system. The results of this work demonstrate the advantage of such systems over standard voting methods which are highly dependent on human factor.

Keywords: anonymous voting, information system, cryptography, data protection, anonymous channel, databases.

I. INTRODUCTION

Classical voting assumes the personal presence of all participants for guaranteed confirmation of identity. Each person receives an individual voting ballot and makes, as it seems, an independent choice which cannot be revealed by others. However, this method is largely dependent on human factor. For example, the counting commission or the people who printed voting ballots may affect on the voting results and may help to determine how a particular participant voted.

In this case, digital voting can help to solve such problem. If it is conducted in accordance with cryptographic protocols which have proven properties and reliability. The organization of remote voting on the network is very popular now. There are existing applications which solve this problem but in most cases they only implement the open voting protocol [1]. If we consider the question of holding a secret ballot then there is a number of scientific problems: on the one hand, the voting ballot should remain secret; on the other hand, everyone should be able to verify that his vote was correctly taken into account. This problem can be solved using cryptographic methods. One of these methods is the anonymous voting protocol. It is used to create a system, which meets all the security requirements established to ensure anonymity of choice.

Anonymity and proven security are based on two cryptographic protocols: the protocol for the "blind" signing of voting ballot and the protocol for organizing an anonymous data transfer channel. Also we to introduce how to apply the blockchain technology to improve database security.

II. DESCRIPTION OF THE «BLIND» SIGNATURE ALGORITHM

This algorithm was invented by David Chaum in 1982 [2] and it was first implemented by him on the basis of the RSA algorithm [3]. The main feature of this digital signature is that the signatory cannot know the contents of the document being signed, it only checks this document for compliance with certain conditions (parameters), and, if the conditions are met, signs it. The security of a blind signature scheme is based on the difficulty of factorizing large composite numbers, this scheme is used in many cryptographic protocols. The application of this signature algorithm in the electronic money system was considered in work [4], but here we consider its application in the anonymous voting protocol.

The blind signature algorithm works on the basis of the RSA protocol, however, the RSA can be replaced with any other public and private key digital signature algorithm, for example, El Gamal's scheme [5] or any of the DSA family [6]. In addition, the signing protocol can be easily changed without violating the essence of the algorithm. This algorithm allows to generate and sign a voting ballot without revealing to server information about how a particular participant voted. We describe this algorithm:

1. When creating a vote on the server, 3 secret parameters (P, Q and c) and 2 open parameters must be generated:

$$N = PQ \tag{1}$$

$$d = c^{-1} \bmod \phi(N), \tag{2}$$

where P, Q are prime numbers ($P, Q \leq 2^{512}$), N is the module by which all operations will be performed, $\phi(N) = (P-1)(Q-1)$ is the Euler function for the number N, c and d are the private and public keys ($c, d < N, cd \bmod \phi(N) = 1$).

2. Let us assume that the user has already made a choice and wants to send a vote. The server passes parameters N and d to user, then user proceeds to create data for signature. It generates a random number R of size 512 bits, and performs concatenation with the number n, which is the encoded decision of the user (this number should not exceed 512 bits, except for the solution itself, service information about the vote is included there). As a result, it gets:

$$\bar{R} = R|n \tag{3}$$

3. Random number X is generated in the range $[2, N-1]$ and data for signature is formed as follows:

$$h = H(\bar{R}) \quad (4)$$

$$\bar{h} = X^d \cdot h \bmod N, \quad (5)$$

where h is the value of the hash function (the developed system uses SHA3-512 hash algorithm)

4. The value of $\bar{h}$ is sent to the server and we start electronic signature process:

$$\bar{s} = \bar{h}^c \bmod N \quad (6)$$

5. The signed ballot is sent back to the user, and he receives the signed value of the original hash function:

$$s = X^{-1} \cdot \bar{s} = h^c \bmod N \quad (7)$$

Actually:

$$s = X^{-1} \cdot \bar{s} = X^{-1} \cdot \bar{h}^c = X^{-1} \cdot (X^d \cdot h)^c = X^{-1} \cdot X^{c \cdot d} \cdot h^c = X^{-1} \cdot X^1 \cdot h^c = h^c \bmod N \quad (8)$$

6. In the last step user sends a signed ballot, a message of the form $\langle \bar{R}, s \rangle$, through the anonymous data channel, and the server authenticates:

$$H(\bar{R}) = s^d \bmod N \quad (9)$$

If the values match, the vote is considered valid and is taken into account by the voting system, and the ballot is added in database.

III. Anonymous Data Channel

Before The organization of anonymous data transmission channel is an important problem and there are a large number of different approaches to solve it, in particular:

- Decentralized anonymous networks
- Hybrid anonymous networks
- TOR
- VPN

Decentralized anonymous networks are computer networks which work on the top of global network and ensure anonymity. Moreover, in a decentralized network, any machine can connect to another and send it a request for resources. In such a network, each computer can operate as a server: receive, process and send requests or do some administrative functions. Also, the connection in this type of anonymous networks is unstable, any participant can break it at any time.

Hybrid anonymous networks contain servers used to coordinate work, search or provide information about existing network machines and their status. Hybrid networks combine the speed of centralized networks and the reliability of decentralized networks, since they use schemes with independent indexing servers which synchronize data with each other. In this case, the network continues to function even if one or more servers fail.

Within the framework of the system was proposed a protocol to ensure the identification of the original sender of the voting ballot is not possible with 100% probability.

Consider a voting system as a fully connected graph of N + 1 vertexes, where the first N vertexes are participants in the vote, and the vertex N + 1 is the receiving server. Figure 1 shows a diagram of such a system. In this case, consider the option where the user at vertex 1 wants to send voting ballots to the server. We describe the protocol:

- The ballot owner with probability p sends it to the server and with probability 1 - p the ballot is sent to a randomly selected participant.
- When the ballot is received from another user, the current one performs a similar algorithm. With probability p, the ballot is sent to the server or, with probability 1 - p, to randomly selected voting participant.
- At any time, none of the voters or the server can unambiguously determine whether the received ballot belongs to the previous sender, or the one just forwarded it.

This scheme with a correctly selected p value makes it possible with a high probability to guarantee delivery of the bulletin to the server. For example, if a value of p = 0.6, the probability that the message will be delivered to the server after exactly three transfers will be $0{,}6 + 0{,}4 \times 0{,}6 + 0{,}6 \times 0{,}4^2 = 0{,}6 + 0{,}24 + 0{,}096 = 0{,}936$. In addition, with such a value of p, the server cannot claim that the probability of belonging the ballot to the previous sender is more than p. Moreover, to guarantee that the ballot belongs to a specific person, collusion of all process participants, except the sender, and the server is necessary.

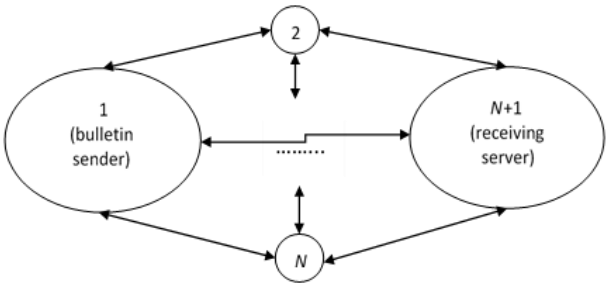

Figure 1. The scheme of nodes of the voting system.

IV. Blockchain Technology

In recent years, the Blockchain method of storing and protecting information [7][8], based on cryptographic methods, has become increasingly popular. This technology can be applied to an anonymous remote voting system: user's voices will be recorded as transactions in blocks that will be linked cryptographically and chronologically into a chain using hash functions. As soon as the registry is updated and a new block is formed, it can't be changed. You can only add new entries to it, while the registry is updated on all computers on the network at the same time.

The newsletter database is open, so the server must be honest. Otherwise, if the server creates an arbitrary number of ballots with the required votes, users can find their own vote at any time and check its correctness, as well as find out the total number of voters. If this number does not match the number of ballots in the database, then the server is not fair and the voting results are canceled.

In this case, it will not be possible to remove voices from the block or fake them, which provides even more security for the system.

CONCLUSION

In this work we show that it is possible to create anonymous digital voting system which can guarantee the security of the transmitted data and the inability to fake it. Obviously, there are many features in the organization of work of such systems, but here we described the main components of the voting protocol that need to be given special attention. Presented protocol is good alternative for tradition voting methods and it has higher reasonable security.

In order to demonstrate in practice the convenience and reliability of systems using the proposed protocol we developed such system for the internal voting in Institute of Computational Technologies SB RAS. This system of remote anonymous voting is available at link [9], it complies with all security requirements for such systems.

BIBLIOGRAPHY

[1] Parhami B. // IEEE Transactions on Reliability — Vol. 43, Iss. 4, Dec 1994 — P. 617–629. — ISSN 0018-9529; 1558-1721 — doi: 10.1109/24.370218

[2] Chaum, D. Blind Signatures for Untraceable Payments. In: Chaum, D., Rivest R.L. and Sherman, A.T., Eds., Advances in Cryptology Proceedings of Crypto 82, Plenum (Springer-Verlag), New York, P. 199-203.

[3] Rivest R., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems // Commun. ACM — New York City: ACM, 1978. — Vol. 21, Iss. 2. — P. 120–126. — ISSN 0001-0782; 1557-7317 — doi:10.1145/359340.359342

[4] Ryabko B. Cryptography and steganography in information technology / B. Ryabko, A. Fionov, Yu. Shokin. - Novosibirsk: Nauka, 2015. – 240 p.

[5] Elgamal T. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Trans. Inf. Theory / F. Kschischang — IEEE, 1985. — Vol. 31, Iss. 4. — P. 469–472. — ISSN 0018-9448 — doi:10.1109/TIT.1985.1057074

[6] "FIPS PUB 186: Digital Signature Standard (DSS), 1994-05-19". qcsrc.nist.gov.

[7] Zyskind G., Nathan O., Pentland A. Decentralizing Privacy: Using Blockchain to Protect Personal Data, Security and Privacy Workshops (SPW), IEEE Symposium, 2015.

[8] Pilkington M. 11 Blockchain technology: principles and applications. Research handbook on digital transformations, P. 225 (2016).

[9] Official site of remote anonymous voting, ICT SB RAS [Electronic resource] – Access mode: http://rvs.ict.nsc.ru/