Вычислительные технологии, 2024, том 29, № 1, с. 59–73. © ФИЦ ИВТ, 2024 ISSN 1560-7534
Computational Technologies, 2024, vol. 29, no. 1, pp. 59–73. © FRC ICT, 2024 eISSN 2313-691X

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

DOI:10.25743/ICT.2024.29.1.006

Система электронного анонимного голосования на основе “слепой” цифровой подписи

И. С. Дьячкова[1,*], А. А. Ракитский[1,2,3]

[1]Сибирский государственный университет телекоммуникаций и информатики, 630102, Новосибирск, Россия

[2]Федеральный исследовательский центр информационных и вычислительных технологий, 630090, Новосибирск, Россия

[3]Новосибирский государственный университет, 630090, Новосибирск, Россия

[*]Контактный автор: Дьячкова Ирина Сергеевна, e-mail: dyach199@gmail.com

Поступила 28 сентября 2022 г., доработана 20 января 2023 г., принята в печать 06 марта 2023 г.

Представлена схема создания системы анонимного дистанционного голосования, в основе которой лежит алгоритм слепой электронной подписи — один из эффективных способов сформировать и подписать бюллетень для голосования. Описан метод построения канала связи для анонимной передачи бюллетеней на сервер и доказана надежность такого метода, а также указан рекомендуемый способ безопасного хранения бюллетеней голосования в виде блокчейн-транзакций. В ходе исследования были изучены возможные угрозы безопасности системы и представлены способы их предотвращения. Таким образом проанализирована надежность представленной системы и продемонстрировано, что система анонимного удаленного голосования не подвержена этим уязвимостям.

Ключевые слова: анонимное голосование, криптография, анонимная передача данных, технология блокчейн, анализ угроз.

Цитирование: Дьячкова И.С., Ракитский А.А. Система электронного анонимного голосования на основе “слепой” цифровой подписи. Вычислительные технологии. 2024; 29(1):59–73. DOI:10.25743/ICT.2024.29.1.006.

Введение

Существует множество различных способов голосования: от классического (бумажного) до электронного, использующего публичные сети. У классического два существенных недостатка: необходимость личного присутствия всех участников и человеческий фактор. При таком способе голосования каждый участник получает индивидуальный бюллетень для голосования и делает самостоятельный выбор. Однако этот метод во многом зависит от человеческого фактора: например, счетная комиссия или люди, печатающие бюллетени для голосования, могут прямо или косвенно повлиять на результаты голосования, а также определить, как проголосовал конкретный участник. Вышеописанные недостатки исключаются при использовании надежного дистанционного голосования, основанного на публичных сетях и гарантирующего анонимность участников.

Актуальной задачей является создание надежной схемы дистанционного электронного голосования. В 2021–2022 гг. в России проводились экспериментальные выборы

с использованием системы ДЭГ (дистанционного электронного голосования) [1], разрабатываемого компанией Ростелеком. Подписание бюллетеней в этой системе основано на протоколе “слепой” подписи. В ДЭГ анонимность выбора голосующих заключается в том, что каждый электронный бюллетень в отдельности не расшифровывается: за счет гомоморфного шифрования операции ведутся над зашифрованными данными, присылаемыми на сервер, и лишь полученный в итоге суммированный шифротекст расшифровывается с помощью ключа. Однако при такой схеме администраторам системы известно, в каком порядке приходили бюллетени от пользователей. Зная конечный результат голосования, они могут исключать по одному бюллетеню из суммированного шифротекста, складывать оставшиеся бюллетени и таким образом постепенно узнавать, как проголосовали пользователи в порядке очереди [2]. Конечно, это достаточно трудоемкий процесс, но можно создать такие условия, при которых выбор конкретных участников будет известен создателям системы ДЭГ, что ставит под сомнение ее анонимность. К тому же исследования, описанные в статьях [3, 4], выявили значительные незадокументированные возможности ДЭГ, которые также ставят под сомнение прозрачность выборов и потенциально могут нарушать тайну голосования.

В разработанной системе голосования анонимность достигается за счет простой, но эффективной схемы создания анонимного канала передачи данных от пользователей к серверу. Такая схема гарантирует, что ни сервер, ни кто-либо из участников системы не узнает, как проголосовал конкретный пользователь. Для повышения надежности в системе предполагается применение блокчейн-технологии, т. е. хранение бюллетеней как транзакций в блоках, связанных между собой хронологически и криптографически.

В представленной работе подробно описываются основные требования к разрабатываемой системе голосования, алгоритм создания и подписи бюллетеней, способы безопасной передачи данных по каналам связи и схема предложенного анонимного канала, а также рассмотрены возможные угрозы и атаки на систему, способы их предотвращения и устранения.

1. Обоснование анонимности при использовании алгоритма “слепой” подписи

Основные требования к разрабатываемой системе голосования заключаются в анонимности голосования (ни сервер, ни кто-либо из участников не должен узнать, как проголосовал конкретный участник), а также в легитимности и уникальности. В данном случае это означает, что каждый участник может получить только один бюллетень, который невозможно подделать или использовать повторно.

1.1. История алгоритма “слепой” подписи

В 1990-х гг. шифрование на уровне протокола только начинало развиваться, и люди боялись передавать данные своих карт по незащищенному каналу. В такой среде возник большой интерес к промежуточной архитектуре и появились компании, которые стали посредниками в платежах. Например, FirstVirtual [5] была первой промежуточной платежной компанией, затем появились CyberCash [6] и др. В подобных платежных системах общение между покупателем и продавцом происходило через компанию-посредника, в таком случае покупатель отправлял информацию о своей кредитной карте этому посреднику, который утверждал транзакцию и уведомлял продавца. Посред-

ник рассчитывался с продавцом в конце каждого дня. Это гарантировало покупателям анонимность перед продавцом, а также сохраняло данные их кредитных карт в безопасности, однако существенным недостатком являлась потеря удобства непосредственного общения с продавцом.

Другой способ оплаты онлайн — электронные деньги — мог бы стать более удобным для Интернет-покупателей в то время, если бы нашелся способ создать аналог наличных денег в Интернете. Он имел бы два дополнительных преимущества: во-первых, анонимность, поскольку людям не нужно использовать свою настоящую личность для оплаты покупок, и банки не смогли бы отслеживать все расходы пользователей, как они это делали по кредитным картам. Во-вторых, электронные деньги позволяют проводить офлайн-транзакции, когда нет необходимости вызывать третье лицо для подтверждения транзакции [7].

Одна из ранних идей применения криптографии к онлайн-платежам и создания электронных денег принадлежит Д. Чауму (D. Chaum) [8]. В 1983 г. он изобрел алгоритм "слепой подписи" и впервые реализовал его на основе метода RSA [9] — алгоритма с открытым ключом, основывающемся на вычислительной сложности задачи факторизации больших целых составных чисел. Основная особенность этой электронной подписи заключается в том, что подписавший не может знать содержание подписываемого документа, он только проверяет этот документ на соответствие определенным условиям (параметрам) и, при соблюдении условий, подписывает его. Данная схема применяется во многих криптографических протоколах, ее использование для системы "электронные деньги" описано Б.Я. Рябко, А.Н. Фионовым, Ю.И. Шокиным в работе [10], мы же рассмотрим его применение к протоколу "анонимное голосование".

1.2. Применение алгоритма "слепой" подписи к протоколу анонимного голосования

Алгоритм позволяет сформировать и подписать бюллетень, не раскрывая информации о том, как проголосовал конкретный участник, для выдающего бюллетени сервера. Опишем указанный алгоритм.

1. При голосовании на сервере согласно RSA генерируются 3 секретных параметра (P, Q и c) и 2 открытых параметра:

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

где P, Q — простые числа ($P, Q \leqslant 2^{512}$); N — модуль, по которому будут выполняться все операции ($N \leqslant 2^{1024}$); $\phi(N) = (P-1)(Q-1)$ — функция Эйлера для числа N; c и d — закрытый и открытый ключи соответственно ($c, d < N$, $cd \bmod \phi(N) = 1$).

2. Допустим, пользователь уже сделал выбор и хочет отправить голос. Тогда сервер передает пользователю параметры N и d и пользователь приступает к созданию данных для подписи. Он генерирует случайное число R размером 512 бит и выполняет конкатенацию с числом n, которое является закодированным решением пользователя (n не должно превышать 512 бит, кроме самого решения туда включается служебная информация о голосовании). В результате получается

$$\bar{R} = R|n.$$

3. После этого генерируется случайное число X в промежутке $[2, N-1]$ (число X должно быть взаимнопростым с N) и формируются данные для подписи:

$$h = H(\bar{R})$$
$$\bar{h} = X^d h \bmod N,$$

где h — значение хеш-функции, в разработанной системе используется алгоритм хеширования SHA3-512 [11].
4. Значение $\bar{h}$ отправляется на сервер по открытому каналу, и происходит процесс электронной подписи:

$$\bar{s} = \bar{h}^c \bmod N.$$

Фиксируется адрес пользователя, которому был выдан подписанный бюллетень, что исключает возможность вторичного голосования этого пользователя.
5. Подписанный бюллетень отправляется обратно пользователю, и он получает подписанное значение исходной хеш-функции:

$$s = X^{-1}\bar{s} = h^c \bmod N.$$

Действительно,

$$s = X^{-1}\bar{s} = X^{-1}\bar{h}^c = X^{-1}(X^d h)^c = X^{-1}X^{cd}h^c = X^{-1}X^1 h^c = h^c \bmod N.$$

6. Затем пользователь по анонимному каналу передачи данных отправляет серверу подписанный бюллетень, сообщение вида $\langle \bar{R}, s \rangle$, и сервер проводит проверку подлинности:

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

В случае совпадения значений голос считается действительным и учитывается системой голосования, а бюллетень вносится в базу данных.

Алгоритм “слепой” подписи хорош тем, что RSA может быть заменен на другой алгоритм электронной подписи с открытым и закрытым ключом, например любой из алгоритмов семейства DSA [12]. Сам протокол подписывания также может быть легко изменен без нарушения сути работы алгоритма.

2. Анонимная отправка данных по каналам связи

2.1. Распространенные методы построения защищенных сетей

Организация анонимного канала передачи данных — отдельная важная проблема, к решению которой существуют различные подходы. Любая анонимная сеть основывается либо на одноранговой, либо на гибридной архитектуре сети, исключая при этом многоранговую (сеть, в состав которой входят один или несколько серверов, выделенных под множество клиентов).

Одноранговая (децентрализованная) сеть является распределенной средой, в которой все узлы равноправны. Компьютеры такой сети могут функционировать в качестве как клиентов, так и серверов. Пользователи одноранговой сети самостоятельно решают, какие ресурсы на своем компьютере сделать общедоступными. При такой организации

любой компьютер может устанавливать соединение с остальными, посылать им запросы на предоставление ресурсов как клиент, а также принимать и отсылать запросы в качестве сервера, выполнять другие вспомогательные и административные функции.

Существует множество децентрализованных анонимных сетей (ДАС), например ANts P2P [13], Bitmessage [14], I2P [15], Freenet [16] и др. Однако децентрализованные анонимные сети имеют недостаток — в таких сетях возможно образование неравномерного распределения соединений и появление "неофициальных" узлов-серверов, часто используемых другими узлами в качестве последующей маршрутизации.

Гибридная система объединяет свойства много- и одноранговых архитектур, пытаясь взять и удержать как можно больше положительных и меньше отрицательных качеств. Плюсом многоранговых архитектур являются некоторые свойства централизации, как, например, возможность разделения логики на серверную и клиентскую, более быстрая и/или статичная скорость маршрутизации. Одноранговые же архитектуры имеют некоторые свойства децентрализации, как собственно возможность построения анонимности и достижения клиентской безопасности.

Наиболее известными и развитыми среди технологий построения гибридных сетей, предлагающих пользователям анонимность, являются VPN [17] и TOR [18].

VPN (virtual private network — виртуальная частная сеть) — обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети, например Интернет. Несмотря на то, что коммуникации могут быть реализованы через публичные сети с неизвестным уровнем доверия, уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений). Значительный недостаток виртуальных частных сетей — возможность утечки данных пользователей (логинов, паролей, банковских реквизитов, данных карт и платежных систем), так как провайдер, который предоставляет пользователю VPN-услуги, получает всю информацию о действиях пользователя во время его подключения к сети Интернет.

TOR (the onion router) — это метод многослойного шифрования данных, т. е. данные шифруются несколько раз, когда проходят через каждый из выбранных случайным образом узлов. С точки зрения анонимности метод TOR лучше VPN, так как направляет сигнал подключившегося пользователя через множество узлов по очереди, а не через один, поэтому предыдущий IP-адрес можно увидеть только перед новым узлом и новый IP-адрес за узлом, где произошла смена адреса. На каждом новом узле данные шифруются, а маршруты между узлами сети могут быть сформированы отправителем или выбраны в случайном порядке. На данный момент не существует методов, позволяющих гарантированно отследить полный путь от сайта до устройства пользователя, применяющего технологию TOR. Однако данная технология уступает VPN в скорости: сеть TOR может быть очень медленной, так как данные передаются через большое количество узлов-посредников.

2.2. Анонимный канал передачи данных

Для защищенной передачи бюллетеней на сервер часто используют более простые, но не менее эффективные способы организации анонимных каналов. Например, в работе [19] для защиты анонимности голосующих и во избежание возникновения ситуации

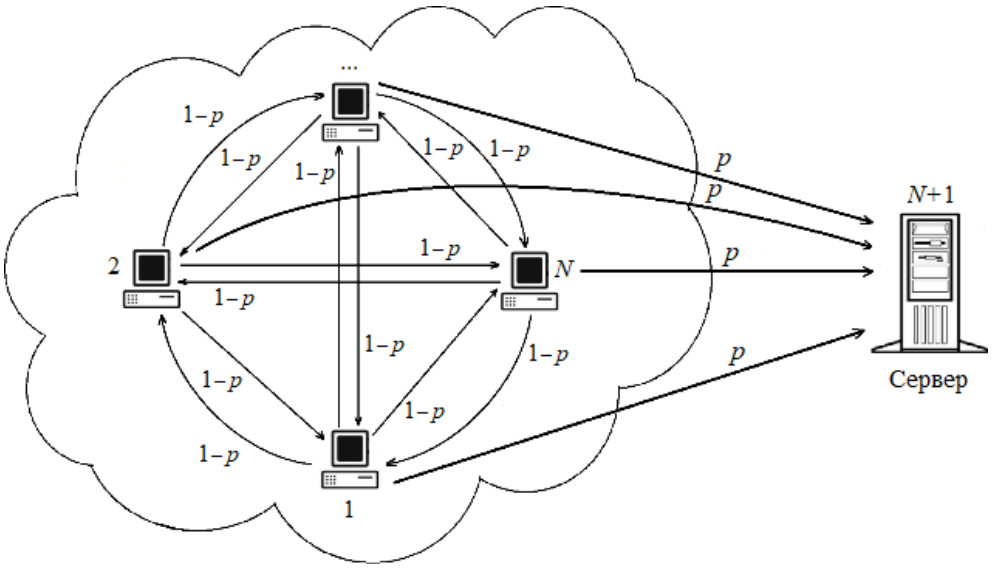

Схема узлов системы
Scheme of system nodes

повторного голосования одного и того же участника наряду с протоколом слепой подписи используется также протокол кольцевой подписи [20]. В такой схеме он представляет собой способ реализации электронной подписи, при котором известно, что сообщение подписано одним из участников голосования, но не раскрывается, кем именно. Голосующий сам формирует список из произвольного числа различных лиц, включая в него и себя. Для наложения подписи подписывающему не требуются разрешение, содействие или помощь со стороны включенных в список лиц — используются только открытые ключи всех членов списка и закрытый ключ лишь самого подписывающего. Такой способ достаточно эффективен и используется в некоторых реализациях блокчейн-технологии (в частности, CryptoNote [21]).

Однако для защиты анонимности голосующих можно предложить более эффективный способ передачи данных от пользователей к серверу. Таким средством является протокол анонимного голосования, предложенный ранее в [22], использованный для создания системы, отвечающей всем требованиям безопасности, которые ставятся для гарантии анонимности выбора. Протокол гарантирует со 100 %-ной вероятностью, что установление личности исходного отправителя бюллетеня невозможно.

Система голосования представляет собой сеть из N узлов и одного сервера, на который будут отправляться данные от этих узлов. Будем считать, что каждый из узлов сети связан с остальными узлами и сервером, не обязательно напрямую, т. е. существует возможность установить соединение и передать данные между любой парой узел – узел и узел – сервер (см. рисунок). В рамках этого протокола не требуется, чтобы сервер передавал какой-либо ответ, необходимо только отправить на сервер данные таким образом, чтобы никто не мог однозначно установить изначального отправителя. Важнейшим параметром системы является общее для всех число $0 < p < 1$ — вероятность передачи сообщения напрямую серверу.

Действия каждого из узлов в рамках передачи сообщения описываются следующим образом.

1. Пусть некоторому узлу требуется анонимно отправить на сервер сообщение. Узел генерирует случайное число $0 \leqslant k \leqslant 1$. Если полученное число $k \leqslant p$, то узел

устанавливает соединение с сервером и пересылает ему сообщение. Если $k > p$, узел случайным образом выбирает один из узлов сети (с вероятностью $1/(N-1)$), устанавливает с ним соединение и передает ему сообщение.

2. Пусть некоторый узел получил сообщение, тогда алгоритм действий будет аналогичен описанному в п. 1. Узел генерирует k и либо отправляет сообщение на сервер, либо пересылает его другому узлу.

Кроме самого сообщения, от узлов не передается никакая другая дополнительная информация, поэтому если какой-либо узел или сервер получил сообщение, то он может утверждать только, что с вероятностью p изначальным отправителем был исходный узел. Можно доказать, что сообщение будет переслано на сервер в любом случае, для этого опишем вероятность отправки сообщения за n или меньше шагов:

$$P(l \leqslant n) = \sum_{i=0}^{n} p(1-p)^i.$$

Здесь l — количество шагов, через которое сообщение дошло до сервера. Предел этой вероятности $\lim\limits_{n\to\infty} P(l \leqslant n) = 1$, кроме того, для любого p можно легко показать, за сколько шагов он приблизится к 1 настолько, что погрешностью можно будет пренебречь. Например, для $p = 0.5 P(l \leqslant 10) \approx 0.999$.

Достигаемую степень анонимности сети можно оценить с помощью информационной энтропии (количественной меры неопределенности некоторой системы) [23]. Для случайной величины x, принимающей n независимых случайных значений x_i с вероятностями p_i $(i = 1, \ldots, n)$, информационная энтропия рассчитывается по формуле Шеннона

$$H(x) = \sum_{i=1}^{n} p_i \log_2 p_i.$$

Неопределенность отправителя сообщения на сервере зависит от вероятности p, с которой любой узел посылает сообщение на сервер. При $p \to 1$ очевидно, что неопределенность на сервере, выраженная с помощью энтропии, стремится к нулю (минимальному значению), так как с очень большой вероятностью сообщение было сформировано участником, приславшим его на сервер. Максимальной энтропия системы будет тогда, когда сообщение, пришедшее на сервер, могло быть создано любым из участников сети с одинаковой вероятностью. В таком случае вероятность того, что автором сообщения был его отправитель на сервер, равна $1/N$, где N — количество клиентских узлов. Из предыдущих утверждений следует, что при настройке системы голосования нужно выбирать такую вероятность p, чтобы по мере возможности приближать значение энтропии на сервере к наибольшему. В этом случае анонимность сети также стремится к максимуму. Для любого количества узлов в сети можно аналитически или экспериментально вычислить такое значение p, при котором автором сообщения, пришедшего на сервер, мог являться как его отправитель, так и любой из остальных участников сети с равной вероятностью. Например, для сети из двух клиентских узлов и одного сервера, по результатам проведенного авторами имитационного моделирования, максимальная энтропия на сервере достигается при $p = 0.00069$, тогда вероятность того, что автором бюллетеня был его отправитель, равна 0.5, энтропия в таком случае стремится к единице (максимальной для данной конфигурации узлов). В дальнейшем планируется исследовать аналитическую модель сети с бóльшим количеством узлов и оценить для

нее неопределенность на сервере. Неопределенность же отправителя сообщения в узлах сети окажется максимальной независимо от выбранного значения p, потому что вероятности получения сообщения от любого из узлов сети одинаковы и равны $(1-p)/(N-1)$, где N — количество клиентских узлов.

3. Безопасное хранение данных голосования

Чтобы обеспечить анонимность голосов участников и при этом оставить голосование прозрачным для всех, каждому участнику нужно дать возможность проверить, что его голос был правильно учтен при подведении итогов голосования. Для этого производятся следующие действия: после того как участник проголосовал, он получает свой уникальный бюллетень; голос из бюллетеня учитывается в голосовании, а сам бюллетень также записывается в базу данных бюллетеней. База данных должна быть открытой, доступной для просмотра всем участникам, чтобы каждый проголосовавший пользователь мог сравнить номер своего бюллетеня с номерами в базе и убедиться, что его голос засчитан. Для того чтобы эти условия выполнялись, предлагается использовать базу данных на основе блокчейн-технологии, т. е. хранить бюллетени как транзакции в блоках, связанных между собой криптографически.

Blockchain (blockchain — цепочка блоков) — это способ хранения данных или цифровой реестр транзакций, сделок, контрактов (публичная база всех транзакций, когда-либо совершенных в системе), другими словами, всего, что нуждается в отдельной независимой записи и при необходимости в проверке.

В разных реализациях блокчейн-технологии для создания нового блока могут использоваться различные алгоритмы консенсуса, для некоторых из них может требоваться специализированная блокчейн-сеть. Самым первым и классическим алгоритмом консенсуса является Proof-of-Work [24] (PoW — доказательство выполнения работы). Для создания блока с помощью PoW майнеру нужно найти некое хеш-значение с определенными свойствами. Чтобы получить такое значение, майнер должен решать сложную математическую задачу, заключающуюся в поиске подходящего результирующего значения хеш-функции, тратя на это вычислительные ресурсы компьютера. Первый, кто успеет создать блок, награждается монетами данной системы. Однако PoW обладает рядом недостатков. Во-первых, майнинг слишком энергозатратен, во-вторых, пользователям приходится платить майнерам комиссии за проверку транзакций. Таким образом, чем более загружена сеть, тем выше в ней комиссии, при небольших транзакциях комиссии могут даже превышать сумму самого перевода. В-третьих, существенными недостатками являются низкая скорость и плохая масштабируемость. Четвертым минусом такого алгоритма может стать централизация майнеров, объединяющихся в пулы. Это снижает безопасность сети, повышает сложность майнинга и способствует росту комиссий.

Альтернативой метода PoW является другой алгоритм консенсуса, называющийся Proof-of-Stake [25] (PoS — доказательство доли владения). В PoS нет майнинга, вместо решения математических задач новые монеты добываются путем стейкинга — механизма, позволяющего добавлять новые блоки за счет доказательства владения криптовалютой этой сети. Узлы такой сети называются валидаторами, а их баланс — стейком. Чем больше у владельца узла монет в кошельке, тем больше у него шансов подтвердить новый блок и получить вознаграждение, т. е. вероятность формирования участником очередного блока в блокчейне пропорциональна доле, которую составляют при-

надлежащие этому участнику расчетные единицы данной криптовалюты от их общего количества. Но стейкинг, так же как майнинг, требует расходов и технических знаний. Чтобы стать валидатором, надо обладать минимально необходимым количеством монет. Эти монеты надо держать заблокированными в кошельке на протяжении как минимум нескольких месяцев. Также понадобится настроить оборудование и держать его постоянно подключенным к сети. Главным же недостатком PoS-алгоритма является угроза централизации. Валидаторы с наибольшим количеством монет в конечном итоге будут контролировать бóльшую часть блокчейн-сети.

Проанализировав вышеуказанные алгоритмы консенсуса, мы пришли к выводу, что для системы голосований с небольшим количеством участников реализовать блокчейн-систему открытого типа, основанную на одном из этих алгоритмов консенсуса, невозможно, так как не все участники голосования будут готовы заниматься майнингом или стейкингом. Поэтому для надежного хранения бюллетеней на сервере разработана модификация протокола анонимного голосования, представленного в подразд. 1.1. В данной модификации на этапе генерации параметров системы по алгоритму RSA секретный ключ и открытые ключи d, N создаются не только для сервера, но и для каждого голосующего пользователя. Открытые ключи сервера и всех клиентов будут храниться в базе данных, и видеть их смогут все участники системы. Подписанный бюллетень отправляется на сервер голосования по анонимному каналу связи.

Когда бюллетень дойдет до сервера, сервер должен проверить корректность бюллетеня и в случае корректности учесть голос пользователя. Когда время, выделенное на голосование, закончится и все отправленные пользователями бюллетени дойдут до сервера, сервер высылает всем клиентам следующую информацию: список всех бюллетеней в случайном порядке и значение хеш-функции от списка всех бюллетеней.

Каждый пользователь, получив эту информацию, на своей стороне проверяет, что его бюллетень действительно находится в списке всех бюллетеней и что значение хеш-функции от списка бюллетеней сервер подсчитал верно, затем подписывает хеш от списка бюллетеней своим секретным ключом и высылает серверу полученное число (подпись).

Если бюллетени всех пользователей оказались в общем списке, то сервер получает от всех участников голосования их подписи, подтверждающие, что их бюллетени действительно находятся в списке всех бюллетеней. Затем сервер приступает к формированию блока, содержащего всю информацию о прошедшем голосовании. Блок для каждого голосования будет содержать значение хеш-функции от предыдущего блока, список всех бюллетеней в случайном порядке, а также для каждого клиента его логин, его подпись списка всех бюллетеней и его открытый ключ (позволяющий проверить корректность подписи этого пользователя). Таким образом, все блоки в цепочке будут связаны криптографически и хронологически, и никто не сможет изменить информацию о прошедших голосованиях.

4. Возможные угрозы и атаки на систему

Для того чтобы в полной мере проанализировать надежность представленной системы, необходимо рассмотреть все потенциальные уязвимости. Их можно разделить на две категории: уязвимости, допускаемые при описании системы, и уязвимости, возникающие в системе на этапе ее программной реализации.

Угрозы, возникающие при программной реализации системы. Большинство уязвимостей в системе не относятся напрямую к ее описанию, но возникают в процессе ее программной реализации и могут быть обнаружены и исправлены на этапе тестирования. Подобные уязвимости могут возникать в неограниченном количестве вследствие некорректной организации системы голосования, а также некачественной разработки программного кода. Например, одна из распространенных уязвимостей может возникнуть, если не разделять интерфейс администратора системы и интерфейс рядовых пользователей. В таком случае любой пользователь сможет получить доступ к исходному коду и, взломав систему, управлять функциями администратора.

Угрозы, возникающие при описании системы. Такие аспекты, как организация надежного протокола для создания, подписывания и конечной отправки бюллетеней на сервер, а также для хранения данных голосования, должны быть проработаны на этапе теоретического описания системы.

Угрозы, возникающие при создании и подписании бюллетеня. Самая очевидная уязвимость могла бы возникнуть из-за использования в системе алгоритма RSA, который обладает мультипликативным свойством. Вследствие этого, если некий злоумышленник имеет хотя бы два настоящих (возможно, чужих) подписанных бюллетеня одного и того же голосования $\langle \bar{R}_1, s_1 \rangle$ и $\langle \bar{R}_2, s_2 \rangle$, то он может создать новый подписанный фальшивый бюллетень $\langle \bar{R}_3, s_3 \rangle$, получив его с помощью перемножения основных частей имеющихся бюллетеней:

$$\bar{R}_3 = \bar{R}_1 \bar{R}_2 \bmod N,$$
$$s_3 = s_1 s_2 \bmod N.$$

Таким образом,

$$\bar{R_3}^c = (\bar{R}_1 \bar{R}_2)^c = \bar{R_1}^c \bar{R_2}^c = s_1 s_2 = s_3 \bmod N,$$

т. е. s_3 будет являться подлинной подписью для $\bar{R}_3$. Тогда злоумышленник мог бы отправить сфабрикованный бюллетень $\langle \bar{R}_3, s_3 \rangle$ на сервер и повлиять на результаты голосования. Однако в данной схеме подобная уязвимость устранена, поскольку для борьбы с мультипликативным свойством алгоритма RSA сервером подписывается не просто основная часть бюллетеня с выбранным пользователем вариантом ответа на голосование и служебной информацией внутри, а значение хеш-функции SHA3-512, вычисляемое от $\bar{R}$. Так как данная хеш-функция не обладает мультипликативным свойством, создать новый бюллетень посредством перемножения двух старых становится невозможно.

Еще одна уязвимость — повторное использование бюллетеней в одном голосовании — исключается за счет присваивания каждому бюллетеню своего номера, сохранения всех зачтенных бюллетеней в базу данных на сервере и сравнения каждого нового приходящего на сервер бюллетеня с уже лежащими в базе.

Если же говорить о других возможных уязвимостях вышеописанной системы, следует рассмотреть такой случай фальсификации голосов, когда злоумышленник возьмет бюллетень из одного голосования и проголосует в другом, используя данный бюллетень. Однако такая ситуация возможна только в том случае, когда ключи N и c одинаковы для разных голосований. В представленной системе для каждого голосования генерируются новые ключи, таким образом она защищена от подобной атаки.

Угрозы, возникающие при отправке данных по анонимному каналу. Если каждый пользователь отправляет свой бюллетень, а также пересылает чужие бюллетени с вероятностью p на сервер и с вероятностью $1 - p$ другому участнику голосования,

то может возникнуть следующая ситуация. Какой-то недобросовестный пользователь захочет саботировать процесс голосования и не станет отправлять свой или чужой бюллетень. При этом невозможно отследить, на каком узле сети произошло такое недобросовестное поведение. Для устранения данной уязвимости предлагается добавить в протокол анонимного голосования, представленный в подразд. 1.1, следующее.

Участник, получивший чужой бюллетень по каналу связи, вычисляет значение хеш-функции от этого пришедшего бюллетеня, подписывает это хеш-значение своим секретным ключом и отправляет обратно приславшему. Затем он отправляет присланный ему бюллетень дальше (на сервер или любому другому участнику голосования). В результате на сервере формируется общий список пришедших бюллетеней и рассылается всем участникам. Если пользователь на данном этапе обнаружил, что его бюллетеня нет в общем списке бюллетеней, то он может доказать, что его бюллетень был отправлен другому пользователю и от данного пользователя пришел подписанный им хеш полученного бюллетеня. И так далее по цепочке до сервера. На этом этапе станет понятно, кто не отправил бюллетень дальше и саботировал голосование.

Другие угрозы. При использовании системы голосования может произойти сговор всех участников, кроме одного отправителя. Тогда сговорившиеся участники смогут узнать выбор пользователя, не участвующего в сговоре. Если же в сговоре не будут участвовать хотя бы два узла, то определить, кто из них как проголосовал, становится проблематично (если они не проголосуют одинаково).

Также стоит рассмотреть ситуацию с недобросовестным сервером. Если сервер начнет фальсифицировать голоса, это легко выявить: если в данных о голосовании, записанных в блок, количество бюллетеней в общем списке не совпадет с количеством подписей от участников, притом что все участники подписали общий список. В таком случае очевидно, что сервер добавил лишние бюллетени, и тогда голосование должно считаться недействительным.

Заключение

Описана схема создания анонимного дистанционного голосования с обоснованной надежностью и анонимностью, при котором в протоколе используется слепая подпись, алгоритм создания анонимного канала передачи данных и блокчейн-технология для безопасного хранения данных голосования. Рассмотрены аналоги предложенной системы голосований, проанализированы их достоинства и недостатки.

Использующийся в системе протокол слепой подписи действительно гарантирует невозможность подделки бюллетеней или их повторного использования. Кроме того, в бюллетенях не будет находиться никаких лишних данных, которые могли бы раскрыть личность голосующего. Представленная в работе схема организации анонимного канала передачи бюллетеней позволяет пользователям отправлять свои голоса на сервер, не раскрывая их выбор. Хранение приходящих на сервер бюллетеней как транзакций в блокчейне, связывая их криптографически и хронологически, не дает злоумышленникам или недобросовестному серверу возможностей добавить лишние бюллетени или удалить уже зарегистрированные в системе.

Представленная схема тайного дистанционного голосования является хорошей альтернативой традиционному голосованию и другим анонимным цифровым системам для голосований. Чтобы на практике продемонстрировать удобство и надежность системы, использующей предложенные протоколы, такая система была разработана для внут-

ренних голосований в Институте вычислительных технологий СО РАН. Эта система удаленного анонимного голосования доступна по ссылке [26], она соответствует всем требованиям безопасности для подобных систем.

Благодарности. Исследование выполнено в рамках НИОКТР № 122031600164-6 от 15.03.2022.

Список литературы

[1] Портал дистанционного электронного голосования. Адрес доступа: https://vybory.gov.ru (дата обращения 16.01.2024).

[2] Как устроено дистанционное электронное голосование в России, и какие у него перспективы. Адрес доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B0%D0%BA_%D1%83%D1%81%D1%82%D1%80%D0%BE%D0%B5%D0%BD%D0%BE_%D0%B4%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B5_%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%BE%D0%B5_%D0%B3%D0%BE%D0%BB%D0%BE%D1%81%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8,_%D0%B8_%D0%BA%D0%B0%D0%BA%D0%B8%D0%B5_%D1%83_%D0%BD%D0%B5%D0%B3%D0%BE_%D0%BF%D0%B5%D1%80%D1%81%D0%BF%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D1%8B (дата обращения 16.01.2024).

[3] Что же не так с ДЭГ в Москве? Адрес доступа: https://habr.com/ru/post/579350 (дата обращения 16.01.2024).

[4] Что же не так с любыми электронными голосованиями? Адрес доступа: https://habr.com/ru/post/579968 (дата обращения 16.01.2024).

[5] **Huff S., Wade M.** First virtual holdings incorporated. ICIS 1999 Proceedings. 1999: 76. Available at: https://dl.acm.org/doi/pdf/10.5555/352925.353020.

[6] **Eastlake 3rd D., Boesch B., Crocker S., Yesil M.** CyberCash credit card protocol version 0.8 (No. rfc1898). 1996. Available at: https://www.rfc-editor.org/rfc/rfc1898.html.

[7] **Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S.** Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press; 2016: 336.

[8] **Chaum D., Rivest R.L., Sherman A.T.** Blind signatures for untraceable payments. Advances in Cryptology Proceedings of Crypto 82. N.Y.: Plenum (Springer-Verlag); 1982: 199–203.

[9] **Rivest R., Shamir A., Adleman L.** A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. N.Y.: ACM; 1978; 21(2):120–126. DOI:10.1145/359340.359342.

[10] **Рябко Б.Я., Фионов А.Н., Шокин Ю.И.** Криптография и стеганография в информационных технологиях. Новосибирск: Наука; 2015: 240.

[11] **Bertoni G., Daemen J., Peeters M., Assche G.V.** The Keccak reference. 2011. Available at: https://keccak.team/files/Keccak-reference-3.0.pdf.

[12] **Kerry C.F., Gallagher P.D.** Digital signature standard (DSS). FIPS PUB; 2013: 130. Available at: http://people.csail.mit.edu/alinush/6.857-spring-2015/papers/dsa.pdf.

[13] ANts P2P file-sharing peer-to-peer. Available at: https://antsp2p.sourceforge.net (accessed 25.12.2022).

[14] **Warren J.** Bitmessage: a peer-to-peer message authentication and delivery system. 2012. Available at: https://bitmessage.org/bitmessage.pdf.

[15] The Invisible Internet Project (I2P). Available at: https://geti2p.net/en (accessed 16.01.2024).

[16] HYPHANET. Available at: https://freenetproject.org (accessed 16.01.2024).

[17] **Ferguson P., Huston G.** What is a VPN?. 1998: 22. Available at: https://www.potaroo.net/papers/vpn.pdf.

[18] **Dingledine R., Mathewson N., Syverson P.** Tor: the second-generation onion router. Naval Research Lab Washington DC. 2004: 17. Available at: https://svn-archive.torproject.org/svn/projects/design-paper/tor-design.pdf.

[19] **Zhu Y., Zeng Z., Lv C.** Anonymous voting scheme for boardroom with blockchain. International Journal of Performability Engineering. 2018; 14(10):2414–2422. DOI:10.23940/ijpe.18.10.p17.24142422. Available at: https://www.ijpe-online.com/EN/10.23940/ijpe.18.10.p17.24142422.

[20] **Rivest R.L., Adi S., Yael T.** How to leak a secret. Proceedings of 7th International Conference on the Theory and Application of Cryptology and Information Security. Gold Coast, Australia; 2001: 552–565.

[21] **Van Saberhagen N.** CryptoNote v 2.0. 2013. Available at: https://bytecoin.org/old/whitepaper.pdf.

[22] **Dyachkova I., Rakitskiy A.** Anonymous remote voting system. 2019 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON). Novosibirsk; 2019: 0850–0852.

[23] **Shannon C.E.** A mathematical theory of communication. Bell System Technical Journal. 1948; 27(3):379–423. DOI:10.1002/j.1538-7305.1948.tb01338. Available at: https://onlinelibrary.wiley.com/doi/10.1002/j.1538-7305.1948.tb01338.x.

[24] **Jakobsson M., Juels A.** Proofs of work and bread pudding protocols. Secure Information Networks: Communications and Multimedia Security. Kluwer Academic Publishers; 1999: 258–272. DOI:10.1007/978-0-387-35568-9_18. Available at: https://link.springer.com/chapter/10.1007/978-0-387-35568-9_18.

[25] **Chohan Usman W.** Proof-of-Stake algorithmic methods: a comparative summary. SSRN Electronic Journal. 2018; DOI:10.2139/ssrn.3131897. Available at: https://ssrn.com/abstract=3131897.

[26] Система дистанционного анонимного голосования. Адрес доступа: https://rvs.ict.nsc.ru/ (дата обращения 16.01.2024).

Вычислительные технологии, 2024, том 29, № 1, с. 59–73. © ФИЦ ИВТ, 2024 ISSN 1560-7534
Computational Technologies, 2024, vol. 29, no. 1, pp. 59–73. © FRC ICT, 2024 eISSN 2313-691X

INFORMATION TECHNOLOGIES

DOI:10.25743/ICT.2024.29.1.006

Electronic anonymous voting system based on "blind" digital signature

I. S. Dyachkova[1,*], A. A. Rakitskiy[1,2,3]

[1]Siberian State University of Telecommunications and Informatics, 630102, Novosibirsk, Russia
[2]Federal Research Center for Information and Computational Technologies, 630090 Novosibirsk, Russia
[3]Novosibirsk State University, 630090, Novosibirsk, Russia
*Corresponding author: Irina S. Dyachkova, e-mail: dyach199@gmail.com
Received September 28, 2022, revised January 20, 2023, accepted March 06, 2023.

Abstract

Nowadays, remote voting systems and applications become very popular, but they have some drawbacks, especially in terms of anonymity. The aim of the paper is to create a scheme for

developing a reliable anonymous remote voting system. The methodology for designing such a scheme is based on the algorithm of "blind" ballots digital signature. This algorithm is one of the effective ways to generate and sign a voting ballot, where its encrypted voting results are transmitted to the ballot server without any information about user. A secret channel protocol was created to anonymously transfer ballots from voters to a server. This article proves the reliability of this method and also presents a recommended method for securely storing ballots as block chain transactions. In addition, possible threats to the security of the system were investigated and analyzed and there were presented possible ways to prevent them. As the result of this work, an effective scheme for creating an anonymous remote voting system with relatively small number of participants was described. Moreover, the reliability of the presented system was analyzed and it was demonstrated that the system of anonymous remote voting is not affected by possible vulnerabilities discovered during the investigation. As a result of the performed research, it was shown that the presented anonymous remote voting scheme is a good alternative to traditional voting and other similar systems.

Keywords: anonymous voting, cryptography, anonymous data transmission, blockchain technology, threat analysis.

Citation: Dyachkova I.S., Rakitskiy A.A. Electronic anonymous voting system based on "blind" digital signature. Computational Technologies. 2024; 29(1):59–73. DOI:10.25743/ICT.2024.29.1.006. (In Russ.)

Acknowledgements. The work was carried out within the framework of R&D No. 122031600164-6 dated March 15, 2022.

References

1. Portal Distantsionnogo elektronnogo golosovaniya [Remote electronic voting portal]. Available at: https://deg.rt.ru (accessed 28.07.2022). (In Russ.)
2. Kak ustroeno distantsionnoe elektronnoe golosovanie v Rossii, i kakie u nego perspektivy [How remote electronic voting works in Russia, and what are its prospects]. Available at: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B0%D0%BA_%D1%83%D1%81%D1%82%D1%80%D0%BE%D0%B5%D0%BD%D0%BE_%D0%B4%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B5_%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%BE%D0%B5_%D0%B3%D0%BE%D0%BB%D0%BE%D1%81%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8,_%D0%B8_%D0%BA%D0%B0%D0%BA%D0%B8%D0%B5_%D1%83_%D0%BD%D0%B5%D0%B3%D0%BE_%D0%BF%D0%B5%D1%80%D1%81%D0%BF%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D1%8B (accessed 16.01.2024). (In Russ.)
3. Chto zhe ne tak s DEG v Moskve [What is wrong with the remote anonymous voting in Moscow]? Available at: https://habr.com/ru/post/579350 (accessed 16.01.2024). (In Russ.)
4. Chto zhe ne tak s lyubymi elektronnymi golosovaniyami [What is wrong with any electronic voting]? Available at: https://habr.com/ru/post/579968 (accessed 16.01.2024). (In Russ.)
5. **Huff S., Wade M.** First virtual holdings incorporated. ICIS 1999 Proceedings. 1999: 76. Available at: https://dl.acm.org/doi/pdf/10.5555/352925.353020.
6. **Eastlake 3rd D., Boesch B., Crocker S., Yesil M.** CyberCash credit card protocol version 0.8 (No. rfc1898). 1996. Available at: https://www.rfc-editor.org/rfc/rfc1898.html.
7. **Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S.** Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press; 2016: 336.
8. **Chaum D., Rivest R.L., Sherman A.T.** Blind signatures for untraceable payments. Advances in Cryptology Proceedings of Crypto 82. N.Y.: Plenum (Springer-Verlag); 1982: 199–203.
9. **Rivest R., Shamir A., Adleman L.** A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. N.Y.: ACM; 1978; 21(2):120–126. DOI:10.1145/359340.359342.
10. **Ryabko B.Ya., Fionov A.N., Shokin Yu.I.** Kriptografiya i steganografiya v informatsionnykh tekhnologiyakh [Cryptography and steganography in information technologies]. Novosibirsk: Nauka; 2015: 240. (In Russ.)
11. **Bertoni G., Daemen J., Peeters M., Assche G.V.** The Keccak reference. 2011. Available at: https://keccak.team/files/Keccak-reference-3.0.pdf.

12. **Kerry C.F., Gallagher P.D.** Digital signature standard (DSS). FIPS PUB; 2013: 130. Available at: http://people.csail.mit.edu/alinush/6.857-spring-2015/papers/dsa.pdf.
13. ANts P2P file-sharing peer-to-peer. Available at: https://antsp2p.sourceforge.net (accessed 25.12.2022).
14. **Warren J.** Bitmessage: a peer-to-peer message authentication and delivery system. 2012. Available at: https://bitmessage.org/bitmessage.pdf.
15. The Invisible Internet Project (I2P). Available at: https://geti2p.net/en (accessed 16.01.2024).
16. HYPHANET. Available at: https://freenetproject.org (accessed 16.01.2024).
17. **Ferguson P., Huston G.** What is a VPN?. 1998: 22. Available at: https://www.potaroo.net/papers/vpn.pdf.
18. **Dingledine R., Mathewson N., Syverson P.** Tor: the second-generation onion router. Naval Research Lab Washington DC. 2004: 17. Available at: https://svn-archive.torproject.org/svn/projects/design-paper/tor-design.pdf.
19. **Zhu Y., Zeng Z., Lv C.** Anonymous voting scheme for boardroom with blockchain. International Journal of Performability Engineering. 2018; 14(10):2414–2422. DOI:10.23940/ijpe.18.10.p17.24142422. Available at: https://www.ijpe-online.com/EN/10.23940/ijpe.18.10.p17.24142422.
20. **Rivest R.L., Adi S., Yael T.** How to leak a secret. Proceedings of 7th International Conference on the Theory and Application of Cryptology and Information Security. Gold Coast, Australia; 2001: 552–565.
21. **Van Saberhagen N.** CryptoNote v 2.0. 2013. Available at: https://bytecoin.org/old/whitepaper.pdf.
22. **Dyachkova I., Rakitskiy A.** Anonymous remote voting system. 2019 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON). Novosibirsk; 2019: 0850–0852.
23. **Shannon C.E.** A mathematical theory of communication. Bell System Technical Journal. 1948; 27(3):379–423. DOI:10.1002/j.1538-7305.1948.tb01338. Available at: https://onlinelibrary.wiley.com/doi/10.1002/j.1538-7305.1948.tb01338.x.
24. **Jakobsson M., Juels A.** Proofs of work and bread pudding protocols. Secure Information Networks: Communications and Multimedia Security. Kluwer Academic Publishers; 1999: 258–272. DOI:10.1007/978-0-387-35568-9_18. Available at: https://link.springer.com/chapter/10.1007/978-0-387-35568-9_18.
25. **Chohan Usman W.** Proof-of-Stake algorithmic methods: a comparative summary. SSRN Electronic Journal. 2018; DOI:10.2139/ssrn.3131897. Available at: https://ssrn.com/abstract=3131897.
26. Sistema distantsionnogo anonimnogo golosovaniya [Remote anonymous voting system]. Available at: https://rvs.ict.nsc.ru/ (accessed 16.01.2024). (In Russ.)