

32. Chechin G., Ryabov D. Exact solutions of nonlinear dynamical equations for large-amplitude atomic vibrations in arbitrary monoatomic chains with fixed ends, *arXiv:2109.09101v1*, 2021. Available at: <https://doi.org/10.1016/j.cnsns.2023.107176>.
33. Semenov A.S., Ryabov D.S., Chechin G.M., Dmitriev S.V. Lokalizovannye i delokalizovannye nelineynye kolebatel'nye mody treugol'noy reshetki [Localized and delocalized nonlinear vibrational modes of a triangular lattice], *Kompleksnyy analiz, matematicheskaya fizika i nelineynye uravneniya* [Complex Analysis, Mathematical Physics and Nonlinear Equations], 2021, pp. 64-65.
34. Chechin G., Ryabov D. Properties of large-amplitudes vibrations in dynamical systems with discrete symmetry. Geometrical aspects, *arXiv:2005.13343v1*, 2020. Available at: <https://arxiv.org/abs/2005.13343v1>.

Бурлаченко Иван Сергеевич – Южный федеральный университет; e-mail: iburlachenko@sfedu.ru; г. Таганрог, Россия; тел.: +79054395264; кафедра физико-математических основ инженерного образования; ассистент.

Чечин Георгий Михайлович – НИИ Физики, Южный федеральный университет; e-mail: gmchechin@sfedu.ru; г. Ростов-на-Дону, Россия; тел.: +79054315081; с.н.с.; к.ф.-м.н.

Burlachenko Ivan Sergeevich – Southern Federal University; e-mail: iburlachenko@sfedu.ru; Taganrog, Russia; phone: +79054395264; the Department of Physical and Mathematical Foundations of Engineering Education; assistant.

Chechin Georgy Mikhailovich – Research Institute of Physics, Southern Federal University; e-mail: gmchechin@sfedu.ru; Rostov-on-Don, Russia, phone: +79054315081; senior researcher; cand. phys. and math. sc.

УДК 003.26

DOI 10.18522/2311-3103-2026-4-201-212

Ж.-М.Н. Дакуо, С.В. Беззатеев, В.В. Давыдов, И.Д. Иогансон, А.Ф. Хуцаева

МОДЕЛЬ СХЕМЫ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ С ВОЗМОЖНОСТЬЮ ИЗМЕНЕНИЯ РЕШЕНИЯ УЧАСТНИКОМ ДО МОМЕНТА ОКОНЧАНИЯ ГОЛОСОВАНИЯ

Существующие протоколы электронного голосования, как правило, обладают архитектурой, в которой отправка бюллетеня является необратимым действием. Такой подход ограничивает удобство использования системы, поскольку участник не может исправить случайную ошибку или изменить свое решение в течение периода голосования без прохождения повторной процедуры аутентификации либо аннулирования ранее поданного бюллетеня. Целью настоящей работы является разработка теоретической модели криптографического протокола электронного голосования, обеспечивающей нативную возможность многократного изменения решения для повышения удобства использования при сохранении анонимности и корректности подсчета. Архитектура предлагаемой модели основана на совместном использовании схемы обязательств с потайным входом для реализации свойства изменения решения, проверяемой случайной функции (VRF) для формирования бюллетеней, протокола Privacy Pass для анонимной авторизации участников и смешанных сетей (Mix-Nets), обеспечивающих сокрытие связи между пользователем и передаваемыми сообщениями. Разработан протокол электронного голосования, позволяющий участнику неоднократно изменять свое решение без повторного обращения к центру регистрации после получения права на участие в голосовании, что уменьшает количество интерактивных действий и повышает удобство использования системы. Проведен теоретический анализ стойкости предложенной модели, подтверждающий выполнение основных и ряда расширенных свойств, включая, полноту, устойчивость, приемлемость, проверяемость, конфиденциальность участника, одноразовость, справедливость, атомарную и универсальную проверяемость, а также возможность изменения решения. Благодаря модульной архитектуре модель допускает применение различных криптографических примитивов, включая постквантовые алгоритмы, без изменения общей логики функционирования протокола, что делает предложенный подход перспективной основой для построения защищенных систем электронного голосования, стойких к атакам квантового компьютера.

Электронное голосование; схема обязательств с потайным входом; изменение решения; проверяемая случайная функция; универсальная проверяемость; Privacy Pass; анонимность.

Z.-M.N. Dakuo, S.V. Bezzateev, V.V. Davydov, I.D. Ioganson, A.F. Khutsaeva

MODEL OF AN ELECTRONIC VOTING SCHEME WITH THE POSSIBILITY OF CHANGING THE PARTICIPANT'S DECISION BEFORE THE END OF VOTING

Existing electronic voting protocols often feature an architecture where ballot submission is an irreversible action. This significantly reduces system usability, depriving the participant of the right to correct an accidental error or change their opinion during lengthy decision-making procedures. The aim of the work is to develop a model of a cryptographic protocol that provides a native capability for multiple decision changes to enhance usability while maintaining strict anonymity and counting correctness. The architecture is based on the integration of a trapdoor commitment scheme to implement choice flexibility, a verifiable random function (VRF) for ballot generation, the Privacy Pass protocol for anonymous authorization, and mix-networks. An electronic voting protocol has been developed that implements the possibility for a participant to change their decision multiple times. The fulfillment of basic and some extended security properties, including, but not limited to, participant confidentiality and universal verifiability, has been theoretically proven. It is shown that, unlike existing analogs, changing a decision in the proposed model does not require repeating a complex authentication procedure or key revocation, which minimizes the number of interactive user actions. The proposed solution aligns the user experience of secure voting with the standards of modern digital services by providing a choice editing function, thereby increasing the convenience of the voting procedure for participants. The modular structure of the model allows for the application of any robust cryptographic algorithms, including post-quantum ones.

Electronic voting; trapdoor commitment scheme; revisability; verifiable random function; universal verifiability; Privacy Pass; anonymity.

Введение. В условиях цифровой трансформации общества системы электронного голосования (ЭГ) становятся широко используемым инструментом для дистанционного принятия коллективных решений. Данные технологии находят применение не только в государственных избирательных процессах, но и в корпоративном управлении, деятельности акционерных обществ и децентрализованных автономных организаций. Однако переход к цифровому формату требует реализации сложных криптографических протоколов, способных обеспечить уровень доверия и безопасности, сопоставимый с традиционным голосованием.

Проектирование систем ЭГ требует соблюдения комплекса обязательных условий. В современной теории [1–3] эти требования классифицируются на три группы: **основные, расширенные**, а также **эксплуатационные**, отражающие практичность и удобство использования системы.

К основным требованиям относят:

- ♦ **Полнота (Completeness):** все действительные решения участников подсчитываются правильно.
- ♦ **Устойчивость (Soundness):** недействительные решения участников не учитываются.
- ♦ **Приемлемость (Eligibility):** только легитимные участники могут принимать участие в голосовании.
- ♦ **Проверяемость (Verifiability):** никто не может фальсифицировать результаты голосования.
- ♦ **Конфиденциальность участника (Privacy):** решение отдельного участника хранится в тайне.
- ♦ **Одноразовость (Unreusability):** решение каждого участника учитывается единожды.
- ♦ **Справедливость (Fairness):** ничто не должно влиять на голосование, т. е. никакие промежуточные результаты никому не могут быть известны.

К расширенным требованиям относят:

- ♦ **Надежность (Robustness):** никакая коалиция участников или организаторов разумного размера не может сорвать процедуру голосования.
- ♦ **Атомарная проверяемость (Atomic verifiability):** отдельные участники могут убедиться, что их решения были подсчитаны должным образом.

- ♦ *Универсальная проверяемость (Universal verifiability)*: любой может проверить результаты подсчета.
 - ♦ *Отсутствие квитанций (Receipt-freeness)*: ни один участник не может составить квитанцию, подтверждающую содержание его бюллетеня.
 - ♦ *Декларируемость (Declarability)*: можно проверить, проголосовал ли конкретный участник.
 - ♦ *Непринуждаемость (Uncoercibility)*: невозможность злоумышленника определить, соответствует ли участник, подвергнутый принуждению, его требованиям.
 - ♦ *Изменения решения (Revisability)*: возможность изменения участником своего решения в течение периода голосования.
- К свойствам практичности относят:*
- ♦ *Гибкость (Flexibility)*: допускается множество форматов бюллетеней.
 - ♦ *Эффективность (Efficiency)*: процедура голосования использует разумное количество ресурсов.
 - ♦ *Мобильность (Mobility)*: участники могут принимать решение из любого места.
 - ♦ *Удобство (Convenience)*: процедура голосования состоит из одного раунда общения с организаторами.

Развитие протоколов электронного голосования началось в 1981 году с работы Дэвида Чаума [4], предложившего использование смешанных сетей (Mix-Nets) для обеспечения анонимности каналов связи. В 1992 году А. Фудзиока, Т. Окамото и К. Ота представили протокол [5] с использованием слепых цифровых подписей, что позволило эффективно разделить процессы регистрации и подачи голоса.

В последующие десятилетия научное сообщество активно разрабатывало альтернативные теоретические модели, направленные на решение узкоспециализированных задач. Так, схема MIZAN [6] стала одной из первых попыток реализовать свойство изменения решения в рамках традиционной PKI-инфраструктуры. С развитием технологий распределенного реестра появились протоколы на базе технологии блокчейн [7, 8], предлагающие децентрализованное хранение бюллетеней для повышения доверия к системе без единого администратора. Особое внимание уделяется защите от квантовых угроз: в частности, предлагаются усовершенствованные смешанные сети на основе криптографии на решетках [9]. Параллельно с разработкой архитектур развивается и теоретический базис: исследователи формализуют понятия проверяемости [10], создавая строгие критерии для оценки стойкости протоколов. В отечественной науке также существуют оригинальные подходы, например схема защищенного голосования с использованием «слепых посредников» [11].

В настоящее время системы ЭГ активно эксплуатируются на государственном уровне. Первой страной, внедрившей общенациональное интернет-голосование, стала Эстония в 2005 году [12]. В Российской Федерации технологии дистанционного электронного голосования (ДЭГ) применяются с 2019 года, а в 2024 году масштабно использовались в ходе выборов Президента РФ [13].

Несмотря на широкое распространение, значительная часть существующих протоколов обладает существенным ограничением: в таких системах изменение решения участником либо технически невозможно, либо требует сложной процедуры повторной аутентификации и аннулирования предыдущего бюллетеня, что снижает эффективность системы. При этом свойство изменения решения является критически важным для защиты от принуждения. Если протокол позволяет многократно перезаписывать голос, то участник, находящийся под давлением злоумышленника, может отдать требуемый голос, а затем, оказавшись в безопасности, изменить его на истинный. Отсутствие удобного механизма смены решения в существующих моделях является актуальной научной проблемой.

Отсутствие механизма простой процедуры изменения решения не учитывает специфику современных цифровых процедур. Во-первых, существенную роль играет временной фактор: электронные процедуры часто растянуты во времени и могут продолжаться несколько дней. За этот период внешние обстоятельства могут измениться, или

участник может получить новую существенную информацию, влияющую на его позицию. Во-вторых, нельзя исключать влияние человеческого фактора – участник может совершить случайную ошибку. В системе, не предусматривающей возможность коррективки решения, такая ошибка становится фатальной.

Целью данной работы является разработка модели протокола электронного голосования, обеспечивающего нативную возможность изменения решения участником без компрометации анонимности. В основе предлагаемой модели лежит семейство криптографических схем обязательства с потайным входом [14].

Следует отметить, что работа носит теоретический характер и посвящена построению алгоритмической модели взаимодействия участников. Предложенная архитектура является универсальной: выбор конкретных криптографических примитивов может варьироваться в зависимости от требований реализации, в том числе с учетом необходимости защиты от квантовых угроз.

Предварительные сведения. В данном разделе введем формальные определения криптографических примитивов, используемых для построения предлагаемой модели протокола.

Симметричная схема шифрования представляет собой набор алгоритмов, позволяющих двум сторонам, обладающим общим секретным ключом, обмениваться конфиденциальной информацией. В контексте отечественных стандартов в качестве базового примитива может использоваться блочный шифр «Кузнечик», регламентированный ГОСТ Р 34.12-2015 [15].

Формально симметричная криптосистема Π_{sym} определяется как кортеж из трех полиномиальных алгоритмов ($KeyGen, Enc, Dec$):

1. $KeyGen(1^\lambda) \rightarrow k$: алгоритм, который принимает на вход параметр безопасности λ и возвращает секретный ключ k .
2. $Enc(k, m) \rightarrow c$: алгоритм, который принимает на вход секретный ключ k и сообщение $m \in \mathcal{M}$ где $\mathcal{M}$ – пространство сообщений, и возвращает шифртекст c .
3. $Dec(k, c) \rightarrow m$: алгоритм, который принимает на вход секретный ключ k и шифртекст c . Он возвращает сообщение m или ошибку $\perp$, если шифртекст некорректен.

Для корректности схемы требуется, чтобы для любого ключа k , выработанного $KeyGen(1^\lambda)$, и любого сообщения $m \in \mathcal{M}$ выполнялось равенство:

$$Dec(k, Enc(k, m)) = m.$$

Асимметричные криптосистемы позволяют осуществлять шифрование и расшифрование данных с использованием пары математически связанных ключей: открытого и закрытого. Стойкость таких систем основывается на вычислительной сложности решения определенных математических задач. Классическим примером асимметричной криптосистемы шифрования является работа Ривеста, Шамира и Адельмана [16].

Формально асимметричная криптосистема Π_{asym} задается кортежем из трех алгоритмов ($KeyGen, Enc, Dec$):

1. $KeyGen(1^\lambda) \rightarrow (pk, sk)$: вероятностный алгоритм, который по параметру безопасности λ вырабатывает пару ключей: открытый ключ pk и закрытый ключ sk .
2. $Enc(pk, m) \rightarrow c$: вероятностный алгоритм, который принимает на вход открытый ключ pk и сообщение m , возвращая шифртекст c .
3. $Dec(sk, c) \rightarrow m$: детерминированный алгоритм, который использует закрытый ключ sk , и возвращает исходное сообщение m или ошибку $\perp$.

Условие корректности аналогично симметричному случаю: для любой пары ключей (pk, sk) и любого сообщения m :

$$Dec(sk, Enc(pk, m)) = m.$$

В предлагаемой модели асимметричное шифрование используется для обеспечения конфиденциальности каналов связи между участниками и серверами (например, при передаче бюллетеней через Mix-Nets), а также применяется при процедуре аутентификации сторон.

Проверяемая случайная функция (Verifiable Random Function, VRF) – это криптографический примитив, который позволяет владельцу секретного ключа вычислять псевдослучайное значение для заданного входного параметра и генерировать общедоступное доказательство корректности этого вычисления [17]. В контексте предлагаемой модели данный примитив используется для формирования анонимного бюллетеня с возможностью последующего аудита.

Формально схема VRF определяется как кортеж из трех полиномиальных алгоритмов ($VRF.keyGen, VRF.eval, VRF.verify$):

1. $VRF.keyGen(1^\lambda) \rightarrow (vpk, vsk)$. Вероятностный алгоритм, принимающий параметр безопасности λ и возвращающий пару ключей: открытый pk и закрытый sk .
2. $VRF.eval(vsk, m) \rightarrow (v, proof)$. алгоритм, состоящий из пары функций F_1 и F_2 , принимающий на вход сообщение m и закрытый ключ vsk . Алгоритм возвращает двоичные строки $v = F_1(vsk, m)$ и $proof = F_2(vsk, m)$.
3. $VRF.verify(vpk, m, v, proof) \rightarrow 1/0$: детерминированный алгоритм, принимающий открытый ключ vpk , сообщение m , псевдослучайное значение v и доказательство $proof$. Возвращает либо 1 (проверка успешна), либо 0 (проверка неуспешна).

Для криптосистемы VRF должны выполняться следующие свойства:

- ♦ *Корректность (Correctness)*: для любой пары ключей (vpk, vsk) и любого сообщения m , если $(v, proof) \leftarrow VRF.eval(vsk, m)$, то проверка $VRF.verify(vpk, m, v, proof)$ всегда возвращает 1.

- ♦ *Уникальная доказуемость (Unique Provability)*: для любого открытого ключа vpk и любого сообщения m вычислительно невозможно найти такие значения $v_1 \neq v_2$ и доказательства $proof_1, proof_2$, что $VRF.verify(vpk, m, v_1, proof_1) = 1$ и $VRF.verify(vpk, m, v_2, proof_2) = 1$.

- ♦ *Псевдослучайность (Pseudorandomness)*: для любого вероятностного полиномиального злоумышленника, не владеющего секретным ключом vsk , и для любого сообщения m , для которого злоумышленник не запрашивал значение $VRF.eval(vsk, m)$, выходное значение v вычислительно неотличимо от равномерно случайного значения.

Схема обязательств с потайным входом (Trapdoor Commitment, TC) – это криптосистема, являющаяся модификацией классической схемы обязательств, которая позволяет зафиксировать значение, а впоследствии изменить его при наличии секретного ключа, не меняя при этом самого обязательства [14].

Пусть $\mathcal{M}$ – пространство сообщений, $\mathcal{R}$ – пространство случайностей, $\mathcal{K}$ – пространство ключей и $\mathcal{C}$ – пространство обязательств.

Тогда схема обязательств с потайным входом TC определяется как кортеж из пяти полиномиальных алгоритмов:

1. $TC.parGen(1^\lambda) \rightarrow pp$: вероятностный алгоритм, принимающий на вход параметр безопасности λ и возвращающий набор открытых параметров pp .
2. $TC.keyGen(pp) \rightarrow (cpk, csk)$: алгоритм, принимающий параметры pp и возвращающий пару ключей: открытый ключ $cpk \in \mathcal{K}_{pk}$ и закрытый ключ $csk \in \mathcal{K}_{sk}$.
3. $TC.tCom(cpk, m) \rightarrow (c, r)$: алгоритм принимает открытый ключ cpk и сообщение $m \in \mathcal{M}$. Возвращает обязательство $c \in \mathcal{C}$ и случайность $r \in \mathcal{R}$.
4. $TC.tVer(cpk, c, m, r) \rightarrow 1/0$: детерминированный алгоритм, который проверяет соответствие обязательства c паре (m, r) . Возвращает 1, если $c = TC.tCom(cpk, m)$, и 0 в противном случае.
5. $TC.tOpen(csk, cpk, c, m') \rightarrow r'$: алгоритм принимает закрытый ключ csk , открытый ключ cpk , текущее обязательство c и новое сообщение $m' \in \mathcal{M}$ ($m' \neq m$). Алгоритм вычисляет и возвращает новое значение случайности $r' \in \mathcal{R}$, такое что проверка для нового сообщения проходит успешно:

$$TC.tVer(cpk, c, m', r') = 1.$$

Для схемы обязательств с потайным входом должны выполняться следующие свойства безопасности:

♦ *Соккрытие (Hiding)*: по значению обязательства c вычислительно невозможно извлечь информацию о сообщении m без знания r .

♦ *Связывание (Binding)*: для стороны, не владеющей секретным ключом csk , вычислительно трудно найти две различные пары (m, r) и (m', r') , соответствующие одному и тому же обязательству c .

Протокол Privacy Pass [18] представляет собой механизм аутентификации, который позволяет пользователю доказать право доступа к серверу без идентификации пользователя сервером. Кроме клиента (Client) и сервера (Origin) в данном протоколе также участвуют аттестатор (Attester) и издатель (Issuer). Аттестатор выполняет роль проверяющего, то есть он отвечает за аутентификацию клиента в системе. Далее, если аутентификация была пройдена успешно, то издатель и клиент совместно генерируют заданное количество токенов для клиента. Эти токены затем могут быть использованы клиентом для получения анонимного доступа к серверу. Следует отметить, что сервер, аттестатор и издатель могут быть одной сущностью.

В основе работы протокола лежит криптографический примитив, называемый забывчивой псевдослучайной функцией (Oblivious PseudoRandom Function, OPRF) [19]. Данный примитив выполняется двумя сторонами, назовем их отправитель и получатель, и позволяет им вычислить значение псевдослучайной функции от их секретных входных данных, таким образом, что получатель получает результат вычисления, не раскрывая своего входа, а отправитель не узнаёт вычисленного значения. Другими словами, пусть получатель имеет некоторое секретное значение X , отправитель секретное значение Y . В результате выполнения протокола получатель совместно с отправителем вычислит значение $z = \text{OPRF}(x, y)$. Использование OPRF в протоколе Privacy Pass позволяет реализовать механизм выдачи анонимных криптографических токенов, обеспечивающий невозможность связывания этапа их получения с последующим использованием при обращении к серверу.

Смешанные сети (Mix-Network, Mix-Net) представляют собой криптографический протокол, выполняемый набором mix -серверов, для обеспечения анонимности группы пользователей. Основная цель протокола заключается в разрыве связи между входящим и исходящим трафиком на каждом узле, делая невозможным для наблюдателя, не контролирующего все узлы сети, отследить, кто с кем общается [20–22].

Как правило, архитектура протокола предполагает последовательность независимых mix -серверов, совместно исполняющих протокол. Далее приводится краткое описание выполняемых шагов каждого из участников протокола.

Пусть n пользователей желают передать сообщения $m_1, \dots, m_n$ соответственно получателю (R) с помощью mix -серверов $\text{Mix}_1, \text{Mix}_2$:

1. Каждый пользователь с помощью открытого ключа R шифрует сообщение $c^{(i)} = \text{Enc}_R(m_i)$, а затем повторно шифрует $c^{(i)}$ с помощью открытых ключей mix -серверов $\text{Mix}_1, \text{Mix}_2$, вкладывая в отправляемые сообщения путь до следующего узла (add):

$$c_{\text{Mix}_2}^{(i)} = \text{Enc}_{\text{Mix}_2}(c^{(i)}, \text{add}_R),$$

$$c_{\text{Mix}_1}^{(i)} = \text{Enc}_{\text{Mix}_1}(c_{\text{Mix}_2}^{(i)}, \text{add}_{\text{Mix}_2}).$$

2. Каждый mix -сервер принимает список закрытых текстов от предыдущего узла, расшифровывает с помощью своего закрытого ключа, применяет секретную перестановку к порядку элементов и передает полученный результат следующему узлу или конечному получателю.

Таким образом, если хотя бы один сервер в цепочке честно выполняет перестановку и не хранит логи соответствия входов и выходов, анонимность участников сохраняется.

Предлагаемое решение. В данной работе предлагается теоретическая модель протокола электронного голосования с возможностью изменения решения участника до момента окончания голосования (E-Voting with Vote Changing, EVVC). Главной особенностью данного протокола является то, что каждый участник имеет возможность произвольное количество раз изменять свое решение в течение периода голосования, но при этом в итоговом подсчёте учитывается только его последнее решение.

Важно подчеркнуть, что представленная схема является алгоритмической моделью взаимодействия сторон и описывает логику работы протокола, абстрагируясь от конкретных программно-аппаратных реализаций.

В схеме принимают участие следующие субъекты:

1. *Участник (User)*: пользователь системы, обладающий правом принятия решения, и желающий его зафиксировать.
2. *Центр регистрации (Registration Center, RC)*: узел системы, проводящий аутентификацию участников и выдающий права на участие (бюллетени/тикеты) валидным пользователям.
3. *Центр подсчета (Counting Center, CC)*: узел системы, проводящий сбор зашифрованных решений, их проверку, подсчёт и публикацию итоговых результатов.
4. *Смешанные сети (Mix-Nets)*: промежуточные узлы, осуществляющие анонимизацию участников при передаче сообщений центру подсчета.

Основное преимущество предлагаемой модели перед современными аналогами заключается в том, что участник может изменить свое решение без повторного обращения к организаторам (Центру регистрации). Другим преимуществом является минимизация количества взаимодействий между сторонами протокола.

Ниже представлено формальное описание необходимых алгоритмов и протоколов:

♦ $RC.setup(1^\lambda) \triangleq VRF.keyGen(1^\lambda) \rightarrow (vsk, vpk)$ (Центр регистрации): алгоритм вырабатывает ключевую пару центра регистрации (закрытый vsk и открытый vpk ключи для VRF).

♦ $User.setup(1^\lambda) \triangleq TC.parGen(1^\lambda) \rightarrow pp \& TC.keyGen(pp) \rightarrow (cpk, csk)$ (Участник): Алгоритм вырабатывает параметры схемы обязательств и ключевую пару участника (открытый cpk и закрытый csk ключи).

♦ $User.decide(decision, cpk) \triangleq TC.tCom(decision, cpk) \rightarrow (C_{decision}, r)$ (Участник): данный алгоритм принимает на вход решение участника $decision$ и его открытый ключ cpk , а на выходе возвращает обязательство $C_{decision}$, которое фиксирует выбор участника, и некоторое случайное число r .

♦ $UserRC.PrivacyPass(ID) \rightarrow token$ (Участник $\leftrightarrow$ Центр регистрации): данный интерактивный протокол основан на механизме Privacy Pass и предназначен для анонимного подтверждения права участника на получение бюллетеня без раскрытия его личности центру подсчёта и внешним наблюдателям. В рамках протокола участник проходит предварительную проверку, подтверждающую его право на участие в голосовании, после чего получает криптографический токен $token$, удостоверяющий это право. Центр регистрации обеспечивает, что каждому участнику может быть выдано не более одного такого токена, при этом полученный токен не содержит информации, позволяющей связать его с личностью участника при последующем использовании.

♦ $UserRC.TicketReceive(cpk \parallel C_{decision}, token) \rightarrow (ticket, proof)$ (Участник $\leftrightarrow$ Центр регистрации): данный интерактивный протокол отвечает за создание подтвержденного бюллетеня (тикета). Используя ранее полученный анонимный токен $token$, участник передаёт центру регистрации свой псевдоним (открытый ключ cpk) и замаскированное решение (обязательство $C_{decision}$). Центр регистрации, верифицировав токен, формирует индивидуальный тикет с помощью алгоритма проверяемой случайной функции:

$$VRF.eval(vsk, cpk \parallel C_{decision}) \rightarrow (ticket, proof).$$

После этого центр регистрации возвращает полученный тикет $ticket$ и доказательство $proof$ обратно через анонимный канал:

♦ $UserCC.SendTicket(ticket, proof, C_{decision}, cpk)$ (Участник $\rightarrow$ Центр подсчета): данный протокол при помощи Mix-Nets передает информацию о решении участника (набор данных $m = \{ticket, proof, C_{decision}, cpk\}$ центру подсчета, скрывая личность отправителя.

♦ $CC.TicketVerify(vpk, C_{decision} \parallel cpk, ticket, proof) \triangleq VRF.verify(vpk, C_{decision} \parallel cpk, ticket, proof) \rightarrow 1/0$ (Центр подсчета): данный алгоритм отвечает за проверку входящих данных на подлинность. Для этого на вход центр

подсчета принимает набор $\{ticket, proof, C_{decision}, cpk, vpk\}$ и возвращает 1 (данные подлинны) или 0. Далее в открытый доступ публикуются $ticket, proof, cpk$ и $C_{decision}$, чтобы каждый мог проверить их правильность.

♦ $User.DecisionChange(csk, cpk, C_{decision}, decision') \triangleq$

$TC.tOpen(csk, cpk, C_{decision}, decision') \rightarrow r'$ (Участник): при желании участник имеет возможность изменить свое решение $decision$. Если данный протокол не применялся, то $decision' = decision$ и $r' = r$. Если же изменение необходимо, участник использует свой секретный ключ csk для вычисления новой случайности r' для нового решения $decision'$, соответствующей старому обязательству $C_{decision}$.

♦ $UserCC.DecisionReveal(r', decision', ticket)$ (Участник $\rightarrow$ Центр подсчета): данный протокол при помощи Mix-Network передает информацию для раскрытия решения $m = \{r', decision', ticket\}$ центру подсчета, скрывая личность участника.

♦ $CC.Reveal(r', decision', ticket, cpk, C_{decision}) \rightarrow 1/0$ (Центр подсчета): центр подсчета ищет по уникальному значению $ticket$ соответствующие ему данные $\{C_{decision}, cpk\}$ и проверяет, что решение валидно при помощи алгоритма:

$$TC.tVer(cpk, C_{decision}, decision', r') \rightarrow 1/0.$$

Центр подсчитывает все полученные решения и публикует результаты $\{r', decision', ticket, cpk, C_{decision}\}$, чтобы любой желающий мог их проверить.

♦ $Verify(cpk, C_{decision}, decision', r') = TC.tVer(cpk, C_{decision}, decision', r') \rightarrow 1/0$ (Любой желающий): данный алгоритм позволяет любому внешнему наблюдателю проверить честность и правильность учета решений на основе опубликованных данных.

Для протокола EVVC должны выполняться следующие свойства:

1. Полнота (Completeness): все действительные решения участников подсчитываются правильно.
2. Устойчивость (Soundness): недействительные решения участников не учитываются.
3. Конфиденциальность участника (Voter's Privacy): решение отдельного участника хранится в тайне.
4. Одноразовость (Unreusability): решение каждого участника учитывается единожды.
5. Приемлемость (Eligibility): принимать участие могут только те, кому разрешено голосовать.
6. Справедливость (Fairness): ничто не должно влиять на голосование, т. е. никакие промежуточные результаты никому не могут быть известны.
7. Проверяемость (Verifiability): никто не может фальсифицировать результаты голосования.
8. Атомарная проверяемость (Atomic verifiability): отдельные участники могут убедиться, что их решения были подсчитаны должным образом
9. Универсальная проверяемость (Universal verifiability): любой может проверить результаты подсчета.
10. Изменение решения (Revisability): возможность изменения участником своего решения в течение периода голосования.

Стойкость предлагаемой модели. В данном разделе мы приводим краткое обоснование стойкости предлагаемого решения, в котором намечаем основные пути доказательства свойств. Пусть все используемые криптографические примитивы (VRF, Trapdoor Commitment, Privacy Pass, Mix-Nets и алгоритмы шифрования) являются криптографически стойкими. Также предполагается модель нарушителя, в которой Центр подсчета (CC) и Центр регистрации (RC) не вступают в сговор и не могут обмениваться закрытой информацией друг с другом.

Далее покажем, что при выполнении данных допущений для протокола выполняются все заявленные свойства безопасности:

Полнота (Completeness). Данное свойство выполняется, так как алгоритмы $CC.TicketVerify$ и $CC.Reveal$ публикуют информацию в открытом доступе (на публичной доске). Каждый желающий может проверить наличие своего уникального тикета, а также провести независимую проверку правильности подсчета с помощью алгоритма $Verify(TC.tVer)$.

Устойчивость (Soundness). Выполнение свойства гарантируется корректностью используемой схемы обязательств с потайным входом. Если на вход проверки будут поданы некорректные параметры r' , $decision'$ или cpk , протокол при проверке соответствия обязательству $C_{decision}$ выдаст ошибку. Таким образом, недействительные решения технически не могут быть учтены в итоговом результате.

Конфиденциальность пользователя (User's Privacy). Данное свойство обеспечивается свойством «сокрытия» (hiding) схемы обязательств с потайным входом: сторона, знающая обязательство $C_{decision}$, не может извлечь из него информацию о решении $decision$. Анонимность личности пользователя гарантируется использованием протокола Privacy Pass при взаимодействии с Центром регистрации (разрыв связи ID-токен) и использованием Mix-Nets при взаимодействии с Центром подсчета (разрыв связи IP-сообщение).

Одноразовость (Unreusability). Свойство выполняется за счет того, что на этапе аутентификации Центр регистрации при помощи протокола $User \leftrightarrow RC.PrivacyPass$ фиксирует факт выдачи токена для каждого идентификатора ID . Пользователь технически не может получить валидный токен повторно и, следовательно, не может отправить более одного учитываемого голоса (даже если он меняет решение, учитывается только последняя валидная пара).

Приемлемость (Eligibility). Выполняется, так как каждому пользователю необходимо пройти строгую аутентификацию (проверку права на участие) перед получением токена. Проверка осуществляется Центром регистрации в момент выполнения протокола $PrivacyPass$.

Справедливость (Fairness). Свойство обеспечивается стойкостью используемых примитивов. Никакой злоумышленник (включая организаторов), обладающий современными вычислительными мощностями, не может узнать содержание решений до момента их официального раскрытия (публикации ключей раскрытия или самих значений), что исключает влияние промежуточных итогов на мнение пользователей.

Проверяемость (Verifiability). Свойство выполняется при предположении об отсутствии сговора между RC и CC. Центр регистрации не может сгенерировать больше валидных тикетов, чем реальных пользователей (так как $PrivacyPass$ требует взаимодействия), а Центр подсчета публикует все полученные данные $\{ticket, proof, C_{decision}, cpk\}$ в открытом доступе. Стойкость VRF гарантирует, что тикеты не могут быть подделаны.

Атомарная проверяемость (Atomic verifiability). После завершения процедуры Центр подсчета публикует полный набор данных $\{decision', r', cpk, C_{decision}, ticket\}$. Любой пользователь может найти свой тикет на «доске» и криптографически убедиться, что его решение учтено верно.

Универсальная проверяемость (Universal verifiability). Поскольку все данные $\{decision', r', cpk, C_{decision}, ticket\}$ для всех пользователей публикуются открыто, любой внешний наблюдатель может перепроверить математическую корректность каждого голоса и итоговой суммы.

Возможность изменения решения (Revisability). Пользователь, зная свой секретный ключ csk , может изменить решение $decision$ на $decision'$ даже после отправки обязательства. С помощью алгоритма $TC.tOpen(csk, cpk, C_{decision}, decision') \rightarrow r'$ он вычисляет новую случайность r' , которая делает новое решение валидным для старого обязательства $C_{decision}$. Центр подсчета примет это обновление, проверив его через $TC.tVer$, и учтет последнее пришедшее валидное сообщение.

Таким образом, проведенный анализ показывает, что предлагаемая модель EVVC удовлетворяет всем ключевым требованиям, предъявляемым к защищенным системам электронного голосования. Использование комбинации криптографических примитивов (VRF, Trapdoor Commitment, Privacy Pass и Mix-nets) позволяет достичь баланса между строгой анонимностью участников и прозрачностью процесса подсчета (универсальной проверяемостью). При этом, в отличие от большинства классических подходов, модель успешно реализует свойство изменения решения, обеспечивая пользователю гибкость в принятии решений и дополнительную защиту от внешнего давления.

Заключение. В данной работе была разработана и формально описана теоретическая модель протокола электронного голосования, отличительной особенностью которой является свойство изменения решения участником. Предложенная архитектура позволяет пользователю многократно изменять свое решение в течение отведенного времени без необходимости повторного прохождения процедуры аутентификации или взаимодействия с администраторами системы, что существенно повышает удобство использования.

Проведенный анализ стойкости показал, что модель удовлетворяет всем критически важным требованиям, предъявляемым к системам электронного голосования, включая полную анонимность пользователей, невозможность фальсификации результатов, а также обеспечивая универсальную проверяемость итогов любым внешним наблюдателем.

Предложенная модель характеризуется криптографической гибкостью. Благодаря модульной архитектуре в качестве базовых «строительных блоков» протокола могут быть использованы как классические, так и постквантовые криптографические примитивы без изменения общей логики взаимодействия сторон. Переход к использованию постквантовых криптографических стандартов позволит гарантировать неизменность и тайну принятых решений даже при появлении полномасштабных квантовых компьютеров.

Работа выполнена в рамках государственного задания (проект FSER-2025-0003).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Lee B., Kim K. Receipt-free electronic voting scheme with a tamper-resistant randomizer // International conference on information security and cryptology. – Berlin, Heidelberg: Springer Berlin Heidelberg, 2002. – P. 389-406.
2. Gritzalis D.A. Principles and requirements for a secure e-voting system // Computers & Security. – 2002. – Vol. 21, No. 6. – P. 539-556.
3. Sampigethaya K., Poovendran R. A survey on mix networks and their secure applications // Proceedings of the IEEE. – 2006. – Vol. 94, No. 12. – P. 2142-2181.
4. Chaum D.L. Untraceable electronic mail, return addresses, and digital pseudonyms // Communications of the ACM. – 1981. – Vol. 24, No. 2. – P. 84-90.
5. Fujioka A., Okamoto T., Ohta K. A Practical Secret Voting Scheme for Large Scale Elections // Advances in Cryptology – AUSCRYPT '92. LNCS. Vol. 718. – Springer, 1993. – P. 244-251.
6. Mohammadi M. K., Yaghoobi M. MIZAN: A secure E-voting schema with vote changeability // 2010 International Conference on Information Society. – IEEE, 2010. – P. 1-5.
7. Maddaloni F. Voting Verification Mechanism for a Distributed Ledger-based Remote Electronic Voting System. – University of Zurich, 2021.
8. Yi L., Wang Q. An E-voting Protocol Based on Blockchain // IACR Cryptology ePrint Archive. – 2022. – Report 2022/1132.
9. Farzaliyev V., Willemson J., Kaasik J. K. Improved Lattice-Based Mix-Nets for Electronic Voting // IET Information Security. – 2022. – Vol. 16, Issue 6. – P. 423-438.
10. Cortier V., Galindo D., Küsters R., Truderung T. SoK: Verifiability Notions for E-Voting Protocols // 2016 IEEE Symposium on Security and Privacy (SP). – IEEE, 2016. – P. 779-798.
11. Бабенко Л.К., Писарев И.А., Макаревич О.Б. Защищенное электронное голосование с использованием слепых посредников // Известия ЮФУ. Технические науки. – 2017. – № 6 (191). – С. 26-36.
12. Heiberg S., Willemson J. Verifiable internet voting in Estonia // 2014 IEEE 2nd International Workshop on Security and Privacy in Big Data (BigSecurity). – IEEE, 2014. – P. 1-8.
13. Федеральный закон от 12.06.2002 № 67-ФЗ (ред. от 23.05.2025) «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации».
14. Беззатеев С.В., Давыдов В.В., Дакуо Ж.Н., Иогансон И.Д., Хуцаева А.Ф. Постквантовая схема обязательств с потайным входом // Прикладная дискретная математика. Приложение. – 2025. – № 18. – С. 226-229.
15. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – Введ. 2016-01-01. – М.: Стандартинформ, 2015.
16. Rivest R.L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems // Communications of the ACM. – 1978. – Vol. 21, No. 2. – P. 120-126.
17. Дакуо Ж.Н. WaveVRF: постквантовая проверяемая псевдослучайная функция, основанная на кодах, исправляющих ошибки // Научно-технический вестник информационных технологий, механики и оптики. – 2025. – Т. 25, № 1. – С. 174-177.

18. Davidson A., et al. Privacy Pass: Bypassing Internet Challenges Anonymously // *Proceedings on Privacy Enhancing Technologies*. – 2018.
19. Jarecki S., Kiayias A., Krawczyk H. Round-optimal password-protected secret sharing and TPAKE in the password-only model. In: P. Sarkar, T. Iwata (eds.) // *ASIACRYPT 2014, Part II, LNCS*. Vol. 8874. – P. 233-253. – Springer, Heidelberg, December 2014.
20. Sampigethaya K., Poovendran R. A survey on mix networks and their secure applications // *Proceedings of the IEEE*. – 2007. – Vol. 94, No. 12. – P. 2142-2181.
21. Furukawa J., Mori K., Sako K. An implementation of a mix-net based network voting scheme and its use in a private organization // *Towards Trustworthy Elections: New Directions in Electronic Voting*. – Springer, 2010. – P. 141-154.
22. Oluranti J., Olajide F., Ayo C. Network forensics tools in a mixed-network environment and the adoption of e-voting system in developing countries // *International Journal of Pharmacy and Technology*. – 2016. – Vol. 8, No. 4. – P. 23115-23118.

REFERENCES

1. Lee B., Kim K. Receipt-free electronic voting scheme with a tamper-resistant randomizer, *International conference on information security and cryptology*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 389-406.
2. Gritzalis D.A. Principles and requirements for a secure e-voting system, *Computers & Security*, 2002, Vol. 21, No. 6, pp. 539-556.
3. Sampigethaya K., Poovendran R. A survey on mix networks and their secure applications, *Proceedings of the IEEE*, 2006, Vol. 94, No. 12, pp. 2142-2181.
4. Chaum D.L. Untraceable electronic mail, return addresses, and digital pseudonyms, *Communications of the ACM*, 1981, Vol. 24, No. 2, pp. 84-90.
5. Fujioka A., Okamoto T., Ohta K. A Practical Secret Voting Scheme for Large Scale Elections, *Advances in Cryptology – AUSCRYPT '92. LNCS*. Vol. 718. Springer, 1993, pp. 244-251.
6. Mohammadi M. K., Yaghoobi M. MIZAN: A secure E-voting schema with vote changeability, *2010 International Conference on Information Society*. IEEE, 2010, pp. 1-5.
7. Maddaloni F. Voting Verification Mechanism for a Distributed Ledger-based Remote Electronic Voting System. University of Zurich, 2021.
8. Yi L., Wang Q. An E-voting Protocol Based on Blockchain, *IACR Cryptology ePrint Archive*, 2022, Report 2022/1132.
9. Farzaliyev V., Willemson J., Kaasik J. K. Improved Lattice-Based Mix-Nets for Electronic Voting, *IET Information Security*, 2022, Vol. 16, Issue 6, pp. 423-438.
10. Cortier V., Galindo D., Küsters R., Truderung T. SoK: Verifiability Notions for E-Voting Protocols, *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2016, pp. 779-798.
11. Babenko L.K., Pisarev I.A., Makarevich O.B. Zashchishchennoe elektronnoe golosovanie s ispol'zovaniem slepykh posrednikov [Secure electronic voting using blind intermediaries], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2017, No. 6 (191), pp. 26-36.
12. Heiberg S., Willemson J. Verifiable internet voting in Estonia, *2014 IEEE 2nd International Workshop on Security and Privacy in Big Data (BigSecurity)*. IEEE, 2014, pp. 1-8.
13. Federal'nyy zakon ot 12.06.2002 № 67-FZ (red. ot 23.05.2025) «Ob osnovnykh garantiyakh izbiratel'nykh prav i prava na uchastie v referendumе grazhdan Rossiyskoy Federatsii» [13. Federal Law of 12.06.2002 No. 67-FZ (as amended on 23.05.2025) “On the Basic Guarantees of Electoral Rights and the Right to Participate in Referendums of Citizens of the Russian Federation”].
14. Bezzateev S.V., Davydov V.V., Dakuo Zh.N., Ioganson I.D., Khutsaeva A.F. Postkvantovaya skhema obyazatel'stv s potaynym vkhodom [Post-quantum commitment scheme with a trapdoor], *Prikladnaya diskretnaya matematika. Prilozhenie* [Applied Discrete Mathematics. Supplement], 2025, No. 18, pp. 226-229.
15. GOST R 34.12-2015. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Blochnye shifry [GOST R 34.12-2015. Information technology. Cryptographic protection of information. Block ciphers]. Introduced 2016-01-01. Moscow: Standartinform, 2015.
16. Rivest R.L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, 1978, Vol. 21, No. 2, pp. 120-126.
17. Dakuo Zh.N. WaveVRF: postkvantovaya proverayemaya psevdosluchaynaya funktsiya, osnovannaya na kodakh, ispravlyayushchikh oshibki [WaveVRF: Post-quantum verifiable pseudorandom function based on error-correcting codes], *Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki* [Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics], 2025, Vol. 25, No. 1, pp. 174-177.
18. Davidson A., et al. Privacy Pass: Bypassing Internet Challenges Anonymously, *Proceedings on Privacy Enhancing Technologies*, 2018.

19. Jarecki S., Kiayias A., Krawczyk H. Round-optimal password-protected secret sharing and TPAKE in the password-only model, In: P. Sarkar, T. Iwata (eds.), *ASIACRYPT 2014, Part II, LNCS. Vol. 8874*, pp. 233-253. Springer, Heidelberg, December 2014.
20. Sampigethaya K., Poovendran R. A survey on mix networks and their secure applications, *Proceedings of the IEEE*, 2007, Vol. 94, No. 12, pp. 2142-2181.
21. Furukawa J., Mori K., Sako K. An implementation of a mix-net based network voting scheme and its use in a private organization, *Towards Trustworthy Elections: New Directions in Electronic Voting*. Springer, 2010, pp. 141-154.
22. Oluranti J., Olajide F., Ayo C. Network forensics tools in a mixed-network environment and the adoption of e-voting system in developing countries, *International Journal of Pharmacy and Technology*, 2016, Vol. 8, No. 4, pp. 23115-23118.

Дакуо Жан-Мишель Никодэмович – Национальный исследовательский университет ИТМО; e-mail: jeandakuo@mail.ru; г. Санкт-Петербург, Россия; тел.: +79217863122; факультет безопасности информационных технологий; аспирант.

Беззатеев Сергей Валентинович – Государственный университет аэрокосмического приборостроения; e-mail: bsv@guar.ru; г. Санкт-Петербург, Россия; тел.: +79045170951; кафедра информационной безопасности; зав. кафедрой.

Давыдов Вадим Валерьевич – ООО «КуАпп»; e-mail: vadimdavydov@outlook.com; г. Москва, Россия; криптограф-исследователь.

Иогансон Иван Дмитриевич – Национальный исследовательский университет ИТМО; e-mail: ivan.ioganson@yandex.ru; г. Санкт-Петербург, Россия; тел.: +79052278519; факультет безопасности информационных технологий; м.н.с.

Хуцаева Алтана Феликсовна – Государственный университет аэрокосмического приборостроения; e-mail: afkhutsaeva@itmo.ru; г. Санкт-Петербург, Россия; кафедра информационной безопасности; ассистент.

Dakuo Zhan-Mishel Nikodemovich – ITMO University; e-mail: jeandakuo@mail.ru; St. Petersburg, Russia; phone: +79217863122; Faculty of Secure Information Technologies; graduate student.

Bezzateev Sergey Valentinovich – State University of Aerospace Instrumentation; e-mail: bsv@guar.ru; St. Petersburg, Russia; phone: +79045170951; the Department of Information Security; head of the Department.

Davydov Vadim Valerievich – QApp LLC, Cryptographer-Researcher; e-mail: vadimdavydov@outlook.com; Moscow, Russia; cryptographer researcher.

Ioganson Ivan Dmitrievich – ITMO University; e-mail: ivan.ioganson@yandex.ru; St. Petersburg, Russia; phone: +79052278519; Faculty of Secure Information Technologies; junior scientific researcher.

Khutsaeva Altana Felixovna – State University of Aerospace Instrumentation; e-mail: afkhutsaeva@itmo.ru; St. Petersburg, Russia; the Department of Information Security; assistant.

УДК 681.5

DOI 10.18522/2311-3103-2026-4-212-226

А.Н. Каркищенко

КОЛИЧЕСТВЕННЫЕ ОЦЕНКИ ПОГРЕШНОСТИ ПОДДЕРЖАНИЯ СТРОЯ ПОДВОДНЫХ АППАРАТОВ ПРИ ЗАДЕРЖКАХ НАВИГАЦИОННЫХ ДАННЫХ

Изучается влияние задержек в получении навигационной информации на поддержание строя подводных аппаратов в режиме «лидер-ведомые». Исследование опирается на предположение о градиентном принципе управления строем в процессе движения. Сложность задачи обусловлена неизвестностью траектории лидера, неполным знанием и нестационарностью среды, ошибками измерений. Полученные результаты не зависят от конфигурации аппаратов в строю. Показано, что достаточно исследовать влияние навигационных задержек на движение одного аппарата. Основные предположения: траектория движения лидера неизвестна; все взаимодействия между лидером и ведомыми аппаратами синхронизированы; лидер с определенной частотой передает свои координаты другим аппаратам; смещения ведомого аппарата от его места в строю могут