# Отчет

по курсовой работе

**«Протокол тайного голосования на основе подписи “вслепую”»**

по предмету «Криптографические средства защиты информации»

Выполнил: Фёдоров Д.Ю.

Санкт-Петербург
2007 г.

## Традиционные системы голосования

Большинство традиционных систем голосования еще далеки от идеала. Эти системы, как правило, реализуемы, поскольку большая часть доверенных участников либо надежные, либо мало доверяют друг другу [1].

Большие профессиональные, общественные и специализированные организации, как правило, проводят свои выборы путем подсчета голосов. Эти системы позволяют избирателям отдать свои голоса практически из любой удаленной точки, но они, зачастую жертвуют точностью и конфиденциальностью. Этот метод работает, так как организации, которые используют эту систему, как правило, не проводят спорных выборов. Кроме того, они часто нанимают незаинтересованную сторону, чтобы заниматься этими выборами.

Многие штаты на некоторых выборах используют почтовое голосование, особенно на малых участках. Обычно избиратели просят предоставить свои бюллетени в двойных конвертах в целях защиты их частной жизни. Пожалуй, на сегодняшний день самая крупная организация, использующая почтовое голосование, это Teamsters. В 1988 Teamsters отправили почтовые бюллетени к 1,5 млн. своих участников. Согласно руководителям Teamsters, было лишь несколько попыток проголосовать несколько раз или запугать избирателей. Тем не менее, многие люди до сих пор скептически относятся к безопасности почтового голосования. В Верховных судах Калифорнии и Канзаса решали дела [8], касающиеся почтового голосования. В обоих случаях суды отказались отменять законы, разрешающие почтовое голосование, несмотря на признание судом Канзаса, что “голосование по почте, увеличивает вероятность компрометации секретности и возможностей для мошенничества”.

Большинство традиционных выборных систем могут быть проверены только представителями партий или третьей доверенной стороной. Как правило, избирателям невозможно проверить, что отдельные голоса были подсчитаны правильно. Кроме того, хотя процесс проверки часто может выявлять процедурные проблемы и большие расхождения между окончательным подсчетом и количеством избирателей, посетивших избирательные участки, как правило, не может исправить ошибки.

## Криптографические протоколы голосования

В 1981 году Чаумом впервые опубликован криптографический протокол голосования, документ по анонимной электронной почте и цифровым псевдонимам [3]. Этот протокол использует криптографию с открытым ключом и списки цифровых псевдонимов, скрывающих личность избирателей. Однако протокол не гарантирует того, что личность избирателей, не будет установлена. Позже Чаум предложил протокол, который безоговорочно скрывает личность избирателей [5]. Однако выборы, проведенные по этому протоколу, может быть нарушены одним избирателем. Хотя протокол Чаума позволяет обнаруживать такие нарушения, он не сможет восстановиться без повторного запуска всех выборов в целом [11].

В 1985 году Коэн (он же Benaloh) и Фишер (Fischer) опубликовали описание схемы безопасных выборов, в которой очень трудно смошенничать и сорвать выборы [7]. Однако эта схема не защищает личность граждан от руководителей выборами. Позже Коэн

представил расширение для этой схемы, в которой полномочия правительства были распределены [6]. Однако, в предложенном протоколе, из-за большой сложности коммуникационной схемы, подсчет голосов может занять недопустимо много времени [12].

Были предложены и ряд других криптографических схем, которые требуют взаимодействия между избирателями. Эти схемы, в том числе [9], могут оказаться полезными в зале заседаний, но также не подходят для крупномасштабных выборов.

**Безопасные выборы**

Компьютерное голосование никогда не будет использовано для обычных выборов, пока не появится протокол, который одновременно предохраняет от мошенничества и защищает тайну личности. Идеальный протокол должен обладать, по меньшей мере, следующими шестью свойствами [2]:

1. Голосовать могут только те, кто имеет на это право.
2. Каждый может голосовать не более одного раза.
3. Никто не может узнать, за кого проголосовал конкретный избиратель.
4. Никто не может проголосовать вместо другого.
5. Никто не может тайно изменить чей-то голос.
6. Каждый голосующий может проверить, что его голос учитывался при подведении итогов голосования.
7. Каждый знает, кто голосовал, а кто нет.

Прежде чем описывать сложные протоколы, имеющие приведенные характеристики, рассмотрим ряд простых протоколов.

**Упрощенный протокол голосования №1**

1. Каждый голосующий шифрует свой бюллетень открытым ключом ЦИК (Центральной избирательной комиссии).
2. Каждый голосующий посылает свой бюллетень в ЦИК.
3. ЦИК расшифровывает бюллетени, подводит итоги и опубликовывает результаты голосования.

Недостатки протокола:

- ЦИК не может узнать, откуда получены бюллетени, и даже, принадлежат ли присланные бюллетени правомочным избирателям.
- у ЦИК нет ни малейшего представления о том, не голосовали ли правомочные избиратели больше одного раза.

**Упрощенный протокол голосования №2**

1. Каждый голосующий подписывает свой бюллетень своим закрытым ключом.
2. Каждый голосующий шифрует свой бюллетень открытым ключом ЦИК.
3. Каждый голосующий посылает свой бюллетень в ЦИК.
4. ЦИК расшифровывает бюллетени, проверяет подписи и опубликовывает результаты голосования.

Возможности протокола:

Этот протокол обладает свойствами 1 и 2: только правомочные избиратели могут голосовать, и никто не может голосовать более одного раза – ЦИК может записывать бюллетени, полученные на этапе 3. Каждый бюллетень подписан закрытым ключом голосующего, поэтому ЦИК знает, кто голосовал, а кто нет и, как голосовал каждый избиратель. Если получен бюллетень, который не подписан правомочным пользователем, или бюллетень, подписанный избирателем, который уже проголосовал, то такой бюллетень игнорируется комиссией. Кроме того, из-за цифровой подписи никто не может изменить бюллетень другого избирателя, даже если сумеет перехватить его на этапе 2.

Недостатки протокола:

Подпись добавляется к бюллетеню, ЦИК знает, кто за кого голосовал, поэтому приходится полностью доверять ЦИК.

Следующие примеры показывают, как трудно обеспечить хотя бы первые три требования к протоколу безопасного голосования.

**Протоколы двух агентств**

Нурми, Салома и Сантин (Nurmi, Salomaa, Santean) [4] предложили подход, который решает множество проблем, упомянутых выше. В "Протоколе двух агентств", изображенном на Рисунке 1, электронное Центральное управление регистрации, далее ЦУР, (англ. validator) распределяет секретную опознавательную метку (англ. tag) каждому избирателю до голосования. Затем ЦУР отправляет в ЦИК (англ. tallier) список всех опознавательных меток, с отсутствующими записями об избирателях. Каждый избиратель отправляет в ЦИК его или ее опознавательную метку и зашифрованный файл, содержащий копию метки и бюллетень голосования. В этот момент ЦИК может удостовериться в надежности опознавательной метки, но программа не имеет возможности для изучения содержимого бюллетеня. ЦИК публикует зашифрованный файл (для того, чтобы голосующий мог проверить, что файл подан на рассмотрение), и избиратель отвечает ЦИК отправкой необходимого для дешифрования ключа. На этом голосование заканчивается, ЦИК публикует список всех бюллетеней и соответствующих зашифрованных файлов. В этот момент избиратели могут проверить, что их голоса были учтены должным образом. Любой избиратель, который обнаружит ошибку, может подать апелляцию, продемонстрировав снова зашифрованный файл и ключ дешифрования. Так как зашифрованный файл публиковался ранее, ЦИК не может отрицать факт его получения [10].

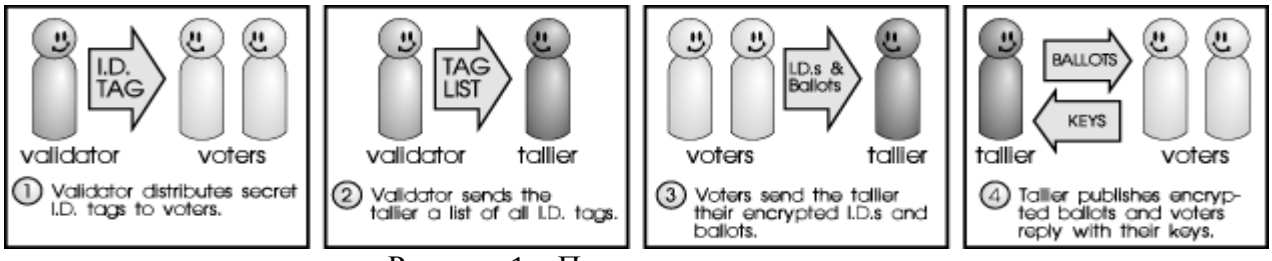


Рисунок 1 – Протокол двух агентств

Протокол двух агентств поддается контролю со стороны отдельных избирателей (в отличие от простого протокола, обсуждаемого ранее), тем не менее, он обладает некоторыми

проблемами. Наиболее важная состоит в не обеспечении конфиденциальности избирателей, если ЦИК и ЦУР вступят в тайный сговор. Поэтому, авторы уточняют, что, если два агентства работают совместно, тогда полномочия будут аналогичны одному агентству.

**Протоколы на основе подписи вслепую**

Когда Дэвид Чаум (David Chaum) впервые представил концепцию подписи вслепую в 1982 году он предположил, что ею можно воспользоваться для проведения тайного голосования и выборов. Десять лет спустя, Фудзиока, Окамото и Охта (Fujioka, Okamoto, Ohta) разработали практическую схему голосования, которая, используя подпись вслепую, разрешила проблему сговора в протоколах, подобную Протоколу Двух Агентств (Two Agency Protocol) без существенного увеличения общей сложности протокола (также были предложены ряд других, менее удачных, протоколов подписи вслепую).

В протоколе Фудзиока, Окамото и Охта, как показано на Рисунке 2, избиратели подготавливают бюллетень для голосования, шифруют его секретным ключом и маскируют (ослепляют). Затем избиратели подписывают бюллетень и отправляют его в ЦУР. ЦУР проверяет, что подпись принадлежит зарегистрированному избирателю, который еще не голосовали. Если бюллетень действительный, то ЦУР подписывает его и возвращает обратно избирателю. Избиратель удаляет слой ослепляющего шифрования, раскрывая зашифрованный бюллетень подписанный ЦУР.

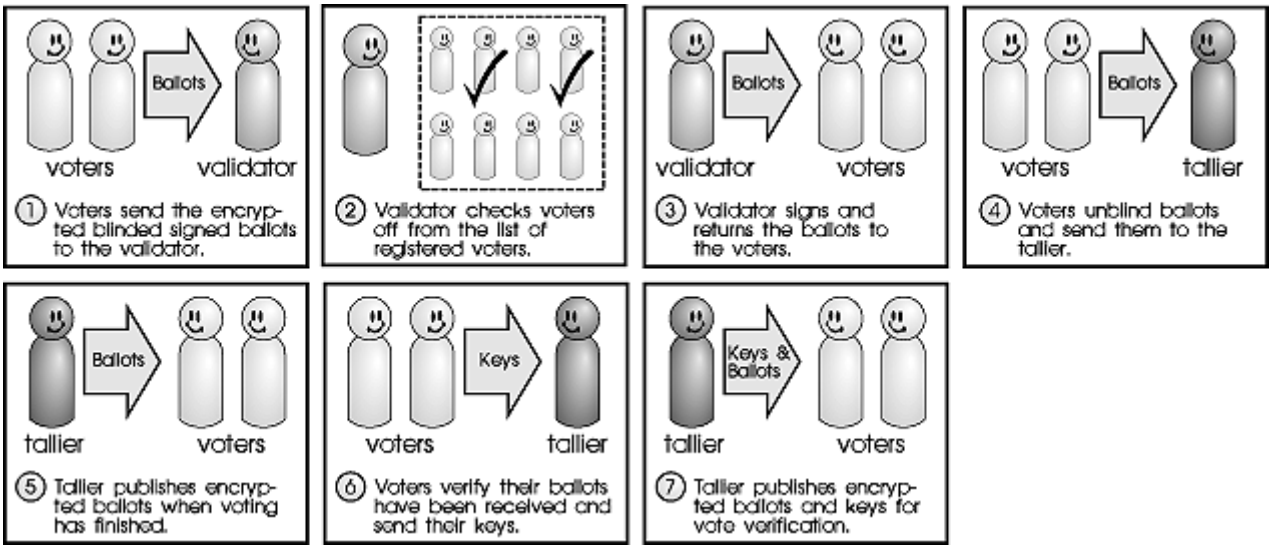


Рисунок 2 – Протокол Фудзиока, Окамото и Охта

Затем избиратель отправляет подписанный зашифрованный бюллетень в ЦИК. ЦИК проверяет подпись на зашифрованном бюллетене. Если бюллетень действительный, то ЦИК помещает его в список, который публикуется после всеобщего голосования. После того как список был опубликован, избиратели следят за тем, чтобы их бюллетени оказались в списке и отправляют в ЦИК декодирующие ключи, необходимые для открытия их бюллетеней. ЦИК использует эти ключи для расшифровки бюллетеней и добавления голосов на выборах. После выборов ЦИК публикует декодирующие ключи вместе с зашифрованными бюллетенями, чтобы избиратели смогли самостоятельно проверить результаты выборов.

Система Sensus Кранора и Ситрона (Cranor, Cytron), которую далее рассмотрим более подробно, в значительной степени основывается на схеме Фудзиока, Окамото и Охта. Основное отличие этих систем появляется после того, как избиратель предоставляет в ЦИК зашифрованный бюллетень. В протоколе Sensus ЦИК отвечает отправкой квитанции избирателю. Избиратель может представлять ключ дешифрования сразу же после получения этой квитанции, завершив весь процесс голосования в течение одного сеанса. Испытания, проводимые при реализации прототипа Sensus свидетельствуют о том, что весь избирательный процесс можно будет завершить в течение нескольких минут.

Sensus протокол является одним из немногих протоколов электронного голосования, которые фактически были реализованы. Еще одна вариация протокола Фудзиока, Окамото и Охта реализована Давенпортом, Ньюбергером и Белиль (Davenport, Newberger, Woodard) и используется для проведения студенческих правительственных выборов.

Протокол Sensus обладает большинством желательных характеристик, однако он не исправляет проблем, присущих Протоколу двух агентств.

## Протокол Sensus

В 1996 году была представлена реализация системы Sensus [13], практической, безопасной и частной системы для проведения опросов и голосований через компьютерные сети. Sensus позволяет избирателям самостоятельно проверить, что их голоса были подсчитаны.

Протокол, реализованный в системе Sensus, в значительной степени основывается на схеме, предложенной Фудзиока, Окамото и Охта, использующей подпись вслепую в целях обеспечения безопасности при защите личности избирателя.

Протокол Sensus требует от избирателя подготовить бюллетень для голосования, зашифровать его с секретным ключом и замаскировать (“ослепить”). Затем избиратель подписывает бюллетень и отправляет его в ЦУР (англ. validator). ЦУР проверяет принадлежность подписи зарегистрированному избирателю, который еще не голосовал. Если бюллетень действительный, ЦУР подписывает бюллетень и возвращает его избирателю. Избиратель удаляет слой ослепляющего шифрования, разоблачая зашифрованный бюллетень, подписанный ЦУР. Затем этот бюллетень отправляется в ЦИК (англ. tallier). ЦИК проверяет подпись на зашифрованном бюллетене. Если бюллетень действительный, ЦИК помещает его в список действительных избирательных бюллетеней, которые будут опубликованы после того, как все избиратели проголосуют. Затем ЦИК подписывает зашифрованный бюллетень и возвращает его избирателю в качестве квитанции. Получив квитанцию, избиратель посылает в ЦИК ключ дешифрования бюллетеня. ЦИК использует ключ для расшифровки бюллетеня и добавляет голос.

### Модули Sensus

Система Sensus разбита на отдельные модули, три из которых являются обязательными для проведения выборов с помощью Sensus: ЦУР, ЦИК и Сборщик (англ. pollster). Кроме того, возможно использовать дополнительные модули: Регистратор (англ. registrar), ballot-authoring и другие. Дополнительные модули позволяют автоматизировать выборную задачу, сэкономив время и сократив вероятность ошибок, связанных с человеческим фактором. Далее, мы подробно рассмотрим применение основных модулей для

выполнения протокола Sensus. На Рисунке 3 показана диаграмма, иллюстрирующая транзакции, которые должны выполняться между модулями Сборщик, ЦУР и ЦИК.

Основные модули Sensus были реализованы в системе UNIX на языках C и Perl с использованием бесплатной библиотеки от RSA Data Security, Inc.

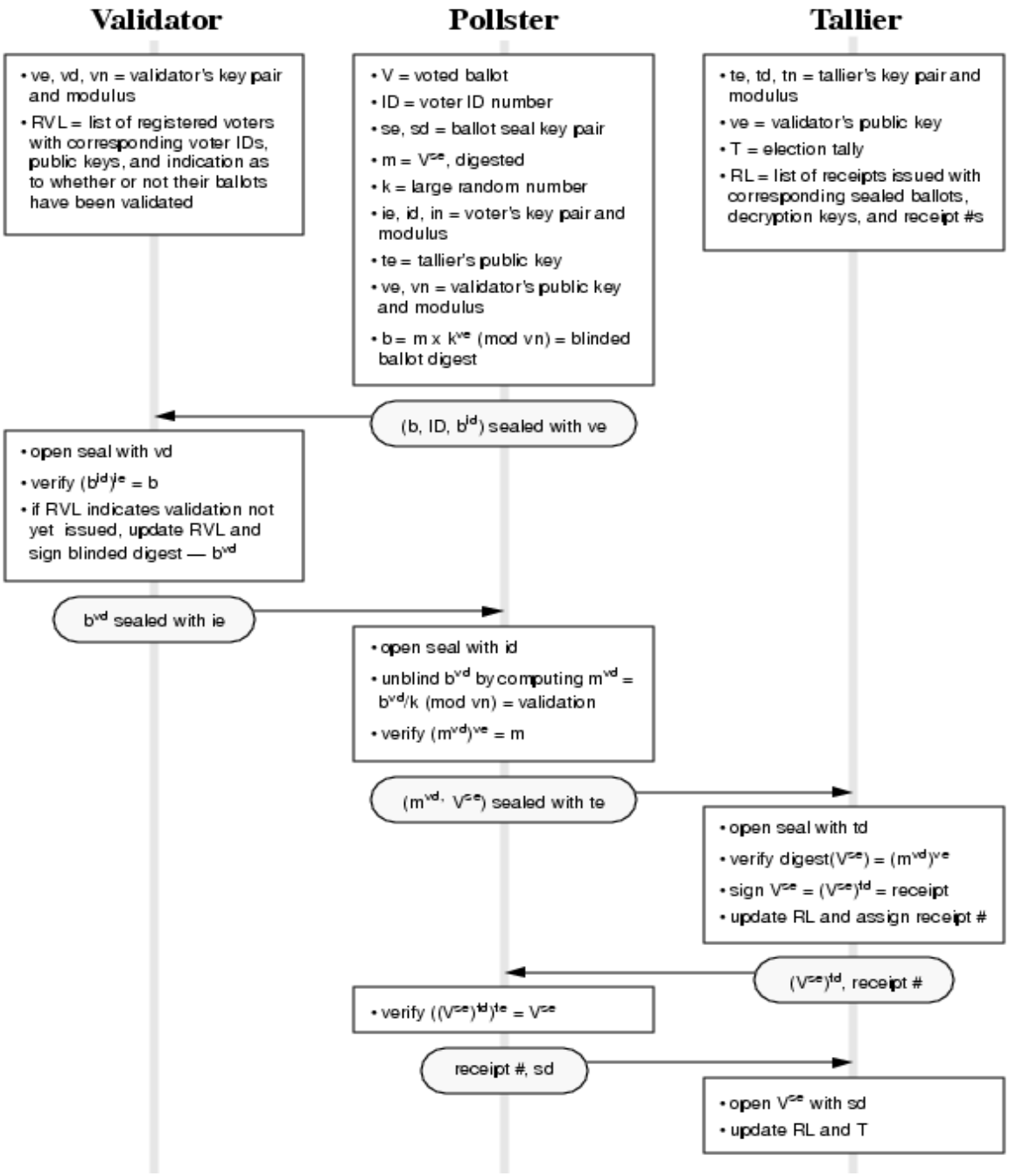


Рисунок 3 – Схема протокола Sensus

**Регистратор**

Регистратор несет ответственность за регистрацию избирателей до выборов или опроса. Регистратор должен держать у себя список людей, имеющих право на регистрацию (перечень населения), список людей, которые подали заявки на регистрацию и, личность которых не была установлена (список на проверку), подготовить список зарегистрированных избирателей. Зарегистрированные избиратели будут включаться в список по именам или идентификационным кодам, или открытым ключам шифрования, и необязательно – по *e-mail*.

Как и в случае с традиционными системами голосования, главная трудность в осуществлении регистрации является проверка личности кандидата, задача, которая может быть невыполнима без личной встречи. По этой причине, некоторые администраторы выборов вправе не автоматизировать процесс регистрации. Тем не менее, для большинства целей, процесс автоматической регистрации может дать достаточно точные результаты.

Регистратор в системе Sensus требуется, чтобы каждый избиратель до начала процесса регистрации отправлял идентификационный номер (он не обязательно должен быть тайным), и секретный символ *T*.

Избиратели генерируют пару открытый/секретный ключ и зарегистрируются для участия в голосовании, направив регистратору свои идентификационный номер избирателя, символ *T*, и открытый ключ. Регистратор проверяет, что кандидаты представили правильные символы и добавляет их идентификационные номера и ключи к списку зарегистрированных избирателей. Список зарегистрированных избирателей содержит также поле для подтверждения каждого избирателя, которое устанавливается в *0* перед каждыми выборами и изменяется на *1*, после того, как избирательный бюллетень будет проверен в ЦУР.

**Сборщик**

Сборщик выступает в роли избирательного агента, представляющего бюллетени в понятном для избирателей виде, собирающего ответы избирателей на вопросы бюллетеня, выполняя криптографические функции от имени избирателя, получающего необходимые подтверждений и квитанций, и доставляющего избирательные бюллетени в урны для голосования.

Сборщик является единственным компонентом системы Sensus, которому избиратели должны полностью доверять. Модуль Сборщик может быть выполнен с различными интерфейсами пользователя. К тому же, Сборщик можно использовать для оказания помощи избирателям при проверке, что их голоса были подсчитаны правильно и в оспаривания выборов.

В системе Sensus Сборщик реализован в виде простого текстового интерфейса. Он способен отображать отмененные повторным голосованием бюллетени, описанные с помощью языка описания голосования, BLT (формат LISP). BLT был разработан для достижения максимальной гибкости при создании бюллетеней.

**ЦУР**

ЦУР отвечает за проверку регистрации избирателей и за то, чтобы только один голос был подан каждым из зарегистрированных избирателей.

В системе Sensus ЦУР использует список зарегистрированных избирателей для получение открытого ключа каждого избирателя и проверки подписи на избирательных бюллетенях. ЦУР изменяет содержимое поля проверки в списке с *0* на *1* после подтверждения бюллетеня. При использовании этого метода не записывается порядок, в котором проверяются бюллетени.

**ЦИК**

ЦИК отвечает за сбор бюллетеней голосования и подсчет результатов выборов или опроса.

Отметим, что существует очень небольшой шанс, что два или более избирателей могут представлять идентичные зашифрованные бюллетени.

## Безопасный протокол голосования со слепыми подписями

Рассмотрим схему голосования со слепыми подписями, предложенную в 1998 году Qi He и Zhongmin Su [13].

Данная схема удовлетворяет всем необходимым требованиям голосования и благодаря ограничению полномочий ЦУР решает проблему сговора ЦИК и ЦУР.

В отличие от предыдущих схем, в которых ЦУР сразу ставил подпись на бюллетене избирателя, в этой схеме ЦУР ставит слепую подпись на открытом ключе избирателя. Такое отличие позволяет избирателям изменить свой выбор в течение голосования, кроме того, избиратели могут без проблем скорректировать свой голос, если в ЦИК произошла ошибка подсчета.

В предложенной схеме электронного голосования содержится три стороны:

1. Избиратели (voters)
2. ЦУР (authority)
3. ЦИК (tallier)

Схема содержит три этапа:

1. Этап регистрации.
2. Этап передачи (предоставления) открытого ключа
3. Этап голосования

**Обозначения**

| | |
|---|---|
| *V* (voter) | : избиратель |
| *A* (authority) | : ЦУР |
| *T* (tallier) | : ЦИК |
| $E_a$ | : открытый ключ ЦУР |
| $D_a$ | : секретный ключ ЦУР |
| $E_v$ | : открытый ключ (*tallying key*) избирателя |
| $D_v$ | : секретный ключ (*private key*) избирателя |
| *R* | : случайное число |
| *h* | : однонаправленная хеш-функция |
| $K_v$ | : симметричный ключ шифрования избирателя |
| $B_v$ | : открытый текст бюллетеня, заполненного избирателем |
| $K_v(M)$ | : шифрование сообщения *M* на ключе $K_v$ с использованием симметричной криптографии |
| $K_v^{-1}(M)$ | : расшифрование сообщения *M* на ключе $K_v$ |
| $D_x(h(M))$ | : подпись сообщения *M* |
| $E_x(C)$ | : расшифрование *C* с использованием открытого ключа |

**Этап регистрации**

Избиратель:

1) генерирует пару ключей $D_v$ и $E_v$ по аналогии с *RSA*

2) генерирует случайное число *R*

3) вычисляет $E_a(R) * (h(E_v))$ и отправляет результат в *ЦУР*

ЦУР:

4) проверяет право избирателя

5) если избиратель правомочный, ЦУР подписывает сообщение, полученное от избирателя:

$$D_a(E_a(R) * (h(E_v))) = R * D_a(h(E_v))$$

Избиратель:

6) удаляет *R* из $R * D_a(h(E_v))$:

$$D_a(h(E_v)) = R * D_a(h(E_v))/R$$

7) проверяет сравнение:

$$E_a(D_a(h(E_v))) = h(E_v)$$

8) если равенство выполняется, то подпись ЦУР $D_a(h(Ev))$ – действительная.

*Замечание*: после завершения голосования ЦУР публикует список всех зарегистрированных избирателей.

**Этап передачи (предоставления) открытого ключа**

Избиратель:

1) отправляет в ЦИК: $\{E_v , D_a(h(E_v)\}$

ЦИК:

2) проверяет подлинность открытого ключа избирателя:

$E_a(D_a(h(E_v))) = h(E_v)$

3) если равенство выполняется, то открытый ключ $E_v$ авторизуется

*Замечание*: после завершения процесса голосования ЦИК публикует все авторизованные открытые ключи

**Этап голосования**

Избиратель:

1) отправляет в ЦИК: $\{E_v, K_v(B_v), D_v(h(K_v(B_v)))\}$

ЦИК:

2) проверяет по списку, авторизован ли $E_v$, затем проверяет подлинность $K_v(B_v)$, сравнивая:

$Ev(Dv(h(Kv(Bv)))) = h(Kv(Bv))$

3) если $E_v$ авторизован и выполняется предыдущее равенство, то публикует:

$\{E_v, K_v(B_v), D_v(h(K_v(B_v)))\}$

Избиратель:

4) проверяет наличие своего зашифрованного бюллетеня в списке, опубликованном ЦИК; если не обнаружил, то через сообщество публикует:

$\{E_v, K_v(B_v), D_v(h(K_v(B_v)))\}$

5) отправляет в ЦИК: $\{E_v, K_v, D_v(h(K_v))\}$

ЦИК:

6) проверяет подлинность $K_v$, сравнивая:

$E_v(D_v(h(K_v))) = h(K_v)$

7) если $K_v$ верный, расшифровывает $K_v(B_v)$, используя $K_v$:

$K_v^{-1}(K_v(B_v)) = B_v$

8) публикует все данные:

$\{B_v, K_v(B_v), K_v, D_v(h(K_v(B_v))), D_v(h(K_v)), E_v\}$

## Итог

В течение последних 14 лет для выборов были предложены различные криптографические протоколы, они были спроектированы для сведения к минимуму мошенничества и обеспечения максимальной конфиденциальности. Кроме того, некоторые преследуют дополнительные цели, к примеру, сделать невозможным доказать для избирателей, что они голосовали определенным образом. Но многие из предложенных протоколов не являются практически осуществимыми для большого числа территориально удаленных друг от друга избирателей, однако, они представляют теоретический интерес.

## Список используемой литературы


[1] Cranor, L.F. and Cytron, R.K. *Design and Implementation of a Security-Conscious Electronic Polling System.* Washington University Computer Science Technical Report WUCS-96-02. February 1996.

[2] B. Schneier, *Applied Cryptography*

[3] Chaum, D. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM 24*, 2 (1981)

[4] Nurmi, H., Salomaa, A., and Santean, L. Secret ballot elections in computer networks. *Computers and Security,* 36, 10 (1991), pp. 553-560.

[5] Chaum, D. Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA. In *Advances in Cryptology - EUROCRYPT '88* (Berlin, 1988), C. G. Gunther, Ed., vol. 330 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 177-182.

[6] Cohen, J. D. Improving privacy in cryptographic elections. Tech. Rep. YALEU/DCS/TR-454, Yale University, February 1986.

[7] Cohen, J. D., and Fischer, M. J. A robust and verifiable cryptographically secure election scheme (extended abstract). Tech. Rep. YALEU/DCS/TR-454, Yale University, July 1985. Also appeared in 1985 Foundations of Computer Science conference proceedings.

[8] Mutch, R. E. Voting by mail. *State Legislatures* (December 1992).

[9] Demillo, R., and Merritt, M. Protocols for data security. *Computer* (February 1983), 39-51.

[10] Electronic Voting, Computerized polls may save money, protect privacy by Lorrie Faith Cranor

[11] Iversen, K. R. A cryptographic scheme for computerized general elections. In *Advances in Cyptology - CRYPTO '91* (Berlin, 1992), vol. 576 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 405-419.

[12] Sako, K., and Kilian, J. Secure voting using partially compatible homomorphisms. In *Advances in Cryptology, Crypto'94* (1994), Lecture Notes in Computer Science, Springer-Verlag.

[13] Qi He, Zhongmin Su. *A New Practical Secure e-Voting Scheme* (1998)