МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»
(СГУ)

Кафедра теоретических основ компьютерной безопасности и криптографии

# Протоколы электронного голосования

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Фролова Константина Максимовича

Научный руководитель
доцент, к.ф.-м.н. _____ В.Е. Новиков
18.01.2019 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
18.01.2019 г.

Саратов 2019

# ВВЕДЕНИЕ

В современной жизни криптография играет важное значение во многих областях. Например, при проведении электронных коммерческих операций, связи людей, сокрытия конфиденциальной информации и другие. Но мы рассмотрим важность применения криптографии на примере электронного голосования.

Несомненно, голосование является неотъемлемым атрибутом современного мира. Мы постоянно встречаемся с выборами, которые играют важную роль в нашей жизни. Нам предоставляется возможность сделать выбор, начиная от голосования на каком-нибудь сайте с фильмами или за любимое фото на конкурсе и заканчивая довольно-таки серьезным делом, выбором президента или выбором депутатов в Государственную Думу.

Протоколы электронного голосования – это протоколы, в которых избирательные бюллетени существуют только в электронной форме. Данные протоколы обеспечивают тайный характер голосования. Основное свойство протокола голосования – универсальная повторяемость, т.е. предоставление возможности всякому желающему, включая сторонних наблюдателей, в любой момент времени проверить правильность подсчета голосов.

В наше время существует много различных протоколов электронного голосования. Приведем несколько примеров.

Протокол двух агентств: создание двух счетных комиссий, которые контролируют друг друга.

Протокол Фудзиока-Окамото-Охта: протокол похож на протокол двух агенств. Различие лишь в том, что используется маскирующее шифрование – шифрование, в котором каждый пользователь может убедится в истинности автора, но не может узнать сокрытую информацию.

Протокол He-Su: использует слепую подпись, подписывая не бюллетень избирателя, а его ключ, что позволяет избирателю менять свой голос до момента окончания голосования.

Дипломная работа состоит из введения, 3 разделов, заключения, списка использованных источников и 5 приложений. Общий объем работы – 70 страниц, из них 41 страница – основное содержание, список использованных источников из 20 наименований.)

## КРАТКОЕ СОДЕРЖАНИЕ

В первой главе рассматриваются алгебраические структуры, называемые конечными полями. Определяются такие структуры, как группы, циклические группы, поле Галуа, неприводимые многочлены. Центральной теоремой этой главы является теорема 1.5.3 о мультипликативной группе поля Галуа.

**Теорема 1.5.3**. В поле $GF(q)$ существует примитивный элемент $\alpha$, т. е. элемент порядка $q - 1$. Каждый ненулевой элемент поля $GF(q)$ может быть представлен как некоторая степень $\alpha$, т. е. мультипликативная группа поля Галуа $GF(q)$ является *циклической*.

Также представлен пример построения такой группы для поля Галуа $GF(2^4)$.

Во второй главе показан алгоритм вычисления образующих мультипликативной группы поля Галуа, называемые первообразными корнями. Центральной теоремой второй главы является теорема 2.1.2. о первообразном корне по простому модулю.

**Теорема 2.1.2.** Если $p_1^{\alpha_1}\ p_2^{\alpha_2}\ \dots\ p_s^{\alpha_s}$ - каноническое разложение числа $p-1$ и $a^{\frac{p-1}{p_1}} \neq 1(mod\ p), \dots, a^{\frac{p-1}{p_s}} \neq 1(mod\ p)$, то $a$ - первообразный корень по простому модулю $p$.

В третьей главе рассматриваются протоколы электронного голосования Шаума – Педерсена и Крамера – Франклина – Шонмейкерса – Янга с доказанием корректности. Также показано использование конечных полей в криптографии, алгоритмы генерации простых чисел, в том числе больших, имеющие важное значение для алгоритмов. Показано использование проблемы дискретного логарифмирования. Пунктах 3.5 и 3.6 разобраны алгоритмы требуемых протоколов.

**Протокол Шаума - Педерсена**

Пусть $T$ – центр подсчета голосов. Будем полагать, что центр честный, пользуется доверием всех избирателей и не имеет скрытых мотивов при голосовании.

Пусть $p$ – большое простое число, $g$ и $h$ – первообразные корни по простому модулю $p$.

Доверенный центр $T$ выбирает секретный ключ $x$, $0 < x < p$, и публикует в открытом доступе открытый ключ $Y = g^x \bmod p$.

1. $T \to P_i : p, g, h, Y$ (бланк бюллетеня).

Каждый избиратель посылает центру сообщение, содержащее идентификатор этого избирателя и его голос $a_i \in \{-1, 1\}$, зашифрованный с помощью вероятностного шифра на ключе $Y$ следующим образом:$U_i = g^{k_i} \bmod p$, $V_i = Y^{k_i} * h^{a_i} \bmod p$ , ($U_i$, $V_i$) – бюллетень голосования (передается центру $T$), где $k_i$ – некоторое случайное число $0 < k_i < p$. Т.е. каждый избиратель генерирует случайное число $k_i$ ($0 < k_i < p$) — его секретный ключ, вычисляет свой идентификатор :$U_i = g^{k_i} \bmod p$, зашифровывает свой голос $V_i = Y^{k_i} * h^{a_i} \bmod p$ при $1 \le i \le n$.

2. $P_i \to T :$ $U_i$, $V_i$ (заполненный бюллетень голосования)

Центр расшифровывает бюллетени $h^{a_i} = V_i * U_i^{-x} \bmod p$ , откуда получает $a_i$, подсчитывает число голосов $S = \sum_{i=1}^{n} a_i$, и публикует итог $S$.

Поскольку все бюллетени ($U_i$, $V_i$) находятся в открытом доступе в некотором хранилище, называемым доской голосования, любой участник голосования или сторонний наблюдатель может вычислить $A = \prod_{i=1}^{n} U_i = g^{\sum k_i} \bmod p$, $B = h^{-S} \prod_{i=1}^{n} V_i = g^{x \sum k_i} \bmod p$ при $1 \le i \le n$. Откуда видно, что$B = A^x \bmod p$. С другой стороны $Y = g^x \bmod p$, т.е. при правильном подсчёте голосов должно выполняться равенство $\log_A B = \log_g Y \bmod p$. Избиратель не знает $x$, и требует от центра доказать с нулевым разглашением выполнение последнего равенства.

Алгоритм доказательства:

1. Доказывающий выбирает $k \in_R Z_p$ вычисляет ($\beta$, $\gamma$) = ($g^k \bmod p$, $A^k \bmod p$) и посылает ($\beta$, $\gamma$) проверяющему.

2. Проверяющий выбирает запрос $e \in_R Z_p$, случайно сгенерированный и посылает $e$ доказывающему.

3. Доказывающий вычисляет$s = (k + e * x) mod\ p$ и посылает $s$ проверяющему.

4. Проверяющий убеждается, что$g^s = \beta * y^e\ mod\ p$ и$A^s = \gamma * B^e\ mod\ p$, и принимает доказательство. В противном случае, если хотя бы одно из этих сравнений не выполняется, — отвергает.

**Протокол Крамера – Франклина – Шонмейкерса - Янга**

Пусть в голосовании участвуют $n$ избирателей $P_1$, …, $P_n$, которые являются абонентами некоторой сети и подают свои голоса в электронной форме: «за» и «против», которые соответственно представимы значениями 1 и -1. К протоколу предъявлены два основных требования:

1. Голосуют только уполномоченные избиратели.
2. Любой участник может подать не более одного голоса.
3. Ни один из участников не знает, как проголосовал другой.
4. Никто не может воздействовать на голос другого избирателя.
5. Конечный результат будет подсчитан корректно.
6. Любой из участников может проверить корректность подсчета голосов.
7. Протокол должен работать даже в случае, что кто-то голосует нечестно.

Пусть $p$ – большое простое число, $g$ – первообразный корень по простому модулю $p$, $h = g^d$ для некоторого $0 < d < p$, причем нахождение $d$ по известному $h$ вычислительно трудная задача.

Алгоритм:

I.Создание бюллетеней избирательным центром $T$.

На вход подается количество участвующих в голосовании избирателей $n$ и большое простое число $p$. С помощью алгоритма нахождения первообразных корней по простому модулю находиться элемент $g$. Далее для некоторого $0 < d < p$ находится значение $h$. Каждому пользователю направляется бюллетень, в которой находится три значения: $p$, $g$, $h$.

II.Голосование избирателей.

1. Каждый голосующий выбирает значение $b \in \{-1, 1\}$. Вычисляет значение $B_i = g^{\alpha} * h^b$, где $\alpha$ – случайно сгенерированный элемент $Z_p$. Также определяются многочлены $G$ и $H$:

$G(x) = \alpha + \alpha_1 * x + \ldots + \alpha_{t-1} * x^{t-1}$

$H(x) = b + \beta_1 * x + \ldots + \beta_{t-1} * x^{t-1}$,

где $\alpha_i$ и $\beta_i$, $1 <= i < t$, выбранные случайно из $Z_p$. Также вычисляется $B_{ij} = g^{\alpha j} * h^{bj}$.

2. Голосующий публикует $B_i$ , $B_{ij}$,$1<= j < t$.

3. Каждый участник подсчитывает и оправляет значение $(a_{ij}, b_{ij}) = (G_j(j), H_j(j))$ при $1 < i < n$.

4. Голосующие отправляют голос $s \in \{-1, 1\}$, подсчитывают $v = s * b$.

III.Подсчет голосов избирательным центром $T$.

1. Счетная комиссия публикует $S_i = \text{sum}(a_{ij} * s_i)$ и $T_i = \text{sum}\ (b_{ij} * s_i)$, $1 <= i <= n$.

2. Любой другой участник процедуры голосования, будь то счетная комиссия или избиратель, может убедиться в корректности опубликованных сумм, проверяя, что $g^{Sj} * h^{Tj} = B_i * \text{mult}\ (B_{il}^{jl})$, где $1 <= l <= t - 1$.

3. Итогом голосования является уже подсчитанное значение $T_i$. Если результат — отрицательное число, то большинство избирателей написало на бюллетене число -1, а если положителен, то большинство поставило 1.

В заключении дана оценка эффективности работы этих протоколов.

В работе присутствуют приложения, в которых написана программная реализация алгоритмов. В приложении А показан алгоритм нахождения первообразных корней по простому модулю. В приложениях Б и В представлены алгоритмы генерации простых чисел по алгоритмам Рабина – Миллера и Соловея – Штрассена соответственно. В приложении Г написана реализация протокола Шаума – Педерсена с примером работы программы. В приложении Д написана

реализация протокола Крамера – Франклина – Шонмейкерса – Янга с примером работы программы.

# ЗАКЛЮЧЕНИЕ

В наше время существует много других протоколов электронного голосования с разными свойствами. Их применяют тогда, когда нужно решить поставленную задачу, но существуют какие-то ограничения или требуется выполнить определенные задачи.

Например, протокол двух агентств можно реализовать для $m$ счетных комиссий, преследующих различные цели, но заинтересованных в честных выборах. Единственный вариант ложных результатов голосования возможен в том случае, когда счетные комиссии находятся в сговоре. Такой алгоритм использует какую-либо схему не интерактивного, публично проверяемого разделения секрета. Стойкость алгоритма и эффективность обработки данных зависит от выбранного алгоритма разделения секрета. Зачастую используют проблему дискретного логарифмирования для обеспечения эффективного сокрытия данных.

Как было сказано ранее, единственный вариант неверных итогов возможен при сговоре всех счетных комиссий. Но сорвать выборы может любая комиссия в одиночку. Решить эту проблему может следующая модификация: пусть распределение голосов могут восстановить $k < m$ счетных комиссий. Но тогда подделать результаты смогут уже $k$ сговорившихся центров, а сорвать выборы — $m - k$. Схему можно улучшить, например, возможностью нескольких вариантов ответа в бюллетени или поэтапное или параллельное голосования. Плюс ко всему, присутствует полная анонимность.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Шнайер Б. Прикладная криптография / Б. Шнайер - М: Триумф, 2-е изд. 2002. — 610 с.

2 Реализация протоколов тайного электронного голосования [Электронный ресурс]. URL: https://sibac.info/studconf/tech/xxxii/42180 (дата обращения: 1.12.2018). Загл. с экрана. Яз. рус.

3 Протокол Шаума-Педерсена [Электронный ресурс]. URL: http://info.sernam.ru/book_crypt.php?id=21 (дата обращения: 1.12.2018). Загл. с экрана. Яз. рус.

4 Смарт Н. Крипография / Н. Смарт - М: Техносфера, 2005. – 529 с.

5 Cramer R. Multi-Authority Secret-Ballot Elections with Linear Work / R. Cramer, M. Franklin, B. Shoenmakers , M. Yung // Proc. EUROCRYPT’96, Lect. Notes in Comput. Sci. 1996. Vol. 1070. P. 72–83.

6 Рацеев С.М. О протоколах электронного голосования / С.М. Рацеев, О.И. Череватенко 8 с. / Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика. 2018. Т. 18, вып. 1. С. 62-67.

7 Chaum D. Wallet databases with observers / D. Chaum, T. P. Pedersen // Proc. Crypto’92, Lect. Notes in Comput. Sci. 1993. Vol. 740. P. 89–105.

8 Протоколы электронного голосования [Электронный ресурс]. URL: https://studfiles.net/preview/4483753/page:15/ (дата обращения: 1.12.2018). Загл. с экрана. Яз. рус.

9 Cramer R. A secure and optimally efficient multi-authority election scheme / R. Cramer, R. Gennaro, B. Schoenmakers // Proc. EUROCRYPT’97, Lect. Notes in Comput. Sci. 1997. Vol. 1233. P.103–118.

10 Алфёров А.П. Основы криптографии / А.П. Алфёров, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин // М: Гелиос АРВ. 2-е издание. 2002 г. – 480 с.

11 Теория групп [Электронный ресурс]. URL: http://www.studfiles.ru/preview/6072831/ (дата обращения: 1.12.2018). Загл. с экрана. Яз. рус.

12 Теория групп [Электронный ресурс]. URL:

http://www.studfiles.ru/preview/6072831/ (дата обращения: 1.12.2018). Загл. с экрана. Яз. рус.

13 Теория групп [Электронный ресурс]. URL http://studopedia.ru/view_algebra.php?id=1 (дата обращения: 1.12.2018). Загл. с экрана. Яз. рус.

14 Поле Галуа [Электронный ресурс]. URL: http://www.studfiles.ru/preview/5621791/page:8/ (дата обращения: 1.12.2018). Загл. с экрана. Яз. рус.

15 Группа Галуа [Электронный ресурс]. URL: http://info.sernam.ru/book_code.php?id=43 (дата обращения: 1.12.2018). Загл. с экрана. Яз. рус.

16 Мультипликативная группа поля Галуа [Электронный ресурс]. URL: http://info.sernam.ru/book_code.php?id=43 (дата обращения: 1.12.2018). Загл. с экрана. Яз. рус.

17 Лидл Р. Конечные поля / Р. Лидл, Г. Нидеррайтер // В 2-х тт. — М.: Мир, 1998. — 430 с

18 Бухштаб А.А. Теория чисел / А.А. Бухштаб // М.: Просвещение, 1966.

19 Виноградов И.М. Основы теории чисел / И.М. Виноградов // Москва-Ленинград: Из-во Технико-Теоретической Литературы, 1952.

20 Конечные поля [Электронный ресурс]. URL: http://sernam.ru/book_tec.php?id=79 (дата обращения: 1.12.2018). Загл. с экрана. Яз. рус.