МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Протокол тайного голосования на основе ANDOS

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Коваленко Глеба Дмитриевича

Научный руководитель
доцент _____ В. Е. Новиков
23.01.2021 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
23.01.2021 г.

Саратов 2021

ВВЕДЕНИЕ

Протоколы тайного голосования в криптографии — это процесс обмена данными для реализации безопасного тайного электронного голосования при помощи электронно-вычислительных машин (например, телефонов или компьютеров). Хоть данное направление пока ещё только развивается, оно уже начинает находить применение в реальном мире.

Различные страны уже сейчас занимаются внедрением электронных голосований на разных уровнях. Для уверенности в правильности, надежности и конфиденциальности организованных таким способом мероприятий и используют протоколы с подтвержденной защищенностью, в основе которых лежат проверенные криптографические системы, вроде асимметричного шифрования и электронной подписи.

В дипломной работе рассматривается конкретная реализация одного из протоколов тайного электронного голосования, а именно протокол тайного голосования на основе протокола ANDOS.

Сейчас в открытом доступе находится не так много доступных решений для проведения своего тайного электронного голосования, а реализаций рассмотренного в дипломной работе варианта на момент написания этой работы обнаружено не было.

Уже довольно продолжительно наблюдается общемировая тенденция по переходу от физических реализаций тех или иных аспектов человеческой жизни к их электронным аналогам, которые будут менее ресурсозатратны и более удобны. А в текущих мировых реалиях вопрос перехода на эти самые электронные аналоги, позволяющие дистанцировать людей друг от друга, встаёт особенно остро.

Исключением не стала и сфера электронных голосований. Развитие этой отрасли позволит проводить выборы и голосования без необходимости физического присутствия избирателей на избирательных участках, что удобно

как для конечных пользователей, поскольку требует от них меньше времени и усилий, так и для субъекта, проводяшего данное голосование, поскольку оно потребует меньше средств, ресурсов и времени.

Особенно сильно будет ощущаться экономическая выгода при проведении последующих голосований, так как, фактически, нужно один раз вложиться в разработку и реализацию системы голосования, а все последующие разы – просто использовать её с минимальными изменениями и вложениями. Причем всё вышесказанное применимо как к большим государственным выборам, так и к совсем маленьким голосованиям внутри небольших компаний или даже просто групп людей.

При написании дипломной работы ставилось несколько целей: изучение имеющихся протоколов тайного голосования, более глубокое изучение одного из них, а именно протокола на основе протокола ANDOS, реализация этого протокола и последующие тестирование. В процессе написания решались разного рода задачи, такие как изучение необходимых алгоритмов и подпротоколов, изучение математических обоснований, реализация или интеграция дополнительных модулей, необходимых для корректной работы приложения, которое было реализовано.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 2 приложений. Общий объем работы – 55 страниц, из них 38 страниц – основное содержание, включая 14 рисунков, список использованных источников из 15 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе дипломной работы, который называется «Математические основы протоколов тайного голосования» рассматриваются теоретические вопросы, понимание которых необходимо для дальнейшей реализации протокола и написания приложения. Каждый из подразделов первого раздела посвящен одному из таких вопросов.

Первый подраздел первого раздела называется «Алгоритм Евклида» и содержит в себе теоретическую информацию о самом алгоритме, доказательство его корректности, а так же его следствие – расширенный алгоритм Евклида. Именно расширенный алгоритм Евклида и будет задействован при работе над практической реализацией основного протокола.

Второй подраздел первого раздела называется «Односторонние функции с потайным входом», в нём рассказывается о том, что такое односторонняя функция для того, чтобы затем дать определение непосредственно тому, что такое односторонняя функция с потайным входом. Это необходимо, так как в работе будет использоваться одна из таких функций – RSA. Краткое описание её принципов работы так же содержится в этом подразделе.

Третий подраздел первого раздела называется «Тест Ферма на простоту». В этом подразделе идёт речь о самом простом способе проверить число на простоту. В подразделе формулируется малая теорема Ферма, на которой как раз основан тест, а так же лемма с доказательством, необходимая для доказательства теоремы Ферма. Этот тест так же необходим для практической реализации, с помощью него проводится первичное тестирование чисел кандидатов на простоту.

Четвертый подраздел первого раздела называется «Тест Миллера-Рабина». В нём рассказывается о самом тесте Миллера-Рабина, формулируются его условия и описывается идея теста. Серия таких тестов задействуется для

конечной проверки числа на простоту, чтобы его можно было в дальнейшем использовать в ходе работы пакета приложений.

Все подразделы вместе представляют собой математическую базу, на которой основан рассматриваемый протокол тайного голосования.

Во втором разделе дипломной работы, который называется «Протоколы тайного голосования», рассматриваются основные протоколы тайного голосования. Этот раздел так же разбит на подразделы.

Первый подраздел второго раздела посвящен истории возникновения и развития протоколов тайного голосования. Этот подраздел важен для понимания актуальности рассматриваемого вопроса и лучшего погружения в тему дипломной работы.

Второй подраздел рассказывает об основных требованиях, которые выдвигаются к протоколам тайного голосования, в том числе и об опциональных требованиях. Знания, полученные после изучения этого раздела, помогут лучше понять достоинства и недостатки каждого из описанных далее протоколов, а так же понять, какие цели и задачи ставили перед собой авторы этих протоколов и удалось ли им в конечном итоге их решить.

Остальные подразделы 2.3 — 2.7 описывают каждый по одному из тех протоколов тайного голосования, реализация которых не будет рассматриваться в данной дипломной работе. Протоколы расположены в порядке возрастания их сложности и совершенности, хотя среди последних нескольких приведенных протоколов довольно сложно выделить самый совершенный.

Этот раздел является вводным в тему и ознакомительным. Он позволяет ближе познакомиться с протоколами тайного голосования, их вариациями, требованиями, которые к ним выдвигаются, задачами, которые они могут решать, а так же историей их появления. Важно обратить внимание, что у всех протоколов есть свои плюсы и минусы, которые описываются в подразделах, относящихся к протоколам, и даже самый простой протокол имеет право жизнь и может использоваться в определенных условиях.

В третьем разделе дипломной работы, который называется «Протокол ANDOS и его приложение», рассматривается протокол ANDOS и его приложение – протокол тайного голосования на основе протокола ANDOS, который является основным протоколом этой дипломной работы и именно он будет реализован на практике. Этот раздел так же, как и предыдущие, разделяется на подразделы.

В первом подразделе третьего раздела идт речь о протоколе ANDOS. Именно на этом протоколе построен протокол тайного голосования, который является центровым в данной дипломной работе. В этом разделе приводится описание алгоритма, его шаги и пояснения к его работе.

Алгоритм:

Пусть $s_1, \dots, s_k$ секреты, которым обладает **S**, каждый из них содержит *m* бит. Для каждого s_j **S** публикует описание секрета. Предположим, что покупатели $\boldsymbol{E}_i$ и $\boldsymbol{E}_j$ хотят купить секреты s_i и s_j соответственно.

Шаг 1. S даёт $\boldsymbol{E}_i$ и $\boldsymbol{E}_j$индивидуальные односторонние функции f_i и f_j, но сохраняет обратные к ним для себя;

Шаг 2. $\boldsymbol{E}_i$ сообщает $\boldsymbol{E}_j$ (соответственно $\boldsymbol{E}_j$ — $\boldsymbol{E}_i$) *k* случайных *m*-битных чисел $x_1^i, \dots, x_k^i$ (соответственно $x_1^j, \dots, x_k^j$);

$f_i\left(x_l^i\right)_{1 \le l \le k} = a_l^i$, где a_l^i – также *n*-разрядное число. Определим Индекс Фиксированного Бита (ИФБ) как $\mathrm{I}(x_l^i, a_l^i) = z_1 z_2 \dots z_m$ *m*-разрядное двоичное число, где

$$z_u = \begin{cases} 1, \text{если } u - \text{тый бит в } x_l^i \text{ равен } u - \text{тому биту в } a_l^i \\ 0, \text{в противном случае} \end{cases}, 1 \le u \le m$$

Шаг 3. $\boldsymbol{E}_i$ сообщает $\boldsymbol{E}_j$ (соответственно $\boldsymbol{E}_j$ — $\boldsymbol{E}_i$) индекс $I_{\boldsymbol{E}_i}$, соответствующий (x_i^j, f_i) (соответственно индекс $I_{\boldsymbol{E}_j}$, соответствующий $\left(x_j^i, f_j\right)$;

Шаг 4. $\boldsymbol{E}_i$ (соответственно $\boldsymbol{E}_j$) сообщает **S** числа $y_1, \dots, y_k$ (соответственно $y'_1, \dots, y'_k$), где y_i — результат, полученный заменой каждого бита в x_i^i, который равен нулю в $I_{\boldsymbol{E}_i}$, на ему противоположным;

Шаг 5. **S** сообщает $\boldsymbol{E}_i$ (соответственно $\boldsymbol{E}_j$) числа

$s_i \oplus f_i^{-1}(y'_i)$ (соответсвенно $s_i \oplus f_j^{-1}(y_i)), i = 1,\ldots,k$

Шаг 6. $\boldsymbol{E}_i$ (соответственно $\boldsymbol{E}_j$) может вычислить s_j (соответственно s'_j), с помощью побитового сложения x_i^j и i-того числа (соответственно x_j^i и j-того числа), полученного от **S**.[1]

В случае, ели число покупателей $t \geq 3$ протокол действует по совершенно той же схеме, но каждый покупатель получает *t*-1 функцию от продавца наравне с наборами чисел от других покупателей.

Во втором подразделе третьего раздела идёт речь о центровой теме дипломной работы – протоколе тайного голосования на основе протокола ANDOS. Именно этот протокол рассматривается особенно глубоко и именно он был реализован в процессе написания дипломной работы. В подразделе оприведено его описание, шаги и немного дополнительной информации.

Шаг 1. **A** утверждает список пользователей, участвующих в голосовании;

Пусть набралось *n* легитимных избирателей. Тогда **A** выбирает не менее чем *n* идентификаторов и применяет протокол ANDOS к избирателям. Идентификаторы — большие простые числа, которые пронумерованы как $1,\ldots,n$

Шаг 2. **E** получает *i*-ое простое число p_i из списка (**A** не знает ничего о взаимосвязи между **E** и *i*);

E выбирает криптографическую функцию шифрования с открытым ключом h_E;

E отправляет **A** пару $(p_i, h_E(p_i, v_E))$, где v_E — выбор (например, имя кандидата, или в более общем виде, выборочная стратегия), который представлен численно.

Шаг 3. **A** опубликовывает все полученные $h_E(p_i, v_E)$;

[1] Brassard G., Crepeau C., Robert J.-M. All-or-Nothing Disclosure of Secrets/ Brassard G., Crepeau C., Robert J.-M - M.: CRYPTO, 1986.

Шаг 4. После публикации $h_E(p_i, v_E)$ в открытом списке **E** отсылает **A** пару (p_i, h_E^{-1}). Таким образом **A** теперь знает связь между $h_E(x, y)$ и h_E^{-1} (но не знает связь между **E** и его выбором v_E).

Шаг 5. Когда все избиратели отправили **A** свои обратные функции, голосование подходит к концу, **A** производит вычисления и объявляет промежуточные результаты, публикуя списки выборочных стратегий с числами $h_E(p_i, v_E)$ соответствующими участникам, голосовавшим за v_E.

Шаг 6. Если участник **E** замечает, что его голос размещён в неверном списке, то он посылает **A** жалобу в виде тройки $(p_i, h_E(p_i, v_E), h_E^{-1})$, которая явным образом показывает верность либо ошибочность результата.[2] [3]

Протокол ANDOS требует достаточно много ресурсов и плохо масштабируется (нужно заранее знать количество голосующих), но зато для него не нужен независимый регистратор **V**. Помимо этого, избирателям необходимо выбирать и пересылать не только идентификаторы, но и функции, что может быть долго и сложно. При этом **A** всё ещё имеет возможность жульничать, распределяя по своему выбору голоса тех, кто заявил о своём намерении принять участие в голосовании, но так и не совершил свой выбор, а **E** имеют повышенный стимул купли/продажи голосов, так как можно убедиться в результате сделки.

Третий раздел является первым из двух основных разделов дипломной работы, именно на основе приведенной в нём информации о протоколах было написано приложение, реализующее протокол тайного голосования на основе протокола ANDOS.

В четвертом разделе, который называется «Практическая часть. Реализация протокола тайного голосования на основе протокола ANDOS», происходит описание разработанного в процессе написания дипломной работы

[2] Brassard G., Crepeau C., Robert J.-M. All-or-Nothing Disclosure of Secrets/ Brassard G., Crepeau C., Robert J.-M - M.: CRYPTO, 1986.

[3] SpringerLink. Nurmi H., Salomaa A. Conducting secret ballot elections in computer networks: Problems and solutions. [Электронный ресурс] – URL: https://link.springer.com/article/10.1007/BF02032763 (дата обращения 11.09.2020) Загл. с экрана. Яз англ.

приложения. В нём пошагово расписывается, как работает клиентское приложение, а как работает серверное, какие команды можно ввести и какой результат получить, а так же в целом описывается весь процесс проведения тайного голосования с использованием разработанного программного обеспечения. Каждый шаг сопровождается приложенным скриншотом и описанием, что на скриншоте происходит и с какой целью.

Четвертый раздел является вторым из двух основных разделов дипломной работы. В нём рассказывается о результате все проведенных исследований – о пакете приложений, который позволяет провести тайное электронное голосование, в основе которого лежит протокол тайного голосования на основе ANDOS.

ЗАКЛЮЧЕНИЕ

В результате написания дипломной работы был изучен вопрос проведения тайных голосований, рассмотрены различные протоколы, позволяющие провести подобные голосования, а особенно глубоко был изучен процесс проведения тайного голосования на основе протокола ANDOS.

Так же была изучена и рассмотрена вся необходимая для понимания данного вопроса математика, и даже немного затронута история протоколов тайного голосования.

С использованием всех полученных при изучении теоретической части знаний стало возможным написание реализации одного из протоколов тайного голосования, который был рассмотрен лушче всех, а именно – вышеупомянутого протокола тайного голосования на оснвове протокола ANDOS. Данная реализация, позволяющая провести тайное голосование, представляет собой пакет приложений, в который входят серверное и клиентское приложения.

Четвертый раздел дипломной работы содержит очень подробное и понятное описание работы как клиентского, так и серверного приложений, что позволяет легко разобраться, как пользовать разработанным программным обеспечением.

Разработанный пакет приложений является готовым ядром, которое, при желании, можно интегрировть в различные системы или просто обернуть в любую оболочку для большей наглядности и удобства.

Но даже без какой-либо оболочки или интеграции в другую систему данная разработка самодостаточна и представляет возможность провести тайное голосование, причем достаточно безопасно и эффективно.

Однако стоит упомянуть, что, как уже было сказано в дипломной работе, протокол тайного голосования на основе протокола ANDOS плохо

масштабируется, поэтому его эффективность сильно зависит от того, как и для каких задач его используют.

К сожалению, сопоставить работу разработанного программного обеспечения с аналогами не представляется возможным, так как на момент написания работы в открытом доступе не было обнаружено других разработок по этой теме.

В заключении хочется сказать, что все цели работы были достигнуты, все поставленные задачи, а так же задачи, возникшние в процессе написания, были решены, и итоговая работа достаточно глубоко и широко рассматривает вопрос проведения тайного голосования с помощью протокола на основе протокола ANDOS и является исчерпывающим материалом по данному вопросу.