Электронные выборы

Ю. Лифшиц*

4 октября 2005 г.

Содержание

1 Постановка задачи

Тема электронных выборов весьма трудна. На этой лекции будет дан лишь общий обзор.

Идея электронных выборов привлекла всеобщее внимание в последние 20 лет. Первая публикация на эту тему появилась в 1981 году. Окончательного решения всех вопросов до сих пор нет, тема всё ещё развивается.

*Законспектировал А. Богатов

1.1 Мотивация

У электронных выборов немало преимуществ перед выборами обычными. Хотя придумать схему и сделать электронные устройства достаточно дорого, в действительности электронные выборы дешевле, поскольку затраты на них являются одноразовыми. Одно и тоже оборудование можно будет использовать многократно. Появляется возможность чаще проводить выборы, люди будут больше участвовать в управлении государством, оказывать большее влияние на политику.

Второй важный аргумент в пользу электронных выборов — мобильность. Электронные коммуникации можно провести даже в те уголки земного шара, где трудно организовать избирательные участки.

Наконец, результаты электронных выборов проверяемы, т.е. можно полностью контролировать подсчёт голосов.

Проекты внедрения системы электронных выборов всерьёз обсуждаются в Дании, Эстонии, в штате Аризона (США).

1.2 Типы выборов

В зависимости от задаваемых избирателям вопросов можно выделить такие типы выборов:

- с ответом типа «да / нет»;
- выбор одного из нескольких кандидатов (“1 из L”);
- выбор некоторого количества из нескольких кандидатов (“K из L”) — применяется, к примеру, на муниципальных выборах;
- выбор не более чем определённого количества из кандидатов (“$\leq K$ из L”);
- выбор некоторого количества из нескольких кандидатов с расстановкой приоритетов, когда стоящий в итоговом списке раньше считается важнее (упорядоченный вариант “K из L”);
- “1-L-K” — выбор K элементов из одного из L списков; такая система применяется в США при избрании выборщиков (есть списки кандидатов в выборщики от L партий, нужно сформировать команду от одной партии);
- открытый вопрос, подразумевающий открытый ответ (можно писать любой текст).

1.3 Фазы выборов

Выборы обычно проводятся в 3 фазы.

1. **Инициализация:** объявляется вопрос, составляется список голосующих, генерируются ключи для криптосистем.

2. **Голосование:** в англоязычных источниках голосующие называются voters, организаторы выборов — authority. Голосующие взаимодействуют с организаторами. В итоге организаторы получают информацию, которая является отражением голоса (“электронный контейнер” с голосом).

3. **Подсчёт голосов:** организаторы вычисляют и публикуют результат выборов, желающие проверяют честность выборов.

1.4 Требования к схеме выборов

1. **Контроль над избирателями.** В выборах могут участвовать только занесённые в список избиратели, один человек имеет лишь один голос.

2. **Анонимность, тайна голосования.** Нельзя узнать выбор конкретного избирателя.

3. **Индивидуальный контроль.** Каждый человек может проверить, что его голос подсчитан.

4. **Универсальный контроль.** Можно проверить, что результат выборов верен (что не были вброшены лишние бюллетени).

5. **Устойчивость.** Некорректные действия некоторых избирателей либо небольшой части организаторов не могут сорвать выборы.

6. **Неподтверждаемость.** После выборов нельзя доказать, что человек проголосовал определённым образом. При невыполнении этого требования можно будет, во-первых, заключать договор на покупку голоса, во-вторых, заставлять голосовать каким-либо образом (например, в армии или в тюрьме).

   Комментарий. В случае индивидуального контроля мы проверяем, подсчитан ли наш голос вообще, а не то, как он интерпретирован. Обсуждение:

   > Требование неподтверждаемости несовместимо с тем, чтобы избиратель имел возможность проверить, правильно ли учли его голос.

7. Нельзя голосовать за другого человека.

8. Нельзя скопировать чужой голос или обратить его (создать противоположный).

9. Не должно быть возможности узнать промежуточные результаты.

Сначала голосование проводится в зашифрованном виде, потом избиратели дают расшифровать свои голоса.

2 Примитивы и идеи

2.1 Гомоморфное шифрование

Криптосистема с открытым ключом — пара алгоритмов E и D, таких что $D(E(x)) = x$ и, зная E (а тем более не зная E), трудно построить D.

Криптосистему называют *гомоморфной относительно сложения*, если существует полиномиально вычислимая функция F, такая что $F(E(x_1), E(x_2)) = E(x_1+x_2)$. Аналогичным образом определяется гомоморфность относительно умножения и любой другой бинарной операции.

Факт: есть криптосистема (основанные на трудности дискретного логарифмирования), обладающие этим свойством. В ней F — просто умножение.

Криптосистема RSA гомоморфна относительно умножения, но не сложения: если x_1 в зашифрованном виде выглядит как $f(x_1) = x_1^a$, а x_2 в зашифрованном виде — как $f(x_2) = x_2^a$, то, зашифровав произведение, мы получим $f(x_1x_2) = (x_1x_2)^a = x_1^a x_2^a = f(x_1)f(x_2)$.

Система, обладающая гомоморфностью относительно сложения и умножения, называется алгебраически гомоморфной. Существуют ли такие системы — открытая научная проблема.

Комментарий. Блочные шифры, очевидно, не обладают никакой гомоморфностью.

2.2 Слепая подпись

Допустим, что Алиса — директор, а Боб — секретарь. Боб хочет отдать документ на подпись Алисе так, чтобы она не узнала ничего о содержимом документа; при этом требуется, чтобы Боб не смог подделать подпись Алисы (в криптографических терминах, не узнал её секретного ключа). Протокол обмена сообщениями между Алисой и Бобом, в результате которого Боб получит подпись Алисы на нужном ему сообщении, а Алиса не узнает, что она подписала, называется **протоколом слепой подписи**.

Комментарий. Подпись — нечто, что заверяет документ. Она никак не встраивается в документ, а прикрепляется к нему. Подпись зависит и от человека, который её поставил, и от содержимого документа, на котором она поставлена. Подпись данного человека задаётся неизменным для него алгоритмом (параметром которого является текст документа). При необходимости можно проверить:

1. что подпись принадлежит именно тому человеку, который об этом заявляет;
2. что подпись была поставлена именно на этот документ (что в документ не были внесены изменения или не был подложен другой документ).

Простейшая физическая реализация слепой подписи такова: в конверт с письмом мы кладём копирку, человек расписывается на конверте, благодаря копирке (которую мы после этого вынимаем) подпись появляется на письме.

Протоколы слепой подписи были разработаны около 20 лет назад. Они основаны на дискретном логарифме.

2.3 Тайна голосования

Пусть мы отказываемся от тайны голосования. Тогда можно предложить некоторую схему проведения выборов. Каковы предложения?

Обсуждение:

- Каждый говорит своё решение; недостаток — можно сказать дважды, это трудно заметить.
- Все объявляют своё решение, присылают его со своим именем и подписью.

Два основных пути к тайне голосования:

1. Все видят голос, но никто не знает, чей он.

   Обсуждение:

   В таком случае становится невозможно не опубликовывать промежуточные результаты.

   Действительно, у этого подхода множество недостатков.
   Главный инструмент для реализации — анонимный канал (в канал посылается сообщение, неизвестно, от кого оно исходило).
   Основная проблема — контроль за избирателями (не проконтролировать, кто проголосовал два раза).

2. Все знают, кому принадлежит данный голос, но никто не может расшифровать выбор. Для того чтобы получить шифротекст всех бюллетеней, можно использовать гомоморфное шифрование. Затем, расшифровав этот объединённый шифротекст, получаем сумму всех голосов.
   Ситуация такова: имеется множество независимых организаторов,

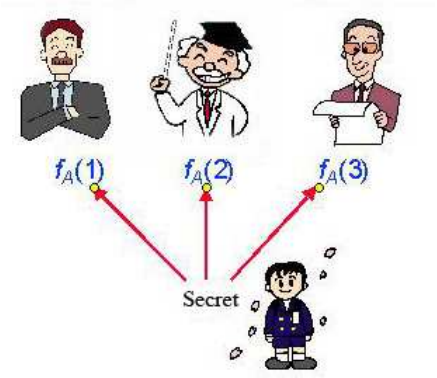

Рис. 1. Разделение секрета

   большинство из которых честны. Голоса раздаются по частям каждому из организаторов. Мы считаем, что организаторы не соберутся вместе для расшифровки отдельных голосов, поскольку они являются честными.

Сегодня мы рассмотрим лишь первый путь. Однако существуют схемы, реализующие как один, так и другой.

2.4 Псевдонимы

Итак, главная проблема анонимного канала — обеспечение контроля за избирателями. Решается она созданием псевдонима.

Во время первой фазы избиратель, общаясь с организаторами, создаёт специальное сообщение (псевдоним). Организаторы не знают, какому избирателю какой псевдоним принадлежит. Избиратель может создать лишь один псевдоним. Организаторы могут проконтролировать избирателей, составив список участвующих в выборах псевдонимов.

Во второй фазе происходит собственно голосование. Избиратель посылает по анонимному каналу пару, состоящую из псевдонима и голоса. Организаторы суммируют соответствующие корректным псевдонимам голоса, могут проконтролировать, сколько различных избирателей приняло участие в выборах. Избиратель, в свою очередь, может проконтролировать, что его пара была включена в список.

3 Два протокола электронных выборов

3.1 Протокол Шаума

В 1981 году Шаум предложил первую схему проведения электронных выборов. Хотя она и не удовлетворяет примерно половине требований, впоследствии в некоторых аспектах её удалось улучшить. В этой схеме считается, что организаторы честны. Реализуется идея анонимного канала.

Имеется N организаторов, у каждого есть своя система шифрования с открытым ключом E_i и закрытым ключом D_i $(i = 1, \ldots, N)$. Есть также общая область памяти ("доска бюллетеней"), с которой могут читать все избиратели и все организаторы. Ширина доски (допустимое количество проголосовавших) фиксирована.

Рассмотрим протокол. Выборы начинаются с того, что каждый участник посылает на доску свой зашифрованный голос, к которому применены в определённой последовательности все открытые ключи организаторов (т.е. посылается $E_1(E_2(\ldots E_N(K_i)))$, где K_i — зашифрованный голос i-го избирателя). Организаторы по очереди снимают своё шифрование (j-й организатор оставляет после себя от голоса i-го избирателя $E_{j+1}(E_{j+2}(\ldots E_N(K_i))))$ и случайным образом переставляют сообщения местами, после чего записывают полученную последовательность сообщений на доску в $(j+1)$-ю строчку. После N раундов получаем список голосов, многократно переставленных между собой. Ни один организатор не знает, какими перестановками пользовались другие; поэтому, если все организаторы не сговорятся, невозможно будет понять, где чей голос.

Обсуждение:

— Хорошо, но $(j+1)$-й организатор знает $E_{j+1}(E_{j+2}(\dots E_N(K_i)))$ для всех i. Поэтому он, применив известный ему открытый ключ E_j и сравнив полученную последовательность с предыдущей строчкой, может понять, какую перестановку использовал предыдущий организатор. Более того, проделав эту же операцию многократно, он может узнать всё о перестановках в предыдущих строках.
— Проблема решается очень просто – добавлением в шифруемые сообщения случайных строк. Например, в первой строке публикуется $E_1(E_2(E_3(K_i, r_3), r_2), r_1)$, во второй – $E_2(E_3(K_i, r_3), r_2)$, в третьей – $E_3(K_i, r_3)$, где r_j – случайные последовательности битов. Тогда по следующей строке невозможно восстановить переставленное содержимое предыдущей.

Напомним, в нижней строке находятся зашифрованные избирателями голоса в перепутанном порядке. Теперь избиратель может посмотреть на этот список и, не обнаружив в нём своего голоса (вид которого он знает), заявить об этом организаторам. Более того, проследив всю трассу расшифровки своего голоса, избиратель может сказать, какой из организаторов ошибся (или сжульничал).

Далее избиратели могут посылать открытые голоса, конкатенированные с соответствующими зашифрованными голосами K_i (даже не обязательно накладывать на них все открытые ключи E_j). При этом, очевидно, избиратель полностью контролирует правильный учёт своего голоса.

3.2 Недостатки схемы Шаума

Во-первых, если обнаружены ошибки (возможно, кто-то из организаторов таким способом намеренно сорвал выборы), то выборы придётся проводить заново, а вся информация о голосах уже раскрыта. Во-вторых, не выполнено свойство неподтверждаемости. В-третьих, объединившись, организаторы могут узнать, кто как голосовал, ещё до присылки открытых голосов. Наконец, легко скопировать чужой голос. Последняя проблема решается подписыванием зашифрованного голоса индивидуальной подписью. Если же подписи нет, то первый избиратель, добравшийся до компьютера, имеет шанс проголосовать за всех, а любой избиратель может проголосовать за не принявшего участия в выборах.

А как предотвратить мошенничество со стороны избирателя, который утверждает, что его голос не подсчитан, хотя в действительности это не так? Казалось бы, выход есть: избиратели должны опубликовать хеш своих случайных битов, тогда к выделенным организаторами случайным битам можно будет применить хеш-функцию и убедиться в нечестности голосующего. Но ничто не мешает избирателю сразу опубликовать ложный хеш. Можно решать проблему при помощи идентификации, однако под угрозой оказывается анонимность.

3.3 FOO-схема

Опишем теперь FOO-схему (”схему трёх японцев”). В ней выделяются два организатора: ”Раздающий бюллетени” и ”Считающий голоса”. (Могут быть и другие организаторы, задействованные в анонимном канале – см. протокол Шаума.)

Сначала каждый избиратель шифрует свой голос своим ключом и вслепую подписывает этот шифротекст у раздающего. (Кстати, заметим, что голоса по-английски называются `ballots`.) Раздающий при этом ведёт список проголосовавших псевдонимов. Подписанные голоса отдаются считающему, который публикует их в виде списка. На этом этапе избиратели могут проверить, что их голос включён в список (и пожаловаться, если не включён). Когда избиратель станет доволен списком голосов, он отправляет по анонимному каналу номер своего голоса в списке и ключ для его расшифровки. (Это действие так долго откладывалось для того, чтобы не были известны промежуточные результаты.) В конце концов голоса расшифровываются, публикуются (в расшифрованном виде), подсчитываются результаты.

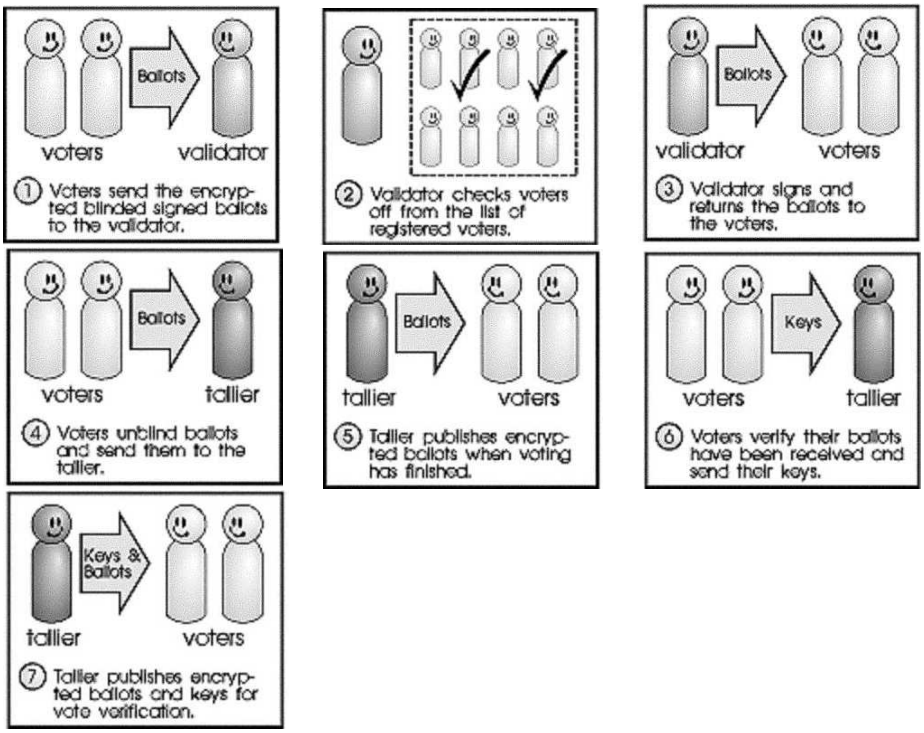

Рис. 2. FOO-схема

3.4 Анализ FOO-схемы

Для проверки того, что пришедший избиратель имеет право голоса, он должен предъявить раздающему свою электронную подпись (аналог паспорта).

В схеме выполнены требования контроля над избирателями (осуществляется у раздающего), тайны голоса (анонимный канал), индивидуального контроля (избиратель проверяет наличие своего голоса в списке). Результаты открываются только после завершения выборов.

Не выполняется требование универсального контроля (к примеру, если человек зарегистрировался, но не голосовал, организаторы могут добавить фиктивный голос, якобы принадлежащий ему). Ясно также, что не выполнено требование неподтверждаемости.