УДК 004.056.5

КОНФИДЕНЦИАЛЬНОСТЬ ВЫБОРА В СИСТЕМАХ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

М.А. Казловский

Белорусский государственный университет,
пр. Независимости 4, 220030, г. Минск, Беларусь, mkazl@yahoo.com

В работе рассматривается проблема обеспечения конфиденциальности выбора в системах электронного голосования. Выполнен аналитический обзор криптографических механизмов, обеспечивающих выполнение конфиденциальности выбора. Построены ограничения на использование сочетаний данных механизмов, в результате чего получены оптимальные наборы. Приведены примеры использования этих наборов в реальных системах электронного голосования.

***Ключевые слова*:** Электронное голосование; конфиденциальность выбора; доказательство с нулевым разглашением; mix сети; гомоморфное шифрование.

FAIRNESS IN ELECTRONIC VOTING SYSTEMS

M. A. Kazlouski

Belarusian State University, 4 Nezavisimosti Avenue, Minsk, 220030, Belarus,
mkazl@yahoo.com

The paper deals with the problem of ensuring the fairness in electronic voting systems. An analytical review of cryptographic mechanisms that ensure the fairness is carried out. Restrictions on the use of combinations of these mechanisms are built, as a result, optimal sets are obtained. Examples of the use of these sets in real electronic voting systems are given.

***Keywords*:** Electronic voting; fairness; zero-knowledge proof; mix networks; homomorphic encryption.

Введение

В процессе голосования избиратель, как правило, получает бюллетень, заполняет его и опускают в урну для голосования. Не нарушая общности, можно считать, что до завершения процедуры голосования никто не имеет доступа к урне и, соответственно, не может узнать промежуточные итоги голосования. Данное требование позволяет обеспечить объективность голосования: избиратели не смогут учитывать текущие результаты при принятии решений о своем участии в выборах и схеме заполнения бюллетеня, а заинтересованные лица не будут иметь соблазна осуще-

ствить подкуп избирателей, если, согласно текущим результатам, для победы нужного им варианта не хватает сравнительно небольшого числа голосов.

В случае проведения электронного голосования такой подход может не сработать, так как обычно сразу после публикации бюллетеня доступ к его содержимому имеют все участники избирательного процесса (избиратели, избирательная комиссия, наблюдатели). Таким образом, возникает необходимость в защите содержимого бюллетеня, которая обеспечит его конфиденциальность до завершения процедуры голосования. На английском языке такое свойство протокола электронного голосования называется «fairness», в качестве русского аналога мы будем использовать словосочетание «конфиденциальность выбора».

В научных статьях, посвященным децентрализованным системам электронного голосования, вопрос соблюдения конфиденциальности выбора обычно либо не поднимается вовсе, либо свойство выполняется неявно (например, если система голосования обеспечивает защиту от принуждения, то обязательно будет достигаться и конфиденциальность выбора). Данная работа рассматривает системы электронного голосования в контексте соблюдения указанного свойства. Выделены криптографические механизмы, которые могут использоваться для достижения конфиденциальности выбора, изучена их сочетаемость и установлены оптимальные сочетания. Найденные наборы соотнесены с известными системами электронного голосования.

1. Криптографические механизмы при обеспечении конфиденциальности выбора

Единственным возможным вариантом защиты содержимого бюллетеня является его шифрование. Однако организовать шифрование можно используя различные криптографические механизмы. Рассмотрим криптографические механизмы, между вариантами реализации которых необходимо выбирать при проектировании системы обеспечении конфиденциальности выбора.

1) *Выполняющий расшифрование субъект*. Расшифрование бюллетеня может осуществляться:

a. избирателем – используется симметричный или ассиметричный алгоритм шифрования с публикацией после завершения голосования секретного или личного ключа соответственно;

b. избирательной комиссией – используется асимметричный алгоритм шифрования: открытый ключ публикуется до начала голосования

и используется избирателем для зашифрования, а личный ключ используется избирательной комиссией для расшифрования.

2) *Формат публикации бюллетеня.* Избиратель всегда публикует зашифрованный бюллетень. При этом:

a. ничего дополнительно не публикуется;

b. дополнительно публикуются неинтерактивные доказательства с нулевым разглашением, подтверждающие корректность зашифрованного значения и процедуры зашифрования.

3) *Подтверждение корректности расшифрования.* Если расшифрование выполняется избирательной комиссией, то подтверждение корректности расшифрования может осуществляться путем:

a. публикации личного ключа – любой желающий может проверить результаты расшифрования;

b. публикации неинтерактивных доказательств с нулевым разглашением для расшифрованного бюллетеня или суммы бюллетеней – любой желающий может проверить корректность опубликованных доказательств.

4) *Подсчет результатов.* Если расшифрование выполняется избирательной комиссией и алгоритм шифрования обладает гомоморфизмом, то подсчет результатов может осуществляться путем:

a. суммирования результатов в расшифрованных по отдельности бюллетенях;

b. суммирования бюллетеней в зашифрованном виде с последующим расшифрованием итогового результата голосования.

5) *Обработка бюллетеней.* Если расшифрование выполняется избирательной комиссией, то при обработке бюллетеней:

a. ничего дополнительно не выполняется;

b. избирательная комиссия осуществляет перемешивание бюллетеней с помощью mix сетей.

6) *Организация избирательной комиссии.* Если расшифрование выполняется избирательной комиссией, то она может организовываться различными способами:

a. централизованная комиссия, личный ключ которой разделен на несколько частичных секретов;

b. децентрализованная комиссия, в которой у каждого члена комиссии есть свой личный ключ.

2. Оптимальные сочетания криптографических механизмов при обеспечении конфиденциальности выбора

Комбинируя различные варианты описанных выше криптографических механизмов, можно получить $2^6 = 64$ сочетания. Но часть этих сочетаний невозможна, а часть не имеет смысла. Сформулируем правила, позволяющие снизить число рассматриваемых сочетаний:

- Если выбран вариант 1.a, то механизмы 3 – 6 не имеют смысла, т.к. избирательная комиссия не участвует в расшифровании бюллетеней.
- Если выбран вариант 1.a или вариант 3.a, то нет смысла выбирать вариант 2.b, т.к. в данном случае нет необходимости блокировать некорректные бюллетени на этапе голосования.
- Если выбран вариант 3.a, то нет смысла выбирать вариант 4.b, т.к.
  в случае раскрытия личного ключа избирательной комиссии любой желающий сможет расшифровать все бюллетени по отдельности.
- Если выбран вариант 4.b, то должен использоваться вариант 2.b, т.к. иначе избиратель может зашифровать некорректные данные и подсчет голосов будет проведен некорректно.
- Если выбран вариант 5.b, то обязательно должен быть выбран вариант 2.b, т.к. для использования mix сетей необходимо, чтобы бюллетень имел корректный формат.
- Если выбран вариант 5.b, то обязательно должен быть выбран вариант 3.b, т.к. если проводимые избирательной комиссией перемешивания не будут сопровождаться доказательствами, то возможно нарушение принципа состоятельности голосования.
- Если выбран вариант 5.b, то нет смысла выбирать вариант 4.b, т.к.
  получение итогового результата с помощью гомоморфного шифрования после использования mix сетей не дает дополнительных гарантий безопасности.
- Если выбран вариант 5.b, то обязательно должен быть выбран вариант 6.b, т.к. использование mix сетей предполагает перемешивание бюллетеней каждым членом комиссии, что невозможно для централизованной комиссии.
- Если выбран вариант 6.a, то нет смысла выбирать вариант 3.b, т.к. доказательства с нулевым разглашением нужны лишь при

частичном расшифровании бюллетеня, что характерно для децентрализованной комиссии.

После применения сформулированных выше ограничений к списку из 64 возможных сочетаний криптографических механизмов, получим семь возможных наборов сочетаний: усеченный набор [1.a, 2.a], который обозначим как (0) и ряд полных наборов:

- [1.b, 2.a, 3.a, 4.a, 5.a, 6.a] – (1);
- [1.b, 2.a, 3.a, 4.a, 5.a, 6.b] – (2);
- [1.b, 2.a, 3.b, 4.a, 5.a, 6.b] – (3);
- [1.b, 2.b, 3.b, 4.a, 5.a, 6.b] – (4);
- [1.b, 2.b, 3.b, 4.a, 5.b, 6.b] – (5);
- [1.b, 2.b, 3.b, 4.b, 5.a, 6.b] – (6).

Разделим найденные наборы на классы. По типу субъекта, выполняющего расшифрование голосов, можно выделить три класса. Класс A – расшифрование выполняется пользователем, в который входит набор (0), класс B – расшифрование выполняется централизованной избирательной комиссией, в который входит набор (1) и класс C – расшифрование выполняется децентрализованной избирательной комиссией, в который входят наборы (2) – (6). В свою очередь класс C можно разделить на 3 подкласса: подкласс C1 – протокол голосования использует mix сети, в который входит набор (5), подкласс C2 – протокол голосования использует гомоморфное шифрование, в который входит набор (6) и подкласс C3 – протокол голосования не использует дополнительных криптографических механизмов в процессе обработки зашифрованных голосов, в который входят наборы (2) – (4).

Таким образом, все классы и подклассы, кроме подкласса C3 содержат по одному набору. Подкласс C3 состоит из трех наборов, при этом с ростом номера набора наблюдается увеличение вычислительной сложности протокола голосования. Так набор (3) отличается от набора (2) тем, что комиссия не раскрывает ключ расшифрования, при этом предоставляя доказательства корректности расшифрования. А набор (4) отличается от набора (3) тем, что избиратель дополнительно строит доказательства корректности содержимого бюллетеня. Отметим, что в контексте свойства конфиденциальность выбора такие «усиления» видятся избыточными, так как добавляют дополнительную вычислительную нагрузку при формировании и проверке доказательств, не предоставляя при этом дополнительных гарантий безопасности. Однако, возможно, они могут быть полезны для поддержания каких-либо других свойств протоколов электронного голосования.

Среди популярных систем электронного голосования большинство входит или в подкласс C1 (например, JCJ [1], Civitas [2]), или в подкласс C2 (например, Cobra [3], система голосования на выборах в РФ [4]). Это связно с тем, что протокол электронного голосования должен поддерживать не только конфиденциальность выбора, но и ряд других криптографических свойств, таких как анонимность и защита от принуждения, для выполнения которых и используются такие криптографические механизмы как mix сети и гомоморфное шифрование.

Таким образом, получена классификация криптографических механизмов, используемых для соблюдения свойства конфиденциальности выбора, которую можно использовать при проектировании и реализации систем электронного голосования, обладающих данным свойством.

Библиографические ссылки

1. Juels A., Catalano D., Jakobsson M. Coercion-resistant electronic elections [Electronic resource]. URL: https://eprint.iacr.org/2002/165.pdf
2. Clarkson M.R., Chong S., Myers A.C. Civitas: toward a secure voting system [Electronic resource]. URL: https://www.cs.cornell.edu/andru/papers/civitas-tr.pdf
3. Essex A., Clark J., Hengartner U. Cobra: toward concurrent ballot authorization for internet voting [Electronic resource]. URL: https://users.encs.concordia.ca/~clark/papers/2012_evt.pdf
4. Программно-технический комплекс, обеспечивающий дистанционное электронное голосование избирателей (участников референдума) вне зависимости от места их нахождения. Описание протокола ДЭГ к выборам, голосование на которых состоится 17, 18 и 19 сентября 2021 г. [Электронный ресурс]. URL: https://deg.rt.ru/landing/materials/7/deg2021_protocol.pdf