УДК 003.26 + 004.057.4 Вестник УрФО № 4(22) / 2016, с. 21–25

Бортник Д. А., Кротова Е. Л., Савочкина А. А.

КЛАССИФИКАЦИЯ РЕАЛИЗАЦИЙ ПРОТОКОЛОВ ТАЙНОГО ГОЛОСОВАНИЯ

В статье приведены основные требования, предъявляемые к протоколам тайного голосования. Рассмотрены несколько разновидностей абстрактных протоколов – простейший протокол голосования с центром подсчета голосов, усложненный протокол голосования с центром подсчета голосов, протокол голосования со слепыми подписями. Указаны основные недостатки данных схем голосования. Далее рассмотрены два реальных протокола голосования – Fujioka-Okamoto-Ohta и He-Su. Также описаны их преимущества и недостатки.

Ключевые слова: *протокол тайного голосования, слепая подпись, протокол He-Su, протокол Fujioka-Okamoto-Ohta.*

Bortnik D. A., Krotova E. L., Savochkina A. A.

CLASSIFICATION OF THE SECRET VOTING PROTOCOLS

The main requirements imposed to protocols of ballot are adduced in the article. The several versions of abstract protocols are considered. For example, the elementary protocols of ballot with counting center, complicated protocol of ballot with counting center and protocols with blind signatures. The main disadvantages of these schemes of ballot are specified. Then two present protocols of ballot are considered – Fujioka-Okamoto-Ohta and He-Su. Their advantages and disadvantages are also described.

Keywords: *protocol of ballot, blind signature, protocol He-Su, protocol Fujioka-Okamoto-Ohta.*

Введение

В некоторых странах, например, Эстонии, Бельгии, Франции, Норвегии и других[1], возможность электронного голосования предусмотрена законодательством. Однако следует отметить, что электронное голосование никогда не будет внедрено, если не будет разработан надежный протокол, удовлетворяющий ключевым требованиям[2]. Таким образом, протоколы тайного голосования являются одним из типов современных прикладных криптографических протоколов.

Можно выделить несколько основных требований, предъявляемых к данным протоколам:

1. Голосовать могут только легальные избиратели;

2. Каждый избиратель может проголосовать только один раз;

3. Избиратели не могут проголосовать вместо кого-то другого;

4. Голосование является тайным;

5. Никто не может изменить чужой голос;

6. Каждый голосующий может проверить, что его голос был учтен при подведении итогов.

Протоколы тайного голосования можно разделить на 2 группы: децентрализованные и централизованные.

В децентрализованных протоколах взаимодействуют только избиратели без участия какого-либо центрального органа. Недостатком протоколов этой группы является их сложность с точки зрения количества вычислений и количества пересылаемой информации, из-за чего уже при сравнительно небольшом k они практически невыполнимы[2]. В централизованных протоколах создается центр подсчета голосов. Особенностью протоколов данной группы является тот факт, что центр должен быть честным и пользоваться безусловным доверием избирателей[3].

Рассмотрим протоколы обеих групп и выявим их характерные черты.

Простейший протокол голосования с центром подсчета голосов

Данный протокол основывается на схеме ассиметричного шифрования. Электронные выборы с помощью него можно разделить на 3 этапа[2]:

1) Избиратель шифрует свой бюллетень открытым ключом Центральной избирательной комиссии (ЦИК)

2) Избиратель посылает зашифрованный бюллетень ЦИК

3) ЦИК расшифровывает бюллетень закрытым ключом, подводит итоги и опубликовывает результаты

На рисунке 1 изображен принцип работы протокола. Public key и private key – открытый и закрытый ключи ЦИК соответственно.

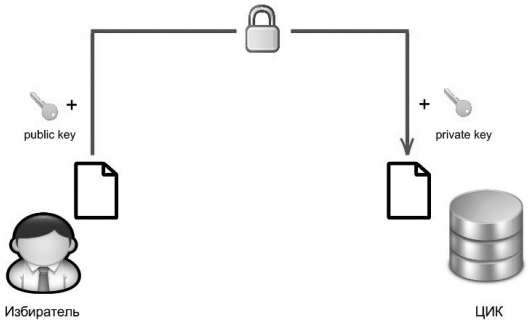

Рис. 1. Простейший протокол электронного голосования

У этой схемы отсутствует процедура аутентификации избирателей, из-за чего становится невозможным отследить легальность голосующих и их уникальность (любой избиратель может проголосовать сколько угодно раз). Положительной стороной протокола является невозможность изменить голос другого избирателя, но, ввиду описанных выше недостатков, это является не таким важным.

Усложненный протокол голосования с центром подсчета голосов

Кроме ассиметричного шифрования в усложненном протоколе используется электронная подпись избирателя. Процесс голосования можно разбить на 4 этапа[2]:

1) Избиратель подписывает бюллетень своим закрытым ключом;

2) Избиратель шифрует свой бюллетень открытым ключом Центральной избирательной комиссии (ЦИК);

3) Избиратель посылает зашифрованный бюллетень ЦИК;

4) ЦИК расшифровывает бюллетень, проверяет подпись, подводит итоги и опубликовывает результаты.

На рисунке 2 изображен принцип работы усложненного протокола. Public key 1 и private key 1 –ключи избирателя, public key 2 и private key 2 –ключи ЦИК.

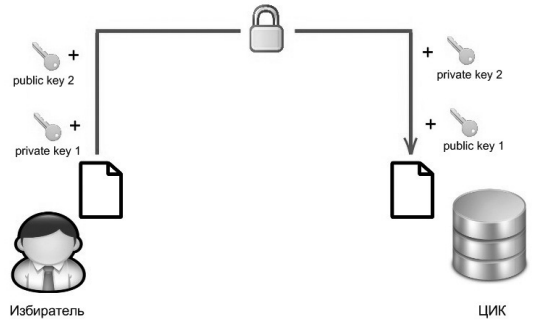

Рис. 2. Усложненный протокол электронного голосования

Данная схема позволяет аутентифицировать избирателя и удостовериться в том, что каждый голосовал не более одного раза. В этом алгоритме присутствуют недостаток – ЦИК знает, за кого проголосовал каждый избиратель. Чтобы данный протокол работал, необходимо, чтобы избиратели полностью доверяли ЦИК.

Протокол голосования со слепыми подписями

Аутентификацию избирателей, не нарушающую принципа тайного голосования, можно реализовать с использованием слепой подписи[4, 5].

В выборах участвуют три стороны: избиратель, валидатор и счетчик (например, ЦИК). Валидатор – сторона, проверяющая уникальность избирателя и подписывающая его бюллетень. Счетчик – сторона, подсчитывающая результаты голосования. Валидатор не должен знать кандидата, за которого проголосовал избиратель, а счетчик не должен знать личность избирателя.

Процесс голосования можно разделить на 7 этапов.

1) Избиратель и валидатор устанавливают надежное соединение со взаимной аутентификацией;

2) Избиратель создает бюллетень, голосует за произвольного кандидата, добавляет к бюллетеню уникальную последовательность и хеширует бюллетень;

3) Избиратель добавляет к хешу маскирующий множитель и отправляет на подпись к валидатору;

4) Валидатор проверяет уникальность избирателя (избиратель не должен голосовать более одного раза) и подписывает полученное сообщение;

5) Избиратель извлекает маскирующий множитель и получает корректную подпись для хеша бюллетеня;

6) Избиратель анонимно отправляет подписанный хеш счетчику;

7) Счетчик проверяет подпись и подводит итоги.

Слепую подпись можно реализовать разными способами, например, с помощью алгоритма RSA[2] или с использованием криптографии на эллиптических кривых[6].

У описанной выше схемы также присутствуют недостатки. Если на этапе (6) избиратель отошлет бюллетень не анонимно, ЦИК сможет узнать, кто за кого голосовал. Кроме того, ЦИК может создать любое число правильных и подписанных бюллетеней и смошенничать, прислав их сама себе. И если какой-либо избиратель обнаружит, что бюллетень был подменен, он не сможет этого доказать[2].

Рассмотрим также несколько реальных протоколов тайного голосования.

Протокол Fujioka-Okamoto-Ohta

Протокол Fujioka-Okamoto-Ohta[7] основывается на рассмотренном выше протоколе голосования со слепыми подписями. В голосовании так же участвуют избиратель, валидатор (администратор) и счетчик.

Процесс голосования можно разбить на 7 этапов:

1) - Администратор утверждает списки легитимных избирателей.

2) - Избиратель генерирует пару ключей e_{public} и $e_{private}$ и секретный ключ e_{secret};

- Ставит свой голос в бюллетене B;

- Шифрует бюллетень ключом e_{secret} – encrypt(e_{secret}, B);

- Маскирует зашифрованный бюллетень – blind(encrypt(e_{secret}, B));

- Шифрует результат личным ключом - blind(sign($e_{private}$, encrypt(e_{secret}, B)));

- Отправляет полученное сообщение администратору.

3) - Администратор создает пару ключей v_{public} и $v_{private}$;

- Удостоверяется в действительности бюллетеня;

- Подписывает полученное сообщение M личным ключом – sign($v_{private}$, M);

- Возвращает результат избирателю.

4) - Избиратель снимает с подписанного бюллетеня маскировку в силу коммутативности слепой подписи - sign($v_{private}$, sign($e_{private}$, encrypt(e_{secret}, B)));

- Отправляет получившееся сообщение счетчику (анонимно);

5) - Счетчик проверяет подписи избирателя и администратора;

- Помещает зашифрованный бюллетень encrypt(e_{secret}, B) в список, который будет опубликован после того, как закончится заранее оговоренный срок.

6) - Избиратель анонимно посылает счетчику ключ e_{secret} и номер строки, в которой находится его бюллетень.

7) - Счетчик расшифровывает бюллетень;

- Подсчет результатов.

Как указано в примечании авторов[7], возможна ситуация, когда избиратель посылает неверный ключ, который не может расшифровать бюллетень. В этом случае невозможно определить, кто является нечестным, избиратель или счетчик. Для предотвращения этого избирателям следует посылать ключи третьей, независимой стороне, например, кандидатам выборов, которые, скорее всего, не сотрудничают.

Протокол He-Su

Еще одним протоколом, основанным на идее слепой подписи, является протокол He-Su. Он удовлетворяет почти всем предъявляемым требованиям. В данном алгоритме участвуют три стороны – избиратель, администратор и счетчик. Но, в отличие от протокола Fujioka-Okamoto-Ohta, в схеме He-Su подписывается ключ избирателя, а не бюллетень.

Процесс голосования можно разделить на 10 этапов[8]:

1) - Избиратель генерирует пару ключей - D_v (закрытый) и E_v (открытый);

- Генерирует случайное число R (маскирующий множитель);

- Вычисляет $E_a(R) * (h(E_v))$, где E_a – открытый ключ администратора, h – хеш-функция;

- Отправляет результат администратору.

2) - Проверяет приемлемость избирателя;

- Подписывает принятое сообщение: $D_a(E_a)R * D_a(h(E_v)) = R * D_a(h(E_v))$, где D_a – личный ключ администратора.

- Отправляет результат избирателю;

- Публикует список авторизованных избирателей.

3) - Избиратель убирает маскирующий множитель R из полученного сообщения;

- Проверяет равенство $E_a(D_a(h(E_v))) = h(E_v)$;

- При верном равенстве избиратель убеждается в том, что имеет подписанный ключ.

4) - Избиратель отправляет счетчику E_v и $D_a(h(E_v))$.

5) - Счетчик проверяет равенство $E_a(D_a(h(E_v))) = h(E_v)$;

- При верном равенстве счетчик авторизует ключ E_v;

- Публикует список авторизованных ключей.

6) - Избиратель отправляет счетчику E_v, $K_v(B_v)$, $D_v(h(K_v(B_v)))$, где K_v – секретный ключ избирателя (для симметричного шифрования), B_v – бюллетень;

7) - Счетчик проверяет, является ли ключ E_v авторизованным;

- Проверяет равенство $E_v(D_v(h(K_v(B_v)))) = h(K_v(B_v))$;

- При положительном результате публикует E_v, $K_v(B_v)$, $D_v(h(K_v(B_v)))$.

8) - Избиратель проверяет в опубликованном счетчиком листе наличие записи о своем голосе (из пункта 7);

- В случае отсутствия записи обращается в соответствующие органы.

9) - Избиратель отправляет счетчику E_v, K_v, $D_v(h(K_v))$;

10) - Счетчик проверяет равенство $E_v(D_v(h(B_v))) = h(B_v)$;

- В случае равенства получает бюллетень $K_v^{-1}(K_v(B_v)) = B_v$;

- Публикует информацию: B_v, $K_v(B_v)$, K_v, $D_v(h(K_v(B_v)))$, $D_v(h(K_v))$, E_v.

К преимуществам протокола He-Su можно отнести возможность избирателя изменить свой голос во время выборов. Избиратель может сделать это, не раскрывая свой бюллетень. Кроме того, протокол достаточно прост и имеет малую вычислительную сложность[8].

Заключение

Протоколы тайного голосования основываются на широко известных и проверенных алгоритмах шифрования, хеширования, цифровой подписи. Но для претворения их в жизнь необходимо учесть множество требований и факторов. Реализация какого-либо требования, предъявляемого к данным протоколам, может стать хорошей задачей для дальнейшего исследования .

Примечания

1. Антонов Я. В. Международный опыт электронного голосования // Сборник конкурсных работ в области избирательного права и избирательного процесса выполненных студентами, аспирантами в 2010/2011 учебном году. М.: РЦОИТ. 2011.

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М.: Триумф, 2002. — 816 с.

3. Введение в криптографию / Под общ. ред. В. В. Ященко. - 4-е изд., доп. М.: МЦНМО, 2012. - 348 с.

4. Клюжев А. Электронное голосование [Электронный ресурс] // Gosbook.ru. – URL: http://www.gosbook.ru/node/28337 (дата обращения: 13.06.2016).

5. Иванов Е. Слепая подпись на основе ГОСТ 34.10-2001 [Электронный ресурс] // Habrahabr.ru. – URL: https://habrahabr.ru/post/136022/ (дата обращения: 13.06.2016).

6. Козина Г. Л., Никулищев Г. И. Протокол слепой подписи на основе ГОСТ Р 34.10-2012 [Электронный ресурс] // Aticmd.md. – URL: http://www.aticmd.md/wp-content/uploads/2014/04/V_2_33_MMOTI_Kozina.pdf (дата обращения: 13.06.2016).

7. Fudjioka A., Okamoto T., Ohta K. A Practical Secret Voting Scheme for Large Scale Elections [Электронный ресурс] // Csail.mit.edu. – URL: https://people.csail.mit.edu/rivest/voting/papers/FujiokaOkamotoOhta-APracticalSecretVotingSchemeForLargeScaleElections.pdf (дата обращения: 17.06.2016).

8. He Q., Su Z. A New Practical Secure e-Voting Scheme [Электронный ресурс] // Cs.cmu.edu. – URL: http://www.cs.cmu.edu/~qihe/paper/e_voting (дата обращения: 17.06.2016).

БОРТНИК Дмитрий Аркадьевич, студент Пермского национального исследовательского политехнического университета. 614990, г. Пермь, Комсомольский пр-кт, 29. E-mail: bortnikdmitriy@mail.ru.

КРОТОВА Елена Львовна, кандидат физико-математических наук, доцент кафедры высшей математики Пермского национального исследовательского политехнического университета. 614990, г. Пермь, Комсомольский пр-кт, 29. E-mail: lenkakrotova@yandex.ru.

САВОЧКИНА Анна Александровна, старший преподаватель кафедры высшей математики Пермского национального исследовательского политехнического университета. 614990, г. Пермь, Комсомольский пр-кт, 29. E-mail: aidas_76@mail.ru.

BORTNIK Dmitrii Arkad'evich, is a student of Perm National Research Polytechnic University. 614990, Perm, 29, Komsomolsky pr. E-mail: bortnikdmitriy@mail.ru.

KROTOVA Elena L'vovna, is a Ph. D. in Physico-Mathematical Sciences, Associate Professor, Department of Higher Mathematics, Perm National Research Polytechnic University. 614990, Perm, 29, Komsomolsky pr. E-mail: lenkakrotova@yandex.ru.

SAVOCHKINA Anna Alexandrovna, is a senior lecturer, Department of Higher Mathematics, Perm National Research Polytechnic University. 614990, Perm, 29, Komsomolsky pr. E-mail: aidas_76@mail.ru.