Применение криптографических протоколов для проведения выборов

О.А. Басов, А.А. Болотов

В статье рассматривается приложение криптографических протоколов в области финансовых расчетов и проведения выборов.

Введение

В настоящей статье рассматривается приложение криптографических протоколов в области секретных банковских расчетов и проведения выборов и тайных голосований ([2], [3]). Предлагается возможное применение протокола из [5] для электронных денежных перечислений как базового для построения протокола проведения широкомасштабных выборов. В результате достигается выигрыш в эффективности в сравнении с протоколом для тайных голосований из [6]. При практическом использовании предлагаемого протокола воспрепятствовать возможным покупкам голосов избирателей можно аналогично [4].

В первом параграфе этой статьи даются определения основных используемых понятий и терминов, а именно, понятия криптографической функции и криптографического протокола, открытого ключа и электронной подписи и приводится алгоритм шифрования в криптосистеме RSA. Более полные сведения о криптографии с открытым ключом можно почерпнуть из учебника [1]. Во втором параграфе изложен протокол получения случайной электронной подписи. В третьем параграфе обсуждаются требования к протоколам

голосования и приводится план построения протокола на основе базового. Окончательно протокол голосования строится в четвертом параграфе.

Пользуясь случаем, авторы хотели бы поблагодарить заведующего кафедрой МаТИС академика АТН РФ В.Б. Кудрявцева за поддержку темы, а также профессора В.А. Буевича и доцента А.А. Часовских за дружеские и плодотворные дискуссии.

1. Криптографические функции и протоколы

В этом параграфе неформально излагаются некоторые основные понятия криптографии с открытым ключом. В дальнейшем мы подразумеваем под *эффективным*, или *простым алгоритмом (вычисления)* такой (возможно, вероятностный) алгоритм, для которого (со сколь угодно близкой к единице вероятностью верности полученного результата) время вычислений (для получения результата) ограничивается полиномом от размера входного блока информации. Также под *сложным алгоритмом* подразумевается то, что этот алгоритм имеет на практике существенно более чем полиномиальный рост объема производимых вычислений в зависимости от величины входного блока информации.

Под *криптографическим протоколом* понимается заранее оговоренная последовательность вычислений и информационного обмена, производимых его участниками, с целью получения некоторой информации каждым из них в соответствии с предварительными договоренностями. При этом каждый из них с целью получения дополнительной информации (большей, чем оговорено в протоколе) может выступить в качестве *криптоаналитика*, или нарушителя протокола. Для этого возможно или применение иных методов вычислений, или одностороннее нарушение предписанной последовательности действий. Если доказано, что эти усилия не могут быть эффективными, протокол считается *криптостойким*. В случае, если прикладная задача допускает перехват информации техническими средствами, при анализе криптостойкости нужно добавить еще одного участника, которому считается доступной вся информация, проходящая по уязвимым средствам связи.

Он автоматически считается пассивным нарушителем, если может только принимать информацию, или активным, если может сам посылать сообщения, выдавая их за сообщения других участников.

Заметим, что участники криптографических протоколов по криптографической традиции, как правило, называются либо именами, либо в соответствии с их должностями, предполагаемыми протоколом.

Мы будем называть функцию $f : X \to Y$ с обратной $f^{-1} : Y \to X$ *односторонней функцией*, если существует эффективный алгоритм (возможно, вероятностный) вычисления f и не существует (возможно, неизвестен) алгоритм вычисления f^{-1}. Одностороннюю функцию, перестающую быть односторонней при раскрытии некоторой дополнительной секретной информации K об этой функции, будем называть *криптографической*.

Пусть теперь задано семейство функций $f_K : X \to Y$ и $g_K : Y \to X$, где X, Y – некоторые множества , $K \in \mathbf{K}$ – индексы из множества $\mathbf{K}$, и функции f_K и g_K взаимно обратны. Пусть при известном K функции f_K и g_K могут быть вычислены эффективно, а если K не известен, то эффективно вычисляется лишь f_K, а алгоритм вычисления $g_K(x)$ сложен. Тогда мы будем называть f *криптографической функцией с открытым ключом*, подразумевая под *открытым ключом* функцию f_K (или какой-нибудь ее идентификатор, отличающий ее от функций ее семейства), а *закрытым ключом* – функцию g_K и индекс K (или соответствующие алгоритмы их вычисления).

Теперь предположим, что некто (будем называть ее Алисой) выбрала два больших (скажем, по 500 бит) простых числа p и q, нашла их произведение $n = pq$, затем вычислила функцию Эйлера φ от этого произведения:

$$\varphi(n) = (p-1)(q-1),$$

после чего выбрала любое число $v < n$, взаимно простое с $\varphi(n)$. Тогда Алиса может при помощи алгоритма Евклида найти такое d, что

$$vd \equiv 1 \bmod (\varphi(n)), \tag{1.1}$$

и, согласно малой теореме Ферма, возведение x в степень v, а затем в степень d по модулю n дает в итоге то же самое число x:

$$(x^v)^d \equiv x \bmod (n). \tag{1.2}$$

Если Алиса опубликует пару чисел (n, v), то любой другой участник протокола (здесь и далее именуемый Бобом) может теперь послать Алисе шифрованное сообщение, разбивая информацию на блоки из 998 бит и производя над блоками операцию возведения в степень v по модулю n (в результате получаются блоки по 1000 или по 999 бит – в зависимости от длины двоичной записи числа n) и передав их Алисе. Для дешифрования Алиса производит операцию возведения в степень d по модулю n, (числа d при этом она не раскрывает).

Вышеизложенный алгоритм шифрования (дешифрования) широко известен под названием криптосистемы RSA. В роли открытого ключа здесь выступает пара чисел (n, v), в роли ключа дешифрования K – число d либо разложение n на простые. Заметим, что хотя задача дешифрования выглядит, в принципе, легче, чем задача разложения на простые (теоретически можно придумать алгоритм дешифрования, не использующий нахождение числа $\varphi(n)$), но, исходя из доказанной на практике стойкости системы RSA, это в итоге не является проще задачи разложения n на простые сомножители. Известные же в настоящее время алгоритмы разложения имеют порядок экспоненты от некоторой дробной степени числа n и не являются эффективными для достаточно больших n.

С другой стороны, алгоритмы, используемые для построения криптосистемы, являются эффективными.

Из понятия шифрования с открытым ключом естественным образом возникает понятие *цифровой (электронной) подписи*. А именно,

если Алиса опубликовала и зарегистрировала свой открытый ключ f шифрования (оставляя засекреченным ключ дешифрования g), то Боб может, проверив в соответствующем юридическом органе факт регистрации f и договорившись с Алисой о подписании некоторого документа d, получить электронную подпись s по компьютерной сети как

$$s = g(D), \tag{1.3}$$

и доказать подлинность подписи, демонстрируя, что

$$f(s) = D. \tag{1.4}$$

Как вариант, документ может быть также опубликован и зарегистрирован вместе с некоторым уравнением в криптографических функциях

$$f_1(s_1) = f_2(s_2), \tag{1.5}$$

и обязательствами в отношении предъявителя решения (s_1, s_2) этого уравнения. Вместо одного уравнения может быть целая система уравнений от нескольких переменных, но в векторной форме она может быть записана как

$$F(S, D) = 0, \tag{1.6}$$

где F есть некоторая композиция криптографических функций (сама являющаяся криптографической).

Эти обобщения бывают необходимы для использования дополнительных возможностей, даваемых криптографическими протоколами. А именно, результатом некоторого криптографического протокола может быть выдача Алисой Бобу такой подписи S, что Алиса имеет о виде S нулевую информацию. При этом для Боба форма этой подписи является случайной. Если эти свойства S действительно имеют место, мы будем говорить, что выдана *забываемая цифровая подпись* S.

И еще одна деталь, нуждающаяся в реализации – одноразовость предъявления. Если это достигается, например, для забываемой цифровой подписи, то она как средство документооборота приобрета-

ет заметные преимущества перед такими средствами, как расчетная банковская карточка или избирательский бюллетень. Действительно, они имеют ограниченную приватность – расчеты карточкой отслеживаемы банком, который, как говорится, «знает о клиенте больше, чем врач», а судьба урны с избирательными бюллетенями полностью в руках региональных избирательной и наблюдательной комиссий, которые априорно объективны лишь в случае баланса представленных в них сил, что маловероятно для всех регионов в совокупности.

Идея одноразового предъявления реализуема при помощи развития идеи забываемой цифровой подписи. А именно, пусть по-прежнему Алиса подписывает документы Бобу и Биллу, которые предъявляют их Дику или Джеку (при этом не называя своих имен). Позже Дик демонстрирует подписанные документы Алисе, получая за это права, деньги, информацию или что-либо иное, обусловленное протоколом. А Алиса должна контролировать одноразовость подписей, и при ее несоблюдении привлекать нарушителей к ответственности. Для этого она в протоколе выдачи забываемой подписи должна выдать клиенту идентификационный номер U, который не является для нее секретом в момент подписания, в отличие от выдаваемой подписи S. По протоколу предъявления подписи Боб (или Билл) показывает, что S есть решение уравнения $F_0(S) = 0$, и получает от Дика запрос R_1. Далее Боб, не раскрывая U, показывает, что

$$F_1(S, R_1, U) = 0, \tag{1.7}$$

причем эта система сама по себе неразрешима относительно U. Вся эта информация является доказательством обладания подписью и позже передается Диком Алисе. Если же Боб решит позже предъявить эту же подпись Джеку, то он, получив от Джека запрос R_2 и продемонстрировав, что

$$F_1(S, R_2, U) = 0, \tag{1.8}$$

даст Алисе возможность решить систему уравнений

$$F_1(S, R_i, U) = 0, \qquad i = 1, 2 \tag{1.9}$$

относительно U, в то время как каждое в отдельности уравнение в криптографических функциях неразрешимо за приемлемое время.

2. Забываемая электронная подпись

В этом параграфе мы рассмотрим протокол выдачи забываемой электронной подписи по [5]. Этот протокол будет использоваться при построении протокола для широкомасштабных тайных голосований в следующем параграфе.

В протоколе принимают участие Алиса и Боб – последний получает электронную подпись от первой.

Протокол выдачи забываемой электронной подписи

По протоколу считаются опубликованными Алисой открытый RSA-ключ (n, v), v – в разумной степени большое простое из $Z_{\varphi(n)}$, основание g из Z_n^*, и любую одностороннюю функцию $f : Z_n^* \to Z_{\varphi(n)}$. Засекреченными остаются разложение $n = pq$ на простые, $\varphi(n)$ и RSA-ключ дешифрования d, такой, что $vd \equiv 1 \bmod (\varphi(n))$. Все действия выполняются по соответствующим модулям.

Шаг 1.

Боб вычисляет случайные числа a_1, $x \in Z_n^*$, $y \in Z_{\varphi(n)}$ и посылает Алисе сообщение

$$M_1 = a_1 x^v g^y. \tag{2.1}$$

Шаг 2.

Алиса отвечает случайным

$$a_2 \in Z_n^*. \tag{2.2}$$

Шаг 3.

Боб вычисляет $a = a_1 a_2$ и посылает Алисе сообщение

$$M_2 = f(a) - y. \tag{2.3}$$

Шаг 4.

Алиса вычисляет

$$M_3 = (M_1 a^{M_2})^d = (a g^{f(a)})^d$$

и передает его Бобу. Боб выполняет деление

$$A = M_3/x,$$

и получает пару (a, A), обладающую таким свойством –

$$a g^{f(a)} = A^v, \tag{2.4}$$

что и будет необходимым условием для электронной подписи.

Сделаем краткий криптоанализ приведенного протокола.

Для получения информации о паре (a, A), Алиса должна решать систему уравнений (2.1), (2.2) и (2.3) относительно a_1, x, y. Она очень скоро убеждается, что для каждого допустимого a_1 имеется решение, и, коль скоро все a_1 равновероятны, Алиса не обладает относительно распределения $a_1 \in Z_n^*$ большей информацией, чем какой-либо человек с улицы.

Для отклонения от протокола Боб должен получить более одного решения уравнения (2.4) относительно (a, A), имея лишь соотношение

$$M_1 a_2^{M_2} = M_3^v.$$

Детальный криптоанализ этой возможности приводится в [5].

3. Протокол электронного голосования

В этом параграфе приводится полный протокол для проведения широкомасштабного тайного голосования. Предварительно мы изложим некоторые требования к такого рода протоколам.

Постановка задачи создания криптографического протокола для проведения тайных голосований

1. Участники протокола делятся на две группы – Избиратели и Кандидаты. Для каждого Кандидата необходимо обеспечить доказуемость наличия всех бюллетеней, в которых выражена поддержка ему. Для каждого Избирателя необходимо обеспечить возможность убедиться в факте, что Кандидат, поддерживаемый им, воспользовался этим своим правом (относительно бюллетеня *этого* избирателя), а также приватность его бюллетеня (никакое множество скооперировавшихся Кандидатов и Избирателей не может установить его личность).

2. В случае, если какой-либо Избиратель проголосовал дважды, его личность должна быть раскрыта, а бюллетень проигнорирован. Исполнение этого требования должно быть возложено на Кандидатов (формирование каких-либо групп контроля из избирателей за этим требованием не представляется эффективным) и имеет смысл лишь тогда, когда существует хотя бы одна пара в реальности сопричастных Кандидатов, другими словами, если все Кандидаты не являются подставными лицами какого-либо одного.

Заметим, что требование 1 должно выдерживать даже в той сложной ситуации, когда все Кандидаты скооперировались с целью раскрытия личностей Избирателей, и установления распределения поданных голосов. Второе требование в этом случае не столь существенно (коль скоро голосование превращается в шоу по вине Кандидатов, честные Избиратели, следующие своим моральным принципам и, как следствие, исполнившие официально объявленные правила, не пострадают).

Еще некоторые соображения о процедуре голосования. Каждый Избиратель должен получить право на участие после предъявления удостоверения личности в некоторое физически существующее Избирательское Агентство, которое не должно заниматься ничем, кроме проверки удостоверений, получения от Избирателя подписи за факт получения цифрового бюллетеня и подключению Избирателя к компьютерной сети с целью получения цифрового бюллетеня. Заполнить бюллетень и отправить его Избиратель может уже не из Агентства.

Считается, что каждое свое сообщение Кандидаты подписывают своими открытыми ключами, с тем, чтобы никто из них не смог отказаться от факта передачи сообщения.

И последнее. Должна быть устранена и возможность оплаты голосов по предъявлении цифрового бюллетеня с голосом отданным за Кандидата, обещавшего за это деньги.

ГОЛОСОВАНИЕ

(Вступительная фаза)

Кандидаты (m человек) публикуют свои открытые RSA-модули n_i. После этого они проходят дополнительный протокол по получению общего для всех большого простого числа v, меньшего, чем все $\varphi(n_i)$ и публикуют его. В результате получаются их персональные открытые RSA-ключи (n_i, v), и каждый из них вычисляет для себя и оставляет в секрете персональные дешифрующие ключи (n_i, d).

Избиратель, получив опубликованные открытые ключи Кандидатов, является в избирательское Агентство и предъявляет свое удостоверение личности. После этого он получает право вступить в протокол получения цифрового бюллетеня В протоколе получения цифрового бюллетеня считается, что вся информация, адресуемая кому-либо из кандидатов, доступна любому из них, но информация, которая не предназначена для кого-либо, кроме Избирателя, шифруется его открытым ключом, который он передает Кандидатам в начале протокола получения бюллетеня и сам подписывает им свои сообщения.

Протокол получения цифрового бюллетеня

Шаг 1.

Избиратель вычисляет или имеет подготовленными числа

$$a_i, b_i, c_i, x_{b,i}, x_{c,i} \in Z_n^*,$$

$$y_{a,i}, y_{b,i}, y_{c,i} \in Z_v$$

Здесь и далее $i = 1, \ldots, m$. Он посылает Кандидатам числа:

$$x_{a,i}^{v_i} a_{1,i} g_{a,i}^{y_{a,i}}, x_{b,i}^{v_i} b_{1,i} g_{b,i}^{y_{b,i}}, x_{c,i}^{v_i} c_{1,i} g_{c,i}^{y_{c,i}}.$$

Шаг 2.

Кандидаты, получив сообщения, должны ответить набором чисел

$$h_{b,i}, h_{c,i}, a_2.$$

Шаг 3.

Избиратель вычисляет для всех $i = 1, \ldots, m$

$$k \in Z_v, e_{b,i} = f\left(h_{b,i}^{b_1, b_{2,i}}\right) - y_{b,i},$$

$$e_{c,i} = f\left(h_{c,i}^{c_1, c_{2,i}}\right) - y_{c,i},$$

$$a_i = a_{1,i} a_{2,i} f_2(e_{b,i}, e_{c,i})^{k_1},$$

$$e_a = \frac{1}{k_{1,i}} f(a_i) - y_{b,i},$$

и передает соответственно i-ому кандидату числа

$$e_{a,i}, e_{b,i}, e_{c,i},$$

зашифрованные его RSA-ключом.

Шаг 4.

Кандидаты, шифруя RSA-ключом Избирателя свои ответы, вычисляют

$$\bar{C}_i = x_{c,i}^{v} c_{1,i} g_{c,i}^{y_{c,i}} c_{2,i} g_{c,i}^{e_{c,i}}, \bar{B}_i = x_{b,i}^{v} b_{1,i} g_{b,i}^{e_{b,i}},$$

$$\bar{A}_i = x_{a,i}^{v} a_{1,i} g_{a,i}^{e_{c,i}} f_2(e_{c,i}, e_{b,i}),$$

и передают Избирателю в зашифрованном его RSA-ключом виде числа

$$c_{2,i}, b_{2,i}, k_2, \left(\bar{C}_i^{k_2}, \bar{A}_i\right)^{d_i}, \left(\bar{C}_i^{U} \bar{B}_i\right)^{d_i},$$

где $k_2 \in Z_v^*$ является произведением случайных чисел $k_{2,i} \in Z_{n_i}$, которые генерирует, а потом выдает остальным сначала в зашифрованном (RSA-ключом), а потом в явном виде каждый кандидат. Таким образом, k с точки зрения каждого участника есть случайная величина, равномерно распределенная в Z_v^*.

После этого Избиратель вычисляет числа

$$c_i = c_{1,i}c_{2,i}; b_{1,i}b_{2,i}; k = k_1k_2; A_i = \frac{\bar{A}_i}{x_{a,i}}; B_i = \frac{\bar{B}_i}{x_{b,i}}; C_i = \frac{\bar{C}_i}{x_{c,i}}.$$

(Конец протокола)

Заметим, что все возведения в степень Избиратель производит по модулю v, домножая впоследствии на соответствующие основания в соответствующих степенях.

Ясно, что тройки из пар (a_i, A_i), (b_i, B_i), (c_i, C_i) могут служить забываемыми электронными подписями всех Кандидатов.

К тому же, они модифицированы с тем, чтобы обеспечить одноразовость предъявления, что будет использовано в дальнейшем в процедуре голосования, которая следует за закончившейся на этом процедурой регистрации. Для голосования Избиратель не обязан появляться в каком-либо заранее определенном месте, а лишь подключается к некоторой компьютерной сети, в которой его сетевой адрес невозможно определить (кроме того, адрес выбирается Избирателем самостоятельно и может никак его не идентифицировать). Далее, чтобы проголосовать за Кандидата j, Избиратель должен передать ему все электронные подписи (свои и его конкурентов). Общим в этих подписях окажется число $k \in Z_v$. Поскольку v достаточно велико (скажем, 250 бит), случайно такое совпадение может произойти с очень малой вероятностью (даже за всю историю эры технологического развития, и, соответственно, эры тайных голосований в компьютерных сетях). Если в наборе из m подписей обнаруживаются имеющие разный параметр k, то бюллетень считается недействительным.

Протокол передачи электронных подписей приведен ниже. Для упрощения обозначений индекс $i = 1, \ldots, m$ всюду опущен. Все вычисления, как и прежде, производятся по соответствующим модулям.

Протокол передачи забываемых электронных подписей

Шаг 1.

Избиратель подключается к сети и вызывает Кандидата, за которого намерен отдать свой голос. После этого Избиратель посылает Кандидату числа a, b, c, и, таким образом, Кандидат может подучить $\bar{A}, \bar{B}, \bar{C}$.

Шаг 2.

Кандидат посылает Избирателю запрос $r \in Z_v$.

Шаг 3.

Избиратель вычисляет числа $x = kr + U$, и $C^x A^r B$, которые он может легко вычислить из имеющейся у него информации, и передает их Кандидату, который возводит их в степень v, чтобы убедиться в соответствии их числу $\bar{A}\bar{B}\bar{C}$.

После того, как Избиратель передал таким образом Кандидату подписи, полученные от всех Кандидатов, участие Избирателя в выборах закончено (если он не отклонялся от протоколов и в результате не будет привлечен к ответственности за это, а также, конечно, если настоящая система голосования достаточно криптостойкая).

(Конец протокола)

Далее, при подсчете голосов, каждый Кандидат предъявляет остальным блоки из m электронных подписей (по одной от каждого Кандидата, в том числе и от себя). Каждый блок засчитывается ему как поданный за него голос, если для всех подписей этого блока параметр k одинаков и если у какого-либо другого Кандидата не обнаружится подписей с теми же тройками (a_i, b_i, c_i). В последнем случае, если у обоих Кандидатов совпали все запросы r для этих блоков, эти два бюллетеня игнорируются, а при несовпадении запросов система уравнений $x_1 = kr_1 + U$ и $x_2 = kr_2 + U$ может быть решена относительно U, что даст Кандидатам номер нарушителя.

В заключение отметим достоинства представленной системы в сравнении с уже опубликованными. Вне сомнения, достоинством предлагаемого протокола является минимальное количество шагов информационного обмена – действительно, можно доказать, что для передачи забываемой электронной подписи нужно как минимум по два шага с каждой стороны. Опубликованные же на настоящий мо-

мент системы (см., например, [6], [8]) обычно требуют даже не фиксированное число шагов, а количество шагов, требуемое параметрами безопасности в доказательствах с нулевым знанием – (см., например, [7]). Это представляется достаточно важным при технической реализации голосований, поскольку длительность информационного обмена часто является критической в массовом обслуживании (передача данных в крупномасштабной вычислительной сети).

Список литературы

[1] Саломаа А. Криптография с открытым ключом, М.: Мир, 1996.

[2] Renvall A. Cryptographic Protocols and Techniques for Communication. University of Turku, 1994.

[3] Niemi V., Renvall A. Cryptographic Protocols and voting. Proc. Results and Trends in Theoretical computer Science, LNCS 812, 1994, pp. 307-316.

[4] Niemi V., Renvall A. How to Prevent Buying of Votes in Computer Elections. Proc. ASIACRYPT' 94.

[5] Fergusson N. Single-Term Off-Line Coins. Pre-proceeding of EUROCRYPT'93. Lofthus, Norway, 1993.

[6] Iversen K.R. A Cryptographic Scheme for Computerized General Elections. Lecture notes in Computer Science, vol. 576. Springer, Berlin Heidelberg New York, 1992, pp. 405-419.

[7] Blum D. How to Prove a Theorem so that No one Else Can Claim it. Proc. of the ICM, 1987.

[8] Behaloh. Verifiable Secret Ballot Elections. Yale University, Computer Science Department, Technical Report 561, 1987.

От классических задач регулирования к интеллектуальному управлению. I*

С.Н. Васильев

На стыке современной теории управления и искусственного интеллекта активно формируется и развивается область исследований и разработок, именуемая интеллектным управлением. В работе рассматривается эволюция задач и методов теории управления и дается обзор некоторых средств искусственного интеллекта, применяющихся сегодня и перспективных в задачах управления.

Введение

Согласно определению, данному выдающимся ученым А.М. Летовым, стоявшим у истоков современной теории управления и сделавшим многое для ее развития [1], *теория управления* «есть совокупность методов, позволяющих выработать и обосновать решение, которое принимается для достижения заранее поставленной цели, в условиях как-либо определенной ситуации» [2]. В частности, теория *автоматического* управления – «наука о методах определения законов управления какими-либо объектами, допускающих реализацию с помощью технических средств автоматики» [3].

Обычно различают *объект управления* (ОУ) и *устройство управления* (УУ). В ОУ реализуется некоторый процесс, нуждающийся в организованных воздействиях (решениях, управлениях) со стороны

*Работа выполнена при поддержке РФФИ, гранты 98-01-01137, 98-07-90314 и федеральной целевой программы «Интеграция».