П. О. Джунковский, А. С. Дитенкова

ПОРОГОВАЯ СХЕМА ЦИФРОВОЙ ПОДПИСИ С РАЗДЕЛЕННЫМ СЕКРЕТОМ НА БАЗЕ ГОСТ Р 34.10-2001[1]

Схемы разделения секрета [1] используются для распределения полномочий доступа к некоторому информационному ресурсу между несколькими лицами, а также для формирования электронной подписи документа этими лицами. Секрет (как правило, закрытый ключ ключевой пары) разделяется на доли и распределяется между участниками схемы разделения секрета по установленному алгоритму. В дальнейшем, для осуществления доступа к ресурсу или формировании ЭЦП необходимо объединение t частей из n, где n — общее количество долей и t — минимальное необходимое количество долей для восстановления всего секрета, $t \leq n$ (такая схема называется (t,n)-пороговой схемой), либо всех долей секрета, т. е. $t = n$ (в этом случае схема носит название простой).

Данная статья представляет реализацию пороговой схемы разделения секрета для n участников на базе отечественного алгоритма ЭЦП ГОСТ Р 34.10-2001 [2—4]. К особенностям данной схемы относится, прежде всего, простота реализации. Фактически в явном виде используется алгоритм формирования ЭЦП, определенный стандартом. Как следствие, высокая производительность и возможность реализации на различных устройствах, таких как токены, смарт-карты и мобильные клиенты на базе платформы J2ME или других программно-аппаратных платформ. Область применения также различна.

Физическое разделение ключа на доли обеспечивает стойкость системы после компрометации одной или нескольких долей (обычно если число скомпрометированных долей меньше порога схемы). Это является основной особенностью схем разделения секрета.

Участники представленной схемы могут быть разделены на две категории: клиенты, один из которых выполняет операцию генерации ключа и распределения долей секрета (на практике — отчуждаемый носитель, токен, смарт-карта или мобильный клиент или аппаратный модуль безопасности HSM), другие — промежуточные шаги ЭЦП; еще одним участником является сервер, выполняющий финальный шаг по формированию ЭЦП документа (например, АРМ с установленным криптопровайдером JCE или CSP либо другое программно-аппаратное средство). Подобное разделение участников по ролям весьма условно и может быть изменено в процессе реализации для конкретной системы документооборота или системы аутентификации, так как и клиент и сервер выполняют практически симметричные операции в процессе подписания.

[1] Статья написана в рамках НИР «Обеспечение безопасности информации в открытых распределенных вычислительных системах», заданной Государственным контрактом № П2397 в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009—2013 годы.

В основе данной схемы лежит примитивная схема ЭЦП с разделенным секретом [5]. Приведем ее краткое описание для двух участников (клиента и сервера). Итак, на предварительном этапе клиент генерирует ключевую пару (d, Q) d в соответствии с ГОСТ Р 34.10-2001 и разделяет закрытый ключ на две доли. Для этого он выбирает случайное значение d_2, удовлетворяющее условию $0 < d_2 < q$. Вычисляется разность:

$$d_1 = (d - d_2) \bmod q,$$

и проверяется соответствие результата диапазону $0 < d_1 < q$. Закрытый ключ d уничтожается, после чего значение d_1 передается серверу по защищенному каналу и также уничтожается на стороне клиента. Значения d_1 и d_2 являются компонентами разделенного секрета d (долями) и сохраняются в ключевом хранилище сервера и клиента соответственно.

Процесс формирования ЭЦП происходит в 3 этапа. На первом этапе сервер вычисляет хеш подписываемого сообщения m по алгоритму ГОСТ Р 34.11-94, $e = h(m) mod\ q$, генерирует сессионный ключ k_1 $(0 < k_1 < q)$ и точку эллиптической кривой $R_1 = k_1 P$ в соответствии со стандартом. Набор значений (e, R_1) отправляется клиенту. Состояния k_1 и e сохраняются.

На втором этапе клиент генерирует сессионный ключ k_2 $(0 < k_2 < q)$ и точку эллиптической кривой $R_2 = k_2 P$, вычисляет сумму точек эллиптической кривой $R = (R_1 + R_2)$ и находит x-координату данной точки (называемой также рандомизатором)

$$r = R_x \bmod q.$$

Далее вычисляется компонента подписи:

$$s_2 = (rd_2 + k_2 e) \bmod q.$$

Значения (r, s_2) передаются серверу. Состояния r, R_2, s_2 и k_2 уничтожаются. На третьем этапе сервер вычисляет собственную компоненту подписи:

$$s_1 = (rd_1 + k_1 e) \bmod q$$

и сумму:

$$s = (s_2 + s_1) \bmod q.$$

Состояния k_1 и e уничтожаются. Результирующая пара значений (r, s) является ЭЦП в соответствии с ГОСТ Р 34.10-2001. Проверка подписи осуществляется обычным образом.

Таким образом, в процессе подписания клиент и сервер обмениваются лишь открытыми параметрами. Злоумышленник, перехвативший на каком-либо этапе значения, передаваемые клиентом и сервером, не сможет получить представление о закрытых долях. В случае подмены одного из значений результирующая подпись не будет валидной, что станет очевидным на последнем этапе формирования подписи: сервер выполняет проверку результирующей подписи с помощью открытого ключа.

Стойкость данной схемы обеспечивается криптографическими свойствами стандарта ЭЦП. На рис. 1 приведена примитивная схема ЭЦП с разделенным секретом.

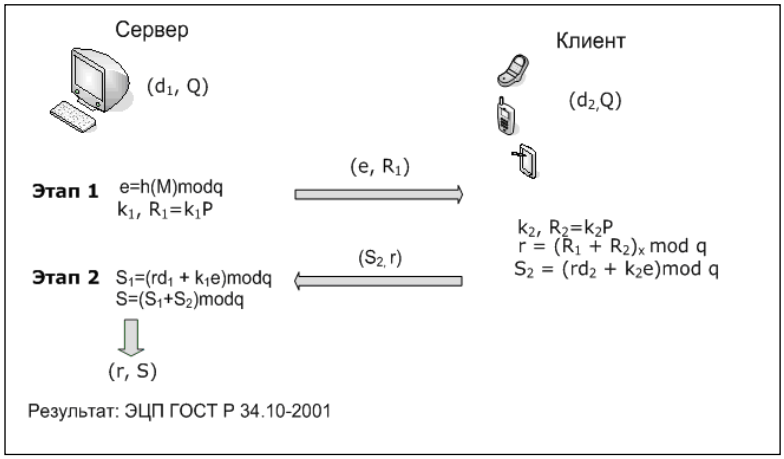

Рис. 1. Схема ЭЦП с разделенным секретом

Приведем доказательство данной схемы. Воспользуемся свойством:

$(a+b)\bmod c=(a \bmod c + b \bmod c) \bmod c$,

запишем:

$$s = (s_1 + s_2) \bmod q = ((rd_2 + k_2 e) \bmod q + (rd_1 + k_2 e) \bmod q) \bmod q =$$

$$(rd_1 + k_1 e + rd_2 + k_2 e) \bmod q = (r(d_1 + d_2) + (k_1 + k_2) e) \bmod q =$$

$$(r(d - d_2 + d_2) + k' e) \bmod q = (rd + k' e) \bmod q$$

Следовательно, схема корректна. Приведен пример для двух участников, однако эта схема также в явном виде применима и для большего числа участников.

На основе предложенной схемы ЭЦП с разделенным секретом предлагается ее пороговая модификация. Закрытый ключ d представляется в качестве суммы случайных значений $d_2 ... d_N$ и значения d_1, вычисляемого как:

$d_1 = d - (d_2 + ... + d_N)$.

Значение d_n назовем долей секрета d, соответствующей участнику n. Ключевым набором назовем картеж значений $(d_1, .., d_m)$, соответствующих одному из вариантов сочетаний взаимодействующих пользователей в пороговой схеме. Используя формулу количества сочетаний без повторений, найдем общее количество ключевых наборов для N участников и в зависимости от порога t:

$$C = \frac{N!}{t!(N-t)!}$$

Например, для $N = 4$, $t = 2$ общее количество таких наборов составит $C = 6$. Это продемонстрировано в таблице 1.

Таблица 1. Ключевые наборы для четырех участников

Участник, № / Набор, №	1	2	3	4
1	d_1^1	d_2^1	–	–
2	d_1^2	–	d_3^2	–
3	d_1^3	–	–	d_4^3
4	–	d_2^4	d_3^4	–
5	–	d_2^5	–	d_4^5
6	–	–	d_3^6	d_4^6

Верхний индекс показывает номер ключевого набора, нижний — номер участника, которому принадлежит данная доля секрета.

Количество долей секрета для одного порога ($t < N$), хранимых одним пользователем, составляет

$T = N - 1$

при $t = N$, $T = 1$.

Общее количество долей секрета, хранимых одним пользователем для всех порогов, составляет

$T_{общ} = KT$,

где K — количество порогов, поддерживаемых схемой (например, для $t = 3, 4, 5$ $K = 3$).

Общее количество долей секрета, генерируемое клиентом-дилером для одного значения порога при $t < N$, составляет

$S = NT$.

Общее количество долей секрета для каждого порога составляет

$S_{общ} = KS$.

Общее количество ключевых наборов для каждого из порогов составит

$$C_{общ} = \sum_{K} \frac{N!}{t_i!(N - t_i)!}$$

При $t = N$ — тривиальный случай схемы, $S = N$. Наборы независимы друг от друга, значения долей секрета являются случайными значениями. Рассмотрим следующий пример. Количество участников $N = 5$, число допустимых порогов ($t = 3, 4, 5$), $K = 3$. Вычислим общее количество ключевых наборов и число долей секрета для каждого из значений порога:

$C_{t=3}^{N=5} = 10, S_{t=3} = 20$

$C_{t=4}^{N=5} = 5, S_{t=4} = 20$

$C_{t=4}^{N=5} = 1, S_{t=5} = 5$

$S_{общ} = 45$

$C_{общ} = 16$

Приведем оценку расхода памяти для хранения долей секрета. Максимальный размер закрытого ключа в соответствии с ГОСТ Р 34.10-2001 составляет не более 255 бит ≈ 32 байта. Для генерации 45 долей потребуется 1440 байт, при этом каждый пользователь будет хранить около 288 байт ключевой информации.

Протокол формирования электронной подписи (равно как и аутентификации группы пользователей при доступе к информационному ресурсу) может быть представлен следующей схемой. На первом этапе сервер определяет активных участников схемы, рассылая им хеш подписываемого документа (Рис. 2).

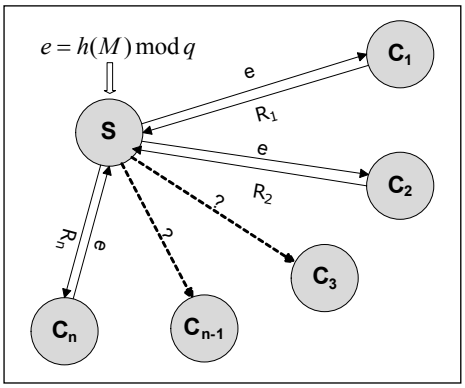

Рис. 2. Определение активных участников схемы

Активные участники схемы (C_n) генерируют сессионный ключ k и параметры подписи R — точку эллиптической кривой. Далее клиенты передают точки R его серверу (S). Сервер выбирает ключевые наборы для данного порога и количества активных участников, после чего вычисляет x-координату суммы точек эллиптической привой $r = R_x$. Сервер отправляет значение r и номер ключевого набора каждому активному участнику (Рис. 3). После этого каждый участник формирует свой компонент подписи s и пересылает его серверу.

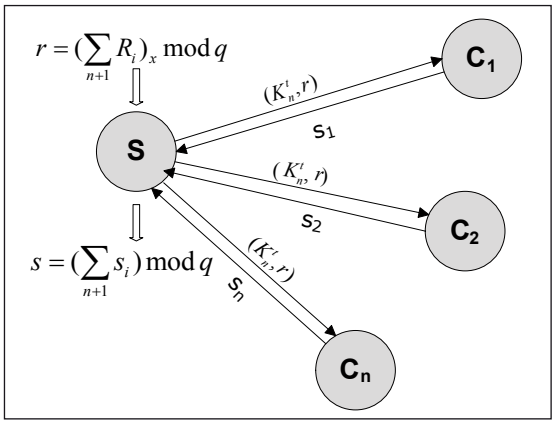

Рис. 3. Второй этап обмена с клиентами

На заключительном этапе сервер вычисляет сумму компонент подписи *s* аналогично случаю примитивной пороговой схемы. Пара значений (*r, s*) является электронной цифровой подписью ГОСТ Р 34.10-2001. Проверка осуществляется стандартным образом.

Поскольку в схемах ЭЦП с разделенным секретом, в отличие от коллективных схем подписи, подразумевается изначальное наличие доверенной третьей стороны, генерирующей ключевую пару и распределяющей доли секрета между участниками, это может быть слабым местом системы. Должно быть обеспечено «доверие» к данному участнику схемы, должно быть предъявлено требование физического уничтожения закрытого ключа (очистка памяти и т. д.). Также протокол распределения ключевых долей должен обеспечивать конфиденциальность ключевого материала и невозможность перехвата злоумышленником хотя бы одной из долей секрета.

Подобные схемы могут найти широкое распространение в различных системах аутентификации при доступе к ресурсам, а также при создании отказоустойчивых систем без единого якоря доверия (а, следовательно, без точки отказа).

Изложенные результаты получены в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы.

СПИСОК ЛИТЕРАТУРЫ:

1. *Heil H.* Secret Sharing // Cryptography Seminar. 2001.
2. ГОСТ Р 34.10–2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: ИПК «Издательство стандартов», 2001.
3. *Архангельская А. В., Запечников С. В.* Схемы цифровой подписи на основе алгоритмов ГОСТ Р 34.10-2001 с применением аппарата парных отображений // Научная сессия МИФИ. XIV Всероссийская научная конференция. Проблемы информационной безопасности в системе высшей школы. М.: МИФИ, 2007.
4. *Спельников А. Б.* Эллиптическая пороговая схема разделения секрета // Вестник Самарского гос. техн. ун-та. Сер. Физ.-мат. науки. 2009. № 1 (18). С. 251–259.
5. *Джунковский П. О., Дитенкова А. С.* Реализация схемы цифровой подписи с разделенным секретом на базе ЭЦП ГОСТ Р34.10-2001 (в печати).