С. Н. Кяжин

СХЕМЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ С ДОПОЛНИТЕЛЬНОЙ ФУНКЦИОНАЛЬНОСТЬЮ И ИХ ПРИМЕНЕНИЕ

Введение

Электронная цифровая подпись — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию [1]. По своему существу электронная подпись представляет собой реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования электронной цифровой подписи и проверить принадлежность подписи владельцу. Электронная цифровая подпись предназначена для аутентификации лица, подписавшего электронный документ, и является полноценной заменой собственноручной подписи в случаях, предусмотренных законом [2].

Использование электронной подписи позволяет осуществить следующие функции.

- Контроль целостности передаваемого документа. При любом случайном или преднамеренном изменении документа подпись станет недействительной, потому что вычислена она на основании исходного состояния документа и соответствует лишь ему.
- Защиту от изменений (подделки) документа. Гарантия выявления подделки при контроле целостности делает подделывание нецелесообразным в большинстве случаев.
- Невозможность отказа от авторства. Так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, владелец не может отказаться от своей подписи под документом.
- Доказательное подтверждение авторства документа. Так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, владелец пары ключей может доказать свое авторство подписи под документом. В зависимости от деталей определения документа могут быть подписаны такие поля, как «автор», «внесенные изменения», «метка времени» и т. д.

Но помимо «стандартных» функций с помощью электронной цифровой подписи можно выполнять и другие функции. В таком случае схемы цифровой подписи называют схемами с дополнительной функциональностью. В настоящей статье проанализированы примеры использования следующих схем:

- неоспоримая электронная цифровая подпись;
- электронная цифровая подпись с назначенным конфирмантом;
- электронная цифровая подпись вслепую;
- групповая электронная цифровая подпись;
- электронная цифровая подпись с дополнительной защитой.

В России юридически значимый сертификат электронной цифровой подписи выдает удостоверяющий центр. Правовые условия использования электронной цифровой подписи в электронных документах регламентирует Федеральный закон Российской Федерации от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [1]. При использовании электронной цифровой подписи в электронном документообороте между кредитными организациями и кредитными бюро активно стала развиваться инфраструктура электронного документооборота между налоговыми органами и налогоплательщиками. Благодаря электронной цифровой подписи, в частности, многие российские компании осуществляют свою торгово-закупочную деятельность в Интернете, через системы электронной торговли, обмениваясь с контрагентами необходимыми подписанными

документами в электронном виде. Это значительно упрощает и ускоряет проведение конкурсных торговых процедур.

1. Неоспоримая электронная цифровая подпись

Копию обычной электронной цифровой подписи получить несложно. Иногда это полезно, например, если цифровая подпись стоит под документом для всеобщего пользования. Однако очевидно наличие опасности, которая может возникнуть в случае, если в подлинности какого-либо тайного документа может убедиться каждый. Поэтому лучше применять такую электронную цифровую подпись, которую нельзя проверить без согласия ее владельца.

Основная идея схемы неоспоримой электронной цифровой подписи состоит в следующем [3].

1. Пользователь 1 отправляет Пользователю 2 свою электронную цифровую подпись.

2. Пользователь 2 генерирует случайное число и отправляет его Пользователю 1.

3. На основе полученного от Пользователя 2 случайного числа и собственной затемняющей функции Пользователь 1 получает результат некоторых вычислений, который отсылает Пользователю 2.

Данная схема проиллюстрирована на рис. 1.

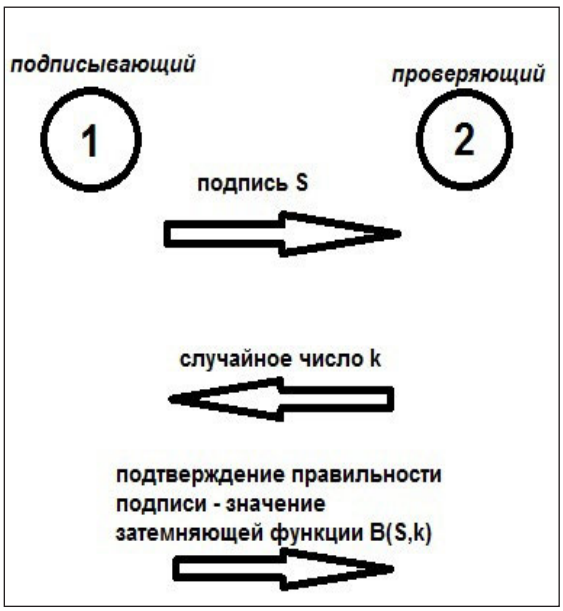

Рис. 1. Схема неоспоримой электронной цифровой подписи

Кроме того, Пользователь 1 не может отказаться от подписи, если подпись действительно принадлежит ему, и, с другой стороны, может доказать, что он не подписывал документ, если ему вменяют в вину авторство не принадлежащей ему подписи.

Как и обыкновенная электронная цифровая подпись, неоспоримая подпись зависит от содержания документа и закрытого ключа автора. Основное отличие неоспоримой электронной цифровой подписи от обыкновенной состоит в том, что подлинность неоспоримой подписи может подтвердить только ее автор. Неоспоримая электронная цифровая подпись обладает следующим свойством (вследствие чего и имеет такое название): автор подписи вынужден либо признать подлинность предъявленной ему подписи, либо отвергнуть ее, причем он не может отказаться от нее в случае, если эта подпись является настоящей.

Рассмотрим применение данной схемы на примере. Предположим, что некоторая Компания производит некоторый программный Продукт. Компания снабжает каждую копию Продукта

электронной цифровой подписью с целью защиты от копирования. Т. е. необходимо, чтобы покупатели только легальной копии Продукта могли проверить подлинность электронной цифровой подписи.

Предположим, Покупатель 1 приобретает копию Продукта на законных основаниях, делает с нее копию и передает Покупателю 2. Как только Покупатель 2 захочет проверить подлинность электронной цифровой подписи под копией Продукта, полученной от Покупателя 1, он обратится в Компанию с просьбой проверить подпись. Сгенерированное Покупателем 2 случайное число наверняка отличается от числа Покупателя 1, и Компания сделает заключение о нелегальности подписи копии Покупателя 2, так как подписана была только копия для случайного числа Покупателя 1.

Недостатком схемы является тот факт, что каждую копию подписи необходимо проверять подписавшему документ лицу. В некоторых случаях это может оказаться неэффективным. Отчасти данную проблему решает электронная цифровая подпись с назначенным конфирмантом.

2. Электронная цифровая подпись с назначенным конфирмантом

Электронная цифровая подпись с назначенным конфирмантом позволяет найти компромисс между обыкновенной и неоспоримой подписями. Подробно схема описана в [3]. Рассмотрим ее на примере, использованном в разделе 1. В случае, если Компания крупная, она не в состоянии проверять подпись от каждой копии производимого Продукта. Поэтому она назначает конфирмантов — лиц, которые возьмут на себя проверку подписей Компании. Для этого Компания будет ставить под копиями Продукта электронную цифровую подпись с назначенным конфирмантом. В результате Компания сможет переложить ответственность за проверку подлинности своей электронной цифровой подписи целиком на конфирманта.

Электронная цифровая подпись с назначенным конфирмантом может быть полезной не только для компании, производящей программное обеспечение. Любой пользователь может разместить свой открытый ключ в некоторый справочник, доступный всем компаниям, и любое подписывающее лицо может воспользоваться его услугами в качестве назначенного конфирманта.

3. Электронная цифровая подпись вслепую

Особенностью электронной цифровой подписи вслепую является анонимность, т. е. подписывающая сторона не знает содержимое подписываемого документа. Основная идея электронной цифровой подписи вслепую заключается в следующем [4].

1. Пользователь 1 посылает измененный с помощью специальной затемняющей функции документ Пользователю 2.

2. Пользователь 2 подписывает полученный документ и возвращает Пользователю 1.

3. Используя полученную подпись, Пользователь 1 может выделить из нее подпись Пользователя 2 к настоящему документу.

По завершении схемы Пользователь 2 ничего не знает ни о документе, ни о подписи под этим документом. Схема проиллюстрирована на рис. 2.

Эту схему можно сравнить с конвертом, в котором размещены документ и копировальный лист. Если подписать конверт, то подпись отпечатается на документе и при вскрытии конверта документ уже будет подписан.

Наиболее широкое применение схема электронной цифровой подписи вслепую нашла в сфере электронных платежей. Например, чтобы вкладчик не обманул банк, может использоваться такой протокол: вкладчик пишет одинаковый номинал купюр на ста документах с разными номерами и депонирует в зашифрованном виде у банка. Банк выбирает случайным образом и требует раскрыть 99 конвертов, убеждается, что везде написано $10, а не $1000, тогда подписывает оставшийся конверт вслепую, не видя номера купюры.

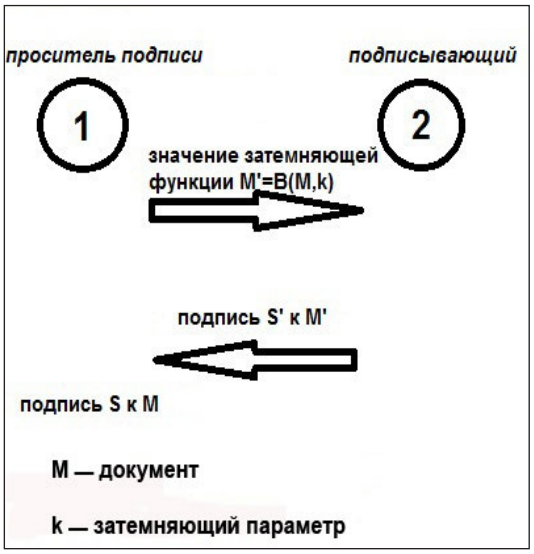

Рис. 2. Схема электронной цифровой подписи вслепую

Кроме того, электронная цифровая подпись вслепую используется для тайного голосования. Рассмотрим протокол Фуджиока, Окамото и Охта [5].

1. Избиратель подготавливает избирательный бюллетень со своим выбором и добавляет к нему некоторое случайное число (осуществляет маскировку затемняющей функцией).

2. Избиратель подписывает избирательный бюллетень и отправляет его в избирательный комитет.

3. Избирательный комитет проверяет, что подпись принадлежит непроголосовавшему избирателю, и отмечает его участие, не вскрывая бюллетеня.

4. Если избирательный бюллетень действителен, избирательный комитет подписывает избирательный бюллетень и возвращает его избирателю.

5. Избиратель удаляет маскировку, раскрывая тем самым избирательный бюллетень, подписанный избирательным комитетом.

6. Избиратель отправляет полученный бюллетень в коллектор подсчета голосов.

7. Коллектор подсчета голосов проверяет подпись на избирательном бюллетене. Если избирательный бюллетень действителен, коллектор подсчета голосов размещает сгенерированное избирателем случайное число в списке, который будет издан после завершения голосования.

4. Групповая электронная цифровая подпись

Групповая электронная цифровая подпись обладает следующими свойствами, отличными от свойств обыкновенной подписи:

- автором подписи могут быть только члены группы;
- в любое время можно убедиться, что ее автор является членом группы;
- невозможно определить, кто именно из членов группы является автором подписи.

Схема групповой подписи выглядит следующим образом [3].

1. Пользователь генерирует большое количество пар ключей (открытый и закрытый). Каждый член группы получает от Пользователя свой набор ключей. При этом все наборы ключей у пользователей различны.

2. Пользователь помещает все открытые ключи в некоторый справочник в случайном порядке, сохраняя в секрете информацию, кому какой из ключей принадлежит.

3. Чтобы подписать документ, член группы выбирает ключ из предоставленных ему Пользователем.

4. Чтобы проверить подлинность подписи, необходимо выбрать соответствующий открытый ключ из справочника.

В случае возникновения разногласий Пользователь знает, кому принадлежит ключ, с помощью которого была поставлена подпись, вызвавшая спор.

Недостатком схемы является наличие арбитра (Пользователя), который знает все закрытые ключи и может подделать любую подпись. К тому же множество пар ключей, генерируемое Пользователем, должно быть чрезвычайно велико, чтобы попытки выяснить, какой ключ кому принадлежит, не имели смысла.

5. Электронная цифровая подпись с дополнительной защитой

Стойкость обыкновенной электронной цифровой подписи зависит от секретности закрытого ключа автора подписи. Предположим, что злоумышленник обладает достаточными средствами, чтобы вскрыть закрытый ключ Пользователя. Чтобы уменьшить вероятность вскрытия, предлагается схема электронной цифровой подписи с дополнительной защитой.

Идея, которая лежит в основе электронной цифровой подписи с дополнительной защитой, в следующем [3]. Каждому открытому ключу ставится в соответствие не один закрытый ключ, а некоторое множество. Каждый из них позволяет подписать документ, но при использовании разных ключей подписи также будут различаться. Пользователь знает только один ключ, остальные ему неизвестны.

Тогда злоумышленник в лучшем случае отыщет единственный ключ. А количество возможных закрытых ключей, соответствующих данному открытому, чрезвычайно велико. И вероятность нахождения именно того ключа, который использует Пользователь, очень мала.

Таким образом, цифровая подпись с дополнительной защитой позволяет отразить атаку, предпринятую злоумышленником, обладающим самыми большими вычислительными мощностями.

Заключение

В настоящее время электронная цифровая подпись получила широкое распространение. Электронный документооборот используется повсеместно. Реализуются новые атаки на схемы электронной цифровой подписи, выявляются новые недостатки. В связи с этим становится необходимым введение дополнительной функциональности в схемы электронной цифровой подписи.

Проанализированные в настоящей статье схемы электронной цифровой подписи предназначены для различных целей и имеют относительно широкое применение, но каждая из них выполняет основную функцию подписи — аутентификация автора подписи и защита от искажений документа. Данные схемы имеют большую эффективность и практическую ценность по сравнению со схемами обыкновенной электронной цифровой подписи. Учитывая высокую полезность функциональных возможностей, реализуемых ими, можно говорить о перспективности использования проанализированных схем или их модификаций.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон Российской Федерации от 6 апреля 2011 г. № 63-ФЗ.
2. Гражданский кодекс Российской Федерации, часть 1, глава 9, статья 160.
3. *Анин Б.* Защита компьютерной информации. СПб.: BHV-Санкт-Петербург, 2002. — 384 с.
4. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. М.: Триумф, 2002. — 610 с.
5. *Fujioka A., Okamoto T., Ohta K.* A practical secret voting scheme for large scale elections // Advances in Cryptology. AUSCRYPT'92. Berlin. 1993. P. 244–251.