А. В. Артамонов, П. Н. Васильев, Е. Б. Маховенко

МОДИФИКАЦИЯ СХЕМЫ ГРУППОВОЙ ПОДПИСИ BBS С ИНТЕРАКТИВНЫМ ДОБАВЛЕНИЕМ ЧЛЕНОВ ГРУППЫ

В ряде прикладных задач, помимо формирования ЭЦП для электронного документа, может потребоваться наличие возможности создания подписи одним лицом от имени группы лиц, обладающих правом подписи. Кроме того, должно соблюдаться требование по анонимности подписи, т. е. проверяющий не должен иметь возможность определить, кто именно из группы сформировал подпись. Только специальное уполномоченное лицо, обладающее особым ключом, должно иметь возможность, в случае проведения расследования, определить, кто конкретно из группы сформировал подпись для заданного документа.

Перечисленным выше требованиям удовлетворяют схемы групповой подписи. В отличие от обычных схем ЭЦП, они обладают следующими свойствами:

- нет необходимости для каждого пользователя создавать свою уникальную пару: секретный ключ — сертификат. В случае групповой подписи создается только один сертификат, применяемый пользователями для проверки подписи, что упрощает процедуру проверки;
- пользователи (за исключением специального уполномоченного лица) не имеют возможности определить, кто конкретно из группы сформировал подпись. Для ряда задач это может быть важным свойством, чтобы, например, исключить возможность вычисления пользователем конкретного автора подписи для использования в корыстных целях;
- возможность отзывать право подписи у отдельных членов группы.

В данной работе предлагается решение, построенное на основе схемы групповой подписи на билинейных отображениях (спариваниях) [1, 2]. За основу взята схема групповой подписи BBS [3], идея которой заключается в предоставлении в подписи знания решения проблемы SDH: знания пары $(A, x) \in G_1 \times Z_p$, такой, что $A^{x+g} = g_1$. Такая пара генерируется с помощью менеджера группы, знающего значение g. Но для того чтобы обеспечить возможность отзыва анонимности, т. е. операцию раскрытия подписи раскрывающим менеджером группы, доказательство должно обладать не полностью нулевым разглашением, а только частичным: менеджер должен иметь возможность восстановить A.

В системе предусмотрена работа следующих категорий пользователей:

1. Менеджер группы. Отвечает за формирование начальных параметров подписи, секретных и открытых ключей. В некоторых схемах менеджер группы наделяется правом отзыва подписи у отдельных пользователей.

2. Вскрывающий менеджер. Обладает возможностью раскрыть автора групповой подписи.

3. Члены группы — пользователи, обладающие секретным ключом и правом формирования подписи.

4. Пользователи — внешние пользователи системы, обладающие открытым ключом и выполняющие проверку подписи.

Чтобы подписать сообщение m, пользователь сначала зашифровывает A на открытом ключе менеджера группы, а затем предоставляет доказательство с нулевым разглашением того факта, что открытый текст на самом деле содержит A, для которого он знает x.

Схема доработана для соответствия требуемым прикладным свойствам. Основные отличия от базовой версии:

- интерактивный протокол добавления новых членов группы. Стандартная схема групповой подписи BBS не предусматривает возможности интерактивного добавления новых членов группы.

Поэтому в схему был внедрен протокол Join. Для этого потребовалось изменить состав ключей членов группы. Они стали содержать три элемента $(A, x, y) \in G_1 \times Z_p^2$, такие, что $A^{x+g} = g_1 h^y$. В свою очередь, это потребовало соответствующей адаптации алгоритмов формирования и проверки подписи. В работе представлено доказательство безопасности адаптированной схемы;

- возможность отзыва сформированных подписей члена группы с заданного момента времени;
- интерактивный процесс формирования подписи с участием удостоверяющего центра.

СПИСОК ЛИТЕРАТУРЫ:

1. *Chaum D., Van Heyst E.* Group signatures // Proceedings of Eurocrypt 1991. Springer-Verlag, 1991. LNCS. Vol. 547. P. 257–265.
2. *Bellare M., Micciancio D., Warinschi B.* Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions // Proceedings of Eurocrypt 2003. Springer-Verlag, May 2003. LNCS. Vol. 2656. P. 614–629.
3. *Boneh D., Shacham H.* Group signatures with verifier-local revocation // Proc. 11th ACM Conference on Computer and Communications Security (ACM-CCS'04). 2004. P. 168–177.

И. Р. Бегишев

ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ РАБОТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ УСТРОЙСТВ, ИХ СИСТЕМ И СЕТЕЙ

Всеобщая информатизация общества все больше влияет на нашу жизнь. В силу этого нарушения работы информационно-телекоммуникационных устройств, их систем и сетей могут привести к катастрофическим последствиям.

Ответственность за нарушение правил эксплуатации ЭВМ установлена законодателем в статье 274 Уголовного кодекса Российской Федерации (далее – УК РФ) «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети». Данная норма является бланкетной и отсылает к нормативноправовым актам, инструкциям и правилам, устанавливающим правила эксплуатации ЭВМ.

При описании объективной стороны данного вида общественно опасного посягательства указание в диспозиции статьи на действие (бездействие) носит общий характер: используются слова «нарушение правил». Конкретное содержание этих правил раскрывается в нормативных актах других отраслей права. Ими могут быть федеральные законы, постановления Правительства Российской Федерации, правила, инструкции, предписания, например такие, как Общероссийские временные санитарные нормы и правила для вычислительных центров, паспорта качества, технические описания и инструкции по эксплуатации, а также инструкции по использованию программ для ЭВМ. Правила эксплуатации ЭВМ могут быть предусмотрены как в общих требованиях по технике безопасности и эксплуатации ЭВМ и периферийных устройств, так и в специальных правилах и инструкциях, регламентирующих особые условия эксплуатации ЭВМ (например, продолжительность работы и последовательность операций) [1].

Нарушение правил эксплуатации ЭВМ может выражаться в двух формах: в несоблюдении установленных правил эксплуатации аппаратного обеспечения ЭВМ, систем ЭВМ или их сети либо в нарушении правил эксплуатации программного обеспечения, предусмотренного для работы ЭВМ, системы ЭВМ или их сети. Так, например, нарушения правил эксплуатации