УДК 681.3.06

К.А. ПОГРЕБНЯК, Ю.М. ИЩЕНКО

Харьковский национальный университет радиоэлектроники, Украина

АНАЛИЗ СОВРЕМЕННЫХ ГРУППОВЫХ ПОДПИСЕЙ НА ОСНОВЕ ПАРНЫХ ОТОБРАЖЕНИЙ И ПЕРСПЕКТИВЫ ИХ ИСПОЛЬЗОВАНИЯ В НАЦИОНАЛЬНОМ ЭЛЕКТРОННОМ ДОКУМЕНТООБОРОТЕ

В данной статье представлен анализ современных групповых подписей на основе парных отображений, проводится исследование свойств групповых подписей и сфера их применения. А также исследуются некоторые вопросы возможностей применения таких подписей в национальной системе электронного документооборота. Выделяется одна из наиболее важных проблемных задач применения групповых подписей в Украине, а именно ее несоответствие с действующим стандартом электронной цифровой подписи и инфраструктурой открытых ключей на базе сертификатов.

Ключевые слова: *электронная цифровая подпись, групповые подписи, парные отображения.*

Введение

Согласно законам Украины «Про электронные документы и электронный документооборот» и «Про электронную цифровую подпись» в Украине введены электронный документооборот и электронная отчетность. Стремительная информатизация деловодства и документооборота выдвигает все более жесткие требования к предоставлению базовых услуг безопасности: конфиденциальности, целостности, доступности и неотказуемости.

Основным средством для обеспечения услуг неотказуемости и целостности электронных документов является электронная цифровая подпись (ЭЦП). Но обычная ЭЦП, в традиционном ее представлении, уже не может удовлетворить потребности всех форм ведения электронного бизнеса. По этой причине, в последние годы особое внимание уделяется схемам ЭЦП с различными модификациями, например: пороговым, кольцевым и групповым подписям.

Среди них следует выделить групповые подписи, которые обладают свойствами анонимности, невозможности обвинения, отслеживаемости и т. д. Обеспечения этих свойств является чрезвычайно важной задачей для развития сфер электронных услуг, электронной коммерции и торговли. Фактически, групповые подписи позволяют доказать принадлежность пользователя информационной системы к определенной группе без предоставления идентификационных данных проверяющему. Данная работа посвящена анализу существующих схем групповых подписей и исследованию возможности их применения в национальной системе электронного документооборота.

1. Свойства групповых подписей на основе парных отображений и сфера их применения

Впервые механизм групповой подписи был предложен Чаумом и Ван Хейстом [1]. Такой тип электронных подписей предполагает существование некой группы пользователей, которая возглавляется руководителем. Любой член группы может сформировать цифровую подпись от лица группы с использованием своего закрытого ключа. Для проверки подписи необходим открытый ключ группы, что обеспечивает невозможность определения фактического подписчика. Специфическая архитектура групповых подписей позволяет решить ряд практических задач криптологии, которые характеризуются сферой применения таких подписей (табл. 1).

Недавнее применение парных отображений в криптографии, с одной стороны, позволило построить инновационные криптопротоколы, а с другой – улучшить функциональные характеристики существующих протоколов. Учитывая положительные характеристики криптографических протоколов с применением парных отображений, возникает потребность в наделении этими характеристиками групповых подписей. Одно из направлений парных отображений применительно к групповым подписям состоит в сокращении длины подписи [2]. Другое направление связано с применением групповых подписей в инфраструктурах открытых ключей (ИОК) на основе идентификаторов, а также в комбинированных ИОК. Независимо от характера групповых подписей, они должны обладать рядом свойств, которые представлены в табл. 2 [3].

Таблица 1

Сферы применения групповых подписей

№	Сферы применения	Необходимость применения
1.	Системы закрытого электронного голосования	Гарантированное сохранение анонимности индивидуальных предпочтений голосующего
2.	Системы разграничения доступа	Повышение экономической эффективности за счет уменьшения издержек на поддержание в актуальном состоянии каталога с индивидуальной информацией о сотруднике предприятия (целесообразно применять в тех случаях, когда достаточно аутентифицировать пользователя, как члена группы)
3.	Доступ на охраняемые объекты на основе использования смарт-карт	В случае необходимости проверки доступа уполномоченных лиц на конкретные объекты, в условиях недопустимости сохранения данных о перемещениях этих лиц
4.	Взаимодействие между отделами большой компании	Непредвзятость оценивания результатов каждого члена группы
5.	Защита интересов персонала	Сокрытие информации о роде и виде деятельности сотрудника от посторонних лиц с целью обеспечения его защиты от попыток вымогательства, шантажа или т. п.

Таблица 2

Свойства групповых подписей

№	Свойства	Описание свойств
1.	Корректность (Correctness)	Валидные подписи, сформированные членами группы должны проходить процедуру проверки, не валидные подписи – заканчиваться неудачей
2.	Невозможность подделки (Unforgeability)	Только члены группы могут подписывать сообщения от лица группы
3.	Анонимность (Anonymity)	Для всех, кроме менеджера группы, вычислительно-сложно идентифицировать личность подписчика, имея валидную подпись
4.	Отсутствие привязки (Unlinkability)	Для всех, кроме менеджера группы, вычислительно-сложно решить, были ли две различные валидные подписи сформированы одним и тем же членом группы
5.	Отслеживаемость (Traceability)	Имея валидную подпись, менеджер группы может определить, кем именно из членов группы была сформирована эта подпись
6.	Невозможность обвинения (Exculpability)	Ни менеджер группы, ни члены группы не могут подписывать сообщения от имени другого члена группы. Таким образом, член группы не может обвинить менеджера группы (одного или в сговоре с другими членами группы) в том, что он (они) сформировали подпись от его имени
7.	Защищенность от сговора (Coalition-resistance)	Сговор нескольких членов группы не дает возможности сформировать валидную подпись, которая не будет принадлежать ни одному из участников сговора
8.	Ответственность группы (Framing)	Члены группы, даже совместно с менеджером группы, не в состоянии сформировать валидную цифровую подпись, не принадлежащую ни одному из членов группы

2. Общая структура групповых подписей на основе парных отображений

На наш взгляд, ГП в системах на основе идентификаторов возможно в общем виде охарактеризовать согласно рис. 1.

Формально, в схеме групповой подписи можно выделить следующие этапы:

– Инициализация системы.

– Регистрация участника.

– Формирование ЭЦП.

– Проверка ЭЦП.

– Выявление подписчика.

Отметим, что УГК является руководителем группы. На этапе *Инициализации системы* (выполняется руководителем группы) устанавливаются общесистемные параметры, генерируется личный ключ S руководителя группы (РГ), на основании предопределенного защищенного параметра k. Руководитель группы выбирает случайный секретный параметр $s \in Z_q^*$ и вычисляет свой открытый ключ $Y = sP$, а затем формирует открытые параметры системы.

Предположим, что заданы G_1 - промежуточная группа Диффи-Хеллмана простого порядка q, G_2 – циклическая мультипликативная группа некоторого порядка q и некоторое парное отображение (отображение Вейля или Тейта) $e: G_1 \times G_1 \to G_2$.

В зависимости от архитектуры цифровой подписи, определяется набор хеш-функций. Например, определим две криптографические хеш-функции:

$$H_1 : \{0,1\}^* \times G_1 \to Z_q;$$

$$H_2 : \{0,1\}^* \times G_1 \to G_1.$$

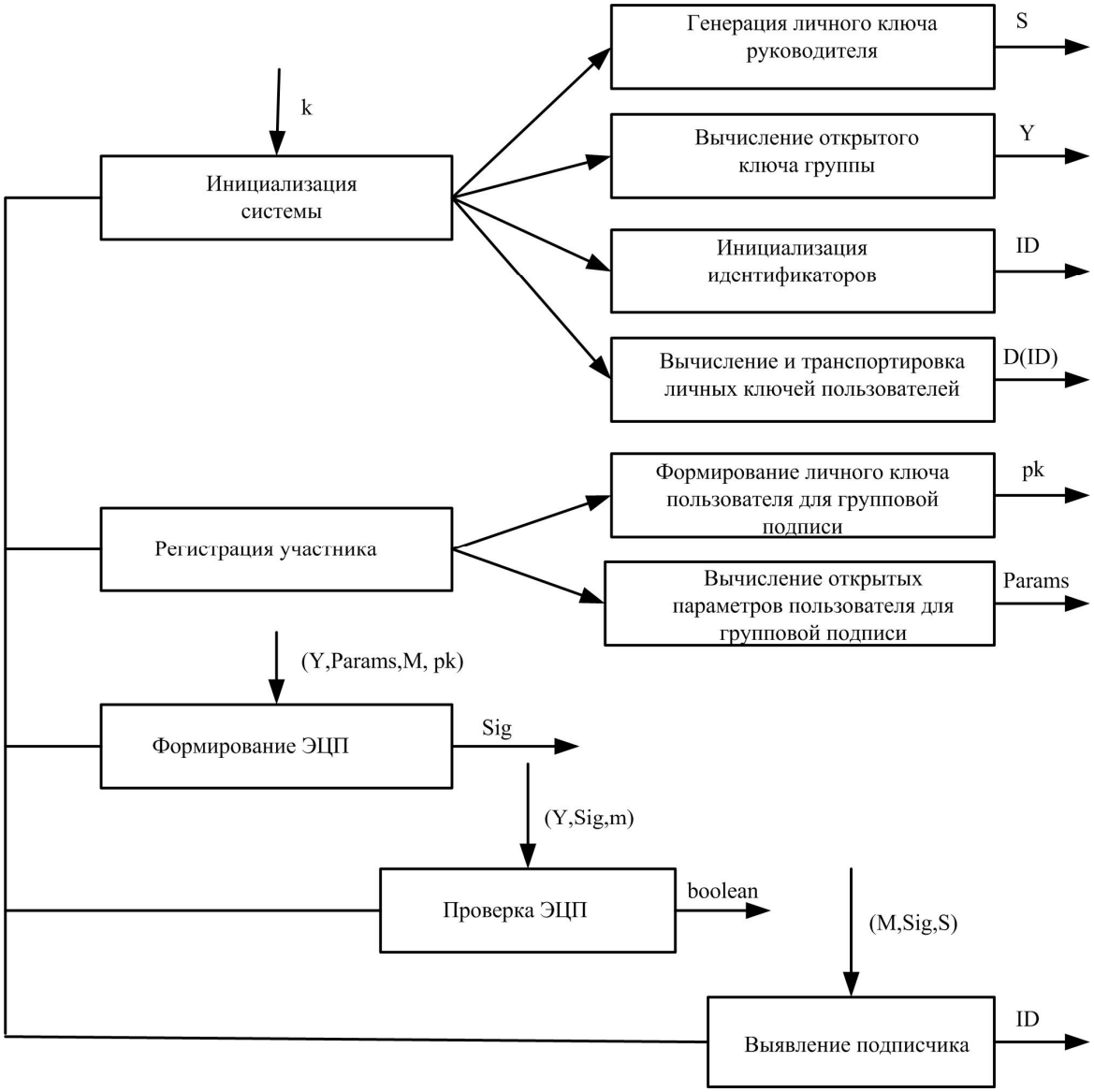

Рис. 1. Схема групповой подписи

Далее РГ инициализирует идентификаторы пользователей ID.

Тогда открытыми параметрами системы будут DomainParameters= $\{G_1, G_2, e, q, P, Y, H_1, H_2\}$.

На завершающем шаге данного этапа РГ вычисляет личные ключи пользователей D(ID), которые впоследствии передает им по защищенному каналу вместе с аутентичными общесистемными параметрами.

На этапе *Регистрации участника* группы пользователь отсылает свои идентификационные данные и проходит процедуру аутентификации в системе. Затем совместно с УГК пользователь формирует свой личный ключ для групповой подписи – pk, а также некоторые открытые параметры, которые принадлежат фиксированному пользователю.

Результатом этапа регистрации участника является выработка личного ключа пользователя для схемы групповой подписи, открытых параметров члена группы Params, которые зависят от архитектуры групповой подписи, а также занесение этих параметров в каталог РГ.

Затем, на этапе *Формирования ЭЦП* пользователь формирует подпись Sig сообщения M, используя открытый ключ группы Y, открытые параметры системы DomainParameters, сообщение M и личный ключ пользователя pk.

Проверка ЭЦП выполняется получателем сообщения и заключается в формировании решения о валидности/невалидности подписи, на основании открытого ключа группы Y, подписи Sig и сообщения M.

Этап *Выявления подписчика* выполняется руководителем группы в случае возникновения конфликтной ситуации. На данном этапе РГ имеет возможность выявить личность пользователя на основании своего личного ключа S, подписи Sig и сооб-

щения M, что обеспечивает неотказуемость источника сообщения.

Заметим, что в общем случае построение групповой подписи в системах на основе идентификаторов является тяжелой задачей. Это связано с архитектурой подобных систем. Полное доверие к уполномоченному на генерацию ключей, а фактически третий уровень стойкости согласно классификации Жиро [4], является существенным недостатком. Фактически третья доверенная сторона полностью владеет базой данных личных ключей пользователей, что означает возможность подделки подписи любого участника группы.

В тоже время, идентификатор пользователя не должен давать возможность установления данных фактического подписчика. Таким образом, мы приходим к ряду противоречий. В некоторой степени указанные противоречия разрешены в работе [5].

3. Применение групповых подписей на основе парных отображений в национальном электронном документообороте

Сегодня активно развиваются комбинированные инфраструктуры открытых ключей [6], которые позволяют устранить основные недостатки традиционной ИОК. Такие инфраструктуры предполагают построение традиционной ИОК на верхних уровнях иерархии и систем на основе идентификаторов на нижних уровнях. Создание и развитие ИОК Украины подтвердило существенные недостатки ИОК на основе сертификатов. Реализация подхода построения комбинированной ИОК предполагает разработку специфических криптопримитивов [5]. Немаловажной задачей является построение групповой подписи в комбинированных ИОК. Однако следует отметить ряд проблемных вопросов, связанных с указанной задачей. Сама архитектура инфраструктур на основе идентификаторов предполагает полное доверие к УГК. На практике устранение такого противоречия существенно усложняет схему групповой электронной цифровой подписи. Усложнение подписи влечет за собой появление новой модификации вычислительно сложной проблемы (дискретного логарифмирования, Диффи-Хеллмана и др.), которая будет положена в основу доказательства стойкости такой подписи. Учитывая, что групповая подпись ориентирована на механизмы парных отображений, следует отметить, что оценка стойкости подобной подписи также усложнится. На сегодня известны только оценки сверху относительно стойкости криптосистем на основе парных отображений. Еще одним проблемным вопросом является длина групповой подписи. Большинство реализаций криптографических протоколов на основе парных отображений предполагают использование суперсингулярных кривых, которые обеспечивают малый индекс вложения.

Учитывая результаты работ [7, 8], необходимо использовать гладкие кривые с небольшим индексом вложения, что влечет за собой достаточно большой размер групповой подписи. Таким образом, на наш взгляд, использование подобных групповых подписей возможно пока лишь в рамках корпоративного решения.

Заключение

Традиционная электронная цифровая подпись уже не может удовлетворить возрастающих потребностей электронного бизнеса, связанных с добавлением свойств инновационного характера, повышением стойкости, быстродействия криптопротоколов и т.д. Анализ зарубежных публикаций показывает, что ряд свойств, обеспечение которых крайне необходимо в новых электронных системах, позволяют обеспечить применение схем групповых подписей.

Отличительной особенностью таких подписей является возможность члена группы подписывать сообщения от лица группы. В статье особое внимание уделяется применению ГП совместно с системами на идентификаторах, в которых члены группы должны быть предварительно зарегистрированы.

В связи с этим, возникает ряд проблемных вопросов. Во-первых, очевидная противоречивость схем ГП и схем на идентификаторах, которая заключается в том, что в системах на идентификаторах идентификатор является открытым ключом пользователя и однозначно определяет его в системе, в отличие от ГП, которая должная обладать свойством анонимности. Также групповые подписи имеют ряд существенных недостатков, связанных с большей длиной подписи и значительно повышенной сложностью по сравнению с традиционными схемами ЭЦП. Одной из наиболее важных проблемных задач, без решения которой невозможно широкое применение ГП в Украине, является ее несоответствие с действующим стандартом электронной цифровой подписи и инфраструктурой открытых ключей на базе сертификатов, которая принята в качестве базовой национальной архитектуры легитимных систем ассиметричной криптографии, а соответственно и с активно развивающейся комбинированной ИОК.

Таким образом, можно сделать вывод о том, что до тех пор, пока не будут разрешены возникшие задачи, групповые подписи могут использоваться пока лишь в корпоративном решении.

Литература

1. Chaum D. Group signatures. In Advances in Cryptology / D. Chaum, E. van Heyst // EUROCRYPT'91, Springer-Verlag, 1991. – V. 547. – P. 257–265.

2. Chen X. A new ID-based group signatures scheme from bilinear pairings / X. Chen, F. Zhang, K. Kim // Cryptology ePrint Archive Report, Report 2003/116.

3. Boneh D. Short group signatures / D. Boneh, X. Boyen, and H. Shacham // CRYPTO, Lecture Notes in Computer Science, Springer-Verlag, 2004. – V. 3152. – P. 41–55.

4. M. Girault. Self-certified public keys / M. Girault // In D.W. Davies, editor, Advances in Cryptology – EUROCRYPT 1991, Lecture Notes in Computer Science, Springer-Verlag, 1992. – V. 547. – P. 490–497.

5. Горбенко І.Д. Схема цифрового підпису із використанням парних відображень на основі стандарту ДСТУ4145-2002 / І.Д. Горбенко, К. А. Погребняк // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения информационной безопасности. Х.: ХНУРЭ, – 2009. – Т. 9, № 3. – С. 290–295.

6. Callas J. Identity-Based Encryption with Conventional Public-Key Infrastructure / J. Callas // In 4th Annual PKI R&D Workshop, number 7224 in Interagency Reports. – 2005. – P. 102 – 115.

7. Koblitz N. Pairing-based cryptography at high security levels, Proceedings of the Tenth IMA International Conference on Cryptography and Coding. / N. Koblitz, A.J. Menezes // Springer-Verlag, LNCS 3796. – 2005. – P. 13–36.

8. Granger R. High security pairing-based cryptography revisited. / Granger R., Page D., Smart N. // Proceedings ANTS-7, Springer LNCS 4096. – 2006. – P. 480–494.

Поступила в редакцию 20.01.2010

Рецензент: д-р техн. наук, заместитель главного конструктора А.В. Потий, ЗАТ "ИИТ", Харьков, Украина.

АНАЛІЗ СУЧАСНИХ ГРУПОВИХ ПІДПИСІВ НА ОСНОВІ ПАРНИХ ВІДОБРАЖЕНЬ ТА ПЕРСПЕКТИВИ ЇХ ВИКОРИСТАННЯ У НАЦІОНАЛЬНОМУ ЕЛЕКТРОННОМУ ДОКУМЕНТООБІГУ

К.А. Погребняк, Ю.М. Іщенко

У цій статті представлено аналіз сучасних групових підписів на основі парних відображень, проводиться дослідження властивостей групових підписів і сфера їх застосування. А також досліджуються деякі питання можливостей застосування таких підписів у національній системі електронного документообігу. Визначається одна з найважливіших проблем застосування групових підписів в Україні, а саме її невідповідності діючому стандарту електронному цифровому підпису та інфраструктурі відкритих ключем на базі сертифікатів.

Ключові слова: електронний цифровий підпис, групові підписи, парні відображення.

ANALYSIS OF CONTEMPORARY GROUP SIGNATURE FROM BILINEAR PAIRINGS AND PROSPECTS OF THEIR USE IN THE NATIONAL SYSTEM OF ELECTRONIC DOCUMENT

K.A. Pogrebnyak, Yu.M. Ishchenko

This article presents an analysis of contemporary group of signatures from bilinear pairings, is to study the properties of group signatures and the scope of their application. And also examines some issues of the use of such signatures in the national system of electronic document. One of the most important problem tasks of group signatures applying in Ukraine is marked out, notably its incompatibility to current electronic digital signature standard and to infrastructure of open keys based on certificates.

Key words: digital signature, group signature, bilinear pairings.

Погребняк Константин Анатольевич – ассистент кафедры Безопасности информационных технологий, Харьковский национальный университет радиоэлектроники, Харьков, Украина, e-mail: iitkostya@gmail.com.

Ищенко Юлия Михайловна – аспирант кафедры Безопасности информационных технологий, Харьковский национальный университет радиоэлектроники, Харьков, Украина, e-mail: ischenko_julia@mail.ru.