О СХЕМАХ «АНОНИМНОЙ ЦИФРОВОЙ ПОДПИСИ» И СХЕМАХ ЦИФРОВОЙ ПОДПИСИ, ОБЕСПЕЧИВАЮЩИХ АНОНИМНОСТЬ

***Варфоломеев Александр Алексеевич**, кандидат физико-математических наук, доцент, г. Москва*

Рассматриваются схемы анонимной цифровой подписи и их отличие от схем цифровой подписи, обеспечивающих анонимность, таких как групповая подпись, кольцевая подпись, подпись вслепую. Предлагается общая конструкция преобразования подписи вслепую в схему анонимной цифровой подписи. Показывается, как на основе произвольной однонаправленной функции с секретом (trapdoor one way function) построить схему кольцевой подписи, обеспечивающей (1 из n) анонимность.

***Ключевые слова**: анонимность, цифровая подпись, анонимная цифровая подпись.*

ON «ANONYMOUS DIGITAL SIGNATURE» SCHEMES AND DIGITAL SIGNATURE SCHEMES TO ENSURE ANONYMITY

***Alexander Varfolomeyev**, Ph.D. (in Math.), Associate Professor, Moscow*

Considered anonymous digital signature schemes and their difference from the digital signature schemes that ensure anonymity, such as group signature, ring signature, blind signature. This paper proposes a general method for conversion blind signature scheme in an anonymous signature. We show how based on an arbitrary trapdoor one–way function to build a ring signature scheme, which provides (1 of n) anonymity.

***Keywords**: anonymity, digital signature, anonymous digital signature.*

Свойство анонимности в некоторых прикладных протоколах, например, в протоколах электронных тайных платежей (Bitcoin и др.), оказалось нежелательным по ряду требований государственных регулирующих органов. Но есть приложения, где без анонимности не обойтись, например, в протоколах электронного тайного голосования (e-Voting), в протоколах электронных аукционов(e-Auctions), в протоколах электронных лотерей (e-Lottery), при анонимном рецензировании документов.

Целью данной работы является выяснение отличий в трактовке понятий схемы «анонимной цифровой подписи» и схем цифровых подписей, обеспечивающих анонимность, а также предложение некоторых методик преобразования известных схем цифровой подписи с дополнением в указанные выше схемы, в частности дающее расширение области применения российских криптографических стандартов.

При этом под анонимностью можно понимать, согласно трактовке Словаря криптографических терминов [10], свойство взаимодействия, обеспечивающее возможность субъекту выполнять какое-либо действие анонимно, т. е. не идентифицируя себя, при этом доказывая свое право на выполнение этого действия. Как известно, родственными понятиями анонимности являются понятия неотслеживаемости (untracebility) и несвязываемости (unlinkability). В криптографической литературе свойство анонимности имеет разные значения, например, различают абсолютную и отзываемую (revocable anonymity) анонимность. В последнем случае должен быть предусмотрен ме-

ханизм, который при определенных условиях может нарушать анонимность и идентифицировать субъекта, выполнившего конкретное действие.

По времени первым было сформулировано понятие анонимности для схем шифрования с открытым ключом [6]. Противнику известен только список возможных открытых ключей шифрования и не известен адресат шифрованного текста. Вводится понятие «неразличимости двух ключей» (indistinguishability) PK_0 и PK_1, заключающееся в невозможности определить по шифрованному тексту C, какой открытый ключ был использован для его получения. У нас нет стандартов на схемы шифрования с открытым ключом, поэтому далее это направление не рассматривается.

Наиболее близким по звучанию к рассматриваемому вопросу кажется понятие «анонимной подписи» (anonymous signature), предложенное в 2006г. в работе [11]. Далее это понятие пересматривалось другими авторами [14, 15], кроме того, оно породило понятие «сильной анонимной подписи» (strong anonymous signature) [16].

Как известно, схема цифровой подписи определяется тройкой алгоритмов $DS = (SKG, SIG, SVF)$, где SKG - алгоритм генерации ключевой пары (pk, sk), SIG – алгоритм выработки цифровой подписи s на основе секретного ключа подписи sk и подписываемого сообщения M, SVF – алгоритм проверки цифровой подписи к сообщению M по открытому ключу проверки подписи pk, который принимает значение 1 или 0 в зависимости от того получено ли s по правилу $s = SIG(sk, M)$ или нет.

Само понятие анонимной подписи вначале представляется невозможным и противоречивым, так как цифровая подпись служит для доказательства аутентичности (подлинности), целостности и неотказуемости (non-repudation). Если злоумышленнику известны открытые ключи проверки подписи некоторого круга лиц, предположительно подписавших документ, то он может установить идентичность подписавшего документ перебором этих открытых ключей и проверкой подписи к документу.

В работе [11] анонимность подписи гарантируется тем, что противник получает в свое распоряжение только саму подпись без подписанного сообщения или, когда сообщение изменено неизвестным противнику случайным образом. Существует много применений, где не требуется предоставления полного сообщения. Например, на аукционе участник может добавить случайную строку r к сообщению m со своей ставкой, подписать это объединенное сообщение, и послать подпись организаторам аукциона. После окончания аукциона и сверки ставок только победитель может предъявить строку r, раскрыв свою идентичность, в то время как остальные участники аукциона могут остаться анонимными. Похожая идея использовалась в работе [13].

Предложенные в работах [15] и [14] схемы, как отмечается во второй работе, близки и могут быть названы схемами «анонимной подписи за счет частичного сокрытия подписи» в отличие от схем подписей из работы [11], которые могут быть названы схемами «анонимной подписи за счет сокрытия сообщения». Если обозначить через $ADS = (AKG, ASIG, AVF)$ – тройку алгоритмов выработки ключей, выработки анонимной подписи и проверки анонимной подписи, то особенностью алгоритма $ASIG$ является выработка двух объектов (as, k) на стадии подписания, где as и является анонимной подписью, а k – является де-анонимайзером (ключом отзыва анонимности) и предоставляется подписавшим на стадии открытия. Требуется, чтобы только зная k проверяющий мог восстановить личность подписавшего и не мог это сделать только по документу M и анонимной подписи as на первой стадии.

В работе [15] предлагается общая конструкция преобразования произвольной схемы цифровой подписи в схему анонимной цифровой подписи с помощью применения схемы секретного залога (обязательства) (commitment scheme) [5], когда анонимная подпись есть секретное обязательство к базовой подписи, а де-анонимайзер это ключ снятия секрета с обязательства. Напомним, что схема секретного залога (обязательства) состоит из двух алгоритмов: CMT – алгоритм выработки секретного залога (обязательства) cs к сообщению M и ключа w раскрытия M по секретному залогу (обязательству); CVF – алгоритм проверки такой, что $CVF(cs, M, w) = 1$ тогда и только тогда, когда $(cs, w) = CMT(M)$. Раскрыть M по известному cs вычислительно невозможно.

Другой подход к требованию обеспечения анонимности можно видеть в схеме «подписи вслепую» (blind signature), идея которой предложена в работах Чаума [2, 3]. В этой схеме требуется обеспечить анонимность не подписывающего, а того, кто создал документ и желает получить

корректную подпись подписывающего так, чтобы подписывающий при подписании не знал содержание подписываемого документа и не мог впоследствии по документу и своей корректной подписи определить, кому и когда он его подписал. В схеме подписи вслепую различают таким образом три роли: создатель документа, подписывающий документы (например, нотариус) и проверяющий подпись под документом.

В схемах подписи вслепую различают следующие стадии: инициализация, затемнение сообщения, запрос подписи затемненного сообщения, подпись затемненного сообщения, выделение из подписи затемненного сообщения корректной подписи исходного сообщения.

На стадии инициализации подписывающий объявляет об открытых параметрах своей цифровой подписи. Например, [3], подписывающий использует цифровую подпись по схеме RSA с открытым ключом проверки (n, e).

На стадии затемнения документ M «затеняется» с помощью функции затенения Z = U(M, k) и ключа затенения k. В примере с цифровой подписью RSA: Z = U(M, k) = M (k^e). Именно затененный документ Z направляется на подпись подписывающему лицу, который не может знать документ M без знания ключа k.

На стадии подписи затененного документа подписывающий вычисляет свою цифровую подпись под документом Z с помощью своего секретного ключа подписи SK_DS: R = Sign(Z, SK_DS). Значение R возвращается создателю исходного документа M. В примере с цифровой подписью RSA: R = Sign (Z, SK_DS) = (Z^d) mod n.

На стадии выделения подписи создатель документа, зная секретный ключ k, вычисляет подпись s к документу M на секретном ключе подписи SK_DS с помощью функции снятия затемнения s = V(R, k) = Sign (M, SK_DS). В примере с цифровой подписью RSA: s = (M^d) mod n, V(R, k) = = (R / k) mod n.

В данной работе предлагается общая конструкция преобразования произвольной схемы подписи вслепую в схему анонимной цифровой подписи. Именно предлагается использовать стадию снятия затемнения как вторую стадию в схеме анонимной подписи с сокрытием подписи, стадию затемнения и запроса подписи объединить и сделать первой стадией в схеме анонимной подписи с сокрытием подписи. В приведенных выше обозначениях, документ и анонимная цифровая подпись к нему есть пара (M, R), вычисляемые по схеме подписи вслепую (M, Sign(U(M, k), SK_DS). Здесь роли создателя документа и подписывающего его вслепую объединены в одну роль, а ключ затенения k выполняет роль де-анонимайзера. При этом схема базовой цифровой подписи может быть любой (в том числе и по ГОСТ Р 34.10). На второй стадии протокола анонимной подписи подписывающий предъявляет проверяющему ключ k. В примере с цифровой подписью RSA значения M и R приведены выше. Известно, что можно схему подписи вслепую реализовать на основе ГОСТ 34.10.

Задачу обеспечения анонимности члена некоторой группы, подписавшего документ, ранее решали схемы групповой подписи (group signature) и кольцевой подписи (ring signature), название которых не говорит явно об анонимности. Концепции этих схем подписи предложили соответственно в работах [4] и [7] ранее, чем понятие анонимной подписи из работы [11]. Групповая подпись отличается от кольцевой наличием некоторого выделенного участника, способного при необходимости восстановить идентичность подписавшего, то есть отозвать анонимность. В 2013 году вышли международные стандарты, в названии которых непосредственно содержится термин «анонимные цифровые подписи» ([21], [22]). Из введения к этим стандартам сразу становится понятным, что они связаны именно с групповой и кольцевой подписями. Но групповая/кольцевая подпись имеет сложную структуру (включая открытые ключи проверки участников кольца/группы) и анонимность зависит от числа членов в группе (1-из-n). Анонимная же подпись по определению [11] должна иметь обычную структуру, но дополнительно обеспечивать анонимность подписавшего.

В заключении работы рассмотрим общую схему построения кольцевой подписи, обеспечивающей (1 из n) анонимность, на основе произвольной однонаправленной функции с секретом. Как известно, понятие однонаправленной функции с секретом (с потайной дверью, с лазейкой) y = f_k (x) было дано в работе [1], и оно может быть использовано для построения как схем шифрования с открытым ключом, так и схем цифровой подписи. Символ k здесь обозначает дополнительную секретную информацию (секрет, лазейка),

позволяющую вычислять прообраз для случайно выбранного значения y. Например, в схемах RSA эта функция имеет вид y = f_k (x) = (x^e) mod n, где n = p q, а секретная информация заключается в знании больших простых чисел p и q.

В случае использования функции y = f_k (x) для построения цифровой подписи с дополнением DS = (SKG, SIG, SVF) в качестве алгоритма SIG выработки цифровой подписи s на основе секретного ключа подписи sk и подписываемого сообщения M может быть использован алгоритм вычисления прообраза этой функции от сообщения M, а секретный ключ определяется указанной секретной дополнительной информацией, позволяющей ее владельцу это делать. s = SIG (sk, M) = f^(-1)_k(M). В качестве алгоритм SVF проверки цифровой подписи s1 к сообщению M1 по открытому ключу проверки подписи pk может быть использован алгоритм вычисления функции

f_k (s1) от s1 и сравнение этого значения с M1, то есть проверка выполнения соотношения

f_k (s1) = M1. В этом случае цифровая подпись s1 считается корректной к сообщению M1. Открытым ключом pk является описание алгоритма вычисления функции.

Заметим, что злоумышленник без знания секретного ключа не может вычислить прообраз из выбранного им сообщения M, но он может создать корректную пару (s2, M2) цифровой подписи и сообщения, выбирая s2 и вычисляя M2 = f_k (s2), так как проверка заключается именно в проверке выполнения этого условия, как сказано выше. Поэтому, чтобы избежать этого в схемах цифровой подписи подписывается значение однонаправленной функции (в частности хэш-функции) от сообщения M. В этом случае злоумышленнику, в отличие от законного пользователя, пришлось бы вычислять прообраз однонаправленной функции от сгенерированного им ложного текста M2. Но именно это свойство строить корректные пары в отсутствии использования однонаправленной функции будет использовано при построении кольцевой подписи.

Кольцевая подпись s группы из n человек, обладающих ключевыми парами открытых и секретных ключей (PK_1, SK_1), (PK_2, SK_2), ... ,(PK_n, SK_n) обычной цифровой подписи с дополнением, вычисляется i – тым членом группы для сообщения M на основе знания открытых ключей группы и своего секретного ключа. Требуется, чтобы корректную пару из сообщения M и кольцевой подписи s к нему мог создать только знающий один из секретных ключей подписи.

Предложенную в работе [7] схему кольцевой подписи на основе схемы RSA можно обобщить на произвольные цифровые подписи с использованием однонаправленных функций с секретом fi_ki(x).

При выработке кольцевой подписи подписывающий создает за остальных членов группы корректные пары (Mj, sj) зная алгоритмы вычисления однонаправленных функций с секретом, как это делал бы злоумышленник описанным выше способом без знания секретной информации. Mj = fj_kj (sj). Далее вычисляет сообщение Mi из соотношения, определяемого так называемой комбинационной функцией [7] вида

$C_{k,v} = E_k(Mn \oplus E_k(M(n-1) \oplus E_k(\dots \oplus E_k(M1 \oplus v) \dots) = v.$

Именно получаем $Mi = D_k(M(i+1) \oplus \dots D_k(Mn \oplus D_k(v)) \oplus (\dots \oplus D_k(M1 \oplus v) \dots))$.

$\oplus$ – операция побитового сложения векторов по модулю 2.

Здесь E_k (D_k) обозначает преобразование зашифрования (расшифрования) на ключе k = H(M), вычисляемом как значение хэш - функции от подписываемого по схеме кольцевой подписи сообщения M, v – случайный вектор инициализации, размеры векторов выравниваются дописыванием до наибольшего. В предположении случайно выбранных sj и полученных Mj (модель случайного оракула), значение Mi будет также случайным даже при известной комбинационной функции. После нахождения Mi – го вычисляет, зная свою секретную информацию, прообраз si функции fi_ki(x) от значения Mi. Тогда значением кольцевой подписи к сообщению M будет набор $(PK_1, PK_2, \dots, PK_n, v, s1, \dots, sn)$.

При проверке проверяющий зная M, кольцевую подпись $(PK_1, PK_2, \dots, PK_n, v, s1, \dots, sn)$ и вид комбинационной функции находит k = H(M), проверяет равенства Mi = fi_ki (si) для всех i = 1, …, n и равенство $C_{k,v}(M1, \dots, Mn) = v$.

В качестве комбинационной функции могут выступать и отличные от приведенной выше функции, в частности не использующие преобразование зашифрования, а только преобразование с помощью хэш-функции [12]. В заключении отметим, что данная конструкция может быть реализована с использованием только российских криптографических стандартов.

Литература (References)

1 Diffie W., Hellman M., New directions in cryptography, IEEE Trans. On IT, v. IT-22, n.6, 1976, 644-654.
2 Chaum D., Blind signatures for untraceable payments. Crypto'82, 1983, 199-203.
3 Chaum D., Security without identification: transaction systems to make big brother obsolete, Comm. Of the ACM, v.28, n.10, 1985, 1030-1044.
4 Chaum D., Heyst V. E., Group signature. Eurocrypt'91. LNCS v. 547, 1991, 257-265.
5 Schneier B. Applied cryptography. Protocols, algorithms, and source code in C, 1996.
6 Bellare M., Boldyreva A., Desai A., Pointcheval D., Key-Privacy in Public-Key Encryption. Asiacrypt'01, LNCS 2248, 566–582. Springer, 2001.
7 Rivest R., Shamir A., Tauman Y., How to leak a secret. Asiacrypt'01, LNCS v.2248, 2001, 552-565.
8 Saeednia S.. An identity-based society oriented signature scheme with anonymous signers. Information Processing Letters, 2002, 83: 295-299.
9 Guilin Wang, Bo Zhu, Remarks on Saeednia's Identity-based Society Oriented Signature Scheme with Anonymous Signers. ePrint archive 2003/046, 6.
10 Словарь криптографических терминов. Под. ред. Б.А. Погорелова и В.Н. Сачкова. - М: МЦНМО, 2006, 94с.
11 Yang G., Wong D., Deng X., Wang H., Anonymous Signature Schemes. PKC'06, LNCS v. 3958, 347–363. Springer, 2006.
12 Ren J., Harn L., Ring signature based on ElGamal Signature, LNCS v. 4138, 2006, 445-456.
13 Fischlin M., Anonymous Signatures Made Easy. PKC'07, LNCS v. 4450, 31–42, 2007.
14 Saraswat V., Yun A., Anonymous Signatures Revisited, 2009.
15 Bellare M., Duan S., New Definitions and Designs for Anonymous Signatures, 2006.
16 Zhang R., Imai H., Strong Anonymous Signatures, Inscrypt 2008, LNCS v. 5487, 60-71, 2009.
17 Ma C., Ao J., Anonymous signature scheme, ePrint archive 2009/017, 6c.
18 Lee H., Choi J., Kim K.K., Impact of anonymity on information sharing (Anonymity, Unobservability, and Pseudonymity).
19 Saraswat V., Anonymity and Privacy in Public key Cryptography, diss. Doctor of Philosophy.2012, 67c.
20 Kuzhalvaimozhi S., Rao G.R., Generating of anonymous Signature and Message using ID based Group Blind Signature. ACEEE Int. J. on Network Security, v. 4, n. 1, 2013.
21 ISO/IEC 20008-1:2013 Information technology -- Security techniques -- Anonymous digital signatures -- Part 1: General. 20c.
22 ISO/IEC 20008-2:2013 Information technology -- Security techniques -- Anonymous digital signatures -- Part 2: Mechanisms using a group public key. 86c.