СПЕЦИАЛЬНЫЕ СХЕМЫ ЦИФРОВОЙ ПОДПИСИ

Долгов В.И., Неласая А.В.
Харьковский национальный университет радиоэлектроники,
61166, Харьков, пр. Ленина, каф. безопасности информационных технологий,
email: gorbenko@kture.kharkov.ua.

The given work is devoted to the collective digital signature protocols on elliptical and hyperelliptical curves based on the idea of general use public key worked out by the authors. These curves have a property that the size of the signature do not increase proportionally for the number of signature participant and if we use the hyperelliptical curve of the size of the signature is decreased proportionally for genus of curve yet . It is shown that the result of strength analysis of the proposed protocols to coupled key attack, only reuse key attack, existential falsification and in the presence of more then one signed message attack.

Принятие украинского стандарта цифровой подписи ДСТУ 4145 стало заметным событием в украинской криптографии, и его достоинства получили заслуженную высокую оценку специалистов. Однако он специфицирует лишь двухточечный протокол цифровой подписи и не покрывает все многообразие отношений, возникающих при взаимодействии сторон. В некоторых ситуациях могут потребоваться специальные схемы электронной подписи, отличные от классических двухточечных схем.

Групповая подпись позволяет верификатору убедиться в принадлежности полученного сообщения некоторой группе претендентов, но кто именно из членов группы подписал документ, верификатор определить не в состоянии. Концепция групповой подписи предложена Д. Шаумом и Е. Хейстом в 1991 году [1]. Это метод, позволяющий членам группы анонимно подписать сообщение от лица всей группы. Например, схема групповой подписи может быть использована служащим большой компании, если для верификатора важно, что сообщение подписано служащим этой компании, но не важно, каким именно. Для этой схемы существенно наличие менеджера группы, который формирует группу и имеет возможность выявить действительного подписанта в случае возникновения разногласий. В некоторых системах ответственность за создание группы и аннулирование анонимности разделены и существуют два различных менеджера соответственно.

Кольцевая подпись [2] делает возможным специфицировать набор возможных подписантов без разоблачения, кто именно из них действительно произвел подписание. В отличие от групповой подписи, кольцевая подпись не имеет менеджеров группы, процедур установки (setup), процедур аннулирования и координации: любой пользователь может выбрать любой набор возможных подписантов, включающий его самого, и подписать любое сообщение, используя свой секретный ключ и открытые ключи остальных без получения их одобрения или помощи. Кольцевая подпись обеспечивает элегантный путь рассеять аутентификационные секреты анонимным путем.

Схема подписи с назначенным получателем [3] – это схема, в которой подпись может быть проверена только единственным «назначенным получателем», выбранным подписантом. Например, две компании могут обмениваться проектами предполагаемых контрактов. Они хотят добавлять к каждому e-mail аутентификатор, но не реальную подпись, которая может быть показана третьей стороне (немедленно или годы спустя) как доказательство, что частный проект был предложен второй компанией. Схема подписи с назначенным получателем может также рассматриваться как «легкая схема подписи», которая может аутентифицировать сообщения для их непосредственного получателя без наделения свойством строгого выполнения обязательств.

Слепая электронная подпись была предложена Д. Шаумом [4] для защиты от подделки электронных денег. В этом случае абонент подписывает документ, не зная его содержимого. Такая технология была предложена для того, чтобы сделать электронную купюру анонимной.

Схема подписи с открытым ключом, основанным на идентификаторе пользователя [5] позволяет любой паре пользователей проверять подписи друг друга без обмена

секретными или открытыми ключами, без хранения ключей в каталогах, без использования услуг третьей стороны. Эта схема предполагает существование доверенных центров генерации ключей, чья единственная цель состоит в том, чтобы дать каждому пользователю смарт-карту, когда он первый раз входит в сеть. Информация, записанная на этой карте, позволяет пользователю подписывать и зашифровывать сообщения, которые он посылает, и расшифровывать и проверять сообщения, которые он получает совершенно независимо, не обращая внимания на идентификатор другой стороны.

В схеме конфиденциальной (неотвергаемой) подписи подпись не может быть проверена без участия сформировавшего ее участника протокола.

Схема разделяемой (коллективной) подписи [6,7] формируется только при участии определенного количества участников протокола, иначе говоря, данная схема является объединением классической схемы подписи и схемы разделения секрета.

Кроме рассмотренных имеются и другие варианты построения специфических схем цифровой подписи.

В докладе предлагаются разработанные авторами протоколы коллективной цифровой подписи на эллиптических и гиперэллиптических кривых, базирующейся на понятии общего (коллективного) открытого ключа. Они обладают тем качеством, что размер подписи не увеличивается пропорционально числу подписавших участников, а в случае использования гиперэллиптических кривых даже уменьшается пропорционально роду кривой. Приводятся результаты анализа стойкости предложенных протоколов к атаке на связанных ключах, атаке при повторном использовании разового ключа, экзистенциальной подделке, атаке при наличии нескольких подписанных сообщений.

Приведем для иллюстрации пример анализа стойкости протокола коллективной подписи на эллиптической кривой [8] на основе ECPR, предложенного авторами в [9]. В этом случае речь идет о формировании одной и той же цифровой подписи при передаче двух разных сообщений M_1 и M_2.

По сравнению с двухточечным протоколом задача злоумышленника осложняется тем, что для осуществления этой атаки ему необходимо знать значения временных секретов k_i всех участников протокола коллективной подписи с учетом того, что эти значения получены на разных клиентских станциях и не передаются на сервер.

Выберем связанные ключи k_i, $k_i' = n - k_i$ и выясним условия, при которых ЦП $<r,s>$ и $<r',s'>$ для сообщений M_2 и M_1 и будут одинаковыми.

Алгоритм выработки ЦП для сообщений M_1 и M_2 в соответствии с таблицей 1 предопределяет:

Таблица 1. Атака на связанных ключах.

Для сообщения M_1	Для сообщения M_2
1. Определяется $h_1 = H(M_1) (\mathrm{mod}\, n)$;	1. Определяется $h_2 = H(M_2) (\mathrm{mod}\, n)$;
2. Каждый пользователь выбирает $0 < k_i < n$;	2. Вычисляются $k_i' = n - k_i$;
3. Каждый пользователь вычисляет $t_i = \frac{k_i}{h_1} (\mathrm{mod}\, n)$;	3. Вычисляются $t_i' = \frac{k_i'}{h_2} = \frac{n-k_i}{h_2} \to \frac{n-k_i}{h_2} \equiv -\frac{k_i}{h_2} (\mathrm{mod}\, n)$;
4. Каждый пользователь вычисляет точку $R_i = (t_i \times P)$ и отправляет на сервер;	4. Вычисляются точки $R_i' = (t_i' \times P)$;
5. На сервере вычисляется общая точка $R = \sum_{i=1}^{l} R_i = (X_R, Y_R)$,	5. Вычисляется общая точка $R' = \sum_{i=1}^{l} R_i' = (X_{R'}, Y_{R'})$;
6. значение $w = \pi(R) = X_R \bmod n$,	6. Вычисляется значение $w' = \pi(R') \bmod n = X_{R'} \bmod n$;

7. формируется точка $wR = w\sum_{i=1}^{l} t_i P = (x, y)$, 8. вычисляется первая часть коллективной подписи $r = \pi(wR) = x(\mathrm{mod}\, n)$ и рассылается всем пользователям; 9. Каждый пользователь вычисляет $s_i = (wk_i + h_1 d_i)(\mathrm{mod}\, n)$ и отправляет на сервер; 10. На сервере вычисляется вторая часть коллективной подписи $s = \sum_{i=1}^{l} s_i (\mathrm{mod}\, n)$.	7. Формируется точка $w' \times R' = w' \sum_{i=1}^{l} t_i' \times P = (x', y')$; 8. Вычисляется первая часть подписи $r' = \pi(w' \times R') = x'(\mathrm{mod}\, n)$; 9. Вычисляются составные части второй части подписи $s_i' = (w'(n - k_i) + h_2 d_i)(\mathrm{mod}\, n)$; 10. Вычисляется вторая часть коллективной подписи $s' = \sum_{i=1}^{l} s_i' (\mathrm{mod}\, n)$.

Таким образом, при разных сообщениях M_1 и M_2 равенство $r = r'$ возможно либо при наличии коллизии: $h_2 = h_1 \rightarrow t_i' = -t_i(\mathrm{mod} n) \rightarrow R_i' = -R_i \rightarrow R' = -R \rightarrow X_{R'} = X_R \rightarrow w' = w(\mathrm{mod}\, n) \rightarrow (x', y') = w' \times R' = -wR \rightarrow x' = x(\mathrm{mod}\, n) \rightarrow r' = r(\mathrm{mod}\, n)$, либо при $h_2 = -h_1 \rightarrow t_i' = \frac{(n - k_i)}{h_2} = \frac{(n - k_i)}{(-h_1)} = \frac{(-k_i)}{(-h_1)} = \frac{k_i}{h_1} = t_i(\mathrm{mod} n) \rightarrow R_i' = R_i \rightarrow R' = R \rightarrow X_{R'} = X_R \rightarrow w' = w(\mathrm{mod}\, n) \rightarrow (x', y') = w' \times R' = wR \rightarrow x' = x(\mathrm{mod}\, n) \rightarrow r' = r(\mathrm{mod}\, n)$.

Равенство $t_i' = t_i$ можно получить для разных хэш-значений $h_1 \neq h_2$, но при $\frac{k_i}{h_1} = \frac{k_i'}{h_2}(\mathrm{mod}\, n)$, что при $k_i' = n - k_i'(\mathrm{mod}\, n)$ приводит к условию $\frac{k_i}{h_1} = \frac{(n - k_i)}{h_2}(\mathrm{mod}\, n)$, либо $\frac{k_i}{h_1} = \frac{-k_i}{h_2}(\mathrm{mod}\, n) \rightarrow k_i h_2 = -k_i h_1(\mathrm{mod}\, n) \rightarrow k_i(h_2 + h_1) = 0(\mathrm{mod}\, n)$.

Так как необходимо, чтобы выполнялось еще и равенство $s' = s$, то, приравнивая соответствующие выражения в десятой строке таблицы, получим:

В первом случае $h_2 = h_1$, а, следовательно, $w' = w$ имеем

$s' = \sum_{i=1}^{l} s_i'(\mathrm{mod}\, n) = \sum_{i=1}^{l} (w'(n - k_i) + h_2 d_i)(\mathrm{mod}\, n) = \sum_{i=1}^{l} (-wk_i + h_1 d_i)(\mathrm{mod}\, n)$ и соответственно

$s = \sum_{i=1}^{l} s_i (\mathrm{mod}\, n) = \sum_{i=1}^{l} (wk_i + h_1 d_i)(\mathrm{mod}\, n) \rightarrow (wk_i + h_1 d_i) = (-wk_i + h_1 d_i)(\mathrm{mod}\, n) \rightarrow$

$2wk_i = 0(\mathrm{mod}\, n)$, что маловероятно.

Во втором случае при $h_2 = -h_1$, когда также $w' = w$ имеем:

$s' = \sum_{i=1}^{l} s_i'(\mathrm{mod}\, n) = \sum_{i=1}^{l} (w'(n - k_i) + h_2 d_i)(\mathrm{mod}\, n) = \sum_{i=1}^{l} (-wk_i - h_1 d_i)(\mathrm{mod}\, n)$ и

$s = \sum_{i=1}^{l} s_i (\mathrm{mod}\, n) = \sum_{i=1}^{l} (wk_i + h_1 d_i)(\mathrm{mod}\, n) \rightarrow (wk_i + h_1 d_i) = (-wk_i - h_1 d_i)(\mathrm{mod}\, n) \rightarrow$

$2(wk_i + h_1 d_i) = 0(\mathrm{mod}\, n)$, что также маловероятно.

В результате можно сделать вывод, что предложенный протокол является устойчивым к атаке на связанных ключах.

Анализ стойкости рассматриваемого протокола к атаке при повторном использовании параметра k_i показал, что предложенный протокол коллективной подписи являет-

ся стойким даже к этой атаке в том случае, когда каналы связи участников протокола с сервером являются защищенными. В противном случае предложенная схема уязвима и необходимо тщательно следить, чтобы участники протокола не использовали повторно в ключи. Однако уязвимость проявляется лишь в том случае, если все участники одновременно в одних и тех же сеансах подписи используют повторно ключи. На практике такая ситуация представляется крайне маловероятной.

Все многообразие рассмотренных специальных схем подписи может найти практическое применение лишь при появлении соответствующих им государственных стандартов.

Перечень ссылок:

1. D. Chaum and E. van Heyst. "Group signatures". Advances in Cryptology — EUROCRYPT ’91, volume 547 of Lecture Notes in Computer Science: 257-265.
2. R. Rivest, A. Shamir, Y. Tauman. How to leak a secret, Advances in Cryptology - ASIACRYPT 2001, LNCS 2248, Springer-Verlag, 2001, pp. 552-565.
3. M.Jakobsson, K.Sako, R.Impagliazzo. Designated verifier proofs and their applications, LNCS 1070, Proc. Eurocrypt'96, Springer Verlag, (1996), pp. 67-74.
4. D. Chaum. Blind signatures for untraceable payments. Advances in Cryptology - Crypto '82, Springer-Verlag (1983), pp. 199-203.
5. A. Shamir. Identity-Based Cryptosystems and Signature Schemes. Advances in Cryptology: Proceedings of CRYPTO 84 (1984), Lecture Notes in Computer Science, 7: pp. 47-53.
6. Min-Shiang Hawng, Cheng-Chi Le. Research issues and challenges for multiple digital signature// Int. J. of Network Security. – 2005. – Vol. 1. – No 1. –P. 1-7.
7. Гортинская Л.В., Молдовян Н.А., Козина Г.Л. Реализация протоколов коллективной подписи на основе стандартов ГОСТ 34.310–95 и ДСТУ 4145-2002 // Правове, нормативне та метрологичне забезпечення системи захисту інформації в Україні. – Киев: НТУУ “КПІ”. – 2008. – № 1. – С.21.
8. Неласая А.В, Козина Г.Л, Молдовян Н.А. Протоколы коллективной цифровой подписи на эллиптических и гиперэллиптических кривых.// Радіоелектроніка. Інформатика. Управління. №1(19).-Запоріжжя, 2008, с.127-133.
9. Долгов В.И., Неласая А.В., Погорелый А.Н. К вопросу применения и совершенствования стандарта электронной цифровой подписи в Украине// Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации, ХНУРЭ, 2008.