computing@computingonline.net
www.computingonline.net

ISSN 1727-6209
International Journal of Computing

ПРОТОКОЛЫ ЦИФРОВОЙ ПОДПИСИ С БЫСТРОЙ ПРОЦЕДУРОЙ ПРОВЕРКИ ПОДПИСИ

Неласая А.В. [1], Долгов В.И. [2], Погорелый А.Н. [3]

[1] Запорожский национальный технический университет, кафедра программных средств,
ул. Жуковского 64, г. Запорожье, 69063, Украина, nelasa@mail.zp.ua
[2] Харьковский национальный университет радиоэлектроники,
кафедра безопасности информационных технологий,
пр. Ленина, 14, г. Харьков, 61166, Украина, dolgovvi@mail.ru
[3] Государственное предприятие "Радиоприбор", отдел защиты информации
пр. Ленина 3, г. Запорожье, 69000 Украина, anpogo@yandex.ru

Резюме: *В статье предлагаются индивидуальный и коллективный протоколы цифровой подписи на эллиптических кривых с быстрой процедурой проверки подписи для использования в корпоративной сети.*

Ключевые слова: *Эллиптическая кривая, протокол цифровой подписи, секретный ключ, открытый ключ, корпоративная сеть.*

ВВЕДЕНИЕ

В 2007 году нашему национальному стандарту электронной цифровой подписи ДСТУ 4145-2002 [1] исполнилось 5 лет, что является хорошим поводом для обмена опытом по его применению. Само появление подобного стандарта стало заметным событием в украинской криптографии, и его достоинства получили заслуженную высокую оценку специалистов. К сожалению, за прошедшие 5 лет так и не состоялся процесс широкого внедрения электронной цифровой подписи (ЭЦП) реальную жизнь граждан и государства.

Требования, предъявляемые к реализации стандарта в виде программных или аппаратных средств специфицируют скорость процедуры формирования подписи. Однако на практике процедура проверки подписи выполняется значительно чаще. При этом время проверки подписи по процедуре действующего стандарта в практических реализациях значительно превышает время формирования подписи. Целью данной работы является попытка устранить это противоречие.

Развитие технологий электронного документооборота требует также новых механизмов обеспечения юридической силы коллективных электронных документов. В частности, при разработке коллективных проектов важной проблемой является использование протоколов [2-5], обеспечивающих реализацию коллективной электронной цифровой подписи.

Предложенные недавно протоколы [3-5] формирования и проверки подлинности коллективной электронной цифровой подписи используют общий (коллективный) открытый ключ, который формируется на основе индивидуальных открытых ключей группы пользователей.

Важен также вопрос минимизации размера коллективной электронной цифровой подписи при необходимости ее записи в виде штрих-кода на бумажных носителях, например, в методах защиты от подделки документов с помощью электронной цифровой подписи [5].

В данном аспекте представляет интерес изучение вопроса о возможности реализации новых протоколов коллективной электронной цифровой подписи как с использованием процедур проверки электронной цифровой подписи, специфицируемых стандартами подписи, так и новых протоколов, позволяющих уменьшить размер подписи.

1. ПРОТОКОЛ ЦИФРОВОЙ ПОДПИСИ С ПРЕДВЫЧИСЛЕНИЯМИ ДЛЯ КОРПОРАТИВНОЙ СЕТИ

В настоящей работе предлагается протокол цифровой подписи для корпоративной сети,

широко использующий возможности предвычислений в операции скалярного умножения точки эллиптической кривой на число. Назовем этот протокол ECPR (Elliptic Curve with PRecomputation).

В существующих протоколах цифровой подписи в алгоритме проверки присутствует операция умножения числа открытый ключ, точку эллиптической кривой, традиционно обозначаемую Q. Методика проверки подписи основана на операциях с индивидуальными открытыми ключами абонента. В отличие от базовой точки P, которая является одним из параметров криптосистемы и является единой для множества абонентов, точка Q – индивидуальна для каждого субъекта, обладающего правом подписи. Если таких субъектов в корпоративной сети множество, выполнять предвычисления для точки Q бессмысленно, в отличие от предвычислений для точки P. Поэтому основная сложность возникает при проверке множества подписей абонентов в центрах или у потребителей документов множества абонентов. При этом реализация алгоритма вычисления ЭЦП требует существенно меньше времени, чем для проверки. Естественно, возникает вопрос: как ускорить проверку ЭЦП?

Нельзя ли заменить методику проверки ЭЦП так, чтобы использовать одну базовую точку множества корпоративных абонентов а результат проверки сравнивать с открытым ключом абонента? Такой подход позволил бы хранить в базах данных корпоративные базовые точки и в полной мере использовать возможности предвычислений, которые ныне бессмысленны для множества абонентов. Разумеется, с математической и криптографической точек зрения изменения методик выработки и проверки ЭЦП не должны затрагивать вопросы криптографической стойкости и математической эквивалентности. Одно из разработанных нами предложений в этом направлении излагается ниже.

Анализ протоколов цифровой подписи на эллиптических кривых [1,6-8] таких, как ДСТУ 4145, ГОСТ Р 34.10, ECDSA, ECSS, EC-GDSA, EC-KCDSA, алгоритм Шнорра, показал, что в процедуре верификации подписи во всех перечисленных протоколах присутствует операция скалярного умножения открытого ключа Q на число. Как упоминалось ранее, для этой операции использование предвычислений бессмысленно, так как в отличие от базовой точки P, которая является единой для всех абонентов корпоративной сети, открытый ключ Q у каждого свой.

Главная идея предлагаемого авторами подхода – уйти от умножения открытого ключа Q на какой бы то ни было числовой множитель. В таблице 1 приведен один из вариантов реализации подобного подхода.

Таблица 1. Протокол цифровой подписи на эллиптической кривой ECPR

Формирование ЭЦП
Вход: эллиптическая кривая C, секретный ключ d, открытый ключ $Q = -d \times P$, P - базовая точка, n - порядок базовой точки, сообщение M. **Выход**: ЦП $\langle r, s \rangle$ для сообщения M.
1. $h = H(M) \bmod n$; **2.** Генерируем случайное $k \in \{1, ..., n-1\}$; **3.** $t = \frac{k}{h} \bmod n$; **4.** $R = t \times P$; **5.** $w = \pi(R) \bmod n$; **6.** $(x, y) = w \times R = w \times t \times P$; **7.** $r = \pi(x, y) \bmod n$; **8.** $s = (wk + hd) \bmod n$.
Верификация ЭЦП
Вход: эллиптическая кривая C, открытый ключ Q, P - базовая точка, n - порядок базовой точки, ЦП $\langle r', s' \rangle$, для сообщения M'. **Выход:** Подпись действительна или нет.
1. $h' = H(M) \bmod n$; **2.** $t = \frac{s'}{h'} \bmod n$; **3.** $(x', y') = t \times P + Q$; **4.** $v = \pi(x, y) \bmod n$; **5.** $r' \stackrel{?}{=} v$

Обозначения: $h(M)$ – хеш-функция, π – функция выделение $x \bmod n$.

Определяющее соотношение для предложенного протокола выглядит следующим образом:

$$\frac{(wk + hd)}{h} P + Q = \frac{wk}{h} P + dP - dP = \frac{wk}{h} P$$

Как видно из процедуры формирования подписи $r = \pi(\frac{wk}{h} P)$. Соответственно в процедуре верификации $v = \pi(\frac{wk}{h'} P)$. Следовательно, значения r и v равны, если сообщения и подписи в обоих случаях идентичны.

2. ОЦЕНКА СЛОЖНОСТИ ПРОТОКОЛА ECPR

Сравним количество различных операций предложенного авторами протокола и основных стандартов ЭЦП на эллиптических кривых.

За счет добавления одной операции умножения в поле, одной операции инверсии в поле и одной операции скалярного умножения на базовую точку, которую можно выполнять с предвычислениями, в процедуре формирования подписи, разгружается процедура проверки подписи. В ней, в отличие от других стандартов, напрочь отсутствует наиболее трудоемкая операция скалярного умножения на открытый ключ Q, которую затруднительно выполнять с предвычислениями в корпоративной сети.

Приведенные алгоритмы были реализованы авторами с использованием библиотеки Miracl. В случае простого поля длина модуля преобразований была выбрана 256 бит. В случае расширенного поля в качестве модуля был выбран полином 191 степени. Величина окна для предвычислений в обоих случаях выбрана равной 5. Время предвычислений не учитывалось при измерении времени выполнения операций формирования и проверки. В случае простого поля оно составило приблизительно 2,2E+04 мкс, в случае расширенного – 1,0 E+04 мкс.

Таблица 2. Сравнительный анализ количества операций протоколов цифровой подписи

	ECPR		**ГОСТ Р 34.10**		**ДСТУ 4145**		**ECDSA**	
Операция	Форми-рование	Про-верка	Форми-рование	Про-верка	Форми-рование	Про-верка	Форми-рование	Про-верка
$h(M)$	1	1	1	1	1	1	1	1
$\pi(x,y) \bmod n$	2	1	1	1	2[1]	1[2]	1	1
Умножение в F_n	3	1	2	2	2	1	2	2
Инверсия в F_n	1	1	-	1	-	-	1	1
Групповое сложение точек ЭК	-	1	-	1	-	1	-	1
Скалярное умножение на P	2	1	1	1	1	1	1	1
Скалярное умножение на Q	-	-	-	1	-	1	-	1

Таблица 3 Сравнительный анализ скорости протоколов цифровой подписи

	ECPR над GF(p)		**ГОСТ Р 34.10 над** GF(p)		**ECDSA над** GF(p)		**ECPR над** GF(2^m)		**ДСТУ 4145 над** GF(2^m)	
	Форми-рование	Проверка	Форми-рование	Провер-ка	Форми-рование	Провер-ка	Форми-рование	Проверка	Форми-рование	Проверка
Время, мкс	2,6E+08	1,4E+08	1,3E+08	5,0E+08	1,3E+08	5,2E+08	1,6E+08	8,7E+07	8,0E+07	2,4E+08

[1] В процедуре формирования один раз используется операция π и один раз операция преобразования элемента поля F_{2^m} в число.

[2] В процедуре проверки используется операция преобразования элемента поля F_{2^m} в число.

Эксперименты проводились на компьютере Dell Inspiron I6400 Intel(R) Core(TM)2 CPU T5600 @1.83GHz 987МГц, 512 МБ ОЗУ. В таблице 3 приведено время выполнения 100000 операций формирования и проверки цифровой подписи.

3. ПРОТОКОЛ КОЛЛЕКТИВНОЙ ПОДПИСИ НА ОСНОВЕ ECPR

Протокол электронной цифровой подписи с предвычислениями ECPR предложен с целью уменьшить трудоемкость операции верификации подписи в корпоративной сети за счет умножения только на базовую точку, которое можно выполнить с предвычислениями. Модифицируем этот протокол для реализации коллективной подписи.

Введем обозначения:

P -базовая точка эллиптической кривой;

l - количество пользователей;

n - порядок циклической подгруппы точек эллиптической кривой;

d_i - секретный ключ i-го пользователя;

h – хэш–образ сообщения;

$\pi(R) = X_R \bmod n$ - выделение x-координаты точки $R=(X_R, Y_R)$ эллиптической кривой.

Генерация открытого коллективного ключа.

1. Каждый i-й пользователь $(i=1..l)$ формирует открытый ключ вида

$$Q_i = -d_i P$$

.

2. Коллективный открытый ключ вычисляется как сумма открытых ключей группы из l пользователей

$$Q = \sum_{i=1}^{l} Q_i = \sum_{i=1}^{l} -d_i P$$

Формирование коллективной подписи.

1. Каждый i-й пользователь $(i=1..l)$ рассчитывает точку R_i следующим образом:

а) выбирает случайный параметр k_i, $1 < k_i < n$,

б) вычисляет значение $t_i = \frac{k_i}{h} \bmod n$;

в) и точку $R_i = t_i P$.

2. По представленным пользователями точкам R_i вычисляется общая точка

$$R = \sum_{i=1}^{l} R_i = (X_R, Y_R)$$

3. и значение $w = \pi(R) = X_R \bmod n$.

4. Формируется точка $wR = (x, y)$ и

5. первая часть коллективной подписи $r = \pi(x, y) = x \bmod n$.

6. Каждый пользователь вычисляет свой параметр s_i

$$s_i = (wk_i + hd_i) \bmod n$$

7. и предоставляет его для вычисления второй части коллективной подписи

$$s = \sum_{i=1}^{l} s_i$$

.

Коллективной подписью является пара чисел – (r,s).

Проверка коллективной подписи.

1. Проверяющий вычисляет хэш-образ h' общего сообщения

$$t = \frac{s}{h'} \bmod n$$

2. и значение .

3. Используя открытый коллективный ключ Q, формирует точку $tP + Q = (x, y)$

4. и вычисляет значение $v = \pi(x, y) = x \bmod n$.

5. Если $v = r$, то подпись признается подлинной.

Обоснование корректности представленного протокола

Поскольку при формировании подписи значение r определяется формулой

$$r = \pi(wR) = \pi(w\sum_{i=1}^{l} \frac{k_i}{h} P)$$

,

а при проверке подписи проверочное выражение $tP + Q$ дает точку wR

$$tP + Q = \frac{s}{h} P - \sum_{i=1}^{l} d_i P = \frac{\sum_{i=1}^{l} (wk_i + hd_i)}{h} P - \sum_{i=1}^{l} d_i P,$$

$$= w\sum_{i=1}^{l} \frac{k_i}{h} P + \sum_{i=1}^{l} d_i P - \sum_{i=1}^{l} d_i P = w\sum_{i=1}^{l} \frac{k_i}{h} P = wR$$

в итоге имеем:

$v = \pi(tP + Q) = \pi(wR)$, что соответствует r при формировании подписи.

В качестве источника абелевой группы для редложенного протокола коллективной подписи на основе ECPR можно взять группу дивизоров гиперэллиптической кривой.

Основное преимущество использования гиперэллиптических кривых состоит в том, что размер основного поля, над которым определена кривая, уменьшается пропорционально роду кривой без потери стойкости, хотя сама формула группового сложения выглядит более громоздко. При этом размер цифровой подписи также уменьшается пропорционально роду кривой.

Модификация протокола в этом случае состоит в замене группы точек эллиптической кривой на группу дивизоров гиперэллиптической кривой в формулах протокола.

4. ВЫВОДЫ

Таким образом, преимущество протокола ECPR заключается в том, что и при формировании и при проверке ЦП выполняется умножение только на базовую точку, которое в корпоративной сети может быть эффективно выполнено с предвычислениями. Экспериментальная проверка показала, что в сравнении с известными алгоритмами цифровой подписи на эллиптических кривых, такими как ECDSA, ДСТУ 4145, ГОСТ 34.10, процедура формирования замедляется приблизительно в 2 раза, но процедура проверки, которая выполняется гораздо чаще, ускоряется приблизительно в 3-4 раза.

Представленный в статье протокол коллективной цифровой подписи, основанный на протоколе ECPR, базируется на способе формирования и проверки подлинности коллективной цифровой подписи с помощью общего открытого ключа. Он также имеет облегченную процедуру проверки подписи. Размер подписи не увеличивается пропорционально числу подписавших участников, а в случае применения гиперэллиптических кривых даже уменьшается пропорционально роду кривой.

5. СПИСОК ЛИТЕРАТУРЫ

[1] ДСТУ 4145-2002. *Державний стандарт України. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка.* Київ:-Держстандарт України, 2003.-39 с.

[2] 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.

[3] Молдовян Н.А., Молдовян П.А. Новые протоколы слепой подписи // *Безопасность информационных технологий.* – М.:МИФИ. – 2007. – № 3. – С. 17-21.

[4] Артамонов А.В., Маховенко Е.Б. Применение алгоритма Шнорра в протоколе коллективной подписи *// Материалы XIV Всероссийской научной конференции "Проблемы информационной безопасности в системе высшей школы"*. – 2007. – С. 17-18.

[5] 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.82-86.

[6] ГОСТ Р 34.10-2001. *Государственный стандарт российской федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки цифровой подписи.* М.: Госстандарт России, 2001. -20 с.

[7] Don Johnson, Alfred Menezes, Scott Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA)// *Certicom Research*, Canada, 2001. -56 с.

[8] И.Д. Горбенко, С.И. Збитнев, А.А. Поляков. Сравнительный анализ ЦП в группах точек эллиптических кривых *// Радиотехника: Всеукр. межвед. науч.-техн. сб.* 2002. -10 с.

Неласая Анна Викторовна
Окончила Запорожский государственный технический университет в 1996 г. по специальности "Программное обеспечение вычислительной техники". В настоящее время старший преподаватель ЗНТУ и соискатель каф. "Безопасность информационных технологий" ХНУРЕ.

Научные интересы: эллиптическая и гиперэл-липтическая криптография.

Долгов Виктор Иванович,
Специальность защиты диссертации на соискание ученой степени доктора технических наук 20.01.09 – системы управления, в том числе связь в Вооруженных Силах (1973). Тема диссертационной работы посвящена развитию теории адаптивной фильтрации процессов в интересах повышения точности траекторных измерений.

Научные интересы: Технологии криптографической защиты информации в телекоммуникационных и компьютерных системах.

Погорелый Анатолий Николаевич *Окончил Запорожский машиностроительный институт по специальности Радиотехника в 1972г. Работа: с 1972 г. в ПО "Радиоприбор", ОКБ "Элмис" ПО "Гамма" на инженерных и руководящих должностях в конструкторских бюро, в метрологическом подразделении ОАО "Укртелеком". В настоящее время - начальник КБ ГП "Радиоприбор", г. Запорожье.*

Научные интересы: вопросы внедрения ДСТУ 4145-2002.

computing@computingonline.net
www.computingonline.net

ISSN 1727-6209
International Journal of Computing

DIGITAL SIGNATURE PROTOCOLS WITH FAST VERIFYING PROCEDURE

Anna Nelasa [1)], Victor Dolgov [2)], Anatolij Pogorily [3)]

[1)] Computer's Department, Zaporizhzhya National Technical University,
64 Zhukovskogo Street, Zaporizhzhya, 69063, Ukraine, nelasa@mail.zp.ua
[2)] Security Information Technology Department, Kharkiv National University of Radioelectronics,
14 Lenin Avenue, Kharkiv, 61166, Ukraine, dolgovvi@mail.ru
3) Information Security Department, Government enterprise "Radiopribor",
3 Lenin Avenue 3, Zaporizhzhya, 69000, Ukraine, anpogo@yandex.ru

Abstract: *In this paper the modified algorithms of the individual and collective digital signature on elliptic curves with fast verification for a corporate network are offered.*

Keywords: *Elliptic curve, digital signature protocol, secret key, open key, corporate network.*

The analysis of digital signature protocols on elliptic curves such as ДСТУ 4145, GOST P 34.10, ECDSA, ECSS, EC-GDSA, EC-KCDSA has shown, that in procedure of verification of the signature in all listed protocols have operation of scalar multiplication of open key Q by number. As use of precomputation senselessly, as unlike base point P which is uniform for all subscribers of the corporate network, open key Q at everyone the was mentioned earlier, for this operation.

The main idea of the approach offered by authors – to leave from multiplication of open key Q to any numerical multiplier. In Table 1 one of variants of realization of the similar approach, modified digital signature protocol on elliptic curve with precomputation (ECPR) is given.

Designations in table: – $h(M)$ -hash-function, π - function allocation $x \bmod n$.

The defining parity for the offered protokol report looks as follows:

$$\frac{(wk+ed)}{e}P+Q=\frac{wk}{e}P+dP-dP=\frac{wk}{e}P$$

Apparently from procedure of formation of the signature

$$r=\pi(\frac{wk}{e}P)$$

.

Accordingly in procedure of verification

$$v=\pi(\frac{wk}{e'}P)$$

.

Hence, values r and v are equal, if messages and signatures in both cases are identical.

Due to addition of one operation of multiplication in the finite field, one operation of inversion in a finite field and one operation of scalar multiplication to a base point which can be carried out with precomputation, in procedure of forming of the signature, procedure of check of the signature unloads. In it, unlike other standards, at all there is no the most labour-consuming operation of scalar multiplication to open key Q which is inconvenient for carrying out with precomputation in a corporate network.

The presented protocols have been realized by authors with use of library Miracl. In case of a prime field the length of the module of transformations has been chosen 256 bits. In case of the extended field as the module the polynomial of 191 degrees has been chosen. Experiments were conducted on computer Dell Inspiron I6400 Intel (R) Core (TM) 2 CPU T5600 @1.83GHz 987MHz, 512 MB of the RAM.

Thus, for all protocols over a prime field we lose approximately two times in procedure of formation of the signature, but thus we win four times at verification of the signature. For protocols over a extended field a prize at verification is approximately 2,75 times. These parameters can be improved if to increase a window of precomputation.

The resistance analysis of ECPR protocol in relation to attack to the connected keys, attack at a reuse of a single key, an existential forgery, attack under condition of presence of the several signed

messages had been lead by authors. The analysis has shown that the given protocol does not concede on resistance to the standardized reports and in some cases is more proof due to complication of formation signature procedure.

Table 1 Modified digital signature protocol on elliptic curve ECPR

Forming digital signature
Input: elliptic curve *C*, secret key d, open key $Q = -d \times P$, base point P, order of base point n, message *M*. **Output**: digital signature $\langle r, s \rangle$ for message M.
1. $e = h(M) \bmod n$; **2.** Generate random $k \in \{1, ..., n-1\}$; **3.** $t = \frac{k}{e} \bmod n$; **4.** $R = t \times P$; **5.** $w = \pi(R) \bmod n$; **6.** $(x, y) = w \times R = (w \times t) \times P$; **7.** $r = \pi(x, y) \bmod n$; **8.** $s = (wk + ed) \bmod n$.
Verification digital signature
Input: elliptic curve *C*, open key Q, base poin P, order of base point n, digital signature $\langle r, s \rangle$ for message M'. **Output:** digital signature right or wrong.
1. $e' = h(M) \bmod n$; **2.** $t = \frac{s'}{e'} \bmod n$; **3.** $(x', y') = t \times P + Q$; **4.** $v = \pi(x, y) \bmod n$; **5.** $r' \overset{?}{=} v$

We modify this protocol for realization of the collective signature.

Let

P – base point of an elliptic curve;

l – number of users;

n - the order of a cyclic subgroup of points of an elliptic curve;

d_i - a secret key of i-th user;

h – a digest of the message;

$\pi(R) = X_R \bmod n$ – detachment of x-coordinate of point R = (X_R, Y_R) of an elliptic curve.

Generation of the open collective key.

1. Each i-th user *(i=1.. l)* forms the open key of a kind

$Q_i = -d_i P$.

2. The collective open key is calculated as the sum of the open keys of group from l users

$$Q = \sum_{i=1}^{l} Q_i = \sum_{i=1}^{l} -d_i P$$

.

Forming of the collective signature.

1. Each *i*-th user *(i=1.. l)* calculates a point R_i as follows:

a) chooses random parameter k_i, $1 < k_i < n$,

b) calculates value $t_i = \frac{k_i}{h} \bmod n$;

c) and a point $R_i = t_i P$.

2. On the points R_i presented by users the general point

$$R = \sum_{i=1}^{l} R_i = (X_R, Y_R)$$

3. and value $w = \pi(R) = X_R \bmod n$ are calculated.

4. The point $wR = (x, y)$ and

5. the first part of the collective signature

$r = \pi(x, y) = x \bmod n$

are formed.

6. Each user calculates the parameter s_i

$s_i = (wk_i + hd_i) \bmod n$

7. and gives it for calculation of the second part of the collective signature

$$s = \sum_{i=1}^{l} s_i$$

.

The collective signature is the pair numbers (r, s).

Verification of the collective signature.

1. Verifier calculates a digest h' of the general message

$$t = \frac{s}{h'} \bmod n$$

2. and value .

3. Using the open collective key Q, forms a point $tP + Q = (x, y)$

4. and calculates value $v = \pi(x, y) = x \bmod n$.

5. If $v = r$, the signature is right.

Use of the offered protocols will allow to increase by the order speed of procedure of verification of the digital signature.