Смысл работы первого метода заключается в постановке программных фильтров на «уязвимые» части файлов, такие как зарезервированные поля в mp3-формате, поля расширений в видеофайлах, наименее значимые биты в картинках (последнее больше всего относится к bmp-формату). Помимо этих указанных частей существует множество полей, которые должны оставаться неизменными на протяжении всего файла. Также в первом методе ставятся фильтры на известные стегосистемы и, учитывая свойства их работы, делаются предположения о внедрении или не внедрении данных. Таким образом, метод применим при условии, что мы представляем себе те средства, с помощью которых потенциальный противник производит вставку информации, и, используя систему фильтров, находим передаваемое скрытое сообщение.

Второй метод носит теоретический характер, однако он позволяет с высокой степенью вероятности определять факт наличия в файле-контейнере стеганографической вставки. Смысл его действия сводится к следующему: проводится множество экспериментов над мультимедийными файлами без вставки данных, затем проводится то же самое над этими же файлами только с внедрением информации, произведенной по определенной схеме. После этого строятся статистики некоторых служебных величин, влияющих на воспроизведение файла-контейнера, и находятся отличия в исходных файлах и файлах с внедрением. На основе этого ставятся фильтры, работающие на построении данной статистики и реагирующие на ее существенные изменения. Примером может стать резкое изменение дисперсии параметров part23_length и main_data_end при использовании известного стеганографического продукта MP3Stego в mp3-файлах. Сложность метода заключается в том, что многие мультимедийные файлы получены с помощью различных кодеков. Это предполагает дополнительные требования при построении стегофильтров, так как для некоторых стегосистем первоначальной задачей будет определение того, каким именно кодеком был закодирован файл.

В заключение хотелось бы отметить, что первый метод стегоанализа более подходит для обнаружения скрытия данных в форматной области файлов, тогда как второй больше ориентирован на обнаружение факта передачи в неформатных частях и является более сложным в создании, однако имеющим большее применение в решении практических задач.

СПИСОК ЛИТЕРАТУРЫ:

1. ISO 11172 Annex A., Annex B., Annex C.
2. *Грибунин В. Г., Оков И. Н.* Цифровая стеганография. М., 2007.

Д. С. Булавский, Е. Б. Маховенко

ЦИФРОВАЯ ПОДПИСЬ ГОСТ Р.34.10-2001 НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ В ФОРМЕ ЭДВАРДСА

Значительное время работы функций формирования и проверки цифровой подписи, реализованных в соответствии с ГОСТ 34.10-2001, занимает арифметика на эллиптической кривой. Чтобы ускорить время работы функций, возможен переход к кривой в другой форме, на которой арифметика будет работать быстрее.

Эллиптической кривой в форме Эдвардса [1] над полем F_p с характеристикой $p \neq 2$ назовем кривую $E_{E,1,d} : x'^2 + y'^2 = 1 + d'x'^2 y'^2$, $d' \in F_p$. Скрученной кривой в форме Эдвардса над полем F_p с характеристикой $p \neq 2$ назовем кривую $E_{E,a,d} : ax^2 + y^2 = 1 + dx^2 y^2$, $a, d \in F_p$. Арифметика кривой рассмотрена в работе [2].

Рассмотрим механизм перехода от кривой в форме Вейерштрасса к кривой в форме Эдвардса и обратно.

Пусть $f(x) = x^3 + ax + b$ и эллиптическая кривая задана уравнением в форме Вейерштрасса $E_{W,a,b} : y^2 = f(x)$ над полем F_p. Найдем хотя бы один из корней $\alpha \in F_p$ уравнения $f(x) = 0$. Проверим, что $3\alpha^2 + \alpha$ — квадратичный вычет в поле F_p. Такую кривую можно преобразовать к кривой в форме Монтгомери, а затем к кривой в форме Эдвардса.

Найдем коэффициенты A, B кривой в форме Монтгомери $E_{M,A,B} : Bv^2 = u^3 + Au^2 + u$:

$$s = \sqrt{(3\alpha^2 - a)^{-1}}; A = 3\alpha s; B = s .$$

Изоморфизм кривых $E_{W,a,b}$ и $E_{M,A,B}$ над полем F_p задается отображением $(u, v) = (s(x - \alpha), sy)$. Корректность перехода от кривой $E_{W,a,b}$ к кривой $E_{M,A,B}$ рассмотрена в работе [3].

Найдем коэффициенты a, d скрученной кривой в форме Эдвардса $E_{E,a,d} : x^2 + y^2 = 1 + dx^2 y^2$:

$$a = (A + 2)/B; d = (A - 2)/B .$$

Изоморфизм кривых $E_{M,A,B}$ и $E_{E,a,d}$ задается отображением $(x, y) = (u/v, (u-1)/(u+1))$.

Если хотя бы один из коэффициентов a, d — квадратичный вычет в поле F_p, то кривую $E_{E,a,d}$ можно преобразовать к кривой $E_{E,1,d'}$ по следующим формулам:

$$d' = \frac{d}{a}; x' = x\sqrt{a}; y' = y \cdot$$

Корректность перехода от кривой $E_{M,A,B}$ к кривой $E_{E,a,d}$ рассмотрена в работе [2].

Эксперимент, проведенный для эллиптических кривых, удовлетворяющих требованиям ГОСТ Р.34.10-2001, позволил оценить время сложения $t_{ариф.}$ точек на кривых $E_{E,1,d'}$ и $E_{E,a,d}$ относительно времени сложения $t_{W,a,b}$ точек на кривой $E_{W,a,b}$ (табл. 1).

Таблица 1.

Тип арифметики	$(t_{ариф.} / t_{W,a,b}) * 100\%$
$E_{E,a,d}$ (якобиевы координаты)	$\approx 20\%$
$E_{E,1,d'}$ (обратные проективные координаты Эдвардса)	$\approx 27\%$

Для формирования и проверки подписи по стандарту ГОСТ Р.34.10-2001 были получены следующие оценки времени работы арифметики $t_{ариф.}$ в группе точек эллиптической кривой относительно полного времени работы функций $t_{полн.}$ (табл. 2).

Таблица 2.

Название функции	$(t_{ариф.} / t_{полн.}) * 100\%$
Функция формирования цифровой подписи	$\approx 94\%$
Функция проверки цифровой подписи	$\approx 95\%$

Таким образом, рассмотренный метод позволяет сократить время работы функций формирования и проверки цифровой подписи в соответствии с ГОСТ Р 34.10-2001. Метод не требует каких-либо дополнительных действий со стороны пользователя, кроме ввода стандартных параметров цифровой подписи.

СПИСОК ЛИТЕРАТУРЫ:

1. *Bernstein D., Birkner P., Joye M., Lange T., Peters C.* Twisted Edwards Curves // AFRICACRYPT 2008. Lecture Notes in Computer Science 5023. Springer-Verlag, New York, 2008. P. 389–405. URL: http://cr.yp.to/newelliptic/twisted-20080313.pdf.
2. *Bernstein D., Lange T.* Faster Addition and Doubling on Elliptic Curves // Advances in Cryptology – ASIACRYPT 2007. Lecture Notes in Computer Science 4833. Springer-Verlag, New York, 2007. P. 29–50.
3. *Imai H., Zheng Y.* Public Key Cryptography // Lecture Notes in Computer Science 1751. Melbourne, 2000. – 504 p.

А. А. Варфоломеев

О КЛАССИФИКАЦИИ СХЕМ ЦИФРОВОЙ ПОДПИСИ ПО ДОВЕРЕННОСТИ

В системах электронного документооборота широко используются различные схемы цифровых подписей, как классические, так и с дополнительными функциональными возможностями. К таким схемам относятся и схемы цифровой подписи по доверенности, для краткости — схемы прокси-подписи (proxy signature).

Схема прокси-подписи применяется, например, когда лицо, имеющее право подписи электронного документа, само не может поставить подпись и желает передать это право своему доверенному лицу. Например, руководитель организации во время своего отсутствия хочет, чтобы его секретарь (заместитель, технический специалист и т. п.) подписывал документы от его имени. При этом позднее любой проверяющий подпись должен быть уверен, что доверенное лицо подписало документ с согласия доверителя.

Для решения этой проблемы М. Мамбо, К. Усадо и Е. Окамото предложили в 1996 г. так называемую цифровую подпись по доверенности (proxy signature schemes) [1]. С момента предложения первой реализации схемы прокси-подписи появилось много публикаций по этой тематике, появились новые разновидности подписи, такие как подписи по доверенности на основе идентификаторов (identity based proxy signature), пороговые цифровые подписи по доверенности (threshold proxy signature), подписи с полностью делегированными правами (fully distributed proxy signature), подписи по доверенности вслепую (proxy blind signature) и др. Это делает необходимым сбор информации по всем таким схемам подписи, их упорядочивание и классификацию для практической реализации.

Как известно, классификация — это процесс группировки объектов исследования в соответствии с их общими признаками. Примером первой классификации является классификация по видам делегирования права подписи: полная делегация, частичная делегация и делегация по доверенности (ордеру) [2]. Предлагаемая в данной работе классификация основана на принципах классификации из работы Ж. Као, которая уточняется и дополняется в виде требований к функциональным возможностям схемы.

A-тип: по требованиям к подписывающей стороне;

B-тип: по требованиям к проверяющей подпись стороне;

C-тип: по требованиям к ясности содержания сообщения;

D-тип: по требованиям к методу производства открытого ключа;

E-тип: по требованиям к последовательности изменения секретного ключа.

На основе многочисленных проанализированных работ по схемам прокси-подписи в классификации Ж. Као предлагается расширение в виде дополнительных параметров F, G, H, I,