УДК 681.326

О ВВЕДЕНИИ ПАРАМЕТРА ВРЕМЕНИ В СМАРТ-КАРТЫ

НЕМЧЕНКО С.В.

Рассматривается проблема введения таймера в структуру смарт-карты, что позволяет повысить надежность работы карты и расширить набор выполняемых функций на фоне улучшения параметров защиты информации. Большое внимание уделяется как теоретическим, так и практическим проблемам, связанным с этим. Анализируются различные варианты коррекции параметра времени. Даются рекомендации по их реализации.

1. Введение в проблему

Ужесточение требований к надежности функционирования смарт-карт приводит к необходимости поиска новых путей решения этой проблемы. Среди возможных решений обращает на себя особое внимание способ, основанный на введении в смарт-карту параметра времени, что не только повышает надежность работы карт, но и расширяет набор их возможных функций. Кроме того, значительно улучшаются характеристики карты, связанные с параметрами защиты информации в ней, а также систем, использующих смарт-карты [1].

В настоящей работе рассмотрена возможность введения таймера в структуру смарт-карты. Большое внимание уделено как теоретическим, так и практическим проблемам, возникающим при этом.

В качестве одной из главных назовем проблему схемной реализации генератора тактовой частоты (ГТЧ). Как известно, наибольшей прецизионностью обладает кварцевый ГТЧ. Однако невозможность его интегральной реализации приводит к необходимости использовать внешний навесной монтаж, когда наряду с чипом в карту необходимо встроить еще и дискретные элементы. Такая конструкция может быть легко подвергнута атаке извне, что резко снижает безопасность карты и может привести к потере или искажению хранящейся на ней информации.

Автор, как и большинство специалистов в данной области, придерживается той точки зрения, что в нашем случае ГТЧ целесообразно строить на базе RC-генератора, поскольку его неоспоримым достоинством является возможность интегрального исполнения. Вместе с тем, следует учитывать, что одним из серьезных недостатков данного типа генераторов является низкая стабильность генерируемой ими частоты. При этом погрешность генератора зависит от ряда внешних факторов, таких как температура, атмосферное давление и т. п. Все это приводит к необходимости предусмотреть возможность коррекции времени при эксплуатации такого рода смарт-карт.

Отметим сразу, что метод прямого изменения значения счетчика таймера следует полностью исключить из рассмотрения, поскольку это открывает путь для несанкционированного изменения значения внутреннего времени карты. Поэтому примем, что значение счетчика может быть изменено только путем коррекции работы ГТЧ.

Предлагается ввести коррекцию параметра времени на этапе расчета текущего значения времени исходя из значения счетчика. Для этого после получения реального значения счетчика B оно преобразуется по выбранному алгоритму в новую величину B'. Далее, на основе B' вычисляется текущее значение времени. Графически процесс коррекции времени в карте показан на рис. 1.

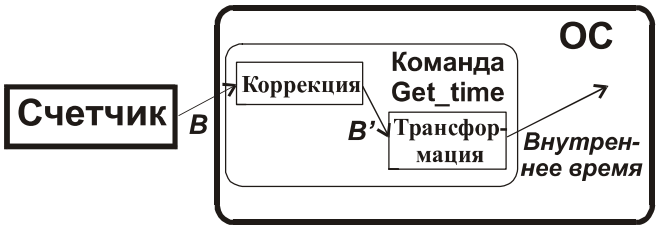

Рис. 1

2. Методы коррекции параметра времени

Весь процесс коррекции параметра времени можно разделить на два этапа (рис. 2):

этап 1: изменение параметра времени;

этап 2: уточнение параметра времени.

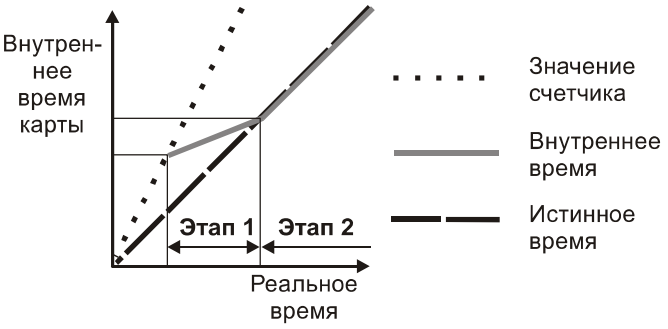

Рис. 2

Этап *изменения параметра времени* может быть реализован двумя путями: *постепенным* изменением или *мгновенным* изменением (рис. 3).

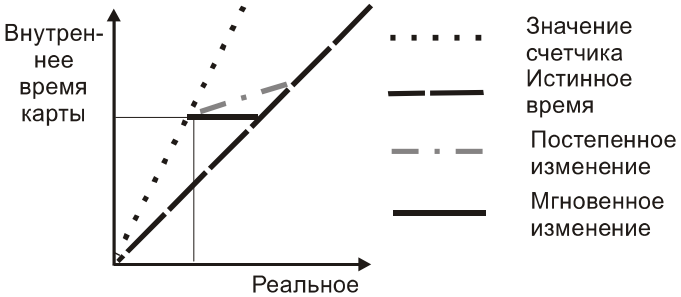

Рис. 3

Второй этап (*уточнение параметра времени*) вводит коэффициент изменения времени. Коэффициент может быть равен "1" или рассчитываться на основе полученных статистических данных (рис. 4).

Как видно из рис. 4, все методы коррекции параметра времени можно подразделить на два больших класса: методы *с уточнением* и *без уточнения* параметра времени. В результате, путем

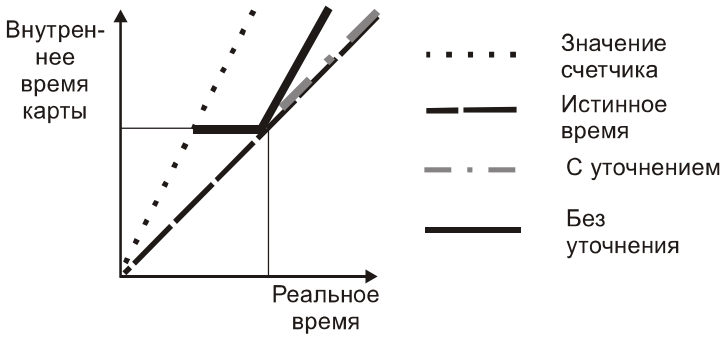

Рис. 4

перебора различных вариантов коррекции параметра времени на первом и втором этапах, мы приходим к классификации, состоящей из четырех методов коррекции параметра времени в смарт-картах:

– постепенное изменение параметра времени с уточнением;

– постепенное изменение параметра времени без уточнения;

– мгновенное изменение параметра времени с уточнением;

– мгновенное изменение параметра времени без уточнения.

3. Проблемы коррекции параметра времени

Анализ методов коррекции может производиться исходя из двух следующих критериев:

– критерий последовательности времени;

– критерий точности времени.

Рассмотрим два случая, которые требуют учитывать приведенные выше критерии.

Пример необходимости использования критерия последовательности времени.

Предположим, что смарт-карта используется для сертификации фотографий в цифровом фотоаппарате. А именно, карта должна гарантировать достоверность значения времени, когда была сделана фотография.

Представим ситуацию, когда фотограф-злоумышленник хочет сфальсифицировать время съемки некоторой фотографии. Для этого он помещает карту близко к источнику тепла на некоторое время либо изменяет параметры окружающей среды таким образом, чтобы ГТЧ выдавал повышенную частоту. Для схемы *RC* при экстремальных условиях за пятнадцать дней может накопиться погрешность вплоть до 10 минут. После этого он делает фотографию и сразу же подключает карту к считывателю для коррекции времени. Если карта использует метод мгновенного изменения параметра времени, то операционная система “останавливает” ГТЧ на десять минут. Теперь фотограф-злоумышленник имеет 10 минут для того, чтобы сфабриковать (смонтировать) фотографию и сделать снимок. Таким образом, в результате получается две фотографии с цифровыми подписями, отличающимися друг от друга на несколько секунд, но реально разнесенными во времени на 10 минут.

Чтобы полностью устранить возможность такой фальсификации, целесообразно использовать метод с постепенным изменением параметра времени на первом этапе коррекции.

Пример необходимости использования критерия точности времени.

Одним из наиболее характерных примеров подобного рода является смарт-карта, которая осуществляет контроль доступа в помещение (бэдж). В этом случае предпочтение отдается критерию точности времени. Очевидно, необходимость использования критерия последовательности времени в данном случае отсутствует.

Анализ приведенных выше методов показал, что методы с постепенным изменением параметра времени на первом этапе предпочтительны для приложений, требующих использования критерия *последовательности времени*. А методы с мгновенным изменением параметра времени на первом этапе и без уточнения на втором этапе коррекции предпочтительны для приложений, требующих использования критерия *точности времени*.

Автором статьи была создана программа, моделирующая функционирование карты с коррекцией методом мгновенного изменения параметра времени на первом этапе и без уточнения на втором этапе.

Характерно, что многофункциональные смарт-карты могут иметь два внутренних времени. В этом случае одно отвечает требованиям критерия точности, другое – требованиям критерия последовательности времени.

4. Реализация коррекции параметра времени

В процессе работы автором был реализован программным путем метод мгновенного изменения параметра времени на первом этапе коррекции. Чтобы избежать конфликтов во время исполнения приложения, карта реализует коррекцию параметра времени в момент, когда она не подсоединена к считывателю. В действительности изменения параметра времени происходят сразу же после первого подсоединения карты к считывателю. Карта анализирует продолжительность промежутка времени, в течение которого она была отключена от считывателя (назовем это время T). Это необходимо для случая, когда данный промежуток времени короче периода, на который необходимо изменить текущее время (пусть это время T’).

Если $T > T'$, тогда текущее время изменяется на требуемое время T’ и далее продолжается нормальное функционирование карты. Если же $T < T'$, тогда текущее время изменяется на величину (T-d), где d - некоторая величина, введенная для соблюдения продолжительности времени, т.е. для того, чтобы избежать ситуации, когда событие, совершенное перед отключением карты от считывателя, и первое действие после подключения карты к считывателю имеют одно и то же время. При последующем подключении карта аналогично выполнит компенсацию остатка погрешности, которая равна (T’-(T-d)). Таким образом, коррекция внутреннего времени карты имеет вид, представленный на рис. 5.

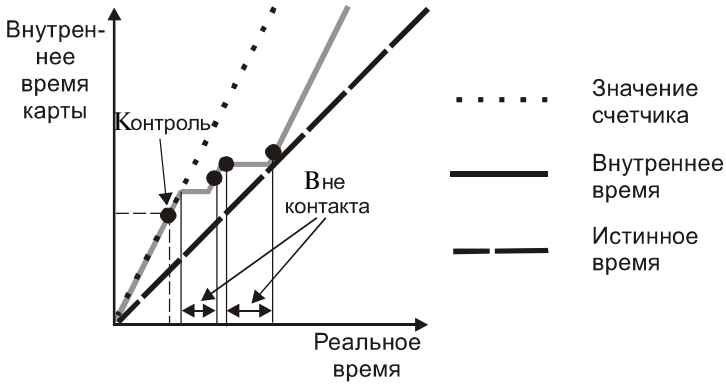

Рис. 5

В заключение отметим, что рассмотренная выше задача введения параметра времени в смарт-карты в настоящее время еще не решена до конца и находится в стадии разработки [2]. Вместе с тем, интерес, который проявляют специалисты в этой области к подобного рода разработкам, говорит об их актуальности. Естественно, рамки статьи не позволяют в полном объеме проанализировать все аспекты проблемы. Однако и рассмотренное выше позволяет сделать вывод о том, что задача введения параметра времени в смарт-карты является перспективной и ее решение позволит во многом повысить надежность и универсальность их функционирования.

Литература: 1. *Robyn A. Lindley*. Smart Card Innovation. The University of Wollongong Printery, Australia. 1997. 2. *Cordonnier V., Watson A., Nemchenko S.* / Time as an aid to improving security in smart cards / 7th Annual Working Conference on Information Security Management and Small Systems Security. Amsterdam, The Netherlands. 1999.

Поступила в редколлегию 04.04.2000

Рецензент: д-р техн. наук, проф. Загарий Г.И.

Немченко Сергей Владимирович, магистр технических наук, аспирант ХТУРЭ. Имеет диплом DEA Informatique Лилльского университета науки и технологий, Франция. Во время учебы в Лилле в 1998-1999 гг. участвовал в научных исследованиях, связанных с разработкой и совершенствованием смарт-карт. Научные интересы: смарт-карты, техническая диагностика. Увлечения и хобби: автомобилизм, спорт, музыка, путешествия. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. (0572) 40-93-26.

УДК 681.323

СИНТЕЗ ИЗОБРАЖЕНИЙ ОТДЕЛЬНЫХ ОБЛАЧНЫХ ОБРАЗОВАНИЙ

ОСТРОУШКО А.П., ГУСЯТИН В.М.

Излагается алгоритм синтеза изображений отдельных облачных образований для систем визуализации, использующих метод обратного трассирования лучей.

1. Введение

Системы синтеза визуальной обстановки должны обеспечивать формирование высокореалистичного изображения. Отображение таких природных явлений, как вода, туман, огонь, облака, значительно повышают реалистичность синтезируемого изображения. Отработка тумана и облачного слоя просто необходима в тренажерах летательных аппаратов, где полет в условиях плохой видимости является одним из элементов программы обучения пилотов. В данной статье предлагается метод формирования трехмерной модели облака, позволяющий при минимальном числе задаваемых параметров формировать реалистичное изображение облачного слоя.

Существующие методы создания моделей облаков можно разделить на две группы. К первой относятся методы, основанные на моделировании физических процессов, происходящих при формировании облаков [1, 2]. Эти методы требуют задания большого числа входных данных, а также значительных затрат вычислительных ресурсов. Вторую группу составляют методы вычислительного моделирования формы облаков [3-5]. Такие методы используют, когда необходимо получить изображение произвольного облачного образования или похожего на оригинал, заданный каким-либо способом. Они, как правило, имеют более простые алгоритмы вычисления, однако также позволяют формировать реалистичное трехмерное изображение облачного слоя. Предлагаемый метод относится ко второй группе. В результате выполнения алгоритма получается трехмерная модель облака, заданная набором метасфер [6]. Для визуализации такой модели удобно использовать метод обратного трассирования [1].

2. Алгоритм построения модели облака

Входными данными в этой модели являются параметры эллипсоида, ограничивающего формируемое облако – значения размеров полуосей a, b, c, и координаты его центра x, y, z. В процессе формирования модели облака исходный эллипсоид разбивается на пять подобных ему фигур, размеры главных полуосей которых определяются по формуле:

$$a_i = k_i a,\ b_i = k_i b,\ c_i = k_i c.\,, \qquad (1)$$

где $i \in \{1,2,...,5\}$ – номер фигуры; k – случайная величина в диапазоне от 0 до 1.

Координаты центров получаемых эллипсоидов определяются следующим образом:

$$\begin{aligned} &x_1 = x + a(1-k_i),\ y_1 = y,\ z_1 = z,\\ &x_2 = x - a(1-k_i),\ y_2 = y,\ z_2 = z,\\ &x_3 = x,\ y_3 = y,\ z_3 = z + c(1-k_i),\\ &x_4 = x,\ y_4 = y,\ z_4 = z - c(1-k_i),\\ &x_5 = x,\ y_5 = y + b(1-k_i),\ z_5 = z. \end{aligned} \qquad (2)$$

На следующем шаге алгоритма каждый из полученных эллипсоидов также разбивается на пять фигур согласно формулам (1) и (2). Этот процесс продолжается до тех пор, пока не будет достигнут задан-