А. А. Любко

ТЕХНОЛОГИЯ ПРОВЕРКИ ПОДЛИННОСТИ ТОВАРА С ИСПОЛЬЗОВАНИЕМ ФИЗИЧЕСКОГО ЭКВИВАЛЕНТА ЦИФРОВОЙ ПОДПИСИ

На текущий момент существует достаточно большое количество систем защиты товаров от подделки. К ним относятся — голограммы, SMS-защита от подделки, объемные сертификаты.

Существующие системы защиты условно можно разделить на три класса:

- защита непосредственно товара;
- защита целостности упаковки (от замены содержимого);
- защита логистики распространения (проверка лицензий мест распространения, условий распространения).

Технологии первого класса основываются на добавлении непосредственно в защищаемый объект маркировочного вещества, по составу которого, а также по его концентрации в лабораторных условиях возможно определить происхождение защищаемого объекта.

Второй класс систем представлен голографическими наклейками, акцизными марками, микромаркировкой и другими системами.

Для защиты логистики распространения активно используются бумажные лицензии с информацией о правах на распространение продукции определенного типа.

Разрабатываемая технология относится ко второму и третьему классам и позволяет автоматизировать валидацию товара по защитному маркеру на упаковке, а также проверять дополнительные условия для защиты логистики распространения.

Рассматриваемые системы защиты обладают рядом существенных недостатков:

- плохо приспособлены для использования конечными пользователями (требуют профессионального подхода);
- не имеют возможности автоматически проверять дополнительные условия распространения товара (логистику, срок годности и пр.);
- защита от подделки часто не несет дополнительной ценности для производителя (отсутствие сервисов для конечного пользователя).

Для устранения перечисленных недостатков в разрабатываемой системе совмещены два различных подхода — традиционная маркировка физических объектов машинно-читаемыми маркерами (двумерными штрих-кодами), а также специализированный физический объемный маркер, позволяющий создавать эквивалент электронной цифровой подписи для физических объектов.

Таким образом, защитный маркер состоит из трех основных компонентов, представленных на рисунке:

- случайного компонента маркера подлинности;
- разрушаемой клеевой основы;
- компонента электронной цифровой подписи маркера подлинности.

Физический компонент маркера подлинности представляет собой физически трудно клонируемую функцию, параметризованную уникальными физическими характеристиками маркера подлинности.

В качестве уникальных физических характеристик маркера подлинности используются случайный рисунок, образованный ниткой, помещенной в эпоксидную объемную основу, а также добавленное в состав маркера стоксовое флуоресцентное вещество, возбуждаемое видимым светом и излучающее в ближнем инфракрасном диапазоне. Благодаря добавлению флуоресцентного вещества, при достаточном освещении маркера подлинности изображение маркера, полученное камерой любого мобильного устройства, будет отличаться от изображения, видимого невооруженным глазом, что является дополнительной степенью защиты маркера подлинности, не позволяющей произвести его клонирование.

Для удостоверения авторства маркера подлинности в разрабатываемой системе используется Инфраструктура открытых ключей. Она широко применяется для создания электронного документооборота, таким образом, ее применение в системе валидации позволяет маркеру подлинности играть роль удостоверяющего документа защищаемого товара.

В качестве модели доверия для Инфраструктуры открытых ключей выбрана иерархическая модель доверия. Якорем доверия системы является корневой сертификат владельца всей системы контроля.

Каждый участник системы является владельцем сертификата, выданного корневым Удостоверяющим центром системы проверки подлинности. Данный сертификат используется для формирования электронной цифровой подписи маркера подлинности товара.

На данном этапе в системе предполагается использовать два типа сертификатов изготовителей маркеров:

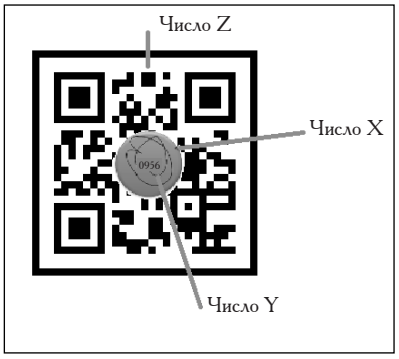
- сертификат производителя;
- сертификат органа лицензирования.

Сертификат производителя позволяет формировать электронную цифровую подпись для маркера подлинности товаров. Маркер подлинности, сформированный на основе данного сертификата, позволяет удостовериться в подлинности товара, заверенной производителем.

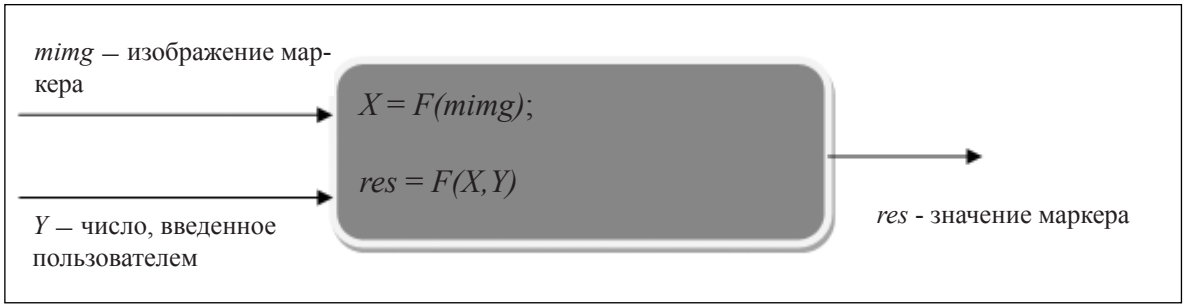
Сертификат органа лицензирования позволяет формировать электронную цифровую подпись для маркеров подлинности документов. Данный маркер подлинности может использоваться совместно с маркером подлинности товара и проводить валидацию продавца на предмет возможности продажи данного товара в соответствии с маркером на лицензии.

Валидация маркера подлинности должна производиться мобильным устройством пользователя (телефоном) с установленным специализированным программным обеспечением.

Для проверки подлинности защищаемого объекта используются три вычисляемых значения: число X — значение, вычисленное с помощью камеры мобильного устройства; Y — число, вводимое пользователем; число Z — значение электронной цифровой подписи маркера, закодированное с помощью двумерного кода.



Для валидации маркера подлинности производится вычисление значения случайной компоненты маркера. Для этого используется изображение маркера подлинности (*mimg*) и дополнительное число, нанесенное на маркер подлинности Y, вводимое пользователем.



После получения основных компоненов маркера подлинности производятся следующие шаги:

• вычисляется значение хеш-функции от числа $res = X + Y$;

• на основе полученного числа производится поиск сертификата подписчика и извлекается его открытый ключ;

• производится шифрование с помощью открытого ключа вычисленного значения хеш-функции $Z1 = ШИФР(HASH(X+Y))$;

• производится сравнение значений Z и $Z1$; в случае их равенства электронная цифровая подпись верна, что подтверждает подлинность маркера.

СПИСОК ЛИТЕРАТУРЫ:

1. *Pappu R., Recht B., Taylor J., Gershenfeld N.* Physical One-Way functions // Science. September 2002. URL: http://dx.doi.org/10.1126/science.1074376.

2. *Skoric B., Maubach S., Kevenaar T., Tuyls P.* Information-theoretic Analysis of Capacitive Physical Unclonable Functions // J. Appl. Phys. July 2006. URL: http://dx.doi.org/10.1063/1.2209532.

3. *Skoric B., Schrijen G.-J., Ophey W., Wolters R., Verhaegh N., van Geloven J.* Experimental Hardware for Coating PUFs and Optical PUFs // Security with Noisy Data – On Private Biometrics, Secure Key Storage and Anti-Counterfeiting / P. Tuyls, B. Skoric, T. Kevenaar (ed.). Springer.London, 2008. P. 255–268. URL: http://dx.doi.org/10.1007/978-1-84628-984-2_15.