

基于 SM2 智能安全芯片的高档酒防伪系统设计

左黎明^{1,2} 陈祚松^{1,2} 汤鹏志¹ 易传佳^{1,2}

(1.华东交通大学 理学院 江西 南昌 330013;

2.华东交通大学 系统工程与密码学研究所 江西 南昌 330013)

摘 要: 高档酒的假冒伪劣行为严重影响了生产厂商的利益和消费者的合法权益,而高档酒的防伪技术研究也一直是—个热点课题。提出了一种由内嵌 SM2 智能安全芯片的防伪瓶盖、配套验证器、防伪认证服务系统组成的防伪解决方案。在防伪认证时,使用配套验证器读取瓶盖上内嵌 SM2 智能安全芯片中的产品身份标识码和签名信息后间接发送到防伪认证服务系统进行签名验证,签名验证通过后,防伪认证服务系统产生新的产品身份标识码和对应的签名信息并通过配套验证器间接发送到瓶盖上的 SM2 智能安全芯片上进行签名验证。通过 SM2 智能安全芯片与防伪认证服务系统之间的双向数字签名认证,保证了产品的身份可信和认证服务器的身份可信并最终实现产品防伪的安全性、可靠性和易用性。

关键词: 防伪技术; SM2 智能安全芯片; SM2 系列算法; 双向数字签名认证

中图分类号: TP391

文献标识码: A

文章编号: 1673-629X(2019)02-0166-06

doi: 10.3969/j.issn.1673-629X.2019.02.035

Design of Top Grade Liquor Anti-counterfeiting System Based on SM2 Intelligent Security Chip

ZUO Li-ming^{1,2}, CHEN Zuo-song^{1,2}, TANG Peng-zhi¹, YI Chuan-jia^{1,2}

(1.School of Science, East China Jiaotong University, Nanchang 330013, China;

2.SEC Institute, East China Jiaotong University, Nanchang 330013, China)

Abstract: The counterfeit and inferior behavior of top grade liquor seriously affects the interests of the manufacturers and the legitimate rights of consumers, and the research on anti-counterfeiting technology of top grade liquor has always been a hot topic. We present an anti-counterfeiting solution composed of anti-counterfeiting bottle cap with embedded SM2 intelligent security chip, matching verifier and anti-counterfeiting authentication service system. In anti-counterfeiting authentication, the product identification code and signature information embedded in the SM2 intelligent security chip on the bottle cap are obtained by a matching verifier and then sent indirectly to the anti-counterfeiting authentication service system for signature verification. After the signature verification, the security authentication service system generates the new product identification code and corresponding signature information, and then indirectly sends it to the SM2 smart security chip on the bottle cap for signature verification. Bidirectional digital signature authentication between the security chip and the anti-counterfeiting authentication service system ensures the identity of the product and the identity of the authentication server, finally realizing the security, reliability and usability of the product.

Key words: anti-counterfeiting technology; SM2 intelligent security chip; SM2 series algorithm; bi-directional digital signature authentication

0 引言

随着国民经济的高速发展和人民生活水平的不断提高,人们对于商品的档次有了更高的追求。但由于受到暴利的驱使,高档商品的假冒伪劣行为屡禁不止。

其中高档酒类的仿冒行为极其严重。1998 年的“山西朔州假酒案”造成 27 人死亡,200 多人住院治疗^[1]。2016 年 6 月,湖南常德警方破获涉案金额逾两千万元的特大假酒案。2017 年 6 月,南阳市警方侦破的特大

收稿日期: 2018-03-22

修回日期: 2018-07-25

网络出版时间: 2018-11-15

基金项目: 国家自然科学基金(11361024); 江西省自然科学基金(20171BAB201009); 江西省教育科技项目(GJJ161417, GJJ170386); 江西省研究生创新专项资金项目(YC2017-S257)

作者简介: 左黎明(1981-),男,硕士,副教授,CCF 会员(E20-0013632M),通讯作者,研究方向为信息安全、非线性系统;陈祚松(1993-),男,硕士研究生,研究方向为信息安全。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20181115.1048.056.html>

制售假酒案,涉案总价值 2.8 亿元。这些假冒伪劣产品不仅严重影响着国家的经济发展,还危及着合法企业和消费者的切身利益^[2]。这也不断地推动着防伪技术的发展。

目前大多数防伪技术主要分为结构防伪和防伪标志认证两种形式。其中结构防伪如 1996 年付正华^[3]提出的防伪瓶盖注射模的设计,公开了一种结构型的防伪技术,但因为结构无法还原的特性使得瓶中酒没有及时饮用而导致酒精挥发后影响酒的品质。通过防伪标志进行认证的如 1993 年 Tirkel 等^[4]提出的数字水印技术^[5-7]。1994 年,日本 Denso-Wave 公司发明了二维条码技术^[8-9]。2010 年,法国 ProofTag 公司推出气泡防伪技术^[10]以及一些其他的印刷防伪技术^[11-12]。但由于这些信息都是静态的,每次防伪识别时都是相同的内容,所以很难做到完全防止被恶意复制。而随着高级印刷技术的普及,以及电子信息技术的进步,这些静态的防伪标志的仿造变得非常容易。

针对这些问题,文中提出了一种基于 SM2 智能安全芯片的高档酒防伪系统,以智能安全芯片为核心,通过智能安全芯片与防伪认证服务系统之间的双向数字签名认证,并且每次认证后都更新产品防伪信息,保证防伪信息的新鲜性,以实现产品防伪的安全性、可靠性和易用性。

1 SM2 公钥密码算法

1.1 SM2 算法简介

SM2 椭圆曲线公钥密码算法(elliptic curve cryptography, ECC)是国内于 2010 年 12 月公开的商用密码算法标准^[13-14]。ECC 的求解是基于求解椭圆曲线离散对数问题(elliptic curve discrete logarithm problem, ECDLP),而将椭圆曲线应用于公钥密码系统的思想是由 Koblitz^[15]和 Miller^[16]各自独立提出的。ECDLP 与大数分解和有限域上离散对数问题相比求解难度大多。

因此, ECC 在密钥规模小得多的情况下能够达到其他公钥密码算法相同的安全程度。正是由于 ECC 的密钥规模小、安全程度高的优势,使其在国内商用密

码行业得到了大规模的应用和推广。

1.2 SM2 签名算法

1.2.1 系统参数

元素数目为 q 的有限域 F_q ; 椭圆曲线 $E(F_q)$ 属于方程 $E(F_q)$ 的两个元素 a 和 b ($a, b \in F_q$); $E(F_q)$ 上的无穷远点或零点 O ; $E(F_q)$ 上阶为 n 的基点 $G = (x_G, y_G)$ ($G \neq O$ 且 $x_G, y_G \in F_q$)。

1.2.2 用户公/私钥的建立

用户 A 随机选取整数 d_A ($1 \leq d_A \leq n-1$), 并计算 $P_A = d_A G = (x_A, y_A)$ 。其中 d_A 作为用户私钥, P_A 作为用户公钥对外公开。

1.2.3 签名生成

对于消息 M 的签名生成过程如下:

- (1) 使用杂凑函数对待签名消息 M 进行处理得到 e ;
- (2) 选择随机数 $k \in [1, n-1]$, 然后计算椭圆曲线点 $(x_1, y_1) = kG$;
- (3) 计算 $r = (e + x_1) \bmod n$, 若 $r = 0$ 或 $r + k = n$ 则返回第二步;
- (4) 计算 $s = ((1 + d_A)^{-1}(k - r d_A)) \bmod n$, 若 $s = 0$ 则返回第二步;
- (5) 将 (r, s) 作为消息 M 的数字签名输出。

1.2.4 签名验证

对于签名信息 (r, s) 进行以下验证:

- (1) 验证 $r \in [1, n-1]$ 和 $s \in [1, n-1]$ 是否成立, 若不成立则验证不过;
- (2) 使用杂凑函数对待签名消息 M 进行处理得到 e' ;
- (3) 计算 $t = (r + s) \bmod n$, 若 $t = 0$ 则验证不通过;
- (4) 计算椭圆曲线点 $(x'_1, y'_1) = sG + tP_A$;
- (5) 计算 $R = (e' + x'_1) \bmod n$, 然后验证 R 与 r 是否相等, 如果相等则验证通过, 否则验证不通过。具体参数定义与计算过程参考文献[12]。

2 系统架构设计

如图 1 所示, 整个防伪系统由三部分组成: 内嵌 SM2 智能安全芯片的瓶盖体、配套验证器、防伪认证

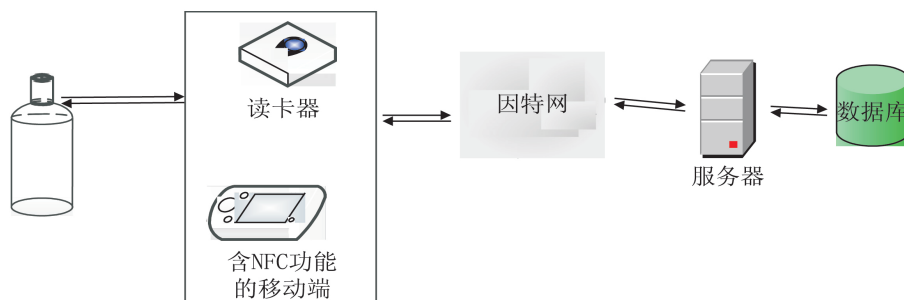


图 1 防伪系统架构

服务系统。首先使用配套验证器读取瓶盖体上内嵌的 SM2 智能安全芯片中的产品身份标识码的签名信息及其他基本信息;然后通过配套验证器间接发送到防伪认证服务系统进行签名验证,签名验证通过后,防伪认证服务系统产生新的产品身份标识码和该产品身份标识码的签名信息,并通过配套验证器间接发送到瓶盖上的 SM2 智能安全芯片上进行签名验证。通过双向签名信息的验证过程来达到产品防伪的效果。每一次防伪验证后,SM2 智能安全芯片和防伪认证服务系统都会更新防伪认证信息以保证防伪信息的新鲜性。

2.1 瓶盖结构设计

防伪瓶盖的结构如图 2 所示。SM2 智能安全芯片内嵌在瓶盖顶部中心,用于射频感应供电的线圈两端连接芯片的同时以芯片为中心向外绕圈,并且与瓶盖的下端连通。在瓶盖开启时瓶盖体与下端分离,线圈也随之断开,智能芯片受损从而无法进行防伪认证。这种设计的目的是防止不法分子回收瓶盖进行产品仿冒行为,但在轻微结构损坏的情况下仍然保证了瓶盖原有的密封产品的功能。

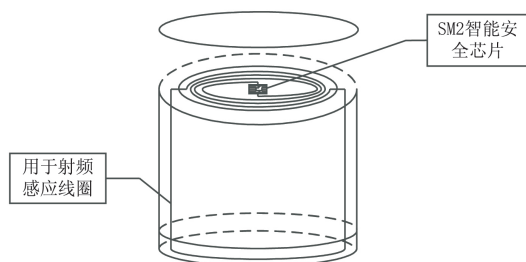


图 2 防伪瓶盖结构

该方案中的 SM2 智能安全芯片采用深圳华视微电子有限公司设计的型号为 CVF1040D 的安全芯片。其拥有唯一的 ID,可重复擦写 10 万次,最大可达 8 MB 程序存储器映射和 8 MB 数据存储器映射,并且含了 SM2 协处理器,支持 ISO/IEC 7816 和 ISO/IEC 14443 接口。

2.2 配套验证器

配套验证器主要分为两类:一类是由显示屏模块、用于网络连接的无线模块和 GPRS 模块组成的配套读卡器;另一类是含有 NFC 功能并安装了配套 APP 的移动终端^[17-18]。

2.3 防伪认证服务系统

防伪认证服务系统由数据中心、签名服务模块和产品管理模块组成,并通过防火墙保证对外数据交互的安全。数据中心存储了产品防伪认证所需的关键信息(如表 1 所示)和其他产品信息,为产品防伪认证和产品管理提供了数据支持。

签名服务模块包括了 SM2 系列算法的插件,提供了密钥对生成、签名信息生成、签名信息验证等功能,

并为其他应用提供了远程接口调用服务。

表 1 数据中心防伪关键数据结构

符号	说明
SystemID	系统唯一 ID,系统部署时生成
SystemPKey	系统公钥,系统部署时生成
SystemSKey	系统私钥,系统部署时生成
CardID	产品唯一 ID,SM2 智能安全芯片自身唯一 ID
CardPublicKey	产品公钥,签名服务模块生成的产品公钥,一个产品对应一个公钥
CardPrivateKey	产品私钥,签名服务模块生成的产品私钥,一个产品对应一个私钥
CardCode	产品身份标识码,系统生成的 8 字节长的随机码
CardSign	产品签名信息,使用 CardPrivateKey 对 CardCode 签名的结果
InfoSign	系统签名信息,使用 SystemSKey 对 (CardID CardPublicKey) 签名的结果
New CardCode	新的产品身份标识码,防伪认证服务器端在产品签名认证通过后产生的
New CardSign	新的产品签名信息,防伪认证服务器端在产品签名认证通过后产生的

产品管理模块对外提供产品信息查询服务,对内提供产品信息新增、修改、删除、出入库管理以及各类报表统计服务。

3 防伪认证流程

防伪认证流程主要分为两个阶段:SM2 智能安全芯片的防伪信息初始化阶段;产品流通和消费者购买时的产品防伪认证阶段。

3.1 防伪认证协议

在防伪认证协议中 C (Client) 为待防伪认证产品, S (Server) 为防伪认证服务器, V (Validator) 为配套验证器,该协议的具体过程如下:

- (1) $V \rightarrow C: \{APDUCommand\};$
- (2) $C \rightarrow V: \{SM2_Sign(SystemPKey || CardID), CardID, SystemID, SM2_Sign(CardID)\};$
- (3) $V \rightarrow S: \{SM2_Sign(SystemPKey || CardID), CardID, SystemID, SM2_Sign(CardCode)\};$
- (4) $S \rightarrow V: \{SM2_Sign(NewCardCode), NewCardCode\};$
- (5) $V \rightarrow C: \{APDUCommand, SM2_Sign(NewCardCode), NewCardCode\};$
- (6) $C \rightarrow V: \{Result\};$

3.2 SM2 智能安全芯片初始化阶段

当一个产品生产完成时,生产厂商在防伪认证服务系统中为该产品生成相应的产品防伪认证关键信息及其他基本信息,其中产品唯一 ID、产品公钥、产品私

钥、产品身份标识码存储到数据中心,而系统唯一 ID、产品唯一 ID、产品公钥、产品签名信息、系统签名信息则通过配套工具写入到智能安全芯片中。

3.3 产品防伪认证阶段

如图3所示,在产品流通或者消费者购买后需要验证产品的真伪时可以通过以下步骤进行防伪认证:

步骤1: 使用配套验证器靠近瓶盖体向 SM2 智能安全芯片发送 APDU 指令, SM2 智能安全芯片响应指令,将基本信息返回给配套验证器,然后配套验证器将该基本信息发送到防伪认证服务系统的签名服务模块。

步骤2: 签名服务模块接收到产品基本信息后,根据系统唯一 ID 从数据中心获得系统公钥,并使用系统公钥、产品唯一 ID、系统公钥验证系统签名信息,验证通过则进行下一步验证,否则返回验证失败并结束防伪认证;根据产品唯一 ID 从数据中心查找产品身份标识码、产品公钥和产品私钥,使用产品公钥、产品身份标识码验证产品签名信息,验证通过则签名服务模块

产生一个新的产品身份标识码并使用产品私钥对新的产品身份标识码签名后得到新的产品签名信息,将新的产品身份标识码和新的产品签名信息返回,同时将新的产品身份标识码更新到数据中心,验证失败则直接返回验证失败并结束防伪认证。

步骤3: 配套验证器接收到防伪认证服务系统的签名服务模块返回认证信息后,如果验证失败则结果直接显示给用户并结束认证,如果接收到的是新的产品身份标识码和新的产品签名信息则结合相应的 APDU 指令发送给 SM2 智能安全芯片。

步骤4: SM2 智能安全芯片接收到新的产品身份标识码和新的产品签名信息后使用产品公钥、新的产品身份标识码、新的产品签名信息进行签名验证,并将验证结果返回到配套验证器中同时将新的产品签名信息更新到 SM2 智能安全芯片中。

步骤5: 配套验证器根据 SM2 智能安全芯片返回的验证结果显示防伪认证结果。

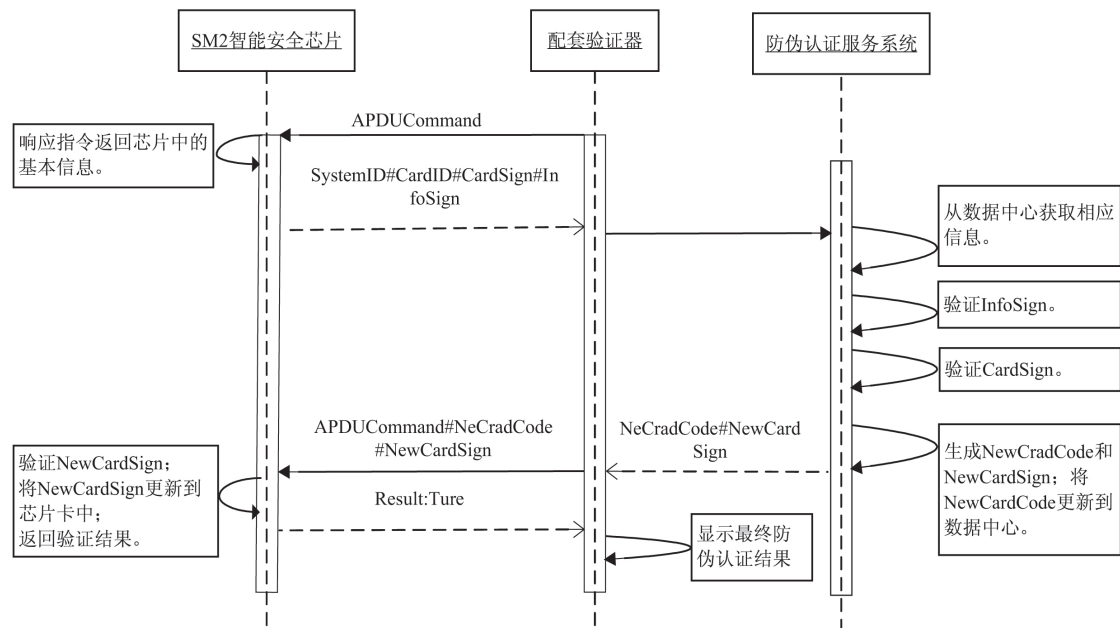


图3 防伪认证时序

4 实验仿真与效率分析

4.1 智能安全芯片初始化

根据系统设计,需要对产品内嵌的智能安全芯片进行初始化,这个过程中将产品基本信息写入到智能安全芯片中,其部分核心代码如下:

```
public static SmartSecurityChip CardInit()
{
    SmartSecurityChip ssc = new SmartSecurityChip(); //生成芯片对象
    ssc.SystemID = SystemID; //将系统唯一 ID 初始化
    ssc.CardID = GetCardID(); //读取产品唯一 ID
    ssc.CardCode = GenerateCardCode(); //生成产品身份标
```

识码

```
SM2.TanGenSM2KeyPair( out ssc.CardPublicKey, out Card-
PrivateKey); //生成公钥/私钥
SM2.TanSM2Sign( ssc.CardCode, out ssc.CardSign); //生成
产品身签名信息
SM2.TanSM2Sign( ssc.CardID + ssc.CardPublicKey, SystemS-
Key, out ssc.InfoSign); //生成系统签名信息
WirteToCard( ssc); //基本信息写入智能安全芯片中
return ssc;
}
```

图4所示为智能安全芯片初始化过程生成的基本信息,同时将基本信息写入到智能安全芯片中。

智能安全芯片初始化阶段:

防伪认证服务系统生产产品基本信息:

```
SystemID: 012389d8-849f-4f18-b597-ecb174c7cbe
SystemPKey: bHzU9haP66dKadFSvLyrDHkbnNU1Fe010DiXr8xphHo=,PL61iznv04qIOkn81hTDqd7vQG0E1OKiorUXRH7nOgQ=
SystemSKey: ANuUU3aLRyYnyk/PyjWn8Rah1ikdQSQIiyH9oqg0HKQA
CardID: 15947147-1c81-4072-b0de-d04cf5b737c1
CardCode: Ec4JQFeG
CardPublicKey: X6dpBrqU5ufCjuvGxfMiWnSEc2WZeGP1Kyq1042KHqg=,AIm9s1dN6X+oQyC7mvUyqjmkMUNstp0+6CD/dkEc4Ko0
CardPrivateKey: LfUFE4HB/1YZAXGQsAP0c4GJzEk3U11a16ysxE0gRGg=
CardSign: TveL78I+65WMBNcQq45dnhKKWRJUKS79ahmX9Y6ZuRE=,R41fAcK54dFQ0ZS7Mmnhc+1a1Be/4fJSuT6aE3hc8Gk=
InfoSign: AIt14Uqs5Sd7cIsLUnh17X2ealUFivAm/3zP8TE+rm0J,J44Jb8ACU3GfvJaC0X0f+h5FjnQHUGg1QUeKBtU7q88=
```

写入智能安全芯片中.....

图 4 智能安全芯片初始化产生的基本信息

4.2 产品防伪认证模拟

在产品防伪认证时,服务器接收到产品基本信息后分别对 InfoSign 和 CardSign 进行验证,然后生成 NewCardCode、NewCardSign,其部分核心代码如下:

```
//服务端根据 System、CardID、CardPublicKey 验证 InfoSign
SCServiceSystem.VerifyInfoSign( ssc.CardID + ssc.CardPub-
licKey ssc.InfoSign SCServiceSystem.SystemPKey);
//服务端根据 CardPublicKey、CardCode 验证 CardSign
SCServiceSystem.VerifyCardSign( ssc.CardCode ,ssc.Card-
```

Sign ,ssc.CardPublicKey);

stringNewCardCode=string.Empty;

stringNewCardSign=string.Empty;

//服务端生成 NewCardCode 和 NewCardSign;

SCServiceSystem.GenNewCardCodeAndSign(out NewCard-
Code ,out NewCardSign);

图 5 所示为产品认证模拟中服务端根据产品发送的认证信息进行 InfoSign 和 CardSign 验证的具体过程和结果,以及生成的 NewCardCode 和 NewCardSign。

防伪认证阶段:

验证InfoSign:

```
输入CardID+CardPublicKey: 15947147-1c81-4072-b0de-d04cf5b737c1X6dpBrqU5ufCjuvGxfMiWnSEc2WZeGP1Kyq1042KHqg=,AIm9s1dN6X+oQyC7mvUyqjmkMUNstp0+6CD/dkEc4Ko0
输入systemPKey: bHzU9haP66dKadFSvLyrDHkbnNU1Fe010DiXr8xphHo=,PL61iznv04qIOkn81hTDqd7vQG0E1OKiorUXRH7nOgQ=
输入InfoSign: AIt14Uqs5Sd7cIsLUnh17X2ealUFivAm/3zP8TE+rm0J,J44Jb8ACU3GfvJaC0X0f+h5FjnQHUGg1QUeKBtU7q88=
验证结果: True
```

验证CardSign:

```
输入CardCode: Ec4JQFeG
输入CardPublicKey: X6dpBrqU5ufCjuvGxfMiWnSEc2WZeGP1Kyq1042KHqg=,AIm9s1dN6X+oQyC7mvUyqjmkMUNstp0+6CD/dkEc4Ko0
输入CardSign: TveL78I+65WMBNcQq45dnhKKWRJUKS79ahmX9Y6ZuRE=,R41fAcK54dFQ0ZS7Mmnhc+1a1Be/4fJSuT6aE3hc8Gk=
验证结果: True
```

生成NewCardCode 和 NewCardSign:

```
输出NewCardCode: iPqc5U4z
输出NewCardSign: A1716A8G/7ci+aWDC1o3+kBdPDDNyxQsRacF5Gjn4roT,SmZdi3E9Gf1zDaT2trRUgln2cqeHTWHIPTIH/cBDNh0=
```

图 5 防伪认证阶段各认证步骤结果

防伪认证服务器端对产品基本信息认证通过后,通过配套验证器间接发送 NewCardCode 和 NewCardSign 至产品内嵌的智能安全芯片中,智能安全芯片根据 CardPublicKey 和 NewCardCode 验证 NewCardSign,其部分核心代码如下:

```
//根据 newCardCode、CardPublicKey 验证 newCardSign
publicbool Verify( string newCardCode ,string newCardSign)
{
```

```
验证NewCardSign:
输入NewCardCode: iPqc5U4z
输入NewCardSign: A1716A8G/7ci+aWDC1o3+kBdPDDNyxQsRacF5Gjn4roT,SmZdi3E9Gf1zDaT2trRUgln2cqeHTWHIPTIH/cBDNh0=
输入CardPublicKey: X6dpBrqU5ufCjuvGxfMiWnSEc2WZeGP1Kyq1042KHqg=,AIm9s1dN6X+oQyC7mvUyqjmkMUNstp0+6CD/dkEc4Ko0
NewCardCode签名验证结果为: True
```

bool result = SM2.TanSM2Verify(newCardCode ,this.Card-
PublicKey newCardSign);

ShowDetails(newCardCode newCardSign ,result);

return result;

}

图 6 所示为智能安全芯片根据 CardPublicKey 和 NewCardCode 验证 NewCardSign 的具体过程及结果。

图 6 智能安全芯片签名认证信息及结果

4.3 效率分析

经过 20 组防伪认证仿真后,得到智能安全芯片的初始化平均耗时为 0.239 518 8 s,防伪认证服务系统的认证平均耗时为 0.339 992 9 s,智能安全芯片的签名认证平均耗时为 0.142 21 s。智能安全芯片的

0.239 518 8 s 的产品初始化时间相较于整个产品生产流程而言是非常快速的,而模拟的整个产品防伪认证过程时间合计为 0.482 202 9 s,对于消费者和经销商而言产品的防伪认证过程可以实现“所见即所得”的效果。

5 结束语

基于 SM2 智能安全芯片的高档酒防伪系统是一个由防伪瓶盖、配套验证器、防伪认证服务系统组成的防伪解决方案。采用 SM2 智能安全芯片内嵌瓶盖顶部线圈连通开盖结构的设计,在瓶盖开启时的结构轻微损坏,既保证了瓶盖原有的封口功能又使智能安全芯片因结构损坏而失去防伪功能,从而杜绝了不法商家回收瓶盖来制造伪冒产品的行为。以 SM2 系列算法为防伪认证核心并通过防伪产品与防伪认证服务系统之间的双向身份认证保证了防伪认证的安全性和可靠性。并且每次防伪验证后 SM2 智能安全芯片和防伪认证服务系统都会更新防伪认证信息,充分保证了认证信息的新鲜性。通过仿真模拟证明了防伪认证在高安全性的前提下保证了防伪验证的高效性。

参考文献:

- [1] 杨高义.山西朔州假酒案背后[J].新闻知识,1998(6):16-17.
- [2] 孟友新,姚立新,王娟.RFID 追溯系统信息安全及防伪技术的研究与探讨[J].电子技术与软件工程,2016(6):212-213.
- [3] 付正华.防伪瓶盖注射模设计[J].模具工业,1996(8):33-34.
- [4] TIRKEL A Z, RANKIN G A, SCHYNDEL R V, et al. Electronic watermark[C]//Digital image computing, technology and applications. Sydney: Macquarie University, 1993: 666-673.
- [5] 胡军全,黄继武,张龙军,等.结合数字签名和数字水印的多媒体认证系统[J].软件学报,2003,14(6):1157-1163.
- [6] 郝彦军,朱琴,王丽娜,等.数字水印演化设计[J].计算机工程,2006,32(6):157-159.
- [7] CHEN Musheng. Certificate anti-counterfeiting system based on QR code and digital watermarking[J]. International Journal of Hybrid Information Technology, 2016, 9(10): 109-116.
- [8] PAVLIDIS T, SWARTZ J, WANG Y P. Information encoding with two-dimensional bar codes[J]. Computer, 2002, 25(6): 18-28.
- [9] 冯林,孙焘,吴昊,等.基于手机和二维条码的无线身份认证方法[J].计算机工程,2010,36(3):167-168.
- [10] 朱建.法国 ProofTag TM 推出气泡防伪技术——“气泡标签”技术演示会报道[J].中国防伪报道,2010(9):56-57.
- [11] 吴柯.图像版权保护与认证的双水印算法[J].计算机技术与发展,2009,19(9):136-139.
- [12] 董峰,金俭.一种基于混沌脆弱水印的可逆双层图像认证方案[J].计算机技术与发展,2016,26(6):92-96.
- [13] 国家密码管理局.SM2 椭圆曲线公钥密码算法[M].北京:国家密码管理局,2010.
- [14] 汪朝晖,张振峰.SM2 椭圆曲线公钥密码算法综述[J].信息安全研究,2016,2(11):972-982.
- [15] KOBLITZ N. Elliptic curve cryptosystems[J]. Mathematics of Computation, 1987, 48(177): 203-209.
- [16] MILLER V S. Use of elliptic curves in cryptography[C]//Advances in cryptography. Berlin: Springer-Verlag, 1986: 417-426.
- [17] 周杨,李燕,李范鸣.基于新型软件架构的 NFC 管理系统的设计实现[J].计算机技术与发展,2018,28(2):1-4.
- [18] 夏文栋,林凯.融合 NFC 的 3G 智能卡系统[J].计算机工程,2011,37(2):229-231.