一种具有数字签名的二维码技术

谭德林,李均利
(四川师范大学,四川 成都 610068)

摘 要: 由于当前的二维码技术无身份认证技术,因此当用户扫描来源不明的二维码时,隐藏在二维码中的各种危害就将被传播给扫描者而造成一些不必要的损失。同时,当前的二维码技术也无抗否定性,因此其无法确定制作者身份的真伪。鉴于此,提出了一种具有数字签名的二维码技术。该技术使用 RSA 数字签名原理以完成二维码制作者身份的识别。因此在具有数字签名的二维码技术中,即使在扫描过程中发生了问题,也可以追究责任者。经过实验验证可知,具有数字签名的二维码技术不但可行,且可以使扫描者扫描到正规用户制作的二维码,进而在一定程度上保证了二维码技术的安全性。

关键词: 二维码;数字签名;RSA;身份识别;认证
中图分类号: TP31 **文献标识码:** A **文章编号:** 1673-629X(2018)03-0143-03
doi:10.3969/j.issn.1673-629X.2018.03.030

A Two-dimension Bar Code Technology with Digital Signature

TAN De-lin,LI Jun-li
(Sichuan Normal University,Chengdu 610068,China)

Abstract: The hidden hazards in the 2-dimensional bar code will spread to the scanner and cause unnecessary losses when a user scans a 2-dimensional bar code with unknown origin because of the current 2-dimensional bar code without identity authentication technology. At the same time, the current 2-dimensional bar code technology has no resistance, so it can not determine the authenticity of the identity of the producer. For this, we put forward a kind of 2-dimensional bar code technology with digital signature, which uses RSA digital signature principle to complete the identification of 2-dimensional bar code. Therefore, if there are problem during the scanning, it can also be held accountable in the digital signature of the 2-dimensional bar code technology. The experiments show that the proposed technology is not only feasible, but also can enable the scanners to scan the 2-dimensional bar code from the regular user, which in turn guarantee the safety of the 2-dimensional bar code technology.

Key words: 2-dimensional bar code; digital signature; RSA; identity recognition; authentication

0 引 言

二维码技术最早是由日本在 20 世纪 70 年代提出的,它使用某种特定的二维图形按一定的规律在二维平面上绘制黑白相间的二维条形码图形来保存和记录信息。而二维码在存储数据时,一般使用二进制对其进行编码。也即使用“0”和“1”的信息串来表示二维码中存储的信息,这也符合计算机的信息表示方式。二维码中存储的数据只有被相应的设备扫描后,方可获取其所存储的信息。二维码的种类很多,其相应的编码和读取方式也不同,常见的有堆叠式二维码和矩阵式二维码[1]。其中堆叠式二维码也称为行排式二维码,主要有 Code 16K、Code 49、PDF417 等编码方式;矩阵式二维码主要有 QR Code、Code One、MaxiCode、Data Matrix[2]、HanXinCode、GridMatrix 等编码方式[3]。在以上编码方式中,QR 码的使用最为广泛。

随着二维码的应用越来越广泛,特别是二维码制作过程的简单和开放[4],许多不法分子瞅准机会,将二维码作为其犯罪作案的新途径[5]。如利用二维码传播病毒、植入木马;利用二维码引导用户访问钓鱼网站等恶意网站;利用二维码访问吸费软件等。这不但影响了人们的日常生活,同时也造成了一定的社会经济损失。而究其原因,主要是用户在扫描二维码时,无法识别该二维码来源的真伪,从而导致在扫描时不能对二维码制作者进行识别,也无法在出问题后追究二维码制作者的责任[6-7]。

鉴于上述问题,文中提出了基于 RSA 数字签名的

收稿日期: 2017-04-17 **修回日期:** 2017-08-23 **网络出版时间:** 2017-12-05
基金项目: 四川省教育科研计划项目(17ZB0352)
作者简介: 谭德林(1981-),男,博士研究生,实验师,研究方向为密码学;李均利,研究员,研究方向为进化算法、视频评价、医学图像处理。
网络出版地址: http://kns.cnki.net/kcms/detail/61.1450.TP.20171205.0906.060.html

二维码技术,并通过实验对该技术进行验证。

1 QR 码工作原理

QR 码于 1994 年由日本的 Denso-Wave 公司发明,其主要支持文本、图片、网址链接、音频、视频等,并通过掩膜技术对存储的信息进行保密,其编解码过程[8]如图 1 和图 2 所示。

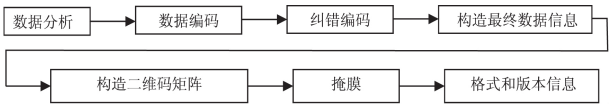


图 1 编码过程

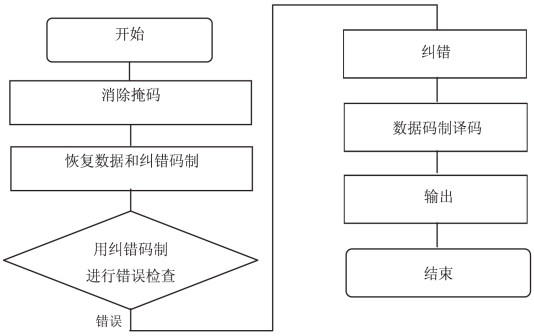


图 2 解码过程

2 RSA 数字签名

2.1 RSA 数字签名简介

数字签名是众多密码学工具中最重要的一种,目前已经得到了广泛应用。数字签名与不安全信道上的密钥简历共同构成了公钥密码学中最重要的内容。数字签名与手写签名一样,能够提供对签名内容的识别。尤其是它们都提供了一种能保证每个用户验证消息的方法,即能够确认消息来源于何处,有谁可传递等。

数字签名如同手写签名一样,用来证明某个人的确生成了某个消息。但是与手写签名不同的是,数字签名只适用于数字信息中。数字签名的基本原理是对消息签名的一方使用私钥,而对消息接收的一方使用公钥。此时,只有拥有私钥的一方才能对数字消息进行签名,进而保证了数字签名的正确性。数字签名与密码学一样,也具有安全服务要求,其种类也较多。主要包括保密性、完整性、消息验证、不可否认性、身份验证/实体验证、访问控制、可用性、审计、匿名等。

目前能作为数字签名算法的主要是公钥密码算法,如 RSA 公钥密码算法、Elgamal 数字签名算法及其变体 DSA。为了方便和易于理解,对 RSA 数字签名方案进行介绍。RSA 数字签名是由 RSA 公钥密码方案演变过来的,而 RSA 公钥密码体制由 Rivest,Shamir 和 Adleman 等于 1977 年提出,以它的发明者们的名字首字母命名[9]。其算法思想如下:

密钥生成:p,q 是两个大素数,且有 $n = pq$,根据欧拉定理,$\varphi(n) = (p-1)(q-1)$。随机选择整数 d,e,使得 $\gcd(d,\varphi(n)) = 1$,$ed \equiv 1(\varphi(n))$,则公钥 $\mathrm{pk} = (n,e)$,私钥 $\mathrm{sk} = d$。

加密:明文空间 M 中的任意消息 m,对应密文为 $c = E_{\mathrm{pk}}(m) = m^e(\mathrm{mod}n)$。

解密:$m = D_{\mathrm{sk}}(c) = c^d(\mathrm{mod}n)$。

而 RSA 数字签名与加解密过程刚好相逆。假设用户 A 发送一个签名的消息 x 给用户 B,且密钥与上面 RSA 密码方案相同,则数字签名过程为:

$$s = \mathrm{sig}_{k_{pr}}(x) \equiv x^d \mathrm{mod}n$$

验证过程为:

$$x' \equiv \mathrm{ver}_{k\mathrm{pub}}(x,s) \equiv s^e \mathrm{mod}n$$

$x' \equiv x\mathrm{mod}n$,表示签名有效,否则表示签名无效。

2.2 RSA 数字签名安全性分析

安全性是密码学方案或数字签名的首要考虑因素。一个不安全的密码学方案是无实用价值的。与其他所有非对称方案一样,数字签名也需要保证其公钥是可信的,也即验证方所拥有的公钥的确是与签名所用的私钥相对应的。目前针对 RSA 数字签名的攻击主要包括:算法攻击和存在性伪造攻击。其中算法攻击,也即通过计算私钥来破解底层的 RSA 方案,其所面对的困难性是基于大整数因式分解,为了单纯地防止该类攻击,则要求有较长的模长度。对于智能手机,明显是不理想的,因而实际使用 RSA 数字签名时,都不是使用单纯的 RSA 数字签名,而是使用 RSA 的概率签名标准,也即 PSS;而存在性攻击,也即允许攻击者生成随机消息 x 的有效签名,以冒充正常签名,从而获得相应的公钥或者从中破解出私钥,最后达到攻击数字签名的目的。

为了解决以上攻击,一般方案是使用 RSA 填充技术,也即概率签名标准技术。粗略地讲,即是对消息格式化。所谓消息格式化,就是使用一定规则,让消息验证者能够区分消息的有效性和无效性。RSA 填充技术是基于 RSA 密码体制的签名方案,它结合了消息验证、消息编码以及数字签名技术。应该说,RSA 填充技术能够很好地防止以上各种攻击,在目前的 RSA 数字签名中应用广泛。

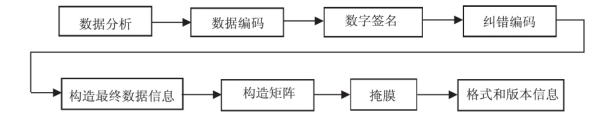
3 具有数字签名的二维码技术

为了解决目前二维码技术无法对二维码制作者进行认证以及无法追究制作者责任的现状[10],文中提出了具有数字签名的二维码技术。该技术主要是借助 RSA 数字签名的工作原理来完成对二维码制作者的验证。其工作过程如图 3 所示。

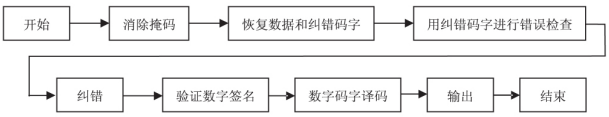
3.1 具有数字签名的 QR 编码端

由图 3(a)可知,具有数字签名的 QR 码编码阶段

与普通 QR 码编码相比,增加了“数字签名”步骤。也即具有数字签名的 QR 码编码是在其编码阶段的数据码字序列的首部加上数字签名和明文,也即相应的签名和明文,即 s 和 x 。其中 $s = x^d$,x 即为明文,然而该明文却并不是具有隐私性的明文,而是经过哈希函数 H 摘要后的信息。



(a)具有数字签名的 QR 码编码过程



(b)具有数字签名的 QR 码解码过程

图 3　具有数字签名的 QR 码编解码过程

3.2　具有数字签名的 QR 解码端

由图 3(b)可知,具有数字签名的 QR 码解码分为很多步骤。与普通 QR 解码端相比,其增加了“验证数字签名”步骤。该步骤通过获取数据码字序列中存储的数字签名 s 以及与签名相对应的明文 x ,然后利用公布的公钥 e 进行计算,也即 $e.s = (x^d)^e \bmod n$ 。如果以上运算结果与明文 x 相等,则表示通过数字签名验证,扫描者可以继续扫描二维码中的数据码字序列以读取二维码中存储的信息;如果以上运算结果与明文 x 不相等,则表示没通过验证,扫描者将停止扫描二维码中的数据码字序列。

4　实验测试

实验操作平台为 Windows 7 旗舰版,二维码生成平台使用 Visual C++ 6.0 对开源的 QR 二维码生成算法源码进行编辑与运行[11] ,也即在其数据码字序列生成后,再在其序列首加上需要签名的明文 x 以及对应的签名 s ,并生成最终的二维码,且以图像形式进行存储。在源代码中,生成二维码的函数原型为 BOOL EncodeData(int nLevel, int nVersion, BOOL bAutoExtent, int nMaskingNo, LPCSTR lpsSource, int ncSource)。只需在生成的数据码字序列的首部加上要签名的明文 x 以及对应的签名 s 即可。

然后使用 Android 模拟器 pc 版模拟微信扫描功能[12-14] 。具体做法是将上述生成的二维码图像导入模拟器相册,并在模拟器中点击登录微信,再点击扫一扫功能,并选择模拟器相册中相应二维码图像,即可以进行扫描。在扫描过程中,首先分别获取要签名的明文 x 以及对应的签名 s ,然后根据获取的签名 s 与公钥 e 进行模指数运算,并得到一个值 x' ,最后将 x' 与 x 进行比较。如果 x' 与 x 相等,则继续扫描下面的数据码字序列并获得其中所存储的信息;如果 x' 与 x 不相等,则扫描端停止扫描。

5　结束语

针对二维码存在的安全隐患,提出了一种具有数字签名的二维码技术。该技术使得在扫描二维码数据之前,先对二维码的来源进行识别。只有当识别通过后,才能继续读取二维码中的相应信息;如果二维码识别未通过,则停止读取二维码中的信息。实验测试表明,该技术可以有效防止用户去扫描一些非法二维码,如通过二维码访问吸费软件、非法网站、木马或感染病毒等,进而提高了二维码技术的安全性。然而,该技术也存在一些问题,如其扫描速度比普通的二维码扫描速度低。因此,接下来的工作就是在保证二维码制作者身份认证的同时,提高二维码扫描的速度。

参考文献:

[1] 黄文培.一种基于信息隐藏的图像二维码设计[D].成都:西南交通大学,2015.
[2] 汉信码[S].北京:中国标准出版社,2008.
[3] 娄良宇,张　健,梅　锋,等.二维码应用与安全[J].通信管理与技术,2014(3):60-61.
[4] 郑　君,李海霞.基于动态二维码的安全身份认证方案的研究[J].湖北理工学院学报,2015,31(2):35-38.
[5] 马立林.云计算环境下基于二维码的移动终端身份认证方案[J].微电子学与计算机,2016,33(1):140-143.
[6] 张新文,李华康,杨一涛,等.基于二维码技术的个人信息隐私保护物流系统[J].计算机应用研究,2016,33(11):3455-3459.
[7] 凌康杰,岳学军,刘永鑫,等.基于移动互联的农产品二维码溯源系统设计[J].华南农业大学学报,2017,38(3):118-124.
[8] 张　丰,施　勇,薛　质.二维 QR 码在电子商务中应用的安全性研究[J].计算机技术与发展,2017,27(3):131-135.
[9] MERKLE R C,HELLMAN M.Hiding information and signatures in trapdoor knapsacks[J].IEEE Transactions on Information Theory,1978,24(5):525-530.
[10] 马尚寅,高关心,刘嘉吉,等.基于微信的考勤管理系统身份认证及位置识别方法的实现机制[J].计算机与现代化,2017(3):8-12.
[11] 祁　慧.基于 Android 系统的 QR 码识别技术研究与实现[D].南京:东南大学,2015.
[12] 罗春玲.二维条码 QR 的纠错改进研究[D].武汉:武汉理工大学,2013.
[13] 韩　芳.主动式二维码考勤系统研究[J].网络安全技术与应用,2017(1):134-135.
[14] 周平平.微信小程序会杀死 APP 吗[J].计算机与网络,2017,43(1):47.