一种基于二维码的公函防伪方案的设计

梁一峰
（西南电子设备研究所，四川 成都 610036）

摘要：公函是党政机关、人民团体、企事业单位间商洽和联系工作时使用的一种文体。公函具有法定效力，目前社会上伪造公函诈骗的犯法活动时有发生。随着计算机软件技术及网络技术的飞速发展，很多需要出具公函的业务已经线上办理。然而也有一些情况，比如公民在办理某些业务时，企事业单位与管理机关的网络是物理隔离的，文章提供一种基于二维码的公函防伪方案，实现公函信息跨平台的安全传输。

关键词：公函；防伪；安全；传输
中图分类号：TP391.44　　**文献标识码：**A　　**文章编号：**2096-9759(2023)06-0137-03

Design of a public letter anti-counterfeiting scheme based on two-dimensional code

LIANG Yifeng
（Southwest China Research Institute of Electronic Equ，SiChuan ChengDu 610036）

Abstract: The official letter is a style of writing used in the negotiation and contact between the party and government organs, people's organizations, enterprises and institutions. Official letters have legal effect. At present, the illegal activities of forging official letters and cheating often occur in society. With the rapid development of computer software technology and network t echnology, many businesses requiring official letters have been handled online. However, there are also some cases, for example, when citizens handle certain businesses, the network of enterprises and institutions is physically isolated from the management authority. This paper provides a public letter anti-counterfeiting scheme based on QR code to realize the secure transmission of public letter information across platforms.

Key words: official letter; Anti-counterfeiting; Safety; transmission

0 引言

纸质公函的防伪一般主要依靠签署的公章，这样的公函非常易于伪造，伪造的公函不易辨识。电子公函的防伪引入了一些信息安全行业主流的加密和哈希算法，能够完全实现公函信息的安全传输。对称加密算法具有加密速度快的优点，实现正文信息的加密传输。非对称加密算法实现随机密钥的安全传输，做到一函一密。散列算法配合非对称加密算法，完成报文的数字签名，使得发送方的信息可鉴别、不可抵赖。

1 相关知识

1.1 对称加密技术

所谓对称加密技术[1]是一类加密技术的总称，发送方和接收方在通信的过程中，使用的是相同的密钥对明文、密文信息进行加密、解密。其中，算法是一种规则，规定加密、解密的具体流程。密钥是控制加密及解密过程的指令。随着现代密码学的发展，对称加密技术应用于信息通信的各个领域，因为加密、解密速度快，它非常适合于有大量信息需要加密传输的情景。

现代密码学界普遍认为，加密的安全性不再依赖于算法本身。在许多国际公认的加密标准中，加密算法是完全公开的，信息的安全传输完全取决于密钥的保密性。如何解决密钥传输的安全性，是工程应用的关键问题。

常见的对称加密算法有，DES、AES、3DES、IDEA、RC2、RC4、RC5、Blowfish、TDEA 等。

1.2 非对称加密技术

非对称加密技术也是一类加密技术的总称，与对称加密技术不同的是，非对称加密中发送方和接收方使用的是不同的密钥对信息进行加密和解密。非对称加密技术是针对对称加密技术的缺陷而提出的。在非对称加密系统中，加密和解密是相对独立的，通信双方各自会拥有自己的公钥和私钥，其中公钥向公众公开，私钥对外保密。在发送信息的时候，使用对方的公钥进行加密，这样由于攻击者没有接收方的私钥，也无法根据公开的公钥推算出私钥，所有接收方可以解密密文得到明文信息。

在实际的工程应用中，非对称加密技术与对称加密技术配合使用常常能事半功倍，在通信前产生一个会话密钥（对称加密密钥）用于对明文信息进行加密生成密文，同时通过非对称加密技术实现与接收方的会话密钥共享。这样既实现了密钥的高效分配和管理，同时解决了非对称加密技术速度慢的问题。

常见的非对称加密技术有RSA、Elgamal、背包算法、Rabin、D-H、ECC 椭圆曲线加密算法等。

1.3 消息摘要

Hash 算法（哈希）又称 Digest 算法[2]（摘要），它的作用是对一组任意输入数据进行计算，计算的结果是得到一个固定长度的摘要。Hash 函数的主要作用不是实现数据加密与解密，它是一种检验数据完整性的重要技术，运算结果不可逆。通过哈希函数，可以创建数据的“数组指纹”，哈希值一般是一个短的随机数字和字母组成的字符串，它是一个唯一对应一个消息或文本的固定长度的值，它由一个单向 Hash 加密函数对消息进行作用而产生。如果消息在途中改变了，则接收者通过对收到消息的新产生的摘要与原摘要比较，就可知道消息是否被改变了。因此消息摘要保证了消息的完整性。

2 防伪方案的设计

二维码[3]公函防伪传输方案，是国际标准信息安全传输方案与二维码这种信息载体的有机融合。发送方和接收方通过可信站点的方式共同维护自己的一套密钥，其中公钥对外公开，私钥用于加密和签名。具体的方案设计如图 1 所示：

收稿日期：2023-03-04
作者简介：梁一峰（1987-），男，黑龙江绥化人，工程师，硕士；研究方向：信息安全、机器学习。

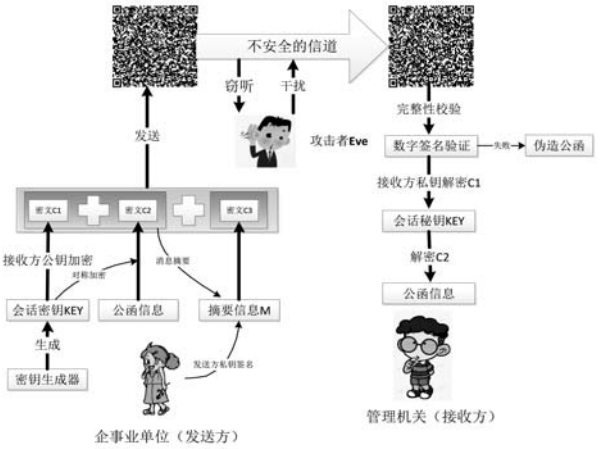


图 1　二维码公函防伪方案设计

发送方最终生成的密文由三部分组成，分别为C1、C2和C3。为了叙述方便，本文做如下假设。

（1）因员工办理业务需要出具公函的企事业单位为发送方，发送方和接收方共同维护同一套基于RSA算法公钥密码基础设施，发送方的公钥为 Pu_{Alice}，发送方的私钥为 Pr_{Alice}。

（2）管理公函的机关单位为接收方，接收方的公钥为 Pu_{Bob}，私钥为 Pr_{Bob}。

（3）发送方和接收方对公函信息的加密采用美国高级加密标准 AES 算法，会话密钥为 Key。

（4）发送的公函信息明文为P，密文信息为C，C有C1、C2、C3 三部分组成。报文的摘要算法可自主选择，本文用 Hash 代替，摘要的结果信息为 M。

2.1　密文的设计

密文C主要有三部分组成，分别是加密后的会话密钥C1、密文 C2 和数字签名 C3。C1 为加密的会话密钥，在每次生成公函时，系统会随机生成一个符合AES标准的会话密钥，使用接收方公钥对该会话密钥进行加密后生成密文 C1。C2 为密文信息，该密文信息是使用AES密钥对明文进行加密后产生。C3 为数字签名，一般使用 RSA 公钥加密算法，为了降低计算的复杂度，方案采取对密文 C1 和 C2 的摘要消息进行签名的方式，并不影响数字签名验证的可靠性。

2.2　加密的过程及安全性设计

加密的过程就是将公函信息进行加密和数字签名的过程，具体加密过程可分为4个主要步骤，它们分别是产生密文C1、产生密文C2、产生密文C3 和产生密文C。加密过程的示意图如图 2 所示：

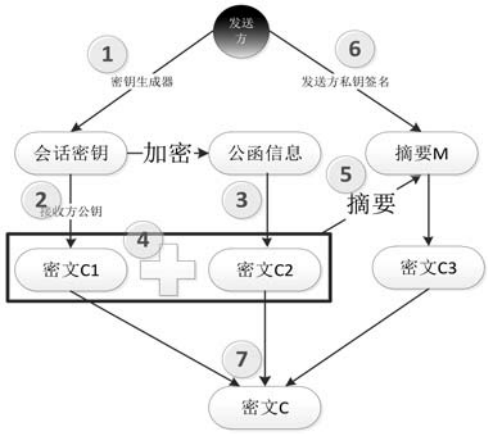


图 2　加密过程示意图

（1）产生密文 C1：使用密钥生成器随机生成 AES 加密密钥 Key，使用接收方的公钥对 Key 进行加密，产生密文 C1，密文 C1 的安全性是基于接收方私钥 Pr_{Bob} 的保密性。

$$C1 = Pu_{Bob}(Key) \quad (1)$$

（2）产生密文 C2：使用会话密钥 Key 对公函信息 P 进行加密，产生密文C2，密文C2的安全性是基于会话密钥Key的保密性。

$$C2 = \mathrm{Key}(P) \quad (2)$$

（3）产生密文 C3：对密文 C1 和 C2 进行拼接产生 C12，计算 C12 的消息摘要产生 M，使用发送方的私钥 Pr_{Actice} 对 M 进行数字签名产生C3，密文C3 的安全性是基于发送方私钥 Pr_{Actice} 的保密性。

（4）产生密文 C：将密文 C1、C2 和 C3 拼接，产生密文 C。为二维码发送方便，对 C 进行 Base64 编码后发送。

2.3　解密的过程及防伪性设计

解密的过程就是将加密后的公函信息进行数字签名验证和解密，具体解密过程可分为 3 个步骤，它们分别是数字签名验证、解密会话密钥、解出明文。解密过程的示意图如图 3 所示：

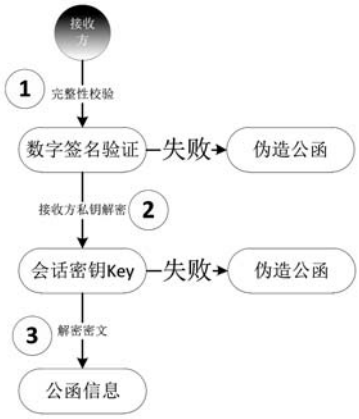


图 3　解密过程示意图

（1）接收方对收到的二维码信息进行数字签名验证，具体方法是先对 C1+C2 的密文信息进行摘要生成 M1，再使用发送方的公钥 Pu_{Alice} 对密文 3 的内容进行解密得到摘要 M2，对比 M1 和 M2 如果相同，则可证明密文是由发送方发送的。签名的防伪性设计是基于发送方私钥 Pr_{Alice} 的保密性。

$$\mathrm{Hash}(C1 + C2) \triangleq Pu_{Alice}(C3) \quad (3)$$

（2）在完成数字签名验证后，使用接收方私钥 Pr_{Bob} 对密文 C1 进行解密，得到会话密钥Key，攻击者在不知道接收方Bob的私钥 Pr_{Bob} 的情况下是无法解出会话密钥 Key 的。

$$\mathrm{Key} = Pr_{Bob}(C1) \quad (4)$$

（3）在解出密钥Key之后，使用Key对C2 信息进行解密，即可得到发送方发送的公函信息 P。

$$\mathrm{P} = \mathrm{Key}(C2) \quad 5)$$

2.4　应用场景

本方案的应用场景如图 4 所示，出具公函的主管部门和需要办理的公函的相关企事业单位共同维护一套离线信息系统。需要办理的公函的相关企事业单位出具相关的纸质公函，公函的内容是办理的具体事项及信息，在公函的左上角附一个包含经过加密和签名的公函信息的二维码。这样在出具公函的主管部门在接收到该公函后，对二维码信息进行身份认证和内容解密，从而实现对公函内容及发送方的身份确认。如果攻击者想伪造这样一份公函，在没有发送方私钥的情况下是几乎不可能的。带数字签名的电子公函是公函防伪的非常重要的手段，它与普通公函相比具有更高的安全性。

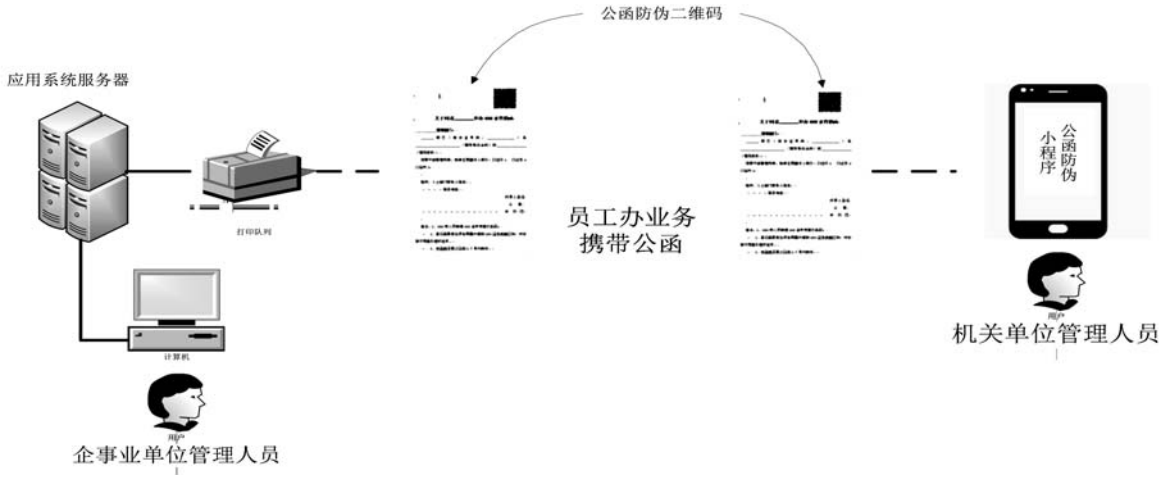
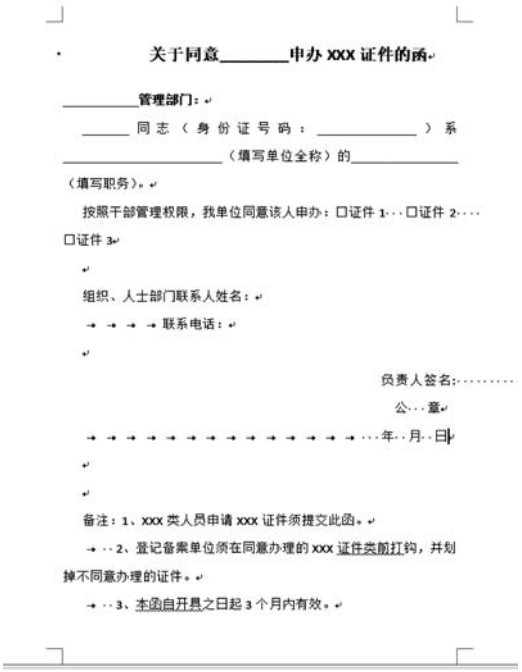


图 4 二维码公函防伪应用场景示意图

3 效果

在确定了方案后，选取了某公函出具的系统实现公函防伪的功能，该系统出具公函主要包含了人员的姓名、身份证、职务、单位联系人姓名、电话等信息，具体公函见图 5：



关于同意_____申办 XXX 证件的函

_____管理部门：

_____同志（身份证号码：_____）系_____（填写单位全称）的_____（填写职务）。

按照干部管理权限，我单位同意该人申办：□证件 1 □证件 2 □证件 3

组织、人士部门联系人姓名：

联系电话：

负责人签名：

公章

年 月 日

备注：1、XXX 类人员申请 XXX 证件须提交此函。

2、登记备案单位须在同意办理的 XXX 证件类前打钩，并划掉不同意办理的证件。

3、本函自开具之日起 3 个月内有效。

图 5 公函示例

系统的发送方使用 C#语言进行开发，开具公函属于业务系统的一部分功能。系统的接收方采用的是手机应用程序的方式，使用 Android 语言进行开发，接收方在接收到公函后，只需要使用安装定制应用程序的手机即可解密公函内的电子信息。使用普通终端无法解密信息，见图 6：

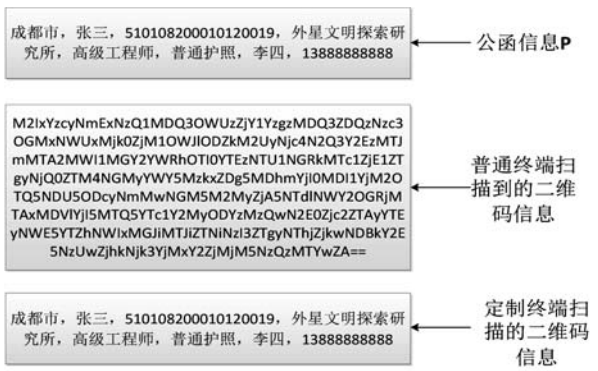


图 6 普通终端与定制终端扫描结果图

4 结语

本文提供了一种基于二维码的公函防伪传输方案，确保了公函电子信息在不安全的信道下传输的安全性。使用了非对称加密算法、对称加密算法、消息摘要等算法，实现了公函的防伪性、不可抵赖性，在实际应用中效果良好。

参考文献：

[1] 林銮云.数据加密技术在计算机软件安全中的应用研究[J].无线互联科技,2022,19(23),90-92.
[2] 刘振兴.一种基于消息摘要的人机验证应用研究[J].网络安全技术与应用,2017:07,54-57.
[3] 李林.二维码技术的应用案例分析[J].集成电路应用,2022:39(06),96-97.

（上接第 136 页）

4 监测界面

软件同时会实时监测当前界面的用户输入参数和控制指令，当检测到用户更改了设备参数或者触发了控制指令时，软件会将这些数据和指令按照表二的格式进行封装，然后通过串口端口发送给控制器，从而实现全屋设备的智能互联。

5 结语

基于 LabView 的智能家居设计，将温度，声音，温湿度进行实时监测，控制在一个安全合理的范围之内。用户使用搭配了 LabView 的智能终端可以实现远程对家具设备的控制。这一设计不仅便捷了人们的生活方式，更提高了人们的生活水平。

参考文献：

[1] 张冷,钟山,刘飞,张鹏展.基于 LabView 的智能家居系统设计[J].金陵科技学院电子信息工程学院学报,2020(01):40-43.
[2] 钱声强.基于 LabView 的智能家居监控系统设计[J].现代电子技术,2013(24):103-105.
[3] 王晓品,周日勇.基于 LabView 的智能家居系统设计[J].计算机与数字工程,2008(12):204-207.