

基于签名认证的电子发票真伪性验证方案

谢绒娜¹, 毛卫华², 史国振³

(1. 北京电子科技学院密码科学与技术系, 北京 100070;

2. 中国邮政储蓄银行, 北京 100034;

3. 北京电子科技学院电子与通信工程系, 北京 100070)

摘要: 随着网络与信息技术的快速发展, 无纸化、电子化成为当今经济生活的发展趋势。电子发票作为一种消费凭证, 在电子商务中的需求越来越广。现有的电子发票验证方法, 是根据发票号码、发票代码、开票日期、金额查询国家电子底账库中的发票信息, 实现对比查询的功能, 不能检测非颁发机构发行发票的造假行为, 不能保证电子发票完全的合法性与真实性。针对以上问题, 提出一种基于签名认证的电子发票真伪性验证方案, 通过验证税务机构签名对空白电子发票进行合法性验证, 验证销售方数字签名以确定开票内容的真实性, 确保证通过的电子发票真实可靠。

关键词: 电子发票; 数字签名; 签名认证; 真伪性验证

中图分类号: TP399

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019067

E-invoice authenticity verification scheme based on signature verification

XIE Rongna¹, MAO Weihua², SHI Guozhen³

1. Department of Cryptography and Technology, Beijing Electronic Science and Technology Institute, Beijing 100070, China

2. Postal Savings Bank of China, Beijing 100034, China

3. Department of Electronics and Communication Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China

Abstract: With the rapid development of network and information technology, paperless and electronic have become the development trend of today's economic life. As a consumption certificate, electronic invoices have become more and more demanding in e-commerce. The existing electronic invoice verification method is to inquire the invoice information in the national electronic account base according to the invoice number, invoice code, billing date, and amount, and realize the function of comparison inquiry, and can not detect the fraudulent behavior of issuing invoices by non-issuing institutions, and cannot guarantee the full legality and authenticity of elec-

收稿日期: 2019-01-14; 修回日期: 2019-03-20

通信作者: 谢绒娜, 486503266@qq.com

基金项目: 国家重点研发计划基金资助项目 (No.2017YFB0802705)

Foundation Item: The National Key Research and Development Program of China (No.2017YFB0802705)

论文引用格式: 谢绒娜, 毛卫华, 史国振. 基于签名认证的电子发票真伪性验证方案[J]. 网络与信息安全学报, 2019, 5(6): 105-112

XIE R N, MAO W H, SHI G Z. E-invoice authenticity verification scheme based on signature verification[J]. Chinese Journal of Network and Information Security, 2019, 5(6): 105-112.

tronic invoices. Aiming at the above problems, a verification scheme for electronic invoice authenticity based on signature authentication was proposed. By verifying the signature of the tax agency, the legality verification of the blank electronic invoice is verified, and the digital signature of the seller is verified to determine the authenticity of the invoiced content. Ensure that the electronic invoices passed for verification are true and reliable.

Key words: electronic invoice, digital signature, signature recognition, authenticity

1 引言

电子商务是利用电子信息技术进行信息生成、存储或通信的商业活动^[1],近年来,随着信息技术的进步,电子商务得到了快速发展。2016年中国电子商务总交易额达到28.9万亿,相比2015年的20.8万亿增长了38.9%,过去5年,中国电子商务交易额的年均增长率高达38.2%^[2]。因其具有很强的灵活性,能够提供全天候的服务,访问速度快^[3],没有地域限制,能够缩短商业供应链等特点,电子商务在旅游、餐饮、娱乐、购物等领域得到了快速推广。电子商务在为人们提供快速、安全、便捷服务的同时,也带来了新的挑战,支付凭证方面的挑战就是其中之一。凭证的真实有效是发挥其凭证作用的前提,验证支付凭证的有效性是急需解决的关键问题。

传统的纸质发票是最常用的支付凭证,纸质发票通过使用特殊纸张打印进行防伪,提高发票造假的难度,降低发票造假的可能性。然而,纸质发票的开具不仅消耗大量的特殊纸张,还会产生一定的运输成本。在发票报销环节,报销人员需要花费时间来核验发票、粘贴发票;财会人员需要花费大量时间来核对发票内容,核验发票的真实性,人工核验容易出现差错,导致效率低、错误率高。

纸质发票从开具到入账的申领发票、邮递、报销、入账均会消耗大量的资源与人工成本,时间周期较长,显然不能满足现阶段社会高速发展的需要。而电子发票的开具、核准、交付都由计算机系统完成,查询、报销更加便捷。使用电子发票有利于节约社会资源、减少发票管理成本、

提高经济运行效率^[4]。电子发票的推广和使用能够有效解决纸质发票存在的核验困难、人工成本高、时间周期长等问题,能够满足互联网科技高速发展下的电子商务市场需求。

为解决发票中存在的造假、冒用、篡改、串用等安全隐患,在电子发票的使用过程中必须确保发票信息的来源真实性和内容完整性。“来源真实性”意味着要有明确的销售方或者发票的开具者,“内容完整性”意味着所需的发票内容没有修改^[5]。怎样确保电子发票的真实性和完整性,是电子发票验证需要解决的核心问题,也是电子发票安全使用的关键。

电子商务的高速发展促使消费者对电子发票的需求愈加强烈,部分地方或企业已经开始试行提供电子发票,但是电子发票的推广和使用范围仍然较小,主要原因是电子发票存在易修改、重复打印的问题,电子发票的真实性难以验证^[6],企业或单位对电子发票的认可度较低。高效验证是电子发票安全使用广泛应用的重要保障,解决了电子发票的真伪性验证问题,电子发票的推广与使用就能得到较快增长。

数字签名是建立在公钥密码技术上的非对称加密技术。每一个使用者都有一对公私钥。私钥由个人单独保存,公钥可以公布于众,数字签名是用私钥进行加密,用公钥进行解密。任何想要确认文件真实性的用户都能用公钥验证数字签名的正确性。因私钥只有签名者知晓,其他人不能仿造签名者的签名数据,数字签名提供了身份认证的功能,既能识别签名者身份,又使签名者不能否认对数据签名的事实,提供不可抵赖性。数

字签名技术的这些特性能够解决电子发票的造假、篡改、冒用等问题。

因此,本文提出了一种基于签名验证的电子发票真伪性验证方案,能够验证电子发票的合法性与真实性。本方案在验证过程中通过验证税务机构的签名对其身份进行验证,确保此发票是税务机构授权开具的发票;对发票信息的合规性进行验证,保证开具的发票在企业的经营范围內,开票时间在使用有效期内;对发票内容进行验证,验证发票是否被篡改,只需验证开具方签名是否真实,就可以确定,三重验证保障验证结果的正确性。电子发票的验证可以与支付系统或销售系统相结合,从根本上杜绝利用发票造假逃税避税的行为。最终实现电子发票的真伪性有效验证。

2 相关工作

电子发票是生成、处理、存储和传输都以电子化的形式进行的发票^[7]。目前,电子发票在北欧和智利的应用与发展较快,欧洲、美洲大部分国家已经建立了电子发票运作体系^[8],国外电子发票大多数采用数字签名技术以及用户信息与银行绑定等方式进行鉴定^[9-10]。中国电子发票的应用则处于逐步增长阶段,大型企业已经开始提供电子发票,小微企业则很少使用。在电子发票系统的安全性方面,国内外学者进行了不同方案的研究。

Spanic 等^[11]提出了一种能够为不同用户提供服务的电子发票系统。该系统在电子发票的生成过程中使用数字签名技术使交易双方都不能否认交易的发生,在数据的完整性方面,使用数字签名和时间戳技术确保电子发票在传递、存储过程中不可被篡改。该系统所生成电子发票的验证可以通过对接数据库进行查询,发票的合法性是通过登录系统人的权限来控制的,但不能从发票本身信息确定发票的合法性。

Netter 等^[12]提出了电子发票的安全模式,将电子发票的安全分为生成、存储、传输3个部分进行保护。对发票的存储使用访问控制方法,运用数字签名技术对发票的完整性进行保护,使用安全信道进行传输,保证发送和接收过程的安全性。该方案对电子发票的全生命周期分段保护,能够确保电子发票的完整性,不易丢失或者非法访问。但该方案不能对电子发票的合法性进行验证。

在国内,Chu 等^[13]首次提出了以数据为导向的电子发票框架。该方案在电子发票的防伪方面使用了数字签名技术,即在电子发票的生成(也就是数据流转)过程中,对添加交易信息的电子发票模板数据进行签名,这样就能够保证发票的完整性,确保交易的不可否认性。但是该方案生成的电子发票没有税务机构签名,不能保证使用的电子发票模板的合法性,对该方案生成的电子发票进行验证时也不能确认此电子发票颁发机构的合法性。

以上几种方案在电子发票的生成过程中都使用了数字签名技术,这个签名是销售方或者发送方的签名,能够保证交易双方的不可否认性及发票的完整性,但是发票未能验证税务机构的签名合法性,因此不能保证电子发票的合法性,存在伪造发票的可能性。

实际上,现有的电子发票验证方案应用的仍是传统思维——比对需查验发票与电子底账库的发票信息,没有从电子发票本身提取信息来验证电子发票的合法性与有效性验证。有效的验证方案需要验证电子发票中的数字签名以确保验证结果的正确性。

3 电子发票的生成原理

3.1 电子发票的安全需求

电子发票是原始的交易凭证^[14],其中含有买

卖双方的大量信息，很多信息涉及商业秘密，对销售方和购买方具有重要的商业价值，如果由于电子发票的安全性出现问题，这些信息泄露或者被恶意第三方窃取，将会对相关方产生很大的不利影响。因此在电子发票的使用过程中，不仅要方便快捷、便于各参与方使用，还应保证电子发票的安全，确保电子发票在开具、传输、存储和查验的过程中信息不被泄露、窃取^[15]。电子发票生成过程要有对应的措施保证数据的完整性、唯一性和有效性，即使发票出现问题，也能够通过验证过程及时发现。

使用数字签名技术保障电子发票的安全，签名算法的选取至关重要。密码算法是保障信息安全的核心技术，尤其电子发票关系到国家的税收征管，使用国家密码管理局颁布的国密算法能够实现完全的安全可控。在国密算法中，SM2 是基于非对称加密的技术，能够满足数字签名非对称加密的需求。在电子发票中使用 SM2 算法进行数字签名，既能实现认证性、不可否认性的要求，又能够保障数据的安全可控。因此，本文的设计方案选用基于 SM2 的数字签名技术来实现。

3.2 电子发票的生成过程

电子发票的信息是由交易双方和交易的具体内容决定的，一个完整的电子发票需要有销售方基本信息、购买方基本信息来确定发票的利益关系人，还有日期、金额、项目名称等交易信息明确交易内容，还需要有税务机构的签名和销售方签名，以便有争议时进行裁决。因此，电子发票生成系统根据交易信息自动生成的电子发票上应有如下信息。

交易信息：包括交易日期、电子发票号码、电子发票代码、校验码，还可以有订单编号、机器码等信息。

商品信息：包括所售商品的品类名称、规格型号、单位、数量、单价、税率、应付税额、应付总额等信息。

销售方信息：包括销售方的名称、纳税人识别号、地址电话、开户行及账号，开票人、收款人及复核人的名称。

购买方信息：包括购买方的名称、纳税人识别号、地址电话、开户行账号等，其中名称和纳税人识别号必须填写，地址电话及开户行账号信息可以选择性填写。

一般的电子发票的生成过程如图 1 所示，是将交易信息转换成标准格式添加到电子发票模板，然后销售方进行签名，形成有效的电子发票。

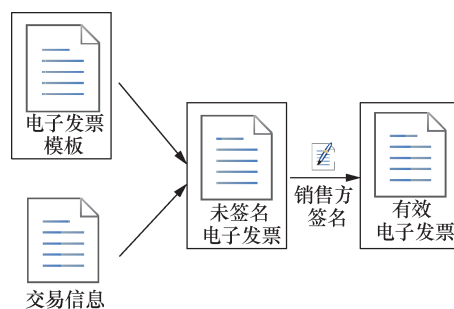


图 1 电子发票生成过程

这种方式生成的电子发票权威性不能确定，如果使用的电子发票模板不是税务机构发行的，不法分子能够很容易地仿制电子发票模板，开具假发票。传统的纸质发票为防止发票造假和偷税漏税等行为，发票上不仅有销售方的公章，而且有税务机关的公章，和纸质发票一样，电子发票不仅需要销售方签名，还需要税务机构签名。

为保证电子发票的合法性，税务机关应该在电子发票模板上签名，生成具有权威性的空白电子发票，以防出现造假行为，交易信息添加之后销售方进行签名，才能生成有效的电子发票。改进后的电子发票生成过程如图 2 所示，具体过程如下。

1) 销售方向税务机关申请电子发票。

2) 税务机关制定电子发票模板，模板中的票面信息包括电子发票号码、电子发票代码、电子发票名称、额度等信息。

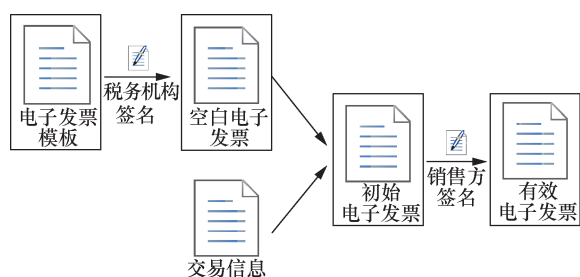


图2 改进电子发票生成过程

3) 税务机关核对模板上的票面信息, 确认无误后, 用私钥对票面信息和销售方公钥进行签名 $s_T = \text{Sig}(sk_T, m_1 \parallel pk_S)$, 生成空白电子发票, 其中 s_T 为税务机关签名, m_1 为电子发票票面信息, pk_S 为销售方公钥。

4) 交易发生后, 购买方提交发票抬头信息, 销售方将交易信息添加到空白电子发票, 生成初始电子发票。

5) 销售方核对交易信息、销售方信息及购买方信息, 确认无误后, 用私钥对交易信息及空白发票上的票面信息、税务机关公钥、销售方名称进行签名 $s_S = \text{Sig}(sk_S, m_2 \parallel (m_1 \parallel pk_S))$, 生成有效电子发票, 其中, s_S 为销售方签名, m_2 为交易信息, sk_S 为销售方私钥。

4 电子发票验证方案

4.1 验证方案描述

电子发票的真伪性验证需要验证发票的合法性与真实性。一般电子发票的校验实际上实现的是电子发票的信息查询功能, 个人购买的物品能够查看金额是否正确, 但不能检测电子发票是否合法。对于单位报销的电子发票, 财会人员不仅需要查看金额, 还需要判断电子发票是否被篡改, 验证过程需要检验电子发票的合法性、真实性与完整性, 仅校验发票信息是否正确无法满足这些需求, 电子发票仍有造假的可能。要验证电子发票的真实性, 需要验证电子发票所携带信息的正确性、完整性和无篡改性。

验证电子发票真实性的过程, 需要确保查询交易信息、购买方信息、销售方信息这3种信息的准确性、完整性和无篡改性, 需要对3种信息进行验证。现有的电子发票查验平台基本上只是提供查询功能, 通过发票号码、发票代码、发票日期、校验码等信息查询商家所开发票的数据库, 给出查询结果, 并没有实现验证功能。

相对于文献[13]的方案, 本文设计的电子发票验证方案增加了对空白电子发票的验证, 通过验证税务机关签名, 验证发票的合法性, 然后验证销售方签名, 检验其完整性, 最后验证交易信息内容的合规性, 完成合法性、完整性与真实性验证。

4.2 具体过程

验证方案主要分为两个部分, 分别为空白电子发票的验证和有效电子发票的验证。具体验证方案详细流程如图3所示, 验证过程描述如下。

Step1 用户向电子发票验证客户端发起验证请求, 并提交电子发票信息。

Step2 验证空白电子发票的合法性。

① 验证平台从电子发票中提取空白电子发票的关键信息, 包括税务机关公钥 pk_T 、税务机关签名 s_T 及票面信息 m_1 。

② 验证税务机关公钥 pk_T 是否有效。可以通过查询公钥列表验证税务机关公钥 pk_T 的正确性, 也可以通过发票中税务机关的数字证书验证税务机关公钥 pk_T 的正确性。若验证通过, 则进行下一步; 若验证不通过, 则查询最新税务机关公钥及过往公钥。

③ 用税务机关私钥 sk_T 验证税务机关签名 s_T 的正确性 $\text{Ver}(sk_T, s_T) = \text{Ver}(sk_T, \text{Sig}(sk_T, m_1 \parallel pk_S))$ 。

如果验证通过, 则说明此空白发票确实是税务机关发出的, 并且未被篡改过; 若验证不通过, 因税务机关公钥 pk_T 已经验证正确, 则说明签名被篡改, 此发票不是税务机关授权发出的, 此发票为假发票, 跳转到 Step4, 返回无效

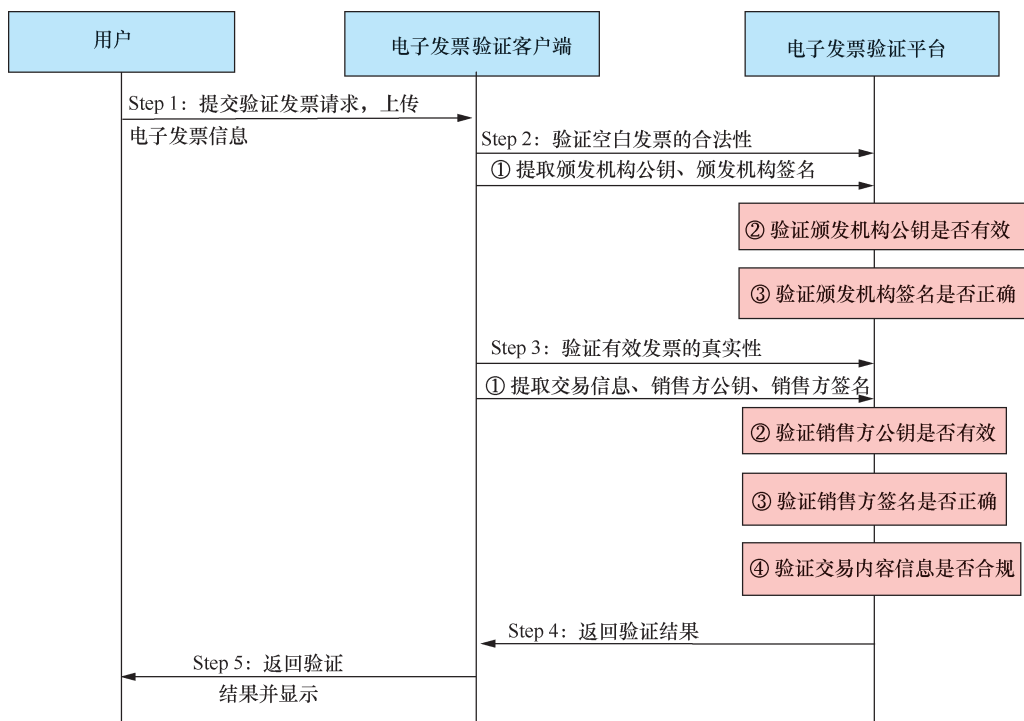


图3 电子发票验证方案详细流程

发票结果。

Step3 验证有效发票的真实性。

① 从电子发票中提取有效电子发票上的关键信息,包括交易内容信息 m_2 、销售方公钥 pk_s 、销售方签名 s_s 。

② 验证销售方公钥 pk_s 是否有效。通过查询公钥列表验证销售方公钥的正确性,也可以通过发票中销售方的数字证书验证销售方公钥的正确性。若验证通过,则进行下一步。若验证不通过,则查询销售方最新公钥以及过往公钥。

③ 用销售方私钥 sk_s 验证销售方签名 s_s $Ver(sk_s, s_s) = Ver(sk_s, Sig(sk_s, m_2 || (m_1 || pk_s)))$ 。若验证通过,则进行合规性验证,若验证不通过,则说明销售方签名被篡改过,转到 Step4, 返回无效发票结果。

④ 验证交易内容信息的合规性。验证此电子发票开具的金额是否在允许额度内, 验证发票的开票日期是否在有效期限内, 验证所开发票

的业务类型是否符合规定。都验证通过, 则判定此发票为有效发票, 返回有效发票验证结果; 若有一项及以上验证出现错误, 则判定此发票为无效发票, 进行下一步, 返回无效发票验证结果。

Step4 验证平台向客户端返回验证结果。

Step5 客户端给用户返回最终验证结果并显示, 发票真伪性验证完成。

5 安全性分析

5.1 可靠性

1) 不可伪造性

签名算法的不可伪造性保证了攻击者不能篡改发票上的任何信息, 并且只有税务机构和销售方才能用私钥生成有效签名。即使攻击者想篡改发票上的信息, 攻击者没有税务机构或销售方的私钥, 就不能形成相应签名, 用数字证书中的公钥验证销售方签名时就能够识别被

篡改的发票。

即使攻击者用真实的空白发票伪造了一张发票, 没有销售方的私钥, 依然不能生成相应签名, 验证签名的过程中, 就能发现伪造发票。

2) 完整性

完整的电子发票包括销售方基本信息、受票方基本信息、日期、金额、业务类型、交易明细、税务机关签名、销售方签名。由不可伪造性可知发票不可能被篡改或伪造, 验证过程需要用到上述信息, 有信息缺漏也属于非法发票, 整个验证过程能够确保发票的完整性。

3) 可追踪

电子发票存在的造假行为包括非税务机构颁发发票, 非销售方所开具发票, 交易明细出现差错, 超过有效期限, 业务类型不匹配。针对每一个有可能造假的生成环节, 验证过程都做了相应验证, 易于追溯问题来源。若是税务机关签名验证错误, 说明不是合法的电子发票; 如果销售方签名验证错误, 则说明发票内容被篡改, 发票的真实性不可信; 如果发票内容合规性验证不通过, 则说明是销售方对发票的使用不合格, 此发票不是有效发票。

5.2 有效性

1) 合法性

合法性是指符合国家税收体制, 税务机关认可的。验证过程中首先通过验证税务机关签名来验证空白发票的合法性, 如果验证通过, 则说明该发票是税务机构颁发, 国家税务部门承认的发票, 从国家税收体制上能够确定发票是合法的; 如果验证不通过, 则说明该发票不是税务机构颁发的, 是不合法的发票, 方案能够确保验证通过的皆为合法发票。

2) 时效性

发票真实性验证: 主要时间消耗为信息提取时间, 验证税务机关签名是否有效, 即一次签名

验证时间。

发票有效性验证: 主要时间消耗为信息提取阶段、验证销售方签名是否有效, 即一次签名验证时间。

每次验证过程中, 本文发票验证方案共调用了两次签名验证算法, 步骤简便, 验证效率高, 能够缩短响应时间。

3) 普适性

本文方案验证了电子发票可能造假的全部内容, 验证原理适用于所有种类的电子发票。验证方案是在现有电子发票生成方案上进行的改进, 适用于现有的电子发票系统。

6 结束语

电子商务的发展使电子发票的需求与应用越来越广, 但电子发票的查验却还只是通过发票号码、发票代码、交易日期等信息查询税务机构数据库中的电子发票, 对比需核验发票与查询到的信息, 没有从发票本身数据验证电子发票的真实性和完整性。本文设计的电子发票验证方案运用数字签名技术所具有的完整性、认证性、不可抵赖性, 对发票生成过程中涉及的税务机构和销售方的签名进行验证, 确保发票是由税务机构权威发行, 解决了发票来源的造假问题, 并且能够鉴别是否存在发票信息被篡改的问题, 再对交易信息的合规性验证, 完成了电子发票的真伪性验证和内容真实性验证, 确保了发票的真实性、完整性和合法性。

参考文献:

- [1] HILL R, WALDEN I. The draft UNCITRAL model law for electronic commerce: issues and solutions[J]. Computer Lawyer, 1996, 13(3): 18-22.
- [2] HONGFEI Y. National report on e-commerce development in China[R]. United Nations Industrial Development Organization, Inclusive and Sustainable Industrial Development Working Paper Series, 2017.

- [3] XIANG J Y, JING L B. Electronic commerce in China: current status, development strategies, and new trends[J]. China Finance and Economic Review, 2014, 3(3): 71-94.
- [4] HUMSKI L, VRDOLJAK B, SKOCIR Z. Concept, development and implementation of FER e-invoice system[C]//International Conference on Software, Telecommunications & Computer Networks. 2012: 1-5.
- [5] 谢波峰, 刘萧优. 欧盟及我国台湾地区电子发票的经验借鉴和启示[J]. 国际税收, 2016(7): 70-74.
XIE B F, LIU X Y. Reference and enlightenment of the electronic invoice in the EU and Taiwan district[J]. International Taxation in China, 2016 (7): 70-74.
- [6] JOUNGY -J, TSENGY C, CHA S C, et al. Motivations, deployment, and assessment of taiwan's e-invoicing system: an overview[C]// International Conference on System Sciences. IEEE, 2014: 2200- 2209.
- [7] European commission. European electronic invoicing (EEI) final report[R]. European Commission Informal Task Force on e-Invoicing, 2007.
- [8] 柴跃廷, 于潇, 黄亚东. 电子发票管理与公共服务体系设计与实现[J]. 清华大学学报(自然科学版), 2018, 58(6): 598-602.
CHAI Y T, YU X, HUANG Y D. Electronic invoice management and public service system[J]. Journal of Tsinghua University(Science and Technology), 2018, 58(6): 598-602.
- [9] PONNAPALLI H K B, SAXENA A. A digital signature architecture for web apps[J]. IT Professional, 2013, 15(2): 42-49.
- [10] CHUCHAISRI P, NEWMAN R E. Multi-resolution elliptic curve digital signature[C]// IEEE, Conference on Local Computer Networks, IEEE Computer Society. 2012: 93-101.
- [11] ŠPANIĆ D, RISTIĆ D, VRDOLJAK B. An electronic invoicing system[C]//IEEE International Conference on Telecommunications. 2011:149 - 156.
- [12] NETTER M, PERNUL G. Integrating security patterns into the electronic invoicing process[C]//20th International Workshop on Database and Expert Systems Application. 2009: 150-154.
- [13] CHU H, CHAI Y, LIU Y, et al. A novel e-invoice framework to ards data-oriented taxation system[C]//IEEE International Conference on Computer Supported Cooperative Work in Design. 2014: 242-246.
- [14] LINDE S, HANSEN B. Key factors for the adoption and subsequent use of e-invoicing[J]. Academia Revista Latinoamericana De Administración, 2012, 111(50): 15-30.
- [15] MATUS A, GUERRA E, FUERTES W, et al. On the development of an electronic invoicing solution to integrate SMEs with a tax-collection e-government-platform[C]//IEEE Fourth International Conference on Edemocracy & Egovernment. 2017: 94-101.

[作者简介]



谢绒娜(1976-), 女, 山西永济人, 北京电子科技学院副教授, 主要研究方向为密码应用安全, 网络与系统安全。



毛卫华(1992-), 女, 河南周口人, 北京电子科技学院硕士生, 主要研究方向为电子发票和信息安全。



史国振(1974-), 男, 河南济源人, 博士, 北京电子科技学院副教授、硕士生导师, 主要研究方向为网络与系统安全、嵌入式安全。