

基于 SM2 联合签名的电子发票公开验证方案

罗琦榕, 曹进, 李晖, 赵兴文, 尚超

(西安电子科技大学网络与信息安全学院, 陕西 西安 710071)

摘要: 为解决当前电子发票防伪困难、隐私泄露、验证效率低等问题, 针对全程无纸化的电子发票文件, 提出了一种基于国密签名算法的电子发票公开验证架构。面向电子发票文件数据来源复杂、票面用户信息敏感、数据流转频繁等特征及电子发票高效公开查验需求, 在电子发票服务架构下设计电子发票生成及查验协议, 基于无证书联合签名提出发票防伪签名码生成方案, 实现开票方与税务主管部门的多重数据核验与签名, 支持各类型的发票持有者对电子发票的真伪及数据完整性进行公开查验。融合数据加密算法对电子发票中的用户隐私数据进行保护, 同时可满足各类发票应用场景下的真伪或状态验证需求, 解决了当前电子发票文件中用户消费信息等敏感数据在传递中泄露的问题, 突破了电子发票仅能通过在线系统核对真伪的局限。查验方仅需验证单次签名即可确认开票方及主管部分等双方签名的电子发票真伪性, 同时利用公钥加密实现了隐私数据, 方案中使用国密算法符合电子发票应用需求。调用 Scyther 安全仿真工具对方案安全性进行分析, 在各类攻击下可安全验证数据的完整性及来源真实性并保证隐私数据的保密性。在查验计算开销及发票文件数据量两方面, 与国外已实行的典型电子发票查验方案及同类型基于数字签名的电子发票查验方案进行对比, 所提电子发票公开查验方案在查验效率及发票文件大小等两方面具有明显的优势。

关键词: 电子发票; 公开查验; 国密算法; 无证书签名

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022020

Electronic invoice public verification scheme based on SM2 coalition signature algorithm

LUO Yurong, CAO Jin, LI Hui, ZHAO Xingwen, SHANG Chao

School of Cyber Engineering, Xidian University, Xi'an 710071, China

Abstract: In order to solve the current problems of electronic invoices, such as anti-counterfeiting, privacy leakage and low verification efficiency, an electronic invoice public verification architecture based on the national

收稿日期: 2021-10-11; 修回日期: 2022-03-02

通信作者: 曹进, caoj897@126.com

基金项目: 国家重点研发计划(2018YFB0803900); 陕西省重点研发计划(2020ZDLGY08-08)

Foundation Items: The National Key Research and Development Program of China (2018YFB0803900), The Key Research and Development Program of Shaanxi (2020ZDLGY08-08)

引用格式: 罗琦榕, 曹进, 李晖, 等. 基于 SM2 联合签名的电子发票公开验证方案[J]. 网络与信息安全学报, 2022, 8(2): 122-131.

Citation Format: LUO Y R, CAO J, LI H, et al. Electronic invoice public verification scheme based on SM2 coalition signature algorithm[J]. Chinese Journal of Network and Information Security, 2022, 8(2): 122-131.

signature algorithm was proposed. Electronic invoice documents have complex data sources, sensitive user information on the ticket surface, frequent data flow and other characteristics as well as the demand for efficient public verification. Based on these motivations, the e-invoice generation and verification protocol was designed. Besides, a signature code generation scheme for invoice anti-counterfeiting was proposed based on certificate-free joint signature. Then multiple data verification and signatures of the invoicing party and the taxation authority can be realized. All kinds of invoice holders can not only verify the authenticity and data integrity of electronic invoices, but also publicly check the authenticity and data integrity of electronic invoices. The integration of data encryption algorithms protects user privacy data in electronic invoices, and at the same time can fulfill the requirements for authenticity or status verification under various invoice application scenarios. The checking party only needs to verify one signature to confirm the authenticity of the electronic invoice signed by both parties. Scyther security simulation tools were used to analyze the security of the proposed solution, which can verify the integrity and authenticity of the data source and check the confidentiality of the privacy data under various types of attacks. Compared with a typical overseas e-invoice checking scheme and a similar digital signature-based e-invoice checking scheme, the proposed scheme has obvious advantages in terms of checking efficiency and invoice file size.

Keywords: electronic invoice, public verification, national cryptographic algorithms, certificateless signature

0 引言

随着移动互联网及电子商务的迅速发展,我国网络/移动支付逐渐普及,目前已有 7.68 亿网络支付用户,占网络用户的 85%^[1]。发票是支付消费的凭证文件,而在网络支付盛行环境中,基于环保与便利的需求,传统纸质发票逐步实现电子化,网络支付与电子发票技术体系融合程度逐步加深,能够推动行业效能及发展的大幅提升。电子发票具有无纸化、易存储、便于传递与交付、低消耗等优势,但电子发票文件因失去物理防伪特征,给发票防伪及其查验操作带来许多安全挑战^[2]。

纸质发票可通过特殊的制造工艺进行防伪,并同时保证发票的唯一性,防止重复报销。由于电子发票数据易于复制且流转频繁,收票方难以保证所持有的电子发票的完整性、有效性及合法性^[3]。电子发票防伪数据简单、开票核验方单一等,导致伪造成本低,易重复报销。电子发票因缺乏相关安全标准,从 2013 年京东集团发布中国网络支付首张电子发票至今,我国尚未形成完备的电子发票防伪体系,也为电子发票的推行带来阻碍。因此,电子发票的防伪码生成及公开查验成为电子发票技术应用推广的核心问题之一。此外,目前电子发票查验模式为四要素对比查验,

且开具、交付与流转方式未进行安全管控,电子发票文件中交易信息以明文形式存储,导致销售方商业数据外流,同时引发购买方隐私数据泄露等严重的数据安全问题,在公开查验的同时保护交易双方隐私数据成为未来电子发票查验技术发展的必然趋势。为实现发票的全面安全无纸化,建立统一普适的电子发票公开查验架构具有非常重要的理论意义和应用前景。

电子发票防伪技术主要分为三类:①税控码防伪;②电子签章或电子签名防伪;③二维条码防伪。税控码防伪方案与纸质发票统一,采用在线开具系统,由税务机关生成与交易信息一致的税控防伪码,发票内容与电子发票图形文件保存完全一致从而进行对比查验。文献[4]实现了税控码防伪查验系统,是目前税务机关官方采用的查验方案。持票人登录国家税务总局全增值税发票查验平台进行复杂的查验操作,需要手动输入发票号码及税控信息,因为系统并发服务资源控制了用户每日查验次数,导致用户无法根据自身需求随时随地进行便捷的真伪查验。电子签章或电子签名可以实现与纸质发票税务机关盖章相同的效果,并可通过对发票数据签名保障发票信息的完整性及不可否认性。文献[5]设计了一种适应差异化用户的电子发票生成及查验系统,其方案采用数字签名对发票信息进行传递完整性保护,

但系统仍采用数据库要素对比的方式进行真伪查验, 查验的便捷性和效率仍未提升。文献[6]提出了一种基于 SM2 数字签名的发票真伪查验方案, 融合了税务机关及开票方的双重签名, 查验者可通过验证签名从而进行公开查验。但该方案中, 税务机关仅对发票模板进行签名, 未对发票交易信息进行核验, 可能引发发票数据造假等问题。此外, 该方案未对发票交易信息进行传输安全性保护, 导致交易双方隐私泄露。文献[7]为巴西官方电子发票设计管理系统, 采用公钥体制对电子发票数据进行签名, 但其中仅包括税务机关的核验及签名, 发票交易信息的正确性无法得到保障。文献[8]提出一种通用的基于数字签名的发票真伪查验方案, 但其需要多重验证, 导致计算开销过大。二维条码防伪方式基于我国自主知识产权的二维码技术^[9-10], 可将发票要素信息加密编码, 具有存储量大及防伪效率高等优势, 文献[11]详细说明了我国基于二维码的电子发票防伪查验方案, 但二维码查验方式对硬件需求高, 需要手机摄像头或专用查验机器扫描后与税务系统数据库进行发票对比查验, 查验流程复杂且难实现全票面信息防伪查验。此外, 有一些基于新技术的电子发票查验方案, 文献[12-13]提出基于区块链的电子发票查验及异常追溯方案, 其本质是传统发票要素对比方案, 并且造成大量存储冗余, 不适用于当前的电子商务环境。以上方案均需在客户端在线请求税务系统数据库信息对比税控信息, 从而实现发票真伪验证, 实时性和便捷性较低。我国税务信息化从“纸质控税”发展至“互联网+电子票据融合”, 急需一种电子发票查验方案实现发票数据真伪性、完整性、有效性等全方位的验证, 为收票方、报销单位等各种角色提供公开、隐私保护控制、便捷高效的查验方案, 支撑电子发票服务的全面落地与实施。

本文主要的研究工作如下。

1) 建立基于电子签名的电子发票公开查验架构。针对开票、流转、查验等三大流程, 综合考虑电子发票信息的多方来源, 设计融合了开票方及税务主管部门核验的电子发票通用防伪码生成机制。

2) 基于 SM2 签名算法设计了适用于电子发票系统的联合无证书签名方案, 实现电子发票信息与交易信息的双重完整性、真伪性、有效性保护, 对发票交易信息进行加密保护, 控制用户敏感信息的传播。联合签名有效降低查验者的验签次数, 提高查验效率及便捷性。

3) 仿真结果及安全分析表明, 本文方案具有很高的计算效率及简洁的发票存储结构, 能实现具有隐私保护的电子发票公开多维信息查验并能抵抗各类协议攻击。与传统基于数字签名的发票查验方案进行性能对比, 验证了本文方案的高效性及安全功能的多样性。

1 电子发票查验模型

1.1 安全模型

文献[14]的电子发票服务架构包含电子发票服务系统、收票方、开票方、查验方(如图1所示)。

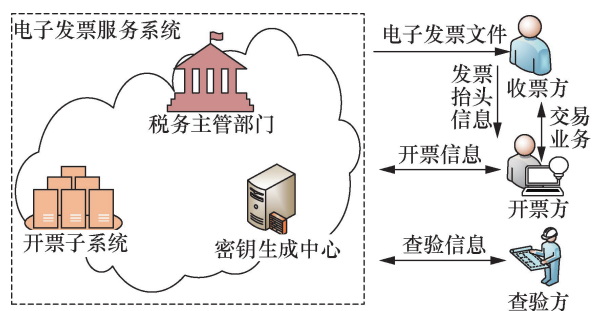


图1 电子发票服务架构
Figure 1 Electronic invoice service structure

1) 电子发票服务系统。电子发票服务系统由国家税务机关进行管理及运营, 为包括商家和消费者在内的实体用户提供开票、查验及安全监管服务, 在本文的查验架构中, 电子发票服务系统中应包含密钥生成中心(KGC, key generation center)及开票子服务系统。

2) 开票方。开票方一般为商品销售方, 为购买者提供电子发票。

3) 收票方。收票方一般为商品消费者, 需要获得发票进行报销等活动。

4) 查验方。查验方即查验者, 本文方案中任何获得电子发票文件的实体均可进行发票真伪查验。

本文方案中攻击者可监听、截获或篡改公开信道传输的消息，本文电子发票查验方案应满足以下安全需求。

1) 电子发票真伪公开可验证性：获得电子发票文件的任意实体可验证电子发票真伪，即可准确判断该电子发票为攻击者伪造/篡改的假票或为税务机关及开票方均认可的真票。发票真伪性包括电子发票数据的准确性、完整性及有效性。

2) 电子发票防伪造性：攻击者无法根据公开信道所截获的信息伪造出能通过真伪性验证的发票数据。攻击者可能是服务架构中任何一方，也可能是电子发票服务系统中无身份的攻击者。

3) 发票隐私信息保护性：电子发票包含商品购买者的隐私信息（如购买的具体商品及数量信息），本文方案应保障除报销等用途外的查验者可获得发票具体信息，其他查验者仅能查验其真伪而无法获取购买者的隐私信息。

1.2 电子发票公开查验架构

电子发票元数据由发票唯一标识、交易数据及税控信息等部分组成，其中税控信息为税务部门生成的发票信息安全保障数据，如防伪码、真伪验证码等。交易信息主要为两部分：①由收票方提供包括购买方名称、纳税人识别号、开户银行等信息在内的发票抬头；②由开票方提交包括购买商品详情/价格/数量、销售方信息、交易时间等在内的交易明细。

为保障电子发票的可验证性，电子发票应由税务主管部门及开票方共同签名，保证交易信息的正确性及发票的有效性。文献[6]提出一种可验证的税务主管部门/开票方双签名方案，但该方案中由主管部门对模板签名后直接交予开票方，无法由主管部门确认及记录交易信息，不利于发票的追溯与稽查，该方案需要两次签名验证，造成极大的计算消耗。因此，本文引入一种基于 SM2 算法的联合无证书签名方案，设计了一种电子发票公开查验架构（如图 2 所示），具体过程如下。

1) 收票方发起开票请求，向开票方提供发票抬头信息。

2) 开票方向电子发票服务系统提出开票申请，开票子系统反馈发票唯一标识及发票抬头单位或个人公钥至开票方。

3) 开票方生成开票信息（含交易明细、发票抬头等信息），通过其交易安全信道发送至收票方，如购物平台客户端发送至消费者。

4) 收票方确认交易信息等开票信息无误后，开票方将交易信息与发票唯一标识签名后发送至开票子系统。

5) 税务主管部门验证签名及交易信息合规后，对发票内容进行签名，并根据标准电子发票模板生成电子发票数据发送至收票方。

6) 收票方可直接通过签名内容验证发票内容的有效性，或提交至报销单位由报销单位查验。其他获得电子发票数据的实体也可直接验证签名有效性进行真伪性查验。

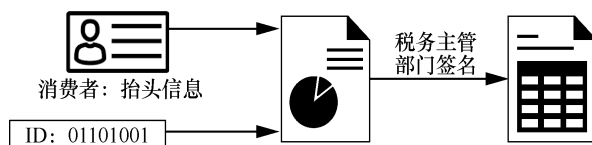


图2 电子发票公开查验架构
Figure 2 electronic credentials public verification architecture

2 公开查验方案

2.1 系统初始化

基于 SM2^[15]无证书签名方案可生成电子发票税控信息，实现电子发票真伪公开查验。为适用于电子发票服务架构，基于文献[16]中的无证书 SM2 加密方案设计无证书联合签名方案生成电子发票查验码，形成具有隐私保护的电子凭据查验架构，防止发票信息泄露、篡改、造假等，保障电子发票数据的准确性、完整性、有效性。表 1 为系统参数符号对照。

电子发票服务系统遵循国家标准^[17]生成椭圆曲线参数，其中 G 为椭圆曲线的基点， G 的阶为素数 n ，KGC 生成系统公私钥对 (PK_s, SK_s) 。

2.2 系统 n 用户注册

对任意用户（包括开票方商户、收票方及查验方） i 在电子发票服务系统注册，将生成一对用户公私钥，并与税务主管 $Q_i = (d_i)^{-1} Q_{ED} + k_i G$ 部门生成一对联合公私钥。注册步骤如下。

表 1 系统参数符号对照
Table 1 System parameter symbol cross-reference

参数	含义
G	系统椭圆曲线基点
n	基点 G 的阶
(PK_S, SK_S)	KGC 系统公私钥对
ED	税务主管部门
V	发票抬头中开票单位或个人 (系统标识)
IE	开票方 (系统标识)
IR	收票方 (系统标识)
d_i	实体 i 的私钥
Q_i	实体 i 的部分公钥
P_i	实体 i 的公钥
k_i	实体 i 的随机参数 $t_i (r, s_i)$
t_i	实体 i 的联合公钥参数
R_i	实体 i 的联合签名参数
(r, s_i)	实体 i 的部分签名
(x_A, y_A)	椭圆曲线上的点 A
T	开票时间戳
I	发票唯一标识符
M	开票交易信息
N	收票方选取的随机数
$H(\cdot)$	使用 SM3 Hash 函数
$\text{Sig}_{SK(\cdot)}$	基于 SM2 算法, 使用私钥 SK 签名
$\text{Ver}_{PK(\cdot)}$	基于 SM2 算法, 使用公钥 PK 验签
$\text{Enc}_{PK(\cdot)}$	基于 SM2 算法, 使用公钥 PK 加密
$\text{Dec}_{SK(\cdot)}$	基于 SM2 算法, 使用私钥 SK 解密

- 1) 税务主管部门选取随机数 $k_{ED} \in [1, n-1]$, 计算 $Q_{ED} = k_{ED}G$ 并通过公开信道发送至用户 i 。
- 2) 用户 i 选取随机数 $k_i \in [1, n-1]$ 及 $d_i \in [1, n-2]$, 计算 $Q_i = (d_i)^{-1}Q_{ED} + k_iG$ 并通过公开信道发送至 KGC。
- 3) KGC 选取随机数 $k_0 \in [1, n-1]$, 计算 $Q = Q_i + k_0G$ 、 $t_0 = k_0 + H(i \| Q)SK_S \pmod{n}$, 其中, Q 作为用户 i 的部分公钥发布, t_0 发送至 i 。
- 4) 用户 i 计算 $t_i = d_i(k_i + t_0 + 1) \pmod{n}$ 及公钥 $P_i = (d_i)^{-1}G$ 作为公钥发布, 私钥为 d_i 。
- 5) 税务主管部门计算相关的私钥, 用于与用户 i 联合签名, 即 $d_{ED} = (k_{ED} + t_i)^{-1} \pmod{n}$ 及对应公钥 $P_{ED} = (d_{ED})^{-1}P_i$ 。
- 6) 用户 i 与税务主管部门的联合公钥为 $P = Q + H(i \| Q)PK_S$ 。

2.3 电子发票防伪码生成

电子发票信息由税务主管部门、开票方、收票方三方数据共同生成, 并由税务主管部门和开票方核验交易信息后联合签名形成电子发票防伪码。发票防伪码生成步骤如下。

步骤 1 接收开票请求后, 税务主管部门创建一份新的电子发票。

1) 生成发票唯一标识码 I 。

2) 再次选取随机数 $k_{ED} \in [1, n-1]$, 并计算

$$R_{ED} = k_{ED}P_{ED}。$$

3) 发送 (I, R_{ED}) 至开票方 IE。

步骤 2 开票方 IE 与收票方 IR 通过线下或线上安全交易平台确认开票交易信息 M 及收票方自选随机数 N , 其中收票方 IR 提供的发票抬头单位或个人为 V 。

步骤 3 开票方对发票信息进行 SM2 签名算法中的标准预处理^[16]生成算法参数, 并对交易信息签名, 具体如下。

1) 预处理 1 输出字符串用于预处理 2:

$Z = H(\text{ENTL} \| \text{IE} \| a \| b \| x_G \| y_G \| x_p \| y_p)$; 其中, ENTL 为实体标识符 IE 的比特长度, a 、 b 为系统椭圆曲线参数。

2) 预处理 2 生成用于签名的消息 $\overline{M}$ 。

$$\overline{M} = H(Z \| I \oplus N \| \text{Enc}_{P_i}(M \oplus T)) \quad (1)$$

步骤 4 开票方签名。

1) 开票方选取随机数 $k_{IE} \in [1, n-1]$, 计算

$$R_{IE} = R_{ED} + k_{IE}P_{IE} = (x_1, y_1) \quad (2)$$

$$r = (\overline{M} + x_1) \pmod{n} \quad (3)$$

$$s_{IE} = k_{IE} + rd_{IE} \pmod{n} \quad (4)$$

开票方生成的部分签名 (r, s_{IE}) 和交易数据 $(T, M, \overline{M}, N)$ 均通过电子凭据系统安全信道传输至税务主管部门。

步骤 5 税务主管部门对开票方签名、开票信息进行核查。

1) 计算 $R_{ED} + s_{IE}P_{IE} - rG = (x_1', y_1')$ 。

2) 验证 $r = (\overline{M} + x_1') \pmod{n}$ 是否成立, 验证开票信息 (T, M) 是否异常。

3) 若等式成立, 未出现异常, 则税务主管部

门正常签名生成电子发票。

$$s_{ED} = k_{ED} + s_{IE} d_{ED} \pmod{n} \quad (5)$$

$$s = s_{ED} - r \pmod{n} \quad (6)$$

最终防伪码签名为 (r, s) 。发票数据为

$$M_I = (I, N, T, (r, s), \text{Enc}_{P_I}(M \oplus T), \text{IE}) \quad (7)$$

2.4 发票冲销或作废

目前, 发票使用规定中表明在发生销货退回、开票有误等情形, 或开具时发现有误的, 可作废处理。作废发票需在防伪税控系统中将相应的数据或文件标记“作废”处理。本文方案中, 需由开票方提出申请并签名后, 由税务部门审核并签名生成“作废发票”发送至发票抬头所指定的个人或单位, 防止作废发票的使用, 发票冲销或作废步骤如下。

开票方收到退货或发票开具错误提醒时, 生成作废发票信息 $(I \oplus N, \text{invalid}, C)$, 其中 C 为开票方选取的随机数, 称为冲销编号。

1) 预处理 2 生成作废发票签名信息 M_V 。

$$M_V = H(Z \| I \oplus N \| \text{invalid} \| C) \quad (8)$$

2) 开票方将消息 M_V 及 $(I \oplus N, \text{invalid}, C)$ 发送至税务主管部门申请发票冲销, 主管部门批准后选取随机数 $k'_{ED} \in [1, n-1]$ 并计算 $R'_{ED} = k'_{ED} P_{ED}$ 发送至开票方。

3) 开票方采取发票防伪码生成步骤 4 中方式对 M_V 进行签名, 并将部分签名 (r', s'_{IE}) 发送至税务主管部门。

4) 税务主管部门采取发票防伪码生成步骤 5 中方式生成签名 (r', s') , 冲销 (作废) 发票数据为

$$M_{IV} = (\text{invalid}, I, N, T', C, (r', s'), \text{IE}) \quad (9)$$

5) 税务主管部门将冲销 (作废) 发票 M_{IV} 存储记录, 并发送至开票方 IE 及发票抬头中的单位或个人 V , 防止作废发票的使用。

2.5 发票公开查验

对于任意获得发票数据的验证者, 均可通过验证发票中的联合签名有效性判断发票真伪。查验方公开查验步骤如下。

1) 查询开票方部分公钥后, 计算开票方 IE 的联合公钥 $P = Q + H(\text{IE} \| Q) \text{PK}_S$ 。

2) 与发票防伪码生成中步骤 3 一致, 完成预

处理计算获得 $\overline{M}$ 。

3) 提取发票信息计算 $u = r + s \pmod{n}$, $sG + uP = (x_2, y_2)$ 。

4) 验证 $r = (\overline{M} + x_2) \pmod{n}$ 是否成立, 若等式成立, 则判断为有效真发票, 若等式不成立, 则判断发票无效。

5) 对发票抬头中指定的单位或个人 V 应首先检查发票编号是否在冲销发票数据库中或已报销, 若为有效发票编号则按照步骤 1)~步骤 3) 进行验证, 并使用私钥计算 $\text{Dec}_{d_V}(\text{Enc}_{P_I}(M \oplus T)) \oplus T$ 获得发票具体交易信息, 进行报销等操作。

3 方案安全分析

3.1 安全功能正确性分析

3.1.1 签名有效性

由式(2)及 $P_{IE} = (d_{IE})^{-1}G$ 可推得税务机关验证部分签名有

$$\begin{aligned} (x'_1, y'_1) &= R_{ED} + s_{IE} P_{IE} - rG = \\ R_{ED} + k_{IE} P_{IE} + rG - rG &= R_{ED} + k_{IE} P_{IE} = (x_1, y_1) \end{aligned}$$

从上式可得 $x_1 = x'_1$, 继而可推得 $r = (\overline{M} + x_1) \pmod{n} = (\overline{M} + x'_1) \pmod{n}$ 成立, 部分签名验证有效。

对标准 SM2 签名算法, 仅需验证等式 $sG + uP = R_{IE} = (x_1, y_1)$ 成立。

由式(6)及等式 $u = r + s \pmod{n}$ 可推得

$$\begin{aligned} sG + uP &= (s_{ED} - r)G + s_{ED}(P_{ED} - G) = s_{ED}P_{ED} - rG = \\ (k_{ED} + s_{IE}d_{ED})P_{ED} - rG &= k_{ED}P_{ED} + s_{IE}P_{IE} - rG = \\ R_{ED} + s_{IE}P_{IE} - rG &= R_{IE} \end{aligned}$$

可证本文方案中所采用的联合签名有效性与标准 SM2 签名一致。

3.1.2 公开可验证性

任何获得发票数据 M_I 可通过提取签名及查询开票方公钥计算签名联合公钥, 对发票真伪进行验证, 仅需一次验签即可验证税务主管部门及开票方双方签名的发票数据。税务主管部门的有效签名代表该发票符合国家税务相关法规, 即发票合法性。开具方有效签名代表发票交易信息经开具方及消费方核验认可, 即发票的正确性。此外, 签名有效可证明发票数据未被篡改, 即发票

的完整性。综上,发票数据所有者可便捷地实现电子发票真伪的公开验证。

3.1.3 防伪造性

由签名不可伪造性可知,仅由税务主管部门及开票方双方核验签名后才可生成有效签名,攻击者需要同时持有税务主管部门私钥 d_{ED} 及开票方私钥 d_{IE} 或仅持有联合私钥 $d=(d_{ED}d_{IE})^{-1}-1 \pmod n$ 才能生成有效签名,其中任意一方或其他攻击者无法仿冒或伪造签名。本文方案中,发票由税务机关给出的唯一标识码 I 及收票方选择的发票随机数编码 N 保持发票唯一性,并添加电子发票开具时间戳 T 防止重放攻击伪造发票,同时发票报销单位可通过记录已报销/已处理发票的 (I,N) 防止不合规的重复使用。

3.1.4 隐私保护性

本文方案形成的发票数据中交易信息等用户敏感隐私数据以 $Enc_{P_r}(M \oplus T)$ 加密形式存储或流转。发票抬头中指向的单位或个人 V 可使用私钥解密获得具体的发票交易信息,用于报销等后续操作。在本文方案设计中,仅开票方、消费方(申请开票者)、税务主管部门及发票抬头中单位或个人可检查交易信息,在保障发票可追踪、可用性的同时保护了交易双方的隐私信息。

3.1.5 抗协议攻击

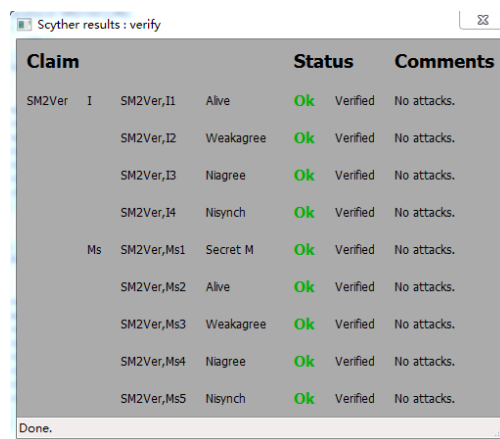
本文方案能够抵抗多种协议攻击。首先,税务系统需核验开票方签名有效性后生成最终联合签名,能够抵抗中间人攻击。其次,电子发票标识由税务系统给出的唯一标识及开票方所选定的随机数组成,并在发票数据中加入时间戳后由双方签名,能够保证发票的唯一性防止重放攻击。本文方案还具有抗仿冒攻击能力,即防伪造性。此外,本文采用无证书联合签名方案,有效解决了密钥托管问题,能防止单方面密钥泄露导致的签名仿冒攻击。

3.2 协议安全仿真

本文使用协议安全仿真软件 Scyther^[18]进行协议总体安全仿真验证,基于模型改进算法,Scyther 可用于协议攻击搜索、协议角色执行模拟和安全验证。Scyther 是一种在完全密码假设下对安全协议进行形式化分析的工具,可用于发现由协议构建方式引发的问题,该工具

下设立了一系列的声明包括保密性及可信认证,如保密性 secrecy、有效性 aliveness、抗重放攻击 Niagree 及仿冒与中间人攻击 Weakagree 等^[19]。

本次仿真采用了 Dolev-Yao^[20]攻击模型,和 1.1 节中设定的安全模型一致,攻击者可以控制公开信道并在应用场景中实施一系列攻击,模型中需要验证可信性的角色为发票票面信息 M_s 及发票唯一标识符 I ,以及验证发票交易信息 M 的公开信道保密性。使用安全协议描述语言(SPDL, security protocol description language)在 Scyther 中构建第 2 节中描述协议,仿真结果如图 3 所示,发票票面信息 M_s 及唯一标识符 I 可以成功抵抗各类攻击下验证消息的有效性,并保障交易信息 M 的保密性,本文方案在 Scyther 工具仿真下未发现有效攻击。



Claim	Status	Comments
SM2Ver, I	Alive	Ok Verified No attacks.
SM2Ver, I2	Weakagree	Ok Verified No attacks.
SM2Ver, I3	Niagree	Ok Verified No attacks.
SM2Ver, I4	Nisynch	Ok Verified No attacks.
Ms SM2Ver, Ms1	Secret M	Ok Verified No attacks.
SM2Ver, Ms2	Alive	Ok Verified No attacks.
SM2Ver, Ms3	Weakagree	Ok Verified No attacks.
SM2Ver, Ms4	Niagree	Ok Verified No attacks.
SM2Ver, Ms5	Nisynch	Ok Verified No attacks.

图 3 查验协议在 Scyther 工具下的安全仿真结果
Figure 3 Formal verification results of Scyther

表 2 列举了本文方案与文献[8]中电子发票典型验证方案、文献[12]中基于数字签名的查验方案在安全功能上的对比。通过以上分析可知,本文方案在实现电子发票公开真伪性查验的基础上,同时实现交易双方隐私信息的保护,并能抵抗多种类型的协议攻击。

4 方案性能分析

4.1 计算开销分析

本节主要分析本文所提电子发票公开查验架构的计算开销。在本文方案、文献[8]中电子发票典型验证方案与文献[12]中基于数字签名的查验

方案中统一使用 SM2 数字签名/加解密算法及 SM3 杂凑函数,可对比协议整体流程计算开销。因实际电子发票场景中,服务各方所依托的设备算力具有差异,分别在 3 个计算能力不同的设备上实施 C 语言封装的 SM2 及 SM3 算法统计所消耗的时间以接近现实应用场景。设备 1 模拟税务机关电子发票服务系统 ED, CPU 参数为 Intel Xeon Gold 6240 2.60 GHz 72 核。设备 2 模拟开票方客户端 IE, CPU 参数为 Intel Xeon E5-2682 v4 2.50 GHz 2 核。设备 3 模拟查验方客户端 IR, CPU 参数为 Intel Core 2 2.40 GHz 2 核。SM2-256 及 SM3 算法计算消耗时间如表 3 所示,其中,SM2 签名及验签消耗中不包括两项 SM3 预处理时间。

表 2 本文方案与同类方案安全功能对比

Table 2 Comparison of security features between the proposed scheme and other schemes

方案	真伪 查验	隐私 保护	多方 核验	抗中间 人攻击	抗重放 攻击	抗密钥 泄露
本文方案	✓	✓	✓	✓	✓	✓
文献 ^[8] 方案	✓	×	×	×	×	×
文献 ^[12] 方案	✓	×	✓	✓	✓	×

表 3 各算法计算消耗时间

Table 3 Time consumption of each algorithm

算法	消耗时间/ μs		
	设备 1 (税务机关)	设备 2 (开票方)	设备 3 (查验方)
SM2 签名 (S)	4 900	5 920	10 620
SM2 验签 (C)	4 890	6 330	11 150
SM2 加密 (E)	6 530	8 570	14 920
SM2 解密 (D)	4 590	5 840	10 640
SM3 哈希 (H)	0.4	0.5	0.7

各方案计算消耗时间对比如表 4 所示,计算消耗对比如图 4 所示,通过引入基于 SM2 的联合签名在保障多方核验的情况下有效减少了查验方的计算消耗,考虑到查验方一般使用移动终端且查验是较为频繁的操作,本文方案能大幅提高查验服务效率,此外,在税务机关、开票方计算效率方面具有一定优势。由于各方案签名方不同,签名方计算消耗有所差异,本文方案计算消耗主要集中在计算能力较强的电子发票服务系统中,且本文方案中税务机关及开票方计算总体消耗较

其他方案低。此外,本方案使用联合签名,对同一开票方具有相同公钥签名的特征,在处理来自同一开票方(如京东等大型电商企业)的发票时可共享公共参数,有效降低计算开销,大批量同一开票方发票查验计算消耗对比如图 5 所示。综上,本文方案在提高查验效率的同时对交易双方的敏感隐私数据进行了保护和传播控制。

表 4 各方案计算消耗时间对比

Table 4 Computation time comparison of each scheme

方案	消耗时间/ μs		
	设备 1(税务机关)	设备 2(开票方)	设备 3(查验方)
本文方案	$S+C$ (9 790)	$S+E+2H$ (14 491)	$C+2H$ (11 151.4)
文献 ^[8] 方案	$2S+4H$ (9 801.6)	$2E$ (17 140)	$2C+2E+4H$ (52 142.8)
文献 ^[12] 方案	$2S+2H$ (9 800.8)	$S+C+2H$ (12 251)	$2C+4H$ (22 302.8)

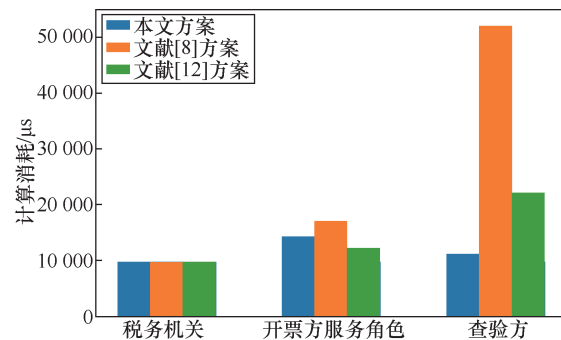


图 4 各方案计算消耗对比

Figure 4 Verification calculated consumption comparison of each scheme

4.2 电子发票数据量分析

电子发票文件需要便于存储与传输,因此电子发票的数据量大小是其重要参数。本节主要分析发票文件大小,即各方案生成的每张可查验发票所占存储数量的对比。基于本文中使用的 SM2-256 及 SM3 算法,对电子发票方案中的各参数做出以下长度定义。① SM2 签名长度 32 byte。② SM2 加密长度与明文一致(不含校验码)。③ SM3 哈希长度 32 byte。④ 身份标识、发票标识、时间戳均为 4 bytes; ⑤ 发票交易信息为 64 byte。同类型方案发票数据量对比如表 5 所示,相比其他方案,本文方案因使用联合签名精简了发票存储内容,有效降低了多方核验签名的数据量,有利于生成简洁的电子发票文件,适用于大规模电子商务交易场景。

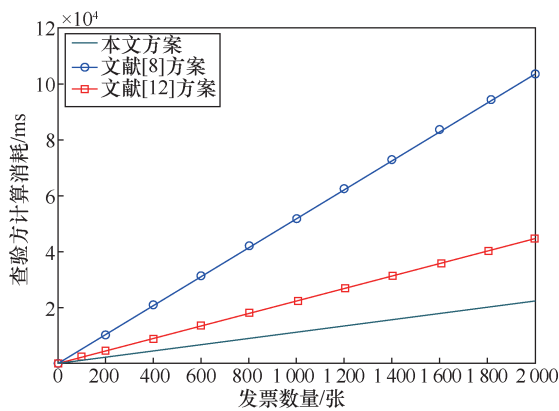


图5 大批量同一开票方发票查验计算消耗对比

Figure 5 Comparison of the consumption of large quantities of the same invoicing party invoice verification calculation

表5 同类型方案发票数据量对比

Table 5 Comparison of data bytes of related solutions

方案	发票数据	总数据/byte
本文方案	(I, N, T, SIGN, ENC, IE)	112
文献[8]方案	(I, T, M, SIGN, ENC, IE)	172
文献[12]方案	(I, T, M, SIGN, SIGN, IE)	140

5 结束语

本文针对电子发票查验问题,结合 SM2 数字签名算法,设计了基于无证书联合签名的电子发票真伪公开验证方案。本文方案充分考虑了电子发票流转频繁、交易信息敏感、易复制伪造等特点,设计了多方核验签名的电子发票查验架构,在保障公开高效查验的前提下,对发票交易信息进行传输保护,防止交易双方隐私泄露。理论及仿真分析表明,本文方案不仅保障了电子发票的多方核验生成、即时公开真伪查验、抵抗协议攻击等安全需求,还能实现用户隐私信息保护。与同类型方案相比,本文方案在提供更多安全功能及更强安全性的基础上,有效提高查验效率且具有更精简的发票结构,利于电子发票存储及传输,更适用于海量电子商务交易下的电子发票应用场景,支撑电子发票服务的推广与应用。

参考文献:

- [1] 中国互联网络信息中心. 第45次《中国互联网络发展状况统计报告》[EB]. China Internet Network Information Center. The 45th statistical report on china's internet development[EB].
- [2] 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.
- [3] TANG P, QIU W D, HUANG Z, et al. Anomaly detection in electronic invoice systems based on machine learning[J]. Information Sciences, 2020, 535:172-186.
- [4] 梁又升. 某市税务发票真伪查询系统的设计与实现[D]. 西安: 电子科技大学, 2018.
- LIANG Y S. Design and implementation of a city tax invoice authenticity query system[D]. Xi'an: University of Electronic Science and Technology of China, 2018
- [5] ILKNUR G N. Technical and communicational standards of e-invoicing: a country example: turkey[C]//IEEE International Conference on Application of Information and Communication Technologies (AICT). 2016.
- [6] 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
- [7] FERREIRA L, CONSTANTE L, BRAGA Z, et al. ISO 27001 certification process of electronic invoice in the state of minas gerais[C]//International Carnahan Conference on Security Technology. 2014.
- [8] ŠPANIĆ D, RISTIĆ D, VRDOLJAK B. An electronic invoicing system[C]//IEEE International Conference on Telecommunications. 2011: 149-156.
- [9] SUN Y, MAO X, HONG S, et al. Template matching-based method for intelligent invoice information identification[J]. IEEE Access, 2019, 7: 28392-28401.
- [10] ISO/IEC 15415:2004(E) Information technology—automatic identification and data capture techniques—bar code print quality test specification—two-dimensional symbols[S]. Switzerland: International Organization for Standardization, 2004.
- [11] 魏巍, 和红杰, 陈帆. 基于块分类编码的电子发票图像自恢复水印算法[J]. 应用科学学报, 2016, 34(5): 490-502.
- WEI W, HE H J, CHEN F. Self-recovery watermarking for e-invoice image based on block classification and RS coding[J]. Journal of Applied Sciences, 2016, 34(5): 490-502.
- [12] NGUYEN V C, PHAM H L, TRAN T H, et al. Digitizing invoice and managing VAT payment using blockchain smart contract[C]//2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). 2019.
- [13] ZHANG Y, XIE C, MA X. Blockchain for smart city-public service integration by strategic alliance[J]. International Journal of Simulation and Process Modelling, 2020, 15(4): 358-368.
- [14] UNE-EN 16931-1-2019 Electronic invoicing - part 1: semantic data model of the core elements of an electronic invoice[S]. Spain: ES-AENOR, 2019.
- [15] GB/T 32918.1-2016 信息安全技术 SM2 椭圆曲线公钥密码算法

第1部分：总则[S]. 中国：全国信息安全标准化技术委员会, 2017.
GB/T 32918.1-2016 Information security technology—public key cryptographic algorithm SM2 based on elliptic curves—part 1: general[S]. China: National Information Security Standardization Technical Committee, 2017

- [16] 程朝辉. 基于 SM2 的无证书加密算法[J]. 密码学报, 2021, 8(1): 87-95.

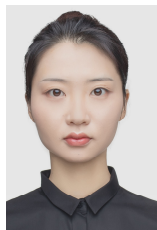
CHENG Z H. Certificateless public key encryption based on SM2[J]. Journal of Cryptologic Research, 2021, 8(1): 87-95.

- [17] GB/T 32918.2-2016 信息安全技术 SM2 椭圆曲线公钥密码算法第2部分：数字签名算法[S]. 中国：全国信息安全标准化技术委员会, 2017.

GB/T 32918.2-2016 information security technology—public key cryptographic algorithm SM2 based on elliptic curves—part 2: digital signature algorithm[S]. China: National Information Security Standardization Technical Committee, 2017.

- [18] CREMERS C. The Scyther tool[R]. University of Oxford, Department of Computer Science, 2006.
- [19] CREMERS C, MAUW S. Operational semantics and verification of security protocols[M]//Information Security and Cryptography. Berlin: Springer, 2012.
- [20] DOLEV D, YAO C C. On the security of public key protocols[C]//Symposium on Foundations of Computer Science. 1981.

[作者简介]



罗珣榕（1994-），女，江西吉安人，西安电子科技大学博士生，主要研究方向为无线网络安全、安全方案与协议设计。



曹进（1985-），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为 4G/5G 网络、天地一体化网络安全性及认证协议设计与分析。



李晖（1968-），男，河南灵宝人，博士，西安电子科技大学教授、博士生导师，主要研究方向为密码学、无线网络网络安全、云计算安全、信息论与编码理论。



赵兴文（1977-），男，广西玉林人，西安电子科技大学副教授，主要研究方向为基于机器学习的互联网安全应用、隐私保护密码协议、数字签名。



尚超（1997-），男，山东济南人，西安电子科技大学博士生，主要研究方向为智能汽车内部网络安全、认证协议设计与分析。