高效的隐私保护在线开票服务认证方案

马如慧[①] 曹 进*[①] 李 晖[①] 杨朝中[②]
[①](西安电子科技大学网络与信息安全学院 西安 710126)
[②](中国科学院国家授时中心 西安 710600)

摘 要：近年来，发票形式由传统的纸质凭据向电子凭据转变。相比于开具纸质凭据，在线开具电子凭据具有流程简化、成本降低以及便于存储等优势。但是，如何保证在线开具电子凭据服务中实体身份的合法性以及身份信息的隐私性是当前研究的重点问题。为了解决此问题，利用预共享密钥机制，该文提出一种隐私保护在线开具电子凭据的认证方案。在此方案中，合法用户与企业完成交易后可以本地在线发起开票申请，国家税务总局的电子凭据系统成功核验实体身份和交易信息后可为该用户提供电子凭据。安全和性能分析结果表明提出方案可以在耗费较少认证开销的情况下提供鲁棒的安全属性。

关键词：网络；电子凭据；认证；隐私保护
中图分类号：TN918; TP393.0 **文献标识码**：A **文章编号**：1009-5896(2022)03-1075-11
DOI: 10.11999/JEIT210049

Efficient Privacy Preserving Authentication Scheme for Online E-invoice Service

MA Ruhui[①] CAO Jin[①] LI Hui[①] YANG Chaozhong[②]
[①](*School of Cyber Engineering, Xidian University, Xi'an* 710126, *China*)
[②](*National Time Service Center, Chinese Academy of Sciences, Xi'an* 710600, *China*)

Abstract: In recent years, the form of invoice has changed from the traditional paper invoice to e-invoice. Compared with issuing paper invoice, there are the advantages of simpler process, lower cost, and easier storage for online issuing e-invoice. However, how to ensure the legitimacy of user identity and the privacy of identity information in online issuing e-invoice service is the focus issue of current research. In order to solve this issue, by using the pre- shared key mechanism, a privacy preserving authentication scheme for online issuing e-invoice is proposed. By this scheme, a legitimate user who has completed a transaction with an enterprise can initiate an e-invoice request locally and online, and the e-invoice system of the State Administration of taxation can provide the user with e-invoices after verifying the identity information and transaction information successfully. Security and performance analysis results show that the proposed scheme can provide robust security properties with less authentication overhead.

Key words: Network; E-invoice; Authentication; Privacy preserving

1 引言

随着我国科学技术的飞速发展，互联网技术的应用逐渐普及，各个领域与互联网的关系也越来越密切。我国《国民经济与社会发展第十三个五年规划纲要》明确指出“完善税收征管方式，提高税收征管效能，推行电子发票”。传统的纸质发票存在难以分发、存储、管理以及高成本等特点，不利于促进财务管理。推行电子发票凭据有利于进一步提高税务部门工作效率、降低管理成本、杜绝虚假发票、促进绿色发展[1]。

但是，在线开具电子凭据也带来了许多新的挑战。首先，电子凭据需由国家税务总局授权开具。国家税务总局应进一步完善电子凭据系统功能，提供功能全面、统一、可信的操作平台，以满足用户

收稿日期：2021-01-18；改回日期：2021-11-11；网络出版：2021-12-20
*通信作者： 曹进 caoj897@gmail.com
基金项目：国家重点研发计划(2018YFB0803900)，国家自然科学基金(61772404, U1836203)，陕西省重点研发计划(2020ZDLGY08-08)
Foundation Items: The National Key Research and Development Program of China (2018YFB0803900), The National Natural Science Foundation of China (61772404, U1836203), The Key Research and Development Program of Shaanxi Province (2020ZDLGY08-08)

通过电子凭据系统进行电子凭据开具等日常服务功能。其次，电子凭据的开具依托于互联网，需要在网络中传输大量的个人隐私信息和企业信息。如果公共传输信道被不法分子入侵，与交易有关的隐私信息将泄露[2]。因此，开具电子凭据过程中保护用户和企业的隐私至关重要。最后，为防止企业或个人虚开发票以骗取出口退税、偷税等问题，在线开具电子凭据的过程中应该认证企业和个人的合法性，保障只有合法的用户可申请开具电子凭据，且只有合法的企业才可授权用户开具电子凭据。此外，为防止恶意用户盗取他人身份申请开具电子凭据，在开具电子凭据的过程中应多方面验证申请者的身份，例如只有提供有效身份证信息且人脸检测一致的情况下，才可发起电子凭据开具申请。综上所述，研究安全可靠的隐私保护在线开具电子凭据认证方案是十分必要的。

近年来，学术界已有大量的研究者提出了电子凭据系统设计方案[3–9]，但是均未考虑在线开具电子凭据的认证安全性。学术界的研究者针对不同的应用场景已经提出了大量的认证方案。由于电子凭据的开具涉及用户、企业以及国家税务总局三方，所以主要考虑三方认证方案[10–16]。文献[10–12]针对无线传感网络分别提出了一个认证方案。这3个方案都实现了用户侧与网关的认证以及服务网络侧与网关的认证。但是，文献[10]并未实现用户匿名性、不可链路性等，文献[11]未实现不可链路性且无法抵抗用户假冒攻击等，文献[12]未实现不可链路性。文献[13,14]针对工业物联网场景提出了两个隐私保护的认证方案。这两个方案都可以实现相互认证、匿名性、不可链路性等。但是，文献[13]由于用户和服务器的身份标识易于暴露导致增加了长期密钥泄露的风险。文献[14]采用椭圆曲线密码学(Elliptic Curve Cryptography, ECC)保护用户的隐私标识，产生了较多的计算开销。文献[15]针对多个云服务器的车联网场景提出了一个隐私保护的认证方案。但是，该方案并未完美实现相互认证且耗费了大量的计算和通信开销。文献[16]针对无线医疗传感器网络提出了一个认证方案。该方案可以实现相互认证、匿名性等安全特性，但是该方案基于大整数分解困难问题加密隐私数据，产生了较多的通信开销。综上所述，现有三方认证方案存在各种安全和性能缺陷。因此，针对电子凭据在线开具场景设计安全高效的认证方案是当前亟需解决的问题。

本文针对电子凭据在线开具场景设计了一个隐私保护认证方案。在该方案中，国家税务总局管理一个电子凭据系统，申请开具电子凭据的用户和合法的企业均需注册到电子凭据系统中以获得长期共享密钥。注册完成后，与企业完成交易的用户利用长期共享密钥在电子凭据收票方手机应用(APPlication, APP)上发起开票申请，电子凭据系统验证用户身份并通过相应合法企业验证用户的交易信息，进而为用户开具电子凭据。本文的贡献总结如下：

(1) 本文提出了一个统一的电子凭据在线开票系统，该系统包括3部分：电子凭据系统、电子凭据收票方手机APP以及电子凭据开票方服务器，分别用于国家税务总局、用户以及企业完成交易后电子凭据的在线开具。

(2) 本文在电子凭据在线开票系统的基础之上提出了在线开票服务认证方案。该方案利用椭圆曲线Diffie-Hellman算法实现了用户、企业等实体在线注册过程中的隐私安全，依据身份证信息和人脸信息完成了发票开具请求前的本地验证避免恶意用户盗取他人身份申请开具电子凭据，基于预共享密钥机制分别实现了用户、企业与电子凭据系统的相互认证，并且采用对称加解密算法确保了电子凭据的安全传输等。此外，在该方案中，用户和企业的真实身份标识信息、交易信息以及发票信息等隐私内容均加密后传输，且采用及时更新的匿名标识代表用户的真实身份标识。

(3) 本文采用形式化分析工具Tamarin和非形式化安全分析证明了提出方案的安全性，结果证明本文方案可以满足相互认证、匿名性、不可链路性、数据机密性以及抵抗重放攻击和用户假冒攻击。此外，本文在计算开销和通信开销方面评估了提出方案的性能，结果显示本文方案耗费较少的通信开销和计算开销。

2 系统模型、安全需求和设计思想

2.1 系统模型

如图1所示，电子凭据开票系统主要包括3个部分：电子凭据系统，开票方以及收票方。

电子凭据系统是国家税务总局管理的在线电子凭据开具系统，主要负责为合法用户开具电子凭据，内置电子凭据开具服务器、用户认证服务器以及信息核验服务器。

(1) 电子凭据开具服务器：负责根据收票方与开票方交易的产品或服务的项目和金额等信息形成电子凭据，并反馈给收票方。

(2) 用户认证服务器：负责验证收票方的合法性，若验证成功，则向信息核验服务器反馈成功认证通知并将用户交易信息传输给信息核验服务器。若验证失败，则直接向收票方发送开票失败消息。

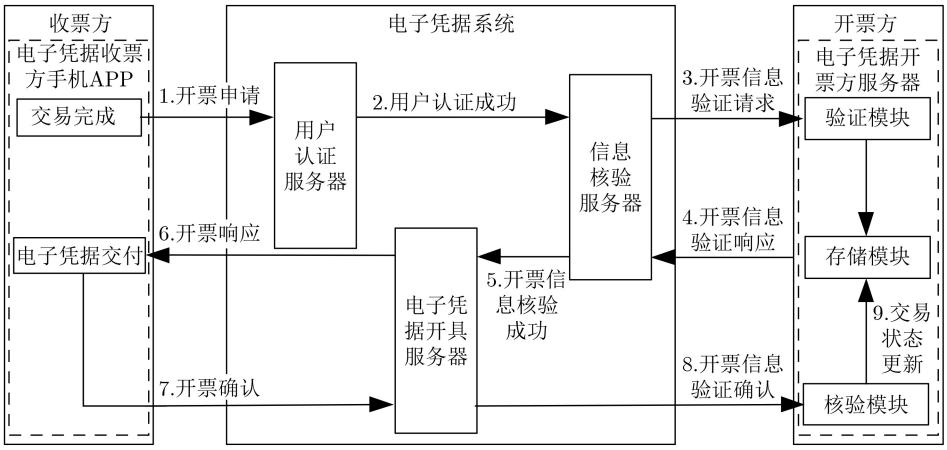

图 1 电子凭据开票系统

(3) 信息核验服务器：负责核验用户交易相关信息的正确性。若核验成功，则向电子凭据开具服务器反馈成功核验通知。若核验失败，则向收票方发送开票失败消息。

开票方是指与收票方完成在线支付交易并为收票方提供产品或者服务的企业，例如京东等。每个合法企业都需要在本地安装一个电子凭据开票方服务器，负责电子凭据交易信息的核验等。每个合法的开票方都具备一个唯一合法的企业标识。

收票方是指支付购买产品或服务的费用而收取电子凭据的个人或单位用户。每个需要开具电子凭据的收票方用户需本地下载一个电子凭据收票方手机APP，并且在该APP上完成电子凭据的申请与获取。每个合法的收票方都具备一个唯一合法的身份证。

2.2 安全需求

为防止攻击者执行假冒攻击虚开发票或提供虚假发票等问题，在线开票服务认证方案应该满足以下几个安全需求。

相互认证：收票方与电子凭据系统以及开票方与电子凭据系统间均需完成相互认证以抵抗假冒攻击以及中间人攻击等。

隐私保护：开具电子凭据过程中保护收票方与开票方的隐私是至关重要的。隐私保护主要涉及3方面内容：收票方和开票方身份标识的匿名性、不可链路性以及隐私数据的机密性。

(1) 匿名性：应防止攻击者获得收票方和开票方的真实身份标识[17]。

(2) 不可链路性：应防止攻击者通过认证过程中公开传输的消息区分出两条消息是否来自同一个收票方/开票方[17]。

(3) 数据机密性：应防止攻击者窃取收票方和开票方的隐私数据，例如交易信息、电子凭据信息等。

抵抗重放攻击：开具电子凭据过程中应防止攻击者重放之前的数据以重复开具电子凭据等问题。

2.3 设计思想

收票方用户在开票方企业提供的官方APP上成功完成货品或者服务交易之后，可在线从电子凭据系统获取此次交易的电子凭据，具体包括以下两个步骤。首先，收票方需本地下载电子凭据收票方手机APP并利用其有效身份证以及人脸信息完成注册，而开票方则需安装电子凭据开票方服务器并利用其合法的营业执照等信息完成注册。随后，收票方通过电子凭据收票方手机APP向电子凭据系统发起某次交易开票请求消息。电子凭据系统收到收票方的开票请求后，首先验证收票方的身份信息，验证成功后，通过相应的开票方企业的电子凭据开票方服务器核验该收票方此次开具电子凭据交易信息的正确性。核验成功后，电子凭据系统为收票方开具电子凭据并安全地交付给收票方。收票方验证电子凭据有效后，向电子凭据系统发送确认消息。进而，电子凭据系统向开票方发送核验确认消息，开票方记录此次交易已开具电子凭据。

3 方案设计

方案主要包括3个阶段：系统设置阶段、在线注册阶段以及开具电子凭据认证阶段。完成系统设置之后，开票方与收票方分别向电子凭据系统发起在线注册请求，电子凭据系统分别为开票方和收票方分配长期共享密钥。随后，当收票方完成交易并请求开具电子凭据时，电子凭据系统、开票方以及收票方利用各自的长期共享密钥执行开具电子凭据认证过程完成三方认证以及电子凭据的安全分发。

3.1 系统设置阶段

电子凭据系统执行如下操作：

(1) 选择主密钥K_e，选取一个椭圆曲线E上的

循环群G，其中G的阶为q，生成元为P，选取私钥$\mathrm{sk} \in Z_q^*$，公钥$\mathrm{pk}=\mathrm{sk}\cdot P$。

(2) 选择两个安全的哈希函数h_1,h_2，一个带密钥的哈希函数f_1以及一个密钥导出函数KDF。

(3) 根据公安部身份验证系统所需的身份证信息与人脸信息的绑定关系，选择一个bind函数。bind函数一般为哈希函数，不会泄露输入信息。

(4) 选择对称加密算法ENC和解密算法DEC以及模糊提取生成算法Gen和再生算法Rep。模糊提取算法的详细内容可参考文献[18,19]。

(5) 公开$(q, P, \mathrm{pk}, h_1, h_2, f_1, \mathrm{KDF}, \mathrm{bind}, \mathrm{ENC}, \mathrm{DEC}, \mathrm{Gen}, \mathrm{Rep})$。表1列出了本文用到的主要符号及定义。

3.2 在线注册阶段

由于电子凭据收票方手机APP和电子凭据开票方服务器与电子凭据系统之间都是通过网络连接，所以本文考虑在线注册。

3.2.1 收票方在线注册阶段

收票方i将其身份证标识等内容安全地传输给电子凭据系统。电子凭据系统验证内容的有效性后，为收票方提供长期共享密钥。具体如下：

(1) 电子凭据收票方手机APP首先需要本地验证收票方用户提供的身份证照片与活体人脸采集照片的一致性，如果一致，则根据用户提供的人脸信息B_i计算人脸信息相关字符串$(\alpha_i, \beta_i)=\mathrm{Gen}(B_i)$，然后导出身份证信息$\mathrm{eID}_i$与人脸信息字符串$\alpha_i$的绑定关系$A_i=\mathrm{bind}(\mathrm{eID}_i, \alpha_i)$。随后，选择两个随机数$r_i \in Z_q^*$和$h_i \in Z_q^*$，计算哈希值$H_i=h_1(\mathrm{eID}_i, \alpha_i, h_i)$，ECC临时公钥$R_i=r_i\cdot P$，共享值$Z_i=r_i\cdot \mathrm{pk}$，临时共享密钥$\mathrm{MLK}_i=h_2(Z_i, t_{i0})=\mathrm{MK}_i||\mathrm{LK}_i$，密文$c_i=\mathrm{ENC}_{\mathrm{MK}_i}(\mathrm{eID}_i||A_i||H_i)$，消息认证码$s_i=f_1(\mathrm{LK}_i, c_i||R_i||t_{i0})$，其中$\mathrm{MK}_i$和$\mathrm{LK}_i$分别代表注册过程中收票方的临时加密密钥和完整性密钥，t_{i0}为当前时间戳。随后，电子凭据收票方手机APP将注册请求消息(c_i, s_i, R_i, t_{i0})发送给电子凭据系统。

(2) 电子凭据系统收到后，首先检验时间戳t_{i0}的有效性，如果有效，计算共享值$Z_i'=R_i\cdot \mathrm{sk}$，临时共享密钥$\mathrm{MLK}_i'=h_2(Z_i', t_{i0})=\mathrm{MK}_i'||\mathrm{LK}_i'$，并且验证$s_i=f_1(\mathrm{LK}_i', \mathrm{c}_i||R_i||t_{i0})$，验证成功后解密获得$\mathrm{eID}_i'||\ A_i'||H_i'=\mathrm{DEC}_{\mathrm{MK}_i'}(c_i)$，并将$\mathrm{eID}_i'||A_i'$安全地发送给第三方公安部身份验证系统，核实用户身份信息。核实成功后，电子凭据系统选择一个随机数b_i，计算收票方的长期共享密钥$K_i=\mathrm{KDF}(K_\mathrm{e}, \mathrm{eID}_i')$，隐藏密钥值$\mathrm{HK}_i=K_i\oplus h_1(\mathrm{eID}_i', H_i', A_i')$，收票方本地验证值$F_i=h_1(\mathrm{eID}_i', H_i')$，匿名身份标识$\mathrm{HID}_i=\mathrm{eID}_i'\oplus h_1(b_i||K_\mathrm{e})$，隐藏随机数$\mathrm{Hb}_i=b_i\oplus h_1(\mathrm{HID}_i, K_\mathrm{e})$。最后电子凭据系统计算密文$c_{\mathrm{ei}}=\mathrm{ENC}_{\mathrm{MK}_i'}(\mathrm{HK}_i||\mathrm{Hb}_i||F_i||\ \mathrm{HID}_i)$，消息认证码$s_{\mathrm{ei}}=f_1(\mathrm{LK}_i', c_{\mathrm{ei}}||\mathrm{eID}_i'||A_i'||t_{i0})$并将注册响应$(c_{\mathrm{ei}}, s_{\mathrm{ei}})$传输给电子凭据收票方手机APP。

(3) 电子凭据收票方手机APP收到消息后，首先验证$s_{\mathrm{ei}}=f_1(\mathrm{LK}_i, c_{\mathrm{ei}}||\mathrm{eID}_i||A_i||t_{i0})$，验证成功后解密$c_{\mathrm{ei}}$，计算隐藏随机数$\mathrm{Hh}_i=h_i\oplus h_1(\mathrm{eID}_i, A_i)$，并且存储$(\mathrm{HK}_i, \mathrm{Hh}_i, \mathrm{Hb}_i, F_i, \mathrm{HID}_i, \beta_i)$。

3.2.2 开票方在线注册阶段

电子凭据开票方服务器j将开票方企业的标识信息等内容安全传输给电子凭据系统。电子凭据系统验证成功后，为开票方提供长期密钥。具体如下：

(1) 企业法人将开票方企业的标识信息sID_j以及营业执照、法人身份证等信息M_j输入电子凭据开票方服务器。电子凭据开票方服务器选择一个随机数$r_j \in Z_q^*$，计算ECC临时公钥$R_j=r_j\cdot P$，共享值$Z_j=r_j\cdot \mathrm{pk}$，临时共享密钥$\mathrm{MLK}_j=h_2(Z_j, t_{j0})=\mathrm{MK}_j||\mathrm{LK}_j$，密文$c_j=\mathrm{ENC}_{\mathrm{MK}_j}(\mathrm{sID}_j||M_j)$以及消息认证码$s_j=f_1(\mathrm{LK}_j, \mathrm{c}_j||R_j||t_{j0})$，其中

表 1 符号定义

符号	定义	符号	定义
q/Z_q^*	大素数/模q的正整数集合	M_j/m_j	开票方的企业信息/开票方存储的订单交易信息
E/G	椭圆曲线E上的循环群G	h_1/h_2	$(0,1)^*\to(0,1)^l/(0,1)^*\to(0,1)^k$
P	循环群G的生成元	f_1	$(0,1)^*\xrightarrow{\text{key}}(0,1)^l$
K_e	电子凭据系统主密钥	bind	身份证信息与人脸信息的绑定函数
sk/pk	电子凭据系统私钥/公钥	KDF	$(0,1)^*\to(0,1)^l$
$\mathrm{eID}_i/\mathrm{HID}_i$	收票方用户i的身份证信息/匿名身份标识信息	ENC/DEC	对称加密/解密函数
K_i/B_i	收票方用户i的长期共享密钥/人脸信息	Gen/Rep	模糊提取生成/再生函数
α_i/β_i	人脸信息相关的随机字符串/辅助字符串	$\|\|$	连接符
sID_j/K_j	开票方j的企业标识/长期共享密钥	$\oplus$	异或操作
$t_{i0}/t_{j0}/t_i/t_{ej}/t_j$	时间戳	$\cdot$	椭圆曲线上的点乘操作
$M_i/m_i/M_e$	收票方的订单交易信息/订单编号信息/电子凭据信息		

MK_j和LK_j分别代表注册过程中开票方的临时加密密钥和完整性密钥，t_{j0}为当前时间戳。最后，电子凭据开票方服务器将注册请求消息(c_j, s_j, R_j, t_{j0})发送给电子凭据系统。

(2) 电子凭据系统收到消息后，首先检验时间戳t_{j0}的有效性，如果有效，则计算共享值$Z_j' = R_j \cdot \mathrm{sk}$，临时共享密钥$\mathrm{MLK}_j' = h_2(Z_j', t_{j0}) = \mathrm{MK}_j'||\mathrm{LK}_j'$，验证$s_j = f_1(\mathrm{LK}_j', c_j||R_j||t_{j0})$，验证成功后，解密$\mathrm{sID}_j'||M_j' = \mathrm{DEC}_{\mathrm{MK}_j'}(c_j)$并核实$\mathrm{sID}_j'||M_j'$的合法性，如果合法则计算开票方$j$的长期共享密钥$K_j = \mathrm{KDF}(K_\mathrm{e}, \mathrm{sID}_j')$，密文$c_\mathrm{ej} = \mathrm{ENC}_{\mathrm{MK}_j'}(K_j)$以及消息认证码$s_\mathrm{ej} = f_1(\mathrm{LK}_j', c_\mathrm{ej}||\mathrm{sID}_j'||M_j'||t_{j0})$。最后，电子凭据系统将注册响应消息$(c_\mathrm{ej}, s_\mathrm{ej})$发送给电子凭据开票方服务器。

(3) 电子凭据开票方服务器验证s_ej，验证成功后解密c_ej获得K_j，并且本地安全存储K_j。

3.3 开具电子凭据认证阶段

交易完成后收票方i在其已注册的电子凭据收票方手机APP上发起开票申请。电子凭据系统验证收票方的合法性并通过相应开票方j核验交易信息的正确性并为收票方提供电子凭据。具体如下：

(1) 用户i在其电子凭据收票方手机APP上录入身份证正反面信息eID_i以及人脸信息B_i。电子凭据收票方手机APP首先需要本地验证收票方用户提供的身份证照片与活体人脸采集照片的一致性。如果一致，电子凭据收票方手机APP计算人脸信息相关的字符串$\alpha_i = \mathrm{Rep}(B_i, \beta_i)$，$A_i = \mathrm{bind}(\mathrm{eID}_i, \alpha_i)$，$h_i = \mathrm{Hh}_i \oplus h_1(\mathrm{eID}_i, A_i)$，$H_i = h_1(\mathrm{eID}_i, \alpha_i, h_i)$，并验证$h_1(\mathrm{eID}_i, H_i)$与其数据库中存储的$F_i$是否一致。如果一致，则计算长期共享密钥$K_i = \mathrm{HK}_i \oplus h_1(\mathrm{eID}_i, H_i, A_i)$，临时共享密钥$\mathrm{TK}_i = h_2(K_i, t_i) = \mathrm{TMK}_i||\mathrm{TLK}_i$，进而计算密文$C_i = \mathrm{ENC}_{\mathrm{TMK}_i}(\mathrm{sID}_j||M_i)$，消息认证码$S_i = f_1(\mathrm{TLK}_i, C_i||\mathrm{eID}_i||t_i)$，其中$\mathrm{TMK}_i$和$\mathrm{TLK}_i$分别代表认证过程中收票方的临时加密密钥和完整性密钥，M_i代表开具电子凭据交易相关的信息，例如订单编号、金额、纳税人识别号等信息，sID_j代表交易的企业方标识，t_i是当前时间戳。最后，电子凭据收票方手机APP将开票请求消息$(\mathrm{HID}_i, \mathrm{Hb}_i, C_i, S_i, t_i)$发送给电子凭据系统。

(2) 电子凭据系统收到开票请求消息后，首先验证时间戳t_i的有效性。如果有效，电子凭据系统计算$b_i' = \mathrm{Hb}_i \oplus h_1(\mathrm{HID}_i, K_\mathrm{e})$，导出收票方真实身份标识$\mathrm{eID}_i' = \mathrm{HID}_i \oplus h_1(b_i'||K_\mathrm{e})$，长期共享密钥$K_i' = \mathrm{KDF}(K_\mathrm{e}, \mathrm{eID}_i')$，进而导出临时共享密钥$\mathrm{TK}_i' = h_2(K_i', t_i) = \mathrm{TMK}_i'||\mathrm{TLK}_i'$。随后，验证$S_i = f_1(\mathrm{TLK}_i', C_i||\mathrm{eID}_i'||t_i)$，验证成功后，解密$\mathrm{sID}_j'||M_i' = \mathrm{DEC}_{\mathrm{TMK}_i'}(C_i)$获得相应开票方标识$\mathrm{sID}_j'$以及交易信息$M_i'$，然后计算出开票方的长期共享密钥$K_j = \mathrm{KDF}(K_\mathrm{e}, \mathrm{sID}_j')$，进而导出与开票方的临时共享密钥$\mathrm{TK}_j = h_2(K_j, t_\mathrm{ej}) = \mathrm{TMK}_j||\mathrm{TLK}_j$，其中$\mathrm{TMK}_j$和$\mathrm{TLK}_j$分别代表认证过程中开票方的临时加密密钥和完整性密钥，t_ej为当前系统时间戳。最后，计算密文$C_\mathrm{ej} = \mathrm{ENC}_{\mathrm{TMK}_j}(\mathrm{eID}_i'||m_i)$，消息认证码$S_\mathrm{ej} = f_1(\mathrm{TLK}_j, C_\mathrm{ej}||\ \mathrm{sID}_j'||t_\mathrm{ej})$并将开票信息核验请求消息$(C_\mathrm{ej}, S_\mathrm{ej}, t_\mathrm{ej})$发送给对应的开票方，其中$m_i$是从$M_i'$中提取出的订单编号信息。

(3) 开票方j的电子凭据开票方服务器收到消息后，计算临时共享密钥$\mathrm{TK}_j' = h_2(K_j, t_\mathrm{ej}) = \mathrm{TMK}_j'||\mathrm{TLK}_j'$，验证$S_\mathrm{ej} = f_1(\mathrm{TLK}_j', C_\mathrm{ej}||\mathrm{sID}_j||t_\mathrm{ej})$，验证成功后，计算$\mathrm{eID}_i''||m_i' = \mathrm{DEC}_{\mathrm{TMK}_j'}(C_\mathrm{ej})$。随后，电子凭据开票方服务器根据收票方标识$\mathrm{eID}_i''$以及订单编号信息$m_i'$在本地数据库中查找订单交易信息$m_j$并计算密文$C_j = \mathrm{ENC}_{\mathrm{TMK}_j'}(m_j)$，消息认证码$S_j = f_1(\mathrm{TLK}_j', C_j||\mathrm{eID}_i''||m_i'||t_j)$，并且将开票信息核验响应消息$(C_j, S_j, t_j)$发送给电子凭据系统，其中$t_j$为当前系统时间戳。

(4) 电子凭据系统收到后，首先核验t_j和$S_j = f_1(\mathrm{TLK}_j, C_j||\mathrm{eID}_i'||m_i||t_j)$的有效性，核验成功后，解密获得$m_j' = \mathrm{DEC}_{\mathrm{TMK}_j}(C_j)$并判断收票方提供的$M_i'$以及开票方提供的$m_j'$是否一致，如果一致则根据交易商品或服务项目和金额等信息形成电子凭据M_e。此外，为保证用户开具电子凭据的隐私性，电子凭据系统选择一个随机数$b_i{}^*$，计算新的匿名身份标识$\mathrm{HID}_i{}^* = \mathrm{eID}_i' \oplus h_1(b_i{}^*||K_\mathrm{e})$以及隐藏随机数$\mathrm{Hb}_i{}^* = b_i{}^* \oplus h_1(\mathrm{HID}_i{}^*, K_\mathrm{e})$。然后，电子凭据系统计算密文$C_\mathrm{ei} = \mathrm{ENC}_{\mathrm{TMK}_i'}(M_\mathrm{e}||\mathrm{HID}_i{}^*||\mathrm{Hb}_i{}^*)$以及消息认证码$S_\mathrm{ei} = f_1(\mathrm{TLK}_i', C_\mathrm{ei}||\mathrm{eID}_i'||M_i')$并将开票响应消息$(C_\mathrm{ei}, S_\mathrm{ei})$传输给电子凭据收票方手机APP。

(5) 收票方i的电子凭据收票方手机APP验证$S_\mathrm{ei} = f_1(\mathrm{TLK}_i, C_\mathrm{ei}||\mathrm{eID}_i||\mathrm{M}_i)$，验证成功后，解密获得电子凭据以及新的匿名身份标识$M_\mathrm{e}'||\mathrm{HID}_i{}^{*'}||\mathrm{Hb}_i{}^{*'} = \mathrm{DEC}_{\mathrm{TMK}_i}(C_\mathrm{ei})$，计算消息认证码$R_i = f_1(\mathrm{TLK}_i, \mathrm{eID}_i||\mathrm{sID}_j||M_i||\mathrm{succ})$并将开票确认消息$(R_i)$发送给电子凭据系统，其中succ代表开票成功标识。

(6) 电子凭据系统验证R_i，验证成功则记录此次开具操作，计算消息认证码$R_\mathrm{e} = f_1(\mathrm{TLK}_j, \mathrm{eID}_i'||\mathrm{sID}_j'||m_i||\mathrm{succ})$并将开票信息核验确认消息$(R_\mathrm{e})$发送给开票方；验证失败则记录已开具电子凭据$M_\mathrm{e}$无效。

(7) 开票方j的电子凭据开票方服务器验证R_e，验证成功后在其存储模块中记录此次交易已经开具发票。

4 安全分析

4.1 非形式化安全分析

相互认证。在注册过程中，电子凭据系统通过验证收票方提供的身份标识等信息以及开票方提供的营业执照等信息分别认证收票方与开票方。此外，由于收票方与开票方都采用了电子凭据系统的公钥加密隐私数据后传输给电子凭据系统，所以只有电子凭据系统可以获得收票方与开票方提供的隐私信息，进而产生有效的消息认证码s_{ei}和s_{ej}。因此，收票方与开票方可分别通过验证电子凭据系统返回的s_{ei}和s_{ej}认证电子凭据系统。在认证过程中，收票方、开票方和电子凭据系统之间分别共享临时密钥$\mathrm{TK}_i,\mathrm{TK}_j$，进而可利用$\mathrm{TK}_i/\mathrm{TK}_j$导出消息认证码$S_i/S_{\mathrm{ei}}/S_j/S_{\mathrm{ej}}$。电子凭据系统可通过核验$S_i$和$S_j$分别认证收票方与开票方。收票方可通过核验$S_{\mathrm{ei}}$认证电子凭据系统，而开票方可通过核验$S_{\mathrm{ej}}$认证电子凭据系统。因此，本文的方案可以实现收票方与电子凭据系统以及开票方与电子凭据系统之间的相互认证。

匿名性。在注册过程中，收票方/开票方的身份标识信息$\mathrm{eID}_i/\mathrm{sID}_j$采用临时密钥$\mathrm{MK}_i/\mathrm{MK}_j$加密后传输给电子凭据系统。只有电子凭据系统可以计算出$\mathrm{MK}_i/\mathrm{MK}_j$进而导出收票方/开票方的真实身份标识。在认证过程中，采用匿名身份标识HID_i代表收票方且每次认证完成后均会更新HID_i，只有电子凭据系统可以根据其主密钥K_{e}从HID_i中导出收票方的真实身份标识eID_i。任何不知道主密钥K_{e}的攻击者是无法获得收票方的真实身份标识。此外，收票方/开票方的真实身份标识$\mathrm{eID}_i/\mathrm{sID}_j$均采用临时加密密钥$\mathrm{TMK}_j/\mathrm{TMK}_i$加密后传输，攻击者没有解密密钥不可能获得。因此，本方案可以实现匿名性。

不可链路性。在注册过程中，由于随机数r_i/r_j以及时间戳t_{i0}/t_{j0}的使用，消息随机变化，攻击者无法推断出两条公开传输的消息是否来自同一个发送者。在认证过程中，由于每个开具电子凭据的认证过程都需更新匿名身份标识HID_i且更新过程中采用随机数b_i^*来计算新的匿名标识，攻击者不可能将匿名身份标识与某特定的收票方关联。此外由于时间戳t_i/t_j的使用，收票方、开票方以及电子凭据认证系统在每个会话中使用的临时密钥$\mathrm{TK}_i/\mathrm{TK}_j$都不相同，进而每个会话中产生的消息$(\mathrm{HID}_i,\mathrm{Hb}_i,C_i,S_i,t_i)/(C_j,S_j,t_j)/(C_{\mathrm{ei}},S_{\mathrm{ei}})/(C_{\mathrm{ej}},S_{\mathrm{ej}},t_{\mathrm{ej}})$各不相同，攻击者无法将不同的消息链路到同一个发送者。因此本方案可实现不可链路性。

数据机密性。在注册过程中，收票方的身份信息eID_i和开票方的企业信息sID_j, M_j等隐私数据均采用临时共享密钥$\mathrm{MK}_i/\mathrm{MK}_j$加密后传输，攻击者没有相应的密钥，不可能获得隐私数据。在认证过程中，收票方的交易信息M_i，订单编号信息m_i，企业侧存储的订单交易信息m_j以及电子凭据信息M_{e}均采用临时密钥$\mathrm{TMK}_i/\mathrm{TMK}_j$加密后传输，攻击者没有相应的密钥，不可能获得隐私数据。因此本方案可确保数据机密性。

抵抗重放攻击。由于随机数r_i/r_j，时间戳t_{i0}/t_{j0}以及$t_i/t_{\mathrm{ej}}/t_j$的使用，本文的方案可以抵抗重放攻击。

抵抗用户假冒攻击。在注册过程中，电子凭据收票方手机APP会检测身份证照片信息与活体人脸采集信息的一致性，如果一致才会允许收票方发起注册。其次，电子凭据系统会借助第三方公安部身份验证系统识别用户身份信息的有效性，识别成功后，才会给电子凭据收票方手机APP预置长期共享密钥。然后，在认证过程中，只有收票方给电子凭据收票方手机APP提供特定有效的身份证信息和人脸信息，收票方才能通过验证并发起开票请求。因此，本方案可以抵抗用户假冒攻击。

4.2 形式化验证工具：Tamarin

本小节采用形式化验证工具Tamarin[20]证明了本文提出方案的安全性。Tamarin是当前主流的协议形式化分析工具，可以建立无限验证、可变全局状态、归纳和循环引用，内置Diffie-Hellman幂指数运算、XOR运算、对称加密以及解密运算等操作[21]。Tamarin内置Dolev-Yao敌手模型，即敌手对通信网络有绝对控制权，可以窃听、删除、插入、修改和拦截公共信道上的消息。Tamarin工具是基于硬件工作过程的模拟，将协议流程采用多集重写规则rule模型化，而协议的安全目标则采用lemma描述。Tamarin工具能够自动输出lemma验证结果，即如果某lemma满足，输出verified；如果某lemma不满足，则输出falsified并给出反例，以便设计者能够快速发现协议安全漏洞并对协议进行修改。在Tamarin模型化过程中，Fr($\sim x$)代表选择新值x，\$代表公开，All代表全局量化，Ex代表存在量化，= = >代表推出，#代表时间戳前缀，而$F@\#i$代表事件F发生在时间点i。我们在Linux平台下搭建了Tamarin仿真测试模型，在本方案的Tamarin模型中，主要有3个实体User, Enterprise以及System，分别代表方案中的收票方、开票方以及电子凭据系统。具体过程如下：

(1) Tamarin初始配置过程为：

由于提出方案中仅采用了一些简单的哈希、对称加密以及异或等操作，因此初始配置过程本文采用Tamarin内置的hashing, symmetric-encryption以及xor函数。具体设置为：

theory authentication
begin
builtins:hashing,symmetric-encryption,xor

(2) 协议过程采用多个重写规则模型化为：

(a)由于Tamarin处理资源有限，本文直接采用规则Setup表示注册过程，即分别向收票方、开票方以及电子凭据系统预置认证密钥相关内容。具体为：

rule Setup:
let
HIDi=~eIDi XOR h(<~bi,~Ke>)
Hbi=~bi XOR h(<HIDi,~Ke>)
Ki=h(<~Ke,~eIDi,~bi>)
Kj=h(<~Ke, ~sIDj>)
in[Fr(~Ke), Fr(~eIDi), Fr(~bi), Fr(~sIDj)]--[Setup()]->[SystemUinit($User, ~Ke), SystemEinit($System, ~Ke), Userinit($User, ~eIDi, Ki, HIDi, Hbi, ~sIDj), Enterpriseinit($System, ~sIDj, Kj)]

(b) 收票方在开具电子凭据认证过程中的操作采用两个重写规则User1和User2模型化，其中规则User1表示收票方向电子凭据系统发送开票请求消息的过程，而规则User2表示收票方接收到开票响应消息并发送开票确认消息的过程。具体为：

rule User1:
let
TKi=h(<Ki,~ti>)
Ci1=senc(~sIDj,TKi)
Ci2=senc(~Mi,TKi)
Si=h(<TKi,Ci1,Ci2,~eIDi,~ti>)
in[Userinit($User,~eIDi,Ki,HIDi,Hbi,~sIDj),Fr(~ti),Fr(~Mi)]--[SendRequest($User,Si)]->[Userstore($User,TKi,~sIDj,~eIDi,~Mi),Out(<HIDi,Hbi,Ci1,Ci2,Si,~ti>)]

rule User2:
let
se1=h(<TKi, ce, eIDi,Mi>)
Me=sdec(ce, TKi)
Ri=h(<TKi, eIDi, ~sIDj,Mi>)
in[Userstore($User, TKi, ~sIDj, eIDi, Mi), In(<ce, se>)]--[Eq(se, se1), SecretMsg(Mi), SecretMsg(Me), RecvResponse($User, se1), SendConfirm($User, Ri)]->[Out(<Ri>)]

(c) 电子凭据系统在开具电子凭据认证过程中的操作采用4个重写规则System1, System2, System3以及System4模型化，其中，规则System1表示电子凭据系统收到收票方发送的开票请求消息并向开票方发送开票信息核验请求消息的过程，规则System2表示电子凭据系统收到开票方发送的开票信息核验响应消息之后的验证过程，规则System3表示电子凭据系统向收票方发送开票响应消息的过程，规则System4表示电子凭据系统收到开票确认消息之后的验证过程。具体为：

rule System1:
let
bi=Hbi XOR h(<HIDi,Ke>)
eIDi=HIDi XOR h(<bi,Ke>)
Ki=h(<Ke,eIDi,bi>)
TKi=h(<Ki,ti>)
Si1=h(<TKi,Ci1,Ci2,eIDi,ti>)
sIDj=sdec(Ci1,TKi)
Mi=sdec(Ci2,TKi)
Kj=h(<Ke,sIDj>)
TKj=h(<Kj,~te>)
Ce=senc(~mi,TKj)
Se=h(<TKj,Ce,sIDj,~te>)
in[SystemUinit($User,Ke),SystemEinit($System,Ke),In(<HIDi,Hbi,Ci1,Ci2,Si,ti>),Fr(~te),Fr(~mi)]
--[Eq(Si1, Si), RecvRequest($User, Si), SendVerifyRequest($System, Se)]->[SystemEstore($System, TKj, ~mi), SystemUstore($User, TKi, sIDj, eIDi, Mi), Out(<Ce, Se, ~te>)]

rule System2:
let
mj=sdec(Cj,TKj)
Sj1=h(<TKj,Cj,mi,tj>)
in[SystemEstore($System,TKj,mi),In(<Cj,Sj,tj>)]--[Eq(Sj1,Sj),SecretMsg(mj),SecretMsg(mi),RecvVerifyResponse($System,Sj1)]->[]

rule System3:
let
ce=senc(~Me,TKi)
se=h(<TKi,ce,eIDi,Mi>)
Ri1=h(<TKi,eIDi,sIDj,Mi>)
in[SystemUstore($User,TKi,sIDj,eIDi,Mi),Fr(~Me)]--[SendResponse($User,se)]->[Systemstore3($User,Ri1),Out(<ce,se>)]

rule System4:
[Systemstore3($User,Ri1),In(<Ri>)]--[Eq(Ri,Ri1),RecvConfirm($User,Ri1)]->[]

(d) 开票方在开具电子凭据认证过程中的操作

采用两个重写规则Enterprise1和Enterprise2模型化，其中Enterprise1表示开票方收到开票信息核验请求消息之后的验证过程，Enterprise2表示开票方向电子凭据系统发送开票信息核验响应消息的过程。具体为：

rule Enterprise1:

let

TKj=h(<Kj,te>)

Se1=h(<TKj,Ce,sIDj,te>)

mi=sdec(Ce,TKj)

in[Enterpriseinit($System,sIDj,Kj),In(<Ce,Se,te>)]--[Eq(Se,Se1),RecvVerifyRequest($System,Se1)]->[Enterprise1store($System,sIDj,TKj,mi)]

rule Enterprise2:

let

Cj=senc(~mj,TKj)

Sj=h(<TKj,Cj,mi,~tj>)

in[Enterprise1store($System,sIDj,TKj,mi),Fr(~mj),Fr(~tj)]--[SendVerifyResponse($System,Sj)]->[Out(<Cj,Sj,~tj>)]

(3)协议安全目标采用lemma定义为：

在定义lemma之前，本文定义了两个等式限制restriction，其中restriction Equality代表Eq追踪的两个值必须相同，restriction OneSetup代表Setup行为唯一。

restriction Equality: "All xy #i. Eq(x,y) @i ==> $x = y$"

restriction OneSetup: "All #i #j. Setup() @i & Setup() @j ==> #i = #j "

本文定义了多个all-traces类型的lemma证明了方案的安全特性。具体地，SystemAuthUser涉及电子凭据系统对收票方的认证。为了实现该属性，我们在规则User1中标记了SendRequest($User, Si)行为，且在规则System1中标记了Eq(Si1, Si)以及RecvRequest($User, Si)行为。若RecvRequest($User, Si)行为发生则表明电子凭据系统已成功核验消息认证码。而当RecvRequest($User, Si)行为发生时，SendRequest($User, Si)行为一定已经发生过且RecvRequest($User, Si)行为只发生了1次，则表明电子凭据已成功认证收票方。同理，EnterpriseAuthSystem涉及开票方对电子凭据系统的认证，SystemAuthEnterprise涉及电子凭据系统对开票方的认证，userAuthSystem涉及收票方对电子凭据系统的认证，SystemAuthUser2再次涉及电子凭据系统对收票方的认证。此外，本文采用Secrecy-Message定义方案中隐私数据M_i, m_i, M_e以及m_j的机密性。具体定义为：

lemma SystemAuthUser:

"(All entity m #i. RecvRequest(entity, m) @ #i==>/* Whenever the RecvRequest(entity, m) action occurs, */

((Ex #a. SendRequest(entity, m) @ a & a<i)/* there is an entity that has sent the request */

&(All #j. RecvRequest(entity, m) @ #j ==> #i = #j)))" /*no other has the same action*/

lemma EnterpriseAuthSystem:

"(All entity m #i. RecvVerifyRequest(entity, m) @ #i==> /* Whenever the RecvVerifyRequest(entity, m) action occurs, */

((Ex #a. SendVerifyRequest(entity, m) @ a & a<i)/* there is an entity that has sent the request */

&(All #j. RecvVerifyRequest(entity, m) @ #j ==> #i = #j)))" /*no other has the same action*/

lemma SystemAuthEnterprise:

"(All entity m #i. RecvVerifyResponse(entity, m) @ #i==> /* Whenever the RecvVerifyResponse(entity, m) action occurs, */

((Ex #a. SendVerifyResponse(entity, m) @ a & a<i)/* there is an entity that has sent the request */

&(All #j. RecvVerifyResponse(entity, m) @ #j ==> #i = #j)))" /*no other has the same action*/

lemma userAuthSystem:

"(All entity m #i. RecvResponse(entity, m) @ #i==> /* Whenever the RecvResponse(entity, m) action occurs, */

((Ex #a. SendResponse(entity, m) @ a & a<i)/* there is an entity that has sent the request */

&(All #j. RecvResponse(entity, m) @ #j ==> #i = #j)))" /*no other has the same action*/

lemma SystemAuthUser2:

"(All entity m #i. RecvConfirm(entity, m) @ #i==> /* Whenever the RecvConfirm(entity, m) action occurs, */

((Ex #a. SendConfirm(entity, m) @ a & a<i)/* there is an entity that has sent the request */

&(All #j. RecvConfirm(entity, m) @ #j ==> #i = #j)))"/*no other has the same action*/

lemma SecrecyMessage: "All n #i. SecretMsg(n) @i ==>(not (Ex #j. K(n) @j))"/* no attacker knowns n */

此外，为防止协议空跑导致验证结果假性verified，本文定义了5个exists-trace类型的lemma：ExecutableRequest, ExecutableVerifyRequest, ExecutableVerifyResponse, ExecutableResponse以及ExecutableConfirm。具体定义为：

lemma ExecutableRequest: exists-trace "Ex entity m #i #j. SendRequest(entity,m)@i & RecvRequest(entity,m)@j"

lemma ExecutableVerifyRequest: exists-trace "Ex entity m #i #j. SendVerifyRequest(entity,m)@i & RecvVerifyRequest(entity,m)@j"

lemma ExecutableVerifyResponse: exists-trace "Ex entity m #i #j. SendVerifyResponse(entity, m)@i & RecvVerifyResponse(entity,m)@j"

lemma ExecutableResponse: exists-trace "Ex entity m #i #j. SendResponse(entity,m)@i & RecvResponse(entity,m)@j"

lemma ExecutableConfirm: exists-trace "Ex entity m #i #j. SendConfirm(entity,m)@i & RecvConfirm(entity,m)@j"

end

(4)协议过程模型化结束且协议安全目标定义完成之后，执行命令tamarin-prover authentication.spthy --prove输出验证结果。

本方案Tamarin工具验证结果如图2所示，结果证明Tamarin模型中定义的所有lemma均已成功验证，即本方案可以实现收票方与电子凭据系统之间的相互认证、开票方与电子凭据系统之间的相互认证以及收票方与开票方隐私数据的机密性。

```
==========================================================
summary of summaries:

analyzed: authentication.spthy

  SystemAuthUser (all-traces): verified (18 steps)
  EnterpriseAuthSystem (all-traces): verified (27 steps)
  SystemAuthEnterprise (all-traces): verified (115 steps)
  userAuthSystem (all-traces): verified (44 steps)
  SystemAuthUser2 (all-traces): verified (26 steps)
  SecrecyMessage (all-traces): verified (319 steps)
  ExecutableRequest (exists-trace): verified (20 steps)
  ExecutableVerifyRequest (exists-trace): verified (23 steps)
  ExecutableVerifyResponse (exists-trace): verified (26 steps)
  ExecutableResponse (exists-trace): verified (22 steps)
  ExecutableConfirm (exists-trace): verified (23 steps)

==========================================================
```

图 2 Tamarin验证结果

5　性能分析

本节评估了本文所提方案与其他认证流程较为相似的方案[13,14,16]的计算开销和通信开销。

5.1　计算开销

本小节对比了所提方案与其他方案[13,14,16]在认证过程中的计算开销。本文仅考虑耗时较多的密码学操作，具体包括点乘操作T_{p}、模平方操作T_{e}、中国剩余定理求解操作T_{crt}、切比雪夫多项式操作T_{c}、模糊提取操作T_{r}、对称加解密操作T_{s}以及哈希操作T_{h}。本文方案中采用的h_1, h_2, f_1以及KDF等函数操作均采用T_{h}标识。根据文献[22,23]可得上述密码学操作计算时间为T_{p} = 63.08 ms, T_{c} = 21.02 ms, T_{r} = 63.08 ms , T_{s} = 8.70 ms , T_{h} = 0.50 ms , T_{e} = 60 T_{h} 以及T_{crt} = 22 T_{h} 。

由于注册过程只需执行1次，而认证需执行多次，因此本文仅对比相关方案在认证过程中的计算开销。文献[13]在认证过程中执行了3次点乘操作以协商临时密钥保护身份标识、3次点乘操作计算会话密钥保护后续数据的安全性、1次模糊提取操作以及多次轻量级的哈希操作等。文献[14]在认证过程中执行了3次点乘操作以协商临时密钥保护身份标识的安全性、8次对称加解密操作、1次模糊提取操作以及多次哈希操作等。文献[16]在认证过程中执行了4次切比雪夫多项式操作以计算会话密钥保护后续数据的安全性、1次模平方操作以保护身份标识的安全性、1次中国剩余定理求解操作以及多次哈希操作等。本文方案在认证过程中执行了8次对称加解密操作以保护隐私数据的安全性、1次模糊提取操作以及多次哈希操作等。表2列出了对比方案在认证过程的计算开销。基于上述密码学操作的计算时间，图3显示了对比方案在认证过程中随着认证次数的增加的总计算开销的对比结果。结果显示，本文方案认证过程中的计算开销远小于文献[13,14]方案认证过程中的计算开销，而稍大于文献[16]认证过程中的计算开销，但是文献[16]方案会耗费大量的通信开销。

5.2　通信开销

本小节对比了提出方案与其他方案在认证过程中的通信开销。为了公平起见，本文定义对比方案

表 2　计算开销

方案	开具电子凭据认证过程（ms）
文献[13]	$22T_{\mathrm{h}} + 6T_{\mathrm{p}} + T_{\mathrm{r}} = 452.56$
文献[14]	$19T_{\mathrm{h}} + 3T_{\mathrm{p}} + 8T_{\mathrm{s}} + T_{\mathrm{r}} = 331.42$
文献[16]	$16T_{\mathrm{h}} + 4T_{\mathrm{c}} + T_{\mathrm{e}} + T_{\mathrm{crt}} = 133.08$
本文方案	$27T_{\mathrm{h}} + 8T_{\mathrm{s}} + T_{\mathrm{r}} = 146.18$

中的安全等级均等价于高级加密标准(Advanced Encryption Standard, AES) 128 bit[24,25]。具体地，假设用于对称加密、解密的密钥为128 bit，基于椭圆曲线密码学算法的密钥长度为256 bit以及基于大整数分解密码算法的密钥长度为3072 bit等。另外，普通哈希的输出值一般为256 bit，带密钥哈希的输出值一般为128 bit，随机数为128 bit，时间戳为32 bit。此外，在同一场景下，由于对比方案均需传输相同的隐私数据M_i等内容，假设隐私数据的长度以及身份标识信息等内容的长度均为128 bit。本文方案中，哈希函数h_1和h_2的输出均为256 bit，但是h_1仅保留128 bit有效位；f_1输出为128 bit；KDF采用带密钥的哈希函数计算，输出值也为128 bit；bind采用h_2计算，输出值为256 bit。

在认证过程中，文献[13,14,16]方案均有4条信令消息，而本文方案额外考虑到发票确认需要6条信令消息。表3列出了本文方案与其他相关方案在认证过程的通信开销的对比结果。对比结果显示，本文方案认证过程中的通信开销小于文献[13,14,16]方案认证过程中的通信开销。

6 结论

本文提出了一个统一的电子凭据开票系统，并此系统基础之上提出了一个隐私保护的电子凭据在线开具认证方案。通过该方案，完成交易的用户可在线发起开具电子凭据请求，请求消息核验通过后即可获得相应的电子凭据。安全和性能分析结果表明该方案可以在耗费较少的认证开销的情况下实现较多的安全属性，包括相互认证、匿名性、不可链路性、数据机密性以及抵抗重放攻击和用户假冒攻击等。

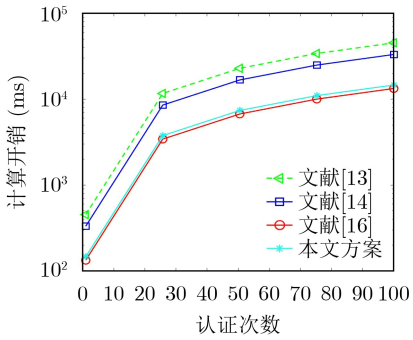

图 3 计算开销对比结果

表 3 通信开销

方案	开具电子凭据认证过程（Byte）
文献[13]	400
文献[14]	272
文献[16]	520
本文方案	268

参 考 文 献

[1] 王玢. 电子发票系统与企业会计信息系统的协同对接研究[D]. [硕士论文], 首都经济贸易大学, 2017.
WANG Fen. Study on synergy effect between E-invoice system and enterprise's accounting system[D]. [Master dissertation], Capital University of Economics and Business, 2017.

[2] 徐丽军, 刘馨月. 关于电子发票推行的安全性问题研究[J]. 辽宁经济, 2018(7): 90–91. doi: 10.14041/j.cnki.1003-4617.2018.07.040.
XU Lijun and LIU Xinyue. Research on the security of electronic invoice[J]. *Liaoning Economy*, 2018(7): 90–91. doi: 10.14041/j.cnki.1003-4617.2018.07.040.

[3] 张庆胜, 刘海法. 基于区块链的电子发票系统研究[J]. 信息安全研究, 2017, 3(6): 516–522. doi: 10.3969/j.issn.2096-1057.2017.06.005.
ZHANG Qingsheng and LIU Haifa. Research of electronic invoice system based on block chain[J]. *Journal of Information Security Research*, 2017, 3(6): 516–522. doi: 10.3969/j.issn.2096-1057.2017.06.005.

[4] 李涛, 杜晓平, 杜晓媛, 等. 基于“互联网+”的发票一体化管理平台[J]. 国网技术学院学报, 2019, 22(4): 48–51. doi: 10.3969/j.issn.1008-3162.2019.04.014.
LI Tao, DU Xiaoping, DU Xiaoyuan, *et al*. Invoice integrated management platform based on "Internet Plus"[J]. *Journal of State Grid Technology College*, 2019, 22(4): 48–51. doi: 10.3969/j.issn.1008-3162.2019.04.014.

[5] 郝天新, 王海翔. 网络发票技术解决方案[J]. 现代电信科技, 2011, 41(10): 67–71. doi: 10.3969/j.issn.1002-5316.2011.10.024.
HAO Tianxin and WANG Haixiang. Technology solution for online invoicing[J]. *Modern Science & Technology of Telecommunications*, 2011, 41(10): 67–71. doi: 10.3969/j.issn.1002-5316.2011.10.024.

[6] JAIN S and ASADULLAH A M. Aggregating bills and invoices on cloud for anytime anywhere access: A sustainable system[C]. The 3rd International Conference on Services in Emerging Markets, Mysore, India, 2012: 1–5. doi: 10.1109/ICSEM.2012.8.

[7] CHU Hongyang, CHAI Yueting, LIU Yi, *et al*. A novel E-Invoice Framework towards data-oriented taxation system[C]. The IEEE 18th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Hsinchu, China, 2014: 242–246. doi: 10.1109/CSCWD.2014.6846849.

[8] ZHANG Wei. Online invoicing system based on QR code recognition and cloud storage[C]. The 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Xi'an, China,

2018: 2576–2579. doi: 10.1109/IMCEC.2018.8469461.

[9] ŠPANIĆ D, RISTIĆ D, and VRDOLJAK B. An electronic invoicing system[C]. The 11th International Conference on Telecommunications, Graz, Austria, 2011: 149–156.

[10] CHOI Y, LEE D, KIM J, *et al*. Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography[J]. *Sensors*, 2014, 14(6): 10081–10106. doi: 10.3390/s140610081.

[11] HE Debiao, KUMAR N, and CHILAMKURTI N. A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks[J]. *Information Sciences*, 2015, 321: 263–277. doi: 10.1016/j.ins.2015.02.010.

[12] CHANG C C and LE H D. A provably secure, efficient, and flexible authentication scheme for Ad hoc wireless sensor networks[J]. *IEEE Transactions on Wireless Communications*, 2016, 15(1): 357–366. doi: 10.1109/TWC.2015.2473165.

[13] LI Xiong, NIU Jianwei, BHUIYAN M Z A, *et al*. A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things[J]. *IEEE Transactions on Industrial Informatics*, 2018, 14(8): 3599–3609. doi: 10.1109/TII.2017.2773666.

[14] LI Xiong, PENG Jieyao, OBAIDAT M S, *et al*. A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems[J]. *IEEE Systems Journal*, 2020, 14(1): 39–50. doi: 10.1109/JSYST.2019.2899580.

[15] CUI Jie, ZHANG Xiaoyu, ZHONG Hong, *et al*. Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment[J]. *IEEE Transactions on Information Forensics and Security*, 2020, 15: 1654–1667. doi: 10.1109/TIFS.2019.2946933.

[16] XU Guoai, WANG Feifei, ZHANG Miao, *et al*. Efficient and provably secure anonymous user authentication scheme for patient monitoring using wireless medical sensor networks[J]. *IEEE Access*, 2020, 8: 47282–47294. doi: 10.1109/ACCESS.2020.2978891.

[17] YANG Qingyou, XUE Kaiping, XU Jie, *et al*. AnFRA: Anonymous and fast roaming authentication for space information network[J]. *IEEE Transactions on Information Forensics and Security*, 2019, 14(2): 486–497. doi: 10.1109/TIFS.2018.2854740.

[18] WANG Feifei, XU Guoai, and XU Guosheng. A provably secure anonymous biometrics-based authentication scheme for wireless sensor Networks Using Chaotic Map[J]. *IEEE Access*, 2019, 7: 101596–101608. doi: 10.1109/ACCESS.2019.2930542.

[19] QI Mingping, CHEN Jianhua, and CHEN Yitao. A secure biometrics-based authentication key exchange protocol for multi-server TMIS using ECC[J]. *Computer Methods and Programs in Biomedicine*, 2018, 164: 101–109. doi: 10.1016/j.cmpb.2018.07.008.

[20] The Tamarin Team. Tamarin-Prover manual security protocol analysis in the symbolic model[EB/OL]. https://tamarin-prover.github.io/manual/tex/tamarin-manual.pdf, 2021.

[21] BASIN D, CREMERS C, KIM T H J, *et al*. Design, analysis, and implementation of ARPKI: An attack-resilient public-key infrastructure[J]. *IEEE Transactions on Dependable and Secure Computing*, 2018, 15(3): 393–408. doi: 10.1109/TDSC.2016.2601610.

[22] ROY S, CHATTERJEE S, DAS A K, *et al*. Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing internet of things[J]. *IEEE Internet of Things Journal*, 2018, 5(4): 2884–2895. doi: 10.1109/JIOT.2017.2714179.

[23] SRINIVAS J, DAS A K, KUMAR N, *et al*. Cloud centric authentication for wearable healthcare monitoring system[J]. *IEEE Transactions on Dependable and Secure Computing*, 2020, 17(5): 942–956. doi: 10.1109/TDSC.2018.2828306.

[24] National Institute of Standards and Technology. SP 800-57 Recommendation for key management, part 1: General (Revised 4)[S]. National Institute of Standards and Technology, 2016.

[25] National Institute of Standards and Technology. SP 800-56A Recommendation for pair-wise key establishment schemes using discrete logarithm cryptography (Revision 2)[S]. National Institute of Standards and Technology, 2013.

马如慧：女，1991年生，讲师，研究方向为4G/5G网络、天地一体化网络安全认证机制等.

曹　进：男，1985年生，教授，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等.

李　晖：男，1968年生，教授，研究方向为密码学、无线网络安全、信息理论和网络编码等.

杨朝中：男，1986年生，副研究员，研究方向为授时技术与方法.

责任编辑：马秀强