·实践平台·

一种基于椭圆曲线密码体制的电子投票方案

陈 英 (浙江科技学院网络管理中心 浙江杭州 310023)
马洪涛 (杭州市港航管理局 浙江杭州 310008)

摘 要: 传统的手工投票已越来越不适应社会快速发展的需要,而电子投票已逐步进入人们的视野中,如何创建一个既安全而又合理的电子投票协议是人们目前所普遍关注的。数字签名是安全领域中的一项重要技术,盲签名有着与传统签名不同的特性,这使得电子投票的应用成为可能。文章主要介绍了一种基于椭圆曲线密码体制的电子投票协议并对其进行了分析。

关键词: 数字签名 电子投票 盲签名 椭圆曲线

中图分类号: TN918 文献标识码: A 文章编号: 1003-6938(2007)03-0107-05

An Electronic Vote Plan Based on Cryptographic System of Elliptic Curve

Chen Ying (Network Management Center, Zhejiang University of Science and Technology, Hangzhou, Zhejiang, 310023)
Ma Hongtao (Hangzhou Port & Waterway Management Department, Hangzhou, Zhejiang, 310008)

Abstract: Traditional manual vote cannot satisfy the demand for the rapid development of society, so the electronic vote has been paid attention to gradually. It is widely concerned how to set up a safe and reasonable electronic vote agreement in recent years. Digital signature is an important technique in security field, and blind digital signature differs from traditional signature in characteristics, which make it possible to apply electronic vote. The paper mainly introduces and analyses electronic vote agreement based on cryptographic system of elliptic curve.

Key words: digital signature; electronic vote; blind digital signature; elliptic curve

CLC number: TN918 Document code: A Article ID: 1003-6938(2007)03-0107-05

引言

数字签名作为一项重要的安全技术,在保证数据的完整性、可用性、保密性、可控性方面起着极其重要的作用。随着信息技术的发展,应用需求的复杂化,数字签名技术也从最初意义上的单人签名、单人验证的模式发展到如今各种特殊签名并存的局面。盲签名、收方不可否认签名、代理签名、群签名等新技术不断地涌现,将数字签名推向一个更为广阔的领域。该文介绍了盲签名的原理及其在电子投票中的应用。

1 数字签名原理

数字签名是附加在数据单元上的一些数据,或是对数据单元所作的密码变换,这种数据或变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性,并保护数据防止被他人(例如接收方)进行伪造。

数字签名主要涉及到发送方和接收方。发送方对所发数据先通过某种算法进行处理得到报文摘要与之相对应的一组散列码,数据不同所得的散列码也不同。然后发送方用自己的私有密钥 TS 对该报文摘要进行加密,并将加密结果和原始数据附加在一起形成了数字签名。最后将该数字签名发往接收方。接收方收到该数字签名后要验证签名。用自己的私钥 RS 解密信息后,对发过来的原始数据先采用与发送方相同的摘要算法得到一个报文摘要,然后用发送的公共密钥对数字签名进行签名算法得到另一个报文摘要,比较两个报文摘要,如相同,就可以确认签名方数据的完整性。发送方的

收稿日期: 2006-10-11; 责任编辑: 宋 戈

公共密钥是可以公开发布的，但只有拥有私有密钥 TS 才能对数据进行签名，这使得数字签名可以确认来源，一旦签名就具有不可抵赖性。只有拥有私钥 RS 的接收方才可以对数据进行解密，保证发送方所发数据在发送过程中不会被任何第三方篡改。

2　盲签名协议

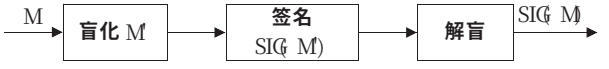
盲签名由 D.Chaum 40(1982)[1]首次提出。D.Chaum 用一个形象的示例说明了盲签名：签名前先把文件放入一个带有复写纸的信封(盲化)，签名人直接在信封上签名，透过复写纸写到文件上。这个过程中信封没有打开，所以无法了解文件的真实内容。事后当文件持有人打开信封(去盲)，签名者可以验证签名，但他不能在签名和文件间建立联系。盲签名的这种特性[2]恰好满足电子投票的保密需求：在认证的同时不泄露内容。

2.1　盲签名的基本思想

(1) 消息拥有者将消息 M 乘以一个随机数(即盲因子)，得到 M′，将原消息内容隐藏起来，即变成了盲消息，并由消息拥有者将该盲消息送给签名者；

(2) 签名者收到盲消息 M′，他并不知道该消息的具体内容，只是证明他已经知道了这个消息，并在盲消息 M′上签名，得 SIG(M′)，然后将其送回给消息拥有者；

(3) 消息拥有者收到经过盲签名的消息 SIG(M′)后，将其去除盲因子，得到原消息 M 的签名 SIG(M)。



2.2　盲签名的基本性质

(1) 盲签名具有一般数字签名的所有特性；

(2) 可以证明消息 M 上签名者 S 的签名是合法的，无论何时，S 都相信他签过这个消息；

(3) S 不能将签名的消息与签过这个消息的行为联系起来，既使保存了他所签的每一个盲签名的记录，他也不能确定他什么时候签过某一个给定的消息，即签名者的协议信息和消息—签名对是不可链接的；

(4) 签名接收者 R 的身份是保密的，且永远不会被泄露，具有无条件的不可追踪性；

(5) 盲签名是无法伪造的，假设攻击者收集了 J 个盲签名，他也无法计算出第 J + 1 个盲签名。

2.3　盲签名的协议内容

为防止签名者在不知内容的情况下误签不利于他的内容，盲签名实施时还要采用分割选择(cut and choose)技术，以概率方式审查文件的内容。一般的盲签名协议[3]如下，其中 U 为用户，S 为签名人：

(1) U 准备 N 份内容相同的文件，分别乘以不同的随机数(盲因子)实现盲化。

(2) U 将盲化后的 N 份文件提交给 S。

(3) S 随机选择一部分(如：N-1 个)文件，向 U 索要盲因子，恢复出文件(去盲)，审查内容是否符合要求。

(4) 如果审查通过，S 从未审查的文件中任取一份盲签名，并发给 U；否则协议终止。

(5) U 对收到的签名文件去盲，得到原文件和签名。

其中(3)可以有多种方案，来减少 U 欺骗的可能性。如不考虑(3)，可以用标记(下文同)表示盲签名：文件 m《签名函数 S，盲化函数 R，去盲化函数 R′，签名认证函数 C，则盲签名算法一般过程为：

(a) 盲化 U→S：R(m)。

(b) 签名 S→U：$(R(m))。

(c) 去盲 U：R′(S(R(m)))=$(m)。

(d) 验证：C($(m))。

3　电子投票系统

3.1　电子投票的概况

对于电子投票的研究开始于 20 世纪 80 年代中期，近年来电子投票作为消息认证系统的重要课题之一和作为盲签名的重要应用受到社会各界的广泛关注，这主要是由于它可以省去通常投票活动在组织工作、选票采集、选票统计和安全保密等方面所需花费的大量人力和物力；其次，投票人也可以不必去有关管理部门所设置的特定的投票处。因此，与通常的投票相比，电子投票既省钱、省力又安全。

目前，电子投票已逐步开始投入使用，比利时举行的联邦议会选举中，全国 750 万选民中的 44 %将采用电子投票方式，这是比利时大选中首次大规模使用电脑来选举。另外，美国已投入巨资对各地的投票系统进行改进，以使投票标准化。

3.2　电子投票的安全性要求

(1) 完备性　即所有合法选票应被正确统计和认证；

(2) 正当性　即不诚实的投票者无法扰乱和破坏整个投票过程；

(3) 匿名性　即所有选票都是秘密的，任何人无法将投票人和其所投的选票联系起来；

(4) 一次性　即任何人只能投一次票，不可进行多次或重复投票；

(5) 合法性　即只有经过许可的投票人才能投票，而没

有获得许可权的任何人都不得获取选票,即使获得选票,也不能进入计票系统计票;

(6) 公正性　即任何事情不能影响投票结果,特别是投票的中间结果不可在投票过程中被泄露;

(7) 可验证性　即选票统计结果是否正确,任何投票人均可对其进行验证。如果发生选票被改动和漏掉而未公布,则投票人可以很容易发现。

3.3　电子投票的基本步骤

由于电子投票方案采用的模型不同,其步骤也会有所区别,本次使用盲签名的电子投票方案的实施按照以下 6 个基本步骤来完成。

(1) 注册　投票人首先将投票的内容进行盲化,并连同自己的身份一起送投票管理中心。在一些方案中还要求投票人对盲化的消息进行签名,此签名也应送管理中心。

(2) 签名　中心先验证投票人是否第一次投票,如果不是,则拒绝签名;如果是第一次投票,则中心对盲化的消息进行签名,并将此签名送投票人。

(3) 投票　投票人从盲签名获得关于真实消息的签名后,既可构造自己认为安全的选票,并将此选票送计票人。

(4) 统计　计票人收到全部选票后,将其编号并公开。

(5) 核查　投票者根据计票人公开的选票可得知自己的选票是否被正确计入,若发现选票被篡改或未公开,则投票者可提出质疑。

(6) 公开　投票者若无异议,则可将真实投票内容及有关密钥或秘密参数送计票人验证。如果这些数据和计票人收到并与公开的有关数据吻合,则计票人公开投票的最终结果。

3.4　电子投票的设计模型

电子投票主要采用由一个注册机构审核投票人资格,一个投票机构接受投票的模式。

投票过程大体可分为三阶段:注册、投票和计票。设投票人为 U,注册机构 R,投票机构 V,以 yes 和 no 方式投票,则盲签名协议可以简单描述为:

(1) 注册:

① U-R,U 向 R 证明自己的身份,并提交两张内容分别为 yes、no 选票(每张选票各选一随机数为唯一序列号加入),选票分别盲化;

②R-U,R 确认 U 的身份合法,并尚未参加投票,若符合条件,则将两张选票签名后返回给 U,否则拒绝 U 的请求。

(2) 投票:

①U 去盲后得到两张合法选票;

② U-V,U 按自己的意愿向 V 提交一张选票,并用 V 的公钥加密后发送给 V;

③ V-U,V 用私钥解密后,验证签名。如签名有效,再查看数据库,选票中的序列号是否有记录。若有,则为重复选票,此票作废,终止协议;否则计票,并记录该序列号。

(3) 计票:

① V 统计选票,并公布结果,以及选票对应的序列号。

协议中采用盲签名使投票内容保密,在注册和投票时,R 和 V 分别检查各自的数据库,确保只有经授权的投票人才能投票,每人投票不会超过一次。统计汇总时列出每个序列号所对应的选票内容,投票人若没找到自己的序列号,或发现选票内容改变了,可以发现舞弊现象,因此该方案满足电子投票安全性的基本要求。

4　基于椭圆曲线密码体制的盲数字签名方案

将基于椭圆曲线密码体制的盲数字签名方案[4]与一般的数字签名方案相比,可以看出其符合盲数字签名方案的特点,具体过程如下:

(1) 系统初始化:

①构造椭圆曲线 $E: y^2=x^3+ax+b$,该曲线是非超奇异的;

②$P\in E(F_p)$ 是一个公开的基点;

③$l=ord(P)$ 是公开基点的阶。

(2) 密钥生成:

用户 A 随机选取一个整数 n_1 作为秘密钥,将公开点 $P_A=n_1P$ 作为公开钥。

(3) 签名生成:

①用户 A 随机选取一个整数 n_2,计算 $R=n_2P$,并将 R 传送给用户 B;

②用户 B 随机选取一个整数 $r_1\in\{1,2,\cdots,l-1\}$,计算 $R=r_1R=(rx,ry)$,式中:rx 和 ry 分别是 R 的 x 坐标和 y 坐标;

③用户 B 再随机选取一个整数 $r_2\in\{1,2,\cdots,l-1\}$,计算 $m=mr_2 \bmod(l)$ 和 $J_1=r_2rx \bmod(l)$,并且将 m 和 J1 传送给用户 A;

④用户 A 计算 $y=((mh_1+J_1)/n_2) \bmod(l)$,将 y 传送给用户 B;

⑤用户 B 计算 $y=(r_1^{-1}r_2^{-1}y) \bmod(l)$,输出签名(R,y)。

(4) 签名验证:

检验 $yR=mP_A+r_xP$ 是否成立,若成立,则签名正确;否则,签名不正确。

5　基于椭圆曲线的电子投票协议

椭圆曲线系统的参数是 (F_q,E,P,n),C 为投票主持人,投票成员为 U_j $(j=1,2,\cdots,m)$ 密钥分别为 KC、K_j,公钥为 $P_C=K_CP$、$P_j=K_jP$。投票管理机构为 A,其私钥为 K_A,公钥为 $P_A=K_AP$,公钥均公开,A 与 C 共享一密钥 K_{AC} 及一传统的加密算

法。b的值代表相应的投票选择，例如，b取2、3、7可以分别表示赞成、反对、弃权，也可以分别表示张三、李四、王五。b的值的具体含义可由投票主持人选择并公开。投票过程中的签名等式取 $s=t^{-1}(e+rk)$，但由于我们用数字签名是为了身份认证和加密，因此可以取 $e=1$，签名等式为 $s=t^{-1}(1+rk)$。协议[5]如下：

(1) 投票人i根据自己的选择，选择相应的表示自己投票选择的b的值，用 b_i 表示，并选择两个大随机数 a_i、t_i（小于n且 $r_i\neq t_i$），随机数 a_i 称为盲因子（盲因子每一次投票应该不同），计算

$$Q_i=(b_i+a_i)P+t_iP_A \quad ①$$

$$G_i=t_iP=(x_i,y_i),\ r_i=x_i \bmod n,\ s_i=t_i^{-1}(1+rik_i) \bmod n \quad ②$$

随后投票人将 (ID_i, Q_i, r_i, s_i) 传送给投票管理机构A（ID_i 表示自己的身份标识）。

(2) 投票管理机构A首先检查投票人i有无投票权利，若无，则A拒绝给i签名；否则A再检查投票人i是不是已投过票，若投过票，则A拒绝给i签名；否则A做如下计算

$$G'_i=s_i^{-1}P+s_i^{-1}r_iP_i=s_i^{-1}(1+r_ik_i)P=(x'_i,y'_i) \quad ③$$

若 $x'_i \bmod n=r_i$，则接受i的签名，随后A选择一随机数 t_{Ai}，计算

$$Q'_{Ai}=Q_i-kAG'_i+t_{Ai}P_C \quad ④$$

$$G_{Ai}=t_{Ai}P=(x_{Ai},y_{Ai}),\ r_{Ai}=x_{Ai} \bmod n,\ s_{Ai}=t_{Ai}^{-1}(1+r_{Ai}k_A) \bmod n \quad ⑤$$

并根据投票的顺序给出顺序号j，然后采用传统加密算法用 k_{AC} 加密j得 $Ei=E(j,k_{AC})$，A将 $(Q'_{Ai}, r_{Ai}, s_{Ai}, j, E_i)$ 传给投票者i，在投票结束时投票管理机构A公布所有的 (ID_i, Q'_{Ai})。

(3) 投票人i根据 $(Q'_{Ai}, r_{Ai}, s_{Ai}, j, E_i)$ 计算

$$Q_{Ai}=Q'_{Ai}-aiP \quad ⑥$$

然后将 $(Q_{Ai}, r_{Ai}, s_{Ai}, j, E_i)$ 匿名传给投票主持人C。

(4) 投票主持人C接收到 $(Q_{Ai}, r_{Ai}, s_{Ai}, j, E_i)$ 后先用与A共享的密钥 k_{AC} 加密j得到 E_i，然后与 E_i 比较是否相等，若不等，则不接受本张选票，否则查询在此选票之前是否有顺序号为j的选票，若有则拒绝接受本张选票，否则随后计算

$$G'_{Ai}=s_{Ai}^{-1}P+s_{Ai}^{-1}r_{Ai}P_A=s_{Ai}^{-1}(1+r_{Ai}k_A)P=(x'_{Ai},y'_{Ai}) \quad ⑦$$

若 $x'_{Ai} \bmod n=r_{Ai}$，则可以证实此选票经过投票管理机构A的签名，然后计算

$$B_i=Q_{Ai}-k_CG'_{Ai}=b_iP \quad ⑧$$

因为 b_i 的取值很小，所以C可以预先计算出作为选票结果的 b_iP，然后根据 B_i 的值就可以得到本张选票的投票结果。当C统计完所有选票后公布所有的 Q_{Ai} 及其对应的投票结果。

6　基于椭圆曲线的电子投票协议分析

下面给出对上述电子投票协议进行的分析过程。[6]

(1) 在第1步中，选择随机数 a_i 的目的是盲化自己的投票选择，然后将盲化的投票选择用数字签名的方式签名并加密（只有投票管理机构A可以解密）传送给A。

(2) 在第2步中，A可以通过式③验证盲化并加密的选票来自于投票人i，然后通过式④先解密出盲化的选票，然后再加密（只有投票主持人可以解密），并加上自己的签名传送给投票人i，式③的推导如下：$G'_i=s_i^{-1}P+s_i^{-1}r_iP_i=s_i^{-1}(1+r_ik_i)P$，而由式② $s_i=t_i^{-1}(1+r_ik_i) \bmod n$ 有 $t_i=s_i^{-1}(1+r_ik_i) \bmod n$，所以 $G'_i=t_iP$。而式④的计算如下：$Q'_{Ai}=Q_i-k_AG'_i+t_{Ai}P_C=(b_i+a_i)P+t_iP_A-k_At_iP+t_{Ai}P_C=(b_i+a_i)P+t_{Ai}P_C$。

(3) 在第3步中，投票人i将A加密盲化的 Q'_{Ai} 通过式⑥进行脱盲，式⑥的计算如下：$Q_{Ai}=Q'_{Ai}-a_iP=(b_i+a_i)P+t_{Ai}P_C-a_iP=b_iP+t_{Ai}P_C$。

(4) 在第4步中，投票主持人C进行相应的验证，通过式⑦验证投票管理机构A对该选票的签名，签名正确则是有效的选票，接着解密得到相应的选票。式⑦的推导如下：$G'_{Ai}=s_{Ai}^{-1}P+s_{Ai}^{-1}r_{Ai}P_A=s_{Ai}^{-1}(1+r_{Ai}k_A)P$，再由式⑤ $s_{Ai}=t_{Ai}^{-1}(1+r_{Ai}k_A) \bmod n$ 有 $t_{Ai}=s_{Ai}^{-1}(1+r_{Ai}k_A)$，所以 $G'_{Ai}=t_{Ai}P$，式⑧的计算如下：$B_i=Q_{Ai}-k_CG'_{Ai}=b_iP+t_{Ai}P_C-k_Ct_{Ai}P=b_iP$。

(5) 作为投票协议很重要的一点是匿名性，即要求投票主持人不能知道具体的人投的是什么票，而本协议在投票人投票时选择一个盲因子对投的票进行盲化，使得A对投票人的票无法知晓，然后A对盲化的票进行签名，随后投票人将其中的盲化因子去掉，则C得到的仅仅是A签过名的一张票，而不知道这张票是谁投的，从而达到匿名性。

(6) 当投票完成时，投票者应当能够查询自己的选票是否被统计以及自己的选票是否被更改，在本协议中，当C统计完所有选票后公布所有的 Q_{Ai} 及其对应的投票结果，此时投票者可以根据自己发送给C的 Q_{Ai} 查询 Q_{Ai} 是否被公开，以判断自己的选票是否被统计，若 Q_{Ai} 被公开，然后查询相对应的投票结果是否是自己的投票，从而完成对自己选票的查询。

(7) 在本协议中加入j及 E_i 的作用是防止投票者的重复投票，在第2步中，A为每一个投票者给出一个顺序号j，并将j加密，在第3步中，投票者由于没办法计算 $E'_i=E(j',k_{AC})$，因此不可能用j'替换j，而且在第4步中，C的检测只允许j出现一次，所以投票者即使重复发送相同的选票，亦可被检测出来。

(8) 假设在通信过程中有窃听者,想在第 3 步中替换(Q_{Ai}, r_{Ai}, s_{Ai}, j, E_j),以达到更改他人选票,但因为(Q_{Ai}, r_{Ai}, s_{Ai}, j, E_j)中有 A 的签名,所以(Q_{Ai}, r_{Ai}, s_{Ai})没有办法伪造的,而唯一可以替换的是(j, E_j),即窃听者可以用窃听到的别人的(j, E_j)来替换,但此法可以被 C 察觉或造成选票缺票,又由于 A 可以对自己的选票查询,则可以查出相应的替换。

(9) 若有人进行欺诈或投票者发现自己的投票被更改或投票者对所投选票否认时,则 A 和 C 的合作可以知道具体的欺诈者或投票在何处被更改或证实投票者所投的票。

结束语

尽管现在已有许多关于电子投票的各种特色方案的提出,但是仍然没有一个方案能够满足电子投票的所有安全要求,尤其是在防止投票中心伪造选票这一方面。本协议具有很高的安全性、灵活性和实用性,但协议中认为选举管理机构 A 和选举主持人 C 均是诚实的,一旦 A 和 C 联合进行欺骗,则可以获得选举者本次选举的盲因子,则有可能更改选举结果。因此基于安全多方计算的电子投票系统有待于我们的开发和实现。

参考文献:

[1] Chaum D.Blind Signatures for Untraceable Payments[A].ProcCryto'82[C].Santa Barbara, California: Springer-Verlag, 1983: 199-203.

[2] 周怡丹,张曙光,付志峰.一个基于盲签名的电子选举方案[J].计算机工程与应用,2003,(15):171-172.

[3] 杨磊,陈小龙.盲签名在电子投票中的安全应用服务[J].信息网络安全,2006,(3):4-6.

[4] 韩然,周梦.基于椭圆曲线的盲数字签名与电子投票协议[J].北京电子科技学院学报,2004,12(4):18-20.

[5][6] 王文龙,王泽成,李志斌.基于椭圆曲线电子选举协议[J].计算机工程,2003,29(22):144-145.

作者简介:陈英(1981-),女,浙江科技学院网络管理中心助理工程师;马洪涛(1981-),男,本科,杭州市港航管理局网络工程师。

(上接第 99 页) 必须保证每一个成员都有权向其他成员获取信息资源,有权从网络收益中取得自己的份额。文化共享工程是以图书馆集群的方式将一个区域内的图书馆紧密联系起来,组成职责明确、管理规范、便捷高效的图书馆联合体,统一业务管理,开展联合服务。各级中心有各级中心的责任和义务,在资源建设形式、内容等方面都作了统一的要求和规范,通过利用文化共享工程开展协作,实现了集群体系内各图书馆业务管理自动化,并以目录管理为核心,将图书报刊、电子文献、随书光盘、视音频资料、专题数据库、网上信息等多种资源整合起来予以揭示,提供集群体系内图书馆的联合采编、图书的通借通还、电子文献的全文传递、文化信息资源等数字资源共建共享、图书馆书目联合查询等服务。

3.3 利用文化共享工程,加强与其他系统图书馆的合作

不同系统图书馆的馆藏重点不同。通过跨系统合作可以获取大量有价值的信息资源。如公共图书馆与高校图书馆之间的合作,公共图书馆可以弥补其科技性、学术性文献资源的不足,而高校图书馆可以补充地方史料性文献资源的欠缺。而文化共享工程是通过广泛的渠道将我国的优秀文化信息资源传递到学校、军营、社区、农村等,为广大的群众享用优秀文化资源提供便利,因此,这就为不同系统的图书馆加强协作提供了渠道。例如,全国文化信息资源贵州省分中心将文化信息资源送到贵州师范大学图书馆,在国内开展了第一个文化信息资源高等学校基层服务点,贵州师范大学图书馆利用文化共享工程提供的资源为全校师生服务,为大学生了解相关的地方性资源提供了便利。同时贵州师范大学图书馆也可以将自身特色的资源在文化共享工程相关标准的要求下进行数字化加工,在文化共享工程体系内为除了本校师生外的广大读者服务。

社会的发展,科学技术的进步,使用户对信息资源的需求方式及内容也产生了根本的变化。用户不再满足于单一的馆藏信息服务,迫切需求内容新颖全面、类型完整、形式多样、来源广泛的信息。用户的这种全方位、综合化的信息需求,显然不是一个图书馆所能够满足的。多个信息单位协作进行信息资源共建共享已成为信息服务界急需解决的问题,利用文化共享工程的优势加强区域合作,实现图书馆信息资源的共建共享,更好地为广大读者服务,是我们当代图书馆人的一项重要历史使命。[3]

参考文献:

[1] 谷雨.共同的理想:信息资源共建与共享—访广东省立中山图书馆莫少强副馆长[J].广东科技,2006,(4).

[2] 孙思习.略论图书馆信息资源的共建共享[J].科技情报开发与经济,2005,(21).

[3] 贾昆嵩.网络环境下图书馆信息资源的共建共享[J].科技情报开发与经济,2004,(10).

作者简介:张永环(1977-),男,贵州省图书馆馆员。