一种公平有效的假名管理模型

朱晓玲[1] 陆 阳[1,2] 张本宏[1] 侯整风[1]
(合肥工业大学计算机与信息学院 合肥 230009)[1]
(安徽省矿山物联网与安全监控技术重点实验室 合肥 230088)[2]

摘 要 匿名是实现隐私保护的有效方法。由于恶意用户的存在,一些应用需要匿名追踪。针对当前可追踪匿名方案存在的两个问题:管理员的权利过大,ID和秘密关联的追踪机制产生的存储和搜索开销随着用户数量的增加而增加,提出了一种公平有效的假名管理模型。模型由假名证书发行、应用和协同追踪组成;采用新的部分盲签名协议确保CA参与假名证书发行,但无权追踪;采用秘密共享机制确保追踪机构必须协同才可揭露假名。由于实现了发行和追踪的分离且追踪机构无需存储、搜索ID与秘密的关联,因此所提模型有效地解决了上述问题。分析表明,模型具有匿名性、可追踪性、不可伪造性、健壮性、公平性,可应用于有匿名追踪需求的Internet安全通信,且能够与传统的PKI应用较好地衔接。

关键词 匿名,假名管理,部分盲签名,协同追踪
中图法分类号 TP309 **文献标识码** A

Efficient Fair Pseudonym Management Model

ZHU Xiao-ling[1] LU Yang[1,2] ZHANG Ben-hong[1] HOU Zheng-feng[1]
(School of Computer and Information, Hefei University of Technology, Hefei 230009, China)[1]
(The Anhui Provincial Key Laboratory of Mine IoT and Mine Safety Supervisory Control, Hefei 230088, China)[2]

Abstract Anonymity is an effective approach to achieve privacy protection. Due to the illegal operation of a malicious user, anonymity requires to be disclosed in some applications. However there are two problems in the existing traceable anonymous schemes. The first one is that the rights of the administrator are too large. Secondly the overhead of storage and search for the relation between ID and a secret increases as the number of users increases. The paper proposed an efficient fair pseudonym management model. The model is composed of pseudonym issuance, pseudonymous application and joint tracking. The new partially blind signature protocol was given to ensure that CA takes part in pseudonym issuance, however, it is unable to track. A secret sharing method was proposed to ensure that tracking authorities jointly disclose a pseudonym. The above two problems are solved effectively by the separation of issuance and tracking without storage and search for the relation between ID and secret. The analysis shows the model has the characteristic of anonymity, traceability, unforgeability, robustness and fairness. So it can be applied in anonymous communication with tracking requirements in Internet. Moreover, it can link up with traditional PKI technique well.

Keywords Anonymity, Pseudonymous management, Partially blind signature, Joint tracking

1 引言

随着Internet的快速发展,Internet中的安全和隐私保护变得非常重要。在一些应用领域如电子现金、电子投票等,对隐私信息的保护是评估整个系统安全性能的重要因素。加密和数字签名提供了数据的保密性、真实性、完整性和不可抵赖性,是目前普遍使用的信息安全技术。但传统技术难于保护用户的隐私,如含有用户身份的数字证书的使用导致了用户隐私的泄露。由于匿名是实现隐私保护的有效方法,本文将匿名技术与传统CA技术相结合,提出可追踪的假名证书管理模型,其能够与基于PKI的应用较好地衔接。

目前,匿名认证已有一定的研究成果。文献[1]提出了匿名无线认证协议,该协议在移动节点与访问网络之间以及访问网络与本地网络之间通过一次交互实现了身份认证,并在移动节点和访问网络之间协商了一次性密钥。文献[2]分析了文献[1]的匿名性安全缺陷,提出了一种改进的匿名无线认证协议,并进行了形式化的安全分析。文献[3]基于零知识证明和ID加解密机制,提出了新的可信芯片证书产生办法,身

到稿日期:2013-01-18 返修日期:2013-04-13 本文受国家自然科学基金项目(60873195),国家"863"计划项目(2011AA060406),安徽省自然科学基金项目(090412051)资助。

朱晓玲(1974—),女,博士生,讲师,主要研究方向为信息安全、移动互联网,E-mail:zhuxl@hfut.edu.cn;陆 阳(1967—),男,博士,教授,主要研究方向为无线传感器网络和分布式控制技术;张本宏(1972—),男,博士,副教授,主要研究方向为分布式控制和可靠性工程;侯整风(1958—),男,教授,主要研究方向为计算机网络和信息安全。

份权威只需要存储可信厂商的公钥证书，不再需要为每个终端设备维护其证书，并可支持管理员平台身份的建立和撤销。文献[4]提出一种基于可信平台模块的可控可信匿名通信系统架构，该架构通过群组通信技术实现发送方的身份匿名，在通信链路上采用加密嵌套封装的数据通信方法实现隐私保护。由于存在恶意用户的非法操作，在一些场景中需要揭示匿名者的真实身份，以上文献较少提及匿名追踪。

群签名[5]具有匿名和可追踪的特点。文献[6]给出基于群签名的匿名认证方案，方案中无需匿名证书，群管理员可以揭示用户身份，但这种认证方案管理员权力过大，群成员的撤销困难。文献[7]提出基于环签名的匿名认证方案，方案中管理员必须和验证者合作才能追踪示证人身份，防止了管理员滥用权利；但每次签名时，示证人都需管理员参加，增加了协议的复杂性。文献[8]提出基于盲签名的电子现金匿名控制，取款时用户将秘密加密作为标记，需要跟踪时银行要求用户解密，这样做的代价是仅一次的追踪就会使同一时间戳的其他诚实用户失去匿名性。这些方案实现追踪的基本思想是：用户注册时得到一些秘密，同时管理员存储用户身份 ID 与秘密的对应关系；用户认证或签名时将秘密嵌入；在匿名追踪时管理员利用陷门打开秘密，进一步在数据库中搜索与秘密关联的 ID。这种 ID 和秘密关联的追踪机制随着成员的增加导致管理员存储和搜索开销增加，加重了管理员负担。

针对上述问题，本文提出新的假名证书发行协议以及协同追踪协议，限制了管理中心的权限，防止了用户欺骗。追踪组无需和其他管理人员交互，可直接打开假名获得 ID，节省了存储和搜索的开销。

2 假名管理模型

模型中有两类实体：①用户 U，U 的身份和假名标识分别用 ID_U 和 ID_{PU} 表示，ID_U 的 RSA 公钥（N_U，e_U）、私钥 d_U 长期使用，ID_{PU} 的 RSA 公钥（N_{PU}，e_{PU}）、私钥 d_{PU} 短期使用。用户配备硬件安全模块（Hardware Security Module，HSM），用来产生密钥，存储私钥，提供与私钥相关的数字签名功能。②中心，包括证书中心 CA、假名证书中心（Pseudonym CA，PCA）、追踪中心（Tracking Authority，TA）。CA、PCA、TA 的 RSA 公钥和私钥分别表示为（N，e_{CA}）和 d_{CA}、（N，e_{PCA}）和 d_{PCA}、（N，e_{TA}）和 d_{TA}。CA 为 U 颁发普通证书 $Cert_U$，PCA 为 U 颁发假名证书 $Cert_{PU}$，TA 进行匿名追踪。将 TA 扩展为 k 个权威组成的权威组，记为 TAs，$TAs=\{TA_1, TA_2, \cdots, TA_k\}$（$1\leqslant i\leqslant k$），$TA_i$ 可能为执法机构、法官或隐私保护机构等。

模型由 3 个协议组成：①假名证书发行；②假名应用；③协同追踪。协议间的依存关系如图 1 所示，用户通过发行协议获取假名和假名证书，将其应用于假名通信；假名通信若发现可疑用户，就将其假名提交给协同追踪协议；追踪协议根据假名恢复出身份，可进行责任判定，并将身份提交给发行协议，以拒绝该用户以后的假名申请。

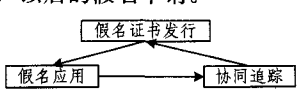

图 1 协议族

其工作流程如下：①U 用证书签名机制向 CA 证明身份 ID_U 并申请假名 ID_{PU}，CA 为 U 颁发 ID_{PU} 签名；②PCA 验证 CA 对 ID_{PU} 签名通过后，为 U 颁发假名证书 $Cert_{PU}$；③U 使用 $Cert_{PU}$ 与其他用户 U' 进行安全通信；④一旦发现可疑情况，其他用户可以向 TAs 提交追踪请求；⑤TAs 恢复出与 ID_{PU} 对应的 ID_U。⑥TAs 提交 ID_U 给 CA，CA 将 U 列入黑名单。

3 假名证书发行协议

为避免 CA 权力过大，使其无法获得 ID_U 和 ID_{PU} 的关联，CA 采用盲签名对假名 ID_{PU} 数字签名。盲签时，用户可能欺骗，如在假名中嵌入其他用户的 $ID_{U'}$ 以备日后冒充。由于部分盲签名允许签名人在签名中嵌入一个和用户一起协商的公共信息，而这个公共信息不可以被移除或修改，因此考虑使用部分盲签名。

部分盲签名已有一定的研究成果，文献[9]基于 RSA 算法建议了安全随机的部分盲签名，方案在选择消息攻击下是不可伪造的。文献[10]基于改进的 RSA 密码系统提出可证安全的强壮门限部分盲签名方案。文献[11]提出了一个基于身份的无可信 PKG 的部分盲签名方案，其可抵抗选择消息攻击和身份攻击下的存在性伪造。

这些部分盲签名方案都需要公布嵌入的信息，用于对签名的验证。因为 ID_U 为 CA 和 U 共有的关键信息，由 CA 嵌入，但 ID_U 不能对外公开，以上方案无法满足本模型中对 ID_U 匿名的需求。因此，我们设计了新的部分盲签名协议，在对外不泄露 ID_U 的情况下，实现假名证书的发行。协议内容如下：

1）U 向 CA 秘密发送 $ID_U \| n \| \sigma_U \| Cert_U$，其中 n 为 U 申请的假名数，σ_U 为 U 对前数据项的签名。

2）CA 验证 U 签名，如验证通过，且 CA 同意颁发假名，则向 U 秘密发送 $ID_{CA} \| ID_U \| \exp \| \sigma_{CA}$，其中 exp 为有效期，$\sigma_{CA}$ 为 CA 对前数据项的数字签名。

3）U 验证 CA 签名，如验证通过，随机选取 $r_i, x_i \in Z_N^*$，向 CA 发送关于 r_i 的盲化 $x_i^{e_{CA}} r_i$。其中 N 为 CA、PCA 和 TAs 共有的模，e_{CA} 为 CA 公钥，$1\leqslant i\leqslant n$。

4）CA 计算并发送 $a_i=(x_i^{e_{CA}} r_i \cdot (i \| ID_U \| \exp))^{d_{CA}}$，$b_i=((i \| ID_U \| \exp)^{e_{TA}})^{d_{CA}}$，其中 e_{TA} 为 TAs 公钥。

5）U 检查 $b_i^{e_{CA}}=(i \| ID_U \| \exp)^{e_{TA}}$，如验证通过，脱盲得

$$s_{1,i}=a_i/x_i, s_{2,i}=\frac{s_{1,i}^{e_{TA}}}{b_i} \tag{1}$$

令假名

$$ID_{PU_i}=r_i \cdot (i \| ID_U \| \exp) \| r_i^{e_{TA}} \tag{2}$$

U 向 PCA 发送$(ID_{CA} \| \{ID_{PU_i} \| s_{1,i} \| s_{2,i} \| \exp \| e_{PU_i} \| N_{PU_i} \| \sigma_{PU_i}\}_{1\leqslant i\leqslant n})^{e_{PCA}}$，其中 σ_{PU_i} 为 U 用临时私钥 d_{PU_i} 的数字签名。

6）PCA 解密后检查 U 的签名，如验证通过，提取出假名前项 $r_i \cdot (i \| ID_U \| \exp)$、后项 $r_i^{e_{TA}}$、$s_{1,i}$ 和 $s_{2,i}$，验证盲签名

$$s_{1,i}^{e_{CA}}=r_i \cdot (i \| ID_U \| \exp), s_{2,i}^{e_{CA}}=r_i^{e_{TA}} \tag{3}$$

是否成立。如验证通过，PCA 向 U 发送假名证书

$$Cert_{PU_i}=ID_{PCA} \| ID_{PU_i} \| \exp \| e_{PU_i} \| N_{PU_i} \| \sigma_{PCA} \tag{4}$$

执行该协议的前提是 U 已获取 e_{CA}、e_{PCA}、e_{TA} 和模 N，并产生与 ID_{PU_i} 对应的公钥（N_{PU_i}，e_{PU_i}）和私钥 d_{PU_i}。步骤 1）U 向 CA 发送申请 n 个假名的请求。步骤 2）CA 验证 U 身份后回应同意受理。步骤 3）U 用 x_i 将 r_i 盲化后发给 CA。步骤 4）CA 嵌入 ID_U 和 exp 并盲签。步骤 5）U 脱盲得 CA 对 n 个

假名 ID_{PU_i} 的签名 $s_{1,i}$ 和 $s_{2,i}$，以此为凭证，向 PCA 申请假名证书。步骤 6)PCA 检测 n 个盲签，如正确，为 U 颁发假名证书 $Cert_{PU_i}(1\leqslant i\leqslant n)$。检测式(3)显然成立，因为 $s_{1,i}^{e_{CA}}=(\frac{a_i}{x_i})^{e_{CA}}=((r_i\cdot(i\parallel ID_V\parallel \exp))^{d_{CA}})^{e_{CA}}=r_i\cdot(i\parallel ID_U\parallel \exp)s_{2,i}^{e_{CA}}=(\frac{s_{1,i}^{e_{TA}}}{b_i})^{e_{CA}}=\frac{(r_i\cdot(i\parallel ID_U\parallel \exp))^{e_{TA}}}{(i\parallel ID_U\parallel \exp)^{e_{TA}}}=r_i^{e_{TA}}$。

4 假名应用

假名证书与传统数字证书的功能一致，可提供数字签名、身份认证和密钥协商等服务。以数字签名为例，其流程如下：

1)U 从 n 个假名中随机选一假名，不妨假设选中假名证书和短期私钥分别为 $Cert_{PU}$ 和 d_{PU}，对消息进行 RSA 签名生成签名消息。

2)U 向服务器提交签名消息，服务器从消息中提取出假名证书，对签名进行验证，验证通过后，服务器向 U 提供服务。

假名证书与传统数字证书的结构基本一致，签名消息格式如图 2 所示，包括 5 个字段。消息 ID 表示在同一个假名周期内的消息编号，数据净荷即消息内容，时戳用来防止重放攻击，签名即用短期私钥 d_{PU} 对前 3 个字段 RSA 签名的结果。当 RSA 密钥长度为 1024 比特时，签名结果为 1024 比特，即 128 字节。由于假名证书 $Cert_{PU}=ID_{PCA}\parallel ID_{PU}\parallel \exp\parallel e_{PU}\parallel N_{PU}\parallel \sigma_{PCA}$，在 RFC2459[12] 中，有效期 exp 长度为 26B，因此假名证书长度=2+256+26+128+128+128=668(B)，消息总长度=2+100+4+128+668=902(B)。

消息ID	数据净荷	时戳	签名	假名证书
2B	100B	4B	128B	668B

图 2 签名消息的格式

5 协同追踪协议

假名追踪的基本思路是 TAs 先用私钥从 ID_{PU} 的后项解密出 r，再由前项得到 ID_U。由于可以由 ID_{PU} 直接求得 ID_U，因此无需追踪组存储 ID_U 和 ID_{PU} 的对应关系，节省了存储和搜索的开销。多个权威协同追踪比单个权威追踪更加公平可靠，基于门限秘密共享方案[13]，将 TAs 私钥 d_{TA} 分配给 k 个权威，至少 m 个权威协同才可恢复身份。系统在初始化阶段，选取素数 $P>\phi(N)$，构造 $Z_P[x]$ 上 $m-1$ 次多项式 $f(x)$，使 $f(0)=d_{TA}$，计算 $f(ID_i)=s_i$，其中 ID_i 为 TA_i 身份，将 s_i 秘密发送给 TA_i，TA_i 获得秘密份额 s_i。系统追踪协议如下：

1)用户 U' 向某追踪机构如 TA_1 举报可疑 $Cert_{PU}$。

2)TA_1 检查时戳和签名是否有效，如验证通过，TA_1 从 $Cert_{PU}$ 提取 ID_{PU}，从 ID_{PU} 提取 $r^{e_{TA}}$，向其他成员 TA_i 发送 $req\parallel r^{e_{TA}}$，其中 req 为追踪请求。m 个成员同意追踪，组成参与追踪组，不妨假设其标识为 $ID_1,ID_2,\cdots,ID_m$。

3)参与成员 $TA_i(2\leqslant i\leqslant m)$ 将 $(r^{e_{TA}})^{a_i}\bmod N$ 发送给 TA_1，其中 $a_i=s_il_i(0)\bmod P$，$l_i(0)=\prod_{\substack{j=1\\ j\neq i}}^{m}\frac{ID_j}{ID_j-ID_i}\bmod P$。

4)TA_1 尝试 x 所有可能$(-m<x\leqslant 0)$，计算得到

$$r=(r^{e_{TA}})^{xP}\cdot\prod_{i=1}^{m}(r^{e_{TA}})^{a_i}\bmod N \tag{5}$$

从 ID_{PU} 提取 $r\cdot(i\parallel ID_U\parallel \exp)$，则 $i\parallel ID_U\parallel \exp=r^{-1}\cdot r\cdot(i\parallel ID_U\parallel \exp)$，根据字符串的实际意义确定 ID_U。

6 分析

命题 1 CA、PCA 和其他用户，在协议中无法确定假名与身份的关系，模型具有匿名性。

证明：根据假名证书发行协议可得到：

①在 CA 知道 ID_U、exp、$x_i^{e_{CA}}$ r_i、a_i、b_i 的情况下，由于 x_i 是 U 随机选取的，并由 U 唯一秘密保存，因此 CA 不可能从 $x_i^{e_{CA}}$ r_i、a_i 和 b_i 中获取 r_i，进而得到 $ID_{PU_i}=r_i\cdot(i\parallel ID_U\parallel \exp)\parallel r_i^{e_{TA}}$。

②在 PCA 知道 ID_{PU_i}、$s_{1,i}$、$s_{2,i}$、exp、e_{PU_i}、N_{PU_i} 的情况下，PCA 由于不知道 TAs 的私钥，因此不可能从 $s_{1,i}$、$s_{2,i}$ 和 ID_{PU_i} 的后项 $r_i^{e_{TA}}$ 获取 r_i，进而由前项得到 ID_U。

③其他用户在仅知道 ID_{PU_i} 的情况下，要获得 ID_U，即要求其在不知 TAs 私钥 d_{TA} 的情况下对 $r_i^{e_{TA}}$ 进行解密，这在计算上是不可行的。

命题 2 TAs 中 m 个机构协同可以由假名 ID_{PU} 恢复出身份 ID_U，模型具有可追踪性。

证明：$Z_P[x]$ 上 $m-1$ 次多项式 $f(x)$，满足 $f(0)=d_{TA}$，$f(ID_i)=s_i$。根据拉格朗日插值公式 $d_{TA}=\sum_{i=1}^{m}s_il_i(0)\bmod P$，记 $a_i=s_il_i(0)\bmod P$，$d_{TA}=\sum_{i=1}^{m}a_i+xP$。

因为 $0\leqslant d_{TA}<\phi(N)$，$0\leqslant a_i<P$，$0\leqslant\sum_{i=1}^{m}a_i<mP$，$\phi(N)<P$，所以 $-m<x\leqslant 0$。故

$$r=(r^{e_{TA}})^{d_{TA}}=(r^{e_{TA}})^{\sum_{i=1}^{m}a_i+xP}=(r^{e_{TA}})^{xP}\prod_{i=1}^{m}(r^{e_{TA}})^{a_i}\bmod N$$

进一步由 r 求得 ID_U。

命题 3 CA、用户、攻击者伪造假名及证书是困难的，模型具有不可伪造性。

证明：①如果 CA 将假身份嵌入盲签名，U 验证检测式 $b_i^{e_{CA}}=(i\parallel ID_U\parallel \exp)^{e_{TA}}$ 时可发现。

②如果 U 企图把其他用户的身份嵌入假名中，需要伪造 $s_{1,i}$ 和 $s_{2,i}$，使其满足 $s_{1,i}^{e_{CA}}=r_i\cdot(i\parallel ID_{U'}\parallel \exp)$ 和 $s_{2,i}^{e_{CA}}=r_i^{e_{TA}}$，由于 U 不知道 d_{CA}，求解 $s_{1,i}$ 和 $s_{2,i}$ 在计算上是不可行的。同时，假名前项中的 $i\parallel ID_U\parallel \exp$ 具有实际意义，给实际的伪造带来困难。

③对于外部攻击者，假名证书发行协议具有双向认证性，攻击者必须伪造 U 和 CA 的 RSA 签名。

由于伪造 RSA 签名计算不可行，模型具有不可伪造性。

命题 4 权威机构的妥协不影响用户的隐私保护，模型具有健壮性。

证明：由于假名证书的发行和追踪实现了分离，CA 和 PCA 负责发行，无权追踪，因此 CA 或 PCA 的妥协不会导致假名用户身份的泄露。

在追踪阶段，只要 TAs 中妥协成员的数量不超过 $m-1$，就无法由假名 ID_{PU} 恢复出身份 ID_U。

命题 5 在协议执行过程中，参与协议的任何一方都不占优势，模型具有公平性。

在假名证书发行协议中，假名 ID_{PU_i} 由 U 和 CA 共同产生，U 提供随机数 r_i，CA 提供 exp 和 ID_U。CA 嵌入假的 $ID_{U'}$，会被 U 发现；U 伪造假的 $ID_{U'}$，使其通过 PCA 检测，并保证 $i\parallel ID_{U'}\parallel \exp$ 的有效性是困难的(命题 3)。CA 知 ID_U，却无法获知 ID_{PU_i}；PCA 知 ID_{PU_i}，却无法获知 ID_U(命

题 1)。

在假名追踪协议中,将 TA 私钥分配给 k 个权威,至少 m 个权威协同才可恢复用户身份(命题 2),显然,多个权威协同追踪比单个权威追踪更加公平可靠。而且,假名 $ID_{PU_i}=r_i\cdot(i\parallel ID_U\parallel \exp)\parallel r_i^{e_{TA}}$ 加入了随机成分 r_i,即使是 TAs 得到一个假名,也需对 r_i 进行穷搜索才可以获得 U 的其他假名,只要 r_i 足够长,即使多个权威协同也无法由用户 U 的一个假名 ID_{PU_i} 推出另一个假名 ID_{PU_j}。

因此,在匿名、不可伪造、可追踪方面,模型都体现了公平性。

结束语 本文提出新的部分盲签名方法,用以解决 CA 对假名盲签时,能够嵌入 ID,又不对外泄露 ID 的问题。通过该方法,能够防止用户欺骗,限制 CA 的权限,实现假名发行与追踪的分离,保证假名证书发行协议的公平性。身份和秘密关联的追踪机制导致管理员存储和搜索开销随着用户数量的增加而增加,本文提出将身份嵌入在假名中,由追踪组直接打开,提高了假名追踪的有效性。追踪时引入秘密共享方案,增强了系统的健壮性。同时,由于假名证书与传统数字证书的结构基本一致,本模型能够与基于 PKI 的应用较好地衔接。

参 考 文 献

[1] 朱建明,马建峰. 一种高效的具有用户匿名性的无线认证协议[J]. 通信学报,2004,25(6):12-18

[2] 彭华熹,冯登国. 匿名无线认证协议的匿名性缺陷和改进[J]. 通信学报,2006,27(9):78-85

[3] 于爱民,初晓博,冯登国. 基于可信芯片的终端平台匿名身份建立方法研究[J]. 计算机学报,2010,33(9):1703-1712

[4] 吴振强,周彦伟,乔子芮. 一种可控可信的匿名通信方案[J]. 计算机学报,2010,33(9):1686-1702

[5] Boneh D, Boyen X, Shacham H. Short group signatures[C]// Proceedings of Crypto'04. Springer Berlin Heidelberg, 2004: 41-55

[6] Sun Xiao-ting, Ho Pin-han, Shen Xue-min. GSIS: Secure vehicular communications with privacy preserving [J]. IEEE Transactions on vehicular technology, 2007, 56(6): 3442-3456

[7] 田子健,王继林,伍云霞. 一个动态的可追踪匿名认证方案[J]. 电子与信息学报,2005,27(11):1737-1740

[8] 李梦东,杨义先. 无可信第三方的离线电子现金匿名性控制[J]. 电子学报,2005,33(3):456-458

[9] Cao Tian-jie, Lin Dong-dai, Xue Rui. A randomized RSA-based partially blind signature scheme for electronic cash[J]. Computers & Security, 2005, 24(1): 44-49

[10] 曹珍富,朱浩瑾,陆荣幸. 可证安全的强壮门限部分盲签名[J]. 中国科学 E 辑信息科学,2005,35(12):1254-1265

[11] 冯涛,彭伟,马建峰. 安全的无可信 PKG 的部分盲签名方案[J]. 通信学报,2010,31(1):12-18

[12] Housley R, Ford W, Polk W, et al. Internet X. 509 Public Key Infrastructure Certificate and CRL Profile[EB/OL]. http://www.ietf.org/rfc/rfc2459.txt, 2012-03

[13] Shamir A. How to share a secret [J]. Communications of the ACM, 1989, 22(11): 612-613

(上接第 116 页)

[6] Barbosa M, Farshim P. Certificateless signcryption[C]// Proceedings of ASIACCS 2008. ACM, New York, 2008: 369-372

[7] Aranha D, Castro R, Lopez J, et al. Efficient certificateless signcryption[EB/OL]. http://labcom.inf.ufrgs.br/labcom/ceseg/anais/2008/data/pdf/st03_01_resumo.pdf

[8] Wu Chen-huang, Cheng Zhi-xiong. A new efficient certificateless signcryption scheme[C]// Proceedings of ISISE 2008. IEEE Computer Society, 2008: 661-664

[9] Selvi S S D, Vivek S S, Rangan C P. Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing[EB/OL]. Cryptology ePrint Archive, 2009. http://eprint.iacr.org/2009/298

[10] Selvi S S D, Vivek S S, Shukla D, et al. Efficient and provably secure certificateless multi-receiver signcryption[C]// Proceedings of ProvSec 2008, LNCS 5324. Berlin: Springer-Verlag, 2008: 52-67

[11] Xie Wen-jian, Zhang Zhang. Efficient and provably secure certificateless signcryption from bilinear maps[C]// Proceedings of WCNIS 2010. IEEE Press, 2010: 558-562

[12] Barreto P S L M, Libert B, Mccullagh N, et al. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps[C]// Proceedings of ASIACRYPT 2005, LNCS 3788. Berlin: Springer-Verlag, 2005: 515-532

[13] Chen Yan, Zhang Fu-tai. A new certificateless public key encryption scheme[J]. Wuhan University Journal of Natural Sciences, 2008, 13(6): 721-726

[14] Selvi S S D, Vivek S S, Rangan C P. Security weaknesses in two certificateless signcryption schemes[EB/OL]. Cryptology ePrint Archive, 2010. http://eprint.iacr.org/2010/092

[15] Liu Zhen-hua, Hu Yu-pu, Zhang Xiang-song, et al. Certificateless signcryption scheme in the standard model[J]. Information Sciences, 2010, 180(3): 452-464

[16] Weng Jian, Yao Guo-xiang, Deng R H, et al. Cryptanalysis of a certificateless signcryption scheme in the standard model[J]. Information Sciences, 2011, 181(3): 661-667

[17] Li Peng-cheng, He Ming-xing, Li Xiao, et al. Efficient and provably secure certificateless signcryption from bilinear pairings[J]. Journal of Computational Information Systems, 2010, 6(11): 3643-3650

[18] Du Hong-zhen, Wen Qiao-yan. Efficient and provably-secure certificateless short signature scheme from bilinear pairings[J]. Computer Standards and Interfaces, 2009, 31(2): 390-394

[19] Javier H, German S. Forking lemmas for ring signature schemes [C]// Proceedings of INDOCRYPT 2003, LNCS 2904. Berlin: Springer-Verlag, 2003: 266-279