一种面向付费个性化服务的匿名认证方案*)

刘景森　戴冠中

(西北工业大学自动化学院　西安 710072)

摘　要　个性化服务系统为每个用户提供了满足个性化需求的差异服务，但用户模型的建立和更新依赖于用户的个人信息，存在着隐私泄漏的风险，从而降低了用户使用个性化服务的意愿。本文基于可信计算环境下直接匿名证言方案的可变假名机制，设计了一个面向通用网络环境下个性化服务的匿名认证方案，并针对付费系统的匿名保持问题做了进一步改进。理论分析和实验结果表明，个性化服务提供者可以鉴别用户是否合法付费用户，并具有何种访问权限，但无法确定用户的具体身份，即使服务提供者将访问信息泄漏，也不会危及用户隐私。

关键词　个性化服务，等级会费制，隐私保护，匿名认证

An Anonymous Authentication Method for Toll Personalized Service

LIU Jing-Sen　DAI Guan-Zhong

(College of Automation, Northwestern Polytechnical University, Xi'an 710072)

Abstract　Personalized service system provides differential services that satisfy the personalized needs of users. However, both generating and updating users' models depend on private information, thus disclosure of privacy is possible. This could limit users' willingness to use these personalized services. Basing on the pseudonymity of direct anonymous attestation scheme, this paper proposes an anonymous authentication method for personalized service in general networks. Some fringe improvements are also done for holding anonymity in a toll system. Theoretical analysis and experimental results demonstrate that the service provider can know whether a user is regular, and which access right the user has, but it cannot identify the user. Even if the service provider reveals access information, users' privacy will not be endangered.

Keywords　Personalized service, Graded fee system, Privacy protection, Anonymous authentication

1　引言

个性化服务是一种体现个性化特征、满足个性化需求、培养个性化趋势的信息服务方式，非常适用于 Internet 环境下的海量信息检索。近年来，国内外在个性化服务领域取得了大量研究成果，出现了不少个性化信息检索服务系统，如 Personal WebWatcher[1]，WebPersonalizer[2]，DOLTRI-Agent[3] 等等。

用户模型是实现个性化服务的基础。现有系统虽然在用户建模方面各具特色，但在本质上都依赖于对用户信息的收集与学习。由于用户模型及用户信息中包含着用户隐私，而上述系统并没有实现相应的隐私保护机制，服务提供者可通过用户登录唯一地确定用户身份，跟踪用户的个人信息，因此存在着用户隐私可能泄漏的问题。解决这一问题的方法主要有两种：一是制订隐私保护的相关法律条文，二是实现用户的匿名访问[4]。但法律手段只是一种事后追究机制，而且服务提供者遭到入侵导致隐私泄漏的问题也难以解决。匿名访问可以较好地解决这些问题，但个性化服务又需要跟踪用户的个人信息，对于大多数基于等级会费制的商业付费系统而言，用户的付费期限和访问权限管理也增加了实现匿名访问的复杂性和难度。

随着用户对个人信息保护的日益关注，最近几年，对匿名认证问题的研究明显增加，也取得了一些研究成果。T. Saito 等提出了一种基于 SPKI(Simple Public Key Infrastructure)授权证书的匿名认证方案[5,6]，Y. Kakizaki 等提出了一种基于 PKIX(Public Key Infrastructure with X. 509)属性证书的匿名认证方案[7]。这些方案可在用户向服务提供者出示的证书中包含权限和时限字段，非常适用于等级会费制系统。但是，在 Saito 方案的授权证书五元组中虽不包含用户 ID，但包含了用户公钥，服务提供者仍可跟踪某一用户的信息。Kakizaki 方案解决了这一问题，用户每次与服务提供者建立会话前，都要向可信第三方 AA(Attribute Authority)申请一次性属性证书，服务提供者无法根据属性证书鉴别和跟踪用户。但随着用户规模的增加，AA 将成为影响认证效率的瓶颈。此外，这些方案都要引入一个完全独立于服务提供者和用户的、不同于 PKIX CA(Certificate Authority)的、新的可信第三方来鉴别用户身份。可信第三方既不能由用户来建立，否则用户身份的合法性无法得到保证；也不能由服务提供者来建立，否则两者串通就无法实现匿名性，这就使得由谁来建立可信第三方缺乏合适的商业模式，成为一个难以解决的问题。

组签名是实现匿名认证的另一种重要技术，但大多数组签名方案中的组管理员能够鉴别用户身份。与可信第三方一样，组管理员由谁来建立仍是一个问题。k 次匿名认证[8](k-times Anonymous Authentication，k-TAA)、直接匿名证言[9](Direct Anonymous Attestation，DAA)等方案解决了这一问题。在 k-TAA 方案中，只要用户在服务提供者限定的次数内访问服务系统，即使组管理员与服务提供者串通，也不能识别用户的身份。在 DAA 方案中，用户只需向发布者申请一次 DAA 证书，就可无限制地访问服务系统，即使服务提供者与发布者串通，也无法识别用户的身份。但 k-TAA 方案主要适用于限制用户访问次数的应用环境，并不适合等级会费制系统。而 DAA 方案是为可信计算环境设计的，不支持非可信

*)河南省自然科学基金项目(0511014300)、国家"863"高技术研究发展计划项目(200AA142170)。**刘景森**　博士生，副教授；**戴冠中**　教授，博士生导师。

计算的通用网络环境，而且无法限定用户的等级和时限。

为了解决付费个性化服务的匿名认证问题，本文提出了一个 GT-APIRS 系统模型，个性化处理完全运行于客户端，信息检索服务运行于服务器端，匿名认证方案采用一种我们称为非可信计算环境下直接匿名证言的机制，并针对等级会费制系统的匿名保持问题，对认证方案作了进一步改进。服务提供者可以确定用户是一个拥有何种权限的合法付费用户，但并不知道该用户具体是哪个用户，即使服务提供者跟踪用户的访问信息，并将这些信息泄漏出去，也不会造成用户隐私的泄漏。

本文其余部分结构如下：第 2 节描述 GT-APIRS 的系统结构；第 3 节讨论面向等级会费制的匿名认证方案；第 4 节分析该方案的安全性和匿名性，对匿名效果进行模拟实验；第 5 节与 DAA 方案进行比较；最后总结全文。

2 GT-APIRS 的系统结构

如图 1 所示，GT-APIRS 系统由用户个性化子系统和检索服务子系统组成。用户个性化子系统位于客户端，由用户界面、个性化处理模块、用户特征库和匿名登录器组成。其中，用户界面提供对 GT-APIRS 系统的操作，并收集用户信息；个性化处理模块负责建立和更新用户模型，并依据该模型优化查询表达式、对查询结果进行分析和过滤；用户特征库用于存储用户信息和用户模型；匿名登录器负责向检索服务子系统申请证书，并产生登录签名。检索服务子系统位于服务器端，由用户管理中心、登录验证服务器和检索服务器组成。其中，用户管理中心负责管理用户的服务器帐户，并向用户发布证书；登录验证服务器负责验证用户的登录签名；检索服务器负责提供对分布式信息资源的统一查询。

用户进行个性化信息检索的流程为：用户在客户端本地登录用户个性化子系统，用户个性化子系统自动匿名登录服务器端的检索服务子系统；用户提交查询请求，用户个性化子系统依据用户模型优化查询表达式，并将该表达式提交给检索服务子系统；检索服务子系统执行联合资源发现，并将检索结果返回用户个性化子系统；用户个性化子系统依据用户模型对检索结果进行过滤、分类和排序，将最终结果提交给用户。

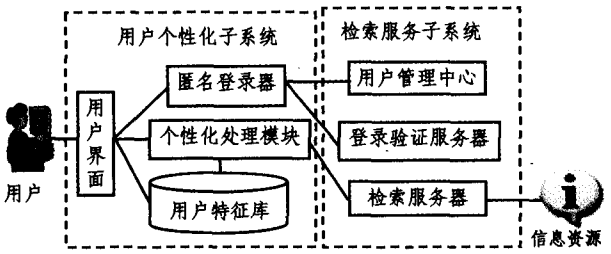

图 1 GT-APIRS 的系统结构

3 面向等级会费制的匿名认证方案

GT-APIRS 系统采用等级会费制的用户付费策略。用户被划分为若干个等级（如：普通会员、专业会员、高级会员、…），系统向缴纳不同会费的用户提供不同等级和时限的信息检索服务，允许用户在有效时限内获得相应等级的服务。这种付费策略目前为大多数付费检索系统所使用。

与现有个性化服务系统基于用户名的完全身份识别登录方式不同，GT-APIRS 系统采用了基于可变假名的匿名登录方式，这种匿名登录方式的实现基础是一种我们称之为非可信计算环境下直接匿名证言的机制。DAA 方案是可信计算组织 2003 年发布的匿名认证方案[9,10]，其实现基础为 Camenisch-Lysyanskaya 组签名方案[11]和基于离散对数的知识证明[12]，它是为可信计算环境设计的，不支持非可信计算环境。为此，我们修改了 DAA 方案的实现机制，设计了一种基于 DAA 原理的面向通用网络环境的匿名认证方案，并针对等级会费制系统，对认证方案作了进一步补充和改进。

下面介绍 GT-APIRS 系统中用户匿名登录方案的处理流程，讨论集中于对 DAA 方案的补充与改进部分。与现有 DAA 方案相同的变量、过程、相关计算和知识证明细节，本文不再重新定义和赘述。

3.1 注册帐户

(1)用户管理中心产生一对 RSA 签名密钥(M_U,M_R)，用户可通过用户管理中心的 PKIX 身份证书公开获得 M_U。用户按等级和时限标准缴纳会费，并向用户管理中心申请注册。用户管理中心确认后，为用户建立一个用户名、口令为(U_S,P_S)的服务器账户，该服务器账户不是用于登录并使用检索服务，而是用于匿名登录器向用户管理中心申请证书。

(2)用户执行“创建本地帐户”操作，本地账户用于该用户本地登录用户个性化子系统。该操作除了要求用户设置本地帐户的用户名和口令(U_L,P_L)外，还要求用户输入其服务器帐户的(U_S,P_S)。用户个性化子系统为用户创建本地帐户，并将(U_L,P_L)与(U_S,P_S)的映射关系存储在本地帐户中。

3.2 申请证书

(1)用户执行“申请证书”操作，匿名登录器将用 M_U 加密的(U_S,P_S)传送给用户管理中心，以登录该用户的服务器帐户。

(2)用户管理中心用 M_R 解密获得(U_S,P_S)，验证用户的合法性，并检查该用户服务器账户中证书申请标志是否为 0。若该标志为 0，表示该用户尚未申请过证书或(f_0,f_1)泄漏后执行了“证书挂失”操作；若该标志不为 0，则表示该用户已申请过证书，用户管理中心将拒绝这次申请。为了防止重复使用“证书挂失”和“申请证书”操作进行拒绝服务攻击，用户执行“证书挂失”操作一段时间后（比如 1 天），用户管理中心才将其服务器账户中的证书申请标志清 0。

(3)用户管理中心将用户等级值 j、时限值 k、对应于等级 j 的 DAA 发布者公钥 $PK_{I_j}=(n,g',g,h,S,Z,R_0,R_1,\gamma,\Gamma,\rho)$和用 M_R 签名的等级证明 S_G 发送给用户。

$$S_G=Sign_{M_R}(H((U_S\|P_S)\|j\|k\|(n\|g'\|g\|h\|S\|Z\|R_0\|R_1\|\gamma\|\Gamma\|\rho)))$$

(4)匿名登录器用 M_U 对 S_G 解签名，验证 j、k 和 PK_{I_j} 的正确性，然后产生秘密数(f_0,f_1)，选择一个随机整数 v'，计算 $U=R_0^{f_0}R_1^{f_1}S^{v'} \bmod n$ 和 $N_I=\zeta^{f_0+f_1 2^{l_f}} \bmod \Gamma$（其中：$l_f$ 为 f_0 和 f_1 的位数，$\zeta_I=(H_\Gamma(1\|bsn_I))^{(\Gamma-1)/\rho} \bmod \Gamma$，$bsn_I$ 为用户管理中心的 DAA 发布者基名），并将 U、N_I 和身份证明 $I_U=H(U_S\|P_S\|U\|N_I)$发送给用户管理中心。

(5)用户管理中心验证 I_U 中(U_S,P_S,U,N_I)的正确性，根据服务器帐户中记录的用户(j,k)，验证 k 是否在有效期内，依据等级 j 对应的发布者公钥，用 N_I 检查该用户的(f_0,f_1)是否在记录着所有已泄漏(f_0,f_1)的黑名单中，通过知识证明验证 U 和 N_I 确实由(f_0,f_1,v')计算产生。由于使用了基于离散对数的知识证明，用户管理中心并不能获得(f_0,f_1,v')。

(6)用户管理中心选择一个随机整数 v''和一个随机素数 e，计算 $A'=\left(\frac{Z}{US^{v''+k}}\right)^{1/e} \bmod n$，然后将($A'$,$e$,$v''$)发送给匿名登录器。$A'$相当于 DAA 方案中的 A，但不同的是，A'中包含了时限值 k。

(7)匿名登录器通过知识证明验证 A'的正确性，将(f_0,f_1,A',e,$v=v'+v''$)存储在本地账户中，(A',e,v)成为该用户

关于(f_0,f_1)的DAA证书。以后用户每次使用TG-ARIRS系统时只需登录本地帐户，匿名登录器将自动完成对检索服务子系统的匿名登录过程。

3.3 匿名登录

(1)每次进行匿名登录时，匿名登录器首先从登录验证服务器获得一个用于防范重放攻击的临时值n_v和一个验证者基名bsn_v，然后计算$\zeta_v=(H_\Gamma(1\|bsn_v))^{(\Gamma-1)/\rho} \bmod \Gamma$和$N_v=\zeta_v^{f_0+f_1 2^{l_f}} \bmod \Gamma$，选择随机整数$w,r$，计算$T_1=A'h^w \bmod n$和$T_2=g^w h^e (g')^r \bmod n$。

(2)匿名登录器计算相关的知识证明值$\tilde{T}_1,\tilde{T}_2,\tilde{T}_{2'}$ $N_{v'}$[9]，并由此产生散列值c'。c'相当于DAA方案中的c，但不同的是，c'的计算不包含AIK公钥m，新包含了等级值j和时限值k。

$$c'=H((n\|g\|g'\|h\|R_0\|R_1\|S\|Z\|\gamma\|\Gamma\|\rho)\|\xi_v\|(T_1\|T_2)\|N_v\|(\tilde{T}_1\|\tilde{T}_2\|\tilde{T}'_2)\|N_{v'}\|n_v\|j\|k)$$

(3)匿名登录器计算相关的知识证明值$(s_v,s_{f_0},s_{f_1},s_e,s_{e'},s_w,s_{ew},s_r,s_{er})$[9]，并生成DAA签名$\sigma'$，与DAA方案不同，$\sigma'$中包含了$j$和$k$。

$$\sigma'=(\zeta_v,(T_1,T_2),N_v,c,(s_v,s_{f_0},s_{f_1},s_e,s_{e'},s_w,s_{ew},s_r,s_{er}),j,k)$$

(4)匿名登录器将σ'发送给登录验证服务器，登录验证服务器使用等级j对应的发布者公钥，通过知识证明可以验证T_1,T_2来自于一个DAA证书，N_v由伴随此证书的秘密(f_0,f_1)产生，且时限值k在有效期内。尽管匿名登录器产生的σ'和c'与DAA方案有所不同，但知识证明的方法却是一样的。由于使用了基于离散对数的知识证明，登录验证服务器不能获得(f_0,f_1,v)或(A',e)。

(5)登录验证服务器用N_v检查该用户的(f_0,f_1)是否在记录着所有已泄漏(f_0,f_1)的黑名单中。若一切正常，则匿名登录成功，登录验证服务器将给该用户分配一个临时内部标识和对应于等级j的访问权限，检索服务器将允许该用户按权限使用。

4 安全性与匿名性

4.1 安全性分析

(1)DAA方案的安全性分析见文[9]，本文不再讨论与其处理相同或对安全性没有影响的修改部分的安全性。用户获得M_U、缴纳会费和建立服务器帐户的过程，可通过PKIX证书、离线或E-mail等方式进行，其安全性也不再讨论。

(2)即使攻击者截取了匿名登录器与用户管理中心之间的所有通信，也无法冒充合法用户。由于攻击者不能从截取的信息中得到(U_S,P_S)，无法为自己产生的假秘密数(f_0,f_1)生成I_U，因而无法向用户管理中心申请关于假(f_0,f_1)的DAA证书。由于攻击者不知道(f_0,f_1)，无法自己产生合法的DAA签名σ'，因而无法通过登录验证服务器对σ'的验证。由于c'的计算包含了登录验证服务器提供的临时值n_v，因而攻击者重放合法用户的DAA签名σ'也无法通过登录验证服务器的验证。

(3)若攻击者篡改了(j,k,PK_{I_j},S_G)或重放其他用户的(j,k,PK_{I_j},S_G)，由于S_G是用户管理中心的私钥签名，且散列值计算中包含了该用户的(U_S,P_S)，因而无法通过用户对$H((U_S\|P_S)\|j\|k\|(n\|g'\|g\|h\|S\|Z\|R_0\|R_1\|\gamma\|\Gamma\|\rho))$的正确性检验。

(4)由于服务器帐户中记录着每个用户的(j,k)，且每个用户等级对应的发布者公钥PK_{I_j}不同，因而用户无法申请其他等级的DAA证书，也无法在时限过期后申请DAA证书。

(5)匿名登录时，由于不同用户等级对应的发布者公钥不同，用户若在DAA签名中使用了虚假的等级j值，将无法通过登录验证服务器的知识证明验证。由于A'的计算中包含了k，用户若在DAA签名中使用了虚假的时限值k，将无法通过登录验证服务器对DAA证书的知识证明。

4.2 匿名性分析

从上述匿名登录方案的处理流程可以清楚地看到，虽然每个用户都要在检索服务子系统中注册一个服务器账户，匿名登录器在向用户管理中心申请DAA证书时也要使用该账户，但由于用户只需向用户管理中心申请一次DAA证书，以后的每次登录不再使用该账户，而是使用DAA证书，因而检索服务子系统并不能根据用户的服务器账户确定登录者的身份。在每次登录时，尽管DAA签名的验证者登录验证服务器与DAA证书的发布者用户管理中心是同一实体，但由于无法获得(f_0,f_1,v,A',e)，而(T_1,T_2)的值又随着(w,r)的不同而变化，只要bsn_v不是一个长期固定值(事实上，在GT-APIRS系统的登录验证服务器中包含着一个用于定时更新bsn_v的定时器)，检索服务子系统就无法获得能唯一对应于用户的值，从而实现了用户登录的匿名性。

与DAA方案只有一个匿名组不同，上述方案实现的是基于用户等级和时限的匿名。检索服务子系统将用户划分为$n_j\times n_k$个匿名小组(其中n_j为系统划分的用户等级个数，n_k为系统划分的时限个数)，由于登录验证服务器知道用户的等级和时限，因而知道用户属于哪个匿名小组，但无法知道用户具体是该组的哪个成员。从表面上看，这种方案的匿名强度似乎不如DAA方案。但事实上，当匿名小组的成员数达到一定规模后，成员数就不再是影响匿名强度的重要因素，真正决定匿名强度的因素还是匿名实现机制，此时该方案的匿名强度与DAA方案基本相同，这一点可从后面的实验结果中得到验证。

检索服务子系统可根据用户规模灵活调整匿名小组的划分粒度，以保证每个匿名小组具有匿名强度所要求的规模。例如：在系统投入商业运行的初期，由于用户数较少，为了吸引用户，可给予所有用户最高用户等级，时限值也设置为一个固定日期(如1年后的某一天)，这时在检索服务子系统中只有一个匿名小组，匿名组的规模与DAA方案完全相同。当用户规模较大时，再适当增加用户等级和划分较细粒度的时限。从上述匿名方案的处理流程可以看到，这一过程是平滑的，不会对已有用户产生任何影响。

对于检索服务子系统利用IP地址跟踪确定用户身份的问题，用户可采用代理服务器、分布式匿名网络和动态IP地址等方式隐藏自己的IP地址，用户的匿名性仍然可以得到保持。

4.3 实验结果

在实现GT-APIRS原型系统的匿名登录功能后，我们对匿名效果进行了测试。为了实验方便，我们将登录验证服务器中bsn_v的更新周期设置为1天，并为用户个性化子系统和检索服务子系统分别增加了分类日志的保存功能，分类日志保存了一个bsn_v更新周期内用户个性化子系统/检索服务子系统所观察到的用户操作记录和查询表达式。其中用户个性化子系统分类日志的内容是基于用户身份(本地账号)的，而检索服务子系统分类日志的内容是基于用户可变假名N_v、等级j值和时限值k的。具体实验过程如下：

(1)随机选取3个用户样本组，每组$n_i(1\leqslant i\leqslant 3)$个用户，$n_1=20,n_2=40,n_3=150$。一个测试周期为30天，不要求用户每天都必须参加测试，但每个用户在一个测试周期内至少

参加 20 次测试，且每次测试有足够的查询强度。

(2)只设置 1 个用户等级值和 1 个时限值(如：$j=1,k=20080318$)。一个测试周期后，分别对各组的 30 个检索服务子系统分类日志进行用户相似性比较，推算出每组的 n_i 个用户跟踪链。对照用户个性化子系统分类日志，求出每组检索服务子系统分类日志的 n_i 个真实用户链。其中，$20\leqslant$一个跟踪/真实用户链的项数$\leqslant 30$。

(3)计算每个样本组中用户跟踪链的单项平均正确率 r_{items} 和全链正确率 r_{series}，实验结果如表 1 所示，计算公式为：

$$r_{items}=\frac{\sum_{1}^{n_i} q_{ci}}{\sum_{1}^{n_i} q_{ti}}$$

q_{ci} 为一个用户跟踪链的正确项数，q_{ti} 为一个真实用户链的项数。

$r_{series}=q_{cs}/n_i$，q_{cs} 为全链正确的用户跟踪链个数。

表 1　各样本组的匿名性测试结果

用户样本组	r_{item}	r_{chain}
第 1 组	61.3%	35.0%
第 2 组	34.7%	2.5%
第 3 组	14.1%	0.0%

(4)设置 2 个用户等级值和 2 个时限值(如：$j_1=1,j_2=2,k_1=20080318,k_2=20090318$)，将第 3 组的用户划分为 4 个匿名小组，其中：j_1k_1 组 10 人，j_1k_2 组 20 人，j_2k_1 组 40 人，j_2k_2 组 80 人。一个测试周期后，计算每个匿名小组中用户跟踪链的单项平均正确率 r_{items} 和全链正确率 r_{series}，实验结果如表 2 所示。

实验结果表明，当用户数很少时，系统的匿名性效果还不能得到有效体现。但是随着用户数的增加，系统的匿名性效果迅速增强，检索服务子系统难以区分和跟踪某一特定用户。系统将用户划分为多个等级和时限后，若匿名小组的成员数很少，匿名性效果就会显著下降。但随着匿名小组中成员数的增加，匿名性效果又迅速增强。事实上，实际运行的个性化服务系统的用户数远远高于实验中的用户数，每个匿名小组拥有足够多的成员数，而且随着用户数的增加，还会出现许多用户模型相似的用户，这些用户更加难以区分。因此，系统的匿名性是可以得到保证的。

表 2　各匿名小组的匿名性测试结果

匿名小组	r_{item}	r_{chain}
j_1k_1 组	93.2%	70.0%
j_1k_2 组	65.7%	30.0%
j_2k_1 组	38.6%	5.0%
j_2k_2 组	22.8%	0.0%

此外，尽管匿名登录需要花费一定的时间代价(我们用一组 2.8 GHz Intel P4 CPU，1 GB RAM 的台式计算机进行了测试，匿名登录过程大约需要 3.8 秒)，但由于匿名登录是在用户本地登录到用户个性化子系统后自动进行的一次性后台事件，此时用户还需要输入查询关键字才能开始首次查询，因而匿名登录的时间代价对用户而言并不是一个严重问题。对于检索服务子系统而言，用户的匿名登录由登录验证服务器专门处理，与检索服务器无关，因而不会影响检索服务的性能。

5　与 DAA 方案的比较

现有 DAA 方案是为可信计算环境设计的，其算法实现依赖于可信平台模块的硬件加密和签名功能，并在申请 DAA 证书时要使用可信平台模块的 RSA 背书密钥，这就要求用户节点必须是嵌入了可信平台模块的可信计算机，因而不支持非可信计算环境。在 GT-APIRS 系统的匿名认证方案中，匿名证书申请过程是通过基于服务器帐户的一系列安全处理来实现的，不需要用户拥有自己的密钥对和第三方证书，可信平台模块和主机两个实体的功能也由匿名登录器这一软件实体来实现。因而，该方案是一个面向通用网络环境的软件实现方案。GT-APIRS 系统的匿名登录过程是基于 DAA 原理的，但在 DAA 方案中，用户向发布者申请一次证书后，就可无限制地匿名访问服务系统。为了解决等级会费制系统中既要确定用户付费期限和访问权限又要继续保持匿名的问题，新方案在发布者公钥、匿名证书、登录签名和相关知识证明中都加入了对用户等级和时限的处理。

通过第 4 节的安全性分析可以看到，对安全性有影响的改进部分仍然是安全的，因而新方案具有与 DAA 方案等价的安全性。通过匿名性分析和实验结果可以看到，尽管匿名组的划分粒度变细，但仅在用户规模较小时对匿名强度有影响，当用户规模较大时该方案与 DAA 方案具有等价的匿名性。

结论　个性化服务需要收集用户的个人信息，这些信息包含着用户隐私，可能造成隐私泄漏，匿名访问是解决这一问题的主要技术手段。但对于商业付费系统而言，用户付费期限和访问权限的管理增加了匿名保持的困难性。为了解决这一问题，本文提出了一个 GT-APIRS 系统模型和一种面向等级会费制个性化服务的匿名认证方案。个性化处理运行于客户端，检索服务运行于服务器端，用户匿名登录服务器，服务提供者能够知道用户是否付费且具有何种权限，但无法区分用户的具体身份，该方案可满足付费个性化服务的隐私保护需要。

参 考 文 献

1　Mladenic D. Machine learning for better Web browsing. In: AAAI 2000 Spring Symposium Technical Reports on Adaptive User Interfaces, AAAI Press, 2000. 82～84

2　Mobasher B, Cooley R, Srivastava J. Automatic personalization based on Web usage mining. Communications of the ACM, 2000, 43(8): 142～151

3　潘金贵，胡学联，李俊，等. 一个个性化的信息搜集 Agent 的设计与实现. 软件学报，2001, 12(7): 1074～1079

4　Teltzrow M, Kobsa A. Impacts of user privacy preferences on personalized systems: A comparative study. In: Designing Personalized User Experiences for eCommerce, Kluwer Academic Publishers, 2004. 315～332

5　Saito T, Umesawa K, Okuno H. Privacy-enhanced access control by SPKI and its application to Web server. In: Proc. of IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, IEEE Computer Society, 2000. 201～206

6　Saito T, Umesawa K, Kito T, et al. Privacy-enhanced SPKI access control on PKIX and its application to Web server. In: Proc. of the 17th International Conference on Advanced Information Networking and Application, IEEE Computer Society, 2003. 696～703

7　Kakizaki Y, Yamamoto H. A proposal of an anonymous authentication method for flat-rate service. In: Proc. of the First International Conference on Availability, Reliability and Security, IEEE Computer Society, 2006. 551～557

8　Teranishi I, Furukawa J, Sako K. k-times anonymous authentication. In: ASIACRYPT 2004, LNCS 3329, Springer-Verlag, 2004. 308～322

9　Brickell E, Camenisch J, Chen L. Direct anonymous attestation. In: Proc. of the 11th ACM Conference on Computer and Communications Security, ACM Press, 2004. 132～145

10　Trusted Computing Group. TPM main part 1 design principles specification version 1.2. http://www.trustedcomputinggroup.org, 2003

11　Camenisch J, Lysyanskaya A. A signature scheme with efficient protocols. In: Proc. of the Third International Conference on Security in Communication Networks, LNCS 2576, Springer Verlag, 2003. 268～289

12　Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems. In: Advances in Cryptology — CRYPTO '86, LNCS 263, Springer-Verlag, 1987. 186～194