普适环境中基于一次性公钥的匿名认证方案

罗长远[1]，霍士伟[2]，邢洪智[1]
(1. 信息工程大学 电子技术学院，河南 郑州 450004；2. 西安通信学院，陕西 西安 710106)

摘 要：提出一种基于身份的一次性公钥及签名算法，与现有算法相比，该算法具有较小的计算和通信开销。基于该算法设计了一种普适环境中的匿名认证方案，当用户进行恶意操作时，服务提供者通过和可信中心合作可以揭示恶意用户身份。方案在提供强匿名性的同时，可有效防止用户进行恶意活动。

关键词：普适计算；匿名认证；一次性公钥；基于身份的密码体制
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2012)02-0093-06

Anonymous authentication scheme based on one-off public key in pervasive computing environments

LUO Chang-yuan[1], HUO Shi-wei[2], XING Hong-zhi[1]
(1.Electronic Technology Institute, Information Engineering University, Zhengzhou 450004, China;
2.Xi'an Communications Institute, Xi'an 710106, China)

Abstract: A signature scheme with the one-off public key was proposed based on identity-based cryptography, which had less calculating and communicating expense compared with available schemes. An anonymous authentication scheme was designed based on the proposed signature scheme. When users committed, service provider together with the trusted center could reveal the malicious user's identity. The proposed scheme can realize strong anonymity and prevent the user committing.

Key words: pervasive computing; anonymous authentication; one-off public key; identity-based cryptography

1 引言

普适计算是一种开放的网络环境，用户可以随时随地获得服务。开放性和无所不在性使普适环境相对于传统网络更容易受到各种恶意攻击。为了保证普适环境的安全，需要实施加密、访问控制等安全措施。其中认证是各种安全措施的基础，对构建安全的普适环境具有重要意义[1]。

普适环境中存在大量不可见的设备(如传感器)，它们不停地搜集用户的身份、位置等敏感信息，用户的敏感信息随时有被泄露的可能。所以，普适环境下用户的隐私保护被提到了重要的高度[2]。在认证中，同样需要考虑用户隐私保护的问题。现有的认证机制需要用户提供身份信息，这会造成用户身份信息泄露，使用户的会话和位置被恶意实体跟踪。为了保护用户隐私，普适环境下的认证方案在实现安全认证的基础上要满足以下要求[2]：1) 用户匿名性，在认证过程中，服务方和外部用户都无法确定用户的真实身份；2) 无关联性，服务方和外部用户都无法确定不同的会话来自相同的用户。另外

收稿日期：2011-03-25；**修回日期**：2011-11-25
基金项目：国家高技术研究发展计划(“863”计划)基金资助项目(2009AAJ124)；现代通信国家重点实验室基金资助项目(9140C1107020905)
Foundation Items: The National High Technology Research and Development Program of China(863 Program)(2009AAJ124); The National Laboratory for Modern Communications Project Foundation (9140C1107020905)

由于普适环境下用户一般使用计算能力有限的便携设备，因此认证方案要满足用户端计算量小的要求[3]。

文献[4]提出了一种普适环境中的匿名认证和密钥协商方案，该方案需要证书的支持，证书管理开销较大。文献[5]基于椭圆曲线上的离散对数问题提出了一种普适环境中的匿名认证和密钥协商方案，具有较小的计算开销。文献[4,5]中方案只能实现对外部用户匿名，而服务方可以确定用户身份，无法满足用户的强匿名需求，即用户希望在认证过程中，外部用户和服务方都无法确定自己的身份，从而更好地保护隐私。文献[2]利用盲签名技术设计了一种新的普适环境中的匿名认证方案，方案可以满足强匿名要求。文献[6]在文献[2]方案的基础上增加了抵御拒绝服务攻击的功能。文献[7]指出文献[2]方案存在安全缺陷，非法用户可以假冒合法用户通过认证，并对方案进行了改进，使方案可以避免假冒攻击。

上述基于盲签名的匿名认证方案在认证过程中保证了用户的身份无法被外部用户和服务方获得，有效保护了用户隐私。但是由于盲签名的不可追踪性，当合法用户进行恶意活动时，服务方仍然无法确定用户的身份，给犯罪分子带来可乘之机[8]。针对盲签名的缺点，研究者提出了一次性公钥的思想[8]。在一次性公钥中，可信中心只需给用户生成一次私钥，用户每次签名时可以生成不同的公钥，使得用户的每次签名之间不存在关联性，从而保证了用户身份匿名性和会话无关联性。此外，在必要时签名验证者可以向可信中心递交签名者的一次性公钥，可信中心可以揭示签名者身份，防止签名者进行恶意活动。文献[9]提出了基于身份的一次性公钥及签名算法，但是该算法是可伪造的，非法用户利用合法用户的一次性公钥可以伪造签名。文献[10]提出了一种新的基于身份的一次性公钥及签名算法，并证明了算法的安全性。上述基于身份的一次性公钥及签名算法需要多次双线性对运算，一次性公钥长度较长，这会造成较大的计算开销和通信开销，不适合在资源受限的普适环境下应用。并且上述算法都存在密钥托管问题，可信中心的主密钥如果被恶意实体获得，恶意实体就可以计算出合法用户的签名私钥，从而可以冒充合法用户。所以方案中的系统主密钥成为安全瓶颈。本文提出了一种新的基于身份的一次性公钥及签名算法，在保证安全性的基础上，通过对算法优化，减少了双线性对运算次数和一次性公钥长度，并且不存在密钥托管问题。基于该算法设计了普适环境中的匿名认证方案，在提供强匿名性的同时，能够防止用户进行恶意活动。

2 基于身份的一次性公钥及签名算法

2.1 算法设计

本算法基于双线性对运算实现，包括以下算法。

1) 系统初始化

可信中心 TC 选择椭圆曲线上满足双线性对要求 e、G_1、G_2、q，G_1 的生成元为 P。随机选择 $s \in Z_q^*$ 作为系统主密钥，系统公钥为 $P_{\text{pub}} = sP$。定义安全的散列函数：$H_1 : \{0,1\}^* \times G_1 \to Z_q^*$ 和 $H_2 : \{0,1\}^* \to Z_q^*$。TC 妥善保管 s，公开系统参数 $\{G_1, G_2, e, q, P, P_{\text{pub}}, H_1, H_2\}$。

2) 用户私钥生成

假设用户 A 的身份标识为 ID_{A}，随机选择 $x_{\text{A}} \in Z_q^*$ 作为秘密数，计算 $R_1 = x_{\text{A}}P$，然后将 R_1 和 ID_{A} 发送给 TC，TC 可以通过零知识证明方法确认 A 具有与 R_1 对应的秘密数 x_{A}。TC 对用户身份和 R_1 鉴定后，按如下步骤计算用户 A 的部分私钥：

① 随机选择 $r_{\text{A}} \in Z_q^*$，计算 $R_2 = r_{\text{A}}P$，$R_{\text{A}} = R_1 + R_2$；

② 令 $c = H_1(ID_{\text{A}}, R_{\text{A}})$，计算部分私钥 $d_{\text{A}} = r_{\text{A}} + sc$。

TC 保存 $(ID_{\text{A}}, c, R_{\text{A}})$，用作以后确认 A 的身份。将 R_{A} 和 d_{A} 通过安全信道发送给 A。A 计算 $s_{\text{A}} = x_{\text{A}} + d_{\text{A}}$ 作为完整私钥，通过检验 $s_{\text{A}}P = R_{\text{A}} + H_1(ID_{\text{A}}, R_{\text{A}})P_{\text{pub}}$ 是否成立来验证私钥的正确性，验证通过后 A 妥善保存 $(s_{\text{A}}, R_{\text{A}})$。

3) 一次性公钥生成

如果 A 要与 B 通信，需要构造一次性公钥。A 随机选择 $a \in Z_q^*$，计算 $P_{\text{A}} = as_{\text{A}}P$，$U_{\text{A}} = aR_{\text{A}}$，$V_{\text{A}} = acP(c = H_1(ID_{\text{A}}, R_{\text{A}}))$。$(P_{\text{A}}, U_{\text{A}}, V_{\text{A}})$ 称为用户 A 的一次性公钥，A 将 $(P_{\text{A}}, U_{\text{A}}, V_{\text{A}})$ 发送给 B。

4) 签名

用户 A 对消息 $m \in \{0,1\}^*$ 签名时，随机选择 $y \in Z_q^*$，计算 $Y = yP$，计算 $h = H_2(m, Y)$，计算

$z = y + as_{\mathrm{A}}h$，签名为$< z,Y >$，A 将签名$< z,Y >$和消息 m 发送给验证者 B。

5) 验证

B 首先验证一次性公钥的合法性，验证等式

$$e(P_{\mathrm{A}},P) = e(U_{\mathrm{A}},P)e(V_{\mathrm{A}},P_{\mathrm{pub}}) \tag{1}$$

是否成立，若成立则确定发送方确实在可信中心进行了注册。

因为

$$\begin{aligned} &e(P_{\mathrm{A}},P) = e(as_{\mathrm{A}}P,P) = e(a(x_{\mathrm{A}} + d_{\mathrm{A}})P,P)\\ &= e(a(x_{\mathrm{A}} + r_{\mathrm{A}} + sc)P,P)\\ &= e(a(x_{\mathrm{A}}P + r_{\mathrm{A}}P) + ascP,P)\\ &= e(a(R_1 + R_2) + ascP,P)\\ &= e(aR_{\mathrm{A}} + ascP,P)\\ &= e(aR_{\mathrm{A}},P)e(ascP,P)\\ &= e(U_{\mathrm{A}},P)e(V_{\mathrm{A}},P_{\mathrm{pub}}) \end{aligned}$$

若等式成立，则说明 P_{A} 含有系统主密钥，因此发送方在可信中心进行过注册。

然后 B 验证签名，计算 $h = H_2(m,Y)$，验证等式

$$zP = Y + hP_{\mathrm{A}} \tag{2}$$

是否成立。若成立，则验证通过，否则拒绝。

2.2　算法安全性分析

1) 算法可保证发送方匿名

首先，用户 A 的一次性公钥和签名中不包含身份信息。其次，用户 A 的一次性公钥$(P_{\mathrm{A}},U_{\mathrm{A}},V_{\mathrm{A}})$都经过了随机数 a 的处理，a 不同则一次性公钥不同，因此用户 B 无法获得 A 的真实身份，并且 A 的不同活动之间不存在任何联系。

2) 算法可保证匿名用户的可追踪性

如果用户 A 执行了非法的操作，验证者 B 通过和可信中心合作，可以揭示用户 A 的真实身份。用户 B 只需要将$U_{\mathrm{A}},V_{\mathrm{A}}$发送给 TC，TC 就可以揭示 A 的身份。因为 TC 保存了 A 的相关信息$(ID_{\mathrm{A}},c,R_{\mathrm{A}})$，TC 通过验证

$$e(U_{\mathrm{A}},cP) = e(V_{\mathrm{A}},R_{\mathrm{A}}) \tag{3}$$

是否成立来揭示用户 A 的身份。事实上，$e(U_{\mathrm{A}},cP) = e(aR_{\mathrm{A}},cP) = e(acP,R_{\mathrm{A}}) = e(V_{\mathrm{A}},R_{\mathrm{A}})$。因此，该算法既保证了用户 A 的匿名性，也可以防止用户 A 进行恶意的活动。

3) 算法可抵御伪造攻击

① 合法用户 A 无法伪造虚假的一次性公钥和签名来欺骗用户 B

首先，对消息 m 的签名 z 无法伪造。因为，通过验证等式(1)，B 确定 P_{A} 中含有系统主密钥 s，通过验证等式(2)，可以确定 z 含有主密钥 s，因此 z 是利用合法的私钥生成的，z 不可伪造。其次，P_{A} 无法伪造，由于 z 是利用合法的私钥生成的，如果 P_{A} 是伪造的，则等式(2)无法验证通过。同样U_{A}和V_{A}无法伪造，由于 P_{A} 是按照正确的步骤生成的，如果 U_{A} 和V_{A}是伪造的，则无法通过等式(1)的验证。

其次，A 企图消灭进行恶意活动的证据，即躲开式(3)的检查是不可行的。假设 A 选择 $a,b \in Z_q^*(a \neq b)$，计算 $P_{\mathrm{A}} = aR_{\mathrm{A}} + bcP_{\mathrm{pub}}$，$U'_{\mathrm{A}} = aR_{\mathrm{A}}$，$V'_{\mathrm{A}} = bcP$ 作为一次性公钥，此时可以通过式(1)验证且式(3)无法成立。但是，A 无法生成相应的签名私钥 $a(x_{\mathrm{A}} + r_{\mathrm{A}}) + bsc$ 对 m 进行签名，因此无法通过式(2)验证。因此，A 无法伪造虚假的一次性公钥和签名来进行恶意活动。

② 非法用户 C 无法伪造虚假的一次性公钥和有效的签名

首先，C 无法任意选择 $a,b \in Z_q^*$，计算 $P_{\mathrm{C}} = aP + bP_{\mathrm{pub}}$，$U_{\mathrm{C}} = aP$，$V_{\mathrm{C}} = bP$，将$(P_{\mathrm{C}},U_{\mathrm{C}},V_{\mathrm{C}})$作为自己的一次性公钥。虽然$(P_{\mathrm{C}},U_{\mathrm{C}},V_{\mathrm{C}})$可以通过式(1)验证，但是 C 无法计算出相应的签名私钥 $a + bs$ 生成正确的签名，因此无法通过式(2)验证。

其次，C 无法利用合法用户 A 的公开信息$(P_{\mathrm{A}},U_{\mathrm{A}},V_{\mathrm{A}})$和对消息 m 的签名$< z,Y >$进行伪造。C 如果选择 $b \in Z_q^*$，计算 $P_{\mathrm{C}} = bP_{\mathrm{A}}$，$U_{\mathrm{C}} = bU_{\mathrm{A}}$，$V_{\mathrm{C}} = bV_{\mathrm{A}}$，将$(P_{\mathrm{C}},U_{\mathrm{C}},V_{\mathrm{C}})$作为自己的一次性公钥。虽然$(P_{\mathrm{C}},U_{\mathrm{C}},V_{\mathrm{C}})$可以通过式(1)验证，但是 C 无法计算出相应的签名私钥bas_{A}生成正确的签名。因为通过 $P_{\mathrm{A}} = as_{\mathrm{A}}P$ 获得 as_{A} 面临解决椭圆曲线群上的离散对数问题，而通过 $z = y + as_{\mathrm{A}}h$ 获得 as_{A} 首先要获得 y，y 没有公开传送，要通过 $Y = yP$ 获得 y 同样面临解决椭圆曲线群上的离散对数问题。因此 C 无法生成正确签名通过式(2)验证。

4) 算法无密钥托管

在算法中，用户 A 的完整私钥为 $s_{\mathrm{A}} = x_{\mathrm{A}} + d_{\mathrm{A}}$，其中，$d_{\mathrm{A}}$ 是 TC 为用户产生的部分私钥，x_{A} 是用户自己选择的秘密数构成另一部分私钥。x_{A} 是保密的，其他用户包括 TC 都无法获得 x_{A}。即使获得 TC 的主密钥，由于无法获得 x_{A}，仍无法得到用户

表 1　　**算法效率比较**

密码运算	文献[9]算法	文献[10]算法	本文算法
发方生成一次性公钥	5Pm	4Pm	3Pm
发方生成签名	1P+2Pm+1Pa+1MtP	1Pm+1MtP	1Pm
收方验证公钥	7P+1Gm	5P+1Gm	3P+1Gm
收方验证签名	1Pm +2P+1Gm+1MtP	2P+1MtP	2Pm +1Pa
一次性公钥长度	$G_1\times G_1\times G_1\times G_1\times G_1$	$G_1\times G_1\times G_1\times G_1$	$G_1\times G_1\times G_1$
签名长度	$G_1\times G_2$	G_1	$G_1\times Z_q^*$

A 的完整私钥，因此本算法不存在密钥托管问题。

2.3　算法效率分析

以下将对算法的计算开销和通信开销进行分析，并与文献[9,10]中的算法进行比较，如表 1 所示。考虑的运算包括双线性对运算(P)、G_1 上的点乘运算(Pm)、G_1 上的点加运算(Pa)、G_2 上的点乘运算(Gm)和映射到椭圆曲线上点的散列运算(MtP)，相对于这些运算，其他运算可以忽略不计[10]。

由表 1 中数据可以看出，本算法具有更小的计算开销，同时本算法的一次性公钥和签名长度较短，因此通信开销较小，所以本算法具有更高的执行效率，更适合在普适环境中应用。

3　普适环境中基于一次性公钥的匿名认证方案

3.1　方案设计

系统包括 3 类实体：可信中心(TC)、用户(A)和服务提供者(SP)。TC 负责为系统中的合法用户签发基于身份的私钥，并在服务提供者出示用户恶意活动证据的情况下，揭示用户的身份。服务提供者在为用户提供服务前，要对用户进行认证，确认用户的合法性，即用户拥有 TC 签发的私钥。同时用户也要确认服务提供者是合法的。在认证过程中要满足以下要求。首先，服务提供者和其他实体都无法确定用户的真实身份，充分保护用户的隐私。另外，当用户进行恶意活动时，服务提供者通过和 TC 合作可以揭示用户身份。本方案的安全性基于以下假设，TC 是诚实可信的，即 TC 不会发送虚假的信息，不会利用掌握的用户密钥信息实施假冒攻击，不会随意向其他实体揭露用户的真实身份，除非合法的 SP 提供了某用户的恶意活动证据。

方案利用第 2 节中的一次性公钥及签名算法结合散列链认证技术来实现匿名认证。散列链认证技术可以减少签名次数，提高认证效率。方案中用户只需要在首次访问服务时执行一次性公钥及签名算法，在之后访问服务时利用散列链作为认证凭证。方案包括 4 个阶段：系统建立、私钥生成、认证和恶意用户身份恢复。

1) 系统建立

TC 按照 2.1 节中描述的方法产生系统参数，选定系统公私钥对 (s,P_{pub})，定义安全的散列函数：$H_1:\{0,1\}^*\times G_1\to Z_q^*$，$H_2:\{0,1\}^*\to Z_q^*$，$H_3:G_1\to\{0,1\}^*$，$H_4:\{0,1\}^*\to\{0,1\}^*$。并公布系统参数 $\{G_1,G_2,e,q,P,P_{\text{pub}},H_1,H_2,H_3,H_4\}$。

2) 私钥生成

私钥生成方法同 2.1 节中描述方法相同。用户 A 的身份标识为 ID_{A}，经过与 TC 交互 A 获得的完整私钥为 $s_{\text{A}}=x_{\text{A}}+d_{\text{A}}$，其中，$d_{\text{A}}=r_{\text{A}}+sc(c=H_1(ID_{\text{A}},R_{\text{A}}))$ 是 TC 为用户 A 生成的部分私钥，x_{A} 是用户 A 选择的秘密数，R_{A} 是 TC 为用户 A 生成的辅助参数。A 妥善保存 $(s_{\text{A}},R_{\text{A}})$，TC 保存了与用户 A 身份相关的信息 $(ID_{\text{A}},c,R_{\text{A}})$。SP 的长期私钥为 $s_P\in Z_q^*$，SP 的公钥为 $PK_P=s_PP$，SP 妥善保存 s_P，将 PK_P 向全网公开。

3) 认证

当用户 A 第一次要求 SP 提供服务时，通过以下步骤向 SP 证明自己是合法用户。

step1　用户 A 随机选择 $x\in\{0,1\}^*$，计算 $C_0=H_4(x)$，$C_i=H_4^i(C_0),1\leqslant i\leqslant n$，A 安全的保存所有的散列值，散列值的计算可以利用空闲时间离线完成。用户 A 随机选择 $a\in Z_q^*$，计算 $P_{\text{A}}=as_{\text{A}}P$，$U_{\text{A}}=aR_{\text{A}}$，$V_{\text{A}}=acP(c=H_1(ID_{\text{A}},R_{\text{A}}))$，得到一次性

公钥$W_A=(P_A,U_A,V_A)$。A 获取当前时间戳T_A，随机选择$y_A\in Z_q^*$，计算$Y_A=y_AP$，$Y'_A=y_APK_P$，$h=H_2(C_n,T_A,Y_A)$，计算签名$z=y_A+as_Ah$。A 计算$k=H_3(Y_A)$并保存k，加密C_n得$\sigma=C_n\oplus k$，向 SP 发送消息$<T_A,W_A,Y'_A,z,\sigma>$。

step2　SP 收到消息后，检查时戳T_A的新鲜性，若T_A新鲜，则按照 2.1 节中方法验证一次性公钥W_A是否合法。验证通过后，SP 计算$Y_A=s_P^{-1}Y'_A$，计算$k=H_3(Y_A)$，解密$C_n=\sigma\oplus k$，验证签名$zP=Y_A+H_2(C_n,T_A,Y_A)P_A$是否成立。验证通过后，则确认 A 为合法用户。SP 将C_n保存到一个列表 L 中。SP 选择$y_P\in Z_q^*$，计算$Y_P=y_PP$，计算会话密钥$k_{AP}=H_3(y_PY_A)$，获取当前时间戳T_P，向 A 发送消息$<T_P,E_k(Y_P,T_P,T_A)>$，E为对称加密算法。

step3　A 收到消息后，检查时戳T_P的新鲜性，若新鲜，则利用k解密$E_k(Y_P,T_P,T_A)$并核对T_P和T_A是否一致。若一致，则通过对 SP 的认证，然后计算$k_{AP}=H_3(y_AY_P)$，并把k_{AP}作为之后通信的会话密钥。

当用户再次要求 SP 提供服务时，可以利用保存的散列值$C_i,0\leqslant i<n$作为认证凭证，不需要构造一次性公钥及签名，SP 仅需要进行简单的散列运算就可以实现对用户 A 的认证，利用散列链进行认证可以减少认证的计算开销和通信开销。以用户 A 的第 2 次认证为例，具体过程如下。

step1　A 随机选择$y_A\in Z_q^*$，计算$Y_A=y_AP$，$Y'_A=y_APK_P$，计算$k=H_3(Y_A)$并保存k，对C_{n-1}加密得$z=C_{n-1}\oplus k$，向 SP 发送消息$<Y'_A,z>$。

step2　SP 收到消息后，计算$Y_A=s_P^{-1}Y'_A$，$k=H_3(Y_A)$，解密$C_{n-1}=z\oplus k$，计算$H_4(C_{n-1})$，查找列表L中是否存在$H_4(C_{n-1})$，若存在则证明当前用户为已通过认证的合法用户，将列表L中的C_n替换为C_{n-1}。SP 选择$y_P\in Z_q^*$，计算$Y_P=y_PP$，计算会话密钥$k_{AP}=H_3(y_PY_A)$，获取当前时间戳T_P，向 A 发送消息$<T_P,E_k(Y_P,T_P,Y'_A)>$，E为对称加密算法。

step3　A 收到消息后，检查时戳T_P的新鲜性，若新鲜，则利用k解密$E_k(Y_P,T_P,Y'_A)$并核对T_P和Y'_A，若一致，则通过对 SP 的认证，然后计算$k_{AP}=H_3(y_AY_P)$，并把k_{AP}作为之后通信的会话密钥。

4) 恶意用户身份恢复

如果用户 A 在访问 SP 服务的过程中，进行了恶意操作，SP 将 A 的恶意操作证据和 A 的一次性公钥$W_A=(P_A,U_A,V_A)$发送给 TC。TC 首先验证 SP 提供的证据属实，然后利用保存的信息(ID_A,c,R_A)验证$e(U_A,cP)=e(V_A,R_A)$是否成立，若成立则证明进行恶意操作的用户为 A。

3.2　方案安全性分析

1) 双向认证

本方案可以实现用户 A 和服务提供者 SP 之间的双向认证。SP 可以确定当前请求访问服务的用户 A 是合法的。在 A 首次访问服务时，SP 通过验证 A 的一次性公钥及对C_n和T_A的签名完成对 A 的认证。由 2.2 节中分析可知一次性公钥及签名算法是安全的，同时签名中包含了时间戳可以保证签名的新鲜性，所以 SP 对用户 A 的认证是安全的。在用户之后访问服务时，SP 通过散列链来认证用户 A。以第 2 次认证过程为例，SP 通过验证$H_4(C_{n-1})$是否等于C_n来认证用户，由于C_n已经通过 SP 的认证，根据散列函数的单向计算特性，只有已通过认证的合法用户 A 才能出示正确的C_{n-1}。用户 A 也可以确定当前的服务提供者 SP 是合法的，A 通过解密$E_k(Y_P,T_P,T_A)$并核对T_P和T_A完成对 SP 的认证，因为只有合法的 SP 才能利用私钥由Y'_A计算出Y_A，进而计算出正确的密钥k。

2) 用户匿名性

在认证过程中，其他用户和 SP 都无法确定用户 A 的真实身份。用户 A 首次认证时，利用一次性公钥及对C_n和T_A的签名作为认证信息，根据一次公钥的匿名特性，其他用户和 SP 都无法根据认证信息确定用户 A 的真实身份。在之后的认证过程中，A 利用$C_i(0\leqslant i<n)$作为认证凭证，同样不会泄露 A 的身份。

3) 无关联性

对于外部用户，本方案具有完善的无关联性。A 提供的一次性公钥都经过随机数的处理，具有随机性，外部用户无法根据一次性公钥将不同的会话联系起来。虽然同一个散列链中的$C_i(0\leqslant i\leqslant n)$存在关联性，但是本方案对$C_i(0\leqslant i\leqslant n)$进行了加密处理，外部用户无法得到$C_i(0\leqslant i\leqslant n)$的明文，因此外部用户同样无法根据$C_i(0\leqslant i\leqslant n)$将不同的会话联系起来。对于 SP，本方案具有部分无关联性。由于 SP 可以解密获得$C_i(0\leqslant i\leqslant n)$的明文，SP 可以将利用同一个散列链认证的$n$个会话联系起来。由于不同散列链之间不存在联系，对于采用不同散列链认证的会话，SP 无法将其联系起来。

4) 安全的会话密钥建立

方案中用户和 SP 可以建立安全的会话密钥 k_{AP}。会话密钥是由双方选择的密钥协商参数 y_A 和 y_P 共同决定的，并且公开发送的 Y'_A 和加密传送的 Y_P 不会导致 y_A 和 y_P 的泄露，因此协商的密钥满足已知会话密钥安全、前向安全性和密钥控制安全。

5) 用户身份可追踪性

由于一次性公钥在提供匿名性的同时具有可追踪性，当用户 A 进行恶意活动后，SP 将 A 的一次性公钥提交给 TC，TC 利用保存的 (ID_A, c, R_A) 可以揭示用户 A 的身份。该特性可以有效防止用户进行非法操作。

将本方案与现有普适环境中的匿名认证方案进行安全性比较，结果如表 2 所示。其中，“Y”表示满足安全要求，“N”表示不满足，“P”表示部分满足(对服务提供者 SP 不满足)。由表 2 中数据可以看出，同文献[2,6,7]中方案相比，本方案在满足双向认证、用户匿名性等安全要求的同时，能够对恶意用户身份进行追踪，从而可以防止用户进行恶意活动。同文献[4,5]中方案相比，本方案具有更强的匿名性，而文献[4,5]中方案只能实现部分匿名性(对服务提供者 SP 不满足匿名性)。因此，本方案在安全性上优于其他方案。

表 2 安全性比较

安全特性	文献[2,6,7]方案	文献[4,5]方案	本方案
双向认证	Y	Y	Y
用户匿名性	Y	P	Y
无关联性	P	P	P
安全的会话密钥建立	Y	Y	Y
用户身份可追踪性	N	Y	Y

3.3 方案效率分析

本方案在认证过程中主要的计算开销来自于验证一次性公钥，需要 3 次双线性对运算，这些主要的运算由计算能力较强的服务提供者来完成，而用户只需要进行椭圆曲线上的点乘和点加运算，因此方案不会给用户端带来较大的计算开销，满足普适环境中用户端计算量小的要求。同时，本方案只需在用户首次认证时进行双线性对运算，在之后的访问中，只需要进行椭圆曲线上的点乘和点加运算，因此在多次访问过程中方案的平均计算开销较小。

4 结束语

为了保护用户隐私，普适环境下的认证方案需要满足用户匿名性要求。本文提出了一种基于身份的一次性公钥及签名算法，算法在保证安全性的基础上具有较小的计算和通信开销。基于该算法和散列链认证技术设计了一种普适环境中的匿名认证方案，在提供强匿名性的同时，可防止用户进行恶意活动。同现有普适环境中的匿名认证方案相比，本方案具有更好的安全性。

参考文献：

[1] YAO L, WANG L, KONG X W, *et al*. An inter-domain authentication scheme for pervasive computing environment[J]. Computers and Mathematics with Applications, 2010, 59(2):811-821.

[2] REN K, LOU W J, KIM K, *et al*. A novel privacy preserving authentication and access control scheme for pervasive computing environments[J]. IEEE Transactions on Vehicular Technology, 2006, 55 (4):1373-1384.

[3] FORNE J, HINAREJOS F, MARIN A, *et al*. Pervasive authentication and authorization infrastructures for mobile users[J]. Computers & Security, 2010, 29(4):501-514.

[4] KANG M H, RYOU H B, CHOI W C. Design of anonymity-preserving user authentication and key agreement protocol for ubiquitous computing environments[A]. International Workshop on Internet and Network Economics[C]. Hong Kong, China, 2005. 491-499.

[5] WANG R C, JUANG W S, WU C C, *et al*. A lightweight key agreement protocol with user anonymity in ubiquitous computing environments[A]. International Conference on Multimedia and Ubiquitous Engineering[C]. Seoul, Korea, 2007. 313-318.

[6] REN K, LOU W J. Privacy-enhanced, attack-resilient access control in pervasive computing environments with optional context authentication capability[J]. Mobile Networks and Applications, 2007, 12(1):79-92.

[7] LI C T, HWANG M S, CHU Y P. Further improvement on a novel privacy preserving authentication and access control scheme for pervasive computing environments[J]. Computer Communications, 2008, 31(18):4255-4258.

[8] 张秋璞，郭宝安. 基于 ID 的一次性盲公钥[J]. 电子学报, 2003, 31(5):669-771.
ZHANG Q P, GUO B A. One-off blind public key based on ID[J]. Acta Electronica Sinica, 2003, 31(5):669-771.

[9] 张胜，徐国爱，胡正名等. 一种基于身份一次性公钥的构造[J]. 电子与信息学报, 2006, 28(8):1412-1414.
ZHANG S, XU G A, HU Z M, *et al*. Construction of the one-off public key based on identity[J].Journal of Electronics&Information Technology, 2006, 28(8):1412-1414.

（下转第 109 页）

sensor networks[A]. Proc of 35th International Conference on Very Large Data Bases (VLDB)[C]. Lyon, France, 2009. 169-180.

[22] XU Y, LEE W, XU J, *et al*. Processing window queries in wireless sensor networks[A]. Proc of TEEE Intl Conf on Data Engineer (ICDE)[C]. Atlanta, GA, USA, 2006.70.

作者简介：

高静（1985-），女，黑龙江大兴安岭人，哈尔滨工业大学博士生，主要研究方向为无线传感器网络查询处理。

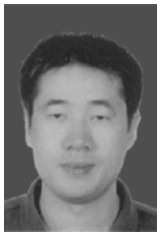
李建中（1950-），男，黑龙江哈尔滨人，哈尔滨工业大学教授、博士生导师，主要研究方向为海量数据管理、无线传感器网络和信息物理融合系统等。

刘禹（1981-），男，黑龙江哈尔滨人，哈尔滨工业大学博士生，主要研究方向为传感器网络、CPS 和移动对象数据管理。

（上接第 98 页）

[10] 刘宏伟, 谢维信, 喻建平等. 基于身份的公平不可否认协议[J]. 通信学报, 2009, 30(7):119-123.
LIU H W, XIN W X, YU J P, *et al*. Fare non-repudiation protocol based on identity-based cryptography[J]. Journal on Communications, 2009, 30(7):119-123.

作者简介：



罗长远（1973-），男，河南信阳人，博士，信息工程大学副教授、硕士生导师，主要研究方向为装备工程和无线通信系统安全。

霍士伟（1985-），男，河北邯郸人，硕士，西安通信学院助教，主要研究方向为普适计算安全和无线网络安全。

邢洪智（1986-），男，河北石家庄人，信息工程大学硕士生，主要研究方向为无线网络安全和移动 IPv6。