普适环境中基于身份的跨域认证方案

罗长远，霍士伟，邢洪智
（解放军信息工程大学 电子技术学院，河南 郑州 450004）

摘 要：利用椭圆曲线加法群提出了一种基于身份的签名算法，算法中签名的验证结果相对于签名者身份是一个常量，该算法可保证跨域认证中用户身份的匿名性，并且避免了复杂的双线性对运算。基于该算法设计了一种普适环境中的跨域认证方案，方案中用户利用该算法对时戳签名作为认证信息，在实现安全跨域认证的同时实现了用户匿名性。分析表明，该方案同时具有安全和效率上的优势，更加适合在普适环境下应用。

关键词：普适计算；跨域认证；基于身份的密码体制；匿名
中图分类号：TP309 **文献标识码**：B **文章编号**：1000-436X(2011)09-0111-05

Identity-based cross-domain authentication scheme in pervasive computing environments

LUO Chang-yuan, HUO Shi-wei, XING Hong-zhi
(Electronic Technology Institute, Information Engineering University, Zhengzhou 450004, China)

Abstract: An identity-based signature scheme was proposed based on additive elliptic curve group. The verification result of the signature was a constant with respect to the signer's identity. The scheme could guarantee user anonymity in the process of cross-domain authentication and avoided the pairing operation. Then a cross-domain authentication scheme was constructed by combining the proposed signature scheme. During the authentication, a user constructed the signature of timestamp as authentication proof, which realized secure cross-domain authentication and user anonymity. It is shown that the proposed scheme has superiority in both security and efficiency, and is more suitable for pervasive computing.

Key words: pervasive computing; cross-domain authentication; identity-based cryptography; anonymity

1 引言

普适计算是一种开放的分布式环境，用户可以随时随地获得服务。普适环境由不同的安全域构成，每个安全域设置有认证服务器来对域内的资源进行管理，为访问资源的用户提供认证服务。普适环境具有高度动态性，用户经常会漫游到不同的安全域中访问服务，这就存在跨安全域认证的问题[1]。当用户跨域访问资源时，由于和访问域的认证服务器之间不存在事先的信任关系，因此访问域的认证服务器需要联合用户家乡域的认证服务器对用户进行认证[2]。另外在跨域访问的过程中，为了防止恶意实体跟踪用户的资源访问记录和会话，需要在认证过程中隐藏用户真实身份，提供匿名性服务[3]。普适环境中的跨域认证方案在实现安全认证和会话密钥建立的同时应满足匿名性和不可跟踪性，即

收稿日期：2010-10-08；**修回日期**：2011-05-24
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)

访问域认证服务器和其他用户无法确定跨域访问的合法用户的真实身份及不同会话的来源。由于普适环境下用户一般使用计算能力有限的便携设备[4]，因此跨域认证方案还要满足用户端计算量小的要求。

文献[1]利用属性证书实现了普适环境中的跨域认证，但是方案涉及到复杂的证书管理过程，计算开销较大。文献[2]采用签密技术来实现普适环境中的跨域认证，避免了复杂的证书管理过程。文献[1,2]中的方案都无法保证用户的匿名性。文献[3]基于单点登录技术和身份联盟技术设计了一种普适环境中的跨域认证方案，可以保证用户匿名性和不可跟踪性。但是，用户每次跨域认证时，认证服务器都需要进行域间通信，认证时间较长。文献[5]提出一种基于身份的跨域认证方案，认证服务器只需要在用户首次跨域认证时进行域间通信，在之后的跨域认证过程中，不需要进行域间通信，避免了域间通信造成的过大时间延迟。但是该方案中用户需要进行多次双线性对运算，用户计算开销较大。文献[6]提出了一种新的基于身份的跨域匿名认证方案，方案通过减少双线性对运算次数，提高了执行效率。但是，方案在匿名性方面存在缺陷，因为当用户首次跨域认证后获得了一个临时证书，在之后的资源访问中，用户利用相同的临时证书作为认证凭证，这会使用户的会话被跟踪。

本文在分析上述方案的基础上，设计了一种普适环境中基于身份的跨域认证方案。首先提出了一种基于身份的签名算法，算法中签名的验证结果相对于用户身份是一个常量，并且避免了复杂的双线性对运算。基于该算法设计了一种普适环境中的跨域认证方案，方案中用户利用该算法对时戳签名作为认证信息，在保证用户身份不被泄漏的前提下，实现了用户与访问域认证服务器间的安全认证，并减少了用户端计算开销。分析表明，方案可以满足普适环境跨域认证的安全要求，并具有较高的执行效率。

2 基于身份的签名算法

自从基于身份的密码体制被提出以来，研究者设计了多个基于身份的签名算法，这些算法大都是基于 pairing 实现的，具有较大的计算开销。文献[7]提出了一种无 pairing 的基于身份的签名算法，该算法基于椭圆曲线加法群实现，不需要复杂的 pairing 运算，具有较高的执行效率，作者在随机预言机模型下证明了算法的安全性。但是，该算法中签名的验证结果相对于签名者身份是变量，无法实现匿名认证。在文献[7]算法的基础上，本文提出了一种新的基于身份的签名算法，算法中签名的验证结果相对于签名者身份是一常量，并保持了原算法执行效率高的优点。算法描述如下。

1) 系统建立：给定安全参数 k，PKG 线选择椭圆曲线 $E(F_p)$ 上的 q 阶循环加法群 G_1，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 $P_{\text{pub}}=sP\in G_1$。定义以下安全散列函数：$H_1:\{0,1\}^*\times G_1\to Z_q^*$，$H_2:\{0,1\}^*\to Z_q^*$。PKG 妥善保管 s，公开系统参数 $\{G_1,q,P,P_{\text{pub}},H_1,H_2\}$。

2) 私钥产生：假设用户 A 的身份标识为 ID_A，PKG 随机选择 $r_A\in Z_q^*$，计算 $R_A=r_AP$，$s_A=r_A+sc$，其中，$c=H_1(ID_A,R_A)$，A 的私钥为 (s_A,R_A)，通过安全信道将 (s_A,R_A) 发送给 A。A 通过检验 $s_AP=R_A+H_1(ID_A,R_A)P_{\text{pub}}$ 是否成立来验证私钥的正确性。

3) 签名：用户 A 对消息 $m\in\{0,1\}^*$ 进行签名，A 随机选择 $y\in Z_q^*$，计算 $Y=yP$，$h=H_2(ID_A,m,R_A,Y)$，$z=y+s_Ah$，则 A 对 m 的签名为 (R_A,Y,z)。

4) 验证：A 将签名 (R_A,Y,z)、消息 m 和身份标识 ID_A 发送给验证者，验证者对签名进行验证。验证者计算 $c=H_1(ID_A,R_A)$ 和 $h=H_2(ID_A,m,R_A,Y)$，验证等式：

$$h^{-1}(zP-Y)=R_A+cP_{\text{pub}} \tag{1}$$

是否成立，若成立则输出“真”，否则输出“假”。

该签名算法具有以下特点，对于特定用户 A，其签名的验证结果 R_A+cP_{pub} 是一个确定的常量。因此，根据签名的验证结果可以确定签名者的身份。本文将基于这个特性保证跨域认证中用户身份的匿名性。本算法不需要 pairing 运算，只需要进行椭圆曲线上的点乘和点加运算。pairing 的计算开销远大于点乘和点加运算，因此同现有基于 pairing 的算法相比，本算法具有更高的执行效率。

同文献[7]中算法相比，本算法对验证部分进行了改进，把原算法中的验证等式 $zP=Y+h(R_A+cP_{\text{pub}})$ 改为式(1)，这样可以使签名的验证结果是一常量，便于实现匿名认证。可以证明这种改变不会给攻击者增加任何优势，本算法与原算法具有相同的安全

性，是存在性不可伪造的。

文中称本算法为 IBS-Ⅰ，文献[7]中算法为 IBS-Ⅱ。

定理 1　若 IBS-Ⅱ是存在性不可伪造的，则 IBS-Ⅰ算法同样是存在性不可伪造的。

证明　假设存在敌手 B 不知道 ID 的私钥，在时间 t 内以不可忽略的概率 ε 伪造出 ID 对消息 m 的有效 IBS-Ⅰ签名 (R_A, Y, z)，则敌手 B 同样可以在时间 t 内以不可忽略的概率 ε 伪造出 ID 对消息 m 的有效 IBS-Ⅱ签名 (R_A, Y, z)。

若 B 能够伪造出 ID 对消息 m 的有效 IBS-Ⅰ签名 $\sigma = (R_A, Y, z)$，则 B 输出 $\sigma' = (R_A, Y, z)$ 作为 ID 对消息 m 的 IBS-Ⅱ签名。σ' 将是一个有效的伪造，若式(2)成立：

$$zP = Y + h(R_A + cP_{\text{pub}}) \tag{2}$$

由于 $\sigma = (R_A, Y, z)$ 是一个有效的 IBS-Ⅰ签名，因此式(3)成立：

$$h^{-1}(zP - Y) = R_A + cP_{\text{pub}} \tag{3}$$

式(3)两边同乘以 h 得：

$$zP - Y = h(R_A + cP_{\text{pub}}) \tag{4}$$

式(4)两边同加上 Y 得：

$$zP = Y + h(R_A + cP_{\text{pub}}) \tag{5}$$

因此，式(2)成立，定理 1 成立。所以，本算法是存在性不可伪造的。

3　普适环境中基于身份的跨域认证方案设计

3.1　系统结构

如图 1 所示，系统包括 2 个安全域 A 和 B，每个安全域有一个认证服务器对本域中的资源和用户进行管理，为访问本域资源的用户提供认证服务。用户 U 属于安全域 A，称安全域 A 中的认证服务器为 HA（home authenticator）；称安全域 B 中的认证服务器为 FA（foreign authenticator）。用户 U 事先在 HA 处进行注册，HA 为 U 签发基于身份的私钥，并为用户建立账户。当用户 U 访问安全域 A 中的资源时，可以直接通过 HA 的认证。但是，当用户 U 访问安全域 B 中资源时，FA 需要联合 HA 来对用户进行认证。本方案的安全性基于以下假设：HA 和 FA 都是诚实的并互相信任对方做出的判断。

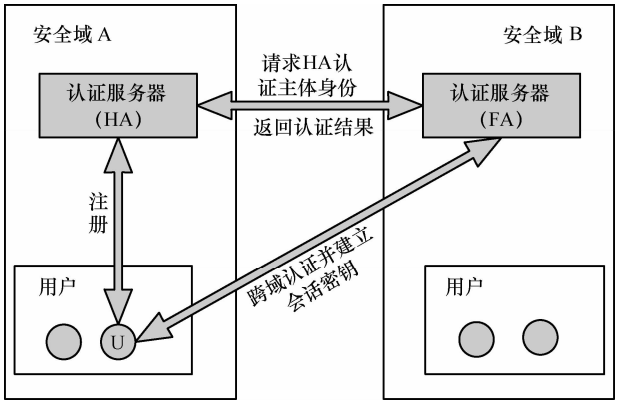

图 1　系统结构

3.2　方案设计

方案包括系统建立、用户注册、全认证和重认证 4 个阶段。系统建立阶段，HA 和 FA 分别选择系统参数；用户注册阶段，HA 为用户签发私钥，并为用户建立相关账户；当用户 U 首次访问安全域 B 中资源时，运行全认证协议，需要 HA 和 FA 的共同参与；当用户 U 再次访问安全域 B 中资源时，FA 可以通过重认证协议来快速认证用户 U，无需 HA 的参与。

3.2.1　系统建立

HA 按照本文第 2 节中的方法选择安全参数，选择 $s_{\text{HA}} \in Z_q^*$ 作为私钥，公钥为 $P_{\text{HA}} = s_{\text{HA}}P$，定义以下安全散列函数：$H_1 : \{0,1\}^* G_1 \to Z_q^*$，$H_2 : \{0,1\}^* \to Z_q^*$，$H_3 : G_1 \to \{0,1\}^*$。公开参数 $\{G_1, q, P, P_{\text{HA}}, H_1, H_2, H_3\}$。FA 选择和 HA 相同的参数和散列函数，选择 $s_{\text{FA}} \in Z_q^*$ 做为私钥，公钥为 $P_{\text{FA}} = s_{\text{FA}}P$，公开参数 $\{G_1, q, P, P_{\text{FA}}, H_1, H_2, H_3\}$。

3.2.2　用户注册

1) 用户 U 将身份标识 ID_U 发送给 HA。

2) HA 检验用户身份的合法性，然后随机选择 $r_{\text{U}} \in Z_q^*$，计算 $R_{\text{U}} = r_{\text{U}}P$，$s_{\text{U}} = r_{\text{U}} + s_{\text{HA}}c$，其中，$c = H_1(ID_{\text{U}}, R_{\text{U}})$，HA 通过安全信道将 $(s_{\text{U}}, R_{\text{U}})$ 发送给 U。U 通过检验 $s_{\text{U}}P = R_{\text{U}} + H_1(ID_{\text{U}}, R_{\text{U}})P_{\text{HA}}$ 是否成立来验证私钥的正确性。

3) HA 为 U 建立账户，$(Ind_{\text{U}}, ID_{\text{U}}, R_{\text{U}})$，其中，账户索引 $Ind_{\text{U}} = R_{\text{U}} + H_1(ID_{\text{U}}, R_{\text{U}})P_{\text{HA}}$。

3.2.3　全认证

1) 用户 U 选择 x，$y \in Z_q^*$，获取当前时戳 T_{U}，计算 $Y = yP$，$X = xP$，$Y' = Y + xP_{\text{HA}}$，$h = H_2(ID_{\text{U}}, T_{\text{U}}, R_{\text{U}}, Y)$，$z = y + s_{\text{U}}h$，然后发送消息 $< ID_{\text{HA}},$

$T_U, X, Y', h, z>$给 FA。

2) FA 收到消息后，若T_U新鲜，获取时戳T_{FA}，构造消息$m_{FA}=\{ID_{HA}, T_U, X, Y', h, z, ID_{FA}, T_{FA}\}$，计算消息的签名$Sig_{FA}(m_{FA})$，$Sig(\cdot)$为椭圆曲线签名算法 ECDSA，FA 向 HA 发送消息$<m_{FA}, Sig_{FA}(m_{FA})>$。

3) HA 收到消息后，若T_{FA}新鲜，且签名$Sig_{FA}(m_{FA})$验证正确，则 HA 通过对 FA 的认证。HA 计算$Y=Y'-s_{HA}X$，$Ind_U=h^{-1}(zP-Y)$，然后在用户列表中检索Ind_U，若存在以Ind_U为索引的账户，则取出账户信息验证$h=H_2(ID_U, T_U, R_U, Y)$是否成立，若成立则通过对 U 的认证。HA 计算$k=H_3(Y)$，获取当前时戳T_{HA}，构造消息$m_{HA}=\{ID_{FA}, ID_{HA}, T_{FA}, T_{HA}, E^{ECC}_{P_{FA}}(k)\}$，计算消息的签名$Sig_{HA}(m_{HA})$，$E^{ECC}_{P_{FA}}$为椭圆曲线加密算法，向 FA 发送消息$<m_{HA}, Sig_{HA}(m_{HA})>$。

4) FA 收到消息后，若T_{HA}新鲜且签名验证正确，则通过对 HA 和 U 的认证，即相信用户 U 为安全域 A 中的合法用户。FA 为用户 U 生成一个临时身份ID'_U和对应的临时私钥(s'_U, R'_U)，为 U 建立临时账户$(Ind'_U, ID'_U, R'_U, time)$，其中，账户索引$Ind'_U=R'_U+H_1(ID'_U, R'_U)P_{FA}$，$time$为临时账户有效期，超过有效期后则删除该临时账户。$ID'_U$和$(s'_U, R'_U)$可以在空闲时刻计算，以节省时间。FA 解密$E^{ECC}_{P_{FA}}(k)$获得会话密钥$k$，获取时戳$T'_{FA}$，向 U 发送消息$<T_{FA}, E_k(T_{FA}, T_U, s'_U, R_U, ID'_U)>$，$E$为对称加密算法。

5) 用户 U 收到消息后，若T'_{FA}新鲜，则计算$k=H_3(Y)$，解密$E_k(T'_{FA}, T_U, s'_U, R'_U, ID'_U)$并核对$T'_{FA}$和$T_U$，若一致则通过对 FA 的认证并把$k$作为之后通信的会话密钥。用户 U 妥善保存临时身份ID'_U和对应的私钥(s'_U, R'_U)。

3.2.4 重认证

在有效期内，当用户 U 再次访问安全域 B 中资源时，可以利用临时私钥(s'_U, R'_U)构造签名作为认证信息。FA 通过验证签名可以确定用户是已通过认证的用户，不需要 HA 的参与，可以实现对用户 U 的快速认证。

1) 用户 U 选择x，$y\in Z^*_q$，获取当前时戳T_U，计算$Y=yP$，$X=xP$，$Y'=Y+xP_{FA}$，$h=H_2(ID'_U, T_U, R'_U, Y)$，$z=y+s'_U h$，然后发送消息$<T_U, X, Y', h, z>$给 FA。

2) FA 收到消息后，若T_U新鲜则计算$Y=Y'-s_{FA}X$，$Ind'_U=h^{-1}(zP-Y)$，然后在用户列表中检索Ind'_U，若存在以Ind'_U为索引的账户，则取出账户信息验证$h=H_2(ID'_U, T_U, R'_U, Y)$是否成立，若成立则通过对用户 U 的认证。FA 计算会话密钥$k'=H_3(Y)$，获取当前时戳T_{FA}，向用户 U 发送消息$<T_{FA}, E_{k'}(T_{FA}, T_U)>$。

3) 用户 U 收到消息后，若T_{FA}新鲜，则计算$k'=H_3(Y)$，解密$E_{k'}(T_{FA}, T_U)$并核对T_{FA}和T_U，若一致则通过对 FA 的认证并把k'作为之后通信的会话密钥。

4 方案分析

4.1 安全性分析

1) 双向认证

在全认证过程中，方案可以实现各实体间的安全双向认证。

HA 对用户 U 的认证：在全认证的步骤 3)中 HA 完成了对用户 U 的认证，该认证过程实质上是对签名(Y', h, z)的验证过程，(Y', h, z)是用户 U 利用本文提出的基于身份的签名算法对时戳T_U的签名，只是对Y进行了加密处理，使得只有 HA 可以验证签名。由于签名算法是安全的，并且签名中包含了时间戳T_U可以保证签名的新鲜性，因此 HA 对用户 U 的认证是安全的。

HA 和 FA 之间的认证：HA 和 FA 之间的认证是通过验证对方的签名来实现的。由于所有的签名算法 ECDSA 是安全的，并且签名中包含了时间戳可以防止重放攻击，因此 HA 和 FA 之间的认证是安全的。

用户 U 对 FA 的认证：在全认证的步骤 5)中，用户 U 通过解密$E_k(T'_{FA}, T_U, s'_U, R'_U, ID'_U)$并核对$T'_{FA}$和$T_U$完成对 FA 的认证。因为，HA 生成将生成的$k$利用 FA 的公钥加密传送，只有合法的 FA 可以利用私钥解密得到密钥k。

FA 对用户 U 的认证是通过 FA 认证 HA 和 HA 认证用户 U 间接实现的。

在重认证过程中，FA 和用户 U 同样可以实现双向认证，原理与上述相同。

2) 安全的会话密钥建立和更新

在安全认证过程中，用户 U 和 FA 可以建立安

表 1　　**效率比较**

方案	双线性对(U/FA/HA)	公钥签名与验证(U/FA/HA)	公钥加解密(U/FA/HA)	点乘(U/FA/HA)	消息交互数(U-FA/FA -HA)
IDAKE-MA	4/4/4	0/1/1	0/0/0	7/6/4	3/2
AWAP	0/0/1	0/2/2	0/0/0	5/1/2	2/2
本方案	0/0/0	0/2/2	0/1/1	3/0/3	2/2

全的会话密钥 $k = H_3(Y)$。因为只有 HA 才能利用私钥解密 Y' 得到 Y，所以只有用户 U 和 HA 可以计算出 k。$(Y^{'}, h, z)$ 是用户对时间戳 T_A 和 Y 的签名，因此 HA 通过验证签名可以确定密钥的新鲜性。HA 将 k 利用 FA 的公钥加密并利用自己的私钥签名后传送，加密可以保证密钥不会泄露，FA 通过验证签名可以确认 k 来源的正确性。最后用户 U 通过解密 $E_k(T'_{FA}, T_U, s'_U, R'_U, ID'_U)$ 并核对 T'_{FA} 和 T_U 可以确认 FA 确实获得了正确的会话密钥 k。

在每次重认证的过程中，用户 U 和 FA 可以建立新的会话密钥，实现了一次一密。

3) 完善的用户匿名性和不可跟踪性

首先，其他用户和 FA 无法确定用户 U 的真实身份。在全认证过程中，用户 U 提交的的认证信息中没有身份信息，只包含了时戳 T_U 及其签名信息，只有 HA 可以通过验证签名计算出用户的账户索引，因此除了 HA 其他用户和 FA 无法确定用户 U 的真实身份。在重认证过程中，FA 仅能确定用户的临时标识符，无法确定用户真实身份。

其次，其他用户无法确定不同的会话来自相同的用户。在全认证过程中，用户每次对不同的时间戳签名作为认证信息，认证信息具有随机性，其他用户无法将不同的认证信息联系起来。在重认证过程中提供了相同的机制保证了用户会话的不可跟踪性，只有 FA 可以将用户的会话联系起来。

本方案达到了文献[5]方案的安全强度。文献[6]中方案在重认证过程中存在匿名缺陷，在重认证过程中用户使用相同的临时证书来作为认证凭证，其他用户可以据此跟踪用户的会话，因此本方案在安全性上优于文献[6]中方案。

4.2　效率分析

本节对方案的关键部分全认证协议的效率进行分析，并与文献[5]中的 IDAKE-MA 方案和文献[6]中的 AWAP 方案进行比较（如表 1 所示），因为 3 个方案都采用了基于身份的密码体制。在比较方案的计算开销时，忽略对称密钥运算和普通散列运算，仅考虑公钥操作。由表 1 中数据可以看出，本方案中所有实体均不需要进行复杂的双线性对运算，整体性能优于 IDAKE-MA 和 AWAP。本方案用户端只需要进行 3 次点乘运算，计算量低于 IDAKE-MA 和 AWAP。另外，本方案中 U 与 FA 以及 FA 与 HA 之间的消息交互数均为 2 次，而且不需要在无线信道上传递证书，具有较小的通信开销。结合考虑，本方案具有更高的执行效率，更加适合在资源受限的普适环境中应用。

5　结束语

在多安全域的普适环境下，跨域认证有着特殊的要求。本文提出了一种普适环境中基于身份的跨域认证方案，方案可以满足双向认证、安全的会话密钥建立、完善的用户匿名性等安全要求。与现有同类方案相比，本方案在保证安全性的基础上，用户端计算开销和总计算开销明显减小。本方案同时具有安全性和效率上的优势，更加适合在普适环境下应用。

参考文献：

[1] LEE D G, KANG S I, SEO D H, *et al*. Authentication for single/multi domain in ubiquitous computing using attribute certification[A]. International Conference on Computational Science and Its Applications[C]. Glasgow, UK, 2006. 326-335.

[2] 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.

[3] CHAN Y Y, FLEISSNER S. Single sign-on and key establishment for ubiquitous smart environments[A]. International Conference on Computational Science and Its Applications[C]. Glasgow, UK, 2006. 406-415.

（下转第 122 页）