Software Engineering and Applications 软件工程与应用, 2023, 12(6), 958-964
Published Online December 2023 in Hans. https://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2023.126094

Hans汉斯

无证书的普适环境匿名认证方案

罗长远

郑州工业应用技术学院信息工程学院，河南 郑州

收稿日期：2023年11月16日；录用日期：2023年12月20日；发布日期：2023年12月28日

摘　要

针对普适环境下的匿名认证问题，利用双线性对的相关特性，提出了一种无证书签名算法，算法中的签名矢量相对于签名者身份是一常量。基于该算法设计了一种匿名认证方案，方案中用户利用该算法对时戳签名作为认证信息，在安全认证的同时实现了用户匿名性。分析表明，用户端认证需要116.1 ms，计算量较小，方案在满足双向认证、用户匿名性和无关联性安全要求的同时，解决了现有方案存在的密钥托管问题。

关键词

普适计算，匿名认证，无证书签名，双线性对

Certificate-Less Based Anonymous Authentication Scheme in Pervasive Computing Environments

Changyuan Luo

School of Information Engineering, Zhengzhou Institute of Industrial Technology, Zhengzhou Henan

Received: Nov. 16th, 2023; accepted: Dec. 20th, 2023; published: Dec. 28th, 2023

Abstract

Considered the anonymous authentication in pervasive computing environments, a certificateless signature scheme was proposed based on bilinear parings. The verification result of the signature was a constant with respect to the signer's identifier. Then an anonymous 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 authentication and user anonymity. It is showed that it takes the client 116.1ms to realize authentication and

文章引用: 罗长远. 无证书的普适环境匿名认证方案[J]. 软件工程与应用, 2023, 12(6): 958-964.
DOI: 10.12677/sea.2023.126094

the proposed scheme has less computation on the client side. It can achieve such security requirements as mutual authentication, user anonymity and non-linkability. Moreover, it resolves the problem of key escrow.

Keywords

Pervasive Computing, Anonymous Authentication, Certificateless Signature, Bilinear Pairings

1. 引言

普适环境计算是继主机和桌面计算后出现的新计算模式，其目的是使计算机服务融入日常生活空间，形成一个“时时存在、处处存在而又不可见”的计算服务环境[1]。在普适环境中当向服务提供方申请服务时，它需要对申请者进行认证，以防止非法用户获取服务。同时申请者也需要对服务提供方进行认证，以防止假冒实体的攻击。为了更好的保护用户隐私，在普适环境下的认证除了提供安全认证和密钥建立服务之外，还要求[2] [3] [4]：1) 满足用户匿名，即认证时，不能获得用户的真实身份；2) 满足无关联特性，即不能确定不同的会话来自同一用户。

文献[5]采用传统的公钥体制实现匿名认证，用户基于服务器的公钥加密身份实现匿名，用自己的私钥签名作为认证凭证。该方案涉及到较多的公钥操作，公钥证书管理复杂，不适合普适计算中的资源受限的设备。文献[6]应用基于身份的密码体制设计匿名认证方案，来避免公钥体制中管理证书问题，但方案中用户和服务器都需要多次的双线性对的运算，带来较大的计算量。文献[7]采用基于身份的签名算法对时间戳签名产生认证请求，该签名只有服务器方能够验证，所以对外部用户是匿名的，而且用户端不需要计算双线性对，比较适合普适计算环境。

以上匿名认证方案都有密钥托管方面的问题，密钥生成中心的主密钥如果泄露，攻击者通过计算合法用户的签名私钥，来假冒合法用户。针对该问题，本文基于无证书签名算法来设计匿名认证方案，该方案可满足用户匿名性和用户端计算量小的要求，同时不存在密钥托管问题。

2. 无证书签名算法

2.1. 算法设计

2003 年 Al-Ryami 和 K.G. Paterson 提出了无证书公钥密码系统[8] (certificateless public key cryptography, CL-PKC)的概念，通过密钥生成中心(Key Generation Center, KGC)为系统用户生成部分私钥。

(1) 系统建立

KGC 输入系统安全参数 k；获得满足双线性对要求的 e、G_1、G_2、q，G_1 的生成元为 P；随机选取 $s \in Z_q^*$ 作为系统私钥；计算系统公钥 $P_0 = sP$；选取安全哈希函数 $H_1 : \{0,1\}^* \to G_1$ 和 $H_2 : \{0,1\}^* \times G_1 \to Z_q^*$；最后 KGC 公布系统参数 $\{G_1, G_2, e, q, P, P_0, H_1, H_2\}$。

(2) 用户部分私钥产生

ID_A 为用户 A 的惟一身份标识，用户 A 向 KGC 提交 ID_A，KGC 验证 ID_A 是否合法，若 ID_A 合法，KGC 为生成 A 的部分私钥 $D_A = sQ_A$，其中 $Q_A = H_1(ID_A)$，并安全地将 D_A 传送给 A。

(3) 秘密数产生

用户 A 随机选取 $x_A \in Z_q^*$ 作为用户秘密数，并安全保存。

(4) 用户私钥产生

用户 A 计算 $S_A = x_A D_A$ 作为自己的私钥。

(5) 用户公钥产生

用户 A 计算 $X_A = x_A P$ 和 $Y_A = x_A P_0$，将 $P_A = \langle X_A, Y_A \rangle$ 作为自己的公钥。

(6) 签名

为了对 m 消息进行签名，A 选择随机数 $r \in Z_q^*$，计算 $R = rP$、$h = H_2(m \| R)$，$V = S_A/(h+r)$，A 对 m 的签名为 $\delta = \langle R, V \rangle$，$A$ 向验证者发送 ID_A、m、δ 和 P_A。

(7) 验证

验证者首先验证 $e(X_A, P_0) = e(Y_A, P)$ 是否成立；然后计算 $h = H_2(m \| R)$，验证 $e(V, hP + R) = e(Q_A, Y_A)$ 是否成立。只有两者验证都通过时才接受签名。

由上述过程可知，对用户 A，$e(Q_A, Y_A)$ 是一个确定的常量。对于不同的 δ_1 和 δ_2，只要是同一个签名人，验证结果必定相同，从而可以确定签名者的身份。即通过预计算 $e(Q_A, Y_A)$，收到 δ 后计算 $e(V, hP + R)$ 是否等于 $e(Q_A, Y_A)$，来确认 δ 是否来自 A。

2.2. 算法安全性分析

采用文献[7]中的方法来分析上述签名算法的安全性。

(1)若 A 对消息 m 的合法签名 $\delta = \langle R, V \rangle$，则 Adv 无法计算出 A 的私钥 S_A。因为要从 V 中解得 S_A 就需要 Adv 从 $R = rP$ 求得 r，这是 ECDL 问题。

(2)假设 Adv 可以伪造签名 $\delta' = \langle R', V' \rangle$，满足 $e(V', H_2(m \| R')P + R') = e(Q_A, Y_A)$。对于循环群 G_1，$\forall Q \in G_1$，$\exists y \in Z_q^*$，则有 $Q = yQ_A$。因此任意 δ' 总有 $y \in Z_q^*$ 满足：(a) $V' = yQ_A \wedge H_2(m \| R')()P + R' = y^{-1}Y_A$；(b) $V' = yY_A \wedge H_2(m \| R')P + R' = y^{-1}Q_A$。若 (a) 成立，Adv 需要计算 R' 使其满足等式：$R' = y^{-1}Y_A - H_2(m \| R')P$，但是对于单向函数 H_2，Adv 无法获取符合条件的 R'，故(a)条件不成立；同理可证(b)条件不成立。

3. 匿名认证方案设计

3.1. 方案描述

KGC 负责为合法用户生成部分私钥，服务器是普适环境中可以向用户提供某种服务的实体，合法用户在获得服务时必须首先通过服务器的认证。

(1) 系统建立

KGC 依照 2.1 节中描述过程生成系统参数，选定公私钥对 (s, P_0)，并对外发布系统参数 $\{G_1, G_2, e, q, P, P_0, H_1, H_2\}$。

(2) 用户公私钥生成

用户公私钥的生成方法同 2.1 节中描述方法相同。ID_U 为用户 U 的身份标识，KGC 生成用户部分私钥 $D_U = sQ_U$，$Q_U = H_1(ID_U)$，用户选取随机数 $x_U \in Z_q^*$，计算出完整私钥 $S_U = x_U D_U$，用户公钥为 $P_U = \langle X_U, Y_U \rangle$，其中 $X_U = x_U P$，$Y_U = x_U P_0$。

(3) 用户注册

在使用服务器的服务之前，用户 U 须先向服务器注册并成为服务器的合法用户。服务器 S 具有长期私钥 $SK_S \in Z_q^*$，相对应的公钥为 $PK_S = SK_S P$。在注册时，用户向服务器提供 ID_U 和公钥 $P_U = \langle X_U, Y_U \rangle$。

服务器首先审核用户身份，审核通过后，通过验证 $e(X_U,P_0)=e(Y_U,P)$ 来确定用户的公钥是否合法。验证通过后，服务器为用户建立帐户 $\langle ind_U,ID_U\rangle$，其中 $ind_U=e(Q_U,Y_U)$ 是用户帐户索引。注册过程中，用户会获得服务器公钥 PK_S、一个哈希函数 $H_3:G_1\times G_1\to\{0,1\}^*$ 和消息认证算法 MAC。

(4) 认证

当用户需要使用服务器提供的服务时，通过以下步骤进行双方向认证。

用户选择随机数 $r\in Z_q^*$，获得当前时间戳 T，计算 $R=rP$，$R'=rPK_S$，$h=H_2(T\|R)$，计算临时身份 $Tid_U=S_U/(h+r)$，用户将 $\langle T,R',Tid_U\rangle$ 发送给 S，然后计算会话密钥 $K=H_3(R\|R')$ 并保存 K。

服务器收到消息后，需验证时戳 T 的新鲜性。若 T 是新鲜的，S 计算 $R=SK_S^{-1}R'$，$h=H_2(T\|R)$，$ind_U=e(Tid_U,hP+R)$。S 以 ind_U 来索引用户列表，若用户存在，则认证通过。计算 $K=H_3(R\|R')$、$MAC_K(ID_U,S)$，并向用户发送认证应答 $MAC_K(ID_U,S)$。用户 U 收到 $MAC_K(ID_U,S)$ 后，利用 K 验证认证应答的完整性。若验证通过，则通对服务器的认证，并在以后的通信中使用 K 作为会话密钥。

3.2. 方案安全性分析

(1) 双向认证

本方案可以实现用户和服务器之间的双向认证以及相互之间会话密钥协商。下面利用采用 BAN 逻辑对方案的认证安全性进行分析证明，由于双向认证在认证阶段实现，所以只需分析认证阶段协议。

为了便于 BAN 逻辑证明，需对原协议进行转化。按照 BAN 逻辑的描述规则，U 和 S 之间的共享密钥 K 用 K_{US} 表示，U 和 S 的公私钥分别为 K_U、K_U^{-1}、K_S 和 K_S^{-1}。

消息转化：

消息 1 $U\to S$：T,R',Tid_U 可转化为 $U\to S$：$T,\{K_{US},\{K_{US},T\}_{K_U^{-1}}\}_{K_S}$

消息 1 中虽然没有密钥 K_{US}，由于 S 可以利用私钥由 R' 计算出 R 进而计算出 K_{US}，并且 K_{US} 只能由 S 计算得到，所以 K_{US} 可以看作由 S 的公钥加密传送。由于 Tid_U 是 U 对 R 和 T 的签名，而 K_{US} 由 R 计算得到，所以 Tid_U 可以看作是对 K_{US} 和 T 的签名 $\{K_{US},T\}_{K_U^{-1}}$。由于签名 Tid_U 只有 S 可以验证，所以 $\{K_{US},T\}_{K_U^{-1}}$ 可以看作由 S 的公钥加密。因此，上述转化是合理的。

消息 2 $S\to U$：$MAC_K(ID_U,S)$ 可转化为 $S\to U$：$\{U,S\}_{K_{US}}$

消息 2 的转化中，将消息码认证算法 MAC 用对称加密算法代替，因为两者都由对称密钥控制，所以转化是合理的。

协议理想化：

消息 1 $U\to S$：$\{U\xleftrightarrow{K_{US}}S,\{U\xleftrightarrow{K_{US}}S,T\}_{K_U^{-1}}\}_{K_S}$

消息 2 $S\to U$：$\{U\xleftrightarrow{K_{US}}S\}_{K_{US}}$

初始化假设：

(1) $U|\equiv U\xleftrightarrow{K_{US}}S$；(2) $U|\equiv\#(U\xleftrightarrow{K_{US}}S)$ (3) $S|\equiv\xrightarrow{K_S}S$；

(4) $S|\equiv\xrightarrow{K_U}U$；(5) $S|\equiv\#(T)$；(6) $S|\equiv U\Rightarrow U\xleftrightarrow{K_{US}}S$

由于 K_{US} 由 R 和 R' 计算得出，R 和 R' 都是由 U 产生的参数，所以 K_{US} 是由 U 产生的，进而可得出假设(1)、(2)、(6)。由于 S 可以对 U 的签名 Tid_U (临时身份)进行验证，可得假设(4)。由于 S 可以判断时戳 T 的新鲜性，可得假设(5)。假设(3)显然成立。

证明过程为：

由消息 1 得

$$S\triangleleft\{U\xleftrightarrow{K_{US}}S,\{U\xleftrightarrow{K_{US}}S,T\}_{K_U^{-1}}\}_{K_S}\tag{7}$$

由公式(7)、假设(3)和接收规则得

$$S \triangleleft \left\{U \xleftrightarrow{K_{US}} S, \left\{U \xleftrightarrow{K_{US}} S, T\right\}_{K_U^{-1}}\right\} \tag{8}$$

由公式(8)和接收规则可得

$$S \triangleleft \left\{U \xleftrightarrow{K_{US}} S, T\right\}_{K_U^{-1}} \tag{9}$$

由公式(9)、假设(4)和消息含义规则得

$$S \left| \equiv U \sim \left\{U \xleftrightarrow{K_{US}} S, T\right\}\right. \tag{10}$$

由假设(5)和新鲜性规则得

$$S \left| \equiv \#\left(U \xleftrightarrow{K_{US}} S, T\right)\right. \tag{11}$$

由公式(10)、(11)和临时值验证规则得

$$S \left| \equiv U \left| \equiv \left\{U \xleftrightarrow{K_{US}} S, T\right\}\right.\right. \tag{12}$$

由公式(12)和信仰规则得

$$S \left| \equiv U \left| \equiv U \xleftrightarrow{K_{US}} S\right.\right. \tag{13}$$

由假设(6)、公式(13)和仲裁规则得

$$S \left| \equiv U \xleftrightarrow{K_{US}} S\right. \tag{14}$$

由消息 2 得

$$U \triangleleft \left\{U \xleftrightarrow{K_{US}} S\right\}_{K_{US}} \tag{15}$$

由公式(15)、假设(1)和消息含义规则得

$$U \left| \equiv S \sim \left\{U \xleftrightarrow{K_{US}} S\right\}\right. \tag{16}$$

由公式(16)、假设(2)和临值验证规则得

$$U \left| \equiv S \left| \equiv U \xleftrightarrow{K_{US}} S\right.\right. \tag{17}$$

结论：由上述证明过程可知，认证阶段协议满足一级信仰：假设(1)和公式(14)，二级信仰：公式(13)和公式(17)，所以该方案可以实现安全的双向认证和密钥协商。

(2) 用户匿名性

在认证的过程中，除了服务器外其它用户均不能获取用户的真识身份。这是因为在整个认证过程中用户只是提供了签名矢量$\mathbf{£} = \left\langle T, R^{'}, Tid_U \right\rangle$，而$\mathbf{£}$中不含有用户的身份信息，并且$\mathbf{£}$只能由服务器才能计算出用户帐户的索引，其它用户无法由签名矢量获取该用户身份。

(3) 非关联性

在认证过程中，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，其它用户无法将不同的认证信息联系起来。

(4) 无密钥托管

在本方案中 KGC 只是为用户生成了部分私钥，要生成签名私钥还需获取用户选择的秘密参数。因此，

当 KGC 被攻破导致主密钥泄露后，因没有用户秘密参数而无法生成用户的签名私钥，从而无法假冒合法用户获得服务。

同文献[6]和文献[7]中方案相比，本方案不存在密钥托管问题，具有更强的安全特性。

3.3. 方案效率分析

分析方案的计算开销，并同双线性对基础上实现方案的文献[6]和文献[7]中进行分析比较。由于注册协议只在新用户加入系统时运行，并且可以离线进行，所以在分析方案计算开销时只考虑认证阶段。在分析比较方案的计算开销时，忽略对称密钥操作和普通哈希操作，仅考虑双线性对运算(P)、映射到 G_1 上点的 Map-to-Point 杂凑函数运算(MtP)、G_1 上点的数乘运算(gM)。方案的计算开销如表 1 所示。

Table 1. Comparison of computational overhead
表 1. 计算开销比较

方案	用户计算开销	服务器计算开销
本文方案	3 gM	2 gM + P
文献[6]方案	4 P	4 P
文献[7]方案	3 gM	2 gM + P

采用文献[9] [10] [11] [12]中方法可分别计算出用户端密码操作运行时间，若给定密码操作在服务器端运行时间为 t_S，则用户端的运行时间为 $t_U = t_S \times 2100/206$，密码操作的运行时间如表 2 所示。

Table 2. Cipher operation runtime
表 2. 密码操作运行时间

运算	用户(ms)	服务器(ms)
P	128.4	12.6
MtP	30.6	3.0
gM	38.7	3.8

表 3 为根据上述假设来计算出的各方案运行时间。

Table 3. Performance comparisons
表 3. 性能比较

方案	用户运行时间(ms)	服务器运行时间(ms)
本文	116.1	20.2
文献[6]	513.6	50.4
文献[7]	116.1	20.2

由表 3 可以得出，本文所设计方案中用户端的计算开销较小，能够满足普适环境下用户计算量要求较小的需求。与文献[6]方案相比，本文所设计的方案中用户和服务器的计算开销大大减小。这是由于本文方案中用户不需要进行双线性对运算，并减少了服务器方双线性对的运算次数。本文方案同文献[7]方案具有相同的计算开销，但是本方案不存在密钥托管问题，具有更好的安全特性，因此本方案优于文献[7]方案。

4. 总结

利用无证书公钥设计了一种匿名认证方案，方案既能很好地满足了双向认证，又能实现用户匿名性，

而且用户端计算量小，并且解决了现有方案中的密钥托管问题。通过分析，方案能够满足普适计算环境的高安全性要求。

基金项目

河南省科技攻关课题(No.222102210223)，河南省科技研发计划联合基金项目(No.222103810044)。

参考文献

[1] Weiser, M. (1991) The Computer for the Twenty-First Century. *Scientific American*, **265**, 94-104. https://doi.org/10.1038/scientificamerican0991-94

[2] Leung, A. and Mitchell, C.J. (2007) Ninja: Non Identity Based, Privacy Preserving Authentication for Ubiquitous Environments. In: Krumm, J., Abowd, G.D., Seneviratne, A. and Strang, T., Eds., *UbiComp* 2007: *Ubiquitous Computing. UbiComp* 2007. *Lecture Notes in Computer Science*, Vol. 4717, Springer, Berlin, 73-90. https://doi.org/10.1007/978-3-540-74853-3_5

[3] 武海鹰, 基于上下文的普适计算使用控制模型[J]. 计算机应用, 2012,32(2): 489-492.

[4] 高大利, 孙凌, 辛艳. 基于角色-权限的普适计算受限委托方法[J]. 计算机应用, 2011, 31(5): 1298-1301.

[5] 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.

[6] 彭华熹. 一种基于身份的多信任域认证模型[J]. 计算机学报, 2006, 29(8): 1271-1281.

[7] Cao, X.F., Zeng, X.W., Kou, W.D. and Hu, L.B. (2009) Identity-Based Anonymous Remote Authentication for Value-Added Services in Mobile Networks. *IEEE Transactions on Vehicular Technology*, **58**, 3508-3517. https://doi.org/10.1109/TVT.2009.2012389

[8] Al-Riyami, S.S. and Paterson, K.G. (2003) Certificateless Public Key Cryptography. In: Laih, CS. Eds., *Advances in Cryptology-ASIACRYPT* 2003. *ASIACRYPT* 2003. *Lecture Notes in Computer Science*, Vol. 2894, Springer, Berlin, Heidelberg, 452-473. https://doi.org/10.1007/978-3-540-40061-5_29

[9] Dai, W. (2004) Crypto++ 5.2.1 Benchmarks. https://www.cryptopp.com/wiki/Main_Page

[10] Zhang, Y., Liu, W., Lou, W. and Fang, Y. (2006) Securing Mobile Ad Hoc Networks with Certificateless Public Keys. *IEEE Transactions on Dependable and Secure Computing*, **3**, 386-399. https://doi.org/10.1109/TDSC.2006.58

[11] Ren, K., Lou, W., Zeng, K. and Moran, P.J. (2007) On Broadcast Authentication in Wireless Sensor Networks. *IEEE Transactions on Wireless Communications*, **6**, 4136-4144. https://doi.org/10.1109/TWC.2007.060255

[12] MIRACL (2012) Multiprecision Integer and Rational Arithmetic C/C++ Library. http://indigo.ie/~mscott/