

基于证书的匿名跨域认证方案

丁永善, 李立新, 李作辉

(信息工程大学三院, 河南 郑州 450001)

摘要: 针对物联网中移动设备的跨域认证问题, 提出一种基于证书的匿名跨域认证方案。首先, 结合 PKI 和 IBS 的相关特性, 提出一种基于证书的签名 (CBS, certificate based signature) 方案, 并对提出的 CBS 方案的安全性进行了证明。方案中签名的验证结果为常量, 保证跨域过程中认证实体的匿名性。该签名方案不仅避免了复杂的对运算, 而且避免了传统 PKI 中复杂的证书管理和 IBS 中的密钥托管和分发问题。然后, 基于 CBS 方案设计了一种适用于移动设备的跨域认证方案, 该算法能在安全、高效的同时保证认证的匿名性。最后, 同其他跨域认证方案进行了对比, 对比结果表明, 所提方案具有更强的安全性和更小的计算和通信开销, 为计算能力和功率受限的移动设备进行跨域认证提供了一种较为实用的解决方案。

关键词: 移动设备; 跨域认证; 匿名; CBS; 对运算

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018040

Certificate-based cross-domain authentication scheme with anonymity

DING Yongshan, LI Lixin, LI Zuohui

The 3rd College, Information Engineering University, Zhengzhou 450001, China

Abstract: Considered the cross-domain authentication of mobile devices in the Internet of things, a certificate based anonymous cross-domain authentication scheme was proposed. First, combined with the characteristics of PKI and IBS, a certificate based signature (CBS) algorithm was proposed, and the security of the proposed CBS scheme was proved. The verification result of the signature in the algorithm was constant, which ensured the anonymity of the authentication entities in the cross-domain process. The algorithm does not contain pairing, and avoids complex certificate management in traditional PKI and the key escrow and distribution of IBS. Then a cross-domain authentication scheme for mobile devices was constructed by combining the proposed signature algorithm. The scheme ensures the anonymity of authentication at the same time. Finally, compared with other schemes, the scheme proposed is more secure and has less computation cost and communication cost. Moreover, the scheme is simple and efficient, and could be applied to the cross-domain authentication of mobile devices.

Key words: mobile devices, cross-domain authentication, anonymity, CBS, pairing

收稿日期: 2018-02-10; 修回日期: 2018-04-16

通信作者: 李立新, 870708605@qq.com

基金项目: 国家重点研发计划基金资助项目 (No.2017YFB0802100, No.2016YFB0501900)

Foundation Item: The National Key R&D Plan Program of China (No.2017YFB0802100, No.2016YFB0501900)

1 引言

物联网是一种将人与人、人与物、物与物连接起来的一种泛化的互联网，具有动态感知、可靠传送与智能处理等特点，提高了社会的信息化能力。近年来随着物联网的迅猛发展，其安全问题日益突出^[1,2]，惠普安全研究院调查 10 个最流行的物联网智能设备后发现，几乎所有设备都存在高危漏洞；腾讯发布的互联网安全报告指出，2017 年上半年物联网攻击增加 280%。张玉清等^[3]通过分析现有关于物联网研究工作中的不足和安全问题产生的原因，指出物联网安全存在的 5 大技术挑战：数据共享的隐私保护方法；有限资源的设备安全保护方法；更加有效的入侵检测防御系统与设备测试方法；针对自动化操作的访问控制策略；移动设备的跨域认证方法。

在移动设备组成的通信网络中，除人与设备的交互外，存在越来越多设备之间的交互，移动设备会频繁地从一个网络移动到另一个网络。当移动设备漫游到外域网络时，只有通过了该域网络认证才允许被接入，同时为防止攻击者对移动设备的跟踪，需要提供匿名服务隐藏移动设备的真实身份，因此，匿名跨域认证方案在移动设备组网中至关重要。

适用于移动设备的跨域认证方案除了满足匿名性和不可跟踪性外，由于移动设备的计算能力和功率受限，因此方案还应该满足移动设备计算开销小的要求^[4]。

文献[5,6]利用证书和 PKI 技术实现跨域认证方案，但方案都涉及复杂的证书管理过程，并且计算开销相对较大；文献[7]提出一种无对运算的基于身份的签名（IBE）方案，具有较高的执行效率；在该签名方案的基础上，文献[8]设计了一种匿名跨域认证方案，然而该方案涉及密钥托管问题，其安全性依赖对 PKG 完全可信。基于证书的加密（CBE）方案^[9]将 IBS 的优点集成到 PKI 中，文献[10]基于 CBE 提出了基于证书的签名（CBS）方案，该算法不需要 PKI 中复杂的证书管理，同时避免了 IBS 中的密钥托管和分发问题。但其依赖于对运算，计算开销较大，针对该问题，文献[11]提出一种无对运算的 CBS 方案，降低了

计算开销。

在研究上述方法的基础上，本文提出一种基于证书的匿名跨域认证方案。本文的主要贡献如下。

- 1) 提出了一种无对运算的 CBS 方案，该方案融合了 PKI 和 IBS 的优势，并且避免了对运算，另外，方案中的签名验证结果为常量。
- 2) 对 CBS 方案的不可伪造性进行了证明。
- 3) 将 CBS 方案运用到移动设备的跨域认证中，用户提交的认证信息中不包含移动设备的真实身份，实现匿名认证。
- 4) 对基于证书的匿名跨域认证方案的安全性和效率进行了分析。

2 预备知识

2.1 数学定义和假设

定义 1 （对运算^[12]）假设双线性映射 $e: G \times G \rightarrow G_T$ ，其中， G 、 G_T 为素数 q 阶循环乘法群， g 为 G 的生成元。则 e 满足

- 1) 双线性：对于所有的 $x, y \in G$ 和 $a, b \in \mathbb{Z}_q$ ，均有 $e(x^a, y^b) = e(x, y)^{ab}$ ；
- 2) 非退化性： $e(g, g) \neq 1$ 。

定义 2 （离散对数（DL）假设）假设 q 阶循环乘法群 G ，生成元为 g 。对于 $M \in G$ ，求 $x \in \mathbb{Z}_q^*$ 使其满足 $M = g^x$ 的问题，称为群 G 的离散对数问题。对于敌手 B ，若 $\Pr[B(g, M) = x | M = g^x] \geq \varepsilon$ ，则敌手 B 的优势为 ε 。

群 G 的 (ε, t) -DL 假设：没有算法能在 t 时间内以至少 ε 的优势解决群 G 的离散对数问题。

2.2 基于证书的签名（CBS）方案的基本步骤

一个 CBS 方案主要包括 Setup、UserKeyGen、Certify、Sign 和 Verify 这 5 步^[13]。

- 1) Setup：该算法生成系统主密钥 msk 和系统公开参数 $params$ 。
- 2) UserKeyGen：该算法根据 $params$ 生成用户公钥 PK_{ID} 和私钥 usk_{ID} 。
- 3) Certify：该算法根据系统主密钥 msk 、公开参数 $params$ 、用户标识 ID 和用户公钥 PK_{ID} ，生成用户证书 $Cert_{ID}$ 。
- 4) Sign：该算法根据系统公开参数 $params$ 、消息 m 、用户标识 ID 、用户公钥 PK_{ID} 和用户证书 $Cert_{ID}$ ，生成签名值 σ 。
- 5) Verify：该算法根据 (m, σ) ，系统公开参数

params、用户标识 ID 和用户公钥 PK_{ID} ，验证签名值。若输出为真，则签名值可用，否则不可用。

2.3 安全模型

本文假设敌手 A 希望在已知用户公钥 PK_{ID} 而不知用户证书的情况下伪造用户签名，针对该敌手定义以下游戏^[14]。

1) 挑战者 C 运行 Setup 产生系统参数 params，并将系统参数 params 发送给敌手 A 。

2) 敌手 A 进行以下询问。

UserKeyGen-query: 敌手 A 提供 ID，若 ID 已经存在，则返回用户公钥 PK_{ID} ；否则挑战者 C 运行算法 UserKeyGen，获取公私钥对 (usk_{ID}, PK_{ID}) ，将其添加到用户列表，并返回用户公钥 PK_{ID} 。

Corruption-query: 敌手 A 提供 ID，挑战者 C 检查用户列表，若 ID 存在，返回相应私钥 usk_{ID} 。

Certification-query: 挑战者根据敌手 A 提供的 ID，以 $(msk, params, PK, ID)$ 为输入运行算法 Certify，并返回 Cert。

Sign-query: 挑战者运行算法 Sign，根据 (ID, PK, m) 计算签名值 σ 。

敌手 A 执行多项式有界次询问后，敌手 A 产生消息 m 的签名 σ ；在第二阶段敌手 A 未曾进行相关的私钥、证书和签名询问，但得到用户 ID^* 的签名 σ^* 、消息 m^* 、公钥 PK^* ，若 σ^* 为有效签名，则敌手 A 赢得游戏。敌手 A 的优势为赢得游戏的概率。

3 基于 Certificate 的签名算法

基于证书的签名方案大多是基于线性对运算实现的^[15-17]，经当前的 MIRACL 库测试可知，对运算具有较大的计算开销。文献[11]提出了一种无对运算的 CBS 算法，该算法相较于上述方法具有更高的效率。本节在文献[11]的基础上，提出一种新的无对运算的 CBS 算法，该算法不仅保持了原算法的执行效率高的优点，同时签名的验证结果保持常数，便于实现跨域过程中的匿名认证。其中，3.1 节对无对运算的 CBS 算法进行描述，3.2 节对该算法进行了不可伪造性证明。

3.1 CBS 方案描述

基于证书的签名方案描述如下。

1) Setup: PKG 选择 q 阶循环乘法群 G ， G 的生成元为 g ；选择随机数 $x \in Z_q^*$ ，计算 $X = g^x$ ；

定义以下 Hash 函数 $H_1: \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q^*$ ， $H_2: G \times G \times \{0,1\}^* \rightarrow Z_q^*$ 。公开系统参数 $params = \{G, q, g, X, H_1, H_2\}$ 并妥善保管系统主密钥 $msk = x$ 。

2) UserKeyGen: 用户随机选择 $u \in Z_q^*$ 作为用户私钥，即 $usk = u$ ；并计算用户公钥 $PK = (g^u, X^u)$ 。

3) Certify: CA 随机选择 $r \in Z_q^*$ ，计算 $h_1 = H_1(PK, ID)$ ， $R = g^{-r}$ ， $s = r^{-1}(h_1 - xR) \bmod q$ ，则用户证书为 $Cert_U = (R, s)$ ，用户可以通过式(1)验证证书的正确性。

$$R^{-s} X^R = g^{h_1} \quad (1)$$

4) Sign: 签名者对消息 $m \in \{0,1\}^*$ 进行签名。签名者随机选取 $y \in Z_q^*$ ，并计算 $Y = R^{-y}$ ， $h_2 = H_2(Y, R, m)$ ， $z = y + h_2 su \bmod q$ ，则签名消息为 $\sigma = (Y, R, z)$ 。

5) Verify: 验证者收到消息 $m \in \{0,1\}^*$ ，签名值 $\sigma = (Y, R, z)$ 和系统参数 $params = \{G, q, g, X, H\}$ 后，进行计算 $h_2 = H_2(Y, R, m)$ ， $h_1 = H_1(PK, ID)$ ，并验证

$$\frac{(g^u)^{h_2} R^z Y}{(X^u)^{h_2 R}} = 1 \quad (2)$$

是否成立，若成立输出“真”，否则输出“假”。

该算法中，用户独自生成私钥和公钥并向 CA 申请用户证书，CA 拥有用户证书却不掌握用户私钥，不具备解密任何密文的能力。该算法不具有 pairing，具有较高的执行效率，同时签名验证结果为常数，便于实现跨域过程中的匿名认证。

3.2 CBS 方案安全性证明

该方案中，认为证书颁发者 CA 是诚实且可信的，针对 2.3 节中定义的敌手 A 对 CBS 方案的不可伪造性进行证明。

定理 1 在随机预言模型中，针对 CBS 方案，若存在敌手 A 经过至多 q_e 次 Certification-query， q_s 次 Sign-query， q_{h_1} 次 H_1 -query， q_{h_2} 次 H_2 -query，在 t 时间内以 ε 优势伪造该签名方案，则存在算法 B 在 t' 时间内以 ε' 的优势解决 DL 问题。

其中， $t' = t + O(q_e + q_s)E$

$\varepsilon' \geq \left(1 - \frac{q_{h_1}(q_e + q_s)}{q}\right) \left(1 - \frac{1}{q}\right) \left(\frac{1}{q_{h_2}}\right) \varepsilon$ (E 为幂操作时间)

证明 假设存在敌手 A 在 t 时间内以 ε 优势伪造该签名方案, 构造算法 B 。选择 q 阶循环乘法群 G , G 的生成元为 g ; 在已知 G 和 $M \in G$ 的情况下, 要求求得 $x \in G$ 满足 $g^x = M$ 。

建立阶段: 算法 B 选择 Hash 函数 $H_1: \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q^*$, $H_2: G \times G \times \{0,1\}^* \rightarrow Z_q^*$ 作为随机语言模型。算法 B 生成 $X=M$ 和公开参数 $params = \{G, q, g, X, H_1, H_2\}$, 并发送给敌手 A 。

询问阶段: 敌手 A 进行以下询问。

1) H_1 -query (ID_i, PK_i): 算法 B 拥有包含元组 $\langle ID, PK, h_i \rangle$ 的 H_1 列表, 当敌手 A 进行询问时, 首先检查 H_1 列表是否包含 $\langle ID_i, PK_i, h \rangle$, 若包含则返回 h ; 否则随机选择 $h \in Z_q^*$, 并把 $\langle ID_i, PK_i, h \rangle$ 加入 H_1 列表, 返回 h 。

2) H_2 -query (Y, R, m): 随机选择 $h_2 \in Z_q^*$, 令 $H_2(Y, R, m) = h_2$, 返回 h_2 。

3) UserKeyGen-query (ID_i): 算法 B 拥有包含元组 $\langle ID, usk, PK \rangle$ 的 Key 列表, 当敌手 A 进行询问时, 首先检查 Key 列表是否包含 $\langle ID_i, usk_i, PK_i \rangle$, 若包含则返回 PK_i ; 否则执行算法 $UserKerGen$ 生成公私钥对 $\langle usk_i, PK_i \rangle$, 并把 $\langle ID_i, usk_i, PK_i \rangle$ 加入 Key 列表, 返回 PK_i 。

4) Corruption-query (ID_i): 当敌手 A 进行询问时, 算法 B 首先检查 Key 列表是否包含 $\langle ID_i, usk_i, PK_i \rangle$, 若包含则返回 usk_i ; 否则返回 $\perp$ 。

5) Certification-query (ID_i, PK_i): 敌手 A 进行证书查询, 算法 B 进行以下操作: ①若 $\langle ID_i, usk_i, PK_i \rangle$ 存在, 则随机选取 $a, b \in Z_q$, 并令 $R = X^a g^b$, $s = a^{-1} R \bmod q$, $h_1 = -b \cdot s \bmod q$, 返回证书 (R, s) , 计算可知 (R, s) 满足 $R^{-s} X^R = g^{h_1}$, 同时存储 (R, s, h_1, PK, ID) 更改 H_1 列表中的 $\langle ID_i, PK_i, h \rangle$ 为 $\langle ID_i, PK_i, h_1 \rangle$; ②若 $\langle ID_i, usk_i, PK_i \rangle$ 不存在, 则执行算法 $Certify$, 存储 (R, s, h_1, PK, ID) 并返回 h_1 。

6) Sign-query (ID_i, PK_i, m): 算法 B 检查 (ID_i, PK_i) 是否进行过 H_1 询问, 若是, 算法 B 则查询 (R, s, h_1, PK, ID) , 并令 $\tilde{h} = h_1$, 随机选择

$z \in Z_q$, 进行 H_2 询问得到 h_2 , 计算 $Y = \frac{(X^u)^{h_2 R}}{R^z (g^u)^{h_2 \tilde{h}}}$ 。

返回签名 (Y, R, z) 。若否, 算法 B 则执行算法 $Certify$, 并用得到的证书用上述方法对消息进行签名, 返回签名信息。

计算阶段: 敌手 A 对 (ID^*, PK^*, m^*) 得到伪造签名 $\sigma_{(1)}^* = (Y^*, R^*, z_{(1)}^*)$ 。对同一 (Y^*, R^*, m^*) 经过 4 次 H_2 询问, 得到不同的 h_2 , 假设分别为 c_1 、 c_2 、 c_3 、 c_4 。多次询问后可以得到 $\sigma_{(2)}^* = (Y^*, R^*, z_{(2)}^*)$ 、 $\sigma_{(3)}^* = (Y^*, R^*, z_{(3)}^*)$ 和 $\sigma_{(4)}^* = (Y^*, R^*, z_{(4)}^*)$ 。同时 $u, r, x, y \in Z_q$ 且 $g^r = R^*$, $g^x = X$, $g^y = Y^*$, $PK^* = (g^u, X^u)$, $h_1 = H_1(PK^*, ID^*)$ 。根据式(2), 则有

$$\frac{(g^u)^{h_1 c_i} R^{*z} Y^*}{(X^u)^{c_i R^*}} = 1, \quad i = 1, 2, 3, 4$$

即 $uh_1 c_i + rz + y = xuc_i R^* \bmod q$, $i = 1, 2, 3, 4$ 。其中, u, r, x, y 对于敌手 A 为未知的, 解上述线性方程可以得到 x 即 DL 问题的解。

分析阶段: 当对 $H_1(PK, ID)$ 进行随机赋值时, 前后出现不一致时导致随机预言模型失败, 可能性为 $\frac{q_{h_1}}{q}$; 由于 Certification-query 和 Sign-query 阶段都可能进行 H_1 询问, 则最多询问次数为 $q_e + q_s$ 。根据随机语言模型的理性随机性, 存在 H_2 询问的可能性为 $\varepsilon_{h_2} \geq 1 - \frac{1}{q}$, 敌手 A 通过询问得到正确 H_2 的可能性为 $\frac{1}{q_{h_2}}$ 。因此敌手 A 成功的可能性为

$$\varepsilon' \geq \left(1 - \frac{q_{h_1}}{q}\right)^{q_e + q_s} \left(1 - \frac{1}{q}\right) \frac{1}{q_{h_2}} \geq \left(1 - \frac{q_{h_1}(q_e + q_s)}{q}\right) \left(1 - \frac{1}{q}\right) \frac{1}{q_{h_2}}$$

时间复杂度是由 Certification 询问和 Sign 询问中的幂操作影响的, 故 $t' = t + O(q_e + q_s)E$ 。

4 物联网环境下基于证书的跨域认证方案设计

4.1 系统模型

移动网络环境主要由移动设备 (MD)、移动

设备在本网络的认证代理 (HA) 和移动设备在外地网络的接入点代理 (FA) 构成, 其架构如图 1 所示。

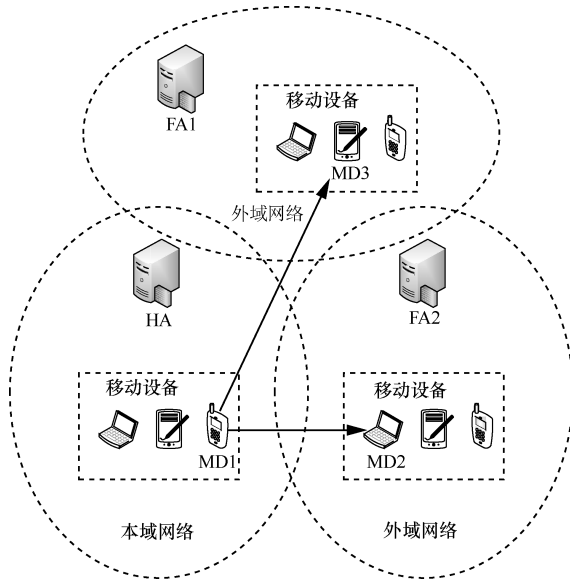


图 1 移动设备网络系统模型

当 MD 漫游到域外网络时, 只有通过了该域 FA 的认证才被允许接入。移动设备 MD 首先在 HA 进行注册, 生成公私钥; HA 为 MD 颁发证书并建立账户。当 MD 访问本域网络时, 可直接通过 HA 进行认证; 当 MD 访问域外网络时, 为了保证 MD 不被跟踪, 需要通过匿名跨域认证隐藏 MD 的真实身份, FA 对 MD 的匿名认证通过 FA 认证 HA 身份、HA 认证 MD 身份两步实现。由于 MD 发送的所有数据都经过 FA 转发, 因此 MD 的认证信息不能包含任何真实身份信息, 但同时又能使 HA 验证其真实身份。

4.2 方案设计

方案分为系统建立、移动设备注册、全认证、重认证 4 个阶段。

1) 系统建立

HA 选择素数 q 阶乘法循环群 G , 生成元为 g ; 选取 $s_{HA} \in Z_q^*$ 为其私钥, 计算 $P_{HA} = g^{s_{HA}}$ 为其公钥; 选取 $H_1: \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q^*$, $H_2: G \times G \times \{0,1\}^* \rightarrow Z_q^*$, 公开参数 $\{G, q, g, P_{HA}, H_1, H_2\}$ 。FA 选择与 HA 相同的参数 $\{G, q, g, H_1, H_2\}$, 并选取 $s_{FA} \in Z_q^*$ 作为私钥, 计算公钥 $P_{FA} = g^{s_{FA}}$, 公开参数 $\{G, q, g, P_{FA}, H_1, H_2\}$ 。

2) 移动设备注册

① 移动设备 MD 将 ID_{MD} 发送给 HA。

② HA 验证移动设备身份, 若通过, 则发送

P_{HA} 给移动设备, 移动设备选取 $s_{MD} \in Z_q^*$ 作为私钥, 计算 $PK_{MD} = (g^{s_{MD}}, P_{HA}^{s_{MD}})$, 并将公钥 PK_{MD} 发送给 HA。HA 选取 $r \in Z_q^*$, 计算 $h_1 = H_1(ID_{MD}, PK_{MD})$, $R = g^{-r}$, $s = r^{-1}(h_1 - s_{HA}R) \bmod q$, 生成证书 $Cert_{MD} = (R, s)$ 发送给移动设备, 移动设备可以通过 $R^{-s} P_{HA}^R = g^{h_1}$ 验证证书的正确性。

③ HA 为移动设备 MD 建立账户 (Ind_{MD}, Acc_{MD}) , 其中, $Ind_{MD} = R^s P_{HA}^R$ 为移动设备账户的索引, Acc_{MD} 是账户信息, 包括移动设备身份、有效期等。

3) 全认证

① 移动设备选取 $x, y \in Z_q^*$, 获取时间戳 T_{MD} , 计算 $K = P_{FA}^x$, $k = g^x$, $PK'_{MD} = (g^{s_{MD}}, P_{FA}^{s_{MD}})$, $h_1 = H_1(ID_{MD}, PK_{MD})$, $Y = R^{-y}$, $h_2 = H_2(Y, R, T_{MD})$, $z = y + h_2 s_{MD} \bmod q$; 发送消息 $(ID_{HA}, T_{MD}, K, h_1, h_2, Y, z, PK'_{MD})$ 给 FA。

② FA 收到消息后, 若 T_{MD} 新鲜, 则获取时间戳 T_{FA} , 签名并发送消息 $(ID_{HA}, Y, h_1, h_2, z, Cert_{FA}, Sig(ID_{HA}, Y, h_1, h_2, z, Cert_{FA}))$ 给 HA。

③ HA 收到消息后, 若 T_{FA} 新鲜且签名验证通过, 则 HA 通过对 FA 的认证, HA 计算 $Ind_{MD} = g^{h_1}$, 取出移动设备信息, 验证 $\frac{(g^{s_{MD}})^{h_1 h_2} R^z Y}{(P_{HA}^{s_{MD}})^{h_2 R}} = 1$ 是否成立, 若成立则 HA 通过对移动设备 MD 的认证。HA 获取时间戳 T_{HA} , 签名并发送消息 $(ID_{FA}, Cert_{HA}, T_{HA}, T_{FA}, Sig(ID_{FA}, Cert_{HA}, T_{HA}, T_{FA}))$ 给 FA。

④ FA 收到消息后, 若 T_{HA} 新鲜且签名验证通过, 则 FA 通过对 HA 的认证。FA 创建移动设备临时身份 ID' , 选取 $r' \in Z_q^*$, 计算 $R' = g^{-r'}$, $h'_1 = H_1(ID', PK'_{MD})$, $s' = r'^{-1}(h'_1 - s_{FA}R') \bmod q$, 为移动设备颁发临时证书 $Cert'_{MD} = (R', s')$, 建立临时账户 (Ind'_{MD}, Acc'_{MD}) , 其中 $Ind'_{MD} = R'^{s'} P_{FA}^{R'}$ 为移动设备账户的索引, Acc'_{MD} 是临时账户信息, 包括移动设备临时身份、有效期等。FA 计算 $k_0 = k = K^{s_{FA}^{-1}}$, 获取时间戳 T'_{FA} , 发送 $(T'_{FA}, E_{k_0}(T'_{FA}, T_{MD}, R', s', ID'))$ 给移动设备 MD, 其中, E_{k_0} 为对称加密。

⑤ 移动设备 MD 收到消息后, 若 T'_{FA} 新鲜, 则用 k 解密 $E_{k_0}(T'_{FA}, T_{MD}, R', s', ID')$, 并核对 T'_{FA} 、

T_{MD} ，若一致，则移动设备通过对 FA 的认证，并把 k 作为之后的会话密钥。

4) 重认证

当移动设备 MD 再次访问域 B 中的资源时，若临时证书在有效期，则移动设备 MD 可以通过临时身份 ID' 和临时证书 (R', s') 进行快速认证，而无需通过 HA 参与。

① 移动设备选取 $y \in Z_q^*$ ，获取时间戳 T_{MD} ，计算 $Y = R^{-y}$ ， $h_2 = H_2(Y, R, T_{MD})$ ， $z = y + h_2 s_{MD} \bmod q$ ， $h_1 = H_1(ID_{MD}, PK_{MD})$ ， $PK_{MD}' = (g^{s_{MD}}, P_{FA}^{s_{MD}})$ ；发送消息 $(ID_{FA}, T_{MD}, h_1, h_2, Y, z)$ 给 FA。

② FA 收到消息后，若 T_{MD} 新鲜，计算 $Ind_{MD}' = g^{h_1}$ ，取出移动设备信息，验证 $\frac{(g^{s_{MD}})^{h_1 h_2} R^z Y}{(P_{FA}^{s_{MD}})^{h_2 R}} = 1$ 是否成立，若成立则通过对移动设备 MD 的认证。FA 获取时间戳 T_{FA} ，选取 $r_i \in Z_q^*$ ，计算 $k_i = H_1(r_i, k_{i-1})$ ，发送消息 $(T_{FA}, E_{k_{i-1}}(T_{FA}, T_{MD}, r_i))$ 给移动设备 MD。

③ 移动设备 MD 收到消息后，若 T_{FA} 新鲜，则用 k_{i-1} 解密 $E_{k_{i-1}}(T_{FA}, T_{MD}, r_i)$ ，核对 T_{FA} 、 T_{MD} ，若一致，则移动设备通过对 FA 的认证。计算 $k_i = H_1(r_i, k_{i-1})$ ，并把 k_i 作为本次通信的会话密钥。

5 基于证书的匿名跨域认证方案分析

5.1 认证安全性

在跨域认证方案的全认证过程中，实现了实体间的双向认证。在全认证过程中，HA 和 FA 之间的认证是基于公钥密码实现的，签名中包含时间戳，有效避免了重放攻击；HA 对 MD 的认证是基于 CBS 方案实现的，3.2 节对 CBS 方案的不可伪造性进行了证明；MD 对 FA 的认证是基于对称密码实现的，用于认证的密钥只有认证双方可以通过计算获得，确保了认证的安全性；FA 对 MD 的认证是通过 FA 对 HA、HA 对 MD 的认证

间接实现的。

5.2 匿名性和不可跟踪性

用户的真实身份只对本域的认证服务器 HA 公开，用户和其他域的认证服务器 FA 都无法确定用户的真实身份。在全认证过程中，用以交互进行身份认证的消息不包含用户的身份信息，HA 通过验证用户签名信息、计算用户索引认证用户身份，因此除 HA 外其他实体不能获得用户真实身份。在全认证阶段，FA 为用户建立临时身份，在重认证时，FA 仅能确认用户的临时身份，通过验证签名信息完成用户认证，而无法得到用户的真实身份。

另外，用户每次进行认证时选择对时间戳进行签名作为认证信息，认证消息具有随机性，除本域认证服务器 HA 和访问域认证服务器 FA 外，其他实体无法将不同的认证消息联系起来。

5.3 会话密钥建立与更新

在认证过程中，会话密钥是在会话双方之间建立的，移动设备选择秘密参数 $x \in Z_q^*$ ，计算 $K = P_{FA}^x$ ， $k = g^x$ ，并将 k 作为会话密钥，将 K 发送给访问域认证服务器 FA，访问域 FA 用自己的私钥 s_{FA} ，计算 $k_0 = k = K^{s_{FA}^{-1}}$ 得到会话密钥，移动设备可以通过解密 $E_{k_0}(T_{FA}, T_{MD}, R', s', ID')$ ，核对 T_{MD} 确认 FA 计算得到了正确的会话密钥。其他实体无法获得会话密钥，包括本域认证服务器 HA。

在重认证过程中，新的会话密钥是在原会话密钥的基础上通过杂凑得到的，使每次会话的密钥均不相同。

文献[18]方案用户和 FA 之间的会话密钥是通过 HA 间接建立的，HA 同样掌握会话密钥，因此本方案的安全性优于文献[18]方案。

5.4 效率分析

本文方案集成了 PKI 和 IBS 的特性和优点，并且在整个认证过程中没有对运算。本文方案与文献[8,12,18]中方案的效率进行对比结果如表 1 所示。

表 1 效率比较

方案	对运算 (MD/FA/HA)	公钥加解密 (MD/FA/HA)	对称加解密 (MD/FA/HA)	散列 (MD/FA/HA)
文献[8]	0/0/0	0/3/3	2/1/1	2/1/1
文献[12]	0/0/1	0/2/2	1/1/0	1/0/1
文献[18]	0/0/0	0/3/3	1/1/0	2/1/1
本文方案	0/0/0	0/2/2	1/1/0	2/1/0

通过对比可知,相对于文献[8]的方案,本文方案有更少的公钥和对称加解密;相对文献[12]的方案,本文方案所有实体均不进行对运算,虽然MD多进行一次散列运算,但整体计算开销较小;相对于文献[18]的方案,有更少的公钥加解密。本文方案中虽然使用证书和用户私钥一起进行签名操作,但并不涉及复杂的证书管理,同时相对于基于身份的跨域认证方案,没有密钥托管和密钥分发问题,因此更适合应用在移动设备的跨域认证中。

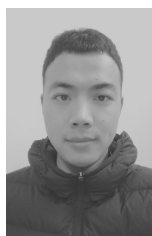
6 结束语

移动设备的跨域认证是物联网发展过程中面临的主要问题之一。本文提出一种适用于移动设备的跨域认证方案,该方案在保证安全性和匿名性的基础上,具有更少的计算量和通信开销,提高了认证的效率。通过与其他跨域认证方案相比,本文方案在安全上和效率上具有明显优势,使其能够满足网络漫游中移动设备的匿名认证要求。

参考文献:

- [1] ROMAN R, ZHOU J, LOPEZ J. On the features and challenges of security and privacy in distributed internet of things[J]. Computer Networks, 2013, 57(10):2266-2279.
- [2] 武传坤. 物联网安全关键技术与挑战[J]. 密码学报, 2015, 2(1):40-53.
WU C K. An overview on the security techniques and challenges of the Internet of things[J]. Journal of Cryptologic Research, 2015, 2(1):40-53.
- [3] 张玉清, 周威, 彭安妮. 物联网安全综述[J]. 计算机研究与发展, 2017, 54(10):2130-2143.
ZHANG Y Q, ZHOU W, PENG A N. Survey of Internet of things security[J]. Journal of Computer Research and Development, 2017, 54(10): 2130-2143.
- [4] HINAREJOS F, LOPEZ J, MONTENEGRO J A, et al. Pervasive authentication and authorization infrastructures for mobile users[J]. Computers & Security, 2010, 29(4):501-514.
- [5] LEE D G, KANG S I, SEO D H, et al. Authentication for single/multi domain in ubiquitous computing using attribute certification[C]//International Conference on Computational Science and ITS Applications. 2006:326-335.
- [6] AYE N, KHIN H S, WIN T T, et al. Multi-domain public key infrastructure for information security with use of a multi-agent system[M]//Intelligent Information and Database Systems. Berlin: Springer, 2013:365-374.
- [7] BELLARE M, NAMPREMPRE C, NEVEN G. Security proofs for identity-based identification and signature schemes[C]//Advances in Cryptology Eurocrypt 2004. 2004:268-286.
- [8] 罗长远, 霍士伟, 邢洪智. 普适环境中基于身份的跨域认证方案[J]. 通信学报, 2011, 32(9):111-115.
- LUO C Y, HUO S W, XING H Z. Identity-based cross-domain authentication scheme in pervasive computing environments[J]. Journal on Communications, 2009, 30(4):130-136.
- [9] GENTRY C. Certificate-based encryption and the certificate revocation problem[C]//International Conference on Theory and Applications of Cryptographic Techniques. 2003:272-293.
- [10] KANG B G, PARK J H, SANG G H. A certificate-based signature scheme[C]//Cryptographers Track Research Conference. 2004: 99-111.
- [11] LIU J K, BAEK J, SUSILO W, et al. Certificate-based signature schemes without pairings or random oracles[C]//International Conference on Information Security. 2008:285-297.
- [12] 朱辉, 李晖, 苏万力, 等. 基于身份的匿名无线认证方案[J]. 通信学报, 2009, 30(4):130-136.
ZHU H, LI H, SHU W L, et al. ID-based wireless authentication scheme with anonymity[J]. Journal on Communications, 2009, 30(4):130-136.
- [13] LI J, WANG Z, ZHANG Y. Provably secure certificate-based signature scheme without pairings[M]. Elsevier Science Inc. 2013:313-320.
- [14] LI J, HUANG X, MU Y, et al. Certificate-based signature: security model and efficient construction[J]. Public Key Infrastructure, 2007, (4582):110-125.
- [15] VERMA G K, SINGH B B. Short certificate-based proxy signature scheme from pairings[J]. Transactions on Emerging Telecommunications Technologies, 2017(1):3214.
- [16] ZHANG Y, LI J G, WANG Z, et al. A new efficient certificate-based signature scheme[J]. Chinese Journal of Electronics, 2015, 24(4):776-782.
- [17] MAN H A, LIU J K, SUSILO W, et al. Certificate based (linkable) ring signature[C]//International Conference on Information Security Practice and Experience. 2007:79-92.
- [18] 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.
PENG H X, FENG D G. Security flaws and improvement to a wireless authentication protocol with anonymity[J]. Journal on Communications, 2006, 27(9):78-85.

[作者简介]



丁永善(1992-), 男, 河南周口人, 信息工程大学硕士生, 主要研究方向为信息安全。

李立新(1967-), 男, 重庆人, 博士, 信息工程大学研究员, 主要研究方向为数据库、信息安全。

李作辉(1981-), 男, 湖南衡阳人, 博士, 信息工程大学副研究员, 主要研究方向为信息安全。