文章编号:1005-0523(2020)01-0113-06

一种基于密钥捆绑的无证书签名方案

涂晓斌[1],艾美珍[1,2],左黎明[1,2],易传佳[1,2],周 晓[1],邓国健[3]

(华东交通大学 1. 理学院; 2. 系统工程与密码学研究所; 3. 信息工程学院,江西 南昌 330013)

摘要:针对传统无证书签名方案中公钥和公钥持有者之间缺乏认证的问题,提出了一种基于密钥捆绑的无证书签名方案。在随机预言机模型和Inv-CDH困难问题假设下证明了方案的安全性。同时与其他无证书签名方案进行了效率比较,结果表明所提方案在计算效率上有一定优势,适用计算能力受限的物联网应用场合。

关键词:密钥捆绑;无证书签名;随机预言机模型;可证明安全

中图分类号:TP309.7 **文献标志码**:A

DOI:10.16749/j.cnki.jecjtu.2020.01.016

1976年,传统公钥密码体制被Diffie和Hellman[1]首次提出,该密码体制中公钥需依赖可信证书机构(certificate authority, CA)与用户身份关联,但CA的管理增加了系统维护成本。基于身份的密码体制在1984年被Shamir[2]提出,解决了公钥与用户的关联问题,却带来了密钥托管问题[3]。Al-Riyami和Paterson[4]在2003年提出了无证书密码体制,不仅克服了公钥密码体制中的CA证书管理问题,还解决了基于身份的密码体制的密钥托管问题。由此,无证书密码体制被广泛应用于数字签名[5]中,成为了当前国内外专家的研究热点[6-8]。2015年,汤永利等人[9]提出了一类无证书签名方案,且通过形式化的安全证明表明该方案具有较高安全性。2017年,周彦伟等人[10]提出了一个高效安全的无证书签名方案,实验表明该方案具有较高的计算效率。2018年,吴涛等人[11]指出Huang等人[12]所提出的无证书方案不能抵抗第二类敌手的攻击,并给出了改进方案。本文针对于无证书签名方案中公钥与持有者之间没有认证关系,提出了一种基于密钥捆绑的无证书签名方案,通过对用户自选参数和公钥进行密钥捆绑,可有效防止公钥替换攻击,阻断针对无证书签名的第一类攻击者,另一方面该方案中的部分私钥可以通过所申请的部分私钥授权码广播吊销,可以阻断密钥泄露后带来的进一步安全问题。

1 基础知识

1.1 安全性假设

定义1 双线性对[13](bilinear pairing,BP)

若G_1为q阶加法循环群,G_2为q阶乘法循环群,映射$e:G_1\times G_1\rightarrow G_2$称为双线性对映射则满足以下3条性质:

1) 双线性性:$e(aP,bQ)^{ab}$,其中$P,Q\in G_1$, $a,b\in Z_q$;

2) 非退化性:存在$P,Q\in G_1$,使得$e(P,Q)\neq 1$;

收稿日期:2019-04-17

基金项目:国家自然科学基金项目(11761033);江西省教育厅科技项目(GJJ180323,GJJ170386);江西省学位与研究生教育教学改革研究项目(JXYJG-2018-095)

作者简介:涂晓斌(1967—),男,教授,研究方向为工程制图。

3）可计算性：任给 $P,Q\in G_1$，$e(P,Q)$是可以被计算的。

定义 2 逆计算性 Diffie-Hellman 问题（inverse computational diffie-hellman problem，Inv-CDH）

给定 $P,aP\in G_1$，其中 $a\in Z_q^*$，且 a 未知，计算 $\frac{1}{a}P\in G_1$。值得注意的是该问题有多个变体，例如：给定 $P,aP\in G_1,b\in Z_q^*$ 其中，且 a 未知，计算 $\frac{1}{a+b}P$。

1.2 改进后的无证书数字签名定义

由于在传统无证书签名方案中，用户公钥与用户身份缺乏认证关系，使得该签名方案容易遭受恶意攻击。文献[14]提出基于双重的无证书短签名方案，实现了用户身份与秘密值的绑定，避免了恶意用户的公钥替换攻击，但该方案所提出的双重的设置较为复杂，在实际应用中部署较为繁琐。本文提出了基于密钥捆绑的无证书签名方案，该方案由七个算法组成，其定义如图 1 所示。

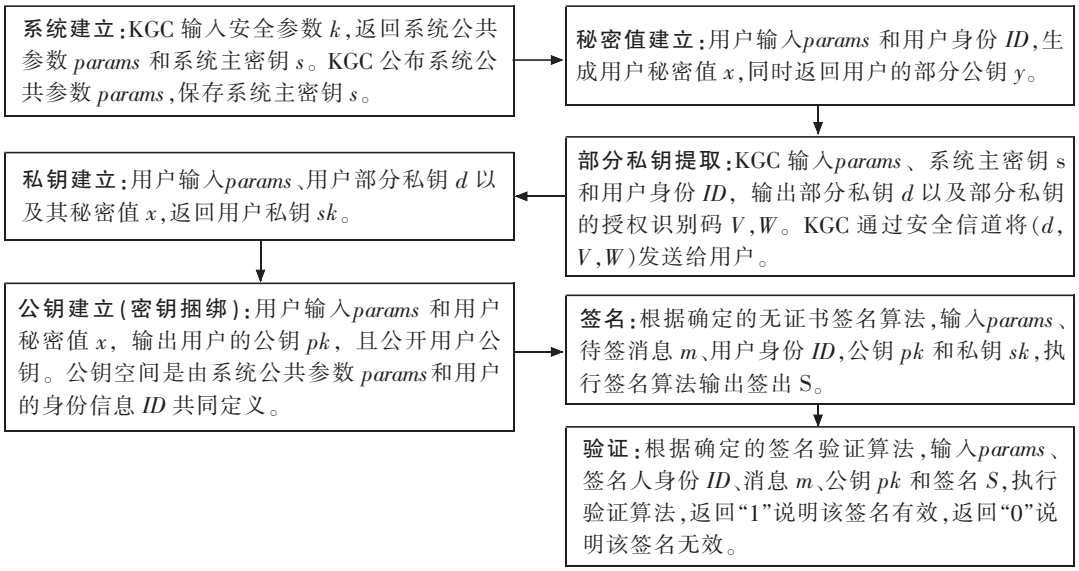

图 1 改进的无证书签名定义

Fig.1 Improved certificate-free signature definition

2 基于密钥捆绑的无证书签名方案构造

方案由 7 个算法组成，具体描述如下：

1）系统建立：给定安全参数 k，选择阶都为素数 $q>2^k$ 的加法循环群 G_1 和乘法循环群 G_2，设 P 是 G_1 的生成元，选择双线性对 $e:G_1\times G_1\rightarrow G_2$，选择安全抗碰撞哈希函数：$H_1:\{0,1\}^*\rightarrow Z_q^*$，$H_2:\{0,1\}^*\rightarrow Z_q^*$。*KGC* 任选一个随机数 $s\in Z_q^*$ 作为系统主密钥，秘密保存 s，计算 $y_{pub}=sP\in G_1$ 作为系统公钥，公布系统参数：$params=\{k,G_1,G_2,e,q,P,y_{pub},H_1,H_2\}$。

2）秘密值建立：签名用户 *user* 随机选择秘密值 $x\in Z_q^*$，计算并公开用户部分公钥 $y=xP\in G_1$。

3）部分私钥提取：签名用户 *user* 身份为 $ID\in(0,1)^*$，*KGC* 随机选择 $v,w\in Z_q^*$，计算 $V=vP,W=wP,Q=H_1(ID,y_{pub},y,V,W)$，计算私钥 $d=s^{-1}(w+vQ)$，其中 V,W 作为用户 *user* 申请部分私钥的授权识别码，可用于广播吊销泄露的部分私钥，最后 *KGC* 通过安全信道发送(d,V,W)给用户。部分私钥合理性可以通过等式 $e(dP,y_{pub})=e(W+QV,P)$验证。

4）私钥建立：签名用户 *user* 的私钥为(x,d)。

5）公钥建立（密钥捆绑）：签名用户 *user* 计算：$U=xy_{pub}$，并将用户公钥(y,U,V,W)公开，其中参数 U 用于对 KGC 和用户进行密钥捆绑，防止公钥替换，任何人可以用 $e(U,P)=e(y_{pub},y)$来验证有效性。

6）签名：签名用户 *user* 对消息 $m\in(0,1)^*$ 签名得到签名 S 的步骤如下：

① 计算 $h=H_2(m,y_{pub},y,U,V,W)$;

② 计算 $S=\frac{d}{x+h}P$。

7) 签名验证:签名验证者验证签名 $\sigma=(m,S)$,步骤如下:

① 计算 $Q=H_1(ID,y_{pub},y,V,W)$,这个可以预计算后一直使用;

② 计算 $h=H_2(m,y_{pub},y,U,V,W)$;

③ 当 $e(S,U+hy_{pub})=e(W+QV,P)$成立,则签名验证成功,否则签名验证失败。

方案的正确性证明如下

$$e(S,U+hy_{pub})=e(\frac{d}{x+h}P,xsP+hsP)=e(\frac{(w+vQ)}{s(x+h)}P,s(x+h)P)=e(W+QV,P)$$

3　安全性证明

在无证书签名方案中,其安全模型所讨论的敌手[15]主要分为以下两类:

1) 第一类敌手 A(模拟不诚实的用户):不知道系统主密钥和用户部分私钥,但可以替换用户公钥。

2) 第二类敌手 A_2(模拟恶意但被动的 KGC):掌握了系统主密钥和用户部分私钥,但不能替换用户公钥。

关于两类敌手的安全游戏模型的形式化描述详见文献[16],限于篇幅,本文不再赘述。由于本方案在用户公钥建立时进行了密钥捆绑,用户与用户公钥之间存在关联且可公开验证,可以避免了第一类敌手的公钥替换攻击。因此本文针对掌握系统主密钥和部分私钥的第二类敌手攻击,给出随机预言机下的安全性证明。

定理　在随机预言机模型下,针对第二类敌手 A_2,在适应性选择消息攻击下本文所提出的无证书签名方案是存在性不可伪造的。

引理　假设 A_2 在概率多项式时间 t 内以不可忽略的概率 ε 攻破了本文方案, 记 $q_x,q_{H_1},q_{H_2},q_E,q_{pk},q_S$ 分别为敌手 A_2 做秘密值询问,H_1 询问,H_2 询问,部分私钥解析询问,公钥询问以及签名询问的次数;记 $t_x,t_{H_1},t_{H_2},t_E,t_{pk},t_S$ 分别为敌手 A_2 做秘密值询问,H_1 询问,H_2 询问、部分私钥解析询问,公钥询问以及签名询问的一次所需的时间,则存在概率多项式时间算法 C,在时间 t'内以不可忽略的优势 ε'解决 Inv-CDH 问题。其中

$$t'<t+q_xt_x+q_Et_E+q_{pK}t_{pK}+q_St_S+2(q_{H_1}t_{H_1}+q_{H_2}t_{H_2}),\varepsilon'>(\varepsilon-\frac{1}{2^k})\cdot(\frac{q_x-1}{q_x})^{q_S}\cdot\frac{1}{q_x}$$

证明:给定一个 Inv-CDH 问题实例:已知 $P,aP\in G_1,b\in Z_q^*$,其中 $a\in Z_q^*$,且 a 未知,要输出$\frac{1}{a+b}P$。

C 选择 $s\in Z_q^*$ 作为系统主密钥, 计算 $y_{pub}=sP\in G_1$ 作为系统公钥, 运行系统建立算法, 将公开参数 $Params=\{k,G_1,G_2,e,q,P,y_{pub},H_1,H_2\}$和系统主密钥 s 发送给 A_2,且选择 ID^* 作为挑战身份,C 的目标是通过 A_2 的能力计算出$\frac{1}{a+b}P\in G_1$。

记列表 $L_x,L_{H_1},L_{H_2},L_E,L_{pk},L_S$ 为 A_2 的秘密值询问,H_1 询问,H_2 询问,部分私钥解析询问,公钥询问以及签名询问的跟踪记录。A_2 询问过程如下:

1) 秘密值询问:当 A_2 对 ID_i 进行秘密值询问时,查找由数组(ID_i,x_{ID_i},y_{ID_i})构成的列表 L_x 是否存在 ID_i 的记录,若存在则将查找的值返回给 A_2,否则:①若 $ID_i\neq ID^*$,则 C 随机选取 $x_{ID_i}\in Z_q^*$,计算 $y_{ID_i}=x_{ID_i}P\in G_1$,并将值 x_{ID_i} 发送给 A_2,且将数组(ID_i,x_{ID_i},y_{ID_i})记录到 L_x 中;②若 $ID_i=ID^*$,则令 $aP\in G_1$ 为用户部分公钥 y_{ID_i},并将“⊥”返回给 A_2,同时将数组$(ID_i,\perp,y_{ID_i})$记录到 L_x 中,其中“⊥”表示为空。

2) H_1 询问:当 A_2 对 ID_i 进行 H_1 询问时,查找由数组$(ID_i,v_{ID_i},w_{ID_i},V_{ID_i},W_{ID_i},Q_{ID_i})$构成的列表 L_{H_1} 是否存在 ID_i 的记录,若存在则向 A_2 返回对应的值,否则:C 随机选取 $v_{ID_i},w_{ID_i}\in Z_q^*$,计算 $V_{ID_i}=v_{ID_i}P,W_{ID_i}=w_{ID_i}P$,选取 $Q_{ID_i}\in Z_q^*$ 作为 $H_1(ID_i,y_{pub},y_{ID_i},V_{ID_i},W_{ID_i})$的值,将值返回给 A_2,同时将数组$(ID_i,v_{ID_i},w_{ID_i},V_{ID_i},W_{ID_i},Q_{ID_i})$记录到 L_{H_1} 中。

3) 部分私钥询问:当 A_2 对 ID_i 进行部分私钥询问时,C 检查由数组$(ID_i,Q_{ID_i},v_{ID_i},w_{ID_i},d_{ID_i})$构成的列表 L_E 中是否存在 ID_i 的记录,若存在则将值返回给 A_2;否则:C 查找出 L_{H_1} 中 ID_i 的记录,计算 $d_{ID_i}=s^{-1}(w_{ID_i}+v_{ID_i}Q_{ID_i})$,并

将 d_{ID_k} 发送给 A_2，同时将 $(ID_i, Q_{ID_k}, v_{ID_k}, w_{ID_k}, d_{ID_k})$ 记录到 L_E 中。

4）公钥询问：当 A_2 对 ID_i 进行公钥询问时，C 检查由数组 $(ID_i, y_{ID_k}, U_{ID_k}, V_{ID_k}, W_{ID_k})$ 构成的列表 L_{pk} 中是否存在 ID_i 的记录，若存在则将值返回值 A_2，否则：C 查找出 ID_i 在 L_x 以及 L_{H_1} 中 ID_i 的记录，若 $ID_i \neq ID^*$，则计算 $U_{ID_k}=x_{ID_k}y_{pub}$，否则计算 $U_{ID_k}=x_{ID_k}y_{pub}=y_{ID_k}s$，将 $(y_{ID_k}, U_{ID_k}, V_{ID_k}, W_{ID_k})$ 返回给 A_2，并将 $(ID_i, y_{ID_k}, U_{ID_k}, V_{ID_k}, W_{ID_k})$ 记录到 L_{pk} 中。

5）H_2 询问：当 A_2 对 (ID_i, m_j) 进行 H_2 询问时，查找由数组 (ID_i, m_j, h_j) 构成的列表 L_{H_2} 是否存在 (ID_i, m_j) 的记录，若存在则向 A_2 返回对应的值，否则 C 查找列表 L_{pk} 中 ID_i 的记录，若 $ID_i \neq ID^*$，随机选取 $h_j \in Z_q^*$ 作为 $H_2(m_j, y_{pub}, y_{ID_k}, U_{ID_k}, V_{ID_k}, W_{ID_k})$ 的值，并将 h_j 返回给 A_2，同时将 (ID_i, m_j, h_j) 记录到列表 L_{H_2} 中，否则，将给定的实例中的 $b \in Z_q^*$ 作为 $H_2(m_j, y_{pub}, y_{ID_k}, U_{ID_k}, V_{ID_k}, W_{ID_k})$ 的值，并将 b 返回给 A_2，同时将数组 (ID_i, m_j, b) 记录到 L_{H_2} 中。

6）签名询问：当 A_2 对 (ID_i, m_j) 进行签名询问时，C 判断 ID_i 是否为挑战身份 ID^*，若 $ID_i=ID^*$，则输出“⊥”（即输出空值，记此事件为 E_1），否则，C 从 L_x 和 L_E 查找 ID_i 的记录，同时从 L_{H_2} 查找 (ID_i, m_j) 的记录，计算 $S_j=\frac{d_{ID_k}}{x_{ID_k}+h_j}P$，输出签名 S_j。

最后，A_2 停止询问，输出一个有效签名 σ。若签名 $\sigma=(m^*, S^*)$ 是挑战身份 ID^* 的，则 C 通过查询所维护的列表 $L_x, L_{H_1}, L_{H_2}, L_E, L_{pk}, L_S$，提取与 ID^* 的相关记录数组，其中：$y_{ID^*}=aP, h=b$ 为关于 m^* 的 H_2 询问值。

因为 $S^*=\frac{d_{ID^*}}{a+b}P$，则 C 可以成功的计算出 $\frac{1}{a+b}P=d_{ID^*}^{-1}S^*$，$C$ 输出 $d_{ID^*}^{-1}S^*$ 作为对挑战实例的应答，从而解决了 Inv-CDH 问题。

以下为解决 Inv-CDH 困难问题的优势：

1）A_2 对哈希函数 H_1, H_2 询问的应答在 Z_q^* 中是均匀分布的。

2）事件 E_1 不发生，则签名询问中的应答为有效应答。事件 E_1 一直不发生，且 A_2 输出一个有效签名 σ 是挑战身份 ID^* 的，才能成功解决 Inv-CDH 困难问题。其中事件 E_1 一直不发生的概率为 $(\frac{q_x-1}{q_x})^{q_s}$，$A_2$ 输出一个有效签名 σ 是挑战身份 ID^* 的概率为 $\frac{1}{q_x}$。

3）在没有做 H_2 询问的情况下，A_2 成功伪造了一个有效的签名，其发生的概率小于等于 $\frac{1}{2^k}$。

C 解决 Inv-CDH 困难问题的优势的下界估计为

$$\varepsilon' > (\varepsilon - \frac{1}{2^k}) \cdot (\frac{q_x-1}{q_x})^{q_s} \cdot \frac{1}{q_x}$$

而 C 所需的多项式时间上界估计为

$$t' < t + q_x t_x + q_E t_E + q_{pk} t_{pK} + q_S t_S + 2(q_{H_1} t_{H_1} + q_{H_2} t_{H_2})$$

综上所述，存在概率多项式时间算法，在时间内以不可忽略的优势解决 Inv-CDH 问题，这与 Inv-CDH 问题困难性矛盾。因此在随机预言机模型下，针对第二类敌手，在适应性选择消息攻击下本文所提出的无证书签名方案是存在性不可伪造的。

4 效率分析

4.1 性能比较

表 1 为本文方案性能比较分析，其中，M 代表倍乘运算，E 代表指数运算，P 代表双线性对运算。

由表 1 可知，在签名阶段本方案仅使用了 1 次的倍乘运算，而文献[4]方案使用了 1 次双线对运算和 3 次倍乘运算，文献[6]方案使用了 3 次倍乘运算，文献[7]方案使用了 1 次倍乘运算，文献[11]方案使用了 3 次指数运算和 1 次倍乘运算。本方案在签名阶段的计算量与文献[7]方案相近，较低于文献[4,6,11]方案；在签

名验证阶段本方案使用了 1 次双线对运算和 1 次倍乘运算。文献[4]方案使用了 4 次双线对运算和 1 次指数运算,文献[6]方案使用了 2 次双线对运算和 1 次倍乘运算,文献[7]方案使用了 1 次双线对运算和 2 次指数运算以及 1 次倍乘运算,文献[11]方案使用了 3 次双线对运算,通过对比可知,在此阶段本文方案计算量较低于文献[4,6,7,11]方案。综上,本方案计算复杂度较低,在性能效率方面略优于其他方案。

4.2　运行效率比较

在 64 位 windows7 操作系统、Intel(R) Core(TM) i3-4150 CPU @ 3.50 GHz 的 CPU 和 DDR3 1 600 MHz 16 G 的内存以及华硕 B85M-V5 PLUS 主板的运行环境下, 结合斯坦福大学开发的 PBC (Pairing-Based Cryptography)库,实现本文方案和文献[4,6,7,10]方案,并比较各个方案在经过 100 次运行后的平均耗时,其实验结果如表 2 所示。由表 2 可知,本文方案在签名阶段的平均耗时为 0.011 s,在验证阶段平均耗时为 0.030 s,方案的平均总耗时为 0.098 s。在方案的平均总耗时上,本文方案与文献[4]方案相比,减少了约 50.5%,与文献[6]方案相比,减少了约 28.5%,与文献[7]方案相比,减少了约 10.1%,与文献[11]方案相比,减少了约 45.6%,由此可知,本文提出的签名方案具有较高的运行效率。

表 1　方案效率分析与比较

Tab.1　Analysis and comparison of scheme efficiency

方案	签名阶段	验证阶段	签名长度
文献[4]	$P+3M$	$4P+E$	$2\|G_1\|$
文献[6]	$3M$	$2P+M$	$2\|G_1\|$
文献[7]	M	$P+2M$	$\|G_1\|$
文献[11]	$3E+M$	$3P$	$3\|G_1\|$
本文方案	M	$P+M$	$\|G_1\|$

表 2　方案运行 100 次平均耗时比较

Tab.2　The average time-consuming comparison of scheme running 100 times

s

方案	签名平均耗时	验证平均耗时	方案平均总耗时
文献[4]	0.053	0.096	0.198
文献[6]	0.032	0.052	0.137
文献[7]	0.012	0.043	0.109
文献[11]	0.045	0.068	0.180
本文方案	0.011	0.030	0.098

5　结束语

本文提出了一种基于双线对的无证书签名方案,并在随机预言机的模型下,基于 Inv-CDH 困难问题给出了方案的安全性证明。与传统的无证书签名方案对比,本文方案实现了公钥与持有者之间的捆绑认知,防止了公钥替换攻击。通过对比分析可知,本方案具有较高的计算效率。

参考文献:

[1] DIFFIE W,HELLMAN M. New directions in cryptography[J]. IEEE transactions on Information Theory,1976,22(6):644-654.

[2] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Workshop on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg,1984:47-53.

[3] 李林,李志华. 基于改进的动态密钥托管方案的研究及其应用[J]. 计算机工程与设计,2015,36(7):1732-1736.

[4] AL-RIYAMI S S,PATERSON K G. Certificateless public key cryptography[C]//International conference on the theory and application of cryptology and information security. Springer,Berlin,Heidelberg,2003:452-473.

[5] 马金花,刘江华,伍玮,等. 可修订数字签名研究综述[J]. 计算机研究与发展,2017,54(10):2144-2152.

[6] GAYATHRI N B,REDDY P V. Efficient certificateless signature scheme with provable security[C]//IEEE International Conference on Advanced Computing. New Jersey,2016:322-337.

[7] TSAI J L. A new efficient certificateless short signature scheme using bilinear pairings[J]. IEEE Systems Journal,2017,11(4):2395-2402.

[8] 程贤福,万冲,邱浩洋,等. 基于密度算法和DSM的模块划分方法[J]. 华东交通大学学报,2019,36(2):105-110.
[9] 汤永利,王菲菲,闫玺玺,等. 高效可证明安全的无证书签名方案[J]. 计算机工程,2016,42(3):156-160.
[10] 周彦伟,李骏. 可证安全的高效无证书签名方案[J]. 陕西师范大学学报(自然科学版),2017,45(5):17-22.
[11] 吴涛,景晓军. 一种强不可伪造无证书签名方案的密码学分析与改进[J]. 电子学报,2018,46(3):602-606.
[12] HUNG Y H,HUANG S S,TSENG Y M,et al. Certificateless signature with strong unforgeability in the standard model[J]. Informatica,2015,26(4):663-684.
[13] BONEH D,FRANKLIN M. Identity-based encryption from the weil pairing[J]. Siam Journal on Computing,2003,32(3):213-229.
[14] 左黎明,张梦丽,胡凯雨,等. 一种基于双重KGC的无证书短签名方案[J/OL]. 计算机应用研究:1-6[2019-04-05].https://doi.org/10.19734/j.issn.1001-3695.2018.10.0828.
[15] GONG ZHENG,LONG YU,HONG XUAN et al. Two certificateless aggregate signatures from bilinear maps[J]. Journal of Information Science & Engineering, 2007, 26(6):2093-2106.
[16] 王圣宝,刘文浩,谢琪. 无双线性配对的无证书签名方案[J]. 通信学报,2012,33(4):93-98.

A Certificateless Signature Scheme Based on Key Binding

Tu Xiaobin[1],Ai Meizhen[1,2],Zuo Liming[1,2],Yi Chuanjia[1,2],Zhou Xiao[1],Deng Guojian[3]

(1. School of Science,East China Jiaotong University,Nanchang 330013, China; 2. SEC Institute,East China Jiaotong University,Nanchang 330013,China; 3. School of Information Engineering,East China Jiaotong University,Nanchang 330013,China)

Abstract:Aiming at the problem of lack of authentication between the public key and public key holder in the traditional certificateless signature scheme, a certificateless signature scheme based on key binding is proposed. And the security of the scheme is ensured by the random oracle model and the assumption of Inv-CDH difficulty. At the same time, efficiency comparison with other certificateless signature schemes is carried out. The results show that the scheme has certain advantages in computational efficiency which is suitable for applications of Internet of Things with limited computational power.

Key words: key binding;certificateless signature;ability training;provably secure