公钥不可替换无证书签名方案

夏 峰[1,2] 杨 波[3]
(华南农业大学信息学院 广州 510642)[1] (广东医学院信息工程学院 东莞 523808)[2]
(陕西师范大学计算机科学学院 西安 710062)[3]

摘 要 基于 Al-Riyami 框架的无证书签名(CLS)的安全性以密钥分发中心(KGC)不能实施公钥替换攻击为前提,存在能被 KGC 实施公钥替换攻击这一缺陷。给出公钥不可替换攻击无证书签名体制的定义,提出通过对用户的公钥签名来抵抗任何敌手(包括 KGC)实施的公钥替换攻击,以将无证书签名的安全性提升到一个新的级别。基于 Al-Riyami 的方案给出了新方案的构造实例,基于随机预言机模型证明了公钥签名算法的安全性。该方案构造的对公钥的签名方法适用于所有基于 Al-Riyami 框架的双线性对无证书签名方案。

关键词 双线性对,无证书签名,公钥替换攻击,ROM
中图法分类号 TP309.2 **文献标识码** A

Certificateless Signature Scheme without Public Key Replaced

XIA Feng[1,2] YANG Bo[3]
(College of Informatics, South China Agricultural University, Guangzhou 510642, China)[1]
(School of Information Engineering, Guangdong Medical College, Dongguan 523808, China)[2]
(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)[2]

Abstract In certificateless signature (CLS) based on Al-Riyami frame, the secure condition is key generation center (KGC) which can not implement public key replacement attack. So CLS can not resist this attack from KGC. A new signature system called certificateless signature without public key replaced was presented. It shows that public key signature for users can resist the public key replacement attack from KGC and raise the security of CLS to a new level. An instance of constructing this class of certificateless signature scheme based on Al-Riyami frame was afforded. The public key signature was proven unforgery under the random oracle model. The method to construct the public key signature can be applied to any certificateless signature schemes based on Al-Riyami frame.

Keywords Bilinear pairing, Certificateless signature, Public key replacement attack, ROM

1 引言

Al-Riyami 和 Paterson 于 2003 年提出了无证书的密码系统[1],给出了无证书签名 CLS(Certificateless Signature)的详细定义,基于该定义构造了第一个无证书签名系统。该签名系统用到一个第三方密钥分发中的 KGC(Key Generation Center),其作用是生成用户的部分私钥。用户的完整私钥由用户随机选取的秘密值以及 KGC 帮他生成的部分私钥共同产生,其公钥由用户根据系统参数以及自己的秘密值进行一定运算生成。无证书签名的优势在于:相对基于证书的公钥体制,不需要系统在计算、存储和管理证书方面付出大量的代价;与基于身份的公钥体制下的数字签名相比,其没有基于身份的密码系统中的密钥托管问题。无证书签名系统在实践中具有较强的实用性,因为近几年它已成为签名系统的一个研究热点。Hung 等人基于文献[1]的工作定义了两类无证书签名的安全性证明模型[2],证明文献[1]的方案在随机预言机模型下对第 2 类攻击是可证安全的。后来,许多学者提出一些高效的基于双线性对的无证书签名方案[3-13]。葛等人[14]基于一般的离散对数困难性问题,提出具有强安全性的不含双线性对的无证书签名方案,相对其他方案效率较高。刘等人[15]利用知识证明方法构造了一个无证书签名方案,其通信复杂度较高,与其它方案相比效率较低。

然而,由于缺少对公钥的认证,无证书签名方案必须能抵抗公钥替换攻击。但在已有的方案中,许多方案不具备这一特性,如文献[1,3-5],对这些方案的攻击分别见文献[2,16-18]。同时,现有的能抵抗公钥替换攻击的方案都是以假定 KGC 不能实施公钥替换攻击和用户的部分密钥对其他人保密为前提的。拥有私钥的用户和 KGC 都能产生多个该用户的有效公钥,也都拥有该用户的部分密钥,若 KGC 实施替换公钥攻击,或是部分密钥泄露,则用户无法向第三方证明

到稿日期:2011-09-23 返修日期:2011-12-23 本文受国家自然科学基金(60973134,61173164),广东省自然科学基金(10351806001000000)资助。

夏 峰(1975-),男,博士生,讲师,主要研究方向为公钥密码算法、安全多方计算,E-mail:xiafeng166@yahoo.com.cn;杨 波(1963-),男,博士,教授,博士生导师,主要研究方向为密码算法、安全多方计算协议。

KGC 或获得部分密钥的敌手所伪造的公钥。因此，已有的无证书签名方案并不能抵抗来自 KGC(包括因泄露部分密钥所引起)的公钥替换攻击。从安全角度而言，它的有效性完全依赖于 KGC 的可信度，本质上讲，它与基于身份的签名方案无多大区别，这一点限制了它的发展和应用。基于该缺陷，本文给出能抵抗来自任何敌手(包括 KGC)的公钥替换攻击的无证书签名方案的新定义，提出在 KGC 和要注册的用户(即该 KGC 的申请者)之间执行公钥签名协议。其主要思想是：在保密注册用户 ID 的前提下，使其能安全地获取 KGC 对其公钥(绑定了该用户的 ID 和私钥)的部分签名，以作为其公钥的有效性的证据。但只有该用户向 KGC 发送 ID，并且通过 KGC 验证了公钥的有效性后，该用户才能获得在无证书签名的验证过程所使用的有效公钥签名。在签名的接收者验证该公钥签名的有效性时，只需要该用户的公钥和相应的系统参数，而并不需要公钥证书，因此仍保持了其无证书性质。该协议借用了数字承诺[19]原理，即申请者发送公钥的同时，承诺了使用公钥的 ID 及对应的私钥，在他获得对该公钥的认证后，必须打开其中的一个承诺(即 ID)，才能获得全部有效的公钥签名。基于随机预言机模型，对公钥签名协议中的验证公式进行了安全性证明。表明，该协议能抵抗任何 KGC 或是 ID 用户的恶意攻击。

2 预备知识

2.1 双线性映射及数学困难问题

假设 G_1 是一个阶为素数 q 的加法群，P 是它的一个生成元；G_2 是与 G_1 具有相同阶的乘法群。若一个映射：$G_1\times G_1\to G_2$ 满足以下 3 条性质，则称其为双线性映射。

(1) 双线性：对于任何 $U,V,W\in G_1$，有 $e(U,V+W)=e(U,V)e(U,W)$，从而对于任意 $a,b\in Z_q$，有 $e(aU,bV)=(U,V)^{ab}=e(abU,W)=e(U,abW)$；

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

(3) 可计算性：对任何 $U,V\in G_1$，存在一个高效算法以计算 $e(U,V)$。

基于双线性映射的困难问题描述如下。

定义 1(双线性对的离散对数问题，BCDH) 设 G_1，P 是前面双线性映射中定义的参数，则 G_1 中的离散对数问题描述如下：给定 $h\in G_1$，找到一个值 $a\in Z_q$，使得 $h=aP$。

2.2 无证书签名方案定义

定义 2[1] 一个无证书签名方案由系统参数生成、部分密钥生成、设置秘密值、设置私钥、设置公钥、签名以及验证 7 个算法组成。通常，前两个算法由 KGC 执行，而其它算法由签名者或验证者执行。下面是对各个算法的描述。

系统参数生成：输入安全参数 k，输出系统主密钥 master-key 和系统公开参数 params，其中系统公开参数 params 向系统中的全体用户公开，而主密钥 master-key 则由 KGC 秘密保存。

部分密钥生成：输入系统参数 params、用户的身份 ID 和系统主密钥 master-key，KGC 为用户输出部分私钥 D_{ID}。

设置秘密值：输入系统参数 params 和用户身份 ID，输出该用户的秘密值 x_{ID}。

设置私钥：输入系统参数 params、用户的身份 ID、该用户的秘密值 x_{ID} 和部分私钥 D_{ID}，输出该用户的私钥 S_{ID}。

设置公钥：输入系统参数 params、用户的身份 ID、秘密值 x_{ID} 和部分私钥 D_{ID}，输出该用户的公钥 P_{ID}。

签名：输入系统参数 params、消息 M、用户的身份 ID、其公钥 P_{ID} 及私钥 S_{ID}，输出该用户对消息 M 的签名 σ。

验证：输入系统参数 params、消息 M、签名 σ、签名者的身份 ID 及公钥 P_{ID}，当检验签名有效时，输出 1；否则，输出 0。

2.3 安全模型

在无证书系统中有两类攻击者，即第 1 类攻击者 AI 与第 2 类攻击者 AII。第 1 类攻击者不知道系统主密钥，但可以任意替换用户的公钥。第 2 类攻击者知道系统的主密钥，但不能替换目标用户的公钥。在实际应用中，AI 模拟的是除 KGC 之外的攻击者；而 AII 模拟的是恶意的 KGC。

无证书签名方案的安全性可用下面的挑战者 C 和攻击者 AI 或 AII 间的两个游戏来定义[2]。游戏 1(适用于第 1 类攻击者)：

初始化：C 运行系统参数生成算法，输入安全参数 k，输出系统主密钥 master-key 和系统参数 params。C 将 params 发送给 AI，而对主密钥 master-key 严格保密。

攻击：AI 可以适应性地进行公钥询问、部份私钥询问、秘密值询问、公钥替换询问以及签名询问，C 模拟签名方案中的相应算法，分别做出回答。

伪造：最后 AI 输出一个四元组(M^*,σ^*,ID^*,P^*)。AI 赢得了这个游戏，当且仅当：

(1)σ^* 是公钥为 P^*、身份为 ID^* 的用户对消息 M^* 的一个有效签名；

(2)AI 没有询问过身份为 ID^* 的用户的部分私钥；

(3)AI 没有询问过身份为 ID^*、公钥为 P^* 的用户对 M^* 的签名。

游戏 2(适用于第 2 类攻击者)：

初始化：C 运行系统参数生成算法，输出系统主密钥 master-key 和系统参数 params。C 将 master-key 和 params 发送给 AII。

攻击：AII 可以适应性地进行公钥询问、秘密值询问、公钥替换询问以及签名询问，C 模拟签名方案中的相应算法分别做出回答。

伪造：最后 AII 输出一个四元组(M^*,σ^*,ID^*,P^*)。我们说 AII 赢得了这个游戏，当且仅当：

AII 没有询问过身份为 ID^* 的用户的秘密值且没替换用户 ID^* 的公钥。其他的同第 1 类攻击中的描述。一个无证书签名方案在适应性选择消息攻击下是存在不可伪造的，当且仅当任何计算能力多项式受限的攻击者赢得以上两个游戏的概率是可忽略的。

2.4 可信机构的信任级别

在公钥密码系统中，可将第三方的信任机构(Trusted Third Party，TTP，即本文的 KGC)划分为 3 类信任级别[20]：

第一级：TTP 知道用户的私钥，能在任何时候假冒任何注册用户而不被发现。绝大多数基于身份的签名方案中的 TTP 属于这一信任级别。

第二级：TTP 不知道注册用户的私钥，但可伪造一公钥(即进行公钥替换攻击)来假冒该用户而不被发现。到目前为

止，已有的无证书方案的 TTP 都属于这一信任级别。

第三级：TTP 不知道注册用户的私钥，若伪造一个用户的公钥，该用户就可（用某一证据）证明该公钥是伪造的。

对于传统的基于 PKI 的公钥密码系统而言，若 TTP 进行公钥替换攻击，对同一用户就会出现两个不同的公钥证书，这显然是不可行的。而对于无公钥证书的签名方案而言（包括基于身份的签名方案和无证书签名方案），研究如何将 KGC 的信任级降低到第三级以抵抗来自恶意的 KGC 的公钥替换攻击，具有重要意义。

3 公钥不可替换无证书签名

在给出公钥不可替换攻击无证书签名的定义之前，先给出如下 3 个假定：1）KGC 不能对非注册用户进行公钥替换攻击。这是合理的，因为如果一个用户不使用无证书签名系统，而 KGC 使用公钥替换攻击冒充他进行签名则无任何意义，这反而暴露了其恶意性。2）KGC 和任何其他用户在某个用户向 KGC 注册前不知道该用户的身份 ID（或者是他使用哪个 ID 进行注册）。3）KGC 有一个列表 PkSignlist，其用于保存注册用户的公钥的相关信息，但并不对外公开。上面说的注册用户指的是该 KGC 的无证书签名者。

3.1 无证书签名者的公钥签名协议

无证书签名的公钥签名协议是一个在 KGC 和 ID 拥有者之间进行的双方协议。该协议执行的结果是 ID 拥有者得到 KGC 对其所选定的公钥的签名，成为其注册用户，同时，KGC 将在 PkSignlist 列表保留该用户的 ID 等相关信息。

假设 KGC 属于先前所定义的第三级的信任中心，ID 拥有者可能是恶意的，即他们随时都可能中止公钥签名协议，并获取有用的信息。协议中所用的参数包括 2.1 节所定义的双线性对，s 表示系统主密钥，$P_0=sP$ 为系统公钥，x_i 是 ID 拥有者选定的私钥，杂凑函数：$H(\cdot):\{0,1\}^*\rightarrow Z_q$，公钥签名协议定义如下：

（1）用户将公钥 $P_{ID}=x_iH(ID)P_0$ 发送给 KGC；

（2）KGC 用主密钥 s 对其进行（部分）签名为 $\sigma_{Y_i}=sP_{ID}$，并将 σ_{Y_i} 发送给用户；

（3）用户保留 σ_{Y_i}，并将 $X_i=x_iP_0$ 和 ID 发送给 KGC；

（4）KGC 先验证 $P_{ID}=H(ID)X_i$ 是否成立，若不成立，则中止对公钥的签名；否则，查看表 PkSignlist 中是否存在该 ID，若有，则中止签名，否则计算对公钥的签名为 $\sigma_{P_{ID}}=s(P_{ID}+H(ID,P_{ID}))$；

（5）用户验证等式 $e(P,\sigma_{P_{ID}})=e(P_0,P_{ID})e(P_0,H(P_{ID},ID))$ 是否成立，若成立，则接收；否则，拒绝。

因为：

$$\begin{aligned}e(P,\sigma_{P_{ID}})&=e(P,s(P_{ID}+H(ID,P_{ID})))\\&=e(P,sP_{ID})e(P,sH(ID,P_{ID}))\\&=e(sP,P_{ID})e(sP,H(P_{ID},ID))\\&=e(P_0,P_{ID})e(P_0,H(P_{ID},ID))\end{aligned}$$

所以该验证等式正确。

对用户公钥签名协议的安全性（抗恶意性）分析如下。

（1）若 KGC 收到 P_{ID} 后中止签名过程，由于它无法从 P_{ID} 求得用户的 ID，因此无法用该 P_{ID} 冒充该 ID 的拥有者进行签名。

（2）若用户获得 σ_{Y_i} 后中止签名过程，他由于无法获得对公钥的签名，因此无法用私钥和 ID 进行有效的签名。

（3）若 KGC 获取用户 ID 和 P_{ID} 后中止签名过程，此时，KGC 可利用 ID 伪造另一个 P'_{ID}，并冒充该 ID 的拥有者进行签名。然而，该 ID 拥有者可出示 σ_{Y_i} 和他自己先选定的私钥 x_i，任何其他人输入系统公钥、ID 和 x_i，验证 $\sigma_{Y_i}=sP_{ID}$ 的有效性，以揭露 KGC 的替代公钥攻击行为。

（4）公钥签名有效性的验证确保用户和 KGC 在协议执行过程不被造假，否则签名验证无法通过，这一点将在 3.3 节基于随机预言机模型给出详细证明。

公钥签名协议的本质在于用户发送给 KGC 的公钥承诺了他的 ID 和选定的私钥，在用户不主动打开该承诺之前，基于双线性对上 CDH 的困难性，KGC 无法计算出 ID 及用户私钥。而用户获得所选公钥的部分签名后，即相当于获得了 KGC 对该公钥签名的证据，以防止 KGC 的恶意攻击。然而，他必须向 KGC 发送 ID 后，才能获得有效的公钥签名，以防止他对 KGC 的攻击。公钥签名的验证等式确保在协议执行过程双方不能利用假的数据进行欺骗。

3.2 公钥不可替换无证书签名的定义

定义 3 不可替代无证书签名方案由系统参数生成、部分密钥生成、设置秘密值、设置私钥、设置公钥、公钥签名过程、消息签名及签名验证等 8 个算法（协议）组成。

其中，公钥签名过程即调用 3.1 节定义的公钥签名协议。

签名验证修改为：

（1）公钥签名 $\sigma_{P_{ID}}$ 验证：输入系统参数 params，签名者公钥 P_{ID} 和其 ID，当公钥签名验证等式有效时，转到（2）；否则，输出 0。

（2）消息签名 σ 验证：输入系统参数 params、消息 M、签名 σ、签名者的身份 ID 及公钥 P_{ID}，签名验证等式有效时，输出 1；否则，输出 0。

其它部分定义与原有的无证书签名方案的定义相同。

已有的无证书签名方案中，一个用户可以生成多个有效的公私钥对。本文的公钥不可替换攻击无证书签名方案中，每个用户只允许有一对有效的公钥私钥对。

3.3 对公钥签名验证等式的安全性证明

基于随机预言机模型，给出公钥签名验证等式 $e(P,\sigma_{P_{ID}})=e(P_0,P_{ID})e(P_0,H(P_{ID},ID))$ 的安全性证明。

定理 1 假定系统主密钥 s 保密，在随机预言模型下，若群 G_1 中的离散对数问题是困难的，除 KGC 以外的任何第三方无法伪造 $\sigma_{P_{ID}}$。

证明：假设 C 是挑战者，想解决 G_1 中的离散对数问题，其输入为任意的 aP，需要计算出 a，假设 A_0 是攻击者，他能以不可忽略的概率攻破公钥签名方案。

（1）C 设置 $P_0=aP$，选择系统参数 params$=\{e,G_1,G_2,P,P_0,H_1\}$。然后 C 将系统参数$\{e,G_1,G_2,P,P_0\}$发送给 A_0。这里将杂凑函数 H_1 看成随机预言机。

（2）公钥询问：C 维护一个列表 Klist，其每一项的格式为 (ID,x,P_{ID})，并将该列表初始化为空。当 C 接收到 A_0 对身份 ID_i 的公钥询问时，C 首先检索 Klist。若 Klist 中存在一项 (ID_i,x_i,P_i)，则 C 返回 P_i 作为应答；否则，C 随机选择 $x_i\in Z_q^*$，计算 $P_i=x_iP$，返回 P_i 作为回答，并将 (ID_i,x_i,P_i) 加入

到 Klist。

(3) H_1 询问:C 维护一个列表 H1list,其每一项的格式为 (ID, P_{ID}, y, U),并将该列表初始化为空。当 A_0 询问 H_1 (ID_i, P_i)时,C 首先检索 H1list。若 H1list 中存在一项(ID_i, P_i, y_i, U_i),则 C 返回 U_i 作为应答;否则,C 随机选择 $y_i \in Z_q^*$,计算 $U_i = y_i P$,将(ID_i, P_i, y_i, U_i)加入到 H1list 并将 U_i 返回给 AI。

(4) 签名询问:当 A_0 向 C 请求身份为 ID_i,公钥为 P_i 的系统对一个公钥的签名时,C 按照如下步骤回答:

1. 计算 $\sigma_{P_{ID}} = x_i P_0 + y_i P_0$;

2. 返回$(P_i, \sigma_{P_{ID}})$。

最后,如果 A_0 能以不可忽略的概率成功地攻破该方案,则输出一个伪造$(ID^*, P_{ID}^*, \sigma_{P_{ID}}^* = x_i P_0 + y_i P_0)$。根据分叉原理[21],C 重排 Hash 函数 H_1,并再次利用 A_0 的能力,它可以得到对同一个身份 ID 的另一个伪造$(ID^*, P_{ID}^*, \sigma_{P_{ID}}^{*'} = x_i P_0 + y_i' P_0)$,从而 C 得到了两个有效的伪造,并且它们满足:

$$e(P, \sigma_{P_{ID}}^*) = e(P_0, P_{ID}^*) e(P_0, U) \quad (1)$$

$$e(P, \sigma_{P_{ID}}^{*'}) = e(P_0, P_{ID}^*) e(P_0, U') \quad (2)$$

式中,$U = y_i P$,$U' = y_i' P$ 并以(ID^*, P_{ID}^*, y, U)的形式存在于 H1list 中。

由式(1)和式(2)计算可得 $\sigma_{P_{ID}}^{*'} - \sigma_{P_{ID}}^* = a(U' - U)$,然后求出 $a = \sigma_{P_{ID}}^{*'} - \sigma_{P_{ID}}^* / U' - U$。

即挑战者 C 以不可忽略的概率根据在给定 aP 的情况下,求出 a 的值。因为 aP 的任意性,相当于敌手帮助 C 以不可忽略的概率解决了 G_1 中的离散对数问题,这与 G_1 中的离散对数问题是难解的相矛盾。定理 1 得证。

3.4 效率分析

文章提出的公钥签名协议可有效地将已有的基于 Al-Riyami 框架的双线性对无证书签名方案改造成公钥不可替换无证书签名方案。改造方法是在已有方案上(基于文章给出的 3 个合理假设的前提下)增加对注册用户公钥的签名协议,并在验证签名之前增加对公钥的有效性验证。在效率上,对公钥的签名协议只需运行一次,因而对整个签名算法效率的影响可以忽略不计,而对公钥的有效性验证只需(在已有方案上)多 3 个双线性运算。其签名长度也只需(在已有方案上)增加 G_1 中的一个点的长度。总体而言,现有方案改造成公钥不可替换方案后,几乎没增加复杂性,但其安全性获得了很大的提高,有效地将 KGC 的信任级别降低到了第三级。

结束语 现有的无证书签名方案大都以 KGC 不能实施公钥替换攻击和用户的部分密钥对其他人保密为前提,对该类方案的安全性分析和改进也基于这一前提,并没解决恶意 KGC 进行公钥替代攻击这一安全隐患。因此,无证书的签名方案与基于身份的签名方案相比,其在安全性上并无多大提高。提出的公钥不可替换无证书签名方案是对基于 Al-Riyami 框架的无证书签名方案的一种改进。因为有了对注册用户的公钥签名协议,所以在实际的签名系统构造过程,部分密钥这一项就可以不用。新方案的安全模型由原来的两类变为一类,且不存在公钥替换询问。本文定义的公钥不可替换无证书签名方案的构造方法对改造已有的基于 Al-Riyami 框架的双线性对无证书签名方案具有普适性。

参 考 文 献

[1] Al-Riyami S, Paterson K. Certificateless public key cryptography [C]// ASIACRYPT 2003, LNCS 2894. Springer Verlag, 2003: 452-473

[2] Huang X, Susilo W, Mu Y, et al. On the security of a certificateless signature scheme[C]// Proceedings of the CANS 2005. Xiamen, China, 2005: 13-25

[3] Yum D H, Lee P J. Genericconstruction of certificateless signature[C]// Proceedings of ACISP 2004. Sydney, Australia, 2004: 200-211

[4] Gorantla M C, Saxena A. An efficient certificateless signature scheme[C]// Proceedings of CIS 05. Springer Verlag, 2005: 110-116

[5] Yap W, Heng S, Goi B. An efficient certificateless signature scheme[C]// Proceedings of the EUC Workshops 2006. Seoul, Korea, 2006: 322-331

[6] Choi K, Park J, Hwang J, et al. Efficient certificateless signature schemes[C]// Proceedings of the ACNS 2007. Zhuhai, China, 2007: 443-458

[7] Zhang J, Mao J. Security analysis of two signature schemesand their improved schemes[C]// Proceedings of the ICCSA 2007. Kuala Lumpur, Malaysia, 2007: 589-602

[8] Zhang Z, Wong D, Xu J, et al. Certificateless public-key signature: security model and efficient construction[C]// Proceedings of the ACNS 2006. Singapore, 2006: 293-308

[9] Hu B, Wong D, Zhang Z, et al. Key replacement attack against a generic construction of certificateless signature[C]// Proceedings of the ACISP 2006. Melbourne, Australia, 2006: 235-346

[10] Huang X, Mu Y, Susilo W, et al. Certificateless signature revisited[C]// Proceedings of the ACISP 2007. Towns-ville, Australia, 2007: 308-322

[11] Zhang L, Zhang F, Zhang F. New efficient certificateless signature scheme[C]// Proceedings of the EUC Workshops 2007. Taipei, China, 2007: 692-703

[12] 张磊,张福泰. 一类无证书签名方案的构造方法[J]. 计算机学报,2009,32(5):940-945

[13] 陈虎,朱昌杰,宋如顺. 高效的无证书签名和群签名方案[J]. 计算机研究与发展,2010,47(2):231-237

[14] 葛爱军,陈少真. 具有强安全性的不含双线性对的无证书签名方案[J]. 电子与信息学报,2010,32(7):1765-1768

[15] 刘景伟,孙蓉,马文平. 高效的基于 ID 的无证书签名方案[J]. 通信学报,2008,29(2):87-94

[16] Zhang Z, Feng D. Key replacement attack on a certificateless signature scheme[R]. Cryptology ePrint Archive. Report 2006/453, 2006

[17] 曹雪菲, Paterson K G, 寇卫东. 对一类无证书签名方案的攻击及改进[J]. 北京邮电大学学报,2008,31(2):64-67

[18] 明洋,詹阳,王育民,等. 一个改进的无证书签名方案[J]. 西安电子科技大学学报:自然科学版,2008,35(6):1094-1099

[19] Naor M. Bit commitment using pseudo-randomness[J]. Journal of Cryptology, 1991, 12(4): 151-158

[20] Girault M. Self-certified public keys [C]// Eurocrypt 1991, LNCS 547. Springer Verlag, 1991: 490-497

[21] Pointcheval D, Stern J. Security proofs for signature schemes [J]. Journal of Cryptology, 2000, 13(3): 1-12