第 38 卷 第 3 期 计 算 机 工 程 2012 年 2 月
Vol.38 No.3 Computer Engineering February 2012

• 安全技术 • 文章编号：1000—3428(2012)03—0110—03 文献标识码：A 中图分类号：TP309

一种不含双线性对的可截取签名方案

曹素珍[1]，王彩芬[1]，陈小云[2]，吕浩音[3]

(1. 西北师范大学数学与信息科学学院，兰州 730070；2. 平凉市第一中学信息中心，甘肃 平凉 744000；
3. 陇东学院计算机与信息科学学院，甘肃 庆阳 745000)

摘 要：现有可截取签名方案需要计算双线性对，计算效率较低。针对该问题，基于无证书思想，提出一个不含双线性对的可截取签名方案。采用绑定技术，通过哈希函数将用户公钥绑定在部分私钥的生成算法及签名算法中，以降低公钥替换攻击的可能性。在随机预言机模型下证明方案效率较高，签名是不可伪造的。

关键词：可截取签名；离散对数问题；双线性对；哈希函数；随机预言机模型

Content Extraction Signature Scheme Without Bilinear Pairings

CAO Su-zhen[1], WANG Cai-fen[1], CHEN Xiao-yun[2], LV Hao-yin[3]

(1. College of Mathematics and Information Science, Northwest Normal University, Lanzhou 730070, China;
2. Information Center of Pingliang First Middle School, Pingliang 744000, China;
3. College of Computer and Information Science, Longdong University, Qingyang 745000, China)

【Abstract】For the existing content extraction signature scheme, because calculated bilinear pairings caused the problem of low efficiency, based on certificateless thinking, this paper proposes an efficient content extraction signature scheme without pairings. Scheme of binding techniques, use hash functions will the public key binding to the partial private key generates and signature algorithms, reduce the possibility of public key substitution attack, and in the random oracle model proved scheme is existentially unforgeable under adaptive chosen-message attacks assuming. Compared with known solutions, the efficiency is higher.

【Key words】content extraction signature; Discrete Logarithm Problem(DLP); bilinear pairings; Hash function; random oracle model

DOI: 10.3969/j.issn.1000-3428.2012.03.037

1 概述

可截取签名[1]是指在多方参与的应用环境中，对于一个已签名的消息，允许任何人根据需要，针对原消息的一部分，截取一个可公开并可验证的签名，而无需与最初的签名者进行交互。相对于标准签名体制而言，可截取签名体制在某些应用领域具有较强的优势。目前，已有许多与可截取相关的签名方案[2-4]被提出，其中，文献[4]的签名方案是基于昂贵的双线性对运算的，因此，方案的效率并不高。本文在现有研究基础上[4-6]，借鉴 Schnorr 签名的方法，构造了一种新的不需要双线性对的可截取签名方案，其安全性基于离散对数问题(Discrete Logarithm Problem, DLP)的难解性。

2 基础知识

2.1 相关困难问题

设 p、q 是 2 个大素数且 $q|(p-1)$，设 G 是 Z_p^* 的一个阶为 q 的子群，g 是 G 的生成元，假设 G 中的下列问题是难解的：

(1)离散对数问题：给定元素 $y\in G$，求解 x，使得 $y=g^x(\mathrm{mod}\,p)$ 成立。

(2)计算 Diffie-Hellman 问题(CDHP)：已知 g、g^a、g^b，其中，$a,b\in Z_q^*$，计算 $g^{ab}(\mathrm{mod}\,p)$。

2.2 基于无证书的可截取签名方案的一般化模型

一个基于无证书的可截取签名方案一般由 6 个概率多项式时间算法组成：

(1)系统初始化算法

输入安全参数 k，输出系统公开参数 $params$ 和系统主密钥。

(2)用户部分密钥生成算法

输入系统公开参数 $params$、主密钥及用户的身份标识 ID，输出用户的部分私钥 D_{ID} 和部分公钥 P_{ID}。

(3)用户完整密钥生成算法

用户随机选择一个秘密值，并利用系统公开参数 $params$、用户部分私钥 D_{ID}、部分公钥 P_{ID} 及用户的身份标识 ID，计算出自己的完整私钥 SK_{ID} 和完整公钥 PK_{ID}。

(4)签名算法

输入系统公开参数 $params$、用户的私钥 SK_{ID}、消息 M 及内容截取访问控制结构 $CEAS$，输出对消息 M 的可截取签名 σ。

(5)签名截取算法

输入消息 M、可截取签名 σ、截取子集 $CI(M')$ 及用户公钥 PK_{ID}，输出截取后子消息 M' 的签 名 σ'。

基金项目：国家自然科学基金资助项目(61063041)；教育部科学技术研究基金资助重点项目(208148)；甘肃省教育厅基金资助重点项目(0801-01)

作者简介：曹素珍(1976－)，女，讲师，主研方向：信息安全；王彩芬，教授、博士生导师；陈小云，一级教师；吕浩音，讲师

收稿日期：2011-07-11 **E-mail：**caosuz@nwnu.edu.cn

(6)签名验证算法

输入子消息 M'、截取后的签名 σ' 及用户公钥 PK_{ID}，输出验证结果。

3　不含双线性对的可截取签名方案

为降低无证书签名体制中密钥替换攻击的可能性，本文提出的方案运用绑定技术，将用户的部分公钥通过哈希函数绑定到部分私钥的生成中，并且对签名的顺序做了一定调整，主要由 7 个算法组成。

3.1　系统初始化算法

输入安全参数 k，PKG 产生大素数 p、q 且 $q|(p-1)$，设 G 是 Z_p^* 的一个阶为 q 的子群，g 是 G 的生成元，PKG 随机选择 $s\in Z_q^*$ 作为系统主密钥，并计算 $f=g^s(\bmod p)$，选择密码学哈希函数：$H_1:\{0,1\}^*\times Z_p^*\to Z_q^*$，$H_2:\{0,1\}^*\to\{0,1\}^k$，$H_3:\{0,1\}^*\to\{0,1\}^k$，$H_4:\{0,1\}^*\times Z_p^*\to Z_q^*$，公开系统参数 $params=\{p,q,g,G,f,H_1,H_2,H_3,H_4\}$。

3.2　用户秘密值选择算法

用户随机选择 $x\in Z_q^*$ 作为秘密值，计算 $y=g^x(\bmod p)$，同时计算 $Q_{ID}=H_1(ID,y)$，并将 Q_{ID} 发送给 PKG。

3.3　系统生成用户部分密钥算法

PKG 收到 Q_{ID} 后，随机选择 $z\in Z_q^*$，计算 $u=g^z(\bmod p)$，$d=z+sQ_{ID}(\bmod q)$，并通过安全信道将 $D_{ID}=d$ 作为部分私钥、$P_{ID}=u$ 作为部分公钥发送给用户。

3.4　用户完整密钥生成算法

用户收到 PKG 发送的 D_{ID}、P_{ID} 后，验证 $g^d=u\cdot f^{Q_{ID}}(\bmod p)$ 是否成立，若结果为“真”，则用户生成自己的完整私钥 $SK_{ID}=(x,d)$ 和完整公钥 $PK_{ID}=(y,u)$；若结果为“假”，则终止算法。

3.5　签名算法

M 为待签名原始消息，且按照要求被分成用 m_i 表示的 n 个子消息段，其中，$i\in\{1,2,\cdots,n\}$，代表子消息段在 M 中的编号；M' 表示截取后的消息，$CI(M')$ 表示 M' 中所包含的 M 中子消息段编号的集合，$CEAS$ 是内容截取访问控制结构。签名者完成如下操作：

(1)对每个子消息段 m_i，计算 $H_2(m_n\|CEAS)$，并按照 M 中子消息段的顺序从左向右级联，然后计算级联后的值，即：

$$\bar{M}=H_3(H_2(m_1\|CEAS)H_2(m_2\|CEAS)\|\cdots\|H_2(m_n\|CEAS))$$

(2)随机选择 $r_1,r_2\in Z_q^*$，计算 $c_1=g^{r_1}\bmod p$，$c_2=g^{r_2}\bmod p$，令 $h=H_4(\bar{M},ID,c_1,c_2,PK_{ID})$。

(3)计算 $v=r_1-hx(\bmod q)$，$w=r_2-hd(\bmod q)$，输出 M 的可截取签名 $\sigma=(CEAS,h,v,w)$。

3.6　签名截取算法

截取者收到签名者对 M 的可截取签名 σ 后，按照 3.5 节中的操作(1)计算出总散列值 $\bar{M}$，同时计算 $Q_{ID}=H_1(ID,y)$，验证等式 $h=H_4(\bar{M},ID,g^vy^h,g^w(uf^{Q_{ID}})^h,PK_{ID})$是否成立，若成立，则执行如下截取算法：

(1)根据 $CEAS$ 构造 $CI(M')$。

(2)用 $M'=(m'_1,m'_2,\cdots,m'_n)$ 替代 $M=(m_1,m_2,\cdots,m_n)$，具体方法是：若 $i\in CI(M')$，则 $m'_i=m_i$，表示该子消息段是被截取的；否则，$m'_i=H_2(m_i\|CEAS)$，表示该子消息段没有被截取。

(3)输出截取后子消息 M' 的签名 $\sigma'=(M',CEAS,CI(M'),h,v,w)$。

3.7　签名验证算法

验证者收到 M' 的签名 σ' 后，做如下验证操作：

(1)判断 $CI(M')\in CEAS$ 是否成立，若成立，则继续，否则，终止算法。

(2)根据 $CI(M')$ 和 M' 恢复总的散列值 $\bar{M}$，具体方法是：首先判断 $i\in CI(M')$ 是否成立，若成立，则用 $H_2(m_i\|CEAS)$ 恢复 m'_i 的值；否则，保持原值不变。然后按消息 M' 中的顺序从左向右级联，依照 3.5 节(1)的方式计算出级联后的散列值 $\bar{M}$。

(3)计算 $Q_{ID}=H_1(ID,y)$，验证等式 $h=H_4(\bar{M},ID,g^vy^h,g^w(uf^{Q_{ID}})^h,PK_{ID})$ 是否成立，若结果为“真”且 $CI(M')\in CEAS$，则截取后的签名 σ' 为有效签名；否则，为无效签名。

4　本文方案性能分析

4.1　正确性分析

本文方案的正确性可以通过以下 2 个方面证明：

(1)确保签名算法中 $\bar{M}$ 值与验证算法中所恢复的 $\bar{M}$ 值一致

截取算法中对各子消息段的替换方法是：

$$m'_i=\begin{cases}m_i & \text{if } i\in CI(M')\\ H_2(m_i\|CEAS) & \text{if } i\notin CI(M')\end{cases}\tag{1}$$

验证算法中的恢复方法是：

$$m_i=\begin{cases}H_2(m_i\|CEAS) & \text{if } i\in CI(M')\\ m'_i & \text{if } i\notin CI(M')\end{cases}\tag{2}$$

由式(1)和式(2)可知验证时各子消息段的值为 $H_2(m_i\|CEAS)$，与签名算法中保持一致。

(2)确保验证等式的正确性

由于有 $g^vy^h=g^{r_1}=c_1$，$g^w(uf^{Q_{ID}})^h=g^{r_2}=c_2$ 成立，因此验证等式 $h=H_4(\bar{M},ID,g^vy^h,\ g^w(uf^{Q_{ID}})^h,PK_{ID})$ 是正确的。

通过上述分析可知，本文方案是正确的。

4.2　安全性证明与分析

以下给出在随机预言机模型下方案的安全性证明。

由于在第 1 类攻击下的证明过程与第 2 类攻击下的证明过程类似，鉴于篇幅限制，本文只给出在第 1 类攻击下的完整证明。

引理　在随机预言机模型下，若群 G 中的 CDH 问题是困难的，则用上述方法构造的无证书可截取签名方案对于第 1 类攻击是安全的。

证明：假设 A_I 能够以一定的优势攻破本文方案，则构造一个算法，使挑战者 C 可以通过已知的 g 和 $\beta=g^\alpha$，利用 A_I 求解出 α，进而求解出离散对数问题。

C 运行系统初始化算法，随机选择 $s\in Z_q^*$，计算 $f=g^s(\bmod p)$，并生成系统参数 $params=\{p,q,g,G,f,H_1,H_2,H_3,H_4\}$，C 将系统参数给 A_I 并保管系统主密钥 s。C 与 A_I 做如下模拟算法：

假设 A_I 最多能做 q_{H_1} 次询问，C 在 $[1,q_{H_1}]$ 中随机选取一个值 J，记为 $ID^*=ID_J$，代表 A_I 的第 i 次询问。

(1) H_1 询问

C 维护初值为空、结构为 (ID_i,Q_{ID_i}) 的列表 L_1。当 C 收到

A_I 对 $H_1(ID,y)$ 的询问时，如果 $i \neq J$，C 查看列表 L_1，若存在 Q_{ID_i} 项，则直接返回该值给 A_I；若不存在，则做秘密值询问，查找列表 K_{list}，计算出相应的 Q_{ID_i} 值给 A_I，并把 Q_{ID_i} 添加到列表 L_1 中。如果 $i=J$，C 随机选择 $Q_{ID_i} \in Z_q^*$ 给 A_I 并将相应值添加到列表 L_1 中。

(2)部分私钥询问

当 C 收到 A_I 询问对应 ID_i 的部分私钥时，若 $i \neq J$，C 查找结构为 (ID_i,d_i,u) 的列表 D_{list}，若存在该项，则直接返回 ID_i 的部分私钥 d_i 给 A_I；否则，C 首先查找 L_1 列表，获得相应 Q_{ID_i} 的值，然后随机选择 $z \in Z_q^*$，计算 $d_i = z + sQ_{ID_i} (\mathrm{mod}\, q)$ 及 $u = g^z (\mathrm{mod}\, p)$，并且添加 (ID_i,d_i,u_i) 项到 D_{list} 中。若 $i=J$，C 设置 $u = \beta = g^\alpha$，$d_i = \perp$，返回“失败”给 A_I 并把相应值添加到 D_{list} 中。

(3)秘密值询问

当 A_I 询问对应 ID_i 的秘密值时，C 查看结构为 (ID_i,x_i,y_i) 的列表 K_{list}，若存在，则返回相应的 x_i 给 A_I；否则，C 随机选择 $x_i \in Z_q^*$，计算 $y_i = g^{x_i} (\mathrm{mod}\, p)$，返回 x_i 给 A_I 并添加相应值到 K_{list}。

(4)公钥询问

当 A_I 询问对应 ID_i 的公钥时，C 查看列表 K_{list} 和列表 D_{list}，分别找到与 ID_i 相对应的 y_i 项和 u_i 项，并把 (y_i,u_i) 项返回给 A_I。

(5)公钥替换询问

当 C 收到 A_I 对身份为 ID_i 的用户做公钥替换询问时，首先验证等式 $g^{d_i'} = u' \cdot f^{H_1(ID_i,y_i')} (\mathrm{mod}\, p)$ 是否成立，若成立，则将列表 K_{list} 和 D_{list} 中的公钥 (y_i,u) 替换为 (y_i',u')，否则，拒绝替换。

(6)签名询问

若 $i \neq J$ 且对应 ID_i 的公钥没有被替换，则首先查看列表 K_{list} 和 D_{list}，获得相应的私钥 (x_i,d_i)，然后随机选择 $r_1,r_2,h \in Z_q^*$，计算 $c_1 = g^{r_1} \bmod p$，$c_2 = g^{r_2} \bmod p$，并设置 $h = H_4(\bar{M},ID,c_1,c_2,PK_{ID})$，计算 $v = r_1 - hx (\mathrm{mod}\, q)$，$w = r_2 - hd (\mathrm{mod}\, q)$，输出 $\sigma = (CEAS,h,v,w)$ 作为用户 ID_i 对消息 M 的签名；否则，若 $i \neq J$ 且对应 ID_i 的公钥被替换过，或者 $i=J$ 且不考虑公钥是否被替换时，C 随机选择 $u,v,w \in Z_q^*$，并且设置 $h = H_4(\bar{M},ID,g^v y^h,g^w (uf^{Q_{ID}})^h,PK_{ID})$，输出 $\sigma = (CEAS,h,v,w)$ 作为用户 ID_i 对消息 M 的签名。

根据 Forking Lemma[7]，通过重放上述模拟过程，得到满足等式 $g^w (uf^{Q_{ID}})^h = g^{w'} (uf^{Q_{ID}})^{h'}$ 的 2 个有效签名 σ 和 σ^*，若将等式两边以 g 为底各取对数，那么 C 可计算出 $\alpha = \log_g \beta = (w-w')(h'-h)^{-1} + sQ_{ID}$，至此，$C$ 利用 A_I 解决了离散对数问题。出现矛盾。

最后，讨论 C 解决离散对数问题成功的概率。由于 Schnorr 签名是存在性不可伪造的，从而保证 A_I 利用新的公钥 (y',u') 对用户公钥 (y,u) 进行替换时，不可能找到另外的 $y' \neq y$ 满足等式 $g^{d_i'} = u' \cdot f^{H_1(ID_i,y_i')} (\mathrm{mod}\, p)$，因此只讨论对用户公钥 u 进行替换的情况下 C 解决离散对数问题的成功概率。

假设 A_I 最多进行了 q_k 次部分私钥询问，则 A_I 不询问对应 ID^* 的部分私钥的概率至少为 $(1-(1/q_{H_1}))^{q_k}$，又因为 A_I 输出的伪造签名中 $ID = ID^*$ 的概率至少为 $(1/q_{H_1})$，所以 C 成功求解 α 的概率为 $Adv_C \geqslant \frac{1}{q_{H_1}}(1-q_{H_1})^{q_k} \cdot Succ_{A_1}$，其中，$Succ_{A_1}$ 是 A_I 在第 1 类攻击类型下对方案伪造成功的概率。如果 $Succ_{A_1}$ 是不可忽略的，那么在 q_{H_1} 和 $(1/q_{H_1})^{q_k}$ 均为常数的情况下，Adv_C 也是不可忽略的。

综合上述分析可知，本文方案是安全的。

4.3 效率分析

本文方案与文献[4]方案的效率分析见表 1，其中，p 表示对运算；e 表示指数运算。

表 1 2 种方案的效率比较

方案	签名及截取算法	验证算法
文献[4]方案	2p	2p
本文方案	5e	3e

由于椭圆曲线上的双线性对运算是已知最复杂的密码运算，在相同的安全级别下，运行一次双线性对所需要的时间约为有限域上指数运算的 10 倍，因此与文献[4]方案相比，本文方案在计算效率方面具有极大的优势。

5 结束语

本文提出了一个基于无证书的不含双线性对的可截取签名方案。与现有可截取签名方案相比，本文方案在计算效率方面具有较大的优势，在电子商务或电子政务系统中具有更高的实际应用价值。如何将现有签名方案应用于 Ad Hoc 网络将是下一步要探讨的问题。

参考文献

[1] Steinfeld R, Bull L, Zheng Yuliang. Content Extraction Signatures[C]//Proceedings of the 4th International Conference on Information Security and Cryptology. Berlin, Germany: Springer-Verlag, 2001: 285-304.

[2] Bull L, Stanskip P. Content Extraction Signature Using XML Digital Signatures and Custom Transforms On-demand[C]// Proceedings of the 12th International World Wide Web Conference. New York, USA: ACM Press, 2003: 170-177.

[3] Bull L, Squire M D, Zheng Yuliang. A Hierarchical Extraction Policy for Content Extraction Signatures[J]. International Journal of Digital Libraries, 2004, 4(3): 208-222.

[4] 蓝才会, 王彩芬. 基于身份的可截取签名方案[J]. 计算机应用, 2007, 27(10): 2456-2458.

[5] 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.

[6] 张玉磊, 王彩芬. 无证书签名改进方案的安全性证明[J]. 计算机工程, 2010, 36(12): 170-172.

[7] Rafael C, Ricardo D. Two Notes on the Security of Certificateless Signature[M]. Berlin, Germany: Springer-Verlag, 2007.

编辑 张正兴