# 两个高效无证书签名方案的安全性分析*

宗志雄[1]，胡国政[1]，陈加忠[2]，韩兰胜[2]
（1. 武汉理工大学 理学院，武汉 430070；2. 华中科技大学 计算机学院，武汉 430074）

**摘 要**：对两个高效的无证书签名方案进行了安全性分析，证明了这两个方案都是不安全的。对于第一个方案，类型Ⅰ敌手可以利用公钥替换伪造任何用户对任意消息的签名。对于第二个方案，它不仅在类型Ⅰ敌手攻击下不安全，而且在类型Ⅱ敌手攻击下也不安全。类型Ⅱ敌手即恶意 KGC 可在系统参数生成阶段利用预选目标用户的身份生成含有陷门信息的系统参数，然后计算该目标用户的私钥并伪造对任意消息的签名。

**关键词**：无证书签名；公钥替换攻击；恶意 KGC 攻击；可证安全；双线性映射
**中图分类号**：TP393.04 **文献标志码**：A **文章编号**：1001-3695(2012)08-3046-02
doi:10.3969/j.issn.1001-3695.2012.08.063

## Security analysis of two efficient certificateless signature schemes

ZONG Zhi-xiong[1], HU Guo-zheng[1], CHEN Jia-zhong[2], HAN Lan-sheng[2]
(1. *School of Science, Wuhan University of Technology, Wuhan* 430070, *China*; 2. *School of Computer, Huazhong University of Science & Technology, Wuhan* 430074, *China*)

**Abstract**: This paper analyzed two efficient certificateless signature schemes. It indicated that the two schemes were insecure. For the first scheme, a Type I adversary could forge a valid signature for any message of any user by substituting the target user's public key. For the other scheme, it was vulnerable against both Type I and Type Ⅱ adversaries. After generating the trapdoor system parameters according to the identity information of a pre-selected target user, the Type II adversary (malicious private key generator) was able to compute the user's private key and forge a signature on any message of the user.

**Key words**: certificateless signature; public key replacement attack; malicious KGC attack; provable security; bilinear pairing

为了避免传统公钥基础设施中代价高昂的证书管理问题，消除基于身份的公钥密码体制中固有的密钥托管问题，Al-Riyami等人[1]于2003年首次提出了无证书公钥密码体制的概念。自提出之后，大量无证书签名方案相继被提出和分析[2~7]。一般地，无证书签名方案的安全模型中需要考虑两类敌手[1~4]，即类型Ⅰ与类型Ⅱ敌手。类型Ⅰ敌手是指普通的第三方攻击者，它不知道系统主密钥，但是可以任意替换用户的公钥。类型Ⅱ敌手是指恶意但被动的KGC(key generation centre)，它可以不遵照系统说明生成系统参数，知道系统的主密钥，但是不能替换目标用户的公钥。

最近，洪东招等人[8]和李凤银等人[9]分别提出了高效的无证书签名方案(记为HX方案和LLZ方案)，并对所提出方案的安全性进行了形式化证明，声称这些方案是安全的。本文通过对HX方案和LLZ方案进行分析，得出HX方案对于第一类敌手是不安全的，LLZ方案对于两类敌手都不安全。利用公钥替换攻击，类型Ⅰ敌手可以伪造任何用户对任意消息的签名。利用预选目标用户的身份生成含有陷门信息的系统参数，类型Ⅱ敌手KGC可以根据陷门信息从该用户的公钥计算出该用户的私钥。因此，恶意KGC能够伪造该目标用户的签名。

## 1 双线性映射

设 $G_1$ 与 $G_2$ 分别是阶为 $q$ 的加法循环群和乘法循环群，其中 $q$ 为大素数。若映射 $e:G_1\times G_1\to G_2$ 满足下列性质，则此映射称为双线性映射。

**性质1** 双线性性。对所有的 $U,V\in G_1$ 和 $a,b\in Z_q^*$，总有 $e(aU,bV)=e(U,V)^{ab}$。

**性质2** 非退化性。存在 $U,V\in G_1$，使得 $e(U,V)\neq 1_{G_2}$，其中 $1_{G_2}$ 是 $G_2$ 的单位元。

**性质3** 可计算性。对所有的 $U,V\in G_1$，存在一个高效的算法计算 $e(U,V)$。

## 2 两个高效的无证书签名方案

HX、LLZ方案其均由七个算法组成，涉及到KGC、签名者和验证者。

### 2.1 HX方案描述

a)系统设置。设 $k$ 是安全参数，KGC选择双线性群($G_1$，$G_2$，$G_T$)阶为素数 $p>2^k$ 并且 $Q$ 为群 $G_2$ 的生成元，$P=\psi(Q)\in G_1$ 为 $G_1$ 生成元，$e:G_1\times G_2\to G_T$ 是一个安全的双线性对。设

**收稿日期**：2011-12-19；**修回日期**：2012-02-19 **基金项目**：国家自然科学基金资助项目(60703048)；湖北省自然科学基金资助项目(2007ABA313)；武汉理工大学自主创新研究基金资助项目(2012-Ia-035)

**作者简介**：宗志雄(1968-)，男，湖北武汉人，讲师，硕士，主要研究方向为密码学(zongzhix@163.com)；胡国政(1967-)，男，湖北浠水人，副教授，博士，主要研究方向为密码学和信息安全；陈加忠(1970-)，男，浙江嘉善人，副教授，博士，主要研究方向为信息处理和信息安全；韩兰胜(1972-)，男，山东济宁人，副教授，博士，主要研究方向为密码学和信息安全.

$g=e(P,Q)$,随机选择 $s\in Z_p^*$ 作为系统主密钥,计算 $Q_{\text{pub}}=sQ$,选择两个 hash 函数:$H_1:\{0,1\}^*\to Z_q^*$ 和 $H_2:\{0,1\}^*\times G_T\to Z_q^*$。KGC 秘密保存主密钥 $s$,公开系统参数 params = $\{G_1,G_2,G_T,e,p,P,Q,Q_{\text{pub}},g,\psi,H_1,H_2\}$。

b)部分私钥提取。对于一个身份为 ID $\in\{0,1\}^*$ 的用户,KGC 计算 $Q_{\text{ID}}=H_1(\text{ID})$,$d_{\text{ID}}=(s+Q_{\text{ID}})^{-1}P$,并通过安全信道发送 $d_{\text{ID}}$给用户 ID 作为部分密钥。用户 ID 验证等式 $e(d_{\text{ID}},Q_{\text{pub}}+Q_{\text{ID}}Q)=g$,若等式成立,则接收 $d_{\text{ID}}$为部分密钥。

c)秘密值设置。用户 ID 随机选取 $r\in Z_p^*$,把 $r$ 作为用户自己的秘密值。

d)私钥设置。用户 ID 利用部分私钥 $d_{\text{ID}}$和秘密值 $r$,计算用户私钥 $sk_{\text{ID}}=rd_{\text{ID}}$。

e)公钥设置。用户 ID 利用系统参数 params 和秘密值 $r$,计算用户公钥 $pk_{\text{ID}}=r^{-1}(Q_{\text{pub}}+Q_{\text{ID}}Q)$。

f)签名。对于待签名的消息 $m$,签名者首先选择随机值 $x\in Z_p^*$,然后计算 $R=g^x$,$h=H_2(m,R)$,$S=(x+h)sk_{\text{ID}}$,最后输出签名者在公钥 $PK_{\text{ID}}$下对消息 $m$ 的签名 $\sigma=(S,R)$。

g)验证。在收到身份为 ID 的签名者用公钥 $PK_{\text{ID}}$对消息 $m$ 的签名 $\sigma=(S,R)$后,验证者首先计算 $h=H_2(m,R)$,然后验证等式 $e(S,pk_{\text{ID}})g^{-h}=R$ 是否成立。如果等式成立,则接受该签名;否则,拒绝该签名。

### 2.2　LLZ 方案描述

a)系统参数生成。输入一个安全参数 $k$,密钥生成中心 KGC 选定满足第 1 章所述性质的 $G_1$、$G_2$、$e$、$P$,计算 $g=e(P,P)$,并随机选取 $s\in Z_q^*$ 作为系统主密钥,计算 $P_0=sP$,选择两个密码学 hash 函数 $H_1:\{0,1\}^*\to G_1$ 和 $H_2:\{0,1\}^*\to Z_q^*$。设置系统安全参数:Params = $\{G_1,G_2,e,q,P,P_0,g,H_1,H_2\}$。

b)部分私钥生成。KGC 利用系统主密钥生成用户的部分私钥。当输入一个用户的身份 ID,KGC 计算并输出该用户的部分私钥 $D_{\text{ID}}=sQ_{\text{ID}}=sH_1(\text{ID})\in G_1$。

c)设置秘密值。身份为 ID 的用户随机选取一个值 $x_{\text{ID}}\in Z_q^*$ 作为其秘密值。

d)设置私钥。身份为 ID 的用户设置其私钥为 $S_{\text{ID}}=x_{\text{ID}}D_{\text{ID}}\in G_1$,其中 $x_{\text{ID}}$为该用户的秘密值,$D_{\text{ID}}$为其部分私钥。

e)设置公钥。身份为 ID 的用户利用秘密值 $x_{\text{ID}}$设置其公钥为 $P_{\text{ID}}=x_{\text{ID}}P_0$。

f)签名。假设签名者的身份为 ID,公钥为 $P_{\text{ID}}$,私钥为 $S_{\text{ID}}$。当输入一个消息 $M$,该签名者按以下方式对消息 $M$ 进行签名:

(a)随机选取 $r\in Z_q^*$,计算 $R=g^r\in G_2$;

(b)计算 $h=H_2(M\parallel\text{ID}\parallel R\parallel P_{\text{ID}})\in Z_q^*$,$V=rP+hS_{\text{ID}}\in G_1$;

(c)输出签名 $\sigma=(h,V)$。

g)验证。给定身份为 ID 的签名者在公钥 $P_{\text{ID}}$下对消息 $M$ 的签名 $\sigma=(h,V)$,验证者首先计算 $R'=e(V,P)e(Q_{\text{ID}},P_{\text{ID}})^{-h}$,然后检验等式 $h=H_2(M\parallel\text{ID}\parallel R'\parallel P_{\text{ID}})\in Z_q^*$ 是否成立,如果等式成立,则认为签名合法,输出 1;否则认为签名非法,输出 0。

## 3　安全性分析

### 3.1　对 HX 方案的安全性分析

下面给出一种公钥替换攻击,证明 HX 方案是不安全的。对于任意选择的消息 $m$ 和任意身份为 ID 的用户,敌手通过替换公钥可以伪造用户 ID 对该消息 $m$ 的有效签名。敌手伪造签名过程如下:

a)随机选择 $t_k\in Z_p^*$,计算 $pk_{\text{ID}}=t_kQ$;

b)随机选择 $t_r\in Z_p^*$,计算 $R=g^{t_r}$;

c)计算 $h=H_2(m,R)$;

d)计算 $S=t_k^{-1}(t_r+h)P$;

e)输出伪造签名 $\sigma=(S,R)$。

下面证明伪造签名 $\sigma=(S,R)$是有效签名。由于

$$e(S,pk_{\text{ID}})g^{-h}=e(t_k^{-1}(t_r+h)P,t_kQ)g^{-h}=e((t_r+h)P,Q)g^{-h}=$$
$$e(t_rP,Q)e(hP,Q)g^{-h}=e(P,Q)^{t_r}e(P,Q)^he(P,Q)^{-h}=$$
$$e(P,Q)^{t_r}=g^{t_r}=R$$

所以签名 $\sigma=(S,R)$是一个有效的伪造签名。

### 3.2　对 LLZ 方案的安全性分析

下面给出公钥替换攻击和恶意 KGC 攻击,证明 LLZ 方案是不安全的。

1)公钥替换攻击　对于任意选择的合法用户 ID 和消息 $M$,敌手总可以按如下步骤伪造用户 ID 对消息 $M$ 的签名:

a)随机选择 $t_{\text{ID}}\in Z_q^*$,计算 $P_{\text{ID}}=t_{\text{ID}}P$;

b)随机选择 $t_v\in Z_q^*$,计算 $R=g^{t_v}=e(P,P)^{t_v}$;

c)计算 $h=H_2(M\parallel\text{ID}\parallel R\parallel P_{\text{ID}})$;

d)计算 $V=t_vP+t_{\text{ID}}hQ_{\text{ID}}$;

e)输出消息 $M$ 的伪造签名 $\sigma=(h,V)$。

下面验证伪造签名 $\sigma=(h,V)$是有效的。因为

$$R'=e(V,P)e(Q_{\text{ID}},P_{\text{ID}})^{-h}=e(t_vP+t_{\text{ID}}hQ_{\text{ID}},P)e(Q_{\text{ID}},t_{\text{ID}}P)^{-h}=$$
$$e(t_vP+t_{\text{ID}}hQ_{\text{ID}},P)e(-hQ_{\text{ID}},t_{\text{ID}}P)=$$
$$e(t_vP+t_{\text{ID}}hQ_{\text{ID}},P)e(-t_{\text{ID}}hQ_{\text{ID}},P)=$$
$$e(t_vP,P)=g^{t_v}=R$$

所以 $h=H_2(M\parallel\text{ID}\parallel R\parallel P_{\text{ID}})=H_2(M\parallel\text{ID}\parallel R'\parallel P_{\text{ID}})$。这说明 $\sigma=(h,V)$是用户 ID 在替换公钥 $P_{\text{ID}}$下对消息 $M$ 的有效签名。因此,LLZ 方案对于公钥替换攻击是不安全的。

2)恶意 KGC 攻击　这种攻击是恶意 KGC 从系统设置阶段就开始有预谋地针对特殊目标用户设置特殊的系统参数。这种特殊的系统参数对所有用户而言,与正常系统参数不可区分。根据这种特殊的系统参数和目标用户公布的公钥,KGC 可以计算出该目标用户的私钥,从而可以伪造该目标用户对任意消息的签名。下面详细描述这种攻击的过程。

当建立系统参数时,恶意 KGC 选择某一身份为 $\text{ID}_T$ 的目标用户,并选择任意随机数 $t\in Z_q^*$,计算 $P=tH_1(\text{ID}_T)$。其他系统参数的构造与原来基本一样。

当用户 $\text{ID}_T$ 提取部分私钥时,KGC 把 $D_T=sQ_T=sH_1(\text{ID}_T)$ 作为部分私钥通过安全信道交给用户 $\text{ID}_T$。

当诚实的用户 $\text{ID}_T$ 利用提取的部分私钥 $D_T$ 计算私钥时,选择随机数 $x_T\in Z_q^*$ 并计算其私钥为

$$S_T=x_TD_T=x_TsQ_T=x_TsH_1(\text{ID}_T)$$

一旦用户 $\text{ID}_T$ 计算并公布了所使用的公钥 $P_T$,KGC 就可以计算出用户 $\text{ID}_T$ 的私钥。因为 $P=tH_1(\text{ID}_T)$,所以恶意 KGC 由 $P_T=x_TP_0=x_TsP=x_TstH_1(\text{ID}_T)$ 可以得到 $x_TsH_1(\text{ID}_T)=t^{-1}P_T$,即用户 $\text{ID}_T$ 的私钥 $S_T=t^{-1}P_T$。

由于恶意 KGC 同时知道了用户 $\text{ID}_T$ 的部分私钥和用户私钥,所以它可以冒充用户 $\text{ID}_T$ 对任意消息伪造签名。因此,LLZ 方案对于恶意 KGC 攻击是脆弱的。

(下转第 3052 页)

相比于 Morales-Rocha 等人的方案,改进方案是为进一步保证安全性而进行的改进。

(1)原方案中选票是邮寄的,改进方案中选票直接通过 email 传送,便捷可靠,节省成本。

(2)改进方案中加入选票生成机构以生成选票,同时会在选票分发前对选票加密。削弱了选票分发机构的权限,降低了投票者身份泄露的危险性。

(3)改进方案没有用到投票者签名,而是由投票平台 *VP* 对投票者身份进行认证,相比于 Morales-Rocha 方案,改进方案因不使用投票者签名,统计阶段就不会暴露投票者身份,并且改进方案中,投票阶段公布了与 $R-\mathrm{ID}_i$ 对应的候选人,如果继续使用 Morales-Rocha 等人的方案中投票者的签名方式,投票服务器将能直接由 $S_i$ 将投票者与所选候选人联系起来。

(4)改进方案中,统计中心公布和 $R-\mathrm{ID}_i$ 对应的候选人。由此,投票者能确定自己的选票是否被正确接收并统计。如果统计中心公布了与 $R-\mathrm{ID}_i$ 对应的候选人而并未统计,那么从最终的总结果中可以看出统计中心进行了错误统计。

(5)在改进方案中,统计中心公布了与 $R-\mathrm{ID}_i$ 对应的候选人。而在原方案中 $R_i=[r_i]_{S_{VS}}$,投票者只要将 $R_i=[r_i]_{S_{VS}}$、$R-\mathrm{ID}_i$ 发送给买票者,买票者通过解密 $r_i$,再验证 $r_i=[H(R-\mathrm{ID}_i\mid E-\mathrm{ID}_i)]$ 是否成立,即可确定 $R-\mathrm{ID}_i$ 有效性,并从公布的数据中找到对应的候选人。改进方案加入了整个投票系统的公钥 $P_{\mathrm{system}}$,除非由所有投票系统共同恢复出对应私钥,否则无法确认 $r_i$,从而是在防止选票收买的前提下对原方案进行的改进。

## 6 结束语

本文回顾了文献[6]中的预加密可验证电子投票方案,在原方案的预加密基础上,采用分发选票前再进行一次加密的策略,改进了该方案中分发机构权限过大,容易得到投票者隐私的漏洞。同时,通过投票平台 *VP* 验证投票者的合法性,避免了统计选票时投票者身份不必要的暴露。因原方案的统计过程事实上不可验证,本文在统计过程中公布了最终候选人结果以保证可验证性,同时在原方案中创建一个投票系统的公钥 $P_{\mathrm{system}}$ 并将私钥成分分发以协作解决纠纷,这种方式很好地解决了为保证可验证性而带来的买卖选票问题。

**参考文献:**


[1] SAMPIGETHAY K, POOVENDRAN R. A framework and taxonomy for comparison of electronic voting schemes[J]. Computers & Security, 2006,25(2):137-153.

[2] FUJIOK A, OKAMOTO T, OHATA K. A practical secret voting scheme for large scale election[C]//Proc of Workshop on the Theory and Application of Cryptographic Techniques. London: Springer-Verlag,1993:244-251.

[3] COHEN J D,FISCHER M J. A robust and verifiable cryptographically secure election scheme[C]//Proc of the 26th Annual IEEE Symposium on Foundations of Computer Science. Washington DC:IEEE Computer Society, 1985:372-382.

[4] CHAUM D. Untraceable electronic mail, return address and digital pseudonyms[J]. Communications of the ACM,1981,24 (2):84-88.

[5] KUN P. A general and efficient countermeasure to relation attacks in mix-based e-voting[J]. International Journal of Information Security,2011,10(1):49-60.

[6] STORE T, DUNCAN I. Pollsterless remote electronic voting[J]. Journal of E-Government, 2004,1(1):75-103.

[7] MORALES-ROCHA V,SORIANO M,PUIGGALI J. New voter verification scheme using pre-encrypted ballots[J]. Computer Communications, 2009,32(7-10):1219-1227.

[8] ADIDA B. Helios: Web-based open-audit voting[C]//Proc of the 17th Conference on Security Symposium. Berkeley: USENIX Association,2008:335-348.

[9] JOAQUIM R,RIBEIRO C. Code voting: protection against automatic vote manipulation in an uncontrolled environment[C]//Proc of the 1st International Conference on E-voting and Identity. Berlin:Springer-Verlag, 2007:178-188.

[10] RIERA A,RIFA J,BORRELL J. Efficient construction of vote-tags to allow open objection to the tally in electronic elections[J]. Information Processing Letters,2000,75 (4):211-215.


(上接第 3047 页)

## 4 结束语

无证书签名方案既能克服普通公钥签名方案的证书管理问题,又能克服基于身份签名方案固有的密钥托管问题。本文对两个高效的无证书签名方案进行了安全性分析,证明了这两个方案对于公钥替换攻击和恶意 KGC 攻击是不安全的,给出了详细的攻击方法。在公钥替换攻击下,类型 I 敌手可以伪造任意用户对任意消息签名的签名。类型 II 敌手(恶意 KGC)首先在系统参数生成阶段利用预选目标用户的身份生成含有陷门信息的系统参数,然后利用该目标用户公布的公钥计算该用户的私钥,并伪造该用户对任意消息的签名。

**参考文献:**


[1] AL-RIYAMI S, PATERSON K. Certificateless public key cryptography[C]//LNCS, vol 2894. Berlin: Springer-Verlag, 2003: 452-473.

[2] HUANG X, SUSILO W, MU Y,*et al*. On the security of certificateless signature schemes from Asiacrypt [C]//LNCS, vol 3810. Berlin: Springer-Verlag,2005:13-25.

[3] ZHANG Z F,WONG D S,XU J,*et al*. Certificateless public-key signature:security model and efficient construction[C]//LNCS,vol 3989. Berlin:Springer-Verlag,2006:293-308.

[4] AU M H, CHEN J, LIU J K,*et al*. Malicious KGC attacks in certificateless cryptography[C]//Proc of ASIACCS. New York:ACM Press, 2007:302-311.

[5] CASTRO R, DAHAB R. Two notes on the security of certificateless signatures[C]//LNCS,vol 4784. Berlin:Springer-Verlag, 2007:85-102.

[6] 王化群,徐名海,郭显久. 几种无证书数字签名方案的安全性分析及改进[J]. 通信学报, 2008,29(5):88-92.

[7] 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.

[8] 洪东招,谢琪. 有效的无证书签名方案[J]. 计算机应用,2010,30(7):1809-1811.

[9] 李凤银,刘培玉,朱振方. 高效的无证书签名方案[J]. 计算机工程与应用, 2011,47(10):23-26.