信阳师范学院学报: 自然科学版
第 25 卷　第 4 期　2012 年 10 月

Journal of Xinyang Normal University
Natural Science Edition Vol. 25 No. 4 Oct. 2012

DOI: 10.3969/j.issn.1003-0972.2012.04.032

一种无证书签密方案的安全性分析及改进

樊爱京*

(平顶山学院 网络计算中心,河南 平顶山 467002)

摘　要: 利用无证书密码体制的安全模型,分析了一种无证书数字签密方案,发现其存在安全性缺陷. 针对这些安全性缺陷,对原方案进行了改进. 分析结果表明,该方案具有安全保密性、不可伪造性、不可否认性,改进的方案是有效安全的.

关键词: 无证书签密; 双线性对; 机密性; 不可伪造性

中图分类号: TP309　　文献标志码: A　　文章编号: 1003-0972(2012)04-0551-04

Security Analysis and Improvement of a Certificateless Signcryption Scheme

FAN Ai-jing*

(Network Computer Center, Pingdingshan University, Pingdingshan 467002, China)

Abstract: A kind of certificateless digital signcryption scheme was analyzed by using the certificateless cryptosystem security model, and the security flaws were found. Furlhermore, the improved scheme was proposed to eradicate the security flaws. The analysis results show that the improved scheme is characterized by its confidentiality, unforgeability, nonrepudiation, which implies that the improved scheme is safe and effective.

Key words: certificateless cryptosystem; bilinear pairing; confidentiality; unforgeability

0　引言

Riyami 和 Paterson 在 2003 年提出的无证书的密码系统(CL-PKC)解决了基于身份的密码系统中的密钥托管问题[1]. 但是部分私钥由密钥生成中心(Key Generation Center, KGC)生成的行为可能使用户受到恶意的 KGC 攻击[2]. 于是围绕无证书密码系统的安全性研究也逐渐展开.

近年来,一些研究者基于 CL-PKC 的思想,提出了基于无证书的签密方案[3-4]. 无证书的签密是指在一个合理的逻辑步骤内同时完成数字签名和加密两项功能,计算量和通信代价低于传统的先签名后加密方法. 文献[5]提出一个可公开验证的无证书签密方案,使用 4 个对运算,使其方案易于实现. 文献[5]认为文献[5]方案不满足机密性,是一种不安全的无证书签密方案,但并未给出相应的改进方案. 本文分析文献[5]中的无证书签密方案,发现方案既不能判别 KGC 的积极不诚实行为,也无法抵抗伪造攻击. 针对这些安全性缺陷对原方案进行改进. 通过正确性及安全性分析说明改进方案具有安全保密性、不可伪造性、不可否认性.

1　预备知识

1.1　双线性映射及相关困难问题

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 是一个阶为 q 的乘法群. 若一个映射 $e: G_1 \times G_1 \to G_2$ 满足以下三条性质,则称这个映射为双线性映射[7].

(1) 双线性: 对于任何 $U, V \in G_1$: $a, b \in \mathbf{Z}_q^*$,

$$e(aU, bV) = e(U, V)^{ab}.$$

(2) 非退化性: 存在 $U, V \in G_1$ 使得

$$e(U, V) \neq 1.$$

(3) 可计算性: 对于任何的 $U, V \in G_1$,存在一个高效的算法来计算 $e(U, V)$ 的值.

双线性映射可以通过有限域上超椭圆曲线上的 Tate 对和 Weil 对来构造. 本文涉及到的相关困难问题如下[8]:

收稿日期: 2012-03-22; 修订日期: 2012-07-04; * . 通讯联系人, E-mail: fajlp@yahoo.com.cn
基金项目: 河南省科技计划重点项目(102102210416)
作者简介: 樊爱京(1970-),男,河南内乡人,副教授,硕士,主要从事网络研究.

定义 1　(离散对数问题(DHP)): P 是 G_1 的生成元,任取 $Q \in G_1$. 在已知 P,Q 的条件下,求 $n \in \mathbf{Z}_q^*$,使得 $Q = nP$ 的问题.

定义 2　(Diffie-Hellman 问题(CDHP)): 已知 P,aP,$bP \in G_1$,求 abP 的问题,其中 a,$b \in \mathbf{Z}_q^*$.

假设 DHP 问题和 CDHP 问题是困难的,即不存在多项式时间算法以不可忽略的概率求解 DHP 问题和 CDHP 问题. 群 G_1 的选取可满足 DHP 问题、CDHP 问题难解.

1.2　无证书签密体制

一个无证书签密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、签名以及验证等 7 个算法组成. 通常,前两个算法由 KGC 执行,而其他算法由签名或验证用户执行[8].

在无证书签密机制的安全模型中,存在 2 种类型的敌手攻击以及在适应性选择密文攻击下具有不可区分性和在适应性选择消息攻击下存在不可伪造性.

Type-Ⅰ 攻击者 A_{I}: 不能获取系统主密钥,但可以替换任意用户公钥,同时 A_{I} 能够多项式次进行 Hash 询问.

Type-Ⅱ 攻击者 A_{II}: 拥有主密钥,可以自己产生部分私钥,但是不能替换用户的公钥.

2　文献[6]方案及攻击方法

2.1　文献[6]方案描述

系统参数生成: KGC 选定满足 1.1 节所述性质的 e,G_1,G_2,P,并在 $\mathbf{Z}_q^*$ 中随机选取系统主密钥 s,计算系统公钥 $P_0 = sP$. 选择哈希函数 $H_1: \{0,1\}^* \rightarrow G_1$; $H_2: \{0,1\}^* \rightarrow \mathbf{Z}_q^*$; $H_3: G_2 \rightarrow \{0,1\}^*$,设置系统参数$\{e, G_1, G_2, P, P_0, H_1, H_2, H_3\}$.

设置秘密值: 用户(其身份为 ID)在 $\mathbf{Z}_q^*$ 中随机选取一个值 S_{ID1} 作为其秘密值,计算 $Q_{ID1} = S_{ID1}P$ 并公布.

部分私钥生成: KGC 利用系统主密钥帮用户生成部分私钥. 当输入一个用户的身份 ID,KGC 计算 $Q_{\mathrm{ID}} = H_1(ID)$,并输出该用户的部分私钥 $S_{ID2} = sQ_{ID}$.

设置公钥: 用户(其身份为 ID)设置部分公钥为 $Q_{ID2} = S_{ID1}Q_{ID}$,公钥为(Q_{ID1}, Q_{ID2}).

设置私钥: 身份为 ID 的用户设置其私钥为 $sk_{ID} = S_{ID1}S_{ID2}$.

假设签密者的身份为 A,其公钥为(Q_{A1}, Q_{A2}),私钥为 sk_A. 解签密者的身份为 B,其公钥为(Q_{B1}, Q_{B2}),私钥为 sk_B.

签密: 当输入一个消息 m,该签名者按以下方式对消息 m 进行签密:

1) 选取 $k \in \mathbf{Z}_q^*$,计算 $U = kP_0$.

2) 计算 $r = H_2(m \| U)$,$V = k \cdot r \cdot sk_A$.

3) 计算 $y = e(S_{A1}Q_{B2}, P_0)$,$C = H_3(y) \oplus m$.

4) 输出签密文 $\sigma = (V, U, C)$.

解签密: 解签密者收到 $\sigma = (V, U, C)$ 后,按照以下方式进行解签密:

1) 计算 $y = e(sk_B, Q_{A1})$,$m = H_3(y) \oplus C$.

2) 计算 $r = H_2(m \| U)$,

3) 检验等式 $e(V, P) \stackrel{?}{=} e(Q_{A2}, U)^r$. 若成立则输出 1,否则输出 0.

2.2　对文献[6]方案的攻击

设已知签密者的身份为 A,其公钥为(Q_{A1}, Q_{A2}),私钥为 sk_A. 解签密者的身份为 B,其公钥为(Q_{B1}, Q_{B2}),私钥为 sk_B. 消息 m 和签名 $\sigma = (V, U, C)$,攻击者分别对机密性与不可伪造性进行攻击.

2.2.1　机密性攻击

文献[6]提出了基于攻击者 A_{I} 在不知道主密钥 s 情况下进行的机密性攻击. 该攻击方法是攻击者 A_{I} 对签密者 A 的公钥替换攻击. 借助

$$y = e(sk_B, Q_{A1}) = e(S_{B1}sQ_B, S_{A1}P) = e(S_{A1}Q_{B2}, P_0)$$

的理论依据,绕过主密钥 s,攻击者 A_{I} 只需要知道 S_{A1} 就可以获取 y 的值,继而破解 m. 但是,攻击者 A_{I} 如何获取 S_{A1} 的值,文献[6]并未给出详细过程.

事实上,在公钥替换攻击中,攻击者 A_{I} 只能自己产生私钥,并以此产生一个公钥对,从而使用该公钥对替代签密者 A 的公钥对. 在这个过程中,是先生成私钥,然后再生成公钥对,并非文献[6]所说先替换公钥,再得出签密者 A 的 S_{A1} 值. 由此可见,即使攻击者 A_{I} 对签密者 A 进行公钥替换攻击,也不能得出签密者 A 的 S_{A1} 值. 文献[6]提出的基于攻击者 A_{I} 的机密性攻击是无效攻击. 但是,这并不妨碍对文献[6]的基于攻击者 A_{II} 的 KGC 攻击.

攻击者 A_{II} 在知道主密钥 s 情况下,充当恶意 KGC. 可使用 $y = e(sQ_{B2}, Q_{A1})$ $m = H_3(y) \oplus C$,即可破解. 原因如下:

$$y = e(S_{A1}Q_{B2}, P_0) = e(S_{A1}Q_{B2}, sP) = e(sQ_{B2}, Q_{A1}).$$

2.2.2　不可伪造性攻击

针对签名 $\sigma = (V, U, C)$,攻击者伪造签名如

下:

1) 签名者选取计算 $U=P$;

2) $r=H_2(m\|U)$, $V=rQ_{A2}$;

3) 将 $\sigma=(V,U,C)$ 发送给验证者.

验证者收到已经替换的签名后,仍然按照验证算法验证,即计算 $e(V,P)\stackrel{?}{=}e(Q_{A2},U)^r$,验证一定会通过. 原因如下:

$$e(V,P)=e(rQ_{A2},P)=e(Q_{A2},U)^r.$$

由此可见,方案宣称的签密算法是无效的.

2.3 对文献[5]方案的安全性分析

在无证书数字签密机密性攻击中,攻击者 A_{II} 主要利用 $y=e(sk_B,Q_{A1})$ 可等价 $y=e(sQ_{B2},Q_{A1})$ 进行了攻击. 攻击成功的原因是:(1) 由于 sk_{ID} 中原来的两个秘密值 (S_{ID1},s) 实质上只有 1 个 s 起作用,$sk_{ID}=S_{ID1}S_{ID2}=S_{ID1}sQ_{ID}=sS_{ID1}Q_{ID}=sQ_{ID2}$;(2) 方案的公钥 (Q_{ID1},Q_{ID2}) 的构成都是由一个参数 S_{ID1} 决定,这就使得签密者在签名时逃避使用部分私钥的行为成为可能.

在无证书数字签密伪造攻击中,攻击者 A_{I} 和 A_{II} 攻击成功的主要原因在于: 伪造签名者可以根据验证算法构建虚假签名算法,替代原有签名算法. 其中,$V=k\cdot r\cdot sk_A$ 表面上是 3 个参数,实质上是一个参数作为秘密值存在. 如果要使伪造的签名算式通过确认,就需签名方构造参数 V 和 U. 假设构造的 $U=X$,其中 X 可为 P,tP,Q_{ID1},则构造 V 的过程如下:

$$e(V,P)=e(Q_{A2},U)^r=e(rQ_{A2},X),$$
$$V=rQ_{ID2},U=P.$$

方案中的参数 V 和 U 没有关联. 这就导致了 U 变化确定后,V 就可以变化适应 U. 如果改变 U,则 V 变化; V 变化,则 U 变化,两个参数相互影响,就很难让攻击者构造绕过系统主密钥的 V,然后再构造出适应 V 的 U. 防止构造 V 和 U 的方法,就是 V 和 U 的参数应该有共同的三个或者两个秘密值共同决定.

3 改进方案

系统参数生成、设置秘密值、部分私钥生成的过程与文献[5]方案相同.

设置公钥: 用户(其身份为 ID)设置部分公钥为 $Q_{ID2}=Q_{ID}$,公钥为 (Q_{ID1},Q_{ID2}).

设置私钥: 身份为 ID 的用户设置其私钥为 (S_{ID1},S_{ID2}).

签密: 假设签密者的身份为 A,其公钥为 (Q_{A1},Q_{A2}),私钥为 (S_{A1},S_{A2}). 解签密者的身份为 B,其公钥为 (Q_{B1},Q_{B2}),私钥为 (S_{B1},S_{B2}).

1) 选取 $k\in\mathbf{Z}_q^*$,计算 $U=kP_0$.

2) 计算

$$y=e(kS_{A1}Q_{B1},P_0)e(S_{A2},Q_{B2}),$$
$$C=H_3(y)\oplus m.$$

3) 计算 $V=S_{A1}U+H_3(y)S_{A2}$.

4) 输出签密文 $\sigma=(V,U,C)$.

验证: 解签密者收到 $\sigma=(V,U,C)$ 后,按照以下方式进行解签密:

1) 计算

$$y=e(S_{B1}Q_{A1},U)e(Q_{A2},S_{B2}),$$
$$m=H_3(y)\oplus C.$$

2) 检验等式

$$e(V,P)\stackrel{?}{=}e(U,Q_{A1})e(H_3(y)Q_{A2},P_0).$$

若成立则输出 1,否则输出 0.

4 改进方案性能分析

4.1 正确性分析

该无证书签密方案是正确的.

事实上,假如无证书签密文 $\sigma=(V,U,C)$ 是按签密过程计算得到的,则必有以下等式成立.

$$\begin{aligned}y&=e(kS_{A1}Q_{B1},P_0)e(S_{A2},Q_{B2})=\\&e(S_{A1}S_{B1}P,kP_0)e(sQ_{A2},Q_{B2})=\\&e(S_{B1}S_{A1}P,kP_0)e(Q_{A2},sQ_{B2})=\\&e(S_{B1}Q_{A1},U)e(Q_{A2},S_{B2}),\end{aligned}$$

$$\begin{aligned}e(V,P)&=e(S_{A1}U+H_3(y)S_{A2},P)=\\&e(S_{A1}U,P)e(H_3(y)S_{A2},P)=\\&e(U,S_{A1}P)e(H_3(y)sQ_{A2},P)=\\&e(U,Q_{A1})e(H_3(y)Q_{A2},sP)=\\&e(U,Q_{A1})e(H_3(y)Q_{A2},P_0).\end{aligned}$$

以上无证书签密算法是满足验证等式的,故方案是正确的.

4.2 安全性分析

(1) 机密性

本文方案具有内部安全的保密性,分析攻击者 A_{I} 和 A_{II}.

如果要获取明文 $m=H_3(y)\oplus C$,就必须先知道 y 的值. $y=e(kS_{A1}Q_{B1},P_0)e(S_{A2},Q_{B2})$ 或者 $y=e(S_{B1}Q_{A1},U)e(Q_{A2},S_{B2})$. 前者为 A 的两把私钥,一把是由自身产生,另一把与系统密钥相关. 后者为 B 的两把私钥. 对于攻击者 A_{I},在不知道主密钥的

前提下,可以替换 S_{A1} 和 S_{B1},但是由于部分私钥 $S_{A2}=sQ_{A2}$,$S_{B2}=sQ_{B2}$ 是由 s 控制的,无法替换. 如果求 s,需要通过 $P_0=sP$,这相当于 DHP 难题. 对于攻击者 A_{II},在知道主密钥 s 的前提下,替换用 s 决定的部分私钥. 但是另一部分私钥是合法用户自己生成,$S_{A1}=S_{A1}P$,$S_{B1}=S_{B1}P$. 攻击者 A_{II} 无法知道用户自定义的私钥. 求自定义私钥的困难相当于 DHP 难题. 如果绕开自定义私钥攻击,则需要求 $kS_{A1}Q_{B1}$ 和 $S_{B1}Q_{A1}$,求解的代价为 CDHP 难题. 因此,本文方案具有内部安全保密性.

(2) 不可为造性

本文方案具有不可伪造性,它是在无证书签名方案的基础上提出的. 本文采用文献 [6-7] 结论,改进后的方案在 CDHP 困难性的假设下,2 种类型的敌手都不能伪造有效的签名. 对攻击者 A_I 和 A_{II},如果伪造签名,就必须知道密钥对及秘密值. 而密钥对的求解相当于 DHP 的难题. 由于密钥对及秘密值决定了 $V=S_{A1}U+H_3(y)S_{A2}$,如果使用 3.2 节的攻击方式,攻击是无效的. 因此,本文方案具有不可伪造性.

(3) 不可否认性

在签密验证环节中,

$$e(V,P)\stackrel{?}{=}e(U,Q_{A1})\,e(H_3(y)Q_{A2},P_0)$$

中涉及到两个公钥,一个 s 参数. 其中,两个公钥隐含着两把私钥. 私钥和主密钥 s 决定发送方的不可否认性.

(4) 公开验证性

在 $e(V,P)\stackrel{?}{=}e(U,Q_{A1})\,e(H_3(y)Q_{A2},P_0)$ 中,没有涉及到私钥及秘密值. 将 $\sigma=(V,U,C)$ 发送给验证者,验证者通过已公布的参数,能够进行公开验证.

5　结论

本文对文献 [5] 提出的无证书签密方案进行了分析. 由于密钥值在签名中未完全利用,并且未对两个重要参数建立关联,导致攻击者可进行构造算法,并实施签名伪造攻击的行为成为可能. 针对原方案出现的错误,本文对方案进行了改进. 改进方案正确性及安全性分析结果说明,改进方案具有安全保密性、不可伪造性、不可否认性等特点. 但是,改进方案没有考虑到运算速度的问题. 如何将运算速度与签密算法的正确性相结合,是今后研究的重点.

参考文献:

[1] Al-Riyami S, Paterson K. *Certificateless public key cryptography* [C] // Proceedings of the Asiacrypt 2003, Lecture Notes in Computer Science 2894. Taipei: Springer-Verlag, 2003: 452-473.

[2] 蔡伟艺,杨晓元. 可公开验证的高效无证书签密方案 [J]. 计算机工程, 2011, 37(17): 108-110.

[3] Choi K, Park J, Hwang J, et al. *Efficient certificateless signature schemes* [C] // Proceedings of the ACNS 2007, Lecture Notes in Computer Science 4521. Zhuhai: Springer-Verlag, 2007: 443-458.

[4] Barbosa M, Farshim P. *Certificateless signcryption* [C] //Proceedings of Computer and Communications Security Conference. Berlin: Springer-Verlag, 2008: 919-931.

[5] 王会歌,王彩芬,易玮,等. 高效的无证书可公开验证签密方案 [J]. 计算机工程,2009,35(5): 147-149.

[6] 陈 明,吴开贵,何盼. 一种新的无证书签密方案 [J]. 计算机应用研究,2011,28(10): 3800-3804.

[7] 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.

[8] 张玉磊. 高效的无证书紧致有序多重签名方案 [J]. 计算机工程,2011,37(8): 109-111.

[9] 宋明明, 张彰, 谢文坚. 一种无证书签密方案的安全性分析 [J]. 计算机工程,2011,37(9): 163-164.

责任编辑: 郭红建