Journal of Computer Applications
计算机应用,2013,33(8):2250 - 2252
ISSN 1001-9081
CODEN JYIIDU
2013-08-01
http://www.joca.cn

文章编号:1001-9081(2013)08-2250-03
doi:10.11772/j.issn.1001-9081.2013.08.2250

无双线性对的无证书签名方案的分析及改进

王　怡*,杜伟章
(长沙理工大学 计算机与通信工程学院,长沙 410114)
(*通信作者电子邮箱 ewayi28@qq.com)

摘　要:对王圣宝等(王圣宝,刘文浩,谢琪.无双线性配对的无证书签名方案.通信学报,2012,33(4):93 - 98)提出的不使用双线性配对运算的无证书签名方案进行安全性分析,指出该方案无法抵抗积极不诚实的恶意密钥生成中心(KGC)攻击,并给出了该攻击方式的具体攻击方法。针对这种攻击方式,提出了改进方案,并对改进的方案进行了安全性分析。分析结果表明,改进后的方案在保持原方案高效性的同时,能抵抗恶意 KGC 攻击,具有更高的安全性,并且改进后的方案不再需要使用安全通道,降低了通信复杂度。

关键词:无证书签名;椭圆曲线;离散对数问题;双线性对;密钥生成中心
中图分类号:TP309.7　　**文献标志码**:A

Security analysis and improvement of certificateless signature scheme without bilinear pairing

WANG Yi*, DU Weizhang
(*College of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha Hunan* 410114, *China*)

Abstract: By analyzing the security of a certificateless signature scheme without bilinear pairing proposed by Wang Shengbao, *et al.* (WANG S B, LIU W H, XIE Q. Certificateless signature scheme without bilinear pairings. Journal on Communications, 2012, 33(4): 93 - 98), it indicated that the scheme could not resist malicious attack of positive dishonest Key Generation Center (KGC). For this kind of attack, detailed attack method was given, and an improved scheme was proposed. Finally, the security of the improved scheme was analyzed. The result shows that the proved scheme can resist the malicious KGC attack, maintain efficiency of the original scheme and has higher security. Meanwhile, the communication complexity is reduced due to the elimination of the security channel.

Key words: certificateless signature scheme; elliptic curve; Discrete Logarithm Problem (DLP); bilinear pairing; Key Generation Center (KGC)

0　引言

无证书公钥密码系统[1]是由 Al-Riyami 等提出的,在该系统中,用户的私钥由密钥生成中心(Key Generation Centre, KGC)生成的部分私钥和用户自己选取的秘密值共同组成,恶意 KGC 由于不知道用户秘密值而无法获得用户的私钥。由于无证书公钥系统具有非常突出的优势,基于无证书公钥系统的签名方案被相继提出[2-7]。但是,这些方案大多都使用双线性对来完成签名及验证过程,存在计算效率不高的问题。于是许多学者致力于提高无证书签名方案计算效率的研究,但是往往在提高了计算效率的同时忽略了方案的安全性。如文献[8]提出了一个无证书签名方案,该方案没有进行双线性对的运算,提高了签名和验证效率。然而该方案被杨波等[9]指出存在安全缺陷,任何敌手都能进行公钥替换攻击完成签名伪造。另外,有的方案在安全性上满足了要求,效率却有待提高,没有做到在签名过程和签名验证过程均不使用双线性对运算,如张玉磊等[10]和李凤银等[11]分别于 2010 年和 2011 年提出的高效的无证书签名方案,虽然这两个方案在签名过程中都没有使用双线性对,但在签名验证过程中却进行了双线性对运算。2012 年,王圣宝等[12]提出了一个不使用双线性对的无证书签名方案,以下简称 WLX 方案。该方案无论是在签名阶段还是在签名验证阶段都没有使用双线性对运算,运算效率得到了很大的提高,而且在离散对数问题难解的条件下,证明了方案的安全性。然而 WLX 方案的安全性是在保证 KGC 完全可信的前提下达到的。

本文对 WLX 方案进行了安全性分析,发现该方案无法抵抗积极不诚实的 KGC 攻击。积极不诚实的 KGC 指的是 KGC 可以伪造出有效的密钥冒充用户完成签名。本文针对这种攻击者的特点,改进了用户密钥的生成方式,使得 KGC 生成部分私钥受到用户的约束,积极不诚实的 KGC 无法伪造出有效的用户密钥。改进后的方案在保持了原方案高效性的同时,具有更高的安全性,同时消除了安全通道,降低了通信复杂度。

1　预备知识

定义 1　椭圆曲线离散对数问题(Elliptic Curve Discrete Logarithm Problem, ECDLP)。给定椭圆曲线上的两点 $P,Q \in G_1$,已知 $Q = kP$,计算 $k \in \mathbf{Z}_q^*$。

定义 2　椭圆曲线计算 Diffie-Hellman 问题(Elliptic Curve Computational Diffie-Hellman Problem, ECCDH)。设 P 是循环群 G_1 中的生成元,已知 $P, aP, bP \in G_1$,其中 $a,b \in \mathbf{Z}_q^*$,计算 $Y = abP$。

收稿日期:2013-03-04;**修回日期**:2013-04-04。

作者简介:王怡(1987 -),女,湖南衡阳人,硕士研究生,主要研究方向:信息安全;　杜伟章(1965 -),女,湖南长沙人,教授,博士,主要研究方向:信息安全、纠错编码、计算数学。

2　WLX 方案简介

1) 系统建立阶段。

输入安全参数 k,输出2个大素数 p,q, 满足 $q|p-1$。设 P 为循环群 G_1 中任意一个阶为 q 的生成元。选择 Hash 函数: $H_1:\{0,1\}^* \times G_1 \rightarrow \mathbf{Z}_q^*$, $H_2:\{0,1\}^* \rightarrow \mathbf{Z}_q^*$, KGC 随机选择主密钥 $z \in \mathbf{Z}_q^*$, 计算 $y = zP$, 并公开系统参数 $\{p,q,P,y,H_1,H_2\}$, 保密系统主密钥 z。

2)用户密钥生成。

给定用户身份标识 ID_i, KGC 随机选取 $r_i \in \mathbf{Z}_q^*$, 然后计算 $R_i = r_iP, D_i = r_i + zH_1(ID_i,R_i)$, 通过安全信道将 D_i 发给用户。用户将 D_i 作为部分私钥,将 $R_i = r_iP$ 作为他的部分公钥。

用户随机选取 $x_i \in \mathbf{Z}_q^*$ 作为其长期私钥,生成相应私钥 (x_i,D_i), 接着计算 $X_i = x_iP$, 生成公钥 (X_i,R_i)。用户可以通过验证等式 $R_i + H_1(ID_i,R_i)y = D_iP$ 是否成立来判断 KGC 发送的部分私钥是否有效。

3)签名。

假定用户 A 为签名者,随机选择整数 $a \in \mathbf{Z}_q^*$, 然后计算 $T_A = aP, h = H_2(T_A,X_A,ID_A,m), s_1 = a/(x_A + D_A + h), s_2 = x_A/(x_A + D_A + h)$, 从而得到签名 $\sigma = (h,s_1,s_2)$, 并将其与部分公钥 R_A 一道传递给用户 B。

4)签名验证。

假定 B 为签名验证者, 当收到签名 σ 和 R_A 后,B 计算 $h_1 = H_1(ID_A,R_A)$,验证:$s_1(R_A + X_A + h_1y + hP) = T_A, s_2(R_A + X_A + h_1y + hP) = X_A$。

关于 WLX 方案的正确性和安全证明详见文献[12]。

3　对 WLX 方案的攻击

文献[12]指出,在随机预言模型下,基于离散对数困难假设证明了所提出的方案的安全性,其结果显示方案是安全的,而实际上积极不诚实的 KGC 可以伪造出有效密钥,对消息产生签名并通过验证。下面将给出针对此方案的具体攻击方法。

假设积极不诚实的 KGC 攻击者要伪造在消息 m' 上的签名,具体的攻击方法如下:

1)攻击者随机选择 $r_A' \in \mathbf{Z}_q^*$, 计算 $R_A' = r_A'P, D_A' = r_A' + zH_1(ID_A,R_A')$, 然后通过安全信道发送给用户;

2)攻击者随机选择 $u \in \mathbf{Z}_q^*$, 计算 $K = uP$;

3)计算 $h_1' = H_1(ID_A,R_A')$, $X_A' = K - R_A' - h_1'y$;

4)随机选择 $a' \in \mathbf{Z}_q^*$,计算 $T_A' = a'P$, $h' = H_2(T_A',X_A',ID_A,m'), s_1' = a'/(u + h'), s_2' = (u - r_A' - zh_1')/(u + h')$;

5) 输出伪造签名 $\sigma' = (h',s_1',s_2')$。

以上攻击者伪造的签名 σ' 是有效的,首先伪造的部分密钥可以通过 WLX 方案中的部分密钥有效性验证式 $R_i + H_1(ID_i,R_i)y = D_iP$; 另外,由攻击者伪造的签名 σ' 能通过签名验证式 $s_1(R_A + X_A + h_1y + hP) = T_A$ 和 $s_2(R_A + X_A + h_1y + hP) = X_A$。具体证明如下:

$$R_A' + H_1(ID_A,R_A')y = r_A'P + H_1(ID_A,R_A')zP = (r_A' + H_1(ID_A,R_A')z)P = D_A'P$$

验证者收到签名 σ' 和 R_A' 后,计算 $h_1' = H_1(ID_A,R_A')$, 然后验证:

$$s_1'(R_A' + X_A' + h_1'y + h'P) = (a'/(u + h'))\times(R_A' + X_A' + h_1'y + h'P) = (a'/(u + h'))\times(R_A' + K - R_A' - h_1'y + h_1'y + h'P) = (a'/(u + h'))\times(K + h'P) = (a'/(u + h'))\times(uP + h'P) = a'P = T_A'$$

$$s_2'(R_A' + X_A' + h_1'y + h'P) = ((u - r_A' - zh_1')/(u + h'))\times(R_A' + X_A' + h_1'y + h'P) = ((u - r_A' - zh_1')/(u + h'))\times(R_A' + K - R_A' - h_1'y + h_1'y + h'P) = ((u - r_A' - zh_1')/(u + h'))\times(K + h'P) = (u - r_A' - zh_1')P = K - R_A' - h_1'y = X_A'$$

由上面的证明可知,伪造的签名可以满足验证式,即伪造的签名是有效的。

4　改进方案

在 WLX 方案中,在签名前对 KGC 发送的部分密钥进行了有效性验证,有效地防止了除 KGC 之外的攻击者进行公钥替换攻击,而该验证却无法抵抗积极不诚实的 KGC 攻击。这是因为部分密钥有效性验证式 $R_i + H_1(ID_i,R_i)y = D_iP$ 中的部分私钥 D_i 和部分公钥 R_i 均由 KGC 生成,并且 KGC 知道系统主密钥,对于恶意 KGC 来说,要想伪造出能通过验证式的部分密钥是可以实现的。只要恶意 KGC 再伪造出有效的公钥,就可以对消息进行伪造签名。为了避免积极不诚实的 KGC 进行密钥伪造攻击,可以对方案进行如下两个方面的改进:1)部分私钥由用户最终生成;2)在部分私钥生成以及验证过程中均加入用户部分公钥信息 X_i, 使得 X_i 必须在部分私钥产生之前就生成,从而使 KGC 生成部分私钥的行为受到用户的限制,避免积极不诚实的 KGC 在没有用户约束的前提下伪造出公钥 X_i'。

改进方案包含系统参数建立、部分密钥生成、公钥生成、私钥生成、签名和签名验证 6 个算法,各算法的具体描述如下:

1)系统建立阶段。

输入安全参数 k, 输出 2 个大素数 p、q,q 为 $p-1$ 的大素数因子满足 $q|p-1$。设 P 为循环群 G_1 中任意一个阶为 q 的生成元。选择三个 Hash 函数: $H_1:\{0,1\}^* \times G_1 \times G_1 \rightarrow \mathbf{Z}_q^*$, $H_2:\{0,1\}^* \rightarrow \mathbf{Z}_q^*, H_3:G_1 \rightarrow \mathbf{Z}_q^*$。KGC 随机选择系统的主密钥 $z \in \mathbf{Z}_q^*$, 然后计算系统主公钥 $y = zP$。系统公开参数是: $\{p,q,P,y,H_1,H_2,H_3\}$。

2)用户部分密钥生成。

假设签名人为 A, 用户身份标识为 ID_A, 其中 $ID_A \in \{0,1\}^*$, 用户随机选取 $x_A \in \mathbf{Z}_q^*$ 作为其长期私钥,计算 $X_A = x_AP$, 将 X_A 和 ID_A 发送给 KGC;

KGC 随机选取 $r \in \mathbf{Z}_q^*$, 计算 $R = rP$。KGC 获得用户的 X_A 后,计算 $D_{KGC} = r + zH_1(ID_A,R,X_A) + H_3(zX_A)$, 然后通过公开信道将 R 和 D_{KGC} 发给用户 A;

用户收到 R 和 D_{KGC} 后,首先通过验证式(1)是否成立来判断 KGC 发送的 D_{KGC} 是否有效:

$$R + yH_1(ID_A,R,X_A) + PH_3(x_Ay) = D_{KGC}P \quad (1)$$

然后计算部分私钥 $D_A = D_{KGC} - H_3(x_Ay)$,将 $R = rP$ 作为部分公钥。任何人都无法通过 $y = zP$ 和 $X_A = x_AP$ 求解出 zx_AP, 因为这是一个 ECCDH 问题。

3) 用户公钥生成。

用户 A 设置自己的公钥为 $PK_A = (X_A, R)$。

4) 用户私钥生成。

用户 A 设置自己的私钥为 $SK_A = (x_A, D_A)$。

5) 签名。

对于消息 $m \in \{0,1\}^*$，签名者随机选择整数 $a \in \mathbf{Z}_q^*$，计算 $T_A = aP, h = H_2(T_A, PK_A, ID_A, m), s = (ah + x_A)/(x_A h + D_A)$，从而得到签名 $\sigma = (h, s)$，将其与 R 一起发送给签名验证者。

6) 签名验证。

假定用户 B 为签名验证者，B 收到签名 $\sigma = (h, s)$ 和 R 后，首先计算 $h_1 = H_1(ID_A, R, X_A)$，然后验证式(2)是否成立，若成立则接收签名 σ，否则拒绝。

$$s(hX_A + R + h_1 y)) = hT_A + X_A \tag{2}$$

5 改进方案的分析

5.1 改进方案的安全性分析

5.1.1 正确性

1) 部分私钥有效性验证式(1)的证明：

$$\begin{aligned} &R + yH_1(ID_A, R, X_A) + PH_3(x_A y) = \\ &\quad rP + zPH_1(ID_A, R, X_A) + PH_3(x_A y) = \\ &\quad (r + zH_1(ID_A, R, X_A) + H_3(zx_A P))P = \\ &\quad (r + zH_1(ID_A, R, X_A) + H_3(zX_A))P = D_{KGC}P \end{aligned}$$

2) 签名有效性验证式(2)的证明：

$$\begin{aligned} &D_A = D_{KGC} - H_3(x_A y) = \\ &\quad r + zH_1(ID_A, R, X_A) + H_3(zX_A) - H_3(x_A y) = \\ &\quad r + zH_1(ID_A, R, X_A) + H_3(zx_A P) - H_3(x_A zP) = \\ &\quad r + zH_1(ID_A, R, X_A) \end{aligned}$$

$$\begin{aligned} &s(hX_A + R_A + yh_1) = \\ &\quad ((ah + x_A)/(x_A h + D_A)) \times (X_A h + R + yh_1) = \\ &\quad ((ah + x_A)/(x_A h + D_A)) \times (x_A hP + rP + zhP_1) = \\ &\quad ((ah + x_A)/(x_A h + D_A)) \times (x_A h + r + zh_1)P = \\ &\quad ((ah + x_A)/(x_A h + D_A)) \times (x_A h + D_A)P = \\ &\quad (ah + x_A)P = ahP + x_A P = hT + X_A \end{aligned}$$

5.1.2 不可伪造性

原方案的不安全性主要在于无法抵抗积极不诚实的 KGC 进行密钥伪造攻击，改进方案针对这一问题进行了改进。原方案在离散对数困难问题的前提下，对于除积极不诚实的 KGC 之外的其他攻击者，对方案的安全性进行了详细证明。以下针对该攻击敌手的不可伪造性进行安全性分析。

改进的新方案中，在部分私钥生成前，由用户先生成自己的部分公钥 X_A，然后发送给密钥生成中心 KGC，再由 KGC 计算 $D_{KGC} = r + zH_1(ID_A, R, X_A) + H_3(zX_A)$，式中包含了由用户所产生的 X_A，因此 KGC 生成 D_{KGC} 的行为要受到用户的限制。首先，由于式中对 X_A 进行了哈希函数的处理，根据哈希函数的单向性可知，恶意的 KGC 试图通过部分私钥验证式来伪造出满足条件的公钥 X_A' 是不可能的；其次，即使积极不诚实的 KGC 通过自己所拥有的主密钥 z 和自己随机选择的特殊参数 r，伪造出了一个公钥 X_A'，也无法满足包含用户公钥信息的部分私钥有效性验证式 $R + yH_1(ID_A, R, X_A) + PH_3(x_A y) = D_{KGC}P$。所以改进后的方案可以抵抗积极不诚实的 KGC 攻击，即该攻击敌手无法伪造出有效密钥冒充用户签名，满足不可伪造性。

5.2 改进方案的效率分析

新方案在原方案的基础上，改进了用户密钥的生成方式，并未增加运算量较大的双线性对运算和指数运算。根据文献[13]的实验结论可知，双线性对运算耗时远大于其他运算。表 1 给出了改进方案与其他高效无证书签名方案的运算量对比，其中 P、E、H 分别表示双线性对运算、循环群 G_2 中的指数运算以及散列运算，S 和 A 分别表示循环群 G_1 中的标量乘运算和点加运算，忽略了其他运算量较小的运算。

表 1 运算量对比

签名方案	签名阶段	验证阶段	总运算量
文献[10]方案	2H + 2S + 1A	2P + 1S + 2H	2P + 4H + 3S
文献[11]方案	1E + 1H + 2S + 1A	2P + 1E + 1H	2P + 2E + 1H + 2S + 1A
文献[12]原方案	1H + 1S	1H + 8S + 6A	2H + 9S + 6A
改进方案	1H + 1S	1H + 4S + 3A	2H + 5S + 3A

由表 1 可知本文所改进的方案仍未使用双线性配对运算，且减少了循环群 G_1 中的标量乘运算和点加运算。因此改进后的方案相比其他无证书签名方案，效率优势明显。

6 结语

本文分析了文献[12]所提出的无双线性配对运算的无证书签名方案，指出该方案在安全方面具有缺陷，不能抵抗积极不诚实的 KGC 所进行的密钥替换攻击。分析了存在这一安全缺陷的原因，并针对这一问题，改进了用户的密钥生成方式，使得 KGC 无法伪造出有效密钥冒充用户进行签名。改进后的方案同样未使用双线性对运算，并且无需安全通道用于传输部分私钥，降低了通信复杂度。通过安全性分析和效率分析可知，改进后的方案在保持高效性的同时，克服了原方案的安全缺陷。

参考文献：

[1] AL-RIYAMI S, PATERSON K G. Certificateless public key cryptography [C] // Advances in Cryptology — ASIACRYPT 2003, LNCS 2894. Berlin: Springer-Verlag, 2003: 452 - 473.

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

[3] 魏春艳, 蔡晓秋. 新的无证书代理盲签名方案[J]. 计算机应用, 2010, 30(12): 3343 - 3345.

[4] 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.

[5] 胡国政, 王展青, 陆济湘, 等. 无证书代理盲签名方案的安全性分析[J]. 计算机工程, 2012, 38(13): 112 - 114.

[6] 陈江山, 黄振杰. 没有双线性对的无证书签名方案的分析与改进[J]. 计算机应用, 2010, 30(2): 510 - 512.

[7] 张建中, 彭丽慧, 薛荣红. 一个无证书代理盲签名方案[J]. 计算机工程, 2011, 37(14): 112 - 113.

[8] 张燕燕, 王亮亮. 新型的基于 DLP 的无证书签名方案[J]. 计算机工程与应用, 2011, 47(12): 62 - 64.

[9] 杨波, 肖自碧, 李寿贵, 等. 一种无证书签名方案的分析与改进[J]. 计算机工程, 2012, 38(9): 15 - 18.

[10] 张玉磊, 王彩芬, 张永洁, 等. 一个新的高效无证书签名方案[J]. 计算机工程与应用, 2010, 46(14): 84 - 87.

[11] 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.

[12] 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.

[13] CHOI K Y, PARK J H, LEE D. Efficient certificateless signature schemes [C]// Proceedings of the 5th International Conference on Applied Cryptography and Network Security. Berlin: Springer-Verlag, 2007: 443 - 458.