文章编号:1009-3087(2013)04-0111-06

具有强安全性不含双线性对的基于证书盲签名

周 萍, 何大可, 张文芳*
(西南交通大学 信息科学与技术学院,四川 成都 610031)

摘 要:基于证书密码体制是传统公钥密码体制的最新演进,但现有基于证书签名方案大都采用双线性对构造,计算效率较低。为了解决这个问题,基于离散对数难题,提出1种不含双线性映射的基于证书盲签名方案。方案以有限域上模幂运算为主构造,避免了复杂的对运算,用二元仿射变换盲化消息,计算量小、效率高。每次验证签名前用验证方程检验证书及公钥的真实性,实现了2者之间的相互认证。方案在随机预言机模型下证明能够抵抗用户伪造攻击、认证中心伪造攻击和公钥替换攻击,并具有强盲性。分析表明,与同类方案相比,本方案具有签名长度短,计算量和通信量小的优势,特别适用于计算能力和带宽受限的领域。

关键词:基于证书密码体制;盲签名;双线性对;离散对数难题
中图分类号:TP309 **文献标志码**:A

Strongly Secure Certificate-based Blind Signature Scheme Without Pairings

*ZHOU Ping, HE Da-ke, ZHANG Wen-fang**
(College of Info. Sci. & Technol., Southwest Jiaotong Univ., Chengdu 610031, China)

Abstract: Certificate-based Cryptosystem is the latest evolution of traditional public key cryptosystem, but most of existing certificate-based signature schemes were constructed by pairings, which led to low calculation efficiency. Based on discrete logarithm problem, a certificate-based blind signature scheme without pairings was presented. The new scheme had higher efficiency, as it was mainly based on modular exponentiation arithmetic in the finite field instead of pairings and messages were blinded by affine transformation. The validities of public key and certificate were verified before verifying signature, so the mutual authentication of both public key and certificate was achieved. Under the random oracle model, it was proved that the scheme was blind and existentially unforgeable against user forgery attack, CA forgery attack and public key replacing attack. Efficiency analysis showed that, compared with other similar schemes, the proposed scheme had shorter signature length, smaller computation and communication complexity, so it was suitable for application fields of lower computing power and limited bandwidth.

Key words: certificate-based cryptosystems; blind signature; bilinear pairing; discrete logarithm problem

为了解决传统公钥密码体制的证书管理问题及基于身份密码体制的密钥托管问题, Gentry[1] 于2003年提出了基于证书密码体制(certificate-based cryptographic primitives, CBC)。在该体制中,用户首先生成自己的公私钥对,然后把自己的身份信息和公钥发送给认证中心CA。CA在验证了用户身份信息是真实有效的后,用自己的主密钥签名,生成证书发送给用户。用户用私钥及证书的某种组合进行签名或解密消息,用身份信息、公钥和CA的公钥验证签名或加密消息。

CBC消除了传统公钥密码体制中对证书的第三方询问问题,简化了证书撤销过程,此外证书还可以用来构造签名密钥。与基于身份密码体制相比,CA不参与用户私钥的生成,也就不能伪造用户的签名,因而彻底解决了基于身份密码体制中的密钥分发和密钥托管问题。与无证书密码体制相比,证书的存在避免了该体制容易遭受公钥替换攻击的缺陷。此外,CBC还克服了基于身份密码体制和无证书密码体制中,用户与PKG之间需要安全信道来传递私钥或部分私钥的问题。

收稿日期:2013-03-04
基金项目:国家自然科学基金资助项目(61003245;60903202);四川省杰出青年学术带头人培育计划资助项目(2011JQ0027);中央高校基本科研业务费专项资金资助项目(SWJTU12CX099;SWJTU11CX041)
作者简介:(1968—),女,博士生,副教授. 研究方向:普通和特殊数字签名、认证理论. E-mail:zzpp0086@163.com.
* 通信联系人 E-mail: wfzhang2001@163.com

现阶段对基于证书密码体制的研究仍然处于起步阶段,已有的研究成果主要集中在基于证书加密方面,基于证书签名方面的相对较少,而基于证书特殊数字签名方面的则少之又少。2004 年 Kang 等[2]提出了 1 种基于证书签名方案,在随机预言机模型下证明了方案的安全性。2007 年 Li 等[3]指出 Kang 方案不能抵抗公钥替换攻击,并提出 1 种新的基于证书签名方案。2008 年 Liu 等[4]提出了 2 种新型基于证书签名方案,第 1 种因不使用双线性对而提高了效率,第 2 种因证明了方案在标准模型下的安全性而更为安全。但在 2009 年 Zhang 等[5]指出 Liu[4]的第 1 种方案是不安全的,并提出 1 种更高效的签名方案。同年 Wu 等[6]提出 1 种更加合理和准确的基于证书签名的安全性定义,并在此基础上提出从无证书签名方案构造基于证书签名方案的一般性方法。同在 2009 年 Li 等[7]基于证书密码体制提出了 1 种代理签名方案,并在随机预言机模型下证明了方案的安全性。2012 年,Li 等[8]提出了 1 种高效的基于证书短签名方案,方案仅在验证阶段有 1 个对运算,且签名长度仅为 1 个 G_1 群元素的长度。此外,2012 年还有一些研究成果[9-10]。以上这些成果或者使用双线性对构造,计算开销较大,或者安全性较弱,不能抵抗多种攻击。因此,构造强安全、不含双线性对的、基于证书普通或特殊数字签名方案具有重要的理论意义和实际意义。

盲签名因为签名内容对签名人具有盲性,可以保护盲签名申请者的个人隐私,因而被广泛应用于电子现金支付系统和匿名电子选举系统等多种应用领域。目前对于盲签名的研究成果虽然很多,但都是基于传统公钥、基于身份、基于无证书密码体制的,还没有基于证书密码体制的盲签名。

将基于证书密码体制引入到盲签名中,基于离散对数难题,首次提出了 1 种不含对运算、具有强安全性的基于证书盲签名方案,证明了方案的强盲性和在随机预言机模型下的安全性:可抵抗用户伪造攻击、CA 伪造攻击和公钥替换攻击。效率分析表明,本文方案比同类方案具有更小的计算量和通信量。

1 基于证书数字签名的安全性定义

一般地,基于证书签名方案通常由 Setup 系统建立算法、KeyGen 用户密钥生成算法、CertGen 证书生成算法、Sign 签名算法、Verify 签名验证算法几个算法组成[6]。

对基于证书签名方案的攻击一般存在两类 - 用户伪造攻击和 CA 伪造攻击。前者指攻击者知道用户私钥,但不知道与公钥相对应的证书。后者指攻击者知道系统主密钥,可以自己伪造用户证书,但不知道用户的私钥。记第 1 种攻击者为 A_1,第 2 种攻击者为 A_2。

定义 1 对于一种基于证书签名方案,如果不存在攻击者 A_1,借助挑战者 B, 能够以不可忽略的概率在多项式时间内赢得下面的游戏 Game1 时,称该方案可以抵抗用户伪造攻击[6]。

Game1: B 和 A_1 进行下面的游戏:

1) Setup: B 运行 Setup 算法,生成系统参数 *params* 和主私钥 S_C。B 将 *params* 发送给 A_1,自己秘密保存 S_C。

2) Query: A_1 向 B 提交下述一系列查询。查询方式为适应性选择查询,次数为多项式次。设 U 为任意一个用户。

①UserKeyGen 查询: A_1 输入 U 的身份信息 ID, B 返回 U 的公私钥对(PK_{ID}, S_{ID})。

②ReplacePublicKey 查询: A_1 可以将 U 的公钥替换为其他公钥。A_1 输入(ID,PK_{ID}'),B 将 U 的公钥替换为 PK_{ID}'。

③CertGen 查询: A_1 输入(ID,PK_{ID}),B 返回 U 的证书 $Cert_{ID}$。

④Hash 查询: A_1 可以询问方案中所有 Hash 函数在任意输入时的函数值, B 返回对应的函数值。

⑤Sign 查询: A_1 询问 U 对任意消息 m 的签名。A_1 输入(ID,m),B 返回签名 σ。

3) Forge:经过以上多项式次适应性选择方式查询后, A_1 伪造出公钥为 PK_{ID^*} 身份为 ID^* 的用户对消息 m^* 的签名 σ^*,并且 ID^* 没有做过 ReplacePublicKey 查询,(ID^*, K_{ID^*})没有做过 CertGen 查询,(ID^*,m^*)没有做过 Sign 查询。如果 σ^* 在方案的签名验证算法中被证明“有效”,则称 A_1 赢得游戏 Game1。

定义 2 对于 1 种基于证书签名方案,当不存在攻击者 A_2,借助挑战者 B, 能够以不可忽略的概率在多项式时间内赢得下面的游戏 Game2 时,称方案可以抵抗 CA 伪造攻击[6]。

Game2: B 和 A_2 进行下面的游戏:

1) Setup:类似于定义 2。

2) Query:类似于 Game1, A_2 向 B 提交下述一系列查询。

①UserKeyGen 查询: A_2 输入 U 的身份信息 ID,

B 返回 U 的公钥 PK_{ID},秘密保存 U 的私钥 S_{ID}。

②PrivateKey 查询:A_2 输入(ID,PK_{ID}),B 检查 PK_{ID} 是否是 UserKeyGen 查询的输出,如果是,返回对应的私钥 S_{ID},否则返回"无效"。

③ReplacePublicKey 查询。

④Hash 查询。

⑤Sign 查询。

③④⑤均类似于定义 2。

3)Forge:在进行了以上多项式次适应性选择方式查询后,A_2 伪造出用户(公钥 PK_{ID^*},身份信息 ID^*)对消息 m^* 的签名 σ^*,并且 ID^* 没有做过 ReplacePublicKey 查询,(ID^*,PK_{ID^*})没做过 PrivateKey 查询,(ID^*,m^*)没做过 Sign 查询。如果 σ^* 在方案验证算法中被证明"有效",则称 A_2 赢得游戏 Game2。

Game1 中,A_1 可以询问任何用户的公私钥对,可以替换任何用户的公钥,但不知道欲伪造用户的证书。如果不存在攻击者 A_1 能够以不可忽略的概率在多项式时间内赢得 Game1,说明方案不仅可以抵抗用户伪造攻击,还可以抵抗公钥替换攻击。A_1 模拟的是除 CA 以外的攻击者。

Game2 中,A_2 知道系统主密钥,可以生成任何用户的证书,但不知道欲伪造用户的私钥。如果不存在攻击者 A_2 能够以不可忽略的概率在多项式时间内赢得 Game2,说明方案可以抵抗 CA 伪造攻击。A_2 模拟的是恶意 CA。

定义 3　如果一个基于证书签名方案在适应性选择消息和身份攻击下,能够抵抗用户伪造攻击和 CA 伪造攻击,抵抗公钥替换攻击,则称该方案是安全的。

2　新的基于证书盲签名方案

新方案详述如下:

1)Setup 算法:根据安全参数 1^k 的要求,CA 随机选择 2 个大素数 p,q 使 $q|(p-1)$ 成立,再随机选择 1 个 Z_p^* 的生成元 g,g 的阶为 q。记由 g 生成的子群为 G。CA 随机选择 $S_C \in Z_q^*$ 作为私钥,计算公钥 $PK_C = g^{S_C} \bmod p \in G$,并且选择 Hash 函数 $H_1: \{0,1\}^* \times (Z_p^*)^3 \rightarrow Z_q^*$,$H_2: \{0,1\}^* \times (Z_p^*)^4 \rightarrow Z_q^*$。CA 秘密保存主密钥 S_C,公布 $params = \{p,q,g,G,PK_C,H_1,H_2\}$。

2)KeyGen 算法:用户 Bob 随机选择私钥 $S_A \in Z_q^*$,计算公钥 $PK_A = g^{S_A} \bmod p$。

3)CertGen 算法:Bob 将自己的身份 ID_A 和公钥 PK_A 发送给 CA。CA 收到后,检验 ID_A 的真实性。如检验通过,CA 任选 $c \in Z_q^*$,计算 $P_A = g^c \bmod p$,$R_A = H_1(ID_A,PK_A,PK_C,P_A)$,$T_A = c + S_C R_A \pmod q$,将证书$(P_A,T_A)$发送给 Bob 并秘密删除 c。

Bob 收到后,进行有效性验证:计算 $R_A = H_1(ID_A,PK_A,PK_C,P_A)$,再检查证书 - 公钥双向验证方程:$W_1 = g^{T_A} = P_A \cdot (PK_C)^{R_A} \bmod p$ 是否成立。如果成立则接受此证书并保存(R_A,W_1),否则要求 CA 重新为自己生成证书。注意这里不需要安全信道传递证书。

4)Sign 算法:设 Alice 请求 Bob 对消息 m 进行盲签名,他们之间的交互过程如下:

①Bob 随机选取 $k \in_R Z_q^*$,计算 $K = (W_1)^k \bmod p$,将 K 秘密发送给 Alice。

②盲化消息:Alice 随机选取 3 个整数 $\alpha,\beta,\lambda \in_R Z_q^*$,计算:

$$R_A = H_1(ID_A,PK_A,PK_C,P_A),$$
$$W_2 = (PK_A)^{R_A} \bmod p,$$
$$U = g^{\alpha}(K \cdot W_2^{\beta})^{\lambda} \bmod p,$$
$$h = H_2(m,ID_A,U,PK_A,PK_C,P_A),$$
$$h' = \lambda^{-1}h + \beta \pmod q。$$

将 h' 发送给 Bob。

③签名:Bob 用私钥 S_A 和证书(P_A,T_A)签名:$\sigma' = h'S_A R_A + k \cdot T_A \pmod q$。将 σ' 发送给 Alice。

④脱盲:Alice 对签名 σ' 进行脱盲运算:

$$\sigma = \lambda\sigma' + \alpha \pmod q。$$

则消息 m 的盲签名即为(σ,h)。

5)Verify 算法:

①实施对 Bob 公钥和证书的双向认证:计算 $R_A = H_1(ID_A,PK_A,PK_C,P_A)$,然后检查验证方程 $g^{T_A} = P_A \cdot (PK_C)^{R_A} \bmod p$ 是否成立。如不成立则公钥和证书无效验证中断,否则进行下一步。

② 计算 $U = g^{\sigma} \cdot (PK_A)^{-hR_A} \bmod p$,验证:

$$h = H_2(m,ID_A,U,PK_A,PK_C,P_A) \qquad (1)$$

是否成立,如果成立,则签名有效,否则签名无效。

3　安全性分析

3.1　正确性

定理 1　方案中的签名是有效的。即消息 m 的盲签名(σ,h)满足验证式(1)。

证明:由签名算法可知,消息的盲化方法主要基于如下的二元仿射变换。即:

$$U = g^{\alpha}(K \cdot W_2^{\beta})^{\lambda} = g^{\alpha} \cdot g^{k\lambda T_A} \cdot g^{\beta\lambda S_A R_A} = g^{\alpha + k\lambda T_A + \beta\lambda S_A R_A} (\mathrm{mod}\ p),$$

$$\sigma = \lambda\sigma' + \alpha = \lambda(\lambda^{-1}h + \beta)S_A R_A + k\lambda \cdot T_A + \alpha = hS_A R_A + \lambda\beta S_A R_A + k\lambda T_A + \alpha (\mathrm{mod}\ q)。$$

因此有:

$$g^{\sigma} = U \cdot g^{hS_A R_A} = U \cdot (PK_A)^{hR_A} (\mathrm{mod}\ p),$$

故

$$U = g^{\sigma} \cdot (PK_A)^{-hR_A} (\mathrm{mod\ p})。$$

因此,式(1)成立。证毕。

3.2 强盲性

定理2 方案是强盲的。

证明:签名过程中,若签名者Bob保存了每一次签名过程的中间数据(k,K,h',σ')。当Alice或消息接收者公开消息m及签名(σ,h)时,Bob可以得到它们。这样Bob就可以得到2组数据(k,K,h',σ')和(m,σ,h),Bob想找出它们之间有无链接关系。

因为在签名过程中,使用了3个随机数α、β、λ,因此从理论上说,只要有4个等式连接这2组数据,就可以找出2者之间的链接关系,其中3个等式用于求出α、β、λ,第4个等式用于判断2者之间有没有关系。

但在本方案中,只有3个连接等式:

$$h' = \lambda^{-1}h + \beta (\mathrm{mod}\ q),$$

$$\sigma = \lambda\sigma' + \alpha (\mathrm{mod}\ q),$$

$$U = g^{\alpha}(K \cdot PK_A^{R_A\beta})^{\lambda} = g^{\sigma} \cdot (PK_A)^{-hR_A} (\mathrm{mod}\ p)。$$

因此无法判断2者之间有无关系。而且由于离散对数问题的难解性,无法从3个等式中求出α、β、λ。故方案是强盲的。证毕。

3.3 安全性

定理3 对于本文方案,在随机预言机模型下,如果存在攻击者A_1,能够以不可忽略的概率ε在多项式时间内赢得Game1,则挑战者B借助A_1能够以不可忽略的概率$O(\varepsilon)$在多项式时间内解决离散对数问题。

证明:设1个离散对数问题的随机实例为{已知g,β,求使$\beta = g^{\alpha}$成立的α}。设A_1是方案的1个攻击者,能够以不可忽略的概率ε在多项式时间内赢得Game1。下面证明B可以借助于A_1解决此随机实例。

B运行本文方案的Setup算法,生成*params*和主密钥S_C。B自己秘密保存S_C,同时将*params*发送给A_1。

B模拟随机预言机服务,A_1可以向B查询,B回答这些查询,并建立几个列表保存以下内容:T_0保存UserKeyGen查询结果,T_1、T_2保存H_1、H_2查询结果,T_3保存CertGen查询结果,T_4保存Sign查询结果。

设A_1最多进行了q_{ask}次UserKeyGen查询。B随机选择$i^* \in [1,q_{\mathrm{ask}}]$,记$ID^* = ID_{i^*}$,令$PK_{ID^*} = \beta$,$S_{ID^*} = \|$($\|$表示空),将$(ID^*, PK_{ID^*}, S_{ID^*})$保存在$T_0$中。

A_1与B进行如下交互:

1)UserKeyGen查询:A_1输入ID_i。①若$i \neq i^*$,B在表T_0中查询,若$(ID_i, *, *) \in T_0$,返回对应的公私钥对(PK_i, S_i),否则任选随机数$S_i \in Z_q^*$且$(*, *, S_i) \notin T_0$,计算$PK_i = g^{S_i} \bmod p$,再将(PK_i, S_i)返回A_1,将(ID_i, PK_i, S_i)保存在表T_0中。②若$i = i^*$,挑战失败,终止游戏。

2)ReplacePublicKey查询:A_1输入$(ID_i, (PK_{ID})_i')$,B查询$(ID_i, *, *)$是否在表T_0中,如在则用$(PK_{ID})_i'$替代原来的公钥,同时私钥不变,否则将$(ID_i, (PK_{ID})_i', \|)$保存在T_0中。

3)CertGen查询:A_1输入$(ID_i, (PK_{ID})_i)$,B检查$(ID_i, (PK_{ID})_i, *)$是否在表T_3中,如果在返回对应的证书,否则B检查$(ID_i, (PK_{ID})_i, *)$是否属于T_0,如果不属于则输出"无效",否则选择2个随机数$c, R_A \in Z_q^*$,计算:$P_{ID} = g^c \bmod p$,$T_{ID} = c + S_C R_A (\mathrm{mod}\ q)$,将$(P_{ID}, T_{ID})$发送给$A_1$,再将$(ID_i, (PK_{ID})_i, (P_{ID}, T_{ID}))$保存在表$T_3$中,将$((ID_i, (PK_{ID})_i, PK_C, P_{ID}), R_A)$保存在表$T_1$中并秘密删除$c$。保存之前先查看$((ID_i, (PK_{ID})_i, PK_C, P_{ID}), *)$是否已包含在$T_1$中,如未包含则保存,否则重选$c, R_A$进行上述操作。

4)H_1查询:A_1输入任意(ID_A, PK_A, PK_C, P_A),B查看表T_1。如果表中存在该输入,返回对应的输出,否则任选1个随机数$y \in Z_q^*$(y满足$((*, *, *, *), y) \notin L_1$),将$((ID_A, PK_A, PK_C, P_A), y)$保存在表$T_1$中,将$y$返回给$A_1$。

5)H_2查询:A_1输入任意$(m, ID_A, U, PK_A, PK_C, P_A)$,$B$查看表$T_2$。如果已存在该输入则返回对应的输出,否则任选1个随机数$h \in Z_q^*$(h满足$((*, *, *, *, *, *), h) \notin L_2$),将$((m, ID_A, U, PK_A, PK_C, P_A), h)$保存在表$T_2$中,将$h$返回给$A_1$。

6)Sign查询:A_1输入(m, ID_i)。如果:

①$ID_i \neq ID^*$且B在表T_0中找到了与ID_i对应的公私钥(PK_{ID}, S_{ID}),且该公钥未被替换(即$PK_{ID} = g^{S_{ID}} \bmod p$成立),则$B$先在表$T_3$中找到对应的证

书(P_{ID},T_{ID}),在表 T_1 中找到对应的 R_A(注:如果该证书不存在,则 B 按 CertGen 查询的步骤生成证书(P_{ID},T_{ID})并将(ID_i,PK_{ID},(P_{ID},T_{ID}))保存在 T_3 中,将((ID_i,PK_{ID},PK_C,P_{ID}),R_A)保存在 T_1 中)。然后 B 任意选择 5 个随机数 $k,\alpha,\beta,\lambda,h \in Z_q^*$,计算:

$$K = g^{k \cdot T_{ID}} \bmod p,\ W_2 = (PK_{ID})^{R_A} \bmod p,$$

$$U = g^{\alpha}(K \cdot W_2^{\beta})^{\lambda} \bmod p,$$

$$\sigma = hS_{ID}R_A + \beta\lambda S_{ID}R_A + k\lambda T_{ID} + \alpha (\bmod q)。$$

检查表 T_2 中是否已有((m,ID_i,U,PK_{ID},PK_C,P_{ID}),*),如没有就将((m,ID_i,U,PK_{ID},PK_C,P_{ID}),h)保存在 T_2 中,否则另选随机数 $k,\alpha,\beta,\lambda,h \in Z_q^*$ 重复上述步骤。最后 B 将盲签名(σ, h) 返回给 A_1。

② 如果 $ID_i \neq ID^*$ 且与 ID_i 相对应的公钥被替换过,或者 $ID_i = ID^*$,则此时 B 并不知道与 ID_i 相对应的私钥。B 采用以下方法生成盲签名:首先从表 T_0 中找到对应的公钥 PK_{ID},在表 T_3 中找到对应的证书(P_{ID},T_{ID}),在 T_1 中找到对应的 R_A(如果证书和 R_A 不存在,B 可以生成它们,方法同①)。然后 B 任意选择 2 个随机数 $h,\sigma \in Z_q^*$,计算 $U = g^{\sigma}(PK_{ID})^{-hR_A} \bmod p$,令 $h = H_2(m,ID_i,U,PK_{ID},PK_C,P_{ID})$。检查表 T_2 中是否已有((m,ID_i,U,PK_{ID},PK_C,P_{ID}),*),如果没有就将((m,ID_i,U,PK_{ID},PK_C,P_{ID}),h)保存在 T_2 中;否则重选随机数 $h,\sigma \in Z_q^*$ 进行上述计算。最后 B 将盲签名(σ, h) 返回给 A_1。

查询结束后,A_1 输出 1 个伪造的有效盲签名(m,ID,(σ,h))。如果 $ID \neq ID^*$,则挑战该随机实例失败,B 放弃。否则,根据分叉引理,B 重复上述过程,可以生成 2 个有效签名(m, U, h, σ) 和(m, U, h', σ'),满足 $h \neq h'$ 及 $\sigma \neq \sigma'$。

记:

$$R = H_1(ID^*,PK_{ID^*},PK_C,P_{ID^*}),$$

有:

$$g^{\sigma} = (PK_{ID^*})^{h \cdot R} \cdot U, g^{\sigma'} = (PK_{ID^*})^{h' \cdot R} \cdot U,$$

得到:

$$g^{\sigma-\sigma'} = (PK_{ID^*})^{(h-h') \cdot R},$$

$$\alpha = S_{ID^*} = (\sigma - \sigma')/((h - h')R) \bmod q。$$

于是,B 成功解决了该随机实例。

设 A_1 最多进行了 q_{ask} 次 UserKeyGen 询问,且 A_1 输出合法签名的概率为 ε。由证明过程可知,伪造出 $ID = ID^*$ 的合法签名的概率至少为 $1/q_{ask}$,在 UserKeyGen 查询中不查询 ID^* 的公私钥的概率至少为 $(1 - 1/q_{ask})^{q_{ask}}$。因此 B 解决 DLP 随机实例的概率 $Adv \geq \varepsilon \cdot (1 - 1/q_{ask})^{q_{ask}}/q_{ask} = O(\varepsilon)$。

由此可知,定理 3 成立。证毕。

定理 4　对于本文方案,在随机预言机模型下,如果存在攻击者 A_2,能够以不可忽略的概率 ε 在多项式时间内赢得 Game2,则 B 借助 A_2 能够以不可忽略的概率 $O(\varepsilon)$ 在多项式时间内解决离散对数问题。

证明:证明方法同定理 3。

定理 5　方案能够抵抗公钥替换攻击。

证明:攻击者 A 可分为 2 种类型 - 普通攻击者或 CA。设 U 是 A 要攻击的对象。

1) 如果 A 是普通攻击者

① 虽然 A 可以得到 U 的身份信息、公钥和证书,但 A 不知道 U 的私钥。由定理 3、4 可知,A 不能伪造 U 的签名。

② 如果 A 用另外伪造的数对(y, x) 替代 U 的公私钥对(PK_U, S_U),其中,$y = g^x \bmod p$。

若 A 保持 U 的证书(P_U,T_U) 不变来伪造签名,由 *Hash* 函数的抗强碰撞性,$R_U' = H_1(ID_U,y,PK_C,P_U)$,$R_U = H_1(ID_U,PK_U,PK_C,P_U)$,必有 $R_U \neq R_U'$,因此验证方程 $g^{T_U} = P_U(PK_C)^{R_U'} \bmod p$ 不成立,签名无效。

若 A 用伪造的证书(P_U',T_U') 代替 U 的证书,则因为 A 并不知道主密钥 S_C, 由 Hash 函数的抗强碰撞性和 DLP 的难解性, A 不能伪造出能使验证方程 $R_U' = H_1(ID_U,y,PK_C,P_U')$,$g^{T_U'} = P_U'(PK_C)^{R_U'} \bmod p$ 成立的假证书,进而不能伪造出合法签名。因此 A 不能对 U 实施有效的公钥替换攻击。

2) 如果 A 是 CA

此时 CA 知道 S_C,能够成功伪造 U 的证书和公私钥对。这时 U 可以用要求仲裁方(可信第三方) 进行仲裁的方法来抵抗这种攻击。具体过程为:

当 U 发现有人伪造自己的签名时,可以向仲裁方提出仲裁要求,同时向他提供证据证明这个签名是 *CA* 伪造的。U 将自己的身份、证书、公钥、伪造的签名发送给仲裁方。仲裁方先计算 $R_U = H_1(ID_U,PK_U,PK_C,P_U)$,验证 $g^{T_A} = P_A \cdot (PK_C)^{R_A} \bmod p$ 是否成立,再验证伪造的盲签名是否有效。若都成立,而验证签名时用的证书、公钥与 U 的证书、公钥并不相同,仲裁者可据此判定是 CA 实行了公钥替换攻击。这是因为,某一身份的公钥和证书应该只有 1 对,但现在有 2 对不同的同样合法有效的证书和公钥,说明或者 CA 伪造了 U 的签名,或者 CA 已被攻破, S_C 已泄露。

因此,方案能抵抗公钥替换攻击。证毕。

定理6 方案在适应性选择消息和身份攻击下,能够抵抗用户伪造攻击、CA伪造攻击和公钥替换攻击。方案是强安全的。

证明:由定理3、4、5,易证得定理6。

4 效率分析

同等安全级别下,对运算的复杂度和计算量远远高于模幂运算和其他运算。据统计,一个对运算大约相当于8个有限域上模幂运算的计算量。

表1比较了本文方案和其他4种方案的计算量和性能。为简单起见,表中只统计了对运算和指数运算,其他运算如G_1上的标量乘,Z_p或Z_q中的模乘等和它们相比,计算量可忽略不计。

采用以下标记:

P:双线性对运算;

H:Hash操作;

E:有限域上的模幂运算;

$|G_1|$或$|Z_p|$:G_1或Z_p中元素的二进制位数。

表1 几种基于证书签名方案的计算量和性能比对

Tab.1 Comparison of certificate-based signature schemes

	签名阶段计算量	验证阶段计算量	总计算量	公钥长度	签名长度	CA-用户通信量	证书-公钥的双向认证
Liu的第2方案[4]	6E+2H	6P+3E+2H	6P+9E+4H	$2\|G_1\|$	$3\|G_1\|$	$4\|G_1\|+\|ID\|$	无
Zhang方案[5]	5E+2H	3P+3E+3H	3P+8E+5H	$2\|G_1\|$	$2\|G_1\|$	$3\|G_1\|+\|ID\|$	无
Li方案[8]	E+H	P+E+2H	P+2E+3H	$2\|G_1\|$	$\|G_1\|$	$3\|G_1\|+\|ID\|$	有
Li方案[10]	2P+1H	2P+1H	4P+2H	$\|G_1\|$	$\|G_1\|$	$4\|G_1\|+2\|ID\|$	无
本文方案	5E+2H	4E+2H	9E+4H	$\|Z_p\|$	$\|Z_q\|+\|Z_p\|$	$2\|Z_p\|+\|Z_q\|+\|ID\|$	有

由表1可知,综合来看,本文方案在计算量及公钥长度、签名长度、通信量、证书-公钥的双向认证等性能上优于其他方案。

5 总 结

针对不含双线性对的基于证书盲签名展开研究,提出了1种不含对运算的基于证书盲签名方案,并基于离散对数难题和分叉引理,证明了方案的强盲性和在随机预言机模型下的安全性:可抵抗用户伪造攻击、CA伪造攻击和公钥替换攻击。相比于其他基于证书签名方案,本文方案具有以下优势:1)以有限域上模幂运算为主构造,不含对运算,因此具有明显的效率优势。2)采用二元仿射变换盲化消息,计算量小,效率高。3)方案具有强安全性。4)公钥和证书的不可替换性基于离散对数难题和Hash函数的抗强碰撞性,由证书-公钥双向验证方程保证和实现。5)效率分析表明,与同类方案相比,本方案具有签名长度短,计算量和通信量小的优点,尤其适用于计算能力和带宽受限的领域,如智能卡、无线传感器、移动通信等。

参考文献:

[1] Gentry C. Certificate-based encryption and the certificate revocation problem[C]//Proceedings of the Eurocrypt'03. Berlin:Springer-Verlag,2003,LNCS 2656:272-293.

[2] Kang B G,Park J H,Hahn S G. A certificate-based signature scheme[C]//Proceedings of the CT-RSA 2004. Berlin:Springer-Verlag,2004,LNCS 2964:99-111.

[3] Li Jiguo,Huang Xinyi,Mu Yi,et al. Certificate-based signature:Security model and efficient construction[C]//Proceedings of the EuroPKI 2007. Berlin:Springer-Verlag,2007,LNCS 4582:110-125.

[4] Liu J K,Baek J,Susilo W,et al. Certificate-based signature scheme without pairings or random oracles[C]//Proceedings of the ISC 2008. Berlin:Springer-Verlag,2008,LNCS 5222:285-297.

[5] Zhang Jianhong. On the security of a certificate-based signature scheme and its improvement with pairings[C]//Proceedings of the ISPEC 2009. Berlin:Springer-Verlag,2009,LNCS 5451:47-58.

[6] Wu Wei,Mu Yi,Susilo W,et al. Certificate-based signatures:new definitions and a generic construction from certificateless signatures[C]//Proceedings of the WISA 2008. Berlin:Springer-Verlag,2009,LNCS 5379:99-114.

[7] Li Jiguo,Xu Lizhong,Zhang Yichen. Provably secure certificate-based proxy signature schemes[J]. Journal of Computers,2009,4(6):444-452.

[8] Li Jiguo,Huang Xinyi,Zhang Yichen,et al. An efficient short certificate-based signature scheme[J]. Journal of Systems and Software,2012,85(2):314-322.

[9] Wu Wei,Mu Yi,Susilo W,et al. A provably secure construction of Certificate-based encryption from certificateless encryption[J]. The Computer Journal,2012,55(10):1157-1168.

[10] Li Jiguo,Qian Na,Huang Xinyi,et al. Certificate-based strong designated verifier signature scheme[J]. Chinese Journal of Computers,2012,35(8):1579-1587.[李继国,钱娜,黄欣沂,等.基于证书强指定验证者签名方案[J].计算机学报,2012,35(8):1579-1587.]

(编辑 杨 蓓)