高效不含双线性对的基于证书签名方案*

周 萍[1,2], 何大可[1]
(1. 西南交通大学 信息科学与技术学院, 成都 610031; 2. 四川城市职业学院 信息工程系, 成都 610101)

摘 要: 目前大多数基于证书密码体制的数字签名方案都使用双线性对构造,计算开销较大、计算效率低,因此有必要研究更安全、更高效的基于证书签名方案。基于离散对数难题和分叉引理,提出了一个不含双线性对运算的基于证书数字签名方案,并在随机预言模型下证明了方案的安全性,分析了方案的效率。分析表明,方案可以抵抗用户伪造攻击和 CA 伪造攻击,抵抗公钥替换攻击,并且计算效率较高,适合应用于移动通信等计算能力和带宽受限的领域。

关键词: 基于证书签名; 随机预言模型; 离散对数难题; 双线性对
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2013)05-1504-04
doi:10.3969/j.issn.1001-3695.2013.05.057

Efficient certificate-based signature scheme without pairings

ZHOU Ping[1,2], HE Da-ke[1]
(1. *College of Information Science & Technology, Southwest Jiaotong University, Chengdu* 610031, *China*; 2. *Dept. of Information Engineering, Urban Vocational College of Sichuan, Chengdu* 610101, *China*)

Abstract: There are pairing operations in most current certificate-based signature schemes, so the efficiencies of those schemes are low. It is necessary to research certificate-based signature schemes with higher security and higher efficiency. Based on discrete logarithm problem and the forking lemma, this paper presented a certificate-based signature scheme without pairings, which efficiency had been analyzed, and it proved security under the random oracle model. Analysis show that the scheme is existentially unforgeable against user attack and CA attack, against public key replacing attack. Because of its efficiency, it can be used in the computation power and bandwidth limited environment.

Key words: certificate-based signature; random oracle model; discrete logarithm problem; bilinear pairing

0 引言

数字签名是信息安全领域最基本最重要的概念之一,是指消息的发送者通过某种签名算法产生一段别人无法伪造的签名,然后将该签名和消息绑定在一起发送给消息接收者;消息接收者或其他任何消息验证者能够根据数字签名验证消息确实是由签名者签署的,而且是未被修改的、完整的;但是除了签名者外其他任何人伪造该签名者的数字签名却是困难的。因此,数字签名是一种实现数字通信过程中可认证性、数据完整性和不可否认性的技术,是应用最广泛的信息安全技术之一。

数字签名首先被应用于公钥基础设施中公钥证书的认证,公钥证书由可信第三方采用数字签名技术绑定用户身份和其公钥信息。同时,数字签名还被广泛应用于电子商务、电子政务、电子货币、网络通信、访问控制、软件验证以及其他许多重要领域。比如由于数字签名具有身份鉴别、数据验证和不可否认的功能,可被用于数字版权保护中,作为版权拥有者的版权声明和验证。又比如,为了平衡网络负载,一个主服务器会多级授权给多个其他服务器提供下载服务,终端用户怎样验证下载的消息确是主服务器授权给其他服务器且没有被网络攻击者所窜改了的? 这时就可以采用一种特殊的数字签名——传递签名,解决服务器多级授权的安全验证问题。

在传统公钥密码体制中,用户的公钥与其身份之间的绑定关系是通过公钥证书来实现的,而公钥证书的签发、存储、更新、撤销等都是由可信赖的第三方——认证中心(certificate authority,CA)来完成。公钥证书的管理需要很大的计算量和很强的存储能力。为此,Shamir 在 1984 年提出了基于身份的密码学思想,即用户的公钥直接从其唯一身份信息(如 IP 地址、e-mail 地址)中得到,而用户的私钥由一个可信赖的第三方——私钥生成中心(private key generator,PKG)生成。但是这种基于身份的密码体制有一个不可避免的缺陷——密钥托管问题,即 PKG 知道所有人的私钥,PKG 也就有能力伪造系统内任何人的签名,或解密发给系统内任何人的消息。

为克服这两种密码体制的缺点,在 2003 年的欧密会上,Gentry[1] 提出了基于证书密码体制(certificate-based cryptographic primitives,CBC)。在该体制中,用户生成自己的私钥和公钥,然后把自己的公钥和身份信息发送给 CA,CA 在验证用户信息的真实性后,用自己的系统主密钥签名,生成用户证书并发送给用户。用户把自己的私钥和证书的某种组合作为签名密钥或解密密钥,而用户的公钥、身份信息和 CA 的公钥作为该用户的签名验证密钥或加密密钥。CBC 与传统公钥密码体制的主要区别是,用户证书不仅具有传统 PKI 证书的所有功能,而且还可以用来构造签名密钥或解密密钥。而与基于身份公钥密码体制相比,由于 CA 不知道用户的私钥,所以彻底解

收稿日期: 2012-08-23; **修回日期**: 2012-10-08 **基金项目**: 成都市 2007 年科技攻关项目(07GGYB050GX-010)

作者简介: 周萍(1968-),女,湖北宜都人,副教授,博士研究生,主要研究方向为信息安全、密码学(963647440@qq.com);何大可(1944-),男,教授,博导,主要研究方向为密码学、信息安全、并行计算.

决了基于身份密码体制中的密钥托管问题。另外,用户证书只是为了证明用户公钥的真实性以及与身份的唯一对应关系,不需要保密,因此克服了基于身份密码体制中 PKG 与用户之间的密钥传递需要安全信道问题。而与无证书公钥密码体制相比,由于证书的存在,避免了无证书公钥密码体制容易遭受公钥替换攻击问题以及 PKG 与用户之间的密钥传递需要安全信道问题。

目前对基于证书密码体制的研究还处于起步阶段,取得的研究成果主要集中在基于证书加密方面,而基于证书签名方面还比较少。2004 年,Kang 等人[2]提出了一种基于证书签名方案,并在随机预言模型下证明了其安全性。2007 年,Li 等人[3]把密钥替换攻击引入到基于证书密码体制中,指出 Kang 的方案不能抵抗密钥替换攻击,同时提出了一个新的基于证书签名方案。为了进一步提高基于证书签名方案的效率,Liu 等人[4]于 2008 年提出两个新型的基于证书签名方案,一个不使用双线性对,另一个在标准模型下证明了方案的安全性。Wu 等人[5]于 2009 年提出了一个更加精确和合理的基于证书签名的安全定义,同时提出了一个从任意安全的无证书签名方案构造基于证书签名方案的一般方法。此外还有一些研究成果[6,7],在此不再赘述。但这些方案绝大多数都是基于双线性对的,计算开销较大。因此,构造高效的、具有强安全性的、不使用双线性对的基于证书签名方案是亟待解决的问题之一。

1　基于证书数字签名方案的相关定义

1.1　基于证书数字签名方案

定义 1　一个基于证书数字签名方案通常由以下几个算法组成[5,6]:

a)系统建立算法(setup)。输入系统安全参数 1^k,由 CA 生成系统参数 params 和主密钥 S_C,params 可以公开,S_C 由 CA 秘密保存。

b)用户密钥生成算法(keyGen)。输入系统参数 params 和用户身份 ID,由用户生成自己的私钥 S 和公钥 PK。

c)证书生成算法(certGen)。输入系统参数 params、主密钥 S_C,用户身份 ID、用户公钥 PK、由 CA 生成用户证书 cert。

d)签名算法(sign)。输入系统参数 params、用户私钥 S、用户证书 cert、待签署消息 m,由用户生成 m 的签名 σ。

e)签名验证算法(verify)。输入系统参数 params、用户公钥 PK、用户身份 ID、消息 m 和 m 的签名 σ,输出 invalid 或 valid。

1.2　基于证书数字签名方案的安全性定义

一般地,基于证书签名方案存在两类攻击者,即用户攻击和 CA 攻击。用户攻击是指攻击者知道用户的私钥但不知道与该公钥(该公钥与用户私钥相对应)对应的证书,CA 攻击是指攻击者知道主密钥 S_C,可以生成用户的证书,但不知道用户的私钥。记前一种攻击者为 A_1,后一种攻击者为 A_2。

定义 2　如果不存在攻击者 A_1,通过借助挑战者 B,能够在多项式时间内以不可忽略的概率赢得下面的游戏,则称一种基于证书数字签名方案可以抵抗用户伪造攻击[5,6]。

Game1　攻击者 A_1 和挑战者 B 共同进行下面的游戏:

a)Setup。B 根据安全参数 1^k,运行系统建立算法 setup,生成系统参数 params 和主密钥 S_C。B 将 params 发送给 A_1,自己秘密保存 S_C。

b)Query。A_1 可以向 B 提交一系列查询,查询次数由 A_1 决定,为多项式次,查询方式为自适应选择查询方式。

(a)UserKeyGen 查询。A_1 可以询问任意用户 U 的公私钥对,A_1 输入 ID,B 返回公私钥对$(PK_{\mathrm{ID}}, S_{\mathrm{ID}})$。

(b)ReplacePublicKey 查询。A_1 可以用任意公钥替换任意指定用户 U 的公钥,A_1 输入$(\mathrm{ID}, PK'_{\mathrm{ID}})$,$B$ 用 PK'_{ID}替换用户 U 原来的公钥。

(c)CertGen 查询。A_1 可以询问任意用户 U 的证书,A_1 输入$(\mathrm{ID}, PK_{\mathrm{ID}})$,$B$ 返回 U 的证书 $\mathrm{cert}_{\mathrm{ID}}$。

(d)Hash 查询。针对方案中用到的 hash 函数,A_1 可以询问任意输入的 hash 函数值,B 返回所对应的 hash 值。

(e)Sign 查询。A_1 可以向 B 询问任意用户 U 对任意消息 m 的签名,A_1 输入(ID, m),B 返回对应的签名 σ。

c)Forge。在经过上述的自适应方式多项式次查询后,A_1 输出伪造的用户(身份信息为 ID^*,公钥为 PK_{ID^*})对消息 m^* 的签名 σ^*,满足条件:$(\mathrm{ID}^*, PK_{\mathrm{ID}^*})$没有做过 certGen 查询,$\mathrm{ID}^*$ 没有做过 replacePublicKey 查询,(ID^*, m^*)没有做过 sign 查询。

如果伪造的签名 σ^* 可以通过方案的签名验证算法 verify,则称 A_1 赢得游戏 Game1。

定义 3　如果不存在攻击者 A_2,通过借助挑战者 B,能够在多项式时间内以不可忽略的概率赢得下面的游戏,则称一种基于证书数字签名方案可以抵抗 CA 伪造攻击[5,6]。

Game2　攻击者 A_2 和挑战者 B 共同进行下面的游戏:

a)Setup。B 根据安全参数 1^k,运行系统建立算法 setup,生成系统参数 params 和主密钥 S_C。B 将 params 和 S_C 发送给 A_2。

b)Query。A_2 可以向 B 提交一系列查询,查询次数由 A_2 决定,为多项式次,查询方式为自适应选择查询方式。

(a)UserKeyGen 查询。A_2 可以询问任意用户 U 的公钥。A_2 输入 ID,B 返回 U 的公钥 PK_{ID} 给 A_2,秘密保存 U 的私钥 S_{ID}。

(b)PrivateKey 查询。A_2 可以询问任意用户 U 的和公钥相对应的私钥,A_2 输入$(\mathrm{ID}, PK_{\mathrm{ID}})$,$B$ 验证 PK_{ID}是否是 userKeyGen 查询的输出,如是返回对应的私钥 S_{ID}给 A_2,否则返回 invalid。

(c)ReplacePublicKey 查询。A_2 可以用任意公钥替换任意指定用户 U 的公钥,A_2 输入$(\mathrm{ID}, PK'_{\mathrm{ID}})$,$B$ 用 PK'_{ID}替换用户 U 原来的公钥。

(d)Hash 查询。针对方案中用到的 hash 函数,A_2 可以询问任意输入的 hash 函数值,B 返回所对应的 hash 值。

(e)Sign 查询。A_2 可以向 B 询问任意用户 U 对任意消息 m 的签名,A_2 输入(ID, m),B 返回对应的签名 σ。

c)Forge。在经过上述的自适应方式多项式次查询后,A_2 输出伪造的用户(身份信息为 ID^*,公钥为 PK_{ID^*})对消息 m^* 的签名 σ^*,满足条件:$(\mathrm{ID}^*, PK_{\mathrm{ID}^*})$没有做过 privateKey 查询,$\mathrm{ID}^*$ 没有被做过 replacePublicKey 查询,且(ID^*, m^*)没有做过 sign 查询。

如果伪造的$(\mathrm{ID}^*, PK_{\mathrm{ID}^*}, m^*)$的签名 σ^* 可以通过签名验证算法 verify,则称 A_2 赢得游戏 Game2。

游戏 Game1 中,A_1 可以查询任意用户的公私钥对,可以替换任意用户的公钥,但不知道主密钥,不知道欲伪造用户 ID^* 的证书 $\mathrm{cert}_{\mathrm{ID}^*}$。如果不存在攻击者 A_1 能够在多项式时间内以

不可忽略的概率赢得游戏 Game1,说明签名方案不仅可以抵抗用户伪造攻击,也可以抵抗替换公钥攻击。这里 A_1 模拟的是除 CA 以外的攻击者。

游戏 Game2 中,A_2 知道主密钥,可以生成任意用户的证书,但不知道欲伪造用户 ID^* 的私钥 S_{ID*}。如果不存在攻击者 A_2 能够在多项式时间内以不可忽略的概率赢得游戏,说明签名方案可以抵抗 CA 伪造攻击。这里 A_2 所做攻击模拟的是恶意 CA 所进行的伪造攻击。

定义 4 如果一个基于证书签名方案在自适应选择消息和身份攻击、公钥替换攻击下,可以抵抗用户伪造攻击和 CA 伪造攻击,则称该方案是安全的。

1.3 离散对数难题和分叉引理

设 p、q 是两个大素数且 $q|(p-1)$,随机选择 Z_p^* 的一个阶为 q 的生成元 g,由 g 生成的子群记为 G。假设以下的离散对数问题 DLP 是难解的。

定义 5 设 p、q、g 如上定义,是已知的。已知 $\beta \in G$,求满足 $g^\alpha = \beta \bmod p$ 的 $\alpha \in Z_q^*$。该问题称为离散对数问题 DLP。

引理(分叉引理[8]) 设 A 是一个仅以公开数据作为输入的概率多项式时间图灵机。如果 A 能够以一个不可忽略的概率找到一个有效签名(m,K,h,σ),则以相同参数不同 hash 函数 $h(\cdot)$重放 A,能够找到另一个有效签名(m,K,h',σ'),且 $h \neq h'$。

2 新的基于证书数字签名方案

本章基于离散对数难题,提出一种具有强安全性的不含双线性对运算的基于证书数字签名方案,如下所述:

a)系统建立算法(setup)。按照安全参数 1^k 的要求,CA 随机选择两个大素数 p、q 满足 $q|(p-1)$,再随机选择 Z_p^* 的一个阶为 q 的生成元 g,记由 g 生成的子群为 G。CA 再随机选择私钥 $S_C \in Z_q^*$,计算公钥 $PK_C = g^{S_C} \bmod p \in G$,并选择 hash 函数 $H_1:\{0,1\}^* \times (Z_p^*)^3 \to Z_q^*$,$H_2:\{0,1\}^* \times (Z_p^*)^4 \to Z_q^*$。CA 公布系统参数 params = $\{p,q,g,G,PK_C,H_1,H_2\}$,秘密保存系统主密钥 S_C。

b)用户密钥生成算法(keyGen)。设用户 A 的身份信息为 ID_A,A 随机选择自己的私钥 $S_A \in Z_q^*$,计算公钥 $PK_A = g^{S_A} \bmod p$。

c)证书生成算法(certGen)。用户 A 将自己的身份信息 ID_A 和公钥 PK_A 发送给 CA。CA 收到(ID_A,PK_A)后,首先验证 ID_A 的真实性,如果验证通过,CA 随机选择 $s_0 \in Z_q^*$,计算 $p_0 = g^{s0} \bmod p$,$Y_A = H_1(ID_A,PK_A,PK_C,p_0)$,$cert_A = s_0 + S_C Y_A \pmod q$,将用户证书$(p_0,cert_A)$发送给 A 并秘密删除 s_0。A 收到$(p_0,cert_A)$后,验证其有效性:首先计算 $Y_A = H_1(ID_A,PK_A,PK_C,p_0)$并保存起来,然后验证 $g^{cert_A} = p_0(PK_C)^{Y_A} \bmod p$ 是否成立,如成立则接受此证书,否则要求 CA 重新为自己生成签名证书。这里证书的传递并不需要安全信道。

d)签名算法(sign)。用户 A 按如下步骤对消息 m 签名:A 任意选择随机数 $k \in Z_q^*$,计算 $K = g^k \bmod p$,$h = H_2(m,ID_A,K,PK_A,PK_C,p_0)$,$\sigma = hS_AY_A + k \cdot cert_A \bmod q$,则消息 m 的签名即为(σ, K)。

e)签名验证算法(verify)。任何验证者都可以用 A 的公钥 PK_A、身份 ID_A、证书$(p_0,cert_A)$验证消息 m 的签名(σ, K)的有效性,过程如下:计算 $Y_A = H_1(ID_A,PK_A,PK_C,p_0)$,验证 $g^{cert_A} = p_0(PK_C)^{Y_A} \bmod p$ 是否成立,如果不成立则签名无效验证中断,否则计算 $h = H_2(m,ID_A,K,PK_A,PK_C,p_0)$,验证 $g^\sigma = (PK_A)^{h \cdot Y_A} K^{cert_A} \bmod p$ 是否成立,如果成立,则签名有效输出 valid,否则签名无效输出 invalid。

签名算法的正确性是因为:设用户 A 的身份信息为 ID_A,公私钥对为(PK_A, S_A),证书为$(p_0,cert_A)$,A 对消息 m 的签名为(σ, K)。按签名算法 sign 有:$\sigma = hS_AY_A + k \cdot cert_A \bmod q$,因此:

$$g^\sigma = g^{hS_AY_A + k \cdot cert_A} = (PK_A)^{h \cdot Y_A} K^{cert_A} \bmod p$$

成立。

3 安全性分析

定理 1 对于上述基于证书数字签名方案,在随机预言模型下,如果存在一个攻击者 A_1,能够在多项式时间内以不可忽略的概率 ε 赢得游戏 Game1,则挑战者 B 借助于 A_1 能够在多项式时间内以不可忽略的概率 $O(\varepsilon)$解决 G 上的离散对数难题。

证明 设$\{$已知 $g,\beta = g^\alpha$,求 $\alpha\}$是一个离散对数难题的随机实例,设 A_1 是一个攻击者,能够在多项式时间内以不可忽略的概率 ε 赢得游戏 Game1。下面证明 B 可以借助 A_1 解决该离散对数难题,求出 α。

B 首先运行方案中的系统建立算法 setup,生成系统参数 params = $\{p,q,g,G,PK_C,H_1,H_2\}$ 和主密钥 S_C,其中 $PK_C = g^{S_C} \bmod p$ 是系统主公钥。B 将 params 发送给 A_1,自己秘密保存 S_C。

B 模拟随机预言机服务,A_1 可以向 B 提交一系列查询。为了回答这些查询,避免碰撞,B 维护如下列表:L_0 用来存储 UserKeyGen 查询的结果,L_1、L_2 用来存储 hash 函数 H_1、H_2 的查询结果,L_3 存储 certGen 查询的结果,L_4 存储 sign 查询的结果。设 A_1 最多进行了 q_{UK}次 userKeyGen 询问,B 随机选择 $i^* \in [1, q_{UK}]$,记 $ID^* = ID_{i^*}$,并令 $PK_{ID*} = \beta$,$S_{ID*} = null$(null 表示空),将(ID^*,PK_{ID*},S_{ID*})保存在 L_0 中。

B 与 A_1 进行如下模拟算法:

a)UserKeyGen 查询。A_1 输入 ID_i,进行第 i 次用户密钥查询。(a)如果 $i \neq i^*$,B 检查 L_0 表,若$(ID_i,*,*) \in L_0$,返回与 ID_i 相对应的公私钥(PK_i, S_i),否则任选 $S_i \in Z_q^*$ 且$(*,*,S_i) \notin L_0$,计算 $PK_i = g^{S_i} \bmod p$,将(PK_i, S_i)返回给 A_1,并将(ID_i,PK_i,S_i)保存在 L_0 中。(b)如果 $i = i^*$,则挑战失败,终止游戏。

b)ReplacePublicKey 查询。A_1 进行替换公钥查询,输入$(ID_i,(PK_{ID})'_i)$,B 检查$(ID_i,*,*)$是否属于 L_0,如果属于则用$(PK_{ID})'_i$ 替换用户 U 原来的公钥,同时私钥保持不变,否则将$(ID_i,(PK_{ID})'_i,null)$保存在 L_0 中。

c)CertGen 查询。A_1 输入$(ID_i,(PK_{ID})_i)$进行证书查询。B 检查 L_3 表,如果$(ID_i,(PK_{ID})_i,*) \in L_3$,返回与其相对应的证书$(p_0,cert_{ID})$,否则 B 检查$(ID_i,(PK_{ID})_i,*)$是否属于 L_0。如果属于则随机选择 $s_0, Y_A \in Z_q^*$,计算 $p_0 = g^{s0} \bmod p$,$cert_{ID} = s_0 + S_C Y_A \pmod q$,将$(p_0,cert_{ID})$发送给 A_1,再将$(ID_i,(PK_{ID})_i,(p_0,cert_{ID}))$保存在 L_3 中,将$((ID_i,(PK_{ID})_i,PK_C,p_0),Y_A)$保存在 L_1 中(保存之前先检查$((ID_i,(PK_{ID})_i,PK_C,p_0),*)$是否包含在 L_1 中,如未包含则保存,否则重选 s_0、Y_A 进行上述操作),并秘密删除 s_0。如果$(ID_i,(PK_{ID})_i,*)$不属于 L_0 则输出 invalid。

d)H_1 查询。A_1 询问随机预言机 H_1,A_1 输入任意$(ID_A,PK_A,PK_C,p_0) \in \{0,1\}^* \times (Z_q^*)^3$,$B$ 检查 L_1 表,如果表中已存

在该输入,返回对应的输出,否则任选一个((*,*,*,*),y) $\notin L_1$ 的随机数 $y \in Z_q^*$,将 y 返回给 A_1 同时将((ID$_A$,PK_A,PK_C,p_0),y)保存在 L_1 表中。

e)H_2查询。A_1 询问随机预言机 H_2,A_1 输入任意(m,ID$_A$,K,PK_A,PK_C,p_0) $\in \{0,1\}^* \times (Z_q^*)^4$,$B$ 检查 L_2 表,如果表中已存在该输入,返回对应的输出,否则任选一个((*,*,*,*,*,*),h) $\notin L_2$ 的随机数 $h \in Z_q^*$,将 h 返回给 A_1 同时将((m,ID$_A$,K,PK_A,PK_C,p_0),h)保存在 L_2 表中。

f)Sign 查询。A_1 输入(ID$_i$,m),询问身份为 ID$_i$ 的用户对消息 m 的签名。B 首先检查是否有 ID$_i$ = ID*,如果:

(a)ID$_i \neq$ ID*,且 B 在表 L_0 中找到的对应公私钥(ID$_i$,PK_{ID},S_{ID})满足 $PK_{\mathrm{ID}} = g^{S_{\mathrm{ID}}} \bmod p$(即该公钥未被替换),则 B 首先在 L_3 表中找到对应的证书(p_0,cert$_{\mathrm{ID}}$)在表 L_1 中查到相对应的 Y_A(注:如果该 ID$_i$ 的证书不存在则 B 按 certGen 查询的方法生成证书(p_0,cert$_{\mathrm{ID}}$)并将(ID$_i$,PK_{ID},(p_0,cert$_{\mathrm{ID}}$))保存在表 L_3 中,将((ID$_i$,PK_{ID},PK_C,p_0),Y_A)保存在表 L_1 中),然后 B 任意选择随机数 k,$h \in Z_q^*$,计算 $K = g^k \bmod p$,$\sigma = hS_{\mathrm{ID}}Y_A + k \cdot \mathrm{cert}_{\mathrm{ID}} \bmod q$。检查(($m$,ID$_i$,$K$,$PK_{\mathrm{ID}}$,$PK_C$,$p_0$),*)在表 L_2 中是否出现过,如没有出现就将((m,ID$_i$,K,PK_{ID},PK_C,p_0),h)保存在 L_2 中,否则重选 k,$h \in Z_q^*$ 进行上述计算。B 将(σ, K)返回给 A_1。

(b)如果 ID$_i \neq$ ID* 且 ID$_i$ 所对应的公钥被替换过,或者 ID$_i$ = ID*,此时 B 虽然不知道对应私钥,仍然可以生成(ID$_i$,m)的签名:B 首先从 L_0 中找到与 ID$_i$ 相对应的公钥 PK_{ID},在 L_3 中找到对应的证书(p_0,cert$_{\mathrm{ID}}$),在表 L_1 中查到相对应的 Y_A(注:如果证书和 Y_A 不存在,B 可以重新生成证书与 Y_A,方法同(a)),然后 B 任意选择随机数 h,$\sigma \in Z_q^*$,计算 $c = (\mathrm{cert}_{\mathrm{ID}})^{-1} \bmod q$,$K = [g^{\sigma}(PK_{\mathrm{ID}})^{-h \cdot Y_A}]^c \bmod p$,令 $h = H_2(m, \mathrm{ID}_i, K, PK_{\mathrm{ID}}, PK_C, p_0)$,检查(($m$,ID$_i$,$K$,$PK_{\mathrm{ID}}$,$PK_C$,$p_0$),*)在表 L_2 中是否出现过,如没有出现就将((m,ID$_i$,K,PK_{ID},PK_C,p_0),h)保存在 L_2 中,否则重选 h,$\sigma \in Z_q^*$ 进行上述计算。B 将(σ, K)返回给 A_1。

上述查询过程结束后,A_1 以不可忽略的概率输出一个伪造的可以通过签名验证算法的签名(m,ID,(σ, K))。如果ID$\neq$ID*,则挑战离散对数难题——{已知 g,$\beta = g^{\alpha}$,求 α}——失败,B 放弃;否则,根据分叉引理,B 将上述模拟过程重复进行两次,可以在时间 $T \leqslant 120686QT/\varepsilon$ 内生成两个有效的签名(m,K,h,σ)和(m,K,h',σ'),满足 $h \neq h'$ 且 $\sigma \neq \sigma'$,其中 Q 是 A_1 询问随机预言机的次数,T 是询问签名的次数,ε 是伪造有效签名的概率。记 $Y = H_1(\mathrm{ID}^*, PK_{\mathrm{ID}^*}, PK_C, p_0)$,有 $g^{\sigma} = (PK_{\mathrm{ID}^*})^{h \cdot Y} K^{\mathrm{cert}_{\mathrm{ID}}}$,$g^{\sigma'} = (PK_{\mathrm{ID}^*})^{h' \cdot Y} K^{\mathrm{cert}_{\mathrm{ID}}}$,得 $g^{\sigma - \sigma'} = (PK_{\mathrm{ID}^*})^{(h-h') \cdot Y}$,$\alpha = S_{\mathrm{ID}^*} = (\sigma - \sigma')/((h - h')Y) \bmod q$,解决了离散对数难题 DLP。

下面计算 B 成功解决 DLP 难题的概率。设 A_1 最多进行了 q_{UK}次 userKeyGen 询问,设 A_1 输出有效签名的概率为 ε,则在用户密钥提取询问中,不询问 ID* 的公私钥的概率至少为 $(1 - 1/q_{UK})^{q_{UK}}$,输出有效伪造签名(m,ID,(σ,K))中 ID = ID* 的概率至少为 $1/q_{UK}$,故 B 解决 DLP 难题的概率 $\geqslant \varepsilon \cdot (1 - 1/q_{UK})^{q_{UK}}/q_{UK} = O(\varepsilon)$。因此如果 A_1 能够在多项式时间内以不可忽略的概率 ε 赢得游戏 Game1,B 可以以不低于 $O(\varepsilon)$的概率解决离散对数难题。证毕。

定理 2　对于上述基于证书数字签名方案,在随机预言模型下,如果存在一个攻击者 A_2,能够在多项式时间内以不可忽略的概率 ε 赢得游戏 Game2,则 B 能够在多项式时间内以不可忽略的概率 $O(\varepsilon)$解决 G 上的离散对数难题。

证明过程类似于定理 1 的证明。

下面证明方案可以抵抗公钥替换攻击。

定理 3　上述基于证书数字签名方案可以抵抗公钥替换攻击。

证明　假设有攻击者 A 对用户 U 实施公钥替换攻击,则攻击者 A 可以分为普通攻击者和 CA。

若 A 是普通攻击者,则 A 可以很容易地得到 U 的身份信息 ID$_U$、公钥 PK_U、证书(p_0,cert$_U$),但 A 不知道 U 的签名私钥 S_U,因此不能伪造 U 的签名(定理 1、2 已证明)。若 A 任选 $x \in Z_q^*$,计算 $y = g^x \bmod p(\neq PK_U)$,然后用($y$, x)代替 U 的公私钥对(PK_U, S_U)。对于 U 的证书,此时 A 有两种选择,一种是 A 继续使用 U 的证书(p_0,cert$_U$),另一种是 A 伪造 U 的证书。第一种情况中,由 hash 函数的抗强碰撞性,$Y_U = H_1(\mathrm{ID}_U, PK_U, PK_C, p_0)$,$Y'_U = H_1(\mathrm{ID}_U, y, PK_C, p_0)$,一定有 $Y_U \neq Y'_U$,因此证书验证方程 $g^{\mathrm{cert}_U} = p_0 (PK_C)^{Y'_U} (\bmod p)$ 不成立,签名验证失败。第二种情况中,若 A 伪造 U 的证书,用伪造的证书(p'_0,cert$'_U$)代替 U 的证书,则因为 A 并不知道系统主密钥 S_C,由离散对数难题及 hash 的抗强碰撞性,A 不能伪造出能够通过证书验证方程 $Y'_U = H_1(\mathrm{ID}_U, y, PK_C, p'_0)$,$g^{\mathrm{cert}'_U} = p'_0 (PK_C)^{Y'_U} (\bmod p)$ 的假证书。因此普通攻击者 A 不能对用户 U 实施公钥替换攻击。

若攻击者 A 是认证中心 CA,则与第一种情况不同的是 CA 知道 S_C,因此能够成功伪造用户 U 的公私钥(y, x)和证书(p'_0,cert$'_U$)。这时用户 U 可以用要求仲裁方进行仲裁的方式抵抗 *CA* 的公钥替换攻击。具体过程为:当身份为 ID$_U$ 的用户 U 发现有人伪造自己的签名时,可以向仲裁方要求进行仲裁,他可以向仲裁方提供证据证明这个签名是 *CA* 伪造的。用户将自己的身份信息 ID$_U$、公钥 PK_U、证书(p_0,cert$_U$)发送给仲裁方。仲裁方计算 $Y_U = H_1(\mathrm{ID}_U, PK_U, PK_C, p_0)$,然后验证 $g^{\mathrm{cert}_U} = p_0 (PK_C)^{Y_U} (\bmod p)$是否成立。若成立,则说明 *CA* 或者伪造了身份为 ID$_U$ 的合法用户的签名,或 CA 已被攻破,S_C 已泄露,仲裁者可据此判定是 CA 实行了公钥替换攻击。这是因为身份信息为 ID$_U$ 的公钥 PK_U 和证书(p_0,cert$_U$)应该只有一对,但现在有两对同样合法的不同的公钥和证书,说明 CA 对用户 U 实行了公钥替换攻击。因此,该方案可以抵抗公钥替换攻击。证毕。

由定理 1、2、3 可以得到以下结论:

定理 4　该方案可以抵抗用户伪造攻击和 CA 伪造攻击,抵抗公钥替换攻击,方案是安全的。

4　效率分析

在同等安全级别下,对运算相对于其他运算(如群上的模幂运算)是最耗时的。据文献[9]统计,一个对运算大约相当于 10 个有限域上模幂运算的计算量。设 Pa 表示一次双线性对运算,E 表示一次有限域上模幂运算,Mul 表示一次有限域上乘法运算,M 表示一次形如 aP 的加法群上的标量乘,SM 表示一次形如 aP + bQ 的群上同时标量乘,则本方案与其他基于证书方案相比,结果如表 1 所示。　(下转第 1519 页)

对方案的任何攻击方案都可以转换为近似最大公约数问题的解决方案,若攻击者可以破解本文中的方案,则攻击者可以由 $x_i = pq_i + 4r_i (1 \leqslant i \leqslant \tau)$ 求出 p,而实际上最大公约数问题到目前为止是不能被解决的,所以,本文方案是安全的。

在压缩的方案中,需要在公钥中添加对私钥的暗示 y,这引入了另外一个安全假设:稀疏子集和难题(sparse subset sum problem,SSSP)。在 server-aided cryptography[13] 加密方案中,给出了稀疏子集和难题的详细介绍。对于本文中的方案,只要让 θ 足够大,就可以避免对 SSSP 的暴力攻击。

4　结束语

本文在 Dijk 等人方案的基础上,将模 2 运算变为模 4 运算,从而得到了一种整数上的仅使用简单代数运算的全同态加密方案;并且本文使用了 Jean-Sebastien 等人的思想[11] 降低了方案的公钥尺寸。方案一次可以加密 2 bit 的明文,因此比 Dijk 等人的方案具有更高的效率和更短的公钥尺寸。方案的安全性基于近似最大公约数问题和稀疏子集和问题。

参考文献:

[1] RIVEST R, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM,1978,21(2):120-126.

[2] RIVEST R, SHAMIR A, DERTOUZOS M. On data banks and pri-vacy homomorphisms [J]. Foundations of Secure Computation, 1978,7(1):169-177.

[3] BONEH D, GENTR Y. A fully homomorphic encryption scheme [D]. Stanford:Stanford University,2009.

[4] GENTR Y. Fully homomorphic encryption using ideal lattices[C]// Proc of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM Press,2009:169-178.

[5] Van DIJK, GENTR Y, HALEV I,*et al*. Fully homomorphic encryption over the integers[C]//Proc of the 29th Annual International Conference on Theory and Applications of Cryptograhic Techniques. Berlin:Springer-Verlag,2010:24-43.

[6] GENTRY C. Computing arbitrary function of encryped data[J]. Communications of the ACM,2010,53(3):97-105.

[7] SMART N P,VERCAUTEREN F. Fully homomorphic encryption with relatively small key and ciphertext sizes[C]//Proc of the 13th International Conference on Practice and Theory in Public Key Cryptography. Berlin:Springer-Verlag,2010:420-443.

[8] STEHLE D, STEINFELD R. Faster fully homomorphic encryption [C]//Proc of International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2010: 377-394.

[9] 汤殿华,祝世雄,曹云飞. 一个较快速的整数上的全同态加密方案[J]. 计算机工程与应用,2012,48(28):117-122.

[10] 汤殿华,祝世雄,曹云飞. 整数上的全同态加密方案的重加密技术[J]. 信息安全与通信保密,2012,2012(1):76-79.

[11] JEAN-SEBASTIEN C, MANDAL A, NACACHE D, *et al*. Fully-homomorphic encryption over the integers with shorter public-keys [C]//Proc of the 31st Annual Conference on Advances in CRYPTOLOGY. Berlin:Springer-Verlag,2011:487-504.

[12] KARP R M, RAMACHANDRAN V. A survey of parallel algorithms for shared-memory machines,CSD-88-408[R]. [S. l.]:UC Berkeley,1988.

[13] NGUYEN P Q, STERN J. Adapting density attacks to low weight knapsacks[C]//Proc of Asiacrypt'05. Heidelberg: Springer-Verlag, 2005:41-58.

(上接第 1507 页)

表 1　三个基于证书签名方案的计算量比较

比较项	文献[3]方案	文献[7]方案	本文方案
签名阶段	1M + 2SM	1E + 1M	3Mul
验证阶段	3Pa	3Pa + 1E + 2M	2Mul + 5E
总计算量	3Pa + 1M + 2SM	3Pa + 2E + 3M	5Mul + 5E

由表 1 可知,由于对运算的复杂度和计算量远远高于模幂运算和其他运算,本文方案在计算效率方面明显高于其他含有对运算的基于证书签名方案。同时本方案中签名长度仅为 $\mathrm{bit}(q) + \mathrm{bit}(p)$($\mathrm{bit}(x)$ 表示 x 的二进制位数)。由于计算量小,计算效率高,证书的传递不需要安全信道,CA 和用户之间传递的数据量很少(具体见方案),且签名的长度很短是固定值,因此本文方案特别适用于移动通信等计算能力和带宽受限的应用领域。具体如何将本文方案应用于移动应用环境及其他领域,限于篇幅,这里就不详细分析了。

5　结束语

本文围绕着基于证书签名方案展开研究,提出了一个基于证书的、强安全的、不含对运算的签名方案,证明了方案在随机预言机模型下可以抵抗适应性选择消息和身份攻击,抵抗公钥替换攻击和 CA 攻击,并进行了效率分析。目前对基于证书数字签名方案的研究还很少,特别是具有特殊性质的基于证书签名及标准模型下可证安全的基于证书签名等。对这些内容的研究具有重要意义,也是下一步研究的方向。

参考文献:

[1] GENTRY C. Certificate-based encryption and the certificate revocation problem[C]//Lecture Notes in Computer Science, vol2656. Berlin: Springer-Verlag,2003:272-293.

[2] KANG B G, PARK J H, HAHN S G. A certificate-based signature scheme[C]//Lecture Notes in Computer Science, vol2964. Berlin: Springer-Verlag,2004:99-111.

[3] LI Ji-guo, HUANG Xin-yi, MU Yi, *et al*. Certificate-based signature: security model and efficient construction[C]//Lecture Notes in Computer Science, vol4582. Berlin: Springer-Verlag, 2007: 110-125.

[4] LIU J K, BAEK J, SUSILO W, *et al*. Certificate-based signature scheme without pairings and random oracles[C]//Lecture Notes in Computer Science, vol5222. Berlin: Springer-Verlag, 2008: 285-297.

[5] WU W, MU Y, SUSILO W. Certificate-based signatures: new definitions and a generic construction from certificateless signatures[C]// Lecture Notes in Computer Science,vol5379. Berlin: Springer-Verlag, 2009: 99-114.

[6] 李志敏,徐馨,李存华. 高效的基于证书数字签名设计方案[J]. 计算机应用研究,2012,29(4):1430-1433,1444.

[7] 王雯娟,黄振杰,郝艳华. 一个高效的基于证书数字签名方案[J]. 计算机工程与应用,2011,47(6):89-92.

[8] POINTCHEVAL D, STERN J. Security proofs for signatures schemes [C]//Advances in Cryptology-Eurocrypt. Berlin: Springer-Verlag, 1996:387-398.

[9] KAWAHARA Y, TAKAGI T, OKAMOTO E. Efficient imple mentation of tate pairing on a mobile phone using java[C]//Lecture Notes in Computer Science, vol4456. Berlin: Springer-Verlag, 2007: 396-405.