高效的基于证书数字签名设计方案*

李志敏, 徐 馨, 李存华
(淮海工学院 计算机工程学院, 江苏 连云港 222005)

摘 要: 基于证书加密结合了传统公钥密码加密和基于身份加密的优点,并克服了这两类加密体制中存在的问题。在计算性 Diffie-Hellman 问题困难的假设下,利用双线性对,构造了一个基于证书的数字签名方案,并在随机预言模型下证明了方案的安全性。方案设计简单,签名算法中不需要双线性对运算,仅在签名验证算法中存在一个双线性对运算,非常适合使用在计算能力和带宽受限的环境。

关键词: 数字签名; 基于证书; 可证明安全; 双线性对; 随机预言模型
中图分类号: TP309.7 **文献标志码**: A **文章编号**: 1001-3695(2012)04-1430-04
doi:10.3969/j.issn.1001-3695.2012.04.064

Design of efficient certificate-based signature

LI Zhi-min, XU Xin, LI Cun-hua
(*School of Computer Engineering, Huaihai Institute of Technology, Lianyungang Jiangsu* 222005, *China*)

Abstract: Certificate-based encryption combines public key encryption and identity-based encryption while it preserves their features. Based on computational Diffie-Hellman assumption, using bilinear pairing, this paper constructed a new certificate-based signature scheme. The security of the scheme had been proved under the random oracle model. The scheme was efficient to be used in the power and bandwidth limited environment, since its signing algorithm did not need the computation of the bilinear pairing and the verification algorithm needs that computation only once.

Key words: signature; certificate-based; provably secure; bilinear pairings; random oracle model

0 引言

传统公钥密码学(public key cryptography, PKC)模式中,用户使用的公钥仅是一串随机数字,用户需要使用一个可信第三方,称之为认证中心(certificate authority, CA)颁发的证书和公钥绑定来证明自己的身份。在 PKC 中,如果用户收到其他用户发送的签名,他必须经过两次验证才能判断签名的有效性,首先需要获得签名者的证书,在验证证书的合法性后再使用相应的公钥验证签名。因此签名算法效率不高,且当用户过多时,证书管理也是一个棘手的问题。

基于身份密码学(identity-based cryptography, IBC)通过使用能够代表用户身份的字符串(如 e-mail 地址)作为用户的公钥来解决传统公钥密码学中存在的签名验证效率不高以及证书管理问题。在 IBC 中,用户的私钥是利用用户的公钥和一个可信第三方(私钥生成中心,private key generator, PKG)的主密钥生成的。在 IBC 中,用户收到其他用户发送的签名后不需要再认证签名者的公钥,因此可提高签名验证的效率;由于不需要证书,因此也不存在证书管理问题。但 IBC 模式最大的缺点是必须对 PKG 无条件信任。由于所有用户的私钥都是由 PKG 生成的,PKG 可以伪装成任意用户,并且可以解密任意密文。因此 IBC 仅适用于小型组织或系统,如一个单位或部门。

Gentry[1] 于 2003 年首次提出基于证书密码学(certificate-based cryptography, CBC)的概念,它结合了 PKC 和 IBC 的优点,并克服了 PKC 中存在的证书管理问题以及 IBC 中存在的密钥托管问题。在 CBC 中,用户生成自己的公钥和私钥,CA 利用用户的身份和公钥生成证书,该证书将与用户的私钥共同组成用户的解密密钥(签名密钥)。此时尽管 CA 知道证书,但它并没有用户的私钥,因此不能解密任何密文或者伪造成用户进行签名。用户收到其他用户发送的签名后也不需要认证签名者的公钥。目前,基于证书签名的研究成果还很少,Kang 等人[2] 于 2004 年首次给出了基于证书签名的安全定义,给出了两个签名方案,并指出其中一个方案存在替换公钥攻击。2007 年,Li 等人[3] 认为该替换公钥攻击是不可克服的,并认同 Kang 等人的观点,通过附加一个关于私钥的知识签名(signature of knowledge)来防止替换公钥攻击,但这会降低算法的效率;此外文献[3]提出了一个效率相比于文献[2]更高的基于证书签名方案。上述基于证书签名方案都是基于双线性映射,并在随机预言模型下证明了它们的安全性。2008 年,Liu 等人[4] 提出了两个基于证书签名方案,一个不使用双线性映射,另一个则是利用标准模型证明的安全性。王雯娟等人[5] 也于最近提出了一个基于证书签名方案,该方案仅在签名密钥生成阶段和签名验证阶段各使用了一个双线性运算,运算效率较高,并在随机预言模型下证明了它的安全性。

本文提出了一个新的基于证书数字签名方案,在基于计算

收稿日期: 2011-09-12; **修回日期**: 2011-10-18 **基金项目**: 江苏省自然科学基金资助项目(BK20082140);淮海工学院引进人才科研启动基金资助项目(KQ10121);淮海工学院校内课题(KX10530)

作者简介: 李志敏(1981-),女,辽宁沈阳人,博士,主要研究方向为密码学、信息安全、网络安全(lizhimin1981@gmail.com);徐馨(1976-),女,江苏连云港人,讲师,硕士,主要研究方向为信息安全、网络安全、算法分析等;李存华(1963-),男,江苏徐州人,教授,博士,主要研究方向为数据库理论与系统、数据挖掘、模式识别等.

Diffie-Hellman 问题困难的假设下,利用随机预言模型给出了方案的安全证明。该方案在签名生成算法中不需要双线性对运算,在签名验证算法中也仅需要一个双线性对运算,因此运算效率非常高,适用于计算能力受限的设备,如智能卡、PDA、无线传感器等。

1　预备知识

1.1　基于证书数字签名方案的标准模式

基于证书数字签名方案通常由以下五种算法组成:

a)参数生成算法。给定安全参数 1^κ,CA 生成主密钥 s 和公开参数 params,其中 params 是公开的,s 由 CA 秘密保存。本算法简记为 Setup。

b)密钥生成算法。用户使用自己的身份 ID(可以是任意字符串)和公开参数 params,生成用户自己的公钥 PK_{ID}、私钥 K_{ID}。本算法简记为 KeyGen。

c)证书生成算法。CA 利用本算法使用主密钥 s、公开参数 params,对用户身份 ID 和公钥 PK_{ID} 进行认证,生成证书 $Cert_{ID}$。本算法简记为 CertGen。

d)签名生成算法。用户利用本算法使用自己的私钥 K_{ID}、证书 $Cert_{ID}$、公开参数 params,对消息 m 进行签名得到 σ。本算法简记为 Sign。

e)签名验证算法。输入系统公开参数 params,用户的公钥 PK_{ID}、身份 ID、消息 m、签名 σ。如果 σ 是一个真实有效的关于 m 的签名值,算法输出"Valid";否则输出"Invalid"。本算法简记为 Verify。

1.2　形式化的安全定义

基于证书的数字签名方案存在两类潜在伪造攻击者,即用户伪造和 CA 伪造。用户伪造是指攻击者 A 知道用户的私钥,但不知道 CA 颁发给用户的证书值;CA 伪造是指攻击者 A 知道系统主密钥,可以生成用户的证书,但不知道用户的私钥。

定义 1　称一个基于证书的签名方案能够抵抗用户伪造,如果不存在攻击者能够在多项式时间内以不可忽略的优势赢得下面的游戏。

Game1:攻击者 A 和应答者 C 共同参与下面的游戏:

a)参数生成。应答者 C 选择安全参数 1^k 运行参数生成算法得到公开参数 params 以及主密钥 s。C 将参数 params 发送给 A。

b)查询阶段。攻击者 A 向 C 提交一系列查询,查询次数为多项式次数,方式为自适应查询,即下一次查询的内容可依赖于上一次查询的结果。可进行的查询内容如下:

(a)密钥查询。A 选择身份 ID 向 C 进行查询,C 计算 $\text{userKeyGen}(\text{ID}) = (K_{ID}, PK_{ID})$,并将$(K_{ID}, PK_{ID})$发送给 A。

(b)密钥替换。A 可任意替换用户的公、私钥,A 提交 $(\text{ID}, K_{ID}, PK_{ID})$,$C$ 验证 PK_{ID}是否是 K_{ID}对应的公钥。如果是,C 用该公、私钥替换用户原来的公、私钥;否则,C 输出"Invalid",表示 A 是无效操作。

(c)哈希值查询。A 可以对签名算法中使用的哈希函数进行查询,C 返回相应的哈希函数查询值。

(d)证书查询。A 选择 ID,PK_{ID} 向 C 进行查询,C 计算 $\text{certGen}(\text{ID}, PK_{ID}) = Cert_{ID}$,并将 $Cert_{ID}$发送给 A。

(e)签名查询。A 可询问任意用户关于任意消息 m 的签名,C 调用算法 Sign 得到 σ,并将 σ 发送给 A。

c)伪造。由攻击者 A 来决定查询阶段何时结束,当结束后,A 向 C 提交(m, σ, ID),其中 A 不可以在查询阶段查询 ID 对应的证书,也不允许查询 $\text{sign}(m,\text{ID})$来获得 m 对应的签名 σ。

如果 σ 确实是身份为 ID 的用户对 m 的有效签名,A 赢得游戏。A 在游戏中的优势 $\text{adv}(A)$即为 A 赢得游戏的概率。

定义 2　称一个基于证书的签名方案能够抵抗 CA 伪造,如果不存在攻击者能够在多项式时间内以不可忽略的优势赢得下面的游戏。

Game2:攻击者 A 和应答者 C 共同参与下面的游戏:

a)参数生成。应答者 C 选择安全参数 1^k 运行参数生成算法得到公开参数 params 以及主密钥 s。C 将参数 params 和主密钥 s 发送给 A。

b)查询阶段。攻击者 A 向 C 提交一系列查询,查询次数为多项式次数,方式为自适应查询,即下一次查询的内容可依赖于上一次查询的结果。可进行的查询内容如下:

(a)公钥查询。A 选择身份 ID 向 C 进行查询,C 计算 $\text{userKeyGen}(\text{ID}) = (K_{ID}, PK_{ID})$,并将 PK_{ID}发送给 A。

(b)私钥查询。A 选择(ID, PK_{ID})向 C 进行查询,如果 PK_{ID}存在,C 将对应的 K_{ID}发送给 A;否则,C 输出"Invalid",表示 A 是无效操作。

(c)哈希值查询。A 可以对签名算法中使用的哈希函数进行查询,C 返回相应的哈希函数查询值。

(d)证书查询。A 选择 ID,PK_{ID} 向 C 进行查询,C 计算 $\text{certGen}(\text{ID}, PK_{ID}) = Cert_{ID}$,并将 $Cert_{ID}$发送给 A。

(e)签名查询。A 可以询问任意用户关于任意消息 m 的签名,C 调用算法 Sign 得到 σ,并将 σ 发送给 A。

c)伪造。由攻击者 A 来决定查询阶段何时结束。当结束后,A 向 C 提交(m, σ, ID),其中 A 不可以在查询阶段查询身份为 ID 的用户私钥 K_{ID},也不可以查询 $\text{sign}(m, \text{ID})$来获得 m 对应的签名 σ。

如果 σ 确实是身份为 ID 的用户对 m 的有效签名,A 赢得游戏。A 在游戏中的优势 $\text{adv}(A)$即为 A 赢得游戏的概率。

Game1 和 Game2 的区别:Game1 中攻击者不知道主密钥 s,但可以任意替换用户的公、私钥,因此,如果不存在攻击者能够赢得 Game1,则说明方案不仅能够抵抗用户伪造,还能够抵抗替换公钥攻击。Game2 中攻击者不允许替换用户的公、私钥,但知道用户的确切证书值(攻击者知道主密钥 s),因此,如果不存在攻击者能够赢得 Game2,则说明方案能够抵抗 CA 伪造。

1.3　双线性映射和计算 Diffie-Hellman 问题

设$(G_1, +)$和$(G_2, \cdot)$是两个 q 阶循环群,双线性映射 $\hat{e}: G_1 \times G_1 \to G_2$ 满足如下性质:

a)双线性性。任意 $P, Q \in G_1$, $a, b \in Z_q$,有等式 $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ 成立。

b)退化性。存在 $Q, R \in G_1$,使得 $\hat{e}(Q, R) \neq 1$。

c)可计算性。任意 $P, Q \in G_1$,存在有效的算法来计算 $\hat{e}(P, Q)$。

定义 3　给定 q 阶循环群$(G, \cdot)$,P 是 G 的生成元,计算 Diffie-Hellman 问题(CDH)是指任意给定三元组(P, aP, bP),计算 abP,其中 a、b 是未知的。

本文始终假定 CDH 问题是困难的,这意味着不存在有效的多项式时间算法能够以不可忽略的概率计算该问题。

2 新的基于证书的数字签名方案

G_1、G_2、$\hat{e}$ 如第 1 章所定义，设 $H_i(i = 1, 2, 3)$ 是三个安全的密码学哈希函数，其中 $H_1: \{0, 1\}^* \times G_1 \to G_1$，$H_2: \{0, 1\}^* \times G_1 \to G_1$，$H_3: \{0, 1\}^* \times G_1 \to G_1$。方案细节如下：

a）参数生成算法。P 是 G_1 的任意一个生成元，CA 任意选择 $s \in Z_q^*$，$P_{pub} = sP$。其中，主密钥为 s，由 CA 秘密保存，公开参数 params 为 $(G_1, G_2, q, P, P_{pub}, \hat{e}, H_1, H_2, H_3)$。

b）密钥生成算法。具有身份为 ID_A 的用户 A 任意选择 $x \in Z_q^*$，用户的公钥 $PK_A = xP$，私钥 $K_A = x$。

c）证书生成算法。给定公钥 PK_A 和身份 ID_A，CA 计算对应证书 $C_A = sH_1(ID_A, PK_A)$，CA 将证书值 C_A 返回给用户。

d）签名生成算法。对于消息 $m \in \{0, 1\}^*$，用户 A 计算如下：

（a）任意选择 $r \in Z_q^*$；

（b）计算 $W = r^{-1}(C_A + K_A H_2(m, ID_A, PK_A))$；

（c）计算 $V = rH_3(m, W)$；

（d）签名 $\sigma = (W, V)$。

e）验证算法。当得到 A 发送的消息以及签名值 (m, σ) 后，任意用户 B 可使用本算法对签名进行验证。实际上即为验证下述等式是否成立：

$$\hat{e}(PW, V) = \hat{e}(P_{pub}H_1(ID_A, PK_A) + PK_A H_2(m, ID_A, PK_A), H_3(m, W))$$

如果等式不成立，说明得到的签名值是无效的；否则签名值有效，σ 即为 A 的关于消息 m 的有效签名。

方案的正确性验证如下：如果 $\sigma = (W, V)$ 是由签名算法产生的对消息 m 对应于身份 ID_A、公钥 PK_A 的签名，那么可计算为

$$\begin{aligned}\hat{e}(PW, V) &= \hat{e}(r^{-1}P(C + K_A H_2(m, ID_A, PK_A)), rH_3(m, W)) = \\ &\hat{e}(sPH_1(ID_A, PK_A) + PK_A H_2(m, ID_A, PK_A), H_3(m, W)) = \\ &\hat{e}(P_{pub}H_1(ID_A, PK_A) + PK_A H_2(m, ID_A, PK_A), H_3(m, W))\end{aligned}$$

3 方案安全性分析

本节利用第 2 章给出的安全性定义来讨论方案的安全性，可证明本方案是不可伪造的。

定理 1 在随机预言模型下，如果存在攻击者 A 能够以不可忽略的优势 ε 赢得 Game1，那么应答者 C 能够以 $O(\varepsilon)$ 的优势 ξ 解决 CDH 问题。

证明 如果存在攻击者 A 能够以不可忽略的优势 ε 赢得 Game1，下面证明应答者 C 可以 $O(\varepsilon)$ 的优势 ξ 利用 A 来解决 CDH 问题。在游戏中，A 可以向 C 查询随机预言模型 H_1、H_2、H_3 的输出值。通常这些值是随机生成的，为了避免碰撞，C 使用三个列表 L_1、L_2、L_3 来存储回答的这些输出值。此外，C 使用列表 L_0 来存储 A 查询的公、私钥，L_4 来存储 A 查询的证书值，L_5 来存储 A 查询的签名值。假定应答者 C 收到 (P, aP, bP)，P 是 G_1 的一个生成元，C 利用 A 通过 Game1 来计算 abP。

1）参数生成 应答者 C 选择 $P_{pub} = aP$，公开参数 params 为 $(G_1, G_2, q, P, P_{pub})$。$C$ 将参数 params 发送给 A。

2）查询阶段 在此阶段攻击者 A 可向 C 查询，查询次数为多项式次数，方式为自适应查询。A 可进行的预言模型查询如下：

a）密钥模型（Ω_{KeyGen}）查询。A 提交身份 ID_i，C 响应如下：C 检查列表 L_0，如果该身份存在，C 将对应密钥值返回给 A；否则 C 任意选择 $x_i \in Z_q^*$，计算得到用户的公钥 $PK_i = x_i P$，私钥 $K_i = x_i$。C 将 (ID_i, K_i, PK_i) 存储在列表 L_0 中，并将 (K_i, PK_i) 返回给 A。

b）密钥替换。A 向 C 提交 (ID_i, K_i, PK_i) 替换用户 i 的公、私钥，C 响应如下：C 验证 PK_i 是否是 K_i 对应的公钥，如果不是，C 输出“Invalid”，表示 A 是无效操作；否则，C 操作如下：C 首先检查列表 L_0，如果身份存在，则用该公、私钥替换用户 i 原来的公、私钥；如果不存在，C 将 (ID_i, K_i, PK_i) 存储在列表 L_0 中。

c）H_1 随机预言模型（Ω_{H1}）查询。当 A 查询关于某一身份 ID_i 的哈希值时，C 检查列表 L_1，如果该身份存在，C 将对应哈希值返回给 A；否则 C 随机选择 α_i，$\alpha_i \in G_1$，将 (ID_i, α_i) 存储在列表 L_1 中，并将 α_i 返回给 A。在 A 的所有查询中，C 选择身份 ID_{i0}，并设置 $\Omega_{H1}(ID_{i0}) = bP$。由于 bP 是 CDH 问题给出的随机值，因此并不影响 Ω_{H1} 的随机性。

d）H_2 随机预言模型（Ω_{H2}）查询。当 A 查询 (m, ID_i, PK_i) 的哈希值时，C 检查列表 L_2，如果 (m, ID_i, PK_i, β_i) 存在，C 将对应哈希值 β_i 返回给 A；否则，C 随机选择 β_i，$\beta_i \in G_1$，将 (m, ID_i, PK_i, β_i) 存储在列表 L_2 中，并将 β_i 返回给 A。

e）H_3 随机预言模型（Ω_{H3}）查询。当 A 查询 (m, W) 的哈希值时，C 响应如下：如果 (m, W, γ) 在列表 L_3 中，C 将对应哈希值 γ 返回给 A；否则，C 随机选择 γ，$\gamma \in G_1$，C 将 (m, W, γ) 存储在列表 L_3 中，并将 γ 返回给 A。

f）证书（$\Omega_{CertGen}$）查询。A 选择 (ID_i, PK_i) 向 C 进行查询，C 响应如下：C 检查列表 L_4，如果 (ID_i, PK_i, C_i) 存在，C 将对应证书值 C_i 返回给 A；否则，如果 $i \neq i_0$，C 随机选择 C_i，$C_i \in G_1$，C 将 (ID_i, PK_i, C_i) 存储在列表 L_4 中，并将 C_i 返回给 A；如果 $i = i_0$，C 挑战 CDH 问题失败，因为 C 不知道 a 值，故无法计算 i_0 的证书 $C_{i0} = abP$。

g）签名（Ω_{Sign}）查询。A 提交身份 ID_i 以及消息 m，C 响应如下：C 检查列表 L_5，如果该数值曾经被查询，C 将之前的回答响应值返回给 A；否则，C 利用 $\Omega_{KeyGen}(ID_i)$ 计算其公、私钥，以及 $\Omega_{CertGen}(ID_i, PK_i)$ 计算其证书，并利用签名算法生成签名值 σ。C 将签名值 $\sigma = (W, V)$ 返回给 A，并将 (ID_i, m, σ) 存储在列表 L_5 中。

3）伪造 查询阶段结束后，A 向 C 提交 (ID_i, m, σ)。其中 A 不可以在查询阶段查询 ID_i 的证书，也不允许查询 $\Omega_{Sign}(ID_i, m)$ 来获得 σ。如果 $i \neq i_0$，C 挑战 CDH 问题失败；如果 $i = i_0$，并且 σ 是一个有效签名值，此时 C 计算如下：

a）计算 $r = H_3(m, W)V^{-1}$；

b）计算 $C_{i0} = rW - x_{i0}H_2(m, ID_{i0}, PK_{i0})$。

由于 $C_{i0} = abP$，因此 C 可解决 CDH 问题。

C 解决 CDH 问题的概率分析：令 q_{H1}、q_{H2}、q_{H3}、q_K、q_C 分别是 A 可以向 Ω_{H1}、Ω_{H2}、Ω_{H3}、Ω_{KeyGen}、$\Omega_{CertGen}$ 提交的最大查询次数。如果 A 查询 ID_{i0} 的证书，由于 C 不知道 a 值，故无法提供 i_0 的证书 $C_{i0} = abP$，记此事件为 E_1。E_1 不发生的概率为

$$Pr(\neg E_1) = \left(\frac{q_K - 1}{q_K}\right)\left(\frac{q_K - 2}{q_K - 1}\right)\cdots\left(\frac{q_K - q_C}{q_K - q_C + 1}\right) = \frac{q_K - q_C}{q_K}$$

如果 A 不选择 i_0 作为伪造阶段的签名者，那么 C 也无法

解决 CDH 问题,记此事件为 E_2、E_2 不发生的概率为

$$Pr(\neg E_2)=\left(\frac{q_K-q_C-1}{q_K-q_C}\right)\left(\frac{1}{q_K-q_C-1}\right)=\frac{1}{q_K-q_C}$$

故 C 解决 CDH 问题的概率 ξ 为

$$\xi=\varepsilon\left(\frac{q_K-q_C}{q_K}\right)\left(\frac{1}{q_K-q_C}\right)=\varepsilon\left(\frac{1}{q_K}\right)$$

因此,如果存在攻击者 A 能够以不可忽略的优势 ε 赢得 Game1,那么应答者 C 能够以 $O(\varepsilon)$ 的优势 ξ 解决 CDH 问题。

定理 2　在随机预言模型下,如果存在攻击者 A 能够以不可忽略的优势 ε 赢得 Game2,那么应答者 C 能够以 $O(\varepsilon)$ 的优势 ξ 解决 CDH 问题。

证明　如果存在攻击者 A 能够以不可忽略的优势 ε 赢得 Game2,下面证明应答者 C 可以 $O(\varepsilon)$ 的优势 ξ 利用 A 来解决 CDH 问题。在游戏中,A 可以向 C 查询随机预言模型 H_1、H_2、H_3 的输出值。通常这些值是随机生成的,为了避免碰撞,C 使用三个列表 L_1、L_2、L_3 来存储回答的这些输出值。此外,C 使用列表 L_0 来存储 A 查询的公、私钥,L_4 来存储 A 查询的证书值,L_5 来存储 A 查询的签名值。假定应答者 C 收到(P, aP, bP),P 是 G_1 的一个生成元,C 利用 A 通过 Game2 来计算 abP。

1)参数生成　应答者 C 选择安全参数 1^κ 运行参数生成算法得到公开参数 params 以及主密钥 s。C 将参数 params 和主密钥 s 发送给 A。

2)查询阶段　在此阶段攻击者 A 可以向 C 查询,查询次数为多项式次数,方式为自适应查询,即下一次查询的内容依赖于上一次查询的结果。A 可进行的预言模型查询如下:

a)公钥查询。A 提交身份 ID_i,C 响应如下:C 检查列表 L_0,如果 ID_i 在 L_0 中,C 将对应的公钥值返回给 A;否则,C 任意选择 $x_i\in Z_q^*$,用户的公钥 $PK_i=x_iP$,私钥 $K_i=x_i$。C 将(ID_i, K_i, PK_i)存储在列表 L_0 中;在 A 的所有查询中,C 选择身份 ID_{i0},并设置 $PK_{i0}=aP$,并将$(ID_{i0}, \perp, PK_{i0})$ 存储在列表 L_0 中,将 PK_i 返回给 A。由于 aP 是 CDH 问题给出的随机值,因此并不影响 Ω_{KeyGen}的随机性。

b)私钥查询。A 提交(ID_i, PK_i),C 响应如下:如果 $i=i_0$,C 挑战 CDH 问题失败,因为 C 不知道 i_0 的私钥 $K_{i0}=a$;如果 $i\neq i_0$,C 检查列表 L_0,如果(ID_i, PK_i)在 L_0 中,C 将对应的私钥值返回给 A,否则 C 输出“Invalid”,表示 A 是无效操作。

c)H_1 随机预言模型(Ω_{H1})查询。当 A 查询关于某一身份 ID_i 的哈希值时,C 检查列表 L_1,如果该身份存在,C 将对应哈希值返回给 A;否则 C 随机选择 α_i,$\alpha_i\in G_1$,将(ID_i, α_i)存储在列表 L_1 中,并将 α_i 返回给 A。

d)H_2 随机预言模型(Ω_{H2})查询。当 A 查询(m, ID_i, PK_i)的哈希值时,C 检查列表 L_2,如果(m, ID_i, PK_i, β_i)存在,C 将对应哈希值 β_i 返回给 A;否则,如果 $i\neq i_0$,C 随机选择 β_i,$\beta_i\in G_1$,将(m, ID_i, PK_i, β_i)存储在列表 L_2 中,并将 β_i 返回给 A,如果 $i=i_0$,C 设置 $\beta_{i0}=bP$。由于 bP 是 CDH 问题给出的随机值,因此并不影响 Ω_{H2}的随机性。

e)H_3 随机预言模型(Ω_{H3})查询。当 A 查询(m, W)的哈希值时,C 响应如下:如果(m, W, γ)在列表 L_3 中,C 将对应值 γ 返回给 A;否则,C 随机选择 γ,$\gamma\in G_1$,C 将(m, W, γ)存储在列表 L_3 中,并将 γ 返回给 A。

f)证书$(\Omega_{\text{CertGen}})$查询。$A$ 选择(ID_i, PK_i)向 C 进行查询,C 响应如下:C 检查列表 L_1 和 L_4,如果身份 ID_i 存在于列表 L_1 中,C 计算 $C_i=\Omega_{\text{CertGen}}(ID_i, PK_i)=s\alpha_i$;如果$(ID_i, PK_i, C_i)$在列表 L_4 中,C 将对应证书值 C_i 返回给 A;否则,C 随机选择 C_i,$C_i\in G_1$,C 将(ID_i, PK_i, C_i)存储在列表 L_4 中,并将 C_i 返回给 A。

g)签名(Ω_{Sign})查询。A 提交身份 ID_i 以及消息 m,C 响应如下:C 检查列表 L_5,如果该数值曾经被查询,C 将之前的回答响应值返回给 A;否则,如果 $i=i_0$,C 挑战 CDH 问题失败,因为 C 不知道 a 值,即不知道 i_0 的私钥 $K_{i0}=a$,无法计算对应的签名,如果 $i\neq i_0$,C 利用 $\Omega_{\text{KeyGen}}(ID_i)$ 计算其公、私钥,以及 $\Omega_{\text{CertGen}}(ID_i, PK_i)$ 计算其证书,并利用签名算法生成签名值 σ。C 将签名值 $\sigma=(W, V)$ 返回给 A,并将(ID_i, m, σ)存储在列表 L_5 中。

3)伪造　查询阶段结束后,A 向 C 提交(ID_i, m, σ)。其中 A 不可以在查询阶段查询 ID_i 的私钥,也不可以查询 $\Omega_{\text{Sign}}(ID_i, m)$来获得 σ。如果 $i\neq i_0$,C 挑战 CDH 问题失败;如果 $i=i_0$,并且 σ 是一个有效签名值,此时 C 计算如下:

a)计算 $C_{i0}=\Omega_{\text{CertGen}}(ID_{i0}, PK_{i0})$;

b)计算 $r=H_3(m, W)V^{-1}$;

c)计算 $K_{i0}H_2(m, ID_{i0}, PK_{i0})=rW-C_{i0}$。

由于 $K_{i0}=a$,$H_2(m, ID_{i0}, PK_{i0})=bP$,所以 $abP=K_{i0}\times H_2(m, ID_{i0}, PK_{i0})=rW-C_{i0}$。因此 C 可解决 CDH 问题。

C 解决 CDH 问题的概率分析:令 q_{H1}、q_{H2}、q_{H3}、q_C、q_S 分别是 A 可以向 Ω_{H1}、Ω_{H2}、Ω_{H3}、Ω_{CertGen}、Ω_{Sign}提交的最大查询次数,q_K 是 A 可以提交的对密钥查询的最大次数。如果 A 查询用户 i_0 的私钥,由于 C 不知道 a 值,即 i_0 的私钥, C 失败,记此事件为 E_1。E_1 不发生的概率为

$$Pr(\neg E_1)=\left(\frac{q_K-1}{q_K}\right)\left(\frac{q_K-2}{q_K-1}\right)\cdots\left(\frac{q_K-q_{H_1}-q_C}{q_K-q_{H_1}-q_C+1}\right)=\frac{q_K-q_{H_1}-q_C}{q_K}$$

如果 A 查询用户 i_0 的签名,由于 C 不知道 i_0 的私钥,故也无法计算 i_0 的签名,记此事件为 E_2。E_2 不发生的概率为

$$Pr(\neg E_2)=\left(\frac{q_S-1}{q_S}\right)\left(\frac{q_S-2}{q_S-1}\right)\cdots\left(\frac{q_S-q_K}{q_S-q_K+1}\right)=\frac{q_S-q_K}{q_S}$$

如果 A 不选择 i_0 作为伪造阶段的签名者,那么 C 也无法解决 CDH 问题,记此事件为 E_3。E_3 不发生的概率为

$$Pr(\neg E_2)=\left(\frac{q_K-q_{H_1}-q_C-1}{q_K-q_{H_1}-q_C}\right)\left(\frac{1}{q_K-q_{H_1}-q_C-1}\right)=\frac{1}{q_K-q_{H_1}-q_C}$$

故 C 解决 CDH 问题的概率 ξ 为

$$\xi=\varepsilon\left(\frac{q_K-q_{H_1}-q_C}{q_K}\right)\left(\frac{q_S-q_K}{q_S}\right)\left(\frac{1}{q_K-q_{H_1}-q_C}\right)=\varepsilon\left(\frac{q_S-q_K}{q_Sq_K}\right)$$

因此,如果存在攻击者 A 能够以不可忽略的优势 ε 赢得 Game2,那么应答者 C 能够以 $O(\varepsilon)$ 的优势 ξ 解决 CDH 问题。

由定理 1 和 2 可得,在假定 CDH 问题是难解的假设下,新的方案在自适应选择消息和身份的前提下,可以抵抗替换公钥攻击,并且是不可伪造的。

(下转第 1444 页)

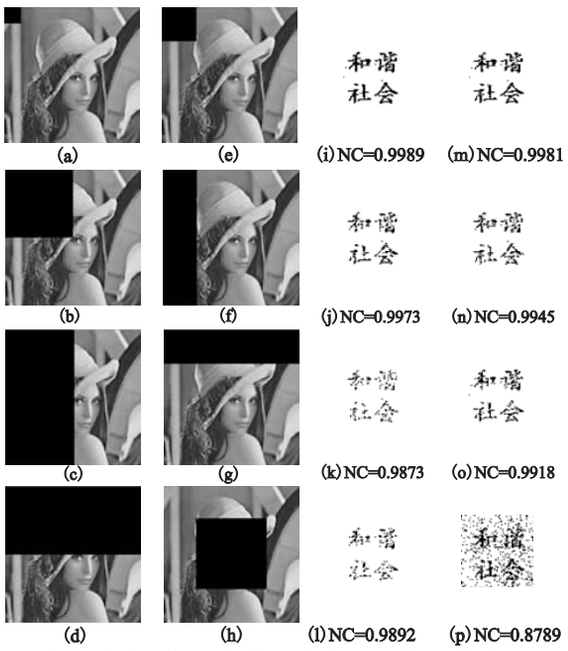

图4 含水印的Lena图像受到不同位置剪切后的结果及所提取的水印结果

总之,由表 3 ~5 和图 4 的实验可以看出,本文算法具有较强的鲁棒性。

4 结束语

本文提出一种新的彩色图像盲水印技术,其突出的优点是:a)用空域技术代替 DCT 域技术将数字水印嵌入在 DC 系数中,与 DCT 域算法相比,所提算法的执行时间减少了一半,并且减少了计算误差,提高了算法的性能;b)利用基于密钥 K_1 的哈希置乱和基于密钥 K_2 的量化步长,水印算法的安全性得到了保障;c)所提算法不但具有较强的鲁棒性,而且算法简单,能够在空域中达到盲提取的目的。

参考文献:

[1] 苏庆堂. 基于整型小波变换的彩色图像盲水印算法[J]. 计算机应用研究, 2009,26(6):2168,2169-2172.

[2] LOU D C, TSO H K, LIU J L. A copyright protection scheme for digital images using visual cryptography technique[J]. Computer Standards & Interfaces,2007,29(1):125-131.

[3] FLEET D J, HEEGER D J. Embedding invisible information in color images[J]. IEEE Trans on Image Processing,1977,1(1):532-535.

[4] QI Xiao-jun, QI Ji. A robust content-based digital image watermarking scheme[J]. Signal Processing,2007,87(6):1264-1280.

[5] USMAN I, KHAN A. BCH coding and intelligent watermark embedding: employing both frequency and strength selection[J]. Applied Soft Computing,2010,10(1):332-343.

[6] LIN S D, SHIE S C, GUO Jian-yi. Improving the robustness of DCT-based image watermarking against JPEG compression[J]. Computer Standards & Interfaces,2010,32(1-2):54-60.

[7] SAMI B, LALA K, THAWAR A, *et al*. Watermarking of digital images in frequency domain[J]. International Journal of Automation and Computing,2010,7(1):17-22.

[8] LIU Lian-shan, LI Ren-hou, GAO Qi. A new watermarking method based on DWT green component of color image[C]//Proc of International Conference on Machine Learning and Cybernetics. 2004: 3949-3954.

[9] LIU Kuo-cheng. Wavelet-based watermarking for color images through visual masking [J]. AEU-International Journal of Electronics and Communications,2010,64(2):112-124.

[10] CHAN C K, CHENG L M. Hiding data in images by simple LSB substitution [J]. Pattern Recognition,2004,37(3):469-474.

[11] SHIH F Y, WU S Y T. Combinational image watermarking in the spatial and frequency domains[J]. Pattern Recognition,2003,36(4):969-975.

(上接第 1433 页)

4 效率分析

新的方案与已有随机预言模型下可证明安全的使用双线性对运算的基于证书签名方案所使用的运算比较分析如表 1 所示。其中,M 表示群 G_1 或 G_2 上的形如 aP 的标量乘法;SM 表示群 G_1 或 G_2 上形如 $aP+bQ$ 的标量乘法;E 表示指数运算;P 表示双线性对运算。

表 1 与已有基于证书签名方案的运算效率比较

方案	签名算法	验证算法	签名长度
文献[2]	$3M$	$3P$	$\|G_1\|\times\|G_1\|\times\|Zq\|$
文献[3]	$1M+2SM$	$3P$	$\|G_1\|\times\|G_1\|$
文献[5]	$1E+2M+2P$	$1M+3P+1E$	$\|G_1\|\times\|Zq\|$
本文	$3M$	$1M+2SM+2P$	$\|G_1\|\times\|G_1\|$

从表 1 可以看出,新的基于证书签名方案无论计算效率还是签名长度均不高于已有可证明安全的基于证书签名方案。

5 结束语

本文提出了一个新的基于证书的数字签名方案。利用随机预言模型,在基于 CDH 问题是难解的假设下,证明了方案的安全性。经过效率比对分析,新的方案设计简单,运算效率高,适用于实际使用,特别是计算能力受限的设备。目前,对基于证书数字签名的研究还不够深入,事实上,如何利用 CDH 问题以及 BDH(判定 Diffie-Hellman)问题(包括它们的变形)的难解性,来设计更多可证安全、有效的基于证书签名方案是一个有意义的课题,也是下一步要研究的工作。

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 schemes without pairings or random Oracles[C]//Lecture Notes in Computer Science, vol5222. Berlin: Springer-Verlag, 2008: 285-297.

[5] 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.