无证书强指定验证者签名方案

张亦辰 李继国 钱 娜
(河海大学计算机与信息学院 南京 211100)

摘 要 无证书强指定验证者签名,能够很好地解决传统密码体制下强指定验证者签名证书管理复杂问题和基于身份密码体制下强指定验证者签名的密钥托管问题,因此研究无证书强指定验证者签名具有重要的理论意义。提出了一个无证书强指定验证者签名方案。基于CDH(Computational Diffie Hellman)问题和CBDH(Computational Bilinear Diffie-Hellman)问题困难假定,在随机预言模型下证明了该方案对自适应选择消息攻击是存在不可伪造的,分析表明该方案具有较小的计算代价和通信代价。

关键词 公钥密码学,无证书签名,强指定验证者签名,CBDH问题,CDH问题

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.3.027

Certificateless Strong Designated Verifier Signature Scheme

ZHANG Yi-chen LI Ji-guo QIAN Na
(College of Computer & Information Engineering, Hohai University, Nanjing 211100, China)

Abstract It has great academic significance to research certificateless strong designated verifier signature(CLSDVS) that can solve the certificate management complexity problem in traditional public key cryptosystem and key escrow problem in identity-based public key cryptosystem. We constructed a CLSDVS scheme and proved that our scheme is existentially unforgeable against adaptive chosen message attack under the assumption of the computational bilinear Diffie-Hellman problem and computational Diffie-Hellman problem in the random oracle model. Then, we analyzed the computation cost and communication cost of our scheme.

Keywords Public key cryptography, Certificateless signature, Strong designated verifier signature, CBDH problem, CDH problem

1 引言

在1996年欧密会上,Jackobsson[1]等人首次提出了具有指定验证者的签名方案。在指定验证者签名中,签名人能够指定可以验证其签名的人,只有指定验证者才能判别签名人是否对消息签了名,同时签名人又不能完全控制其签名的验证。指定验证者签名不但解决了标准签名中任何人都可以验证签名的问题,而且解决了不可否认签名中签名人完全控制签名的问题。但是这样的指定验证者签名由于任何人都可以验证签名有效性,可以确定潜在的两个签名者:签名者和指定验证者,因此如果签名在发送途中被截取,敌手就可以判断是谁做的有效签名。

为了解决以上问题,2003年Saeednia[2]等人提出了强指定验证者的概念,签名的验证需要引入指定验证者的私钥。强指定验证者签名中任何人都能生成一个与原始签名不能区分、具有相同分布的副本,只有指定验证者借助自己的私钥才能验证原始签名的有效性。强指定验证者签名的概念一提出,便有很多学者进行了研究[3-7]。

对于传统的公钥密码体制下的指定验证者签名,签名者的公钥本质上就是签名者自己选择的一个随机字符串,无法证明给定签名者的身份,需要一个可信的第三方用一个证书来将公钥和签名人的身份绑定,所以在验证一个签名之前首先需要验证公钥的有效性,并且证书管理的过程需要很大的计算量和很强的存储能力。针对这一问题,Susilo、Zhang和Mu[6]于2004年提出了基于身份的强指定验证者签名,解决了传统公钥密码体制的两次验证问题,随后又有很多基于身份的指定验证者签名方案被提出[7-13]。然而基于身份的指定验证者签名仍存在密钥托管问题,文献[8]提出了一个新的基于身份的广义指定验证者签名方案,其通过引入两个PKG的方法部分地解决了密钥托管问题,但是仍无法从根本上解决密钥托管问题。

为了更好地解决传统公钥密码体制和基于身份密码体制下指定验证者签名的固有问题,2006年Huang等[14]首次提出了无证书的指定验证者签名的定义,并给出了一个具体的方案,证明了方案的安全性。随后,文献[15-18]也提出了有效的无证书指定验证者签名方案。其中,文献[15]提出了无

到稿日期:2014-08-20 返修日期:2014-09-27 本文受国家自然科学基金(61272542),河海大学中央高校基本科研业务费专项资金项目(2013B07014)资助。

张亦辰(1971-),女,博士生,讲师,主要研究方向为密码学理论与技术,E-mail:zyc_718@163.com;李继国(1970-),男,博士,教授,博士生导师,主要研究方向为密码学理论与技术、信息安全、云计算安全等,E-mail:lijiguo@hhu.edu.cn;钱 娜(1985-),女,硕士,主要研究方向为密码学理论与技术。

证书的短指定验证者签名方案，其有效地缩短了签名长度。文献[16]提出了一个有效的无证书强指定验证者签名，并证明了方案的安全性。文献[17]首次提出了无证书广义指定验证者签名的概念和构造，文献[18]中将这个概念扩展到了无证书的广义指定多个验证者签名，并给出了一个有效的签名方案，该方案满足无证书指定验证者签名的安全要求。

本文基于 CDH 和 CBDH 困难问题假定，构造了一个无证书强指定验证者签名方案，并分析了方案的通信代价和计算代价；在随机预言模型下证明了方案的安全性。该方案解决了传统公钥密码体制签名中的证书管理复杂问题和基于身份指定验证者签名中的密钥托管问题。

2 双线性映射及困难问题

2.1 双线性映射

定义 1(双线性映射) 设 G_1 是阶为大素数 q 的加法群，G_2 是阶为大素数 q 的乘法群。P 是 G_1 的生成元，G_1，G_2 之间的映射 $e:G_1\times G_1\to G_2$ 如果满足以下性质，则称为双线性映射。

双线性性：对所有 $P,Q\in G_1$，$a,b\in Z_q$，有 $e(aP,bQ)=e(P,Q)^{ab}$；

非退化性：存在 $P,Q\in G_1$，使得 $e(P,Q)\neq 1$；

可计算性：存在一个有效的算法，对所有 $P,Q\in G_1$，可以计算 $e(P,Q)$。

2.2 困难问题

设 G_1 是阶为大素数 q 的加法群，G_2 是阶为大素数 q 的乘法群。P 是 G_1 的生成元，$e:G_1\times G_1\to G_2$ 是双线性映射。

定义 2(CDH 问题) 对于 $a,b\in Z_q^*$，给定 $P,aP,bP\in G_1$，计算 abP。

定义 3(CBDH 问题) 给定 $P,aP,bP,cP\in G_1$，其中 $a,b,c\in Z_q^*$ 且未知，计算 $e(P,P)^{abc}\in G_2$。

3 无证书强指定验证者签名的定义和安全模型

3.1 无证书强指定验证者签名的定义

参照文献[16]中对无证书强指定验证者签名的定义，给出如下定义：

无证书强指定验证者签名(CLSDVS)系统中有 3 个实体参与：签名者 ID_A、指定验证者 ID_B 以及可信第三方 KGC。该系统由系统设置、部分私钥产生、用户密钥产生、签名、验证、副本模拟 6 个算法组成。

系统设置：输入安全参数 l，生成系统参数 $param$。KGC 选择主密钥 msk，并计算主公钥 mpk。公开参数 $params=\{param,mpk\}$。

部分私钥产生：输入参数 $params$、用户的身份 ID_i 以及主密钥 msk，KGC 生成该用户的部分私钥 D_{ID_i}，$i=A,B$。

用户密钥产生：输入参数 $params$、用户的身份 ID_i，输出用户的秘密值 s_{ID_i} 和公钥 P_{ID_i}，$i=A,B$。

签名：输入参数 $params$、消息 m、ID_A 的部分私钥 D_{ID_A}、秘密值 s_{ID_A} 以及 ID_B 的公钥 P_{ID_B}，输出有效的消息签名对 (m,δ)。

验证：输入参数 $params$、消息签名对 (m,δ)、ID_B 的秘密值 s_{ID_B}、部分私钥 D_{ID_B} 以及 ID_A 的公钥 P_{ID_A}，判断签名 δ 是否为对消息 m 的有效指定验证者签名，输出 $d\in\{acc,rej\}$。

副本模拟：这个算法是由指定验证者运行，用来生成一个与原始签名不可区分的副本。

3.2 无证书强指定验证者签名的安全模型

类似于文献[16]中的定义，本文定义了两类具有不同能力的敌手。第一类敌手是恶意用户，可以得到用户秘密值，并且可以用自己随机选择的值替换所有用户的公钥，但是不能得到主私钥以及目标用户的部分私钥。第二类敌手是恶意的第三方，可以得到主私钥以及用户的部分私钥，但是不能得到目标用户的秘密值，也不能替换用户的公钥。无证书强指定验证者签名的安全性用下面两个挑战者与敌手之间的游戏来描述，并生成该用户的部分私钥 。

3.2.1 CLSDVS 游戏 1

用以下挑战者与敌手 A_{I} 交互的游戏，模拟第一类敌手的适应性选择消息攻击。

(1)初始化：挑战者运行系统设置算法产生系统参数 $param$ 和主公钥 mpk，运行用户密钥产生算法产生 P_{ID_i}，$i=A,B$(ID_A 为目标签名者，ID_B 为目标指定验证者)；并公开参数 $params=\{param,mpk\}$ 和 P_{ID_i}($i=A,B$)。

(2)部分私钥询问：敌手 A_{I} 询问用户 ID_i($ID_i\notin\{ID_A,ID_B\}$)的部分私钥，挑战者运行部分私钥产生算法生成用户 ID_i 的部分私钥 D_{ID_i}。

(3)公钥询问：询问 ID_i 的公钥 P_{ID_i}，运行用户密钥产生算法产生用户的秘密值和公钥元组(ID_i,s_{ID_i},P_{ID_i})，$i\in\{1,2,\cdots\}$，将 P_{ID_i} 返回给敌手 A_{I}。

(4)秘密值询问：询问 ID_i 的私钥 s_{ID_i}，挑战者查询包含(ID_i,s_{ID_i},P_{ID_i})($i\in\{1,2,\cdots\}$)元组的列表，将 s_{ID_i} 返回给敌手 A_{I}。

(5)用户公钥替换：敌手 A_{I} 随机选择公钥 P'_{ID_i} 替换任意用户 ID_i 的公钥 P_{ID_i}。

(6)签名询问：询问对消息(m_k,ID_i,ID_j,P'_{ID_i})的签名，用签名算法产生签名 δ，返回 δ 给敌手 A_{I}。

(7)验证询问：询问消息签名对($m_k,\delta_k,ID_i,ID_j,P'_{ID_i}$)，运行验证算法判断是否为有效的消息签名对，返回 $d\in\{acc,rej\}$ 给 A_{I}。

(8)伪造：敌手 A_{I} 给出五元组($m^*,\delta^*,ID_A,ID_B,P'_{ID_A}$)满足：

(a)δ^* 是 ID_A,ID_B 关于消息 m^* 的有效签名，且(m^*,ID_A,ID_B)没有在签名询问中询问过。

(b)ID_A,ID_B 都没有在部分私钥询问中出现过。

3.2.2 CLSDVS 游戏 2

用以下挑战者与敌手交互的游戏，模拟第二类敌手 A_{II} 的适应性选择消息攻击。

(1)初始化：挑战者运行系统设置算法产生系统参数 $param$ 和主公私钥对(msk,mpk)。挑战者将参数 $params=\{param,mpk\}$ 和 msk 发送给敌手 A_{II}。

(2)公钥询问：询问任意用户 ID_i 的公钥 P_{ID_i}，运行用户密钥产生算法产生用户的秘密值和公钥元组(ID_i,s_{ID_i},P_{ID_i})($i\in\{1,2,\cdots\}$)，将 P_{ID_i} 返回给敌手 A_{II}。

(3)秘密值询问：询问非目标用户 ID_i(除目标签名者和目标指定验证者之外的用户)的秘密值 s_{ID_i}，查询包含元组(ID_i,s_{ID_i},P_{ID_i})($i\in\{1,2,\cdots\}$)的列表，将 s_{ID_i} 返回给敌手 A_{II}。

(4)签名询问：询问对消息(m_k,ID_i,ID_j)的签名，用签名算法产生签名 δ_k，返回 δ_k 给敌手 A_{II}。

(5)验证询问:询问消息签名对(m_k,δ_k,ID_i,ID_j),运行验证算法判断是否为有效的消息签名对,返回$d\in\{acc,rej\}$给敌手A_{II}。

(6)伪造:敌手给出四元组(m^*,δ^*,ID_A,ID_B)满足以下条件:

(a)δ^*是ID_A,ID_B关于消息m^*的有效签名,且(m^*,ID_A,ID_B)没有在签名询问中询问过。

(b)ID_A,ID_B都没有在秘密值询问中出现过。

4 无证书强指定验证者签名方案

系统设置:输入系统安全参数l,输出系统参数$\{G_1,G_2,q,e,P\}$,其中,G_1是阶为大素数q的加法循环群,G_2是阶为大素数q的乘法循环群。P是G_1的生成元,$e:G_1\times G_1\rightarrow G_2$是双线性映射。

*KGC*做如下操作:

步骤1 随机选择秘密值$s\in Z_q^*$作为主私钥,计算主公钥$mpk=P_{pub}=sP$;

步骤2 选择两个hash函数$H_0:\{0,1\}^*\rightarrow G_1;H_1:\{0,1\}^*\times G_1\times G_1\rightarrow Z_q^*$;

步骤3 公开参数$params=(G_1,G_2,q,e,P,H_0,H_1,P_{pub})$,主私钥$msk=s$保密。

部分私钥产生:*KGC*用参数*params*和主私钥*msk*来产生用户的部分私钥。给定一个用户的身份$ID_i(i\in\{A,B\})$,*KGC*计算$Q_{ID_i}=H_0(ID_i)\in G_1$,$D_{ID_i}=sQ_{ID_i}$。通过秘密信道将$D_{ID_i}$发送给用户$ID_i$作为部分私钥。

用户密钥产生:输入参数*params*以及用户身份ID_i,随机选择用户ID_i的秘密值s_{ID_i},计算对应的公钥$P_{ID_i}=s_{ID_i}P$,$i\in\{A,B\}$。

签名:用户ID_A对消息m签名,并指定验证者ID_B。ID_A随机选择$r\in Z_q^*$,计算

$U=rQ_{ID_B}$

$h=H_1(m,U,s_{ID_A}P_{ID_B})$

$V=(h/r)D_{ID_A}$

$\delta=(U,V)$

验证:用户ID_B得到消息m的签名$\delta=(U,V)$,验证签名的有效性。计算$h=H_1(m,U,s_{ID_B}P_{ID_A})$,判断$e(V,U)\overset{?}{=}e(hQ_{ID_A},D_{ID_B})$。如果满足,则是有效的签名,否则签名无效。

副本模拟:用户ID_B能够生成有效的副本。ID_B随机选择$r'\in Z_q^*$,计算

$U'=r'Q_{ID_A}$

$h'=H_1(m,U',s_{ID_B}P_{ID_A})$

$V'=(h'/r')D_{ID_B}$

$\delta'=(U',V')$

对于无证书的指定验证者签名方案,如果签名者ID_A正确地执行签名算法产生的签名δ,指定验证者ID_B可以通过验证算法验证δ是有效的。

$$h=H_1(m,U,s_{ID_B}P_{ID_A})=H_1(m,U,s_{ID_B}s_{ID_A}P)=H_1(m,U,s_{ID_A}P_{ID_B})$$

$$e(V,U)=e((h/r)D_{ID_A},rQ_{ID_B})=e(hD_{ID_A},Q_{ID_B})=e(hsQ_{ID_A},Q_{ID_B})=e(hQ_{ID_A},D_{ID_B})$$

5 无证书强指定验证者签名的安全性分析

定理1 在随机预言模型下,基于CBDH困难问题,该方案对第一类攻击者是存在不可伪造的。

证明:给定一个CBDH问题实例$P,P_1,P_2,P_3\in G_1$,其中$P_1=aP,P_2=bP,P_3=cP,a,b,c$未知。构造算法$B$利用敌手$A_1$,计算$e(P,P)^{abc}\in G_2$的值。在证明过程中假设敌手$A_1$不会重复两个相同请求。

设置:输入安全参数l,输出系统参数$\{G_1,G_2,q,e,P\}$。方案中的两个目标用户分别为签名者ID_A和指定验证者ID_B。B令$P_{pub}=sP=P_3=cP$,将$\{G_1,G_2,q,e,P,P_{pub}\}$发送给敌手$A_1$。

H_0询问:挑战者B保存一个包含元组$(ID_i,\alpha_{ID_i},Q_{ID_i})$的列表$H_0$-*list*。$H_0$-*list*初始化为空。敌手$A_1$询问$ID_i$。

(1)如果$ID_i=ID_A$,设置$Q_{ID_A}=P_1=aP$,添加$(ID_A,\perp,Q_{ID_A})$到H_0-*list*,返回Q_{ID_i}给敌手A_1。

(2)如果$ID_i=ID_B$,设置$Q_{ID_B}=P_2=bP$,添加$(ID_B,\perp,Q_{ID_B})$到H_0-*list*,返回Q_{ID_i}给敌手A_1。

(3)否则,随机选取$\alpha_{ID_i}\in Z_q^*$,计算$Q_{ID_i}=\alpha_{ID_i}P$,将$(ID_i,\alpha_{ID_i},Q_{ID_i})$加入$H_0$-*list*中,返回$Q_{ID_i}$给敌手$A_1$。

部分私钥询问:敌手询问$ID_i(ID_i\notin\{ID_A,ID_B\})$的部分私钥$D_{ID_i}$,挑战者查询$H_0$-*list*。

(1)如果已存在,计算$D_{ID_i}=\alpha_{ID_i}cP$。

(2)否则,随机选取$\alpha_{ID_i}\in Z_q^*$,计算$Q_{ID_i}=\alpha_{ID_i}P$,将$(ID_i,\alpha_{ID_i},Q_{ID_i})$加入$H_0$-*list*中,并计算$D_{ID_i}=\alpha_{ID_i}cP$,返回$D_{ID_i}$给敌手$A_1$。

公钥询问:挑战者B保存一个包含元组$(ID_i,s_{ID_i},P_{ID_i},a_i)$的列表*pk-list*,初始化为空。敌手$A_1$询问$ID_i$的公钥,挑战者查询*pk-list*。

(1)如果已存在,并且$a_i=0$,返回P_{ID_i}给敌手A_1。

(2)否则,挑战者随机选取$s_{ID_i}\in Z_q^*$,计算$P_{ID_i}=s_{ID_i}P$,将$(ID_i,s_{ID_i},P_{ID_i},0)$加入*pk-list*中,返回$P_{ID_i}$给敌手$A_1$。

秘密值询问:敌手A_1询问ID_i的秘密值,挑战者查询*pk-list*。

(1)如果存在,并且$a_i=0$,返回s_{ID_i}给敌手A_1。

(2)否则,挑战者随机选取$s_{ID_i}\in Z_q^*$,计算$P_{ID_i}=s_{ID_i}P$,将$(ID_i,s_{ID_i},P_{ID_i},0)$加入*pk-list*中,返回$s_{ID_i}$给敌手$A_1$。

用户公钥替换:敌手随机选择$P'_{ID_i}\in G_1$替换用户ID_i的公钥,挑战者查询*pk-list*。

(1)如果存在$(ID_i,\perp,P_{ID_i},1)$形式元组,则用元组$(ID_i,\perp,P'_{ID_i},1)$替换元组$(ID_i,\perp,P_{ID_i},1)$。

(2)否则如果存在$(ID_i,s_{ID_i},P_{ID_i},0)$形式元组,将元组$(ID_i,\perp,P'_{ID_i},1)$加入*pk-list*。

(3)否则,挑战者随机选取$s_{ID_i}\in Z_q^*$,计算$P_{ID_i}=s_{ID_i}P$,将元组$(ID_i,s_{ID_i},P_{ID_i},0)$和$(ID_i,\perp,P'_{ID_i},1)$加入*pk-list*中。

H_1询问:挑战者B保存一个包含元组(m_i,U_i,T_i,h_i)的列表H_1-*list*,初始化为空。敌手询问(m_i,U_i,T_i),挑战者随机选择$h_i\in Z_q^*$,添加(m_i,U_i,T_i,h_i)到H_1-*list*中,返回h_i给敌手。

签名询问:敌手询问$(m_k,ID_i,ID_j,P'_{ID_i})$(第$k$次签名询问,签名者为$ID_i$,指定验证者为$ID_j$,签名者的公钥为$P'_{ID_i}$)。

(1)如果$ID_i\notin\{ID_A,ID_B\}$,挑战者随机选择$r_k\in Z_q^*$,计算$U_k=r_kQ_{ID_j}$,$h_k=H_1(m,U_k,s_{ID_j}P'_{ID_i})$,$V_k=(h_k/r_k)D_{ID_i}$,$\delta_k=(U_k,V_k)$,返回$\delta_k$给敌手。

(2)如果$ID_j\notin\{ID_A,ID_B\}$,挑战者随机选择$r_k\in Z_q^*$,计算$U_k=r_kQ_{ID_i}$,$h_k=H_1(m,U_k,s_{ID_j}P'_{ID_i})$,$V_k=(h_k/r_k)D_{ID_j}$,$\delta_k=$

(U_k, V_k)，返回 δ_k 给敌手。

(3)否则，挑战者拒绝敌手请求。

验证询问：敌手询问$(m_k, \delta_k, ID_i, ID_j, P'_{ID_i})$，$\delta_k=(U_k, V_k)$(第 k 次验证询问，签名者为 ID_i，指定验证者为 ID_j)。

(1)如果 $ID_i \notin \{ID_A, ID_B\}$，挑战者计算 $h_k = H_1(m_k, U_k, s_{ID_j}P'_{ID_i})$，验证 $e(V_k, U_k) \stackrel{?}{=} e(h_k D_{ID_i}, Q_{ID_j})$。如果成立，敌手认为$(m_k, \delta_k, ID_i, ID_j, P'_{ID_i})$是有效的签名，否则是无效签名。

(2)否则如果 $ID_j \notin \{ID_A, ID_B\}$，挑战者计算 $h_k = H_1(m_k, U_k, s_{ID_j}P'_{ID_i})$，验证 $e(V_k, U_k) \stackrel{?}{=} e(h_k Q_{ID_i}, D_{ID_j})$。如果成立，敌手认为$(m_k, \delta_k, ID_i, ID_j, P'_{ID_i})$是个有效的签名，否则是无效签名。

(3)否则$\{ID_i, ID_j\}=\{ID_A, ID_B\}$，挑战者拒绝敌手请求。

伪造：敌手输出一个有效的指定验证者签名$(m^*, \sigma^*, ID_A, ID_B, P'_{ID_A})$，$\delta^*=(U^*, V^*)$。敌手在 H_1-*list* 中查询$(m^*, U^*, s_{ID_B}P'_{ID_A})$，得到$(m^*, U^*, s_{ID_B}P'_{ID_A}, h^*)$，因为 $e(V^*, U^*)=e(h^* Q_{ID_A}, D_{ID_B})$，所以 $e(V^*, U^*)^{h^{*-1}} = e(Q_{ID_A}, D_{ID_B})=e(aP, bcP)=e(P, P)^{abc}$，即 B 可以成功地解决 CBDH 问题。

定理 2 在随机预言模型下，基于 CDH 困难问题，我们的方案对第二类攻击者是存在不可伪造的。

证明：给定一个 CDH 问题实例 $P, P_1, P_2 \in G_1$，其中 $P_1=aP$，$P_2=bP$，a, b 未知。构造算法 B，利用敌手 A_{II} 计算 $abP \in G_1$ 的值。在证明过程中假设敌手 A_{II} 不会重复两个相同请求。

设置：输入安全参数 l，输出系统参数$\{G_1, G_2, q, e, P\}$。方案中的两个目标用户分别为签名者 ID_A 和指定验证者 ID_B。B 随机选择 $s \in Z_q^*$，计算 $P_{pub}=sP$，令 $P_{ID_A}=P_1=aP$，$P_{ID_B}=P_2=bP$。将$\{G_1, G_2, q, e, P, s, P_{pub}, P_{ID_A}, P_{ID_B}\}$发送给敌手 A_{II}。

H_0 询问：挑战者 B 保存了一个包含元组(ID_i, Q_{ID_i})的列表 H_0-*list*，初始化为空。敌手 A_I 询问 ID_i，随机选择 $Q_{ID_i} \in G_1$，将(ID_i, Q_{ID_i})加入 H_0-*list* 中，返回 Q_{ID_i} 给敌手。

公钥询问：挑战者 B 保存了一个包含元组$(ID_i, s_{ID_i}, P_{ID_i})$元组的列表 *pk-list*，初始化为$\{(ID_A, \perp, P_{ID_A}), (ID_B, \perp, P_{ID_B})\}$。敌手 A_{II} 询问 ID_i 的公钥，挑战者查询 *pk-list*。

(1)如果存在，返回 P_{ID_i}。

(2)否则，随机选取 $s_{ID_i} \in Z_q^*$，计算 $P_{ID_i}=s_{ID_i}P$，将$(ID_i, s_{ID_i}, P_{ID_i})$加入 *pk-list* 中，返回 P_{ID_i} 给敌手。

秘密值询问：敌手 A_{II} 询问 ID_i 的秘密值 $ID_i \notin \{ID_A, ID_B\}$，挑战者查询 *pk-list*。

(1)如果存在，返回 s_{ID_i} 给敌手 A_{II}。

(2)否则，随机选取 $s_{ID_i} \in Z_q^*$，计算 $P_{ID_i}=s_{ID_i}P$，将$(ID_i, s_{ID_i}, P_{ID_i})$加入 *pk-list* 中，返回 s_{ID_i} 给敌手 A_{II}。

H_1 询问：挑战者保存一个包含(m_i, U_i, T_i, h_i)元组的列表 H_1-*list*，初始化为空。敌手询问(m_i, U_i, T_i)，挑战者随机选择 $h_i \in Z_q^*$，添加(m_i, U_i, T_i, h_i)到 H_1-*list* 中，返回 h_i 给敌手。

签名询问：敌手询问(m_k, ID_i, ID_j)。

(1)如果 $ID_i \notin \{ID_A, ID_B\}$，挑战者随机选择 $r_k \in Z_q^*$，计算 $U_k=r_k Q_{ID_j}$，$h_k=H_1(m, U, s_{ID_i}P_{ID_j})$，$V_k=(h_k/r_k)D_{ID_i}$，$\delta_k=(U_k, V_k)$，返回 δ_k 给敌手。

(2)如果 $ID_j \notin \{ID_A, ID_B\}$，挑战者随机选择 $r_k \in Z_q^*$，计算 $U_k=r_k Q_{ID_i}$，$h_k=H_1(m, U_k, s_{ID_j}P_{ID_i})$，$V_k=(h_k/r_k)D_{ID_j}$，$\delta_k=(U_k, V_k)$，返回 δ_k 给敌手。

(3)否则挑战者拒绝敌手请求。

验证请求：敌手询问$(m_k, \delta_k, ID_i, ID_j)$，$\delta_k=(U_k, V_k)$。

(1)如果$\{ID_i, ID_j\}=\{ID_A, ID_B\}$，挑战者拒绝敌手请求。

(2)如果 $ID_i \notin \{ID_A, ID_B\}$，挑战者计算 $h=H_1(m_k, U_k, s_{ID_i}P_{ID_j})$，验证 $e(V_k, U_k) \stackrel{?}{=} e(h_k D_{ID_i}, Q_{ID_j})$，如果成立，敌手认为$(m_k, \delta_k, ID_i, ID_j)$是个有效的签名，否则是无效签名。

(3)如果 $ID_j \notin \{ID_A, ID_B\}$，挑战者计算 $h_k=H_1(m_k, U_k, s_{ID_j}P_{ID_i})$，验证 $e(V_k, U_k) \stackrel{?}{=} e(h_k Q_{ID_i}, D_{ID_j})$，如果成立，敌手认为$(m_k, \delta_k, ID_i, ID_j)$是个有效的签名，否则是无效签名。

伪造：敌手输出一个有效的指定验证者签名$(m^*, \delta^*, ID_A, ID_B)$，$\delta^*=(U^*, V^*)$。挑战者在 H_1-*list* 中查询(m^*, U^*)，如果不能得到一个满足 $e(V^*, U^*)=e(h^* Q_{ID_A}, D_{ID_B})$ 的元组(m^*, U^*, T^*, h^*)，则失败；否则 $T^*=s_{ID_A}s_{ID_B}P=abP$。挑战者成功地解决了 CDH 问题。

6 计算代价与通信代价分析

表 1 分析了本文提出的高效的指定验证者签名方案的计算代价与通信代价，其中需要用到的标识符如下：$|Z_q|$ 为 Z_q 中元素的长度；$|G_1|$ 为 G_1 中元素的长度；$|G_2|$ 为 G_2 中元素的长度；BP 为双线性对操作；E 为 G_1 中的指数操作；PA 为 G_1 中元素上的加法操作；INV 为 Z_q 上的求逆运算；H 为 hash 操作。

表 1 计算代价与通信代价分析

	签名	验证	签名长度
Huang[14]方案	1 BP+1H+1E+1PA+1INV	3BP+1H+1E+1PA	$\|Z_q\|$
Chen[15]方案	1 BP+1H+1E	1 BP+1H+1E	$\|Z_q\|$
Yang[16]方案	1 BP+1H+4E+1PA	1 BP+1H+2E+1PA	$\|G_1\|+\|G_2\|$
本文方案	1H+3E+1INV	2BP+1H+2E	$2\|G_1\|$

结束语 无证书的公钥密码体制不需要公钥证书，并且消除了基于身份的密码体制中的密钥托管问题，在实际中具有很好的应用。本文给出了无证书指定验证者签名的定义和安全模型，并提出了一个无证书指定验证者签名方案。该方案在随机预言模型下对自适应选择消息攻击是存在不可伪造的，并且具有较好的计算代价和通信代价。目前提出的指定验证者签名方案均没有考虑密钥泄漏问题，我们将使用前向安全技术[22]、密钥隔离技术[23]和弹性泄漏密码技术[24]来解决指定验证者签名方案中的密钥泄漏问题。

参 考 文 献

[1] Jakobsson M, Sako K, Impagliazzo R. Designated Verifier Proofs and Their Applications [C]// Proceedings of the Eurocrypt'96. LNCS 1070, Berlin: Springer-Verlag, 1996: 143-154

[2] Saeednia S, Kramer S, Markowitch O. An Efficient Strong Designated Verifier Signature Scheme [C]// Proceedings of the 6th International Conference on Information Security and Cryptology 2003. LNCS 2971, Berlin: Springer-Verlag, 2004: 40-54

[3] Huang X, Mu Y, Susilo W, et al. Short Designated Verifier Proxy Signature from Pairings [C]// The First International Work shop on Security in Ubiquitous Computing Systems. LNCS 3823, Berlin: Springer Verlag, 2005: 835-844

(下转第 166 页)

像加上密文态的补偿矩阵来对图像进行恢复，是无法得到正确的图像的。

结束语 本文基于空域可恢复信息隐藏，提出了一种可完整精确恢复原始图像的人工退化算法；利用控制因子实现了对嵌入深度的控制，使得嵌入端可以控制最后图像的失真程度；并且通过置乱、加密等安全措施，保证了只有合法的接收端可以获得正确的原始图像。

参 考 文 献

[1] 赵亮，廖晓峰，向涛，等. 基于Z矩阵映射和选择加密的彩色图像退化算法研究[J]. 物理学报，2010，59(3)：1507-1523

[2] Huang H-C, Chang F-C, Fang W-C. Reversible Data Hiding with Histogram-Based Difference Expansion for QR code Application[J]. IEEE Transactions on Consumer Electronics，2010，57(7)：779-787

[3] Wang J X, LU Z M. A Path Optional Lossless Data Hiding Scheme Based on VQ Joint Neighboring Coding[J]. Information Sciences，2009，19(9)：3332-3348

[4] Jung S W，Ha L T，Ko S J. A new histogram modification based reversible data hiding algorithm considering the human visual system[J]. IEEE Signal Processing Letters，2011，18(2)：721-724

[5] Lin C C，Tai W L，Chang C C. Multilevel Reversible Data Hiding Based on Histogram Modification of difference images[J]. Pattern Recognition，2009，41(12)：3582-3591

[6] 柳玲，陈同孝，曹晨，等. 一种随机嵌入抗SPAM检测的可逆数据隐藏算法[J]. 计算机应用研究，2013，30(7)：2111-2114

[7] 邱应强. 一种大嵌入容量的可逆数据隐藏方法[J]. 计算机应用研究，2014，31(3)：850-852

[8] Deng C, Gao X B, Li X L, et al. A local Tchebichef moments-based robust image watermarking[J]. Signal Processing，2009，89(8)：1531-1539

[9] Gao X-B，Deng C，et al. Geometric distortion insensitive image watermarking in affine covariant regions[J]. IEEE Transactions on System，Man and Cybernetics，2010，40(3)：278-286

[10] 肖旭韬，张雪锋. 基于线性反馈移位寄存器和组合猫映射的伪随机序列生成方法[J]. 计算机应用研究，2013，30(1)：161-164

(上接第135页)

[4] Tso R, Okamoto T, Okamoto E. Practical Strong Designated Verifier Signature Schemes Based on Double Discrete Logarithms[C]//CISC 2005. LNCS 3822，Berlin：Springer-Verlag，2005：113-127

[5] Huang Q, Yang G M, Wong D S, et al. Efficient Strong Designated Verifier Signature Schemes without Random Oracle or with Non-delegatability [J]. International Journal of Information Security，2011，10(6)：373-385

[6] Susilo W, Zhang F, Mu Y. Identity-based Strong Designated Verifier Signature Schemes [C]// Proceedings of the ACISP 2004. LNCS 3108，Berlin：Springer-Verlag，2004：313-324

[7] Huang X，Susilo W，Mu Y，et al. Short (Identity-Based) Strong Designated Verifier Signature Schemes [C]//Proceedings of the ISPEC 2006. LNCS 3903，Berlin：Springer-Verlag，2006：214-225

[8] 王晓峰，张璟，王尚平，等. 新的基于身份的广义指定验证者签名方案[J]. 电子学报，2007，35(8)：1432-1436

[9] Zhang Jian-hong. A Novel ID-based Designated Verifier Signature Scheme [J]. Information Science，2008，178(3)：766-773

[10] Yang Bo，Xiao Zi-bi，Hu Zheng-ming. A Secure ID-Based Strong Designated Verifier Signature Scheme [C]//Proceedings of the IC-NIDC 2009. IEEE，2009：543-547

[11] Kang Bao-yuan. A Novel Identity-based Strong Designated Verifier Signature Scheme [J]. Journal of Systems and Software，2009，82(2)：270-273

[12] 张学军. 高效的基于身份的指定验证者签名[J]. 计算机工程，2009，35(5)：131-132

[13] 邵健，曹珍富，魏立斐. 基于身份的强指定验证者签名方案 [J]. 计算机工程，2010，36(8)：167-169

[14] Huang X，Susilo W，Mu Y，et al. Certificateless Designated Verifier Signature Schemes[C]// Proceedings of the 20th International Conference on Advanced Information Networking and Applications 2006. IEEE，2006：15-19

[15] Chen Hu，Song Ru-shun，Zhang Fu-tai，et al. An Efficient Certificateless Short Designated Verifier Signature Scheme [C]// Proceedings of the Wireless Communications，Networking and Mobile Computing 2008. IEEE，2008：1-6

[16] Yang Bo，Hu Zheng-ming，Xiao Zi-bi. Efficient Certificateless Strong Designated Verifier Signature Scheme [C]//2009 International Conference on Computational Intelligence and Security. IEEE，2009：432-436

[17] Ming Yang，Shen Xiao-qin，Wang Yu-min. Certificateless Universal Designated Verifier Signature Schemes [J]. The Journal of China Universities of Posts and Telecommunications，2007，14(3)：85-94

[18] 韩亚宁，王彩芬. 无证书的广义指定多个验证者签名体制 [J]. 计算机应用研究，2009，26(6)：2158-2161

[19] Miyaji A，Nakabayashi M，Takano S. New Explicit Conditions of Elliptic Curve Traces for FR-reduction [J]. IEICE Trans. on Fundamentals，2002，E85-A(2)：481-484

[20] Koblitz N，Menezes A. Pairing-based Cryptography at High Security Levels [C]// Cryptography and Coding'2005. Berlin：Springer-Verlag，2005：13-36

[21] Chatterjee S，Hankerson D，Knapp E，et al. Comparing Two Pairing-based Aggregate Signature Schemes [J]. Designs，Codes and Cryptography，2010，55(2/3)：141-167

[22] Li Ji-guo，Teng Hui-yun，Huang Xin-yi，et al. A Forward-Secure Certificate-Based Signature Scheme in the Standand Model[J]. The Computer Journal，2012，7672：362-376

[23] Li Ji-guo，Du Hai-ting，Zhang Yi-chen，et al. Provably Secure Certificate-based Key-Insulated Signature Scheme[J]. Concurrency and Computation Practice and Experience，2014，26：1546-1560

[24] Naor M，Segev G. Public-key Cryptosystems Resilient to Key Leakage [J]. SIAM J. Comput，2010，41(4)：772-814