基于证书强指定验证者签名方案

李继国[1)] 钱 娜[1)] 黄欣沂[2),3)] 张亦辰[1)]

[1)](河海大学计算机与信息学院计算机系 南京 210098)

[2)](新加坡管理大学信息系统学院 新加坡)

[3)](福建师范大学数学与计算机科学学院 福州 350007)

摘 要 借鉴无证书指定验证者签名的思想,提出了基于证书密码体制的强指定验证者签名的概念和安全模型.构造了基于证书的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.基于GBDH困难问题假定,在随机预言模型下证明了方案对适应性选择消息攻击是存在不可伪造的.提出的方案较好地解决了基于身份指定验证者签名中的密钥托管问题.此外,提出的方案具有通信代价低、能够抵抗密钥替换攻击等优点.

关键词 公钥密码学;基于证书签名;强指定验证者签名;GBDH问题;随机预言模型

中图法分类号 TP309 **DOI号**: 10.3724/SP.J.1016.2012.01579

Certificate-Based Strong Designated Verifier Signature Scheme

LI Ji-Guo[1)] QIAN Na[1)] HUANG Xin-Yi[2),3)] ZHANG Yi-Chen[1)]

[1)](*Department of Computer, College of Computer & Information Engineering, Hohai University, Nanjing* 210098)

[2)](*School of Information Systems, Singapore Management University, Singapore*)

[3)](*School of Mathematics and Computer Science, Fujian Normal University, Fuzhou* 350007)

Abstract Inspired by the idea of the certificateless designated verifier signature, we propose the notion and security model of the certificate-based strong designated verifier signature (CBSDVS). Then, we construct the CBSDVS scheme and analyze the computation cost and communication bandwidth of our scheme. Furthermore, we prove that our scheme is existentially unforgeable against adaptive chosen message attack under the assumption of the gap bilinear Diffie-Hellman problem in the random oracle model. The proposed scheme partially solves key escrow problem in identity-based designated verifier signature. In addition, the proposed scheme has low communication bandwidth and can resist against key replacement attack.

Keywords public key cryptography; certificate-based signature; strong designated verifier signature; GBDH problem; random oracle model

1 引 言

Jakobsson等人[1]在1996年欧密会(Eurocrypt Conference)上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

收稿日期:2010-05-20;最终修改稿收到日期:2011-10-31.本课题得到国家自然科学基金(60842002,61003232,61072080,61103183,61103184)、中央高校基本科研业务费专项资金项目(2009B21114,2010B07114)、江苏省"六大人才高峰"项目(2009182)、河海大学优秀创新人才支持计划、网络安全与密码技术福建省高校重点实验室开放课题(2011001)资助.**李继国**,男,1970年生,博士,教授,博士生导师,主要研究领域为信息安全、密码学理论与技术.E-mail: ljg1688@163.com; lijiguo@hhu.edu.cn. **钱 娜**,女,1984年生,硕士,主要研究方向为密码学理论与技术. **黄欣沂**,男,1981年生,博士,主要研究方向为信息安全、密码学理论与技术. **张亦辰**,女,1971年生,博士研究生,讲师,主要研究方向为密码学理论与技术.

名的验证.这样既解决了普通签名中任何人都可以验证签名的问题,又解决了不可否认签名中签名人完全控制签名的问题.

指定验证者签名的概念随后被扩展到强指定验证者签名[2]和广义指定验证者签名[3].强指定验证者签名中任何人都能生成一个与原始签名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.在强指定验证者签名中,知道两个可能的签名者(A_0,A_1)和指定验证者 B 的公钥,任何人无法区分一个指定验证者签名是 A_0 指定验证者 B 的签名还是 A_1 指定验证者 B 的签名.广义指定验证者签名具有保护签名持有者隐私的特殊性质,即允许任何一个签名持有者(可以不是签名者)通过引入验证者的公钥将签名指定给他所期望的任意指定验证者,指定验证者能够验证签名有效性,但无法使其他人相信这个事实.

原始的指定验证者签名多是基于传统的公钥密码体制.传统的公钥密码体制中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联系起来,所以在验证一个签名之前首先需要验证公钥的有效性.2004 年,Susilo、Zhang 和 Mu[4]提出了基于身份的强指定验证者签名.2009 年,Kang 等人[5]提出了基于身份的强指定验证者签名方案的安全模型并给出了一个具体的构造.上述方案较好地解决了传统公钥密码体制的两次验证问题,可是基于身份的指定验证者签名存在密钥托管问题.2007 年,王晓峰等人[6]提出了新的基于身份的广义指定验证者签名方案,通过引入两个 PKG 的方法部分解决密钥托管问题.为了更好地解决密钥托管问题,很多专家学者提出了无证书的指定验证者签名方案[7-8].2006 年 Huang、Susilo、Mu 和 Zhang[7]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,解决了传统公钥密码体制和基于身份密码体制中存在的固有问题.2008 年,Chen 等人[8]也提出了一个高效的无证书短指定验证者签名方案.随后,Yang 等人[9-10]首先形式化了无证书强指定验证者签名的定义和安全模型并提出了一个较为高效的无证书强指定验证者签名方案.但是,无证书公钥密码体制中仍存在需要安全通道来传输秘密值的缺陷.

在 2003 年的欧密会上,Gentry[11]提出了基于证书密码体制,克服了基于身份公钥密码体制和传统公钥密码体制的缺陷.因为证书只是为了证明用户公钥的真实性以及与身份的惟一对应关系,证书并不需要保密,所以很好地解决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.与无证书公钥密码体制相比,由于证书的存在,它也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 KGC 与用户之间的密钥传递需要安全信道问题.在 CT-RSA'04 上,Kang 和 Park 等人[12]首次提出了基于证书签名方案,并在随机预言模型证明了安全性.Li 等人[13]把密钥替换攻击引入到基于证书密码体制中,指出 Kang 和 Park 等人[12]提出的基于证书签名方案不能抵抗密钥替换攻击,并且对 Kang 和 Park 等人的基于证书签名方案的安全模型进行了增强.进一步,基于计算 Diffie-Hellman 假定他们提出了一个新的基于证书签名方案,并在增强的安全模型下证明了方案的安全性.与现有的基于证书签名方案相比,提出的方案具有签名长度短,计算代价低等优点.Wu 等人[14]提出了一个更加合理和精确的基于证书签名的安全定义.在该定义中,根据攻击者具有的能力区分了三种类型的攻击者.进一步,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,并证明了方案的安全性.Au 等人[15]提出了基于证书的环签名方案,较好地解决了传统 PKI 中复杂的证书链验证问题,并在随机预言模型下证明了方案的安全性.Liu 等人[16]提出两个新型的基于证书签名方案,一个是不使用双线性对的方案,在计算代价上具有一定优势,另一个方案是在标准模型下证明方案的安全性.Zhang[17]指出 Liu 等人[16]提出的不使用双线性对的基于证书签名方案是不安全的.2009 年,Li 等人[18]提出了一个基于证书代理签名方案,并在随机预言模型下证明了方案的安全性.Ming 和 Wang[19]提出了一个高效的基于证书签名方案.2010 年,Li 等人[20]提出两个能抵抗密钥替换攻击的基于证书签名方案.第一个方案,基于计算 Diffie-Hellman 假定,在随机预言模型下证明提出的方案对自适应选择消息攻击是存在不可伪造的,具有较短的签名长度,较小的计算代价等优点,是一个可证安全的高效签名方案.第二个方案,首次构造了标准模型下安全的基于证书签名方案,并在计算 Diffie-Hellman 假定下证明方案对自适应选择消息攻击是存在不可伪造的.最近,Li 等人[21]提出一个基于证书的高效短签名方案,签名和验证仅需一个 Pairing 运算,签名长度为一个群元素,非常适合于计算和应用在带宽受限的网络环境中.

本文将基于证书的概念引入到指定验证者签名中，借鉴无证书指定验证者签名的思想，提出了基于证书强指定验证者签名的概念和安全模型. 基于GBDH困难问题假定，构造了一个基于证书强指定验证者签名方案，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. 较好地解决了传统公钥密码体制签名中需要二次验证的问题、密钥替换攻击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 $e:G_1\times G_1\rightarrow G_2$ 如果满足以下性质，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，$e:G_1\times G_1\rightarrow G_2$ 是双线性映射.

定义 2.　CBDH 问题(Computational Bilinear Diffie-Hellman Problem). 给定 $P,aP,bP,cP\in G_1$，其中 $a,b,c\in Z_q^*$ 且未知，计算 $e(P,P)^{abc}\in G_2$.

定义 3.　DBDH 问题(Decisional Bilinear Diffie-Hellman Problem). 给定 $P,aP,bP,cP\in G_1$，其中 $a,b,c\in Z_q^*$ 且未知，并给定 $h\in G_2$，判定 $h=e(P,P)^{abc}$ 是否成立，如果成立则输出 1；否则输出 0.

定义 4.　GBDH 问题(Gap Bilinear Diffie-Hellman Problem). 给定 $P,aP,bP,cP\in G_1$，其中 $a,b,c\in Z_q^*$ 且未知，在 DBDH 预言机的帮助下，计算 $e(P,P)^{abc}\in G_2$ 的值.

3　基于证书强指定验证者签名的定义和安全模型

3.1　基于证书强指定验证者签名的定义

基于证书强指定验证者签名(CBSDVS)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 CA. 该系统由设置、用户密钥产生、证书产生、签名、验证、副本模拟 6 个算法组成.

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

用户密钥产生：输入参数 $params$，输出用户的私钥-公钥对 (s_{ID_i},P_{ID_i})，$i=A,B$.

证书产生：输入参数 $params$、用户的身份 ID_i、公钥 P_{ID_i} 以及主密钥 msk，CA 生成该用户的证书 $cert_{ID_i}$，$i=A,B$.

签名：输入参数 $params$、消息 m、ID_A 的证书 $cert_{ID_A}$、私钥 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 的私钥 s_{ID_B}、证书 $cert_{ID_B}$ 以及 ID_A 的公钥 P_{ID_A}，判断签名 δ 是否是消息 m 上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　基于证书强指定验证者签名的安全模型

类似于无证书指定验证者签名方案，基于证书强指定验证者签名方案也定义了两类具有不同能力的敌手. 第一类敌手 A_{I} 可以按照自己的意愿替换所有用户的公钥，并得到替换公钥后对应的私钥，并且能够得到除目标指定验证者之外用户的私钥. 还能得到除目标签名者以外的用户的证书和替换公钥后的证书，但是不能得到主密钥. 这类敌手还可以欺骗任意第三方用替换后的公钥来验证签名有效性. 第二类敌手 A_{II} 模仿一个恶意的证书发放者，拥有主密钥，故可以产生任意用户的证书. 基于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.

3.2.1　CBSDVS 游戏 1

用以下挑战者与敌手交互的游戏，模拟第一类敌手的适应性选择消息攻击.

(1) 初始化. 挑战者运行设置算法产生系统参数 $param$ 和主公钥 mpk，并公开参数 $params=\{param,mpk\}$. 同时，挑战者运行用户密钥产生算法产生 P_{ID_i}，$i=A,B$.

(2) 用户公钥替换. 敌手 A_{I} 随机选择公钥 P'_{ID_i} 替换任何用户 ID_i 的公钥 P_{ID_i}，并且 A_{I} 知道 P'_{ID_i} 对应的私钥 s'_{ID_i}.

(3) 密钥询问. 敌手 A_{I} 询问除指定验证者 ID_B 之外的用户 ID_i 的私钥 s_{ID_i}，运行用户密钥产生算法产生用户的私公钥对 (ID_i,s_{ID_i},P_{ID_i})，$i\in\{1,2,\cdots\}$，

将 s_{ID_i} 返回给敌手 A_{I}.

(4) 证书询问. 敌手 A_{I} 询问除目标签名者 ID_A 之外的用户 (ID_i, P_{ID_i}) 对应的证书,运行证书产生算法产生 $cert_{ID_i}$,返回 $cert_{ID_i}$ 给敌手 A_{I}.

(5) 签名询问. 询问对消息 m 的签名,用签名算法产生签名 δ,返回 δ 给敌手 A_{I}.

(6) 验证询问. 询问消息签名对 (m, δ, P_{ID_A}),运行验证算法判断是否是有效的消息签名对,返回 $d \in \{acc, rej\}$ 给 A_{I}.

(7) 伪造. 敌手 A_{I} 给出三元组 $(m^*, \delta^*, P^*_{ID_A})$ 满足:

(a) δ^* 是在公钥 $P^*_{ID_A}$ 下对消息 m^* 的有效签名,且 m^* 没有在签名询问中询问过;

(b) ID_B 都没有在密钥询问中出现过;

(c) ID_A 没有在证书询问中出现过.

3.2.2 CBSDVS 游戏 2

用以下挑战者与敌手交互的游戏,模拟第二类敌手的适应性选择消息攻击.

(1) 初始化. 挑战者运行设置算法产生系统参数 $param$,主密钥和主公钥对 (msk, mpk),并公开参数 $params = \{param, msk, mpk\}$. 同时,挑战者运行用户密钥产生算法产生 $P_{ID_i}, i = A, B$.

(2) 密钥询问. 询问非目标用户(除目标签名者 ID_A 和目标指定验证者 ID_B 之外的用户) ID_i 的私钥 s_{ID_i},运行用户密钥产生算法产生用户的私公钥对 $(ID_i, s_{ID_i}, P_{ID_i}), i \in \{1, 2, \cdots\}$,将 s_{ID_i} 返回给敌手 A_{II}.

(3) 签名询问. 对消息 m 进行签名询问,用签名算法产生签名 δ,返回 δ 给敌手 A_{II}.

(4) 验证询问. 询问消息签名对 (m, δ),运行验证算法判断是否是有效的消息签名对,返回 $d \in \{acc, rej\}$ 给敌手 A_{II}.

(5) 伪造. 敌手给出二元组 (m^*, δ^*) 满足以下条件:

(a) δ^* 是对消息 m^* 的有效签名,且 m^* 没有在签名询问中询问过;

(b) ID_A, ID_B 都没有在密钥询问中出现过.

4 基于证书强指定验证者签名方案

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;$e: G_1 \times G_1 \to G_2$ 是双线性映射.

CA 做如下操作:

(1) 随机选择秘密值 $s \in Z_q^*$,作为主密钥 $msk = s$,计算它的主公钥 $mpk = P_{\mathrm{pub}} = sP$.

(2) 选择两个 Hash 函数 $H_0: \{0,1\}^* \times G_1 \to G_1$; $H_1: \{0,1\}^* \times G_2 \times G_2 \to G_1$.

(3) 公开参数 $params = (G_1, G_2, q, e, P, H_0, H_1, P_{\mathrm{pub}})$,主密钥 $msk = s$ 保密.

用户密钥产生:用户 ID_i 选择自己的私钥 s_{ID_i},计算对应的公钥 $P_{ID_i} = s_{ID_i} P$,生成自己的私公钥对 $(s_{ID_i}, P_{ID_i}), i \in \{A, B\}$.

证书产生:*CA* 用系统参数和主密钥 msk 来产生用户证书.

(1) 用户 ID_i 发送一个数据串 $data$ 给 *CA*,这个数据串包含了用户的公钥信息 P_{ID_i} 和身份信息 ID_i.

(2) *CA* 像传统 PKI 注册公钥一样验证用户信息,如果满足公钥 P_{ID_i} 是用户 ID_i 的有效公钥,计算 $Q_{ID_i} = H_0(ID_i, P_{ID_i}) \in G_1$, $cert_{ID_i} = sQ_{ID_i}$,并将证书 $cert_{ID_i}$ 发送给用户 $ID_i, i \in \{A, B\}$.

签名:用户 ID_A 对消息 m 签名,并指定验证者 ID_B.

$$K_1 = e(cert_{ID_A} + s_{ID_A} Q_{ID_A}, P_{ID_B}),$$

$$K_2 = e(P_{\mathrm{pub}} + P_{ID_B}, s_{ID_A} Q_{ID_B}),$$

$$\delta = H_1(m, K_1, K_2).$$

验证:用户 ID_B 验证签名的有效性.

$$\delta \stackrel{?}{=} H_1(m, e(s_{ID_B} Q_{ID_A}, P_{\mathrm{pub}} + P_{ID_A}), e(P_{ID_A}, cert_{ID_B} + s_{ID_B} Q_{ID_B})).$$

副本模拟:用户 ID_B 能够生成有效的副本.

$$K_1' = e(s_{ID_B} Q_{ID_A}, P_{\mathrm{pub}} + P_{ID_A}),$$

$$K_2' = e(P_{ID_A}, cert_{ID_B} + s_{ID_B} Q_{ID_B}),$$

$$\delta' = H_1(m, K_1', K_2').$$

对于基于证书强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.

$$\begin{aligned} K_1 &= e(cert_{ID_A} + s_{ID_A} Q_{ID_A}, P_{ID_B}) \\ &= e(sQ_{ID_A} + s_{ID_A} Q_{ID_A}, P_{ID_B}) \\ &= e((s + s_{ID_A}) Q_{ID_A}, s_{ID_B} P) \\ &= e(s_{ID_B} Q_{ID_A}, (s + s_{ID_A}) P) \\ &= e(s_{ID_B} Q_{ID_A}, sP + s_{ID_A} P) \\ &= e(s_{ID_B} Q_{ID_A}, P_{\mathrm{pub}} + P_{ID_A}), \\ K_2 &= e(P_{\mathrm{pub}} + P_{ID_B}, s_{ID_A} Q_{ID_B}) \\ &= e(sP + s_{ID_B} P, s_{ID_A} Q_{ID_B}) \\ &= e((s + s_{ID_B}) P, s_{ID_A} Q_{ID_B}) \\ &= e(s_{ID_A} P, (s + s_{ID_B}) Q_{ID_B}) \\ &= e(P_{ID_A}, cert_{ID_B} + s_{ID_B} Q_{ID_B}), \end{aligned}$$

$\delta=H_1(m,K_1,K_2)=H_1(m,e(s_{ID_B}Q_{ID_A},P_{\text{pub}}+P_{ID_A}),e(P_{ID_A},cert_{ID_B}+s_{ID_B}Q_{ID_B}))$.

5　安全性分析

定理 1.　假设敌手 A_{I} 是 CBSDVS 方案的第一类适应性选择消息攻击敌手，在最多询问了 q_{H_1} 个 H_1 询问、q_S 个签名询问、q_V 个验证询问之后，能够伪造成功的概率是 ε. 存在一个算法 B 可以利用 A_{I} 以概率 $\varepsilon'\geqslant(1-1/(2^l-q_{H_1}-q_S))^{q_V+1}\varepsilon$ 解决 GBDH 问题，其中 l 是 CBSDVS 方案的安全参数.

证明.　给定一个 GBDH 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. 我们构造算法 B，B 模拟挑战者与敌手 A_{I} 交互，并在 DBDH 预言机的帮助下，计算 $e(P,P)^{abc}\in G_2$ 的值. 在证明过程中我们假设敌手 A_{I} 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为签名者 ID_A 和指定验证者 ID_B. B 令 $P_{\text{pub}}=P_1=aP,P_{ID_B}=P_2=bP$，随机选择 $s_{ID_A}\in Z_q^*$，计算 $P_{ID_A}=s_{ID_A}P$. 将 $\{G_1,G_2,q,e,P,P_{\text{pub}},s_{ID_A},P_{ID_A},P_{ID_B}\}$ 发送给敌手 A_{I}.

密钥询问：B 保存一个 $(ID_i,s_{ID_i},P_{ID_i},a_i)$ 元组的列表 L，这个列表初始化为 $\{(ID_A,s_{ID_A},P_{ID_A},0),(ID_B,\perp,P_{ID_B},0)\}$. 敌手 A_{I} 询问 ID_i，B 随机选择 $s_{ID_i}\in Z_q^*$，计算 $P_{ID_i}=s_{ID_i}P$，将 $(ID_i,s_{ID_i},P_{ID_i},0)$ 加入到 L 中，返回 s_{ID_i} 给敌手 A_{I}.

替换公钥：敌手 A_{I} 替换用户 ID_i 的公钥为 P'_{ID_i}，其中 $P'_{ID_i}=s'_{ID_i}P$（s'_{ID_i} 已知），将 L 中的 $(ID_i,*,*,*)$ 替换为 $(ID_i,s'_{ID_i},P'_{ID_i},1)$.

H_0 询问：B 保存一个 $(ID_i,\alpha_{ID_i},Q_{ID_i})$ 元组的列表 H_0，H_0 初始化为空. 敌手 A_{I} 询问 ID_i，B 查询 L.

(1) 如果 ID_i 在 L 中不存在，B 随机选择 $s_{ID_i}\in Z_q^*$，计算 $P_{ID_i}=s_{ID_i}P$，将 $(ID_i,s_{ID_i},P_{ID_i},0)$ 加入到 L 中. 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 中，返回 Q_{ID_i} 给敌手 A_{I}.

(2) 如果 ID_i 在 L 中已存在，

(a) 如果 $ID_i\neq ID_A$，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 中，返回 Q_{ID_i} 给敌手 A_{I}；

(b) 如果 $ID_i=ID_A$，随机选取 $\alpha_{ID_i}\in Z_q^*$，计算 $Q_{ID_i}=\alpha_{ID_i}P_3=\alpha_{ID_i}cP$，将 $(ID_i,\alpha_{ID_i},Q_{ID_i})$ 加入 H_0 中，返回 Q_{ID_i} 给敌手 A_{I}.

证书询问：敌手 A_{I} 询问用户 ID_i 的证书，B 查询 L 列表.

(1) 如果不存在，B 随机选择 $s_{ID_i}\in Z_q^*$，计算 $P_{ID_i}=s_{ID_i}P$，将 $(ID_i,s_{ID_i},P_{ID_i},0)$ 加入到 L 中. 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 中. 计算 $cert_{ID_i}=\alpha_{ID_i}P_{\text{pub}}$，并返回 $cert_{ID_i}$ 给敌手 A_{I}.

(2) 如果存在，

(a) 如果 $ID_i\neq ID_A$，查询 H_0，计算 $cert_{ID_i}=\alpha_{ID_i}P_{\text{pub}}$，返回 $cert_{ID_i}$ 给敌手 A_{I}；

(b) 否则 $ID_i=ID_A$，拒绝敌手请求.

H_1 询问：B 保存了一个 $(m_i,K_{1i},K_{2i},\delta_i,P^i_{ID_A})$ 元组的 H_1，这个列表初始化为空. 敌手 A_{I} 询问元组 (m_i,K_{1i},K_{2i}).

(1) 如果不存在元组 $(m_i,*,*,*,*)$ 在 H_1 中，B 随机选择 $\delta_i\in G_1$，满足 $(*,*,*,\delta_i,*)$ 不在 H_1 中，添加 $(m_i,K_{1i},K_{2i},\delta_i,\perp)$ 到 H_1 中，并返回 δ_i 给敌手 A_{I}.

(2) 如果存在元组 $(m_i,*,*,*,*)$ 在 H_1 中，

如果存在 $(m_i,K_{1j},K_{2j},\delta_j,\perp)$ 形式的元组，则 $(m_i,K_{1i},K_{2i})\neq(m_i,K_{1j},K_{2j})$，$B$ 随机选择 $\delta_i\in G_1$，满足 $(*,*,*,\delta_i,*)$ 不在 H_1 中，添加 $(m_i,K_{1i},K_{2i},\delta_i,\perp)$ 到 H_1 中，并返回 δ_i 给敌手 A_{I}；

否则存在 $(m_i,\perp,\perp,\delta_j,P^j_{ID_A})$ 形式的元组，验证 $K_{2i}\stackrel{?}{=}e(P^j_{ID_A},cert_{ID_B}+\alpha_{ID_B}P_{ID_B})$，且将 $(P,P_1,P_2,P_3,K_{1i}/e(Q_{ID_A},s^j_{ID_A}P_{ID_B}))$ 输入 DBDH 预言机，判断是否是 DBDH 元组（$P^j_{ID_A}$ 是指第 j 次签名询问时对应的 ID_A 的公钥的值）.

(a) 如果不同时满足上述两个条件，B 随机选择 $\delta_i\in G_1$，满足 $(*,*,*,\delta_i,*)$ 不在 H_1 中，添加 $(m_i,K_{1i},K_{2i},\delta_i,\perp)$ 到 H_1 中，并返回 δ_i 给敌手 A_{I}；

(b) 如果同时满足上述两个条件，B 用 $(m_i,K_{1i},K_{2i},\delta_j,P^j_{ID_A})$ 替换 H_1 中的 $(m_i,\perp,\perp,\delta_j,P^j_{ID_A})$ 元组，并返回 δ_j 给敌手 A_{I}.

签名询问：B 模拟签名算法，在任意时间敌手 A_{I} 可以询问签名算法. 在接收到敌手请求 $(m_i,P^i_{ID_A})$ 之后，B 检查 H_1.

(1) 如果不存在元组 $(m_i,*,*,*,*)$ 在 H_1 中，B 随机选择 $\delta_i\in G_1$，满足 $(*,*,*,\delta_i,*)$ 不在 H_1 中，添加 $(m_i,\perp,\perp,\delta_i,P^i_{ID_A})$ 到 H_1 中，并返回 δ_i 给敌手 A_{I}.

(2) 否则存在元组 $(m_i,*,*,*,*)$ 在 H_1 中.

如果存在 $(m_i,\perp,\perp,\delta_j,P^j_{ID_A})$ 形式的元组，则 $P^i_{ID_A}\neq P^j_{ID_A}$，$B$ 随机选择 $\delta_i\in G_1$，满足 $(*,*,*,\delta_i,*)$ 不在 H_1 中，添加 $(m_i,\perp,\perp,\delta_i,P^i_{ID_A})$ 到 H_1 中，并返回 δ_i 给敌手 A_{I}；

否则存在 $(m_i,K_{1j},K_{2j},\delta_j,\perp)$ 形式的元组，验

证 $K_{2j}\stackrel{?}{=}e(P^i_{ID_A},cert_{ID_B}+\alpha_{ID_B}P_{ID_B})$，且将$(P,P_1,P_2,Q_3,K_{1j}/e(Q_{ID_A},s^i_{ID_A}P_{ID_B}))$输入 DBDH 预言机，判断是否是 DBDH 元组.

(a) 如果不同时满足上述两个条件，B 随机选择 $\delta_i\in G_1$，满足$(*,*,*,\delta_i,*)$不在 H_1 中，添加$(m_i,\perp,\perp,\delta_i,P^i_{ID_A})$到 H_1 中，并返回 δ_i 给敌手 A_{I}；

(b) 如果满足上述两个条件，B 用元组$(m_i,K_{1j},K_{2j},\delta_j,P^i_{ID_A})$替换 H_1 中$(m_i,K_{1j},K_{2j},\delta_j,\perp)$元组，并返回 δ_j 给敌手 A_{I}.

验证请求：B 模拟验证算法，在任意时间敌手 A_{I}可以询问验证算法. 在接收敌手 A_{I}请求$(m_i,\delta_i,P^i_{ID_A})$时，$B$ 查看 H_1.

(1) 如果不存在$(*,*,*,\delta_i,*)$在 H_1 中，B 拒绝(m_i,δ_i)，它是一个无效的签名.

(2) 否则，存在一个$(*,*,*,\delta_i,*)$在 H_1 中.

(a) 如果存在一个元组$(m_i,*,*,\delta_i,P^i_{ID_A})$在 H_1 中，B 接收它为一个有效的签名；

(b) 如果存在一个元组$(m_i,K_{1i},K_{2i}\delta_i,\perp)$，$B$ 验证 $K_{2i}\stackrel{?}{=}e(P^i_{ID_A},cert_{ID_B}+\alpha_{ID_B}P_{ID_B})$，且将$(P,P_1,P_2,Q_3,K_{1i}/e(Q_{ID_A},s^i_{ID_A}P_{ID_B}))$输入 DBDH 预言机，判断是否是 DBDH 元组，如果满足上述两个条件则接收它为一个有效的签名. 否则拒绝它，认为它是一个无效的签名.

注 1. 这个算法如果发生这种情况，(m_i,δ_i)是个有效的签名，却没有在 H_1 询问和签名询问中询问过，将失败. 因为 H_1 是一个一致性的描述，这种情况发生的可能性小于 $1/(2^l-q_{H_1}-q_S)$，则验证请求成功的概率为大于$(1-1/(2^l-q_{H_1}-q_S))^{q_V}$.

伪造：假设敌手 A_{I}给出一个有效的指定验证者签名$(m^*,\delta^*,P^*_{ID_A})$，满足：

(a) m^* 没有在签名询问中询问过；

(b) ID_B都没有在密钥询问中出现过；

(c) ID_A没有在证书询问中出现过.

因为(m^*,δ^*)是一个有效的消息签名对，意味着以概率 $1-1/(2^l-q_{H_1}-q_S)$存在一个$(*,*,*,\delta^*,*)$元组在 H_1 中. 在定义的安全模型中，说明了 m^* 没有在签名询问中询问过，所以$(*,*,*,\delta^*,*)$元组是在 H_1 询问中得到的值. 也就是说存在一个$(m^*,K^*_1,K^*_2,\delta^*,\perp)$在 H_1 中满足：

$$K^*_2=e(P^*_{ID_A},cert_{ID_B}+\alpha_{ID_B}P_{ID_B}),$$

$$\begin{aligned}K^*_1&=e(Q_{ID_A},s^*_{ID_A}P_{ID_B})e(s_{ID_B}Q_{ID_A},P_{\mathrm{pub}})\\&=e(Q_{ID_A},s^*_{ID_A}P_{ID_B})e(b\alpha_{ID_A}cP,aP)\\&=e(Q_{ID_A},s^*_{ID_A}P_{ID_B})e(P,P)^{abc\alpha_{ID_A}}.\end{aligned}$$

计算$(K^*_1/e(Q_{ID_A},s^*_{ID_A}P_{ID_B}))^{-\alpha_{ID_A}}=e(P,P)^{abc}$，因为$K^*_1,Q_{ID_A},P_{ID_B},s^*_{ID_A},\alpha_{ID_A}$已知，所以 B 可以成功地解决 GBDH 问题. B 成功的概率大于$(1-1/(2^l-q_{H_1}-q_S))^{q_V+1}$，因此能够成功解决 GBDH 问题的概率是 $\varepsilon'\geq(1-1/(2^l-q_{H_1}-q_S))^{q_V+1}\varepsilon$. 证毕.

定理 2. 假设敌手 A_{II}是 CBSDVS 方案的第二类适应性选择消息攻击敌手，在最多询问了 q_{H_1} 个 H_1 询问、q_s个签名询问、q_V个验证询问之后，伪造成功的概率是 ε. 则存在一个算法 B 可以利用 A_{II}以概率 $\varepsilon'\geq(1-1/(2^l-q_{H_1}-q_S))^{q_V+1}\varepsilon$ 解决一个 GBDH 问题，这里面的 l 是 CBSDVS 方案的安全参数.

证明. 给定一个 GBDH 问题实例 $P,aP,bP,cP\in G_1$，我们构造算法 B，B 模拟挑战者与敌手A_{II}交互，并在 DBDH 预言机的帮助下，计算 $e(P,P)^{abc}\in G_2$的值. 在证明过程中我们假设 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$\{G_1,G_2,q,e,P\}$. 两个目标实体，签名者 ID_A和指定验证者 ID_B. B 随机选择 $s\in Z^*_q$，计算 $P_{\mathrm{pub}}=sP$，令 $P_{ID_A}=aP$，$P_{ID_B}=bP$，$Q_{ID_A}=cP$，随机选取 $\alpha_{ID_B}\in Z^*_q$，计算 $Q_{ID_B}=\alpha_{ID_B}P$. 将$\{G_1,G_2,q,e,P,P_{\mathrm{pub}},P_{ID_A},P_{ID_B}\}$发送给敌手 A_{II}.

密钥询问：B 保存一个(ID_i,s_{ID_i},P_{ID_i})元组的列表 L，这个列表初始化为$\{(ID_A,\perp,aP),(ID_B,\perp,bP)\}$. 敌手 A_{II} 询问 ID_i，如果 $ID_i\in\{ID_A,ID_B\}$，拒绝敌手请求. 否则，B 随机选择$s_{ID_i}\in Z^*_q$，计算 $P_{ID_i}=s_{ID_i}P$，将(ID_i,s_{ID_i},P_{ID_i})加入到 L 中，返回 s_{ID_i}.

H_1询问：B 模拟 Hash 函数 H_1，在任意时间敌手 A_{II}可以询问这个随机预言 H_1. 为了回答这些请求，B 保存了一个$(m_i,K_{1i},\delta_i,c_i)$元组的 H_1. 这个列表初始化为空. 敌手 A_{II} 询问元组(m_i,K_{1i})，B 将$(P,Q_{ID_A},P_{ID_A},P_{ID_B},K_{1i}/e(cert_{ID_A},P_{ID_B}))$输入 DBDH 预言，判断它是否是 DBDH 元组.

(1) 如果$(P,Q_{ID_A},P_{ID_A},P_{ID_B},K_{1i}/e(cert_{ID_A},P_{ID_B}))$是 DBDH 元组，

(a) 如果不存在元组$(m_i,*,*,*)$在 H_1 中，B 随机选择 $\delta_i\in G_1$，满足$(*,*,\delta_i,*)$不在H_1 中，并设置 $c_i=1$，添加$(m_i,K_{1i},\delta_i,1)$到 H_1 中，并返回 δ_i 给敌手 A_{II}；

(b) 如果有元组$(m_j,K_{1j},\delta_j,*)$在 H_1 中，则 $m_i=m_j$，$K_{1i}\neq K_{1j}$，B 随机选择 $\delta_i\in G_1$，满足$(*,*,\delta_i,*)$不在 H_1 中，并设置 $c_i=1$，添加$(m_i,K_{1i},\delta_i,1)$到 H_1 中，并返回 δ_i 给敌手 A_{II}；

(c) 否则存在这样形式的一个元组$(m_i,\perp,\delta_i,1)$，它只能在签名询问中产生并加入到 H_1 中. 用元组$(m_i,K_{1i},\delta_i,1)$替换 H_1 中的元组$(m_i,\perp,\delta_i,1)$，并返回 δ_i给敌手 A_{II}.

(2) 如果$(P,Q_{ID_A},P_{ID_A},P_{ID_B},K_{1i}/e(cert_{ID_A},P_{ID_B}))$不是 DBDH 元组，$B$ 设置 $c_i=0$，随机选择 $\delta_i\in G_1$，满足$(*,*,\delta_i,*)$不在 H_1 中，添加$(m_i,K_{1i},\delta_i,0)$到 H_1 中，并返回 δ_i给敌手 A_{II}.

签名询问：B 模拟签名算法，在任意时间敌手 A_{II}可以询问签名算法. 在接收到敌手 A_{II}请求 m_i之后，B 查询 H_1.

(1) 如果不存在元组$(m_i,*,*,*)$在 H_1 中，B 设置 $c_i=1$，并随机选择 $\delta_i\in G_1$，满足$(*,*,\delta_i,*)$不在 H_1 中，添加$(m_i,\perp,\delta_i,1)$到 H_1 中，并返回 δ_i 给敌手 A_{II}.

(2) 否则存在元组$(m_i,*,*,*)$在 H_1 中，则存在元组$(m_j,K_{1j},\delta_j,c_j)$在 H_1 中，满足$m_i=m_j$.

(a) 如果 $c_j=1$，意味着$(P,Q_{ID_A},P_{ID_A},P_{ID_B},K_{1i}/e(cert_{ID_A},PK_{ID_B}))$是 DBDH 元组，返回 δ_j给敌手 A_{II}；

(b) 如果 $c_j=0$，挑战者设置 $c_i=1$，并随机选择 $\delta_i\in G_1$，满足$(*,*,\delta_i,*)$不在 H_1 中，添加$(m_i,\perp,\delta_i,1)$到 H_1中，并返回 δ_i给敌手 A_{II}.

验证请求：B 模拟验证算法，在任意时间敌手可以询问验证算法. B 回答敌手 A_{II}请求. 在接收敌手 A_{II}请求(m_i,δ_i)，B 查看 H_1.

(1) 如果不存在$(*,*,\delta_i,*)$在 H_1 中，B 拒绝(m_i,δ_i)，它是一个无效的签名.

(2) 否则，存在一个$(*,*,\delta_i,*)$在 H_1 中，

(a) 存在一个元组$(m_i,\perp,\delta_i,1)$或者$(m_i,K_{1i},\delta_i,1)$在 H_1 中，B 接受它为一个有效的签名；

(b) 否则，B 拒绝它，认为它是一个无效的签名.

注 2. 这个算法如果发生这种情况，(m_i,δ_i)是个有效的签名，却没有在 H_1 询问和签名询问中询问过，将失败. 因为 H_1 是一个一致性的描述，这种情况发生的可能性小于 $1/(2^l-q_{H_1}-q_S)$，则验证请求成功的概率大于$(1-1/(2^l-q_{H_1}-q_S))^{q_V}$.

伪造：假设敌手给出一个有效的指定验证者签名(m^*,δ^*). 满足：

(a) m^* 没有在签名询问中询问过；

(b) ID_A，ID_B都没有在密钥询问中出现过.

因为(m^*,δ^*)是一个有效的消息签名对，意味着以概率 $1-1/(2^l-q_{H_1}-q_S)$存在一个$(*,*,\delta^*,*)$元组在 H_1 中. 在定义的安全模型中，说明了 m^* 没有在签名询问中询问过，所以$(*,*,\delta^*,*)$元组是在 H_1 询问中得到的值. 也就是说存在一个$(m^*,K_1^*,\delta^*,1)$在 H_1 中满足 $K_1^*=e(s_{ID_B}Q_{ID_A},P_{\mathrm{pub}}+P_{ID_A})=e(cert_{ID_A},P_{ID_B})e(Q_{ID_A},P)^{s_{ID_A}s_{ID_B}}$，即 $K_1^*/e(cert_{ID_A},P_{ID_B})=e(Q_{ID_A},P)^{s_{ID_A}s_{ID_B}}=e(P,P)^{abc}$，因为 $K_1^*,cert_{ID_A},P_{ID_B}$已知，所以 B 可以成功地解决 GBDH 问题. B 成功的概率大于$(1-1/(2^l-q_{H_1}-q_S))^{q_V+1}$，因此能够成功解决 GBDH 问题的概率是 $\varepsilon'\geq(1-1/(2^l-q_{H_1}-q_S))^{q_V+1}\varepsilon$.　　证毕.

6　计算代价与通信代价分析

下面我们将分析本文的计算代价与通信代价，并定义表 1 中需要用到的标识符. $|G_1|$：G_1 中元素的长度；$|Z_q|$：Z_q中元素的长度；BP(bilinear pairing operation)：双线性对操作；M：G_1 中的模乘操作；E(exponentiation in G_2)：G_2 中的指数操作；I：取逆操作；H(hash function operation)：Hash 操作，假设在群 G_1上的加法操作为可忽略. 本文方案与其它相关方案的性能及优缺点比较结果如表 1 所示.

表 1　计算代价、通信代价及相关性质分析

	签名	验证	签名长度	强指定验证者签名	密钥托管	安全信道
文献[4]方案	BP+E+3M+H+I	2BP+E+M+H	$\|G_1\|+2\|Z_q\|$	是	有	使用
文献[5]方案	2BP+E+2M+H	BP+E+M+H	$2\|G_2\|$	是	有	使用
文献[6]方案	3BP+4M+3H	BP+M+2H	$2\|G_1\|$	不详	有	使用
文献[7]方案	BP+M+H+I	3BP+M+H	$\|Z_q\|$	不详	无	使用
文献[8]方案	BP+M+H	BP+M+H	$\|Z_q\|$	不详	无	使用
文献[9]方案	BP+4M+H	BP+2M+H	$\|G_1\|+\|G_2\|$	是	无	使用
文献[10]方案	4M+H+I	2BP+E+M+H	$2\|G_1\|$	是	无	使用
本文方案	2BP+2M+1H	2BP+2M+1H	$\|G_1\|$	是	无	不使用

由表 1 分析可知，本文方案的计算代价与文献[6-7]相当，略低于文献[4-5,8-10]. 但是与其它方案相比，本文方案也具有明显的优点：(1) 签名长度最短(仅为群 G_1 中的一个群元素)；(2) 满足强指

定验证者签名的性质;(3)不使用安全信道;(4)较好地解决了基于身份指定验证者签名方案中的密钥托管问题.

7 结束语

指定验证者签名由于其具有的特殊性质,已经被广泛地应用在生活的各个领域.本文首先提出了基于证书强指定验证者签名的概念和安全模型,然后构造了基于证书强指定验证者签名方案.基于GBDH假设,在随机预言模型下证明了方案对适应性选择消息攻击是存在不可伪造的.提出的方案能够抵抗密钥替换攻击问题并且较好地解决了基于身份指定验证者签名中的密钥托管问题.我们分析了方案的通信代价和计算代价,方案的签名长度仅为群 G_1 中的一个群元素,是目前签名长度最短的基于证书签名方案之一,非常适合通信受限的网络环境中.方案的计算代价略高,为4个双线性对操作,下一步将把减少计算代价作为研究工作的重点.

致 谢 匿名审稿专家对本文进行了仔细审阅并提出了宝贵的修改意见,作者在此表示衷心感谢!

参 考 文 献

[1] Jakobsson M, Sako K, Impagliazzo R. Designated verifier proofs and their applications//Maurer U ed. Proceedings of the Eurocrypt 96. Saragossa, Spain. LNCS 1070. Berlin: Springer-Verlag, 1996: 143-154

[2] Saeednia S, Kramer S, Markowitch O. An efficient strong designated verifier signature scheme//Lim J I, Lee D H eds. Proceedings of the 6th International Conference on Information Security and Cryptology (ICISC 2003). Seoul, Korea. LNCS 2971. Berlin: Springer-Verlag, 2004: 40-54

[3] Steinfeld R, Bull L, Wang H, Piperzyk J. Universal designated verifier signatures//Laih C S ed. Proceedings of the Asiacrypt 2003. Taipei, China. LNCS 2894. Berlin: Springer-Verlag, 2003: 523-542

[4] Susilo W, Zhang F, Mu Y. Identity-based strong designated verifier signature schemes//Proceedings of the ACISP 2004. Sydney, Australia, 2004: 313-324

[5] Kang B Y, Boyd C, Dawson E. A novel identity-based strong designated verifier signature scheme. The Journal of Systems and Software, 2009, 82(2): 270-273

[6] Wang Xiao-Feng, Zhang Jing, Wang Shang-Ping, Zhang Ya-Ling, Qin Bo. New ID-based universal designated-verifier signature scheme. Acta Electronica Sinica, 2007, 35(8): 1432-1436(in Chinese)
(王晓峰, 张璟, 王尚平, 张亚玲, 秦波. 新的基于身份的广义指定验证者签名方案. 电子学报, 2007, 35(8): 1432-1436)

[7] Huang X Y, Susilo W, Mu Y, Zhang F T. Certificateless designated verifier signature schemes//Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA2006). Vienna, Australia, 2006: 15-19

[8] Chen H, Song R S, Zhang F T, Song F G. An efficient certificateless short designated verifier signature scheme//Proceedings of the Wireless Communications, Networking and Mobile Computing (WiCOM'08). Dalian, China, 2008: 1-6

[9] Yang B, Hu Z M, Xiao Z B. Efficient certificateless strong designated verifier signature scheme//Proceedings of the Computational Intelligence and Security (CIS'09). Beijing, China, 2009: 432-436

[10] Xiao Z B, Yang B, Li S G. Certificateless strong designated verifier signature scheme//Proceedings of the e-Business and Information System Security (EBISS'2010). Wuhan, China, 2010: 1-5

[11] Gentry C. Certificate-based encryption and the certificate revocation problem//Proceedings of the Eurocrypt 2003. Warsaw, Poland, 2003: 272-293

[12] Kang B G, Park J H, Hahn S G. A certificate-based signature scheme//Proceedings of the CT-RSA 2004. San Francisco, CA, USA, 2004: 99-111

[13] Li J G, Huang X Y, Mu Y, Susilo W, Wu Q H. Certificate-based signature: Security model and efficient construction//Lopez J, Samarati P, Ferrer J L eds. Proceedings of the EuroPKI 2007. Palma de Mallorca, Spain. LNCS 4582. Berlin: Springer-Verlag, 2007: 110-125

[14] Wu W, Mu Y, Susilo W, Huang X Y. Certificate-based signatures: New definitions and a generic construction from certificateless signatures//Chung K I, Sohn K, Yung M eds. Proceedings of the WISA 2008. Jeju Island, Korea. LNCS 5379. Berlin: Springer-Verlag, 2009: 99-114

[15] Au M H, Liu J K, Susilo W, Yuen T H. Certificate based (Linkable) ring signature//Dawson E, Wong D S eds. Proceedings of the ISPEC 2007. Hong Kong, China. LNCS 4464. Berlin: Springer-Verlag, 2007: 79-92

[16] Liu J K, Baek J, Susilo W, Zhou J Y. Certificate-based signature schemes without pairings or random oracles//Wu T C et al eds. Proceedings of the ISC 2008. Taipei, China. LNCS 5222. Berlin: Springer-Verlag, 2008: 285-297

[17] Zhang J H. On the security of a certificate-based signature scheme and its improvement with pairings//Bao F, Li H, Wang G eds. Proceedings of the ISPEC 2009. Xi'an, China. LNCS 5451. Berlin: Springer-Verlag, 2009: 47-58

[18] Li J G, Xu L Z, Zhang Y C. Provably secure certificate-based proxy signature schemes. Journal of Computers, 2009, 4(6): 444-452

[19] Ming Y, Wang Y M. Efficient certificate-based signature scheme//Proceedings of the Fifth International Conference on Information Assurance and Security (IAS 2009). Xi'an, China, 2009: 87-90

[20] Li J G, Huang X Y, Mu Y, Susilo W, Wu Q H. Constructions of certificate-based signature secure against key replacement attacks. Journal of Computer Security, 2010, 18(3): 421-449

[21] Li J G, Huang X Y, Zhang Y C, Xu L Z. An efficient short certificate-based signature scheme. Journal of Systems and Software, 2012, 85(2): 314-322

LI Ji-Guo, born in 1970, Ph. D., professor, Ph. D. supervisor. His main research interests include information security, cryptography theory and technology.

QIAN Na, born in 1984, M. S.. Her main research interests include cryptography theory and technology.

HUANG Xin-Yi, born in 1981, Ph. D.. His main research interests include information security, cryptography theory and technology.

ZHANG Yi-Chen, born in 1971, Ph. D. candidate, lecturer. Her main research interests include cryptography theory and technology.

Background

This research is supported by the National Natural Science Foundation of China (Grant Nos. 60842002, 61003232, 61072080, 61103183, 61103184), the Fundamental Research Funds for the Central Universities, the "Six Talent Peaks Program" of Jiangsu Province of China under Grant No. 2009182, the Fundamental Research Funds for the Central Universities (Grant Nos. 2009B21114, 2010B07114), Funds of Key Laboratory of Fujian Province University Network Security and Cryptology under Grant No. 2011001, and Program for New Century Excellent Talents in Hohai University.

In 1996, Jakobsson, Sako and Impagliazzo proposed the concept of designated verifier signature (DVS). In a DVS scheme, signer can designate a single party, i. e. the designated verifier and only this designated verifier who can be convinced about its validity or invalidity of the signatures. Furthermore, signer can not completely control the signature. It solves the problems that anyone can verify signature in traditional signature and signer can completely control the signature in undeniable signature. In 2003, the conception of designated verifier signature was extended to strong designated verifier signature (SDVS). SDVS scheme have an additional property that anyone should be able to produce an identically distributed transcripts that are indistinguishable from the original protocol that is run between the signer and the verifier.

The existing schemes are in traditional public key cryptosystem, identity-based public key cryptosystem and certificateless public key cryptosystem. However, in traditional setting, it is very complex to manage certificate. In order to solve this problem, identity-based SDVS was proposed by Susilo et al. in 2004. In the identity-based cryptography, the private key generator (PKG) can generate the private keys of all its users, and hence, the private key escrow becomes an inherent problem. Moreover, the private key must be sent over secure channel, which makes private key distribution a daunting task. In the certificateless cryptography, it also must use secure channels. In Eurocrypt 2003, Gentry introduced the notion of certificate-based encryption. The certificate-based cryptography preserves advantage of the above cryptography and overcomes disadvantage of them. Therefore, research on the certificate-based designated verifier signature is an interesting research topic.

In the paper, the authors propose the notion and security model of certificate-based strong designated verifier signature (CBSDVS) and construct the CBSDVS scheme. The scheme is existentially unforgeable against adaptive chosen message attacks under the gap bilinear Diffie-Hellman assumption in the random oracle model, and solves the inherent problem in traditional public key cryptosystem, identity-based public key cryptosystem and certificateless public key cryptosystem.