无随机预言模型下可否认的基于属性的指定证实人签名方案

任 燕
(运城学院应用数学系 运城 044000)

摘 要 首次在无随机预言模型下构建了可否认的基于属性的指定证实人签名方案。在该方案中,签名者和指定的证实人均可通过执行相同的协议来对签名的有效性进行确认,同时可以通过执行相同的协议来否认无效的签名。最后,对方案的正确性进行了分析,并在无随机预言模型下证明了方案的安全性。分析表明,本方案具有不可伪造性和隐形性。

关键词 数字签名,基于属性签名,指定证实人签名,无随机预言模型,可否认
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.7.029

Deniable Attribute-based Designated Confirmer Signature without Random Oracles

REN Yan
(Department of Applied Mathematics, Yuncheng University, Yuncheng 044000, China)

Abstract In this paper, we first proposed a deniable attribute-based designated confirmer signature's model without random oracles. In this signature scheme, both the signer and the designated confirmer can run the same protocols to confirm a valid designated confirmer signature or disavow an invalid signature. Finally, the proof of correctness and security in the standard model is provided. Analytical results show that this scheme obtains the advantages of unforgeability and invisibility.

Keywords Digital signature, Attribute-based signature, Designated confirmer signature, Random oracles, Deniable

1 引言

1994年DChaum[1]首次提出指定证实人签名。在指定证实人签名方案中,签名者指定某一证实人对签名进行确认,如果签名者无法验证签名,指定证实人也能对签名的有效性进行确认。随后,T. Okamoto提出了更加有效的指定证实人签名[2];MMichels等人[3]指出Okamoto方案中的一个缺点并给出了修正方案;Gentry等人也提出了一些指定确认者签名方案[4-9]。但是这些方案要么不安全,要么效率较低。

为了解决现有的指定证实人签名方案中签名者没有权利否认无效的指定证实人签名的缺点,2003年Galbraith和Mao首次指出指定证实人签名应该允许签名者有否认无效签名的能力[10],但是他们没有给出更进一步的研究;2012年王桂林等人[11]给出了一个签名者和指定证实人具有否认能力的指定证实人签名正式的安全模型,同时利用双线性映射构建了一个具体的方案;文献[12]提出一个可否认的基于属性的指定证实人签名方案,但这个方案是在随机预言模型下提出的。

本文在无随机预言模型下构建了一个基于属性的可否认的指定证实人签名方案。在该方案中,签名者和指定的证实人均可对签名的有效性进行确认,并且可以否认无效的签名。同时,在无随机预言模型下对方案的正确性和安全性进行了分析,证明了本方案具有不可伪造性和隐形性。

2 预备知识

2.1 双线性映射

设G_1,G_2是两个循环乘法群,G_1,G_2的阶均为素数q。设$e:G_1\times G_1\to G_2$为一个双线性映射。假定在G_1,G_2上的离散对数问题(DLP问题)都是困难的,则双线性映射满足以下性质。

1)双线性性:对任意的$P,Q\in G_1$和所有的$a,b\in Z_q$,有$e(aP,bQ)=e(P,Q)^{ab}$。

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

3)可计算性:对于$P,Q\in G_1$,存在一个高效的算法计算$e(P,Q)$。

2.2 拉格朗日插值定理

设$f(x)$为x的一个次数为n的多项式f的函数,如果给定多项式$n+1$个不同点$(x_i,f(x_i))$,则通过式(1)能唯一确定任意一个x所对应的多项式$f(x)$值:

$$f(x)=\sum_{i=1}^{n}f(x_i)\left(\prod_{1\leqslant k\neq i\leqslant n}\frac{(x-x_k)}{x_j}-x_k\right) \tag{1}$$

对于式(1)可以定义拉格朗日系数$\Delta_{i,s}$,其中$i\in Z_p$,集合s中的元素取自Z_p:

$$\Delta_{i,s}(x)=\prod_{i\in s,j\neq i}\frac{x-j}{i-j}$$

2.3 本方案依赖以下困难性问题

1)离散对数问题(DLP):给定$P,Q\in G_1$,求$n\in Z_q$,使得

到稿日期:2015-06-16 返修日期:2015-09-28 本文受国家自然科学基金(11241005),运城学院生物数学重点实验室开放课题(SWSX201306)资助。

任 燕(1982-),女,博士生,主要研究方向为密码学、信息安全。

$P=nQ$。

2)双线性对求逆问题:已知 $a=e(P,Q)$,给定 $P\in G_1$,求 $Q\in G_1$。

3)计算 Diffie-Hellman 问题(CDHP):对 $a,b\in Z_q$,给定 (P,aP,bP),计算 abP。

3 无随机预言模型下可否认的基于属性的指定证实人签名方案的定义和安全模型

定义 1 一个正确的可否认的基于属性的指定证实人签名方案包括签名者、指定证实人和验证者,由以下 8 部分组成。

1)系统初始化:由系统运行的一个概率性算法。输入为系统安全参数,输出系统主密钥集合 mk 和公开的参数 pk。

2)密钥生成(G_S,G_C):分别生成原始签名人 S 和指定证实人 C 的秘钥对。G_S 的输入为公共参数 pk、系统的主密钥 mk 和签名者的属性集合 ω,输出为 S 的密钥 d_ω。类似地,G_C 的输入为公共参数 pk、系统的主密钥 mk,输出是字符串对 (sk_C,pk_C),分别为指定证实人的私钥和公钥。

3)签名生成:输入为系统参数、断言 Γ、满足 $\Gamma(\omega)=1$ 的签名者的属性集合、签名者的私钥 d_ω 和消息 m,输出为签名者对消息 m 的签名 σ。

4)验证算法:输入为系统参数、对应于断言 Γ 的属性集、消息 m 和对消息的签名 σ,σ 是对消息 m 的正确签名且 $\Gamma(\omega)=1$ 时该算法输出 True,其它输出 False。

5)指定证实人签名:输入为消息 m、签名者的私钥 d_ω 和证实人的公钥 pk_C,输出为对消息 m 的指定证实人签名 σ'。

6)抽取:输入为消息 m、指定证实人签名 σ'、证实人的私钥 sk_C 和证实人的公钥 pk_C,输出为满足验证算法的对消息 m 的签名 σ。如果可以成功地从 σ' 抽取出 σ,则称 σ' 是可抽取的,否则是不可抽取的。

7)确认:确认过程是一个交互协议,签名者和证实人都可以利用自己的私有输入与验证者运行确认协议来确定指定证实人签名是可抽取的。

8)否认:否认过程也是一个交互协议,签名者和证实人都可以利用自己的私钥与验证者运行确认协议来确定指定证实人签名是不可抽取的。

用文献[11]中所提到的可否认的指定证实人签名的安全性定义。

定义 2(不可伪造性) 令 F 是一个输入为 1^n 的多项式时间的伪造算法,pk_S,pk_C,sk_C 可以要求访问 $O_F=\{DCSSign,Confirm_{(S,F)},Disavow_{(S,F)}\}$ 多项式次,然后输出指定证实人消息签名对(m,σ'),这里 m 不是先前在指定证实人签名查询中出现的。我们说一个指定证实人签名方案对存在伪造性是安全的,若对 F 有:

$$\Pr[Verify(m,Extract(m,\sigma',sk_C,pk_C,pk_S),pk_S)=Accept]<negl(n)$$

定义 3(隐形性) 首先,对签名者和指定证实人运行输入为 1^n 的秘钥生成算法。给定 D 签名者的公钥 pk_S 和指定证实人的公钥 pk_C。作为培训的目的,D 允许创建签名秘钥对(sk_D,pk_D)(不一定通过秘钥生成)且可以用这些相应的秘钥与证实人交互。进一步地,D 可以在以下集合中做任意查询:

$O_D=[Sign,DCSSign,Confirm_{(S,D)},Confirm_{(C,D)},Disavow_{(S,D)},Disavow_{(C,D)},Extract]$

然后,区分者提出一个消息 m,在一个掷硬币后:

若 $b=0$,则敌手给定一个相应的 $DCS=DCSSign(m,sk_S,pk_C)$;

若 $b=1$,则敌手在从签名空间中随机均匀选择一个假的指定证实人签名。

现在,D 再次被允许访问上述预言,但是它不能通过这些预言查询 σ'。

最后,区分者要求输出 1 比特的信息 b' 来猜测 b 的值。

我们说一个具有同一验证过程的指定证实人签名是隐形的,若对任意多项式时间的区分者 D:

$$\Pr[b=b']\leqslant 1/2+negl(n)$$

定义 4(安全性) 如果一个可否认的基于属性的指定确认者签名满足不可伪造性和隐形性,则称该方案是安全的。

4 方案的构造

定义拉格朗日差值 $\Delta_{i,s}(x)$ 如下:

$$\Delta_{i,s}(x)=\prod_{j\in S,j\neq i}\frac{x-j}{i-j}$$

(1)初始化阶段(Setup)

1)定义属性集合 U,简单起见令 $|U|=1$,且可以取 Z_p 的前 l 个元素作为这个集合,即:

$1,2,\cdots,l(\mathrm{mod})p$

2)在上述的安全级别生成一对群的集合。

3)随机选择一个生成元 $g\in G_1$,随机选取 $x,y\in Z_p^*$,g_1,$g_2\in G_1$,令 $X=g^x$。

4)随机选择一个长度为 d 和一个长度为 n 的向量:$H=(h_i)$,$U=(u_i)$,这里的 h_i,u_i 是群 G_1 中的元素。

则公共参数为:$params=(g,g_1,g_2,X,d,H,U)$;主密钥为 x。

(2)密钥生成(Key Generation)

首先为具有属性集合 ω 的签名者 S 生成公私钥。

1)选择一个 $d-1$ 阶的多项式 $q(x)$ 满足 $q(x)=0$。

2)对每个 $i\in\omega$ 选择 $r_i\in_R Z_p$,并计算:

$d_{i0}=g_1^{q(i)}Xh_i^{r_i}$,$d_{i1}=g^{r_i}$

3)对每个 $i\in\omega$,输出 $D_i=(d_{i0}\cdot d_{i1})$作为私钥。

然后为指定证实人 C 生成公私钥。

指定证实人随机选取 $x_C\in Z_q^*$ 作为私钥,$y_C=g^{x_C}$ 是其公钥。

(3)签名生成(Sign)

假设 $m=(\mu_1,\mu_2,\cdots,\mu_n)\in\{0,1\}^n$,一个用户对属性 ω 有密钥。在断言 $\Gamma_{d,\omega}(\cdot)$ 下对消息 m 进行签名,即证明至少拥有 n 元属性集合中的 d 个属性,他先选择一个含 d 个元素的子集 $S\subseteq\omega\cap\omega^*$,签名过程如下:

对 $i\in S$ 随机选择 d 个值 $r_i'\in Z_P$。计算:

$$\sigma_0=\prod_{i\in S}g_1^{q(i)}(Xh_i)^{\Delta_{i,S^{(0)}}}\prod_{i\in S}(Xh_i)^{r_i'}\cdot(\prod u_j^{\mu_j})^s$$

$$\{\sigma_i=(g^{r_i})^{\Delta_{i,S^{(0)}}}g^{r_i'}\},i\in S$$

$$\sigma_s=g^s$$

则生成的签名为 $\sigma=(\sigma_0,\{\sigma_i\},\sigma_s)$。

(4)签名验证(Verify)

收到签名 σ 后，验证等式 $\frac{e(\sigma_0,g)}{\prod e(Xh_i,\sigma_i)e(\prod u_j^{\mu_j},\sigma_0)}=e(g_1,X)$ 是否成立。

(5)指定证实人签名(DCSSign)

为 m 生成一个基本签名 σ 之后，通过如下计算为 m 生成一个指定证实人签名 σ'：$\sigma_0=\sigma_0,\sigma_i'=\sigma',\sigma_1=g^r,\sigma_2=\sigma_s Y_C^r$，这里 $r\in Z_q^*$ 是随机选取的数。

(6)抽取过程(Extract)

给定消息 m 和指定证实人签名 σ'，若验证等式成立，则证实人可以抽取基本签名：$\sigma_0=\sigma_0,\sigma_i'=\sigma_i',\sigma_s=\frac{\sigma_2}{\sigma_1^{x_C}}$；否则输出 $\perp$。

(7)确认过程(Confirm)

给定 (m,σ',Y_S,Y_C)，证实人 C 可以通过证明以下等式成立来说明 DCS 的有效性。

$$\frac{e(g_3\prod u_j^{\mu_j},\sigma_2)\prod_{i\in S}e(Xh_i^{r_i},\sigma_i')}{e(g_3\prod_{i\in s}u_j^{\mu_j},\sigma_1)^{x_C}}=\frac{e(\sigma_0,g)}{e(g_1,X)}$$

签名人可以通过证明等式 $\frac{e(g_3\prod u_j^{\mu_j},\sigma_2)\prod e(Xh_i^{r_i},\sigma_i')}{e(\prod u_j^{\mu_j},\sigma_1)}\times\frac{e(\prod u_j^{\mu_j},g)^r}{e(\prod u_j^{\mu_j},Y_C)^r}=\frac{e(\sigma_0,g)}{e(g_1,X)}$ 成立来确认签名。

令：$A_1=e(g_3\prod u_j^{\mu_j},\sigma_1)$，$B_1=\frac{e(g_1,X)e(\prod u_j^{\mu_j},\sigma_2)}{e(\sigma_0,g)}\times\prod_{i\in S}e(Xh_i^{r_i},\sigma_i')$，$C_1=Y_C$，$A_2=\frac{e(\prod u_j^{\mu_j},g)}{e(\prod u_j^{\mu_j},Y_C)}$，$B_2=\frac{e(g,\sigma_0)e(\prod u_j^{\mu_j},\sigma_1)}{e(g_1,X)e(\prod u_j^{\mu_j},\sigma_2)}\times\frac{1}{\prod_{i\in S}e(Xh_i^{r_i},\sigma_i')}$，$C_2=Y$，则无论是证实人还是签名者，都可以与验证者施行如下的交互零知识协议。

$$PK\{(x_C\vee r):[A_1^{x_C}=B_1\wedge C_1=g^{x_C}]\vee A_2^r=B_2\wedge C_2=g^r]\}$$

(8)否定过程(Disavow)

给定 (m,σ',Y_S,Y_C)，当 $\frac{e(g_3\prod u_j^{\mu_j},\sigma_2)\prod_{i\in S}e(Xh_i^{r_i},\sigma_i')}{e(g_3\prod_{i\in s}u_j^{\mu_j},\sigma_1)^{x_C}}\neq\frac{e(\sigma_0,g)}{e(g_1,X)}$ 或者 $\frac{e(\prod u_j^{\mu_j},\sigma_2)\prod e(Xh_i^{r_i},\sigma_i')}{e(\prod u_j^{\mu_j},\sigma_1)}\times\frac{e(\prod u_j^{\mu_j},g)^r}{e(\prod u_j^{\mu_j},Y_C)^r}\neq\frac{e(\sigma_0,g)}{e(g_1,X)}$ 时，则说明 σ' 是对消息 m 的无效签名。从而无论是证实人还是签名者，都可以与验证施行如下的交互零知识协议。

$$PK\{(x_C\vee r):[A_1^{x_C}\neq B_1\wedge C_1=g^{x_C}]\vee A_2^r\neq B_2\wedge C_2=g^r]\}$$

5 正确性和安全性分析

5.1 正确性分析

5.1.1 验证的正确性

验证等式 $\frac{e(\sigma_0,g)}{\prod e(Xh_i,\sigma_i)e(\prod u_j^{\mu_j},\sigma_0)}=e(g_1,X)$ 是成立的。

证明：

$$\begin{aligned}&\frac{e(\sigma_0,g)}{\prod e(Xh_i,\sigma_i)e(\prod u_j^{\mu_j},\sigma_0)}\\&=\frac{e(\prod_{i\in S}(g_1^{q(i)}(Xh_i)^{r_i})^{\Delta_{i,S^{(0)}}},g)}{\prod_{i\in S}e(Xh_i,g^{r_i\Delta_{i,S^{(0)}}})}\times\\&\quad\frac{e(\prod_{i\in S}(Xh_i)^{r_i},g)e((\prod(u_j)^{\mu_j})^s,g)}{\prod_{i\in S}e(Xh_i,g^{r_i\prime})\prod e(\prod(u_j)^{\mu_j},g^s)}\\&=e(\prod g_1^{q(i)})^{\Delta_{i,S^{(0)}}},g)\\&=e(g_1,X)\end{aligned}$$

5.1.2 抽取的正确性

可以通过如下过程验证抽取过程的正确性。

$$\frac{\sigma_2}{\sigma_1^{x_C}}=\frac{\sigma_s Y_C^r}{(g^r)^{x_C}}=\frac{\sigma_s Y_C^r}{Y_C^r}=\sigma_s$$

5.1.3 确认的正确性

在确认协议中，知识的声明如下：

$$PK\{(x_C\vee r):[A_1^{x_C}=B_1\wedge C_1=g^{x_C}]\vee A_2^r=B_2\wedge C_2=g^r]\}$$

采用文献[13]中的协议可以直接得到该确认协议是正确的。类似地，可证明否认协议是正确的。

5.2 安全性分析

定理 1 本方案是不可伪造的。

证明：假设一个敌手 F 可以以 ε 的优势攻破我们的方案，则可以构建一个算法 A 来解决 CDH 问题。即算法 A 在给定 $g,X=g^r,Y=g^y$ 时，可计算出 g^{xy}。具体过程如下：

Setup

F 输出挑战断言，即 n 个元素的属性集合 ω^* 的门限为 d 的函数。

令 $g_1=X,g_2=Y$。

KeyGen

A 可以对私钥进行查询，按照如下方式模拟生成属性 ω 的私钥：

1)随机选取 $s_1\in Z_p^*$，令 $s=-y+s_1$。

2)定义 3 个集合 $\Gamma=\omega^*\cap\omega,\Gamma',S=\Gamma\cup\{0\}$，这里 Γ' 满足 $\Gamma\subseteq\Gamma'\subseteq\omega$。若 $i\in\Gamma'$，则 $d_{i0}=g_2^{r_i}Xh_i^{r_i},d_{i1}=g^{r_i}$，这里的 τ_i,r_i 是在 Z_p 中随机选取的。

若 $i\notin\Gamma'$，令 $h_i=g^{\beta_i},u_i=g^{a_i}$，则

$$d_{i0}=g_2^{\sum_{j\in\Gamma'}\Delta_{j,S^{(i)}q(j)+\Delta_{0,S^{(i)}q(0)}}}g_1^{\Delta_{0,S^{(i)}+r_i'}}g^{\beta_i\Delta_{0,S^{(i)}}}h_i^{r_i}$$

$$d_{i1}=g^{\Delta_{0,S^{(i)}}}g^{r_i'}$$

由 $q(i)=\sum_{j\in\Gamma}\Delta_{j,S}(i)q(j)+\Delta_{0,S}(i)q(0)$ 可知 A 正确模拟了私钥。

因为令 $r_i=\Delta_{0,S}(i)+r_i'$，有：

$$g_2^{q(i)}(Xh_i)^{r_i}=g_2^{\sum_{j\in\Gamma}\Delta_{j,S^{(i)}q(j)+\Delta_{0,S^{(i)}q(0)}}}\times g_1^{\Delta_{0,S^{(i)}+r_i'}}g^{\beta_i\Delta_{0,S^{(i)}}}h_i^{r_i}$$

$$g^{r_i}=g^{\Delta_{0,S^{(i)}}}g^{r_i'}$$

然后，A 通过运行 G_C 随机生成证实人的一个秘钥对 (x_C,y_C)。

DCSSign 模拟

A 可以用属性集合 ω 和证实人的秘钥对消息 m 做一个

签名查询。

若$|\omega\cap\omega^*|\geqslant d$，则$A$通过如下过程模拟签名：

选择随机的$r\in Z_q$，按照正常的方式得到属性集合ω对消息m的签名。

若$d\geqslant|\omega\cap\omega^*|\geqslant k$，则$A$可以如下模拟签名：

$g^s=g_2^{-1}g^{s_1}$，$g_2^r\prod_{i\in S}(Xh_i)^{r_i}(g_3\prod(u_j)^{\mu_j})^s$

敌手选择随机$r\in Z_q$，并计算g^r，$(g^sY_C)^r$。

最后，输出一个属性集合ω^*对消息m^*的伪造签名：

$\sigma^*=(\sigma_0^*,\{\sigma_i'^*\},\sigma_1^*,\sigma_2^*)$

$=(g_2^s\prod_{i\in S}(Xh_i)^{r_i}(\prod(u_j')^{\mu_j})^s,\{g^{r_i}\},g^r,(g^sY_C)^r)$

A可以计算：

$$g^{xy}=\frac{\sigma_0^*}{\prod_{i\in S}g_1^{r_i}(\sigma_i'^*)^{\beta_i}(\frac{\sigma_2^*}{\sigma_1^{*x_C}})^{a_i\mu_i}}$$

下面分析成功的概率：

要求伪造的签名满足$\omega^*\cap\omega\geqslant d$，而从$n-k$个元素中正确猜出$d-k$个的概率是$\frac{1}{C_{n-k}^{d-k}}$，所以$A$可以以$\frac{1}{C_{n-k}^{d-k}}$的概率解决CDH问题。

定理2 我们的方案在CDH假设下具有隐形性。

证明：假设一个挑战者算法C给定CDH挑战，即给定g，g^a，$g^b\in G$以不可忽略的概率计算$g^{ab}\in G$，这里a,b从Z_q^*中随机选取，g是阶为素数q的乘法循环群G的生成元。考虑隐形游戏，C要为一些多项式时间的区分者D模拟一个DCS环境，在这个环境里D想区分(m,sig)和$(m,sigR)$，这里：

$sig=DCSSign(m,sk_S,pk_C)$

而$sigR$是从签名空间中均匀随机选取的。

D在挑战请求之前或者之后都可以访问sign、DCSSign、Confirm和Disavow预言。所以C可以初始化一个DCS方案的实例，且为D模拟这个游戏如下。

首先令$pk_C=g^b$，然后C如下为D模拟所有的预言：

Sign query和DCSSign query同定理1。

Extract query：

若$\frac{e(g_3\prod u_j^{\mu_j},\sigma_2)\prod_{i\in S}e(Xh_i^{r_i},\sigma_i')}{e(g_3\prod_{i\in s}u_j^{\mu_j},\sigma_1)^{x_C}}\neq\frac{e(\sigma_0,g)}{e(g_1,X)}$，输出⊥；否则，$C$知道要求的指定证实人签名消息对是有效的，所以可以输出基本签名σ。

Confirm/Disavow query：

同抽取预言相似，C可以很容易地检验请求的DCS的有效性。为了让D相信请求的DCS的有效性，C只需要直接运行CZK模拟器。

对于D提交的挑战消息m'，若掷硬币结果是头，则C令$\sigma_1=g^y$，$\sigma_2=g^{s+by}$来获得计算DCS签名sig，这里的y可以看作是原始的DCSSign阶段的随机数；若掷硬币的结果是尾，则C输出一个伪造的DCS：$sigR=(\sigma_0\{\sigma_i'\},\sigma_1,\sigma_2)$，其中，$\sigma_1=g^y$，$\sigma_2=g^z$。

在此之后，C可以用上面的模拟不断地应答D的查询。

最后，若D可以用一个不可忽略的优势通过计算一个正确的猜测比特b'来区分sig和$sigR$，则可以直接看到C可以计算：

$g^{by}=g^{z-s}$

即C可以以不可忽略的优势解决给定的挑战。

结束语 本文在无随机预言模型下构建了一个基于属性的可否认的指定证实人签名方案。在该方案中，签名者和指定的证实人均可对签名的有效性进行确认，并且可以否认无效的签名。同时，对方案的正确性和安全性进行了分析，证明了本方案具有不可伪造性和隐形性。

参考文献

[1] Chaum D. Designated Confirmer Signatures[C]// Proceedings of Eurocrypto'94, LNCS 950. Springer-Verlag, 1995: 86-91

[2] Okamoto T. Designated Confirmer Signatures and Public-key Encryption are Equivalent[C]// Proceedings of Crypto'94. LNCS 839, Springer-Verlag, 1994: 61-74

[3] Michel, M, Stadler M. Generic Constructions for Secure and Efficient Confirmer Signature Schemes [C]// Proceedings of Eurocypto'98. LNCS 1403, Springer-Verlag, 1998: 405-421

[4] Gentry C, Molnar D, Ramzan Z. Efficient designated confirmer signatures without random oracles or general zero-knowledge proofs[C]// Advances in Cryptology-ASIACRYPT 2005. LNCS 3788, 2005: 662-681

[5] Goldwasser S, Waisbard E. Transformation of digital signature schemes into designated confirmer signature schemes[C]// Proceedings of TCC 2004. LNCS 2951, 2004: 77-100

[6] Michels M, Stadler M. Generic constructions for secure and efficient confirmer signature schemes[C]// Proceedings of Eurocrypt 1998. LNCS 473, Springer-Verlag, 1998: 458-464

[7] Okamoto T. Designated confirmer signatures and public-key encryption are equivalent[C]// Proceedings of Crypto 1994. LNCS 2894, 1994: 61-74

[8] Wang G, Baek J, Wong D S, et al. On the generic and efficient constructions of secure designated confirmer signatures[C]// Proceedings of PKC 2007. LNCS 4450, 2007: 43-60

[9] Zhang F, Chen X, Wei B. Efficient designated confirmer signature from bilinear pairings[C]// Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security. ACM, 2008: 363-368

[10] Galbraith S D, Mao W. Invisibility and anonymity of undeniable and confirmer signatures[C]// Proceedings of the 2003 RSA Conference on the Cryptographers' track. 2003: 80-97

[11] Wang G, Xia F, Zhao Y. Designated confirmer signatures with unified verification[M]// Cryptography and Coding. Springer Berlin Heidelberg, 2011: 469-495

[12] Ren Yan, Tang Chun-ming. Deniable attribute-based designated confirmer signature[J]. Application Research of Computers, 2014(1): 213-216(in Chinese)
任燕，唐春明. 可否认的基于属性的指定证实人签名方案[J]. 计算机应用研究，2014(1): 213-216

[13] Camenisch J, Michels M. Conrmer signature schemes secure against adaptive adversaries[C]// Proceedings of Advances in Cryptology-EUROCRYPT'00. LNCS 1870, 2000: 243-258