一种高效的广义指定验证者签名证明

明 洋, 李恕海, 王育民
(西安电子科技大学综合业务网络国家重点实验室, 陕西西安 710071)

摘 要: Joonsang Baek 等人提出了一种新型的广义指定验证者签名(UDVS)称为广义指定验证者签名证明(UDVSP). 本文提出一个高效的基于 Zhang-Safavi-Susilo(ZSS)签名方案的广义指定验证者签名证明. 利用双线性对的性质和预计算, 所提方案中仅仅需要 2 个对运算, 同时只使用通常密码学上的 hash 函数, 而不需要特殊的 hash 函数(映射到点). 在随机预言机模型中, 证明该方案是安全的.

关键词: 广义指定验证者签名; hash 函数; 随机预言机; 双线性对
中图分类号: TN918.1 文献标识码: A 文章编号: 0372-2112 (2006) 12A-2434-04

An Efficient Universal Designated Verifier Signature Proof

MING Yang, LI Shu-hai, WANG Yu-min
(*State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, Shaanxi 710071, China*)

Abstract: Joonsang Baek et al. proposed a new type of universal designated verifier signature (UDVS) which is called universal designated verifier signature proof(UDVSP). We present an efficient UDVSP scheme based on Zhang-Safavi-Susilo (ZSS) signature scheme. Using the properties and pre-computing of the bilinear pairings, our proposed scheme only needs two parings computations. Furthermore the scheme uses general cryptographic hash function, and does not require special hash function (Map to Point). The security of our UDVSP scheme is then proven in the random oracle model.

Key words: universal designated verifier signature; hash function; random oracle; bilinear pairing

1 引言

数字签名能够提供完整性、认证性和不可否认性的服务, 所以在现代密码学中是一个非常重要的安全概念. 在数字签名中, 签名者使用自己的私钥生成消息的签名, 能够得到相应公钥的任何人可以验证消息的真实性. 那么一个签名的验证者通过给出这个消息的签名就能够使任何第三方相信这个事实. 数字签名的易拷贝性和易传播性在一些应用中非常的便利, 然而在许多其它的应用中, 这又非常的不适合. 例如, 验证者在一些情况下不愿意把公开可验证的签名给其他人, 如医疗记录、收入等等.

1996 年, Jakobsson 等人提出指定验证者签名(DVS)的概念[1]. 指定验证者签名能够提供消息的认证但不能提供传统数字签名的不可否认性的特征. 在指定验证者签名中, 仅仅指定的验证者可以验证签名的有效性, 然而指定验证者不能使任何第三方相信这个签名是真实有效的, 这是因为指定验证者总是可以生成一个有效的签名和签名者生成的签名不可区分. 在 2003 年, Saeednia 等人正式提出了强指定验证者签名(SDVS)的概念[2]. 在这个签名中, 除了指定验证者任何第三方都不能验证指定验证者签名因为签名的验证中需要指定验证者的私钥.

在 2003 年亚密会上, Steinfeld 等人提出了广义指定验证者签名(UDVS)的概念[3] 同时提出第一个广义指定验证者签名方案, 它是保护签名持有者隐私的一个重要工具. 在广义指定验证者签名中, 从"签名者"得到一个有效签名的"指定者(签名持有者)"能够使"指定验证者"相信他拥有一个从签名者那里得到的有效签名, 但是其他任何人(包括指定验证者)都不能使其他任何人相信这个事实. 在 PKC2004, Steinfeld 等人在文献[4]中提出如何从 Schnorr/RSA 签名中得到广义指定验证者签名. 在文献[5]中, 张方国等人扩展这个概念到基于身份的环境中并提出两个基于身份的广义指定验证者签名方案. 第一个无随机预言机下的广义指定验证者签名方案在文献[6]中被提出.

在 2005 年亚密会上, Joonsang Baek 等人在文献[7]中指出, 以前所有 UDVS 方案缺陷在于: 需要指定验证者根据签名者的公钥参数来建立自己的公钥并使它能够被认证以保证这个公钥和签名者提供的环境相匹配. 然而这个需求在实际中是不现实的. 因此文献[7]提出一个新型的广义指定验证者签名, 称为"广义指定验证者签名证明(UDVSP)", 在签名持有者和验证者之间使用高效的交互式协议解决了 UDVS 中存在的问题. 同时给出了 UDVSP 模型和安全定义, 并给出两个方案, 一个在随机预言机模型中基于 Boneh-Lynn-Shacham(BLS)签名方案[8](记为 UDVSP-BLS), 另一个在标准模型下基于 Boneh-Boyen(BB)签名方案[9](记为 UDVSP-BB).

本文中, 基于 Zhang-Safavi-Susilo(ZSS)签名方案[10]提出一个新的有效的广义指定验证者签名证明(记为 UDVSP-ZSS), 并在随机预言机模型中证明了方案的安全性. 和 UDVSP-BLS 相比, 所提方案中签名算法不需要对的运算, 验证算法和交互

收稿日期: 2006-10-27; 修回日期: 2006-11-28
基金项目: 国家自然科学基金(No. 60473027)

验证协议都仅仅需要一个对的运算,所以整个方案仅仅需要2个对运算,同时不需要使用特殊的hash函数(映射到点),因此方案更加有效,实用.

2 基础知识

2.1 双线性对

设$(G_1,+)$是由P生成的加法群,其阶数为素数q,$(G_2,\cdot)$是阶数为q的乘法群.设$e: G_1\times G_1\to G_2$是一个映射具有下面的性质:

(1)双线性性:对所有的$R, Q\in G_1$, $a, b\in Z_q$,都有$e(aR, bQ)=e(R, Q)^{ab}$.

(2)非退化性:存在$R, Q\in G_1$,满足$e(R, Q)\neq 1$.

(3)可计算性:对所有的$R, Q\in G_1$存在有效的算法计算$e(R, Q)$.

那么e称为双线性对.

2.2 多离散对数问题(OMDL)

文献[7]中,定义这个问题的实验为$\mathrm{Exp}^{\mathrm{OMDL}}(k)$:在给定参数$(q, P, e, G_1, G_2)$下一个多项式时间的攻击者$A$进行$n$次询问challenge预言机$C(\cdot)$和$m$次询问离散对数预言机$\mathrm{DL}_{q,P}(\cdot)$且$m<n$. $C(\cdot)$定义为:输入一个询问(空),$C(\cdot)$输出一个随机点$h\in_R G_1$; $\mathrm{DL}_{q,P}(\cdot)$定义为:输入一个询问z,$\mathrm{DL}_{q,P}(\cdot)$输出一个s满足$z=sP$.攻击者A的目标是生成由$C(\cdot)$输出的n个随机点的所有离散对数.

$\mathrm{Exp}^{\mathrm{OMDL}}(k)$: $(s_1,\cdots,s_n)\leftarrow A^{C(\cdot),\mathrm{DL}_{q,P}(\cdot)}(q, P, e, G_1, G_2)$, $h_1,\cdots,h_n$是由$C(\cdot)$输出的G_1中的随机点,如果满足$s_iP=h_i$ $(i=1,\cdots,n)$,则返回1;否则返回0.

攻击者A的优势(Advantage)定义为$\mathrm{Adv}_A^{\mathrm{OMDL}}(k)=\Pr[\mathrm{Exp}^{\mathrm{OMDL}}(k)=1]$,如果在参数$k$下$\mathrm{Adv}_A^{\mathrm{OMDL}}(k)$是可忽略的,那么OMDL问题是困难的.

2.3 k个叛逆者共谋攻击算法问题(k-CAA)

文献[10]中,定义这个问题的实验为$\mathrm{Exp}^{k\text{-}\mathrm{CAA}}(k)$:在给定参数$(q, P, e, G_1, G_2)$下一个多项式时间攻击者$A$

$\mathrm{Exp}^{k\text{-}\mathrm{CAA}}(k)$: $x, h_1,\cdots,h_k\overset{R}{\leftarrow}Z_q^*$, $k\leftarrow A(xP,\frac{1}{h_1+x}P,\cdots,\frac{1}{h_k+x}P)$,如果$k=\frac{1}{h+x}P$且$h\notin\{h_1,\cdots,h_k\}$,那么返回1;否则返回0.

攻击者A的优势(Advantage)定义为$\mathrm{Adv}_A^{k\text{-}\mathrm{CAA}}(k)=\Pr[\mathrm{Exp}^{k\text{-}\mathrm{CAA}}(k)=1]$,如果在参数$k$下$\mathrm{Adv}_A^{k\text{-}\mathrm{CAA}}(k)$是可忽略的,那么$k$-CAA问题是困难的.

3 广义指定验证者签名证明

3.1 模型

在广义指定验证者签名证明(UDVSP)中,包含三方:签名者,指定者(签名持有者)D和指定验证者DV.

定义1 一个广义指定验证者签名证明包含4个多项式时间算法和一个协议UDVSP=(KeyGen, Sign, Verify, Transform, IVerify).

(1)密钥生成算法(KeyGen):输入安全参数$k\in N$,输出签名者公钥私钥对(pk, sk).

(2)签名生成算法(Sign):输入签名者私钥sk,消息m,输出消息m的签名σ.

(3)签名验证算法(Verify):输入签名者的公钥pk,消息m以及签名σ,如果σ是消息m的有效签名,则输出1;否则输出0.

(4)转换算法(Transform):输入签名者公钥pk和签名σ下,该算法选取秘密值$\overline{\mathrm{sk}}$,使用这个值生成转换签名$\overline{\sigma}$,并输出$\overline{\sigma}$和$\overline{\mathrm{sk}}$.

(5)交互验证协议(IVerify):是指定者D和指定验证者DV之间的交互验证协议.D和DV共同输入为:签名者公钥pk,转化签名$\overline{\sigma}$以及消息m,秘密值$\overline{\mathrm{sk}}$仅仅为D的输入.在协议中,拥有$\overline{\mathrm{sk}}$的D试图使DV相信转换签名$\overline{\sigma}$是由有效签名σ而生成的.如果DV接受,则输出1;否则输出0.

在UDVSP中,密钥生成和签名两个算法由签名者完成.验证和转换算法由指定者完成.我们强调验证算法不能公开提供,签名必须在安全信道中传递.

3.2 安全定义

文献[7]中正式定义了UDVSP的安全性需求.对于UDVSP方案第一个安全需求和通常签名方案一样,需要满足适应性选择消息攻击下的存在性不可伪造[11].

对UDVSP第二个安全需求是能够抵抗伪装攻击,即攻击者(不拥有签名者生成的有效签名σ)不能伪装成诚实指定者D(拥有签名者生成的有效签名σ).伪装攻击被分为两类:TYPE-1和TYPE-2.在TYPE-1攻击中,攻击者(拥有转换签名$\overline{\sigma}$)伪装成一个不诚实指定验证者参与到交互验证协议中,并和诚实的指定者进行多次交互.然后,攻击者试图伪装成一个诚实的指定者和诚实的验证者交互.在TYPE-2攻击中,攻击者不拥有转换签名$\overline{\sigma}$,而是自己生成一个新的转换签名$\overline{\sigma}'$,并伪装成一个诚实的指定者在交互验证协议中和诚实的指定验证者交互.

4 高效的广义指定验证者签名证明

基于ZSS方案[10],提出一个有效的广义指定验证者签名证明(UDVSP-ZSS).具体如下:

(1)密钥生成算法KeyGen(k):随机选取$x\in_R Z_q^*$,计算$P_{\mathrm{pub}}=xP$.选取密码学hash函数$H:\{0,1\}^*\to Z_q^*$.则公钥为$\mathrm{pk}=(G_1, G_2, e, q, P, H, P_{\mathrm{pub}})$,私钥为$\mathrm{sk}=(x)$.

(2)签名生成算法Sign(sk, m):给定私钥x,消息$m\in\{0,1\}^*$,计算$\sigma=\frac{1}{H(m)+x}P$.则签名为σ.

(3)签名验证算法Verify(pk, m, σ):检验$e(H(m)P+P_{\mathrm{pub}},\sigma)\overset{?}{=}e(P, P)$.如果等式成立,输出1;否则输出0.

(4)转换算法Transform(pk, σ):随机选取$z\in_R Z_q^*$,计算$z\sigma=\frac{z}{H(m)+x}P$.输出$\overline{\sigma}=z\sigma$和$\overline{\mathrm{sk}}=z$.

(5)交互验证协议IVerify($[D(\overline{\mathrm{sk}})\leftrightarrow DV]$(pk, $\overline{\sigma}$, m)):指定者D和指定验证者DV共同计算$v_1=e(H(m)P+P_{\mathrm{pub}},\overline{\sigma})$和$v_2=e(P, P)$并进行以下交互

(a)D选取随机$s\in_R Z_q^*$,计算$w=v_2^s$并发送w给DV.

(b)DV选取随机$c\in_R Z_q^*$并发送给D.

(c) D 计算 $t = s + \alpha \bmod q$ 并发送 t 给 DV.

(d) DV 检验 $v_2^t \stackrel{?}{=} wv_1^c$. 如果等式成立, 则输出 1; 否则输出 0.

交互验证协议可以看作是证明 z 满足关系 $e(H(m)P + P_{pub}, \overline{\sigma}) = e(P, P)^z$ 的一个协议. 同时和以前所有 UDVS 方案相比, 新方案中不需要指定验证者去建立自己公钥私钥对.

5 所提方案的分析

5.1 安全性证明

在随机预言机模型中 ZSS 方案[10] 在假设 k-CAA 问题困难下能够抵抗适应性选择消息攻击的存在性伪造, 所以我们提出的 UDVSP-ZSS 方案也是安全的. 因此, 这里仅仅需要证明在伪装攻击下的安全性.

定理 1 假设 OMDL 问题在 G_1 中是困难的, 那么 UDVSP-ZSS 在随机预言机模型中能够抵抗 TYPE-1 伪装攻击.

证明 设 $A = (\overline{DV}, \overline{D})$ 是一个伪装者试图攻破 UDVSP-ZSS 方案, 设 B 是一个 OMDL 问题的攻击者, 同时给定 OMDL 问题的参数 $\{G_1, G_2, e, q, P\}$.

B 询问 OMDL 问题中的 challenge 预言机 $C(\cdot)$ 得到一个点 h_0, 假设对于某个随机 $s_0 \in_R Z_q^*$ 满足 $h_0 = s_0 P$, 注意 B 不知道 s_0. B 选取随机 $m \in \{0,1\}^*$ 以及 $x \in_R Z_q^*$, 计算 $P_{pub} = xP$, 选取 hash 函数 $H: \{0,1\}^* \rightarrow Z_q^*$, 那么输出 $pk = \{G_1, G_2, e, q, P, H, P_{pub}\}$ 作为签名者公钥.

在随机预言机模型中, B 模拟 hash 函数 H 具体如下: 当询问 m 时, B 返回 $H(m) = l \in Z_q^*$; 当询问 $m' \neq m$ 时, B 选取随机 $l' \in_R Z_q^*$, 返回 $H(m') = l'$. B 计算 $\overline{\sigma} = \frac{1}{l + x} h_0$ 作为转换签名发送给伪装者 A.

B 模拟 n 次不诚实指定验证者 $\overline{DV}$ 和诚实指定者 D 之间的交互验证协议 (IVerify) 具体如下: 首先 B 询问 challenge 预言机 $C(\cdot)$ 得到 n 个随机点 $h_i (i \in \{1, \cdots, n\})$, 并计算 $w_i = e(h_i, P)$ 发送给 $\overline{DV}$. $\overline{DV}$ 返回随机 $c_i \in_R Z_q^*$. B 向 $DL_{q,P}(\cdot)$ 询问 $h_i + c_i h_0$ 得到相应的回答 t_i 并返回给 $\overline{DV}$. $\overline{DV}$ 检验 $e(P, P)^{t_i} \stackrel{?}{=} w_i e(H(m)P + P_{pub}, \overline{\sigma})^{c_i}$.

由于 $s_0 \in_R Z_q^*$ 以及 $l, x \in_R Z_q^*$ 是随机的, 因此

$$\overline{\sigma} = \frac{1}{l + x} h_0 = \frac{s_0}{H(m) + x} P = s_0 \sigma$$

是随机的, 那么在上述模拟中转换签名 $\overline{\sigma}$ 的分布和真实攻击中的相同.

B 模拟的交互验证协议 (IVerify) 是正确的. (1) 因为 $s_i \in_R Z_q^*$ 是随机的, 所以 $w_i = e(h_i, P) = e(s_i P, P) = e(P, P)^{s_i}$ 是随机的, 由此可知在模拟中的 w_i 和真实协议 (a) 中由 D 发送的值具有相同的分布. (2) 因为 t_i 是 $h_i + c_i h_0$ 的离散对数, 则 $t_i = s_i + c_i s_0 \bmod q$, 即

$$\begin{aligned} e(P, P)^{t_i} &= e(P, P)^{s_i + c_i s_0} \\ &= e(P, P)^{s_i} e(P, P)^{c_i s_0} \\ &= w_i e(H(m)P + P_{pub}, \sigma)^{c_i s_0} \\ &= w_i e(H(m)P + P_{pub}, s_0 \sigma)^{c_i} \\ &= w_i e(H(m)P + P_{pub}, \overline{\sigma})^{c_i} \end{aligned}$$

B 完成上述的 n 次模拟后, B 目的是计算出 h_0 的离散对数, 然后计算出所有 $h_1, \cdots, h_n$ 的离散对数. 具体如下: 首先 B 运行 $\overline{D}$ 得到交互验证协议 (a) 中的 w, 其次随机选取 $c \in_R Z_q^*$ 发送给 $\overline{D}$, $\overline{D}$ 返回其响应 t, B 检验 $e(P, P)^t \stackrel{?}{=} we(H(m)P + P_{pub}, \overline{\sigma})^c$. 如果成立, B 在相同状态下选取不同的 $c' \in_R Z_q^*$ 发送给 $\overline{D}$, 并从 $\overline{D}$ 得到其相应的响应 t' 并检验 $e(P, P)^{t'} \stackrel{?}{=} we(H(m)P + P_{pub}, \overline{\sigma})^{c'}$. 如果成立, 根据"重排引理[12]" B 计算 $\frac{t - t'}{c - c'} \bmod q$ 即为 h_0 的离散对数 s_0. 因为

$$\begin{aligned} e\left(P, \frac{t - t'}{c - c'} P\right) &= e(P, (t - t')P)^{\frac{1}{c - c'}} \\ &= (e(P, P)^{t - t'})^{\frac{1}{c - c'}} \\ &= (e(P, P)^t \cdot e(P, P)^{-t'})^{\frac{1}{c - c'}} \\ &= (e(H(m)P + P_{pub}, \overline{\sigma})^c \cdot e(H(m)P \\ &\quad + P_{pub}, \overline{\sigma})^{-c'})^{\frac{1}{c - c'}} \\ &= e(H(m)P + P_{pub}, \overline{\sigma}) \\ &= e(H(m)P + P_{pub}, \frac{s_0}{H(m) + x} P) \\ &= e((H(m) + x)P, \frac{s_0}{H(m) + x} P) \\ &= e(P, s_0 P) \end{aligned}$$

由 $s_0 = \frac{t - t'}{c - c'} \bmod q$ 计算出 $s_i = t_i - cs_0 (i = 1, \cdots, n)$, 则 $s_1, \cdots, s_n$ 即为点 $h_1, \cdots, h_n$ 的离散对数. 最后 B 输出 $s_0, s_1, \cdots, s_n$ 即为 OMDL 问题的解. 证毕

定理 2 假设 k-CAA 问题在 G_1 中是困难的, UDVSP-ZSS 在随机预言机模型中能够抵抗 TYPE-2 伪装攻击.

证明 已知在随机预言机模型中假设 k-CAA 问题困难下, ZSS 签名方案[10]能够抵抗适应性选择消息攻击的存在性伪造, 因此可以得到 ZSS 方案的不可伪造性到 TYPE-2 攻击下 UDVSP-ZSS 安全性的规约.

假设 A 是一个伪装者试图攻破 UDVSP-ZSS, B 是 ZSS 签名方案的伪造者.

假设 B 被给定 ZSS 方案的公钥 $\{G_1, G_2, e, q, P, H, P_{pub}\}$ 满足 $P_{pub} = xP$, hash 函数 $H: \{0,1\}^* \rightarrow Z_q^*$ 被看作是随机预言机. 那么 B 输出 $\{G_1, G_2, e, q, P, H, P_{pub}\}$ 作为签名者的公钥, 并任意选取 $m \in \{0,1\}^*$.

首先 B 得到由 A 生成的转换签名 $\overline{\sigma}$, 然后 B 运行 A 得到交互验证协议 (a) 中的 w, B 随机选取 $c \in_R Z_q^*$ 发送给 A, 并从 A 得到响应 t 并检验 $e(P, P)^t \stackrel{?}{=} we(H(m)P + P_{pub}, \overline{\sigma})^c$. 如果成立, B 在相同状态下选取不同的 $c' \in_R Z_q^*$, 并从 A 得到其响应 t' 并检验 $e(P, P)^{t'} \stackrel{?}{=} we(H(m)P + P_{pub}, \overline{\sigma})^{c'}$. 如果成立, 由"重排引理[12]"可知, B 计算 $\frac{c - c'}{t - t'} \overline{\sigma}$ 即为消息 m 有效的伪造 ZSS 签名. 由上述两个方程可知:

$$\begin{aligned} e(P, P)^t / e(P, P)^{t'} &= e(H(m)P + P_{pub}, \overline{\sigma})^c / e(H(m)P \\ &\quad + P_{pub}, \overline{\sigma})^{c'} \\ e(P, P)^{t - t'} &= e(H(m)P + P_{pub}, \overline{\sigma})^{c - c'}, \end{aligned}$$

$$e(P, P) = e(H(m)P + P_{pub}, \overline{\sigma})^{\frac{c-c'}{t-t'}}$$

$$e(P, P) = e(P, \overline{\sigma})^{\frac{c-c'}{t-t'}\cdot(H(m)+x)},$$

$$e(P, P)^{\frac{1}{H(m)+x}} = e\left(P, \frac{c-c'}{t-t'}\overline{\sigma}\right)$$

$$e\left(P, \frac{1}{H(m)+x}P\right) = e\left(P, \frac{c-c'}{t-t'}\overline{\sigma}\right)$$

因此$\frac{c-c'}{t-t'}\overline{\sigma} = \frac{1}{H(m)+x}P$即为消息$m$的有效ZSS签名,由规约可知定理得证.　　证毕

5.2　效率

表1中比较提出的UDVSP-ZSS方案和UDVSP-BLS方案[3]的计算代价.定义Pa为对运算,Pm为群G_1中标量乘运算,Ad为群G_1中点加运算,Inv为Z_q中逆运算,MTP为映射到点(MapToPoint)特殊的hash运算,Pro为证明离散对数知识的协议(我们考虑预计算,忽略通常hash函数运算).

表1　计算代价的比较

阶段	UDVSP-ZSS						UDVSP-BLS					
	Pa	Pm	Ad	Inv	MTP	Pro	Pa	Pm	Ad	Inv	MTP	Pro
签名	0	1	0	1	0	0	1	0	0	0	1	0
验证	1	1	1	0	0	0	2	0	0	0	1	0
转换	0	1	0	0	0	0	0	1	0	0	0	0
交互协议	1	1	1	0	0	1	2	0	0	0	1	1

我们强调对(pairing)的计算是最费时间的,尽管有许多文章讨论对的复杂性以及如何加速对的运算[13],但是对的运算仍然是耗费时间的.和UDVSP-BLS方案相比,提出的UDVSP-ZSS方案中,转换算法相同,签名算法不需要对的运算,同时$e(P,P)$能够通过预计算并且作为签名者公钥的一部分,所以在验证算法和交互验证协议中都仅仅需要一个对的运算.此外,所提方案中不需要使用映射到点(MapToPoint)特殊的hash函数,通常这种hash函数的运算是概率性的,至少需要解有限域上的一个平方或立方方程,所以其运算量大于z_q中逆的运算[10].因此我们提出的UDVSP-ZSS方案更加的有效和实际.

6　结论

基于ZSS签名方案,我们提出一个高效的广义指定验证者签名证明(UDVSP-ZSS),并在随机预言机模型下,给出该方案的安全性证明.新方案中签名算法不需要对的运算,在预计算下,验证算法和交互验证协议中仅仅需要一个对的运算,同时不需要使用映射到点特殊的hash函数,所提方案更加的有效.

参考文献:

[1] M Jakobsson, K Sako, R Impagliazzo. Designated verifier proofs and their applications[A]. Eurocrypt'96, LNCS 1070[C]. Berlin: Springer Verlage, 1996. 143-154.

[2] S Saeednia, S Kramer, O Markovitch. An efficient strong designated verifier signature scheme[A]. ICISC'03, LNCS 2971[C]. Berlin: Springer Verlage, 2003. 40-54.

[3] R Steinfeld, L Bull, H Wang, et al. Universal designated-verifier signatures[A]. Asiacrypt'03, LNCS 2894[C]. Berlin: Springer-Verlage, 2003. 523-542.

[4] R Steinfeld, H Wang, J Pieprzyk. Efficient extension of standard Schnorr/RSA signatures into universal designated-verifier signatures[A]. PKC'04, LNCS 2947[C]. Berlin: Springer Verlage, 2004. 86-100.

[5] F Zhang, W Susilo, Y Mu, et al. Identity-based universal designated verifier signatures[A]. SecUbiq'05, LNCS 3823[C]. Berlin: Springer-Verlage, 2005. 825-834.

[6] R Zhang, J Furukawa, H Imai. Short signature and universal designated verifier signature without random oracles[A]. ACNS'05, LNCS 3531[C]. Berlin: Springer Verlage, 2005. 483-898.

[7] Joonsang Baek, Reihaneh Safavi-Naini, Willy Susilo. Universal designated verifier signature proof (or how to efficiently prove knowledge of a signature)[A]. Asiacrypt'05, LNCS 3788[C]. Berlin: Springer-Verlage, 2005. 644-661.

[8] D Boneh, B Lynn, H Shacham. Short signatures from the weil pairing[A]. Asiacrypt'01, LNCS 2248[C]. Berlin: Springer Verlage, 2001. 566-582.

[9] D Boneh, X Boyen. Short signatures without random oracles[A]. Eurocrypt'04, LNCS 3027[C]. Berlin: Springer Verlage, 2004. 56-73.

[10] Fangguo Zhang, Reihaneh Safavi-Naini, Willy Susilo. An efficient signature scheme from bilinear pairings and its applications[A]. PKC'04, LNCS 2947[C]. Berlin: Springer Verlage, 2004. 277-290.

[11] S Goldwasser, S Micali, R Rivest. A digital signature scheme secure against adaptive chosen message attack[J]. SIAM Journal on Computing, 1988, 17(2): 281-308.

[12] M Bellare, A Palacio. GQ and schnorr identification schemes: proofs of security against impersonation under active and corrcurrent attack[A]. Crypto'02, LNCS 2442[C]. Berlin: Springer Verlage, 2002. 162-177.

[13] P S L M Barreto, H Y Kim, B Lynn, et al. Efficient algorithms for pairing-based cryptosystems[A]. Crypto'02, LNCS 2442[C]. Berlin: Springer Verlage, 2002. 354-368.

作者简介:

明　洋　男,1979年12月出生于陕西省榆林市,现为西安电子科技大学博士研究生.主要研究方向为密码学、数字签名理论.

E-mail: mingyang2001@sohu.com