A Secure ID-based Verifiably Encrypted Signature Scheme

Xin Xiangjun[1], Zhang Hongwei[2]

1. Department of Mathematics and Information Science, Zhengzhou University of Light Industry, Zhengzhou, China

2. Department of Mathematics, Henan University of Technology, Zhengzhou, China

xinsubmission@tom.com

Abstract: To improve the security and efficiency of the id-based verifiably encrypted signature (ID-VES) schemes, constructing a fraction in which the mast key is included in the numerator and the sum of the session key and the output of the hash function is included in the denominator, and using the fraction to multiply the generator of the gap Diffie-Hellman group, an id-based signature scheme is proposed. Then, by dividing the private key of the signer into two parts in which the former is used to generate an ID-based signature and the later is used to generator ID-VES, a novel ID-VES scheme is proposed, which can be proved to be secure in random oracle model. Compared with the other schemes, the new scheme is more efficient, since it has the shortest signature and the least pairing operations.

Keywords: signature; id-based signature; verifiably encrypted signature; bilinear pairing

一个安全的基于身份的可验证加密签名方案

辛向军[1]，张宏伟[2]

1.郑州轻工业学院数学与信息科学系，郑州，中国，450002

2.河南工业大学理学院，郑州，中国，450002

xinsubmission@tom.com

【摘要】为提高基于身份的可验证加密签名的安全性和效率，构造分数使得其分母与分子分别含有主密钥以及 Hash 函数与临时密钥之和，并用该分数乘以间隙 Diffie-Hellman 群的生成元，给出了一个基于身份的签名．然后将签名者的私钥分为两部分，前者用于生成签名，后者用来生成可验证加密签名，从而给出了一个新的基于身份的可验证加密签名方案，该方案在随机预言机下是可证明安全的．与已知方案相比，新方案具有最短的签名和最少的对运算，故其更为高效．

【关键词】签名；基于身份的签名；可验证加密签名；双线性对

1 引言

可验证加密签名方案(VESS)[1, 2]是普通签名的一种扩展，其可用于构建优化的公平交换协议[3]．一个VESS中有三个参与方：签名者，验证者和仲裁者．其中，签名者用仲裁者的公钥对自己签发的一个标准签名(SS)加密而产生一个可验证加密签名(VES)，任何人都可验证VES的合法性．并且，仲裁者能够解密VES而恢复出相应的SS．一个VESS应满足两个安全性要求[1]：(1)不可伪造性，即敌手伪造一个VES是困难的；(2)不透明性(Opacity)，即敌手很难由VES恢复出相应的SS。

最近，Gu和Cheng等[4-6]提出三种基于身份的可验证加密签名方案(ID-VESS)．然而，文[4]方案并不能抵抗伪造VES攻击和合谋攻击[7]，文[5]并未给出相应的安全模型．并且，文[4-6]的每个方案至少需要三个对运算，而较多的对运算明显地影响着方案的计算速度[8]．为此，我们给出了一种新的ID-VESS，其有最短的签名和最少的对运算．因此，我们的方案的计算效率优于类似的方案，并且，该方案在强化的安全模型下是可证明安全的。

本文安排如下：第2节简要回顾一些基本知识；第3节构造一个基于身份的签名方案(IBS)；第4节给出一个新的ID-VESS；第5节和第6节分别给出方案的效率分析和安全性分析。

2 预备知识－双线性对

令 λ 为一个安全参数，双线性对定义为e：$G_1\times G_1\to G_2$，其中G_1和G_2分别为阶为素数p(p的二进制长度为

基金项目：河南省教育厅自然科学研究项目(No. 2009B120003)；郑州轻工业学院博士科研基金资助.

978-1-935068-01-3

λ)的循环加群和循环乘群，P为G_1的生成元．e有以下性质：(1) 双线性：任给$R, S\in G_1$和$a, b\in Z_p^*$, $e(aR, bS) = e(R, S)^{ab}$. (2) 非退化性：存在$R, S\in G_1$使得$e(R, S)\neq I$. (3) 可计算性：给定$R, S\in G_1$，存在有效算法计算$e(R, S)$.

定义1 离散对数问题(DLP)：给定$Q\in G_1^*$，计算$a\in Z_p^*$,使得$Q=aP$.

定义2 计算Diffie-Hellman问题(CDHP)：任给(P, aP, bP)，其中$a, b\in Z_p^*$，计算abP.

定义3 逆计算Diffie-Hellman问题(Inv-CDHP)：对于$b\in Z_p^*$和bP，计算$b^{-1}P$.

定义4 k-合谋攻击问题(k-CAAP)[9, 10]：给定$(P, Q = xP, h_1, \ldots, h_k\in Z_p, P/(h_1+x),\ldots,P/(h_k+x))$，计算$P/(h+x)$使得$h\notin\{h_1, \ldots,h_k\}$.

假定 CDHP, Inv-CDHP 和 k-CAAP 是困难的.

3 一个新的基于身份的签名方案

3.1 方案的构造

Setup: 设参数$\{\lambda, G_1, G_2, P, p, e\}$如上节所述，定义密码Hash函数$H_1$: $\{0, 1\}^*\rightarrow Z_p^*$, H_2: $\{0, 1\}^*\times G_1\rightarrow Z_p^*$. PKG随机选取$s\in Z_p^*$，计算$P_{pub}=sP$. s用作PKG的主密钥，而P_{pub}用作PKG的公钥．系统公开参数为$\{\lambda, G_1, G_2, P, p, e, H_1, H_2, P_{pub}, g\}$，其中$g=e(P, P)$.

Extract: PKG计算私钥$S_{ID}=P/(H_1(ID)+s)$并将S_{ID}通过安全信道发送给用户ID.

Sign: 用户ID通过以下步骤对消息$m\in\{0, 1\}^*$进行签名：(S1)随机选取$x\in Z_p^*$并计算$r=xP$, $h=H_2(m, r)$；(S2) 计算$W=(x+h)S_{ID}$. 消息m的签名为(r, W).

Verify: 验证者计算$h=H_2(m, r)$，而签名(h, W)有效当且仅当$e(W, H_1(ID)P+P_{pub})=e(r+hP, P)$，或者

$$e(W, H_1(ID)P+P_{pub})=e(r, P)g^h.$$

3.2 安全性分析

游戏1：称一个IBS方案在适应性选择消息和ID攻击下是不可伪造的，如果不存在概率多项式时间(PPT)敌手A能够以不可忽略的概率赢取以下游戏[11]：(1)挑战者运行Setup算法产生系统公开参数并将它们发送给敌手A; (2) A进行如下一系列适应性询问：

－Hash询问：当A询问Hash函数的值时，挑战者计算其相应的值并将其发送给A。

－密钥提取询问(Extract-O(ID))：输入用户ID，挑战者运行Extract(ID)算法得到相应的私钥s_{ID}并返回s_{ID}.

－签名询问(Sign-O(ID, m))：任给(ID, m)，挑战者运行Sign(ID, m)算法返回相应的签名σ。

最后，A输出(ID^*, m^*, σ^*)，其中ID^*为一个身份，m^*为一个消息，σ^*为关于(ID^*, m^*)的签名，并且A从未询问过Extract(ID^*)和Sign(ID^*, m^*)。

游戏2：文[11]给出了适应性选择消息和给定ID攻击的定义：在上述的游戏中，首先固定一个ID_0，在步骤1中挑战者将系统公开参数和ID_0发送给敌手A；在步骤3中，A必须输出给定ID_0的一个消息m以及与它们相应的一个签名，其中ID_0从未作为密钥提取询问的输入，且从来未在签名询问中询问过关于(ID_0, m)签名．若A能够以不可忽略的概率赢取这种游戏，则称方案在适应性选择消息和给定ID攻击下是抗存在性伪造攻击的.

定理1 我们的签名方案在适应性选择消息和ID攻击下是抗存在性伪造攻击的。

证明：由文[11]可知：若存在多项式时间算法$A0$能够通过适应性选择消息和ID攻击以不可忽略的概率在游戏1中获胜，则存在多项式时间敌手$A1$能够通过适应性选择消息和给定ID攻击以一个不可忽略的概率在游戏2中获胜．这样,只须证明我们的方案可抵抗适应性选择消息和给定ID攻击下的存在性伪造。

Setup: 令公开参数$\{\lambda, G_1, G_2, P, p, e, H_1, H_2, P_{pub}\}$如3.1节所述, C为挑战者．假定敌手$A1$至多分别对H_1、H_2、Extract-O和Sign-O提问q_{H1}, q_{H2}, q_E, q_S次．现在C收到了参数$h_1,\ldots,h_k\in Z_p$以及$P/(h_1+s),\ldots, P/(h_k+s)$，其中$k=q_{H1}$．$C$保存列表list_H1和list_H2，并将它们初始化为空. $A1$可适应性地进行如下询问:

－$H_1(ID_i)$询问：当询问$H_1(ID_i)$时，C首先检查在list_H1中是否存在$(ID_i, H_1(ID_i), \delta_i, t_i)$. 若存在，$C$返回$(ID_i, H_1(ID_i))$;否则, C随机选取$t_i\in Z_p^*$满足$t_i\notin\{h_1, \ldots,h_k\}$，抛硬币$\delta_i\in\{0, 1\}$，其中Pr $[\delta_i=0]=1/(q_E+1)$，然后置$H_1(ID_i):= \delta_i h_i+(1-\delta_i)t_i$，并将$(ID_i, H_1(ID_i))$作为回答，同时，$C$将$(ID_i, H_1(ID_i), \delta_i, t_i)$添加到列表list_H1中。

－$H_2(m_i, r_i)$询问：当询问$H_2(m_i, r_i)$时，C检查是否在list_H2中存在(m_i, r_i, a_i). 若存在，则C返回a_i；否则，C随机选取$a_i\in Z_p^*$并置$H_2(m_i, r_i):=a_i$，并将a_i作为对$A1$的回答，同时，C将(m_i, r_i, a_i)添加至列表list_H2之中。

－E-O(ID_i)询问：当询问E-O(ID_i)时，C询问自己$H_1(ID_i)$. 若$\delta_i=0$，则C返回$fail$;否则，C置$s_{IDi}:=P/(h_i+s)$并将s_{IDi}作为对$A1$的回答。

－Sign-O(ID_i, M_i): 当询问Sign-O(ID_i, M_i)时，C执行步骤：(Step 1) 询问自己$H_1(ID_i)$; (Step 2) 随机选取d_i, $l_i\in Z_p^*$，计算$W_i=l_iP$和$r_i=l_iP_{pub}+(l_iH_1(ID_i)-d_i)P$; (Step 3) 若$H_2(M_i, r_i)$已被询问过，则$C$宣布$fail$(这个事件以一个可忽略的概率发生). 否则，$C$定义$H_2(M_i, r_i)=d_i$，将$(M_i, r_i, d_i)$添加至list_H2，并返回$(ID_i, M_i, r_i, W_i)$作为回答．易证$(r_i, W_i)$的有效性。

最后，敌手$A1$以一个不可忽略的概率ε_0输出有效签名$(ID, m, r, W; h)$，其中$h=H_2(m, r)$，且ID从未作为密

钥提取询问的输入, Sign-O从未输出(ID, m, r, W). 若相应list_H1中($ID, H_1(ID), \delta, t$)的δ=1, 则C宣布失败$fail$.

在上述游戏中C成功得到(ID, m, r, W)且δ=0的概率 $\varepsilon_1 \geq \varepsilon_0/(\omega(q_E+1))$, 其中 ω 为自然对数的底数. 将C视为文[12]的Fork引理中的敌手, 可知存在多项式时间算法B, 其产生签名($ID, m, r, W; h$)和($ID, m, r, W^*; h^*$), 并且它们满足等式$e(W, H_1(ID)P+P_{pub})=e(r+hP, P)$和等式$e(W^*, H_1(ID)P+P_{pub})=e(r+h^*P, P)$, 则由此$B$便可计算出$(W^*-W)/(h^*-h)= P/(H_1(ID)+s)$. 可知$H_1(ID)=t$, $t \notin \{h_1,\ldots,h_k\}$, 即 B 和 C 结合可计算 $P/(t+s)$ 使得 $t \notin \{h_1,\ldots, h_k\}$, 这与$k$-CAAP困难假设相矛盾. 这说明我们方案在适应性选择消息和ID攻击下是抗存在性伪造攻击的。

4 新的基于身份的可验证加密签名方案

Setup: 令参数{ λ, G_1, G_2, P, p, e, H_1, H_2 , P_{pub}}如3.1节所述, 其中$P_{pub}=sP$, s用作PKG的主密钥, 而P_{pub}用作PKG的公钥. 设仲裁者T的公钥为$P_T=s_TP$, 其中$s_T \in Z_p^*$为仲裁者的私钥. 令$g=e(P, P)$, $g_T=e(P_T, P)$. 公开参数为{ λ, G_1, G_2, P, p, e, H_1, H_2, P_{pub}, P_T, g, g_T}。

VesExtract: 任给一个用户ID, PKG计算其私钥($S_{ID}, S_{ID\text{-}VES}$), 其中$S_{ID}=P/(H_1(ID)+s)$, $S_{ID\text{-}VES}=P_T/(H_1(ID)+s)$. PGK通过一个安全的信道将私钥($S_{ID}, S_{ID\text{-}VES}$)发送给用户ID。

Sign, Verify: 同3.1节.

VesSign: 用户ID通过以下步骤产生关于(ID, m)的ID-VES: (Step 1) 随机选取$x \in Z_p^*$并计算$r=xP$, $h=H_2(m, r)$; (Step 2) 计算$V=(x+h)S_{ID\text{-}VES}$.

关于(ID, m)的ID-VES为(r, V).

VesVerify: 当且仅当 $e(V, P_{pub}+H_1(ID)P)=e(P_T, r+hP)$或者$e(V, P_{pub}+H_1(ID)P)=e(P_T, r)g_T^h$成立时D-VES签名($r, V$)有效, 其中$h=H_2(m, r)$,.

Adjudication: 仲裁者由 ID-VES 签名(r, V)计算$W=V/s_T$得到相应的签名(r, W)。

5 方案的正确性与效率分析

5.1 正确性要求

ID-VESS应满足以下正确性要求: (R1) 任给一个(ID, m)及其相应的ID-VES签名(r, V), (r, V)的有效性都能得到公开验证; (R2) 任给一个(ID, m)及其相应的有效的ID-VES签名(r, V), 仲裁者对(r, V)的解密输出都必定是关于(ID, m)的一个有效的基于身份的签名。

易知我们的方案满足R1和R2, 而由文[7]的分析可知, 文[4]的ID-VESS不满足正确性要求R2。

5.2 效率分析

假定P_m和P_a分别表示群G_1中的标量乘法运算和加法运算, P_p表示G_2中元素的幂指数运算, P_e表示对运算. 假定文[4-6]与本文使用了参数 λ, 则可给出如下的效率比较(表1)。

表1 类似方案的比较

方 案	ID-VES 的长度	产 生 ID-VES	验 证 ID-VES	解 密 ID-VES
新方案	2 λ	$2P_m$	$2P_e+1P_a+1P_m+1P_p$	$1P_m$
[4]	4 λ	$5P_m+2P_p$	$3P_e+1P_a+1P_m$	$1P_e+1P_m+2P_a$
[5]	3 λ	$5P_m+2P_a$	$3P_e+1P_a+1P_m$	$1P_m+1P_a$
[6]	3 λ	$5P_m+2P_a$	$3P_e+1P_a+1P_m$	$1P_m+1P_a$

由以上比较可知, 新方案具有最短的签名和最少的对运算, 即新方案的签名生成速度比类似方案至少提高两倍, 而签名验证时间比类似方案减少约1/3. 另外, 文[4]的方案并不安全[7], 而文[5]并未给出安全模型下的安全证明, 这都直接影响到它们在实践中的应用。

6 安全性分析

6.1 不可伪造性

定义5 称ID-VESS在适应性选择消息、ID、签名和ID-VES攻击(A-M-ID-S-VES)下进行存在性伪造是困难的, 若不存在PPT敌手F能够以不可忽略的概率在以下的游戏中成功: (G1) 挑战者C运行ID-VESS的Setup并将公开参数Ω发送给F; (G2) 敌手适应性进行如下询问:

－VesExtract预言机VES-E-O: 输入身份ID, 则输出相应的私钥Key_{ID}, 即Key_{ID}←VES-E-O(ID);

－Sign预言机Sign-O: 输入身份-消息对(ID, m), 输出对应的签名(ID, m, σ), 即(ID, m, σ)←Sign-O(ID, m);

－VesSign预言机VesSign-O: 输入身份-消息对(ID, m), 输出对应的ID-VES签名(ID, m, δ);

－Adjudication预言机A-O: 输入有效的ID-VES签名(ID, m, δ), 输出(ID, m, δ)所包含的有效基于身份签名(ID, m, ω), 即(ID, m, ω)←A-O(ID, m, δ);

最后, F输出关于身份标识-消息对(ID^*, m^*)的有效ID-VES 签名 (ID^*, m^*, ω *), 而 F 从未询问过VES-E-O(ID^*), 且VesSign-O从未输出过(ID^*, m^*, ω *)。

可知文[4, 5]的方案并不能抵抗A-M-ID-S-VES攻击, 这是由于当敌手通过询问Sign-O(ID^*, m^*)得到签名(ID^*, m^*, σ *)时, 则敌手利用类似文[4, 5]中ID-VESS的

978-1-935068-01-3 © 2009 SciRes.

生成步骤很容易构造出VesSign-O从未输出的签名(ID^*, m^*, ω^*)。

定理2 若k-CAAP问题是困难的，则我们的签名方案在A-M-ID-S-VES攻击下是抗存在性伪造攻击的.

证明：假定存在PPT敌手F能够以一个不可忽略的概率 ε 在定义5的游戏中获胜. 算法中C作为挑战者回答对预言机的提问。

Setup：假定参数{ λ, G_1, G_2, P, p, e, H_1, H_2, P_{pub}}如3.1节所述，其中P_{pub}为PKG的公钥，s为主密钥. 现在C收到了参数h_1, …, $h_k \in Z_p$, $P/(h_1+s)$,…,$P/(h_k+s) \in G_1$. C随机选取$a \in Z_p^*$并计算$P_T=aP$. 将P_T模拟作为仲裁者的公钥. 令$g=e(P, P)$, $g_T=g^a$. 在下面的游戏中，F至多能够进行q_{H1}次H_1询问，q_{H2}次H_2询问，q_E次VES-E-O询问，q_S次Sign-O询问，q_{VS}次VesSign-O询问，q_A次A-O询问. 为简化证明，假定$k=q_{H1}$，并且所有的预言机在使用Hash函数H_1之前，需先进行H_1询问. C保存列表list_H1和list_H2，并将它们初始化为空. 假定下面的询问从不重复。

－$H_1(ID_i)$询问，$H_2(m_i, r_i)$询问：同定理1中的证明。

－VES-E-O(ID_i)询问：当F询问VES-E-O(ID_i)时，C调用定理1中的E-O(ID_i). 若E-O(ID_i)返回*fail*，则C返回*fail*;否则C得到S_{ID_i}=E-O(ID_i)，计算$S_{IDi\text{-}VES}=aS_{IDi}$，并将 ($S_{IDi}$, $S_{IDi\text{-}VES}$)作为对F的回答.。

－Sign-O(ID_j, M_j)：同定理1中的证明。

－VesSign-O(ID_n, R_n)：输入身份标识-消息对(ID_n, R_n)，C询问自己Sign-O(ID_n, R_n)而得到相应的签名(r_n, W_n). C计算$V_n=aW_n$，并将(r_n, V_n)作为回答。

－A-O(ID_n, R_n, r_n, V_n)：当询问A-O(ID_n, R_n, r_n, V_n)时，C计算$W_n=V_n/a$，并将(ID_n, R_n, r_n, W_n)作为回答。

最后F以概率 ε 输出有效ID-VES签名(ID, m, r, V)，且F从未询问过VES-E-O(ID)，且VesSign-O从未输出过(ID, m, r, V). 若C通过运行算法F得到上述的(ID, m, r, V)并且在list_H1中相应的 δ=0，则C成功，否则C宣布*fail*。

假定C在上述游戏中成功的概率为 ε_1. 类似于定理1的证明，可知 $\varepsilon_1 \geq \varepsilon/[\zeta(q_E+1)]$，其中 ζ 为自然对数的底数. 并由定理1的证明思想及Fork引理可知存在PPT算法B能够以不可忽略的概率得到不同的有效ID-VES签名(ID, m, r, V; h)及(ID, m, r, V^*; h^*)，满足$e(V, P_{pub}+H_1(ID)P)=e(P_T, r+hP)$和 $e(V^*, P_{pub}+H_1(ID)P)=e(P_T, r+h^*P)$，由此可知$(V^*-V)/(h^*-h)=P_T/(H_1(ID)+s)$. 算法$B$和$C$结合便可计算出$(V^*-V)/[a(h^*-h)]=P/(H_1(ID)+s)$. 由于其中$ID$从未作为密钥提取询问的输入，且由 δ=0 知成立 $P/(H_1(ID)+s) \notin \{P/(h_1+s),\ldots,P/(h_k+s)\}$，可知 $H_1(ID)=t$，且$t \notin \{h_1,\ldots,h_k\}$. 这与$k$-CAAP假设相矛盾. 故我们的方案在A-M-ID-S-VES攻击下可抗存在性伪造攻击。

6.2 不透明性

定义6 称ID-VESS在A-M-ID-S-VES攻击下具有不透明性，若不存在PPT敌手F能够以一个不可忽略的概率在以下的游戏中成功：(G1) 挑战者C运行ID-VESS的Setup算法并将系统公开参数 Ω 发送给F; (G2) 敌手可适应性地询问预言机VES-E-O、Sign-O、VesSign-O和A-O; (G3) F输出一个关于(ID, m)的有效ID-VES签名(ID, m, ω)和相应的签名(ID, m, σ)，而F从未询问过VES-E-O(ID)，且Sign-O及A-O从未输出过(ID, m, σ)。

定理3 在k-CAAP和Inv-CDHP问题困难假设下，我们的方案在A-M-ID-S-VES攻击下具有不透明性.

证明：假定挑战者 C 及敌手 F 执行如定理 2 中的算法及询问. 最后敌手以一个不可忽略的概率输出一个关于(ID, m)的有效 ID-VES 签名(ID, m, r, V)及相应的签名(ID, m, r, W)，而 F 从未询问过 VES-E-O(ID)，且 Sign-O 及 A-O 从未输出过(ID, m, r, W). 由定理 2 可知，我们的 ID-VESS 具有不可伪造性，因此，(ID, m, r, V)必定为 VesSign-O 的一个输出. 由定理 2 中 VesSign-O 算法的构造可知，V 为 G_1 中任意的一个元素，$W=a^{-1}V$. 这样，F 并不知道 a(否则敌手 F 可求解 P_T 关于 P 的离散对数)，但 F 可由(V, aV)计算出 $a^{-1}V=W$，这与 Inv-CDHP 困难假设相矛盾. 因此，在 k-CAAP 和 Inv-CDHP 困难假设下，我们的签名方案在 A-M-ID-S-VES 攻击下具有不透明性。

7 结束语

本文通过构造一个 IBS，给出一个新的 ID-VESS 及相应的安全模型. 与同类的方案相比，新 ID-VESS 具有最短的签名和最少的对运算. 因此，我们的方案效率高于其他类似方案. 在 A-M-ID-S-VES 和 A-M-ID-S-VES 攻击下，新方案是可证明安全的。

References (参考文献)

[1] Boneh D, Gentry C, Lynn B, et al. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps [A]. EURCRYPT'03, LNCS 2656[C]. Berlin: Springer-Verlag, 2003, P514−532.

[2] Ateniese G. Verifiable Encryption of Digital Signatures and Applications [J]. ACM Transactions on Information and System Security, 2004, 7(1), P1−20.

[3] Camenish J, Shoup V. Practical Verifable Encryption and Decryption of Discrete Logarithm [A]. CRYPTO 2003, LNCS 2729[C]. Berlin: Springer-Verlag, 2003: P195−211.

[4] Gu C, Zhu Y. An ID-based Verifiable Encrypted Signature Scheme Based on Hess' Scheme [A]. CISC 2005, LNCS 3882[C]. Berlin: Springer-Verlag, 2005, P42−52.

[5] Cheng X, Liu J, Wang X. Identity-Based Aggregate and Verifiably Encrypted Signatures from Bilinear Pairing [A]. ICCSA 2005, LNCS 3483[C]. Berlin: Springer-Verlag, 2005, P1046−1054.

[6] Gu Chunxiang, Zhang Yajuan, Zhu Yuefei. A Mixed Verifiably Encrypted Signature Scheme and It's Applications [J]. Acta Electronica Sinica, 2006, 34(5), P878−882(Ch).
顾纯祥, 张亚娟, 祝跃飞. 混合可验证加密签名体制及应用[J]. 电子学报, 2006, 34(5), P878−882.

[7] Zhang Zhenfeng. Cryptanalysis of an Identity-Based Verifiably Encrypted Signature Scheme [J]. Chinese Journal of Computers, 2006, 29(9), P1688−1693.
张振峰. 基于身份的可验证加密签名协议的安全性分析[J]. 计算机学报, 2006, 29(9), P1688−1693.

[8] Barreto P. S. M, Lynn B, Scott M. On the Selection of Pairing-friendly Groups [A]. SAC 2003, LNCS 3006[C]. Berlin: Springer-Verlag, 2003: P203−256.

[9] Mitsunari S, Sakai R, Kasahara M. A New Traitor Tracing [J]. IEICE Trans., 2002, E85-A (2), P481−484.

[10] Zhang F, Safavi-Naini R, Susilo W. An Efficient Signature Scheme from Bilinear Pairings and Its Applications [A]. PKC 2004, LNCS 2947[C]. Berlin: Springer-Verlag, 2004, P277−290.

[11] Cha C J, Cheon J H. An Identity-based Signature from Gap Diffie-Hellman Groups [A]. PKC 2003, LNCS 2567[C]. Berlin: Springer-Verlag, 2003, P18−30.

[12] Pointcheval D, Stern J. Security Arguments for Digital Signatures and Blind Signatures [J]. J. Cryptology, 13(3), 2000, P361–396.

978-1-935068-01-3 © 2009 SciRes.