标准模型下安全的基于身份的可验证加密签名

王天芹[1] 苏莉文[2]

(华北水利水电学院信息工程系 郑州 450011)[1] (国家质检总局信息中心 北京 100088)[2]

摘 要 可验证加密签名是保证通过开放的Internet进行安全电子商务活动的有效方法之一。基于Waters数字签名方案,提出一个基于身份的可验证加密签名方案。方案具有可验证性和可恢复性,这是区别于普通签名方案的主要特性。关于方案的安全性,首先给出确切的安全模型,然后在标准模型下证明了方案的安全性可以归约为双线性群中CDH问题的难解性。从而证明方案是安全有效的。

关键词 可验证加密签名,安全模型,计算Diffie-Hellman问题,双线性映射

中图法分类号 TP309 **文献标识码** A

Secure ID-based Verifiably Encrypted Signature without Random Oracles

WANG Tian-qin[1] SU Li-wen[2]

(Department of Information Engineering, North China University of Water Resources and Electric Power, Zhengzhou 450011, China)[1]
(Information Centre, General Administration of Quality Supervision, Inspection and Quarantine of the Republic of China, Beijing 100088, China)[2]

Abstract Verifiably encrypted signature can be used in secure electronic transactions. We presented the first efficient identity-based verifiably encrypted signature scheme which has the properties of verifiability and recoverability. We gave a security model with precise definitions and showed that the scheme is secure under the computational Bilinear Diffie-Hellman assumption without random oracles.

Keywords Verifiably encrypted signature, Security model, Computational diffie-Hellman problem, Bilinear map

1 引言

基于身份的密码体制(IBC)的概念是由Shamir[1]于1984年首次提出的。在此密码体制中,用户的身份标识符(如:姓名、Email地址等)可以看作用户的公钥,而相应的私钥由可信中心来产生。IBC的主要优点是消除了对用户证书的需求和依赖,因此极大地简化了密钥管理问题。应用Weil配对技术,Boneh和Franklin[2]于2001年提出了第一个有效的基于身份的加密方案。自此之后,IBC引起了众多学者的广泛关注,并得到了快速发展,很多基于身份的加密和签名方案被相继提出[3-6]。

随着电子商务的广泛应用,如何保证互不信任的双方通过Internet公平地交换信息是其中的关键问题之一。可验证加密签名是用于构建公平交换协议,从而保证通过开放的Internet进行安全电子商务活动的有效方法之一。一个可验证加密签名方案涉及3个主体:签名者、验证者和仲裁者。其基本思想是,签名者将其对某一消息的原始签名用仲裁者的公钥进行加密,产生可验证的加密签名ves并发送给验证者。可验证性和可恢复性是其能够保证交换协议的公平性的必要特性。可验证性是指任意用户能够验证ves的确是签名者对消息的原始签名的加密结果,但验证者不能从中得到原始签名。可恢复性是指仲裁者能够从中提取出原始签名。

近来,学者们提出了一些可用于构建公平交换协议的基于身份的可验证加密签名[7,8],这些方案的安全性或者基于强困难问题假定,或者基于随机预言模型。虽然随机预言模型有其自身的优势,但它是一理想的假设。不依赖于理想化的随机预言模型,设计在标准模型下可证明安全的方案是本文研究工作的动机之一。近年来,基于标准模型下的安全性证明受到广泛关注。Waters[9]于2005年首次创造性地提出了标准模型下安全的基于身份的高效加密/签名方案,并且方案的安全性可归约为标准困难问题假定。此后,Waters方法受到关注,很多标准模型下安全的基于身份的密码方案被提出[10,11]。

本文应用Waters方法,在Boyen和Waters[10]基于身份的签名(IBS)方案(以下简称BW方案)的基础上,基于文献[7]中的设计思想和安全模型,提出一个标准模型下安全的基于身份的可验证加密签名(IDVES)方案,方案的安全性可归约为计算Diffie-Hellman(CDH)假定。

2 预备知识

设A是随机算法,以$A(x_1,x_2,\cdots;O_1,O_2,\cdots)$表示$A$的输入为$x_1,x_2,\cdots$,在运行过程中可以对预言机$O_1,O_2,\cdots$做

本文受国家自然科学基金(11071070)资助。

王天芹(1968—),女,博士,教授,主要研究方向为数论、密码学与信息安全,E-mail:wangtq@amss.ac.cn;苏莉文(1963—),女,博士,研究员,主要研究方向为信息管理。

询问。

2.1 基本定义

定义 1(双线性对) 设 G 和 G_1 是两个 p 阶循环乘法群，其中 p 为素数，g 是 G 的生成元。如果存在函数 $e:G\times G\rightarrow G_1$，且满足下面的性质，则称 e 为双线性对或双线性映射，G 为双线性群。

(1) 双线性性：对任意 $u,v\in G,a,b\in \mathbb{Z}_p$，有 $e(u^a,v^b)=e(u,v)^{ab}$。

(2) 非退化性：$e(g,g)\neq 1$。

(3) 可计算性：对任意 $u,v\in G$，存在有效算法计算 $e(u,v)$。

定义 2((t,ε)-CDH 假定) 阶为 p，生成元为 g 的循环群 G 中的 CDH 问题定义为：给定 $g^a,g^b\in G$，计算 $g^{ab}\in G$。如果不存在任何概率多项式时间算法在时间 t 内以至少 ε 的概率解决 G 中的 CDH 问题，则称 G 中的(t,ε)-CDH 假定成立。

2.2 IDVES 方案及安全模型

IDVES 方案由以下 7 个算法组成：

(1) *Setup*(系统参数设置)：输入安全参数 k，可信中心 PKG 由此产生公开的系统参数 PK 和主密钥 SK，仲裁者产生密钥对(tpk,tsk)，公开 tpk 作为一个系统参数，相应的 tsk 由仲裁者保密。

(2) *Ext*(用户密钥产生)：给定用户的身份标识 ID，PKG 根据系统参数和主密钥，产生身份标识为 ID 的用户的私钥 sk，并通过安全信道发送给用户。

(3) *Sig*(普通签名)：给定消息 m，签名者根据其私钥 sk 和系统参数 PK 产生签名 σ。

(4) *Vf*(验证)：验证者根据系统参数 PK 和签名者的身份标识 ID 对消息 m 的签名 σ 予以验证。

(5) *VESig*(可验证加密签名)：与普通签名类似，不同之处是该算法还依赖于仲裁者的公钥 tpk。给定消息 m，签名者根据其私钥 sk 和参数 $params=(PK,tpk)$ 产生签名 σ'。

(6) *VEVf*(验证)：根据参数 $params$ 和签名者的身份标识 ID，验证者对消息 m 的签名 σ' 予以验证。

(7) *Res*(仲裁)：仅当签名者和验证者发生争端时由仲裁者运行该算法。仲裁者首先检验可验证加密签名 σ' 的有效性，然后利用自己的私钥 tsk 由 σ' 得到签名者的有效普通签名 σ。

一个正确的 IDVES 方案应该满足：

$$Vf\ (m,Sig\ (m,sk),ID)=1$$

$$VEVf\ (m,VESig\ (m,sk,tpk),ID,tpk)=1$$

$$Vf\ (m,Res\ (m,VESig\ (m,sk,tpk),tsk),ID)=1$$

普通签名方案的安全性要求是在自适应选择消息攻击下具有存在不可伪造性，而 IDVES 方案的安全性是在此基础上的一种扩展，由以下 3 个方面来保证：抵抗签名者的安全性、抵抗验证者的安全性、抵抗仲裁者的安全性。在下面的描述中，设 k 为安全参数，以 O_{Sig} 表示模拟普通签名算法的预言机，以 O_{Ext} 表示模拟用户密钥产生算法的预言机，以 O_{Res} 表示模拟仲裁算法的预言机，以 O_{VESig} 表示模拟可验证加密签名算法的预言机。

抵抗签名者的安全性。即签名者不应该产生这样一个签名 σ'，它是有效的可验证加密签名，但仲裁者却不能从中得到普通签名。确切地说，要求任何概率多项式时间(PPT)敌手 A 在下面的试验中成功的概率可忽略：

$$(tpk,tsk)\leftarrow Setup(1^k)$$

$$sk_A^*\leftarrow Ext^*(ID_A)$$

$$(m,\sigma')\leftarrow A(sk_A^*,tpk:O_{Res},O_{Ext})$$

$$\sigma\leftarrow Res(m,\sigma',tsk)$$

Sucess of $A=[VEVf(m,\sigma',ID_A,tpk)=1\wedge Vf(m,\sigma,ID_A)=0]$

式中，Ext^* 表示不诚实的签名者运行的 Ext 算法，之后得到的信息为 sk_A^*。

抵抗验证者的安全性。即验证者不能将任意签名者的可验证加密签名转化为相应的普通签名(除非询问仲裁者)。确切地说，要求任何 PPT 敌手 B 在下面的试验中成功的概率可忽略：

$$(tpk,tsk)\leftarrow Setup(1^k)$$

$$sk_A\leftarrow Ext(ID_A)$$

$$(m,\sigma)\leftarrow B(ID_A,tpk,(m,\sigma'):O_{VESig},O_{Res},O_{Ext})$$

Sucess of $B=[Vf(m,\sigma,ID_A)=1\wedge ID_A\notin Query(B,O_{Ext})\wedge(m,\sigma')\notin Query(B,O_{Res})]$

式中，$Query(B,O_{Ext})$ 表示 B 对预言机 O_{Ext} 所做的所有有效询问的集合，$Query(B,O_{Res})$ 表示 B 对预言机 O_{Res} 所做的所有有效询问的集合。

抵抗仲裁者的安全性。即仲裁者不能直接产生签名者的普通签名。确切地说，要求任何 PPT 敌手 T 在下面的试验中成功的概率可忽略：

$$(tpk,tsk^*)\leftarrow Setup^*(1^k)$$

$$sk_A\leftarrow Ext(ID_A)$$

$$(m,\sigma)\leftarrow T(tsk^*,tpk:O_{VESig},O_{Ext})$$

Sucess of $T=[Vf(m,\sigma,ID_A)=1\wedge ID_A\notin Query(T,O_{Ext})\wedge(m,ID_A)\notin Query(T,O_{VESig})]$

式中，$Setup^*$ 表示不诚实的仲裁者运行的 Setup 算法，之后得到的信息为 tsk^*，$Query(T,O_{Ext})$ 表示 T 对预言机 O_{Ext} 所做的所有有效询问的集合，$Query(T,O_{VESig})$ 表示 T 对预言机 O_{VESig} 所做的所有有效询问的集合。

定义 3 一个 IDVES 方案是安全的，如果它能够抵抗签名者攻击、验证者攻击和仲裁者攻击。

2.3 BW 方案

假定用户身份标识是长度为 l 的比特串，待签名的消息是长度为 n 的比特串。g 是阶为素数 p 的双线性群 G 的生成元，双线性映射为 $e:G\times G\rightarrow G_1$。BW 方案是一个 4 元组 $BW=(Setup,Ext,Sig,Vf)$。

Setup：随机选择 $a\in \mathbb{Z}_p^*$，$y',z'\in \mathbb{Z}_p$，l 维向量 $y=(y_1,\cdots,y_l)\in \mathbb{Z}_p^l$，$n$ 维向量 $z=(z_1,\cdots,z_n)\in \mathbb{Z}_p^n$。系统参数和主密钥分别为：

$$PP=(G,G_1,p,e,g,u'=g^{y'},u=(g^{y_1},\cdots,g^{y_l}),v'=g^{z'},$$
$$v=(g^{z_1},\cdots,g^{z_n}),A=e(g,g)^a)$$

$$SK=a$$

$Ext(PP,SK,ID)$：对于 $ID=(k_1\cdots k_l)\in\{0,1\}^l$ 的用户，随机选取 $r\in Z_p^*$，计算并返回

$$K_{ID}=(g^{\alpha}(u'\prod_{i=1}^{l}u_i^{k_i})^r,g^{-r})$$

$Sig(PP,K_{ID},M)$：设 $M=(m_1\cdots m_n)\in\{0,1\}^n$，$K_{ID}=(K_1,K_2)$。随机选取 $s\in Z_p^*$，计算并返回

$$\sigma=(K_1(v'\prod_{j=1}^{n}v_j^{m_j})^s,K_2,g^{-s})$$

$Vf(PP,ID,M,\sigma)$：设 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$。计算并验证是否有：

$$e(\sigma_1,g)\cdot e(\sigma_2,u'\prod_{i=1}^{l}u_i^{k_i})\cdot e(\sigma_3,v'\prod_{j=1}^{n}v_j^{m_j})=A$$

如果等式成立，则返回"valid"；否则返回"invalid"。

在 G 中 CDH 问题难解的假设下，BW 方案在自适应选择消息和自适应选择身份攻击下具有存在不可伪造性（见文献[10]定理 C.1）。

3 基于身份的可验证加密签名

不失一般性，假定待签名的消息是长度为 n 的比特串，用户身份标识是长度为 l 的比特串。对于任意长度的身份和消息，利用抗冲突 Hash 函数进行处理，可以分别将它们映射到方案所要求的长度。

3.1 方案描述

方案 Σ 由以下算法构成：

(1) Setup　设 G 和 G_1 是两个 p 阶循环乘法群，其中 p 是与安全参数相关的随机素数，g 是 G 的生成元，双线性映射为 $e:G\times G\to G_1$。

PKG 随机选择 $a\in Z_p^*$，计算 $A=e(g,g)^a$。随机选择 $u',v'\in G$，l 维向量 $u=(u_i)$，n 维向量 $v=(v_j)$，其中 $u_i,v_j\in G$。系统公钥 $PK=(G,G_1,p,e,g,u',u,v',v,A)$，主密钥 $SK=a$。

仲裁者随机选择 $b\in Z_p^*$，计算 $g'=g^b$。仲裁者公钥 $tpk=g'$，仲裁者私钥 $tsk=b$。

系统公开参数 $PP=(PK,g')$。

(2) Ext　给定用户的身份标识 $ID_X=(k_1\cdots k_l)$，PKG 随机选取 $\tilde{r}\in Z_p^*$，计算

$$d_X=(d_1,d_2)$$

式中，$d_1=g^{\alpha}(u'\prod_{i=1}^{l}u_i^{k_i})^{\tilde{r}}$，$d_2=g^{-\tilde{r}}$。

(3) Sig 和 $VESig$　给定签名者私钥 d_X 和消息 $M=(m_1\cdots m_n)$，随机选取 $r,s,r',s',t'\in Z_p^*$，计算并输出普通签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$，可验证加密签名 $\sigma'=(\sigma_1',\sigma_2',\sigma_3',\sigma_4')$，其中：

$$\sigma_1=d_1(u'\prod_{i=1}^{l}u_i^{k_i})^r(v'\prod_{j=1}^{n}v_j^{m_j})^s$$

$$\sigma_2=d_2g^{-r}$$

$$\sigma_3=g^{-s}。\ \sigma_1'=d_1(u'\prod_{i=1}^{l}u_i^{k_i})^{r'}(v'\prod_{j=1}^{n}v_j^{m_j})^{s'}(g')^{t'}$$

$$\sigma_2'=d_2g^{-r'},\sigma_3'=g^{-s'},\sigma_4'=g^{-t'}$$

(4) Vf 和 $VEVf$　定身份标识为 ID_X 的签名者对消息 M 的普通签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$，验证者接受该签名当且仅当

$$e(\sigma_1,g)\cdot e(\sigma_2,u'\prod_{i=1}^{l}u_i^{k_i})\cdot e(\sigma_3,v'\prod_{j=1}^{n}v_j^{m_j})=A \qquad (1)$$

给定身份标识为 ID_X 的签名者对消息 M 的可验证加密签名 $\sigma'=(\sigma_1',\sigma_2',\sigma_3',\sigma_4')$，验证者接受该签名当且仅当

$$e(\sigma_1',g)\cdot e(\sigma_2',u'\prod_{i=1}^{l}u_i^{k_i})\cdot e(\sigma_3',v'\prod_{j=1}^{n}v_j^{m_j})\cdot e(\sigma_4',g')=A \qquad (2)$$

(5) Res　给定身份标识为 ID_X 的签名者对消息 M 的可验证加密签名 $\sigma'=(\sigma_1',\sigma_2',\sigma_3',\sigma_4')$，仲裁者首先验证式(2)是否成立。如果验证通过，则随机选取 $r,s\in Z_p^*$，计算

$$\sigma_1=\sigma_1'(\sigma_4')^b(u'\prod_{i=1}^{l}u_i^{k_i})^r(v'\prod_{j=1}^{n}v_j^{m_j})^s$$

$$\sigma_2=\sigma_2'g^{-r},\sigma_3=\sigma_3'g^{-s}$$

输出 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$ 作为 ID_X 对 M 的普通签名。

注：由 $(Setup,Ext,Sig,Vf)$ 组成的方案是 BW 方案。

3.2 安全性分析

根据定义 3 给出的 IDVES 方案的安全性定义，有如下结论。

定理 1　方案 Σ 在 (t,ε)-CDH 假定下是安全的。

证明：首先，由文献[10]中的已知结论知，BW 方案在假设条件下是安全的。下面证明方案 Σ 是安全的。

(1) 抵抗签名者攻击

一个恶意的签名者，其目的是在预言机 O_{Res} 和 O_{Ext} 的帮助下产生有效的可验证加密签名 (M,σ')，而仲裁者却不能恢复相应的有效普通签名 (M,σ)。事实上，任意有效的可验证加密签名都满足式(2)，根据仲裁算法，由 (M,σ') 得到的 (M,σ) 满足式(1)，是有效的普通签名。因此，方案 Σ 能够无条件抵抗签名者攻击。

(2) 抵抗验证者攻击

一个恶意的验证者，其目的是在预言机 O_{VESig}，O_{Res} 和 O_{Ext} 的帮助下产生有效的普通签名 (M,σ)，而相应的可验证加密签名 (M,σ') 不曾向 O_{Res} 询问过。下面说明，如果这样一个敌手 B 能够攻击成功，则可以构造一个算法 S 来解决 CDH 困难问题。

对于给定的元素 $g,g^{\alpha},g^{\beta}\in G$，$S$ 的目标是计算 $g^{\alpha\beta}$。

S 在与 B 交互之前，先进行参数设置。令

$$g_1=g^{\alpha},g_2=g^{\beta},A=e(g_1,g_2),$$

$$\lambda_1=2q_E,\lambda_2=2q_V$$

式中，$q_E\ll p$，$q_V\ll p$，分别表示 B 所做的密钥询问和可验证加密签名询问的次数。首先，随机选取

$$ID^*=(k_1^*\cdots k_l^*)\in\{0,1\}^l$$

$$\gamma_1\in\{0,\cdots,l\},y',y_1,\cdots,y_l\in Z_{\lambda_1},$$

满足

$$-\gamma_1\lambda_1+y'+\sum_{i=1}^{l}y_ik_i^*\equiv 0(\mathrm{mod}\ p)。$$

然后，随机取

$$\gamma_2\in\{0,\cdots,n\},x',x_1,\cdots,x_n\in Z_{\lambda_2}$$

$$z',z_1,\cdots,z_n\in Z_p,w',w_1,\cdots,w_l\in Z_p$$

令

$$u'=g_2^{y'-\gamma_1\lambda_1}g^{w'},u_i=g_2^{y_i}g^{w_i}$$

$$v'=g_2^{x'-\gamma_2\lambda_2}g^{z'},v_j=g_2^{x_j}g^{z_j}$$

式中，$i=1,\cdots,l,j=1,\cdots,n$。随机取 $g'\in G$。系统参数 $PP=(g,u',u_i,v',v_j,A,g')$，$g'$ 为仲裁者公钥，主密钥 $SK=\alpha\beta$（未知）。

对于

$ID=(k_1\cdots k_l)\in\{0,1\}^l$，$M=(m_1\cdots m_n)\in\{0,1\}^n$，定义

$H(ID)=-\gamma_1\lambda_1+y'+\sum_{i=1}^{l}y_ik_i$

$L(ID)=w'+\sum_{i=1}^{l}w_ik_i$

$F(M)=-\gamma_2\lambda_2+x'+\sum_{j=1}^{n}x_jm_j$

$J(M)=z'+\sum_{j=1}^{n}z_jm_j$

S 与 B 进行交互，回答 B 的各类询问。

1. 密钥询问(O_{Ext})

考虑对身份 $ID=(k_1\cdots k_l)\in\{0,1\}^l$ 的密钥询问。若 $H(ID)\equiv0(\mathrm{mod}\ p)$，$S$ 不能回答询问，失败退出。若 $H(ID)\neq0(\mathrm{mod}\ p)$，$S$ 随机选取 $r\in\mathbf{Z}_p^*$，计算

$$d_{ID}=(d_1,d_2)=(g_1^{-L/H}(u'\prod_{i=1}^{l}u_i^{k_i})^r,g_1^{1/H}g^{-r})$$

并将 d_{ID} 发送给 B。

注意到，对于随机数 $\tilde{r}=r-\alpha/H$，有

$$\begin{aligned}d_1&=g_1^{-L/H}(g_2^Hg^L)^r\\&=g_1^{-L/H}(g_2^Hg^L)^{\alpha/H}(g_2^Hg^L)^{\tilde{r}}\\&=g^{\alpha\beta}(u'\prod_{i=1}^{l}u_i^{k_i})^{\tilde{r}}\\d_2&=g_1^{1/H}g^{-r}\\&=g^{-(r-\alpha/H)}=g^{-\tilde{r}}\end{aligned}$$

因此，d_{ID} 是关于身份 ID 的有效私钥。

2. 可验证加密签名询问(O_{VESig})

考虑关于身份 $ID=(k_1\cdots k_l)\in\{0,1\}^l$，消息 $M=(m_1\cdots m_n)\in\{0,1\}^n$ 的询问。若 $H(ID)\neq0(\mathrm{mod}\ p)$，$S$ 随机选取 $r,s,t\in\mathbf{Z}_p^*$，计算

$$\sigma_1=g_1^{-L/H}(u'\prod_{i=1}^{l}u_i^{k_i})^r(v'\prod_{j=1}^{n}v_j^{m_j})^s(g')^t$$

$$\sigma_2=g_1^{1/H}g^{-r},\sigma_3=g^{-s},\sigma_4=g^{-t}$$

返回 $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4)$。若 $H(ID)\equiv0(\mathrm{mod}\ p)$，如果 $F(M)\equiv0(\mathrm{mod}\ p)$，$S$ 不能回答询问，失败退出。如果 $F(M)\neq0(\mathrm{mod}\ p)$，$S$ 随机选取 $r,s,t\in\mathbf{Z}_p^*$，计算

$$\sigma_1=g_1^{-J/F}g^{Lr}(v'\prod_{j=1}^{n}v_j^{m_j})^s(g')^t$$

$$\sigma_2=g^{-r},\sigma_3=g_1^{1/F}g^{-s},\sigma_4=g^{-t}$$

返回 $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4)$。

注意到，若 $H(ID)\neq0(\mathrm{mod}\ p)$，对于随机数 $\tilde{r}=r-\alpha/H$，s,t，有

$$\begin{aligned}\sigma_2&=g_1^{1/H}g^{-r}=g^{-(r-\alpha/H)}=g^{-\tilde{r}}\\\sigma_3&=g^{-s},\sigma_4=g^{-t}\\\sigma_1&=g_1^{-L/H}(g_2^Hg^L)^r(v'\prod_{j=1}^{n}v_j^{m_j})^s(g')^t\\&=g_1^{-L/H}(g_2^Hg^L)^{\alpha/H}(g_2^Hg^L)^{\tilde{r}}(v'\prod_{j=1}^{n}v_j^{m_j})^s(g')^t\\&=g^{\alpha\beta}(u'\prod_{i=1}^{l}u_i^{k_i})^{\tilde{r}}(v'\prod_{j=1}^{n}v_j^{m_j})^s(g')^t\end{aligned}$$

则，$\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4)$ 是关于身份 ID、消息 M 的有效可验证加密签名。

若 $H(ID)\equiv0(\mathrm{mod}\ p)$，$F(M)\neq0(\mathrm{mod}\ p)$，对于随机数 $r,\tilde{s}=s-\alpha/F,t$，有

$$\begin{aligned}\sigma_1&=g_1^{-J/F}g^{Lr}(v'\prod_{j=1}^{n}v_j^{m_j})^s(g')^t\\&=g_1^{-J/F}g^{Lr}(g_2^Fg^J)^s(g')^t\\&=g_1^{-J/F}g^{Lr}(g_2^Fg^J)^{\tilde{s}}(g_2^Fg^J)^{\alpha/F}(g')^t\\&=g_2^{\alpha}g^{Lr}(g_2^Fg^J)^{\tilde{s}}(g')^t\\&=g^{\alpha\beta}(u'\prod_{i=1}^{l}u_i^{k_i})^r(v'\prod_{j=1}^{n}v_j^{m_j})^{\tilde{s}}(g')^t\end{aligned}$$

则，$\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4)$ 是关于身份 ID、消息 M 的有效可验证加密签名。

3. 仲裁询问(O_{Res})

考虑关于身份 $ID=(k_1\cdots k_l)\in\{0,1\}^l$，消息 $M=(m_1\cdots m_n)\in\{0,1\}^n$ 的可验证加密签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4)$ 的仲裁询问。在 σ 有效的情况下，若 $H(ID)\neq0(\mathrm{mod}\ p)$，$S$ 随机选取 $r,s\in\mathbf{Z}_p^*$，计算

$$\sigma_1=g_1^{-L/H}(u'\prod_{i=1}^{l}u_i^{k_i})^r(v'\prod_{j=1}^{n}v_j^{m_j})^s$$

$$\sigma_2=g_1^{1/H}g^{-r},\sigma_3=g^{-s}$$

返回$(\sigma_1,\sigma_2,\sigma_3)$。若 $H(ID)\equiv0(\mathrm{mod}\ p)$，如果 $F(M)\equiv0(\mathrm{mod}\ p)$，$S$ 不能回答询问，失败退出。如果 $F(M)\neq0(\mathrm{mod}\ p)$，$S$ 随机选取 $r,s\in\mathbf{Z}_p^*$，计算

$$\sigma_1=g_1^{-J/F}g^{Lr}(v'\prod_{j=1}^{n}v_j^{m_j})^s$$

$$\sigma_2=g^{-r},\sigma_3=g_1^{1/F}g^{-s}$$

返回$(\sigma_1,\sigma_2,\sigma_3)$。

注意到，B 关于(ID,M)已经做过可验证加密签名询问。

最后，B 输出 ID^* 对于 $M^*=(m_1^*\cdots m_n^*)$ 的有效伪造签名 $\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*)$，而关于$(ID^*,M^*)$未曾做过仲裁询问。若 $F(M^*)\neq0(\mathrm{mod}\ p)$，$S$ 失败退出。否则，有 $v'\prod_{j=1}^{n}v_j^{m_j^*}=g^{J(M^*)}$。从而有

$$\begin{aligned}e(g^{\alpha\beta},g)&=e(g_1,g_2)=A\\&=e(\sigma_1^*,g)\cdot e(\sigma_2^*,u'\prod_{i=1}^{l}u_i^{k_i*})\cdot e(\sigma_3^*,v'\prod_{j=1}^{n}v_j^{m_j*})\\&=e(\sigma_1^*,g)\cdot e(\sigma_2^*,g^{L(ID^*)})\cdot e(\sigma_3^*,g^{J(M^*)})\\&=e((\sigma_1^*)(\sigma_2^*)^{L(ID^*)}(\sigma_3^*)^{J(M^*)},g)\end{aligned}$$

有 $g^{\alpha\beta}=(\sigma_1^*)(\sigma_2^*)^{L(ID^*)}(\sigma_3^*)^{J(M^*)}$。算法 S 成功解决 CDH 困难问题。

设敌手 B 攻击成功的概率为 ε'。下面分析算法 S 成功的概率。

首先，S 关于目标身份 ID^* 的猜测必须是正确的，其概率为 $1/2^l$。其次，在与 B 交互过程中，S 均不能失败退出，这需要满足 3 个条件：

(1) 密钥询问成功，即 $\forall\,1\leqslant i\leqslant q_E$，$H(ID_i)\neq0(\mathrm{mod}\ p)$。

(2) 可验证加密签名询问成功，即

$\forall\,1\leqslant j\leqslant q_V$，$H(ID_j)\neq0(\mathrm{mod}\ p)\vee F(M_j)\neq0(\mathrm{mod}\ p)$。

(3) 伪造签名成功且 S 正常返回，即 $F(M^*)\equiv0(\mathrm{mod}\ p)$。

在仲裁询问中，关于对应的输入已做过可验证加密签名询问且没有失败退出，因此，仲裁询问过程不会失败退出。

注意到，

$H(ID_i)\neq0(\mathrm{mod}\ \lambda_1)\Rightarrow H(ID_i)\neq0(\mathrm{mod}\ p)$

$F(M_j)\neq0(\mathrm{mod}\ \lambda_2)\Rightarrow F(M_j)\neq0(\mathrm{mod}\ p)$

因此，有

$$\Pr[Sucess]\geqslant\frac{1}{2^l}\cdot\Pr[\wedge_{i=1}^{q_E}(H(ID_i)\neq 0(\bmod\lambda_1))]\cdot\Pr[\wedge_{j=1}^{q_V}(H(ID_j)\neq 0(\bmod\lambda_1)\vee F(M_j)\neq 0(\bmod\lambda_2))]\cdot Pr[(F(M^*)\equiv 0(\bmod p))]\cdot\varepsilon'$$

$$=\frac{1}{2^l}\cdot(1-\Pr[\vee_{i=1}^{q_E}(H(ID_i)\equiv 0(\bmod\lambda_1))])\cdot(1-\Pr[\vee_{j=1}^{q_V}(H(ID_j)\equiv 0(\bmod\lambda_1)\wedge F(M_j)\equiv 0(\bmod\lambda_2))])\cdot\Pr[(F(M^*)\equiv 0(\bmod p))]\cdot\varepsilon'$$

$$\geqslant\frac{1}{2^l}\cdot(1-\frac{q_E}{\lambda_1})\cdot(1-\frac{q_V}{\lambda_2})\cdot\frac{1}{n\lambda_2}\cdot\varepsilon'$$

$$=\frac{\varepsilon'}{2^{l+3}nq_V}$$

(3) 抵抗仲裁者攻击

一个不诚实的仲裁者 T,其目的是借助预言机 O_{VESig},O_{Ext} 的帮助,在没有相应的可验证加密签名的情况下,直接产生有效的普通签名(M,σ)。由于 T 拥有仲裁私钥 tsk,它可以由任意可验证加密签名得到普通签名。对于 T 来说,预言机 O_{VESig} 可以看作普通签名预言机。因此,T 对方案 Σ 的伪造签名就是对 BW 方案的有效伪造签名。

综上所述,在(t,ε)-CDH 假定下,方案 Σ 是安全的。

结束语 本文应用 Waters 方法,提出了一个基于身份的可验证加密签名方案,并在标准模型下,证明了方案的安全性可以归约为双线性群中 CDH 问题的难解性。本文方案满足可验证性和可恢复性,这是其区别于普通签名方案的主要特性,在电子商务中具有重要的应用价值。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proceedings of the Advances in Cryptology-Crypto'84. LNCS 196. Berlin, Heidelberg: Springer-Verlag, 1984: 47-53

[2] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]// Proceedings of the Advances in Cryptology-Crypto' 2001. LNCS 2139. Berlin, Heidelberg: Springer-Verlag, 2001: 213-229

[3] Hess F. Efficient identity based signature schemes based on pairings[C]// Proceedings of the SAC 2002. LNCS 2595, Berlin, Heidelberg: Springer-Verlag, 2003: 310-324

[4] Boneh D, Boyen X. Secure identity based encryption without random oracles[C]// Proceedings of the Advances in Cryptology—Crypto' 2004. LNCS 3152. Berlin, Heidelberg: Springer-Verlag, 2004: 443-459

[5] Paterson K G, Schuldt J C N. Efficient identity-based signatures secure in the standard model[C]// Proceedings of the ACISP 2006. LNCS 4058, Berlin. Heidelberg: Springer-Verlag, 2006: 207-222

[6] 李进,张方国,王燕鸣. 两个高效的基于分级身份的签名方案[J]. 电子学报,2007,35(1):150-152

[7] Zhang Z F, Feng D G, Xu J, et al. Efficient ID-based optimistic fair exchange with provable security[C]// Proceedings of the 7th International Conference on Information and Communication Security. LNCS 3783. Berlin, Heidelberg: Springer-Verlag, 2005: 14-26

[8] Xu J, Zhang Z F, Feng D G. Constructing optimistic ID-based fair exchange protocols via proxy signature[J]. Journal of Software, 2007, 18(3): 746-754

[9] Waters B. Efficient identity-based encryption without random oracles[C]// Cramer R, ed. EUROCRYPT' 2005. LNCS 3494. Berlin, Heidelberg: Springer-Verlag, 2005: 114-127

[10] Boyen X, Waters B. Compact group signatures without random oracles[C]// Berlin, LNCS 4004. Heidelberg: Springer-Verlag, 2006: 427-444

[11] 李继国,姜进平. 标准模型下可证明安全的基于身份的高效签名方案[J]. 计算机学报,2009,32(11):2130-2136

(上接第 100 页)

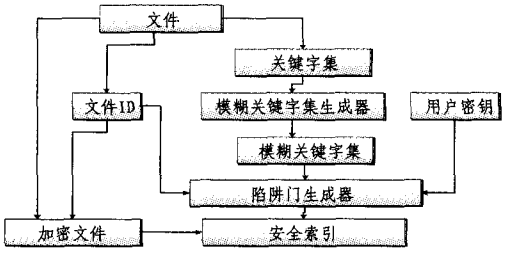

图 2 用户段的文件索引生成

2. 当被授权的用户检索他所感兴趣的文件时,首先根据用户输入的关键字生成模糊关键字集合,然后使用密钥 k_s 加密生成关键字陷阱门,将这个陷阱门上传到云服务器进行检索。

3. 云服务器接受到授权用户上传的陷阱门后,通过和数据拥有者上传的索引表进行对比(此时对比的是数据拥有者上传的数据模糊关键字集索引表和由检索用户输入关键字生成的模糊关键字集合陷阱门),返回所有相关联的加密文件 id,然后发送加密文件给授权的用户。用户使用密钥 k_s 进行解密后得到期望的文件。对于用户的检索关键字信息,检索到的文件信息都是经过加密的,对服务器是不可见的。

结束语 本文提出了一种在加密的云计算环境下进行高效模糊检索的方案。将生成的模糊关键字集与加密文档 ID 一起生成安全的索引。在保证数据私密性的情况下,可以进行高效的数据模糊检索。

在接下来的工作里面,会从服务器检索的方面来考虑提升系统的效率和安全性。安全性方面我们考虑将存储以及查询分离;效率方面我们将设计一种特殊的新的索引来辅助检索。

参 考 文 献

[1] Li Jin, Wang Qian, Wang Cong, et al. Fuzzy Keyword Search over Encrypted Data in Cloud Computing[C]// Proceedings of INFOCOM'2010. 2010: 441-445

[2] An Introduction to Information Retrieval[M]. Cambridge University Press, 2008

[3] Goh E-J. Secure Indexes[Z]. Stanford University, March 2004

[4] Kamara S, Kistin S, Lauter K. Cryptographic Cloud Storage[Z]. January 2010

[5] Shay A, Adam K, Calvin N, et al. Encrypted Keyword Search in a Distributed Storage System