·安全技术· 文章编号：1000-3428(2017)04-0126-07 文献标志码：A 中图分类号：TP309

白盒可追踪的属性签名方案

刘雨阳，赵一鸣

（复旦大学 软件学院，上海 201203）

摘 要： 基于属性的签名协议具有匿名性，且私钥不与用户身份绑定，恶意用户可能利用此性质出售私钥而逃过追究。为此，提出可追踪性属性签名方案，使得系统能够通过泄露的私钥破解匿名性并追踪用户身份。给出具有白盒可追踪性的基于属性数字签名协议的密码学原型。通过将 Boneh-Boyen 签名算法有机嵌入到用户私钥中，实现白盒可追踪性。分析结果表明，该方案具有可证明安全的不可伪造性和完美隐私性，其时间复杂度与目前最优的可追踪属性签名方案仅相差一个常数。

关键词： 数字签名；属性；可追踪性；隐私；不可伪造性；双线性对

中文引用格式： 刘雨阳，赵一鸣. 白盒可追踪的属性签名方案[J]. 计算机工程，2017，43(4)：126-132，140.

英文引用格式： Liu Yuyang，Zhao Yiming. White-box Traceable Attribute Signature Scheme[J]. Computer Engineering，2017，43(4)：126-132，140.

White-box Traceable Attribute Signature Scheme

LIU Yuyang，ZHAO Yiming

（Software School，Fudan University，Shanghai 201203，China）

【Abstract】 Attribute-based Signature（ABS） protocol has the property of anonymity，and its private keys are not band to identities. Malicious users might make use of this to leak their private keys for financial benefits. Therefore，this paper proposes a traceable signature scheme，which allows the system to break anonymity and trace the identity by the leaked private key. Acryptography model of attribute-based digital signature protocol along with white-box traceability is presented. It achieves white-box traceability by injecting Boneh-Boyen signature algorithm into private keys. Analysis results show that the scheme has provable security of unforgeability and perfect privacy，and its time complexity differs only one comstant from the current best traceable attribute signature scheme.

【Key words】 digital signature；attribute；traceability；privacy；unforgeability；bilinear group

DOI： 10.3969/j.issn.1000-3428.2017.04.022

0 概述

基于属性加密（Attribute-based Encryption，ABE）是对基于身份加密[1-2]的扩展，在分布式环境下有巨大应用潜力。近年来，大量文献如文献[3-5]等对基于属性的加密系统做了研究。

随着 ABE 的发展，基于属性的签名方案（Attribute-based Signature，ABS）也得到了广泛研究。文献[6]最早提出了 ABS 的形式化定义，并给出了具体实例。在 ABS 中，每个用户拥有一系列属性，并从属性授权中心取得他的私钥。其后用户可以使用私钥和签名谓词对消息进行签名，只要用户的属性集合满足签名谓词，签名即是有效的。目前已提出的 ABS 方案有文献[7-9]等。

在传统的公钥密码学系统中，私钥与用户是一一对应的关系。私钥仅关系到持有者本人的安全和隐私，用户有很强的意愿保护私钥不泄露。但在 ABE 和 ABS 方案中，用户私钥与属性集相关联，由于不同用户可以拥有相同的属性，且实际场景中，系统中用户的数量远多于属性的数量，因此对于给定的私钥，判断其拥有者的身份往往是困难的。这就为用户秘密出售私钥提供了动力。即便系统管理者通过调查掌握了被出售的私钥，也无法断定私钥拥有者的身份，恶意用户为出售私钥行为所承担的风险非常小。

为应对这一问题，文献[10]提出了基于属性密码学方案中的可追踪性定义，文献[11]将可追踪性分为白盒可追踪性和黑盒可追踪性。其中，白盒可追踪性

作者简介： 刘雨阳（1990—），男，硕士研究生，主研方向为属性密码学；赵一鸣，副教授。

收稿日期： 2016-05-03 **修回日期：** 2016-06-13 **E-mail：** liuyuyang13@fudan.edu.cn

是指恶意用户出售私钥时,系统可根据私钥计算出用户身份。黑盒可追踪性是指恶意用户出售黑盒解密装置时,系统可根据黑盒装置计算出用户身份。文献[12-14]研究了白盒可追踪的 ABE 方案。

文献[15]定义并提出了 ABS 方案的可追踪性。但该方案中大量使用了非交互式零知识证明,导致协议效率较低。随后,文献[16]对该方案进行了改进,但效率仍不够理想。文献[17]发表了一个可追踪的基于属性签名协议,未使用非交互式零知识证明,因而大大提高了效率。但该方案借助可联系性实现追踪算法,在隐私性方面有所欠缺。具体来说,对于文献[17]中给定的任意 2 个签名,任何人均可以判断它们是否由同一个私钥签发。

按照类似文献[11]的定义方法,以上各 ABS 方案均属于黑盒可追踪性。目前对白盒可追踪的基于属性签名方案尚无相关研究。本文参照文献[11]的定义,给出了白盒可追踪的基于属性签名方案密码学原型,并提出了一个方案实例。本文方案通过将 Boneh-Boyen 签名算法[18]有机融入到私钥抽取算法中,实现白盒可追踪性,使 PKG 可以在必要时通过泄露的私钥计算出恶意用户身份。

1　预备知识

本节介绍本文中用到的背景知识,包括相关代数结构和困难性假设、形式化定义及安全模型。

1.1　双线性对及相关困难性假设

设 p 为大质数,G 和 G_T 是 2 个阶为 p 的乘法循环群,并设 g 是群 G 的一个生成元。设 e 是映射关系 $e:G\times G\to G_T$,称 e 是一个双线性对,如果 e 满足:

1)双线性(Bilinearity):对任意 $x,y\in G$ 及任意 $a,b\in Z_p$,都有:$e(x^a,y^b)=e(x,y)^{ab}$,这里 Z_p 是模 p 的剩余类环。

2)非退化性(Non-degeneracy):$e(g,g)\neq 1$,这里 1 是 G_T 中的单位元。

则称群 G 是双线性群(Bilinear Group)。

定义 1　q-强 Diffie-Hellman(q-Strong Diffie-Hellman,SDH)问题:设 p 是大质数,G_1,G_2 是阶为 p 的乘法循环群,分别是 G_1,G_2 的生成元,给定 $(q+2)$-元组 $(g_1,g_2,g_2^x,g_2^{x^2},\cdots,g_2^{x^q})$,其中,$x,q\in Z_p$,输出元组 $(c,g_1^{1/(x+c)})$,其中,$c\in Z_p^*$。

本文对可追踪性的证明基于 q-SDH 问题困难性假设。

1.2　访问结构

定义 2　访问结构(Access Structure):设 $\{P_1,P_2,\cdots,P_n\}$ 是关于各主体的集合,称集合 $A\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}$ 是单调的(monotone),如果 A 满足:对所有的 B,C,若 $B\in A$ 且 $B\subseteq C$ 则必有 $C\subseteq A$。称 $\{P_1,P_2,\cdots,P_n\}$ 上的非空单调子集 A 为(单调)访问结构,并称 A 中的集合为授权集,不在 A 中的集合为非授权集。

在基于属性的密码体系中,上述定义中的主体 $P_1,P_2,\cdots,P_n$ 可以理解为属性,因此访问结构是以属性集合为元素的集合。本文中使用的访问结构均指单调访问结构。

习惯上基于属性签名协议中的访问结构称为签名谓词(Signing Predict)。设有签名谓词 Γ 和其对应的访问结构 A,对属性集合 S,记 $\Gamma(S)=1$,若 $S\in A$,否则记 $\Gamma(S)\neq 1$。

本文使用线性秘密共享方案作为访问结构。

定义 3　线性秘密共享方案(Linear Secret Sharing Scheme,LSSS)称主体集合 $\mathcal{P}$ 上的秘密共享方案 Π 是线性的,如果:

1)各个主体持有的秘密分量构成 Z_p 上的一个向量;

2)存在一个 l 行 k 列的 Π 秘密生成矩阵 $\boldsymbol{M}$,具有如下性质:定义 $\rho(i)$ 为矩阵第 i 行对应的主体 $(i=1,2,\cdots,l)$,考虑列向量 $\boldsymbol{v}=(s,v_2,v_3,\cdots,v_k)$,其中 $s\in Z_p$ 是要分享的秘密,$v_2,v_3,\cdots,v_k\in Z_p$ 是随机数,那么 $\boldsymbol{Mv}$ 是 s 根据 Π 的 l 个秘密分量构成的向量,且 $\boldsymbol{Mv}$ 属于主体 $\rho(i)$。

LSSS 具有线性重构性质:设 Π 是访问结构 A 对应的 LSSS,且 $S\in A$ 为任一授权集合,$I\subseteq\{1,2,\cdots,\ell\}$ 定义为 $I=\{i:\rho(i)\in S\}$,那么给定任一秘密 s 关于 Π 的合法秘密份额 $\{\lambda_i\}_{i\in I}$,必然存在常量 $\{w_i\in Z_p\}_{i\in I}$ 满足 $\sum_{i\in I}w_i\lambda_i=s$,并且这些常量 $\{w_i\}_{i\in I}$ 可以在多项式时间内计算出来。

1.3　形式化定义

本文参考文献[17]给出白盒可追踪数字签名协议的形式化定义。协议由以下 5 个算法构成:

1)初始化算法 Setup(λ):由 PKG 执行,输出安全参数 λ,定义系统属性全集 U,计算系统公钥 PK 和主私钥 mk。

2)私钥抽取算法 $Extract(id,S,mk)$:由 PKG 执行,输入用户身份 id,用户属性集合 S,系统主私钥 mk,验证属性集合的有效性,若验证通过则输出属性集合 S 对应的私钥 SK_S,若验证失败则中止。

3)签名算法 $Sign(m,SK_S,\Gamma)$:由签名者执行,输入消息 m,签名谓词 Γ 和签名者私钥 SK_S 及属性集 S,算法验证属性集合 S 是否满足签名谓词 Γ,若满足则计算生成合法签名 σ,否则算法输出 $\perp$。

4)验证算法 $Verify(m,\Gamma,\sigma,PK)$:由验证者执行,输入消息 m,签名谓词 Γ,签名 σ 和系统公共参数 PK,若签名是满足签名谓词 Γ 的合法有效签名,则输出 True,否则输出 False。

5)追踪算法 $Trace(SK_S, PK, mk)$:由 PKG 执行,输入私钥 SK_S,公共参数 PK 和主私钥 mk,若私钥合法且对应用户存在,则输出用户身份 id,否则输出 $\perp$。

1.4 不可伪造性

通过一个交互式游戏(Game)来定义不可伪造性。设计敌手 $\mathcal{A}$(Adversary)与挑战者 $\mathcal{C}$(Challenger)之间的游戏,该游戏分 4 个阶段进行:

1)开始阶段(InitPhase)

敌手 $\mathcal{A}$ 公布要攻破的签名谓词 Γ^*。

2)初始化阶段(Setup Phase)

挑战者 $\mathcal{C}$ 执行 PKG 初始化算法并公布系统公共参数。

3)查询阶段(Query Phase)

敌手 $\mathcal{A}$ 可以根据前次查询结果适应性地(Adaptively)向挑战者 $\mathcal{C}$ 控制的 2 个预言机发送查询请求:

(1)私钥预言机(Extract Oracle):每次私钥预言机查询可以获取对任意一个属性集合 S(要求 $\Gamma(S)\neq 1$)的合法对应私钥。

(2)签名预言机(Sign Oracle):每次签名预言机查询可以获取对任意一个消息 m 在签名谓词下 Γ 的签名。

4)伪造阶段(Forge Phase)

敌手 $\mathcal{A}$ 输出一个消息 m^* 在签名谓词 Γ^* 下的签名 σ^*,且敌手 $\mathcal{A}$ 未向签名预言机查询过(m^*, Γ^*)的签名。

将敌手 $\mathcal{A}$ 获胜的优势(Advantage)Adv_A 定义为签名(m^*, Γ^*, σ^*)能够通过验证算法的概率。在此游戏的基础上,定义不可伪造性:

定义 4 不可伪造性(Unforgeability)对一个白盒可追踪的基于属性签名协议 Σ,如果任意概率多项式时间敌手在上述选择谓词游戏中获胜的优势都是可忽略的,则称 Σ 在选择谓词安全模型下满足存在性不可伪造性。

1.5 白盒可追踪性

参考文献[12],通过一个交互式游戏来定义白盒可追踪性。如下设计敌手 $\mathcal{A}$ 与挑战者 $\mathcal{C}$ 之间的交互式游戏,游戏分以下 3 个阶段进行:

1)初始化阶段(Setup Phase)

挑战者 $\mathcal{C}$ 执行 PKG 初始化算法并公布系统公共参数。

2)查询阶段(Query Phase)

敌手 $\mathcal{A}$ 可以根据前次查询结果适应性地(Adaptively)向挑战者 $\mathcal{C}$ 控制的私钥预言机(Extract Oracle)发送查询请求,每次查询可以获取对任意一个身份 id 和属性集合 S 的合法对应私钥。

3)伪造阶段(Forge Phase)

敌手 $\mathcal{A}$ 输出一个私钥 SK^*。

将敌手 $\mathcal{A}$ 获胜的优势 Adv_A 定义为 SK^*,使追踪算法 Trace 输出一个此前未查询过的身份的概率。

定义 5 白盒可追踪性(White-box Traceability)对一个白盒可追踪签名协议 Σ,如果任意概率多项式时间敌手在上述游戏中获胜的概率都是可忽略的,则称 Σ 具有白盒可追踪性。

1.6 完美隐私性

参照文献[17]定义完美隐私性。

定义 6 完美隐私性(Perfect Privacy)对一个白盒可追踪签名协议 Σ,如果对任一给定的签名谓词 Γ 和消息 m,任意 2 个属性集合 S_1, S_2 若满足 $\Gamma(S_1)=\Gamma(S_2)=1$,签名 $Sign(m, SK_{S_1}, \Gamma)$ 和 $Sign(m, SK_{S_2}, \Gamma)$ 具有完全相同的分布,则称 Σ 具有完美隐私性。

2 白盒可追踪的基于属性签名协议

2.1 设计思路

考虑如何将向一个 ABS 方案添加白盒可追踪性,这一过程中遇到的主要问题是私钥盲化。私钥盲化是 ABS 方案中用以实现隐私性的常用手段。具体来说,通过盲化,对于给定的私钥,用户可以通过再次随机化得到另一个合法的私钥。这就为追踪算法制造了困难。为此,需要向私钥中添加不动点,使其在私钥重新随机化的过程中保持不变,从而保证私钥与签名者身份的联系不变。

为做到这一点,最直观的设计是由 PKG 对不动点进行数字签名,在签名算法和追踪算法中对不动点进行验证。但这种人为组合的方式对于基于属性签名算法本身并非必要。且非常低效。在本文协议中,参照文献[12]中的设计思想,将 Boneh-Boyen 签名算法[18]有机嵌入到文献[17]方法中,以极小的效率代价实现白盒可追踪性。

具体的构造方法上,先对文献[17]方法做一些修改,在不破坏其不可伪造性证明的前提下去除可联系性(同时牺牲了黑盒可追踪性),实现完美隐私性。为叙述方便,修改后的协议称为隐私保护的基于属性签名的协议。随后向隐私保护的基于属性签名协议添加白盒可追踪性,得到最终的方案,并通过归约证明其安全性不弱于原方案。

2.2 隐私保护的基于属性签名协议

先在文献[17]方法的基础上做以下修改以去除可联系性,实现完美隐私性:

1)私钥抽取算法 $Extract(S, mk)$:私钥中的 $K=g^{\alpha}g^{a(t+t^2)}$ 改为 $K=g^{\alpha}g^{at}$,并去掉 $T=g^{t^2}$。

2)签名算法 $Sign(m, SK_S, \Gamma)$:随机选择 $s\in_R Z_p^*$,

修改向量 $\boldsymbol{a}=(\alpha_1,\alpha_2,\cdots,\alpha_\ell)$ 的条件为满足 $\boldsymbol{aM}=(s,0,\cdots,0)$,向量 $\boldsymbol{b}=(\beta_1,\beta_2,\cdots,\beta_\ell)$ 的条件不变,仍要求满足 $\boldsymbol{bM}=(0,0,\cdots,0)$。同样对 $i\in\{1,2,\cdots,l\}$ 计算 $s_i=L^{\alpha_i}g^{\beta_i}$,然后选取随机数 $r\in Z_p$ 并计算:

$$y=\prod_{i=1}^{\ell}(K_{\rho(i)}^{\alpha_i}h_{\rho(i)}^{\beta_i})$$

$$A=yK^sH(m)^r,B=g^r,D=Y^s$$

最终,签名者得到(m,Γ)的签名:

$$\sigma=(s_1,s_2,\cdots,s_\ell,A,B,D)$$

3)验证算法 $Verify(m,\Gamma,\sigma,PK)$:验证等式改为

$$De(H(m),B)\prod_{i=1}^{l}e(Z^{\lambda_i}h_{\rho(i)},s_i)=e(g,A)$$

与文献[17]方案相比,本文方案做了 2 点修改:1)从私钥抽取算法中去除了参数 $T=at^2$,并将参数 $K=g^\alpha g^{a(t+t^2)}=g^\alpha g^{at}T$ 对应变为 $K=g^\alpha g^{at}$;2)签名生成算法中,要求 $aM=(s,0,\cdots,0)$,并对应修改了签名参数和签名验证算法。容易验证,改动之后方案正确性和不可伪造性的证明过程依然成立。

2.3　白盒可追踪的基于属性签名协议

本协议由以下 5 个算法构成:

1)初始化算法 $Setup(\lambda)$

算法由 PKG 运行。算法接受参数 λ 作为系统安全参数,并确定属性全集 U。算法根据 λ 选取双线性群 G 和双线性映射 $e:G\times G\to G_T$,其中,G 和 G_T 都是阶为大素数 p 的循环群;g 是群 G 的一个生成元。然后算法随机选取 G 中 U 个元素 $h_1,h_2,\cdots,h_U\in G$,分别对应 U 个属性,并选取随机数 $\alpha,\beta,a\in Z_p$ 和一个抗碰撞的哈希函数 $H:\{0,1\}^*\to G$,然后计算:

$$Y=e(g,g)^\alpha,Z=g^a,W=g^\beta$$

最终算法输出公共参数:

$$PK=\{G,G_T,e,g,Y,Z,W,h_1,h_2,\cdots,h_U,H\}$$

输出主私钥 $mk=\{a,\alpha,\beta\}$

PKG 公布公共参数并秘密保存主私钥,并初始化一个表格 T 用于存放身份与私钥的关联。

2)私钥抽取算法 $Extract(id,S,mk)$

算法由 PKG 运行。算法接受用户身份 id,用户属性集 S 和系统主私钥 mk 为输入参数,首先验证用户属性的真实性和有效性,若验证失败则中止,若验证通过则继续。算法随机选择 $c\in Z_p^*$(若 c 已存在于 T 中则重新选择),将(c,id)加入表格 T。随机选择 $t\in_R Z_p^*$,并计算:

$$K=g^{\frac{\alpha}{\beta+c}}g^{at},L=g^{(\beta+c)t},R=c,\{K_x=h_x^{(\beta+c)t}\}_{x\in S}$$

其中,h_x 是属性 x 在公共参数 $h_1,h_2,\cdots,h_U$ 中对应的值。最终算法输出用户私钥:

$$SK_S=\{K,L,R,\{K_x\}_{x\in S}\}$$

PKG 将用户私钥返回给用户。

3)签名算法 $Sign(m,SK_S,\Gamma)$

算法由签名者运行。算法接受一个任意长度的消息 $m\in\{0,1\}^*$,签名者私钥 SK_S,和签名谓词 $\Gamma=(\boldsymbol{M},\rho)$,其中,$\boldsymbol{M}$ 是一个 $l\times k$ 的矩阵;ρ 是一个将 $\boldsymbol{M}$ 的某一行映射到 U 中某一个属性的单射函数。这里单射的确切含义是,$\boldsymbol{M}$ 中的不同两行不会被映射到同一个属性。算法首先检查属性集 S 是否满足签名谓词 Γ,如果不满足,则算法中止;如果满足则继续。算法然后随机选择 $s\in_R Z_p^*$,根据 LSSS 的性质,可以找到向量 $\boldsymbol{a}=(\alpha_1,\alpha_2,\cdots,\alpha_\ell)$ 满足 $\boldsymbol{aM}=(s,0,\cdots,0)$,和向量 $\boldsymbol{b}=(\beta_1,\beta_2,\cdots,\beta_\ell)$ 满足 $bM=(0,0,\cdots,0)$。然后对 $i\in\{1,2,\cdots,l\}$ 计算:

$$s_i=L^{\alpha_i}g^{\beta_i}$$

选取随机数 $r\in Z_p$ 并计算:

$$y=\prod_{i=1}^{\ell}(K_{\rho(i)}^{\alpha_i}h_{\rho(i)}^{\beta_i})$$

$$A_1=yH(m)^rK^{sR},A_2=K^s,B=g^r,D=Y^s$$

最终,签名者得到(m,Γ)的签名:

$$\sigma=(s_1,s_2,\cdots,s_\ell,A_1,A_2,B,D)$$

并返回给签名请求者。

4)验证算法 $Verify(m,\Gamma,\sigma,PK)$

算法由验证者运行,输入消息 m,签名谓词 $\Gamma=(\boldsymbol{M}_{\ell\times k},\rho)$,签名 $\sigma=(s_1,s_2,\cdots,s_\ell,A_1,A_2,B,D)$ 以及公共参数 PK。算法首先选择随机向量 $\boldsymbol{v}=(v_1=1,v_2,\cdots,v_k)$ 并对$i\in\{1,2,\cdots,l\}$计算:

$$\lambda_i=\sum_{j=1}^{k}(v_j\boldsymbol{M}_{i,j})$$

然后验证等式成立与否:

$$De(H(m),B)\prod_{i=1}^{l}e(Z^{\lambda_i}h_{\rho(i)},s_i)$$

$$?\ =e(g,A_1)e(A_2,W)$$

若成立,则判定 σ 是对消息 m 在签名谓词 Γ 下的有效签名,算法输出 True。否则输出 False。

5)追踪算法 $Trace(SK_S,PK,mk)$

算法由 PKG 运行。输入待查询的私钥 SK,公共参数 PK 和 PKG 保存的表格 T。算法首先检查私钥有效性:

$$e(K,Wg^R)=e(g^\alpha,g)e(L,g)$$

若检查通过,则以 R 为索引在 T 表中查找项$(c=R,id)$,若找到则返回 id,否则返回 $\perp$。

3　协议分析

本节从正确性、安全性(包括不可伪造性、白盒可追踪性、完美隐私性)和效率等方面对提出的方案进行分析。

3.1　正确性分析

定理 1　本文提出的白盒可追踪的基于属性签名协议满足正确性。

证明:设 $\sigma=(s_1,s_2,\cdots,s_\ell,A_1,A_2,B,D)$ 是消息 $m\in\{0,1\}^*$ 在签名谓词 $\Gamma=(\boldsymbol{M}_{l\times k},\rho)$ 下的合法签

名,并设生成签名的用户属性集为 S,私钥为 $SK_S=\{K,L,R,\{K_x\}_{x\in S}\}$,则根据协议有:

$A_1=yH(m)^rK^{sR},A_2=K^s,B=g^r,D=Y^s$

于是:

$$e(g,A_1)e(A_2,W)=e(g.y)\cdot e(B,H(m))\cdot D\cdot e(g,g^{as(\beta+c)t})$$

$e(y,g)e(g^{as(\beta+c)t},g)=\prod_{i=1}^{l}e(Z^{\lambda_i}h_{\rho(i)},s_i)$ 根据验证算法,验证者会选择向量 $\boldsymbol{v}=(v_1=1,v_2,v_3,\cdots,v_k)$ 并计算:

$\lambda_i=\sum_{j=1}^{k}(v_j\boldsymbol{M}_{i,j}),i\in[1,\ell]$

通过交换求和次序有:

$$\sum_{i=1}^{\ell}\alpha_i\lambda_i=\sum_{i=1}^{\ell}\alpha_i\sum_{j=1}^{k}(v_j\boldsymbol{M}_{i,j})=\sum_{j=1}^{k}v_j\sum_{i=1}^{\ell}(\alpha_i\boldsymbol{M}_{i,j})=s$$

类似地,有:

$$\sum_{i=1}^{\ell}\beta_i\lambda_i=\sum_{j=1}^{k}v_j\sum_{i=1}^{\ell}(\beta_i\mathrm{M}_{i,j})=0$$

因此:

$$\sum_{i=1}^{l}a\lambda_i((\beta+c)t\alpha_i+\beta_i)=a((\beta+c)t\sum_{i=1}^{\ell}\alpha_i\lambda_i+\sum_{i=1}^{\ell}\beta_i\lambda_i)=as(\beta+c)t$$

可以将 $e(g^{as(\beta+c)t},g)$ 展开为:

$$e(g^{as(\beta+c)t},g)=\prod_{i=1}^{l}e(g^{a\lambda_i},g^{(\beta+c)t\alpha_i+\beta_i})=\prod_{i=1}^{l}e(Z^{\lambda_i},s_i)$$

于是:

$$e(y,g)e(g^{as(\beta+c)t},g)=\prod_{i=1}^{l}(e(h_{\rho(i)}^{(\beta+c)t\alpha_i+\beta_i},g)e(Z^{\lambda_i},s_i))=\prod_{i=1}^{l}e(Z^{\lambda_i}h_{\rho(i)},s_i)$$

综合以上各式可以得到:

$$De(H(m),B)\prod_{i=1}^{l}e(Z^{\lambda_i}h_{\rho(i)},s_i)=e(g,A_1)e(A_2,W)$$

至此白盒可追踪的基于属性签名协议的正确性得证。

3.2 安全性分析

3.2.1 不可伪造性

采用归约的手法,将 2.3 节白盒可追踪的基于属性签名协议(以下称为 Σ_{wbtabs})的不可伪造性归约到 2.2 节隐私保护的基于属性签名(以下称为 Σ_{ppabs})的不可伪造性上。

定理 2 假设存在多项式时间敌手 $\mathcal{A}$,能够在选择谓词模型下攻破 Σ_{wbtabs},则可以构造一个多项式时间算法 $\mathcal{B}$,能够在选择谓词模型下攻破 Σ_{ppabs}。

证明:通过 1.4 节所定义的交互式过程证明上述定理。

1)初始化阶段(Init Phase)

$\mathcal{A}$ 向 $\mathcal{B}$ 提交要挑战的签名谓词 Γ^*,$\mathcal{B}$ 提交给 Σ_{ppabs}。

2)参数设置阶段(Setup Phase)

Σ_{ppabs} 生成公共参数 $PK_{\text{ppabs}}=\{G,G_{\mathrm{T}},e,p,g,Y,Z,h_1,h_2,\cdots,h_U,H\}$ 并传递给 $\mathcal{B}$,$\mathcal{B}$ 随机选择 $\beta\in_R Z_p^*$,计算 $W=g^{\beta}$,生成 Σ_{wbtabs} 的公共参数。

$PK_{\text{wbtabs}}=\{G,G_T,e,p,g,W,Y,Z,h_1,h_2,\cdots,h_U,H\}$ 并初始化表 $T=\varnothing$。

3)询问阶段(Query Phase)

(1)私钥预言机:$\mathcal{A}$ 可以向 $\mathcal{B}$ 提交任意(id,S)参数询问身份为 id,属性集合为 S,且 $\Gamma^*(S)\neq 1$ 的私钥。$\mathcal{B}$ 收到请求后,先向 Σ_{ppabs} 请求属性集合 S 的私钥,假设 Σ_{ppabs} 返回的私钥为:

$\overline{SK}_{\text{ppabs}}=\{\bar{K}=g^{\alpha}g^{at},\bar{L}=g^{t},\{\bar{K}_x\}_{x\in S}\}$

$\mathcal{B}$ 得到私钥后随机选择 $c\in_R Z_p^*$ 且 $c\neq-\beta$,如果 c 已经在表 T 中则重新选择,直到得到可用的 c。然后令 $R=c$ 并计算:

$$K=(\bar{K})\frac{1}{\beta+c},L=\bar{L},\{K_x=\bar{K}_x\}_{x\in S}$$

注意到上述各式相当于隐式设置 $t=\dfrac{\beta+c}{}$,且令:

$$K=(\bar{K})\frac{1}{\beta+c}=g^{\frac{\alpha}{\beta+c}}g^{a\frac{t}{\beta+c}}=g^{\frac{\alpha}{\beta+c}}g^{at}$$

$$L=\bar{L}=g^{t}=g^{(\beta+c)t}$$

$$K_x=\bar{K}_x=h_x^{t}=h_x^{(\beta+c)t},x\in S$$

然后 $\mathcal{B}$ 将私钥 $\overline{SK}_{\text{wbtabs}}=\{K,L,\{K_x\}_{x\in S},R\}$ 返回给 $\mathcal{A}$。

(2)签名预言机:假设 $\mathcal{A}$ 请求对(m,Γ)签名。$\mathcal{B}$ 首先检查是否存在属性集合 S 使得 $\Gamma(S)=1$ 且 $\Gamma^*(S)\neq 1$,若这样的 S 存在,则 $\mathcal{B}$ 直接生成 S 和任意 id 的对应私钥,并运行签名算法对(m,Γ)签名。否则,$\mathcal{B}$ 寻找随机向量 $\boldsymbol{\alpha}=(\alpha_1,\alpha_2,\cdots,\alpha_l)$ 使得 $\boldsymbol{aM}=(s,0,0,\cdots,0)$ 和随机向量 $\boldsymbol{b}=(\beta_1,\beta_2,\cdots,\beta_\ell)$ 使得 $\boldsymbol{bM}=(0,0,\cdots,0)$,然后 $\mathcal{B}$ 随机选择 $t,r\in_R Z_p$,$c\in_R Z_p^*$,并计算:

$s_i=g^{(\beta+c)t\alpha_i}g^{\beta_i}=L^{\alpha_i}g^{\beta_i},(i=1,2,\cdots,l)$

$y=\prod_{i=1}^{l}h_{\rho(i)}^{t(\beta+c)\alpha_i+\beta_i}=\prod_{i=1}^{l}(K_{\rho(i)}^{\alpha_i}h_{\rho(i)}^{\beta_i})$

$A_1=y(g^{\frac{\alpha}{\beta+c}}g^{at})^{sc}H(m)^r=yK^{sc}H(m)^r$

$A_2=(g^{\frac{\alpha}{\beta+c}}g^{at})^s=K^s$

$B=g^r,D=Y^s$

4)伪造阶段(Forge Phase)

最终 $\mathcal{A}$ 输出一个消息 m^* 在签名谓词 Γ^* 下的签名:

$\bar{\sigma}^*=(\bar{s}_1,\bar{s}_2,\cdots,\bar{s}_l,\bar{A}_1,\bar{A}_2,\bar{B},\bar{D})$

$\mathcal{B}$ 计算并输出签名:

$\sigma^* = (\bar{s}_1, \bar{s}_2, \cdots, \bar{s_l}, A = \bar{A}_1 \cdot (\bar{A}_2)^{\beta}, \bar{B}, \bar{D})$

容易验证,σ^* 是 Σ_{ppabs} 协议下消息 m^* 在签名谓词 Γ^* 下的合法签名,于是 $\mathcal{B}$ 以 $Adv_{\Sigma\text{ppabs}} = Adv_A \Sigma_{\text{wbtabs}}$ 的优势攻破基于属性隐私保护协议 Σ_{ppabs},定理得证。

3.2.2　白盒可追踪性

按照 2.2 节所述的安全性定义,证明本文提出的 Σ_{wbtabs} 签名协议在 q-SDH 假设下具有白盒可追踪性。该证明的构造过程使用了文献[18]的签名协议证明中的技巧。

定理 3　如 q-SDH 假设成立,则本文提出的白盒可追踪基于属性签名协议 Σ_{wbtabs} 具有白盒可追踪性。

证明:设有概率多项式时间的敌手 $\mathcal{A}$ 能够在 q 次询问后以 ϵ 的优势赢得可追踪性游戏,不失一般性设 $q = q + 1$,则可以构造一个概率时间多项式算法 $\mathcal{B}$ 以 ϵ 的优势攻破 q-SDH 假设。过程如下:

1)参数设置阶段(Setup Phase)

$\mathcal{B}$ 接受一个q-SDH假设的参数$(\bar{g}, \bar{g}^{\beta}, \cdots, \bar{g}^{\beta^q})$作为输入,其中 $\bar{g}$ 是 G 上的元素,并记 $A_i = \bar{g}^{x^i}, i = 0, 1, \cdots, q$。然后 $\mathcal{B}$ 选择 q 个随机数 $c_1, c_2, \cdots, c_q \in Z_p^*$,并设多项式函数$f(y)$为如下形式:

$$f(y) = \prod_{i=1}^{q} (y + c_i)$$

将 $f(y)$做多项式展开并记作:

$$f(y) = \sum_{i=0}^{q} \eta_i y^i$$

其中,$\eta_0, \eta_1, \cdots, \eta_q \in Z_p$ 是多项式的各项系数。$\mathcal{B}$ 随后计算:

$$g \leftarrow \prod_{i=0}^{q-1} A_i^{\eta_i} = \prod_{i=0}^{q-1} (\bar{g}^{\beta^i})^{\eta_i} = \bar{g}^{f(\beta)}$$

$$g^{\beta} \leftarrow \prod_{i=1}^{q} A_i^{\eta_{i-1}} = \prod_{i=1}^{q} (\bar{g}^{\beta^i})^{\eta_{i-1}} = \bar{g}^{\beta f(\beta)}$$

$\mathcal{B}$ 公布公共参数:

$PK = \{G, G_T, e, g, Y = e(g,g)^{\alpha}, Z = g^a, W = g^{\beta}\}$

主私钥为:

$mk = \{a, \alpha, \beta\}$

2)私钥询问阶段(KeyQuery Phase)

在第 i 次询问中,敌手 $\mathcal{A}$ 向 $\mathcal{B}$ 提交参数(id_i, S_i)询问身份为 id_i,属性集合为 S_i 的对应私钥。设多项式函数 $f_i(y)$为如下形式:

$$f_i(y) = \frac{f(y)}{y + c_i} = \prod_{j=1, j \neq i}^{q-1} (y + c_i)$$

类似地,做多项式展开得到:

$$f_i(y) = \sum_{j=0}^{q-2} \theta_j y^j$$

$\mathcal{B}$ 计算:

$$\sigma_i = \prod_{j=0}^{q-2} A_j^{\theta_j} = \prod_{j=0}^{q-2} (\bar{g}^{\beta^j})^{\theta_j} = \bar{g}^{f_i(\beta)} = g^{\frac{1}{\beta + c_i}}$$

随后 $\mathcal{B}$ 随机选择 $t \in Z_p^*$,计算:$K = \sigma_i^{\alpha} g^{at}$,$L = g^{(\beta + c_i)t}$,$\{K_x = h_x^{(\beta + c_i)t}\}_{x \in S}$,$R = c_i$ 并将(c_i, id_i)添加到表 T 中。

3)伪造阶段(Forge Phase)

$\mathcal{A}$ 向 $\mathcal{B}$ 提交一个私钥$\text{SK}^* = \{K^*, L^*, R^*\}$,根据假设,私钥能够通过有效性验证且 $R^* \notin \{c_1, c_2, \cdots, c_q\}$。$\mathcal{B}$ 收到私钥后,首先将多项式函数 $f(y)$改写成:

$$f(y) = \gamma(y)(y + R^*) + \gamma_{-1} \qquad (*)$$

其中,余项 $\gamma_{-1} \in Z_p$,而 $\gamma(y)$是一个关于 y 的多项式:

$$\gamma(y) = \sum_{i=0}^{q-2} \gamma_i y^i$$

在式$(*)$两边同时除以$(y + R^*)$,得到有理分式:

$$\frac{f(y)}{y + R^*} = \gamma(y) + \frac{\gamma_{-1}}{y + R^*}$$

因为 $f(y) = \prod_{i=1}^{q} (y + c_i)$且 $R^* \notin \{c_1, c_2, \cdots, c_q\}$,于是由代数基本定理可知$(y + R^*)$必不能整除 $f(y)$,所以余项 $\gamma_{-1} \neq 0$,依次计算:

$$\sigma^* \leftarrow \left(\frac{K^*}{(L^*)^a}\right)^{\frac{1}{\alpha}} = \left(\frac{g^{\frac{\alpha}{\beta + R^*}} g^{at}}{g^{at}}\right)^{\frac{1}{\alpha}} = g^{\frac{1}{\beta + R^*}} = \bar{g}^{\frac{f(\beta)}{\beta + R^*}}$$

$$= (\bar{g})^{\gamma(\beta)} (\bar{g})^{\frac{\gamma_{-1}}{\beta + R^*}} = \prod_{i=0}^{q-1} A_i^{\gamma_i} (\bar{g}^{\frac{1}{\beta + R^*}})^{\gamma_{-1}}$$

$$w^* \leftarrow (\sigma^* \cdot \prod_{i=0}^{q-1} A_i^{-\gamma_i})^{\frac{1}{\gamma_{-1}}} = \bar{g}^{\frac{1}{\beta + R^*}}$$

至此,得到了 q-SDH 问题的一个解:(R^*, w^*),于是定理得证。

3.2.3　完美隐私性

定理 4　本文提出的白盒可追踪的基于属性签名协议 Σ_{wbtabs}具有完美隐私性。

证明:首先,对于任一给定的合法签名,任何人均无法计算出哪些属性被用于签名。这一性质是由随机向量 β 保证的:对于任一给定的签名谓词 $\Gamma = (\boldsymbol{M}, \rho)$,其中 $\boldsymbol{M}$ 是 $l \times k$ 的矩阵,且 Γ 不是一个 (n,n)门限谓词(否则签名者必然具备所有属性,分析没有意义),那么有 $rank(\boldsymbol{M}) < l$,使得 $\boldsymbol{\beta M} = (0, 0, \cdots, 0)$成立的 $\boldsymbol{\beta}$ 有多项式个,从而 β 隐藏了哪些属性被使用。其次,对任意的签名谓词 Γ 和给定的消息 m,使用任意满足签名谓词的属性集合 S 和对应私钥 SK_S,签名算法所生成的签名 σ 中的各个分量都在各自值域上随机均匀分布,因此 σ 具有完全随机分布。

3.3　效率分析

表 1 将本文提出的白盒可追踪基于属性签名协议与其他基于属性签名协议在安全性、效率、隐私性、可追踪性等方面整体进行比较。与文献[6,9,15]等

同类协议相比,本文提出的协议在性能上有明显提升。相比于文献[17]协议,私钥长度不变,签名长度增加了一项,效率相差一个常数。但本文协议实现了不可联系性和完美隐私性,隐私性比文献[17]协议更强。

表 1 基于属性签名协议对比

项目	文献[6]协议	文献[9]协议	文献[15]协议	文献[17]协议	本文协议
签名长度	$l+k+2$	$7l+11$	$8l+k+7$	$l+3$	$l+4$
复杂度	$kl+k+3$	$7l+15$	–	$l+3$	$l+4$
安全性	完全	完全	完全	选择谓词	选择谓词
安全模型	通用群	标准	随机预言	随机预言	随机预言
隐私性	完美隐私性	完美隐私性	隐私性	隐私性	完美隐私性
不可联系性	√	√	√	×	√
可追踪性	×	×	黑盒可追踪	黑盒可追踪	黑盒可追踪

表中的复杂度指签名算法与验证算法的复杂度之和,且只统计复杂度最高的双线对运算。安全性和安全模型均指不可伪造性的安全性、安全模型。表中文献[15]协议采用非交互式不可区分证明,无法简单统计其复杂度。

4 结束语

本文提出白盒可追踪基于属性签名协议的形式化定义和安全模型,并给出了一个签名协议的实例。协议通过将 Boneh-Boyen 签名算法[18]融入基于属性签名算法中实现了白盒可追踪性。经过分析,本文提出的协议在效率上仅比最优的同类方案相差一个常数,但隐私性更强。如何将相关设计思想推广到黑盒可追踪性是未来值得研究的方向,目前尚无基于属性数字签名协议在不借助非交互式不可区分证明的前提下实现不可联系性与黑盒可追踪性。此外,本文协议的安全性证明是在选择谓词游戏下进行的,未来可研究如何实现具备完全安全性的可追踪基于属性签名协议。

参考文献

[1] Sahai A, Waters B. Fuzzy Identity-based Encryption[C]//Proceedings of International Conference on Theory & Applications of Cryptographic Techniques. Berlin, Germany: Springer, 2005: 457-473.

[2] Shamir A. Identity-based Cryptosystems and Signature Schemes[C]//Proceedings of CRYPTO'84. Berlin, Germany: Springer, 1984: 47-53.

[3] Goyal V, Pandey O, Sahai A, et al. Attribute-based Encryption for Fine-grained Access Control of Encrypted Data[C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria, USA: ACM Press, 2006: 89-98.

[4] Bethencourt J, Sahai A, Waters B. Ciphertext-policy Attribute-based Encryption[C]//Proceedings of IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2007: 321-334.

[5] Waters B. Ciphertext-policy Attribute-based Encryption: An Expressive, Efficient, and Provably Secure Realization[C]//Proceedings of International Workshop on Public Key Cryptography. Berlin, Germany: Springer, 2011: 53-70.

[6] Maji H K, Prabhakaran M, Rosulek M. Attribute-based Signatures[C]//Proceedings of International Conference on Topics in Cryptology. Berlin, Germany: Springer, 2011: 376-392.

[7] Li Jin, Au M H, Susilo W, et al. Attribute-based Signature and Its Applications[C]//Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. New York, USA: ACM Press, 2010: 60-69.

[8] Shahandashti S F, Safavi-Naini R. Threshold Attribute-based Signatures and Their Application to Anonymous Credential Systems[C]//Proceedings of International Conference on Topics in Cryptology. Berlin, Germany: Springer, 2009: 198-216.

[9] Okamoto T, Takashima K. Efficient Attribute-based Signatures for Non-monotone Predicates in the Standard Model[J]. IEEE Transactions on Cloud Computing, 2014, 2(4): 409-421.

[10] Goyal V. Reducing Trust in the PKG in Identity Based Cryptosystems[C]//Proceedings of International Cryptology Conference on Advances in Cryptology. Berlin, Germany: Springer, 2007: 430-447.

[11] Goyal V, Lu S, Sahai A, et al. Black-box Accountable Authority Identity-based Encryption[C]//Proceedings of the 15th ACM Conference on Computer and Communications Security. Alexandria, USA: ACM Press, 2008: 427-436.

[12] Liu Zhen, CaoZhenfu, Wong D S. White-box Traceable Ciphertext-policy Attribute-based Encryption Supporting Any Monotone Access Structures[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(1): 76-88.

[13] Ning Jianting, Dong Xiaolei, Cao Zhenfu, et al. White-box Traceable Ciphertext-policy Attribute-based Encryption Supporting Flexible Attributes[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(6): 1274-1288.

[14] Ning Jianting, Cao Zhenfu, Dong Xiaolei, et al. Large Universe Ciphertext-policy Attribute-based Encryption with White-box Traceability[C]//Proceedings of the 19th European Symposium on Research in Computer Security. Berlin, Germany: Springer, 2014: 55-72.

(下转第 140 页)

规则、位移-速度限制规则、数据分组修改限制规则、贪婪转发限制规则和边界转发限制规则。根据这些检测规则,给出了入侵检测算法的基本框架和运行流程,包括位置请求信标信号检测流程、位置响应信标信号检测流程和 GPSR 数据分组检测流程。在网络模拟器 NS3 中构建运行 GPSR 协议的 MANET,以及本文提出的入侵检测系统进行仿真实验,结果表明,提出的入侵检测方法对恶意攻击具有较高的检测率和较低的误报率。

参考文献

[1] 易 平,蒋嶷川,张世永,等. 移动 Ad Hoc 网络安全综述[J]. 电子学报,2005,33(5):893-899.

[2] 钱 钊. 基于位置信息的移动自组织网络路由算法研究[D]. 哈尔滨:哈尔滨工业大学,2013.

[3] Karp B, Kung H T. GPSR: Greedy Perimeter Stateless Routing for Wireless Networks[C]//Proceedings of the 6th International Conference on Mobile Computing and Networking. Boston, USA: ACM Press, 2000: 243-254.

[4] Zhang Yongguang, Lee W. Intrusion Detection in Wireless Ad-hoc Networks[C]//Proceedings of the 6th International Conference on Mobile Computing and Networking. Boston, USA: ACM Press, 2000: 275-283.

[5] Zhang Yongguang, Lee W. Intrusion Detection Techniques for Mobile Wireless Networks[J]. Mobile Networks and Applications, 2003, 9(5): 545-556.

[6] Kachirski O, Guha R. Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks[C]//Proceedings of IEEE Workshop on Knowledge Media Networking. Kyoto, Japan: IEEE Computer Society, 2002: 153-158.

[7] 姚越鹏,钟求喜. 基于代理的分级 MANET 入侵检测系统[J]. 计算机工程,2009,35(3):192-194.

[8] Huang Yi-an, Lee W. A Cooperative Intrusion Detection System for Ad Hoc Networks[C]//Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks. New York, USA: ACM Press, 2003: 135-147.

[9] Cretu G F, Parekh J, Wang Ke, et al. Intrusion and Anomaly Detection Model Exchange for Mobile Ad-Hoc Networks[C]//Proceedings of IEEE Consumer Communication and Networking Conference. Las Vegas, USA: IEEE Communications Society, 2006: 635-639.

[10] Jabbehdari S, Talari S H, Modiri N. A Neural Network Scheme for Anomaly Based Intrusion Detection Systems in Mobile Ad Hoc Networks[J]. Journal of Computing, 2012, 4(2): 61-66.

[11] Vgina G, Gawalani S, Srinivasan K, et al. An Intrusion Detection Tool for AODV Based Ad Hoc Wireless Networks[C]//Proceedings of IEEE Annual Computer Security Application Conference. Tucson, USA: IEEE Computer Society, 2004: 16-27.

[12] Subhadrabandhu D, Sarkar S, Anjum F. A Framework for Misuse Detection in Ad Hoc Networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 274-289.

[13] Nadeem A, Michael P H. A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks[J]. IEEE Communications Surveys & Tutorials, 2013, 15(4): 2027-2045.

[14] Tseng C Y, Balasubramanyam P, Ko C, et al. A Specification-based Intrusion Detection System for AODV[C]//Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks. Fairfax, USA: ACM Press, 2003: 125-134.

[15] Hassan H M, Mahmoud, El-Kassas S. Securing the AODV Protocol Using Specification-based Intrusion Detection[C]//Proceedings of Q2SWinet'06. Torremolinos, Spain: ACM Press, 2006: 33-36.

[16] Lin Hsiao-ching, Sun Ming-kung, Huang Hanwei, et al. A Specification-based Intrusion Detection Model for Wireless Ad Hoc Networks[C]//Proceedings of the 3rd International Conference on Innovations in Bio-Inspired Computing and Applications. Washington D. C., USA: IEEE Press, 2012: 252-257.

[17] 易 平,柳 宁,吴 越. 基于时间自动机的 Ad hoc 网络入侵检测[J]. 电子与信息学报,2009,31(19):2310-2315.

[18] 易 平. 移动 Ad Hoc 网络入侵检测与主动响应机制研究[D]. 上海:复旦大学,2005.

[19] 王 芳,易 平,吴 越,等. 基于规范的移动 Ad Hoc 网络分布式入侵检测[J]. 计算机科学,2010,37(10):118-122.

[20] Orset J M, Alcalde B, Cavalli A. An EFSM-based Intrusion Detection System for Ad Hoc Networks[C]//Proceedings of the 3rd International Symposium on Automated Technology for Verification and Analysis. Berlin, Germany: Springer, 2005: 399-412.

[21] Tseng C H, Song T, Balasubramanyam P, et al. A Specification-based Intrusion Detection Model for OLSR[C]//Proceedings of the 8th International Symposium on Recent Advances in Intrusion Detection. Berlin, Germany: Springer, 2005: 330-350.

编辑 顾逸斐

(上接第 132 页)

[15] Escala A, Herranz J, Morillo P. Revocable Attribute-based Signatures with Adaptive Security in the Standard Model[C]//Proceedings of International Conference on Progress in Cryptology in Africa. Berlin, Germany: Springer, 2011: 224-241.

[16] 张秋璞,徐 震,叶顶峰. 一个可追踪身份的基于属性签名方案[J]. 软件学报,2012,23(9):2449-2464.

[17] Ding Shenglong, Zhao Yiming, Liu Yuyang. Efficient Traceable Attribute-based Signature[C]//Proceedings of the 13th International Conference on Trust, Security and Privacy in Computing and Communications. Washington D. C., USA: IEEE Press, 2014: 582-589.

[18] Boneh D, Boyen X. Short Signatures Without Random Oracles[C]//Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer, 2004: 56-73.

编辑 顾逸斐