具有强指定验证者的属性基可净化签名方案

李继国[1),2),5)] 朱留富[1)] 沈 剑[3)] 陆 阳[4)] 张亦辰[1),2)]

[1)](福建师范大学计算机与网络空间安全学院 福州 350117)

[2)](福建省网络安全与密码技术重点实验室(福建师范大学) 福州 350117)

[3)](浙江理工大学信息科学与工程学院 杭州 310018)

[4)](南京师范大学计算机与电子信息学院/人工智能学院 南京 210023)

[5)](分析数学及应用教育部重点实验室(福建师范大学) 福州 350117)

摘 要 属性基签名(Attribute-Based Signature, ABS)利用一组属性代替用户身份从而实现签名者匿名性,并且提供了细粒度访问控制功能. 生成的签名可以被任何人公开验证,确保了签名的真实性和有效性. 但在一些特定的应用场景中,比如电子投票,电子投标或软件销售许可中,签名者希望签名只能被指定的验证者验证从而防止数字签名恶意传播. 同时,当签名消息中包含一些敏感信息时,若未执行脱敏操作也会导致数据隐私泄露. 因此,为了实现用户隐私保护以及数据中敏感信息隐藏,本文提出了具有强指定验证者的属性基可净化签名方案. 基于双线性Diffie-Hellman(BDH)困难问题假设,在标准模型下证明了方案的安全性. 提出的方案不但具有匿名性保护用户身份隐私,而且方案通过对消息进行脱敏操作来保护敏感信息的安全. 同时,通过指定验证者验证签名的合法性,使第三方无法判断签名是否由原始签名者生成,因为指定验证者也能产生合法的签名,从而达到控制数字签名/版权恶意传播的目的. 进一步,分析了方案的通信开销和计算开销,基于虚拟机Ubuntu 18.4,在Charm0.5框架下实现了提出的方案,实验分析表明提出的方案具有可行性.

关键词 属性基签名;强指定验证者;可净化;隐私性;标准模型

中图法分类号 TP391 **DOI号** 10.11897/SP.J.1016.2023.01806

Attribute-Based Sanitizable Signature Scheme with Strong Designated Verifier

LI Ji-Guo[1),2),5)] ZHU Liu-Fu[1)] SHEN Jian[3)] LU Yang[4)] ZHANG Yi-Chen[1),2)]

[1)](*College of Computer and Cyber Security, Fujian Normal University, Fuzhou* 350117)

[2)](*Fujian Provincial Key Laboratory of Network Security and Cryptology, Fuzhou* 350117)

[3)](*School of Information Science and Engineering, Zhejiang Sci-Tech University, Hangzhou* 310018)

[4)](*School of Computer and Electronic Information/School of Artificial Intelligence, Nanjing Normal University, Nanjing* 210023)

[5)](*Key Laboratory of Analytical Mathematics and Applications (Ministry of Education), Fuzhou* 350117)

Abstract Attribute-based signature (ABS) uses a set of attributes to replace user's identity to achieve anonymity, which can provide data integrity, authentication and non-repudiation, and the fine-grained access control function. In attribute-based signature scheme, the signature generated by the original signer can be publicly verified by anyone to ensure the authenticity and validity of the signature. However, in some specific application scenarios, such as electronic voting, electronic bidding or software sales license, the original signer only wants the signature to be verified by the designated verifier to prevent the malicious spread of the digital signature. Even if the designated verifier discloses its secret information, he/she cannot make other people believe the original signer's signature behavior. In addition, the signature message may contain some sensitive

收稿日期:2022-08-15;在线发布日期:2023-02-03. 本课题得到国家自然科学基金项目(62072104, 61972095, U21A20465, 61922045, 62172292, 61877034)、福建省自然科学基金项目(2020J01159)资助.**李继国**(**通信作者**),博士,教授,中国计算机学会会员,主要研究方向为公钥密码学、云计算安全. E-mail: ljg1688@163.com. **朱留富**,硕士研究生,主要研究方向是公钥密码学. **沈 剑**,博士,教授,中国计算机学会高级会员,主要研究方向为公钥密码学、云计算安全. **陆 阳**,博士,教授,主要研究方向为信息安全,公钥密码学. **张亦辰**(**通信作者**),博士,副教授. 主要研究方向为公钥密码学、云计算安全. E-mail: zyc_718@163.com.

information, for example, in e-health, e-finance, or e-government. The signature message also contains some personal privacy records, business transaction secrets or secret government information. It will lead to privacy leakage if we do not perform desensitization operation, which brings great security risks to individuals and society. The idea of strong-designated verifier signature is that only the designated verifier can verify validity of the signature, and other users can not verify validity of the signature, because the designated verifier can also generate a valid signature by using its secret key. A sanitizable signature is a method that can make the sensitive information be modified or deleted by the sanitizer to generate a sanitizable message. The sanitizer can still generate a valid signature without the signer's secret key. Therefore, sanitizable signature scheme can protect the privacy of the user. It is challenging problem for the existing ABS scheme to solve privacy leakage and the malicious spread of the signature. In order to address above problems, we propose an attribute-based sanitizable signature scheme with strong designated verifier (ABSS-SDV), which prevents the signature from being spread maliciously and protects the privacy of users by hiding the sensitive information in the message. The proposed scheme uses a set of attributes to replace the real identity of the user, which is anonymous to protect the privacy of the user's identity. The proposed scheme avoids data privacy leakage by desensitizing messages and protects the security of sensitive information. At the same time, the authenticity and validity of the signature can only be verified by the designated verifier. Even if the designated verifier exposes its secret information, it cannot make the other people judge whether the signature is generated by the original signer because the designated verifier can also produce a legal signature. Therefore, the proposed scheme achieves the goal of controlling the malicious dissemination of digital signature/copyright. We prove that the proposed scheme is existentially unforgeable against adaptive chosen message attack and immutable in the standard model. The security of our scheme is reduced to the bilinear Diffie-Hellman (BDH) problem assumption. Finally, based on the virtual machine Ubuntu 18.4, the proposed scheme is implemented under the framework of Charm0.5. The experimental analysis shows that the proposed scheme is feasible. Therefore, it can be applied to electronic voting, electronic bidding or software sales licensing applications and so on.

Keywords　attribute-based signature; strong designated verifier; sanitizable; privacy; standard model

1　引　言

自 2005 年 Sahai 和 Waters[1] 提出模糊身份基加密概念后,属性基加密的概念被正式提出. 在属性基加密方案中,用户身份用一组属性集描述,只要属性集满足事先定义访问策略,用户便能获得访问控制权限对密文进行正确解密,在获得保密性的同时还实现了一对多的通信方式,并可以通过设置访问策略提供细粒度访问控制,所以属性基密码方案[2-4]得到了学术界和工业界的广泛关注. 尽管属性基加密方案[1,2]能够提供数据的细粒度访问控制和保密性,但是无法实现云存储环境下的数据完整性和认证性. 为解决这一问题,2011 年,Maji 等人[5]提出了属性基签名方案. 在属性基签名(Attribute-Based Signature, ABS)方案[4-7]中,签名者的密钥与一组属性相关联,密钥生成中心根据关联属性为签名者产生签名密钥. 签名者利用密钥对消息产生一个公开可验证的签名. 虽然 ABS 方案实现了细粒度访问控制功能和匿名性,但在某些特殊的场合需要对签名者的签名行为进行保护防止签名被恶意传播,同时需要对消息中的敏感信息进行编辑修改防止敏感信息泄露. 例如在电子医疗中,甲医院将采集的医疗数据交给有资质的医疗检测机构做肿瘤个性化用药基因检测. 为了防止检测结果恶意传播造成同业竞争,只有甲医院能够验证医疗检测机构提供的化疗相关检测结果、免疫治疗相关检测结果、遗传风险相关检测结果、靶向治疗相关检测结果以及肿瘤个性化用药基因检测结果的有效性. 原始检测报告包含病情、基因是否匹配等敏感信息.

但是,病人家属出于人文关怀角度出发,希望甲医院不要将包含敏感信息的检测报告直接发送给病人.为了解决这一问题,本文利用强指定验证者签名技术对签名者的行为进行指定验证防止签名恶意传播,同时利用净化签名技术对消息中的敏感数据进行脱敏保护数据隐私.

2 相关工作

属性基密码主要包括属性基加密和属性基签名.在属性基加密方案中,根据访问策略部署的位置不同可分为密文策略[2,8-9]和密钥策略[10]的属性基加密.密文策略的属性基加密(CP-ABE)[2,8-9]方案中,访问策略与密文关联,一个属性集与密钥关联.当属性集满足密文中的访问策略时,用户可以正确解密.在许多情况下,由于某种原因,授权解密用户可能无法及时解密密文.为了解决这一问题,Chen等人[8]提出一个共享解密的密文策略属性基加密方案.授权用户可以独立恢复消息.同时,半授权用户可以合作获取消息.在 CP-ABE 中,访问策略和密文一起发送给接收方,但是访问策略中包含一些敏感信息,会泄露用户的隐私.此外,在 CP-ABE 中,有些数据用户出于商业目的故意泄露属性密钥给非授权用户解密,这种密钥滥用问题严重阻碍了属性基加密的应用.为了保护用户隐私和防止密钥滥用,Li 等人[9]提出了具有隐私保护和审计功能的密文策略属性基加密方案.在密钥策略[10]的属性基加密方案中,访问策略与密钥关联,属性集嵌入在密文中,当且仅当密文中的属性集满足密钥中的访问策略时,用户可以正确解密.

为了实现通信数据的完整性、认证性和不可否认性,2011 年,Maji 等人[5]提出了属性基签名方案,但该方案只在一般群模型中证明方案的安全性.2012 年,Okamoto 等人[4]提出一种支持非单调访问策略的高效 ABS 签名方案,并在标准模型下给出了方案的安全性证明.上述的签名方案都是签名可公开验证,即任何人都可以通过验证算法验证签名的有效性.但在一些特殊的应用中,签名者不希望泄露自己的身份信息和签名行为,除了指定的验证者可以验证签名的真实性和有效性,其他人无法验证该签名.1996 年,Jakobsson 等人[11]首次提出指定验证者签名方案,不仅解决了任何人可验证签名的问题,还解决了签名者对签名的完全控制问题.随着云计算的发展,云存储设备中的数据验证成为一个亟待解决的问题,Yan 等人[12]提出了云存储中的指定验证者远程数据验证方案,只有指定的验证者才能对存储数据进行远程验证.在原始的指定验证者签名方案中,由于签名只能由签名者产生,那么一旦该指定验证者向其他用户证明签名者行为,则指定验证者可以泄露签名者的隐私信息.而强指定验证者签名方案确保指定验证者能模拟一个有效的签名副本,从而无法使其他用户相信其泄露的信息是否真实可信.同时,原始的指定验证者签名方案大多基于传统公钥密码体制,用户的身份与一个随机字符串关联,在验证一个签名之前需要通过可信机构验证公钥的有效性.2004 年,Susilo 等人[13]提出了基于身份的强指定验证者签名,强指定验证者可以模拟一个有效的签名副本,从而避免了指定验证者恶意泄露签名者隐私.同时,用户的公钥被公开的身份信息代替从而避免了公钥验证.然而基于身份的密码学方案中存在密钥托管问题,为了解决密钥托管问题,李继国等人[14-15]提出了基于证书的指定验证者和强指定验证者签名方案.但使用公开身份作为公钥往往泄露了签名者隐私,无法提供匿名性.2011 年,Fan 等人[16]提出了具有强指定验证者的属性基签名方案,利用一组属性代替用户身份实现了签名者匿名性并具有指定验证者功能.2022 年,Blazy 等人[17]提出了匿名的具有强指定验证者签名方案,实现了匿名身份验证功能.在签名时不仅需要保护签名者隐私,同时也要保护消息中敏感数据的隐私性.在特定的应用场景中,如电子医疗、电子政务等,因为病患的病情或者涉及国家安全的政务信息要求保密,需要对消息中的敏感数据进行修改使敏感部分不再公开,该方法称为“净化”.可净化数字签名(sanitizable signature)允许净化者在不知道签名者私钥的前提下修改已签名数据的部分内容,并为净化后的数据生成有效签名.可净化签名方案应满足不变性和透明性,其中不变性是指净化者只允许修改可净化范围内的数据而无法对范围之外的数据做任何修改.透明性是指除净化者外和签名者外其他任何人无法区分出签名是否执行净化操作.2005 年,Ateniese 等人[18]利用变色龙哈希函数提出一种可净化签名方案并在随机模型下证明了方案的安全性,提出的方案具有不变性和透明性.2009 年,Brzuska 等人[19]给出了可净化签名的安全性要求并定义了其安全模型.2011 年,Ming 等人[20]提出了基于身份的可净化签名方案并在标准模型下证明了方案的安全性.由于该方案在验证过

程中需要使用签名者身份作为公钥,无法提供匿名性. 为了实现签名者的匿名性,2013 年刘西蒙等人[21]提出属性基可净化签名方案,不仅可以保证签名者的匿名性而且实现了敏感信息的隐藏. 为了丰富访问结构的表达性,莫若等人[22-23]先后提出了具有树形访问结构的属性基可净化签名方案和具有灵活访问结构的属性基可净化签名方案,支持与门、或门和门限结构. 最近,Samelin 等人[24]提出了属性基可净化签名,具有完全可审计性功能. 为了解决属性基密码中签名用户身份追踪问题以及敏感消息泄露问题,李继国等人[25]提出一种可追踪的属性基净化签名方案,并在标准模型下证明了方案的安全性. Afia 等人[26]提出具有不可链接性的属性基可净化签名,使攻击者从外部无法区分两次会话中的签名是否源自同一签名者,保护了签名者隐私.

本文的主要工作包括以下四方面:

(1) 提出了具有强指定验证者的属性基可净化签名(Attribute-Based Sanitizable Signature Scheme with Strong Designated Verifier, ABSS-SDV)方案. 在标准模型下证明方案的安全性,其安全性可以规约到 BDH 困难问题.

(2) 通过指定验证者验证签名的合法性,使第三方无法判断签名是否由原始签名者生成,从而达到控制数字签名/版权恶意传播的目的.

(3) 提出的方案不仅保护了签名者隐私,而且还利用净化操作实现了敏感数据隐藏.

(4) 分析了方案的计算开销和通信开销,仿真实验表明提出的方案是可行的.

3　预备知识

本节介绍相关知识,包括双线性映射、拉格朗日插值、BDH 困难问题.

3.1　双线性映射

假设 G_1 和 G_2 是 p 阶乘法循环群,其中 p 是大素数. g 是 G_1 的生成元. 一个双映射 $e:G_1\times G_1\rightarrow G_2$ 具有下列性质.

(1) 双线性. 对任意 $a,b\in Z_n$,有 $e(g^a,g^b)=e(g,g)^{ab}$.

(2) 非退化性. $e(g,g)\neq 1$.

(3) 可计算性. 对所有 $u,v\in G_1$,存在多项式时间算法计算 $e(u,v)$.

3.2　拉格朗日插值

p 为大素数,集合 $S\subseteq Z_p$. 定义拉格朗日系数 $\Delta_{i,S}(x)=\prod_{j\in S,j\neq i}\frac{x-j}{i-j}$, $i\in Z_p$. 给定 Z_p 中的 d 个点 $(1,q_1),(2,q_2),\cdots,(d,q_d)$,若存在一个多项式 $q(x)$ 满足 $q(i)=q_i$,则 $d-1$ 次多项式 $q(x)$ 可以通过以下方式重构: $q(x)=\sum_{i\in S}q_i\Delta_{i,S}(x)$,其中 $|S|=d$.

3.3　BDH 问题和困难问题假设

令 G_1 是 p 阶的乘法循环群, p 是大素数. g 是 G_1 的生成元. BDH 问题为对任意的 $a,b,c\in Z_p^*$,已知 (g,g^a,g^b,g^c),计算 g^{abc}.

ε-BDH 困难问题假设. 若不存在多项式时间算法以不可忽略的概率 ε 解决 G_1 上的 BDH 困难问题,则称 ε-BDH 困难问题假设在群 G_1 上是成立的.

4　方案的形式化定义和安全模型

根据文献[13]中强指定验证者方案的形式化定义,本节给出具有强指定验证者的属性基可净化签名方案的形式化定义.

4.1　ABSS-SDV 方案的形式化定义

ABSS-SDV 方案包含六个算法:设置、密钥生成、签名、净化、验证、模拟,具体定义如下.

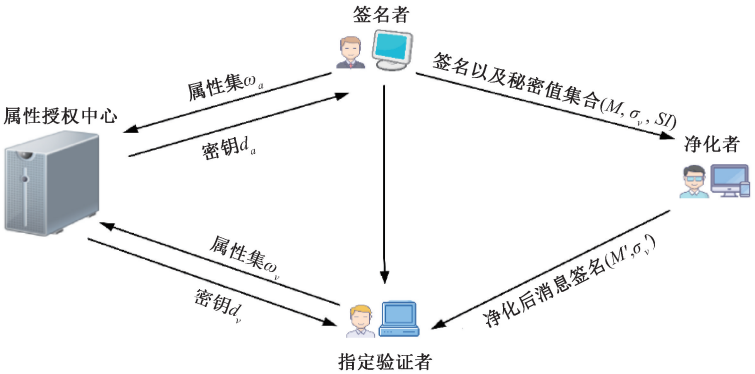

图 1　ABSS-SDV 方案框架

设置. 算法输入安全参数 λ，生成公共参数 $params$ 和主密钥 msk.

密钥生成. 算法输入公开参数 $params$，主密钥 msk，签名者属性集 ω_a /指定验证者属性集 ω_v，输出签名者密钥 d_{ω_a} /指定验证者密钥 d_{ω_v}.

签名. 算法输入公开参数 $params$，消息 M，签名者属性集 ω_a 与密钥 d_{ω_a}，净化者属性集 ω_b 以及指定验证者属性集 ω_v，输出签名 σ_v. 签名者同时产生秘密值集合 SI 发送给净化者.

净化. 签名者声明可净化的消息索引集合 $I_N \subseteq \{1,2,\cdots,n_m\}$. 净化者输入消息 M，公共参数 $params$，签名 σ_v，签名者属性集 ω_a，净化者属性集 ω_b，指定验证者属性集 ω_v 和秘密值集合 SI，执行净化操作.净化者输出净化消息 M' 和净化签名 σ'_v.

验证. 算法输入公开参数 $params$，净化消息和签名（M',σ'_v），指定验证者密钥 d_{ω_v}，签名者属性集 ω_a，指定验证者属性集 ω_v 以及净化者属性集 ω_b. 若 σ'_v 为 M' 有效签名，输出 accept；否则，输出 reject.

模拟. 验证者输入公开参数 $params$，签名者属性集 ω_a，净化者属性集 ω_b，指定验证者属性集 ω_v，净化消息 M' 和指定验证者密钥 d_{ω_v}，指定验证者输出一个模拟签名 $\bar{\sigma}_v$. 由于产生的模拟签名也能通过验证算法，因此即使指定验证者公开自己的密钥信息也无法使任何人相信签名是由原始签名者生成，因为指定验证者自己也能产生合法的签名.

ABSS-SDV 系统模型如图 1 所示，属性授权机构收到签名者和指定验证者发送的属性集 ω_a 和 ω_v 后，为签名者和指定验证者产生密钥 d_{ω_a} 以及 d_{ω_v}. 利用签名算法，签名者产生关于消息 M 的签名 σ_v，并计算一个秘密值集合 SI，将 (M,σ_v,SI) 发送给净化者. 净化者对可净化范围内的敏感数据进行修改，并重新生成关于净化后消息 M' 的签名 σ'_v. 净化者将净化签名 (M',σ'_v) 发送给指定验证者，指定验证者利用自己的密钥 d_{ω_v} 执行验证算法判断签名是否有效. 若有效，则输出 accept；否则输出 reject. 此外，指定验证者还可以模拟一个有效签名 $\bar{\sigma}_v$.

4.2 安全模型

4.2.1 不可伪造性

ABSS-SDV 方案的不可伪造性可以通过敌手 A 和挑战者 B 之间的交互游戏刻画. 基于文献[17]的安全模型，重新定义方案的不可伪造性游戏.

设置. 挑战者 B 运行设置算法，生成公共参数 $params$ 和主密钥 msk，将公开参数 $params$ 发送给敌手，自己保存主密钥 msk.

询问. A 可以自适应地执行密钥生成询问、签名询问、验证询问以及模拟询问. 具体询问过程如下.

密钥生成询问. A 自适应地向 B 询问签名者属性集 ω_a 对应的密钥 d_{ω_a}. B 执行密钥生成算法产生密钥并发送给 A. 同理，A 能够以相同的方式询问并获得指定验证者属性集 ω_v 对应的密钥 d_{ω_v}.

签名询问. A 自适应地选择签名者属性集 ω_a、净化者属性集 ω_b 以及指定验证者属性集 ω_v，通过密钥生成算法生成签名者私钥 d_{ω_a}. B 利用签名者密钥、签名者的属性集 ω_a，净化者的属性集 ω_b，指定验证者属性集 ω_v 以及消息 M，通过签名算法生成签名 σ_v 并发送给 A.

验证询问. A 可以询问消息签名对 (M,σ_v) 是否有效. 若是有效签名，B 返回 accept. 否则，返回 reject.

模拟询问. A 自适应地选择签名者属性集 ω_a、净化者属性集 ω_b 以及指定验证者属性集 ω_v. B 通过模拟签名算法生成消息 M 的模拟签名 $\bar{\sigma}_v$ 并发送给 A.

伪造. A 输出关于消息 M^*、签名者属性集 ω_a^*、指定验证者属性集 ω_v^* 以及净化者属性集 ω_b^* 的签名 σ^*. 若满足下列条件，则 A 赢得不可伪造游戏，

(1) 没有对 ω_a^* 以及 ω_v^* 进行密钥询问；

(2) 没有对 M^*,ω_a^* 以及 ω_v^* 进行签名询问；

(3) 将 $M^*,\omega_a^*,\omega_v^*$ 以及 σ^* 输入验证算法，算法输出 accept.

定义 1. 如果任意概率多项式时间 t 的敌手进行至多 q_k 次密钥询问，q_s 次签名询问，q_{ver} 次验证询问以及 q_{sim} 次模拟询问，以不超过 ε 的优势赢得上述不可伪造游戏，则 ABSS-SDV 方案是 $(t,q_k,q_s,q_{ver},q_{sim},\varepsilon)$- 不可伪造的.

4.2.2 不变性

ABSS-SDV 方案的不变性要求净化者只能对允许净化范围内的消息进行修改，无法对净化范围之外的消息进行任何操作. ABSS-SDV 的不变性可以通过敌手 A 和挑战者 B 的交互游戏证明.

初始化. A 将挑战索引集合 I_N^* 和策略 (d_a^*,S_a^*) 发送给 B，I_N^* 表示净化者可以执行净化操作的消息索引集合.

设置. B 执行该算法产生公开参数 $params$ 和

主密钥 msk,将公开参数 $params$ 发送给 A,自己保留主密钥 msk.

询问. A 自适应地进行有限次密钥生成询问和签名询问.在签名询问中,B 将秘密值集合 SI 发送给 A.

伪造. A 输出关于消息 $M^*=(m_1^*,m_2^*,\cdots,m_n^*)$ 和策略 (d_a^*,S_a^*) 的签名 σ^*,满足

(1) σ^* 是一个有效签名.

(2) 没有对 ω_a^* 进行密钥询问.

(3) 对于任何 $j\in\{1,2,\cdots,q_s\}$,存在 $i\notin I_N^*$ 使得 $m_{j,i}\neq m_i^*$.

定义 2. 如果任意概率多项式时间 t 的敌手 A 进行至多 q_k 次密钥询问和至多 q_s 次签名询问,最终赢得不变性游戏的概率 ε 是可忽略的,则 ABSS-SDV 方案具有 ε-不变性.

5　方案构造

为了方便阅读,表 1 给出方案构造中的主要参数及其意义.

表 1　主要参数对照表

参数	参数含义	参数	参数含义
Υ	访问策略	e	双线性映射
d_k	门限值	$params$	公共参数
ω_k	属性集	M	消息
Z_p	模 p 剩余类	d_{ω_k}	属性密钥
Z_p^*	模 p 非零剩余类	Ω,Ω_a	缺省属性集
G_1,G_2	乘法循环群	S_k^*	授权属性集
$Q_k(x)$	多项式	$q_k(x)$	多项式
SI	秘密值集	m_i	消息第 i 位
I_N	可净化索引集	σ_v,σ'_v	签名/净化签名

方案使用门限访问策略 $\Upsilon_{d_k,S_k^*}(\omega_k)$,为简便表述,令 $S_k^*\subseteq Z_p,\omega_k\subseteq Z_p,k\in\{a,b\}$,其中 $d_k\in Z_p^*$. 定义如下,若 $|\omega_k\cap S_k^*|\geqslant d_k$,则 $\Upsilon_{d_a,S_a^*}(\omega_a)=$ True;否则为 False.

下面给出方案的具体构造.ABSS-SDV 方案包含六个算法:设置、密钥生成、签名、净化、验证和模拟.

设置. 属性授权机构执行以下步骤. 选择两个 p 阶乘法循环群 G_1 和 G_2,其中 p 为大素数. G_1 和 G_2 之间存在双线性映射 $e:G_1\times G_1\to G_2$. 设置签名者需要满足的访问策略为 $\Upsilon_{d_a,S_a^*}(\cdot)$,指定验证者需要满足的访问策略为 $\Upsilon_{d_v,S_v^*}(\cdot)$,设置一个缺省属性集 $\Omega\subseteq Z_p$. 令 g 为 G_1 的一个生成元,随机选择 $\alpha\in Z_p^*$. 计算 $g_1=g^\alpha$. 随机选取 $g_2\in G_1$ 和长度为 $n+d-1$ 的向量 $\boldsymbol{H}=(h_1,h_2,\cdots,h_{n+d-1})$,其中 $h_i\in G_1$,$1\leqslant i\leqslant n+d-1$,其中 $d=\max(d_a,d_v)$,n 表示消息的长度. 随机选取 $u'\in G_1$ 和集合 $U=\{u_1,u_2,\cdots,u_n\}$,其中 $u_i\in G_1,1\leqslant i\leqslant n$. 随机选取 d_a-1 阶多项式 $Q_a(x)$,d_v-1 阶多项式 $Q_v(x)$,满足 $Q_a(0)=Q_v(0)=1$. $params=(G_1,G_2,e,g,g_1,g_2,u',\boldsymbol{H},\Omega,U,Q_a(x),Q_v(x))$ 为公开参数,$msk=g^\alpha$ 为主密钥.

密钥生成. 令 $\omega_a\subseteq Z_p$ 为签名者属性集,$\omega_v\subseteq Z_p$ 表示指定验证者属性集,属性授权机构随机选取 $\beta_{sv}\in Z_p^*$,计算 $e(g_1,g_2)^{\beta_{sv}}=Y$. 随机选取 d_a-1 阶多项式 $q_a(x)$,d_v-1 阶多项式 $q_v(x)$,满足 $q_a(0)=q_v(0)=\beta_{sv}$. 对 $i\in\omega_a$,随机选取 $r_i\in Z_p$,计算签名者密钥 $d_{\omega_a}=(d_{\omega_a,1},d_{\omega_a,2})$,其中 $d_{\omega_a,1}=g_2^{aq_a(i)}(g_2h_i)^{r_i}$;$d_{\omega_a,2}=g^{r_i}$. 同理,对 $j\in\omega_v$,随机选取 $r_j\in Z_p$,计算指定验证者密钥 $d_{\omega_v}=(d_{\omega_v,1},d_{\omega_v,2})$,其中 $d_{\omega_v,1}=g_2^{aq_v(j)}(g_2h_j)^{r_j}$;$d_{\omega_v,2}=g^{r_j}$.

签名. 输入签名者、净化者以及指定验证者属性集 $\omega_a,\omega_b,\omega_v$,消息 $M=(m_1m_2\cdots m_n)$,其中 $m_i\in\{0,1\}$,$i\in\{1,2,\cdots,n\}$,$n=|M|$. 签名者随机选取 $\omega_a^*\subseteq\omega_a$ 满足 $|\omega_a^*|\geqslant d_a$,随机选取 $\Omega_a\subseteq\Omega$ 满足 $\omega_a^*\cap\Omega_a=\phi$. 随机选取 $r_{a,i},r_{v,j},r_{b,k},r_s,r'_{a,i},r'_{b,k},r'_{v,j},r'_s\in Z_p$,其中 $i\in\omega_a,j\in\omega_v,k\in\omega_b$,计算 $\sigma_v=(\sigma_{v0},\sigma_{v1},\sigma_{v2},\sigma_{v3},\sigma_{v4})$. 通过以下步骤计算.

$$y_0=\Big[\prod_{k\in\omega_b}(g_2h_i)^{r_{b,k}}\Big]\Big[\prod_{j\in\omega_v}(g_2h_j)^{r_{v,j}}\Big]\Big[\prod_{i\in\omega_a^*}d_{\omega_a,1}^{\triangle_{i,S_a^*}^{(0)}}\Big]\cdot\Big[\prod_{i\in\omega_a^*\cup\Omega_a}(g_2h_i)^{r_{a,i}}\Big]\Big(u'\prod_{j=1}^{n}u_j^{m_j}\Big)^{r_s}$$

$$y_{1,i}=\begin{cases}d_{\omega_a,2}^{\triangle_{i,S_a^*}^{(0)}}g^{r_{a,i}},i\in\omega_a^*\\ g^{r_{a,i}},i\in\Omega_a\end{cases};$$

$y_{2,k}=g^{r_{b,k}},k\in\omega_b$;$y_{3,j}=g^{r_{v,j}},j\in\omega_v$;$y_4=g^{r_s}$.

$$\sigma_{v0}=[(y_0)^{Q_v(j)}]\Big[\prod_{k\in\omega_b}(g_2h_k)^{r'_{b,k}}\Big]\Big[\prod_{i\in\omega_a^*\cup\Omega_a}(g_2h_i)^{r'_{a,i}}\Big]\cdot\Big[\prod_{j\in\omega_v}(g_2h_j)^{r'_{v,j}}\Big]\Big(u'\prod_{j=1}^{n}u_j^{m_j}\Big)^{r'_s}$$

$$\sigma_{v1}=\{(y_{1,i})^{Q_v(j)}g^{r'_{a,i}}\mid i\in\omega_a^*\cup\Omega_a,j\in\omega_v\};$$

$$\sigma_{v2}=\{(y_{2,k})^{Q_v(j)}g^{r'_{b,k}}\mid k\in\omega_b,j\in\omega_v\};$$

$$\sigma_{v3}=\{(y_{3,j})^{Q_v(j)}g^{r'_{v,j}}\mid j\in\omega_v\};$$

$$\sigma_{v4}=\{(y_4)^{Q_v(j)}g^{r'_s}\mid j\in\omega_v\}.$$

同时，签名者计算秘密值 $SI_i = u_i^{r_s}$，其中 $i \in I_N$. 令 $SI = \{SI_1, SI_2, \cdots, SI_{|I_N|}\}$ 表示秘密值集合，$I_N = \{1,2,\cdots,N\}$ 表示签名者允许净化的消息索引集合，其中 $1 \leqslant N \leqslant n$.

净化. 净化者获得签名 $\sigma_v = (\sigma_{v0}, \sigma_{v1}, \sigma_{v2}, \sigma_{v3}, \sigma_{v4})$ 和秘密值集合 SI. 净化者设置需要净化的消息索引集 $I \subseteq I_N$. 令 $I_1 = \{i \in I : m_i = 0, m'_i = 1\}$，$I_2 = \{i \in I : m_i = 1, m'_i = 0\}$. 净化者随机选取 $r''_{a,i}$，$r''_{b,k}, r''_{v,j}, r''_s \in Z_p$，其中 $i \in \omega_a, j \in \omega_v, k \in \omega_b$，计算

$$\sigma'_{v0} = \sigma_{v0} \frac{\prod_{i \in I_1} SI_i}{\prod_{i \in I_2} SI_i} \left(u' \prod_{j=1}^{n} u_j^{m'_j}\right)^{r''_s} \left[\prod_{i \in \omega_a^* \cup \Omega_a} (g_2 h_i)^{r''_{a,i}}\right] \cdot \left[\prod_{j \in \omega_v} (g_2 h_i)^{r''_{v,j}}\right] \left[\prod_{k \in \omega_b} (g_2 h_k)^{r''_{b,k}}\right];$$

$$\sigma'_{v1} = \sigma_{v1} g^{r''_{a,i}} = \{(y_{1,i})^{Q_v(j)} g^{r'_{a,i} + r''_{a,i}} \mid i \in \omega_a^* \cup \Omega_a, j \in \omega_v\}; \sigma'_{v2} = \sigma_{v2} g^{r''_{b,k}} = \{(y_{2,k})^{Q_v(j)} g^{r'_{b,k} + r''_{b,k}} \mid k \in \omega_b, j \in \omega_v\}; \sigma'_{v3} = \sigma_{v3} g^{r''_{v,j}} = \{(y_{3,j})^{Q_v(j)} g^{r'_{v,j} + r''_{v,j}} \mid j \in \omega_v\}; \sigma'_{v4} = \sigma_{v4} g^{r''_s} = \{(y_4)^{Q_v(j)} g^{r'_s + r''_s} \mid j \in \omega_v\}.$$ 净化后的签名为 $\sigma'_v = \{\sigma'_{v0}, \sigma'_{v1}, \sigma'_{v2}, \sigma'_{v3}, \sigma'_{v4}\}$.

验证. 给定签名 σ'_v，指定验证者通过验证以下等式是否成立判断签名是否有效.

$$\prod_{i \in \omega_a^* \cup \Omega'_a} \prod_{j \in \omega_v} e(d_{\omega_v,1}^{\triangle_{j,S_v^*}^{(0)} Q_a(i)}, g)^{\triangle_{i,S_a^*}^{(0)}} \cdot \prod_{j \in \omega_v} e(\sigma'_{v0}, g))^{\triangle_{j,S_v^*}^{(0)}} \cdot \prod_{j \in \omega_v} \left\{ \prod_{i \in \omega_a^* \cup \Omega'_a} e(g_2 h_i, \sigma'_{v1}[i]) \prod_{j \in \omega_v} e(\sigma'_{v3}[j], g_2 h_j) \prod_{k \in \omega_b} e(g_2 h_k, \sigma'_{v2}[k]) \prod_{k \in \omega_b} e(u' \prod_{j=1}^{n} u_j^{m'_j}, \sigma'_{v4}[j]) \right\}^{-\triangle_{j,S_v^*}^{(0)}} \cdot \prod_{i \in \omega_a^* \cup \Omega_a} (e((g_2 h_i)^{Q_a(i)}, d_{\omega_v,2}))^{-\triangle_{i,S_a^*}^{(0)} \triangle_{j,S_v^*}^{(0)}}$$

$$= e(g_1, g_2)^{\beta_{sv}} e(g_1, g_2)^{\beta_{sv}} = Y^2.$$

模拟. 给定公开参数 $params$、签名者属性集 ω_a、净化者属性集 ω_b、验证者属性集 ω_v 以及净化后消息 M'，指定验证者随机选取 $\bar{r}_{a,i}, \bar{r}_{b,k}, \bar{r}_{v,j}, \bar{r}_s, \bar{r}'_{a,i}, \bar{r}'_{b,k}, \bar{r}'_{v,j}, \bar{r}'_s \in Z_p$，并计算

$$\bar{\sigma}_{v0} = [(\bar{y}_3[j])^{Q_a(i)}] \left[\prod_{j \in \omega_v} (g_2 h_j)^{\bar{r}'_{v,j}}\right] \left[\prod_{k \in \omega_b} (g_2 h_k)^{\bar{r}'_{b,k}}\right] \cdot \left[\prod_{i \in \omega_a^* \cup \Omega_a} (g_2 h_i)^{\bar{r}'_{a,i}}\right] (u' \prod_{j=1}^{n} u_j^{m'_j})^{\bar{r}'_s};$$

$$\bar{\sigma}_{v1} = \{(\bar{y}_{1,i})^{Q_a(i)} g^{\bar{r}'_{a,i}} \mid i \in \omega_a^* \cup \Omega_a\};$$

$$\bar{\sigma}_{v2} = \{(\bar{y}_{2,k})^{Q_a(i)} g^{\bar{r}'_{b,k}} \mid k \in \omega_b, i \in \omega_a^* \cup \Omega_a\};$$

$$\bar{\sigma}_{v3} = \{(\bar{y}_{3,j})^{Q_a(i)} g^{\bar{r}'_{v,j}} \mid j \in \omega_v, i \in \omega_a^* \cup \Omega_a\};$$

$$\bar{\sigma}_{v4} = \{(\bar{y}_4)^{Q_a(i)} g^{\bar{r}'_s} \mid i \in \omega_a^* \cup \Omega_a\}.$$

其中，$\bar{y}_{1,i} = g^{\bar{r}_{a,i}}, i \in \omega_a^* \cup \Omega'_a$；$\bar{y}_{2,k} = g^{\bar{r}_{b,k}}, k \in \omega_b$；$\bar{y}_{3,j} = d_{v,2}^{\triangle_{j,S_v^*}^{(0)}} g^{\bar{r}_{v,j}}, j \in \omega_v$；$\bar{y}_4 = g^{\bar{r}_s}$.

$\bar{\sigma}_v = (\bar{\sigma}_{v0}, \bar{\sigma}_{v1}, \bar{\sigma}_{v2}, \bar{\sigma}_{v3}, \bar{\sigma}_{v4})$ 为指定验证者模拟签名. 可知指定验证者模拟的签名 $\bar{\sigma}_v$ 和原始签名者签名 σ_v 具有相同的分布.

6 正确性和安全性分析

6.1 正确性分析

通过计算以下等式成立证明 ABSS-SDV 方案满足正确性要求.

$$\prod_{i \in \omega_a^* \cup \Omega'_a} \prod_{j \in \omega_v} e(d_{\omega_v,1}^{\triangle_{j,S_v^*}^{(0)} Q_a(i)}, g)^{\triangle_{i,S_a^*}^{(0)}} = e(g_2^{\alpha\beta_{sv}}, g) \prod_{j \in \omega_v} e((g_2 h_j)^{r_j \triangle_{j,S_v^*}^{(0)}}, g);$$

$$\prod_{j \in \omega_v} (e(\sigma'_{v0}, g))^{\triangle_{j,S_v^*}^{(0)}} = \prod_{i \in \omega_a^* \cup \Omega'_a} e(g, (g_2 h_i)^{r_i \triangle_{i,S_a^*}^{(0)}}) e((g_2^{\alpha\beta_{sv}}, g) \prod_{i \in \omega_a^* \cup \Omega'_a} (e(g, (g_2 h_i)^{r_{a,i} + (r'_{a,i} + r''_{a,i}) \triangle_{j,S_v^*}^{(0)}}) \prod_{k \in \omega_b} e(g, (g_2 h_k)^{r_{b,k} + (r'_{b,k} + r''_{b,k}) \triangle_{j,S_v^*}^{(0)}}) \prod_{j \in \omega_v} e(g, g_2 \cdot h_j)^{r_{v,j} + (r'_{v,j} + r''_{v,j}) \triangle_{j,S_v^*}^{(0)}} (u' \prod_{j=1}^{n} (u_j^{m'_j}))^{r_s + (r'_s + r''_s) \triangle_{j,S_v^*}^{(0)}};$$

$$\prod_{j \in \omega_v} \left\{ \prod_{i \in \omega_a^* \cup \Omega'_a} e(g_2 h_i, \sigma'_{v1}[i]) \prod_{j \in \omega_v} e(\sigma'_{v3}[j], g_2 h_j) \cdot \prod_{k \in \omega_b} e(g_2 h_k, \sigma'_{v2}[k]) e\left(u' \prod_{j=1}^{n} u_j^{m'_j}, \sigma'_{v4}[j]\right) \right\}^{-\triangle_{i,S_v^*}^{(0)}}$$

$$= \prod_{i \in \omega_a^* \cup \Omega'_a} e(g, (g_2 h_i)^{r_i \triangle_{i,S_a^*}^{(0)}})^{-1} \cdot \prod_{i \in \omega_a^* \cup \Omega'_a} (e(g, (g_2 h_i)^{-r_{a,i} - (r'_{a,i} + r''_{a,i}) \triangle_{j,S_v^*}^{(0)}}) \cdot \prod_{k \in \omega_b} e(g, (g_2 h_k))^{-r_{b,k} - (r'_{b,k} + r''_{b,k}) \triangle_{j,S_v^*}^{(0)}} \cdot \prod_{j \in \omega_v} e(g, g_2 h_j)^{-r_{v,j} - (r'_{v,j} + r''_{v,j}) \triangle_{j,S_v^*}^{(0)}} \cdot \left(u' \prod_{j=1}^{n} (u_j^{m'_j})\right)^{-(r_s + (r'_s + r''_s) \triangle_{j,S_v^*}^{(0)})};$$

$$\prod_{j \in \omega_v} \prod_{i \in \omega_a^* \cup \Omega_a} (e((gh_j)^{Q_a(i)}, d_{v,2}))^{-\triangle_{i,S_a^*}^{(0)}} = \prod_{j \in \omega_v} e((g_2 h_j)^{r_j \triangle_{j,S_v^*}^{(0)}}, g);$$ 化简后将上述多项式相乘可得 $e(g_1, g_2)^{\beta_{sv}} e(g_1, g_2)^{\beta_{sv}} = Y^2$. 因此提出

的方案满足正确性要求.

6.2　安全性分析

下面将通过两个定理给出方案的安全性证明.

6.2.1　不可伪造性

定理 1. 若存在概率多项式时间的敌手在经过 q_k 次密钥生成询问，q_s 次签名询问，q_{sim} 次模拟询问，q_{ver} 次验证询问后，能够以ϵ的优势赢得不可伪造性游戏，则存在一个概率多项式时间算法以 ε 的概率解决 BDH 困难问题，其中 $\varepsilon \geqslant \frac{\epsilon}{4(n+1)(q_s+q_{sim}+q_{ver})}$.

证明. 假设存在一个 $(\epsilon,q_k,q_s,q_{ds},q_{sim},q_{dv})$－敌手 A 能够多项式时间内攻破提出的方案，那么就存在一个多项式时间算法 B 解决 BDH 困难问题. 通过以下方式模拟敌手 A 和算法 B 之间的交互.

设置. 给定一个 BDH 困难问题实例 (g,g^a,g^b,g^c)，其中 $a,b,c \in Z_p$. B 通过以下方式生成公开参数. 令 $g_1=g^a$，$g_2=g^b$. 选取一个随机值 $k \in \{0,1,\cdots,q\}$，随机选取 $x',x_1,x_2,\cdots,x_q \in \{0,1,\cdots,2l-1\}$，其中 $q=\max(|\omega_a|,|\omega_v|)$，$l=2(q_s+q_k)$，$|\omega_a|$ 表示签名者属性集中属性的数量，$|\omega_v|$ 表示指定验证者属性集中属性的数量，max() 表示取最大值函数. 选取两个 n 阶多项式 $f(x)$ 和 $u(x)$，当且仅当 $x \in \alpha$ 时，$u(x)$ 满足，$\forall x, u(x)=-x^n$. 令 $h_i=g_2^{u(i)+i^{n-1}}g^{f(i)}$，故 $g_2h_i=g_2^{u(i)+i^n}g^{f(i)}$. 假设 A 至多进行 q_k 次密钥生成询问，q_s 次签名询问，q_{sim} 次模拟签名询问以及 q_{ver} 次验证询问. 令 $l_m=2(q_s+q_{sim}+q_{ver})$，随机选取 $k_m \in Z_p$，满足 $0 \leqslant k_m \leqslant n$. B 选取随机 $z',z_1,z_2,\cdots,z_p \in Z_p$，令 $u'=g_2^{x'-l_mk_m}g^{z'}$，$u_k=g_2^{x_k}g^{z_k}$，其中 $1 \leqslant k \leqslant q$. 定义两个函数 $F(M)$ 和 $J(M)$，其中 $F(M)=x'-l_mk_m-\sum_j x_jm_j$，$J(M)=z'+\sum_j z_jm_j$. 因此有以下等式成立：$u'\prod_{j=1}^{n}u_j^{m_j}=g_2^{F(M)}g^{J(M)}$. 设置主密钥为 $g_2^a=g_2^a=g^{ab}$.

询问. 询问阶段包括密钥生成询问、签名询问、验证询问以及模拟询问. B 通过以下方式产生应答.

密钥生成询问. B 定义三个属性集 Γ,Γ',S，使得 $\Gamma=(w_a \cap S_a^*)\cup\Omega'$，$\Gamma \subseteq \Gamma' \subseteq S_a^*$，其中 $|\Gamma'|=d_a-1$. 令 $S=\Gamma' \cup \{0\}$. 随机选取 $\lambda_i,r'_i \in Z_p$，并定义一个 d_a-1 次多项式 $q_a(x)$，满足 $q_a(0)=c$，$q_a(i)=\lambda_i$. 当 $u(i)+i^n \neq 0$ 时，B 通过以下方式生成 A 询问的密钥

$$d_{\omega_a,1}=\Big[\Big(g_1^{-\frac{f(i)}{u(i)+i^n}}(g_2^{u(i)+i^n}g^{f(i)})^{r'_i-\frac{\alpha}{u(i)+i^n}}\Big)\cdot\prod_{i\in\Gamma'}g_2^{\lambda_i}\Big]^{\triangle_{i,S_a^*}(0)}$$

$$d_{\omega_a,2}=\Big(g^{r'_i-\frac{\alpha}{u(i)+i^n}}\Big)^{\triangle_{i,S_a^*}(0)}=\Big(g_1^{-\frac{1}{u(i)+i^n}}g^{r'_i}\Big)^{\triangle_{i,S_a^*}(0)}.$$

此时，令 $r_i=\Big(r'_i-\frac{\alpha}{u(i)+i^n}\Big)^{\triangle_{i,S_a^*}(0)}$，有

$$d_{a,1}=\Big(g_2^{\alpha}(g_2^{u(i)+i^n}g^{f(i)})^{r'_i-\frac{\alpha}{u(i)+i^n}}\Big)^{\triangle_{i,S_a^*}(0)}\cdot\Big(\prod_{k\in\Gamma'}g_2^{\lambda_i\triangle_{i,S_a^*}(0)}\Big)=g_2^{aq_a(i)}(g_2h_i)^{r_i};$$

$$d_{\omega_a,2}=\Big(g^{r'_i-\frac{\alpha}{u(i)+i^n}}\Big)^{\triangle_{i,S_a^*}(0)}=\Big(g_1^{-\frac{1}{u(i)+i^n}}\cdot g^{r'_i}\Big)^{\triangle_{i,S_a^*}(0)}.$$

同样可以生成指定验证者的密钥 $d_{\omega_v}=(d_{\omega_v,1},d_{\omega_v,2})$.

签名询问. A 询问关于属性集 ω_a 和消息 M 的签名，若 $F(M)=0$，则模拟终止. 若 $F(M)\neq 0$，当 $u(i)+i^n \neq 0(\mathrm{mod}\,p)$ 时，B 通过签名算法生成 M 的有效签名；当 $u(i)+i^n=0(\mathrm{mod}\,p)$ 时，B 随机选择一个集合 $\omega'_a \subseteq \omega_a^*$，满足 $|\omega'_a|=d_a-1$. 令 $g^{q_a(i)}=g^{\lambda_i}=\Big(\prod_{i=1}^{d_a-1}g^{\lambda'_i\Delta_{i,\omega_a^*}(i)}\Big)g^{a\Delta_{i,\omega_a^*}(0)}$，其中 $i \in \omega_a^*-\omega'_a$. B 随机选取 $r_{a,i},r_{v,j},r_{b,k},r_s,r'_{a,i},r'_{b,k},r'_{v,j},r''_s \in Z_p^*$，其中 $i \in w_a, j \in \omega_v, k \in \omega_b$，并进行以下计算：

$$\sigma_{v0}=g_1^{-q_a(i)Q_v(j)\frac{J(M)}{F(M)}}(g_2^{F(M)}g^{J(M)})^{r_sQ_v(j)+r'_s}\cdot\prod_{i\in\omega_a^*\cup\Omega'_a}(gh_i)^{r_{a,i}Q_v(j)+r'_{a,i}}\prod_{j\in\omega_v}(g_2h_j)^{r_{v,j}Q_v(j)+r'_{v,j}}\cdot\prod_{i\in\omega_a^*\cup\Omega'_a}((gh_i)^{r_{a,i}})^{\Delta_{i,S_a^*}(0)Q_v(j)}\prod_{k\in\omega_b}(gh_k)^{r_{b,k}Q_v(j)+r'_{b,k}}$$

$$=g_2^{aq_a(i)Q_v(j)}\prod_{i\in\omega_a^*\cdot\Omega_a}((gh_i)^{r_{a,i}})^{\Delta_{i,S_a^*}(0)Q_v(j)}\cdot\prod_{i\in\omega_a^*\cup\Omega'_a}(gh_i)^{r_{a,i}Q_v(j)+r'_{a,i}}\prod_{j\in\omega_v}(g_2h_j)^{r_{v,j}Q_v(j)+r'_{v,j}}\cdot(g_2^{F(M)}g^{J(M)})^{r_sQ_v(j)+r'_s-aq_a(i)Q_v(j)/F(m)}\cdot\prod_{k\in\omega_b}(gh_k)^{r_{b,k}Q_v(j)+r'_{b,k}}$$

令 $r'_s=r''_s-\alpha q_a(i)Q_v(j)/F(M)$，则有：

$$\sigma_{v0}=g_2^{aq_a(i)Q_v(j)}(u'\prod_{j=1}^{n}u_j^{m_j})^{r'_s+r_sQ_v(j)}$$

$$\cdot \prod_{i\in\omega_a^*\cup\Omega_a'}(g_2h_i)^{r_{a,i}Q_v(j)+r'_{a,i}}\prod_{j\in\omega_v}(g_2h_j)^{r_{v,j}Q_v(j)+r'_{v,j}}$$

$$\cdot \prod_{i\in\omega_a^*\cup\Omega_a'}((gh_i)^{r_{a,i}})^{\Delta_{i,S_a^*}^{(0)}Q_v(j)}\prod_{k\in\omega_b}(g_2h_k)^{r_{b,k}Q_v(j)+r'_{b,k}}$$

$$=(y_0)^{Q_v(j)}\Big[\prod_{i\in\omega_a^*\cup\Omega_a'}(g_2h_i)^{r'_{a,i}}\Big]\prod_{k\in\omega_b}(g_2h_k)^{r'_{b,k}}$$

$$\cdot \prod_{j\in\omega_v}(g_2h_j)^{r'_{v,j}}\Big(u'\prod_{j=1}^{n}u_j^{m_j}\Big)^{r'_s};$$

$$\sigma_{v1}=\{(y_{1,i})^{Q_v(j)}g^{r'_{a,i}}\mid i\in\omega_a^*\cup\Omega_a,j\in\omega_v\};$$

$$\sigma_{v2}=\{(y_{2,k})^{Q_v(j)}g^{r'_{b,k}}\mid k\in\omega_b,j\in\omega_v\};$$

$$\sigma_{v3}=\{(y_{3,j})^{Q_v(j)}g^{r'_{v,j}}\mid j\in\omega_v\};$$

$$\sigma_{v4}=\Big\{g^{r_sQ_v(j)-\frac{\alpha q_a(i)(i)Q_v(j)}{F(M)}}g^{r'_s}\mid j\in\omega_v\Big\}.$$ 因此,可知 $\sigma_v=(\sigma_{v0},\sigma_{v1},\sigma_{v2},\sigma_{v3},\sigma_{v4})$ 是一个有效签名.

验证询问. 给定消息签名对 (M,σ_v),若 $F(M)=0$,B 终止游戏;否则,A 可以进行验证询问. B 首先通过密钥生成算法计算指定验证者密钥 d_v,然后通过验证算法验证签名. 若签名有效,返回 accept;否则,返回 reject.

模拟询问. A 对消息 M,签名者属性集 ω_a 和指定验证者属性集 ω_v 进行模拟签名询问. 若 $F(M)=0$,模拟终止. 若 $F(M)\neq 0$,当 $u(i)+i^n\neq 0(\mathrm{mod}\,p)$,B 可以通过模拟算法产生模拟签名;当 $u(i)+i^n=0(\mathrm{mod}\,p)$ 时,B 随机选取 $\bar{r}_{a,i},\bar{r}_{b,k},\bar{r}_{v,j},\bar{r}''_s\in Z_p$,计算

$$\bar{\sigma}_{v0}=g_1^{-q_v(j)\frac{J(M)}{F(M)}Q_a(i)}\prod_{j\in\omega_v}(g_2h_j)^{\bar{r}_{v,j}Q_a(i)+\bar{r}'_{v,j}}$$

$$\cdot\prod_{k\in\omega_b}(g_2h_k)^{\bar{r}_{b,k}Q_a(i)+\bar{r}'_{b,k}}(g_2^{F(M)}g^{J(M)})^{\bar{r}_sQ_a(i)+\bar{r}''_s}$$

$$\cdot\prod_{i\in\omega_a^*\cup\Omega'_a}(g_2h_i)^{\bar{r}_{a,i}Q_a(i)+\bar{r}'_{a,i}}$$

$$=g_2^{\alpha q_v(j)Q_a(i)}\prod_{i\in\omega_a^*\cup\Omega'_a}(g_2h_i)^{\bar{r}_{a,i}}\prod_{k\in\omega_b}(g_2h_k)^{\bar{r}_{b,k}}$$

$$\cdot(g_2^{F(M)}g^{J(M)})^{\bar{r}_sQ_a(i)+\bar{r}''_s-\alpha q_v(j)Q_a(i)/F(M)}\prod_{j\in\omega_v}(g_2h_j)^{\bar{r}_{v,j}}$$

令 $\bar{r}'_s=\bar{r}''_s-\alpha q_v(j)Q_a(i)/F(M)$,有

$$\bar{\sigma}_{v0}=g_2^{\alpha q_v(j)Q_a(i)}\prod_{i\in\omega_a^*\cup\Omega'_a}(g_2h_i)^{\bar{r}_{a,i}Q_a(i)+\bar{r}'_{a,i}}$$

$$\cdot\Big[\prod_{j\in\omega_v}(g_2h_j)^{\bar{r}_{v,j}Q_a(i)+\bar{r}'_{v,j}}\Big]\Big(u'\prod_{j=1}^{n}u_j^{m_j}\Big)^{\bar{r}_sQ_a(i)+\bar{r}'_s}$$

$$\cdot\prod_{k\in\omega_b}(g_2h_k)^{\bar{r}_{b,k}Q_a(i)+\bar{r}'_{b,k}};$$

$$\bar{\sigma}_{v1}=\{g^{\bar{r}_{a,i}Q_a(i)+\bar{r}'_{a,i}}\mid i\in\omega_a^*\cup\Omega_a,j\in\omega_v\};$$

$$\bar{\sigma}_{v2}=\{g^{\bar{r}_{b,k}Q_a(i)+\bar{r}'_{b,k}}\mid k\in\omega_b,j\in\omega_v\};$$

$$\bar{\sigma}_{v3}=\{g^{\bar{r}_{v,j}Q_a(i)+\bar{r}'_{v,j}}\mid j\in\omega_v\};$$

$$\bar{\sigma}_{v4}=\{g^{\bar{r}_sQ_a(i)+\bar{r}'_s}\mid j\in\omega_v\}.$$ 可知 $\bar{\sigma}_v=(\bar{\sigma}_{v0},\bar{\sigma}_{v1},\bar{\sigma}_{v2},\bar{\sigma}_{v3},\bar{\sigma}_{v4})$ 是一个有效的模拟签名.

伪造. 若模拟阶段 B 没有终止,那么 A 就能以 ϵ 的概率对属性 (ω_a^*,ω_v^*) 和消息 M^* 成功伪造一个有效签名 $\sigma_v^*=(\sigma_{v0}^*,\sigma_{v1}^*,\sigma_{v2}^*,\sigma_{v3}^*,\sigma_{v4}^*)$. 当 $F(M^*)\neq 0,u(i)+i^n\neq 0$ 以及 $u(j)+j^n\neq 0$ 时,B 计算

$$\sigma_{v0}^*=\prod_{j\in\omega_v^*}(\sigma_{v,0})^{\Delta_{j,S_v^*}^{(0)}}=g^{abc}\prod_{j\in\omega_v^*}\Big\{\prod_{j\in\omega_v^*}(g^{r_{v,i}Q_v(j)f(j)}$$

$$\cdot g^{r'_{v,i}}g^{J(M)(r'_s+r_sQ_v(j))})$$

$$\cdot\prod_{i\in\omega_a^*\cup\Omega'_a}(g^{r_{a,i}\Delta_{i,S_a^*}^{(0)}Q_v(j)f(i)})(g^{(r_{a,i}Q_v(j)+r'_{a,i})f(i)})$$

$$\cdot\prod_{k\in\omega_b^*}g^{(r'_{b,k}+r_{b,k}Q_v(j))f(k)}\Big\};$$

$$\sigma_{v1}^*=\{g^{r'_{a,i}+r_{a,i}\Delta_{i,S_a^*}^{(0)}Q_v(j)}\mid i\in\omega_a^*\cup\Omega_a,j\in\omega_v\};$$

$$\sigma_{v2}^*=\{g^{r'_{b,k}+r_{b,k}Q_v(j)}\mid k\in\omega_b,j\in\omega_v\};\sigma_{v3}^*=\{g^{r'_{v,j}+r_{v,j}Q_v(j)}\mid j\in\omega_v\};\sigma_{v4}^*=\{g^{r'_s+r_sQ_v(j)}\mid j\in\omega_v\}.$$

因此,B 计算

$$g^{abc}=\frac{1}{\prod_{j\in\omega_v^*}(\sigma_{v4,j}^*)^{J(M)}\prod_{j\in\omega_v^*}(\sigma_{v3,j}^*)^{f(j)}}$$

$$\cdot\frac{\sigma_{v0}^*}{\prod_{j\in\omega_v^*}\prod_{i\in\omega_a^*\cup\Omega'_a}(\sigma_{v1,i}^*)^{f(i)}\prod_{j\in\omega_v^*}\prod_{k\in\omega_b^*}(\sigma_{v2,k}^*)^{f(k)}}$$

6.2.2 概率分析

分析 B 在上述模拟过程中没有终止的概率,需要定义以下事件,

(1) $E_{1l}:F(M_i)\neq 0,l\in\{1,2,\cdots,q_s\}$;

(2) $E_{2k}:F(M_i)\neq 0,k\in\{1,2,\cdots,q_{sim}\}$;

(3) $E_3:F(M^*)=0$;

(4) $E_4:u(i^*)+(i^*)^n=0,u(j^*)+(j^*)^n=0$,

其中 $i\in\omega_a^*,j\in\omega_v^*$.

B 不发生终止的概率为

$$\Pr[\overline{abort}]\geqslant\Pr[E_{1i}\wedge E_{2i}\wedge E_3\wedge E_4]=\Pr[E_{1i}\wedge E_{2i}\wedge E_3]\cdot\Pr[E_4]$$

$$=\Pr[E_3](1-\Pr[E_{1i}\wedge E_{2i}\mid E_3)\times\Pr[E_4]\geqslant\Pr[E_3]$$

$$\cdot\Big(1-\sum_{i=1}^{q_s}\Pr[\overline{E_{1i}}\mid E_3]\Big)\Big(1-\sum_{i=1}^{q_{sim}}\Pr[\overline{E_{2i}}\mid E_3]\Big)\Pr[E_4]$$

$$=\frac{1}{l_m(n+1)}\cdot\Big(1-\frac{q_s+q_{sim}+q_{ver}}{l_m}\Big)$$

$$\geqslant\frac{\epsilon}{4(n+1)(q_s+q_{sim}+q_{ver})}$$,若 A 能够以 ϵ 的优势

成功伪造签名，那么 B 就能以 $\varepsilon \geqslant \frac{\epsilon}{4(n+1)(q_s+q_{sim}+q_{ver})}$ 的概率成功解决 BDH 困难问题.

6.2.3　不变性

定理 2. 若存在概率多项式时间的敌手能够以ϵ的优势赢得不变性游戏,则存在一个概率多项式时间的算法能够以ϵ'概率解决 BDH 困难问题. 其中存在常数 γ,满足$\epsilon \leqslant \gamma \epsilon'$.

假设给定可净化消息索引集合 $I_N \subseteq \{1,2,\cdots,n\}$,净化者获得秘密值集合 SI,此时除了可净化范围内的消息,净化者无法对该集合之外的数据进行修改,首先证明下列引理 1.

引理 1. 若存在任意多项式时间的敌手 A_1 能对 I_N 内 κ 位长的数据进行修改,其中 $1 \leqslant \kappa \leqslant n, n = |M|$. 并以 ε_{A_1} 的优势赢得不变性游戏,则存在一个多项式时间敌手 A 以 ε_A 的优势在不可伪造游戏中成功伪造一个 $(n-\kappa)$ 长消息的签名,其中 $\varepsilon_A \geqslant \varepsilon_{A_1}$.

证明. 假设存在一个多项式时间的敌手 A_1 能够以 ε_{A_1} 的优势对 I_N 中 κ 长度的消息进行不变性游戏,考虑一个随机的多项式时间敌手 A 可以对 $(n-\kappa)$ 长度的消息进行不可伪造游戏. 在下面的游戏中,本文将 A 模拟成挑战者与 A_1 进行交互. 在收到 A_1 的询问后,A 与不可伪造游戏中的算法 B 交互并将询问结果返回给 A_1,最后证明 A 能够以 $\varepsilon_A \geqslant \varepsilon_{A_1}$ 的优势成功赢得不可伪造性游戏,交互游戏如下.

设置. A_1 将可净化索引集合 I_N 发送给 A,其中 $I_N \subseteq \{1,2,\cdots,n\}$. 简化起见,令 $I_N = \{n-\kappa+1,\cdots,n\}$,其中 $|\kappa| = |I_N|$. B将公共参数 $params' = \{G_1, G_2, e, g, g_1, g_2, u', H, U_{n-\kappa}, \Omega, Q_a(x), Q_v(x)\}$ 发送给 A,其中 $U_{n-\kappa} = (u_1, u_2, \cdots, u_{n-\kappa})$. A 随机选取 $c_i \in Z_p$,计算 $u'_i = g^{c_i}, i \in \{n-\kappa+1,\cdots,n\}$. 令 $U = U_{n-\kappa} \cup U_{n-\kappa+1}$,其中 $U_{n-\kappa+1} = \{u_{n-\kappa+1}, \cdots, u_n\}$. A 将公开参数 $params = \{G_1, G_2, e, g, g_1, g_2, u', H, U, \Omega, Q_a(x), Q_v(x)\}$ 发送给 A_1.

询问. 在 $j = 1,2,\cdots,q_s$ 次的原始签名询问中,A 通过与 B 的交互回答 A_1 的询问. A_1 首先询问消息 $M_j = (m_{j,1} m_{j,2}, \cdots, m_{j,n})$ 的签名,此时 A 向 B 询问消息 $\bar{M}_j = (m_{j,1} m_{j,2}, \cdots, m_{j,n-\kappa})$ 的签名. B 将签名 $\sigma = (\sigma_{j,0}, \sigma_{j,1}, \sigma_{j,2}, \sigma_{j,3}, \sigma_{j,4})$ 发送给 A. A 计算 $\sigma'_{j,0} = \sigma_{j,0} \prod_{i=u_{n-\kappa+1}}^{n} \sigma_{j,1}^{c_i m_{j,i}}, \sigma'_{j,1} = \sigma_{j,1}, \sigma'_{j,2} = \sigma_{j,2}, \sigma'_{j,3} = \sigma_{j,3}, \sigma'_{j,4} = \sigma_{j,4}$,并将签名 $\sigma' = (\sigma'_{j,0}, \sigma'_{j,1}, \sigma'_{j,2}, \sigma'_{j,3}, \sigma'_{j,4})$ 以及秘密消息 $\{\sigma_{j,1}^{c_i m_{j,i}} \mid i = n-\kappa+1,\cdots,n\}$ 发送给 A_1.

伪造. 若 A_1 成功伪造消息 $M^{*\prime} = (m^{*\prime}_0 m^{*\prime}_1 \cdots m^{*\prime}_n)$ 的签名 $\sigma^{*\prime} = \{\sigma^{*\prime}_0, \sigma^{*\prime}_1, \sigma^{*\prime}_2, \sigma^{*\prime}_3, \sigma^{*\prime}_4\}$. 此时,$\forall j \in \{1,2,\cdots,q_s\}, \exists i \notin \{n-\kappa+1,\cdots,n\}$,有 $m_{j,i} \neq m^{*\prime}_i$. A 获得该签名后定义 $M^* = (m^*_0 m^*_1 \cdots m^*_n)$,当 $i \in \{1,2,\cdots,n-\kappa\}$ 时,$m^*_i = m^{*\prime}_i$. 计算 $\sigma^*_0 = \frac{\sigma^{*\prime}_0}{\prod_{i=u_{n-\kappa+1}}^{n} (\sigma^{*\prime}_1)^{c_i m^*_i}}, \sigma^*_1 = \sigma^{*\prime}_1, \sigma^*_2 = \sigma^{*\prime}_2, \sigma^*_3 = \sigma^{*\prime}_3, \sigma^*_4 = \sigma^{*\prime}_4$. 若 A_1 伪造的签名能通过验证算法,那么 A 计算生成的签名也可以通过验证. 因此,A 赢得不可伪造性游戏的优势 $\varepsilon_A \geqslant \varepsilon_{A_1}$,其中 ε_{A_1} 是 A_1 赢得不变性游戏的优势.

由定理 1 可知,在 ε-BDH 困难问题假设下敌手赢得不可伪造性游戏的优势是可忽略的. 通过证明引理 1 可知,在 ε-BDH 困难问题假设下,任何概率多项式时间敌手赢得不变性游戏的优势也是可忽略的. 综上所述,定理 2 得证.

7　方案分析

本文提出了可具有强指定验证者的属性基可净化签名方案. 本节将提出的方案与已有文献[4,13,17,21,26]比较,并分析方案优势. 文献[4]给出了标准模型下安全的属性基签名方案,提供了细粒度访问控制功能但无法保证签名者签名行为的隐私性,任何人都可以通过验证算法确定验证该签名为签名者所签订. Susilo 等[13]提出了基于身份的具有指定验证者签名方案,签名者通过指定验证者保护了自身签名行为隐私,但算法利用签名者的真实身份作为公钥,不具有细粒度访问控制功能. 文献[17]给出了具有指定验证者的属性基签名方案,利用一组属性代替真实身份,在指定验证者验证签名的同时也实现了细粒度访问控制功能,但没有解决签名消息中的数据脱敏问题. 文献[21]给出了属性基可净化方案,通过净化者对可净化范围内的消息进行修改从而实现数据脱敏,但没有考虑特定场景中需要保护签名者的签名行为隐私.

本文提出的 ABSS-SDV 方案不仅实现了签名者隐私保护和细粒度访问控制,同时也提供了敏感信息隐藏功能,将方案的安全性规约到 BDH 困难问题,并在标准模型下给出了方案的安全性证明. 方案对比如表 2 所示.

表 2 方案比较

方案	文献[4]	文献[13]	文献[17]	文献[21]	文献[26]	本方案
匿名性	√	×	√	√	√	√
可净化性	×	×	×	√	√	√
指定验证者	×	√	√	×	×	√
透明性	×	×	×	√	×	√
访问控制	√	×	√	√	√	√

8 性能分析

令 ω_a,ω_b,ω_v 分别表示签名者、净化者以及指定验证者属性数量，n 表示消息长度，I 表示需要净化消息索引集合. θ 表示访问策略中析取操作的次数. P 表示双线性对运算，E 表示指数运算. ABSS-SDV(本方案)与文献[17,26]方案通信开销比较如表 3 所示. 本方案与文献[17,26]方案计算开销比较如表 4 所示.

表 3 方案通信开销比较

方案	密钥	签名
文献[17]	$(2\lvert\omega_a\rvert+3)\lvert G_1\rvert$	$3k\lvert G_1\rvert+\theta\lvert Z_p\rvert$
文献[26]	$(2\lvert\omega_a\rvert+2)\lvert G_1\rvert+2\lvert Z_p\rvert$	$(2\lvert\omega_a\rvert+5)\lvert G_1\rvert$
本方案	$(2\lvert\omega_a\rvert)\lvert G_1\rvert$	$(\lvert\omega_a\rvert+\lvert\omega_b\rvert+\lvert\omega_v\rvert+2)\lvert G_1\rvert$

表 4 方案计算开销比较

方案	签名	净化	验证
文献[17]	$\lvert\omega_a\rvert$P+[3$\lvert\omega_a\rvert+n+k(\lvert\omega_a\rvert+1)$]E	——	5P+5E
文献[26]	[3$\lvert\omega_a\rvert$+3]E	[5$\lvert\omega_a\rvert$+5]E	[3$\lvert\omega_a\rvert$+6]P+4E
本方案	[8$\lvert\omega_v\rvert$+4($\lvert\omega_b\rvert+\lvert\omega_a\rvert$)+2n+4]E	[2($\lvert\omega_v\rvert+\lvert\omega_a\rvert+\lvert\omega_b\rvert$)+I+n+2]E	[5$\lvert\omega_v\rvert$+3$\lvert\omega_a\rvert+n$]E+[2($\lvert\omega_v\rvert+\lvert\omega_a\rvert+\lvert\omega_b\rvert+1$)]P

基于虚拟机 Ubuntu 18.4，在 Charm0.5 框架下实现了提出的方案. 在 Intel(R) Core(TM) i5-3230M CPU @2.60GHz，4GB RAM 性能计算环境下，利用 Charm 库中的超奇异椭圆曲线(SS512)测试方案. 实验中群 G_1 的阶 p 为 512bit 大素数. 在计算机上测试主要密码学操作开销，经过 1000 次测量取平均值后得到实验中计算双线对所需时间为 12.58ms，在群 G_1 和 G_2 中执行指数运算所需时间分别为 5.03ms 和 4.96ms. 本方案与文献[17,26]方案的实验结果如图 2～5 所示. 实验结果表明本方案及其比较方案[17,26]的运行时间随着签名者和指定验证者属性数量的线性增长. 图 2 表明在签名产生阶段文献[26]中方案具有一定优势，本方案和文献[17]中方案的运行时间基本相当. 从图 3 可以看出，由于文献[17]中方案没有净化功能，所以验证算法的性能明显优于本方案和文献[26]中方案. 图 4 表明当属性数量较少时文献[26]中方案的净化算法略有优势，但随着属性数量的增加，本方案净化算法的时间开销会略优于文献[26]中方案.

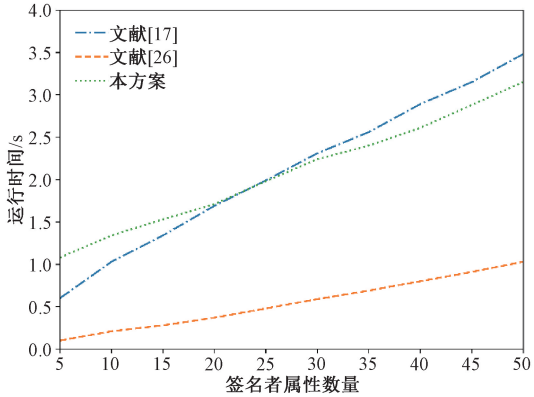

图 2 签名算法性能分析

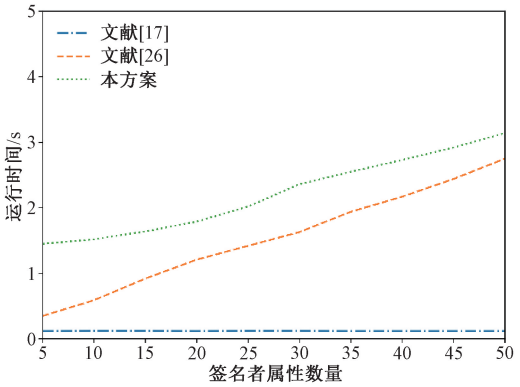

图 3 验证算法性能分析

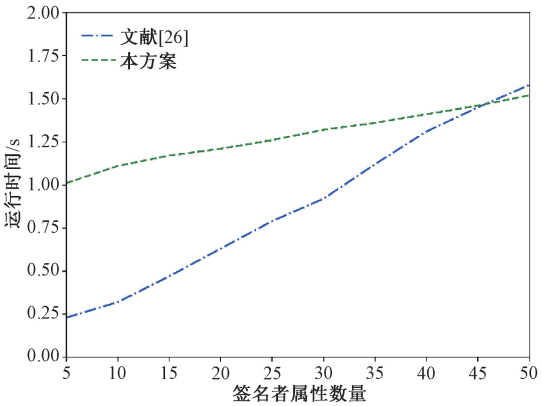

图 4 净化算法性能分析

从图 5 可以看出，由于本方案增加了净化和指定验证者功能，随着消息长度的增加，方案各个算法的计算开销也随之增大. 因此，如何降低方案中签名、验证和净化算法计算开销值得深入研究.

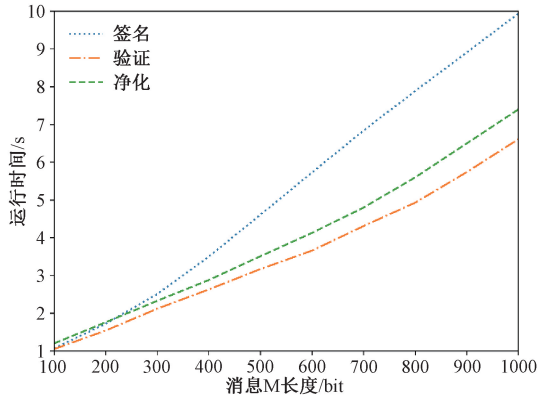

图 5　消息 M 长度下的算法性能分析

9　结束语

本文给出了方案的安全模型,提出一种具有强指定签名者的属性基可净化签名方案,在标准模型下证明方案的安全性.不仅解决了敏感信息脱敏问题,保护用户隐私,而且能够控制数字签名/版权恶意传播.通过与现有方案的功能和性能对比分析可知,提出的方案适用于电子医疗等特殊应用场景中.由于方案增加了净化和指定验证者功能,方案的签名、验证和净化的计算开销随着消息长度的增加而增加,因此方案的计算效率有待进一步提高.为了解决这一问题,将进一步研究如何降低消息长度对算法效率的影响,如采用变色龙哈希函数对消息进行映射,再利用变色龙哈希函数的碰撞性进行修订,以提高方案的计算效率.随着量子计算机的快速发展,传统公钥密码算法的安全性将受到严重威胁.为了抵抗量子计算机攻击,在未来工作中,将设计基于格的/多变量属性基可净化签名方案.

参　考　文　献

[1] Sahai A, Waters B. Fuzzy identity-based encryption//Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer, 2005: 457-473

[2] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption//Proceedings of the 28th IEEE Symposium on Security and Privacy. Los Alamitos, USA: IEEE Computer Society, 2007: 321-334

[3] Gu Ke, Wang Ke-Ming, Yang Lu-Lu. Traceable attribute-based signature. Journal of Information Security and Applications, 2019, 49(11), https://doi.org/10.1016/j.jisa.2019.102400

[4] Okamoto T, Takashima K. Efficient attribute-based signatures for non-monotone predicates in the standard model//Proceedings of the 16th International Conference on. Practice and Theory in Public Key Cryptography. Berlin, Germany: Springer, 2013: 125-142

[5] Maji K, Prabhakaran M, Rosulek M. Attribute-based signatures //Proceedings of the 11th International Conference on Topics in Cryptology. Berlin, Germany: Springer, 2011: 376-392

[6] Li Ji-Guo, Chen Yu, Han Jin-Guang, et al. Decentralized attribute-based server-aid signature in the internet of things. IEEE Internet of Things Journal, 2021, 9(6): 4573-4583

[7] Chen Yu, Li Ji-Guo, Liu Cheng-Dong, et al. Efficient attribute-based server-aided verification signature. IEEE Transactions on Services Computing, 2021, https://doi.org/10.1109/TSC.2021.3096420

[8] Chen Ning-Yu, Li Ji-Guo, Zhang Yi-Chen, et al. Efficient CP-ABE scheme with shared decryption in cloud storage. IEEE Transactions on Computers, 2022, 71(1): 175-184

[9] Li Ji-Guo, Zhang Yi-Chen, Ning Jian-Ting, et al. Attribute based encryption with privacy protection and accountability for cloudIoT. IEEE Transactions on Cloud Computing, 2020, 10(2): 762-773

[10] Goyal V, Pandey O, Saha A, et al. Attribute-based encryption for fine-grained access control of encrypted data//Proceedings of the 13th ACM Conference on Computer and Communications Security. New York, USA: ACM, 2006: 89-98

[11] Jakobsson M, Sako K, Impagliazzo R. Designated verifier proofs and their applications//Proceedings of the 15th International Conference on the Theory and Application of Cryptographic Techniques. Berlin, Germany: Springer 1996: 143-154

[12] Yan Hao, Li Ji-Guo, Zhang Yi-Chen. Remote data checking with designated verifier in cloud storage. IEEE Systems Journal, 2020, 14(2): 1788-1797

[13] Susilo W, Zhang F, Mu Y. Identity-based strong designated verifier signature schemes//Proceedings of the 9th Australasian Conference on Information Security and Privacy. Berlin, Germany: Springer 2004: 313-324

[14] Li Ji-Guo, Qian Na, Huang Xin-Yi, et al. Certificate-based strong designated verifier siganture scheme. Chinese Journal of Computers, 2012, 35(8): 1579-1587(in Chinese)
(李继国, 钱娜, 黄欣沂等. 基于证书强指定验证者签名方案. 计算机学报, 2012, 35(8): 1579-1587)

[15] Li Ji-Guo, Qian Na, Zhang Yi-Chen, et al. An efficient certificate-based designated verifier signature scheme. Computing and Informatics, 2016, 35(5): 1210-1230

[16] Fan Chuni, Wu Chiennan, Chen Weikuei, et al. Attribute-based strong designated-verifier signature scheme. Journal of Systems and Software, 2011, 85(4): 944-959

[17] Blazy O, Brouilhet L, Conchon E, et al. Anonymous attribute-based designated verifier signature. Journal of Ambient

Intelligence and Humanized Computing, 2022, https://doi.org/10.1007/s12652-022-03827-8

[18] Ateniese G, Chou D H, De Medeiros B, et al. Sanitizable signatures //Proceedings of the 10th European Symposium on Research in Computer Security. Berlin, Germany: Springer, 2005: 159-177

[19] Brzuska C, Fischlin M, Freudenreich T, et al. Security of sanitizable signatures revisited//Proceedings of the 12th International Workshop on Public Key Cryptography. Berlin, Germany: Springer, 2009: 317-336

[20] Ming Yang, Shen Xiao-Qin, Peng Ya-Mian. Identity-based sanitizable signature scheme in the standard model//Proc of International Conference on Information Computing and Applications. Berlin, Germany: Springer, 2010: 9-16

[21] Liu Xi-Meng, Ma Jian-Feng, Xiong Jin-Bo, et al. Attribute based sanitizable signature scheme. Journal on Communications, 2013, 34(S1): 148-155(in Chinese)
(刘西蒙, 马建峰, 熊金波等. 基于属性的可净化签名方案. 通信学报, 2013, 34(S1): 148-155)

[22] Mo Ruo, Ma Jian-Feng, Liu Xi-Meng, et al. An attribute-based sanitizable signature supporting dendritic access structure. ACTA ELECTRONICA SINICA, 2017, 45(11): 2715-2720(in Chinese)
(莫若, 马建峰, 刘西蒙等. 一种支持树形访问结构的属性基可净化签名方案. 电子学报, 2017, 45(11): 2715-2720)

[23] Mo Ruo, Ma Jian-Feng, Liu Xi-Meng, et al. FABSS: Attribute-based sanitizable signature for flexible access structure//Proceedings of the 19th International Conference on Information and Communications Security. ICICS 2017. Berlin, Germany: Springer, 2018: 39-50

[24] Samelin K, Slamanig D. Policy-based sanitizable signatures //Proceedings of the Cryptographers' Track at the RSA Conference. Berlin, Germany: Springer, 2020: 538-563

[25] Li Ji-Guo, Zhu Liu-Fu, Liu Cheng-Dong, et al. Provably secure traceable attribute-based sanitizable signature scheme in the standard model. Journal of Computer Research and Development, 2021, 58(10): 2253-2264(in Chinese)
(李继国, 朱留富, 刘成东等. 标准模型下证明安全的可追踪属性基净化签名方案. 计算机研究与发展, 2021, 58(10): 2253-2264)

[26] Afia I, Altawy R. Unlinkable policy-based sanitizable signatures. Cryptology ePrint Archive, 2022, 1422. https://eprint.iacr.org/2022/1422

LI Ji-Guo, Ph. D., professor. His main research interests include public key cryptography and cloud computing security.

ZHU Liu-Fu, master candidate. His main research is public key cryptography.

SHEN Jian, Ph. D., professor. His main research interests include public key cryptography and cloud computing security.

LU Yang, Ph. D., professor. His main research interests include information security and public key cryptography.

ZHANG Yi-Chen, Ph. D., associate professor. Her main research interests include public key cryptography and cloud computing security.

Background

This work was supported by the National Natural Science Foundation of China (62072104, 61972095, U21A20465, 61922045, 62172292, 61877034), and Natural Science Foundation of the Fujian Province, China (2020J01159).

In 2011, Maji et al. first proposed the attribute-based signature scheme, which not only realizes fine-grained access control, but also ensures data integrity and authentication. In 2012, Okamoto et al. proposed an efficient ABS signature scheme supporting non-monotonic access policy, and gave the security proof of the scheme under the standard model. The above signature schemes are all publicly verifiable signatures, that is, anyone can verify the validity of the signature through the verification algorithm. However, in some special applications, the signer does not want to reveal his identity information and signing behavior. In order to solve above problem, in 1996, Jakobsson et al. first proposed the designated verifier signature scheme, which the others cannot verify the signature except the designated verifier.

In the original designated verifier signature scheme, since the signature can only be generated by the signer, once the designated verifier proves the signer's behavior to others, the designated verifier can reveal the signer's privacy. The strong designated verifier signature scheme ensures that the designated verifier can simulate a valid signature, so that the others cannot believe that the information leaked is authentic. In 2004, Susilo et al. proposed an identity-based signature with strong designated verifier, which can simulate a valid signature, thereby avoiding the malicious disclosure of the signer's privacy by the designated verifier. However, using public identities as public keys leaks the signer's privacy

and cannot provide fine-grained access control. In 2011, Fan et al. proposed an attribute-based signature scheme with strong designated verifier, which uses a set of attributes instead of user identity to achieve signer anonymity and has the function of designated verifier.

Besides the privacy of the signer, it's necessary to protect the sensitive data in messages. Sanitizable signatures allow the sanitizer to modify sensitive data in messages without knowing the signer's private key and generate a valid signature for the sanitized data. In 2005, Ateniese et al. first proposed a sanitizable signature scheme using the chameleon hash function. For realizing fine-grained access control, Liu et al. proposed an attribute-based sanitizable signature scheme, which not only ensures fine-grained access control, but also realizes the information desensitization.

This paper proposes an attribute-based sanitizable signature scheme with strong designated verifier. Based on the bilinear Diffie-Hellman (BDH) hard problem assumption, we show the security of the scheme under the standard model. The proposed scheme not only has fine-grained access control, but also protects the security of sensitive information by desensitizing messages. At the same time, by designating the verifier to verify the valid of the signature, it is impossible for third party to determine whether the signature was generated by the original signer, because the designated verifier can also generate a valid signature, so as to control the malicious spread of digital signatures/copyrights.