高效可证明安全的无证书有序聚合签名方案

王竹[1,2]，杨思琦[1,2]，李凤华[1,2]，耿魁[1]，彭婷婷[1,2]，史梦瑶[1,2]
（1. 中国科学院信息工程研究所，北京 100093；2. 中国科学院大学网络空间安全学院，北京 100049）

摘 要：针对目前的方案多采用后一个签名者对前一个签名者的签名进行验证后，再将签名传递给下一个签名者，导致整体签名时间过长的效率问题，基于双线性对构造了一种无证书有序聚合签名方案。多个用户按照一定的顺序对文件进行签名和认证生成聚合签名，验证者只需验证最终一个签名就可以确认签名顺序的正确性以及多个用户签名的合法性。所提方案有效降低了验证多用户顺序签名的复杂性，实现了当用户处于离线状态或者处于节点缓存能力与网络资源受限的容迟网络时，对签名合法性的离线验证。在随机预言机模型下，仿真实验证明了所提方案在敌手适应性选择消息下是存在性不可伪造的。

关键词：无证书公钥密码；有序聚合签名；双线性映射；随机预言机
中图分类号：TN309
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2022073

Efficient and provably-secure certificateless sequential aggregate signature scheme

WANG Zhu[1,2], YANG Siqi[1,2], LI Fenghua[1,2], GENG Kui[1], PENG Tingting[1,2], SHI Mengyao[1,2]
1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract: Aiming at the problem that current schemes mostly let the latter signer to verify the multiple signatures of the previous signer, and the message is signed and then passed to the next signer, leading to the efficiency problem of long overall signature time. A sequential aggregate signature scheme based on bilinear pairs was proposed. The aggregate signatures of documents were generated by multiple users in a certain order, and only the final signature was needed to be verified to confirm the correct order of signatures and the legitimacy of multiple user signatures. The complexity of verifying the multi-user sequential signature was effectively reduced and the offline verification of the authenticity of signature was realized when the user was offline or in a delay-tolerant network with limited node caching capacity and network resources. It is shown that the proposed scheme is existential unforgeability against chosen-message attacks under adversary adaptive selection messages in the random oracle model.

Keywords: certificateless public key cryptography, sequential aggregate signature, bilinear map, random oracle

0 引言

聚合签名是解决多用户多信息大量认证授权的一种有效方案，聚合算法可将指定的 n 个用户对 n 个消息的签名聚合生成一个签名，签名在经过一系列流转之后，验证方只需要验证聚合后的一个签名为真，便可确认消息是由确定的 n 个用户发送的。Boneh 等[1]提出了第一个签名聚合方案，并给出了基于 BLS（Boneh-Lynn-Shacham）短签名的签名构造方案。近年来，聚合签名主要应用于车载自组网（VANET, vehicular ad- hoc network）中的安全认证、安全路由协议、安全交易等众多领域，用于解决分

收稿日期：2021−12−16；修回日期：2022−03−13
通信作者：耿魁，gengkui@iie.ac.cn
基金项目：国家重点研发计划基金资助项目（No.2018YFB0803903）
Foundation Item: The National Key Research and Development Program of China (No.2018YFB0803903)

布式系统中需要批量验证多个不同用户对不同信息的签名问题。

现实中需要不同机构对某一个流转消息进行数字签名的分布式环境，该环境中，企业需要将经过一系列机构签名后的信息交付给用户，用户在使用时需要检验其真实性。例如电子发票在开具流程中需要通过不同机构对相关信息进行核验，用户在进行报销时需要对其真伪进行查验。此时电子发票的数字签名过程涉及信任传播问题并需要保证其真伪，更适合采用有序聚合签名的方案。如图 1 所示，当前互联网服务主要分为 3 个主体，包括企业用户、个人用户和服务器端。不同机构需要在确认前面节点信息的真实性之后附加自己的签名，以保证信任链的安全。但是如果没有安全有效的验证机制来检验信息在传输链上是否被篡改，就无法防止恶意攻击者对文件的相关信息进行篡改和伪造，进而造成经济损失，因此需要采取数字签名技术确保信息的真实性和完整性。有序聚合签名除了需要作为一个普通的聚合签名方案保证安全性之外，还必须在签名者的排序方面强制附加不可伪造性。也就是说，在排列顺序安全中，有 2 个安全问题值得注意：1) 在得到单个用户的签名和已完成聚合签名的情况下，不能交换用户的签名顺序来合成新的签名；2) 在得到多组有序聚合签名计算结果的情况下，不能将其结果合成一个有序聚合签名[2]。

当前，应用于互联网服务中的签名验证的一种常用方法是通过签发系统将不同机构签署的签名收集在一起，形成批量的签名。当需要对其真伪进行判断时，验证者可将签名及相关信息发送给查验系统，查验系统会匹配相应的签发机构对文件中的签名进行逐一验证。但该验证方法在传输过程中体量大、速度慢，考虑到多方参与，对于各参与方的通信和计算要求也是十分苛刻和复杂的，这对于查验的效率有很大的影响。

同时，当前查验系统并没有考虑到当用户处于离线状态或者处于节点缓存能力与网络资源受限的容迟网络（DTN, delay tolerant network）[3]典型应用场景时，需要对签名进行离线验证。在容迟网络的应用场景下，无法直接访问数据库对文件信息查验要素进行对比来查验信息的合法性。目前针对信息的离线验证暂无可行的解决方案。

本文针对电子发票中存在的问题，设计了一种高效安全的无证书有序聚合签名方案。为了解决目前签名在实际应用场景下的不足，本文方案实现了电子发票的防伪，保证了签名的安全性，提升了签名的验证效率并满足了离线验证需求。在安全性方面，本文方案不仅解决了证书分发和管理以及密码托管的安全问题，还确保了签名方案是存在性不可伪造的。在验证效率方面，本文方案进行签名和验证需要的时间比同类方案更少，降低了计算开销。在应用场景方面，本文方案不仅支持在线验证，也考虑了在容迟网络等典型应用场景下的离线验证。

本文的主要贡献如下。

1) 设计了一种无证书有序聚合签名方案，有效地解决了多用户有序签名的安全问题，并提高了安全性。

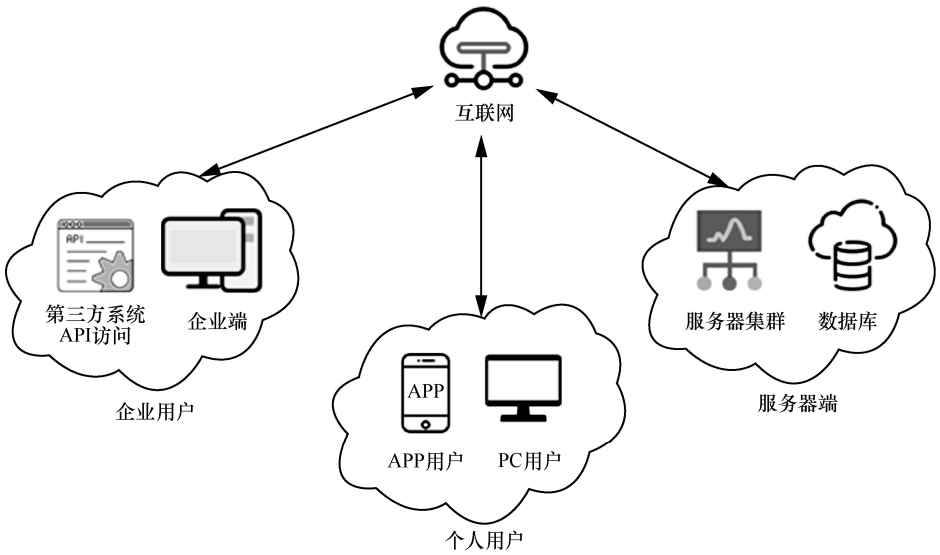

图 1　互联网服务

2) 相比于其他签名方案，本文方案降低了计算开销，有效地减少了验证所需时间，提高了检验效率。

3) 当用户处于离线状态或者处于节点缓存能力与网络资源受限的容迟网络的应用场景时，可以进行离线验证。

1 相关工作

从公钥密码体制的角度看，聚合签名主要分为三类：基于公钥基础设施（PKI, public key infrastructure）的聚合签名[4]、基于身份的聚合签名[5]和无证书聚合签名。

对于基于 PKI 的聚合签名，Liu 等[6]引入了第一个基于证书的顺序聚合签名方案，缩短了签名者发送消息的总带宽，此方案在 M-LRSW（M- Lysyanskaya-Rivest-Sahai-Wolf）和 DH（Diffie-Hellman）假设下是可证明安全的。2017 年，Verma 等[7]提出了一种适用于分布式系统、应用于无线传感网络的基于证书的短聚合签名方案，此方案为当前基于配对的最短签名构造方案。2020 年，Verma 等[8]提出了应用于电子医疗的基于证书的配对自由聚合签名方案，保证了生成源的完整性和认证，简化了基于传统公钥基础设施的证书管理过程，适用于带宽和计算受限的环境。然而，基于 PKI 的签名方案需要大量存储空间来存放证书，可能存在证书管理问题。

对于基于身份的聚合签名，Boldyreva 等[2]提出了一种基于身份的有序聚合签名 IBSAS（identity-based sequential aggregate signature）方案，它依赖于第三方可信服务器密钥生成中心（KGC, key generation center），用户通过计算 KGC 生成的主私钥和自己生成的秘密密钥来计算其完整私钥。2016 年，Muranaka 等[9]基于 IBSAS 方案进行改进，提出针对动态源路由协议的基于身份的有序聚合签名 ISDSR（secure DSR with ID-based sequential aggregate signature）方案，相比于 IBSAS 方案，该方案有效提高了计算性能。2019 年，Kojima 等[10]针对新设备在加入动态路由协议时 ISDSR 与集中式 KGC 通信可能产生的问题，提出了一种基于身份的公钥密码体制，采用分布式密钥的有序聚合签名 ISDSR+方案，消除了集中式 KGC，将分布式 KGC 应用于基于身份的有序聚合签名中。基于身份的聚合签名解决了基于 PKI 聚合签名中证书的发放管理问题，但因为其密钥的生成依赖于可信第三方，所以存在密钥托管问题。

对于无证书聚合签名，相比于基于 PKI 的聚合签名，其解决了证书的发放和管理问题；相比于基于身份的聚合签名，因为无证书聚合签名只需要半可信的第三方为用户提供部分私钥，所以解决了密钥托管问题，是目前飞速发展的一类聚合签名。2015 年，Horng 等[11]为车联网引入了无证书聚合签名方案，以防止自适应选择的消息攻击。然而 Gayathri 等[12]提出文献[11]方案无法抵抗恶意 KGC 被动攻击。2016 年，刘丹等[13]提出一种无线网络中基于无证书聚合签名方案，保证了用户的隐匿性和不可追踪性，但该方案不能抵抗单个签名伪造攻击。2019 年，Kamil 等[14]提出了一种基于椭圆曲线加密（ECC, elliptic curve cryptography）的无证书聚合签名方案，以满足 VANET 的批量验证、自治和有条件的隐私保护。Zhao 等[15]提出了一种对文献[14]方案的攻击模型，证明了其方案并不安全。Xie 等[16]引入格中困难问题，提出了一种基于 NTRU（number theory research unit）的无证书聚合签名方案，提高了计算复杂性。Cahyadi 等[17]对目前应用于车载自组网中的无证书聚合签名方案进行了调研。可以看出，目前应用于计算资源受限的环境提出的聚合签名方案大部分采用基于椭圆曲线的密码算法，因为椭圆曲线在相同安全强度下只需要更小的密钥，从而可以减轻计算负担。综合以上方案，本文方案将采用基于椭圆曲线的无证书聚合签名，支持离线验证的应用场景。

聚合签名按照聚合的方式主要分为三类：完全聚合签名[1]、同步聚合签名[18]和有序聚合签名[19]。1) 完全聚合签名允许任何用户自由聚合不同签名者的不同签名，这种聚合方式虽然十分灵活，但不能对聚合步骤进行限制，没有任何安全约束。2) 同步聚合签名具有一定的安全约束，允许用户将具有相同同步信息的不同签名组合成单个签名。同步聚合签名允许所有签名者共享相同的同步信息，如时钟或其他共享值。3) 有序聚合签名是三类聚合签名中安全性要求最高的一种签名，有较严格的顺序要求，每个签名者必须按照一定的顺序将自己的签名聚合到当前的签名中，否则生成的聚合签名会查验失败；每个签名者都必须在接收到上一个指定用户的签名之后，才能对签名进行聚合签名的操作，并且将签名发送给下一个指定的签名者。Lysyanskaya 等[19]首次提出有序聚合签名的概念，并利用随机预言模型中的认证陷门置换设计了一种有序聚合签名。

本文基于身份的有序聚合签名[2]，采用三维变量作为聚合签名；基于 BLS 多重签名[20]，通过构造双线性

对形成验证等式并修改等式，以支持本文的应用场景。

2　背景知识

2.1　双线性对

定义 1　假设 G_1 是阶为素数 q 的加法循环群，G_2 为同阶的乘法循环群，P 是 G_1 的生成元，则称映射 $e: G_1 \times G_1 \to G_2$ 是一个双线性映射，它满足以下特性。

1) 双线性性。对 $\forall\ a,b \in Z_p^*$，$P,Q \in G_1$，满足 $e(aP,bQ)=e(P,Q)^{ab}$。

2) 非退化性。对 $\forall\ P,Q \in G_1$，满足 $e(P,Q) \neq 1_{G_2}$，其中 1_{G_2} 为 G_2 的单位元。

3) 可计算性。对 $\forall\ P,Q \in G_1$，存在有效算法可以计算出 $e(P,Q)$。

2.2　困难性假设

CDH（Computational Diffie-Hellman）问题。假设 G 是阶为素数 q 的加法循环群，对 $\forall a,b \in Z_p^*$，$P \in G$，给定 (P,aP,bP)，计算 abP。

CDH 问题困难性假设是指在多项式时间内，不存在一个有效算法以不可忽略的概率解决 CDH 问题。

3　无证书有序聚合签名的定义及安全模型

3.1　无证书有序聚合签名方案的定义

无证书有序聚合签名主要由第三方可信机构 KGC、签名用户 $N_i(i=1,2,\cdots,n)$、签名顺序 K 和验证者 V 构成，需要执行以下 5 个算法：Setup（初始化系统参数的生成算法）、Partial-Private-Key-Extract Phase（部分私钥生成算法）、KeyGen（密钥生成算法）、Sign（签名算法）和 Verify（验证算法）。

1) Setup。该算法由 KGC 发起执行。KGC 首先选取随机正整数 k 作为安全参数，然后向所有签名用户 $N_i(i=1,2,\cdots,n)$ 返回系统公共参数 mpk 并将主私钥 msk 秘密保存在本地。

2) Partial-Private-Key-Extract Phase。该算法由 KGC 执行。KGC 首先从用户数据库中获取签名用户身份标识 ID_i，如果数据库中没有相关用户的数据，则数据库先向各个签名用户发送请求，获取用户身份标识 ID_i 并保存到数据库中。通过用户身份标识 ID_i、系统公共参数 mpk 和主私钥 msk 等参数计算出部分私钥并发送给各个签名用户。

3) KeyGen。该算法由各个签名用户 $N_i(i=1,2,\cdots,n)$ 执行。签名用户选取随机数作为秘密值，将秘密值与从 KGC 接收的部分私钥结合，生成签名用户的私钥，签名用户根据私钥计算得到公钥。

4) Sign。该算法由签名用户 $N_i(i=1,2,\cdots,n)$ 按照一定的顺序执行。用户 N_1 对消息 m_1 进行签名之前先对签名进行初始化，作为第 0 轮的签名 σ_0。签名用户 $N_i(i=1,2,\cdots,n)$ 在对消息 m_i 进行签名时，首先需要获取上一轮的签名 σ_{i-1}，依据 σ_{i-1} 和 mpk 计算消息 m_i 的签名，得到签名 σ_i。然后将签名用户的身份标识 ID_i、用户公钥 pk_i、消息 m_i 的组合顺序列表 $L_i=\{(\mathrm{ID}_j,\mathrm{pk}_j,m_j)\}_{j=1}^{i}$ 以及此轮的签名 σ_i 传递给下一用户。参与签名的最后一位用户将保留系统公共参数 mpk、列表 $L_n=\{(\mathrm{ID}_i,\mathrm{pk}_i,m_i)\}_{i=1}^{n}$ 以及最后一位用户的签名 σ_n，此时完成签名算法。

5) Verify。该算法由验证者 V 执行。首先验证者 V 需要获取系统公共参数 mpk、n 个签名用户的身份标识 ID_i、用户公钥 pk_i 和消息 m_i 的组合顺序列表 $L_n=\{(\mathrm{ID}_i,\mathrm{pk}_i,m_i)\}_{i=1}^{n}$ 以及最终的完整签名 σ_n。然后验证者 V 进行验证计算，并以一个判定 $\in$ {真, 假}作为输出，当且仅当输出为真时签名有效。

3.2　无证书有序聚合签名方案安全模型

Shim[21]提出一种无证书签名方案的安全模型，被广泛用于无证书签名方案的安全证明。该模型中存在 2 种类型的攻击者：1) 攻击者 A_1，其实质为恶意的参与用户，被赋予的能力为可以替换用户的公钥，但不能获知系统主私钥；2) 攻击者 A_2，其实质为恶意的 KGC，被赋予的能力为可以获知系统主私钥，但不能替换用户的公钥。本文定义无证书有序聚合签名方案的安全模型可以通过挑战者 D 和攻击者 $A \in (A_1,A_2)$ 之间的攻击游戏来定义，其安全模型具体如下。

1) 系统参数设置。挑战者 D 运行算法 Setup，输出系统公共参数 mpk 和主密钥 msk，得到系统参数 para 和系统主密钥。如果 $A=A_1$，D 将系统公共参数发送给攻击者 A；如果 $A=A_2$，D 将系统公共参数和主密钥发送给 A。

2) 询问。假设攻击者 A 能攻破 k 个签名者，即 A 能知道 k 个签名者的私钥并能伪造他们的部分签名。攻击者 A 为了获得未被攻破签名者的部分签名，向挑战者 D 发起一系列的询问，包括散列询问、密钥生成询问（只适用于攻击者 A_1）和签名询问，并得到输出。

3) 伪造。攻击者输出签名者集合 $N_i(i=1,2,\cdots,n)$ 对消息 m^* 的聚合签名 σ_n，若满足以下条件，则攻击成功。

① 攻击者 A 未对 m^* 执行部分签名询问。

② σ_n^* 的签名者 $N_i(i=1,2,\cdots,n)$ 按签名顺序 K 对 m^* 的有效签名。

若上述条件全部成立，则 D 挑战成功，输出结果；否则挑战失败，不输出结果。

通过采用上述安全模型，可以检验无证书聚合签名是否能抵抗两类攻击者 A_1 和 A_2 的攻击，从而确认方案的安全性。Horng 等[11]为车联网引入无证书聚合签名方案，但该方案不能抵抗 A_2 的攻击。Cui 等[22]为车联网引入不采用双曲线配对的无证书聚合签名方案，但该方案不能抵抗 A_2 的攻击。Kamil 等[14]提出的无证书聚合签名方案能提供隐私保护，但该方案不能抵抗 A_1 和 A_2 的攻击。本文提出的无证书有序聚合签名方案可以同时抵抗 A_1 和 A_2 的攻击。

4 无证书有序聚合签名方案

4.1 方案描述

本节采用椭圆曲线密码体制提升方案安全性，基于双线性映射支持方案的计算特性，设计一种无证书有序聚合签名方案。设某条有序聚合签名在网络传输路径上的顺序为 $N_1 \to N_2 \to \cdots \to N_n$，其中签名用户 N_i 对传输消息 m_i 进行聚合签名，用户 $N_i(1 \leqslant i < n)$ 的身份信息为 $\mathrm{ID}_i \in \{0,1\}^*(1 \leqslant i < n)$。本文方案包含 5 个多项式时间算法，具体介绍如下。

1) Setup。该算法由 KGC 发起执行。首先选取随机正整数 k 作为安全参数，返回系统参数并将主私钥保存在 KGC 中。KGC 执行以下步骤。

①选择由椭圆曲线上的点构成的阶为素数 p 的加法循环群 $(G,+)$ 和阶为 p 的乘法循环群 $(G_T,\times)$，双线性映射 $e: G \times G \to G_T$。

② g 为 G 的一个生成元。

③选择随机数 $\alpha_1 \in Z_P^*$，$\alpha_2 \in Z_P^*$。

④选择安全哈希函数 $H_1:\{0,1\}^* \to G^*$，$H_2:\{0,1\}^* \to G^*$，$H_3:\{0,1\}^* \to Z_P^*$。公布系统参数 $\Omega=(G,G_T,e,g,\alpha_1 g,\alpha_2 g,H_1,H_2,H_3)$ 作为系统公共参数 mpk 并发送给各个用户。将 (α_1,α_2) 作为主私钥 msk 保存在 KGC。

2) Partial-Private-Key-Extract Phase。该算法由 KGC 执行。首先，KGC 从用户数据库中获取签名用户身份标识 ID_i，如果数据库中没有相关用户的数据，则数据库先向各个签名用户发送请求，获取用户身份标识 ID_i 并保存到数据库中。然后，KGC 计算 $(d_{i,1},d_{i,2})=(\alpha_1 H_1(\mathrm{ID}_i),\alpha_2 H_2(\mathrm{ID}_i))$ 并将其作为部分私钥发送给各个签名用户。

3) KeyGen。该算法由各个签名用户 $N_i(i=1,2,\cdots,n)$ 执行。签名用户选取随机数 $s_i \in Z_p$ 作为秘密值，将秘密值与从 KGC 接收的部分私钥结合，生成签名用户的私钥 $\mathrm{sk}_i=(s_i d_1, s_i d_2)$，签名用户计算 $\mathrm{pk}_i=(\mathrm{pk}_{i,1},\mathrm{pk}_{i,2})=(s_i d_1 g, s_i d_2 g)$ 并将其作为公钥。

4) Sign。该算法由签名用户 $N_i(i=1,2,\cdots,n)$ 执行。其具体签名算法如下。

① 首先，签名用户 N_1 对 m_1 进行签名之前，签名进行初始化 $\sigma_0=(1_G,1_G,1_G)$。

② 然后，该条信任路径上的节点 $N_i(1 \leqslant i < n)$ 将以 $N_1 \to \cdots \to N_n$ 为签名顺序，对 m_i 进行聚合签名。每个签名用户的具体算法如下。

a. 选择随机数 $r \in Z_P^*$，$x \in Z_P^*$。

b. 获取上一节点的签名 $\sigma_{i-1}=(\sigma_a,\sigma_b,\sigma_c)$，计算本节点的签名 $\sigma_i=(\sigma_a',\sigma_b',\sigma_c')$，其中，$\sigma_c'=\sigma_c+xg$，$\sigma_b'=\sigma_b+rg$，$\sigma_a'=\sigma_a+r\sigma_c+x\sigma_b'+s_i d_{i,2}+H_3(\mathrm{pk}_i \| m_i)s_i d_{i,1}$。

c. 将 $\sigma_i=(\sigma_a',\sigma_b',\sigma_c')$ 作为签名用户 N_i 对 m_i 的签名。将签名用户的身份标识 ID_i、用户公钥 pk_i、消息 m_i 的组合顺序列表 $L_i=\{(\mathrm{ID}_j,\mathrm{pk}_j,m_j)\}_{j=1}^i$ 以及此轮的签名 σ_i 传递给下一用户，直到 N_n 完成对 m_n 的签名。在此过程中，维护变量 $V_1=V_1+\mathrm{pk}_{i,1}$，$V_2=V_2+\mathrm{pk}_{i,2}$。

③ 信任路径上的节点 $N_1,N_2,\cdots,N_n$ 依次完成对信息 m 的有序聚合签名 σ，并将签名用户的身份标识 ID_i、用户公钥 pk_i、消息 m_i 的组合顺序列表 $L_n=\{(\mathrm{ID}_i,\mathrm{pk}_i,m_i)\}_{i=1}^n$ 以及最后完整签名 σ_n 存储到文件中，完成此签名算法。

5) Verify。查询节点在收到用户的查验请求后，会接收由各个签名用户计算完成并在非安全通道中流转的信息。此时，查询节点首先会提取存储文件的相关信息，包括签名用户的身份标识 ID_i、用户公钥 pk_i、消息 m_i 的组合顺序列表 $L_n=\{(\mathrm{ID}_i,\mathrm{pk}_i,m_i)\}_{i=1}^n$ 以及最后完整签名 σ_n。若要对聚合签名的真伪进行验证，则执行以下步骤。

① 首先，对查验环境进行检测。若查验环境网络良好，则将相关的信息发送给服务器，相关算

法在服务器端进行；若查验环境处于节点缓存能力与网络资源受限的容迟网络，则根据相关的信息在本地终端上进行验证。

② 然后，确定正确的签名顺序 ID_i 用于验证。根据顺序列表，判断列表中每个用户身份标识 ID_i 是否存在重复的情况，若存在则停止验证，签名验证失败。

③ 计算

$$e(\sigma_a,g)=e(\sigma_b,\sigma_c)e\left(\sum_{i=1}^{n}H_2(\mathrm{ID}_i),V_2\right)\cdot e\left(\sum_{i=1}^{n}H_3(\mathrm{pk}_i\,\|\,m_i)H_1(\mathrm{ID}_i),V_1\right) \tag{1}$$

若式(1)成立，则可以确认各参与方按照指定的顺序进行了信息的传递，并且在信息流转的过程中并没有受到恶意节点篡改和第三方攻击。若式(1)不成立，则证明签名中间过程存在攻击，签名验证失败。

因为检验所需要的信息都存储在相关文件中，所以在查验系统获取了系统公共参数后，根据查验步骤就可以判断签名的合法性，而不需要与其他系统进行交互。在离线状态或者处于节点缓存能力与网络资源受限的容迟网络时，也可以对签名的合法性进行验证。

4.2　正确性证明

证明　假设基于无证书的有序聚合签名 $\sigma_n=(\sigma_a,\sigma_b,\sigma_c)$ 是由上述签名方案得到的，则必然满足

$$e(\sigma_a,g)=e\left(rxg+\sum_{i=1}^{n}s_id_{i,2}+\sum_{i=1}^{n}H_3(\mathrm{pk}_i\,\|\,m_i)s_id_{i,1},g\right)=e\left(rxg+\sum_{i=1}^{n}s_i\alpha_2H_2(\mathrm{ID}_i)+\sum_{i=1}^{n}H_3(\mathrm{pk}_i\,\|\,m_i)s_i\alpha_1H_1(\mathrm{ID}_i),g\right)=e(xg,rg)e\left(\sum_{i=1}^{n}s_i\alpha_2H_2(\mathrm{ID}_i),g\right)\cdot e\left(\sum_{i=1}^{n}H_3(\mathrm{pk}_i\,\|\,m_i)s_i\alpha_1H_1(\mathrm{ID}_i),g\right)=e(\sigma_b,\sigma_c)e\left(\sum_{i=1}^{n}H_2(\mathrm{ID}_i),V_2\right)\cdot e\left(\sum_{i=1}^{n}H_3(\mathrm{pk}_i\,\|\,m_i)H_1(\mathrm{ID}_i),V_1\right)=e(\sigma_b,\sigma_c)e\left(\sum_{i=1}^{n}H_2(\mathrm{ID}_i),V_2\right)\cdot e\left(\sum_{i=1}^{n}H_3(\mathrm{pk}_i\,\|\,m_i)H_1(\mathrm{ID}_i),V_1\right) \tag{2}$$

证毕。

5　安全性分析

定义 2　对于无证书有序聚合签名方案，本文假设攻击者 A 在随机预言机模型下能获知所有 n 个签名成员中第 $k(1\leqslant k<n)$ 个签名者的私钥。当挑战者 D 能以超过 ε 的概率在时间 t 内参与攻击游戏，并在游戏中输出结果，则称 A 以 $(\varepsilon,q_h,q_k,q_p,q_v,q_c,q_s,(n,k),t)$ 攻破该方案。其中，A 至多做 q_h 次散列询问、q_k 次部分私钥询问、q_p 次公钥询问、q_v 次秘密值询问、q_c 次公钥替换询问和 q_s 次签名询问。

定义 3　一个无证书有序聚合签名方案在适应性选择消息攻击下是 $(\varepsilon,q_h,q_k,q_p,q_v,q_c,q_s,(n,k),t)$ 不可伪造的，当且仅当不存在敌手 A 时可利用概率多项式时间攻破该方案。

定义 4　在本文方案中，如果存在敌手 A_1 和 A_2 以不可忽略的概率在游戏 1 和游戏 2 中获胜，则该方案在适应性选择消息下不可伪造。

定义 5　本文命名一种安全假设无证书有序聚合签名假设 CLSAS-CDH，并定义 CLSAS-CDH 假设如下。假设给出一组随机数 $(a_1,a_2,b_1,b_2)\in Z_p^*$，并建立列表 (g,a_1g,a_2g,b_1g,b_2g)。随机预言机 $O^{\mathrm{CLSAS\text{-}CDH}}_{g,a_1g,a_2g,b_1g,b_2g}$ 将 $m\in Z_p^*$ 作为输入，计算 $(rxg+a_1b_1g+ma_2b_2g,rg,xg)$ 作为返回值，其中 $(r,x)\in Z_p$，可进行 q 次查询，其中，每个查询中涉及的元素 m 必须不同于最终输出中涉及的元素 m，如果不能以大于 ε 的概率多项式时间解决此问题，则 CLSAS-CDH 假设成立。

定理 1　在随机预言模型下，如果存在敌手 A_1 能够在时间 t 内进行 H_1 询问、H_2 询问、H_3 询问、密钥生成询问和签名询问，然后以不可忽略的概率 ε 伪造出签名，那么存在一个算法 B 能够在时间 $t'<t+(q_h+q_k+q_p+q_v+q_c+q_s)t_{\mathrm{sm}}$ 内，以 $\varepsilon'\geqslant\dfrac{1}{e(q_k+N(q_s+1)+1)}$ 的优势解决 CDH 问题，其中 t_{sm} 表示群上标量乘法的计算时间。

证明　A_1 是攻击者，首先，挑战者 D 输入安全参数 K 运行算法 Setup，得到系统参数 mpk 和主密钥 s，D 保留 s，发送系统参数给 A_1。D 需要维护表 H_1-list、H_2-list、H_3-list、ID-list、PK-list，并需要对 H_1、H_2、H_3 进行散列询问、部分私钥询

问、公钥询问、秘密值询问、公钥替换询问和签名询问，各表均初始化为空。D 与 A_1 模拟过程中，A_1 可以询问以下预言机。

1) H_1 询问 $(\mathrm{ID}_i(h))$。攻击者 A_1 输入要询问的参数 $(\mathrm{ID}_i(h))$。

① 如果 H_2-list 包含 $(\mathrm{ID}_i(h),\beta_i,B_i)$，$D$ 将 $H_2(\mathrm{ID}_i(h))$ 作为询问结果返回给攻击者 A_1。

②如果 H_2-list 不包含 $(\mathrm{ID}_i(h),\alpha_i,B_i)$，则执行抛币协议 $B_i=\{0,1\}$，概率为 $P[B_i=0]=1-\varepsilon$，$P[B_i=1]=\varepsilon$。B 生成随机数 $\alpha_i\in Z_P^*$，若 $B_i=0$，则 $H_1(\mathrm{ID}_i(h))=\alpha_i g$；若 $B_i=1$，则 $H_1(\mathrm{ID}_i(h))=\alpha_i g+b_1 g$。将 $H_1(\mathrm{ID}_i(h))$ 返回给 A_1，同时将 $(\mathrm{ID}_i(h),\alpha_i,B_i)$ 写入 H_1-list。

2) H_2 询问 $(\mathrm{ID}_i(h))$。攻击者 A_1 输入要询问的参数 $(\mathrm{ID}_i(h))$。

① 如果 H_1-list 包含 $(\mathrm{ID}_i(h),\beta_i,B_i)$，$D$ 将 $H_1(\mathrm{ID}_i(h))$ 作为询问结果返回给攻击者 A_1。

②如果 H_1-list 不包含 $(\mathrm{ID}_i(h),\beta_i,B_i)$，则执行抛币协议 $B_i=\{0,1\}$，概率 $P[B_i=0]=1-\varepsilon$，$P[B_i=1]=\varepsilon$。B 生成随机数 $\alpha_i\in Z_P^*$，若 $B_i=0$，则 $H_1(\mathrm{ID}_i(h))=\beta_i g$；若 $B_i=1$，则 $H_1(\mathrm{ID}_i(h))=\beta_i g+b_2 g$，将 $H_1(\mathrm{ID}_i(h))$ 返回给 A_1，同时将 $(\mathrm{ID}_i(h),\beta_i,B_i)$ 写入 H_2-list。

3) H_3 询问 $(\mathrm{pk}_i(h)\|m_i(h))$。攻击者 A_1 输入要询问的参数 $(\mathrm{pk}_i(h)\|m_i(h))$。

B 生成随机数 $\delta_i=Z_p^*$ 并且定义 $H_3(\mathrm{pk}_i(h)\|m_i(h))=\delta_i$。$B$ 返回 $H_3(\mathrm{pk}_i(h)\|m_i(h))$ 同时将 $(\mathrm{pk}_i(h)\|m_i(h),\delta_i)$ 写入 H_3-list。

4) 部分私钥询问。攻击者 A_1 询问相应的部分私钥 $(d_{i,1},d_{i,2})$，挑战者 D 执行以下步骤。

①对 $(\mathrm{ID}_i(h))$ 执行 H_1 询问和 H_2 询问，如果 $(\mathrm{ID}_i(h))$ 不存在于 H_1-list 和 H_2-list 中，则失败退出。

② H_2 计算 $(d_{i,1},d_{i,2})=(\alpha_i a_1 g,\beta_i a_2 g)$。从 H_1-list 和 H_2-list 来看，$(d_{i,1},d_{i,2})$ 可以写作 $a_1H_1(\mathrm{ID}_i(h))=\alpha_i a_1 g$ 和 $a_2H_2(\mathrm{ID}_i(h))=\beta_i a_2 g$。

③ B 将 $(d_{i,1},d_{i,2})$ 作为询问结果返回给攻击者 A_1，同时将 $(\mathrm{ID}_i(h),a_1H_1(\mathrm{ID}_i(h)),a_2H_2(\mathrm{ID}_i(h)))$ 写入 ID-list。

5) 公钥询问(pk_i)。攻击者 A_1 询问相应的公钥(pk_i)。

B 保持列表 $\mathrm{PK}=\{\mathrm{ID}_i,s_i,\mathrm{pk}_i,B_i\}$。$A_1$ 询问 ID_i，若 PK 包含询问内容，则返回给 A_1。否则，执行抛币协议 $B_i=\{0,1\}$，概率为 $P[B_i=0]=1-\varepsilon$，$P[B_i=1]=\varepsilon$。选取随机数 $s_i\in Z_p$，计算 $\mathrm{pk}_i=s_i g$，B 将 pk_i 作为询问结果返回给攻击者，同时将 $\{\mathrm{ID}_i,s_i,\mathrm{pk}_i,B_i\}$ 写入 PK-list。

6) 秘密值询问(s_i)。攻击者 A_1 询问相应的秘密值 s_i。

攻击者 A_1 询问秘密值 s_i 时，B 查询 PK-list。若 s_i 存在 PK-list，则返回对应值；若 s_i 不存在 PK-list，则 B 执行公钥询问并将 $\{\mathrm{ID}_i,s_i,\mathrm{pk}_i,B_i\}$ 写入 PK-list，返回 s_i 值。

7) 公钥替换询问(pk_i)。攻击者 A_1 将 pk_i' 新的公钥替换原有公钥 pk_i。

攻击者 A_1 进行公钥替换询问时，B 查询 PK-list。若 PK-list 包含对应的 pk_i，则令 pk_i=pk_i'；若 PK-list 不包含对应的 pk_i，则将 pk_i' 添加到 PK-list 中，最后返回 pk_i' 值。

8) 签名询问 $(\mathrm{para},\mathrm{mpk},m_i(h),\mathrm{ID}_i(h),\mathrm{PK}_i(h),L,\sigma)$。签名询问首先进行密钥生成询问，然后生成签名。

① 对于 PK-List 中的每个 PK_i，首先判断其对应的 B_i 是否为 1，若为 1，则执行密钥生成询问，并通过列表 L_n 检查前 $i-1$ 项 $\mathrm{ID}_i(h)$ 在 H_1-list 和 H_2-list 中的 B_i 值是否为 1。若为 0，则失败退出。

② B 向随机预言机 $O^{\text{CLSAS-CDH}}_{g,a_1g,a_2g,b_1g,b_2g}$ 中输入 δ_i，并从中获取 $(rxg+a_1b_1g+\delta_i a_2b_2g,rg,xg)$。

③ B 从 H_1-list 中获得 α_i，从 H_2-list 中获得 β_i，计算 $\left(rxg+a_1b_1g+\delta_i a_2b_2g+\sum_{j=1}^{i}\alpha_j a_1 g+\delta_j\beta_j a_2 g\right)$ 并将其作为 σ_1。同时设置 $\sigma_2=rg$，$\sigma_3=xg$。σ_1 也可写作

$$\left(rxg+\sum_{j=1}^{i}(a_2H_2(\mathrm{ID}_j)+a_1H_3(\mathrm{pk}_j\|m_j)H_1(\mathrm{ID}_j)\right) \tag{3}$$

B 返回签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$

输出 通过以上模拟，A 输出伪造的 (L^*,σ^*)，其中正好有一个 ID_j^* 没有被查询过。假设其中有且仅有一个 ID_j^* 不存在于 H_1-list 和 H_2-list 中，其他 $\mathrm{ID}_j^*\in L$ 都存在于 H_1-list 和 H_2-list 中。若不符合此条件，则 B 失败退出。

然后，签名可以通过式(4)解出。

$$\sigma_1=\left(rxg+a_1b_1g+\delta_j a_2b_2g+\sum_{i=1}^{n}\left(\alpha_1 a_1 g+\delta_i\beta_i a_2 g\right)\right) \tag{4}$$

因此，D 解决了 CDH 问题。

进一步，D 成功解决 CDH 问题的概率可以转化为

$$\sigma'=\sigma_1-\sum_{i=1}^{n}(\alpha_i a_1 g+\delta_i\beta_i a_2 g)= rxg+a_1b_1g+\delta_j^* a_2b_2g \tag{5}$$

其中，δ_j^* 没有被询问过。

为了完善这个证明，接下来对 B 的成功可能性 ε' 进行分析。

询问过程在以下 3 个场景下会失败退出。1) 在进行部分私钥询问时，如果 $\mathrm{ID}_i(h)$ 不存在于 H_1-list 和 H_2-list 中，则失败退出。2) 在进行签名询问时，如果 $\mathrm{ID}_i(h)$ 不存在于 H_1-list 和 H_2-list 中，则失败退出。3) 在输出阶段，有且仅有一个 ID_j^* 不存在于 H_1-list 和 H_2-list 中，其他 $\mathrm{ID}_j^*\in L$ 都存在于 H_1-list 和 H_2-list 中，否则失败退出。成功率的计算方式为

$$\begin{aligned}&\varepsilon=p\left[\neg\mathrm{abort}_k\right]\left[\neg\mathrm{abort}_s\right]\left[\neg\mathrm{abort}_{\mathrm{output}}\right]=\\&\varepsilon^{q_k}\varepsilon^{Nq_s}\varepsilon^{N-1}(1-\varepsilon)=\\&\varepsilon^{q_k+Nq_s+N-1}(1-\varepsilon)\end{aligned} \tag{6}$$

设 $f(\varepsilon)=\varepsilon^z(1-\varepsilon)$，$z=q_k+N(q_s+1)$，$f(\varepsilon)$ 的最大值为 $\varepsilon_{\max}=\dfrac{z}{z+1}$，所以

$$\begin{aligned}&f(\varepsilon_{\max})=\left(\frac{z}{z+1}\right)^z\left(1-\frac{z}{z+1}\right)=\\&\left(1+\frac{1}{z+1}\right)^{-z}\left(\frac{1}{z+1}\right)\geqslant \mathrm{e}^{-1}\frac{1}{z+1}\end{aligned} \tag{7}$$

所以 $\varepsilon'\geqslant\dfrac{1}{\mathrm{e}\left(q_k+N(q_s+1)+1\right)}$

D 所用的时间为

$t'<t+(q_h+q_k+q_p+q_v+q_c+q_s)t_{\mathrm{sm}}$

证毕。

定理 2　在随机预言模型下，如果存在敌手 A_2 能够在时间 t 内进行 H_1 询问、H_2 询问、H_3 询问、密钥生成询问和签名询问，然后以不可忽略的概率 ε 伪造出签名，那么存在一个算法 B 能够在时间 $t'<t+(q_h+q_k+q_p+q_v+q_c+q_s)t_{\mathrm{sm}}$ 内以 $\varepsilon'\geqslant\dfrac{1}{\mathrm{e}\left(q_k+N(q_s+1)+1\right)}$ 的优势解决 CDH 问题，其中 t_{sm} 表示群上标量乘法的计算时间。

证明　过程与定理 1 相同，此处不再赘述。

6　效率分析

为了更好地评估有序聚合签名方案，本文还考虑了协议的计算开销等效率问题。本文将签名的生成和查验分为单个签名生成、聚合签名生成和聚合签名验证这 3 个部分。不同方案计算时间开销对比如表 1 所示。由表 1 可知，本文方案在聚合签名生成部分具有明显优势。因为本文方案中每个用户需要在上一轮签名的基础上进行计算，签名的计算开销也分担到每个用户的计算中，为聚合节点分担了计算开销，所以本文方案具有更高的计算效率，并且适合在多用户参与的应用环境下使用。为了便于比较，本文将双线性对运算时间记为 BP，椭圆曲线 G 上的标量点乘运算时间记为 SM，G 上的标量点加运算时间记为 P，G_T 上的乘法运算时间记为 E，多个用户参与时间开销记为 n。

表 1　不同方案计算时间开销对比

方案	单个签名生成	聚合签名生成	聚合签名验证
文献[23]方案	3BP+SM+2P+3E	nP+nE	(n+2)BP+nSM+nP
文献[13]方案	3BP+5E+3P	2nP	3BP+(2n+1)P+2nE
文献[24]方案	3BP+2P+3E	nP	3BP+3nP+nE
文献[25]方案	4BP+3E+2P	2nP+nE	4BP+2nP
文献[26]方案	3BP+P+4E	2nP	3BP+2nE
文献[27]方案	2BP+5P+5E	3nP	2BP+(3n+1)P+2nE
文献[28]方案	3P+2E	nP+nE	3BP+nE
本文方案	2E+5P	0	4BP

为了更加直观地展示本文方案与多种聚合签名方案在聚合签名生成阶段和聚合签名验证阶段的时间开销问题，本节对其进行了仿真实验。实验环境为 Intel E-2288G CPU，频率为 3.7 GHz，内存为 128 GB，采用 PBC 函数库。聚合签名生成和验证时间开销与消息数量的关系如图 2 所示。由图 2 可知，本文方案在聚合签名生成和验证时间开销方面具有显著的优势，相比于已有聚合签名方案，本文方案与文献[28]方案均大幅降低了聚合签名和验证时间开销。

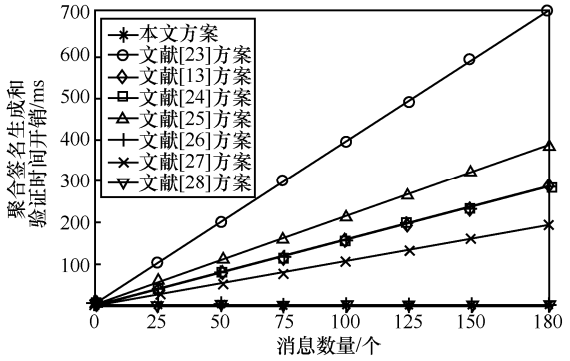

图 2 聚合签名生成和验证时间开销与消息数量的关系

7 结束语

对于多用户参与的分布式场景，本文方案在安全性和计算通信开销方面比普通签名方案更具优势。在安全性方面，本文方案不仅解决了证书分发和管理以及密码托管的安全问题，还确保了签名方案是存在性不可伪造的，并且添加了顺序安全约束，确保消息流转的顺序性。在效率方面，相比于完全聚合签名，有序聚合签名在每个节点都是在上一轮签名的基础上聚合了本轮签名，因此每个签名节点都分担了计算开销，减轻了单个聚合节点的负担；与同类的无证书聚合签名相比，本文方案聚合签名生成和验证时间开销更低，具有明显的优势。总体来看，本文方案具有可证明安全、通信代价小、计算成本低和验证时间短等优点，并且可在离线状态或者处于节点缓存能力与网络资源受限的容迟网络中进行查验，更适合多用户参与签名的网络环境。

参考文献：

[1] BONEH D, GENTRY C, LYNN B, et al. Aggregate and verifiably encrypted signatures from bilinear maps[C]//Lecture Notes in Computer Science. Berlin: Springer, 2003: 416-432.

[2] BOLDYREVA A, GENTRY C, O' NEILL A, et al. Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing[C]//Proceedings of the 14th ACM Conference on Computer and Communications Security. New York: ACM Press, 2007: 276-285.

[3] BANERJEE N, CORNER M D, LEVINE B N. An energy-efficient architecture for DTN throwboxes[C]//Proceedings of IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications. Piscataway: IEEE Press, 2007: 776-784.

[4] HA J. An efficient and robust anonymous authentication scheme in global mobility networks[J]. International Journal of Security and Its Applications, 2015, 9(10): 297-312.

[5] SHEN L M, MA J F, LIU X M, et al. A provably secure aggregate signature scheme for healthcare wireless sensor networks[J]. Journal of Medical Systems, 2016, 40(11): 244.

[6] LIU J K, BAEK J, ZHOU J Y. Certificate-based sequential aggregate signature[C]//Proceedings of the Second ACM Conference on Wireless Network Security. New York: ACM Press, 2009: 21-28.

[7] VERMA G K, SINGH B B. Short certificate-based proxy signature scheme from pairings[J]. Transactions on Emerging Telecommunications Technologies, 2017, 28(12): e3214.

[8] VERMA G K, SINGH B B, KUMAR N, et al. CB-CAS: certificate-based efficient signature scheme with compact aggregation for industrial Internet of things environment[J]. IEEE Internet of Things Journal, 2020, 7(4): 2563-2572.

[9] MURANAKA K, YANAI N, OKAMURA S, et al. ISDSR: secure DSR with ID-based sequential aggregate signature[C]//Proceedings of the 13th International Joint Conference on e-Business and Telecommunications. [S.l.]: SciTePress, 2016: 376-387.

[10] KOJIMA H, YANAI N, CRUZ J P. ISDSR: improving the security and availability of secure routing protocol[J]. IEEE Access, 2019, 7: 74849-74868.

[11] HORNG S J, TZENG S F, HUANG P H, et al. An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks[J]. Information Sciences, 2015, 317: 48-66.

[12] GAYATHRI N B, THUMBUR G, REDDY P V, et al. Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks[J]. IEEE Access, 2018, 6: 31808-31819.

[13] 刘丹, 石润华, 张顺, 等. 无线网络中基于无证书聚合签名的高效匿名漫游认证方案[J]. 通信学报, 2016, 37(7): 182-192.
LIU D, SHI R H, ZHANG S, et al. Efficient anonymous roaming authentication scheme using certificateless aggregate signature in wireless network[J]. Journal on Communications, 2016, 37(7): 182-192.

[14] KAMIL I A, OGUNDOYIN S O. An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks[J]. Journal of Information Security and Applications, 2019, 44: 184-200.

[15] ZHAO Y N, HOU Y Z, WANG L L, et al. An efficient certificateless aggregate signature scheme for the Internet of vehicles[J]. Transactions on Emerging Telecommunications Technologies, 2020, 31(5): e3708.

[16] XIE J, HU Y P, GAO J T, et al. Certificateless sequential aggregate signature scheme on NTRU lattice[J]. Chinese Journal of Electronics, 2019, 28(2): 294-300.

[17] CAHYADI E F, HWANG M S. A comprehensive survey on certificateless aggregate signature in vehicular ad hoc networks[J]. IETE Technical Review, 2022: doi.org/10.1080/02564602.2021.2017800.

[18] GALBRAITH S D, PATERSON K G, SMART N P. Pairings for cryptographers[J]. Discrete Applied Mathematics, 2008, 156(16): 3113-3121.

[19] LYSYANSKAYA A, MICALI S, REYZIN L, et al. Sequential aggregate signatures from trapdoor permutations[C]//Advances in Cryptology - EUROCRYPT 2004. Berlin: Springer, 2004: 74-90.

[20] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[C]//Advances in Cryptology - ASIACRYPT 2001. Berlin: Springer, 2001: 514-532.

[21] SHIM K A. Security models for certificateless signature schemes revisited[J]. Information Sciences, 2015, 296: 315-321.

[22] CUI J, ZHANG J, ZHONG H, et al. An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks[J]. Information Sciences, 2018, 451/452: 1-15.

[23] 秦艳琳, 吴晓平. 高效的无证书有序多重签名方案[J]. 通信学报, 2013, 34(7): 105-110.
QIN Y L, WU X P. Efficient certificateless sequential multi-signature scheme[J]. Journal on Communications, 2013, 34(7): 105-110.

[24] 许芷岩, 吴黎兵, 李莉, 等. 新的无证书广义指定验证者聚合签名方案[J]. 通信学报, 2017, 38(11): 76-83.
XU Z Y, WU L B, LI L, et al. New certificateless aggregate signature scheme with universal designated verifier[J]. Journal on Communications, 2017, 38(11): 76-83.

[25] 张玉磊, 周冬瑞, 李臣意, 等. 高效的无证书广义指定验证者聚合签名方案[J]. 通信学报, 2015, 36(2): 52-59.
ZHANG Y L, ZHOU D R, LI C Y, et al. Certificateless-based efficient aggregate signature scheme with universal designated verifier[J]. Journal on Communications, 2015, 36(2): 52-59.

[26] MEI Q, XIONG H, CHEN J H, et al. Efficient certificateless aggregate signature with conditional privacy preservation in IoV[J]. IEEE Systems Journal, 2021, 15(1): 245-256.

[27] WANG H W, WANG L L, ZHANG K, et al. A conditional privacy-preserving certificateless aggregate signature scheme in the standard model for VANETs[J]. IEEE Access, 2022, 10: 15605-15618.

[28] 张振超. 可证明安全的无证书签名方案研究[D]. 扬州: 扬州大学, 2021.
ZHANG Z C. Research on provably secure certificateless signature scheme[D]. Yangzhou: Yangzhou University, 2021.

[作者简介]

王竹（1972− ），女，山西太原人，博士，中国科学院信息工程研究所研究员，主要研究方向为密码理论与技术。

杨思琦（1997− ），女，四川绵阳人，中国科学院信息工程研究所硕士生，主要研究方向为信息安全、安全协议。

李凤华（1966− ），男，湖北浠水人，博士，中国科学院信息工程研究所研究员、博士生导师，主要研究方向为网络与系统安全、大数据安全与隐私保护、密码工程。

耿魁（1989− ），男，湖北红安人，博士，中国科学院信息工程研究所高级工程师、硕士生导师，主要研究方向为网络安全、信息保护。

彭婷婷（1998− ），女，河南信阳人，中国科学院信息工程研究所博士生，主要研究方向为信息安全。

史梦瑶（1998− ），女，河南许昌人，中国科学院信息工程研究所硕士生，主要研究方向为安全协议理论与设计。