软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(12):3204−3214 [doi: 10.13328/j.cnki.jos.004830]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

高效可证安全的无证书聚合签名方案*

周彦伟[1,2,3], 杨 波[1,2,3], 张文政[2]

[1](陕西师范大学 计算机科学学院,陕西 西安 710062)

[2](国家保密通信重点实验室,四川 成都 610041)

[3](信息安全国家重点实验室(中国科学院 信息工程研究所),北京 100093)

通讯作者: 杨波, E-mail: byang@snnu.edu.cn

摘 要: 由于现有聚合签名方案多数是基于双线性映射构造,存在计算效率低的不足.针对不同的网络环境,提出了2种不使用双线性映射的无证书聚合签名方案CLAS-I和CLAS-II,并在随机预言机模型下,基于离散对数困难问题证明了方案的不可伪造性;同时,分析了该方案所具有的公开验证性等安全属性.与现有方案相比较,由于未使用双线性映射运算,该方案具有更高的计算效率.由于方案 CLAS-I 的聚合签名长度较长,将用于带宽较高的网络环境;CLAS-II 具有较短的签名长度,且长度与用户数无关,将用于带宽较低的网络环境.

关键词: 无证书聚合签名;随机预言机模型;无双线性映射;离散对数问题

中图法分类号: TP309

中文引用格式: 周彦伟,杨波,张文政.高效可证安全的无证书聚合签名方案.软件学报,2015,26(12):3204−3214. http://www.jos.org.cn/1000-9825/4830.htm

英文引用格式: Zhou YW, Yang B, Zhang WZ. Efficient and provide security certificateless aggregate signature scheme. Ruan Jian Xue Bao/Journal of Software, 2015,26(12):3204−3214 (in Chinese). http://www.jos.org.cn/1000-9825/4830.htm

Efficient and Provide Security Certificateless Aggregate Signature Scheme

ZHOU Yan-Wei[1,2,3], YANG Bo[1,2,3], ZHANG Wen-Zheng[2]

[1](School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

[2](Science and Technology on Communication Security Laboratory, Chengdu 610041, China)

[3](State Key Laboratory of Information Security (Institute of Information Engineering, the Chinese Academy of Sciences), Beijing 100093, China)

Abstract: Almost all existing aggregate signature schemes are based on bilinear pairing which leads to high computational cost. In order to solve this problem under different network environment, two new certificateless aggregate signature schemes without bilinear pairing CLAS-I and CLAS-II are proposed in this paper. The proposed schemes are provably unforgeable in the random oracle model under the discrete logarithm assumption, and also have the security properties of public verifiability. Moreover, compared with other existing aggregate signature schemes in the computationally complexity, the proposal are more efficient. Meanwhile, the scheme CLAS-I can be used for high bandwidth network environment because the length of signature is long, and the scheme CLAS-II can be used in a narrow

* 基金项目: 国家自然科学基金(61272436, 61402275, 61303092, 61572303); 中国科学院信息工程研究所信息安全国家重点实验室开放课题(2015-MS-10); 保密通信重点实验室基金(9140C110206140C11050); 陕西省自然科学基金(2014JQ8309); 中央高校基本科研业务费专项资金(GK201504016, GK20130205); 陕西师范大学优秀博士论文资助项目(X2014YB01)

Foundation item: National Natural Science Foundation of China (61272436, 61402275, 61303092, 61572303); Foundation of State Key Laboratory of Information Security, IIE CAS (2015-MS-10); Foundation of Science and Technology on Communication Security Laboratory (9140C110206140C11050); National Natural Science Foundation of Shaanxi Province (2014JQ8309); Fundamental Research Funds for the Central Universities (GK201504016, 20130205)

收稿时间: 2014-12-19; 修改时间: 2015-02-15; 定稿时间: 2015-03-14

bandwidth network environment since it is the shortest certificateless aggregate signature and the number of users does not correlate to the length of the signatures generated by CLAS-II,.

Key words: certificateless aggregate signature; random oracle model; without bilinear pairing; discrete logarithm problem

Shamir 于 1984 年提出基于身份的公钥密码体制(ID-PKC)[1],改进了传统公钥密码体制中公钥证书的管理问题.在 ID-PKC 体制中,用户的身份信息(如电话号码、姓名、电子邮件等)直接被作为公钥使用,而用户私钥由可信第三方——密钥生成中心(key generation center,简称 KGC)提供.由于公钥无需与证书绑定,使得 ID-PKC 成为密码学领域的研究热点之一,目前已有很多基于身份的加密、签名方案相继被提出.但是由于 KGC 生成了用户私钥,使得 KGC 具有伪造任意用户的合法签名或替代任意用户进行签名验证的能力,即:ID-PKC 存在密钥托管的不足,该不足制约了 ID-PKC 在实际生活中的应用.Al-Riyami 和 Paterson 于 2003 年提出无证书公钥密码系统(CL-PKC)[2],减少了对 KGC 的依赖.在 CL-PKC 中,用户基于 KGC 计算的部分私钥和自身随机选取的秘密值生成用户完整的私钥;公钥由用户的秘密值、身份和系统参数计算得出.因此,CL-PKC 克服了 ID-PKC 中用户密钥托管的问题,也消除了传统公钥密码学中公钥证书的复杂性管理问题,提高了密码系统的运行效率.

聚合签名的概念是由 Boneh 等人[3]在 2003 年提出的,是一种具有广阔应用前景的关键签名密码技术,对许多应用都有良好的支撑作用.聚合签名可同时给多个消息、多个用户提供不可否认服务,也可把任意多个用户的签名压缩成一个签名.因此,聚合签名既降低了签名的存储空间,也降低了对签名传输网络带宽的要求.同时,将任意多个签名的验证简化为一次验证,也降低了签名验证的工作量[4].

近年来,国内外学者对聚合签名领域进行了深入研究.在 CL-PKC 的基础上,已有若干无证书聚合签名(certificateless aggregate signature,简称 CLAS)方案[5−19]相继被提出.文献[5]构造了两个 CLAS 方案,但在方案 I 中,聚合签名的长度随签名用户数的增加而变长,并且签名的验证计算量较大;由于签名验证阶段验证者需要计算(n+2)个耗时的双线性运算,导致方案 II 存在运行效率低的缺点.并且这两个方案的安全性证明均是在较弱的敌手模型假设下进行的,其安全性有待进一步检测.在文献[6]中,因为验证者需计算(n+3)个双线性运算才能完成签名的合法性验证,致使该方案存在运行效率低的不足.文献[7]在文献[6]的基础上提出了相应的改进方案,与文献[6]中的方案相比较,该方案提高了运行效率,但仍存在下述不足:① 为用户生成部分私钥时,KGC 需要额外增加 2 个群元素;② 为完成签名,需要签名用户维护一个共同的状态信息.文献[8,9]分别提出基于身份的聚合签名方案和具有常数次双线性运算的聚合签名方案,各方案中均需进行双线性映射运算,具有较高的计算效率.但文献[10]发现文献[8,9]中的方案均存在安全性缺陷,在对原始方案进行安全性分析的基础上,文献[10]分别构造了针对上述方案的攻击算法.文献[11]提出进行常数次双线性运算,且签名长度固定的无证书聚合签名方案,并证明了方案的安全性.但文献[12]发现文献[11]中方案存在安全性缺陷,并在安全性分析的基础上构造了具体的安全性攻击算法.文献[13]提出新的进行常数次双线性运算的无证书聚合签名方案,同时对方案的安全性进行了证明.但文献[14,15]均发现文献[13]中的无证书聚合签名方案无法满足其所声称的安全性,在安全性分析的基础上,分别构造了对文献[13]方案安全性的具体攻击算法.文献[16−19]分别基于双线性映射提出了相应的聚合签名方案.

文献[5−7]分别提出了相应的无证书聚合签名方案,但是各方案中均使用了双线性映射运算,导致相关方案存在计算负载高的不足.虽然文献[8,9,11,13]提出的聚合签名方案具有较高的计算效率,但遗憾的是,上述方案均存在安全性缺陷[10,12,14,15].相较于文献[5−7]而言,文献[16]具有聚合签名长度短和验证效率高的优点,但该方案中,签名合法性验证阶段要进行 4 次双线性映射运算,由于双线性映射运算具有较高的计算量[20],所以该方案的高效性是相对而言的.文献[17−19]中,聚合签名的长度较长,并且计算效率较低.由于现有的聚合签名方案都是基于双线性映射构造,因此在不使用双线性映射的前提下进行聚合签名方案的设计,已成为聚合签名研究领域的热点问题.

针对不同网络环境对消息传输性能的要求,本文提出两种不使用双线性映射的无证书聚合签名方案,在随机预言机模型下,基于离散对数困难问题证明了方案的不可伪造性.相较与现有的无证书聚合签名方案而言,本文方案的签名及签名验证阶段无需进行双线性映射运算,具有更高的计算效率.方案 CLAS-I 的聚合签名较长,

将用于带宽较高的网络环境,方案 CLAS-II 具有较短的聚合签名长度,且长度与用户数无关,将用于带宽较低的网络环境.

1 基础知识

1.1 困难性假设

定义 1(离散对数(discrete logarithm,简称 DL)问题). 令 $q(q>2^k,k$ 为安全参数)是大素数,循环群 G 的阶为 q,P 是群 G 的生成元;给定 $P,bp\in G$,对于任意且未知的 $b\in Z_q^*$,DL 困难问题的目标是计算 b.

DL 假设. 定义概率多项式时间算法 $\mathcal{A}$ 解决 DL 问题的优势为 $Adv^{DL}(\mathcal{A})=\Pr[\mathcal{A}(P,bp)=b]$.对于任意的多项式时间算法 $\mathcal{A}$,优势 $Adv^{DL}(\mathcal{A})$ 都是可忽略的,则称之为满足 DL 假设.其中,概率来源于 b 在 Z_q^* 上的随机选取和算法 $\mathcal{A}$ 的随机选择.

1.2 聚合签名

定义 2. 聚合签名[4]是一种支持聚合特性的数字签名变体,即:给定 n 个用户 $U_{ID_i}\in U$ $(1\leqslant i\leqslant n,U$ 为用户集合),对消息 $m_i\in M(M$ 为消息集合)的 n 个签名,聚合签名的生成者可以将这 n 个签名聚合成一个唯一的短签名.并且,当给定该聚合签名,参与生成聚合签名用户 U_{ID_i} 的身份标识 ID_i 及其签名的原始消息 m_i 等相关信息时,可以使验证者确信是用户 U_{ID_i} 对消息 m_i 做的签名.

文献[4]详细介绍了聚合签名的工作原理及特点,并综述了聚合签名领域的研究现状;同时,在研究现状的基础上介绍了未来的研究方向.

1.3 无证书聚合签名方案及安全模型

无证书聚合签名方案[16]由算法 Setup(初始化)、PartialPrivateExtract(部分密钥提取)、UserKeyGen(用户密钥生成)、Sign(签名)、Aggregate(聚合)和 Verify(验证)构成.聚合签名方案的合法参与者有 KGC、用户 U_{ID_i} $(1\leqslant i\leqslant n)$、聚合签名者 U_{Agg} 和签名验证者 U_{Ver},对各算法功能的介绍详见文献[16].本文方案中将算法 PartialPrivateExtract 和 UserKeyGen 的功能集成到算法 KeyGen(密钥生成)中实现.

参照文献[7]所定义的安全模型,无证书聚合签名方案将面临 $\mathcal{A}_{\mathrm{I}}$ 和 $\mathcal{A}_{\mathrm{II}}$ 两类敌手的不可伪造性攻击.

$\mathcal{A}_{\mathrm{I}}$ 类敌手无法掌握系统的主密钥,但其具有替换合法用户公钥的能力,则 $\mathcal{A}_{\mathrm{I}}$ 类敌手为恶意的用户.本文中,敌手 $\mathcal{A}_1$ 即为 $\mathcal{A}_{\mathrm{I}}$ 类敌手.

$\mathcal{A}_{\mathrm{II}}$ 类敌手可掌握系统的主密钥,但其不具有替换合法用户公钥的能力,则 $\mathcal{A}_{\mathrm{II}}$ 类敌手为恶意的 KGC.本文中,敌手 $\mathcal{A}_2$ 即为 $\mathcal{A}_{\mathrm{II}}$ 类敌手.

文献[7]详细介绍了无证书聚合签名方案在 $\mathcal{A}_{\mathrm{I}}$ 和 $\mathcal{A}_{\mathrm{II}}$ 两类敌手适应性选择消息攻击下不可伪造性的定义及相应的游戏,本文不再赘述,安全模型及游戏的具体定义见文献[7].

2 无双线性映射的无证书聚合签名方案

2.1 无证书聚合签名方案I(CLAS-I)

2.1.1 初始化(setup)

KGC 执行下述操作:

① 定义阶为素数 $q(q>2^k,k$ 为安全参数)的循环群 G,P 为群 G 的一个生成元;

② 定义抗碰撞的安全哈希函数: $H_1:\{0,1\}^{L_1}\times G\times G\to Z_q^*,H_2:\{0,1\}^{L_1}\times\{0,1\}^{L_2}\times G\to Z_q^*$,其中,$L_1$ 为用户身份标识的长度,L_2 为消息长度;

③ 随机选取主密钥 $s\in Z_q^*$,计算系统公钥 $P_{Pub}=sP$,公开参数 $Params=\langle q,P,G,P_{Pub},H_1,H_2\rangle$,并秘密保存主密钥 s.

2.1.2 密钥生成(KeyGen)

用户 U_{ID_i} 的密钥生成过程如下:

① U_{ID_i} 随机选取秘密值 $x_{ID_i} \in Z_q^*$,计算公开参数 $X_{ID_i} = x_{ID_i}P$,发送身份标识 ID_i 和公开参数 X_{ID_i} 给密钥生成中心 KGC;

② 给定用户 U_{ID_i} 的身份标识 ID_i 及公开参数 X_{ID_i},KGC 随机选取秘密数 $r_{ID_i} \in Z_q^*$,计算 $Y_{ID_i} = r_{ID_i}P$ 和 $y_{ID_i} = r_{ID_i} + sH_1(ID_i, X_{ID_i}, Y_{ID_i})$,通过已认证的安全信道将 y_{ID_i} 和 Y_{ID_i} 返回给用户 U_{ID_i},其中 y_{ID_i} 为 U_{ID_i} 的部分私钥,Y_{ID_i} 为 U_{ID_i} 的部分公钥;

③ U_{ID_i} 通过验证等式 $y_{ID_i}P = Y_{ID_i} + P_{Pub}H_1(ID_i, X_{ID_i}, Y_{ID_i})$ 是否成立,完成对 KGC 生成的部分私钥及公钥的正确性验证,则 U_{ID_i} 的公私钥分别为 $PK_{ID_i} = \langle X_{ID_i}, Y_{ID_i} \rangle$ 和 $SK_{ID_i} = \langle x_{ID_i}, y_{ID_i} \rangle$.

2.1.3 聚合签名(aggregate signature)

(1) 用户 U_{ID_i} ($1 \leqslant i \leqslant n$)对消息 m_i 进行签名,并将生成的签名 σ_{ID_i} 发送给聚合签名者 U_{Agg};

用户 U_{ID_i} 随机选取秘密数 $a_{ID_i} \in Z_q^*$,计算 $V_{ID_i} = a_{ID_i}P, h_{ID_i}^2 = H_2(ID_i, m_i, V_{ID_i})$ 和 $S_{ID_i} = a_{ID_i} + (x_{ID_i} + y_{ID_i})h_{ID_i}^2$,生成签名 $\sigma_{ID_i} = \langle V_{ID_i}, S_{ID_i} \rangle$.

(2) U_{Agg} 收到 U_{ID_i} ($1 \leqslant i \leqslant n$)关于消息 m_i 的签名 $\sigma_{ID_i} = \langle V_{ID_i}, S_{ID_i} \rangle$ 后,分别计算 $h_{ID_i}^1 = H_2(ID_i, X_{ID_i}, Y_{ID_i})$ 和 $h_{ID_i}^2 = H_2(ID_i, m_i, V_{ID_i})$,当且仅当 $S_{ID_i}P = V_{ID_i} + h_{ID_i}^2(X_{ID_i} + Y_{ID_i} + P_{Pub}h_{ID_i}^1)$ 成立时,U_{Agg} 接收 U_{ID_i} 对 m_i 的签名 σ_{ID_i}.

因为: $S_{ID_i}P = (a_{ID_i} + (x_{ID_i} + y_{ID_i})h_{ID_i}^2)P = V_{ID_i} + h_{ID_i}^2(X_{ID_i} + Y_{ID_i} + P_{Pub}h_{ID_i}^1)$;其中, $y_{ID_i} = r_{ID_i} + sh_{ID_i}^1$.

当用户 U_{ID_i} ($1 \leqslant i \leqslant n$)关于消息 m_i 的签名 σ_{ID_i} 的合法性验证都通过后,U_{Agg} 生成聚合签名 σ:构造集合 $V=\{V_1, V_2, \ldots, V_n\}$,并计算 $S = \sum_{i=1}^n S_{ID_i}$,则 $\sigma=(V,S)$ 是 U_{Agg} 关于身份-消息-公钥对 $(ID_i, m_i, PK_{ID_i})(1 \leqslant i \leqslant n)$ 的聚合签名.

2.1.4 聚合签名验证(AS-verify)

给定身份-消息-公钥对 $(ID_i, m_i, PK_{ID_i})(1 \leqslant i \leqslant n)$ 及聚合签名 $\sigma=(V,S)$,签名验证者 U_{Ver} 进行如下操作:

① 对于每个签名者 U_{ID_i} ($1 \leqslant i \leqslant n$),计算 $h_{ID_i}^1 = H_2(ID_i, X_{ID_i}, Y_{ID_i})$ 和 $h_{ID_i}^2 = H_2(ID_i, m_i, V_{ID_i})$;

② 验证等式 $SP = \sum_{i=1}^n [V_{ID_i} + h_{ID_i}^2(X_{ID_i} + Y_{ID_i} + P_{Pub}h_{ID_i}^1)]$ 是否成立:若成立,则接收签名 $\sigma=(V,S)$,输出 True,表明 $\sigma=(V,S)$ 是 U_{Agg} 关于身份-消息-公钥对 $(ID_i, m_i, PK_{ID_i})(1 \leqslant i \leqslant n)$ 的聚合签名;否则拒绝,并输出 False.

因为: $SP = \sum_{i=1}^n S_{ID_i}P = \sum_{i=1}^n (a_{ID_i} + (x_{ID_i} + y_{ID_i})h_{ID_i}^2)P = \sum_{i=1}^n [V_{ID_i} + h_{ID_i}^2(X_{ID_i} + Y_{ID_i} + P_{Pub}h_{ID_i}^1)]$.

2.2 无证书聚合签名方案II(CLAS-II)

方案 CLAS-II 的初始化算法和密钥生成算法与方案 CLAS-I 的 Setup 和 KeyGen 算法相同,并且在该方案中,各参与者基于认证的安全信道进行相关信息的共享.

2.2.1 聚合签名(aggregate signature)

(1) 用户 U_{ID_i} ($1 \leqslant i \leqslant n$)对消息 m_i 进行签名,并将生成的签名 σ_{ID_i} 发送给聚合者 U_{Agg};同时,各用户间进行相关信息的共享.

用户 U_{ID_i} 随机选取秘密数 $a_{ID_i} \in Z_q^*$, 计算共享信息 $V_{ID_i} = a_{ID_i}P$, 并将 V_{ID_i} 发送给其他的 $n-1$ 个用户 U_{ID_j} ($1 \leqslant j \leqslant n, j \neq i$); 当 U_{ID_i} 收到其他 $n-1$ 个用户 U_{ID_j} 的共享信息 V_{ID_j} 后,首先计算 $V = \sum_{i=1}^n V_{ID_i}$, 然后计算 $h_{ID_i}^2 = H_2(ID_i, m_i, V)$ 和 $S_{ID_i} = a_{ID_i} + (x_{ID_i} + y_{ID_i})h_{ID_i}^2$, 生成签名 $\sigma_{ID_i} = \langle V, V_{ID_i}, S_{ID_i} \rangle$.

(2) U_{Agg} 收到 U_{ID_i} ($1 \leqslant i \leqslant n$)关于消息 m_i 的签名 $\sigma_{ID_i} = \langle V, V_{ID_i}, S_{ID_i} \rangle$ 后,首先计算 $V' = \sum_{i=1}^n V_{ID_i}$,若 $V'=V$,则 U_{Agg} 计算 $h_{ID_i}^1 = H_2(ID_i, X_{ID_i}, Y_{ID_i})$ 和 $h_{ID_i}^2 = H_2(ID_i, m_i, V)$,当且仅当 $S_{ID_i}P = V_{ID_i} + h_{ID_i}^2(X_{ID_i} + Y_{ID_i} + P_{Pub}h_{ID_i}^1)$ 成立时,U_{Agg} 接收 U_{ID_i} 对消息 m_i 的签名 σ_{ID_i};否则,U_{ID_i} 关于消息 m_i 的签名 σ_{ID_i} 在生成过程中出现错误,则 U_{Agg} 要求 U_{ID_i} ($1 \leqslant i \leqslant n$)重新生成对相应消息 m_i 的签名 σ_{ID_i}. 当 U_{ID_i} ($1 \leqslant i \leqslant n$)关于消息 m_i 的签名 σ_{ID_i} 的合法性验证都通过后,

计算 $S=\sum_{i=1}^{n}S_{ID_i}$,则σ=(V,S)是 U_{Agg} 关于身份-消息-公钥对 $(ID_i,m_i,\langle X_{ID_i},Y_{ID_i}\rangle)(1\leqslant i\leqslant n)$ 的聚合签名.

2.2.2 聚合签名验证(AS-verify)

给定身份-消息-公钥对 $(ID_i,m_i,PK_{ID_i})(1\leqslant i\leqslant n)$ 及聚合签名σ=(V,S),签名验证者 U_{Ver} 进行如下操作:

① 对于每个签名者 U_{ID_i} $(1\leqslant i\leqslant n)$,计算 $h_{ID_i}^1=H_2(ID_i,X_{ID_i},Y_{ID_i})$ 和 $h_{ID_i}^2=H_2(ID_i,m_i,V)$;

② 验证等式 $SP=V+\sum_{i=1}^{n}h_{ID_i}^2(X_{ID_i}+Y_{ID_i}+P_{Pub}h_{ID_i}^1)$ 是否成立:若成立则输出 True,表明σ=(V,S)是 U_{Agg} 关于身份-消息-公钥对 $(ID_i,m_i,PK_{ID_i})(1\leqslant i\leqslant n)$ 的聚合签名;否则拒绝,并输出 False.

因为:

$$\begin{aligned}SP&=\sum_{i=1}^{n}S_{ID_i}P\\&=\sum_{i=1}^{n}(a_{ID_i}+(x_{ID_i}+y_{ID_i})h_{ID_i}^2)P\\&=\sum_{i=1}^{n}a_{ID_i}P+\sum_{i=1}^{n}(x_{ID_i}+y_{ID_i})h_{ID_i}^2P\\&=\sum_{i=1}^{n}V_{ID_i}+\sum_{i=1}^{n}h_{ID_i}^2(X_{ID_i}+Y_{ID_i}+P_{Pub}h_{ID_i}^1)\\&=V+\sum_{i=1}^{n}h_{ID_i}^2(X_{ID_i}+Y_{ID_i}+P_{Pub}h_{ID_i}^1).\end{aligned}$$

3 安全性证明

本节在随机预言机模型下,基于离散对数问题对方案 CLAS-I 和 CLAS-II 的不可伪造性进行证明.

引理 1. 在随机预言机模型下,若存在$\mathcal{A}_I$类敌手$\mathcal{A}_1$能在多项式时间内,以不可忽略的优势ε攻破本文聚合签名方案 CLAS-I 的不可伪造性(其中,$\mathcal{A}_1$最多进行 q_S 次签名询问、q_K 次部分密钥生成询问和 q_{SK} 次私钥生成询问,聚合签名的用户数为 n),则存在算法$\mathcal{T}_1$,能在多项式时间内以不可忽略的优势 $Adv(\mathcal{T}_1)\geqslant\left(1-\frac{q_K}{2^k}\right)\left(1-\frac{q_{SK}}{2^k}\right)\frac{\varepsilon}{ne(q_S+n)}$(其中,$e$ 是自然对数底数)成功解决离散对数问题.

证明:假设算法$\mathcal{T}_1$ 是一个离散对数问题的解决者,输入为元组(P,bP),其中 $b\in Z_q^*$ 且未知,目标是计算 b.$\mathcal{T}_1$ 以 $\mathcal{A}_1$ 为子程序并充当挑战者,$\mathcal{T}_1$ 运行 Setup 算法,生成公开参数 $Params=\langle q,P,G,P_{Pub},H_1,H_2\rangle$,令 $P_{Pub}=bP$,并发送 $Params$ 给$\mathcal{A}_1$,同时,$\mathcal{T}_1$ 维护列表 $\boldsymbol{L}_1,\boldsymbol{L}_2,\boldsymbol{L}_K,\boldsymbol{L}_{SK},\boldsymbol{L}_{PK},\boldsymbol{L}_S$ 分别用于跟踪$\mathcal{A}_1$ 对预言机 $\boldsymbol{H}_1$、预言机 $\boldsymbol{H}_2$、部分密钥生成、私钥生成、公钥生成和签名的询问.开始时,各列表均为空.$\mathcal{T}_1$ 选择身份 ID_j(询问阶段对 q_S 个身份进行签名询问,挑战阶段生成 n 个用户的聚合签名)作为其猜测的挑战身份,则$\mathcal{T}_1$ 选择身份 ID_j 的概率为 $\delta\in\left[\frac{1}{q_S+n},\frac{1}{q_S+1}\right]$.

询问阶段:敌手$\mathcal{A}_1$ 进行下述询问:

$\boldsymbol{H}_1$ 查询:当$\mathcal{A}_1$ 向预言机 $\boldsymbol{H}_1$ 询问 $H_1(ID_i,X_{ID_i},Y_{ID_i})$ 时,$\mathcal{T}_1$ 进行下述操作:

① 若列表 $\boldsymbol{L}_1$ 中存在相应的元组$\langle ID_i,X_{ID_i},Y_{ID_i},h_1\rangle$,则$\mathcal{T}_1$ 返回 h_1 给$\mathcal{A}_1$;

② 否则,$\mathcal{T}_1$ 随机选取 $h_1\in Z_q^*$,使得 $\boldsymbol{L}_1$ 中不存在相应的元组$\langle *,*,*,h_1\rangle$(避免哈希函数 H_1 碰撞的产生),并添加相应的元组 $\langle ID_i,X_{ID_i},Y_{ID_i},h_1\rangle$ 到 $\boldsymbol{L}_1$ 中,同时返回 h_1 给$\mathcal{A}_1$.

$\boldsymbol{H}_2$ 查询:当$\mathcal{A}_1$ 向预言机 $\boldsymbol{H}_2$ 询问 $H_2(ID_i,m_i,V_{ID_i})$ 时,$\mathcal{T}_1$ 进行下述操作:

① 若列表 $\boldsymbol{L}_2$ 中存在相应的元组$\langle ID_i,m_i,V_{ID_i},h_2\rangle$,则返回 h_2 给$\mathcal{A}_1$;

② 否则,$\mathcal{T}_1$ 随机选取 $h_2\in Z_q^*$,使得列表 $\boldsymbol{L}_2$ 中不存在元组$\langle *,*,*,h_2\rangle$,并添加元组 $\langle ID_i,m_i,V_{ID_i},h_2\rangle$ 到 $\boldsymbol{L}_2$ 中,同时返回 h_2 给$\mathcal{A}_1$.

部分密钥生成询问:当收到$\mathcal{A}_1$ 对 ID_i 和公开参数 X_{ID_i} 的部分密钥生成询问时,$\mathcal{T}_1$ 进行下述操作:

① 若列表 $\boldsymbol{L}_K$ 中存在相应的元组$\langle ID_i,y_{ID_i},Y_{ID_i}\rangle$,则返回相应的值 (y_{ID_i},Y_{ID_i}) 给$\mathcal{A}_1$;

② 否则,若 $ID_i \neq ID_j$,$\mathcal{T}_1$ 随机选取 $y_{ID_i}, h_1 \in Z_q^*$,计算 $Y_{ID_i} = y_{ID_i}P - P_{Pub}h_1$,添加元组 $\langle ID_i, y_{ID_i}, Y_{ID_i}\rangle$ 到 $\boldsymbol{L}_K$ 中,返回 (y_{ID_i}, Y_{ID_i}) 给 $\mathcal{A}_1$,若列表 $\boldsymbol{L}_1$ 中不存在相应的元组,则添加元组 $\langle ID_i, X_{ID_i}, Y_{ID_i}, h_1\rangle$ 到 $\boldsymbol{L}_1$ 中;若 $ID_i = ID_j$,$\mathcal{T}_1$ 随机选取 $y_{ID_i}, h_1 \in Z_q^*$,令 $Y_{ID_j} = r_{know}P$ (其中,$r_{know} \in Z_q^*$ 是 $\mathcal{T}_1$ 已知的随机数),添加元组 $\langle ID_j, y_{ID_j}, Y_{ID_j}\rangle$ 到列表 $\boldsymbol{L}_K$ 中,返回 (y_{ID_j}, Y_{ID_j}) 给 $\mathcal{A}_1$,若列表 $\boldsymbol{L}_1$ 中不存在相应的元组,则添加元组 $\langle ID_i, X_{ID_i}, Y_{ID_i}, h_1\rangle$ 到 $\boldsymbol{L}_1$ 中.

私钥生成询问:当 $\mathcal{T}_1$ 收到 $\mathcal{A}_1$ 对 ID_i 的私钥生成询问时,$\mathcal{T}_1$ 进行下述操作:

① 若 $\boldsymbol{L}_{SK}$ 中存在元组 $\langle ID_i, x_{ID_i}, y_{ID_i}\rangle$,则返回相应的值 $SK_{ID_i} = (x_{ID_i}, y_{ID_i})$ 给 $\mathcal{A}_1$;

② 否则,$\mathcal{T}_1$ 随机选取 $x_{ID_i} \in Z_q^*$,计算 $X_{ID_i} = x_{ID_i}P$,通过对 ID_i 和 X_{ID_i} 进行部分密钥生成询问获知相应的元组 $\langle ID_i, y_{ID_i}, Y_{ID_i}\rangle$,添加元组 $\langle ID_i, x_{ID_i}, y_{ID_i}\rangle$ 到列表 $\boldsymbol{L}_{SK}$ 中,并返回 $SK_{ID_i} = (x_{ID_i}, y_{ID_i})$ 给 $\mathcal{A}_1$,同时添加元组 $\langle ID_i, X_{ID_i}, Y_{ID_i}\rangle$ 到列表 $\boldsymbol{L}_{PK}$ 中.

公钥生成查询:当收到 $\mathcal{A}_1$ 对身份 ID_i 的公钥生成询问时,$\mathcal{T}_1$ 进行下述操作:

① 若列表 $\boldsymbol{L}_{PK}$ 中存在元组 $\langle ID_i, X_{ID_i}, Y_{ID_i}\rangle$,则返回 $PK_{ID_i} = (X_{ID_i}, Y_{ID_i})$ 给 $\mathcal{A}_1$;

② 否则,$\mathcal{T}_1$ 随机返选取 $x_{ID_i} \in Z_q^*$,计算 $X_{ID_i} = x_{ID_i}P$,通过对 ID_i 和 X_{ID_i} 进行部分密钥生成询问获知相应的元组 $\langle ID_i, y_{ID_i}, Y_{ID_i}\rangle$,添加元组 $\langle ID_i, X_{ID_i}, Y_{ID_i}\rangle$ 到列表 $\boldsymbol{L}_{PK}$ 中,并返回 $PK_{ID_i} = (X_{ID_i}, Y_{ID_i})$ 给 $\mathcal{A}_1$,同时添加元组 $\langle ID_i, x_{ID_i}, y_{ID_i}\rangle$ 到列表 $\boldsymbol{L}_{SK}$ 中.

公钥替换询问:$\mathcal{A}_1$ 可选择一个新的公钥 $PK'_{ID_i} = (X'_{ID_i}, Y'_{ID_i})$ 替换任意合法用户的原始公钥 PK_{ID_i}.

签名询问:当 $\mathcal{T}_1$ 收到 $\mathcal{A}_1$ 关于身份-消息-公钥 $\langle ID_i, m_i, PK_{ID_i}\rangle$ 的签名询问时,操作如下:

① 若 $ID_i = ID_j$,则 $\mathcal{T}_1$ 放弃,并终止模拟;

② 否则,$\mathcal{T}_1$ 随机选取秘密数 $a_{ID_i} \in Z_q^*$,计算 $V_{ID_i} = a_{ID_i}P, h_{ID_i}^2 = H_2(ID_i, m_i, V_{ID_i})$ 和 $S_{ID_i} = a_{ID_i} + (x_{ID_i} + y_{ID_i})h_{ID_i}^2$,生成签名 $\sigma_{ID_i} = \langle V_{ID_i}, S_{ID_i}\rangle$ 返回给敌手 $\mathcal{A}_1$.

聚合签名询问:当 $\mathcal{T}_1$ 收到 $\mathcal{A}_1$ 关于身份-消息-公钥对 $\langle ID_i, m_i, PK_{ID_i}\rangle (1 \leqslant i \leqslant n)$ 的聚合签名询问时,操作如下:

① 若对于所有的 $ID_i (1 \leqslant i \leqslant n)$,都有 $ID_i \neq ID_j$,则 $\mathcal{T}_1$ 对每个用户 $ID_i (1 \leqslant i \leqslant n)$ 随机选取秘密数 $a_{ID_i} \in Z_q^*$,计算 $V_{ID_i} = a_{ID_i}P, h_{ID_i}^2 = H_2(ID_i, m_i, V_{ID_i})$ 和 $S_{ID_i} = a_{ID_i} + (x_{ID_i} + y_{ID_i})h_{ID_i}^2$ 后,构造集合 $V=\{V_1, V_2, \ldots, V_n\}$,并计算 $S = \sum_{i=1}^{n} S_{ID_i}$,生成聚合签名 $\sigma=(V,S)$ 返回给 $\mathcal{A}_1$.

② 否则,$\mathcal{T}_1$ 放弃,并终止模拟.

签名验证询问:当 $\mathcal{T}_1$ 收到 $\mathcal{A}_1$ 关于身份-消息-签名 $\langle ID_i, m_i, \sigma_{ID_i}\rangle$ 的验证询问时,$\mathcal{T}_1$ 查询 $\boldsymbol{L}_{PK}$ 中是否存在 ID_i 所对应的元组:

① 若 $\boldsymbol{L}_{PK}$ 中存在 ID_i 所对应的元组且 $ID_i \neq ID_j$,则 $\mathcal{T}_1$ 计算 $h_{ID_i}^1 = H_2(ID_i, X_{ID_i}, Y_{ID_i})$ 和 $h_{ID_i}^2 = H_2(ID_i, m_i, V_{ID_i})$,并验证 $S_{ID_i}P = V_{ID_i} + h_{ID_i}^2(X_{ID_i} + Y_{ID_i} + P_{Pub}h_{ID_i}^1)$ 是否成立:若成立,则 $\mathcal{T}_1$ 返回 True 给 $\mathcal{A}_1$;否则,返回 False 给 $\mathcal{A}_1$;

② 若 $\boldsymbol{L}_{PK}$ 中存在 ID_i 所对应的元组且 $ID_i = ID_j$,则当 $\boldsymbol{L}_2$ 中存在 ID_i 相对应的元组 $\langle ID_i, m_i, V_{ID_i}, h_2\rangle$ 时,$\mathcal{T}_1$ 返回 True 给 $\mathcal{A}_1$;否则,返回 False 给 $\mathcal{A}_1$;

③ 若 $\boldsymbol{L}_{PK}$ 中不存在 ID_i 所对应的元组,则当 $\boldsymbol{L}_2$ 中存在 ID_i 相对应的元组 $\langle ID_i, m_i, V_{ID_i}, h_2\rangle$ 时,$\mathcal{T}_1$ 返回 True 给 $\mathcal{A}_1$;否则,返回 False 给 $\mathcal{A}_1$.

伪造:经过多项式有界次的上述询问后,$\mathcal{A}_1$ 输出关于身份-消息-公钥对 $\langle ID_i, m_i, PK_{ID_i}\rangle (1 \leqslant i \leqslant n)$ 聚合签名 $\sigma=(V,S)$,其中至少有一个 $ID_i (i \in [1,n])$ 未进行部分密钥生成询问和私钥生成询问,同时至少有一个 $m_i (i \in [1,n])$ 未进行签名询问.

① 若对于所有的 $ID_i (1 \leqslant i \leqslant n)$ 都有 $ID_i \neq ID_j$,则 $\mathcal{T}_1$ 放弃,并终止模拟;

② 否则(有一个 $ID_i (1 \leqslant i \leqslant n)$ 与 ID_j 相等),则 $\mathcal{T}_1$ 在列表 $\boldsymbol{L}_{PK}, \boldsymbol{L}_{SK}, \boldsymbol{L}_1$ 和 $\boldsymbol{L}_2$ 中查询身份 $ID_i (1 \leqslant i \leqslant n)$ 所对应的记录值,并验证等式 $SP = \sum_{i=1}^{n}[V_{ID_i} + h_{ID_i}^2(X_{ID_i} + Y_{ID_i} + P_{Pub}h_{ID_i}^1)]$ 是否成立:

- 若等式成立,则$\mathcal{T}_1$ 输出 $b=(h^1_{ID_j}h^2_{ID_j})^{-1}\{S-\sum_{i=1,i\neq j}^{n}[a_{ID_i}+h^2_{ID_i}(x_{ID_i}+y_{ID_i})]-a_{ID_j}-h^2_{ID_j}(x_{ID_j}+r_{know})\}$ 作为离散对数问题的有效解;
- 否则,$\mathcal{T}_1$ 没有解决离散对数问题.因为:

$$\begin{aligned}S&=\sum_{i=1}^{n}[a_{ID_i}+h^2_{ID_i}(x_{ID_i}+y_{ID_i})]\\&=\sum_{i=1,i\neq j}^{n}[a_{ID_i}+h^2_{ID_i}(x_{ID_i}+y_{ID_i})]+a_{ID_j}+h^2_{ID_j}(x_{ID_j}+y_{ID_j})\\&=\sum_{i=1,i\neq j}^{n}[a_{ID_i}+h^2_{ID_i}(x_{ID_i}+y_{ID_i})]+a_{ID_j}+h^2_{ID_j}(x_{ID_j}+r_{know}+bh^1_{ID_j}).\end{aligned}$$

若$\mathcal{A}_1$在询问阶段对$ID_i(1\leqslant i\leqslant n)$进行了部分密钥生成询问和私钥生成询问,则$\mathcal{T}_1$会终止模拟.事件$\mathcal{E}_1$表示至少存在一个 $ID_f(f\in[1,n])$未进行部分密钥生成询问和私钥生成询问,事件$\mathcal{E}_2$ 表示$\mathcal{T}_1$ 在签名询问时未终止.则有:

$$\Pr[\mathcal{E}_1]\geqslant\frac{1}{n}\left(1-\frac{q_K}{2^k}\right)\left(1-\frac{q_{SK}}{2^k}\right),\Pr[\mathcal{E}_2\mid\mathcal{E}_1]=(1-\sigma)^{q_S}.$$

因此,$\mathcal{T}_1$ 在询问阶段不终止的概率为 $\Pr[\mathcal{E}_1\wedge\mathcal{E}_2]=\Pr[\mathcal{E}_2\mid\mathcal{E}_1]\Pr[\mathcal{E}_1]\geqslant\frac{1}{n}\left(1-\frac{q_K}{2^k}\right)\left(1-\frac{q_{SK}}{2^k}\right)(1-\sigma)^{q_S}$.

事件$\mathcal{E}_3$ 表示算法$\mathcal{T}_1$ 在挑战阶段未终止,即,$\mathcal{A}_1$ 在挑战阶段伪造的聚合签名中包含身份 ID_j,则$\mathcal{T}_1$ 在挑战阶段不终止的概率为 $\Pr[\mathcal{E}_3]=\delta$.

在整个模拟过程中,$\mathcal{T}_1$ 不终止的概率至少为 $\frac{1}{n}\left(1-\frac{q_K}{2^k}\right)\left(1-\frac{q_{SK}}{2^k}\right)(1-\sigma)^{q_S}\delta$. 由于 $\delta\in\left[\frac{1}{q_S+n},\frac{1}{q_S+1}\right]$, 则当 q_S 足够大时, $(1-\sigma)^{q_S}$ 趋向于 e^{-1};因此,模拟过程中$\mathcal{T}_1$ 不终止的概率至少为 $\left(1-\frac{q_K}{2^k}\right)\left(1-\frac{q_{SK}}{2^k}\right)\frac{1}{ne(q_S+n)}$.

综上所述,若$\mathcal{T}_1$ 在模拟过程中未终止,并且$\mathcal{A}_1$ 以不可忽略的优势ε攻破了本文聚合签名方案 CLAS-I 的不可伪造性,则$\mathcal{T}_1$ 能以不可忽略的优势 $Adv(\mathcal{T}_1)\geqslant\left(1-\frac{q_K}{2^k}\right)\left(1-\frac{q_{SK}}{2^k}\right)\frac{\varepsilon}{ne(q_S+n)}$ 成功解决离散对数问题.

引理 2. 在随机预言机模型下,若存在一个$\mathcal{A}_{\mathrm{II}}$ 类敌手$\mathcal{A}_2$,能在多项式时间内,以不可忽略的优势ε攻破本文聚合签名方案 CLAS-I 的不可伪造性(其中,$\mathcal{A}_2$ 最多进行 q_S 次签名询问、q_K 次部分密钥生成询问和 q_{SK} 次私钥生成询问,聚合签名的用户数为 n),则存在算法$\mathcal{T}_2$,能在多项式时间内,以不可忽略的优势 $Adv(\mathcal{T}_2)\geqslant\left(1-\frac{q_K}{2^k}\right)\left(1-\frac{q_{SK}}{2^k}\right)\frac{\varepsilon}{ne(q_S+n)}$ (其中,e 是自然对数底数)成功解决离散对数问题.

证明:假设算法$\mathcal{T}_2$ 是一个离散对数问题的解决者,输入为元组(P,bP),其中,$b\in Z_q^*$ 且未知,目标是计算 b.$\mathcal{T}_2$ 以$\mathcal{A}_2$ 为子程序并充当挑战者,$\mathcal{T}_2$ 运行 Setup 算法,生成公开参数 $Params=\langle q,P,G,P_{Pub},H_1,H_2\rangle$和主密钥.发送 $Params$ 和主密钥给$\mathcal{A}_2$;同时,$\mathcal{T}_2$ 维持列表 $\boldsymbol{L}_1,\boldsymbol{L}_2,\boldsymbol{L}_K,\boldsymbol{L}_{SK},\boldsymbol{L}_{PK},\boldsymbol{L}_S$ 分别用于跟踪$\mathcal{A}_2$ 对预言机 $\boldsymbol{H}_1$、预言机 $\boldsymbol{H}_2$、部分密钥生成、私钥生成、公钥生成和签名的询问.开始时,各列表均为空.$\mathcal{T}_2$ 选择身份 ID_j 作为其猜测的挑战身份,则$\mathcal{T}_2$ 选择身份 ID_j 的概率为 $\delta\in\left[\frac{1}{q_S+n},\frac{1}{q_S+1}\right]$.

询问:敌手$\mathcal{A}_2$ 对预言机 $\boldsymbol{H}_1$、预言机 $\boldsymbol{H}_2$、私钥生成、公钥生成、签名和聚合签名询问的执行过程与引理 1 中的相应询问相同.

部分密钥生成询问:当收到$\mathcal{A}_2$ 对 ID_i 和公开参数 X_{ID_i} 的部分密钥生成询问时,$\mathcal{T}_2$ 进行下述操作:

① 若 $\boldsymbol{L}_K$ 中存在相应的元组 $\langle ID_i,y_{ID_i},Y_{ID_i}\rangle$, 则返回 (y_{ID_i},Y_{ID_i}) 给$\mathcal{A}_2$;

② 否则,若 $ID_i\neq ID_j$,$\mathcal{T}_2$ 随机选取 $y_{ID_i},h_1\in Z_q^*$, 计算 $Y_{ID_i}=y_{ID_i}P-P_{Pub}h_1$, 添加元组 $\langle ID_i,y_{ID_i},Y_{ID_i}\rangle$ 到列表 $\boldsymbol{L}_K$ 中,返回 (y_{ID_i},Y_{ID_i}) 给$\mathcal{A}_2$,同时添加 $\langle ID_i,X_{ID_i},Y_{ID_i},h_1\rangle$ 到 $\boldsymbol{L}_1$ 中;若 $ID_i=ID_j$,$\mathcal{T}_2$ 随机选取 $y_{ID_i},h_1\in Z_q^*$, 令 $Y_{ID_j}=bP$, 添加

$\langle ID_j, y_{ID_j}, Y_{ID_j}\rangle$ 到 $\boldsymbol{L}_K$ 中,返回 (y_{ID_j}, Y_{ID_j}) 给 $\mathcal{A}_2$,同时添加 $\langle ID_i, X_{ID_i}, Y_{ID_i}, h_1\rangle$ 到 $\boldsymbol{L}_1$ 中.

签名验证询问:当 $\mathcal{T}_2$ 收到 $\mathcal{A}_2$ 关于身份-消息-签名 $\langle ID_i, m_i, \sigma_{ID_i}\rangle$ 的验证询问时,$\mathcal{T}_2$ 查询 $\boldsymbol{L}_{PK}$ 中是否存在 ID_i 所对应的元组:

① 若 $\boldsymbol{L}_{PK}$ 中存在 ID_i 所对应的元组且 $ID_i \neq ID_j$,则 $\mathcal{T}_2$ 计算 $h^1_{ID_i} = H_2(ID_i, X_{ID_i}, Y_{ID_i})$ 和 $h^2_{ID_i} = H_2(ID_i, m_i, V_{ID_i})$,并验证 $S_{ID_i}P = V_{ID_i} + h^2_{ID_i}(X_{ID_i} + Y_{ID_i} + P_{Pub}h^1_{ID_i})$ 是否成立:若成立,则 $\mathcal{T}_2$ 返回 True 给 $\mathcal{A}_2$;否则,返回 False 给 $\mathcal{A}_2$;

② 若 $\boldsymbol{L}_{PK}$ 中存在 ID_i 所对应的元组且 $ID_i = ID_j$,若 $\boldsymbol{L}_2$ 中存在 ID_i 相对应的元组 $\langle ID_i, m_i, V_{ID_i}, h_2\rangle$,则 $\mathcal{T}_2$ 返回 True 给 $\mathcal{A}_2$;否则,返回 False 给 $\mathcal{A}_2$.

伪造:经过多项式有界次上述询问后,$\mathcal{A}_2$ 输出关于身份-消息-公钥 $\langle ID_i, m_i, PK_{ID_i}\rangle (1 \leqslant i \leqslant n)$ 的聚合签名 $\sigma=(V,S)$,其中至少有一个 $ID_i (i \in [1,n])$ 未进行部分密钥生成询问和私钥生成询问.同时也至少有一个 $m_i (i \in [1,n])$ 未进行签名询问.

① 若对于所有的 $ID_i (1 \leqslant i \leqslant n)$ 都有 $ID_i \neq ID_j$,则 $\mathcal{T}_2$ 放弃,并终止模拟;

② 否则(存在一个 $ID_J (J \in [1,n])$ 与 ID_j 相等,$ID_J = ID_j$),则 $\mathcal{T}_2$ 在列表 $\boldsymbol{L}_{PK}, \boldsymbol{L}_{SK}, \boldsymbol{L}_1$ 和 $\boldsymbol{L}_2$ 中查询身份 $ID_i (1 \leqslant i \leqslant n)$ 所对应的记录值,并验证等式 $SP = \sum_{i=1}^{n}[V_{ID_i} + h^2_{ID_i}(X_{ID_i} + Y_{ID_i} + P_{Pub}h^1_{ID_i})]$ 是否成立:

- 若成立,则 $\mathcal{T}_2$ 输出 $b = (h^2_{ID_j})^{-1}\{S - \sum_{i=1,i\neq j}^{n}[a_{ID_i} + h^2_{ID_i}(x_{ID_i} + y_{ID_i})] - a_{ID_j} - h^2_{ID_j}(x_{ID_j} + sh^1_{ID_j})\}$ 作为离散对数问题的有效解;
- 否则,$\mathcal{T}_2$ 没有解决离散对数问题.因为:

$$\begin{aligned} S &= \sum_{i=1}^{n}[a_{ID_i} + h^2_{ID_i}(x_{ID_i} + y_{ID_i})] \\ &= \sum_{i=1,i\neq j}^{n}[a_{ID_i} + h^2_{ID_i}(x_{ID_i} + y_{ID_i})] + a_{ID_j} + h^2_{ID_j}(x_{ID_j} + y_{ID_j}) \\ &= \sum_{i=1,i\neq j}^{n}[a_{ID_i} + h^2_{ID_i}(x_{ID_i} + y_{ID_i})] + a_{ID_j} + h^2_{ID_j}(x_{ID_j} + b + sh^1_{ID_j}). \end{aligned}$$

由引理 1 证明可知:在模拟过程中,$\mathcal{T}_2$ 不终止的概率至少为 $\left(1-\frac{q_K}{2^k}\right)\left(1-\frac{q_{SK}}{2^k}\right)\frac{1}{ne(q_S+n)}$,因此,若 $\mathcal{T}_2$ 在模拟过程中未终止,并且 $\mathcal{A}_2$ 以不可忽略的优势 ε 攻破了本文聚合签名方案 CLAS-II 的不可伪造性,则 $\mathcal{T}_2$ 能以不可忽略的优势 $Adv(\mathcal{T}_2) \geqslant \left(1-\frac{q_K}{2^k}\right)\left(1-\frac{q_{SK}}{2^k}\right)\frac{\varepsilon}{ne(q_S+n)}$ 成功解决离散对数问题.

定理 1. 在随机预言机模型下,由于离散对数问题是困难的,则本文聚合签名方案 CLAS-I 在适应性选择消息攻击下是存在性不可伪造的,即,方案 CLAS-I 的聚合签名是不可伪造的.

证明:由引理 1 和引理 2 的证明可知,定理 1 成立. □

定理 2. 在随机预言机模型下,由于离散对数问题是困难的,则本文聚合签名方案 CLAS-II 在适应性选择消息攻击下是存在性不可伪造的,即,方案 CLAS-II 的聚合签名是不可伪造的.

定理 2 的证明与定理 1 相类似,采用相同的方式将困难问题嵌入到对敌手相关询问的应答中,并构造相应的引理证明方案 CLAS-II,分别抵抗 $\mathcal{A}_{\mathrm{I}}$ 和 $\mathcal{A}_{\mathrm{II}}$ 类敌手的伪造性攻击.与定理 1 证明的区别在于应答敌手的聚合签名询问和签名验证询问时部分参数的计算方式不相同,具体的计算过程由 CLAS-II 中相应的算法所决定.篇幅所限,对于定理 2 的证明过程本文不再赘述.

4 性能及效率分析

4.1 性能分析

4.1.1 无密钥托管

在本文方案中,KGC 基于用户 U_{ID_i} 身份标识 ID_i 和公开参数 X_{ID_i} 为 U_{ID_i} 生成部分私钥 y_{ID_i} 和部分公钥 Y_{ID_i}.由于 $X_{ID_i} = x_{ID_i}P$,若 KGC 欲通过 X_{ID_i} 求解用户 U_{ID_i} 的秘密值 x_{ID_i},则其将面临求解离散对数问题,因此,KGC 无

法掌握用户 U_{ID_i} 的私钥 $SK_{ID_i}=(x_{ID_i},y_{ID_i})$, 所以,本文方案中不存在密钥托管问题.

4.1.2 公开验证性

本文方案中,当签名发送者和签名接收者关于签名的有效性发生争执,需要公开验证发送者身份时,接收者可发送身份-消息-公钥对 $(ID_i,m_i,\langle X_{ID_i},Y_{ID_i}\rangle)(1\leqslant i\leqslant n)$ 及聚合签名 $\sigma=(V,S)$ 给任意可信第三方,无需接收者的任何私有信息,可信第三方只需进行相应的验证即可.

对于方案 CLAS-I,第三方只需验证等式 $SP=\sum_{i=1}^{n}[V_{ID_i}+h_{ID_i}^2(X_{ID_i}+Y_{ID_i}+P_{Pub}h_{ID_i}^1)]$ 是否成立即可;对于方案 CLAS-II,第三方只需验证等式 $SP=V+\sum_{i=1}^{n}h_{ID_i}^2(X_{ID_i}+Y_{ID_i}+P_{Pub}h_{ID_i}^1)$ 是否成立即可.由于本文方案中签名具有不可伪造性,所以上述等式成立,则表明 $\sigma=(V,S)$ 是 U_{Agg} 关于身份-消息-公钥对 $(ID_i,m_i,PK_{ID_i}=\langle X_{ID_i},Y_{ID_i}\rangle)(1\leqslant i\leqslant n)$ 的聚合签名,因此,本文方案具有公开验证性.

4.1.3 不可否认性

本文方案中,由定理 1 和定理 2 可知,本文聚合签名方案对敌手具有不可伪造性,则用户不能否认其对消息进行签名的事实;同时,由公开验证性可知:任何可信第三方均可公开验证签名发送者的身份,因此,本文方案具有不可否认性.

4.2 效率分析

将本文方案与现有相关方案[5−7,16−19]的计算效率和通信效率进行比较,由于文献[8,9,11,13]中的方案存在安全性缺陷,并且文献[10,12,14,15]仅对现有方案进行安全性分析,并未提出相应的新方案,因此上述方案[8−15]不作为对比方案.效率分析时,计算效率主要以聚合签名合法性验证算法的计算量来衡量,通信效率主要以聚合签名的长度来衡量,具体的效率比较结果见表 1.

表 1 中,相关符号的具体含义为:E_M 表示群上的乘法运算,E_B 表示双线性映射运算;L_G 表示群中元素的长度,L_z 表示 Z_q^* 中元素的长度,$|\triangleright|$表示用户状态信息的长度.

Table 1 Efficiency comparison

表 1 效率比较结果

方案	签名长度	计算量	效率分析	
			通信效率	计算效率
文献[5]方案 I	$(n+1)L_G$	$2nE_M+(2n+1)E_B$	低	低
文献[5]方案 II	$3L_G$	$4nE_M+(n+2)E_B$	较高	低
文献[6]	$(n+1)L_G$	$3nE_M+(n+3)E_B$	低	低
文献[7]	$L_G+L_z+\|\triangleright\|$	$7nE_M+5E_B$	较高	较低
文献[16]	$2L_G$	$6nE_M+4E_B$	高	较低
文献[17]	$(n+1)L_G$	$2nE_M+3E_B$	低	较低
文献[18]	$(n+1)L_G$	$nE_M+(n+2)E_B$	低	低
文献[19]	$(n+1)L_G$	$(2n+1)E_B$	低	低
本文 CLAS-I	L_z+nL_G	$(2n+1)E_M$	低	高
本文 CLAS-II	L_z+L_G	$(2n+1)E_M$	高	高

在计算效率方面,由于双线性映射具有较高的计算量[20],而文献[5–7,16–19]中的方案均使用了双线性映射,导致其计算效率较低;但是本文聚合签名方案 CLAS-I 和 CLAS-II 中无需进行双线性映射运算,仅进行群上的乘法运算,因此相较与现有聚合签名方案[5−7,16−19]而言,本文方案 CLAS-I 和 CLAS-II 具有较高的计算效率.

在通信效率方面,本文方案 CLAS-I 的签名长度高于文献[7,16],与文献[6,17–19]中相关方案的聚合签名长度相同;本文方案 CLAS-II 的签名长度明显优于文献[5–7,17–19]中的相关方案,与文献[16]一样具有固定的签名长度.本文方案 CLAS-II 是目前最短的不使用双线性映射的无证书聚合签名方案之一,即,本文方案 CLAS-II 与文献[16]具有较高的通信效率,但文献[16]中签名验证阶段需进行 4 次双线性映射运算,导致该方案[16]的计算效率较低.

5 结束语

由于聚合签名特点突出,已经广泛应用在诸多领域.现有的聚合签名方案多数是基于双线性映射来构建,而双线性映射运算具有较高的计算量,导致现有的聚合签名方案普遍存在计算效率低的不足.针对上述不足,根据不同应用环境对传输效率的需求,本文提出了两种不使用双线性映射的无证书聚合签名方案 CLAS-I 和 CLAS-II,并在随机预言机模型下基于离散对数困难性假设证明了方案的不可伪造性;相较于其他方案而言,本文方案无需进行双线性映射运算,运算量较少,具有更高的计算效率.其中:方案 CLAS-I 的聚合签名长度较长,将用于带宽较高的网络环境;方案 CLAS-II 中聚合签名的长度与用户数无关,是固定的,是目前签名长度最短且计算效率较高的无证书聚合签名方案之一,将用于带宽较低的网络环境.

虽然方案 CLAS-I 的签名较长,方案 CLAS-II 中用户需要进行相关信息的共享,但是本文首次对不使用双线性映射的无证书聚合签名方案进行了探索性的研究,并且大幅度提高了聚合签名的计算效率.下一阶段,本文将对方案进行优化,在保证聚合签名方案高计算效率的同时提高其执行效率.

References:

[1] Shamir A. Identity-Based cryptosystems and signature schemes. In: Proc. of the Advances in Cryptology-Crypto'84. MLNCS 196, Berlin: Springer-Verlag, 1985. 47−53. [doi: 10.1007/3-540-39568-7_5]

[2] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: Proc. of the Asiacryft 2003. LNCS 2894, Berlin: Springer-Verlag, 2003. 452−473. [doi: 10.1007/978-3-540-40061-5_29]

[3] Boneh D, Gentry C, Lynn B, Shacham H. Aggregate and verifiably encrypted signatures from bilinear maps. In: Proc. of the Cryptology- Eurocrypt. Berlin: Springer-Verlag, 2003. 416−432. [doi: 10.1007/3-540-39200-9_26]

[4] Yang T, Kong LB, Hu JB, Chen Z. Survey on aggregate signature and its applications. Journal of Computer Research and Development, 2012,49(S2):192−199 (in Chinese with English abstract).

[5] Gong Z, Long Y, Hong X, Chen KF. Two certificateless aggregate signatures from bilinear maps. In: Proc. of the IEEESNPD 2007. IEEE, 2007. 188−193. [doi: 10.1109/SNPD.2007.132]

[6] Zhang L, Zhang FT. A new certificateless aggregate signature scheme. Computer Communications, 2009,32(6):1079−1085. [doi: 10.1016/j.comcom.2008.12.042]

[7] Zhang L, Qin B, Wu QH, Zhang FT. Efficient many-to-one authentication with certificateless aggregate signatures. Computer Networks, 2010,54(14):2482−2491. [doi: 10.1016/j.comnet.2010.04.008]

[8] Wang Z, Wu Q, Ye DF, Chen HY. Practical identity-based aggregate signature scheme from bilinear maps. Shanghai Jiaotong University Press, 2008,13(6):684−687. [doi: 10.1007/s12204-008-0684-5]

[9] Wen YL, Ma JF. An aggregate signature scheme with constant pairing operations. IEEE Computer Society, 2008,CSSE(3): 830−833. [doi: 10.1109/CSSE.2008.941]

[10] Selvi SSD, Vivek SS, Shriram J, Kalaivani S, Rangan CP. Security analysis of aggregate signature and batch verification signature schemes. Cryptology ePrint Archive. https://eprint.iacr.org/2009/290.pdf [doi: 10.1109/INCoS.2011.151]

[11] Xiong H, Wu QH, Chen Z. Strong security enabled certificateless aggregate signatures applicable to mobile computation. In: Proc. of the 2011 3rd Int'l Conf. on Intelligent Networking and Collaborative Systems. IEEE, 2011.

[12] Shen LM, Sun YX. On security of a certificateless aggregate signature scheme. Cryptology ePrint Archive. https://eprint.iacr.org/2012/152.pdf

[13] Xiong H, Guan Z, Chen Z, Li F. An efficient certificateless aggregate signature with constant pairing computations. Information Sciences, 2013,219:225−235. [doi: 10.1016/j.ins.2012.07.004]

[14] Cheng L, Wen QY, Jin ZP, Zhang H, Zhou LM. On the security of a certificateless aggregate signature scheme. Cryptology ePrint Archive. http://eprint. iacr.org/2013/093.pdf

[15] He DB, Tian MM, Chen JH. A note on 'An efficient certificateless aggregate signature with constant pairing computations'. http://eprint.iacr.org/2012/445.pdf

[16] Du HZ, Huang MJ, Wen QY. Efficient and provably-secure certificateless aggregate signature scheme. Acta Electronica Sinica, 2013,41(1):74−76 (in Chinese with English abstract).

[17] Liu H, Wang SJ, Liang MG, Chen YQ. New construction of efficient certificateless aggregate signatures. Int'l Journal of Security and its Applications, 2014,8(1):411−422. [doi: 10.14257/ijsia.2014.8.1.38]

[18] Chen YC, Horng G, Liu CL, Tsai YY, Chan CS. Efficient certificateless aggregate signature scheme. Journal of Electronic Science and Technology, 2012,10(3):209−214. [doi: 10.3969/j.issn.1674-862X.2012.03.004]

[19] Gong Z, Long Y, Hong X, Chen KF. Practical certificateless aggregate signatures from bilinear maps. Journal of Information Science and Engineering, 2008.

[20] Chen L, Cheng Z, Smart NP. Identity-Based key agreement protocols from pairings. Journal of Information Security, 2007,6(4): 213−241. [doi: 10.1007/s10207-006-0011-9]

附中文参考文献:

[4] 杨涛,孔令波,胡建斌,陈钟.聚合签名及其应用研究综述.计算机研究与发展,2012,49(S2):192−199.

[16] 杜红珍,黄梅娟,温巧燕.高效的可证明安全的无证书聚合签名方案.电子学报,2013,41(1):74−76.

周彦伟(1986－),男,甘肃通渭人,博士生,主要研究领域为密码学,匿名通信技术,可信计算.

杨波(1963－),男,博士,教授,博士生导师,主要研究领域为密码学,信息安全.

张文政(1966－),男,博士,研究员,主要研究领域为密码学,信息安全.