

基于SM9的指定验证者聚合签名方案

李继国, 方淳

(福建师范大学计算机与网络空间安全学院, 福建 福州 350117)

摘要: 聚合签名能够显著提升签名效率, 减少签名者的计算代价, 降低通信成本, 并且能更好地保护签名者的隐私, 因此, 得到国内外学者的广泛关注。但聚合签名方案大多数采用国外密码算法设计, 不符合我国密码技术自主可控的要求。SM9数字签名算法是国内自主研发的标识签名方案, 其仅能实现一对一的签名和验证, 无法满足多对一的签名和验证需求。针对上述问题, 构造了基于SM9的指定验证者聚合签名(designated verifier aggregate signature, DVAS)方案。该方案利用假名和散列函数单向性, 避免签名者个人信息泄露。在签名聚合阶段, 通过制定验证者控制数据访问权限, 实现了签名者的隐私保护。基于 q -SDH(q -strong Diffie-Hellman)困难问题, 所提方案在随机谕言机模型下证明了安全性。方案分析显示该方案能够避免签名者隐私泄露。理论分析和实验仿真结果表明, 与现有聚合签名方案相比, 所提方案在单个签名生成和验证方面性能更加优越, 并且能有效降低签名批量验证的计算代价, 同时具有较高的运算效率, 更能适用于云服务应用场景。

关键词: SM9; 隐私保护; q -SDH困难问题; 聚合签名

DOI: 10.11959/j.issn.2096-109x.2024053

Designated verifier aggregate signature scheme based on SM9

LI Jiguo, FANG Chun

School of Computer and Cyberspace Security, Fujian Normal University, Fuzhou 350117, China

Abstract: Aggregate signatures have been recognized for significantly improving signing efficiency, reducing the computational cost for signers, lowering communication costs, and better protecting the privacy of signers. Currently, many aggregate signature schemes have been designed using foreign cryptographic algorithms, which do not meet the requirements for independent and controllable cryptography technology in China. The SM9 algorithm, a domestically developed identity-based signature scheme in China, was only capable of achieving one-to-one signature and verification, failing to meet the requirements for multiparty signature and verification. To address these issues, a designated verifier aggregate signature (DVAS) scheme was proposed based on the SM9 signature algorithm. Pseudonyms and the one-way property of hash functions were utilized to prevent the leakage of the signer's personal information. The privacy of the signer was protected during the signature aggregation phase by controlling data access per-

收稿日期: 2024-04-24; 修回日期: 2024-07-20

通信作者: 李继国, ljg1688@163.com

基金项目: 国家自然科学基金(62072104, 61972095, U21A20465)

Foundation Item: The Natural Science Foundation of China (62072104, 61972095, U21A20465)

引用格式: 李继国, 方淳. 基于SM9的指定验证者聚合签名方案[J]. 网络与信息安全学报, 2024, 10(4): 63-71.

Citation Format: LI J G, FANG C. Designated verifier aggregate signature scheme based on SM9[J]. Chinese Journal of Network and Information Security, 2024, 10(4): 63-71.

missions for designated verifiers. The security of the scheme was proven under the random oracle model, based on the q -strong Diffie-Hellman (q -SDH) hard problem. Scheme analysis demonstrates that it could prevent the leakage of the signer's privacy. Theoretical analysis and experimental simulation show that, compared to other similar aggregate signature schemes, the proposed scheme exhibits superior performance in terms of signature generation and verification. The proposed scheme is capable of effectively reducing the computational cost of batch signature verification and offered higher computational efficiency, making it more suitable for applications such as cloud services.

Keywords: SM9, privacy protection, q -SDH problem, aggregate signature

0 引言

2003 年, Boneh 等^[1]首次提出聚合签名概念, 聚合签名的主要目的是在不暴露单个签名者身份的情况下, 允许多个签名者共同生成一个代表整个群体的数字签名。与传统数字签名技术相比, 聚合签名能够显著提升签名效率, 降低通信成本, 减少签名者的负担, 并且能更好地保护签名者的隐私。虽然聚合签名具有签名压缩功能, 能够有效降低通信代价和计算代价, 但目前的聚合签名方案主要围绕国外密码算法展开, 缺乏基于国产密码算法的聚合签名方案设计。为应对新时代网络空间安全挑战, 国家密码管理局自主研制了 SM9 标识密码算法。SM9 标识密码算法被采纳为国际标准 ISO/IEC 148883: 2018 的一部分^[2], 受到了国际的广泛认可。但原始的 SM9 标识密码算法不支持签名聚合功能, 且不适用于需要保护签名者签名行为的场景, 如电子医疗领域。在电子医疗中^[3], 嵌入式医疗设备可收集相关数据并定期批量提交患者体征数据给云服务器。云服务器将数据传输至指定医疗机构, 由专业医务人员对患者进行诊断和治疗。当医疗设备收集患者体征数据时, 应注重患者隐私保护, 仅授权医务人员访问数据。这些数据在传输过程中容易遭受窃听、非法访问等攻击^[4]。Hill 等^[5]指出, 在无线设备的信息传输能量消耗中, 传输信息所需要的能耗远高于计算所带来的能耗, 因此要求控制方案的通信代价以降低通信能耗。综上所述, 基于国产密码标准 SM9 设计能够实现隐私保护的聚合签名方案成为亟待解决的问题。

本文主要贡献如下: 首次提出基于 SM9 算法的指定验证者聚合签名 (designated verifier aggregate signature, DVAS) 方案。提出的方案不仅可以完成传统签名的身份认证, 而且能够实现指定验证者和用户隐私保护, 显著提升签名效

率, 减少签名者计算开销和降低通信成本, 因此适用于云服务应用环境。

1 相关工作

聚合签名方案是基于密码学的数据验证方法, 其主要作用是将多个签名者的签名聚合成一个单独的签名, 不仅保护了签名者的隐私性, 而且能有效降低通信代价和签名的验证代价。在 2003 年欧密会议上, Boneh 等^[1]首次提出聚合签名概念和具体方案, 方案允许将多个签名聚合为一个签名以提高多个签名的验证效率。为了解决信息的批量认证问题, Cheon 等^[6]在 2004 年提出了基于身份的完全聚合签名方案, 强调聚合签名方案的安全性取决于签名方案的安全性和签名聚合过程的有效性。对于基于身份的聚合签名, Lysyanskaya 等^[7]提出首个有序聚合方案, 但方案的灵活性较差。此后, 许多针对特定运用场景的基于身份的聚合签名方案被设计出来。2016 年, Iwasaki 等^[8]提出了紧安全的基于身份聚合签名方案。2019 年, Yang 等^[9]将伪身份机制引入聚合签名以实现用户对用户的隐私保护。2020 年, Yao 等^[10]利用 2-level HIBE 方案提出了 IBSAS 方案的通用构造, 并证明了方案的不可伪造性, 实现了基于身份聚合签名中的细粒度访问控制功能。目前, 大多数密码方案基于国外密码标准设计, 不符合密码算法自主设计需求。SM9^[11]标识密码算法, 其方案基于椭圆曲线上的配对运算设计。2020 年, SM9 标识密码算法成为中国国家标准 (GM/T 38635.2-2020)^[12]。在对 SM9 的研究中^[12-23], Cheng 等^[13]给出了 SM9 密钥协商协议和 SM9 加密方案的形式化安全性分析。为了提高 SM9-IBS 的运算速度, 胡芯忆等^[14]设计了双线性对的快速软件实现方法。赖建昌等^[15]将广播加密与 SM9 标识加密算法相结合, 提出基于 SM9 的高

效标识广播加密方案，并实现了多用户信息共享和数据共享。为了改进签名效率，Lai等^[16]提出基于SM9的在线/离线方案，将签名过程拆分为离线及在线两个环节以满足即时通信的需求。进一步，朱留富等^[17]构造了基于商密SM9中的属性基在线/离线签名方案，通过制定访问策略实现了细粒度访问控制。2023年，崔岩等^[18]构造了第一个基于SM9的匿名广播加密方案，有效实现多用户数据的安全共享。为保护用户隐私、提高通信效率和实现数据访问控制，本文基于SM9标识签名算法设计了指定验证者聚合签名方案。在随机预言机模型下，本文利用分叉引理^[24]证明了方案安全性可规约到 q -SDH困难问题假设。并分析了方案的计算代价，与文献[25-27]方案进行比较，提出的方案性能具有明显优势。

2 预备知识

本节介绍相关理论基础，包括双线性配对和困难问题假设。

2.1 双线性配对

给定安全参数输出双线性群 $\mathcal{B} = (G_1, G_2, G_T, e, p)$ 的生成器 G ，其中，群 G_1 、群 G_2 和群 G_T 是循环群，其素数阶皆为 p 。令 P 和 Q 分别是群 G_1 和 G_2 的生成元。存在双线性映射 $e: G_1 \times G_2 \rightarrow G_T$ 满足如下条件。

- 1) 双线性：对任意 $P \in G_1$ ，任意 $Q \in G_2$ ，任意 $a, b \in \mathbb{Z}_p^*$ ，存在 $e(aP, bQ) = e(P, Q)^{ab}$ ；
- 2) 非退化性：对任意 $P \in G_1$ ，任意 $Q \in G_2$ ，有 $e(P, Q) \neq 1$ ；
- 3) 可计算性：对任意 $P \in G_1$ ，任意 $Q \in G_2$ ，存在一个高效算法计算 $e(P, Q)$ 。

此外，存在一个可公开计算且有效的同构 $\varphi: G_2 \rightarrow G_1$ ， $\varphi(Q) = P$ 。其中， P 是群 G_1 的生成元， Q 是群 G_2 的生成元。

2.2 困难问题假设

设 P 为群 G_1 的生成元， Q 为群 G_2 的生成元。 q -SDH (q -strong Diffie-Hellman) 困难问题在群 (G_1, G_2) 中的具体描述是：给定 $q+2$ 个元素的元组 $(P, Q, aQ, a^2Q, \dots, a^qQ)$ ，可以找到一对元素 $(c, \frac{1}{c+a}P)$ ， $c \in \mathbb{Z}_p^*$ 。 q -SDH困难问题假设不存在概率多项式时间敌手可以以不可忽略的概率求解出 q -SDH问题。

3 DVAS方案的形式化定义和安全模型

本节给出DVAS方案具体的形式化定义和相应的安全模型。图1给出了基于SM9 DVAS方案框架。DVAS方案框架包括了4个实体：用户、密钥生成中心 (key generation center, KGC)、聚合签名设备和指定验证者。KGC为用户颁发假名和产生私钥，用户利用私钥对信息进行签名。指定验证者选定聚合签名私钥，计算聚合签名公钥并公布。聚合签名设备对签名按照算法流程聚合后将聚合签名提交给指定验证者。指定验证者按照算法流程对聚合签名进行验证，若签名有效，指定验证者返回accept；否则，返回reject。

3.1 DVAS方案形式化定义

指定验证者聚合签名方案描述如下。

- 1) 设置。输入安全参数 λ ，输出公开参数params、主公钥mpk和主私钥msk，密钥生成中心保留主私钥msk。由KGC执行。
- 2) 密钥生成。输入公开参数params、主私钥msk和给定用户假名 PID_i ，输出该签名者的私钥 sk_{PID_i} 。由KGC执行。
- 3) 签名。输入签名消息 M_i 、公开参数params和签名者私钥 sk_{PID_i} ，输出签名 σ_i 。由轻量级签名设备执行。

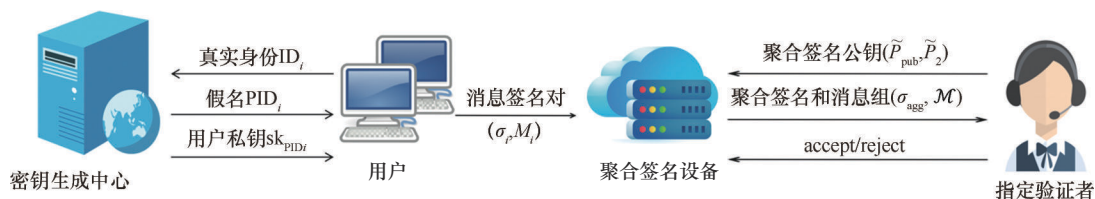


图1 基于SM9的指定验证者聚合签名方案框架

Figure.1 The framework of a designated verifier aggregate signature scheme based on SM9

4) 验证。输入公开参数 params 、消息 M_i 和签名 σ_i 。若签名有效, 则输出 **accept**; 否则, 输出 **reject**。单个签名验证可由方案系统框架中任意实体执行。

5) 聚合密钥生成。输入公开参数 params , 输出聚合签名私钥 y 和聚合签名公钥 $(\tilde{P}_{\text{pub}}, \tilde{P}_2)$ 。由指定验证者执行。

6) 聚合签名。输入聚合签名公钥 $(\tilde{P}_{\text{pub}}, \tilde{P}_2)$, 公开参数 params , 用户组 $\mathcal{U}$ 的用户假名 PID_i , $i \in [1, n]$, 消息组 $\mathcal{M} = (M_1, M_2, \dots, M_n)$ 和签名组 $(\sigma_1, \sigma_2, \dots, \sigma_n)$, 输出聚合签名 σ_{agg} 。由聚合签名设备执行。

7) 聚合验证。输入聚合私钥 y 、聚合签名 σ_{agg} 和消息组 $\mathcal{M}$, 若签名有效, 则输出 **accept**; 否则, 输出 **reject**。由指定认证者执行。

3.2 安全模型定义

参考文献[16]的思想, 本节定义针对选择身份和选择消息攻击存在性不可伪造 (existential unforgeable against selected identity and chosen message attacks, EUF-sID-CMA) 安全模型, 安全模型中身份 PID^* 在初始化阶段给定, 敌手不允许查询 PID^* 对应私钥。安全游戏的具体交互如下。

1) 初始化。给定安全参数 λ , 挑战者运行设置算法生成主公钥 mpk 和公开参数 params 。将主公钥 mpk , 公开参数 params 发送给敌手。

2) 私钥查询。敌手对于基于身份 PID 的私钥进行查询, 挑战者运行密钥生成算法生成私钥 sk_{PID} , 并将 sk_{PID} 返回给敌手。

3) 签名查询。敌手基于一对给定 (PID, M) 上的签名进行查询, 挑战者运行签名算法生成签名 $\sigma = (S, W)$, 然后将签名 σ 发送给敌手。

4) 伪造。在新一轮游戏中, 敌手没有查询 PID^* 的私钥 sk_{PID} 和 (PID^*, M^*) 上的签名, 能够对于 (PID^*, M^*) 伪造出一个有效签名 σ^* , 则敌手输出元组 $(\sigma^*, \text{PID}^*, M^*)$, 并赢得游戏。

4 DVAS 方案构造

DVAS 方案构造的具体描述如下。

1) 设置。给定安全参数 λ , 生成双线性元组

$\mathcal{B} = (G_1, G_2, G_T, e, p)$ 。KGC 随机选取 P_1, P_2 为群 G_1, G_2 生成元, 选择 $\alpha \in \mathbb{Z}_p^*$ 作为主私钥, 计算主公钥 $\text{mpk} = P_{\text{pub}} = \alpha P_2$ 和 $g = e(P_1, P_{\text{pub}}) \in G_T$ 。选取散列函数 $H: \{0, 1\}^* \rightarrow \mathbb{Z}_p^*$, $H_1: \{0, 1\}^* \rightarrow \mathbb{Z}_p^*$ 和 $H_2: \{0, 1\}^* \rightarrow \mathbb{Z}_p^*$ 。hid 是用一个字节表示的签名私钥生成函数标识符, 由 KGC 选择。最后 KGC 公开系统参数 $\text{params} = (P_1, P_2, \text{hid}, H, H_1, H_2, g)$ 。

2) 密钥生成。设 $\mathcal{U} = u_1, u_2, \dots, u_n$ 为包含了 n 个签名者的用户组, 用户选定自己的真实身份标识 $\text{ID}_i \in \{0, 1\}^*$ 。为保护用户隐私, KGC 给用户组 $\mathcal{U}$ 中的用户颁发假名 PID_i 。颁发的假名 PID_i 应满足 $H_1(\text{PID}_i \| \text{hid}, p) + \alpha \neq 0$ 。KGC 利用 PID_i 计算用户私钥如下: $\text{sk}_{\text{PID}_i} = \frac{\alpha}{\alpha + H_1(\text{PID}_i \| \text{hid}, p)} \cdot P_1$ 。

3) 签名。算法输入公开参数 params , 用户 u_i 假名 PID_i , 私钥 sk_{PID_i} 和该用户发送的消息 M_i , 用户 u_i 使用自己所持有的 sk_{PID_i} 进行如下计算:

① 签名者随机选取整数 $r_i \in [1, p-1]$, 计算 $w_i = g^{r_i}$ 。

② 计算哈希值 $h_i = H_2(M_i \| w_i, p)$ 。

③ 计算 $S_i = (r_i - h_i) \text{sk}_{\text{PID}_i}$ 。

④ 输出签名 $\sigma_i = (S_i, w_i)$ 。

4) 验证。系统中任意方获得消息签名对 (M_i, σ_i) , 可以通过执行算法验证签名:

① 计算 $P = P_{\text{pub}} + H_1(\text{PID}_i \| \text{hid}, p) \cdot P_2$;

② 计算哈希值 $h_i = H_2(M_i \| w_i, p)$;

③ 验证等式 $e(S_i, P) = w_i g^{-h_i}$ 是否成立, 若等式成立, 则签名 S_i 有效, 输出 **accept**; 否则签名无效, 输出 **reject**。

5) 聚合密钥生成。输入公开参数 params , 指定验证者随机选择 $y \in \mathbb{Z}_p^*$ 作为聚合签名私钥, 计算 $\tilde{P}_2 = y P_2$ 和 $\tilde{P}_{\text{pub}} = y P_{\text{pub}}$ 作为聚合签名公钥, 公开 $(\tilde{P}_{\text{pub}}, \tilde{P}_2)$ 。

6) 聚合。聚合签名设备收到签名组 $(\sigma_1, \sigma_2, \dots, \sigma_n)$ 和消息组 $\mathcal{M} = (M_1, M_2, \dots, M_n)$ 后, 利用聚合签名公钥 $(\tilde{P}_{\text{pub}}, \tilde{P}_2)$, 按如下所述方法产生相应的聚合签名:

- ①计算 $h_{1,i} = H_1(\text{PID}_i \parallel \text{hid}, p)$;
- ②计算 $Y_i = \tilde{P}_{\text{pub}} + h_{1,i} \cdot \tilde{P}_2, i \in [1, n]$;
- ③计算 $S_{\text{agg}} = H(e(S_1, Y_1), \dots, e(S_n, Y_n))$;
- ④生成聚合签名 $\sigma_{\text{agg}} = (S_{\text{agg}}, w_1, \dots, w_n)$ 。

7) 聚合验证。指定验证者收到聚合签名 σ_{agg} 消息组 $\mathcal{M}$ 后, 通过执行以下2个步骤验证聚合签名:

- ①计算 $h_i = H_2(M \parallel w_i, p), i \in [1, n]$;
- ②验证等式 $S_{\text{agg}} = H(w_1^y g^{-y h_1}, \dots, w_n^y g^{-y h_n})$ 是否成立, 若等式成立, 接受聚合签名有效, 输出 accept; 否则视为无效, 输出 reject。

5 正确性和安全性分析

5.1 正确性分析

1) 若签名有效, 则签名可以通过以下步骤验证算法。

$$\begin{aligned}
 e(S_i, P) &= e\left(\frac{\alpha(r_i - h_i)}{\alpha + H_1(\text{PID}_i \parallel \text{hid}, p)} \cdot P_1, (\alpha + H_1(\text{PID}_i \parallel \text{hid}, p)) \cdot P_2\right) \\
 &= e(\alpha(r_i - h_i) \cdot P_1, P_2) \\
 &= e(P_1, P_{\text{pub}})^{r_i - h_i} \\
 &= g^{r_i - h_i} \\
 &= w_i g^{-h_i}
 \end{aligned}$$

此 $e(S_i, P) = w_i g^{-h_i}$, 提出的签名方案满足正确性要求。

2) 在签名聚合阶段, 按照以下步骤确保具有假名 $\text{PID}_i, i \in [1, n]$ 的用户生成的单个签名有效。

$$\begin{aligned}
 e(S_i, Y_i) &= e\left(\frac{\alpha(r_i - h_i)}{\alpha + H_1(\text{PID}_i \parallel \text{hid}, p)} \cdot P_1, (\alpha + H_1(\text{PID}_i \parallel \text{hid}, p)) \cdot P_2 \cdot y\right) \\
 &= e(\alpha(r_i - h_i) \cdot P_1, y \cdot P_2) \\
 &= e(P_1, P_{\text{pub}})^{y(r_i - h_i)} \\
 &= g^{y(r_i - h_i)} \\
 &= w_i^y g^{-h_i y}
 \end{aligned}$$

3) 在聚合签名验证阶段, 指定验证者通过以下步骤确保聚合签名有效。

$$\begin{aligned}
 S_{\text{agg}} &= H(e(S_1, Y_1), e(S_2, Y_2), \dots, e(S_n, Y_n)) \\
 &= H\left(e\left(\alpha(r_i - h_{1,i}) \cdot P_1, \tilde{P}_{\text{pub}} + h_{1,i} \cdot \tilde{P}_2\right)\right) \\
 &= H\left(e\left(\alpha(r_i - h_{1,i}) \cdot P_1, P_{\text{pub}} + h_{1,i} \cdot P_2\right)\right)^y \\
 &= H\left(e\left(P_1, P_{\text{pub}}\right)\right)^{y(r_i - h_i)} \\
 &= H\left(w_1^y g^{-h_1 y}, \dots, w_n^y g^{-h_n y}\right)
 \end{aligned}$$

因此, 方案的聚合签名阶段满足正确性要求。

5.2 安全性分析

本节证明在 q -SDH 困难问题的假设下, 提出的方案 EUF-sID-CMA 是安全的。当主公钥 mpk 生成时, hid 和 p 为固定值。为方便表述, 在证明过程中将 $H_1(\text{ID} \parallel \text{hid}, p)$ 和 $H_2(M \parallel w, p)$ 分别简记为 $H_1(\text{ID} \parallel \text{hid})$ 和 $H_2(M \parallel w)$ 。

定理1 令散列函数 H_1, H_2 是随机谕言机。如果 q -SDH 问题是困难的, 则本文提出的 DVAS 方案 EUF-sID-CMA 是安全的。

证明 假定在 EUF-sID-CMA 安全模型中, 存在多项式时间敌手 A , 在对随机谕言机 H_1 进行 q_{H_1} 次查询, 对随机谕言机 H_2 进行 q_{H_2} 次查询后, 能够以不可忽略概率攻破提出的方案。则可以构建模拟器 B 与敌手 A 交互, 模拟器 B 以不可忽略概率解决 q -SDH 问题。假定模拟器 B 给定随机 q -SDH 实例 $(P, Q, aQ, a^2Q, \dots, a^q Q)$, 其中 a 未知, $q = q_{H_1}$,

模拟器 B 的目标是找到一对 $\left(c, \frac{1}{c+a} P\right), c \in \mathbb{Z}_p^*$ 。

初始化: 模拟器 B 根据如下方法生成系统参数和主公钥。

1) 选取 q 个随机数 $x^*, x_1, x_2, \dots, x_{q-1} \in \mathbb{Z}_p^*$ 并计算如下多项式: $f(z) = \prod_{i=1}^{q-1} (x_i + z)$, $f(z) = \sum_{i=0}^{q-1} c_i z^i$ 。其中, c_i 为 $f(z)$ 的系数。

2) 计算 $P_2 = f(a)Q = \sum_{i=0}^{q-1} c_i (a^i Q)$, P_2 可从给定的 q -SDH 实例中计算得到。后计算 P_1 和 P_{pub} 如下。

$$\begin{aligned}
 P_1 &= \varphi(P_2) = f(a)P \\
 P_{\text{pub}} &= \sum_{i=1}^q c_{i-1} (a^i Q) = aP_2
 \end{aligned}$$

此外, $g = (p_1, p_{\text{pub}})$ 。

3) 对 $i \in [1, q-1]$, 有 $f_i(z) = \frac{f(z)}{a+x_i} = \sum_{i=0}^{q-2} d_i z^i$, 并计算: $\sum_{i=0}^{q-2} d_i \varphi(a^{i+1}Q) = af_i(a)P = \frac{af(a)}{a+x_i}P = \frac{a}{a+x_i}P_1$ 。因此对任意 $i \in [1, \dots, q-1]$, 双线性对 $(x_i, \frac{a}{a+x_i}P_1)$ 是可计算的。

4) 模拟器B随机挑选身份假名 $PID^* \in \{0,1\}^*$ 作为挑战发送方的身份并发送给敌手A。

5) 模拟器B挑选主密钥且不公布, 设置系统主公钥 $mpk = P_{pub}$ 和公开系统参数 $params = (P_1, P_2, g, H_1, H_2, hid)$, 其中, H_1 和 H_2 被看成是由模拟器B控制的随机谰言机。

H_1 -查询。敌手A进行关于身份假名 PID_i 的 H_1 查询, 为了响应这些查询, 模拟器B建立初始为空的元组 (PID_i, x_i) 的列表 $\mathcal{L}_1$, 若要查询内容 PID_i 已经出现在 $\mathcal{L}_1$ 中的元组 (PID_i, x_i) 上, 模拟器B回复 $H_1(PID_i) = x_i$ 。若 $PID_i = PID^*$, 则 $H_1(PID^*) = x^*$, 否则, 令 PID_i 为随机谰言生成机 H_1 的第 i 个新身份, 模拟器B设定 $H_1(PID_i) = x_i$, 并将元组 (PID_i, x_i) 添加到 $\mathcal{L}_1$ 中, 其中 x_i 在初始阶段生成。最后, 模拟器B以 x_i 响应敌手A。

H_2 -查询。敌手A进行基于元组 (M_i, w_i) 上的 H_2 查询。为响应这些查询, 模拟器B建立一个初始为空的元组 (M_i, w_i, h_i) 的列表 $\mathcal{L}_2$ 。若要查询内容 (M_i, w_i) 已经出现在 $\mathcal{L}_2$ 中的元组 (M_i, w_i, h_i) 上, 则模拟器B以 $H_2(M_i || w_i) = h_i$ 响应。否则, 模拟器B随机选取 $h_i \in Z_p^*$, 并令 $H_2(M_i || w_i) = h_i$, 同时将新元组 (M_i, w_i, h_i) 添加到 $\mathcal{L}_2$ 中。最后模拟器B对敌手A回复 h_i 。

私钥查询。敌手A选定一个用于私钥查询的身份 $PID_i \neq PID^*$, 模拟器B以 PID_i 查询随机谰言机 H_1 得到 x_i , 并以 $\frac{a}{a+x_i}P_1$ 回复给敌手A, 如初始阶段所述可计算 $\sum_{i=0}^{q-2} d_i \varphi(a^{i+1}Q)$, $\frac{a}{a+x_i}P_1$ 也是可计算的。

签名查询。敌手A对身份和消息组成的元组 (PID_i, m_i) 进行签名询问。模拟器B尝试从 $\mathcal{L}_1$ 中恢复 (PID_i, x_i) 如下: 首先检查 PID_i 是否在 $\mathcal{L}_1$ 中存

在。若为否, 模拟器B中断; 否则, 输出 $H_1(PID_i) = x_i$ 。

完成 H_1 查询之后, 利用查询结果 x_i , 计算 $P = x_i P_2 + P_{pub}$, 模拟器B随机选取 $h \in Z_p^*$, $S \in G_T$, 有 $w = e(S, P) \cdot g^h$ 。最后, 将元组 (M, w) 添加到列表 $\mathcal{L}_2$ 中。定义 $H_2(M || w) = h$ 。

注意: 若列表 $\mathcal{L}_2$ 中已定义 $H_2(M || w)$, 则模拟器B不能成功回答签名查询造成模拟中止。该事件以 $\frac{q_s + q_{H_2}}{2^i}$ 的概率发生, (可以忽略不计), 其中 q_s 和 q_{H_2} 分别为签名查询和 H_2 查询的次数。

仿造。敌手A输出一个元组 (σ^*, M^*, PID^*) , 元组中 σ^* 是与 (M^*, PID^*) 相关的有效签名。由文献[24]提出的分叉引理可知: 若算法 $\mathcal{A}'$ 在输入 (mpk, PID^*) 上重复 $\mathcal{A}$ 攻击流程足够多的次数, 可得到两个有效签名元组 (M^*, w^*, h_1^*, S_1^*) 和 (M^*, w^*, h_2^*, S_2^*) , 其中 $h_1^* \neq h_2^*$ 。

由分叉引理可知, 模拟器B运行 $\mathcal{A}'$ 可以得到基于相同的消息 M^* , 身份假名 PID^* 和承诺 w^* 的两个有效伪造签名元组 (M^*, w^*, h_1^*, S_1^*) 和 (M^*, w^*, h_2^*, S_2^*) 。模拟器B从列表 $\mathcal{L}_1$ 中获得元组 (PID^*, x^*) , 因两个签名元组都有效, 可同时满足验证方程。则有: $w = e(S_1^*, P^*) \cdot g^{h_1^*} = e(S_2^*, P^*) \cdot g^{h_2^*}$

其中 $P^* = x^* P_2 + P_{pub} = (x^* + a)P_2$ 。

显然有: $e((S_1^* - S_2^*), P^*) = g^{h_2^* - h_1^*}$, 所以可求得 $e(a^{-1}(h_2^* - h_1^*)^{-1}(S_1^* - S_2^*), (x^* + a)P_2) = e(P_1, P_2)$ 。

因此, $(h_2^* - h_1^*)^{-1}(S_1^* - S_2^*) = \frac{a}{(x^* + a)}P_2$ 。

令 $X^* = (h_2^* - h_1^*)^{-1}(S_1^* - S_2^*)$, 当 $P_1 = f(a)P$ 有: $\frac{a}{x^* + a}P_1 = \frac{af(a)}{x^* + a}P = \frac{\alpha}{x^* + a}P + \sum_{i=0}^{q-1} \alpha_i a^i P$ 。已知系数 α_i 和 $\alpha \neq 0$ 。最后, 模拟器B计算 $\pi^* = \frac{1}{x^* + a}P = \frac{1}{\alpha} \cdot \left(X^* - \sum_{i=0}^{q-1} \alpha_i \cdot \varphi(a^i Q) \right)$, 并输出 (x^*, π^*) 对作为给定 q -SDH 实例的解。

综上, 若敌手A能以不可忽略概率 ε 伪造一个有效签名, 那么模拟器B就能以相同概率 ε 解决 q -SDH 问题。在此情况下模拟成功的概率为

$\frac{1}{q_{H_1}}$ 。因此, $\mathcal{B}$ 就可以以 $\frac{\varepsilon}{q_{H_1}}$ 的概率解决 q -SDH 问题。

定理2 若散列函数 H 能够抗碰撞, 则在上述聚合签名方案中, 聚合签名有效当且仅当用于聚合中的每个签名有效。

单个签名有效时, 有 $e(S_i, Y_i) = w_i^y g^{-h_i y}$ 和 $H(e(S_i, Y_i)) = H(w_i^y g^{-h_i y})$ 。

对于 $i \in 1, \dots, n$, 则有: $S_{\text{agg}} = H(e(S_1, Y_1), e(S_2, Y_2), \dots, e(S_n, Y_n)) = H(e(S_i, Y_i)) = H(w_i^y g^{-h_i y})$ 。

当每个个体签名有效时, 这个聚合签名有效。

如果聚合签名有效时, 对于每一个 $j \in 1, \dots, n$, 则有:

$$\begin{aligned} S_{\text{agg}} &= H(e(S_1, Y_1), e(S_2, Y_2), \dots, e(S_n, Y_n)) \\ &= H(e(S_j, Y_j)) \\ &= H(w_j^y g^{-h_j y}) \end{aligned}$$

对用户组内任意用户 $j \in 1, \dots, n$, 有:

$$\begin{aligned} H(w_j^y g^{-h_j y}) &= H(g^{r_j y} g^{-h_j y}) \\ &= H(g^{(r_j - h_j) y}) \\ &= H(e(\tilde{P}_1, \tilde{P}_{\text{pub}})^{r_j - h_j}) \\ &= H(e(S_j, Y_j)) \end{aligned}$$

即签名聚合中使用的每个签名有效时聚合签名有效。

6 方案分析

(1) 隐私保护

用户不用真实身份标识 ID_i 参与签名而是用假名 PID_i , 实现了用户隐私保护。在签名聚合之前指定聚合签名验证者, 仅指定验证者可查看聚合签名内容。设参与签名聚合人数为 n , 签名聚

合后传输签名内容为 $(S_{\text{agg}}, w_1, \dots, w_n)$ 。 S_{agg} 为散列函数处理后的用户签名标志信息, w_i 为用户选取的随机数承诺。传输签名内容无用户个人签名信息, 因此避免用户隐私泄露。

(2) 性能分析

为了便于比较, 本文将参与签名聚合的用户数量记为 n 。经测试发现, 散列函数运算效率高, 故其时间消耗可忽略。聚合签名方案计算开销比较如表1所示。

为更直观地比较本文方案与现有方案在聚合签名生成和验证阶段时间开销, 本文在 Linux Ubuntu 20.04 操作系统下使用 python 语言库中 Charm 0.5 框架实现了所提方案。配置使用 AMD Ryzen 7 4800HS with Radeon Graphics 2.90 GHz 16 GB 处理器计算机, 利用 Charm 中的超奇异椭圆曲线 (SS512) 测试方案。实验中群的阶为 512 bit 的大素数。在计算机上经过 1 000 次实验取平均值后得到结果如图2~图3所示。

实验仿真分析结果表明, 提出的 DVAS 方案在聚合签名生成和验证时间开销优于文献[25-27]。在单个签名生成和验证过程中, 本文提出的方案签名生成和验证计算开销也优于文献[25-27]。

7 结束语

本文在 SM9 算法基础上首次提出指定验证者聚合签名方案。提出的方案不仅适用于云服务等应用环境, 此外能够实现用户隐私保护功能。在随机预言机模型下, 本方案安全性可归约到 q -SDH 困难问题。在保障用户隐私的前提下, 通过与现有方案的对比分析, 本文提出的方案在单个签名的生成与验证的计算开销, 以及聚合签名验证阶段的计算开销方面均表现出明显优势。

表1 聚合签名方案计算开销比较

Tabel 1 Comparison of computation cost of aggregate signature schemes

对比方案	签名生成验证开销	聚合签名生成开销	聚合签名验证开销
文献[25]方案	$3BP + 5Ex + 5P$	nBP	$(2n + 3)BP + 2nP$
文献[26]方案	$3BP + 7Ex + 2P$	nBP	$2nBP + 3nEx + 2nP$
文献[27]方案	$4BP + 2E + 2M + P$	$nBP + (n + 1)M$	$(2n + 1)BP + 2nEx + 2nE$
本文方案	$BP + Ex + M + 2P$	$nBP + nE + nP$	$2nEx + nM$

注: BP 是双线性对配对运算时间, M 是椭圆曲线 G 上的标量点乘运算时间, P 是 G 上的标量点加运算时间, E 是群上的乘法运算时间, Ex 是群上指数运算时间。

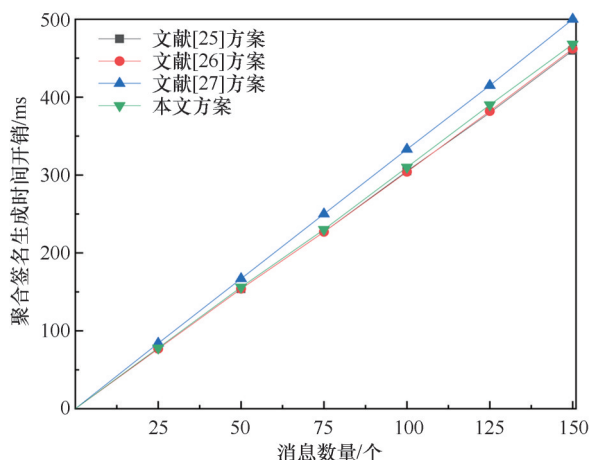


图2 聚合签名生成时间开销与消息数量的关系

Figure 2 The relationship between aggregate signature generation time overhead and the number of messages

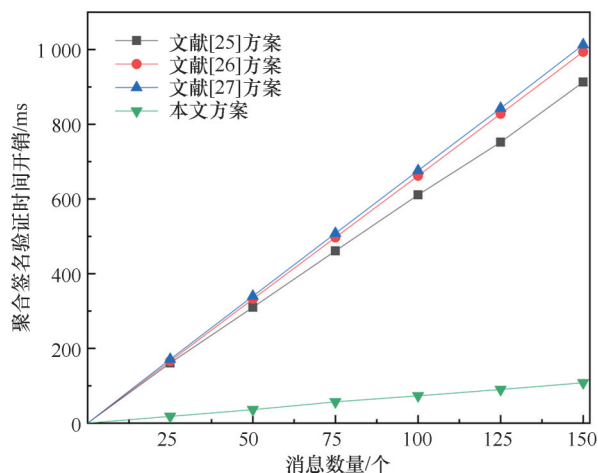


图3 聚合签名验证时间开销与消息数量的关系

Figure 3 The relationship between aggregate signature verification time overhead and the number of messages

参考文献:

- [1] BONEH D, GENTRY C, LYNN B, et al. Aggregate and verifiably encrypted signatures from bilinear maps[C]//Proceedings of the 22nd International Conference on Theory and Applications of Cryptographic Techniques. New York: ACM, 2003: 416-432.
- [2] International Organization for Standardization (ISO). Information technology-security techniques-digital signatures with appendix-part 3: digital logarithm based mechanisms. ISO/IEC 14888 - 3:2018[S]. Switzerland: International Organization for Standardization, 2018: 11.
- [3] ALZHRANI B A, IRSHAD A, ALBESHRI A, et al. A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks[J]. Wireless Personal Communications, 2021, 117(1): 47-69.
- [4] 李尚, 周志刚, 张宏莉, 等. 大数据安全高效搜索与隐私保护机制展望[J]. 网络与信息安全学报, 2016, 2(4): 21-32.
- LI S, ZHOU Z G, ZHANG H L, et al. Prospect of secure-efficient search and privacy-preserving mechanism on big data[J]. Chinese Journal of Network and Information Security, 2016, 2(4): 21-32.
- [5] HILL J, SZEWCZYK R, WOO A, et al. System architecture directions for networked sensors[J]. ACM Sigplan Notices, 2000, 35(11): 93-104.
- [6] CHEON J H, KIM Y, YOON H J. A new ID-based signature with batch verification[J]. Cryptology EPrint Archive, 2004.
- [7] LYSYANSKAYA A, MICALI S, REYZIN L, et al. Sequential aggregate signatures from trapdoor permutations[C]//Proceedings of the 23th International Conference on the Theory and Applications of Crypto-graphic Techniques, Interlaken, Switzerland: Advances in Cryptology-EUROCRYPT 2004, 2004: 74-90.
- [8] IWASAKI T, YANAI N, INAMURA M, et al. Tightly-secure identity-based structured aggregate signature scheme under the computational Diffie Hellman assumption[C]//Proceedings of the 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA). Piscataway: IEEE Press, 2016: 669-676.
- [9] YANG X D, LIU R, WANG M D, et al. Identity-based aggregate signature scheme in vehicle ad-hoc network[C]//Proceedings of the 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE). Piscataway: IEEE Press, 2019: 1046-10463.
- [10] YAO Y Q, LI Z J, GUO H. A unified framework of identity-based sequential aggregate signatures from 2-level HIBE schemes[J]. Information Sciences, 2020, 516: 505-514.
- [11] 国家密码管理局. GM/T 0044—2016 SM9 标识密码算法[S]. 北京: 中国标准出版社, 2016.
- State Cryptography Administration. GM/T0044—2016 Information security technology Identity-based cryptographic algorithms SM9 [S]. Beijing: China Standards Press, 2016.
- [12] 国家市场监督管理总局, 国家标准化管理委员会. 信息安全技术 SM9 标识密码算法 第2部分: 算法: GB/T 38635.2—2020[S]. 北京: 中国标准出版社, 2020.
- State Administration of Market Supervision and State Standardization Administration Committee. Standardization Administration of the People's Republic of China. Information security technology —Identity-based cryptographic algorithms SM9: Part 2: algorithms: GB/T 38635.2—2020[S]. Beijing: Standards Press of China, 2020.
- [13] CHENG Z H. Security analysis of SM9 key agreement and encryption[C]//Proceedings of 14th International Conference, Fuzhou: Information Security and Cryptology, 2019: 3-25.
- [14] 胡芯忆, 何德彪, 彭聪, 等. 一种 SM9 算法 R-ate 对的快速实现方法[J]. 密码学报, 2022, 9(5): 936-948.
- HU X Y, HE D B, PENG C, et al. A fast implementation of R-ate pairing in SM9 algorithm[J]. Journal of Cryptologic Research, 2022, 9(5): 936-948.
- [15] 赖建昌, 黄欣沂, 何德彪. 一种基于商密 SM9 的高效标识广播加密方案[J]. 计算机学报, 2021, 44(5): 897-907.
- LAI J C, HUANG X Y, HE D B. An efficient identity-based broadcast encryption scheme based on SM9[J]. Chinese Journal of Computers, 2021, 44(5): 897-907.
- [16] LAI J C, HUANG X Y, HE D B, et al. Provably secure online/off-line identity-based signature scheme based on SM9[J]. The Com-

- puter Journal, 2022, 65(7): 1692-1701.
- [17] 朱留富, 李继国, 赖建昌, 等. 基于商密SM9的属性基在线/离线签名方案[J]. 计算机研究与发展, 2023, 60(2): 362-370.
ZHU L F, LI J G, LAI J C, et al. Attribute-based online/offline signature scheme based on SM9[J]. Journal of Computer Research and Development, 2023, 60(2): 362-370.
- [18] 崔岩, 黄欣沂, 赖建昌, 等. 基于SM9的匿名广播加密方案[J]. 信息安全学报, 2023, 8(6): 15-27.
CUI Y, HUANG X Y, LAI J C, et al. Anonymous broadcast encryption based on SM9[J]. Journal of Cyber Security, 2023, 8(6): 15-27.
- [19] 王后珍, 秦婉颖, 刘芹, 等. 基于身份的群组密钥分发方案[J]. 计算机研究与发展, 2023, 60(10): 2203-2217.
WANG H Z, QIN W Y, LIU Q, et al. Identity based group key distribution scheme[J]. Journal of Computer Research and Development, 2023, 60(10): 2203-2217.
- [20] 杨亚涛, 蔡居良, 张筱薇, 等. 基于SM9算法可证明安全的区块链隐私保护方案[J]. 软件学报, 2019, 30(6): 1692-1704.
YANG Y T, CAI J L, ZHANG X W, et al. Privacy preserving scheme in block chain with provably secure based on SM9 algorithm[J]. Journal of Software, 2019, 30(6): 1692-1704.
- [21] 朱宏颖, 张新有, 邢焕来, 等. 边缘计算环境下轻量级终端跨域认证协议[J]. 网络与信息安全学报, 2023, 9(4): 74-89.
ZHU H Y, ZHANG X Y, XING H L, et al. Lightweight terminal cross-domain authentication protocol in edge computing environment[J]. Chinese Journal of Network and Information Security, 2023, 9(4): 74-89.
- [22] 唐飞, 甘宁, 阳祥贵, 等. 基于区块链与国密SM9的抗恶意KGC无证书签名方案[J]. 网络与信息安全学报, 2022, 8(6): 9-19.
TANG F, GAN N, YANG X G, et al. Anti malicious KGC certificateless signature scheme based on blockchain and domestic cryptographic SM9[J]. Chinese Journal of Network and Information Security, 2022, 8(6): 9-19.
- [23] 吕尧, 侯金鹏, 聂冲, 等. 基于SM9算法的部分盲签名方案[J]. 网络与信息安全学报, 2021, 7(4): 147-153.
LYU Y, HOU J P, NIE C, et al. Partial blind signature scheme based on SM9 algorithm[J]. Chinese Journal of Network and Information Security, 2021, 7(4): 147-153.
- [24] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396.
- [25] WU G, ZHANG F T, SHEN L M, et al. Certificateless aggregate signature scheme secure against fully chosen-key attacks[J]. Information Sciences, 2020, 514: 288-301.
- [26] 杨小东, 麻婷春, 陈春霖, 等. 面向车载自组网的无证书聚合签名方案的安全性分析与改进[J]. 电子与信息学报, 2019, 41(5): 1265-1270.
YANG X D, MA T C, CHEN C L, et al. Security analysis and improvement of certificateless aggregate signature scheme for vehicular ad hoc networks[J]. Journal of Electronics & Information Technology, 2019, 41(5): 1265-1270.
- [27] SHEN L M, MA J F, MIAO Y B, et al. Provably secure certificateless aggregate signature scheme with designated verifier in an improved security model[J]. IET Information Security, 2019, 13(3): 167-173.

[作者简介]



李继国 (1970-), 男, 黑龙江齐齐哈尔人, 福建师范大学教授, 主要研究方向为公钥密码学、云计算安全。



方淳 (2001-), 男, 湖北黄冈人, 主要研究方向为公钥密码学、云计算安全。