中国科学: 信息科学 2021 年 第 51 卷 第 11 期: 1900–1913
SCIENTIA SINICA Informationis
论文

国密 SM9 数字签名和密钥封装算法的安全性分析

赖建昌[1], 黄欣沂[1*], 何德彪[2], 伍玮[3]

1. 福建师范大学计算机与网络空间安全学院, 福建省网络安全与密码技术重点实验室, 福州 350117
2. 武汉大学网络安全学院, 空天信息安全与可信计算教育部重点实验室, 武汉 430072
3. 福建师范大学数学与统计学院, 福建省应用数学中心, 福州 350117
* 通信作者. E-mail: xyhuang@fjnu.edu.cn

收稿日期: 2021–02–09; 修回日期: 2021–04–08; 接受日期: 2021–04–12; 网络出版日期: 2021–11–02

国家自然科学基金 (批准号: 61902191, 62032005, 61872089, 61972294)、江苏省自然科学基金 (批准号: BK20190696) 和福建省自然科学基金 (批准号: 2020J02016) 资助项目

摘要 安全性分析为密码方案的安全性提供重要依据和有力保障. 我国自主设计的商用标识密码 SM9 已成为国家标准, 其中, SM9 数字签名算法和加密算法已成为 ISO/IEC 国际标准. 然而, 现有关于 SM9 标识密码算法安全性分析的公开发表研究成果较少. Cheng 在 Inscrypt 2018 基于 Gap-q-BCAA1 假设, 给出了 SM9 密钥交换协议、密钥封装机制和公钥加密算法的安全性证明. 本文首先基于 q-SDH 假设和随机谕言模型, 证明 SM9 数字签名算法具有 EUF-CMIA 的安全性. 其次, 为了消除对 Gap 类困难假设的依赖, 采用 Twin-Hash-ElGamal 技术, 提出基于 SM9 密钥封装机制的新型密钥封装机制 Twin-SM9. 与 SM9 密钥封装机制相比, Twin-SM9 的系统公钥和用户私钥分别增加了一个群元素, 而封装密文长度保持不变. 在随机谕言模型中证明, 若 q-BDHI 假设成立, 则 Twin-SM9 密钥封装机制满足 IND-CCA. 然后进一步阐明了 SM9 标识密码的安全性, 研究结果有助于基于 SM9 的高级密码协议和算法的设计与分析.

关键词 SM9, 安全性分析, 数字签名, 密钥封装, CCA

1 引言

为消除传统公钥系统中对证书的依赖, Shamir [1] 于 1984 年开创性地提出了标识密码的概念. 在标识密码系统中, 用户的公钥不再通过证书获得, 而是由能唯一标识用户身份的任意字符串组成, 比如电话号码、邮箱地址等. 用户的私钥由私钥生成中心 (key generator center, KGC) 生成并通过安全信道传送给用户. 只有拥有私钥的用户才能正确解密匹配标识加密的密态数据. 自标识密码的概念提出后, 标识密码得到了广泛的研究. 2001 年, Boneh 和 Franklin [2] 采用双线性对技术, 提出首个实用且可证明安全的标识加密方案. 此后, 双线性对技术被用于构造多种高效的标识密码算法 [3~8].

引用格式: 赖建昌, 黄欣沂, 何德彪, 等. 国密 SM9 数字签名和密钥封装算法的安全性分析. 中国科学: 信息科学, 2021, 51: 1900–1913, doi: 10.1360/SSI-2021-0049
Lai J C, Huang X Y, He D B, et al. Security analysis of SM9 digital signature and key encapsulation (in Chinese). Sci Sin Inform, 2021, 51: 1900–1913, doi: 10.1360/SSI-2021-0049

虽然标识密码取得了积极进展, 但是从整体上看, 标识密码算法以国外算法为主. 为满足核心技术自主创新、信息安全自主可控的要求, 我国自主设计了包括密钥交换协议、数字签名算法、密钥封装机制和公钥加密算法的 SM9 标识系列密码 [9]. SM9 标识密码分别于 2016 年和 2020 年成为了我国商用密码行业标准和国家标准, 其中, SM9 数字签名算法和加密算法先后成为 ISO/IEC 国际标准.

随着 SM9 标识密码算法陆续成为国家标准和国际标准, 国内学者越来越关注 SM9 标识密码, 并取得重要的相关研究成果. Cheng [10] 分析了 SM9 密码算法的安全性, 并基于 Gap 类困难假设给出 SM9 密钥交换协议、密钥封装机制和公钥加密算法的安全性证明. 文献 [11] 结合盲签名技术, 首先利用 SM3 杂凑算法对消息进行盲化处理, 并提出基于 SM9 的盲签名方案. 文献 [12] 采用构建预计算矩阵的方法, 提高了 SM9 数字签名中签名和验证算法的计算效率. Xu 等 [13] 改进了 Wang 等 [14] 的私钥分发方案和 Gesiler 等 [15] 的私钥产生方案, 并提出基于 SM9 的可分离匿名分布式私钥产生分发方案. 私钥的产生过程不涉及双线性对运算. 针对区块链交易过程中存在隐私泄露问题, Yang 等 [16] 基于 SM9 提出一种满足不可伪造、保证节点匿名和前向安全等性能的群签名方案. 文献 [17] 研究 SM9 标识加密算法中用户的撤销, 提出具有鲁棒性的服务器辅助撤销方案. SM9 中 R-ate 双线性对计算的优化方法在文献 [18,19] 中得到进一步研究.

安全性分析是密码学的重要研究领域, 它为密码方案的安全性提供有力保障和重要依据. 尽管近几年 SM9 标识密码的研究取得优秀成果, 但主要集中在算法效率的提升和功能的扩展. 关于 SM9 标识密码算法安全性分析的公开研究成果较少. 目前仅有文献 [10] 基于 Gap-q-BCAA1 困难假设, 给出了 SM9 密钥交换协议、密钥封装机制和加密算法的安全性证明. 尚未发现关于 SM9 标识签名算法安全性证明的公开研究成果.

1.1 本文贡献

本文首先分析了 SM9 数字签名算法的安全性, 给出 SM9 数字签名算法的安全性证明. 基于 q-strong Diffie-Hellman (q-SDH) 假设, 证明 SM9 数字签名算法在随机谕言模型下满足 EUF-CMIA 安全性.

其次, 为了消除文献 [10] 对 Gap 类困难假设的依赖, 本文采用 Twin-Hash-ElGamal 技术, 在不弱化安全性的前提下改进 SM9 密钥封装算法, 提出新型的密钥封装机制 Twin-SM9. Twin-SM9 的安全性可归约到 q-bilinear Diffie-Hellman inversion (q-BDHI) 假设. 在随机谕言模型下, 证明 Twin-SM9 在适应性选择密文攻击下具有不可区分的安全性. 与 SM9 密钥封装机制相比, Twin-SM9 的系统公钥和用户私钥分别只增加一个群元素, 但封装密文格式保持不变, 安全性基于更弱的 q-BDHI 假设. 本文结果进一步阐明了 SM9 标识密码的安全性, 有助于基于 SM9 的高级密码协议和算法的设计与分析.

1.2 本文组织结构

第 2 节回顾双线性群、困难假设、标识数字签名算法和密钥封装机制的形式化定义等预备知识. 第 3 节回顾 SM9 数字签名算法, 并给出规范化安全证明. 第 4 节基于 SM9 密钥封装机制, 提出一个新的密钥封装算法 Twin-SM9, 根据安全模型证明了算法的安全性, 并分析算法性能. 第 5 节对本文的工作进行总结.

2 预备知识

本节回顾双线性群、困难假设、标识数字签名和标识密钥封装算法的形式化定义及其安全模型等

基本知识. 在描述基本知识之前, 先给出符号说明. $\mathcal{BP}$ 表示双线性群, xP 表示加法群中元素 P 的 x 倍, g^x 表示乘法群中元素 g 的 x 次幂, $x||y$ 表示 x 与 y 的拼接, x 和 y 是比特串或者字符串. 如果 A 是一个概率算法, 则 $y \leftarrow \mathsf{A}(x)$ 表示以 x 为输入, 将算法 A 的输出赋值给 y. 令 $\mathbb{N}$ 表示自然数集合, 则函数 $\epsilon : \mathbb{N} \to [0,1]$ 是可忽略的, 如果对每个 $d \in \mathbb{N}$, 存在 $\lambda_d \in \mathbb{N}$ 使得对所有 $\lambda > \lambda_d$, 都有 $\epsilon(\lambda) \leqslant \lambda^{-d}$.

2.1 双线性群

设 λ 为安全参数, p 是与 λ 相关的大素数. $\mathbb{G}_1$, $\mathbb{G}_2$ 和 $\mathbb{G}_T$ 都是阶为 p 的循环群, 映射 $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ 称为双线性映射若满足以下条件:

(1) 双线性性 (bilinearity). 对任意的元素 $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$ 和 $a, b \in \mathbb{Z}_p$, 有 $e(aP, bQ) = e(P, Q)^{ab}$;

(2) 非退化性 (non-degeneracy). 至少存在元素 $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$, 满足 $e(P, Q) \neq 1$;

(3) 可计算性 (computability). 对任意的 $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$, 存在多项式时间算法高效计算 $e(P, Q)$.

双线性群 $\mathcal{BP}$ 由以上五元组 $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, p)$ 组成. 若 $\mathbb{G}_1 = \mathbb{G}_2$, 则称为对称双线性群 (第 1 类), 否则称为非对称双线性群 (第 2 和 3 类). 设 P, Q 分别为群 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 的生成元, 则在第 2 类双线性群中, 存在有效的公开可计算同构映射 $\psi : \mathbb{G}_2 \to \mathbb{G}_1$, 使得 $\psi(Q) = P$. SM9 标识密码基于第 2 类双线性群.

2.2 困难问题假设

令 P, Q 分别为群 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 的生成元, 则基于非对称双线性群的 q-SDH 问题和 q-BDHI 问题的定义如下.

定义1 (q-SDH 问题) 已知 $q+2$ 个元素 $(P, Q, aQ, a^2Q, \ldots, a^qQ) \in \mathbb{G}_1 \times \mathbb{G}_2^{q+1}$, 其中 a 未知, 找到一个二元组 $(c,\ \frac{1}{c+a}P)$, 其中 $c \in \mathbb{Z}_p^*$.

定义2 (q-BDHI 问题) 已知 $q+2$ 个元素 $(P, Q, aQ, a^2Q, \ldots, a^qQ) \in \mathbb{G}_1 \times \mathbb{G}_2^{q+1}$, 其中 a 未知, 计算 $e(P, Q)^{\frac{1}{a}}$.

若 q-SDH 问题在多项式时间内可解的概率是可忽略的, 则称 q-SDH 假设成立. 同理, 若 q-BDHI 问题在多项式时间内可解的概率是可忽略的, 则称 q-BDHI 假设成立.

2.3 标识签名的定义和安全模型

标识签名 (identity-based signature) 由以下 4 个多项式时间算法组成.

• $(\mathrm{mpk}, \mathrm{msk}) \leftarrow \mathbf{Setup}(\lambda)$. 已知系统安全参数 λ, 系统建立算法 **Setup** 以 λ 为输入, 输出系统主公钥 mpk 和主私钥 msk, 其中 mpk 是公开的, msk 由 KGC 秘密保存. 此算法由 KGC 执行.

• $\mathrm{sk}_{\mathrm{ID}} \leftarrow \mathbf{KeyGen}(\mathrm{mpk}, \mathrm{msk}, \mathrm{ID})$. 已知标识 ID, 用户私钥生成算法 **KeyGen** 以系统主公私钥对 $(\mathrm{mpk}, \mathrm{msk})$ 和 ID 为输入, 输出用户 ID 的私钥 $\mathrm{sk}_{\mathrm{ID}}$. 此算法由 KGC 执行.

• $\sigma \leftarrow \mathbf{Sign}(\mathrm{mpk}, M, \mathrm{sk}_{\mathrm{ID}})$. 已知消息 M, 签名算法 **Sign** 以系统主公钥 mpk、M 和签名者的私钥 $\mathrm{sk}_{\mathrm{ID}}$ 为输入, 输出 M 的签名 σ. 此算法由签名者执行.

• $1/0 \leftarrow \mathbf{Verify}(\mathrm{mpk}, M, \sigma, \mathrm{ID})$. 验证算法 **Verify** 以系统主公钥 mpk、签名消息 M 及其签名 σ 和签名者的标识 ID 为输入, 输出 “1” 或者 “0”. “1” 表示签名有效, “0” 表示签名无效. 此算法由验证者执行.

标识签名算法的正确性要求对任意的 $(\mathrm{mpk}, \mathrm{msk}) \leftarrow \mathbf{Setup}(\lambda)$, $\mathrm{sk}_{\mathrm{ID}} \leftarrow \mathbf{KeyGen}(\mathrm{mpk}, \mathrm{msk}, \mathrm{ID})$ 和 $\sigma \leftarrow \mathbf{Sign}(\mathrm{mpk}, M, \mathrm{sk}_{\mathrm{ID}})$, 有 $\mathbf{Verify}(\mathrm{mpk}, M, \sigma, \mathrm{ID}) = 1$.

标识签名安全模型. 数字签名的标准安全模型为存在性不可伪造. 本文参考文献 [20], 给出适应性选择消息和标识攻击下的存在性不可伪造 (existentially unforgeable against adaptive chosen message and identity attacks, EUF-CMIA) 安全模型. 该安全模型通过挑战者 (challenger) 和攻击者 (adversary) 完成的游戏定义. EUF-CMIA 安全模型的定义如下:

• 系统建立阶段. 已知安全参数 λ, 挑战者运行算法 **Setup**(λ), 生成系统主公私钥对 $(\mathrm{mpk}, \mathrm{msk})$, 并将 mpk 发送给攻击者.

• 私钥询问. 已知标识 ID, 挑战者运行用户私钥生成算法 **KeyGen** 生成私钥 $\mathrm{sk}_{\mathrm{ID}}$, 并发送给攻击者.

• 签名询问. 已知标识 ID 和消息 M, 挑战者首先运行用户私钥生成算法 **KeyGen** 生成用户 ID 的私钥 $\mathrm{sk}_{\mathrm{ID}}$, 然后以 $\mathrm{sk}_{\mathrm{ID}}$ 和 M 为输入, 运行算法 **Sign** 生成签名 σ, 并将 σ 发送给攻击者.

• 伪造阶段. 最后, 攻击者输出标识 ID^* 对消息 M^* 的伪造签名 σ^*. 模型要求攻击者没有询问过标识 ID^* 的私钥. 若攻击者没有询问过标识 ID^* 对消息 M^* 的签名且 σ^* 是消息 M^* 的有效签名, 则攻击者获胜.

定义模型中攻击者 $\mathcal{A}$ 的优势 $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{EUF\text{-}CMIA}}(\lambda)$ 为赢得以上 EUF-CMIA 游戏的概率.

定义3 在 EUF-CMIA 安全模型中, 如果对任意多项式时间攻击者 $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{EUF\text{-}CMIA}}(\lambda)$ 都是可忽略的, 称标识签名算法是 EUF-CMIA 安全的.

2.4 标识密钥封装的定义和安全模型

标识密钥封装 (identity-based key encapsulation) 由以下 4 个多项式时间算法描述.

• $(\mathrm{mpk}, \mathrm{msk}) \leftarrow$ **Setup**(λ). 已知系统安全参数 λ, 系统建立算法 **Setup**(λ) 为输入, 输出系统主公钥 mpk 和主私钥 msk, 其中 mpk 是公开的, msk 由 KGC 秘密保存. 此算法由 KGC 执行.

• $\mathrm{sk}_{\mathrm{ID}} \leftarrow$ **KeyGen**$(\mathrm{mpk}, \mathrm{msk}, \mathrm{ID})$. 已知标识 ID, 用户私钥生成算法 **KeyGen** 以 $(\mathrm{mpk}, \mathrm{msk})$ 和 ID 为输入, 输出用户 ID 对应的私钥 $\mathrm{sk}_{\mathrm{ID}}$. 此算法由 KGC 执行.

• $(C, K) \leftarrow$ **Encap**$(\mathrm{mpk}, \mathrm{ID})$. 密钥封装算法 **Encap** 以系统主公钥 mpk 和接收者标识 ID 为输入, 输出密文 C 和封装的会话密钥 (简称封装密钥) K. 此算法由密钥封装者执行.

• $K/\perp \leftarrow$ **Decap**$(\mathrm{mpk}, C, \mathrm{sk}_{\mathrm{ID}})$. 解封装算法 (解密算法) **Decap** 以系统主公钥 mpk, 密钥封装密文 C 和接收者私钥 $\mathrm{sk}_{\mathrm{ID}}$ 为输入, 输出封装密钥 (会话密钥) K 或者解密失败符号 "$\perp$". 此算法由解密者执行.

标识密钥封装算法的正确性要求对任意的 $(\mathrm{mpk}, \mathrm{msk}) \leftarrow$ **Setup**(λ), $\mathrm{sk}_{\mathrm{ID}} \leftarrow$ **KeyGen**$(\mathrm{mpk}, \mathrm{msk}, \mathrm{ID})$ 和 $(C, K) \leftarrow$ **Encap**$(\mathrm{mpk}, \mathrm{ID})$, 有 **Decap**$(\mathrm{mpk}, C, \mathrm{sk}_{\mathrm{ID}}) = K$.

标识密钥封装安全模型. 标识密钥封装机制在适应性选择密文攻击下的不可区分 (indistinguishability against adaptive chosen-ciphertext attacks, IND-CCA) 安全模型确保只有拥有正确私钥的用户才能获得封装的会话密钥. 模型通过挑战者和攻击者参与的游戏定义. IND-CCA 安全模型的定义如下:

• 系统建立阶段. 已知安全参数 λ, 挑战者运行算法 **Setup**(λ), 生成系统主公私钥对 $(\mathrm{mpk}, \mathrm{msk})$, 并将 mpk 发送给攻击者.

• 询问阶段 1. 攻击者允许适应性发起解密私钥询问和密文解密询问.

(1) 解密私钥询问. 已知标识 ID, 挑战者运行算法 **KeyGen** 生成私钥 $\mathrm{sk}_{\mathrm{ID}}$, 并发送给攻击者.

(2) 密文解密询问. 已知封装密文 (C, ID), 挑战者首先运行算法 **KeyGen** 产生私钥 $\mathrm{sk}_{\mathrm{ID}}$, 然后以 $\mathrm{sk}_{\mathrm{ID}}$ 和 C 为输入运行算法 **Decap**, 并将输出结果发送给攻击者.

• 挑战阶段. 询问阶段 1 结束后, 攻击者输出挑战标识 ID^*. 模型要求攻击者没有询问过 ID^* 的私钥. 挑战者运行算法 $\mathbf{Encap}(\mathrm{mpk}, \mathrm{ID}^*)$ 生成挑战封装密文和封装密钥 (C^*, K^*). 接着, 随机选择一个比特 $\mu \in \{0,1\}$, 设 $K_\mu = K^*$, 并从封装密钥空间中随机选择一个会话密钥设为 $K_{1-\mu}$, 返回 (C^*, K_0, K_1) 给攻击者.

• 询问阶段 2. 攻击者允许继续向挑战者发起解密私钥询问和密文解密询问. 模型要求攻击者不能询问 ID^* 的私钥, 也不能提出密文 (C^*, ID^*) 的解密询问. 挑战者根据询问阶段 1 回复攻击者.

• 猜测阶段. 最后, 攻击者输出 μ 的猜测 $\mu' \in \{0,1\}$. 如果 $\mu' = \mu$, 则攻击者获胜.

定义攻击者 $\mathcal{A}$ 获胜的优势为

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}CCA}}(\lambda) = \left| \Pr[\mu' = \mu] - \frac{1}{2} \right|.$$

定义4 在 IND-CCA 安全模型中, 如果对任意多项式时间攻击者 $\mathcal{A}$, $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IND\text{-}CCA}}(\lambda)$ 都是可忽略的, 称密钥封装算法是 IND-CCA 安全的.

3 SM9 签名算法

本节将根据文献 [9] 回顾 SM9 签名算法, 算法描述采用文献 [9] 的符号.

3.1 算法描述

• **Setup.** 已知安全参数 λ, KGC 首先选取一个第 2 类双线群 $\mathcal{BP} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, N)$, 其中 N 为大素数且 $N > 2^\lambda$, 并随机选择群 $\mathbb{G}_1, \mathbb{G}_2$ 的生成元 P_1, P_2, 则有 $P_1 = \psi(P_2)$. 选择随机数 $\alpha \in [1, N-1]$, 两个密码杂凑函数 $H_1 : \{0,1\}^* \times \mathbb{Z}_N^* \to \mathbb{Z}_N^*$ 和 $H_2 : \{0,1\}^* \times \mathbb{Z}_N^* \to \mathbb{Z}_N^*$. 计算群 $\mathbb{G}_2$ 中的元素 $P_{\mathrm{pub}} = \alpha P_2$, 计算群 $\mathbb{G}_T$ 中的元素 $g = e(P_1, P_{\mathrm{pub}})$, 并选取用一个字节表示的私钥生成函数识别符 hid. 输出系统主公钥 mpk 和主私钥 msk

$$\mathrm{mpk} = (\mathcal{BP}, P_1, P_2, P_{\mathrm{pub}}, g, H_1, H_2, \mathrm{hid}), \quad \mathrm{msk} = \alpha.$$

• **KeyGen.** 已知用户标识 $\mathrm{ID} \in \{0,1\}^*$, KGC 首先在有限域 F_N 上计算非零元素 $t_1 = H_1(\mathrm{ID}||\mathrm{hid}, N) + \alpha$, $t_2 = \alpha \cdot t_1^{-1}$, 然后计算 $\mathrm{sk}_{\mathrm{ID}} = t_2 \cdot P_1$, 把 $\mathrm{sk}_{\mathrm{ID}}$ 作为用户的签名私钥.

• **Sign.** 令待签名的消息为 $M \in \{0,1\}^*$, 签名者的标识为 ID, 签名私钥为 $\mathrm{sk}_{\mathrm{ID}}$, 签名者执行以下运算生成消息 M 的签名.

A1. 产生随机数 $r \in [1, N-1]$;

A2. 计算群 $\mathbb{G}_T$ 中的元素 $w = g^r$;

A3. 计算整数 $h = H_2(M||w, N)$;

A4. 计算整数 $\ell = (r - h) \mod N$, 若 $\ell = 0$ 则返回 A1;

A5. 计算群 $\mathbb{G}_1$ 中的元素 $S = \ell \mathrm{sk}_{\mathrm{ID}}$;

A6. 输出消息 M 的签名 $\sigma = (h, S)$.

• **Verify.** 已知消息 M' 及其签名 $\sigma' = (h', S')$, 验证者执行以下运算验证签名的有效性.

B1. 计算群 $\mathbb{G}_T$ 中的元素 $t' = g^{h'}$;

B2. 计算整数 $h_1 = H_1(\mathrm{ID}||\mathrm{hid}, N)$;

B3. 计算群 $\mathbb{G}_2$ 中的元素 $P = h_1 P_2 + P_{\mathrm{pub}}$;

B4. 计算群 $\mathbb{G}_T$ 中的元素 $u = e(S', P)$;

B5. 计算群 $\mathbb{G}_T$ 中的元素 $w' = u \cdot t$;

B6. 计算整数 $h_2 = H_2(M'||w', N)$, 检查 $h_2 = h'$ 是否成立, 若成立则验证通过, 输出 "1"; 否则验证不通过, 输出 "0".

3.2 SM9 签名算法安全性分析

本小节分析 SM9 签名算法的安全性, 在 q-SDH 假设和随机谕言模型下证明 SM9 签名算法是 EUF-CMIA 安全的.

定理1 设 SM9 签名算法中的密码杂凑函数 H_1, H_2 是随机谕言器. 如果 q-SDH 假设成立, 则 SM9 签名算法是 EUF-CMIA 安全的.

证明 假设在 EUF-CMIA 安全模型中存在多项式时间概率攻击算法 $\mathcal{A}$, 在询问 q_{H_i} 次随机谕言器 H_i $(i = 1, 2)$ 后, 能以不可忽略的优势 (概率) ϵ 成功伪造签名. 我们可构造一个多项式时间概率模拟算法 $\mathcal{B}$ 与 $\mathcal{A}$ 交互后, 能以 $\frac{\epsilon}{q_{H_1}}$ 的概率解决 q-SDH 问题. 已知 $\mathcal{B}$ 以一个 q-SDH 问题的实例 $(P, Q, aQ, a^2Q, \ldots, a^qQ) \in \mathbb{G}_1 \times \mathbb{G}_2^{q+1}$ 为输入, 其中群 $\mathbb{G}_1, \mathbb{G}_2$ 的阶为大素数 N, $q = q_{H_1}$. $\mathcal{B}$ 的目标是找到一对元素 $(c, \frac{1}{c+a}P)$, 其中 $c \in \mathbb{Z}_N^*$. 在不影响安全性的前提下, 为描述方便, 证明中忽略密码杂凑函数 H_1, H_2 中 hid 和 N 的输入.

系统建立阶段. $\mathcal{B}$ 首先隐式 (implicitly) 设系统主私钥 msk 为 $\alpha = a$, 其中 a 是未知的, 并执行以下步骤生成系统主公钥.

(1) 随机选择 $i^* \in [1, q]$, 从 $\mathbb{Z}_N^*$ 中随机选取 q 个两两不同的数 $x^*, x_1, x_2, \ldots, x_{i^*-1}, x_{i^*+1}, \ldots, x_q$, 并定义多项式

$$f(z) = \prod_{i=1, i\neq i^*}^{q} (z + x_i) = \sum_{i=0}^{q-1} c_i z^i \mod N,$$

其中 c_i 为多项式 $f(z)$ 的系数.

(2) 计算群 $\mathbb{G}_2$ 的生成元 $P_2 = \sum_{i=0}^{q-1} c_i(a^iQ) = f(a)Q$, 计算群 $\mathbb{G}_1$ 的生成元 $P_1 = \psi(P_2) = f(a)P \in \mathbb{G}_1$. 计算群 $\mathbb{G}_2$ 的元素 $P_{\text{pub}} = \sum_{i=0}^{q-1} c_i(a^{i+1}Q) = aP_2$, 群 $\mathbb{G}_T$ 的元素 $g = e(P_1, P_{\text{pub}})$, 其中 $\psi(Q) = P$.

(3) 对任意的 $i \in [1, q]\backslash i^*$, 定义

$$f_i(z) = \frac{f(z)}{z + x_i} = \sum_{i=0}^{q-2} d_i z^i,$$

计算

$$\sum_{i=0}^{q-2} d_i \psi(a^{i+1}Q) = a f_i(a) P = \frac{a f(a)}{a + x_i} P = \frac{a}{a + x_i} P_1.$$

因此, 对任意的 $i \in [1, q]\backslash i^*$, 二元组 $(x_i, V_i = \frac{a}{a+x_i}P_1)$ 是可以计算的.

最后 $\mathcal{B}$ 设系统主公钥 $\text{mpk} = (P_1, P_2, g, P_{\text{pub}})$, 其中 H_1, H_2 是由 $\mathcal{B}$ 掌控的随机谕言器.

哈希询问阶段. $\mathcal{A}$ 允许询问谕言器 H_1 和 H_2.

• H_1 – 询问. 已知标识 ID_i, $\mathcal{B}$ 为 H_1 询问建立列表 L_1, 表中元素以二元组 (ID, x) 的形式存储. 若询问的 ID_i 在 L_1 中, 则返回相应的 x_i. 否则, 记 ID_i 为第 i 个新标识的询问. 如果 $i = i^*$, 设 $H_1(\text{ID}_{i^*}) = x^*$ 并发送 x^* 给 $\mathcal{A}$, 以 (ID_{i^*}, x^*) 更新 L_1. 如果 $i \neq i^*$, 设 $H_1(\text{ID}_i) = x_i$, 发送 x_i 给 $\mathcal{A}$ 并以 (ID_i, x_i) 更新 L_1.

• H_2 – 询问. 已知二元组 (M_i, w_i), $\mathcal{B}$ 为 H_2 询问建立列表 L_2, 表中元素以三元组 (M, w, h) 的形式存储. 如果 (M_i, w_i) 在 L_2 中, 则返回相应的 h_i. 否则, 从 $\mathbb{Z}_N^*$ 中随机选取一个元素 h_i, 设 $H_2(M_i, w_i) = h_i$, 发送 h_i 给 $\mathcal{A}$ 并以 (M_i, w_i, h_i) 更新 L_2.

询问阶段.

• 私钥询问. 记 ID_i 为第 i 个新标识的询问. 若 $i = i^*$, $\mathcal{B}$ 停止模拟并输出失败. 若 $i \neq i^*$, $\mathcal{B}$ 询问 H_1 谕言器可获得 x_i, 返回 $V_i = \frac{a}{a+x_i} P_1$ 作为 ID_i 的签名私钥.

• 签名询问. 记第 i 个消息标识对为 (M_i, ID_i), 若 $i \neq i^*$, 则 $\mathcal{B}$ 可获得对应的签名私钥, 并根据签名算法生成有效的签名. 若 $i = i^*$, $\mathcal{B}$ 随机选取 $S \in \mathbb{G}_1, h \in \mathbb{Z}_N^*$, 计算 $P^* = x^* P_2 + P_{\mathrm{pub}}$, 计算 $\mathbb{G}_T$ 中的元素 $w = e(S, P^*)\, e(P_1, P_{\mathrm{pub}})^h$, 并定义 $H_2(M||w) = h$. 若 (M, w) 被询问过, $\mathcal{B}$ 输出模拟失败. 但该事件发生的概率为 $\frac{q_{H_2}+q_s}{2^\lambda}$ 是可忽略的, 其中 q_s 为签名询问的次数. 最后 $\mathcal{B}$ 把 (h, S) 作为签名发送给 $\mathcal{A}$.

伪造阶段. $\mathcal{A}$ 输出伪造签名 $(\sigma^*, M^*, \mathrm{ID}^*)$, 其中 $\sigma^* = (h^*, S^*)$. 令 ID^* 的下标为 i. 若 $i \neq i^*$, $\mathcal{B}$ 停止模拟并输出失败. 若 $i = i^*$, $\mathcal{B}$ 执行以下步骤. 根据分叉引理 (Forking Lemma) [21], 设签名方案的签名为 (M, w, h, S), 其中 w, h, S 是一个三次交互零知识协议. 则存在一个 CMA 的攻击算法 $\mathcal{A}$ 能在时间 t 内以 $\epsilon > \frac{10(q_s+1)(q_s+q_h)}{2^\lambda}$ 的概率成功伪造签名 (M, w, h, S), 其中 q_s 和 q_h 分别为签名询问和随机谕言器的次数. 如果 (M, w, h, S) 是在不知道相应签名私钥情况下伪造的, 则存在一个图灵机 $\mathcal{A}'$ 通过 $\mathcal{A}$ 的帮助, 以相同的输入 $(\mathrm{mpk}, M, \mathrm{ID})$ 在时间 $t' < 120686 q_h t/\epsilon$ 内输出两个有效的签名 (M, w, h_1, S_1) 和 (M, w, h_2, S_2), 其中 $h_1 \neq h_2, S_1 \neq S_2$.

据此, $\mathcal{B}$ 运行 $\mathcal{A}'$, 获得两个关于 $(\mathrm{mpk}, \mathrm{ID}^*)$ 的有效签名 (M^*, r^*, h_1^*, S_1^*) 和 (M^*, r^*, h_2^*, S_2^*), 则满足验证等式

$$e(S_1^*, H_1(\mathrm{ID}^*)P_2 + P_{\mathrm{pub}}) \cdot e(P_1, P_{\mathrm{pub}})^{h_1^*} = e(S_2^*, H_1(\mathrm{ID}^*)P_2 + P_{\mathrm{pub}}) \cdot e(P_1, P_{\mathrm{pub}})^{h_2^*}.$$

化简得到

$$e((a^{-1}(h_2^* - h_1^*)^{-1})(S_1^* - S_2^*), (x^* + a)P_2) = e(P_1, P_2).$$

令 $Y^* = \frac{1}{h_2^* - h_1^*}(S_1^* - S_2^*)$, 则根据等式有 $Y^* = \frac{a}{x^*+a} P_1$. 又

$$\frac{zf(z)}{z + x^*} = \frac{\gamma}{z + x^*} + \sum_{i=0}^{k-1} \gamma_i z^i,\ P_1 = f(a)P,$$

其中 γ, γ_i 是可求的系数且 $\gamma \neq 0$. 最后计算

$$X^* = \frac{1}{\gamma}\left(Y^* - \sum_{i=0}^{k-1} \gamma_i \psi\left(a^i Q\right)\right) = \frac{1}{a + x^*} P,$$

并输出 (x^*, X^*) 作为 q-SDH 问题实例的解.

根据以上证明可知, 在伪造阶段, 若 $\mathcal{A}$ 输出伪造签名中 $\mathrm{ID}^* = \mathrm{ID}_{i^*}$, 则 $\mathcal{A}$ 未询问标识 ID_{i^*} 的签名私钥. 此事件发生的概率为 $\frac{1}{q_{H_1}}$, 即 $\mathcal{B}$ 能成功模拟的概率为 $\frac{1}{q_{H_1}}$. 因此, 若 $\mathcal{A}$ 能以不可忽略的概率 ϵ 成功伪造有效签名, 则 $\mathcal{B}$ 能以 $\frac{\epsilon}{q_{H_1}}$ 的概率成功求解 q-SDH 问题.

4 Twin-SM9 密钥封装算法

2018 年, Cheng [10] 给出了 SM9 密钥封装算法的安全性分析, 基于 Gap-q-BCAA1 假设 [22], 在随机谕言模型下证明 SM9 密钥封装算法是 IND-CCA 安全的. 本节采用 Twin-Hash-ElGamal 技术 [23]

改进 SM9 密钥封装算法, 提出一个新的密钥封装算法 Twin-SM9. 算法在不改变 SM9 密钥封装算法安全性和密文格式的前提下, 安全性可归约到 q-BDHI 问题. 本节给出 Twin-SM9 密钥封装算法的详细描述, 算法描述采用 SM9 密钥封装算法中的符号.

4.1 方案描述

• **Setup.** 已知安全参数 λ, KGC 首先选择一个第 2 类双线群 $\mathcal{BP}=(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,N)$, 其中 N 为大素数且 $N>2^{\lambda}$, 并随机选择群 $\mathbb{G}_1,\mathbb{G}_2$ 的生成元 P_1,P_2, 则 $P_1=\psi(P_2)$. 选择随机数 $\alpha,\beta\in[1,N-1]$, 两个密码杂凑函数 $H_1:\{0,1\}^*\times\mathbb{Z}_N^*\to\mathbb{Z}_N^*$ 和 $H_2:\{0,1\}^*\times\mathbb{Z}_N^*\to\{0,1\}^{\mathrm{klen}}$, 其中 klen 为封装密钥的长度. 计算群 $\mathbb{G}_1$ 中的元素 $P_{\mathrm{pub}}=\alpha P_1$, 群 $\mathbb{G}_T$ 中的元素 $g_1=e(P_1,P_2)^{\alpha},g_2=e(P_1,P_2)^{\beta}$, 选取用一个字节表示的私钥生成函数识别符 hid. 输出系统主公钥 mpk 和主私钥 msk

$$\mathrm{mpk}=(\mathcal{BP},P_1,P_2,P_{\mathrm{pub}},g_1,g_2,H_1,H_2,\mathrm{hid}),\quad \mathrm{msk}=(\alpha,\beta).$$

• **KeyGen.** 已知用户标识 $\mathrm{ID}\in\{0,1\}^*$, KGC 首先在有限域 F_N 上计算非零元素 $t_1=H_1(\mathrm{ID}||\mathrm{hid},N)+\alpha$, 然后计算 $d_1=\alpha\cdot t_1^{-1}\cdot P_2$, $d_2=\beta\cdot t_1^{-1}\cdot P_2$, 将 $\mathrm{sk}_{\mathrm{ID}}=(d_1,d_2)$ 作为用户的解密私钥.

• **Encap.** 设需封装长度为 klen 的密钥给用户 ID, 封装者执行以下运算生成封装密文.

A1. 计算群 $\mathbb{G}_1$ 中的元素 $Q=H_1(\mathrm{ID}||\mathrm{hid},N)P_1+P_{\mathrm{pub}}$;

A2. 产生随机数 $r\in[1,N-1]$;

A3. 计算群 $\mathbb{G}_1$ 中的元素 $C=rQ$;

A4. 计算群 $\mathbb{G}_T$ 中的元素 $w_1=g_1^r,w_2=g_2^r$;

A5. 计算 $K=H_2(C||w_1||w_2||\mathrm{ID},\mathrm{klen})$, 若 K 为全 0 的比特串, 则返回 A2;

A6. 输出 (K,C), 其中 K 是被封装的密钥, C 是封装密文.

• **Decap.** 已知封装密文 C, 解密者标识 ID 及其私钥 $\mathrm{sk}_{\mathrm{ID}}$, 解密者执行以下解封装运算.

B1. 计算群 $\mathbb{G}_T$ 中的元素 $w_1'=e(C,d_1),w_2'=e(C,d_2)$;

B2. 计算封装的私钥 $K'=H_2(C||w_1'||w_2'||\mathrm{ID},\mathrm{klen})$, 若 K' 为全 0 比特串, 则报错并退出;

B3. 输出私钥 K'.

4.2 正确性分析

假设 C 为封装密文, 则通过以下等式可证明算法满足密钥封装的的正确性要求.

$$\begin{aligned}
w_1' &= e\left(C,d_1\right)\\
&= e\left(r\left(H_1\left(\mathrm{ID}||\mathrm{hid},N\right)P_1+P_{\mathrm{pub}}\right),\frac{\alpha}{H_1\left(\mathrm{ID}||\mathrm{hid},N\right)+\alpha}P_2\right)\\
&= e\left(rP_1,\alpha P_2\right)\\
&= w_1,\\
w_2' &= e\left(C,d_2\right)\\
&= e\left(r\left(H_1\left(\mathrm{ID}||\mathrm{hid},N\right)P_1+P_{\mathrm{pub}}\right),\frac{\beta}{H_1\left(\mathrm{ID}||\mathrm{hid},N\right)+\alpha}P_2\right)\\
&= e\left(rP_1,\beta P_2\right)\\
&= w_2.
\end{aligned}$$

4.3 安全性分析

定理2 设算法中的密码杂凑函数 H_1, H_2 为随机谕言器. 如果 q-BDHI 假设成立, 则本文提出的新密钥封装算法 Twin-SM9 是 IND-CCA 安全的.

证明 假设存在多项式时间概率攻击算法 $\mathcal{A}$ 以不可忽略的优势 ϵ 攻破 Twin-SM9 密钥封装算法. 我们可构造一个多项式时间概率模拟算法 $\mathcal{B}$ 以 $\frac{\epsilon}{q_{H_1}}$ 的概率成功求解 q-BDHI 问题. 已知 $\mathcal{B}$ 以一个 q-BDHI 问题实例 $\left(P, Q, aQ, a^2Q, \ldots, a^qQ\right)$ 为输入, 其目标是求 $e(P,Q)^{\frac{1}{a}}$, 其中 a 未知, $q = q_{H_1}$ 为询问随机谕言器 H_1 的次数.

系统建立阶段. $\mathcal{B}$ 选取不同的随机数 $x^*, z_1, z_2 \in \mathbb{Z}_N^*$, 在不知道 a 的前提下隐含的设 $\alpha = a - x^*$, $\beta = z_1 + z_2\alpha$. 接着, 随机选择 $i^* \in [1, q]$, 并从 $\mathbb{Z}_N^*$ 中选取 $q-1$ 个两两不同且不同于 x^* 的随机数 $x_1, x_2, \ldots, x_{i^*-1}, x_{i^*+1}, \ldots, x_q$. 定义

$$f(z) = \prod_{i=1, i\neq i^*}^{q} (z - x^* + x_i) = \sum_{i=0}^{q-1} c_i z^i \mod N,$$

$$f_i(z) = \frac{f(z)}{z - x^* + x_i} = \sum_{i=0}^{q-2} b_i z^i \mod N,$$

则

$$f(a)Q = \sum_{i=0}^{q-1} c_i \left(a^iQ\right), \quad af(a)Q = \sum_{i=0}^{q-1} c_i \left(a^{i+1}Q\right),$$

$$f_i(a)Q = \sum_{i=0}^{q-2} b_i \left(a^iQ\right), \quad af_i(a)Q = \sum_{i=0}^{q-2} b_i \left(a^{i+1}Q\right)$$

可通过已知问题实例计算得到. 接着计算

$$\begin{aligned}
&P_2 = \sum_{i=0}^{q} c_i \left(a^iQ\right) \mod N = f(a)Q,\\
&P_1 = \psi(P_2) = f(a)P,\\
&P_{\text{pub}} = \psi(af(a)Q) - x^*\psi(P_2) = \alpha P_1,\\
&g_1 = e(P_{\text{pub}}, P_2) = e(P_1, P_2)^{\alpha},\\
&g_2 = e\left(P_1, P_2\right)^{z_1} \cdot e\left(P_{\text{pub}}, P_2\right)^{z_2} = e(P_1, P_2)^{z_1 + z_2\alpha} = e(P_1, P_2)^{\beta}.
\end{aligned}$$

最后发送 $\text{mpk} = (P_1, P_2, P_{\text{pub}}, g_1, g_2)$ 给攻击算法 $\mathcal{A}$. H_1 和 H_2 在证明中被看成是由模拟算法 $\mathcal{B}$ 掌控的随机谕言器. 从系统公钥的设置可知, mpk 中的元素都可通过已知问题实例计算得到.

哈希询问阶段. $\mathcal{A}$ 允许询问随机谕言器 H_1 和 H_2.

(1) H_1 – 询问. 已知标识 ID_i, $\mathcal{B}$ 首先建立列表 $\mathcal{L}_1$ 用于记录 H_1 询问的输入和输出, 表中元素以 (ID, x) 形式存储. 令 ID_i 为第 i 个 H_1 询问, 若 ID_i 在 $\mathcal{L}_1$ 中, 则返回相应的 x_i. 否则设

$$H_1\left(\text{ID}_i\right) = \begin{cases} x^*, & \text{if } i = i^*,\\ x_i, & \text{otherwise.} \end{cases}$$

最后, $\mathcal{B}$ 发送 x_i 或者 x^* 给 $\mathcal{A}$ 并以 (ID_i, x_i) 或者 (ID_{i^*}, x^*) 更新 $\mathcal{L}_1$.

(2) H_2 – 询问. $\mathcal{B}$ 首先建立列表 $\mathcal{L}_2$ 用于记录 H_2 询问的输入和输出, 表中元素以 $(C, w_1, w_2, \mathrm{ID}, K)$ 形式存储. 令 $(C_i, w_{1,i}, w_{2,i}, \mathrm{ID}_i)$ 为第 i 个 H_2 询问, 如果 $(C_i, w_{1,i}, w_{2,i}, \mathrm{ID}_i)$ 在列表 $\mathcal{L}_2$ 中, 则返回相应的 K_i. 否则根据以下步骤回复 $\mathcal{A}$.

• 如果 $\mathrm{ID}_i = \mathrm{ID}_{i^*}$. $\mathcal{B}$ 首先从 $\mathcal{L}_1$ 中获得 $H_1(\mathrm{ID}_{i^*})$ 的值 x^* (若不存在, 以 ID_i 为输入询问 H_1 得到 x^*), 判断以下等式是否成立:

$$w_{2,i} = \left(\frac{e(C_i, P_2)}{w_{1,i}}\right)^{\frac{z_1}{x^*}} \cdot w_{1,i}^{z_2}. \tag{1}$$

• 若等式 (1) 成立, 则检查列表 $\mathcal{L}_D$(解密询问所建列表) 中是否存在元素 (C_i, ID_i). 若存在, 则获取列表 $\mathcal{L}_D$ 中相应的 K_i. 若不存在, 则以 (C_i, ID_i) 为输入发起密文解密询问获得 K_i, 并设 $H_2(C_i||w_{1,i}||w_{2,i}||\mathrm{ID}_i) = K_i$.

• 若等式 (1) 不成立, $\mathcal{B}$ 从 $\{0,1\}^{\mathrm{klen}}$ 中随机选取一个元素 K_i, 设 $H_2(C_i||w_{1,i}||w_{2,i}||\mathrm{ID}_i) = K_i$.

• 如果 $\mathrm{ID}_i \neq \mathrm{ID}_{i^*}$. $\mathcal{B}$ 从 $\{0,1\}^{\mathrm{klen}}$ 中随机选取一个元素 K_i, 设 $H_2(C_i||w_{1,i}||w_{2,i}||\mathrm{ID}_i) = K_i$.

最后 $\mathcal{B}$ 发送 K_i 给 $\mathcal{A}$ 并以 $(C_i, w_{1,i}, w_{2,i}, \mathrm{ID}_i, K_i)$ 更新 $\mathcal{L}_2$.

询问阶段 1. 在这一阶段, $\mathcal{B}$ 允许询问私钥和密文解密.

(1) 解密私钥询问. 已知标识 ID_i, 如果 $\mathrm{ID}_i = \mathrm{ID}_{i^*}$, $\mathcal{B}$ 停止模拟并输出失败. 否则计算

$$d_{1,i} = (a - x^*) f_i(a) Q = \frac{(a - x^*) f(a)}{a - x^* + x_i} Q = \frac{\alpha}{H_1(\mathrm{ID}_i) + \alpha} P_2, \tag{2}$$

$$d_{2,i} = (z_1 + z_2(a - x^*)) f_i(a) Q = \frac{z_1 + z_2(a - x^*) f(a)}{a - x^* + x_i} Q = \frac{\beta}{H_1(\mathrm{ID}_i) + \alpha} P_2, \tag{3}$$

并发送 $\mathrm{sk}_{\mathrm{ID}_i} = (d_{1,i}, d_{2,i})$ 给攻击算法 $\mathcal{A}$. 不难看出, $\mathrm{sk}_{\mathrm{ID}_i}$ 是正确的私钥.

(2) 密文解密询问. 已知密文 (C_i, ID_i), 模拟算法 $\mathcal{B}$ 建立列表 $\mathcal{L}_D$ 用于记录密文解密询问的输入和输出, 列表元素以 (C, ID, K) 的形式存储. 若 (C_i, ID_i) 在列表 $\mathcal{L}_D$ 中, 则返回相应的 K_i, 否则根据以下步骤回复.

• $\mathrm{ID}_i \neq \mathrm{ID}_{i^*}$. $\mathcal{B}$ 首先计算标识 ID_i 的私钥 $\mathrm{sk}_{\mathrm{ID}_i}$, 然后以 $\mathrm{sk}_{\mathrm{ID}_i}$ 和 C_i 为输入运行解密算法获得 $w_{1,i}$ 和 $w_{2,i}$, 以 $(C_i, w_{1,i}, w_{2,i}, \mathrm{ID}_i)$ 为输入询问 H_2 谕言器得到 K_i 并发送 K_i 给 $\mathcal{A}$.

• $\mathrm{ID}_i = \mathrm{ID}_{i^*}$. $\mathcal{B}$ 从 $\{0,1\}^{\mathrm{klen}}$ 中随机选取元素 K_i 作为解密结果, 并发送给 $\mathcal{A}$.

最后 $\mathcal{B}$ 以 $(C_i, \mathrm{ID}_i, K_i)$ 更新 $\mathcal{L}_D$.

挑战阶段. $\mathcal{A}$ 输出挑战标识 ID^*, 如果 $\mathrm{ID}^* \neq \mathrm{ID}_{i^*}$, $\mathcal{B}$ 停止模拟并输出失败, 否则有 $H_1(\mathrm{ID}^*) = x^*$. $\mathcal{B}$ 随机选取 $r \in \mathbb{Z}_N^*$, $K^* \in \{0,1\}^{\mathrm{klen}}$, 计算挑战密文 $C^* = rP_1$, 要求 (C^*, ID^*) 没有询问过解密操作, 否则重新选取 r. 最后发送 (C^*, K^*) 给 $\mathcal{A}$. 设生成挑战密文的随机数为 $r^* = \frac{r}{a}$, 有

$$C^* = r^*(H_1(\mathrm{ID}^*)P_1 + P_{\mathrm{pub}}) = \frac{r}{a}(x^* P_1 + (a - x^*)P_1) = rP_1.$$

因此, C^* 是由随机数 r^* 生成的有效挑战密文.

询问阶段 2. $\mathcal{A}$ 允许继续询问私钥和密文解密, 但不能询问挑战标识 ID^* 的私钥和挑战密文 (C^*, ID^*) 的解密, $\mathcal{B}$ 根据询问阶段 1 回复 $\mathcal{A}$.

猜测阶段. 最后, $\mathcal{A}$ 输出它的猜测. 此时, $\mathcal{B}$ 忽略 $\mathcal{A}$ 的猜测结果, 并定义 H_2 中的挑战询问为 $(C^*, w_1^*, w_2^*, \mathrm{ID}^*)$, 其中 $w_1^* = e(P_1, P_2)^{r^*\alpha}$, $w_2^* = e(P_1, P_2)^{r^*\beta}$. 接着, $\mathcal{B}$ 从列表 $\mathcal{L}_2$ 中找到满足等式 (4) 的 w_1^*, w_2^*,

$$w_2^* = \left(\frac{e(rP_1, P_2)}{w_1^*}\right)^{\frac{z_1}{x^*}} \cdot (w_1^*)^{z_2}. \tag{4}$$

表 1　通信代价和困难假设比较

Table 1　Comparison of communication costs and assumptions

Scheme	Public key	Private key	Ciphertext	Assumption
SM9 key encapsulation [10]	$2\|\mathbb{G}_1\|+1\|\mathbb{G}_2\|+1\|\mathbb{G}_T\|$	$1\|\mathbb{G}_2\|$	$1\|\mathbb{G}_1\|$	Gap-q-BCAA1
Twin-SM9	$2\|\mathbb{G}_1\|+1\|\mathbb{G}_2\|+2\|\mathbb{G}_T\|$	$2\|\mathbb{G}_2\|$	$1\|\mathbb{G}_1\|$	q-BDHI

则有

$$w_1^* = e\left(P_1,P_2\right)^{r^*\alpha} = e\big(f(a)P, f(a)Q\big)^{\frac{r}{a}(a-x^*)} = e\big(f(a)P, f(a)Q\big)^{r}\cdot e(P,Q)^{\frac{-rx^*f^2(a)}{a}}.$$

又

$$z \nmid f^2(z),\quad \frac{-rx^*f^2(z)}{z} = F(z)+\frac{d}{z},$$

其中 $F(x)$ 是一个 $2q-3$ 次多项式, d 是一个可求的非零整数. 注意到 $\psi(Q)=P$, $f(a)P=\psi(f(a)Q)$, 则 $e(P,Q)^{F(a)}$ 是可求的.

最后, 模拟算法 $\mathcal{B}$ 计算

$$\left(\frac{w_1^*}{e\big(P_1,P_2\big)^{r}\cdot e(P,Q)^{F(a)}}\right)^{\frac{1}{d}} = \left(\frac{e(f(a)P,f(a)Q)^{r}\cdot e(P,Q)^{F(a)+\frac{d}{a}}}{e(P_1,P_2)^{r}\cdot e(P,Q)^{F(a)}}\right)^{\frac{1}{d}} = \big(e(P,Q)^{\frac{d}{a}}\big)^{\frac{1}{d}} = e(P,Q)^{\frac{1}{a}}$$

作为 q-BDHI 问题实例的解.

从以上设置可知, 证明中选取的元素都是随机的, 模拟环境和真实攻击具有不可区分性. 若挑战标识 ID^* 是第 i^* 个询问 H_1 的标识, 则 $\mathcal{A}$ 没有询问过 ID^* 的私钥, 模拟成功的概率为 $\frac{1}{q_{H_1}}$.

此外, 若攻击算法 $\mathcal{A}$ 没有对 $(C^*, w_1^*, w_2^*, \mathrm{ID}^*)$ 执行 H_2 询问, 则没有优势攻破 Twin-SM9 密钥封装算法. 根据假设, $\mathcal{A}$ 能以不可忽略的优势 ϵ 攻破算法, 则 $\mathcal{A}$ 将以 ϵ 概率询问 $(C^*, w_1^*, w_2^*, \mathrm{ID}^*)$ 对应 H_2 的值. 通过等式 (4), $\mathcal{B}$ 可成功找到 (w_1^*, w_2^*) 并求出给定 q-BDHI 问题的解. 综上所述, $\mathcal{B}$ 可以成功求解 q-BDHI 困难问题的概率为 $\frac{\epsilon}{q_{H_1}}$.

4.4　算法性能分析

本小节从通信代价和计算开销两个方面分析新密钥封装算法 Twin-SM9 的性能, 并与文献 [10] (SM9) 进行比较. 符号说明: $|\mathbb{G}_i|$ 表示群 $\mathbb{G}_i$ $(i=1,2,T)$ 中元素大小, p 表示双线性对运算, SM_i 表示群 $\mathbb{G}_i$ $(i=1,2)$ 中的标量乘 (scalar multiplication) 运算, E_t 表示群 $\mathbb{G}_T$ 中的指数 (exponentiation) 运算, $\mathcal{H}_N$ 表示映射到 $\mathbb{Z}_N^*$ 的密码杂凑函数, $\mathcal{H}_B$ 表示映射到 $\{0,1\}^{\mathrm{klen}}$ 的密码杂凑函数. 比较结果见表 1 和 2.

表 1 和 2 显示, 与 SM9 密钥封装算法相比较, 本文提出的 Twin-SM9 密钥封装算法的系统公钥和用户私钥分别增加一个群元素, 密文长度不变, 安全性没有降低. 虽然在私钥生成、密文生成和解密过程计算开销有小幅度增长, 但本算法的安全性基于更弱的 q-BDHI 假设, 消除了 Gap 类困难假设, 具有一定的理论意义.

5　结论

本文首次给出了 SM9 数字签名算法的形式化安全性证明. 结果表明, 若 q-SDH 假设成立, 则 SM9 数字签名算法具有 EUF-CMIA 的安全性. 接着, 采用 Twin-Hash-ElGamal 技术, 在不降低安全性的

表 2 计算开销和安全性比较

Table 2 Comparison of computational costs and security

Scheme	Key generation	Encryption	Decryption	Security
SM9 key encapsulation [10]	$1\mathrm{SM}_2+1\mathcal{H}_N$	$2\mathrm{SM}_1+1E_t+1\mathcal{H}_N+1\mathcal{H}_B$	$1p+1\mathcal{H}_B$	IND-CCA
Twin-SM9	$2\mathrm{SM}_2+1\mathcal{H}_N$	$2\mathrm{SM}_1+2E_t+1\mathcal{H}_N+1\mathcal{H}_B$	$2p+1\mathcal{H}_B$	IND-CCA

前提下改进 SM9 密钥封装算法, 提出新的标识密钥封装算法 Twin-SM9. 新算法消除了文献 [10] 中的 Gap 类复杂性假设, 算法安全性基于 q-BDHI 假设, 安全假设更弱. 在随机谕言模型下证明 Twin-SM9 标识密钥封装算法具有 IND-CCA 的安全性.

参考文献

1 Shamir A. Identity-based cryptosystems and signature schemes. In: Proceedings of Workshop on the Theory and Application of Cryptographic Techniques, Santa Barbara, 1984. 47–53

2 Boneh D, Franklin M K. Identity-based encryption from the weil pairing. In: Proceedings of the 21st Annual International Cryptology Conference, Santa Barbara, 2001. 213–229

3 Boneh D, Boyen X. Efficient selective-id secure identity-based encryption without random oracles. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, 2004. 223–238

4 Gentry C. Practical identity-based encryption without random oracles. In: Proceedings of the 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, 2006. 445–464

5 Xue J T, Xu C X, Zhao J N, et al. Identity-based public auditing for cloud storage systems against malicious auditors via blockchain. Sci China Inf Sci, 2019, 62: 032104

6 Langrehr R, Pan J. Hierarchical identity-based encryption with tight multi-challenge security. In: Proceedings of the 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, 2020. 153–183

7 Qin B D, Liu X M, Wei Z, et al. Space efficient revocable IBE for mobile devices in cloud computing. Sci China Inf Sci, 2020, 63: 139110

8 Mu Y H, Xu H X, Li P L, et al. Secure two-party SM9 signing. Sci China Inf Sci, 2020, 63: 189101

9 Cryptography Standardization Technical Committee. SM9 identity-based cryptographic algorithm. GM/T0044-2016. http://www.gmbz.org.cn/main/postDetail.html?id=20180322410400 [密码行业标准化技术委员会. SM9 标识密码算法. GM/T0044-2016. http://www.gmbz.org.cn/main/postDetail.html?id=20180322410400]

10 Cheng Z H. Security analysis of SM9 key agreement and encryption. In: Proceedings of the 14th International Conference Information Security and Cryptology, Fuzhou, 2018. 3–25

11 Zhang X F, Peng H. Blind signature scheme based on SM9 algorithm. Netinfo Secur, 2019, 19: 61–67 [张雪锋, 彭华. 一种基于 SM9 算法的盲签名方案研究. 信息网络安全, 2019, 19: 61–67]

12 Wang S, Fang L G, Han L B, et al. Fast implementation of SM9 digital signature and verification algorithms. Commun Technol, 2019, 52: 2524–2527 [王松, 房利国, 韩炼冰, 等. 一种 SM9 数字签名及验证算法的快速实现方法. 通信技术, 2019, 52: 2524–2527]

13 Xu S W, Ren X P, Yuan F, et al. A secure key issuing scheme of SM9. Comput Appl Softw, 2020, 37: 314–319 [许盛伟, 任雄鹏, 袁峰, 等. 一种关于 SM9 的安全私钥分发方案. 计算机应用与软件, 2020, 37: 314–319]

14 Wang C J, Lin W L, Lin H T. Design of an instant messaging system using identity based cryptosystems. In: Proceedings of the 4th International Conference on Emerging Intelligent Data and Web Technologies, Xi'an, 2013. 277–281

15 Geisler M, Smart N P. Distributing the key distribution centre in Sakai-Kasahara based systems. In: Proceedings of the 12th IMA International Conference on Cryptography and Coding, Cirencester, 2009. 252–262

16 Yang Y T, Cai J L, Zhang X W, et al. Privacy preserving scheme in blockchain with provably secure based on SM9 algorithm. J Softw, 2019, 30: 1692–1704 [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. 软件学报, 2019, 30: 1692–1704]

17 Sun S Z, Ma H, Zhang R, et al. Server-aided immediate and robust user revocation mechanism for SM9. Cybersecur,

2020, 3: 12
18 Gan Z W, Liao F Y. Rapid calculation of R-ate bilinear pairing in China state cryptography standard SM9. Comput Eng, 2019, 45: 171–174 [甘植旺, 廖方圆. 国密 SM9 中 R-ate 双线性对快速计算. 计算机工程, 2019, 45: 171–174]
19 Wang M D, He W G, Li J, et al. Optimal design of R-ate pair in SM9 algorithm. Commun Technol, 2020, 53: 2241–2244 [王明东, 何卫国, 李军, 等. 国密 SM9 算法 R-ate 对计算的优化设计. 通信技术, 2020, 53: 2241–2244]
20 Barreto P S L M, Libert B, McCullagh N, et al. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In: Proceedings of the 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, 2005. 515–532
21 Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures. J Cryptology, 2000, 13: 361–396
22 Chen L Q, Cheng Z H. Security proof of Sakai-Kasahara's identity-based encryption scheme. In: Proceedings of the 10th IMA International Conference on Cryptography and Coding, Cirencester, 2005. 442–459
23 Cash D, Kiltz E, Shoup V. The twin Diffie-Hellman problem and applications. In: Proceedings of the 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, 2008. 127–145

Security analysis of SM9 digital signature and key encapsulation

Jianchang LAI[1], Xinyi HUANG[1*], Debiao HE[2] & Wei WU[3]

1. *Fujian Provincial Key Lab of Network Security and Cryptology, College of Computer and Cyber Security, Fujian Normal University, Fuzhou* 350117*, China*;
2. *Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan* 430072*, China*;
3. *Center for Applied Mathematics of Fujian Province, School of Mathematics and Statistics, Fujian Normal University, Fuzhou* 350117*, China*
* Corresponding author. E-mail: xyhuang@fjnu.edu.cn

Abstract Security analysis provides strong guarantees and evidence for security cryptosystems. SM9 is an identity-based cryptosystem designed by China and has become a Chinese standard. The SM9 digital signature and encryption algorithm also became ISO/IEC International standards. However, there are few published research results on the security of SM9 cryptosystems. Based on Gap-q-BCAA1 assumption, Cheng gave the security analysis of SM9 key exchange protocol, key encapsulation and encryption algorithm in Inscrypt 2018. In this paper, we first give the formal security analysis for SM9 digital signature. Based on the q-SDH assumption, we prove that SM9 signature algorithm is EUF-CMIA secure. To eliminate the Gap assumption, we then use the technique of Twin-Hash-ElGamal to modify SM9 key encapsulation slightly without compromising its security and propose a new identity-based key encapsulation mechanism called Twin-SM9. Compared to SM9 key encapsulation, both the system public key and user private key contain one additional group element only and the ciphertext size remains the same. We prove that Twin-SM9 achieves IND-CCA security in the random oracle model based on the q-BDHI assumption. Our results clarify the security of SM9 and are useful for the design of SM9-based cryptosystems.

Keywords SM9, security analysis, digital signature, key encapsulation, CCA

Jianchang LAI was born in 1988 and received his Ph.D. degree from University of Wollongong, Australia in 2018. Currently, he is an associate professor at the College of Computer and Cyber Security, Fujian Normal University, China. His research interests include public-key cryptography and cloud computing.

Debiao HE was born in 1980 and received his Ph.D. degree from Wuhan University in 2009. Currently, he is a professor at the School of Cyber Science and Engineering, Wuhan University, China. His research interests include cryptography and information security, in particular, cryptographic protocols.

Xinyi HUANG was born in 1981 and received his Ph.D. degree from University of Wollongong, Australia in 2009. Currently, he is a professor at the Fujian Provincial Key Laboratory of Network Security and Cryptology, College of Computer and Cyber Security, Fujian Normal University, China. His research interests include cryptography and information security.

Wei WU was born in 1981 and received her Ph.D. degree from University of Wollongong, Australia in 2009. Currently, she is a professor at the School of Mathematics and Statistics, Fujian Normal University, China. Her research interests include cryptography and information security.