计 算 机 研 究 与 发 展
Journal of Computer Research and Development
https://crad.ict.ac.cn
63(11): 2843−2855, 2026

RCCA 安全的支持等式测试的 SM9 标识加密方案

陈思宇[1] 欧阳梦迪[2] 李发根[2]

[1](电子科技大学信息与软件工程学院 成都 610054)

[2](电子科技大学计算机科学与工程学院(网络空间安全学院) 成都 611731)

(18738690019@163.com)

RCCA Secure Identity-Based SM9 Encryption Scheme with Equality Test

Chen Siyu[1], Ouyang Mengdi[2], and Li Fagen[2]

[1](*School of Information and Software Engineering*, *University of Electronic Science and Technology of China*, *Chengdu* 610054)

[2](*School of Computer Science and Engineering* (*School of Cyber Security*), *University of Electronic Science and Technology of China*, *Chengdu* 611731)

Abstract In cloud computing environments, equality test can effectively address the challenge of comparing whether two ciphertexts are encrypted under the same plaintext without decryption. Among existing schemes, identity-based encryption with equality test (IBEET) significantly simplifies certificate management compared with traditional public-key encryption schemes, demonstrating considerable value. While China's independently developed SM9 encryption algorithm has been successfully selected as an ISO/IEC international standard, existing SM9-based equality test schemes generally remain vulnerable to subversion attacks. Specifically, by subverting the randomness generation process, an adversary in possession of a backdoor key can recover the plaintext, thereby compromising the security of the scheme. To address this issue, an RCCA (relaxed chosen-ciphertext attack) secure identity-based SM9 encryption scheme with equality test (RCCA-SM9-IBEET) is proposed. The scheme employs cryptographic reverse firewalls (CRF) to re-randomize the inputs and outputs of potentially compromised users, thereby resisting subversion attacks. Furthermore, we define the concept of OW-ID-RCCA (one-way chosen-ciphertext security against a relaxed chosen identity attack) security model, which supports ciphertext re-randomization for compatibility with the reverse firewalls. A rigorous security proof is provided in the random oracle model. Finally, we analyze the computational and communication costs of the proposed scheme from both theoretical and experimental perspectives.

Key words SM9; subversion attack; RCCA; equality test; cryptographic reverse firewall

摘 要 在云计算环境中,等式测试有效解决了加密数据无法进行底层明文比较的问题,其中支持等式测试的标识加密(identity-based encryption with equality test, IBEET)算法有效简化了传统公钥加密的证书管理,具有重要价值。我国自主研发的 SM9 加密算法已入选 ISO/IEC 国际标准,但现有基于 SM9 的等式测试方案普遍难以抵抗颠覆攻击,即通过篡改随机数生成方式掌握后门密钥的敌手可恢复明文,从而破坏算法的安全性。针对该问题,提出了一种 RCCA(relaxed chosen-ciphertext attack)安全的支持等式测试的 SM9 标识加密方案(RCCA secure identity-based SM9 encryption scheme with equality test, RCCA-SM9-IBEET),通过部署密码逆向防火墙(cryptographic reverse firewalls, CRF)重随机化用户输入/输出信息来抵抗颠覆

收稿日期: 2025-12-24; **修回日期**: 2026-07-17

基金项目: 国家自然科学基金项目(62272090); 四川省科技计划项目(2025YFHZ0320)

This work was supported by the National Natural Science Foundation of China (62272090) and Sichuan Science and Technology Program (2025YFHZ0320).

通信作者: 李发根(fagenli@uestc.edu.cn)

攻击;然后定义了 OW-ID-RCCA(one-way chosen-ciphertext security against a relaxed chosen identity attack)安全模型,支持密文可重随机化以兼容逆向防火墙;同时在随机谕言机模型下给出了安全证明。最后,从理论与实验 2 个维度对方案的计算成本和通信成本进行了分析。

关键词 SM9;颠覆攻击;宽松的 CCA;等式测试;密码逆向防火墙

中图法分类号 TP391

DOI: 10.7544/issn1000-1239.202550933 **CSTR:** 32373.14.issn1000-1239.202550933

随着云计算技术的快速发展,越来越多公司/个人选择将数据上传到服务器[1]。然而,云服务器的第三方管理特性使用户难以完全信任其数据在云端的可用性、保密性和完整性(例如云服务人员可能存在恶意行为或出于好奇)[2-3]。为此,用户通常将数据加密后上传云端,但这使得对数据的搜索变得极为复杂且需要极大开销,因为用户在搜索前需要将密文解密。其中一种解决办法是可搜索加密,它允许服务器代表数据持有者搜索加密数据而不泄露数据。目前,相关方案已在安全模型扩展和区块链等热门领域结合方面取得重要进展[2,4-9]。然而,可搜索加密通常应用于基于关键词的复杂查询,但在跨用户数据比对场景中存在局限性。相比之下,等式测试更适用于高效的密文等价性判定,它允许指定测试方(如云服务器)在不进行解密操作、不泄露任何明文的前提下,直接对由不同公钥加密的密文进行比对,以判断其对应的明文是否相同。基于这一核心思想,Yang 等人[10]提出了支持等式测试的公钥加密(public-key encryption with equality test, PKEET)方案,Ma[11]进一步提出了支持等式测试的标识加密(identity-based encryption with equality test, IBEET)方案。

现有的 IBEET 方案虽然在可证明安全下是安全的,但“棱镜门”等相关事件表明,实际生活中所使用的密码系统可能偏离其应遵守的部署规范,无法达到理论上的安全性。Young 等人[12]提出的盗码学(kleptography)以及 Bellare 等人[13]提出的算法替换攻击(algorithm substitution attack, ASA),都表明敌手可以利用篡改随机数生成方式等手段实现密钥渗漏或数据窃取。为应对这些威胁,学术界提出多种防御机制,本文主要运用密码逆向防火墙(cryptographic reverse firewalls, CRF)来抵抗颠覆攻击。CRF 由 Mironov 等人[14]于 2015 年提出,是一个部署在用户私人网络边界的实体,通过重随机化用户的输入/输出消除可能携带的隐蔽信息,使敌手无法区分被颠覆的密文和纯净密文,来达到抗颠覆攻击的效果。

逆向防火墙通过对算法输出进行重随机化操作来清除可能隐含的敏感信息,从而抵抗颠覆攻击。然而,传统 CCA 安全的公钥加密方案难以兼容此类操作,因为重随机化往往会导致密文无法被接收者成功解密。为了解决这一矛盾并抵抗 ASA,学界开始探索放宽 CCA 安全性的可能。Canetti 等人[15]于 2003 年提出可重放 CCA(replayable CCA)安全。Phan 等人[16]在其安全模型上进一步限制,提出宽松的 CCA(relaxed CCA, RCCA)安全并构造了具有 RCCA 安全性的高效非对称加密方案。这些工作为重随机化与安全性的兼容提供了解决方案。

SM9 是我国自主研发的商用密码算法,已获得国际认可并入选 ISO/IEC 国际标准,然而其设计并未考虑颠覆攻击。欧阳梦迪等人[17]提出了针对 SM9 加密算法的颠覆攻击,敌手仅需 2 个连续的密文即可恢复明文。Chen 等人[18]构造了第 1 个可重随机化的 SM9 标识加密方案,实现了 RCCA 安全。2024 年,熊虎等人[19]提出了 SM9-IBEET-CRF。该方案虽然部署了逆向防火墙,但只重随机化了部分密文。通过颠覆随机数生成方式,掌握后门密钥的敌手仅需获取 2 个连续的密文即可恢复明文,因此该方案仍无法有效防御 ASA。为此,本文提出了一种 RCCA 安全的支持等式测试的 SM9 标识加密方案 RCCA-SM9-IBEET。主要贡献包括 3 个方面:

1)提出了 OW-ID-RCCA 安全性并设计了相应的安全模型。在支持等式测试功能的同时,该模型允许密文重随机化以兼容密码逆向防火墙;

2)设计了一种 RCCA 安全的支持等式测试的 SM9 标识加密算法,成功部署 CRF,解决了基于 SM9 的等式测试方案难以抵抗颠覆攻击的问题;

3)在 OW-ID-RCCA 安全模型下证明了该方案的安全性,并从理论与实验 2 个维度,对方案的计算成本和通信成本进行了分析。经过大量的仿真实验证明,RCCA-SM9-IBEET 的等式测试模块在计算开销上具有显著优势,单次测试仅需 0.066 ms,适用于云计算场景。

1 相关工作

为实现在不解密的情况下对不同公钥加密的密文进行明文对比，Yang 等人[10]提出了密文等式测试，并给出了可证明 OW-CCA（one-wayness against chosen ciphertext attacks）安全的具体构造。为实现 PKEET 的授权机制，2011 年 Tang[20]利用授权令牌机制实现细粒度授权——仅限经过认证的 2 个用户进行测试。Huang 等人[21]提出授权式公钥加密等式测试（public key encryption with authorized equality test, PKE-AET），接收方可对所有密文或特定密文的密钥授权进行双重认证。Ma 等人[22]研究了 PKEET 的授权机制，提出了一种支持 4 种授权类型的灵活 PKEET 方案。在 2016 年，Ma[11]将等式测试与标识加密结合，提出了第 1 个具有 OW-ID-CCA（one-way chosen-ciphertext security against a chosen identity attack）安全的 IBEET 方案，简化了 PKEET 的证书管理。Susilo 等人[23]于 2022 年提出了支持多密文等式测试的公钥加密概念，利用秘密分享技术替代双线性对。为实现后量子安全，Yang 等人[24]提出了基于 LWE（learning with errors）假设的后量子 IBEET 方案。2025 年，韩金广等人[25]提出了一种前向安全的 SM9 密文等值测试，拓展了 IBEET 的安全模型。

作为 CCA 安全的松弛版本，可重放 CCA 安全性由 Canetti 等人[15]提出，其允许解密谕言机将等价密文标记为“重放”。这种松弛在保持安全性的同时，为密文可重随机化提供了设计空间。后续研究在此基础上进一步实现了诸如公开可验证性等功能增强与性能优化[26-29]。Phan 等人[16]在可重放 CCA 的基础上进一步进行限制，定义了 RCCA，并构造了具有 IND-RCCA 安全性的高效非对称加密方案（如 ElGamal 和 Paillier），但他们并未专门针对密文可重随机化这一核心问题展开研究。2021 年 Wang 等人[30]提出了基于哈希证明系统的具有匿名性的可重随机 RCCA 加密方案框架，解决了在可重放 CCA 安全性下同时实现可重随机性和匿名性的难题。在国密算法方面，陈荣茂等人[31]设计了一种可重随机化的可重放 CCA 安全的 SM2 加密方案。2024 年 Chen 等人[18]提出了满足 Phan 等人定义的安全概念[16]的可重随机化 IBE 方案——RCCA-SM9，为兼容 CRF 的高效安全 IBE 方案发展做出了贡献。

逆向防火墙由 Mironov 等人[14]提出，其具备 3 个基本特性：功能保持性、安全保持性与抗泄露性。具体而言，逆向防火墙能够有效抵抗算法替代攻击以保护用户隐私，同时不影响底层密码学原语功能与安全性。基于这一原语，逆向防火墙已成功应用于安全多方计算[32]、代理重加密[33]、属性基加密[34]与聚合签名[35]等多个领域。近年来，逆向防火墙逐渐应用于对密文进行功能性操作（如等式测试）的场景。Zhou 等人[36]和 Ming 等人[37]的研究集中于可搜索加密领域，为云存储中的数据检索构建了具备逆向防火墙的安全方案。Elhabob 等人[38]面向远程医疗系统，设计了支持等值测试和逆向防火墙的标识加密方案，在保障患者隐私的前提下实现安全的医疗数据分析。这些成果共同推动了逆向防火墙在复杂应用场景下的应用。

2 预备知识

2.1 符号表示

令$\lambda\in\mathbb{N}$表示安全参数，$poly(\lambda)$表示关于λ的多项式函数，$negl(\lambda)$表示任意关于λ的可忽略函数。令元组$(p,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,\hat{e},P_1,P_2)$为非对称双线性对群，其中$\mathbb{G}_1$，$\mathbb{G}_2$，$\mathbb{G}_T$是阶为素数$p$的循环群，$P_1$是群$\mathbb{G}_1$的生成元，$P_2$是群$\mathbb{G}_2$的生成元。$\hat{e}:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$是一个可高效计算且非退化的双线性映射。对于任意非空集合$\mathcal{X}$，$x\leftarrow\$\mathcal{X}$表示从$\mathcal{X}$中随机选取元素$x$。对于任意随机性算法$\mathcal{F}(\cdot)$，$y\leftarrow\$\mathcal{F}(x)$表示算法$\mathcal{F}$输出随机结果$y$。对于任意确定性算法$\mathcal{F}'(\cdot)$，$y\leftarrow\mathcal{F}'(x)$表示算法$\mathcal{F}'$输出确定结果$y$。

2.2 密码逆向防火墙

密码逆向防火墙$\mathcal{W}$是对协议参与方发出或接收的消息进行实时修改的实体[14]。$\mathcal{W}$是一种具有状态的算法，它接收输入消息和当前状态，修改后输出消息并更新自身状态。参与方P的密码协议$\mathcal{P}$具有 3 个算法，$receive_{\mathcal{W}\circ P}(\tau,m)$在接收到消息$m$时更新状态$\tau$，$next_{\mathcal{W}\circ P}(\tau)$输出待传输的消息，$output_{\mathcal{W}\circ P}(\tau)$输出$P$的结果。它们的组成$\mathcal{W}\circ P$被定义为

$$\begin{aligned}\mathcal{W}\circ P:=&(receive_{\mathcal{W}\circ P}(\tau,m)=receive_P(\tau,\mathcal{W}(m)),\\&next_{\mathcal{W}\circ P}(\tau)=\mathcal{W}(next_P(\tau)),\\&output_{\mathcal{W}\circ P}(\tau)=output_P(\tau))。\end{aligned}$$

定义 1. 设协议$\mathcal{P}$满足功能性要求$\mathbb{F}$和安全性要求$\mathbb{S}$，且$\mathcal{W}\circ P$遵循协议$\mathcal{P}$。若逆向防火墙$\mathcal{W}$具有以下 3 个属性，则称其为安全的。

1）功能保持性。对于任意逆向防火墙$\mathcal{W}$和任意

参与方P, 令$\mathcal{W}^{1\circ}P=\mathcal{W}\circ P$, 且对于任意多项式有界的整数$k\geqslant 2$, 令$\mathcal{W}^{k\circ}P=\mathcal{W}\circ(\mathcal{W}^{k-1\circ}P)$。当且仅当对于所有多项式有界的$k\geqslant 1$, $\mathcal{W}^{k\circ}P$都能在协议$\mathcal{P}$中保持P的功能性$\mathbb{F}$时, 称$\mathcal{W}$具有功能保持性。

2)弱安全保持性。对于任意功能保持的敌手, 若将协议$\mathcal{P}$中的参与方P替换为$\mathcal{W}\circ\bar{P}$(记为$\mathcal{P}_{P\to\mathcal{W}\circ\bar{P}}$)后, 该协议仍满足安全性要求$\mathbb{S}$, 则称$\mathcal{W}$在$\mathcal{P}$中为$P$弱保持$\mathbb{S}$, 其中$\bar{P}$表示任意的 PPT 函数保持颠覆。

3)弱抗泄露性。游戏 *LEAK* 如图 1 所示, 其中$LEAK(\mathcal{P},P_A,P_B,\mathcal{W},\lambda)$是协议$\mathcal{P}$中逆向防火墙$\mathcal{W}$针对具有安全参数$\lambda$的参与方$P_A$与参与方$P_B$的抗泄露安全博弈。$\mathcal{A}$是攻击者, τ_{P_B}是协议$\mathcal{P}$运行后$\bar{P}_B$的状态, I是$\mathcal{P}$的有效输入, $\mathcal{T}*$是$\mathcal{P}_{\bar{P}_A\to P^*}$, $P_B\to\bar{P}_B$的运行记录。若不存在 PPT 功能保持的敌手$\mathcal{A}$能够以不可忽略的优势赢得游戏 *LEAK*, 则称$\mathcal{W}$是弱抗泄露的。当$\bar{P}_A,\bar{P}_B,\mathcal{P}$明确时, 简记为$\mathcal{W}$对$\bar{P}_B$是弱抗泄露的。在$P_B$未被破坏的特殊情况下, 我们称$\mathcal{W}$对窃听者具有弱抗渗漏性。

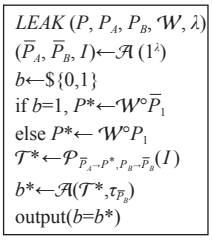


Fig. 1 Game of *LEAK*

图 1 游戏 *LEAK*

敌手$\mathcal{A}$在游戏 *LEAK* 中的优势定义为

$$Adv_{\mathcal{A},\mathcal{W}}^{LEAK}(\lambda)=Pr[LEAK(\mathcal{P},P_A,P_B,\mathcal{W},\lambda)=1]-1/2\text{。}$$

值得注意的是: 本文主要考虑现实中最常见且不破坏算法正常运行的功能保持型敌手。由于方案采用 OW-ID-RCCA 安全模型, 因此我们探讨弱安全保持性与弱抗泄露性这 2 个概念。

2.3 困难问题

定义 2. q-DBDHI*假设[18]。设$\hat{e}$: $\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$是 1 个双线性映射, 其中$\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$是阶为素数p的循环群, P_1,P_2,P_T分别是群$\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$的生成元。对于任意$\alpha,\beta\in\mathbb{Z}_p$, 给定元组$(P_1,[\alpha]P_1,(h_0,[\beta(h_0+\alpha)]P_1),P_2,(h_1,[\alpha/(\alpha+h_1)]P_2),\cdots,(h_q,[\alpha/(\alpha+h_q)]P_2))$,其中$h_i\in\mathbb{Z}_p$,$\alpha+h_i\neq 0$, 并且$h_i$互不相同($i=0,1,\cdots,q$)。对于任何高效的概率多项式时间敌手$\mathcal{A}$, 在$\mathcal{A}$能够查询$O_{q\text{-DBDHI}^*}$的情况下, 其输出$\hat{e}(P_1,P_2)^{\alpha\beta}$的成功概率是可忽略的。其中$O_{q\text{-DBDHI}^*}$是 1 个 q-DBDHI*谕言机, 输入$(P_1,[\alpha]P_1,(h_0,[\beta(h_0+\alpha)]P_1),P_2,(h_1,[\alpha/(\alpha+h_1)]P_2),\cdots,(h_q,[\alpha/(\alpha+h_q)]P_2),R)$可以判断$R$是否等于$\hat{e}(P_1,P_2)^{\alpha\beta}$。

引理 1[18]**.** 设$\mathcal{A}$为 1 个针对使用任何陷门单向概率函数族$(\varphi_{pk})_{pk}$的 OAEP-3 轮构造的 IND-ID-RCCA 敌手, 在时间τ内运行。假设在向随机谕言机F,G,H和解密谕言机O_{Dec}分别进行$q_{\mathrm{f}},q_{\mathrm{g}},q_{\mathrm{h}},q_{\mathrm{d}}$次查询后, 其优势$Adv_{\mathcal{A},\text{OAEP-3}}^{\text{IND-ID-RCCA}}(\tau)>\epsilon$。则$Succ_{\varphi}^{\mathrm{gap}}(\tau',q_{\mathrm{d}}(q_{\mathrm{g}}q_{\mathrm{h}}+q_{\mathrm{d}}))$的上界为

$$\frac{\epsilon}{2}-q_{\mathrm{d}}^2\cdot\left(\frac{1}{2^l}+\frac{6}{2^k}\right)-(4q_{\mathrm{d}}+1)\cdot\left(\frac{q_{\mathrm{g}}}{2^l}+\frac{q_{\mathrm{f}}}{2^k}\right)-q_{\mathrm{d}}\cdot\frac{q_{\mathrm{f}}+1}{2^k}\text{,}$$

其中$\tau'\leqslant\tau+(q_{\mathrm{f}}+q_{\mathrm{g}}+q_{\mathrm{h}}+q_{\mathrm{d}})T_{lu}+q_{\mathrm{d}}^2T_{Same}+(q_{\mathrm{d}}+1)q_{\mathrm{g}}q_{\mathrm{h}}\times(T_{\varphi}+T_{Same})$, T_{φ}是评估任何函数φ_{pk}的时间复杂度, T_{Same}是决策谕言机$Same_{\varphi_{pk}}$给出答案的时间, T_{lu}是在列表中查找的时间复杂度。

3 方案定义

3.1 系统模型

图 2 揭示了 RCCA-SM9-IBEET 的系统模型。

该模型总共包括 5 个实体: 云服务器、CRF、密钥生成中心(KGC)以及 2 个数据拥有者 Alice 和 Bob。KGC 作为可信第三方负责初始化系统公共参数, 供云服务器和数据所有者使用。Alice 和 Bob 分别使用各自的公钥加密其本地数据, 将生成的密文(记为C_A和C_B)上传至云服务器存储, 并委托云服务器执行等式测试。在密文上传至云服务器前, CRF 会对密文进行重随机化处理, 以消除潜在的后门信息。云服务器接收到重构密文后, 在安全存储的同时可在无需解密的条件下对密文执行等式测试。当 Alice 需要向 Bob 传递消息时, 她可使用 Bob 的身份加密消息并发送密文; 若要获取明文, 则需 Bob 使用其私钥通过$Dec(mpk,sk_{id},C')$自行解密。

其中, CRF 是 1 个部署在用户私人网络边界和外部网络之间的实体, 对输入输出数据进行重随机化处理。CRF 为半可信任实体, 该实体会严格执行所有规定的操作, 但可能利用其在执行过程中获得的信息来窥探敏感信息。在密钥管理方面, CRF 无需用户私钥, 因此不需要与用户或 KGC 进行额外的密钥同步。

3.2 形式化定义

RCCA-SM9-IBEET 方案由以下 6 个算法组成。

1)$Setup(1^{\lambda})$。该算法输入安全参数λ, KGC 运行该算法并输出主公钥mpk和系统主私钥msk。

2)$Ext(mpk,msk,id)$。该算法输入主公钥mpk、主私钥msk和任意身份标识id, 输出对应私钥sk_{id}。

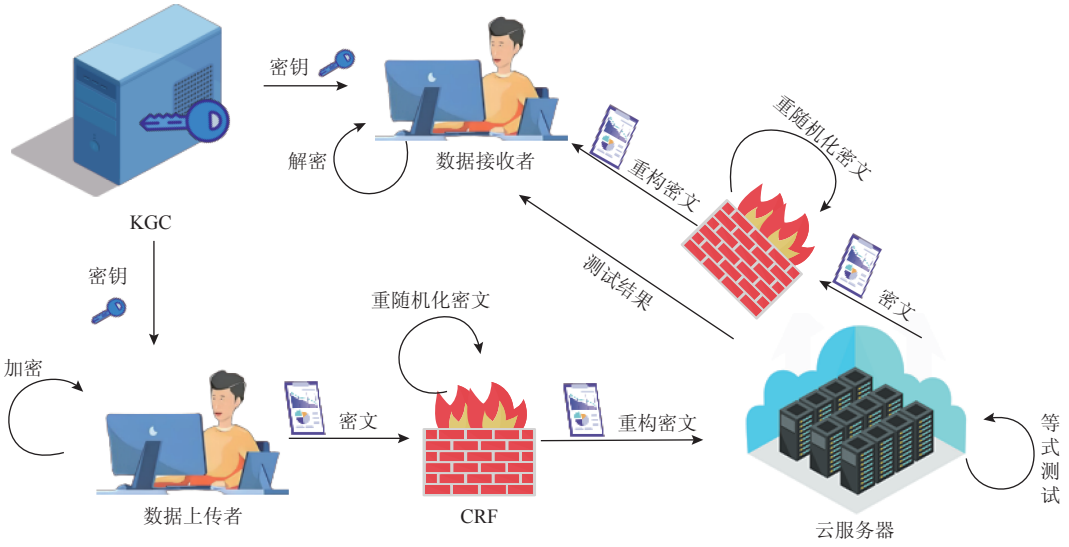


Fig. 2 System model diagram

图 2 系统模型图

3) $Enc(mpk,id,m)$。该算法输入主公钥 mpk、身份标识 id 和明文 m，输出密文 C。

4) $Rerand(mpk,C,id)$。该算法输入密文 C、主公钥 mpk 和身份标识 id，输出重随机化后的密文 C'。

5) $Dec(mpk,sk_{id},C')$。该算法输入主公钥 mpk、私钥 sk_{id} 和密文 C'，输出明文 m 或错误符号 $\perp$。

6) $Test(C_A,C_B)$。该算法以 id_A 的密文 C_A 和 id_B 的密文 C_B 作为输入，云服务器执行等式测试，如果 C_A 和 C_B 对应的明文相同，则返回 1；否则返回 0。

3.3 OW-ID-RCCA 安全模型

Chen 等人[18]将 Phan 等人[16]提出的 IND-RCCA 定义扩展至基于身份的场景，提出适应性身份松弛选择密文攻击下的不可区分性(IND-ID-RCCA)。文献[10]明确指出在支持公开等式测试的环境中，传统的不可区分性安全模型(如 IND-CCA 安全模型)不再适用，等式测试与不可区分性安全本质上是冲突的。与 Yang 等人[10]设计的 PKEET 方案类似，本文的 RCCA-SM9-IBEET 方案未引入陷门机制，无法进行授权操作，因而敌手能够自主进行等式测试，本文方案无法满足 IND-ID-RCCA 安全。受此启发，本文引入了新的安全目标，将 RCCA 定义扩展到 IBEET，提出了基于身份的单向松弛选择密文攻击(OW-ID-RCCA)安全性，以此作为合理的安全目标并进行安全性证明，后续再进行优化(如设置陷门等)以满足更高的安全性。

由图 3 所示的安全游戏定义，其中敌手 $\mathcal{A}$ 获胜的优势被定义为

$$Adv_{\mathcal{A},\Pi}^{\text{OW-ID-RCCA}}(\lambda)=|Pr[m=m']|\leqslant negl(\lambda)。$$

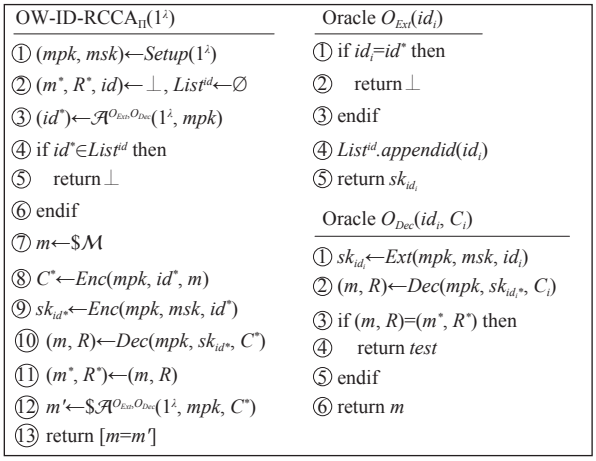


Fig. 3 Attack game for OW-ID-RCCA security

图 3 OW-ID-RCCA 安全攻击游戏

本文基于 Chen 等人[18]构造的 RCCA-SM9 方案作出改进以融合等式测试，遵循 Phan 等人[16]提出的 RCCA 三轮通用架构。

定义 3. 若不存在多项式时间敌手 $\mathcal{A}$ 能以不可忽略的优势 $Adv_{\mathcal{A},\Pi}^{\text{OW-ID-RCCA}}(\lambda)$ 赢得上述游戏，则称 IBEET 方案 $\prod$ 是 OW-ID-RCCA 安全的。

OW-ID-RCCA 安全性允许敌手公开执行等式测试并观察重随机化后的密文，但仍能保证敌手无法从挑战密文中恢复完整明文；然而该模型不提供语义不可区分性，因此对于低熵明文空间，敌手仍可通过枚举所有可能取值并与目标密文执行等式测试来推导明文。这一安全边界表明，本方案适用于明文具有高熵或随机性的场景，对于低熵数据则需额外引入盲化或填充机制以加固实际部署中的安全性。

4 RCCA-SM9-IBEET

4.1 具体方案

本文工作基于 Chen 等人[18]的研究，通过将等式测试模块融入基于 SM9 的 RCCA 安全的可重随机化公钥加密算法，提出了 RCCA 安全的支持等式测试的 SM9 标识加密方案。为克服双线性对操作的计算瓶颈以提高测试效率，在$Test$函数中本文采用 Shamir 秘密分享方案代替双线性对实现密文等价性判定。同时，由于A与$f(A)$是明文的确定性函数，攻击者无法通过操纵其随机性建立隐蔽信道，因此无需对其重随机化。具体方案如图 4 所示，其中$(p,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,\hat{e},P_1,P_2)$是一个非对称双线性映射。设$F,G,H$: $\mathbb{G}_T\to\mathbb{G}_T$; H_1,H_2: $\mathcal{ID}\to\mathbb{Z}_p$; H_3: $\mathbb{G}_T\to\mathbb{Z}_p$; H_4: $\{0,1\}^*\to\mathbb{Z}_p$。

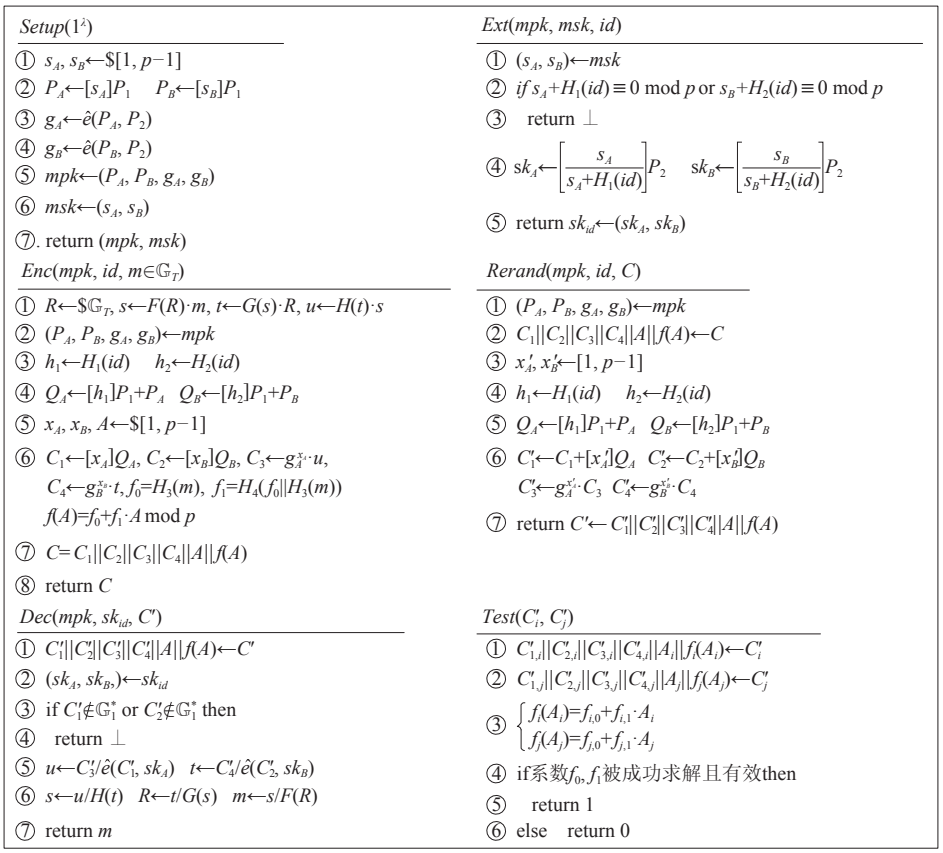


Fig. 4 The scheme of RCCA-SM9-IBEET

图 4 RCCA-SM9-IBEET 方案

如图 4 所示，各阶段算法如下：

$Setup$算法输入λ，输出$mpk = P_A, P_B, g_A, g_B$，$msk = (s_A, s_B)$；

Ext算法输入mpk, msk, id，输出$sk_{id} = ([s_A/(s_A + H_1(id))]P_2, [s_B/(s_B + H_2(id))]P_2)$；

Enc算法输入$mpk, id, m \in \mathbb{G}_T$，输出$C = x_A(H_1(id)+[s_A])\ P_1 \| x_B(H_2(id)+[s_B])\ P_1 \| g_A^{x_A}\cdot u \| g_B^{x_B}\cdot t \| A \| H_3(m)+H_4(f_0 \| H_3(m))\cdot A$；

Dec算法输入mpk, sk_{id}, C'，输出 m；

$Rerand$算法输入mpk, id, C，输出$C' = [x_A + x'_A](H_1(id)+[s_A])\ P_1 \| [x_B + x'_B](H_2(id)+[s_B])\ P_1 \| g_A^{x_A+x'_A}\cdot u \| g_B^{x_B+x'_B}\cdot t \ \| A \| H_3(m)+H_4(f_0 \| H_3(m))\cdot A$；

$Test$算法输入C'_i, C'_j，输出 0 或 1。

4.2 正确性分析

1）重随机化正确性。根据算法Dec和$Rerand$的描述，对于任意密文C，$x' \leftarrow \$[1, p-1]$，假设其底层随机数为$(r, x)$，对其进行重随机化操作重加密后得到的新密文$C'$的底层随机数为$(r, x+x')$，所以$Rerand$算法的输出$C'$除了底层随机变量由$x$被替换为$x+x'$外，与输入$C$完全相同。

2）解密正确性。对任意$(mpk, msk) \leftarrow Setup(1^\lambda), id \in \mathcal{ID}, m \in \mathcal{M}, sk_{id} \leftarrow Ext(mpk, msk, id), C \leftarrow Enc(mpk, id, m)$和$C' \leftarrow \$Rerand(mpk, id, C)$，在$Dec(mpk, sk_{id}, C')$中，我们可以验证步骤⑤的正确性如下：

$$C_3'/\hat{e}(C_1', sk_A) = \frac{g_A^{x_A+x_A'}\cdot u}{\hat{e}\left([x_A+x_A']Q_A, \left[\frac{s_A}{s_A+H_1(id)}\right]P_2\right)} = \frac{\hat{e}(P_1,P_2)^{(x_A+x_A')s_A}\cdot u}{\hat{e}\left([x_A+x_A'](H_1(id)+[s_A])P_1, \left[\frac{s_A}{s_A+H_1(id)}\right]P_2\right)} = \frac{\hat{e}(P_1,P_2)^{(x_A+x_A')s_A}\cdot u}{\hat{e}([x_A+x_A']P_1,[s_A]P_2)} = \frac{\hat{e}(P_1,P_2)^{(x_A+x_A')s_A}\cdot u}{\hat{e}(P_1,P_2)^{(x_A+x_A')s_A}} = u,$$

$$C_4'/\hat{e}(C_2', sk_B) = \frac{g_B^{x_B+x_B'}\cdot t}{\hat{e}\left([x_B+x_B']Q_B, \left[\frac{s_B}{s_B+H_2(id)}\right]P_2\right)} = \frac{\hat{e}(P_1,P_2)^{(x_B+x_B')s_B}\cdot t}{\hat{e}\left([x_B+x_B'](H_2(id)+[s_B])P_1, \left[\frac{s_B}{s_B+H_2(id)}\right]P_2\right)} = \frac{\hat{e}(P_1,P_2)^{(x_B+x_B')s_B}\cdot t}{\hat{e}([x_B+x_B']P_1,[s_B]P_2)} = \frac{\hat{e}(P_1,P_2)^{(x_B+x_B')s_B}\cdot t}{\hat{e}(P_1,P_2)^{(x_B+x_B')s_B}} = t,$$

步骤⑥的正确性显然，如图 4 所示。因此，算法 Dec的解密结果为原明文m。

3）等式测试正确性。对任意$(mpk,msk)\leftarrow Setup(1^\lambda)$，$id_i,id_j,m_i,m_j,C_i\leftarrow Enc(mpk,id_i,m_i)$，$C_j\leftarrow Enc(mpk,id_j,m_j)$，$C_i'\leftarrow Rerand(mpk,id_i,C_i)$和$C_j'\leftarrow Rerand(mpk,id_j,C_i)$在$Test(C_i',C_j')$中，我们可以验证步骤③~⑥的正确性如下。由$A_i,f_i(A_i),A_j,f_j(A_j)$，我们可以建立以下方程组：

$$\begin{cases} f_i(A_i) = f_{i,0} + f_{i,1}\cdot A_i, \\ f_j(A_j) = f_{j,0} + f_{j,1}\cdot A_j。 \end{cases}$$

当且仅当 2 个密文对应同一明文$m_i=m_j$时，其多项式系数满足$f_{i,0}=f_{j,0},f_{i,1}=f_{j,1}$（为方便书写后面统一记为$f_0,f_1$），此时我们可以得到一个包含 2 个方程和 2 个未知变量的方程组，写为矩阵形式如下：

$$\begin{pmatrix} 1 & A_i \\ 1 & A_j \end{pmatrix}\begin{pmatrix} f_0 \\ f_1 \end{pmatrix} = \begin{pmatrix} f_i(A_i) \\ f_j(A_j) \end{pmatrix}, \tag{1}$$

该系数矩阵 $\boldsymbol{V}$为范德蒙矩阵，其行列式为$\det(\boldsymbol{V})=A_j-A_i$。当且仅当行列式$\det(\boldsymbol{V})\neq 0$时，该方程组存在唯一解。由于$A_i,A_j$是从$\mathbb{Z}_p$中随机选取的，所以$\det(\boldsymbol{V})\neq 0$的概率为$1/p(p-1)$，这意味着方程组以压倒性概率存在唯一解$f_0,f_1$。接着验证$f_1$是否等于$H_4(f_0,f_0)$，“等于”则系数合法使测试算法输出 1。反之，当$m_i\neq m_j$时，$f_{i,0}\neq f_{j,0},f_{i,1}\neq f_{j,1}$，显然式(1)有无穷解，因此测试算法输出为 0。

5 安全性分析

定理 1. 设方案中的密码函数$H_i,i\in\{1,2,3,4\}$为随机谕言机，如果 q-DBDHI*假设成立，则本文提出的 RCCA-SM9-IBEET 方案满足 OW-ID-RCCA 安全性。

证明. 我们定义一系列游戏，记作 Game$_j$（其中j=0, 1），其中 Game$_0$是敌手$\mathcal{A}$针对$\prod_{\text{RCCA-SM9-IBEET}}$进行 OW-ID-RCCA 安全游戏的初始设定。在每个游戏中，m由挑战者随机选择，而m'是敌手$\mathcal{A}$在游戏结束时输出的结果。对于j=0, 1, 我们定义事件W_j表示在Game$_j$中$m=m'$成立。

1）Game$_0$。游戏中挑战者的逻辑如图 5 所示。

敌手$\mathcal{A}$可以进行多次私钥查询、解密查询、H_1随机谕言机查询和H_2随机谕言机查询，但只能进行 1 次加密查询。在初始化阶段，挑战者计算(mpk,msk)，设置$(m^*,R^*,id^*)\leftarrow\perp$，并像真实游戏一样准备一个空列表$List^{id}$，同时初始化 2 个有关联的数组$Map$，$Map'$：$\mathcal{ID}\rightarrow\mathbb{Z}_p$来记录随机谕言机$H_1,H_2$的响应。由于没有设置陷门，$\mathcal{A}$可以对任意 2 个用户的密文进行等式测试。当$\mathcal{A}$进行私钥查询、解密查询和等式测试时，挑战者的行为与实际游戏一致，不同之处在于当需要计算$H_i,i\in\{1,2,3,4\}$时，调用的是随机谕言机。对于每个随机谕言机查询，挑战者从哈希函数映射到的群中均匀随机选取 1 个群元素作为响应，并使用数组记录该响应。除额外的记录操作外，挑战者的行为与实际游戏完全相同。因此，我们有

$$|Pr[W_0]| = Adv_{\mathcal{A},\Pi}^{\text{OW-ID-RCCA}}(\lambda)。$$

2）Game$_1$。此游戏中，我们改变了初始化和随机谕言机查询的步骤，如图 6 所示，其中q_{H_1},q_{H_2}分别表示对H_1,H_2随机谕言机查询总次数。

修改的主要目的是让挑战者在初始化阶段就确定哈希值。对于挑战身份，挑战者需要查询随机谕言机以获得h_1^*,h_2^*，但它并不知道查询的确切索引位置。因此，在步骤①和步骤②中，挑战者需要分别在H_1,H_2随机谕言机中猜测索引h_1^*,h_2^*（对应的响应在步骤④和步骤⑥中。此后，挑战者的行为与 Game$_0$完全相同。为保持一致性，在加密查询步骤中添加了 1 条额外的终止规则（图 6 中的步骤⑦）。因此，

$$|Pr[W_1]-Pr[W_0]| \leqslant \frac{1}{q_{H_1}\cdot q_{H_2}}。$$

3）Game$_2$。此游戏中，挑战者替换挑战密文中的$A^*\|f(A^*)$为$\mathbb{Z}_p$中的随机元素。在原方案中，$f(A)==H_3(m)+H_3(H_3(m)\|H_3(m))A \bmod p$，其中$H_3,H_4$被建模为随机谕言机。在敌手未查询$H_3(m^*)$的情况下，$f_0^*=H_3(m^*)$和$f_1^*=H_4(H_3(m^*)\|H_3(m^*))$对敌手来说是未知的随机值，因此$f^*(A^*)=H_3(m^*)+H_4(H_3(m^*)\|H_3(m^*))A^* \bmod p$在敌手视角中是均匀随机的$\mathbb{Z}_p$元素。Game$_2$的其他部分与Game$_1$相同。我们定义事件$E$：敌手$\mathcal{A}$在游戏过程中查询了$H_3(m^*)$。由于敌手最多进行$q_{H_3}$次$H_3$查询，且$m^*$是从消息空间$\mathcal{M}$中随机选取，因此$|Pr[E]|\leqslant q_{H_3}/p$。

初始化：

$s_A, s_B \leftarrow \$[1, p-1]$ $P_A \leftarrow [s_A]P_1$ $P_B \leftarrow [s_B]P_1$ $g_A \leftarrow \hat{e}(P_B, P_2)$ $g_B \leftarrow \hat{e}(P_B, P_2)$

$mpk \leftarrow (P_A, P_B, g_A, g_B)$ $msk \leftarrow (s_A, s_B)$ $(m^*, R^*, id^*) \leftarrow \perp List^{id} \leftarrow \varnothing$

初始化2个空的关联数组：Map, Map'：$\mathcal{ID} \leftarrow \mathbb{Z}_p$，向$\mathcal{A}$发送$mpk$

当收到加密查询$id^* \in \mathcal{ID}$

if $id^* \in List^{id}$ then return $\perp$ endif

$h_1^* \leftarrow H_1(id^*)$ $h_2^* \leftarrow H_2(id^*)$

if $s_A + h_1^* \equiv 0 \bmod p$ or $s_B + h_2^* \equiv 0 \bmod p$ then return $\perp$ endif

$\mathrm{sk}_A^* \leftarrow \left[\frac{s_A}{s_A + h_1^*}\right]P_2$ $\mathrm{sk}_B^* \leftarrow \left[\frac{s_A}{s_A + h_2^*}\right]P_2$

$m \leftarrow \$$ $m^* \leftarrow m$ $R^* \leftarrow \$\mathbb{G}_T$ $s^* \leftarrow F(R^*) \cdot m^*$ $t^* \leftarrow G(s^*) \cdot R^*$ $u^* \leftarrow H(t^*) \cdot s^*$

$Q_A^* \leftarrow [h_1]P_1 + P_A$ $Q_B^* \leftarrow [h_2]P_1 + P_B$ $x_A^*, x_B^*, A^* \leftarrow \$[1, p-1]$ $C_1^* \leftarrow [x_A^*]Q_A^*$

$C_2^* \leftarrow [x_B^*]Q_B^*$ $C_3^* \leftarrow g_A^{x_A^*} \cdot u^*$ $C_4^* \leftarrow g_B^{x_B^*} \cdot t^*$ $f_0^* = H_3(m^*)$, $f_1^* = H_4(f_0^* || H_3(m^*))$

$f^*(A^*) = f_0^* + f_1^* \cdot A^* \bmod p$ $C^* = C_1^* || C_3^* || C_4^* || A^* || f^*(A^*)$

将挑战密文C^*发送给$\mathcal{A}$

当收到私钥查询$id_i \in \mathcal{ID}$

if $id^* = id^*$ then return $\perp$ endif

$List^{id}.append(id_i)$ $h_{1,i} \leftarrow H_1(id_i)$ $h_{2,i} \leftarrow H_2(id_i)$

if $s_A + h_{1,i} \equiv 0 \bmod p$ or $s_B + h_{2,i} \equiv 0 \bmod p$ then return $\perp$ endif

$\mathrm{sk}_{A,i} \leftarrow \left[\frac{s_A}{s_A + h_{1,i}}\right]P_2$ $\mathrm{sk}_{B,i} \leftarrow \left[\frac{s_B}{s_B + h_{2,i}}\right]P_2$ $\mathrm{sk}_{id_i} \leftarrow (\mathrm{sk}_{A,i}, \mathrm{sk}_{B,i})$

将私钥sk_{idi}发送给$\mathcal{A}$

当收到解密查询$(id_i, C_i) \in \mathcal{ID} \times C$

$\mathrm{sk}_{id_i} \leftarrow Ext(mpk, msk, id_i)$

$(m, R) \leftarrow Dec(mpk, \mathrm{sk}_{id_i}, C_i)$

if $(m, R) = (m^*, R^*)$ then return $test$ endif

return m

当收到H_1随机谕言机查询$idi \in \mathcal{ID}$

if $id_i \notin Domain(Map)$ then $Map[id_i] \leftarrow \$\mathbb{Z}_p$ endif

将$Map[id_i]$发送给$\mathcal{A}$

当收到H_2随机谕言机查询$idi \in \mathcal{ID}$

if $id_i \notin Domain(Map')$ then $Map'[id_i] \leftarrow \$\mathbb{Z}_p$ endif

将$Map'[id_i]$发送给$\mathcal{A}$

Fig. 5 Game_0

图 5 游戏$_0$

现在考虑2种情况：第1种，当事件E发生时，敌手可能直接发现$A^* || f(A^*)$为随机值，因此在最坏情况下，敌手$\mathcal{A}$在事件E发生时总能区分，因此$|Pr[W_2|E] - Pr[W_1|E]| \leqslant 1$。第2种，当事件$E$不发生时，根据上面的论述显然$f_0^*$和$f_1^*$对敌手来说是随机的，因此$f^*(A^*)$也是随机的。由此推导$Pr[W_2|\neg E] = Pr[W_1|\neg E]$。所以可以得出：

$$\begin{aligned}|Pr[W_2] - Pr[W_1]| &\leqslant Pr[E] \cdot |Pr[W_2|E] - Pr[W_1|E]| + \\ &Pr[\neg E] \cdot |Pr[W_2|\neg E] - Pr[W_1|\neg E]| \leqslant \\ &Pr[E] \cdot 1 + Pr[\neg E] \cdot 0 \leqslant q_{H_3}/p\ 。\end{aligned}$$

4）Game_3。在此游戏中，我们构建模拟器$\mathcal{B}$，它接收变种的q-DBDHI*问题实例$(P_1, [\alpha]P_1, (h_0, [\beta(h_0+\alpha)]P_1, P_2), P_2)$，并向敌手发送挑战密文$C_1^* || C_2^* || C_3^* || C_4^* \leftarrow \beta \times (h_0 + \alpha)P_1 || ([x_B h_B]P_1 + [x_B] \cdot [\alpha]P_1) || R || \hat{e}(P_1, P_2)^{s_B x_B} \cdot M_B$。根据引理1[18]，在不考虑等式测试功能的情况下，本文方案中用于解密的密文生成过程构成一个陷门单向函数，如图4所示，其具体形式为

$$\begin{aligned}f_{mpk,id}((M_A, M_B), x_A, x_B) = C_1 || C_2 || C_3 || C_4 = \\ ([x_A]Q_A) || ([x_B]Q_B) || (g_A^{x_A} \cdot M_A) || (g_B^{x_B} \cdot M_B)\ ,\end{aligned}$$

其中$mpk = (P_A, P_B, g_A, g_B) = (P_A, P_B, \hat{e}(P_A, P_2), \hat{e}(P_B, P_2)) = ([s_A]P_1, [s_B]P_2, \hat{e}(P_1, P_2)^{s_A}, \hat{e}(P_1, P_2)^{s_B}), M_A, M_B \in \mathbb{G}_T$，$Q_A = [s_A + H_1(id)]P_1, Q_B = [s_B + H_2(id)]P_1$，且$x_A, x_B \leftarrow \$[1, p-1]$。陷门$msk = (s_A, s_B)$，且$f_{mpk,id*}^{-1}(C_1 || C_2 || C_3 || C_4) = (C_3 / \hat{e}(C_1, [s_A / [s_A + H_1(id)]]P_2), C_4 / \hat{e}(C_2, [s_B / [s_B + H_2(id)]]))$。

现在本文给出$f_{mpk,id*}$是一个带陷门的单向函数[①]

① 一个陷门单向概率函数f满足：1）$f: E \times R \to F$是一个双射；2）在不知道陷门的情况下，即使敌手能够访问判定谕言机$Same_f(y, y')$(该谕言机回答$g(y) = g(y')$是否成立)，在E上求f的逆仍然是难解的(更多细节参见文献[16])。

初始化：

$s_A, s_B \leftarrow \$[1, p-1]$ $P_A \leftarrow [s_A]P_1$ $P_B \leftarrow [s_B]P_1$

$g_A \leftarrow \hat{e}(P_A, P_2)$ $g_B \leftarrow \hat{e}(P_B, P_2)$ $mpk \leftarrow (P_A, P_B, g_A, g_B)$ $mpk \leftarrow (s_A, s_B)$

① $i_1^* \leftarrow \$[1, qH_1]$, $h_1^*, h_{1,1}, \ldots, h_{1,qH_1} \leftarrow \$\mathbb{Z}_p$

② $i_1^* \leftarrow \$[1, qH_2]$, $h_1^*, h_{1,1}, \ldots, h_{1,qH_2} \leftarrow \$\mathbb{Z}_p$

$(m^*, R^*, id^*) \leftarrow \perp List^{id} \leftarrow \varnothing$

初始化2个空的关联数组：Map, Map'：$\mathcal{ID} \leftarrow \mathbb{Z}_p$，向$\mathcal{A}$发送$mpk$

当收到H_1随机谕言机查询$idi \in \mathcal{ID}$

③ if $id_i \notin Domain(Map)$ then $Map[id_i] \leftarrow h_{1,i}$ endif

④ if $i = i_1^*$ then $Map[id_i] \leftarrow h_{1,i}^*$ endif

将$Map[id_i]$发送给$\mathcal{A}$

当收到H_2随机谕言机查询$idi \in \mathcal{ID}$

⑤ if $id_i \notin Domain(Map')$ then $Map'[id_i] \leftarrow h_{1,i}$ endif

⑥ if $i = i_2^*$ then $Map'[id_i] \leftarrow h_{2,i}^*$ endif

将$Map'[id_i]$发送给$\mathcal{A}$

当收到私钥查询$id^* \in \mathcal{ID}$

if $id^* \in List^{id}$ then return $\perp$endif

$h_1^* \leftarrow H_1(id^*)$ $h_2^* \leftarrow H_2(id^*)$

⑦ if $id^* \neq id_{i_1^*}$ and $id^* \neq id_{i_2^*}$ then return $\perp$endif

if $s_A + h_1^* \equiv 0 \bmod p$ or $s_B + h_2^* \equiv 0 \bmod p$ then return $\perp$endif

将私钥sk_{idi}发送给$\mathcal{A}$

Fig. 6 Game$_1$

图 6 游戏$_1$

的具体证明。

可以看出，$f_{mpk,id^*}: \mathbb{G}_T^2 \times \mathbb{Z}_p^2 \to \mathbb{G}_1 \| \mathbb{G}_1 \| \mathbb{G}_T \| \mathbb{G}_T$是一个双射。

现在考虑 q-DBDHI*假设的一个变体：对于任意有效敌手$\mathcal{A}$，

$$Pr[\mathcal{A}^{O_{\text{DBDHI}^*}(\cdot)}(P_1, [\alpha]P_1, (h_0, [\beta(h_0+\alpha)]P_1), P_2) = \hat{e}(P_1, P_2)^{\alpha\beta} : \alpha, \beta \leftarrow \mathbb{Z}_p] \leqslant negl(\lambda),$$

其中$O_{\text{DBDHI}^*}(\cdot)$是一个 DBDHI*预言机，其输入为$(P_1, [\alpha]P_1, (h_0, [\beta(h_0+\alpha)]P_1), P_2, R)$，若$R = \hat{e}(P_1, P_2)^{\alpha\beta}$则输出 1，否则输出 0。

显然，如果q-DBDHI*假设在$\hat{e}$上成立，则上述变体也成立。假设存在 1 个敌手$\mathcal{A}$，在判定预言机$Same_f(g, g')$的帮助下可以反演f_{mpk,id^*}，那么我们可以通过模拟器$\mathcal{B}$来攻破该变体问题，具体如下：

1）当接收到问题实例$(P_1, [\alpha]P_1, (h_0, [\beta(h_0+\alpha)]P_1), P_2)$时，$\mathcal{B}$令$H_1(id) \leftarrow h_0$，计算$h_B \leftarrow H_1(id)$，随机选择$s_B, x_B \leftarrow \$[1, p-1]$，$R, M_B \leftarrow \mathbb{G}_T$，构造挑战密文$C_1^* \| C_2^* \| C_3^* \| C_4^* = ([\beta(h_0+\alpha)]P_1) \| \quad ([x_B h_B]P_1 + [\alpha x_B]P_1) \quad \| R \| \hat{e}(P_1, P_2)^{s_B x_B} \cdot M_B$，然后将$C_1^* \| C_2^* \| C_3^* \| C_4^*$发送给$\mathcal{A}$。

2）当接收到判定预言机查询$Same_f(C_1 \| C_2 \| C_3 \| C_4, C_1' \| C_2' \| C_3' \| C_4')$时，$\mathcal{B}$返回：$O_{\text{DBDHI}^*}(P_1, [\alpha]P_1, (h_0, C_1' - C_1), P_2, C_3'/C_3) \wedge O_{\text{DBDHI}^*}(P_1, [s_B]P_1, (h_B, C_2' - C_2), P_2, C_4'/C_4)$。

3）当$\mathcal{A}$输出$C_1^* \| C_2^* \| C_3^* \| C_4^*$对应的正确像$(M_1, M_2)$时，则$C_3^*/M_1$即为DBDHI*问题的解。

因此，如果敌手$\mathcal{A}$能以不可忽略的优势赢得 Game$_3$，那么$\mathcal{B}$就能破解 q-DBDHI*问题。所以有

$$|Pr[W_3] - Pr[W_2]| \leqslant Adv_{\mathcal{B}}^{q\text{-DBDHI}^*}(\lambda),$$

其中$Adv_{\mathcal{B}}^{q\text{-DBDHI}^*}(\lambda)$是可忽略的。

综上，我们可以推断出：

$$Adv_{\mathcal{A},\Pi}^{\text{OW-ID-RCCA}}(\lambda) \leqslant Adv_{\mathcal{B}}^{q\text{-DBDHI}^*}(\lambda) + \frac{q_{H_3}}{p} + \frac{1}{q_{H_1} \cdot q_{H_2}}。$$

定理 1（即本方案在 OW-ID-RCCA 安全模型下的安全性）得证。 证毕.

6 实验性能分析

本节对方案的计算开销和通信开销进行理论分析和实验测试，并与文献 [18] 提出的 RCCA-SM9 加密方案、文献 [19] 提出的 SM9-IBEET-CRF 方案、文献 [25] 提出的 SM9-FSET 方案展开对比。上述对比方案的选择主要基于以下考虑：一是功能可比性，所选方案分别覆盖基础 SM9 加密、等式测试以及抗颠覆等典型功能；二是安全模型相关性，文献 [18] 选择 IND-ID-RCCA 作为安全模型，文献 [19] 聚焦抗颠覆

攻击, 文献 [25] 支持 IND-ID-CCA 与 OW-ID-CCA 安全性, 与本文研究目标一致; 三是系统模型一致性, 其均基于 SM9 标识加密体制, 保证对比结果的公平性与合理性。

6.1 理论分析

对于计算开销, 考虑初始化、私钥生成、加密、密文重随机化、解密算法和等式测试中各项耗时运算的次数(预计算的步骤未计入), 分析结果如表 1 所示。

相较于 RCCA-SM9, 本文方案仅在加密阶段多进行 1 次 A_Z 和 M_Z 操作, 其他阶段开销完全一致。由于有限域 F_N 上的加法和乘法耗时与其他群上的运算至少相差 2 个数量级, 所以开销基本可以忽略, 增加等式测试模块并未额外增加计算开销。对比 SM9-IBEET-CRF, 在私钥生成方面少了 1 次哈希运算操作, 在加密方面减少了 $3H+2BP+A_1+2M_2+B_2$, 但增加了 $5M_T+A_Z+M_Z$。虽然群 $\mathbb{G}_T$ 的乘法较多, 但哈希运算与双线性对运算的减少降低了计算耗时, 且实现了全密文重随机化。对比 SM9-FSET, 由于本文方案不设置前向安全性, 无 0/1 编码操作, 加密方面少了接近集合元素个数倍乘量的哈希运算和群 $\mathbb{G}_2$ 的标量乘运算, 在解密方面虽然增加了 $2M_T$, 但减少了 $5H+M_1+E_T$, 在解密效率上具有一定优势。这表明引入逆向防火墙实现重随机化机制, 在理论计算层面并未带来较大的计算开销, 且实现了等式测试功能。

对于通信开销, 考虑系统公钥、用户私钥和密文的比特位数, 分析结果如表 2 所示。

可见, 本文方案在系统公钥方面上的开销均大于或等于另外 3 个方案, 用户私钥大小与其他方案相同。在密文大小方面, 本文方案虽大于文献 [18], 但额外实现了等式测试功能, 拓展了应用。对比文献 [19], 因群 $\mathbb{G}_T$ 上的元素比特位数远大于群 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 的, 所以本文方案密文略大, 但实现了全部密文的重随机化, 在安全性和隐私保护方面具有更强的优势。综合来看, 本文方案虽然在通信开销未领先对比方案, 但通过适度增加开销, 换取了更强的安全特性与功能性, 整体设计在安全性-开销的权衡中处于合理区间。

6.2 实验分析

本文基于国密算法开源 Python 库 hggm, 采用 SM9 国标规定的参数设置, 通过 Python 编程实现了上述方案, 并对各方案算法的性能进行测试。实验计算机配置为 64 位 Windows10 操作系统, CPU 为 11thGen Intel Core i7-11800H, 配备 16 GB 内存, 使用 Python 版本为 3.8.20。同时, 为了确保实验结果的准确性, 运行了 1 000 次实验获取平均值, 结果如图 7 所示。其中 SM9-FSET 的时间编码集合大小取 16。

在初始化阶段, 本文方案与 RCCA-SM9 耗时相近(约 23 ms), 但显著高于 SM9-IBEET-CRF。这是由于本文方案在主密钥生成中引入了增强安全的参数结构, 计算复杂度相对较高, 属于实现可证明安全所必需的基础开销。在加密方面, 本文方案耗时略高于 RCCA-SM9, 多出约 2.6 ms。这部分差异主要源于为

Table 1 Computational Overhead Analysis

表 1 计算开销分析

方案	*Setup*	*Ext*	*Rerand*	*Enc*	*Dec*	*Test*
RCCA-SM9[18]	$2M_1+2BP$	$2M_2+2H$	$2H+4M_1+4A_1+2E_T+2M_T$	$4M_1+2H+5M_1+2A_1+2E_T$	$2BP+2M_T$	
SM9-IBEET-CRF[19]	$2M_1$	$H+2M_2$	M_1	$4M_1+7H+A_1+2E_T+2M_2+2BP+B_2$	$BP+3H$	$4BP+2H$
SM9-FSET[25]	$M_1+2BP+2E_T$	$2M_2$		$3E_T+5H+2M_1+\|S_i^j\|(H+B_2)$	$2BP+5H+E_T+2M_1$	$4BP+2H+2M_1+2E_T$
RCCA-SM9-IBEET(本文)	$2M_1+2BP$	$2M_2+2H$	$2H+4M_1+4A_1+2E_T+2M_T$	$4M_1+4H+5M_1+2A_1+2E_T+A_Z+M_Z$	$2BP+2M$	$H+3A_Z+2M_Z$

注: M_1, M_2 分别表示群 $\mathbb{G}_1$, $\mathbb{G}_2$ 的标量乘, A_1, A_2 表示群 $\mathbb{G}_1$, $\mathbb{G}_2$ 上的加法运算, B_2 表示群 $\mathbb{G}_2$ 的乘法, BP 表示双线性对运算, M_T 和 E_T 分别表示群 $\mathbb{G}_T$ 的乘法和幂, A_Z 和 M_Z 分别表示 $\mathbb{Z}_p$ 上的加法和乘法运算, H 表示哈希运算(含文献 [19] 的 KDF 和 MAC 运算), $|S_i^j|(i=0, 1)$ 表示对时间 t 进行 0/1 编码之后的集合元素个数。

Table 2 Comparison of Communication Overhead and Security

表 2 通信开销和安全性对比

方案	系统公钥	陷门	用户私钥	密文	安全
RCCA-SM9[18]	$3\|\mathbb{G}_1\|+\|\mathbb{G}_2\|+2\|\mathbb{G}_T\|$		$2\|\mathbb{G}_2\|$	$2\|\mathbb{G}_1\|+2\|\mathbb{G}_T\|$	IND-ID-RCCA
SM9-IBEET-CRF[19]	$3\|\mathbb{G}_1\|+\|\mathbb{G}_2\|$	$\|\mathbb{G}_2\|$	$2\|\mathbb{G}_2\|$	$3\|\mathbb{G}_1\|+\|\mathbb{G}_2\|+2n$	IND-ID-CCA&OW-ID-CCA
SM9-FSET[25]	$2\|\mathbb{G}_1\|+\|\mathbb{G}_2\|+2\|\mathbb{G}_T\|$	$\|S_i^1\|(\|\mathbb{G}_1\|+\|\mathbb{G}_2\|)+sum_{S_i^1}$	$2\|\mathbb{G}_2\|$	$3\|\mathbb{Z}_p\|+2\|\mathbb{G}_1\|+\|S_i^0\|\|\mathbb{G}_2\|+sum_{S_i^0}+n$	IND-ID-CCA&OW-ID-CCA
RCCA-SM9-IBEET(本文)	$3\|\mathbb{G}_1\|+\|\mathbb{G}_2\|+2\|\mathbb{G}_T\|$		$2\|\mathbb{G}_2\|$	$2\|\mathbb{G}_1\|+2\|\mathbb{G}_T\|+2\|\mathbb{Z}_p\|$	OW-ID-RCCA

注: $|\mathbb{G}_1|$, $|\mathbb{G}_2|$, $|\mathbb{G}_T|$, $|\mathbb{Z}_p|$ 对应群(或域), n 表示明文的二进制比特长度, $sum_{S_i^j}$ ($i=0, 1$) 表示时间 t 进行 0/1 编码得到的集合所有元素的二进制比特长度之和。具体而言, 对于 SM9 国标规范使用的 256 b 的 BN 曲线, $|\mathbb{G}_1|=512$, $|\mathbb{G}_2|=1\,024$, $|\mathbb{G}_T|=3\,072$, $|\mathbb{Z}_p|=256$。

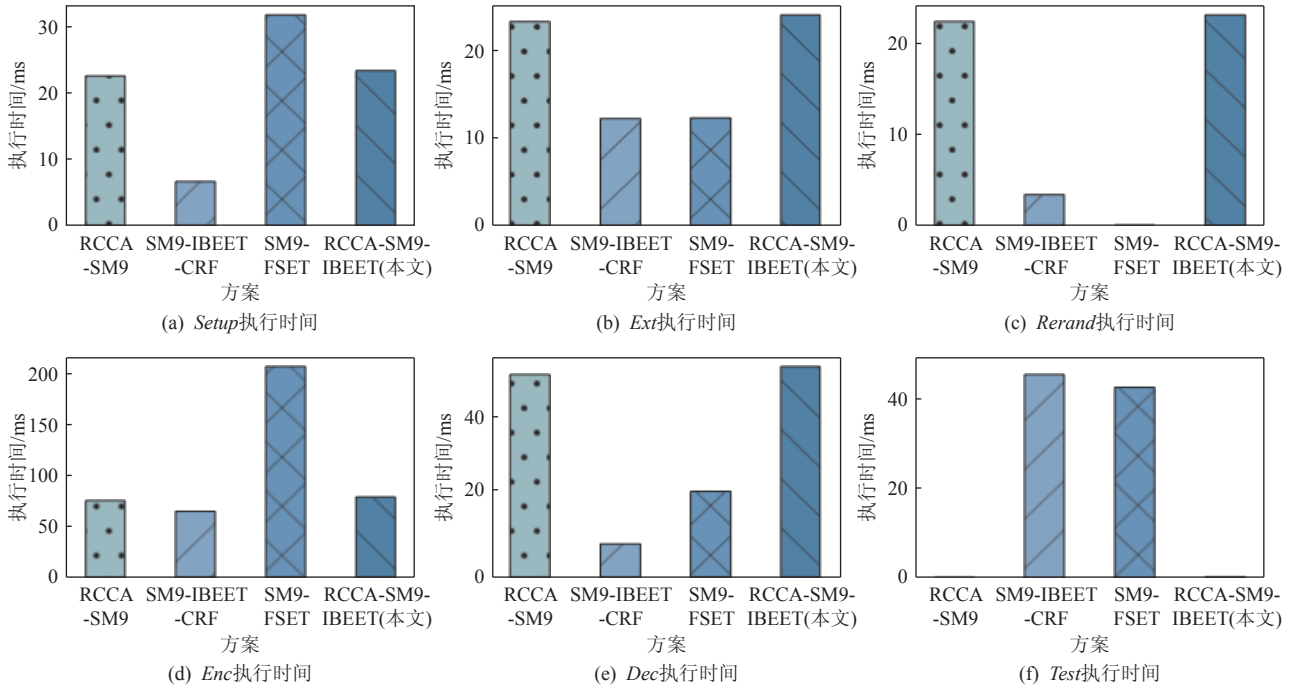


Fig. 7 Execution time comparison in each stage

图 7 各阶段执行时间对比

支持密文等式测试而额外引入的哈希运算与有限域运算，可视为在加密功能扩展上的合理性能代价。相较于同样支持等值测试的 SM9-FSET 方案，本文方案未设置前向安全性，避免了运算量的大幅增加，加密效率具有明显优势。重随机化阶段，本文方案耗时与 RCCA-SM9 基本一致（约 23 ms），远高于 SM9-IBEET-CRF。这部分开销主要用于实现抵抗后门攻击的能力，通过更充分的随机化过程提升方案的安全性，属于为实现更强安全目标所接受的开销代价。在解密方面，由于本文方案与 RCCA-SM9 均进行 2 次双线性对运算以及 2 次群 $\mathbb{G}_T$ 上的乘法，因此解密耗时相对于另外 2 个方案耗时较长。等式测试阶段，本文方案表现出显著优势，仅需 0.066 ms，远低于 SM9-IBEET-CRF 和 SM9-FSET。这是因为本文方案在设计上避免了双线性对运算，仅通过有限域与群运算完成测试，在保证功能完整的同时大幅提升了执行效率，体现出良好的实用性。

为了确保实验分析的全面性和可靠性，本文详细研究了所提出 RCCA-SM9-IBEET 各阶段的时间开销，如图 8 所示。分析可见，在初始化阶段（*Setup*）、私钥生成阶段（*Ext*）和重随机化阶段（*Rerand*），实际运行开销分别占 11.6%，12.0%，11.5%，而加密阶段（*Enc*）和解密阶段（*Dec*）运行开销占比最大，分别为 38.8%，26.1%。这表明加密与解密阶段是算法的主要时间开销来源，而初始化、私钥生成和重随机化阶段

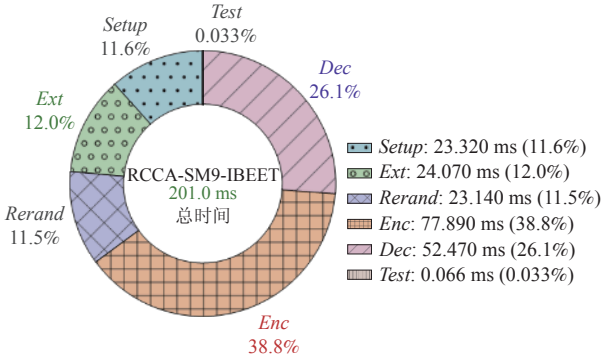


Fig. 8 Time distribution of RCCA-SM9-IBEET

图 8 RCCA-SM9-IBEET 时间分布

的合计开销占 35.1%，虽不可完全忽略，但相对较小。此外，RCCA-SM9-IBEET 加密阶段的开销大于解密阶段的开销，这意味着在整个算法运行过程中加密部分需要的时间更多。因此，后续若要提高算法效率，应考虑优化加密算法。

7 结 论

针对已有 IBEET 算法难以抵抗颠覆攻击的问题，本文首先提出了一种 RCCA 安全的支持等式测试的 SM9 标识加密算法（RCCA-SM9-IBEET），该方案可以运用于云服务器中加密数据的外包计算方案。本文方案在用户与云服务器之间的上行信道分别部署了

密码逆向防火墙;定义了 OW-ID-RCCA 安全模型;然后在 q-DBDHI*假设下的随机谕言机模型中证明了它的安全性;最后通过严格的理论分析和实验分析表明,在本文实验环境下,RCCA-SM9-IBEET 单次等式测试时间仅需 0.066 ms,在计算效率上较已有同类方案具有明显优势。

作者贡献声明:陈思宇负责方案整体设计、方案实现、安全性分析以及论文撰写;欧阳梦迪提出研究思路并参与方案讨论与修改;李发根提出指导意见并修改论文。

参 考 文 献

[1] Armbrust M, Fox A, Griffith R, et al. A view of cloud computing[J]. Communications of the ACM, 2010, 53(4): 50−58

[2] Bösch C, Hartel P, Jonker W, et al. A survey of provably secure searchable encryption[J]. ACM Computing Surveys, 2014, 47(2): 1−51

[3] Iqbal S, Kiah M L M, Dhaghighi B, et al. On cloud security attacks: A taxonomy and intrusion detection and prevention as a service[J]. Journal of Network and Computer Applications, 2016, 74: 98−120

[4] Chen Liqing, Xu Shiguo, Jin Chunhua, et al. Partially hidden policy attribute-based multi-keyword searchable encryption with verification and revocation[J]. IEEE Transactions on Mobile Computing, 2025, 24(9): 9020−9035

[5] Kamara S, Papamanthou C, Roeder T. Dynamic searchable symmetric encryption[C]//Proc of the 19th ACM Conf on Computer and Communications Security. New York: ACM, 2012: 965−976

[6] Sun Shifeng, Yuan Xingliang, Liu J K, et al. Practical backward-secure searchable encryption from symmetric puncturable encryption[C]//Proc of the 25th ACM Conf on Computer and Communications Security. New York: ACM, 2018: 763−780

[7] Xu Yongliang, Cheng Hang, Liu Ximeng, et al. PCSE: Privacy-preserving collaborative searchable encryption for group data sharing in cloud computing[J]. IEEE Transactions on Mobile Computing, 2025, 24(5): 4558−4572

[8] Zhang Rui, Xue Rui, Liu Ling. Searchable encryption for healthcare clouds: A survey[J]. IEEE Transactions on Services Computing, 2017, 11(6): 978−996

[9] Zhang Kai, Hu Boli, Ning Jianting, et al. Pattern hiding and authorized searchable encryption for data sharing in cloud storage[J]. IEEE Transactions on Knowledge and Data Engineering, 2025, 37(5): 2802−2815

[10] Yang Guomin, Tan C, Huang Qiong, et al. Probabilistic public key encryption with equality test[C]//Proc of the 10th Cryptology-CT-RSA. Berlin: Springer, 2010: 119−131

[11] Ma Sha. Identity-based encryption with outsourced equality test in cloud computing[J]. Information Sciences, 2016, 328: 389−402

[12] Young A, Yung M. Kleptography: Using cryptography against cryptography[C]//Proc of the 16th Cryptology-EUROCRYPT. Berlin: Springer, 1997: 62−74

[13] Bellare M, Paterson K G, Rogaway P. Security of symmetric encryption against mass surveillance[C]//Proc of the 34th Cryptology-CRYPTO. Berlin: Springer, 2014: 1−19

[14] Mironov I, Stephens-Davidowitz N. Cryptographic reverse firewalls[C]//Proc of the 34th Cryptology-EUROCRYPT. Berlin: Springer, 2015: 657−686

[15] Canetti R, Krawczyk H, Nielsen J B. Relaxing chosen-ciphertext security[C]//Proc of the 23rd Cryptology-CRYPTO. Berlin: Springer, 2003: 565−582

[16] Phan D H, Pointcheval D. OAEP 3-round: A generic and secure asymmetric encryption padding[C]//Proc of the 15th Cryptology-ASIACRYPT. Berlin: Springer, 2004: 63−77

[17] Ouyang Mengdi, Sun Qinshuo, Li Fagen. Subversion attacks and countermeasures of SM9 encryption[J]. Netinfo Security, 2024, 24(6): 831−842 (in Chinese)
(欧阳梦迪, 孙钦硕, 李发根. SM9 加密算法的颠覆攻击与改进[J]. 信息网络安全, 2024, 24(6): 831−842)

[18] Chen Rongmao, Chen Jingrong, Huang Xinyi, et al. RCCA-SM9: Securing SM9 on corrupted machines[J]. Science China: Information Sciences, 2024, 67(11): 212103

[19] Xiong Hu, Lin Ye, Yao Ting. SM9 identity-based encryption scheme supporting equality test and key reverse firewall[J]. Journal of Computer Research and Development, 2024, 61(4): 1070−1084 (in Chinese)
(熊虎, 林烨, 姚婷. 支持等式测试及密码逆向防火墙的 SM9 标识加密方案[J]. 计算机研究与发展, 2024, 61(4): 1070−1084)

[20] Tang Qiang. Towards public key encryption scheme supporting equality test with fine-grained authorization[C]//Proc of the 16th Security-ACISP. Berlin: Springer, 2011: 389−406

[21] Huang Kaibin, Tso R, Chen Y C, et al. PKE-AET: Public key encryption with authorized equality test[J]. The Computer Journal, 2015, 58(10): 2686−2697

[22] Ma Sha, Huang Qiong, Zhang Mingwu, et al. Efficient public key encryption with equality test supporting flexible authorization[J]. IEEE Transactions on Information Forensics and Security, 2014, 10(3): 458−470

[23] Susilo W, Guo Fuchun, Zhao Zhen, et al. PKE-MET: Public-key encryption with multi-ciphertext equality test in cloud computing[J]. IEEE Transactions on Cloud Computing, 2022, 10(2): 1476−1488

[24] Yang Zhichao, He Debiao, Qu Longjiang, et al. An efficient identity-based encryption with equality test in cloud computing[J]. IEEE Transactions on Cloud Computing, 2023, 11(3): 2983−2992

[25] Han Jinguang, Zhang Jianlong. Security-oriented ciphertext equivalence test for SM9[J]. SCIENTIA SINICA Informationis, 2025, 55(8): 2002−2017 (in Chinese)
(韩金广, 张健龙. 面向安全的 SM9 密文等值测试[J]. 中国科学: 信息科学, 2025, 55(8): 2002−2017)

[26] Chase M, Kohlweiss M, Lysyanskaya A, et al. Malleable proof systems and applications[C]//Proc of the 31st Cryptology-EUROCRYPT. Berlin: Springer, 2012: 281−300

[27] Libert B, Peters T, Chen Qian. Structure-preserving chosen-ciphertext

security with shorter verifiable ciphertexts[C]//Proc of the 20th Cryptology-PKC. Berlin: Springer, 2017: 247−276

[28] Faonio A, Fiore D, Herranz J, et al. Structure-preserving and re-randomizable RCCA-secure public key encryption and its applications[C]//Proc of the 30th Cryptology-ASIACRYPT. Berlin: Springer, 2019: 159−190

[29] Faonio A, Fiore D. Improving the efficiency of re-randomizable and replayable CCA secure public key encryption[C]//Proc of the 18th Security-ACNS. Berlin: Springer, 2020: 271−291

[30] Wang Yi, Chen Rongmao, Yang Guomin, et al. Receiver-anonymity in rerandomizable RCCA-secure cryptosystems resolved[C]//Proc of the 41st Cryptology-CRYPTO. Berlin: Springer, 2021: 270−300

[31] Chen Rongmao, Wang Yi, Huang Xinyi. RCCA security design for the SM2 encryption algorithm[J]. SCIENTIA SINICA Informationis, 2023, 53(2): 266−281 (in Chinese)
(陈荣茂, 王毅, 黄欣沂. 国密 SM2 加密算法的 RCCA 安全设计[J]. 中国科学: 信息科学, 2023, 53(2): 266−281)

[32] Chakraborty S, Dziembowski S, Nielsen J B. Reverse firewalls for actively secure MPCs[C]//Proc of the 40th Cryptology-CRYPTO. Berlin: Springer, 2020: 732−762

[33] Zhou Yuyang, Zhao Liang, Li Fagen, et al. Exfiltration-resistant proxy re-encryption for IoT data sharing in unreliable clouds[J]. IEEE Transactions on Dependable and Secure Computing, 2025, 22(4): 4070−4085

[34] Yang Xiaodong, Luo Xilai, Liao Zefan, et al. A CP-ABE-based access control scheme with cryptographic reverse firewall for IoV[J]. Journal of Systems Architecture, 2025, 160: 103331

[35] Ouyang Mengdi, Sun Qinshuo, Li Fagen. Subversion-resistant identity-based aggregate signature with reverse firewalls for IoV[J]. IEEE Transactions on Vehicular Technology, 2025, 74(7): 10841−10852

[36] Zhou Yuyang, Hu Zhebin, Li Fagen. Searchable public-key encryption with cryptographic reverse firewalls for cloud storage[J]. IEEE Transactions on Cloud Computing, 2023, 11(1): 383−396

[37] Ming Yang, Liu Hang, Wang Chenhao, et al. Generic construction: Cryptographic reverse firewalls for public key encryption with keyword search in cloud storage[J]. IEEE Transactions on Cloud Computing, 2024, 12(2): 405−418

[38] Elhabob R, Eltayieb N, Hu Xiong, et al. Equality test on identity-based encryption with cryptographic reverse firewalls for telemedicine systems[J]. IEEE Internet of Things Journal, 2025, 12(2): 2106−2121



Chen Siyu, born in 2005. Undergraduate. Her main research interests include post-snowden cryptography and applied cryptography.
陈思宇, 2005 年生。本科生。主要研究方向为后斯诺登密码学、应用密码学。



Ouyang Mengdi, born in 1996. PhD. Her main research interests include post-snowden cryptography and applied cryptography.
欧阳梦迪, 1996 年生。博士。主要研究方向为后斯诺登密码学、应用密码学。



Li Fagen, born in 1979. PhD, professor, PhD supervisor. His main research interests include cryptography and network security.
李发根, 1979 年生。博士, 教授, 博士生导师。主要研究方向为密码学、网络安全。