中国科学: 信息科学 2023 年 第 53 卷 第 2 期: 266–281
SCIENTIA SINICA Informationis
论文

国密 SM2 加密算法的 RCCA 安全设计

陈荣茂[1], 王毅[1], 黄欣沂[2*]

1. 国防科技大学计算机学院, 长沙 410073
2. 香港科技大学 (广州) 信息枢纽人工智能学域, 广州 511466
* 通信作者. E-mail: xinyi@ust.hk

收稿日期: 2022–07–13; 修回日期: 2022–08–25; 接受日期: 2022–08–31; 网络出版日期: 2023–02–03

国家自然科学基金 (批准号: 62122092, 62032005, 61702541) 资助项目

摘要 国密 SM2 密码算法已经成为保障我国网络信息系统安全自主可控的关键技术. 然而近期研究发现, SM2 加密算法在实际部署应用时面临高效的算法替换攻击. 该种攻击可以从当前的密文预测下一次加密所使用的随机数, 从而可以在不知道解密密钥的情况下成功解密后续密文. 密码逆向防火墙技术已被证实可以有效抵抗该种攻击, 但其要求密文具有可重随机性, 与 SM2 加密算法本身所具备的 CCA (chosen-ciphertext attack) 安全性相冲突. 针对该问题, 本文改进 SM2 加密算法, 构造了具有 RCCA (可重放 CCA) 安全性的公钥加密方案. 该方案具有与 SM2 加密算法近似的安全性, 且同时支持密文重随机操作, 因此可以有效兼容密码逆向防火墙. 方案的设计遵循 Phan 等提出的 OAEP 三轮构造范式, 结合 SM2 加密算法进行改进, 并在随机预言机模型下给出了严谨的安全证明. 本文提出了首个基于国密算法的可重随机 RCCA 公钥加密方案, 研究结果有助于提升 SM2 密码算法在实际应用中的安全性.

关键词 SM2, 加密算法, RCCA, 可重随机性, 密码逆向防火墙

1 引言

安全性是密码算法的根本属性, 如何设计安全的密码算法一直以来都是密码学研究人员所面临的挑战性难题. 在早期阶段, 密码算法设计主要依赖人工经验和复杂的机械装置, 缺乏科学的理论指导, 导致算法安全问题频出. 20 世纪 80 年代, 麻省理工学院 (Massachusetts Institute of Technology) 的 Goldwasser 和 Micali [1] 首次提出可证明安全技术, 通过采用计算复杂性理论, 将攻破密码算法与解决数学难题建立近似等价关系, 为密码算法的安全性提供了科学的理论依据. 他们的工作奠定了现代密码学可证明安全理论的基础, 使得密码学从艺术走向科学, 并极大地促进密码技术应用的蓬勃发展.

引用格式: 陈荣茂, 王毅, 黄欣沂. 国密 SM2 加密算法的 RCCA 安全设计. 中国科学: 信息科学, 2023, 53: 266–281, doi: 10.1360/SSI-2022-0282
Chen R M, Wang Y, Huang X Y. RCCA-secure public-key encryption based on SM2 (in Chinese). Sci Sin Inform, 2023, 53: 266–281, doi: 10.1360/SSI-2022-0282

可证明安全的鲁棒性依赖于一系列的条件假设. 其中一个非常重要的假设是密码算法的实际部署严格遵守相应的标准规范. 然而 2013 年的 “斯诺登事件” 以及越来越多的供应链攻击事件表明, 实际生活中用户所使用的密码系统可能偏离应该遵守的部署规范, 甚至遭受恶意篡改植入隐蔽后门, 使得攻击者可以获取系统密钥, 彻底破坏密码系统安全. 2014 年国际密码年会上, Bellare 等 [2] 首次提出了 “算法替换攻击” (algorithm substitution attack) 的概念, 展示了如何通过对加密算法进行隐蔽篡改, 在用户无法察觉的情况下实现加密算法的密钥渗漏. 事实上, 在早期阶段, Yung 等 [3] 也提出了类似的攻击思想, 即 “盗码学攻击” (kleptographic attack). 该攻击也是通过设计隐蔽后门窃取算法密钥. 然而由于当时密码技术发展处在比较早期的阶段, 该种攻击在学术界并没有得到广泛的重视. 因此, “算法替换攻击” 可以看作是 “盗码学攻击” 的延伸. 2013 年的 “斯诺登事件” 促使了越来越多的学者相信该种攻击存在于现实世界中, 并投入精力开展研究.

商用密码算法 (SM 系列) 是我国自主设计的密码算法, 近年来已经在越来越多的行业得到推广应用 [4, 5], 为实现我国网络信息系统自主可控提供了关键技术支撑. 然而, 近期黄等 [6] 研究发现, SM2 加密算法面临极其高效的算法替换攻击威胁. 攻击者通过修改加密算法中随机数的选取方式, 可以从两个连续的密文恢复出整个底层明文. 考虑到 SM2 密码算法的重要性, 本文拟重点针对 SM2 加密算法, 设计能够抵抗算法替换攻击的防护技术, 强化 SM2 加密算法安全保障功能. 事实上, 目前学术界在算法替换攻击防护研究方面已经取得了若干积极进展. 根据防护机制的核心思想, 主要分为阻止型 (prevention-based) 和检测型 (detection-based). 前者假设存在可信的 “密码逆向防火墙” (cryptographic reverse firewall) [7], 通过重随机的方式净化密码算法输出, 消除可能携带的隐蔽信息. 后者假设存在可信的 “看护犬” (watchdog) 对组成密码算法的各个模块进行标准测试 [8], 确保通过测试的模块所组装的算法能够抵抗算法替换攻击. 这两种类型的防护方法所依赖的假设不同, 然而密码逆向防火墙 (简称逆向防火墙) 因为其简洁的工作模式, 被认为具有较高的实用性, 也因此得到了学术界的广泛研究.

逆向防火墙设计所面临的主要难点是如何在不影响原有算法功能的前提下, 对算法输出进行重随机操作, 从而消除可能携带的潜在信息. 然而对于具有标准安全性即适应性选择密文攻击 (chosen-ciphertext attack, CCA) 安全的公钥加密算法而言, 重随机操作会导致密文无法被接收者正常解密. 针对该问题, Dodis 等 [9] 在 2016 年国际密码年会上指出, 可重放适应性选择密文攻击 (replayable chosen-ciphertext attack, RCCA) 安全是一种理想的解决方案. 具备该安全性的公钥加密方案可以在提供近似 CCA 安全保障的同时支持对密文的重随机化操作. 因此, 本文主要考虑如何对 CCA 安全的 SM2 加密算法进行拓展设计, 构造具有 RCCA 安全性的 SM2 加密方案变体, 从而实现逆向防火墙的兼容性, 抵抗潜在的算法替换攻击.

1.1 本文贡献

针对 SM2 加密密文不具备可重随机性的问题, 本文提出了具有可重随机 RCCA 安全性的公钥加密方案. 方案设计的核心思想是采用 Phan 等 [10] 提出的 OAEP 三轮范式, 将其应用于 SM2 加密算法得到 RCCA 安全变体, 并在随机预言机模型下证明该方案满足 Canetti 等 [11] 所定义的 RCCA 安全性. 此外, 相比原有的 SM2 公钥加密算法, 该方案包含了一个新的密文重随机化算法, 能够在不影响密文可解密性的情况下对密文进行修改, 从而支持逆向防火墙对密文进行净化操作, 消除算法替换攻击所引起的潜在信息渗漏. 本文所设计的方案是首个基于国密算法的可重随机 RCCA 公钥加密方案, 研究结果有助于提升 SM2 密码算法在实际应用中的安全性.

1.2 相关工作

本小节简要介绍现有可重随机 RCCA 安全的公钥加密方案. Groth [12] 首次提出了在通用群模型 (generic group model) 下的可重随机 RCCA 安全的公钥加密方案. 该方案的缺点在于密文大小随消息比特长度线性增长. 标准模型下的可重随机 RCCA 安全的公钥加密方案则由 Prabhakaran 和 Rosulek [13] 在 2007 年国际密码年会上首次提出. 该方案的核心思路是针对 Cramer-Shoup 密文的变种应用双股结构实现可重随机性与抗主动攻击安全之间的平衡. 遗憾的是, 该方案并不具有匿名性. 而在 RCCA 安全性下同时实现可重随机性和匿名性对于提升现有隐私保护应用的安全性具有重要意义. 该问题一直未能得到解决, 直到 Wang 等 [14] 在 2021 年国际密码年会上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. 此外, 一些工作在构造可重随机 RCCA 加密方案的同时实现了新的性质. Chase 等 [15] 提出使用可延展的非交互零知识证明系统构造具有公开可验证性的加密方案. Libert 等 [16] 尝试对 Chase 等方案的效率进行优化, 但非交互零知识证明系统的应用仍然带来了较大的计算开销和密文大小. 为此, Faonio 等 [17] 提出了基于 MDDH 假设的方案构造, 将密文大小减少至只有 6 个群元素. 该方案同样基于椭圆曲线构造, 但其加解密过程涉及许多耗时的双线性对运算, 因此效率比较低. 随后, Faonio 和 Fiore [18] 在随机预言机模型下提出了更为高效的 RCCA 方案, 但该方案仅满足弱可重随机性. 近来, Wang 等 [19] 将 RCCA 安全性拓展至标识加密的背景下, 提出了 ID-RCCA 安全性, 并给出了具有匿名性的可重随机 ID-RCCA 标识加密构造方案. 该方案可用于构造基于标识的混淆网络, 以实现对隐私保护应用中恶意滥用行为的审计.

1.3 本文组织结构

第 2 节回顾公钥加密方案、单向陷门函数、困难性假设以及安全性定义等预备知识. 第 3 节重点阐述了本文所提出的新型公钥加密方案, 并详细给出了该方案在随机预言机模型下的 RCCA 安全性分析. 第 4 节对本文工作做了总结.

2 预备知识

2.1 符号表示

令 $\mathsf{poly}(\lambda)$ 表示关于 λ 的多项式函数. 给定函数 $f(\lambda):\mathbb{N}\to\mathbb{R}^+$, 若对于任意多项式函数 $\mathsf{poly}(\lambda)$, 存在正整数 N_c 使得 $f(\lambda)<|1/\mathsf{poly}(\lambda)|$ 对于所有 $n>N_c$ 成立, 那么函数 $f(\lambda)$ 是可忽略的. 令 $\mathsf{negl}(\lambda)$ 表示任意关于 λ 的可忽略函数. 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 公钥加密方案

定义1 (公钥加密方案) 一个公钥加密方案 $\Pi=(\mathsf{KGen},\mathsf{Enc},\mathsf{Dec})$ 由以下 3 个算法组成:

- 密钥生成算法 $\mathsf{KGen}(1^\lambda)$, 该算法输入安全参数 λ, 输出公私钥对 $(\mathsf{pk},\mathsf{sk})$;
- 加密算法 $\mathsf{Enc}(\mathsf{pk},M)$, 该算法输入公钥 pk 和明文 $M\in\mathcal{M}$, 输出密文 $\zeta\in\mathcal{CT}$;
- 解密算法 $\mathsf{Dec}(\mathsf{sk},\zeta)$, 该算法输入私钥 sk 和密文 ζ, 输出明文 M,

其中集合 $\mathcal{M}$ 和 $\mathcal{CT}$ 分别表示明文空间和密文空间.

$\mathsf{KGen}(1^\lambda)$	$\mathsf{Enc}(\mathsf{pk}, M \in \{0,1\}^\ell)$	$\mathsf{Dec}(\mathsf{sk}, \zeta)$
$d_B \leftarrow_\$ [1, n-1]$	$k \leftarrow_\$ [1, n-1]$	$(x_2, y_2) \leftarrow [d_B]\zeta_1$
$P_B \leftarrow [d_B]P$	$\zeta_1 \leftarrow [k]P$	$klen \leftarrow \lvert\zeta_2\rvert$
$\mathsf{sk} \leftarrow d_B$	$(x_2, y_2) \leftarrow [k]P_B$	$t \leftarrow \mathsf{KDF}(x_2 \lvert\lvert y_2, klen)$
$\mathsf{pk} \leftarrow P_B$	$klen \leftarrow \lvert M\rvert$	$M' \leftarrow \zeta_2 \oplus t$
return $(\mathsf{pk}, \mathsf{sk})$	$t \leftarrow \mathsf{KDF}(x_2 \lvert\lvert y_2, klen)$	$u \leftarrow H(x_2 \lvert\lvert M' \lvert\lvert y_2)$
	$\zeta_2 \leftarrow M \oplus t$	**if** $u \neq \zeta_3$ **then**
	$\zeta_3 \leftarrow H(x_2 \lvert\lvert M \lvert\lvert y_2)$	**return** $\perp$
	$\zeta = \zeta_1 \lvert\lvert \zeta_2 \lvert\lvert \zeta_3$	**return** M'
	return ζ	

图 1 SM2 公钥加密方案

Figure 1 SM2 public key encryption

公钥加密方案 Π 需要满足如下正确性: 对于任意 $(\mathsf{pk}, \mathsf{sk}) \leftarrow_\$ \mathsf{KGen}(1^\lambda)$, $M \leftarrow_\$ \mathcal{M}$, 以下公式成立:

$$\Pr\left[\mathsf{Dec}(\mathsf{sk}, \zeta) \neq M : \zeta \leftarrow_\$ \mathsf{Enc}(\mathsf{pk}, M)\right] \leqslant \mathsf{negl}(\lambda).$$

定义2 (可重随机公钥加密方案) 令 $\Pi = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ 为一个公钥加密方案. 当方案 Π 满足以下两个条件时, 我们称该公钥加密方案是可重随机的.

(1) 存在概率多项式时间算法 Rerand. 该算法输入公钥 pk 和密文 ζ, 输出新密文 ζ';

(2) 对于任意 $(\mathsf{pk}, \mathsf{sk}) \leftarrow_\$ \mathsf{KGen}(1^\lambda)$, $\zeta \leftarrow_\$ \mathcal{CT}$, 以下公式成立:

$$\Pr\left[\mathsf{Dec}(\mathsf{sk}, \zeta) \neq \mathsf{Dec}(\mathsf{sk}, \zeta') : \zeta' \leftarrow_\$ \mathsf{Rerand}(\mathsf{pk}, \zeta)\right] \leqslant \mathsf{negl}(\lambda).$$

若对于任意 $(\mathsf{pk}, \mathsf{sk}) \leftarrow_\$ \mathsf{KGen}(1^\lambda)$, $M \leftarrow_\$ \mathcal{M}$, $\zeta \leftarrow_\$ \mathsf{Enc}(\mathsf{pk}, M)$, 算法 $\mathsf{Rerand}(\mathsf{pk}, \zeta)$ 和 $\mathsf{Enc}(\mathsf{pk}, M)$ 输出密文的分布相同, 那么 Π 是完美可重随机的.

SM2 公钥加密方案如图 1 所示, 其中 P 为具有素数阶 n 的椭圆曲线循环群中随机选取的生成元, KDF 为输入字符串 S 和整数 ℓ 输出比特长度为 ℓ 的字符串的密钥派生函数, H 为密码杂凑函数.

2.3 单向陷门函数

定义3 (单向陷门函数) 令 $f : E \times R \to F$ 为一个陷门函数. 若对于任意概率多项式时间敌手 $\mathcal{A}$, 以下优势是可忽略的, 则函数 f 满足单向性:

$$\mathsf{Adv}_f^{\mathsf{ow}}(1^\lambda) = \Pr\left[\mathcal{A}^{\mathsf{Same}_f}(y) = x : x \leftarrow_\$ E, w \leftarrow_\$ R, y = f(x, w)\right],$$

其中 $\mathsf{Same}_f(y, y')$ 是一个判断 $f^{-1}(y) = f^{-1}(y')$ 是否成立的预言机.

2.4 困难性假设

定义4 (gap Diffie-Hellman (GDH) 困难性假设 [20]) 令 λ 为安全参数, $\mathbb{G}$ 为一个具有素数阶 p 的循环群, g 为群 $\mathbb{G}$ 的任意生成元. 若 GDH 困难性假设在群 $\mathbb{G}$ 上成立, 则对于任意概率多项式时间敌手 $\mathcal{A}$, 以下公式成立:

$$\Pr\left[\mathcal{A}^{\mathsf{DDH}}(g, g^a, g^b) = g^{ab} : a, b \leftarrow_{\$} \mathbb{Z}_p\right] \leqslant \mathsf{negl}(\lambda),$$

其中预言机 DDH 以任意四元组 (g, g^a, g^b, h) 为输入, 若 $h = g^{ab}$, 则返回 1; 否则, 返回 0.

2.5 安全性定义

定义5 (RCCA 安全性 [11]) 令 Π 为一个公钥加密方案. 对于任意概率多项式时间挑战者 $\mathcal{C}$ 和敌手 $\mathcal{A}$, 考虑如下 RCCA 安全游戏.

• 初始阶段: $\mathcal{C}$ 生成公私钥对 $(\mathsf{pk}, \mathsf{sk}) \leftarrow_{\$} \mathsf{KGen}(1^\lambda)$, 并将 pk 发送给 $\mathcal{A}$;

• 询问阶段 I: $\mathcal{A}$ 将密文 ζ 发送给 $\mathcal{C}$, $\mathcal{C}$ 返回 $\mathsf{Dec}(\mathsf{sk}, \zeta)$. $\mathcal{A}$ 可发起多项式次询问;

• 挑战阶段: $\mathcal{A}$ 选择两个长度相同的明文 M_0 和 M_1, 并发送给 $\mathcal{C}$. $\mathcal{C}$ 随机选择比特 b, 并将挑战密文 $\zeta^* \leftarrow_{\$} \mathsf{Enc}(\mathsf{pk}, M_b)$ 发送给 $\mathcal{A}$;

• 询问阶段 II: $\mathcal{A}$ 将密文 ζ 发送给 $\mathcal{C}$. 令 $M = \mathsf{Dec}(\mathsf{sk}, \zeta)$, 若 $M \in \{M_0, M_1\}$, $\mathcal{C}$ 返回 "`replay`"; 否则, 返回 M. $\mathcal{A}$ 可发起多项式次询问;

• 猜测阶段: $\mathcal{A}$ 输出猜测的比特 b'.

上述游戏中, 敌手 $\mathcal{A}$ 的优势为 $\mathsf{Adv}^{\mathsf{rcca}}_{\Pi}(1^\lambda) = |\Pr[b = b'] - 1/2|$. 若对于任意敌手 $\mathcal{A}$, 优势 $\mathsf{Adv}^{\mathsf{rcca}}_{\Pi}(1^\lambda)$ 均为可忽略的, 则方案 Π 是 RCCA 安全的.

3 基于 SM2 的 RCCA 安全可重随机公钥加密方案

3.1 具体方案

本文将 OAEP 三轮范式 [10] 应用于 SM2 公钥加密方案, 得到 RCCA 安全的可重随机公钥加密方案. 具体方案如图 2 所示, 其中 $\mathbb{G}$ 为一个具有素数阶 n 的椭圆曲线循环群, P 为 $\mathbb{G}$ 中随机选取的生成元, $\mathcal{F}, \mathcal{G}$ 和 $\mathcal{H}$ 为 3 个将 $\mathbb{G}$ 中元素映射到自身的双射.

3.2 正确性分析

解密正确性: 根据算法 Enc 和 Dec 的描述, 对于任意密文 $\zeta = (\zeta_1, \zeta_2, \zeta_3)$, 可得 $\zeta_2 - [d_B]\zeta_1 = ([w]P_B + U) - [d_B]([w]P) = U$ 以及 $\zeta_3 - [d_C]\zeta_1 = ([w]P_C + T) - [d_C]([w]P) = T$. 算法 Dec 中还原得到的 U, T 与算法 Enc 中的 U, T 相等. 因此, 算法 Dec 的解密结果, 即原明文 M.

重加密正确性: 根据算法 Dec 和 Rerand 的描述, 对于任意密文 ζ, 假设其底层随机数为 (R, w), 对其进行重加密操作得到的新密文 ζ' 的底层随机数为 $(R, w + w')$. 因此, 密文 ζ 和 ζ' 的解密结果相同.

3.3 安全性分析

在证明公钥加密方案 Π 的 RCCA 安全性之前, 构造陷门函数

$$f_{\mathsf{pk}}((M, M'), w) = (\zeta_1, \zeta_2, \zeta_3) = ([w]P, [w]P_B + M, [w]P_C + M'),$$

$\mathsf{KGen}(1^\lambda)$	$\mathsf{Enc}(\mathsf{pk}, M \in \mathbb{G})$	$\mathsf{Dec}(\mathsf{sk}, \zeta)$	$\mathsf{Rerand}(\mathsf{pk}, \zeta)$
$d_B \leftarrow_\$ [1, n-1]$	$R \leftarrow_\$ \mathbb{G}$	$U \leftarrow \zeta_2 - [d_B]\zeta_1$	$w' \leftarrow_\$ [1, n-1]$
$d_C \leftarrow_\$ [1, n-1]$	$S \leftarrow M + \mathcal{F}(R)$	$T \leftarrow \zeta_3 - [d_C]\zeta_1$	$\zeta_1' \leftarrow \zeta_1 + [w']P$
$P_B \leftarrow [d_B]P$	$T \leftarrow R + \mathcal{G}(S)$	$S \leftarrow U - \mathcal{H}(T)$	$\zeta_2' \leftarrow \zeta_2 + [w']P_B$
$P_C \leftarrow [d_C]P$	$U \leftarrow S + \mathcal{H}(T)$	$R \leftarrow T - \mathcal{G}(S)$	$\zeta_3' \leftarrow \zeta_3 + [w']P_C$
$\mathsf{sk} \leftarrow (d_B, d_C)$	$w \leftarrow_\$ [1, n-1]$	$M \leftarrow S - \mathcal{F}(R)$	$\zeta' \leftarrow (\zeta_1', \zeta_2', \zeta_3')$
$\mathsf{pk} \leftarrow (P_B, P_C)$	$\zeta_1 \leftarrow [w]P$	**return** M	**return** ζ'
return $(\mathsf{pk}, \mathsf{sk})$	$\zeta_2 \leftarrow [w]P_B + U$		
	$\zeta_3 \leftarrow [w]P_C + T$		
	$\zeta \leftarrow (\zeta_1, \zeta_2, \zeta_3)$		
	return ζ		

图 2 基于 SM2 的可重随机公钥加密方案

Figure 2 SM2-based rerandomizable public key encryption

其中 $\mathsf{pk} = (P_B, P_C) = ([d_B]P, [d_C]P)$, $M, M' \in \mathbb{G}$, $w \in [1, n-1]$, P 为群 $\mathbb{G}$ 中随机选取的生成元. 显然, 该函数是一个双射, 其反函数 $f_{\mathsf{pk}}^{-1}(\zeta_1, \zeta_2, \zeta_3) = (\zeta_2 - [d_B]\zeta_1, \zeta_3 - [d_C]\zeta_1)$. 下面证明陷门函数 f_{pk} 具有单向性.

定理1 若 GDH 困难性假设在群 $\mathbb{G}$ 上成立, 陷门函数 f_{pk} 具有单向性.

证明 考虑 GDH 困难性假设的变体如下: 对于任意概率多项式时间敌手 $\mathcal{A}$, 以下公式成立:

$$\Pr\left[\mathcal{A}^{\mathsf{DDH}}(g, g^a, g^b, g^c) = (g^{ab}, g^{ac}) : a, b, c \leftarrow_\$ \mathbb{Z}_p\right] \leqslant \mathsf{negl}(\lambda),$$

其中预言机 DDH 以任意六元组 $(g, g^b, g^c, g^a, h_1, h_2)$ 为输入, 若 $(h_1, h_2) = (g^{ab}, g^{ac})$, 则返回 1; 否则, 返回 0.

显然, 若 GDH 困难性假设在群 $\mathbb{G}$ 上成立, 上述变体也在群 $\mathbb{G}$ 上成立. 假设存在可以攻破函数 f_{pk} 单向性的敌手 $\mathcal{A}$, 那么可以构造解决上述困难性问题的敌手 $\mathcal{A}'$. 具体构造方案如下.

给定四元组 $(P, [a]P, [b]P, [c]P)$, 敌手 $\mathcal{A}'$ 随机选择 $R, R' \in \mathbb{G}$, 构造 $\zeta = (\zeta_1, \zeta_2, \zeta_3) = ([a]P, [b]P + R, [c]P + R')$ 并发送给 $\mathcal{A}$. 若敌手 $\mathcal{A}$ 发起询问 $\mathsf{Same}_{f_{\mathsf{pk}}}(\zeta, \zeta^*)$, 则敌手 $\mathcal{A}'$ 发起询问 $\mathsf{DDH}(P, P_B, P_C, \zeta_1 - \zeta_1^*, \zeta_2 - \zeta_2^*, \zeta_3 - \zeta_3^*)$. 如果 DDH 询问的结果为 1, 那么 $\mathsf{Same}_{f_{\mathsf{pk}}}$ 询问的结果则表明 $f_{\mathsf{pk}}^{-1}(\zeta) = f_{\mathsf{pk}}^{-1}(\zeta^*)$; 否则, $f_{\mathsf{pk}}^{-1}(\zeta) \neq f_{\mathsf{pk}}^{-1}(\zeta^*)$. 如果敌手 $\mathcal{A}$ 返回正确的 (M, M'), 那么 $(\zeta_2 - M, \zeta_3 - M')$ 即为 GDH 困难性问题变体的答案.

定理2 若 $\mathcal{A}$ 是一个攻击公钥加密方案 Π 在随机预言机模型下 RCCA 安全性的敌手, 在分别询问随机预言机 $\mathcal{F}$, $\mathcal{G}$, $\mathcal{H}$ 和解密预言机 $\mathcal{DO}$ q_f, q_g, q_h 和 q_d 次之后, 其优势 $\mathsf{Adv}_{\Pi}^{\mathsf{rcca}}(1^\lambda)$ 为 ϵ. 那么, 优势 $\mathsf{Adv}_{f_{\mathsf{pk}}}^{\mathsf{ow}}(1^\lambda)$ 的上界为

$$\frac{\epsilon}{2} - \frac{7q_d^2 + (4q_d + 1)(q_f + q_g) + q_d(q_f + 1)}{n},$$

其中 n 为群 $\mathbb{G}$ 的阶.

证明 考虑以下一系列游戏.

游戏 G_0: 即 RCCA 安全游戏. 挑战者 $\mathcal{C}$ 生成公私钥对 $(\mathsf{pk},\mathsf{sk})$, 并将公钥 pk 发送给敌手 $\mathcal{A}$. 随后, $\mathcal{A}$ 输出一对挑战明文 (M_0,M_1). $\mathcal{C}$ 选择随机比特 $b\in\{0,1\}$ 并计算挑战密文 $\zeta^*\leftarrow_{\$}\mathsf{Enc}(\mathsf{pk},M_b)$, 其中的随机数为 R^* 和 w^*. 在收到 ζ^* 之后, $\mathcal{A}$ 返回比特 b'. 如果 $b'=b$, 则 $\mathcal{A}$ 赢得游戏. 在整个游戏过程中, $\mathcal{A}$ 可以询问解密预言机 $\mathcal{DO}(\mathsf{sk},\cdot)$. 当解密结果等于 M_0 或者 M_1 时, 解密预言机输出 "`replay`". 同时, $\mathcal{A}$ 还可以询问 3 个随机预言机 $\mathcal{F}(\cdot)$, $\mathcal{G}(\cdot)$ 和 $\mathcal{H}(\cdot)$. 令 S_n 表示事件 $b'=b$ 在游戏 G_n 中发生, 可得

$$\Pr[S_0]=\frac{1}{2}+\mathsf{Adv}_{\Pi}^{\mathsf{rcca}}(1^{\lambda}).$$

游戏 G_1: 随机预言机 $\mathcal{F}(R)$, $\mathcal{G}(S)$, $\mathcal{H}(T)$ 和解密预言机 $\mathcal{DO}(\mathsf{sk},\zeta)$ 的模拟如图 3 所示, 其中挑战者 $\mathcal{C}$ 可以询问预言机 DDH 判断两个密文的底层明文是否相等. 显然, 该模拟是完美的, 可得

$$\Pr[S_1]=\Pr[S_0].$$

游戏 G_2: 该游戏与 G_1 的区别在于挑战密文 ζ^* 的生成. 该游戏中的挑战密文生成如下所示:

$$R^*\leftarrow_{\$}\mathbb{G};\ \boxed{F^+\leftarrow_{\$}\mathbb{G};\ S^*\leftarrow M_b+F^+;}\ T^*\leftarrow R^*+\mathcal{G}(S^*);\ U^*\leftarrow S^*+\mathcal{H}(T^*);$$
$$w^*\leftarrow_{\$}[1,n-1];\ \zeta^*\leftarrow([w^*]P,[w^*]P_B+U^*,[w^*]P_C+T^*).$$

游戏 G_2 与 G_1 等价, 除非 $\mathcal{A}$ 向 $\mathcal{F}$ 询问了 R^*. 将该事件在游戏 G_n 中发生表示为 QF_n, 可得

$$|\Pr[S_2]-\Pr[S_1]|\leqslant\Pr[\mathrm{QF}_2].$$

注意到 F^+ 仅在生成挑战密文 ζ^* 时被用到, 并且 $\mathcal{F}(R^*)\neq F^+$. 挑战密文 ζ^* 完美地隐藏了比特 b 的信息. 因此, $\mathcal{A}$ 在游戏 G_2 中的优势为 0, 即 $\Pr[S_2]=1/2$.

游戏 G_3: 该游戏中对解密预言机模拟的修改如图 4 所示.

引理1 $|\Pr[\mathrm{QF}_3]-\Pr[\mathrm{QF}_2]|\leqslant q_d(3q_d+2q_f+q_g)/n$.

证明 为了证明该引理, 我们考虑 G_2 和 G_3 之间的一系列游戏.

游戏 $\mathrm{G}_{2.1}$: 修改后的解密预言机模拟如图 5 所示. 在解密过程中, 随机预言机 $\mathcal{H}$ 未被询问. 在解密执行到行 21∼23 的情况下, $\mathcal{A}$ 没有在解密前向 $\mathcal{H}$ 询问 T, 但是有可能向 $\mathcal{G}$ 询问了 S. 因此, $\mathrm{G}_{2.1}$ 与 G_2 等价, 除非元组 $(S,\cdot)$ 已经存在于列表 $\mathcal{L}_{\mathcal{G}}$ 中. 由于 H 在 $\mathbb{G}$ 上随机均匀分布, $S=U-H$ 也是均匀分布的. S 已经被询问的概率为 $(q_d+q_g)/n$, 并且

$$|\Pr[\mathrm{QF}_{2.1}]-\Pr[\mathrm{QF}_2]|\leqslant q_d(q_d+q_g)/n.$$

游戏 $\mathrm{G}_{2.2}$: 修改后的解密预言机模拟如图 6 所示. $\mathrm{G}_{2.2}$ 与 $\mathrm{G}_{2.1}$ 等价, 除非元组 $(R,\cdot)$ 已经存在于列表 $\mathcal{L}_{\mathcal{F}}$ 中. 由于 G 是随机选取的, $R=T-G$ 在 $\mathbb{G}$ 上均匀分布. R 已经被询问的概率是 $(q_d+q_f)/n$, 并且

$$|\Pr[\mathrm{QF}_{2.2}]-\Pr[\mathrm{QF}_{2.1}]|\leqslant q_d(q_d+q_f)/n.$$

游戏 $\mathrm{G}_{2.3}$: 在图 7 中, 对解密预言机的修改只是形式上的. 游戏 $\mathrm{G}_{2.3}$ 等价于 $\mathrm{G}_{2.2}$. 因此,

$$\Pr[\mathrm{QF}_{2.3}]=\Pr[\mathrm{QF}_{2.2}].$$

游戏 $\mathrm{G}_{2.4}$: 修改后的解密预言机模拟如图 8 所示. $\mathrm{G}_{2.4}$ 与 $\mathrm{G}_{2.3}$ 等价, 除非元组 $(R,\cdot)$ 已经存在于列表 $\mathcal{L}_{\mathcal{F}}$ 中. 由于 G 是随机选取的, $R=T-G$ 在 $\mathbb{G}$ 中随机均匀分布. 因此, R 已经被询问的概率为 $(q_d+q_f)/n$ 并且

$$|\Pr[\mathrm{QF}_{2.4}]-\Pr[\mathrm{QF}_{2.3}]|\leqslant q_d(q_d+q_f)/n.$$

$\mathcal{F}(R)$

1 : **if** $\exists F : (R, F) \in \mathcal{L}_{\mathcal{F}}$:
2 : **return** F
3 : $F \leftarrow\!\!\$\ \mathbb{G}$
4 : $\mathcal{L}_{\mathcal{F}} \leftarrow \mathcal{L}_{\mathcal{F}} \cup \{(R, F)\}$
5 : **return** F

$\mathcal{G}(S)$

1 : **if** $\exists G : (S, G) \in \mathcal{L}_{\mathcal{G}}$:
2 : **return** G
3 : $G \leftarrow\!\!\$\ \mathbb{G}$
4 : $\mathcal{L}_{\mathcal{G}} \leftarrow \mathcal{L}_{\mathcal{G}} \cup \{(S, G)\}$
5 : **return** G

$\mathcal{H}(T)$

1 : **if** $\exists H : (T, H) \in \mathcal{L}_{\mathcal{H}}$:
2 : **return** H
3 : $H \leftarrow\!\!\$\ \mathbb{G}$
4 : $\mathcal{L}_{\mathcal{H}} \leftarrow \mathcal{L}_{\mathcal{H}} \cup \{(T, H)\}$
5 : **return** H

$\mathcal{DO}(\mathsf{sk}, \zeta)$

1 : **if** $\mathcal{A}$ has received ζ^* :
2 : **if** $\mathsf{DDH}(P, P_B, P_C, \zeta_1 - \zeta_1^*, \zeta_2 - \zeta_2^*, \zeta_3 - \zeta_3^*)$:
3 : **return replay**
4 : **for** $(M', \zeta') \in \mathcal{L}_{\mathcal{DO}}$:
5 : **if** $\mathsf{DDH}(P, P_B, P_C, \zeta_1 - \zeta_1', \zeta_2 - \zeta_2', \zeta_3 - \zeta_3')$:
6 : **return** M'
7 : $U \leftarrow \zeta_2 - [d_B]\zeta_1$
8 : $T \leftarrow \zeta_3 - [d_C]\zeta_1$
9 : **if** $\exists H : (T, H) \in \mathcal{L}_{\mathcal{H}}$:
10 : $S \leftarrow U - H$
11 : **if** $\exists G : (S, G) \in \mathcal{L}_{\mathcal{G}}$:
12 : $R \leftarrow T - G$
13 : **if** $\exists F : (R, F) \in \mathcal{L}_{\mathcal{F}}$:
14 : $M \leftarrow S - F$
15 : **else**
16 : $F \leftarrow \mathcal{F}(R);\ M \leftarrow S - F$
17 : **else**
18 : $G \leftarrow \mathcal{G}(S);\ R \leftarrow T - G$
19 : $F \leftarrow \mathcal{F}(R);\ M \leftarrow S - F$
20 : **else**
21 : $H \leftarrow \mathcal{H}(T);\ S \leftarrow U - H$
22 : $G \leftarrow \mathcal{G}(S);\ R \leftarrow T - G$
23 : $F \leftarrow \mathcal{F}(R);\ M \leftarrow S - F$
24 : **if** $M \in \{M_0, M_1\}$:
25 : **return replay**
26 : $\mathcal{L}_{\mathcal{DO}} \leftarrow \mathcal{L}_{\mathcal{DO}} \cup \{(M, \zeta)\}$
27 : **return** M

图 3　游戏 G_1 中预言机的模拟

Figure 3　Simulation of oracles in game G_1

游戏 $\mathrm{G}_{2.5}$: 图 9 中的修改只是形式上的变化. $\mathrm{G}_{2.5}$ 与 $\mathrm{G}_{2.4}$ 等价. 因此,

$$\Pr\left[\mathrm{QF}_{2.5}\right] = \Pr\left[\mathrm{QF}_{2.4}\right].$$

游戏 $\mathrm{G}_{2.6}$: 图 10 中的修改只是形式上的变化. $\mathrm{G}_{2.6}$ 与 $\mathrm{G}_{2.5}$ 等价. 因此,

$$\Pr\left[\mathrm{QF}_{2.6}\right] = \Pr\left[\mathrm{QF}_{2.5}\right].$$

G_3 等价于 $\mathrm{G}_{2.6}$. 该引理由此得证.

游戏 G_4: 该游戏对解密预言机和随机预言机 $\mathcal{G}$ 模拟的修改如图 11 所示. 游戏 G_4 与 G_3 等价, 除非 $\mathcal{A}$ 在向 $\mathcal{G}$ 询问 S 之前就已经向 $\mathcal{F}$ 询问了 R. 我们将该事件记为 QRbS_4. 事实上, 如果 $\mathcal{A}$ 询问 R

$\mathcal{DO}(\mathsf{sk},\zeta)$

The same as $\mathcal{DO}(\mathsf{sk},\zeta)$ in Figure 2 except that following lines are modified

Line 16 $\Rightarrow$ $M \leftarrow_{\$} \mathbb{G}$; $F \leftarrow S - M$; $\mathcal{L}_{\mathcal{F}} \leftarrow \mathcal{L}_{\mathcal{F}} \cup \{(R,F)\}$

Line 18-19 $\Rightarrow$ $M \leftarrow_{\$} \mathbb{G}$; $G \leftarrow_{\$} \mathbb{G}$; $R \leftarrow T - G$; $F \leftarrow S - M$;
$\mathcal{L}_{\mathcal{F}} \leftarrow \mathcal{L}_{\mathcal{F}} \cup \{(R,F)\}$; $\mathcal{L}_{\mathcal{G}} \leftarrow \mathcal{L}_{\mathcal{G}} \cup \{(S,G)\}$

Line 21-23 $\Rightarrow$ $M \leftarrow_{\$} \mathbb{G}$; $G \leftarrow_{\$} \mathbb{G}$; $H \leftarrow_{\$} \mathbb{G}$; $S \leftarrow U - H$; $R \leftarrow T - G$; $F \leftarrow S - M$;
$\mathcal{L}_{\mathcal{F}} \leftarrow \mathcal{L}_{\mathcal{F}} \cup \{(R,F)\}$; $\mathcal{L}_{\mathcal{G}} \leftarrow \mathcal{L}_{\mathcal{G}} \cup \{(S,G)\}$; $\mathcal{L}_{\mathcal{H}} \leftarrow \mathcal{L}_{\mathcal{H}} \cup \{(T,H)\}$

图 4 游戏 G_3 中解密预言机的模拟

Figure 4 Simulation of the decryption oracle in game G_3

$\mathcal{DO}(\mathsf{sk},\zeta)$

The same as $\mathcal{DO}(\mathsf{sk},\zeta)$ in Figure 2 except that following lines are modified

Line 21-23 $\Rightarrow$ $G \leftarrow_{\$} \mathbb{G}$; $H \leftarrow_{\$} \mathbb{G}$; $S \leftarrow U - H$; $R \leftarrow T - G$; $F \leftarrow \mathcal{F}(R)$; $M \leftarrow S - F$
$\mathcal{L}_{\mathcal{G}} \leftarrow \mathcal{L}_{\mathcal{G}} \cup \{(S,G)\}$; $\mathcal{L}_{\mathcal{H}} \leftarrow \mathcal{L}_{\mathcal{H}} \cup \{(T,H)\}$

图 5 游戏 $\mathrm{G}_{2.1}$ 中解密预言机的模拟

Figure 5 Simulation of the decryption oracle in game $\mathrm{G}_{2.1}$

$\mathcal{DO}(\mathsf{sk},\zeta)$

The same as $\mathcal{DO}(\mathsf{sk},\zeta)$ in Figure 2 except that following lines are modified

Line 21-23 $\Rightarrow$ $G \leftarrow_{\$} \mathbb{G}$; $H \leftarrow_{\$} \mathbb{G}$; $S \leftarrow U - H$; $R \leftarrow T - G$; $\boxed{F \leftarrow_{\$} \mathbb{G}}$; $M \leftarrow S - F$
$\boxed{\mathcal{L}_{\mathcal{F}} \leftarrow \mathcal{L}_{\mathcal{F}} \cup \{(R,F)\}}$; $\mathcal{L}_{\mathcal{G}} \leftarrow \mathcal{L}_{\mathcal{G}} \cup \{(S,G)\}$; $\mathcal{L}_{\mathcal{H}} \leftarrow \mathcal{L}_{\mathcal{H}} \cup \{(T,H)\}$

图 6 游戏 $\mathrm{G}_{2.2}$ 中解密预言机的模拟

Figure 6 Simulation of the decryption oracle in game $\mathrm{G}_{2.2}$

$\mathcal{DO}(\mathsf{sk},\zeta)$

The same as $\mathcal{DO}(\mathsf{sk},\zeta)$ in Figure 2 except that following lines are modified

Line 21-23 $\Rightarrow$ $G \leftarrow_{\$} \mathbb{G}$; $H \leftarrow_{\$} \mathbb{G}$; $S \leftarrow U - H$; $R \leftarrow T - G$; $\boxed{M \leftarrow_{\$} \mathbb{G};\ F \leftarrow S - M}$
$\mathcal{L}_{\mathcal{F}} \leftarrow \mathcal{L}_{\mathcal{F}} \cup \{(R,F)\}$; $\mathcal{L}_{\mathcal{G}} \leftarrow \mathcal{L}_{\mathcal{G}} \cup \{(S,G)\}$; $\mathcal{L}_{\mathcal{H}} \leftarrow \mathcal{L}_{\mathcal{H}} \cup \{(T,H)\}$

图 7 游戏 $\mathrm{G}_{2.3}$ 中解密预言机的模拟

Figure 7 Simulation of the decryption oracle in game $\mathrm{G}_{2.3}$

发生在其询问 S 之后, 那么, 根据图 11 中随机预言机 $\mathcal{G}(S)$ 的模拟, 在询问 S 时, 我们可以从列表 $\mathcal{L}_{\mathcal{H}}$ 中找到元组 (T,H) 并且以确保一致性的方式计算元组 (R,F).

对每个密文 ζ 而言, 其底层的 T,H 和 S 均不相同. 因此, 对于每次解密询问, $\mathcal{G}(S)$ 中新增的行最多被执行一次. 在 S 被询问之前, G 是均匀分布的. R 也是如此. 因此, $\mathcal{A}$ 向 $\mathcal{F}$ 询问 R 的概率为 q_f/n,

$\mathcal{DO}(\mathsf{sk},\zeta)$

The same as $\mathcal{DO}(\mathsf{sk},\zeta)$ in Figure 6 except that following lines are modified

Line 18-19 $\Rightarrow$ $G \leftarrow_{\$} \mathbb{G}$; $F \leftarrow_{\$} \mathbb{G}$; $R \leftarrow T - G$; $M \leftarrow S - F$

$\mathcal{L}_{\mathcal{F}} \leftarrow \mathcal{L}_{\mathcal{F}} \cup \{(R,F)\}$; $\mathcal{L}_{\mathcal{G}} \leftarrow \mathcal{L}_{\mathcal{G}} \cup \{(S,G)\}$

图 8 游戏 $\mathrm{G}_{2.4}$ 中解密预言机的模拟

Figure 8 Simulation of the decryption oracle in game $\mathrm{G}_{2.4}$

$\mathcal{DO}(\mathsf{sk},\zeta)$

The same as $\mathcal{DO}(\mathsf{sk},\zeta)$ in Figure 6 except that following lines are modified

Line 18-19 $\Rightarrow$ $G \leftarrow_{\$} \mathbb{G}$; $\boxed{M \leftarrow_{\$} \mathbb{G}}$; $R \leftarrow T - G$; $\boxed{F \leftarrow S - M}$

$\mathcal{L}_{\mathcal{F}} \leftarrow \mathcal{L}_{\mathcal{F}} \cup \{(R,F)\}$; $\mathcal{L}_{\mathcal{G}} \leftarrow \mathcal{L}_{\mathcal{G}} \cup \{(S,G)\}$

图 9 游戏 $\mathrm{G}_{2.5}$ 中解密预言机的模拟

Figure 9 Simulation of the decryption oracle in game $\mathrm{G}_{2.5}$

$\mathcal{DO}(\mathsf{sk},\zeta)$

The same as $\mathcal{DO}(\mathsf{sk},\zeta)$ in Figure 8 except that following lines are modified

Line 16 $\Rightarrow$ $M \leftarrow_{\$} \mathbb{G}$; $F \leftarrow S - M$; $\mathcal{L}_{\mathcal{F}} \leftarrow \mathcal{L}_{\mathcal{F}} \cup \{(R,F)\}$

图 10 游戏 $\mathrm{G}_{2.6}$ 中解密预言机的模拟

Figure 10 Simulation of the decryption oracle in game $\mathrm{G}_{2.6}$

并且

$$\Pr[\mathrm{QRbS}_4] \leqslant q_d(q_d+q_f)/n.$$

修改解密预言机使得列表 $\mathcal{L}_{\mathcal{G}}$ 和 $\mathcal{L}_{\mathcal{F}}$ 中的一些元组 (S,G) 和 (R,F) 不存在了. 这会对本游戏中后续的解密询问以及事件 QF 产生一些影响.

- 如果元组 $(R^*,\cdot)$ 不在列表中, 那么事件 QF_4 不会发生. 由于 $R = T - G$ 以及 G 是随机选取的, $R = R^*$ 的概率为 $1/n$;
- 在后续解密询问 ζ' 的模拟中, 如果其底层的 $S' = S$, 那么在游戏 G_3 中元组 (S,G) 可以从列表中被找到, 但是在游戏 G_4 中, 元组 (S,G) 就找不到了. 在 G_3 中, G 的值在第一次解密时就被确定了, 并且未在后续过程中公开. 因此, $R' = T' - G' = T' - G$ 在列表 $\mathcal{L}_{\mathcal{F}}$ 中的概率为 $(q_d+q_f)/n$. 如果 R' 不在列表 $\mathcal{L}_{\mathcal{F}}$ 中, M' 一直都是随机的.

$$\begin{aligned}|\Pr[\mathrm{QF}_4] - \Pr[\mathrm{QF}_3]| &\leqslant \Pr[\mathrm{QRbS}_4] + q_d(q_d+q_f+1)/n\\ &\leqslant q_d(2q_d+2q_f+1)/n.\end{aligned}$$

游戏 G_5: 修改后的解密预言机模拟如图 12 所示.

对解密预言机的修改使得列表 $\mathcal{L}_{\mathcal{H}}$ 发生了改变. 因此, G_5 在以下情况中与 G_4 不同:

$\mathcal{DO}(\mathsf{sk}, \zeta)$

The same as $\mathcal{DO}(\mathsf{sk}, \zeta)$ in Figure 3 except that following lines are modified

Line 18-19 $\Rightarrow$ $M \leftarrow_{\$} \mathbb{G}$

Line 21-23 $\Rightarrow$ $M \leftarrow_{\$} \mathbb{G}$; $H \leftarrow_{\$} \mathbb{G}$; $\mathcal{L}_{\mathcal{H}} \leftarrow \mathcal{L}_{\mathcal{H}} \cup \{(T, H)\}$

$\mathcal{G}(S)$

The same as $\mathcal{G}(S)$ in Figure 2 except that following lines are added before Line 5

for $(T, H) \in \mathcal{L}_{\mathcal{H}}$:

  for $(M, \zeta) \in \mathcal{L}_{\mathcal{DO}}$:

    $w \leftarrow_{\$} [1, n-1]$; $(\zeta_1', \zeta_2', \zeta_3') \leftarrow ([w]P, [w]P_B + (S+H), [w]P_C + T)$

    if $\mathsf{DDH}(P, P_B, P_C, \zeta_1 - \zeta_1', \zeta_2 - \zeta_2', \zeta_3 - \zeta_3')$:

      $R \leftarrow T - G$; $F \leftarrow S - M$; $\mathcal{L}_{\mathcal{F}} \leftarrow \mathcal{L}_{\mathcal{F}} \cup \{(R, F)\}$

图 11 游戏 G_4 中解密预言机和随机预言机 $\mathcal{G}$ 的模拟

Figure 11 Simulation of the decryption oracle and random oracle $\mathcal{G}$ in game G_4

$\mathcal{DO}(\mathsf{sk}, \zeta)$

The same as $\mathcal{DO}(\mathsf{sk}, \zeta)$ in Figure 10 except that following lines are modified

Line 21-23 $\Rightarrow$ $M \leftarrow_{\$} \mathbb{G}$

图 12 游戏 G_5 中解密预言机的模拟

Figure 12 Simulation of the decryption oracle in game G_5

- 向 $\mathcal{G}$ 询问 S 早于向 $\mathcal{H}$ 询问 T (记为 QSbT_5). 在这种情况下, 随机预言机 $\mathcal{G}$ 中新增的行不会被执行. 注意到, 在 T 被询问之前, H 和 $S = U - H$ 都是均匀分布的. 因此, S 已经被询问的概率是 q_g/n 并且

$$\Pr[\mathrm{QSbT}_5] \leqslant q_d q_g / n.$$

- 移除元组 (T, H) 可能影响后续解密询问 ζ' 的结果.
- S' 存在于列表 $\mathcal{L}_{\mathcal{G}}$ 中并且 $T' = T$. 在游戏 G_4 中, $H' = H$ 的值在第一次解密时就被确定了, 但在后续过程中未公开. 因此, $S' = U' - H'$ 存在于列表 $\mathcal{L}_{\mathcal{G}}$ 的概率小于 q_g/n.
- S' 不存在于列表 $\mathcal{L}_{\mathcal{G}}$ 中并且 $T' = T$. 在该情况下, 解密结果都是随机的明文并且没有向列表中加入新的元组.

$$|\Pr[\mathrm{QF}_5] - \Pr[\mathrm{QF}_4]| \leqslant \Pr[\mathrm{QSbT}_5] + q_d q_g / n \leqslant 2 q_d q_g / n.$$

此时, 列表 $\mathcal{L}_{\mathcal{G}}$ 和 $\mathcal{L}_{\mathcal{H}}$ 中只包含 $\mathcal{A}$ 询问以及生成挑战密文 ζ^* 产生的元组. 解密预言机模拟的过程中仅产生 $\mathcal{L}_{\mathcal{F}}$ 中的元组. 我们将 $\mathcal{A}$ 询问 S^* (T^*) 记为 QGA_5 (QHA_5). 令 $\mathrm{QGHA}_5 = \mathrm{QGA}_5 \wedge \mathrm{QHA}_5$.

游戏 G_6: 增加如下规则, 一旦规则被触发, 游戏中止执行并输出随机比特.

- $\mathrm{QGA}_6 \wedge \neg \mathrm{QHA}_6$ 在游戏结束前.

当 QHA_6 不发生, $\mathcal{H}(T^*) = U^* - (M_b + F^+)$ 的值未知时. 由于 F^+ 对 $\mathcal{A}$ 来说是均匀分布的, $\mathcal{H}(T^*)$ 以及 $S^* = U^* - \mathcal{H}(T^*)$ 同样也是均匀分布的, 因此, S^* 被询问的概率是 q_g/n, 这条规则被触发的概率

为 q_g/n.

$$|\Pr[\mathrm{QF}_6]-\Pr[\mathrm{QF}_5]|\leqslant q_g/n.$$

引理2 $\Pr[\mathrm{QF}_6]\leqslant q_f/n+\Pr[\mathrm{QGHA}_6]$.

证明 考虑以下游戏.

游戏 $\mathrm{G}_{6.1}$: 游戏中止执行的规则为

- $\mathrm{QGA}_{6.1}$ 在游戏结束前.

$$\Pr[\mathrm{QF}_{6.1}]=\Pr[\mathrm{QF}_6\wedge\neg\mathrm{QGA}_6].$$

游戏 $\mathrm{G}_{6.2}$: 如下修改挑战密文的生成方式:

$$\begin{aligned}&R^*\leftarrow_{\$}\mathbb{G};\ S^*\leftarrow_{\$}\mathbb{G};\ G^*\leftarrow_{\$}\mathbb{G},\\&F^*\leftarrow S^*-M_b;\ T^*\leftarrow R^*+G^*;\ U^*\leftarrow S^*+\mathcal{H}(T^*).\end{aligned}$$

该游戏与 $\mathrm{G}_{6.1}$ 等价, 除非 $\mathcal{A}$ 向 $\mathcal{G}$ 询问了 S^*. 然而, 这一事件已经在 $\mathrm{G}_{6.1}$ 中被排除了, 并且解密预言机不会询问 $\mathcal{G}$. 因此,

$$\Pr[\mathrm{QF}_{6.2}]=\Pr[\mathrm{QF}_{6.1}].$$

同时, 由于 G^* 的值是不会公开的, $R^*=T^*-G^*$ 在 $\mathcal{A}$ 看来是均匀分布的.

$$\Pr[\mathrm{QF}_{6.2}]=q_f/n.$$

结合上述等式, 可得

$$\begin{aligned}\Pr[\mathrm{QF}_6]&=\Pr[\mathrm{QF}_6\wedge\neg\mathrm{QGA}_6]+\Pr[\mathrm{QF}_6\wedge\mathrm{QGA}_6\wedge\neg\mathrm{QHA}_6]\\&\quad+\Pr[\mathrm{QF}_6\wedge\mathrm{QGHA}_6]\\&\leqslant\Pr[\mathrm{QF}_{6.1}]+\Pr[\mathrm{QGA}_6\wedge\neg\mathrm{QHA}_6]+\Pr[\mathrm{QGHA}_6]\\&\leqslant\Pr[\mathrm{QF}_{6.2}]+0+\Pr[\mathrm{QGHA}_6]\\&\leqslant q_f/n+\Pr[\mathrm{QGHA}_6],\end{aligned}$$

该引理由此得证.

游戏 G_7: 该游戏中止执行的规则如下.

- $\mathrm{QGA}_7\wedge\neg\mathrm{QHA}_7$ 在游戏结束前.
- 解密预言机中行 14 或者行 16 已经被执行并且 $T=T^*$, 但 $\mathcal{A}$ 还没有向 $\mathcal{H}$ 询问 T^*.
- 解密预言机中行 14 已经被执行并且 $S=S^*$, 但 $\mathcal{A}$ 还没有向 $\mathcal{G}$ 询问 S^*.

引理3 $|\Pr[\mathrm{QGHA}_7]-\Pr[\mathrm{QGHA}_6]|\leqslant q_d(q_f+q_d+q_g)/n$.

证明 我们重用之前引理中游戏 $\mathrm{G}_{6.1}$ 和 $\mathrm{G}_{6.2}$ 编号, 从 G_6 开始重新考虑以下游戏.

游戏 $\mathrm{G}_{6.1}$: 该游戏中止执行的规则如下.

- $\mathrm{QGA}_{6.1}\wedge\neg\mathrm{QHA}_{6.1}$ 在游戏结束前.
- 解密预言机中行 14 或者行 16 已经被执行并且 $T=T^*$, 但 $\mathcal{A}$ 还没有向 $\mathcal{H}$ 询问 T^*.

在 $\mathcal{A}$ 询问 $\mathcal{H}(T^*)$ 之前, $\mathcal{H}(T)=\mathcal{H}(T^*)=U^*-(M_b+F^+)$ 未曾被公开. F^+ 在 $\mathcal{A}$ 看来是均匀分布的. 因此, $\mathcal{H}(T)$ 和 $S=U-\mathcal{H}(T^*)$ 在 $\mathcal{A}$ 看来是随机的. 由于加密方案的单向性, $T=T^*$ 以及我们已经在

$\mathcal{DO}(\mathsf{sk}, \zeta)$

The same as $\mathcal{DO}(\mathsf{sk}, \zeta)$ in Figure 11 except that following lines are modified

Line 16 $\Rightarrow$ **if** $S = S^* \wedge S^*$ has not been asked by $\mathcal{A}$ **then** $M \leftarrow_\$ \mathbb{G}$

else $M \leftarrow_\$ \mathbb{G}$; $F \leftarrow S - M$; $\mathcal{L}_\mathcal{F} \leftarrow \mathcal{L}_\mathcal{F} \cup \{(R, F)\}$

图 13 游戏 G_8 中解密预言机的模拟

Figure 13 Simulation of the decryption oracle in game G_8

解密的初始阶段就已经对和挑战密文 ζ^* 具有相同 (U^*, T^*) 的密文进行了处理, 因此, S 一定是不等于 S^* 的. 故 S 在 $\mathcal{L}_\mathcal{G}$ 中的概率小于 q_g/n.

$$|\Pr[\mathrm{QGHA}_{6.1}] - \Pr[\mathrm{QGHA}_6]| \leqslant q_d q_g / n.$$

游戏 $\mathrm{G}_{6.2}$: 该游戏中止执行的规则如下.

- $\mathrm{QGA}_{6.2} \wedge \neg\mathrm{QHA}_{6.2}$ 在游戏结束前.
- 解密预言机中行 14 或者行 16 已经被执行并且 $T = T^*$, 但 $\mathcal{A}$ 还没有向 $\mathcal{H}$ 询问 T^*.
- 解密预言机中行 14 已经被执行并且 $S = S^*$, 但 $\mathcal{A}$ 还没有向 $\mathcal{G}$ 询问 S^*.

由于 $\mathcal{A}$ 没有询问 $S = S^*$, $\mathcal{G}(S^*) = T^* - R^*$ 对 $\mathcal{A}$ 来说是随机的. 因此, $R = T - \mathcal{G}(S^*)$ 已经被 $\mathcal{A}$ 询问的概率是 $(q_d + q_f)/n$.

$$|\Pr[\mathrm{QGHA}_{6.2}] - \Pr[\mathrm{QGHA}_{6.1}]| \leqslant q_d(q_d + q_f)/n.$$

$\mathrm{G}_{6.2}$ 即 G_7. 该引理由此得证.

游戏 G_8: 如图 13 所示对解密预言机的模拟进行修改.

在解密过程中, 如果 $S = S^*$ 但 S^* 未被 $\mathcal{A}$ 询问, $F = \mathcal{F}(R)$ 是均匀分布的, 那么我们可以随机生成 M 作为解密的结果. 然而, 在该情况下, 我们不再保存元组 (R, F). 这可能会导致一些问题: 如果后续的解密询问 ζ' 的底层 $R' = R$, 那么 $T' - G' = T - G^*$. 因此, 如果 $S' = S$, 那么 $T' = T$ 以及 M' 应当等于 M. 这在解密过程中可以通过询问预言机 DDH 检测出来. 如果 $S' \neq S$, $G = \mathcal{G}(S) = G^*$ 与 G' 无关. 此外, S^* 未被询问, 由此 $R = T - G^*$ 是均匀分布的. 因此, 后续解密询问 ζ' 满足 $R' = R$ 的概率为 $1/n$.

$$|\Pr[\mathrm{QGHA}_8] - \Pr[\mathrm{QGHA}_7]| \leqslant q_d^2/n.$$

游戏 G_9: 在游戏 G_8 中, 解密预言机没有使用生成挑战密文期间产生的向 $\mathcal{G}$ 和 $\mathcal{H}$ 的询问.

- 行 14:

(1) $R = R^*$: 如果 $\mathcal{A}$ 没有直接询问 R^*, 该情况不大可能发生. 因为在生成挑战密文 ζ^* 期间, R^* 未被询问;

(2) $S = S^*$: 该情况在 G_7 中被排除了;

(3) $T = T^*$: 该情况在 G_7 中被排除了;

- 行 16:

(1) $S = S^*$: 从游戏 G_8 开始, 与行 18 和 19 类似;

(2) $T = T^*$: 该情况在 G_7 中被排除了;

- 行 18 和 19:

$T = T^*$: 从游戏 G_5 开始, 与行 21~23 类似.

$\mathcal{DO}(\mathsf{sk}, \zeta)$

The same as $\mathcal{DO}(\mathsf{sk}, \zeta)$ in Figure 12 except that following lines are modified

Line 7-8 $\Rightarrow$

isFound $\leftarrow$ False

for $(T, H) \in \mathcal{L}_{\mathcal{H}}$:

  for $(S, G) \in \mathcal{L}_{\mathcal{G}}$:

    $w' \leftarrow_{\$} [1, n-1]$; $\zeta' \leftarrow ([w']P, [w']P_B + (S+H), [w']P_C + T)$

    if $\mathsf{DDH}(P, P_B, P_C, \zeta_1 - \zeta_1', \zeta_2 - \zeta_2', \zeta_3 - \zeta_3')$:

      isFound $\leftarrow$ True

      $U \leftarrow S + H$; $T \leftarrow T$

if $\neg$ isFound:

  $U \leftarrow \perp$; $T \leftarrow \perp$

图 14 游戏 G_9 中解密预言机的模拟

Figure 14 Simulation of the decryption oracle in game G_9

在该游戏中, 挑战密文的生成将不再询问 $\mathcal{G}$ 或者 $\mathcal{H}$:

$$R^* \leftarrow_{\$} \mathbb{G};\ F^* \leftarrow_{\$} \mathbb{G};\ G^* \leftarrow_{\$} \mathbb{G};\ H^* \leftarrow_{\$} \mathbb{G};$$
$$S^* \leftarrow M_b + F^*;\ T^* \leftarrow R^* + G^*;\ U^* \leftarrow S^* + H^*.$$

上述修改并不会对解密预言机的模拟以及随机预言机 $\mathcal{G}$ 中新增行的执行产生影响. 因为游戏 G_5 已经对该修改进行了考虑. 因此, 各种事件发生的概率不变. 接着, 如图 14 所示修改解密预言机.

当事件 QGHA_9 发生时, 列表 $\mathcal{L}_{\mathcal{G}}$ 和 $\mathcal{L}_{\mathcal{H}}$ 存在元组 (S, G) 和 (T, H) 使得布尔值 isFound 为真. 此时, 我们可以还原 U^* 以及 T^*.

$$\Pr[\mathrm{QGHA}_9] \leqslant \mathsf{Adv}^{\mathsf{ow}}_{f_{\mathsf{pk}}}(1^\lambda),$$

定理由此得证.

4 结论

本文提出了首个基于 SM2 加密算法的 RCCA 安全公钥加密方案. 该方案具有密文可重随机性, 因此可以支持密码逆向防火墙对密文进行合法修改, 达到抵抗算法替换攻击的安全性, 进一步增强国密算法在保障我国网络信息系统自主可控上的功能. 本文证明了所提出的加密方案在随机预言机模型下具有 RCCA 安全性, 未来可以考虑如何在标准模型下基于 SM2 加密算法构造具有 RCCA 安全的公钥加密方案.

参考文献

1 Goldwasser S, Micali S. Probabilistic encryption. J Comput Syst Sci, 1984, 28: 270–299

2 Bellare M, Paterson K G, Rogaway P. Security of symmetric encryption against mass surveillance. In: Proceedings of International Cryptology Conference, 2014. 1–19

3 Young A, Yung M. Kleptography: using cryptography against cryptography. In: Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, 1997. 62–74
4 Lai J C, Huang X Y, He D B, et al. Security analysis of SM9 digital signature and key encapsulation. Sci Sin Inform, 2021, 51: 1900–1913 [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]
5 Chen B W, Xiang T, He D B, et al. An efficient public-key broadcast encryption scheme based on SM2. Sci Sin Inform, 2022, 52: 2321–2335 [陈泌文, 向涛, 何德彪, 等. 基于国产密码 SM2 的实用公钥广播加密方案. 中国科学: 信息科学, 2022, 52: 2321–2335]
6 Huang X Y, Chen R M, Wang Y, et al. Key exfiltration on SM2 cryptographic algorithms. J Cryptol Res, 2021, 8: 684–698 [黄欣沂, 陈荣茂, 王毅, 等. SM2 密码算法密钥渗漏分析. 密码学报, 2021, 8: 684–698]
7 Mironov I, Stephens-Davidowitz N. Cryptographic reverse firewalls. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2015. 657–686
8 Russell A, Tang Q, Yung M, et al. Cliptography: clipping the power of kleptographic attacks. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, 2016. 34–64
9 Dodis Y, Mironov I, Stephens-Davidowitz N. Message transmission with reverse firewalls—secure communication on corrupted machines. In: Proceedings of Annual International Cryptology Conference, 2016. 341–372
10 Phan D H, Pointcheval D. OAEP 3-round: a generic and secure asymmetric encryption padding. In: Proceedings of the 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, 2004. 63–77
11 Canetti R, Krawczyk H, Nielsen J B. Relaxing chosen-ciphertext security. In: Proceedings of the 23rd Annual International Cryptology Conference, Santa Barbara, 2003. 565–582
12 Groth J. Rerandomizable and replayable adaptive chosen ciphertext attack secure cryptosystems. In: Proceedings of the 1st Theory of Cryptography Conference, 2004. 152–170
13 Prabhakaran M, Rosulek M. Rerandomizable RCCA encryption. In: Proceedings of the 27th Annual International Cryptology Conference on Advances in Cryptology, 2007. 517–534
14 Wang Y, Chen R M, Yang G M, et al. Receiver-anonymity in rerandomizable RCCA-secure cryptosystems resolved. In: Proceedings of the 41st Annual International Cryptology Conference, 2021. 270–300
15 Chase M, Kohlweiss M, Lysyanskaya A, et al. Malleable proof systems and applications. In: Proceedings of the 31st Annual international conference on Theory and Applications of Cryptographic Techniques, 2012. 281–300
16 Libert B, Peters T, Qian C. Structure-preserving chosen-ciphertext security with shorter verifiable ciphertexts. In: Proceedings of International Workshop on Public Key Cryptography, 2017. 247–276
17 Faonio A, Fiore D, Herranz J, et al. Structure-preserving and rerandomizable RCCA-secure public key encryption and its applications. In: Proceedings of the 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, 2019. 159–190
18 Faonio A, Fiore D. Improving the efficiency of re-randomizable and replayable CCA secure public key encryption. In: Proceedings of Applied Cryptography and Network Security, 2020. 271–291
19 Wang Y, Chen R M, Huang X Y, et al. Identity-based encryption for fair anonymity applications: defining, implementing, and applying rerandomizable RCCA-secure IBE. In: Proceeding of the 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, 2021. 427–455
20 Okamoto T, Pointcheval D. The gap-problems: a new class of problems for the security of cryptographic schemes. In: Proceedings of PKC 2001, 2001. 104–118

RCCA-secure public-key encryption based on SM2

Rongmao CHEN[1], Yi WANG[1] & Xinyi HUANG[2*]

1. *School of Computer, National University of Defense Technology, Changsha* 410073*, China*;
2. *Artificial Intelligence Thrust, Information Hub, Hong Kong University of Science and Technology* (*Guangzhou*)*, Guangzhou* 511466*, China*
* Corresponding author. E-mail: xinyi@ust.hk

Abstract SM2 cryptographic algorithms have become vital in achieving independently controllable security for national networks and information systems. However, recent studies have shown that in a real-world implementation, the SM2 encryption algorithm might suffer from effective algorithm substitution attacks, which enable attackers to obtain the randomness used in the next-round encryption from the current ciphertext, and thus could decrypt all the successive ciphertexts without a decryption key. A cryptographic reverse firewall has been considered a useful tool to defend against such an attack by rerandomizing a ciphertext, which, however, is incompatible with the CCA security of the SM2 encryption algorithm. To tackle this problem, this work improves the SM2 encryption algorithm for Replayable-CCA (RCCA) security, which could offer a similar security guarantee as CCA while supporting ciphertext rerandomizability for using cryptographic reverse firewalls. The core idea is to apply the OAEP three-round design paradigm by Phan et al. to the context of the SM2 encryption algorithm and rigorously prove its RCCA security in the random oracle model. The proposed scheme is the first rerandomizable RCCA-secure public-key encryption scheme based on SM serial algorithms and could help enhance the security of the SM2 encryption algorithm in real-world applications.

Keywords SM2, encryption, RCCA, rerandomizability, cryptographic reverse firewall