软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2023,34(7):3354−3364 [doi: 10.13328/j.cnki.jos.006531]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于 SM9 的 CCA 安全广播加密方案*

赖建昌[1], 黄欣沂[1], 何德彪[2], 宁建廷[1,3]

[1](福建省网络安全与密码技术重点实验室 (福建师范大学), 福建 福州 350007)
[2](空天信息安全与可信计算教育部重点实验室 (武汉大学), 湖北 武汉 430072)
[3](信息安全国家重点实验室 (中国科学院 信息工程研究所), 北京 100093)
通信作者: 黄欣沂, E-mail: xyhuang@fjnu.edu.cn

摘　要: 选择密文安全模型能有效刻画主动攻击, 更接近现实环境. 现有抵抗选择密文攻击的密码算法以国外算法为主, 缺乏我国自主设计且能抵抗选择密文攻击的密码算法. 虽然实现选择密文安全存在通用转化方法, 代价是同时增加计算开销和通信开销. 基于国密 SM9 标识加密算法, 提出一种具有选择密文安全的标识广播加密方案. 方案的设计继承了 SM9 标识加密算法结构, 用户密钥和密文的大小都是固定的, 其中用户密钥由一个群元素组成, 密文由 3 个元素组成, 与实际参与加密的接收者数量无关. 借助随机谕言器, 基于 GDDHE 困难问题可证明方案满足 CCA 安全. 加密算法的设计引入虚设标识, 通过该标识可成功回复密文解密询问, 实现 CCA 的安全性. 分析表明, 所提方案与现有高效标识广播加密方案在计算效率和存储效率上相当.

关键词: SM9; 广播加密; CCA 安全; 定长密文
中图法分类号: TP309

中文引用格式: 赖建昌, 黄欣沂, 何德彪, 宁建廷. 基于SM9的CCA安全广播加密方案. 软件学报, 2023, 34(7): 3354–3364. http://www.jos.org.cn/1000-9825/6531.htm
英文引用格式: Lai JC, Huang XY, He DB, Ning JT. CCA Secure Broadcast Encryption Based on SM9. Ruan Jian Xue Bao/Journal of Software, 2023, 34(7): 3354–3364 (in Chinese). http://www.jos.org.cn/1000-9825/6531.htm

CCA Secure Broadcast Encryption Based on SM9

LAI Jian-Chang[1], HUANG Xin-Yi[1], HE De-Biao[2], NING Jian-Ting[1,3]

[1](Fujian Provincial Key Lab of Network Security and Cryptology (Fujian Normal University), Fuzhou 350007, China)
[2](Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education (Wuhan University), Wuhan 430072, China)
[3](State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences), Beijing 100093, China)

Abstract: The chosen-ciphertext attack (CCA) security model can effectively figure active attacks in reality. The existing cryptosystems against CCA are mainly designed by foreign countries, and China is lack of its CCA secure cryptosystems. Although there are general transformation approaches to achieving CCA security, they lead to an increase in both computational overhead and communication overhead. Based on the SM9 encryption algorithm, this study proposes an identity-based broadcast encryption scheme with CCA security. The design is derived from the SM9, and the size of the private key and ciphertext is constant and independent of the number of receivers chosen in the data encryption phase. Specifically, the private key includes one element, and the ciphertext is composed of three elements. If the GDDHE assumption holds, the study proves that the proposed scheme has selective CCA security under the random oracle model. In order to achieve CCA security, a dummy identity is introduced in designing the encryption algorithm, and the identity can be used to

* 基金项目: 国家自然科学基金 (61902191, 62032005, 61972294, 61972094, 61932016); 江苏省自然科学基金 (BK20190696); 福建省科技厅科学基金 (2020J02016); 山东省重点研发计划 (2020CXGC010115)
收稿时间: 2021-06-21; 修改时间: 2021-10-01; 采用时间: 2021-11-08; jos 在线出版时间: 2022-09-20
CNKI 网络首发时间: 2022-12-01

© 中国科学院软件研究所 http://www.jos.org.cn

answer the decryption query successfully. Analysis shows that the proposed scheme is comparable to the existing efficient identity-based broadcast encryption schemes in terms of computational efficiency and storage efficiency.

Key words: SM9; broadcast encryption; CCA security; constant size ciphertexts

数据加密是公钥密码学研究的一个重要领域, 安全的加密系统能有效保证数据的机密性. 公钥加密算法的安全性通常由包含敌手攻击模式和攻击目标的安全模型刻画. 攻击模式描述了攻击者能获得的信息, 而攻击目标描述了攻击者最终的攻击目的. 选择明文攻击 (chosen plaintext attack, CPA) 和选择密文攻击 (chosen ciphertext attack, CCA) 是传统公钥加密体制的标准攻击模式, 分别用于刻画被动攻击和主动攻击. 除允许敌手获取加密算法和部分密文外, 前者允许敌手获取自己选择的明文通过加密生成的密文, 后者允许敌手获取自己选择的密文通过解密获得的明文. 攻击目标主要考虑不可区分性 (indistinguishability, IND), 即给定两个明文消息和一个密文, 判断密文是由哪一个明文消息生成. 由于选择密文攻击能有效刻画主动攻击, 更符合现实应用. 因此, 设计满足抵抗选择密文攻击 (也称为选择密文安全) 的密码算法意义更大, 但相比于设计抵抗选择密文攻击 (也称为选择明文安全) 的密码算法, 挑战性更强.

虽然设计选择密文安全的加密方案更难, 但存在一般性转化方法. 即先设计 CPA 安全的加密方案, 然后采用一般性转化方法转化为 CCA 安全的加密方案. Fujisaki 和 Okamoto (FO) 于 1999 年在文献 [1] 的方案设计中引入额外哈希函数, 用于绑定随机数和待加密数据, 提出一种实现 CCA 安全的一般性转化技术. 即如果一个公钥加密方案在随机谕言机模型下可证明是 CPA 安全或者单向安全的, 则可利用 FO 方法把该方案转化为 CCA 安全的方案. 2004 年, Canetti, Halevi 和 Katz (CHK) [2]利用一次签名技术, 给出了标准模型 (非随机谕言机模型) 下的通用转化方法. 如果加密方案在标准模型下可证明是 CPA 安全的且满足密钥可授权 (delegation of secret keys) 的性质, 则可通过 CHK 方法把 CPA 安全的方案转化为 CCA 安全的方案. FO 方法对所有公钥加密系统都成立, 而 CHK 方法只适用于 (分层) 标识加密系统和属性加密系统. 虽然这两种通用方法能有效实现从 CPA 安全到 CCA 安全的转化, 代价是同时增加计算开销和通信开销. 此外, 直接构造选择密文安全的加密方案在文献 [3−5] 中得到进一步研究.

标识 (也称为身份基) 密码体制[6]采用标识作为用户公钥, 有效消除了传统公钥密码体系中出现的证书问题 (验证、撤销、更新等), 显著提高了系统效率. 2001 年, Boneh 等人[7]利用椭圆曲线上的双线性配对技术, 首次给出了真正实用并且可证明安全的标识加密方案. 随后基于双线性对的标识密码在学术界和工业界得到广泛的研究与应用. 然而, 标识密码的研究主要围绕国外算法展开, 缺乏我国自主设计的标识密码. 在此背景下, 我国自主研制了我国密码行业标准—SM9 标识密码, 该密码算法于 2021 年提升为国家标准. 但是, 其设计初衷是适配单接收者应用场景的安全需求, 无法满足新应用对多接收者的需求. 最近, Lai 等人[8]根据 SM9 标识密码算法特征, 融合广播加密技术[9], 提出首个基于 SM9 的标识广播加密方案, 并给出了相应的安全性分析. 该方案与文献 [9] 具有相同的存储效率但只能实现 CPA 的安全性.

本文在文献 [8] 的基础上, 进一步研究如何实现 CCA 的安全性. 基于 SM9 标识加密算法, 设计了一个新的标识广播加密方案并在随机谕言机模型中分析了新方案的安全性. 若 GDDHE 假设 (详见第 2 节) 是难解的, 则可证明新方案具有静态选择密文的安全性. 方案的设计思路采用标识聚合技术[9]实现定长密文, 密文长度不会随着参与用户数量的增加而增加. 为实现抵抗选择密文攻击, 在密文构造时嵌入一个虚设标识, 并通过该虚设标识成功应答攻击者的密文解密询问. 与通用转化方法相比, 本方案具有较短的密文和更小的计算开销. 最后, 对新方案比较分析, 结果表明, 新方案和现有高效标识广播加密方案在计算效率和存储效率方面是可比的.

本文第 1 节介绍标识广播加密的研究现状. 第 2 节描述了必要的数学基础知识和相关密码学原语的定义. 第 3 节介绍本文设计的 CCA 安全的标识广播加密方案, 并分析了方案的安全性和性能. 在第 4 节对全文进行总结.

1 相关工作

自 Boneh 等人在文献 [7] 中采用椭圆曲线上的双线性配对技术设计首个实用且可证明安全的标识加密方案

© 中国科学院软件研究所 http://www.jos.org.cn

后, 围绕双线性对设计标识加密方案得到广泛的研究和应用[3,10,11], 但上述方案的设计初衷都是针对单个接收者. 文献 [9] 采用标识聚合技术给出了首个具有固定大小密文和密钥的标识广播加密方案, 密文和密钥长度与加密阶段选取的用户数量无关. 密文可同时被加密时选定的用户 (授权用户) 解密, 非授权用户即使相互合谋也无法解密密文. 该方案在随机谕言机模型中可证明能够抵抗选择明文攻击. Kim 等人[12]采用对偶加密技术 (dual system encryption)[13], 设计了一个合数阶群标识广播加密方案, 方案在标准模型中满足自适应性选择明文安全. Liu 等人[5]基于文献 [9], 融合 Boyen-Mei-Waters 方法, 引入虚假标识, 构造了具有定长密文 CCA 安全的标识广播加密方案.

Susilo 等人[14]研究标识广播加密体系中用户解密权限的撤销问题, 提出面向云计算的接收者可撤销的标识广播加密方案. 云服务器在无需知道明文的情况下撤销部分用户的解密权限, 并在随机谕言机模型中证明方案是 CPA 安全的. He 等人[15]利用多项式构造了一个具有 CCA 安全的匿名标识广播加密方案, 并在随机谕言机模型中分析了方案的安全性. Liu 等人在文献 [16] 中首先基于素数阶群提出了一个 CPA 安全的分层标识广播加密方案, 然后利用一次签名技术, 基于 CPA 安全的方案提出 CCA 安全的方案. 文献 [17] 提出 CPA 安全的可撤销标识广播加密方案. 文献 [18] 提出内积标识广播加密方案. 方案的解密结果和传统加密方案的解密结果不同, 解密结果为明文与密钥计算得到的一个内积值, 不是具体的明文数据, 可应用于数据统计等特殊应用. 具有其他不同性质的标识广播加密方案在文献 [19−21] 中得到进一步的研究, 但都只满足 CPA 的安全性.

SM9 是我国自主研制基于椭圆曲线的系列标识密码, 包括密数字签名算法, 密钥交换协议, 密钥封装机制和公钥加密算法. 目前, SM9 标识密码算法不仅是我国密码行业标准, 也是国家标准和 ISO/IEC 国际标准, 得到了国内外专家的高度认可, 在云计算、物联网、区块链等多个领域广泛使用. 国内学者对 SM9 标识密码的研究也取得了积极进展[22−26]. 最近, Lai 等人[8]基于 SM9 标识加密算法, 借鉴文献 [9] 中的技术, 提出首个基于 SM9 的广播加密方案. 方案的通信效率与文献 [9] 相同, 但方案只实现 CPA 的安全性. 虽然可通过 FO 技术实现 CCA 安全, 但存在增加计算代价和通信开销的问题. 综上, 具有选择密文安全的标识广播加密方案比较缺乏, 特别是以我国自主设计的国产密码为基础的 CCA 安全高效标识广播加密方案.

2 预备知识

本节描述必要的数学基础知识和密码学技术.

2.1 双线性群

设 λ 为安全参数, p 是由 λ 决定的大素数, G_1,G_2 和 G_T 为通过安全参数 λ 生成的循环群且阶都为 p. 定义映射 $e:G_1\times G_2\to G_T$ 为双线性映射如果对任意群元素 $g\in G_1,h\in G_2$ 和整数 $a,b\in Z_p$, 能有效地计算 $e(g,h)$ 且等式 $e\left(g^a,h^b\right)=e(g,h)^{ab}$ 成立, 此外, 至少存在群元素 $g\in G_1,h\in G_2$, 使得 $e(g,h)\neq 1$.

双线性群表示为 $BP=(G_1,G_2,G_T,e,p)$, 当 $G_1=G_2$ 时, 此双线性群称为对称双线性群, 当 $G_1\neq G_2$ 时, 此双线性群称非对称双线性群. 本文方案的设计基于非对称双线性群.

2.2 困难问题假设

本文提出的方案的安全性基于广义判定性 Diffie-Hellman 困难假设 (general decision Diffie-Hellman exponent assumption, GDDHE), 记为 $(q,m+1,f,g)$-GDDHE 假设. $(q,m+1,f,g)$-GDDHE 问题定义如下.

令 $BP=(G_1,G_2,G_T,e,p)$ 是由系统安全参数 λ 生成的双线性群, 循环群 G_1,G_2 的生成元分别为 g_0,h_0. f 和 g 分别是阶为 q 和 m+1 且根两两不同的互质多项式. 已知:

$$I=\left(\begin{matrix}h_0^a,h_0^{a^2},\ldots,h_0^{a^q}, & h_0^{a^2f(a)},h_0^{ra^2f(a)},\\ g_0,g_0^a,g_0^{a^2},\ldots,g_0^{a^{2m+2}}, & g_0^{rg(a)},\end{matrix}\right),$$

和群 G_T 中的元素 T, 判断 T 为 $e(g_0,h_0)^{raf(a)}$ 还是群 G_T 中的随机元素, 其中 a 和 h_0 是未知的.

定义多项式算法 D 成功解决 $(q,m+1,f,g)$-GDDHE 问题的优势为:

$$Adv(\lambda)=\left|\Pr\left[D\left(I,T=e(g_0,h_0)^{raf(a)}\right)=1\right]-\Pr\left[D\left(I,T\neq e(g_0,h_0)^{raf(a)}\right)=1\right]\right|.$$

© 中国科学院软件研究所 http://www.jos.org.cn

在广义群模型中, 若对任意多项式时间算法 D, 成功解决 $(q,m+1,f,g)$ -GDDHE 问题的优势 $Adv(\lambda)$ 是可忽略的, 则称 $(q,m+1,f,g)$ -GDDHE 假设成立.

不难发现, $(q,m+1,f,g)$ -GDDHE 问题与文献 [8,9] 中 GDDHE 问题相似. 因此, 可用文献中的方法在广义群模型中分析 $(q,m+1,f,g)$ -GDDHE 问题的困难性, 本文不再重复.

2.3 标识广播加密定义

标识广播加密方案通常由以下 4 个多项式时间算法描述, 为描述方便, 仅给出密钥封装的形式化定义.

(1) $(mpk,msk)\leftarrow Setup(\lambda,m)$: 系统建立算法 $Setup$ 输入系统安全参数 λ 和最大用户数量 m, 输出系统主公私钥对 (mpk,msk), 其中 mpk 是公开的且包含对密钥空间 $\mathcal{K}$ 和密文空间 C 的描述. 该算法由密钥生成中心 (key generator center, KGC) 运行.

(2) $sk_{ID}\leftarrow KeyGen(mpk,msk,ID)$: 密钥生成算法 $KeyGen$ 输入系统主公私钥对 (mpk,msk) 和给定的用户标识 ID, 输出用户 ID 的密钥 sk_{ID}. 该算法由 KGC 运行.

(3) $(K,CT)\leftarrow Encrypt(mpk,S)$: 加密算法 $Encrypt$ 输入系统主公钥 mpk 和一个标识集合 S, 输出封装密钥 (会话密钥) $K\in\mathcal{K}$ 和封装密文 $CT\in C$. 该算法由加密者运行. 当需要广播数据 M 时, 加密者首先根据该算法生成封装密钥 K, 同时, 选取安全的对称加密方案, 以 K 和 M 为输入生成密态数据 C_M, 最后广播 (CT,C_M).

(4) $K\leftarrow Decrypt(mpk,CT,S,sk_{ID_i})$: 解密算法 $Decrypt$ 输入系统主公钥 mpk, 收到的密文 CT, 密文对应的标识集合 S 和用户密钥 sk_{ID_i}. 若 $ID_i\in S$, 算法输出封装密钥 K. 若 $ID_i\notin S$, 算法输出解密失败提示符号“$\perp$”. 该算法由解密者运行. 解密者计算出 K 后, 把 K 和 C_M 输入到对称加密方案的解密算法中进而获取明文数据 M.

标识广播加密方案应满足正确性, 即对任意的 $sk_{ID}\leftarrow KeyGen(mpk,msk,ID)$ 和 $(K,CT)\leftarrow Encrypt(mpk,S)$, 有:

$$\begin{cases} Decrypt\ (mpk,C,sk_{ID_i})=K & 若\ \ ID_i\in S \\ Decrypt\ (mpk,C,sk_{ID_i})=\perp & 若\ \ ID_i\notin S \end{cases}.$$

● 安全模型. 本文描述标识广播加密系统的安全模型, 并给出静态选择密文攻击模型中的不可区分 (indistinguishbility against selective-ID chosen-ciphertext attacks, IND-sID-CCA) 安全定义. IND-sID-CCA 安全模型由挑战者 (challenger) 和攻击者 (adversary) 参与的游戏来定义. 在该定义中假设挑战者和攻击者都知道用户最大数量 m.

● 初始化. 攻击者输出挑战标识集合 $S^*=(ID_1,ID_2,\ldots,ID_{s^*})$, 其中 $s^*\leqslant m$.

● 系统建立. 针对给定的安全参数 λ 和 m, 挑战者运行系统参数生成算法 $Setup$ 建立系统, 为系统生成主公私钥对 (mpk,msk), 并将系统主公钥 mpk 发送给攻击者, 秘密保留系统主私钥.

● 询问 1. 攻击者可根据需求自适应性地询问用户密钥和密文解密. 针对用户密钥询问 $ID\notin S^*$, 挑战者运行算法 $KeyGen$ 生成密钥 sk_{ID}, 并以 sk_{ID} 作为回复. 针对密文解密询问 (CT,S,ID), 其中 $S\subseteq S^*$ 且 $ID\in S$. 挑战者首先运行算法 $KeyGen$ 生成密钥 sk_{ID}, 然后以 sk_{ID} 和 CT 为输入, 运行解密算法 $Decrypt$, 并以解密结果作为回复.

● 挑战. 挑战者首先运行加密算法 $Encrypt(mpk,S^*)$ 生成挑战封装密钥和封装密文 (K^*,CT^*). 接着, 随机选择 $c\in\{0,1\}$, 把生成的挑战封装密钥设为 $K_c=K^*$, 并从 $\mathcal{K}$ 中随机选择一个会话密钥设为 K_{1-c}. 最后回复 (CT^*,K_0,K_1).

● 询问 2. 攻击者可继续自适应性地询问用户密钥和密文解密, 但不能询问挑战密文 (CT^*,S^*) 的解密. 挑战者的响应方式与询问 1 相同.

● 猜测. 攻击者输出对 c 的猜测 $c'\in\{0,1\}$. 若 $c'=c$, 则攻击者赢得游戏.

定义攻击者 $\mathcal{A}$ 获胜的优势为:

$$Adv_{\mathcal{A}}^{\text{IND-sID-CCA}}(\lambda)=\left|\Pr[c'=c]-\frac{1}{2}\right|.$$

定义 1. 在 IND-sID-CCA 安全模型中, 如果不存在多项式时间攻击者 $\mathcal{A}$ 能以不可忽略的优势 $Adv_{\mathcal{A}}^{\text{IND-sID-CCA}}(\lambda)$ 赢得游戏, 则称方案满足 IND-sID-CCA 的安全性.

注: 在密文解密询问中, 若 $S\not\subset S^*$, 则至少存在一个标识 $ID\in S$, 且 $ID\notin S^*$. 那么攻击者或者挑战者可获知该标识的正确密钥, 通过该密钥能够自行解密密文. 因此, 在安全模型中, 要求 $S\subseteq S^*$.

© 中国科学院软件研究所 http://www.jos.org.cn

2.4 SM9 标识加密方案

为更好理解本文方案, 首先给出 SM9 标识加密方案的构造. 为描述方便, 仅给出 SM9 密钥封装机制, 且方案设计乘法群表示方案描述如下.

● Setup. 针对安全参数 λ, KGC 首先根据安全参数生成非对称双线性群 $BP=(G_1,G_2,G_T,e,p)$, 其中 $p>2^{\lambda}$. 接着, 随机选取循环群 G_1,G_2 的生成元 g,h, 随机数 $\alpha\in Z_p^*$, 密码函数 $H_1:\{0,1\}^*\times Z_p^*\to Z_p^*$ 和 $KDF:G_1\times G_T\times\{0,1\}^*\times Z_p^*\to\{0,1\}^{\ell}$, 其中 ℓ 为封装密钥的长度. 计算 $P_{\text{pub}}=g^{\alpha}$, $v=e(g,h)^{\alpha}$. 最后, 选择合适的密钥生成函数识别符 hid, 并输出系统的主公钥 mpk 和主私钥 msk:

$$mpk=\left(BP,g,h,P_{\text{pub}},v,H_1,KDF,hid,\ell\right),msk=\alpha.$$

● KeyGen. 已知标识 $ID\in\{0,1\}^*$, KGC 计算用户的解密密钥:

$$sk_{ID}=h^{\frac{\alpha}{\alpha+H_1(ID\|hid,p)}}.$$

● Encrypt. 设封装密钥的比特长度为 ℓ, 接收者的标识为 ID, 首先选取随机数 $r\in Z_p^*$, 接着计算 $C=\left(g^{H_1(ID\|hid,p)}\cdot P_{\text{pub}}\right)^r$, $w=v^r$. 最后计算封装密钥 $K=KDF(C\|w\|ID,\ell)$, 并输出 (C,K), 其中 C 为对应的封装密文.

● Decrypt. 设用户 ID 的密钥为 sk_{ID}, 封装密文为 C, 解密算法计算 $w'=e(C,sk_{ID})$, $K'=KDF(C\|w'\|ID,\ell)$. 如果 K'为全 0 比特串, 则输出报错提示并退出, 否则输出 K'作为正确的封装密钥.

3 CCA 安全的 SM9 广播加密方案

本节基于 SM9 标识加密方案提出具有 CCA 安全的广播加密方案, 方案构造采用乘法群, 且使用密码函数 H_3 代替 SM9 标识加密算法中的密钥派生函数 $KDF(\cdot)$. H_3 是用于生成封装密钥的密码函数, 其输入参数有 5 个元素, 具体定义为 $H_3:G_1\times G_2\times G_T\times\left(Z_p^*\right)^2\to\{0,1\}^{\ell}$.

3.1 算法描述

● Setup. 针对安全参数 λ 和加密允许的最大用户数量 m, 首先以安全参数为输入生成非对称双线群 $BP=(G_1,G_2,G_T,e,p)$, 其中 $p>2^{\lambda}$, 并随机选取循环群 G_1,G_2 的生成元 g,h, 随机数 $\alpha\in Z_p^*$, 3 个密码函数 $H_1:\{0,1\}^*\times Z_p^*\to Z_p^*$, $H_2:G_2\to Z_p^*$ 和 $H_3:G_1\times G_2\times G_T\times\left(Z_p^*\right)^2\to\{0,1\}^{\ell}$, 其中 ℓ 为消息的长度 (封装密钥长度). 计算 $P_{\text{pub}}=\left(g^{\alpha},g^{\alpha^2},\ldots,g^{\alpha^{m+1}}\right)$, $u=h^{\alpha^2}$, $v=e(g,h)^{\alpha}$. 最后, 选择适当的密钥生成函数识别符 hid, 系统的主公钥 mpk 和主私钥 msk 为:

$$mpk=\left(BP,g,P_{\text{pub}},u,v,H_1,H_2,H_3,hid,\ell\right),msk=(\alpha,h).$$

● KeyGen. 已知标识 $ID\in\{0,1\}^*$, KGC 计算用户的解密密钥:

$$sk_{ID}=h^{\frac{\alpha}{\alpha+H_1(ID\|hid,p)}}.$$

● Encrypt. 给定标识集合 $S=(ID_1,ID_2,\ldots,ID_n)(n\leqslant m)$, 选取随机数 $r\in Z_p^*$, 计算:

$$w=v^r,\quad C_1=u^{-r},\quad C_2=g^{r\cdot(\alpha+H_2(C_1))\cdot\prod_{i=1}^{n}(\alpha+H_1(ID_i\|hid,p))},$$

$$\tau=\prod_{i=1}^{n}H_1(ID_i\|hid,p)\bmod p,\quad K=H_3(C_1,C_2,w,\tau,\ell),$$

输出三元组 (C_1,C_2,K), 其中 (C_1,C_2) 为封装密文, K 为封装的加密密钥.

● Decrypt. 为恢复封装密文 (C_1,C_2,S) 中的加密密钥 K, 用户 $ID_i\in S$ 以密钥 sk_{ID_i} 为输入, 首先验证公式 (1) 是否成立:

$$e\left(C_2,u^{-1}\right)=e\left(g^{(\alpha+H_2(C_1))\cdot\prod_{j=1}^{n}(\alpha+H_1(ID_i\|hid,p))},C_1\right)\tag{1}$$

若公式 (1) 不成立, 表示该密文是无效的密文, 则停止并退出算法, 输出解密失败符号“$\perp$”. 若公式 (1) 成立, 接着计算:

$$w'=\left(e\left(g^{f_{i,S}(\alpha)},C_1\right)\cdot e(C_2,sk_{ID_i})\right)^{\frac{1}{H_2(C_1)\cdot\prod_{j=1,j\neq i}^{n}H_1(ID_j\|hid,p)}},$$

© 中国科学院软件研究所 http://www.jos.org.cn

其中,

$$f_{i,S}(\alpha)=\frac{1}{\alpha}\cdot\left((\alpha+H_2(C_1))\prod_{j=1,j\neq i}^{n}\left(\alpha+H_1\left(ID_j\|hid,p\right)\right)-H_2(C_1)\cdot\prod_{j=1,j\neq i}^{n}H_1\left(ID_j\|hid,p\right)\right).$$

最后, 计算 $\tau'=\prod_{ID_i\in S}H_1(ID_i\|hid,p) \bmod p$. 若 $K'=H_3(C_1,C_2,w',\tau',\ell)$ 为全 0 比特串, 则报错并结束算法, 否则输出 K' 作为封装密钥.

3.2 正确性分析

假设 (C_1,C_2) 为封装给用户集合 S 的有效密文, 标识 $ID_i\in S$ 且对应的密钥为 $sk_{ID_i}=h^{\frac{\alpha}{\alpha+H_1(ID_i\|hid,p)}}$. 又系统主公钥 mpk 确定后, hid 和 p 的值是固定的. 为描述方便, 在下文中使用 $H_1(ID_i)$ 代替 $H_1(ID_i\|hid,p)$, 则有:

$$e\left(C_2,u^{-1}\right)=e\left(g^{r\cdot(\alpha+H_2(C_1))\cdot\prod_{i=1}^{n}(\alpha+H_1(ID_i))},u^{-1}\right)=e\left(g^{(\alpha+H_2(C_1))\cdot\prod_{i=1}^{n}(\alpha+H_1(ID_i))},u^{-r}\right)=e\left(g^{(\alpha+H_2(C_1))\cdot\prod_{i=1}^{n}(\alpha+H_1(ID_i))},C_1\right),$$

公式 (1) 成立. 接着计算:

$$\begin{aligned}A&=e\left(g^{f_{i,S}(\alpha)},C_1\right)\cdot e(C_2,sk_{ID_i})=e\left(g^{f_{i,S}(\alpha)},h^{-r\cdot\alpha^2}\right)\cdot e\left(g^{r\cdot(\alpha+H_2(C_1))\cdot\prod_{j=1}^{n}(\alpha+H_1(ID_j))},h^{\frac{\alpha}{\alpha+H_1(ID_i)}}\right)\\&=e(g,h)^{-r\cdot\alpha\cdot\left((\alpha+H_2(C_1))\prod_{j=1,j\neq i}^{n}(\alpha+H_1(ID_j))\right)-H_2(C_1)\cdot\prod_{j=1,j\neq i}^{n}H_1(ID_j))}\cdot e(g,h)^{r\cdot\alpha\cdot(\alpha+H_2(C_1,w))\cdot\prod_{j=1,j\neq i}^{n}(\alpha+H_1(ID_j))}\\&=e(g,h)^{r\cdot\alpha\cdot H_2(C_1)\cdot\prod_{j=1,j\neq i}^{n}H_1(ID_j)},\end{aligned}$$

$$w'=A^{\frac{1}{H_2(C_1)\cdot\prod_{j=1,j\neq i}^{n}H_1(ID_j)}}=\left(e(g,h)^{r\cdot\alpha\cdot H_2(C_1)\cdot\prod_{j=1,j\neq i}^{n}H_1(ID_j)}\right)^{\frac{1}{H_2(C_1)\cdot\prod_{j=1,j\neq i}^{n}H_1(ID_j)}}=e(g,h)^{r\cdot\alpha}=w.$$

因此, 若 (C_1,C_2) 为封装给用户集合 S 的有效密文, 则 $K'=H_3(C_1,C_2,w',\tau',\ell)=H_3(C_1,C_2,w,\tau,\ell)=K$, 授权用户可恢复出正确的会话密钥, 方案满足广播加密的正确性要求.

3.3 安全性分析

定理 1. 令上述方案中的密码函数 H_1, H_2 为随机谕言器. 如果 $(q,m+1,f,g)$ -GDDHE 假设成立, 则方案满足 IND-sID-CCA 的安全性.

证明: 假定存在多项式时间攻击算法 $\mathcal{A}$ 在 IND-sID-CCA 安全模型中能以不可忽略的优势 ϵ 攻破方案, 则可以构造一个模拟算法 $\mathcal{B}$ 以不可忽略的优势解决 $(q,m+1,f,g)$ -GDDHE 问题. 设询问随机谕言器 H_1 和 H_2 的总次数为 q, 攻击算法 $\mathcal{A}$ 和模拟算法 $\mathcal{B}$ 都以 m, q 为输入, 且 $\mathcal{B}$ 额外输入一个 $(q,m+1,f,g)$ -GDDHE 问题实例:

$$I=\left(\begin{array}{c}h_0^a,\ h_0^{a^2},\ldots,\ h_0^{a^q},\quad h_0^{a^2f(a)},\ h_0^{ra^2f(a)},\\ g_0,\ g_0^a,\ g_0^{a^2},\ldots,\ g_0^{a^{2m+2}},\quad g_0^{rg(a)},\end{array}\right)$$

和元素 T, 其中 $T\in G_T$, 且 $T=(g_0,h_0)^{raf(a)}$ 或是随机群元素. 多项式 $f(z)$ 和 $g(z)$ 分别是定义在 Z_p^* 中阶为 q 和 $m+1$ 的互质多项式. 不妨设 $f(z)$ 的 q 个不同根为 $x_1,x_2,\ldots,x_q$, $g(z)$ 的 $m+1$ 个不同根为 $x_{q+1},x_{q+2},\ldots,x_{q+m+1}$, 则 $x_1,\ldots,x_{q+m+1}$ 各不相同. 定义 $f(z)$ 和 $g(z)$ 为:

$$f(z)=\prod_{i=1}^{q}(z+x_i)=\sum_{i=0}^{q}b_iz^i,\quad g(z)=\prod_{i=q+1}^{q+m+1}(z+x_i),$$

其中, b_i 为多项式 $f(z)$ 的系数, 是可求的. 对任意的 $i\in[1,q]$, 定义 $f_i(z)=\dfrac{f(z)}{z+x_i}=\sum_{j=0}^{q-1}d_{i,j}z^j$, $d_{i,j}$ 为多项式 $f_i(z)$ 的系数, 是可求的. 对任意的 $i\in[q+1,q+m+1]$, 定义 $g_i(z)=\dfrac{g(z)}{z+x_i}$, 则 $f_i(z)$ 的次数为 $q-1$, $g_i(z)$ 的次数为 m.

- 初始化. $\mathcal{A}$ 输出一个挑战标识集合 $S^*=\left(ID_1^*,ID_2^*,\ldots,ID_{s^*}^*\right)(s^*\leqslant m)$.
- 系统建立. $\mathcal{B}$ 根据如下方式生成系统主公钥. 首先隐式的令 $\alpha=a$, $h=h_0^{f(a)}$, 并设挑战密文的 C_1^* 部分为 $C_1^*=h_0^{-ra^2f(a)}$. 接着, 设 $u=h_0^{a^2f(a)}=h^{a^2}$, 定义多项式 $\prod_{i=q+s^*+1}^{q+m}(a+x_i)=\sum_{i=0}^{m-s^*}c_ia^i$, 其中 c_i 为多项式系数. 计算:

$$g=\prod_{i=0}^{m-s^*}\left(g_0^{a^i}\right)^{c_i}=g_0^{\sum_{i=0}^{m-s^*}c_ia^i}=g_0^{\prod_{i=q+s^*+1}^{q+m}(a+x_i)},$$

© 中国科学院软件研究所 http://www.jos.org.cn

$$g^{a^j}=\prod_{i=0}^{m-s^*}\left(g_0^{a^{i+j}}\right)^{c_i}=g_0^{a^j\cdot\prod_{i=q+s^*+1}^{q+m}(a+x_i)},j=1,2,\ldots,m,$$

$$v=e\left(g_0^{\prod_{i=q+s^*+1}^{q+m}(a+x_i)},h_0^{ab_0}\right)e\left(g_0^{a\prod_{i=q+s^*+1}^{q+m}(a+x_i)},h_0^{\sum_{i=1}^{q}b_ia^i}\right)=e\left(g_0^{a\prod_{i=q+s^*+1}^{q+m}(a+x_i)},h_0^{f(a)}\right)=e(g,h)^{\alpha}.$$

在给定困难问题实例中, $g_0^{a^i}$ 是已知的, 又 c_i 是可计算的多项式系数. 因此 g,g^{a^j} 是可计算的. 虽然 h_0 是未知的, $h=h_0^{f(a)}$ 也是未知的, 但 v 可利用双线性对的性质, 通过输入的困难问题实例计算得到. u 可直接从困问题实例获得. 最后 $\mathcal{B}$ 选择密钥生成函数识别符 hid, 密码函数 $H_3:G_1\times G_2\times G_T\times\left(Z_p^*\right)^2\to\{0,1\}^{\ell}$, 输出系统主公钥:

$$mpk=\left(g,u,v,\ell,H_3,hid,\{g^{a^j}\}_{j=1}^{m}\right),$$

其中, H_1,H_2 被看成是由模拟算法 $\mathcal{B}$ 控制的随机谕言器. 为方便描述, 下文省略 hid 和 p 的输入.

● 哈希询问. $\mathcal{A}$ 在任何时候可询问谕言器 H_1 和 H_2.

(1) H_1-询问. 已知标识 ID_i, 不妨设 H_1 询问的次数为 q_1. 为回复询问, $\mathcal{B}$ 首先建立列表 $\mathcal{L}_1$, 列表中元素的初始状态为:

$$\{(\perp,x_i)\}_{i\in[1,q_1]},\quad \{(ID_i,x_i)\}_{i\in[q+1,q+s^*]},$$

其中, "$\perp$"代表空, $\left(ID_{q+1},ID_{q+2},\ldots,ID_{q+s^*}\right)=\left(ID_1^*,ID_2^*,\ldots,ID_{s^*}^*\right)$. 当 $\mathcal{A}$ 询问标识 ID_i 的 H_1 值时, 若 (ID_i,x_i) 在列表 $\mathcal{L}_1$ 中, $\mathcal{B}$ 返回 x_i. 否则, 记 ID_i 为第 i 个新标识, 设 $H_1(ID_i)=x_i$, 并返回 x_i.

(2) H_2-询问. 已知 C_i, 不妨设 H_2 询问的次数为 $q_2(q_2=q-q_1)$, 为回复询问, $\mathcal{B}$ 首先建立列表 $\mathcal{L}_2$, 列表中元素的初始状态为:

$$\{(\perp,y_i)\}_{i\in[1,q_2]}=\{(\perp,x_i)\}_{i\in[q_1+1,q]},\quad \{(C_1^*,x_{q+m+1})\},$$

其中, "$\perp$"代表空. 当攻击算法 $\mathcal{A}$ 询问 C_i 的 H_2 值时, 若 (C_i,x_i) 在列表 $\mathcal{L}_2$ 中, $\mathcal{B}$ 返回 y_i. 否则, 记 C_i 为第 i 个新询问, 设 $H_2(C_i)=y_i$, 并返回 y_i.

● 询问 1. $\mathcal{A}$ 可以自适应性地询问用户密钥和密文解密.

(1) 密钥询问. 已知标识 $ID_i\notin S^*$, $\mathcal{B}$ 首先检查列表 $\mathcal{L}_1$ 获取 x_i (若不存在, 以 ID_i 为输入询问 H_1, 获得 x_i). 接着, 计算:

$$sk_{ID_i}=\prod_{j=0}^{q-1}\left(h_0^{a^{j+1}}\right)^{d_{i,j}}=h_0^{\sum_{j=0}^{q-1}d_{i,j}a^{j+1}}=h_0^{af_i(a)}=h_0^{\frac{af(a)}{a+x_i}}=h^{\frac{a}{a+H_1(ID_i)}}.$$

最后, $\mathcal{B}$ 将 sk_{ID_i} 发送给 $\mathcal{A}$. 不难看出, sk_{ID_i} 是正确的密钥, $\mathcal{B}$ 能通过给定的困难问题实例成功模拟任意标识 $ID_i\notin S^*$ 的密钥.

(2) 密文解密询问. 已知解密询问密文 (C_1,C_2,S), 其中 $S\subseteq S^*$, $\mathcal{B}$ 首先判断公式 (2) 是否成立.

$$e\left(C_2,u^{-1}\right)=e\left(g^{(\alpha+H_2(C_1))\cdot\prod_{ID_i\in S}(\alpha+H_1(ID_i\|hid,p))},C_1\right)\tag{2}$$

若公式 (2) 不成立, 表示 (C_1,C_2,S) 是无效密文, 返回解密失败符号"$\perp$". 若公式 (2) 成立, 则 $C_1=C_1^*$ 的概率是可忽略的, 即 $C_1\neq C_1^*$. 在该情况下, 存在某个 y_i, 满足 $H_2(C_1)=y_i=x_{q_1+i}$ (若不存在 y_i, 则以 C_1 为输入询问 H_2 获取 y_i). 接着, 按密钥询问的步骤计算:

$$\widetilde{sk_{C_1}}=h_0^{af_{q_1+i}(a)}=h_0^{\frac{af(a)}{a+x_{q_1+i}}}=h^{\frac{a}{a+H_2(C_1)}}.$$

以 $\left(\widetilde{sk_{C_1}},C_1,C_2,S\right)$ 为输入运行解密算法, 并把解密结果返回给 $\mathcal{A}$. 注意到 $\widetilde{sk_{C_1}}$ 不是正确的解密密钥, 但是, 根据证明设置, 该值能够正确解密密文.

● 挑战. 当 $\mathcal{A}$ 决定询问阶段 1 结束后, $\mathcal{B}$ 计算:

$$C_2^*=g_0^{rg(a)},\tau^*=\prod\nolimits_{ID_i\in S^*}H_1(ID_i),w^*=T^{\prod_{i=q+s^*+1}^{q+m}x_i}\cdot e\left(g_0^{\frac{1}{a}\left(\prod_{i=q+s^*+1}^{q+m}(a+x_i)-\prod_{i=q+s^*+1}^{q+m}x_i\right)},h_0^{ra^2f(a)}\right).$$

计算 $K^*=H_3\left(C_1^*,C_2^*,w^*,\tau^*,\ell\right)$. 接着, 在封装密钥空间 $\mathcal{K}$ 中选取一个随机密钥 K, 随机选取 $c\in\{0,1\}$. 最后, 设 $K_c=K^*,K_{1-c}=K$, 并发送挑战密文 $\left(C_1^*,C_2^*,K_0,K_1\right)$ 给 $\mathcal{A}$, 其中 C_1^* 在系统建立阶段已求. 设生成挑战密文所选取的随

© 中国科学院软件研究所 http://www.jos.org.cn

机数为 $r^*=r$, 则有:

$$\begin{cases} C_1^* = h_0^{-ra^2 f(a)} = u^{-r^*} \\ C_2^* = g_0^{rg(a)} = g_0^{r\cdot\prod_{i=q+1}^{q+m+1}(a+x_i)} = g_0^{r\cdot(a+x_{q+m+1})\cdot\prod_{q+s^*+1}^{q+m}(a+x_i)\cdot\prod_{i=q+1}^{q+s^*}(a+x_i)} \\ \quad = g^{r\cdot(a+x_{q+m+1})\cdot\prod_{i=q+1}^{q+s^*}(a+x_i)} = g^{r^*\cdot(a+H_2(C_1^*))\cdot\prod_{i=1}^{s^*}(a+H_1(ID_i^*))} \end{cases}.$$

若 $T=e(g_0,h_0)^{raf(a)}$, 有:

$$w^* = T^{\prod_{i=q+s^*+1}^{q+m}x_i}\cdot e\left(g_0^{\frac{1}{a}\left(\prod_{i=q+s^*+1}^{q+m}(a+x_i)-\prod_{i=q+s^*+1}^{q+m}x_i\right)}, h_0^{ra^2f(a)}\right) = \left(e(g_0,h_0)^{raf(a)}\right)^{\prod_{i=q+s^*+1}^{q+m}x_i}\cdot e\left(g_0^{\left(\prod_{i=q+s^*+1}^{q+m}(a+x_i)-\prod_{i=q+s^*+1}^{q+m}x_i\right)}, h_0^{raf(a)}\right)$$

$$= e(g_0,h_0)^{raf(a)\cdot\left(\prod_{i=q+s^*+1}^{q+m}(a+x_i)\right)} = v^{r^*}.$$

因此, 当 $T=e(g_0,h_0)^{raf(a)}$ 时, 挑战密文是正确的封装密文.

● 询问 2. $\mathcal{A}$ 允许继续自适应性地询问用户密钥和密文解密, 但不能询问挑战密文 $\left(C_1^*,C_2^*\right)$ 的解密, $\mathcal{B}$ 根据询问 1 的步骤回复 $\mathcal{A}$.

● 猜测. $\mathcal{A}$ 输出对 c 的猜测 $c'\in\{0,1\}$. 若 $c=c'$, $\mathcal{B}$ 输出 1, 表示猜测 $T=(g_0,h_0)^{raf(a)}$. 否则输出 0, 表示猜测 T 为群 G_T 中的随机值.

最后, 分析 $\mathcal{B}$ 成功解决 $(q,m+1,f,g)$ -GDDHE 问题的优势. 从证明的设置可知, 当 $T=e(g_0,h_0)^{raf(a)}$ 时, 挑战密文是正确的封装密文, 攻击者 $\mathcal{A}$ 无法区分是模拟还是真实攻击环境. 在该情况下, 根据假设 $\mathcal{A}$ 能以不可忽略的优势 ε 攻破上述方案, 则有 $\Pr\left[c=c'|T=e(g_0,h_0)^{raf(a)}\right]=\frac{1}{2}+\varepsilon$. 当 $T\neq e(g_0,h_0)^{raf(a)}$, 为群 G_T 中的随机值时, w^* 是随机的, 与 C_1^*,C_2^* 无关, 挑战密文由一次一密加密得到, 有 $\Pr\left[c=c'|T\neq e(g_0,h_0)^{raf(a)}\right]=\frac{1}{2}$. 综上有:

$$Adv(\lambda)=\left|\Pr\left[\mathcal{A}\left(\mathcal{I},T=e(g_0,h_0)^{raf(a)}\right)=1\right]-\Pr\left[\mathcal{A}\left(\mathcal{I},T\neq e(g_0,h_0)^{raf(a)}\right)=1\right)\right|$$

$$=\left|\Pr\left[c=c'|T=e(g_0,h_0)^{raf(a)}\right]-\Pr\left[c=c'|T\neq e(g_0,h_0)^{raf(a)}\right]\right|=\left|\frac{1}{2}+\varepsilon-\frac{1}{2}\right|=\varepsilon.$$

综上, 若 $\mathcal{A}$ 能以不可忽略的优势 ε 攻破上述方案, 则 $\mathcal{B}$ 能以同样的优势 ε 给出 $(q,m+1,f,g)$ -GDDHE 问题的正确解.

3.4 性能分析

本节从计算效率和存储效率两个方面对本文方案进行分析, 并与具有定长密文的标识广播加密方案进行比较, 结果如表 1 和表 2 所示. 表 1 不统计映射到 Z_p^* 和映射到字符串的哈希运算. 表 2 只考虑密钥封装, 即不考虑封装密钥加密数据部分. 符号说明如下, p: 基于椭圆曲线的双线性配对运算; E_i $(i=1,2,T,N)$: 循环群 G_i 中的指数运算; G_N: 合数阶群; E: 对称群 G 中的指数运算; M: 模运算; $|G_i|(i=1,2,N)$: 群 G_i 中元素的大小; $|G|$: 对称群 G 中元素的大小, $\mathcal{SE}$: 对称加密方案的加密算法; $\mathcal{SD}$: 对称加密方案的解密算法; ROM: 随机谕言模型; m: 加密允许的最大用户数量; n: 加密时实际用户数量, 即集合 S 的大小.

表 1 计算开销比较

方案	加密	解密	群阶
文献[9]	$E_1+(n+1)E_2+E_t$	$2p+(n-1)E_2+E_t$	素数阶
文献[5]	$E_1+(n+2)E_2+E_t$	$4p+2nE_2+E_t$	素数阶
文献[12]	$(2n+5)E_N+E_t$	$4p+nE_N$	合数阶
文献[21]	$(2n+2)E+2\mathcal{SE}$	$3p+2nE+2\mathcal{SD}$	素数阶
文献[8]	$(n+1)E_1+E_2+E_t$	$2p+(n-1)E_1+E_t$	素数阶
本方案	$(n+2)E_1+E_2+E_t+M$	$4p+2nE_1+E_t+M$	素数阶

© 中国科学院软件研究所 http://www.jos.org.cn

表 2 存储开销和安全性比较

方案	公钥	密钥	密文	困难假设	安全性	安全模型
文献[9]	$\|G_T\|+(m+1)\|G_2\|+\|G_1\|$	$\|G_1\|$	$\|G_1\|+\|G_2\|$	q-type	IND-sID-CPA	ROM
文献[5]	$\|G_T\|+(m+2)\|G_2\|+\|G_1\|$	$\|G_1\|$	$\|G_1\|+\|G_2\|$	q-type	IND-sID-CCA	ROM
文献[12]	$\|G_T\|+(2m+5)\|G_N\|$	$(m+4)\|G_N\|$	$4\|G_N\|$	GSD	IND-CPA	Standard
文献[21]	$(3m+1)\|G\|$	$\|G\|$	$4\|G\|$	DB-DHES	IND-CPA	Standard
文献[8]	$\|G_T\|+\|G_2\|+(m+1)\|G_1\|$	$\|G_2\|$	$\|G_1\|+\|G_2\|$	q-type	IND-sID-CPA	ROM
本方案	$\|G_T\|+\|G_2\|+(m+2)\|G_1\|$	$\|G_2\|$	$\|G_1\|+\|G_2\|$	q-type	IND-sID-CCA	ROM

从表 1 和表 2 可知, 本方案在数据加密和密文解密的计算开销上与现有高效标识广播加密方案相当, 都与消息接收者数量呈线性关系. 虽然解密开销大约是文献 [8,9] 的两倍, 但文献 [8,9] 只满足 CPA 的安全性. 所有比较方案中, 只有文献 [5] 和本方案是 CCA 安全的. 本方案的密钥和密文长度与文献 [5,8,9] 中方案相同, 都分别由一个群元素和两个群元素组成, 优于文献 [12,21]. 虽然文献 [12,21] 中方案的安全性基于标准困难问题和标准模型, 但只满足 CPA 的安全性, 且方案的公钥长度远大于本方案公钥的长度. 此外, 文献 [12] 的方案设计基于合数阶群, 而文献 [21] 的方案依赖于对称加密系统. 根据表 1, 两者的加密效率皆低于本文方案. 其他比较方案的安全性都基于 q 类型的困难假设和随机谕言机模型. 注意到, 文献 [27] 提出了一个在标准模型下, 基于标准困难问题可证明具有自适应性 CCA 安全的标识广播加密方案, 方案同时具有短密钥和短密文的特性. 但是该方案只能为集合 S 中的用户 (加密时选定的一组接收者) 生成密钥, 且每个用户的密钥都与集合中其他用户相关, 不具备一般性. 在不采用通用转化方法的情况下, 如何设计具有短密文和短密钥, 且在非随机谕言机模型中可证明满足自适应性 CCA 安全的广播加密方案是一个具有挑战性的研究问题.

4 总 结

本文基于国产密码 SM9 标识加密算法提出一个能抵抗选择密文攻击的广播加密方案. 方案的设计有效融合了标识聚合技术和虚设标识技术. 通过该虚设标识, 模拟者可以成功回复攻击者的解密询问, 实现 CCA 安全. 相比于采用通用转化方法 (FO 技术[1]), 本文提出的方案具有较短的密文且计算开销较小. 方案与文献 [8] 相比, 密钥长度和密文长度并没有增加, 但满足更高的安全性. 方案的安全性基于随机谕言机模型和 q 类型广义判定性 Diffie-Hellman 困难假设. 最后, 对方案进行比较分析, 结果表明本方案和现有高效标识广播加密方案在计算开销和通信代价方面是可比的.

References:

[1] Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes. In: Proc. of the 19th Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 1999. 537–554. [doi: 10.1007/3-540-48405-1_34]

[2] Canetti R, Halevi S, Katz J. Chosen-ciphertext security from identity-based encryption. In: Proc. of the Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Interlaken: Springer, 2004. 207–222. [doi: 10.1007/978-3-540-24676-3_13]

[3] Gentry C. Practical identity-based encryption without random oracles. In: Proc. of the 25th Int'l Conf. on the Theory and Applications of Cryptographic Techniques. St. Petersburg: Springer, 2006. 445–464. [doi: 10.1007/11761679_27]

[4] Ge AJ, Zhang R, Chen C, Ma CG, Zhang ZF. Threshold ciphertext policy attribute-based encryption with constant size ciphertexts. In: Proc. of the 17th Australasian Conf. on Information Security and Privacy. Wollongong: Springer, 2012. 336–349. [doi: 10.1007/978-3-642-31448-3_25]

[5] Liu X, Liu WR, Wu QH, Liu JW. Chosen ciphertext secure identity-based broadcast encryption. Journal of Cryptologic Research, 2015, 2(1): 66–76 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000061]

[6] Shamir A. Identity-based cryptosystems and signature schemes. In: Blakley GR, Chaum D, eds. Advances in Cryptology. Berlin: Springer, 1985. 47–53. [doi: 10.1007/3-540-39568-7_5]

[7] Boneh D, Franklin M. Identity-based encryption from the weil pairing. In: Proc. of the 21st Annual Int'l Cryptology Conf. Santa Barbara: Springer, 2001. 213–229. [doi: 10.1007/3-540-44647-8_13]

© 中国科学院软件研究所 http://www.jos.org.cn

[8] Lai JC, Huang XY, He DB. An efficient identity-based broadcast encryption scheme based on SM9. Chinese Journal of Computers, 2021, 44(5): 897–907 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2021.00897]

[9] Delerablée C. Identity-based broadcast encryption with constant size ciphertexts and private keys. In: Proc. of the 13th Int'l Conf. on the Theory and Application of Cryptology and Information Security. Kuching: Springer, 2007. 200–215. [doi: 10.1007/978-3-540-76900-2_12]

[10] Boneh D, Boyen X. Efficient selective-ID secure identity-based encryption without random oracles. In: Proc. of the Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Interlaken: Springer, 2004. 223–238. [doi: 10.1007/978-3-540-24676-3_14]

[11] Waters B. Efficient identity-based encryption without random oracles. In: Proc. of the 24th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Aarhus: Springer, 2005. 114–127. [doi: 10.1007/11426639_7]

[12] Kim J, Susilo W, Au MH, Seberry J. Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext. IEEE Trans. on Information Forensics and Security, 2015, 10(3): 679–693. [doi: 10.1109/TIFS.2014.2388156]

[13] Waters B. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In: Proc. of the 29th Annual Int'l Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2009. 619–636. [doi: 10.1007/978-3-642-03356-8_36]

[14] Susilo W, Chen RM, Guo FC, Yang GM, Mu Y, Chow YW. Recipient revocable identity-based broadcast encryption: How to revoke some recipients in IBBE without knowledge of the plaintext. In: Proc. of the 11th ACM on Asia Conf. on Computer and Communications Security. Xi'an: ACM, 2016. 201–210. [doi: 10.1145/2897845.2897848]

[15] He K, Weng J, Liu JN, Liu JK, Liu W, Deng RH. Anonymous identity-based broadcast encryption with chosen-ciphertext security. In: Proc. of the 11th ACM on Asia Conf. on Computer and Communications Security. Xi'an: ACM, 2016. 247–255. [doi: 10.1145/2897845.2897879]

[16] Liu WR, Liu JW, Wu QH, Qin B, Li Y. Practical chosen-ciphertext secure hierarchical identity-based broadcast encryption. Int'l Journal of Information Security, 2016, 15(1): 35–50. [doi: 10.1007/s10207-015-0287-8]

[17] Ge AJ, Wei PW. Identity-based broadcast encryption with efficient revocation. In: Proc. of the 22nd IACR Int'l Conf. on Practice and Theory of Public-Key Cryptography. Beijing: Springer, 2019. 405–435. [doi: 10.1007/978-3-030-17253-4_14]

[18] Lai JC, Mu Y, Guo FC, Jiang P, Ma S. Identity-based broadcast encryption for inner products. The Computer Journal, 2018, 61(8): 1240–1251. [doi: 10.1093/comjnl/bxy062]

[19] Xu P, Jiao TF, Wu QH, Wang W, Jin H. Conditional identity-based broadcast proxy re-encryption and its application to cloud email. IEEE Trans. on Computers, 2016, 65(1): 66–79. [doi: 10.1109/TC.2015.2417544]

[20] Lai JC, Mu Y, Guo FC, Susilo W, Chen RM. Anonymous identity-based broadcast encryption with revocation for file sharing. In: Proc. of the 21st Australasian Conf. on Information Security and Privacy. Melbourne: Springer, 2016. 223–239. [doi: 10.1007/978-3-319-40367-0_14]

[21] Kim J, Camtepe S, Susilo W, Nepal S, Baek J. Identity-based broadcast encryption with outsourced partial decryption for hybrid security models in edge computing. In: Proc. of the 2019 ACM Asia Conf. on Computer and Communications Security. Auckland: ACM, 2019. 55–66. [doi: 10.1145/3321705.3329825]

[22] Zhang XF, Peng H. Blind signature scheme based on SM9 algorithm. Netinfo Security, 2019, 19(8): 61–67 (in Chinese with English abstract). [doi: 10.3969/j.issn.1671-1122.2019.08.009]

[23] Yang YT, Cai JL, Zhang XW, Yuan Z. Privacy preserving scheme in block chain with provably secure based on SM9 algorithm. Ruan Jian Xue Bao/Journal of Software, 2019, 30(6): 1692–1704 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5745.htm [doi: 10.13328/j.cnki.jos.005745]

[24] Wang S, Fang LG, Han LB, Liu HB. Fast implementation of SM9 digital signature and verification algorithms. Communications Technology, 2019, 52(10): 2524–2527 (in Chinese with English abstract). [doi: 10.3969/j.issn.1002-0802.2019.10.035]

[25] Wang MD, He WG, Li J, Mei R. Optimal design of R-ate pair in SM9 algorithm. Communications Technology, 2020, 53(9): 2241–2244 (in Chinese with English abstract). [doi: 10.3969/j.issn.1002-0802.2020.09.025]

[26] Xu SW, Ren XP, Yuan F, Guo CR, Yang S. A secure key issuing scheme of SM9. Computer Applications and Software, 2020, 37(1): 314–319 (in Chinese with English abstract).

[27] Zhang LY, Wu Q, Hu YP. Direct CCA secure identity-based broadcast encryption. In: Proc. of the 6th Int'l Conf. on Network and System Security. Wuyishan: Springer, 2012. 348–360. [doi: 10.1007/978-3-642-34601-9_26]

附中文参考文献:

[5] 刘潇, 刘魏然, 伍前红, 刘建伟. 选择密文安全的基于身份的广播加密方案. 密码学报, 2015, 2(1): 66–76. [doi: 10.13868/j.cnki.jcr.

© 中国科学院软件研究所 http://www.jos.org.cn

000061]
[8] 赖建昌, 黄欣沂, 何德彪. 一种基于商密SM9的高效标识广播加密方案. 计算机学报, 2021, 44(5): 897–907. [doi: 10.11897/SP.J.1016.2021.00897]
[22] 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(8): 61–67. [doi: 10.3969/j.issn.1671-1122.2019.08.009]
[23] 杨亚涛, 蔡居良, 张筱薇, 袁征. 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(6): 1692–1704. http://www.jos.org.cn/1000-9825/5745.htm [doi: 10.13328/j.cnki.jos.005745]
[24] 王松, 房利国, 韩炼冰, 刘鸿博. 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(10): 2524–2527. [doi: 10.3969/j.issn.1002-0802.2019.10.035]
[25] 王明东, 何卫国, 李军, 梅瑞. 国密SM9算法R-ate对计算的优化设计. 通信技术, 2020, 53(9): 2241–2244. [doi: 10.3969/j.issn.1002-0802.2020.09.025]
[26] 许盛伟, 任雄鹏, 袁峰, 郭春锐, 杨森. 一种关于SM9的安全密钥分发方案. 计算机应用与软件, 2020, 37(1): 314–319.

赖建昌(1988－), 男, 博士, 副教授, 主要研究领域为公钥密码学, 信息安全.

何德彪(1980－), 男, 博士, 教授, 博士生导师, CCF 高级会员, 主要研究领域为密码学, 信息安全.

黄欣沂(1981－), 男, 博士, 教授, 博士生导师, CCF 专业会员, 主要研究领域为公钥密码学, 信息安全.

宁建廷(1988－), 男, 博士, 教授, 主要研究领域为密码学, 信息安全.

© 中国科学院软件研究所 http://www.jos.org.cn