计算机科学
COMPUTER SCIENCE

基于国密算法SM9的加法同态加密方案

谢振杰, 刘奕明, 尹小康, 刘胜利, 张永光

引用本文

谢振杰, 刘奕明, 尹小康, 刘胜利, 张永光. 基于国密算法SM9的加法同态加密方案[J]. 计算机科学, 2025, 52(11): 408-414.

XIE Zhenjie, LIU Yiming, YIN Xiaokang, LIU Shengli, ZHANG Yongguang. Additively Homomorphic Encryption Scheme Based on Domestic Cryptographic Algorithm SM9 [J]. Computer Science, 2025, 52(11): 408-414.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.241100188

基于国密算法 SM9 的加法同态加密方案

谢振杰[1,2]　刘奕明[3]　尹小康[1]　刘胜利[1]　张永光[4,5]
1 信息工程大学网络空间安全教育部重点实验室　郑州 450001
2 中国人民解放军 78156 部队　重庆 400039
3 中国人民解放军 92330 部队　山东 青岛 266000
4 电磁空间安全全国重点实验室　浙江 嘉兴 314033
5 中国电子科技集团公司第三十六研究所　浙江 嘉兴 314033
(jsonxie@126.com)

摘　要　在云计算环境下,传统加密方案在保护数据机密性的同时,也使密文丧失了可计算性。同态加密解决了这一矛盾,已被广泛应用于数据聚合、安全多方计算、联邦学习等隐私计算领域。因此,以基于标识密码体制的国密算法 SM9 加密算法为基础,构造了具有加法同态性质的标识加密方案,细致推导了方案的正确性和加法同态性,从 q-BCAA1 和 DDH 困难问题出发证明了方案具有 IND-CPA 安全性,并对改进的消息恢复算法进行了详细描述。测试结果表明,提出的加法同态加密方案的加密效率相较于同类方案提升了 42%,解密效率提升了 20%～62%。

关键词:国密算法;SM9;加法同态加密;隐私计算
中图分类号　TP309.7

Additively Homomorphic Encryption Scheme Based on Domestic Cryptographic Algorithm SM9

XIE Zhenjie[1,2],LIU Yiming[3],YIN Xiaokang[1],LIU Shengli[1] and ZHANG Yongguang[4,5]
1 Key Laboratory of Cyberspace Security,Ministry of Education,Information Engineering University,Zhengzhou 450001,China
2 Troop 78156 of PLA,Chongqing 400039,China
3 Troop 92330 of PLA,Qingdao,Shandong 266000,China
4 National Key Laboratory of Electromagnetic Space Security,Jiaxing,Zhejiang 314033,China
5 The 36th Research Institute of China Electronics Technology Group Corporation,Jiaxing,Zhejiang 314033,China

Abstract　In the cloud computing environment,traditional encryption schemes not only protect data confidentiality but also cause the ciphertext to lose its computability. Homomorphic encryption solves this contradiction and has been widely applied in privacy computing fields such as data aggregation,secure multi-party computing,and federated learning. Based on the encryption algorithm of the domestic cryptographic algorithm SM9,an identity-based encryption scheme with additive homomorphism property is constructed. The correctness and additive homomorphism of the scheme are carefully derived. Starting from the q-BCAA1 and DDH difficulty problems,the scheme is proven to have IND-CPA security. And the improved message recovery algorithm is described in detail. Test results show that the encryption efficiency of the proposed additively homomorphic encryption scheme increases by 42% compared to the similar scheme,and the decryption efficiency increases by 20% to 62%.

Keywords　Domestic cryptographic algorithm,SM9,Additively homomorphic encryption,Privacy computing

1　引言

作为海量数据计算与管理的理想平台,云计算不仅使用户享受到弹性资源、实时共享和高可靠性,同时也引发了对数据隐私和安全性的担忧。在云计算场景下,加密是一种常见的数据隐私保护方式,然而,采用传统加密方案加密后的密文无法直接进行计算,用户必须对其进行解密操作,难以充分利用云环境强大的计算能力。而同态加密(Homomorphic Encryption)则很好地解决了这一痛点,因为同态加密的密文保留了原始数据的某种计算性质,直接对密文进行计算再解密,可以获得对原始数据计算的结果。云服务器参与同态计算,却无法得到原始数据,既实现了对云计算资源的利用,又保护

到稿日期:2024-11-28　返修日期:2025-03-11
基金项目:装备预先研究项目(30603010601)
This work was supported by the Equipment Pre Research Project(30603010601).
通信作者:尹小康(yxksjtu@sjtu.edu.cn)

了用户隐私和数据机密性。

同态加密一般分为全同态加密和部分同态加密两类。全同态加密(Fully Homomorphic Encryption，FHE)是指同时满足加法同态和乘法同态且不限制运算次数的加密算法，目前主流的 FHE 方案[1-8]大多基于容错学习(Learning With Errors，LWE)问题。文献[9]细致梳理了 FHE 领域十余年的研究进展；文献[10]总结了 2009 年以后的 FHE 方案并将其归纳为 4 条核心技术路线；文献[11]着重分析了软、硬件两个层面的 FHE 加速实现方法；文献[12]综述了多参与方下的 FHE 前沿进展。仅支持加法或乘法同态运算的加密方案为部分同态加密(Partially Homomorphic Encryption，PHE)，尽管其仅支持单一类型的运算，但通常具有比 FHE 更高的运算效率，在特定应用场景下更有实用性。具有代表性的 PHE 方案有 Paillier[13]，Twisted-ElGamal[14]，Exp-ElGamal[15]，BGN[16]等，此类方案在数据聚合[17]、安全多方计算[18]、联邦学习[19]等场景已有成熟的应用范例。本文提出的加法同态加密(Additively Homomorphic Encryption，AHE)方案就属于 PHE，其加法同态性质可表述为 $Enc(m_1) * Enc(m_2) = Enc(m_1 + m_2)$。

国密算法 SM9 是我国自主设计的基于标识的密码体制(Identity-Based Cryptography，IBC)，包含数字签名算法、密钥交换协议、密钥封装机制和加密算法[20-21]。IBC 将用户身份信息作为公钥，公钥的真实性无需通过第三方颁发的证书来确认，不用建立复杂的公钥基础设施(Public Key Infrastructure，PKI)。将 IBC 用于同态加密可节约更新密钥的时间开销。另外，SM9 基于椭圆曲线群上的双线性对，相对于 Paillier[13]等类型的公钥密码具有更强的安全性，达到同等安全强度所需的密钥更短，计算效率更高。

文献[22]提出了基于国密算法 SM2 和 SM9 的 AHE 方案，并进一步构造了具有门限解密性质的方案，其中基于 SM9 的 AHE 方案的解密耗时约为 Paillier 方案[13]的 1/6、Exp-ElGamal 方案[15]的 3/4。此外，同态加法的运算效率也有很大优势，但其安全性的证明过程与加密步骤不完全对应，且论证尚不充分。文献[23]是文献[22]团队的后续工作，他们针对基于椭圆曲线的 AHE 方案在解密过程中须求解的小指数椭圆曲线离散对数问题(Elliptic Curve Discrete Logarithm Problem，ECDLP)提出了 FastECDLP 算法，对计算和内存开销进行深度优化，确保在明文长度尽可能长时也可高效解密。该方案虽无法直接应用于基于 SM9 的 AHE 方案(因其不涉及双线性对)，但其优化时空开销的思路有重要的参考价值。文献[24]以 SM9 为基础设计的同态加密算法具有任意次密文加法和 1 次密文乘法同态性质，适合二次多项式的隐私计算，但该算法失去了标识密码特性，需要 PKI 作为支撑。

本文以基于 IBC 的国密算法 SM9 加密算法为基础，构造了具有加法同态性质的 IBC 加密方案，细致论证了方案的正确性、加法同态性和安全性，详细描述了改进后的消息恢复算法。理论分析和测试表明，本文提出的 AHE 方案相较于文献[22]基于 SM9 的同类方案，在加密和解密算法的效率上具有明显的优势。

2 基于标识的加法同态加密概述

本章描述证明方案安全性需用到的数学困难问题，以及基于 IBC 的 AHE 方案的系统模型和安全模型。

2.1 困难问题

令 P,Q 分别为群 G_1 和 G_2 的生成元，e 表示从 $G_1 \times G_2$ 到 G_T 的双线性对，群 G_1,G_2,G_T 的阶为 N，则在非对称双线性群上定义的 q-BCAA1 问题和 DDH 问题如下。

定义 1(q-Bilinear Collision Attack Assumption，q-BCAA1 问题) 对于未知的正整数 $a \in [1,N-1]$，给定 $q+1$ 个两两不同的正整数 $h_0,h_1,\cdots,h_q \in [1,N-1]$，以及元素 $(P,[a]P,Q,[a(h_1+a)^{-1}]Q,[a(h_2+a)^{-1}]Q,\cdots,[a(h_q+a)^{-1}]Q) \in G_1^{\,2} \times G_2^{\,q+1}$，计算 $e(P,[a(h_0+a)^{-1}]Q)$。

定义 2(Decisional Diffie-Hellman Problem，DDH 问题) 对于未知的正整数 $a,b,c \in [1,N-1]$，给定 $([a]P,[b]P,[c]P) \in G_1^3$，判断 $c=ab$ 是否成立。

若在多项式时间内求解上述问题的概率是可忽略的，则称该问题的困难性假设成立。

2.2 系统模型

典型的基于 IBC 的 AHE 方案通常由系统建立 Setup、用户加密私钥生成 KeyGen、加密 Encrypt、解密 Decrypt 和同态加法 HomoAdd 这 5 项算法构成。密钥生成中心(Key Generation Center，KGC)运行 Setup 算法完成系统初始化、运行 KeyGen 算法为用户生成加密私钥，加密者和解密者分别运行 Encrypt 和 Decrypt 算法，其他用户(通常是具有较强算力的服务器)运行 HomoAdd 算法。

(1)系统建立 $Setup(\lambda) \rightarrow (params,msk)$：由 KGC 运行的概率多项式时间(Probabilistic Polynomial Time，PPT)算法，输入安全参数 λ，输出系统公开参数 $params$ 和加密主私钥 msk。

以下算法的输入都包含 $params$，为简化描述，不再额外标注。

(2)用户加密私钥生成 $KeyGen(ID,msk) \rightarrow sk$：由 KGC 运行的确定性算法，输入用户身份标识 ID 和加密主私钥 msk，输出用户加密私钥 sk。

(3)加密 $Encrypt(M,ID) \rightarrow HC$：由加密者运行的 PPT 算法，输入待加密消息 M 和解密者的标识 ID，输出同态密文 HC。

(4)解密 $Decrypt(HC,sk) \rightarrow M/\perp$：由解密者运行的确定性算法，输入同态密文 HC 和解密者私钥 sk，解密成功则输出被加密消息 M，否则输出 $\perp$。

(5)同态加法 $HomoAdd(HC_1,HC_2,\cdots,HC_n) \rightarrow HC$：可由其他用户运行的确定性算法，输入有限个同态密文 $(HC_1,HC_2,\cdots,HC_n)$，输出经同态加法计算后的同态密文 HC。

一个合格的 AHE 方案，应满足正确性、加法同态性和安全性。正确性指对于合法的同态密文，成功解密的概率为 1。方案正确性和加法同态性的形式化表达如下：

$$\Pr\left[Decrypt(HC,sk)\rightarrow M_1+M_2+\cdots+M_n \left| \begin{array}{l} Setup(\lambda)\rightarrow(params,msk) \\ KeyGen(ID,msk)\rightarrow sk \\ Encrypt(M_1,ID)\rightarrow HC_1 \\ \cdots \\ Encrypt(M_n,ID)\rightarrow HC_n \\ HomoAdd(HC_1,HC_2,\cdots,HC_n)\rightarrow HC \end{array} \right. \right]=1$$

2.3 安全模型

机密性是各类加密方案最核心的安全性质。本文方案的机密性，以选择明文攻击下的不可区分性（Indistinguishability Under Chosen-Plaintext Attack，IND-CPA）安全模型来定义。

定义 3（IND-CPA） 该性质由挑战者 C 与 PPT 敌手 A 之间的游戏来定义，游戏过程分为以下 4 个阶段。

（1）初始化。挑战者 C 调用 Setup 生成系统公开参数 $params$ 和加密主私钥 msk，将 $params$ 发送给敌手 A。

（2）私钥询问。A 询问身份标识 ID，C 调用 KeyGen 生成对应的用户加密私钥 sk 返回给 A。

（3）挑战。A 向 C 提供 2 个等长的消息 (M_0^*, M_1^*) 和解密者标识 ID^*，要求 A 从未询问过 ID^* 的加密私钥。C 随机选择 $b\in\{0,1\}$，再调用 $Encrypt(M_b^*, ID^*)$ 生成同态密文 HC^* 返回给 A。

（4）猜测。A 输出 $b'\in\{0,1\}$，如果 $b'=b$，则 A 赢得游戏。

定义 A 赢得该游戏的优势为 $Adv_A^{\text{IND-CPA}}=\left|\Pr[b'=b]-\frac{1}{2}\right|$。如果对于任意 PPT 敌手 A，该优势是可以忽略的，则称该方案是 IND-CPA 安全的。

3 基于 SM9 的加法同态加密方案构造

基于 IBC 的 AHE 方案通常由系统建立、用户加密私钥生成、加密、解密和同态加法 5 项算法构成，并且满足正确性、加法同态性和安全性 3 项性质。本文的符号含义与 SM9 国标[20-21]一致，G_1 和 G_2 是椭圆曲线加法循环群，P_1 和 P_2 分别是群 G_1 和 G_2 的生成元，G_T 是乘法循环群（其元素均为有限域 12 次扩域上的元素），$e(a,b)$ 表示从 $G_1\times G_2$ 到 G_T 的双线性对，$[k]P$ 表示椭圆曲线点 P 的 k 倍（即椭圆曲线标量乘），$x\parallel y$ 表示 x 与 y 的字节串拼接，H_1 是将任意长度比特串映射到 $[1,N-1]$ 范围内整数的哈希函数。

3.1 系统建立 Setup

首先，KGC 产生随机数 $ke\in[1,N-1]$ 作为加密主私钥，计算群 G_1 中的元素 $P_{\text{pub-e}}=[ke]P_1$ 作为加密主公钥，则加密主密钥对为 $(ke,P_{\text{pub-e}})$。KGC 秘密保存 ke，公开 $P_{\text{pub-e}}$。KGC 选择并公开大小为 1B 的加密私钥生成函数识别符 hid。

3.2 用户加密私钥生成 KeyGen

用户 A 的标识为 ID_A，为产生用户 A 的加密私钥 de_A，KGC 首先在有限域 F_N 上计算 $t_1=H_1(ID_A\parallel hid,N)+ke$，若 $t_1=0$ 则需重新产生系统加密主密钥，并更新已有用户的加密私钥；否则计算 $t_2=ke\cdot t_1^{-1}$，再计算 $de_A=[t_2]P_2$，最后将加密私钥 de_A 通过安全途径传递给用户 A。

3.3 加密算法 Encrypt

设用户 A 发送给用户 B 的消息为比特串 M，用户 A 通过以下步骤将明文 M 转换成只能由用户 B 解密的密文 C。

（1）计算群 G_1 中的元素 $Q_B=[H_1(ID_B\parallel hid,N)]P_1+P_{\text{pub-e}}$；

（2）产生随机数 $r\in[1,N-1]$；

（3）计算群 G_1 中的元素 $C_1=[r+M]Q_B$；

（4）计算群 G_T 中的元素 $g=e(P_{\text{pub-e}},P_2)$；

（5）计算群 G_T 中的元素 $C_2=g^r$；

（6）将 C_1，C_2 转换成比特串并拼接，即 $C=C_1\parallel C_2$，C 为输出密文。

在上述加密步骤中，对于特定的系统参数，步骤（4）产生的 g 是常量，可预先计算并保存，实际加密过程可省略步骤（4）；另外，如果用户 B 是常用联系人，可提前计算并保存 Q_B，省略步骤（1）。

3.4 解密算法 Decrypt

用户 B 收到用户 A 发送的密文 C 后进行解密，步骤如下。

（1）将 C 拆分成比特串 C_1 和 C_2，将 C_1 转换成椭圆曲线上的点，并检验其是否为椭圆曲线群 G_1 中的元素，若不是则报错并停止解密；

（2）计算群 G_T 中的元素 $w=e(C_1,de_B)$；

（3）将 C_2 转换成 G_T 中的元素，计算 $g^M=w\times C_2^{-1}$；

（4）通过算法 2（见 3.6 节）从 g^M 恢复明文 M'。

3.5 同态加法 HomoAdd

令发送给用户 B 的 2 个消息分别为 M 和 M'，密文分别为 C 和 C'，需生成加法同态密文 C''。计算步骤如下。

（1）拆分密文 $C=C_1\parallel C_2$，$C'=C_1'\parallel C_2'$，将 C_1 和 C_1' 转换成群 G_1 中的元素，将 C_2 和 C_2' 转换成群 G_T 中的元素；

（2）计算群 G_1 中的元素 $C_1''=C_1+C_1'$；

（3）计算群 G_T 中的元素 $C_2''=C_2\times C_2'$；

（4）将 C_1'' 和 C_2'' 转换成比特串并拼接，即 $C''=C_1''\parallel C_2''$，C'' 为同态密文。

解密者将同态密文 C'' 输入解密算法，即可得到同态消息 $M''=M+M'$。上述步骤以 2 个密文为例进行描述，对于多个消息，只要解密者相同，都可通过累加 C_1 和累乘 C_2 来进行同态加法计算。而解密者不同的密文，无法进行同态加法计算，即使执行上述同态加法，其结果也无法被任何用户解密。

此外，同一密文多次相加，可通过同态标量乘进行简化：计算群 G_1 中的元素 $C_1'=[r]C_1$ 与群 G_T 中的元素 $C_2'=C_2^r$，$C'=C_1'\parallel C_2'$ 即为消息 $M'=r\cdot M$ 对应的同态密文。

3.6 消息恢复算法

AHE 方案的解密过程通常包含求解指数较小的离散对数问题，本文方案解密算法的步骤（4）即从群 G_T 元素 g^M 中恢复消息 M。ECDLP 现有攻击方法有 Pohlig-Hellman 方法、BSGS 方法、Pollard 方法等，对于一般曲线的离散对数问题，尚未发现亚指数级计算复杂度的一般攻击方法[20]。ECDLP

的困难性是椭圆曲线群上双线性对安全性的重要基础，同样意味着群 G_T 上的离散对数问题难解。

本文设计的消息恢复算法旨在利用预计算、以空间换时间等思路，以及群 G_T 的性质，实现群 G_T 中小指数离散对数问题的快速求解。具体实现方法为：预先计算当 M 值为 $1\sim2^{24}$（大小为 3B）时 g^M 的一系列哈希值（见算法 1），令 g_0 为 $M=2^{25}$ 时的 g^{-M} 值，不断执行 $g^M=g^M\times g_0$ 并计算 g^M 和 g^{-M} 的哈希值，尝试查表恢复 M（见算法 2）。令 $hash(\cdot)$ 表示哈希函数，$conj(\cdot)$ 表示群 G_T 的共轭运算（在群 G_T 中，可用开销更小的共轭运算实现求逆[25]），$sqr(\cdot)$ 表示群 G_T 的平方运算，生成预计算数据的伪代码如算法 1 所示。

算法 1 预计算数据生成算法

输入：G_T 中的元素 g

输出：字典 M_dict，G_T 中的元素 g_0

```
1. M_dict[hash(g)]←1, t←g
2. for i from 2 to 2^24 do
3.     t ← t×g
4.     M_dict[hash(t)] ← i
5. end for
6. g0←conj(sqr(t))
```

算法 1 输出的字典 *M_dict* 用于从 g^M 的哈希值查表恢复不超过 3B 的 M，而 g_0 用于将超过 3B 的 M 压缩至 3B。当哈希值大小为 8B 时，保存字典 *M_dict* 需要 $8\text{B}\times2^{24}=128\text{ MB}$。解密者加载 *M_dict* 和 g_0，通过执行算法 2 完成解密算法的步骤(4)。假设 M 不超过 5B，通过查表从 g^M 恢复消息 M 的伪代码描述如算法 2 所示。

算法 2 通过查表从 g^M 恢复消息 M

输入：字典 M_dict，G_T 中的元素 g_0，g^M

输出：原始消息 M

```
1. if hash(g^M) in M_dict do
2.     M ← M_dict[hash(g^M)]
3.     return
4. end if
5. t ← g^M×g0
6. for i from 1 to 2^15 do
7.         if hash(conj(t)) in M_dict do
8.         M ← i×2^25−M_dict[hash( conj(t) )]
9.     break
10.    end if
11.    if hash(t) in M_dict do
12.            M ← M_dict[hash(t)]+i×2^25
13.            break
14.    end if
15.    t ← t×g0
16. end for
```

通常限制单次加密的消息 M 不超过 4B，此时算法 2 最多需要群 G_T 中的 128 次乘法、128 次共轭和 256 次哈希运算。而文献[22]的 g_0 为 $M=2^{24}$ 时的 g^{-M} 值，恢复 4B 的 M 最多需要群 G_T 中的 255 次乘法和 256 次哈希运算。另外，当密文经多次同态加法计算后，恢复 M' 所需迭代次数更多。当 M' 为 5B 时，算法 2 最多需迭代 $2^{16-1}=32\,768$ 次，而文献[22]中的方法最多需迭代 $2^{16}=65\,536$ 次。

总之，本文方案利用群 G_T 中开销更小的共轭运算使乘法次数减半，改进后的消息恢复算法将显著提升解密效率。

4 方案性质推导与证明

本章通过理论推导，证明所提方案的正确性和加法同态性质，并以形式化的安全分析来证明方案的安全性。

4.1 正确性

如果用户 A 和用户 B 诚实地执行加解密步骤，且密文 C 在传输过程中未被篡改，记 $h_B=H_1(ID_B\|hid,N)$，则解密的正确性来自以下推导：

$$
\begin{aligned}
g&=e(P_{\text{pub-e}},P_2)\\
&=e([ke]P_1,P_2)\\
&=e(P_1,P_2)^{ke}\\
g^M&=w\times C_2^{-1}\\
&=e(C_1,de_B)\times(g^r)^{-1}\\
&=e([r+M]Q_B,[ke(h_B+ke)^{-1}]P_2)\times g^{-r}\\
&=e([r+M]([h_B]P_1+P_{pu\,b\text{-}e}),[ke(h_B+ke)^{-1}]P_2)\times\\
&\quad e(P_{\text{pub-e}},P_2)^{-r}\\
&=e([r+M]([h_B]P_1+[ke]P_1),[ke(h_B+ke)^{-1}]P_2)\times\\
&\quad e([ke]P_1,P_2)^{-r}\\
&=e([(r+M)(h_B+ke)]P_1,[ke(h_B+ke)^{-1}]P_2)\times\\
&\quad e([ke]P_1,P_2)^{-r}\\
&=e(P_1,P_2)^{(r+M)ke}\times e(P_1,P_2)^{-ke\cdot r}\\
&=e(P_1,P_2)^{ke\cdot M}
\end{aligned}
$$

因此，用户 B 计算得到的 g^M 是以常量 g 为底数、消息 M 为指数的幂值，其中 g^M 和 g 均为群 G_T 中的元素，用户 B 可通过算法 2 从 g^M 中求 M。

4.2 加法同态性

以 2 个密文进行同态加法计算为例，同态密文为 C_1'' 和 C_2''，解密者为用户 B，同态消息 $M''=M+M'$，加法同态性推导如下：

$$
\begin{aligned}
C_1''&=C_1+C_1'=[r+M+r'+M']Q_B\\
C_2''&=C_2\times C_2'=g^r\times g^{r'}=g^{r+r'}\\
g^{M'}&=e(C_1'',de_B)\times C_2''^{-1}=g^{r+M+r'+M'}\times g^{-r-r'}=g^{M+M'}
\end{aligned}
$$

因此，用户 B 计算得到的 $g^{M''}$ 是以常量 g 为底数、同态消息 M'' 为指数的幂值，用户 B 可通过算法 2 从 $g^{M''}$ 中求 M''。

由于该同态加法的计算过程无需任何秘密信息，可由任意第三方完成，参与计算的第三方也无法从计算过程和结果中得到有关明文的任何有用信息，只有加密时指定的解密者用户 B 能完成最终解密，从而保证了同态计算的隐私性。

4.3 机密性

本文 AHE 方案的安全性，主要来自 q-BCAA1 问题和 DDH 问题的难解性。下文通过形式化的安全规约方法，在 IND-CPA 安全模型下证明本文方案的机密性。

定理 1 假设哈希函数 H_1 是随机预言机，如果 q-BCAA1 问题和群 G_1 上的 DDH 问题难解，则本文方案是 IND-CPA 安全的。

证明：假设在 IND-CPA 安全模型下，存在一个 PPT 敌手 A 能以不可忽略的优势 ε 区分所选消息的密文，则可构建模拟器 S 解决 DDH 问题。S 以 1 个 q-BCAA1 问题实例(P,Q,$[a]P$,$(h_1,[a(h_1+a)^{-1}]Q)$,$(h_2,[a(h_2+a)^{-1}]Q)$,…,$(h_q,[a(h_q+a)^{-1}]Q)$)和 1 个群 G_1 上的 DDH 问题实例($[a]P$,$[b]P$,$[c]P$)作为输入，控制随机预言机并运行 A，进行以下操作。

(1)初始化。S 设 $P_1=P$，$P_2=Q$，$P_{pub\text{-}e}=[a]P$。以上公开参数均可通过问题实例得到，只有加密主私钥 $ke=a$ 是隐式的。S 建立初始为空的列表 L，以四元组(i,ID_i,$H_1(ID_i)$,de_i)的形式记录对 H_1 及私钥的询问/应答。

(2)哈希询问。H_1 是由 S 控制的随机预言机，A 可在任意阶段向 S 发起 H_1 询问，假设询问次数(相同询问不重复计数，下同)为 $q_{H_1}=q$。为方便描述，省略 H_1 的输入项 hid 和 N。令第 i 个 H_1 询问为 ID_i，若 L 中已有 ID_i 对应项，则 S 根据 L 的记录来应答；否则，S 将 $H_1(ID_i)=h_i$ 作为应答，并在 L 中记录(i,ID_i,$H_1(ID_i)$,#)，# 表示对应私钥暂未被询问。

(3)私钥询问。在此阶段，A 自适应地向 S 发起私钥询问，约定询问次数小于 q。A 询问 ID_i 的加密私钥，令(i,ID_i,$H_1(ID_i)$,#/de_i)为 L 中对应的记录(若 L 中无此项，则先向 H_1 询问)，若已记录私钥 de_i，则 S 应答 de_i；否则，$H_1(ID_i)=h_i$，S 在 q-BCAA1 问题实例中找到 h_i 对应的 $[a(h_i+a)^{-1}]Q$ 作为私钥 de_i 进行应答，并在 L 中记录(i,ID_i,$H_1(ID_i)$,de_i)。

(4)挑战。A 选定解密者标识为 ID^*，并向 S 提供 2 个等长的消息(M_0^*,M_1^*)，要求 A 从未询问过 ID^* 的私钥。令(i,ID^*,h^*,#)为 L 中对应的记录(若 L 中无此项，则先向 H_1 询问)，S 产生随机比特 $\beta\in\{0,1\}$，利用问题实例计算：

$$C_1^*=[h^*]([b]P)+[c]P+[M_\beta\cdot h^*]P+[M_\beta]([a]P)$$

$$C_2^*=e([c]P,Q)$$

S 将 $C^*=C_1^*\|C_2^*$ 返回给 A。

上述密文模拟过程中，S 将问题实例中的 b 隐式地设为加密步骤(2)的随机数 r^*，当 $c=ab$ 时，有：

$$Q^*=[H_1(ID^*)]P_1+P_{pub\text{-}e}=[h^*]P+[a]P$$

$$\begin{aligned}C_1^*&=[r^*+M_\beta]Q^*\\&=[b+M_\beta]([h^*]P+[a]P)\\&=[h^*]([b]P)+[c]P+[M_\beta\cdot h^*]P+[M_\beta]([a]P)\end{aligned}$$

$$C_2^*=e(P_{pub\text{-}e},P_2)^{r^*}=e([a]P,Q)^b=e([c]P,Q)$$

此时，在 A 看来，C_1^* 和 C_2^* 是与正常加密算法的输出无法区分的密文。

(5)猜测。A 将猜测结果 $\beta'\in\{0,1\}$ 发送给 S。c' 表示 S 对 c 值的猜测，若 $\beta=\beta'$，令 $c'=ab$；若 $\beta\neq\beta'$，令 $c'=r$。若 $c=c'$，则 S 猜对了该 DDH 问题实例。

为推导 S 破解 DDH 问题的优势，进行如下定义：

$\alpha=1:c=ab$

$\alpha=0:c=r$

当 $\alpha=1$ 时，C^* 理论上能被解密，定义此时 A 获胜的优势为：

$$Adv_A^{IND\text{-}CPA}=\Pr[\beta=\beta'\mid\alpha=1]-1/2=\varepsilon$$

当 $\alpha=0$ 时，C^* 理论上无法解密，不能为 A 的猜测提供任何依据，故 A 猜测正确的概率为 1/2。则 S 破解 DDH 问题的优势可推导如下：

$$\begin{aligned}Adv_S^{DDH}&=\Pr[c=c']-1/2\\&=\Pr[\beta=\beta'\mid\alpha=1]\cdot\Pr[\alpha=1]+\Pr[\beta\neq\beta'\mid\alpha=0]\cdot\Pr[\alpha=0]-1/2\\&=(\varepsilon+1/2)\cdot1/2+1/2\cdot1/2-1/2\\&=\varepsilon/2\end{aligned}$$

综上，在 q-BCAA1 问题困难性假设成立的基础上，如果存在 PPT 敌手 A 能以不可忽略的优势 ε 区分所选消息的密文，则可以构造模拟器 S 以不可忽略的优势 $\varepsilon/2$ 破解 DDH 问题，这与 DDH 问题的困难性假设相矛盾。因此，本文所提基于 SM9 的 AHE 方案是 IND-CPA 安全的。

5 性能分析与实验

本章对所提方案的计算和通信开销进行理论分析及实验测试，并与文献[22]基于 SM9 的 AHE 方案展开对比。

5.1 性能分析

对于计算开销，考虑用户加密私钥生成、加密、同态加法、解密(不含消息恢复)和消息恢复算法中各项耗时运算的次数(可预计算的步骤未计入)，分析结果如表 1 所列。其中，SM_1 和 SM_2 分别表示群 G_1 和 G_2 的标量乘；A_1 表示群 G_1 的加法；BP 表示双线性对；M,C,E 分别表示群 G_T 的乘法、共轭和幂；HA 表示哈希运算(包含文献[22]的 KDF 和 MAC 运算)。其余运算(如有限域 F_N 的加法、乘法和模逆等)耗时与上述运算至少相差 2 个数量级，为突出重点已将其忽略。表 1 中“消息恢复”列出的是在最坏情况下恢复 1 个 4B 消息的开销。

表 1 AHE 方案的计算开销

Table 1 Calculation overhead of AHE schemes

方案	私钥生成	加密	同态加法	解密	消息恢复
文献[22]	$HA+SM_2$	$2SM_1+A_1+2E+M+3HA$	A_1+M	$BP+C+M+2HA$	$255M+256HA$
本文方案	$HA+SM_2$	$2SM_1+A_1+E+HA$	A_1+M	$BP+C+M$	$128M+128C+256HA$

相较于文献[22]方案，本文方案的加密算法将群 G_T 的乘法和幂各减少 1 次，消息恢复算法的优势已在 3.6 节阐述。二者的用户加密私钥生成和同态加法具有相同的计算开销，如果不考虑文献[22]方案在解密单个消息时保留了 KDF 和 MAC 运算，二者的解密开销基本一致。

对于通信开销，考虑系统公钥、用户私钥和密文的比特位数，结果如表 2 所列。其中，$|G_1|$,$|G_2|$,$|G_T|$,$|F_N|$ 分别表示对应群(或域)元素的比特位数。具体而言，对于 SM9 国标规范使用的 256b 的 BN 曲线[20]，$|G_1|=512$ b，$|G_2|=1024$ b，$|G_T|=3072$ b，$|F_N|=256$ b。SM9 国标已做规定的 P_1 和 P_2

等公共参数未计入系统公钥。

表 2 AHE 方案的通信开销

Table 2 Communication overhead of AHE schemes

方案	系统公钥	用户私钥	密文
文献[22]	$\|G_1\|$	$\|G_2\|$	$\|G_1\|+\|G_T\|+\|F_N\|$
本文方案	$\|G_1\|$	$\|G_2\|$	$\|G_1\|+\|G_T\|$

由表 2 可见，本文方案与文献[22]方案的通信开销基本一致。文献[22]方案在密文中保留的 c_3 仅适用于单个密文解密时的 MAC 校验，无法校验同态计算后的密文，考虑到 AHE 方案的设计目标是方便密文参与同态加法计算，本文省略了 MAC 校验步骤，密文长度更短。

5.2 实验测试

本文基于国密算法开源 Python 库 hggm[26]，采用 SM9 国标规定的参数设置[20]，通过 Python 编程实现了本文方案的各项算法以及文献[22]基于 SM9 的 AHE 方案，并对各方案算法的性能进行测试。实验计算机的配置如表 3 所列。

表 3 实验配置

Table 3 Experimental configuration

项目	配置
设备类型	PC
操作系统	Windows 10 64 位
CPU	Intel Core i3-10110U(2 核心 4 线程)
内存	8 GB LPDDR3 2133 MHz
硬盘	SAMSUNG MZVLB512HBJQ-000L7
Python 版本	3.7.1

除算法 1 执行 10 次外，其余各项测试均执行 500 次，取平均值作为有效数据。设定单个消息 M 的大小不超过 4 B，经同态加法计算得到的消息 M'' 大小不超过 5 B。

首先测试单个消息的加密和解密，然后从密文集合随机抽取 2，16，256 个密文进行同态加法计算，最后对产生的同态密文进行解密。表 4 列出了上述各算法的单次执行耗时。

表 4 各项算法的测试结果

Table 4 Test results of each algorithm

(ms)

算法	本文方案	文献[22]
加密(单个消息)	5.80	8.24
解密(单个消息)	31.41	37.63
同态加法(2 个消息)	0.14	0.14
解密同态密文(2 个消息)	43.23	56.97
同态加法(16 个消息)	2.06	2.02
解密同态密文(16 个消息)	197.48	313.23
同态加法(256 个消息)	33.73	33.97
解密同态密文(256 个消息)	2744.46	4444.78

由表 4 数据可知，相较于文献[22]方案，本文方案的加密算法有 42%的性能优势，主要原因是其减少了 1 次群 G_T 中以消息 M 为指数的幂运算；解密耗时随消息长度增加而延长，本文方案在解密单个消息和解密 2，16，256 个消息的同态密文时，较文献[22]方案的性能提升幅度分别为 20%，32%，59%，62%，主要原因是消息恢复算法中有一半群 G_T 的乘法被替换为开销更小的共轭运算，且消息恢复开销占总开销的比例随消息数值的增大而增大，故被解密消息越大，本文方案的性能优势越明显；二者同态加法的效率相当，且同态加法的耗时与同态加法次数成正比(同态加法次数＝消息数－1)。

此外，执行算法 1 生成 128 MB 预计算数据的耗时为 1792.39 s；首次解密前需加载该数据并转换为字典，耗时约 9.36 s。然而，预计算数据是通用的，可由服务器生成并提供下载，只要 KGC 不更换加密主密钥对，该数据长期有效。理论上，当用户下行带宽为 100 Mb/s 时，下载该数据耗时为 10.24 s；带宽为 10 Mb/s 时，下载耗时为 102.4 s。二者均显著短于执行算法 1，因此用户仅需在离线环境下自行生成该数据。

结束语 本文基于国密算法 SM9，设计了一种具有加法同态性质的加密方案，为标识密码体制下的同态加密应用提供了基于国密算法的选项。通过理论推导，证明了本文方案的正确性和加法同态性，以形式化的安全分析证明了本文方案具有 IND-CPA 安全性。通过理论分析、编程实现和性能对比测试，体现了本文方案的有效性、实用性，以及相对于文献[22]方案在加密和解密算法上的性能优势。本文方案具有较高的加密、解密和同态加法计算效率，对于提高基于标识密码的加法同态加密计算性能，具有理论价值和实践意义。然而，目前同类方案的解密效率主要受限于群 G_T 上的离散对数困难问题，明文一般不超过 4B，相较于一般加密方案的效率仍有数量级上的差距，下一步将重点研究解密算法，使得在明文长度超过 4B 时也能高效解密。本文方案实现与测试的全部 Python 代码，已在“码云”平台开源[26]。

参 考 文 献

[1] GARG S, GUPTA D. Efficient round optimal blind signatures [C]// Proceedings of the EUROCRYPT 2014. 2014: 477-495.

[2] CHILLOTTI I, GAMA N, GEORGIEVA M, et al. TFHE: Fast fully homomorphic encryption over the torus [J]. Journal of Cryptology, 2020, 33(1): 34-91.

[3] JOYE M, PAILLIER P. Blind rotation in fully homomorphic encryption with extended keys [C]// Proc eedings of the 2022 Cyber Security, Cryptology, and Machine Learning. 2022: 1-18.

[4] XIANG B W, ZHANG J, DENG Y, et al. Fast blind rotation for bootstrapping FHEs [C]// Proceedings of the 2023 Annual International Cryptology Conference. 2023: 3-36.

[5] CHEN H, CHILLOTTI I, SONG Y Z. Improved bootstrapping for approximate homomorphic encryption [C]// Proceedings of the EUROCRYPT 2019. 2019: 34-54.

[6] KANG H, LEE J, LEE Y, et al. Bootstrapping on SEAL [EB/OL]. https://eprint.iacr.org/2020/1594.pdf.

[7] HAN K, KI D. Better bootstrapping for approximate homomorphic encryption [C]// Proceedings of the 2020 Cryptographers Track at the RSA Conference. 2020: 364-390.

[8] JUNG W, KIMW, AHN J H, et al. Over 100x faster bootstrapping in fully homomorphic encryption through memory-centric optimization with GPUs [EB/OL]. https://eprint.iacr.org/2021/508.pdf.

[9] BAI L F, ZHU Y F, LI Y J, et al. Research progress of fully homomorphic encryption [J]. Journal of Computer Research and Development, 2024, 61(5): 3069-3087.

[10] DAI Y R, ZHANG J, XIANG B W, et al. Overview on the research status and development route of fully homomorphic encryption technology [J]. Journal of Electronics & Information

Technology, 2024, 46(5): 1774-1789.
[11] BIAN S, MAO R, ZHU R Q, et al. A survey on software-hardware acceleration for fully homomorphic encryption[J]. Journal of Electronics & Information Technology, 2024, 46(5): 1790-1805.
[12] XU K X, WANG L P. Research progress on multi-party fully homomorphic encryption[J]. Journal of Cryptologic Research, 2024, 11(4): 719-739.
[13] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes [C]// Proceedings of the EUROCRYPT 1999. 1999: 223-238.
[14] CHEN Y, MA X C, TANG C, et al. PGC: Decentralized confidential payment system with auditability [C]// Proceedings of the 2020 European Symposium on Research in Computer Security. 2020: 591-610.
[15] CRAMER R, GENNARO R, SCHOENMAKERS B. A secure and optimally efficient multi-authority election scheme[J]. European Transactions on Telecommunications, 1997, 8(5): 481-490.
[16] BONEH D, GOH E J, NISSIM K. Evaluating 2-DNF formulas on ciphertexts [C]// Proceedings of the 2nd Theory of Cryptography Conference. 2005: 325-341.
[17] GUAN Z T, SI G L, ZHANG X S, et al. Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities[J]. IEEE Communications Magazine, 2018, 56(7): 82-88.
[18] MOHAMMADALI A, HAGHIGHI M S. A privacy-preserving homomorphic scheme with multiple dimensions and fault tolerance for metering data aggregation in smart grid [J]. IEEE Transactions on Smart Grid, 2021, 12(6): 5212-5220.
[19] YANG Q, LIU Y, CHEN T J, et al. Federated machine learning: Concept and applications[J]. ACM Transactions on Intelligent Systems and Technology, 2019, 10(2): 1-19.
[20] GB/T 38635.1—2020, Identity-based cryptographic algorithms SM9-Part 1: General[S]. Beijing: China Standard Press, 2020.
[21] GB/T 38635.2—2020, Identity-based cryptographic algorithms SM9-Part 2: Algorithms [S]. Beijing: China Standard Press, 2020.
[22] TANG F, LING G W, SHAN J Y. Additive homomorphic encryption schemes based on SM2 and SM9[J]. Journal of Cryptologic Research, 2022, 9(3): 535-549.
[23] TANG F, LING G W, CAI C C, et al. Solving small exponential ECDLP in EC-based additively homomorphic encryption and applications[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 3517-3530.
[24] QIN T H, WANG Z B, LIU Y, et al. Homomorphic encryption scheme based on commercial cryptography SM9[J]. Journal of Information Securyity Research, 2024, 10(6): 513-518.
[25] WANG M D, HE W G, LI J, et al. Optimal design of R-ate pair in SM9 algorithm [J]. Communications Technology, 2020, 53(9): 2241-2244.
[26] BASDDSA. hggm—Domestic cryptographic algorithm SM2/SM3/SM4/SM9/ZUC—Complete source code for Python implementation [EB/OL]. (2024-07-11) [2024-08-15]. https://gitee.com/basddsa/hggm.

XIE Zhenjie, born in 1995, Ph.D candidate. His main research interests include cloud security and cryptography applications.

YIN Xiaokang, born in 1993, Ph.D, lecturer. His main research interests include network security, binary code analysis and machine learning.

(责任编辑:何杨)