计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.241200049

基于国密算法 SM9 的签密方案

谢振杰[1,2]　罗友强[1,3]　赵方方[1]　任　帅[1]
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 32158 部队　新疆 喀什 844000
(jsonxie@126.com)

摘　要　签密是一种结合了数字签名与加密的密码学技术,通过同时执行这 2 项功能,减少了计算量和通信开销。国密算法 SM9 作为一款我国自研的标识密码算法,不仅安全高效,还能有效降低公钥基础设施的建设成本以及证书管理开销。针对现有签密方案在计算效率和签密消息长度方面存在的不足,提出了一种基于国密算法 SM9 的签密方案。通过创新设计签密私钥元组,将密钥和签名的信息合并封装,有效降低计算复杂度并压缩签密消息长度。在随机预言机模型下,分别基于 Gap-q-BDHI 和 q-SDH 困难问题,证明了所提方案具有 IND-CCA 和 EUF-CMIA 安全性。经过理论分析和实验测试,证实了所提方案的签密和解密验证效率较现有同类方案分别提升 67%和 62%,而签密消息长度减少 25%。

关键词:签密;国密算法;SM9;基于标识的密码
中图分类号　TP309.7

Signcryption Scheme Based on SM9 Domestic Cryptographic Algorithm

XIE Zhenjie[1,2],LUO Youqiang[1,3],ZHAO Fangfang[1] and REN Shuai[1]
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 32158 of PLA,Kashi,Xinjiang 844000,China

Abstract　Signcryption is a cryptographic technique that combines digital signature and encryption,reducing computational and communication overhead compared to executing them separately. The SM9 domestic cryptographic algorithm,developed independently in China as an identity-based cryptographic algorithm,is not only secure and efficient,but also effectively lowers the costs associated with public key infrastructure construction and certificate management. Addressing the inefficiencies in computational performance and signcryptext length in existing schemes,a new signcryption scheme based on the SM9 algorithm is proposed. By innovatively designing the signcryption secret key tuple,and combining the key and signature information into a single element,the scheme significantly reduced computational complexity and compressed the signcryptext length. Under the random oracle model,the scheme is proven to have IND-CCA and EUF-CMIA security based on the Gap-q-BDHI and q-SDH hard problems,respectively. Theoretical analysis and experimental tests confirme that the proposed scheme improved signcryption and decryption verification efficiency by 67% and 62%,respectively,compared to the existing similar scheme,while reducing the signcryptext length by 25%.

Keywords　Signcryption,Domestic cryptographic algorithm,SM9,Identity-based cryptography

现代密码学是网络安全的基石,而物联网、云计算、区块链等前沿技术的发展应用,均离不开加密和数字签名等密码技术的坚实支撑。加密能有效保护数据机密性,数字签名则可实现身份认证,确保数据的完整性以及签名者的不可否认性。通常,系统根据安全需求选择合适的密码技术,而数字签名和加密经常同时出现,先签名后加密的传统做法会导致计算开销和密文长度增加,时空效率尚有优化空间。在 1997 年的美密会上,Zheng 首次提出了签密这一概念[1]。签密融合了公钥密码和对称加密,通过一次运算同时完成数字签名和加密的功能,只有签密者指定的接收者才能正确解密并验证签名的有效性。相较于传统的先签名后加密的技术,签密技术能显著减少计算和通信开销。

传统的公钥密码通常依赖公钥基础设施(Public Key Infrastructure,PKI),通过证书绑定公钥和特定用户的联系。但 PKI 的建设和运维成本不菲,且证书的申请、验证和管理易导致系统性能瓶颈。在基于标识的密码(Identity-based Cryptography,IBC)体系下,公钥的验证不依赖证书,而是以能唯一标识用户身份的邮箱、手机号、证件号等字符串作为公钥。IBC 一定程度上避免了对第三方证书机构的可信度依赖,是一类具有广阔应用前景的公钥密码。国密算法 SM9 是

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:赵方方(fangfangzhaowlc@163.com)

我国自主研发的标识密码，涵盖了数字签名算法、密钥交换协议、密钥封装机制和加密算法[2-3]。SM9 基于椭圆曲线构造，除了具备 IBC 的优势，相比 RSA 等传统公钥密码算法，在提供同等安全强度的同时，所需的密钥长度更短，计算效率更高，有利于增强系统的整体安全性和性能。近年来，基于 SM9 算法设计的密码方案不断扩展，包括环签名[4-6]、可搜索加密[7]、分层标识加密[8-10]、广播加密[10-11]和容错加密[12]等领域的方案相继问世，展示了 SM9 出色的性能及其在各种密码应用领域的拓展潜力。

本文基于国密算法 SM9 的数字签名和加密算法，设计了一种基于标识的签密方案。本方案的系统初始化和公共参数与 SM9 数字签名算法一致，通过重新设计签密私钥元组，将密钥和签名的信息合并封装进同一群元素，有效降低了计算复杂度并压缩了签密消息长度。分别基于 Gap-q-BDHI 和 q-SDH 困难问题假设，在随机预言机模型下依次证明了本方案的机密性和不可伪造性，其符合一般签密方案的安全模型。理论分析和实验测试的综合评估结果表明，与现有方案相比，本方案在签密与解密验证算法方面均展现了更佳的计算性能以及更精简的签密消息。

1 相关工作

自从 Zheng[1]于 1997 年提出签密概念后，后续出现的早期签密方案通常依赖 PKI 体系。2002 年，文献[13]首次基于标识密码设计了一种签密方案，但该方案采用先加密后签名的顺序，无法实现语义安全。文献[14]针对以上问题，提出一种更安全高效的标识签密方案。文献[15]提出的标识签密方案继续改进了计算效率，并且在随机预言机模型下证明了方案满足 IND-CCA 安全性，以及在给定标识和选择消息攻击下(Selective Identity and Chosen-message Attacks，sID-CMA)满足存在性不可伪造。文献[16]首次提出了一个在标准模型下可证明安全的标识签密方案，然而，文献[17]指出其同样无法实现语义安全，并提出在保证不可伪造性的同时实现语义安全的改进设计。文献[18]提出了一个在标准模型下具有强不可伪造性的标识签密方案。文献[19]提出的标识签密方案通过增加计算量和签密消息长度，实现了标准模型下的完全安全。文献[20]同样针对文献[16]方案的安全性问题进行改进，并且在计算效率上有所提高。文献[21]针对物联网环境设计了一种可证明安全的标识签密方案。文献[22-24]分别基于格密码、属性和三因素认证设计了签密方案。

2021 年，文献[25]首次将国密算法 SM9 应用于签密方案设计，该方案的计算和通信开销与近年基于国际标识密码的签密方案相当，且其在随机预言机模型下具有 IND-CCA 和 EUF-CMIA 安全性。文献[26]结合 SM9 密钥封装机制和文中 SM9 代理签名方案，设计了一种基于 SM9 的代理签密方案，但相比分别执行代理签名和加密，该方案优化幅度尚不明显。文献[27]调整了文献[25]方案的系统公钥和用户私钥生成方式，描述了改动后的基于 SM9 的签密算法，以适配所提出的基于签密的可认证密文检索方案。文献[28]针对车联网中的用户隐私保护问题，提出了基于 SM9 的环签密方案，并在随机预言机模型下证明了其安全性，相较于现有环签密方案，该方案有效优化了计算效率。总之，当前基于 SM9 算法设计的签密方案较少，现有方案对数字签名和加密算法的融合还比较简单，仍有较大优化空间。

在签密方案的安全性证明方面，文献[29]于 2000 年首次提出并证明了分叉引理(Forking Lemma)，为证明数字签名方案的不可伪造性提供了有效途径。文献[30]将分叉引理扩展至一般的基于身份的签名体制。2018 年，文献[31]基于 Gap-q-BCAA1 困难问题假设，给出了 SM9 密钥交换协议、密钥封装机制和加密算法的安全性证明，SM9 密钥封装机制在随机预言机模型下被证明是 IND-CCA 安全的。2021 年，文献[32]在随机预言机模型下，基于 q-SDH 困难问题假设，给出了 SM9 数字签名算法的 EUF-CMIA 安全性证明；基于 q-BDHI困难问题假设，证明改进的 Twin-SM9 密钥封装机制满足 IND-CCA 安全性。这些研究成果，以及现有签密方案的安全性分析，为签密方案的机密性和不可伪造性证明提供了重要的理论基础和方法支撑。

2 基于标识的签密概述

2.1 符号含义

本文的符号含义与 SM9 国标[2-3]基本一致。G_1，G_2 是椭圆曲线加法循环群；P_1，P_2 分别是群 G_1，G_2 的生成元，且满足 $P_1=\psi(P_2)$(ψ 为 G_2 到 G_1 的同态映射)，G_T 是乘法循环群(其元素均为有限域 12 次扩域上的元素)；群 G_1，G_2，G_T 的阶均为素数 N。$[k]U$ 表示群 G_1 或 G_2 中元素 U 的 k 倍(即椭圆曲线上点的标量乘)，e 表示从 $G_1\times G_2$ 映射到 G_T 的双线性对，$x\parallel y$ 表示 x 与 y 的字节串拼接，H_1 和 H_2 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。为简化符号并与方案公开参数 P_1，P_2 有所区分，在困难问题的实例中，也使用 P，Q 表示群 G_1，G_2 的生成元。

2.2 困难问题

在非对称双线性群上定义以下困难问题。

定义 1(q-Strong Diffie-Hellman Problem，q-SDH 问题) 对于未知的正整数$a\in[1,N-1]$，给定 $q+2$ 个元素$(P,Q,[a]Q,[a^2]Q,\cdots,[a^q]Q)\in G_1\times G_2^{q+1}$，计算$\left(c,\left[\frac{1}{c+a}\right]P\right)$，其中 c 是$[1,N-1]$范围内的任意整数。

定义 2(Decision Bilinear Inversion Diffie-Hellman Problem，DBIDH 问题) 对于未知的正整数 $a,b,r\in[1,N-1]$，区分$(P_1,P_2,[a]P_i,[b]P_j,e(P_1,P_2)^{\frac{b}{a}})$和$(P_1,P_2,[a]P_i,[b]P_j,e(P_1,P_2)^r)$，其中 $i,j\in\{1,2\}$。

定义 3(q-Bilinear Diffie-Hellman Inversion Problem，q-BDHI 问题) 对于未知的正整数 $a\in[1,N-1]$，给定 $q+2$ 个元素$(P,Q,[a]Q,[a^2]Q,\cdots,[a^q]Q)\in G_1\times G_2^{q+1}$，计算 $e(P,Q)^{\frac{1}{a}}$。

定义 4(Gap-q-BDHI 问题) 对于未知的正整数 $a\in[1,N-1]$，给定 $q+2$ 个元素$(P,Q,[a]Q,[a^2]Q,\cdots,[a^q]Q)\in G_1\times G_2^{q+1}$和 DBIDH 确定算法，计算$e(P,Q)^{\frac{1}{a}}$。

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。上述问题的困难性可以规约到 G_1，G_2，G_T 上离散对数问题的困难性，它们是基于双线性对的标识密码体制的安全性的重要基础。

2.3 系统模型

一个典型的基于标识的签密方案，通常由系统建立 Setup、用户签密私钥生成 KeyGen、签密消息生成 Signcrypt 和解

密验证 Unsigncrypt 这 4 项算法构成。方案包含 3 种角色：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 算法为用户生成签密私钥；签密者（Signcryptor）和接收者（Receiver）分别运行 Signcrypt 和 Unsigncrypt 算法。

1）系统建立 Setup(λ)→($params$,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 $params$ 和签密主私钥 msk。

以下算法的输入都包含 $params$，为简化描述，不再额外标注。

2）用户签密私钥生成 KeyGen(ID,msk)→sk：由 KGC 运行的确定性算法，输入用户身份标识 ID 和签密主私钥 msk，输出用户签密私钥 sk。

3）签密消息生成 Signcrypt(M,ID_R,sk_S)→SC：由签密者（标识为 ID_S）运行的 PPT 算法，输入待签密消息 M、接收者的标识 ID_R 和签密者签密私钥 sk_S，输出签密消息 SC。

4）解密验证 Unsigncrypt(SC,ID_S,sk_R)→$M/\perp$：由接收者（标识为 ID_R）运行的确定性算法，输入签密消息 SC、签密者的标识 ID_S 和接收者签密私钥 sk_R，验证通过则输出被签密消息 M，否则输出 $\perp$（$\perp$ 表示解密失败或验证不通过）。

方案的正确性要求如下：对于合法的签密消息，成功解密并通过验证的概率为 1；对于非法的签密消息，验证通过的概率是可忽略的。

$$\Pr\left[\text{Unsigncrypt}(SC,ID_S,sk_R)=M \,\middle|\, \begin{matrix}\text{Setup}(\lambda)\to(params,msk)\\ \text{KeyGen}(ID,msk)\to sk\\ \text{Signcrypt}(M,ID_R,sk_S)\to SC\end{matrix}\right]=1$$

2.4 安全模型

签密包含加密和签名，故应同时具备公钥加密算法和数字签名算法的安全性，即合格的签密方案应保护数据的机密性，并确保签名的不可伪造性。基于标识的签密方案，须满足以下两个特性：1）在自适应选择密文攻击下的不可区分性（Indistinguishability Against Adaptive Chosen-ciphertext Attacks，IND-CCA）；2）在自适应选择消息和身份攻击下的存在性不可伪造（Existential Unforgeability Under Adaptive Chosen-message-and-identity Attack，EUF-CMIA）。

定义 5（IND-CCA） 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 5 个阶段。

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

2）询问 1。A 以自适应的方式向 C 发起私钥询问、消息签密询问和解密验证询问。

（1）私钥询问。A 询问身份标识 ID，C 调用 KeyGen 生成对应的用户签密私钥 sk 并返回。

（2）消息签密询问。A 询问消息 M、签密者标识 ID_S 和接收者标识 ID_R，C 调用 KeyGen 生成签密者签密私钥 sk_S，再调用 Signcrypt 生成签密消息 SC 并返回。

（3）解密验证询问。A 询问签密消息 SC、签密者标识 ID_S 和接收者标识 ID_R，C 调用 KeyGen 生成接收者签密私钥 sk_R，再调用 Unsigncrypt 并返回算法输出。

3）挑战。A 向 C 提供 2 个等长的消息（$M_0{}^*$，$M_1{}^*$）、签密者标识 ID_S^* 和接收者标识 ID_R^*，要求 A 从未询问过 ID_R^* 的签密私钥。C 调用 KeyGen 生成 ID_S^* 对应的签密私钥 sk_S^*，随机选择 $b\in\{0,1\}$，再调用 Signcrypt($M_b{}^*$，ID_R^*，sk_S^*）生成签密消息 SC^* 并返回给 A。

4）询问 2。A 可继续以自适应的方式向 C 发起私钥询问、消息签密询问和解密验证询问，C 的应答方式同询问 1，但要求 A 不能询问 ID_R^* 的签密私钥，也不能对签密消息 SC^* 发起解密验证询问。

5）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 $Adv_A{}^{\text{IND-CCA}}=\left|\Pr[b'=b]-\frac{1}{2}\right|$。如果对于任意 PPT 敌手 A，该优势是可以忽略的，则称该签密方案是 IND-CCA 安全的。

定义 6（EUF-CMIA） 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 3 个阶段。

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

2）询问。A 以自适应的方式向 C 发起私钥询问、消息签密询问和解密验证询问。

（1）私钥询问。A 询问身份标识 ID，C 调用 KeyGen 生成对应的用户签密私钥 sk 并返回。

（2）消息签密询问。A 询问消息 M、签密者标识 ID_S 和接收者标识 ID_R，C 调用 KeyGen 生成签密者签密私钥 sk_S，再调用 Signcrypt 生成签密消息 SC 并返回。

（3）解密验证询问。A 询问签密消息 SC、签密者标识 ID_S 和接收者标识 ID_R，C 调用 KeyGen 生成接收者签密私钥 sk_R，再调用 Unsigncrypt 并返回算法输出。

3）伪造。A 伪造签密者（标识为 ID_S^*）对消息 M^* 的签密消息 SC^*（接收者标识为 ID_R^*），要求 A 从未询问过 ID_S^* 的签密私钥，也从未询问过（ID_S^*，ID_R^*）对 M^* 的签密消息。如果 A 伪造的签密消息 SC^* 能在 Unsigncrypt 算法下通过验证并输出原始消息 M^*，则 A 赢得游戏。

定义 A 赢得该游戏的优势为 $Adv_A^{\text{EUF}}=\Pr[\text{Unsigncrypt}(SC^*,ID_S^*,sk_R^*)=M^*]$。如果对于任意 PPT 敌手 A，该优势是可以忽略的，则称该签密方案是 EUF-CMIA 安全的。

3 基于 SM9 的签密方案构造

3.1 系统建立 Setup

KGC 产生随机数 $ks\in[1,N-1]$ 作为签密主私钥，计算群 G_2 中的元素 $P_{\text{pub-s}}=[ks]P_2$ 作为签密主公钥，则签密主密钥对为（ks，$P_{\text{pub-s}}$）。KGC 秘密保存 ks，公开 $P_{\text{pub-s}}$。KGC 选择并公开大小为 1B 的签密私钥生成函数识别符 hid。

3.2 用户签密私钥生成 KeyGen

用户 A 的标识为 ID_A，为产生用户 A 的签密私钥 sk_A，KGC 首先在有限域 F_N 上计算 $t_1=H_1(ID_A\|hid,N)+ks$，若 $t_1=0$ 则需重新产生系统签密主密钥，并更新已有用户的签密私钥；否则计算 $t_2=ks\cdot t_1^{-1}$，再计算 $ds_A=[t_2]P_1$，$de_A=[ks\cdot t_2]P_2$，最后将签密私钥元组 $sk_A=(ds_A,de_A)$ 通过安全途径传递给用户 A。

3.3 签密消息生成算法 Signcrypt

设待签密的消息为比特串 M，签密者的标识为 ID_S，接收者的标识为 ID_R，生成签密消息 SC 的运算步骤如下：

1)预先计算群 G_T 中的元素 $g=e(P_1,P_{\text{pub-s}})$；

2)计算整数 $v_S=H_1(ID_S\|hid,N)$ 和 $v_R=H_1(ID_R\|hid,N)$；

3)产生随机数 $r\in[1,N-1]$，计算群 G_T 中的元素 $\omega=g^r$；

4)计算整数 $h=H_2(M\|\omega,N)$；

5)计算整数 $l=(r-h) \bmod N$，若 $l=0$ 则返回步骤 3)；

6)计算群 G_1 中的元素 $S=[l(1-v_R\cdot v_S^{-1})]ds_S+[l\cdot v_R\cdot v_S^{-1}]P_1$；

7)计算 $K=KDF(S\|\omega\|ID_R,klen)$；

8)计算 $C=Enc_K(M)$；

9)输出签密消息 $SC=(C,h,S)$。

步骤 7)中的 KDF 表示密钥派生函数，整数 $klen$ 表示密钥的比特位数。步骤 8)中的 $Enc_K(M)$ 表示使用某种对称加密算法以密钥 K 加密消息 M(下文的 $Dec_K(M)$ 表示对应的解密算法)，例如采用基于 KDF 的序列密码或国密分组密码算法 SM4。本方案不限定具体的对称密码算法。

3.4 解密验证算法 Unsigncrypt

接收者 ID_R 收到签密者 ID_S 发送的签密消息 $SC'=(C',h',S')$ 后，运算步骤如下：

1)预先计算群 G_T 中的元素 $g=e(P_1,P_{\text{pub-s}})$；

2)检验 $h'\in[1,N-1]$ 和 $S'\in G_1$ 是否均成立，若不完全成立则验证不通过；

3)计算整数 $v_S=H_1(ID_S\|hid,N)$ 和 $v_R=H_1(ID_R\|hid,N)$；

4)计算群 G_2 中的元素 $T=[1-v_S\cdot v_R^{-1}]de_R+[v_S\cdot v_R^{-1}]P_{\text{pub-s}}$；

5)计算群 G_T 中的元素 $\omega'=e(S',T)\cdot g^{h'}$；

6)计算 $K'=KDF(S'\|\omega'\|ID_R,klen)$；

7)计算 $M'=Dec_{K'}(C')$；

8)计算整数 $h_2=H_2(M'\|\omega',N)$；

9)检验 $h_2=h'$ 是否成立，若成立则验证通过并输出解密后的消息 M'，否则验证不通过。

4 方案性质推导与证明

4.1 正确性

如果签密者和接收者诚实地执行上述运算步骤，且签密消息 SC 在传输过程中未被篡改，即 $C=C'$，$h=h'$，$S=S'$，则方案的正确性来自以下推导：

$$\begin{aligned}\omega'&=e(S',T)\cdot g^{h'}\\&=e([l(1-v_R\cdot v_S^{-1})]ds_S+[l\cdot v_R\cdot v_S^{-1}]P_1,[1-v_S\cdot v_R^{-1}]de_R+[v_S\cdot v_R^{-1}]P_{\text{pub-s}})\cdot g^h\\&=e\left(\left[l\frac{(v_S-v_R)ks}{v_S(v_S+ks)}+l\frac{v_R(v_S+ks)}{v_S(v_S+ks)}\right]P_1,\left[\frac{(v_R-v_S)ks^2}{v_R(v_R+ks)}+\frac{v_S(v_R+ks)ks}{v_R(v_R+ks)}\right]P_2\right)\cdot g^h\\&=e\left(\left[l\frac{v_R+ks}{v_S+ks}\right]P_1,\left[\frac{(v_S+ks)ks}{v_R+ks}\right]P_2\right)\cdot g^h\\&=g^l\cdot g^h=g^{r-h}\cdot g^h=g^r=\omega\end{aligned}$$

故 $K=K'$，双方正确执行加解密算法后有 $M=M'$，因此 $h_2=h=h'$。本签密方案的正确性证毕。

4.2 机密性

通过形式化的安全规约方法，在 IND-CCA 安全模型下证明所提签密方案的机密性。

定理 1 假设哈希函数 H_1，H_2 以及密钥派生函数 KDF 是随机预言机，如果 Gap-q-BDHI 问题是困难的，则本文所提签密方案在 IND-CCA 安全模型下是安全的。

证明：假设在 IND-CCA 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 Gap-q-BDHI 问题。S 以 1 个 q-BDHI 问题实例 $(P,Q,[a]Q,[a^2]Q,\cdots,[a^q]Q)\in G_1\times G_2^{q+1}$ 作为输入，掌握可解决 DBIDH 问题的预言机 O_{DBIDH}，控制随机预言机并运行 A，进行以下操作。

1)初始化。令 ψ 为 G_2 到 G_1 的同态映射，满足 $[a^i]P=\psi([a^i]Q)$，$0\leqslant i\leqslant q$；模拟器 S 随机选择 q 个互不相同的数 w^*，$w_1,w_2,\cdots,w_{q-1}\in[1,N-1]$，令 $f(x)=\prod_{i=1}^{q-1}(w_i+x-w^*)$，$f(x)$ 是 $Z_N[x]$ 中次数为 $q-1$ 的多项式；设 $P_1=[f(a)]P$，$P_2=[f(a)]Q$，$P_{\text{pub-s}}=[(a-w^*)f(a)]Q$。除了签密主私钥 $ks=a-w^*$ 是隐式的，其余公开参数可通过问题实例和所选参数计算得到。约定签密者和接收者的标识不相同。

为适当简化证明，将加解密过程中的密钥派生与对称密码合并为模 2 加法，即 Signcrypt 算法步骤 7)和步骤 8)合并为 $C=KDF(S\|\omega\|ID_B,mlen)\oplus M$，Unsigncrypt 算法步骤 6)和步骤 7)合并为 $M'=C'\oplus KDF(S'\|\omega'\|ID_B,mlen)$，$mlen$ 为待签密消息 M 的比特长度。如此简化后，可避免对对称密码算法安全性的考虑，而不影响安全证明的有效性。

2)哈希询问。H_1，H_2，KDF 是由 S 控制的随机预言机，询问次数(相同询问不重复计数)分别为 q_{H_1}，q_{H_2}，q_{KDF}，假设 $q_{H_1}=q-1$。为方便描述，省略 H_1，H_2，KDF 的输入项 hid，N，$mlen$。开始询问前，S 随机选择 $i^*\in[1,q_{H_1}]$，并建立 3 个初始为空的哈希列表 L_1，L_2，L_3，分别记录对 H_1，H_2，KDF 的询问和应答。A 可以在任意阶段向 S 发起以下哈希询问。

(1)H_1 询问。令第 i 个 H_1 询问为 ID_i，若 L_1 中已有 ID_i 对应项，则 S 根据 L_1 的记录来应答。否则，当 $i=i^*$ 时，设 $H_1(ID_i)=w^*$；$i\neq i^*$ 时，设 $H_1(ID_i)=w_i$。S 将 $H_1(ID_i)$ 作为该询问的应答，并在 L_1 中记录 $(i,ID_i,H_1(ID_i))$。

(2)H_2 询问。令第 i 个 H_2 询问为消息 M_i 和群 G_T 中的元素 y_i，若 L_2 中已有其对应项，则 S 根据 L_2 的记录来应答。否则，S 随机选择 $Y_i\in[1,N-1]$，将 $H_2(M_i\|y_i)=Y_i$ 作为该询问的应答，并在 L_2 中记录 (i,M_i,y_i,Y_i)。

(3)KDF 询问。令第 i 个 KDF 询问为群 G_1 中的元素 S_i、群 G_T 中的元素 y_i 和标识 ID_{R_i}，若 L_3 中已有其对应项，则 S 根据 L_3 的记录来应答。否则，S 随机生成 $K_i\in\{0,1\}^{\text{mlen}}$，将 $KDF(S_i\|y_i\|ID_{R_i})=K_i$ 作为该询问的应答，并在 L_3 中记录 (i,S_i,y_i,ID_{R_i},K_i)。

3)询问 1。在此阶段，A 以自适应的方式向 S 发起私钥询问、消息签密询问和解密验证询问。

(1)私钥询问。A 询问身份标识 ID_i 的签密私钥，令 $(i,ID_i,H_1(ID_i))$ 为 L_1 中对应的记录。若 $i=i^*$，则中止。否

则，$H_1(ID_i)=w_i$，令 $f_i(x)=(x-w^*)\prod_{j=1,j\neq i}^{q-1}(w_j+x-w^*)$，则 $f_i(x)$ 是 $Z_N[x]$ 中次数为 $q-1$ 的多项式，$(x-w^*)f_i(x)$ 是 $Z_N[x]$ 中次数为 q 的多项式，用问题实例和所选参数可计算 ID_i 的签密私钥 $ds_i=[f_i(a)]P$，$de_i=[(a-w^*)f_i(a)]Q$。由于：

$$ds_i=[f_i(a)]P=\left[\frac{(a-w^*)f(a)}{w_i+a-w^*}\right]P=\left[\frac{a-w^*}{w_i+a-w^*}\right]P_1$$

$$de_i=[(a-w^*)f_i(a)]Q=\left[\frac{(a-w^*)^2f(a)}{w_i+a-w^*}\right]Q=\left[\frac{(a-w^*)^2}{w_i+a-w^*}\right]P_2$$

因此 $sk_i=(ds_i,de_i)$ 是一个有效的签密私钥。

(2)消息签密询问。A 指定签密者标识为 ID_S、接收者标识为 ID_R，询问 ID_S 对消息 M 的签密。若 $ID_S\neq ID_{i^*}$，S 计算 ID_S 对应的私钥 ds_S，再调用 Signcrypt 生成签密消息 SC 并返回。否则，S 随机选择 $h\in[1,N-1]$，$S\in G_1$，计算 ID_R 对应的私钥 de_R，执行 Unsigncrypt 步骤 4)和步骤 5)得到 $\omega\in G_T$，在 L_2 中记录 $(len(L_2)+1,M,\omega,h)$（$len(L_2)$ 表示当前列表 L_2 的项数，若曾向 H_2 询问过 (M,ω) 且 $H_2(M\|\omega)\neq h$，需重新选择 h 再计算），计算 $C=KDF(S\|\omega\|ID_R)\oplus M$，向 A 返回 $SC=(C,h,S)$。

(3)解密验证询问。A 指定签密者标识为 ID_S、接收者标识为 ID_R，询问 ID_R 对签密消息 $SC=(C,h,S)$ 的解密验证结果。若 $ID_R\neq ID_{i^*}$，S 计算 ID_R 对应的私钥 de_R，再调用 Unsigncrypt 并返回算法输出。否则，记 $w_S=H_1(ID_S)\in\{w_1,w_2,\cdots,w_{q-1}\}$，$S$ 按以下步骤执行：

①遍历列表 L_1 查找 ID_S，若未向 H_1 询问过 ID_S 则返回 $\perp$ 并结束，否则执行步骤②；

②遍历列表 L_2，查询满足 $Y_i=h$ 的记录 (i,M_i,y_i,Y_i)，若不存在则返回 $\perp$ 并结束，否则执行步骤③；

③对于尚未执行的记录 (i,M_i,y_i,h) 执行步骤④，如果全部执行完毕后仍没有返回结果，返回 $\perp$ 并结束；

④计算 $K_i=C\oplus M_i$，遍历列表 L_3 查找 (S,y_i,ID_R,K_i) 所在记录，若不存在则返回步骤③，否则执行步骤⑤；

⑤向 O_{DBIDH} 询问 $\left(P_1,P_{\text{pub-s}},\left[\frac{a\cdot f(a)}{w_S+a-w^*}\right]P,S,y_i\cdot g^{-h}\right)$，若 O_{DBIDH} 返回 1，则向 A 返回 M_i 作为解密结果，否则返回步骤③。

预言机 O_{DBIDH} 可解决 2.2 节定义 2 描述的 $i=j=1$ 时的 DBIDH 问题，主要用于确认签密消息 SC 的有效性。向 O_{DBIDH} 询问形如 $(P_1,P_2,[a]P_1,[b]P_1,y)\in G_1\times G_2\times G_1{}^2\times G_T$ 的 5 元组，若 $y=e((P_1,P_2)^{\frac{b}{a}}$，则 O_{DBIDH} 返回 1，否则 O_{DBIDH} 返回 0。

若 A 能成功求解 ID_S 的私钥 ds_S 并生成有效的 $SC=(C,h,S)$，必定在执行 Signcrypt 算法的过程中正确发起 H_1，H_2，KDF 询问，且相关参数能通过 O_{DBIDH} 的验证。记 Signcrypt 步骤 3)的随机数为 r，则 L_2 中必有 $y_i=\omega=g^r$，又 $H_1(ID_R)=w^*$，$H_1(ID_R)+ks=w^*+a-w^*=a$，O_{DBIDH} 询问中的 $\left[\frac{a\cdot f(a)}{w_S+a-w^*}\right]P,S,y_i\cdot g^{-h}$ 可推导如下：

$$\left[\frac{af(a)}{w_S+a-w^*}\right]P=\left[\frac{a}{w_S+a-w^*}\right]P_1$$

$$S=\left[(r-h)\left(1-\frac{H_1(ID_R)}{H_1(ID_S)}\right)\right]ds_S+\left[\frac{(r-h)H_1(ID_R)}{H_1(ID_S)}\right]P_1$$

$$=\left[(r-h)\frac{H_1(ID_R)+ks}{H_1(ID_S)+ks}\right]P_1$$

$$=\left[\frac{(r-h)a}{w_S+a-w^*}\right]P_1$$

$$e\left(\left[\frac{(r-h)a}{w_S+a-w^*}\Big/\frac{a}{w_S+a-w^*}\right]P_1,P_{\text{pub-s}}\right)$$

$$=e([r-h]P_1,P_{\text{pub-s}})=g^{r-h}=g^r\cdot g^{-h}=y_i\cdot g^{-h}$$

因此，当且仅当 SC 可正确解密时，O_{DBIDH} 返回 1。通过上述推导，即使 S 不掌握接收者 ID_{i^*} 的私钥，也可利用随机预言机的询问记录和 O_{DBIDH}，成功模拟解密验证过程。

4)挑战。A 选定签密者标识为 ID_S^*、接收者标识为 ID_R^*，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_R^* 的签密私钥。若 $ID_R^*\neq ID_{i^*}$，则中止。否则，有 $H_1(ID_R^*)=w^*$，记 $w_S^*=H_1(ID_S^*)\in\{w_1,w_2,\cdots,w_{q-1}\}$，$S$ 随机选择 r'，$h^*\in[1,N-1]$，利用问题实例和所选参数计算 $S^*=\left[\frac{r'\cdot f(a)}{w_S^*+a-w^*}\right]P$，生成与 (M_0^*,M_1^*) 等长的随机比特串 R，将模拟的签密消息 $SC^*=(R,h^*,S^*)$ 返回给 A。

S^* 可视为以随机数 $r^*=\frac{r'}{a}+h^*$ 模拟生成，因为：

$$S^*=\left[(r^*-h^*)\left(1-\frac{w^*}{w_S^*}\right)\right]ds_S^*+\left[\frac{(r^*-h^*)w^*}{w_S^*}\right]P_1$$

$$=\left[\frac{(r^*-h^*)a}{w_S^*+a-w^*}\right]P_1$$

$$=\left[\frac{r'\cdot f(a)}{w_S^*+a-w^*}\right]P$$

所以，在 A 看来，在执行解密步骤（Unsigncrypt 步骤 6））前，模拟的 SC^* 与正常签密消息无法区分。

5)询问 2。A 可继续以自适应的方式向 S 发起私钥询问、消息签密询问和解密验证询问，S 的应答方式同询问 1，但要求 A 不能询问 ID_R^* 的签密私钥，也不能对 SC^* 发起解密验证询问。

6)猜测。A 输出猜测结果 $b'\in\{0,1\}$。

S 忽略 A 的猜测，如果 A 成功伪造 ID_R^* 对应的私钥 de_R^*，则在调用 Unsigncrypt 的过程中，有：

$$T^*=\left[1-\frac{w_S^*}{w^*}\right]de_R^*+\left[\frac{w_S^*}{w^*}\right]P_{\text{pub-s}}$$

$$=\left[\frac{(w_S^*+a-w^*)(a-w^*)}{a}\right]P_2$$

$$=\left[\frac{(w_S^*+a-w^*)(a-w^*)f(a)}{a}\right]Q$$

$$\omega^*=e(S^*,T^*)\cdot g^{h^*}$$

$$=e\left(\left[\frac{r'\cdot f(a)}{w_S^*+a-w^*}\right]P,\left[\frac{(w_S^*+a-w^*)(a-w^*)f(a)}{a}\right]Q\right)\cdot g^{h^*}$$

$$=e\left(P,\left[\frac{r'(a-w^*)f^2(a)}{a}\right]Q\right)\cdot g^{h^*}$$

L_3 中必有 1 项记录包含 $y_i=\omega^*$（$1\leqslant i\leqslant q_{\mathrm{KDF}}$），记其为 y^*；令 $\frac{r'(x-w^*)f^2(x)}{x}F(x)+\frac{d}{x}$，其中 $F(x)$ 是 $Z_N[x]$ 中次数为 $2q-2$ 的多项式，d 是非零整数；又令 $F(x)=F_1(x)\cdot x^{q-1}+F_2(x)$，其中 $F_1(x)$ 和 $F_2(x)$ 均为 $Z_N[x]$ 中次数为 $q-1$ 的多项式，$F_1(x)$ 和 $F_2(x)$ 的各项系数和 d 均可通过所选

参数计算。则可计算：

$$\left(\frac{y^*}{e([a^{q-1}]P,[F_1(a)]Q)\cdot e(P,[F_2(a)]Q)\cdot g^{h^*}}\right)^{\frac{1}{d}}$$
$$=\left(\frac{e\left(P,\left[\frac{r'(a-w^*)f^2(a)}{a}\right]Q\right)\cdot g^{h^*}}{e(P,[F(a)]Q)\cdot g^{h^*}}\right)^{\frac{1}{d}}$$
$$=\left(\frac{e\left(P,\left[F(a)+\frac{d}{a}\right]Q\right)}{e(P,[F(a)]Q)}\right)^{\frac{1}{d}}$$
$$=e\left(P,\left[\frac{d}{a}\right]Q\right)^{\frac{1}{d}}$$
$$=e(P,Q)^{\frac{1}{a}}$$

作为 Gap-q-BDHI 问题实例的一个解。

以下是对S成功模拟概率和破解 Gap-q-BDHI 问题优势的分析。首先，只有当 A 所挑战的接收者标识 ID_R^* 在 L_1 中的序号恰好为 i^* 时，S才能成功模拟，其概率为 $1/q_{H_1}$，而 q_{H_1} 是多项式级别且有上界，所以此概率是不可忽略的。其次，在成功模拟的基础上，根据假设，A 能以不可忽略的优势 ε 区分所选消息的密文，则 A 将以 ε 概率向 KDF 发起包含 y^* 的挑战询问。令 (i,S^*,y_i,ID_R^*,K_i) 为 L_3 中可能包含 y^* 的记录，逐一向 O_{DBIDH} 询问 $\left(P_1,P_{\text{pub-s}},\left[\frac{a\cdot f(a)}{ws^*+a-w^*}\right]P,S^*,y_i\cdot g^{-h^*}\right)$，当 O_{DBIDH} 返回 1 时，有 $y_i=y^*$（推导过程同解密验证询问），即只要 L_3 中包含挑战询问，S可在 O_{DBIDH} 的帮助下找到 y^*。因此，若假设成立，则S能以 ε/q_{H_1} 的优势成功求解 Gap-q-BDHI 问题，该优势同样是不可忽略的。然而，这与 Gap-q-BDHI 问题的困难性假设相矛盾，故本签密方案在 IND-CCA 安全模型下是安全的。

4.3 不可伪造性

通过形式化的安全规约方法，在 EUF-CMIA 安全模型下证明所提签密方案的不可伪造性。

定理 2 假设哈希函数 H_1，H_2 以及密钥派生函数 KDF 是随机预言机，如果 q-SDH 问题是困难的，则本文所提签密方案在 EUF-CMIA 安全模型下是安全的。

证明：假设在 EUF-CMIA 安全模型下，存在一个 PPT 敌手 A 能以不可忽略的优势 ε 伪造本方案签密，则可构建模拟器S解决 q-SDH 问题。S以 1 个 q-SDH 问题实例 $(P,Q,[a]Q,[a^2]Q,\cdots,[a^q]Q)\in G_1\times G_2{}^{q+1}$ 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。除了签密主私钥隐式地设为 $ks=a$，公开参数 $P_{\text{pub-s}}=[af(a)]Q$，其余与 4.2 小节相同。

2）哈希询问。与 4.2 节相同。

3）询问。在此阶段，A 以自适应的方式向S发起私钥询问、消息签密询问和解密验证询问。

（1）私钥询问。A 询问身份标识 ID_i 的签密私钥，令 $(i,ID_i,H_1(ID_i))$ 为 L_1 中对应的记录。若 $i=i^*$，则中止。否则，有 $H_1(ID_i)=w_i$，令 $f_i(x)x\prod_{j=1,j\neq i}^{q-1}(w_j+x)$，则 $f_i(x)$ 是 $Z_N[x]$ 中次数为 $q-1$ 的多项式，$xf_i(x)$ 是 $Z_N[x]$ 中次数为 q 的多项式，利用问题实例和所选参数可计算 ID_i 的签密私钥 $ds_i=[f_i(a)]P$，$de_i=[af_i(a)]Q$。由于：

$$ds_i=[f_i(a)]P=\left[\frac{a\cdot f(a)}{w_i+a}\right]P=\left[\frac{a}{w_i+a}\right]P_1$$
$$de_i=[af_i(a)]Q=\left[\frac{a^2\cdot f(a)}{w_i+a}\right]Q=\left[\frac{a^2}{w_i+a}\right]P_2$$

所以 $sk_i=(ds_i,de_i)$是一个有效的签密私钥。

（2）消息签密询问。与 4.2 节相同。

（3）解密验证询问。与 4.2 节相同。

4）伪造。A 指定签密者标识为 ID_S^*、接收者标识为 ID_R^*，伪造 ID_S^* 对消息 M^* 的签密消息 SC^*，要求 A 从未询问过 ID_S^* 的签密私钥，也从未询问过 (ID_S^*,ID_R^*) 对 M^* 的签密消息。若 $ID_S^*\neq ID_{i^*}$，则中止。否则，根据分叉引理，在不掌握 ID_S^* 的签密私钥的情况下，如果存在 PPT 敌手 A 能成功伪造签密消息 SC^*，则S可构造一个图灵机 A'通过多次运行 A，以相同的输入 (M^*,ID_S^*,ID_R^*) 得到 2 个有效的签密消息 $SC_1^*(C_1^*,h_1^*,S_1^*)$ 和 $SC_2^*(C_2^*,h_2^*,S_2^*)$，满足 $h_1^*\neq h_2^*$，$S_1^*\neq S_2^*$。由于 $ID_S^*=ID_{i^*}$，则 $H_1(ID_S^*)=w^*$，且令 $H_1(ID_R^*)=w_R^*$。令 $\frac{(w_R^*+x)f(x)}{w^*+x}=F(x)+\frac{d}{w^*+x}$，其中 $F(x)$ 是 $Z_N[x]$ 中次数为 $q-1$ 的多项式，d 是非零整数，$F(x)$ 的各项系数和 d 均可通过所选参数计算。S计算 $W^*=\left[\frac{1}{d}\right]\left(\left[\frac{1}{h_2^*-h_1^*}\right](S_1^*-S_2^*)-[F(a)]P\right)$，输出 (w^*,W^*) 作为 q-SDH 问题实例的解。这是由于，当 A 选定用于伪造的签密者标识恰好为 ID_{i^*} 时，有：

$$S_1^*=\left[(r^*-h_1^*)\left(1-\frac{w_R^*}{w^*}\right)\right]ds_S^*+\left[\frac{(r^*-h_1^*)w_R^*}{w^*}\right]P_1$$
$$=\left[(r^*-h_1^*)\left(\frac{(w^*-w_R^*)a}{w^*(w^*+a)}+\frac{w_R^*}{w^*}\right)\right]P_1$$
$$=\left[\frac{(r^*-h_1^*)(w_R^*+a)f(a)}{w^*+a}\right]P$$

同理，$S_2^*=\left[\frac{(r^*-h_2^*)(w_R^*+a)f(a)}{w^*+a}\right]P$，则有：

$$W^*=\left[\frac{1}{d}\right]\left(\left[\frac{1}{h_2^*-h_1^*}\right](S_1^*-S_2^*)-[F(a)]P\right)$$
$$=\left[\frac{1}{d}\left(\frac{(r^*-h_1^*)-(r^*-h_2^*)}{h_2^*-h_1^*}\cdot\frac{(w_R^*+a)f(a)}{w^*+a}-F(a)\right)\right]P$$
$$=\left[\frac{1}{d}\left(\frac{(w_R^*+a)f(a)}{w^*+a}-F(a)\right)\right]P$$
$$=\left[\frac{1}{d}\left(F(a)+\frac{d}{w^*+a}-F(a)\right)\right]P$$
$$=\left[\frac{1}{w^*+a}\right]P$$

因此，(w^*,W^*)可作为 q-SDH 问题实例的一个解。

以下是对S成功模拟概率和破解 q-SDH 问题优势的分析。只有当 A 伪造签密私钥的标识 ID_S^* 在 L_1 中的序号恰好为 i^* 时，S才能成功模拟并计算 q-SDH 问题实例的解，其概率为 $1/q_{H_1}$，而 q_{H_1} 是多项式级别且有上界，所以此概率是不可忽略的。因此，若 A 能以不可忽略的优势 ε 伪造本方案签密，则S能以 ε/q_{H_1} 的优势成功求解 q-SDH 问题，该优势同样是不可忽略的。然而，这与 q-SDH 问题的困难性假设相矛盾，故本签密方案在 EUF-CMIA 安全模型下是安全的。

5 性能分析与实验

5.1 性能分析

首先对本方案的计算和通信开销进行定量分析，引入标

准 SM9 算法的“签名＋加密”组合作为参考，并与其他同类方案展开对比。对于计算开销，考虑用户签密私钥生成、签密消息生成和解密验证 3 项算法中各项耗时运算的次数（可预计算完成的步骤以及对称加解密未计入），对比分析结果如表 1 所列。其中，SM 表示对称群 G 上的标量乘运算，SM_1 和 SM_2 分别表示群 G_1 和 G_2 上的标量乘运算，BP 表示双线性对运算，E 表示群 G_T 上的幂运算。经实测，其余运算（如有限域 F_N 上的模逆，以及群 G，G_1，G_2 上的加法、群 G_T 上的乘法和哈希运算 H_1，H_2 等）耗时与上述运算至少相差 2 个数量级，为突出分析重点，已将它们忽略。

表 1　SM9 签密方案的计算开销

Table 1　Calculation overhead of SM9 signcryption schemes

方案	私钥生成	签密消息生成	解密验证
文献[21]	2SM	3SM＋E	2SM＋2BP
SM9 签名＋加密	SM_1＋SM_2	3SM_1＋2E	SM_2＋E＋2BP
文献[25]	SM_1＋SM_2	3SM_1＋E	SM_2＋E＋2BP
本文	SM_1＋SM_2	2SM_1＋E	2SM_2＋E＋BP

各方案私钥生成的计算量基本相同；在签密消息生成环节，文献[25]方案相较于“SM9 签名＋加密”减少 1 次群 G_T 上的幂运算，本方案相比文献[25]方案再减少 1 次群 G_1 上的标量乘；在解密验证环节，文献[25]方案与“SM9 签名＋加密”的计算量基本相同，而本方案相比它们减少 1 次耗时更大的双线性对运算，多出 1 次群 G_2 上的标量乘。因此，本方案在签密消息生成和解密验证的计算性能上，相较于现有方案具有优势。

对于通信开销，考虑系统公钥、用户私钥和签密消息的比特位数（原始消息 M 对应的密文未计入），对比分析结果如表 2 所列。其中，$|G|$，$|G_1|$，$|G_2|$，$|G_T|$，$|F_N|$ 分别表示对应群（或域）元素的比特位数。具体而言，$|G|=512$ b，对于 SM9 国标规范使用的 256 b 的 BN 曲线[2]，$|G_1|=512$ b，$|G_2|=1\,024$ b，$|G_T|=3\,072$ b，$|F_N|=256$ b。SM9 国标已做规定的 P_1，P_2 等公共参数未计入系统公钥。

表 2　SM9 签密方案的通信开销

Table 2　Communication overhead of SM9 signcryption schemes

方案	系统公钥	用户私钥	签密消息
文献[21]	$4\|G\|$	$2\|G\|$	$3\|G\|+\|F_N\|$
SM9 签名＋加密	$\|G_2\|+\|G_1\|$	$\|G_2\|+\|G_1\|$	$2\|G_1\|+2\|F_N\|$
文献[25]	$\|G_2\|+\|G_1\|$	$\|G_2\|+\|G_1\|$	$2\|G_1\|$
本文	$\|G_2\|+\|G_1\|$	$\|G_2\|+\|G_1\|$	$\|G_1\|+\|F_N\|$

可见，基于 SM9 的 3 个方案的系统公钥和用户私钥长度相同。具体地，不考虑原始消息 M 对应的密文时，表中各方案签密消息长度分别为 224 B，192 B，128 B，96 B，即本方案为“SM9 签名＋加密”的 1/2、文献[25]方案的 3/4，有效降低了传递签密消息的通信开销。

5.2　实验测试

本文基于国密算法开源 Python 库 hggm[33] 的 SM9 模块，采用 SM9 国标规定的参数设置[2]，通过 Python 编程实现了文献[25]方案和本方案，并引入“SM9 签名＋加密”作为参考，以验证本方案的有效性与性能优势。实验计算机的配置如表 3 所列。

表 3　实验计算机配置

Table 3　Configuration of experimental computer

项目	配置
设备类型	PC
操作系统	Windows10 64 位
CPU	Intel Core i3-10110U(2 核心 4 线程)
内存	8GB LPDDR3 2133 MHz
硬盘	SAMSUNG MZVLB512HBJQ-000L7
Python 版本	3.7.1

由于系统建立和用户签密私钥生成 2 项算法无需用户计算且运行频次很低，因此重点测试签密消息生成和解密验证耗时，结果如表 4 所列。对于可预计算的步骤，已提前进行预计算，预计算耗时不包括在内。对称加解密采用基于 KDF 的序列密码，为避免对称加解密耗时占比过大，原始消息 M 长度仅为 15～17B。各项算法均执行 500 次，取平均值为有效数据。

表 4　各项算法测试结果

Table 4　Test results of algorithms

(ms)

方案	签密消息生成	解密验证
SM9 签名＋加密	14.71	53.29
文献[25]	10.18	51.71
本文	6.08	31.88

由表 4 数据可知，本方案签密消息生成的计算效率为“SM9 签名＋加密”的 2.42 倍，为文献[25]方案的 1.67 倍，而对于解密验证，本方案的计算效率为“SM9 签名＋加密”的 1.67 倍，为文献[25]方案的 1.62 倍，符合计算开销的理论分析结果。

综上，相较于现有签密方案，本方案在通信开销、签密消息生成和解密验证算法性能上都具有明显优势。

结束语　基于标识的签密作为一种融合数字签名与加密的密码学技术，应用场景广泛，既有利于提高算法执行效率，又避免了 PKI 的建设管理成本。本文基于国密算法 SM9 的数字签名和加密算法，设计了一种高效的签密方案。通过形式化的安全规约方法，证明其在随机预言机模型下具有 IND-CCA 和 EUF-CMIA 安全性。本文所提方案和文献[25]方案都是基于 SM9 设计的签密方案，而本方案将封装密钥和封装签名信息的群元素合二为一，通过理论分析和编程实现，验证了本方案在计算效率和通信开销上的比较优势，提升了基于 SM9 的签密方案的时空效率和实用性。下一步将在不降低算法效率的同时进行改进，在证明 IND-CCA 安全性的过程中，尝试消除对 Gap 类困难假设的依赖，以及在本方案基础上设计基于 SM9 的环签密方案。

本方案实现与测试的全部 Python 代码，已在“码云”平台开源[1)]。

参 考 文 献

[1] ZHENG Y L. Digital signcryption or how to achieve cost (signature & encryption)≪cost(signature)＋cost(encryption)[C]// Proceedings of Advances in Cryptology—CRYPTO'97. Springer Berlin Heidelberg, 1997: 165-179.

[2] Identity-based cryptographic algorithms SM9-Part 1: General: GB/T 38635.1-2020[S]. Beijing: National Information Security

1) https://gitee.com/basddsa/hggm

Standardization Technical Committee, 2020-04-28.
[3] Identity-based cryptographic algorithms SM9-Part 2: Algorithms: GB/T 38635. 2-2020[S]. Beijing: National Information Security Standardization Technical Committee, 2020-04-28.
[4] PENG C, HE D B, LUO M, et al. An identity-based ring signature scheme for SM9 algorithm[J]. Journal of Cryptologic Research, 2021, 8(4): 724-734.
[5] RAO J T, CUI Z. Secure evoting protocol based on SM9 blind signature and ring signature[J]. Computer Engineering, 2023, 49(6): 13-23, 33.
[6] AN H Y, HE D B, BAO Z J, et al. Ring signature based on the SM9 digital signature and its application in blockchain privacy protection[J]. Journal of Computer Research and Development, 2023, 60(11): 2545-2554.
[7] PU L, LIN C, WU W, et al. A public-key encryption with keyword search scheme from SM9[J]. Journal of Cyber Security, 2023, 8(1): 108-118.
[8] LAI J C, HUANG X Y, HED B, et al. An efficient hierarchical identity-based encryption based on SM9[J]. SCIENTIA SINICA Informations, 2023, 53(5): 918-930.
[9] LIU K, NING J T, WU W, et al. Multi-ciphertext batch auditable decryption outsourcing SM9-HIBE key encapsulation mechanism[J]. Journal on Communications, 2023, 44(12): 158-170.
[10] LI C, LIANG J K, DING Y J, et al. Hierarchical identity-based broadcast inner product functional encryption based on SM9[J]. SCIENTIA SINICA Informations, 2024, 54(6): 1400-1418.
[11] CUI Y, HUANG X Y, LAIJ C, et al. Anonymous broadcast encryption based on SM9[J]. Journal of Cyber Security, 2023, 8(6): 15-27.
[12] LIU X H, HUANG X Y, CHENG Z H, et al. Fault-tolerant identity-based encryption from SM9[J]. Science China(Information Sciences), 2024, 67(2): 104-117.
[13] MALONE-LEE J. Identity-based signcryption[J/OL]. https://eprint.iacr.org/2002/098.pdf.
[14] LIBERT B, QUISQUATER J. A new identity based signcryption scheme from pairings[C]// Proc of 2003 IEEE Information Theory Workshop(ITW 2003). IEEE, 2003: 155-158.
[15] BARRETO P S L M, LIBERT B, MCCULLAGH N, et al. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps[C]// Proc of Advances in Cryptology—ASIACRYPT 2005. Springer Berlin Heidelberg, 2005: 515-532.
[16] YU Y, YANG B, SUN Y, et al. Identity based signcryption scheme without random oracles[J]. Computer Standard & Interfaces, 2009, 31(1): 56-62.
[17] JIN Z P, WEN Q Y, DU H Z. An improved semantically-secure identity-based signcryption scheme in the standard model[J]. Computer & Electrical Engineering, 2010, 36(3): 545-552.
[18] SELVI S S D, VIVEK S S, VINAYAGAMURTHY D, et al. ID based signcryption scheme in standard model[C]// Proceedings Provable Security—ProvSec 2012. Springer Berlin Heidelberg, 2012: 35-52.
[19] LI F G, TAKAGI T. Secure identity-based signcryption in the standard model[J]. Mathematical and Computer Modelling, 2013, 57(11/12): 2685-2694.
[20] LI X X, QIAN H F, WENG J, et al. Fully secure identity-based signcryption scheme with shorter signcryptext in the standard model[J]. Mathematical and Computer Modelling, 2013, 57(3/4): 503-511.
[21] KARATI A, ISLAM S H, BISWASG P, et al. Provably secure identity-based signcryption scheme for crowdsourced industrial internet of things environments[J]. IEEE Internet of Things Journal, 2018, 5(4): 2904-2914.
[22] WANG X M, ZHANG Y, GUPTA B B, et al. An identity-based signcryption on lattice without trapdoor[J]. Journal of Universal Computer Science, 2019, 25(3): 282-293.
[23] ELTAYIEB N, ELHABOB R, HASSAN A, et al. A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud[J]. Journal of Systems Architecture, 2020, 102: 101653.
[24] MANDAL S, BERA B, SUTRALAA K, et al. Certificateless-signcryption-based three-factor user access control scheme for IoT environment[J]. IEEE Internet of Things Journal, 2020, 7(4): 3184-3197.
[25] LAI J C, HUANG X Y, HE D B, et al. An efficient identity-based signcryption schemebased on SM9[J]. Journal of Cryptologic Research, 2021, 8(2): 314-329.
[26] WANG Y T. Application research of digital signature algorithm based on SM9[D]. Beijing: Beijing Jiaotong University, 2021.
[27] ZHANG C. Research on identity-based searchable encryption schemes[D]. Guiyang: Guizhou University, 2022.
[28] BAO J B. Identity-based ring signcryption scheme based on SM9 algorithm[D]. Wuhan: Wuhan University, 2022.
[29] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-369.
[30] ZHOU J, ZHANG Y J, ZHU Y F. Generic ID-based signature schemes and forking lemma[J]. Journal of Information Engineering University, 2007, 8(2): 129-133.
[31] CHENG Z H. Security analysis of SM9 key agreement and encryption[C]// Proc of the 14th International Conference Information Security and Cryptology. Fuzhou, 2018: 3-25.
[32] LAI J C, HUANG X Y, HED B, et al. Security analysis of national secret SM9 digital signature and key encapsulation algorithm[J]. SCIENTIA SINICA Informationis, 2021, 51(11): 1900-1913.
[33] Basddsa. hggm—Domestic cryptographic algorithm SM2/SM3/SM4/SM9/ZUC—Complete source code for Python implementation[EB/OL]. (2024-07-11) [2024-07-11]. https://gitee.com/basddsa/hggm.

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

ZHAO Fangfang, born in 1990, Ph.D, lecturer. Her main research interests include network security and network traffic anomaly detection.