基于 Cocks 身份密码体制的高效签密方案

彭长根[1,2,3]，张小玉[1,3]，丁红发[2,4]，杨善慧[1,3]

（1. 贵州大学数学与统计学院公共大数据国家重点实验室，贵州 贵阳 550025；2. 贵州大学计算机科学与技术学院，贵州 贵阳 550025；
3. 贵州大学密码学与数据安全研究所，贵州 贵阳 550025；4. 贵州财经大学信息学院，贵州 贵阳 550025）

摘 要：现有的基于身份签密方案多是基于双（多）线性对构造的，针对其复杂的对运算导致签密效率低下的问题，基于 Cocks 的身份密码体制提出了一种新的高效签密方案。首先，形式化所提方案的安全模型，给出了保密性和不可伪造性的定义；然后，利用二次剩余难解问题实现了所提方案的具体构造，进一步结合雅可比符号运算巧妙地在一个逻辑步骤内实现了签密算法设计；最后，在随机预言模型下，给出了所提方案满足保密性和不可伪造性的安全性证明。效率分析表明，相对于已有的基于身份签密的方案，所提方案较大幅度地提升了运算效率，同时具备基于身份密码的良好特性。

关键词：签密；Cocks 身份密码体制；二次剩余问题；可证明安全

中图分类号：TP30

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2020214

Efficient signcryption scheme based on Cocks' identity cryptosystem

PENG Changgen[1,2,3], ZHANG Xiaoyu[1,3], DING Hongfa[2,4], YANG Shanhui[1,3]

1. College of Mathematics and Statistics, State Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China
2. College of Computer Science and Technology, Guizhou University, Guiyang 550025, China
3. Institute of Cryptography and Data Security, Guizhou University, Guiyang 550025, China
4. College of Information, Guizhou University of Finance and Economics, Guiyang 550025, China

Abstract: Most of the existing identity-based signcryption schemes are based on bilinear or multilinear pairing operations construction. To solve the problem of low efficiency caused by complex pair operation, a new efficient signcryption scheme based on the identity cryptosystem of Cocks was proposed. Firstly, the security model of the proposed scheme was formalized, and the definition of confidentiality and unforgeability was given. Secondly, the quadratic residue problem was used to realize the concrete construction of the proposed scheme, and the signature algorithm was designed in a logical step by combining Jacobi symbol operation. Finally, the security proofed that the scheme satisfied the confidentiality and unforgeability was given under the random prediction model. The efficiency analysis shows that compared with the existing identity-based signcryption scheme, the proposed scheme greatly improves the computing efficiency and has good characteristics of identity-based cryptosystem.

Key words: signcryption, Cocks' identity cryptosystem, quadratic residue problem, provable security

---

收稿日期：2020−08−10；**修回日期**：2020−10−15

基金项目：国家自然科学基金资助项目（No.U1836205，No.61662009，No.61772008）；贵州省科技计划基金资助项目（No.[2018]3001, No.[2018]3007, No.[2017]3002, No.[2019]2004, No.[2018]2162, No.[2018]2159, No.[2020]5017, No.[2020]1Y265）；贵州省高等学校创新人才团队基金资助项目（No.[2013]09）；“十三五”国家密码发展基金资助项目（No.MMJJ20170129）

Foundation Items: The National Natural Science Foundation of China (No.U1836205, No.61662009, No.61772008), The Science and Technology Program of Guizhou Province (No.[2018]3001, No.[2018]3007, No.[2017]3002, No.[2019]2004, No.[2018]2162, No.[2018]2159, No.[2020]5017, No.[2020]1Y265), The Project of Innovative Group in Guizhou Education Department (No.[2013]09), The 13th Five-Year National Cryptography Development Foundation (No.MMJJ20170129)

1　引言

签密能在一个逻辑步骤内同时实现加密和签名，相比于单纯地将加密和签名方案组合，其在计算效率和通信开销上都具有明显的优势。自 Zheng 等[1]基于椭圆曲线上的离散对数提出第一个签密方案后，构造安全有效的签密方案便成为研究热点，不同的签密方案也被广泛地应用于电子支付、移动代理安全等轻量级计算场景。2002 年，Malone-Lee[2]首次提出了基于身份密码的签密方案，赋予了签密方案便捷密钥管理的优势。

5G 中除了终端基本的安全需求外，增强型移动宽带（eMBB, enhance mobile broadband）场景[3]的传输效率非常高，终端必须具备高速率的加解密能力。此外，eMBB 场景涉及的敏感信息较多（如个人身份标识、地址信息等），因此终端还需要重视用户隐私数据的保护，这种场景下需要设计安全高效的密码算法和认证协议来确保其正常运行。现有的基于身份的签密方案大多是由双线性对构造的，利用双线性对构造的签密方案在不牺牲安全性的前提下可使用较短的密钥，但其在签密过程中需要进行大量复杂的双线性对运算，会造成高昂的计算开销，也会降低签密和解签密速率。5G 时代的到来，使人们对签密方案也提出了更高的要求，导致基于双线性对的签密方案在类似于上述 eMBB 场景下形成了新的应用瓶颈。如何利用新的密码技术，设计更加高效的签密方案，为 5G 网络提供安全基础保障，成为一个极具挑战的课题。

1997 年，Zheng[4]提出了一种名为签密的密码原语，由于其能有效地解决传统的先签名后加密方案中计算效率低和通信开销大的问题，迅速成为研究热点。2002 年，Shin 等[5]提出了基于数字签名算法（DSA, digital signature algorithm）的可验证签密方案，其签名通过 DSA 进行验证，但因消息 m 部分显式地出现在验证式中，导致该方案不能满足语义安全。2017 年，Yu 等[6]提出了一种无配对的无证书签密方案，该方案在随机预言机模型中利用计算型 Diffie-Hellman（CDH, computational Diffie-Hellman problem）问题和离散对数（DL, discrete logarithm）问题证明其具有机密性和不可伪造性，但该方案对恶意的密钥生成中心（KGC, key generation center）和恶意的发送者是不安全的。2019 年，Rezaeibagha 等[7]提出了一个可证明安全的同态签密方案，该方案证明了同态签密可推广到可证明的安全广播签密方案，允许在不需要解密的情况下聚合广播的签密数据项，但该方案因需要大量的双线性对运算，导致加解密效率较低。基于身份的密码系统具有便捷管理密钥的优势，自 2002 年 Malone-Lee[2]利用双线性对构造了首个基于身份的签密方案以来，基于身份的签密方案[8-11]就得到各专家学者的广泛研究。

2003 年，Libert 等[8]指出 Malone-Lee[2]的方案不具有语义安全性，同时构造了基于椭圆曲线上双线性对的签密方案，但该方案不能同时满足前向安全性与公开验证性这 2 个重要的安全特性。2016 年，Wang 等[9]构造了基于多线性映射的聚合签密方案，该方案在标准模型下可抵抗适应性选择明文攻击，但其同样存在多线性对运算带来的计算效率不高的问题。2017 年，Reddi 等[10]利用双线性映射构造了基于身份的群签密密钥协商协议，该协议使用签名对参与的用户进行认证，并验证 2 个用户之间传输消息的正确性，在物联网中具有一定的实用性。2018 年，Zhou 等[11]提出了基于身份的广义代理签密方案，该方案可以在代理签密模式下进行公开验证，并在随机预言机模型中证明了方案的不可伪造性和机密性，但方案的密文膨胀较大，导致密文空间效率偏低。上述基于双线性对构造的签密方案都存在计算效率不高的问题，基于此，专家学者致力于研究减少双线性配对的次数或直接构造无配对的签密方案[12-14]。而传统数论中的雅可比符号的求值运算，因相对于双线性对运算在计算效率上有较大的优势，适于解决签密方案运算效率不高的问题。

基于二次剩余的加密源于 2001 年 Cocks[12]提出的基于二次剩余的基于身份的加密（IBE, identity-based encryption）方案，该方案加密过程仅需进行简单的雅可比（Jacobi）符号求值和模的求逆运算，计算执行效率较高，但 Cocks[12]对方案的安全性只做了简单的描述，并未进行详细证明。2013 年，Clear 等[13]将文献[12]方案的密文视为多项式商环 $\mathbb{Z}_N[x]/(x^2-r_{\mathrm{id}})$ 中的元素，在此基础上，构建了一个强异或运算（XOR, exclusive OR）同态 IBE 方案。同年，Dan 等[14]的广义 Cocks 方案自然地将二次剩余推广到高次剩余，允许一次加密多个比特，加密 l bit 明文，得到的密文大小约为 $2^{l+\mathrm{lb}N}$ bit，但这

种泛化的缺点是密文膨胀规模大。2019 年，Clear 等[15]扩展了文献[14]方案，使其满足加法同态性，并证明了该方案在随机预言机模型中的 e 次剩余假设下是 IND-ID-CPA 安全的，但该方案同样面临密文膨胀的问题。

1997 年，Chang 等[16]提出了基于二次剩余的数字签名协议，协议允许任何发送者发送无限量的消息块，并在每个块上签名，解决了基于传统密码体制一次只能签名 N bit 的问题。2007 年，Chai 等[17]利用计算二次剩余的 2^l 根的技术构造基于身份的签名方案，并在随机预言机模型中证明其在选择明文攻击下具有不可区分性。2015 年，Zhao 等[18]提出了一种有效的部分盲签名方案，该方案利用二次剩余求值的困难问题在随机预言机模型中证明了方案的盲性与不可伪造性，其签名空间被限制在二次剩余类群中。2018 年，Ateniese 等[19]提出了一类基于二次剩余假设的全域哈希签名方案，构造了 2 种不同的方案，一种方案具有签名唯一的特性，另一种方案在签名验证过程中最多进行 3 次模乘运算，验证阶段效率较快。可见，基于二次剩余的签名、加密方案的构造一直是密码学领域的研究热点，但尚未有安全高效的签密方案被设计。如何设计计算效率高、通信成本低的签密方案仍是一个具有挑战性的课题。

鉴于上述分析，本文提出了一种基于 Cocks 身份密码体制的高效签密（CBSC, Cocks IBE signcryption）方案。本文的主要贡献如下。

1) 构造适合 CBSC 方案的安全模型，给出方案保密性和不可伪造性的相关“攻击−挑战”游戏的形式化定义。在改进 Cocks 基于身份的加密方案的基础上，利用二次剩余问题构造签名部分在一个逻辑步骤内完成签密方案的设计。

2) 在随机预言机模型下对所提方案的安全性进行证明，将其安全性归约到数论中的二次剩余判别困难问题，证明了所提方案在适应性选择密文攻击下具有不可区分性，在适应性选择消息下满足不可伪造性，具有较好的安全性。

3) 效率分析表明，所提方案相较于已有的基于双线对和椭圆曲线离散对数的签密方案，由于其不存在复杂的双线性对运算，且所提方案构造中主要利用运算效率较高的雅可比符号求值运算，故所提方案在计算效率方面具有明显的优势。

2 基础知识

2.1 定义及定理

定义 1 二次剩余定义[19]。令 $x\in\mathbb{Z}_N^*$，若存在 $x\in\mathbb{Z}_N^*$，使 $x^2\equiv a \bmod N$，则称 a 是模 N 的二次剩余，否则称 a 是模 N 的二次非剩余。所有模 N 的二次剩余组成的集合为 $\mathbb{QR}_N=\left\{x^2 \bmod N \mid x\in\mathbb{Z}_N^*\right\}$，其中 $\mathbb{Z}_N^*=\left\{x \mid x\in\mathbb{Z}_N,(x,N)=1\right\}$。

定义 2 雅可比符号定义[15]。设 N 为正整数且 $N=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$，定义雅可比符号 $\left(\frac{a}{N}\right)$ 为

$$\left(\frac{a}{N}\right)=\left(\frac{a}{p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}}\right)=\left(\frac{a}{p_1}\right)^{e_1}\left(\frac{a}{p_2}\right)^{e_2}\cdots\left(\frac{a}{p_k}\right)^{e_k} \tag{1}$$

记雅可比符号值为 1 的所有元素的集合为 $\mathbb{J}_N=\left\{x\in\mathbb{Z}_N \middle| \left(\frac{x}{N}\right)=1\right\}$，令 $\mathbb{Z}_N=\left\{x \mid 0\leqslant x<N, N\in\mathbb{Z}\right\}$。

定义 3 二次剩余假设[19]。令 $\mathrm{RSAgen}(\lambda)$ 是一个概率多项式时间（PPT, probability polynomial time）算法，产生 2 个大小相同的素数 p,q。

令 $\mathcal{P}_{\mathbb{QR}}(\lambda)$ 是 (N,v) 的分布，即 $(p,q)\xleftarrow{R}\mathrm{RSAgen}(\lambda)$, $N\leftarrow pq, v\xleftarrow{R}\mathbb{QR}_N$。

令 $\mathcal{P}_{\mathbb{NQR}}(\lambda)$ 是 (N,v) 的分布，即 $(p,q)\xleftarrow{R}\mathrm{RSAgen}(\lambda)$, $N\leftarrow pq, v\xleftarrow{R}\mathbb{J}_N\setminus\mathbb{QR}_N$。

令 $D(\mathcal{A},\mathcal{P})=\Pr\left[(N,v)\xleftarrow{R}\mathcal{P}(\lambda):\mathcal{A}(N,v)=1\right]$，其中，$\mathcal{P}(\lambda)$ 是对 $\mathcal{P}_{\mathbb{QR}}(\lambda)$ 和 $\mathcal{P}_{\mathbb{NQR}}(\lambda)$ 的一个形式化描述。对于任何多项式时间内的敌手 $\mathcal{A}$ 判断模 N 二次剩余的优势 $\mathrm{Adv}_{\mathcal{A}}^{\mathbb{QR}}$，存在一个可忽略的函数 $\mathrm{negl}(\lambda)$，满足

$$\mathrm{Adv}_{\mathcal{A}}^{\mathbb{QR}}(\lambda)=\left|D(\mathcal{A},\mathcal{P}_{\mathbb{QR}}(\lambda))-D(\mathcal{A},\mathcal{P}_{\mathbb{NQR}}(\lambda))\right|\leqslant\mathrm{negl}(\lambda)$$

即若不知道 $N=pq$ 的分解，判定 $v\in\mathbb{J}_N$ 是否为模 N 的二次剩余是困难的。

定理 1 欧拉判别条件[16]。若 $(a,p)=1$，则 a 是模 p 的平方剩余的充分必要条件是 $a^{\frac{p-1}{2}}\equiv -1 \bmod p$；而 a 是模 p 的平方非剩余的充要条件是 p。

2.2 Cocks 公钥密码方案

Cocks 公钥密码[12]是由 Cocks 在 2001 年提出的一种新的基于二次剩余的身份密码体制，该方案将用户的身份等公共已知值作为公钥，具有优良的性质，计算执行效率较高，可用于构造高效的密码算

法。该算法由 Setup、KeyGen、Encrypt和Decrypt 这 4 个部分组成。

Setup$\left(1^{\lambda}\right)$。给定一个安全参数 λ，初始化阶段生成 2 个不同的大素数 p,q $(p=q=3 \bmod 4)$，计算 $N=pq$。选择哈希函数 $H:\{0,1\}^{*}\to\mathbb{Z}_{N}^{*}$，输出主密钥 MSK=$\{p,q\}$，系统公开参数 PP=$\{N,H\}$。

KeyGen$(\mathrm{id},\mathrm{MSK})$。计算 $a=H(\mathrm{id})$，满足 $r^{2}\equiv\pm a \bmod N$，计算出 $r=a^{\frac{N+5-(p+q)}{8}} \bmod N$，返回私钥 $\mathrm{sk}=\{r\}$。

Encrypt$(\mathrm{id},x,\mathrm{PP})$。用户 Bob 首先生成一个传输密钥，使用对称加密的方式加密数据，并依次向接收者 Alice 发送传输密钥的每个位，步骤如下。

1) 设 x 是传输密钥的单个位，编码 x 为 1 或−1。

2) Bob 随机选择 t，使 $\left(\frac{t}{N}\right)=x$。

3) Bob 通过加密算法计算 $s=\left(t+\frac{a}{t}\right) \bmod N$ 并发送给 Alice。

Decrypt(s,r)。Alice 通过对式(2)进行计算

$$s+2r=t\left(1+\frac{r}{t}\right)^{2} \bmod N \tag{2}$$

得到雅可比符号 $\left(\frac{s+2r}{N}\right)=\left(\frac{t}{N}\right)=x$，由此恢复 x。

3　CBSC 签密方案安全模型形式化定义

本节构造适合 CBSC 方案的安全模型，给出方案保密性和不可伪造性的相关“攻击−挑战”游戏的形式化定义。通过攻击游戏的定义，可以对方案的安全性进行更准确的证明。

3.1　保密性定义

游戏由系统初始化阶段、询问阶段、挑战阶段和猜测阶段 4 个阶段组成，参与方包括敌手 $\mathcal{A}$ 和挑战者 C，具体步骤如下。

1) 系统初始化阶段。输入安全参数 λ，C 维护各个列表记录相应预言机询问及密钥生成询问的数据，同时运行 Setup 算法，生成系统主密钥 MSK 和公开参数 PP，并将公开参数 PP 发送给 $\mathcal{A}$。

2) 询问阶段。敌手 $\mathcal{A}$ 向挑战者 C 发起多项式有界次如下询问。

① 密钥生成（KeyGen）询问。$\mathcal{A}$ 以身份 ID_i 询问，C 查询私钥对应列表，运行 KeyGen 算法产生一个对应的私钥 $\mathrm{SK}_{\mathrm{ID}_i}$ 发送给 $\mathcal{A}$。

② 签密（Signcrypt）询问。$\mathcal{A}$ 以发送者身份 ID_s、接收者身份 ID_r 和明文 m 进行询问，C 计算发送者私钥 $\mathrm{SK}_{\mathrm{ID}_s}$，并以相同的输入向相应的预言机进行签密询问，预言机将密文 σ 返回给挑战者 C，C 将 $\sigma\leftarrow\mathrm{Signcrypt}\left(\mathrm{SK}_{\mathrm{ID}_s},\mathrm{ID}_r,m,\mathrm{PP}\right)$ 发送给 $\mathcal{A}$。

③ 解签密（Unsigncrypt）询问。$\mathcal{A}$ 以发送者身份 ID_s、接收者身份 ID_r 和合法密文 σ 进行询问，C 计算接收者私钥 $\mathrm{SK}_{\mathrm{ID}_r}$，并以相同的输入向相应的预言机进行解签密询问，预言机将明文 m 返回给 C，C 将结果 $m\leftarrow\mathrm{Unsigncrypt}\left(\mathrm{SK}_{\mathrm{ID}_r},\mathrm{ID}_s,\sigma,\mathrm{PP}\right)$ 发送给 $\mathcal{A}$。

以上询问可以是自适应的，即执行每一次的询问时都可以根据前一次询问时得到的结果进行相应的调整。

3) 挑战阶段

① 敌手 $\mathcal{A}$ 选择 2 个明文 m_0、m_1 和希望挑战的身份 ID_1、ID_2，其中 ID_1 和 ID_2 在之前的询问中都未进行过 KeyGen 询问。

② 挑战者 C 随机选择 $b\in_R\{0,1\}$，并将消息 m_b、$\mathcal{A}$ 指定的发送者 ID_1 的私钥 $\mathrm{SK}_{\mathrm{ID}_1}$、接收者身份 ID_2 及公共参数 PP 作为输入向预言机进行签密询问，返回密文 $\sigma^{*}\leftarrow\mathrm{Signcrypt}\left(\mathrm{SK}_{\mathrm{ID}_1},\mathrm{ID}_2,m_b,\mathrm{PP}\right)$ 给挑战者 C，C 将 σ^{*} 发送给 $\mathcal{A}$。

③ $\mathcal{A}$ 可以继续像询问阶段那样进行多项式有界次询问，但此时对 ID_1 和 ID_2 不能进行 KeyGen 询问，对 σ^{*} 也不能进行 Unsigncrypt 询问。

4) 猜测阶段。$\mathcal{A}$ 输出 $b'\in\{0,1\}$ 作为对 b 的猜测，如果 $b'=b$，则 $\mathcal{A}$ 赢得游戏的优势可以定义为 $\mathrm{Adv}(\mathcal{A})=\left|\Pr\left[b'=b\right]-\frac{1}{2}\right|$。

定义 4　如果不存在任何多项式有界敌手 $\mathcal{A}$ 以不可忽略的优势赢得上述游戏，则 CBSC 方案可以抵抗适应性选择密文攻击（IND-ID-CCA2），即在适应性选择密文攻击下具有保密性。

3.2　不可伪造性定义

游戏由系统初始化阶段、询问阶段和伪造阶段 3 个阶段组成，游戏双方仍为敌手 $\mathcal{A}$ 和挑战者 C，具体步骤如下。

1) 系统初始化阶段。输入安全参数 λ，C 运行

Setup 算法，生成系统主密钥 MSK 和公开参数 PP，并将公开参数 PP 发送给 $\mathcal{A}$。

2) 询问阶段。和机密性的询问阶段一样，$\mathcal{A}$ 执行多项式有界次相应的 KeyGen、Signcrypt、Unsigncrypt 询问。

3) 伪造阶段（Forge Phase）。$\mathcal{A}$ 输出元组 $\left(\sigma^*,\mathrm{ID}_1,\mathrm{ID}_2\right)$ 作为对明文消息的伪造，挑战者 C 将上述元组作为输入提交给预言机进行解签密询问，预言机将密文 σ^* 的解签密结果返回给挑战者 C，如果密文 σ^* 不是由 Signcrypt 询问产生，ID_1 未执行过 KeyGen 询问，且 $\mathrm{Unsigncrypt}\left(\sigma^*,\mathrm{SK}_{\mathrm{ID}_2},\mathrm{ID}_1,\mathrm{PP}\right)$ 的输出不是失败符号 $\perp$，则 $\mathcal{A}$ 赢得游戏。$\mathcal{A}$ 赢得游戏的优势定义为其的概率 $\mathrm{Adv}(\mathcal{A})=\Pr\left[\mathcal{A}\ \mathrm{win}\right]$。

定义 5 如果不存在多项式时间敌手 $\mathcal{A}$ 以不可忽略的优势赢得上述游戏，则称 CBSC 方案在适应性选择明文攻击下具有不可伪造性（CBSC-EUF-CMA）。

4 CBSC 签密方案构造

本节提出的 CBSC 签密方案是基于 Cocks 的 IBE 体制构造的签密方案，方案的参与者包括 PKG 和签密通信双方 $\mathrm{ID}_1,\mathrm{ID}_2$，由 4 个算法组成，即系统初始化算法 Setup、密钥生成算法 KeyGen、签密算法 Signcrypt 和解签密算法 Unsigncrypt，算法运行过程如下。

首先定义函数

$$\mathcal{J}_N(x)=\begin{cases}\perp, & \gcd(x,N)\neq 1\\ i, & \gcd(x,N)=1\text{且}\left(\dfrac{x}{N}\right)=(-1)^i\end{cases}\tag{3}$$

1) 系统初始化算法 (1^λ)

该算法由 PKG 执行。PKG 输入安全参数 λ，生成 2 个不同的大素数 p,q $(p=q=3\bmod 4)$，计算 $N=pq$。选择 4 个哈希函数 $H_0:\{0,1\}^*\to\mathcal{J}_N$，$H_1:\{0,1\}^*\to\{0,1\}^{\lambda_2}$，$H_2:\{0,1\}^*\to\{0,1\}^{\lambda_0+\lambda_1}$，$H_3:\{0,1\}^*\to\{0,1\}^{\lambda}$，其中 λ_0 为明文消息的长度，并且 $\left(\frac{1}{2}\right)^{\lambda_1}$ 和 $\left(\frac{1}{2}\right)^{\lambda_2}$ 为 2 个可忽略的量。PKG 输出主密钥 $\mathrm{MSK}=\{p,q\}$，并将其秘密保存。随机选择模 N 的二次非剩余 $\mu\in\mathcal{J}_N\setminus\mathbb{QR}_N$，即满足 $\left(\frac{\mu}{p}\right)=\left(\frac{\mu}{q}\right)=-1$，PKG 发布系统公开参数 $\mathrm{PP}=\{N,H_0,H_1,H_2,H_3,\mu\}$。

2) 密钥生成算法 $(\mathrm{PP},\mathrm{ID}_1,\mathrm{ID}_2)$

该算法由 PKG 执行。计算公钥 $R_i=H_0(\mathrm{ID}_i)$，$i=1,2$，若 $R_i\in\mathrm{QR}_N$，计算私钥 $r_i=R_i^{\frac{1}{2}}\bmod N$；否则计算 $r_i=\left(\mu R_i\right)^{\frac{1}{2}}\bmod N$。由此可得，签密双方的公私钥分别为 $\mathrm{PK}_{\mathrm{ID}_1}=R_1$，$\mathrm{PK}_{\mathrm{ID}_2}=R_2$，$\mathrm{SK}_{\mathrm{ID}_1}=r_1$，$\mathrm{SK}_{\mathrm{ID}_2}=r_2$ 且 $|R_1|=|R_2|=\lambda=\lambda_0+\lambda_1+\lambda_2$，通过安全通道将 r_i 发送给 ID_i。

3) 签密算法（$\mathrm{PP},\mathrm{SK}_{\mathrm{ID}_1},\mathrm{PK}_{\mathrm{ID}_2},m$）

该算法由签密者 ID_1 执行。签密者 ID_1 要发送消息 $m\in\{0,1\}$ $(|m|=\lambda_0)$ 给 ID_2，则签密者 ID_1 完成如下步骤。

Step1 $k_0\xleftarrow{R}\{0,1\}^{\lambda_1},\omega\leftarrow H_1\left(m\|k_0\right)$，输出 $s\leftarrow\left(m\|k_0\right)\oplus H_2\left(\omega\right)$。

Step2 随机选择 $t,\bar{t}\in\mathbb{Z}_N$，使其满足 $\left(\frac{t}{N}\right)=\left(\frac{\bar{t}}{N}\right)=(-1)^s=m'$，计算 $c_0=t+\frac{R_2}{t}\bmod N$，$\overline{c_0}=\bar{t}+\frac{\mu R_2}{\bar{t}}\bmod N$。

Step3 若 Step2 中 $|c_0|>\lambda$，令 $c_0=c_1\|c_2$（满足 $|c_2|=\lambda$），如果 $c_1=c_2$，则返回 Step2，若 $|c_0|>\lambda$，则令 $c_0=c_1=c_2$，$\overline{c_0}$ 同理。

Step4 如果 $|c_0|>\lambda$，则有 $s_1=H_3\left(c_1\right)\oplus c_2$；如果 $|c_0|\leqslant\lambda$，则 $s_1=H_3\left(c_1\right)\oplus\left(\underbrace{00\cdots0}_{l}\|c_2\right)$，其中 l 表示在 c_2 前补 0 的个数。若 $s_1>R_1$，则 $s_1=s_1-\left(\frac{1}{2}\right)^{\lambda-1}$，$\overline{c_0}$ 同理。

Step5 计算 $s_2=\left(R_1^{-c_1}s_1\right)^{-\left(2^{-1}\bmod r_1\right)}\bmod N$，签密者 ID_1 发送给接收者 ID_2 关于 m 的签密 $\sigma=\left(c_1,s_2\right)$。

4) 解签密算法 $(\mathrm{PP},\mathrm{SK}_{\mathrm{ID}_2},\mathrm{PK}_{\mathrm{ID}_1},\sigma)$

该算法由签密接收者 ID_2 执行。接收者 ID_2 对 ID_1 发送的签密 $\sigma=\left(c_1,s_2\right)$ 进行解签密。具体步骤如下。

Step1 计算 $s_1=s_2{}^2R_1^{c_1}\bmod N$。

Step2 计算 $c_2=H_3\left(c_1\right)\oplus s_1$，如果 $c_1=c_2$，则 $c_0=c_1=c_2$，否则有 $c_0=c_1\|c_2$。则通过运行 Cocks

公钥密码体制中的 Decrypt 算法解出 s，即如果有 $(r_2)^2 \equiv H(\mathrm{ID}_2) \equiv R_2 \bmod N$，设置 $\gamma=c_0$，通过计算得 $(-1)^s=\left(\frac{\gamma+2r_2}{N}\right)=m'$，否则设置 $\gamma=\overline{c_0}$，恢复 $(-1)^s=\left(\frac{\gamma-2r_2}{N}\right)=m'$。

Step3　由 Step2，若 $(m\|k_0)=H_2(\omega)\oplus s$，$H_1(m\|k_0)=\omega$，则输出消息 $m=\mathcal{J}_N(m')$，否则再计算 $c_2=H_3(c_1)\oplus\left(s_1+\left(\frac{1}{2}\right)^{\lambda-1}\right)$，并重复运行 Step2，若 $H_1(m\|k_0)=\omega$，则输出消息 $m=\mathcal{J}_N(m')$，否则返回拒绝接受签密文符号 ID_2，解签密失败。

5　CBSC 签密方案分析

5.1　正确性

1) 密文 $\sigma=(c_1,s_2)$ 正确性验证分析。接收者 ID_2 收到密文 s_2 后，有 $R_1^{c_1}s_2{}^{c_1}=R_1^{c_1}R_1^{-c_1}s_1=s_1$，再利用 c_1 和 s_1 计算出 $c_2=H_3(c_1)\oplus s_1$ 然后验证式(4)是否成立。

$$H_1(H_2(\omega)\oplus s)=H_1(m\|k_0)=\omega \tag{4}$$

如果式(4)成立，则签密过程是可信的，得到的密文 $\sigma=(c_1,s_2)$ 是正确的；否则，发送者在签密过程中或数据发送过程中存在伪造行为。

2) 解签密正确性分析。如果接收者 ID_2 收到的是正确的密文 $\sigma=(c_1,s_2)$，并且持有合法的解密密钥，则利用自己的私钥 r_2、身份 ID_2 和发送者的公钥 R_1，根据 c_1 与 c_2 数值上是否相等，可以得到相应的 c_0 或 $\overline{c_0}$ 的值，运行 Cocks 密码体制中的 Decrypt 算法可以得到 m'。

① 当 $(r_2)^2 \equiv H_0(\mathrm{ID}_2) \equiv R_2 \bmod N$，令 $\gamma=c_0$，有

$$\gamma\pm2r_2 \equiv t+\frac{R_2}{t}+2r_2 \equiv t+\frac{(r_2)^2}{t}+2r_2 \equiv t\left(1+2\frac{r_2}{t}+\left(\frac{r_2}{t}\right)^2\right)\equiv t\left(1+\frac{r_2}{t}\right)^2 \bmod N \tag{5}$$

输出

$$\left(\frac{\gamma\pm2r_2}{N}\right)=\left(\frac{t\left(1+\frac{r_2}{t}\right)^2}{N}\right)=\left(\frac{t}{N}\right)=(-1)^s=m'$$

② 当 $(r_2)^2 \equiv \mu R_2 \bmod N$，令 $\gamma=\overline{c_0}$，则 $\gamma\pm2r_2 \equiv \bar{t}\left(1+\frac{r_2}{\bar{t}}\right)^2 \bmod N$，有 $\left(\frac{\gamma\pm2r_2}{N}\right)=\left(\frac{\bar{t}}{N}\right)=(-1)^s$，进而可以得到相应的明文 $m=\mathcal{J}_N(m')$。

5.2　保密性

定理 2　如果存在一个概率多项式时间敌手 $\mathcal{A}$ 能够以 $\mathrm{Adv}_{\mathcal{A}}^{\text{CBSC-IND-CCA2}}=\varepsilon_{\text{CCA2}}$ 的优势来赢得 3.1 节中的游戏（最多进行 q_{H_1} 次 H_1 询问、q_{H_2} 次 H_2 询问、q_{H_3} 次 H_3 询问、q_{SK} 次密钥生成询问、q_{SC} 次签密询问、q_{USC} 次解签密询问），那么存在一个挑战者 C 可以以 $\mathrm{Adv}_C^{\mathbb{QR}}=\varepsilon'$ 的优势判断出模 N 的二次剩余问题，其中

$$\varepsilon' \geqslant \theta\frac{\varepsilon_{\text{CCA2}}}{q_{H_1}+q_{H_2}+q_{\text{SC}}} \tag{6}$$

$$\theta=\left(1-q_{\text{SK}}2^{-\lambda_2}\right)\left(1-q_{\text{SC}}\left(q_{H_2}+q_{\text{SC}}\right)2^{-(\lambda_0+\lambda_1)}\right)\cdot\left(1-q_{\text{SC}}\left(q_{H_3}+q_{\text{SC}}\right)2^{-\lambda}\right)\left(1-q_{\text{USC}}2^{-\lambda_2}\right) \tag{7}$$

证明　设敌手 $\mathcal{A}$ 是攻击签密体制 CBSC-IND-CCA2 安全性的攻击者，通过定义 L_{H_1}、L_{H_2}、L_{H_3}、L_{SK} 这 4 个记录表来记录相应的预言机询问和密钥生成询问。定义 $f_U=\left(t+\frac{R_U}{t}\right)\bmod N$，其中，$\left(\frac{t}{N}\right)=\left(\frac{\bar{t}}{N}\right)=(-1)^s$，$g_U(x,y)\to\sigma=(c_1,s_2)$，令 $x\leftarrow c_0$，$y\leftarrow H_3(c_1)$；则签密过程可以看作 $g_S(f_R,H_3(c_1))\to\sigma$。对询问阶段的各个预言机询问、密钥生成询问、签密询问和解签密询问的定义如下。

H_1 询问。如果向 H_1-oracle 询问 $(m\|\beta)$，在记录表 L_{H_1} 中查询记录 $(m\|\beta,\omega,\Delta,\nabla)$（其中符号 Δ 与 ∇ 对应签密体制中产生的 c_0 与 σ），若记录表中存在相应记录，则直接返回 ω；否则，随机选取 $\omega\xleftarrow{R}\{0,1\}^{\lambda_2}$，并在表 L_{H_1} 中添加相应记录 $(m\|\beta,\omega,\nabla,\Delta)$，同时返回 ω。

H_2 询问。如果向 H_2-oracle 询问 ω，在记录表 L_{H_2} 中查找记录 (ω,h)，若记录存在，则返回 h；否则，随机生成 $h\xleftarrow{R}\{0,1\}^{\lambda_0+\lambda_1}$，将 (ω,h) 添加到 L_{H_2} 表中，并返回 h。

H_3 询问。如果向 H_3-oracle 询问 c_1，查询记录 (c_1,ρ) 在记录表 L_{H_3} 中，若该记录存在，则直接返

回 ρ；否则，预言机随机选取 $\rho \xleftarrow{R} \{0,1\}^{\lambda}$，添加 (c_1,ρ) 到 L_{H_3} 记录表中，并返回 ρ。

KeyGen 询问。进行密钥生成询问，当接收到对身份 ID_i 对应的私钥 $\mathrm{SK}_{\mathrm{ID}_i} \leftarrow x_i$ 询问时，查询 L_{SK} 记录表，若存在对应项，则返回 x_i；否则选择任意随机数 $a \xleftarrow{R} \mathbb{Z}_N^*$，计算 $x_i = X_i^{\frac{1}{2}} \bmod N$，将该项添加到列表 L_{SK} 中，并返回 x_i。

Signcrypt 询问。设签密过程中签密者的身份为 ID_i，接收者身份为 ID_r，明文为 m，进行签密询问。随机生成 $\beta \xleftarrow{R} \{0,1\}^{\lambda_1}$，由此得到 $m \| \beta$；通过调用 H_1-oracle 得到 ω，调用 H_2-oracle 得到 h，计算得 $s = h \oplus m \| \beta, c_0 = f_S$，调用 H_3-oracle 随机选取 $\rho \xleftarrow{R} \{0,1\}^{\lambda}$，则有 $\sigma = g_S(c_0,\rho)$，如果 H_2-oracle 已经定义 ω 作为输入，或输入 c_1 已经在 H_3-oracle 中被定义，则算法模拟失败；反之，则分别将记录 $(\omega, h \oplus m \| \beta)$、$(c_1,\rho)$、$(m \| \beta, \omega, c_0, \sigma)$ 添加到表 L_{H_2}、L_{H_3}、L_{H_1} 中，并返回 σ。

Unsigncrypt 询问。设签密者的身份为 ID_i，接收者身份为 ID_r，签密文为 σ，在记录表 L_{H_1} 中寻找 $(m \| \beta, \omega, c_0, \sigma)$ 的记录，若该记录存在，则返回明文消息 m；否则，拒绝这个签密文 σ。

若有下列情形发生，则上述各类预言机的模拟被认为是失败的。

KeyGen 询问中，若询问 x_i 时，该记录在列表 L_{SK} 中不存在，则对应的公钥被替换，从而导致模拟失败，该事件发生的概率不超过 $q_{\mathrm{SK}} 2^{-\lambda_2}$。

Signcrypt 询问中，若输入 ω 在 H_2 - oracle 中已经被定义，或 H_3-oracle 已经定义了 c_1 作为输入，均会导致模拟失败，此事件发生的概率分别不超过 $q_{\mathrm{SC}}(q_{H_2}+q_{\mathrm{SC}})2^{-(\lambda_0+\lambda_1)}$ 和 $q_{\mathrm{SC}}(q_{H_3}+q_{\mathrm{SC}})2^{-\lambda}$。

在 H_1 询问输入 $m \| \beta$ 时，若该记录不存在于记录表 L_{H_1} 中，则 Unsigncrypt 预言机将拒绝一些有效密文，其发生的概率不会大于 $q_{\mathrm{USC}} 2^{-\lambda_2}$。

综上所述，预言机模拟成功的概率不会低于

$$\theta = \left(1 - q_{\mathrm{SK}} 2^{-\lambda_2}\right)\left(1 - q_{\mathrm{SC}}\left(q_{H_2} + q_{\mathrm{SC}}\right)2^{-(\lambda_0+\lambda_1)}\right) \cdot \left(1 - q_{\mathrm{SC}}\left(q_{H_3} + q_{\mathrm{SC}}\right)2^{-\lambda}\right)\left(1 - q_{\mathrm{USC}} 2^{-\lambda_2}\right) \tag{8}$$

下面，定义通过上述模拟的预言机来攻破签密体制的游戏。

1) 初始化阶段。挑战者 C 运行 Setup 算法，生成系统主密钥 MSK 和公开参数 PP，并将 PP 发给敌手 $\mathcal{A}$。

2) 询问阶段。$\mathcal{A}$ 通过上述预言机向挑战者发起多次的 KeyGen、Signcrypt 和 Unsigncrypt 询问。

3) 挑战阶段。$\mathcal{A}$ 输出 2 个消息 $\{m_0, m_1\}$，挑战者 C 随机选择一个比特 b，对消息 m_b 计算签密文 σ^*，并将 σ^* 发送给 $\mathcal{A}$。

4) 第二次询问阶段。敌手 $\mathcal{A}$ 仍可进行各种预言询问，但不能对将要挑战的密文 σ^* 进行相应的 Unsigncrypt 询问。

5) 猜测阶段。攻击者 $\mathcal{A}$ 输出比特 b'，经分析知，该模拟等同于敌手 $\mathcal{A}$ 的实际攻击环境，敌手 $\mathcal{A}$ 只有通过询问 H_1-oracle 得到 ω，才能猜测成功，定义事件 E_A 为挑战者 C 在记录表 L_{H_1} 中选择正确记录 ω，则该事件发生的概率为 $\dfrac{1}{q_{H_1}+q_{H_2}+q_{\mathrm{SC}}}$；若由选择的记录得到 $b = b'$，则 C 将能有效判别 ω 是否为模 N 的二次剩余。

下面，对挑战者 C 成功的概率进行分析，定义事件 E 表示敌手 $\mathcal{A}$ 在猜测阶段成功输出比特 $b = b'$，事件 E' 表示模拟成功。在模拟成功并选择正确记录的情况下，敌手 $\mathcal{A}$ 输出正确比特说明挑战者 C 可以成功解决困难假设。

定义 C 成功的优势为 $\varepsilon' = \Pr[E \cap E' \cap E_A]$，则有

$$\begin{cases} \Pr[E \cap E' \cap E_A] = \Pr[E]\Pr[E']\Pr[E_A] \\ \Pr[E] = \varepsilon_{\mathrm{CCA2}} \\ \Pr[E'] \geqslant \theta \\ \Pr[E_A] = \dfrac{1}{q_{H_1}+q_{H_2}+q_{\mathrm{SC}}} \end{cases}$$

$$\Rightarrow \varepsilon' \geqslant \theta \frac{\varepsilon_{\mathrm{CCA2}}}{q_{H_1}+q_{H_2}+q_{\mathrm{SC}}} \tag{9}$$

证毕。

保密性分析表明，敌手 $\mathcal{A}$ 成功攻破 CBSC 方案保密性的优势与一个不可忽略量的乘积不大于挑战者 C 成功解决二次剩余假设的优势。

5.3 不可伪造性

定理 3 如果在概率多项式时间内存在一个敌手 $\mathcal{A}$ 能够以 $\mathrm{Adv}_{\mathcal{A}}^{\text{CBSC-IND-CPA}} = \varepsilon_{\mathrm{CPA}}$ 的优势来赢得 3.2 节的游戏（最多进行 q_{H_1} 次 H_1 询问、q_{H_2} 次 H_2 询问、q_{H_3} 次 H_3 询问、q_{SK} 次密钥生成询问、q_{SC} 次签密询问、q_{USC} 次解签密询问），那么存在一个挑战者 C 以

$\mathrm{Adv}_C^{\mathbb{QR}}=\varepsilon'$ 的优势判断出模 N 的二次剩余问题，其中

$$\varepsilon' \geqslant \theta \frac{\varepsilon_{\mathrm{CPA}}}{\left(q_{H_1}+q_{\mathrm{SC}}\right)\left(q_{H_2}+q_{\mathrm{SC}}\right)} \tag{10}$$

$$\theta=\left(1-q_{\mathrm{SK}}2^{-\lambda_2}\right)\left(1-q_{\mathrm{SC}}\left(q_{H_2}+q_{SC}\right)2^{-(\lambda_0+\lambda_1)}\right)\cdot \left(1-q_{\mathrm{SC}}\left(q_{H_3}+q_{\mathrm{SC}}\right)2^{-\lambda}\right)\cdot \left(1-q_{\mathrm{USC}}2^{-\lambda_2}\right) \tag{11}$$

证明　设敌手 $\mathcal{A}$ 是攻击 CBSC-EUF-CMA 安全性的攻击者，定义 L_{H_1}、L_{H_2}、L_{H_3}和L_{SK} 这 4 个记录表来记录相应的预言机询问和密钥生成询问。与保密性分析中定义相同，签密过程可以看作 $g_S\left(f_R,H_3\left(c_1\right)\right)\to\sigma$。

在攻击签密体制不可伪造性时进行和定理 2 询问阶段一样的多项式有界次询问，并且其询问也是适应性的，只是不返回明文消息 m。

下面，定义通过上面模拟的预言机来攻破签密体制的游戏。

1) 初始化阶段。挑战者 C 运行 Setup 算法，生成系统主密钥 MSK 和公开参数 PP，并将 PP 发给敌手 $\mathcal{A}$。

2) 询问阶段。敌手 $\mathcal{A}$ 通过上述预言机发起各种询问，同定理 2 询问阶段相同。

3) 伪造阶段。进行上述有界次询问后，敌手 $\mathcal{A}$ 输出伪造的密文，假设签密接收者为 R，由机密性分析可知，该模拟等同于敌手 $\mathcal{A}$ 的实际攻击环境，敌手 $\mathcal{A}$ 必须通过 H_1 询问和 H_2 询问来得到消息 m^* 对应的 ω^*，才能伪造成功，其中定义事件 E_A 为挑战者 C 在记录表 L_{H_1} 和 L_{H_2} 中选择正确记录 ω^*，则该事件发生的概率为 $\dfrac{1}{\left(q_{H_1}+q_{\mathrm{SC}}\right)\left(q_{H_2}+q_{\mathrm{SC}}\right)}$；若选择的记录正确，则 C 将能有效判别 ω^* 是否为模 N 的二次剩余。

下面，分析挑战者 C 成功的概率，事件 E 表示敌手 $\mathcal{A}$ 成功伪造一个有效的密文 σ^*，并通过了验证，事件 E' 表示模拟成功。在模拟成功并选择正确记录的情况下，敌手 $\mathcal{A}$ 成功伪造有效密文说明挑战者 C 可以成功解决困难假设。

定义 C 成功的优势为 $\varepsilon'=\Pr\left[E\cap E'\cap E_A\right]$，则有

$$\begin{cases}\Pr\left[E\cap E'\cap E_A\right]=\Pr\left[E\right]\Pr\left[E'\right]\Pr\left[E_A\right]\\ \Pr\left[E\right]=\varepsilon_{\mathrm{CPA}}\\ \Pr\left[E'\right]\geqslant\theta\\ \Pr\left[E_A\right]=\dfrac{1}{\left(q_{H_1}+q_{\mathrm{SC}}\right)\left(q_{H_2}+q_{\mathrm{SC}}\right)}\end{cases}$$

$$\Rightarrow \varepsilon' \geqslant \theta \frac{\varepsilon_{\mathrm{CPA}}}{\left(q_{H_1}+q_{\mathrm{SC}}\right)\left(q_{H_2}+q_{\mathrm{SC}}\right)} \tag{12}$$

证毕。

不可伪造性分析表明，敌手 $\mathcal{A}$ 成功攻破 CBSC 方案不可伪造性的优势与一个不可忽略量的乘积不大于挑战者 C 成功解决二次剩余假设的优势。

已知任意多项式时间的攻击者都不可能以不可忽略的优势解决二次剩余假设问题，即可知任意多项式时间的敌手不可能攻破 CBSC 方案的保密性和不可伪造性。

6　效率分析

6.1　计算效率分析

目前，缺乏同类基于 Cocks 的 IBE 密码体制的签密方案，本节则将 CBSC 方案与其他现有的基于双线性对[10-11,15-16]及椭圆曲线离散对数[6,13]的方案进行对比分析。由于不同方案的效率运算单位及其耗时不统一，为了能够使不同方案的签密与解签密过程在同一指标下进行效率对比，本节首先基于文献[14]方案中的数据定义了不同的符号及符号换算，如表 1 所示。

表 1　　**符号定义及换算**

符号	定义
T_m	执行模乘运算所需的时间
T_b	执行双线性配对操作所需的时间，$T_b\approx 87T_m$
T_{be}	执行双线性配对幂运算所需的时间，$T_{be}\approx 43.5T_m$
T_{em}	执行椭圆曲线标量点乘法运算所需的时间，$T_{em}\approx 29T_m$
T_i	执行模逆运算所需的时间，$T_i\approx 11.6T_m$
T_a	执行雅可比符号运算所需的时间，$T_a\approx 6.5T_m$

表 1 中，与文献[14]方案数据相似，为了实现与 1 024 bit 的 RSA 密钥相当的安全性，基于双线性配对的方案在具有嵌入度 2 和素数阶 p 的超奇异椭圆曲线 $E\left(F_p\right):y^2=x^3+x$ 上执行 Tate 配对，其中

形式为 $p=2^{159}+2^{17}+1$ 的 160 bit 的 Solinas 素数和至少为 512 bit 的素数 q 满足条件 $q+1=12pr$。为了达到相同的安全性，基于无配对的椭圆曲线方案在 $F_{2^{163}}$ 上定义为 $y^2=x^3+ax^2+b$ 的 Koblitz 曲线上执行运算，其中 $a=1$ 且 b 为一个 163 bit 的随机数。基于配对构造的方案中 512 bit 随机数提供的安全性等同于无配对方案中 160 bit 随机数提供的安全性。因此，在本文方案中，假设 $H_i\left(i=0,1,2,3\right)$ 的输出为 160 bit，雅可比符号运算为 1 024 bit。

由表 1 可知，执行一次双线性配对运算的时间是执行一次模乘运算所需时间的 87 倍，而执行一次椭圆曲线标量点乘运算所需时间是执行一次模乘运算所需时间的 29 倍，但执行一次雅可比符号运算的时间只有执行一次模乘运算所需时间的 6.5 倍。因此，执行一次双线性对运算相当于可以执行 13 次雅可比符号运算，执行一次椭圆曲线标量点乘运算相当于可以执行 4 次雅可比符号运算。综上所述，执行雅可比符号运算的计算效率相对较高。

表 2 对比了 CBSC 方案与其他方案中用户执行一次签密操作、一次解签密操作需花费的计算成本，对比过程忽略了方案中都存在的哈希函数运算以及异或运算。

表 2　　计算效率比较

方案类别	方案	签密	解签密
双线性对	文献[10]	$2T_{em}+T_b\approx 203T_m$	$T_b+T_{be}\approx 130.5T_m$
	文献[11]	$3T_{em}+T_b+T_{be}\approx 217.5T_m$	$4T_b+4T_{be}\approx 522T_m$
	文献[15]	$4T_{be}\approx 174T_m$	$3T_{be}+T_b\approx 217.5T_m$
	文献[16]	$T_b+5T_{em}\approx 232T_m$	$3T_b+3T_{em}\approx 348T_m$
椭圆曲线离散对数	文献[13]	$7T_{em}\approx 203T_m$	$8T_{em}\approx 232T_m$
	文献[6]	$4T_{em}\approx 116T_m$	$2T_{em}\approx 58T_m$
二次剩余	CBSC	$2T_a\approx 13T_m$	$2T_a+2T_i\approx 36.2T_m$

分析结果表明，在签密和解签密的计算效率上 CBSC 方案明显优于其他方案。一方面，与基于双线性对的签密方案[10-11, 15-16]相比，由表 2 可以看出，文献[15]方案签密过程中不需要进行配对运算，解签密过程只需进行一次配对运算。尽管文献[15]方案相比于文献[10-11,16]方案所需的配对数量都要少，但签密过程所需时间仍是 CBSC 方案的 13 倍，解签密过程也需花费 CBSC 方案 6 倍的时间。因此，由于 CBSC 方案主要用到计算量较小的雅可比符号求值和模的求逆运算，在签密和解签密的时间上远小于基于双线性对的签密方案；另一方面，与基于椭圆曲线离散对数的签密方案[6,13]相比，虽然两者都不存在双线性对运算，但从表 2 可知，签密过程中文献[6]方案所需时间仍是 CBSC 方案的 8 倍，解签密过程花费时间虽与 CBSC 方案相差不大，但也是 CBSC 方案的 1.5 倍。综上所述，本文提出的 CBSC 方案有较高的计算效率。

6.2 仿真实验分析

对 CBSC 方案进行仿真实验，在 3.60 GHz 的 8 核 64 位 Intel(R) Core(TM)i7-4790U 处理器、8 GB 内存（RAM）、Windows 7 操作系统的实验环境进行实验，选用 Visual studio 2017 作为实验平台、C++ 作为实验编程语言，分别对 KeyGen 算法、Signcrypt 算法和 Unsigncrypt 算法进行模拟运行。使用不同长度的明文消息运行 9 次实验，比较了不同明文消息进行签密、解签密的执行时间，以达到对方案的计算效率进行验证的目的，实验结果如图 1 所示。

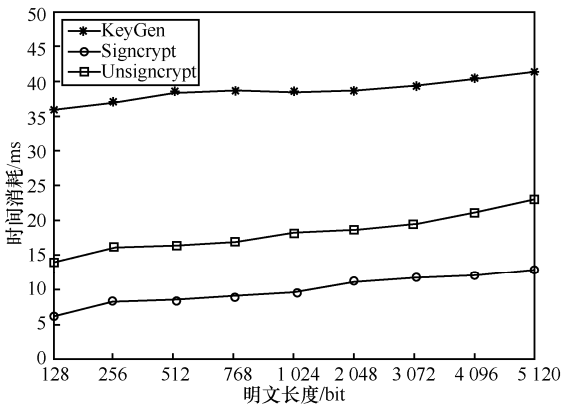

图 1　不同明文长度下方案执行时间

图 1 的实验数据表明，CBSC 签密方案最耗时的部分是密钥生成部分，签密算法的耗时低于解签密算法耗时，并从某一个初值开始随消息长度增大呈缓慢的增长趋势。由于 CBSC 签密方案在签密过程中除哈希运算外只存在雅可比符号求值运算耗时，而解签密过程除哈希运算外还存在雅可比符号求值及模的求逆运算的耗时，此外，因为签密方案中雅可比符号运算及模逆运算计算效率都相对较高，因此方案的签密、解签密过程的耗时都相对少。综上可以得出，实验结果与理论分析是一致的。

进一步地，类似于文献[17]，基于表 1 一样的数据设置，在与上述相同的实验环境下，只是实验过程采用密码函数库 miracl 进行操作，得到表 1 相

关运算操作的单次运行时间，如表 3 所示。

表 3　　相关操作单次运行时间

符号	运行时间/ms
T_b	30.624
T_{be}	14.312
T_{em}	9.541
T_i	4.832
T_a	2.288

基于表 3，将 CBSC 方案用图 1 相同的实验环境及操作语言与目前较高效的基于双线性对的签密方案[10-11,15-16]进行对比，实验结果如图 2 所示。

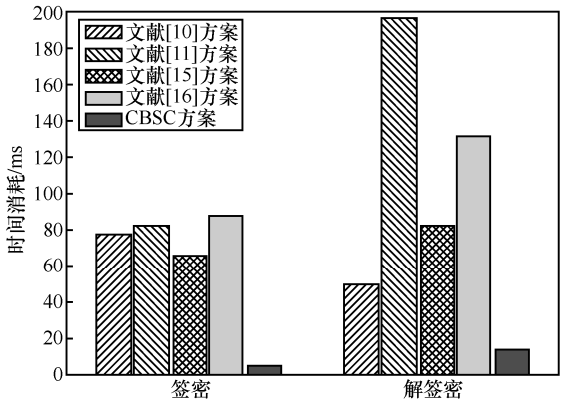

图 2　与基于双线性对的方案执行时间对比

图 2 的实验结果表明，对比基于双线性对的签密方案，无论是在签密算法还是解签密算法的执行时间都远少于有双线性配对运算的签密方案，签密过程中相对于时间最短的文献[15]方案仍然快出接近 13 倍的时间，解签密过程与耗时最少的文献[10]方案相比仍快出 3 倍左右，与 6.1 节中理论分析的计算效率结果一致。

同理，基于表 3 将 CBSC 方案与基于椭圆曲线离散对数的签密方案[6,13]进行对比并仿真实现，实验结果如图 3 所示。

图 3 的实验数据表明，将 CBSC 方案与基于椭圆曲线上的离散对数方案对比后，与计算效率较高的文献[6]方案对比数据发现，解签密过程虽然耗时相差不大，但签密过程的耗时显著减少。综上可得，该方案的计算效率具有显著提升。效率分析表明，CBSC 方案适合 5G 网络下的基础安全保障，特别是类似于 eMBB 场景下的安全需求。

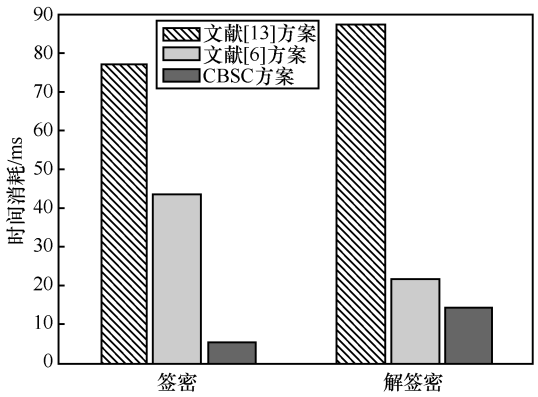

图 3　与基于离散对数的方案执行时间对比

7　结束语

本文针对基于双线性对构造的签密方案计算开销大的问题，利用二次剩余判定困难问题，提出了一种基于 Cocks 的 IBE 体制的高效签密方案。首先，利用二次剩余问题及雅可比求值运算具体构造该签密算法，在 Cocks 基于身份的加密方案的基础上结合二次剩余问题构造签名，在单个逻辑步骤中实现消息的保密性与认证性，该方案适用于对短会话密钥进行签密；然后，在随机预言机模型下对方案的安全性进行证明，将其安全性归约到数论中的二次剩余判别困难问题，证明了方案满足保密性和不可伪造性；最后，通过方案分析进行计算效率对比发现，所提方案无论是与已有的基于双线性对还是椭圆曲线上的离散对数构造的签密方案相比，都具有较高的计算效率。综上，本文所提 CBSC 方案在确保签密方案具有基于身份特性的同时，实现了高安全性和高效计算。因此，CBSC 方案的高效性与安全性能为 5G 网络提供了基础安全保障。

参考文献：

[1] ZHENG Y, IMAI H. How to construct efficient signcryption schemes on elliptic curves[J]. Information Processing Letters, 1998, 68(5): 227-233.

[2] MALON-LEE J. Identity-based signcryption[J]. IACR Cryptology ePrint Archive, 2002: 98.

[3] 冯登国, 徐静, 兰晓. 5G 移动通信网络安全研究[J]. 软件学报, 2018, 29(6): 1813-1825.
FENG D G, XU J, LAN X. Study on 5G mobile communication network security[J]. Journal of Software, 2018, 29(6): 1813-1825.

[4] ZHENG Y. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)[C]//International Cryptology Conference. Berlin: Springer, 1997: 165-179.

[5] SHIN J, LEE K, SHIM K, et al. New DSA-verifiable signcryption schemes[C]//International Conference on Information Security and

Cryptology. Berlin: Springer, 2002: 35-47.
[6] YU H, YANG B. Pairing-free and secure certificateless signcryption scheme[J]. The Computer Journal, 2017, 60(8): 1187-1196.
[7] REZAEIBAGHA F, MU Y, ZHANG S, et al. Provably secure (broadcast) homomorphic signcryption[J]. International Journal of Foundations of Computer Science, 2019, 30(4): 511-529.
[8] LIBERT B, QUISQUATER J. A new identity based signcryption scheme from pairings[C]//IEEE Information Theory Workshop. Piscataway: IEEE Press, 2003: 155-158.
[9] WANG H, LIU Z, LIU Z, et al. Identity-based aggregate signcryption in the standard model from multilinear maps[J]. Frontiers of Computer Science in China, 2016, 10(4): 741-754.
[10] REDDI S, BORRA S. Identity-based signcryption groupkey agreement protocol using bilinear pairing[J]. Informatica (Iithuanian Academy of Sciences), 2017, 41(1): 31-37.
[11] ZHOU C, ZHANG Y, WANG L. A provable secure identity-based generalized proxy signcryption scheme[J]. International Journal of Network Security, 2018, 20(6): 1183-1193.
[12] ZHOU Y, YANG B, ZHANG W, et al. Provably secure and efficient leakage-resilient certificateless signcryption scheme without bilinear pairing[J]. Discrete Applied Mathematics, 2016, 204: 185-202.
[13] ZHOU C, ZHAO Z, ZHOU W, et al. Certificateless key-insulated generalized signcryption scheme without bilinear pairings[J]. Security and Communication Networks, 2017, 2017: 1-17.
[14] ISLAM S K, KHAN M K, ALKHOURI A M, et al. Anonymous and provably secure certificateless multireceiver encryption without bilinear pairing[J]. Security and Communication Networks, 2015, 8(13): 2214-2231.
[15] KARATI A, BISWAS G P. A practical identity based signcryption scheme from bilinear pairing[C]//International Conference on Advances in Computing. Piscataway: IEEE Press, 2016: 832-836.
[16] GUO H, DENG L. Certificateless ring signcryption scheme from pairings[J]. International Journal of Network Security, 2020, 22(1): 102-111.
[17] HE D, WANG H, WANG L, et al. Efficient certificateless anonymous multi-receiver encryption scheme for mobile devices[J]. Soft Computing, 2017, 21(22): 6801-6810.
[18] COCKS C. An identity based encryption scheme based on quadratic residues[C]//IMA International Conference on Cryptography and Coding. Berlin: Springer, 2001: 360-363.
[19] CLEAR M, HUGHES A, TEWARI H, et al. Homomorphic encryption with access policies: characterization and new constructions[C]// International Conference on Cryptology in Africa. Berlin: Springer, 2013: 61-87.

[作者简介]

彭长根（1963− ），男，贵州锦屏人，博士，贵州大学教授、博士生导师，主要研究方向为隐私保护、密码学和大数据安全。

张小玉（1995− ），女，四川苍溪人，贵州大学硕士生，主要研究方向为密码学。

丁红发（1988− ），男，河南南阳人，贵州大学在站博士后，主要研究方向为隐私保护和大数据安全。

杨善慧（1994− ），女，贵州遵义人，贵州大学硕士生，主要研究方向为密码学。