基于编码的多接收方广义签密方案

韩益亮，王众
（武警工程大学密码工程学院，陕西 西安 710086）

摘 要：为解决具有多个接收方时的消息安全传输问题，设计了一种基于编码的多接收方广义签密方案。首先，设计了一个能够满足 IND-CCA2 安全的多次加密 McEliece 方案；然后，与 CFS 签名方案相结合设计了基于编码的多接收方签密与广义签密方案。安全性分析表明，该多接收方广义签密方案在机密性方面能够满足 IND-CCA2 安全，在不可伪造性方面能够满足 EUF-CMA 安全。与其他类似多接收方签密方案相比，所提方案不包含指数运算、双线性对运算等操作，具有较高的计算效率和抗量子计算的优势。与先签名后加密的方式相比，所提方案私钥数据量更少，效率更高。

关键词：编码密码；签密；广义签密；多接收方加密
中图分类号：TP309.7
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2020002

Code-based generalized signcryption scheme with multi-receiver

HAN Yiliang, WANG Zhong
College of Cryptographic Engineering, Engineering University of PAP, Xi’an 710086, China

Abstract: In order to solve the problem of secure transmission of messages with multiple receivers, a code-based generalized signcryption scheme with multi-receiver was designed. Firstly, a multi-encrypted McEliece scheme that can meet the security of IND-CCA2 was designed. Combined with the CFS signature scheme, the multi-receiver signcryption and generalized signcryption scheme based on code were designed. The security analysis shows that the multi-receiver generalized signcryption scheme can meet the security of IND-CCA2 in terms of confidentiality and can meet EUF-CMA security in terms of unforgeability. Compared with other similar multi-receiver signcryption schemes, the proposed scheme does not include exponential, bilinear pairing operations, etc., and has high computational efficiency and the advantage of anti-quantum computing. Compared with the method of signing-then-encrypting method, the proposed scheme has the smaller private key and higher efficiency.

Key words: code-based encryption, signcryption, generalized signcryption, multi-receiver encryption

1 引言

公钥密码技术是网络通信安全的核心技术，当前常用的公钥密码方案基于整数分解、离散对数、椭圆曲线离散对数等困难问题。Shor[1]提出了一种可以在量子计算机上运行的算法，能够解决整数分解、离散对数等问题，这给传统公钥密码带来了严重威胁，一旦实用化量子计算机出现，传统公钥密码就不再安全。整数分解和离散对数等问题都可归结为交换群的隐含子群问题，这类问题在量子计算机上可在多项式时间内求解，而在经典计算机上最好的算法仍然是指数级的。目前，一般认为抗量子

收稿日期：2019–06–27；**修回日期**：2019–11–15
基金项目：国家自然科学基金资助项目（No.61572521, No.U1636114）；国家重点研发计划基金资助项目（No.2017YFB0802000）；武警工程大学创新团队科学基金资助项目（No.KYTD201805）
Foundation Items: The National Natural Science Foundation of China (No.61572521, No.U1636114), The National Key Research and Development Program of China (No.2017YFB0802000), Engineering University of PAP Innovation Team Science Foundation (No.KYTD201805)

计算攻击的密码体制有如下几种[2]：基于多变量的密码体制[3]、基于格的密码体制[4]、基于编码的密码体制[5]以及基于 Hash 函数的密码体制[6]等。这些密码体制之所以能够抵抗量子计算攻击，是因为它们建立在 NP 完全问题（NP-complete problem）之上，量子计算机相比经典计算机对此类问题并没有明显优势[7]。基于编码的密码是目前比较受关注的一种抗量子密码，所依赖的困难问题是一般线性码的译码问题，主要思路是向码字中加入错误向量或根据纠错码的校验矩阵计算伴随式，在生成矩阵或校验矩阵未知时该问题为 NP 完全问题，且尚未发现该问题能归结为隐含子群问题，因而可以作为抗量子公钥算法比较好的候选方案之一。1978 年，Mceliece[8]最早利用 Goppa 码的性质提出了第一个编码密码方案，通常被称为 McEliece 方案。1986 年，Niederreiter[9]提出了 McEliece 方案的对偶体制，即 Niederreiter 方案。上述 2 种方案在安全性上完全等价，但是 Niederreiter 方案相比 McEliece 方案具有更高的传信率。2001 年，Courtois 等[10]提出了基于编码密码的签名方案——CFS 方案。2013 年，Mathew 等[11]通过密钥构造的改变使 CFS 签名方案的密钥量减少，提高了签名方案的使用效率。为了解决编码密码密钥量大的问题，用其他码字来代替 Goppa 码已经成为一种趋势，但是这会对方案的安全造成影响，这种影响已经出现在基于准循环（QC, quasi-cyclic）码[12]、低密度奇偶校验（LDPC, low density parity check）码[13]、准循环低密度奇偶校验（QC-LDPC, quasi-cyclic low-density parity-check）码[14]、卷积码[15]等码字的第一代 McEliece 变体方案中。还有一些使用 QC-LDPC 码[16]、准循环中密度奇偶校验（QC-MDPC, quasi-cyclic medium-density parity-check）码[17]等码字的变体方案，能够在不损坏安全性的前提下较好地达到密钥压缩的目的，例如 2017 年 Deneuville 等[18]提出的 Ouroboros 密钥交换协议、2018 年 Baldi 等[19]提出的 LEDAkem 密钥封装机制等。2018 年，Eaton 等[20]还提出通过多次加密的方式使编码密码方案的安全性达到 IND-CCA2（indistinguishability under adaptive chosen-ciphertext attack）的安全级别。

另一方面，保密和认证是信息安全的 2 个主要目标，在公钥密码领域，通常用加密技术来实现保密，用数字签名来实现认证。当需要同时满足保密和认证的要求时，通常的做法是先“签名”再“加密”或者先“加密”再“签名”，但这种方法效率不高，同时也无法确保安全性。Zheng[21]提出了在一个逻辑步骤内同时实现加密与签名功能的密码技术，能够提高效率和安全性。当系统中同时存在多种安全需求时，韩益亮等[22]提出的广义签密能够在签名方案、加密方案以及签密方案三者之间自适应地转换，能够单独或者同时提供保密和认证功能，更有效地节省系统资源。公钥密码是签密技术的基础，但是公钥密码存在一类密钥托管问题。2003 年，Al-Riyami 等[23]首次提出无证书密码体制，该体制的重点为密钥的管理，其将用户的私钥分成两部分：一部分由密钥生成中心（KGC, key generator center）生成，另一部分则由用户生成，这样就缓解了密钥托管问题。2008 年，Barbosa 等[24]将签密与无证书密码体制相结合，使无证书密码体制可以在一个逻辑步骤内完成加密与签名操作。同年，Selvi 等[25]将无证书签密方案推广到多接收者模型中。目前，已经提出的各种签密方案大多基于整数分解、离散对数、椭圆曲线离散对数等困难问题，也不能抵抗量子计算攻击。

本文通过对编码密码进行研究，设计了一个多接收方的广义签密方案。首先采用 QC-LDPC 码借鉴文献[20]中密钥封装机制中的加密方法，提出一种能够满足 IND-CCA2 的加密方案，在加密方案的基础上设计了一个多接收方的签密方案；然后进行改进得到一个基于编码密码的广义签密方案。

2 相关知识

2.1 校验子译码问题

给定一个(n, k)维的线性码，已知该码的最小汉明距离为 d，其校验矩阵为 $\boldsymbol{H} \in F_2^{(n-k)\times n}$，纠错能力为 t，满足 $d = 2t+1$。给定向量 $\boldsymbol{v} \in F_2^{(n-k)}$，寻找一个错误向量 $\boldsymbol{e} \in F_2^n$，使其汉明重量满足 $\mathrm{wt}(\boldsymbol{e}) \leqslant t$，且与向量 $\boldsymbol{v}$ 以及矩阵 $\boldsymbol{H}$ 满足方程 $\boldsymbol{v} = \boldsymbol{e}\boldsymbol{H}^{\mathrm{T}}$，寻找错误向量 $\boldsymbol{e}$ 的问题即为校验子译码问题（SD, syndrome decoding problem）。

校验子译码问题已被证明是 NP 完全问题，尚未发现该问题能归结为隐含子群问题。该问题是基于编码的密码所依赖的困难问题。

2.2 Mceliece 方案

Mceliece[8]于 1978 年提出一个基于 Goppa 码的密码方案，该方案是第一个基于编码的加密方案。

目前，采用 Goppa 码的 McEliece 方案仍是较为安全的方案。下面将具体介绍该方案的参数生成以及加解密过程。

参数生成。选择一个(n, k)维的线性码，该码的最小汉明距离为 d，其生成矩阵为 $\boldsymbol{G} \in F_2^{k\times n}$，能纠错重量为 t 的信息，满足 $d=2t+1$。选择一个 $k\times k$ 阶的二元随机非奇异矩阵 $\boldsymbol{M}$ 和一个 $n\times n$ 阶的二元随机置换矩阵 $\boldsymbol{P}$。那么，该方案的公钥为重量 t 以及矩阵 $\boldsymbol{G}^{\text{pub}}=\boldsymbol{MGP}$，私钥为矩阵 $\boldsymbol{G}$、$\boldsymbol{M}$、$\boldsymbol{P}$ 以及译码算法 β。

加密过程。对明文信息 $\boldsymbol{m}\in F_2^k$ 进行加密，随机选择一个重量为 t 的错误向量 $\boldsymbol{e}\in F_2^n$，计算 $\boldsymbol{c}=\boldsymbol{m}\boldsymbol{G}^{\text{pub}}+\boldsymbol{e}=\boldsymbol{mMGP}+\boldsymbol{e}$，得到密文为 $\boldsymbol{c}\in F_2^n$。

解密过程。首先对密文 $\boldsymbol{c}$ 右乘置换矩阵 $\boldsymbol{P}$ 的逆，即 $\boldsymbol{cP}^{-1}=\boldsymbol{mMG}+\boldsymbol{eP}^{-1}$。对 $\boldsymbol{cP}^{-1}$ 进行译码操作消除错误向量 $\boldsymbol{eP}^{-1}$，进而得到 $\overline{\boldsymbol{m}}=\boldsymbol{mM}$，$\overline{\boldsymbol{m}}$ 右乘私钥矩阵 $\boldsymbol{M}$ 的逆即可得明文 $\boldsymbol{m}$。

2.3　CFS 签名方案

基于 McEliece 方案，2001 年 Courtois 等[10]提出 CFS 签名方案，该方案是目前为数不多的安全的编码签名方案。CFS 签名方案的初始化、签名与验证过程如下。

初始化过程。取 C 是有限域 GF_q 上线性(n, k, d)Goppa 码，$n=2^a$，$d=2t+1$，$k=n-at$。$(n-k)\times n$ 阶矩阵 $\boldsymbol{H}$ 为二元(n, k, d)Goppa 码的校验矩阵，随机选取 GF(2)上的可逆矩阵 $\boldsymbol{S}$，其阶为 $(n-k)\times(n-k)$，再选取置换矩阵 $\boldsymbol{T}$，其阶为 $n\times n$。选择一个散列函数 $h:\{0,1\}^*\to F_2^{(n-k)}$。Goppa 码的快速译码算法为 $\beta_{H_t}()$，σ 为待签名消息。将 $(h,t,\overline{\boldsymbol{H}}=\boldsymbol{SHT})$ 公开，将 $(\boldsymbol{S},\boldsymbol{T},\boldsymbol{H},\beta_{H_t}())$ 保密。

签名过程如下。

1) 计算 σ 的散列值 $\boldsymbol{m}$，$\boldsymbol{m}=h(\sigma)$。

2) 在集合 $\{0,1,2,\cdots\}$ 中选择一个 i，计算 $\boldsymbol{m}_i=\boldsymbol{S}^{-1}h(\boldsymbol{m}\,\|\,i)$，找到一个最小的 i_0 使 $\beta_{H_t}(\boldsymbol{m}_i)$ 存在，则 $\boldsymbol{m}_{i_0}=\boldsymbol{S}^{-1}h(\boldsymbol{m}\,\|\,i_0)$。

3) 令 $\boldsymbol{v}=\beta_{H_t}(\boldsymbol{m}_{i_0})$，签名即为 $(i_0\,\|\,\boldsymbol{vT})$。

验证过程如下。

1) 计算 $a=h(h(\sigma)\|i_0)$，$\boldsymbol{b}=\overline{\boldsymbol{H}}(\boldsymbol{vT})^{\text{T}}$。

2) 如果 $\boldsymbol{a}=\boldsymbol{b}$，则签名成功；否则失败。

2.4　多接收方签密与广义签密

根据文献[26]，多接收方签密方案由以下步骤组成：系统参数生成、部分密钥生成、用户密钥生成、签密过程和解签密过程。

1) 系统参数生成。由密钥生成中心（KGC）进行，输入一个秘密参数 φ，进而返回系统参数 τ。

2) 部分密钥生成。由 KGC 进行，KGC 首先产生系统密钥 λ，然后输入 λ 和 τ，产生部分公钥 P 和部分私钥 S。

3) 用户密钥生成。输入公共参数 τ、部分公钥 P、部分私钥 S 以及用户的身份信息 ID_U，用户 U 执行该算法产生自己的公钥 P_U 和私钥 S_U。

4) 签密过程。由发送方 A 执行，输入公共参数 τ、明文 m、A 的身份信息 ID_A、私钥 S_A 以及接收者组 L 的公钥信息，最终输出签密文 c。

5) 解签密过程。由接收者 B 执行，输入公共参数 τ、签密文 c、A 的身份信息 ID_A、A 的公钥 P_A，以及接收者 B 的身份信息 ID_B 与私钥 S_B，若验证通过则最终解密得到明文 m，否则解签密失败。

多接收方的广义签密与多接收方的签密过程大致类似，不同之处在于需要再定义一个区分函数 $f(x)$ 来实现签名方案、加密方案以及签密方案这三者之间的转换。区分函数往往通过用户的公钥进行判断，进而实现转换的功能，具体来讲即当发送方 A 与接收者 B 均有公私钥时为签密方案，当发送方 A 没有公私钥而接收者 B 拥有时为加密方案，当接收者 B 没有公私钥而发送方 A 拥有时为签名方案，当收发双方均无公私钥时为普通的传信过程。

2.5　多接收方签密的安全模型

参考文献[26-27]可以得到适用于本文多接收方签密方案的安全模型。从机密性与不可伪造性入手，针对多接收方的签密方案，存在以下 2 种类型的攻击者：可以替换用户公钥信息但是不能获得 KGC 的主密钥，用攻击者 α_1 表示；可以获取 KGC 的主密钥但是不能替换其他用户公钥的攻击者，用 α_2 表示。

定义 1　机密性 1。在攻击游戏 1 中，没有一个攻击者 α 能够在多项式时间内以不可忽略的优势赢得 IND-CCA2-1 游戏，则说明该基于编码的多接收方签密方案满足适应性选择密文攻击下的不可区分性。

攻击者在 IND-CCA2-1 游戏中需满足以下 3 个限制：不能对挑战密文进行解签密询问，不能对挑战者的私钥进行询问，不能对系统的主密钥进行询问。

定义 2　机密性 2。在攻击游戏 2 中，没有一个攻击者 α 能够在多项式时间内以不可忽略的优势赢得 IND-CCA2-2 游戏，则说明该基于编码的多接收方签密方案满足适应性选择密文攻击下的不可区分性。

攻击者在 IND-CCA2-2 游戏中需要满足以下 3 个限制：不能对挑战密文进行解签密询问，不能对挑战者的私钥进行询问，不能对系统的主密钥进行替换。

定义 3　不可伪造性 1。在攻击游戏 1 中，没有一个攻击者 α 能够在多项式时间内以不可忽略的优势赢得 EUF-CMA（existential unforgeability against adaptive chosen messages attack）-1 游戏，则说明该基于编码的多接收方签密方案满足适应性选择消息攻击下的不可伪造性。

攻击者在 EUF-CMA-1 游戏中需满足以下 2 个限制：不能对挑战者的私钥进行询问，不能对系统的主密钥进行询问。

定义 4　不可伪造性 2。在攻击游戏 2 中，没有一个攻击者 α 能够在多项式时间内以不可忽略的优势赢得 EUF-CMA-2 游戏，则说明该基于编码的多接收方签密方案满足适应性选择消息攻击下的不可伪造性。

攻击者在 EUF-CMA-2 游戏中需满足以下 2 个限制：不能对挑战者的私钥进行询问，不能对系统的主密钥进行替换。

3　方案描述

3.1　多接收方的通信模型

具有多个接收方的一对多通信是当前最普遍的通信模式之一，如网络广播、多播等。在无线局域、物联网等网络环境下，也存在着许多一对多通信的方式。这种具有多个接收方的一对多通信由于其自身的开放性、智能化以及计算环境的复杂性带来了许多安全问题，最明显的是用户隐私的安全问题[28]。多接收方通信中的身份认证问题同样重要，通过有效的消息认证、设备认证，才能够防止冒名顶替和否认行为[29]。计算机系统需要根据不同用户的性质来提供不同的访问控制策略以有效地对用户隐私、数据安全以及身份进行保护。图 1 为多接收方通信模型。

1) 当发送方无密钥以及接收用户组存在无密钥成员时，发送方将不能对待签密消息 $\boldsymbol{m}$ 进行签名以及加密的操作，相当于直接把消息发送给接收用户组。由于对明文进行了处理，使合法的系统用户（设备）才能得到明文 $\boldsymbol{m}$。这种情况适用于普通用户（设备），即没有自己公私钥的用户（设备）与普通的用户或者设备组之间进行密级较低的通信，传输的信息对于系统用户（设备）是公开的，而对于非系统用户（设备）是加密的。

2) 当发送方有密钥而接收用户组存在无密钥成员时，相当于纯签名的过程。当接收用户组收到该信息后，可以利用系统私钥来解密得到明文 $\boldsymbol{m}$，再对签名 $\boldsymbol{s}$ 验证，确保信息来自对应的发送方且明文未被篡改。这种情况适用于发送方是高级的用户、计算机系统或者设备，而接收组是普通的用户或者设备，进而防止对高级用户（设备）所传输的信息进行篡改，以及对其冒名顶替，保障了可认证性。

3) 当发送方没有密钥而接收用户组中的成

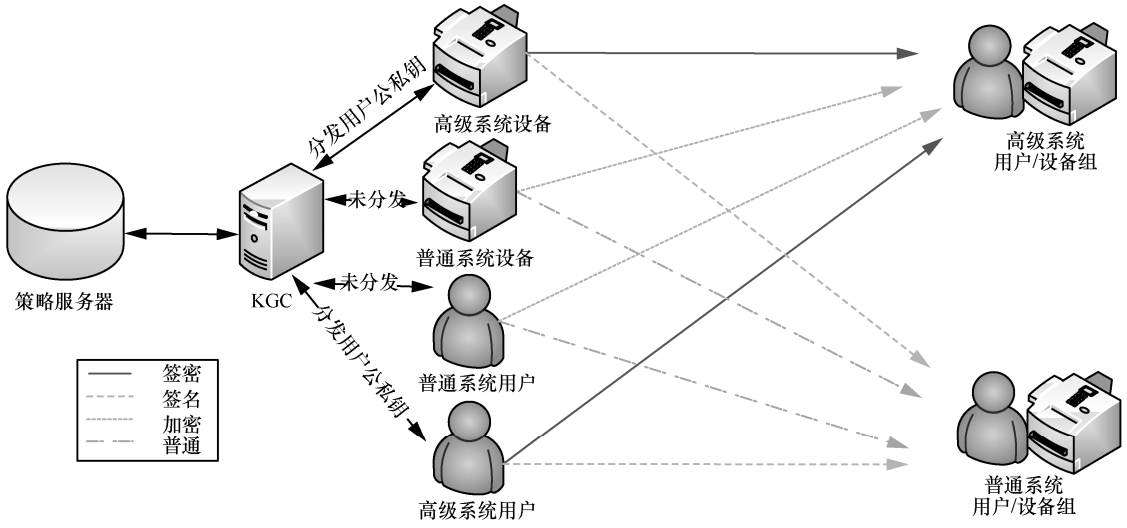

图 1　多接收方通信模型

员均有密钥时，相当于纯加密的过程。接收组收到该信息后利用各自的私钥以及系统私钥进行解密操作即可得到明文消息 $\boldsymbol{m}$。这种情况适用于发送方为普通用户或者计算机系统，其所发出的消息只想让指定的接收组收到，且接收方为高级的用户或者设备。这就保障了在多接收方的开放环境下数据传输的机密性。

4) 当接收用户组中的成员、发送方都有各自密钥时，该方案即为一个签密方案。只有拥有相应私钥的接收者可以对信息进行解签密。解签密的过程是接收组中的成员运用自己的私钥以及系统私钥进行解密得到明文，再利用发送方的公钥通过 $\boldsymbol{m}$ 对签名进行验证。这种情况适用于收发双方均为高级的用户、设备，进行密级较高的保密通信。

综上分析可知，当一个系统用户或者设备给其他多个接收者发送信息时，可以根据接收组成员的公私钥的存在情况自适应地实现多接收方的签密、加密与签名的转换。若接收组成员中有一个没有公钥即为签名过程或者是普通传输过程，若接收组成员中都有公钥即为签密或者加密的传输过程。本文所提广义签密方案需要实现不同安全级别的访问控制，而非系统用户则得不到任何信息。

3.2　多次加密的 McEliece 方案

根据文献[20]，一般编码密码方案的安全性达不到 IND-CCA2 的安全级别，但文献[20]给出了一种加密方法使编码密码的安全性能够达到 IND-CCA2 的安全级别。该加密方法是将待加密信息运用编码加密的方式进行多次加密产生多个密文，对这些密文进行解密，只有当这些密文全部解密失败时返回错误值 $\perp$，这样可以有效避免译码错误对安全性的影响。本节多次加密的 McEliece 方案采用 QC-LDPC 码，并以这种多次加密的方式来构造方案，以增加方案的安全性。

参数及密钥生成。取 Ω 是有限域 GF_q 上 (n, k, d) 阶的 QC-LDPC 码，$n=2^a$，$d=2t+1$，$k=n-at$。其生成矩阵为 $\boldsymbol{G}\in F_2^{k\times n}$，随机选取 GF(2)上的可逆矩阵 $\boldsymbol{S}$，其阶为 $k\times k$；再选取置换矩阵 $\boldsymbol{P}$，其阶为 $n\times n$。计算公钥为 $\overline{\boldsymbol{G}}=\boldsymbol{SGP}$，私钥即为矩阵 $(\boldsymbol{S},\boldsymbol{G},\boldsymbol{P})$ 以及译码算法 $\beta_t()$。另设一错误向量生成函数 $X:\{0,1\}^*\to\{\boldsymbol{e}|\boldsymbol{e}\in F_2^n,\mathrm{wt}(\boldsymbol{e})\leqslant t\}$ 以及二进制数字的循环左移函数。

根据文献[20]密钥封装中的加密方式，基于 QC-LDPC 码构造多次加密的 McEliece 方案。

1) 加密过程

Enc：输入待加密消息 $\boldsymbol{m}\in F_2^k$ 以及公钥 $\overline{\boldsymbol{G}}$。

for i=1 to b do

$X(\boldsymbol{m}\,\|\,i)\to\boldsymbol{e}_i$;

$\boldsymbol{m}\oplus\mathrm{PRF}(\boldsymbol{e}_i\,\|\,i)=\boldsymbol{x}_i$;

$\boldsymbol{x}_i\overline{\boldsymbol{G}}=\boldsymbol{x}_i\boldsymbol{SGP}+\boldsymbol{e}_i=\boldsymbol{c}_i$;

return $C=(\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_b)$;

2) 解密过程

Dec：输入密文消息组 $C=(\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_b)$，私钥 $(\boldsymbol{S},\boldsymbol{G},\boldsymbol{P})$，公钥 $\overline{\boldsymbol{G}}=\boldsymbol{SGP}$。

for i=1 to b do

$\mathrm{McEliece.Dec}(\boldsymbol{S},\boldsymbol{G},\boldsymbol{P},\boldsymbol{c}_i,\beta_t())\to(\boldsymbol{x}_i,\boldsymbol{e}_i)$;

if McEliece.Dec 首次解密成功

　set j=i;

if McEliece.Dec 的 b 次解密全部失败

　return $\perp$;

计算 $\boldsymbol{m}=\boldsymbol{x}_j\oplus\mathrm{PRF}(\boldsymbol{e}_j\,\|\,j)$;

$\mathrm{Enc}(\boldsymbol{m},\overline{\boldsymbol{G}})\to\overline{C}=(\overline{\boldsymbol{c}}_1,\overline{\boldsymbol{c}}_2,\cdots,\overline{\boldsymbol{c}}_b)$;

if $\boldsymbol{c}_i=\overline{\boldsymbol{c}}_i$ for all $i\in\{1,\cdots,b\}$

　return $\boldsymbol{m}$;

else

　return $\perp$;

加密过程中，每加密一次产生一个新的错误向量 $\boldsymbol{e}_i$ 来加密。解密过程中，需要对所有密文进行解密操作，译码成功则保留下来，所有密文译码不成功则解密失败，最终得到明文，根据明文 $\boldsymbol{m}$ 以及公钥 $\overline{\boldsymbol{G}}$ 并利用之前的加密算法进行加密操作，得到一组密文 $\overline{C}$ 来与原密文组 C 进行比较，每组都相同则解密成功，可以得到明文 $\boldsymbol{m}$。这种加密方法大大降低了译码错误所带来的安全性影响，这也是本文构造多次加密的 McEliece 方案最主要的原因。

3.3　多接收方签密方案

本节将依托 3.2 节中的多次加密的 McEliece 方案以及 CFS 签名方案并参考文献[26]，构造一个具有抗量子计算能力的多接收方签密方案。

1) 系统参数建立

取 Ω 是有限域 GF_q 上 (n, k, d)阶的 QC-LDPC 码，$n=2^a$，$d=2t+1$，$k=n-at$。其生成矩阵为 $\boldsymbol{G}\in F_2^{k\times n}$，校验矩阵为 $\boldsymbol{H}\in F_2^{(n-k)\times n}$，译码算法为 $\beta_t()$。设置 2 个安全函数 h_1 与 h_2，$h_1:\{0,1\}^*\to\{0,1\}^{n-k}$，$h_2:\{0,1\}^*\to\{0,1\}^k$。如 3.2 节中方案的参数及密钥生成过程，再设置错误向量生

成函数 $X:\{0,1\}^* \to \{\boldsymbol{e}|\boldsymbol{e}\in F_2^n, \mathrm{wt}(\boldsymbol{e})\leqslant t\}$ 以及二进制数字的循环左移函数 PRF。公开 (n,k,t,h_1,h_2)。

2) 部分密钥生成

① KGC 根据 QC-LDPC 码 Ω 随机选择 GF(2) 上的 $k\times k$ 阶可逆矩阵 $\boldsymbol{S}$，以及 $(n-k)\times(n-k)$ 阶可逆矩阵 $\boldsymbol{M}$，再选取 $n\times n$ 阶置换矩阵 $\boldsymbol{P}$。KGC 的系统公钥为 $\boldsymbol{G}^{\mathrm{pub}}=\boldsymbol{SGP}$ 和 $\boldsymbol{H}^{\mathrm{pub}}=\boldsymbol{MHP}$，$\boldsymbol{G}^{\mathrm{pub}}$ 与加密有关，$\boldsymbol{H}^{\mathrm{pub}}$ 与签名有关。系统私钥为 $(\boldsymbol{S},\boldsymbol{G},\boldsymbol{P},\boldsymbol{M},\beta_t())$，这里不再将 QC-LDPC 码的校验矩阵 $\boldsymbol{H}$ 写入私钥组，因为根据码的性质，有了生成矩阵便可根据 $\boldsymbol{GH}^{\mathrm{T}}=0$ 求得校验矩阵。

② KGC 根据 QC-LDPC 码 Ω 随机选择 GF(2) 上的 $k\times k$ 阶可逆矩阵 $\boldsymbol{S}_0$，以及 $(n-k)\times(n-k)$ 阶可逆矩阵 $\boldsymbol{M}_0$，再选取 $n\times n$ 阶置换矩阵 $\boldsymbol{P}_0$。计算 $\boldsymbol{G}_0=\boldsymbol{S}_0\boldsymbol{G}^{\mathrm{pub}}\boldsymbol{P}_0$，$\boldsymbol{H}_0=\boldsymbol{M}_0\boldsymbol{H}^{\mathrm{pub}}\boldsymbol{P}_0$，则部分公钥为 $(\boldsymbol{G}_0,\boldsymbol{H}_0)$，部分私钥为 $(\boldsymbol{S}_0\boldsymbol{S},\boldsymbol{G},\boldsymbol{PP}_0,\boldsymbol{M}_0\boldsymbol{M},\beta_t())$。KGC 通过秘密信道将部分私钥传递给合法用户，并公开自己的系统公钥。

3) 用户密钥生成

① 用户 U 取得 KGC 的部分公钥和部分私钥，并随机选择 GF(2)上的 $k\times k$ 阶可逆矩阵 $\boldsymbol{S}_U$，以及 $(n-k)\times(n-k)$ 阶可逆矩阵 $\boldsymbol{M}_U$，再选取 $n\times n$ 阶置换矩阵 $\boldsymbol{P}_U$。计算 $\boldsymbol{G}_U=\boldsymbol{S}_U\boldsymbol{G}_0\boldsymbol{P}_U$，$\boldsymbol{H}_U=\boldsymbol{M}_U\boldsymbol{H}_0\boldsymbol{P}_U$，则部分公钥为 $(\boldsymbol{G}_U,\boldsymbol{H}_U)$，部分私钥为 $(\boldsymbol{S}_U\boldsymbol{S}_0\boldsymbol{S},\boldsymbol{G},\boldsymbol{PP}_0\boldsymbol{P}_U,\boldsymbol{M}_U\boldsymbol{M}_0\boldsymbol{M},\beta_t())$。$F_0$ 代表采用系统公钥加密，F_i 代表采用用户 i 的公钥加密。

② 用户 U 将公钥 F_U（F_U 即为 $(\boldsymbol{G}_U,\boldsymbol{H}_U)$）传回 KGC。

4) 签密

身份为 ID_A 的用户 A，将 $\boldsymbol{m}\in F_2^k$ 传输给用户组 $L=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_\varsigma\}$。首先向 KGC 查询得到用户组 L 的公钥信息，进行如下操作。

① $F_2^k \xrightarrow{\$} \boldsymbol{r}, F_0(\boldsymbol{r})\to\boldsymbol{x}$。

② $\boldsymbol{Y}=h_1(\boldsymbol{m}\,\|\,ID_A\,\|\,\boldsymbol{x})$。

③ 在集合 $\{0,1,\cdots\}$ 中选择一个 a，并计算 $\boldsymbol{Y}_a=\boldsymbol{M}_A^{-1}h_1(\boldsymbol{Y}\,\|\,a)$，找到一个最小的 a_0 使 $\beta_t(\boldsymbol{Y}_a)$ 存在，则 $\boldsymbol{Y}_{a_0}=\boldsymbol{M}_A^{-1}h_1(\boldsymbol{Y}\,\|\,a_0)$。

④ 令 $\boldsymbol{v}=\beta_t(\boldsymbol{Y}_{a_0})$，$\boldsymbol{s}=(a_0\,\|\,\boldsymbol{vP}_A)$。

⑤ 对于 ID_i，$i=1,2,\cdots,\varsigma$，计算 $\boldsymbol{q}_i=h_2(\mathrm{ID}_i)$。

⑥ $\boldsymbol{W}_i=F_i(\boldsymbol{m}\oplus\boldsymbol{r}\oplus\boldsymbol{q}_i)$。

⑦ 对于用户组 L，计算 $\overline{L}=F_0(L)$。

⑧ 生成签密文 $\sigma=(\boldsymbol{s},\boldsymbol{W}_1,\boldsymbol{W}_2,\cdots,\boldsymbol{W}_\varsigma,\overline{L},x)$。

5) 解签密

用户 ID_i，$i=1,2,\cdots,\varsigma$，收到 $\sigma=(\boldsymbol{s},\boldsymbol{W}_1,\boldsymbol{W}_2,\cdots,\boldsymbol{W}_\varsigma,\overline{L},x)$ 后进行如下计算。

① 获取身份列表，$L=F_0^{-1}(\overline{L})$，提取对应的密文信息 $(\boldsymbol{s},\boldsymbol{W}_i,x)$。

② 计算 $\overline{\boldsymbol{r}}=F_0^{-1}(x)$，$\boldsymbol{q}_i=h_2(ID_i)$，$F_i^{-1}(\boldsymbol{W}_i)\to\boldsymbol{c}=\overline{\boldsymbol{m}}\oplus\overline{\boldsymbol{r}}\oplus\boldsymbol{q}_i$。

③ $\overline{\boldsymbol{m}}=\boldsymbol{c}\oplus\overline{\boldsymbol{r}}\oplus\boldsymbol{q}_i$。

④ 验证：$\eta=\boldsymbol{H}_A(\boldsymbol{vT}_A)^{\mathrm{T}}$，$\xi=h_1(h_1(\overline{\boldsymbol{m}}\,\|\,ID_A\,\|\,\boldsymbol{x})\|a_0)=h_1(\overline{\boldsymbol{Y}}\,\|\,a_0)$，判断 η 与 ξ 是否相等，相等则验证通过，获得正确明文；否则接收失败。

正确性分析。当签密与解签密过程正确时则说明签密方案正确。用户 ID_i（$i=1,2,\cdots,\varsigma$）收到 $\sigma=(\boldsymbol{s},\boldsymbol{W}_1,\boldsymbol{W}_2,\cdots,\boldsymbol{W}_\varsigma,\overline{L},x)$ 后，首先利用系统私钥提取出自己的那一部分密文，再利用系统私钥求解出随机数 $\overline{\boldsymbol{r}}$，然后就可以利用自己的私钥来求解密文，即 $F_i^{-1}(\boldsymbol{W}_i)\to\boldsymbol{c}=\overline{\boldsymbol{m}}\oplus\overline{\boldsymbol{r}}\oplus\boldsymbol{q}_i$。由于已知 $\overline{\boldsymbol{r}}$、$\boldsymbol{c}$ 和 $\boldsymbol{q}_i$，因此可以求出明文 $\overline{\boldsymbol{m}}$。拥有了明文后，可运用发送方 A 的公钥进行下一步的验证，根据 CFS 签名方案，当且仅当 $\eta=\boldsymbol{H}_A(\boldsymbol{vT}_A)^{\mathrm{T}}=\xi=h_1(h_1(\overline{\boldsymbol{m}}\,\|\,\mathrm{ID}_A\,\|\,\boldsymbol{x})\|a_0)$ 时，才可得到正确的明文。

3.4 基于编码密码的多接收方广义签密方案

本节基于编码密码的多接收方广义签密方案仍然是依托 3.2 节中多次加密的 McEliece 方案以及 CFS 签名方案，在 3.3 节基于编码密码的多接收方签密方案的基础上加以改进而构造的，因此其参数、部分密钥以及用户密钥的生成都与 3.3 节中基本相同，只是在参数生成时多构造一个安全函数 $h_3:\{0,1\}^*\to\{0,1\}^k$。

3.4.1 区分函数构造以及签密与解签密过程

1) 定义区分函数 $f(x)$

区分函数实现签名、加密或签密功能三者之间转换，往往以用户是否存在公钥来进行判断。当用户的公钥 $\boldsymbol{G}_U=\varnothing$ 时即为不存在公私钥，则 $f(x)=\boldsymbol{0}$，此处 $\boldsymbol{0}$ 代表 k 维零向量；当用户的公钥 $\boldsymbol{G}_U\neq\varnothing$ 时即存在公私钥时，则 $f(x)=\boldsymbol{1}$，此处 $\boldsymbol{1}$ 代表 k 维单位向量。因此区分函数可表示如下。

$$f(x)=\begin{cases}\boldsymbol{0}, & \boldsymbol{G}_U=\varnothing\\ \boldsymbol{1}, & \boldsymbol{G}_U\neq\varnothing\end{cases} \tag{1}$$

2) 签密

身份为 ID_A 的用户 A，将 $\boldsymbol{m}\in F_2^k$ 传输给用户组 $L=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_\varsigma\}$。首先向 KGC 查询得到用户组 L 的公钥信息，进行如下操作。

① $F_2^k \xrightarrow{\$}\boldsymbol{r}, F_0(\boldsymbol{r})\to\boldsymbol{x}$。

② 若 $f(\boldsymbol{G}_A)\neq\boldsymbol{0}$，$\boldsymbol{Y}=h_1(\boldsymbol{m}\,\|\,ID_A\,\|\,\boldsymbol{x})$，在集合 $\{0,1,\cdots\}$ 中选择一个 a，并计算 $\boldsymbol{Y}_a=\boldsymbol{M}_A^{-1}h_1(\boldsymbol{Y}\,\|\,a)$，找到一个最小的 a_0 使 $\beta_t(\boldsymbol{Y}_a)$ 存在，则 $\boldsymbol{Y}_{a_0}=\boldsymbol{M}_A^{-1}h_1(\boldsymbol{Y}\,\|\,a_0)$，令 $\boldsymbol{v}=\beta_t(\boldsymbol{Y}_{a_0})$，$\boldsymbol{s}=(a_0\,\|\,\boldsymbol{v}\boldsymbol{P}_A)$；否则 $\boldsymbol{s}=\varnothing$。

③ 对于用户 ID_i ($i=1,2,\cdots,\varsigma$)，$F_2^k\xrightarrow{\$}\boldsymbol{r}_i$ 计算 $\boldsymbol{q}_i=h_2(\mathrm{ID}_i)$。

④ 对于用户组 L，设 $\kappa=f(\boldsymbol{G}_1)f(\boldsymbol{G}_2)\cdots f(\boldsymbol{G}_{\varsigma-1})f(\boldsymbol{G}_\varsigma)$，若 $\kappa\neq\boldsymbol{0}$ 则 $F_i(\boldsymbol{r}_i)\to\boldsymbol{c}_i$，否则 $\boldsymbol{r}_i\to\boldsymbol{c}_i$。

⑤ $\boldsymbol{W}_i=\boldsymbol{m}\oplus h_3(\boldsymbol{r})\oplus h_2(\boldsymbol{r}_i\oplus\boldsymbol{q}_i)\kappa$。

⑥ 对于用户组 L，计算 $\overline{L}=F_0(L)$。

⑦ 生成签密文 $\sigma=(\boldsymbol{s},\boldsymbol{W}_1,\boldsymbol{W}_2,\cdots,\boldsymbol{W}_\varsigma,\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_\varsigma,\overline{L},x)$。

3) 解签密

用户 ID_i ($i=1,2,\cdots,\varsigma$)收到 $\sigma=(\boldsymbol{s},\boldsymbol{W}_1,\boldsymbol{W}_2,\cdots,\boldsymbol{W}_\varsigma,\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_\varsigma,\overline{L},x)$ 后进行如下计算。

① 获取身份列表，$L=F_0^{-1}(\overline{L})$，提取对应的密文信息 $(\boldsymbol{s},\boldsymbol{W}_i,\boldsymbol{c}_i,x)$。

② 若 $\kappa=f(\boldsymbol{G}_1)f(\boldsymbol{G}_2)\cdots f(\boldsymbol{G}_{\varsigma-1})f(\boldsymbol{G}_\varsigma)=\boldsymbol{0}$，则 $\boldsymbol{c}_i\to\tilde{\boldsymbol{r}}_i$；否则 $F_i^{-1}(\boldsymbol{c}_i)\to\tilde{\boldsymbol{r}}_i$。

③ 计算 $\overline{\boldsymbol{r}}=F_0^{-1}(x)$，$\boldsymbol{q}_i=h_2(\mathrm{ID}_i)$。

④ $\overline{\boldsymbol{m}}=\boldsymbol{W}_i\oplus h_3(\overline{\boldsymbol{r}})\oplus h_2(\tilde{\boldsymbol{r}}_i\oplus\boldsymbol{q}_i)\kappa$。

⑤ 若 $f(\boldsymbol{G}_A)=\boldsymbol{0}$，输出 $\overline{\boldsymbol{m}}$；否则进行以下验证：

$\eta=\boldsymbol{H}_A(\boldsymbol{v}\boldsymbol{T}_A)^{\mathrm{T}}$

$\xi=h_1(h_1(\overline{\boldsymbol{m}}\,\|\,\mathrm{ID}_A\,\|\,\boldsymbol{x})\,\|\,a_0)=h_1(\overline{\boldsymbol{Y}}\,\|\,a_0)$

判断 η 与 ξ 是否相等，相等则验证通过获得正确明文，否则接收失败。

3.4.2 正确性分析

当用户 ID_i ($i=1,2,\cdots,\varsigma$)收到 $\sigma=(\boldsymbol{s},\boldsymbol{W}_1,\boldsymbol{W}_2,\cdots,\boldsymbol{W}_\varsigma,\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_\varsigma,\overline{L},x)$ 后，最终得到的密文组有以下 4 种形式：$(\boldsymbol{s},\boldsymbol{W}_i,\boldsymbol{c}_i,x)$、$(\varnothing,\boldsymbol{W}_i,\boldsymbol{c}_i,\boldsymbol{x})$、$(\boldsymbol{s},\boldsymbol{m}\oplus h_3(\boldsymbol{r}),\boldsymbol{r}_i,\boldsymbol{x})$、$(\varnothing,\boldsymbol{m}\oplus h_3(\boldsymbol{r}),\boldsymbol{r}_i,\boldsymbol{x})$。

当收发双方都拥有公私钥时，密文组为 $(\boldsymbol{s},\boldsymbol{W}_i,\boldsymbol{c}_i,x)$。接收者利用自己的私钥解密得到随机数 $\tilde{\boldsymbol{r}}_i$，利用系统私钥进行解密得到随机数 $\overline{\boldsymbol{r}}$，进而可以利用 $\overline{\boldsymbol{m}}=\boldsymbol{W}_i\oplus h_3(\overline{\boldsymbol{r}})\oplus h_2(\tilde{\boldsymbol{r}}_i\oplus\boldsymbol{q}_i)\kappa$ 求解得出明文，将该明文利用 CFS 签名方案中的验证方法进行验证：$\eta=\boldsymbol{H}_A(\boldsymbol{v}\boldsymbol{T}_A)^{\mathrm{T}}=\xi=h_1(h_1(\overline{\boldsymbol{m}}\,\|\,\mathrm{ID}_A\,\|\,\boldsymbol{x})\,\|\,a_0)=h_1(\overline{\boldsymbol{Y}}\,\|\,a_0)$，等式成立则说明获得了正确的信息。

当发送方没有公私钥而接收方有时，密文组为 $(\varnothing,\boldsymbol{W}_i,\boldsymbol{c}_i,\boldsymbol{x})$，接收方收到密文组后，利用自己的私钥进行解密得到随机数 $\tilde{\boldsymbol{r}}_i$，利用系统私钥进行解密得到随机数 $\overline{\boldsymbol{r}}$，再利用 $\overline{\boldsymbol{m}}=\boldsymbol{W}_i\oplus h_3(\overline{\boldsymbol{r}})\oplus h_2(\tilde{\boldsymbol{r}}_i\oplus\boldsymbol{q}_i)\kappa$ 求解得出明文。

当发送方拥有公私钥而接收方不具有时即为签名方案，不同于普通签名，只有系统中的合法用户才可以得到正确的信息，此时的密文组为 $(\boldsymbol{s},\boldsymbol{m}\oplus h_3(\boldsymbol{r}),\boldsymbol{r}_i,\boldsymbol{x})$，接收方收到密文后，可以直接获取随机数 $\tilde{\boldsymbol{r}}_i$，再利用系统私钥进行解密得到随机数 $\overline{\boldsymbol{r}}$，进而可以利用 $\overline{\boldsymbol{m}}=\boldsymbol{W}_i\oplus h_3(\overline{\boldsymbol{r}})\ \oplus h_2(\tilde{\boldsymbol{r}}_i\oplus\boldsymbol{q}_i)\kappa$ 求解得出明文，最后利用与第一种情况相同的方法进行验证即可。

当收发双方均无公私钥时，相对于直接传输明文，发送方只对明文用系统公钥进行了加密，当接收方为系统用户时，便可利用系统私钥进行解密最终获得明文。

3.5 广义签密方案自适应性

根据多接收方广义签密的模型[30]并结合上述方案的构造可以看出，当发送方向某一用户组发送信息时，根据发送方以及接收用户组的密钥拥有情况存在以下 4 种情况。

1) 发送方以及接收用户组均无密钥。根据 3.4 节中的签密过程可以看出，签密的步骤②即签名过程将不再进行，而步骤⑤所得的 $\boldsymbol{W}_i$ 即为 $\boldsymbol{m}\oplus h_3(\boldsymbol{r})$，说明合法的系统用户作为接收方可以直接得到明文。这种情况下，合法的系统用户均无自己的密钥，也即普通系统设备与用户之间进行的一般的通信过程。这种过程与 3.1 节所设计的多接收方通信模型的第一种情况相适应。

2) 发送方有密钥，而接收用户组中存在没有密钥的成员。此时，根据 3.4 节中的签密过程可以看出，签密的步骤②即签名过程将进行，但是由于接收用户组中存在无密钥成员，因此 $\kappa=f(\boldsymbol{G}_1)f(\boldsymbol{G}_2)\cdots f(\boldsymbol{G}_{\varsigma-1})f(\boldsymbol{G}_\varsigma)=\boldsymbol{0}$，步骤⑤所得的 $\boldsymbol{W}_i$ 即为 $\boldsymbol{m}\oplus h_3(\boldsymbol{r})$。说明签名功能得到实现但未进行加密，合法的系统接收用户均可以对发送方的签名进行验证，并得到

明文。这种安排是根据文献[30]中提到的安全性，防止发送方向用户组发送信息时，存在有的用户得到加密后的信息，而有的用户得到未加密信息，造成明密文对比，使攻击者可以进行分析而造成漏洞。这种情况与 3.1 节所设计的通信模型的第二种情况相适应，即高级的系统用户或者设备向存在普通用户或设备的接收用户、设备组传输信息，接收组可以对信息来源以及信息是否被篡改进行确认。

3) 发送方没有密钥，而接收用户组中的成员均有密钥。根据 3.4 节中对签密过程的描述可以看出，签密的步骤②即签名的过程将跳过，但是由于接收用户组成员均有密钥，因此 $\boldsymbol{W}_i=\boldsymbol{m}\oplus h_3(\boldsymbol{r})\oplus h_2(\boldsymbol{r}_i\oplus\boldsymbol{q}_i)$，只有接收用户组中的第 i 个成员使用自己的密钥，才可以对 $\boldsymbol{W}_i=\boldsymbol{m}\oplus h_3(\boldsymbol{r})\oplus h_2(\boldsymbol{r}_i\oplus\boldsymbol{q}_i)$ 进行正确解密，再利用系统密钥处理得到明文。这种情况与 3.1 节中通信模型的第三种情况相适应，普通系统用户或者设备向高级的接收用户、设备组发送信息，只有该接收用户、设备组能够对信息进行正确解密，得到对应的明文。

4) 发送方以及接收用户组均有密钥。3.4 节中的全部过程将进行，即签密功能的实现。这种情况与 3.1 节通信模型的第四种情况相适应，高级的系统用户或设备与另一组高级的用户、设备进行高安全级别的通信。

综上所述，3.4 节所设计的多接收方广义签密方案可以与 3.1 节所设计的多接收方通信模型相适应。

4 安全性分析

本文多接收方的签密以及广义签密方案是一脉相承的，因此第 4 节的安全性分析主要是从广义签密方案出发，对具有签密功能的广义签密方案入手，分析方案的机密性以及不可伪造性，证明过程在文献[26-27,31]的基础上进行。

4.1 机密性

1) 游戏类型 1

定理 1 在随机预言机模型下，假设存在一个 IND-CCA2 的攻击者 α_1，能够以优势 $\mathrm{Adv}_{\alpha_1}^{\text{IND-CCA2}}$ 赢得如下定义的游戏（定义 1 中的游戏），那么就存在一个算法 β，它解决 SD 问题的优势 ε 如式(2)所示，其中算法 β 作为攻击者 α_1 在游戏中的挑战者，而 α_1 则作为 β 的子程序。

$$\varepsilon\geqslant\frac{\mathrm{Adv}_{\alpha_1}^{\text{IND-CCA2}}}{\varsigma(q_{\text{SC}}+q_{h_1})}\left(1-\varsigma\frac{q_{SC}+q_{h_2}+q_{h_3}}{2^k}\left(1-\frac{q_{\text{DSC}}}{2^k}\right)\right)\tag{2}$$

证明 给定一个 SD 问题实例 $\boldsymbol{x}=F(\boldsymbol{r})$，挑战者成功求解出 $\boldsymbol{r}$ 即可。

q_{SC}、q_{DSC}、q_{h_1}、q_{h_2}、q_{h_3} 分别代表攻击者 α_1 所能进行的签密询问、解签密询问，以及对随机预言机 h_1、h_2 以及 h_3 的询问的最大次数，q_{S} 、q_{P}、q_{R} 分别代表私钥询问、公钥询问以及公钥替换询问的最大次数。为了方便回答询问，并设立 2 个询问列表 List_1、List_2，来对以上询问进行记录。

① 游戏初始化。β 根据 QC-LDPC 码 Ω 随机选择 GF(2)上的 $k\times k$ 阶可逆矩阵 $\boldsymbol{S}$ 和 $(n-k)\times(n-k)$ 可逆矩阵 $\boldsymbol{M}$，选取 $n\times n$ 阶置换矩阵 $\boldsymbol{P}$。KGC 的系统公钥为 $\boldsymbol{G}^{\text{pub}}=\boldsymbol{SGP}$ 和 $\boldsymbol{H}^{\text{pub}}=\boldsymbol{MGP}$，系统私钥为 $(\boldsymbol{S},\boldsymbol{G},\boldsymbol{P},\boldsymbol{M},\beta_t())$，根据 QC-LDPC 码 Ω 随机选择 GF(2)上的 $k\times k$ 阶可逆矩阵 $\boldsymbol{S}_0$ 和 $(n-k)\times(n-k)$ 阶可逆矩阵 $\boldsymbol{M}_0$，选取 $n\times n$ 阶置换矩阵 $\boldsymbol{P}_0$。计算 $\boldsymbol{G}_0=\boldsymbol{S}_0\boldsymbol{G}^{\text{pub}}\boldsymbol{P}_0$，$\boldsymbol{H}_0=\boldsymbol{M}_0\boldsymbol{H}^{\text{pub}}\boldsymbol{P}_0$，则部分公钥为 $(\boldsymbol{G}_0,\boldsymbol{H}_0)$，部分私钥为 $(\boldsymbol{S}_0\boldsymbol{S},\boldsymbol{G},\boldsymbol{PP}_0,\boldsymbol{M}_0\boldsymbol{M},\beta_t())$。$\beta$ 将公共参数 (n,k,t,h_1,h_2,h_3) 发送给攻击者 α_1，并保留自己的系统密钥。攻击者 α_1 给出目标用户组 $L^*=\{\text{ID}_1^*,\text{ID}_2^*,\cdots,\text{ID}_\varsigma^*\}$。

② 询问阶段。攻击者 α_1 可以向挑战者 β 进行如下询问。

h_1 询问。输入元组 $(\boldsymbol{m},\text{ID}_i^*,\boldsymbol{x},L^*)$，查看表 List_1，如果存在相应记录 $\boldsymbol{Y}_i$ 则返回该记录；若不存在则随机选取一个 $\boldsymbol{Y}_i$，将其以及用户 ID_i^* 对信息 $\boldsymbol{m}$ 签密产生的密文与签名存入表 List_1，并返回 $\boldsymbol{Y}_i$。

h_2 询问。有以下几种情况。输入 ID_i^* 进行询问时，对表 List_2 进行查询是否有相应记录 $\boldsymbol{q}_i$，存在则返回，不存在则随机选择一个 $\boldsymbol{q}_i$ 存入 List_2，并将用户 ID_i^* 的公钥、私钥以及一个记录用户公钥是否被替换的标识 ϖ（$\varpi=0$表示未被替换，ϖ=1表示被替换）一同记录下来，返回 $\boldsymbol{q}_i$。输入 $(\boldsymbol{r}_i,\boldsymbol{q}_i)$ 进行询问，同样先对表 List_2 进行查询是否有相应记录 $h_2(\boldsymbol{r}_i\oplus\boldsymbol{q}_i)$，存在则返回，该记录存在的概率很小，为 $\frac{1}{2^k}$，不存在则随机选择一个 $h_2(\boldsymbol{r}_i\oplus\boldsymbol{q}_i)$ 记录在 List_2，并将用户 ID_i^* 的公钥、私钥以及一个记录用户公钥是否被替换的标识 ϖ 一同记录下来，返回

$h_2(\overline{\boldsymbol{r}_i \oplus \boldsymbol{q}_i})$。

h_3 询问。输入随机数 $\boldsymbol{r}$ 询问时，返回值 $h_3(\overline{\boldsymbol{r}})$ 如果存在相应记录，则返回 $h_3(\overline{\boldsymbol{r}})$，但这种概率存在的可能极小，为 $\frac{1}{2^k}$。因为是对随机数查询，所以查询过的概率很小。

私钥询问。攻击者输入用户 ID_i，若该用户存在于目标用户组中，则挑战者 β 丢弃该询问；否则，β 查找 List_2。首先查看该用户的替换标识 ϖ 检查其公钥是否被替换，若未被替换，则返回该用户私钥 $(\boldsymbol{S}_i\boldsymbol{S}_0\boldsymbol{S}, \boldsymbol{G}, \boldsymbol{PP}_0\boldsymbol{P}_i, \boldsymbol{M}_i\boldsymbol{M}_0\boldsymbol{M}, \beta_t())$；若被替换，则 β 向 α_1 询问用户 ID_i 的私钥参数。最终返回攻击者 $(\boldsymbol{S}_i\boldsymbol{S}_0\boldsymbol{S}, \boldsymbol{G}, \boldsymbol{PP}_0\boldsymbol{P}_i, \boldsymbol{M}_i\boldsymbol{M}_0\boldsymbol{M}, \beta_t())$。

公钥询问。攻击者输入用户 ID_i，首先查询 List_2 中是否有相应记录，存在则返回 F_i；否则选择随机矩阵 $(\boldsymbol{S}_i, \boldsymbol{P}_i, \boldsymbol{M}_i)$，并进行相应计算产生对应公钥 F_i。把该值更新记录到表 List_2 中并返回。

公钥替换询问。输入二元组 $(\mathrm{ID}_i, \overline{F_i})$ 进行询问，首先查询 List_2，若存在记录 (ID_i, F_i)，则使用 $\overline{F_i}$ 替换 F_i，并更新标识 ϖ；若没有对应公钥，则对 ID_i 进行公钥询问，得到新公钥后，再进行替换询问。

签密询问。输入元组 $(\boldsymbol{m}, \mathrm{ID}_s, L=\{\mathrm{ID}_{R_1}, \mathrm{ID}_{R_2}, \cdots, \mathrm{ID}_{R_\varsigma}\})$，若 ID_s 存在于身份集合 L 中，或 L 中有元素存在于目标身份集合 L^* 中，β 丢弃此次询问；若 ID_s 不在目标身份集合 L^* 中，则可以知道发送方的私钥，并在 List_1、List_2 中记录。进行本文的签密算法，得到相应的签密文 $\sigma=(\boldsymbol{s}, \boldsymbol{W}_1, \boldsymbol{W}_2, \cdots, \boldsymbol{W}_\varsigma, \boldsymbol{c}_1, \boldsymbol{c}_2, \cdots, \boldsymbol{c}_\varsigma, \overline{L}, x)$。如果在目标身份集合中，则挑战者无法获知发送方的私钥，可通过以下方法来进行签密：β 询问 List_2，得到 ID_s 的公私钥，选择随机数 $\boldsymbol{r}$ 用公钥加密得到 $F_S(\boldsymbol{r}) \to \boldsymbol{x}$，再进行 h_1 询问以及签名算法得到签名 $\boldsymbol{s}$。β 随机选择 $\boldsymbol{q}_i$，对 List_2 进行查询得到记录 $(\mathrm{ID}_{R_i}, \varpi_{R_i})$，首先查看替换标识，检查公钥是否被替换，未被替换则进行 h_2 询问以及加密算法，得到密文 $\boldsymbol{W}_i$ 与用户组标识 $\overline{L}$；否则进行公钥替换询问与公钥询问，并将该记录存入表 List_2，若表 List_2 中已经存在了相应记录则说明模拟签密失败。由 β 返回给攻击者 α_1 签密文 $(\boldsymbol{s}, \boldsymbol{W}_1, \boldsymbol{W}_2, \cdots, \boldsymbol{W}_\varsigma, \boldsymbol{c}_1, \boldsymbol{c}_2, \cdots, \boldsymbol{c}_\varsigma, \overline{L}, x)$。模拟签密失败的概率为 $\frac{q_{\mathrm{SC}} + q_{h_2} + q_{h_3}}{2^k}$。

解签密询问。输入签密文 σ，发送方以及接收者身份 ID_S、ID_R。首先提取出对应接收者的签密文 $(\boldsymbol{s}, \boldsymbol{W}_i, \overline{L}, \boldsymbol{c}_i, x)$，若该接收者属于目标用户组，则 β 知道该接收者的私钥，便可进行解密算法求出明文；否则需要查看 List_1 中是否有该签名 $\boldsymbol{s}$ 以及密文 $\boldsymbol{W}_i$ 的记录，若没有相应记录则 β 拒绝该签密文。再看表 List_2，若没有关于接收者 ID_R 的用户标识、公私钥、替换标识的记录，β 也拒绝该签密文。当对密文解密时，运用系统私钥以及接收者私钥进行解密得到明文 $\boldsymbol{m}$，利用签名验证算法与该信息 $\boldsymbol{m}$ 对签名 $\boldsymbol{s}$ 进行验证，当且仅当签名验证成功时，可获得正确明文 $\boldsymbol{m}$，否则解签密失败。一个有效的密文被拒绝的概率为 $\frac{q_{\mathrm{DSC}}}{2^k}$。

③ 挑战阶段。攻击者 α_1 提供 2 个 k 维的消息 $\boldsymbol{m}_1$、$\boldsymbol{m}_2$ 以及发送方 ID_S，且发送方不在目标用户身份集合 L^* 中，向 β 进行询问。β 选择一个消息 $\boldsymbol{m}_b$，其中 $b \in \{0,1\}$，并发送给目标用户组 $L^* = \{\mathrm{ID}_1^*, \mathrm{ID}_2^*, \cdots, \mathrm{ID}_\varsigma^*\}$。$\beta$ 进行如下操作 $F_2^{n-k} \xrightarrow{\$} \boldsymbol{Y}$，进而利用 CFS 算法产生签名 $\boldsymbol{s}^*$。产生签名后，由 β 产生相应的密文 $(\boldsymbol{W}_1^*, \boldsymbol{W}_2^*, \cdots, \boldsymbol{W}_\varsigma^*, \boldsymbol{c}_1^*, \boldsymbol{c}_2^*, \cdots, \boldsymbol{c}_\varsigma^*)$，具体方法如下：由 β 进行操作 $F_2^k \xrightarrow{\$} h_3(\overline{\boldsymbol{r}}), F_2^k \xrightarrow{\$} h_2(\overline{\boldsymbol{r}_i \oplus \boldsymbol{q}_i})$，得到密文 $\boldsymbol{W}_i^* = \boldsymbol{m}_b \oplus h_3(\overline{\boldsymbol{r}}) \oplus h_2(\overline{\boldsymbol{r}_i \oplus \boldsymbol{q}_i})$，$\overline{L}^* = F_0(L^*)$，最终的签密文为 $\sigma^* = (\boldsymbol{s}^*, \boldsymbol{W}_1^*, \boldsymbol{W}_2^*, \cdots, \boldsymbol{W}_\varsigma^*, \boldsymbol{c}_1^*, \boldsymbol{c}_2^*, \cdots, \boldsymbol{c}_\varsigma^*, \overline{L}^*, x^*)$。

④ 询问阶段。攻击者 α_1 仍可进行如阶段②的询问，但是不能为接收者 $L^* = \{\mathrm{ID}_1^*, \mathrm{ID}_2^*, \cdots, \mathrm{ID}_\varsigma^*\}$ 向挑战密文 σ^* 进行询问。

⑤ 猜测阶段。α_1 输出 1 bit $\overline{b}$ 作为猜测。如上所述，若 α_1 猜测成功，那么必须通过 h_1 询问得到密文，β 在 List_1 中随机选择一个记录且包含正确签名、密文的概率为 $\frac{1}{\varsigma(q_{\mathrm{SC}} + q_{h_1})}$。最后将 β 输出的 $\boldsymbol{r}, \boldsymbol{r}_i$ 作为 SD 问题的解。

根据以上分析，β 成功即攻击者 α_1 输出正确比特的概率需要考虑以下几个因素。首先设攻击者 α_1 成功这件事为 E，其概率为 $\Pr[\mathrm{E}] = \mathrm{Adv}_{\alpha_1}^{\mathrm{IND\text{-}CCA2}}$。设 E_1 表示挑战者对目标用户组中的私钥进行询问，E_2

表示发送方以及存在一个接收者属于目标用户组，若这 2 个事件发生，β 自动放弃此次询问；E_3 表示挑战者 β 在进行 h_2 询问时，$List_2$ 中的相应记录出现了碰撞情况，则签密模拟失败，其概率为 $\Pr[E_3]\leqslant\varsigma\frac{q_{SC}+q_{h_2}+q_{h_3}}{2^k}$。$E_4$ 表示一个有效签名被拒绝，其概率为 $\Pr[E_4]\leqslant\frac{q_{DSC}}{2^k}$。$E_5$ 表示 β 在表 $List_1$ 中随机选择一个记录且包含了正确元素，其概率为 $\Pr[E_5]\leqslant\frac{1}{\varsigma(q_{SC}+q_{h_1})}$。所以概率为 $\Pr[E\cap E_1\cap E_2\cap E_3\cap E_4\cap E_5]$。$\beta$ 成功解决 SD 问题的优势 ε 为

$$\varepsilon\geqslant\frac{\mathrm{Adv}_{\alpha_1}^{\text{IND-CCA2}}}{\varsigma(q_{SC}+q_{h_1})}\frac{1-\varsigma(q_{SC}+q_{h_2}+q_{h_3})}{2^k}\frac{1-q_{DSC}}{2^k}$$

定理 1 证毕。

2) 游戏类型 2

定理 2 在随机预言机模型下，假定存在一个 IND-CCA2 的攻击者 α_2，它能够以优势 $\mathrm{Adv}_{\alpha_2}^{\text{IND-CCA2}}$ 赢得定义 2 中的游戏，那么就存在一个算法 β，它解决 SD 问题的优势 ε 如式(3)所示，其中算法 β 作为攻击者 α_2 在游戏中的挑战者，而 α_2 则作为 β 的子程序。

$$\varepsilon\geqslant\frac{\mathrm{Adv}_{\alpha_2}^{\text{IND-CCA2}}}{\varsigma(q_{SC}+q_{h_1})}\frac{1-\varsigma(q_{SC}+q_{h_2}+q_{h_3})}{2^k}\frac{1-q_{DSC}}{2^k}\tag{3}$$

证明 在游戏类型 2 中，不同于游戏类型 1，攻击者 α_2 可以获得系统主密钥信息，但是不能对用户的公钥进行替换，对于定理 2 的证明与定理 1 的证明类似，易得定理 2 成立。证毕。

4.2 不可伪造性

1) 游戏类型 1

定理 3 在随机预言机模型下，假设存在一个 EUF-CMA 的攻击者 α_1，它能够以优势 $\mathrm{Adv}_{\alpha_1}^{\text{EUF-CMA}}$ 赢得如下定义的游戏（定义 3 中的游戏），那么就存在一个算法 β，它解决 SD 问题的优势 υ 如式(4)所示，其中算法 β 作为攻击者 α_1 在游戏中的挑战者，而 α_1 则作为 β 的子程序。

$$\upsilon\geqslant\frac{\mathrm{Adv}_{\alpha_1}^{\text{EUF-CMA}}}{\varsigma(q_{SC}+q_{h_2})}\frac{1-\varsigma(q_{SC}+q_{h_2}+q_{h_3})}{2^k}\frac{1-q_{DSC}}{2^k}\tag{4}$$

证明 给定一个编码密码中的问题实例 $(\boldsymbol{H}_S=\boldsymbol{M}_S\boldsymbol{H}_0\boldsymbol{P}_S,\boldsymbol{H}_0)$，$\beta$ 需要求出 $\boldsymbol{M}_S,\boldsymbol{P}_S$。

① 游戏初始化。同 4.1 节中游戏类型 1 中的①。

② 询问阶段。与 4.1 节中游戏类型 1 中的②相似，不同之处在于最后的解签密询问换为了验证询问，具体询问过程如下。输入签密文 σ、发送方身份 ID_S、接收者身份 ID_R。首先提取出对应接收者的签密文 $(\boldsymbol{s},\boldsymbol{W}_i,\overline{L},\boldsymbol{c}_i,x)$，若该接收者属于目标用户组，则 β 知道该接收者的私钥，可以进行解密算法求出明文，否则需要查看 $List_1$ 中是否有该签名 $\boldsymbol{s}$ 以及用户组 $\overline{L}$ 的记录，若没有相应记录则 β 拒绝该签密文。若 $List_2$ 中没有关于接收者 ID_R 的用户标识、公私钥、替换标识的记录，β 也拒绝该签密文。当对密文解密时，运用系统私钥以及接收者私钥进行解密得到明文 $\boldsymbol{m}$，利用签名验证算法与该信息 $\boldsymbol{m}$ 对签名 $\boldsymbol{s}$ 进行验证。一个有效的密文被拒绝的概率为 $\frac{q_{DSC}}{2^k}$。

③ 伪造阶段。攻击者 α_1 输出伪造的签密文 $\sigma^*=(\boldsymbol{s}^*,\boldsymbol{W}_1^*,\boldsymbol{W}_2^*,\cdots,\boldsymbol{W}_\varsigma^*,\boldsymbol{c}_1^*,\boldsymbol{c}_2^*,\cdots,\boldsymbol{c}_\varsigma^*,\overline{L}^*,x^*)$，其中发送方 ID_S 是属于目标身份用户组 L^* 的，接收者 ID_{R_i} 中至少有一个是属于 L^* 的。

通过上述的分析可知，若攻击者 α_1 伪造签密文成功，需要通过 h_2 询问得到发送方 ID_S 的私钥 $\boldsymbol{M}_S,\boldsymbol{P}_S$，$\beta$ 需要在 $List_2$ 中随机选择一个记录且包含了正确元素 $\boldsymbol{M}_S,\boldsymbol{P}_S$，概率为 $\frac{1}{\varsigma(q_{SC}+q_{h_2})}$。将正确记录中的 $\boldsymbol{M}_S,\boldsymbol{P}_S$ 作为 β 对问题实例 $(\boldsymbol{H}_S=\boldsymbol{M}_S\boldsymbol{H}_0\boldsymbol{P}_S,\boldsymbol{H}_0)$ 的求解。设攻击者 α_1 伪造的签名 σ^* 通过验证这件事为 E，其概率为 $\Pr[E]=\mathrm{Adv}_{\alpha_1}^{\text{EUF-CMA}}$。设 E_1 表示挑战者对目标用户组中的私钥进行询问，设 E_2 表示发送方以及存在一个接收者属于目标用户组中，若这 2 个事件发生 β 会自动放弃此次询问。设 E_3 表示挑战者 β 在进行 h_2 询问时，$List_2$ 中的相应记录出现了碰撞情况，则签密模拟失败，其概率为 $\Pr[E_3]\leqslant\frac{\varsigma(q_{SC}+q_{h_2}+q_{h_3})}{2^k}$。设 E_4 表示一个有效签名被拒绝，其概率为 $\Pr[E_4]\leqslant\frac{q_{DSC}}{2^k}$。设 E_5 表示 β 在表 $List_1$ 中随机选择一个记录且包含了正确元素，其概率为 $\Pr[E_5]\leqslant\frac{1}{\varsigma(q_{SC}+q_{h_2})}$。所以概率为 $\Pr[E\cap E_1\cap E_2\cap E_3\cap E_4\cap E_5]$。$\beta$ 解决 SD 问题的优势 υ 为

$$\upsilon \geqslant \frac{\mathrm{Adv}_{\alpha_1}^{\text{EUF-CMA}}}{\varsigma(q_{\mathrm{SC}}+q_{h_2})}\frac{1-\varsigma(q_{\mathrm{SC}}+q_{h_2}+q_{h_3})}{2^k}\frac{1-q_{\mathrm{DSC}}}{2^k}$$

证毕。

2) 游戏类型 2

定理 4　在随机预言机模型下，假设存在一个 EUF-CMA 的攻击者 α_2，它能够以优势 $\mathrm{Adv}_{\alpha_2}^{\text{EUF-CMA}}$ 赢得如下定义的游戏（定义 4 中的游戏），那么就存在一个算法 β，它解决 SD 问题的优势 υ 如式(5)所示，其中算法 β 作为攻击者 α_2 在游戏中的挑战者，而 α_2 则作为 β 的子程序。

$$\upsilon \geqslant \frac{\mathrm{Adv}_{\alpha_2}^{\text{EUF-CMA}}}{\varsigma(q_{\mathrm{SC}}+q_{h_2})}\frac{1-\varsigma(q_{\mathrm{SC}}+q_{h_2}+q_{h_3})}{2^k}\frac{1-q_{\mathrm{DSC}}}{2^k} \tag{5}$$

证明　在游戏类型 2 中，不同于游戏类型 1，攻击者 α_2 可以获得系统主密钥信息，但是不能对用户的公钥进行替换，对于定理 4 的证明与定理 3 的证明类似，易得定理 4 成立。证毕。

5　效率分析

5.1　加密方案效率

本文的多接收方签密方案以及广义签密方案是在 3.1 节中提出的多次加密 McEliece 方案基础上进行构造的。由 3.1 的加密方案可以看出，该方案采用的是 QC-LDPC 码，该码相比于 Goppa 码等其他码字存储起来消耗更少的空间，且具有更高的传信率。另一方面，虽然该方案进行了多次加密，但是采用同一个码字产生的同一个公钥，解密也采用该码字产生的同一个私钥，因此多次加密的 McEliece 方案能够保持与采用 QC-LDPC 码的普通 McEliece 方案同样的密钥存储量，且能够满足更高的安全需求。具体比较如表 1 所示。

由表 1 可以看出，采用 Goppa 码的 McEliece 方案所选用的 Goppa 码维度相比(QC-LDPC)-M 以及多次加密的 McEliece 方案小许多，尽管如此，采用 Goppa 码的 McEliece 方案的公钥量为 67 072 B，相比另外两者 6 048 B 的公钥量还是大了许多，而且能够加密的明文量仅为 524 bit，相比另外两者的 12 096 bit 少了许多。通过公钥量一栏还可以看出，多次加密的 McEliece 方案虽然采用多次加密的方法降低对译码错误的影响，从而具有了更高的安全性，但是与普通的采用 QC-LPDC 码的 McEliece 方案的密钥量相同，正如之前所述，这是由于多次加解密所采用的密钥是相同的，因此多次加密的 McEliece 方案具有较好的性能。其中 b 代表多次加密的次数，即产生的密文数量。

5.2　多接收方的签密与广义签密方案效率

3.3 节与 3.4 节的签密和广义签密方案在参数生成以及系统密钥和用户密钥的生成上是相同的，因此从多接收方的广义签密分析方案的密钥量相等即可。取(16 128, 12 096)维的 QC-LDPC 码进行如表 2 所示的比较。

由表 2 对比分析可以看出，本文的多接收方广义签密方案不仅可以实现签密功能以及在签名、加密、签密方案三者之间的自适应转换，而且相比先签名后加密方案在私钥量上减少了 31 752 KB，这些减少量的存在是由于 CFS 签名方案与多次加密-M 方案在置换矩阵 $\boldsymbol{P}$ 上的共用。先签名后加密方案与本文广义签密方案的密文量都是 16 128(b+2) bit，相比直接将二者相加的密文量多了 16 128 bit，这是

表 1　方案性能对比

方案	(n, k)维码字	公钥量/B	明文量/bit	密文量/bit	信息率
Goppa-M 方案	(1 024, 524)	67 072	524	1 024	0.51
(QC-LDPC)-M 方案	(16 128, 12 096)	6 048	12 096	16 128	0.75
多次加密-M 方案	(16 128, 12 096)	6 048	12 096	b16 128	0.75

表 2　密钥量对比

方案	公钥/B	私钥/KB	明文量/bit	密文量/bit
CFS 签名方案	6 048	33 742.4	12 096	16 128
多次加密-M 方案	6 048	49 618.4	12 096	16 128 b
签名加密方案	12 096	83 360.8	12 096	16 128(b+2)
本文广义签密方案	12 096	51 608.8	12 096	16 128(b+2)

因为还存在使用系统公钥加密产生的密文 $\boldsymbol{x}$，但这保证了系统用户以外的用户无法获知系统内部的信息。通过表 2 可以看出，本文多接收方广义签密方案具有较好的使用前景。

将本文多接收方的广义签密方案与其他多接收方签密方案进行效率比较，如表 3 所示。其中，ς 代表多接收方用户数量。由表 3 可以看出，本文的广义签密方案相比 Li 等[32]方案、朱辉等[33]方案、Selvi 等[25]方案，没有复杂的指数运算以及双线性对运算，而本文方案多了矩阵运算。指数运算以及双线性对运算相比矩阵运算的效率较低，且消耗更多的资源，因此本文方案没有复杂的指数运算以及双线性对运算，这是提高效率的一大优势，由于是基于编码密码进行广义签密方案的构造，因此能够抵抗量子计算机攻击，这也是相比基于传统公钥密码构造签密方案的优势之一。

表 3　　签密方案效率对比

方案	指数运算	双线性对运算	Hash 函数运算
Li 等[32]方案	ς+1	2	2ς+2
朱辉等[33]方案	3ς+4	0	3ς+3
Selvi 等[25]方案	2ς+2	2	ς+7
本文广义签密方案	0	0	ς+11

6 结束语

本文提出了能够满足 IND-CCA2 安全的多次加密 McEliece 方案，该加密方案采用 QC-LDPC 码进行构造且多次加密与解密所采用的都是同一对公私钥，因此能够在保证密钥储存量合适的前提下达到更高的安全级别。依托多次加密的 McEliece 方案与 CFS 签名方案，提出基于编码的多接收方的签密方案，进而在该签密方案的基础上进行改进提出了基于编码的多接收方的广义签密方案。新的广义签密方案在机密性方面满足 IND-CCA 2 安全，在不可伪造性方面满足 EUF-CMA 安全。本文广义签密方案在密钥量以及密文量方面具有一定优势，而且相比基于传统公钥密码的多接收方签密方案没有复杂的双线性对运算以及指数运算。最后将该多接收方的广义签密与多接收方通信模型相结合能够实现对不同安全级别用户的访问控制，能够满足系统的多种安全需求。

参考文献：

[1] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer [J]. SIAM Journal on Computing, 1997, 26(5): 1484-1509.

[2] BERNSTEIN D J, BUCHMANN J, DAHMEN E. Post quantum cryptography[C]// Springer, 2009: 73-80.

[3] 郭秋玲, 向宏, 蔡斌, 等. 基于多变量公钥密码体制的门限环签名方案[J]. 密码学报, 2018, 5(2): 140-150.
GUO Q L, XIANG H, CAI B, et al. Threshold ring signature scheme based on multivariate public key cryptosystems[J]. Journal of Cryptologic Research, 2018, 5(2): 140-150.

[4] 汤海婷,汪学明.一种基于格的属性多重加密方案[J].计算机工程,2018,44(2):193-196.
TANG H T, WANG X M. An attribute multiple encryption scheme based on lattices[J]. Computer Engineering, 2018, 44(2): 193-196.

[5] 徐权佐,蔡庆军.一种基于编码的公钥密码体制的参数选择研究[J].信息网络安全,2014(10):54-58.
XU Q Z, CAI Q J. Research on parameter selection of a code-based public-key cryptosystem[J]. Netinfo Security, 2014(10): 54-58.

[6] 张焕国,管海明,王后珍.量子计算的挑战与思考[J].云南民族大学学报(自然科学版),2011,20(5):388-395.
ZHANG H G, GUAN H M, WANG H Z. The challenge of quantum computing to information security and our countermeasures[J]. Journal of Yunnan University of Nationalities(Natural Sciences Edition), 2011, 20(5): 388-395.

[7] YAN S Y. Quantum attacks on public-key cryptosystems[M]. Berlin: Springer, 2013.

[8] MCELIECE R J. A public-key cryptosystem based on algebraic coding theory[J]. The Deep Space Network Progress Report, 1978, 4244: 114-116.

[9] NIEDERREITER H. Knapsack-type cryptosystems and algebraic coding theory[J]. Problems Control Inform Theory, 1986, 15(2): 159-166.

[10] COURTOIS N T, FINIASZ M, SENDRIER N. How to achieve a McEliece-based digital signature scheme[C]//Advances in Cryptology-ASIACRYPT 2001. 2001: 157-174.

[11] MATHEW K P, VASANT S, RANGAN C P. A provably secure signature and signcryption scheme using the hardness assumptions in coding theory[C]//Information Security and Cryptology—ICISC 2013. Springer International Publishing, 2013: 342-362.

[12] GABORIT P. Shorter keys for code based cryptography[C]// The International Workshop on Coding and Cryptography (WCC 2005). Bergen, Norway, 2005: 81-90.

[13] MONICO C, ROSENTHAL J, SHOKROLLAHI A. Using low density parity check codes in the McEliece cryptosystem[C]// IEEE International Symposium on Information Theory. IEEE, 2000:215.

[14] OTMANI A, TILLICH J P, DALLOT L. Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes[J]. Mathematics in Computer Science, 2010, 3(2):129-140.

[15] LONDAHL C, JOHANSSON T. A new version of McEliece PKC based on convolutional codes[C]//International Conference on Information and Communications Security. Springer, 2012: 461-470.

[16] BALDI M. QC-LDPC code-based cryptography[M]. Berlin: Springer, 2014.

[17] 李梦东, 孙玉情, 韦依儿, 等. 改进的基于奇偶校验码的 McEliece 变型方案[J]. 计算机应用研究, 2019(11): 1-7.
LI M D, SUN Y Q, WEI Y E, et al. Improved McEliece variant scheme based on parity-check codes[J]. Application Research of Computers, 2019(11): 1-7.

[18] DENEUVILLE J C, GABORIT P, ZÉMOR G. Ouroboros: a simple, secure and efficient key exchange protocol based on coding theory[C]//International Workshop on Post-quantum Cryptography. Springer, 2017:18-34.

[19] BALDI M, BARENGHI A, CHIARALUCE F, et al. LEDAkem: a post-quantum key encapsulation mechanism based on QC-LDPC codes[C]//International Conference on Post-Quantum Cryptography. Springer, 2018: 3-24.

[20] EATON E, LEQUESNE M, PARENT A, et al. QC-MDPC: a timing attack and a CCA2 KEM[C]//International Conference on Post-Quantum Cryptography. Springer, 2018: 47-76.

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

[22] 韩益亮, 杨晓元. ECDSA 可公开验证广义签密[J].计算机学报, 2006,29(11): 105-114.
HAN Y L, YANG X Y. New ECDSA-verifiable generalized signcryption[J]. Chinese Journal of Computers, 2006, 29(11): 105-114.

[23] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptograph[C]// International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2003:452-473.

[24] BARBOSA M, FARSHIM P. Certificateless signcryption [C]//The ACM Symposium on Information, Computer and Communications Security. ACM, 2008:369-372.

[25] SELVI S S D, VIVEK S S, SHUKLA D, et al. Efficient and provably secure certificateless multi-receiver signcryption[C]// International Conference on Provable Security. Springer, 2008:52-67.

[26] 李慧贤, 陈绪宝, 庞辽军, 等. 基于多变量公钥密码体制的无证书多接收者签密体制[J]. 计算机学报, 2012, 35(9):93-101.
LI H X, CHEN X B, PANG L J, et al. Certificateless multi-receiver signcryption scheme based on multivariate public key cryptography[J]. Chinese Journal of Computers, 2012, 35(9): 93-101.

[27] YUNG M. Practical signcryption[M]. Springer Science & Business Media, 2010.

[28] 屈娟,李艳平,李丽.普适计算中匿名跨域认证协议的分析与改进[J].信息网络安全,2018(1):73-79.
QU J, LI Y P, LI L. Cryptanalysis and security enhancement of an efficient secure authentication scheme with user anonymity for roaming user in ubiquitous networks[J].Netinfo Security, 2018(1): 73-79.

[29] 周彦伟,杨波,张文政.普适计算环境下的安全访问模型[J].电子学报,2017,45(4):959-965.
ZHOU Y W, YANG B, ZHANG W Z. Security access model in pervasive computing environment[J]. Acta Electronica Sinica, 2017, 45(4): 959-965.

[30] HAN Y, GUI X. Adaptive secure multicast in wireless networks [J]. International Journal of Communication Systems, 2009, 22(9): 1213-1239.

[31] 韩益亮,蓝锦佳,杨晓元.基于 LRPC 码和多变量的签密方案[J].密码学报,2016,3(1):56-66.
HAN Y L, LAN J J, YANG X Y. A signcryption scheme based on LRPC and multivariate cryptosystem[J]. Journal of Cryptologic Research, 2016, 3(1): 56-66.

[32] LI P C, HE M X, LI X, et al. Efficient and provably secure certificateles signcryption from bilinear pairings[J]. Journal of Computational Information Systems, 2010, 6(11):3643-3650.

[33] 朱辉, 李晖, 王育民. 不使用双线性对的无证书签密方案[J].计算机研究与发展, 2010, 47(9):1587-1594.
ZHU H, LI H, WANG Y M. Certificateless signcryption scheme without bilinear pairing[J]. Journal of Computer Research and Development, 2010, 47(9): 1587-1594.

[作者简介]

韩益亮（1977– ），男，甘肃会宁人，博士，武警工程大学教授、博士生导师，主要研究方向为公钥密码学、网络安全等。

王众（1995– ），男，山东泰安人，武警工程大学硕士生，主要研究方向为抗量子密码、签密等。