基于HQC的周期性可否认环签名方案设计与分析

张艳硕[1]，屠桢昊[2]，蒋奕帆[1]，杨亚涛[3]，刘冰[1]
（1.北京电子科技学院密码科学与技术系，北京100070；2.北京电子科技学院网络空间安全系，北京100070；3.北京电子科技学院电子与通信工程系，北京100070）

摘要：针对现有周期性可否认环签名方案依赖传统密码假设、难以满足后量子长期安全需求的问题，本文提出一种基于汉明准循环码（Hamming Quasi-Cyclic，HQC）的周期性可否认环签名方案。该方案以HQC公钥诱导的线性一致性关系为证明语句，结合Stern-like Σ协议、OR组合结构和Fiat–Shamir变换构造非交互式环签名，并通过上下文标签与时窗控制机制实现确认/否认接口的周期性开放。在随机预言机模型下，本文基于支持恢复问题与准循环综合译码判定问题，证明了方案的不可伪造性、匿名性、可追踪性和不可诽谤性。与现有典型可否认环签名方案以及编码型相关方案的对比分析表明，该方案虽增加一定通信与计算开销，但在编码型签名框架中同时实现了后量子安全性、可否认性与周期性控制，可为责任受限场景下的匿名认证提供一种编码型实现路径。

关键词：抗量子密码；HQC；周期性可否认环签名；Stern-like Σ协议；Fiat–Shamir变换

Design and Analysis of a Periodically Deniable Ring Signature Scheme Based on HQC

Zhang Yanshuo[1], Tu Zhenhao[2], Jiang Yifan[1], Yang Yatao[3], Liu Bing[1]
1. Department of Cryptology Science and Technology, Beijing Electronic Science and Technology Institute, Beijing;100070, China
2. Department of Cyberspace Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China
3. Department of Electronic and Communication Engineering, Beijing Electronic Science and Technology Institute, Beijing;100070, China

Abstract: To address the problem that existing periodically deniable ring signature schemes rely on conventional cryptographic assumptions and are therefore difficult to adapt to long-term post-quantum security requirements, this paper proposes a periodically deniable ring signature scheme based on the Hamming Quasi-Cyclic (HQC) code-based cryptosystem. The scheme takes the linear consistency relation induced by the HQC public key as the proof statement, and constructs a non-interactive ring signature by combining a Stern-like Σ-protocol, an OR-composition structure, and the Fiat–Shamir transformation. A context tag and a time-window control mechanism are further introduced to realize the periodic opening of the confirmation and disavowal interfaces. In the random oracle model, the unforgeability, anonymity, traceability, and non-slanderability of the scheme are proved based on the Support Recovery problem and the Quasi-Cyclic Decision Decoding problem. Comparative analysis with existing representative deniable ring signature schemes and related code-based schemes shows that, although the proposed scheme incurs additional communication and computation overhead, it simultaneously achieves post-quantum security, deniability, and periodic control within a code-based signature framework, thus providing a code-based implementation path for anonymous authentication in accountability-constrained scenarios.

Key words: Post-Quantum Cryptography, HQC, Periodically Deniable Ring Signatures, Stern-like Σ protocols, Fiat–Shamir transform

收稿日期：2026–XX–XX；**修回日期：**XXXX–XX–XX
通信作者：屠桢昊 Email:761429685@qq.com
基金项目：国家密码科学基金资助项目（No.2025NCSF02028）；国家重点研发计划项目（2024YFB3108103）；中央高校基本科研业务费（No. 3282025036）。

0 引言

随着量子计算技术的持续发展，传统基于大整数分解和离散对数问题的公钥密码体制在长期安全性方面面临潜在风险。自1994年Shor算法[1]提出以来，学术界逐渐认识到，一旦具备实用规模的量子计算机出现，现有大量经典密码方案将难以继续保障信息系统的安全性。近年来，基于格、编码以及多变量多项式等困难问题的密码体制相继被提出[2-4]，其中编码密码体制由于其安全性建立在综合译码等NP困难问题之上，在后量子密码研究背景下受到了广泛关注。

环签名作为一种重要的匿名签名技术，自2001年提出以来在隐私保护和匿名认证领域得到了持续研究[5]。进入2010年后，随着电子投票[6]、匿名通信[7]和区块链[8]等应用场景的发展，环签名的可扩展性与计算效率问题逐渐受到重视。在国际密码学会议CRYPTO 2021会议上，相关研究也在紧凑构造和性能优化方面不断推进[9-10]。然而，传统环签名在提供强匿名性的同时，通常缺乏有效的责任澄清机制，一旦发生争议，难以区分真实签名者与环内其他成员，导致不可追责或恶意诬陷的问题。

为缓解匿名性与责任澄清之间的矛盾，2004年Naor等学者提出了可否认认证的思想[11]，为在隐私保护条件下实现身份澄清提供了新的研究视角。随后，2006年Komano等将可否认性引入环签名场景，提出了可否认环签名的概念[12]。该概念使得非签名者在遭受不实指控时能够否认其签名身份，而真实签名者在特定条件下也可以确认自身行为。近年来，基于SM2和SM9等密码体制的可否认环签名方案相继被提出[13][14]，推动了该方向在功能设计与性能优化方面的发展。

然而，传统可否认环签名技术难以直接适应“仅在特定时间范围内允许身份澄清”的应用需求。随着实际应用场景对时效性要求的进一步增强，研究者开始关注时间因素在可否认环签名中的作用。自2024年以来，张等提出的周期性可否认环签名方案[15-17]，将周期性机制引入可否认环签名。这类方案有助于在隐私保护与责任控制之间实现动态平衡，在电子投票、金融交易以及具有法律时效要求的安全通信场景中具有实际应用价值。然而，现有周期性可否认环签名方案大多建立在传统公钥密码假设之上，其在量子计算模型下的安全性仍有待进一步研究。

在后量子密码研究领域，编码型密码体制自1970年代提出以来[18]，已在加密和密钥封装等方向形成较为成熟的研究基础，并在近年来的后量子密码标准化进程中受到广泛关注。如HQC已于2025年被NIST选定进入后量子公钥加密标准化序列，用作补充型标准算法之一，这进一步提升了基于HQC构造后量子密码原语的现实意义[19]。相比之下，编码型密码在匿名签名和可否认签名等隐私保护方向上的研究仍相对有限。近两年，围绕后量子匿名签名与编码型高级匿名原语的研究仍在持续推进：一方面，后量子环签名方向出现了面向小环规模优化的NTRU-based构造与新型可链接环签名框架[20]；另一方面，编码型零知识证明及其对高级隐私保护原语的支撑能力也在进一步增强，例如基于VOLE-in-the-Head的代码基零知识新构造已被用于多类code-based privacy-preserving systems[21]。上述进展表明，如何在后量子背景下进一步实现兼具匿名性、可否认性与应用可控性的环签名方案，仍具有持续研究价值。

基于上述研究背景，本文在现有周期性可否认环签名方案的设计思想基础上，提出一种基于Hamming Quasi-Cyclic（HQC）编码体制[19][22]的周期性可否认环签名方案。该方案利用HQC公钥所诱导的线性一致性关系作为零知识证明的基本原语，并结合Stern-like Σ协议[23-24]、OR组合结构（OR-proof）[25]与Fiat－Shamir转换[26]，构造周期性可否认环签名方案。

本方案在不削弱环签名匿名性的前提下，引入周期性控制机制，使签名身份的确认与否认仅在指定时间窗口内有效，并在窗口结束后恢复长期匿名性。该机制适用于电子投票、金融交易及具有时效要求的安全通信等场景，可在争议期内支持核查、审计与责任澄清，并在争议期结束后降低敏感身份线索的持续暴露风险。因此，本文方案为后量子背景下实现“期限内可追责、期限外强匿名”的匿名认证机制提供了一种编码型实现路径。

本文其余内容安排如下：第1章介绍预备知识、系统模型与安全模型；第2章给出基于HQC的周期性可否认环签名方案并分析其正确性；第3章在随机预言机模型下证明方案的不可伪造性、匿

名性、可追踪性及不可诽谤性；第4章对方案进行同层量化对比分析以及结构性对比分析；第5章全文总结。

1　预备知识

1.1　符号描述

为便于后续方案描述与安全性分析，本文首先统一给出全文中反复使用的核心符号及其含义，如表1所示。

除表1中的全局符号外，个别仅在局部证明或局部算法中出现的记号，将在其首次出现处说明。

1.2　准循环编码

设$F_2=\{0,1\}$为二元有限域，$\mathbb{F}_2^n$表示长度为n的二元向量空间，其中n为正整数。本文采用HQC编码算法中的准循环结构[27]，其核心运算基于循环卷积定义。在准循环表示下，给定公开量$h\in\mathbb{F}_2^n$，由其诱导的线性关系可统一表示为$s=x\oplus(h\circ y)$,其中$x,y\in\mathbb{F}_2^n$，$\oplus$表示按位异或运算，$\circ$表示HQC算法中采用的循环卷积运算。上述表示满足可计算性、线性结构性、准循环表示性三个基本性质。

1.3　HQC算法

本节基于HQC算法的公开规范与经典编码密码构造思想，介绍HQC算法中的关键算法模块[22][27]。HQC由系统初始化、密钥生成、密钥封装和密钥解封装四个算法组成，其核心在于由公开参数诱导的线性一致性关系。本文后续并不直接使用完整KEM流程，而是主要利用密钥生成阶段形成的公钥关系作为零知识证明语句。

1） *系统初始化*(Setup)

由系统初始化算法执行，生成公开参数。设参数包括向量长度n、重量参数ω_x，ω_y以及公开向量$h\in\mathbb{F}_2^n$。其中h用于定义HQC体制中的循环卷积运算$\circ$。此外，系统选取若干安全哈希函数作为后续派生挑战、绑定上下文或生成随机化种子的工具。初始化输出公开参数pp，并公开发布。

2） *密钥生成*(KeyGen)

参与方根据pp生成密钥对。具体地，用户随机选取满足重量约束的稀疏向量$x,y\in\mathbb{F}_2^n$，并计算$s=x\oplus(h\circ y)$，将公钥定义为$pk=(h,s)$，将私钥定义为$sk=(x,y)$。由上述构造可知，对合法密钥对有确定的线性一致性关系成立，即给定pk与sk，等式$s=x\oplus(h\circ y)$必然成立；而对外部验证者而言，在不知道(x,y)的情况下，仅由(h,s)直接恢复满足重量约束的(x,y)在计算上被认为是困难的。

3） *密钥封装*(Encaps)

发送方在接收方公钥$pk=(h,s)$下执行封装算法。发送方首先随机生成满足重量约束的稀疏向量对$(r_1,r_2)\in\mathbb{F}_2^n\times\mathbb{F}_2^n$，并基于公开参数计算与$pk$相关的线性组合量，例如$u=r_1\oplus(h\circ r_2)$,以及由$s$参与的进一步派生量，从而形成密文$ct=(u,aux)ct=(u,aux)$,其中$aux$表示与哈希派生、纠错或完整性校验相关的辅助字段。随后发送方对(ct,pk)进行哈希或密钥派生，得到会话密钥$K=H(ct\|pk\|\cdots)$最

表1　**符号说明**

符号	说明	符号	说明
$\mathbb{F}_2$	二元域	$\mathcal{R}$	准循环环$\mathbb{F}_2^n[x]/\left(x^n-1\right)$
n	HQC参数，对应$\mathbb{F}_2^n$	ω	汉明重量
Ω	权重约束	st	签名实例生成时间
(x,y)	私钥，$x,y\in\mathbb{F}_2^n$	t	当前争议处理时间
h,s	公钥分量，$s=x\oplus(h\circ y)$	T_w	争议时间窗口长度
R	环公钥集合	ctx	争议上下文
r	环大小	ε	三挑战空间
T	Σ协议并行轮	map	将比特串形式的挑战份额映射为三挑战格式的函数
ρ	签名随机盐	$stmt_i$	成员i的基础证据语句
u	Tag绑定向量	$stmt2_i$	扩展关系语句
Tag	签名标签	q_H	随机预言机查询次数

终输出封装结果(ct,k)。

4） 密钥解封装（Decaps）

接收方获得密文ct后，使用私钥$sk=(x,y)$执行解封装。接收方利用sk与pk的一致性关系，对密文中的关键分量进行恢复与校验，并据此重新计算派生密钥$K'=H(ct\|pk\|\cdots)$。若密文结构检查与一致性校验均通过，则输出K'；否则输出$\perp$。封装与解封装的正确性依赖于密文结构与公钥一致性关系所诱导的可验证计算过程。

因此，本文主要利用HQC公钥诱导的线性一致性关系刻画零知识证明语句，而不依赖封装/解封装过程中的具体密文结构。基于该关系，后续将构造Stern-like Σ协议，并通过Fiat–Shamir变换实现非交互式证明机制。

1.4　困难问题假设

本节在2024年张等人提出的基于SM2的周期性可否认环签名方案[16]的基础上，并结合编码密码体制中广泛研究的综合译码相关困难问题给出本文所采用的计算困难性假设[22][28-29]。相关困难问题建立在准循环编码结构及其诱导的线性关系之上。

本文在安全证明中采用两类困难问题：一类是与HQC公钥生成关系直接对应的关系型问题，主要服务于不可伪造性中的提取式归约；另一类是用于刻画结构分布与均匀分布可区分性的判定型问题，主要服务于匿名性分析中的分布不可区分论证。二者均建立在HQC准循环结构及其线性一致性关系之上，并非脱离HQC背景单独设定。

需要指出的是，本文不将Support Recovery问题表述为与HQC KEM的不可区分性（indistinguishability under chosen-ciphertext attack, IND-CCA）安全性完全等价的假设，而是将其作为由HQC公钥一致性关系诱导出的关系型搜索假设。该问题关注的是：在给定公开关系$s=x\oplus(h\circ y)$的条件下，恢复一组满足重量约束的低重量证据(x,y)。其困难性来源与准循环综合译码及低重量向量恢复问题保持一致。

为适配本文不可伪造性证明中的证据提取过程，首先给出由HQC公钥关系诱导的关系型支持恢复问题定义。

定义1　由HQC公钥一致性关系诱导的支持恢复问题（Support Recovery Problem）

设参数n为正整数，$h\in\mathbb{F}_2^n$为公开向量。假设存在未知向量对$(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n$，其满足预定的重量约束条件$wt(x)+wt(y)=\Omega$，并使得$s=x\oplus(h\circ y)$。求解一组满足上述等式与重量约束的$(x,y)$。攻击者$A$的优势定义为：$\mathrm{Adv}_A^{\mathrm{SR}}(\lambda)=\Pr[(x,y)\leftarrow A(h,s)\wedge s=x\oplus(h\circ y)\wedge wt(x)+wt(y)=\Omega]$。对任意概率多项式时间（probabilistic polynomial-time, PPT）攻击者A，$\mathrm{Adv}_A^{\mathrm{SR}}(\lambda)$为可忽略函数则称Support Recovery在给定参数下困难。

上述问题与本文不可伪造性证明中的证据提取目标相匹配。若攻击者能够从公开的(h,s)中恢复满足$s=x\oplus(h\circ y)$的低重量向量对(x,y)，则其破坏了HQC公钥关系中低重量秘密证据的隐藏性。因此，本文将Support Recovery作为不可伪造性归约中的搜索型困难假设。

为刻画HQC准循环结构在公开分布层面的不可区分性，进一步给出本文匿名性分析中使用的判定型困难问题。

定义2　准循环综合译码判定问题（Decision-DCC Decoding Problem）

在与定义1相同的参数条件下，考虑如下判定任务：给定$h\in\mathbb{F}_2^n$以及样本$s\in\mathbb{F}_2^n$，判定s是否来源于以下两种分布之一：

1）结构分布：从满足重量约束的稀疏向量对(x,y)中随机选取样本，并令$s=x\oplus(h\circ y)$；

2）均匀分布：从$\mathbb{F}_n^2$上随机采样s。

攻击者B的区分优势定义为：$\mathrm{Adv}_B^{\mathrm{DCC}}(\lambda)=\Pr\left[B(h,s)=1\middle|s\leftarrow D_R\right]-\Pr[B(h,s)=1|\ s\leftarrow D_U]$。对任意PPT攻击者$B$，为可忽略函数则称Decision-DCCDecoding在给定参数下困难。

综上，Support Recovery与Decision-DCC Decoding分别服务于不可伪造性中的证据提取和匿名性中的分布不可区分论证。二者均建立在HQC准循环结构及其公开线性关系之上，后续安全性分析将基于上述假设展开。

1.5　系统模型

为便于在安全模型中刻画签名查询、确认查询与否认查询等接口，本文首先给出基于HQC的周期性可否认环签名方案的系统模型。本文方案涉及系统公共参数、环公钥集合、签名者、验证者以及争议处理阶段的确认/否认过程。系统通过*Setup*算

法生成公共参数pp，并设定争议时间窗口长度T_w；每个用户通过*KeyGen*算法生成公私钥对(pk_i,sk_i)，其中公钥pk_i被纳入环公钥集合R，私钥sk_i用于生成签名或在争议期内生成确认/否认transcript。

从系统结构上看，本方案采用分层设计思想：在底层利用HQC公钥所诱导的线性一致性关系构造零知识证明语句，在此基础上通过Stern-like Σ协议及OR组合结构通过Fiat–Shamir变换实现匿名环签名，并进一步通过系统级时间窗口控制机制引入确认与否认功能，从而实现周期性可否认语义。整体结构如图1所示。

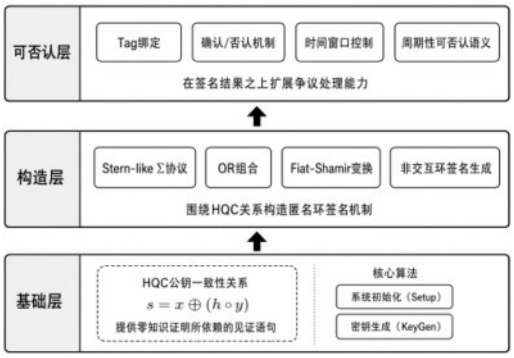

图1　基于HQC的周期性可否认环签名系统模型

图1从整体上展示了本文方案的系统模型。最底层是由HQC公钥一致性关系$s = x\oplus(h \circ y)$所刻画的基础关系层，用于提供后续零知识证明所依赖的证据语句；中间层是由Stern-like Σ协议、OR组合结构与Fiat–Shamir变换构成的匿名环签名生成机制；最上层是在签名结果之上进一步叠加Tag绑定与时间窗口控制，从而实现确认/否认功能及周期性可否认语义。

1） *基础层*

基础层建立在HQC编码结构之上，本文方案以HQC密钥生成过程中形成的公钥一致性关系$s = x\oplus(h \circ y)$作为零知识证明的基础关系，其中h为系统公共参数，(x,y)为满足重量约束的秘密向量。该层主要对应系统初始化与密钥生成算法，为后续签名与证明构造提供安全基础。本层主要包含*Setup*与*KeyGen*两个算法。

2） *构造层*

构造层用于生成可公开验证的环签名。在签名阶段，真实签名者利用自身私钥作为证据，通过Stern-like Σ协议证明其满足对应的HQC公钥一致性关系；同时，通过OR组合结构实现“环中至少一名成员掌握合法证据”的证明语义。对于非真实签名者对应的环成员，其证明转录由模拟器生成；真实签名者仅在自身分支中使用真实证据。随后，方案通过Fiat–Shamir变换将交互式OR-Σ协议转化为非交互式环签名，使验证者能够在不获知真实签名者身份的情况下验证签名有效性。本层主要包含*DRS - Sign*与*DRS - Verify*两个算法。

3） *可否认层*

可否认层用于实现争议时间窗口内的确认与否认功能。本文在签名结果中引入与消息、环公钥集合及随机盐绑定的标签Tag，并将其作为争议上下文的一部分。对于任一签名实例，设其生成时间为st，当前争议处理时间为t。当$t - st \leqslant T_w$时，系统接受与该签名实例相关的确认或否认请求：真实签名者可执行确认算法，生成确认transcript，用于证明该签名确由其生成；非签名者可执行否认算法，生成否认transcript，用于证明该签名与自身私钥不一致。当$t - st > T_w$时，系统不再受理与该签名实例相关的确认或否认请求，从而使签名者恢复长期匿名性。其中则争议期是指针对某一签名实例设置的确认/否认有效时间窗口。它从签名生成时间st开始，持续T_w，在该时间范围内允许用户围绕该签名实例发起确认或否认；超过该时间范围后，系统不再受理该签名实例的确认/否认请求。本层主要包含*Conf - Vrfy*和*Dis - Vrfy*算法。

1.6　安全模型

在第1.5节系统模型与文献[14]的基础上，本文建立适用于周期性可否认环签名的安全模型。该模型通过“对手A—挑战者C”之间的安全游戏进行刻画；Fiat–Shamir变换[26]所用哈希函数在随机预言机模型[30]（random oracle model, ROM）下建模为随机预言机H，A可对H进行自适应查询 。本文所称的“争议上下文”是指确认算法或否认算法所绑定的公开争议实例，而并非确认或否认过程本身的交互记录。确认与否认算法执行过程中产生的交互记录分别记为transcriptπ_C与π_D，这些记录用于后续第三方对争议进行复核。

除上述公共输入外，本文进一步为每个签名实例引入时间相关参数。具体地，设st表示该签名的生成时间，$T_w > 0$表示系统预设的争议时间窗口长度，t表示攻击者发起确认或否认查询时的当前时

间。对于给定签名实例，其确认/否认接口仅在满足 $t - st \leqslant T_w$ 时开放；若 $t - st > T_w$，则认为该签名已超出争议有效期，系统不再接受与之相关的确认或否认请求。由此，时间窗口条件被视为确认/否认阶段的公共接受前提，而非签名生成算法内部的隐含过程。

在安全游戏中，A 默认可以访问如下查询接口：

1）签名查询 $\mathcal{O}_{\text{Sign}}(m,R,i)$：返回诚实执行签名算法得到的签名 $\sigma \leftarrow \text{DRS - Sign}(\text{pp,m,R,sk}_i)$；

2）确认查询 $\mathcal{O}_{Conf}(m,R,\sigma,i,t)$：若该签名实例的生成时间记为 st，且满足 $t - st \leqslant T_w$，则返回诚实执行确认算法得到的 transcript π_C，否则返回 $\perp$；

3）否认查询 $\mathcal{O}_{Dis}(m,R,\sigma,i,t)$：若该签名实例的生成时间记为 st，且满足 $t - st \leqslant T_w$，则返回诚实执行否认算法得到的 transcript π_D；否则返回 $\perp$；

4）腐化查询 $\mathcal{O}_{\text{Cor}}(i)$：返回用户 i 的私钥 sk_i 对手可自适应腐化，但在挑战阶段会受到相应限制。

确认查询与否认查询返回的 transcript 仅对应于给定争议上下文下的诚实执行结果，其主要作用是支持事后争议处理，而不是提供可重用的签名证据。此外，其有效性不仅依赖于争议上下文的一致性，还依赖于时间窗口条件 $t - st \leqslant T_w$ 的满足，因此即便攻击者在争议期内获得某一有效 transcript，也不能在争议期结束后通过简单重放使其再次被系统接受。过期 transcript 重放、超期确认或否认请求不构成安全模型下的合法成功事件。在匿名性与不可伪造性实验中，依赖于底层 Stern-like Σ 协议的零知识可模拟性，这些 transcript 不应泄露真实签名者身份或私钥信息；而相应挑战由验证者均匀随机选取，不依赖随机预言机。

接下来在文献[14]的基础上，对本文的安全模型从不可伪造性、匿名性、可追踪性、不可诽谤性4个方面进行展开：

定义3 不可伪造性 任何多项式时间攻击者在自适应选择消息攻击下，都无法生成一个能够通过验证算法的有效可否认环签名。对手 A 与挑战者 C 进行如下游戏：

1）系统建立：C 运行 $pp \leftarrow \text{Setup}(1^\lambda)$，为1个用户生成密钥对 $(\text{pk}_i,\text{sk}_i)$，并将 pp 与环公钥集合 R 发送给 A。

2）查询阶段：A 可以自适应访问 $\mathcal{O}_{\text{Sign}}$、$\mathcal{O}_{\text{Conf}}$、$\mathcal{O}_{\text{Dis}}$、$\mathcal{O}_{\text{Cor}}(i)$ 以及随机预言机 H。

3）挑战阶段：A 输出 $(m^\star,R^\star,\sigma^\star,\tau^\star)$ 若同时满足 $\text{DRS - Verify}(pp,m^\star,R^\star,\sigma^\star)=1$；$(m^\star,R^\star)$ 未曾作为输入询问过 $\mathcal{O}_{\text{Sign}}$ 并得出；A 未腐化环 $R^\star$ 中至少一名成员，即存在 $\exists j \in [r]$ 使得 $\text{pk}_j \in R^\star$ 且 sk_j 未被腐化。则 A 赢得该游戏胜利。对手优势定义为 $\text{Adv}_\Pi^{\text{euf}}(A) = \Pr[\text{Exp}_\Pi^{\text{euf}}(\lambda)=1]$。

定义4 匿名性 在给定环公钥集合 R 与合法签名 $\sigma \leftarrow \text{DRS - Sign}(pp,m,R,\text{sk}_i)$ 的前提下，A 无法以非可忽略优势区分真实签名者是谁。A 输出挑战消息与环 $(m^\star,R^\star)$ 以及两个不同索引 $i_0 \neq i_1$ 且要求 $\text{pk}_{i_0},\text{pk}_{i_1} \in R^\star$；$C$ 检查 A 未腐化 i_0，i_1 后随机取 $b \leftarrow \{0,1\}$ 生成签名 $\sigma^\star \leftarrow \text{DRS - Sign}(pp,m^\star,R^\star,\text{sk}_{i_b})$ 并发送 $\sigma^\star$ 给 A；A 输出猜测 $b'=b$ 则 A 获胜。A 优势定义为 $\text{Adv}_\Pi^{\text{anon}}(A) = |\Pr[\text{Exp}_\Pi^{\text{anon}}] - \frac{1}{2}|$。

定义5 可追踪性 根据文献[14]的定义，可追踪性指对于任一能够通过验证的周期性可否认环签名，若其真实签名者属于环公钥集合，则在争议时间窗口内，不能出现环中所有成员均可成功否认该签名的情况。本文中的可追踪性不依赖独立的打开算法，而是通过验证算法 DRS - Verify、否认验证算法 Dis - Vrfy 实现责任澄清。形式化地，攻击者 A 输出：$(m^\star,R^\star,\sigma^\star,\{\pi_{D,i}\}_{i\in[r]})$。定义否认验证算法 $\text{Dis - Vrfy}(pp,m,R,\sigma,i,\pi_D) \in \{0,1\}$ 用于判定否认 transcript π_D 是否有效。若同时满足：$\text{DRS - Verify}(pp,m^\star,R^\star,\sigma^\star)=1$，并且同时满足 $\forall i \in [r]$，$\text{Dis - Vrfy}(pp,m^\star,R^\star,\sigma^\star,i,\pi_{D,i})=1$。则 A 赢得可追踪性实验。上述条件表示 $\sigma^\star$ 是一个有效签名，但环中所有成员均能生成可接受的否认 transcript π_D，从而使该签名无法在争议期内完成责任澄清。攻击者优 A 的势定义为：$\text{Adv}_\Pi^{\text{trace}}(A) = \Pr[\text{Exp}_\Pi^{\text{trace}}(\lambda)=1]$。

定义6 不可诽谤性 A 不能在不知道某用户私钥的情况下，构造一个确认性证明 π_C，使其通过确认验证并被判定为与该用户私钥一致。定义验证算法 $\text{Conf - Vrfy}(pp,m,R,\sigma,i,\pi_C) \in \{0,1\}$。$A$ 获胜的条件为 $\text{DRS - Verify}(pp,m^\star,\text{R}^\star,\sigma^\star)=1$，并且 A 伪造的 π_C 满足 $\text{Conf - Vrfy}(pp,m^\star,\text{R}^\star,\sigma^\star,i^\star,\pi_C{}^\star)=1$。

即$\pi_C^{\star}$为一个有效的交互记录，用于证明用户$i^{\star}$为该签名的生成者。证明优势定义为$\mathrm{Adv}_{\Pi}^{\mathrm{conf-snd}}(A)=\Pr\left[\mathrm{Exp}_{\Pi}^{\mathrm{conf-snd}}(\lambda)=1\right]$。

本文所称“周期性可否认”并不意味着签名文本本身随时间变化，而是指确认/否认接口的可访问性受到时间窗口约束。因而，时间因素对安全模型的影响主要体现在争议阶段的查询合法性与transcript验证条件中。对于任意签名实例，一旦其满足$t-st>T_w$，则系统不再受理与该实例有关的确认或否认请求。由此可知，过期后的transcript重放、超期确认或否认尝试以及脱离原始签名实例的时间参数篡改，均不构成安全模型下的合法成功事件。

本文后续安全分析除依赖HQC公钥关系所诱导的困难性假设外，还依赖底层Stern-like Σ协议及其OR组合结构的标准性质。其中，不可伪造性证明依赖固定承诺、不同挑战下的特殊可靠性以支持证据抽取；匿名性证明依赖零知识可模拟性及OR组合中的证据隐藏特征，以保证模拟分支与真实分支在分布上不可区分。Fiat–Shamir变换则仅引入随机预言机模型下的标准归约损耗，而不改变相关安全性质的基本论证结构。

2　基于HQC的周期性可否认环签名方案

2.1　方案设计

在第1.5节系统模型的基础上，本节给出具体方案，该方案由系统初始化、密钥生成、环签名生成、签名验证以及确认/否认算法等五类算法组成。系统通过设置长度为T_w的争议时间窗口，在该时间窗口内开放确认与否认接口，从而支持对真实签名者行为的责任澄清，并为非签名者提供免责能力。当争议时间窗口结束后，系统停止接受与该签名相关的确认或否认请求，使签名者重新获得长期匿名性，从而在责任追溯与隐私保护之间取得平衡。方案的总体算法执行流程如图2所示。

图2给出了本文方案的整体算法执行流程。系统首先通过 生成公共参数，并在 阶段建立HQC公钥一致性关系；随后在 阶段围绕该关系构造Stern-like Σ协议证明并生成可否认环签名，在 阶段对挑战一致性和各分支转录进行统一校验；当争议发生时，系统首先检查当前请求是否仍处于有效时间窗口 内，只有在满足时间窗口合法性条件的情况下，

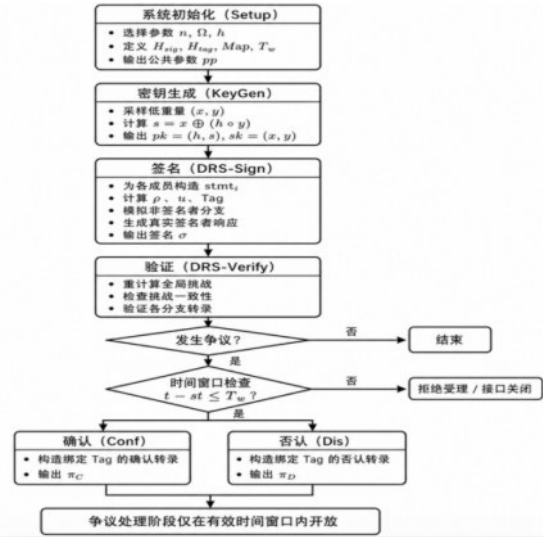

图2　基于HQC的周期性可否认环签名方案算法流程

才允许执行确认或否认算法。由此，图2体现了本文方案中“签名主流程”与“争议处理流程”的层次区分。

1） *系统初始化*(Setup)

输入安全参数1^{λ}，根据HQC推荐安全级别确定一组全局公共参数，输出系统公共参数集合pp。设参数包括：

（1）确定二元准循环多项式环$\mathcal{R}=\mathbb{F}_2[X]/(X^n-1)$，并确定向量长度参数$n$、权重阈值$\Omega$以及公开元素$h$。后续算法中出现的向量与运算均视为在$\mathcal{R}$上进行，采用二元向量形式实现。

（2）设挑战空间为$\varepsilon=\{0,1,2\}$，为将Fiat–Shamir导出的比特串挑战份额转换为底层Stern-like Σ协议所需的三挑战格式，定义映射函数$Map:\{0,1\}^k\times[T]\to\varepsilon$，用于比特串形式的挑战映射为Stern-like Σ协议三挑战格式。选取两个相互独立的哈希函数族$H_{sig}:\{0,1\}^*\to\{0,1\}^k$，$H_{tag}:\{0,1\}^*\to\{0,1\}^k$其中$H_{sig}$用于环签名Fiat–Shamir挑战生成，$H_{tag}$用于争议上下文绑定。

（3）设定争议时间窗口长度为$T_w>0$，在争议时间窗口内，系统向用户开放确认/否认接口，当争议时间窗口结束时，系统不再接受与该会话相关的确认/否认请求。

输出公共参数$pp=(\mathcal{R},n,\Omega,H_{sig},H_{tag},Map,T)$。

2） *密钥生成*($KeyGen$)

用户执行密钥生成算法$KeyGen(pp)$，随机生成满足权重约束的稀疏向量对$(x,y)\in\mathcal{R}^2$，使得

$wt(x)+wt(y)=\Omega$。随后计算公钥一致性关系$s=x\oplus(h\circ y)$，输出公钥$pk=(h,s)$，私钥$sk=(x,y)$，上述公钥一致性关系是本文后续环签名、确认与否认算法构造的基础。

3）可否认环签名生成($DRS\text{-}Sign$)

环公钥集合为$R=\{pk_1,...,pk_r\}$，真实签名者索引为$\pi\in\{1,...,r\}$，其私钥为sk_π，对消息m生成环签名σ：

（1）对每个成员$i\in\{1,...,r\}$,由公钥构造声明语句，记为$stmt_i:\exists(x_i,y_i)|s.t.|s_i=x_i\oplus h\circ y_i,|wt(x_i)+wt(y_i)=\Omega$其中，真实签名者$\pi$持有对应证据$w_\pi=(x_\pi,y_\pi)$，其余成员不掌握证据。

（2）采样签名随机盐$\rho\leftarrow\{0,1\}^\lambda$并对环集合进行确定性编码$Enc(R)=||_{i=1}^{r}(h_i||s_i)$定义绑定向量$u=H_{tag}(pp||m||\rho||r||Enc(R))$，并由真实签名者计算争议绑定标签$Tag=x_\pi\oplus(u\circ y_\pi)$该Tag将被纳入签名输出，并作为确认/否认阶段的一致性判定对象。

（3）对每个$i\neq\pi$，先随机选取k比特挑战份额$c_i\xleftarrow{\$}\{0,1\}^k$，令对每轮$t\in T$，$e_{i,t}=Map(c_i,t)\in\varepsilon$再调用Stern-like Σ协议的模拟器生成可接受转录$(Com_{i,t},rsp_{i,t})\leftarrow Sim(pp,stmt_i,e_{i,t})$

（4）对真实成员π，先生成其承诺集合$\{Com_{\pi,t}\}_{t=1}^{T}$保留用于响应的随机性，然后计算全局挑战

$c^*=H_{sig}(pp||m||\rho||r||Enc(R)||Tag||\{Com_{i,t}\}_{i\in[r],t\in[T]})$令真实成员的挑战份额为$c_\pi=c^*\oplus(\oplus_{i\neq\pi}c_i)$并对每轮$t$令$e_{\pi,t}=Map(c_\pi,t)$。随后按Stern-like Σ协议计算真实响应：$rsp_{\pi,t}\leftarrow\text{Prove}(pp,stmt_\pi,\omega_\pi,e_{\pi,t},Com_{\pi,t})$。

（5）输出可否认环签名$\sigma=(\rho,Tag,\{c_i\}_{i=1}^{r},\{(Com_{i,t},rsp_{i,t})\}_{i\in[r],t\in[T]})$。

4）可否认环签名验证($DRS\text{-}Verify$)

验证者在接收到消息m、环公钥集合R以及签名σ后，执行如下步骤验证签名有效性：

（1）解析签名σ，得到ρ，Tag，$\{c_i\}$，$\{Com_{i,t},Rsp_{i,t}\}$计算$Enc(R)$与$c^*=H_{sig}(pp||m||\rho||r||Enc(R)||Tag||\{Com_{i,t}\}_{i\in[r],t\in[T]})$。检查$\oplus_{i=1}^{r}c_i=c^*$若不成立则拒绝。

（2）对所有$i\in\{1,...,r\}$，验证Stern-like Σ协议转录$Verify(pp,stmt_i,Com_{i,t},e_{i,t},rsp_{i,t})=1$。

若以上检查均通过，则输出accept；否则输出reject。

5）确认/否认算法($Conf\&Dis$)

在执行确认或否认算法前，系统首先进行周期性检查。设签名生成时间为st，当前时间为t。通过计算$t-st$判断是否仍在该签名对应的争议时间窗口内，是则允许执行确认或否认算法，否则拒绝执行，具体如下：

（1）若$t-st\leqslant T_w$则认为仍在争议时间窗口内，系统向用户开放确认/否认接口。此时，受到诬陷的非签名者可调用否认算法以证明其并非真实签名者；真实签名者亦可调用确认算法以证明该签名确由其生成。

（2）若$t-st>T_w$则认为争议时间窗口已结束，系统不再受理与该签名实例相关的确认或否认请求，并输出$\perp$，从而恢复签名者的长期匿名性。这一时间合法性条件是确认/否认阶段的公共接受前提，不改变签名文本本身及其分布，而仅约束争议接口在何种时间范围内可被调用。

当$t-st\leqslant T_w$时，系统则向用户开放确认/否认接口，具体确认/否认算法如下：

在给定的争议上下文$(pp,m,R,\sigma,\text{Tag})$的条件下，证明者$P$与验证者$V$之间执行确认或否认算法，以证明$P$是否为该可否认环签名的实际签名者。为使确认/否认与签名标签绑定，引入扩展关系语句，记为$stmt2_i$。该语句除要求满足公钥一致性关系外，还要求标签关系与目标标签TagTarget保持一致：

$$stmt2_i:\exists(x_i,y_i)\text{s.t.}\begin{cases}s_i=x_i\oplus(h_i\circ y_i),\\ TagTarget=x_i\oplus(u\circ y_i),\\ wt(x_i)+wt(y_i)=\Omega,\end{cases}\text{其}$$

中在确认时令TagTarget = Tag，否认时令TagTarget = Tag$\oplus\Delta$。

（1）确认算法

若P为真实签名者i，其令TagTarget = Tag，并基于私钥$\text{sk}_i=(x_i,y_i)$生成Stern-like Σ协议的交互式证明transcriptπ_C，使验证者接受$stmt2_i$。验证算法Conf - Vrfy$(pp,m,R,\sigma,i,\pi_C)\in\{0,1\}$用于判定$\pi_C$是否有效。

（2）否认算法

若P非实际签名者i，其先计算自身标签$\text{Tag}_i=x_i\oplus(u\circ y_i)$令差分$\Delta=\text{Tag}\oplus\text{Tag}_i$。若$\Delta=0$则否认

失败；否则令 TagTarget = Tag⊕Δ，并生成否认证明 transcriptπ_D 使验证者接受 $stmt2_i$，验证算法 Dis - Vrfy$\left(pp,m,R,\sigma,i,\pi_D\right)\in\{0,1\}$ 用于判定否认证明是否有效。

确认与否认算法生成的交互记录分别记为 π_C 与 π_D，其可被第三方独立验证，但不会泄露任何超出安全模型允许范围的秘密信息。

2.2　正确性分析

本节在文献[15]基础上，通过签名验证、确认算法、否认算法三个方面进行本方案的正确性分析。

定理1 方案满足签名验证的正确性

证明　设真实签名者索引为 π，其私钥为 $sk_\pi=(x_\pi,y_\pi)$，满足公钥一致性关系 $s_\pi=x_\pi\oplus(h\circ y_\pi)$，且 $wt=(x_\pi)+wt(y_\pi)=\Omega$。在签名生成过程中：

1）真实签名者首先计算 $u=H_{tag}(pp\|m\|\rho\|r\|Enc(R))$，并构造绑定标签 $Tag=x_\pi\oplus(u\circ y_\pi)$。

2）对所有 $i\neq\pi$，调 Stern-like Σ 协议模拟器生成可接受转录 $(Com_{i,t},rsp_{i,t})$ 其分布与真实执行一致。

3）对真实成员 π，生成承诺集合 $\{Com_{\pi,t}\}_{t=1}^{T}$，计算全局挑战 $e^*=H_{sig}(pp\|m\|\rho\|r\|Enc(R)\|Tag\|\{Com_{i,t}\})$ 并令 $c_\pi=e^*\oplus\oplus_{i\neq\pi}c_i$，于是有 $\oplus_{i=1}^{r}c_i=c_\pi\oplus\oplus_{i\neq\pi}c_i$。

4）验证算法重新计算 $e^*=H_{sig}(pp\|m\|\rho\|r\|Enc(R)\|Tag\|\{Com_{i,t}$，并检查 $\oplus_{i=1}^{r}c_i=e^*$，该等式必然成立。

由 Stern-like Σ 协议的完备性可知：对真实成员 π，其响应满足关系 $stmt_\pi$；对模拟成员，其转录由模拟器生成且满足验证条件。因此对所有 i，均有 $Verify(pp,stmt_i,Com_{i,t},e_{i,t},rsp_{i,t})=1$，验证算法输出 accept。证毕。

定理2 方案满足确认算法的正确性。

证明　确认阶段使用扩展关系：$Stmt2_i$:

$$\begin{cases}s_i=x_i\oplus(h\circ y_i),\\ Tag=x_i\oplus(u\circ y_i),\\ wt(x_i)+wt(y_i)=\Omega\end{cases}$$

当 $i=\pi$ 时，由签名生成阶段知 $Tag=x_\pi\oplus(u\circ y_\pi)$，且公钥一致性关系成立，因此 $(x_\pi\circ y_\pi)$ 满足 $Stmt2_\pi$。确认算法对 $Stmt2_\pi$ 执行 Stern-like Σ 协议交互证明，由于该协议满足完备性，诚实证明者生成的 transcriptπ_C 必然能接受即 $Conf\text{ - }Vrfy(pp,m,R,\sigma,\pi,\pi_C)=1$。证毕。

定理3 方案满足否认算法的正确性。

证明　设用户 P 的索引为 i，$i\neq\pi$。其计算自身标签 $Tag_i=x_i\oplus(u\circ y_i)$，由于真实签名标签为 $Tag=x_\pi\oplus(u\circ y_\pi)$，若存在 $Tag_i=Tag$，则有 $x_i\oplus(u\circ y_i)=x_\pi(u\circ y_\pi)$，即 $x_i\oplus x_\pi=u\circ(y_\pi\oplus y_i)$。这意味着在已知公开向量 u 的情况下，存在一组满足重量约束的向量对 $(x_i\oplus x_\pi,y_\pi\oplus y_i)$ 满足线性一致性关系，违背了 Support Recovery 困难问题。

因此 $Tag_i=Tag$ 成立的概率可忽略。令 $\Delta=Tag\oplus Tag_i$，若 $\Delta=0$，则说明二者一致，否认失败；否则令 $TagTarget=Tag\oplus\Delta$，代入得 $TagTarget=Tag_i$。此时 (x_i,y_i) 满足：

$$\begin{cases}s_i=x_i\oplus(h\circ y_i),\\ Tag=x_i\oplus(u\circ y_i),\\ wt(x_i)+wt(y_i)=\Omega\end{cases}$$

因此其确实满足 $Stmt2_i$。由 Stern-like Σ 协议完备性，诚实生成的否认证明 transcriptπ_D 必然被接受，即 $Dis\text{ - }Vrfy(pp,m,R,\sigma,i,\pi_D)=1$。证毕。

3　安全性分析

本章在随机预言机模型（ROM）下对所提出的基于 HQC 的周期性可否认环签名方案进行安全性证明。分析表明，该方案能够同时满足不可伪造性、匿名性、可追踪性以及不可诽谤性等安全性质。

在安全分析中，本文环签名本质上是一个“单证据真实、其余分支可模拟”的 OR 组合结构：对环中非真实成员，调用底层 Stern-like Σ 协议模拟器生成可接受转录；对真实成员，仅在对应分支使用合法证据生成真实响应。因此在不可伪造性证明中，全局挑战由随机预言机对公开输入的查询结果确定，因此可结合分叉引理与底层协议在固定承诺、不同挑战下的特殊可靠性进行证据抽取。

在匿名性证明中底层 Stern-like Σ 协议满足零知识可模拟性，OR 组合结构中仅真实分支使用合法证据，其余分支均可由模拟器生成；同时，Fiat－Shamir 变换仅将交互式挑战替换为随机预言机输出，不改变上述分布不可区分性质。因此，当全部成员分支均被替换为模拟转录时，所得挑战签名分布仅依赖公开输入、随机盐与标签等公开上下文，

而与真实签名者索引无关。

3.1 不可伪造性

根据1.6节给出的定义3，本文在文献[14]所采用的不可伪造性分析框架基础上，对定理4进行分析，证明了基于HQC的周期性可否认环签名方案的不可伪造性。

定理4 在随机预言机模型下，若由HQC公钥一致性关系诱导的Support Recovery问题在给定参数下困难，则本文提出的HQC周期性可否认环签名方案满足不可伪造性。更具体地，若存在攻击者A以优势ε成功伪造有效签名，则可据此构造挑战者C，使其以至少与ε成多项式关系的优势求解相应的Support Recovery实例；该关系中的损耗主要来自关键随机预言机查询定位、分叉重运行以及局部可提取实例的定位过程。

证明：假设存在概率多项式时间PPT对手A，其在随机预言机模型下以优势ε赢得定义3所对应的不可伪造性安全游戏。记q_H为A对随机预言机H_{sig}的最大查询次数，r为环规模，T为并行轮数。这里q_H是多项式有界的查询次数，会进入分叉引理的概率损耗，不能作为可忽略项省略。下面构造挑战者C，利用A作为子程序求解第1.4节定义的关系型Support Recovery实例，并进一步分析由A的伪造优势到C的求解优势之间的量化关系。

1）系统建立阶段：挑战者C接收Support Recovery挑战样本$\left(h^{\star},s^{\star}\right)$，其中未知$\left(x^{\star},y^{\star}\right)$满足$s^{\star}=x^{\star}\oplus\left(h^{\star}\circ y^{\star}\right)$，$wt\left(x^{\star}\right)+wt\left(y^{\star}\right)=\Omega$。$C$的目标是恢复一组满足上述关系与重量约束的$\left(x^{\star},y^{\star}\right)$。随后$C$运行系统初始化得到公共参数$pp$，并为$r$个用户生成密钥对。$C$随机选取一个目标索引$i^{\star}\in[r]$，并设置$\mathrm{pk}_{i^{\star}}=\left(h^{\star},s^{\star}\right)$，而不掌握$\mathrm{sk}_{i^{\star}}$。对任意$i\neq i^{\star}$，$C$正常运行密钥生成算法得到$\left(\mathrm{pk}_i,\mathrm{sk}_i\right)$。最后$C$将$pp$与全部公钥发送给$A$。$C$初始化并维护3个列表：$\mathrm{List}_1$记录$H_{\mathrm{sig}}$的查询-应答对、$\mathrm{List}_2$记录$H_{tag}$的查询-应答对、$\mathrm{List}_3$记录签名查询$\mathcal{O}_{\mathrm{Sign}}$的输入输出。

2）查询阶段：A可以自适应访问随机预言机H与$\mathcal{O}_{\mathrm{Sign}}$、$\mathcal{O}_{\mathrm{Conf}}$、$\mathcal{O}_{\mathrm{Dis}}$、$\mathcal{O}_{\mathrm{Cor}}$。挑战者$C$依次应答如下。

（1）随机预言机查询：以H_{sig}为例，若A查询输入X，则C检索List_1。若存在记录则返回对应输出；否则均匀采样$c^{\star}\leftarrow\{0,1\}^{k}$，将$\left(X,c^{\star}\right)$写入$\mathrm{List}_1$并返回，对$H_{\mathrm{tag}}$同理，记录在$\mathrm{List}_2$。

（2）腐化查询$\mathcal{O}_{\mathrm{Cor}}$：若$i\neq i^{\star}$则$C$终止并宣告失败，记为事件$\mathrm{Bad}_1$，否则返回$\mathrm{sk}_i$。

（3）签名查询$\mathcal{O}_{\mathrm{Sign}}$：$A$给出消息$m$、环公钥集合$R=\left\{\mathrm{pk}_1,...,\mathrm{pk}_r\right\}$以及签名者索引$i\in\{1,...,r\}$。

□ C先采样盐并计算争议绑定向量$u=H_{\mathrm{tag}}\left(pp\ //\ m\ //\ \rho\ //\ r\ //\ \mathrm{Enc}(R)\right)$；

□ 随后对环中每个成员$t\in\{1,...,r\}$与每轮$k\in\{1,\cdots,\mathrm{T}\}$，$C$运行Stern-like Σ协议的模拟器生成可接受的单轮transcript$\left(Com_{t,k},rsp_{t,k}\right)\leftarrow\mathrm{Sim}\left(pp,\mathrm{stmt}_t,e_{t,k}\right)$。其中挑战$\mathrm{e}_{t,k}\in\{0,1,2\}$由稍后确定的挑战份额派生得到。

□ 记全部承诺集合为$\mathrm{COM}=\{\mathrm{Com}_{t,k}\}_{t\in[r],k\in[T]}$，$C$在随机预言机$H_{\mathrm{sig}}$上对输入点$\mathrm{X_{sig}}:=(\mathrm{DST_{SIG}}\ //\ pp\ //\ \mathrm{m}//\ \rho\ //\ \mathrm{Enc(R)}//\ Tag\ //\ COM)$择任意满足OR约束的挑战份额向量$\{c_t\}_{t=1}^{r}$并令$c^{\star}:=\bigoplus_{i=1}^{r}c_t$，$H_{\mathrm{sig}}\left(\mathrm{X_{sig}}\right)\leftarrow c^{\star}$再由$c_{\mathrm{t}}$确定各轮挑战$e_{t,k}\in\{0,1,2\}$使之与上述模拟transcript一致。

□ 输出签名：

$$\sigma=\left(\rho,Tag,\{c_t\}_{t=1}^{r},\{\left(Com_{t,k},rsp_{t,k}\right)\}_{t\in[r],k\in[T]}\right)\quad 3)$$

伪造阶段：A最终输出$m^{\star},R^{\star},\sigma^{\star}$，其中$\sigma^{\star}$为其伪造的可否认环签名。若同时满足

（**1**） $\mathrm{DRS\text{-}Verify}\left(pp,m^{\star},R^{\star},\sigma^{\star}\right)=1$；

（2）$(m^{\star},R^{\star})$未曾作为输入询问过$\mathcal{O}_{\mathrm{Sign}}$并得到签名输出。

（3）A未腐化环$R^{\star}$中至少一名成员。

则A赢得不可伪造性游戏。记事件Good为$\mathrm{pk}_{i^{\star}}\in R^{\star}$且$i^{\star}$未被腐化。

在事件Good发生的条件下，伪造签名σ^{*}中的全局挑战值由随机预言机H_{sig}在关键输入点X_{sig}^{*}上的响应确定。若A未曾查询X_{sig}^{*}而直接输出可通过验证的σ^{*}，则A相当于在未知$H_{sig}(X_{sig}^{*})$的情况下猜中全局挑战值，该事件概率至多为$\frac{1}{|FS|}$（$|FS|$表示Fiat－Shamir全局挑战空间大小），可并入$negl(\lambda)$。因此，在排除该可忽略事件后，A的成功伪造必然对应于H_{sig}的某一次关键查询。挑战者需要在至多q_H次查询中猜中该关键查询，并在同一

关键点X_{sig}^{*}上重新编程随机预言机输出，才能应用分叉引理得到两份有效伪造。下面说明如何利用这一点从有效伪造中恢复满足公钥一致性关系的证据，具体分为以下三个步骤：

（1）分叉提取

在事件Good发生且C猜中关键查询X_{sig}^{*}的条件下，C固定A的内部随机性，并保持除X_{sig}^{*}外所有随机预言机回答不变，仅在第二次运行中将$H_{sig}(X_{sig}^{*})$重新编程为一个独立随机值$c^{*\prime}$，其中$c^{*\prime} \neq c^{*}$。于是，两次运行对应的伪造在公开消息、随机盐、环编码、标签以及全部承诺集合上保持一致，仅由H_{sig}导出的全局挑战值不同。这一过程保证了两次伪造是在同一关键输入点上分叉得到的，从而为后续定位相同承诺下的不同挑战响应并进行证据抽取提供基础。

（2）伪造签名

由分叉引理可得到第2份有效伪造签名σ‘$=\left(\rho^{*},Tag^{*},\{c_i^{\prime}\}_{i=1}^{r},\{\left(Com^{*}_{t,k},rsp^{\prime}_{t,k}\right)\}_{i\in[r],t\in[T]}\right)$，其中$\rho^{*}$、$Tag^{*}$以及全部承诺集合$COM^{*}$与第一次伪造保持一致，仅全局挑战值由$c^{*}$变为$c^{*\prime}$。由于验证算法要求挑战份额满足$\oplus_{i=1}^{r}c_i=c^{*}$以及$\oplus_{i=1}^{r}c_i^{*}=c^{*\prime}$，且$c^{*\prime}\neq c^{*}$，因此至少存在某一成员索引$i_0\in[r]$，使得对应挑战份额满足$c^{\prime}_{i_0}\neq c_{i_0}$。又由于每个成员的逐轮挑战由映射$Map$作用于挑战份额得到，故必存在某一轮$t_0\in[T]$，使得在相同承诺$Com^{*}_{i_0,t_0}$下，两次运行得到的局部挑战不同，即$e^{*}_{i_0,t_0}\neq e_{i_0,t_0}$。这说明我们已经定位到一个“相同承诺—不同挑战—均可接受响应”的底层Stern-like Σ协议实例，可据此进行证据抽取。因此，问题已经从“全局两份伪造签名”归约为“同一底层Stern-like Σ协议实例在相同承诺下对应两个不同挑战的两组有效响应”。

（3）证据抽取

由于两次运行所得伪造签名σ^{*}与$\sigma^{*\prime}$均能通过验证，因此对应于索引i_0、轮次t_0的局部转录$(Com^{*}_{i_0,t_0},e_{i_0,t_0},rsp_{i_0,t_0})$与$(Com^{*}_{i_0,t_0},e^{\prime}_{i_0,t_0},rsp^{\prime}_{i_0,t_0})$在验证算法下均为可接受，且二者具有相同承诺$Com^{*}_{i_0,t_0}$而挑战不同，即$e_{i_0,t_0}\neq e^{\prime}_{i_0,t_0}$。根据底层Stern-like Σ协议的特殊可靠性，对于同一承诺若能够给出两组针对不同挑战的有效响应，则存在一个多项式时间提取算法，可以从这两组可接受转录中恢复相应证据。

在本文构造中，成员i_0的底层声明语句$stmt_{i_0}$:$\exists(x_{i_0},y_{i_0})|s.t.|s_{i_0}=x_{i_0}\oplus h\circ y_{i_0}+wt(y_{i_0})=\Omega$，。因而，提取算法可由上述两组转录恢复出一组证据$(x^{*},y^{*})$，使其满足$s^{*}=x^{*}\oplus(h\circ y^{*})$且$wt(x^{*})+wt(y^{*})=\Omega$。换言之，$C$已成功从目标公钥关系中恢复出满足重量约束的低重量秘密对，从而求解了Support Recovery实例。

下面分析挑战者C的成功概率。设攻击者A成功伪造的优势为$\varepsilon=\mathrm{Adv}_{\Pi}^{\mathrm{euf}}(A)$，并令$\varepsilon'=\varepsilon-negl(\lambda)$。其中，$negl(\lambda)$表示随机预言机碰撞、承诺碰撞、$A$未查询关键输入点$X_{sig}^{*}$却成功猜中全局挑战值等可忽略失败事件的概率总和。

在排除上述可忽略失败事件后，A的有效伪造必然对应H_{sig}的某一次关键查询。挑战者C需要在至多q_H次查询中猜中该关键查询，随后才能在同一个关键点X_{sig}^{*}上对H_{sig}的输出进行重编程。根据分叉引理，C能够以概率$\mathrm{Fork}(\varepsilon',q_H,|FS|)$得到两份有效伪造$\sigma^{*}$和$\sigma'$。二者具有相同的公开输入、相同的随机盐、相同的标签和相同的承诺集合，但对应不同的全局挑战值。其中$\mathrm{Fork}(\varepsilon',q_H,|FS|)$表示标准分叉引理给出的概率下界，其已经包含关键查询定位、第二次运行成功以及挑战空间大小带来的概率损耗。因此，$q_H(\lambda)$不能在优势分析中被忽略，分叉成功概率也不能简单写成ε。

获得两份有效伪造后，挑战者还需从r个环成员和T个并行轮次中定位可抽取的局部转录，保守地引入$\frac{1}{(rT)}$的概率损耗。由Stern-like Σ协议的特殊可靠性，C可从该位置的两份接受转录中抽取满足HQC公钥一致性关系的证据，从而求解Support Recovery问题。因此，C的成功概率满足：$Adv^{CSR}(C)\geqslant\frac{\mathrm{Fork}(\varepsilon',q_H,|FS|)}{(rT)}$。由于$q_H$、$r$和$T$均为多项式有界，且$\mathrm{Fork}(\varepsilon',q_H,|FS|)$与$\varepsilon'$之间仅存在标准分叉引理带来的多项式级损耗，若攻击者A的伪造优势ε为非可忽略量，则C求解Support Recovery问题的优势同样为非可忽略量。这与Support Recovery困难性假设矛盾，故本文方案满足不可伪造性。

3.2 匿名性

根据1.6节给出的定义4，在文献[14]所采用的匿名性分析框架基础上，对定理5进行分析，证明了基于HQC的周期性可否认环签名方案的匿名性。

定理5 若Decision-DCC Decoding问题在参数pp下是困难的，则任意多项式时间对手A都无法以非可忽略优势区分可否认环签名中真实签名者的身份，本方案满足匿名性。

证明：按定义4的匿名性实验，攻击者A输出挑战消息与环(m^*,R^*)以及两个未被腐化的挑战索引$i_0 \neq i_1$。挑战者随机取$b \in \{0,1\}$，并返回由成员i_b作为真实签名者生成的挑战签名σ^*。为分析攻击者区分b的能力，下面构造一系列混合实验。在真实实验$Hybrid_0$中，挑战签名按照本文签名算法生成，即仅索引i_b对应的分支使用真实证据，其他分支均由模拟器生成。接着构造实验$Hybrid_1$，其中保持全部公开输入、随机盐、标签和承诺格式不变，仅将索引i_b对应分支的真实转录替换为由底层Stern-like Σ协议模拟器生成的可接受转录。由于底层Stern-like Σ协议满足零知识可模拟性，因此$Hybrid_0$与$Hybrid_1$对攻击者而言计算上不可区分。进一步地，在$Hybrid_1$中，所有成员分支均由模拟器生成，因此该签名实例不再依赖真实证据所属索引，而仅依赖公开输入和随机预言机导出的挑战值。换言之，在该混合实验中挑战签名的分布与随机比特b无关，攻击者对b的最优策略不优于随机猜测。

若攻击者A仍能以非可忽略优势区分b，则可据此构造区分器，在随机预言机模型下结合上述混合替换过程，以非可忽略优势区分准循环结构样本与均匀样本，从而破坏Decision-DCC Decoding的困难性假设。应当指出，在该归约过程中，多轮并行与Fiat–Shamir变换仅带来与随机预言机查询次数、环规模及并行轮数相关的标准多项式级损耗，而不会改变“若可区分签名者索引，则可区分底层分布”的基本逻辑。故本文方案满足匿名性。

3.3 可追踪性

根据1.6节给出的定义5，本文在文献[14]所采用的可追踪性分析框架基础上，对定理6进行分析，证明了基于HQC的可否认环签名方案的可追踪性。

定理6 若本文方案满足不可伪造性，且确认/否认算法满足正确性，则方案满足可追踪性。

证明：假设∃PPT对手A能以非可忽略概率赢得定义5的实验，即在输出$(m^\star,R^\star,\sigma^\star,\{\pi_{D,i}\}_{i\in[r]})$使得$\sigma$能够通过公开验证，且环中所有成员均能够生成可被接受的否认transcript，即同时满足：$\mathrm{DRS\text{-}Verify}(pp,m^\star,R^\star,\sigma^\star)=1$ 且 $\forall i\in[r]$,$\mathrm{Dis\text{-}Vrfy}(pp,m^\star,R^\star,\sigma^\star,i,\pi_{D,i})=1$。上述事件表示，$\sigma^\star$是一个有效的周期性可否认环签名，但在争议时间窗口内，环集合$R^\star$中所有成员均能够生成可被接受的否认transcript，从而无法通过确认/否认算法完成责任澄清。对上述成功事件分两种情况讨论：

1）若$\sigma^\star$并非由任一环成员基于其签名私钥生成而仍能通过DRS - Verify，则A实质上构造了一个新的可验证签名，这意味着A能够以非可忽略概率生成未经签名查询得到的合法签名，从而违反定义3中的不可伪造性，与此前安全假设矛盾。

否则，$\sigma^\star$确由环中某真实签名者$i^\star$生成，根据第2.2节确认/否认算法正确性，$i^\star$在相同争议上下文下计算得到的标签与签名中的Tag一致，因此$i^\star$能够生成可被Conf - Vrfy接受的确认transcript；同时，其生成可被Dis-Vrfy接受的否认transcript的概率为可忽略。这与“$\forall i\in[r]$, $\mathrm{Dis\text{-}Vrfy}(pp,m^\star,R^\star,\sigma^\star,i,\pi_{D,i})=1$”的假设矛盾。

综上，若存在PPT对手以非可忽略概率破坏可追踪性，则可以据此构造算法分别破坏不可伪造性或确认/否认算法的正确性，这与前述安全假设相矛盾。因此，A成功破坏可追踪性的概率必然为可忽略量，从而说明本文方案满足可追踪性。

3.4 不可诽谤性

根据1.6节给出的定义6，本文在文献[14]所采用的不可诽谤性分析框架基础上，对定理7进行分析，证明了基于HQC的周期性可否认环签名方案的不可诽谤性。

定理7 方案满足不可诽谤性。

证明：假设敌手A在环R上针对消息m生成一个有效签名σ，并试图使环中某一非签名者用户u_j，无法构造一个会使针对该用户的确认性主张被验证接受的伪造确认记录，从而达到对u_j的诽谤。

根据否认算法的判定条件，若否认失败，则必须存在一份关于索引j的确认transcript使验证者接受，亦即该transcript与pk_j对应的语句成立相一致。由于确认/否认算法基于Stern-like Σ协议构造，确

认算法所证明的关系语句明确要求存在与公钥 pk_i 一致的证据 (x_i, y_i)，使其同时满足公钥一致性关系与标签一致性关系。因此，任意能够生成可被验证者接受之确认 transcript 的对手，依据 Stern-like Σ 协议的知识可靠性，能够抽取出该证据，而该证据在本方案中与用户 i 的签名私钥等价。因此任一能够生成可被验证者接受之确认 transcript 的 PPT 对手，隐含掌握与公钥 pk_j 一致的秘密证据。于是可推出 A 实际上能够给出与 u_j,私钥一致的响应，从而等价于 A 已掌握 u_j 的签名私钥 sk_j。

然而在安全模型中，敌手并未获得 u_j 的腐化权限，因此 A 不可能获得 sk_j。这与“否认失败必然要求掌握 sk_j”相矛盾。故敌手使非签名者无法否认的成功概率为可忽略量，本方案满足不可诽谤性。

此外，周期性机制主要约束争议阶段的接口访问。确认与否认 transcript 的接受不仅依赖争议上下文一致性，也依赖时间合法性条件 $t - st \leqslant T_w$。因此，争议窗口结束后的 transcript 重放、时间参数重声明或脱离原签名实例的确认/否认请求，均不能构成模型下的合法成功事件。

4　方案对比分析

本节从同层量化对比和结构性对比两个角度分析本文方案。首先，将本文方案与 SM9 可否认环签名方案[14]、SM2 周期性可否认环签名方案[16]、SM9 周期性可否认环签密方案[15]以及 SDitH 签名方案[32]进行通信开销、计算开销和功能特性比较；其次，结合近年编码型相关构造，说明本文方案在后量子匿名认证方向中的结构定位。通过上述比较，可更清晰地体现本文方案在抗量子安全性、可否认性、周期性控制和编码型构造范式之间的设计取舍。

4.1　同层量化对比分析

4.1.1　通信开销分析

表 2 给出了通信开销分析中所涉及的相关符号及其含义说明。

在本文方案中，上述参数均由所选安全级别确定。具体而言，在 HQC-128 安全参数下，码长参数 n 及稀疏权重参数 Ω 取值均为标准推荐值，相应向量与多项式的表示长度由此确定。在统一口径下，本文采用“输出对象长度求和”来度量通信负载：

表 2　通信开销相关符号及相应定义

符号	说明
n	HQC 方案中的码长参数
c	OR 组合结构中的单个挑战份额
com	单轮 Stern-like Σ 协议中的承诺
rsp	单轮 Stern-like Σ 协议中的响应
T	Stern-like Σ 协议并行轮数
r	环成员个数
$\lvert\rho\rvert$	随机盐长度
$\lvert Tag\rvert$	争议绑定标签长度
$mlen$	SM9 周期性可否认环签密密文长度
v	放大轮数
τ	并行重复参数
D	挑战相关维度参数

对环签名类方案，通信负载主要由群元素与标量域元素构成；对环签密类方案，还需额外计入密文长度 $mlen$；对 SDitH 编码型方案，则由多轮并行证明 transcript 的承诺与响应的叠加构成。

在本文方案中，一个周期性可否认环签名的格式为 $\sigma = (\rho, Tag, \{c_t\}_{t=1}^{r}, \{(com_{t,k}, rsp_{t,k})\}_{t\in[r],k\in[T]})$，其中 ρ 为随机盐，Tag 为争议绑定标签，$\{ct\}$ 为 OR 组合结构中的挑战份额，$(com_{t,k}, rsp_{t,k})$ 为底层 Stern-like Σ 协议系统在第 t 个环成员、第 k 轮生成的承诺与响应。因此，本文方案的签名通信开销由以下几部分构成：随机盐与标签的传输开销、r 个挑战份额的传输开销，以及 $r \cdot T$ 组 Stern-like Σ 协议转录的传输开销。由此可得，本文方案的签名通信开销为 $|\sigma| = |\rho| + |\mathrm{Tag}| + r \cdot |c| + r \cdot T \cdot (|com| + |rsp|)$。

在确认与否认算法中，证明者仅需针对单个环成员执行 Stern-like Σ 协议，其输出由证明承诺与响应组成，不涉及环中其他成员的证明信息。因此，本文方案中确认与否认算法的通信开销均与环大小 r 无关，仅与并行轮数 T 及底层证明参数相关，可表示为 $|Conf| = |Dis| = T \cdot (|com| + |rsp|)$。下面将从通信阶段和确认否认阶段对本方案进行对比分析：

1）在通信阶段，本文方案的签名通信开销随

环成员个数r及并行轮数T线性增长，该增长主要来源于OR组合结构下多成员证明转录的叠加，以及Stern-like Σ协议在多轮并行执行过程中所引入的通信开销。

SDitH方案同样体现为“多轮transcript叠加”的通信负载，但其通信主项来源于τ轮并行重复与2^D挑战空间相对应的证明转录开销。这一现象源于编码型零知识证明在单轮成功概率受限的情况下，需要通过多轮并行来实现可忽略的伪造概率，从而不可避免地引入T倍的transcript负载。

相较之下，基于SM2与SM9的可否认环签名方案依赖群运算或双线性对，签名长度通常随环规模线性增长，但不包含多轮transcript，在通信层面更为紧凑。但安全性建立在可被量子算法有效求解的数论假设之上。因此，本文方案在通信开销上的增加，本质上是为换取抗量子安全性与可否认性所付出的结构性代价。

2）在确认与否认阶段，本文方案确认与否认阶段仅需对单个成员输出证明记录，其通信开销与环规模无关，因而在大环规模条件下具有更好的可扩展性；而SM2方案的否认阶段通信量含v倍放大项，说明其否认机制通常需要重复以保证可靠性。对于SM9周期性可否认环签密，由于方案目标同时包含保密性，其签密输出中必须计入密文长度$mlen$，当消息较长时通信主导项将由“结构性群元素负载”转变为“密文长度”，这也是签密体制与环签名体制在通信层面的一项本质差异。

4.1.2 计算开销分析

本文对若干典型可否认环签名/环签密方案以及编码型签名方案的计算开销进行了对比分析。本文方案的主要计算开销来源于Stern-like Σ协议系统的执行过程，其计算复杂度随环成员数量及并行轮数线性增长。这一增长趋势本质上由OR组合结构与多轮证明机制所共同决定。从各阶段来看：

1）签名生成阶段

本方案与SDitH方案具有相近的计算开销，均主要由多轮Stern-like Σ协议生成过程构成；相较之下，SM9方案在签名阶段需要执行多次双线性对与目标群相关运算，单次运算代价较高；SM2周期性可否认环签名则由椭圆曲线群运算主导。本文方案以“低代价基础运算+多轮并行”的方式实现安全性，其计算负担集中体现在rT规模的证明生成开销上。而本方案仅涉及二元向量加法/异或运算以及稀疏向量与准循环多项式卷积运算，其基础运算形式相对简单，并具有较好的并行实现潜力。

2）验证阶段

本方案同样保持随环成员数量线性增长的计算特征，其主要计算由rT轮证明验证构成。随着环规模增大，验证端增长趋势与签名端一致。SM2方案验证主要受n次群运算影响；SM9方案验证含常数次配对与若干目标群运算；SDitH验证阶段需要重算TreePRG扩展并检查MPC视图一致性。由此可见，不同方案验证阶段的瓶颈并不相同：传统公钥方案瓶颈集中于高代价代数运算，而编码/零知识方案瓶颈集中于多轮证明结构带来的重复验证。

3）确认与否认阶段

本方案仅需针对单个环成员执行Stern-like Σ协议，其计算开销与环规模无关，主要由底层证明的并行轮数决定，因此在大规模环场景下具有良好的可扩展性。

相比之下，SM9可否认环签名的确认/否认阶段同样不随环规模增长，但其代价集中在配对与目标群运算；SM2方案的确认开销通常为常数阶，而否认阶段含重复放大项，体现出其否认机制对重复轮数的依赖。综合来看，本文方案在确认与否认阶段的计算开销虽然并非最低，但其结构较为清晰，且与编码型零知识证明框架下的可否认语义实现方式保持一致。

本方案的主要成本集中在Stern-like Σ协议的生成与验证过程，其复杂度随环规模线性增长。这种计算特征并非实现层面的低效，而是由编码型可否认环签名所需的零知识模拟与OR组合结构所决定的。与传统公钥体制下依赖指数运算或双线性对的方案相比，本文方案避免了大整数或椭圆曲线运算，其基本操作均为二元向量加法与稀疏卷积，具有良好的并行性与实现可控性。计算效率的劣势是实现抗量子安全性与可否认功能的代价。

4.1.3 功能对比分析

为全面地刻画本方案在抗量子背景下的设计取舍与功能定位，本节从抗量子性、可否认性以及结构特性三个维度，对本文方案与其他方案进行功能性对比分析，具体如下表3所示：

由表3可见，SM2与SM9类方案能够支持环签

表3　功能特性对比分析

方案	抗量子性	环签名匿名性	可否认确认/否认	周期性控制
SM9可否认环签名	否	是	是	否
SM2周期性可否认环签名	否	是	是	是
SM9周期性可否认环签密	否	是	是	是
SDitH签名	是	否	否	否
本文方案	是	是	是	是

名匿名性及确认/否认功能，部分方案还具备周期性控制机制，但其安全性主要建立在椭圆曲线离散对数或双线性对相关假设之上，在量子计算模型下难以提供长期安全保证。SDitH签名方案具有编码型抗量子安全基础，但其本身并不提供环签名匿名性、确认/否认接口和周期性控制机制。相比之下，本文方案直接基于HQC公钥一致性关系构造零知识证明语句，并结合Stern-likeΣ协议、OR组合和Fiat－Shamir变换实现非交互式环签名，同时通过Tag绑定和时间窗口机制引入确认/否认功能。该设计并非追求单项效率最优，而是在编码型后量子框架下统一实现抗量子安全性、环匿名性、可否认性与周期性控制。

因此，本文方案与传统SM2/SM9类方案的主要差异在于安全假设和抗量子能力，与SDitH类方案的主要差异在于功能完整性和应用语义。该结果体现了方案在后量子匿名认证场景下的功能定位。

4.2　结构性对比分析

除上述同层量化比较外，本文进一步结合近年编码型相关研究工作，对所提方案在后量子匿名认证方向中的结构定位作补充说明。这类工作与本文在研究目标上并不完全一致：一类主要关注后量子环签名或相关匿名认证机制的构造与效率优化，另一类主要关注代码基零知识证明及其对隐私保护原语的支撑能力。因此，本文不再沿用统一的通信与计算折算方式，而主要从功能目标与构造范式角度进行补充比较。

表4给出了本文方案与近年若干编码型相关构造在功能定位与结构特征方面的比较结果。

由表4可见，近年编码型相关研究主要沿两类路径推进：一类关注后量子环签名或匿名认证机制的构造与效率优化，如Gajland等方案[20]；另一类关注代码基零知识证明及其在签名或隐私保护原语中的应用，如Ouyang等方案[21]和Feneuil等方案[32]。这些工作说明编码型匿名认证和代码基零知识方向正在持续发展，但其目标通常不直接覆盖“环签名匿名性、确认/否认机制与周期性控制”的组合功能。与上述工作相比，本文方案的特点在于直接利用HQC公钥一致性关系作为零知识证明语句，并在此基础上构造周期性可否认环签名。因此，本文方案与现有编码型相关构造并非简单的效率替代关系，而是面向“期限内可澄清、期限外恢复匿名”应用需求的结构性扩展。

5　结束语

本文提出了一种基于编码体制的周期性可否认环签名方案，在后量子安全背景下同时支持环成员匿名性与可否认语义。方案通过引入Stern-like Σ协议与OR组合结构，在编码体制下系统性地实现了签名确认与非签名者否认功能，并结合周期性控制机制，实现了争议窗口内身份可确认、窗口外自动恢复匿名的设计目标。

表4　近年编码型相关构造补充比较

方案	是否具备环签名匿名性	是否支持确认/否认	是否支持周期性控制	主要构造特点
Gajland等方案[20]	是	否	否	关注后量子环签名及相关匿名认证机制构造
Ouyang等方案[21]	否	否	否	关注代码基零知识及其对隐私保护原语的支撑
Feneuil等方案[32]	否	否	否	关注syndrome decoding in the head框架下的短签名构造
本文方案	是	是	是	基于HQC关系直接构造周期性可否认环签名

参考文献：

[1] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings of the 35th Annual Symposium on Foundations of Computer Science. Los Alamitos: IEEE Computer Society Press, 1994: 124-134.

[2] Bernstein D J, Buchmann J, Dahmen E. Post-quantum cryptography [M]. Berlin: Springer, 2009.

[3] Ducas L, Kiltz E, Lepoint T, et al. CRYSTALS-Dilithium: a lattice-based digital signature scheme[J]. IEEE Transactions on Information Theory, 2018, 65(12): 7830-7853.

[4] Chen L, Jordan S, Liu Y K, et al. Report on post-quantum cryptography [R]. Gaithersburg: NIST, 2016.

[5] Rivest R L, Shamir A, Tauman Y. How to leak a secret[C]//Advances in Cryptology—ASIACRYPT 2001. Berlin: Springer, 2001: 552-565. DOI: 10.1007/3-540-45682-1_32.

[6] Bernhard D, Cortier V, Pereira O, et al. SoK: A comprehensive analysis of game-based ballot privacy definitions[C]//2015 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2015: 499-516.

[7] Jansen R, Syverson P. An analysis of the anonymity properties of onion routing over time[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016: 1533-1546.

[8] Möser M, Böhme R, Breuker D. Towards risk scoring of Bitcoin transactions[C]//Financial Cryptography and Data Security. Berlin: Springer, 2014: 16-32.

[9] Yuen T H, Esgin M F, Liu J K, et al. DualRing: generic construction of ring signatures with efficient instantiations[C]//Advances in Cryptology—CRYPTO 2021. Cham: Springer, 2021: 3-33.

[10] Chatterjee R, Garg S, Hajibabei M, et al. Compact ring signatures from learning with errors[C]//Advances in Cryptology—CRYPTO 2021. Cham: Springer, 2021: 282-312.

[11] Dwork C, Naor M, Sahai A. Concurrent zero-knowledge[J]. Journal of the ACM, 2004, 51(6): 851-898.

[12] Komano Y, Ohta K, Shimbo A, et al. Toward the fair anonymous signatures: Periodically deniable ring signatures[C]//Topics in Cryptology—CT-RSA 2006. Berlin: Springer, 2006: 174-191. DOI: 10.1007/11605805_12.

[13] 包子健, 何德彪, 彭聪, 等. 基于SM2数字签名算法的可否认环签名[J]. 密码学报, 2023, 10(2): 264-275. DOI: 10.13868/j.cnki.jcr.000592.
Bao Z J, He D B, Peng C, et al. Deniable ring signature scheme based on SM2 digital signature algorithm[J]. Journal of Cryptologic Research, 2023, 10(2): 264-275. DOI: 10.13868/j.cnki.jcr.000592.

[14] 丁勇, 罗世东, 杨昌松, 等. 基于SM9标识密码算法的可否认环签名方案[J]. 信息网络安全, 2024, 24(6): 893-902. DOI: 10.3969/j.issn.1671-1122.2024.06.007.
Ding Y, Luo S D, Yang C S, et al. An identity-based deniable ring signature scheme based on SM9 signature algorithm[J]. Netinfo Security, 2024, 24(6): 893-902. DOI: 10.3969/j.issn.1671-1122.2024.06.007.

[15] 张艳硕, 孔佳音, 周幸妤, 等. 基于SM9的周期性可否认环签密方案的设计[J/OL]. 通信学报. DOI: 10.11959/j.issn.1000-436x.2026017.
Zhang Y S, Kong J Y, Zhou X Y, et al. Design of periodic deniable ring signcryption scheme based on SM9[J/OL]. Journal on Communications. DOI: 10.11959/j.issn.1000-436x.2026017.

[16] 张艳硕, 袁煜淇, 李丽秋, 等. 基于SM2的周期性可否认环签名方案[J]. 信息网络安全, 2024, 24(4): 564-573. DOI: 10.3969/j.issn.1671-1122.2024.04.007.
Zhang Y S, Yuan Y Q, Li L Q, et al. Periodically deniable ring signature scheme based on SM2 digital signature algorithm[J]. Netinfo Security, 2024, 24(4): 564-573. DOI: 10.3969/j. issn. 1671-1122.2024.04.007.

[17] Zhang Y, Yuan Y, Yan Z, et al. Practical periodic deniable signature scheme based on ISRSAC[J]. Journal of King Saud University - Computer and Information Sciences, 2025, 37: 210. DOI: 10.1007/s44443-025-00217-w.

[18] McEliece R J. A public-key cryptosystem based on algebraic coding theory[R]. DSN Progress Report, 1978, 42-44: 114-116.

[19] Alagic G, Bros M, Ciadoux P, et al. Status report on the fourth round of the NIST post-quantum cryptography standardization process[R]. NIST IR 8545, 2025. DOI: 10.6028/NIST.IR.8545.

[20] Gajland P, Janneck J, Kiltz E. Ring signatures for deniable AKEM: Gandalf's fellowship[C]//Advances in Cryptology—CRYPTO 2024. Cham: Springer, 2024: 305-338. DOI: 10.1007/978-3-031-68376-3_10.

[21] Ouyang Y, Tang D, Xu Y. Code-Based Zero-Knowledge from VOLE-in-the-Head and Their Applications: Simpler, Faster, and Smaller[C]//Advances in Cryptology—ASIACRYPT 2024. Singapore: Springer, 2024: 436-470.DOI: 10.1007/978-981-96-0935-2_14.

[22] Aguilar Melchor C, Aragon N, Bettaieb S, et al. HQC: A code-based key encapsulation mechanism[R]. NIST Post-Quantum Cryptography Standardization Project, 2022.

[23] Stern J. A new identification scheme based on syndrome decoding[C]//Advances in Cryptology—CRYPTO 1993. Berlin: Springer, 1994: 13-21.

[24] Cayrel P L, Véron P, El Yousfi Alaoui S. A zero-knowledge identification scheme based on the q-ary syndrome decoding problem[C]//Selected Areas in Cryptography. Berlin: Springer, 2010: 171-186.

[25] Cramer R, Damgård I, Schoenmakers B. Proofs of partial knowledge and simplified design of witness hiding protocols[C]//Advances in Cryptology—CRYPTO 1994. Berlin: Springer, 1994: 174-187.

[26] Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems[C]//Advances in Cryptology—CRYPTO 1986. Berlin: Springer, 1987: 186-194.

[27] Aguilar Melchor C, Blazy O, Deneuville J C, et al. Efficient encryption from random quasi-cyclic codes[J]. IEEE Transactions on Information Theory, 2018, 64(5): 3927-3943.

[28] Finiasz M, Sendrier N. Security bounds for the design of code-based cryptosystems[C]//Advances in Cryptology—ASIACRYPT 2009. Berlin: Springer, 2009: 88-105.

[29] Sendrier N. On the structure of a randomly permuted concatenated code[C]//Post-Quantum Cryptography. Berlin: Springer, 2008: 1-17.

[30] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396.

[31] Herranz J, Sáez G. Forking lemmas for ring signature schemes[C]//International Conference on Cryptology in India. Heidelberg: Springer, 2003: 266-279.

[32] Feneuil T, Joux A. Syndrome decoding in the head: Shorter signatures from zero-knowledge proofs[C]//Advances in Cryptology – CRYPTO 2022. Cham: Springer, 2022: 541-572. DOI: 10.1007/978-3-031-15979-4_19.

张艳硕（1979–），男，陕西省宝鸡市，博士，北京电子科技学院副教授、博士生导师，主要研究方向为密码理论及其应用。

屠桢昊（2002–），男，浙江省台州市，北京电子科技学院研究生，主要研究方向为密码学。