基于SM9的周期性可否认环签密方案的设计

张艳硕，孔佳音，周幸妤，谢绒娜，秦晓宏
（北京电子科技学院密码科学与技术系，北京 100070）

摘　要：为解决传统密码方案中隐私保护与责任追溯之间的问题，提出了一种基于SM9的周期性可否认环签密方案。该方案结合基于身份的SM9密码算法和可否认环签名技术，通过引入周期性机制，增强了签密者身份的隐私保护和非签密者的可否认性，确保在特定时间内可以追溯签密者责任，并在诉讼时间结束后进一步保护签密者隐私。该设计不仅在理论上保障了数据完整性和安全性，还通过优化提升了系统效率。分析结果表明，所提方案在隐私保护、安全性和计算开销等方面具有优势，适用于电子投票、金融交易、政府机密通信等高隐私需求场景。

关键词：SM9；周期性可否认；环签密；隐私保护；安全通信
中图分类号：TP309
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2026017

Design of periodic deniable ring signcryption scheme based on SM9

Zhang Yanshuo, Kong Jiayin, Zhou Xingyu, Xie Rongna, Qin Xiaohong
Department of Cryptology Science and Technology, Beijing Electronic Science & Technology Institute, Beijing 100070, China

Abstract: To address the conflict between privacy protection and responsibility tracing in traditional cryptographic schemes, a periodic deniable ring signcryption scheme based on SM9 was proposed. This scheme combined the SM9 identity-based cryptographic algorithm with deniable ring signature technology, and introduced a periodic mechanism to enhance the privacy protection of the signcryptors and the deniability of non-signcryptors. It ensured that the signcryptor’s responsibility could be traced within a specific time period, while further protecting the signcryptor’s privacy once the litigation period expires. The design not only guaranteed data integrity and security theoretically but also improved system efficiency through optimization. Analysis results indicate that the proposed scheme has advantages in privacy protection, security, and computational overhead, making it suitable for high-privacy demand scenarios such as electronic voting, financial transactions, and government confidential communications.

Keywords: SM9, periodic deniable, ring signcryption, privacy protection, secure communication

0　引言

随着信息安全需求的不断提升，传统公钥密码系统由于需要依赖公钥基础设施（public key infrastructure, PKI）进行证书管理，往往面临较高的管理复杂性和安全隐患。为了解决这一问题，Shamir[1]提出了基于身份的密码系统，该系统通过

收稿日期：2025–10–15；**修回日期：**2026–01–13
通信作者：孔佳音，jiayin_kong@163.com
基金项目：国家密码科学基金资助项目（No.2025NCSF02028）；北京市自然科学基金资助项目（No.4232034）；中央高校基本科研业务费专项资金资助项目（No.3282024001）
Foundation Items: The National Cryptography Science Foundation of China (No.2025NCSF02028), Beijing Natural Science Foundation (No.4232034), The Fundamental Research Funds for the Central Universities (No.3282024001)

将密钥与用户身份标识直接绑定，避免了PKI体系中的证书管理难题。作为我国基于身份密码体制的国家标准算法，SM9（标准名称为“SM9标识密码算法”）[2-4]支持数字签名、密钥交换与加密等多种功能，具有高效、安全和易于管理的特性，在身份认证、隐私保护与区块链等场景中具有良好的应用前景。

环签名技术是一种能够提供强隐私保护的密码学方法。在2021年的美密会上，文献[5-7]提出了环签名技术在安全及效率方面的创新方案，该方案可广泛应用于需要匿名性和身份认证的场合。Naor[8]首次提出了可否认环认证的概念，旨在确保在保证用户隐私的同时，能够对其身份进行认证。随后，Komano等[9]提出了可否认环签名方案，允许环内的非签名者在遭遇诬陷时能够否认自己是签名者，同时保持环签名的匿名性和有效性。近年来，随着技术的不断发展，基于SM2和SM9的可否认环签名方案[10-11]应运而生，它们不仅继承了环签名技术的优势，还进一步加强了安全性和标准的兼容性。在环签名技术的发展过程中，越来越多的研究集中于提升隐私保护与责任追溯之间的平衡。袁煜淇等[12]提出了一种基于身份的代理环签名方案，有效地解决了传统环签名在动态环境下隐私保护与认证效率之间的矛盾。在2024年的美密会上，Gajland等[13]提出了一种基于环签名的可否认认证密钥交换机制，通过引入可否认性和环签名，为认证协议提供了更强的隐私保护和安全性。然而，现有的传统签名方案通常仅能验证消息的完整性，而无法同时满足加密的机密性需求。因此，如何在保证数据机密性的同时确保签名的完整性，成为一个亟待解决的问题。

为了解决这一挑战，签密技术[14]应运而生。签密技术结合了加密和签名的功能，不仅能够保护消息的机密性，还能验证其完整性，同时具有更低的计算和通信开销。在2020年的欧密会上，Bellare等[15]提出了一种改进的签密技术，通过派生密钥增强了iMessage通信的安全性，同时保证了信息的机密性和认证。Jaeger等[16]提出了一种基于对称加密的签密方案，应用于端到端加密的群组消息传输，通过将加密和签名操作结合，提供了高效的消息加密与身份认证，确保消息在传输过程中既保密又具有签名验证。基于SM9的签密方案[17]能够有效避免公钥证书管理问题，但其在隐私保护方面的能力有所不足。为此，近年来的研究提出了结合环签名和SM9签密技术的环签密方案[18]，该方案不仅能够保护签名者的隐私，而且还能在需要时提供对责任主体的追溯。张艳硕等[19]提出了一种周期性可否认环签名方案。本文在已有研究基础上，提出了一种新的基于SM9的周期性可否认环签密方案。该方案结合了SM9的高效性与可否认环签名技术的隐私保护优势，并通过创新性地引入周期性机制，解决了现有环签名方案中隐私保护与责任追溯之间的矛盾。传统的环签名技术在保证签名者身份隐匿的同时，往往缺乏有效的责任追溯机制，无法应对需要在特定时间段内进行身份确认的需求。本文构建的周期性可否认环签密方案允许根据安全需求动态调整时间窗口，从而在系统安全性与操作灵活性之间取得平衡。

与传统的静态密码机制不同，周期性设计能够灵活应对如电子投票[20]、金融交易及政府机密通信等多变的应用场景。在电子投票场景中，选民的投票行为可以在投票期间得到有效追溯，但在投票结束后，其身份便完全隐匿，避免了选民身份信息泄露；在金融交易场景中，该方案允许在交易的生命周期内追溯资金来源，但在周期过后，交易双方的隐私得到保护；在政府机密通信场景中，周期性设计为机密信息的交换提供了时限性的安全保障，确保通信双方的身份得到有效验证，且一旦时限过后，所有敏感信息立即得到隐藏，从而最大化保障了通信的隐私性。

1 预备知识

1.1 符号说明

本节介绍本文用到的符号说明，如表1所示。

1.2 双线性对

G_1,G_2是N阶加法循环群，G_T是N阶乘法群，双线性映射$e:G_1 \times G_2 \to G_T$满足以下3个条件[21]。

1) 双线性：对于$\forall P \in G_1,Q \in G_2$以及$a,b \in \mathbb{Z}_N$，有$e(aP,bQ) = e(P,Q)^{ab}$。

2) 非退化性：$\exists P \in G_1,Q \in G_2$，使$e(P,Q) \neq 1$，其中1是$G_T$的单位元。

3) 可计算性：对于$\forall P \in G_1,Q \in G_2$，存在有效的算法计算$e(P,Q)$。

表1　　符号说明

符号	说明
A, B	使用密码系统的两个用户
ds_A	用户A的签名私钥
e	从$G_1 \times G_2$到G_T的双线性映射
G_1, G_2	N阶加法循环群
G_T	N阶乘法群
g^u	乘法群G_T中元素g的u次幂
P_1, P_2	G_1, G_2的生成元
hid	用一个字节表示的私钥生成函数识别符
$H_1(Z,N), H_2(Z,N)$	密码函数，输入为比特串Z和整数N，输出为整数$h \in \mathbb{Z}_N^*$
$H_3(Z,\mathrm{len})$	密码函数，输入为比特串Z和长度值len，输出为长度len的比特串
ID_A	用户A的身份标识，可以唯一确定其公钥
ks	签名主私钥
$\bmod n$	模n运算
N	循环群的阶，为大于2^{191}的素数
$P_{\text{pub-s}}$	签名主公钥
$[u]P$	加法循环群中元素P的u倍
$x\|\|y$	x与y的拼接，x和y是比特串或字节串
$[x,y]$	不小于x且不大于y的整数集合
T	预设诉讼时间周期，由系统统一设定
t_s	某一轮环签密会话的开始时间，由系统记录
t_n	当前时间，由系统时钟给出
Timer	维护会话的计时器，初始为0，随时间流逝增加

1.3　基于身份的SM9密码算法

本节基于国家标准[3]介绍基于身份的密码体制中的国家标准算法SM9。SM9作为一种高效的密码学方案，包含签名与加密两个核心功能模块，分别由4个关键算法构成。

在SM9签名算法中，初始化阶段由密钥生成中心（key generating center, KGC）执行，生成签名主私钥$\mathrm{ks} \in [1,N-1]$及对应的签名主公钥$P_{\text{pub-s}}=[\mathrm{ks}]P_2$，并公开hid。在密钥生成阶段，KGC利用其掌握的主私钥，结合用户的身份标识ID_A，计算并分发该用户专属的签名私钥ds_A。当需执行签名操作时，用户A针对待传输消息M，选取一个范围在$[1,N-1]$的随机整数r，依次计算得到$g=e(P_1,P_{\text{pub-s}})$、$\omega=g^r$、$h=H_2(M\|\omega,N)$、$l=(r-h) \bmod N$和$S=[l]\mathrm{ds}_A$，最终输出形式为$(h,S)$的消息$M$的签名。在验证阶段，接收方$B$获取签名$(h',S')$后，通过一系列计算得到$g=e(P_1,P_{\text{pub-s}})$、$t=g^{h'}$、$h_1=H_1(\mathrm{ID}_A\|\mathrm{hid},N)$、$P=[h_1]P_2+P_{\text{pub-s}}$、$u=e(S',P)$、$\omega'=ut$和$h_2=H_2(M'\|\omega',N)$，判定等式$h_2=h'$是否成立，从而确认签名有效性。

SM9加密算法同样始于初始化阶段，由KGC产生主私钥$\mathrm{ke} \in [1,N-1]$及对应的主公钥$P_{\text{pub-e}}$，并公开hid。在密钥生成阶段，KGC为身份标识分别为ID_A和ID_B的用户生成其对应的加密私钥de_A和de_B。在加密过程中，发送方A向接收方B传输消息M时，计算$Q_B=[H_1(\mathrm{ID}_B\|\mathrm{hid},N)]P_1+P_{\text{pub-e}}$，选取一个范围在$[1,N-1]$的随机整数$r$。接着计算$g=e(P_2,P_{\text{pub-e}})$、$\omega=g^r$和$C_1=[r]Q_B$。接下来，根据加密明文的不同方法计算$C_2,C_3$。若加密明文的方法是基于密钥派生函数（key derivation function, KDF）的序列密码算法，则计算$\mathrm{klen}=K_1_\mathrm{len}+K_2_\mathrm{len}$和$K=\mathrm{KDF}(C_1\|\omega\|\mathrm{ID}_B,\mathrm{klen})$，其中KDF()为密钥派生函数。令$K_1$为$K$最左边的mlen比特，$K_2$为剩下的$K_2_\mathrm{len}$比特，并计算$C_2=M\oplus K_1$。若加密明文的方法是结合KDF的分组密码算法，则计算$\mathrm{klen}=K_1_\mathrm{len}+K_2_\mathrm{len}$和$K=\mathrm{KDF}(C_1\|\omega\|\mathrm{ID}_B,\mathrm{klen})$。令$K_1$为$K$最左边的$K_1_\mathrm{len}$比特，$K_2$为剩下的$K_2_\mathrm{len}$比特，计算$C_2=\mathrm{IV}\|\mathrm{Enc}(K_1,M,\mathrm{IV})$，$C_2$的结构中前16个字节为IV值，其中Enc()为GB/T 32907分组密码算法。然后计算$C_3=\mathrm{MAC}(K_2,C_2)$，并输出密文$C=C_1\|C_2\|C_3$，其中符号||表示将各部分的比特串依次拼接。这种级联结构将各组件绑定在一起，确保了数据的机密性和完整性。相应的，接收方B获得密文C后，首先从密文C中取出C_1，若判断$C_1 \in G_1$，则计算$\omega'=e(C_1,\mathrm{de}_B)$，然后根据加密明文的不同方法进行计算。若加密明文的方法是基于KDF的序列密码算法，则计算$\mathrm{klen}=\mathrm{mlen}+K_2_\mathrm{len}$，然后计算$K'=\mathrm{KDF}(C_1\|\omega'\|\mathrm{ID}_B,\mathrm{klen})$。令$K_1'$为$K'$最左边的mlen比特，$K_2'$为剩下的$K_2_\mathrm{len}$比特，计算$M'=C_2\oplus K_1'$。若加密明文的方法是结合KDF的分组密码算法，则计算$\mathrm{klen}=K_1_\mathrm{len}+K_2_\mathrm{len}$和$K'=\mathrm{KDF}(C_1\|\omega'\|\mathrm{ID}_B,\mathrm{klen})$。令$K_1'$为$K'$最左边的$K_1_\mathrm{len}$比特，$K_2'$为剩下的$K_2_\mathrm{len}$比特，

再计算 $M'=\mathrm{Dec}(K_1',C_2)$。最后计算 $u=\mathrm{MAC}(K_2',C_2)$，从 C 中取出比特串 C_3，若 $u=C_3$，则输出明文 M'。

SM9在计算效率与安全性方面取得了良好平衡，该算法的身份绑定特性有效简化了PKI的管理复杂度，在国家密码标准体系中占据重要地位。

1.4 困难问题假设

本节给出本文方案基于的两个双线性对相关的困难问题假设。

定义1 q-SDH问题[22]。给定 $q+2$ 个元素 $(P_1,P_2,xP_2,x^2P_2,\cdots,x^qP_2)$，$P_1\in G_1,P_2\in G_2$，找到一个二元组 $(c,\frac{1}{c+x}P_1)$ 是困难的，其中 $c\in\mathbb{Z}_N^*$。

定义2 q-BDHI问题[23]。给定 $q+2$ 个元素 $(P_1,P_2,xP_2,x^2P_2,\cdots,x^qP_2)$，$P_1\in G_1,P_2\in G_2$，计算 G_T 中的元素 $e(P_1,P_2)^{\frac{1}{x}}$ 是困难的。

1.5 基于SM9的环签密方案

包嘉斌[18]提出了一种基于SM9的环签密方案，该方案主要包含以下4个核心算法。

1) 初始化：KGC选择群 G_1,G_2,G_T，P_1 和 P_2 分别为 G_1,G_2 的生成元；选择哈希函数 H_1,H_2,H_3；选择随机整数 $s\in\mathbb{Z}_q^*$ 作为主私钥msk并计算得到 $P_{\mathrm{pub}_1}=sP_1$、$P_{\mathrm{pub}_2}=sP_2$ 和 $g=e(P_1,P_2)^s$。

2) 用户私钥生成：KGC根据用户身份标识 ID_i，计算 $v_i=H_1(\mathrm{ID}_i)$、$s_i=s(v_i+s)^{-1}$、$S_i=s_iP_1$ 和 $D_i=s_iP_2$，为用户生成签名私钥 S_i 和解密私钥 D_i。

3) 签密：给定接收者身份标识 ID_η 和身份标识集合 $U_n=\{\mathrm{ID}_1,\cdots,\mathrm{ID}_n\}$，发送者用签名私钥 S_π 进行签密。

① 随机选择整数 $r_0,r_1,\cdots,r_n\in\mathbb{Z}_q^*$，计算 $t_\pi=\sum_{i=1,i\neq\pi}^{n}r_i \bmod q$、$v_\eta=H_1(\mathrm{ID}_\eta)$ 和 $R_0=(r_0v_\eta)P_1+r_0P_{\mathrm{pub}_1}$。

② 对 $i\in\{1,\cdots,n\}\setminus\{\pi\}$，计算 $R_i=r_iP_{\mathrm{pub}_1}$。并计算 $w_0=g^{r_0}$、$R=r_\pi P_1+t_\pi P_{\mathrm{pub}_1}$、$w=w_0e(R,P_{\mathrm{pub}_2})$、$h=H_2(w\|m\|U_n)$ 和 $v_i=H_1(\mathrm{ID}_i)$。计算得到 $l_\pi=r_\pi-h-\sum_{i=1,i\neq\pi}^{n}r_iv_i \bmod q$，为确保签密的有效性，如果 $l_\pi=0$，则需要返回步骤①，重新执行签密过程。

③ 计算得到 $R_\pi=l_\pi S_\pi$，得到密文 $C=m\oplus H_3(R_0\|\cdots\|R_n\|w_0\|\mathrm{ID}_\eta)$。

④ 输出环签密 $\sigma=(h,R_0,\cdots,R_n,C)$，并将 (U_n,σ) 发送给接收者。

4) 解签密：接收者收到 (U_n,σ') 后，计算 $w_0'=e(R_0',D_\eta)$，得到 $m'=C'\oplus H_3(R_0'\|\cdots\|R_n'\|w_0'\|\mathrm{ID}_\eta)$。对所有用户 $i\in\{1,\cdots,n\}$，计算 $v_i'=H_1(\mathrm{ID}_i)$、$u_i'=e(R_i',v_i'P_2+P_{\mathrm{pub}_2})$ 和 $w'=w_0'g^{h'}\prod_{i=1}^{n}u_i'$。验证等式 $h'=H_2(w'\|m'\|U_n)$ 是否成立。若成立，则环签密验证通过，m' 为消息明文；否则，环签密验证不通过。

相较于文献[18]，本文方案主要在以下几个方面进行了改进和扩展。

1) 周期性机制的引入：本文引入周期性机制，使用户在特定时间段内可以进行责任追溯，而在特定时间段结束后则进一步保护用户隐私，实现了隐私保护与责任追溯的动态平衡。

2) 可否认性的增强：本文增加了确认/否认算法，允许非签密者在遭受不实指控时能够有效否认，真实签密者也可以在需要时确认自己的签密行为，增强了方案的公平性和可信度。

3) 安全性模型的完善：本文增加了可追踪性和不可诽谤性的安全定义，提供了更全面的安全保障。

4) 应用场景的扩展：通过周期性设计，本文方案更适用于既需要在特定时期内保证可追溯性，又需要在特定时期结束后保护参与者的长期隐私的场景。

5) 效率优化：本文通过算法优化减少了部分计算开销，在确认/否认阶段采用了更简洁的计算方法。

1.6 安全模型

在文献[18]的基础上，本节定义了一个周期性可否认环签密方案的安全模型。

定义3 不可区分性。如果对于任意多项式时间攻击者，在下面的游戏中，不能以不可忽略的概率赢得游戏，则称该方案具有不可区分性。

1) 系统建立阶段：挑战者运行初始化算法，将系统参数发给攻击者，并秘密保存主私钥。

2) 查询阶段：攻击者可以发起哈希询问查询、私钥生成查询、签密密文生成查询与解签密密文查询，挑战者按相应算法返回对应结果。

3) 挑战阶段：攻击者给出两个长度相同但内容不同的明文(M_0,M_1)、用户身份标识集合U_n^*、发送者的身份标识ID_A^*和接收者的身份标识ID_B^*，挑战者随机选择一个比特$\mu\in\{0,1\}$，生成M_μ的签密密文SC^*并返回给攻击者。

4) 猜测阶段：攻击者输出猜测$\mu'\in\{0,1\}$。若$\mu'=\mu$，则攻击者在该游戏中获胜。

定义 4　不可伪造性。在定义3的系统建立与查询阶段相同的条件下，伪造阶段为：攻击者给出伪造的签密密文SC^*、用户身份标识集合U_n^*、发送者的身份标识ID_A^*和接收者的身份标识ID_B^*。若该密文能够通过解签密过程的验证，且攻击者没有查询过ID_B^*的私钥，则攻击者在该游戏中获胜。

定义 5　匿名性。在定义3的系统建立与查询阶段相同的条件下，挑战阶段为：攻击者给出明文M、用户身份标识集合U_n、两组发送者与接收者的身份标识$(\mathrm{ID}_A,\mathrm{ID}_B)$与$(\mathrm{ID}_A',\mathrm{ID}_B')$，挑战者返回两个签密密文$(\mathrm{SC}_0,\mathrm{SC}_1)$。挑战者随机选择一个比特$\mu\in\{0,1\}$，将签密密文$\mathrm{SC}_\mu$返回给攻击者。猜测阶段为：攻击者输出对$\mathrm{SC}_\mu$的猜测$\mu'\in\{0,1\}$。若$\mu'=\mu$，则攻击者在该游戏中获胜。

定义 6　可追踪性。在定义3的系统建立与查询阶段相同的条件下，确认查询阶段为：攻击者给出用户身份标识集合U_n、发送者的身份标识ID_A和接收者的身份标识ID_B，挑战者返回确认结果。不可追踪阶段为：攻击者给出用户身份标识集合U_n^*。若该身份标识集合中没有任何一个成员能够通过确认查询，则攻击者在该游戏中获胜。

定义 7　不可诽谤性。在定义3的系统建立与查询阶段相同的条件下，否认查询阶段为：攻击者给出用户身份标识集合U_n、发送者的身份标识ID_A和接收者的身份标识ID_B，挑战者返回否认结果。可诽谤阶段为：攻击者给出用户身份标识集合U_n^*。若该身份标识集合中没有任何一个成员能够通过否认查询，则攻击者在该游戏中获胜。

2　基于SM9的周期性可否认环签密方案

2.1　方案设计

基于SM9的周期性可否认环签密方案由参数与密钥生成、环签密、解环签密和确认/否认算法组成，并通过在诉讼时间T内进行确认/否认算法，实现了对签密者的行为追溯和非签密者的行为澄清，避免非签密者受到不实诽谤。当诉讼时间结束，则不能进行确认/否认算法，从而更好地保护了签密者的身份隐私，同时在隐私保护与责任追溯之间实现了平衡。算法的具体内容如下。

1) 参数与密钥生成算法

KGC产生随机数$k\in\mathbb{Z}_N^*$作为主私钥，计算G_1中的元素$P_{\text{pub-e}}=kP_1$，G_2中的元素$P_{\text{pub-s}}=kP_2$作为主公钥并计算群G_T中的元素$g=e(P_1,P_2)^k$。

用户i的身份标识为ID_i，为产生用户的签密私钥，KGC首先在有限域F_N上计算$t_i=H_1(\mathrm{ID}_i\|\mathrm{hid},N)$，再计算$k_i=k(t_i+k)^{-1}$和$\mathrm{de}_i=k_iP_2,\mathrm{ds}_i=k_iP_1$，最后将$(\mathrm{de}_i,\mathrm{ds}_i)$传递给用户$i$，公开系统参数$\mathrm{pp}=\{N,G_1,G_2,G_T,P_1,P_2,H_1,H_2,P_{\text{pub-e}},P_{\text{pub-s}},H_3,g,\mathrm{hid}\}$并秘密保存$k$。

2) 环签密算法

假设发送者的身份标识为ID_A，接收者的身份标识为ID_B，身份标识集合为$U_n=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$。设要发送的消息为$M$，mlen是$M$的比特长度，执行以下步骤。

① 生成$n+1$个随机整数$r_0,r_1,\cdots,r_n\in\mathbb{Z}_N^*$，计算$v=\sum_{i=1,i\neq A}^{n}r_i \bmod N$。

② 计算$Q_B=H_1(\mathrm{ID}_B\|\mathrm{hid},N)P_1+P_{\text{pub-e}}$。

③ 对所有$i\in\{1,2,\cdots,n\},i\neq A$，计算$R_i=r_iP_{\text{pub-e}}$。

④ 计算群G_T中的元素$\omega_0=g^{r_0}$，$R=r_AP_1+vP_{\text{pub-e}}$，$\omega=\omega_0e(R,P_{\text{pub-s}})$。

⑤ 计算整数$h=H_2(M\|\omega\|U_n,N)$，$l=(r_A-h-\sum_{i=1,i\neq A}^{n}r_it_i)\bmod N$，若$l=0$则返回步骤①。

⑥ 计算G_1中的元素$R_A=l\mathrm{ds}_A,R_0=r_0Q_B$。

⑦ 计算密文$C=M\oplus H_3(R_0\|\cdots\|R_n\|\omega\|\mathrm{ID}_B,\mathrm{mlen})$。

⑧ 输出签密密文$\mathrm{SC}=(U_n,\sigma=(C,h,R_0,\cdots,R_n))$。

3) 解环签密算法

为解出签密密文$\mathrm{SC}=(U_n,\sigma'=(C',h',R_0',\cdots,R_n'))$，解签密者$B$首先计算$\omega_0'=e(R_0',\mathrm{de}_B)$。

① clen是C'的比特长度，计算明文数据$M'=C'\oplus H_3(R_0'\|\cdots\|R_n'\|\omega_0'\|\mathrm{ID}_B,\mathrm{clen})$。

② 计算群G_T中的元素$s=g^{h'}$。

③ 对$i=1,2,\cdots,n$，计算$t_i=H_1(\mathrm{ID}_i\|\mathrm{hid},N)$，

$u_i' = e(R_i', t_i P_2 + P_{\text{pub-s}})$，$\omega' = \omega_0' s \prod_{i=1}^{n} u_i'$。

④ 检验等式 $h' = H_2(\omega' \| M' \| U_n, N)$ 是否成立，若成立，则验证通过，返回明文数据 M'，否则验证不通过。

4) 确认/否认算法

证明者 P 为了证明消息 M 是由自己发出的，或者为了否认消息 M 是由自己发出的，需要验证者 B 提供身份标识 ID_B，并执行以下步骤。

① 计算 l、R_i、R_0 和 T，计算方法和签密算法一致。

② 计算 $R_P = l\text{ds}_P$。

③ 输出 PR 并返回给验证者 B，其中 $\text{PR} = H_3(R_0 \| \cdots \| R_A \| \cdots \| R_n \| \omega \| \text{ID}_B, \text{mlen})$。

④ 验证等式 $M = C \oplus \text{PR}$ 是否成立。若成立，则说明 P 是发送者；若不成立，则说明 P 不是发送者，即证明者 P 否认消息由自己发出。

接下来介绍本文提出的周期性机制设计的具体实现方法。

系统在每一轮环签密会话开始时启动一个计时器 Timer，记该会话开始时间为 t_s，诉讼时间周期为全局参数 T。对于任意时刻的当前时间 t_n，系统通过比较 $t_n - t_s \leqslant T$ 来判断当前是否仍处于该会话对应的诉讼时间内，具体流程如下。

1) 发送者与接收者运行环签密与解环签密算法，完成密文的加/解密与环签名的验证。

2) 解环签密算法结束后，系统读取当前时间 t_n，并进行以下计算。

① 若 $t_n - t_s \leqslant T$，则认为仍在诉讼时间内，系统向用户开放确认/否认接口。受到诽谤的非签密者可以调用否认算法，证明自己不是真实签密者；真实签密者可以调用确认算法，证明该消息的确由自己签密。

② 若 $t_n - t_s > T$，则认为诉讼时间已结束，系统不再接受与该会话相关的确认/否认请求。此时再回到环签密步骤，继续执行系统后续任务。

协议算法流程如图 1 所示。

2.2　正确性分析

本节在文献[18]的基础上给出本文方案的正确性证明。

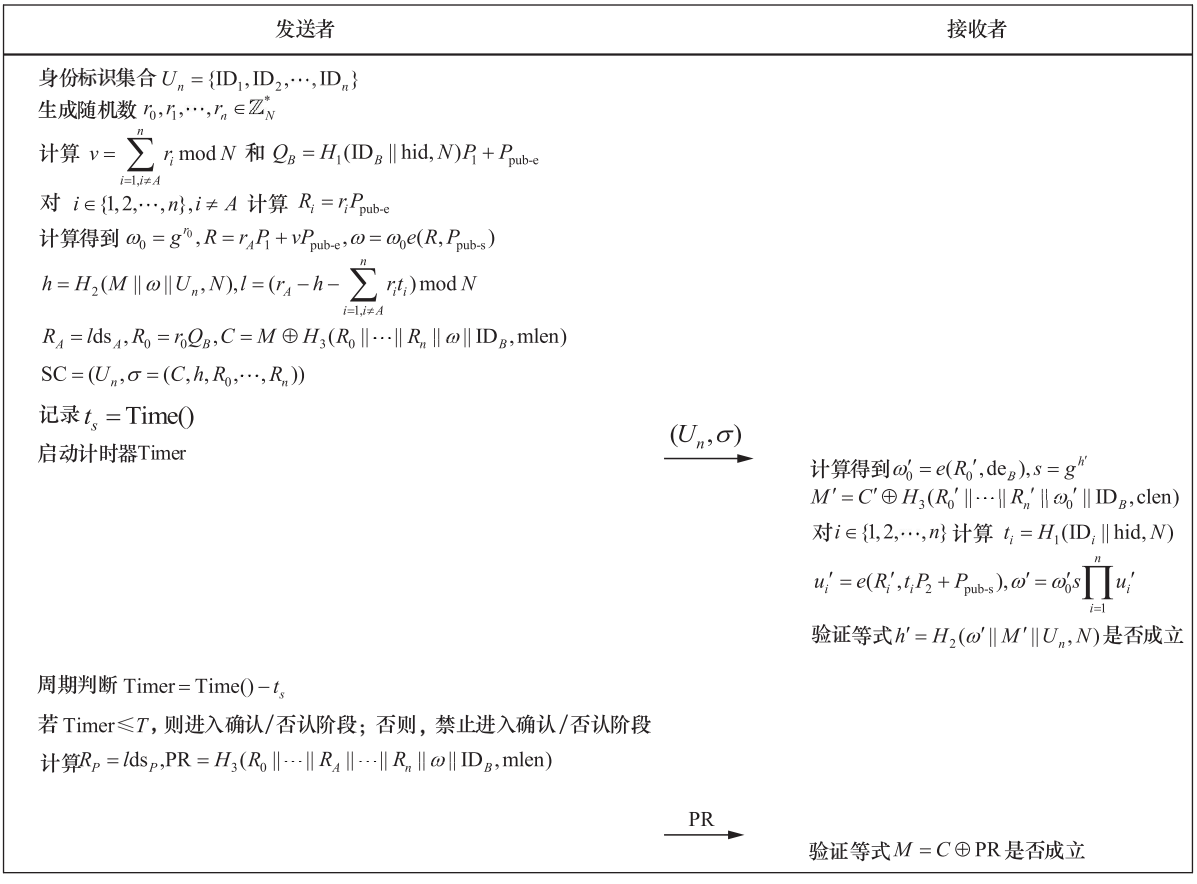

图 1　协议算法流程

定理1　基于SM9的周期性可否认环签密方案满足加解密的正确性。

证明　加解密部分的正确性关键在于$\omega_0' = \omega_0$，通过计算可得

$$\omega_0' = e(R_0',\mathrm{de}_B) = e(r_0(t_B - k)P_1 + r_0kP_1, kt_B^{-1}P_2) = e(P_1,kP_2)^{r_0} = g^{r_0} = \omega_0 \tag{1}$$

由于等式左边等于右边，因此$\omega_0' = \omega_0$成立，证毕。

定理2　基于SM9的周期性可否认环签密方案满足签名验签的正确性。

证明　由于签名验签部分的正确性关键在于$\omega' = \omega$，通过计算可得

$$\omega' = \omega_0 s\prod_{i=1}^{n}u_i = \omega_0 g^h e(R_i,t_AP_2 + kP_2)\prod_{i=1,i\neq A}^{n}e(R_i,t_iP_2 + P_{\text{pub-s}}) = \omega_0 g^h g^{r_A - h - \sum_{i=1,i\neq A}^{n}r_it_i} g^{\sum_{i=1,i\neq A}^{n}r_it_i} g^{k\sum_{i=1,i\neq A}^{n}r_i} = \omega_0 g^{r_A + k\sum_{i=1,i\neq A}^{n}r_i}\omega = \omega_0 e(R,P_{\text{pub-s}}) = \omega_0 e(r_AP_1,kP_2)e(\sum_{i=1,i\neq A}^{n}r_ikP_1,kP_2) = \omega_0 g^{r_Ak\sum_{i=1,i\neq A}^{n}r_i} = \omega_0 g^{r_A + k\sum_{i=1,i\neq A}^{n}r_i} \tag{2}$$

因此$\omega' = \omega$成立，证毕。

定理3　基于SM9的周期性可否认环签密方案满足确认/否认的正确性。

证明　已知

$$R_P = l\mathrm{ds}_P = (r_p - h - \sum_{i=1,i\neq P}^{n}r_it_i)$$
$$k(H_1(\mathrm{ID}_P\|\mathrm{hid},N) + k)^{-1}P_1, R_i = r_iP_{\text{pub-e}}$$
$$R_0 = r_0Q_B = r_0(H_1(\mathrm{ID}_B\|\mathrm{hid},N)P_1 + P_{\text{pub-e}}),$$
$$\mathrm{PR} = H_3(R_0\|\cdots\|R_A\|\cdots\|R_n\|\omega\|\mathrm{ID}_B,\mathrm{mlen}) \tag{3}$$

因为密文$C = M\oplus H_3(R_0\|\cdots\|R_n\|\omega\|\mathrm{ID}_B,\mathrm{mlen})$，若$R_P = R_A$，通过解签密算法计算可以得到$M = C\oplus H_3(R_0\|\cdots\|R_A\|\cdots\|R_n\|\omega_0\|\mathrm{ID}_B,\mathrm{clen})$，则$M = M'$，证明$P$为发送者；否则$M \neq M'$，证明$P$不为发送者。证毕。

3　安全性分析

本节在文献[18]基础上对本文方案的安全性进行分析。

定理4　如果q-BDHI问题是困难的，则本文方案是不可区分安全的。

证明　假设存在攻击者A能以不可忽略的概率ε攻破上述方案，则挑战者B能以不可忽略的概率解决q-BDHI问题。设B以一个q-BDHI问题实例$(P,Q,xQ,x^2Q,\cdots,x^qQ)$为输入，目标是计算$e(P,Q)^{\frac{1}{x}}$。

系统建立阶段。挑战者设置主私钥$\alpha = x$，并随机选择一个整数$k\in[1,q]$，$T_k\in\mathbb{Z}_N^*$，以及$q-1$个随机数$t_1,\cdots,t_{k-1},t_{k+1},\cdots,t_q\in\mathbb{Z}_N^*$。对于$i\in[1,q]$，$i\neq k$，可以计算得到$T_i = T_k - t_i$，定义多项式$f(m) = \prod_{i=1,i\neq k}^{q}(m + t_i) = \sum_{i=0}^{q-1}c_im^i$。然后根据已提供的实例计算得到$P_2 = f(x)Q = \sum_{i=0}^{q-1}c_i(x^iQ)$、$P_1 = f(x)P = \sum_{i=0}^{q-1}c_i(x^iP)$、$P_{\text{pub-s}} = \sum_{i=1}^{q}c_{i-1}(x^iQ)$和$P_{\text{pub-e}} = \sum_{i=1}^{q}c_{i-1}(x^iP)$。令$f_i(m) = \frac{f(m)}{x} + t_i = \sum_{i=0}^{q-2}d_im^i$，可以计算得到$\sum_{i=0}^{q-2}d_i(x^iQ) = f_i(x)Q = (\frac{1}{x} + t_i)P_2$和$\sum_{i=0}^{q-2}d_i(x^iP) = f_i(x)P = (\frac{1}{x} + t_i)P_1$两个等式。因此，对于任意的$i\in[1,q]$，$i\neq k$，三元组$(t_i,U_i = \frac{1}{x + t_i}P_2, V_i = \frac{1}{x + t_i}P_1)$都是可计算的。设$\alpha = -x - T_k$，计算$P_{\text{pub-s}} = -P_{\text{pub-s}} - T_kP_2 = \alpha P_2$和$P_{\text{pub-e}} = -P_{\text{pub-e}} - T_kP_1 = \alpha P_1$。由于$T_i = T_k - t_i$，可计算得到$P_2 + T_iU_i = P_2 + \frac{T_i}{x + t_i}P_2 = \frac{\alpha}{\alpha + T_i}P_2$，同理可得$P_1 + T_iU_i = \frac{\alpha}{\alpha + T_i}P_1$，因此当$i\in[1,q]$，$i\neq k$时，三元组$(T_i,\mathrm{ds}_i = \frac{\alpha}{\alpha + T_i}P_2,\mathrm{de}_i = \frac{\alpha}{\alpha + T_i}P_1)$都是可计算的。

哈希询问阶段。攻击者可以进行哈希询问，挑战者则返回相应结果。

H_1询问：挑战者维护存储二元组(ID,T)的列表L_1，并根据攻击者的询问返回或生成相应的T_i。

H_2询问：挑战者维护列表L_2存储四元组(M,ω,U,h)，并根据攻击者的询问返回或生成相应的h_i。

H_3询问：挑战者维护列表L_3存储五元组$(R,\omega,\mathrm{ID},R_0,E)$，其中$R = (R_1,\cdots,R_n)$，并根据攻击

者的询问返回或生成相应的E_i。

私钥生成查询阶段。攻击者发起ID_i的私钥查询，若$\mathrm{ID}_i=\mathrm{ID}_k$，则输出失败；否则，计算$(\mathrm{ds}_i,\mathrm{de}_i)$并返回给攻击者。

签密密文生成查询阶段。攻击者提供M，U，发送者和接收者身份标识为$(\mathrm{ID}_u,\mathrm{ID}_v)$，若$\mathrm{ID}_u\neq\mathrm{ID}_k$，则挑战者可计算$\mathrm{ID}_u$的私钥并返回密文。若$\mathrm{ID}_u=\mathrm{ID}_k$，挑战者可计算$\mathrm{ID}_v$的私钥并得到$\omega=\omega_0\prod_{i=1}^{n}e(R_i,t_iP_2+P_{\text{pub-s}})g^h$。最后通过$H_3$询问得到$E=H_3(R,\omega,\mathrm{ID}_v,R_0)$，可返回密文$\sigma=(R_0,R,C,h)$。

解签密密文查询阶段。攻击者提供密文$\sigma'=(R_0',R',C',h')$，U_n'。若$\mathrm{ID}_v\neq\mathrm{ID}_k$，挑战者可计算$\mathrm{ID}_v$的私钥并解签密返回明文。否则，输出失败。

挑战阶段。攻击者提供两段明文(M_0,M_1)，U_n^*，$(\mathrm{ID}_u^*,\mathrm{ID}_v^*)$。若$\mathrm{ID}_v^*=\mathrm{ID}_k$，则输出失败。否则，挑战者随机选取$h^*,t,r_0,\cdots,r_n\in\mathbb{Z}_N^*$，$C^*\in\{0,1\}^{\text{len}}$，返回密文$\sigma^*=(R_0{}^*,R^*,C^*,h^*)$。假设$r^*=\frac{t}{x}$，可以得到$R_0=-xP_1r^*=r^*(P_{\text{pub-e}}+T_kP_1)$，由于不能对$\omega^*=g^{r^*}$进行$H_3$询问，所以攻击者无法判断密文$\sigma^*$。

猜测阶段。攻击者输出猜测，挑战者从L_3中随机选择$(R_i,\omega_i,\mathrm{ID}_i,R_{0i})$，其中含$\omega^*$的概率为$\frac{1}{q_{H_3}}$。由于$\omega^*=g^{r^*}=e(P_1,P_{\text{pub-s}})^{r^*}=e(P,Q)^{\frac{f^2(x)t(-x-T_k)}{x}}$，并且有$f^2(x)=(\sum_{i=0}^{q-1}c_ix^i)f(x)t$，所以可以计算得到$\frac{f^2(x)t}{x}=tf(x)\sum_{i=0}^{q-2}c_{i+1}x^i+c_0t(\frac{c_0}{x}+\sum_{i=0}^{q-2}c_{i+1}x^i)$。困难问题的解为$(\omega^*e(tP_1,\sum_{i=0}^{q-1}c_ix^iQ)e(T_kt(P_1+c_0P),\sum_{i=0}^{q-2}c_{i+1}x^iQ))^{-\frac{1}{T_kc_0^2t}}$。

如果攻击者以不可忽略的概率ε攻破本文方案，则挑战者对q-BDHI问题的解决概率为$P[\text{success}]=P_0P_1P_2P_3\frac{1}{q_{H_3}}$，其中$P_0=1-\frac{q_n}{q}$（$q$表示空间大小，$q_n$表示攻击者的私钥查询次数），$P_1=1-\frac{q_{H_2}}{N}$，$P_2=1-\frac{1}{q}$，$P_3=1-\frac{1}{q}$，所以$P[\text{success}]=(1-\frac{q_n}{q})(1-\frac{q_{H_2}}{N})(1-\frac{1}{q})(1-\frac{1}{q})\frac{1}{q_{H_3}}$。证毕。

定理5 如果q-SDH问题是困难的，则本文方案是不可伪造安全的。

证明 假设存在攻击者A能以不可忽略的概率ε攻破上述方案，则挑战者B能以不可忽略的概率解决q-SDH问题。设B以一个q-SDH问题实例$(P,Q,xQ,x^2Q,\cdots,x^qQ)$为输入，目标是计算$e(c,\frac{1}{c+x}P)$。

伪造阶段。攻击者提供伪造密文$\sigma^*=(R_0{}^*,R^*,C^*,h^*)$，$U_n^*$，发送者和接收者的身份标识为$(\mathrm{ID}_u^*,\mathrm{ID}_v^*)$。若$\mathrm{ID}_u^*\neq\mathrm{ID}_k$，则输出失败；否则，根据分叉引理[24]，挑战者可获得另一组伪造密文$\sigma^*=(R_0{}',R',C',h')$。由于这两个密文都是有效的，因此$g^{h^*}e(R_u^*,t^*P_2+P_{\text{pub-s}})=g^{h'}e(R_u{}',t^*P_2+P_{\text{pub-s}})$。

如果攻击者能以不可忽略的概率ε攻破本文方案，则挑战者对q-SDH问题的解决概率为$P[\text{success}]=P_0P_1P_2P_3=(1-\frac{q_n}{q})(1-\frac{q_{H_2}}{N})(1-\frac{1}{q})\frac{1}{q}$。证毕。

定理6 如果本文方案使用的随机数是均匀分布的，则本文方案是匿名安全的。

证明 假设存在一个攻击者A能以不可忽略的概率ε攻破上述方案，则挑战者B能以不可忽略的概率区分出分别以随机数r_1和r_2生成的密文。

挑战阶段。攻击者提供明文M，U_n。挑战者返回两个密文(σ_0,σ_1)，其中σ_0的生成使用随机数r_1，σ_1的生成使用随机数r_2。挑战者随机选择$b\in\{0,1\}$，并将σ_b返回给攻击者。

猜测阶段。攻击者输出猜测b'，若$b'=b$，则攻击者赢得游戏。

由于$R_i=\begin{cases}r_iP_{\text{pub-e}},i\neq A\\(r_A-h-\sum_{i=1,i\neq A}^{n}rt_i)\mathrm{ds}_A,i=A\end{cases}$，其中$r_i$和$r_A$均为随机数，若攻击者能以不可忽略的概率区分出真实密文，则挑战者能以不可忽略的概率区分出均匀分布的随机数r_1和r_2。证毕。

定理7 如果真实发送方存在于身份标识集合

中，则本文方案是可追踪安全的。

证明　假设存在一个攻击者A能以不可忽略的概率ε攻破上述方案，则攻击者能使身份集合中没有任何一个成员通过确认查询。

确认查询阶段。攻击者提供明文M和U_n，发送者和接收者的身份标识为$(\mathrm{ID}_u,\mathrm{ID}_v)$。挑战者通过确认算法返回确认结果。

不可追踪阶段。攻击者给出的U中没有任何一个成员能够通过确认查询，则攻击者赢得游戏。

由于$R_i=\begin{cases}r_iP_{\text{pub-e}},i\neq A\\(r_A-h-\sum\limits_{i=1,i\neq A}^{n}rt_i)\mathrm{ds}_A,i=A\end{cases}$，若发送者存在于$U_n$中，则必然存在$R_A=(r_A-h-\sum\limits_{i=1,i\neq A}^{n}r_it_i)\mathrm{ds}_A$可以通过确认查询。证毕。

定理8　如果身份标识集合中存在除真实发送方外的成员，则本文方案是不可诽谤安全的。

证明　假设存在一个攻击者A能以不可忽略的概率ε攻破上述方案，则攻击者能使身份标识集合中没有任何一个成员通过否认查询。

否认查询阶段。攻击者提供明文M和U，发送者和接收者的身份标识为$(\mathrm{ID}_u,\mathrm{ID}_v)$。挑战者通过否认算法返回否认查询结果。

可诽谤阶段。攻击者给出的U中没有任何一个成员能够通过否认查询，则攻击者赢得游戏。

由于$R_i=\begin{cases}r_iP_{\text{pub-e}},i\neq A\\(r_A-h-\sum\limits_{i=1,i\neq A}^{n}rt_i)\mathrm{ds}_A,i=A\end{cases}$，若$U_n$中存在除发送方外的成员，则必然存在$R_i=(r_A-h-\sum\limits_{i=1,i\neq A}^{n}r_it_i)\mathrm{ds}_i,i\neq A$可以通过否认查询。证毕。

4　方案对比分析

本节将从计算开销的角度对本文方案与其他相关方案进行分析比较，重点关注发送方和接收方两个环节的计算开销。由于系统初始化和密钥生成算法可由KGC事先完成，且对使用过程中的效率没有影响，因此不在本次评估和比较的范围之内。

表2展示了不同方案在发送方和接收方计算开销方面的对比分析结果。具体来说，T_h表示哈希运算时间，T_{pm}表示点乘时间，T_{pa}表示点加时间，T_{bp}表示双线性对运算时间，T_{me}表示模幂时间，T_{inv}表示求逆时间。其他运算所需的时间占整体运算时间的比例较小，因此在评估时进行了适当忽略。

表2数据显示，本文方案在发送方和接收方的点乘与点加运算次数上显著优于对比方案，通过优化哈希、双线性对和模幂计算流程，有效降低了发送方和接收方的计算开销。此外，本文方案在计算步骤的安排上合理分配了各项运算任务，避免了不必要的重复计算，从而进一步提升了整体效率。整体而言，本文方案通过优化关键计算环节，具备了更高的计算效率和较低的资源消耗，尤其适合大规模系统中对性能和效率要求较高的应用场景。

接下来，表3给出了各方案的安全性能对比分析情况。表3数据显示，本文方案在多项安全性能上表现优异，同时具备不可区分性、不可伪造性、匿名性、可追踪性、不可诽谤性和周期性。相比之下，其他方案尽管在某些方面安全性能表现较好，但在周期性、匿名性等方面的安全性能较弱，这可能会影响其在实际应用中的安全性。总体而言，本文方案在安全性能方面具有全面的优势，尤其适合在需要高度安全保障的场景中使用，如隐私保护和防伪验证等应用。

表2　　**各方案发送方和接收方计算开销**

方案	发送方计算开销	接收方计算开销
文献[10]	$(n+1)T_h+(4n-1)T_{\text{pm}}+(2n-2)T_{\text{pa}}+T_{\text{inv}}$	$(n+1)T_h+4nT_{\text{pm}}+2nT_{\text{pa}}$
文献[11]	$T_h+(n+7)T_{\text{pm}}+2T_{\text{pa}}+4T_{\text{bp}}$	$T_h+3T_{\text{pm}}+T_{\text{pa}}+2T_{\text{bp}}+T_{\text{me}}$
文献[17]	$3T_h+3T_{\text{pm}}+T_{\text{pa}}+T_{\text{bp}}+T_{\text{me}}$	$3T_h+T_{\text{pm}}+T_{\text{pa}}+3T_{\text{bp}}+T_{\text{me}}$
文献[19]	$(2n+1)T_h+(7n-3)T_{\text{pm}}+(4n-2)T_{\text{pa}}+T_{\text{inv}}$	$3T_h+(8n+20)T_{\text{pm}}+(4n+10)T_{\text{pa}}$
文献[25]	$nT_h+(3n-1)T_{\text{pm}}+(n-1)T_{\text{pa}}+nT_{\text{bp}}+(n-1)T_{\text{me}}$	$nT_h+2nT_{\text{pm}}+nT_{\text{pa}}+nT_{\text{bp}}+nT_{\text{me}}$
文献[26]	$(n+1)T_h+nT_{\text{pm}}+nT_{\text{pa}}+T_{\text{bp}}$	$(n+1)T_h+3T_{\text{bp}}$
本文方案	$(n+2)T_h+(n+4)T_{\text{pm}}+2T_{\text{pa}}+2T_{\text{bp}}+T_{\text{me}}$	$(n+2)T_h+nT_{\text{pm}}+nT_{\text{pa}}+3T_{\text{bp}}+T_{\text{me}}$

表3 各方案安全性能对比分析情况

方案	不可区分性	不可伪造性	匿名性	可追踪性	不可诽谤性	周期性
文献[10]	×	√	√	√	√	×
文献[11]	×	√	√	√	√	×
文献[17]	√	√	×	×	×	×
文献[18]	√	√	√	×	×	×
文献[19]	×	√	√	√	√	√
文献[25]	×	√	√	×	×	×
文献[26]	√	√	√	×	×	×
本文方案	√	√	√	√	√	√

5 结束语

本文提出的基于SM9的周期性可否认环签密方案，结合了SM9密码算法的高效性与可否认环签名技术的优点，解决了传统签名方案在隐私保护与责任追溯方面的不足。通过引入周期性机制，本文方案确保在特定时间内可以追溯签密者责任，并在诉讼时间结束后进一步保护签密者隐私，在保障用户隐私的同时提供了对签密行为的追溯功能和非签密者在遭遇诬陷时的可否认功能，充分平衡了隐私保护与安全责任的需求。分析结果表明，本文方案在计算效率和安全性能方面均表现出较好的性能，适用于需要同时满足机密性、安全性和隐私性要求的场景，如电子投票、金融交易和政府机密通信等。

参考文献：

[1] Shamir A. Identity-based cryptosystems and signature schemes[C]//Advances in Cryptology. Berlin: Springer, 1985: 47-53.

[2] GB/T 38635.1—2020 信息安全技术 SM9标识密码算法 第1部分：总则[S]. 北京: 中国标准出版社, 2020.
GB/T 38635.1—2020 Information security technology—identity-based cryptographic algorithms SM9: part 1: general[S]. Beijing: Standards Press of China, 2020.

[3] GB/T 38635.2—2020 信息安全技术 SM9标识密码算法 第2部分：算法[S]. 北京: 中国标准出版社, 2020.
GB/T 38635.2—2020 Information security technology—identity-based cryptographic algorithms SM9: part 2: algorithms[S]. Beijing: Standards Press of China, 2020.

[4] GB/T 41389—2022 信息安全技术 SM9密码算法使用规范[S]. 北京: 中国标准出版社, 2022.
GB/T 41389—2022 Information security technology—SM9 cryptographic algorithm application specification[S]. Beijing: Standards Press of China, 2022.

[5] 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. Berlin: Springer, 2021: 251-281.

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

[7] Lyubashevsky V, Nguyen N K, Seiler G. SMILE: set membership from ideal lattices with applications to ring signatures and confidential transactions[C]//Advances in Cryptology-CRYPTO 2018. Berlin: Springer, 2018: 34-63.

[8] Naor M. Deniable ring authentication[C]//Advances in Cryptology-CRYPTO 2002. Berlin: Springer, 2002: 481-498.

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

[10] 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.
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.

[11] 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.
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.

[12] 袁煜淇, 刘宁, 张艳硕. ISRSAC上基于身份的代理环签名方案设计[J]. 北京电子科技学院学报, 2023, 31(3): 62-77.
Yuan Y Q, Liu N, Zhang Y S. Design of identity based proxy ring signature scheme on ISRSAC[J]. Journal of Beijing Electronic Science and Technology Institute, 2023, 31(3): 62-77.

[13] Gajland P, Janneck J, Kiltz E. Ring signatures for deniable AKEM: gandalf's fellowship[C]//Advances in Cryptology-CRYPTO 2024. Berlin: Springer, 2024: 305-338.

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

[15] Bellare M, Stepanovs I. Security under message-derived keys: signcryption in iMessage[C]//Advances in Cryptology-EUROCRYPT 2020. Berlin: Springer, 2020: 507-537.

[16] Jaeger J, Kumar A, Stepanovs I. Symmetric signcryption and E2EE group messaging in Keybase[C]//Advances in Cryptology-EUROCRYPT 2024. Berlin: Springer, 2024: 283-312.

[17] 赖建昌, 黄欣沂, 何德彪, 等. 基于商密SM9的高效标识签密[J]. 密码学报, 2021, 8(2): 314-329.
Lai J C, Huang X Y, He D B, et al. An efficient identity-based signcryption scheme based on SM9[J]. Journal of Cryptologic Research, 2021, 8(2): 314-329.

[18] 包嘉斌. 基于SM9标识密码算法的环签密方案设计及其应用研究[D]. 武汉: 武汉大学, 2022.
Bao J B. Identity-based ring signcryption scheme based on SM9 algorithm[D]. Wuhan: Wuhan University, 2022.

[19] 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.
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.

[20] 兰祥, 郭瑞, 王俊茗. 电子投票系统中基于区块链的无证书环签密方案[J]. 计算机工程与应用, 2024, 60(16): 288-301.
Lan X, Guo R, Wang J M. Certificateless ring signcryption scheme

based on blockchain for electronic voting systems[J]. Computer Engineering and Applications, 2024, 60(16): 288-301.

[21] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]//Advances in Cryptology-CRYPTO 2001. Berlin: Springer, 2001: 213-229.

[22] Boneh D, Boyen X. Short signatures without random oracles[C]//Advances in Cryptology-EUROCRYPT 2004. Berlin: Springer, 2004: 56-73.

[23] Boneh D, Boyen X, Goh E J. Hierarchical identity based encryption with constant size ciphertext[C]//Advances in Cryptology-EUROCRYPT 2005. Berlin: Springer, 2005: 440-456.

[24] Herranz J, Sáez G. Forking lemmas for ring signature schemes[C]// Progress in Cryptology-INDOCRYPT 2003. Berlin: Springer, 2003: 266-279.

[25] 彭聪, 何德彪, 罗敏, 等. 基于SM9标识密码算法的环签名方案[J]. 密码学报, 2021, 8(4): 724-734.
Peng C, He D B, Luo M, et al. An identity-based ring signature scheme for SM9 algorithm[J]. Journal of Cryptologic Research, 2021, 8(4): 724-734.

[26] 俞惠芳, 吕芝蕊. 基于联盟链的身份环签密方案[J]. 电子与信息学报, 2023, 45(3): 865-873.
Yu H F, Lü Z R. Identity ring signcryption based on consortium blockchain[J]. Journal of Electronics & Information Technology, 2023, 45(3): 865-873.

[作者简介]

张艳硕（1979– ），男，陕西宝鸡人，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。

孔佳音（2001– ），女，安徽合肥人，北京电子科技学院硕士生，主要研究方向为密码学。

周幸妤（2000– ），女，江苏镇江人，北京电子科技学院硕士生，主要研究方向为密码理论及其应用。

谢绒娜（1976– ），女，山西永济人，博士，北京电子科技学院教授、博士生导师，主要研究方向为密码理论与协议。

秦晓宏（1976– ），女，内蒙古锡林浩特人，北京电子科技学院讲师，主要研究方向为密码技术和信息安全。