基于双信道动态演进的抗关联区块链双方隐蔽通信方法

宰光军, 董彦男, 王贻鹏, 徐振宇, 佘　维

(郑州大学 网络空间安全学院,河南 郑州 450001)

摘　要: 针对现有区块链隐蔽通信方案普遍存在缺乏前向安全性、抗关联分析能力薄弱以及通信流程不完备等核心问题,提出一种自演进的闭环区块链隐蔽通信协议(SECL-CCP)。该协议通过三大创新机制构建了一个从密钥、协议流程到链上基础设施均能动态演进的安全体系。首先,设计"密钥棘轮"机制,结合"承诺-揭示"方案与区块链未来状态的公共熵,实现密钥的不可逆更新,赋予协议前向安全性。其次,提出"动态合约工厂"模型,利用 CREATE2 操作码为每轮通信动态部署"用完即弃"的交互合约,消除固定链上指纹。最后,引入基于零知识证明的接收回执机制,构建可验证的通信闭环,解决接收方不可抵赖问题。仿真实验基于以太坊 Sepolia 测试网与 Hardhat 环境开展,采集主网真实流量构建了含 20,000 条样本的混合数据集。结果表明,该协议将随机森林与 LSTM 模型下的隐写分析检测率分别降至 12.8%与 11.5%,并在密钥泄露场景下实现历史信息零泄露,有效抵御了智能关联分析攻击。

关键词:隐蔽通信; 区块链; 零知识证明; 前向安全性; 抗关联分析

中图分类号:TP393.0;TN915.08　　**文献标志码**:A　　**doi**:10.13705/j.issn.1671-6833.2026.06.016

随着网络对抗技术不断演进以及各类复杂数据挖掘分析算法的涌现,针对数据隐私的安全威胁日益加剧,传统信息加密已不足以满足高安全场景下的通信需求。隐蔽通信旨在隐藏通信行为本身的存在性,通过将秘密信息嵌入公开载体,实现第三方无法察觉的通信,已成为信息安全领域的核心分支之一。近年来,以比特币[1]和以太坊[2]为代表的区块链[3]技术以其去中心化、假名性、不可篡改以及不断演进的安全共识机制[4]等特性,为构建抗审查、高鲁棒性的隐蔽通信信道提供了全新的范式[5]。

利用区块链的公开账本特性进行隐蔽通信的研究已取得显著进展。早期的研究主要聚焦于存储型信道的构建,即如何将信息比特流嵌入到交易的各个字段中。Partala[6]提出了可证明安全的 BLOCCE 模型,通过修改交易地址的最低有效位嵌入信息。后续研究沿此思路,探索了利用交易数额[7]、OP_RETURN 字段[8]及未使用脚本字段[9]等多种嵌入方式。然而,这类直接嵌入原始数据的方法,其统计特征显著,易于遭受统计分析攻击。

为提升信道的不可区分性,近期研究转向了更为复杂的载体生成与动态编码机制[10]。载体生成方面,研究者利用生成式模型创造更加自然的载体,如应用马尔可夫链生成文本[11]或生成式对抗网络生成图像[12],显著增强了交易的合理否认性;在此基础上,刘媛妮等[13]进一步提出了基于图像多重隐写的方案,通过多重对抗网络生成高隐蔽载体并结合 IPFS 突破了链上存储容量的限制。动态性方面,为对抗基于固定映射规则的分析,研究者提出了动态编码方案,如动态标签信道[14]、交易时间间隔信道、基于时间型二叉树的动态编码模型[15],以及基于地址混淆的受控安全级隐蔽传输方案[16]极大地提升了通信的隐蔽性和抗分析能力。最新进展中,秦姣华等[17]提出一种基于区块链信息映射的无载体隐写方法以降低地址暴露风险;Yuan 等[18]则针

收稿日期:2026-04-16;**修订日期**:2026-05-25

基金项目:国家重点研发计划项目(31703-3)

作者简介:宰光军(1979—),男,河南南阳人,郑州大学教授,硕士,主要从事信息安全、领域软件工程等方面的研究,E-mail:zaiguangjun@zzu.edu.cn。

通信作者:佘维(1977—),男,湖南常德人,郑州大学教授,博士,博士生导师,主要从事区块链、信息安全、智能系统等方面的研究,E-mail:wshe@zzu.edu.cn。

对物联网场景设计了群组隐蔽通信方案。

然而,现有研究在信道构建层面虽日趋成熟,但在协议的完备性与长期安全性上,仍普遍停留在“单向投递”模型,存在以下 3 个深层次问题:

(1)密钥体系的静态依赖问题:大多数现有模型,即便是实现了动态编码,其安全性仍最终依赖于一个长期不变的共享秘密。尽管近期已有研究尝试引入无需私钥直接共享的传输机制以降低密文泄漏风险,但由于缺乏完善的前向安全保护,一旦该核心秘密在未来任意时刻被泄露,历史通信记录仍将面临被回溯解密的威胁。

(2)链上足迹的固化风险问题:尽管研究者利用一次性地址和环签名等技术增强身份匿名性,但多数依赖智能合约的方案,其通信双方仍需与一个或少数几个固定的、长期存在的合约地址进行交互。这个固定的交互点,对于长期观察的攻击者而言,是一个显著的指纹。通过对与该地址交互的所有交易进行长期的流量关联和元数据分析,攻击者仍有可能推断出通信关系的存在,从而破解隐蔽性。

(3)通信流程的单向投递模型问题:现有方案大多采用单向投递模型。发送方将信息投递至区块链后,无法通过协议内生的、可信的方式得知接收方是否已成功接收并正确解密。这导致恶意或受胁迫的接收方可轻易否认收到消息,使协议在需要高可靠性和不可抵赖性的应用中缺乏完备性。

为应对上述挑战,本文从协议顶层设计出发,提出一种自演进的闭环区块链隐蔽通信协议 (SECL-CCP),其核心思想是构建一个从密钥体系、协议流程到链上基础设施均能动态演进和自我更新的安全框架。与现有的基于 OP_RETURN 的存储型或特定合约的中继型隐蔽通信方案相比,本文方案的本质区别在于:实现了从静态地址到动态跳变、从静态密钥到单向棘轮演进的跨越。传统方案在面对全局图谱分析时极易暴露拓扑特征,而本方案通过双信道解耦与公共熵(public entropy,本文特指由区块链共识机制产生的、事先不可预测的未来区块哈希值 B_{hash},作为密码学协议的安全随机源)注入,不仅在物理层切断了通信连通性,还在密码学层面赋予了严格的前向安全性。

为了直观展示现有代表性研究在应对上述安全挑战时的局限性,以及本文 SECL-CCP 方案在协议完备性与抗分析能力上的突破,本文将各方案的核心特性进行了对比总结,如表 1 所示。

表 1　现有代表性隐蔽通信方案核心特性对比

Table 1　Comparison of core characteristics of existing representative covert communication schemes

方案类型	代表文献	核心机制	前向安全性	接收方不可抵赖	抗关联分析能力
数据载体型	[6]-[9],[11]-[13]	字段嵌入与载体伪装	不支持	不支持	差 (静态特征明显)
动态编码型	[14]-[16]	行为调制与动态跳变	不支持	不支持	中(信道高度耦合)
SECL-CCP	本文	信道解耦+密钥棘轮+ZKP	支持	支持	强 (动态合约工厂)

1　威胁模型与符号定义

1.1　威胁模型与安全假设

针对公开区块链环境下的隐蔽通信需求,本系统假设网络中存在一个全局被动监听者(global passive adversary, GPA)。具备以下能力与限制:第一,拥有全局网络视野,可解析所有公开链上数据;第二,掌握多维特征聚类与交易图谱拓扑分析技术,企图通过长期的时空关联性分析推断通信双方的真实物理身份;第三,在极端对抗场景下,允许 GPA 短暂攻破接收方的物理终端,并窃取当前内存中的主密钥与会话状态。假设 GPA 无法在多项式时间内攻破 AES 与 zk-SNARKs 等标准密码学原语。

1.2　安全目标

本协议旨在实现 3 大核心安全目标:

(1)严格前向安全性:在极端物理攻破下,保证历史通信密文无法被逆向推导解密,实现历史信息的零泄露。

(2)强抗关联性(不可链接性):切断交易图谱的时空关联连通性,使 GPA 的聚类分析失效。

(3)闭环状态安全与不可抵赖性:确保接收方无法抵赖已接收信息,且收发双方状态机严格同步。

1.3　核心符号说明

为了表述清晰并严格界定参数空间,本文协议涉及的核心符号及其物理意义约定如下:通信双方记为 Alice 与 Bob;$i, N \in \mathrm{N}^{+}$ 表示通信轮次;$K_{\text{sess}}^{(i)}$、$K_{\text{root}}^{(i)}$, $\in \{0,1\}^{256}$ 分别表示第 i 轮长度为 256 位的会话密钥与主密钥;$\mathcal{H}: \{0,1\}^{*} \rightarrow \{0,1\}^{256}$ 表示输出长度为 256 位的具有抗碰撞特性的哈希函数;$\|$ 表示比特串拼接操作;"STRING" 表示用于哈希域分离的字符串常量;$Nonce, B_{\text{hash}} \in \{0,1\}^{256}$ 分别表示 32 字节的本地高熵伪随机数与公共区块哈希(作为公共熵);Create2(0xff, $Addr, Salt, CodeHash$) 为以太坊标准确定性部署函数,其中 0xff 为固定前缀,

$Addr \in \{0,1\}^{160}$ 为 20 字节工厂地址，$Salt$ 为 32 字节动态盐值，$CodeHash \in \{0,1\}^{256}$ 为合约字节码哈希；密文 $C = \text{AES-256-GCM}_{\text{Enc}}(M,K)$ 中，M 为任意长度明文载荷，C 包含定长的认证标签。

2 自演进闭环隐蔽通信协议设计

2.1 协议整体流程概述

本协议的参与方为通信双方 Alice 和 Bob，其运行环境由链上智能合约与链下客户端软件共同构成。与传统方案不同，本协议的链上部分是动态按需生成的合约体系。整体架构如图 1 所示。

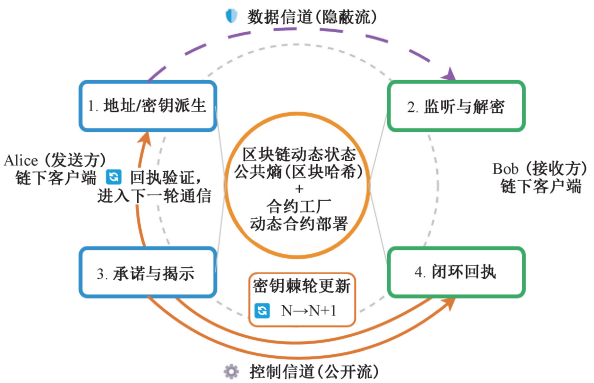

图 1 SECL-CCP 协议整体架构图

Figure 1 Overall architecture of the SECL-CCP protocol

链下客户端(Alice、Bob)负责密钥维护、加解密、地址计算及 ZKP 生成与验证。合约工厂为永久代理合约，利用 CREATE2 与确定性盐值部署一次性交互合约。动态合约含注册合约(Registry，单轮“承诺-揭示”后废弃)与验证合约(Verifier，用于公开验证 ZKP 回执)。链下数据信道将加密消息存入 IPFS 以最小化链上足迹，链上仅传递内容哈希并安全协商一次性密钥。

2.2 协议核心机制与详细工作流程

本协议设计了“双信道并行驱动”机制。此处的“双信道”并非指底层物理网络信道，而是指在智能合约层构建的逻辑信道：即负责秘密信息传输的“数据信道”与负责密钥协商更新的“控制信道”。两者在密码学上紧密绑定于同一个会话密钥[19]，但在链上表现为两条独立的交易路径。整体通信流程如图 2 所示：

在第 N 轮通信开始前，通信双方(Alice 与 Bob)均持有上一轮协商出的会话密钥 $K_{\text{sess}}^{(N-1)}$ 及主密钥 $K_{\text{root}}^{(N-1)}$。一次完整的通信包含以下 5 个核心阶段：

(1) 双信道地址确定性派生(本地计算阶段)：为了避免接收方全网扫描区块链，通信双方首先基于共享的会话密钥 $K_{\text{sess}}^{(N-1)}$，在本地并行计算出本轮

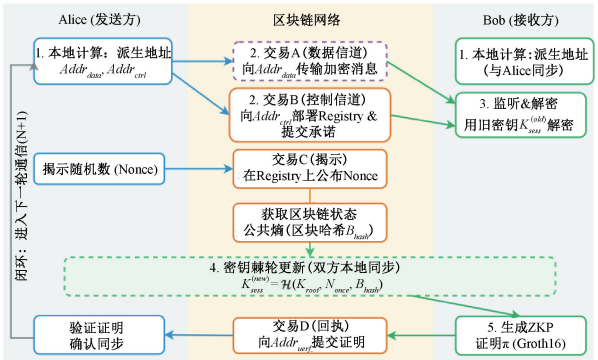

图 2 SECL-CCP 协议通信流程图

Figure 2 SECL-CCP protocol communication flowchart

通信的 2 个目标交互地址：

控制信道地址：控制地址基于以太坊 CREATE2 操作码的确定性算法预测，用于部署注册合约(Registry)，负责密钥协商。首先计算本轮盐值 $Salt_N$，再结合工厂地址与合约代码哈希生成部署地址。

$$Salt_N = \mathcal{H}(K_{\text{sess}}^{(N-1)} \,\|\, \text{"REGISTRY"}); \quad (1)$$

$$Addr_{\text{ctrl}} = \text{Create2}(0\text{xff}, Addr_{\text{Factory}}, Salt_N, \text{CodeHash}_{\text{Registry}})。 \quad (2)$$

数据信道地址用于投递加密载荷，负责数据传输。

$$Addr_{\text{data}} = \mathcal{H}(K_{\text{sess}}^{(N-1)} \,\|\, \text{"DATA"})。 \quad (3)$$

式(1)与式(3)中的 "REGISTRY" 与 "DATA" 字符串常量作为域分离标签，确保基于同一会话密钥派生出的控制信道盐值与数据信道地址相互独立。

(2) 并行隐蔽传输(发送方)：Alice 几乎同时向区块链网络广播两笔在表面上毫无关联的交易：

交易 A(隐蔽数据流与混合载荷分发)：大容量秘密信息易导致交易 Gas 与数据长度特征异常，从而被智能隐写分析模型识别，因此本协议设计了基于特征规避的混合载荷分发策略。Alice 首先采用 AES-256-GCM 算法对秘密消息 M 进行加密：

$$C = \text{AES-256-GCM}_{\text{Enc}}(M, K_{\text{sess}}^{(N-1)})。 \quad (4)$$

随后，协议根据密文规模执行差异化路由：当密文较小(如 $|C| \leqslant 1$ KB)时，直接将其作为普通转账的备注信息写入 Input Data 字段，以降低外部依赖；当传输大容量载荷时，协议将其切片并上传至链下 IPFS 网络，仅将 46 字节内容标识符(CID)作为载荷写入 Input Data。

交易 B(控制流)：Alice 调用工厂合约，在 $Addr_{\text{ctrl}}$ 上动态部署一次性的 Registry 合约，并立即执行“承诺-揭示(commit-reveal)”操作，将利用随机数 $Nonce$ 生成的“承诺值” $Comm$ 和目标区块高度 H_{target} 上链：

$$Comm = \mathcal{H}(Nonce \| K_{root}^{(N-1)})。 \quad (5)$$

抗关联性:对于外部观察者,交易 A 是一笔普通的转账,交易 B 是一次合约部署,两者地址不同、交互对象不同,无法建立关联。

(3)定向监听与即时解密(接收方):接收方 Bob 在本地定向监听预计算出的 $Addr_{data}$ 和 $Addr_{ctrl}$:

捕获数据:一旦 $Addr_{data}$ 上出现交易,Bob 立即提取密文 C。此时,他直接使用手中的会话密钥 $K_{sess}^{(N-1)}$ 对 C 进行解密,获取明文消息 M。

捕获参数:同时,Bob 监听 $Addr_{ctrl}$ 上的 Registry 合约,等待 Alice 完成揭示操作以获取 *Nonce* 和作为公共熵的目标高度区块哈希 B_{hash}。

(4)密钥棘轮演进(状态更新阶段):成功获取链上参数后,双方各自在本地执行密钥更新算法[19]:

会话密钥更新:结合旧主密钥、*Nonce* 和区块哈希,生成下一轮会话密钥 $K_{sess}^{(N)}$。

$$K_{sess}^{(N)} = \mathcal{H}(K_{root}^{(N-1)} \| Nonce \| B_{hash})。 \quad (6)$$

主密钥滚动:利用新会话密钥对旧主密钥进行单向哈希迭代,生成新主密钥 $K_{root}^{(N)}$,并立即销毁旧主密钥 $K_{root}^{(N-1)}$ 及旧会话密钥 $K_{sess}^{(N-1)}$。

$$K_{root}^{(N)} = \mathcal{H}(K_{root}^{(N-1)} \| K_{sess}^{(N)})。 \quad (7)$$

(5)零知识闭环确认(回执阶段):为了通知 Alice 通信成功并证明状态已同步,Bob 利用新生成的密钥 $K_{sess}^{(N)}$ 派生出验证合约(Verifier)的地址 $Addr_{verf}^{(N)}$。Bob 部署该合约并提交一个 zk-SNARK 证明。Alice 验证该证明有效后,确认闭环完成,双方准备进入第 $N+1$ 轮通信。

2.3 动态密钥协商与棘轮演进

针对隐蔽通信中密钥如何安全协商与更新的核心问题,本协议借鉴 Signal 协议的双棘轮算法[19](double ratchet)思想,设计了一套“公共熵注入”的动态密钥协商方案。整个协商机制分为“初始预共享”与“动态棘轮演进”两个阶段:在第 0 轮通信前,发送方利用接收方经带外信道预分发的 RSA 公钥,加密传输随机生成的初始主密钥 $K_{root}^{(0)}$,接收方解密后双方达成初始状态同步,完成初始主密钥 $K_{root}^{(0)}$ 的协商;在随后第 N 轮($N \geq 1$)通信中,发送方提取未来不可预测的区块哈希 $B_{hash}^{(N)}$ 作为公共熵[2],与本地私有随机数共同输入密钥派生函数,协商出本轮的会话密钥 $K_{sess}^{(N)}$。该机制确保了即使当前节点被攻破,历史协商的会话密钥也无法被逆向推导,整体演进流程如图 3 所示。

每一次通信,双方都需要协商出一个全新的、一次性的会话密钥 $K_{sess}^{(i)}$。为此,采用了基于哈希的“承诺-揭示”方案,并将区块链的未来状态作为公共熵源注入密钥生成过程。协商方案分为以下两步:

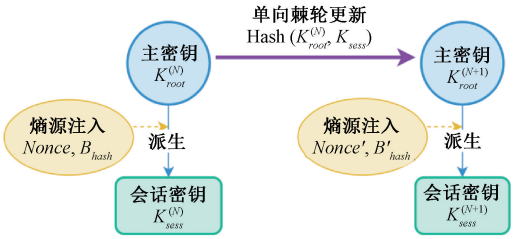

图 3 密钥棘轮演进图

Figure 3 Key ratchet evolution diagram

步骤 1(承诺阶段):发送方 Alice 使用随机数生成器生成一个 32 字节的随机数 *Nonce*,并计算承诺哈希 $Comm = \mathcal{H}(Nonce \| K_{root}^{(N-1)})$。随后,Alice 调用动态部署的 Registry 合约的 Commit()函数将 *Comm* 和一个选定的未来的目标区块高度 H_{target} 发送上链。此时 *Nonce* 被密码学锁定。

步骤 2(揭示与公共熵提取):Alice 和 Bob 监听区块链,当区块链高度到达 H_{target} 后,该区块的哈希 B_{hash} 成为一个公开、不可预知的随机源。Alice 随后调用合约揭示明文 *Nonce*。接收方 Bob 验证 *Comm* 一致后,提取 B_{hash} 作为本轮协商的公共熵。

获取上述链上参数后,双方在本地同步完成最终的密钥协商与演进:

步骤 3(派生会话密钥):双方结合各自持有的旧主密钥、揭示的 *Nonce* 以及不可预测的 B_{hash},计算出第 N 轮的会话密钥用于加解密:

$$K_{sess}^{(N)} = (K_{root}^{(N-1)} \| Nonce \| B_{hash})。 \quad (8)$$

步骤 4(主密钥不可逆更新):协商完成后,立即驱动主密钥进行滚动更新,新的会话密钥 $K_{sess}^{(i)}$ 作为熵源被注入主密钥的更新函数中,并从内存中物理销毁旧密钥,以实现前向安全:

$$K_{root}^{(N)} = \mathcal{H}(K_{root}^{(N-1)} \| K_{sess}^{(N)})。 \quad (9)$$

2.4 动态合约工厂

为解决存在固定交互指纹的问题,设计了“动态合约工厂”模型。该模型利用 CREATE2 操作码[20]的地址确定性预测能力。CREATE2 允许新合约的地址在部署前被精确计算出来,其公式为:$Address = \text{Create2}(0xff, Addr_{Factory}, Salt, CodeHash)$。该模型巧妙地利用了这一点,将地址的派生与密钥棘轮机制绑定。整体流程如图 4 所示:

地址派生:第 N 轮通信开始时,双方使用当前会话密钥 $K_{sess}^{(N-1)}$ 作为核心熵源,计算出本轮通信所需 Registry 合约盐值与预测地址 $Addr_{regi}^{(N)}$:

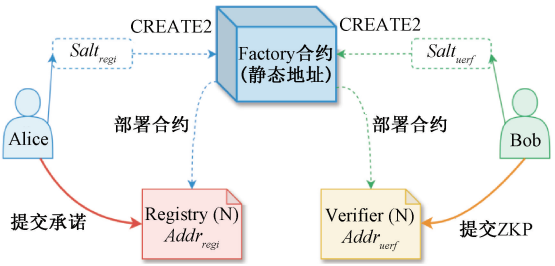

图 4　动态合约工厂流程图

Figure 4　Dynamic contract factory flowchart

$$Salt_N = \mathcal{H}(K_{\text{sess}}^{(N-1)} \| \text{"REGISTRY"})。\quad (10)$$

$$Addr_{\text{regi}}^{(N)} = \text{Create2}(0\text{xff}, Addr_{\text{Factory}}, Salt_{\text{regi}}, CodeHash_{\text{Registry}})。\quad (11)$$

发送方首先检查该地址上是否存在已部署的 Registry 合约:若不存在,则调用永久的 Factory 合约,传入 $Salt_N$ 进行部署;若已存在,则直接连接。

用完即弃:该部署在预测地址上的 Registry 合约,其生命周期仅限于第 N 轮通信。

为了确保回执阶段同样具备抗关联性,验证合约遵循相同的动态演进逻辑,接收方在生成 ZKP 回执前,使用新协商出的会话密钥计算验证合约的盐值 $Salt_{\text{verf}}$ 及地址 $Addr_{\text{verf}}^{(N)}$,随后调用工厂合约在 $Addr_{\text{verf}}^{(N)}$ 部署一次性的 Verifier 实例,并提交证明:

$$Salt_{\text{verf}} = \mathcal{H}(K_{\text{sess}}^{(N)} \| \text{"VERIFIER"});\quad (12)$$

$$Addr_{\text{verf}}^{(N)} = \text{Create2}(0\text{xff}, Addr_{\text{Factory}}, Salt_{\text{verf}}, CodeHash_{\text{Verifier}})。\quad (13)$$

对于外部观察者而言,链上的活动表现为一系列分散的、无规律的、由一个通用工厂创建的、生命周期极短的合约,这极大地增加了进行交易关联分析的难度,实现了高层次的抗关联分析能力。

2.5　零知识回执

为解决协议流程不完备的问题,并为整个动态演进系统提供必要的同步保障,本文引入了零知识证明(zero-knowledge proof)[21]技术实现了协议的状态一致性证明。在动态演进系统中,任何计算偏差引发的密钥或地址脱节均会导致后续通信永久失败,而零知识回执正是这一难题的解法。

为此,接收方 Bob 需在链上提交 ZKP 回执,以证明其已掌握与公开承诺值相匹配的秘密消息。这个证明同时达成了两个至关重要的目标:

1) 协议完备性与不可抵赖性:它证明了 Bob 已经成功接收并正确解密了消息,解决了接收方困境,形成了通信的闭环。

2) 状态同步确认:Bob 能够正确解密消息的前提是,他必须已经使用与 Alice 完全相同的旧密钥 $K_{\text{root}}^{(N-1)}$ 和链上数据,计算出了完全相同的本轮会话密钥 $K_{\text{sess}}^{(N)}$。因此,这个证明也间接地证实了 Bob 已经具备了计算下一轮主密钥和下一轮合约地址的所有正确前提。这避免了因状态不同步而导致发送方将消息发送到错误的地址的可能。

2.6　安全性证明与分析

本节针对 1.1 节与 1.2 节定义的威胁模型与安全目标,从理论证明与定性分析维度对 SECL-CCP 协议的安全性进行评估。本节将首先在随机预言机模型(ROM)下对前向安全性进行正规化的安全性证明;随后对协议在抗关联性与闭环状态安全性方面的防御能力进行逻辑分析。

(1) 前向安全性证明:

定理 1(前向安全性):在随机预言机模型下,若协议底层的单向散列函数$\mathcal{H}$满足抗原像攻击特性,则 SECL-CCP 协议的密钥棘轮机制具有计算上的前向安全性。

证明:假设存在一个多项式时间内的攻击方 A,能够在获取第 N 轮主密钥 $K_{\text{root}}^{(N)}$ 与会话密钥 $K_{\text{sess}}^{(N)}$ 的前提下,以不可忽略的优势破译历史轮次 $N-1$ 的主密钥 $K_{\text{root}}^{(N-1)}$。构建规约游戏如下:

Game 0:真实的攻击游戏,攻击方 A 窃取了当前轮次的密钥状态,试图回溯推导 $K_{\text{root}}^{(N-1)}$。

Game 1:与 Game 0 相同,但在本游戏中,将协议中使用的单向散列函数$\mathcal{H}$模拟为一个理想的随机预言机。根据协议的演进规则,主密钥更新逻辑为 $K_{\text{root}}^{(N)} = \mathcal{H}(K_{\text{root}}^{(N-1)} \| K_{\text{sess}}^{(N)})$。

分析:由于随机预言机$\mathcal{H}$对未知输入的响应是独立且均匀分布的,攻击方 A 从已知输出 $K_{\text{root}}^{(N)}$ 逆推未知输入 $K_{\text{root}}^{(N-1)}$,等价于对随机预言机进行原像求逆。根据抗原像假设,任何多项式时间攻击方对随机预言机求逆成功的概率优势 $Adv_A^{Inv}(\lambda)$ 是可忽略的。

因此,攻击方 A 攻破本方案前向安全的概率优势 $\text{Adv}_A^{\text{FS}}(\lambda) \leqslant \text{Adv}_A^{\text{Inv}}(\lambda) \leqslant \text{negl}(\lambda)$(其中,$\text{Adv}_A^{\text{FS}}(\lambda)$ 表示敌手 A 在安全参数 λ 下攻破协议前向安全性的概率优势;$\text{Adv}_A^{\text{Inv}}(\lambda)$ 表示敌手 A 成功对随机预言机进行原像求逆的概率优势;$\text{negl}(\lambda)$ 表示随安全参数 λ 变化的可忽略函数(negligible function))。即便当前主密钥泄露,其历史隐蔽通信记录在计算上依然是安全的,定理 1 得证。

(2) 抗关联性证明:本协议采用双信道解耦与动态合约工厂。数据信道伪装为普通转账,控制信道通过不可预测的盐值动态部署用完即弃的合约。对于 GPA 而言,每次通信的链上目标地址均呈现伪随机跳变,从物理层面切断了寻址路径与拓扑连通

分量,在逻辑上有效抵御了交易图谱聚类分析。

(3) 闭环状态安全证明:通过要求接收方提交 zk-SNARKs 零知识证明回执,协议通过“不证明即断连”的强约束,实现了 100% 的闭环确认成功率。该证明在不泄露明文秘密的前提下,利用算术电路确保了接收方完成密钥的派生与状态更新,在协议层防止了恶意抵赖并保障了双端状态机的安全同步。

3 实验评估与分析

为了验证 SECL-CCP 协议在真实区块链环境中的性能与安全性,并量化其相对于现有方案的优势,本文基于以太坊 Sepolia 测试网及 Hardhat 本地仿真环境进行实验。实验重点关注抗智能隐写分析、前向安全保障以及安全性与效率平衡三个维度的表现。

3.1 实验设置与数据集

仿真实验在配置 Intel Xeon Gold 6248R CPU 及 64 GB 内存的服务器上进行。链下客户端采用 Python 编写,利用 pycryptodome 库实现 AES-256-GCM 对称加密算法,链上合约使用 Solidity v0.8.19,并利用 Hardhat 框架进行合约的编译、本地仿真与测试网部署。编译时启用了底层代码优化器(Optimizer enabled,设置 runs = 200)以获取最接近真实主网的 Gas 开销估算。零知识证明电路基于 Circom 构建。为了模拟真实的对抗环境,实验利用 Google BigQuery 从以太坊主网采集了 50,000 条真实交易数据作为背景流量。为保证数据均衡,本研究从中随机抽取 10,000 条普通转账交易作为负样本,并利用本协议客户端脚本生成 10,000 条隐蔽交易作为正样本,构建了 20,000 条的混合数据集。在数据预处理阶段,系统主动剔除了 Chain ID、Gas Price 等网络环境标识特征以消除主网与测试网的异构偏差。正负样本按 7:3的比例划分为训练集与测试集进行模型评估。本文对核心分类器的超参数进行了固定配置:随机森林模型设置决策树数量为 100,最大树深限制为 15,以防止模型过拟合;长短期记忆网络(LSTM)采用双层循环结构,每层隐含层节点数设为 64,选用 Adam 优化器,初始学习率设为 0.001,批处理大小为 64,且迭代训练总轮次设为 50。对比方案包括:方案 S (storage-based)[6],代表传统存储嵌入型方案;方案 D (dynamic-label)[14],代表改进的动态编码方案。

3.2 抗智能隐写分析能力评估

为证明协议在高对抗环境下的隐蔽性,相较于其他领域利用深度神经网络进行复杂特征提取与识别的常规方法[22],本实验针对区块链交易特性,构建了一个包含 Gas Limit 分布、Input Data 字节频率等 14 个维度的特征集,并使用随机森林和长短期记忆网络(LSTM)两种模型试图区分“隐蔽通信交易”与“正常背景交易”。实验结果如表 2 所示:

表 2 不同方案在智能隐写分析下的检测准确率对比

Table 2 Comparison of detection accuracy of different schemes under intelligent steganalysis

方案类型	随机森林检测率	LSTM 网络检测率
方案 S[6]	89.4%	92.1%
方案 D[14]	63.2%	58.7%
SECL-CCP	12.8%	11.5%

实验结果显示,方案 S 由于在地址生成上存在非自然统计规律,检测率高达 89%以上。方案 D 虽引入了动态性,但其标签生成算法仍存在可被 LSTM 捕捉的模式。而 SECL-CCP 的检测率(约 12%)极度接近正常流量的误报率。这是因为“动态合约工厂”机制,每次通信都表现为一次独立的合约部署行为,在特征空间上与常见的 DeFi 合约交互高度混淆,实现了对抗智能隐写分析的目标。

3.3 前向安全性量化

前向安全性是衡量协议在长期运行中生存能力的关键指标。实验模拟了通信进行到第 100 轮时,攻击者获得当前主密钥的极端场景,并对比了不同方案的历史信息泄露率。实验结果如图 5 所示:

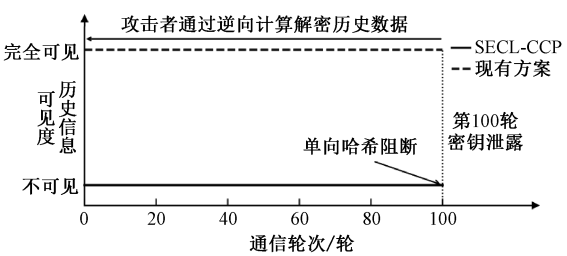

图 5 密钥泄露后的历史信息可恢复性分析

Figure 5 Recoverability analysis of historical information after key leakage

结果表明,静态或弱动态方案(方案 S & D)一旦密钥泄露,攻击者可推导过去所有轮次的密钥,导致系统崩溃。而 SECL-CCP 得益于单向密钥棘轮机制,即使当前密钥暴露,攻击者也无法利用哈希函数的抗原像性反推历史密钥,实现了 0% 的历史信息泄露率,具备极强的自愈能力。

3.4 安全性与效率的权衡分析

引入零知识证明和动态合约必然带来额外的计算开销。为了量化系统的工程可用性,本文从计算开销、通信时延与经济成本三个维度进行了性能测

试,并与近两年的权威区块链隐蔽通信方案进行了系统性对比。最新的混淆寻址隐蔽通信方案[16]虽通过链下预共享与动态地址生成增强了隐蔽性,但其底层仍依赖静态密钥且局限于单向投递,面临密钥泄露无前向安全保障、无回执易遭恶意抵赖等缺陷。相比之下,SECL-CCP 协议于选用了对零知识证明极其友好的 Poseidon 哈希算法[23],客户端在本地生成单次 Groth16 证明[24]的计算耗时仅约 215 ms,链上验证的算术约束被压缩至 1 420 个。如表 3 所示,虽然本协议单次链上逻辑执行消耗约 35 万 Gas,但通过兼容 Arbitrum 等 Layer 2 扩容机制(如图 6 所示),单次闭环通信的端到端确认时延被压缩至 1 秒以内,成本也极大降低。

表 3　成本与安全效用对比

Table 3　Comparison of cost and security utility

方案类型	平均 Gas 开销	前向安全性	接收方不可抵赖	抗关联分析能力
传统存储型方案[6]	低(~2.1w)	不支持	不支持	差(静态特征明显)
最新动态标签方案[14]	中(~12w)	不支持	不支持	中(信道耦合性强)
混淆寻址方案[16]	中高(~18w)	不支持	不支持	较强(多地址混淆)
SECL-CCP	高 (~35w)	支持	支持	强(动态合约工厂)

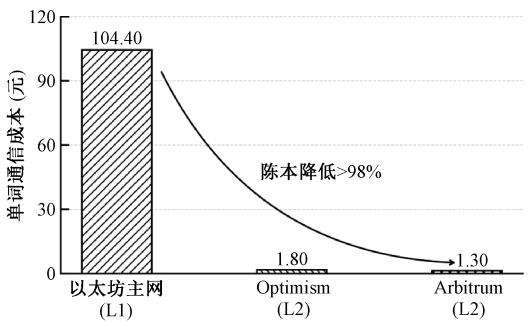

图 6　SECL-CCP 在不同网络环境下单次通信成本对比

Figure 6　Comparison of SECL-CCP single communication costs under different network environments

评估显示,在 Arbitrum One 网络上运行一次完整闭环的成本约为 Layer 1 的 1/50 至 1/100,低至约 1.30 元。这意味着迁移至 Layer 2 后,协议完全能够满足高频、低成本的隐蔽通信需求。

4　结论

针对现有区块链隐蔽通信协议在抗关联分析、长期安全性及流程完备性方面的不足,本文设计并实现了一种自演进的闭环区块链隐蔽通信协议,主要创新如下:

(1) 集成动态密钥棘轮机制,结合“承诺-揭示”方案与区块公共熵,驱动主密钥单向不可逆滚动更新,实现前向安全性。

(2) 提出动态合约工厂模型,利用 CREATE2 操作码为每轮通信动态部署用完即弃的交互合约,消除了固定的链上指纹,阻断了基于全局交易图谱的拓扑关联分析。

(3) 引入零知识证明接收回执,构建了完备的通信闭环,消除了单向投递时接收方恶意抵赖的风险。

未来工作将重点探索本协议向多方群组隐蔽通信场景的演进。

参考文献:

[1] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. (2009-03-01)[2022-06-13]. http://bitcoin.org/bitcoin.pdf.

[2] WOOD G. Ethereum: A secure decentralised generalised transaction ledger[EB/OL]. (2014-04-01)[2025-12-25]. https://ethereum.github.io/yellowpaper/paper.pdf.

[3] Yang Qinglin, Zhao Yetong, Huang Huawei, HUANG H W, et al. Fusing blockchain and ai with metaverse: a survey[J]. IEEE Open Journal of the Computer Society, 2022, 3: 122-136.

[4] Wang Jie, Ge Lina, Zhang Guifen. Improvement scheme for the proof of stake consensus of blockchain incentive mechanism[J]. Journal of Zhengzhou University (Engineering Science), 2023, 44(5): 62-68. [王捷, 葛丽娜, 张桂芬. 区块链的激励机制权益证明共识算法改进方案[J]. 郑州大学学报(工学版), 2023, 44(5): 62-68.]

[5] Zhang Tao, Li Bingyu, Zhu Yan, et al. Covert channels in blockchain and blockchain based covert communication: overview, state-of-the-art, and future directions [J]. Computer Communications, 2023, 205: 136-146.

[6] Partala J. Provably Secure Covert Communication on blockchain[J]. Cryptography, 2018, 2(3): 18.

[7] Tian Yang, Liao Xin, Dong Li, et al. Amount-based covert communication over blockchain[J]. IEEE Transactions on Network and Service Management, 2024, 21(3): 3095-3111.

[8] Xiong Lizhi, Zhu Rong, Fu Zhangjie. Covert communication method of blockchain network based on transaction construction and forwarding mechanism[J]. Journal on Communications, 2022, 43(8): 176-187. [熊礼治, 朱蓉, 付章杰. 基于交易构造和转发机制的区块链网络隐蔽通信方法[J]. 通信学报, 2022, 43(8): 176-187.]

[9] Frkat D, Annessi R, Zseby T. Chainchannels: private botnet communication over public blockchains[C]//Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Piscataway: IEEE, 2018: 1244-1252.

[10] Chen Zhuo, Zhu Liehuang, Jiang Peng, et al. Blockchain meets covert communication: a survey[J]. IEEE Communications Surveys & Tutorials, 2022, 24(4): 2163-2192.

[11] She Wei, Rong Xinpeng, Liu Wei, et al. Generative blockchain-based covert communication model based on markov chain[J]. Journal on Communications, 2022, 43(10): 121-132. [佘维, 荣欣鹏, 刘炜, 等. 基于马尔可夫链的生成式区块链隐蔽通信模型[J]. 通信学报, 2022, 43(10): 121-132.]

[12] She Wei, Huo Lijuan, Liu Wei, et al. A blockchain-based covert communication model for hiding sensitive documents and sender identity[J]. Acta Electronica Sinica, 2022,50(04): 1002-1013. [佘维, 霍丽娟, 刘炜, 等. 一种可隐藏敏感文档和发送者身份的区块链隐蔽通信模型[J]. 电子学报, 2022,50(4): 1002-1013.]

[13] Liu Yuanni, Fan Fei, Zhao Yuyang, et al. A convert communication scheme of blockchain based on image multilevel steganography embedding[J]. Journal of Electronics & Information Technology, 2025, 47(04): 1126-1139. [刘媛妮, 范飞, 赵宇洋, 等. 基于图像多重隐写的区块链隐蔽通信方案[J]. 电子与信息学报, 2025, 47(4): 1126-1139.]

[14] Zhang Can, Zhu Liehuang, Xu Chang, et al. EBDL: effective blockchain-based covert storage channel with dynamic labels[J]. Journal of Network and Computer Applications, 2023, 210: 103541.

[15] She Wei, Ma Jiawei, Zhang Shuhui, et al. Covert communication model based on dynamic time binary trees [J]. Journal on Communications, 2025, 46(2): 147-165. [佘维, 马佳伟, 张淑慧, 等. 基于动态时间型二叉树的隐蔽通信模型[J]. 通信学报, 2025, 46(2): 147-165.]

[16] Zhang Lejun, Zhang Bo, Guo Ran, et al. A blockchain-oriented covert communication technology with controlled security level based on addressing confusion ciphertext [J]. Frontiers of Computer Science, 2024, 19(2): 192807-192807.

[17] Qin Jiaohua, Qing Dashan, Xiang Xuyu, et al. A coverless information steganographic method based on blockchain information mapping[J]. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2024, 52(11): 58-63. [秦姣华, 卿大山, 向旭宇, 等. 一种基于区块链信息映射的无载体隐写方法[J]. 华中科技大学学报(自然科学版), 2024, 52(11): 58-63.]

[18] Yuan Xiangbo, Jiang Peng, Chen Zhuo, CHEN Z, et al. Blockchain-based group covert communication for IoT network[J]. IEEE Internet of Things Journal, 2025, 12(13): 25633-25650.

[19] Cohn-Gordon K, Cremers C, Dowling B, et al. A formal security analysis of the signal messaging protocol[J]. Journal of Cryptology, 2020, 33(4): 1-70.

[20] Qian Peng, Liu Zhenguang, He Qinming, et al. Smart contract vulnerability detection technique: a survey[J]. Journal of Software, 2022, 33(08): 3059-3085. 钱鹏, 刘振广, 何钦铭, 等. 智能合约安全漏洞检测技术研究综述[J]. 软件学报, 2022, 33(08): 3059-3085.]

[21] Goldwasser S, Micali S, RACKOFF C. The knowledge complexity of interactive proof systems[J]. SIAM Journal on Computing, 2006, 18(1): 186-208.

[22] Li Zhixin, Shang Fanqi, Huan Zhan, et al. Human Activity Recognition Based on Hybrid Feature Graph Convolutional Neural Network[J]. Journal of Zhengzhou University (Engineering Science), 2024, 45(04): 46-52. [李志新, 商樊淇, 郇战, 等. 基于混合特征图卷积神经网络的人体行为识别方法[J]. 郑州大学学报(工学版), 2024, 45(4): 46-52.]

[23] Liu Changxu, Zhou Hao, Yang Lan, et al. AcclMT: a highly resource-efficient and flexible poseidon hash-based merkle tree architecture[C]//Proceedings of the 62nd ACM/IEEE Design Automation Conference (DAC). Piscataway: IEEE, 2025: 1-7.

[24] Groth Jens. On the size of pairing-based non-interactive arguments[C]//Advances in cryptology - EUROCRYPT 2016. Berlin: Springer, 2016: 305-326.

Anti-Correlation Two-party Blockchain Covert Communication Method Based on Dual-Channel Dynamic Evolution

ZAI Guangjun, DONG Yannan, WANG Yipeng, XU Zhenyu, SHE Wei

(School of Cyber Science and Engineering, Zhengzhou University, Zhengzhou 450001, China)

Abstract: To address the core problems of lacking forward secrecy, weak anti-correlation analysis capabilities, and incomplete communication processes universally existing in current blockchain covert communication schemes, a self-evolving closed-loop covert communication protocol (SECL-CCP) was proposed. Through three innovative mechanisms, a security architecture capable of dynamic evolution across keys, protocol processes, and on-chain infrastructure was constructed. First, a "key ratchet" mechanism was designed, wherein the "commit-reveal" scheme was combined with the public entropy of blockchain future states, irreversible key updates were realized, and forward secrecy was endowed to the protocol. Secondly, a "dynamic contract factory" model was proposed, and the CREATE2 opcode was utilized to dynamically deploy disposable interactive contracts for each communication round, whereby fixed on-chain fingerprints were eliminated. Finally, a receipt mechanism based on zero-knowledge proof was introduced to build a verifiable communication closed loop, and the receiver non-repudiation problem was resolved. Simulation experiments were conducted based on the Ethereum Sepolia testnet and Hardhat environment, and a mixed dataset containing 20,000 samples was constructed by collecting real mainnet traffic. It was demonstrated by the results that the steganalysis detection rates under random forest and LSTM models were respectively reduced to 12.8% and 11.5%, zero leakage of historical information under key compromise scenarios was achieved, and intelligent correlation analysis attacks were effectively resisted.

Keywords: covert communication; blockchain; zero-knowledge proof; forward secrecy; anti-correlation analysis.