

DOI: 10.3969/j.issn.1671-0673. 2026. 04. 006

一种基于比特币的“一对多”隐蔽通信方法

阮俊鸿, 于 刚, 王永娟, 王 伟, 陆思奇

(信息工程大学, 河南 郑州 450001)

摘要: 针对当前基于加密货币系统的隐蔽通信研究多局限在“一对一”场景且依赖预共享密钥的问题, 通过引入公钥广播加密思想, 提出一种基于比特币的“一对多”隐蔽通信方法。将密文和携带密文加密密钥的广播加密信息序列分别伪装嵌入至比特币特殊交易的输出金额和输出地址中, 无需发送多条消息副本, 即可在指定群组内实现精准的“一对多”隐蔽信息广播, 并允许在系统建立后为每次通信指定不同的接收方。通过解密正确性来识别包含隐蔽信息的特殊交易, 可抵抗内部恶意行为者的信息获取。在比特币测试网上进行了方案验证, 结果表明, 该方法能在无需提前协商会话密钥的情况下, 在不同接收方间实现隐蔽信息广播。

关键词: 区块链; 比特币; 隐蔽信道; 广播加密; 交易过滤

中图分类号: TP393

文献标识码: A

文章编号: 1671-0673(2026)04-0422-08

A Bitcoin-Based One-to-Many Covert Communication Method

RUAN Junhong, YU Gang, WANG Yongjuan, WANG Wei, LU Siqi

(Information Engineering University, Zhengzhou 450001, China)

Abstract: Aiming at the problem that existing covert communication studies based on cryptocurrency systems are restricted to the one-to-one scenario and rely on pre-shared keys, a one-to-many covert communication method based on Bitcoin is proposed by introducing the concept of public-key broadcast encryption. The ciphertext and the broadcast encryption information sequence carrying the ciphertext encryption key are respectively disguised and embedded into the output amounts and output addresses of special Bitcoin transactions. Without sending multiple message copies, precise one-to-many covert information broadcasting within a specified group is achieved, and different receivers can be designated for each communication after system initialization. Special transactions containing covert information are identified by decryption correctness, which can prevent information access by internal malicious entities. The proposed scheme is verified on the Bitcoin testnet. The results demonstrate that the method can realize covert information broadcasting among different receivers without pre-negotiated session keys.

Key words: blockchain; Bitcoin; covert channel; broadcast encryption; transaction filtering

隐蔽通信是指在公共通信环境中利用隐蔽信道进行通信的一种方式, 旨在通过隐蔽的方式传输数据。隐蔽通信的存在, 使第三方难以察觉通信行为的发生。自 2008 年中本聪提出比特币这一著名的加密货币系统后, 基于区块链的隐蔽通信

方法便陆续被提出。

2015 年, 文献[1]通过操纵金额字段, 将信息嵌入到比特币交易中。此后, CCBTC^[2]、Tithonus^[3]、HMAC/HASH-based MBE^[4]、V-BLOCCE^[5]等利用区块链中金额、地址、OP_RETURN 字段等多种数据

收稿日期: 2026-01-29; 修回日期: 2026-03-22

基金项目: 国家重点研发计划(2023YFB2705000)

作者简介: 阮俊鸿(1994—), 男, 工程师, 硕士生, 主要研究方向为区块链、网络通信。E-mail: rjh2026xxgcdx@163.com

结构进行隐蔽通信的方法相继被提出。随着现代密码学的发展,研究人员发现,除传统的编码置换和类隐写术外,利用 DSA (Digital Signature Algorithm)、RSA (Rivest-Shamir-Adleman)、ECDSA (Elliptic Curve Digital Signature Algorithm) 等非对称密码体制中的潜信道,也可以在区块链上实施隐蔽通信,且效果良好,典型的有 Skywhisper^[6]、Chain-Channels^[7]、RDSAC/DDSAC^[8]等。

尽管嵌入手法较为丰富,但承载隐蔽信息的载体(一般是交易)的过滤方式却相对单一,多数采用基于对称加密思想的特征模式。隐蔽通信接收方通过事先约定的规则、预共享的密钥,尝试从一笔或多笔交易中寻找一个指定的特征,如果寻到,说明涉及的交易携带隐蔽信息。这种特征一般是一段序列或是预共享密钥参与下的计算符合性。这意味着,一旦这种模式泄露,任何人都可以通过解析这种模式确切地判断出隐蔽通信的存在,即使其可能暂时还无法获悉隐蔽消息的内容。

此外,由于一般需要对隐蔽信息进行加密,这些方法建立起的隐蔽信道大多是“一对一”的,隐蔽通信只能发生在持有共同加密密钥的双方之间,面向持有不同密钥的接收方,实现“一对多”隐蔽通信的研究目前还比较少。文献[9]通过发送相同消息的不同加密副本给出了一种解决思路。但显然,这种通信方式运用在比特币网络上将导致巨大的开销。

文献[10-11]提出分组的方法,利用不同的预共享密钥来对隐蔽通信接收方进行分组,持有相同密钥的成员可互相群发消息。这种通过扩大会话密钥的持有范围来增加接收方数量的设计,本质上是“一对一”隐蔽通信方案的一种延伸。除非与潜在的不同分组间提前共享多个会话密钥,否则隐蔽通信发送方无法临时调整通信的接收方,难以将特定接收方排除在某次通信之外。为了精细分组,其需要预共享的密钥数量呈亚指数甚至指数级增长,将给接收方带来不可忽视的计算成本。

文献[6,12]将携带隐蔽信息的交易过滤方法与“一对多”隐蔽通信分开考虑,先利用类似分组的思想,将潜在接收方与系统外观察者区分开,然后再利用属性基加密、广播加密等方法对潜在接收方进行更细致的管理,达到类似“一对多”隐蔽通信的效果。由于其在特殊交易的过滤上仍然采用了基于对称加密思想的特征模式,系统内的用户都可以识别出携带隐蔽信息的交易,无法实现非目标通信用户对通信的无感,难以抵抗内部恶意

行为者对隐蔽通信的信息获取,在整体设计上更类似文献[13]使用的访问控制方法。

本文在现有研究的基础上,提出一种基于比特币的“一对多”隐蔽通信方法。主要工作如下。

1) 通过将基于交易结构的隐蔽通信方法与公钥广播加密相结合,提出了一种基于比特币的“一对多”隐蔽通信方法,支持向持有不同密钥的接收方进行精准广播。

2) 设计了一种基于比特币的隐蔽信息嵌入和过滤方法,通过密码学计算来确定一笔交易是否携带隐蔽信息,可抵抗内部恶意行为者的信息获取,允许在一笔交易中完成交易特殊性的验证。

3) 形成了一类群组隐蔽通信方案的基础组件,允许在“一对多”通信过程中临时指定不同的接收方,无需提前分组,且任意一个系统参与者都可发起组内通信。

1 基础知识

1.1 公钥广播加密

文献[14]提出了一种具备常数级密文长度(两个群元素大小)的无状态公钥广播加密方法(简称 BGW1),具体如下。

设 n 为 BGW1 广播加密系统的用户数量, G 为阶为素数 p 的双线性群, G_1 为其对应的能够高效进行双线性映射 $e: G \times G \rightarrow G_1$ 运算的循环群, Z_p 为阶为素数 p 的循环群。系统提供 3 个算法。算法 1 用于生成系统公钥和各个用户的私钥。

算法 1 BGW1 公私钥生成

输入: 系统用户数量 n

输出: 系统公钥 R_{PK} , 各个用户的广播私钥 d_i , 其中, $i \in \{1, \dots, n\}$

1. 随机选择生成元 $g \in G$, 随机数 $\alpha, \gamma \in Z_p$

2. $R_{PK} = (g, g_1, \dots, g_n, g_{n+2}, g_{2n}, v) \in G^{2n+1}$, 其中, $v = g^\gamma \in G$, 对于 $i \in (1, 2, \dots, n, n+2, \dots, 2n)$, $g_i = g^{(\alpha^i)}$

3. 计算各用户的广播私钥 $d_i = g_i^{-\gamma} \in G$, 其中 $i \in (1, \dots, n)$

可以发现, $d_i = v^{(\alpha^i)}$ 。此外, $g_{n+1} = g^{(\alpha^{n+1})}$ 保密, 不作为系统公钥公开。

算法 2 用于生成公开传输的广播头, 以在指定的通信接收方之间秘密协商会话密钥。

算法 2 广播头生成

输入: 通信接收方集合 S , 系统公钥 R_{PK}

输出: 广播头 R_{Hdr}

1. 随机选择 $t \in Z_p$

2. 计算会话密钥 $K = e(g_{n+1}, g)^t \in G_1$ 。其中, $e(g_{n+1}, g) =$

$e(g_n, g_1)$

$$3. \text{ 计算广播头 } R_{\text{Hdr}} = \left(g^t, \left(v \cdot \prod_{j \in S} g_{n+1-j} \right)^t \right) \in G^2$$

算法3用于从广播头中提取会话密钥。

算法3 广播加密会话密钥提取

输入: 系统公钥 R_{PK} , 用户广播私钥 d_i , 用户序号 i , 广播头 R_{Hdr} , 接收方集合 S

输出: 广播加密会话密钥 K

1. 令 $R_{\text{Hdr}} = (C_0, C_1)$

$$2. \text{ 计算 } K = e(g_i, C_1) / e\left(d_i \cdot \prod_{j \in S, j \neq i} g_{n+1-j+i}, C_0\right)$$

可以验算, 算法3提取出来的 K 与算法2中计算出的 K 值相同。

1.2 比特币交易结构

如图1所示, 一笔典型的交易由交易版本、交易输入数组、交易输出数组和锁定时间组成。图中, 红色线表示左边的元素可以展开成右边的元素组合。

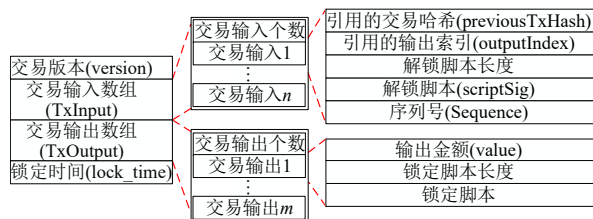


图1 比特币交易结构

其中: 交易输入数组说明了交易资金的来源与所有权; previousTxHash 和 outputIndex 共同表示

一个未花费的交易输出(Unspent Transaction Output, UTXO); scriptSig 用来证明使用者对 UTXO 的所有权, 一般包含其签名与公钥。

交易输出数组表示该笔交易中比特币的去向和花费条件。输出金额是一个 8 byte 整数, 单位为“聪(sats)”。锁定脚本指示该笔输出能够被下一笔交易使用的条件, 也就是谁可以花费这个新生成的 UTXO, 一般使用一个哈希值(输出地址)来表示。

2 方案设计

“一对多”隐蔽通信方案的核心是会话密钥的广播。方案通过广播加密方法指定多个通信接收方并实现与其会话密钥的协商, 以此克服预共享会话密钥带来的各种问题。通过将消息密文、隐含会话密钥的广播头、可从会话密钥派生的公钥分别嵌入同一笔交易的输出金额、输出地址以及解锁脚本中, 实现会话密钥和隐蔽信息的同步发送以及交易特殊性的验证, 从而达成隐蔽信息的“一对多”发送与接收。

2.1 模型架构

方案主要包括系统初始化、特殊交易构造与隐蔽信息嵌入、交易广播、交易过滤与隐蔽信息提取 4 个阶段, 涉及可信机构、隐蔽通信发送方、隐蔽通信接收方、内部恶意行为者以及比特币网络 5 类角色。具体架构如图2所示。

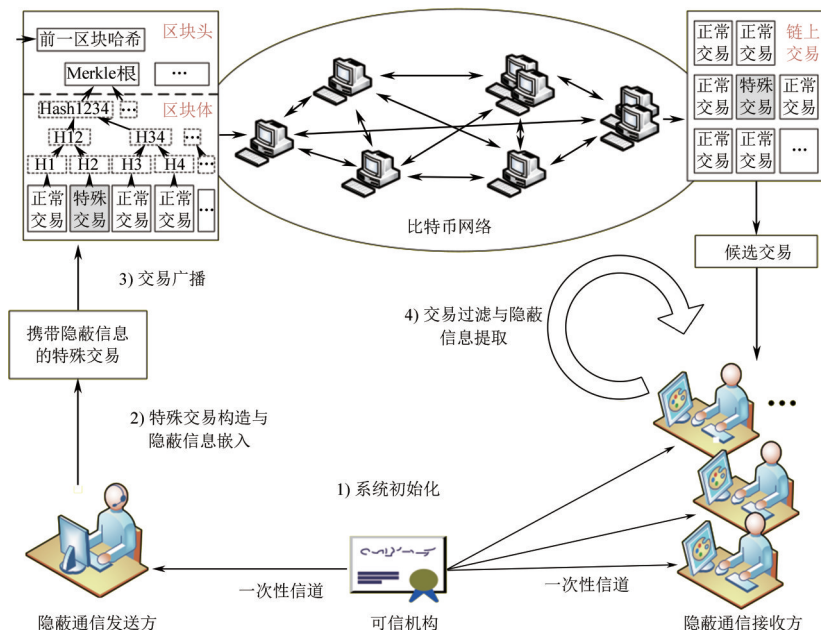


图2 基于比特币的“一对多”隐蔽通信方法模型

其中, 内部恶意行为者是一类合法但“好奇”的隐蔽通信接收方, 除正常进行隐蔽通信外, 还会

尝试发现和获取与自己无关的隐蔽通信信息。系统内任何一个用户都可以是隐蔽通信的发送方,

或被指定为接收方。图3描述了各参与方在不同阶段的具体活动以及相应算法。

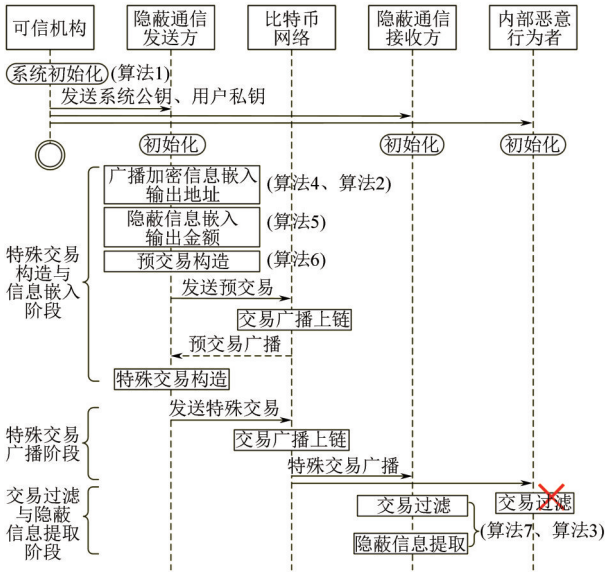


图3 系统活动流程图

2.2 系统初始化阶段

可信机构根据系统参与方的数量,使用第1.1节中的算法1生成系统公钥 R_{pk} 与各个参与方的广播私钥 d_i ,并通过安全的一次性信道,将系统公钥和广播私钥分发给对应的参与方。系统初始化后,可信机构销毁初始化过程中的所有数据,不再参与后续的通信过程。

2.3 特殊交易构造与隐蔽信息嵌入阶段

特殊交易构造与隐蔽信息嵌入具体如图4所示。

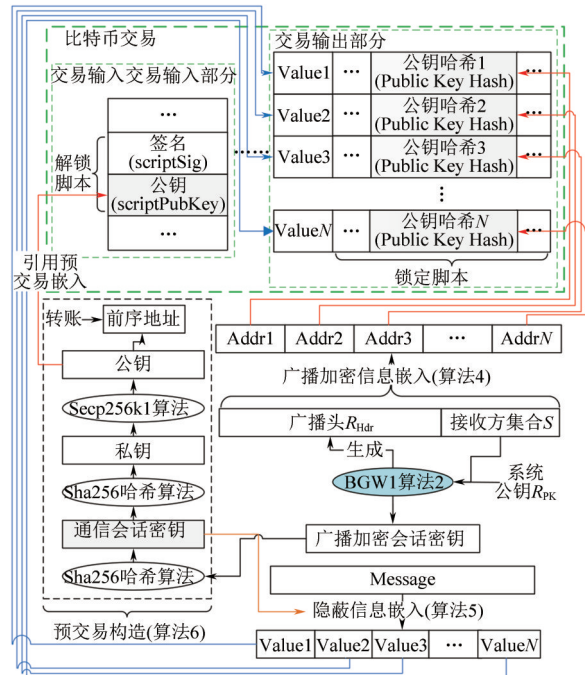


图4 特殊交易构造与信息嵌入示意图

由于各参与方在系统初始化阶段并未预共享会话密钥,隐蔽通信发送方在通信发起时,首先需要指定接收方集合,计算广播头和广播加密会话密钥,从中派生通信会话密钥,加密消息。然后,将广播加密信息和消息密文分别嵌入特殊交易的输出地址和输出金额中。再通过构造预交易,可将从通信会话密钥派生的公钥嵌入特殊交易的解锁脚本中,以此在一笔交易内完成与特定接收方的“非交互式”会话密钥协商、身份确认以及消息传输。

2.3.1 广播加密信息嵌入

隐蔽通信发送方选定一个接收方集合 S ,使用第1.1节中的算法2,计算广播加密会话密钥 K 和广播头 R_{hdr} ,通过算法4将 R_{hdr} 和 S (两者统称为广播加密信息)处理后嵌入同一笔交易的多个输出地址中。

算法4 广播加密信息嵌入

输入:通信接收方集合 S ,广播头 R_{hdr}

输出:输出地址序列 A^L

//序列化 S 和 R_{hdr}

1. $X_s = \text{bitmap}(S), X_{R_{hdr}} = \text{compress}(R_{hdr})$

//拼接得到广播加密信息序列 X_1

2. $X_1 = X_s \| X_{R_{hdr}}$

3. 计算所需的输出地址个数 x

//对 X_1 进行填充

4. $X_2 = X_1 \| X_B, X_B$ 是长度为 $\sum_{i=1}^x \text{len}(A_i) - \text{len}(X_1)$ 的随机

二进制序列, A_i 表示第 i 个地址

//序列自混淆

5. $X_3 = \text{mix}(X_2)$

//将 X_3 拆分为 x 个片段, p_i^x 为其第 i 个片段

6. $X_3 = p_1^x \| p_2^x \| \dots \| p_x^x$

7. $A^L = [A_1, A_2, \dots, A_x]$,其中, $A_i = p_i^x, i \in \{1, \dots, x\}$

序列化时, S 用位向量(0和1组成的向量)表示, R_{hdr} 用压缩形式表示,以便于数据嵌入并缩减空间。

根据类型的不同,锁定脚本中表示输出地址的字段可承载的信息长度为160或256 bit。序列化后, R_{hdr} 长度固定, S 长度为系统用户数量。据此,可计算承载 S 和 R_{hdr} 所需的嵌入地址数量。根据实际情况,可单用一种或混用多种不同类型的输出地址。若多个输出地址提供的承载长度大于所需长度,则可在 X_1 后填充随机序列补齐。

尽管 R_{hdr} 本身随机性可以保证,但若多次与同一接收方集合通信, S 的位向量可能存在一定的统

计特征。为破坏这种特征,还需对包含 S 的序列进行自混淆:将其平均分为两段,后半段的二进制字符均匀地嵌入前半段的空隙中,得到一个与原序列等长的新序列。

由于交易上链时,解锁脚本中表示输出地址的字段真实性无法被验证,可直接用处理后的广播加密信息片段作为输出地址替换解锁脚本中的公钥哈希字段。

2.3.2 隐蔽信息嵌入

方案将隐蔽信息嵌入到与使用算法 4 生成的输出地址对应的输出金额中。首先,使用 K 派生的会话加密密钥对其进行加密,然后分割密文,将密文片段逐一编码进输出金额中。具体过程如算法 5 所示。

算法 5 隐蔽信息嵌入

输入:广播加密会话密钥 K ,隐蔽消息明文 m ,输出地址个数 x ,配平金额 V_b

输出:输出金额序列 V^L

//派生加密密钥

1. $k_{enc} = \text{sha256}(K)$

//加密明文

2. $c = k_{enc} \oplus m$

//分割密文

3. $c = p_1^c \| p_2^c \| \dots \| p_x^c$

//将密文片段映射为十进制金额

4. $V^L = [V_1, V_2, \dots, V_x]$, 其中, $V_i = \text{map}(p_i^c) + V_b, i \in \{1, \dots, x\}$

算法中,配平金额 V_b 用以防止在特殊交易输出金额中出现过小的数值,一般应大于相应比特币网络的粉尘阈值,以免交易被误判为粉尘攻击而无法上链。此外,若需多次发送特殊交易,配平金额还应考虑真实金额的统计特征,以抵抗相应的分析。

2.3.3 预交易

任何一个交易都需要至少一个可验证的输入。如图 3 所示,预交易阶段,方案通过发送一笔完全正常的交易(简称“预交易”),为携带隐蔽信息的特殊交易构造一个可用的 UTXO 输入。预交易无需上链即可被引用。预交易构造步骤如算法 6 所示。

算法 6 预交易构造

输入:广播加密会话密钥 K ,输出金额序列 V^L ,交易费用 N_{Gas} ,预交易支付账户 a_u

输出:预交易 T_x

//生成输入地址私钥

1. $R_{sk}^{pre} = \text{sha256}(\text{sha256}(K))$

//使用比特币标准算法生成输入地址

2. $A_{pre} = \text{bitcoinGenerateAddr}(R_{sk}^{pre})$

//计算特殊交易的输入金额

3. $V_i = \sum_{V \in V^L} V + N_{Gas}$

//构造预交易,使用 a_u 向地址 A_{pre} 转入 V_i 个比特币

4. $T_x = \text{buildTx}(a_u, A_{pre}, V_i)$

预交易构造完成后,隐蔽通信发送方将其发送到比特币网络上,此时,地址 A_{pre} 上将有 V_i 个可用的比特币。这些比特币将在特殊交易中被使用。

2.3.4 特殊交易构造

将输出地址序列 A^L 中的地址与输出金额序列 V^L 中的金额一一对应形成输出数组,并以预交易的输出为输入,构造出同时携带广播加密信息和隐蔽信息的特殊交易。预交易私钥已知,可为特殊交易签名,保证有效性。接收方通过能否从交易输出计算出解锁脚本中的公钥来确认交易是否携带隐蔽信息。具体如图 4 所示。

2.4 交易广播阶段

隐蔽通信发送方完成交易构造并将其发送到比特币网络上后,比特币网络按照既有规则对其进行广播,并由矿工将其打包上链。

2.5 交易过滤与信息提取阶段

交易过滤阶段由隐蔽通信接收方完成。由于无法从交易数据结构(例如地址等)中直接判断隐蔽通信是否存在,隐蔽通信接收方必须监视比特币网络中的每一笔交易,并假设其为携带隐蔽信息的特殊交易且自己被指定为接收方,使用算法 7 尝试对其进行交易验证和信息提取。

算法 7 交易过滤与信息提取

输入:备选交易 T_{x_c} ,系统公钥 R_{PK} ,用户广播私钥 d_i

输出:隐蔽信息明文 m

//提取锁定脚本中的输出地址并按顺序拼接

1. $X_A = A_1^c \| \dots \| A_y^c$, 其中: y 为 T_{x_c} 的输出个数; $A_i^c, i \in \{1, 2, \dots, y\}$

为其各个输出锁定脚本中的地址

//初步过滤

2. if $\text{len}(X_A) < \text{len}(R_{Hdx}) + \text{len}(S)$, return $\perp$

//按算法 4 的逆操作从 X_A 中恢复嵌入信息

3. $X_{ori} = \text{recover}(X_A)$

//分割 X_{ori} , 获取候选广播加密头 H_c 和接收方集合 S_c

4. $(H_c, S_c) \leftarrow \text{Split}(X_{ori})$

5. 使用算法 3 和 (H_c, S_c) 以及广播私钥 d_i 求解潜在的广播加密会话密钥 K_c

//计算输入地址私钥

6. $R_{sk}^c = \text{sha256}(\text{sha256}(K_c))$

//计算比特币标准算法计算输入地址公钥

```
7.  $R_{pk}^c = \text{GenerateECPK}(R_{sk}^c)$ 
//比较  $R_{pk}^c$  和解锁脚本中的公钥  $R_{pk}^s$  是否一致
8. if  $R_{pk}^c \neq R_{pk}^s$ , return  $\perp$ 
//计算解密密钥
9.  $k_{dec} = \text{sha256}(K_c)$ 
//提取输出金额并按顺序拼接
10.  $c = \text{map}^{-1}(V_1) \parallel \dots \parallel \text{map}^{-1}(V_y)$ 
//恢复明文
11.  $m = c \oplus k_{dec}$ 
```

尽管内部恶意行为者也持有其相应的私钥,但由于其未被指定进 S ,无法通过算法 7 计算出正确的会话密钥,从而获取隐蔽信息,也无法判断该笔交易的特殊性。

3 方案实现

利用 Python3 在 Ubuntu 18.04 上实现了原型系统,并在比特币测试网 Testnet 上进行了交易的广播和接收。方案通过 Supersingular 512 实现配对运算,系统用户总数为 80,并将所有输出地址的类型设为 P2PKH,使得刚好可以通过 7 个输出地址完成 R_{hdr} 和 S 的嵌入。配平金额设置为 600 聪。Testnet 上一笔携带隐蔽信息交易的 ID 为 d9bd4d9d598d5678a243afe935f8f2c05f8f78198aeb94c69d0df2b9a13107e4,携带的隐蔽信息为“goodday”。系统内仅被指定进 S 的用户可以获取该信息,且事先未协商会话密钥。

4 方案分析

4.1 安全性分析

保密性。方案基于 BGW1 广播加密算法设计,其安全性基于决策型双线性 Diffie-Hellman 假设。该假设指出,区分真实与随机的目标群元素是困难的,保证了只有在隐蔽通信接收方集合中的用户才可以从其现有知识以及特殊交易中获取到广播加密会话密钥。

抵抗内部恶意行为者的能力。方案通过非对

称加密的解密正确性来实现特殊交易判断。除非被指定为接收方并解密正确,否则内部恶意行为者无法确切地判断交易是否携带隐蔽信息。如果其在某次尝试的过程中失败,则无法将“该交易未携带信息”与“自身不在接收方集合中”这两种可能性有效地区分开来。相比于传统基于对称加密思想的过滤方法,方案在抵抗内部恶意行为者上具备一定的优势。

动态成员管理。尽管系统建立后新增用户较为困难,但借助其可灵活指定接收方的特性,可以较为容易地排除恶意成员。只需与现有合法用户约定不再将该成员指定为接收方,即可将其排除在后续的隐蔽通信之外,并可保证其无法获取后续的通信信息。

4.2 可拓展性分析

方案实现了多用户间通信会话密钥的临时协商,可作为会话密钥协商基础组件,应用于多种隐蔽传输场景。例如,可与文献[7]中的 ECDSA 签名潜信道方案组合,先利用本方案完成群组通信会话密钥协商,再通过签名潜信道完成后续隐蔽信息传输,无需提前分组和预共享密钥,即可实现多用户隐蔽消息群发。

在加密会话密钥协商基础上,可较易结合其他方案,进一步提高信道容量。例如,可通过增加输出金额中嵌入位数或输出地址个数、利用交易中的其他数据结构,或采用文献[3]的多签名隐蔽传输机制,拓展单个特殊交易能携带的信息数量。

4.3 信息分发效率分析

假设在一个由 $(n + 1)$ 个用户组成的系统中,某用户需同时向 n 个用户传输隐蔽信息,接收方接收信息时,需从 m 个交易中进行过滤。本文从对隐蔽信息进行加密的会话密钥的性质、密钥数量(包括各类公/私钥)、交易费用、过滤复杂度、交易容量等方面,将本文方案与通过多次“一对一”实现“一对多”(O2O-O2M)方法以及文献[10]提出的分组方案进行比较。结果如表 1 所示。

表 1 理论比较

方案名称	加密会话密钥		系统实现完全分组 所需的密钥数量	整体消耗的费用/聪	每个用户持有的 密钥数量	交易过滤 复杂度	每交易 容量
	预共享	可变性					
O2O-O2M	需要	不可变	$n(n + 1)/2$	$\text{len}(T_{x_{(U)}}) \times R_{\text{rate}} \times n$	n	$O(n^2m)$	—
文献[10]方案	需要	不可变	$2^{n+1} - n - 2$	$\text{len}(T_{x_{(U)}}) \times R_{\text{rate}} \times 2$	2^n	$O(2^n m^2)$	80
本文方案	不需要	可变	$3n + 4$	$(V_b + 2^{y-1}) \times x + \text{len}(T_{x_{(U)}}) \times R_{\text{rate}} + \text{len}(T_{x_{(U)}}) \times R_{\text{rate}}$	$2n + 4$	$O(m)$	ay

表中: $\text{len}(T_{x(i)})$ 表示以字节计的交易的长度, $(1/x)$ 表示该笔交易由一个输入数组和 x 个输出数组组成; R_{rate} 表示交易发布时比特币的交易费率,一般在2到20 sats/vB(“聪/虚拟字节”)不等; V_b 表示配平金额; a 表示输出金额个数; y 表示每个金额的嵌入位数。

与O2O-O2M以及文献[10]方案相比,本文方案具备通信会话密钥可变、不需要预共享等优势,当系统用户数量较多时,为保证所有潜在分组内部的通信不被其他系统参与方(内部恶意行为者)获取,系统需要生成的密钥总量也最少。尽管本文方案单次通信所需的费用比文献[10]方案稍高,但随着系统用户数的增长,由于本文方案无需用所有预共享密钥逐一进行信息提取尝试,其在密钥管理、交易过滤复杂度方面的优势将逐渐凸显。方案每交易信息容量由输出地址数量和占用的输出金额决定,7个输出地址理论上最多可承载448 bit,而目前容量较高的RDSAC方案^[8]为256 bit。

表2给出了本文方案各个过程的平均耗时。文献[10]给出的数据一并附上。数据表明,二者在隐蔽信道构造与过滤上都是高效的,尤其是相对比特币平均10 min的出块速度而言。但若存在多个分组,后者需使用每个预共享密钥逐一进行过滤尝试,将带来额外的时间开销。

表2 性能比较

单位:s

方案名称	嵌入时间	交易构造时间	过滤时间	提取时间
本文方案	0.070	0.013		0.047
文献[10]方案	0.013	0.034	0.002	0.025

4.4 下一步工作

4.4.1 身份认证与安全增强

方案通过广播加密实现了对接收方的“身份认证”,但受限于加密方法和信道容量,暂未设计针对发送方的身份认证机制。在开放的“一对多”隐蔽信道中,这可能带来身份冒用、重放攻击或伪造广播头等风险。在后续的研究中,可将本文方案作为通信会话密钥协商组件,在与之结合的隐蔽信息传输方法中加入签名元素或引入第三方和额外的认证因素^[15],通过模糊验证等方法,进一步提高隐蔽通信发起方的匿名性和通信的安全性。

4.4.2 抗统计分析能力提升

为检验方案生成的特殊交易与正常交易在输

出金额上的统计不可区分性,采用Mann-Whitney U和K-S检验^[16]对其进行分布差异性检验。图5展示了在不同配平金额以及使用同一配平金额构造交易的不同次数下,Mann-Whitney U检验计算出来的 p 值的变化。 $p < 0.05$ 表示两组分布存在统计学显著差异, $p \geq 0.05$ 则表示无足够证据支持该差异存在。实验表明,相比于配平金额,配平金额的使用次数对 p 值的影响更大。当使用同一配平金额构造输出金额的交易数量不超过一定数量时,难以将其与正常交易区分开来,反之,则可能与人类正常转账行为在统计学上存在差异。K-S检验的结论类似。

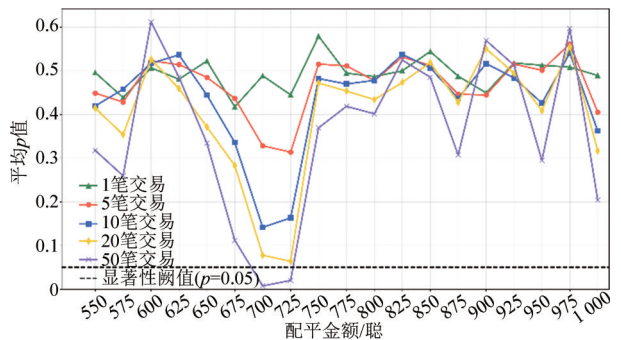


图5 Mann-Whitney U检验结果图

检验结果对方案的使用,尤其是对配平金额的管理提出了严格的要求,需动态调整配平金额。但当方案用作通信会话密钥协商组件时,则无此问题。此时,输出金额不承担信息嵌入功能,可以使用任何符合正常分布的输出金额值。这也是本文方案主要的应用方向之一。在后续的研究中,除进一步将本文方案作为基础组件与其他隐蔽通信方案组合外,还应研究如何提高其与正常交易的统计不可区分性。潜在的路径包括通过调整数据嵌入位置减少交易输出个数,或者借鉴文献[16]的思路,根据历史统计数据在单个交易中灵活采用多个配平金额等。

4.4.3 不可花费UTXO规避

为传输数据,方案产生了不可花费的UTXO。当方案被大规模应用时,可能导致比特币UTXO集急剧膨胀,对比特币的底层生态带来潜在影响^[17]。在后续的研究中,可将数据嵌入至冗余签名等不影响交易正常花费的位置,避免不可花费UTXO的产生,减轻对比特币底层系统的影响。

5 结束语

本文提出了一种基于比特币的“一对多”定向

隐蔽通信方法,可以指定隐蔽通信的接收方,并能防止内部恶意为者对隐蔽通信的信息获取,其安全性由BDHE假设保证。方案综合运用了比特币中的值通道和地址通道,实现了广播加密信息和隐蔽信息的同步发送,并能在一笔交易中完成交易特殊性的验证。方案允许系统内任意一个对象发起组内通信,可以在通信的过程中临时指定不同的通信对象,无需提前分组。随着用户数量的增加,方案在通信效率和综合成本上的优势将逐渐凸显。方案可作为其他区块链上隐蔽通信方案的基础组件,具备一定的应用前景。

参考文献:

- [1] Sleiman M D, Lauf A P, Yampolskiy R. Bitcoin message: data insertion on a proof-of-work cryptocurrency system [C]//Proceedings of the 2015 international conference on cyberworlds. Piscataway, USA: IEEE, 2015:332-336.
- [2] Wang R D, Li B H, Ren W, et al. CCBTC: a blockchain-based covert communication scheme over bitcoin transactions[C]//Web and big data. Berlin, Germany: Springer, 2024:466-480.
- [3] Recabarren R, Carbutar B. Tithonus: a bitcoin based censorship resilient system [J]. Proceedings on Privacy Enhancing Technologies, 2019(1):68-86.
- [4] Liu S Y, Fang Z, Gao F, et al. Whispers on ethereum: blockchain-based covert data embedding schemes [C]//Proceedings of the 2nd ACM international symposium on blockchain and secure critical infrastructure. New York, USA: ACM, 2020:171-179.
- [5] Zhang L J, Zhang Z J, Wang W Z, et al. A covert communication method using special Bitcoin addresses generated by vanitygen[J]. Computers, Materials & Continua, 2020, 65(1):597-616.
- [6] Alsalamy N, Zhang B S. Utilizing public blockchains for censorship-circumvention and IoT communication [C]//Proceedings of the 2019 IEEE conference on dependable and secure computing. Piscataway, USA: IEEE, 2019. DOI: 10.1109/dsc47296.2019.8937637.
- [7] 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 and IEEE green computing and communications and IEEE cyber, physical and social computing and IEEE smart data. Piscataway, USA: IEEE, 2018: 1244-1252.
- [8] Chen Z, Zhu L H, Jiang P, et al. Exploring unobservable blockchain-based covert channel for censorship-resistant systems [J]. IEEE Transactions on Information Forensics and Security, 2024, 19:3380-3394.
- [9] She W, Ma J W, Xia K B, et al. A blockchain-based one-to-many traceless covert communication model for secure high-capacity information transmission [J]. Peer-to-Peer Networking and Applications, 2025, 18(6):289.
- [10] SHEN T Z, ZHU L H, GAO F, et al. A blockchain-enabled group covert channel against transaction forgery [J]. Mathematics, 2024, 12(2):251.
- [11] YUAN X B, JIANG P, CHEN Z, et al. Blockchain-based group covert communication for IoT network [J]. IEEE Internet of Things Journal, 2025, 12(13):25633-25650.
- [12] She W, Huo L J, Tian Z, et al. A double steganography model combining blockchain and interplanetary file system [J]. Peer-to-Peer Networking and Applications, 2021, 14(5):3029-3042.
- [13] 巴阳,陈越,胡学先,等.基于区块链与属性基加密的数据共享方案[J].信息工程大学学报,2022,23(4):443-451.
- [14] Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys [C]//Advances in cryptology-CRYPTO 2005. Berlin, Germany: Springer, 2005:258-275.
- [15] Xu M J, Wang D. Practical two-factor authentication protocol for real-time data access in WSNs [J]. IEEE Transactions on Dependable and Secure Computing, 2025, 22(5):5215-5230.
- [16] Chen Z, Zhu L H, Jiang P, et al. Blockchain-based covert communication: a detection attack and efficient improvement [J]. IEEE Transactions on Information Forensics and Security, 2024, 19:9698-9713.
- [17] Matzutt R, Hiller J, Henze M, et al. A quantitative analysis of the impact of arbitrary blockchain content on bitcoin [C]//Financial cryptography and data security. Berlin, Germany: Springer, 2018:420-438.

(编辑:邵 华)