Journal of Computer Applications
计算机应用, 2022, 42(1): 148 - 156
ISSN 1001-9081
CODEN JYIIDU
2022-01-10
http://www.joca.cn

文章编号:1001-9081(2022)01-0148-09
DOI:10.11772/j.issn.1001-9081.2021020296

门罗币匿名及追踪技术综述

林定康*,颜嘉麒,巴·楠登,符朕皓,姜皓晨
(南京大学 信息管理学院,南京 210023)
(*通信作者电子邮箱 191820116@smail.nju.edu.cn)

摘　要:虚拟数字货币为恐怖分子融资、洗钱、毒品交易等犯罪活动提供了温床,而门罗币作为新兴数字货币的代表,具有公认的高匿名性。针对利用门罗币匿名性犯罪的问题,从技术角度探索门罗币匿名技术及其追踪技术,综述近年来的研究进展,从而为有效应对基于区块链技术的犯罪提供技术支持。具体来说,总结了门罗币匿名技术的演进,并梳理了学术界关于门罗币匿名技术的追溯对策。首先,在匿名技术中,介绍了环签名、保证不可链接性(一次性公钥)、保证不可追溯性、提高匿名性的重要版本升级等。然后,在追踪技术中,介绍了0-mixin攻击、输出合并攻击、最新猜测攻击、封闭集攻击、泛洪攻击、恶意远程节点攻击、钱包环攻击等攻击方法。最后,基于对匿名技术和追溯对策的分析,得出了四点结论:门罗币的匿名技术和追踪技术的发展相互促进;RingCT的应用是一把双刃剑,既使得从币值出发的被动攻击方法失效,也使得主动攻击方法更加容易奏效;输出合并攻击和0-mixin攻击具有互补作用;门罗币的系统安全链条仍待理顺。

关键词:区块链;门罗币;数字货币;追踪技术;匿名技术;文献综述;环签名
中图分类号:TP311.13; TP309　　**文献标志码**:A

Survey of anonymity and tracking technology in Monero

LIN Dingkang*, YAN Jiaqi, BA Nandeng, FU Zhenhao, JIANG Haochen
(*School of Information Management, Nanjing University, Nanjing Jiangsu* 210023, *China*)

Abstract: Virtual digital currency provides a breeding ground for terrorist financing, money laundering, drug trafficking and other criminal activities. As a representative emerging digital currency, Monero has a universally acknowledged high anonymity. Aiming at the problem of using Monroe anonymity to commit crimes, Monero anonymity technology and tracking technology were explored as well as the research progresses were reviewed in recent years, so as to provide technical supports for effectively tackling the crimes based on blockchain technology. In specific, the evolution of Monero anonymity technology was summarized, and the tracking strategies of Monero anonymity technology in academic circles were sorted out. Firstly, in the anonymity technologies, ring signature, guaranteed unlinkability (one-off public key), guaranteed untraceability, and the important version upgrading for improving anonymity were introduced. Then, in tracking technologies, the attacks such as zero mixin attack, output merging attack, guess-newest attack, closed set attack, transaction flooding attack, tracing attacks from remote nodes and Monero ring attack were introduced. Finally, based on the analysis of anonymity technologies and tracking strategies, four conclusions were obtained: the development of anonymity technology and the development of tracking technology of Monero promote each other; the application of Ring Confidential Transactions (RingCT) is a two-edged sword, which makes the passive attack methods based on currency value ineffective, and also makes the active attack methods easier to succeed; output merging attack and zero mixin attack complement each other; Monero's system security chain still needs to be sorted out.

Key words: blockchain; Monero; digital currency; tracking technology; anonymity technology; literature review; ring signature

收稿日期:2021-03-01;**修回日期**:2021-04-15;**录用日期**:2021-04-16。
基金项目:江苏"333高层次人才培养工程"科研项目(BRA2020276);南京大学2021年双创大数据与理论研究双创项目。
作者简介:林定康(2001—),男,湖北十堰人,主要研究方向:区块链、数字货币;　颜嘉麒(1983—),男,福建泉州人,副教授,博士,CCF会员,主要研究方向:区块链、信息系统、数据分析、情报学;　巴·楠登(1999—),女,新疆乌鲁木齐人,主要研究方向:区块链、环签名、匿名数字货币;　符朕皓(2001—),男,河南信阳人,主要研究方向:区块链、信息系统;　姜皓晨(2001—),男,江苏泰州人,主要研究方向:信息系统、区块链、零知识证明。

0　引言

经济和技术全球化程度越来越高,世界和区域之间的差距越来越小,犯罪分子正在采用新的货币形式(例如加密货币)来逃避监管[1],进行跨国的非法交易,并提高其非法活动的匿名性[2]。这种新型的犯罪形式,绕开正规金融机构的监管,成为恐怖分子融资、洗钱、毒品交易的温床[3]。例如,圣战分子和恐怖组织的支持者正在积极寻找并促进使用新兴技术,例如比特币、大零币、门罗币(Monero)等,来减轻与传统资金转移方法相关的监管风险[4]。在暗网和匿名数字货币技术的助推之下,毒品交易格局日益复杂。比特币等匿名交易方式,打破了毒品交易双方必须在同一地点交易的限制,绕开了正规机构的监管,使暗网毒品销售网络日益庞大[5]。很多网站也在利用用户的浏览来操纵他们的计算机帮助不法分子进行门罗币的挖矿[6]。

自2009年比特币[7]诞生以来,它已成为最具代表性的密码货币,占有最大的市场份额。比特币的成功不仅在于它最早产生,也在于比特币声称的匿名性。比特币声称具有匿名性,但实际上比特币提供的匿名性是相对的,因为交易的信息向任何人公开,比特币的金额和流向可以完全确定。不仅如此,研究发现可以通过将地址进行聚类来确定用户集群来揭示用户的身份,挖掘出集群之间的资金流向,从而破解这种匿名性[8]。为了增加交易的匿名性,人们提出了新的数字货币方案,其中具代表性的是运用了环签名技术的门罗币[9]、运用coinjoin技术的达世币[10]和运用了零知识证明技术的大零币[11]。本文对门罗币的匿名技术和追踪技术进行了整理和评价。

门罗币是一种基于CryptoNote加密协议的隐私加密货币,它试图解决比特币中的可追溯性和可链接性问题。门罗币的代号为XMR,XMR也是门罗币的货币单位,1 XMR就是一个门罗币。截至2021年1月,它在最受欢迎的匿名数字货币中占到第16位,市值约为140.44亿人民币[12]。比特币是第一个也是目前最大的加密货币,它明确地标识了交易中使用了哪枚硬币,而门罗币允许用户通过包括被称为“mixin”的交易输入来模糊交易的真正输入[2]。门罗币交易示意图如图1所示。本文用Tx表示一个交易,key表示输入输出的公钥地址,假设有3个交易Tx1、Tx2、Tx3,每一个交易各有一个交易输出key-*a*、key-*b*、key-*c*,创建一个新的交易Tx4将key-*b*的TXO(Transaction Output)转给key-*d*,门罗币根据某些策略将其他两个输出地址key-*a*、key-*c*都标记为Tx4的输入,这样真实的输入key-*b*就被隐藏起来。人们不知道key-*a*、key-*b*、key-*c*哪一个才是真正的输入,其中用来混淆真实输入的输出地址key-*a*、key-*c*就被称为mixin。

门罗币隐私问题要求货币确保以下两个属性[13]:

不可链接性(unlinkability)　对于任何交易,都不可能证明它们是由同一个发送方发送的。即使是一个无限强大的对手,能够访问无限数量的交易,也不能以优势猜测他的身份,也不能将事务链接到同一个发送者[14]。

不可追踪性(untracability)　给定交易输入,被花费的实际输出应该在一组其他输出中匿名[15]。

门罗币的匿名技术保证了交易的不可链接性和不可追踪性[9]。为了保证不可链接性,门罗币通过设计引入了一次性随机地址的概念,其思想是:交易的每个发送方都为收件人生成一个新的一次性随机地址,这种方式只有收件人可以使用长期秘密密钥来花费它。如果每个地址都是使用新的随机性生成的,并且只使用一次,那么对手很难链接两个地址。为了保证不可追踪性,门罗币使用名为环签名的加密技术。环签名让发送人原本的输入混合在其他的输入中一起,发件人代表一组其他用户匿名签名交易信息。因此,被花费的实际输入在多个签名中被隐藏,无法判断到底哪个是真正的输入,从而实现了不可追踪性[15]。

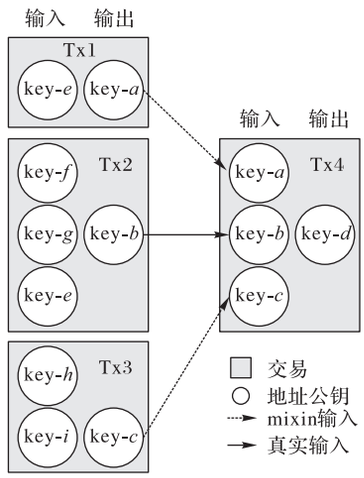

图1　门罗币交易示意图

Fig. 1　Schematic diagram of Monero transaction

本文介绍保证了不可链接性的一次性随机地址、保证了不可追踪性的环签名加密技术以及为提高匿名性的各个版本更新中技术的演进,并介绍针对这些技术和门罗币交易的特征而进行追踪的各种对策。通过对门罗币的匿名技术及其追踪技术的研究,本文主要得到如下4个结论:

1) 门罗币的匿名技术和追踪技术呈现出相互促进的特点。

2) RingCT(Ring Confidential Transactions)的应用是一把双刃剑,它既使从币值出发的被动攻击方法失效,也使主动攻击方法更加容易。

3) 输出合并攻击和0-mixin攻击(Zero Mixin Attack)具有互补作用。

4) 门罗币的系统安全链条仍待理顺。

1　门罗币匿名技术

1.1　环签名

门罗币匿名技术的核心是环签名加密技术。在密码学中,环签名是一种可以由一组各自具有密钥的用户组中的任何成员执行的数字签名。因此,具有环签名的消息被特定人群中的某一个人认可,但是确定使用哪个组内成员的密钥来生成签名在计算上是不可行的,这也是环形签名的安全属性之一[16]。环签名最早由Rivest等[17]在2001年提出。该概念类似于组签名的概念,但是无法识别环签名交易的实际签名者,并且可以在环签名中包含任意数量的用户,而无需任何

其他设置。最初的概念是使环签名成为一种泄漏机密信息的方法，特别是从高级政府官员那里泄漏机密信息，而实际上不透露出签名者是谁。

环签名使用了基于椭圆曲线离散对数问题的EDDSA（EDwards-curve Digital Signature Algorithm）算法[18]。一次环签名由密钥生成算法（key GENeration algorithm，GEN）、签名生成算法（SIgnature Generation algorithm，SIG）、签名验证算法（signature VERification algorithm，VER）和链接性验证算法（LiNKability verification algorithm，LNK）四种算法组成[9]。

GEN　签名者选择一个随机秘密密钥x，计算公钥$P = xG$和密钥镜像$I = H_P(P)$，其中H_P是确定性哈希函数。

SIG　签名者获取一个消息m，一组公钥S'的$\{P_i\}_{i=s}$，并输出一个签名σ和一个密钥集$S = S' \cap \{P_s\}$。

VER　验证者检验签名。

LNK　验证者检查I是否在过去的签名中使用过。

每个交易都有一个环签名，可以识别哪个mixin是真实的，而不透露任何关于它的信息；同时，每个mixin以及实际输入都有一个唯一的密钥镜像，所有节点都可以检查是否有任何密钥镜像在此之前已经显示[19]。

1.2　保证不可链接性

一次性随机地址保证了门罗币的不可链接性。与比特币模型相反，用户拥有唯一的公钥、私钥对对应于地址，在门罗币中，发件人根据收件人的地址和某种随机性生成一次性公钥[20]。从这个意义上说，发送给同一个收件人的交易实际上是发送给不同的一次性公钥（而不是直接发送到唯一地址），只有收件人才能收回一次性私钥及花费金额。

Noether等[21]详细地讲解了一次性随机地址的数学原理，门罗币的一次性随机地址的实现代码在github上公开[22]。举例说明它的作用过程：当一个用户Alice希望向另一个用户Bob付款时，她获得Bob的长期公钥pk-long。然后，她为Bob生成一次性公钥pk-onetime。因为只有Bob知道长期私钥sk-long，只有他才能得到sk-onetime。然后，Alice创建了一个交易，她支付给Bob的一次性公钥pk-long。一次性密钥作为Bob的一次性使用的支付地址。由于地址总是随机性生成，并且只使用一次，因此发送方和接收方以外的任何人都很难将两个地址链接到同一个用户。

如果有多个输出支付给同一个收件人，则每个输出生成一个新的一次性公钥。因此，每个事务输出（Transaction Outputs，TXO）都可以通过其相应的一次性公钥进行标识。

1.3　保证不可追溯性

门罗币使用环签名来确保不可追踪性，使用了Fujisaki等[23]提出的修改版本的环签名。环签名允许用户代表用户的“环”签名消息，签名者只需要知道自己的签名密钥。在签署消息后，签名者提供环中所有用户的公钥。验证者（verifier）能够验证示证者（prover）确实在环中的公钥中，但不能确定到底是哪一个，因而就不能确认身份[24]。

例如，用户Alice希望发送10 XMR到另一个用户Bob。她首先获得Bob的长期公钥pk-long，然后根据该公钥创建一个一次性的随机公钥pk-onetime。现在，Alice没有像比特币那样签署交易，而是在价值10 XMR的区块链上获取其他一些TXO，表现为一些一次性随机公钥。本文将这个集合表示为$S = \{P_1, P_2, \cdots, P_m\}$，$S$还包括Alice自己的输入，其中$P_i = x_i G\left(i \in [1, m]\right)$。她的输入$P_i$在$S$中隐藏，Alice能够创造一个环签名并签署交易。

当其他人看到交易信息时，只能获知真实的花费在几个TXO中，但无法确定哪个是真正的TXO[19]。Alice在S中包含的其他输入密钥称为mixin。由于Alice的实际输入密钥在S中的密钥中是匿名的，所以使用的混合输入mixin数量越大，实现的匿名性就越好。显然，环签名提供了门罗币内部的内置混合服务，每个用户都可以自主地混合mixin[25]。

1.4　提高匿名性的技术演进

1.4.1　最初版本

在2016年1月1日版本之前，在最初的Monero实现中，mixin是从所有具有与所花费的硬币相同面额的先前TXO集合中统一选择的，因此，选择较早的产出比选择较新的产出更频繁。门罗币的mixin选择Cryptonote引用实现包含了统一的选择策略，由于交易输入中引用的所有TXO必须具有相同的面额（即0.01 XMR输入只能引用0.01 XMR输出），因此客户端软件维护可用TXO的数据库，按面额索引。mixin是从这个有序的可用TXO列表中采样的，除了它们在块链中的相对顺序外，不考虑任何时间信息[25]。

1.4.2　mixin选择策略

在2016年1月1日升级之后，引入了一种新的策略，用于选择基于三角形分布的混合策略[26]，有利于较新的硬币作为混合币而不是较旧的硬币。这一变化是为了对抗最新猜测攻击，防止由于总是较新的TXO为真实输入而暴露。在2016年12月13日版本之后，对mixin选择策略进行了更改：更多从新产生的TXO中选择了mixin，即在过去5 d内创建的输入，效果是确保事务中25%的输入从最近的区域采样。

1.4.3　最低mixin要求

在2016年3月，门罗币开始要求每个输入至少2个mixin，禁止了0-mixin交易的存在。至少2个mixin的规定是为了抵御0-mixin攻击，防止因为0-mixin的级联效应而暴露多mixin交易的真实输入。这在2017年9月增加到4个，2018年4月增加到6个；从2018年10月起，所有交易的mixin数量已固定在10个[27]。更多的mixin意味着更高的匿名性。

1.4.4　RingCT更新

2016年9月19日之后，应用了RingCT[28]，允许用户隐藏其硬币的面额，避免了将可用TXO分割成不同面值以防止基于面值的推理攻击[25]。RingCT交易直到2017年1月10日硬叉之后才被认为有效[29]。由于面值被隐藏，mixin的选择从原来必须选择相同面额，到现在可以随机选择；并且由于它是在2-Mixin最小值生效后部署的（版本0.9.0），因此没有0-mixin在RingCT输入造成0-mixin攻击的威胁。

RingCT增加了哈希的次数，但是减少了一半签名的长度，对于数字货币来说，这无疑就提升了很大的竞争力，因为签名的缩短不仅减轻了网络负载，同样还减小了交易的大小；对于按字节数来进行计算交易费的机制来说，也就减小了每笔交易的交易费[19]。

2　门罗币追踪技术

目前,门罗币的追踪技术主要有4类:基于输入输出关系而进行的追踪,如0-mixin攻击、输出合并攻击、封闭集攻击等;基于统计得出总结规律的追踪,如最新猜测攻击等;通过某些方法使得部分公钥已知以进行追踪,如泛洪攻击、钱包环攻击等;利用门罗币安全机制漏洞进行的追踪,如恶意远程节点攻击等。下面对这些追踪技术逐一进行介绍。Kumar等[30]是在门罗币的追溯性领域开创性的研究,最先提出了0-mixin攻击、输出合并攻击、最新猜测攻击。Kumar等[30]首先定义3个名词,用来解释以下的追踪技术,本文将沿用这3个定义以便解释各种追踪方法。

定义1　有效匿名集大小。假设一个交易的某一个输入有 m 个mixin来产生环签名,如果其中的 k 个mixin是可追踪的,那么有效匿名集大小为 $m+1-k$。

定义2　可追踪输入。假设一个交易的某一个输入的有效匿名集大小为1,那么该输入为可追踪输入。

定义3　可追踪交易。假设一个交易的每笔输入都是可追踪输入,那么该交易为可追踪交易。

以下两个启发式0-mixin攻击和输出合并攻击的目的就在于减小有效匿名集,寻找可追踪输入进而确定可追踪交易。

2.1　0-mixin攻击

Kumar等[30]首次提出了0-mixin攻击,此攻击基于这样一个原理:当一个密钥key-a为交易Txa输入i的真实输入时,它就不可能被再次花费,那么在其他的交易Txb中输入j再次出现的key-a就不是j的真实输入。根据定义2,一个0-mixin的输入的有效匿名集大小是1,那么0-mixin的输入都是可追踪输入。也就是说,这些输入都是没有使用mixin来进行混合的,在一个输入中的唯一密钥就是这个输入的真实输入。而当已知此密钥为这一输入的真实输入,就可以在其出现在其他输入中时剔除掉它,以减小有效匿名集的大小,增加可追踪性[30]。

例如,在图2中,第一个交易Tx1中有一个输入,而这个输入为0-mixin,可以确定,这个输入key-a就是它的真实输入。当key-a出现在另一个交易的输入Tx2中时,认定key-a不是交易Tx2的真实输入,那么Tx2的真实输入就在其余的密钥中产生,而恰巧这个输入剩下的密钥只有一个,该输入的有效匿名集的大小为1,可以确定,key-b就是Tx2的真实输入。通过这样的重复过程,不断消减其余交易中输入的有效匿名集大小,确定新的已知密钥,就可以达到追踪的目的。

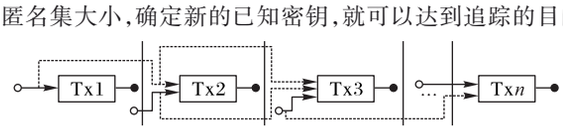

图2　0-mixin攻击示意图

Fig. 2　Schematic diagram of zero mixin attack

0-mixin攻击方法的成功是基于大量的0-mixin交易的存在,得到了许多的已知密钥。文献[30]采集的数据是从2014年4月18日到2017年2月68日,区块高度为1 240 503。其中65%为0-mixin交易,使用此方法破解出了另外22%交易的匿名性,使得87%的输入可追踪。

2018年,Möser等[31]使用同样的数据进行了再次实验来验证0-mixin攻击的有效性。Möser等[31]的贡献在于将0-mixin攻击运用到不同改进阶段的门罗币交易数据,探寻该方法在各个不同阶段的有效性。通过再次验证,Möser等[31]发现在2-mixin的强制要求版本之后,可追踪性急剧下降;而在RingCT推出的版本之后,可追踪性更低了。这说明版本的改进,特别是RingCT的应用使得门罗币的匿名性极大增强。事实上,即使是在此之后发表的论文中,很少有能够真正破解RingCT的攻击办法。

使用越多的mixin确实可以提供更多的匿名性。实验的结果显示,无论是2-mixin的强制要求出现之前还是之后,RingCT出现之前或之后,该方法的有效性大致随着mixin数量的增多而递减。

2020年Ye等[32]对这个方法进行了再次验证,将输出合并攻击(Output Merging Attack)应用于整个区块链,从创始区块到2020年4月15日的第2077094区块。在算法迭代到无法推断任何更多的输入时,部分或完全可推断的交易的百分比已经近零超过两年,这表明RingCT和增加mixin的组合在减少门罗币交易的可追溯性方面相当成功。

2.2　输出合并攻击

如图3,Tx1是一个使用多个mixin的输入的事务,它有两个输出key-a和key-b。TX2是另一个事务,它有两个由 I_1 和 I_2 表示的输入。每个输入都有多个mixin,I_1 和 I_2 都包含TX1的输出。如果满足以上条件,那么使用虚线表示的输入密钥key-a和key-b是在TX2中使用的真正密钥,也就是Tx2的真实输入。

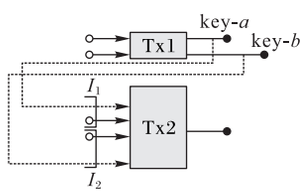

图3　输出合并攻击示意图

Fig. 3　Schematic diagram of output merging attack

这个攻击方法成立的前提是假设选择同一个交易的mixin时,算法被设计为不会选择同一个交易的输出。如果算法没有能够避免这种情况,那么很可能出现同一个交易几个mixin来自同一个交易输出的情况,那么毫无疑问会降低门罗币的匿名性。Kumar等[30]通过实验证实了这一假设,并验证了这个方法的正确性。

可以看到这种方法是可以运用在RingCT出现之后的版本上进行攻击的,因为这种攻击并没有从交易的金额出发。但是这样的方法并没能在文献[30]实验中得到验证,因为2017年RingCT刚刚应用,使用RingCT的区块还不是很多。该方法并没有受到后续研究的重视,在文献[31]中没有提及,而文献[32]中也没有再次验证。但是就实验结果而言,这个方法不同于前面的方法,输出合并攻击对于更多mixin的输入影响更大,且正确率很高。

由于0-mixin攻击的正确率可以认为是100%,可以使用0-mixin攻击追踪的结果来验证其他正确性稍弱的攻击方法。本文定义这3个概念,以便于对实验结果的解释。

定义4　TP(True Positive)。代指由被验证攻击破解出来的真实输入和由0-mixin攻击破解出来的真实输入一致的

交易。

定义 5 FP(False Positive)。是指由被验证攻击破解出来的真实输入与由 0-mixin 攻击破解出来的真实输入不一致的交易。

定义 6 UP(Unknown Positive)。是指由被验证攻击破解出来的真实输入,但是没有办法得到 0-mixin 攻击破解验证的交易。

研究验证了输出合并攻击的准确性和在多 mixin 样本追踪情况下的优越性。0-mixin 的攻击破解结果可以看作一定是正确的,而实验发现两个攻击方法不一致的 FP 非常少,即证明了输出合并攻击的有效性。0-mixin 攻击具有弊端,对较多 mixin 混合的样本攻击有效性极大降低,可破解出的多 mixin 样本的数量也减少,导致能够得到验证的输出合并攻击的多 mixin 破解样本无法得到验证,产生了很多的 UP。而这些大量的 UP 显示了输出合并攻击对于多 mixin 样本破解相较于 0-mixin 攻击的优越性,输出合并攻击可以追踪出 0-mixin 攻击可追踪的交易范围之外的很多交易,甚至在多 mixin 交易的情况下表现优于 0-mixin 攻击[30]。

2.3 最新猜测攻击

基于前面两种方法的结果,Kumar 等[30]经过统计分析又提出了最新猜测攻击(Guess-Newest Attack)。即给定一组用于创建环签名的输入密钥,实际使用的密钥是具有最高块高度的密钥,其中它显示为未花费的 TXO。也就是说,算法选择的 mixin 大多来自更早之前的输入,而非最新的输入。这个攻击的猜测是基于这样的推断,即最新的输入可能是在最新的 100 个区块里面,而更多更早的输入则存在于 100 000 个之前的区块中,显然,旧的输入被抽中当作 mixin 的几率要更大。

Kumar 等[30]用 0-mixin 攻击的结果对最新猜测攻击进行了测试,TP 的占比为 98.1%。这说明截至 2017 年门罗币的绝大多数交易输入的最新输入密钥是其中真正真实的输入。门罗币的开发人员为了避免这个问题,自 2015 年 4 月 5 日以来决定从三角分布中抽取混合样本[26]。三角形分布给较新的 TXO 提供了比旧的更高的概率,而非像之前混合输入是从一个均匀的分布中采样的,因此可以抵御最新猜测攻击。

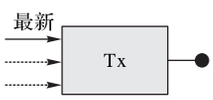

图 4 最新猜测攻击示意图

Fig. 4 Schematic diagram of guess-newest attack

Möser 等[31]运用蒙特卡罗模拟(Monte Carlo Simulation)来检验最新猜测攻击的正确性。他们使用门罗币所使用的 mixin 抽取策略从 0-mixin 攻击已经推断出来的交易数据中抽取 mixin 来作为模拟的交易,并统计最新猜测攻击的正确性。结果是比较好的,总的正确性达到 92.33%。

值得注意的是,2020 年文献[32]中对这个方法进行了再次验证,结果显示,在 RingCT 后(2017 年 1 月)的交易,最新猜测攻击的准确性急剧下降。对于具有 10 个混合素的输入(其中包括自 2018 年秋季以来的所有输入,当每个事务的 mixin 数量固定在 10 时),可以看到该方法的正确性下降到仅剩三成,从大约 90% 下降到大约 30%。这说明三角分布策略和 RingCT 的使用对于最新猜测攻击是十分有效的,极大保护了匿名性。

几个因素导致了最新猜测攻击的准确性下降。首先,RingCT 使得输入和输出金额被隐藏[28]。这意味着现在可以使用任何 RingCT 输出作为 mixin。在 RingCT 之前,只能使用与实际 TXO 相同的 TXO,这极大减少了可以从 mixin 中选择的 TXO 集。第二,mixin 的选择策略已经发生了改变,三角分布选择 mixin 使得近期的 mixin 的权重增大,更容易被选为 mixin,也减小了最新的一个输入密钥为真实输入的几率。

2.4 封闭集攻击

Yu 等[27]首先提出了封闭集攻击(Closed Set Attack),这种攻击是基于这样一个事实,即 n 个交易输入将必须使用 n 个不同的公钥作为实际输入,因为每个公钥只能被真实地使用一次。如果一组输入的数量等于包含的不同公钥的数量,则这一组输入称为封闭集。出现在封闭集中的密钥被视为已经花费的真实输入,那么这些密钥再次在封闭集之外的其他输入中出现,就一定是 mixin 了,可以直接被剔除以减小有效匿名集[2]。这种攻击就是找到所有可能的封闭集,并把在封闭集之外出现的与封闭集中相同的公钥都剔除,以不断减小有效匿名集大小,增加可推断性。

如图 5,假设有这样 4 个交易,每个交易都只有一个输入,Tx1 的输入包括{key-1,key-2,key-3},Tx2 的输入包括{key-2,key-3},Tx3 的输入包括{key-1,key-3},Tx4 的输入包括{key-1,key-2,key-3,key-4}。Tx1、Tx2、Tx3 的交易的输入数量为 3,在这 3 个交易中使用的公钥的数量为 3,与输入数量相同,也就是说,Tx1、Tx2、Tx3 这 3 个交易的输入构成了一个封闭集。由于有 3 个输入,那么必须要有 3 个真实输入的公钥,而封闭集中总共只有 3 个公钥,key-1、key-2、key-3 无论在哪个交易中被花费,都可以确认为已经被花费了。那么可以推断,Tx4 的输入中 key-1、key-2、key-3 都为 mixin,而真实的输入密钥就是 key-4。

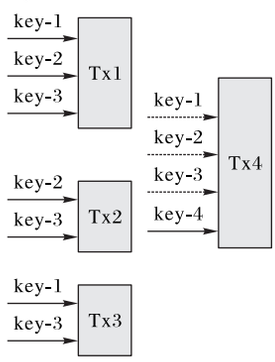

图 5 封闭集攻击示意图

Fig. 5 Schematic diagram of closed set attack

封闭集攻击的优点在于,对于 RingCT 是可用的,因为不涉及面值;但是封闭集攻击的效果并不太好,对于级联效应攻击后的数据集,只能进一步跟踪 0.084% 的输入。而这种攻击的攻击代价是很大的,理论上可行,但是实际来说对于一个如此大的数据集,这样的计算量是不可接受的。如果数据集中输入密钥数量的平均数为 m,找到所有的封闭集需要

的算法复杂度经过优化后最小为$O(m*N^2)$[27]。

2.5　泛洪攻击

泛洪攻击(Transaction Flooding Attack)由 Chervinski 等[33]首先提出,其核心很简单,掌握尽可能多的已知密钥以便将这些密钥从不可能的交易中剔除来缩小有效匿名集确定可追踪输入。可确定的密钥有两种:一种是已知已经在之前某些交易中被花费的密钥,第二种是在手中却没有被花费的密钥。成功的泛洪攻击的主要挑战是拥有足够的密钥作为已知的密钥库,以便系统从攻击者的一组密钥中选择输入的所有混合。要拥有输出密钥,攻击者必须使用有效的事务来淹没网络,最好是使用非常低的成本,从而使攻击可行。如图 6,当攻击者在链上通过制造很多交易获得大量已知密钥,用这些已知密钥去检验链上的其他交易,若交易中的 key-1 和 key-2 都在已知密钥集中,则可以排除在此交易中花费,那么剩下的 key-3 就是真实的输入了。

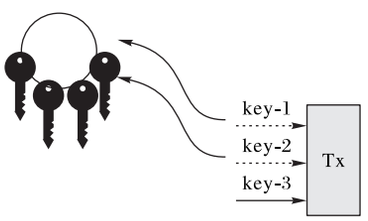

图 6　泛洪攻击示意图

Fig. 6　Schematic diagram of transaction flooding attack

门罗币的系统从过去 1.8 d 产生的输出键中选择 50% 的 mixin,其余 50% 的 mixin 是从旧的事务输出中选择的。要创建自己的输出密钥,攻击者必须向自己的地址发送付款。这些事务将生成新的输出密钥,这些密钥将由攻击者拥有。每个事务输出只用花费 1 piconero(10^{-12} XMR)。对于攻击者来说,创建有效交易的成本主要是交易费用。文献[33]探索了采用每个交易多少个输入时经济和时间成本最低,探索了制造多少交易与最终可破解的交易占比之间的关系,探索了该方法在不同的门罗币版本上的成本和效果。

相较于一些高成本的计算和门罗币本身的价值而言,泛洪攻击的成本非常低。实验发现,攻击者仅需要花费 9.253 XMR 或 582.19 美元的交易费用,就可以在一年内控制 50% 的输出密钥。导致这一结果有两个原因:一是 RingCT 使用后币值不再显示出来,因此 mixin 的选择可以不需要选择相同币值的 mixin,这样就降低了泛洪攻击的成本,使得创建一个新的输入变得十分便宜,可以低成本地建立起一个已知的密钥库;第二,门罗币的级联效应,在掌握一些已知密钥的时候,可以推断出更多的密钥,而这些新的密钥又增加了已知密钥库,从而便于推断出更多的密钥。

事实上采用如此低廉的手段,可以使得如此高比例的门罗币交易可追踪,对于整个门罗币网络的匿名性打击是致命的。显然,门罗币的设计者认为这样的攻击成本很高以至于不可实现,但是他们没有考虑到 RingCT 对这一成本的完全摒弃。RingCT 很好地解决了 0-mixin 攻击等可以从币值上出发来进行破译的方法[9],但是却被泛洪攻击这样的攻击破译。泛洪攻击几乎是目前所有的攻击中对 RingCT 真正有效的方法。

2.6　恶意远程节点攻击

远程恶意节点攻击(Tracing Attacks from Remote Nodes)由 Lee 等[34]首先提出。文献[34]不仅提出了攻击的方法,还设计了如何抵御这种攻击的机制。

2.6.1　门罗币客户端与远程节点运作方式

在解释攻击之前,首先描述门罗币客户端和远程节点的运作方式,Cao 等[35]详细解释了门罗币的网络结构。当门罗币客户端启动交易时,它首先查询远程节点以获得有关块链的信息。接收到的信息中包括最大全局索引,钱包将使用该索引来确定交易中包含哪些 mixin。钱包对候选输出(按全局索引)进行采样,以用作 mixin。为了避免揭示哪一个是真正的输入,客户端还将 mixin 的索引和真正的输入一起包含到请求中,尽管这些冗余数据已经由钱包存储[36]。输出请求通过 get_outs. bin 的应用程序接口(Application Programming Interface, API)端点发送到远程节点,该端点将返回每个请求的所包含的密钥。当收到 get_outs. bin 的响应时,客户端执行部分验证:如果客户端的这些密钥(已经存储在钱包中)不在返回的响应中,则事务被中止,并向用户显示错误。在钱包接收到所有的密钥后,它从这些密钥中统一选择最终的 mixin 数量,并将它们与真正的密钥一起形成事务。在确认交易之后,客户端将这些输出标记为已花费状态,并将交易传输到远程节点,如图 7 所示。

图 7　门罗币客户端与远程节点运作方式示意图

Fig. 7　Schematic diagram of operation mode between Monroe client and remote node

2.6.2　恶意远程节点攻击原理与举例

首先对上面描述的客户端行为进行观察:如果远程节点返回无效响应并在客户端触发异常,则客户端中止交易并向用户显示消息。如果用户再次尝试启动相同的交易,客户端软件将重新开始处理,包括采样所有要作为 mixin 使用的新输出。最终的结果是将两个查询发送到远程节点,而这两次请求中包含的几个密钥中相交的那个,就是真实的输入。

如图 8,假设第一次客户端发出请求,消息中包含 $L1=\{key\text{-}1, key\text{-}2, key\text{-}3, key\text{-}4\}$;当节点返无效响应,用户再次启动相同的交易,客户端采集了不同的 mixin,发送的消息中包含 $L2=\{key\text{-}1, key\text{-}5, key\text{-}6, key\text{-}7\}$。那么可以推断出,$L1 \cap L2=\{key\text{-}1\}$,key-1 就是真实的输入。

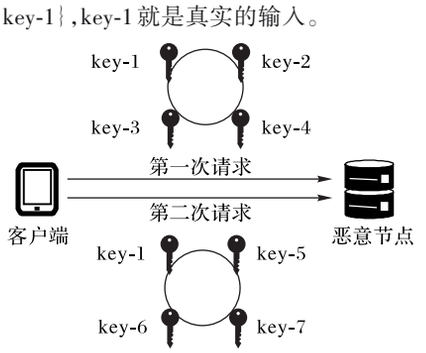

图 8　恶意远程节点攻击示意图

Fig. 8　Schematic diagram of tracing attacks from remote nodes

2.6.3 恶意远程节点攻击有效性评价

恶意远程节点攻击是利用了门罗币系统消息传递的不安全性和节点间通信的验证漏洞。目前节点间的通信还使用简单的明文 HTTP(Hyper Text Transfer Protocol)来传输 JSON(JavaScript Object Notation)文件[34],没有使用加密的可信信道,因此恶意节点可以没有障碍地获得信息,从而从获取的信息中推断出真正的输入。但是保密学发展十分完备,这些问题如果得到门罗币开发人员的重视,可以在新的更新中应用加密、握手协议等很容易地解决。

2.7 钱包环攻击

钱包环攻击(Monero Ring Attack)由 Wijaya 等[37]提出。由于 Monero 系统只检查提交的事务的有效性,环签名的构造完全由钱包处理[38],Wijaya 等[37]使用自己编写的钱包完成攻击。钱包环攻击包括 3 个阶段:

准备阶段 攻击者需要有一些未使用的输出 TXO,数量要大于系统允许的环签名的最小尺寸。

启动阶段 假设有 r 个密钥属于集合 L,那么创建 r 个输入,也就是 r 个环,r 个密钥的 TXO 在 r 个输入中被消耗。每个环的 mixin 的选择也都从集合 L 中来。

攻击阶段 被动攻击:当其他的输入选择到 L 中的密钥作为 mixin 时,可以很容易得知这几个 mixin 不是真实的输入,可以把这几个 mixin 剔除,从而减小了有效匿名集大小。主动攻击:让被攻击者使用一个恶意的钱包,这个钱包创建的交易所选择的 mixin 都是从 L 中选择的。由于这些密钥已知已经被花费,所以真正的输入就是在 L 集合外的那个密钥。

如图 9,先准备 5 个没有花费的输出 L={key-1,key-2,key-3,key-4,key-5},在交易 Tx1、Tx2、Tx3、Tx4、Tx5 中分别把这 5 个输出作为输入,并为每一个输入创建 1 个 5 密钥的环,其余的 4 个 mixin 都来自 L,那么就确保了这 5 个密钥都是已经被花费了的输入。被动攻击类似封闭集攻击,事实上启动阶段的过程就是在创造封闭集的过程,输入的大小和密钥的个数都是 5,那么当在其他的交易输入中出现的时候,就可以判断是 mixin 而非真实的输入予以剔除。如图 9 中 Tx6,由于 key-1、key-2 已经被花费,这个交易的真实输入只能从 key-6、key-7、key-8 中产生,由此有效匿名集的大小减小为 3。主动攻击则是使用一个恶意的钱包,这个钱包的功能是实现在创建环的时候,选择的 mixin 都来自 L,如图 9 中 Tx7,创建一个新的输入时,除了真实的新的输入,其余的密钥都来自 L,那么那个唯一不来自 L 的 key-6 就是真实的输入,从而实现了追踪。

Wijaya 等[39]提出了一种可以缓解钱包环攻击的方法,利用哈希函数来检测出重复出现多次的 mixin,并提出改进门罗币守护进程,增加鉴别限制 mixin 重复使用多次的机制,来防止钱包环攻击。Wijaya 等[39]还提出了钱包环攻击的改进方法,来躲避他们前面提到的鉴别,在创建环的时候有规律地分布各个公钥以达到既全部花费又减少公钥被重复的次数。

钱包环攻击方法中的主动攻击确实可以 100% 确定真实的输入从而实现追踪,而且如果掌握的密钥越多,破解的可能性越大。而且由于 RingCT 的应用,币值不再是问题,可以只使用小额的输入来创建为了攻击的交易,降低了这个方法的使用费用。钱包环攻击主动攻击的前提是这个钱包被追踪人所用,而要达到这个目的却非常难。要是通过被动攻击方法,则需要创建大量的交易输入,在区块中加入自己已知的密钥,而每加入一个密钥,就需要相应产生一笔输入并创建一个环。要真正实现在成千上万个区块中达到现实的可追踪性,那么需要创建数以万计的输入才能实现,无论是从时间还是经济成本来说都不是一个简便的方法。

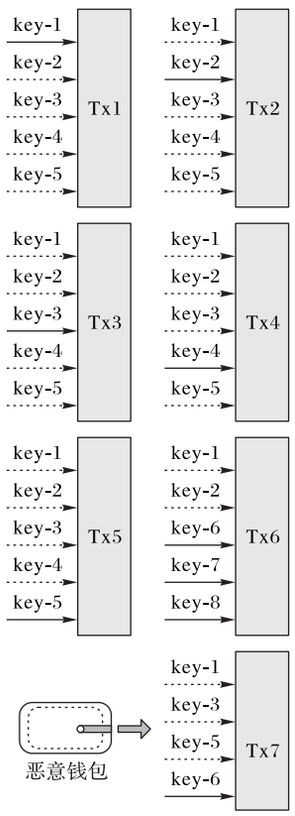

图 9 钱包环攻击示意图

Fig. 9 Schematic diagram of Monero ring attack

3 结语

目前对于门罗币匿名技术和追踪技术的评价和讨论的综述性文献比较少,评价大多还来自每个提出新方法的研究前列出的相关研究。但 Yu 等[15]对门罗币追踪技术和门罗币的不可追踪性进行了总结和反思。Yu 等[15]认为文献[30-31]只考虑了一个只能观察区块链公共信息的被动攻击者,并没有总结和评价文献[33,37]主动攻击方法的优劣。他们还讨论了如何评价不可追踪性,提出要从个体不可追踪性和全局不可追踪性两个角度来思考的方法。Hinteregger 等[40]也总结了除了钱包环攻击和远程恶意节点攻击之外的追踪技术,并且对 Kumar 等[30]的方法进行了跨链的验证。除此之外,Borggren 等[41]尽管没提出新的方法,但是引入了机器学习的方法,该技术可以用来辅助识别个人和群体。

本文通过前面部分的综述得到如下几点结论:

结论 1 门罗币的匿名技术和追踪技术呈现出相互促进的特点。0-mixin 攻击的出现迫使门罗币提高 mixin 使用的最

低限度,也降低了使用 mixin 的成本以诱导用户使用 mixin。最新猜测攻击的出现也使得门罗币改变了 mixin 的选择策略以避免最新的 TXO 总是成为真实的输入[26]。为了防止从币值出发的各种方法,也为了提高 mixin 可选择的范围,RingCT 成功隐藏了币值,使得从币值出发的追踪方法彻底失效。同时这些匿名技术的进步也催生了新的追踪技术。

结论 2　RingCT 的应用是一把双刃剑,它既使从币值出发的被动攻击方法失效,也使主动攻击方法更加容易。RingCT 出现使得被动攻击方法失效。RingCT 的应用使得传统的 0-mixin 攻击、最新猜测攻击等失效,Ye 等[32]对这些方法验证后发现,新区块上可追踪的交易占比几乎降至 0%。RingCT 的出现使得主动攻击方法变得更加有效。RingCT 的出现极大降低了泛洪攻击的成本使得泛洪攻击变得可行,不难想象,如果有对于门罗币追踪的商业性质的需求,泛洪攻击或许会成为攻击者针对 RingCT 的有力攻击武器。诸如钱包环攻击等的方法,也因为 RingCT 隐藏币值使得 mixin 可以从任意其他交易地址中选择的特性而变得成本很低。

结论 3　输出合并攻击和 0-mixin 攻击具有互补作用。实验证明这两种方法的追踪准确性很高,且具有互补的优势。0-mixin 攻击在较少 mixin 的交易中有效性更高,而输出合并攻击在高 mixin 的交易追踪中具有优势,可以追踪出 0-mixin 攻击追踪范围之外的交易。如果单纯利用传统的被动攻击方法,将两者集合起来使用,可以最大限度提高被动攻击方法的有效性。

结论 4　门罗币的系统安全链条仍待理顺。恶意远程节点攻击的成功和钱包环攻击的成功说明门罗币的体系存在安全漏洞。恶意远程节点攻击的成功是基于门罗币的远程节点和客户端之间的通信是公开的、未经加密的,这些交易信息相当于在传输中透明。钱包环攻击的成功基于门罗币系统放任门罗币钱包自己产生环而不加严格的检查,这种宽容性对门罗币的应用有利,但是破坏了门罗币的安全性。Lee 等[34]已经将恶意远程节点攻击的漏洞通报给了门罗币社区,目前该漏洞已经修复。

目前来说,大多研究都从门罗币交易信息等外部特征出发,很少有从门罗币本身机制出发的追踪探索,目前只有恶意远程节点攻击使用了密码学的相关知识来进行追踪。而匿名数字货币作为密码学知识的一种应用,从密码学角度出发的本身机制的探索可能会提供更加有力的科学的追踪方法。未来对于门罗币追踪的研究突破,可能存在于从内部机制或者运营系统等角度出发的追踪方法。

参考文献(References)

[1] LUNTOVSKYY A, GUETTER D. Cryptographic technology blockchain and its applications [C]// Proceedings of the 2018 International Conference on Information and Telecommunication Technologies and Radio Electronics, LNEE 560. Cham: Springer, 2019: 14-33.

[2] REDDY E, MINNAAR A. Cryptocurrency: a tool and target for cybercrime [J]. Acta Criminologica: African Journal of Criminology, 2018, 31(3): 71-92.

[3] IRWIN A S M, URNER A B. Illicit Bitcoin transactions: challenges in getting to the who, what, when and where[J]. Journal of Money Laundering Control, 2018, 21(3): 297-313.

[4] IRWIN A S M, MI8LAD G. The use of crypto-currencies in funding violent jihad[J]. Journal of Money Laundering Control, 2016, 19(4): 407-425.

[5] 乔晶花. 全球毒情新趋势与国际治理新挑战[J]. 现代世界警察, 2020(9): 13-17. (QIAO J H. Global drug abuse and its challenge to drug control [J]. Modern World Police, 2020(9): 13-17.)

[6] RÜTH J, ZIMMERMANN T, WOLSING K, et al. Digging into browser-based crypto mining[C]// Proceedings of the 2018 Internet Measurement Conference. New York: ACM, 2018: 70-76.

[7] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. [2021-01-01]. https://btcpapers. com/bitcoin. pdf.

[8] HARRIGAN M, FRETTER C. The unreasonable effectiveness of address clustering[C]// Proceedings of the 2016 International IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress. Piscataway: IEEE, 2016: 368-373.

[9] van SABERHAGEN N. CryptoNote v2. 0[EB/OL]. [2021-01-01]. https://cryptonote. org/whitepaper. pdf.

[10] DUFFIELD E, DIAZ D. Dash: a payments-focused cryptocurrency [EB/OL]. [2021-01-01]. https://github. com/dashpay/dash/wiki/Whitepaper.

[11] BEN SASSON E, CHIESA A, GARMAN C, et al. Zerocash: decentralized anonymous payments from Bitcoin[C]// Proceedings of the 2014 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2014: 459-474.

[12] 门罗币官网中文版[EB/OL]. [2021-01-01]. https://www. xmr-zh. com/. (Official website of Monero — Chinese Version [EB/OL]. [2021-01-01]. https://www. xmr-zh. com/.)

[13] WIJAYA D A, LIU J K, STEINFELD R, et al. On the unforkability of Monero[C]// Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security. New York: ACM, 2019: 621-632.

[14] SINGH K, HEULOT N, HAMIDA E B. Towards anonymous, unlinkable, and confidential transactions in blockchain [C]// Proceedings of the 2018 IEEE International Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology. Piscataway: IEEE, 2018: 1642-1649.

[15] YU J S, AU M H A, ESTEVES-VERISSIMO P. Re-thinking untraceability in the CryptoNote-style blockchain[C]// Proceedings of the IEEE 32nd Computer Security Foundations Symposium. Piscataway: IEEE, 2019: 94-107.

[16] LIU J K, AU M H, SUSILO W, et al. Linkable ring signature with unconditional anonymity [J]. IEEE Transactions on Knowledge and Data Engineering, 2014, 26(1): 157-165.

[17] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret [C]// Proceedings of the 2001 International Conference on Theory and Application of Cryptology and Information Security, LNCS 2248. Berlin: Springer, 2001:552-565.

[18] SILVERMAN J H. The Arithmetic of Elliptic Curves, GTM 106 [M]. 2nd ed. New York: Springer, 2009:376-386.

[19] SUN S F, AU M H, LIU J K, et al. RingCT 2. 0: a compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency Monero[C]// Proceedings of the 2017

European Symposium on Research in Computer Security, LNCS 10493. Cham: Springer, 2017: 456-474.

[20] LIU J K, WEI V K, WONG D C. Linkable spontaneous anonymous group signature for ad hoc groups[C]// Proceedings of the 2004 Australasian Conference on Information Security and Privacy, LNCS 3108. Berlin: Springer, 2004: 325-335.

[21] NOETHER S, NOETHER S. Monero is not that mysterious: MRL-0003 [R/OL]. (2014-09-25) [2021-01-01]. https://web.getmonero.org/ru/resources/research-lab/pubs/MRL-0003.pdf.

[22] The Monero Project. MiniNero: a Python reimplementation of the one-time ring signatures as found in Monero[CP/OL]. [2021-01-01]. https://github.com/monero-project/mininero.

[23] FUJISAKI E, SUZUKI K. Traceable ring signature [C]// Proceedings of the 2007 International Workshop on Public Key Cryptography, LNCS 4450. Berlin: Springer, 2007: 181-200.

[24] MERCER R. Privacy on the blockchain: unique ring signatures[R/OL]. (2016-12-25) [2021-01-01]. https://arxiv.org/pdf/1612.01188.pdf.

[25] NOETHER S. Ring signature confidential transactions for Monero [EB/OL]. (2015-12-17) [2021-01-01]. https://eprint.iacr.org/2015/1098.pdf.

[26] The Monero Project. Monero: triangular distribution to choose recent outputs more often for mixins [CP/OL]. [2021-01-01]. https://github.com/monero-project/monero/commit/f2e8348be0c91c903e68ef582cee687c52411722.

[27] YU Z X, AU M H, YU J S, et al. New empirical traceability analysis of CryptoNote-style blockchains[C]// Proceedings of the 2019 International Conference on Financial Cryptography and Data Security, LNCS 11598. Cham: Springer, 2019: 133-149.

[28] NOETHER S, MACKENZIE A, The Monero Research Lab. Ring confidential transactions[J]. Ledger, 2016, 1: No. 34.

[29] Official site of Monero. Moneropedia — RingCT[EB/OL]. [2021-01-01]. https://www.getmonero.org/resources/moneropedia/ringCT.html.

[30] KUMAR A, FISCHER C, TOPLE S, et al. A traceability analysis of Monero's blockchain[C]// Proceedings of the 2017 European Symposium on Research in Computer Security, LNCS 10493. Cham: Springer, 2017: 153-173.

[31] MÖSER M, SOSKA K, HEILMAN E, et al. An empirical analysis of traceability in the Monero blockchain[J]. Proceedings on Privacy Enhancing Technologies, 2018, 2018(3): 143-163.

[32] YE C, OJUKWU C, HSU A, et al. Alt-coin traceability[EB/OL]. (2020-07-07) [2021-01-01]. https://eprint.iacr.org/2020/593.pdf.

[33] CHERVINSKI J A M, KREUTZ D, YU J S. FloodXMR: low-cost transaction flooding attack with Monero's bulletproof protocol[EB/OL]. (2019-05-10) [2021-01-01]. https://eprint.iacr.org/2019/455.pdf.

[34] LEE K, MILLER A. Authenticated data structures for privacy-preserving Monero light clients[C]// Proceedings of the 2018 IEEE European Symposium on Security and Privacy Workshops. Piscataway: IEEE, 2018: 20-28.

[35] CAO T, YU J S, DECOUCHANT J, et al. Exploring the Monero peer-to-peer network[C]// Proceedings of the 2020 International Conference on Financial Cryptography and Data Security, LNCS 12059. Cham: Springer, 2020: 578-594.

[36] HEILMAN E, KENDLER A, ZOHAR A, et al. Eclipse attacks on Bitcoin peer-to-peer network[C]// Proceedings of the 24th USENIX Security Symposium. Berkeley: USENIX Association, 2015: 129-144.

[37] WIJAYA D A, LIU J, STEINFELD R, et al. Monero ring attack: recreating zero mixin transaction effect[C]// Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering. Piscataway: IEEE, 2018:1196-1201.

[38] LIU Q Y, LIU Z, LONG Y, et al. Making Monero hard-to-trace and more efficient[C]// Proceedings of the 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering. Piscataway: IEEE, 2019: 514-521.

[39] WIJAYA D A, LIU J, STEINFELD R, et al. Anonymity reduction attacks to Monero[C]// Proceedings of the 2018 International Conference on Information Security and Cryptology, LNCS 11449. Cham: Springer, 2019: 86-100.

[40] HINTEREGGER A, HASLHOFER B. Short paper: an empirical analysis of Monero cross-chain traceability[C]// Proceedings of the 2019 International Conference on Financial Cryptography and Data Security, LNCS 11598. Cham: Springer, 2019: 150-157.

[41] BORGGREN N, KIM H Y, YAO L H, et al. Simulated blockchains for machine learning traceability and transaction values in the Monero network[EB/OL]. (2020-01-12) [2021-01-01]. https://arxiv.org/pdf/2001.03937.pdf.

This work is partially supported by "333 High-Level Talent Training Engineering" Science Research Project of Jiangsu (BRA2020276), Nanjing University 2021 Innovation and Entrepreneurship Big Data and Theoretical Research Innovation and Entrepreneurship Project.

LIN Dingkang, born in 2001. His research interests include blockchain, digital currency.

YAN Jiaqi, born in 1983, Ph. D., associate professor. His research interests include blockchain, information system, data analysis, information science.

BA Nandeng, born in 1999. Her research interests include blockchain, ring signature, anonymous digital currency.

FU Zhenhao, born in 2001. His research interests include blockchain, information system.

JIANG Haochen, born in 2001. His research interests include information system, blockchain, zero-knowledge proof.