FloodXMR: экономичная флуд-атака на транзакции, использующая возможности протокола Bulletproof Monero[*]

Джао Отавио Массари Червинский (João Otavio Massari Chervinski)[1], Диего Крюц (Diego Kreutz)[1, 2] и Янгшан Ю (Jiangshan Yu)[3]

[1] Федеральный университет Пампы, Alegrete-RS, 97546-550, Бразилия
[2] Люксембургский университет, CritiX/SnT, Esch-sur-Alzette, L-4364, Люксембург
joaootaviors@gmail.com, kreutz@acm.org
3 Университет Монаша, Melbourne, VIC 3800, Австралия
jiangshan.yu@monash.edu

Аннотация

Monero — одна из первых и самых популярных криптовалют, решающих проблемы анонимности, присущие другим монетам, таким как Bitcoin. Monero имеет рыночную капитализацию более одного миллиарда долларов США и, по данным CoinMarketCap, на 17 апреля 2019 оценивается как 12-я из самых ценных криптовалют. Эта цифровая монета обеспечивает различные механизмы защиты пользователей, такие как сложные ключи или миксины, позволяющие скрыть входы транзакций. Однако, несмотря на все попытки защитить анонимность пользователей Monero, нападения, направленные на отслеживание транзакций, по-прежнему возможны. Наш вклад состоит из двух частей. Во-первых, мы предлагаем и оцениваем новый вариант флуд-атаки, направленный на отслеживание транзакций, FloodXMR. Во-вторых, нами приводится анализ затрат, необходимых проводящему атаку для реализации FloodXMR. Мы демонстрируем, как проводящий атаку может в своих интересах использовать протокол Bulletproof Monero, снижающий размер комиссий за проведение транзакций, чтобы «наводнить» сеть собственными транзакциями и в последствии удалить миксины из входов транзакций. При заданных временных рамках атаки, составляющих 12 месяцев, полученные нами результаты демонстрируют, что злоумышленник может отследить до 47,63% входов транзакций при затратах всего 1746,53 долларов США. Кроме того, мы также показываем, что наш алгоритм отслеживания повлиял более чем на 90% входов.

Ключевые слова: Monero, анонимность, отслеживаемость, атака.

1 Введение

Шумиха вокруг Bitcoin [7] и более новых криптовалют привела к быстрому развитию инноваций в области платежных систем во всем мире. Одной из основных причин, стоящих за таким ускоренным распространением цифровых валют, является новая распределённая структура данных под названием блокчейн. Блокчейны позволяют создавать децентрализованные не требующие доверия сети, в которых различные стороны могут участвовать в проведении транзакций без какой-либо необходимости в доверии к третьим сторонам, действующим в качестве посредников. В сети Bitcoin участники достигают консенсуса по валидности блоков, используя алгоритм доказательства работы (PoW), предполагающий решение вычислительной задачи. Транзакции, проводимые равноправными участниками сети, подтверждаются криптографическими подписями.

Однако стоит подчеркнуть, что криптомонеты, такие как Bitcoin, не регулируются центральной властью. Вместо этого такие цифровые монеты поддерживаются контрибьюторами со всего мира, и часто абсолютно любой человек имеет доступ как к исходному коду, так и к истории транзакций. В сети Bitcoin у каждого пользователя есть пара публичных и приватных ключей, которые используются для получения и отправки платежей, соответственно. У пользовательского кошелька

* Написание данной работы было частично поддержано Национальным исследовательским фондом Люксембурга (FNR) по гранту PEARL FNR/P14/8149128. Мы благодарим Марчело Резенде Тьело (Marcelo Rezende Thielo) за понимание и уделённое время.

есть адрес (хеш длиной 160 бит), на который можно получать средства. Поскольку такие адреса скрыты под псевдонимом и (предположительно) не раскрывают какой-либо информации о владельце, пользователи были уверены в том, что их транзакции Bitcoin являлись анонимными. Однако отчеты показали, что злоумышленники в состоянии связать адреса Bitcoin с IP-адресами и именами пользователей, найденными на форумах и веб-сайтах [1, 2, 5].

Monero стала одной из первых криптовалют, разработанных, чтобы решить проблемы анонимности (например, связывание данных пользователей с их адресами), которые были характерны для предыдущих цифровых монет. Чтобы обеспечить анонимность транзакций, в основу Monero был заложен протокол CryptoNote [9]. Этот протокол имеет две главные особенности. Во-первых, неотслеживаемость транзакций. При наличии входа транзакции с множеством выходов невозможно определить, какой из выходов использовался, чтобы провести оплату, что не позволяет отследить саму транзакцию. Во-вторых, несвязываемость адресов. Наличие двух различных адресов не позволяет связать оба адреса с одним и тем же пользователем.

В отличие от неизменяемых ключей, используемых такими криптовалютами, как Bitcoin, пользователи Monero имеют возможность использовать две пары ключей: одну пару ключей просмотра и одну пару ключей траты. При наличии публичных ключей просмотра и траты получателя отправитель может создать уникальный адрес для получения платежей. Этот уникальный ключ называют скрытым адресом. Он используется, чтобы защитить личность получателя транзакции. Наконец, информация отправителя защищена посредством ложных ключей, называемых миксинами. Миксины являются выходами предыдущих транзакций. Ложные выходы используются, чтобы скрыть реальный ключ платежа.

Несмотря на применение различных протоколов и механизмов защиты личных данных пользователей, Monero периодически становилась целью атак. Например, в предыдущих версиях системы недостатки технического решения и спецификаций позволяли злоумышленникам отслеживать большое количество входов транзакции [3, 6]. Один из первых недостатков позволял пользователям создавать транзакции вообще без каких-либо ложных выходов. Второй недостаток являлся «избирательностью» алгоритма выбора миксинов Monero, которая облегчала идентификацию реальных ключей платежа.

Атаки на анонимность транзакций, сохранённых в блокчейне Monero, являются попыткой использовать потенциально слабые места системы с целью выявления реальных ключей траты. Для предотвращения таких атак в последней версии Monero (версия 0.13.0) было введено правило, предполагающее обязательное использование постоянного количества ложных выходов, равного десяти, для каждого входа каждой транзакции. Как будет сказано ниже, количество миксинов значительно влияет на результаты проведения атак, направленных на выявление реальных входов. Например, в период с февраля 2017 по февраль 2018 минимальное обязательное количество ложных выходов было меньше, что позволило нам проследить до 89% ключей платежей за этот период при помощи нашей флуд-атаки. В период с февраля 2018 по февраль 2019 в системе Monero было увеличено минимальное (обязательное) количество ложных выходов (до 6 миксинов в марте 2018) и ввело фиксированное количество ложных выходов (10 миксинов на вход транзакции, начиная с октября 2018). В результате за последний указанный период нам удалось проследить примерно половину (47%) ключей платежа, о чём говорится в Разделе 4.

Нами предлагается и приводится оценка нового варианта флуд-атаки под названием FloodXMR, позволяющей проследить ключи платежей в блокчейне Monero. Несмотря на то, что идея довольно проста, то есть переполнить сеть Monero транзакциями, входы и выходы которых будут принадлежать проводящему атаку, нам необходимо решить некоторые проблемы и уделить внимание деталям, которые значительно влияют на результаты, например, на цепные реакции. Во-первых, комиссия за проведение транзакции пропорциональна её размеру в байтах, что означает, что проводящий атаку

должен тщательно выбрать экономичный размер. Во-вторых, так как 50% ложных выходов для входов транзакций выбираются за последние 1,8 дня, проводящему атаку необходимо создавать транзакции непрерывно. В-третьих, нами исследуются критические массовые реакции блокчейна Monero, поскольку это может почти удвоить количество отслеживаемых входов, о чём говорится ниже. В-четвертых, мы пытаемся довести до максимума количество выходов на транзакцию. В идеале проводящий атаку должен создать экономичные (не затратные) транзакции с максимально большим количеством выходов.

Наш основной вклад можно разбить на четыре части: (a) мы представляем новый вариант флуд-атаки на транзакции с целью отслеживания ключей платежа других пользователей системы Monero; (b) мы даём оценку эффективности атаки за два временных периода для блокчейна Monero (с января 2017 по январь 2018 и с февраля 2018 по февраль 2019); (c) нами производится анализ затрат, демонстрирующий, насколько дорогой может быть атака для каждого из указанных периодов; и (d) мы проводим анализ того, как протокол Bulletproof Monero помогает значительно снизить стоимость атаки.

Данная статья имеет следующую структуру. В Разделе 2 рассматриваются связанные с темой работы. В Разделе 3 мы представляет флуд-атаку на транзакции. В Разделе 4 мы оцениваем её, используя данные блокчейна Monero. Наконец, в Разделе 5 нами приводятся некоторые заключительные замечания.

2 Связанные работы

Насколько нам известно, ни одна из существующих стратегий не позволяла привязать реальную информацию к адресам пользователей из блокчейна Monero. Известные атаки против Monero, такие как изменение кода кошелька и персонификация удалённых узлов, ограничиваются раскрытием реальных ключей, потраченных во входах транзакции [3, 4, 10, 11]. В более ранних версиях Monero искажённые результаты алгоритма выбора миксинов и создание транзакций без каких-либо ложных выходов могли быть использованы проводящим атаку с целью прослеживания входов транзакций [3, 6]. Алгоритм при выборе миксинов для включения во вход транзакции отдавал предпочтение более старым выходам. Это приводило к тому, что ключ траты, являвшийся самым последним, то есть сгенерированный в самом высоком блоке среди всех миксинов, в случае более чем с 90% входов, создавался до того, как алгоритм обновлялся. Отсутствие ложных выходов допускалось в виду отсутствия каких-либо правил, устанавливающих минимальное количество миксинов для каждого входа. Входы без миксинов отслеживаемы, поскольку они содержат только потраченный ключ. Если бы потраченный ключ выбирался системой для включения в качестве миксина для будущей транзакции, то это можно было бы проигнорировать, поскольку он уже был потрачен ранее и, таким образом, не мог бы быть ключом, который тратится во входе. Такие стратегии позволяли злоумышленникам ставить анонимность Monero под угрозу путём простого анализа данных транзакций, содержащихся в блокчейне.

Код кошелька Monero также становился целью недавних атак [10]. Результаты показали, что злоумышленник может изменить код кошелька и, следовательно, выбрать миксины для определённого входа. Поскольку система не станет проверять, были или нет потрачены эти ключи в других входах той же транзакции, это позволит пометить все ключи в транзакции как потраченные, независимо от входа, в котором был потрачен каждый ключ. Создавая поддельную службу криптовалютного кошелька, проводящий атаку получает под свой контроль процесс выбора миксинов и может включать потраченные ключи в транзакции, создаваемые другими пользователями, существенно снижая гарантии анонимности, обеспечиваемые Monero.

Злоумышленник, чтобы отследить входы в сети Monero, также может использовать персонифицированные удалённые узлы [4]. Чтобы избежать сложной работы по созданию и

обновлению полной копии блокчейна, клиенты сети обычно полагаются на удалённые узлы для запроса информации транзакций и проведения платежей. После проверки возможных миксинов в запросе, оператор узла может прервать транзакцию клиента и ждать повторной попытки. После получения запроса повторной попытки проводящий атаку может определить реальный ключ, когда найдёт тот, который появляется в обоих запросах.

В недавней работе была предложена стратегия отслеживания входов транзакций путём нахождения замкнутых множеств публичных ключей, включенных во входы транзакций [11]. Замкнутое множество определяется как множество входов транзакций, в котором количество уникальных ключей по всем входам совпадает с количеством входов во множестве. В замкнутом множестве каждый публичный ключ должен быть потрачен в одном из входов во множестве и использован в качестве миксина в других входах. Это позволяет проводящему атаку определить выходы, которые уже были потрачены, и удалить их из других входов. Поскольку количество ложных выходов сокращается, анонимность входов транзакций ослабляется, что делает возможным проведение дальнейших атак.

В таблице 1 нами приводится краткий обзор различных атак, направленных против анонимности транзакций Monero. Как и ожидалось, все атаки основаны на анализе данных блокчейна с целью отслеживания входов транзакций. Некоторые атаки используют пассивные подходы. В этом случае выявляются определенные слабые места системы, такие как смещение в алгоритме выбора миксинов, которые затем используются для анализа и идентификации ключей платежа [3, 6]. Другие атаки основаны на активных подходах, например, создании дополнительных служб [4, 10] или изменении кода кошелька, что позволяет сделать транзакции отслеживаемыми.

Таблица 1. Сравнение атак, описанных в связанных работах

Работа	Анализ данных блокчейна	Изменение кода кошелька	Создание транзакций	Персонификация служб	Атакованные версии
3	×				До 0.9.0
6	×				До 0.9.0
10	×	×	×	×	Все версии
4	×			×	Все версии
11	×				Все версии
Наша атака	×		×		Все версии

3 Флуд-атака на транзакции

Допустим, есть транзакция Monero *tx* с одним входом *tx.in*, содержащим четыре ключа (*tx.in* = {pk_1, pk_2, pk_3, pk_4}), в то время как один из ключей (например, pk_4) представляет монету, которая тратится реально, а оставление три ключа используются в качестве ложных, чтобы спрятать реальный ключ, используемый в транзакции. Однако, если три из четырёх публичных ключей (например, pk_1, pk_2 и pk_3) принадлежат злоумышленнику, легко узнать, который из четырёх ключей является ключом платежа. Это один из самых основных принципов флуд-атаки на транзакции. То есть проводящему атаку необходимо владеть списком действительных выходов, и чтобы он был максимально большим.

Злоумышленник может удалить или пометить ключ pk_x входа транзакции, созданной другим пользователем, как известный, если ключ принадлежит ему/ей. Если проводящий атаку ещё не потратил ключ при проведении оплаты, то ему/ей известно, что pk_x используется в качестве ложного выхода. Второй вариант: если проводящему атаку известно, что ключ уже был потрачен в предыдущей транзакции (например, pk_4), тогда он/она также знает, что ключ является миксином. В обоих случаях ключ pk_x может быть безопасно удален из входа *tx:in* транзакции *tx*.

Предыдущий пример можно реализовать на практике путём проведения флуд-атаки на транзакции. Этот вариант атаки использует схему кольцевой подписи Monero, которая скрывает реальные входы, смешивая их с различными выходами (используемыми в качестве ложных), сгенерированными при проведении предыдущих транзакций. Ключевая идея флуд-атаки на транзакции проста. Человек, проводящий атаку, должен создать экономичные транзакции, чтобы построить большую базу знаний (то есть список выходов), из которой система могла бы выбрать выходы, которые будут использованы в качестве миксинов в будущих транзакциях. Как говорилось выше, если злоумышленнику известны все выходы, кроме одного из входа транзакции *tx:in*, то он/она может легко узнать, какой из ключей реально тратится в том входе транзакции.

В случае с Monero каждый раз, когда создаётся новая транзакция, в каждый вход включается минимальное количество миксинов (в зависимости от версии системы). Система выбирает миксины из выходов предыдущих транзакций и добавляет их к входу транзакции, как показано на рисунке 1. У каждого входа *tx:in* транзакции *tx* будет свой собственный набор миксинов. Наконец, воздаётся цифровая подпись, позволяющая принимающей стороне получить оплату. При этом такой стороне не известны ключи отправителя оплаты.

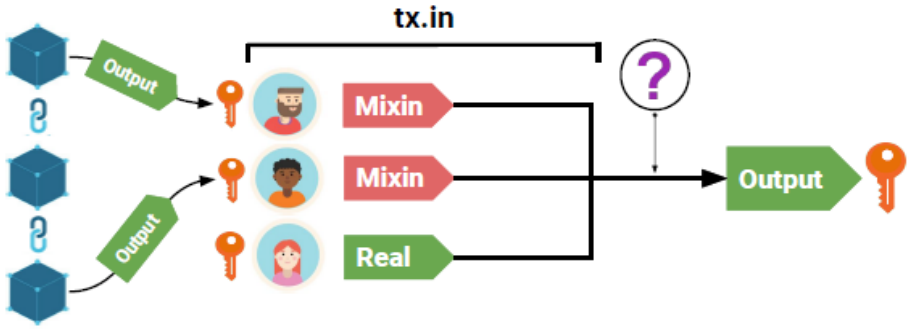

Рисунок 1. Кольцевая подпись Monero

Главной проблемой для успешного проведения флуд-атаки на транзакции является необходимость в наличии достаточного количества ключей, чтобы система выбрала все миксины входа *tx:in* из набора ключей злоумышленника. Чтобы завладеть выходами, проводящему атаку необходимо заполнить сеть действительными транзакциями, в идеале — очень экономичными (недорогими), что сделает атаку вполне реальной. Эти транзакции должны будут использовать ключи платежей и адреса получателя, имеющиеся у злоумышленника.

Количество выходов транзакции (используемых в качестве ложных в будущих транзакциях) непосредственно связано с количеством адресов, на которые должны быть получены монеты. Каждый принимающий адрес получит выход, содержащий некоторое количество монет (XMR). Эти выходы будут позднее отобраны системой в качестве миксинов будущих транзакций.

Стоит подчеркнуть, что у каждой транзакции есть комиссия. Эта комиссия используется для того, чтобы заплатить майнерам, которые выполняют вычислительную работу по валидации транзакции. Помимо этого, комиссия увеличивается вместе с размером транзакции, выраженном в байтах. Количество входов, миксинов и выходов напрямую влияет на размер транзакции. Наконец, что не менее важно, размер комиссии также варьируется в зависимости от текущего размера вознаграждения за блок и другими соответствующими значениями. Сумма, взимаемая в XMR за каждый килобайт данных транзакции, определяется уравнением 1[4].

$$\textit{Размер комиссии за Кбайт} = (R/R_0) \times (M_0/M) \times F_0 \times (60/300) \times 4 \qquad (1)$$

где:

4 https://ww.getmonero.org/2017/12/11/A-note-on-fees.html

R = базовое вознаграждение за блок;

R_0 = исходное базовое вознаграждение (10 XMR);

M = предельный размер блока для майнера, указываемый во избежание штрафа за превышение размера блока;

M_0 = фиксированный максимальный размер блока (300 Кбайт);

F_0 = 0,002 XMR

60/300 = поправочный коэффициент, учитывающий увеличение предельного значения размера блока с 60 до 300 Кбайт

4 = поправочный коэффициент множителя комиссии. По умолчанию транзакции используют значение 4 и y (минимальная комиссия) использует множитель равный 1.

К концу 2017 года размер комиссии за проведение транзакции достиг пикового среднего значения, составившего 20 долларов США[5]. Главным образом это случилось из-за бума на рынке криптовалюты. Данный пример показывает нам, что (в конечном счете) проведение флуд-атаки может стать довольно затратным. Мы полагаем, что это было одной из причин, почему этот вид атаки не исследовался разработчиками Monero.

В октябре 2018 сообществом Monero было объявлено о реализации протокола Bulletproof[6], который пришёл на замену *кольцевым конфиденциальным транзакциям* (RingCT) для решения задачи создания доказательств диапазона. Этот новый протокол позволяет генерировать криптографические доказательства, размер которых на 97% меньше размера доказательств, которые генерировались при помощи RingCT. Меньший размер доказательств снижает размер транзакций и, как следствие, размер комиссий. Если кратко, реализация протокола Bulletproof сделала флуд-атаку на транзакции ещё более интересной, что демонстрируется нами в Разделе 4.

3.1 Модель атаки

Поскольку блокчейн Monero открыт для любого, злоумышленник в состоянии получить доступ к данным, содержащимся в блокчейне Monero. Допустим, проводящий атаку человек готов заплатить некоторую (небольшую) сумму комиссий, чтобы проследить транзакции. Стоимость такой атаки рассматривается в Разделе 4.4.

Также допустим, что злоумышленником были созданы сто различных адресов кошелька Monero. Один из кошельков содержит ту сумму XMR, которая необходима, чтобы покрыть расходы на проведение атаки. Следует отметить, что создать новый кошелёк Monero легко и это не требует никаких дополнительных расходов. Сто адресов обеспечивают хороший баланс между размером транзакции (приблизительно 11 КБайт для транзакции с 1 входом и размером кольца, равном 11) и комиссией за проведение транзакции, о чём говорится в Разделе 3.2.

Наконец, допустим, что злоумышленник в состоянии создать столько транзакций, сколько он хочет в любой момент времени t, пока он в состоянии платить комиссии за проведение транзакций. При этом майнеры выбирают и проводят валидацию транзакций, то есть какие-либо гарантии по времени отсутствуют.

3.2 Переполнение сети Monero

Чтобы отследить входы, злоумышленнику необходимо создать большое количество выходов за время, в течение которого он/она хочет провести атаку. Отслеживаются только те транзакции, которые

5 https://bitinfocharts.com/comparison/monero-transactionfees.html
6 https://www.getmonero.org/2018/10/11/monero-0.13.0-released.html

были созданы с момента начала атаки. Как показано нами в Разделе 4, эффективность атаки повышается с увеличением количества времени, которое на неё отводится.

Система Monero выбирает 50% ложных выходов из всех выходов, сгенерированных за последние 1,8 дня. Остающиеся 50% миксинов выбираются из выходов более старых транзакций. Чтобы создать собственные выходы, проводящему атаку необходимо произвести платежи на свои собственные адреса. При проведении этих транзакций будут сгенерированы новые выходы, которыми будет владеть злоумышленник. Каждый выход транзакции может потратить всего 1 piconero (10^{-12} XMR). Для злоумышленника стоимость создания действительных транзакций, в основном, будет равна размеру комиссий.

На размер комиссии за проведение транзакции влияют криптографические механизмы, которые обеспечивают анонимность и безопасность, такие как доказательства диапазона, обеспечивающие безопасность передаваемой суммы и предотвращающие подделку монеты. С введением протокола Bulletproof Monero увеличение размера комиссии в зависимости от размера транзакции теперь происходит в соответствии с логарифмической функцией. Это означает, что Bulletproof значительно уменьшает стоимость транзакций со множеством выходов. При проведении флуд-атаки транзакциями используется только один адрес кошелька, чтобы заплатить 1 piconero за остальные девяноста девять адресов. На адрес платежа будет получена сдача.

Сто выходов на транзакцию представляется почти оптимальным выбором, поскольку это обеспечивает хороший баланс между размером транзакции, который составляет приблизительно 11 Кбайт, если у транзакции 1 вход, а размер кольца равен 11, и затратами, связанными с комиссией за проведение транзакции. Даже при том, что злоумышленник может создать транзакции с большим количеством выходов (например, 1000), затраты на выход будут снижаться очень медленно для транзакций, содержащих более 100 выходов, то есть использовать транзакции со слишком большим количеством выходов не стоит.

Стоит подчеркнуть, что большие транзакции будут выбраны майнерами с меньшей вероятностью, поскольку злоумышленник платит ту комиссию за проведение транзакции, которая положена по умолчанию. Большая транзакция занимает в блоке много места. С точки зрения майнера, он/она получит большее вознаграждение за большее количество транзакций поменьше, получив больше за килобайт.

Количество миксинов в каждом входе влияет на размер комиссии за проведение транзакции. Несмотря на то, что это было проблемой в случае с предыдущими версиями системы, начиная с версии 0.13.0 под названием Beryllium Bullet, размер кольца стал фиксированным и составляет 11. Это было сделано для обеспечения единообразия транзакций. Поэтому у каждого входа транзакции теперь точно есть 10 ложных выходов.

3.3 Алгоритм отслеживания

Переполнение сети транзакциями начинается с того, что злоумышленник создаёт новые транзакции. При проведении каждой транзакции он осуществляет 99 платежей, что приводит к созданию 99 выходов. Выходы транзакций злоумышленника сохраняются в едином списке, который будет использоваться для отслеживания входов в транзакциях других пользователей. Затем, после получения копии блокчейна Monero, процесс отслеживания будет заключаться в проверке входов всех транзакций, созданных с момента начала атаки. Выходы, принадлежащие проводящему атаку, удаляются из каждого входа *tx.in*. Процесс отслеживания входов описан в Алгоритме 1.

Отслеживание начинается с двух входов, списка блоков, извлеченного из блокчейна Monero, и множества выходов, принадлежащих злоумышленнику (строка 1). Если множество выходов, известных злоумышленнику, увеличивается (строка 20), то анализ начнётся заново для всех блоков,

так как потенциально можно будет отследить большее количество входов (строки 5 - 24). Отслеживание остановится только тогда, когда уже нельзя будет найти никакого нового реального входа (строка 19) при помощи текущего списка выходов, принадлежащих злоумышленнику (строки 4 и 26).

Алгоритм 1. Отслеживание входов

```
1: procedure TRACE_INPUTS(blocks, attackerKeys)
2:     tracedKeys ← {}
3:     while true do
4:         knownKeys ← |attackerKeys|
5:         for each block ∈ blocks do                    ▷ For each block
6:             transactions ← getTransactions(block)
7:             for each transaction ∈ transactions do
8:                 inputs ← getInputs(transaction)
9:                 for each input ∈ inputs do
10:                    keys ← getKeys(input)
11:                    mixinSetSize ← |keys| − 1
12:                    mixinsRemoved ← 0
13:                    for each key ∈ keys do
14:                        if key ∈ attackerKeys then
15:                            mixinsRemoved ← mixinsRemoved + 1
16:                        end if
17:                    end for
18:                    if mixinsRemoved == mixinSetSize then
19:                        realKey ← keys − (attackerKeys ∩ keys)
20:                        attackerKeys ← attackerKeys ∪ realKey
21:                        tracedKeys ← tracedKeys ∪ realKey
22:                    end if
23:                end for
24:            end for
25:        end for
26:        if knownKeys == |attackerKeys| then
27:            break
28:        end if
29:    end while
30:    return tracedKeys
31: end procedure
```

При каждой итерации Алгоритма 1 извлекаются все входы каждой транзакции (строка 8). Для каждого входа (строки 9 - 23) мы должны проверить, какие выходы имеются во множестве выходов, известных злоумышленнику. Если проводящий атаку человек знает все выходы, кроме одного входа транзакции (строки 11 - 18), то остающийся выход является реальным (отслеженным входом), и он добавляется к списку выходов, принадлежащих злоумышленнику (строки 19 — 21).

Все отслеженные входы могут быть удалены из входов транзакций, что позволит отследить ещё большее количество входов. Этот эффект усиливается, повышая эффективность атаки. После того как алгоритм закончит работу, он возвратит список отслеженных входов (строка 30).

4 Оценка

Проведение нашей атаки в сети Monero не только требует времени (например, 1 год) и выплаты комиссий за проведение транзакций, но также может разрушить её сервисы. Поэтому мы моделируем

нашу атаку локально на основе реальных данных Monero. Поскольку в феврале 2018 года проект Monero увеличил минимальное число ложных выходов до 4, а также в октябре 2018 утвердил постоянное обязательное количество ложных выходов, которое составило 10, мы решили провести наш основной эксперимент, используя данные Monero за год, начиная с февраля 2018, так как это должно было дать более точный результат, отражающий новые обновления. Мы приводим результаты нашего анализа с использованием старого набора данных (с февраля 2017 по февраль 2018) в Приложении B.

Чтобы оценить флуд-атаку на транзакции, мы взяли данные за один год (с 1-го февраля 2018 по 1-е февраля 2019) из блокчейна Monero, то есть начиная с блока 1 499 601 и заканчивая блоком 1 761 435. Мы приняли во внимание четыре различных периода, а именно: последние 3 месяца (начальный блок 1 695 128), последние 6 месяцев (начальный блок 1 606 715), последние 9 месяцев (начальный блок 1 562 861) и все 12 месяцев (начальный блок 1 499 601). Что касается выходов проводящего атаку, мы случайным образом выбрали выходы из блокчейна.

Кроме того, мы оценили, какую выгоду может извлечь злоумышленник из небольшой атаки, то есть проводя флуд-атаку в течение всего нескольких дней. Мы использовали блоки с 1 761 435 по 1 782 260 в 5 временных периодах, а именно: за последние 1,8 дня (начальный блок 1 780 976), последние 3,6 дня (начальный блок 1 779 654), последние 7,2 дня (начальный блок 1 777 069), последние 14,4 дня (начальный блок 1 771 847) и за все 28,8 дня (начальный блок 1 761 435). Периоды кратны значению 1,8 дня, потому что именно это количество дней использует в качестве временной зоны алгоритм выбора миксинов Monero. Половина миксинов была выбрана именно из этой временной зоны.

4.1 Отслеживание входов

Мы задействуем алгоритм отслеживания, описанный в Разделе 3.2, чтобы оценить эффективность атаки. Результаты показаны на рисунке 2. Подробности также приводятся в Таблице 4 Приложения A.

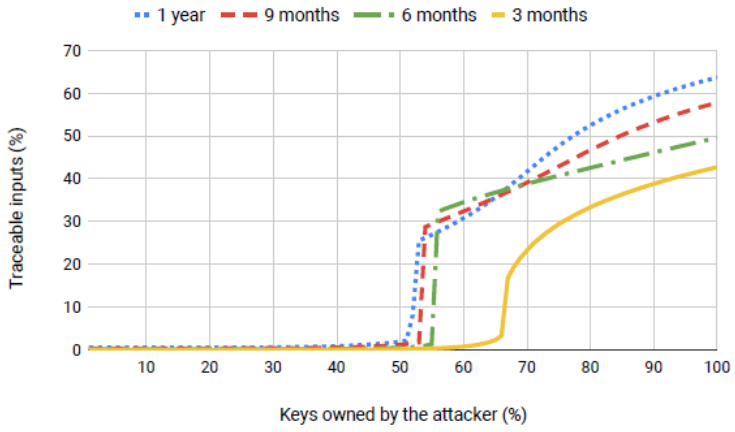

Рисунок 2. Количество отслеживаемых входов в зависимости от мощности проводящего атаку

При наличии большего множества (%) выходов шансы системы на выбор ложных выходов, принадлежащих злоумышленнику, возрастают. Действительно, количество отслеживаемых входов растёт пропорционально проценту выходов, которыми обладает злоумышленник, что показано на рисунке 2. Например, если в течение периода, составляющего 3 месяца, злоумышленник владеет 80% выходов, то он/она способен отследить приблизительно 35% ключей платежа. Однако, если этот временной отрезок будет увеличен до одного года, то злоумышленник сможет отследить уже более 50% входов.

Как можно увидеть, длительность периода атаки влияет на мощность атаки с целью отслеживания входов. Это потому, что выходы более старых транзакций также отбираются системой в качестве ложных. У атаки, проводимой в течение трёх месяцев, самый низкий показатель отслеживания (примерно 43%), в то время как через один год злоумышленник сможет отследить уже почти 64% входов. Однако, чтобы достигнуть таких результатов, ему/ей необходимо владеть 99% выходов. Опять же, отличие более чем на 20% возникает вследствие того, что для транзакций (за этот трёхмесячный период), наиболее вероятно, будут выбраны ложные выходы, принадлежащие более старым транзакциям (например, транзакции, которые были проведены в период между тремя и двенадцатью месяцами назад), которые никак не контролируются злоумышленником.

Также интересно то, что на рисунке 2 имеется два резких скачка между 50% и 70%. Несмотря на то, что при наличии до 50% выходов отслеживаемость входов составила менее 2%, показатель подскакивает более чем до 20% во всех периодах, если злоумышленник владеет более чем 50% выходов. Этот внезапный экспоненциальный рост показателя отслеживания можно объяснить цепными реакциями по протоколу CryptoNote [8]. Критическая массовая реакция происходит, если злоумышленник владеет достаточным количеством выходов, чтобы быть способным отследить входы транзакций, и рекурсивно использует недавно отслеженные входы, чтобы отследить ещё больше входов, вызывая цепную реакцию, которая затрагивает всё большее количество входов. Стоит упомянуть, что при разработке Алгоритма 1 цепная реакция была учтена нами.

Чтобы лучше понять влияние критической массовой реакции при отслеживании входов, на рисунке 3 нами были показаны результаты отслеживания при отключённой цепной реакции, то есть недавно отслеженные входы не используются в процессе обнаружения ещё большего количества входов. Можно заметить, что количество от отслеживаемых ключей увеличивается с количеством выходов, известных злоумышленнику. Однако внезапного экспоненциального роста показателя отслеживания не происходит. Кроме того, количество отслеженных входов значительно ниже. Например, обладая 99% выходов, злоумышленник сможет отследить всего половину входов, если сравнивать с предыдущими результатами.

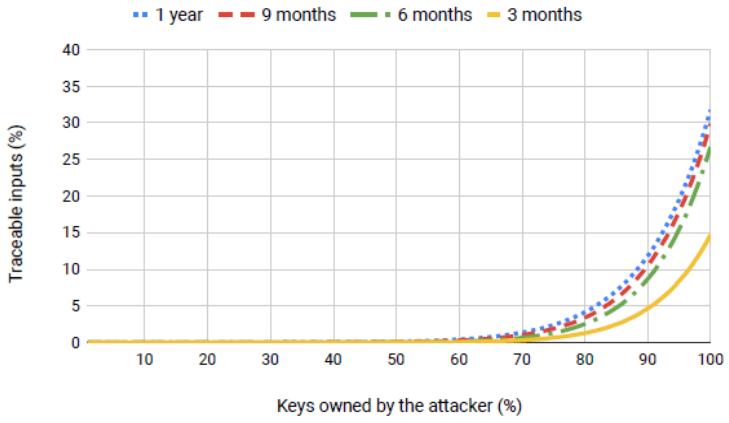

Рисунок 3. Количество отслеживаемых входов в зависимости от мощности проводящего атаку (без цепной реакции)

Мы также оценили показатель отслеживаемости нашего решения, используя более старый набор данных блокчейна Monero, начиная с блока 1 236 197 и заканчивая блоком 1 499 600 (с января 2017 по январь 2018). На рисунке 5 Приложения А показаны результаты отслеживания. Поскольку минимальное количество миксинов составляло не более четырёх, мощность отслеживания входов злоумышленником была намного выше. Проводящий атаку человек, владеющий 99% выходов, мог отследить почти 90% входов. Однако затраты на проведение атаки были на три порядка выше, о чём мы пишем далее в Разделе 4.4.

Наконец, стоит подчеркнуть, что в течение выбранных периодов некоторые транзакции нельзя было отследить, но ложные выходы были удалены из их входов. Это делает входы более чувствительными к последующим атакам. В таблице 2 в Разделе 4.2 мы суммируем количество миксинов, удаленных из входов за годичный период, демонстрируя воздействие атаки на все входы, включая те, которые не могли быть отслежены.

4.2 Удалённые ложные выходы

Как ожидалось, в течение выбранных периодов некоторые транзакции было невозможно отследить. Однако мы сократили количество ложных выходов практически у всех 3 824 858 входов за весь годичный период. Это делает эти входы более уязвимыми для последующих атак. В Таблице 2 мы суммируем количество миксинов, удаленных из входов. В каждой ячейке указан процент входов, затронутых алгоритмом отслеживания. Например, если злоумышленник владеет 99% выходов, у 5,15% входов удаляется от 50 до 59% ложных выходов.

Если злоумышленник владеет 75% или большим количеством выходов, его способность к отслеживанию приближается к максимальной. С этого момента у большого количества входов 6 или 10 миксинов удалено из соответствующих множеств, обеспечивающих анонимность. Это происходит, потому что в настоящее время размер кольца фиксирован и имеет значение 11, а следовательно, существует большое количество транзакций с 10 миксинами. До этого допустимый минимальный размер кольца равнялся 7, в результате чего большое количество транзакций имело 6 миксинов. Только те входы, у которых не было удалено ни одного ложного выхода, не были затронуты флуд-атакой на транзакции. Входы, которые не были затронуты этой атакой, сохраняют 93,85%, 30,12%, 15,08%, 10% и 9,38% входов, когда злоумышленник владеет 1%, 25%, 50%, 75% и 100% выходов, соответственно. Поскольку мы смогли отследить 63,36% входов, когда злоумышленник владел 99% выходов, и 9,38% входов не были затронуты атакой, у нас есть оставшиеся 27,26% входов транзакций с одним или несколькими удаленными ложными выходами. Это означает, что 90,62% всего множества входов было затронуто алгоритмом отслеживания.

Таблица 2. Влияние флуд-атаки на размер множеств транзакций, обеспечивающих анонимность

Сокращение множества, обеспечивающего анонимность (%)	Количество затронутых входов транзакций (%)				
	Контроль над 1%	Контроль над 25%	Контроль над 50%	Контроль над 70%	Контроль над 99%
0	93,85	30,12	15,08	10	9,38
1 - 9	0,15	0,25	0,11	0,01	0
10 - 19	4,99	22,42	8,11	1,41	0,48
20 - 29	0,45	14,21	7,45	2,70	1,37
30 - 39	0,05	16,85	13,06	3,01	1,16
40 - 49	0	5,52	6,69	1,06	0,24
50 - 59	0	7,72	21,16	8,03	5,15
60 - 69	0	1,71	13,28	7,32	4,42
70 - 79	0	0,44	6,65	5,11	4,38
80 - 89	0	0,20	5,71	12,65	9,54
90 - 99	0	0	0,76	1,05	0,48
100	0,47	0,51	1,88	47,63	63,36

4.3 Малые флуд-атаки

Нами также было проанализировано влияние малых атак. Мы взяли периоды от 1,8 до 28,8 дня. На рисунке 4 показаны результаты для набора данных блокчейна Monero с 1-го февраля по 1-е марта

2019. Одной из первых вещей, которые можно отметить, является отсутствие критической массовой реакции для таких коротких периодов.

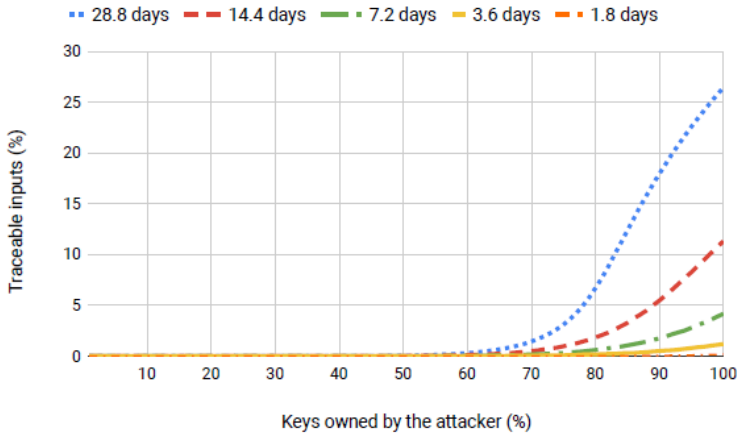

Рисунок 4. Количество отслеживаемых входов в зависимости от мощности проводящего атаку

В случае с маленькими периодами показатель отслеживания начинает значительно увеличиваться, если злоумышленник владеет более чем 70% выходов. При атаке в течение 1,8 дня входы возможно отследить, только если у злоумышленника есть 70% выходов.

Если злоумышленник владеет 75% выходов, то он/она способен отследить 0,02%, 0,09%, 0,32%, 0,97% и 3,09% входов, соответственно. Несмотря на то, что 0,32% кажется довольно небольшим процентом, он составляет 320 отслеживаемых входов за 7,2 дня, учитывая, что в блокчейн ежедневно в среднем добавляется 10k входов. При наличии более чем 75% выходов количество отслеживаемых входов быстро увеличивается, достигая 0,20%, 1,20%, 4,17%, 11,31% и 26,41%, когда злоумышленник контролирует 99% выходов.

Данный анализ демонстрирует, что злоумышленник может отследить входы, даже если период атаки составляет всего 1,8 дня. Однако, если проводящий атаку хочет отследить значительное количество входов, ему/ей необходимо использовать более длительные периоды (например, более 7 дней).

4.4 Анализ затрат

Согласно годичным данным блокчейна Monero, описанным в Разделе 4.1, ежедневное среднее количество генерируемых выходов составляет приблизительно 11 512. Мы используем это среднее количество в качестве основы для анализа затрат на проведение нашей флуд-атаки на транзакции. Допустим, 11 512 является минимальным количеством выходов, генерируемых за один день. Таким образом, если злоумышленник хочет контролировать 50% выходов, то он/она должен генерировать то же количество выходов в день, то есть 11 512.

Как говорилось в Разделе 3.2, допустим, злоумышленник собирается создать транзакции со ста адресами выходов и одним адресом входа с десятью миксинами. Мы используем размер комиссии, установленный в сети по умолчанию за килобайт данных транзакции, которая в настоящее время составляет 0,000020 XMR (0,00125 доллара США по состоянию на 4 апреля 2019, когда 1 XMR стоил приблизительно 62,92 доллара США). Такой же обменный курс используется во всех последующих примерах. В Таблице 5 Приложения C указано количество выходов транзакций, необходимых злоумышленнику, чтобы обладать различными уровнями контроля над входами блокчейна Monero в течение определенного периода.

В Таблице 3 мы указываем размер комиссий при проведении флуд-атаки на транзакции. Если злоумышленник будет обладать 75% выходов, то ежегодная комиссия составит всего 27,758 XMR (или 1746,53 доллара США). Это, возможно, очень немного для проведения атаки, которая позволяет отследить почти 50% входов. Не говоря уже о том, что 1746,53 доллара США - просто пенни, когда дело доходит до крупных компаний или правительств, которые могли бы заинтересоваться отслеживанием входов транзакций Monero. Флуд-атака на транзакции явно представляет большую угрозу для репутации Monero и анонимности ее пользователей.

Мы произвели тот же анализ затрат на проведение флуд-атаки на транзакции для второго набора данных (данные блокчейна Monero с февраля 2017 по февраль 2018). Поскольку протокол Bulletproof в то время ещё не был реализован, стоимость атаки была почти в 1750 выше (например, 49212.418 XMR или 3 086 602,89 доллара США при обладании 75% выходов в течение однолетнего периода). Несмотря на высокую стоимость, уже тогда это была вполне выполнимая атака.

Таблица 3. Комиссии за проведение флуд-атаки на транзакции

Процент выходов, контролируемых злоумышленником	Размер комиссии за проведение транзакций (в XMR)			
	3 месяца	6 месяцев	9 месяцев	1 год
1%	0,023	0,046	0,069	0,093
25%	0,760	1,521	2,281	3,084
50%	2,281	4,563	6,844	9,253
75%	6,844	13,689	20,533	27,758
99%	225,863	451,727	677,590	916,001

5 Заключение

В данной работе был представлен анализ отслеживаемости транзакций Monero при помощи новой атаки под названием FloodXMR. Предложенный вариант атаки предполагает использование протокола Bulletproof для создания большого количества транзакций с целью контроля над большим количеством выходов, используемых для обеспечения анонимности входов в транзакциях Monero.

Результаты моделирования показали, что реализация предлагаемой атаки позволяет злоумышленнику, контролирующему 75% выходов транзакций, созданных за одногодичный период, отследить 47,63% всех входов транзакций, созданных за тот же период времени. Результаты указывают на наличие слабых мест в механизмах обеспечения анонимности Monero с акцентом на недавно реализованный протокол Bulletproof, который был важен с точки зрения экономической выгодности предложенной атаки.

Нами был также представлен анализ затрат на проведение флуд-атаки на транзакции. Была оценена стоимость создания необходимых для выполнения атаки транзакций, и результаты показывают, что злоумышленник должен был бы потратить 9,253 XMR или 582,19 доллара США на комиссии за проведение транзакций, чтобы контролировать 50% выходов в течение одного года. Путём анализа результатов мы приходим к заключению, что стоимость атаки является низкой, учитывая влияние, которое она оказывает на анонимность транзакций ориентированной на обеспечение анонимности криптовалюты.

Представленные результаты анализа подчеркивают важность обнаружения и исправления уязвимых мест в механизмах обеспечения анонимности и безопасности криптовалют.

Ссылки

1 Бирюков А. (Biryukov A.), Ховратович Д. (Khovratovich, D.), Пустогаров, И. (Pustogarov, I.): «Деанонимизация клиентов в p2p сети Bitcoin» (Deanonymisation of clients in bitcoin p2p network). Материалы конференции ACM SIGSAC 2014 по безопасности компьютерной техники и коммуникаций, стр 15-29. ACM (2014)

2 Фледер М. (Fleder M.), Кестер М. С. (Kester M.S.), Пиллай С. (Pillai, S.). «Анализ графа транзакции Bitcoin» (Bitcoin transaction graph analysis). Препринт arXiv, arXiv:1502.01657 (2015)

3 А. Кумар (A. Kumar), С. Фишер (C. Fischer), С. Топл (S. Tople) и П. Саксена (P. Saxena). «Анализ отслеживаемости блокчейна Monero» (A traceability analysis of monero's blockchain) Материалы Европейского симпозиума по исследованиям в области компьютерной безопасности), страницы 153-173. Springer, 2017 г.

4 Ли К. (Lee K.), Миллер А. (Miller A.). «Аутентифицированные структуры данных для лёгких обеспечивающих анонимность клиентов Monero» (Authenticated data structures for privacy-preserving monero light clients). IEEE EuroS&PW. стр. 20-28. IEEE (2018)

5 С. Мекледжон (S. Meiklejohn), М. Помароле (M. Pomarole), Дж. Джордан (G. Jordan), К. Левченко (K. Levchenko), Д. Маккой (D. McCoy), Дж.. М. Вёлькер (G. M. Voelker) и С. Сэведж (S. Savage). «Гора Bitcoin: идентификация платежей, производимых людьми без имени» (A fistful of bitcoins: characterizing payments among men with no names). Протоколы конференции по проведению измерений в сети Интернет 2013, стр. 127-140. ACM, 2013 г.

6 А. Миллер (A. Miller), М. Мёзер (M. Moser), К. Ли (K. Lee) и А. Нараянан (A. Narayanan). «Эмпирический анализ связываемости в блокчейне Monero» (An empirical analysis of linkability in the monero blockchain). Препринт arXiv, arXiv:1704.04299, 2017 г.

7 С. Накамото (S. Nakamoto). «Bitcoin: электронная одноранговая денежная система» (Bitcoin: A peer-to-peer electronic cash system). 2008 г.

8 Ноезер Ш. (Noether S.), Маккензи А. (Mackenzie, A.). «Техническая записка по проблеме цепной реакции при отслеживании протокола CryptoNote 2.0» (A note on chain reactions in traceability in cryptonote 2.0). Исследовательский бюллетень MRL-0001. Monero Research Lab 1, 1-8 (2014).

9 Н. Ван Саберхаген (N. Van Saberhagen). Cryptonote v 2.0, 2013 г. https://static.coinpaprika.com/storage/cdn/whitepapers/1611.pdf

10 Виджая Д. А. (Wijaya D.A.), Лю Дж. (Liu J.), Стейнфельд Р. (Steinfeld R.), Лю Д. (Liu D.). «Атака на кольцо Monero: воссоздание эффекта транзакций с нулевым миксином» (Monero ring attack: Recreating zero mixin transaction effect). 17-я Международная конференция по доверию, безопасности и анонимности в вычислительной технике и коммуникациях IEEE / 12-я международная конференция по большим данным и разработке IEEE 2018 (TrustCom/BigDataSE), стр. 1196{1201. IEEE (2018)

11 Ю З. (Yu Z.), О М. Х. (Au M.H.), Ю Дж. (Yu, J.), Янг Р. (Yang R.), Ксю К. (Xu Q.), Ло В. Ф. (Lau W.F.). «Новый эмпирический анализ отслеживаемости в валютах на базе CryptoNote» (New empirical traceability analysis of cryptonote-style blockchains), 2019 г.

A Отслеживание входов

Для оценки эффективности атаки нами был использован алгоритм отслеживания, описанный в Разделе 3.2. Результаты представлены в таблице 4. В первой колонке указан процент выходов, контролируемых злоумышленником.

На практике невозможно владеть 100% выходов, если только проводящий атаку не является единственным участником сети, получающим средства. Тем не менее интересно отметить, что даже при владении 100% выходов злоумышленник не сможет отследить все входы за заданный период времени, поскольку входы транзакций используют ложные выходы, сгенерированные до того, как была начата атака.

Таблица 4. Количество отслеживаемых входов в зависимости от мощности проводящего атаку

Выходы злоумышленника	Отслеживаемые входы			
	3 месяца	6 месяцев	9 месяцев	1 год
1%	0 (0%)	2202 (0,09%)	9339 (0,31%)	18 227 (0,47%)
25%	1 (0%)	2274 (0,09%)	9647 (0,32%)	19 573 (0,51%)
50%	1241 (0,10%)	10 843 (0,47%)	33 967 (1,15%)	72 155 (1,88%)
75%	332 130 (29,39%)	930 143 (40,74%)	1 265 916 (42,90%)	1 821 946 (47,63%)
99%	482 813 (42,39%)	1 133 145 (49,29%)	1 706 870 (57,45%)	2 437 661 (63,36%)

B Отслеживание входов в старых наборах данных

Для оценки нашей флуд-атаки на транзакции нами был использован второй набор данных. Он начинается с блока 1 236 197 (на 1-го февраля 2017 требовалось использовать минимум 2 миксина) и заканчивается на блоке 1 499 600 (на 1-го февраля 2018 требовалось использовать минимум 4 миксина). С другой стороны, первый набор данных (см. Раздел 4) начинается с 1-го февраля 2018 (обязательное количество миксинов равное 4, увеличенное до 6 миксинов в марте и до 10 миксинов в октябре) и заканчивается 1-м февраля 2019.

Как можно увидеть на рисунке 5, показатель отслеживаемости у злоумышленника, обладающего 75% выходов за годичный период, в два раза выше, если сравнивать с первым набором данных (нашим последним набором данных). Так как количество ложных выходов довольно мало, критическая массовая реакция начинается гораздо раньше, например, когда проводящий атаку владеет всего 16% выходов в течение годичного периода. Это показывает, насколько важно количество миксинов с точки зрения снижения мощности атак, направленных на отслеживание входов.

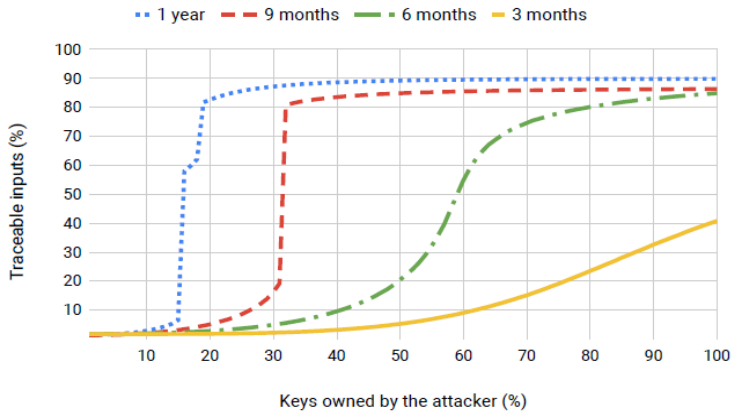

Рисунок 5. Количество отслеживаемых входов в зависимости от мощности проводящего атаку

C Количество выходов

В таблице 5 указано количество выходов, необходимых злоумышленнику, чтобы получить соответствующий процент выходов из сети Monero.

Таблица 5. Количество выходов, необходимых злоумышленнику

Процент выходов, контролируемых злоумышленником	Количество выходов			
	3 месяца	6 месяцев	9 месяцев	1 год
1%	10 465	20 930	31 396	42 443
25%	345 360	690 720	1 036 080	1 400 626
50%	1 036 080	2 072 160	3 108 240	4 201 880
75%	3 108 240	6 216 480	9 324 720	12 605 640
99%	102 571 920	205 143 840	307 715 760	415 986 120

D Математический анализ атаки

Показатель отслеживаемых злоумышленником входов повышается с количеством выходов, которые есть у него/неё в течение периода проведения атаки. Как показано на рисунке 6, показатели атаки в течение различных временных периодов (на графике показаны кривыми) ведут себе схожим образом. Сначала мощность проводящего атаку растёт очень медленно. Затем она внезапно экспоненциально повышается из-за критической массовой реакции. После этого показатель отслеживания снова продолжает расти медленно и ведёт себя, как в случае с кривой *[формула]*.

Для моделирования результатов проведения флуд-атаки на транзакции нами было выбрано уравнение (см. уравнение 2) со структурой *интегральной функции распределения* (CDF), а также функцией мощности. CDF полезна с точки зрения моделирования феномена, при котором переменные демонстрируют различное поведение с различными интервалами как до, так и после достижения точки критической массы на кривой. S-образная форма CDF позволяет нам реплицировать внезапный рост после достижения точки критической массы, в то время как функция мощности описывает стабильное повышение мощности отслеживания, когда количество ключей у злоумышленника приближается к значению 100%.

[формула] (2)

Рисунок 6 воспроизводит результаты проведения флуд-атаки на транзакции, полученные при помощи уравнения 2. Как можно видеть, результаты уравнения представляют собой довольно хорошее приближение результатов, продемонстрированных в Разделе 4.1.

Для моделирования результатов атаки для переменных из уравнения 2 нами были использованы следующие значения. У нас есть набор значений для каждого временного периода.

- 3 месяца: *[формула]*;
- 6 месяцев: *[формула]*;
- 9 месяцев: *[формула]*;
- 1 год: *[формула]*.

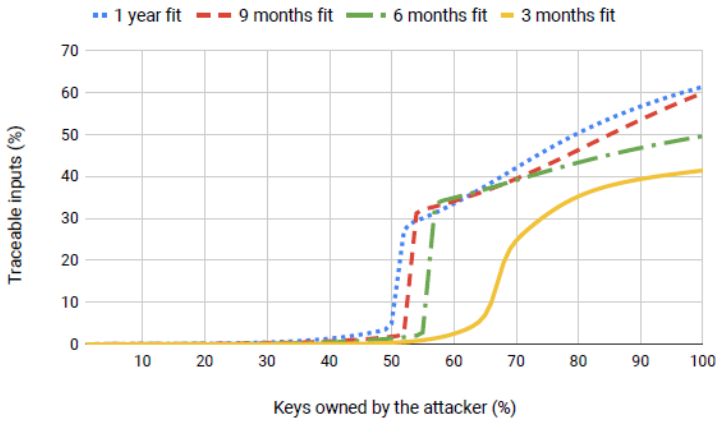

Рисунок 6. Моделирование результатов атаки при помощи уравнения 2