Система для безопасной коммуникации в неиндексируемой сети

Хафизуддин Хафизуддин
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
hafizuddin15-11763@diu.edu.bd

Е. В. Федорченко
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
evfedorchenko@etu.ru

Аннотация. **В данной статье представлены проектирование, реализация и экспериментальная оценка системы безопасной коммуникации в неиндексируемой сети. Рассматриваемый подход ориентирован на обеспечение защищенного обмена данными при работе в публичных и инфраструктурно ограниченных сетевых средах. Предложенная система обеспечивает конфиденциальность и контроль целостности сообщений при использовании общественного Wi-Fi и сетей, а также сетей с повышенными требованиями к защите передаваемых данных. Архитектура системы основана на трехуровневой модульной модели, разделяющей прикладной, сервисный и сетевой уровни. Для защиты информации используется клиентское шифрование на основе AES-GCM, а также механизмы маршрутизации сообщений через промежуточные узлы при наличии соответствующей сетевой инфраструктуры. В работе реализованы режим защищенной передачи данных с контролем целостности сообщений, а также экспериментальный режим защищенного согласования сеансового ключа с последующим шифрованием. Экспериментальные результаты подтверждают корректность функционирования реализованных криптографических механизмов, обеспечение конфиденциальности передаваемых данных и устойчивость коммуникации в условиях ограниченной сетевой доступности. Полученные результаты подтверждают, что предложенная архитектура обеспечивает возможность защищенного обмена сообщениями в распределенных сетевых средах.**

Ключевые слова: безопасная коммуникация; неиндексируемая сеть; многоузловая маршрутизация; криптографические механизмы; анонимность; конфиденциальность

I. Введение

В условиях широкого распространения публичных и распределенных сетевых инфраструктур возрастает актуальность обеспечения защищенной коммуникации и конфиденциальности передаваемых данных. Особую значимость данная задача приобретает при использовании общественных сетей доступа, включая публичные Wi-Fi сегменты, где существует риск перехвата трафика, анализа сетевой активности и нарушения целостности передаваемой информации. Поэтому существует необходимость создания системы безопасной коммуникации, обеспечивающей конфиденциальность сообщений, контроль целостности данных и устойчивость передачи независимо от характеристик внешней сетевой инфраструктуры.

Одним из подходов к повышению защищенности сетевого взаимодействия является использование распределенной маршрутизации сообщений через промежуточные узлы передачи данных. Подобные механизмы позволяют снизить степень прямой корреляции между отправителем и получателем трафика, а также повысить устойчивость коммуникации в распределенных сетевых средах. Известным примером реализации таких подходов являются сети с многоузловой маршрутизацией трафика, использующие последовательную передачу данных через цепочку промежуточных узлов [1]. Однако подобные механизмы в первую очередь ориентированы на защиту сетевого взаимодействия и маршрутизации данных и не обеспечивают в полной мере защиту содержимого сообщений на прикладном уровне. В связи с этим важным требованием при построении систем безопасной коммуникации является использование независимых механизмов прикладного шифрования, обеспечивающих конфиденциальность и контроль целостности передаваемых данных независимо от особенностей сетевой среды. Дополнительную значимость данная задача приобретает в условиях ограниченной доступности внешней инфраструктуры защищенной маршрутизации, нестабильности сетевых соединений или ограничений, связанных с особенностями сети [2].

Многие существующие системы безопасной коммуникации ориентированы либо на использование фиксированной централизованной инфраструктуры, либо на обязательное наличие внешних средств защищенной маршрутизации. Это может снижать устойчивость коммуникации и ограничивать применимость систем в инфраструктурно ограниченных средах. В связи с этим актуальной задачей является разработка архитектуры защищенной коммуникации, способной обеспечивать безопасную передачу данных как при наличии распределенной сетевой инфраструктуры, так и в условиях ее ограниченной доступности.

В данной работе представлены проектирование, реализация и экспериментальная оценка системы безопасной коммуникации в неиндексируемой сети. Предложенная система использует клиентское шифрование на основе AES-GCM, механизмы контроля целостности и маршрутизации сообщений через промежуточные узлы при наличии соответствующей сетевой инфраструктуры. Предложенная система построена на трехуровневой модульной архитектуре, разделяющей прикладной, сервисный и сетевой уровни,

для обеспечения гибкости интеграции и расширяемости компонентов системы.

Статья организована следующим образом. В разделе II представлен обзор релевантных работ и рассмотрены существующие ограничения подходов к обеспечению безопасной коммуникации в распределенных сетевых средах. В разделе III описаны проектирование и архитектура предложенной системы. Раздел IV посвящен экспериментальной оценке реализованного решения. В разделе V представлен анализ безопасности предложенной архитектуры. В разделе VI анализируются полученные результаты.

II. Релевантные работы

Существующие подходы к обеспечению безопасной коммуникации в распределенных сетевых средах можно разделить на три категории: системы на основе многоузловой маршрутизации, платформы обмена сообщениями со сквозным шифрованием и интегрированные коммуникационные решения для работы в неиндексируемых сетевых средах. Сеть Tor и архитектура скрытых сервисов обеспечивают защиту сетевого взаимодействия посредством многоузловой маршрутизации трафика и использования доменов .onion [1]. Данный подход позволяет снизить степень прямой корреляции между отправителем и получателем сетевого трафика. Однако Tor ориентирован на обеспечение защищенной маршрутизации и не предоставляет встроенных механизмов обязательного прикладного шифрования содержимого сообщений. Платформы обмена сообщениями со сквозным шифрованием, такие как Signal, реализуют надежную криптографическую защиту содержимого сообщений с использованием протокола Signal, основанного на алгоритме Double Ratchet и схеме согласования ключей X3DH [3]. Подобные решения обеспечивают высокий уровень конфиденциальности сообщений, однако, как правило работают поверх обычной сетевой инфраструктуры и не используют механизмы распределенной маршрутизации трафика. Интегрированные решения, такие как Ricochet и SecureDrop, сочетают механизмы распределенной маршрутизации и прикладного шифрования, но разработаны как закрытые потребительские продукты с ограниченными настройками [4]. Обзор этих решений позволяет выделить ограничения современных систем защищенной коммуникации: (1) в большинстве инструментов механизмы маршрутизации и криптографической защиты тесно интегрированы, что затрудняет независимую модификацию, анализ и оценку отдельных компонентов системы; (2) существующие исследовательские платформы, как правило, не поддерживает несколько режимов коммуникации в рамках единой архитектуры, что ограничивает возможности сравнительного анализа различных подходов к обеспечению безопасности; (3) исследования систем коммуникации в распределенных и неиндексируемых сетевых средах зачастую предполагают стабильные сетевые условия и ограниченно рассматривают вопросы функционирования при нестабильности соединения или ограниченной доступности инфраструктуры; (4) многие существующие решения не предоставляют базового режима взаимодействия без дополнительных механизмов защиты, что затрудняет количественную оценку влияния отдельных компонентов безопасности на характеристики системы. Предлагаемая в данной статье архитектура ориентирована на устранение указанных ограничений за счет модульного разделения компонентов, поддержки нескольких режимов коммуникации и возможности функционирования в условиях ограниченной сетевой инфраструктуры.

III. Архитектура системы для безопасной коммуникации

Предлагаемая система для безопасной коммуникации основана на трехуровневой модульной архитектуре с независимым разделением прикладного, сервисного и сетевого уровней. Прикладной уровень предоставляет пользовательский интерфейс, предназначенный для формирования сообщений, выбора режимов коммуникации и отображения результатов обмена сообщениями. Интерфейс спроектирован с учетом наглядного представления используемых механизмов защиты, что обеспечивает возможность экспериментального анализа и сравнительного исследования различных режимов коммуникации.

Сервисный уровень реализует криптографическую обработку данных, включая генерацию и управление ключами, операции шифрования и расшифрования, а также механизмы обработки и передачи сообщений. Все криптографические операции выполняются на стороне клиента, что исключает передачу открытого текста сообщений и ключевого материала серверной инфраструктуре. Сетевой уровень управляет маршрутизацией передаваемых сообщений. При наличии соответствующей инфраструктуры система поддерживает передачу данных через многоузловую маршрутизацию с использованием конечных точек .onion. При недоступности распределенной маршрутизации система использует стандартную HTTP-маршрутизацию при сохранении механизмов прикладного шифрования и защиты целостности сообщений. Подобное разделение компонентов является одним из ключевых архитектурных принципов предлагаемого фреймворка. В отличие от существующих инструментов безопасной коммуникации, в которых механизмы шифрования и маршрутизации тесно связаны, предлагаемый фреймворк явно разделяет эти два уровня. Такой подход обеспечивает сохранение конфиденциальности передаваемых данных даже в условиях ограниченной доступности распределенной сетевой инфраструктуры и повышает устойчивость системы к изменениям условий сетевого взаимодействия.

A. Режимы коммуникации

Предлагаемая система поддерживает три режима коммуникации. Режим Normal реализует передачу сообщений без применения криптографических преобразований и используется в качестве базового режима функционирования системы. Включение данного режима позволяет выполнять сравнительный анализ характеристик передачи данных при использовании различных механизмов защиты в идентичных сетевых условиях. Наличие базового режима обеспечивает возможность количественной оценки влияния прикладного шифрования и дополнительных механизмов защиты на конфиденциальность и характеристики коммуникации. Режим AES реализует основной механизм

криптографической защиты системы. Шифрование и расшифровка сообщений выполняется на стороне клиента с использованием алгоритма Advanced Encryption Standard в режиме Galois/Counter (AES-GCM) через Web Crypto API. Общий симметричный ключ используется взаимодействующими сторонами в рамках клиентской среды выполнения и не передается серверной инфраструктуре. Режим AES-GCM был выбран из-за поддержки аутентифицированного шифрования, обеспечивающего конфиденциальность передаваемых данных и контроль целостности сообщений посредством встроенного механизма аутентификационного тега. Режим ESA (Experimental Security Algorithm) представляет собой экспериментальное расширение системы, предназначенное для исследования механизмов автоматизированного согласования ключей и гибридных моделей шифрования. В данном режиме взаимодействующие стороны генерируют пары асимметричных ключей и выполняют согласование общего симметричного секретного ключа на основе протокола Elliptic Curve Diffie-Hellman (ECDH). Полученный общий секретный ключ затем используется в качестве ключа шифрования AES. Текущая реализация ESA носит исследовательский характер и ориентирована на экспериментальную оценку интеграции механизмов согласования ключей в архитектуру системы. Модульная организация системы позволяет расширять и модифицировать криптографические механизмы без изменения сервисного или сетевого уровней архитектуры.

B. Криптографические механизмы

Криптографические механизмы системы реализованы с использованием Web Crypto API — стандартизированного интерфейса браузерной криптографии, поддерживаемого современными веб-браузерами. Для обеспечения конфиденциальности и контроля целостности сообщений применяется алгоритм AES в режиме Galois/Counter Mode (AES-GCM). Процесс шифрования выглядит следующим образом: (1) 256-битный симметричный ключ генерируется или предоставляется в виде строки в кодировке Base64 и импортируется через Web Crypto API, оставаясь исключительно в памяти браузера на протяжении всей сессии; (2) 96-битный вектор инициализации (ВИ) генерируется с помощью криптографически безопасного генератора случайных чисел для каждой отдельной операции шифрования; (3) сообщение открытого текста кодируется в UTF-8 и шифруется с помощью AES-GCM с импортированным ключом и сгенерированным ВИ; (4) полученный шифротекст и ВИ кодируются и передаются на серверный ретранслятор; (5) на принимающей стороне выполняется расшифровка сообщения с использованием того же общего ключа и переданного ВИ. Использование случайного ВИ для каждой криптографической операции предотвращает формирование идентичных шифротекстов для одинаковых входных данных и снижает возможность анализа закономерностей передаваемого трафика. Все криптографические операции выполняются до передачи данных по сети, вследствие чего серверная инфраструктура взаимодействует только с зашифрованными данными и не получает доступа к открытому содержимому сообщений или ключевому материалу [5].

C. Серверный компонент и сетевая инфраструктура

Серверная часть системы реализована в виде облегченного HTTP-сервера, предназначенного для обслуживания статических компонентов пользовательского интерфейса и передачи сообщений между взаимодействующими сторонами. Серверная инфраструктура выполняет функции сетевого ретранслятора и не участвует в криптографической обработке данных или управлении ключевым материалом. Такой подход соответствует архитектурному принципу разделения сетевых и криптографических компонентов, при котором все операции, критичные для обеспечения безопасности, выполняются на стороне клиента. Для поддержки распределенной маршрутизации реализована интеграция с инфраструктурой Tor посредством конфигурации скрытого сервиса и использования адресации .onion. При доступности соответствующей инфраструктуры это обеспечивает возможность передачи данных через многоузловую маршрутизацию. В условиях ограниченной доступности распределенной маршрутизации система сохраняет работоспособность за счет использования стандартной HTTP-передачи при сохранении механизмов прикладного шифрования и защиты целостности сообщений.

IV. Экспериментальная оценка

A. Среда для экспериментов

Эксперименты проводились на рабочей станции macOS на базе ARM с использованием браузера и HTTP-сервера Python по адресу localhost:8080. Две вкладки браузера были открыты одновременно для имитации двух независимых участников коммуникации в контролируемых и воспроизводимых условиях. Такая конфигурация позволила систематически тестировать все три режима коммуникации, одновременно наблюдая за интерфейсами отправителя и получателя в реальном времени. Tor был установлен через Homebrew, сконфигурирован с определением скрытого сервиса, и была предпринята попытка начальной загрузки для оценки интеграции луковой маршрутизации в реальных сетевых условиях.

A. Результаты

Экспериментальный сценарий включал двух участников, взаимодействующих с использованием разработанного прототипа в контролируемой локальной среде. Каждый режим коммуникации тестировался независимо: сначала режим Normal для наблюдения незащищенного поведения, затем режим AES с вручную распределенным ключом для оценки корректности шифрования и, наконец, режим ESA для проверки гибридного рабочего процесса согласования ключей. Сетевой трафик контролировался на каждом этапе.

В режиме Normal сообщения доставлялись мгновенно с полной видимостью открытого текста как на интерфейсе отправителя, так и на интерфейсе получателя. Конфиденциальность сообщений в данном режиме не обеспечивалась, а передаваемые данные были доступны для непосредственного наблюдения в сетевом трафике, что позволило использовать данный режим в качестве базового сценария для сравнительного анализа механизмов защиты. В режиме AES были получены следующие результаты: (1) сформированный

шифротекст визуально и структурно отличался от исходного открытого текста; (2) каждая операция шифрования приводила к генерации уникального шифротекста за счет использования независимого случайного ВИ, включая случаи идентичных входных сообщений; (3) расшифровка корректно восстанавливала исходное содержимое сообщения на принимающей стороне; (4) при использовании неверного ключа расшифровка завершалось ошибкой аутентификации, что подтверждает корректность работы механизмов контроля целостности AES-GCM; (5) в журналах сетевого взаимодействия отсутствовало открытое содержимое сообщений во время работы режима шифрования. В ходе повторяющихся циклов шифрования и расшифровки система сохранила стабильность функционирования и корректность криптографической обработки данных. В режиме ESA согласование ключей ECDH и последующий процесс шифрования AES были проверены на логическую и структурную корректность, результаты подтвердили применимость гибридной модели шифрования для дальнейшего развития и полноценной реализации и интеграции в архитектуру системы. Начальная загрузка Tor не удалась на этапе эксперимента из-за ограничений на сетевом уровне, а именно блокировки TLS-рукопожатия на этапе подключения к ретранслятору, что предотвратило генерацию функционального адреса скрытого сервиса .onion. Этот результат рассматривается не как отказ системы, а как подтверждение одного из ключевых принципов его архитектуры: защищенная коммуникация в режиме AES оставалась полностью работоспособной в условиях недоступности подключения к Tor без снижения уровня конфиденциальности передаваемых данных или нарушения доступности системы. Этот результат подтверждает корректность архитектурного подхода, основанного на независимом разделении механизмов шифрования и маршрутизации.

Экспериментальные и аналитические результаты подтверждают основное положение данного исследования: механизмы прикладного шифрования на основе AES-GCM обеспечивают сохранение конфиденциальности и работоспособности системы независимо от доступности инфраструктуры распределенной маршрутизации.

V. Анализ защищенности

A. Модель угроз

Рассматривая модель угроз ориентирована на анализ защищенности коммуникации в распределенных и неиндексируемых сетевых средах и рассматривает четыре основных типа атакующих. Предполагается, что пассивный наблюдатель способен отслеживать весь передаваемый трафик, но не модифицировать его. Активный атакующий «человек посередине» способен перехватывать и модифицировать сетевые пакеты. Скомпрометированный сервер имеет полный доступ на чтение ко всем получаемым и хранимым им данным. Дополнительно рассматривается сценарий ограниченной доступности распределённой маршрутизации, при котором внешняя сетевая инфраструктура может ограничивать или нарушать соединения с узлами распределённой передачи данных и связанными сетевыми сервисами. Компрометация клиентской конечной точки рассматривается как находящаяся за пределами сферы применения данного прототипа.

B. Конфиденциальность и целостность

В отношении пассивного сетевого наблюдателя режим AES обеспечивает передачу данных исключительно в зашифрованном виде, что исключает возможность непосредственного восстановления содержимого сообщений без доступа к общему симметричному ключу. Использование независимого случайного ВИ для каждой операции шифрования дополнительно снижает возможность выявления закономерностей в передаваемом трафике. В условиях активного сетевого воздействия применение режима AES-GCM обеспечивает встроенную проверку целостности и подлинности передаваемых данных. Любая модификация шифротекста, ВИ или тега аутентификации приводит к ошибке аутентификации на принимающей стороне, вследствие чего измененные сообщения не рассматриваются системой как корректные. В случае компрометации сервера шифрование на стороне клиента гарантирует, что серверный ретранслятор хранит и пересылает только шифротекст. Поскольку открытое содержимое сообщений или ключевой материал не передаются серверу, компрометация сервера не предоставляет атакующему прямого доступа к исходным данным. В табл. I приведены свойства безопасности системы при реализации различных сценариев угроз.

ТАБЛИЦА I. Свойства безопасности при реализации сценариев угроз

Сценарий угрозы	**Режим Normal**	**Режим AES**	**AES + Tor**
Пассивный наблюдатель	Данные раскрыты	Данные защищены	Данные защищены + анонимность
Человек посередине	Уязвим	Обнаружение подделки (тег GCM)	Обнаружение + путь скрыт
Скомпрометированный сервер	Уязвим	Данные защищены (только на клиенте)	Данные защищены
Tor недоступен	Работает, без приватности	Шифр. сохранено; без анонимности	Работает как в режиме AES
Анализ трафика	Полностью раскрыт	Содержимое скрыто; метаданные раскрыты	Содержимое + метаданные защищены

C. Ограничения предложенного подхода

Текущий прототип имеет несколько ограничений, которые определяют направление будущих исследований. В текущей реализации общий симметричный ключ режима AES распределяется вне основного канала коммуникации, что ограничивает масштабируемость подхода при практическом развертывании системы. В случае компрометации канала распределения ключей, конфиденциальность передаваемых данных может быть нарушена независимо от криптографической стойкости используемого алгоритма шифрования. Предлагаемая система также не реализует механизмы формальную аутентификации пользователей, инфраструктуру цифровых удостоверений или поддержку цифровых подписей. Вследствие этого система обеспечивает контроль

целостности сообщений, однако не выполняет криптографически подтвержденную идентификацию отправителя. Кроме того, экспериментальная оценка распределенной маршрутизации проводилась в ограниченных сетевых условиях. Полномасштабное тестирование производительности системы в реалистичных условиях задержек и характеристик распределенных сетевых сред в рамках настоящего исследования не выполнялось.

VI. Анализ результатов

Полученные экспериментальные результаты подтверждают, что предложенная система способна обеспечивать конфиденциальность сообщений и устойчивость коммуникации в условиях ограниченной доступности распределенной маршрутизации. В ходе экспериментов, механизмы прикладного шифрования на основе AES-GCM сохраняли работоспособность при недоступности инфраструктуры многоузловой маршрутизации, без снижения уровня конфиденциальности передаваемых данных или нарушения доступности системы. Данный результат подтверждает корректность архитектурного подхода, основанного на независимом функционировании механизмов прикладного шифрования и сетевой маршрутизации. В отличие от ряда существующих решений, в которых криптографическая защита тесно зависит от доступности внешней инфраструктуры маршрутизации, предложенный фреймворк сохраняет возможность защищенной коммуникации даже при ограничениях сетевой среды. Анализ безопасности является важной частью данного исследования, поскольку предлагаемая система ориентирована на функционирование в распределенных и неиндексируемых сетевых средах, характеризующихся повышенными требованиями к конфиденциальности, ограниченной доступностью инфраструктуры и потенциальными сетевыми воздействиями. Проведение формализованной оценки угроз необходимо для определения степени защищенности предлагаемых режимов коммуникации в условиях практического применения системы. Представленная выше модель угроз определяет набор предположений и сценариев потенциального воздействия, в рамках которых выполняется оценка безопасности предлагаемой системы. Поддержка нескольких режимов коммуникации в рамках единой унифицированной среды является одной из отличительных особенностей предлагаемого фреймворка. Наличие базового режима Normal обеспечивает возможность непосредственного наблюдения и сравнительной оценки влияния механизмов шифрования на характеристики коммуникации, что представляет интерес как для экспериментальных исследований, так и для образовательных и демонстрационных сценариев. Экспериментальный режим ESA формирует основу для дальнейшего расширения криптографических механизмов системы. Модульная архитектура фреймворка допускает интеграцию автоматизированных протоколов согласования ключей, перспективных криптографических схем и адаптивных механизмов конфигурации без необходимости изменения базовой архитектуры системы.

С практической точки зрения клиентская модель выполнения криптографических операций представляет интерес для развертывания системы в средах с ограниченным уровнем доверия к серверной инфраструктуре или ограниченными вычислительными ресурсами. Поскольку серверный компонент взаимодействует исключительно с зашифрованными данными и не осуществляет хранение ключевого материала или открытого содержимого сообщений, требования к доверенности серверной инфраструктуры существенно снижаются. В случае компрометации серверного компонента доступ к ранее переданным данным коммуникации остается ограниченным вследствие отсутствия на серверной стороне открытого текста сообщений и криптографических ключей.

VII. Заключение

В данной статье были представлены проектирование, реализация и оценка безопасности модульной системы защищенной коммуникации для распределенных и неиндексируемых сетевых сред. Предлагаемая архитектура предусматривает независимое функционирование механизмов прикладного шифрования на основе AES-GCM и механизмов распределенной маршрутизации сетевого уровня. В рамках системы реализованы три режима коммуникации — Normal, AES и ESA — интегрированные в единую экспериментальную платформу, построенную на трехуровневой модульной архитектуре и ориентированную на исследование, сравнительный анализ и расширение механизмов защищённой коммуникации. Экспериментальная оценка подтвердила корректную работу AES-GCM с верифицированной конфиденциальностью, обнаружением нарушений целостности и стабильной производительностью в реальных сетевых условиях. Сбой начальной загрузки Tor, произошедший во время экспериментов, подтверждает основной принцип фреймворка: системы коммуникации для скрытой сети не должны полагаться исключительно на инфраструктуру распределенной маршрутизации для обеспечения гарантий безопасности. Фреймворк оставался полностью работоспособным для зашифрованной коммуникации при недоступности Tor, что демонстрирует устойчивость разделенного архитектурного подхода.

Будущие исследования будут сосредоточены на автоматизированных протоколах безопасного обмена ключами для замены ручного распределения ключей, аутентификации цифровых удостоверений на основе PKI для дополнения существующих гарантий целостности, оценке производительности в реалистичных сетевых условиях неиндексируемой сети и настройке конфиденциальности с помощью искусственного интеллекта для пользователей без специальной подготовки. Модульная архитектура фреймворка спроектирована таким образом, чтобы учитывать все эти расширения без структурной переработки, обеспечивая устойчивую основу для продолжения исследований безопасной коммуникации в неиндексируемой сети.

Список литературы

[1] Dingledine R., Mathewson N., Syverson P. Tor: The second-generation onion router // Proc. 13th USENIX Security Symposium. San Diego, CA, USA, 2004. P. 303–320.

[2] Murdoch S. J., Danezis G. Low-cost traffic analysis of Tor // Proc. IEEE Symposium on Security and Privacy. Oakland, CA, USA, 2005. P. 183–195.

[3] Marlinspike M., Perrin T. The Signal Protocol: A cryptographic protocol for end-to-end encrypted messaging. Open Whisper Systems, Technical Report, 2016. URL: https://signal.org/docs/

[4] Biryukov A., Pustogarov I. Trawling for Tor hidden services: Detection, measurement, deanonymization // Proc. IEEE Symposium on Security and Privacy. San Francisco, CA, USA, 2013. P. 80–94.

[5] National Institute of Standards and Technology. Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC. NIST Special Publication 800-38D, Nov. 2007.