

Криптография

Лекция 12. Анонимные сети

Дмитрий Яхонтов

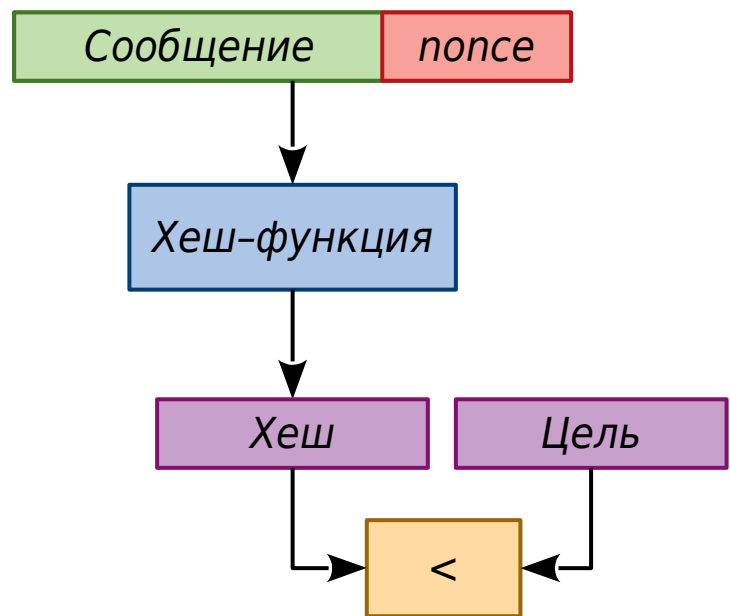
“Кочерга”, 2019

Сеть обмена сообщениями Bitmessage



- Алиса шифрует сообщение с использованием открытого ключа Боба.
 - ECDH для создания общего секрета
 - SHA-512 для создания одноразовых ключей
 - AES-256-CBC для шифрования сообщения
 - HMAC-SHA-256 для контроля целостности
 - ECDSA для цифровой подписи
- Сообщение рассылается всем участникам сети без указания адресата.
- Только Боб, имея закрытый ключ, может расшифровать сообщение.
- Сообщение хранится в сети ограниченный срок, затем уничтожается.
- Для защиты от спама используется Proof-of-Work.

Доказательство выполнения работы (Proof-of-Work)

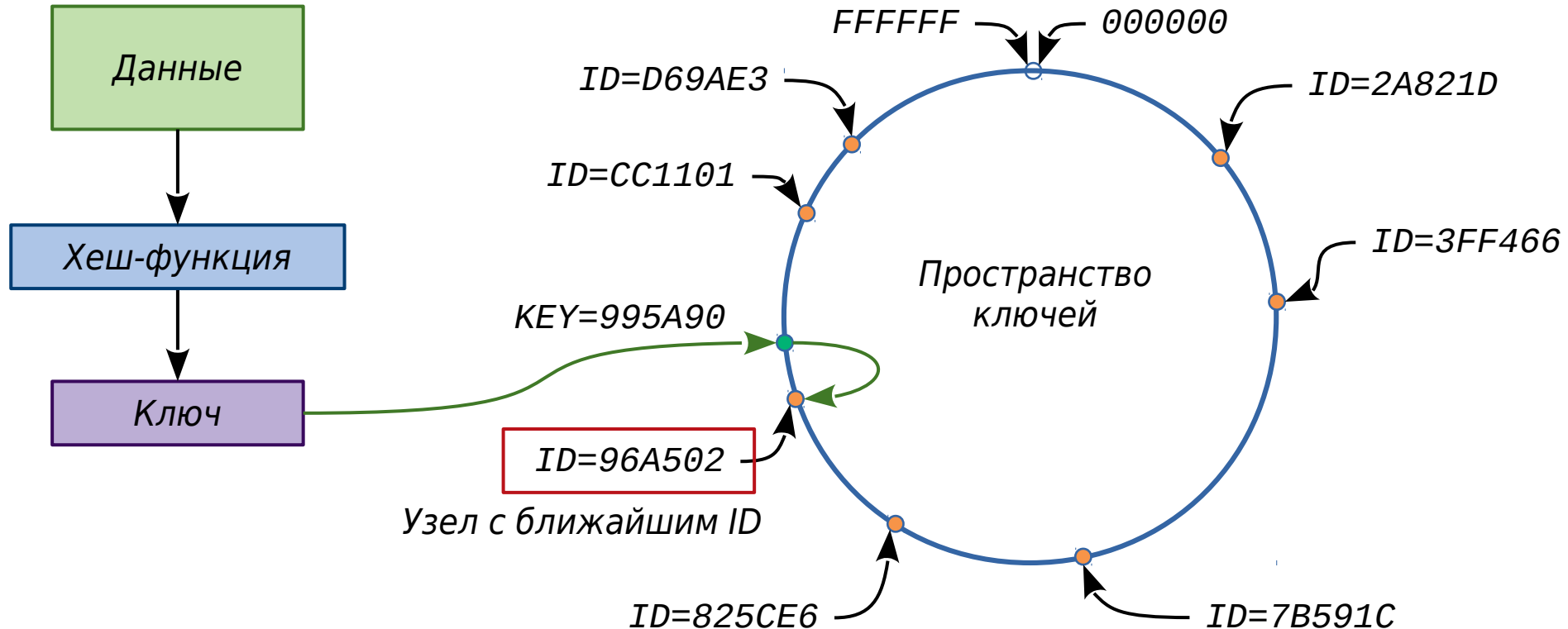


Вычислительная задача: подобрать **nonce** так, чтобы хеш **$H(\text{сообщение} + \text{nonce})$** получился меньше целевого значения (медленно)

Проверка: однократное вычисление **$H(\text{сообщение} + \text{nonce})$** и сравнение с целевым значением (быстро)

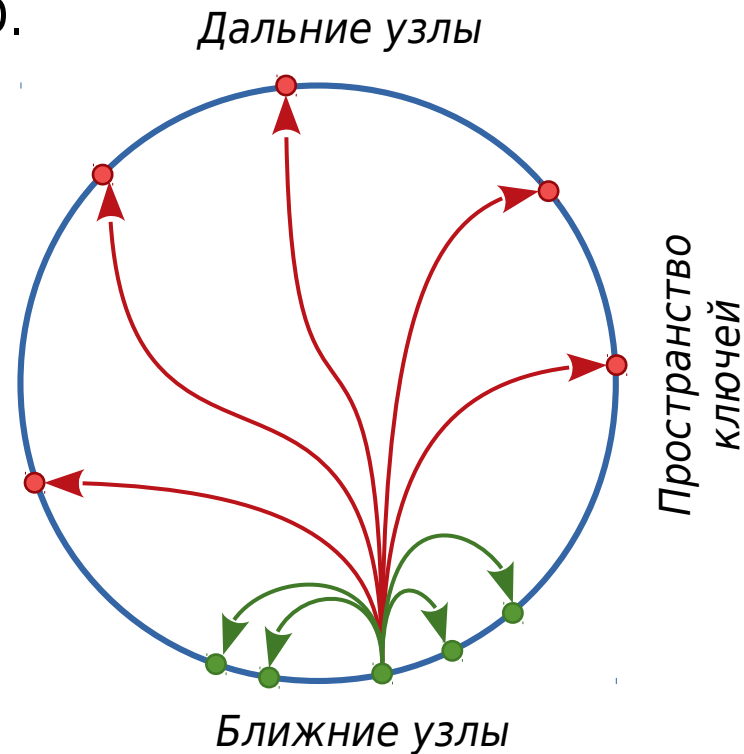
В Bitmessage для выполнения PoW требуется несколько минут процессорного времени (зависит от размера сообщения)

Распределённые хеш-таблицы (DHT – Distributed Hash Table)

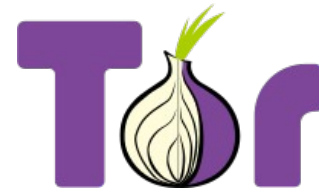


Поиск узлов в DHT

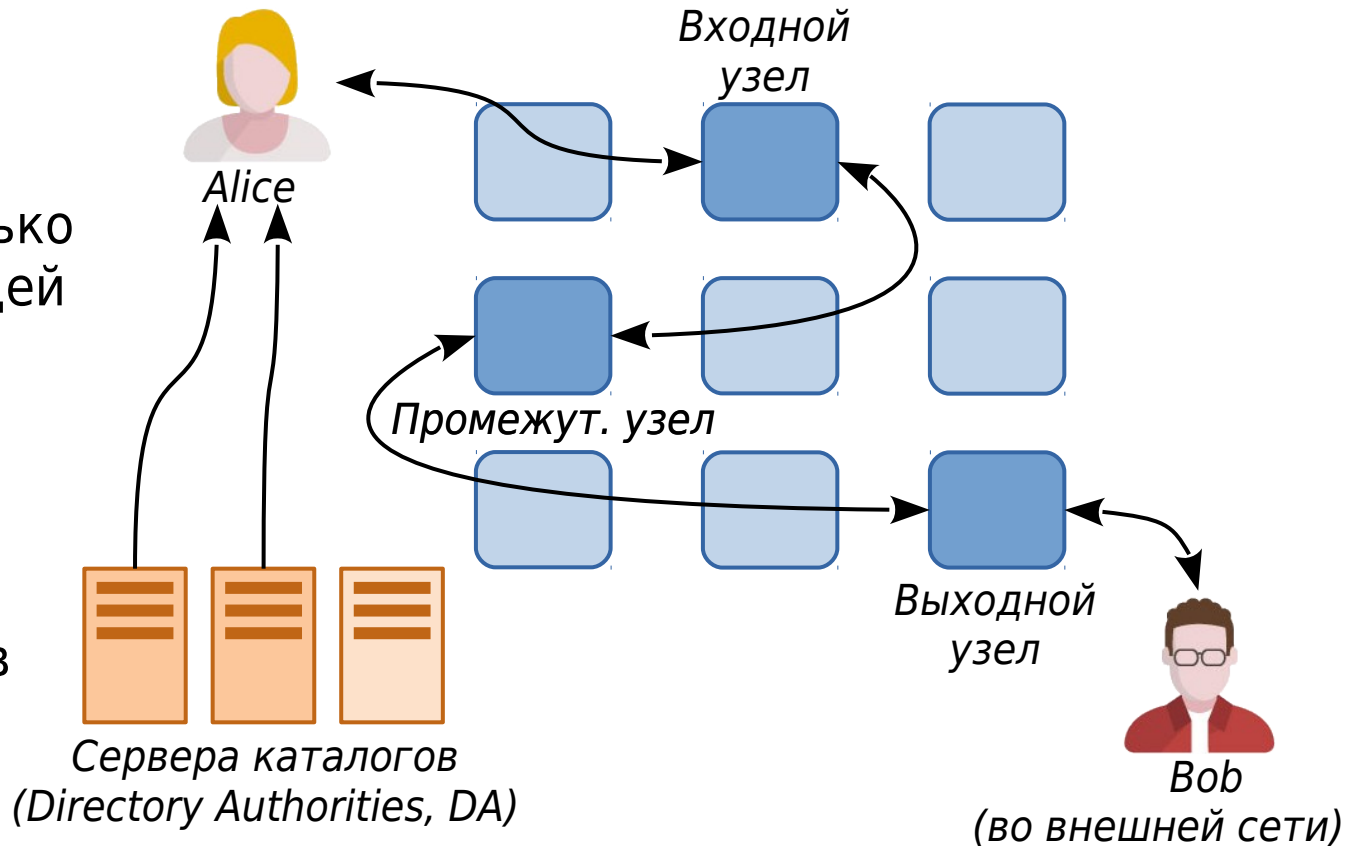
- Каждому узлу присваивается случайный ID.
- Узел хранит информацию о множестве ближайших (по ID) узлов, а также о нескольких дальних узлах.
- Для поиска узла по ID отправляем запрос тому узлу из известных, чей ID ближе всего к искомому. Он присылает информацию о своём соседе, чей ID ещё ближе.
- Для “холодного старта” используется небольшой список узлов, изначально заданных в коде программы.



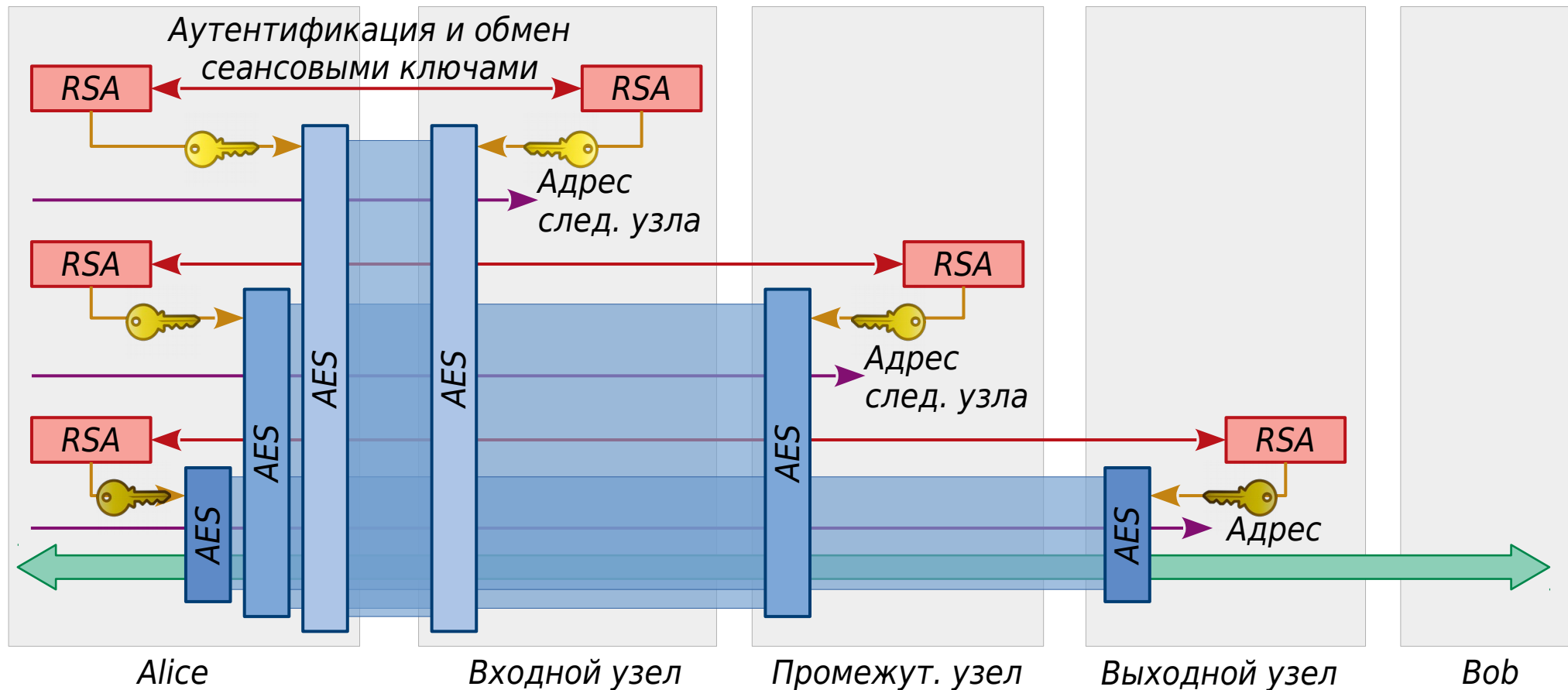
Луковая маршрутизация (Tor — The Onion Routing)



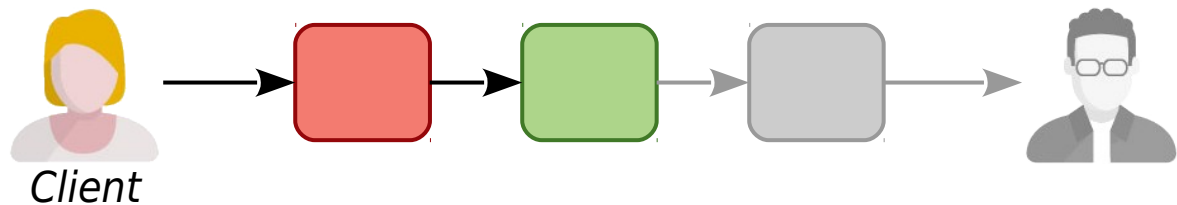
- Сообщение передаётся через цепочку узлов (по умолчанию три)
- Каждый узел знает только своих ближайших соседей
- Цепочки обновляются раз в 10 минут
- Сервера каталогов (DA) собирают статистику и публикуют список узлов



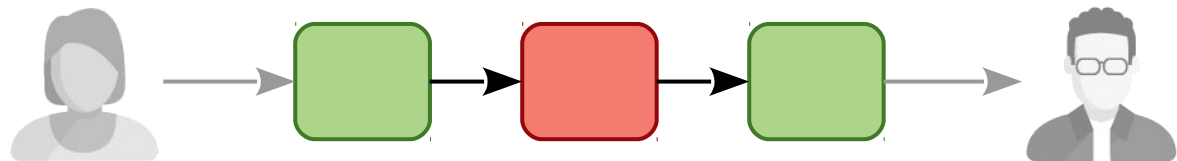
Многослойное (луковое) шифрование



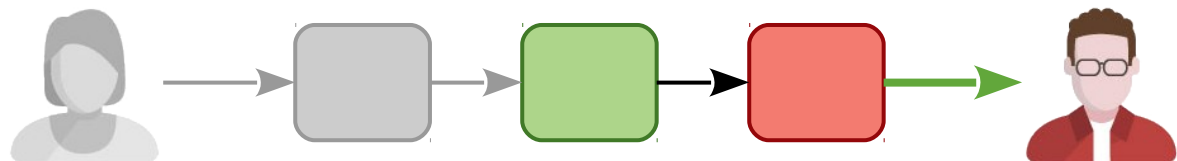
Кому что видно



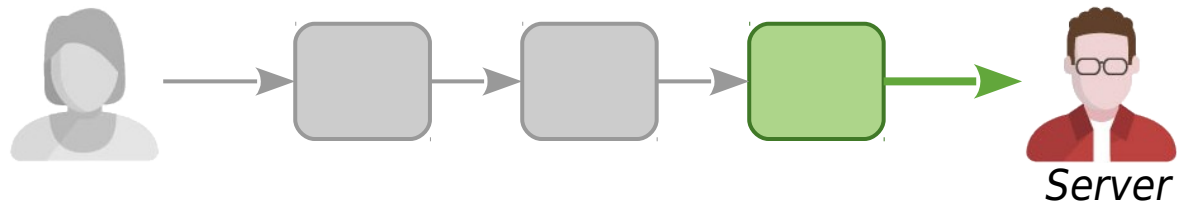
Входному узлу:
клиент и промежуточный.



Промежуточному узлу:
входной и выходной узлы.

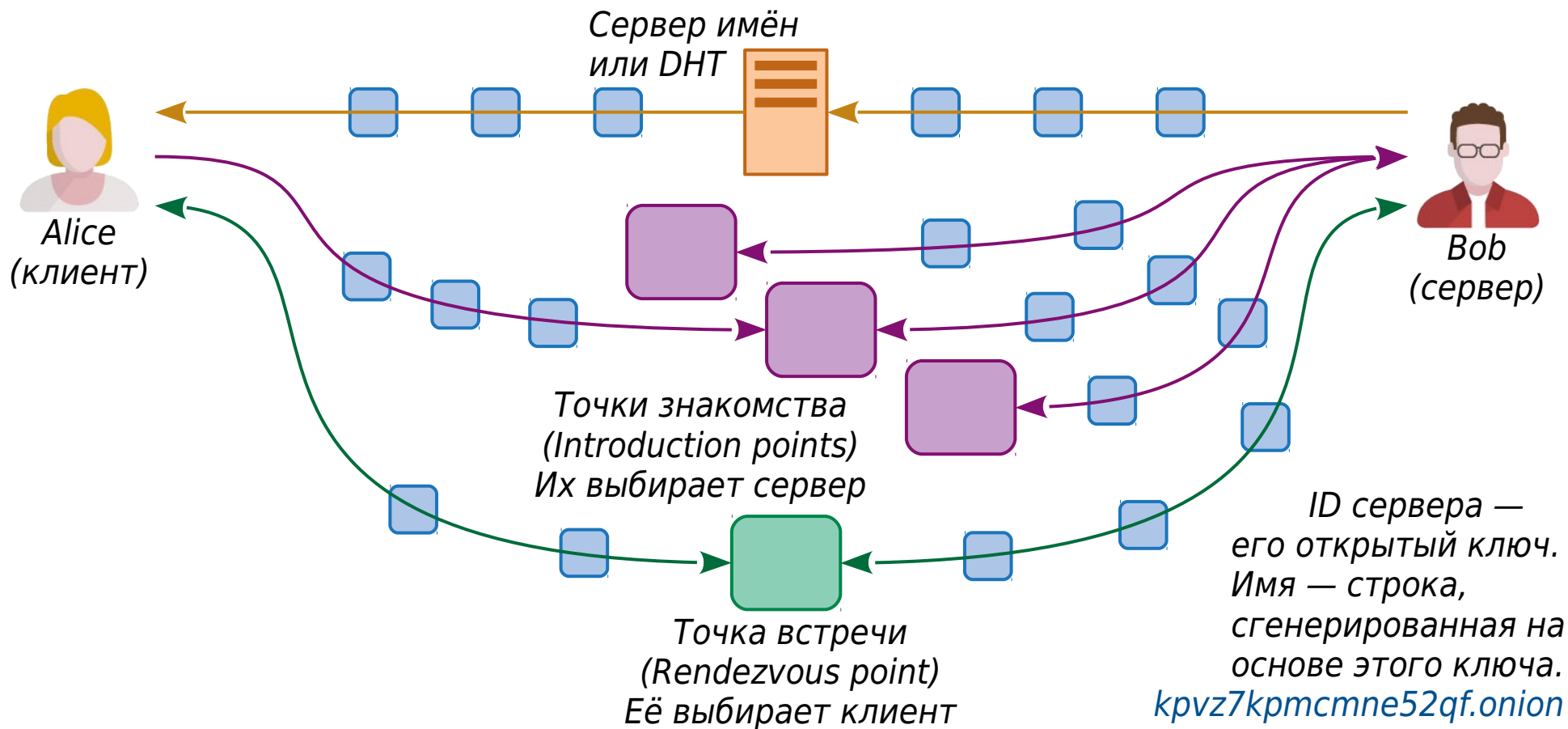


Выходному узлу:
промежуточный узел,
сервер и его трафик.



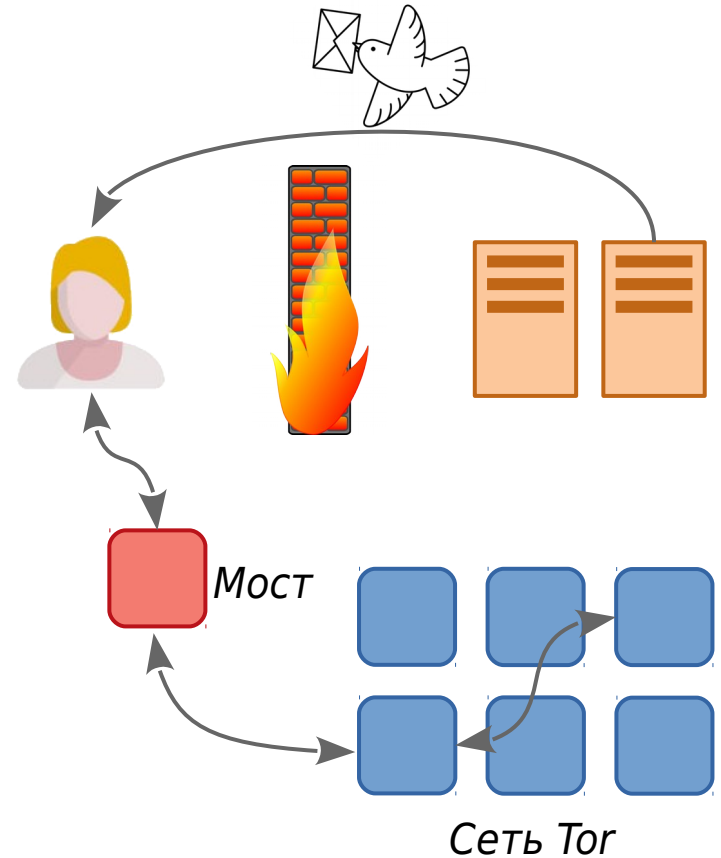
Серверу:
выходной узел.

Скрытые сервисы (Tor Hidden Services)



Мосты (Bridges)

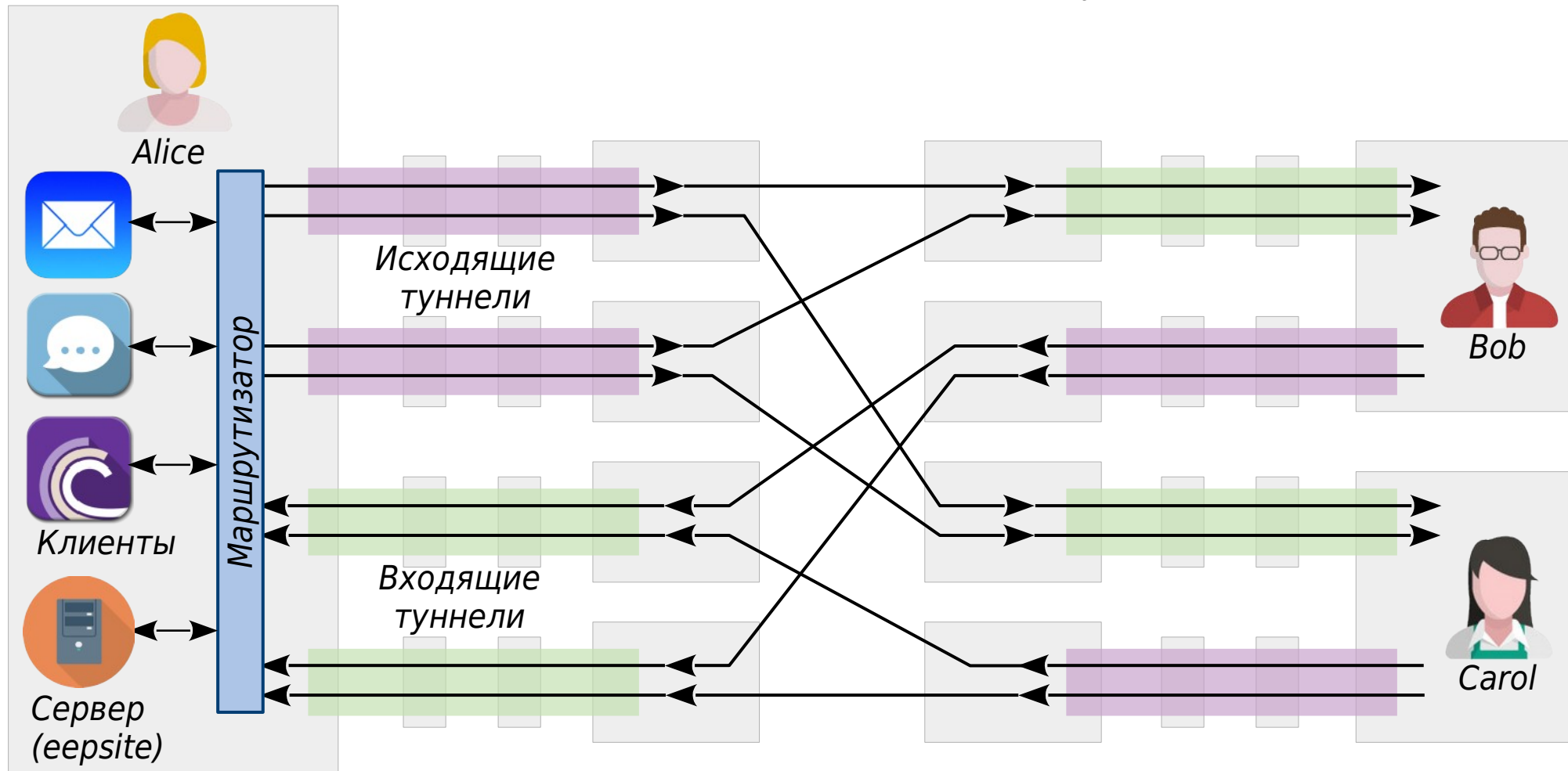
- Мост нужен для доступа к сети в случае отсутствия доступа к серверам каталогов.
- Мост используется как входной узел, а также для получения списка узлов.
- Список мостов секретный, они не публикуются на серверах каталогов.
- Специальный сервер хранит каталог мостов и выдаёт по несколько штук за каждый запрос. Таким образом, собрать полный список мостов долго и трудно.
- Возможна раздача через web, e-mail, службы обмена сообщениями, голубиную почту и т.д.



Уязвимости сети Tor

- Трафик на выходе из сети полностью расшифрован, выходной узел может его читать и модифицировать.
Защита: дополнительный слой сквозного шифрования (например, TLS).
Защита: механизмы отслеживания недобросовестных выходных узлов.
- Нет перемешивания пакетов и искусственных задержек, возможны тайминг атаки. Наблюдая трафик на входных и выходных узлах, можно соотнести начало и конец цепочки по объемам данных и интервалам между ними.
- Активный вариант тайминг-атаки. Внося задержки на входном узле, можно маркировать трафик для более достоверного опознания его на выходном узле.

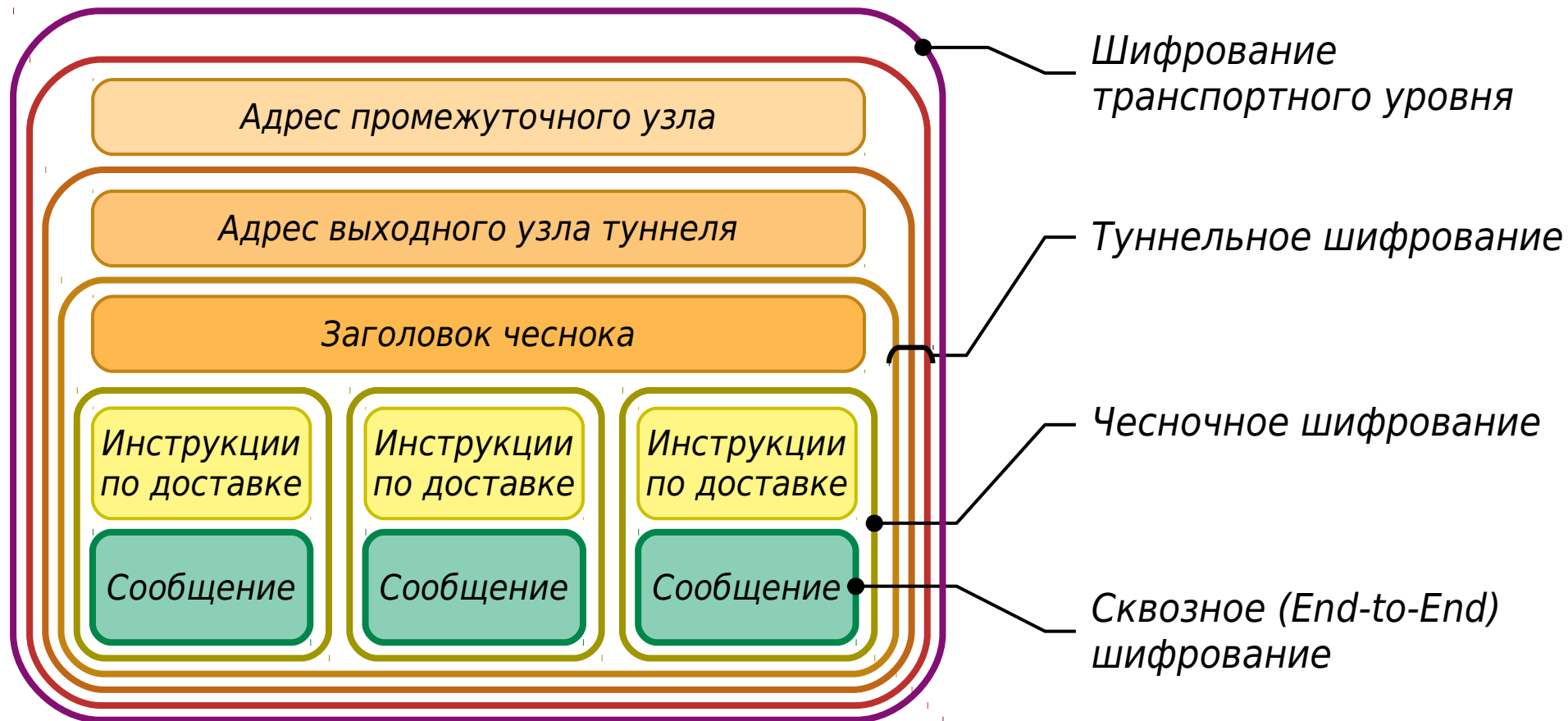
I2P – Invisible Internet Project



Адресация в сети I2P

- Распределённая база данных сети (**netDb**) хранит два типа записей:
 1. **routerInfo** — информация о маршрутизаторе:
IP-адрес, порт и тип транспорта
 2. **leaseSet** — информация о месте назначения:
набор входных шлюзов туннелей
- Для адресации ресурсов могут использоваться:
 1. Полное **Base64** имя — открытый ключ, 516 символов
`m-HrPrIAsdxts0WM~P4mE8mt9P7g-многомногобукв-nPBQAEAAcAAA==`
 2. **Base32** имя — хеш открытого ключа, 52 символа
`udhdrtrhetjm5sxzs1jyr5ztpeszydba4dpl3pl4utgqqw2v4jna.b32.i2p`
 3. **Символьное** имя — строка, хранящаяся на сервере имён
или в локальной адресной книге
`planet.i2p`

Чеснок как развитие идеи лука







Уязвимости сети I2P

- Подмена узлов и захват тоннелей. Атакующий создаёт большое количество узлов, одновременно добиваясь отключения существующих. Захват двух узлов в тоннеле означает захват всего тоннеля. Для успешной атаки требуется подмена от 2 до 20% узлов.
- Атака Сивиллы (Sybil attack). Атакующий создает множество идентификаторов узлов, расположенных в пространстве ключей рядом с атакуемым. Пользуясь “большинством” голосов, можно подменять содержимое DHT для атакуемого.
- Атака методом исключения.
 - составляем список узлов, потенциально являющихся маршрутизаторами для атакуемого узла
 - если атакуемый узел активен, исключаем из списка неактивные узлы
 - если атакуемый узел неактивен, исключаем из списка активные узлы
 - исключаем узлы, не подходящие под правила создания тоннелей

Ссылки

- Обратная связь:

 E-mail: android.ruberoid@gmail.com
 Telegram: [@androidruberoid](https://t.me/@androidruberoid)
 Bitmessage: [BM-2cSxghnvqBUWJ8D7ngfFu7AfsUxGJerxV6](https://bitmessage.org/?addr=BM-2cSxghnvqBUWJ8D7ngfFu7AfsUxGJerxV6)
 Tox: [94C1DEBE4521CC811C4CED57DE9CB9AAB2C1E831F867EED
7BC0145869E87A55577BB3AA996F5](https://tox.chat/94C1DEBE4521CC811C4CED57DE9CB9AAB2C1E831F867EED7BC0145869E87A55577BB3AA996F5)

- Материалы лекций:

 github.com/notOcelot/Kocherga_crypto

- Видео:

 [youtube.com/channel/
UCeLSDFOndI4eKFutg3oowHg](https://youtube.com/channel/UCeLSDFOndI4eKFutg3oowHg)

