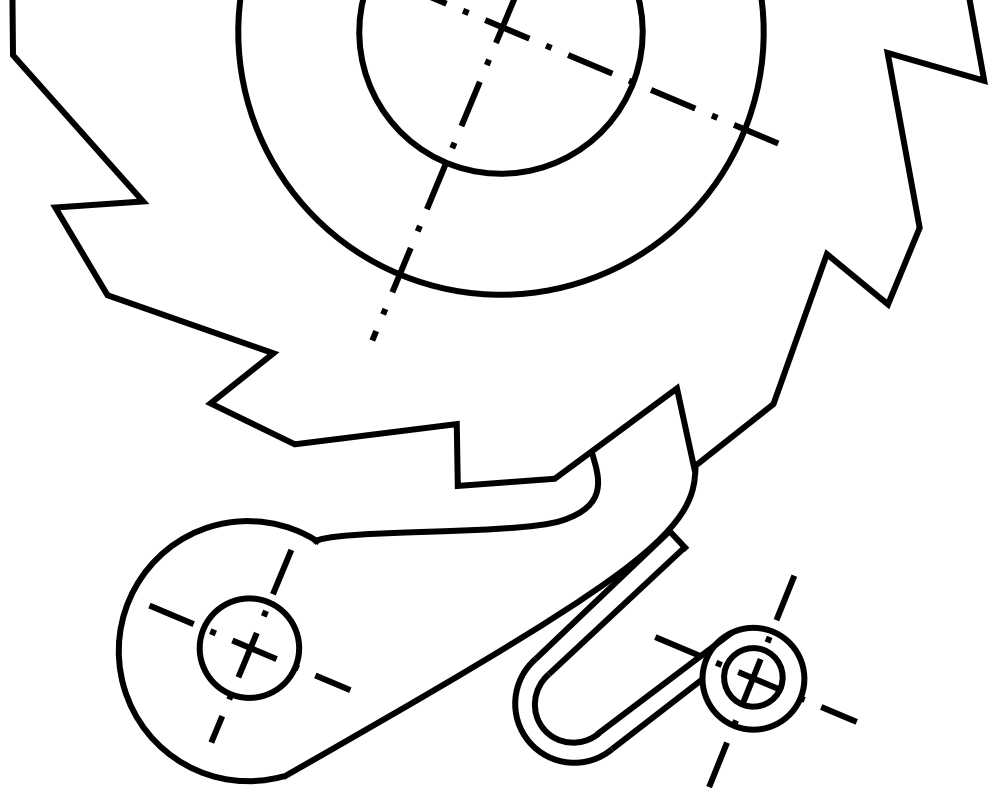
Обмен сообщениями с использованием алгоритма Double Ratchet

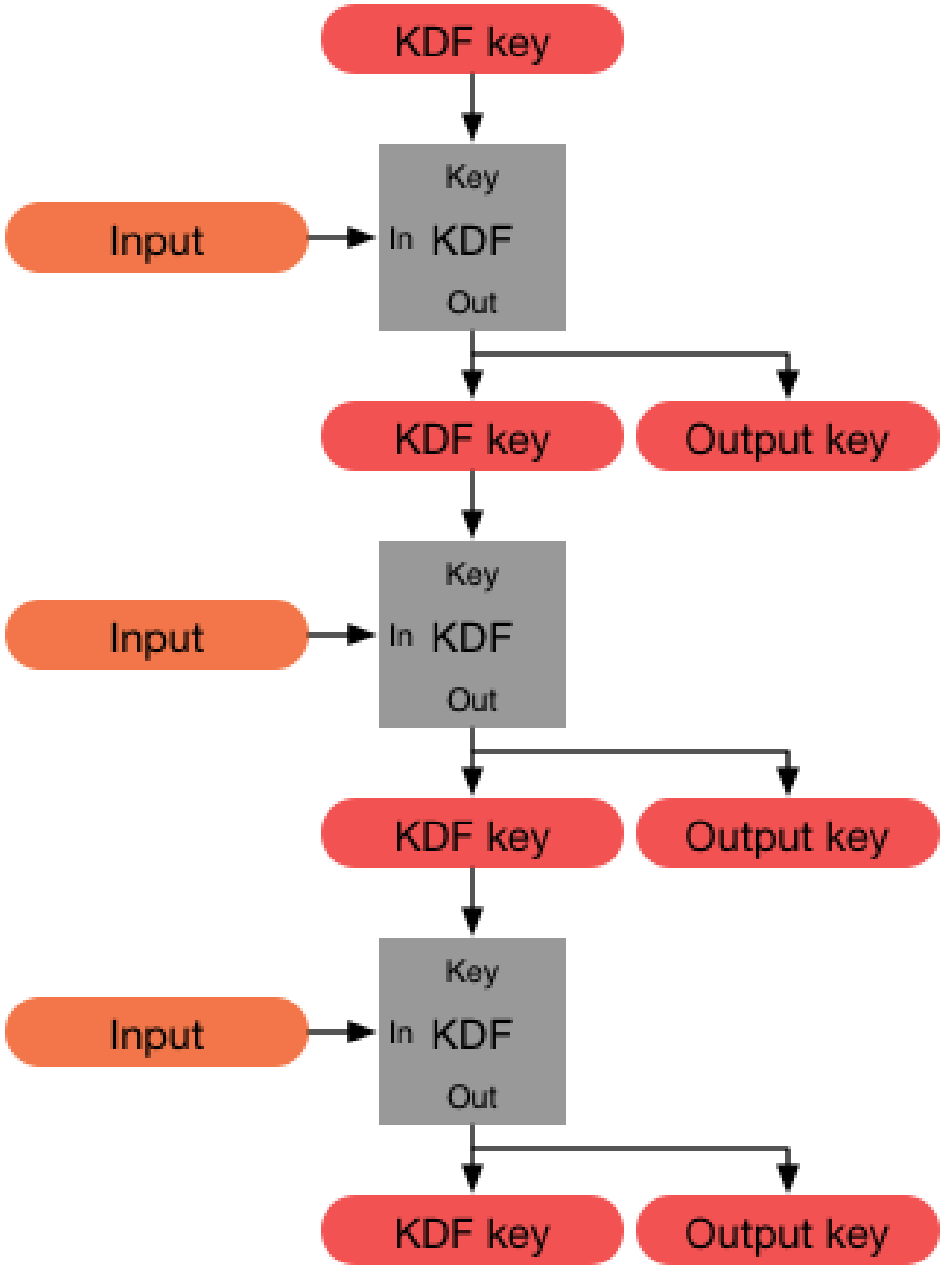


Выполнил студент
группы КБ-211

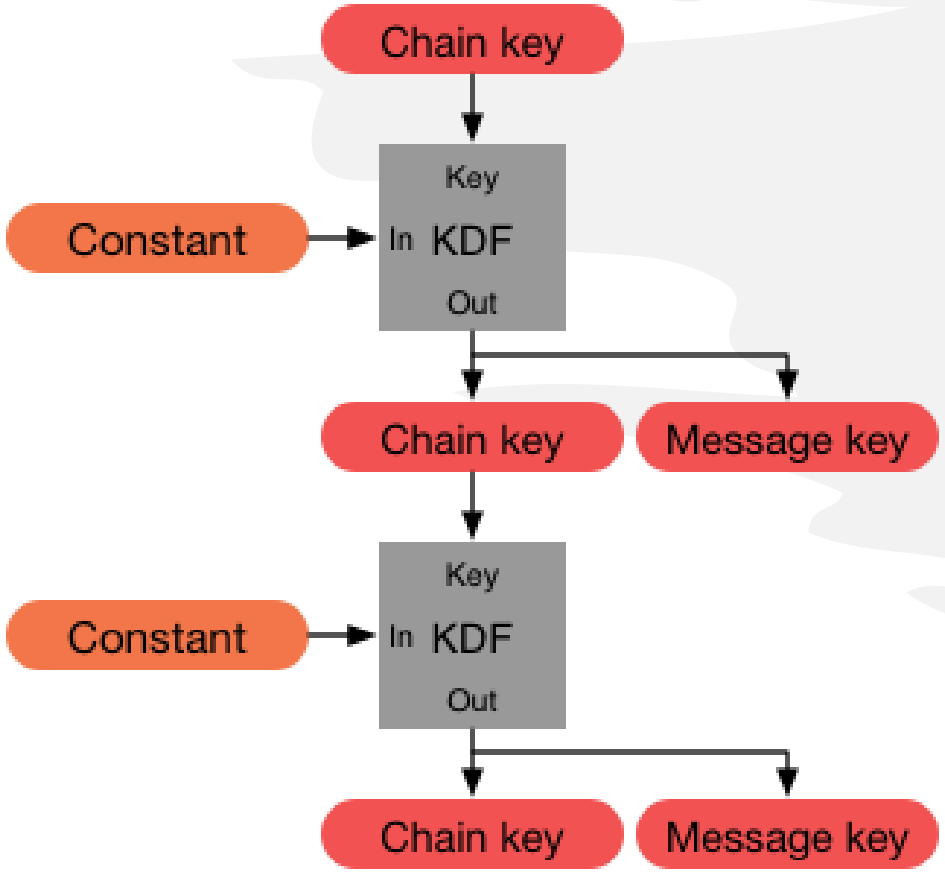
Коренев Денис

Цепочка KDF

- *Key derivation function* - криптографическая функция, которая принимает секретный случайный ключ и некоторые входные данные и возвращает выходные данные.
- Примеры – HMAC и HKDF.

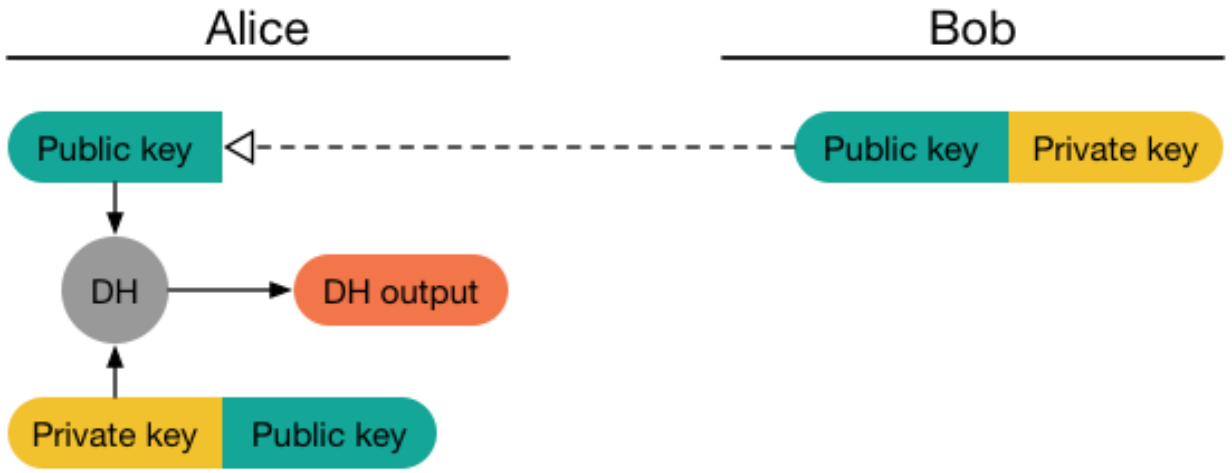


Храповик с симметричным ключом



- Каждое отправленное или полученное сообщение шифруется уникальным ключом сообщения.
- Ключи сообщений являются выходными ключами цепочек KDF отправителя и получателя.

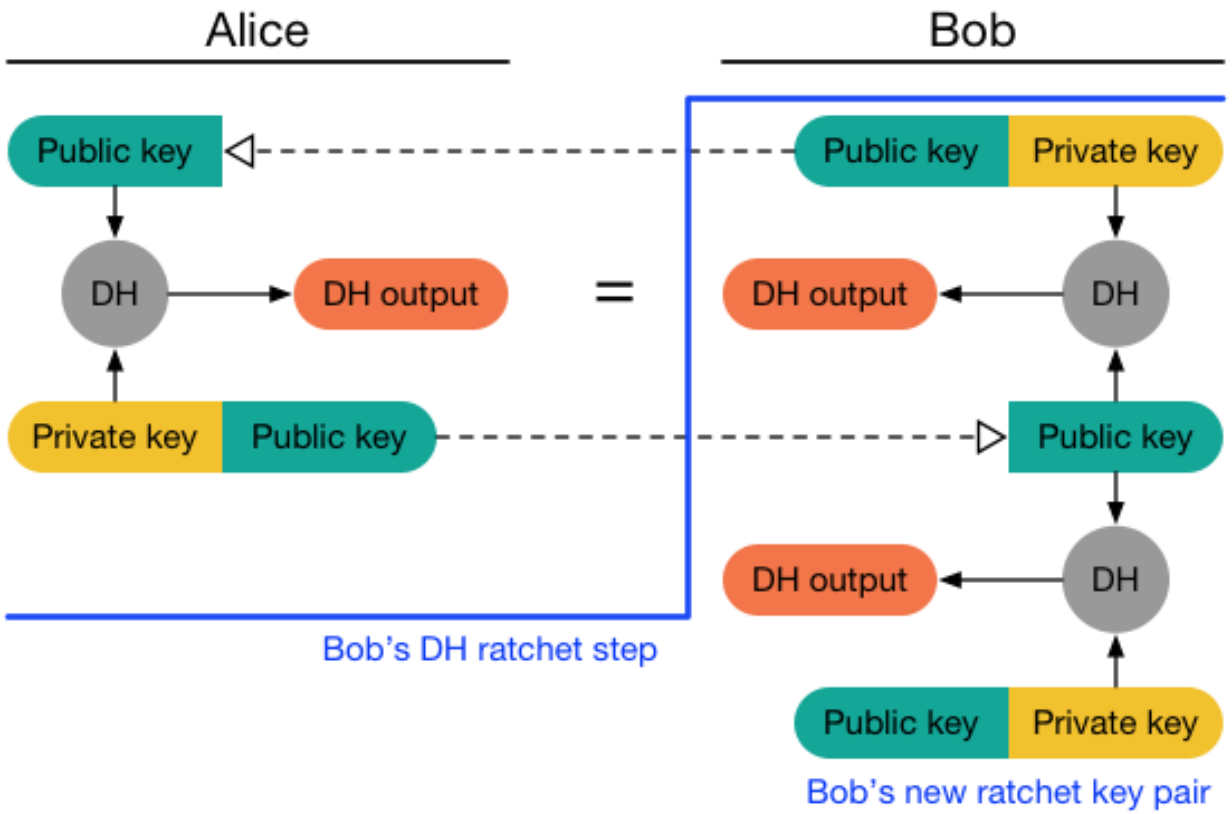
Храповик Диффи-Хеллмана



Когда от удаленной стороны поступает новый открытый ключ храповика, выполняется шаг храповика DH, который заменяет текущую пару ключей храповика локальной стороны новой парой ключей.

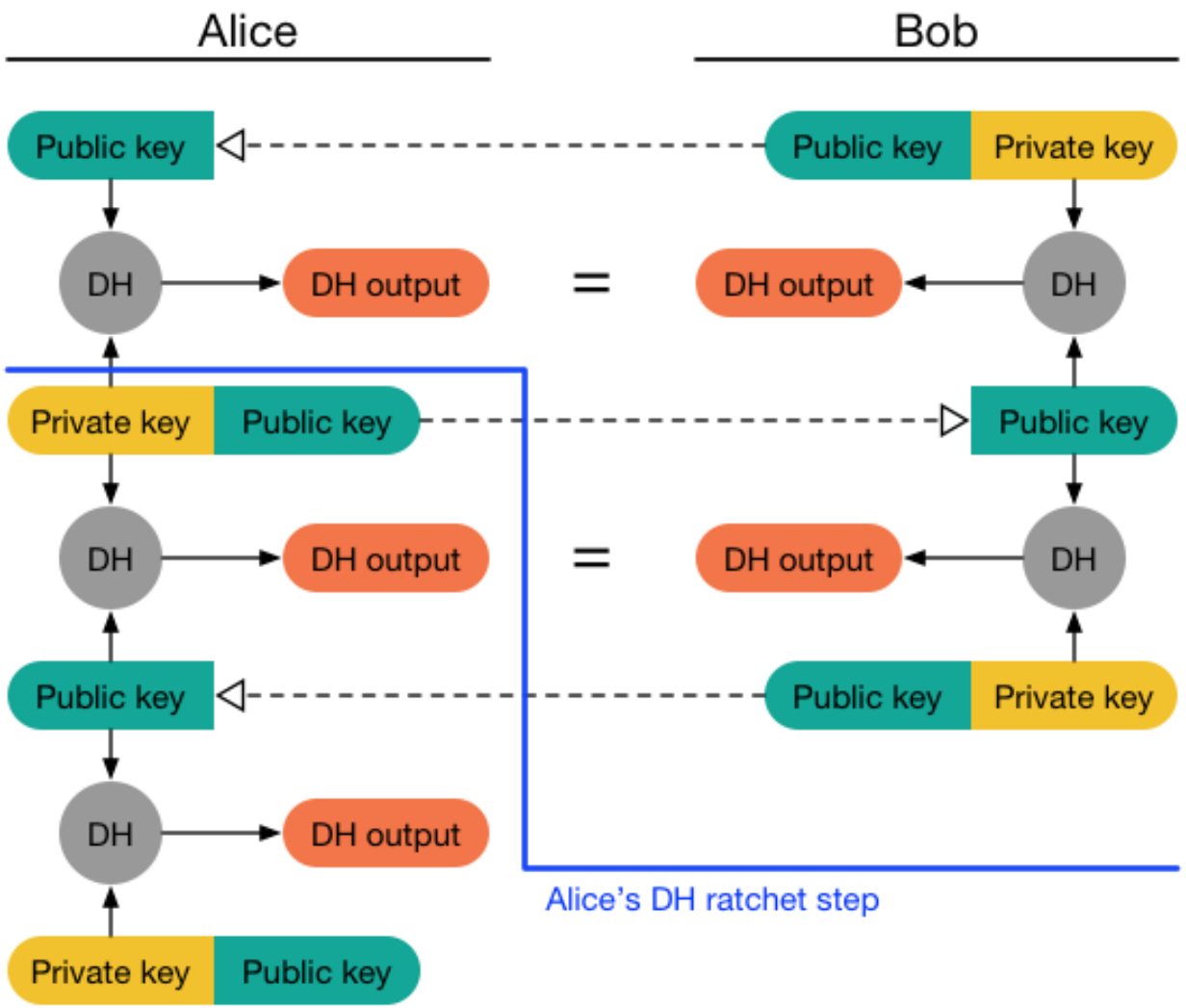
Храповик Диффи-Хеллмана

Когда от удаленной стороны поступает новый открытый ключ храповика, выполняется шаг храповика DH, который заменяет текущую пару ключей храповика локальной стороны новой парой ключей.



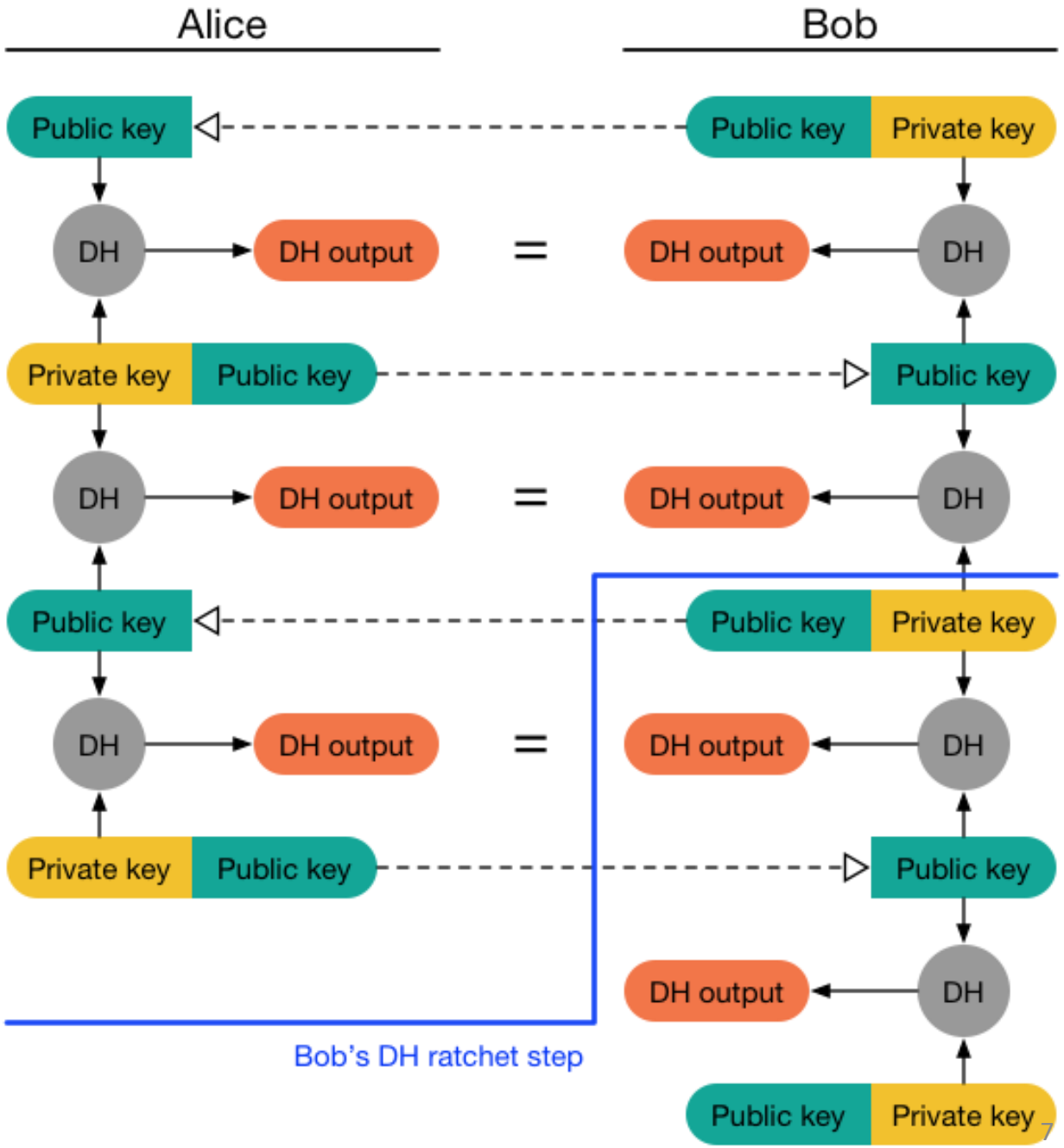
Храповик Диффи-Хеллмана

Когда от удаленной стороны поступает новый открытый ключ храповика, выполняется шаг храповика DH, который заменяет текущую пару ключей храповика локальной стороны новой парой ключей.



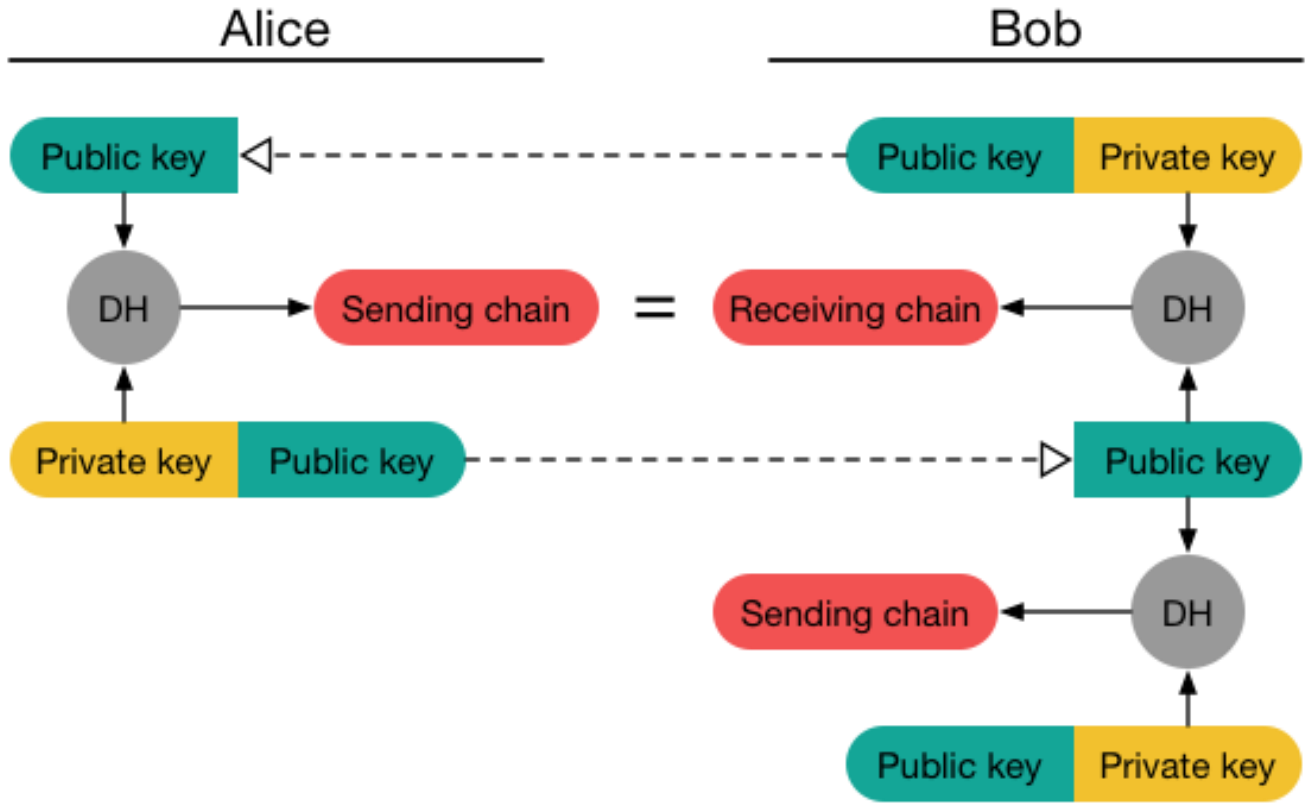
Храповик Диффи-Хеллмана

Когда от удаленной стороны поступает новый открытый ключ храповика, выполняется шаг храповика DH, который заменяет текущую пару ключей храповика локальной стороны новой парой ключей.



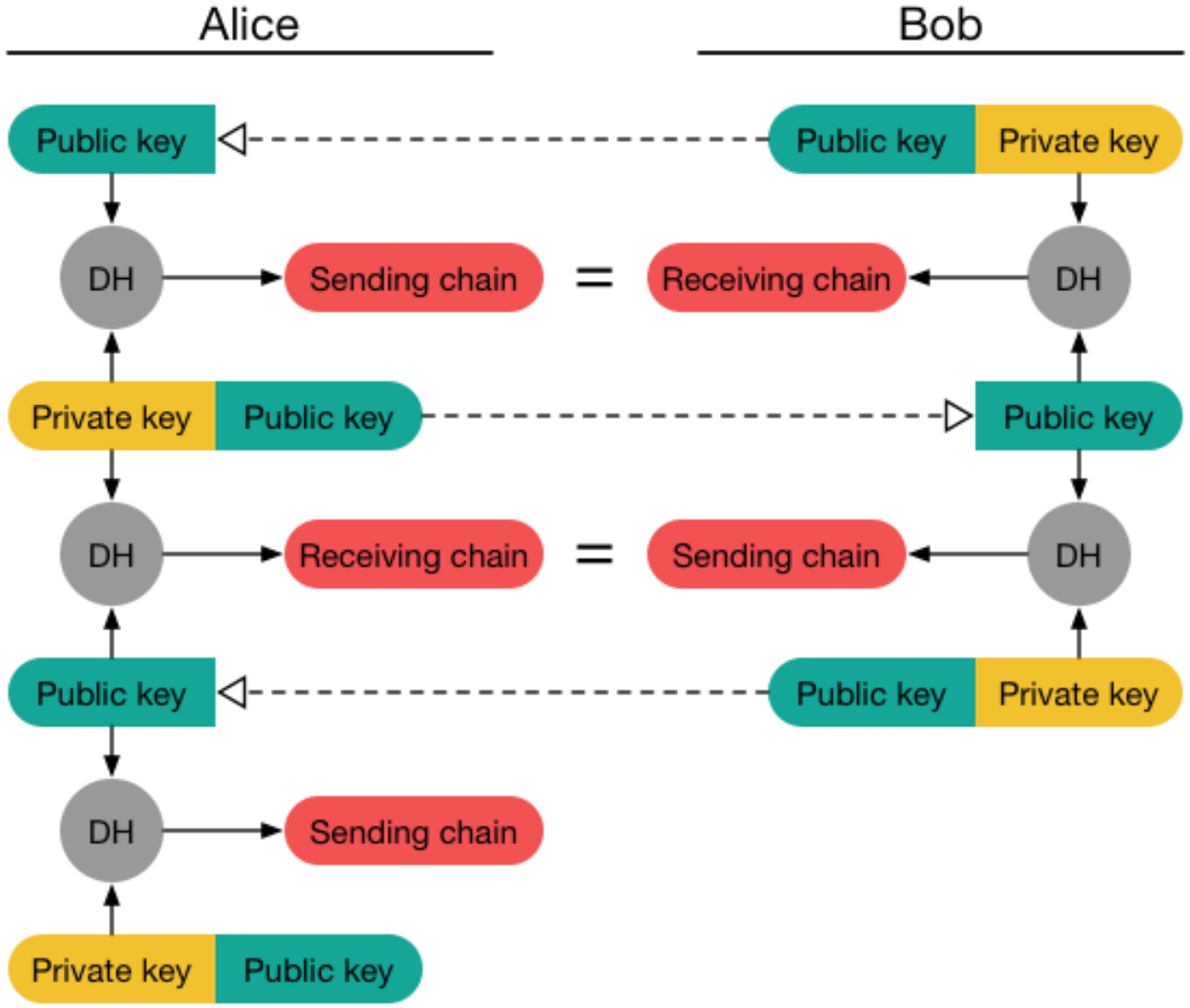
Храповик Диффи-Хеллмана

Когда от удаленной стороны поступает новый открытый ключ храповика, выполняется шаг храповика DH, который заменяет текущую пару ключей храповика локальной стороны новой парой ключей.



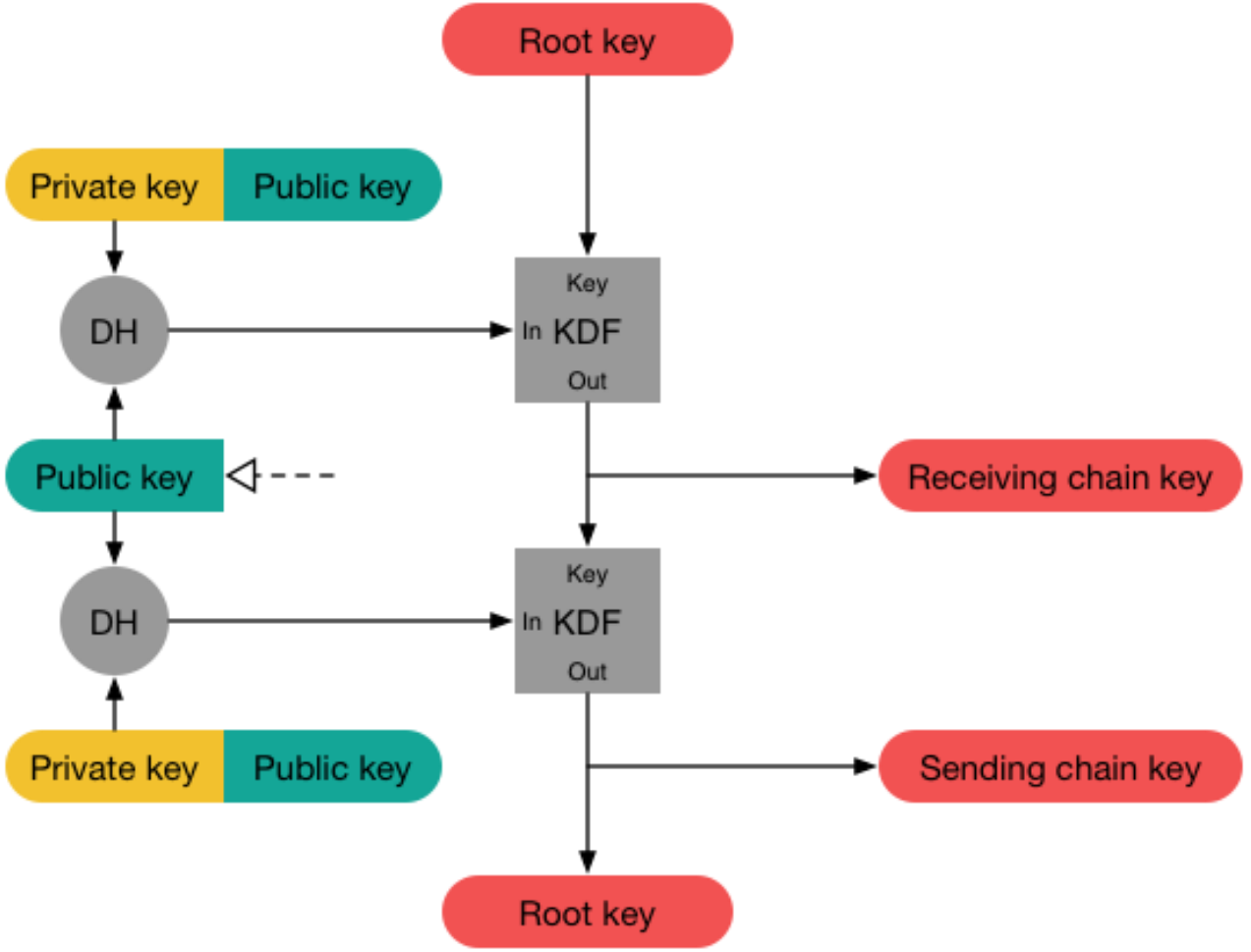
Храповик Диффи-Хеллмана

Когда от удаленной стороны поступает новый открытый ключ храповика, выполняется шаг храповика DH, который заменяет текущую пару ключей храповика локальной стороны новой парой ключей.



Храповик Диффи-Хеллмана

Когда от удаленной стороны поступает новый открытый ключ храповика, выполняется шаг храповика DH, который заменяет текущую пару ключей храповика локальной стороны новой парой ключей.



Двойной Храповик

Сочетание симметрично-ключевого и DH-храповика дает двойной храповик:

- Когда сообщение отправляется или принимается, к цепочке отправителей или получателей применяется шаг храповика симметричного ключа для получения ключа сообщения.
- Когда получен новый открытый ключ храповика, перед храповиком симметричных ключей выполняется шаг храповика DH для замены цепных ключей.

Реализация алгоритма

Double Ratchet

Обмен сообщениями клиент-сервер