Обеспечение криптографически защищенных групповых коммуникаций с функцией отказуемости

Мария Коростелева, Денис Гамаюнов,
лаборатория безопасности информационных систем,
МГУ им. М.В.Ломоносова

История безопасного общения

- До 1991 информация не шифруется
  - IRC, e-mail, BBS (электронная доска объявлений)
- 1991 — появление PGP
  - Конфиденциальность, целостность, аутентификация, невозможность отказа от авторства
- Середина 90-х — системы мгновенного обмена сообщениями
- Начало 2000-х шифрование мгновенных сообщений

Модель нарушителя

Нарушитель — глобальный неограниченный в ресурсах человек в середине, который может перехватывать трафик, контролировать физические устройства, в том числе конечные узлы.

- PGP и др. — защита во время коммуникации, защита от MITM-атак
- Как обеспечить защиту данных после завершения коммуникаций?

Популярные средства обеспечения безопасности общения

	Шифрование потока	ЭЦП	MAC/HMAC	Аутентификация/ идентификация	Абсолютная секретность передачи
PGP	+	+	+	+	–
SSL/TLS	+	–	+	+	–
Проприетарные решения (напр. Skype)	+	?	?	+	?

Пример из реальной жизни

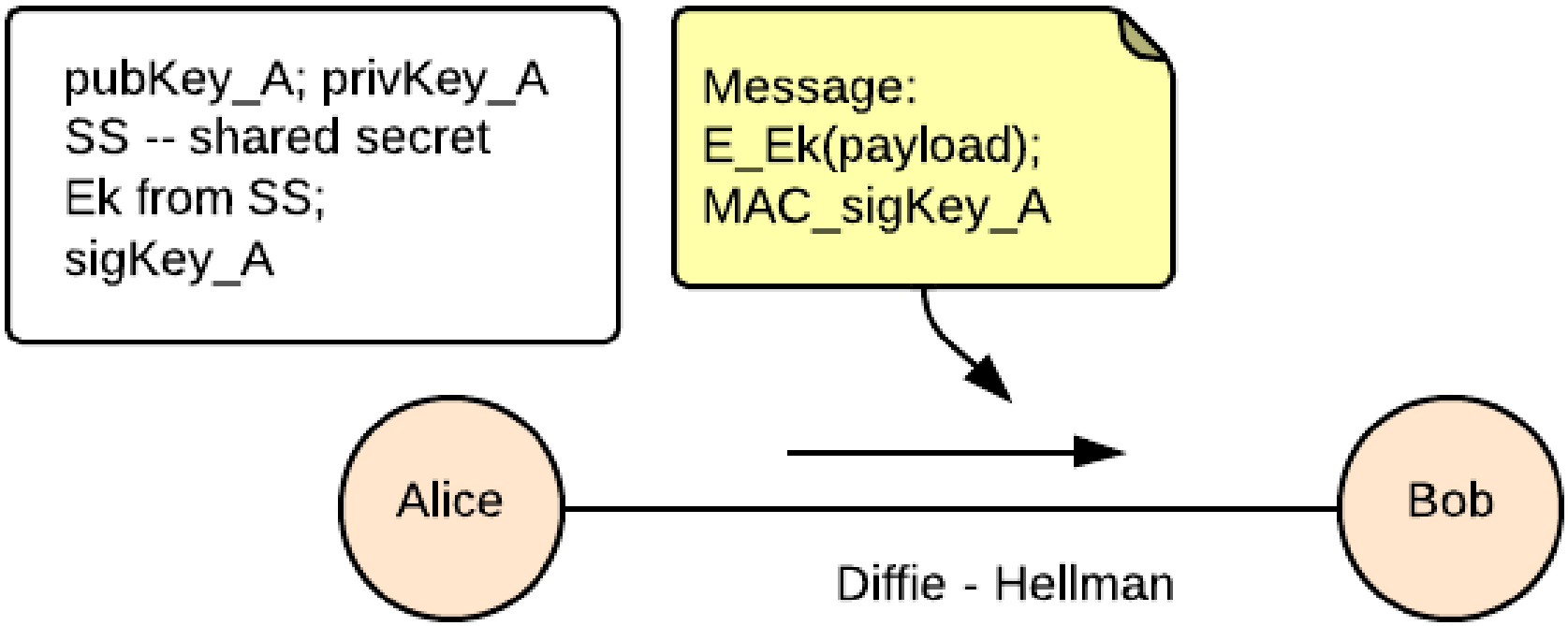
Люди разговаривают в изолированной комнате:

- никто больше не услышит их разговор,
  - если разговор не записывается,
- никто больше не знает, о чем они говорят,
  - если участники сами не расскажут,
- никто не может документально подтвердить сказанное,
  - даже сами участники разговора.

OTR — Off-The-Record messaging

- Ян Голберг и Никита Борисов, 2004
- Ключевые свойства:
  - Абсолютная секретность передачи
  - Отказуемость
- Плагины к клиентам обмена мгновенными сообщениями (Pidgin) — работают поверх стандартных IM-протоколов, OtrSMS, CryptoCat

Схема OTR

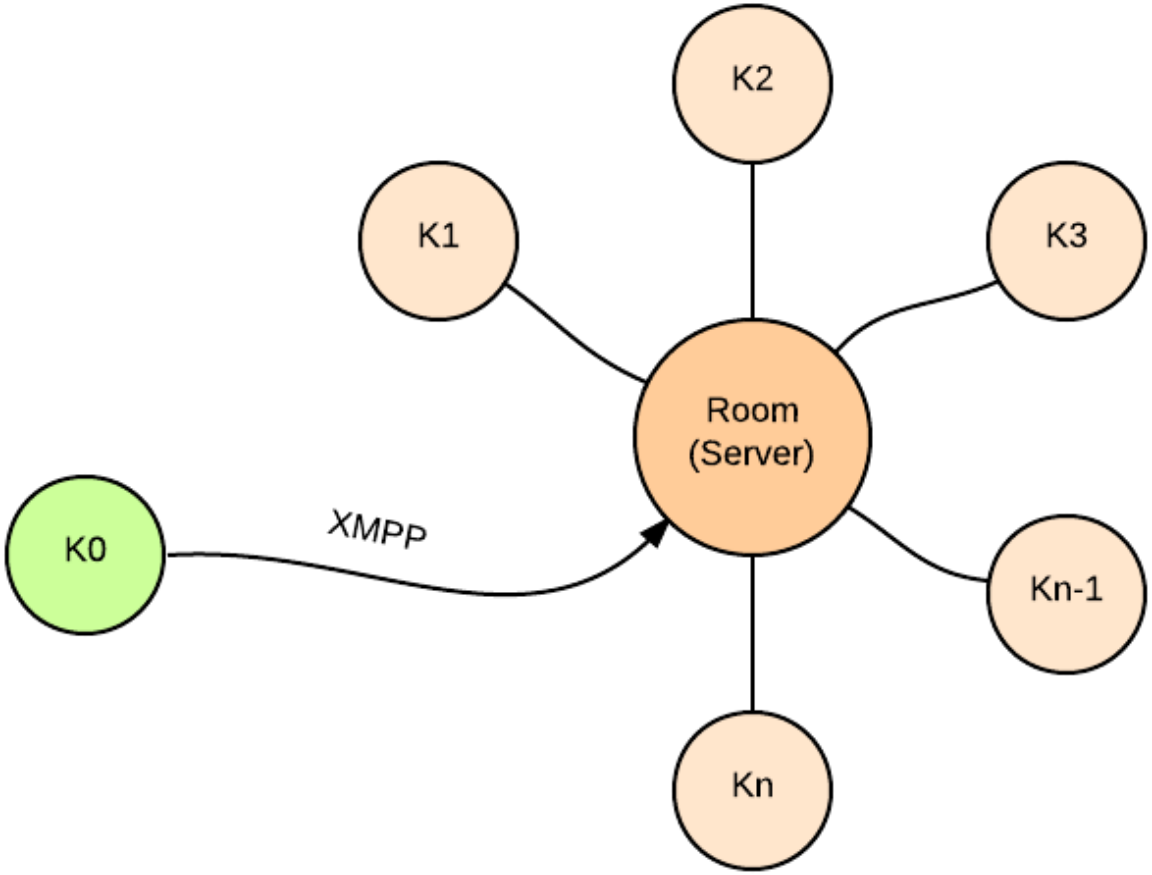


[0] Nikita Borisov, Ian Goldberg, Eric Brewer. Off-the-Record Communication, or, Why Not to Use PGP. Workshop on Privacy in the Electronic Society, 2004

Multy-Party Off-the-Record

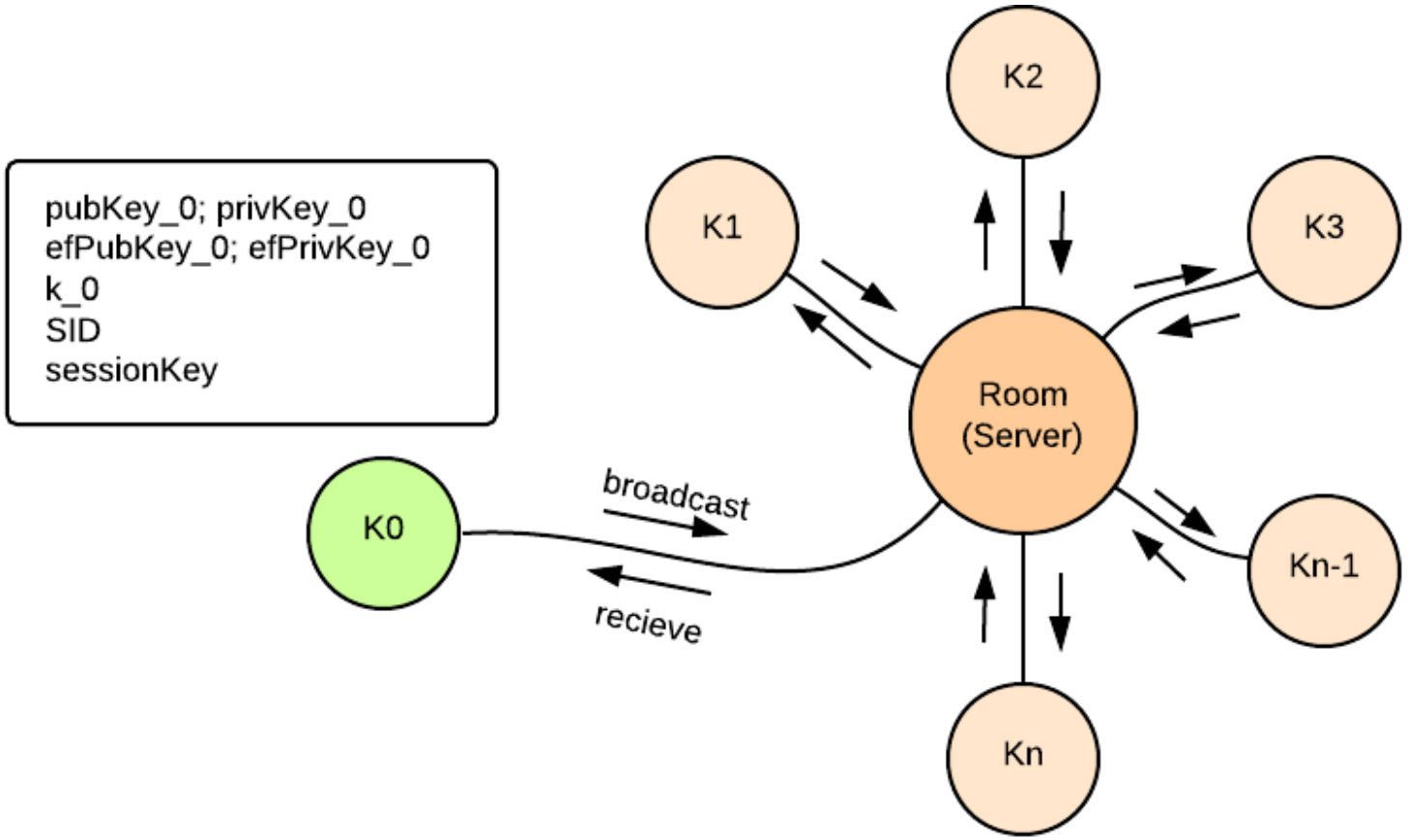
- Протокол, аналогичный OTR, но пригодный для общения группы людей
- Ключевые свойства:
  - Абсолютная секретность передачи
  - Отказуемость
  - Синхронизация потока сообщений
- Четыре основные фазы

mpOTR: фаза установки канала



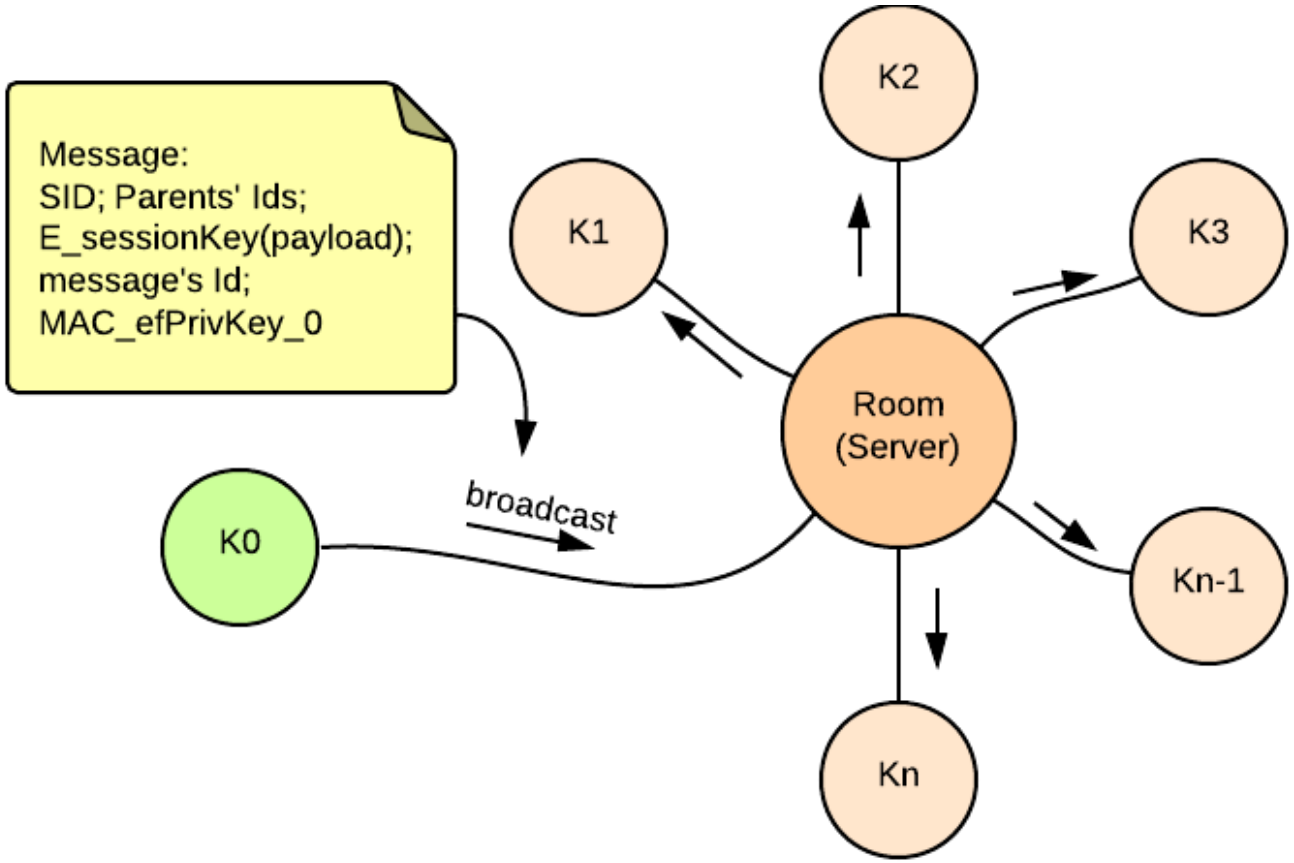
[1] Peter Saint-Andre. XEP-0045: Multy-User Chat. The XMPP Standards Foundation. 1999-2014

mpOTR: фаза аутентификации и обмена ключами



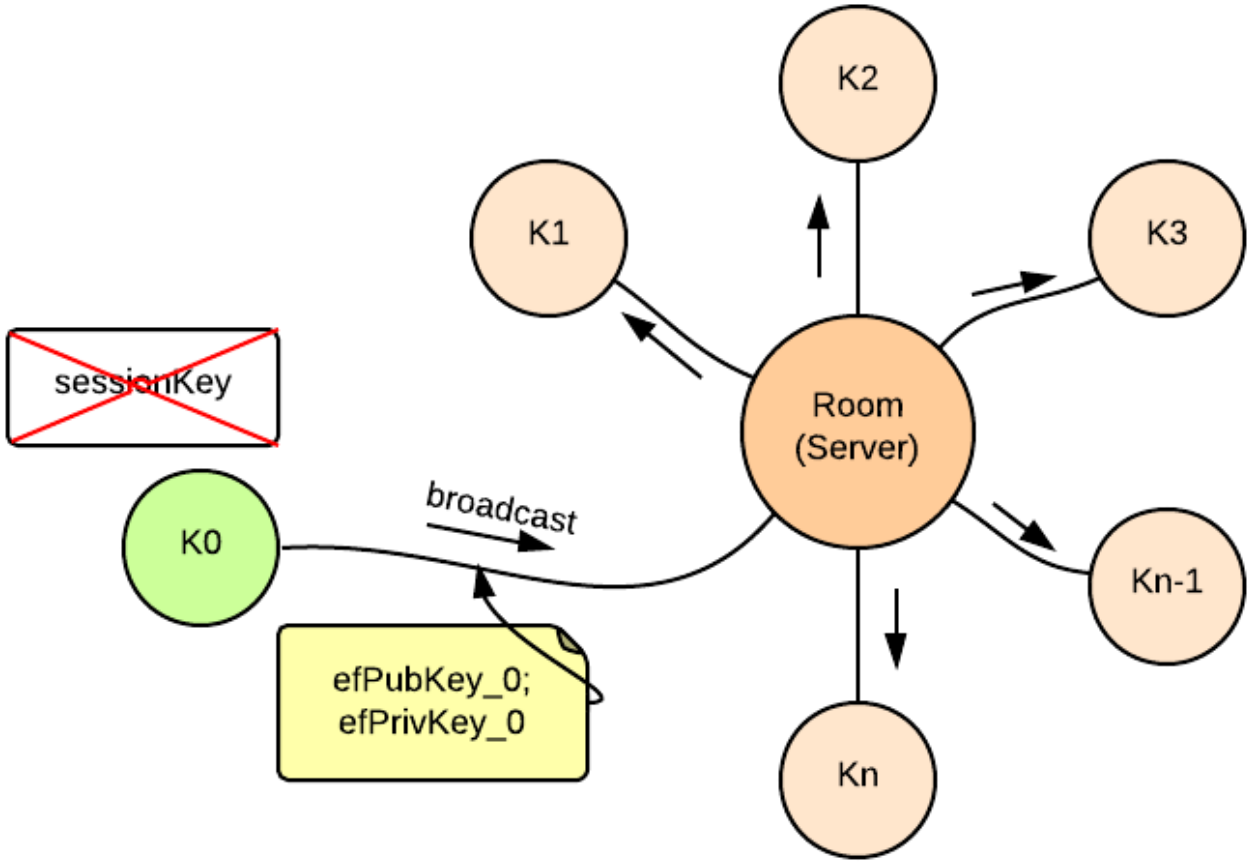
Используется вариант алгоритма Диффи-Хеллмана для группп и схема аутентификации Шнорра:
[2] Matthew Van Gundy. Improved Deniable Signature Key Exchange for mpOTR. 2013

mpOTR: фаза коммуникации



[3] Matthew D. Van Gundy, Hao Chen. OldBlue: Causal Broadcast In A Mutually Suspicious Environment.

mpOTR: фаза завершения



Другие протоколы

- Telegram
  - Использует протокол MTProto
  - Режим «Secret Chat» — end-to-end шифрование с применением AES-256 в режиме IGE (Infinite Garble Extension)
  - https://core.telegram.org/mtproto
- Torchat
  - Анонимный чат с шифрованием
  - Использует Tor Hidden Servicies
  - Особенных функций поверх возможностей Tor не добавляет
- И т.д.

Спасибо за внимание!