конференция РусКрипто

СМАРТС КВАНТТЕЛЕКОМ

Влияние плотности соединений на безопасность квантовой сети

«Любая физическая теория —это своего рода догадка. Тому, как делать наилучшие догадки, учит нас теория вероятностей»
Ричард Фейнман

Гайдаш А.А., Мирошничеко Г.П., **Козубов Антон Владимирович,** к.ф.-м.н.,

Руководитель отдела перспективных исследований ООО «СМАРТС-Квантттелеком»

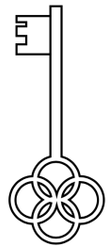
Руководитель теоретической группы лаборатории квантовых процессов и измерений, Университет ИТМО

Научный сотрудник отдела математических методов квантовых технологий, Математический институт им. В.А. Стеклова Российской Академии Наук

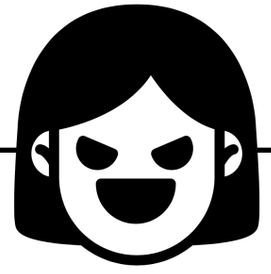
Доступные криптографические примитивы

Дано:

— открытый классический канал



— предраспределенный ключ

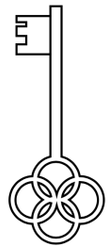


— незащищенный квантовый канал

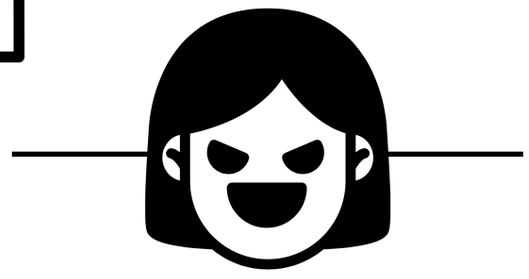
Доступные криптографические примитивы

Дано:

— открытый классический канал

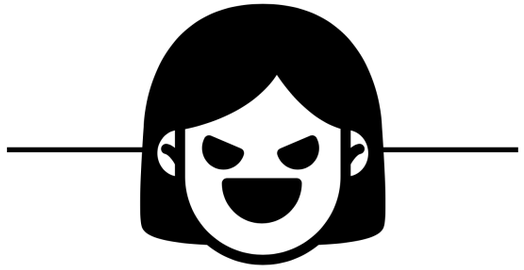


— предраспределенный ключ



— незащищенный квантовый канал

Необходимо:



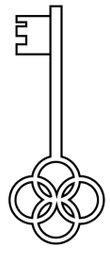
— незащищенный квантовый канал

— аутентифицированный классический канал

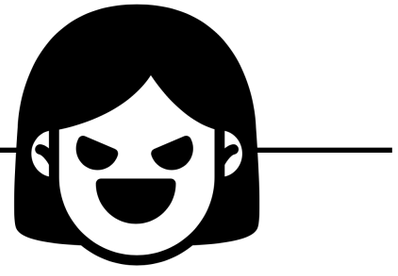
Доступные криптографические примитивы

Дано:

— открытый классический канал

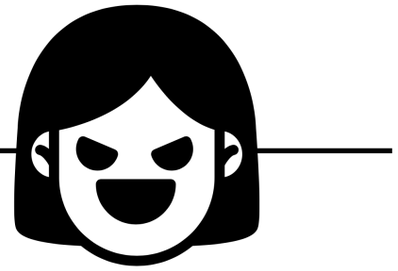


— предраспределенный ключ



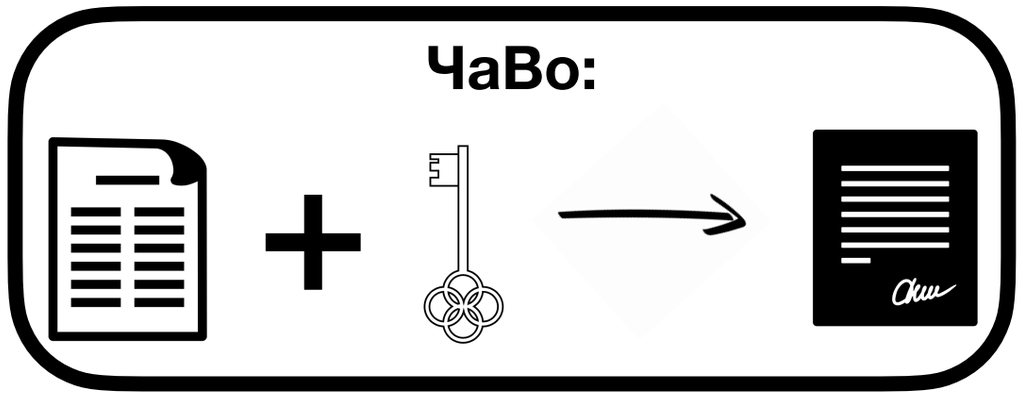
— незащищенный квантовый канал

Необходимо:



— незащищенный квантовый канал

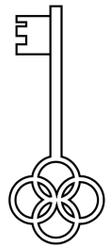
— аутентифицированный классический канал



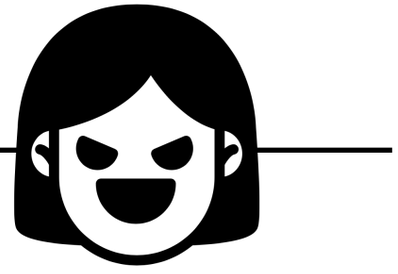
Доступные криптографические примитивы

Дано:

— открытый классический канал

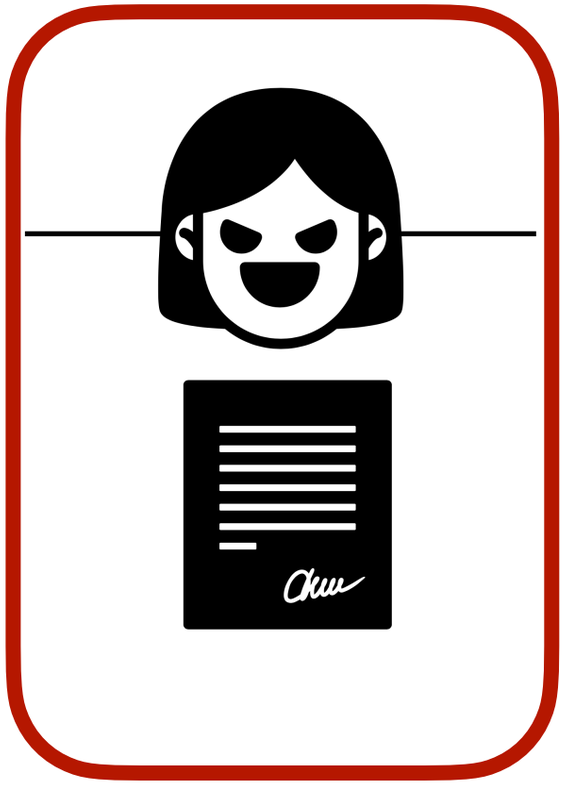


— предраспределенный ключ



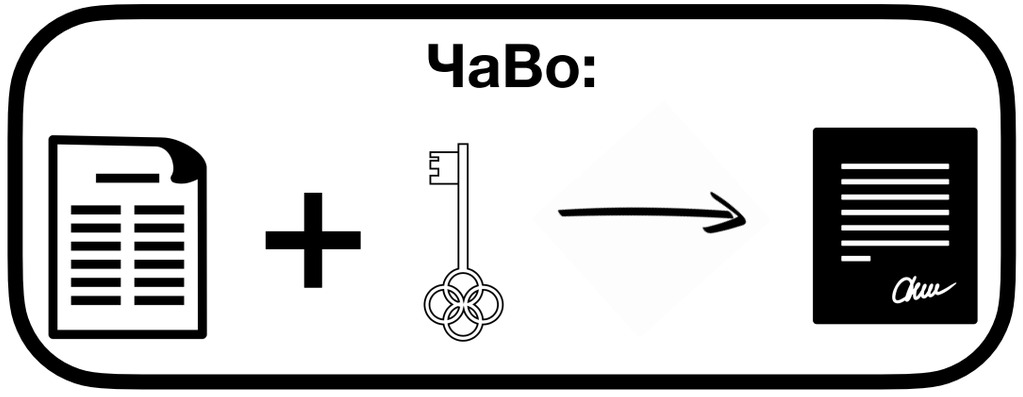
— незащищенный квантовый канал

Необходимо:

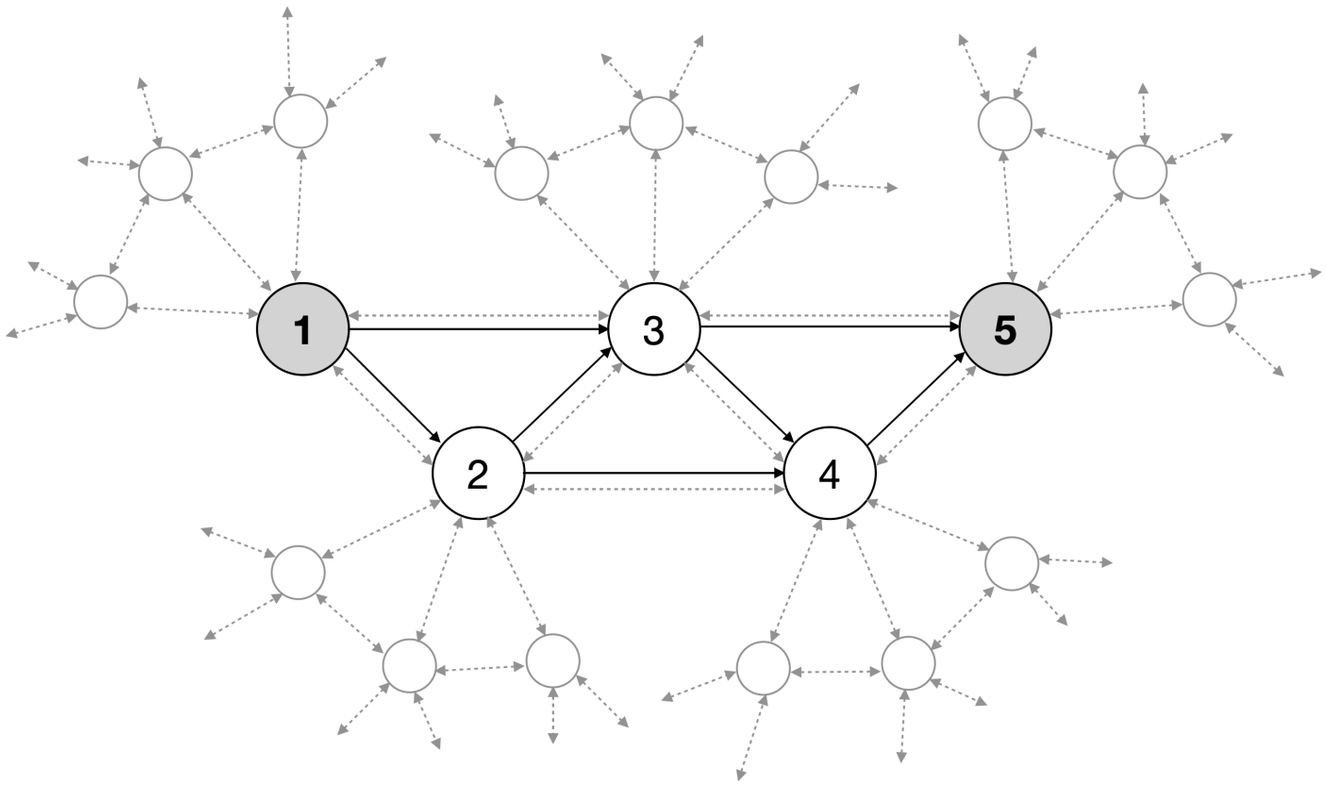


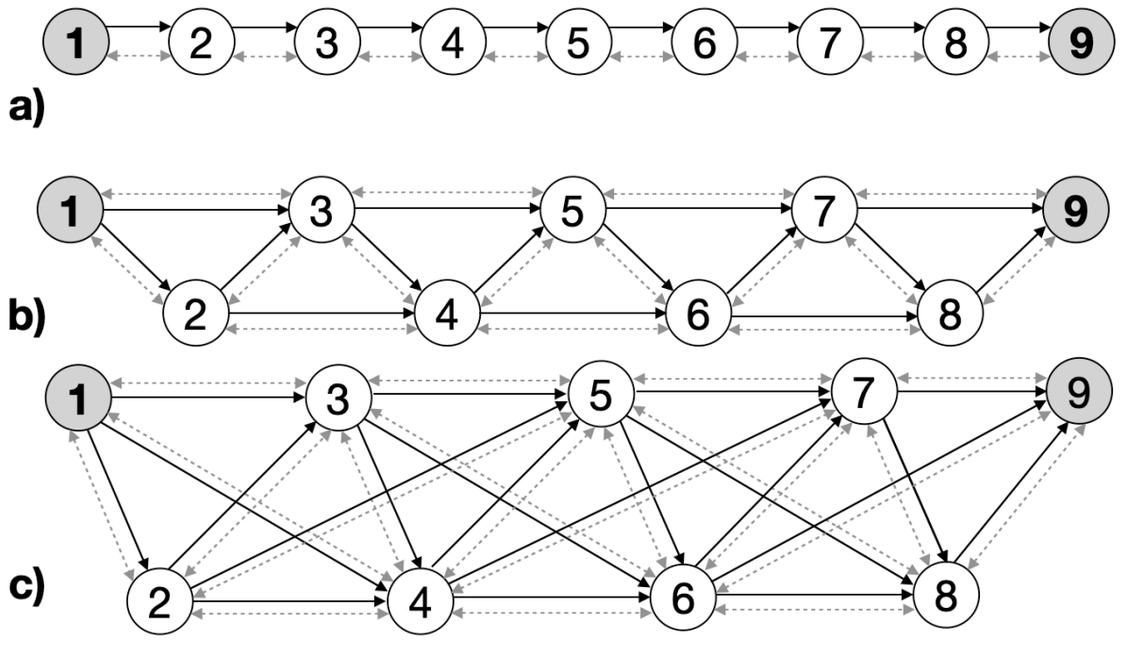
— незащищенный квантовый канал (ε_{qkd} — вероятность получения нарушителем какой-либо информации о ключе)

— аутентифицированный классический канал (ε_{auth} — вероятность успешной атаки на протокол аутентификации)

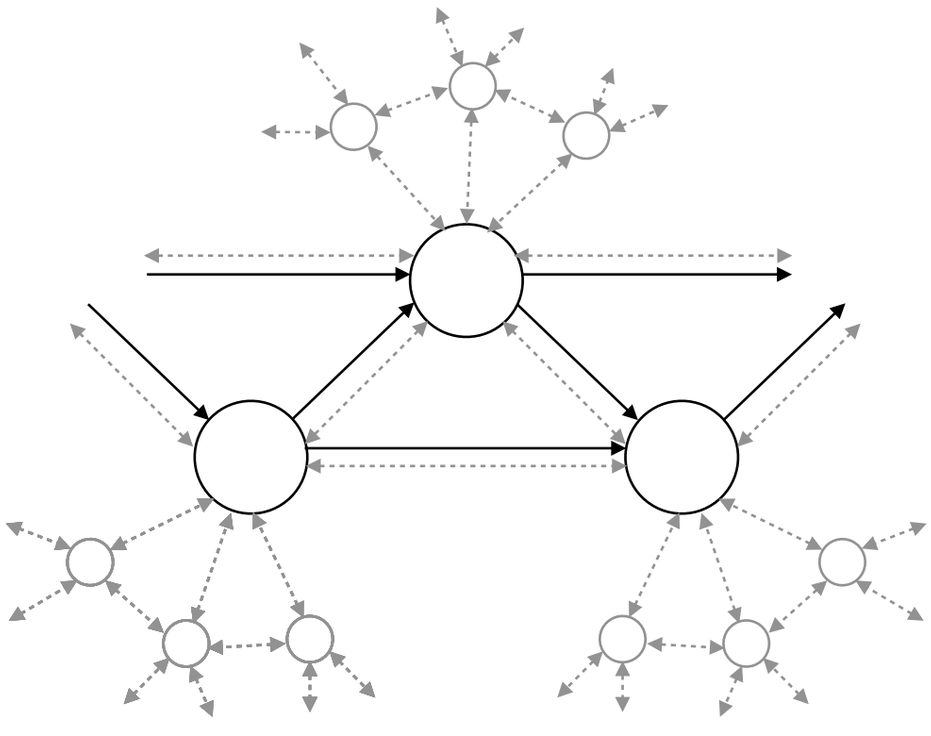


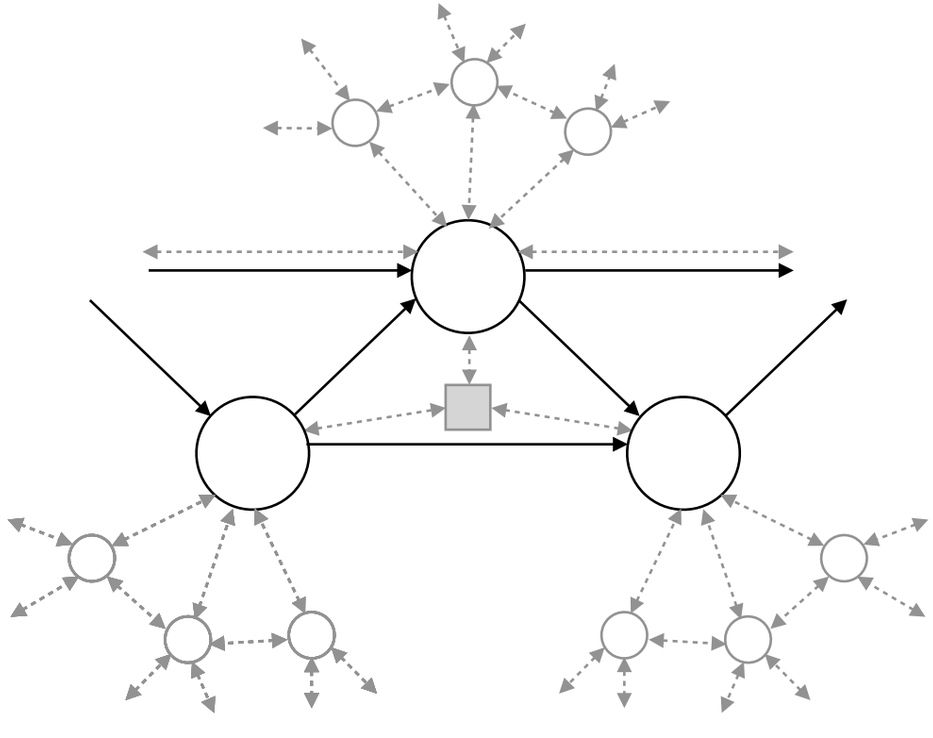
Постановка задачи





— доверенный узел — КРК соединение — направление КТ





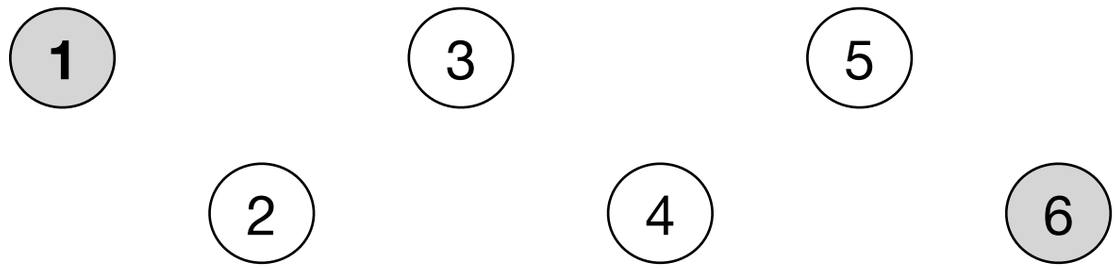
Используемые приближения

- КРК соединения могут быть любого типа, единственное условие: ε_{qkd} — вероятность получения нарушителем какой-либо информации о ключе из КРК соединения между любыми двумя узлами
- Все узлы предполагаются доверенными. ε_{auth} — вероятность успешной атаки на протокол аутентификации на любом из узлом
- Расстояние между двумя соседними узлами должно быть меньше предельного. Расстояние между двумя максимально удаленными узлами с прямым соединение (через $c-1$) следует считать предельным.

Gaidash A., Miroshnichenko G., Kozubov A. Quantum network security dependent on connection density between trusted nodes // arXiv preprint arXiv:2202.09162. – 2022.

Ключевой транспорт

1. Аутентификация

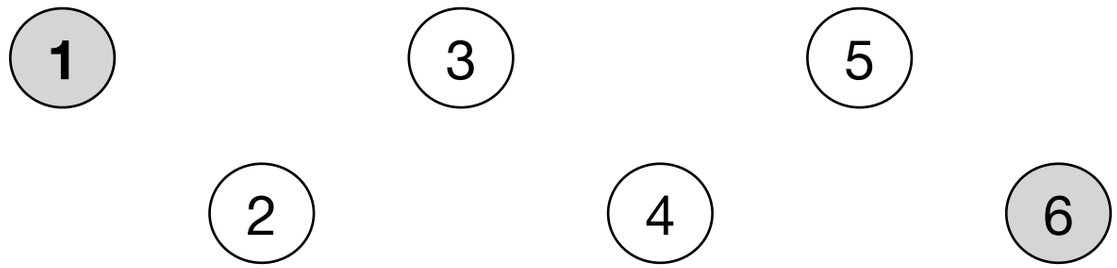


2. Квантовое распределение ключей

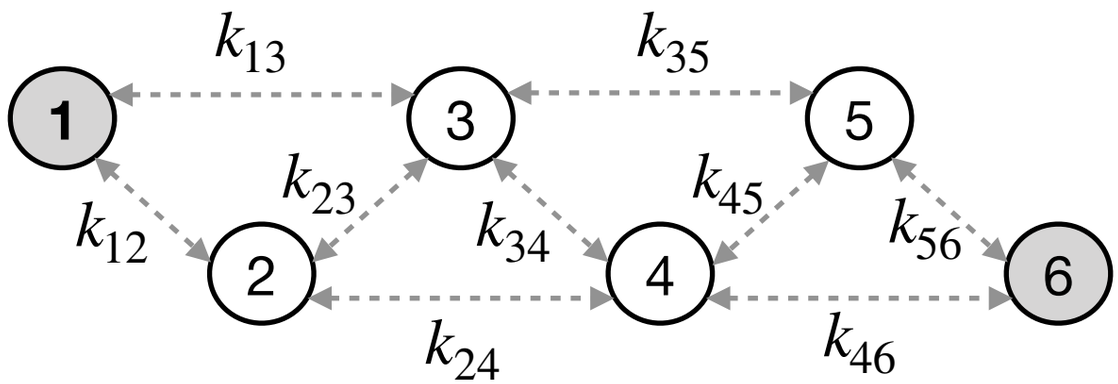
3. Ключевой транспорт

Ключевой транспорт

1. Аутентификация



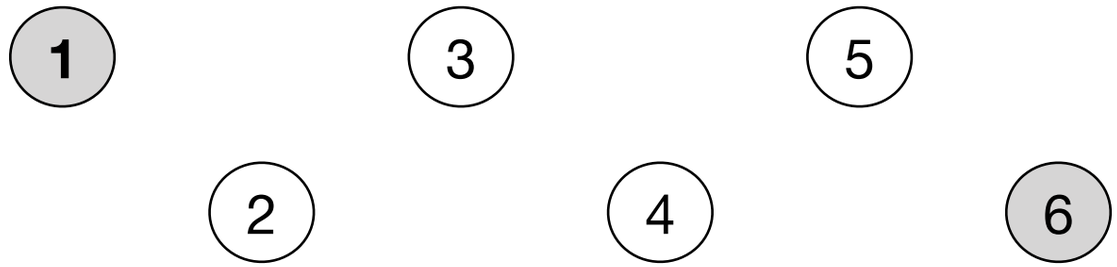
2. Квантовое распределение ключей



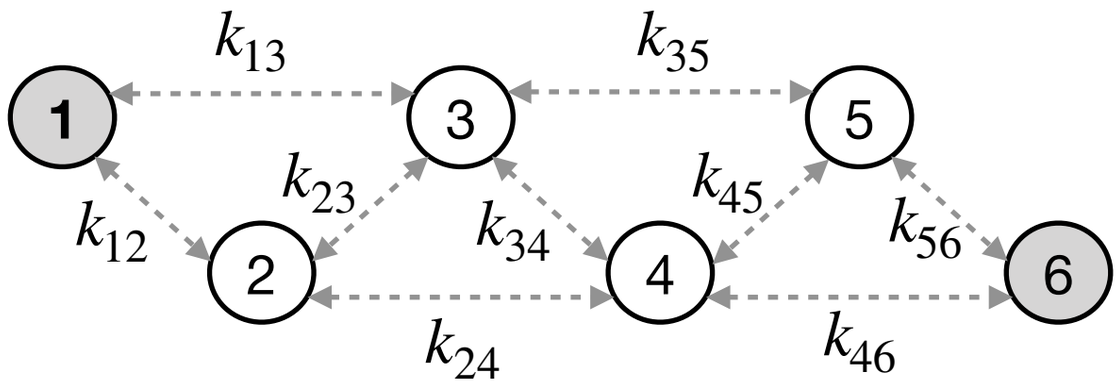
3. Ключевой транспорт

Ключевой транспорт

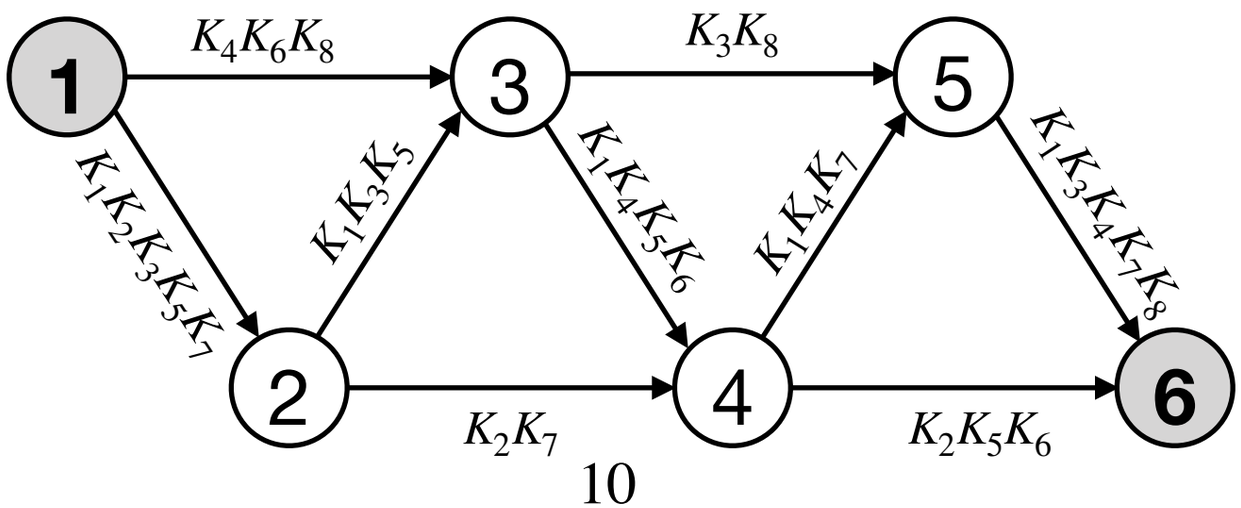
1. Аутентификация



2. Квантовое распределение ключей

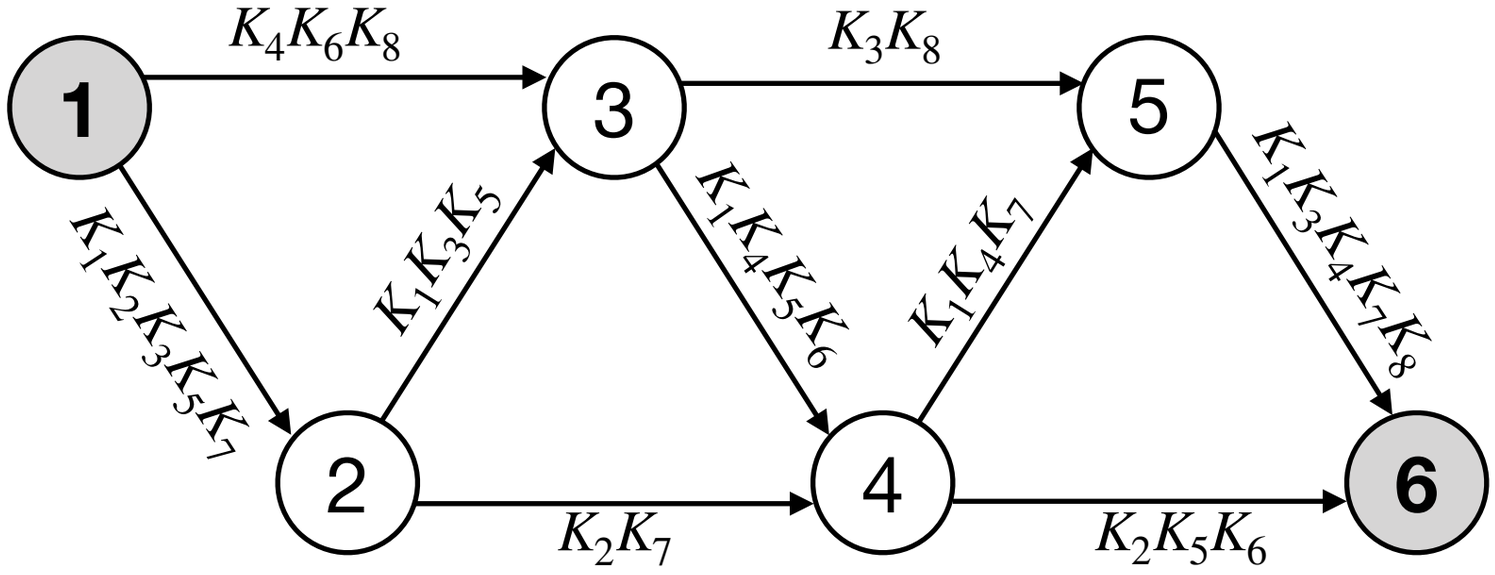


3. Ключевой транспорт

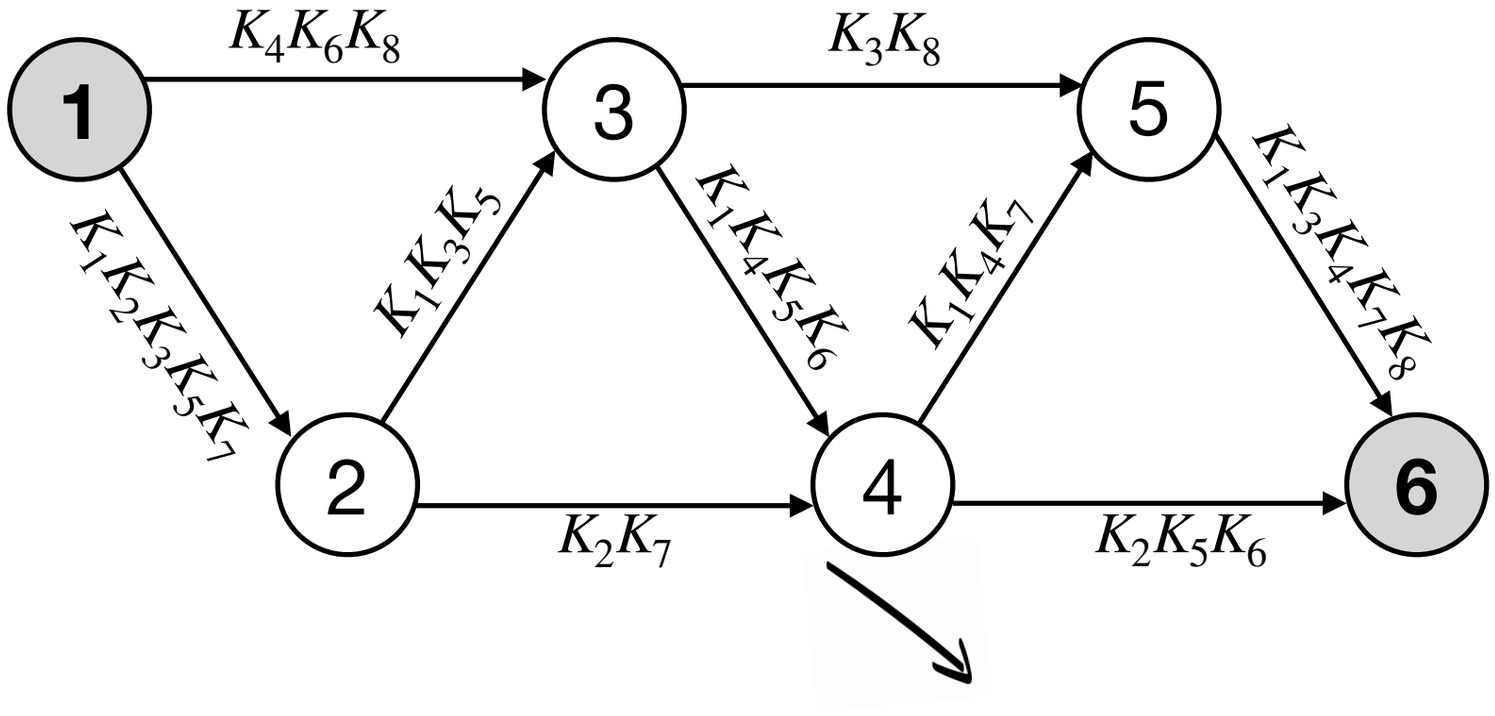


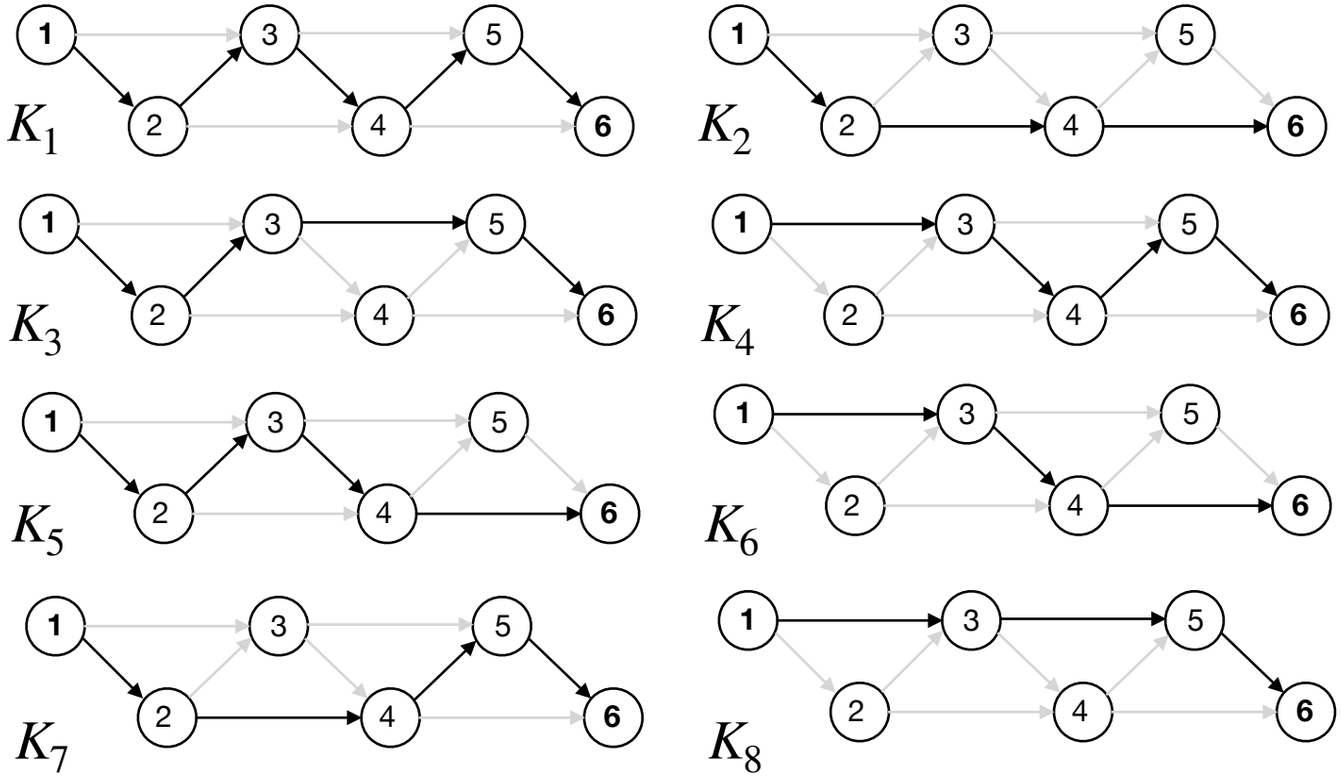
$$K_{16} = \bigoplus_{i=1}^{8} K_i$$

Ключевой транспорт

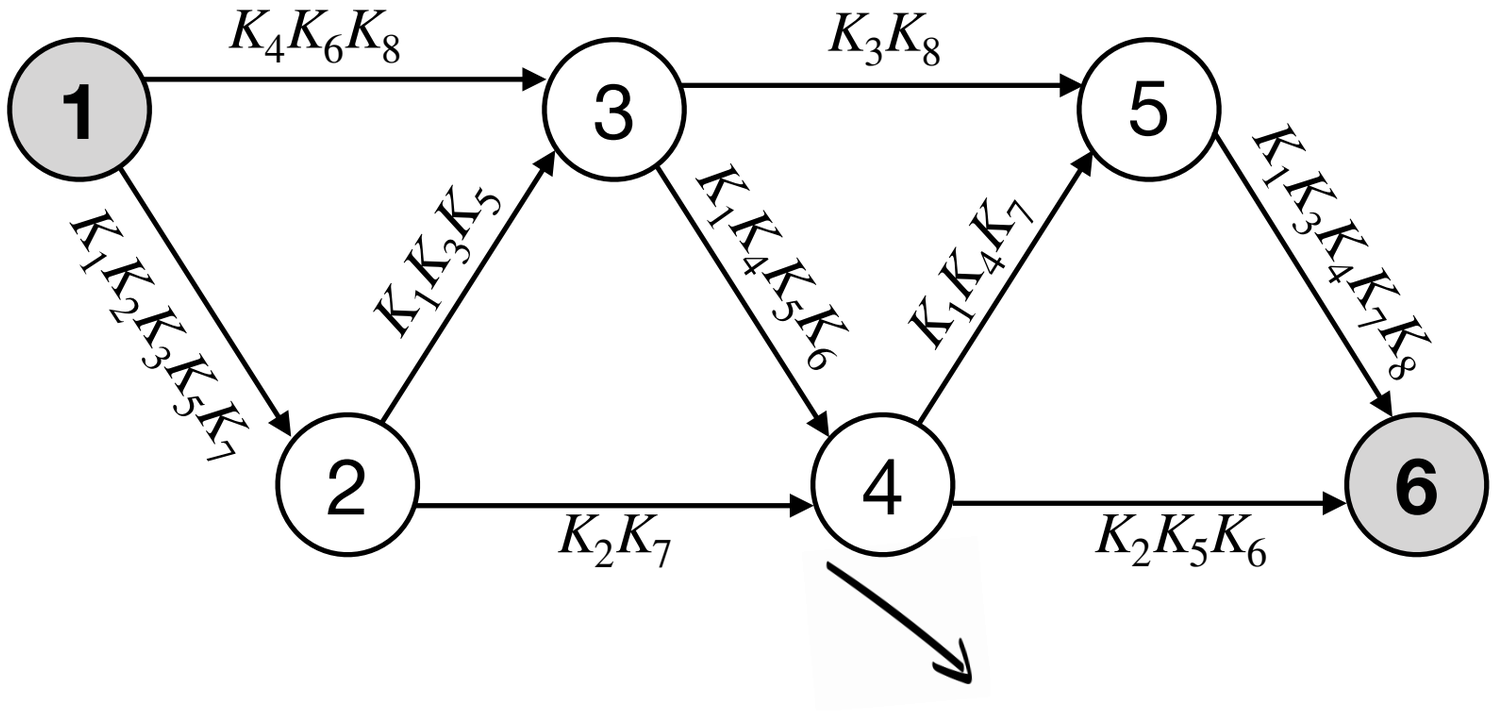


Ключевой транспорт





Ключевой транспорт



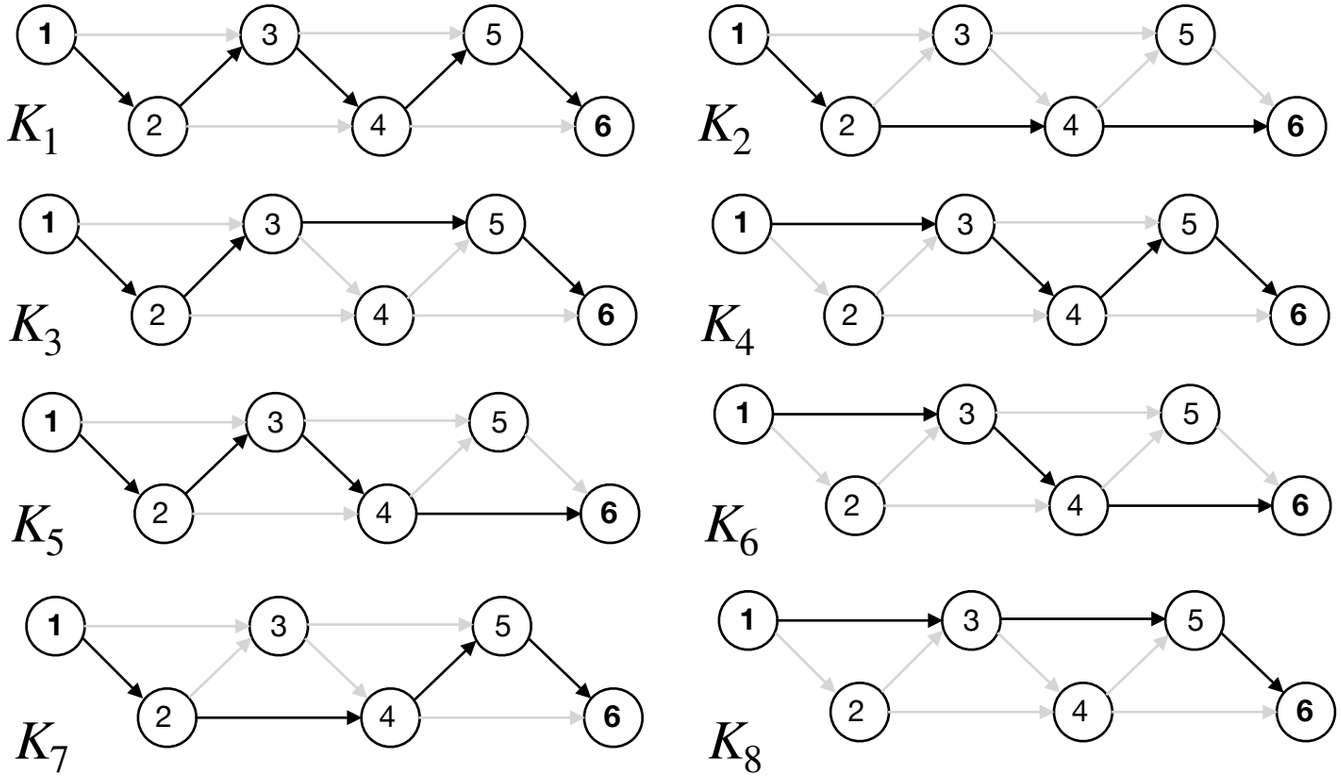
$(K_1K_2K_3K_5K_7) \bigoplus k_{12}$ $(K_4K_6K_8) \bigoplus k_{13}$

$(K_1K_3K_5) \bigoplus k_{23}$ $(K_2K_7) \bigoplus k_{24}$

$(K_1K_4K_5K_6) \bigoplus k_{34}$ $(K_3K_8) \bigoplus k_{35}$

$(K_1K_4K_7) \bigoplus k_{45}$ $(K_2K_5K_6) \bigoplus k_{46}$

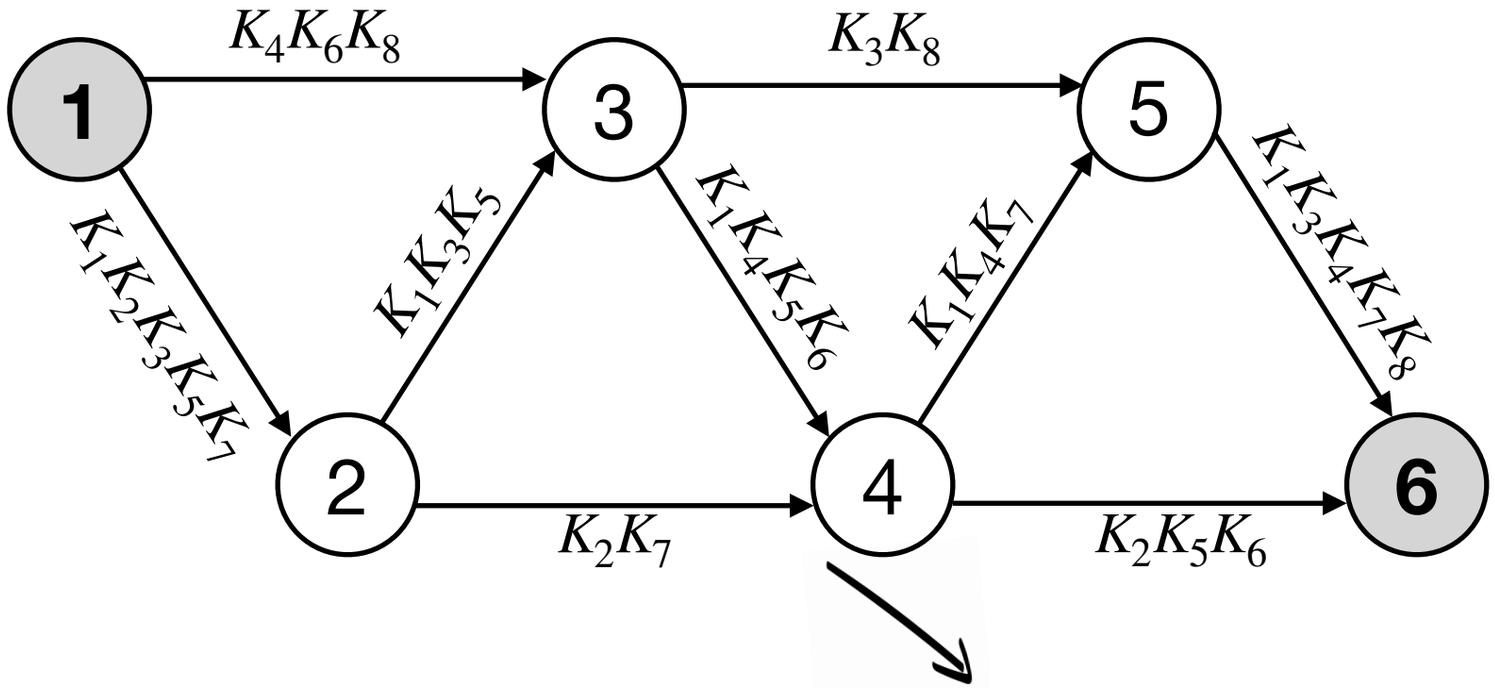
$(K_1K_3K_4K_7K_8) \bigoplus k_{56}$



конференция РусКрипто

Ключевой транспорт

СМАРТС КВАНТТЕЛЕКОМ



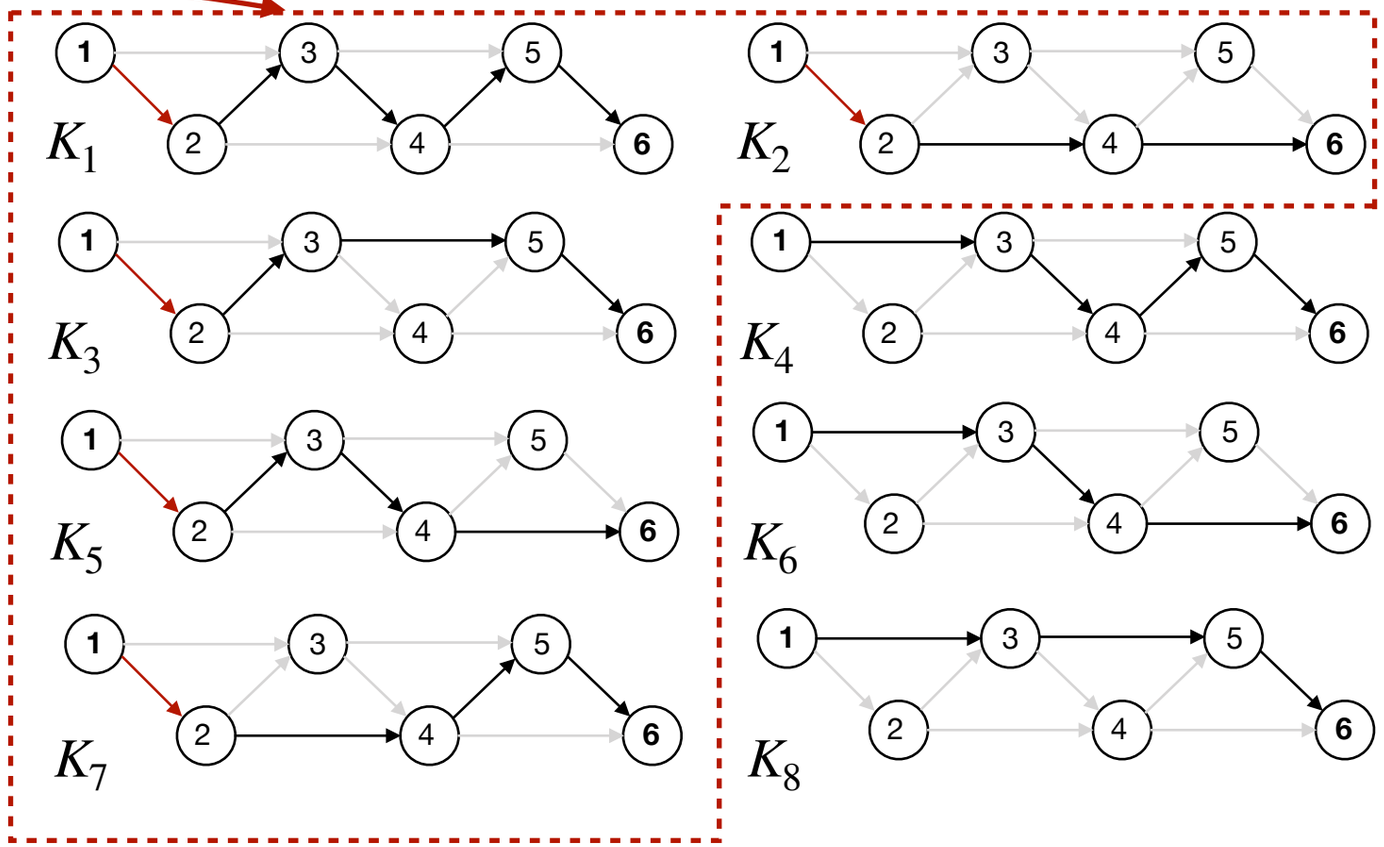
$(K_1K_2K_3K_5K_7) \oplus k_{12}$ $(K_4K_6K_8) \oplus k_{13}$

$(K_1K_3K_5) \oplus k_{23}$ $(K_2K_7) \oplus k_{24}$

$(K_1K_4K_5K_6) \oplus k_{34}$ $(K_3K_8) \oplus k_{35}$

$(K_1K_4K_7) \oplus k_{45}$ $(K_2K_5K_6) \oplus k_{46}$

$(K_1K_3K_4K_7K_8) \oplus k_{56}$

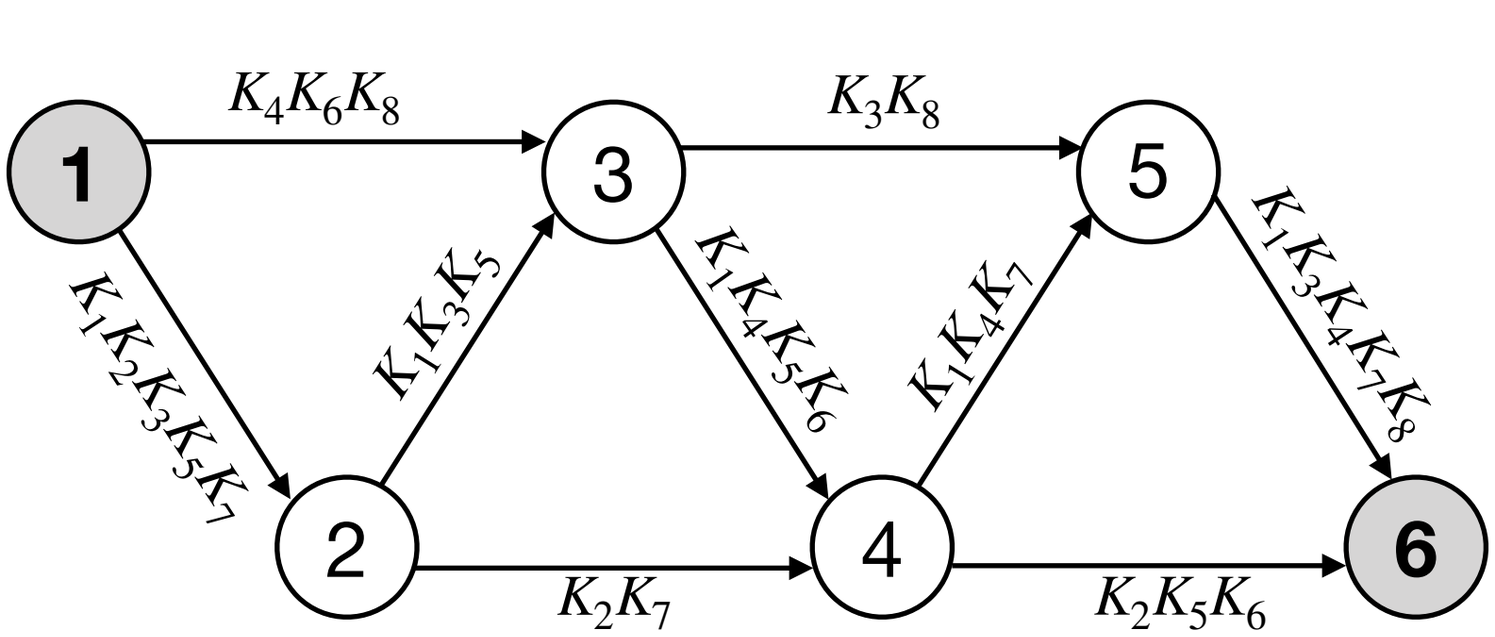


Ключевой транспорт

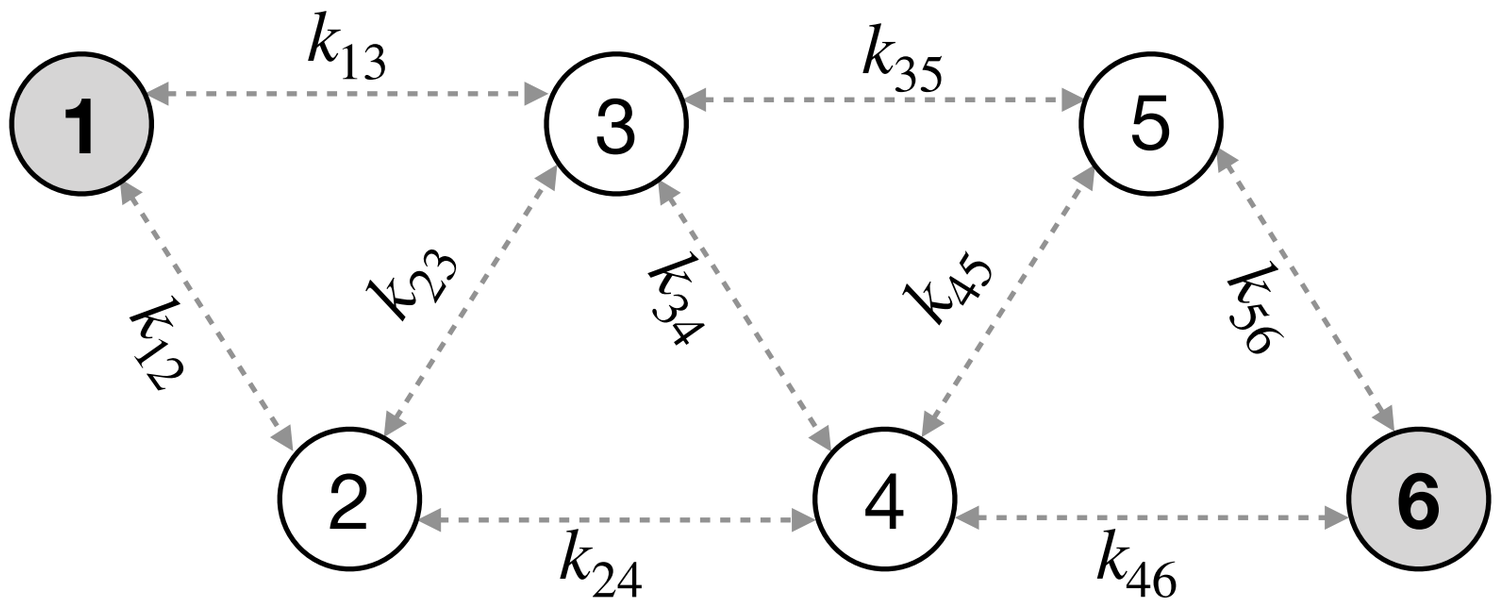
$$\sum_i K_i \bigoplus k_{jk}$$

Gaidash A., Miroshnichenko G., Kozubov A. Quantum network security dependent on connection density between trusted nodes // arXiv preprint arXiv:2202.09162. – 2022.

Ключевой транспорт

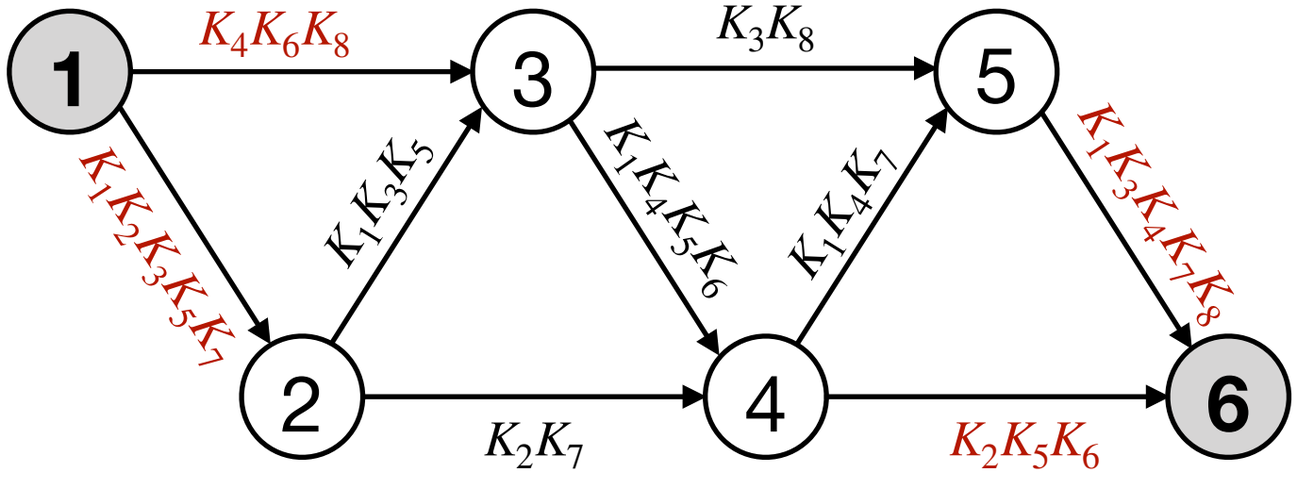


$$\sum_i K_i \oplus k_{jk}$$



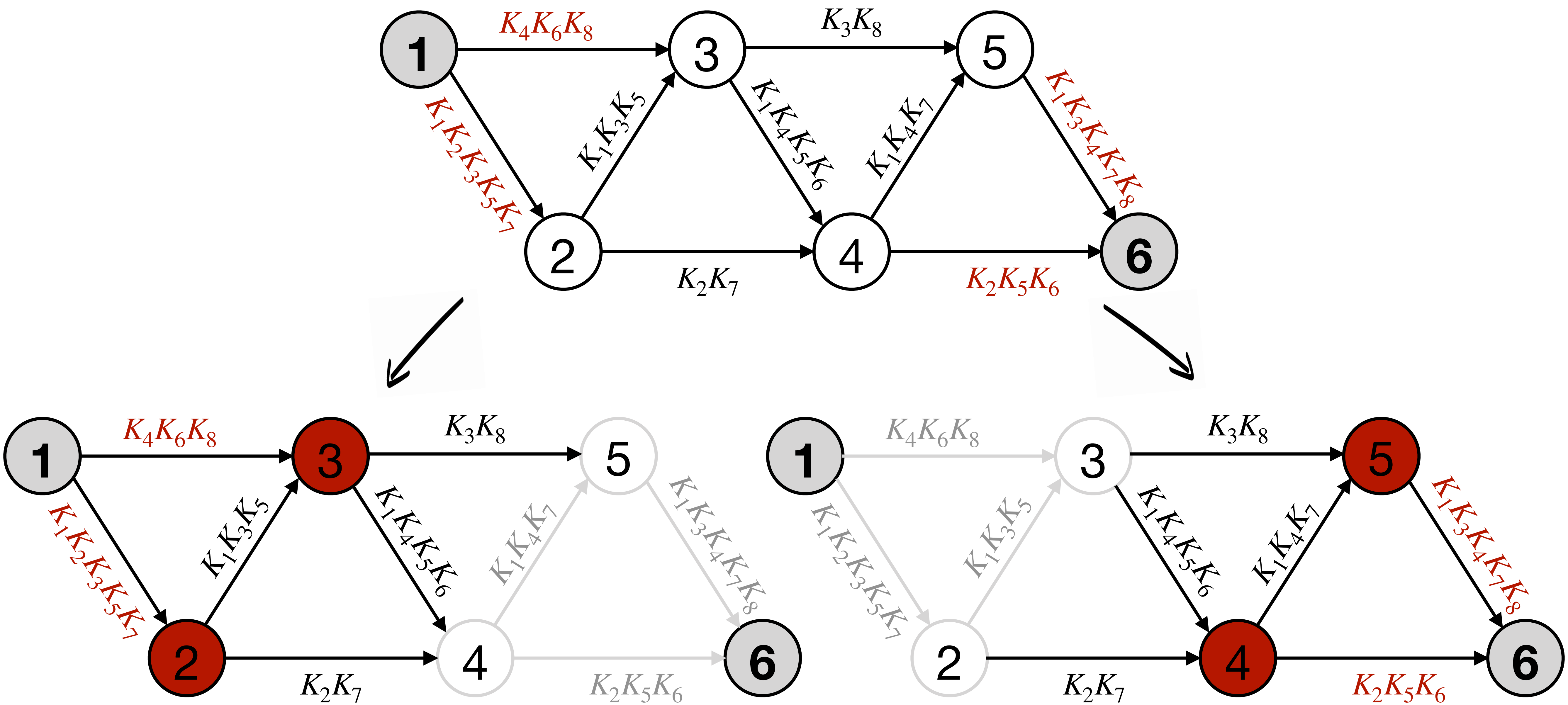
Gaidash A., Miroshnichenko G., Kozubov A. Quantum network security dependent on connection density between trusted nodes // arXiv preprint arXiv:2202.09162. – 2022.

Атака на аутентификацию



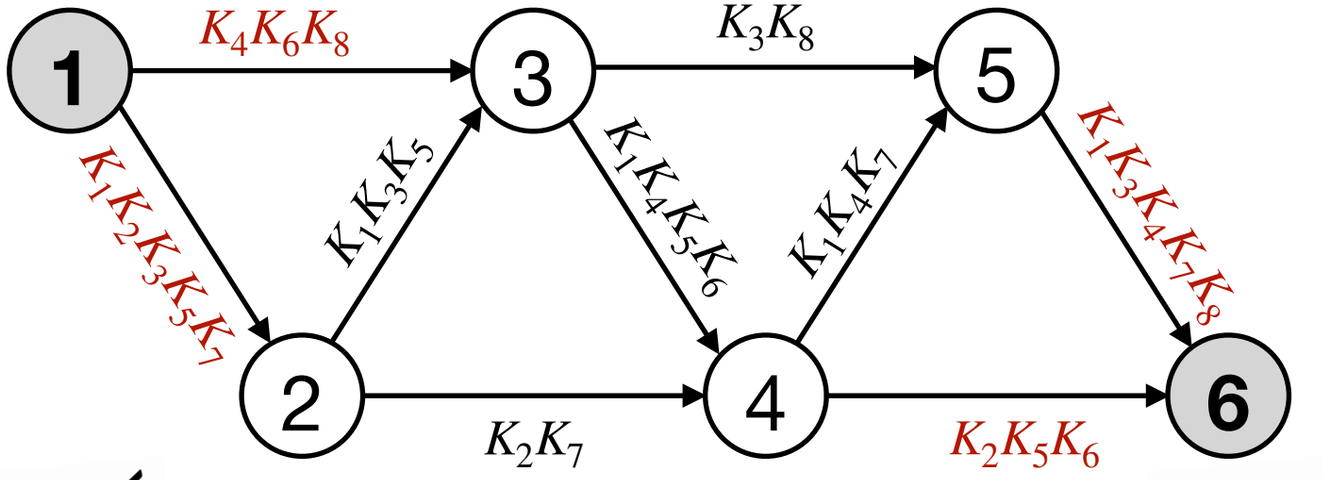
N —число узлов в сети, c —число связей, выходящих из узла

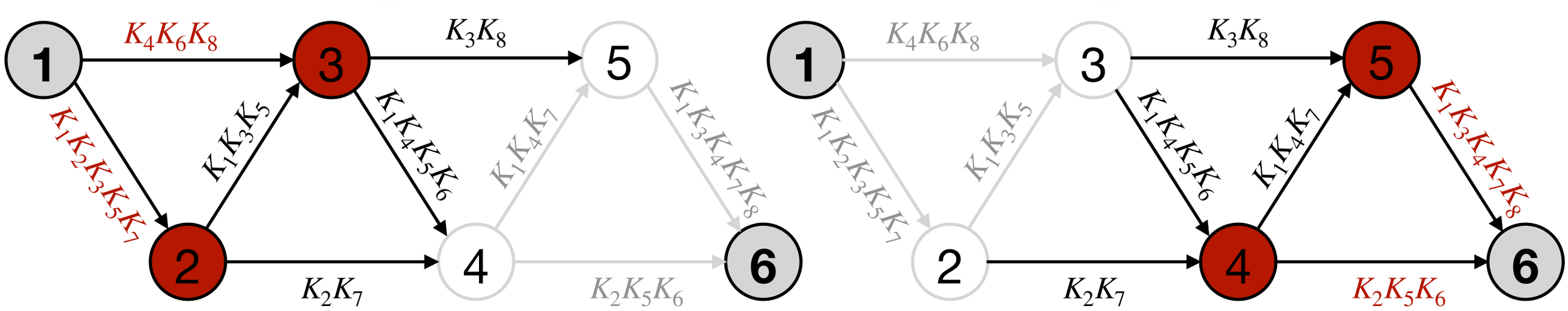
Атака на аутентификацию



N —число узлов в сети, c —число связей, выходящих из узла

Атака на аутентификацию

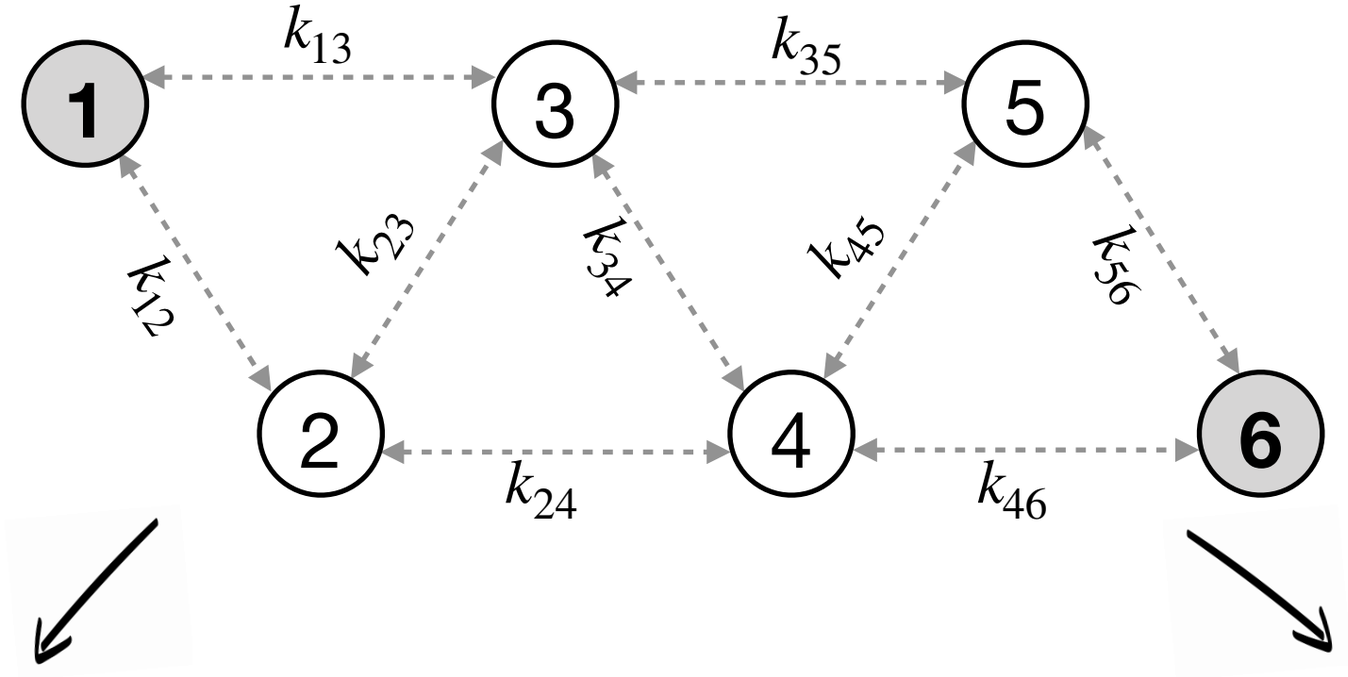


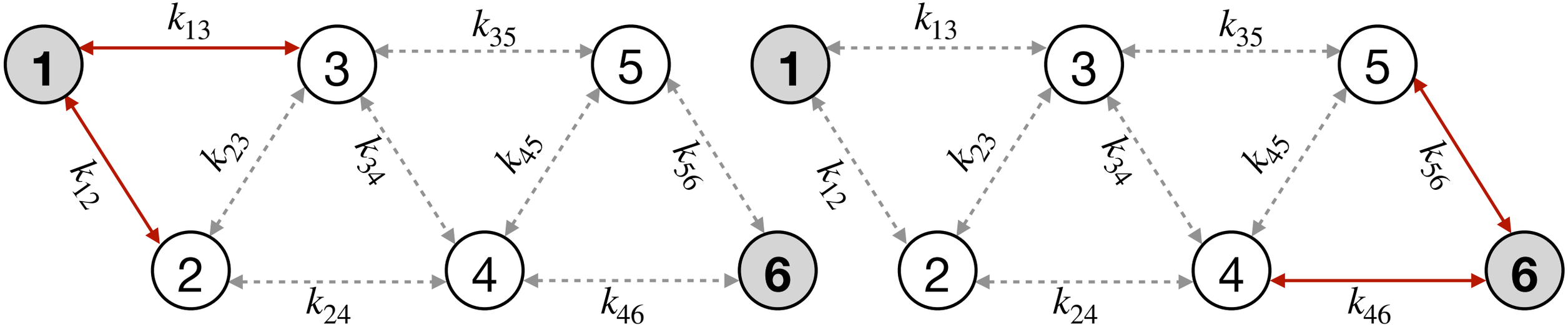


$$\varepsilon_1 \approx (N - c - 1)(\varepsilon_{auth})^c$$

N —число узлов в сети, c —число связей, выходящих из узла

Атака на аутентификацию





$$\varepsilon_2 \approx 2(\varepsilon_{qkd})^c$$

Масштабирование атак на КРК

КРК «точка-точка»

$$\varepsilon_{auth}$$

$$\varepsilon_{qkd}$$

$$\varepsilon \approx \varepsilon_{qkd} + \varepsilon_{auth}$$

Сеть КРК с ключевым транспортом

$$\varepsilon_1 \approx (N - c - 1)(\varepsilon_{auth})^c$$

$$\varepsilon_2 \approx 2(\varepsilon_{qkd})^c$$

$$\varepsilon_{qn} = \varepsilon_1 + \varepsilon_2 \approx$$

$$\approx (N - c - 1)(\varepsilon_{auth})^c + 2(\varepsilon_{qkd})^c$$

Gaidash A., Miroshnichenko G., Kozubov A. Quantum network security dependent on connection density between trusted nodes // arXiv preprint arXiv:2202.09162. – 2022.

Сравнение апроксимации и точного решения

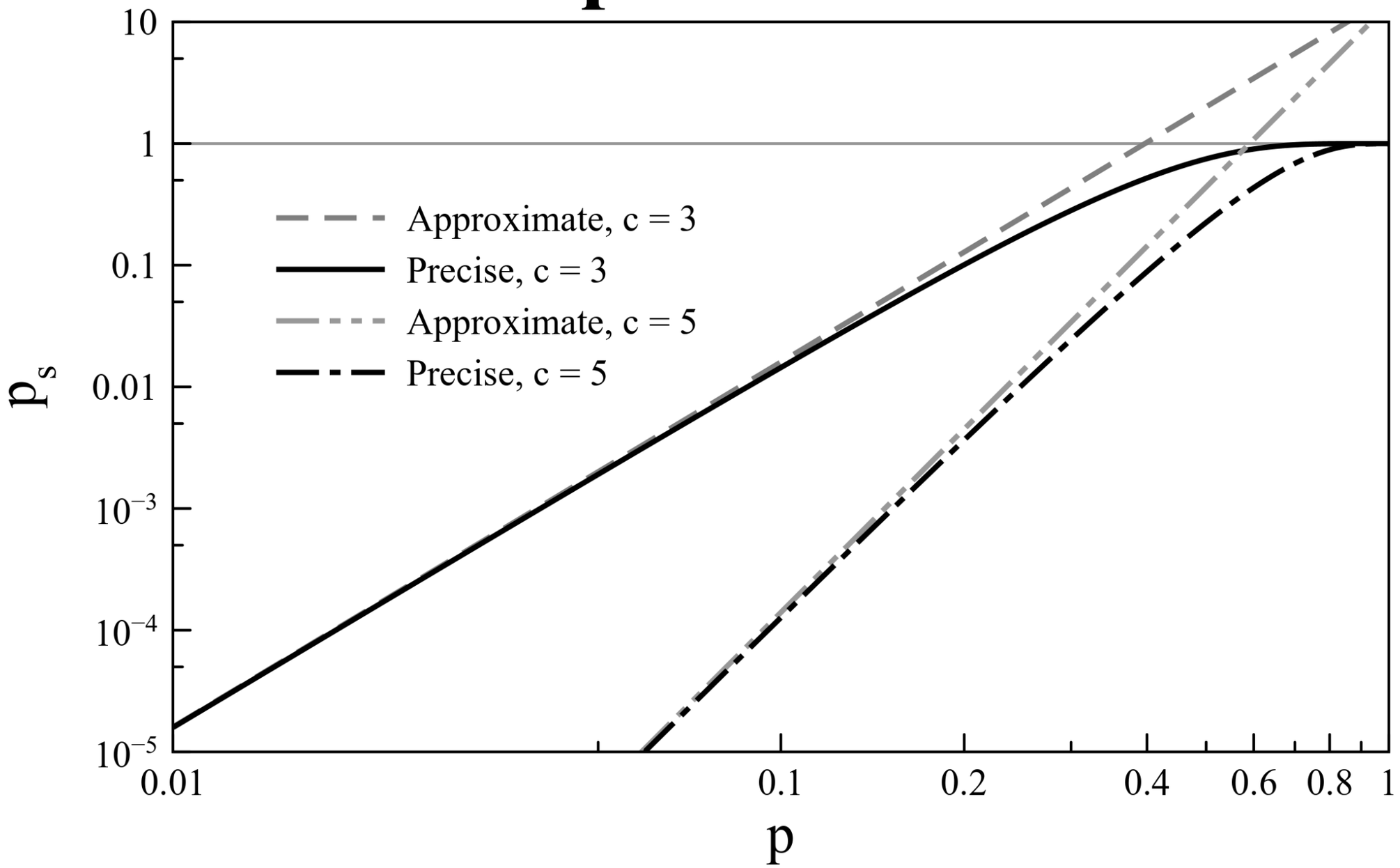
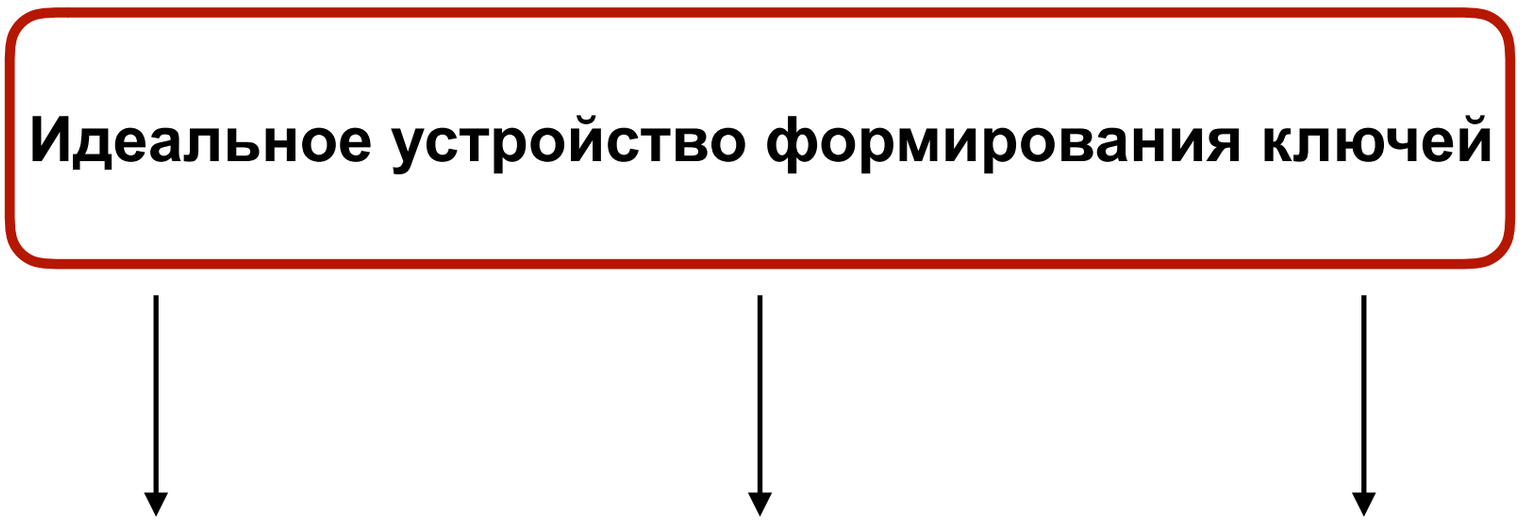


Рис. Зависимости вероятностей p_S успешной атаки на сегмент квантвой сети от средней вероятности p взять узел под контроль. Рассмотрены два случая: $c = 3$ и $c = 5$; $N = 20$ в качестве примера .

Спасибо за внимание!

avkozubov@itmo.ru

Идеальное устройство формирования ключей



$K_{\mathcal{A}}$ E $K_{\mathcal{B}}$

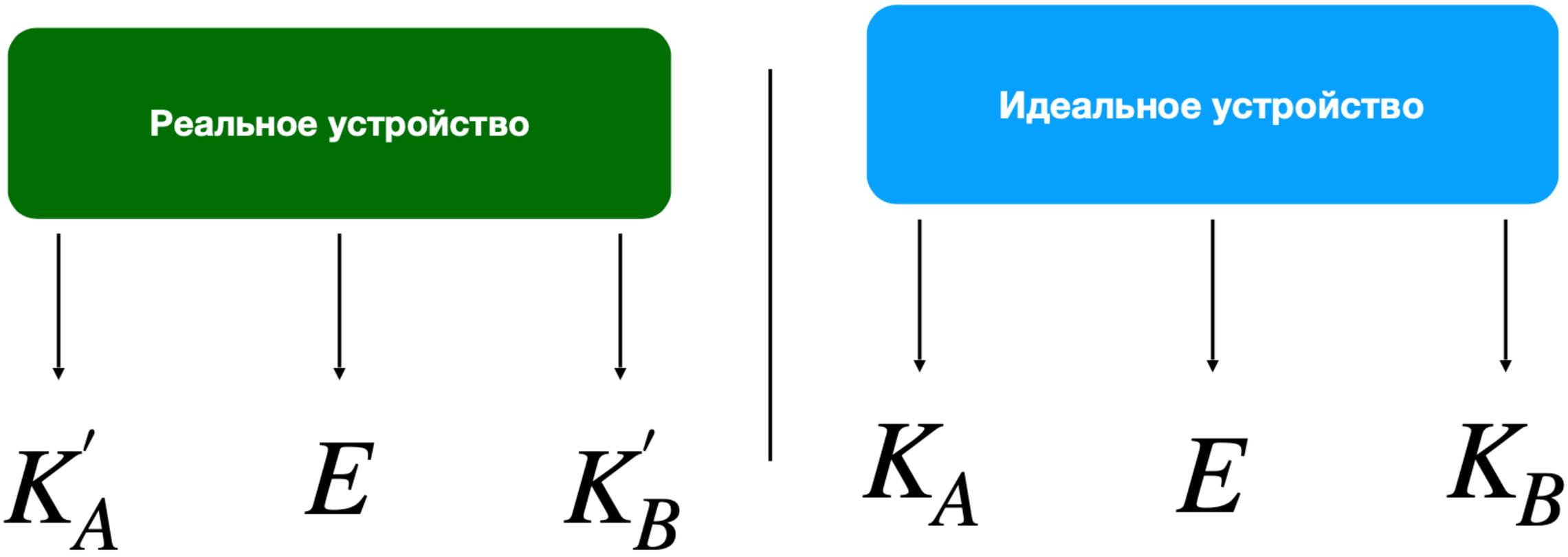
Условия к устройству:

- Корректность — $K_A = K_B = K$, K — идеальный ключ
- Секретность - K равномерно распределен и некоррелирован с E

$$H(\mathbf{K}\,|\,\mathbf{E}) = 1$$

Renato Renner, Tutorial: Finite size effect in QKD, QCrypt 2018

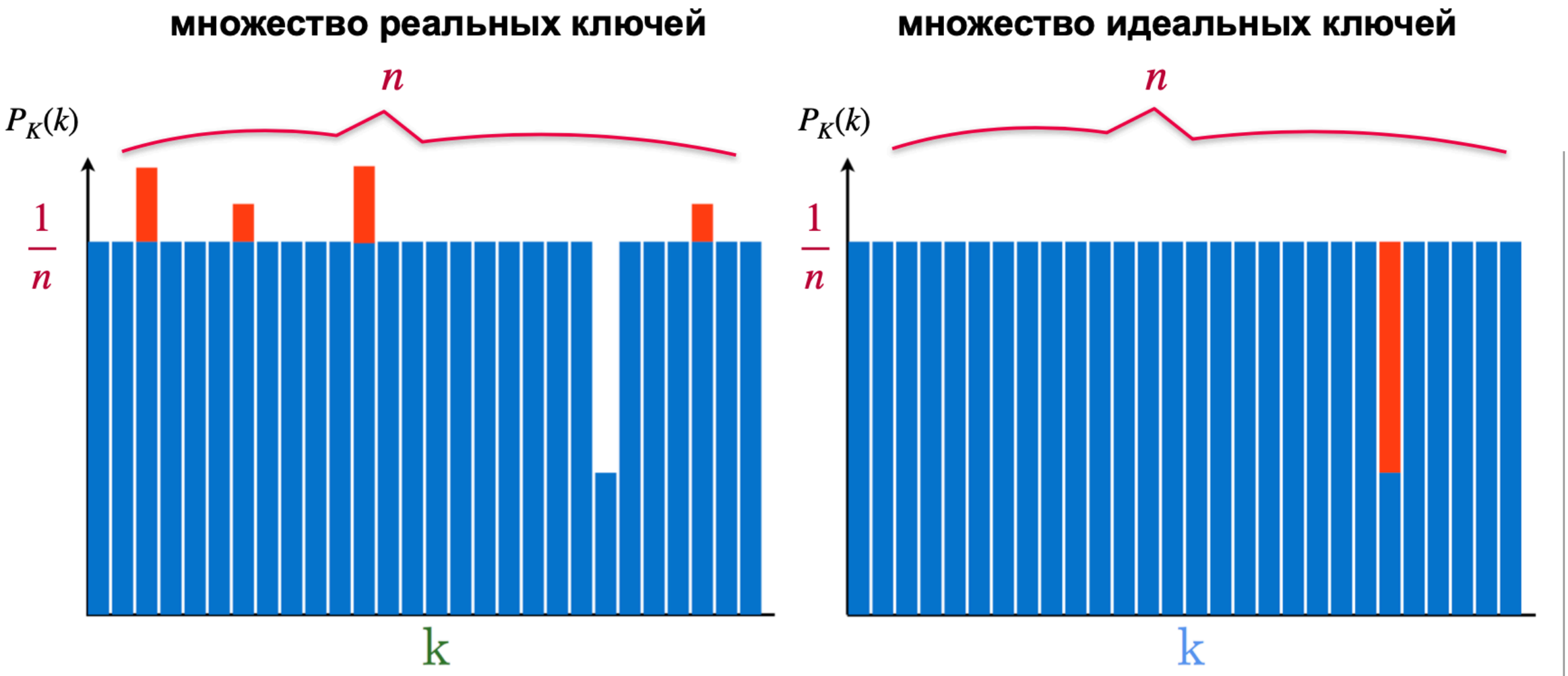
Отличие реального устройства от идеального



$$d = \|\rho_{K'E} - \omega_K \otimes \sigma_E\|_1 \leq \varepsilon$$

Renato Renner, Tutorial: Finite size effect in QKD, QCrypt 2018

Отличие множества реальных ключей от идеальных



ε соответсвует удельному весу красных областей

Необходимо показать, что К = К за исключением красных областей, где К, К - множества реальных и идеальных ключей соответственно. Это может быть сделано с помощью оценок, построенных на энтропиях Реньи