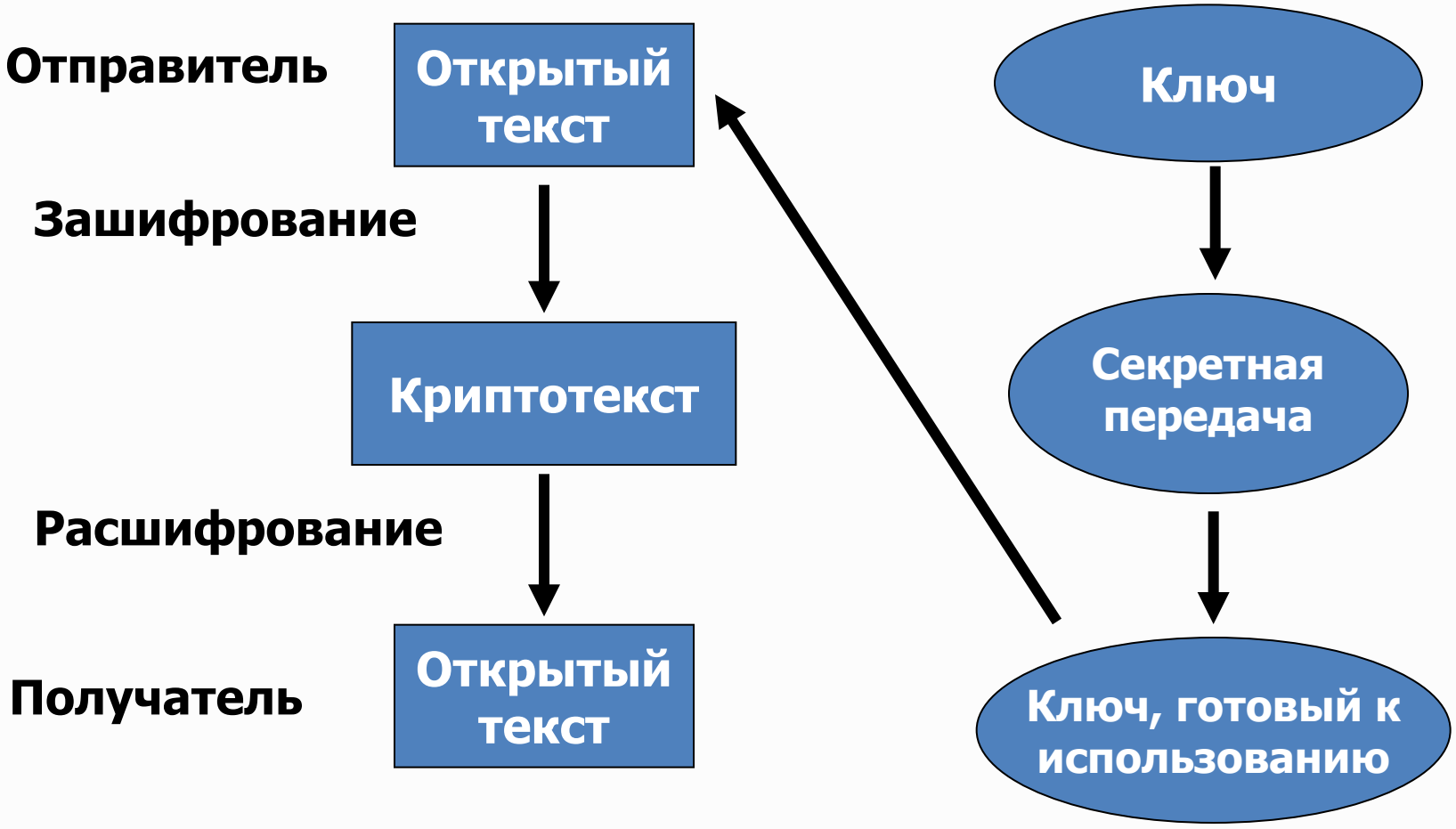
Василиу Е.В., д.т.н., проф.

Одесская национальная академия связи им. А.С. Попова

Современные технологии квантовой защиты информации

Проблемы и перспективы использования

Проблема распределения ключей



Шифрование сообщений

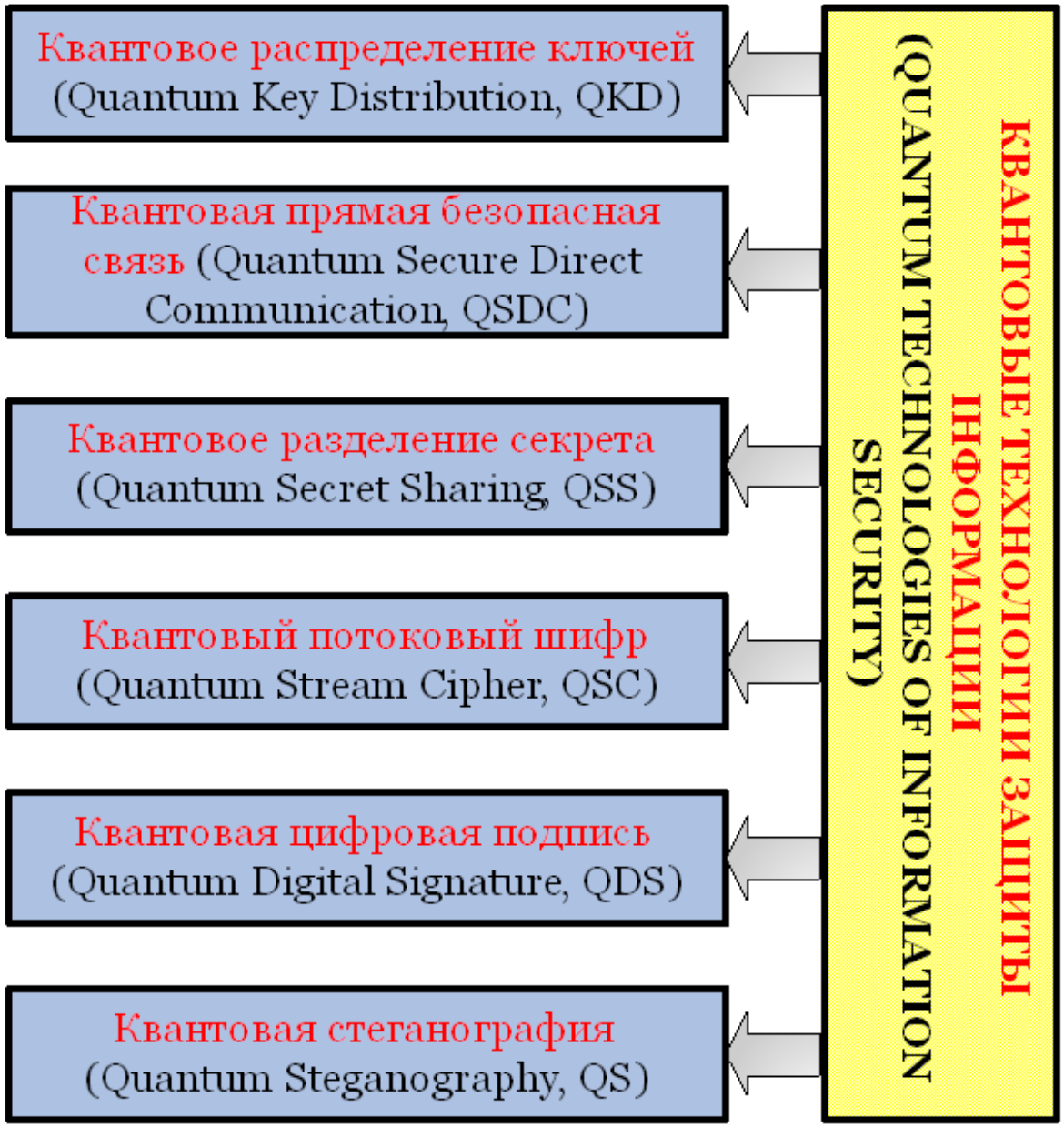
Безопасное распределение ключей

Квантовая криптография

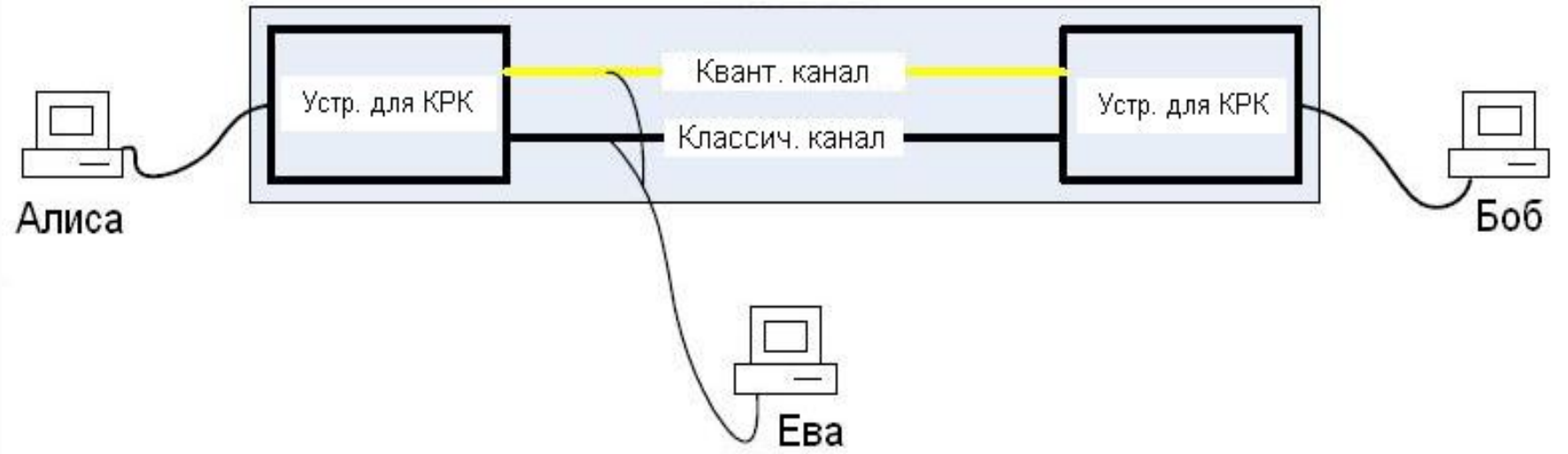
Квантовая криптография – решение задач криптографической защиты информации с использованием квантовых свойств отдельных фотонов (носителей информации в квантовой криптографии)

Фундаментальные свойства квантовых систем:

- Измерения физических характеристик квантовой системы изменяют состояние самой системы.
- Невозможность точного клонирования квантовых состояний.
- Неортогональные квантовые состояния невозможно достоверно отличить.
- Перепутывания (квантовые корреляции) – это исключительно квантовый эффект, который заключается в том, что две и более квантовых систем могут находиться в состоянии взаимной корреляции и влиять друг на друга.


КВАНТОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ
(QUANTUM TECHNOLOGIES OF INFORMATION SECURITY)
Квантовое распределение ключей (Quantum Key Distribution, QKD)
Квантовая прямая безопасная связь (Quantum Secure Direct Communication, QSDC)
Квантовое разделение секрета (Quantum Secret Sharing, QSS)
Квантовый потоковый шифр (Quantum Stream Cipher, QSC)
Квантовая цифровая подпись (Quantum Digital Signature, QDS)
Квантовая стеганография (Quantum Steganography, QS)

Структура канала связи для квантового распределения ключей



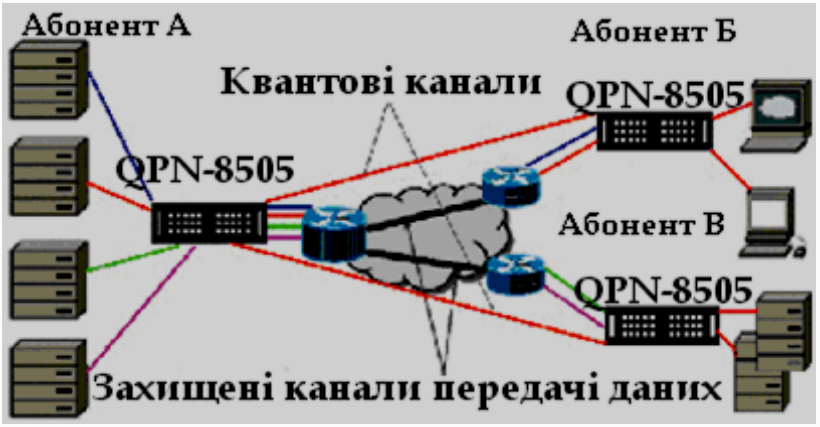
Система квантового распределения ключей

QPN Security Gateway (QPN-8505)

(MagiQ Technologies, США)

MagiQ

*Система **QPN-8505***



*Вариант организации сети на базе **QPN-8505***

- Криптографическое решение, ориентированное на правительственные и финансовые организации;
- Защита VPN с помощью квантового распределения ключей (до ста 256-битных ключей в секунду на расстояние до 140 км) и интегрированного шифрования;
- Используются такие протоколы: квантовый BB84, классические 3DES (112 бит) и AES (256 бит);
- Стоимость минимальной конфигурации € 80 тыс.

Системы квантового распределения ключей

Clavis² та **Cerberis** (ID Quantique, Швейцария)

*Криптосистема **Clavis²***

*Криптосистема **Cerberis***

- Автокомпенсирующая оптическая платформа обеспечивает стабильность и низкий уровень квантовых ошибок;
- Защищенное распределение ключей шифрования между двумя абонентами на расстояние до 100 км;
- Рыночная стоимость системы около € 90 тыс.

- Сервер с автоматическим созданием и секретным обменом ключами по оптоволоконному каналу до 50 км;
- 12 параллельных криптовычислений;
- Шифрование протоколом AES (256 бит), а для КРК - протоколы BB84 и SARG;
- Ориентировочная стоимость такой системы на рынке € 70 тыс.

Основные виды протоколов квантового распределения ключей (QKD)

- **Протоколы с использованием одиночных квантовых систем** (protocols using single quantum systems): *BB84, SARG, протокол з 6-ю состояниями, протокол "4+2", протокол Гольденберга-Вайдмана, протокол Коаши-Имото и др.*
- **Протоколы с использованием фазового кодирования** (protocols using phase coding): *B92 и его различные варианты.*
- **Протоколы с использованием перепутанных состояний** (protocols using entangled states): *протокол Экерта и протоколы с использованием перепутанных состояний многомерных квантовых систем.*
- **Протоколы с состояниями «приманки»** (decoy states protocols).
- **Протоколы с непрерывными квантовыми состояниями** (continuous-variable quantum key distribution).

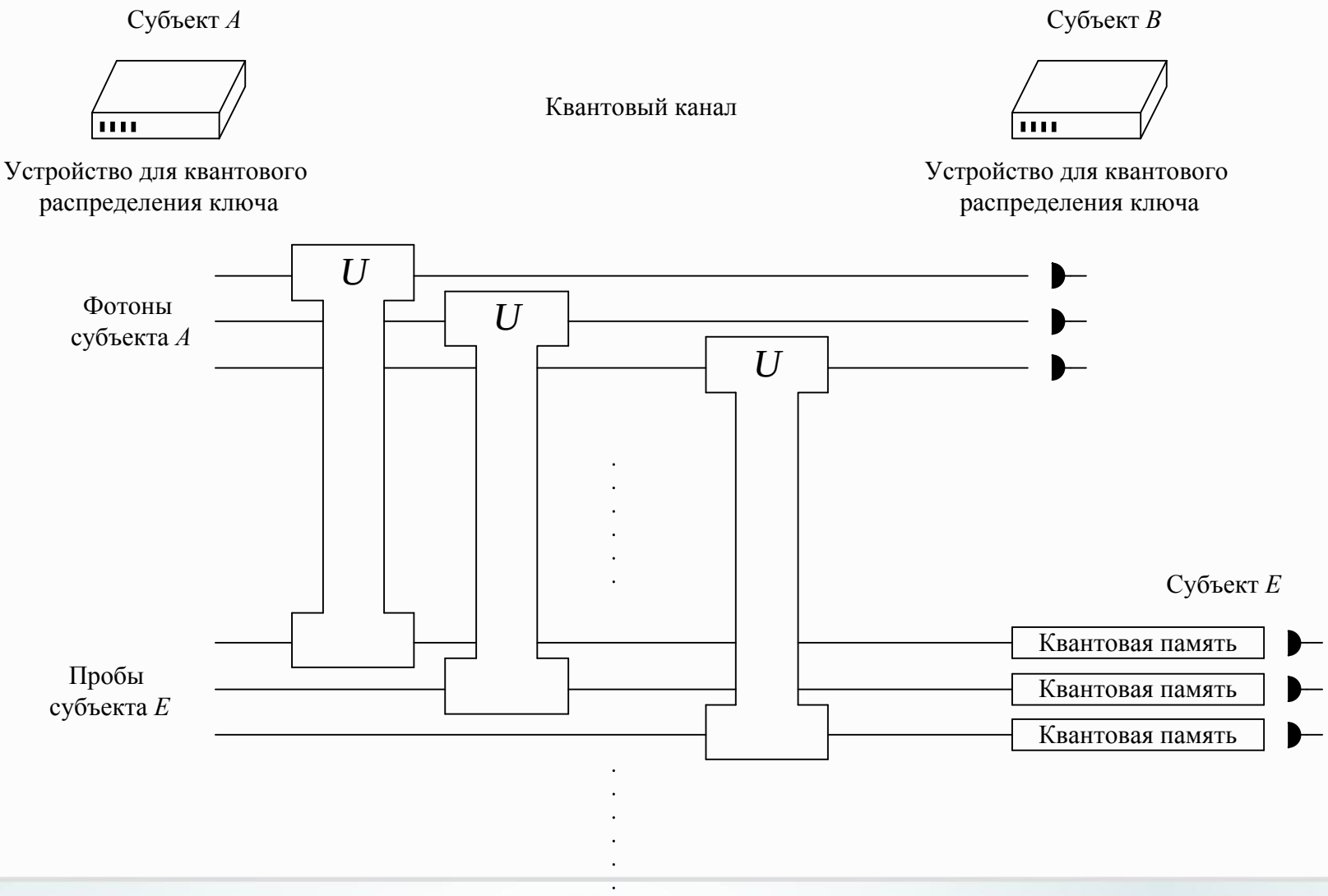
Стек протоколов КРК (stack of QKD)

- Законы квантовой механики позволяют не только обнаружить возмущение состояний, но и связать уровень ошибок при измерениях у легитимных пользователей с количеством информации, которую мог получить злоумышленник.

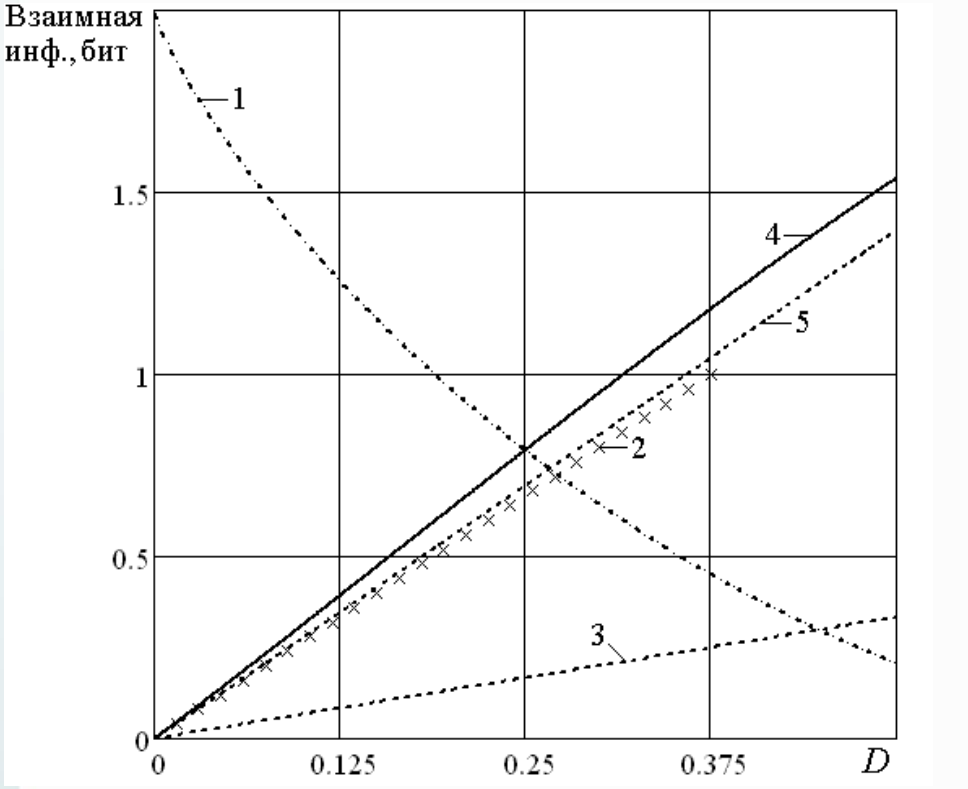
Стек протоколов КРК:

- протокол первичной квантовой передачи;
- протокол исправления ошибок в полученной битовой последовательности;
- протокол оценки количества информации, которая могла утечь к злоумышленнику;
- протокол усиления секретности и формирования итогового ключа.

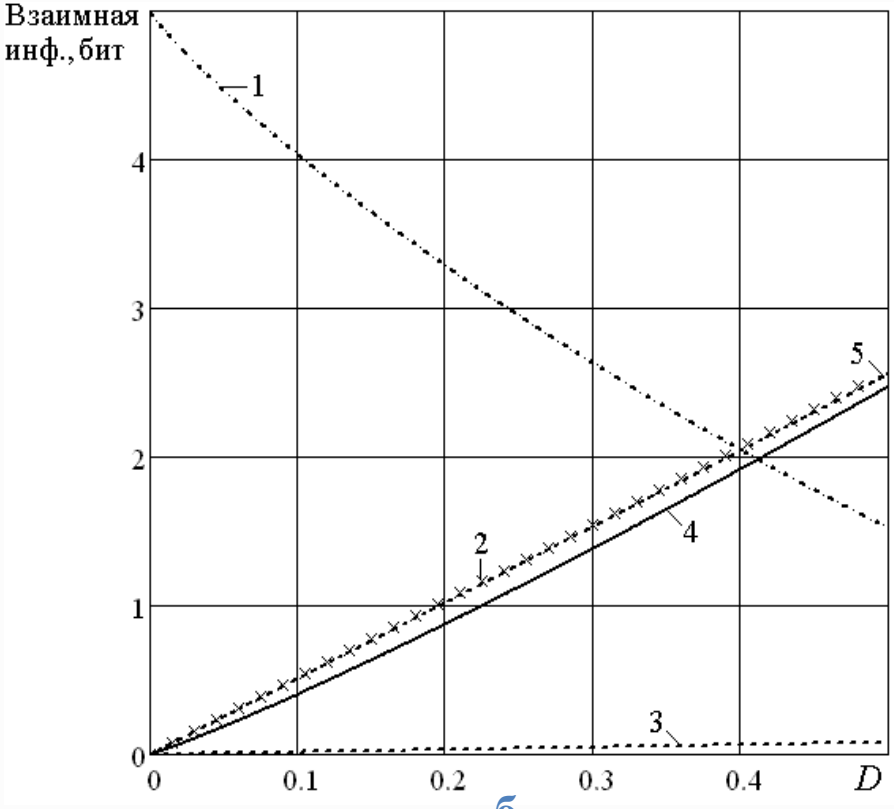
Некогерентная полупрозрачная атака на протокол с одиночными кудитами



Комплексный анализ стойкости к некогерентным атакам и информационной емкости квантовых протоколов распределения ключей с многомерными квантовыми системами (кудитами)



а



б

Взаимная информация для IR-атаки и некогерентной полупрозрачной атаки: а) $n = 4$; б) $n = 32$. 1 – $I_{AB}(D)$ (1); 2 – $I^{(2)}_{AE-IR}(D)$ (2); 3 – $I^{(n+1)}_{AE-IR}(D)$ (3); 4 – $I^{(2)}_{AE}(D)$ (6); 5 – $I^{(n+1)}_{AE}(D)$ (4).

Стойкость протоколов с кудитами по критерию Цизара – Кёрнера

$$I_{AB}(D_{\max}) = I_{AE}(D_{\max})$$

Значения $D_{\max}$ для некогерентных атак:

Протоколы с одиночными кудитами					Протоколы с парами перепутанных кудитов	
1	**2**	**3**	**4**	**5**	**6**	**7**
n	$D_{\max}$					
	n+1 базис, IR-атака	2 базиса, IR-атака	n+1 базис, полупрозрач. атака	2 базиса, полупрозрач. атака	атака несимметрич. клонирования	атака симметрич. клонирования
2	0,22709	0,17054	0,15637	0,14645	0,14645	0,14645
3	0,35885	0,23591	0,22671	0,21132	0,22472	0,23974
4	0,44764	0,27187	0,26656	0,25	0,26582	0,29428
5	0,51245	0,2951	0,2923	0,27639	0,29196	0,32984
7	0,60191	0,324	0,32388	0,31102	0,32377	0,37343
8	0,63436	0,33376	0,33436	0,32322	0,33429	0,38776
9	0,66147	0,34168	0,34278	0,33333	0,34273	0,39916
10	0,68452	0,34826	0,34971	0,34189	0,34968	0,40845
11	0,70437	0,35385	0,35554	0,34924	0,35539	0,41617
13	0,73692	0,36285	0,36484	0,36132	0,36451	0,42825
16	0,77346	0,37281	0,37498	0,375	0,37486	0,44099

Информационная емкость протоколов с кудитами, бит/кудит

n	2	3	4	5	7	8	9	11	13	16
Протоколы "приготовление – измерение", 2 базиса	0,5	0,792	1,0	1,161	1,404	1,5	1,585	1,73	1,85	2,0
Протоколы "приготовление – измерение", n+1 базис	0,333	0,396	0,4	0,387	0,351	0,333	0,317	0,288	0,264	0,235
Протоколы с перепутанными кудитами	0,125	0,198	0,25	0,29	0,351	0,375	0,396	0,432	0,463	0,5

Наилучшими одновременно по критериям информационной емкости и стойкости к некогерентным атакам (по теореме Цизара – Кёрнера) являются протоколы "приготовление – измерение" с использованием двух базисов.

Протоколы КРК

Преимущества:

1. Обнаружение атаки пассивного перехвата (eavesdropping) –
атака злоумышленника вносит значительно больше ошибок, чем их возникает в квантовом канале в результате естественного шума.

2. Теоретико-информационная стойкость распределения ключей (unconditional security of QKD) – ключи, *распределенные с помощью квантовых протоколов с теоретико-информационной стойкостью, используются для дальнейшего шифрования с использованием известных классических симметричных алгоритмов. Поэтому общий уровень стойкости криптосистемы повышается.*

3. Теоретико-информационная стойкость всей криптосистемы (general unconditional security)
КРК + шифр Вернама + аутентификация с теоретико-информационной стойкостью = *абсолютно стойкая гибридная система защиты информации!*

Недостатки:

1. КРК не является полноценным завершенным решением ЗИ – *необходима предварительная аутентификация пользователей; пользователи, не имеющие никакого общего предустановленного начального секрета, не могут обменятся новым ключом для шифрования:* КРК – технология увеличения длины ключа.

2. Ограничения длины квантового канала – *квантовые повторители еще не разработаны.*

3. С увеличением длины квантового канала значительно уменьшается скорость передачи – *если длина канала >100 км, то скорость передачи составляет биты в секунду, хотя на расстояниях в 20–30 км уже достигают мегабитных скоростей.*

4. Проблемы регистрации фотонов – *эффект темнового шума (темновых отсчетов).*

5. Деполяризация фотонов в квантовом канале *приводит к достаточно высокому уровню естественных помех - проценты и десятки процентов.*

6. Сложность реализации протоколов КРК с многомерными квантовыми системами.

7. Высокая рыночная цена готовых систем.

Возможные области применения КРК:

- Области, где требуется высокий уровень безопасности, например, там, где до настоящего времени ключи распределялись с помощью доверенных курьеров.
- Альтернатива схемам распределения сеансовых ключей в симметричных криптосистемах, которые основаны на методах криптографии с открытым ключом (например, альтернатива схеме Диффи – Хеллмана).

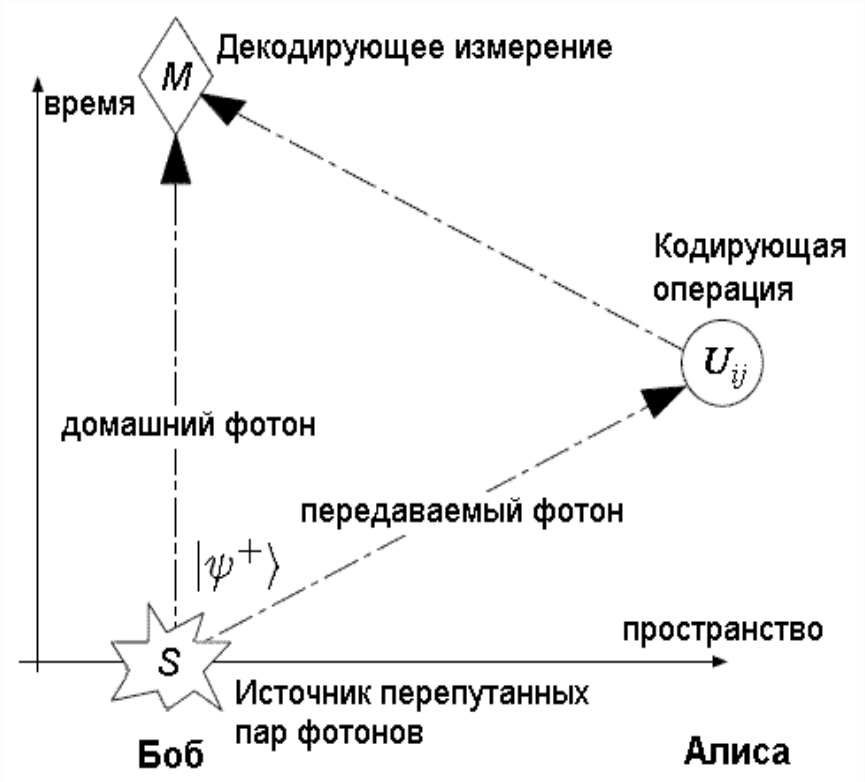
Квантовая прямая безопасная связь (КПБС, QSDC)

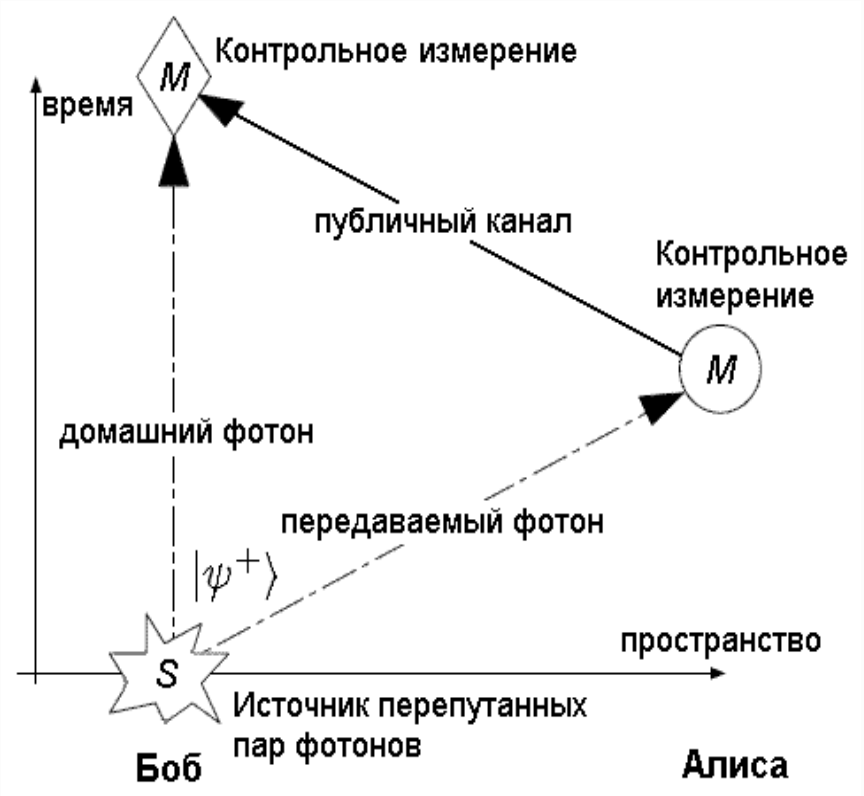
- **Пинг-понг протокол** (ping-pong protocol): *оригинальный протокол, предложенный в 2002 г., и его различные варианты с перепутанными состояниями кубитов и многоуровневых квантовых систем.*

- **Протоколы с использованием одиночных кубитов** (protocol using single qubits transfer).

- **Протоколы с передачей перепутанных квантовых систем блоками** (protocols using block transfer of entangled qubits).

Пинг-понг протокол квантовой прямой безопасной связи

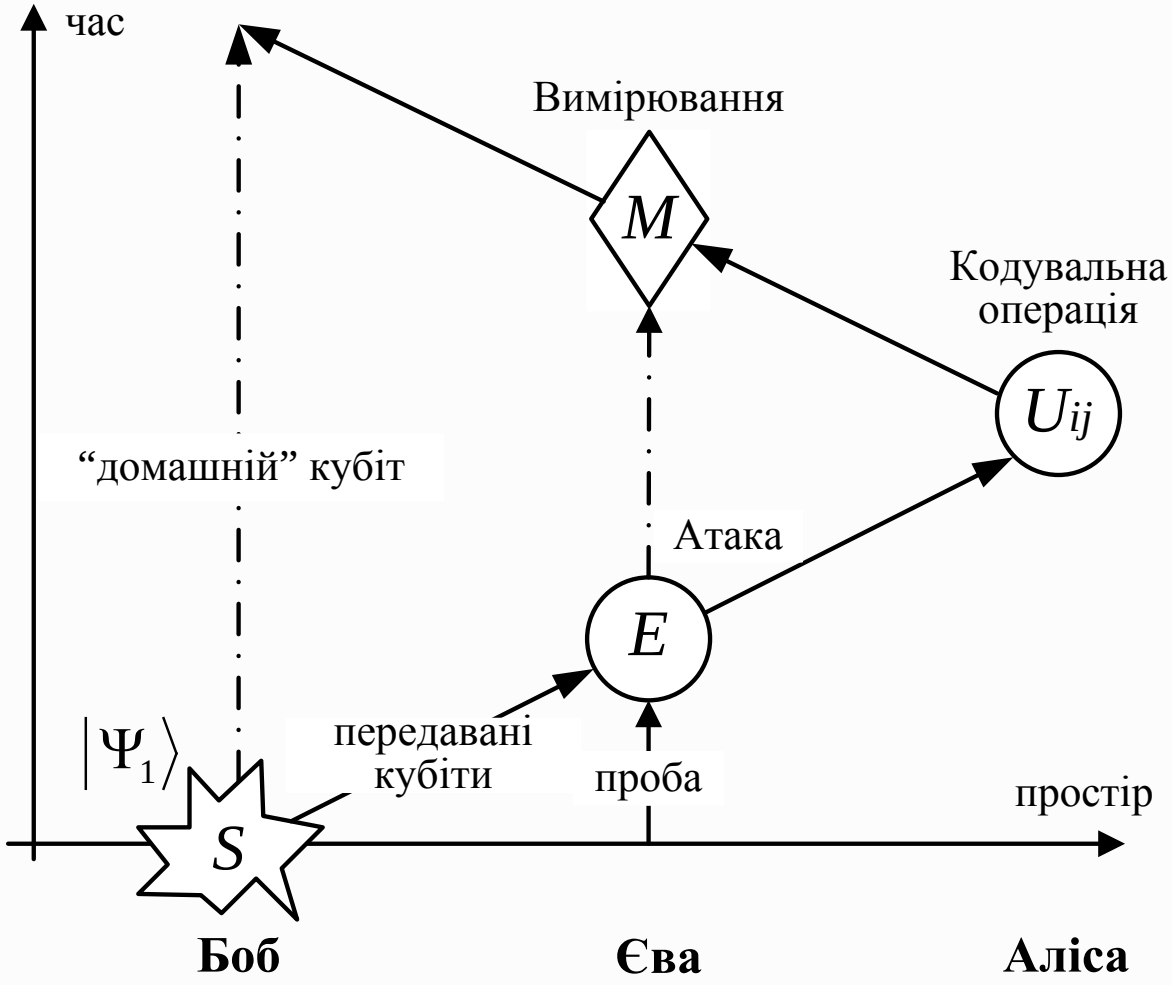


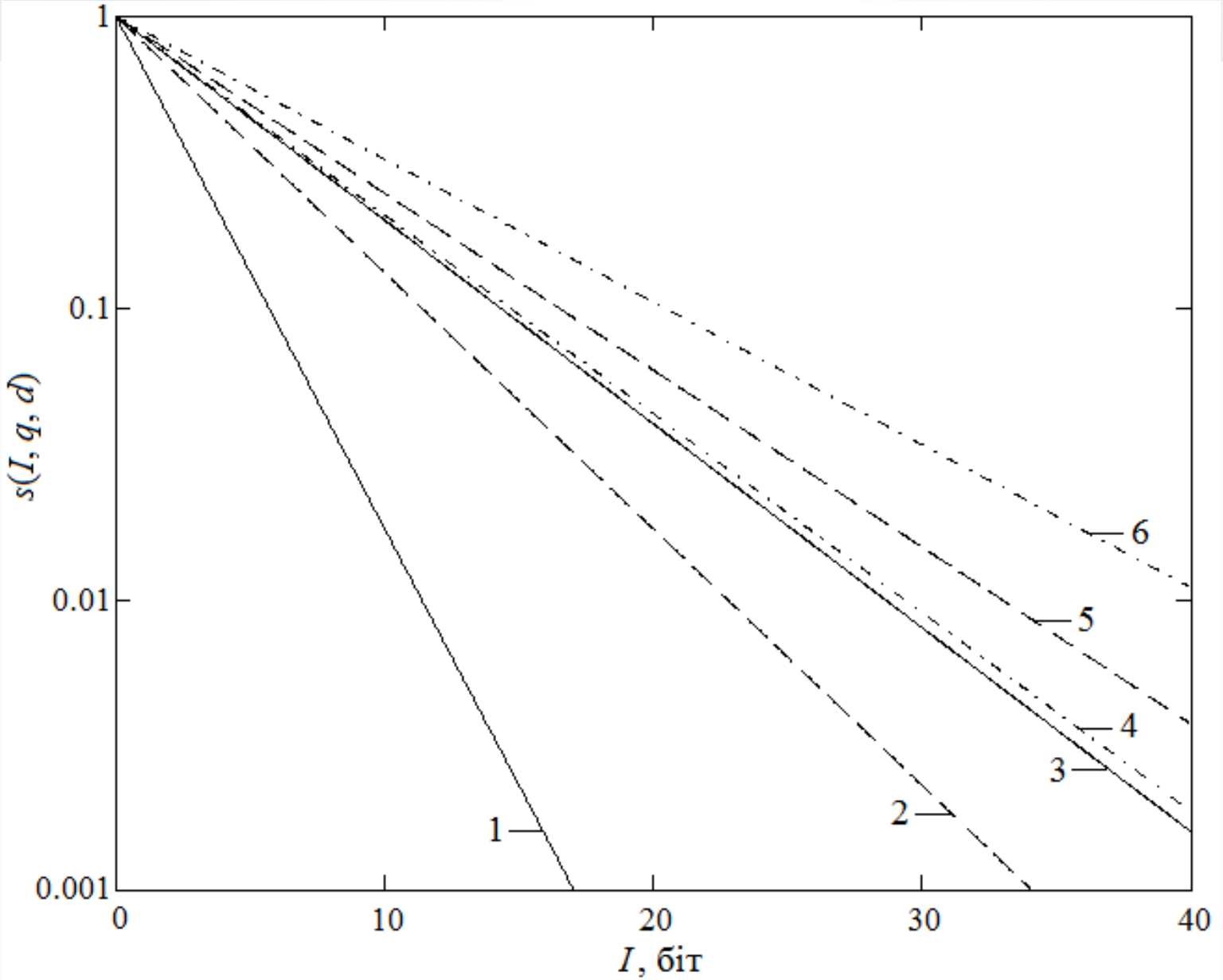


Режим передачи сообщений

Режим контроля прослушивания канала

Атака пассивного перехвата с использованием перепутывания





Полная вероятность необнаружения атаки для разных вариантов пинг-понг протокола

Метод усиления секретности

Обратимое хеширование:

$$b_i = M_i a_i$$

a_i – исходный битовый блок сообщения

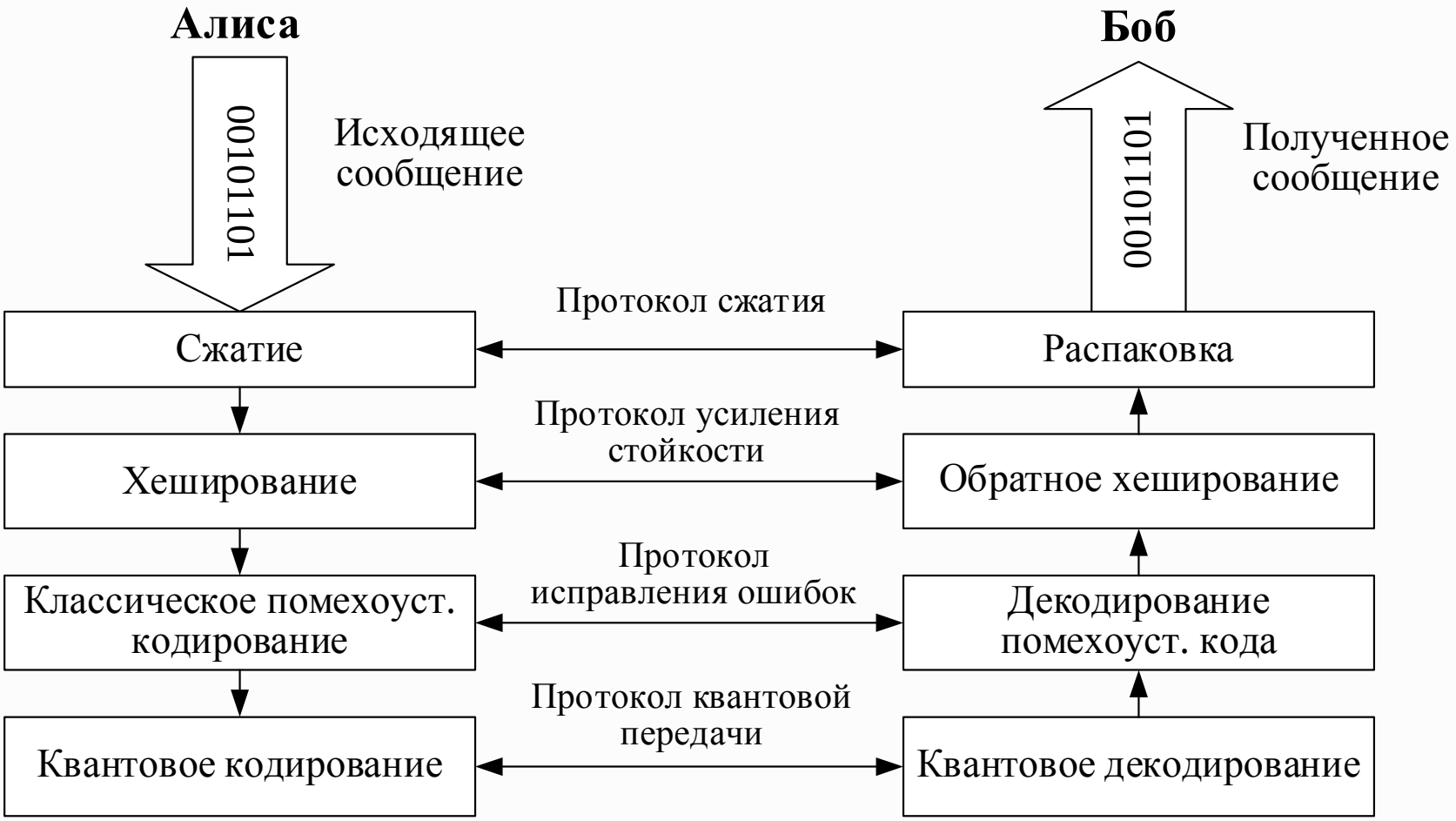
M_i – случайная обратимая двоичная матрица

b_i – хешированный блок, который передается с помощью пинг-понг протокола

Восстановление исходного сообщения:

$$a_i = M_i^{-1} b_i$$

Стек протоколов квантовой прямой безопасной связи



Протоколы КПБС

Преимущества:

1. Отсутствие необходимости распределять секретные ключи - *как следствие отсутствия каких-либо криптопреобразований.*

2. Возможность обмена информацией между более чем двумя пользователями и доверенным центром; конференц-связь.

3. Возможность обнаружения атак.

4. Обеспечение высокого уровня защищенности - *вплоть до теоретико-информационной стойкости для протоколов с передачей квантовых систем блоками.*

Недостатки:

1. Сложность практической реализации.

2. Низкая скорость передачи.

3. Необходимость в квантовой памяти большого объема для всех участников сеанса связи *(для протоколов с передачей квантовых систем блоками).*

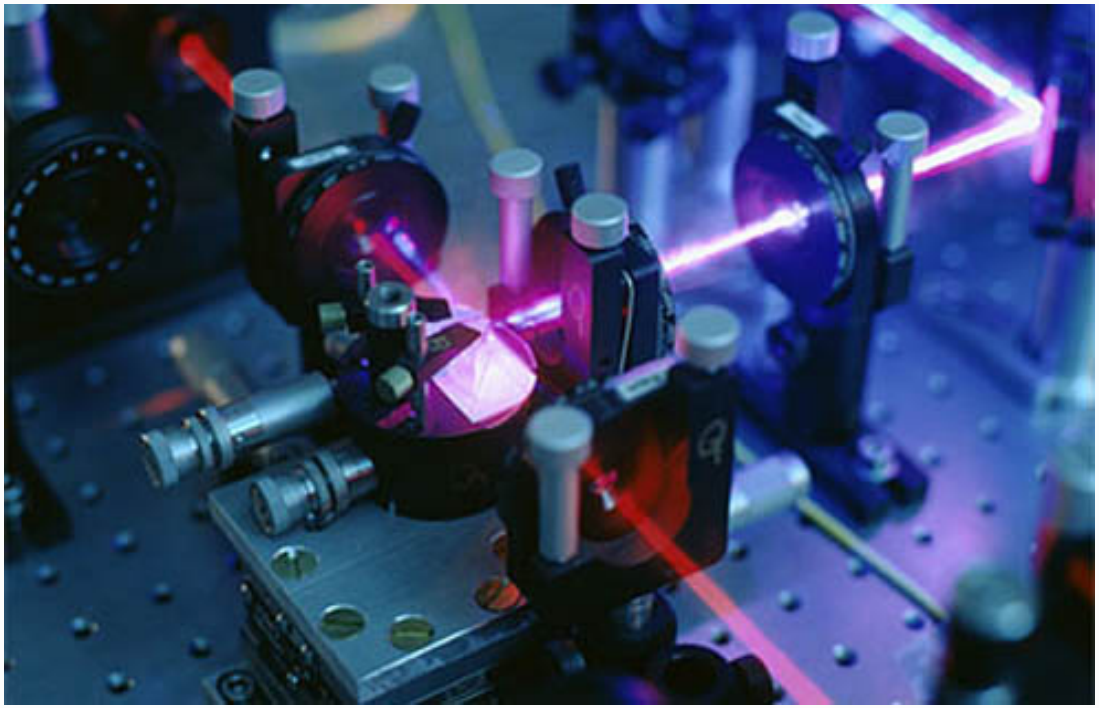
4. Асимптотическая стойкость пинг-понг протокола, *которая может быть усилена классическими методами.*

5. Уязвимость к атаке "человек посредине" *(аналогично системам КРК), которая нейтрализуется предварительной аутентификацией пользователей.*

Перспективы развития квантовых технологий защиты информации

- Разработка глобальной спутниковой криптографической сети.
- Расширение наземных сетей на трансатлантические расстояния.
- Выведение квантовой криптографии на уровень промышленного использования.

БЛАГОДАРЮ ЗА ВНИМАНИЕ!



www.onat.edu.ua

тел.: +380-48-705-04-93
e-mail: irte@onat.edu.ua