Региональный обучающий семинар Центров профессионального мастерства МСЭ в режиме видеоконференции "Технологические, организационные и регуляторные основы построения телекоммуникационных сетей современных и последующих поколений", Одесса, Украина, 4 сентября 2014 г.

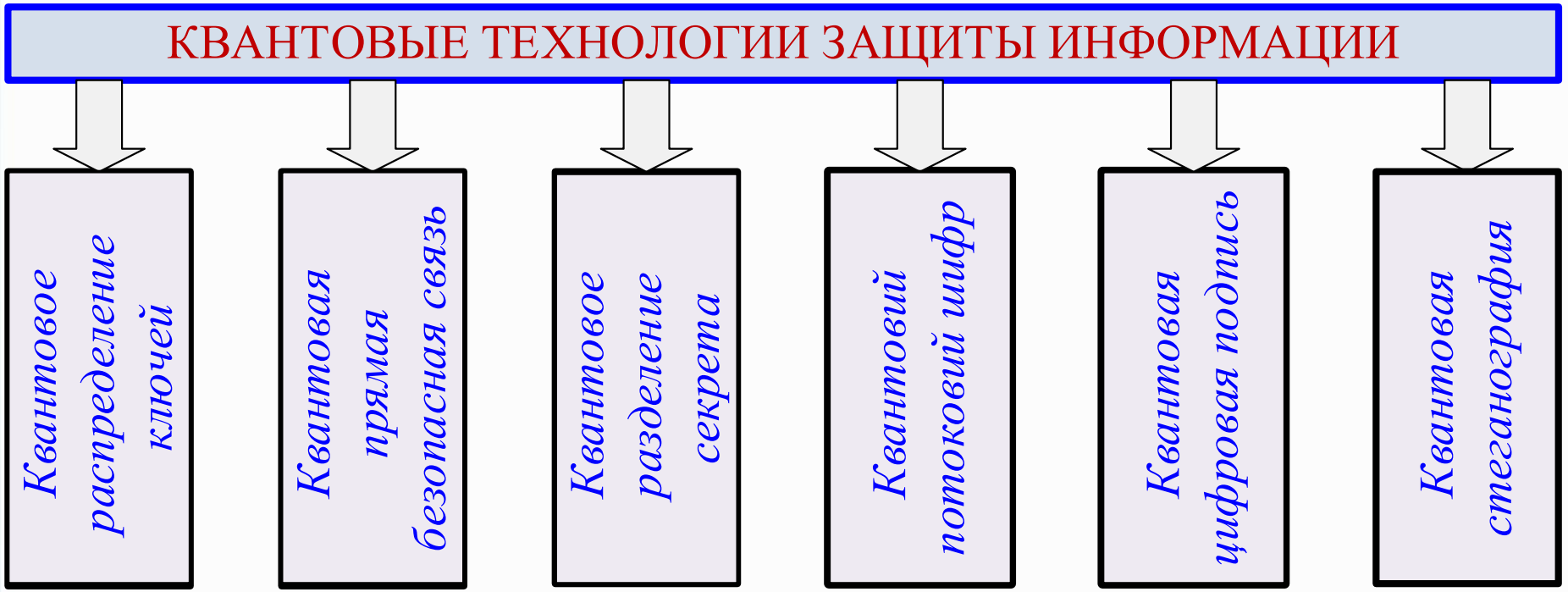
КВАНТОВЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Евгений Василиу

доктор технических наук, профессор, и.о. директора Учебно-научного института Радио, телевидения и информационной безопасности ОНАС им. А.С. Попова

Квантовая криптография

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



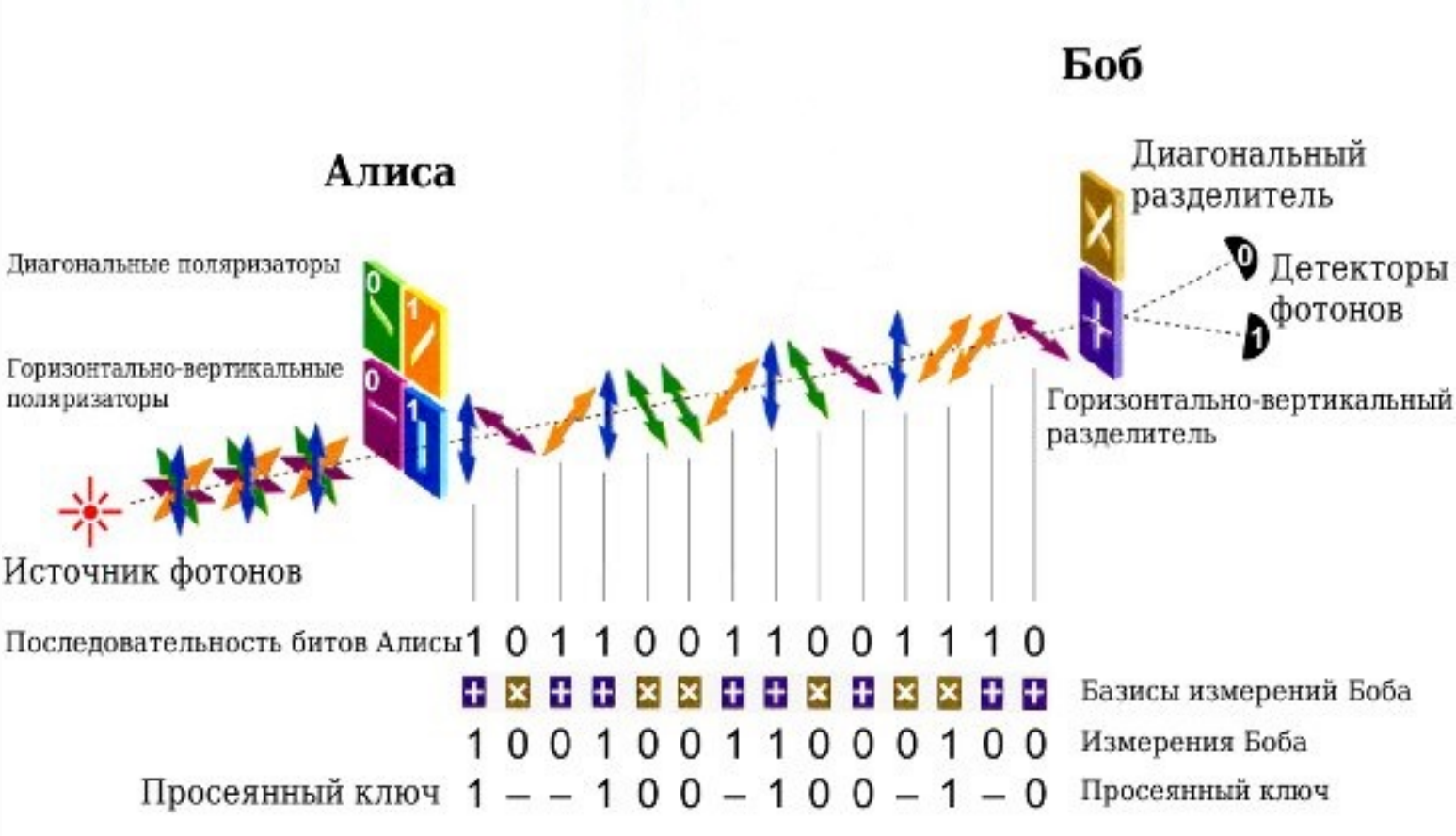
Современные методы распределения секретных ключей

1. • **Применение методов асимметричной криптографии (RSA, Диффи-Хеллмана, схема цифрового конверта, комбинированные методы и т.п.) –** базируется на гипотезе P ≠ NP

2. • **Использование доверенных курьеров –** высокая стоимость, зависимость от человеческого фактора

3. • **Квантовое распределение ключей –** теоретико-информационная стойкость, которая не зависит от вычислительных или других возможностей злоумышленника

Схема протокола Беннетта – Брассарда (протокол BB84)

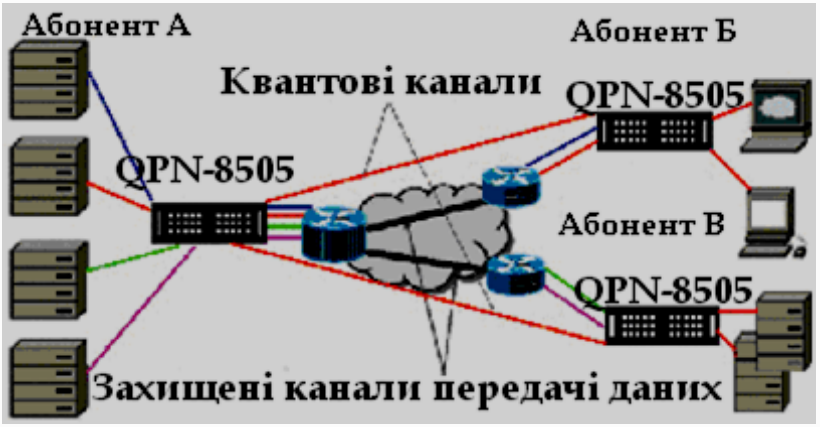


Система квантового распределения ключей

QPN Security Gateway (QPN-8505)

(MagiQ Technologies, США)

*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)

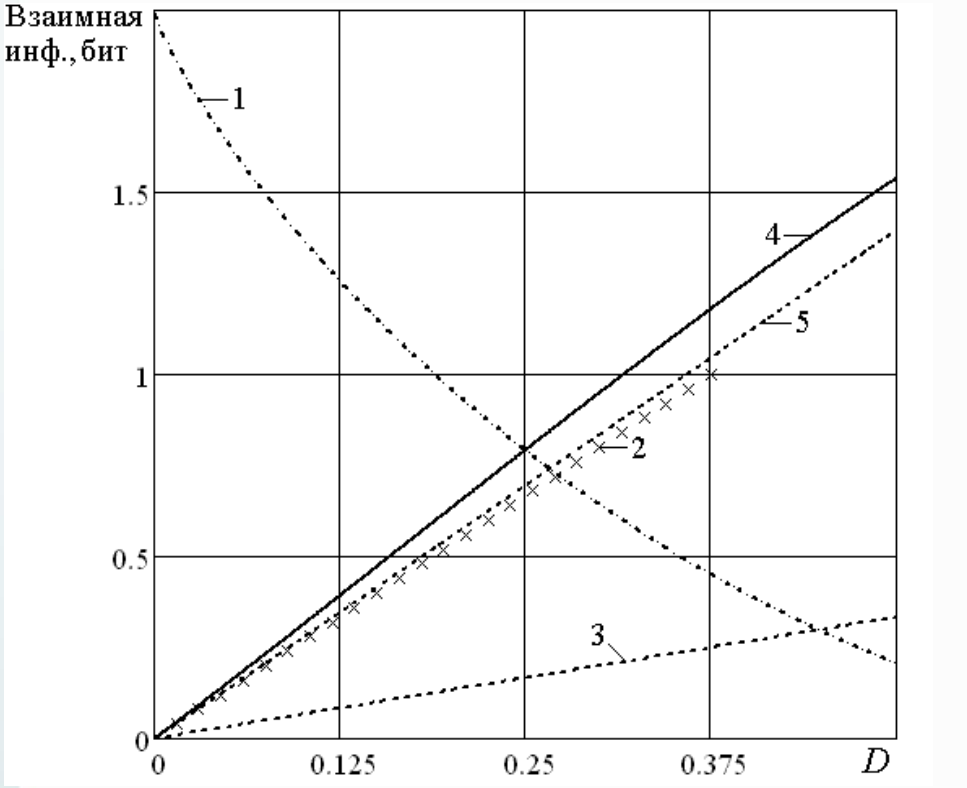
*Криптосистема **Clavis²***

*Криптосистема **Cerberis***

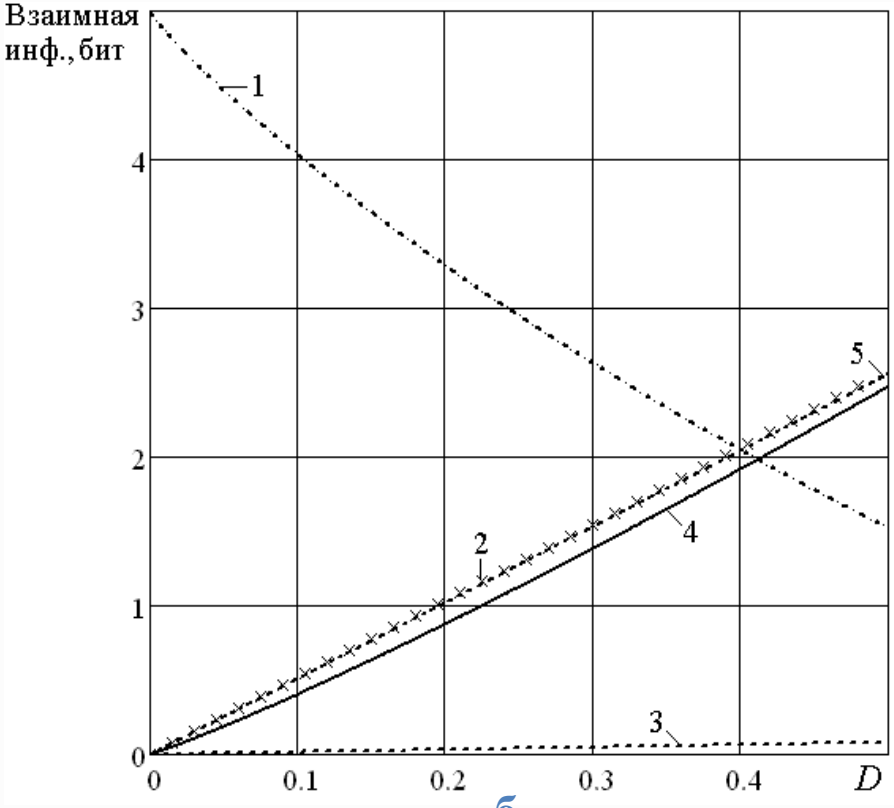
- Автокомпенсирующая оптическая платформа обеспечивает стабильность и низкий уровень квантовых ошибок;
- Защищенное распределение ключей шифрования между двумя абонентами на расстояние до 100 км;
- Рыночная стоимость системы около € 90 тыс.

- 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.

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:

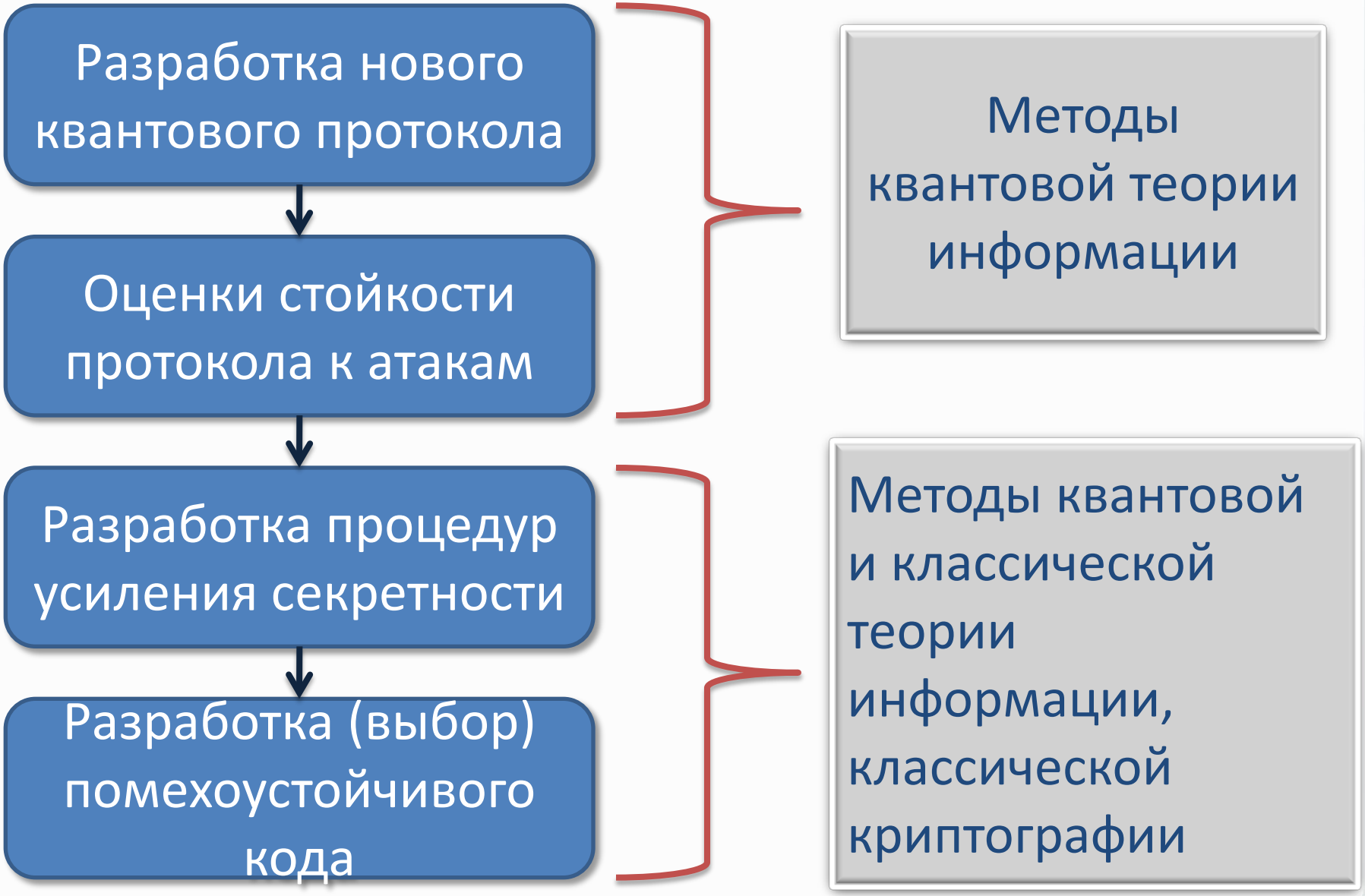
Протоколы с одиночными кудитами					Протоколы с парами перепутанных кудитов	
1	**2**	**3**	**4**	**5**	**6**	**7**
n	$D_{\max}$					
	n+1 базис, IR-атака	2 базиса, IR-атака	n+1 базис, полупрозрач. атака	2 базиса, полупрозрач. атака	атака несимметрич. клонирования	атака симметрич. клонирования
2	0,22709	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

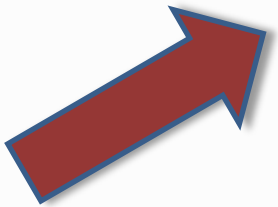
n	2	3	4	5	7	8	9	11	13	16
Протоколы "приготовление – измерение", 2 базиса	0,5	0,792	1,0	1,161	1,404	1,5	1,585	1,73	1,85	2,0
Протоколы "приготовление – измерение", n+1 базис	0,333	0,396	0,4	0,387	0,351	0,333	0,317	0,288	0,264	0,235
Протоколы с перепутанными кудитами	0,125	0,198	0,25	0,29	0,351	0,375	0,396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

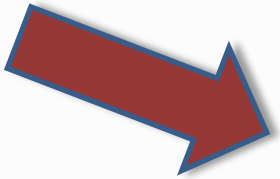
Этапы синтеза структуры квантовых систем прямой безопасной связи



Разработка нового протокола



Разработка схемы кодирования информации



Разработка схемы контроля прослушивания канала

Принципы квантового кодирования классической информации

- Каждой группе классических битов соответствует отдельное квантовое состояние.
- Разным группам битов соответствуют ортогональные состояния.
- Проективное измерение в соответствующем базисе позволяет точно определять закодированную группу битов.

Кодирование для пинг-понг протокола с перепутанными парами кубитов

Четыре перепутанных состояний пары кубитов:

$$\left|\varphi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_1\left|0\right\rangle_2 + \left|1\right\rangle_1\left|1\right\rangle_2\right) \qquad \left|\varphi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_1\left|0\right\rangle_2 - \left|1\right\rangle_1\left|1\right\rangle_2\right)$$

$$\left|\psi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_1\left|1\right\rangle_2 + \left|1\right\rangle_1\left|0\right\rangle_2\right) \qquad \left|\psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_1\left|1\right\rangle_2 - \left|1\right\rangle_1\left|0\right\rangle_2\right)$$

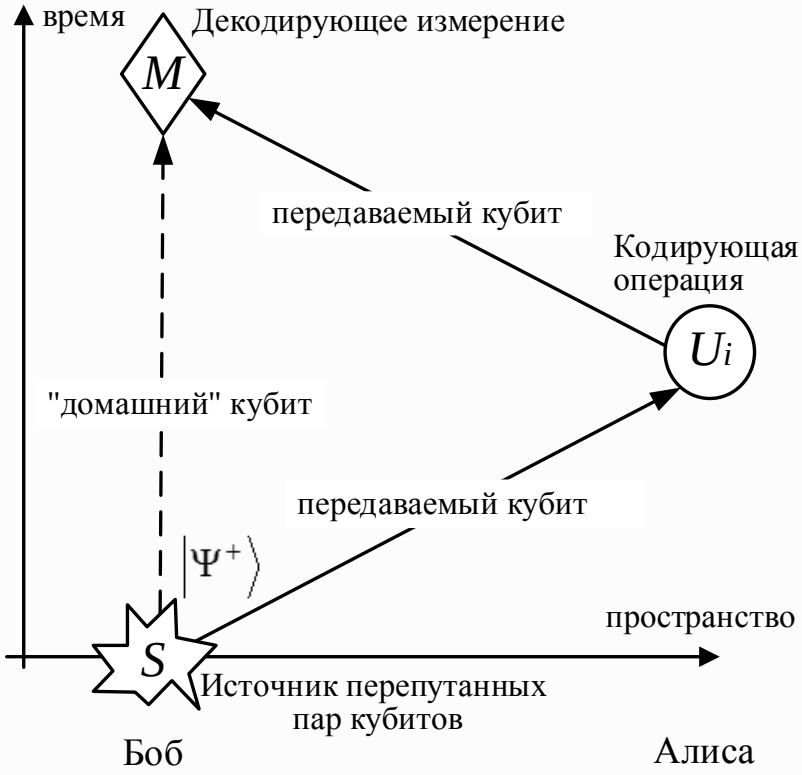
Кодирующие операции:

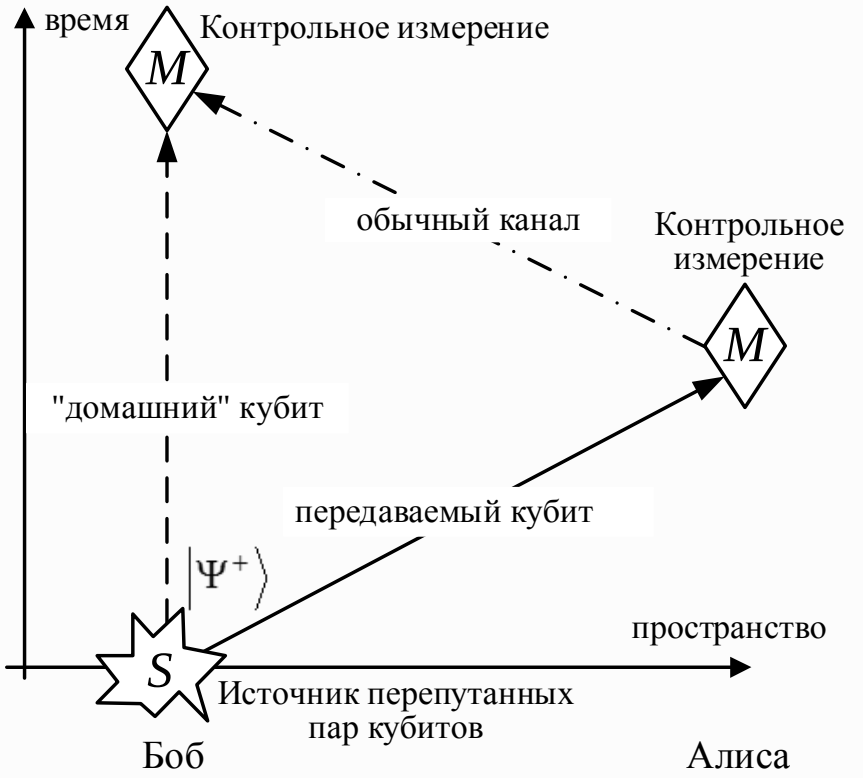
$$U_{00} = I \qquad U_{01} = \sigma_z \qquad U_{10} = \sigma_x \qquad U_{11} = i\sigma_y$$

преобразуют состояние $\left|\psi^{+}\right\rangle$ в состояния $\left|\psi^{+}\right\rangle$ $\left|\psi^{-}\right\rangle$ $\left|\varphi^{+}\right\rangle$ $\left|\varphi^{-}\right\rangle$

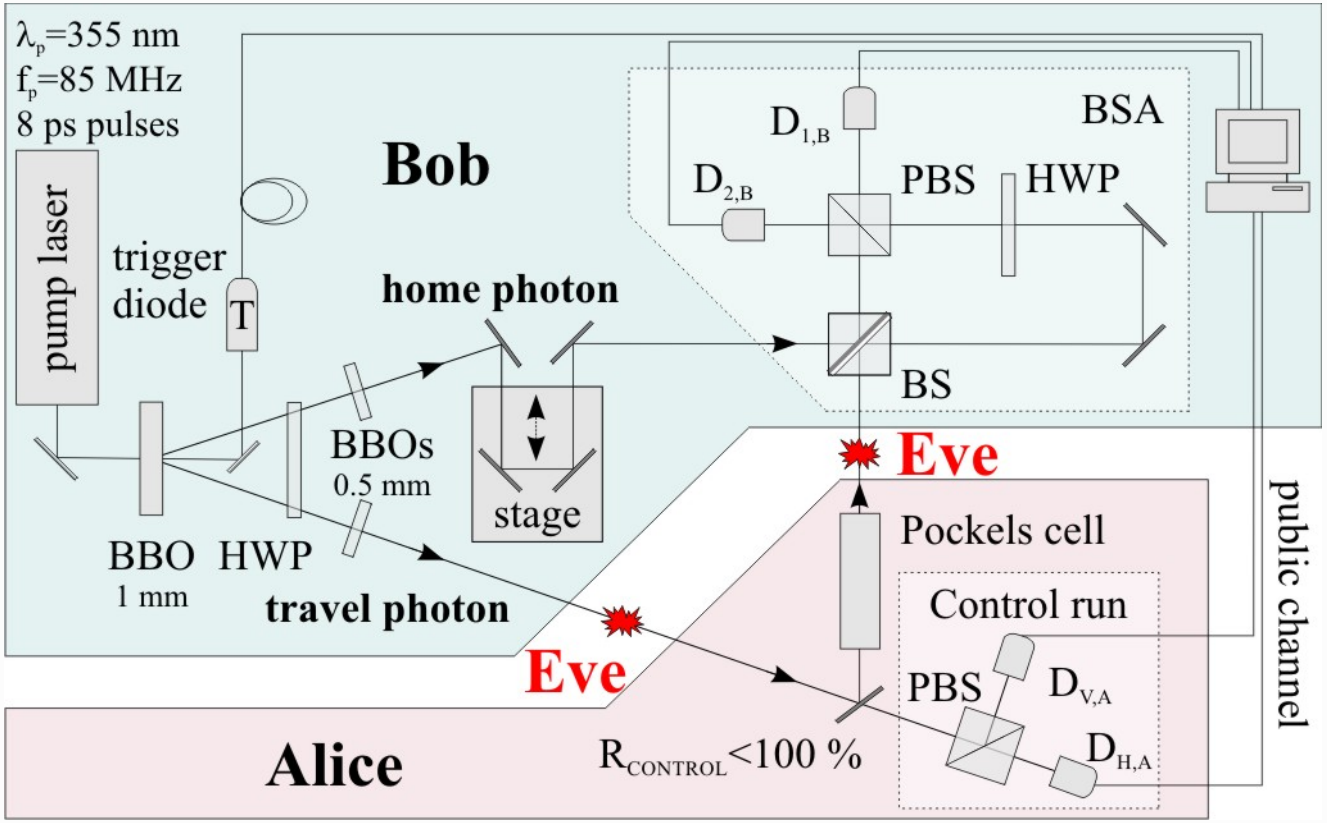
которые будут соответствовать парам классических битов «00», «01», «10», «11»

Схемы режима передачи сообщения и режима контроля подслушивания в пинг-понг протоколе с парами кубитов





Оптическая схема реализации упрощенного пинг-понг протокола с двумя состояниями $|\psi^+\rangle$ и $|\psi^-\rangle$



BBO – кристалл бората бария; **HWP** – пластина в половину длины волны; **PBS** – поляризационный делитель луча; **BS** – делитель луча; **D** – детекторы фотонов; **BSA** – схема для измерений в базисе Белла; **Pockels cell** – ячейка Покельса

Атака пассивного перехвата

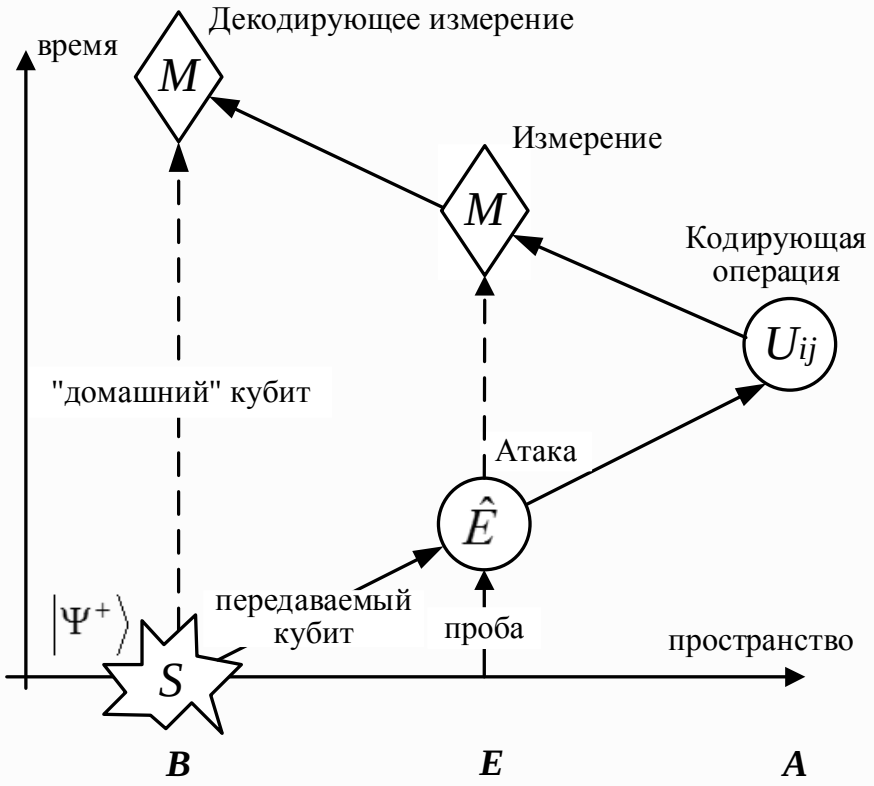
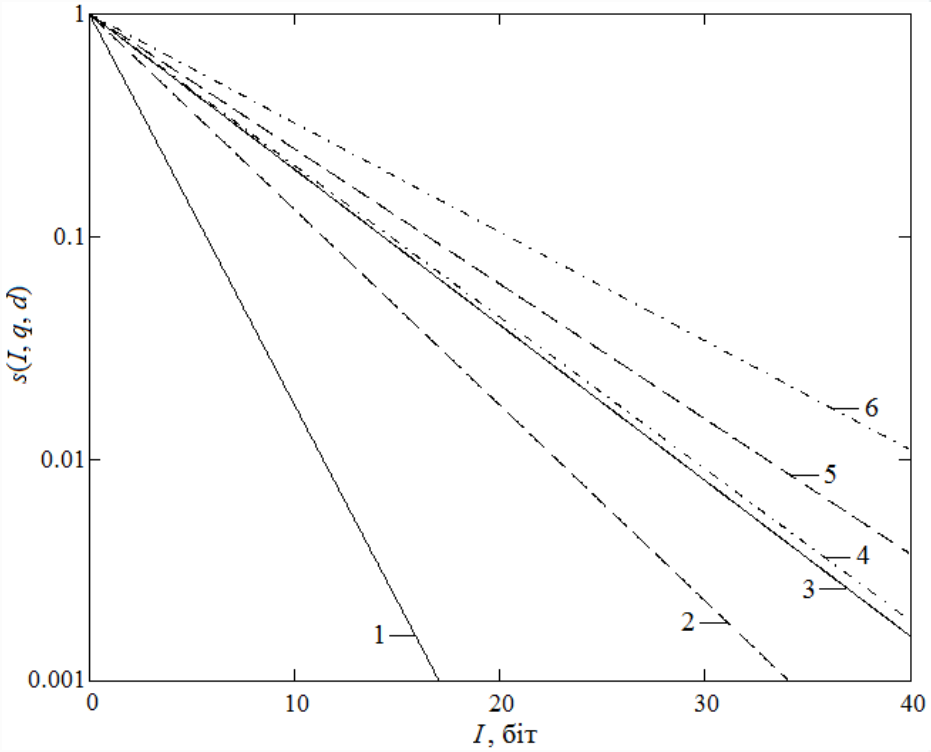


Схема атаки



Полная вероятность **необнаружения** атаки для различных вариантов протокола

Метод усиления секретности

Обратимое хеширование:

$$b_i = M_i a_i$$

a_i – исходный битовый блок сообщения

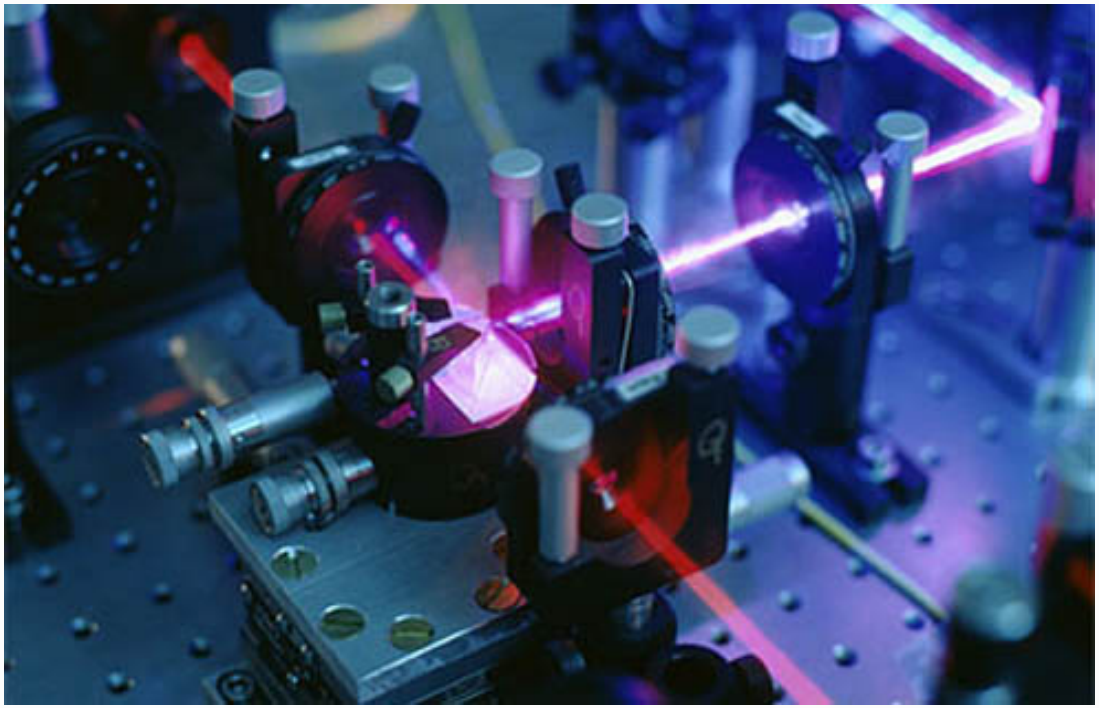
M_i – случайная обратимая двоичная матрица

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

Восстановление исходного сообщения:

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

БЛАГОДАРЮ ЗА ВНИМАНИЕ!



www.onat.edu.ua

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