

**МИНОБРНАУКИ РОССИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «ВГУ»)**

**ФАКУЛЬТЕТ КОМПЬЮТЕРНЫХ НАУК  
КАФЕДРА ЦИФРОВЫХ ТЕХНОЛОГИЙ**

# **Квантовый протокол E91. Неравенства Белла**

**Штанько Валерий Александрович  
ВГУ ФКН, бакалавр, 4 курс  
Научный руководитель: профессор А. Ф. Клиньских**

# Введение

Криптография - наука об изобретении кодов и шрифтов, известная со времен Цезаря. Ее популярность обусловлена особой важностью секретной передачи информации.

Квантовая криптография — метод защиты коммуникаций, основанный на явлениях квантовой физики. Ее отличием стало использование не математических методов, а — физических.

Одним из перспективных направлений в квантовой криптографии является использование перепутанных состояний для создания секретного ключа. Соответствующий протокол был предложен Экертом в 1991 году, и в литературе его обозначают E91.

# Перепутанное состояние

- это совместное состояние не менее двух квантовых систем, которое получается, если системы происходят из одного источника либо взаимодействовали в прошлом.

В настоящее время в качестве источников перепутанных пар фотонов используются кристаллы с квадратичной нелинейностью, в которых в процессе параметрического распада фотон накачки с частотой  $\omega_0$  распадается на сигнальный  $\omega_s$  и холостой  $\omega_i$  фотоны:

$$\omega_0 = \omega_s + \omega_i$$

и соответствующие волновые вектора удовлетворяют условию фазового синхронизма

$$\vec{k}_0 = \vec{k}_s + \vec{k}_i.$$

## ПРОСТЕЙШИЙ СЛУЧАЙ ПЕРЕПУТАННОГО СОСТОЯНИЯ ДВУХ ПОДСИСТЕМ A и B

$$\psi \in \mathcal{H}_A \otimes \mathcal{H}_B,$$

где  $\mathcal{H}_A$  и  $\mathcal{H}_B$  - гильбертовы пространства, соответствующие подсистемам A и B, называется перепутанным, если его невозможно представить в факторизованном виде:

$$\psi = |\psi_A\rangle \otimes |\psi_B\rangle$$

где  $|\psi\rangle_A \in \mathcal{H}_A$ ,  $|\psi\rangle_B \in \mathcal{H}_B$ .

Понятие перепутанности для смешанных состояний является обобщением такого для чистых состояний. Пусть система находится в смешанном состоянии  $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B$ . Состояние  $\rho$  называется факторизованным, если

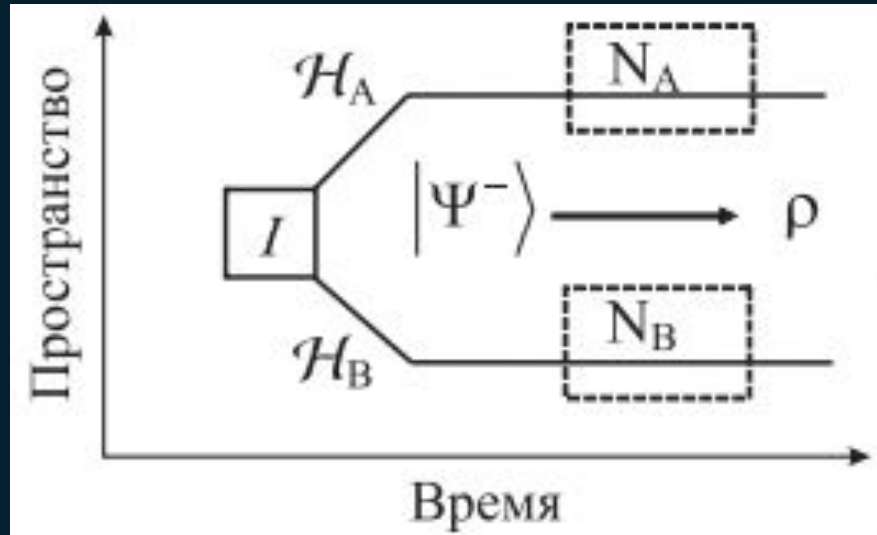
$$\rho = \rho_A \otimes \rho_B,$$

где  $\rho_A \in \mathcal{H}_A$ ,  $\rho_B \in \mathcal{H}_B$ . Состояние  $\rho$  называется сепарабельным, если его можно представить в виде выпуклой комбинации факторизованных состояний,

$$\rho_{\text{sep}} = \sum_n p_n \rho_n^A \otimes \rho_n^B,$$

где  $p_n$  есть вероятность соответствующего факторизованного состояния:  $p_n > 0$ ,  $\sum_n p_n = 1$ . Если состояние невозможно представить в законченном виде, то оно называется перепутанным.

# ВОЗМОЖНОЕ ИЛЛЮСТРАТИВНОЕ ПРЕДСТАВЛЕНИЕ ЧИСТЫХ И СМЕШАННЫХ ПЕРЕПУТАННЫХ СОСТОЯНИЙ



Следуя Д. Бому, перепутанное состояние двух частиц с полуцелым спином (кубитов), которые образуются в результате распада частицы со спином 0. Суммарный спин двух частиц при этом сохраняется и равен 0, поэтому спины кубитов должны быть строго антикоррелированы. Вектор состояния данного синглетного состояния двух кубитов имеет вид

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}} \left( |1\rangle_A \otimes |0\rangle_B - |0\rangle_A \otimes |1\rangle_B \right),$$

где  $|1(0)\rangle_{A(B)}$  обозначает спин вверх (вниз) у кубита, относящегося к подсистеме А (В). Состояние представляет пример, в котором усреднение по одной из подсистем оставляет другую в максимально перемешанном состоянии  $(|0\rangle\langle 0| + |1\rangle\langle 1|) / \sqrt{2}$ .

## ЧЕТЫРЕ МАКСИМАЛЬНО ПЕРЕПУТАННЫХ СОСТОЯНИЯ БЕЛЛА

$$(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) / \sqrt{2} = |\Phi^+\rangle,$$

$$(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle) / \sqrt{2} = |\Phi^-\rangle,$$

$$(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle) / \sqrt{2} = |\Psi^+\rangle,$$

$$(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle) / \sqrt{2} = |\Psi^-\rangle,$$



При проекции спина на произвольный единичный вектор  $\vec{n}$  измеряется наблюдаемая

$$\vec{n} \cdot \vec{\sigma} = n_x \sigma_x + n_y \sigma_y + n_z \sigma_z$$

где  $\sigma_x, \sigma_y, \sigma_z$  — матрицы Паули. Легко проверить, что результаты локальных измерений наблюдаемой  $\vec{n} \cdot \vec{\sigma}$  могут принимать только два значения:  $\pm 1$  (в соответствии с собственными значениями наблюдаемой). С другой стороны, нетрудно убедиться в том, что, как бы ни были направлены векторы  $\vec{n}$  и  $\vec{m}$ , для среднего значения совместной наблюдаемой в состоянии  $|\Psi^-\rangle$ , выполняется равенство

$$\langle \Psi^- | (\vec{n} \cdot \vec{\sigma}_A) \otimes (\vec{m} \cdot \vec{\sigma}_B) | \Psi^- \rangle = -\vec{n} \cdot \vec{m}$$

Из этого следует, что при измерении вдоль одной и той же оси квантовомеханическое среднее в синглетном состоянии равно  $-1$ , являясь математическим выражением антикорреляции. Как было впервые показано Д. Беллом, квантовомеханическое среднее противоречит результату, выводимому из теории “скрытых параметров”.

В теории скрытых параметров ожидаемые значения произведений  $\vec{n} \cdot \vec{\sigma}_A$  и  $\vec{m} \cdot \vec{\sigma}_B$  даются усреднением результатов, получаемых локально и независимо друг от друга Алисой и Бобом, по распределению вероятности  $\rho(\lambda)$  некоего скрытого параметра  $\lambda$ ,

$$E(\vec{n}, \vec{m}) = \int d\lambda \rho(\lambda) N(\vec{n}, \lambda) M(\vec{m}, \lambda),$$

где  $N, M = \pm 1$  описывают зависящие от скрытого параметра  $\lambda$  статистики локальных измерений Алисы и Боба соответственно

## СПЕЦИАЛЬНЫЙ СЛУЧАЙ НЕРАВЕНСТВ БЕЛЛА И КХШХ (CHSH)

Квантовая механика предсказывает следующее значение коррелятора в синглетном состоянии:

$$\langle \Psi^- | (a \otimes c - a \otimes d + b \otimes c + b \otimes d) | \Psi^- \rangle = -2\sqrt{2}$$

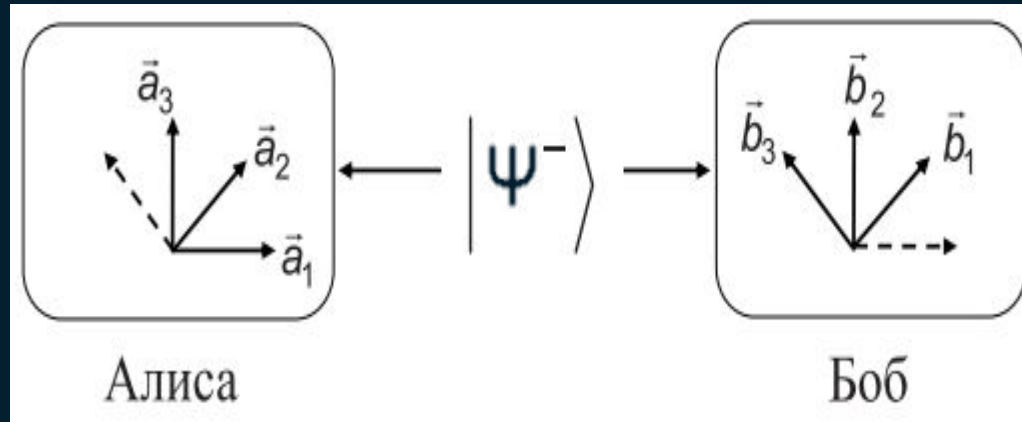
Для вычисления этого же коррелятора в рамках теории скрытых параметров напомним, что в силу принятия значений  $+1$  или  $-1$  наблюдаемыми  $a, b, c, d$ , то есть их дихотомичности, имеем

$$ac - ad + bc + bd = a(c - d) + b(c + d) = \pm 2 \text{ или } 0.$$

Тогда модуль коррелятора мажорируется неравенством:

$$|S| = |E(\vec{a}_1, \vec{b}_1) - E(\vec{a}_1, \vec{b}_3) + E(\vec{a}_3, \vec{b}_1) + E(\vec{a}_3, \vec{b}_3)| \leq 2$$

## СХЕМА ПРОТОКОЛА ЭКЕРТА



Чистое состояние такого источника описывается волновой функцией

$$|\Psi\rangle = |00\rangle \otimes |A\rangle + |01\rangle \otimes |B\rangle + |10\rangle \otimes |C\rangle + |11\rangle \otimes |D\rangle$$

где состояния  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$ ,  $|11\rangle$  представляют базисные векторы двухчастичной системы и, в то время как состояния  $|A\rangle$ ,  $|B\rangle$ ,  $|C\rangle$ ,  $|D\rangle$  — это некие состояния подслушивающей стороны. Единственной возможностью для Евы не быть обнаруженной — это создать источник, генерирующий состояния

$$|\Psi\rangle = (|01\rangle - |10\rangle) \otimes |C\rangle.$$

В любом другом случае состояния кубитов Евы будут перепутаны с состояниями Алисы и Боба, что может быть обнаружено ими при измерениях. Но состояние  $|C\rangle$  является полностью декоррелированным по отношению к синглетному состоянию в (1.18). Следовательно, измерение Евой своей частицы не дает ей никакой информации о состоянии кубитов Алисы и Боба.