НЕКЛАСИЧНІСТЬ КВАНТОВИХ СТАНІВ ТА ЇЇ ЗАСТОСУВАННЯ В КВАНТОВІЙ КРИПТОГРАФІЇ

А.О. СЕМЕНОВ[1,2], **В.К. УСЕНКО**[1,3], **Є.В. ЩУКІН**[2], **Б.І. ЛЕВ**[1]

[1]**Інститут фізики Національної академії наук України**
(Просп. Науки, 46, Київ 03028),

[2]**Institut für Physik, Universität Rostock**
(Universitätsplatz 3, D-18051 Rostock, Germany),

[3]**Dipartimento di Fisica, Università di Milano**
(Via Celoria 16, I-20133 Milano, Italy)

УДК 530.145

Теоретичний та експериментальний прогрес сучасних методів квантової оптики дозволяє проводити досить глибинні фундаментальні дослідження основ квантової фізики. Некласичністю, у найширшому розумінні, називають такі статистичні та динамічні властивості квантових станів, які не мають пояснення в рамках будь-якої класичної теорії. Прикладами є парадокс Ейнштейна—Подольського—Розена, субпуасонівська статистика фотовідліків, квадратурне стиснення тощо. В роботі зроблено огляд сучасного стану теорії некласичних станів та основних експериментальних методів їх дослідження. Розглянуто застосування некласичності до проблеми передачі криптографічного ключа, яка є однією з критично-важливих задач у практиці забезпечення конфіденційного зв'язку.

ЗМІСТ

1. Вступ

Технологічний та науковий прогрес нашого часу багато в чому визначається стрімким розвитком сучасних інформаційних технологій. Це стало основною причиною того, що вже саме поняття інформації із абстрактної категорії перейшло сьогодні у суто практичну площину. Дійсно, ще кілька десятків років назад такі звичні речі як Інтернет, мобільній зв'язок, не кажучи вже про системи електронних платежів, здавалися перспективою віддаленого майбутнього. Проте сьогодні вони стали невід'ємною частиною нашого повсякденного життя.

Основи теорії інформації були закладені в 1948 році відомою роботою Шеннона [1]. З фізичної точки зору інформацією називають стан деякої системи. Так, в класичній механіці стан задається точкою у фазовому просторі, тобто координатою q та імпульсом p. Це твердження еквівалентне тому, що ми зіставляємо з кожною точкою деяке повідомлення. Те ж саме можна сказати про моду електромагнітного поля, яка задається комплексною амплітудою α, дійсну і

уявну частини якої також можна розглядати як пару координата-імпульс.

У більшості практичних та суто теоретичних процесів присутні джерело та споживач інформації. Перше, як правило, характеризується деяким ненульовим значенням ентропії. У нашому прикладі це означає можливість генерації різних повідомлень, яким відповідають певні значення координати та імпульсу. Причому кожне таке повідомлення з'являється з деякою властивою йому імовірністю. Це так само, як у літературному тексті кожній літері відповідає своя імовірність появи. Наприклад, літера "а" зустрічається набагато частіше ніж "щ". Більш того, частота появи тієї чи іншої літери є різною для різних авторів, стилів і т. ін. Інший приклад можна навести із військової справи, коли кулі попадають у ціль із певною купністю, причому відповідний розподіл залежить від зразка стрілецької зброї, майстерності стрілка та інших факторів. Тому кожному джерелу можна приписати деяку функцію розподілу $\varrho(p,q)$.

Щодо споживача, то можна сказати, що для нього стан системи до отримання певних результатів вимірювання координати та імпульсу задається саме функцією розподілу, яка відповідає інформації про джерело, якою він володіє. Наприклад, споживач знає частоту появи всіх літер у текстах певного автора. Або він володіє інформацією про купність пострілів по цілі для певного зразка стрілецької зброї (тобто фактично відповідною функцією розподілу).

Повертаючись до прикладу фазового простору у класичній механіці, необхідно зазначити, що в цьому випадку ми маємо справу з двома, взагалі кажучи скорельованими, джерелами інформації — окремо для координати та імпульсу. Сучасні методи стохастичної оптики дозволяють відтворити відповідну спільну функцію розподілу $\varrho(p,q)$ на експерименті як для класичних, так і для квантових полів, див., наприклад, [2]. Найбільш характерною ознакою квантового випадку є те, що функція розподілу (функція Вігнера [3]) може мати від'ємні значення. Тобто статистичні властивості квантових систем докорінно відрізняються від класичних. Більш того, вони не вписуються у звичну аксіоматику теорії імовірностей, а тому кажуть про неколмогоровість або некласичність квантових станів [4]. Відповідно властивості квантової інформації (яка визначається як стан квантової системи) суттєво відрізняються від класичних.

Взагалі кажучи, поняття некласичності є набагато загальнішим, ніж просто наявність від'ємних значень функції Вігнера для певних станів. Найбільш відомим її прикладом є переплутування (entanglement), яке вперше було розглянуто у знаменитій роботі Ейнштейна, Подольського та Розена (ЕПР) в 1935 році: "Чи можна вважати, що квантово-механічне описання фізичної реальності є повним?" [5]. Власне з цієї роботи і почалася дискусія, яка торкнулася найбільш глибинних аспектів не лише фізики, а й усіх природничих (а на думку деяких авторів і гуманітарних [6]) наук. На запитання, яке ЕПР винесли у назву своєї роботи, їм довелось відповісти негативно. Більше того, вони припустили існування деякої теорії, яка могла б адекватно описати фізичну реальність. З цією точкою зору не погодився Бор [7], зазначивши, що "... quantum mechanics within its scope would appear as a completely rational description of physical phenomena, such as we meet in atomic processes." В ході цієї дискусії Шредінгер у своїй роботі [8] власне і ввів термін "переплутування".

Значно пізніше, в 1964 році, Дж. Белл формалізував ці твердження [9] та показав, що існують деякі нерівності, які можуть порушуватися у тому випадку, якщо квантова теорія повністю та адекватно описує фізичну реальність. На початку 80-х років це було з успіхом підтверджено в дослідах Аспекта із співробітниками [10]. Таким чином, було експериментально доведено, що статистичні властивості квантових і класичних об'єктів є суттєво різними. Більше того, одні не можуть бути зведені до інших.

Окрім наявності від'ємних значень функції Вігнера та переплутування в квантовій оптиці відомі ще кілька статистичних ефектів, що відрізняють квантове світло від класичного. Насамперед, це стиснення за числом фотонів [11] та за квадратурами [12]. Суть цих ефектів полягає у тому, що в процесі фотоелектричного детектування світла завжди присутній так званий дробовий шум, зумовлений квантовою природою детектора. Виявляється, що для певних квантових станів цей шум може значно зменшуватися, а в деяких ідеальних випадках і зовсім зникати [13].

Оскільки властивості квантової інформації суттєво відрізняються від класичних, її обробка (quantum information processing) в перспективі може привести до кардинально нових можливостей в інформаційних технологіях [14]. Насамперед це стосується перспектив створення квантового комп'ютера [15] — пристрою, що може працювати на багато порядків швидше звичайних класичних комп'ютерів. Найвідомішою задачею для квантового комп'ютера є факторизація числа на добуток простих співмножників — алгоритм, запропонований Шором у 1991 р. [16].

Відповідний класичний алгоритм вимагає кількості операцій, що зростає за експонентою в залежності від порядку числа: факторизація числа із тисячі знаків вимагатиме часу більше, ніж існує Всесвіт. Цей факт використовується у класичній криптографії в досить поширеному протоколі Ріверста—Шаміра—Адлемана (RSA) [17] (див. також [18]). Алгоритм Шора впорається з цією задачею за лічені хвилини. Тобто створення квантового комп'ютера приведе до ненадійності криптографічних систем, що базуються на алгоритмі RSA. Більше того, навіть сама перспектива створення подібного пристрою у недалекому майбутньому вимагає вже сьогодні використовувати альтернативні методи для захищеності передачі інформації, конфіденційність якої буде актуальною і через кілька десятків років.

Квантова інформатика пропонує альтернативний шлях для розв'язання цієї задачі, який технологічно доступний вже сьогодні. Методика квантової криптографії ґрунтується на теоремі про неможливість клонування квантових станів (no-cloning theorem) [19]. Вона описує одну з найбільш цікавих властивостей квантової інформації. Суть її така. Припустимо, що потрібно переписати деякий файл з одного носія інформації на інший (наприклад, з жорсткого диска комп'ютера на CD). Як результат, відповідна класична інформація буде існувати на двох носіях одночасно. З квантовою інформацією це неможливо. Подібна операція обов'язково приводить до стирання інформації на першому носії. Такий процес має назву квантової телепортації [20]. Тобто будь-яке втручання у квантовий стан залишає у ньому свій слід, що й може бути використане відправником та споживачем конфіденційної інформації для виявлення несанкціонованого доступу. Безсумнівною перевагою методу квантової криптографії є можливість його реалізації на базі існуючих технологічних можливостей. Так, протокол Беннета та Брассара, запропонований ще у 1984 р. (BB84) [21], на сьогодні вже реалізований у перших комерційних зразках [22, 23].

Метою цієї роботи є огляд найважливіших теоретичних та експериментальних результатів, що стосуються проблеми некласичності квантових станів, а також квантової криптографії — найбільш доступного з практичної точки зору методу, що пропонує квантова інформатика. Структура статті така. У розділі 2 некласичність розглядається з операційної точки зору, тобто з позицій певних експериментальних процедур. Розділ 3 дає строго математичне визначення поняття некласичності та вводить такі суттєві поняття, як когерентні стани, представлення фазового простору, спостережувана-індикатор (witness). Зокрема, у цьому розділі строго математично доводиться, чому квантова механіка не може бути виведена з деякого "розширеного" варіанта класичної. Проте слід зауважити, що цей розділ є формальнішим за попередній та наступні, тому його читання вимагає певної математичної підготовки. У розділі 4 описується явище переплутування — найбільш відомий прояв некласичності квантових станів. Розділ 5 знову присвячений експериментальному визначенню некласичності, проте у ньому розглянуто більш тонкі експериментальні схеми, за допомогою яких можна спостерігати і використовувати це явище. У розділі 6 розглянуті дворівневі системи — кубіти, які є аналогом класичних бітів, за допомогою яких найчастіше кодується інформація. Розділ 7 присвячений застосуванню явища некласичності для секретної передачі квантового ключа. Завершують огляд висновки.

2. Некласичність з операційної точки зору

Увага, яка в наші дні приділяється некласичності багатьма дослідниками, не в останню чергу пов'язана з можливістю прямої експериментальної перевірки фундаментальних законів квантової фізики. В принципі, на сьогодні відомо досить багато систем, які дозволяють виконання такого роду досліджень: одиничні атоми та іони, бозе-ейнштейнівський конденсат, ядерні спіни в атомах молекул, надпровідники, електромагнітне поле в мікрохвильовому і в оптичному діапазонах тощо, див. [14]. В даній роботі основну увагу приділено порівняно простій системі — квантовому світлу. По-перше, вільне електромагнітне поле допускає простий теоретичний опис за допомогою набору гармонічних осциляторів, які відповідають певним модам. По-друге, в оптичному діапазоні при кімнатній температурі практично відсутній тепловий шум — один з основних руйнівників ефектів некласичності, див., наприклад, [24, 25]. По-третє, слід відзначити добре розвинуту техніку генерування і детектування квантових станів світла, що робить виконання відповідних експериментів доступним для багатьох лабораторій.

Вектор-потенціал $\mathbf{A}(\mathbf{r}, t)$ класичного вільного електромагнітного поля, який відповідає вибраній моді, можна записати у вигляді

$$\mathbf{A}(\mathbf{r}, t) = \mathbf{C}(\omega) \left[\alpha(t) e^{i\mathbf{kr}} + \alpha^*(t) e^{-i\mathbf{kr}}\right], \qquad (1)$$

де ω — частота моди, $\mathbf{k}$ — хвильовий вектор, $\mathbf{C}(\omega)$ — деяка векторна стала, яка залежить від частоти,

$$\alpha(t) = \alpha(0)e^{-i\omega t} \tag{2}$$

— безрозмірна комплексна амплітуда поля, яка виражається через дійсні польові координату q і імпульс p,

$$\alpha = \frac{1}{\sqrt{2}}(q + ip). \tag{3}$$

Амплітуда поля α (чи, що те ж саме — польові координата та імпульс) визначають фазовий простір для однієї моди електромагнітного поля. Гамільтоніан, який відповідає цій системі,

$$H = \hbar\omega\alpha^*\alpha \tag{4}$$

є добре відомим гамільтоніаном гармонічного осцилятора, а вираз (2) є розв'язком відповідних рівнянь руху.

Квантування цієї системи зводиться до простої заміни класичних динамічних змінних операторами. Тоді вектор-потенціал є операторною величиною

$$\hat{\mathbf{A}}(\mathbf{r}, t) = \mathbf{C}(\omega)\left[\hat{a}(t)e^{i\mathbf{kr}} + \hat{a}^\dagger(t)e^{-i\mathbf{kr}}\right], \tag{5}$$

де $\hat{a}(t)$ та $\hat{a}^\dagger(t)$ (аналоги $\alpha(t)$ і $\alpha^*(t)$) інтерпретують як оператори знищення і народження фотонів, для яких виконується бозонне комутаційне співвідношення

$$\left[\hat{a}, \hat{a}^\dagger\right] = 1. \tag{6}$$

Повністю аналогічно класичному випадку вводяться оператори польової координати $\hat{q}$ та імпульсу $\hat{p}$:

$$\hat{a} = \frac{1}{\sqrt{2}}(\hat{q} + i\hat{p}). \tag{7}$$

Гамільтоніан системи має вигляд

$$\hat{H} = \hbar\omega\,\hat{a}^\dagger\hat{a}. \tag{8}$$

Оператор $\hat{a}^\dagger\hat{a} = \hat{n}$ є оператором числа фотонів в моді. Далі, згідно із загальним формалізмом теорії, формулюється шредінгерівська або гейзенбергівська картини руху.

У даному розділі ми розглянемо питання про те, як з'являється некласичність однієї моди квантового світла з операційної точки зору, тобто з точки зору експерименту. В першу чергу, буде показано, яким чином можна отримати експериментальне підтвердження того факту, що функція розподілу в квантовому випадку (функція Вігнера) може набувати від'ємних значень. Далі буде розглянуто більш тонкі нюанси некласичності, пов'язані зі стисненням світла — квадратурним і за числом фотонів.

2.1. Функція Вігнера

Плоска хвиля (1), яка задає моду електромагнітного поля, навіть в класичному випадку є дуже сильною ідеалізацією реальних процесів. Справа в тому, що у більшості джерел світла амплітуда α має флуктуації різної природи. Наприклад, світло звичайної лампи утворюється в результаті великої кількості хаотичних атомних переходів. Амплітуда такого світла, навіть якби воно було одномодовим, також хаотично змінюється від вимірювання до вимірювання. Тому в оптиці особливо актуальним є статистичний опис електромагнітної хвилі за допомогою функції розподілу $\varrho(p, q)$.

Оскільки визначення того, чи є світло некласичним, в першу чергу, залежить від його стану, то саме собою напрошується питання про метод експериментальної реконструкції функції розподілу, який би був однаковим як для квантового, так і для класичного випадку. Одночасно виміряти координату та імпульс, щоб шляхом набору статистичних даних отримати інформацію про функцію розподілу $\varrho(p, q)$, ми не можемо. Проте кожну з них можна виміряти окремо, і отримати дві функції розподілу $\varrho(p)$ і $\varrho(q)$. Але, на жаль, в них відсутня інформація про кореляцію між координатою та імпульсом [26]. В сучасній квантовій оптиці існує метод *гомодинного детектування* [27], який дозволяє вимірювати спостережувану

$$\hat{x}(\varphi) = \hat{q}\cos\varphi + \hat{p}\sin\varphi = \frac{1}{\sqrt{2}}\left(\hat{a}e^{-i\varphi} + \hat{a}^\dagger e^{i\varphi}\right), \tag{9}$$

яка називається квадратурою, при різних значеннях параметра φ і отримати серію розподілів $p(x; \varphi)$. Експериментальна процедура отримання таких розподілів ніяк не залежить від квантових властивостей і може бути однаково успішно використана і для класичного світла. Виявляється, що інформації, отриманої методом гомодинного детектування, є досить для того, щоб відновити початкову функцію з двома змінними $\varrho(p, q)$.

В основі методу гомодинного детектування лежить ідея змішування сигнального поля з полем локального осцилятора — лазерного поля достатньо великої інтенсивності, через світлоподільну пластинку 50 : 50, див. рис. 1. Сигнальне поле, чию квадратуру необхідно виміряти, падає на таку пластинку. Фаза локального осцилятора може змінитися за рахунок іншої (фазової) пластинки, встановленої на його

шляху. Далі світлові сигнали з обох виходів світлоподільної пластинки надходять на фотодетектори. За величиною фотоструму можна судити про кількість фотонів n_1 і n_2, зареєстрованих першим і другим детектором відповідно (див. обговорення в [2,28]). Після цього схема віднімання визначає різницю чисел зареєстрованих фотонів $n_1 - n_2$, що виявляється пропорційною квадратурі сигнального поля з фазою φ, яка визначається локальним осцилятором.

Останнє твердження можна довести таким чином. Нехай $\hat{a}$ — оператор знищення (амплітуда) моди сигнального поля, $\hat{a}_{\rm lo}$ — оператор знищення (амплітуда) локального осцилятора, $\hat{b}_1$ і $\hat{b}_2$ — оператори знищення (амплітуди) на виході зі світлоподільної пластинки. Ці оператори зв'язані між собою за допомогою співвідношень входу-виходу (див., наприклад, [29, 30])

$$\hat{b}_1 = \frac{1}{\sqrt{2}} \left(\hat{a} + \hat{a}_{\rm lo}\right), \tag{10}$$

$$\hat{b}_2 = \frac{1}{\sqrt{2}} \left(-\hat{a} + \hat{a}_{\rm lo}\right). \tag{11}$$

Різниця чисел фотонів, яка реєструється схемою віднімання, може бути записана як

$$\hat{n}_1 - \hat{n}_2 = \hat{b}_1^\dagger \hat{b}_1 - \hat{b}_2^\dagger \hat{b}_2. \tag{12}$$

Той факт, що локальний осцилятор являє собою поле лазера з достатньо великою амплітудою, тобто фактично є класичним полем, може бути врахований за допомогою наближення відповідного оператора звичайним комплексним числом

$$\hat{a}_{\rm lo} \approx re^{i\varphi}, \tag{13}$$

де r — модуль амплітуди, а φ — фаза локального осцилятора (точне доведення правильності даного наближення у випадку, який розглядається, див. в [29]). Шляхом підстановки співвідношення входу-виходу (10), (11) у вираз (12) отримуємо

$$\hat{n}_1 - \hat{n}_2 = r\sqrt{2}\hat{x}(\varphi), \tag{14}$$

де квадратура $\hat{x}(\varphi)$ задається виразом (9). Окремо слід відзначити, що загальна форма виразу (14) не залежить від того, є сигнальне поле класичним чи квантовим.

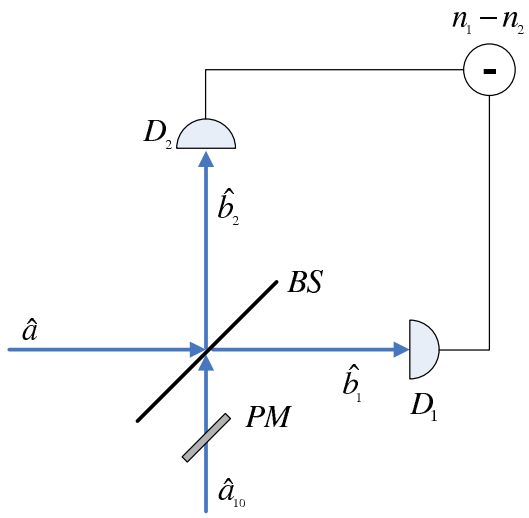

Рис. 1. Схема гомодинного детектування, вперше запропонована в роботі [26]. D_1, D_2 — детектори, BS — світлоподільна пластинка 50:50, PM — фазовий модулятор

Отримавши експериментальним шляхом набір одновимірних розподілів квадратур $p(x;\varphi)$ із різними фазами φ, можна тепер відновити функцію розподілу $\varrho(p,q)$. Цей математичний метод носить назву *оптичної томографії*. Фактично він аналогічний томографії, яку використовують в медицині. Суть його така. Користуючись методами звичайної теорії імовірності, можна записати очевидне співвідношення

$$p(x;\varphi) = \int\limits_{-\infty}^{+\infty} {\rm d}q\, {\rm d}p\, \varrho(p,q)\, \delta\left[x - q\,\cos\varphi - p\,\sin\varphi\right], \tag{15}$$

яке має назву перетворення Радона [31]. Обернене співвідношення можна записати як

$$\varrho(p,q) = \frac{1}{4\pi^2} \int\limits_0^\pi {\rm d}\varphi \int\limits_{-\infty}^{+\infty} {\rm d}z \int\limits_{-\infty}^{+\infty} {\rm d}x \times$$

$$\times\, |z| \exp\left[iz\left(q\cos\varphi + p\sin\varphi - x\right)\right] p(x;\varphi). \tag{16}$$

Даний вираз (томографічне відображення [32, 33]) встановлює зв'язок між набором розподілів однієї змінної і розподілом двох змінних.

Таким чином, методи гомодинного детектування і оптичної томографії дають можливість реконструювати на експерименті функцію розподілу, яка описує стан системи. Для оптичних полів схему квантової томографії вперше було теоретично запропоновано Фогелем і Ріскеном в 1989 р. [34]. Через деякий час Смі-

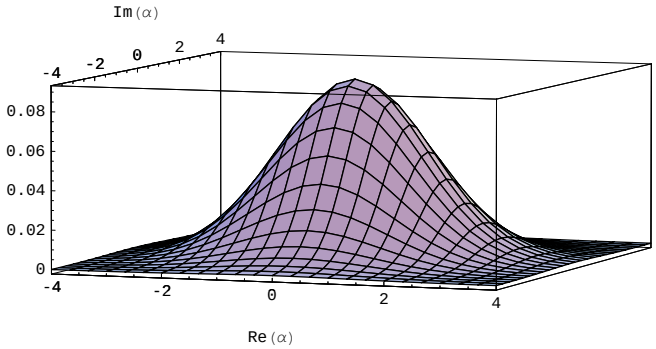

Рис. 2. Функція розподілу термального випромінювання із середнім числом фотонів $\langle n\rangle = 3$

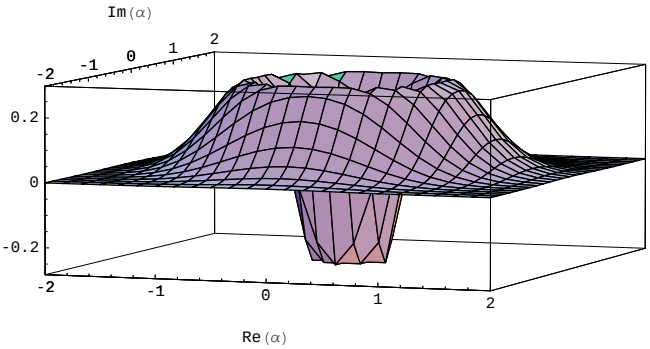

Рис. 3. Функція розподілу (функція Вігнера) однофотонного фоківського стану $|1\rangle$

тей, Бек, Раймер і Фарідані продемонстрували її на експерименті [35]. На сьогодні список об'єктів, для яких розроблено цей метод, виглядає досить вражаюче. Детальний огляд цієї тематики з повним переліком літератури можна знайти в роботі [2].

Відновлюючи функції розподілу від класичного термального джерела, ми отримаємо досить стандартний гаусівський розподіл, рис. 2. Теж саме стосується і когерентного випромінювання лазера. В принципі можливі й інші конфігурації класичних розподілів для оптичних полів. Проте, відновлюючи тепер функцію розподілу для однофотонного фоківського стану $|1\rangle$, який можна одержати, наприклад, як результат одиничного атомного переходу зі збудженого рівня на основний, ми отримаємо функцію розподілу, яка буде мати явно виражені від'ємні значення, рис. 3. Іншими словами, результатом експериментальної процедури є функція розподілу, яка не задовольняє аксіоми теорії імовірності.

Слід особливо підкреслити, що така функція розподілу не може бути отримана з якоїсь загальнішої і "правильної" функції процедурами, які описано в теорії імовірності. Наприклад, вона не є результатом усереднення за деякими "прихованими" змінними, існування яких припускав Ейнштейн. Тому даний приклад є одним з проявів неколмогоровості [4] чи неклассичності квантового стану. Разом з тим, окремо розподіли за координатою та імпульсом є додатними. Тобто некласичність у даному випадку проявляється в специфічних кореляціях між координатою і імпульсом — саме вони не задовольняють аксіоматику теорії імовірності. Одним з наслідків цієї властивості є співвідношення невизначеності — не можна отримати для системи одночасно точні значення координати і імпульсу, хоча б тому, що відповідної події просто не існує (її імовірність є формально негативною). Тому або координата, або імпульс має бути обов'язково невизначеним. А звідси однозначно випливає той факт, що для квантових станів імовірність не може бути видалена з теорії шляхом уточнення наших знань про систему, як це має місце в класичному випадку.

Звернімося тепер до питання про те, яким чином можна зв'язати дану функцію розподілу зі звичним формалізмом, прийнятим в квантовій фізиці. Для цього розглянемо спочатку одне з представлень для функції розподілу в класичному випадку. Характеристичну функцію $\mathcal{C}(\beta)$, яка є фур'є-образом функції розподілу $\varrho(\alpha)$,

$$\mathcal{C}(\beta) = \int\limits_{-\infty}^{+\infty} \mathrm{d}^2\alpha\, \varrho(\alpha) e^{\alpha^*\beta - \alpha\beta^*}, \tag{17}$$

де двовимірне інтегрування ведеться по всьому фазовому простору, можна інтерпретувати як середнє значення експоненти $\exp(\alpha^*\beta - \alpha\beta^*)$. Обернений вираз

$$\varrho\,(\alpha) = \frac{1}{\pi^2} \int\limits_{-\infty}^{+\infty} \mathrm{d}^2\beta\, \mathcal{C}(\beta)\, e^{\alpha\beta^* - \alpha^*\beta} \tag{18}$$

дозволяє відновити функцію розподілу за характеристичною функцією.

Перейдемо до випадку квантової системи. Аналогом формули (17), тобто середнього від експоненти, тепер буде вираз

$$\mathcal{C}(\beta) = \mathrm{Tr}\left[\hat{\varrho}\,\hat{D}(\beta)\right], \tag{19}$$

де $\hat{\varrho}$ є оператором густини, а

$$\hat{D}(\beta) = e^{\hat{a}^\dagger\beta - \hat{a}\beta^*} \tag{20}$$

— операторним аналогом експоненти, який називається оператором трансляцій на фазовому просторі, чи просто оператором трансляцій. Функція розподілу тепер, як і в класичному випадку, визначається формулою (18). Вона називається функцією Вігнера [3] і, слідуючи усталеній традиції, ми будемо позначати її як $W(\alpha)$, залишивши запис $\varrho(\alpha)$ для функції розподілу Ліувілля в класичному випадку.

Саме функцію Вігнера вимірюють в експериментах з квантової томографії, що строго доведено в [2, 29, 30, 34]. У випадку однофотонного фоківського стану, який було розглянуто вище, оператор густини має вигляд

$$\hat{\varrho} = |1\rangle\langle 1| . \tag{21}$$

Звідси безпосереднім обчисленням легко отримати функцію Вігнера такого стану

$$W(\alpha) = -\frac{2}{\pi} L_1\left(4|\alpha|^2\right) e^{-2|\alpha|^2}, \tag{22}$$

де $L_1(x)$ — поліном Лагерра першого порядку. Саме цю функцію і зображено на рис. 3.

2.2. Субпуасонівська статистика

Від'ємністю значень функції Вігнера зовсім не обмежуються усі можливі прояви некласичності для квантового світла. Дійсно, деякі некласичні властивості проявляються навіть у станів з повністю додатною функцією Вігнера. Причина цього полягає в тому, що фотоелектричний ефект, який лежить в основі процесу фотодетектування, є виключно квантовим явищем і не допускає класичного опису. Іншими словами, незважаючи на те, що світло є класичним, ми повинні врахувати квантову природу детектора, яка приводить до додаткової стохастичності процесу.

Навіть світло від лазера, близького до ідеального, яке описується класичною монохроматичною хвилею (1), детектується з певними флуктуаціями числа фотонів. Тому можна говорити про деякий шум, який називають дробовим (shot), вакуумним чи фотонним [4, 36]. Для класичного світла існує певна межа, яка відповідає ідеальному лазеру, нижчим за яку цей шум бути не може. Хоча некласичне світло (наприклад, уже згаданий фоківський стан) може характеризуватися шумом, який лежить нижче цієї межі [13]. Оскільки, як уже було сказано, побудувати повністю класичну теорію фотодетектування не можливо, був запропонований її напівкласичний варіант, який описує взаємодію класичного світла з квантовим детектором. Некласичність описаного тут типу виникає як невідповідність між даною теорією і статистичними властивостями квантового світла.

Висновки напівкласичної теорії можна подати в такому вигляді. Розглянемо взаємодію класичної монохромної хвилі (1) з фотодетектором, який складається з N незбуджених атомів. Це число, звичайно ж, набагато більше за нормовану на $\hbar\omega$ енергію хвилі

$$E = |\alpha|^2, \tag{23}$$

яка є класичним аналогом числа фотонів. В процесі взаємодії в зону неперервного спектра переходить по одному електрону від деякої кількості атомів n, яку визначають за фотовідліками, тобто за величиною фотоструму, що виник.

З точки зору звичайної теорії імовірності, емісію кожного окремого атома можна розглядати як деякий незалежний випадковий експеримент з фіксованою імовірністю "успіху". Тоді імовірність переходу будь-яких n атомів з N задається стандартним біноміальним розподілом

$$p_n^N = C_N^n \left(\frac{\langle n\rangle}{N}\right)^n \left(1 - \frac{\langle n\rangle}{N}\right)^{N-n}, \tag{24}$$

де C_N^n — біноміальні коефіцієнти, $\langle n\rangle$ — середнє число атомів, емітованих в зону неперервного спектра. Умова ідеального (без втрат) детектування полягає в тому, що середнє число фотовідліків точно дорівнює нормованій енергії (23), тобто

$$\langle n\rangle = |\alpha|^2 . \tag{25}$$

Оскільки загальне число електронів досить велике, то в граничному випадку $N \to +\infty$ цей розподіл прямує до пуасонівського, який з врахуванням умови ідеального детектування (25) може бути записаний як

$$p_n(\alpha) = \frac{|\alpha|^{2n}}{n!} e^{-|\alpha|^2}. \tag{26}$$

Тепер необхідно врахувати той факт, що реальне класичне світло має, як правило, стохастичну природу, тобто описується функцією розподілу $\varrho(\alpha)$. Після усереднення (26) за цією функцією, отримаємо для статистики фотовідліків класичного світла вираз

$$p_n = \int\limits_{-\infty}^{+\infty} \mathrm{d}^2\alpha\, \varrho(\alpha) \frac{|\alpha|^{2n}}{n!} e^{-|\alpha|^2}. \tag{27}$$

Цей вираз називається формулою Манделя [28,37,38]. Використавши вираз (23), можна ввести густину імовірності за енергією $p(E)$ і переписати (27) у вигляді

$$p_n = \int\limits_{-\infty}^{+\infty} \mathrm{d}E\, p(E)\, \frac{E^n}{n!} e^{-E}. \tag{28}$$

Формула Манделя в формі рівняння (28) визначає зв'язок між розподілами імовірностей за двома величинами — енергією світла E і числом фотовідліків n, що вимірюється експериментально. Тобто в напівкласичній теорії обидві ці величини зовсім не еквівалентні.

Стандартною характеристикою будь-якого шуму є його відхилення від середнього, тобто дисперсія. У випадку, який розглядається, для дисперсії числа фотовідліків $\langle \Delta n^2 \rangle$, скориставшись розподілом (27), отримаємо такий вираз:

$$\langle \Delta n^2 \rangle = \langle n \rangle + \langle \Delta E^2 \rangle, \tag{29}$$

де також було враховано інший наслідок з (27), який полягає в тому, що

$$\langle E \rangle = \langle n \rangle. \tag{30}$$

Перший доданок у виразі (29) визначає дробовий шум детектора, а другий — надлишковий шум, пов'язаний зі стохастичною природою світла. Нижньою межею дисперсії фотовідліків класичного світла є випадок нульового надлишкового шуму, який відповідає випромінюванню ідеального лазера. В цьому випадку $\langle \Delta n^2 \rangle = \langle n \rangle$, і кажуть про пуасонівську статистику фотовідліків. Для інших класичних станів світла (наприклад, для термального) $\langle \Delta n^2 \rangle > \langle n \rangle$, і говорять про суперпуасонівську статистику. Таким чином, випадок, коли дисперсія числа фотонів дорівнює їх середньому, відповідає мінімальному шуму для класичного світла.

Оскільки для некласичного світла функція розподілу може набувати від'ємних значень, то можна очікувати і негативної дисперсії енергії, коли надлишковий шум подавляє дробовий. В цьому випадку $\langle \Delta n^2 \rangle < \langle n \rangle$ і кажуть про субпуасонівську статистику, яку і було експериментально продемонстровано [11]. Але така некласичність не може бути пояснена простою заміною функції розподілу $\varrho(\alpha)$ на функцію Вігнера $W(\alpha)$ в виразі (27). Дійсно, існують стани з субпуасонівською статистикою фотовідліків та всюди додатною функцією Вігнера. Наприклад, це стосується однофотонного фоківського стану з лінійними втратами

$$\hat{\varrho} = |1\rangle\, \eta\, \langle 1| + |0\rangle\, (1-\eta)\, \langle 0|, \tag{31}$$

який має субпуасонівський характер статистики для будь-яких $0 < \eta \leq 1$, а від'ємну функцію Вігнера тільки для $0,5 < \eta \leq 1$.

Для розуміння цього факту, звернімося до квантового аналога формули Манделя (27). Згідно з основними принципами квантової теорії, якщо світло перебуває у стані, який описується оператором густини $\hat{\varrho}$, то імовірність реєстрації n фотонів при ідеальному фотодетектуванні задається виразом

$$p_n = \mathrm{Tr}\left[\hat{\varrho}\ |n\rangle\langle n|\right]. \tag{32}$$

З нього з урахуванням тотожності (див. [39])

$$|n\rangle\langle n| = :\frac{\left(\hat{a}^\dagger \hat{a}\right)^n}{n!}\, e^{-\hat{a}^\dagger \hat{a}}: \tag{33}$$

(тут :: означає нормальне впорядкування, тобто при розкладі в ряд усі оператори народження необхідно поставити зліва від операторів знищення) отримаємо

$$p_n = \mathrm{Tr}\left[\hat{\varrho}\ :\frac{\left(\hat{a}^\dagger \hat{a}\right)^n}{n!}\, e^{-\hat{a}^\dagger \hat{a}}:\right]. \tag{34}$$

Цей вираз є операторним представленням для формули Манделя, проте для того щоб досягти повної аналогії з (27), його необхідно переписати в термінах квантової функції (квазі) розподілу.

Розглядаючи функцію Вігнера, ми зробили одне суттєве припущення. А саме, узагальнюючи експоненту до оператора трансляцій (20), ми не врахували того, що будь-яке узагальнення c-числової функції на оператор, взагалі то, є неоднозначним через проблеми упорядкування. Дійсно, існує нескінченно багато подібних операторних узагальнень експоненти. Одне з них, нормально упорядковане

$$\hat{D}_P(\beta) = e^{\hat{a}^\dagger \beta} e^{-\hat{a}\beta^*}, \tag{35}$$

може бути використано при розгляді задачі фотодетектування. Означивши нормально упорядковану характеристичну функцію як

$$\mathcal{C}_P(\beta) = \mathrm{Tr}\left[\hat{\varrho}\, \hat{D}_P(\beta)\right], \tag{36}$$

можна записати відповідну їй функцію квазірозподілу

$$P(\alpha) = \frac{1}{\pi^2} \int\limits_{-\infty}^{+\infty} \mathrm{d}^2\beta\, \mathcal{C}_P(\beta)\, e^{\alpha\beta^* - \alpha^*\beta}, \tag{37}$$

яка називається P-функцією Глаубера—Сударшана [40, 41]. Тепер можна довести, що в термінах цього квазірозподілу формула Манделя (34) буде мати такий вигляд:

$$p_n = \int\limits_{-\infty}^{+\infty} \mathrm{d}^2\alpha\, P(\alpha)\, \frac{|\alpha|^{2n}}{n!} e^{-|\alpha|^2}. \tag{38}$$

Суттєвим тут є те, що (38) можна отримати з аналогічної формули для класичного поля (27) шляхом простої заміни функції розподілу $\varrho(\alpha)$ P-функцією $P(\alpha)$.

Таким чином, даний тип некласичності може бути більш формально визначений через недодатність P-функції. Ще раз нагадаємо, що вона виникає як протиріччя між напівкласичною теорією фотодетектування і статистичними властивостями квантового світла. Операційний зміст такої некласичності полягає в подавленні дробового шуму детектора від'ємним надлишковим шумом квантового світла. При цьому однією з найбільш серйозних проблем є той факт, що P-функція часто не є регулярним виразом. Так, наприклад, для однофотонного фоківського стану вона записується у вигляді

$$P(\alpha) = \left(1 + \frac{1}{4}\frac{\partial^2}{\partial\,\mathrm{Re}\,(\alpha)\;\partial\,\mathrm{Im}\,(\alpha)}\right)\delta(\alpha), \tag{39}$$

тобто виражається через похідну другого порядку від дельта-функції. Природно, що томографічно такий розподіл на експерименті відновити не можливо. Тому Фогелем, Ріхтером і Щукіним були запропоновані інші методи [42–44], які дозволяють експериментально встановити факт відсутності додатної визначеності P-функції. Частково вони були реалізовані в експериментах Львовського і Шапіро [45] для стану (31). Ці методи буде розглянуто в розділі 5 даного огляду.

Класична формула (29) для дисперсії числа фотовідліків в квантовому випадку буде мати вигляд

$$\left\langle \Delta n^2 \right\rangle = \langle n \rangle + \left\langle : \Delta n^2 : \right\rangle, \tag{40}$$

тобто надлишковий шум задається тепер нормально впорядкованою дисперсією фотовідліків [39–41] (див. також виведення цієї формули в роботі [4]). Дисперсія надлишкового шуму, нормована на середнє число фотонів є важливою характеристикою некласичності світла. Відповідний параметр

$$\mathcal{Q} = \frac{\left\langle : \Delta n^2 : \right\rangle}{\langle n \rangle} = \frac{\left\langle \Delta n^2 \right\rangle}{\langle n \rangle} - 1 \tag{41}$$

був запропонований Манделем [28, 46] і носить його ім'я. Зрозуміло, що $\mathcal{Q} = 0$ відповідає випадку пуасонівської статистики, $\mathcal{Q} > 0$ — суперпуасонівської, $\mathcal{Q} < 0$ — субпуасонівської. Інколи в літературі субпуасонівські стани в квантовій оптиці називають світлом, стиснутим за числом фотонів.

2.3. Квадратурне стиснення

Ще одним важливим з практичної точки зору проявом некласичності в розумінні від'ємності P-функції є квадратурне стиснення світла, звіт про перше спостереження якого було опубліковано в [12]. Суть даного ефекту досить проста. Записуючи другу степінь квадратури (9) через нормально впорядковану форму

$$\hat{x}^2(\varphi) = \frac{1}{2} + : \hat{x}^2(\varphi) :, \tag{42}$$

для її дисперсії отримаємо вираз

$$\left\langle \Delta\, x^2(\varphi) \right\rangle = \frac{1}{2} + \left\langle : \Delta\, x^2(\varphi) : \right\rangle. \tag{43}$$

Як і у випадку статистики фотовідліків, тут ми знову маємо справу з дробовим і надлишковим шумом. Відмінність між (43) і (40) полягає в тому, що дисперсія дробового шуму для квадратури не залежить від стану і завжди дорівнює 1/2. Для класичного світла надлишковий шум завжди додатний. Рівність його нулю досягається лише для світла, яке генерується ідеальним лазером. Квантове світло, для якого $\left\langle : \Delta \hat{x}^2(\varphi) : \right\rangle < 0$, називається квадратурностисненим. Для такого світла дробовий шум детектора подавлюється від'ємним надлишковим шумом. Нагадаємо, що експериментально квадратура вимірюється за допомогою методу гомодинного детектування (див. розділ 2.).

Квадратурне стиснення часто інтерпретують з позицій співвідношення невизначеності Гейзенберга. Дійсно, вводячи квадратуру $\hat{p}(\varphi)$ канонічно спряжену до (9), тобто таку, що

$$[\hat{x}(\varphi), \hat{p}(\varphi)] = i, \tag{44}$$

можна записати

$$\left\langle \Delta x^2(\varphi) \right\rangle \left\langle \Delta p^2(\varphi) \right\rangle \geq \frac{1}{4}. \tag{45}$$

Таким чином, зменшення дисперсії по одній квадратурі гарантовано приводить до її збільшення по іншій, рис. 4.

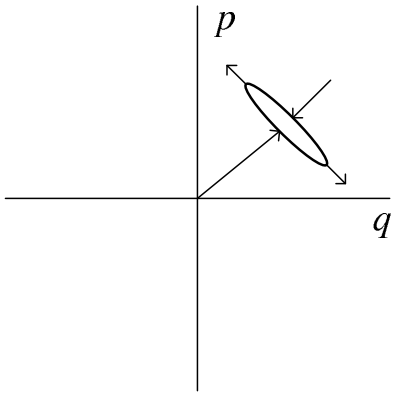

Рис. 4. Схематичне зображення квадратурного стиснення

Принцип генерації квадратурно стисненого світла (для огляду див. [13,47]) частіше усього базується на нелінійній взаємодії декількох мод світла. Так, в середовищах з наявністю нелінійності третього порядку можна говорити про взаємодію гармонік з частотами ω і 2ω. При цьому гамільтоніан взаємодії має вигляд

$$\hat{H}_{\rm int} = -i\hbar\frac{\chi}{2}\left(\hat{a}^2\hat{b}^\dagger - \hat{a}^{\dagger 2}\hat{b}\right), \tag{46}$$

де оператори $\hat{a}$ і $\hat{b}$ описують моди з частотами ω і 2ω відповідно. На практиці досягнути такої взаємодії можна, помістивши нелінійне середовище в резонатор, для якого ці частоти є резонансними. Далі ми припускаємо, що мода з частотою 2ω використовується як лазерна накачка, тому її можна наближено вважати класичною, тобто $\hat{b} \approx re^{2i\omega t}$. Тоді гамільтоніан взаємодії (46) записується у вигляді

$$\hat{H}_{\rm int} = -i\hbar\frac{\xi}{2}\left(\hat{a}^2e^{-2i\omega t} - \hat{a}^{\dagger 2}e^{2i\omega t}\right), \tag{47}$$

де $\xi = r\chi$. Унітарний оператор еволюції в картині взаємодії (за умови, що основний гамільтоніан задається виразом (8)), який відповідає цьому гамільтоніану, має вигляд

$$\hat{U} = \exp\left[\frac{\xi}{2}\left(\hat{a}^2 - \hat{a}^{\dagger 2}\right)\right] = \exp\left[i\xi\hat{q}\hat{p} + \frac{\xi}{2}\right]. \tag{48}$$

При дії на функцію $\psi(q)$ цей оператор стискає її з коефіцієнтом e^{ξ}, тобто

$$\hat{U}\psi(q) = e^{\frac{\xi}{2}}\psi\left(qe^{\xi}\right). \tag{49}$$

Тобто початковий стан, в якому знаходилась мода $\hat{a}$, при нелінійній взаємодії з полем накачки стискається.

Стискання вакуумного стану світла, використовуючи описане тут параметричне підсилення з перетворенням частоти вниз (parametric down-conversion), було здійснено Кімбле і співавторами в 1986 р. [48], було досягнуто 80—90% редукції шуму від вакуумного рівня. Однак вперше стиснуте світло було отримано Слюшером і співавторами [12] за допомогою методу чотирихвильового змішування в атомах натрію в 1985 р. Цей метод було вперше запропоновано для стиснення світла Юеном і Шапіро у 1979 р. [49].

Стиснуте світло, як за числом фотонів, так і за квадратурою, має пряме практичне застосування в багатьох галузях, де важливо звести до мінімуму шуми. Ми згадаємо лише дві з них. В першу чергу, це стосується ідеї використання стиснутого світла для реєстрації гравітаційних хвиль, вперше оприлюдненої в [50] (для огляду див. [13,47]). В цих експериментах стиснення використовується для реєстрації дуже незначних коливань масивних тіл — приймачів гравітаційного випромінювання. Також стиснуте світло застосовують у квантовій інтерферометрії [51,52], яка дозволяє здійснювати надточні вимірювання фазових зсувів. Ці два приклади доводять практичну важливість явища некласичності квантових станів.

3. Основні властивості квантових систем

Експериментальні процедури, розглянуті в попередньому розділі, демонструють статистичні особливості властиві квантовим системам і не властиві класичним. В цьому розділі увагу буде приділено більш формальному обговоренню некласичності. З попереднього розгляду можна зробити висновок, що це поняття виникає як протиріччя між теорією ймовірностей та спробою описати квантові системи в термінах класичної функції розподілу. Дійсно, для квантової теорії можна побудувати представлення аналогічне гамільтоновому формалізму класичної механіки. Таке представлення часто називають *представленням фазового простору*, і воно є повністю еквівалентним стандартному формалізму квантової теорії.

У представленні фазового простору динамічні змінні, як і в класичній механіці, задаються функціями координат та імпульсів, а стан системи — функцією (квазі)розподілу. Таке представлення дозволяє провести пряме порівняння квантових і класичних систем. Відразу привертають до себе увагу дві відмінності. По-перше, це вже відзначені статистичні особливості квантових систем. В класичній статистичній механіці функція розподілу не може набувати від'ємних значень. Інша особливість — це динамічні влас-

тивості. В представленні фазового простору рівняння руху в квантовій механіці задаються не за допомогою дужки Пуассона, як в класичній механіці, а за допомогою складнішої бінарної операції. Одним з найважливіших результатів в цьому напрямку є твердження про те, що статистичні властивості є наслідком динамічних.

В повній мірі цей результат був усвідомлений ще в 70-х роках минулого століття в роботах Широкова [53] (для огляду див. [54]), в яких було показано що квантова і класична теорії допускають уніфіковане формулювання. Всі відмінності між ними зводяться тільки до визначення двох бінарних операцій: добутку і дужки. Замість звичайного комутативного множення двох функцій в класичній механіці, в квантовій механіці доводиться мати справу з добутком, який називають зірковим (star product). Він відповідає некомутативному множенню двох операторів. Замість звичайної дужки Пуассона в класичній механіці, в квантовій, як вже зазначалося, використовується більш складна конструкція, яка відповідає комутатору двох операторів. Всі інші властивості, в тому числі і статистичні, можуть бути виведені з цих двох операцій.

Крім всього іншого, дане твердження пояснює неспроможність спроб вивести квантову механіку з класичної за допомогою локальних прихованих параметрів. Це твердження також відкидає будь-які теорії, які мають на меті продемонструвати, що порушення нерівностей Белла та інші статистичні особливості квантової теорії можуть випливати з класичного описання. Авторам подібних теорій необхідно, в першу чергу, показати, яким чином дві бінарні операції в класичній механіці перетворюються у відповідні операції в квантовій. Зробити це ще нікому не вдалося, і так виглядає на даний момент, що подібну теорію побудувати неможливо.

3.1. Представлення Вейля—Вігнера—Мояла

Вперше ідею щодо представлення фазового простору було сформульовано в 1928 р. в книзі Вейля [55]. Згідно з цією ідеєю поставимо у відповідність довільній функції $A(p,q)$ на фазовому просторі оператор $\hat{A}$, що діє в гільбертовому просторі станів, за таким правилом:

$$\hat{A} = \int\limits_{-\infty}^{+\infty} A(p,q)\,\hat{\Delta}(p-\hat{p},q-\hat{q})\,\mathrm{d}p\,\mathrm{d}q, \tag{50}$$

де операторна функція $\hat{\Delta}(p-\hat{p},q-\hat{q})$ — деяке операторне узагальнення δ-функції на фазовому просторі, яке має назву оператора густини квазіймовірності. Взагалі кажучи, існує багато варіантів цього оператора, що є наслідком неоднозначності процедури впорядкування координати та імпульсу. Одним з них є так зване симетричне впорядкування. У цьому випадку функцію $A(p,q)$ часто називають *символом Вейля оператора* $\hat{A}$. Найпростіший шлях для означення δ-функції — скористатися фур'є-образом експоненти. Тому для її операторного узагальнення можна записати

$$\hat{\Delta}(p-\hat{p},q-\hat{q}) = \frac{1}{(2\pi)^2}\int\limits_{-\infty}^{+\infty}\hat{D}(Q,P)\,e^{i(Qp-Pq)}\,\mathrm{d}P\,\mathrm{d}Q, \tag{51}$$

де $\hat{D}(Q,P)$ — оператор трансляції на фазовому просторі (20), який є оператором представлення групи Гейзенберга—Вейля [56]. Зараз для позначення елемента фазового простору замість комплексної змінної α ми знов користуємося змінними p та q, див. (3). Відповідно дійсні змінні P та Q визначаються як

$$\beta = \frac{1}{\sqrt{2}}(Q+iP), \tag{52}$$

Оператори $\hat{p}$ та $\hat{q}$ пов'язані з операторами народження та знищення виразом (7).

Наступним логічним кроком є знаходження перетворення оберненого до (50), тобто від оператора до символу Вейля. Щоб його знайти використаємо розклад одиниці

$$\int\limits_{-\infty}^{+\infty}|q\rangle\,\mathrm{d}q\,\langle q| = 1 \tag{53}$$

і таку властивість оператора трансляцій:

$$\hat{D}(Q,P)\,|q\rangle = e^{iP\left(q+\frac{Q}{2}\right)}\,|q+Q\rangle\,. \tag{54}$$

Тепер оператор густини квазіймовірності (51) можна записати у вигляді

$$\hat{\Delta}(p-\hat{p},q-\hat{q}) = \frac{1}{2\pi}\int\limits_{-\infty}^{+\infty}\left|q+\frac{Q}{2}\right\rangle e^{iQp}\mathrm{d}Q\left\langle q-\frac{Q}{2}\right|. \tag{55}$$

Підставивши даний вираз в (50), отримаємо, що довільний оператор виражається через символи Вейля

таким чином:

$$\hat{A} = \frac{1}{2\pi} \int\limits_{-\infty}^{+\infty} \left| q + \frac{Q}{2} \right\rangle A\,(p,q)\; e^{iQp}\,\mathrm{d}Q\,\mathrm{d}p\,\mathrm{d}q \left\langle q - \frac{Q}{2} \right|. \tag{56}$$

Звідси знаходимо вираз для матричних елементів оператора $\hat{A}$,

$$\left\langle q + \frac{Q}{2} \right| \hat{A} \left| q - \frac{Q}{2} \right\rangle = \frac{1}{2\pi} \int\limits_{-\infty}^{+\infty} A\,(p,q)\, e^{iQp} \mathrm{d}p, \tag{57}$$

який , як це можна помітити, є фур'є-образом символу Вейля. Виконавши обернене перетворення Фур'є, отримаємо

$$A(p,q) = \int\limits_{-\infty}^{+\infty} \left\langle q + \frac{Q}{2} \right| \hat{A} \left| q - \frac{Q}{2} \right\rangle e^{-iQp}\,\mathrm{d}Q. \tag{58}$$

Даний вираз є оберненим до (50) і задає перетворення від оператора до його символу Вейля.

Тепер замість операторів можна використовувати c-числові функції, подібно до того, як це робиться в класичній механіці. Відмінність квантової механіки від класичної в даному випадку буде міститися в означенні двох бінарних операцій — добутку і дужки [53, 54, 57]. В класичній механіці це звичайне множення і дужка Пуассона. Для того щоб знайти, чому ці операції відповідають в представлені фазового простору квантової механіки, необхідно розглянути їх аналоги в представлені гільбертового простору — некомутативне множення операторів і комутатор. Вперше така задача була поставлена в роботі фон Неймана [58] в 1931 р., а своє остаточне вирішення вона отримала в роботах Мояла [59] і Гренволда [60].

Розглянемо два оператори $\hat{A}$ і $\hat{B}$, яким відповідають символи Вейля $A\,(p,q)$ і $B\,(p,q)$. Символ Вейля їх добутку $\hat{A}\hat{B}$ позначається як $A\,(p,q) \star B\,(p,q)$, а відповідна операція називається *зірковий добуток* (star-product). Використавши формули (53), (58), для цієї операції можна отримати вираз

$$\star = \exp\left[\frac{i}{2}\left(\overleftarrow{\partial_q}\,\overrightarrow{\partial_p} - \overleftarrow{\partial_p}\,\overrightarrow{\partial_q}\right)\right], \tag{59}$$

де символи $\overleftarrow{\partial_q}$, $\overrightarrow{\partial_q}$, $\overleftarrow{\partial_p}$, $\overrightarrow{\partial_p}$, позначають оператори диференціювання по q та p, що діють на функцію зліва та справа від них. Очевидним фактом є те, що, на відміну від звичайного множення функцій в класичній механіці, ця операція не є комутативною. Знаючи явний вираз для зіркового добутку, легко знайти символ Вейля комутатора двох операторів. Для того щоб мати аналогію з дужкою Пуассона в класичній механіці, розглянемо символ комутатора, поділений на уявну одиницю. Відповідна операція має назву дужки Мояла, для якої [1]

$$\{A(p,q), B(p,q)\}_M =$$

$$= \frac{1}{i}\left[A(p,q) \star B(p,q) - B(p,q) \star A(p,q)\right] =$$

$$= 2A(p,q) \sin\left[\frac{1}{2}\left(\overleftarrow{\partial_q}\,\overrightarrow{\partial_p} - \overleftarrow{\partial_p}\,\overrightarrow{\partial_q}\right)\right] B(p,q). \tag{60}$$

Операція дужки Мояла повністю задає динамічні властивості системи, які визначаються рівнянням Гейзенберга в представлені фазового простору (квантовим рівнянням Гамільтона)

$$\partial_t A(p,q;t) = \{A(p,q;t), H(p,q)\}_M\,, \tag{61}$$

де $H(p,q)$ — символ Вейля гамільтоніана.

З формально-математичної точки зору конструкція зіркового добутку і дужки Мояла задають алгебру динамічних змінних в представлені фазового простору. Однак повне формулювання механіки вимагає ще введення поняття стану [53, 54]. В гільбертовому просторі стан задається оператором густини $\hat{\varrho}$, який, в свою чергу, визначає середнє значення динамічної змінної $\hat{A}$ через співвідношення

$$\langle A \rangle = \mathrm{Tr}\left[\hat{\varrho}\,\hat{A}\right]. \tag{62}$$

Тому можна стверджувати, що стан системи задається лінійним функціоналом, який ставить у відповідність деякій динамічній змінній число. Підставивши в даний враз оператор $\hat{A}$, записаний через перетворення Вейля (50) з врахуванням (51), отримаємо

$$\langle A \rangle = \int\limits_{-\infty}^{+\infty} W(p,q)\, A(p,q)\, \mathrm{d}p\,\mathrm{d}q, \tag{63}$$

[1] Для зіркового добутку і дужки Мояла буде корисно навести відповідні вирази в розмірних змінних, записавши сталу Планка $\hbar$ в явному вигляді: $\star = \exp\left[\frac{i\hbar}{2}\left(\overleftarrow{\partial_q}\,\overrightarrow{\partial_p} - \overleftarrow{\partial_p}\,\overrightarrow{\partial_q}\right)\right]$, $\{A(p,q), B(p,q)\}_M = \frac{2}{\hbar} A(p,q) \sin\left[\frac{\hbar}{2}\left(\overleftarrow{\partial_q}\,\overrightarrow{\partial_p} - \overleftarrow{\partial_p}\,\overrightarrow{\partial_q}\right)\right] B(p,q)$. Вочевидь, в класичній границі, при $\hbar \to 0$, вони переходять у звичайний комутативний добуток двох функцій і дужку Пуассона.

де $W\,(p,q)$ — функція Вігнера, що розглядалася в розділі 2.1. Вирази (62) та (63)в деякому сенсі просто задають скалярний добуток. В цьому розумінні можна говорити про те, що множина станів належить алгебрі, спряженій до алгебри динамічних змінних.

Динаміка системи може задаватися також в шредінгерівському представлені, коли спостережувані не залежать від часу, а функція Вігнера задовольняє рівняння Блоха на фазовому просторі (квантове рівняння Ліувілля)

$$\partial_t W(p,q;t) = \{H(p,q), W(p,q;t)\}_M\,. \tag{64}$$

Однак динамічні властивості не є єдиною відмінністю квантової механіки від класичної. Це видно хоча б з тих міркувань, що для систем з квадратичним гамільтоніаном (наприклад для гармонічного осцилятора) рівняння (61) і (64) не відрізняються від своїх класичних аналогів. Різниця між квантовою і класичною механікою в цьому випадку полягає в тому, що функція розподілу належить різним класам функцій [53, 54, 61]. Наприклад, в класичній механіці не існує фоківського стану з функцією розподілу (22), з тієї причини, що такий стан має від'ємне значення густини квазіймовірності. В той же час в квантовій механіці не існує чисто класичного стану

$$\varrho(p,q) = \delta(p-p_0)\,\delta(q-q_0), \tag{65}$$

оскільки за визначенням такий стан порушує принцип невизначеності. Це є прямим наслідком того факту, що оператор, який відповідає цій функції, не є додатно визначеним, а тому не може бути оператором густини, див. розділ 3.4.

3.2. Когерентні стани

До представлень фазового простору можна підійти дещо з іншого боку. У 1926 р. Шредінгер в своїй відомій роботі [62] розглянув задачу квантової механіки про рух гаусових хвильових пакетів в полі гармонічного осцилятора. Виявилося, що хвильові функції станів не змінюють свою форму з часом, а середні значення їх координат та імпульсів поводять себе класичним чином. Більш того, такі стани мінімізують співвідношення невизначеності. Такі дві властивості дозволили вважати ці стани найбільш близькими до класичних. Так вперше були введені в квантову механіку когерентні стани, які пізніше стали одним з основних інструментів квантової фізики, а особливо квантової оптики. Сучасне розуміння важливості когерентних станів склалося в 60-х роках минулого століття. Слід зазначити, що властивості когерентних станів виявилися дуже багатими, а область застосування надзвичайно широкою. Описання історії та детальний розгляд цього питання можна знайти в літературі (див, наприклад, оглядову статтю [63], монографії і підручники [28–30, 39, 56, 64, 65] і багато інших використаних там джерел).

Когерентні стани $|\alpha\rangle$ — це власні стани оператора знищення, які відповідають комплексному числу α:

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,. \tag{66}$$

Звідси випливає той факт, що параметр α задає для них середні координату та імпульс, тобто

$$\langle q\rangle = \sqrt{2}\,\mathrm{Re}\,\alpha, \tag{67}$$

$$\langle p\rangle = \sqrt{2}\,\mathrm{Im}\,\alpha. \tag{68}$$

Когерентні стани можна отримати також дією на вакуум оператора трансляції (20) (див., наприклад, [56])

$$|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle\,. \tag{69}$$

Іншими словами, когерентні стани можна розглядати як вакуумні стани, але зсунуті в фазовому просторі. Як вже зазначалося, такі стани, точно мінімізують співвідношення невизначеності, тобто для них

$$\langle \Delta q^2\rangle\,\langle \Delta p^2\rangle = \frac{1}{4}. \tag{70}$$

Використовуючи визначення (66), можна отримати вираз для розкладу когерентних станів за фоківськими (власними станами гармонічного осцилятора):

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{+\infty} \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,. \tag{71}$$

Як наслідок, можна зробити важливий висновок про те, що світлове поле, що перебуває у когерентному стані, дає пуасонівську статистику фотовідліків. Іншою важливою властивістю є те, що еволюція в часі когерентного стану зводиться до класичної еволюції параметра α згідно з рівнянням (2).

Функція Вігнера когерентного стану $|\beta\rangle$ являє собою розподіл Гаусса з центром у точці β,

$$W(\alpha) = \frac{2}{\pi} e^{-2|\alpha-\beta|^2}. \tag{72}$$

Тобто з цієї точки зору когерентні стани є класичними. Функція Глаубера—Сударшана (37) когерентного стану записується через δ-функцію,

$$P(\alpha) = \delta(\alpha - \beta). \tag{73}$$

З цього можна зробити висновок, що згідно з напівкласичною теорією фотодетектування саме когерентні стани відповідають чистій монохроматичній хвилі, яку випромінює ідеальний лазер.

Когерентні стани, разом з можливими узагальненнями, є частковим випадком ширшого класу станів, які можуть генерувати неперервні представлення [66]. Загальними властивостями таких станів є переповненість та розклад одиниці,

$$\int\limits_{-\infty}^{+\infty} |\alpha\rangle \, \mathrm{d}\mu(\alpha) \, \langle\alpha| = 1, \tag{74}$$

відносно деякої інтегральної міри $\mathrm{d}\mu(\alpha)$. Для звичайних когерентних станів вона має вигляд

$$\mathrm{d}\mu(\alpha) = \frac{\mathrm{d}^2\alpha}{\pi} = \frac{\mathrm{d}\,(\mathrm{Re}\alpha)\;\mathrm{d}\,(\mathrm{Im}\alpha)}{\pi}. \tag{75}$$

Розклад одиниці є тією визначальною властивістю, яка пов'язує формалізм когерентних станів з формалізмом представлень фазового простору.

3.3. s-параметризовані розподіли

Як вже згадувалося раніше, представлення на фазовому просторі визначене неоднозначно. Це пов'язано з існуванням багатьох способів впорядкування при переході від c-числових функцій до операторів. Особливо слід відзначити еквівалентність таких представлень, тобто незалежність кінцевого результату від використаного представлення. Однак функція квазірозподілу має в кожному окремому випадку свій операційний зміст. Так, функцію Вігнера можна отримати при реконструкції оператора густини методом квантової томографії. Її аналогом є функція розподілу Ліувілля в класичній електродинаміці. В той же час P-функція Глаубера—Сударшана визначає статистику фотовідліків. Її аналогом є знову ж таки функція розподілу Ліувілля, але уже в напівкласичній теорії, де класичне світло взаємодіє з квантовим детектором. В принципі, можно сформулювати велику кількість варіантів представлень на фазовому просторі, однак в квантовій оптиці, крім згаданих раніше двох, широко використовується ще одне представлення для оператора густини. Воно відповідає антинормальному впорядкуванню і має назву Q-функції Хусімі—Кано [67,68].

Розглянемо антинормально впорядкований оператор трансляції

$$\hat{D}_Q(\beta) = e^{-\beta^*\hat{a}} e^{\beta\hat{a}^\dagger}. \tag{76}$$

Йому відповідає характеристична функція

$$\mathcal{C}_Q(\beta) = \mathrm{Tr}\left[\hat{\varrho}\,\hat{D}_Q(\beta)\right]. \tag{77}$$

Відповідна їй функція розподілу

$$Q(\alpha) = \frac{1}{\pi^2} \int\limits_{-\infty}^{+\infty} \mathrm{d}^2\beta \, \mathcal{C}_Q(\beta) \, e^{\alpha\beta^* - \alpha^*\beta} \tag{78}$$

і є Q-функцією Хусімі—Кано. Використавши розклад одиниці (74) і визначення когерентних станів (66), для оператора (77) можно отримати такий вираз:

$$\hat{D}_Q(\beta) = \int\limits_{-\infty}^{+\infty} |\alpha\rangle \, \frac{\mathrm{d}^2\alpha}{\pi} e^{\beta\alpha^* - \beta^*\alpha} \, \langle\alpha|. \tag{79}$$

Комбінуючи цей вираз з (77) та (78), для Q-функції отримаємо

$$Q\,(\alpha) = \frac{1}{\pi} \, \langle\alpha|\,\hat{\varrho}\,|\alpha\rangle. \tag{80}$$

А це означає, що така функція розподілу записується через діагональні матричні елементи оператора густини за когерентними станами. Правильним є також твердження, що оператор густини (як і будь-який інший оператор) однозначно визначається тільки діагональними елементами за когерентними станами, що є наслідком їх переповненого базису. На відміну від функції Вігнера і P-функції, Q-функція завжди додатно визначена. Вона може бути використана для визначення середніх від антинормально впорядкованих величин.

P-функція Глаубера—Сударшана вводиться виразом (37) за допомогою нормально впорядкованого оператора трансляції (35). Для неї справедлива властивість дуальна до (80), а саме виявляється, що за її допомогою оператор густини може бути розкладений за проекторами на когерентні стани (або, що теж саме, за операторами густини когерентних станів)

$$\hat{\varrho} = \int\limits_{-\infty}^{+\infty} |\alpha\rangle \, P\,(\alpha) \, \mathrm{d}^2\alpha \, \langle\alpha|. \tag{81}$$

Щоб довести останній вираз, його необхідно підставити в (36) і зробити комбінацію з (37). Як уже зазначалося, когерентні стани з точки зору напівкласичної теорії фотодетектування можуть розглядатися як аналог класичних хвиль (1), що генеруються ідеальним лазером. З цієї причини вираз (81) ще раз підтверджує той факт, що довільні стани з невід'ємною P-функцією є класичними.

Використавши формулу Кемпбела—Хаусдорфа (див., наприклад, [56, 69]), оператори $\hat{D}(\beta)$, $\hat{D}_Q(\beta)$ та $\hat{D}_P(\beta)$ можуть бути виражені один через одного [56]

$$\hat{D}(\beta) = e^{\frac{|\beta|^2}{2}} \hat{D}_Q(\beta), \tag{82}$$

$$\hat{D}(\beta) = e^{-\frac{|\beta|^2}{2}} \hat{D}_P(\beta). \tag{83}$$

Це дає можливість записати узагальнений вираз для всіх функцій квазірозподілу ймовірностей [70]:

$$P(\alpha; s) = \frac{1}{\pi^2} \int\limits_{-\infty}^{+\infty} \mathrm{d}^2\beta\, \mathcal{C}(\beta)\, e^{\alpha\beta^* - \alpha^*\beta + s\frac{|\beta|^2}{2}}, \tag{84}$$

де $\mathcal{C}(\beta)$ — характеристична функція (19) для симетричного (вейлівського) впорядкування. При $s = -1$ цей розподіл є Q-функцією Хусімі—Кано, при $s = 0$ — функцією Вігнера, а при $s = 1$ — P-функцією Глаубера—Сударшана.

Для Q і P-розподілів корисно навести правила розрахунку середніх значень. Для цього необхідно ввести P та Q (або, як їх ще називають, антивіківські та віківські) символи оператора $\hat{A} - A_P(\alpha)$ та $A_Q(\alpha)$ відповідно, що визначаються умовами аналогічними для P- та Q-функцій,

$$\hat{A} = \int\limits_{-\infty}^{+\infty} |\alpha\rangle\, A_P(\alpha)\, \frac{\mathrm{d}^2\alpha}{\pi}\, \langle\alpha|, \tag{85}$$

$$A_Q(\alpha) = \langle\alpha|\, \hat{A}\, |\alpha\rangle. \tag{86}$$

Підставимо тепер (85) в правило обчислення середніх значень (62) і врахуємо властивість Q-функції (80). Внаслідок цього отримаємо

$$\langle A\rangle = \int\limits_{-\infty}^{+\infty} \mathrm{d}^2\alpha\, A_P(\alpha)\, Q(\alpha). \tag{87}$$

Аналогічно, підставивши (81) в правило обчислень середніх значень (62) і приймаючи до уваги визначення Q-символів оператора (86), отримаємо

$$\langle A\rangle = \int\limits_{-\infty}^{+\infty} \mathrm{d}^2\alpha\, A_Q(\alpha)\, P(\alpha). \tag{88}$$

Таким чином, в даному випадку ми зіткнулися з дуальністю: для обчислення середніх значень в P-представлені необхідно використовувати Q-символ оператора і, навпаки, для обчислення середніх значень в Q-представлені необхідно використовувати P-символ оператора. Як уже зазначалося, правило обчислення середніх значень можна розуміти як скалярний добуток. З цієї причини, за аналогією з векторним простором, динамічні змінні є коваріантними, а стани контрваріантними об'єктами [54, 71].

3.4. Класичні і квантові стани

Коли вже визначено уніфіковані методи опису класичних та квантових станів, можна дати точне математичне визначення поняттю некласичності. Для цього, наслідуючи роботи [53, 54], сформулюємо деяку узагальнену механіку, яка містить у собі класичну і квантову як частинні випадки. Далі ми продемонструємо, що абсолютно всі відмінності між цими механіками заховані у визначенні двох операцій — добутку і дужки від спостережуваних величин. Одним з наслідків цього є той факт, що функція розподілу в кожній з механік належить різним класам. При цьому досить важливим є те що, такий формально-математичний розгляд вказує на спосіб операційного детектування некласичності.

Широковим була запропонована узагальнена динаміка, що складається з таких елементів:[2]

1. C^*-алгебри[3] динамічних змінних $\mathfrak{D}$, що складається зі спостережуваних і їх комплексифікацій.

2. Двох бінарних операцій $\mathfrak{D} \times \mathfrak{D} \mapsto \mathfrak{D}$: добутка $A \circ B$ і дужки $\{A, B\}$.

3. Станів системи, що задаються лінійним *додатним* функціоналом $\langle \cdot, \varrho\rangle : \mathfrak{D} \mapsto \mathbb{C}$, який ставить у від-

[2] З метою спрощення викладу, ми свідомо опустили цілий ряд формальних тверджень. Точніше формулювання можна знайти в оригінальних роботах Ю.М. Широкова [53, 54]

[3] Нагадаємо, що термін C^*-алгебра, означає, що в цій алгебрі задана операція інволюції (спряження) така, що для довільного елемента цієї алгебри $(A^*)^* = A$.

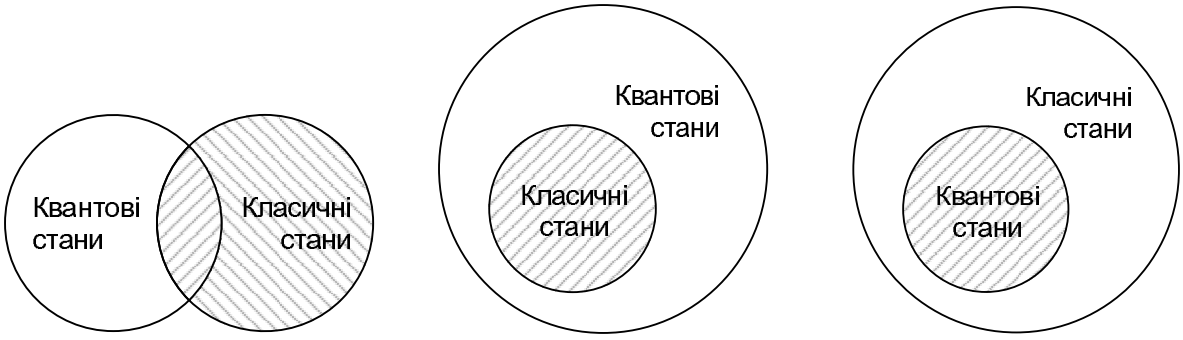

Рис. 5. Схематичне зображення відповідності між множинами класичних та квантових станів: *а* — для представлення Вейля—Вігнера—Мояла; *б* — для представлення Глаубера—Сударшана; *в* — для представлення Хусімі—Кано

повідність кожному елементу A алгебри динамічних змінних комплексне число $\langle A\rangle$ (середнє значення, тобто $\langle A\rangle = \langle A, \varrho\rangle$). Множина станів належить алгебрі, спряженій до $\mathfrak{D}$, на якій задані ті ж самі операції.[4]

4. Гамильтоніан $H \in \mathfrak{D}$, що задає еволюцію системи за допомогою операції дужки рівняннями Гамільтона—Гейзенберга або Ліувілля—Блоха в залежності від картини руху.

Як уже відзначалося, тільки положення 2 (означення добутку і дужки) відрізняє квантову механіку від класичної. В класичній механіці добуток задається простим множенням і дужкою Пуассона, а в квантовій — зірковим добутком і дужкою Мояла. В принципі, можна сказати, що операція дужки 4 повністю задає динамічні властивості системи. Однак у випадку квантової механіки, на відміну від класичної, ці дві алгебраїчні операції пов'язані між собою виразом (60). Саме тому в квантовій механіці як дужка, так і добуток задають динаміку системи.

Статистичні властивості однозначно визначаються множиною станів. При цьому ключовою властивістю функціонала стану, зазначеного в положенні 3, є його додатна визначеність. А це означає, що середнє значення для спостережуваної

$$\mathsf{W} = g^* \circ g, \tag{89}$$

де g — довільний елемент алгебри $\mathfrak{D}$, завжди додатне, тобто

$$\langle \mathsf{W}, \varrho\rangle \geq 0. \tag{90}$$

Іншими словами, очікуване значення спостережуваної, яка задається виразом (89), не може бути від'ємним. Однак це визначення напряму залежить від операції добутку $\circ$, яка різна в квантовій і класичній механіках. Тому простори станів у них різні.

Співвідношення між множинами квантових та класичних станів відображено на рис. 5,*а*. Ці множини різні, але мають деяку спільну область. Стани, які подібні фоківським (з функцією Вігнера, що має від'ємні значення), належать тільки квантовій області, і саме такі стани називаються некласичними. До області перетину належить велика група квантових станів (когерентні, теплові і тому подібне) з усюди невід'ємними значеннями функції Вігнера. Про такі квантові стани прийнято говорити як про стани, що мають класичний аналог. Для некласичних станів завжди існує спостережувана (89), яка визначається за допомогою операції звичайного комутативного множення і така, що її середнє значення є від'ємним. Ця властивість може бути використана для формулювання операційної процедури детектування некласичності. Якщо з експерименту для такої величини випливає, що вона має від'ємні середні значення, то це однозначно вказує на некласичність відповідного стану. Спостережувані W з такими властивостями в літературі прийнято називати індикаторами (witness).

На рис. 5,*а* показана також область класичних станів, для яких не існує квантового аналога. До таких станів належить, наприклад, чистий класичний стан (65) з точно визначеною координатою та імпульсом. Для таких станів існує така спостережувана (89), визначена за допомогою зіркового добутку (59), що її середнє значення буде від'ємним. Однак дана властивість має чисто формальне значення, оскільки насправді в природі таких неквантових станів, напевно, просто не існує. Класична механіка є наближенням квантової механіки, але не навпаки. Тому реально існують тільки стани, що належать до квантової області. А з класичних станів в природі можуть реалі-

[4] Пор. аналог з коваріантними та контрваріантними (кет та бра) векторами в лінійному просторі

зуватися тільки ті, що належать одночасно обом областям. Одним з наслідків спостереження від'ємного значення квантової додатної величини, якби це було можливим, було б порушення співвідношення невизначеності. На сьогодні даних про такі експерименти не існує, як не існує теорій, що описують квантову механіку на основі класичної.

Некласичність квантових станів є операційним поняттям, і говорити про неї можна тільки в зв'язку з певним експериментом. Розбиття області станів на класичну і квантову, що зображено на рис. 5,*а*, відноситься до представлення Вейля—Вігнера—Мояла і може бути зіставлене з експериментами з квантової томографії. У даному випадку некласичність виникає як протиріччя з результатами класичної електродинаміки. Однак, як було показано, некласичність можна інтерпретувати і ширше, як протиріччя експериментальних даних з напівкласичною теорією фотодетектування. Для описання таких некласичних станів необхідно використовувати представлення Глаубера—Сударшана, а для спостережуваних відповідно віківські Q-символи.

Зірковий добуток в цьому представлені відрізняється від моялівського (59), див. [72], відповідно відрізняється розміщення областей квантових і класичних станів, рис. 5,*б*. Тепер множина класичних станів повністю міститься у множині квантових станів. З цієї точки зору в класичній механіці не існує станів, які не могли б реалізуватися в квантовій механіці. В той же час множина некласичних станів суттєво розширена в порівнянні з випадком представлення Вейля—Вігнера—Мояла. Концепція спостережуваної-індикатора (witness) виявляється тут найбільш плідною, оскільки пряме відновлення P-функції в багатьох випадках не можливе в силу її сингулярності. Тому для того, щоб визначити некласичність даного типу, необхідно експериментально підтвердити наявність від'ємних значень для відповідного індикатора [42–45].

Таким чином, некласичність або класичність в багатьох випадках залежить від взаємного розміщення класичних і квантових множин станів. Наслідуючи Широкова [53, 54], можна сказати, що вони залежать від взаємного розміщення класичної і квантової алгебри динамічних змінних. Кожному такому розміщенню, в принципі, повинна відповідати деяка відповідна операційна процедура. Для представлення Хусімі—Кано, наприклад, некласичність взагалі не можливо виявити ніякою операційною процедурою, оскільки відповідна квантова алгебра повністю лежить в класичній області, див. рис. 5,*в*. Тобто ситуація тут прямо протилежна випадку представлення Глаубера—Сударшана.

Таким чином, квантовий стан будемо називати некласичним відносно деякого представлення квантової механіки, якщо він не належить до множини класичних станів за відповідного даному представленню розташування класичної і квантової алгебр динамічних змінних. При цьому кожне таке розташування повинне відповідати деякій операційній процедурі. Можна також довести, що, якщо деякий стан є некласичним відносно представлення, що відповідає параметру s, то він є також некласичним для будь-якого іншого s', такого що $s' < s$. Зокрема, всі стани некласичні відносно представлення Вейля—Вігнера—Мояла, некласичні й відносно представлення Глаубера—Сударшана. Звідси маємо, що всі стани, некласичні відносно будь-якого представлення, некласичні і відносно P-функції (тобто для $s = 1$). Значення параметра s, за якого відповідна функція квазірозподілу стає додатно визначеною, можна використовувати як міру некласичності [24]. Таким чином, некласичність відносно P-представлення Глаубера—Сударшана може розглядатися як універсальна, тобто така, що перекриває всі можливі області її прояву. Більш того, як буде показано в наступному розділі, це визначення поширюється і на досить специфічний випадок — переплутування.

В кінці цього розділу коротко зупинимося ще на деяких підходах до некласичності квантових станів. В першу чергу, необхідно відзначити ймовірнісне представлення квантової механіки, запропоноване В.І. Манько із співавторами [73]. Основна ідея їхнього розгляду полягає в тому, щоб описати стан не функцією квазірозподілу і не оператором густини, а набором істинних розподілів ймовірності за квадратурами. В такому представленні класичні і квантові стани відрізняються властивостями цих наборів (томограмами). Дійсно, далеко не кожній томограмі відповідає двовимірна додатно визначена функція розподілу у фазовому просторі.

Інший підхід, запропонований Л.М. Йохансеном та А. Льюісом [74], розглядає некласичність як протиріччя між квантовою і класичною теоріями слабких вимірювань [75]. З цієї точки зору, навіть термальні і когерентні стани можуть проявляти некласичні властивості [76]. Тому такий тип некласичності є більш сильним ніж некласичність відносно P-функції.

4. Переплутані стани

Як зазначалося у Вступі, історично склалося так, що явище переплутування (entanglement) стало першим широко обговорюваним прикладом некласичності квантових станів. У своїй знаменитій роботі у 1935 р. [5] Ейнштейн, Подольський та Розен (ЕПР) запропонували уявний експеримент (gedanken experiment), який на їхню думку, повинен був виявити неповноту квантової теорії. Коротко відтворимо їх аргументи. Нехай система, що складається з двох частинок, приготована у власному стані оператора загального імпульсу $\hat{p}_o = \hat{p}_1 + \hat{p}_2$ та відносної відстані між ними $\hat{q}_o = \hat{q}_1 - \hat{q}_2$,

$$|p_o, q_o\rangle = \frac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{+\infty} \mathrm{d}q\, e^{ip_o q}\, |q\rangle \otimes |q + q_o\rangle\,. \qquad (91)$$

Відмітимо, що оператори $\hat{q}_o$ та $\hat{p}_o$ комутують, тому стан (91) не входить у протиріччя з квантовою теорією. Також припускається, що відстань q_o між частинками досить велика, взаємодія між ними відсутня і будь-які маніпуляції з однією з них не можуть ніяким чином впливати на іншу.

Якщо тепер виміряти координату q першої частинки, то можна з упевненістю сказати, що координата другої частинки дорівнює $q + q_o$. Оскільки при цьому ніяких маніпуляцій над другою частинкою не проводилося, то, як стверджують ЕПР, існує елемент фізичної реальності, який відповідає значенню координати другої частинки. А це означає, що координату цієї частинки можна передбачити точно і, що важливіше, без будь-якої взаємодії з нею. Однак зазначений стан (91) записується також через власні вектори операторів імпульсів:

$$|p_o, q_o\rangle = \frac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{+\infty} \mathrm{d}p\, e^{-iq_o(p_o - p)}\, |p\rangle \otimes |p_o - p\rangle\,. \qquad (92)$$

А звідси виходить, що так само можна визначити точно імпульс першої частинки p, і можна з впевненістю зробити висновок, що імпульс другої частинки дорівнює $p_o - p$. Таким чином, на думку ЕПР, для другої частинки об'єктивно існують точні значення як координати, так і імпульсу. А це протирічить принципу невизначеності. Тому описання фізичної реальності на основі квантової механіки, на думку авторів, є не повним.

Хоч аргументи ЕПР на даний час визнано незадовільними, саме вони стали вирішальним фактором, який поклав початок обговоренню основних принципів квантової фізики. В першу чергу, необхідно відзначити аналіз Н. Бора [7]. Не піддаючи сумніву математичний бік питання він, тим не менше, вказує на те, що у висновках ЕПР достатнім чином не врахований принцип доповнення, який з однаковим успіхом може бути застосований як до систем з одним ступенем вільності, так і до випадку, що розглядається. Деякої однозначності в цьому питанні вдалося досягнути тільки Дж. Беллу у 1964 р. [9]. Він показав, що, якщо аргументи ЕПР дійсно правильні, то завжди виконуються певні нерівності. І тільки в 1980 р. правильність аргументів Бора було підтверджено експериментально Аспектом із співавторами [10].

В описаному вище прикладі можна уявити собі двох спостерігачів, кожен з яких контролює по одній частинці. Після того, як перший спостерігач визначив координату своєї частинки, значення координати другої частинки повністю визначене також. На протязі досить короткого часу (меншого, ніж необхідно для проходження сигналу між двома частинками) другий спостерігач вимірює імпульс. Якщо Н. Бор правий, а разом з ним і ортодоксальна квантова механіка, то результати обох вимірювань будуть знаходитися в деякій специфічній кореляції, оскільки перший спостерігач "нелокальним чином" змінив стан другої частинки. Якщо ж праві ЕПР, то такого впливу не буде і кореляції будуть мати тільки "класичний" вигляд.

4.1. Сепарабельність і несепарабельність

Сам собою факт наявності "надсвітлових кореляцій" ще ніяким чином не визначає специфіку квантових станів. Подібні кореляції існують і в класичній фізиці, і вони не приводять ні до можливостей надсвітлових комунікацій, ні, тим більше, до порушення принципу причинності. Часто наводять такий приклад (див., наприклад, [78]). Нехай ми маємо закриту коробку з білою і чорною кульками. Після старанного перемішування розділимо цю коробку (не заглядаючи туди) на дві частини, в кожній з яких знаходиться по одній кульці. Тепер два спостерігачі, взявши по одній половинці коробки розійдуться на велику відстань. В деякий момент часу вони відкривають кожен свою половину. Якщо перший спостерігач виявить, наприклад, чорну кульку, то він точно знає, що у другого біла, і навпаки. В цьому випадку присутні "надсвітлові кореляції", однак ніякої передачі інформації при цьому, природно, не відбувається.

Квантові кореляції відрізняються від класичних, оскільки, як було показано в попередніх розділах,

суттєво відрізняються відповідні функції розподілу ймовірностей. Однак і в цьому випадку надсвітлова комунікація не є можливою, і це було показано Буссі [79]. В принципі, в основу доведення даного факту може бути покладено незалежність відповідного протоколу передачі інформації від визначення бінарних операцій множення і дужки на алгебрі динамічних змінних.[5] Тим не менш, квантові кореляції, що є основою явища переплутування, є ключовим ресурсом в квантовій інформації (див., наприклад, [78,81–83]), і тому становлять широкий інтерес.

Розглянемо узагальнення явища переплутування на випадок змішаних станів, запропонований в роботі Вернера [84]. Стан системи з двома ступенями вільності буде повністю не скорельованим, якщо його оператор густини набуває вигляду

$$\hat{\varrho} = \hat{\varrho}^{(1)} \otimes \hat{\varrho}^{(2)}, \tag{93}$$

де $\hat{\varrho}^{(1)}$ и $\hat{\varrho}^{(2)}$ — оператори густини першої та другої підсистем. Припустимо тепер, що в результаті деякого процесу з ймовірністю p_k для першої підсистеми генерується стан $\hat{\varrho}_k^{(1)}$, а для другої в той же час — стан $\hat{\varrho}_k^{(2)}$. При цьому, звичайно,

$$\sum_k p_k = 1, \tag{94}$$

$$p_k \geq 0. \tag{95}$$

Тоді оператор густини системи може бути записаний як

$$\hat{\varrho} = \sum_k p_k \, \hat{\varrho}_k^{(1)} \otimes \hat{\varrho}_k^{(2)}, \tag{96}$$

що часто називають *випуклою комбінацією* станів. Такий стан містить в собі тільки класичні кореляції між різними ступенями вільності і називається *сепарабельним*. Якщо стан не може бути представлений у вигляді (96), то він називається *несепарабельним*.

Несепарабельні стани характеризуються наявністю некласичних кореляцій і являють собою узагальнення чистих переплутаних станів, які були розглянуті ЕПР. Дуже важливо те, що несепарабельність є тільки частинним випадком некласичності у термінах від'ємних значень P-функції. Іншими словами, P-функція несепарабельного стану не є додатно визначеною. Однак протилежне твердження, взагалі кажучи, не правильне. Дійсно, згідно з (81) оператор густини для системи з двома ступенями вільності може бути записаний як

$$\hat{\varrho} = \int_{-\infty}^{+\infty} \mathrm{d}^2\alpha \, \mathrm{d}^2\beta \, P(\alpha,\beta) \, |\alpha\rangle \langle\alpha| \otimes |\beta\rangle \langle\beta| \, . \tag{97}$$

Якщо $P(\alpha,\beta)$ додатно визначена, то даний вираз може бути переписаний у вигляді

$$\hat{\varrho} = \int_{-\infty}^{+\infty} \mathrm{d}^2\alpha \, P(\alpha) \, |\alpha\rangle \langle\alpha| \otimes \hat{\varrho}(\alpha) \, , \tag{98}$$

де

$$P(\alpha) = \int_{-\infty}^{+\infty} \mathrm{d}^2\beta \, P(\alpha,\beta) \tag{99}$$

— редукований вираз P-функції для першої підсистеми, який є додатним, оскільки додатною є величина $P(\alpha,\beta)$;

$$\hat{\varrho}(\alpha) = P^{-1}(\alpha) \int_{-\infty}^{+\infty} \mathrm{d}^2\beta \, P(\alpha,\beta) \, |\beta\rangle \langle\beta| \tag{100}$$

— є додатним нормованим оператором густини деякого стану для другої підсистеми. Таким чином, вираз (98) можна розглядати як континуальний варіант випуклої комбінації (96), а тому стан з додатною P-функцією завжди сепарабельний. Несепарабельні стани, за визначенням, не можуть бути розкладені ні в які випуклі комбінації станів, в тому числі і в (98), а як наслідок їх P-функції не є додатно визначеними.

З наведеного вище обговорення можна зробити висновок, що для систем з двома ступенями вільності джерелом некласичності відносно P-функції може бути як несепарабельність станів, так і некласичність окремих складових елементів комбінації (96). Як наслідок, явище переплутування повністю вписується в загальне визначення некласичності. Однак при цьому досить непростим виявилося формулювання операційних критеріїв, які дозволили б судити тільки про несепарабельність, а не про некласичність в цілому. На даний час в загальному вигляді ця задача ще не розв'язана, а тому доводиться використовувати тільки достатні умови несепарабельності.

[5] В літературі можна зустріти обговорення інших протоколів, див. наприклад [80].

4.2. Критерій Переса—Городецького

Одна з найбільш потужних достатніх умов несепарабельності була запропонована незалежно Пересом [85] та Городецькими [86]. Підхід ґрунтується на ідеї часткового транспонування оператора густини. Для початку розглянемо випадок одного ступеня вільності. Якщо $\hat{\varrho}$ — оператор густини певного стану (тобто він є принаймні додатно визначений), то транспонований оператор $\hat{\varrho}^{\mathrm{T}}$ є також оператором густини деякого стану. Нагадаємо, що операція транспонування не залежить від представлення і в будь-якому базисі визначається як

$$\langle n|\,\hat{\varrho}^{\mathrm{T}}\,|m\rangle = \langle m|\,\hat{\varrho}\,|n\rangle\,. \tag{101}$$

Неважко довести, що у представленні фазового простору операція транспонування виглядає просто як заміна $\alpha \mapsto \alpha^*$, або, що теж саме, $p \mapsto -p$, тобто

$$P^{\mathrm{T}}(\alpha; s) = P(\alpha^*; s)\,. \tag{102}$$

Тепер розглянемо випадок двох ступенів вільності. Для сепарабельного стану, що може бути заданий опуклою комбінацією (96), виконаємо транспонування відносно лише одного ступеня вільності

$$\hat{\varrho}^{\mathrm{PT}} = \sum_k p_k\,\hat{\varrho}_k^{(1)\mathrm{T}} \otimes \hat{\varrho}_k^{(2)}. \tag{103}$$

Цю операцію прийнято називати частковим транспонуванням. Оскільки кожний транспонований оператор $\hat{\varrho}_k^{(1)\mathrm{T}}$ є додатно визначеним оператором густини, то частково транспонований оператор густини $\hat{\varrho}^{\mathrm{PT}}$ також буде додатно визначеним оператором густини деякого іншого стану. Якщо ж стан не є сепарабельним, то частково транспонований оператор густини може й не бути додатно визначеним. Таким чином, критерій Переса—Городецького встановлює достатню умову несепарабельності: *якщо частково транспонований оператор не є додатно визначеним, то відповідний стан є несапарабельним.*

Проте обернене твердження не є, взагалі кажучи, правильним. Існують несепарабельні стани з додатно визначеним частковим транспонуванням. Задача визначення необхідної і достатньої умови несепарабельності в найзагальнішому випадку не розв'язана й досі. Можна без перебільшення сказати, що вона є однією з найбільш інтригуючих проблем сучасної квантової оптики та квантової інформатики.

З формальної точки зору ця задача виглядає таким чином. Нехай $\mathcal{S}$ — це деякий лінійний супероператор (тобто оператор, що діє на просторі операторів), що зберігає додатну визначеність оператора густини одномодового стану. Транспонування є частинним випадком такого супероператора. Якщо стан двомодової системи є сепарабельним, то для будь-якого супероператора $\mathcal{S}$, оператор

$$(1 \otimes \mathcal{S})\hat{\varrho}, \tag{104}$$

що є результатом дії $\mathcal{S}$ лише на одну моду, також буде додатно визначеним. Для несепарабельного стану завжди має існувати такий супероператор $\mathcal{S}$, щоб оператор (104) не був би додатно визначеним. Задача полягає в знаходженні таких супероператорів. На жаль, в загальному випадку з них на сьогодні відомий лише оператор транспонування. Проте для скінченновимірних гільбертових просторів парної вимірності загальний розв'язок цієї задачі нещодавно був знайдений Бройером [87].

В принципі, задача про супероператор $\mathcal{S}$ може бути переформульована в термінах індикатора переплутування (entanglement witness), подібно до того, як це робиться для інших типів некласичності (див. розділ 3.). Дійсно, умова додатної визначеності оператора (104) означає, що існує такий індикатор

$$\hat{\mathsf{W}} = \hat{g}^{\dagger}\hat{g}, \tag{105}$$

означений за допомогою звичайного квантового добутку, що

$$\mathrm{Tr}\left[\hat{\mathsf{W}}\,(1 \otimes \mathcal{S})\hat{\varrho}\right] = \langle \mathsf{W}, (1 \otimes \mathcal{S})\varrho\rangle \geq 0. \tag{106}$$

До операції обчислення середнього ми можемо застосувати такі ж правила, як і до звичайного скалярного добутку. Тому, якщо супероператор $(1 \otimes \mathcal{S}^{\dagger})$ є спряженим до (104), то умова (106) записується у вигляді

$$\mathrm{Tr}\left[\hat{\mathsf{W}}_{\mathrm{E}}\,\hat{\varrho}\right] = \langle \mathsf{W}_{\mathrm{E}}, \varrho\rangle \geq 0, \tag{107}$$

де

$$\hat{\mathsf{W}}_{\mathrm{E}} = (1 \otimes \mathcal{S}^{\dagger})\hat{\mathsf{W}} \tag{108}$$

є індикатором переплутування. Тепер умовою несепарабельності є існування такої спостережуваної (108), середнє значення якої є від'ємним (де $\hat{\mathsf{W}}$ є додатно визначеною величиною (105)). Тобто нерівність (107) для таких станів має порушуватися. У частинному випадку, коли супероператор $\mathcal{S}$ є транспонуванням, спряжений до нього оператор $\mathcal{S}^{\dagger}$ є також транспонуванням. Тому для визначення несепарабельних станів, що мають від'ємне часткове транспонування, достатньо знайти таку спостережувану

$$\hat{\mathsf{W}}_{\mathrm{PT}} = \left(\hat{g}^{\dagger}\hat{g}\right)^{\mathrm{PT}}, \tag{109}$$

середнє значення якої було б від'ємним. Ця властивість може бути використана для застосування критерію Переса—Городецького на експерименті (див. розділ 5.4).

5. Експериментальне спостереження некласичності

Як уже зазначалося, явище некласичності є операційним поняттям і завжди пов'язане з деякою експериментальною процедурою. Спостереження від'ємних значень функції Вігнера, стискання статистики фотовідліків є наслідками більш загальної властивості — наявності від'ємних значень P-функції. Далеко не завжди стани, що мають від'ємні значення P-функції, мають також від'ємну функцію Вігнера або характеризуються від'ємним значенням надлишкового шуму для числа фотонів або квадратур. З іншого боку, пряма реконструкція P-функції на експерименті не є можливою внаслідок її сингулярності. Тут виявляється корисним правило (90). У нашому випадку воно полягає в тому, що повинен існувати такий індикатор (witness) з віківським Q-символом

$$\mathsf{W}(\alpha) = |g(\alpha)|^2, \tag{110}$$

що його середнє значення було б від'ємною величиною, тобто

$$\int_{-\infty}^{+\infty} \mathrm{d}^2\alpha\, P(\alpha)\, \mathsf{W}(\alpha) < 0. \tag{111}$$

Якщо такий індикатор вдалося знайти і експериментально підтвердити негативність його середнього значення, то з упевненістю можна стверджувати, що даний стан є некласичним відносно представлення Глаубера—Сударшана.

В деяких випадках вираз (111) зручно переписати в термінах характеристичної функції (36)

$$\int_{-\infty}^{+\infty} \mathrm{d}^2\alpha\, \mathrm{d}^2\beta\, \mathcal{C}_P(\alpha-\beta)\, f^*(\alpha)\, f(\beta) < 0, \tag{112}$$

де $f(\beta)$ — фур'є-образ $g(\alpha)$. У даному випадку некласичність проявляється як порушення добре відомого в теорії ймовірностей критерію Бохнера [88], який визначає необхідні та достатні умови для характеристичної функції всюди невід'ємного розподілу.

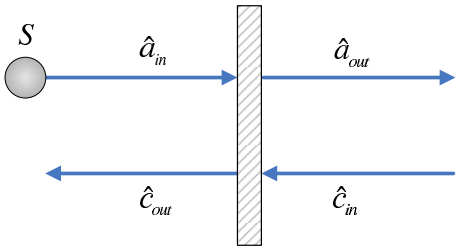

Рис. 6. Діелектрична пластинка як найпростіший приклад застосування формалізму входу-виходу

5.1. Реалістичні умови експерименту

При спостереженні ефектів некласичності досить серйозні перешкоди з'являються через явища декогерентності, зумовлені впливом неконтрольованої взаємодії системи, що досліджується, з деяким оточенням [89] (див. також [78]). Результатом цього впливу є зникнення недіагональних елементів матриці густини, тобто перетворення квантової суперпозиції станів у статистичну суміш. У випадку оптичних полів декогерентність зумовлена поглинанням та розсіюванням, які, як правило, є лінійними процесами.

Для опису таких процесів можна скористатися формалізмом входу-виходу (див. [90]). Нехай $\hat{a}_{\rm in}$ і $\hat{a}_{\rm out}$ — оператори моди електромагнітного поля відповідно до і після взаємодії, а $\hat{c}_{\rm in}$ — оператор системи, що поглинає і розсіює. Всі вони задовольняють стандартні комутаційні співвідношення для бозонів (6), а оператори $\hat{a}_{\rm in}$ та $\hat{c}_{\rm in}$, до того ж, комутують між собою. З точністю до фаз лінійна еволюція операторів поля у найзагальнішому вигляді може бути записана як

$$\hat{a}_{\rm out} = \sqrt{\eta}\, \hat{a}_{\rm in} + \sqrt{1-\eta}\, \hat{c}_{\rm in}, \tag{113}$$

де величина $0 \le \eta \le 1$ називається ефективністю. Вираз (113) носить назву співвідношення входу-виходу. В залежності від системи, що досліджується, це співвідношення може мати різний фізичний зміст.

Найпростішим прикладом є звичайна діелектрична пластинка без поглинання, див. рис. 6. Якщо її показник заломлення відмінний від показника заломлення повітря, то мода світла $\hat{a}_{\rm in}$, падаючи на таку пластинку, проходить тільки частково і перетворюється в моду $\hat{a}_{\rm out}$. Друга частина світлової хвилі відіб'ється (іншими словами, розсіється) в моду $\hat{c}_{\rm out}$. Мода $\hat{c}_{\rm in}$ при цьому є розсіюючою (хоча вона і знаходилася в вакуумному стані). Якщо T — коефіцієнт проходження пластинки, то ефективність в цьому випадку можна визначити як

$$\eta = |T|^2 \tag{114}$$

(див., наприклад, [30]). Для складнішого випадку, коли в пластинці відбувається ще й поглинання, розгляд цієї задачі можна знайти в роботі [30, 91]. Подібні співвідношення описують і втрати поля слабкої інтенсивності в хвилеводах, що є критично важливою проблемою при реалізації схем квантової криптографії.

Інший приклад можна навести з квантової електродинаміки резонаторів [14, 92] — однієї з перспективних галузей, в якій на даний час запропонована та успішно реалізована велика кількість схем генерації і маніпуляції квантовими станами світла і речовини. Сучасна експериментальна техніка дозволяє реалізувати досить сильну взаємодію між однією з мод високодобротного резонатора і атомом, що перебуває всередині нього. Маніпулюючи атомом за допомогою зовнішнього лазера, можна створити практично всі наперед задані стани поля (див., наприклад, [93]). Якщо одне з дзеркал резонатора зроблене частково прозорим, то такий стан можна транслювати назовні для подальшого використання, наприклад в квантових мережах [94]. Основна проблема при цьому полягає в тому, що втрати на поглинання і розсіювання в таких резонаторах хоч і дуже малі, але все ж за порядком величин порівнянні з втратами на звичайний вихід [95]. Тому ефективність такого процесу звичайно нижча за $0,5$. Відповідне для цього випадку співвідношення входу-виходу і вираз для ефективності було отримано в роботах [30, 96].

Для того щоб відповісти на питання, що відбувається з квантовим станом світла у такому процесі, співвідношення входу-виходу (113) необхідно переписати на мові оператора густини, тобто в картині руху Шредінгера. Зробити це найпростіше в представлені Глаубера—Сударшана. Підставивши (113) у вираз для характеристичної функції (36) P-розподілу Глаубера—Сударшана і припустивши, що в початковий момент часу стани системи і оточення є повністю не скорельованими, тобто

$$\hat{\rho} = \hat{\rho}_{\rm in} \otimes \hat{\rho}_{\rm bath}, \tag{115}$$

отримаємо

$$\mathcal{C}_P^{\rm out}(\beta) = \mathcal{C}_P^{\rm in}(\beta\sqrt{\eta})\,\mathcal{C}_P^{\rm bath}(\beta\sqrt{1-\eta}). \tag{116}$$

В даному виразі $\mathcal{C}_P^{\rm out}(\beta)$ і $\mathcal{C}_P^{\rm in}(\beta)$ — характеристичні функції відповідно вхідного та вихідного полів, $\mathcal{C}_P^{\rm bath}(\beta)$ — характеристична функція оточення до взаємодії. В оптичній області спектра при кімнатній температурі теплових (планківських) фотонів дуже мало. Тому з високою точністю стан оточення до взаємодії можна вважати вакуумним, для якого

$$\mathcal{C}_P^{\rm bath}(\beta) = 1. \tag{117}$$

У мікрохвильовій ділянці спектра в загальному випадку це не так, див., наприклад [25]. Якщо тепер застосувати обернене перетворення Фур'є до (116) з врахуванням (117), отримаємо, що для оптичної ділянки спектра P-розподіл Глаубера—Сударшана до і після взаємодії зв'язані таким співвідношенням:

$$P_{\rm out}(\alpha) = \frac{1}{\eta}\, P_{\rm in}\left(\frac{\alpha}{\sqrt{\eta}}\right). \tag{118}$$

Звідси, як частинний випадок, можна отримати вираз (31) для оператора густини однофотонного фоківського стану "з шумом".

Зі співвідношення (118) випливає дуже важливий висновок про те, що в оптичній ділянці спектра стани, що є некласичними відносно представлення Глаубера—Сударшана, залишаються такими і після взаємодії з оточенням. Дане твердження не є правильним для інших типів некласичності. Наприклад, для некласичності відносно представлення Вейля—Вігнера—Мояла або для переплутування. В останньому випадку, вплив оточення є найбільш суттєвим, що створює дуже серйозні проблеми для застосувань, що пов'язані з квантовою інформацією.

Дію, повністю аналогічну декогерентності на кінцевий результат, виявляє також неідеальність фотодетекторів. При розгляді формул Манделя (27), (28), (34), (38) припускалося, що як в квантовому, так і в класичному випадках середня кількість фотовідліків дорівнює інтенсивності, див. (25). Насправді ж в більшості випадків це далеко не так. По-перше, з детектором може не встигнути провзаємодіяти весь хвильовий пакет, що пов'язано із скінченним часом детектування. По-друге, далеко не всі фотони, що попали на детектор, можуть бути поглинутими. Частина з них відіб'ється, а частина пройде через детектор і тому подібне. Особливо це проявляється при детектуванні станів з малою кількістю фотонів. В той же час для багатофотонних станів ефективність може досягати $0,9$ і більше (див., наприклад, [97]).

Цей процес еквівалентний розсіянню світла на деякій світлоподільній пластинці ще до того, як воно попадає на ідеальний фотодетектор, див. рис. 7. Тому замість того, щоб розглядати неідеальний фотодетектор, можна розглянути квантовий стан, який попадає в ідеальний фотодетектор, після втрат згідно з (118). Підставивши цей вираз в формулу Манделя (38), провівши просту заміну змінних та відкинувши при цьому в кінцевому виразі індекс out, отримаємо, що для

ідеального фотодетектування ймовірність фотовідліку пов'язана з P-розподілом Глаубера—Сударшана таким чином:

$$p_n = \int\limits_{-\infty}^{+\infty} \mathrm{d}^2\alpha\, P(\alpha)\, \frac{\eta^n\, |\alpha|^{2n}}{n!} e^{-\eta|\alpha|^2}. \tag{119}$$

Останню формулу можна переписати в операторному вигляді

$$p_n = \mathrm{Tr}\left[\hat{\varrho} : \frac{\left(\eta \hat{a}^\dagger \hat{a}\right)^n}{n!}\, e^{-\eta \hat{a}^\dagger \hat{a}} :\right]. \tag{120}$$

Ці вирази і є формулами Манделя для неідеального детектування.

5.2. Вимірювання квадратур

Згідно з виразами (111) та (112) для детектування некласичності відносно представлення Глаубера—Сударшана необхідно експериментально підтвердити від'ємність середнього значення індикатора типу (110). Процедура гомодинного детектування, розглянута в розділі 2.1, дозволяє відносно просто вимірювати квадратури. Тому, перш за все, розглянемо схему, запропоновану Фогелем і Ріхтером [42,43], в якій середнє значення деякого індикатора може бути визначене з вимірювання квадратур.

Використавши правило (112), виберемо функцію $f(\alpha)$ у вигляді

$$f(\alpha) = \sum_k \xi_k\, \delta(\alpha - \alpha_k), \tag{121}$$

де ξ_k і α_k — деякі комплексні числа. Звідси виходить, що стани будуть некласичними тільки тоді, якщо для деяких ξ_k та α_k нерівність

$$\sum_{k,l} \mathcal{C}_P\left(\alpha_k - \alpha_l\right) \xi_k \xi_l^* \geq 0 \tag{122}$$

порушується. Фактично, нерівність (122) еквівалентна дискретній формі критерію Бохнера [88], що встановлює необхідні і достатні умови для характеристичної функції додатно визначеного розподілу. З формули (36) видно, що величини $\mathcal{C}_P\left(\alpha_k - \alpha_l\right)$ є середніми від функцій квадратур і тому можуть бути виміряні, наприклад, методом гомодинного детектування.

Нерівність (122) можна розглядати і як умову додатної визначеності квадратичної форми, що задана матрицею $\mathcal{C}_{k,l} = \mathcal{C}_P\left(\alpha_k - \alpha_l\right)$, для класичного стану. Використавши відомий з лінійної алгебри критерій

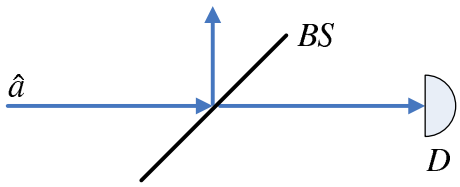

Рис. 7. Ефективна схема неідеального фотодетектування: D — ідеальний детектор, BS — светлоподільна пластинка, коефіцієнт проходження якої пов'язаний з ефективністю детектування співвідношенням (114)

Сільвестра (див., наприклад, [98]), можна зробити висновок, що для класичного стану всі детермінанти вигляду (мінори матриці $\mathcal{C}_{k,l}$)

$$\begin{vmatrix} 1 & \mathcal{C}_{1,2} & \ldots & \mathcal{C}_{1,n} \\ \mathcal{C}_{1,2}^* & 1 & \ldots & \mathcal{C}_{2,n} \\ \ldots & \ldots & \ldots & \ldots \\ \mathcal{C}_{1,n}^* & \mathcal{C}_{2,n}^* & \ldots & 1 \end{vmatrix} \geq 0. \tag{123}$$

Якщо хоч один детермінант для деякого набору значень α_k від'ємний, то відповідний стан є некласичним. Детермінант першого порядку дає тривіальну нерівність $1 \geq 0$. Якщо тепер вибрати $\alpha_1 = 0$ і покласти $\alpha_2 = \alpha$, то детермінант другого порядку дає нерівність

$$\left|\mathcal{C}_P\left(\alpha\right)\right|^2 \leq 1. \tag{124}$$

Для певного класу квантових станів ця нерівність порушується, і тоді можна говорити, що відповідний стан проявляє некласичність першого порядку. Це відноситься до "зашумленого" фоківського стану (31), для якого характеристична функція набуває вигляду

$$\mathcal{C}_P\left(\alpha\right) = 1 - \eta\left|\alpha\right|^2. \tag{125}$$

Очевидно, що для $|\alpha|^2 > 2/\eta$ нерівність (124) порушується. Тим не менш, існують такі некласичні стани, для яких нерівність (124) не порушується, тоді необхідно перевірити на від'ємність третій, четвертий і т. д. детермінанти. В результаті отримаємо ієрархію умов некласичності [43].

Перевірка фоківського стану "з шумом" (31) на некласичність з використанням критерію Фогеля—Ріхтера була проведена Львовським і Шапіро [45]. Схему цього експерименту зображено на рис. 8. На нелінійний кристал падає лазерне поле накачки, і в результаті параметричного перетворення частоти вниз (parametric down conversion) сигнал поділяєть-

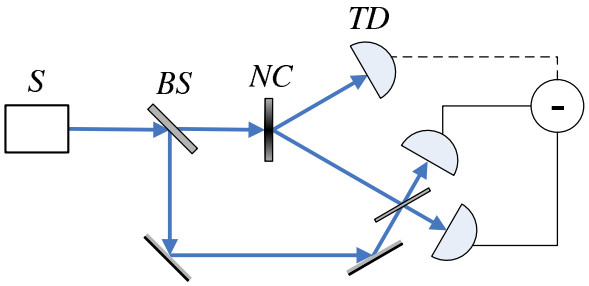

Рис. 8. Схема експерименту з перевірки некласичності "зашумленого" фоківського стану з використанням критерію Фогеля—Ріхтера: S — лазерне джерело, BS — світлоподільна пластинка, NC — нелінійний кристал, TD — тригерний детектор (адаптовано згідно з [45])

ся на звичайний і незвичайний спарені (twin) промені, що перебувають у стані

$$|\Psi\rangle = \sum_n C_n |n\rangle \otimes |n\rangle \tag{126}$$

(див., наприклад, [47]), де $|n\rangle$ — n-фотонні фоківські стани. Один з променів посилають на гомодинний детектор, який спрацьовує тільки в тому випадку, коли до нього надходить сигнал з тригера. Цей тригер, в свою чергу, зв'язаний з високоефективним детектором, який може вирізняти однофотонні стани. Як тільки детектор реєструє один фотовідлік, спрацьовує тригер. Відповідно до (126) це означає, що на гомодинному детекторі також буде однофотонний фоківський стан. Всеможливі втрати в схемі приводять до підмішування вакууму. Однак, як і повинно бути, некласичність відносно представлення Глаубера—Сударшана має місце для довільної ефективності.

5.3. Вимірювання моментів

Інший метод детектування некласичності ґрунтується на процедурі вимірювання моментів. Він був запропонований в роботах [44,99]. Розклавши функцію $g(\alpha)$ в (110) в ряд

$$g(\alpha) = \sum_{mn} \xi_{mn} \alpha^{*n} \alpha^m, \tag{127}$$

правило (111) можна записати у вигляді

$$\sum_{nmkl} M_{n+l,m+k}\, \xi_{nm} \xi^*_{kl} < 0, \tag{128}$$

де

$$M_{n,m} = \int\limits_{-\infty}^{+\infty} \mathrm{d}^2\alpha P(\alpha)\, \alpha^{*n} \alpha^m = \mathrm{Tr}\left[\hat{\varrho}\, \hat{a}^{\dagger n} \hat{a}^m\right] \tag{129}$$

— матриця нормально впорядкованих моментів. Аналогічно попередньому випадку нерівність (128) означає, що відповідна квадратична форма не повинна бути додатно визначеною. Відповідно до критерію Сільвестра з цього випливає, що хоч один з мінорів матриці $\mathcal{M}_{\{nm\},\{lk\}} = M_{n+l,m+k}$, яку можна записати як

$$\begin{pmatrix}
1 & \langle\hat{a}\rangle & \langle\hat{a}^\dagger\rangle & \langle\hat{a}^2\rangle & \langle\hat{a}^\dagger\hat{a}\rangle & \langle\hat{a}^{\dagger 2}\rangle & \dots \\
\langle\hat{a}^\dagger\rangle & \langle\hat{a}^\dagger\hat{a}\rangle & \langle\hat{a}^{\dagger 2}\rangle & \langle\hat{a}^\dagger\hat{a}^2\rangle & \langle\hat{a}^{\dagger 2}\hat{a}\rangle & \langle\hat{a}^{\dagger 3}\rangle & \dots \\
\langle\hat{a}\rangle & \langle\hat{a}^2\rangle & \langle\hat{a}^\dagger\hat{a}\rangle & \langle\hat{a}^3\rangle & \langle\hat{a}^\dagger\hat{a}^2\rangle & \langle\hat{a}^{\dagger 2}\hat{a}\rangle & \dots \\
\langle\hat{a}^{\dagger 2}\rangle & \langle\hat{a}^{\dagger 2}\hat{a}\rangle & \langle\hat{a}^{\dagger 3}\rangle & \langle\hat{a}^{\dagger 2}\hat{a}^2\rangle & \langle\hat{a}^{\dagger 3}\hat{a}\rangle & \langle\hat{a}^{\dagger 4}\rangle & \dots \\
\langle\hat{a}^\dagger\hat{a}\rangle & \langle\hat{a}^\dagger\hat{a}^2\rangle & \langle\hat{a}^{\dagger 2}\hat{a}\rangle & \langle\hat{a}^\dagger\hat{a}^3\rangle & \langle\hat{a}^{\dagger 2}\hat{a}^2\rangle & \langle\hat{a}^{\dagger 3}\hat{a}\rangle & \dots \\
\langle\hat{a}^2\rangle & \langle\hat{a}^3\rangle & \langle\hat{a}^\dagger\hat{a}^2\rangle & \langle\hat{a}^4\rangle & \langle\hat{a}^\dagger\hat{a}^3\rangle & \langle\hat{a}^{\dagger 2}\hat{a}^2\rangle & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots
\end{pmatrix}, \tag{130}$$

від'ємний. Як результат ми отримаємо ієрархію нерівностей на моменти.

Процедура експериментального визначення моментів ґрунтується на такому принципі. З виразу (9) випливає, що k-та нормально впорядкована степінь квадратури може бути записана у вигляді

$$:\hat{x}^k(\varphi) := 2^{-\frac{k}{2}} \sum_{l=0}^{k} C_l^k\, \hat{a}^{\dagger l} \hat{a}^{k-l} e^{i\varphi(2l-k)}, \tag{131}$$

де C_l^k — біноміальний коефіцієнт. Легко бачити, що даний вираз являє собою ряд Фур'є, коефіцієнти якого пропорційні нормально впорядкованим степеням операторів народження і знищення. Тому, зробивши обернене перетворення Фур'є

$$\hat{a}^{\dagger n} \hat{a}^m = \frac{2^{\frac{n+m}{2}}}{2\pi C_n^{n+m}} \int\limits_0^{2\pi} \mathrm{d}\varphi :\hat{x}^{n+m}(\varphi): e^{-i\varphi(n-m)}, \tag{132}$$

можна знайти, що момент $M_{n,m}$ визначається середнім нормально впорядкованим $(n+m)$-им степенем квадратури

$$M_{n,m} = \frac{2^{\frac{n+m}{2}}}{2\pi C_n^{n+m}} \int_0^{2\pi} \mathrm{d}\varphi \left\langle : \hat{x}^{n+m}(\varphi) : \right\rangle e^{-i\varphi(n-m)}. \quad (133)$$

В процедурі гомодинного детектування, що описана в розділі 2.1, квадратура експериментально визначається за допомогою виразу (14) як різниця фотовідліків двох детекторів $\hat{n}_1 - \hat{n}_2$. Тому для даної схеми середнє від k-го степеня квадратури може бути записано у вигляді

$$\left\langle : \hat{x}^k(\varphi) : \right\rangle = \frac{1}{\left(r\sqrt{2}\right)^k} \left\langle : (\hat{n}_1 - \hat{n}_2)^k : \right\rangle \quad (134)$$

$$= \frac{1}{\left(r\sqrt{2}\right)^k} \sum_{l=0}^{k} (-1)^{k-l} C_l^k \left\langle : \hat{n}_1^l \hat{n}_2^{k-l} : \right\rangle. \quad (135)$$

Випадок $k=1$ дозволяє безпосередньо використовувати схему гомодинного детектування, показану на рис. 1, в якій визначається перший степінь квадратури, а потім за формулою (133) розраховуються моменти $M_{1,0}$ та $M_{0,1}$.

Для визначення моментів вищого порядку схему гомодинного детектування необхідно доповнити, як показано на рис. 9, див. [100]. В цьому випадку сигнал, що вимірюється, також змішується за допомогою світлоподільної пластинки з допоміжним лазером, що знаходиться в когерентному стані, фаза якого може змінюватися. Таким чином, на першому рівні схеми утворюються два сигнали на виході світлоподільної пластинки. Ці два сигнали на другому рівні розщеплюються на чотири за допомогою двох світлоподільних пластинок, додаткові входи для яких — вакуум. Чотири вихідних сигнали, в свою чергу, на третьому рівні діляться на вісім і т.д. до деякого рівня d. Схему з d рівнями позначають як MD_d. На виході цієї схеми маємо 2^d сигналів, які детектуються за допомогою 2^d фотодетекторів. Схема MD_d дозволяє виміряти моменти порядку $n+m \leqslant 2^{d-1}$.

Власне, нас цікавлять кореляції $\left\langle : \hat{n}_1^l \hat{n}_2^{k-l} : \right\rangle$ на виході з першої світлоподільної пластинки. Вся інша частина приладу являє собою схему для вимірювання цих кореляцій. Нехай $\hat{b}_i^{(d)}$ — оператори мод поля на виході з приладу MD_d. Через детектування кількості фотонів можна експериментально визначити кореляційну функцію $\left\langle \hat{b}_{j_1}^{(d)\dagger} \hat{b}_{j_1}^{(d)} \ldots \hat{b}_{j_k}^{(d)\dagger} \hat{b}_{j_k}^{(d)} \right\rangle$. Важливо зазначити, що дана кореляційна функція збігається зі

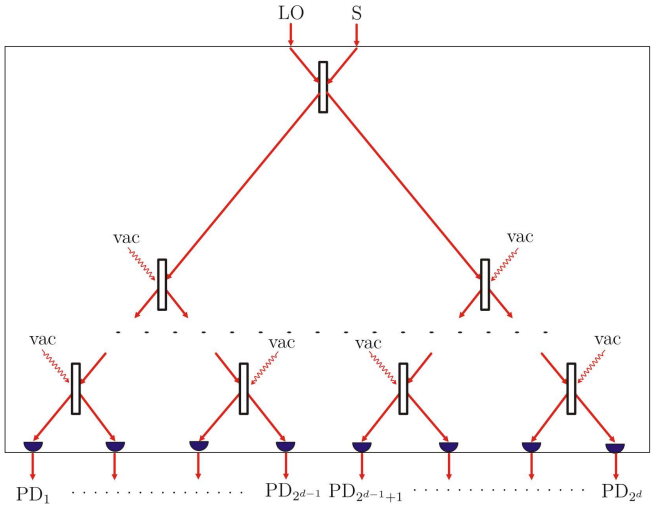

Рис. 9. Схема вимірювання моментів. LO — локальний осцилятор, S — сигнальне поле, PD_j — фотодетектори (адаптовано згідно з [99])

своєю нормально впорядкованою формою, тобто

$$\left\langle \hat{b}_{j_1}^{(d)\dagger} \hat{b}_{j_1}^{(d)} \ldots \hat{b}_{j_k}^{(d)\dagger} \hat{b}_{j_k}^{(d)} \right\rangle = \left\langle \hat{b}_{j_1}^{(d)\dagger} \ldots \hat{b}_{j_k}^{(d)\dagger} \hat{b}_{j_1}^{(d)} \ldots \hat{b}_{j_k}^{(d)} \right\rangle. \quad (136)$$

Відзначимо, що в лівій і в правій частині схеми є по 2^{d-1} детектор. Для довільного індексу $k = 1, \ldots, 2^{d-1}$ і для довільного l, що задовольняють умову $0 \leqslant l \leqslant k$, виберемо l фотодетекторів зліва і $k-l$ справа та виміряємо їх кореляційну функцію (136). Якщо тепер записати в явному вигляді співвідношення вхід-вихід між операторами мод $\hat{b}_i^{(d)}$ на виході з приладу MD_d і оператором мод $\hat{b}_1$, $\hat{b}_2$ на виході першої світлоподільної пластинки,

$$\hat{b}_i^{(d)} = \frac{(-1)^{r_1}}{\sqrt{2^d}} \hat{b}_1 + \mathrm{vac}, \text{ для лівої частини схеми} \quad (137)$$

$$\hat{b}_j^{(d)} = \frac{(-1)^{r_2}}{\sqrt{2^d}} \hat{b}_2 + \mathrm{vac}, \text{ для правої частини схеми} \quad (138)$$

(цілі числа $r_{1,2}$ визначають фазу, яка залежить від конкретного шляху вибраного променя, а символ "vac" означає лінійну комбінацію мод, що перебувають у вакуумному стані), то можна побачити, що (деталі див. в [100])

$$\left\langle \hat{b}_{j_1}^{(d)\dagger} \hat{b}_{j_1}^{(d)} \ldots \hat{b}_{j_k}^{(d)\dagger} \hat{b}_{j_k}^{(d)} \right\rangle = 2^{-k(d-1)} \left\langle : \hat{n}_1^l \hat{n}_2^{k-l} : \right\rangle, \quad (139)$$

де $\hat{n}_{1,2} = \hat{b}^{\dagger}_{1,2}\hat{b}_{1,2}$. Таким чином, виміряне на експерименті значення кореляційної функції (136) дозволяє отримати іншу кореляційну функцію $\langle : \hat{n}_1^l\, \hat{n}_2^{k-l} : \rangle$, а потім, відповідно до виразу (135), отримати значення нормально впорядкованого k-го степеня квадратури і за формулою (133) відтворити значення моментів. Це, в свою чергу, дає можливість прямо на експерименті перевірити критерії некласичності в термінах моментів.

5.4. Операційний критерій несепарабельності

Розглянутий в розділі 4.2 критерій Переса—Городецького визначає деякий математичний принцип, який дозволяє виділити несепарабельні стани. Нагадаємо з цього приводу, що достатньою умовою несепарабельності є від'ємна визначеність частково транспонованого оператора густини. В цій частині огляду розглянемо, як критерій Переса—Городецького можна використати для детектування переплутування на експерименті.

Ідея запропонованого Щукіним і Фогелем [101] (див. також [102]) операційного критерію несепарабельності полягає в тому, щоб оператор $\hat{g}$ в означенні індикатора $\hat{\mathsf{W}}_{\mathrm{PT}}$ (див. (109)) розкласти по операторах народження та знищення двох мод — $\hat{a}$, $\hat{a}^{\dagger}$ та $\hat{b}$, $\hat{b}^{\dagger}$:

$$\hat{g} = \sum_{n,m,k,l=0}^{+\infty} \xi_{nmkl}\hat{a}^{\dagger n}\hat{a}^{m}\hat{b}^{\dagger k}\hat{b}^{l}. \tag{140}$$

Тепер середнє від цього індикатора можна представити у вигляді квадратичної форми

$$\mathrm{Tr}\left[\hat{\varrho}\,\hat{\mathsf{W}}_{\mathrm{PT}}\right] = \sum_{n,m,k,l,p,q,r,s=0}^{+\infty} \xi^{*}_{nmkl}\xi_{pqrs}M^{\mathrm{PT}}_{nmkl,pqrs}, \tag{141}$$

де

$$M^{\mathrm{PT}}_{nmkl,pqrs} = \mathrm{Tr}\left[\hat{\varrho}\left(\hat{a}^{\dagger n}\hat{a}^{m}\hat{a}^{\dagger p}\hat{a}^{q}\hat{b}^{\dagger k}\hat{b}^{l}\hat{b}^{\dagger r}\hat{b}^{s}\right)^{\mathrm{PT}}\right] \tag{142}$$

— матриця частково транспонованих моментів. Узагальнюючи правило (102) на довільний оператор, неважко перевірити, що ця матриця пов'язана з моментами (нетранспонованими)

$$M_{nmkl,pqrs} = \mathrm{Tr}\left[\hat{\varrho}\left(\hat{a}^{\dagger n}\hat{a}^{m}\hat{a}^{\dagger p}\hat{a}^{q}\hat{b}^{\dagger k}\hat{b}^{l}\hat{b}^{\dagger r}\hat{b}^{s}\right)\right] \tag{143}$$

таким чином:

$$M^{\mathrm{PT}}_{nmkl,pqrs} = M_{nmsr,pqlk}. \tag{144}$$

Очевидно, що тепер умови сепарабельності еквівалентні умові невід'ємності відповідної квадратичної форми. Звичайно, цю квадратичну форму необхідно записати в стандартному вигляді, використавши тільки два індекси підсумовування. Відповідний розгляд можна знайти в роботі [101], тут ми наведемо тільки результат. Отже, виходячи з критерію Сільвестра для додатно визначеної квадратичної форми, а також приймаючи до уваги вищенаведений розгляд, можна зробити висновок, що *часткове транспонування двомодового квантового стану є невід'ємним тоді і тільки тоді, коли всі мінори матриці*

$$\begin{pmatrix} 1 & \langle\hat{a}\rangle & \langle\hat{a}^{\dagger}\rangle & \langle\hat{b}^{\dagger}\rangle & \langle\hat{b}\rangle & \dots \\ \langle\hat{a}^{\dagger}\rangle & \langle\hat{a}^{\dagger}\hat{a}\rangle & \langle\hat{a}^{\dagger 2}\rangle & \langle\hat{a}^{\dagger}\hat{b}^{\dagger}\rangle & \langle\hat{a}^{\dagger}\hat{b}\rangle & \dots \\ \langle\hat{a}\rangle & \langle\hat{a}^{2}\rangle & \langle\hat{a}\hat{a}^{\dagger}\rangle & \langle\hat{a}\hat{b}^{\dagger}\rangle & \langle\hat{a}\hat{b}\rangle & \dots \\ \langle\hat{b}\rangle & \langle\hat{a}\hat{b}\rangle & \langle\hat{a}^{\dagger}\hat{b}\rangle & \langle\hat{b}^{\dagger}\hat{b}\rangle & \langle\hat{b}^{2}\rangle & \dots \\ \langle\hat{b}^{\dagger}\rangle & \langle\hat{a}\hat{b}^{\dagger}\rangle & \langle\hat{a}^{\dagger}\hat{b}^{\dagger}\rangle & \langle\hat{b}^{\dagger 2}\rangle & \langle\hat{b}\hat{b}^{\dagger}\rangle & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix} \tag{145}$$

невід'ємні. Іншими словами, якщо існує хоча б один від'ємний мінор цієї матриці, то часткове транспонування не є невід'ємним. А звідси виходить, що відповідний стан, згідно з критерієм Переса—Городецького, є несепарабельним. Процедура вимірювання моментів в даному випадку повністю аналогічна тій, що описана в попередньому розділі. Таким чином, отримуємо операційне формулювання критерію Переса—Городецького. А відповідні умови тепер можна розглядати як ієрархію нерівностей.

Зокрема, певний інтерес становить невід'ємність детермінанта п'ятого порядку. Можна показати, що цей детермінант може бути записаний у вигляді

$$D_5 = \det A_1 \det A_2 + \left(\frac{1}{4} - |\det C|\right)^2 - \mathrm{tr}\Big(A_1 JCJA_2 JC^{\mathrm{T}}J\Big) - \frac{1}{4}\Big(\det A_1 + \det A_2\Big), \tag{146}$$

де

$$A_i = \begin{pmatrix} \langle(\Delta\hat{x}_i)^2\rangle & \langle\{\Delta\hat{x}_i, \Delta\hat{p}_i\}\rangle \\ \langle\{\Delta\hat{x}_i, \Delta\hat{p}_i\}\rangle & \langle(\Delta\hat{p}_i)^2\rangle \end{pmatrix}, \tag{147}$$

$$C = \begin{pmatrix} \langle\Delta\hat{x}_1\Delta\hat{x}_2\rangle & \langle\Delta\hat{x}_1\Delta\hat{p}_2\rangle \\ \langle\Delta\hat{p}_1\Delta\hat{x}_2\rangle & \langle\Delta\hat{p}_1\Delta\hat{p}_2\rangle \end{pmatrix}, \tag{148}$$

$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{149}$$

Дана умова була отримана незалежно Саймоном в роботі [103]. Як видно, критерій Саймона є частинним випадком більш загальної операційної умови несепарабельності.

6. Системи з двома рівнями

Вищенаведений розгляд стосувався важливого класу систем з нескінченновимірним гільбертовим простором станів, в яких координата та імпульс можуть набувати значень з неперервного фазового простору, що являє собою двовимірну площину. Фізично це відповідає розгляду однієї моди електромагнітного поля без врахування поляризації. Такі системи часто називають системами з неперервними змінними (continuous-variable systems). Їх некласичні властивості зручно використовувати в квантовій інтерферометрії і в інших випадках, коли необхідне зменшення дробового шуму. Кодування інформації в системах з неперервним набором змінних відповідає використанню аналогових сигналів і тому має цілий набір таких же недоліків, як і в класичному випадку, див., наприклад, [104]. Тим не менш, в квантовій інформатиці такі системи дуже широко використовуються, оскільки і вони мають ряд практичних переваг [83].

В сучасних інформаційних технологіях частіше використовуються системи, що мають лише два стабільних стани, яким приписують значення 0 та 1 — біти. Наприклад, це може бути перемикач з двома положеннями. Квантові дворівневі системи називаються кубітами, і їх основна відмінність від класичних аналогів полягає в можливості реалізації суперпозиції двох станів

$$|\Psi\rangle = \cos\theta\,|0\rangle + e^{i\varphi}\sin\theta\,|1\rangle\,, \tag{150}$$

де θ і φ — деякі параметри. Такі стани не мають ніяких класичних аналогів. Дійсно, в даному випадку система перебуває в двох стабільних станах одночасно, що повністю не можливо з точки зору класичної фізики. Аналогом стану класичного біта була б статистична суміш

$$\hat{\varrho} = \cos^2\theta\,|0\rangle\langle 0| + \sin^2\theta\,|1\rangle\langle 1|\,, \tag{151}$$

в яку (150) може перейти в результаті процесів декогерентності.

Фізична реалізація кубітів може бути різною. В першу чергу, це звичайно частинка зі спіном 1/2. Як кубіт може використовуватися атом, який має два рівні з великим часом життя. В квантовій криптографії часто використовують оптичні поля слабкої інтенсивності, в яких поява станів з двома і більше фотонів зведена до мінімуму або взагалі неможлива. В цьому випадку дві різні моди електромагнітного поля відповідають двом станам. Це можуть бути моди з перпендикулярними поляризаціями, див., наприклад [4]. Також у квантовій криптографії використовують просторово розділені моди в двох різних хвилеводах або розділені у часі так, що імпульси поширюються один за одним.

6.1. Сфера Пуанкаре

З формально-математичної точки зору, фазовий простір систем з двома рівнями також суттєво відрізняється від фазового простору систем з неперервними змінними. Замість операторів координат та імпульсів тепер використовуються оператори $\hat{S}_1$, $\hat{S}_2$, $\hat{S}_3$, які задовольняють комутаційні співвідношення

$$\begin{aligned}\left[\hat{S}_1, \hat{S}_2\right] &= i\hat{S}_3,\\ \left[\hat{S}_2, \hat{S}_3\right] &= i\hat{S}_1,\\ \left[\hat{S}_3, \hat{S}_1\right] &= i\hat{S}_2.\end{aligned} \tag{152}$$

Ці оператори мають фізичний зміст компонент спіну, у випадку дворівневого атома — псевдоспіну, а у випадку однофотонних станів з різними поляризаціями — параметрів Стокса [4]. Оскільки абсолютне значення спіну є фіксованим, на дані оператори накладається умова

$$\hat{S}_1^2 + \hat{S}_2^2 + \hat{S}_3^2 = \frac{3}{4}. \tag{153}$$

Для атома з двома рівнями або для двох мод електромагнітного поля (перпендикулярних поляризацій, або двох мод у різних хвилеводах) оператори $\hat{S}_i$ можуть бути записані у вигляді

$$\begin{aligned}\hat{S}_1 &= \tfrac{1}{2}\left(\hat{a}_2^\dagger\hat{a}_1 + \hat{a}_1^\dagger\hat{a}_2\right),\\ \hat{S}_2 &= \tfrac{1}{2i}\left(\hat{a}_2^\dagger\hat{a}_1 - \hat{a}_1^\dagger\hat{a}_2\right),\\ \hat{S}_3 &= \tfrac{1}{2}\left(\hat{a}_2^\dagger\hat{a}_2 - \hat{a}_1^\dagger\hat{a}_1\right),\end{aligned} \tag{154}$$

де $\hat{a}_1$ та $\hat{a}_2$ — оператори знищення електрона відповідно на основному і на збудженому рівнях атома або фотона у двох різних модах. Особливо потрібно підкреслити той факт, що комутаційні співвідношення (152) будуть виконуватися незалежно від того, які співвідношення, для бозонів чи ферміонів, задовольняють оператори $\hat{a}_1$ та $\hat{a}_2$. В той же час співвідношення (153) буде виконуватися тільки для одночастинкових станів.

Зазначимо, що в залежності від типу вибраної дворівневої системи зміст і позначення базисних станів можуть змінюватися. Так, для частинки зі спіном 1/2 — це стани $|\pm\rangle$ із значеннями компоненти спіну

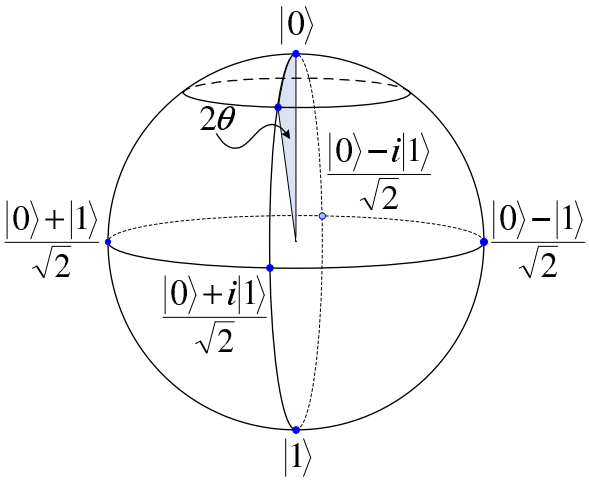

Рис. 10. Сфера Пуанкаре, на якій показано шість різних базисних станів, крім того, точкою показано довільний чистий стан (150), а колом — змішаний (151)

$\pm\frac{1}{2}$. Для поляризованих фотонів — це можуть бути стани з вертикальною $|\updownarrow\rangle$ та горизонтальною $|\leftrightarrow\rangle$ поляризаціями. Для дворівневого атома — це основний $|g\rangle$ та збуджений $|e\rangle$ стани.

Представлення фазового простору для систем з двома рівнями було введено незалежно Стратоновичем та Агарвалом в [105, 106]. Це дозволило в повній мірі сформулювати для них поняття некласичності. Зв'язок (153) при цьому означає, що фазовий простір є тепер не двовимірною поверхнею, а сферою, яка називається сферою Пуанкаре. Таким чином, функції квазірозподілу тепер задаються на цій сфері, по ній же, природно, проводиться інтегрування при обчисленні середнього значення динамічних змінних. Одним з найяскравіших проявів некласичності для систем з одним ступенем вільності є поляризаційно-стиснуте світло, яке вперше було розглянуте Чіркіним, Орловим та Паращуком [107].

Сфера Пуанкаре використовується не тільки для наочнішого зображення представлення Стратоновича—Агарвала. Вона з однаковим успіхом може бути використана в представлені гільбертового простору (див. рис. 10) і виявляється корисною для пояснення ефектів некласичності. Так, чистий стан (150) можна відобразити точкою на сфері Пуанкаре, а змішаний стан (151) — колом. Для чистого стану завжди можна виконати поворот системи координат (вибрати інший базис) так, щоб він збігався з $|0\rangle$ або $|1\rangle$. Для змішаних станів це, звичайно, не можливо. Такий поворот на сфері Пуанкаре відповідає вибору іншого базису для векторів поляризації або внесенню додаткового фазового зсуву при використанні ослабленого електромагнітного поля. Цей факт активно використовується в квантовій криптографії в протоколі BB84, див. розділ 7.2.

6.2. Нерівності Белла

Як вже було сказано, в 1964 р. Дж. Белл у своїй знаменитій роботі [9] довів, що деякі нерівності для других моментів спінів двох частинок повинні завжди виконуватися для "локальної теорії", існування якої припускали в своїй роботі ЕПР [5]. Ці нерівності, взагалі кажучи, повинні порушуватися для переплутаних станів в квантовій теорії. Тому експериментальне підтвердження цього факту в дослідах Аспекта [10] стало своєрідною крапкою в довгих дискусіях про локальний реалізм і детермінізм в квантовій теорії.

Розгляд Белла стосується простого прикладу систем з двома рівнями, який описаний в роботі Бома [108]. По суті, нерівності Белла аналогічні розглянутим вище нерівностям, які виявляють некласичність — вони завжди виконуються, якщо розподіл задовольняє колмогоровські аксіоми теорії ймовірностей, і порушуються в супротивному випадку. Розглянемо прилад, який генерує пари частинок зі спіном 1/2, які потім розлітаються в різні боки. Два спостерігачі вимірюють проекції спіну своєї частинки на два довільні, але фіксовані напрямки $\vec{a}$, $\vec{b}$ для першої частинки і $\vec{c}$, $\vec{d}$ для другої. Таким чином, в даному експерименті існує всього чотири кореляції між проекціями спіну двох частинок. Нерівності Белла накладають деякі обмеження на ці кореляції, які повинні виконуватися, якщо припустити правильність аргументів ЕПР (тобто в припущенні колмогоровості теорії). Зрозуміло, що замість частинок із півцілим спіном можна розглядати будь-яку іншу дворівневу систему. Наприклад, поляризаційна ступінь вільності фотона. У цьому випадку різні напрямки відповідають різним базисам поляризацій.

Тут ми наведемо дещо модифікований варіант нерівності Белла, запропонований Клаузером, Хорном, Шимоні та Хольтом [109]. Розглянемо таку випадкову величину:

$$\begin{aligned} B \quad &= 2\left(S^{(1)}_{\vec{a}} + S^{(1)}_{\vec{b}}\right)\left(S^{(2)}_{\vec{c}} + S^{(2)}_{\vec{d}}\right) \\ &+2\left(S^{(1)}_{\vec{a}} + S^{(1)}_{\vec{b}}\right)\left(S^{(2)}_{\vec{c}} - S^{(2)}_{\vec{d}}\right) \\ &+2\left(S^{(1)}_{\vec{a}} - S^{(1)}_{\vec{b}}\right)\left(S^{(2)}_{\vec{c}} + S^{(2)}_{\vec{d}}\right) \\ &-2\left(S^{(1)}_{\vec{a}} - S^{(1)}_{\vec{b}}\right)\left(S^{(2)}_{\vec{c}} - S^{(2)}_{\vec{d}}\right), \end{aligned} \tag{155}$$

де $S_{\vec{x}}^{(k)}$ — проекція спіну частинки під номером $k = 1, 2$ на напрямок $\vec{x} = \vec{a}, \vec{b}, \vec{c}, \vec{d}$. Легко бачити, що для довільної реалізації випадкових величин $S_{\vec{x}}^{(k)} = \pm\frac{1}{2}$ тільки один член наведеної суми відмінний від нуля і рівний ± 2. А це означає, що випадкова величина B також приймає тільки два значення $+2$ та -2. Припустивши, що спільна функція розподілу величин $S_{\vec{x}}^{(k)}$ задовольняє всі колмогоровські аксіоми теорії ймовірностей, приходимо до висновку, що параметр $\mathcal{B}$, що є модулем середнього значення B (параметр Белла), не перевищує 2 (див. також [4]),

$$\mathcal{B} = |\langle B \rangle| \leq 2. \tag{156}$$

Розкривши добутки в (155), отримаємо цей параметр у такому вигляді:

$$\mathcal{B} = 4\Big|\Big\langle S_{\vec{a}}^{(1)} S_{\vec{c}}^{(2)} \Big\rangle + \Big\langle S_{\vec{a}}^{(1)} S_{\vec{d}}^{(2)} \Big\rangle +$$

$$+ \Big\langle S_{\vec{b}}^{(1)} S_{\vec{c}}^{(2)} \Big\rangle - \Big\langle S_{\vec{b}}^{(1)} S_{\vec{d}}^{(2)} \Big\rangle\Big|. \tag{157}$$

Таким чином, в припущенні ЕПР (тобто теорії, де всі функції розподілу повинні задовольняти аксіоми Колмогорова) нерівність (156) повинна завжди виконуватися.

Однак існують такі стани, для яких параметр $\mathcal{B}$ перевищує допустиме значення 2, порушуючи нерівність Белла. Максимальне порушення в $\sqrt{2}$ раз перевищує класичну межу і таким чином дорівнює $2\sqrt{2}$. Це так для двох станів, які називаються беллівськими і які у випадку фотонних поляризацій мають такий вигляд:

$$|\mathrm{BS1}\rangle = \frac{1}{\sqrt{2}}\Big(|\leftrightarrow\rangle \otimes |\updownarrow\rangle - |\updownarrow\rangle \otimes |\leftrightarrow\rangle \Big). \tag{158}$$

$$|\mathrm{BS2}\rangle = \frac{1}{\sqrt{2}}\Big(|\leftrightarrow\rangle \otimes |\leftrightarrow\rangle + |\updownarrow\rangle \otimes |\updownarrow\rangle \Big), \tag{159}$$

Ці стани відіграють ключову роль як у фундаментальних дослідженнях основ квантової теорії, так і в практичному використанні в квантовій криптографії (див. обговорення протоколу E91 в розділі 7.3).

6.3. Перевірка нерівностей Белла

Цілком зрозуміло, що після того як Беллом було запропоновано тестувати некласичність (або у даному

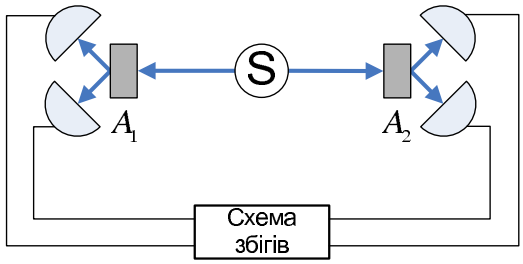

Рис. 11. Загальна схема експериментів з перевірки нерівностей Белла: S — джерело переплутаних пар, A_1, A_2 — аналізатори

контексті — нелокальність) квантової теорії за допомогою певних нерівностей, почали виникати ідеї щодо відповідних експериментів. Втім через недостатній розвиток експериментальної техніки така перевірка деякий час була неможливою внаслідок відсутності або недоліків існуючих джерел, аналізаторів та детекторів. При цьому всі вади практичної перевірки нелокальності потенційно можуть позбавляти її результати достовірності, залишаючи шанси для локальних прихованих параметрів — так звані щілини (loopholes). Згодом із розвитком експериментальної техніки вади поступово усувалися й на сьогодні практично відсутні, хоч і не в усіх експериментах.

Загальна схема експериментів з перевірки нерівностей Белла (див. рис. 11) передбачає застосування джерела переплутаних пар, частинки яких розділяються в просторі та прямують до двох аналізаторів. Ці аналізатори здійснюють вимірювання параметрів $S_{\vec{x}}^{(k)}$. Це, наприклад, можуть бути напрямки орієнтації поляризаторів у випадку експерименту на основі поляризаційно переплутаних пар фотонів, при цьому поляризатор пропускає фотони, які мають поляризацію вздовж напрямку поляризатора (або близьку до неї), та відбивають фотони з ортогональною поляризацією (або близькою до неї). Далі фотони потрапляють відповідно на один з двох детекторів, обидві пари яких підключено до електронної схеми збігів, яка реєструє випадки збігів результатів вимірювань. За кореляцією результатів вимірювань розраховується параметр Белла (157) і перевіряється порушення нерівності (156).

Першою практичною перевіркою порушення нерівностей Белла був експеримент Фрідмана й Клаузера [110] в 1972 р. на основі поляризаційно переплутаних фотонів. Пари генерувалися в релаксаційному каскадному переході атомів кальцію, які збуджувалися зовнішньою накачкою. Аналіз кореляцій між вимірюваннями поляризаційних станів фотонних пар по-

казав порушення нерівності Белла, а отже, нелокальність квантової теорії.

Втім, більш відомою є успішна серія експериментів Аспекта та ін. [9], які вдосконалили джерело з експерименту Фрідмана та Клаузера (застосовуючи селективну накачку з двофотонним поглинанням за допомогою опромінення кальцію двома лазерними пучками). Суттєвою відмінністю цього експерименту було намагання обійти проблему, яка полягає в можливій скорельованості результатів вимірювань внаслідок виникнення взаємозв'язку між частинами установки (аналізаторами), якщо вони настроєні заздалегідь. Оскільки подібна узгодженість, якою б не була її природа, в принципі, можлива, то результати експериментів на статично налаштованих аналізаторах не є достатньо переконливими для прихильників локальних змінних. Отже, в експерименті Аспекта вперше застосовувалося варіювання аналізаторів, настроювання яких змінювалося від однієї переплутаної пари до іншої, що збільшило достовірність отриманих результатів, які обчислювалися для специфічних збігів пар аналізаторних базисів. В наступному експерименті настроювання аналізаторів змінювалося в процесі поширення частинок — задля уникнення можливого узгодження між аналізаторами за припущення, що воно відбувається зі швидкістю світла. Обидва ці експерименти чітко підтвердили порушення нерівності Белла зі значенням, яке може бути отримане із квантової теорії.

Крім фундаментального значення, експерименти Аспекта надали поштовх і практичному застосуванню основ квантової теорії — ідея зміни базисів надихнула Екерта [110] доповнити аналізаторні базиси двома однаковими наборами для отримання з вимірювання станів частинок переплутаної пари скорельованих послідовностей бітів та одночасного з'ясування відсутності втручання в стан частинок шляхом перевірки порушення нерівності Белла, що стало основою для створення відповідного протоколу квантової криптографії (див. розділ 7.3) та започаткувало розвиток цього напряму квантової інформації.

Наступні експерименти з перевірки нерівностей Белла, які здійснювалися вже здебільшого на основі джерел з параметричним діленням частоти в нелінійних кристалах [111], застосовували різноманітні типи переплутання фотонних пар — імпульсне [112] або переплутання енергії-часу [113]. Результати всіх цих експериментів підтвердили некласичні (нелокальні) властивості квантових систем.

7. Квантова криптографія

Як зазначалося у Вступі, некласичні властивості квантових станів, в першу чергу, можуть знайти своє застосування в принципово нових технологіях обробки та передачі інформації. В принципі, йдеться про зовсім інший підхід до самого поняття інформації — між квантовою та класичною інформатиками існують такі ж відмінності, як і між відповідними розділами фізики. Нашу увагу буде приділено лише одному застосуванню некласичності — квантовій криптографії, що не в останню чергу зумовлено практичною цінністю та важливістю цього напряму досліджень, а також тим, що вже зараз відповідні технології доступні для комерційного застосування [21, 22].

Криптографією називають прикладну науку, яка вивчає методи захисту інформації від несанкціонованого доступу, див. [17]. Стрімкий розвиток інформаційних технологій в наш час привів до виникнення "цивільної криптографії", досягненнями якої в тій чи іншій мірі користується переважна більшість як приватних, так і юридичних осіб. Насамперед це стосується різного типу електронних платежів, мобільного зв'язку, prepaid карток, комп'ютерних мереж, шифрування повідомлень електронною поштою, захищених Інтернет-сайтів тощо.

Однією з типових задач криптографії є передача конфіденційного повідомлення між двома сторонами. Ця задача вирішується шляхом шифрування — вихідне повідомлення за якимось правилом перетворюється в свій зашифрований варіант. Саме він може передаватися відкритими, або навіть публічними, каналами від відправника до отримувача. При цьому і шифрування, і обернена до нього процедура дешифрування вимагають використання деякої додаткової інформації, яка називається ключом. В сучасних криптографічних системах він є випадковою послідовністю бітів. В принципі, існує досить багато різноманітних алгоритмів шифрування, кожен з яких відрізняється надійністю, сферами застосування, державними чи корпоративними стандартами тощо. Але абсолютна надійність була доведена Шенноном [1] (див. також [103]) лише для алгоритму одноразового блокнота (one-time pad), запропонованого Вернамом в 1929 р. [114]. Він полягає у тому, що до значення кожного біта вихідного повідомлення додається за модулем 1 значення відповідного біта ключа. При цьому довжина повідомлення має дорівнювати довжині ключа, а надійність зберігається лише за умови одноразового використання останнього.

Таким чином, для забезпечення захищеності каналу зв'язку від несанкціонованого доступу відправник та отримувач інформації мають обмінятися ключем — випадковою послідовністю бітів. Зрозуміло, що у більшості сучасних застосувань, наприклад у системах платежів, захищених Інтернет-сайтах тощо неможливо мати одноразові блокноти між всіма учасниками інформаційного обміну. Тому виникає задача передачі ключа (key distribution). Її сучасне вирішення полягає у застосуванні асиметричних криптосистем, вперше запропонованих в 1976 р. Діффі та Хелмманом [115]. Найбільш відомою реалізацією цієї ідеї є алгоритм Ріверста—Шаміра—Адлемана (RSA) [16] (див. також [17]).

Принцип роботи асиметричних криптосистем полягає в тому, що тепер використовується не один, а два ключі — відкритий (public key), яким відправник може зашифрувати ключ симетричної криптосистеми, та закритий (private key), яким отримувач може його розшифрувати. Маючи закритий ключ, відправник може легко обчислити відкритий і відправити його звичайним незахищеним каналом отримувачу. Обернену операцію — поновлення закритого ключа за відкритим — з обчислювальної точки зору виконати практично не можливо. Цю складність і використовують у більшості сучасних систем передачі ключа. Так, у системі RSA для поновлення закритого ключа за відкритим потрібно розкласти (факторизувати) число на прості множники. Якщо це число має розмір тисячі бітів, то ця операція практично не можлива. Обернену ж операцію отримувач може виконати за долі секунди.

Проте асиметричні криптосистеми мають суттєві вади. По-перше, їх надійність ще й досі не доведено. Тобто можливе існування швидких алгоритмів їх зламування. По-друге, для задачі факторизації існує алгоритм Шора [16] для квантових комп'ютерів. Він дозволяє провести цю операцію за достатньо невеликий час. І хоч квантові комп'ютери ще не створені, проте вже сьогодні існує небезпека того, що конфіденційна інформація, яка передається за допомогою асиметричних криптосистем, може бути перехоплена та розшифрована у недалекому майбутньому. Саме тому на сьогодні є актуальною розробка альтернативних способів для передачі криптографічного ключа, що й пропонується квантовою криптографією. Отже, задача її полягає у тому, щоб передати від відправника до отримувача, яких за традицією у літературі називають Алісою та Бобом, випадкову послідовность бітів. При цьому необхідно достатньо точно оцінити кількість інформації, що могла потрапити до несанкціонованого користувача (підслуховувача), якого за традицією називають Євою.

7.1. Теорема про неможливість клонування

В основі ідеї квантової криптографії лежить фундаментальний фізичний принцип неможливості клонування квантових станів [19]. Він був сформульований та доведений Вуттерзом і Цуреком в 1982 р., але вперше розглянутий Візнером ще в 1970-х роках, проте надрукований лише в 1983 р. Неможливість клонування означає, що чистий квантовий стан не можна перенести з одного носія на інший без руйнування його на першому. Доведення цієї теореми (no-cloning theorem) ґрунтується лише на тому факті, що у квантовій фізиці всі операції над станами у гільбертовому просторі є лінійними.

Отже, в операції клонування мали б брати участь принаймні дві системи — у найпростішому випадку два кубіти, кожен з яких має базисні стани $|0\rangle$ та $|1\rangle$. Нехай $|\text{blank}\rangle$ — початковий стан кубіта, на який необхідно склонувати квантовий стан іншого кубіта. Тоді клонування стану $|0\rangle$, що описується оператором $\hat{\mathsf{C}}$, виглядало б як

$$\hat{\mathsf{C}}\,|0\rangle \otimes |\text{blank}\rangle = |0\rangle \otimes |0\rangle\,. \tag{160}$$

Аналогічно мало б виглядати клонування стану $|1\rangle$,

$$\hat{\mathsf{C}}\,|1\rangle \otimes |\text{blank}\rangle = |1\rangle \otimes |1\rangle\,. \tag{161}$$

А для кубіта в довільному чистому стані (150) клонування мало б виглядати як

$$\hat{\mathsf{C}}\left(\cos\theta\,|0\rangle + e^{i\varphi}\sin\theta\,|1\rangle\right) \otimes |\text{blank}\rangle =$$

$$= \left(\cos\theta\,|0\rangle + e^{i\varphi}\sin\theta\,|1\rangle\right) \otimes \left(\cos\theta\,|0\rangle + e^{i\varphi}\sin\theta\,|1\rangle\right). \tag{162}$$

Оскільки оператор клонування $\hat{\mathsf{C}}$ має бути лінійним, то підстановка (160) та (161) в ліву частину (162) приводить до рівності

$$\cos\theta\,|0\rangle \otimes |0\rangle + e^{i\varphi}\sin\theta\,|1\rangle \otimes |1\rangle =$$

$$= \left(\cos\theta\,|0\rangle + e^{i\varphi}\sin\theta\,|1\rangle\right) \otimes \left(\cos\theta\,|0\rangle + e^{i\varphi}\sin\theta\,|1\rangle\right). \tag{163}$$

Вона може виконуватись лише при одночасному виконанні умов

$$\begin{aligned} &\cos\theta = 1,\\ &\sin\theta = 1,\\ &\cos\theta\sin\theta = 0, \end{aligned} \tag{164}$$

що не можливо. Це й доводить неможливість існування оператора $\hat{\mathsf{C}}$, тобто операції клонування. Наведений розгляд можна розширити на гільбертів простір довільної вимірності, доповнити його ступенями вільності "клонуючої машини", але це принципово не змінить ситуації.

Завдяки теоремі про неможливість клонування, будь-який несанкціонований доступ до каналу захищеного зв'язку приведе до зміни квантового стану носія інформації (оптичного поля), що може бути зареєстровано відправником та отримувачем. Втім попри неможливість ідеального клонування чистого квантового стану системи можливе відтворення станів, що є близькими до клонованого. Принципові схеми таких процесів отримали назву універсальних клонуючих машин і були реалізовані для приблизного копіювання станів фотонів [117]. Тому теорему про неможливість клонування було б коректніше називати теоремою про неможливість ідеального клонування (no-perfect-cloning theorem). Існування операцій неідеального клонування вимагає ретельнішого аналізу протоколів квантової криптографії з метою унеможливлення певних типів атак на канали захищеного зв'язку.

7.2. Протокол Беннета та Брассара — BB84

Перший квантово-криптографічний протокол було запропоновано Беннетом та Брассаром у 1984 р. та згодом названо BB84 [21]. Цей протокол базується на використанні дворівневих систем (кубітів), які передаються від Аліси до Боба. Як такі системи вибирають або поляризаційні стани фотонів, або розділені у просторі (або у часі) моди електромагнітного поля — так зване кодування фазою. У першому випадку світлові імпульси зручно передавати безпосередньо через атмосферу, оскільки вона не змінює поляризацій, а у другому — каналом передачі є, як правило, оптичні хвилеводи. Зрозуміло, що техніка приготування та вимірювання таких станів в обох випадках різна, а тому їх слід розглядати окремо. Для спрощення викладу та досягнення більшої наочності ми спочатку розглянемо в деталях випадок поляризованих фотонів.

Отже, Аліса відправляє до Боба поляризовані фотони, кодуючи станом $|\leftrightarrow\rangle$ значення біта 0, а станом $|\updownarrow\rangle$ — значення біта 1. Це є власні стани оператора $\hat{S}_3$. Так само Аліса може використати для кодування бітів інший базис, кодуючи станом

$$|\nwarrow\!\!\searrow\rangle = \frac{1}{\sqrt{2}}\Big(|\leftrightarrow\rangle - |\updownarrow\rangle\Big) \tag{165}$$

значення біта 0, а станом

$$|\swarrow\!\!\nearrow\rangle = \frac{1}{\sqrt{2}}\Big(|\leftrightarrow\rangle + |\updownarrow\rangle\Big) \tag{166}$$

— значення біта 1. Ці стани є власними для оператора $\hat{S}_1$. Якщо Аліса відправить фотон поляризований в одному базисі, а детектори Боба будуть налаштовані на інший, то згідно з (165) та (166) Боб з рівною імовірністю зареєструє або один, або інший стан. Якщо ж базиси збігаються, то Боб зареєструє саме той стан, який відправила Аліса.

Для кожного фотона Аліса випадково обирає значення біта та базис, див. рис. 12. Кожного разу, коли Боб очікує прибуття фотона, він активує свої детектори та випадково вибирає один з двох базисів, в якому буде відбуватися вимірювання. Він реєструє, який базис було використано та яке значення біта він отримав. Після обміну достатньою кількістю фотонів, він відкрито (через звичайний канал) повідомляє Алісі, в яких випадках він реєстрував фотони та який саме базис при цьому використовував, але не повідомляє, які значення бітів він при цьому отримував. Аліса порівнює випадок за випадком, чи був базис Боба сумісний з тим, в якому вона готувала відповідний фотон. Випадки, в яких базиси не збігалися або Боб не реєстрував фотон, відкидаються. Для тих випадків, що залишилися, Аліса з Бобом можуть бути впевнені, що значення бітів у них збігаються. Ці біти утворюють так званий просіяний ключ.

Будь-які втрати, що пов'язані з передачею, неідеальним детектуванням (див. розділ 5.1), так само, як і недосконалість аналізаторів, приводять до виникнення помилок, тобто до того, що Аліса і Боб будуть мати неідентичні ключі. З іншого боку, будь-яка спроба несанкціонованого доступу у канал передачі інформації також має своїм результатом виникнення додаткових помилок. Тому на наступному етапі Аліса та Боб повинні порівняти значення бітів у деякому випадково вибраному піднаборі бітів ключа. За рівнем помилок у ньому можна оцінити кількість інформації, що могла потрапити до Єви. Далі Алісою та Бобом застосовуються певні криптографічні (класичні) алгоритми корекції ключа та підсилення секретності, які перетворюють просіяний ключ на криптографічний.

Хоча вперше протокол BB84 був реалізований на основі поляризаційних станів фотонів, на практиці

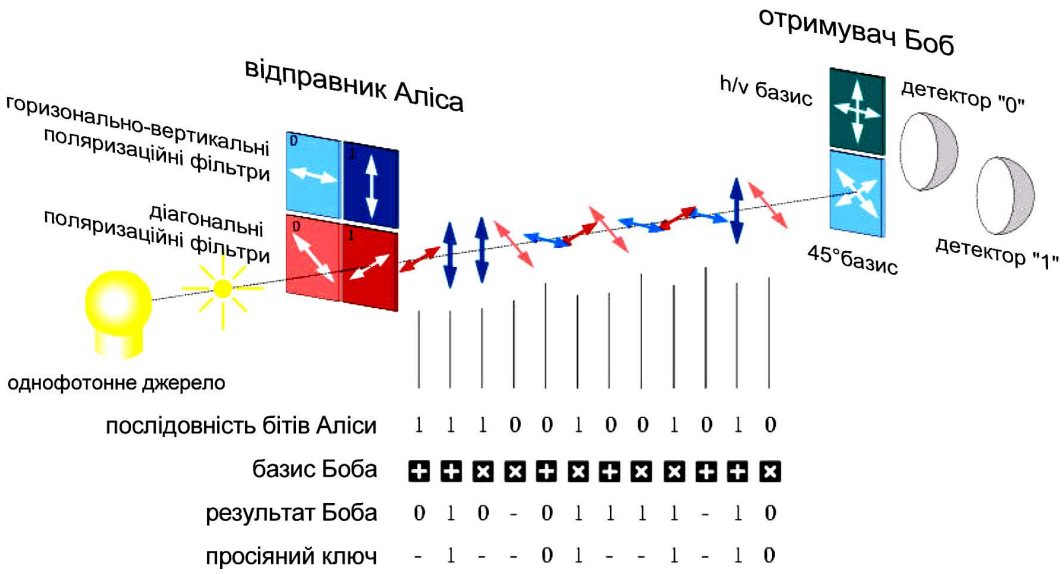

Рис. 12. Протокол BB84: Для кожної частинки Аліса випадково вибирає значення біта (рядок *1*) та базис і готує частинку у відповідному стані. Боб випадково вибирає один з двох базисів, в якому буде відбуватися вимірювання (рядок *2*). Він реєструє, який базис було використано та яке значення біта він отримав (рядок *3*). Після обміну достатньою кількістю частинок Аліса і Боб порівнюють базиси для кожної окремої частинки і відкидають випадки, в яких базиси не збігалися або Боб не реєстрував частинку. Біти, що залишаються, утворюють просіяний ключ (рядок *4*)

він зараз найчастіше реалізується на двох розділених у просторі модах — ця методика має назву фазового кодування бітів ключа [118]. Схема (див. рис. 13) складається з однофотонного джерела, яке знаходиться на боці Аліси, за ним встановлена світлоподільна пластинка, що ділить моду навпіл, фактично, змішуючи стан джерела з вакуумним станом. Далі до кожної з двох мод застосовується модуляція фази, при цьому один фазовий модулятор встановлений на боці Аліси, а інший — на боці Боба. Аліса прикладає до своєї моди один із чотирьох фазових зсувів, фактично вибираючи таким чином значення біта та базис. Значення біта 0, при цьому, відповідає зсувам 0 та $\pi/2$, а 1 — зсувам π та $3\pi/2$. Боб, в свою чергу, випадковим чином вибирає один з двох зсувів для своєї моди: 0 або $\pi/2$. Після цього Боб зводить дві отримані моди на своєму боці, застосовуючи свою світлоподільну пластинку, і спостерігає інтерференційну картину, встановлюючи детектори на кожному з двох виходів інтерферометра. Якщо спостерігається конструктивна інтерференція, то фотон детектується на виході "0", якому Боб співставляє таке саме значення біта, відповідно, якщо інтерференція деструктивна, то фотон спостерігається на виході "1". У випадку відсутності інтерференції фотон може бути отриманий на обох виходах. Якщо різниця фаз в плечах інтерферометра, тобто різниця між фазовими модуляціями Аліси і Боба, дорівнює 0 або π, то це означає, що Аліса і Боб застосовують сумісні базиси, а отже, отримують ідентичні результати. Після оголошення Бобом послідовності налаштувань фазового модулятора, які він застосовував, Аліса може визначити, в яких випадках базиси були сумісними і повідомити Бобу, коли саме він отримував правильні значення бітів — так само, як і в реалізації з поляризаційним кодуванням.

Проблемою такої схеми є те, що різниця фаз між плечима інтерферометра має бути сталою, що практично не можливо навіть на відстані кількох метрів. Тому для фазового кодування застосовується схема на основі двох незбалансованих інтерферометрів: Аліса ділить промінь на своєму боці, прикладає до однієї з половин зсув фази, зводить половини моди, вони разом, через один і той самий канал, поширюється до Боба; той ділить отриману моду, застосовує фазовий зсув до однієї з половин, зводить половини моди і спостерігає інтерференцію. Фактично у даному випадку можна казати про часове розділення мод. При цьому Боб змушений розрізняти три різні випадки шляху, пройденого світлом — або обидва рази короткі шляхи, або обидва рази довгі, або проміжний випадок — довгий шлях у Аліси й короткий у Боба

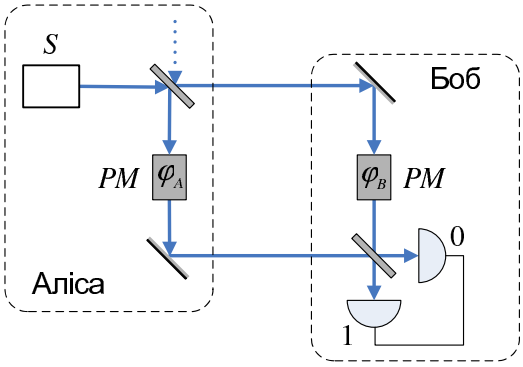

Рис. 13. Схема реалізації протоколу BB84 з фазовим кодуванням бітів ключа: S — джерело, PM — фазові модулятори

та навпаки. Якщо будувати часову залежність інтенсивності, то Боб буде спостерігати три максимуми, в середньому з який і варто шукати ознаки інтерференції. Ефективність такої схеми було підтверджено численними експериментами з передаванням ключа на відстані в кілька десятків кілометрів [119, 120]

У 1992 р. Беннет виявив, що чотирьох станів протоколу BB84 є більш ніж достатньо для реалізації квантової криптографії на основі кубітів — насправді квантово-криптографічний протокол, який отримав назву BB92, може бути реалізований за допомогою лише двох неортогональних станів [118]. Це уточнення зробило простішою реалізацію квантової криптографії на основі поодиноких кубітів, але на практиці виявилося не дуже добрим рішенням. В той час як два неортогональні стани не можуть бути розрізнені точно та без втручання, їх можна точно розрізнити за рахунок невеликих втрат якості, що було продемонстровано на практиці [121]. Для забезпечення захищеності протоколу BB92 було запропоновано застосування інтерференції макроскопічних лазерних імпульсів з послабленими імпульсами, які складаються з поодиноких кубітів. Інтерференція в цьому випадку допомагає відслідковувати підслуховування, оскільки Єва не може поглинути слабкий промінь, не зруйнувавши інтерференційну картину. Ця система відслідковування підслуховування була розширена й на оригінальний протокол BB84 [122].

Поряд з цім було запропоновано протокол, що застосовує шість різних станів кубітів (6-state protocol), які відображають симетрію сфери Пуанкаре [122], див. рис. 10. Шість станів утворюють три базиси, отже, ймовірність того, що Аліса і Боб виберуть один і той самий базис становить не $\frac{1}{2}$, як в BB84, а $\frac{1}{3}$. Але симетрія цього протоколу посилює його захищеність, зменшуючи інформаційний виграш Єви за тієї ж кількості виміряних (а отже, поглинутих) Євою фотонів, оскільки її втручання вносить в цьому випадку більше помилок.

Відомі також інші модифікації вищенаведених протоколів. Зокрема, Скарані та ін. в 2004 р. запропонували протокол SARG (названий за прізвищами авторів) [123]. Цей однокубітний протокол є модифікацією BB84 і може бути реалізований на тому ж самому обладнанні. Його основна відмінність полягає в застосуванні двох пар взаємно неортогональних станів (в той час як BB84 передбачає використання двох пар ортогональних станів). Відповідно змінено процедуру класичного узгодження після передачі — замість оголошення базисів, Аліса повідомляє, яку з двох пар вона застосовувала. Боб вгадує базис правильно, якщо отримує стан, ортогональний до одного з оголошених неортогональних станів. Оскільки під час розділення променя й вимірювання стану додаткових фотонів, Єва частіше отримує помилки, SARG дозволяє захищену передачу ключа на більших відстанях.

У 2003 р. Хвангом був запропонований протокол пасткових (decoy) станів [125], який має на меті протидію атакам проти реалізацій на послаблених імпульсах, а також дозволяє подовжити дистанцію захищеної передачі ключа. Для цього Аліса час від часу відправляє додатковий стан світла, інтенсивніший ніж стани, що застосовуються для кодування (але на тій самій довжині хвилі та синхронно за часом). Ці додаткові стани дозволяють викривати присутність Єви, яка не знає, коли decoy-стани відправляються, й не може їх ідентифікувати. Зміна інтенсивності цих станів дозволяє Бобу визначити намагання Єви здійснити ділення променя. Захищеність цього протоколу аналізувалася в роботах Ло та ін. [126].

7.3. Протокол Екерта — E91

Через сім років після повідомлення про BB84, в 1991 році, Екертом був запропонований протокол, який стали називати E91 [111]. На відміну від BB84 та подібних до нього в цьому протоколі для забезпечення захищеності використовується явище переплутування двох кубітів. Для експериментальної реалізації свого протоколу Екерт запропонував використовувати схему експерименту Аспекта та ін., див. розділ 6.

Отже, дворівневі системи, у найпростішому випадку — поляризовані фотони, готуються у белівському стані (158). При цьому один з фотонів направляється до Аліси, а інший — до Боба. Їх аналізатори випадковим чином налаштовуються на три різні ба-

зиси, повернуті відносно основного на кути 0, $\pi/4$, $\pi/8$ для Аліси, та 0, $-\pi/8$, $\pi/8$ для Боба. Після того як передано достатню кількість бітів, Аліса та Боб відкидають вимірювання, в яких хтось з них або обидва не зареєстрували жодного фотона, а потім через відкритий канал порівнюють орієнтації своїх аналізаторів в кожному окремому вимірюванні та ділять отримані значення бітів на дві частини. Перша — це випадки, в яких орієнтація аналізаторів була різною, друга — в яких орієнтація була однаковою.

За першою групою Аліса та Боб обчислюють значення параметра Белла (157). Воно має порушувати нерівність Белла (156) зі значенням $2\sqrt{2}$. З цього Аліса та Боб можуть зробити висновок стосовно того, чи мало місце несанкціоноване втручання в стан системи, тобто підслуховування. Якщо така перевірка не виявляє ознак порушення стану, то другий набір бітів, які були отримані в однакових базисах, можна вважати повністю антикорельованими, а отже, такими, які можна перетворити на криптографічний ключ, захищеність якого, таким чином, базується на перевірці нерівності Белла.

Наступного року після публікації E91 Беннет, Брассар і Мермін виступили з критикою цього протоколу, стверджуючи, що порушення нерівностей Белла не є необхідним для захищеності квантової криптографії, і підкреслюючи тісний взаємозв'язок між протоколами BB84 та E91 [127]. Втім реалізації квантової криптографії все одно відбувалися на базі як одного, так і другого протоколів, а суперечки з приводу захищеності протоколів та нерівностей Белла як способу її перевірки досі продовжуються. Тим не менш, квантове переплутання є одним з ключових ресурсів квантової інформатики, насамперед завдяки тому, що забезпечує кореляцію між квантовими вимірюваннями. Ця властивість переплутаних станів привела до розробки квантово-криптографічних протоколів у неперервних змінних, про які мова піде нижче.

7.4. Практичні аспекти реалізації

Як уже зазначалося, практична квантова криптографія реалізується на основі станів світла. Таким чином, будь-яка установка квантової криптографії складається з трьох основних елементів: джерела, оптичного каналу та детекторів. Тому, з точки зору практичної реалізації, інтерес становлять саме ці три складові частини.

Носіями інформації у квантово-криптографічних схемах є поодинокі фотони, параметрами станів яких (поляризацією, фазою тощо) кодуються біти ключа, який передається. Втім на практиці й досі немає ефективних засобів створення однофотонних фоківських станів (їх або навчилися поки що створювати лише всередині резонаторів, або, наприклад, однофотонні джерела мають суттєві невизначеності в часі випромінювання фотонів). Тому найчастіше як джерело для реалізації протоколу BB84 застосовують лазер, випромінювання якого суттєво ослаблюється. При цьому розподіл ймовірностей фотонів в моді є пуасонівським (26), а отже, ймовірність появи додаткових фотонів хоч і можна зробити якомога меншою, але її не вдається звести до нуля. При цьому поява зайвих фотонів в імпульсі може бути потенційно небезпечною, оскільки Єва може виміряти стан додаткового фотона, розділивши промінь, і лишитися при цьому непоміченою. Тому імпульси послабляють так, що вони містять набагато менше ніж один фотон в середньому, тобто переважна більшість імпульсів є порожніми. На практиці приблизно 90% імпульсів порожні, при цьому приблизно 5% непорожніх імпульсів виявляється двофотонними.

Для реалізації протоколу E91 застосовуються джерела переплутаних пар. Вони зазвичай базуються на параметричному діленні частоти в нелінійних кристалах, при якому фотон накачки породжує пару фотонів. Недоліком практичної реалізації такої схеми є широкий спектральний діапазон фотонів, які генеруються в процесі ділення частоти, що робить їх чутливішими до хроматичної дисперсії та вимагає спектрального фільтрування.

Як квантові канали застосовують або оптичне волокно, або передачу у відкритому просторі (тобто в повітрі). При цьому поширення фотонів у волокні супроводжується поглинанням, подвійним заломленням променя та хроматичною дисперсією, яка ускладнює реалізації на кодуванні бітів поляризацією. При цьому поглинання слабких сигналів у хвилеводах досить добре описується співвідношенням (118). У відкритому просторі поглинання більше за таке в волокні. Також необхідно враховувати наявність розсіяного світла. Крім того, за рахунок явищ турбулентності, які присутні в атмосфері, ефективність процесу проходження сигналу через атмосферу весь час флуктує. Тобто тепер співвідношення між початковим та кінцевим станами (118) потрібно ще й усереднювати за фазою. Водночас поширення в повітрі практично не змінює поляризаційні стани фотонів, у той час як в оптоволокні поляризація обертається в будь-якій неплоскій петлі. Тому, як вже зазначалося, для коду-

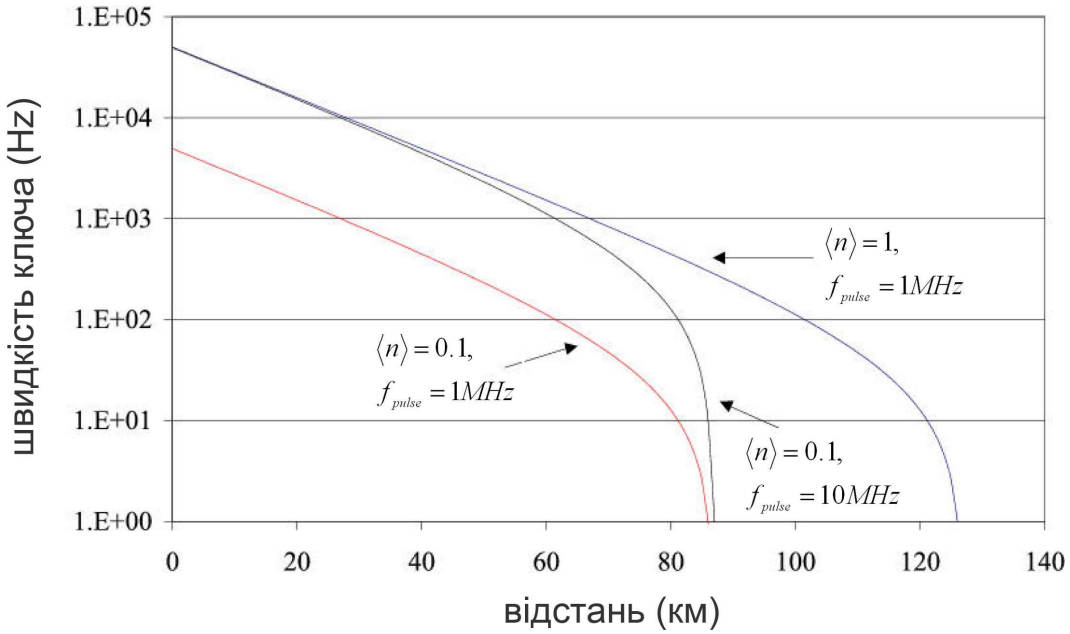

Рис. 14. Графіки залежності швидкості отримання таємного ключа від відстані передачі по оптичному волокну із стандартним затуханням 0,2 дБл/км, наведені для різних значень частот імпульсів f_{pulse} та середнього числа фотонів в імпульсі $\langle n \rangle$ [128]

вання поляризацією краще використовувати відкрите повітря, а для кодування фазою — хвилеводи.

Детектори є третім важливим елементом будь-якої квантово-криптографічної схеми. На практиці найчастіше застосовують лавинні фотодіоди, які працюють в режимі Гейгера. Проблемою таких пристроїв є суперечність між чутливістю та темними відліками, тобто мимовільним проходженням лавини з верхніх заселених рівнів діода. Крім того, існує суперечність між часом відновлення таких діодів і тими ж темними відліками. Ефективним рішенням виявляється схема подібна до того, що була використана в експерименті Львовського та Шапіро з виявлення некласичності "зашумленого" однофотонного фоківського стану, рис. 8 (див. розділ 5.2 та [44]). При цьому один з фотонів детектується менш ефективним, але й менш схильним до темних відліків "тригерним" детектором, який, за наявності відліку на ньому, активує основний, чутливіший детектор, який вже детектує стан основного, сигнального, фотона. Весь інший час сигнальний детектор вимкнений, що зменшує частоту темних відліків. Більш докладно про практичні аспекти і типи обладнання див. в [127].

Взагалі, існує суперечність між захищеністю квантової криптографії, яка вимагає послаблення імпульсів, та її ефективністю, оскільки велика частка порожніх імпульсів призводить до підсилення проявів недосконалості однофотонних детекторів, які схильні до темних відліків. Це можна бачити з узагальнення експериментальних даних, наведених на рис. 14 як графіки залежності швидкості отримання таємного ключа від відстані передачі по оптичному волокну із стандартним затуханням 0,2 дБл/км [128] для різних значень частот імпульсів f_{pulse} та середнього числа фотонів в імпульсі $\langle n \rangle$. Легко бачити, що швидкість передачі ключа (або, що те ж саме, максимальна відстань передачі) практично не залежить від частоти імпульсів, але зростає із збільшенням середнього числа фотонів, що, в свою чергу, вступає в суперечність із захищеністю протоколу, оскільки збільшує частку багатофотонних імпульсів, які можуть бути розділені Євою з наступним непомітним перехопленням інформації. Ця суперечність вимагає як розробки більш ефективних джерел та детекторів, так і створення принципово нових протоколів квантової криптографії, основаних на кодуванні неперервними квантовими змінними, в яких більшість актів вимірювання була б інформативною.

7.5. Захищеність квантової криптографії

Оскільки основна задача квантової криптографії полягає в розробці методів для гарантовано секретної передачі криптографічних ключів, то питання

захищеності є найсуттєвішим при аналізі квантово-криптографічних протоколів. При цьому існує два загальних підходи до визначення захищеності, які розрізняються за рівнем припущень, зроблених щодо можливостей Єви, яка намагається здійснити перехоплення інформації, — це повний та практичний доказ захищеності.

Повний доказ означає, що захищеність гарантується від будь-яких підслуховуючих атак в "ідеальному" припущені, що Єва застосовує не лише найсучасніші сьогоденні технології, але й будь-які можливі технології майбутнього й обмежена лише законами квантової механіки. Такі докази здійснюються в контексті інформаційної теорії, вони мають форму теорем і зводяться до доведення того, що Єва не володіє інформацією про ключ після його остаточної обробки. Результатами таких доказів є, зокрема, визначення верхньої межі кількості помилок в просіяному ключі, за якої ключ ще може бути перетворено на криптографічний, який стане гарантовано захищеним.

Натомість, практичні докази захищеності враховують сучасний стан розвитку технологій і зосереджуються на практично можливих реалізаціях каналів та обладнання для перехоплення інформації. Вони розглядають конкретні техніки перехоплення, які Єва може застосовувати, і зводяться до доведення того, що вплив Єви у випадку такого реалістичного перехоплення інформації може бути помічений внаслідок внесення помилок, або що її знання про просіяний ключ буде достатньо малим, щоб після застосування алгоритмів підсилення захищеності воно звелося нанівець.

Декілька основних реалістичних способів перехоплення вважаються потенційно небезпечними для протоколів квантової криптографії, і відносно них розглядається практична захищеність. Це, зокрема, перехоплення — повторна відправка, коли Єва здійснює вимірювання спостережуваної, застосованої для кодування, поглинаючи при цьому фотони, а потім намагається перевипромінити їх знову. Крім того, Єва може здійснити атаку з діленням променя, розраховуючи на наявність в імпульсі додаткових фотонів. В цьому випадку вона вимірює стан "зайвого" фотона і лишається при цьому непоміченою (втім ця схема не є ефективною стосовно протоколів на основі сплутаних пар, оскільки додаткові фотони в тому ж часовому вікні не обов'язково будуть в такому ж стані). Крім того, Єва може комбінувати ці техніки — наприклад, ділити промінь, детектувати обидва виходи світлоподільної пластинки і/або відправляти Бобу лінійну комбінацію отриманих результатів, якщо фотонів виявилося два, або зводити техніку до перевипромінювання, якщо фотон був один. Крім того, вона може здійснювати вимірювання в так званому проміжному базисі (для випадку реалізації поляризаційними станами з випадковим вибором між вертикально-горизонтальним та діагональним базисом, проміжним буде базис $\pi/8$), що може бути ефективнішим, ніж просте угадування базисів. В більш складних та загальних випадках Єва може забезпечувати взаємодію фотона, що є носієм біта ключа, із своєю додатковою квантовою системою, незначно порушуючи стан фотона та визначаючи потім значення біта із вимірювань своєї квантової системи.

Варто зазначити, що ефективність тих чи інших практичних способів перехоплення часто залежить від безпосередньої схеми реалізації протоколу. Крім того, критично важливим може виявитись рівень шуму в каналі та рівень помилок детектування. (Для загального огляду технік перехоплення, доказів доведення та практичних аспектів захищеності див. [127]).

7.6. Кодування неперервними змінними

Як зазначалося, суттєвим недоліком, який обмежує ефективність квантової криптографії, є той факт, що переважна більшість актів вимірювання, тобто комунікаційних актів, виявляється не результативною. І хоча, якщо вже окремий фотон дістався таки до віддаленого детектора, то майже напевно буде детектований адекватно вибраному базису, ця обмеженість ефективності викликає необхідність розробки таких протоколів квантової криптографії, в яких всі або більшість актів вимірювання були б інформативними. Цю мету може бути досягнуто в разі застосування інтенсивних променів та кодування інформації неперервними змінними (continuous variables). Теорію некласичності для таких систем було викладено в перших розділах цього огляду.

Один з перших таких протоколів був розроблений Хіллері [130], який в 2000 р. запропонував схему, що ґрунтується на застосуванні стисненого світла, а біти ключа кодуються значеннями стисненої квадратури поля (які отримуються шляхом гомодинного детектування, див. розділ 2.1). При цьому Аліса випадково вибирає, яку саме квадратуру стискати та застосовувати для кодування, а Боб так само випадково вибирає, яку з квадратур вимірювати. Ця процедура, яка є аналогом вибору базисів у протоколі BB84, забезпечує захищеність протоколу, оскільки Єва, яка намагається перехопити ключ, не може виміряти обидві квадратури одночасно однаково точно внаслідок

дії принципу невизначеності. Отже, знання Єви про послідовність бітів, отриману Бобом з вимірювань квадратури, вдається зробити достатньо малим задля перетворення цієї послідовності на криптографічний ключ. Крім того, вимірювання, які здійснює Єва, порушують стан, що може бути визначено відповідним аналізом випадково вибраних бітів ключа. Захищеність протоколу було показано стосовно реалістичних атак з вимірюванням та повторною відправкою та з діленням променя. Недоліками даної схеми є те, що вона доволі чутлива до втрат, які зменшують ступінь стиснення (хоча автором і було запропоновано застосування підсилювачів для збільшення відстані передавання), а забезпечення захищеності вимагає високого ступеня стиснення станів, що є технічно складним.

Задля вдосконалення описаного протоколу Церф [130] у 2001 р. запропонував застосовувати не повністю випадкові значення модуляції, а такі, що належать до гаусівського розподілу, тобто фактично накладати на стиснений стан гаусівський шум, наголошуючи на тому, що це робить неперервним не лише квантову змінну, яка застосовується для кодування, а й сам ключ, який потім дискретизується із застосуванням додаткових алгоритмів підсилення захищеності. Було показано, що у випадку атаки з клонуванням стану, за ідеальних умов передачі, кількість інформації, отриманої Бобом, зменшується на величину отриманої Євою кількості інформації.

Згодом Готтсман та Прескілл [132] довели, що гаусівський характер квадратурних модуляцій стисненого променя не є необхідним для забезпечення захищеності протоколу. Проте він виявляється корисним при кодуванні квадратурами звичайного когерентного стану (див. розділ 3.2). Більш того, описані ними додаткові алгоритми підсилення захищеності дозволили провести доведення безумовної захищеності отриманого ключа для протоколів на основі стиснених станів, що є поки що єдиним подібним доведенням в квантовій криптографії на основі неперервного кодування. Втім дана робота лише підтвердила суворі вимоги схем з неперервним кодуванням щодо якості експериментальної техніки та рівня шуму в каналі.

Ральф [132] у 1999 р. описав дві схеми, які розширювали ідеї однокубітної квантової криптографії на багатофотонні стани. Перша схема є подібною до кодування квадратурами стисненого світла, описаного Хіллері, з тією різницею, що застосовується звичайне інтенсивне когерентне світло. Аліса кодує дві послідовності бітів середніми значеннями двох різних квадратур. Боб випадково вибирає одну з них для здійснення гомодинного детектування. Відкритим каналом Боб повідомляє Алісі, яку саме квадратуру він вимірював кожного разу. В роботі було показано, що захищеність такої схеми, незважаючи на принцип невизначеності, який забороняє Єві однаково точно детектувати дві квадратури, є недостатньою, порівняно з однофотонними схемами.

Розвиток ідеї кодування неперервними змінними полягав у застосуванні стиснення та квадратурного переплутування. У відповідній схемі Аліса кодує дві випадкових послідовності амплітудними квадратурами двох стиснених променів — $\hat{a}$ та $\hat{b}$ — з фіксованою фазою. Далі один з променів відчуває фазовий зсув на $\pi/2$, і промені змішуються на симетричній світлоподільній пластинці, у результаті чого отримуються два промені у вихідних модах $\hat{c}$ та $\hat{d}$, які перебувають у переплутаному стані. Додатково до кожної з мод домішуються дві когерентні моди (локальні осцилятори) такої ж інтенсивності та з поляризаціями, ортогональними відносно мод $\hat{c}$ і $\hat{d}$, після чого до однієї з мод застосовується випадкова часова затримка й моди відправляються Бобу. Остання процедура знищує взаємну когерентність між модами, що є додатковим засобом підсилення захищеності, оскільки пряме змішування мод на світлоподільній пластинці не приведе тепер до відтворення станів $\hat{a}$ та $\hat{b}$.

Застосовуючи поляризаційні світлоподільні пластинки, Боб виділяє з мод локальні осцилятори, які, маючи такі ж часи затримки, як і оригінальна сигнальна мода, можуть застосовуватись для гомодинного детектування, з якого Боб може отримати знання про стани мод $\hat{a}$ та $\hat{b}$. Захищеність даної схеми забезпечується принципом невизначеності для квадратур та підсилюється фазовим шумом в модах, що унеможливлює безпосереднє визначення початкових станів без їхнього порушення. Тем не менше, аналіз впливу втрат в каналі показує, що описана схема є набагато чутливішою до втрат порівняно з однокубітними схемами. Згодом було показано [134], що найефективнішою стратегією для Єви з точки зору мінімізації внесення помилок в канал є застосування квантової телепортації, що вимагає великого ступеня стиснення станів для забезпечення захищеності та робить протокол ще більш чутливим до втрат.

Розвитком схеми з відправкою Бобу двох квадратурно-переплутаних променів стало змішування когерентного променя, амплітудою якого кодується ключ, з двома квадратурно-переплутаними променями, створеними в невиродженому параметричному підсилювачі, як було описано Перейрою та ін. [135]. Ці два ортогонально-поляризованих промені, які ві-

діграють роль шуму, після змішування з сигнальним когерентним променем, розділяються в просторі і передаються Бобу, який здійснює незалежні гомодинні вимірювання квадратур променів і з їх різниці відновлює сигнальний промінь. Така схема дозволяє отримати повідомлення в ідеальному випадку з тим самим співвідношенням сигнал-шум, що й в оригінального джерела, хоч в процесі поширення це співвідношення для кожного з двох променів є набагато меншим за одиницю. Експериментальні дані підтвердили можливість подавлення шуму різниці фототоків двох мод до рівня, меншого за дробовий (див. розділ 2). У випадку реалістичних спроб перехоплення ключа в описаній схемі Єва вносить додатковий шум у результати вимірювань Боба, за яким перехоплення може бути детектоване. Втім описаний протокол, крім відсутності повного доведення захищеності, вимагає високих ступенів нелінійності в підсилювачі світла, що створює практичну складність реалізації.

Внаслідок складності реалізації протоколів на основі стисненого світла продовженням розробки схем квантової криптографії на основі неперервних змінних став протокол, описаний Гроссансом і Гран'є [136], в якому передбачається застосування когерентних станів, в яких амплітуда α підкоряється гаусівському розподілу. Боб випадково вимірює одну з квадратур. Далі до отриманих результатів застосовується специфічний алгоритм узгодження базисів, що перетворює результати на послідовність бітів, з яких із застосуванням алгоритмів дистиляції отримується криптографічний ключ, захищеність якого показано стосовно реалістичних спроб перехоплення. При цьому захист базується на теоремі про неможливість клонування, що, як показано, обмежує роздільну здатність можливих вимірювань в каналі, а отже, інформаційний виграш Єви при таких вимірюваннях. Згодом описану схему було реалізовано експериментально [137].

Розширення ідеї протоколу E91 на кодування неперервними змінними було здійснено Рейдом [137] у 2000 р. Аліса генерує квадратурно-сплутаний стан, застосовуючи невироджений параметричний підсилювач, при цьому на один з його входів подається вакуумний стан, а на інший вхід Аліса подає когерентний стан, який має одну з двох інтенсивностей, що відповідають двом значенням біта. Вихідні моди підсилювача розділяються в просторі, одна з них отримується Бобом, інша — Алісою.

Боб здійснює вимірювання однієї з двох випадково вибраних квадратур своєї моди, з яких визначає значення біта, відправленого Алісою, оскільки різним вхідним модам підсилювача відповідає різний статистичний розподіл результатів квадратурних вимірювань. Крім того, Боб фіксує флуктуації отриманих результатів. Аліса так само здійснює послідовність квадратурних вимірювань, реєструючи відхилення отриманих значень від середніх, які відповідають відправленому біту. Після цього через класичний канал Боб та Аліса обчислюють дисперсії виміряних квадратур і перевіряють переплутаність, див. розділ 5.4. Захищеність протоколу було показано відносно реалістичного перехоплення з діленням променя як наслідок помітного порушення квантових кореляцій та внесення помилок у послідовність бітів при його здійсненні.

Іншим варіантом ЕПР-протоколу, що базується на вимірюванні двох квадратурно-переплутаних стиснених променів та досліджені їхніх кореляцій, став протокол, описаний Зільберхорном із співавторами [139]. Пасивному вибору базисів тут відповідає випадкове обрання однієї з квадратур для вимірювання. Як і в оригінальному протоколі E91, біти ключа в даній схемі не відправляються Алісою, а випадковим чином генеруються в процесі вимірювання в разі збігу вибраних спостережуваних. Захищеність протоколу базується на чутливості квантових кореляцій до впливу Єви, який проявляється при її спробах перехопити ключ, як було показано для випадків реалістичного перехоплення.

Протокол з кодуванням числами фотонів був запропонований Фанком та Реймером [139] в 2002 р. Він передбачав кодування Алісою бітів ключа в середньому значенні різниці числа фотонів двох сильнокорельованих інтенсивних мод, які розрізняються за ортогональними поляризаціями та створюються у нелінійному процесі параметричного підсилення. Сильна кореляція між модами приводить до того, що різниця в числах фотонів є добре визначеною і має субпуасонівську статистику, тобто проявляє некласичну поведінку. Було показано, що втручання Єви в канал руйнує цю некласичність, а отже, реалістичні спроби перехоплення стають помітними. Для додаткового ускладнення перехоплення ключа дві моди, які виходять в напрямку Боба, можуть випадково обертатися поляризатором на кут $\pi/4$, а Боб випадково вибирає, в якому поляризаційному базисі здійснювати вимірювання. Описаний протокол був реалізований у 2003 р. Жангом та ін. [140].

Інший протокол, що передбачає кодування числами фотонів та базується на некласичності їхньої статистики запропонували Усенко та Лев [141]. В ньому біти кодуються флуктуаціями чисел фотонів двох

сильнокорельованих мод особливого когерентно скорельованого стану світла. Субпуасонівська статистика кожної з двох мод дозволяє викривати реалістичні спроби перехоплення з клонуванням стану, які порушують цю статистику, в той час як ділення променя руйнує кореляцію між Алісою та Бобом. Перевагою застосування неперервних змінних, при цьому, є можливість розширення алфавіту кодування числами фотонів, яке приводить до збільшення ефективності та захищеності протоколу [143].

Узагальнюючи наведені протоколи, варто відзначити, що схеми [134, 137] можна фактично представити як передачу модульованого променя зі зниженим рівнем шуму. Для того щоб позбавити Єву можливості безпосереднього вимірювання такого променя, він змішується із шумовими модами. Аналогічно квантові властивості добре визначених параметрів світла, які мають шум менший за дробовий, знайшли своє застосування в протоколах з кодуванням числами фотонів [141, 142]. Протоколи на базі сплутаних станів, як і в однокубітній квантовій криптографії, основані на квантових кореляціях між вимірюваннями та перевірці некласичності цих кореляцій із застосуванням відповідного критерію перевірки (див. розділ 5).

Основною проблемою протоколів з неперервними змінними є відсутність, в переважній більшості випадків, повного безумовного доведення їхньої захищеності (для огляду питань захищеності таких протоколів див. [83]). Крім того, на відміну від однокубітних протоколів, в яких дискретні змінні, як правило, або зберігаються в процесі поширення, або можуть бути відновленні після компенсації впливу оточення, неперервні змінні відчувають так само неперервний вплив оточення, який, як правило, не може бути усунений, а отже, питання впливу втрат та шуму на захищеність протоколу часто лишається відкритим і вимагає окремих досліджень з урахуванням безпосереднього способу реалізації протоколу.

Обмеженням ефективності деяких з описаних протоколів є необхідність випадкового вибору базисів, що є спадщиною однокубітних протоколів і приводить до того, що половина актів вимірювання відкидається. Крім того, наведені протоколи мають і суттєві технічні труднощі в реалізації. Для протоколів з квадратурним кодуванням це, серед іншого, необхідність узгодження фази сигнального променя та локального осцилятора, який застосовується для гомодинного детектування квадратур. Це, зокрема, стосується схеми [129] та безумовної захищеної схеми [131]. Складною експериментальною задачею є створення стиснених станів, особливо з великим ступенем стиснення. Це, а також створення сильнокорельованих променів вимагає високих нелінійностей в процесі генерації, а також високоякісної експериментальної техніки.

З огляду на все це квантово-криптографічні протоколи на неперервних змінних досі залишаються перспективним напрямком розробок та досліджень, у той час як практичне, а тим більше, комерційне застосування квантової криптографії відбувається на основі однокубітних протоколів. Тим не менш, розвиток захищених квантових комунікації з неперервним кодуванням є корисним з фундаментальної точки зору і закладає базис для ефективної реалізації схем на основі неперервних змінних в майбутньому.

8. Висновки

Дослідження некласичних властивостей квантових станів речовини та поля випромінювання дивним чином зосередили в собі як шляхи пошуку відповідей на найбільш глибинні питання природознавства, так і розробку прикладних напрямів у сфері інформаційних технологій, надточних вимірювань тощо. Проблема індетермінізму є ключовим питанням, яке так чи інакше виникає в квантовій теорії. В класичній фізиці ймовірність з'являється лише як наслідок неповноти наших знань про систему. Цієї неповноти можна, принаймні в принципі, позбутися, передбачивши точні значення всіх спостережуваних, в довільний момент часу.

В квантовому випадку ймовірність є фундаментальною властивістю матерії, і з цієї причини, навіть якщо стани системи характеризуються точними значеннями однієї змінної (наприклад, координати), згідно з принципом доповненості значення будь-якої спостережуваної, яка не комутує з нею (наприклад, імпульсу), невизначено. На мові представлень фазового простору це означає, що далеко не всі функції розподілу, дозволені теорією ймовірностей, можуть відповідати функції Вігнера реального фізичного стану. З іншого боку, серед фізично реалізованих станів є такі, функції Вігнера яких набувають від'ємних значень, і з цієї причини їх не можна інтерпретувати як розподіл ймовірностей.

Слід особливо підкреслити неможливість отримання квантової теорії з будь-якого "розширеного" варіанта класичної. Глибинною причиною цього є те, що ці дві теорії розрізняються означенням двох операцій для спостережуваних величин — добутку та дужки. Саме вони визначають всі динамічні та, й що є найважливішим, статистичні відмінності між кван-

товою та класичною теоріями. Тому така теорія, якщо б вона була можлива, повинна була б, у першу чергу, показати, яким чином некомутативний добуток та коммутатор (дужка Мояла) в квантовій теорії можуть бути отримані з комутативного добутку та дужки Пуассона в класичній. Звичайно, можливий і інший варіант, який власне й мали на увазі Ейнштейн, Подольський та Розен, — неповнота самої квантової теорії або просто її неадекватність реальному світу. Але експерименти, які є на сьогодні, підтверджують лише протилежне, тобто правильність і повноту квантової теорії.

Функція Вігнера може бути відновлена на експерименті багатьма способами, наприклад методом квантової томографії. В цьому випадку некласичність — це є експериментально спостережуване протиріччя між теорією ймовірностей і повністю класичною електродинамікою. Тим не менш, від'ємність функції Вігнера — не єдиний прояв некласичних властивостей. Квантова природа фотодетектора в усіх випадках приводить до появи так званого дробового шуму. Навіть для поля, що генерується ідеальним лазером, кількість фотовідліків є випадковою величиною, яка розподілена згідно з пуасонівською статистикою. Для будь-якого іншого класичного світла, статистика фотовідліків носить суперпуасонівський, тобто більш стохастичний, характер. Зокрема, це стосується термального світла, яке має додатний надлишковий шум. Однак для квантового світла цей надлишковий шум може характеризуватися негативною дисперсією. При цьому функція Вігнера для такого світла може й не мати від'ємних значень. Причина цього полягає в тому, що відповідно до формули Мандела, статистика фотовідліків визначається не симетризованими, а нормально впорядкованими величинами. Тому даний тип некласичності визначається не функцією Вігнера, а функцією Глаубера—Сударшана.

Некласичність відносно розподілу Глаубера—Сударшана включає в себе практично всі відомі типи некласичності, в тому числі й переплутування. Дійсно, функція Глаубера—Сударшана переплутаного стану завжди не є додатно визначеною. Обернене твердження, взагалі кажучи, неправильне. В принципі, саме по собі явище переплутування (або несепарабельності) можна інтерпретувати, як наявність досить специфічних квантових кореляцій, за яких ймовірність генерації певних квантових станів для різних ступенів вільності формально має від'ємні значення.

Однією з найважливіших властивостей квантових станів є неможливість їх клонування. Іншими словами, спроба переписування квантової інформації з одного носія на інший завжди приведе до її знищення на джерелі. Саме цей факт активно використовують в квантовій криптографії при передачі кориптографічного ключа. Всі подібні алгоритми ґрунтуються на тому факті, що несанкціонований доступ неминуче приводить до зміни початкового квантового стану. А це, в свою чергу, може бути зареєстроване відправником і отримувачем конфіденційної інформації. Найбільшою проблемою при цьому є відокремлення повністю закономірних шумів, пов'язаних з втратами на лінії передачі, від втрат, пов'язаних з несанкціонованим доступом. Тому коректно говорити лише про кількість інформації, яку може отримати підслуховуюча сторона, а не про абсолютний захист. У будь-якому випадку, некласичні властивості квантових станів пропонують принципово нові можливості в галузі обробки і передачі інформації. Їх всебічне дослідження обіцяє привести до досить серйозного технологічного прориву в інформаційних технологіях XXI століття.

Автори цього огляду висловлюють свою щиру подяку багатьом своїм колегам, з якими вони співпрацювали, дискутували та обговорювали різноманітні аспекти некласичності квантових станів. Зокрема А.О.С., В.К.У. та Б.І.Л. вдячні П.М. Томчуку, О.О. Чумаку, О.В. Турчину з Інституту фізики НАН України за обговорення та цікаві поради. Слід також зазначити, що ця робота не була б можливою без плідних дискусій та співпраці А.О.С. та Є.В.Щ. із своїми колегами в Університеті Ростока (ФРН), а саме В. Фогелем (W. Vogel), Т. Ріхтером (Th. Richter), С. Валентовіцем (S. Wallentowitz) та Д. Івановим. А.О.С. та Б.І.Л. вдячні також Дж. Клаудеру (J. Klauder) з Університету Флориди (США) за його увагу до нашої роботи та плідну співпрацю і допомогу. А.О.С. та Є.В.Щ. висловлюють свою подяку В.І. Маньку з Фізичного інституту ім. П.М. Лебедєва Російської академії наук за цікаві дискусії та обговорення різноманітних аспектів некласичності. А.О.С. також вдячний Президенту України за стипендію Президента України для молодих науковців. А.О.С. та Є.В.Щ. висловлюють подяку Deutsche Forschungsgemeinschaft, а В.К.У. — Landau Network та NATO за фінансову підтримку.

1. C.E. Shannon, Bell Syst. Technol. J. **28**, 656 (1949); C.E. Shannon and W. Weaver, *The Mathematical Theory of Communication* (Univ. Illinois Press, Urbana Ill., 1949); К. Шеннон, *Работы по теории информации и кибернетике*, (Изд-во иностр. лит., Москва, 1963).

2. D.-G. Welsch, W. Vogel, T. Opartný, Progr. Opt. **39**, 63 (1999).
3. E. P. Wigner, Phys. Rev. **40**, 749 (1932).
4. D.N. Klyshko, Physics-Uspekhi **41**, 885 (1998); Д.Н. Клышко, УФН, **168**, 975 (1998).
5. A. Einstein, B. Podolsky, N. Rosen, Phys. Rev. **47**, 777 (1935).
6. M.B. Menskii, Physics-Uspekhi **48**, 389 (2005); М.Б. Менский, УФН. **175**, 413 (2005).
7. N. Bohr, Phys. Rev. **48**, 696 (1935).
8. E. Schrödinger, Naturwissenschaften **23**, 807, 823, 844 (1935); Proc. Am. Phil. Soc. **124**, 323 (1980); Э. Шредингер, Успехи Химии **5**, 390 (1936).
9. J.S. Bell, Physics **1**, 195 (1964); *Speakable and Unspeakable in Quantum Mechanics* (Cambridge Univ. Press, Cambridge, 1997), p.14.
10. A. Aspect, G. Roger, S. Reynaud, J. Dalibard, C. Cohen-Tanoudji, Phys. Rev. Lett. **45**, 617 (1980); A. Aspect, P. Grangier, G. Roger, Phys. Rev. Lett. **47**, 460 (1981); A. Aspect, J. Dalibard, G. Roger, Phys. Rev. Lett. **49**, 1804 (1982); A. Aspect, Nature **398**, 189 (1999).
11. R. Short, L. Mandel, Phys. Rev. Lett. **51**, 384 (1983).
12. R. Slusher, L. Hollberg, B. Yurke, J. Mertz, and J. Valley, Phys. Rev. Lett. **55**, 2409 (1985).
13. M.K. Teich and B.E.A. Saleh, Quantum Optics **1**, 153 (1989); М.К. Тайш, Б.Э.А. Салэ, УФН **161**, 101 (1991).
14. *The Physics of Quantum Information*, ed. by D. Bouwmeester, A. Ekert, A. Zeilinger (Springer, Berlin Heidelberg, 2000); *Физика квантовой информации*, под ред. Д. Бауместера, А. Экерта, А. Цайлингера (Постмаркет, Москва, 2002).
15. R. Feynman, Int. J. Theor. Phys. **21**, 467 (1982); D. Deutsch, Proc. R. Soc. London A **400**, 97 (1985).
16. P. Shor, *Proc. of 35th Annual Symposium on the Foundations of Computer Science* (IEEE Computer Society, Los Alamos, 1994), p. 124; S.I.A.M. Journal of Computing **26**, 1484 (1997);[quant-ph/9508027].
17. R. Riverst, A. Shamir, and L. Adleman, *On Digital Signatures and Public-Key Cryptosystems*, MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212 (January 1979); Communications of the ACM **21(2)**, 120 (1978).
18. A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography* (CRC Press, Inc., 1997); С.Г. Баричев, В.В. Гончаров, Р.Е. Серов, *Основы современной криптографии* (Горячая Линия – Телеком, Москва, 2001).
19. S. Wiesner, SIGACT News **15**, 78 (1983); W.K. Wootters and W.H. Zurek, Nature **299**, 802 (1982).
20. C.H. Bennet, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
21. C.H. Bennet and G. Brassard, in *Proc. IEEE Int. Conf. on Computers, Systems and Sygnal Processing* (IEEE, New York, 1984); C.H. Bennet, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptol. **5**, 3 (1992).
22. A. Trifonov and A. Zavriyev, J. Opt. B. **7**, S772 (2005); http://magiqtech.com.
23. http://www.idquantique.com.
24. Ch. T. Lee, Phys. Rev. A. **44**, R2775 (1991).
25. A.A. Semenov, D.Yu. Vasylyev, B.I. Lev, J. Phys. B: At. Mol. Opt. Phys. **39**, 905 (2006).
26. A. Orlowski, H. Paul, Phys. Rev. A. **50**, 921 (1995).
27. H.P. Yuen and V.W.S. Chan, Opt. Lett. **8**, 177 (1982).
28. L. Mandel, E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, 1995); Л. Мандель, Э. Вольф, *Оптическая когерентность и квантовая оптика* (Физматлит, Москва, 2000).
29. W.P. Schleich, *Quantum Optics in Phase Space* (Wiley–WCH, Berlin, 2001); В.П. Шляйх, *Квантовая оптика в фазовом пространстве* (Физматлит, Москва, 2005).
30. W. Vogel and D.-G. Welsch, *Quantum Optics* (Wiley–VCH, Berlin, 2006).
31. J. Radon, Ber. Verh. Sächs. Akad. Wiss. Leipzig, Math.-Nat. Kl. **69**, 262 (1917).
32. F. Natterer, *The Mathematics of Computerized Tomography* (Wiley, Chichester, 1986).
33. J. Bertrand, P. Bertrand, Found. Phys. **17**, 397 (1987).
34. K. Vogel, H. Risken, Phys. Rev. A. **40**, 2847 (1989).
35. D.T. Smithey, M. Beck, M.G. Raymer, A. Faridani, Phys. Rev. Lett. **70**, 1244 (1993).
36. D.N. Klyshko, A.V. Masalov, Physics-Uspekhi **38**, 1203 (1995); Д.Н. Клышко, А.В. Масалов, УФН. **165**, 1249 (1995).
37. L. Mandel, Proc. Phys. Soc. (London) **72**, 1037 (1958).
38. L. Mandel, E.C.G. Sudarshan, and E. Wolf, Proc. Phys. Soc. **84**, 435 (1964).
39. J.R. Klauder, E.C.G. Sudarshan, *Fundamentals of Quantum Optics* (Dover Publication, Inc., New York, 2006); Дж. Клаудер, Э. Сударшан, *Основы квантовой оптики* (Мир, Москва, 1970).
40. R.J. Glauber, Phys. Rev. Lett. **10**, 84 (1963); Phys. Rev. **131**, 2766 (1963).
41. E.C.G. Sudarshan, Phys. Rev. Lett. **10**, 277 (1963).
42. W. Vogel, Phys. Rev. Lett. **84**, 1849 (2000).
43. Th. Richter and W. Vogel Phys. Rev. Lett. **89**, 283601 (2002).
44. E. Shchukin and W. Vogel, Phys. Rev. A. **72**, 043808 (2005).
45. A. Lvovsky and J. Shapiro, Phys. Rev. A. **65**, 033830 (2002).
46. L. Mandel, Opt. Lett. **4**, 205 (1979).
47. D.F. Walls and G.J. Milburn, *Quantum Optics* (Springer, Berlin, 2006).
48. L.A. Wu, H.J. Kimble, J.L. Hall, and H. Wu, Phys. Rev. Lett. **57**, 2520 (1986); L.A. Wu, M. Xiao, and H.J. Kimble, J. Opt. Soc. Am. B.**4**, 1465 (1987).
49. H.P. Yuen and J.H. Shapiro, Opt. Lett. **4**, 334 (1979).
50. C.M. Caves, Phys. Rev. Lett. **45**, 75 (1980).
51. M. Xiao, L.A. Wu, and H.J. Kimble, Phys. Rev. Lett. **59**, 278 (1987).
52. P. Grangier, R.E. Slusher, B. Yurke, A. La Porta, Phys. Rev. Lett. **59**, 2153 (1987).

53. Ю.М. Широков, ТМФ.**25**, 307 (1975); **28**, 308 (1976); **29**, 309 (1976); **30**, 6 (1977).
54. Ю.М. Широков, ФЭЧАЯ. **10**, 5 (1979).
55. H. Weyl, *The Theory of Groups and Quantum Mechanics* (Dover Publications, Inc., 1931); Г. Вейль, *Теория групп и квантовая механика* (Наука, Москва, 1986).
56. A.M. Perelomov, *Generalized Coherent States and Their Applications* (Springer, Berlin, 1987); А. М. Переломов, *Обобщённые когерентные состояния и их применения* (Наука, Москва, 1978).
57. C. Zachos, Int. J. Mod. Phys. A. **17**, 297 (2002).
58. J. von Neumann, Math. Ann. **104**, 570 (1931).
59. J.E. Moyal, Proc. Cambr. Phil. Soc. **45**, 99 (1949).
60. H. Groenewold, Physica **12**, 405 (1946).
61. V.I. Tatarskii, Sov. Physics–Uspekhi **26**, 311 (1983); В.И. Татарский, УФН **139**, 587 (1983).
62. E. Schrödinger, Naturwissenschaften **14**, 664 (1926).
63. V.V. Dodonov, J. Opt. B. **4**, R1 (2002).
64. J.R. Klauder, B.-S. Skagerstam, *Coherent States, Applications in Physics and Mathematical Physics* (World Scientific, Singapore, 1985).
65. И.А. Малкин, В.И. Манько, *Динамические симметрии и когерентные состояния* (Наука, Москва, 1973).
66. J.R. Klauder, J. Math. Phys. **4**, 1055,1058 (1963); **6**, 68 (1965).
67. K. Husimi, Proc. Phys. Math. Soc. Japan **22**, 264 (1940).
68. Y. Kano, J. Math. Phys. **6**, 1913 (1965).
69. П.І. Голод, А.У. Клімик, *Математичні основи теорії симетрій* (Наук. Думка, Київ, 1992).
70. K.E. Cahil, R.J. Glauber, Phys. Rev. **177**, 1857, 1882(1969).
71. Ф.А. Березин, *Метод вторичного квантования* (Наука, Москва, 1986).
72. G. Alexanian, A. Pinzul, and A. Stern, Nucl. Phys. B. **600**, 531 (2001).
73. G.M. D'Ariano, S. Mancini, V.I. Man'ko, P. Tombesi, Quant. Semiclass. Opt. **8**, 1017 (1996); S. Mancini, V. Man'ko, P. Tombesi, J. Mod. Opt. **44**, 2281 (1997).
74. L.M. Johansen and A. Luis, Phys. Rev. A. **70**, 052115 (2004).
75. L.M. Johansen, Phys. Rev. Lett. **93**, 120402 (2004).
76. L.M. Johansen, J. Opt. B. **6**, L21 (2004).
77. I.V. Bargatin, B.A. Grishanin, and V.N. Zadkov, Physics-Uspekhi **44**, 597 (2001); И.В. Баргатин, Б.А. Гришанин, В.Н. Задков, УФН. **171**, 625 (2001).
78. M.B. Menskii, Physics - Uspekhi **43**, 585 (2000); М.В. Менский, УФН **170**, 631 (2000).
79. R.V. Bussey, Phys. Lett. A. **90**, 9 (1982).
80. Б.Б. Кадомцев, *Динамика и информация* (УФН, Москва, 1997).
81. A. Steane, Rep. Progr. Phys. **61**, 117 (1998).
82. S.Ya. Kilin, Phys.-Usp. **42**, 435 (1999); С.Я. Килин, УФН. **169**, 507 (1999).
83. S.L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
84. R.F. Werner, Phys. Rev. A. **40**, 4277 (1989).
85. A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
86. M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A. **223**, 1 (1996); Phys. Rev. Lett. **80**, 5239 (1998).
87. H.-P. Breuer, Phys. Rev. Lett. **97**, 080501 (2006).
88. S. Bochner, Math. Ann. **108**, 378 (1933).
89. E. Joos and H.D. Zeh, Z. Phys. **59**, 223 (1985).
90. C. W. Gardiner and P. Zoller, *Quantum Noise* (Berlin, Springer, 2000).
91. L. Knöll, S. Scheel, E. Schmidt, D.-G. Welsch, and A.V. Chizhov, Phys. Rev. A. **59**, 4716 (1999).
92. *Cavity Quantum Electrodynamics, Advances in Atomic, Molecular and Optical Physics, Suplement 2,* edited by P. Berman (Academic, New York, 1994).
93. C.K. Law and J.H. Eberly, Phys. Rev. Lett. **76**, 1055 (1995).
94. J.I. Cirac, P. Zoller, H.J. Kimble, and H. Mabuchi, Phys. Rev. Lett. **78**, 3221 (1997).
95. C.J. Hood, H.J. Kimble, and J. Ye, Phys. Rev. A. **64**, 033804 (2001).
96. M. Khanbekyan, L. Knöll, A.A. Semenov, W. Vogel, and D.-G. Welsch, Phys. Rev. A. **69**, 043807 (2004); A.A. Semenov, D. Yu. Vasylyev, W. Vogel, M. Khanbekyan, and D.-G. Welsch, Phys. Rev. A. **74**, 033803 (2006).
97. E. Waks, E. Diamanti, B.C. Sanders, S.D. Bartlett, and Y. Yamamoto, Phys. Rev. Lett. **92**, 113602 (2004).
98. F.R. Gantmacher, *The Theory of Matrices* (New York, Chelsea, 1959); Ф.Р. Гантмахер, *Теория матриц* (Наука,Москва, 1967).
99. E. Shchukin, Th. Richter, and W. Vogel, Phys. Rev. A.**71**, 011802 (2005).
100. E. Shchukin and W. Vogel, Phys. Rev. Lett. **96**, 200403 (2006).
101. E. Shchukin and W. Vogel, Phys. Rev. Lett. **95**, 230502 (2005); **96**, 129902 (2006).
102. A. Miranowicz and M. Piani, Phys. Rev. Lett. **97**, 058901 (2006); E. Shchukin and W. Vogel, Phys. Rev. Lett. **97**, 058902 (2006).
103. R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
104. В.И. Дмитриев, *Прикладная теория информации* (Высш. шк., Москва, 1989).
105. R.L. Stratonovich, JETP-USSR **4**, 891 (1957); Р.Л. Стратонович, ЖЭТФ **31**, 1012 (1956).
106. G.S. Agarwal, Phys. Rev. A. **24**, 2889 (1981).
107. A.S. Chirkin, A.A. Orlov, and D.Yu. Paraschuk, Quantum Electron. **23**, 870 (1993); А.С. Чиркин, А.А. Орлов, Д.Ю. Паращук, Квант. электроника **20**, 999 (1993).
108. D. Bohm, Phys. Rev. **85**, 166, 180 (1952).
109. J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
110. S. J. Freedman and J. F. Clauser, Phys. Rev. Lett. **28**, 938 (1972).
111. A.Ekert , Phys. Rev. Lett. **67**, 661 (1991).
112. Z. Y. Ou and L. Mandel, Phys. Rev. Lett. **61**, 50 (1988).

113. J. G. Rarity and P. R. Tapster, Phys. Rev. Lett. **64**, 2495 (1990).

114. J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, Phys. Rev. Lett. **82**, 2594 (1999).

115. G. Vernam, J. Am. Inst. Electrical Eng.**45**, 109 (1926).

116. W. Diffie and M.E. Hellman M.E., IEEE Trans. Inform. Theory **22, 6**, 644 (1976).

117. D. Bruss, A. Ekert, and C. Macchiavello, Phys. Rev. Lett. **81**, 2598 (1998).

118. C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

119. P. Townsend, Opt. Fiber Tech. 4, 345 (1998).

120. R. Hughes, G. J. Modern Opt. 47, 533 (2000).

121. B. Huttner, J.D. Gautier, A. Muller, H. Zbinden, and N. Gisin, Phys. Rev. A. **54**, 3783 (1996).

122. B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A.**51**, 1863 (1995).

123. D. Bruss, Phys. Rev. Lett. **81**, 3018 (1998).

124. V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

125. W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

126. H.-K. Lo, H.F. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005).

127. C.H. Bennett, G. Brassard, N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

128. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

129. W. Tittel and G. Weihs, QIC, **1(2)**, 3 (2001).

130. M. Hillery, Phys. Rev. A. **61**, 022309 (1999).

131. N.J. Cerf, M. Levy and G. Van Assche, Phys. Rev. A. **63**, 052311 (2001).

132. D. Gottesman and J. Preskill, Phys. Rev. A. **63**, 022309 (2001).

133. T.C. Ralph, Phys. Rev. A. **61**, 010303 (2000).

134. T.C. Ralph, Phys. Rev. A. **62**, 062306 (2000).

135. S. F. Pereira, Z. Y. Ou, and H. J. Kimble, Phys. Rev. A. **62**, 042311 (2000).

136. F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

137. F. Grosshans, G. V. Assche, R. M. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).

138. M.D. Reid, Phys. Rev. A. **62**, 062308 (2000).

139. C. Silberhorn, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. **88**, 167902 (2002).

140. A. C. Funk and M. G. Raymer, Phys. Rev. A. 65, 042307 (2002).

141. Y. Zhang, K. Kasai, K. Hayasaka, Opt. Express **11**, 3592 (2003).

142. V.C. Usenko , C.V. Usenko, and B.I. Lev, Ukr. J. Phys. **50**, 1204 (2005).

143. V.C. Usenko and B. I. Lev, Phys. Lett. A. **348**, 17 (2005).

НЕКЛАССИЧНОСТЬ КВАНТОВЫХ СОСТОЯНИЙ И ЕЁ ИСПОЛЬЗОВАНИЕ В КВАНТОВОЙ КРИПТОГРАФИИ

А.А. Семенов, В.К. Усенко, Е.В. Щукин, Б.И. Лев

Р е з ю м е

Теоретический и экспериментальный прогресс современных методов квантовой оптики позволяет проводить достаточно глубокие фундаментальные исследования основ квантовой физики. Неклассичностью, в самом широком смысле, называются такие статистические и динамические свойства квантовых состояний, которые не имеют объяснения в рамках любой классической теории. Примерами являются парадокс Эйнштейна—Подольского—Розена, субпуассоновская статистика фотоотсчётов, квадратурное сжатие и т.п. В обзоре рассматривается современное состояние теории неклассических состояний и основные экспериментальные методы их исследования. Рассмотрено применение данного явления к проблеме передачи криптографического ключа, являющейся одной из критически-важных задач в практике обеспечения конфиденциальной связи.

NONCLASSICALITY OF QUANTUM STATES AND ITS APPLICATION IN QUANTUM CRYPTOGRAPHY

A.A. Semenov[1,2], *V.C. Usenko*[1,3], *E.V. Shchukin*[2], *B.I. Lev*[1]

[1]Institute of Physics, Nat. Acad. Sci. of Ukraine
(*46, Prosp. Nauky, Kyiv 03028, Ukraine*),
[2]Institut für Physik, Universität Rostock
(*Universitätsplatz 3, D-18051 Rostock, Germany*),
[3]Dipartimento di Fisica, Università di Milano
(*Via Celoria 16, Milano I-20133, Italy*)

S u m m a r y

The theoretical and experimental progress in the modern methods of quantum optics enables one to provide the deep research in the fundamentals of quantum physics. In the most general sense, the nonclassicality is referred to the special statistical and dynamical properties of quantum states which cannot be explained within the scope of any classical theory. Examples are the Einstein—Podolsky—Rosen paradox, sub-Poissonian statistics of photocounts, quadrature squeezing, *etc.* The review of the current progress in the theory of nonclassical states and the main experimental methods of their investigation is given. An application to the cryptographic key distribution, which is one of the crucial tasks in the problem of confidential communications, is considered.