

ВИСОКОШВИДКІСНИЙ ОДНОФОТОННИЙ ДЕТЕКТОР ДЛЯ СИСТЕМ КВАНТОВОЇ КРИПТОГРАФІЇ

На сьогодні світ просякнутий дротами, радіохвилями та оптичними волокнами, більшість систем зв'язку використовують їх як канали обміну інформацією. Але зазвичай, з'являється необхідність передати якусь дуже важливу секретну інформацію, однак, використовуючи звичайні канали зв'язку, неможливо бути впевненим у таємності переданих даних. Тому для обміну таємною інформацією були створені системи передачі інформації по швидкісному фізичному каналу, секретність яких забезпечується законами квантової фізики. Таким чином, з'явилися квантово-криптографічні системи. Квантова криптографія спирається на неможливість клонування окремого квантового об'єкта. Під клонуванням розуміється створення точної копії вихідного об'єкта при збереженні його у тому стані, в якому він був до процесу клонування і яке з самого початку *невідоме*. Отже, якщо як передавач таємного коду є стани окремих частинок, тоді при спробі зареєструвати ці стани зовнішнім спостерігачем, вони руйнуються. Заздалегідь, домовляються про кодування: фотон із поляризацією 0° та 45° кодують число 0, а фотони з поляризацією 90° та 135° – одиницю (рис. 1).

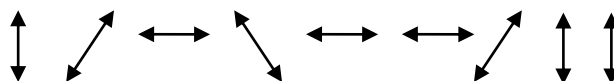


Рис. 1. Кодування фотонів

Причому ця угода може не бути таємною, і, припустимо, що багатьом вона відома. Потім абонент № 1 випадковим чином змінює поляризацію фотонів, що посилаються по квантовому каналу до абонента № 2. Зазвичай для досягнення більшої таємності як генератор випадкових чисел використовується, наприклад, шум діода, але ніколи не використовуються комп'ютерний генератор. Як було сказано, згідно з теорією інформації С.Шеннона, розглянута криптосистема буде таємною тільки в тому випадку, якщо використаний код випадковий. В даний час для реалізації квантового каналу в схемі квантової криптографії найбільш придатним середовищем є оптичне волокно, властивості якого дозволяють передавати криптограми на відстані до 100 км. Але використання волокна накладає обмеження на можливість роботи з поляризаційним кодуванням, оскільки оптоволокно має відчутні флуктуації двоприменезаломлення. Як детектори одиничних фотонів в системах квантової криптографії використовуються лавинні фотодіоди. Вони є найбільш досконалими фотоприймачами для виявлення оптичних сигналів в волоконнооптичних системах передачі. Такі системи працюють переважно в двох спектральних діапазонах: 0,8–0,9 і 1–1,6 мкм.

У першому діапазоні оптимальним є кремнієвий лавинний фотодіод: він перевершує фотоприймачі на інших матеріалах за надійністю, електричними характеристиками, відпрацьованістю технології та дешевизною. У спектральному діапазоні 1–1,6 мкм на даний час практично використовуються германієвий і InGaAs лавинні фотодіоди. Експериментально отримані залежності коефіцієнтів ударної іонізації для германію та кремнію від напруженості електричного поля показані на рисунку 2.

Таким чином, можна зазначити, що для отримання малого шуму в лавинних фотодіодах потрібно звести до мінімуму ефект зворотного зв'язку в процесі множення. Для цього необхідно, щоб коефіцієнти ударної іонізації електронів і дірок сильно розрізнялися за величиною, і щоб процес множення ініціювався носіями з більш високим коефіцієнтом ударної іонізації.

Порівнюючи характеристики InGaAs / InP (Fujitsu FPD5W1KS) лавинного фотодіода з Ge лавинним фотодіодом (NEC NDL5131P1).

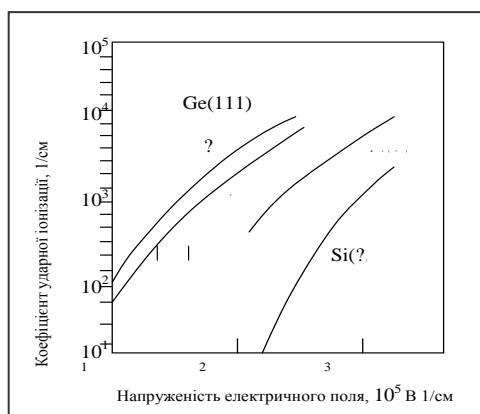
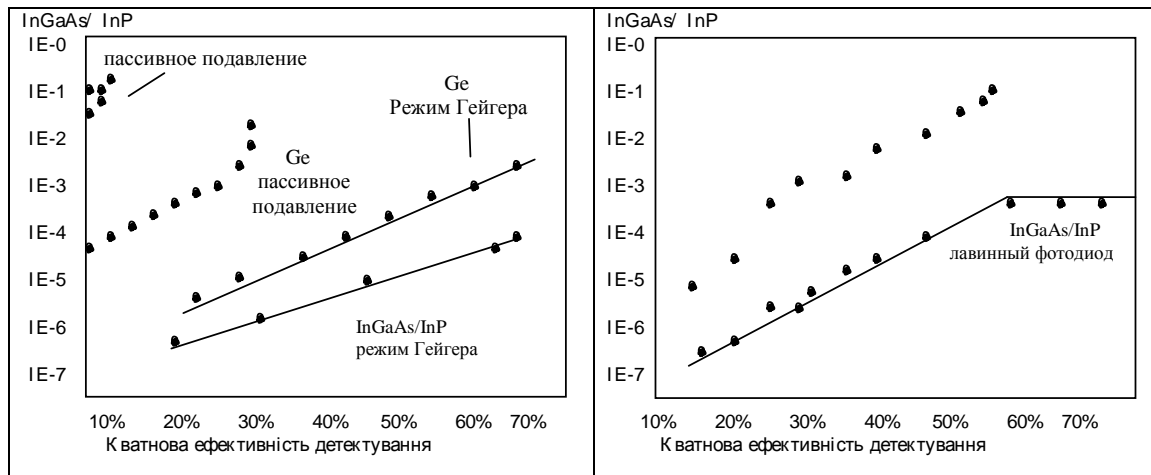


Рис. 2. Залежності коефіцієнтів ударної іонізації для германію та кремнію від напруженості електричного поля

На рисунку 3 показана залежність ймовірності темного відліку від квантової ефективності детектування 1,3 мкм фотонів за температури 77 К в режимі Гейгера. Результати експерименту показують, що InGaAs/InP лавинний фотодіод в режимі очікування показує більш низький шум, ніж германієвий лавинний фотодіод. Більш того, це розходження збільшується зі збільшенням квантової ефективності детектування. Оскільки криві не паралельні, то вони можуть перетнутися при низьких значеннях квантової ефективності, і може статися, що Ge лавинний фотодіод буде давати більш низький шум, ніж InGaAs/InP. Але це тільки експериментальне припущення. Насправді ж, за таких умов фотон світла не може бути просто продетектований. Більше того, оскільки у випадку низьких квантових ефективностей детектування число спрацьовувань знижується, необхідно записувати темнові відліки протягом дуже довгого часу (~1 година), щоб досягти найменшої невизначеності.



а) б)
 Рис. 3. Залежність ймовірності темного відліку в імпульсі, який зміщується від квантової ефективності детектування 1,3 мкм фотонів: а) при 77 К в режимі Гейгера; б) при температурі 123 К

Для порівняння роботи двох лавинних фотодіодів, також наведемо результати експерименту, коли обидва фотодіоди були включені в схему з пасивним придушенням лавини (47 кОм). У цьому випадку система працювала так, що реєструвалися тільки лавини, що виникли при збігу імпульсу з лазера і синхронізуючого сигналу від генератора, який управляє посилкою фотонів на лавинний фотодіод. Робота діодів в цьому режимі не знизил рівень шуму в порівнянні з роботою в режимі Гейгера. Більш того, Ge і InGaAs/InP фотодіоди «помінялися» місцями. При високій температурі (приблизно 123 К) вигідніше використовувати InGaAs/InP лавинний фотодіод, ніж германієвий (рис. 4). При високих коефіцієнтах ефективності детектування ймовірність темного відліку InGaAs/InP фотодіода майже стабілізується і навіть, як видно, злегка знижується. Можна зробити висновок, що InGaAs/InP лавинні фотодіоди припускають можливість поліпшення співвідношення сигнал/шум при детектуванні одиночного фотона. Проте їх властивості погіршені ефектом афтерпалсінга, який особливо важливий при низьких температурах.