**Протоколи передавання квантового ключа**

Ідея квантових грошей була нереалізована, тому що вимагала зберігати фотон в "пастці" (купюрі) досить довгий час. Однак ця ідея підштовхнула Ч.Беннетта та Г.Брассара (C.Bennett і G.Brassard) до винаходу квантової криптографії в 1984 році.

Беннетт і Брассар запропонували не зберігати інформацію про поляризацію фотонів, а передавати її по квантовому каналу, сформованому, наприклад, за допомогою стандартного одномодового волокна, використовуваного в системах передачі даних.

Завдання квантової криптосистеми (яка ставиться до класу симетричних криптосистем) полягають у генерації й передачі послідовності випадково поляризованих фотонів (ПВПФ), що використовувається у формуванні ключа для шифрації та дешифрації повідомлень шляхом маніпуляції чотирма станами поляризації фотонів ( які генеруються дворівневою фізичною системою), що представляють два сполучених ортогональних базиси А и В: |0А>, |1А> і |0в> = (1/√2)/(|0A> + |1А>), |1B> = (1/√2)/(|0A> -|1А>).

Тут стани |0А>і |1А> використовуються для кодування значень "0" і "1" у базисі A, а |0в> і |1в> для кодування тих же значень у базисі B. Ці стани можна подати за допомогою поляризаційних станів фотону.

Наприклад, |0А> і |1А> можна зіставити з горизонтальним (0°) і вертикальним (90°) напрямками лінійної поляризації фотона, а |0в> і |1в> – зіставити із двома діагональними (ортогональними) напрямками лінійної поляризації, спрямованими під кутами 45° і 135° (або -45°).

Два стани, що належать до того ж самого базису, є ортогональними, тобто їх можна надійно розрізнити при вимірі в тому ж базисі, тоді як вимір в іншому (неправильному) базисі, наприклад, у базисі (0°, 45°) дасть абсолютно випадковий результат (з імовірністю 50% це може бути "1" або "0").

Протокол BB84 був запропонований Беннеттом і Брассаром в 1984 році.

Згідно цьому протоколу здійснюються дії, описані нижче й ілюстровані п'ятьома групами малюнків (1-5 зверху вниз) на рис.1:

1. Абонент А надсилає послідовність фотонів, що мають випадкову (0°, 45°, 90°, 135°) поляризацію;

2. Абонент Б вимірює поляризацію фотонів, обираючи базис "+" (0°, 90° – лінійна поляризація) або "х" (45°, 135° – діагональна лінійна поляризація) за випадковим законом;

3. Абонент Б фіксує отримані результати вимірів, зберігаючи їх у секреті (окремі фотони можуть бути не прийняті зовсім – загублені або "стерті");

4. Абонент Б повідомляє потім абоненту А по відкритому каналу, які базиси ("+" або "х") він використав для кожного прийнятого фотона (але не отримані їм результати), а абонент А повідомляє йому, які базиси з використаних були правильними (дані, отримані при вимірах у неправильних базисах, відкидаються);

5. Дані, що залишилися, інтерпретуються відповідно до домовленої схеми (0° і 45° декодуються як "0", а 90° і 135° – як "1") як двійкова послідовність (11001).

Отримана послідовність біт є "чорновим варіантом" ключа, що підлягає уточненню.

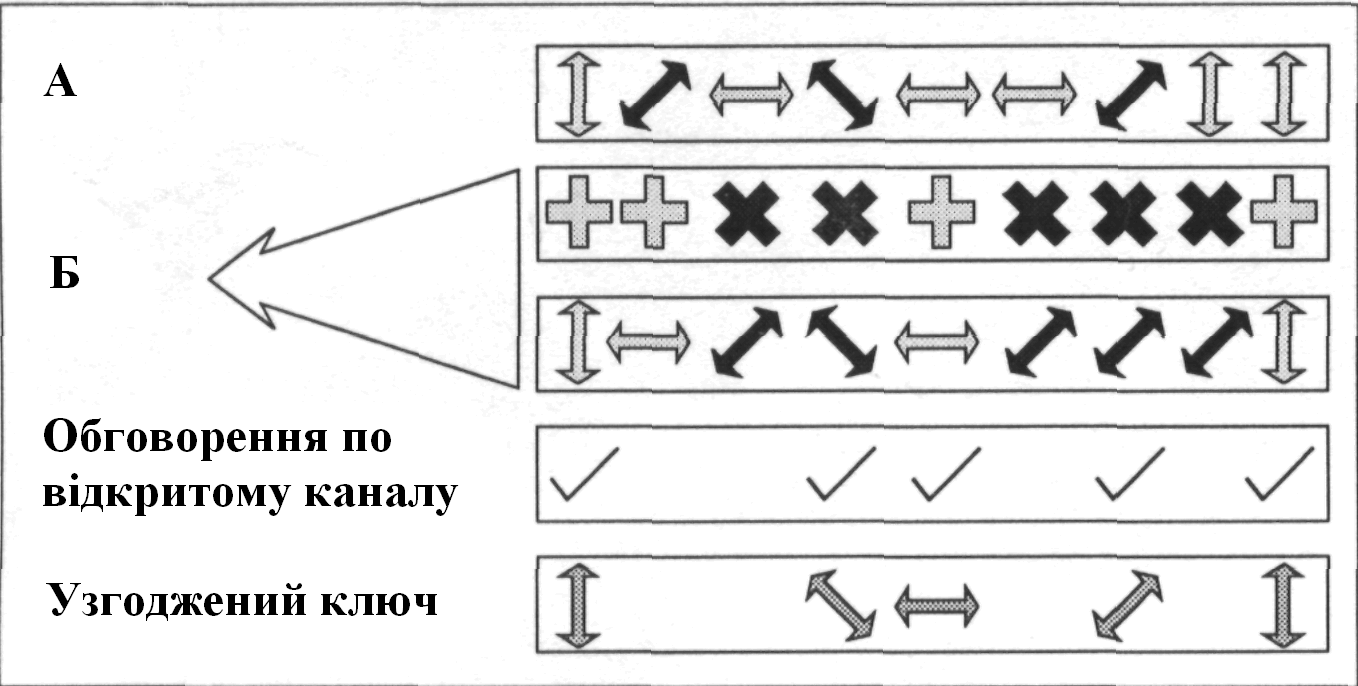


Рисунок 1 – Формування квантового ключа за протоколом BB84

Протокол B92 був запропонований Беннеттом в 1992 році, який показав, що для кодування "0" і "1" можуть бути використані не чотири, як у протоколі BB84, а будь-які два неортогональних поляризованих стани |ψ0> ("0") та |ψ1> ("1"), добуток яких лежить в інтервалі (0,1): 0 < ||<ψ0|ψ1>||2 < 1 .

Для кодування стану "0" абонент А може використати лінійну поляризацію 90° (V), а для "1" – діагональну лінійну поляризацію, повернену на кут 45° [див. рис.2].

Стандартний варіант реалізації припускає, що абонент Б при вимірі буде декодувати як "1" стан з лінійною (горизонтальною) поляризацією 0° (H) і як "0" – стан з діагональною лінійною поляризацією, поверненою на кут 135° (-45°). Можуть бути обрані і інші варіанти.

Ідея такого спрощення ґрунтується на тому, що якщо вимірювання, яке може (відповідно до принципу невизначеності) розрізнити два неортогональні квантові стани, не можна здійснити, то неможливо із упевненістю ідентифікувати конкретний біт.

Більше того, будь-яка спроба вивчення цього біта приведе до помітної модифікації його стану.

Етапи реалізації передачі, прийому й декодування біт квантового ключа в системі с поляризаційним кодуванням показані на рис. 2.

1. Абонент А, погодивши з абонентом Б процедуру порівняння при декодуванні, посилає абоненту Б згенеровану послідовність ПВПФ;

2. Абонент Б застосовує до неї випадковим чином один із двох ортогональних базисів "+" або "х" (як і в протоколі ВВ84), обчислюючи можливі значення надісланих бітів. Таких значень може бути в принципі три – "1", "0" і "?". Останній варіант означає, що з імовірністю 50% результат може бути "1" або "0". Крім цього, у каналі можуть відбутися стирання, коли абонент Б нічого не фіксує в прийнятому бітовому інтервалі;

3. Після прийому абонентом Б послідовності біт і відкидання невизначених позицій залишається N свідомо певних позицій, які й приймаються за "чорновий варіант" ключа.

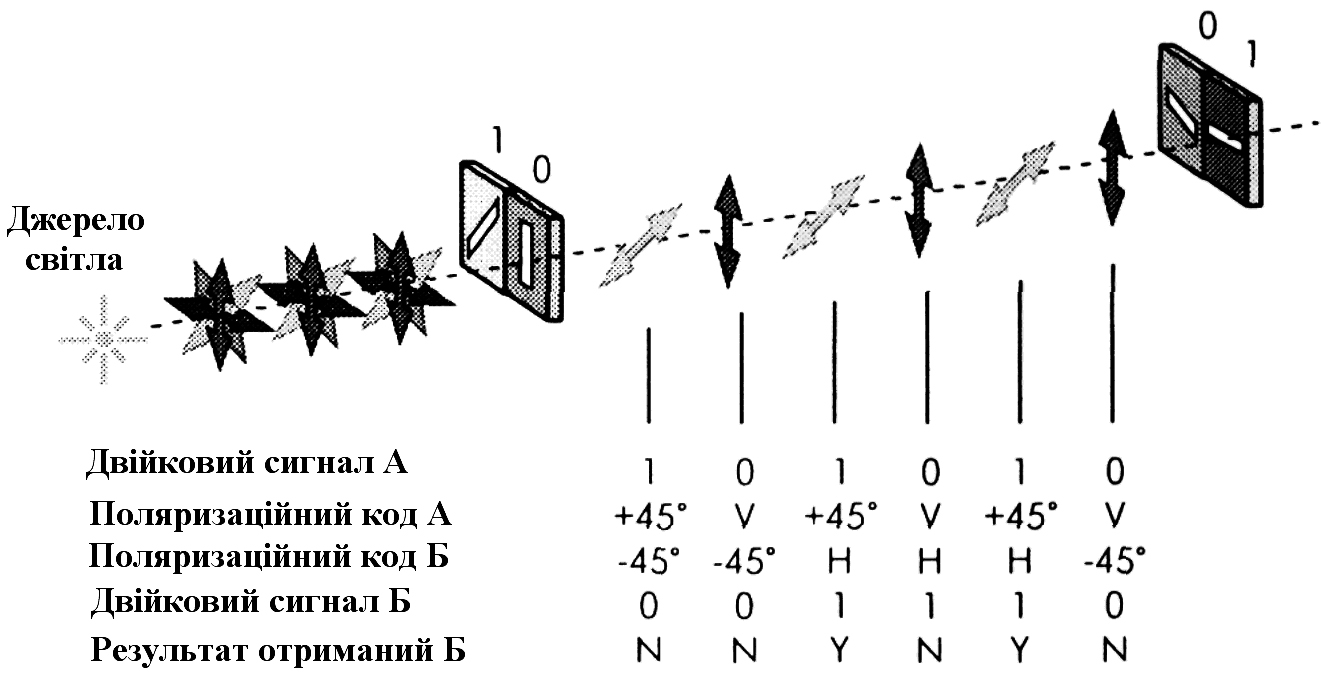


Рисунок 2 – Формування квантового ключа по протоколу B92

1. Абонент А, погодивши з абонентом Б процедуру порівняння при декодуванні, посилає абоненту Б згенеровану послідовність ПВПФ;

2. Абонент Б застосовує до неї випадковим чином один із двох ортогональних базисів "+" або "х" (як і в протоколі ВВ84), обчислюючи можливі значення надісланих бітів.

Таких значень може бути в принципі три – "1", "0" і "?". Останній варіант означає, що з імовірністю 50% результат може бути "1" або "0". Крім цього, у каналі можуть відбутися стирання, коли абонент Б нічого не фіксує в прийнятому бітовому інтервалі;

3. Після прийому абонентом Б послідовності біт і відкидання невизначених позицій залишається N свідомо певних позицій, які й приймаються за "чорновий варіант" ключа.

При наступному уточненні чорнового варіанту ключа шляхом обміну певними даними у відкритому каналу абонентА и абонент Б можуть або одержати варіант ключа, придатний для спільного використання (shared key) (під час відсутності підслуховування приблизно половина отриманих ними даних може бути абсолютно корельованою), або відкинути чорновий ключ і повторити процедуру генерації і передачі квантового ключа.

Відкритим каналом зв'язку може бути будь-який канал зв'язку або Інтернет, на якому реалізований, наприклад, стандартний алгоритм RSA з відкритим ключем. Уточнення може складатися з наступних чотирьох етапів.

Оцінка помилки – абонент А повідомляє підмножину з K позицій чорнового варіанта ключа довжиною N і відповідні їм значення біт. Абонент Б також посилає їй біти, отримані у цих же позиціях.

Обоє ( абонент А и абонент Б) обчислюють по них помилку спостережень є на довжині підмножини K і схвалюють результат передачі квантового ключа, якщо e < eмакс (встановленого абонентом А в процесі конфігурації протоколу В92), або ні – у протилежному випадку, після чого процес передачі повторюється знову.

У випадку схвалення оголошена підмножина з K біт видаляється із чорнового варіанта ключа, і схвалений ключ довжиною N-K піддається процедурі узгодження.

* Узгодження – абонент А та абонент Б здійснюють процедуру узгодження схваленого ключа з використанням ітеративного алгоритму корекції помилок на основі контролю парності (наприклад, використовується спеціальний алгоритм CASCADE).
* Враховуючи, що процедура узгодження дозволяє, з одного боку, зберегти більше біт у підсумковій реалізації квантового ключа, а з іншого боку, істотно вповільнює процес, а значить, і швидкість передачі секретного ключа, потрібно підходити до її реалізації гнучко, віддаючи перевагу або підсумковій довжині (при дорогому квантовому каналі), або швидкості передачі ключа.

Якщо для погодженого ключа оцінка помилки e > eмакс, то процес передачі повинен повторитися знову, якщо ні, то погоджений ключ піддається процедурі підтвердження правильності.

* Підтвердження правильності – абонент А обирає L (наприклад, 10) випадкових підмножин X...XL і повідомляє Xi разом з показником парності біт у них.
* Абонент Б порівнює оголошені абонентом А парності біт і повідомляє їй, де вони в нього збігаються. Якщо деякі біти парності не збігаються, то процес передачі повинен повторитися знову; якщо всі біти збігаються, то ми одержуємо підтверджений погоджений ключ, що вже може розглядатися як ключ, придатний для спільного використання з імовірністю 1-2.
* Враховуючи, що це все-таки не повністю секретний ключ, він може бути підданий процедурі посилення таємності.

Посилення таємності – абонент А повідомляє опис випадково обраної хеш-функції f з деякого класу F, що потім може бути застосована до підтвердженого погодженого ключа для одержання підсумкового повністю випадкового ключа Xf = f(XA) = f(XB), де XA і XB частково секретні підпослідовності в {0,1}N-K, отримані після підтвердження правильності узгодженого ключа.

Ця процедура дозволяє, взагалі-то, одержати статистично секретний ключ.

У результаті абонент А и Б одержують ідентичні послідовності, які і є секретним ключем, за допомогою якого вони зможуть шифрувати й дешифрувати секретну інформацію й обмінюватися нею, використовуючи незахищений від прослуховування канал зв'язку. Зрозуміло, що всі дії, починаючи від передачі ПВПФ і закінчуючи її дешифрацією за допомогою секретного ключа, мають здійснюватися автоматично під управлінням комп'ютера.

Те, що чорновий варіант ключа вимагає такої серйозної перевірки, не дивно. Імпульси реальної послідовності, що генерується передавачем, можуть бути неоднофотонними, а самі однофотонні приймачі можуть мати великий рівень шуму спонтанної емісії.

Тому дані абонентів будуть розрізнятися навіть при відсутності факту підслуховування. Якщо ж такий факт можливий, то очевидно, що противник - Е в результаті підслуховування може одержати правильні відомості про поляризацію не більше ніж половини фотонів, оскільки їй не відомі всі базиси, використовувані абонентом Б.

Якщо в даних А и Б немає розбіжностей у результаті серії зазначених перевірок, то можна зробити висновок, що частина ключа, яка залишилася, містить мало помилок (якщо вони взагалі є), а абоненту Е відома лише мала частина ключа.

Однофотонні стани поляризації більш зручні для передачі даних на великі відстані по оптичних кабелях. Такого роду схема показана на рис. 3 (алгоритм В92; R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson and C. Simmons, "Quantum cryptography over optical fibers", Uni. of California, Physics Division, LANL, Los Alamos, NM 87545, USA).

У алгоритмі В92 приймач і передавач створюють систему, що базується на інтерферометрах Маха-Цендера.

Відправник визначає кути фазового зрушення, відповідні логічному нулю і одиниці (FA=π/2), а приймач задає свої фазові зрушення для логічного нуля (FB=3π/2) і одиниці (FB=π). У даному контексті зміна фази 2π відповідає зміні довжини шляху на одну довжину хвилі використованого випромінювання.

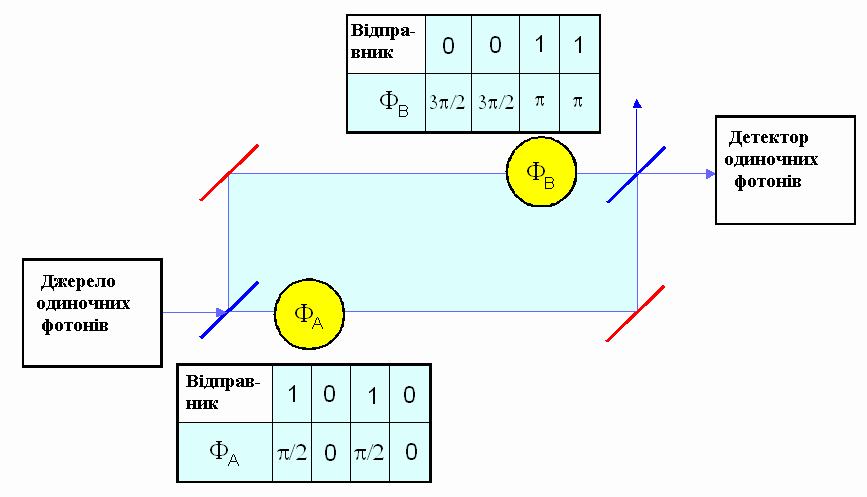


Рисунок 3 – Реалізація алгоритму В92

Хоча фотони поводяться при детектуванні як частинки, вони розповсюджуються як хвилі. Вірогідність того, що фотон, посланий відправником, детектуватиметься одержувачем дорівнює

PD = cos2{(FA - FB)/2} (1)

і характеризує інтерференцію амплітуд хвиль, що розповсюджуються по верхньому і нижньому шляхах (див. риc.4). Вірогідність реєстрації змінюється від 1 (при нульовій різниці фаз) до нуля.

Тут передбачається, що відправник і одержувач використовують фазові зрушення (FA, FB) = (0, 3π/2) для нульових біт і (FA, FB) = (π/2, π) для одиничних бітів (для алгоритму ВВ84 використовуються інші припущення).

Для реєстрації одиночних фотонів, крім ФЕУ, можуть використовуватися твердотільні лавинні фотодіоди (германієві і InGaAs). Для зниження рівня шуму їх слід охолоджувати.

Ефективність реєстрації одиночних фотонів знаходиться в діапазоні 10-40%. При цьому слід враховувати також досить високе поглинання світла оптичним волокном (~0,3-3ДБ/км).

Схема інтерферометра з двома волокнами достатньо нестабільна із-за різних властивостей транспортних волокон і може успішно працювати тільки при малих відстанях. Кращих характеристик можна досягти, мультіплексуя обидва шляхи фотонів в одне волокно (див. рис. 4).

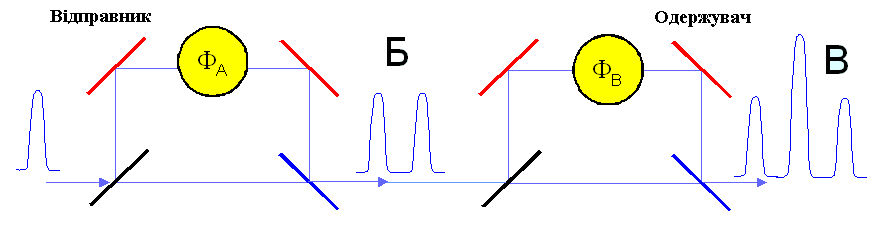


Рисунок 4 – Інтерферометр з одним транспортним волокном

У цьому варіанті відправник і одержувач мають ідентичні нерівноплечі інтерферометри Маха-Цендера.

Різниця фаз довгого і короткого шляхів DT є набагато більшого часу когерентності світлового джерела. З цієї причини інтерференція в межах малих інтерферометрів не відбувається (Б).

Але на виході інтерферометра одержувача вона можлива (В). Вірогідність того, що фотонні амплітуди складуться (центральний пік вихідного сигналу інтерферометра В) дорівнює

P = (1/8)[1 + cos(FA - FB)] (2)

Слід відзначити, що ця амплітуда сигналу є в чотири рази меншого ніж у випадку, показаному на рис.4.

Розгалуджувачі пучка (напівпрозорі дзеркала) можуть бути замінені на оптоволоконні об'єднувачі (coupler). Практичні вимірювання для транспортного кабелю завдовжки 14 км показали ефективність генерації біту ключа на рівні 2,2 10-3 при частоті помилок (BER) близько 1,2%.