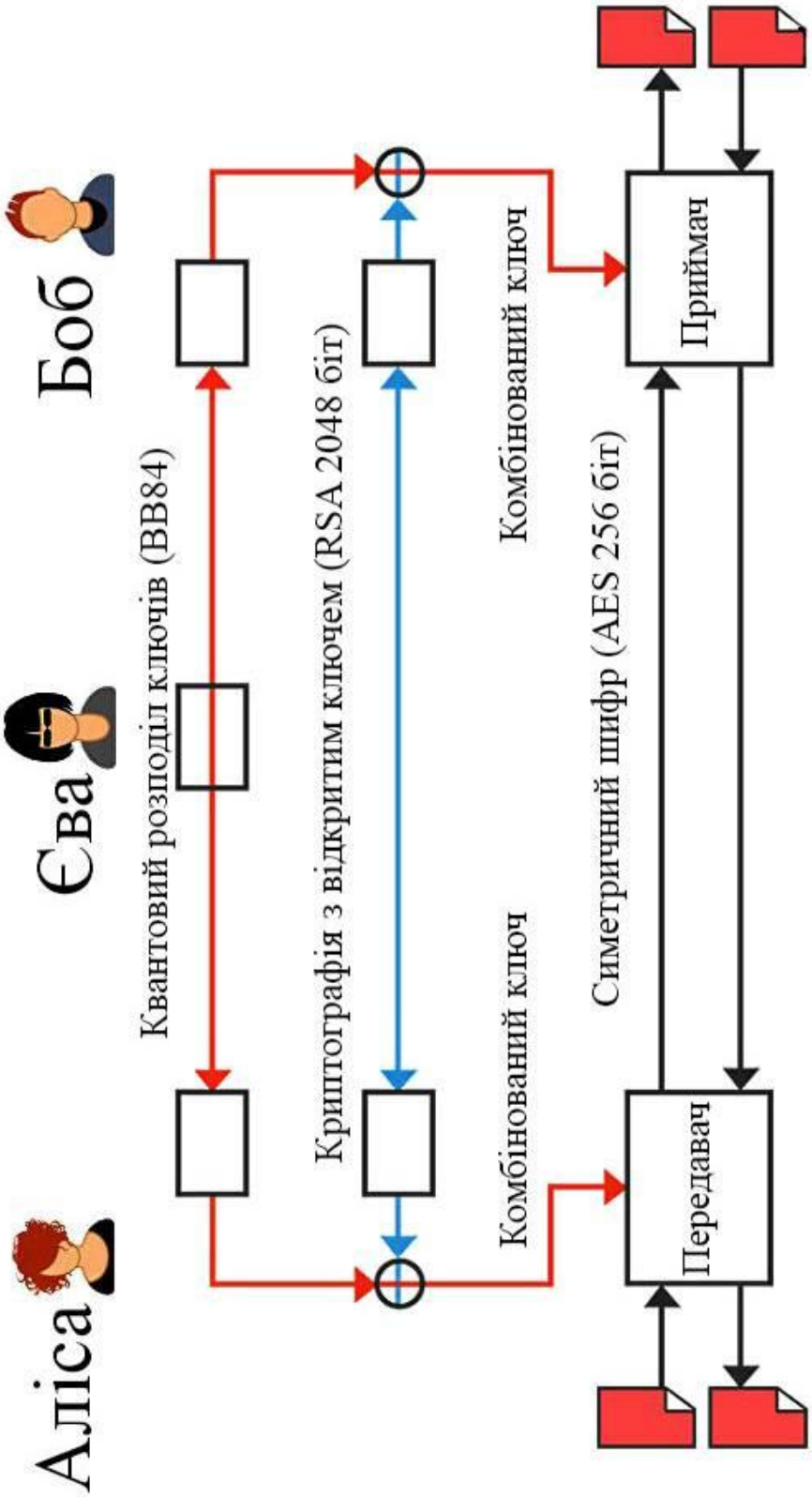
ДОДАТОК А

Графічний матеріал

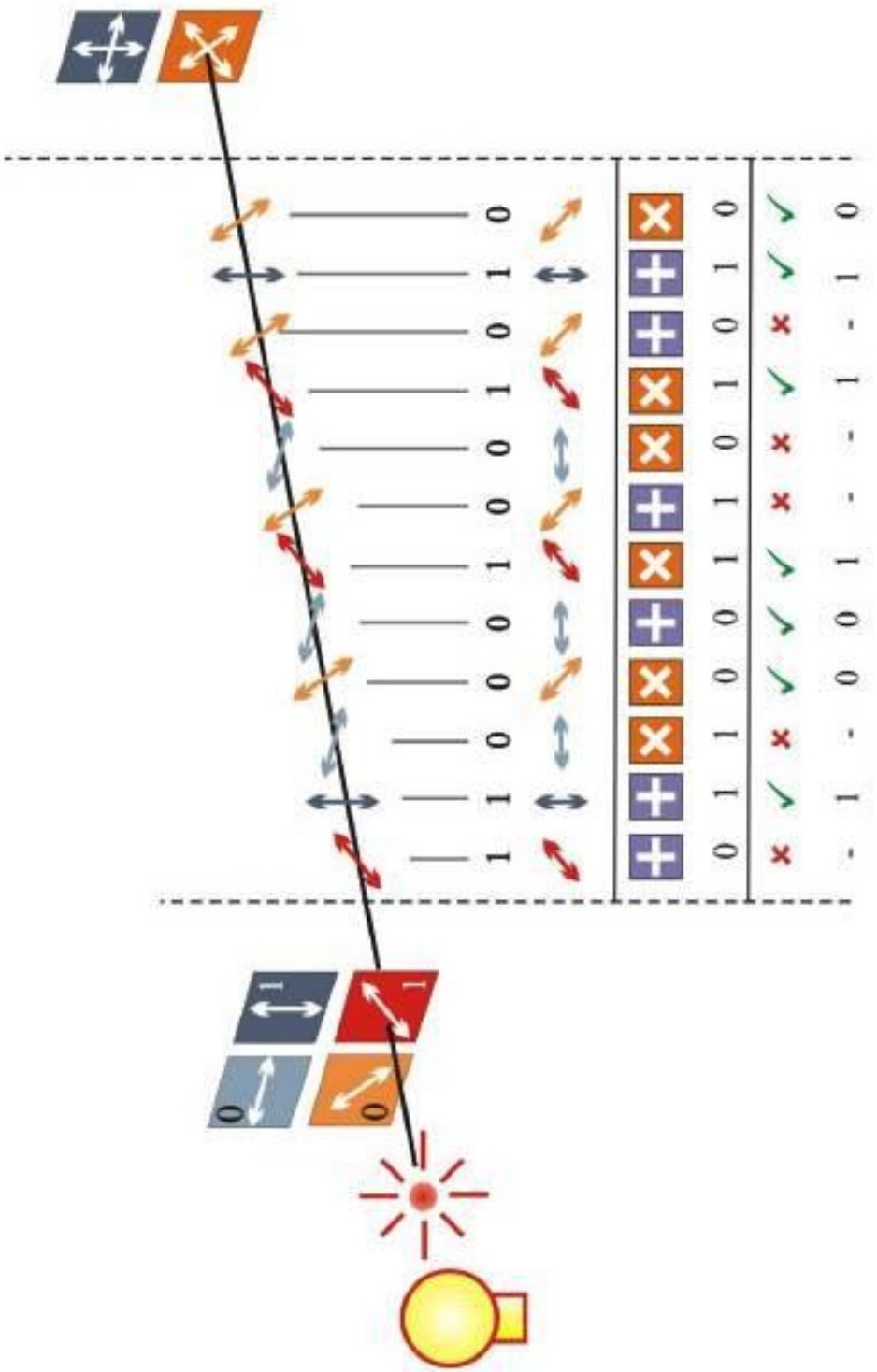
Схема структурна
«Система квантової криптографії»



Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

Изм	Лист	№ докум.	Подпись	Дата	ГЮІК. 433739. 100 Е	Лист 1

Схема структурна
«Реалізації квантового протоколу ВВ84»



Изм	Лист	№ докум.	Подпись	Дата	ГЮІК. 433739. 101 Е	Лист 1

Инв. № подл. | Подпись и дата | Взам. инв. № | Инв. № дубл. | Подпись и дата

ДОДАТОК Б
Демонстраційний матеріал

Харківський національний університет радіоелектроніки
Кафедра фізичних основ електронної техніки

АТЕСТАЦІЙНА РОБОТА

ОСНОВНІ ПОЛОЖЕННЯ КВАНТОВОЇ КРИПТОГРАФІЇ

Рівень вищої освіти – другий (магістерський)
Спеціальність 152 – Метрологія та інформаційно-вимірювальна техніка
Освітня програма – Лазерна і оптоелектронна техніка

Розробив:
студент гр. ЛОЕТм-19-1
Коптяков О. В.

Керівник:
проф., зав. каф.ФОЕТ
Мачехін Ю.П.

Харків
2020

2

Мета роботи:

Ознайомлення з квантовими протоколами шифрування. Визначення проблем та недоліків квантової криптографії. Ознайомлення з фізичною та практичною реалізацією системи квантової криптографії.

Завдання:

1. Задачі криптографії.
2. Способи шифрування даних.
3. Протоколи шифрування.
4. Проблеми, недоліки та тенденції розвитку квантової криптографії.
5. Застосування квантової криптографії на практиці.

Продовження додатку Б

Задачі криптографії

3

Криптографія — наука про методи шифрування.

Основні задачі криптографії:

— Забезпечення конфіденційності даних;

— Забезпечення цілісності даних

— Забезпечення аутентифікації.

— Забезпечення неможливості відмови від авторства

Необхідність застосування криптографічних методів випливає з умов, в яких відбувається зберігання і обмін інформацією. В сучасних інформаційних системах дуже часто відбувається обмін даними в колективах, члени яких не довіряють один одному. Отже, метою застосування криптографічних методів є захист інформаційної системи від цілеспрямованих руйнівних впливів (атак) з боку противника.

Способи шифрування даних

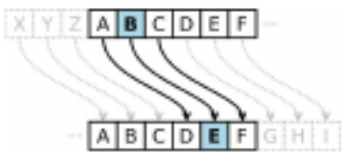
4

Застосування шифрів почалося ще кілька тисячоліть тому, і за минулий час було винайдено величезну кількість технологій шифрування тій чи іншій мірі надійності.

Криптографічні шифри

Шифр «Сцітала»

Шифр Цезаря



Шифр заміни

Продовження додатку Б

Протоколи квантового шифрування

5

У 1984 році були сформульовані принципи квантової криптографії і надані аргументи на користь секретності подібного способу розподілу ключів. Потім прийшов час для розвитку власне формалізму квантової криптографії: були описані необхідні дії легітимних користувачів, формалізовані дії перехоплювача, а також була доведена секретність першого протоколу квантового розподілу ключів, названого BB84.

На даний час існує багато протоколів квантової криптографії. Більшість з них засновані на передачі інформації за допомогою кодування в станах одиночних фотонів, наприклад: BB84, B92, BB84 (4+2), з шістьма станами, Гольденберга-Вайдмана, Коаші-Імото і їх модифікації. Протокол E91 — розроблений для кодування інформації в переплутаних станах.

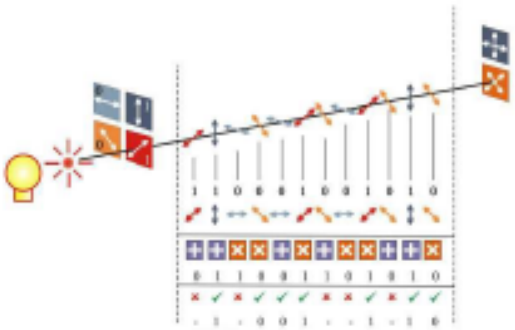
Квантовий протокол BB84

6

Протокол BB84 формулюється на умові одиночних фотонів, хоча його легко узагальнити на будь-яку іншу реалізацію кубітів.

Для кодування інформації в протоколі використовуються 4 поляризаційні стани фотонів, наприклад, напрямок вектору поляризації, однин з яких відправник вибирає в залежності від переданого біта: 90° або 135° для «1», 0° або 45° для «0» .

Схема реалізації квантового протоколу BB84



Продовження додатку Б

Проблеми квантової криптографії

7

При створенні практичних криптосистем, заснованих на квантовому розподілі ключа, доводиться стикатися з такими проблемами:

— низька швидкість передачі даних;

— передача даних здійснюється тільки на невеликі відстані;

— неможливо створити квантові повторювачі;

— інтенсивність квантових імпульсів;

— атаки зловмисників на квантовий канал змінює саме повідомлення.

Тенденції розвитку квантової криптографії

8

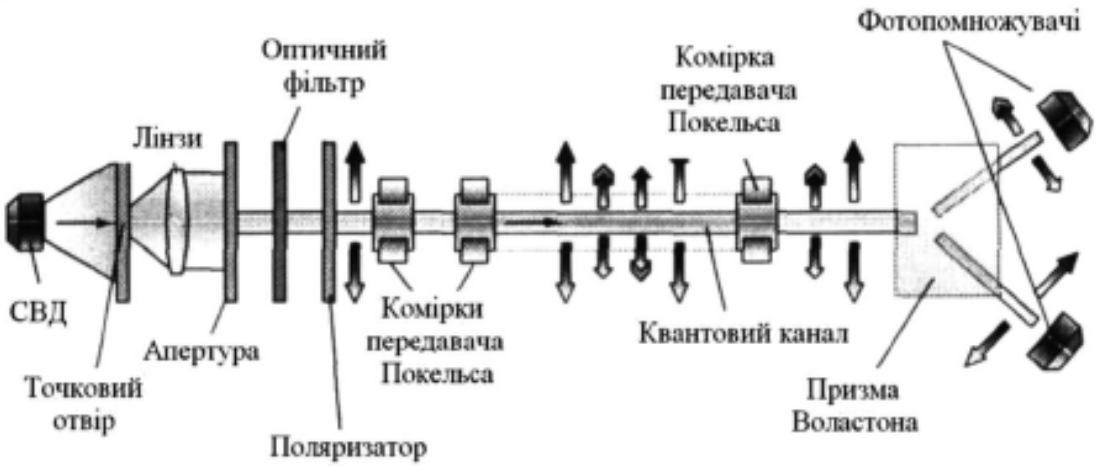
У квантовій криптографії виділяють три потенціальних напрямки розвитку систем розподілу ключів .

1. Базується на принципі неможливості фактично розрізнити два неортогональних квантових станів одного фотону.
2. Засноване на ефекті «переплутаних станів».
3. Засноване на збереженні квантового стану.

Квантова криптографія тільки наближається до повноцінного практичного застосування.

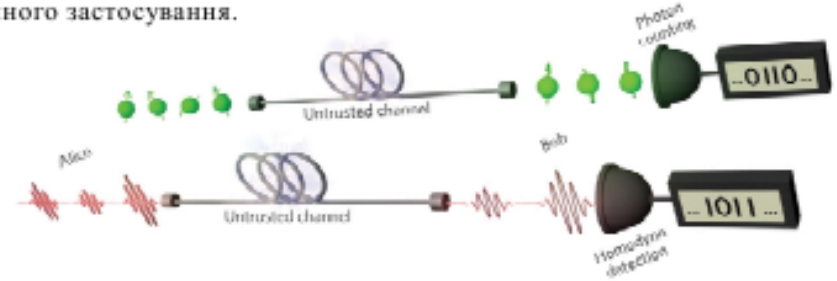
Продовження додатку Б

Схема фізичної реалізації квантової криптографії 9



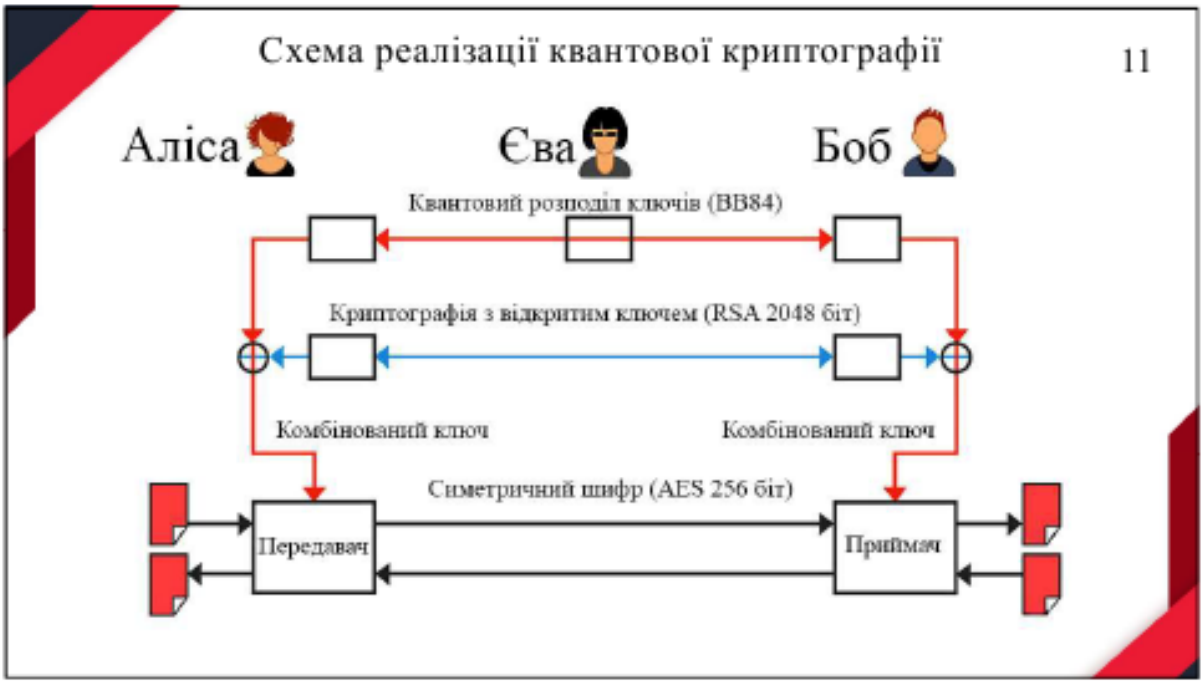
Застосування квантової криптографії на практиці 10

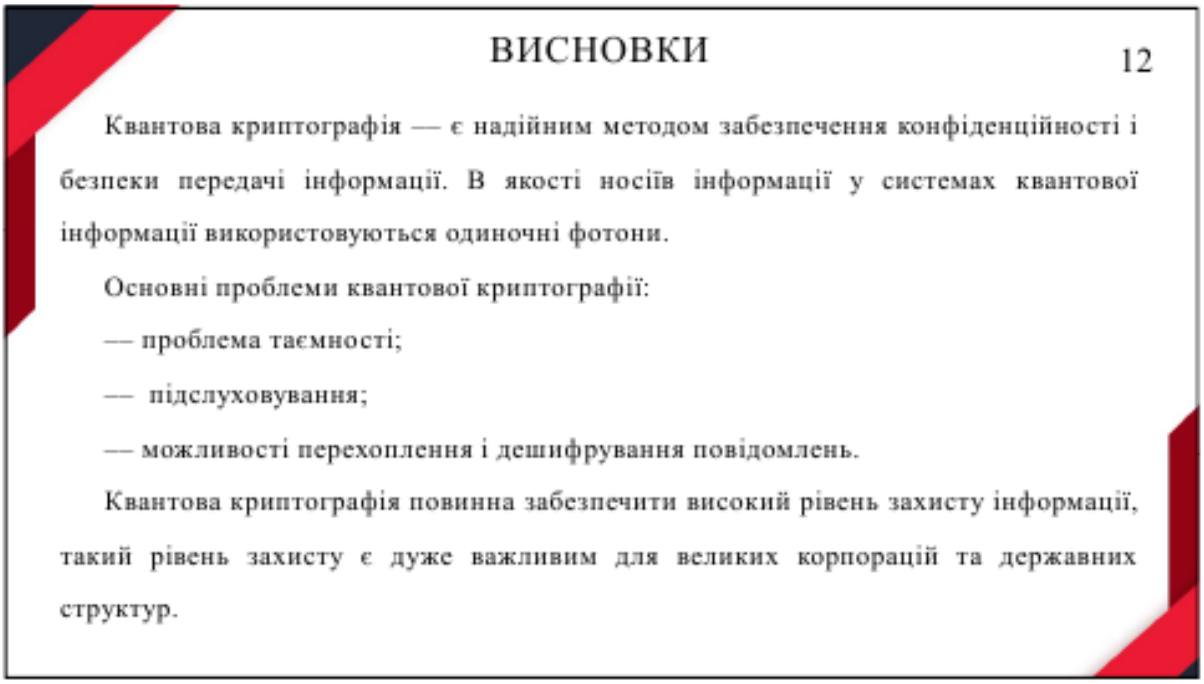
На даний час дослідження щодо безпечної прямої передачі повідомлень (без шифрування) за допомогою квантових систем стають все більш активними, однак така технологія ще не досягла потрібного ступеня надійності, необхідної для її практичного застосування.



Активні дослідження в галузі систем квантової криптографії ведуть IBM, GAP-Optique, Mitsubishi, Toshiba, Національна лабораторія в Лос-Аламосі, Каліфорнійський технологічний інститут, приватна компанія MagiQ і холдинг QinetiQ.

Продовження додатку Б





№ док.	Позначення	Найменування	Кільк. арк..	Прим.
		Текстові документи		
1		Пояснювальна записка	41	ел. ф.
		Графічні матеріали		
2	ГЮІК. 433739. 100 Е	Схема структурна «Система		
		квантової криптографії»	1	ел. ф
3	ГЮІК. 433739. 101 Е	Схема структурна «Реалізації	1	ел. ф
		квантового протоколу ВВ84»		
4		Демонстраційний матеріал	12	ел. ф.

Зм.	Арк.	№ докум.	Підпис	Дата	ГЮІК. 433739. 001 Д1		
Розроб.		Коптяков			Основні положення квантової криптографії Відомість атестаційної роботи	Лит.	Арк. 1 / Аркушів 1
Перевір.		Мачехін					
Т.контр.						ХНУРЕ Кафедра ФОЕТ	
Н.контр.		Чернишова					
Затв.		Мачехін					