НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

«На правах рукопису»

«До захисту допущено»
Завідувач кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2024 р.

Дипломна робота

на здобуття ступеня бакалавра
за освітньо-професійною програмою
«Математичні методи криптографічного захисту інформації»

зі спеціальності: 113 Прикладна математика
на тему: **«Побудова Квантового Протоколу Узгодження Автентичного Ключа QAKAP»**

Виконав:
студент IV курсу, групи ФІ-03
Починок Юрій Сергійович _____

Керівник:
к.ф.-м.н. ст. викладач
Фесенко Андрій В'ячеславович _____

Рецензент:
посада, степінь, звання
_____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

Київ — 2024

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

Рівень вищої освіти — перший (бакалаврський)
Спеціальність — 113 Прикладна математика,
ОПП «Математичні методи криптографічного захисту інформації»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2024 р.

ЗАВДАННЯ
на здобуття ступеня бакалавра

Студент: Починок Юрій Сергійович

1. Тема роботи: «*Побудова Квантового Протоколу Узгодження Автентичного Ключа QAKAP*», науковий керівник дисертації: к.ф.-м.н. ст. викладач Фесенко Андрій В'ячеславович,

затверджені наказом по університету №__ від «__» _____ 2024 р.

2. Термін подання студентом роботи: «__» _____ 2024 р.

3. Об'єкт дослідження: процеси перетворення інформації в квантових протоколах узгодження ключа.

4. Предмет дослідження: забезпечення властивості автентичності ключа в квантових протоколах узгодження ключа.

5. Перелік завдань:

1) дослідити наявні схеми цифрового підпису;

2) побудувати квантовий протокол узгодження автентичного ключа;

3) проаналізувати криптографічні властивості побудованого квантового протоколу узгодження ключа;

4) дослідити наявні протоколи узгодження автентичного ключа та провести порівняльний аналіз з побудованим квантовим протоколом узгодження ключа.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: презентація доповіді.

7. Орієнтовний перелік публікацій: Результати дослідження, описані в роботі, частково були освітлені в доповіді на XXII Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих учених «Теоретичні та прикладні проблеми фізики, математики й інформатики» (м. Київ, 14-17 травня 2024 р.).

8. Дата видачі завдання: 10 вересня 2023 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	01-15 вересня 2023 р.	Виконано
2	Огляд опублікованих джерел за тематикою дослідження	Вересень-жовтень 2023 р.	Виконано
3	Ознайомлення з попередніми результати щодо побудови квантових протоколів узгодження ключа	Жовтень-листопад 2023 р.	Виконано
4	Ознайомлення та аналіз класичних протоколів узгодження ключа	Грудень-січень 2023 р.	Виконано
5	Побудова квантового протоколу узгодження автентичного ключа QAKAP	Лютий-Березень 2023 р.	Виконано
6	Аналіз та модифікація квантового протоколу узгодження автентичного ключа QAKAP	Квітень 2023 р.	Виконано
7	Оформлення дипломної роботи	Травень 2023 р.	Виконано

Студент _____ Юрій ПОЧИНОК

Керівник _____ Андрій ФЕСЕНКО

РЕФЕРАТ

Кваліфікаційна робота містить: 48 стор., 7 рисунків, 1 таблицю, 23 джерела.

У роботі розглянуто протоколи узгодження автентичного ключа: ефемерний Діффі-Геллман, статичний Діффі-Геллман, алгоритм обміну ключа, протокол Менезеса-К'ю-Ванстоуна, квантову схему цифрового підпису Чанга-Готтсмана, квантовий протокол Діффі-Геллмана, квантовий протокол Діффі-Геллмана з автентифікацією. Розглянуто основні криптографічні властивості протоколів узгодження ключа. Побудовано та проаналізовано кватовий протоколу узгодження автентичного ключа QAKAP. Модифіковано кватовий протокол узгодження автентичного ключа QAKAP за допомогою підтвердження ключа і проаналізовано цю модифікацію. Проведено порівняльний аналіз побудованих протоколів з класичними протоколами узгодження автентичного ключа. Розглянуто концепцію активного зловмисника та подувано 1 атаку віддзеркалення повідомлень та 2 атаки паралельних сеансів.

Метою дослідження є побудова квантового протоколу узгодження автентичного ключа.

Об'єкт дослідження є процеси перетворення інформації в квантових протоколах узгодження ключа.

Предмет дослідження є забезпечення властивості автентичності ключа в квантових протоколах узгодження ключа.

АСИМЕТРИЧНА КРИПТОГРАФІЯ, КВАНТОВИЙ ЦИФРОВИЙ ПІДПИС ЧАНГА-ГОТТСМАНА, АВТЕНТИФІКОВАНІ ПРОТОКОЛИ УЗГОДЖЕННЯ КЛЮЧА

ABSTRACT

The qualification work contains: 48 pages, 7 figures, 1 table, 23 sources.

Authentic key agreement protocols are considered in the work: ephemeral Diffie-Hellman, static Diffie-Hellman, key exchange algorithm, Menezes-Qu-Vanstone protocol, Chuang-Gottsman quantum digital signature scheme, quantum Diffie-Hellman protocol, authentication quantum Diffie-Hellman protocol. The main cryptographic properties of key agreement protocols are considered. The QAKAP quantum authentic key agreement protocol modification was built and analyzed. Modification of the quantum authentic key agreement protocol using key confirmation was analyzed. A comparative analysis of the constructed protocols with classic authentic key agreement protocols was carried out. Considered the concept of an active adversary and consrtucted 1 reflection attack and 2 parallel-session attacks.

The goal of the research is to build a quantum authentic key agreement protocol.

The research object is information transformation processes in quantum key agreement protocols.

The research subject is to ensure the property of key authenticity in quantum key agreement protocols.

ASYMETRIC CRYPTOGRAPHY, CHANG-GOTTSMAN QUANTUM DIGITAL SIGNATURE, AUTHENTICATED KEY AGREEMENT PROTOCOLS

ЗМІСТ

ВСТУП

Актуальність дослідження зумовлена стрімким розвитком квантової криптографії і, в той самий час, відсутністю квантових протоколів узгодження автентичного ключа, не дивлячись на повсякденне використання класичних протоколів з автентифікацією.

Причиною відсутності квантових протоколів узгодження автентичного ключа стало твердження Барнума на його колег у роботі [1], про неможливість автентифікації квантової інформації. Не дивлячись на попереднє твердження були побудовані квантові схеми цифрового підпису, що не суперечили твердженню Барнума, а знайшли інший вихід з цієї ситуації. Квантові схеми цифрового підпису взаємодіяли з класичною інформацією. Показовою схемою квантового цифрового підпису стала схема Чанга-Готтсмана [11]. Саме завдяки квантовим схемам цифрового підпису побудова квантового протоколу узгодження автентичного ключа стала можливою.

Метою дослідження є побудова квантового протоколу узгодження автентичного ключа.

Для досягнення необхідно розв'язати наступні завдання:

1) дослідити наявні схеми цифрового підпису;

2) побудувати квантовий протокол узгодження автентичного ключа;

3) проаналізувати криптографічні властивості побудованого квантового протоколу узгодження ключа;

4) дослідити наявні протоколи узгодження автентичного ключа та провести порівняльний аналіз з побудованим квантовим протоколом узгодження ключа.

Об'єктом дослідження є процеси перетворення інформації у квантових протоколах узгодження ключа.

Предметом дослідження є забезпечення властивості автентичності ключа у квантових протоколах узгодження ключа.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: методи лінійної та абстрактної алгебри, теорії імовірностей, методи квантової моделі обчислень.

Наукова новизна та практичне значення одержаних результатів. Вперше побудовано та детально проаналізовано квантовий протокол узгодження автентичного ключа.

Апробація результатів та публікації. Результати дослідження, описані в роботі, частково були освітлені в доповіді на XXII Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих учених «Теоретичні та прикладні проблеми фізики, математики й інформатики» (м. Київ, 14-17 травня 2024 р.).

1 КРИПТОГРАФІЧНІ ВЛАСТИВОСТІ КВАНТОВИХ ПРОТОКОЛІВ

В цьому розділі розглянуто історію розвитку квантової криптографії: квантовий розподіл ключа, квантова автентифікація, розвиток квантових схем цифрового підпису, цифровий відбиток, квантові протоколи узгодження ключа. Описано основні криптографічні властивості як: неявна автентичність ключа, явна автентичність ключа, пряма секретність, новизна ключа, пряма секретність, стійкість до атак з використанням невідомого ключа та інші. Розглянуто класичні протоколи узгодження ключа: ефемерний Діффі-Геллман, статичний Діффі-Геллман, алгоритм обміну ключа, протокол Менезеса-К'ю-Ванстоуна.

1.1 Асиметричні протоколи та криптографічні властивості

Квантова криптографія поєднує в собі теорію квантових обчислень та класичну криптографію. Основною метою цього напрямку є побудова протоколів спираючись на особливості квантової механіки. Одним з найрозвиненіших напрямків квантової криптографії є квантовий розподіл ключа (Quanctum Key Distribution), що вперше продемонстровано Беннетом та Брассардом у 1984 році [3]. Квантовий розподіл ключа вважається одним з перших успішних квантових протоколів безпеку якого доведено [15], [20].

Окрім квантового розподілу ключа досліджується й напрямок автентифікації інформації. Автентифікація або автентифікація користувача – це процедура підтвердження особи користувача чи інформації, що передається. Цей процес допомагає запобігти великій кількості атак, що раніше ставили під загрозу безпечність. Актуальність

схем автентифікації збільшуються з розвитком надання інтернет послуг таких як: онлайн закупівля, онлайн голосування, онлайн банкінг та багатьох інших, де автентифікація особи відіграє ключову роль в наданні тієї чи іншої послуги. Наприклад, онлайн голосування вимагає безпосередню ідентифікацію особи, що хоче здійснити процес голосування або онлайн банкінг, де відсутність ідентифікації користувача могла б привести до незворотних наслідків.

Автентифікація між двома учасниками може бути описана як процедура, що дозволяє користувачу Алісі (відправнику) передати повідомлення X (ключ, у випадку якщо це схема розподілу) іншому користувачу Бобу (отримувачу), таким чином, щоб Боб не мав сумнівів щодо зміни інформації, що початково передавалась через канал зв'язку [9]. Іншими словами, це можна описати як процес, що підтверджує ідентичність користувача, який створив повідомлення X та цілісність повідомлення отриманого Бобом. Це також тісно пов'язано з процедурою цифрового підпису, що дозволяє третьому користувачу (Чарлі), пізніше підтвердити, що Боб не вніс модифікації у початкове повідомлення X, відправлене Алісою [9]. Результати у цьому напрямку продемонстровані Барнумом на його колегами у роботі [1], Женгом та Гуо [23], та інших роботах [12], [2].

Чанг та Готтсман у роботі [11], запропонували схему цифрового підпису, основану на теорії квантової механіки та стверджували, що запропонована схема є абсолютно безпечною, навіть маючи супротивника з необмеженими обчислювальними ресурсами. Не дивлячись на це, квантова схема цифрового підпису може підписувати тільки біти класичної інформації, і не може бути застосовною до квантових станів.

Іншими ж нововведенням, пов'язаним зі схемами цифрового підпису є робота Женга [22], в якій він представив схему квантового цифрового підпису використовуючи арбітра. В такому типі схем, всі передачі інформації здійснюються за допомогою арбітра, який має доступ до вмісту повідомлень, і безпека таких схем за участі посередника (арбітра)

залежить від рівня довіри до того самого посередника. Схема Женга дозволяє підписати квантову інформацію, що завчасно була відома арбітру, але в загальному випадку невідому довільну квантову інформацію підписати неможливо [1], [22], [11].

Цифровий відбиток – це ще один зручний механізм представлений у роботі [19], що може визначити чи є 2 рядки x_1, x_2 однаковими за допомогою асоційованих з цими рядками відбитками x_1^0, x_2^0, які в загальному випадку набагато коротші за початкові рядки x_1, x_2. Цей механізм направлений на зменшення об'єму передачі та сховища для інформації, що передається. Бурман та його колеги, у свою чергу, сформулювали означення квантового відбитку [6], що пізніше стало основою для квантової односторонньої функції з обмеженим використанням у схемі цифрового підпису Чанга-Готтсмана [11].

Протоколи узгодження автентичного ключа являє собою процедуру надання двом або більше користувачам (Алісі і Бобу), що спілкуються за допомогою відкритого каналу зв'язку деякий приватний ключ, за допомогою якого можливе подальше виконання деякого криптографічного протоколу направленого на задовільнення інших цілей, таких як: конфіденційність або цілісності данних. Такі протоколи мають на меті заміну традиційних, класичних протоколів узгодження ключів. Протоколи узгодження ключів розповсюдженні у різній їх варіації як:

1) протоколи транспортування ключа [16], [18], основна ідея яких полягає у створенні одним користувачем (Алісою) деякого ключа x та його подальшу захищену передачу іншому користувачу (Бобу);

2) протоколи узгодження ключа [14], [5], де обидва користувачі (Аліса і Боб) приймають безпосередню участь у створенні приватного ключа x.

Ці види протоколів поділяються на 2 типи: симетричні протоколи, в яких обидва користувачі володіють однаковим особистим ключем, що використовується та асиметричні протоколи, де користувачі поширюють тільки автентифіковані відкриті ключі (інформацію). Симетричні

протоколи ефективні у природі їх обчислень, але вимагають попереднього узгодження спільного секрету (що зазвичай задовільняється за допомогою асиметричних протоколів), де асиметричні протоколи, у свою чергу не вимагають попереднього узгодження спільного секрету, але є більше ресурсомісткими. Побудований в роботі протокол відноситься до класу асиметричних протоколів.

З плином часу, немало асиметричних протоколів запропоновано задля отримання бажаних криптографічних властивостей та збільшення ефективності виконання. Багато з побудованих протоколів переживають цикл нападів (побудови на них атак [13]) та подальшого їх удосконалення [14] або їх покидання авторами. Протоколи, що успішно переживають цикл "атак-модифікацій"пізніше можуть вважатись безпечними для практичного використання.

Протоколи що переживають цикл "атак-модифікацій"мають в собі недоліки, такі як: їх криптографічні властивості зазвичай не чітко визначені або не повністю задані; відсутність гарантій щодо появи нових видів атак у майбутньому. Саме ці недоліки породили поняття чітко визначених криптографічних властивостей, що можна довести. Це вимагає побудови формальної моделі числення, що зможе відобразити як можливу поведінку усіх учасників протоколу та деякого зловмисника, так і формально визначені властивості в рамках цієї моделі, припущення а також доведення того, що протокол відповідає поставленим поставленим цілям у цій моделі.

Основні криптографічні властивості:

Нехай A і B – чесні учасники, тобто учасники, що в точності виконують кроки протоколу.

1) Протокол встановлення ключа забезпечує властивість **неявної автентичності ключа** (implicit key authentication) користувачем A користувачу B, якщо користувач B має впевненість, що користувач A (і, можливо, додатково інші вповноважені довірені учасники) є єдиним учасником сеансу протоколу, який може володіти правильним

відповідним спільним секретним значенням.

2) Протокол встановлення ключа забезпечує властивість **явної автентичності ключа** (explicit key authentication) користувачем A користувачу B, якщо користувач B має впевненість, що користувач A (і, можливо, додатково інші вповноважені довірені учасники) є єдиним учасником сеансу протоколу, який володіє правильним відповідним спільним секретним значенням.

Протоколи підтвердження ключа, що надають властивість неявної автентифікації ключа обом учасникам протоколу називаються протоколами **узгодження автентичного ключа** (authenticated key agreement), AK протоколами. Протоколи підтвердження ключа, що надають властивість явної автентифікації ключа обом учасникам протоколу називаються протоколами **узгодження автентичного ключа з підтвердженням ключа** (authenticated key agreement with key confiramtion), AKC протоколами.

Інші, бажані криптографічні властивості:

Нехай A і B – чесні учасники, тобто учасники, що в точності виконують кроки протоколу.

1) Протокол встановлення ключа забезпечує властивість **новизни ключа**(known-key security), якщо спільне секретне значення є статистично незалежним від будь-якого раніше створеного спільного секретного значення в інших сесіях протоколу.

2) Протокол встановлення ключа забезпечує **пряму секретність** (forward secrecy), якщо компрометація довгострокових ключів суб'єктів з загальної множини суб'єктів не призводить до компрометації спільних секретних значень (сеансових ключів), встановлених у попередніх сеансах цього протоколу за участю цих.

3) **стійкість до атаки з використанням компрометації ключа** (key compromise impersonation attack) — стійкість до атак, в яких зловмисник використовує знання довгострокового особистого ключа суб'єкта A для того, щоб видавати себе за будь-якого суб'єкта у

подальшому спілкуванні з A.

4) **стійкість до атаки з використанням невідомого спільного ключа** (unknown key share attack) — стійкість до атак, в яких тільки вповноважені учасники знають спільне секретне значення, але не мають згоди з ким вони його поділяють.

Інші бажані властивості:

1) мінімальна кількість передач;

2) низька кількість переданих бітів інформації;

3) низька кількість обов'язкових обчислювальних операцій;

4) можливість переобчислення;

5) анонімність;

6) симетричність користувачів;

7) незалежність повідомлень, що передаються.

1.2 Протоколи узгодження ключа з автентифікацією

Розглянемо класичні протоколи узгодження ключа з автентифікацією.

Параметри протоколів:

– A, B – Учасники протоколу.

– p – Деяке велике просте число.

– q – Деякий простий велкиий дільник $p-1$.

– a,b – Статичні особисті ключі користувачів A і B; $a, b \in_R [1, q-1]$

– Y_A, Y_B – Статичні відкриті ключі користувачів A і B; $Y_A = g^a \mod p, Y_B = g^b \mod p$.

– x, y – Ефемерні особисті ключі користувачів A і B; x,$y \in_R [1, q-1]$.

– R_A, R_B – Ефемерні відкриті ключі користувачів A і B; $R_A = g^x \mod p, R_B = g^y \mod p$.

– H – Деяка геш функція.

Протокол 1.1. [5] Ефемерний Діффі-Геллман (EDH)

Крок 1. Користувач A обирає $x_R \in [1, q-1]$ і передає $R_A = g^x$ користувачу B.

Крок 2. Користувач B обирає $y_R \in [1, q-1]$ і передає $R_A = g^y$ користувачу A.

Крок 3. Користувач A обчислює $K = (R_B)^x = g^{xy}$.

Крок 4. Користувач B обчислює $K = (R_A)^x = g^{xy}$.

$$A, x \xrightarrow{\quad g^x \quad} B, y$$
$$K = g^{xy} \xleftarrow{\quad g^y \quad} K = g^{xy}$$

Рисунок 1.1 – Схема протоколу EDH

Протокол 1.2. [5] Статичний Діффі-Геллман (SDH)

Крок 1. Користувач A передає $Cert_A$ користувачу B.

Крок 2. Користувач B передає $Cert_B$ користувачу A.

Крок 3. Користувач A обчислює $K = (Y_B)^a = g^{ab}$.

Крок 4. Користувач B обчислює $K = (Y_A)^b = g^{ab}$.

$$A, a, x \xrightarrow{\quad g^{bx} \quad} B, b, y$$
$$K = g^{xy} \xleftarrow{\quad g^{ay} \quad} K = g^{xy}$$

Рисунок 1.2 – Схема протоколу SDH

Ефемерний протокол Діффі-Геллмана та статичний протокол Діффі-Геллмана є основою протоколів узгодження автентичного ключа та стали мотивацією для багатьох інших подібних протоколів. Наступні протоколи є AK протоколами, тобто ті, що мають явну автентифікацію ключа.

Протокол 1.3. [5] Алгоритм Обміну Ключа (KEA)

Крок 1. Користувачі A і B автентичні копії публічних ключів Y_A, Y_B один одного.

Крок 2. Користувач A обирає $x_R \in [1, q-1]$ і передає $R_A = g^x$ користувачу B.

Крок 3. Користувач B обирає $y_R \in [1, q-1]$ і передає $R_A = g^y$ користувачу A.

Крок 4. Користувач A переконується, що $1 < R_B < p$ і $R_B^q \equiv 1$. За умови провалу, що будь-яка перевірка не виконується A зупиняє виконання протоколу. Інакше, A обчислює $K = (Y_B)^x + (R_B)^a \mod p$. Якщо $K = 0$, A зупиняє виконання протоколу.

Крок 5. Користувач B переконується, що $1 < R_A < p$ і $R_A^q \equiv 1$. За умови провалу, що будь-яка перевірка не виконується B зупиняє виконання протоколу. Інакше, B обчислює $K = (Y_A)^y + (R_A)^b \mod p$. Якщо $K = 0$, A зупиняє виконання протоколу.

Крок 6. Користувачі A і B обчислюють ключ $k = kdf(K)$, де kdf - функція формування ключа виведена зі схеми SKIPJACK [4].

$$A, a, x \xrightarrow{\quad g^x \quad} B, b, y$$
$$K = g^{ay} + g^{bx} \xleftarrow{\quad g^y \quad} K = g^{ay} + g^{bx}$$

Рисунок 1.3 – Схема протоколу KEA

Алгоритм обміну ключами (KEA) був розроблений National Security Agency (NSA) і розсекречений в травні 1998 року [4]. Це протокол узгодження ключа міститься у наборі криптографічних алгоритмів FORTEZZA, розробленими NSA у 1994 році.

Протокол 1.4. [5] Протокол Менезеса-К'ю-Ванстоуна (MQV)

Крок 1. Користувач A обирає $x_R \in [1, q-1]$ і передає $R_A = g^x$, $Cert_A$ користувачу B.

Крок 2. Користувач B обирає $y_R \in [1, q-1]$ і передає $R_A = g^y$, $Cert_B$

користувачу A.

Крок 3. Користувач A переконується, що $1 < R_B < p$ і $R_B^q \equiv 1$. За умови провалу, що будь-яка перевірка не виконується A зупиняє виконання протоколу. Інакше, A обчислює $s_A = x + a\overline{R}_A \mod q$ і спільний секрет $K = (R_B(Y_B)^{\overline{R}_B})^{s_A}$. Якщо $K = 1$, A зупиняє виконання протоколу.

Крок 4. Користувач B переконується, що $1 < R_A < p$ і $R_A^q \equiv 1$. За умови провалу, що будь-яка перевірка не виконується B зупиняє виконання протоколу. Інакше, A обчислює $s_B = y + b\overline{R}_B \mod q$ і спільний секрет $K = (R_A(Y_A)^{\overline{R}_A})^{s_B}$. Якщо $K = 1$, A зупиняє виконання протоколу.

Крок 5. Сесійний ключ $k = H(K)$

$$
\begin{array}{ccc}
 & A, a, x \xrightarrow{\quad g^x \quad} & B, b, y \\
s_A = (x + a\overline{g^x}) \mod q & & s_B = (y + b\overline{g^y}) \mod q \\
 & K = g^{s_A s_B} \xleftarrow{\quad g^y \quad} & K = g^{s_A s_B}
\end{array}
$$

Рисунок 1.4 – Схема протоколу MQV

Зауваження. $\overline{R}_A, \overline{R}_B$ – параметри, що містять половину початкових бітів R_A, R_B. Це зроблено задля більш ефективного обчислення $(Y_B)^{\overline{R}_B}, (Y_A)^{\overline{R}_A}$.

У роботі будується квантовий протокол узгодження автентичного ключа QAKAP та його модифікація з підтвердженням ключа і наводиться його аналіз щодо основних криптографічних властивостей, таких як: неявна автентифікація ключа, явна автентифікація ключа, пряма секретність, новизна ключа, стійкість до атаки з використанням компрометації ключа, стійкість до атаки з використанням невідомого ключа.

Висновки до розділу 1

В розділі розглянуто становлення квантової криптографії та її напрямки розвитку: квантовий розподіл ключа, квантова автентифікація, автентифікація користувача, квантові схеми цифрового підпису, квантовий цифровий відбиток, квантові протоколи узгодження ключа. Розглянуто основні криптографічні властивості протоколів узгодження ключа: неявна автентичність ключа, явна автентичність ключа, пряма секретність, новизна ключа, стійкість до атаки з використанням компрометації ключа, стійкість до атаки з використанням невідомого спільного ключа та інші бажані властивості. Наведено класичні протоколи узгодження ключа з автентифікацією: ефемерний Діффі-Геллман, статичний Діффі-Геллман, алгоритм обміну ключа, протокол Менезеса-К'ю-Ванстоуна.

2 СХЕМА ЦИФРОВОГО ПІДПИСУ ЧАНГА-ГОТТСМАНА ТА КВАНТОВИЙ АНАЛОГ ПРОТОКОЛУ ДІФФІ-ГЕЛЛМАНА

В цьому розділі детально розглянуто квантову схему цифрового підпису Чанга-Готтсмана [11] представленого у трьох кроках: алгоритм створення ключів, створення підпису та перевірка підпису. Надано основні теоретичні відомості квантової нотації, що використовується протягом усієї роботи. Описано квантовий протокол Діффі-Геллмана [10] та його коректність. Наведено приклад виконання квантового протоколу Діффі-Геллмана.

2.1 Основні терміни та позначення квантової моделі обчислень

Задля подальшого розуміння та роботи з qDH необхідно ввести мінімум, що потрібен для розуміння та сприйняття інформації.

Квантова нотація, або ж *bra-ket notation*, також називається *Dirac notation* – це нотація для лінійної алгебри та лінійних операторів на площині комплексних векторів, яка використовується для полегшення обчислень у квантовій механіці.

Bra-ket notation була створена Паулем Діраком і в 1939 році в його публікації *"A New Notation for Quantum Mechanics"* [8].

Означення 2.1. bra (комплексно спряжений та транспонований кет-вектор, лін. функціонал) – представлений у вигляді $\langle f|$ та математично описується як:

$$f : V \to \mathbb{C}$$

Тобто лінійне відображення що поєднує вектор V до відповідного числа на

комплексній площині $\mathbb{C}$

Означення 2.2. ket (вектор стовпчик) – представлений у вигляді $|v\rangle$ та математично представляє собою вектор v в комплексній векторній площині V.

Також нам знадобиться визначення оператора у квантовій моделі числення, а також деякі його властивості.

Означення 2.3. Оператор – це математичний об'єкт, що діє на стан системи (вектор), та результує в отриманні іншого стану системи (вектору).
Діючи деяким оператором $\hat{A}$ на вектор-стовпчик $|\psi\rangle$, що є елементом Гільбертового простору системи, отримуємо стан вектор $|\phi\rangle$, що також належить тому ж Гільбертовому простору:

$$\hat{A}\,|\psi\rangle = |\phi\rangle\,,$$

де матрична форма дії оператору $\hat{A}$ на вектор-стовпчик $|\psi\rangle$ буде мати наступний вигляд:

$$\begin{bmatrix} A_{11} & A_{12} & A_{13} & \cdots \\ A_{21} & A_{22} & A_{23} & \cdots \\ A_{31} & A_{32} & A_{33} & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix} \times \begin{bmatrix} \psi_1 \\ \psi_2 \\ \psi_3 \\ \vdots \end{bmatrix} = \begin{bmatrix} \phi_1 \\ \phi_2 \\ \phi_3 \\ \vdots \end{bmatrix}$$

Дію оператора на стан системи також можна подати наступним чином:

$$\phi_j = \sum_{i=1}^{n} A_{ji}\psi_i,$$

де A_{ji} задовільняє наступній рівності:

$$A_{ji} \equiv \langle e_j | \hat{A} | e_i \rangle ,$$

і e – є базисом для $|\psi\rangle$, тобто:

$$\hat{I} = \sum_{i=1}^{n} |e_i\rangle \langle e_i|,$$
$$|\psi\rangle = \sum_{i=1}^{n} |e_i\rangle \langle e_i|\psi\rangle.$$

Означення 2.4. Добутком двох операторів $\hat{B}\hat{A}|\psi\rangle$ є такий кет-вектор $|\rho\rangle$, що:

$$\hat{B}(\hat{A}|\psi\rangle) \overset{\text{Eq 1}}{=} \hat{B}|\phi\rangle \overset{\text{Eq 2}}{=} |\rho\rangle , \text{ де}$$

$$\textit{Eq 1: } \hat{A}|\psi\rangle = |\phi\rangle ,$$
$$\textit{Eq 2: } \hat{B}|\phi\rangle = |\rho\rangle .$$

Варто пам'ятати, що операція добутку операторів є *некомутативною*.

$$\hat{B}(\hat{A}|\psi\rangle) \neq \hat{A}(\hat{B}|\psi\rangle).$$

Означення 2.5. Тотожнім оператором $\hat{I}$ називається такий оператор, що задовольняє наступній властивості:

$$\hat{I}|\psi\rangle = |\psi\rangle .$$

Означення 2.6. *Комутатором* двох операторів $\hat{A}$ і $\hat{B}$ називається різниця операторів $\hat{A}\hat{B}$ та $\hat{B}\hat{A}$:

$$[\hat{A},\hat{B}] \equiv \hat{A}\hat{B} - \hat{B}\hat{A}$$

Аналогічно до добутку матриць – добуток операторів також некомутативний. *Комутатор*, відповідно, можна подати у наступному

вигляді:

$$[\hat{A},\hat{B}]_{ij} = \sum_{k=1}^{n} A_{ik}B_{kj} - \sum_{k=1}^{n} B_{ik}A_{kj} = \sum_{k=1}^{n}(A_{ik}B_{kj} - B_{ik}A_{kj})$$

Означення 2.7. [17] *Матриці Паулі* – ермітові оператори спіну для часток, зі спіном $\frac{1}{2}$.

Матриці Паулі представлені у вигляді трьох 2×2 матриць.

Відповідні матриці:

$$\sigma_1 = \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$\sigma_2 = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},$$

$$\sigma_3 = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

2.2 Опис квантової схеми цифрового підпису Чанга-Готтсмана

Наведемо ключові означення та схему цифрового підпису, введені Чангом та Готтсманом у роботі [11], а також аналіз квантової схеми цифрового підпису Чанга-Готтсмана.

Означення 2.8. [11] Квантовою односторонньою функцією з обмеженим використанням називають відображення виду $\{0,1\}^l \to \mathcal{H}_n$, тобто відображення множини двійкових рядків довжини l у множину станів n-кубітної квантової системи, для якої виконується умова, що $\langle f(x)|f(y)\rangle \leq \delta$ для довільних різних двійкових рядків $x, y \in \{0,1\}^l$

та деякого фіксованого значення $0 < \delta < 1$. При побудові сімейства квантових односторонніх функцій з обмеженим використанням також має виконуватися умова, що $l = \mathcal{O}(2^n)$.

Квантова схема цифрового підпису Чанга-Готтсмана формує підпис одного біту інформації і передає його використовуючи класичний і квантовий канали зв'язку. Квантовий канал зв'язку використовується для публікації відкритих параметрів, а класичний – для передачі підпису.
Розглянемо

Параметри схеми:

– A, B – учасники протоколу;
– b – біт повідомлення;
– k_b^i – особисті ключі користувача A;
– $|f_{k_b^i}\rangle$ – відкриті ключі;
– c – границя прийняття;
– M – параметр безпеки;
– f – деяка квантова одностороння функція з обмеженим використанням.

Всі користувачі протоколу знають обране відображення f та границі прийняття c.

Алгоритм створення ключів:

1) Створення особистих ключів.
Користувач A обирає M пар двійкових рядків $\{k_0^m, k_1^m\}$, $m = \overline{1,M}$, k_0 використовується для підпису повідомлення $b = 0$, k_1 для підпису повідомлення $b = 1$ відповідно, стани $\{k_0^m, k_1^m\}$ (для кожного m) – особисті ключі користувача A для деякої фіксованої односторонньої

функції f.

$$A : \{k_0^i, k_1^i\}, i = \overline{1,M}.$$

2) Створення відкритих ключів.

Користувач А обчислює пари станів n-кубітної квантової системи $\{|f_{k_0^i}\rangle, |f_{k_1^i}\rangle\}$ за допомогою квантової односторонньої функції з обмеженим використанням f.

$$A : \{|f_{k_0^i}\rangle, |f_{k_1^i}\rangle\}, i = \overline{1,M}.$$

Після створення ключів користувач А публікує пари станів n-кубітної квантової системи $\{|f_{k_0^i}\rangle, |f_{k_1^i}\rangle\}$.

Створення підпису.

Користувач А обирає біт повідомлення b та включає відповідні йому особисті ключі $k_b^1, k_b^2, \ldots, k_b^M$, після чого, створює й відправляє підписане повідомлення $(b, k_b^1, k_b^2, \ldots, k_b^M)$ класичним каналом зв'язку користувачу В.

$$A \to B : (b, k_b^1, k_b^2, \ldots, k_b^M).$$

Перевірка підпису.

Користувач В обчислює кількість неправильних ключів: $|f(k_b^i)\rangle \neq |f_{k_b^i}\rangle$, позначимо цю кількість s. Користувач В приймає підпис користувача А, якщо: $s \leqslant cM$, інакше підпис вважається недійсним і користувач В зупиняє виконання протоколу.

Кінцем виконання квантової схеми цифрового підпису вважається отримання користувачем В підписаного біт повідомлення b від користувача А (або зупинка виконання протоколу). За умови, якщо інформації більше ніж може передати схема цифрового підпису Чанга-Готтсмана – схема повторюється до моменту передання усієї

інформації.

У квантовій схемі цифрового підпису Чанга-Готтсмана можуть брати участь й більш як 2 учасників за виконання деяких додаткових умов [11].

2.3 Опис протоколу квантового Діффі-Геллмана

Результатом класичного протоколу Діффі-Геллмана є деяка спільна змінна ($Y_{AB} \equiv Y_{BA}$). Розглядаючи квантовий протокол Діффі-Геллмана, на відміну від класичного варіанту, результатом буде деякий квантовий стан $|\psi_{AB}\rangle$.

Задля реалізації квантового протоколу Діффі-Геллмана розглянемо двох користувачів A і B, що мають змогу обмінюватись кубітами. Обидва користувачі мають деякі секретні параметри, позначимо їх:

S_A - секретний параметр користувача A,

S_B - секретний параметр користувача B.

Ці секретні параметри будуть використані для генерування спільного секрету й надалі. Аналогічно до DH алгоритму Користувачі мають домовитись про публічний параметр S_P, що слугуватиме основою обчислень.

S_P в свою чергу є деяким спільним ініціалізуючим станом, що надалі будемо позначати як $|0\rangle$.

$$S_P = \{|0\rangle, \dots\},$$

де "$\dots$"– це необов'язкова, публічно відома інформація.

Поширений початковий стан $|0\rangle$ також означає, що обидва користувачі A і B матимуть змогу підготувати саме цей ініціалізуючий стан.

Варто зазначити, що стани S_A, S_B, S_P також ініціалізують індивідуальні унітарні оператори $U(S_A), U(S_B), U(S_P)$, приклад яких буде наведено пізніше.

Зважаючи на попередньо описану інформацію опишемо протокол qDH: Користувачі A і B попередньо узгоджують спільний параметр S_P.

Протокол 2.1. [10] квантовий Діффі-Геллман (qDH)

Крок 1 Користувач A підготовлює початковий стан $|0\rangle$, як було подано в публічно поданому стані S_P. Після чого обраховує та відправляє кубіт

$$|\psi_A\rangle \coloneqq U(S_A)\,|0\rangle$$

користувачу B. Де унітарний оператор $U(S_A)$ залежить від початково сформованого секрету S_A.

Крок 2 Користувач B отримує та модифікує $|\psi_A\rangle$ за допомогою свого власного унарного оператора $U(S_B)$

$$|\psi_{BA}\rangle \coloneqq U(S_B)\,|\psi_A\rangle\,.$$

В цьому випадку унітарний оператор $U(S_B)$ також залежить від попередньо сформованого секрету S_B.

Крок 3 Тепер користувач B підготовлює початковий стан $|0\rangle$, як було подано в публічно поданому стані S_P. Після чого обраховує та відправляє відповідний кубіт

$$|\psi_B\rangle \coloneqq U(S_B)\,|0\rangle$$

користувачу A.

Крок 4 Користувач A, отримавши $|\psi_B\rangle$ модифікує його за допомогою $U(S_A)$, $U(S_B)$, що відповідає:

$$|\psi_{AB}\rangle \coloneqq U(S_P)U(S_A)\,|\psi_B\rangle\,.$$

Обидва користувачі у результаті виконання протоколу 2.1 мають деякі спільні стани $|\psi_{AB}\rangle$, та $|\psi_{BA}\rangle$, що були отримані на кроках 2 і 4 відповідно. Задля успішного виконання протоколу 2.1 повинні виконуватись наступні твердження:

Твердження 2.1. *[10]*

$$U(S_P)U(S_A)U(S_B) = U(S_B)U(S_A)$$

З початкової ініціалізації для $U(S_A), U(S_B), U(S_P)$ випливає наступне твердження:

Твердження 2.2. *[10]*

$$|\psi_{AB}\rangle = |\psi_{BA}\rangle$$

В результаті виконання протоколу 2.1, обидва користувачі A і B мають ідентичні квантові стани без інформації про співрозмовника та його приватні параметри.

$$\begin{aligned} A, S_A &\xrightarrow{|\psi_A\rangle := U(S_A)|0\rangle} B, S_B \\ |\psi_{AB}\rangle &\xleftarrow{|\psi_B\rangle := U(S_B)|0\rangle} |\psi_{BA}\rangle \end{aligned}$$

Рисунок 2.1 – Схема протоколу qDH

Приклад 2.1. Користувачі A і B узгоджують спільний параметр S_P. Нехай $S_P = \{|0\rangle, \hat{n}\}$ - публічно обумовлений параметр, $\hat{n}$ - вектор $\in \mathbb{R}^3$ комплексних модулів. Нехай $S_A = \alpha$, де $\alpha \in \mathbb{R}$ - дійсне число, тоді:

$$U(S_A) = U(\alpha) \coloneqq \exp\Big(-i\frac{\alpha}{2}\hat{n} \times \hat{\sigma}\Big),$$

де $\hat{\sigma}$ з 3-вектор матриць Паулі $\sigma_i = (1..3)$ як компоненти. Це операція оберту кубіту навколо осі $\hat{n}$ на кут α. Аналогічно й для користувача B, $S_B = \beta$, де $\beta \in \mathbb{R}$:

$$U(S_B) = U(\beta) \coloneqq \exp\Big(-i\frac{\beta}{2}\hat{n} \times \hat{\sigma}\Big).$$

З таким вибором унарних операторів отримаємо:

$$[U(S_A), U(S_B)] = 0,$$

що і є потрібною умовою для твердження 2.1 та доводить рівність у твердженні 2.2.

Протоколу 2.1 використовує класичні арифметичні операції над скінченними полями, що описуються поворотами навколо осей, що повністю сходиться з квантовим представленням, як воно є.

Висновки до розділу 2

В розділі детально розглянуто квантову схему цифрового підпису Чанга-Готтсмана [11] та її особливості. Описано алгоритм створення ключів, створення підпису та перевірки підпису для цієї схеми. Наведено основні означення квантової нотації що використовуються впродовж роботи: вектор стовпчик, комплексно спряжений та транспонований вектор стовпчик, оператор, добуток операторів, тотожній оператор, матриці Паулі. Розглянуто квантовий протокол Діффі-Геллмана [10] та його особливості. Наведено приклад виконання цього протоколу.

3 ПОБУДОВА КВАНТОВОГО ПРОТОКОЛУ УЗГОДЖЕННЯ АВТЕНТИЧНОГО КЛЮЧА QAKAP

В розділі представлено побудову квантового протоколу узгодження автентичного ключа QAKAP та його модифікацію: квантовий протокол узгодження ключа з підтвердженням ключа. Наведено аналіз побудованих протоколів щодо основних криптографічних властивостей та їх доведення. Розглянуто порівняльну таблицю з класичними аналогами автентифікованих протоколів узгодження ключа. Розглянуто та проаналізовано квантовий протокол Діффі-Геллмана з автентифікацією [10] та побудовано атаки на цей протокол.

Г. Барнум та інші довели у своїй роботі [2], що квантовий підпис квантової інформації не забезпечує автентичність джерела. Д. Готтсман та І. Чанг побудували схему квантового цифрового підпису [11], що передає класичну інформацію. У зв'язку з результатами попередніх робіт, побудуємо квантовий протокол узгодження автентичного ключа QAKAP з підтвердженням ключа (quantum authenticated key agreement protocol with key confirmation), використавши ефемерний протокол Діффі-Геллмана та схему цифрового підпису Чанга-Готтсмана.

Параметри протоколу:

– A, B – учасники протоколу;
– p – деяке просте велике число;
– q – деякий простий великий дільник $p - 1$;
– g – деяке число порядку q в $\mathbb{Z}_p^*$;
– K_A, K_B – ефемерні відкриті ключі користувачів A, B;
– $R_{AB} = R_{BA}$ – спільний секрет;
– $SignCG(x)$ – схема цифрового підпису Чанга-Готтсмана.

Протокол 3.1. Квантовий Протокол Узгодження Автентичного Ключа (QAKAP)

Користувачі A і B попередньо узгоджують спільні параметри p, g.

Крок 1.

а) Користувач A обирає особистий ключ $K_A \in_R [1, q-1]$ й обчислює відкритий ключ $R_A \equiv g^{K_A} \mod p$.

б) Користувач A ініціалізує квантову схему цифрового підпису Чанга-Готтсмана (підписує і передає R_A відповідно до алгоритму описаного в розділі 2.2).

Крок 2.

а) Користувач B обирає особистий ключ $K_B \in_R [1,q-1]$ й обчислює відкритий ключ $R_B \equiv g^{K_B} \mod p$.

б) Користувач A ініціалізує квантову схему цифрового підпису Чанга-Готтсмана (підписує і передає R_B відповідно до алгоритму описаного в розділі 2.2).

$$A,K_A \xrightarrow{SignCG(g^{K_A})} B,K_B$$
$$g^{K_B K_A} \xleftarrow{SignCG(g^{K_B})} g^{K_A K_B}$$

Рисунок 3.1 – Схема протоколу QAKAP

Твердження 3.1. *Протокол узгодження автентичного ключа QAKAP забезпечує неявну автентифікацію ключа.*

Побудований квантовий протокол узгодження автентичного ключа QAKAP також гарантує новизну ключа за умови явної автентифікації ключів протоколу, у випадку продовження виконання протоколу.

Протокол 3.1 досі не забезпечує властивість явної автентифікації ключа та вразливий до атаки з використанням невідомого ключа. Беручи

до уваги перераховані недоліки протоколу, модифікуємо його за допомогою додаткового підтвердження ключа.

3.1 Побудова квантового протоколу узгодження автентичного ключа QAKAP з підтвердженням ключа

Параметри протоколу:

– A, B – учасники протоколу;

– p – деяке просте велике число;

– q – деякий простий великий дільник $p-1$;

– g – деяке число порядку q в $\mathbb{Z}_p^*$;

– K_A, K_B – ефемерні відкриті ключі користувачів A, B;

– N_0, N_1 – одноразові значення (нонси) користувачів A і B відповідно;

– $R_{AB} = R_{BA}$ – спільний секрет;

– $enc(x)_y$ – автентифіковане шифрування тексту x ключем y;

– $dec(x)_y$ – автентифіковане розшифрування шифротексту x ключем y;

– E_1, E_0 – шифротексти;

– $SignCG(x)$ – схема цифрового підпису Чанга-Готтсмана.

Протокол 3.2. Квантовий протокол автентичного ключа QAKAP з підтвердженням ключа (QAKAP with key conf.)

Користувачі A і B попередньо узгоджують спільні параметри p, g.

Крок 1.

а) Користувач A обирає особистий ключ $K_A \in_R [1,q-1]$ й обчислює відкритий ключ $R_A \equiv g^{K_A} \mod p$.

б) Користувач A обирає нонс N_0.

в) Користувач A ініціалізує квантову схему цифрового підпису Чанга-Готтсмана (підписує і передає R_A, N_0 відповідно до алгоритму

описаного в розділі 2.2).

Крок 2.

а) Користувач B, обирає особистий ключ $K_B \in_R [1,q-1]$ й обчислює відкритий ключ $R_B \equiv g^{K_B} \mod p$.

б) Користувач B (за умови, що підпис не був термінований), обчислює значення спільного секрету R_{AB}, інакше зупиняє виконання протоколу.

в) Користувач B обирає нонс N_1.

г) Користувач B обчислює шифротекст $E_0 = enc(N_0)_{R_{AB}}$.

д) Користувач B ініціалізує квантову схему цифрового підпису Чанга-Готтсмана (підписує і передає R_B, N_1 відповідно до алгоритму описаного в розділі 2.2).

е) Користувач B відправляє E_0 користувачу A.

Крок 3.

а) Користувач A (за умови, що підпис не був термінований), обчислює значення спільного секрету R_{BA}, інакше зупиняє виконання протоколу.

б) Користувач A перевіряє, що: $dec(E_0)_{R_{BA}} = N_0$, якщо перевірка не вдається, користувач A зупиняє виконання протоколу.

в) Користувач A обчислює шифротекст $E_1 = enc(N_1)_{R_{BA}}$.

г) Користувач A передає E_1 користувачу B.

Крок 4.

а) Користувач B перевіряє, що: $dec(E_1)_{R_{AB}} = N_1$, якщо перевірка не вдається, користувач B зупиняє виконання протоколу.

Враховуючи, що підпис Чанга-Готтсмана передає класичну інформацію, такий вигляд протоколу буде працювати без надання додаткових модифікацій.

Попередню версію протоколу QAKAP легко вдалось модифікувати додатковим алгоритмом підтвердження ключа за допомогою автентифікованого шифрування та одноразових значень (нонсів), що значно збільшить степінь захищеності, у порівнянні з попереднім

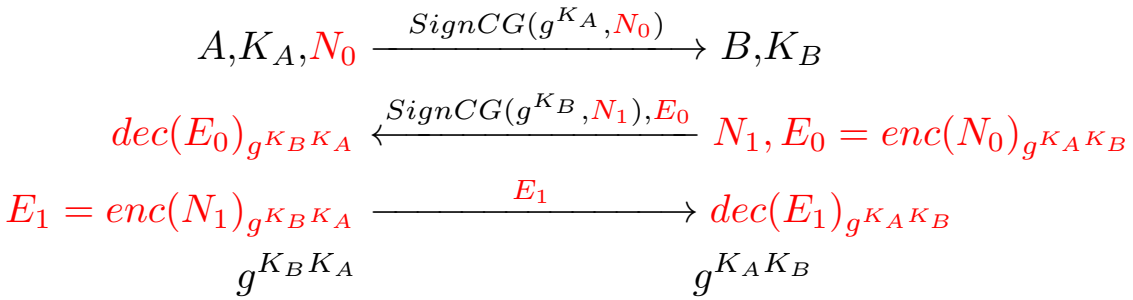

Рисунок 3.2 – Схема протоколу QAKAP з підтвердженням ключа

побудованим протоколом QAKAP, що наявно демонструється у розділі 3.2, а саме у таблиці 3.1.

3.2 Аналіз квантового протоколу узгодження автентичного ключа QAKAP з підтвердженням ключа.

В розділі 3 наведено аналіз протоколу 3.1, якому не вистачало явної автентичності ключа та можливості запобігти атаці з використанням невідомого ключа, тому модифікувавши протокол QAKAP проаналізуємо та продемонструємо його нові можливості у забезпеченні властивостей явної автентичності ключа, новизни ключа та стійкості до атаки з використанням невідомого ключа.

Твердження 3.2. *Протокол узгодження автентичного ключа QAKAP забезпечує явну автентифікацію ключа.*

Доведення. Продемонструємо надання гарантії від користувача B користувачу A.

Нехай $R_{BA} = g^{K_BK_A}$ – спільний секрет користувача A, що він отримав у ході виконання протоколу QAKAP з підтвердженням ключа, тоді на кроці 3.б протоколу 3.2 користувач A переконується у володінні аналогічного спільного секрету $R_{AB} = g^{K_AK_B}$ користувачем B за допомогою перевірки $dec(enc(N_0)_{R_{AB}})_{R_{BA}} = N_0$.

Аналогічно для користувача B (користувач A надає гарантію користувачу B) на кроці 4 протоколу 3.2. □

Твердження 3.3. *Властивість новизни ключа забезпечується при наданні явної автентифікації.*

Доведення. Кожне виконання протоколу 3.2 потребує створення нових випадкових ключів K_A^1, K_B^1, а також тих ключів, що використовуються для передачі інформації за допомогою квантової схеми цифрового підпису Чанга-Готтсмана 2.2. За умови, що протокол продовжується: всі новостворені ключі ніяким чином не залежать від обраних ключів в попередніх виконаннях протоколу K_A^0, K_B^0, а отже і отриманий спільний секрет R. □

Очевидно, що за виконання властивості 3.2 будуть виконуватись наступні твердження:

Твердження 3.4. *Протокол узгодження автентичного ключа QAKAP забезпечує неявну автентифікацію ключа.*

Твердження 3.5. *Протокол узгодження автентичного ключа QAKAP забезпечує стійкість до атаки з використанням невідомого ключа.*

Властивість явної автентифікації ключа забезпечується за допомогою використання автентифікованого розшифрування $dec(x)_y$ на кроках 3.(б), 4 протоколу 3.2. Користувачі A і B впевнені у володінні ідентичного ключа розшифрувавши шифротексти E_0, E_1 використовуючи значення спільного секрету (ключа) й отримавши значення їх одноразових значень N_0, N_1 (нонсів).

Стійкість до атаки з використанням невідомого ключа забезпечується за допомогою схеми квантового цифрового підпису Чанга-Готтсмана та автентифікованому розшифруванню $dec(x)_y$ на кроках 2(б), 3(а), 3(б), 4 протоколу 3.2. Користувачі A і B впевнені в автентичності користувача від якого отримали повідомлення.

Беручи за основу таблицю [5], що демонструє надання основних криптографічних властивостей протоколів: ефемерний Діффі-Геллманом (EDH), статичний Діффі-Геллманом (SDH), алгоритм обміну ключа (KEA), протокол Менезеса-К'ю-Ванстоуна з підтвердженням ключа (MQV with key confirmation) створимо нову таблицю 3.1, що також міститиме побудовані протоколи 3.1, 3.2 та інформації щодо їх криптографічних властивостей. Порівняємо побудовані квантові протоколи узгодження автентичного ключа з класичними аналогами.

Таблиця 3.1 надає інформацію про наступні криптографічні властивості:

– неявна автентичність ключа (*implicit key authentification, IKA*);

– явна автентичність ключа (*explicit key authentification, EKA*);

– новизна ключа (*known-key security, KK-S*);

– пряма секретність (*forward secrecy, FS*);

– стійкість до атаки з використанням компрометації ключа (*key-compromise impersonation, K-CI*);

– стійкість до атаки з використанням невідомого ключа (*unknown key-share, UK-S*).

Також у таблиці 3.1 використовуються наступні позначення:

– $\surd$ – вказує на надання гарантії користувачу A незалежно від того, чи ініціював він протокол.

– $\times$ – вказує на відсутність гарантії користувачу A.

– ? – вказує на надання гарантії за умови, що надається явна автентифікація усіх ключів сеансу.

Спираючись на данні таблиці 3.1 зробимо висновки, що побудований протокол QAKAP без модифікацій поступається більшості класичних автентифікованих протоколів і показує кращі криптографічні властивості тільки у порівнянні з ефемерним протоколом Діффі-Геллмана. В свою чергу, протокол QAKAP з підтвердженням ключа задовольняє усім розглянутим криптографічним властивостям, за винятком тих, що вимагають повторне використання протоколу, що у варіанті використання

Таблиця 3.1 – Порівняння криптографічних властивостей протоколів

Протокол	IKA	EKA	K-KS	FS	K-CI	UK-S
EDH	×	×	?	n/a	n/a	×
SDH	√	×	×	×	×	√
KEA	√	×	√	×	√	√
MQV with key conf.	√	√	√	√	√	√
QAKAP	√	×	?	n/a	n/a	×
QAKAP with key conf.	√	√	√	n/a	n/a	√

квантового цифрового підпису Чанга-Готтсмана та ефемерних ключів не є можливим. Побудований протокол QAKAP з підтвердженням ключа демонструє виключно позитивні результати у порівнянні з іншими протоколами наведеними в таблиці 3.1, за винятком протоколу Менезеса-К'ю-Ванстоуна, ключі якого можна використовувати довгостроково.

3.3 Квантовий протокол Діффі-Геллмана з автентифікацією

В розділі 2, розглянуто квантовий протокол Діффі-Геллмана побудований Дірком Фішером, окрім цього автор протоколу запропонував його варіант з автентифікацією. Розглянемо цей протокол та виділимо його основні недоліки.

Параметри протоколу:

1) A, B – учасники протоколу

2) S_A, S_B – особисті параметри учасників A і B.

3) S_P – публічний параметр.

4) $U(S_A), U(S_B), U(S_P)$ – індивідуальні унітарні оператори.

5) $|\psi_A\rangle, |\psi_B\rangle$ – особисті стани користувачів A і B.

6) $|\phi\rangle$ – стан ідентифікатор користувача A.

Протокол 3.3. [21] Квантовий протокол Діффі-Геллмана з автентифікацією (aqDH)

Крок 1.

а) Користувач A утворює кубіт $|\psi_A\rangle = U(S_A)|0\rangle$ і обирає довільний $|\phi\rangle \in S_A$. $|\phi\rangle$ виконуватиме функцію автентифікації користувача B до користувача A.

б) Користувач A передає у довільній послідовності параметри $|\psi_A\rangle, |\phi\rangle$ за допомогою квантового каналу зв'язку.

Крок 2.

а) Користувач B обирає довільний стан $|\eta_1\rangle \in \{|\psi_A\rangle, |\phi\rangle\}$.

б) Користувач B обчислює $|\eta_1\rangle \to U(S_B)|\eta_1\rangle =: |\psi_{BA}\rangle$.

в) Користувач B утворює кубіт $|0\rangle \to U(S_B)|0\rangle =: |\psi_B\rangle$.

г) Користувач B передає у довільній послідовності $\{|\psi_B\rangle, |\eta_2\rangle\}$, де $|\eta_2\rangle \in \{|\psi_A\rangle, |\phi\rangle\} \setminus |\eta_1\rangle$ користувачу A за допомогою квантового каналу зв'язку.

д) Користувач B повідомляє, який зі станів він використав для утворення спільного секрету, а також порядок відправлених ним кубітів користувачу A за допомогою класичного каналу зв'язку.

Зауваження.

1) Відповідно до кроку 1.а) протоколу 3.3 кубіт $|\phi\rangle$, слугує автентифікатором, але на кроці 2.а) з ймовірністю 1/2 користувач B може обрати його для утворення спільного секрету $|\psi_{BA}\rangle$ на кроці 2.б), що надалі призведе до різних значень спільного секрету.

2) Користувач B на кроці 2.д) протоколу 3.3 повідомляє про порядок використаних ним кубітів для утворення спільного секрету але через те, що він може сказати тільки його порядковий номер (тобто перший чи другий кубіт), користувач B може ввести користувача A в оману, оскільки при транспортуванні кубітів за допомогою квантового каналу зв'язку вони могли потрапити до користувача B в відмінному від

початково запланованого користувачем A порядку.

3) Користувач B не отримує підтвердження про отримання кубітів користувачем A після виконання кроку 2.г) протоколу 3.3, після чого повідомляє ключову інформацію щодо отриманих і відправлених ним кубітів на кроці 2.д), що може призвести до захоплення кубіту, що забезпечує автентифікацію користувача B перед користувачем A. Активний зловмисник M, перехопивши останні повідомлення від користувача B, має змогу ввести в оману користувача A замінивши $|\psi_B\rangle$, на свій кубіт $|\psi_M\rangle$, в такому випадку обидва користувачі будуть впевнені в тому, що протокол був виконаний успішно отримавши різні значення спільного секрету.

Крок 3.

а) Користувач A, отримавши $\{|\psi_B\rangle, |\eta_2\rangle\}$, і порядок отриманих ним кубітів модифікує $|\psi_B\rangle := U(S_P)U(S_A)|\psi_B\rangle$

б) Користувач A перевіряє, що $|\eta_2\rangle = |\phi\rangle$, інакше зупиняє виконання протоколу.

Зауваження. Знову таки, на кроці 1.а) протоколу 3.3 користувач A міг отримати кубіти в відмінній від початкової, відправленої послідовності користувачем B.

Схема 1 (Атака віддзеркалення повідомлення)

1) $A \to B : \{|\psi_A\rangle, |\phi\rangle\}$

2) $B \to A : \{|\psi_B\rangle, |\eta_2\rangle\}$

3) $B \to A$: порядок

Протокол 3.3, за словами автора [10], спрямований на запобігання атаки MitM, і сформульовано наступне твердження на цей рахунок:

Твердження 3.6. *[10] Автентифікований протокол Діффі-Гелльмана виявляє втручання активного зловмисника з ймовірністю* $p(detect) = 3/4$ *після однієї ітерації виконання протоколу, і з ймовірністю* $p(detect, n) = 1 - (1/4)^n$ *для* n *ітерацій виконання протоколу.*

Твердження 3.6 можна вважати справедливим тільки за умови, що користувач B завжди обирає правильний кубіт, і при транспортуванні, кубіти потрапляють до отримувача в початково заданому порядку.

Протокол 3.3 очевидно не задовільняє сучасні вимоги криптографічних протоколів, окрім того, має сумнівну захищеність від атак за участю активного зловмисника. Активний зловмисник – зловмисник, що може безпосередньо взаємодіяти з вмістом повідомлень, що відправляються, а також взаємодіяти з будь-яким користувачем мережі, видаючи себе за будь-якого іншого користувача тієї ж мережі.

Використання активного зловмисника для аналізу протоколів ознайомило світ з великою кількістю атак, найпопулярнішими з яких є:

1) **"Атака посередині"(MitM)**: атака запропонована Діффі та Геллманом у 1977 році [7], що також показала вагомість автентифікації повідомлень, і яка була мотивацією Дірка Фішера для побудови протоколу 3.3 у роботі [10].

2) **Атака повторного надсилання повідомлення (replay attack)**: атака в якій зловмисник затримує або повторює надсилання повідомлення.

3) **Атака паралельних сеансів (parallel-session attack)**: атака в якій 2 або більше сеансів одного протоколу здійснюються одночасно.

4) **Атака віддзеркалення повідомлення (refrection attack)**: атака в якій зловмисник перенаправляє повідомлення до відправника, задля, в основному, автентифікації в протоколах, що використовують конструкцію "виклику-відповіді".

Звичайно перелік атак є неповним і його можна доповнювати. Дірк Фішер надав ймовірнісну оцінку 3.6 виявлення активного зловмисника, що намагається здійснити атаку MitM. Взявши до уваги зауваження до протоколу 3.3, побудуємо атаку віддзеркалення повідомлення та атаку паралельних сеансів за участю активного зловмисника M.

$M(X)$ – активний зловмисник, який видає себе на учасника X.

Атака 3.1. (Атака віддзеркалення повідомлення)

1) $A \to M(A) : \{|\psi_A\rangle, |\phi\rangle\}$
2) $M(A) \to A : \{|\psi_A\rangle, |\phi\rangle\}$

Активний зловмисник $M(A)$ перехоплює повідомлення $\{|\psi_A\rangle, |\phi\rangle\}$, що надсилає користувач A і пересилає його користувачу A без внесення змін. Згідно протоколу 3.3 активний зловмисник може обрати будь-який стан системи за стан автентифікації $|\phi\rangle$, це продемонстровано на кроці 2.a) цього ж протоколу. В такому випадку зловмисник $M(A)$ очевидно може сказати користувачу A, який стан він начебто вибрав для утворення спільного секрету, а який для автентифікації перед користувачем A.

Результатом виконання атаки 3.1, користувач A отримує відмінний, від передбачуваного спільного секрету з користувачем B $|\psi_{AB}\rangle$. Натомість користувач A отримує $|\psi_{AA}\rangle$ залишаючись впевненим в успішному виконанні протоколу 3.3.

Очевидно атака 3.1 не потребує додаткових обрахунків і є дуже прямолінійною у своїй реалізації, звідси можна сказати, що складність атаки 3.1 є поліноміальною.

Атака 3.2. (Атака паралельних сеансів)
1) $A \to M(B) : \{|\psi_A\rangle, |\phi\rangle\}$
1') $M(A) \to B : \{|\psi_A\rangle, |\phi\rangle\}$
2') $B \to M(A) : \{|\psi_B\rangle, |\eta\rangle\}$
3') $B \to M(A)$: порядок кубітів
2) $M(B) \to A : \{|\eta\rangle, |\psi_M\rangle\}$
3) $M(B) \to A$: порядок кубітів

Атака 3.2 реалізується за допомогою перехоплення повідомлення від користувача A зловмисником $M(B)$ у протоколі 3.3, та ініціалізацією того ж протоколу 3.3 з користувачем B (видаючи себе за користувача A). В атаці 3.2 кроки 1), 2), 3) відповідають першому сенсу (сеансу в якому зловмисник M перехопив повідомлення від користувача A), а кроки 1'), 2'), 3') другому сеансу, де зловмисник M видає себе за користувача A.

Активний зловмисник M перехоплює повідомлення $\{|\psi_A\rangle, |\phi\rangle\}$

користувача A й ініціалізує виконання протоколу з користувачем B, після чого зловмисник чесно виконує усі кроки протоколу 3.3 з користувачем B. В результаті користувач B отримає спільний секрет $|\psi_{BA}\rangle$, наче він спілкувався з користувачем A. Зловмисник, в свою чергу, продовжує виконання протоколу 3.3 з користувачем A. Зловмисник, отримавши від користувача B раніше пару станів $\{|\psi_B\rangle, |\eta\rangle\}$ і їх призначення може замінити стан $|\psi_B\rangle$ на свій довільний стан $|\psi_M\rangle$ і передати новоутворене повідомлення $\{|\eta\rangle, |\psi_M\rangle\}$ користувачу A, зазначивши порядок, отриманий від користувача B у другому сеансі. Користувач A отримає задовільний результат перевірки автентичності маючи відмінний від користувача B спільний секрет $|\psi_{AM}\rangle$.

Складність атаки 3.2, не зважаючи на участь у двох сеансах протоколу 3.3 є поліноміальною, оскільки зловмисник не виконував додаткових обчислень, єдину операцію, що виконує зловмисник застосовуючи атаку 3.2 є утворення кубіту $|\psi_M\rangle$, що може бути довільним.

Атака 3.3. (Атака паралельних сеансів)

1) $A \to M(B) : \{|\psi_A\rangle, |\phi\rangle\}$

1') $M(A) \to B : \{|\psi_M\rangle, |\phi\rangle\}$

2') $B \to M(A) : \{|\psi_B\rangle, |\eta\rangle\}$

3') $B \to M(A)$: порядок кубітів

2) $M(B) \to A : \{|\eta\rangle, |\psi_B\rangle\}$

3) $M(B) \to A$: порядок кубітів

Атака 3.3 є аналогічною до атаки 3.2, єдиною різницею є те, що в атаці 3.3 користувач B отримує відмінний від запланованого стану $|\psi_{BA}\rangle$ стан $|\psi_{BM}\rangle$.

Очевидно, що складність атаки 3.3 дублює складність атаки 3.2, тобто є поліноміальною.

В результаті аналізу протоколу 3.3 можна сказати, що цей протокол потребує допрацювання або повного його переопрацювання, оскільки навіть популярні атаки за участю активного зловмисника виявились

фатальними для протоколу 3.3, а атака MitM згідно з твердженням 3.6 для 1 ітерації протоколу успішно реалізується з шансом 1/4.

Висновки до розділу 3

В розділі побудовано квантовий протокол узгодження автентичного ключа QAKAP 3.1 та наведено його аналіз щодо криптографічних властивостей зазначених у розділі 1. Поставлено під сумнів безпечність побудованого протоколу та надано його модифікацію: квантовий протокол узгодження автентичного ключа QAKAP 3.2 з підтвердження ключа та, відповідно, його аналіз. Доведено криптографічні властивості, що забезпечують побудовані протоколи. Надано порівняльну таблицю 3.1, що включає побудовані протоколи, а також розглянуті класичні аналоги у розділі 1 щодо основних криптографічних властивостей. У результаті порівняльного аналізу виділено квантовий протокол узгодження автентичного ключа QAKAP з підтвердження ключа, Розглянуто та виділено недоліки квантового протоколу Діффі-Геллмана з автентифікацією [10]. Розглянуто концепцію активного зловмисника та популярні атаки за його участю. Побудовано атаку віддзеркалення повідомлень 3.1 та атаки паралельних сеансів 3.2, 3.3.

ВИСНОВКИ

У результаті виконання роботи розглянуто квантову схему цифрового підпису Чанга-Готтсмана [11] поділеного на 3 етапи: алгоритм створення ключів, створення підпису та перевірка підпису.

Побудовано новий квантовий протокол узгодження автентичного ключа QAKAP, а також проаналізовано даний протокол щодо основних криптографічних властивостей як: неявна автентичність ключа, явна автентичність ключа, пряма секретність, новизна ключа, стійкість до атаки з використанням компрометації ключа та стійкість до атаки з використанням невідомого спільного ключа.

Модифіковано квантовий протокол узгодження ключа QAKAP за допомогою додаткового підтвердження ключа та проаналізовано новоутворений протокол щодо наявності попередніх криптографічних властивостей.

Проведено порівняльний аналіз побудованих квантових протоколів узгодження автентичного ключа з класичними протоколами узгодження автентичного ключа, таких як: ефемерний Діффі-Геллман, статичний Діффі-Геллман, алгоритм обміну ключа та протокол Менезеса-К'ю-Ванстоуна з підтвердженням ключа щодо криптографічних властивостей цих протоколів.

В результаті порівняльного аналізу виділено квантовий протокол узгодження автентичного ключа QAKAP з підтвердженням ключа, чиї недоліки, у порівнянні з протоколом Менезеса-К'ю-Ванстоуна полягали виключно у використанні ефемерних ключів, що унеможливило задовільнити властивості прямої секретності та стійкості до атаки з використанням компрометації ключа.

Розглянуто та виділено недоліки квантового аналогу протоколу Діффі-Геллмана з автентифікацією [10]. Зважаючи на виділені недоліки побудовано атаку віддзеркалювання повідомлення 3.1 та атаки

паралельних сесій 3.2, 3.3, що є одними з найпопулярніших атак за участю активного зловмисника.

Подальшим напрямком дослідження може стати модифікація, або використання іншої квантової схеми цифрового підпису задля зменшення необхідної кількості кубіт для підпису повідомлення, що також зменшить їх необхідну кількість у побудованих квантових протоколах узгодження автентичного ключа.

ПЕРЕЛІК ПОСИЛАНЬ

[1] H. Barnum та ін. «Authentication of quantum messages». В: *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.* IEEE Comput. Soc. DOI: 10.1109/sfcs.2002.1181969. URL: http://dx.doi.org/10.1109/SFCS.2002.1181969.

[2] Howard N. Barnum. *Quantum secure identification using entanglement and catalysis*. 1999. arXiv: quant-ph/9910072 [quant-ph].

[3] Charles H. Bennett та Gilles Brassard. «Quantum cryptography: Public key distribution and coin tossing». В: *Theoretical Computer Science* 560 (груд. 2014), 7–11. ISSN: 0304-3975. DOI: 10.1016/j.tcs.2014.05.025. URL: http://dx.doi.org/10.1016/j.tcs.2014.05.025.

[4] Alex Biryukov. «Skipjack». В: *Encyclopedia of Cryptography and Security*. За ред. Henk C. A. van Tilborg та Sushil Jajodia. Boston, MA: Springer US, 2011, с. 1220—1221. ISBN: 978-1-4419-5906-5. DOI: 10.1007/978-1-4419-5906-5_616. URL: https://doi.org/10.1007/978-1-4419-5906-5_616.

[5] Simon Blake-Wilson та Alfred Menezes. «Authenticated Diffie-Hellman Key Agreement Protocols». В: *ACM Symposium on Applied Computing*. 1998. URL: https://api.semanticscholar.org/CorpusID:18711708.

[6] Harry Buhrman та ін. «Quantum Fingerprinting». В: *Physical Review Letters* 87.16 (вер. 2001). ISSN: 1079-7114. DOI: 10.1103/physrevlett.87.167902. URL: http://dx.doi.org/10.1103/PhysRevLett.87.167902.

[7] W. Diffie та M.E. Hellman. «Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard». В: *Computer* 10.6 (1977), с. 74—84. DOI: 10.1109/C-M.1977.217750.

[8] P. A. M. Dirac. «A new notation for quantum mechanics». В: *Mathematical Proceedings of the Cambridge Philosophical Society* 35.3 (1939), 416–418. DOI: 10.1017/S0305004100021162.

[9] David P DiVincenzo та Daniel Loss. «Quantum computers and quantum coherence». В: *Journal of Magnetism and Magnetic Materials* 200.1–3 (жовт. 1999), 202–218. ISSN: 0304-8853. DOI: 10 . 1016 / s0304 - 8853(99) 00315 - 7. URL: http://dx.doi.org/10.1016/S0304-8853(99)00315-7.

[10] Dirk Fischer. *Quantum Diffie-Hellman Key Exchange*. Cryptology ePrint Archive, Paper 2021/1279. https://eprint.iacr.org/2021/1279. 2021. URL: https://eprint.iacr.org/2021/1279.

[11] Daniel Gottesman та Isaac Chuang. *Quantum Digital Signatures*. 2001. arXiv: quant-ph/0105032 [quant-ph].

[12] Jens G Jensen та Ruediger Schack. *Quantum authentication and key distribution using catalysis*. 2000. arXiv: quant-ph/0003104 [quant-ph].

[13] Burton S. Kaliski. «An unknown key-share attack on the MQV key agreement protocol». В: *ACM Trans. Inf. Syst. Secur.* 4.3 (2001), 275–288. ISSN: 1094-9224. DOI: 10 . 1145 / 501978 . 501981. URL: https://doi.org/10.1145/501978.501981.

[14] Laurie Law та ін. «An Efficient Protocol for Authenticated Key Agreement». В: *Designs, Codes and Cryptography* 28.2 (2003), с. 119—134. ISSN: 1573-7586. DOI: 10 . 1023 / A : 1022595222606. URL: https://doi.org/10.1023/A:1022595222606.

[15] Dominic Mayers. *Unconditional security in Quantum Cryptography*. 2004. arXiv: quant-ph/9802025 [quant-ph].

[16] Roger M. Needham та Michael D. Schroeder. «Using encryption for authentication in large networks of computers». В: *Commun. ACM* 21.12 (1978), 993–999. ISSN: 0001-0782. DOI: 10 . 1145 / 359657 . 359659. URL: https://doi.org/10.1145/359657.359659.

[17] Michael A. Nielsen та Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[18] Dave Otway та Owen Rees. «Efficient and timely mutual authentication». В: *SIGOPS Oper. Syst. Rev.* 21.1 (1987), 8–10. ISSN: 0163-5980. DOI: 10.1145/24592.24594. URL: https://doi.org/10.1145/24592.24594.

[19] Dömötör Pálvölgyi. *Communication Complexity*. 2010. arXiv: 1007.1841 [cs.CC].

[20] Peter W. Shor та John Preskill. «Simple Proof of Security of the BB84 Quantum Key Distribution Protocol». В: *Physical Review Letters* 85.2 (лип. 2000), 441–444. ISSN: 1079-7114. DOI: 10.1103/physrevlett.85.441. URL: http://dx.doi.org/10.1103/PhysRevLett.85.441.

[21] IEEE Computer Society та ін. *Proceedings of International Conference on Computers, Systems & Signal Processing, Dec. 9-12, 1984, Bangalore, India*. Steering Committee, 1984. URL: https://books.google.com.ua/books?id=H0p0NQAACAAJ.

[22] Guihua Zeng та Christoph H. Keitel. «Arbitrated quantum-signature scheme». В: *Physical Review A* 65.4 (квіт. 2002). ISSN: 1094-1622. DOI: 10.1103/physreva.65.042312. URL: http://dx.doi.org/10.1103/PhysRevA.65.042312.

[23] Yong-Sheng Zhang, Chuan-Feng Li та Guang-Can Guo. *Quantum authentication using entangled state*. 2000. arXiv: quant-ph/0008044 [quant-ph].