Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: «*Використання оптимізованих алгоритмів асиметричної криптографії (CL-PKE) для пристроїв із обмеженими ресурсами*»

Виконав(ла): студент(ка) *VI* курсу, групи СБм-61
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Ганайчук О. В. (прізвище та ініціали)

Керівник (підпис) Александер М.А. (прізвище та ініціали)

Нормоконтроль (підпис) Кареліна О.В. (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н.В. (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль
2021

Міністерство освіти і науки України

Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії

(повна назва факультету)

Кафедра кібербезпеки

(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри

(підпис) (прізвище та ініціали)

« » 20___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня **Магістр**

(назва освітнього ступеня)

за спеціальністю *125 Кібербезпека*

(шифр і назва спеціальності)

студенту *Ганайчуку Олександру Володимировичу*

(прізвище, ім'я, по батькові)

1. Тема роботи *Використання оптимізованих алгоритмів асиметричної криптографії (CL-PKE) для пристроїв із обмеженими ресурсами*

Керівник роботи *Александер Марек Богуслав доктор технічних наук, професор кафедри КБ*

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «___» _____ 20___ року № _____.

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи

4. Зміст роботи (перелік питань, які потрібно розробити)

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г. М.		
Безпека в надзвичайних ситуаціях	Клепчик В.М.		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	*Примітка*
1	Ознайомлення з завданням до кваліфікаційної		
	роботи		
2	Збір літератури по темі кваліфікаційної роботи.		
3	Переклад та класифікування зібраної		
	інформації.		
4	Детальне вивчення та аналіз усієї інформації		
	пов’язаної з алгоритмами асиметричної		
	криптографії		
5	Розоробка оптимізлваного алгоритму		
	асиметричної криптографії		
6	Оформлення розділу”Огляд існуючих		
	алгоритмів”.		
8	Оформлення розділу”Еліптична крива та роль її		
	в криптографії”.		
9	Оформлення розділу”Розробка оптимізованого		
	алгоритму”.		
10	Оформлення кваліфікаційної роботи		
12	Нормоконтроль		
13	Перевірка на плагіат		
14	Захист кваліфікаційної роботи		

Студент _____ Ганайчук О. В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Александер М.А.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Використання оптимізованих алгоритмів асиметричної криптографії (CL-PKE) для пристроїв із обмеженими ресурсами // Дипломна робота ОР «Магістр» // Ганайчук Олександр Володимирович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2021 // С. 48 , рис. – 3 , табл. – 1 , слайдів – 10, додат. – 1.

Ключові с'лова — КРИПТОГРАФІЯ З ЕЛІПТИЧНОЮ КРИВОЮ; КРИПТОСИСТЕМА ВІДКРИТОГО КЛЮЧА БЕЗ СЕРТИФІКАТІВ; ШИФРУВАННЯ ВІДКРИТОГО КЛЮЧА БЕЗ СЕРТИФІКАТІВ; ПІДПИС ВІДКРИТОГО КЛЮЧА БЕЗ СЕРТИФІКАТА

В роботі проведено огляд літературних джерел в області дослідження. Проведено аналіз існуючих оптимізованих алгоритмів CL-PKE. Запропоновано оптимізований алгоритм асиметричної криптографії для пристроїв з обмеженим доступом.

У першій главі проведений огляд існуючих алгоритмів.

У другій главі проведено аналіз еліптичної кривої та способи її використання у криптографії та проведений аналіз криптографії з відкритим ключем без сертифікатів.

У третій главі проведена розробка оптимізованого алгоритму та проведено аналіз безпеки даного алгоритму.

У підрозділі "Охорона праці" розглянуто правила охорони праці під час експлуатації електронно-обчислювальних машин У підрозділі "Безпека в надзвичайних ситуаціях " описано способи підвищення стійкості роботи об'єктів господарської діяльності у воєнний час.

ANNOTATION

Use of Optimized Algorithms of Asymmetric Cryptography (CL-PKE) for Resource Constrained Devices // Thesis of the Master degree // Hanaichuk Oleksandr // Ternopil Ivan Puluj National Technical University, Department of Computer Information Systems and Software Engineering, Department of Cybersecurity // Ternopil, 2021 // P.48 , Tables – 1 , Fig. – 3, Annexes – 1.

Keywords — elliptic curve cryptography; certificate-less public key cryptosystem; certificate-less public key encryption; certificate-less public key signature

The paper reviews the literature in the field of research. The analysis of the existing optimized CL-PKE algorithms is carried out. An optimized asymmetric cryptography algorithm for devices with limited access is proposed.

The first chapter reviews the existing algorithms.

The second chapter analyzes the elliptic curve and ways to use it in cryptography and analyzes public key cryptography without certificates.

In the third chapter the development of the optimized algorithm is carried out and the security analysis of this algorithm is carried out.

The subsection "Occupational Safety" discusses the rules of occupational safety during the operation of electronic computers. The subsection "Safety in Emergencies" describes ways to increase the sustainability of economic activities in wartime.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

CL-PKE шифрування відкритого ключем без сертифікатів

IBE – шифрування на основі ідентифікації

PKE – шифрування з відкритим ключем

CA – центр сертифікації відкритих ключів

PKI – Інфраструктура відкритих ключів

ID-PKC – Криптографія відкритого ключа на основі ідентифікатора

KGC – Центр генерації ключів

ECDSA – алгоритм з відкритим ключем для створення цифрового підпису

ECIES – схема шифрування на відкритих ключах, що ґрунтується на еліптичних кривих.

ВСТУП

Бездротові сенсорні мережі та вбудовані системи реального часу складаються з недорогих пристроїв з обмеженими ресурсами, таких як сенсорні вузли, RFID-чіпи, мікроконтролери тощо, які збирають, аналізують, зберігають або передають конфіденційні дані у віддалене місце . Найбільш підходящим механізмом для забезпечення конфіденційності цих конфіденційних даних є шифрування. Через обмежені обчислювальні та інші типи апаратного забезпечення такі ресурси, як час процесора та енергія, споживані даною схемою безпечного шифрування, повинні бути мінімальними, щоб навіть недорогий пристрій міг брати участь у безпечному зв'язку. Тому звичайні схеми шифрування з вичерпними ресурсами не можуть бути використані. Для цих пристроїв нам потрібна безпечна полегшена схема шифрування, яка споживає мінімальний процесорний час, пам'ять, енергію, пропускну здатність тощо. Однак полегшена схема шифрування не є вимогою лише для обмежених пристроїв. Це також корисно для таких додатків, як електронне здоров'я , у яких конфіденційна статистика про здоров'я тисяч пацієнтів збирається незалежним агрегатором із обмежених датчиків. Для сумісності агрегатор повинен підтримувати легку схему шифрування, яку можуть дозволити нижчі датчики. Шифрування з симетричним ключем зазвичай вимагає низьких витрат на обчислення і може бути використане як рішення-кандидат. Однак він вимагає встановлення унікального ключа між кожною парою комунікаційних об'єктів таким чином, щоб зберігалася конфіденційність та автентичність ключа. Імовірність скомпрометації ключа також висока через його спільну природу. Крім того, криптографія симетричного ключа не може бути використана для досягнення невідмовності.

Обмеження шифрування симетричного ключа можна вирішити за допомогою шифрування з відкритим ключем (PKE), в якому один відкритий ключ використовується всіма користувачами, а кожен користувач має власний закритий ключ, який не ділиться нікому. Його можна використовувати для спільного доступу до симетричного (сесійного) ключа автентичним і безпечним

способом. Для забезпечення автентичності відкритого ключа він використовує сертифікати, отримані від центру сертифікації (ЦС). Однак він страждає від проблеми керування сертифікатами і вимагає постійного онлайнового центру сертифікації. Ці проблеми можна вирішити, використовуючи алгоритми шифрування на основі ідентифікації (IBE) і шифрування без сертифікатів із відкритим ключем (CL-PKE), які не залежать від сертифікатів відкритих ключів і ЦС, що завжди в мережі. І IBE, і CL-PKE залежать від офлайн-довіреної третьої сторони (TTP) для видачі повних приватних ключів (IBE) або часткових приватних ключів (CL-PKE) користувачам у мережі. Однак IBE страждає від проблеми депонування ключів, коли всі приватні ключі користувачів розкриваються, якщо TTP скомпрометований або стає шкідливим. CL-PKE не страждає від проблеми депонування ключів і кваліфікується як безпечна схема шифрування. Однак алгоритм шифрування всіх існуючих схем IBE та CL-PKE вимагає обчислення модульного піднесення до степеня та операцій білінійного парування над адитивною еліптичною кривою, які є дуже дорогими з точки зору обчислень. криптографічні операції [13]. Таким чином, існуючі схеми IBE або CL-PKE занадто дорогі або непридатні, щоб їх розглядати як безпечну та легку схему шифрування. Зауважимо, що в літературі вже існує спрощена схема підпису на основі ідентифікації (IBS) без експоненціювання та білінійної операції парування для генерації підпису. Мета і завдання дослідження. Метою магістерської роботи є дослідження оптимізованих алгоритмів асиметричної криптографії (CL-PKE) та розробка такого алгоритму для пристроїв з обмеженим доступом.

Мета дослідження обумовила поставлення та розв’язання наступних завдань:

- проаналізувати існуючі алгоритми CL-PKE
- проаналізувати як можна оптимізувати алгоритм CL-PKE для пристроїв з обмеженими ресурсами.
- Розробити новий оптимізований алгоритм криптографії для пристроїв з обмеженими ресурсами.

Об’єктом дослідження магістерської роботи є алгоритми асиметричної криптографії.

Наукова новизна роботи: було розроблено новий алгоритм асиметричної криптографії (CL-PKE) для пристроїв з обмеженими ресурсами;

Апробація результатів дослідження. Основні положення та результати дослідження обговорювалися на IX науково-технічній конференції Тернопільського Національного Технічного Університету імені Івана Пулюя “Інформаційні моделі, системи та технології” (Тернопіль, 2021).h

1 ОГЛЯД ІСНУЮЧИХ АЛГОРИТМІВ

Основна проблема сьогодні при розробці безпечних систем на основі криптографії з відкритим ключем полягає не в тому, щоб вибрати відповідні безпечні алгоритми або реалізувати ці алгоритми. Швидше, це розгортання та керування інфраструктурами для підтримки автентичності криптографічних ключів: існує потреба надати користувачеві впевненості у зв'язку між відкритим ключем та ідентичністю (або повноваженнями) власника приватного ключа. ключ. У традиційній інфраструктурі відкритих ключів (PKI) ця гарантія надається у вигляді сертифіката, по суті, підпису центру сертифікації відкритих ключів (CA). Слід звернути увагу на питання, пов'язані з управлінням сертифікатами, включаючи відкликання, зберігання та розповсюдження, а також оцінку вартості сертифікації сертифікатів. Вони особливо гострі в середовищах з процесором або обмеженою пропускною здатністю. Криптографія з відкритим ключем аутентифікації (ID-PKC) вирішує проблему автентичності ключа іншим способом, ніж традиційна PKI. У ID-PKC відкритий ключ об'єкта отримують безпосередньо з певних аспектів його ідентичності, наприклад, IP-адреса, що належить мережевому хосту, або адреса електронної пошти, пов'язана з користувачем. Закриті ключі генеруються для сутностей довіреною третьою стороною, яка називається генератором приватних ключів (PKG). Відтоді ID-PKC швидко розвивався. Зараз існують протоколи обміну ключами на основі аутентифікації (інтерактивні та неінтерактивні), схеми підписів, ієрархічні схеми та багато інших примітивів. Отримання відкритих ключів безпосередньо з ID-PKC усуває потребу в сертифікатах і деякі проблеми, пов'язані з ними. З іншого боку, залежність від PKG, яка використовує загальносистемний головний ключ для генерування приватних ключів, неминуче вносить депозит ключів у системи IDPKC. Наприклад, PKG може розшифрувати будь-який зашифрований текст у схемі шифрування з відкритим ключем на основі ідентифікації. Не менш проблематично те, що PKG може підробити підписи будь-якої сутності в схемі підпису на основі ідентифікації, тому ID-PKC не може запропонувати справжню відмову, як традиційний PKI. Проблему утилізації можна певною мірою

вирішити за допомогою введення кількох PKG та використання порогових методів, але це обов'язково потребує додаткового зв'язку та інфраструктури. Крім того, компрометація головного ключа PKG може бути катастрофічною в системі ID-PKC і зазвичай є більш серйозною, ніж скомпрометація ключа підпису CA в традиційному PKI. З цих причин здається, що використання ID-PKC може бути обмежено невеликими закритими групами або додатками з обмеженими вимогами безпеки.

1.1 Криптографія з відкритим ключем без сертифікатів

Сертифікована криптографія (CL-PKC) була вперше введена Аль-Ріямі та Паттерсоном у їхній роботі [21]. На роботу сильно вплинула схема шифрування, заснована на ідентифікації Боннета і Франкліна, і в результаті є розширенням оригінального IBE. CL-PKC усуває функцію депозиту ключів у генераторі приватних ключів. Натомість генерація приватних ключів поширюється між користувачем і третьою стороною, яка довіряє, під назвою Центр генерації ключів (KGC). Отже, відкритий ключ користувача є парою, що складається з ідентифікатора та відкритого ключа PA. Ключ уже не так легко запам'ятати, як у оригінальному IBE, але рівень довіри до третьої сторони значно нижчий. Функціональність CL-PKC, схоже, знаходиться десь між традиційним сертифікованим PKI та криптографією на основі облікових даних. Гнучкість є одним з найважливіших атрибутів криптографії без сертифікатів; насправді його можна трансформувати в традиційний PKI або IBE. Як і IBE, математична основа CL-PKE базується на еліптичних кривих і складності знаходження дискретних логарифмів у скінченних групах. Основні особливості CL-PKC включають відсутність властивостей депозиту ключів, відсутність сертифікатів для гарантії автентичності відкритих ключів, використання облікових даних та існування третьої сторони, яка бере участь у створенні ключів. Для публічного шифрування потрібні загальнодоступні налаштування, особистість одержувача та відкритий ключ. Використання аутентифікації в шифруванні не дозволяє будь-якій іншій стороні розшифрувати вміст, навіть якщо хтось намагається підробити другу частину відкритого ключа.

Крім того, друга частина відкритого ключа (тобто точка на еліптичній кривій) заважає KGC розшифрувати повідомлення.

Розповсюдження відкритих ключів працює так само, як і в PKI, користувач публікує свій відкритий ключ у загальнодоступному каталозі або додає його до вихідних електронних листів. Поки KGC не намагається підробити ключ, усі зашифровані дані є безпечними. Це означає, що KGC має бути таким же довіреним, як і CA в традиційній інфраструктурі відкритих ключів. Однак будь-яку заборонену діяльність KGC користувачі можуть виявити. На практиці жоден CO не наважується оприлюднити підроблені ключі, оскільки це виводить компанію з прибуткового бізнесу, тож можна вважати, що KGK поводиться чесно. Таким чином, ви можете створити безпечне прозоре шифрування електронної пошти, яке дозволить нетехнічним користувачам спілкуватися конфіденційно. На відміну від PKI, схема без сертифікатів не вимагає дорогої інфраструктури, яка складається з різних органів влади. Як і IBE, все, що вам потрібно, це центр генерації ключів і загальнодоступний сервер. Найкращий вибір — розмістити їх у просторі імен, наприклад у зоні DNS. Ці два сервери оброблятимуть весь вхідний трафік.

1.2 Алгоритми

Шифрування з відкритим ключем без сертифікатів із обраним захистом шифротексту (в [21] називається Full CL-PKE) засноване на семи випадкових алгоритмах:

- Setup: KGC зазвичай запускається для створення загальнодоступних налаштувань і пар головних ключів. Вхідним параметром для алгоритму є параметр безпеки k, який визначає міцність криптосистеми. Вихід складається з загальнодоступних параметрів $P = \langle G_1, G_2, G_T, e, n, P, P_{pub}, H_1, H_2, H_2, H_3, H_4 \rangle$, опис кінцевого простору повідомлень $M = \{0,1\}^n$ і простору зашифрованого тексту $C = G_2 \times \{0,1\}^{2n}$ і головний ключ s. Загальнодоступні параметри завантажуються в

PPS і публікуються потім. Головний ключ $s \in Z_q^*$ тримається в секреті і відомий лише KGC.

- Partial-Private-Key-Extract: Алгоритм запускається KGC, коли хтось запитує його закритий ключ. Вхідними аргументами є загальнодоступні параметри P, головний секрет s та ідентифікаційний рядок$ID_A \in \{0,1\}^*$. Вихідним є частковий закритий ключ D_A, що відповідає заданій ідентичності.
- Set-Secret-Value: Запускається користувачем для створення секретного значення x_A. У загальному випадку загальнодоступні параметри P та відповідний ідентифікатор ID є входами алгоритму.
- Set-Private-Key: Алгоритм обчислює закритий ключ користувача $S_A \in G_2^*$ з відкритих параметрів P, часткового приватного ключа D_A і секретного значення $x_A \in Z_q^*$.
- Set-Public-Key: Алгоритм обчислює відкритий ключ P_A користувача з відкритих параметрів P і секретного значення x_A.
- Encrypt: Викликається відправником для шифрування повідомлення з використанням вказаної особи. Бере загальнодоступні параметри P, ідентифікатор ID_A, відкритий ключ $P_A = \langle X_A, Y_A \rangle$, повідомлення повертає зашифрований текст.
- Decrypt: Виконується одержувачем для розшифрування повідомлення за допомогою відповідного секретного ключа. В якості входу приймає закритий ключ S_A, загальнодоступні параметри P, ідентифікатор ID_A, зашифрований текст виводить повідомлення M.

1.2.1 Переваги

Криптографія без сертифікатів може забезпечити одну з найбільш гнучких інфраструктур для криптографії з відкритим ключем. Він поєднує в собі найкращі аспекти традиційної інфраструктури відкритих ключів і шифрування на основі аутентифікації, наприклад відсутність сертифікатів, відсутність власності на ключ, розумну довіру до надійної третьої сторони та легку

інфраструктуру. Застосування CL-PKE можуть бути такими ж, як і для PKI та IBE, тобто мереж компаній, Інтернету та побутової електроніки. Як і у випадку з IBE, несертифікована криптографія може використовуватися як основний механізм для прозорого шифрування електронної пошти / SMS.

1.2.2 Недоліки

Навіть якщо відкриті ключі не такі прості, як шифрування на основі облікових даних, ви все одно можете отримати числову частину ключа з заданого ідентифікатора. Для надання такого типу послуги CL-PKE повинен включити свого роду каталог відкритих ключів, присутній у довірчій мережі. Крім того, проведені розрахунки досить складні та дорогі, тому є бажання мати швидші алгоритми, перш ніж ви зможете реалізувати реальні системи. Нарешті, оригінальна версія CL-PKE зменшує сертифікати лише для користувачів, але зберігає їх на підключеннях до серверів PPS і KGC. Щоб повністю виключити сертифікати, сервери схеми повинні належати до ієрархічного CL-PKE. Загальнодоступні параметри та ключ кореневого сервера будуть розгорнуті разом із програмним забезпеченням (наприклад, сертифікати кореневого CA в PKI).

2 ЕЛІПТИЧНА КРИВА ТА РОЛЬ ЇЇ В КРИПТОГРАФІЇ

2.1Еліптична крива

Еліптична крива E [15] є алгебраїчною кривою, що задовольняє наступному рівнянню:

$$y^2 = x^3 + ax + b \tag{2.1}$$

Для криптографічних цілей використовуються лише неособливі еліптичні криві. Крива E є еліптичною кривою, якщо її дискримінант Δ не дорівнює нулю, тобто.

$$\Delta = 4a^3 + 27b^2 \neq 0 \tag{2.2}$$

На рисунку 2.1 показано два типи еліптичних кривих:

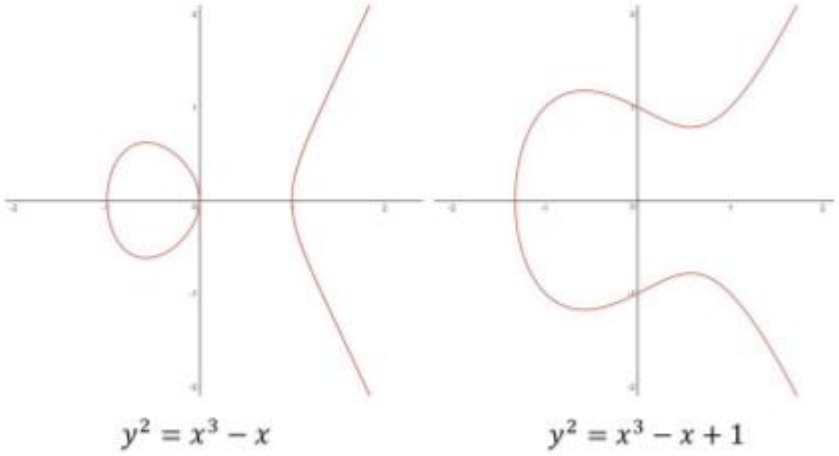

Рисунок 2.1 Еліптичні криві

Над еліптичними кривими можна виконати наступні операції:

- Додавання точок: $R = P + Q$
- Подвоєння точки: $R = P + P$
- Множення точки: $R = nP$

де P,Q, R — точки на еліптичній кривій.

2.1.1 Додавання точок

Операція додавання точок показана на рисунку 2. Вона складає дві точки P, Q на еліптичній кривій і дає третю точку R на тій самій еліптичній кривій. У цій операції спочатку проводиться лінія, що з'єднує дві задані точки. Ця лінія

перетинає еліптичну криву у третій точці -R(x, -y). Відображення цієї точки через вісь дає кінцеву точку R(x, y). Додавання точок позначається як:

$$R = P + Q \tag{2.3}$$

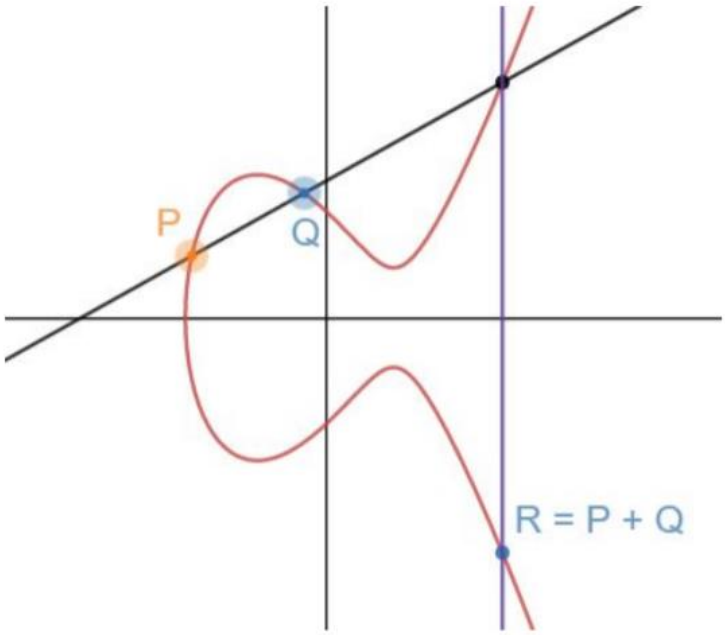

Рисунок 2.2 – Додавання точок

2.1.2 Подвоєння точок

Операція подвоєння точок показана рисунку 2.3. Вона включає у собі додавання точки P до себе на еліптичної кривої. Це майже аналогічно до складання точок, при якому отримуємо лінію, що перетинає еліптичну криву в кінцевій точці P. Так як не має двох точок для обчислення лінії, береться дотична еліптична крива в даній точці P, і ця дотична перетинає еліптичну криву в іншій точці *-R(x, -y)* на еліптичній кривій. Відображення цієї точки через вісь дає кінцеву точку *R(x, y).* Подвоєння точки позначається як:

$$R = P + P \tag{2.4}$$

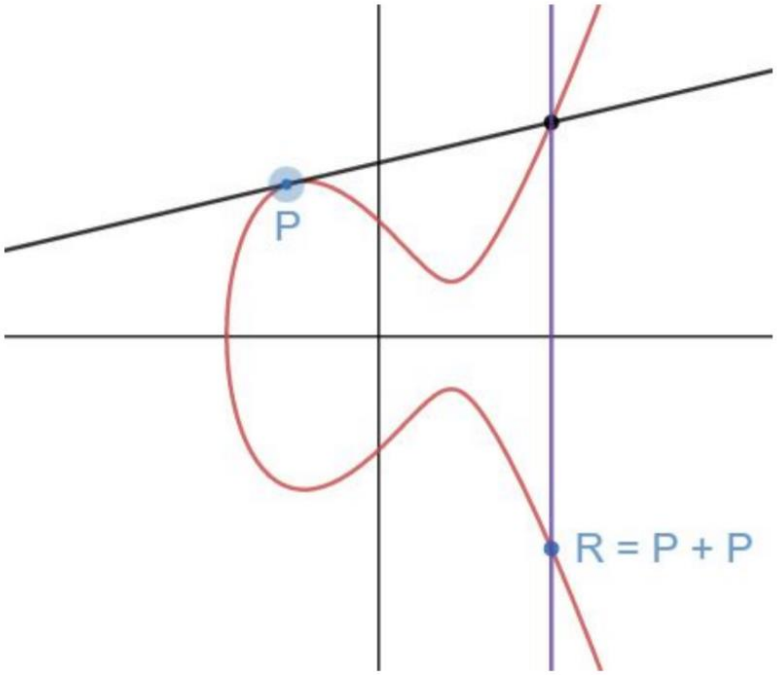

Рисунок 2.3 – Подвоєння точок

2.1.3 Множення точки

Множення точки- це множення скалярного значення на точку еліптичної кривої, у результаті виходить інша точка еліптичної кривої [25]. Воно виходить шляхом повторення операцій подвоєння та складання точок на еліптичній кривій. Наприклад, якщо P – точка, а n – скалярне значення, яке потрібно помножити, то nP виходить як nP = 2(2(2P) + P). . . + P. Кількість операцій подвоєння та складання варіюється при виборі різних підходів до поділу скаляра n. Основний підхід для множення точок - це додавання точки P до себе n раз, тобто. $nP = (\dots(((P + P) + P) + \dots P)$.

2.2 Білінійне створення пари

Нехай G_1, G_2 - дві циклічні групи, такі, що $|G_1| = |G_2| = p$. Нехай P - генератор групи G_1 таe: $G_1 \times G_1 \longrightarrow G_2$, де e називається допустимим білінійним відображенням, якщо називається допустимою білінійною картою, якщо вона відповідає наступним трьом умовам. умови:

- Білійний: $\forall P, Q \in G_1$ і $\forall a, b \in Z_p^*$

  $e(aP, bQ) = e(abP, Q) = e(P, abQ) = e(P, Q)^{ab}$.

- Невироджені: $e(P,Q)$ не дорівнює елементу ідентифікації в $G_2 \forall P,Q \in G_1$. Іншими словами, якщо P є твірною в G_1 , то $e(P,P) \in G_2$ є твірною в G_2.
- Обчислювальним : $\forall P,Q \in G_1, e(P,Q)$ обчислюється за поліноміальний час.

Оскільки вхідні дані, взяті за допомогою білінійної карти е у наведеному вище випадку, належать до однієї групи G1, цей тип парування відомий як симетричне спарювання. В асиметричному парі е отримує вхідні дані від двох різних груп G_1 і G_2 і відображає в третю групу G_T, тобто e: $G_1 \times G_2 \to G_T$.

2.3 Алгоритми криптографії без сертифікатів

Після базового введення в криптографію з еліптичною кривою та спарювання можна зрозуміти точні визначення алгоритмів CL-PKE:

- Налаштування. Алгоритм включає в себе наступні кроки:
  - Створити кортеж $\langle G_1, G_2, G_T, e \rangle$, де G_1 і G_T — групи деякого простого порядку q, порядок кожного елемента, що належить до групи G_2, ділиться q і e: $G_1 \times G_2 \to G_T$ є спарюванням. Переважно q є простим числом Солінаса, тобто має вигляд $q = 2^{e_2} \pm 2^{e_1} \pm 1$, де e_1 і e_2 є показниками.
  - Виберіть випадковий генератор P групи G_1.
  - Виберіть випадковий головний ключ s із Z_q^* і обчисліть відкритий ключ $P_{pub} = sP$
  - Виберіть криптографічні хеш-функції $H_1: \{0,1\}^* \to G_2^*, H_2 : G_T \to \{0,1\}^n, H_3: \{0,1\}^n \times \{0,1\}^n \to Z_q^*$ і $H_4 : \{0,1\}^n \to \{0,1\}^n$, де n – довжина відкритих текстів

- Частково-приватний ключ-витяг. Для обчислення часткового закритого ключа виконуються такі дії:
  - Зобразити тотожність точки на еліптичній кривій шляхом обчислення $Q_A = H_1(ID_A) \in G_2^*$.
  - Обчисліть частковий закритий ключ $D_A = sQ_A \in G_2^*$.

- Встановити-секрет-значення. Алгоритм вибирає випадкове $x_A \in Z_q^*$.
- Набір-Закритий-Ключ. Виводить закритий ключ користувача, обчислюючи $S_A = x_A D_A = x_A s Q_A$.
- Набір-Відкритий-Ключ. Алгоритм повертає $P_A = \langle X_A, Y_A \rangle = \langle x_A P, x_A P_{pub} \rangle = \langle x_A P, x_A s P \rangle$.
- Шифрувати. Шифрування повідомлень виконується наступним чином:
    - Якщо умови $X_A, Y_A \in G_1^*$ і $e(X_A, P_{pub}) = e(Y_A, P)$, якщо учова не виконується то потрібно зупинитися.
    - Обчислити $Q_A = H_1(ID_A) \in G_2^*$.) .
    - Виберіть випадковий $\sigma \in \{0,1\}^n$.
    - Обчисліть $r = H_3(\sigma, M)$.
    - Обчисліть зашифрований текст $C = \langle rP, \sigma \oplus H_2(e(Q_A, Y_A)^r), M \oplus H_4(\sigma) \rangle$. Зауважте, що найскладнішою операцією є сполучення $e(Q_A, Y_A)$, але її значення є постійним для заданої ідентичності та відкритого ключа, тому її не потрібно кожен раз перераховувати.
- Розшифрувати. Розшифровка зашифрованого тексту $C = \langle U, V, W \rangle \in C$ виконується наступним чином:
    - Обчисліть $\sigma = V \oplus H_2(e(S_A, U))$.
    - Обчисліть $M = W \oplus H_4(\sigma)$.
    - Обчисліть $r = H_3(\sigma, M)$, якщо $U \neq rP$ то потрібно зупинитися.
    - Повернення M.

2.4 Криптографія з еліптичною кривою

ECC (криптографія з еліптичною кривою) був введений Віктором Міллером і Нілом Кобліцем у 1985 році, безпека якого залежить від проблеми дискретного логарифма еліптичної кривої (ECDLP). Схема ECC може бути визначена набором параметрів (q, a, b, G, n, h) і застосована до цифрових підписів, шифрування та обміну ключами. ECC має дві функції, які роблять його дуже придатним для середовищ з обмеженими ресурсами.

- Для того ж рівня безпеки йому потрібен набагато менший розмір ключа, ніж інші криптографічні схеми з відкритим ключем (наприклад, RSA).
- Його скалярне множення набагато швидше, ніж модульна експоненційна операція, і його легко реалізувати апаратно.

У даній роботі використовується ECC для створення криптографії з відкритим ключем без сертифікатів, яку можна використовувати як для шифрування, так і для підпису. Алгоритм шифрування заснований на схемі шифрування з еліптичною кривою Діффі-Хеллмана (ECDH) та інтегрованою схемою шифрування з еліптичною кривою (ECIES). Підпис заснований на алгоритмі цифрового підпису еліптичної кривої (ECDSA). Пов'язані попередні етапи ECC розглядаються наступним чином.

2.5 Задача дискретного логарифма еліптичної кривої

Враховуючи еліптичну криву $E = (q, a, b, G, n, h)$ над скінченним полем F_q, вибираючи секретне число s з [1, n-1], можна легко обчислити $Q = s \times G$. Однак дуже важко обчислити s за допомогою Q та G, що називається ECDLP.

2.6 Еліптична крива Діффі-Хеллмана

Еліптична крива Діффі-Хеллмана — це схема обміну ключами Діффі-Хеллмана, заснована на еліптичних кривих, яка може допомогти двом сторонам, які спілкуються через незахищений канал, створити загальний секрет. Спільний секрет можна використовувати (як ключ) для забезпечення конфіденційності та цілісності даних. Крім того, ECDH може досягти такого ж рівня безпеки з набагато меншим розміром ключа, ніж оригінальна схема Діффі-Хеллмана.

Припустимо, що Аліса та Боб використовують одну й ту саму систему ECC (q, a, b, G, n, h) для створення пар ключів (S_A, P_A) та (S_B, P_B) відповідно. Відповідно до схеми ECDH, загальний секрет $K_{A,B}$ може бути згенерований за допомогою (2.5).

$$K_{A,B} = S_A \times P_B = S_B \times P_A = S_A \times S_B \times G \tag{2.5}$$

2.7 Інтегрована схема шифрування з еліптичною кривою

ECIES — це схема шифрування на основі ECC. Як видно з назви, ECIES — це інтегрована схема шифрування, яка може забезпечити як конфіденційність, так і цілісність даних. Він використовує ECDH для створення спільного секрету, з якого отримують ключ шифрування та ключ цілісності (або код аутентифікації повідомлення, MAC). Конфіденційність гарантується симетричним криптографічним алгоритмом з ключем шифрування, а цілісність гарантується функцією генерації MAC з ключем цілісності.

Щоб зашифрувати повідомлення m для Боба, Аліса повинна виконати наступні 7 кроків:

- Виберіть випадкове ціле число r із $[1, n-1]$.
- Обчислення $R = r \times G$.
- Обчислення $K = r \times P_B = (K_X, K_Y)$
- Перевірка, чи $K = \boldsymbol{O}$ чи ні, якщо так, потрібно повернутися до вибору числа r.
- Обчислення $K_{ENC}||K_{MAC} = KDF(K_X)$, де KDF є функцією виведення ключа.
- Обчислення $c = ENC(K_{ENC}|, m)$ і $e = HMAC(K_{MAC}, c)$.
- Надсилання «$R||c||e$» Бобу.

Щоб розшифрувати зашифрований текст «$R||c||e$», Боб повинен зробити 5 кроків:

- Потрібно перевірити, чи знаходиться R на еліптичній кривій, якщо так то продовжуємо
- Обчисліть $K = S_B \times R = (K_X, K_Y)$ і потрібно перевірити, чи $K = O$, якщо ні то продовжуємо
- Обчислити $K_{ENC}||K_{MAC} = KDF(K_X)$.
- Перевірка, чи $e = HMAC(K_{MAC}, c)$, якщо так то продовжуємо.
- Обчисліть $m = DEC(K_{ENC}|, c)$.

2.8 Алгоритм цифрового підпису еліптичної кривої

ECDSA — це варіант алгоритму цифрового підпису (DSA) на еліптичній кривій. Коли Аліса хоче надіслати повідомлення m і підпис Бобу, вона повинна виконати 5 кроків.

- Виберіть випадкове ціле число k з $[1, n-1]$.
- Обчислення $k \times G = (Kx, Ky)$.
- Обчислення $r = K_x \, mod \, n$. Якщо $r = 0$ то потрібно вибрати k.
- Обчислення $e = H(m)$.
- Обчисліть $s = k^{-1}\{e + S_A \times r\} \, mod \, n$. Якщо $s = 0$, то потрібно повернутися до вибору числа k.

  Підпис Аліси для повідомлення m це (r, s).

Щоб перевірити повідомлення m і підпис (r, s), Боб повинен виконати наступні 7 кроків:

- Перевірка, чи є r і s в $[1, n-1]$ чи ні, якщо ні то потрібно зупинитися.
- Обчисліть $e = H(m)$.
- Обчислення $w = s^{-1} \, mod \, n$
- Обчислення $(x_1, y_1) = u_1 \times G + u_2 \times P_A$.
- Обчислення $v = x_1 \, mod \, n$.
- Якщо $v = r$, потрібно прийняти підпис.

2.9 Криптографія відкритого ключа без сертифікатів (CL-PKE)

Криптографічну схему з відкритим ключем без сертифіката можна формально описати наступними 7 алгоритмами.

2.9.1 Підготовка

Підготовку здійснює Центр генерації ключів (КГК). Він використовується для налаштування системи відкритих ключів без сертифікатів, які можуть бути представлені системними відкритими параметрами. Усі параметри системи повинні бути відомі всім учасникам або зацікавленим сторонам. Головний закритий ключ mpk і головний відкритий ключ msk генеруються параметром безпеки l. Алгоритм конфігурації можна позначити як $(params, msk, mpk) = Setup(1^l)$.

2.9.2 Часткове вилучення ключа

Алгоритм часткового вилучення ключа також виконується KGC, який приймає $params$ системних параметрів, головний ключ та ідентифікатор користувача як вхідні дані та виводить закритий закритий ключd_{ID} і частковий відкритий ключ R_{ID}. Неповний ключ може бути представлений (d_{ID}, R_{ID}) і повинен надсилатися користувачеві через захищений канал. Алгоритм часткового вилучення ключа можна позначити.

$$(d_{ID}, R_{ID}) = PartialKeyExtract(params, msterkey, ID) \quad (2.6)$$

2.9.3 Генерація ключів

Алгоритм генерації ключів виконується користувачем, і є три завдання. По-перше, випадковим чином вибрати секретне значенняz_{ID} для ідентифікатора користувача відповідно до параметрів загальнодоступних параметрів системи. По-друге — створити приватний ключ S_{ID} для ідентифікатора користувача з params, d_{ID} та z_{ID} та ID. Третій — створити відкритий ключ P_{ID} відповідно до параметрів, R_{ID} і z_{ID}. Алгоритм генерації ключа можна позначити як $(S_{ID}, P_{ID}) = Generation\ Key\ (params, partialkey, z_{ID}, ID)$.

2.9.4 Шифрування

Алгоритм шифрування запускається відправником, який отримує параметри, ідентифікатор одержувача, відкритий ключ P_{ID} одержувача та повідомлення m, яке має бути зашифровано як вхід, і виводить зашифрований текст c. Тобто , $c = Encryption(params, P_{ID}, ID, m)$.

2.9.5 Розшифровка

Алгоритм дешифрування запускається одержувачем, який приймає параметри, ідентифікатор одержувача, приватний ключ SID одержувача та зашифрований текст c як вхідні дані і виводить відповідний відкритий текст m. Тобто $m = Decryption(params, S_{ID}, ID, c)$.

2.9.6 Підпис

Алгоритм підпису запускається відправником повідомлення, який приймає параметри, ідентифікатор підписувача, приватний ключ S_{ID} підписувача та

повідомлення m як вхідні дані, а також виводить свій підпис підпису в повідомленні m. Тобто $sig = Signature(params, ID, S_{ID}, m)$.

2.9.7 Верифікація

Алгоритм перевірки запускається приймачем повідомлень, який приймає параметри, головний відкритий ключ mpk, ідентифікатор підписувача, P_{ID} відкритого ключа підписувача, повідомлення m та його підпис підпису як вхідні дані, виводить результат перевірки дійсний або недійсний. Тобто $Verification(params, mpk, ID, P_{ID}, m, sig)$.

3 РОЗРОБКА ОПТИМІЗОВАНОГО АЛГОРИТМУ

Запропонована схема складається з 7 компонентів, які представлені таким чином:

3.1 Налаштування системи

На етапі налаштування, відповідно до параметра безпеки l, еліптична крива E над кінцевим полем F_q визначається набором параметрів (q, a, b, G, n, h). Головна пара відкритих і закритих ключів генерується KGC.

KGC випадково вибирає s з інтервалу $[1, n-1]$ як головний закритий ключ системи, який також називається головним ключем і повинен зберігатися в секреті KGC.

KGC обчислює $P_{pub} = s \times G$, який є головним відкритим ключем системи.

Загальнодоступними параметрами системи є $\{F\_q, E/F\_q, G,\ P_{pub}, H\}$.

3.2 Витяг часткового приватного ключа

Для користувача A з ідентифікатором ID_A KGC виконує наступні 4 кроки, щоб отримати часткові відкриті та закриті ключі для нього:

- Виберіть r_A випадковим чином з інтервалу $[1, n-1]$.
- Обчисліть d_A, використовуючи наступну формулу.

$$d_A = (s + r_A \times H(ID_A)) mod\ n \tag{3.1}$$

- Якщо $d_A = 0$, то потрібно знову вибрати r_A
- Обчисліть $R_A = r_A \times G$.

(d_A, R_A) — це частковий ключ, що відповідає ідентифікатору ID_A користувача A. KGC надсилає (d_A, R_A) користувачеві A через захищений канал.

3.3 Генерація ключів

Щоб створити пару відкритих і закритих ключів, користувач A повинен виконати наступні 7 кроків після отримання його часткового ключа.

- Виберіть випадковим чином ціле число z_A з інтервалу$[1, n-1]$.
- Обчисліть закритий ключ A, що відповідає ID_A.

$$S_A = \left(d_A + z_A \times H(ID_A)\right) mod\ n \tag{3.2}$$

- Якщо $S_A = 0$, то потрібно знову сформувати z_A, інакше зберігайте S_A таємно.
- Обчисліть Z_A за наступною формою

$$Z_A = z_A \times G \tag{3.3}$$

- Обчисліть $X_A = R_A + Z_A$
- Якщо $X_A = 0$, то потрібно знову сформувати z_A, щоб повторно вибрати новий z_A.
- X_A є виконавчим відкритим ключем A, що відповідає його ідентифікатору ID_A, і буде надано учасникам. $P_A = S_A \times G$ — це фактичний відкритий ключ A на основі ECC, який можна обчислити за допомогою (5).

$$\begin{aligned} P_A = S_A \times G &= \left(d_A + z_A * H(ID_A)\right) \times G = d_A \times G + z_A \times H(ID_A) \times G \\ &= \left(s + r_A \times H(ID_A)\right) \times G + H(ID_A) \times Z_A \\ &= s \times G + r_A \times H(ID_A) \times G + H(ID_A) + Z_A \\ &= s \times G + r_A \times H(ID_A) \times Z_A \\ &= P_{pub} + H(ID_A) \times (R_A + Z_A) \\ &= P_{pub} + H(ID_A) \times X_A \end{aligned} \tag{3.4}$$

Взаємозв’язок між приватним ключем користувача A та його виконавчим відкритим ключем також можна побачити в (3.4).

Крім того, (3.4) показує, що відкритий ключ P_A не тільки пов′язаний з його ідентичністю, але також побудований на головному відкритому ключі системи P_{pub}, це означає, що сертифікат з’єднання не потрібен для підтвердження з’єднання між відкритим ключем та ідентифікатором. Іншими словами, відкритий ключ може довести свою автентичність сам по собі.

3.4 Шифрування

Для шифрування та дешифрування даних можна використовувати пару відкритих і приватних ключів користувача. Враховуючи, що користувач A хоче надіслати повідомлення m, зашифроване відкритим ключем користувача B, він повинен виконати наступні 7 кроків:

- Довільно виберіть k з інтервалу $[1, n-1]$.

- Обчисліть $R = k \times G$.
- Обчисліть $K = k \times (P_{pub} + H(ID_B) \times X_B) = (K\_x, K\_y)$.
- Якщо $K = O$, то потрібно повернутися до пункту з вибором k
- Обчисліть $K_{ENC} = H(K\_x)$ і $K_{MAC} = H(K\_y)$.
  Тут ENC — це симетрична схема шифрування, така як RSA.
- Надсилання «$K||\, c1||\, c2$» користувачеві B.

3.5 Розшифровка

Після отримання «$K||c1||\, c2$», користувач B може розшифрувати c за допомогою свого приватного ключа S_B. Алгоритм дешифрування описується так:

- Обчисліть $K' = S_B \times K = S_B \times k \times G = (K'\_x, K'\_y)$.
- Перевірте, чи є $K' = O$ чи ні, якщо так, то зашифрований текст слід відхилити.
- Обчисліть $K'_{ENC} = H(K'\_x)$ і $K'_{MAC} = H(K'\_y)$.
- Обчисліть $m' = DEC(K'_{ENC}, c_1)$.
- Обчисліть $c_2' = HMAC(K'_{MAC}, m')$.
- Якщо $c_2 = c_2'$, виведіть m'.

Доказ розшифровки наведено нижче:

$$\begin{aligned} K = k \times \left(P_{pub} + H(ID_B) \times X_B\right) &= k \times \left(s \times G + H(ID_B) \times (R_B + Z_B)\right) \\ &= k \times \left(s \times G + H(ID_B) \times (R_B + Z_B)\right) \\ &= k \times (s \times G + H(ID_B) \times (r_B + z_B)) \times G) \\ &= k \times (s \times G + (r_B + H(ID_B) \times (r_B + z_B)) \times G) \end{aligned} \tag{3.5}$$

$$\begin{aligned} K' = sB \times K = \; sB \times k \times G \; &= \left(d_B + z_B \times H(ID_B)\right) \times K \times G \\ &= s + r_B \times H(ID_B)) \times K \times G \\ &= \left(s + r_B \times H(ID_A) + z_B \times H(ID_A)\right) \times k \times G \\ &= k \times \left(s \times G + \left(r_B \times H(ID_B) + z_B \times H(ID_B)\right) \times G\right) \; = K \end{aligned} \tag{3.6}$$

Як показано вище, одержувач може відновити як ключ шифрування, так і ключ цілісності. Після цього можна перевірити цілісність повідомлення m.

3.6 Створення підпису

Процес створення підпису та перевірки будується на основі базової ідеї алгоритму підпису ECDSA.

Процес створення підпису користувача A для повідомлення m ілюструється наступними 7 кроками:

- Виберіть k випадковим чином з інтервалу $[1, n-1]$.
- Обчисліть $R = k \times G = (r\_x, r\_y)$. R — точка в підгрупі еліптичної кривої E, а r_x — значення осі X точки R.
- Обчисліть s_1 за (6), що є першою частиною підпису.

$$s_1 = r\_x \bmod n \tag{3.7}$$

- Перевірте, чи вірно (7), якщо так, то потрібно повернутися до кроку з вибором k.

$$H(m||ID_A) + S_A \times s_1 = 0 \bmod n \tag{3.8}$$

- Обчисліть s_2 за (8), що є 2-ю частиною підпису.

$$s_2 = k \times (H(m||ID_A) - 1 + S_A \times s_1) \bmod n \tag{3.9}$$

- Сигнатура s складається з s_1 і s_2, тобто $s = (s_1, s_2)$.
- Користувач A надсилає повідомлення «$ID_A||X_A||m||s_1||s_2$» користувачеві B

3.7 Верифікація

Після отримання вищевказаного повідомлення перевіряючий B виконує наступні 8 кроків для перевірки підпису.

- Перевірте, чи знаходяться обидва s_1 і s_2 в інтервалі $[1, n-1]$, якщо ні, підпис слід відхилити.
- Обчисліть хеш-значення HM.

$$HM = H\,(m||ID_A) \tag{3.10}$$

- Розрахувати $v1$

$$v1 = (HM \times s_2) \bmod n \tag{3.11}$$

- Розрахувати $v2$

$$v2 = (s_1 \times s_2) \bmod n \tag{3.12}$$

- Обчислює P_A

$$P_A = P_{pub} + H(ID_A) \times X_A \tag{3.13}$$

- Обчислює R'

$$R' = v1 \times G + v2 \times P_A = (r'\_x, r'\_y) \tag{3.14}$$

r'_x - значення осі X для R'.

- Перевірте, чи r'_x вірно, якщо так, то підпис проходить перевірку; в іншому випадку підпис недійсний.

$$r'\_x \bmod q = s_1 \tag{3.15}$$

Процес верифікації залежить від

$$\begin{aligned}
R' &= v_1 \times G + v_2 \times (P_{pub} + H(ID_A) \times X_A)) \\
&= v_1 \times G + v_2 \times (P_{pub} + H(ID_A) \times X_A)) \\
&= v_1 \times G + v_2 \times (s \times G + H(ID_A) \times (R_A + Z_A)) \\
&= v_1 \times G + v_2 \times (s \times G + H(ID_A) \times (r_A + z_A) \times G) \\
&= v_1 \times G + v_2 \times (s + r_A \times H(ID_A) + z_A \times H(ID_A)) \times G \\
&= v_1 \times G + v_2 \times (d_A + z_A \times H(ID_A)) \times G \\
&= v_1 \times G + v_2 \times s_x \times G \\
&= (H(m||ID_A) \times s_2 + s_1 \times s2 \times s_A) \times G \\
&= (H(m||ID_A) + s_1 \times s_A) \times s_2 \times G \\
&= (H(m||ID_A) + s_1 \times s_A) \times k \times (H(m||ID_A) - 1 \\
&\quad + s_A \times s_1) \times G \\
&= k \times G = (r_x, r_y)
\end{aligned} \tag{3.16}$$

Щоб об’єктивно оцінити запропоновану схему криптографії з відкритим ключем без сертифікатів, аналізується її ефективність як із безпеки, так і з накладних витрат.

3.8 Аналіз безпеки

Безпека має два значення; це безпека ключа і безпека алгоритмів. Безпека ключа відноситься до безпеки відкритого ключа, оскільки закритий ключ генерується та зберігається таємно самим користувачем.

3.8.1 Безпека відкритого ключа

3.8.1.1 Термін дії відкритого ключа

Дійсність відкритого ключа є необхідною умовою для забезпечення безпеки схеми. Запропонована схема побудована на ECC. Дійсність відкритого ключа P_A можна перевірити за допомогою наступних трьох умов:

- X_A і P_A — усі точки на еліптичній кривій E.
- $X_A \neq \boldsymbol{O}$ і $P_A \neq \boldsymbol{O}$.
- $n \times X_A = \boldsymbol{O}$ і $n \times P_A = \boldsymbol{O}$.

Причина описана в явному алгоритмі перевірки відкритого ключа в ECDSA. Виходячи з трьох умов, можна довести дійсність відкритих ключів X_A і P_A наступними кроками:

- Оскільки G є базовою точкою на E, порядок n якого є великим простим числом, точка, встановлена на еліптичній кривій E, породжена G, точка на нескінченності O, і операція додавання точок можуть утворювати циклічну групу з порядком n.
- Відповідно до характеру замикання циклічної групи, для цілого числа i в інтервалі $[1, n-1]$ $i \times G$ все ще має бути в наборі групових точок, що означає, що $i \times G$ є точкою на еліптичній кривій E.
- У запропонованій схемі і r_A, і z_A знаходяться в інтервалі $[1, n-1]$. Отже, R_A і Z_A — точки на еліптичній кривій E.
- $X_A = R_A + Z_A = ((r_A + z_A)\ mod\ n) \times G$.Відповідно до циклічності групи еліптичних кривих, прийнятої в запропонованій схемі (насправді, усі групи еліптичних кривих, прийняті в криптографі, є циклічними групами), X_A також має бути точкою на еліптичній кривій E та в груповій множині точок.
- $P_A = S_A \times G, S_A = (d_A + z_A \times H(ID_A))\ mod\ n$, PA також має бути точкою на еліптичній кривій E та в груповому наборі точок.
- Доведіть, що $X_A \neq \boldsymbol{O}$ і $P_A \neq \boldsymbol{O}$.
  Якщо $X_A = \boldsymbol{O}$, оскільки $X_A = R_A + Z_A = (r_A + z_A) \times G$, то $x_A = (r_A + z_A)\ mod\ n = 0$, що можна виразити.

$$x_A = j \times n \tag{3.17}$$

Оскільки x_A знаходиться в інтервалі $[1, n-1]$, формула вище означає, що x_A має мати два множники x_1 і x_2, які задовольняють $x_1 \times x_2 = n$, що суперечить тому факту, що n є простим числом. Отже, існує x_A таке, що $x_A \; mod \; n \neq 0$.

Відповідно до визначення циклічної еліптичної групи від генератора G з порядком n, для будь-якого $i \in [1, n-1]$ має бути $i \times G \neq \boldsymbol{O}$ і $n \times G = \boldsymbol{O}$. Оскільки $(r_A + z_A) \; mod \; n \neq 0$, маємо $X_A = (r_A + z_A) \times G \neq \boldsymbol{O}$.

- Доведення, що $P_A \neq O$.
- Доведення, що $n \times X_A = \boldsymbol{O}$ і $n \times P_A = \boldsymbol{O}$

Подібно для доведення, що $X_A \neq \boldsymbol{O}$ і $P_A \neq \boldsymbol{O}$,

$$n \times X_A = n \times (r_A + z_A) \times G = (r_A + z_A) \times (n \times G) = (r_A + z_A) \times \boldsymbol{O} = \boldsymbol{O} \tag{3.18}$$

$$n \times P_A = n \times s_A \times G = s_A \times (n \times G) = s_A \times \boldsymbol{O} = \boldsymbol{O} \tag{3.19}$$

Таким чином, ХА є дійсним відкритим ключем виконавця, що відповідає ID_A, а P_A є дійсним відкритим ключем, що відповідає ID_A. Закритим ключем ID_A є S_A.

3.8.1.2 Справжність відкритого ключа

Автентичність відкритого ключа означає, що відкритий ключ дійсно належить заявленому власнику. Як і інша криптографія з відкритим ключем без сертифікатів, автентичність відкритого ключа запропонованої схеми гарантується наступними двома фактами:

- Аутентифікація користувача використовується разом з його відкритим ключем, який обговорювався як в алгоритмі шифрування, так і в алгоритмі автентифікації..
- Секретний ключ KGC використовується для створення приватного ключа користувача, який обговорювався в алгоритмі генерації ключів.

Крім того, алгоритм генерації ключа показує, що і ідентифікатор користувача, і відкритий ключ системи інтегровані у відносини між закритим

ключем і відкритим ключем. Це посилання пов’язує відкритий ключ з ідентифікатором користувача. Навіть якщо зловмисник може успішно замінити відкритий ключ жертви своїм власним відкритим ключем, частковий ключ жертви від авторитету не буде відомий зловмиснику, і зловмисник все одно не зможе створити дійсний підпис або розшифрувати шифрований текст за допомогою підробленого загальнодоступного ключа. ключ та ідентифікатор жертви.

3.8.2 Аналіз ефективності

Оскільки запропонована криптографічна схема відкритого ключа без сертифікатів побудована шляхом інтеграції ідентифікатора користувача в ECC замість шифрування на основі аутентифікації, вона має функції ID-PKC, але усуває дворядкові пари. Операції в ньому включають скалярне множення, хеш, HMAC, симетричне криптографічне шифрування та інші арифметичні операції. Оскільки накладні витрати на хешування, HMAC, симетричну криптографію та інші арифметичні операції набагато нижчі, ніж для скалярного множення, кількість скалярних множень зазвичай включається в обчислювальні накладні витрати.

Відповідно до розділу 3 видно, що алгоритм шифрування має 2 скалярні множення, 1 скалярне множення в алгоритмі дешифрування, 1 скалярне множення в алгоритмі підпису і 3 скалярні множення в алгоритмі перевірки. Порівняння обчислювальних витрат між нашою схемою та існуючими схемами наведено в таблиці 3.1, яка показує, що наша схема має набагато нижчі обчислювальні витрати.

3.8.3 Порівняльний аналіз ефективності

Для об’єктивної оцінки ефективності запропонованої схеми, накладні витрати на зв’язок і обчислення нашої схеми, а також деякі популярні чи ефективні схеми криптографії з відкритим ключем без сертифікатів наведені в таблиці 3.1. Для справедливого порівняння припустимо, що всі схеми мають однакову міцність безпеки (тут ECC з довжиною ключа 160 біт використовується як еталонний рівень безпеки, тобто l = 160). Крім того, накладні витрати на

обчислення вимірюються кількістю скалярних множень. Обчислювальні накладні витрати розраховуються на основі підходів у [10], де одне білінійне парування становить приблизно 20 скалярних множень, а одна модульна експоненціальна операція становить приблизно 2 скалярних множення. А витрати на зв’язок вимірюються в двійкових бітах.

Таблиця 3.1 показує, що запропонована схема забезпечує як алгоритми шифрування, так і алгоритми підпису і має набагато нижчі витрати на зв'язок і обчислення, ніж інші. Однак надійність безпеки може бути нижчою, ніж у схемах, заснованих на BDHP, GBDHP або інших складних припущеннях.

Таблиця 3.1 Порівняння різних алгоритмів CL-PKE

	Обчислювальні накладні витрати				Накладні витрати на зв'язок			Припущення
	Шифрування	Розшифрування	Підпис	Верифікація	Довжина публічного ключа	Довжина шифротексту	Довжина підпису	
CL-PKE1	22	22			$2l$	$3l + \|m\|^a$		$GBDHP^b$
CL-PKE2	7	44			$2l$	$5l + \|m\|$		$GBDHP$
Basic CL-PKE	61	20			$4l$	$2l$+|m|		$GBDHP$
Full CL-PKE	61	21			$4l$	$3l$+|m|		$GBDHP$
CL-PKS			23	80	$4l$		$3l$	$GBDHP$
Схема	2	1	1	3	$2l$	$3l$+|m|	$2l$	$ECDHg^g$ і $ECDLP$

a. |м| довжина повідомлення m

b. GBDHP — це абревіатура загальної білінійної задачі Діффі-Хеллмана

c. Inv-CDHP — це абревіатура зворотної обчислювальної задачі Діффі-Хеллмана

d. CDHP — це абревіатура обчислювальної задачі Діффі-Хеллмана

e. DLP — це абревіатура проблеми дискретного логарифма

f. ECDLP — це абревіатура проблеми дискретного логарифма з рішенням еліптичної кривої

g. ECDH - це абревіатура від еліптичної кривої Діффі-Хеллмана

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

У своїй діяльності розробник використовує комп’ютер, пристрої збереження інформації, а тому є необхідність забезпечення зручного доступу до всіх технічних засобів. Тому в даному розділі докладніше розглянемо відомості про систему ергономічних норм і принципів організації робочого місця відповідно до ДСТУ 8604:2015 та ДСТУ 3943-2000.

Під робочим місцем розуміється зона, оснащена необхідними технічними засобами, у якій відбувається трудова діяльність виконавця або групи виконавців, які спільно виконують одну роботу або операцію.

Організація робочого місця полягає у виконанні заходів, які забезпечують безпечний і раціональний трудовий процес і ефективне використання знарядь та предметів праці, що підвищує продуктивність праці і знижує стомлюваність працівника.

Організація робочого місця залежить від характеру розв'язуваних задач і особливостей предметно-просторового оточення, що визначають робоче положення тіла і можливість пауз для відпочинку, типи і способи засобів відображення і керування, необхідність у засобах захисту, спецодягу, простору для налагодження і ремонту устаткування.

Одним з компонентів діяльності на робочому місці є робочі рухи. Їхня раціональна організація створює умови для зниження стомлення, резерви для підвищеної працездатності. Просторові характеристики руху оператора визначаються траєкторіями руху і розмірами моторного поля (зони досяжності).

При організації робочого місця необхідно забезпечити нормальні умови огляду. Зону огляду описує кут, вершина якого знаходиться в центрі ока, а сторони складають границі, в яких людина при фіксованому положенні голови й ока добре розрізняє їхнє місцезнаходження.

Щоб зберегти нормальну гостроту зору, робочу поверхню розташовують від очей на відстані від 0,3 м до 0,75 м. Робочі меблі повинні бути зручними для виконання робочих операцій. В даному випадку робочий стіл є основним

устаткуванням. Особливо важливе значення має висота столу, його конструкція, яка повинна передбачати шухляди для розміщення інструментів, документації.

Важливе значення має конструкція робочих крісел. Погано підібрані крісла можуть бути причиною надмірної стомлюваності.

Нахил і висота крісла повинні регулюватися відповідно до висоти робочої поверхні і росту працюючого. Рекомендована ширина крісла 370 – 400 мм, глибина 370 – 420 мм, висота спинки 370 – 1000 мм від рівня крісла. Для розміщення ніг необхідно передбачити вільний простір під робочою площиною.

Праця людини, що протікає в умовах надмірного нервово-емоційного напруження, довготривалих статичних навантажень, обмеженої рухової активності призводить до неврозів, відхилень у психіці, захворювань опорно-рухового апарату, серцево-судинної системи тощо. Комп'ютери, телебачення, системи зв'язку та інші засоби, що використовують досягнення радіоелектроніки, є генераторами цілої низки електромагнітних випромінювань, вплив яких на організм людини ще не зовсім вивчено.

Сучасний розвиток науки та техніки приносить принципові нововведення у всі сфери матеріального виробництва, докорінно змінюючи знаряддя та предмети праці, технологію, методи обробки інформації. Разом з тим, захопившись вдосконаленням засобів праці залишено поза увагою проблеми людини в рамках своєрідної технічної та комп'ютерної революції. З широким впровадженням автоматизації та комп'ютеризації виникла потреба врахування психологічних можливостей людини, таких як швидкість реакції, особливості пам'яті та уваги, емоційний стан та ін. Поява операторської діяльності призвела до суттєвих змін у фаховій структурі праці. Зменшились фізична важкість праці, ризик виробничого травматизму, однак разом з тим, на працюючу людину посилюється вплив нових, раніше невідомих чи мало вивчених несприятливих виробничих факторів фізичного, хімічного і особливо психофізіологічного характеру.

Проте, розвиток сучасної обчислювальної техніки відбувається не лише у бік покращення її технічних параметрів, але також звертається увага безпеку

використання цієї техніки людиною шляхом зменшення потужності випромінювачів, зменшенням рівня випромінювання з моніторів, зменшення напруги живлення, покращення ергономічних характеристик.

Таким чином, в розділі з охорони праці виконано огляд питань безпечної роботи при створенні модуля інформаційної системи збору статистики та встановлено, що умови такої роботи відповідають вимогам з охорони праці, які застосовуються в галузі інформаційних технологій.

4.2 Безпека в надзвичайних ситуаціях

4.2.1 Фактори, які забезпечують стійкість функціонування підприємства.

Підвищення стійкості об'єкта досягається посиленням найбільш слабких (вражаючих) елементів і ділянок об'єкта. Для цього на кожному ОГД завчасно на основі досліджень планують і проводять відповідні організаційні й інженерно-технічні заходи. Досягнення науки і техніки дозволяють реалізувати такі рішення, при яких підприємство буде стійке до впливу дуже значних надлишкових тисків, однак це пов'язано з великими витратами засобів і матеріалів і може бути виправдано лише при захисті унікальних, особливо важливих елементів об'єкта. Заходи будуть економічно обґрунтовані, якщо вони максимально узгоджені із завданнями, які розв'язуються в мирний час для забезпечення безаварійної роботи, поліпшення умов праці, удосконалювання виробничого процесу. Тому підвищення характеристик міцності проводять, якщо:

- окремі особливо важливі будинки і спорудження значно слабші за інші і їхню міцність доцільно довести до прийнятої для даного підприємства межі стійкості;
- необхідно зберегти деякі важливі ділянки, які можуть самостійно функціонувати при виході з ладу інших і забезпечать випуск особливо цінної продукції.

Особливо велике значення має розробка інженерно-технічних заходів при новому будівництві, бо у процесі проектування у багатьох випадках можна домогтися логічного поєднання загальних інженерних рішень із захисними заходами ЦЗ, що знизить витрати на їх реалізацію. На існуючих об'єктах заходи

щодо підвищення стійкості доцільно проводити в процесі реконструкції чи виконання інших ремонтно-будівельних робіт.

Підвищення стійкості роботи промислових об'єктів передбачає:

- захист робітників та службовців у надзвичайних ситуаціях мирного і воєнного часу;
- підвищення міцності і стійкості найважливіших елементів і удосконалювання технологічного процесу;
- підвищення стійкості матеріально-технічного постачання;
- підвищення стійкості управління об'єктом;
- розробку заходів щодо зменшення імовірності виникнення вторинних факторів ураження і збитків від них;
- підготовку до відновлення виробництва після ураження об'єкта.

Особлива увага повинна бути приділена забезпеченню укриттям всіх працюючих у захисних спорудженнях. З цією метою розробляється план нагромадження і будівництва необхідної кількості захисних споруджень; у випадку недостачі сховищ, які відповідають сучасним вимогам, у ньому передбачається укриття робітників та службовців у швидкостворюваних сховищах.

4.2.2 Способи підвищення стійкості об’єктів господарювання.

При проектуванні і будівництві нових цехів підвищення стійкості може бути досягнуто застосуванням для несучих конструкцій високоміцних і легких матеріалів (легованих сталей, алюмінієвих сплавів).

При будівництві і реконструкції промислових споруд необхідно застосовувати легкі, вогнестійкі покрівельні матеріали, полегшені міжповерхові перекриття і сходові марші, підсилюючи їх кріплення до балок. Обвалення цих матеріалів і конструкцій принесе меншу шкоду устаткуванню, ніж важких залізобетонних.

Підвищення стійкості технологічного процесу досягається розробкою способів продовження виробництва при виході з ладу окремих верстатів, ліній і навіть окремих цехів за рахунок переведення виробництва в інші цехи;

розміщенням виробництва окремих видів продукції у філіях; шляхом заміни зразків, устаткування, що вийшли з ладу, іншими; а також скороченням числа використовуваних типів верстатів і приладів.

Підвищення стійкості системи енергопостачання досягається проведенням як загальноміських, так і об'єктових інженерно-технічних заходів. Створюються дублюючі джерела електроенергії, газу, води і пари шляхом прокладання декількох електро-, газо-, водо- і паропостачальних комунікацій та подальшого їх закільцювання. Інженерні й енергетичні комунікації переносяться в підземні колектори, найбільш відповідальні пристрої (центральні диспетчерські розподільні пункти) розміщуються в підвальних приміщеннях будинків чи у спеціально побудованих міцних спорудах. Там, де прокладання комунікацій у траншеях чи тунелях неможливе, здійснюється закріплення трубопроводів до естакад, щоб уникнути їх зрушення чи скидання; самі естакади зміцнюються установкою розтяжок у місцях поворотів і розгалужень.

Стійкість систем електропостачання об'єкта підвищують, підключаючи його до декількох джерел живлення, віддалених одне від одного на відстань, що виключає можливість їх одночасного ураження одним ядерним вибухом.
Водопостачання об'єкта більш стійке і надійне, якщо він живиться від декількох систем чи від двох-трьох незалежних джерел, віддалених одне від одного на безпечну відстань. Гарантоване постачання водою забезпечується тільки від захищених джерел з автономними і також захищеними іншими джерелами енергії (наприклад, артезіанські і безнапірні свердловини, приєднані до загальної системи водопостачання об'єкта).

Для стійкого і надійного постачання підприємств газом необхідно передбачити його подачу в газові мережі об'єктів від газорегуляторних пунктів (газороздавальних станцій), а на випадок виходу з ладу останніх влаштовувати обвідні лінії - байпаси. При будівництві нових чи реконструкції старих газових мереж по можливості повинні створюватися закільцьовані системи. Усі вузли і лінії газопостачання бажано розміщувати під землею (заглиблення комунікацій значно зменшує імовірність їх ураження ударною хвилею ядерного вибуху й

інших засобів нападу, а крім того, значно знижує можливість виникнення вторинних факторів ураження).

З метою зменшення пожежної небезпеки (зниження можливості витікання газу) на газопроводах встановлюються автоматичні запірні і перемикаючі пристрої дистанційного керування, що дозволяють при розриві труб безпосередньо з диспетчерського пункту відключати мережі чи переключати потік газу.

Підвищення стійкості систем теплопостачання досягається захистом джерел тепла і заглибленням комунікацій у ґрунт. Якщо на об'єкті передбачається будівництво котельні, її доцільно розміщувати в спеціальній будівлі, яка стоїть окремо. Будинок котельні повинен мати полегшене перекриття і легке стінове заповнення.

Заходи по підвищенню стійкості системи каналізації розробляють окремо для зливових, промислових і господарських (фекальних) зливів. На об'єкті обладнують не менше двох виводів з підключенням до міських каналізаційних колекторів і додатково обладнують виводи для аварійних скидань неочищених вод у прилеглі до об'єкта яри та інші природні заглиблення.

Одним із найважливіших заходів по забезпеченню сталого, безперервного на всіх етапах управління у надзвичайних ситуаціях є розподіл всього персоналу об'єкта на дві групи: працююча зміна (перебуває на об'єкті) і відпочиваюча (перебуває у заміській зоні або по дорозі між заміською зоною та об'єктом). До того ж створюються дві-три групи управління (за кількістю змін), які, крім керівництва виробництвом, повинні бути готові будь-якої миті взяти на себе організацію і керівництво проведенням рятувальних та ремонтних робіт.

Для забезпечення надійного управління діяльністю об'єкта у надзвичайних ситуаціях воєнного часу в одному із сховищ обладнується пункт управління. Диспетчерські пункти і радіовузли розміщують по можливості у найміцніших спорудах і підвальних приміщеннях. Повітряні лінії зв'язку до найважливіших виробничих ділянок переводять на підземно-кабельні. Стійкість засобів зв'язку можна підвищити прокладанням підземно-кабельних ліній на автоматичну

телефонну станцію (АТС) та радіовузол об'єкта, підготовкою пересувних електростанцій для заряджання акумуляторів і для живлення радіовузла при відключенні основних джерел електропостачання. При розширенні мережі підземних кабельних ліній необхідно прокладати дводротові, захищені екранами від впливу ЕМІ (електромагнітних імпульсів). Для більшої надійності повинні бути передбачені дублюючі засоби зв'язку.

У районі розосередження робітників і службовців також обладнують пункт управління. Між міським і заміським пунктами управління проводять зв'язок, як правило, телефонний, передбачаючи його дублювання за допомогою радіо- та пересувних засобів, також вживають заходів по забезпеченню зв'язку із змінними підприємствами по кооперації.

Особливе значення має сталість виробничих та господарських зв'язків з постачання об'єкта всіма видами енергії, водою, парою, газом; з транспортних послуг; з поставок сировини, напівфабрикатів, комплектуючих виробів та ін. Підвищення сталості матеріально-технічного постачання забезпечується створенням запасів сировини, матеріалів, комплектуючих виробів, обладнання, палива. Розміри незменшуваних запасів визначають для кожного об'єкта залежно від можливості їх накопичення, важливості продукції, яка випускається, визначених термінів переходу на виробництво продукції в умовах надзвичайних ситуацій.

Стабільно працююче підприємство повинно бути здатним безперебійно випускати продукцію за рахунок наявних запасів до відновлення зв'язків з поставок або до одержання необхідного від нових постачальників.

ВИСНОВКИ

У даній кваліфікаційній роботі магістра було були розглянуті алгоритми асиметричної криптографії та можливості їх застосування у пристроях з обмеженими ресурсами та був розроблений оптимізований криптографічна алгоритм без сертифікатів, який використовує метод керування ключами в схемах шифрування та підпису без сертифікатів і дозволяє уникнути проблема депонування ключів. Крім того, запропонований алгоритм є дуже ефективним завдяки використанню ECC та використанню простих хеш-операцій замість білінійного сполучення на еліптичній кривій. Детальний аналіз безпеки та накладних витрат показує, що дана схема є безпечною та легкою, що робить її придатною для обмежених ресурсів мобільних пристроїв із високими вимогами до безпеки.

На основі поставлених завдань можна прийти до наступних висновків:

- проаналізувано існуючі алгоритми CL-PKE
- Розроблено оптимізований алгоритм асиметричної криптографії для пристроїв з обмеженими ресурсами.

Запропонований алгоритм використовує ідею інтегрованих схем шифрування з еліптичною кривою для побудови алгоритму шифрування з відкритим ключем без сертифіката, а алгоритм підпису відкритого ключа без сертифіката заснований на ECDSA і ECIES. Алгоритму шифрування потрібно 2 скалярних множення, а алгоритму дешифрування потрібно лише 1 скалярне множення. Кількість скалярних множень для підпису та перевірки дорівнює 1 і 3 відповідно, що є досить небагато. Схема представлена в даній заснована на ECC, але вона має дві особливості CL-PKC. Шифрування, і підпис можуть бути реалізовані за допомогою скалярного множення. Крім того, йому потрібна лише одна проста хеш-функція, тоді як подібні схеми потребують більше. Ці властивості дають даній схемі явні переваги перед існуючими алгоритмами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Z. Cheng, L. Chen, L. Ling, and R. Comley, “General and efficient certificate-less public key encryption constructions”, in Pairing'07 Proceedings of the First international conference on Pairing-Based Cryptography, Lecture Notes in Computer Science, vol. 4575, 2007, pp. 83-107.
2. НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 р., № 22.
3. Elliptic curve-based certificate-less signatures for identity-based Encryption(ECCSI). RFC 6507. http://www.rfc-editor.org/info/rfc6507
4. ISO/IEC27035. Information technology. Security techniques. Information security incedent management.–2011.–78p.
5. A. W. Dent, “A brief Introduction to certificate-less encryption scheme and their infrastructures”, 6th European Workshop, EuroPKI 2009, Pisa, Italy, September 10-11, 2009, Revised Selected Papers. Public Key Infrastructures, Services and Applications, Lecture Notes in Computer Science, vol. 6391, 2010, pp. 1-16.
6. OHSAS 18001:2007 - Occupational Health and Safety Management System http://www.producao.ufrgs.br/arquivos/disciplinas/103_ohsas_18001_2007_ing.pdf
7. H. Du, Q. Wen, “Efficient and provably-secure certificate-less short signature scheme from bilinear pairings”. Computer Standards and Interfaces, 2009, vol.31, no.2, pp. 390-394
8. ДСТУ 2293-93. Система стандартів безпеки праці. Терміни та визначення / уклад. М. В. Панфонюк. – Київ: Вікторія, 2008. – ISBN 448 с. – 966-598-148-X.
9. K. Y. Choi, J. H. Park, J. Y. Hwang, “Efficient certificate-less signature schemes”, in Proceedings of 5th International Conference Applied Cryptography and Network Security (ACNS 2007), Zhuhai, China, June 5-8, 2007, pp. 443-458.

10. X. Cao, W. Kou, X. Du, “A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges”. Information Sciences, 2010, vol. 180, no. 15, pp.2895-2903.
11. J. Baek, R. Safavi-Naini, and W. Susilo, “Certificate-less public key encryption without pairing”, in Proceedings of 8th International Conference on Information Security(ISC 2005), Singapore, September 20-23, 2005, Lecture Notes in Computer Science, vol. 3650, 2005, pp. 134-148.
12. Serge Vaudenay. 2007. On privacy models for RFID. In International Conference on the Theory and Application of Cryptology and Information Security. Springer, 68–87.
13. Kerry A McKay, Kerry A McKay, Larry Bassham, Meltem Sonmez Turan, and Nicky Mouha. 2017. Report on lightweight cryptography. US Department of Commerce, National Institute of Standards and Technology.
14. Craig Gentry. 2006. Practical identity-based encryption without random oracles. In Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 445–464.
15. Ian Blake, Gadiel Seroussi, and Nigel Smart. 1999. Elliptic curves in cryptography. Vol. 265. Cambridge University Press.
16. J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow,”Elliptic curve cryptography in practice”. http://eprint.iacr.org/2013/734.pdf.
17. D. McGrew, K. Igoe, M. Salter, “Fundamental elliptic curve cryptography algorithms”, February 2011. Internet Engineering Task Force (IETF), Request for Comments: 6090.http://tools.ietf.org/html/draft-mcgrew-fundamental-ecc-04.
18. H. Dong, B. Sheng, Q. Li, “Elliptic curve cryptography-based access control in sensor networks”, Int. Journal of Security and Networks, vol.1, no. 3/4, 2006, pp.127-137.

19. C. P. Schnorr, “Efficient identification and signatures for smart cards”, Advances in cryptology — CRYPTO’ 89 Proceedings. Lecture Notes in Computer Science. Vol.435, 1990, pp. 239- 252.
20. D. McGrew, K. Igoe, M. Salter, “Fundamental elliptic curve cryptography algorithms”, February 2011. Internet Engineering Task Force (IETF), Request for Comments: 6090.http://tools.ietf.org/html/draft-mcgrew-fundamental-ecc-04.
21. Sattam S. Al-riyami, Kenneth G. Paterson, and Royal Holloway. Certificateless public key cryptography. pages 452–473. Springer-Verlag, 2003.
22. Ben Lynn. On the Implementation of Pairing-Based Cryptography. PhD thesis, Stanford University, 2007.
23. Dan Boneh and Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. In CRYPTO ’01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, pages 213–229, London, UK, 2001. SpringerVerlag.
24. Craig Gentry. Certificate-based encryption and the certificate revocation problem. In EUROCRYPT, pages 272–293, 2003.
25. Alka Sawlikar. 2012. Point Multiplication Methods for Elliptic curve Cryptography. International Journal of Engineering and Innovative Technology (IJEIT) 1, 1 (2012), 1–4

ДОДАТКИ

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

ІМЕНІ ІВАНА ПУЛЮЯ

МАТЕРІАЛИ

IX НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ,СИСТЕМИ ТА ТЕХНОЛОГІЇ»

8–9 грудня 2021 року

ТЕРНОПІЛЬ

2021

УДК 004.056
О. В. Ганайчук
(Тернопільський національний технічний університет імені Івана Пулюя)

ВИКОРИСТАННЯ ОПТИМІЗОВАНИХ АЛГОРИТМІВ АСИМЕТРИЧНОЇ КРИПТОГРАФІЇ (CL-PKE) ДЛЯ ПРИСТРОЇВ ІЗ ОБМЕЖЕНИМИ РЕСУРСАМИ

UDC 004.056
O. V. Hanaichuk

USE OF OPTIMIZED ALGORITHMS OF ASYMMETRIC CRYPTOGRAPHY (CL-PKE) FOR RESOURCE CONSTRAINED DEVICES

Пристрої з обмеженими ресурсами, такі як датчики та RFID, використовуються в багатьох областях застосування для визначення, зберігання та передачі конфіденційних даних. Ці дані мають бути зашифровані для забезпечення конфіденційності. Реалізація традиційних методів шифрування з відкритим ключем цими пристроями завжди є складною, оскільки вони мають дуже обмежені обчислювальні ресурси.

Щоб подолати загрозу атаки, необхідна інфраструктура відкритих ключів (PKI), яка керує сертифікатами, щоб створити захищену систему в традиційних налаштуваннях криптографії з відкритим ключем. Однак на практиці PKI стикається з багатьма проблемами, особливо з масштабованістю інфраструктури. Ідея, що стоїть за шифруванням із відкритим ключем без сертифікатів (CL-PKE), полягає в тому, що навіть якщо супротивник успішно замінює відкритий ключ жертви своїм власним вибором, він все одно не може розшифрувати повідомлення, зашифроване відкритим ключем, який він опублікував. Хоча ця ідея є досить непоганою, вона не підходить для традиційної системи відкритих ключів, в якій закритий ключ суб'єкта відповідає лише відкритому ключу суб'єкта.

Також PKI вимагає постійного онлайн-сервера сертифікації. Ця проблема вирішується тим, що CL-PKE залежить від офлайн-довіреної третьої сторони (TTP) для видачі повних приватних ключів (IBE) або часткових приватних ключів (CL-PKE) користувачам у мережі. Однак IBE страждає від проблеми депонування ключів, при якій усі приватні ключі користувачів розкриваються, якщо TTP скомпрометований або стає шкідливим. CL-PKE не страждає від проблеми депонування ключів і кваліфікується як безпечна схема шифрування. Однак алгоритм шифрування всіх існуючих схем IBE і CL-PKE вимагає обчислення модульного піднесення до степеня та операцій дволінійного створення пари над адитивною еліптичною кривою, які є обчислювально дуже дорогими криптографічними операціями. У контексті цього була розроблена полегшена оптимізована схема CL-PKE, в якій операції експонування та створення пари повністю виключаються під час шифрування і передбачає лише обчислення простих операцій додавання та множення на еліптичній кривій.

Література.

1. Dent, A., Libert, B., and Paterson, K.: "Certificateless Encryption Schemes Strongly Secure in the Standard Model"; To appear in Proc. PKC 2008, LNCS, Springer-Verlag (2008)
2. Ian Blake, Gadiel Seroussi, and Nigel Smart. 1999. Elliptic cur ves in cryptography.Vol. 265. Cambridge University Press.