Симетрична криптосистема на основі відображень скінченних кілець та її застосування у верифікованому шифруванні

Рябов Кирило

9 квітня 2025 р.

Анотація

Обсяг роботи: XX сторінок, Y ілюстрацій, Z таблиць, N джерел посилань.
КЛЮЧОВІ СЛОВА: ІЗОМОРФІЗМ КІЛЕЦЬ, КРИПТОГРАФІЯ, СИМЕТРИЧНА КРИПТОСИСТЕМА, СИСТЕМИ ЛІНІЙНИХ РІВНЯНЬ, СКІНЧЕННІ КІЛЬЦЯ, СЮР'ЄКТИВНІ ВІДОБРАЖЕННЯ, ДОКАЗИ З НУЛЬОВИМ РОЗГОЛОШЕННЯМ (ZKP), ІНТЕРАКТИВНІ ДОКАЗИ, ВЕРИФІКОВАНЕ ШИФРУВАННЯ

Об'єкт дослідження: Процеси симетричного шифрування та обміну інформацією на основі алгебраїчних структур скінченних кілець, а також методи їх інтеграції з протоколами доведення для забезпечення верифікованості.

Предмет дослідження: Симетрична криптосистема, що використовує сюр'єктивні відображення скінченних асоціативно-комутативних кілець з одиницею та системи лінійних рівнянь над такими кільцями; можливості поєднання даної криптосистеми з доведеннями з нульовим розголошенням та інтерактивними системами доведення для побудови схем верифікованого шифрування.

Мета роботи: Розробка та аналіз алгоритмів симетричної криптосистеми на основі відображень скінченних кілець; дослідження шляхів інтеграції розробленої системи з ZKP та IP/PCP для створення протоколів верифікованого шифрування, що не потребують обчислень з великими простими числами або полями великих порядків для базового шифрування.

Методи дослідження: Теорія скінченних кілець, теорія груп, лінійна алгебра над кільцями, методи побудови ізоморфізмів та сюр'єктивних відображень кілець, методи розв'язання систем лінійних рівнянь над кільцями лишків, методи криптографічного аналізу, теорія доказів з нульовим розголошенням, теорія інтерактивних доказів та ймовірнісно перевірюваних доказів.

Результати та їх новизна: Запропоновано протокол симетричного обміну інформацією на основі властивостей скінченних кілець. Розроблено алгоритм генерації ізоморфних кілець ('GEN-G'). Проаналізовано стійкість базової системи. Досліджено та запропоновано підходи до інтеграції даної криптосистеми з ZKP та IP/PCP для побудови схем верифікованого шифрування, де верифікація може стосуватися коректності шифрування або певних властивостей зашифрованих даних. Новизна полягає у комбінації специфічної симетричної криптосистеми на кільцях з сучасними техніками доведення для досягнення верифікованості обчислень над зашифрованими даними в контексті скінченних кілець.

Взаємозв'язок з іншими роботами: Робота розвиває ідеї симетричної криптографії на кільцях (напр., [**5**]) та досліджує їх застосування у контексті верифікованого шифрування, що є активною сферою досліджень.
Рекомендації щодо використання: Базова симетрична система може бути застосована для ефективного шифрування. Розширення з ZKP/IP/PCP можуть використовуватися у системах, де потрібна перевірка коректності шифрування або властивостей даних без їх розкриття (напр., довірчі обчислення, електронне голосування).
Сфера застосування: Симетрична криптографія, захист каналів зв'язку, верифіковані обчислення, протоколи з нульовим розголошенням.
Значимість роботи: Пропонується альтернативний підхід до побудови симетричних криптосистем та досліджується його потенціал для створення систем верифікованого шифрування на основі алгебраїчних структур скінченних кілець.
Висновки та пропозиції: Розроблена базова криптосистема є коректною. Досліджено потенціал її інтеграції з ZKP/IP/PCP. Подальші дослідження мають включати: поглиблений криптоаналіз базової системи; формальний аналіз безпеки запропонованих схем верифікованого шифрування; розробку ефективних протоколів ZKP/IP, сумісних з арифметикою скінченних кілець; аналіз продуктивності та накладних витрат верифікації.

Зміст

Вступ

Актуальність теми. Сучасна криптографія значною мірою покладається на обчислювально складні задачі теорії чисел, такі як факторизація великих цілих чисел або обчислення дискретних логарифмів у скінченних полях чи на еліптичних кривих cite1, 2. Хоча ці підходи довели свою ефективність, вони мають певні обмеження. По-перше, їх стійкість може бути під загрозою з появою потужних квантових комп'ютерів
citeshor$_q$$uantum. - , iii, ,$
$cite4.iii, i.$

Дана робота досліджує потенціал скінченних асоціативно-комутативних кілець та систем лінійних рівнянь над ними для побудови симетричної криптосистеми. Як зазначено у
cite5, основною мотивацією є створення системи, що не потребує громіздких обчислень з великими простими числами чи полями, а її стійкість ґрунтується на комбінаторній складності задач, пов'язаних з ізоморфізмами та сюр'єктивними відображеннями кілець відносно невеликих порядків.

Окрім базового шифрування, зростає інтерес до *верифікованих обчислень* та *верифікованого шифрування*, де можна довести певні властивості зашифрованих даних або коректність самого шифрування без розкриття секретної інформації. Інтеграція криптографічних систем з техніками доведення, такими як докази з нульовим розголошенням (ZKP) або інтерактивні докази (IP)
citezkp$_i$$ntro, ip_p space, iii.iiiiii, ii, iiiiii$
$citeverifiable_encryption_overview.$

Мета й завдання роботи. Метою даної дипломної роботи є розробка та аналіз симетричної криптосистеми на основі сюр'єктивних відображень скінченних кілець та систем лінійних рівнянь над ними, а також дослідження можливостей її інтеграції з протоколами доведення для створення схем верифікованого шифрування.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Проаналізувати теоретичні основи: теорію скінченних кілець, систем лінійних рівнянь над кільцями, основи симетричної криптографії та криптографічних доведень (ZKP, IP, PCP).

2. Описати алгоритми побудови необхідних алгебраїчних структур, зокрема алгоритм генерації ізоморфних кілець ('GEN-G') та побудови сюр'єктивних відображень.

3. Розробити та формально описати протокол симетричного обміну інформацією на основі запропонованих структур та методів.

4. Провести аналіз безпеки розробленої базової криптосистеми щодо відомих криптоатак (перебір ключа, атаки на основі відомого/обраного відкритого тексту, алгебраїчні атаки).

5. Оцінити обчислювальну ефективність базової системи (складність генерації ключів, шифрування, розшифрування) та порівняти її з існуючими аналогами.

6. Дослідити підходи до інтеграції розробленої симетричної криптосистеми з ZKP та/або IP/PCP для доведення коректності шифрування або властивостей зашифрованих даних.

7. Запропонувати концептуальну схему верифікованого шифрування на базі розробленої системи та протоколів доведення.

8. Сформулювати висновки щодо ефективності, безпеки та потенційних сфер застосування запропонованих підходів, а також окреслити напрямки подальших досліджень.

Об'єкт, предмет та методи дослідження. Об'єктом дослідження є процеси симетричного шифрування та обміну інформацією на основі алгебраїчних структур скінченних кілець, а також методи їх інтеграції з протоколами доведення для забезпечення верифікованості. Предметом дослідження є симетрична криптосистема, що використовує сюр'єктивні відображення скінченних асоціативно-комутативних кілець з одиницею та системи лінійних рівнянь над ними, та її застосування для побудови схем верифікованого шифрування. Методи дослідження включають теорію скінченних кілець, лінійну алгебру над кільцями, методи криптографічного аналізу, теорію доказів з нульовим розголошенням та інтерактивних доказів.

Наукова новизна. Наукова новизна роботи полягає у:

- Подальшому розвитку симетричної криптосистеми, запропонованої в cite5, з детальним описом протоколу та аналізом.

- Дослідженні та пропозиції конкретних шляхів інтеграції даної специфічної криптосистеми на основі скінченних кілець з сучасними техніками криптографічних доведень (ZKP, IP/PCP).

- Обґрунтуванні можливості створення на цій основі схем верифікованого шифрування, де перевірка стосується властивостей даних, зашифрованих за допомогою операцій у скінченних кільцях.

Практичне значення. Базова симетрична криптосистема може бути використана для ефективного шифрування даних у системах, де використання стандартних алгоритмів є небажаним або неможливим. Розширення з використанням ZKP/IP відкривають шлях до створення систем з додатковими гарантіями безпеки та прозорості, таких як системи довірчих обчислень, електронне голосування або інші протоколи, де потрібна верифікація обчислень над зашифрованими даними без їх розкриття.

Структура роботи. Робота складається зі вступу, чотирьох основних розділів, висновків та списку використаних джерел. У першому розділі наведено теоретичні відомості про скінченні кільця, системи лінійних рівнянь над ними, основи симетричної криптографії та вступ до криптографічних доведень. Другий розділ присвячено опису запропонованої симетричної криптосистеми, включаючи побудову алгебраїчних структур та протокол обміну повідомленнями. У третьому розділі проводиться аналіз безпеки та ефективності базової криптосистеми. Четвертий розділ розглядає розширення системи для задач верифікованого шифрування шляхом інтеграції з ZKP та IP/PCP. У висновках підсумовано отримані результати та окреслено напрямки подальших досліджень.

1 Теоретичні основи та огляд літератури

1.1 Основні поняття теорії скінченних кілець

1.1.1 Кільця лишків Z_k

Однією з фундаментальних структур у теорії скінченних кілець є кільце лишків за модулем k, яке позначається як Z_k або $\mathbb{Z}_k$. Це множина цілих чисел $\{0, 1, 2, \ldots, k-1\}$, де k – натуральне число, $k \geq 2$, разом з двома бінарними операціями: додаванням за модулем k (позначається як $+$ або $+_{\pmod k}$) та множенням за модулем k (позначається як $\cdot$ або $\cdot_{\pmod k}$).

Означення. Для будь-яких $a, b \in Z_k$:

- **Додавання за модулем k:** $a+b = (a+b) \pmod k$, де $(a+b) \pmod k$ – остача від ділення звичайного цілочисельного додавання $a + b$ на k.
- **Множення за модулем k:** $a \cdot b = (a \cdot b) \pmod k$, де $(a \cdot b) \pmod k$ – остача від ділення звичайного цілочисельного множення $a \cdot b$ на k.

Структура $(Z_k, +, \cdot)$ утворює скінченне асоціативно-комутативне кільце з одиницею
cite6. Це означає, що виконуються наступні властивості:

- $(Z_k, +)$ є абелевою групою:
  - Асоціативність додавання: $(a + b) + c = a + (b + c)$ для всіх $a, b, c \in Z_k$.
  - Комутативність додавання: $a + b = b + a$ для всіх $a, b \in Z_k$.
  - Існування нульового елемента: $0 \in Z_k$ такий, що $a + 0 = 0 + a = a$ для всіх $a \in Z_k$.
  - Існування протилежного елемента: для кожного $a \in Z_k$ існує $-a \in Z_k$ (зазвичай це $k - a$, якщо $a \neq 0$, і 0 для $a = 0$) такий, що $a + (-a) = (-a) + a = 0$.
- $(Z_k, \cdot)$ є комутативним моноїдом:
  - Асоціативність множення: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ для всіх $a, b, c \in Z_k$.
  - Комутативність множення: $a \cdot b = b \cdot a$ для всіх $a, b \in Z_k$.
  - Існування одиничного елемента: $1 \in Z_k$ (за умови $k \geq 2$) такий, що $a \cdot 1 = 1 \cdot a = a$ для всіх $a \in Z_k$.
- Дистрибутивність множення відносно додавання: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ та $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ для всіх $a, b, c \in Z_k$.

Кількість елементів у кільці Z_k дорівнює k.

Приклад. Розглянемо кільце $Z_6 = \{0, 1, 2, 3, 4, 5\}$.

- Додавання: $3 + 4 = (3 + 4) \pmod 6 = 7 \pmod 6 = 1$.
- Множення: $3 \cdot 4 = (3 \cdot 4) \pmod 6 = 12 \pmod 6 = 0$.
- Протилежний елемент для 2: $6 - 2 = 4$, оскільки $2 + 4 = 6 \pmod 6 = 0$.

Зауважимо, що в Z_6 існують дільники нуля (наприклад, $2 \cdot 3 = 0$, $3 \cdot 4 = 0$), що є важливою відмінністю від полів, де єдиним елементом, що дає нуль при множенні, є сам нуль. Це можливо, коли модуль k є складеним числом. Якщо k є простим числом, то Z_k є полем.

1.1.2 Ізоморфізми та гомоморфізми кілець

Гомоморфізми та ізоморфізми є фундаментальними поняттями в алгебрі, які дозволяють порівнювати та встановлювати зв'язки між різними кільцями. Вони описують відображення, що зберігають структуру кільця, тобто узгоджуються з операціями додавання та множення.

Означення (Гомоморфізм кілець). Нехай $(R, +_R, \cdot_R)$ та $(S, +_S, \cdot_S)$ – два кільця. Відображення $\varphi : R \to S$ називається **гомоморфізмом кілець**, якщо для будь-яких $a, b \in R$ виконуються умови:

1. $\varphi(a +_R b) = \varphi(a) +_S \varphi(b)$ (зберігає додавання)
2. $\varphi(a \cdot_R b) = \varphi(a) \cdot_S \varphi(b)$ (зберігає множення)

Якщо кільця R та S мають одиничні елементи 1_R та 1_S відповідно, то часто вимагається додаткова умова для гомоморфізму унітарних кілець:

3. $\varphi(1_R) = 1_S$ (зберігає одиничний елемент)

Гомоморфізм показує, що структура кільця S певним чином відображає структуру кільця R. Образ гомоморфізму $\varphi(R) = \{\varphi(a) \mid a \in R\}$ є підкільцем кільця S. Ядро гомоморфізму $\ker(\varphi) = \{a \in R \mid \varphi(a) = 0_S\}$, де 0_S – нульовий елемент в S, є ідеалом кільця R.

Означення (Ізоморфізм кілець). Гомоморфізм кілець $\varphi : R \to S$ називається **ізоморфізмом кілець**, якщо він є бієктивним відображенням (тобто одночасно ін'єктивним та сюр'єктивним).

- **Ін'єктивність:** Якщо $\varphi(a) = \varphi(b)$, то $a = b$. Еквівалентно, $\ker(\varphi) = \{0_R\}$, де 0_R – нульовий елемент в R.
- **Сюр'єктивність:** Для будь-якого $s \in S$ існує $a \in R$ такий, що $\varphi(a) = s$. Еквівалентно, $\varphi(R) = S$.

Якщо існує ізоморфізм між кільцями R та S, то кажуть, що кільця R та S є **ізоморфними**, і позначають це як $R \cong S$.

Ізоморфні кільця є алгебраїчно нерозрізнюваними. Вони мають однакову структуру та властивості, відрізняючись лише, можливо, позначеннями своїх елементів. З точки зору теорії кілець, вони вважаються "однаковими". Це поняття є ключовим для даної роботи, оскільки запропонована криптосистема використовує кільце G_k, яке конструюється таким чином, щоб бути ізоморфним стандартному кільцю лишків Z_k (або Z_m у схемі протоколу). Ізоморфізм $\varphi : G_k \to Z_k$ дозволяє виконувати обчислення у зручнішому кільці Z_k, а потім переносити результати назад у G_k, як це описано в
cite5 та використовується у протоколі (див. Розділ 2 та Рис.
reffig:schema).

Приклад. Розглянемо кільце $Z_4 = \{0, 1, 2, 3\}$ та кільце $R = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in Z_2\}$ з операціями матричного додавання та множення за модулем 2. Кільце R має 4 елементи: $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. Відображення $\psi : Z_4 \to Z_2$, визначене як $\psi(x) = x \pmod 2$, є гомоморфізмом кілець: $\psi(2 + 3) = \psi(1) = 1$, $\psi(2) + \psi(3) = 0 + 1 = 1$. $\psi(2 \cdot 3) = \psi(2) = 0$, $\psi(2) \cdot \psi(3) = 0 \cdot 1 = 0$. Однак, це не ізоморфізм (не ін'єктивний, $\psi(0) = \psi(2)$, $\psi(1) = \psi(3)$). Ізоморфізмів між Z_4 та R не існує, оскільки їхні структури відрізняються (наприклад, в Z_4 є елемент 2 такий, що $2 \cdot 2 = 0$, а в R ненульовий елемент $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ при множенні на себе дає одиничну матрицю). Питання побудови ізоморфних кілець $G_k \cong Z_k$ розглядається детальніше в розділі 2.2.

1.1.3 Дільники нуля та одиниці

У кільці лишків Z_k, як і в будь-якому кільці, особливу роль відіграють елементи, що мають специфічні властивості відносно операції множення. Це дільники нуля та дільники одиниці (одиниці кільця).

Означення (Дільник нуля). Ненульовий елемент $a \in Z_k$ називається **дільником нуля**, якщо існує інший ненульовий елемент $b \in Z_k$ такий, що $a \cdot b = 0 \pmod k$.

Дільники нуля існують в кільці Z_k тоді і тільки тоді, коли k є складеним числом. Якщо k – просте число, то Z_k є полем, і в ньому немає дільників нуля (крім самого нуля, який за означенням не є дільником нуля). Властивість існування дільників нуля є ключовою відмінністю кілець Z_k при складених k від полів. Вона впливає на розв'язання рівнянь та систем рівнянь у таких кільцях. Наприклад, рівняння $ax = b$ може мати більше одного розв'язку або не мати жодного, навіть якщо $a \neq 0$.

Приклад (Дільники нуля в Z_6). Розглянемо кільце $Z_6 = \{0, 1, 2, 3, 4, 5\}$.

- $2 \cdot 3 = 6 \equiv 0 \pmod 6$. Отже, 2 і 3 є дільниками нуля.
- $4 \cdot 3 = 12 \equiv 0 \pmod 6$. Отже, 4 також є дільником нуля (і 3, як ми вже знаємо).

Таким чином, дільниками нуля в Z_6 є елементи {2, 3, 4}.

Означення (Дільник одиниці / Одиниця кільця). Елемент $a \in Z_k$ називається **дільником одиниці** або **одиницею кільця** (або **оборотним елементом**), якщо існує елемент $a^{-1} \in Z_k$ такий, що $a \cdot a^{-1} = a^{-1} \cdot a = 1 \pmod k$. Елемент a^{-1} називається оберненим до a.

Твердження. Елемент $a \in Z_k$ є дільником одиниці (має обернений за множенням) тоді і тільки тоді, коли найбільший спільний дільник a та k дорівнює 1, тобто НСД$(a, k) = 1$.

Доведення. Якщо НСД$(a, k) = 1$, то за розширеним алгоритмом Евкліда існують цілі числа x та y такі, що $ax + ky = 1$. Розглядаючи це рівняння за модулем k, отримуємо $ax \equiv 1 \pmod k$. Отже, $x \pmod k$ є оберненим до a в Z_k. Навпаки, якщо існує a^{-1} такий, що $a \cdot a^{-1} = 1 \pmod k$, то $a \cdot a^{-1} = 1 + mk$ для деякого цілого m. Це означає, що $a \cdot a^{-1} - mk = 1$. Будь-який спільний дільник a і k повинен також ділити $a \cdot a^{-1} - mk$, тобто 1. Отже, НСД$(a, k) = 1$. ■

Сукупність усіх дільників одиниці кільця Z_k утворює мультиплікативну групу, яка позначається Z_k^* або $U(Z_k)$. Порядок цієї групи (кількість дільників одиниці) дорівнює значенню функції Ейлера $\varphi(k)$.

Приклад (Дільники одиниці в Z_6). Розглянемо кільце Z_6.

- НСД(1, 6) = 1. $1 \cdot 1 = 1 \pmod 6$. Отже, 1 є дільником одиниці.
- НСД(2, 6) = $2 \neq 1$. 2 не є дільником одиниці.
- НСД(3, 6) = $3 \neq 1$. 3 не є дільником одиниці.
- НСД(4, 6) = $2 \neq 1$. 4 не є дільником одиниці.
- НСД(5, 6) = 1. $5 \cdot 5 = 25 \equiv 1 \pmod 6$. Отже, 5 є дільником одиниці, і $5^{-1} = 5$.

Таким чином, дільниками одиниці в Z_6 є елементи $\{1, 5\}$, і $Z_6^* = \{1, 5\}$. $\varphi(6) = 6(1 - 1/2)(1 - 1/3) = 6(1/2)(2/3) = 2$.

У кільці Z_k при $k > 1$ кожен ненульовий елемент є або дільником нуля, або дільником одиниці. Дійсно, якщо НСД$(a, k) = 1$, то a є дільником одиниці. Якщо ж НСД$(a, k) = d > 1$, то $a \neq 0$. Нехай $b = k/d$. Тоді b є цілим числом, $1 \leq b < k$, отже $b \in Z_k$ і $b \neq 0$. Маємо $a \cdot b = a \cdot (k/d) = (a/d) \cdot k$. Оскільки a/d є цілим, то $a \cdot b$ ділиться на k, тобто $a \cdot b \equiv 0 \pmod k$. Оскільки $a \neq 0$ та $b \neq 0$, то a є дільником нуля.

1.1.4 Мультиплікативна група кільця (Z_k^*)

Як було зазначено в попередньому підрозділі, множина дільників одиниці кільця Z_k утворює групу відносно операції множення за модулем k. Ця група називається **мультиплікативною групою кільця Z_k** і позначається Z_k^*.

Означення. Мультиплікативна група кільця Z_k – це множина $Z_k^* = \{a \in Z_k \mid$ НСД$(a, k) = 1\}$ разом з операцією множення за модулем k.

Властивості групи Z_k^*:

- **Замкненість:** Якщо $a, b \in Z_k^*$, то НСД$(a, k) = 1$ і НСД$(b, k) = 1$. З властивостей НСД випливає, що НСД$(a \cdot b, k) = 1$, отже $a \cdot b \pmod k \in Z_k^*$.
- **Асоціативність:** Випливає з асоціативності множення в кільці Z_k.
- **Існування одиничного елемента:** $1 \in Z_k^*$ (оскільки НСД$(1, k) = 1$ для $k \geq 2$), і $a \cdot 1 = 1 \cdot a = a$ для всіх $a \in Z_k^*$.
- **Існування оберненого елемента:** Для кожного $a \in Z_k^*$ існує $a^{-1} \in Z_k^*$ такий, що $a \cdot a^{-1} = 1 \pmod k$. (Те, що a^{-1} також належить Z_k^*, випливає з того, що якщо $ax \equiv 1 \pmod k$, то НСД$(x, k) = 1$).

Оскільки множення в Z_k комутативне, група Z_k^* є абелевою. Порядок групи $|Z_k^*|$ дорівнює $\varphi(k)$, де φ – функція Ейлера.

Структура групи Z_k^*. Структура групи Z_k^* залежить від розкладу числа k на прості множники.

- **Випадок простого $k = p$:** Якщо $k = p$ – просте число, то Z_p є полем, і $Z_p^* = \{1, 2, \ldots, p - 1\}$. Ця група завжди є **циклічною**, тобто існує елемент $g \in Z_p^*$ (генератор, або первісний корінь за модулем p), такий, що кожен елемент $a \in Z_p^*$ можна подати як степінь g, тобто $Z_p^* = \{g^0, g^1, \ldots, g^{p-2}\}$. Порядок групи $\varphi(p) = p - 1$.

- **Випадок степеня непарного простого $k = p^m$, $m \geq 1$:** Група $Z^*_{p^m}$ також є **циклічною**. Її порядок $\varphi(p^m) = p^m - p^{m-1}$.

- **Випадок $k = 2^m$:**
  - При $k = 2$ ($m = 1$), $Z^*_2 = \{1\}$, циклічна.
  - При $k = 4$ ($m = 2$), $Z^*_4 = \{1, 3\}$, циклічна (генератор 3).
  - При $k = 2^m$, $m \geq 3$, група $Z^*_{2^m}$ **не є циклічною**. Вона є прямим добутком циклічної групи порядку 2 (породженої елементом $-1 \equiv 2^m - 1$) та циклічної групи порядку 2^{m-2} (породженої елементом 5). $Z^*_{2^m} \cong C_2 \times C_{2^{m-2}}$. Її порядок $\varphi(2^m) = 2^m - 2^{m-1} = 2^{m-1}$.

- **Загальний випадок (Теорема Гаусса):** Як зазначено в cite6 (Теорема refgaus у 'papers/theory.tex'), мультиплікативна група Z^*_k є **циклічною** тоді і тільки тоді, коли k дорівнює 2, 4, p^m або $2p^m$, де p – непарне просте число, $m \geq 1$.

- **Структура за Китайською теоремою про остачі (CRT):** Якщо k має розклад на взаємно прості множники $k = n_1 n_2 \cdots n_r$, то Китайська теорема про остачі стверджує, що кільце Z_k ізоморфне прямому добутку кілець $Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_r}$. Цей ізоморфізм індукує ізоморфізм мультиплікативних груп:
$$Z^*_k \cong Z^*_{n_1} \times Z^*_{n_2} \times \cdots \times Z^*_{n_r}$$

  Зокрема, якщо канонічний розклад $k = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$, то
$$Z^*_k \cong Z^*_{p_1^{e_1}} \times Z^*_{p_2^{e_2}} \times \cdots \times Z^*_{p_s^{e_s}}$$

  Це дозволяє визначити структуру Z^*_k через структуру груп $Z^*_{p^e}$. Група Z^*_k буде циклічною лише у випадках, перелічених у теоремі Гаусса.

Приклади.

- Z^*_5: $k = 5$ (просте). $Z^*_5 = \{1, 2, 3, 4\}$. $\varphi(5) = 4$. Група циклічна. Генератори: 2 ($2^1 = 2, 2^2 = 4, 2^3 = 3, 2^4 = 1$) і 3.

- Z^*_8: $k = 8 = 2^3$. $Z^*_8 = \{1, 3, 5, 7\}$. $\varphi(8) = 4$. Група не є циклічною, оскільки $3^2 = 1, 5^2 = 1, 7^2 = 1$, немає елемента порядку 4. $Z^*_8 \cong C_2 \times C_2$.

- Z^*_6: $k = 6 = 2 \cdot 3$. $Z^*_6 = \{1, 5\}$. $\varphi(6) = 2$. Група циклічна (генератор 5). $Z^*_6 \cong Z^*_2 \times Z^*_3 \cong \{1\} \times \{1, 2\}$. Відповідність за CRT: $1 \leftrightarrow (1, 1)$, $5 \leftrightarrow (1, 2)$.

- Z^*_{15}: $k = 15 = 3 \cdot 5$. $Z^*_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$. $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$. Група не є циклічною, оскільки k не має вигляду p^m або $2p^m$. $Z^*_{15} \cong Z^*_3 \times Z^*_5 \cong C_2 \times C_4$.

Розуміння структури Z^*_k, зокрема умов її циклічності, є важливим для деяких криптографічних застосувань, наприклад, пов'язаних з дискретним логарифмуванням. Хоча запропонована система безпосередньо не покладається на складність дискретного логарифмування в Z^*_k, знання властивостей цієї групи є корисним для загального аналізу кільця Z_k.

1.2 Системи лінійних рівнянь над кільцями лишків

Системи лінійних рівнянь (СЛР) над кільцями лишків Z_k відіграють центральну роль у запропонованій криптосистемі, зокрема на етапах шифрування та формування повідомлення
cite5. На відміну від систем над полями, де теорія є добре розвиненою, розв'язання СЛР над кільцями Z_k (особливо при складеному k) має свої особливості, пов'язані з існуванням дільників нуля.

Розглянемо систему p лінійних рівнянь з q невідомими над кільцем Z_k:
$\mathrm{Ax} \equiv b \pmod{k}$

де $A = (a_{ij})$ – матриця коефіцієнтів розмірності $p \times q$ з елементами $a_{ij} \in Z_k$, $x = (x_1, \ldots, x_q)^T$ – вектор невідомих, $b = (b_1, \ldots, b_p)^T$ – вектор вільних членів з $b_i \in Z_k$. У контексті криптосистеми, k часто дорівнює m, а система $l(x) = v$ використовується для кодування повідомлення v у вектор x (див. Розділ 2.4.3 та
citetheory.tex, Крок 2б).

1.2.1 Умови існування та єдиності розв´зків

Питання існування та кількості розв'язків системи $Ax \equiv b \pmod{k}$ є складнішим, ніж над полем.

Випадок квадратних систем ($p = q$) з невиродженою матрицею. Якщо матриця A є квадратною ($p = q$) і її детермінант $\det(A)$ є дільником одиниці в Z_k (тобто $\text{НСД}(\det(A), k) = 1$), то матриця A є оборотною над Z_k. У цьому випадку система $Ax \equiv b \pmod{k}$ має **єдиний** розв'язок для будь-якого вектора b, який можна знайти як $x \equiv A^{-1}b \pmod{k}$, де A^{-1} – обернена матриця до A над Z_k.

Загальний випадок. Якщо $\det(A)$ не є дільником одиниці (або якщо система не квадратна), ситуація ускладнюється.

- **Існування розв´зку: Система $Ax \equiv b \pmod{k}$ має розв'язок тоді і тільки тоді, коли для кожного простого множника p числа k, система $Ax \equiv b \pmod{p^e}$ має розв'язок, де p^e – максимальний степінь p, що ділить k. Далі, система $Ax \equiv b \pmod{p^e}$ має розв'язок тоді і тільки тоді, коли $\text{НСД}(d_1, \ldots, d_n, p^e)$ ділить $\text{НСД}(c, p^e)$ для всіх лінійних комбінацій рядків $\sum r_i A_i = (d_1, \ldots, d_n)$, що дорівнюють нулю за модулем p^e, де $c = \sum r_i b_i$. Більш практичний критерій, наведений у
  cite7 та згаданий у
  citetheory.tex (Розділ 4), пов'язує сумісність системи $Ax \equiv b \pmod{m}$ розмірності $p \times q$ ($p < q$) з існуванням розв'язку певного порівняння $d_1 y_1 + \ldots + d_s y_s \equiv 1 \pmod{m}$, де d_i пов'язані з розв'язками відповідної однорідної системи. Система (??) з
  citetheory.tex $l(x) \equiv b \pmod{m}$ гарантовано має розв'язок для довільного b, якщо рівняння лінійно незалежні і існує підсистема $A_1 u \equiv b \pmod{m}$ ($p \times p$) з $\text{НСД}(\det(A_1), m) = 1$. Це забезпечує можливість кодування будь-якого повідомлення b.**

- **Кількість розв´зків: Якщо система має хоча б один розв'язок x_0, то множина всіх розв'язків має вигляд $x_0 + N(A)$, де $N(A) = \{y \in Z_k^q \mid Ay \equiv 0 \pmod{k}\}$ – множина розв'язків відповідної однорідної системи**

(ядро відображення $x \mapsto Ax$). Кількість розв'язків дорівнює $|N(A)|$. Обчислення $|N(A)|$ в загальному випадку може бути складним.

В контексті криптосистеми
citetheory.tex, Аліса має побудувати систему $l(x)$ так, щоб вона гарантовано мала розв'язок для будь-якого повідомлення v, яке хоче передати Боб. Це досягається вибором матриці A розмірності $p \times q$ $(p < q)$, рядки якої лінійно незалежні над Z_m і яка містить p лінійно незалежних стовпчиків, що утворюють підматрицю A_1 з $\det(A_1)$, взаємно простим з m (тобто $\det(A_1) \in Z_m^*$).

1.2.2 Методи розв´зання

Методи розв'язання СЛР над Z_k залежать від властивостей матриці A та модуля k.

Метод оберненої матриці. Якщо A – квадратна матриця і $\det(A) \in Z_k^*$, то розв'язок єдиний і знаходиться як $x \equiv A^{-1}b \pmod{k}$. Обернену матрицю A^{-1} можна знайти за формулою $A^{-1} \equiv (\det(A))^{-1} \cdot \text{adj}(A) \pmod{k}$, де $\text{adj}(A)$ – союзна матриця (транспонована матриця алгебраїчних доповнень). Обчислення $(\det(A))^{-1}$ вимагає знаходження оберненого до $\det(A)$ за модулем k, що можливо лише коли $\text{НСД}(\det(A), k) = 1$, і виконується за допомогою розширеного алгоритму Евкліда.

Метод Гаусса. Стандартний метод Гаусса (приведення до трикутного або ступінчастого вигляду) можна адаптувати для роботи над Z_k. Однак виникають ускладнення:

- **Ділення:** Операція ділення a/b можлива лише якщо $b \in Z_k^*$. Якщо ведучий елемент (pivot) не є дільником одиниці, не можна просто поділити рядок на нього.
- **Скорочення:** Якщо $ca \equiv cb \pmod{k}$ і $c \notin Z_k^*$, то не можна просто скоротити на c. Правильне скорочення: $a \equiv b \pmod{k/\text{НСД}(c,k)}$.
- **Перестановки рядків/стовпців:** Дозволені.
- **Додавання кратного одного рядка до іншого:** Дозволено.

Модифіковані алгоритми типу Гаусса існують
cite7, вони можуть використовувати операції множення на обернені елементи (якщо можливо) та спеціальні перетворення для роботи з дільниками нуля, іноді зводячи задачу до розв'язання систем за простими модулями p^e за допомогою CRT. Для систем, що використовуються в протоколі
citetheory.tex, де існує невироджена підматриця A_1, розв'язок можна знайти, зафіксувавши $q - p$ вільних змінних (наприклад, прирівнявши їх до нуля) і розв'язавши отриману квадратну систему $A_1 u \equiv b' \pmod{m}$ методом оберненої матриці.

Інші методи. Для невеликих k можна використовувати методи повного перебору або спеціалізовані алгоритми. Для великих систем можуть бути ефективними ітераційні методи, якщо вони збігаються.

Як зазначено в
citetheory.tex, алгоритми розв'язання СЛР над кільцями Z_k (у випадках, що використовуються в протоколі) мають поліноміальну складність від розміру системи та $\log k$.

1.3 Основи симетричної криптографії

Симетрична криптографія, також відома як криптографія з секретним ключем, є одним з двох основних напрямків сучасної криптографії (іншим є асиметрична криптографія). Її ключова особливість полягає у використанні одного й того ж секретного ключа як для шифрування, так і для розшифрування повідомлень. Цей розділ надає огляд фундаментальних понять, моделей безпеки та принципів симетричної криптографії, що є необхідним для розуміння та аналізу запропонованої в даній роботі криптосистеми.

1.3.1 Визначення та моделі безпеки

Формально, симетрична схема шифрування визначається як набір з трьох поліноміальночасових алгоритмів $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$:

- **Генерація ключа (Gen):** Алгоритм, який на вхід отримує параметр безпеки 1^n і на виході видає секретний ключ k. Ключ k вибирається з певного ключового простору $\mathcal{K}$.
- **Шифрування (Enc):** Алгоритм, який на вхід отримує секретний ключ $k \in \mathcal{K}$ та повідомлення (відкритий текст) m з простору повідомлень $\mathcal{M}$, і на виході видає шифротекст c з простору шифротекстів $\mathcal{C}$. Позначається як $c \leftarrow \mathrm{Enc}_k(m)$ або $c \leftarrow \mathrm{Enc}(k, m)$. Процес шифрування може бути детермінованим або ймовірнісним (використовуючи випадковість).
- **Розшифрування (Dec):** Детермінований алгоритм, який на вхід отримує секретний ключ $k \in \mathcal{K}$ та шифротекст $c \in \mathcal{C}$, і на виході видає повідомлення $m' \in \mathcal{M}$ або спеціальний символ помилки $\perp$ (якщо шифротекст недійсний). Позначається як $m' \leftarrow \mathrm{Dec}_k(c)$ або $m' \leftarrow \mathrm{Dec}(k, c)$.

Для коректної схеми шифрування має виконуватися умова: для всіх n, всіх ключів k, згенерованих $\mathrm{Gen}(1^n)$, і всіх повідомлень $m \in \mathcal{M}$, виконується $\mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m$.

Моделі безпеки. Безпека симетричної криптосистеми визначається відносно можливостей супротивника (криптоаналітика) та цілей, яких він намагається досягти. Стандартні моделі безпеки визначаються через "гру в якій супротивник взаємодіє з оракулами, що імітують реальне використання системи.

- **Безпека проти атаки з відомим шифротекстом (Ciphertext-Only Attack - COA):** Найслабша модель. Супротивник має доступ лише до набору шифротекстів і намагається відновити відкритий текст або ключ.
- **Безпека проти атаки з відомим відкритим текстом (Known-Plaintext Attack - KPA):** Супротивник має доступ до деякої кількості пар (відкритий текст, відповідний шифротекст).
- **Безпека проти атаки на основі обраного відкритого тексту (Chosen-Plaintext Attack - CPA):** Супротивник може вибирати довільні повідомлення та отримувати їхні шифротексти від оракула шифрування. Метою є отримання інформації про інші шифротексти або ключ. Формально визначається через гру **нерозрізненності шифротекстів при атаці на основі обраного відкритого тексту (Indistinguishability under Chosen-Plaintext Attack - IND-CPA)**. Супротивник вибирає два повідомлення m_0, m_1, отримує шифротекст $c = \mathrm{Enc}_k(m_b)$

для випадково обраного $b \in \{0, 1\}$ і повинен вгадати b. Система вважається IND-CPA безпечною, якщо перевага супротивника у вгадуванні b над випадковим вибором (1/2) є незначною (зростає повільніше за будь-який поліном від параметра безпеки). Для досягнення IND-CPA безпеки шифрування має бути ймовірнісним або використовувати стан (stateful).

- **Безпека проти атаки на основі обраного шифротексту (Chosen-Ciphertext Attack - CCA):** Найсильніша модель для симетричних систем (розрізняють CCA1 та CCA2). Супротивник має доступ не лише до оракула шифрування, а й до оракула розшифрування, якому може надсилати довільні шифротексти (крім того, який він намагається "зламати") та отримувати відповідні відкриті тексти. Формально визначається через гру **нерозрізненності шифротекстів при атаці на основі обраного шифротексту (IND-CCA)**. Ця модель враховує здатність супротивника маніпулювати шифротекстами. Досягнення IND-CCA безпеки зазвичай вимагає механізмів автентифікації шифротексту (наприклад, через Message Authentication Codes (MAC) або схеми автентифікованого шифрування (Authenticated Encryption - AE)).

Запропонована в роботі система буде аналізуватися з точки зору цих моделей, зокрема IND-CPA.

1.3.2 Класичні шифри та їх аналіз

Історично існувало багато симетричних шифрів, які сьогодні вважаються незахищеними. Їх аналіз допомагає зрозуміти базові принципи криптоаналізу.

- **Шифри простої заміни:** Кожна літера алфавіту замінюється іншою (наприклад, шифр Цезаря, де зсув фіксований). Легко зламуються частотним аналізом, оскільки частота літер у шифротексті відповідає частоті літер у відкритому тексті.

- **Поліалфавітні шифри:** Використовують кілька алфавітів заміни (наприклад, шифр Віженера). Стійкіші до простого частотного аналізу, але можуть бути зламані за допомогою методу Казіскі (пошук повторюваних блоків для визначення довжини ключа) та подальшого частотного аналізу для кожної позиції ключа.

- **Шифр Вернама (One-Time Pad - OTP):** Теоретично досконалий шифр, якщо ключ є абсолютно випадковим, використовується лише один раз і має ту ж довжину, що й повідомлення. Шифрування $c = m \oplus k$, розшифрування $m = c \oplus k$. На практиці складний через необхідність безпечної передачі та зберігання довгих ключів.

Аналіз класичних шифрів показав важливість таких концепцій, як **дифузія** (розсіювання впливу одного символу відкритого тексту на багато символів шифротексту) та **конфузія** (ускладнення зв'язку між ключем та шифротекстом), запропонованих Клодом Шенноном
citeshannon$_c omm_t heory$.

1.3.3 Сучасні симетричні алгоритми (огляд)

Сучасні симетричні алгоритми проектуються з урахуванням принципів дифузії та конфузії та стійкості до відомих методів криптоаналізу (лінійний, диференціальний аналіз тощо). Основні типи:

- **Блокові шифри:** Обробляють дані фіксованими блоками (наприклад, 64 або 128 біт).
  - **DES (Data Encryption Standard):** Застарілий стандарт (розмір ключа 56 біт недостатній).
  - **AES (Advanced Encryption Standard):** Сучасний стандарт (Rijndael), використовує ключі 128, 192 або 256 біт, блоки 128 біт. Вважається безпечним та ефективним. Побудований на принципі SPN (Substitution-Permutation Network).

  Блокові шифри використовуються в різних **режимах роботи** (modes of operation, наприклад, ECB, CBC, CTR, GCM) для шифрування повідомлень довільної довжини. Деякі режими (наприклад, GCM, CCM) забезпечують **автентифіковане шифрування (AEAD - Authenticated Encryption with Associated Data)**, одночасно гарантуючи конфіденційність та цілісність/автентичність даних.

- **Потокові шифри:** Генерують псевдовипадкову послідовність (ключовий потік), яка потім поєднується з відкритим текстом за допомогою операції XOR (подібно до OTP, але з псевдовипадковим ключовим потоком). Приклади: RC4 (застарілий, має вразливості), ChaCha20 (сучасний, швидкий та безпечний). Зазвичай швидші за блокові шифри, але вимагають обережного використання (не можна повторно використовувати той самий стан (ключ+nonce)).

- **Криптографічні геш-функції:** (Не шифри, але важливі в симетричній криптографії) Функції, що відображають дані довільної довжини у вихідний рядок фіксованої довжини (геш). Мають властивості стійкості до знаходження прообразу, другого прообразу та колізій. Використовуються для перевірки цілісності, у MAC. Приклади: SHA-256, SHA-3.

- **Коди автентифікації повідомлень (MAC):** Використовуються для забезпечення цілісності та автентичності повідомлень. Генеруються за допомогою секретного ключа. Приклади: HMAC (на основі геш-функцій), CMAC (на основі блокових шифрів).

Запропонована система є симетричною, але її структура (використання СЛР над кільцями) відрізняється від класичних блокових чи потокових шифрів. Порівняння з ними буде проведено в розділі 3.3.

1.3.4 Принцип Керкгоффса

Основоположний принцип проектування криптосистем, сформульований Огюстом Керкгоффсом у 19 столітті: **стійкість криптосистеми не повинна залежати від секретності самого алгоритму, а лише від секретності ключа.** Це означає, що алгоритм шифрування/розшифрування може бути загальновідомим (опублікованим,

стандартизованим), і система має залишатися безпечною, доки ключ зберігається в таємниці. Цей принцип дозволяє проводити відкритий аналіз алгоритмів спільнотою криптографів, виявляти потенційні вразливості та будувати довіру до стандартизованих систем. Сучасні криптографічні алгоритми (AES, RSA тощо) розробляються відповідно до цього принципу. При аналізі безпеки запропонованої системи також будемо виходити з припущення, що алгоритм відомий криптоаналітику.

1.4 Огляд існуючих підходів до криптографії на основі кілець

Використання алгебраїчних структур кілець, відмінних від полів, є активним напрямком досліджень в сучасній криптографії. Кільця пропонують багатшу математичну структуру порівняно з полями, зокрема через наявність дільників нуля (у випадку кілець Z_k зі складеним k), що може бути використано для побудови нових криптографічних схем або аналізу їхньої безпеки.

Переважно, дослідження криптографії на основі кілець зосереджені в області **асиметричної криптографії**, особливо в контексті **постквантової криптографії**. Одним з найвідоміших прикладів є криптографія на основі задачі **Навчання з Помилками над Кільцями (Ring Learning With Errors - Ring-LWE)** [**lyubashevsky_rlwe**]. Ring-LWE є варіантом задачі Навчання з Помилками (Learning With Errors - LWE) [**regev_lwe**], адаптованим для роботи з поліноміальними кільцями (часто $Z_q[x]/\langle f(x)\rangle$, де $f(x)$ – незвідний поліном, наприклад, циклотомний). Схеми на основі Ring-LWE дозволяють будувати ефективні постквантові системи шифрування з відкритим ключем та схеми цифрового підпису. Хоча ці системи є асиметричними, вони демонструють потенціал використання специфічних властивостей кілець для криптографічних цілей.

У сфері **симетричної криптографії** використання кілець, відмінних від полів (зокрема $GF(2)$ або $GF(2^n)$, які широко застосовуються в AES, SHA-3 тощо), є менш дослідженим напрямком порівняно з асиметричною криптографією. Однак існують певні підходи та пропозиції. Наприклад, деякі конструкції геш-функцій або потокових шифрів можуть використовувати операції в кільцях Z_{2^w} (кільця цілих чисел за модулем степеня двійки), як це робиться в компонентах шифрів RC5/RC6 або геш-функції MD5 (хоча остання вважається зламаною).

Дана робота зосереджена на **симетричній криптосистемі**, що безпосередньо використовує властивості скінченних асоціативно-комутативних кілець Z_k (або ізоморфних їм G_k) та систем лінійних рівнянь над ними. Як зазначалося у Вступі, основна ідея, що розвивається в цій роботі, була запропонована в [**5**]. Цей підхід відрізняється від згаданих вище постквантових схем на поліноміальних кільцях і пропонує альтернативну конструкцію симетричного шифру, стійкість якого пов'язана не з задачами типу LWE, а з комбінаторною складністю знаходження невідомих ізоморфізмів, сюр'єктивних відображень та розв'язання певних систем рівнянь над кільцями лишків. Наступні розділи детально описують та аналізують саме цю систему, що базується на ідеях роботи [**5**].

1.5 Вступ до криптографічних доведень

1.5.1 Доведення з нульовим розголошенням (Zero-Knowledge Proofs - ZKP)

Доведення з нульовим розголошенням (ZKP) є фундаментальним поняттям сучасної криптографії, яке дозволяє одній стороні (Доводжувачу, Prover) переконати іншу сторону (Перевіряючого, Verifier) у істинності певного математичного твердження, не розкриваючи жодної додаткової інформації, окрім самого факту істинності цього твердження
citegoldwasser1989knowledge.

Ідея полягає в інтерактивному протоколі між Доводжувачем (П) та Перевіряючим (В). П володіє певним секретним "свідком"(witness) w, який підтверджує істинність публічного твердження $x \in L$ (де L – деяка мова, що представляє властивість, яку перевіряють, наприклад, "цей шифротекст коректно сформований"). Мета П – переконати В, що $x \in L$, не розкриваючи w.

Формально, інтерактивний протокол доведення (P, V) для мови L називається доведенням з нульовим розголошенням, якщо він задовольняє три властивості:

- **Повнота (Completeness):** Якщо твердження x є істинним (тобто $x \in L$) і Доводжувач та Перевіряючий дотримуються протоколу, то Перевіряючий завжди (або з дуже високою ймовірністю) прийме доведення.

  $$\forall x \in L, \forall w \text{ (свідок для } x), \ \Pr[\text{Output}_V(\langle P(w), V\rangle(x)) = \text{accept}] = 1$$

  (або $\geq 1 - \epsilon$ для незначного ϵ).

- **Обґрунтованість (Soundness):** Якщо твердження x є хибним (тобто $x \notin L$), то жоден нечесний Доводжувач P^*, навіть з необмеженими обчислювальними можливостями (у деяких моделях), не зможе переконати чесного Перевіряючого прийняти доведення, крім як з дуже малою ймовірністю (помилка обґрунтованості).

  $$\forall x \notin L, \forall P^*, \ \Pr[\text{Output}_V(\langle P^*, V\rangle(x)) = \text{accept}] \leq \delta$$

  (де δ – незначна ймовірність).

- **Нульове розголошення (Zero-Knowledge):** Перевіряючий не дізнається нічого, крім істинності твердження $x \in L$. Формально це означає, що все, що Перевіряючий може обчислити після взаємодії з Доводжувачем (транскрипт протоколу), він міг би обчислити самостійно, маючи лише твердження x. Це моделюється за допомогою концепції симулятора: для будь-якого (ймовірносно-поліноміального) Перевіряючого V^* існує симулятор S, який, маючи лише x, може згенерувати транскрипт взаємодії, нерозрізненний від реального транскрипту між P та V^*.

Класичними прикладами проблем, для яких існують ефективні ZKP, є задачі з класу NP, такі як ізоморфізм графів або розфарбування графу в три кольори. Існують різні типи ZKP систем:

- **Інтерактивні ZKP:** Вимагають декількох раундів взаємодії між П та В.

- **Неінтерактивні ZKP (NIZK):** Доведення є єдиним повідомленням від П до В, яке може бути перевірене без подальшої взаємодії. Часто потребують спільної довіреної початкової настройки (Common Reference String - CRS) або використання евристики Фіата-Шаміра
citefiat1986how.

- **Сигма-протоколи (Σ-протоколи):** Ефективний клас трираундових інтерактивних протоколів типу "запит-відповідь-виклик що використовуються для доведення знання секрету, пов'язаного з публічним значенням (напр., доведення знання дискретного логарифму в протоколі Шнорра
citeschnorr1991efficient).

У контексті даної роботи ZKP є ключовим інструментом для побудови схем *верифікованого шифрування*. Вони дозволяють Доводжувачу (наприклад, тому, хто зашифрував дані) довести Перевіряючому (наприклад, отримувачу або аудитору) певні властивості без необхідності розшифрування:

- Доведення того, що даний шифротекст c є коректним шифротекстом *деякого* повідомлення m відповідно до правил криптосистеми та публічних параметрів.

- Доведення того, що зашифроване повідомлення m (приховане в c) задовольняє певну властивість (наприклад, $m > 0$, m належить до певної множини значень тощо).

Це досягається шляхом формулювання твердження про коректність шифрування або властивість повідомлення як мови L та використання відповідного ZKP протоколу. Викликом є розробка ZKP, ефективних для специфічної алгебраїчної структури запропонованої криптосистеми, яка базується на операціях у скінченних кільцях та розв'язанні систем лінійних рівнянь над ними (див. Розділ 4.2).

1.5.2 Інтерактивні докази (Interactive Proofs - IP)

Інтерактивні системи доведення (IP) формалізують поняття доведення як процес взаємодії між двома сторонами: всемогутнім **Доводжувачем (Prover, П)**, який намагається переконати, та ймовірнісним поліноміально-часовим **Перевіряючим (Verifier, В)**, який перевіряє істинність твердження. Модель IP, введена в роботах citebabai1985trading, goldwasser1989knowledge, узагальнює класичний клас NP, дозволяючи взаємодію та випадковість з боку Перевіряючого.

Нехай L – деяка мова (множина тверджень). Інтерактивний протокол (P, V) для L має задовольняти дві основні властивості:

- **Повнота (Completeness):** Якщо твердження x є істинним (
(x $\in L$
)), P, взаємодіючи з чесним Перевіряючим V, переконає V прийняти x з високою ймовірністю (традиційно, $\geq 2/3$ або $1 - \epsilon$ для незначного ϵ).

- **Обґрунтованість (Soundness):** Якщо твердження x є хибним (
(x $\notin L$
)), $(i)P^*$ не зможе переконати чесного Перевіряючого V прийняти x, крім як з малою ймовірністю (традиційно, $\leq 1/3$ або δ для незначного δ).

На відміну від ZKP, стандартна модель IP не вимагає нульового розголошення; Перевіряючий може отримати додаткову інформацію під час взаємодії.

Визначним результатом теорії складності є теорема **IP = PSPACE** citeshamir1992ip. Вона встановлює еквівалентність між класом мов, що мають інтерактивні системи доведення, та класом PSPACE – мов, що розпізнаються детермінованою машиною Тьюрінга з використанням поліноміального обсягу пам'яті. Це показує, що інтерактивність та випадковість надають Перевіряючому значну потужність, дозволяючи йому ефективно (за поліноміальний час) перевіряти твердження, розв'язання яких може вимагати значно більших ресурсів (поліноміальна пам'ять, потенційно експоненційний час).

Ця властивість робить IP важливим інструментом для верифікації обчислень. Наприклад, якщо Доводжувач виконав складне обчислення (скажімо, в рамках PSPACE), він може використати IP протокол, щоб довести коректність результату поліноміальному Перевіряючому без необхідності для Перевіряючого повторювати все обчислення. Це має застосування у:

- Верифікації аутсорсингових обчислень.
- Побудові доказів коректності виконання криптографічних протоколів.
- Перевірці властивостей, що вимагають складних обчислень.

У контексті даної роботи, IP-системи можуть розглядатися як потенційний інструмент для верифікації операцій, пов'язаних із запропонованою криптосистемою на кільцях, наприклад, доведення коректності певних етапів шифрування або розшифрування, особливо якщо ці етапи включають складні алгебраїчні маніпуляції над кільцями. Можливість їх інтеграції досліджується в Розділі 4.3.

1.5.3 Ймовірнісно перевірювані докази (Probabilistically Checkable Proofs - PCP)

Ймовірнісно перевірювані докази (PCP) представляють інший погляд на ефективну верифікацію математичних доведень. На відміну від інтерактивних доказів, де Перевіряючий взаємодіє з Доводжувачем, у моделі PCP доведення π розглядається як статичний рядок (потенційно дуже довгий), який Перевіряючий може запитувати у певних позиціях. Головна ідея полягає в тому, що Перевіряючий може перевірити коректність доведення (і, відповідно, істинність твердження $x \in L$), прочитавши лише *невелику кількість* (часто константну або полілогарифмічну від розміру твердження) випадково обраних бітів доведення π

citearora1998probabilistic, arora1998proof.Формально, мова L належить до класу PCP$(r(n), q(n))$, якщо існує ймовірнісний поліноміально-часовий Перевіряючий (Verifier), який для будь-якого входу x довжини n та доведення π робить наступне:
beginitemize
item Використовує не більше $r(n)$ випадкових бітів.
item Читає не більше $q(n)$ бітів доведення π (в позиціях, що залежать від x та випадкових бітів).
item Задовольняє умови:
beginitemize
item

textbfПовнота: Якщо $x \in L$, то існує доведення π таке, що Перевіряючий завжди приймає.
item
textbfОбґрунтованість: Якщо $x \notin L$, то для будь-якого доведення π^* Перевіряючий приймає з ймовірністю не більше $1/2$ (або іншої константи < 1).
enditemize
enditemizeФундаментальним результатом є **Теорема PCP**: кожна мова в класі NP має ймовірнісно перевірювані докази, де Перевіряючий використовує $O($
$logn)$
$)iiiO(1)$
$)(ii)ii., * * NP = PCP(O($
$logn), O(1)$
$)) * *.$
$citearora1998probabilistic, arora1998proof.iiii, ii :$
$beginitemize$
$item$
$textbfii :PCPiii'iNP - ii.$
$item$
$textbfii :, - NP - ii(i), i, i.iii(PCP -).$
$item$
$textbf'NIZK :PCP - , ii(, i - i), iii(NIZK), NP - .$
$enditemizePCP{-}iii, iii(, zk{-}SNARKs, zk{-}STARKs), ii, PCP{-}i, i/iii.ii4.3iiPCPii, 'i.$

1.5.4 Верифіковане шифрування (Verifiable Encryption)

Верифіковане шифрування (ВШ) – це криптографічний примітив, який поєднує шифрування даних з можливістю доведення певних властивостей цих даних (або самого процесу шифрування) без їх розшифрування. Ідея полягає в тому, щоб створити шифротекст c повідомлення m разом із доказом π, який переконує перевіряючого в істинності деякого твердження $\phi(m, c, k, ...)$ про відкритий текст, шифротекст, ключ або інші параметри, не розкриваючи при цьому сам відкритий текст m (або іншу конфіденційну інформацію)
citecamenisch2007verifiable, verifiable$_e ncryption_o verview$.

Формально, схема ВШ зазвичай включає стандартні алгоритми шифрування (Gen, Enc, Dec) та додаткові алгоритми, пов'язані з доведенням:
beginitemize
item
textbfProveEnc(k, m, r): Алгоритм, який генерує шифротекст $c = \text{Enc}_k(m; r)$ (де r – випадковість) та доказ π, що c є коректним шифруванням m з використанням випадковості r.
item
textbfVerifyEnc(pk, c, π): Алгоритм, який перевіряє, чи є π дійсним доказом для шифротексту c (з використанням публічного ключа pk в асиметричному випадку або публічних параметрів у симетричному).
item
textbfProveProp(k, m, r, ϕ): Алгоритм, який генерує доказ π', що відкритий текст m, зашифрований у $c = \text{Enc}_k(m; r)$, задовольняє властивість ϕ (наприклад, $\phi(m) \equiv m > 0$).

item
textbfVerifyProp(pk, c, ϕ, π'): Алгоритм, який перевіряє, чи є π' дійсним доказом того, що відкритий текст, зашифрований у c, задовольняє ϕ.
enditemize Ці алгоритми доведення часто використовують техніки ZKP або NIZK для забезпечення конфіденційності відкритого тексту.

Основні властивості, яких вимагають від схем ВШ:
beginitemize
item
textbfКоректність шифрування та верифікації: Стандартні вимоги коректності для шифрування та доказів (повнота).
item
textbfБезпека шифрування: Шифротекст не повинен розкривати інформацію про відкритий текст (наприклад, IND-CPA або IND-CCA безпека).
item
textbfОбґрунтованість доказів (Soundness): Неможливо створити переконливий доказ для хибного твердження.
item
textbfНульове розголошення (Zero-Knowledge / Privacy): Докази не повинні розкривати інформацію про відкритий текст, крім тієї, що випливає з самого твердження ϕ.
enditemize

Існуючі підходи до побудови ВШ часто базуються на:
beginitemize
item
textbfКриптографії на основі спарювань (Pairing-based cryptography): Дозволяє будувати елегантні та відносно ефективні схеми ВШ, особливо для асиметричного випадку, використовуючи властивості білінійних відображень

citeboneh2004short.
item
textbfКриптографії на основі ґраток (Lattice-based cryptography): Пропонує постквантові рішення для ВШ, часто використовуючи задачі LWE/Ring-LWE та відповідні ZKP/NIZK системи

citegentry2013homomorphic.
item
textbfЗагальних конструкціях ZKP: Можна комбінувати будь-яку схему шифрування (симетричну чи асиметричну) з загальною ZKP системою (напр., zk-SNARK/STARK), яка доводить твердження про процес шифрування або властивості відкритого тексту, представлені у вигляді арифметичної схеми або іншої відповідної моделі обчислень.
enditemize

Дана робота в Розділі 4 досліджує можливість побудови верифікованого шифрування шляхом комбінації *запропонованої симетричної криптосистеми* на скінченних кільцях з техніками ZKP/IP, що є відмінним від найбільш поширених підходів на спарюваннях чи ґратках.

2 Запропонована симетрична криптосистема на основі кілець

2.1 Формальне визначення криптосистеми

2.2 Побудова базових алгебраїчних структур

2.2.1 Генерація ізоморфних кілець G_k

2.2.2 Алгоритм GEN-G: детальний опис та аналіз

2.2.3 Побудова ізоморфізму $\varphi : G_k \to Z_m$

2.3 Використання сюр'єктивних відображень та систем рівнянь

2.3.1 Визначення та властивості відображень ψ та λ

2.3.2 Побудова бієкцій ψ_1 та λ_1

2.3.3 Роль систем лінійних рівнянь

2.4 Протокол обміну повідомленнями

2.4.1 Етап генерації ключів та параметрів

2.4.2 Формування публічних та секретних даних (Аліса)

2.4.3 Процес шифрування (Боб)

2.4.4 Процес розшифрування (Аліса)

2.5 Ілюстративний приклад роботи системи

3 Аналіз безпеки та ефективності базової криптосистеми

3.1 Аналіз стійкості до основних криптоатак

3.1.1 Атака повного перебору (ключового простору)

3.1.2 Атака на основі відомого відкритого тексту (KPA)

3.1.3 Атака на основі обраного відкритого тексту (CPA)

3.1.4 Атака на основі обраного шифротексту (CCA)

3.1.5 Алгебраїчні атаки

3.1.6 Роль секретності відображень φ, ψ, λ

3.2 Оцінка обчислювальної ефективності

3.2.1 Складність генерації ключів та параметрів

3.2.2 Складність шифрування та розшифрування

3.2.3 Розмір ключів та шифротексту (коефіцієнт розширення)

3.3 Порівняльний аналіз

3.3.1 Порівняння з класичним OTP

3.3.2 Порівняння з іншими симетричними шифрами

3.3.3 Переваги та недоліки запропонованого підходу

3.4 Обмеження та потенційні вразливості

4 Розширення та Застосування: Верифіковане Шифрування

4.1 Мотивація та постановка задачі верифікованого шифрування

4.2 Інтеграція з Доведеннями з Нульовим Розголошенням (ZKP)

4.2.1 Огляд ZKP систем, потенційно сумісних з арифметикою кілець

4.2.2 Протокол ZKP для доведення коректності шифрування

4.2.3 Протокол ZKP для доведення властивостей зашифрованих даних

4.3 Використання Інтерактивних Доказів (IP) та PCP

4.3.1 Застосування IP для верифікації обчислень над шифротекстом

4.3.2 Потенціал PCP для неінтерактивної верифікації

4.4 Побудова схеми верифікованого шифрування

4.4.1 Комбінування симетричної схеми та ZKP/IP

4.4.2 Аналіз безпеки та ефективності верифікованої схеми

4.5 Обговорення та відкриті питання

Висновки