

АНАЛІЗ ВРАЗЛИВОСТЕЙ КРИВИХ ЯК КРИПТОГРАФІЧНИХ ПРИМІТИВІВ

Вінницький національний технічний університет;

Анотація У роботі наведено актуальність захисту чутливих даних із використанням криптографії на базі полів Галуа, що утворюються за допомогою кривих. Проаналізовано основні атаки та шляхи їх усунення для кривих у формі Монтеґомері, кривих Едвардса та кручених кривих Едвардса. Наведено результати аналізу, які формалізовано як таблицю з метою покращення сприйняття інформації. На основі цих результатів порівняльного аналізу зроблено висновок щодо вибору кривої для подальшої розробки та досягнення мети із захистом цілісності, доступності та конфіденційності чутливих даних.

Ключові слова: криптографія, еліптичні криві, криві Едвардса, кібербезпека, вразливість, чутливі дані.

Abstract The paper highlights the relevance of sensitive data protection using elliptic curve cryptography. It analyzes the main attacks and methods of mitigating them for Montgomery curves, Edwards curves, and twisted Edwards curves. The results of the analysis are presented, and a table is provided to enhance the comprehension of the information. Based on these comparative analysis results, a conclusion is drawn regarding the selection of the curve for further development to achieve the goals of protecting the integrity, availability, and confidentiality of sensitive data.

Keywords: cryptography, elliptic curves, Edwards curves, cybersecurity, vulnerability, sensitive data.

Вступ

Проблема забезпечення кібербезпеки на основі криптографічних примітивів набуло особливої актуальності. Вразливості криптографічних примітивів можуть призвести до критичних наслідків, зокрема компрометації приватних ключів, розкриття конфіденційної інформації або навіть підриву безпеки сучасних протоколів зв'язку.

Еліптичні криві широко застосовуються в сучасній криптографії завдяки своїй адаптивності та високому рівню стійкості. Однак, попри їхні переваги, існує низка недоліків, серед них – атаки на криві, які можуть загрожувати безпеці криптографічних алгоритмів на основі еліптичних кривих. Серед них можна виділити атаки на основі побічних каналів, атаки на підбір дискретного логарифма та специфічні атаки, пов'язані з вибором параметрів кривих [1, 2].

Метою цього дослідження є покращення захисту конфіденційності чутливих даних, шляхом вибору відповідної кривої, на основі якої буде зашифровано чутливі дані, з метою унеможливлення їх подальшої модифікації.

Для досягнення мети необхідно розв'язати такі задачі:

- проаналізувати криві, які є підвидами еліптичних;
- проаналізувати можливі вразливості;
- виконати порівняльний аналіз;
- зробити відповідні висновки.

Результати дослідження

Криптографія на еліптичних кривих широко використовується у сфері цифрової безпеки, забезпечуючи захист інформації завдяки складності розв'язання задачі дискретного логарифмування на еліптичних кривих. Ця математична проблема є обчислювально складною, що унеможливорює її швидке вирішення за допомогою класичних алгоритмів, забезпечуючи високий рівень криптографічного захисту.

Однак, попри високу криптостійкість кривих, реалізація може бути вразливою до низки атак, зокрема атака побічних каналів [1], атак з використанням некоректних даних [1] та атак із використанням малих підгруп [1]. Ці методи можуть використовувати недоліки програмного чи апаратного за-

безпечення для компрометації системи.

Атаки побічних каналів використовують непрямі витoki інформації, що виникають під час роботи криптографічної системи, зокрема через аналіз часу обчислень, рівень енергоспоживання або електромагнітні сигнали [1]. Наприклад, якщо час виконання певних операцій залежить від значень секретного ключа, зломисник може проаналізувати ці відмінності та відновити конфіденційні дані. Щоб запобігти таким атакам, необхідно застосовувати алгоритми з рівномірним часом обчислення, спеціальні методи маскуванню даних та фізичні засоби захисту апаратного забезпечення.

Атаки на малі підгрупи виникають, коли в реалізації еліптичної криптографії не перевіряється порядок точок на кривій [1]. Зломисник може скористатися наявністю малих підгруп, щоб поступово отримати інформацію про закритий ключ. Для захисту необхідно перевіряти порядок вхідних точок та використовувати криві з простим порядком або коефіцієнтом співмножника, що дорівнює 1.

Атаки через навмисне спотворення даних спрямовані на внесення помилок у процес обчислень еліптичної криптографії, наприклад, під час множення точок, щоб отримати відомості про закритий ключ [1]. Один із варіантів такої атаки є зміна знаку координати точки, що дозволяє зломиснику відстежувати зміни у вихідних значеннях і таким чином виявити конфіденційну інформацію. Захист включає виявлення та виправлення помилок, випадкове модифікування проміжних обчислень, а також фізичні заходи для запобігання зовнішньому втручання.

У цьому дослідженні було розглянуто детальніше вразливості та шляхи їх усунення для трьох видів кривих, серед яких:

- криві у формі Монтгомері [3,4];
- криві Едвардса [3,4];
- кручені криві Едвардса [3,4].

Результати аналізу представлені у вигляді таблиці (табл.1).

Таблиця 1 – Результати порівняння кривих

Назва кривої	Формула	Вразливість	Шляхи вирішення проблеми	Можливе застосування
Крива у формі Монтгомері	$by^2 = x^3 + ax^2 + x$	Вразлива до атак через спотворення обчислень, атак на малі підгрупи та аналіз часу виконання операцій [1].	Реалізація алгоритмів із постійним часом виконання, фізичний захист пристроїв.	Криптографічні протоколи, зокрема ECDH (Curve25519) [3,4].
Крива Едвардса	$x^2 + y^2 = 1 + dx^2y^2$	Можливі атаки через витік інформації при побічних каналах та атаки на некоректні параметри кривої [1].	Використання випадкових маскувань, перевірка коректності параметрів.	Цифрові підписи (Ed25519), криптографічні протоколи з високою продуктивністю [3,4].
Кручена крива Едвардса	$ax^2 + y^2 = 1 + dx^2y^2$	Вразливість до атак через неправильну перевірку параметрів та можливі атаки побічних каналів [1].	Додаткові перевірки коректності точок, випадкове модифікування проміжних обчислень, застосування методів виявлення та виправлення помилок.	Криптографічні системи, що потребують високої швидкості [3,4].

Як видно з таблиці 1 криві як криптографічний примітив мають спільну вразливість — залежність часу обчислень від значень вхідних/ключових даних, що обумовлює можливість атак побічних каналів. Водночас формалізований опис кривих дозволяє проводити їх дослідження та наводити математичні доведення щодо стійкості кривих із заданими параметрами, що підвищує довіру до таких криптографічних примітивів. З-поміж проаналізованих в таблиці 1 кривих доцільно використовувати кручені криві Едвардса, завдяки своїй швидкості обчислень порівняно з еліптичними кривими у формі Монтгомері. Крім того, очікувана потужність множини прийнятих для криптографічного застосування кручених кривих Едвардса переважає множину аналогічних кривих Едвардса.

Висновки

Таким чином, для розв'язання задачі захисту чутливих даних найбільш доцільним вибором є кручена крива Едвардса. Це пов'язано з кількома важливими перевагами цієї кривої порівняно з іншими типами кривих. Вона має високу швидкодію завдяки спрощеній та ефективній арифметиці, що дозволяє значно зменшити час виконання криптографічних операцій.

Окрім того, кручена крива Едвардса є достатньо гнучкою для застосування в різних криптографічних протоколах, що дає змогу забезпечити як високу безпеку, так і ефективність обчислень у реальному часі.

Отже, використання кручених кривих Едвардса є найбільш доцільним для сучасних криптографічних систем, що обробляють великі об'єми чутливих даних, оскільки це дозволяє забезпечити високий рівень захисту при найменших витратах ресурсів порівняно з іншими розглянутими кривими.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Security of Elliptic Curve Cryptosystems. URL: <https://library.fiveable.me/elliptic-curves/unit-3/security-elliptic-curve-cryptosystems/study-guide/Jga76VareEagtVsI> (дата звернення: 04.02.2025).
2. Briański M. Attacks on cryptosystems based on elliptic curves : licentiate thesis. URL: <https://ruj.uj.edu.pl/xmlui/handle/item/221737> (дата звернення: 04.02.2025).
3. Dusane, Tanay Pramod, "Generation, Verification, and Attacks on Elliptic Curves and their Applications in Signal Protocol" (2021). Thesis. Rochester Institute of Technology. URL: <https://repository.rit.edu/cgi/viewcontent.cgi?article=11856&context=theses> (дата звернення: 04.02.2025).
4. Lange T. Edwards Curves. Encyclopedia of Cryptography and Security. Boston, MA, 2011. P. 380–382. Doi: 10.1007/978-1-4419-5906-5_243 (дата звернення: 04.02.2025).

Баришев Юрій Володимирович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: yuriy.baryshev@vntu.edu.ua.

Ланова Владислава Сергіївна — студентка групи ІБС-24м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: lanovaia02y@gmail.com

Yurii Baryshev — PhD (eng), associated professor of information protection department, Vinnytsia National Technical University, Vinnytsia, email: yuriy.baryshev@vntu.edu.ua

Vladyslava Lanova — student of ІБС-24m group, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : lanovaia02y@gmail.com.