КРИПТОГРАФІЯ

ВИКОРИСТАННЯ ВІДБИТКА ПАЛЬЦЯ ДЛЯ КРИПТОСИСТЕМ НА ЕЛІПТИЧНИХ КРИВИХ

Валеріян Швець[1], Віолета Шестакова[2]

[1]Національний авіаційний університет
[2]ТОВ "ІТ Інновації Україна"

Швець Валеріян Анатолійович, к.т.н., доцент

Рік та місце народження: 1959 рік, с. Окниця, Молдова.
Освіта: Київський інститут інженерів цивільної авіації (з 2000 року – Національний авіаційний університет), 1986 рік.
Посада: завідувач кафедри засобів захисту інформації з 2004 року.
Наукові інтереси: цифрова обробка сигналів, біометрика, інформаційна безпека.
Публікації: понад 60 наукових публікацій, серед яких монографії, підручники, навчальні посібники, наукові статті та патенти на винаходи.
E-mail: hvan@nau.edu.ua

Шестакова Віолета Володимирівна

Рік та місце народження: 1981 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2004 рік.
Посада: спеціаліст з розробки програм в ТОВ "ІТ Інновації Україна".
Наукові інтереси: криптографія, біометрика, інформаційна безпека.
Публікації: більше 10 наукових публікацій, серед яких підручники, наукові статті.
E-mail: vio-shestakova@ukr.net

Анотація. *У даній статті запропоновано використання відбитків пальця як первинного джерела для криптографічних систем на еліптичних кривих, а також методи виявлення характерних фрагментів на відображенні відбитків пальця.*

Ключові слова: *криптографія, еліптичні криві, відбитки пальця, апроксимація, інтерполяція.*

Вступ

В останні роки криптосистеми, ґрунтовані на еліптичних кривих (технологія ECC - Elliptic Curve Cryptography), знаходять ширше застосування в порівнянні з класичними криптосистемами. Вдосконаленням цієї технології займаються такі організації по стандартизації, як NIST (National Institute of Standards and Technology - Національний інститут стандартів і технологій), IEEE (Institute of Electrical and Electronics Engineers - Інститут інженерів по електротехніці і електроніці), ANSI (American National Standards Institute - Національний інститут стандартизації США) ANSI(American National Standards Institute – Національний інститут стандартизації США) і інші.

Одна з областей теорії чисел і геометрії алгебри - теорія еліптичних кривих над кінцевими полями - знайшла застосування в сучасній криптографії. Головна причина цього полягає в тому, що еліптичні криві (ЕК) над кінцевими полями надають практично невичерпне джерело кінцевих абелевих груп, які зручні для обчислень і мають багату структуру [1].

Криптосистеми на еліптичних кривих відносяться до класу криптосистем з відкритим ключем. Їх безпека, як правило, заснована на труднощі розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої над кінцевим полем. Цим і зумовлена їх висока криптостійкість в порівнянні з іншими алгоритмами. Існують стійкі криптоалгоритми на ЕК, засновані на труднощі розкладання великих цілих чисел, коли ЕК задається над кінцевим кільцем по складеному модулю, але вони зустрічаються досить рідко. Однак слід зазначити, що крипостійкість є відносним поняттям, пов'язаним з поняттям найкращого відомого алгоритму злому системи. Стосовно криптосистемам на ЕК це алгоритми Сільвера-поліг-Хеллмана, Полларда і деякі інші. При відсутності деяких відомостей про ЕК (секретного ключа) ці алгоритми виконуються за експоненціальний час.

Крім того, за час що минув з моменту перших публікацій про криптосистеми на ЕК (1985-1986 рр. Н. Коблиц, В. Міллер), помітного падіння стійкості алгоритмів на ЕК не відбулося. У той час як, стійкість системи RSA, заснованої на задачі розкладання на множники, знижувалася приблизно на порядок в рік. Все це свідчить про високу криптостійкости алгоритмів на ЕК. Криптосистеми на ЕК можна ефективно використовувати для систем цифрового підпису та ключового обміну. Вже існує попередній стандарт ANSI X9.62, який пропонує розробникам принципи створення потужних систем цифрового підпису на основі використання ЕК. Зауважимо, що безпека таких систем цифрового підпису спирається не тільки на стійкість алгоритму на ЕК, а й на стійкість використовуваної хеш-функції. Не варто забувати і про вимоги до генератора випадкових чисел. І все ж, на сьогоднішній день криптосистеми на ЕК є найбільш перспективними асиметричними крипто-системами.

У багатьох відношеннях ЕК є природним і зручнішим аналогом мультиплікативних груп полів, оскільки вибір ЕК характеризується більшою свободою, ніж вибір кінцевого поля. Еліптичні криві описуються кубічними рівняннями, загальний вигляд яких :

$$y^2 + axy + by = x^3 + cx^2 + dx + e, \qquad (1)$$

де a, b, c, d і e є дійсними числами, що задовольняють деяким простим умовам.

Для використання еліптичної криптографії не обходимо задати набір параметрів, що визначають еліптичну криву, тобто набір параметрів криптографічного протоколу. Еліптична крива визначається константами і з рівняння (1).

При знаходженні кривої для заданого набору параметрів використовуються два методи: вибрати випадкову криву, потім скористатися алгоритмом підрахунку точок; вибрати точки, після чого побудувати криву по цим точкам, використовуючи техніку множення.

Традиційно джерелом для генерування ключів криптосистем на ЕК застосовувався генератор випадкових чисел. Але в якості джерела можна застосовувати біометричні системи.

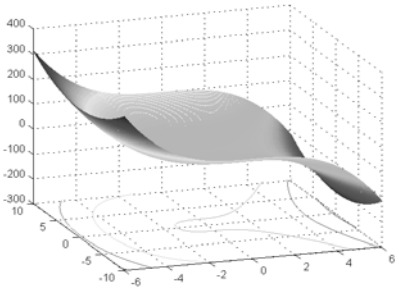
Аналіз існуючих досліджень

У науковій літературі джерелом для генерування ключів криптосистем на ЕК застосовувався генератор випадкових чисел і відсутні відомості про інші первині датчики. Однак біометричні ознаки людини є особливими і унікальними, тому в якості первинних джерел можливо використання біометричних систем.

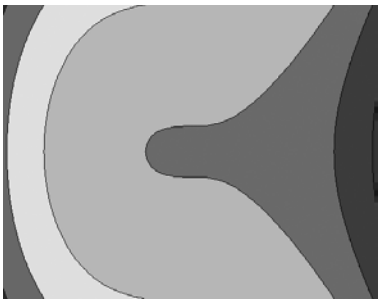
Метою даної роботи запропонувати рішення щодо використання відбитків пальця як первинного джерела для криптосистем на ЕК.

Основна частина дослідження

Для прикладу побудуємо графік ЕК заданої рівнянням $y^2 = x^3 + 3$.



а)



б)

Рис. 1. Графік ЕК а) і її контурна поверхня на площину XY б)

Наведемо відбиток пальця який отримано зі сканеру.

Рис. 2. Зображення відбитка пальця

Якщо розглянути папілярний малюнок відбитка і графік ЕК (рис 1. б), можна сказати, що папілярні лінії можуть описуватися ЕК з деяким набором параметрів. Таким чином за відбитком пальця можна згенерувати будь-який набір точок. Відбиток пальця завжди надійніше, його не втратиш, не запишеш в записну книжку, і пам'ятати, отриманий за відбитком пальця набір немає потреби. Тобто одним з джерел при знаходженні ЕК може служити відбиток пальця, що використовується в біометричних технологіях.

Для використання відбитка пальця в криптосистеми потрібно вирішити ряд завдань:

- перетворити зображення відбитка пальця з відтінків сірого в двох кольорове чорно-біле зображення;
- провести обробку зображення, усунути окремі точки і розриви в папілярному малюнку;
- перетворити папілярні лінії до товщини в 1 піксел;
- виділити характерний фрагмент на відбитку;
- апроксимувати цей фрагмент і знайти рівняння ЕК;
- інтерполювати в цілих числах ЕК і згенерувати ключ.

При повторному скануванні відбитка пальця і виконанні аутентифікації та ідентифікації користувача і підтвердження ключа додається ще ряд завдань:

- інтерполяція в цілих числах і відновлення зображення фрагмента;
- виявлення та прийняття рішення про автентичність фрагменту і підтвердження ключа.

При вирішенні цих завдань будемо використовувати бібліотеку обробки зображень пакета MatLab (IPT).

Ефективно видаляти шуми на зображенні можна використовуючи операцію замикання [2], яка являє собою ерозію, застосовану до результату дилатації:

$$A \cdot B = (A \oplus B) \ominus B ,$$

і розмикання, яка визначається як ерозія A по B, після якої виконується дилатація результату по B:

$$A \circ B = (A \ominus B) \oplus B .$$

У результаті цих дій були вилучені всі точки, що заважають і усунені розриви в папілярних лініях, таким чином отримано оброблений відбиток пальця (рис. 3).

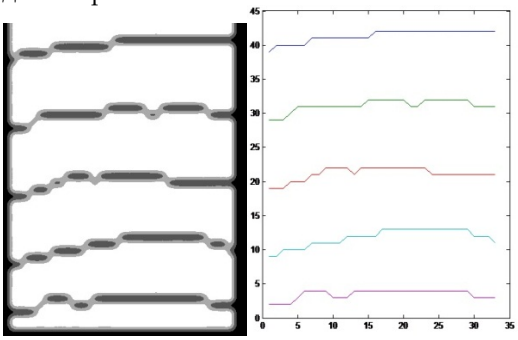
Рис. 3. Оброблений відбиток пальця

Для стоншення папілярних ліній застосуємо функцію *bwmorph* з бібліотеки IPT, ця функція скорочує двійкові об'єкти або форми зображення до окремих ліній, які мають товщину всього в один піксель (рис. 4).

Рис. 4. Стоншений та інвертований відбиток пальця

Таким чином, отримано зображення відбитка пальця, яке може використовуватися як джерело для вибору ЕК.

Виберемо на відбитку фрагмент (рис. 5. а.) і проведемо його апроксимацію, за отриманими точкам в цілих числах інтерполюем ЕК. Результат інтерполяції наведено на рис. 5. б.



а) б)

Рис. 5. Фрагмент відбитку пальця а), результат інтерполяції б)

На рисунку видно повний збіг фрагменту відбитка пальця і обчислених ЕК, тобто маємо відбиток пальця можемо обчислити безліч ЕК, або вибираємо папілярну лінію і підраховуємо точки ЕК.

При повторному скануванні в точності повторити відбиток пальця неможливо, проте можна повторити не сам відбиток, а його фрагменти, як би не був зрушений відбиток, а папілярний малюнок не зміниться. Тоді необхідно вирішити задачу виявлення копії еталонного фрагмента на відбитку пальця. В якості еталонного фрагмента візьмемо зображення, отримане в результаті інтерполяції ЕК (рис. 5 б). Розглянемо два методи виявлення розташування фрагмента на знову введеному відбитку**.**

"Метод пошуку збігів". Будемо "протягати" виділений фрагмент по всій матриці і підраховувати кількість збігів (розбіжностей) чорно-білих точок. Якщо всі крапки збігаються, то розбіжностей в ідеалі буде 0.

Кількість розбіжностей відобразимо у вигляді графіка (рис.6). З рис. 6 видно, що є чіткий мінімум, а це означає, що в другій матриці відбитка присутній еталонний фрагмент першої матриці. Тобто можна провести аутентифікацію і підтвердити генерацію ключа. Другий метод, який можна використовувати - знаходження більш складної залежності між двома відбитками, наприклад знаходження кореляційної функції еталонного фрагмента на другому відбитку пальця, який можна назвати **"кореляційно-координатний метод"** (рис. 7.).

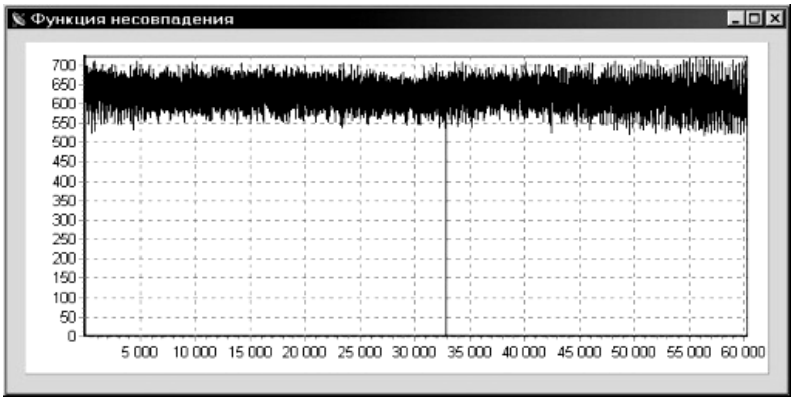


Рис. 6. Графік розбіжності фрагментів.

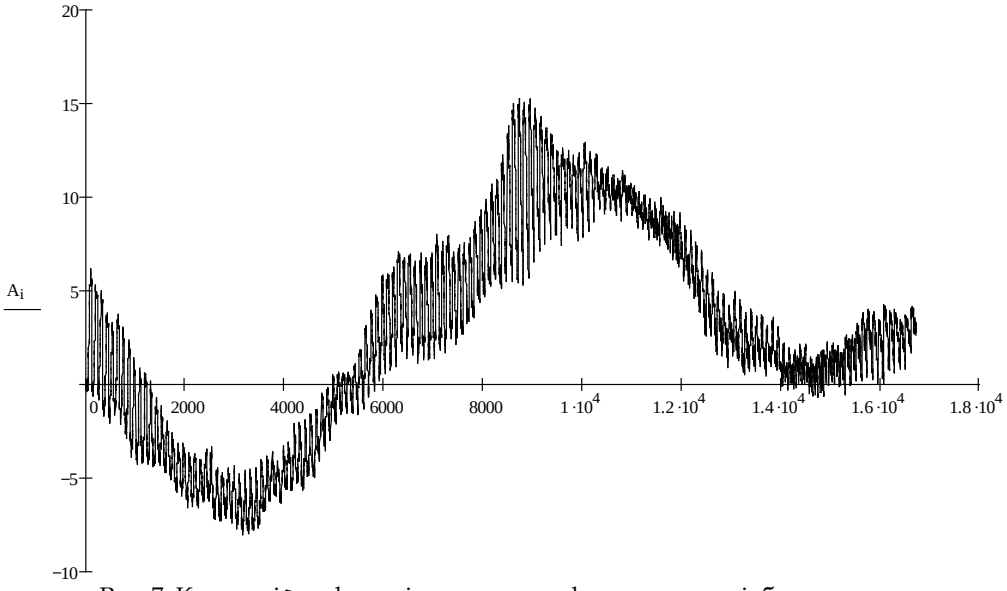


Рис. 7. Кореляційна функція еталонного фрагменту на відбитку пальця

Максимум кореляційної функції вказує на наявність еталонного фрагмента в відбитки пальця введеного другий раз.

Аналізуючи отримані результати можна стверджувати, що обидва методи можуть мати практичне використання для виявлення характерних фрагментів на відбитках пальців введених кілька разів. Хочеться зауважити, що "метод пошуку збігів" більш точний і чутливий по відношенню до "кореляційно-координатного методу".

Використовуючи перший можна обчислювати координати розташування фрагмента на зображенні відбитка та інші параметри, в той час як максимум кореляційної функції не має явно вираженого максимуму, тому використовуючи його можна судити лише про наявність еталонного фрагмента на іншому відбитку.

Висновки

Запропоновані рішення показують можливість використання відбитків пальця як первинного джерела для криптосистем на ЕК

При обробці відбитка пальця можна отримати набір точок для розрахунку ЕК. Після виявлення фрагмента відбитка пальця провести аутентифікацію і генерацію ключів з використанням апарату еліптичних кривих.

Література

[1] Алгоритмические основы эллиптической криптографии / А. А. Болотов, С. Б. Гашков, А. Б. Фролов и др. – М.: МЭИ, 2000. – 100 с.

[2] Цифровая обработка изображений в среде MATLAB / Р. Гонсалес, Р. Вудс, С. Эддинс – М.: Техносфера, 2006. – 616 с.

УДК 651.928 (045)

Швец В. А., Шестакова В. В. Использование отпечатка пальца для криптосистем на эллиптических кривых

Аннотация. *В данной статье предложено использование отпечатков пальца качестве первичного источника для криптографических систем на эллиптических кривых, а также методы выявления характерных фрагментов на изображении отпечатков пальца.*

Ключевые слова: *криптография, эллиптические кривые, отпечатки пальцев, аппроксимация, интерполяция.*

Shvets V. A., Shestakova V. V. Using the fingerprint to the elliptic curve cryptosystems

Abstract. *In this paper proposed the use of fingerprints as the primary source for cryptographic systems on elliptic curves, as well as methods for detection of characteristic fragments reflecting fingerprints.*

Keywords: *cryptography, elliptic curves, fingerprints, approximation, interpolation.*

Отримано *5 квітня 2012 року*, затверджено редколегією 07 *червня 2012 року*
(рецензент к.т.н., доц. В. Ю. Ковтун)