# АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ПЕРЕТВОРЕНЬ В ГРУПІ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ

Уманець М.С.
Науковий керівник – асистент Євгеньєв А.М.
Харківський національний університет радіоелектроніки
61166,Харків,просп.Науки,14,каф.БІТ,тел.(057)702-14-25
e-mail:mariia.umanets@nure.ua

This paper covers relatively new and emerging subject of the elliptic curve crypto systems which fundamental security is based on the algorithmically hard discrete logarithm problem.It presents a comparative analysis of RSA and ECC. Cryptosystems based on elliptic curves emerge as an alternative to the RSA cryptosystems. The security of the RSA cryptosystem is based on the integer factorization problem (IFP) whereas the security of ECC is based on the EC discrete logarithm problem (ECDLP).The experimentation was conducted for finding time lapse during encryption, decryption by RSA and ECC.The conclusion contains a brief summary of the elliptic curve cryptosystem practical applications, the potential practical benefits and disadvantages of ECC.

Комп'ютерні системи активно впроваджуються у всі сфери нашого життя. Внаслідок цього значно збільшився інтерес користувачів до проблем захисту інформації. Проблему передачі деякої конфіденційної інформації адресату можна вирішити за допомогою асиметричних криптосистем.

Широке використання еліптичних кривих (далі ЕК) в криптографії засновано на такій властивості, що завдання дискретного логарифмування (далі ДЛ) на ЕК є більш трудомістким, ніж завдання ДЛ в скінчених полях. Через низку успішних атак на системи, основані на складності ДЛ в скінченних полях, деякі стандарти ЕЦП були переведені на ЕК. Криптосистеми на основі ЕК отримують все більше розповсюдження як альтернатива, а не заміна систем на основі RSA. Вони мають переваги при використанні в пристроях з малопотужними процесорами та / або маленькою пам'яттю.

Експоненціальні алгоритми для вирішення розв'язання задачі ДЛ в групі точок кривої: метод повного перебору, алгоритм Поліга-Сілвера-Хеллманна, алгоритм Шенкса, ρ-метод Полларда тощо.

Таблиця 1 – Порівняння ефективності метода ρ-Полларда та методу факторизації великих чисел за допомогою решета числового поля загального вигляду:

| Еліптична Криптографія | | RSA | |
|---|---|---|---|
| Довжина ключа | Час взлому(MIPS-роки) | Довжина ключа | Час взлому(MIPS-роки) |
| 150 | 3.8·10^10 | 512 | 3·10^4 |
| 205 | 7.1·10^18 | 768 | 2·10^8 |
| 234 | 3.8·10^28 | 1536 | 3·10^16 |

Аналізуючи дані, робимо висновок, що один і той самий рівень захисту досягається у випадку еліптичної криптографії при значно меншій довжини ключа.

Операція скалярного множення-аналог операції піднесення до степеня в кінцевому полі. Тому в еліптичній криптографії в ролі прямої задачі виступає скалярне множення точки кривої (розрахування Q =mP) Обернена задача має назву – дискретне логарифмування на еліптичній кривій, що формулюється таким чином: за відомими P та Q, знайти таке число m, для якого mP=Q. Стійкість шифрів визначається складністю розв'язання рівняння mP=Q відносно m, де точки P та Q належать одній циклічній підгрупі.

Класи криптографічно слабких кривих, яких слід уникати:

- криві над $GF(2^m)$ , де m – непросте число. Шифрування на таких кривих піддається атакам Вейля;
- криві над полем GF(q) із загальним числом точок $N_E = q$ вразливі для атаки, яка відображає точки даної кривої в адитивну групу поля;
- аномальні еліптичні криві над полем GF(q) коли загальне число точок на кривій $N_E = p$ , p – просте число;
- суперсингулярні еліптичні криві.

Криптоалгоритми на ЕК будуються аналогічно алгоритмам в простих кінцевих полях. Фактично піднесення до степеня за великим модулем, що визначає стійкість шифру, замінюється на скалярний добуток точки еліптичної кривої. Найбільш широко застосованими еліптичними аналогами систем з відкритим ключем є: аналоги відкритого розподілу ключів Діффі-Хеллмана (ECDH), системи Мессі-Омури, системи Ель-Гамаля.

У зв'язку з тим, що при використанні груп точок ЕК стійкість до криптоаналізу досить висока, з'являється можливість використовувати модулі перетворення менших розмірів, ніж при перетвореннях у полях та кільцях. Як показує аналіз, достатньо розміру модуля від $2^{192}$ та більше.

Як висновок, можна зазначити, що найближчим часом в якості направленого шифру будуть використовуватися алгоритми (схеми), реалізовані в групах точок на еліптичній кривій.

Список використаної літератури:

1.Жданов О. Методи криптографічного захисту інформації: навч. посіб. / О.Н Жданов, В.В Золотарев. – Красноярск: [б.в.], 2007. 254с.

2.Протоколы направленного шифрования в группах точек на эллиптических кривых и их свойства / Иван Горбенко, Станислав Збитнев, Андрей Поляков. [Б. м.]: НТУУ КПІ, 2001.

3.Урбанович П. Криптографічні методи захисту інформації / П.П Урбанович // Захист інформації методами криптографії, стеганографії та обфускації: навч. посіб. Мінськ, 2016. С. 58-91.