УДК 512.77:512.624.95
Циганенко О. – гр. 6.04.51.11.01
Харківський національний економічний університет імені Семена Кузнеця

ЕЛІПТИЧНА КРИПТОГРАФІЯ

Науковий керівник: к.т.н., доц. Євсеєв С. П.

Tsyhanenko O.
Simon Kuznets Kharkiv National University of Economics

ELLIPTIC CURVE CRYPTOGRAPHY

Supervisor: Ph.D., Associate Professor Evseev S.

Ключові слова: Еліптичні криві, Алгеброгеометричні коди, Еліптичні коди
Keywords: Elliptic Curve, Algebraic-geometrical codes , Elliptical codes

Засоби й системи криптографічного захисту інформації відіграють важливу роль в сучасних комп'ютерних інформаційних системах, що використовуються в сфері фінансової та комерційної діяльності. Інтерес до них обумовлений не тільки зростаючими суспільними потребами в перекладі економічних і державно-правових відносин на «електронну основу», але і сильно розширилися можливості передачі, обробки та зберігання інформації в розподілених обчислювальних системах. Застосування криптографічних протоколів та криптосистем дозволяє здійснювати різноманітні економічні відносини «дистанційно», виключаючи необхідність особистої зустрічі учасників цих відносин, а також підтримувати при цьому належну фінансову і правову дисципліну. До криптографічним протоколам відносять протоколи шифрування, електронного цифрового підпису (ЕЦП), ідентифікації та протоколи аутентифицированного розподілу ключів.

У 1985 році Ніл Коблиц та Віктор Міллер незалежно запропонували використовувати в криптографії деякі алгебраїчні властивості еліптичних кривих. З цього моменту почався бурхливий розвиток нового напряму в криптографії, для якого використовується термін криптографія на еліптичних кривих (Elliptic Curve Cryptography, скорочено ECC). Криптосистеми з відкритим ключем на еліптичних кривих забезпечують таку ж функціональність, як і алгоритм RSA. Проте їх крипостійкість заснована на іншій NP-повній задачі, а саме на проблемі дискретного логарифма в групі точок еліптичної кривої (Elliptic Curve Discrete Logarithm Problem, скорочено ECDLP). В даний час кращі алгоритми для вирішення ECDLP мають експоненціальне час роботи, на відміну від алгоритмів для вирішення проблеми простого дискретного логарифма і проблеми факторизації цілого числа, які мають субекспоненціальное час роботи. Це означає, що в системах на еліптичних кривих бажаний рівень безпеки може бути досягнутий при значно меншій довжині ключа, ніж, наприклад, у схемі RSA. Наприклад, 160-бітний ключ в ECC забезпечує той же рівень безпеки, що і 1024-бітний ключ в RSA [1].

Еліптична крива – це набір точок, описуються рівнянням Вейерштрассе: $y^2 = x^3 + ax + b$.

У криптографії розглядається два види еліптичних кривих: над кінцевим полем Z_p – кільце вирахувань по модулю простого числа. І над полем $GF(2^m)$ – бінарне кінцеве поле.

У еліптичних кривих над полем $GF(2^m)$ є одна важлива перевага, елементи поля можуть бути легко представлені у вигляді n-бітових кодових слів, це дозволяє збільшити швидкість апаратної реалізації еліптичних алгоритмів [2 – 3].

Одним з основних напрямів використання еліптичних кривих є формування алгеброгеометричних кодів по кривій (еліптичних кодів).

Зафіксуемо кінцеве поле GF(q). Нехай X – гладка проективная алгеброгеометрична крива в проективном пространстве Pn над GF(q), g = g(X) – рід кривої, X(GF(q)) – множина її точок над кінцевим полем, N = X(GF(q)) – їх число. Нехай C – клас дивізорів на X степені $\alpha > g - 1$. Тоді C визначає відображення $\varphi: X \to Pk\text{-}1$, где $k \geq \alpha - g + 1$. Набір yi = φ(xi) задает код. Число точок в перетині φ(X) з гіперплощиною дорівнює α, тобто $n - d \leq \alpha$. Ця конструкція дозволяє будувати коди з параметрами $k + d \geq n - g + 1$, довжина n яких меньше чи дорівнює числу точок на кривій X. При $2g < \alpha \leq n$ алгеброгеометричний код має параметри $(n, \alpha - g + 1, d)$, $d \geq n - \alpha$. Двоїстий до нього код також є алгеброгеометричним і має параметри $(n, n - \alpha + g - 1, d\perp)$, $d\perp \geq \alpha - 2g + 2$. Дамо наступне визначення алгеброгеометричного коду: алгеброгеометричний код по кривій X над GF(q) – це лінійний код довжини $n \leq N$, кодові слова C(c1, c2, …, cn) якого задаються рівністю:

$$\sum_{i=0}^{k-1} i_j F_j(P_i) = C_i$$

де Pi(Xi, Yi, Zi) - проективні точки кривої X, тобто (Xi, Yi, Zi) – рішення однорідного алгебраїчного рівняння, що задають криву X, $i = \overline{1,n}$; $F_j(P_i)$ – значення генераторних функцій в точках кривої.

Це визначення рівнозначне матричному поданню алгеброгеометрично-го коду:

$$G\,(i_0, i_1, ..., i_{k-1})^T = (c_0, c_1, ..., c_{n-1}),$$

де G – породжуюча матриця розмірності k×n, $k = \alpha - g + 1$, $\alpha = \deg X \cdot \deg F$.

$$G = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{k-1}(P_0) & F_{k-1}(P_1) & ... & F_{k-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,k}$$

Алгеброгеометричний (n, k, d) код по еліптичній кривій (еліптичний код) над GF(q) побудований через відображення виду $\varphi: EC \to Pk\text{-}1$ пов'язаний характеристиками $k + d \geq n$, причому: $n \leq 2\sqrt{q} + q + 1$, $k \geq \alpha$, $d \geq n - \alpha$, $\alpha = 3 \cdot \deg F$ [4 ; 5].

Таким чином, основними перевагами еліптичної криптографії є:

- набагато менша довжина ключа в порівнянні з «класичною» асиметричною криптографією.

- висока швидкість роботи еліптичних алгоритмів. Це пояснюється як розмірами поля, так і застосуванням ближчою для комп'ютерів структури бінарного кінцевого поля.

- через маленьку довжини ключа і високу швидкості роботи, алгоритми на еліптичних кривих можуть використовуватися в смарт-картах та інших пристроях з обмеженими обчислювальними ресурсами.

Перелік використаних джерел

1. Остапов С.Е. Технології захисту інформаці. / С.Е. Остапов,С.П. Євсеєв,О.Г. Король – «Родовід» Чернівці, 2014. – 428 с.

2. Болотов А. Элементарное введение в эллиптическую криптографию / А. Болотов, С. Гашков, А. Фролов, А. Часовских – М.:КомКнига, 2006. – 608с.

3. Lawrence Washington Elliptic curves, Number theory and Cryptography. – CRC Press, 2000. – 430 с.

4. R.J. McEliece. A Public-Key Criptosystem Based on Algebraic Theory. // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – P. 114-116.

5. H. Niederreiter. Knapsack-Type Cryptosystems and Algebraic Coding Theory. // Probl. Control and Inform. Theory. – 1986. –V.15. – P. 19-34.