ОНАЦЬКИЙ ОЛЕКСІЙ ВІТАЛІЙОВИЧ

Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки, кандидат технічних наук, доцент

ЖАРОВА ОКСАНА ВІТАЛІЇВНА

Національний університет «Одеська політехніка»,
доцент кафедри вищої математики,
кандидат фізико-математичних наук, доцент

ПРОТОКОЛ ОБМІНУ КЛЮЧАМИ ЗІ ВЗАЄМНОЇ АВТЕНТИФІКАЦІЇ СТОРІН НАД РОЗШИРЕНИМ ПОЛЕМ $GF(2^M)$ ЕЛІПТИЧНИХ КРИВИХ

Будь-яка криптографічна система заснована на використанні криптографічних ключів. У симетричній криптосистемі відправник і одержувач повідомлення використовує один секретний ключ. В асиметричних криптосистемах для зашифровування й розшифровування використовуються різні ключі [1; 2].

В роботі запропоновано протокол обміну ключами зі взаємної автентифікації сторін над розширеним полем $GF(2^m)$ еліптичних кривих (elliptic curves – EC). Безпека криптосистем на еліптичних кривих, заснована на труднощах розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої [1; 2]. У криптосистем на EC запропоновано використовувати криптоперетворення, що базуються на перетвореннях у групі точок еліптичних кривих над полями $GF(p)$, $GF(2^m)$, $GF(p^m)$ [1; 2].

У криптосистемах над розширеним полем $GF(2^m)$ рівняння EC має вигляд [2]:

$y^2 + xy \equiv (x^3 + ax^2 + b) \bmod (f(x), 2)$ – несуперсингулярна крива;

$y^2 + cy \equiv (x^3 + ax + b) \bmod (f(x), 2)$ – суперсингулярна крива,

де x, y – точки EC, $x, y \in E(GF(2^m))$;

a, b, c – коефіцієнти EC;

$f(x)$ – незведений поліном над полем $GF(2)$ вигляду

$$f(x) = x^m + h_1 x^{m-1} + h_2 x^{m-2} + \ldots + h_{m-1} x^1 + h_m,$$

причому $h_i \in GF(2)$.

Визначимо над точками з $E(GF(2^m))$ операцію складання та подвоєння. Нехай відомі координати двох точок $P = (x_1, y_1)$ і $Q = (x_2, y_2)$, то сума $P + Q = (x_3, y_3)$ визначається згідно з правилами [1; 2]:

1) несуперсингулярна крива

$$x_3 \equiv (\lambda^2 + \lambda + x_1 + x_2 + a) \bmod (f(x), 2);$$
$$y_3 \equiv [\lambda(x_1 + x_3) + x_3 + y_1] \bmod (f(x), 2);$$

2) суперсингулярна крива

$$x_3 \equiv (\lambda^2 + x_1 + x_2) \bmod (f(x), 2);$$
$$y_3 \equiv [\lambda(x_1 + x_3) + y_1 + c] \bmod (f(x), 2),$$

де $\lambda \equiv \left(\frac{y_1 + y_2}{x_1 + x_2} \right) \bmod (f(x), 2)$.

Точка, що подвоєна $2P = 2(x_1, y_1) = (x_3, y_3)$, визначається згідно з правилами:

1) несуперсингулярна крива

$$x_3 \equiv (\lambda^2 + \lambda + a) \bmod (f(x), 2);$$
$$y_3 \equiv [x_1^2 + (\lambda + 1)x_3] \bmod (f(x), 2),$$

де $\lambda \equiv \left(x_1 + \frac{y_1}{x_1} \right) \bmod (f(x), 2)$.

2) суперсингулярна крива

$$x_3 \equiv \lambda^2 \bmod (f(x), 2);$$
$$y_3 \equiv [\lambda(x_1 + x_3) + y_1 + c] \bmod (f(x), 2),$$

де $\lambda \equiv \left(\frac{x_1^2 + a}{c} \right) \bmod (f(x), 2)$.

Усі параметри є поліномами не вище m-степеня, а $f(x)$ – примітивний поліном над полем $GF(2)$.

Нехай $E_p(a, b)$ – еліптична крива над розширеним полем $GF(2^m)$, відома учасникам інформаційного процесу; $f(x)$ – незведений поліном над полем $GF(2)$; G – попередньо погоджена точка цієї кривої; $\#E_p(a, b) = n$ – порядок групи кривої; k_a і k_b – секретні ключі абонентів; r_1, r_a і r_2, r_b – випадкові числа абонентів A та B; ID_a і ID_b – ідентифікатори абонентів.

Спочатку абоненти A і B обчислює значення відкритих ключів $Y_a = k_aG \bmod (f(x), 2) = (x_a, y_a)$ $(f(x), 2)$ та $Y_b = k_bG \bmod (f(x), 2) = (x_b, y_b)$ $(f(x), 2)$, які передають один одному.

Протокол взаємної автентифікації сторін. Абонент A генерує випадково число r_1 та зашифровує повідомлення $E_{Y_b}(r_1, ID_a)$ яке передає абоненту B. Абонент B розшифровує повідомлення $E_{Y_b}(r_1, ID_a)$ з використанням секретного ключа k_b, потім генерує випадково число r_2 та зашифровує повідомлення $E_{Y_a}(r_1, r_2, ID_b)$, яке передає абоненту A. Абонент A розшифровує повідомлення $E_{Y_a}(r_1, r_2, ID_b)$ з використанням секретного ключа k_a та перевіряє рівність $r_1 = r_1^*$ (r_1^* – значення після розшифрування), якщо рівність виконано, абоненти A передає абоненту B повідомлення $E_{Y_b}(r_2, ID_a)$. Абонент B розшифровує повідомлення $E_{Y_b}(r_2, ID_a)$ та перевіряє рівність $r_2 = r_2^*$ (r_2^* – значення після розшифрування), якщо рівність виконано процедура взаємної автентифікації сторін виконано.

Протокол обміну ключами. Абонент A розраховує параметри:

$$R_a = r_aG \bmod (f(x), 2);$$
$$F_a = r_aY_b \bmod (f(x), 2) = (x_1, y_1) \bmod (f(x), 2);$$
$$S_a \equiv (r_a + k_a x_a x_1) \bmod n.$$

Значення R_a відправляється абоненту B.

Абонент B розраховує параметри:

$$R_b = r_b G \bmod (f(x), 2);$$
$$F_b = r_b Y_a \bmod (f(x), 2) = (x_2, y_2) \bmod (f(x), 2);$$
$$S_b \equiv (r_b + k_b x_b x_2) \bmod n.$$

Значення R_b відправляється абоненту A. Після обмінами значеннями R_a і R_b абоненти A і B розраховують загальний секретний ключ K.

Абоненти A:

$$Q_a = k_a R_b \bmod (f(x), 2) = (x_2, y_2) \bmod (f(x), 2);$$
$$K = S_a(R_b + x_b x_2 Y_b) \bmod (f(x), 2).$$

Абоненти B:

$$Q_b = k_b R_a \bmod (f(x), 2) = (x_1, y_1) \bmod (f(x), 2);$$
$$K = S_b(R_a + x_a x_1 Y_a) \bmod (f(x), 2).$$

Повнота протоколу:

$$S_a(R_b + x_b x_2 Y_b) \bmod (f(x), 2) = (r_a + k_a x_a x_1)(r_b G + x_b x_2 k_b G) \bmod (f(x), 2) =$$
$$= (r_a r_b G + k_a x_a x_1 r_b G + r_a x_b x_2 k_b G + k_a x_a x_1 x_b x_2 k_b G) \bmod (f(x), 2) =$$
$$= S_b(R_a + x_a x_1 Y_a) \bmod (f(x), 2) = (r_b + k_b x_b x_2)(r_a G + x_a x_1 k_a G) \bmod (f(x), 2) =$$
$$= (r_a r_b G + k_a x_a x_1 r_b G + r_a x_b x_2 k_b G + k_a x_a x_1 x_b x_2 k_b G) \bmod (f(x), 2).$$

Для аналізу та перевірки запропонованого протоколу на стійкість до атак противника був застосований програмний продукт AVISPA [3]. В роботі виконано перевірку моделі протоколу та результат моделювання зловмисника на протокол. Програмна верифікація протоколу і стійкість протоколу до атак зловмисника була виконана за допомогою програмних модулів OFMC та CLAtSe AVISPA. В результаті перевірки протоколу відомих атак не знайдено.

Таким чином, у роботі запропоновано криптографічний протокол обміну ключами зі взаємної автентифікації сторін над розширеним полем $GF(2^m)$ еліптичних кривих. Визначено повнота і коректність протоколу, була виконана перевірка моделі і верифікація протоколу. В результаті перевірки протоколу відомих атак на протокол, не знайдено. Для реалізації протоколу можна використовувати рекомендовані еліптичні криві згідно FIPS 186-4 [4], SEC 2 [5] та ДСТУ 4145-2002 [6].

Список використаних джерел:

1. Stavroulakis P., Stamp M. Handbook of Information and Communication Security: Berlin : Springer-Verlag, 2010. – 863 p.
2. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика: монографія, Харків : Видавництво «Форт», 2012. – 880 с.
3. AVISPA. URL: http://www.avispa-project.org/
4. FIPS 186-4. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
5. SEC 2. URL: https://www.secg.org/SEC2-Ver-1.0.pdf
6. ДСТУ 4145-2002. URL: https://ru.wikipedia.org/wiki/ДСТУ_4145-2002

Ключові слова: криптографічний протокол, розподіл ключів, автентифікація, еліптична крива, асиметричні криптосистеми.

Key words: cryptographic protocol, key distribution, authentication, elliptic curve, asymmetric cryptosystems.