АНАЛІЗ КРИПТОСТІЙКОСТІ МЕТОДУ ЦИФРОВОГО ПІДПИСУВАННЯ З ПРИСКОРЕНОЮ ПРОЦЕДУРОЮ ПЕРЕВІРКИ ПІДПИСУ

Костянтин Черняхович[1], Юрій Яремчук[2]

Вінницький національний технічний університет
Хмельницьке шосе, 95, Вінниця, 21021, Україна,
E-mail: [1]k_ch@ukr.net, [2]yurevyar@bigmir.net

Анотація

Проведено аналіз криптостійкості методу цифрового підписування на основі математичного апарату еліптичних кривих для застосування в додатках, що потребують швидкої перевірки цифрового підпису.

Вступ

Сьогодні, існує багато методів цифрового підписування на основі математичного апарату еліптичних кривих, серед яких слід відмітити такі як ДСТУ 4145-2002 [1], ГОСТ Р34.10-2001 [2], ECSS, ECDSA, EC-GDSA, EC-KCDSA [3, 4]. Однак, незважаючи на широке використання та переваги вище вказаних методів цифрового підписування, існують певні проблеми їх практичного застосування в окремих додатках. Зокрема, це стосується додатків, в яких процеси перевірки цифрового підпису домінують над процесами формування. До таких додатків в першу чергу відносяться додатки типу клієнт-сервер, прикладом практичного застосування яких можуть бути центри сертифікації ключів, центри видачі цифрових атестатів, електронні платіжні системи та ін.

Проведено аналіз відомих методів цифрового підписування на основі математичного апарату еліптичних кривих та їх конкретних практичних реалізацій з точки зору обчислювальної складності процедур формування/перевірки підпису. Аналіз показав, що всі вищезгадані методи цифрового підписування на основі математичного апарату еліптичних кривих мають один загальний недолік – це велика обчислювальна складність процедури перевірки цифрового підпису в порівнянні із процедурою формування.

Існує метод цифрового підписування з прискореною процедурою цифрового підпису на основі математичного апарату еліптичних кривих в якому вищерозглянутий недолік усунуто [5, 6]. При цьому, питання про стійкість даного методу залишається актуальним. Таким чином, виникає необхідність проведення досліджень спрямованих на оцінку криптостійкості методу цифрового підписування з прискореною процедурою перевірки підпису.

Проведено аналіз методу цифрового підписування на основі математичного апарату еліптичних кривих з прискореною процедурою перевірки підпису з точки зору теоретичної криптостійкості. Аналіз проводився виходячи з припущення, що в якості зловмисника може виступати як третя сторона, так і будь-який санкціонований користувач криптосистеми. При цьому, вважається, що зловмиснику відомі такі дані, як: m - степінь розширення основного поля; еліптична крива задана рівнянням вигляду

$$y^2 + xy = x^3 + Ax^2 + B\,, \tag{1}$$

де A, B – коефіцієнти рівняння; n – порядок базової точки еліптичної кривої; P – базова точка еліптичної кривої; Q – відкритий ключ; H – обрана функція хешування; цифровий підпис у вигляді великих цілих чисел $\{s, r\}$.

Розглянуто такі можливі спроби зловмисника, як можливість обчислення цифрового підпису без одного із секретних параметрів та можливість підміни повідомлення M.

Показано, що обчислення таємного ключа k та цілих чисел із множини $\{s_0, s_1, ..., s_v\}$ зводиться до розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої, так як необхідно здійснювати обчислення

$$\{\vartheta(\pi(h_0)x_R) \bmod n, \vartheta(\pi(h_1)x_R) \bmod n, ..., \vartheta(\pi(h_v)x_R) \bmod n\}\,, \tag{2}$$

та $\{r_0, r_1, ..., r_v\}$, які в свою чергу, обчислюються відповідно до виразу вигляду

$$\{'m_0(r_0 + h_0) \bmod n, m_1'(r_1 + h_1) \bmod n, ..., m_v'(r_v + h_v) \bmod n\}\,, \tag{3}$$

що значно ускладнюється обчисленням невідомих значень із множини

$$\{z_0, z_1, ..., z_v\} \in \{dr_0 \bmod n, dr_1 \bmod n, ..., dr_v \bmod n\}\,. \tag{4}$$

В зв'язку з цим, задача зводиться до обчислення чисел із множини

$$\{m'_0, m'_1, ..., m'_v\} \in \{\vartheta(\lambda(z_0\mathrm{P})), \vartheta(\lambda(z_1\mathrm{P})), ..., \vartheta(\lambda(z_v\mathrm{P}))\}, \quad (5)$$

що в свою чергу призводить до необхідності обчислення x із виразу вигляду $y = xP$, де x - велике ціле число.

Також, розглянуто можливість підробки підпису при умові, що зловмисник має відкритий ключ Q і може отримувати обчислені значення кожного кроку перевірки цифрових підписів з множини

$$\{DS_0, DS_1, ..., DS_v\} \in \{\{s_0, r_0\}, \{s_1, r_1\}, ..., \{s_v, r_v\}\} \quad (6)$$

та відповідних їм повідомлень $\{M_0, M_1, ..., M_v\}$, де v – кількість підписаних повідомлень. В цьому випадку, всі загальносистемні параметри при підписуванні цих повідомлень вважаються однаковими. Розглянуто можливість отримання зловмисником під час перевірки підписів множини таємних цілих чисел

$$\{m'_0, m'_1, ..., m'_v\} \in \{m''_0, m''_1, ..., m''_v\} \in \{\vartheta(\lambda(r_0Q)), \vartheta(\lambda(r_1Q)), ..., \vartheta(\lambda(r_vQ))\}, \quad (7)$$

що дає йому можливість обчислити цілі числа з множини

$$\{s_0, s_1, ..., s_v\} \in \{m''_0(r_0 + h_0) \bmod n, m''_1(r_1 + h_1) \bmod n, ..., m''_v(r_v + h_v) \bmod n\}. \quad (8)$$

Однак, аналіз показав, що цього не достатньо для формування цифрових підписів DS_i, $i = \overline{0, v}$, оскільки $m' = \vartheta(x_L)$ та $z = dr \bmod n$, де $m'_0 \neq m'_1 \neq ... \neq m'_v$ і, відповідно $m''_0 \neq m''_1 \neq ... \neq m''_v$, за умови, що повідомлення різні, тобто $M_0 \neq M_1 \neq ... \neq M_v$. Таким чином, знаючи множину повідомлень, зловмисник має можливість обчислити тимчасові таємні ключі $m'_i \equiv m''_i$ та цілі числа s_i, але не має можливості обчислити цілі числа r_i і підробити підпис DS_i для відповідного повідомлення, а також будь-якого іншого повідомлення M_i із множини повідомлень.

Також, відзначено, що однією із спроб зловмисника може бути спроба обчислення колізій для функції хешування H, якщо геш-код обчислюється як *h=H(M)*. Для попередження можливості попереднього обчислення колізій функції гешування потрібно здійснити заміщення виразу $h = H(M)$ виразом вигляду $h = H(M \parallel m')$, де m' – ціле число, яке обчислено на основі таємного ключа.

Аналіз показав, що у всіх вищенаведених випадках обчислення зводяться до необхідності розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої.

Таким чином, на основі проведеного аналізу криптостійкості запропонованого методу цифрового підписування, можна зробити висновок, що метод є достатньо криптостійким.

Література:

[1] ДСТУ 4145-2002. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – К.: Держстандарт України, 2003. – 94 с.
[2] ГОСТ Р34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки цифровой подписи// Госстандарт России, М.: 2001.
[3] Болотов А. А., Машков С. Б., Фролов А. Б., Часовских А. А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. – М.: КомКнига, 2006. – 328 с.
[4] Бессалов А. В., Телиженко А. Б. Криптосистемы на эллиптических кривых: Учеб. Пособие. – К.: ІОЦ «Видавництво «Політехніка», 2004. – 224 с.: іл.
[5] Пат. UA24459, МПК(2006) H03M 13/00. «Спосіб цифрового підписування на основі математичного апарату еліптичних кривих» // Яремчук Ю.Є.; Черняхович К.В. – № U200705052. Заявл. 07.05.2007; Опубл. 25.06.2007, Бюл. №9, 2007.
[6] Яремчук Ю.Є., Черняхович К.В. Метод цифрового підписування на основі математичного апарату еліптичних кривих з прискореною процедурою перевірки підпису. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К., 2007. – №1 (14), – С. 119-127.