Отримані результати є підґрунтям для подальших досліджень, зокрема, для аналізу кубічних атак із більшими степенями макстермів. У той же час розглядувана задача має самостійний інтерес з точки зору теорії булевих функцій та комбінаторики.

*Список використаної літератури: 1. Dinur I. Cube attacks on tweakable black box polynomials / Dinur I., Shamir A. – Cryptology ePrint Archive, 2008/385. [Online] Available at: http://eprint.iacr.org/2008/385.pdf. 2. Dinur I. Cube attacks on tweakable black box polynomials / Dinur I., Shamir A. // EUROCRYPT, vol. 5479 of Lecture Notes in Computer Science – Springer, 2009. – P. 278-299. 3. Dinur I. Side Channel Cube Attacks on Block Ciphers / Dinur I., Shamir A. – Cryptology ePrint Archive, 2009/127. [Online] Available at: http://eprint.iacr.org/2009/127.pdf. 4. Aumasson J-P. Cube Testers and Key Recovery Attacks on Reduced Round MD6 and Trivium / Aumasson J-P., Meier W., Dinur I., Shamir A. // Fast Software Encryption 2009, LNCS, vol 5665 – Springer, 2009. – P. 1-22. 5. Dinur I. Cube Attacks and Cube-attack-like Cryptanalysis on the Round-reduced Keccak Sponge Function / Dinur I., Morawiecki P., Pieprzyk J., Srebrny M., Straus M. – Cryptology ePrint Archive, 2014/736. [Online] Available at: http://eprint.iacr.org/2014/736.pdf. 6. Meier W. Cube Testers and Key Recovery in Symmetric Cryptography / Meier W. – 2009. [Online] Available at: http://indocrypt09.inria.fr/slides_cube_ind09.pdf.*

***Анатолій Кочубінський, Володимир Синявський, Олександр Шаталов***
*Інститут кібернетики імені В. М. Глушкова НАН України*

**УДК 002:651.928(083.73)**

# АЛГОРИТМ ВСТАНОВЛЕННЯ СПІЛЬНОГО СЕКРЕТНОГО ЗНАЧЕННЯ, ЩО ҐРУНТУЄТЬСЯ НА ЕЛІПТИЧНИХ КРИВИХ

*Анотація:* **Пропонується алгоритм встановлення спільного секретного значення, який розроблено з використанням криптографічного перетворення, визначеного національним стандартом України ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, заснований на еліптичних кривих. Формування і перевіряння», та криптографічних стандартів, що діють в Україні. Цей алгоритм забезпечує автентичність сторін інформаційного обміну.**

*Summary:* **An algorithm of establishment of shared secret value is presented. The algorithm is based on the cryptographic transformation defined by the national standard of Ukraine DSTU 4145-2002 «Information technology. Cryptographic techniques. Digital signatures based on elliptic curves. Generation and verification» and cryptographic standards which operate in Ukraine. This algorithm provides mutual authenticity of information exchange parties.**

*Ключові слова:* **Асиметричне шифрування, симетричне шифрування, еліптичні криві, спільний секретний ключ.**

## Вступ

Конфіденційність повідомлення забезпечується шифруванням повідомлення за допомогою алгоритму шифрування даних. При великому розмірі документа таким алгоритмом може бути тільки алгоритм симетричного шифрування. Використання симетричного алгоритму шифрування пов'язано з необхідністю вирішення проблеми розподілу секретних ключів шифрування. Одним з можливих рішень є використання алгоритму асиметричного шифрування, яким шифрується разовий ключ симетричного шифрування, однак в системах передачі даних в реальному часі потрібне інше рішення, яке дозволить швидко з'єднатися з будь яким абонентом, встановити спільний секретний ключ та за певним розкладом або у разі потреби сформувати новий спільний ключ та перейти на використання нового спільного ключа. Під час встановлення спільного секретного ключа обов'язково повинна забезпечуватися автентичність сторін інформаційного обміну. Алгоритми цього типу є необхідною складовою частиною основних на цей час методів захисту трафіку в мережі Інтернет, а саме протоколів SSL/TSL та IPSec.

Найбільше поширення як алгоритм встановлення спільного секретного значення мають алгоритми, що базуються на алгоритмі Діффі-Хеллмана. В своєму стандартному вигляді цей алгоритм не забезпечує автентифікації сторін і тому не може протистояти засобам криптоаналізу, що використовують можливість порушення автентичності. Алгоритм встановлення спільного секретного значення має також гарантувати стійкість обчисленого спільного секретного значення, не меншу за стійкість симетричного алгоритму шифрування даних. Реально це можливо тільки за умови застосування криптографічних перетворень у групі точок належно обраних еліптичних кривих. З практичної точки зору важливо уніфікувати обчислювальні засоби, що використовуються для реалізації криптографічних перетворень різного типу.

В роботі пропонується алгоритм встановлення спільного секретного значення, розроблений на основі схеми [1] з використанням криптографічного перетворення, визначеного національним стандартом України ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, заснований на еліптичних кривих. Формування і перевіряння» [2], та криптографічних стандартів, що діють в Україні. Цей алгоритм забезпечує автентичність сторін інформаційного обміну.

Алгоритм призначено для обчислення в режимі реального часу двома учасниками інформаційного обміну спільного секретного значення, розмір якого визначається функцією гешування, що використовується. Це секретне значення використовується для ініціалізації алгоритму симетричного шифрування але не визначає його спосіб ініціалізації та спосіб шифрування потоку даних. Алгоритм встановлення спільного секретного значення можна використовувати для захисту даних в інформаційних системах загального призначення.

## І Терміни, визначення та позначення

В роботі використовуються терміни і визначення з розділу 3 [2], а також наступні.

Загальними параметрами встановлення спільного секретного значення для обох користувачів алгоритму є:

- параметри основного поля $GF\left(2^m\right)$: степінь розширення $m$ і примітивний многочлен $f(t)$ (тричлен, п'ятичлен), що задає поліноміальний базис;
- еліптична крива виду $y^2 + xy = x^3 + Ax + B,$ де $A, B \in GF\left(2^m\right), B \neq 0, A \in \left(0,1\right);$
- базова точка еліптичної кривої $P$;
- функція гешування згідно з 6.2 ДСТУ 4145;
- порядок базової точки $n$.

Загальні параметри алгоритму задаються відповідно до цієї статті, розділу 7 [2], і зображуються відповідно до розділу 5 [2].

Довгостроковий індивідуальний параметр алгоритму встановлення спільного секретного значення, що обчисляється згідно з розділом 9.1 [2]. Кожен користувач алгоритму має свій довгостроковий секретний ключ встановлення спільного секретного значення, що позначаються $d_1$ та $d_2$.

Точка еліптичної кривої $Q$, обчислена відповідно до розділу 9.2 [2]. Довгостроковий відкритий ключ встановлення спільного секретного значення є довгостроковим індивідуальним параметром алгоритму встановлення спільного секретного значення. Кожен користувач алгоритму має свій довгостроковий відкритий ключ встановлення спільного секретного значення, що позначаються $Q_1$ та $Q_2$. Передбачається, що в процесі виконання алгоритму кожен користувач має доступ до автентичної копії довгострокового відкритого ключа іншого користувача**.**

Разовий індивідуальний параметр алгоритму встановлення спільного секретного значення, що обчислюється відповідно до розділу 9.1 [2]. Кожен користувач алгоритму має свій разовий секретний ключ встановлення спільного секретного значення, що позначаються $e_1$ та $e_2$ .

Разовий відкритий ключ встановлення спільного секретного значення є разовим індивідуальним параметром алгоритму встановлення спільного секретного значення. Кожен користувач алгоритму обчислює в процесі виконання алгоритму свій разовий відкритий ключ встановлення спільного секретного значення, що позначаються $R_1$ и $R_2$. В процесі виконання алгоритму користувачі обмінюються разовими відкритими ключами встановлення спільного секретного значення.

Спільне секретне значення – це двійковий рядок, обчислений згідно з цим алгоритмом. Довжина цього рядку дорівнює параметру $L_H$ функції гешування, що використовується разом з цим алгоритмом.

В роботі використовуються позначення з розділу 4 [2], а також позначення, наведені в таблиці 1.

Математичні об'єкти, що використовуються в даному алгоритмі, зображуються відповідно до розділу 5 ДСТУ 4145. Крім того, використовуються наступний формат даних.

Спільне секретне значення є результатом обчислення функції гешування та зображується згідно з розділом 5.6 [2].

Таблиця 1

| | |
|---|---|
| $d_1$ | Довгостроковий секретний ключ алгоритму встановлення спільного секретного значення першого користувача, натуральне число, $0 < d_1 < n$ |
| $Q_1$ | Довгостроковий відкритий ключ алгоритму встановлення спільного секретного значення першого користувача, точка еліптичної кривої |
| $e_1$ | Разовий секретний ключ алгоритму встановлення спільного секретного значення першого користувача, натуральне число, $0 < e_1 < n$ |
| $R_1$ | Разовий відкритий ключ алгоритму встановлення спільного секретного значення першого користувача, точка еліптичної кривої |
| $d_2$ | Довгостроковий секретний ключ алгоритму встановлення спільного секретного значення другого користувача, натуральне число, $0 < d_2 < n$ |
| $Q_2$ | Довгостроковий відкритий ключ алгоритму встановлення спільного секретного значення другого користувача, точка еліптичної кривої |
| $e_2$ | Разовий секретний ключ алгоритму встановлення спільного секретного значення другого користувача, натуральне число, $0 < e_2 < n$ |
| $R_2$ | Разовий відкритий ключ алгоритму встановлення спільного секретного значення другого користувача, точка еліптичної кривої |
| $S$ | Спільне секретне значення, двійковий рядок довжиною $L_H$ |

## II Обчислювальні алгоритми

В алгоритмі встановлення спільного секретного значення використовуються обчислювальні алгоритми, визначені в розділі 6 [2], а також наступні.

***1. Обчислення загальних параметрів алгоритму встановлення спільного секретного значення***

Основне поле вибирається відповідно до підрозділу 7.1 [2]. В алгоритмі встановлення спільного секретного значення використовуються винятково основні поля, що задаються поліноміальним базисом. Еліптична крива вибирається згідно з 7.2 [2]. Базова точка обчислюється згідно з 7.3 [2]. Перевірка правильності загальних параметрів алгоритму асиметричного шифрування проводиться відповідно до розділу 8 [2].

***2. Обчислення ключів алгоритму встановлення спільного секретного значення***

Довгострокові та разові секретні ключі алгоритму встановлення спільного секретного значення обчислюються згідно з розділом 9.1 [2].

Довгострокові та разові відкриті ключі алгоритму встановлення спільного секретного значення обчислюються згідно з розділом 9.2 [2].

## III Перевірка правильності ключів встановлення спільного секретного значення

Правильність ключів алгоритму встановлення спільного секретного значення перевіряється відповідно до розділу 10 [2].

## IV Опис алгоритму встановлення спільного секретного значення

*Вхідні дані алгоритму встановлення спільного секретного значення, спільні для обох користувачів*:

- загальні параметри алгоритму встановлення спільного секретного значення;
- функція гешування H згідно з 6.2 [2];

*Вхідні дані алгоритму встановлення спільного секретного значення першого користувача*

- Довгостроковий секретный ключ першого користувача $d_1$;
- Довгостроковий відкритий ключ першого користувача $Q_1$;
- Довгостроковий відкритий ключ другого користувача $Q_2$;

*Вхідні дані алгоритму встановлення спільного секретного значення другого користувача*

- Довгостроковий секретный ключ другого користувача $d_2$;
- Довгостроковий відкритий ключ другого користувача $Q_2$;
- Довгостроковий відкритий ключ першого користувача $Q_1$;

*Результат виконання алгоритму*: спільне секретне значення *S*.

*Алгоритм встановлення спільного секретного значення*

Обидва користувачі перевіряють правильність загальних параметрів алгоритму встановлення спільного секретного значення відповідно до цього документу. Якщо хоча б один з користувачів з'ясує, що загальні параметри алгоритму встановлення спільного секретного значення обчислено неправильно, то виконання алгоритму припиняється. Цю перевірку не виконують у випадках, передбачених розділами 8.1 – 8.3 [2].

Кожен користувач перевіряє правильність свого довгострокового секретного ключа, свого довгострокового відкритого ключа та довгострокового відкритого ключа іншого користувача згідно з цим документом Якщо хоча б один з користувачів з'ясує, що хоча б один з цих ключей обчислено неправильно то виконання алгоритму припиняється. Цю перевірку не виконують у випадках, передбачених розділом 10 [2].

Перший користувач обчислює свій разовий секретний ключ $e_1$ та свій разовий відкритий ключ $R_1$ згідно з цим документом, обчислює стиснене зображення $f_1$ точки $R_1$ еліптичної кривої згідно з розділом 6.9 [2], та зображує цей елемент основного поля як двійковий рядок $s_1$ згідно з розділом 5.3 [2].

Другий користувач обчислює свій разовий секретний ключ $e_2$ та свій разовий відкритий ключ $R_2$ згідно з цим документом, обчислює стиснене зображення $f_2$ точки $R_2$ еліптичної кривої згідно з розділом 6.9 [2], та зображує цей елемент основного поля як двійковий рядок $s_2$ згідно з розділом 5.3 [2].

Користувачі обмінюються двійковими рядками $s_1$ та $s_2$.

Перший користувач перетворює рядок $s_2$ на елемент поля $f_2$, відновлює точку еліптичної кривої $R_2$ згідно з розділом 6.10 [2], перетворює *x*-координату точки $R_2$ на ціле число $r_2$ згідно з розділом 5.8 [2], перетворює *x*-координату точки еліптичної кривої $R_1$ на ціле число $r_1$ згідно з розділом 5.8 [2], обчислює точку еліптичної кривої *U* за формулами:

$$v = (r_1 d_1 + e_1) \bmod n;$$
$$V = 2v(r_2 Q_2 + R_2);$$
$$U = \begin{cases} V, \text{ якщо } A = 1; \\ 2V, \text{ якщо } A = 0; \end{cases}$$

обчислює стиснене зображення точки *U* еліптичної кривої як елемент основного поля відповідно до розділу 6.9 [2], зображує цей елемент основного поля як двійковий рядок *s* згідно з розділом 5.3 [2], та обчислює геш-код $S = H(s)$.

Другий користувач перетворює рядок на елемент поля $f_1$, відновлює точку еліптичної кривої $R_1$ згідно з розділом 6.10 [2], перетворює *x*-координату точки $R_1$ на ціле число $r_1$ згідно з розділом 5.8 [2], перетворює *x*-координату точки $R_2$ на ціле число $r_2$ згідно з розділом 5.8 [2], обчислює точку еліптичної *U* за формулами:

$$v = (r_2 d_2 + e_2) \bmod n;$$
$$V = 2v(r_1 Q_1 + R_1);$$
$$U = \begin{cases} V, \text{ якщо } A = 1; \\ 2V, \text{ якщо } A = 0; \end{cases}$$

обчислює стиснене зображення точки *U* еліптичної кривої як елемент основного поля згідно з розділом 6.9 [2], зображує цей елемент основного поля як двійковий рядок *s* згідно з розділом 5.3 [2] та обчислює геш-код $S = H(s)$.

Результат виконання алгоритму – спільне секретне значення *S*.

## V Доказ коректності алгоритму

Перший користувач алгоритму має свій довгостроковий таємний ключ $d_1$, свій довгостроковий відкритий ключ $Q_1$ та довгостроковий відкритий ключ другого користувача $Q_2$. Під час виконання першої фази алгоритму перший користувач обчислює свій разовий секретний ключ $e_1$ та свій разовий відкритий ключ $R_1 = -e_1 P$, де *P* – базова точка еліптичної кривої. Перший користувач отримує також разовий відкритий ключ другого користувача $R_2 = -e_2 P$, секретний ключ другого користувача $e_2$ першому користувачеві невідомий. Під час виконання другої фази алгоритму перший користувач обчислює точку еліптичної кривої

$$U_1 = 2k(r_1 d_1 + e_1)(r_2 Q_2 + R_2) = 2k(r_1 d_1 + e_1)(r_2 d_2 + e_2)P, \quad (1)$$

де $r_1$ та $r_2$ - цілі числа, отримані відповідно до разових відкритих ключів $R_1$ та $R_2$ наведеним вище чином, *k*=1, якщо коефіцієнт *A* еліптичної кривої дорівнює 1, та *k*=2, якщо цей коефіцієнт дорівнює 0.

Другий користувач алгоритму має свій довгостроковий таємний ключ $d_2$, свій довгостроковий відкритий ключ $Q_2$ та довгостроковий відкритий ключ першого користувача $Q_1$. Під час виконання першої фази алгоритму другий користувач обчислює свій разовий секретний ключ $e_2$ та свій разовий відкритий ключ $R_2 = -e_2 P$. Другий користувач отримує також разовий відкритий ключ першого користувача $R_1 = -e_1 P$, секретний ключ першого користувача $e_1$ другому користувачеві невідомий. Під час виконання другої фази алгоритму другий користувач обчислює точку еліптичної кривої

$$U_2 = 2k(r_2 d_2 + e_2)(r_1 Q_1 + R_1) = 2k(r_2 d_2 + e_2)(r_1 d_1 + e_1)P. \quad (2)$$

Формули (1) та (2) показують, що точки еліптичної кривої $U_1$ та $U_2$ збігаються, $U_1 = U_2$, тому збігаються стиснені зображення цих точок та зображення елементів основного поля, що відповідають стисненим зображенням цих двох точок у вигляді двійкових рядків. Отже, співпадають геш-коди цих двійкових рядків, які є спільним секретним значенням. Це доводить коректність наведеного алгоритму встановлення спільного секретного значення.

## VI Стійкість алгоритму

Наведений алгоритм є варіантом відомої схеми Діффі-Хеллмана встановлення спільного секретного значення. Фактично для криптоаналізу цієї схеми необов'язково вирішувати задачу дискретного логарифмування на еліптичній кривій, достатньо вміти вирішувати задачу Діффі-Хеллмана, тобто вміти обчислювати точку еліптичної кривої $abP$ за відомими точками цієї ж еліптичної кривої $aP$ та $bP$. У випадку наведеного алгоритму встановлення спільного секретного значення $a = r_1 d_1 + e_1$, $b = r_2 d_2 + e_2$. Ясно, що задача Діффі-Хеллмана легко вирішується, якщо є ефективний алгоритм вирішення задачі дискретного логарифмування. Точніше, якщо обчислення задачі дискретного логарифмування вважати за одну операцію (це називається зверненням до оракула), то задача Діффі-Хеллмана вирішується за поліноміальний час. З моменту винаходу алгоритму Діффі-Хеллмана існує припущення, що ці дві задачі еквівалентні. Це припущення в повному обсязі досі не доведено, однак останні результати у цій галузі роблять це припущення більш ніж вірогідним. У. М. Маурер та С. Вольф в декількох публікаціях [3, 4] довели, що при певних умовах за наявності оракула, що за одну операцію вирішує задачу Діффі-Хеллмана, задача дискретного логарифмування вирішується за поліноміальний час. Це випливає з наступного твердження [3].

Нехай *G* є скінченна циклічна група простого порядку *p* така, що існує еліптична крива над $F_p$, порядок якої є гладким, тобто повністю розкладається на прості множники, обмежені деяким цілим числом *B*. Тоді для цієї групи задачі Діффі-Хеллмана та дискретного логарифмування еквівалентні.

Порівняно недавно доведено [5], що заявлену в наведеному твердженні еліптичну криву завжди можна знайти для еліптичних кривих, що використовуються у практичній криптографії, тобто які включено до національних та міжнародних стандартів, що описують криптографічні алгоритми з використанням еліптичних кривих. Зокрема, можна твердити, що якщо немає алгоритму субекспонеціальної складності для вирішення задачі дискретного логарифмування, то немає алгоритму субекспонеціальної складності для вирішення задачі Діффі-Хеллмана.

Отже, стійкість алгоритму встановлення спільного секретного значення визначається стійкістю криптографічного перетворення, визначеного в [2], яка базується на обчислювальній складності задачі дискретного логарифмування. Відомо, що на цей час стійкість цього перетворення дорівнює $2^{m/2}$, де $m$ – ступінь розширення основного поля. Нехай складність перебору ключів алгоритму симетричного шифрування, для якого виробляється спільний секретний ключ на основі спільного секретного значення, виробленого за наведеним алгоритмом, дорівнює $2^t$, $t>0$. Тоді алгоритм встановлення спільного секретного значення забезпечить адекватну стійкість алгоритму симетричного шифрування, що використовується разом з алгоритмом встановлення спільного значення, тільки в тому випадку, якщо виконується нерівність $m \geq 2t$. Основний вітчизняний алгоритм симетричного алгоритму має ключ довжиною 256 бітів. Таким чином, маємо, що $m \geq 512$. З іншого боку, в алгоритмі встановлення спільного значення використовується функція гешування ГОСТ 34.311, стійкість якої є $2^{128}$. Таким чином, за наявного алгоритму гешування неможливо забезпечити максимальну стійкість алгоритму симетричного шифрування і тому немає сенсу використовувати великі основні поля для реалізації алгоритму встановлення спільного секретного значення. Основне поле з $m=257$ забезпечує еквівалентну стійкість шифрування даних порядку $2^{128}$ з використанням наведеного алгоритму встановлення спільного секретного значення та алгоритму симетричного шифрування ДСТУ ГОСТ 28147:2009. Ця стійкість вважається дуже високою і достатньою для більшості застосувань. Для забезпечення більш високої стійкості необхідна інша функція гешування. З іншого боку, немає ніяких перешкод для використання еліптичних кривих над дуже великими основними полями.

Практичну небезпеку для алгоритмів встановлення спільного секретного значення типу алгоритму Діффі-Хеллмана становлять протоколи реалізації цих алгоритмів, що не забезпечують автентичності сторін, які встановлюють спільне секретне значення. Порушення автентичності надає можливість третій стороні нав'язати себе як учасника інформаційного обміну та отримати доступ до конфіденційних даних. У наведеному алгоритмі така можливість виключається за рахунок того, що у обчисленні спільного секретного значення одночасно використовуються довгострокові та разові секретні та відкриті ключі обох користувачів. Якщо довгострокові відкриті ключі сертифікуються належним чином, то кожен користувач може перевірити автентичність іншого користувача. Додатковий рівень безпеки можливо забезпечити шляхом цифрового підписування разових відкритих ключів користувачів з використанням сертифікованих відкритих ключів цифрового підпису. Таким чином, алгоритм встановлення спільного секретного значення забезпечує автентичність користувачів алгоритму, якщо цей алгоритм функціонує в стандартному середовищі використання криптографічних алгоритмів з відкритими ключами, що базується на існуванні центрів сертифікації відкритих ключів.

*Список використаної літератури:* ***1.*** *L. Law, A. Menezes, M. Qu, J. Solinas and S. Vanstone. An efficient protocol for authenticated key agreement. //Technical report CORR 98-05, University of Waterloo,1998.* ***2.*** *ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння»// К.: Держстандарт України, 2003. 94 с.* ***3.*** *Blake I., Seroussi G., Smart N. Elliptic Curves in Cryptography. – Cambridge University Press, 1999. – p.204.* ***4.*** *U. Maurer and S. Wolf, The Diffie-Hellman protocol, //Designs, Codes and Cryptography, 19 (2000), 147-171.* ***5.*** *A.Muzereau, N.P.Smart, F.Vercauteren. The Equivalence between the DHP and DLP for Elliptic Curves Used in Practical Applications. //LMS J. Comput. Math. 7 (2004), p.- 50-72.*