УДК 004.056

Д.І. Прокопович-Ткаченко

Академія митної служби України, Дніпропетровськ

РЕАЛІЗАЦІЯ МЕТОДУ ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ МАКСИМАЛЬНОГО ПЕРІОДУ ІЗ ВИКОРИСТАННЯМ ПЕРЕТВОРЕНЬ НА ЕЛІПТИЧНИХ КРИВИХ

Розглядається реалізація методу формування псевдовипадкових послідовностей максимального періоду із застосуванням перетворень у групі точок еліптичних кривих (відповідно до удосконаленого методу на основі стандарту NIST SP 800-90) для побудови механізмів підвищення безпеки інформаційних систем і технологій.

Ключові слова: *безпека, генератор, псевдовипадкова послідовність.*

Вступ

Перспективним напрямком побудови криптографічно стійких генераторів псевдовипадкових послідовностей є застосування перетворень у групі точок еліптичних і гіпереліптичних кривих. Це дозволить будувати доказово стійкі криптоалгоритми, задача знаходження таємного ключа в яких пов'язана із вирішенням теоретико-складної задачі дискретного логарифмування у групі точок еліптичних і гіпереліптичних кривих [1 – 3].

Використовуючи отримані в [4] результати та запропоновану формалізацію процедури формування псевдовипадкових послідовностей при застосуванні лінійних рекурентних регістрів обґрунтуємо пропозиції щодо реалізації запропонованого методу формування псевдовипадкових послідовностей максимального періоду із використанням перетворень на еліптичних кривих.

Реалізація методу формування псевдовипадкових послідовностей максимального періоду

Запропонований удосконалений метод формування псевдовипадкових послідовностей максимального періоду із використанням перетворень на еліптичних кривих може бути реалізовано у вигляді пристрою, структурна схема якого зображена на рис. 1. Пристрій, який зображено на рис. 1, містить вхід, вихід, блок вводу ключових даних, блок формування початкових станів, перший та другий блоки скалярного множення точок еліптичної кривої, перший та другий блоки формування внутрішніх станів, блок формування вихідної послідовності, блок узгодження. В пристрій також додатково введені (по відношенню до методу-прототипу, який обрано відповідно до специфікації стандарту NIST SP 800-90) блок рекурентного перетворення та блок додавання.

За рахунок додаткового введення рекурентних перетворень, що реалізуються, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками, у сукупності із використанням перетворень у групі точок еліптичної кривої вдається формувати послідовності псевдовипадкових чисел максимального періоду.

Елементи пристрою з'єднанні таким чином.

Вхід пристрою підключено до входу блоку вводу ключових даних, вихід якого підключено до входу блоку формування початкових станів, виходи блоку формування початкових станів підключено до входу блоку рекурентного перетворення та до входу блоку додавання, вихід блоку рекурентного перетворення підключено до входу блоку додавання, вихід якого підключено до входу першого блоку скалярного множення точок еліптичної кривої, вихід блоку скалярного множення точок еліптичної кривої підключено до входу першого блоку формування внутрішніх станів, перший вихід якого підключено до входу боку додавання, а другий вихід підключено до входу другого блоку скалярного множення точок еліптичної кривої, вихід блоку скалярного множення точок еліптичної кривої підключено до входу другого блоку формування внутрішніх станів, вихід якого підключено до входу блоку формування вихідної послідовності, виходом пристрою є вихід блоку формування вихідної послідовності, а окремі виходи блоку узгодження підключено до окремих входів блоку вводу ключових даних, блоку формування початкових станів, першого та другого блоків скалярного множення точок еліптичної кривої, першого та другого блоку формування внутрішніх станів, блоку формування вихідної послідовності, блоку рекурентного перетворення та блоку додавання, відповідно.

Пристрій функціонує таким чином.

В блок вводу ключових даних вводиться послідовність Key, яка виступає у якості секретного ключа. Вона передається у блок формування початкових станів, який призначений для ініціювання рекурентної функції блока скалярного множення точок еліптичної кривої та рекурентного перетворення, що формує послідовність максимального періоду (наприклад, лінійного рекурентного регістру максимального періоду).

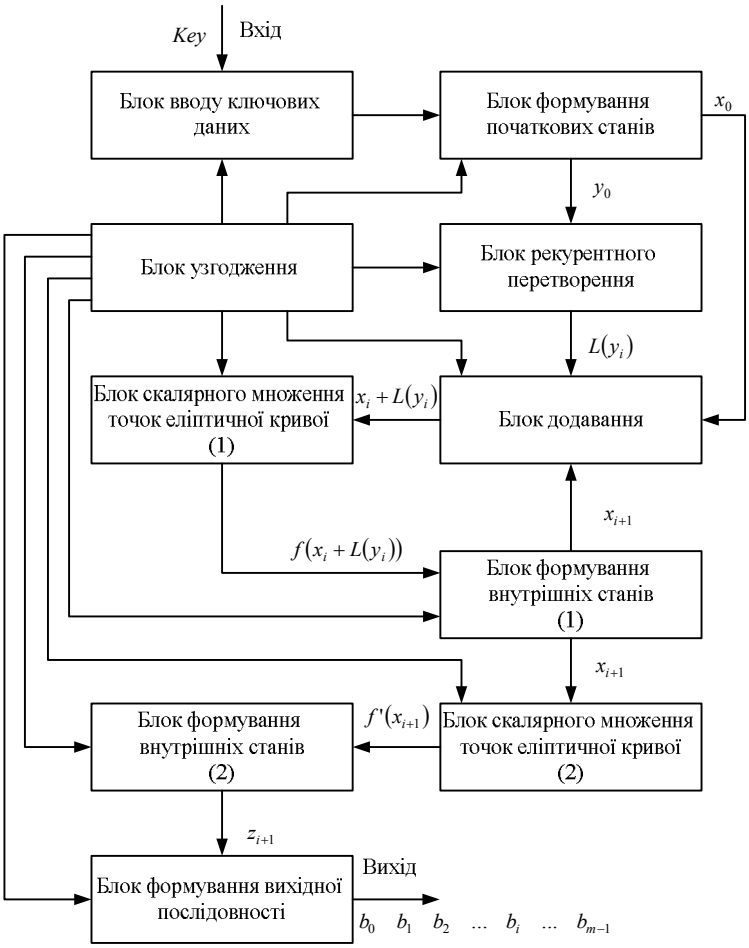

Рис. 1. Структурна схема пристрою формування псевдовипадкових послідовностей максимального періоду із використанням перетворень у групі точок еліптичної кривої

Сформовані початкові стани x_0 та y_0 подаються на входи відповідних пристроїв: значення y_0 подається на блок рекурентного перетворення (наприклад, шляхом заповнення лінійного рекурентного регістру); значення x_0 подається на блок додавання, на другий вхід якого подається значення, зняте з виходу блока рекурентного перетворення $L(y_i)$ (на першій ітерації з виходу блока рекурентного перетворення може бути зчитане значення $L(y_0) = y_0$ як стан лінійного рекурентного регістру).

Блок додавання формує суму $L(y_i) + x_i$, значення якої подається на перший блок скалярного множення точок еліптичної кривої.

У блоку скалярного множення точок еліптичної кривої розраховується значення

$$P'_i = f(x_i + L(y_i)) = (x_i + L(y_i)) \cdot P,$$

яке подається на вхід першого блоку формування внутрішніх станів.

В блоку формування внутрішніх станів виконується функціональне перетворення

$$x_i = \phi(P'_i) = \phi((x_{i-1} + L(y_{i-1})) \cdot P),$$

виходом якого є нове значення внутрішнього стану x_{i+1}, яке подається на блок додавання та на другий блок скалярного множення точок еліптичної кривої.

У другому блоку скалярного множення точок еліптичної кривої обчислюється значення

$$f'(x_{x+1}) = x_{i+1} \cdot Q = Q'_{i+1},$$

яке подається на другий блок формування внутрішніх станів.

У цьому блоку формується значення

$$z_{i+1} = \phi(x_{i+1} \cdot Q) = \\ = \phi(\phi((x_{i-1} + LRR(y_{i-1}))P)Q),$$

яке подається на блок формування вихідної послідовності.

В блоку формування вихідної послідовності зі значення z_{i+1} зчитується найменш значущій біт даних (біт парності), який подається на вихід пристрою як елемент псевдовипадкової послідовності.

Наступна ітерація роботи пристрою починається з подання на блок додавання з першого блоку формування внутрішніх станів значення x_{i+1}.

Одночасно, блок рекурентного перетворення формує наступне значення $L(y_{i+1})$ (наприклад, шляхом виконання процедури зсуву у лінійному регістрі) та видачі отриманого значення, яке також подається на блок додавання.

Блок додавання формує суму $L(y_{i+1}) + x_{i+1}$, яка подається на перший блок скалярного множення точок еліптичної кривої і операція повторюється.

Блок узгодження призначений для погодження роботи окремих блоків пристрою та управління процесом формування псевдовипадкової послідовності.

Пристрій зупиняє свою роботу за командою блоку узгодження (зупинку можна здійснити на кожному кроку).

Висновки

Таким чином, в результаті роботи запропонованого пристрою формування послідовностей псевдовипадкових чисел за рахунок додаткового введення блоку рекурентних перетворень, що реалізуються, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками, та блоку додавання у сукупності із використанням перетворень у групі точок еліптичної кривої вдається формувати послідовності псевдовипадкових чисел максимального періоду.

Список літератури

1. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography – CRC Press, 1997. – 794 p.

2. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004 - Version 0.15 (beta), Springer-Verlag. – 829 p.

3. Barker E. Recommendation for random number generation using deterministic random bit generators / E. Barker, J. Kelsey, National Institute of Standards and Technology, January 2012, 124 p. – Attached to: http://csrc.nist.gov/ publications/nistpubs/800-90A/SP800-90A.pdf.

4. Прокопович-Ткаченко Д.І. Метод формування псевдовипадкових послідовностей максимального періоду із використанням перетворень на еліптичних кривих / Д.І. Прокопович-Ткаченко // Системи обробки ынформацыї. – Х.: ХУПС, 2013. – № 2 (109). – С. 197-203.

Надійшла до редколегії 30.03.2013

Рецензент: д-р техн. наук, проф. О.О. Кузнецов, Харківський національний університет радіоелектроніки, Харків.

РЕАЛИЗАЦИЯ МЕТОДА ФОРМИРОВАНИЯ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ МАКСИМАЛЬНОГО ПЕРИОДА С ИСПОЛЬЗОВАНИЕМ ПРЕОБРАЗОВАНИЙ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Д.И. Прокопович-Ткаченко

Рассматривается реализация метода формирования псевдослучайных последовательностей максимального периода с применением пробразований в группе точек эллиптических кривых (в соответствии с усовершенствованным методом на основе стандарта NIST SP 800-90) для построения механизмов повышения безопасности информационных систем и технологий.

Ключевые слова: *безопасность, генератор, псевдослучайная последовательность.*

REALIZATION OF METHOD OF FORMING OF PSEUDOCASUAL SEQUENCES OF MAXIMAL PERIOD WITH THE USE OF TRANSFORMATIONS ON ELLIPTIC CURVES

D.I. Prokopovich-Tkachenko

Realization of method of forming of pseudocasual sequences of maximal period is examined with the use of пробразований in the group of points of elliptic curves (in accordance with the improved method on the basis of standard of NIST SP 800-90) for the construction of mechanisms of increase of safety of the informative systems and technologies.

Keywords: *safety, generator, pseudocasual sequence.*