УДК 681. 3. 06

АНАЛІЗ АЛГОРИТМІВ ПОБУДОВИ ПАРАМЕТРІВ ДЛЯ КРИПТОСИСТЕМ НА ЕЛІПТИЧНИХ КРИВИХ

О.Є. Ілясова, Харківський банківський інститут УАБС

Криптографічні системи на еліптичних кривих набули поширеного використання в різних криптографічних додатках завдяки забезпеченню належного захисту при достатньо малій, в порівнянні з другими системами, довжині ключа. Генерація загальносистемних параметрів криптосистеми є початковим етапом її використання. До параметрів криптосистеми, яка базується на перетвореннях в групі точок еліптичних кривих, належать параметри рівняння кривої та її порядок. Для забезпечення необхідного рівня стійкості параметри повинні задовольняти наступним умовам: порядок кривої повинен бути великим простим числом, параметри рівняння кривої повинні бути випадковими числами, обчислювальна складність перетворень має бути поліноміальною. Таким чином, виникає задача пошуку недетермінованого алгоритму з поліноміальною обчислювальною складністю, який забезпечував би генерацію криптостійких до відомих атак загальносистемних параметрів. В Україні розроблено стандарт цифрового підпису ДСТУ 4145-2002, що базується на перетвореннях в групі точок еліптичних кривих, які визначені над полем $GF(2^m)$. Згідно з даним стандартом необхідно виконати генерацію параметрів. Це можливо за рахунок використання алгоритму "комплексного множення". Цей алгоритм починається з вибору великого простого числа p так, щоб система мала

необхідний рівень безпеки. Другим кроком є обчислення параметрів рівняння еліптичної кривої. Недоліком вищенаведеного алгоритму є достатньо велика обчислювальна складність побудови мінімального полінома j - інваріанта кривої та пошук його дійсного кореня. Обчислення коефіцієнтів рівняння кривої виконується за умови, що корінь полінома відомий. Після цього перевіряється, чи має побудована крива заздалегідь заданий порядок. Перевірка пов'язана з обчислювальною складністю для поля GF(2^m), де m - велике число.

В зв'язку з цим в даній роботі обгрунтовано необхідність заміни алгоритму "комплексного множення" на інший, який був би більш ефективним за часом, оптимальним за обчислювальною складністю, а також знаходив порядок випадкової еліптичної кривої над вказаним полем. Для цього було проаналізовано три відомих алгоритма: Р. Скуфа, SEA, Т. Сатоха. Результат аналізу показав, що алгоритм Р. Скуфа хоча і має поліноміальну складність, але його практична реалізація займає багато часу. Наприклад, для поля в 2000 біт час реалізації складає 1500 годин. Алгоритм SEA в порівнянні з алгоритмом Р. Скуфа має значну перевагу в часі лише для полів GF(p^m), де $p \geq 3$, але ця умова не відповідає прийнятим в Україні стандартам. І саме алгоритм Т. Сатоха дозволяє обчислювати порядок випадково генерованої еліптичної кривої та є одним з швидких за часом алгоритмів. Його було розроблено для полів GF(p^m), але його можна використовувати і над полем GF(2^m). В результаті програмна реалізація алгоритму дозволить обчислювати порядок еліптичних кривих з випадковими коефіцієнтами з мінімальною за часом складністю. А сам алгоритм можна застосувати при розробці нового стандарту.