СТАТИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

А.В. ГЕМБИЦКИЙ, С.Б. САЛОМАТИН

В задачах защиты информации применяются преобразования на эллиптических кривых (ЭК), которые используют в качестве базовой, операцию умножения точки P ЭК E на число k. Принцип генератора ПСП на эллиптических преобразованиях состоит в последовательном вычислении координат точек, путем суммирования начальной точки с другой точкой (базовой) либо в многократном умножении начальной точки на скаляр. Вычисления могут осуществляться как в аффинных, так и в проективных координатах. Выход ПСП формируется путем конкатенации отдельных или нескольких координат точек, получаемых на каждом шаге работы генератора.

Для тестирования генераторов ПСП был использован статистический пакет NIST STS (NIST Statistical Test Suite). В пакет NIST STS входит 16 статистических тестов, которые в зависимости от входных параметров позволяют получить 189 значений вероятности.

Суть тестирования сводилась к получению с помощью специальной функции и статистики теста значения вероятности, лежащего в диапазоне от 0 до 1. Полученное значение вероятности сравнивалось с уровнем значимости равным 0.01. Если значение вероятности превышало этот уровень, то принималось решение о случайности тестируемой последовательности. Эффективность тестирования оценивалась как проценты прохождения последовательностями тестов и количество тестов, результаты которых превысили соответствующую долю. Результаты тестирования сравнивались с показателями генератора ПСП типа BBS.

Для генератора ПСП на эллиптических преобразованиях минимальное значение вероятности составило 0.96 при проверке неперекрывающихся шаблонов, тогда как для генератора BBS — 0.9403 при проверке случайных отклонений. Генератор на эллиптических преобразованиях проходит тест при установлении порога в 96% последовательностей, тогда как генератор BBS требует порога в 94 %, что свидетельствует о некотором преимуществе генератора на эллиптических преобразованиях и позволяет рекомендовать его для практического применения.