СВОЙСТВА И ФОРМИРОВАНИЕ ДВОИЧНЫХ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ЛЕЖАНДРА И ЯКОБИ

В.А. ЛИПНИЦКИЙ, О.В. ФОЛОМЕЕВА

Двоичные последовательности, обладающие хорошими периодическими и апериодическими корреляционными свойствами, играют важную роль в системах связи (системах синхронизации, передачи информации, локации), а также в защите информации от несанкционированного доступа. За последние десятилетия открыто множество типов таких последовательностей. Все они относятся к классу так называемых кодовых последовательностей (КП).

Особый интерес представляют последовательности, обладающие идеальной двузначной периодической автокорреляционной функцией (ПАКФ). Такими КП являются М-последовательности, ГМВ-последовательности, последовательности квадратичных вычетов и модифицированные последовательности Якоби длины $p(p+2)$, где p — простое число. Последние два типа последовательностей принадлежат к более общим классам КП — таким как последовательности Лежандра и модифицированные последовательности Якоби. В данной работе основное внимание уделяется именно этим типам КП.

Последовательности Лежандра существуют для любой длины L, где L — простое число, модифицированные последовательности Якоби существуют для любой длины $L=pq$, где p и q — простые числа. Последовательности Лежандра длины $L \equiv 3 \bmod 4$, называемые квадратично-вычетными, обладают идеальной двузначной ПАКФ, также эти КП имеют высокую линейную сложность. Модифицированные последовательности Якоби длины $L=pq$, где $q=p+2$, т.е. p и q являются простыми числами-близнецами, также обладают идеальной двузначной ПАКФ.

В данной работе проведена оценка мощности названных последовательностей Лежандра и Якоби, систематизированы методы формирования этих последовательностей, дана оценка степени вычислительной сложности рассмотренных методов, предложены компьютерные реализации наиболее эффективных методов.