КОРРЕЛЯЦИОННЫЕ СВОЙСТВА КРИПТОАЛГОРИТМА RIJNDAEL

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Музыченко М.В

Бильдюк Д.М. –ассист.

В системах связи , сбора и передачи информации широкое распространение получили методы расширения спектра сигналов. Одним из эффективных методов расширения спектра, при котором сигнал-переносчик информации занимает широкую полосу частот, является метод непосредственной модуляции несущей псевдослучайной последовательностью. При этом методе расширение спектра дополнительная модуляция несущей сигнала никак не связана с передаваемой информацией.

В данной работе были исследованы корреляционные свойства: М-последовательности, ЧКП, коды Касами, криптоалгоритм Rijndael.

Самая лучшая апериодическая АКФ найдена у М-последовательности, а периодическая АКФ - у ЧКП (в районе порога нет шума).

В процессе исследования было выяснено, что криптоалгоритм Rijndael совпадает с корреляционными функциями по боковым лепесткам по случайным последовательностям. Хоть Rijndael и имеет большой недостаток - высокий уровень боковых лепестков, но он имеет большие преимущества, которые не имеют другие последовательности. А именно: за счет криптографических свойств у него произвольная длина, обладает высокой структурной скрытностью.

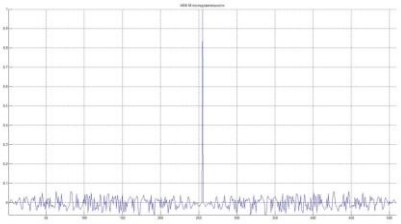

Рис. 1 – Апериодическая АКФ М-последовательности

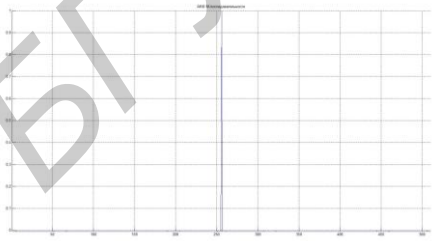

Рис. 2 – Периодическая АКФ М-последовательности

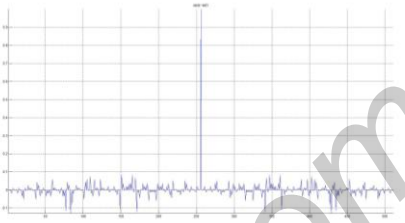

Рис. 3 – Апериодическая АКФ ЧКП

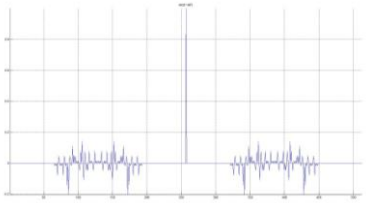

Рис. 4 – Периодическая АКФ ЧКП

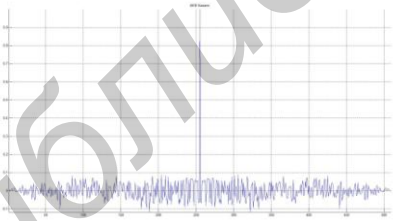

Рис. 5 – Апериодическая АКФ Касами

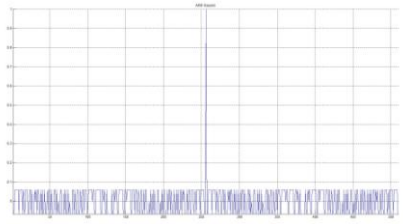

Рис. 6 – Периодическая АКФ Касами

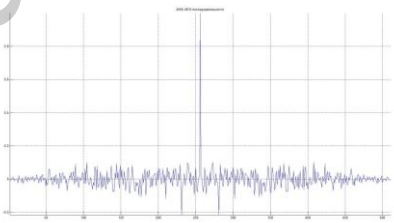

Рис. 7 – Апериодическая АКФ Rijndael

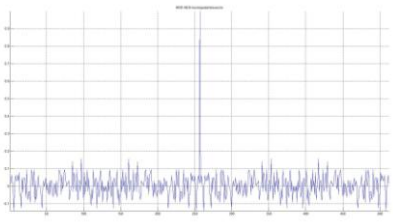

Рис. 8 – Периодическая АКФ Rijndael

Список использованных источников:

1. Варакин Л.Е. Системы связи с шумоподобными сигналами