

В. Канцель и И. Кантер предложили использовать нейронные сети для передачи ключей между удаленными нейронными сетями.

Разработана практическая компьютерная модель функционирования двух нейронных сетей по обмену секретными ключами. Проведены компьютерные испытания данной модели с исследованием возможностей подключения третьей несанкционированной сети. Получены обнадеживающие результаты в криптостойкости данной модели.

ОБ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЯХ НАД ПОЛЯМИ ГАЛУА

В.А. БОГРЕЦОВ, В.А. ЛИПНИЦКИЙ

Проблема решения алгебраических уравнений привлекает внимание научного общества едва ли не с зари человеческой цивилизации. Усилиями Дж. Кардано, К.Ф. Гаусса, Н.Х. Абеля, Э. Галуа и многих других, казалось бы, поставлена точка в этом вопросе. Но решать алгебраические уравнения приходится. При этом привлекаются или методы численного анализа или аппарат специальных функций. Вынужденная специализация полей, из которых берутся коэффициенты уравнений и их корни, возникшая из конкретных задач XX века, привнесла в данную проблему новые сложности.

Проблемы коррекции многократных ошибок, обработки сигналов и изображений, современной физики и генетики привели в 70-е годы XX века к необходимости решения уравнений над конечными полями. Выяснилось, что теория уравнений над полями Галуа практически отсутствует, а классические формулы и методы не работают.

В докладе обсуждаются результаты систематизации подходов и методов решения уравнений над полями Галуа. Предложены компьютерные реализации методов Чэня и формул Чэня, сведения к системам линейных уравнений, модификаций метода Фаддеева–Берлекемпа, нормального метода.

Разработанные программные средства могут быть полезны в приложениях, где требуется практическое решение уравнений над полями Галуа.

ALGORITHMS OF FAST WALSH-TRAHTMAN TRANSFORM

A.A. BUDZKO, O.M.H. ALMIAHI

Walsh functions can be ordered in different ways. But for practical applications it is interesting only symmetrical systems of ordering, like well known Hadamard, Paley, Kachmaz and Trahtman. The main purpose of this report is to introduce the definition of Trahtman system of ordering of Walsh functions. Here is considered representation of Walsh functions in matrix form. The construction of Walsh-Trahtman matrix any size is derived by the mirror imaging rule and can be obtained using recurrent formula which is considered. To obtain any element of Walsh-Trahtman matrix exponent formula is derived. This formula can be used for construction of Walsh function generators of different types and for deriving algorithms of fast Walsh transform. In the report a lot of attention paid to how to derive the «wonderful» algorithms of fast Walsh transform and proposed most interesting.