Караман Д. Г. Україна, Харків

ОСОБЛИВОСТІ АПАРАТНОЇ РЕАЛІЗАЦІЇ СИМЕТРИЧНОГО АЛГОРИТМУ ШИФРУВАННЯ RIJNDAEL

У доповіді розглянуті основні перепони та шляхи їх подолання, які виникають при апаратній реалізації одного з найсильніших алгоритмів шифрування. Подано короткий опис алгоритму, пояснюється принцип його роботи, а також приводяться його можливості і вимоги, висунуті до нього. Наведена одна з можливих структур, адаптована для реалізації на ПЛІС, описані методи апаратного виконання окремих її блоків. Аналізується вибір того чи іншого методу з точки зору продуктивності та оптимальності реалізації.

Караман Д. Г. Украина, Харьков

ОСОБЕННОСТИ АППАРАТНОЙ РЕАЛИЗАЦИИ СИММЕТРИЧНОГО АЛГОРИТМА ШИФРОВАНИЯ RIJNDAEL

В докладе рассматриваются основные препятствия и пути их преодоления при аппаратной реализации одного из самых сильных алгоритмов шифрования. Дается краткое описание алгоритма, объясняется принцип его работы, а так же приводятся его возможности и требования, предъявляемые к нему. Представлена одна из возможных структур, адаптированная для реализации на ПЛИС, описаны методы аппаратного исполнения отдельных ее блоков. Анализируется выбор того или иного метода с точки зрения производительности и оптимальности реализации.

Karaman D. G. Ukraine, Kharkiv

SYMMETRIC ENCRYPTION ALGORITHM RIJNDAEL HARDWARE IMPLEMENTATION FEATURES

In the report common hardware implementation difficulties of one of the strongest encryption algorithms and the ways to solve them are considered. Brief algorithm description is given, principle of its operation is explained and the capabilities of the algorithm as well as its requirements are specified. One of the most probable structures for FPGA implementation is shown; methods for particular blocks hardware implementations are explained. The performance and design optimality of chosen methods are analyzed.