Дербунович Л.В., Гормакова І.В., Україна, Харків

МЕТОДИ СИНТЕЗУ АРИФМЕТИЧНИХ МОДУЛІВ ТА ЇХ ПРАКТИЧНЕ ВИКОРИСТАННЯ

У докладі розлянуті методи синтезу арифметичних модулів, що оперують в полях Галуа, та їх практичне використання в криптосистемах, а також кодуючих та декодуючих пристроях. Дано порівняння розглянутих методів за наступними пунктами: апаратні витрати при реалізації, швидкодія, складніть схеми.

Дербунович Л.В., Гормакова И.В., Украина, Харьков

МЕТОДЫ СИНТЕЗА АРИФМЕТИЧЕСКИХ МОДУЛЕЙ И ИХ ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ

В докладе рассмотрены методы синтеза арифметических модулей, которые опрерируют в полях Галуа, и их практическое применение в криптосистемах, а также кодирующих и декодирующих устройствах. Дано сравнение рассмотренных методов по следующим пунктам: аппаратные затраты при реализации, быстродействие, сложность схемы.

Derbunovych L.V., Gormakova I.V. Ukraine, Kharkiv

THE METHODS OF DESIGNING ARITHMETIC UNITS AND THEIR PRACTICE APPLICATIONS

In the report, the methods of the designing arithmetic units operating in Galois field and their practice applications in cryptosystems and coding/decoding devices are considered. The comparison of considered methods in the following terms: hardware applications, speed and circuit complexity are given.