УДК 004.351

Н. А. Гайнулин

Раундовые функции легковесных блочных шифров

Аннотация. В докладе кратко рассматриваются методы применяемые при построении раундовых преобразований современных "легковесных" блочных шифров. Автор уделяет особое внимание шифрам SIMON и SPECK, которые были представлены широкой общественности в 2013 году исследовательским отделом АНБ США. Приводятся основные результаты, отражающие криптографические свойства функций перестановки данных шифров. В частности приводятся результаты со значением значение нелинейности S-блока шифра SIMON и другими характеристиками раундовой функции. Рассматривается возможность применения вычислительной техники при построении функций, которые будут обладать необходимыми криптографическими свойствами.

Ключевые слова: раундовые преобразования, шифр SIMON, шифр SPEK, S-блок, криптографические свойства.